



Cisco Crosswork Optimization Engine 1.0 User Guide

First Published: 2019-08-06

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



CONTENTS

CHAPTER 1	Overview of Cisco Crosswork Optimization Engine	1
	Audience	1
	Overview of Cisco Crosswork Optimization Engine	1
	Segment Routing Path Computation Element (SR-PCE)	2
	Log In and Log Out	2
	Crosswork Optimization Engine Home Page	4
	Set, Sort and Filter Table Data	6

CHAPTER 2	Get Started	9
	Basic Concepts	9
	Segment Routing	9
	Inventory Management Concepts	11
	Before You Begin	11
	High-Level Workflows	12
	Workflow: Auto-Onboard Devices	13
	Workflow: Manually Import Devices	14

CHAPTER 3	Manage Inventory	17
	Inventory Management Overview	17
	About Adding Devices	17
	Prerequisites for Onboarding Devices	19
	Sample Configuration for Devices in Cisco NSO	20
	Reachability and Operational State	21
	Manage Credential Profiles	23
	Create Credential Profiles	24
	Import Credential Profiles	26

- Edit Credential Profiles 28
- Delete Credential Profiles 28
- Export Credential Profiles 29
- Change a Device's Credential Profile 29
- Change the Credential Profile for Multiple Devices 30
- Manage Providers 30
 - Add Cisco SR-PCE Providers 32
 - Auto-Onboard Property Descriptions 34
 - Cisco SR-PCE Reachability Issues 35
 - Multiple Cisco SR-PCEs 35
 - Add Cisco NSO Providers 37
 - Import Providers 38
 - Get Provider Details 40
 - Edit Providers 41
 - Delete Providers 41
 - Export Providers 42
 - View Devices Assigned to a Provider 42
- Manage Devices 43
 - Import Devices 44
 - Add Devices Through the UI 46
 - Get Device Details 51
 - Filter Devices by Tags 53
 - Edit Devices 53
 - Delete Devices 54
 - Export Devices 54
 - View Device Job History 55
- Manage Tags 56
 - Create Tags 57
 - Import Tags 58
 - Apply or Remove Device Tags 58
 - Delete Tags 59
 - Export Tags 59

CHAPTER 4 **Visualize the Network 61**

Network Topology Map	61
Troubleshoot Network Topology Map	63
Device and Link Icons	64
Configure Geographical Map Settings	65
Change the Layout of a Logical Map	65
Create Custom Map Views	66
Manage Custom Map Views	67
Visualize Devices	68
Get More Information About Devices on the Map	68
Access the Device Console	69
Identify the Members of a Cluster	70
Visualize Links	71
Get More Information About Links	71
Show Bandwidth Utilization for Links on the Map	73
Define Color Thresholds for Link Bandwidth Utilization	73

CHAPTER 5

Visualize and Manage SR Policies	75
SR Policies Topology Map	75
SR Policies Table	77
SR Policy Configuration Sources	79
Visualize SR Policies	80
Visualize SR Policies Example	80
Highlight an SR Policy on the Map	86
Identify Segment Hops	86
Show Participating Nodes and Links	86
Show IGP, Delay, and Traffic Engineering Metrics	86
Create and Manage SR Policies	87
Configure Affinity Mapping	87
Create Explicit Path SR Policies	88
Create Dynamic Path SR Policies	91
Preview Disjoint Policies	94
View SR Policies Belonging to a Disjoint Group	97
Modify SR Policies	97
Get More Information About an SR Policy	98

CHAPTER 6**Perform Administrative Tasks 103**

Manage Users 103

Administrative Users Created During Installation 103

Add Users 104

Edit Users 104

Delete Users 105

Create User Roles 105

Edit User Roles 106

Clone User Roles 106

Delete User Roles 107

Manage TACACS+ Servers 107

Add a TACACS+ Server 107

Edit a TACACS+ Server 108

Delete a TACACS+ Server 108

Define Network Topology Display Settings 108

Manage Certificates 109

Extend Self-Signed Certificate Expiration 110

Substitute a User-Provided Certificate 110

Manage Cisco Crosswork Network Automation 111

Monitor Cisco Crosswork Network Automation Functions in Real Time 114

Collect and Share Cisco Crosswork Network Automation Logs and Metrics 118

Control Cisco Crosswork Network Automation Applications and Services 119

Security Hardening Overview 120

Core Security Concepts 120

HTTPS 120

SSL Certificates 121

1-Way SSL Authentication 121

Disable Insecure Ports and Services 122

Harden Your Storage 123

CHAPTER 7**Configure Collection 125**

Collection Service Overview 125

Collection Modes 125

Prerequisites for Device Telemetry	126
List of Supported MIBs and MDT Model	128

CHAPTER 8

Get Started with Function Packs	129
Install Function Packs	129
Update Network Configuration for Function Packs	131
Bandwidth on Demand	131
Important Notes and Limitation for BWoD	132
Configure Bandwidth on Demand	132
Create Bandwidth on Demand SR Policies	134
Troubleshoot BWoD	136
Bandwidth Optimization	136
Important Notes and Limitations for BWOpt	137
Configure Bandwidth Optimization	137
Bandwidth Optimization Example	139
Troubleshoot BWOpt	141



CHAPTER 1

Overview of Cisco Crosswork Optimization Engine

This section mainly describes what Cisco Crosswork Optimization Engine does and how to navigate the main user interface. To quickly get started, you should understand some basic concepts and look over the high-level workflows described in [Get Started, on page 9](#).

The following topics are addressed in this section:

- [Audience, on page 1](#)
- [Overview of Cisco Crosswork Optimization Engine, on page 1](#)
- [Segment Routing Path Computation Element \(SR-PCE\), on page 2](#)
- [Log In and Log Out, on page 2](#)
- [Crosswork Optimization Engine Home Page, on page 4](#)
- [Set, Sort and Filter Table Data, on page 6](#)

Audience

This guide is for experienced network administrators who want to use Cisco Crosswork Optimization Engine in their network. This guide assumes that you are familiar with the following topics:

- Networking technologies and protocols (BGP-LS, IGP (OSPF and IS-IS), PCEP, model-driven telemetry, and so on)
- Cisco IOS XR Traffic Controller (XTC) or Segment Routing Path Computation Element (SR-PCE) functionality
- Segment routing (SR) and SR policy provisioning

Overview of Cisco Crosswork Optimization Engine

Cisco Crosswork Optimization Engine is part of the Cisco Crosswork Network Automation suite of products. Cisco Crosswork Optimization Engine provides real-time network optimization allowing operators to effectively maximize network utilization as well as increase service velocity.

Crosswork Optimization Engine provides the following:

- A topology map that gives valuable real-time visualization of devices, links, link utilization, and Segment Routing (SR) policies in the network.
- A UI that allows for easy manageability of SR policies. Crosswork Optimization Engine enables the network operator to perform the following tasks:
 - Provision SR policies and modify or remove them using an intuitive workflow
 - Continuously track SR policy dynamic path computations to maintain SLA objectives
 - Preview an SR policy before deploying it to the network
- Crosswork Optimization Engine function packs (with correct licensing) that provide closed-loop optimization to define the optimization intent, implement the intent, and continuously monitor, track, and react to maintain the original intent.
- A framework that enables other function packs that can be developed in the field to support additional use cases that are not available out of the box. By leveraging SDKs and APIs, network operators can build additional function packs to support more optimization workflows.



Note To get a quick overview on how to start using Crosswork Optimization Engine, see [High-Level Workflows, on page 12](#).

Segment Routing Path Computation Element (SR-PCE)

Crosswork Optimization Engine uses the combination of telemetry and Cisco Segment Routing Path Computation Element (SR-PCE) to analyze and compute optimal SR policy paths.

Cisco SR-PCE (formerly Cisco XR Traffic Controller (XTC)) runs on the Cisco IOS XR operating system. SR-PCE provides stateful PCE functionality that helps control and move SR policies to optimize the network. PCE describes a set of procedures by which a Path Computation Client (PCC) can report and delegate control of head-end tunnels sourced from the PCC to a PCE peer. The PCC and PCE establish a Path Computation Element Communication Protocol (PCEP) connection that SR-PCE uses to push updates to the network.

Crosswork Optimization Engine discovers all devices that are part of the IGP domain including those that do not establish PCEP peering with SR-PCE. However, PCEP peering is required to deploy SR policies to the device.

Log In and Log Out

The Cisco Crosswork Optimization Engine user interface is browser based. See the *Cisco Crosswork Optimization Engine Installation Guide* for supported browser versions.

Step 1 Open a web browser and enter:

`https://<CrossworkVMManagementIPAddress>:30603/`

Step 2 The Cisco Crosswork Optimization Engine browser-based user interface displays the login window. Enter your username and password.

Figure 1: Cisco Crosswork Optimization Engine Log In Window



Note The default Cisco Crosswork Optimization Engine administrator user name and password is **admin**. This account is created automatically at installation (see [Administrative Users Created During Installation, on page 103](#)). The initial password for this account must be changed during installation verification. Cisco strongly recommends that you keep the default administrator credential secure, and never use it for routine logins. Instead, create new user accounts with appropriate privileges and their own credentials (as explained in [Add Users, on page 104](#)) and use only those accounts for all subsequent user logins.

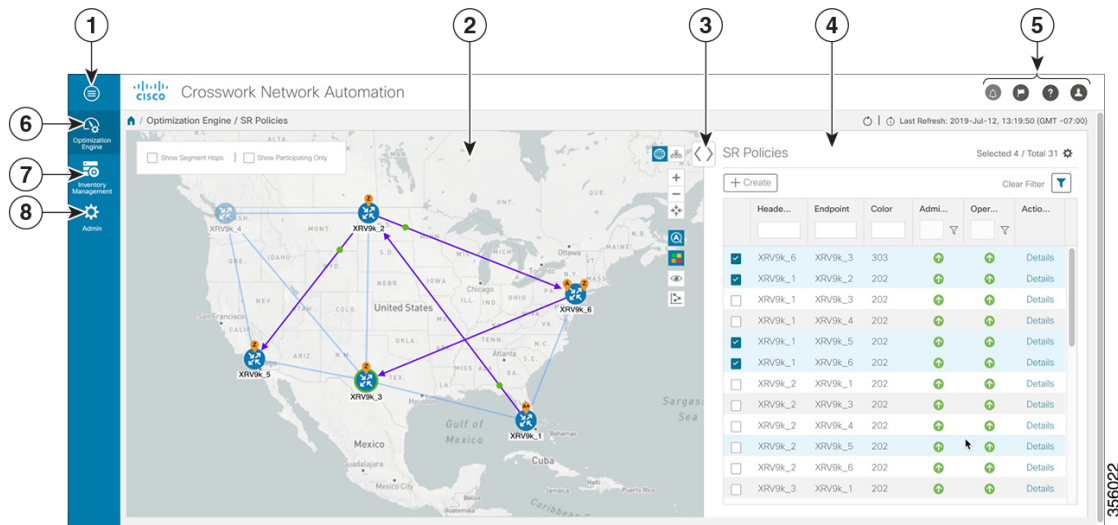
Step 3 Click **Log In**.

When you access Cisco Crosswork Optimization Engine from your browser for the first time, some browsers display a warning that the site is untrusted. When this happens, follow the prompts to add a security exception and download the self-signed certificate from the server. After you do this, the browser accepts the Cisco Crosswork Optimization Engine server as a trusted site in all subsequent logins.





Step 4 To log out, click  in the top right of the Cisco Crosswork Optimization Engine main window and choose **Log out**.

Crosswork Optimization Engine Home Page

Figure 2: Crosswork Optimization Engine Home Page



Callout No.	Description
1	<p>More: Toggles the main menu to compact mode or expanded mode.</p> <p>In compact mode, you must hover over the main menu items to view and select available options.</p> <p>In expanded mode, you must click on the main menu item to display the available options. In this mode, when a main menu item is expanded, it will remain so until you collapse the menu item.</p>
2	<p>Network Topology Map: Displays a geographical or logical map view of the devices, links, and SR policies in your network. It also shows the general condition of devices and links. See Visualize the Network, on page 61.</p> <p>In conjunction with the SR Policies Table, on page 77, it quickly highlights selected SR policies and associated SR policy information such as metrics, adjacency segment IDs, segment hops, source and destination nodes. See Visualize and Manage SR Policies, on page 75.</p>
3	<p>Expand/Collapse/Hide Side Panel: Expand or collapse the contents of the side panel. Close the side panel to get a larger view of the topology map.</p>


Callout No.	Description
4	<p>The SR Policies Table, on page 77 (Optimization Engine > SR Policies) is shown by default. The content of this panel changes depending on what is selected on the topology map, or whether you are in the process of viewing and managing SR policies. You can do the following:</p> <ul style="list-style-type: none"> • Create and Manage SR Policies, on page 87 • Get More Information About an SR Policy, on page 98 • Get More Information About Devices on the Map, on page 68 • Get More Information About Links, on page 71
5	<p>Settings icons:</p> <p> The Alerts icon notifies you of any current error conditions related to the system operations which require attention, and provides a link to detailed information about those conditions.</p> <p> The Events icon notifies you of new events related to system operation, and also provides access to the history of all system events.</p> <p> The About icon displays the current version of Crosswork Optimization Engine.</p> <p> The User Account icon lets you view your username, change your password, and log out.</p>
6	<p>Optimization Engine Menu: You can access the following SR policy related options:</p> <ul style="list-style-type: none"> • SR Policies—Returns you to the main window as shown above. • Affinity Mapping—Lets you map an affinity to a bit position. See Configure Affinity Mapping, on page 87. • Function Packs—Lets you enable and configure function packs. See Get Started with Function Packs, on page 129.
7	<p>Inventory Management Menu: You can access the following inventory related options:</p> <ul style="list-style-type: none"> • Devices—Lets you add, update and view information about the devices in your network. See Manage Devices, on page 43. • Providers—Lets you add, update and manage providers. See Manage Providers, on page 30. • Credentials—Lets you add, update and manage credential profiles that control access to devices and providers. See Manage Credential Profiles, on page 23. • Tags—Lets you add, update and manage the tags you use to sort and group devices. See Manage Tags, on page 56. • Job History—Lets you review device related jobs. See View Device Job History, on page 55.

Callout No.	Description
8	<p>Admin Menu: You can access the following administrative related options:</p> <ul style="list-style-type: none"> • Crosswork Manager—Lets you do the following tasks: <ul style="list-style-type: none"> • Collect logs and metrics. See Collect and Share Cisco Crosswork Network Automation Logs and Metrics, on page 118. • Monitor the general state of containers. See Monitor Cisco Crosswork Network Automation Functions in Real Time, on page 114. • Control (stop, start, or restart) services. See Control Cisco Crosswork Network Automation Applications and Services, on page 119. • Users—Lets you add, update and view users and roles. See Manage Users, on page 103. • AAA—Lets you add, update and view TACACS+ servers to authenticate users. See Manage TACACS+ Servers, on page 107. • Visualization Settings—Lets you update topology map settings. See Configure Geographical Map Settings, on page 65 and Define Color Thresholds for Link Bandwidth Utilization, on page 73. • Certificate Management—Lets you view and manage certificates. See Manage Certificates, on page 109.

Set, Sort and Filter Table Data

Many Cisco Crosswork Optimization Engine windows show database records in tables.

Any window with a table will also provide column selection, sorting, and filter functions that let you control the database records shown in the tables and help you locate particular records quickly.

Click  to display a list of all the fields in the database for the kind of data record displayed in the table. You can choose which fields you want to display as table columns by checking or unchecking the box next to any field in the list. Your choices are enabled immediately and are permanent.

For example: In the **Devices** window shown below, we have unchecked the **Reachability State** and **Inventory Key Type** fields. These are normally shown as part of the default **Devices** table, but are now removed. We have also checked the **MAC Address** field, adding it to the table.

Figure 3: Devices Window With MAC Address Column Added

The screenshot shows a 'Devices' window with a table of device records. The table has the following columns: Host Name, Configured State, Operational State, Lock Status, MAC Address, Product Type, and Device Type. A dropdown menu is open over the table, showing filter options: Host Name, Reachability State, Reachability Check, Inventory Key Type, Inventory ID, MAC Address (checked), and UUID. The table contains 12 rows of data.

	Host Name	Configured State	Operational State	Lock Status	MAC Address	Product Type	Device Type
<input type="checkbox"/>	spnac-a9k-s101	UP			0050.56b8.b145	Cisco XRV9000	ROUTER
<input type="checkbox"/>	spnac-a9k-s105	UP			0050.56b8.309f	Cisco XRV9000	ROUTER
<input type="checkbox"/>	spnac-a9k-s106	UP			0050.56b8.295f	Cisco XRV9000	ROUTER
<input type="checkbox"/>	cw-ncs-r1.cisco.com	UP				NCS-5500	ROUTER
<input type="checkbox"/>	cw-ncs-r4.cisco.com	UP				NCS-5500	ROUTER
<input type="checkbox"/>	spnac-a9k-s102	UP			0050.56b8.48d6	Cisco XRV9000	ROUTER
<input type="checkbox"/>	spnac-a9k-s103	UP			0050.56b8.d83f	Cisco XRV9000	ROUTER
<input type="checkbox"/>	spnac-a9k-s104	UP			0050.56b8.ed1a	Cisco XRV9000	ROUTER
<input type="checkbox"/>	cw-ncs-r2.cisco.com	UP				NCS-5500	ROUTER
<input type="checkbox"/>	cw-a9k-r1.cisco.com	UP			00a7.425b.2172	ASR9K	ROUTER

You can also sort all the records displayed in the table according to the data in any one column by clicking that column's title:

- To sort the records in ascending order, click the column title once.
- To sort the records in descending order, click the column title again.

Sorting takes place immediately. You can only have one active sort at a time. The example **Links** window, below, shows an active sort on the **Link Type** field.

You can also filter the table to show only the records you want, using a quick filter or an advanced filter. Many tables have all these features enabled by default. If you cannot see the quick and advanced filter features

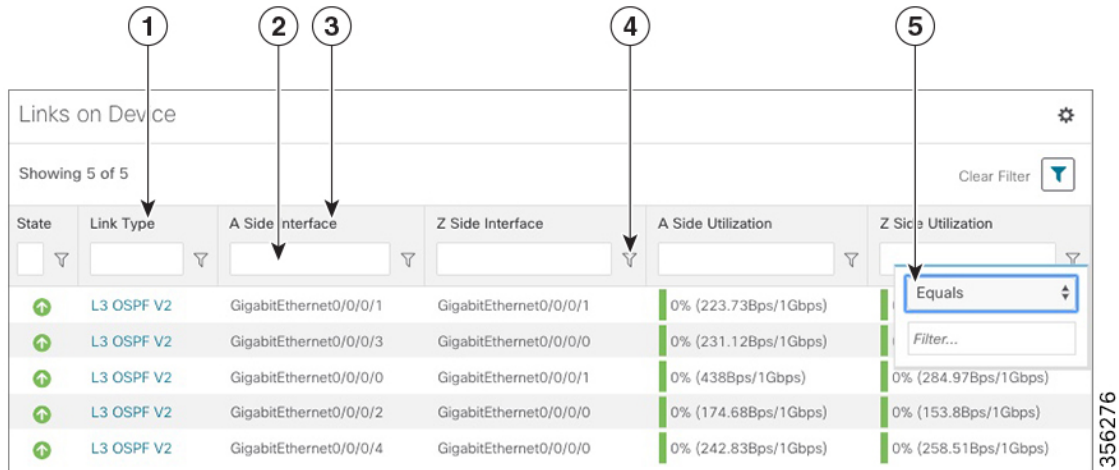
displayed on a window with a table, click



The quick filter displays only the records that match the value you enter above the column in the **quick filter** field (see item 2, below). Filtering takes place immediately, as you type.

The advanced filter narrows the content in the table by applying a filter that includes both a value and a logical operator, such as Equals, Starts with, Contains, and so on. Click in the column header to access the advanced filter (see items 4 and 5, below).

In addition to these quick and advanced filters, you can also use tags to filter the devices shown in the **Devices** window (see [Filter Devices by Tags](#), on page 53).

Figure 4: Links Window With Active Sort and Filters



Item	Description
1	Sort active icon: This arrow icon indicates that the user has sorted the links by clicking on the column header. The arrow's direction shows that the table is sorted by Link Type , in ascending order.
2	Quick filter field: Type a text or numeric value in this field to show only the links that match the value you enter. The field shows the values you entered for both quick and advanced filters.
3	Filter active icon: This icon shows that a quick or advanced filter is currently applied to the data in this column.
4	Advanced filter icon: Click  , shown in each column header, to specify an advanced filter on that column, using logical operators as well as alphanumerical values.
5	<p>Filter criteria fields: These fields appear in a popup next to the column after you click the  icon. Set the filter criteria by selecting the logical operator from the drop down list in the first field, and then entering the filter value in the second field. Your criteria will be applied immediately. You will then be prompted to enter more operators and values, and to decide if you want to concatenate them using logical AND or OR. The quick filter field shows the values you entered (but not the operators). Logical operators include Equals, Not equal, Starts with, Ends with, Contains, and Not contains.</p> <p>Note Some columns will not have all of the logical operators available.</p>



CHAPTER 2

Get Started

This section contains the following topics to help you get started with Crosswork Optimization Engine:

- [Basic Concepts, on page 9](#)
- [Before You Begin, on page 11](#)
- [High-Level Workflows, on page 12](#)

Basic Concepts

Segment Routing

Segment routing is a method of forwarding packets on the network based on the source routing paradigm. The source chooses a path and encodes it in the packet header as an ordered list of segments. Segments are an identifier for any type of instruction. For example, topology segments identify the next hop toward a destination. Each segment is identified by the segment ID (SID) consisting of a flat unsigned 32-bit integer.

Segments

Interior gateway protocol (IGP) distributes two types of segments: prefix segments and adjacency segments. Each router (node) and each link (adjacency) has an associated segment identifier (SID).

- A prefix SID is associated with an IP prefix. The prefix SID is manually configured from the segment routing global block (SRGB) range of labels, and is distributed by IS-IS or OSPF. The prefix segment steers the traffic along the shortest path to its destination. A node SID is a special type of prefix SID that identifies a specific node. It is configured under the loopback interface with the loopback address of the node as the prefix.

A prefix segment is a global segment, so a prefix SID is globally unique within the segment routing domain.

- An adjacency segment is identified by a label called an adjacency SID, which represents a specific adjacency, such as egress interface, to a neighboring router. The adjacency SID is distributed by IS-IS or OSPF. The adjacency segment steers the traffic to a specific adjacency.

An adjacency segment is a local segment, so the adjacency SID is locally unique relative to a specific router.

By combining prefix (node) and adjacency segment IDs in an ordered list, any path within a network can be constructed. At each hop, the top segment is used to identify the next hop. Segments are stacked in order at the top of the packet header. When the top segment contains the identity of another node, the receiving node uses equal cost multipaths (ECMP) to move the packet to the next hop. When the identity is that of the receiving node, the node pops the top segment and performs the task required by the next segment.

Segment Routing for Traffic Engineering

Segment routing for traffic engineering takes place through a tunnel between a source and destination pair. Segment routing for traffic engineering uses the concept of source routing, where the source calculates the path and encodes it in the packet header as a segment. Each segment is an end-to-end path from the source to the destination, and instructs the routers in the provider core network to follow the specified path instead of the shortest path calculated by the IGP. The destination is unaware of the presence of the tunnel.

Segment Routing Policies

Segment routing for traffic engineering uses a “policy” to steer traffic through the network. An SR-TE policy path is expressed as a list of segments that specifies the path, called a segment ID (SID) list. Each segment is an end-to-end path from the source to the destination, and instructs the routers in the network to follow the specified path instead of the shortest path calculated by the IGP. If a packet is steered into an SR-TE policy, the SID list is pushed on the packet by the head-end. The rest of the network executes the instructions embedded in the SID list.



Note Cisco Crosswork Optimization Engine discovers existing SR policies when devices are imported, but cannot manage them. SR policies can be managed only if they were provisioned using Cisco Crosswork Optimization Engine (see [Create and Manage SR Policies, on page 87](#)).

There are two types of SR policies: dynamic and explicit.

Dynamic SR Policy

A dynamic path is based on an optimization objective and a set of constraints. The head-end computes a solution, resulting in a SID-list or a set of SID-lists. When the topology changes, a new path is computed. If the head-end does not have enough information about the topology, the head-end might delegate the computation to a path computation engine (PCE).

Explicit SR Policy

When you configure an explicit policy, you specify an explicit path which consists of a list of prefix or adjacency SIDs, each representing a node or link along on the path.

Disjointness

Cisco Crosswork Optimization Engine uses the disjoint policy to compute two list of segments that steer traffic from two source nodes to two destination nodes along disjoint paths. The disjoint paths can originate from the same head-end or different head-ends. Disjoint level refers to the type of resources that should not be shared by the two computed paths. The following disjoint path computations are supported:

- **Link** – Specifies that links are not shared on the computed paths.
- **Node** – Specifies that nodes are not shared on the computed paths.

- **SRLG** – Specifies that links with the same Share Risk Link Group (SRLG) value are not shared on the computed paths.
- **SRLG-node** – Specifies that SRLG and nodes are not shared on the computed paths.

When the first request is received with a given disjoint-group ID, a list of segments is computed, encoding the shortest path from the first source to the first destination. When the second request is received with the same disjoint-group ID, information received in both requests is used to compute two disjoint paths: one path from the first source to the first destination, and another path from the second source to the second destination. Both paths are computed at the same time. The shortest lists of segments is calculated to steer traffic on the computed paths.

Inventory Management Concepts

Crosswork Optimization Engine makes extensive use of three basic inventory management concepts. It is helpful to be familiar with them before you get started.


- **Tags:** Tags will be familiar from other Web applications. They are simple text strings you can attach to objects to help group them. Crosswork Optimization Engine comes with a short list of ready-made tags used to group network devices. You can create your own tags and use them to identify, find, and group devices for a variety of purposes. For example, in addition to type and geolocation, you may want to identify and group them by their location in your network topology (Spine vs. Leaf), or the function they serve on your network (Provider vs. ProviderEdge). You will want to develop your own tags for your purposes, and rework them as needed to meet changing needs.
- **Providers:** Crosswork Optimization Engine does not perform inventory collection, route segmentation or configuration changes directly. Instead, it relies on an SR-PCE provider to perform these functions. The provider family determines the type of service that provider supplies to Crosswork Optimization Engine, and the parameters unique to that service, which must be configured. This architecture permits Crosswork Optimization Engine to devote all of its resources to processing and interpreting network events and rolling out changes in response to these events.
- **Credential Profiles:** For Crosswork Optimization Engine to be able to access a device or to interact with a provider, it must be able to present credentials. Rather than entering credentials each time they are needed, you can instead create credential profiles to securely store this information. The platform supports unique credentials for each type of access protocol, and allows you to bundle multiple protocols and their corresponding credentials in a single profile. Devices that use the same credentials can share a credential profile. For example, if all of your routers in a particular building share a single SSH user ID and password, you can create a single credential profile to allow Crosswork Optimization Engine to access and manage them.

Before You Begin

Before you begin using Cisco Crosswork Optimization Engine, Cisco recommends that you complete the following planning and information-gathering steps, in any order you wish:

- **User Accounts** : Cisco recommends as a best practice that you create separate accounts for all of your users, so that there is an audit record of user activity on the system. Prepare a list of the people who will use Cisco Crosswork Optimization Engine. Decide on their user names and preliminary passwords, and create user profiles for them (see [Manage Users, on page 103](#)).

- **User Roles:** Cisco recommends that you use role-based access control to confine users to just the software functions needed to perform their job duties. By default, every new user you create has full administrative privileges. Unless you want to extend the same privileges to every user, you will need to plan a system of user roles, create them, and assign them to the user profiles you create (see [Create User Roles, on page 105](#)).
- **Credentials:** Gather access credentials and supported protocols that you will use to monitor and manage your devices. For providers, this always includes user IDs, passwords, and connection protocols. For devices, it includes user IDs, passwords, and additional data such as the SNMP v2 read and write community strings, and SNMPv3 auth and privilege types. You will use these to create credential profiles (see [Inventory Management Concepts, on page 11](#) and [Manage Credential Profiles, on page 23](#)).
- **Tags:** Plan a preliminary list of custom tags to create when setting up the system, so that you can use them to group your devices when you first onboard them. As explained in [Inventory Management Concepts, on page 11](#), you will want to consider grouping devices by functionality. You need not have a complete list of tags at first, as you can always add more later, but please note that all the tags you do plan to use must be in place before you need them; you cannot create them "on the fly" (see [Manage Tags, on page 56](#) and [Create Tags, on page 57](#)).
- **Providers:** As explained in [Inventory Management Concepts, on page 11](#), providers do the basic work of direct interaction with network devices, so that Cisco Crosswork Optimization Engine can automate monitoring and responses to network events. At a minimum, Cisco Crosswork Optimization Engine must have an SR-PCE provider defined in order to discover devices and to distribute policy configuration to devices. You should determine the auto-onboarding mode and device profile you will use (if you auto-onboard devices). See [Add Cisco SR-PCE Providers, on page 32](#).
- **Devices:** Decide how you are going to onboard your devices: manually, via the user interface, or automatically, via synchronization or CSV import. This determines the amount of additional information you will need to onboard your devices, which is covered in [About Adding Devices, on page 17](#).

Note that you can capture the devices, credential profiles, tags, and providers lists in spreadsheet form, convert the spreadsheet to CSV format, and then upload them in bulk to Cisco Crosswork Optimization Engine. You do this using the Import feature (accessed using the Import icon, .

You can access CSV templates for each of these lists by clicking the Import icon in the corresponding places in the user interface. Select the **Download template** link when prompted to choose an export destination path and file name.

High-Level Workflows

These workflows describe the main steps to quickly get started with Cisco Crosswork Optimization Engine. The difference between the two workflows are the steps on how devices are added (see [About Adding Devices, on page 17](#)).



Note If you selected to use Cisco NSO for device management during Cisco Crosswork Optimization Engine installation, you must add NSO as a provider (see [Collection Modes, on page 125](#) and the *Cisco Crosswork Optimization Engine Installation Guide*).

Workflow: Auto-Onboard Devices

The following workflow describes the main steps to get started with Cisco Crosswork Optimization Engine by configuring a Cisco SR-PCE provider to automatically onboard devices.

Table 1: Workflow: Automatic Onboarding of SR-PCE Devices

Step	For more information, see...
1. Ensure that your devices are configured properly for communication and telemetry.	Refer to the guidelines and sample configurations in: <ul style="list-style-type: none"> • Prerequisites for Onboarding Devices, on page 19 • Sample Configuration for Devices in Cisco NSO, on page 20 <p>Note Only if NSO is being used for device management.</p> <ul style="list-style-type: none"> • Prerequisites for Device Telemetry, on page 126
2. Create a device credential profile.	Create Credential Profiles, on page 24
3. (Optional) Create tags for use in grouping new devices.	Manage Tags, on page 56
4. Configure SR-PCE as a provider. Note The auto-onboard provider property value must be set to managed or unmanaged to enable automatic onboarding of devices. For more information see About Adding Devices, on page 17 and Auto-Onboard Property Descriptions, on page 34 .	Add Cisco SR-PCE Providers, on page 32
5. Validate communications with provider.	Get Provider Details, on page 40
6. View device list (Inventory Management > Devices) to check that devices have been added properly. If devices are unreachable, select and edit the device with connectivity details.	Manage Devices, on page 43
7. Confirm visualization of IGP topology (logical view).	Network Topology Map, on page 61
8. (Required if using NSO for device management) Configure NSO credential profile and provider.	<ul style="list-style-type: none"> • Create Credential Profiles, on page 24 • Add Cisco NSO Providers, on page 37

Step	For more information, see...
<p>9. (Required if using NSO for device management, otherwise optional) To update device attributes (such as mapping a device to NSO, adding connectivity IP and geographical coordinates, and so on) export the CSV device list, make and save modifications, and import it back to the device inventory.</p> <p>Note If you wish to use the geographical topology map, you must add geographical location details.</p>	<ul style="list-style-type: none"> • Export Devices, on page 54 • Import Devices, on page 44
10. Visualize discovered SR policies and create new SR policies.	Visualize and Manage SR Policies, on page 75

Workflow: Manually Import Devices

The following workflow describes the main steps to get started with Cisco Crosswork Optimization Engine by importing a CSV file to add devices.

Table 2: Workflow: Importing a CSV file to Onboard Devices

Step	For more information, see...
1. Ensure that your devices are configured properly for communication and telemetry.	<p>Refer to the guidelines and sample configurations in:</p> <ul style="list-style-type: none"> • Prerequisites for Onboarding Devices, on page 19 • Sample Configuration for Devices in Cisco NSO, on page 20 <p>Note Only if NSO is being used for device management.</p> <ul style="list-style-type: none"> • Prerequisites for Device Telemetry, on page 126
2. Create a device credential profile.	Create Credential Profiles, on page 24
3. Configure the SR-PCE provider.	Add Cisco SR-PCE Providers, on page 32
<p>Note Set auto-onboard property value to off for manual device onboarding. For more information see Auto-Onboard Property Descriptions, on page 34.</p>	
4. (Required if using NSO for device management) Configure NSO credential profile and provider.	<ul style="list-style-type: none"> • Create Credential Profiles, on page 24 • Add Cisco NSO Providers, on page 37

Step	For more information, see...
5. (Optional) Create tags for use in grouping new devices.	Manage Tags, on page 56
6. Create a CSV file and import devices.	Import Devices, on page 44
7. (Optional) Modify device details.	Edit Devices, on page 53
8. Visualize discovered SR policies and create new SR policies.	Visualize and Manage SR Policies, on page 75



CHAPTER 3

Manage Inventory

This section contains the following topics:

- [Inventory Management Overview](#), on page 17
- [About Adding Devices](#), on page 17
- [Prerequisites for Onboarding Devices](#), on page 19
- [Sample Configuration for Devices in Cisco NSO](#), on page 20
- [Reachability and Operational State](#), on page 21
- [Manage Credential Profiles](#), on page 23
- [Manage Providers](#), on page 30
- [Manage Devices](#), on page 43
- [Manage Tags](#), on page 56

Inventory Management Overview

The application lets you create, edit, and delete:

- The **credential profiles** that control Crosswork Optimization Engine's access to devices and providers. See [Manage Credential Profiles](#), on page 23.
- The **providers** who supply special services, such as device configuration, data storage, or alert processing, to Crosswork Optimization Engine. See [Manage Providers](#), on page 30.
- The **devices** you manage using Crosswork Optimization Engine. See [Manage Devices](#), on page 43.
- The **tags** you use to sort and group devices. See [Manage Tags](#), on page 56.

You can also use to review the **jobs** executed on your devices. See [View Device Job History](#), on page 55.

About Adding Devices

There are two ways to add devices to Cisco Crosswork Optimization Engine:

1. Automatically onboard devices and populate the inventory.
2. Manually onboard devices using a CSV file or the UI.

Auto-Onboard Devices

Auto-onboarding simplifies and expedites the device onboarding process. It automatically discovers and imports preformatted device data from a Cisco SR-PCE provider and enables you to quickly view the IGP topology (including devices, links and IP addresses) in the Cisco Crosswork Optimization Engine topology map.

To configure auto-onboarding, you add an SR-PCE provider with one of the following auto-onboard options: **managed** or **unmanaged**.

The auto-onboard **managed** option requires a single default credential profile (having SNMP access, at minimum) that will work for all devices.

The devices are auto-onboarded with the following attributes::

- The OSPF Router ID or TE Router ID is assigned as the **Node IP** of the device. **Node IP** is configured as the Device Key Type.
- For devices running IS-IS, a **Hostname** is assigned. It is not available for OSPF.
- The **Connectivity IP** is assigned the same value as the **Node IP**.
- The default credential profile is set as the **Credential Profile** for each device.



Note

If a common credential profile cannot be used for all devices, or a different **Connectivity IP** is required, use the auto-onboard **unmanaged** option or Cisco Crosswork Optimization Engine will keep trying to connect to the devices and fail.

The auto-onboard **unmanaged** option should be used if you prefer devices not to be assigned a **Credential Profile** or **Connectivity IP**. SNMP or any other device collection is not performed. However, IGP topology is still seen on the topology map (logical view), but the information available is restricted to the information SR-PCE provides. Therefore, interface names are not shown, and in the case of OSPF, device Hostnames are also not shown. IP addresses are shown and can be used to identify devices and interfaces.

Auto-Onboard Notes and Limitations:


Consider the following information when choosing between **unmanaged** and **managed** options:

- The OSPF or TE router ID is used as the Connectivity IP of the device. This is the IP address Cisco Crosswork Optimization Engine will use to perform SNMP or CLI collection from the device. If the devices need to be reached over a separate management network, the Connectivity IP of all devices will need to be updated using the CSV **Update Existing** option (see [Import Devices, on page 44](#)). In this case, use the **unmanaged** option for auto-onboarding to prevent repeated unsuccessful collection attempts from the devices.
- The **managed** option works only if a single **Credential Profile** will work for accessing all the devices.
- With the **unmanaged** option, since SNMP collection from the devices cannot be performed, interface names and possibly hostnames will not be available until the devices in inventory are updated with the correct **Connectivity IP** and **Credential Profile** and their state is updated to Managed.
- Several device attributes cannot be discovered and need to be manually supplied. After the inventory is populated, you can download the device inventory CSV file, edit the file to add additional information (such as geographical location), and import it back into Cisco Crosswork Optimization Engine using the CSV **Update Existing** option. See [Import Devices, on page 44](#) and [Export Devices, on page 54](#).

To quickly get up and running with Cisco Crosswork Optimization Engine, follow the high-level steps documented in [Workflow: Auto-Onboard Devices, on page 13](#).

Manually Add Devices

You can manually onboard devices from a CSV file or add them using the UI. After adding credential profiles, configure providers and tags to group new devices (optional) you do one of the following:

- Download the CSV template file from **Inventory Management > Devices** >  and populate it with all the devices you will need (see [Import Devices, on page 44](#)). This method can be time consuming, as you must create and enter all of the data yourself beforehand (including not only devices, but also the providers, credential profiles and tags), and then ensure all of these items are properly associated with the devices.

To quickly get up and running with Cisco Crosswork Optimization Engine by importing devices, follow the high-level steps documented in [Workflow: Manually Import Devices, on page 14](#).

- Add devices using the UI (see [Add Devices Through the UI, on page 46](#)). It is the most time-consuming since all data is validated during entry.

Prerequisites for Onboarding Devices

Before adding devices, you must ensure that the devices themselves are configured to collect and transmit telemetry data properly and communicate successfully with Cisco Crosswork Optimization Engine. The following sections of this topic provide sample configurations for a variety of communications options. Use them as a guide to configuring the devices you plan to manage using Cisco Crosswork Optimization Engine.



Note Only users configured with privilege level 15 can use the NETCONF APIs. Privilege level 15 can be used to configure the "enable" password option in XE devices. In such cases, NETCONF must not be included as one of the protocols to verify reachability and operational state for the onboarded devices.

Pre-Onboarding SNMP v2 Device Configuration

The following commands provide a sample pre-onboarding device configuration that sets the correct SNMPv2 and NETCONF configuration, and SSH and Telnet rate limits. The NETCONF setting is only needed if the device is MDT-capable (XR 612 or higher).

```
logging console debugging
logging monitor debugging
telnet vrf default ipv4 server max-servers 100
telnet vrf default ipv6 server max-servers 100
crypto key generate rsa
line default
  exec-timeout 0 0
  width 107
  length 37
  absolute-timeout 0
!
snmp-server community public RO
snmp-server community robot-demo2 RO
snmp-server ifindex persist
ntp
  server <NTPServerIPAddress>
```

```

!
service cli history size 5000
service cli interactive disable
ssh server v2
ssh server vrf default
ssh server netconf vrf default
ssh server logging
ssh server rate-limit 100
ssh server session-limit 100
grpc
  port 57400
!
netconf agent tty
!
netconf-yang agent
  ssh
!

```

Pre-Onboarding SNMPv3 Device Configuration

If you want to enable SNMPv3 data collection, repeat the SNMPv2 configuration commands in the previous section, and add the following commands:

```

snmp-server group grpauthpriv v3 priv notify v1default
snmp-server user <user-ID> grpauthpriv v3 auth md5 <password> priv aes 128 <password>

```

Sample Configuration for Devices in Cisco NSO

If you plan to use Cisco NSO as a provider to configure devices managed by Cisco Crosswork Optimization Engine, be sure that the Cisco NSO device configurations observe the following guidelines.

The following example shows a Cisco NSO setup that uses the hostname as the device ID. If you are using a CSV file to import devices, use **ROBOT_PROVIDEKEY_HOST_NAME** as the enum value for the provider_node_key field. The example hostname **RouterFremont** used here must match the hostname for the device in the CSV file.

```

configure
set devices device RouterFremont address 198.18.1.11 port 22
set devices device RouterSFO address 198.18.1.12 port 22

```

The authgroup username and password in the CSV file must match the username and password in the credential profile associated with the Cisco NSO provider. For example:

```

set devices authgroups group cisco default-map remote-name cisco remote-password cisco
set devices device Router* device-type cli ned-id cisco-ios-xr
set devices device Router* authgroup cisco

```

The device itself must be synchronized with Cisco NSO before you import that device. For example:

```









set devices device Router* state admin-state unlocked
request devices device Router* ssh fetch-host-keys
request devices device Router* sync-from
commit





```

Reachability and Operational State

Cisco Crosswork Optimization Engine computes the Reachability State of the providers it uses and devices it manages, as well as the Operational State of reachable managed devices. It indicates these states using the icons in the following table.

Table 3: Reachability and Operational State Icons

This Icon...	Indicates...
Reachability State icons show whether a device or a provider is reachable or not	
	Reachable: The device or provider can be reached by all configured protocols configured for it.
	Reachability Degraded: The device or provider can be reached by at least one protocol, but is not reachable by one or more of the other protocols configured for it.
	Unreachable: The device or provider cannot be reached by any protocol configured for it.
	Reachability Unknown: Cisco Crosswork Optimization Engine cannot determine if the device is reachable, degraded, or unreachable.
Operational State icons show whether a device is operational or not.	
	The device is operational and under management, and all individual protocols are "OK" (also known as "up").
	The device is not operational ("down"). The same icon is used when the device has been set "administratively down" by an operator.
	The device's operational or configuration state is unknown.
	The device's operational or configuration state is degraded.

This Icon...	Indicates...
	The device's operational or configuration state is in an error condition. It is either not up, or unreachable, or both, due to errors encountered while attempting to reach it and compute its operational state. The number in the circle shown next to the icon indicates the number of recent errors. Click on the number to see a list of these errors. (Note that the icon badging for errors is not available in the Network Topology application.)
	The device's operational state is currently being checked
	The device is being deleted.
	The device is unmanaged.

The Reachability State of a device is computed as follows:

1. Reachability is always computed for each device as long as the device's configured state (as configured by users) is UP. It is not computed if the device is administratively DOWN or UNMANAGED.
2. Reachability state is always either REACHABLE, UNREACHABLE, or UNKNOWN.
 - The Reachability state is REACHABLE if there is at least one route to the device via at least one protocol AND the device is DISCOVERABLE.
 - The Reachability state is UNREACHABLE if there are no routes to the device via one protocol OR the device does not respond.
 - The Reachability state is UNKNOWN if the device is UNMANAGED.

The Operational State of a device is computed as follows:

1. Operational state is always computed for each device as long as the device's configured state (as configured by users) is UP. It is not computed if the device is administratively DOWN or UNMANAGED.
2. Operational state is always OK or ERROR.
3. For a device to be Operational=OK, the device must be both REACHABLE and DISCOVERABLE. Any other Reachability or Discovery state is ERROR.
4. For XR or XE devices only, Operational=OK also requires that Clock Drift difference between the Crosswork host and device clocks is \leq the default Drift Value, currently 2 minutes.



Note Confirm that devices have Telnet/SSH enabled. If it is not enabled, the Clock Drift throws an error and the operational state will always show a clock synchronization error.

Manage Credential Profiles

Credential profiles are collections of credentials for SNMP, Telnet/SSH, HTTP, and other network protocols. You can have multiple protocols and credentials in a single credential profile.

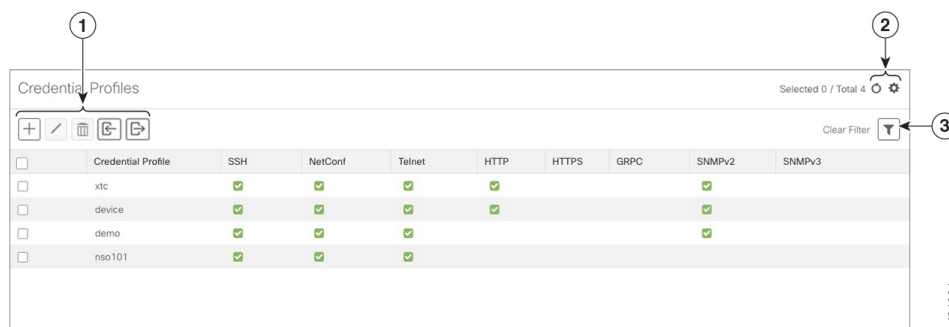
Using credential profiles lets you automate device configuration changes and monitoring, and communicate with providers. When you add or import devices, or create providers, you specify the credential profile(s) those devices and providers use.






Note Credentials just validates authentication since the corresponding protocol configured on the devices does the work. Devices should be present in the **Devices** window and be reachable.

From the **Credential Profiles** window, you can create a new credential profile, update the settings configured for an existing profile, or delete a profile. To open this window, choose **Inventory Management > Credentials** from the main menu.

Figure 5: Credentials Profile window



Item	Description
1	Click to add a credential profile. See Create Credential Profiles, on page 24 .
	Click to edit the settings for the selected credential profile. See Edit Credential Profiles, on page 28 .
	Click to delete the selected credential profile. See Delete Credential Profiles, on page 28 .
	Click to import new credential profiles from a CSV file. You can also download a CSV file template by clicking this icon. The template includes sample data that you can use as a guide for building your own CSV file. See Import Credential Profiles, on page 26 .
	Click to export credential profiles to a CSV file. See Export Credential Profiles, on page 29 .

Item	Description
2	Click  to refresh the Credential Profiles window.
	Click  to choose the columns to make visible in the Credential Profiles window (see Set, Sort and Filter Table Data, on page 6).
3	Click  to set filter criteria on one or more columns in the Credential Profiles window.
	Click the Clear Filter link to clear any filter criteria you may have set.

Create Credential Profiles

Follow the steps below to create a new credential profile. You can then use the profile to apply credentials consistently when you add new devices or providers. You can add as many protocols and corresponding credentials to the profile as you want.

If you have many credential profiles to add, you may find it more efficient to put the information in a CSV file and import the file. See [Import Credential Profiles, on page 26](#)

When creating device credential profiles that contain SNMP credentials, Cisco recommends that the profile contain credentials for the version of SNMP actually enabled on the device, and that version only. For example: If SNMPv3 is not enabled in the device configuration, do not include SNMPv3 credentials in the device credential profile.

If you plan to use the import and export features and CSV files to create credential profiles in bulk, please note that:

- All the characters in each password or community string entry in every credential profile exported to a CSV file are replaced with asterisks ([Export Credential Profiles, on page 29](#)).
- You cannot import credential profiles if the passwords and community strings in the CSV file are blank (see [Import Credential Profiles, on page 26](#)).


To maintain network security, Cisco recommends that you use asterisks in place of real passwords and community strings in any CSV file you plan to import. After the import, follow the steps in [Edit Credential Profiles, on page 28](#) to replace the asterisks with actual passwords and community strings.

Step 1 From the main menu, choose **Inventory Management > Credentials**.

Step 2 Click .

Step 3 In the **Profile Name** field, enter a descriptive profile name. The name can contain a maximum of 128 alphanumeric characters, plus underscores ("_") or hyphens ("-"). No other special characters are allowed.

If you will have many credential profiles, make the name as informative as possible because that information will be displayed on the Credential Profiles panel.

Step 4 Click the  next to **Add Protocol Credentials**.

Step 5 Select a protocol from the **Connectivity Type** dropdown.

Step 6 Complete the credentials fields described in the following table. The required and optional fields displayed will vary with the connectivity type you chose. The values you enter must match the values configured on the device.

Connectivity Type	Fields
SSH	Enter the required User Name , Password , and Confirm Password . The Enable Password is optional.
SNMPv2	Enter the required SNMPv2 Read Community string. The Write Community string is optional.
NETCONF	Enter the required User Name , Password , and Confirm Password .
TELNET	Enter the required User Name , Password , and Confirm Password . The Enable Password is optional.
HTTP	Enter the required User Name , Password , and Confirm Password .
HTTPS	Enter the required User Name , Password , and Confirm Password .
GRPC	Enter the required User Name , Password , and Confirm Password .
SNMPv3	<p>Choose the required Security Level and enter the User Name.</p> <p>If you chose the NO_AUTH_NO_PRIV Security Level of AUTH_NO_PRIV or AUTH_PRIV, the remaining fields are optional.</p> <p>If you chose the AUTH_NO_PRIV Security Level, you must choose an Auth Type and enter an Auth Password.</p> <p>If you chose the AUTH_PRIV Security Level, you must choose an Auth Type and Priv Type, and enter an Auth Password and Priv Password.</p> <p>Only the following SNMPv3 Privacy Types are supported</p> <ul style="list-style-type: none"> • CFB_AES_128 • CBC_DES_56 <p>The following Privacy Types are not supported:</p> <ul style="list-style-type: none"> • AES192 • AES256 • 3DES

Step 7 Repeat steps 4 through 7, as needed, for all other protocols and corresponding credentials you want to add to this credential profile.

Step 8 Click **Save**.

Import Credential Profiles

Complete the steps below to create a CSV file that specifies multiple credential profiles and then import it into Cisco Crosswork Optimization Engine.

Importing credential profiles from a CSV file adds any profiles not already in the database. You cannot import a device credential that already exists.

If you are re-importing a credential profile CSV file that you previously exported and modified, remember that all the passwords and community strings in the exported credential profile CSV file are replaced with asterisks. You cannot re-import an exported credential profile CSV file with blank passwords. To maintain security, Cisco recommends that you use asterisks in place of real passwords and community strings in the CSV file. After the import, follow the steps in [Edit Credential Profiles, on page 28](#) to replace the asterisks with actual passwords and community strings.

Step 1 From the main menu, choose **Inventory Management > Credentials**.

Step 2 Click  to open the **Import CSV File** dialog box.

Step 3 If you have not already created a credential profile CSV file to import:

- a) Click the **Download sample 'Credential template (*.csv)' file** link and save the CSV file template to your local disk.
- b) Open the template using your preferred tool. Begin adding rows to the file, one row for each credential profile.

Use a semicolon to separate multiple entries in the same field. Use two semicolons with no space between them to indicate that you are leaving the field blank. When you separate multiple entries with semicolons, remember that the order in which you enter values in each field is important. For example, if you enter **SSH;NETCONF;TELNET** in the **Connectivity Type** field and you enter **UserTom;UserDick;UserHarry** in the **User Name** field, the order of entry determines the mapping between the two fields:

- SSH: UserTom
- NETCONF: UserDick
- TELNET: UserHarry

Also note:

- Be sure to enter SNMP community string information exactly as currently entered on your devices. Failure to do so may result in loss of device connectivity.
- Password and community string information associated with a user ID are stored in plain text in the CSV file you prepare. Be aware of the security implications of this, and apply appropriate safeguards.

Field	Entries	Required or Optional
Credential Profile	The name of the credential profile. For example: srpce .	Required

Field	Entries	Required or Optional
Connectivity Type	Valid values are: SSH , SNMPv2 , NETCONF , TELNET , HTTP , HTTPS , GRPC or SNMPv3	<ul style="list-style-type: none"> • Devices—SNMP and SSH (to avoid operational errors due to clock synchronization checks) are required. • SR-PCE—Since SR-PCE is considered a provider and a device, SSH, and HTTP are required.
User Name	For example: SRPCEUser	Required if Connectivity Type is SSH , NETCONF , TELNET , HTTP , HTTPS , SNMPv3 or GRPC .
Password	The password for the preceding User Name .	Required if Connectivity Type is SSH , NETCONF , TELNET , HTTP , HTTPS or GRPC
Enable Password	Use the Enable password. Valid Values are: ENABLE , DISABLE , or leave blank (unselected)	
Enable Password Value	The Enable password to use.	Required only if Enable Password is set to Enable .
SntpV2 Read Community	For example: readprivate	Required if Connectivity Type is SNMPv2
SntpV2 Write Community	For example: writeprivate	
SntpV3 User Name	For example: DemoUser	Required if Connectivity Type is SNMPv3
SntpV3 Security Level	Valid values are noAuthNoPriv , AuthNoPriv or AuthPriv	Required if Connectivity Type is SNMPv3
SntpV3 Auth Type	Valid values are HMAC_MD5 or HMAC_SHA	Required if Connectivity Type is SNMPv3 and SntpV3 Security Level is AuthNoPriv or AuthPriv
SntpV3 Auth Password	The password for this authorization type.	Required if Connectivity Type is SNMPv3 and SntpV3 Security Level is AuthNoPriv or AuthPriv
SntpV3 Priv Type	Valid values are CFB_AES_128 or CBC_DES_56 The following SNMPv3 privacy types are not supported: AES192, AES256, 3DES	Required if Connectivity Type is SNMPv3 and SntpV3 Security Level is AuthPriv
SntpV3 Priv Password	The password for this privilege type.	Required if Connectivity Type is SNMPv3 and SntpV3 Security Level is AuthPriv

Be sure to delete the sample data rows before saving the file, or they will be imported along with the data you want. The column header row can stay, as it is ignored during import.

c) When you are finished, save the new CSV file.

Step 4 Click **Browse** to navigate to the CSV file you just created and then click **Open** to select it.

Step 5 With the CSV file selected, click **Import**.

The credential profiles you imported should now be displayed in the **Devices** window.

Edit Credential Profiles

A credential profile can be shared by multiple devices, even hundreds of devices in a large network. Complete the following procedure to edit credential profile settings.



Warning Changing the settings in a credential profile without first changing the settings on the device associated with the profile may result in a loss of connectivity.

Before editing any credential profile, it is always good practice to export a CSV backup of the profiles you want to change (see [Export Credential Profiles, on page 29](#)).

Step 1 From the main menu, choose **Inventory Management > Credentials**.

Step 2 From the left-hand side of the **Credential Profiles** window, click the profile you want to update.

Step 3 Make the necessary changes and then click **Save**.

Delete Credential Profiles

Follow the steps below to delete a credential profile.




Note You cannot delete a credential profile that is associated with one or more devices or providers.

Step 1 Export a backup CSV file containing the credential profile you plan to delete (see [Export Credential Profiles, on page 29](#)).

Step 2 Check whether any devices or providers are using the credential profile you plan to delete. You can do this by filtering on the **Credential Profile** column, which is available on both the **Devices** window (choose **Inventory Management > Credentials**) and the **Providers** window (choose **Inventory Management > Providers**).

Step 3 Reassign the devices or providers to a different credential profile (for help with this task, see [Change a Device's Credential Profile, on page 29](#) or [Change the Credential Profile for Multiple Devices, on page 30](#), and [Edit Providers, on page 41](#)).

Step 4 After all devices and providers have had their credential profiles reassigned: From the main menu, choose **Inventory Management > Credentials**.

Step 5 In the **Credential Profiles** window, choose the profile that you want to delete and then click .

Export Credential Profiles


Exporting credential profiles stores all the profiles you selected in a CSV file. This is a quick way to make backup copies of your credential profiles. You can also edit the CSV file as needed, and re-import it to add new credential profile data. You cannot overwrite existing credential profiles by importing a CSV file.

The exported credential profiles CSV file does not contain real passwords or community strings. All the characters in the passwords and community strings entries in the credential profiles are replaced with asterisks in the exported CSV file. If you plan on modifying your exported CSV file and then re-importing it, Cisco recommends that you use asterisks in place of real passwords and community strings. After the import, follow the steps in [Edit Credential Profiles, on page 28](#) to replace the asterisks with actual passwords and community strings.

Step 1 From the main menu, choose **Inventory Management > Credentials**.

Step 2 (Optional) In the **Credential Profiles** window, filter the credential profile list as needed.

Step 3 Check the check boxes for the profiles you want to export. Check the check box at the top of the column to select all the profiles for export.

Step 4 Click . Depending on your browser, you will be prompted to select a path and file name to use when saving the CSV file, or to open it immediately

Change a Device's Credential Profile

You can edit device information, including changing the credential profile in the device record. This operation changes an existing association between a device and a credential profile.

Before you begin


You need a credential profile to complete this task. To create a credential profile, see [Create Credential Profiles, on page 24](#).



Note Make sure the profile's credential settings are correct before following this procedure.

Step 1 From the main menu, choose **Inventory Management > Devices**.

Step 2 (Optional) In the **Devices** window, filter the device list by entering text in the **Search** field or filtering specific columns.

Step 3 Check the check box of the device you want to change, and click .

Step 4 Choose a different credential profile from the **Credential Profile** drop-down list.

Step 5 Click **Save**.

After the device record is updated, the system attempts to communicate with the device using the new profile. Confirm that the device is reachable without any errors.

Change the Credential Profile for Multiple Devices




If you want to change the credential profile for a large number of devices, you may find it more efficient to make the change by editing a devices CSV file. The basic method is:

1. Export a CSV file containing the devices whose credential profiles you want to change (see [Export Devices, on page 54](#)).
2. Edit the CSV file, changing the credential profile for each device (this credential profile must already exist). Save the edited file.
3. Import the edited devices CSV file using the **Update Existing** option. You will overwrite the credential profile data for each device (see [Import Devices, on page 44](#)).

You will need to make sure that the credential profile to which you are changing already exists. If you have not yet created that credential profile, the CSV import will fail. The credential profile you associate with these devices must also have the authorization credentials for every protocol that was configured for these devices during onboarding. If any credential for a specific protocol configured on the devices is missing from or incorrect in the credential profile, then the CSV import will succeed, but reachability checks will fail for these devices.

Step 1 From the main menu, choose **Inventory Management > Devices**.

Step 2 In the **Devices** window, choose the devices whose credential profiles you want to change. Your options are:

- Click  to include all devices.
- Filter the device list by entering text in the **Search** field or by filtering specific columns. Then click  to include only the filtered list of devices.
- Check the boxes next to the device records you want to change. Then click  to include only the devices that have been checked.

Step 3 Edit and save the new CSV file using the tool of your choice. Be sure to enter the correct credential profile name in the **Credential Profile** field for each device.

Step 4 In the **Devices** window, click .

Step 5 In the **Import** dialog box, click **Browse**, choose the new CSV file, and click **Update Existing**.

Manage Providers

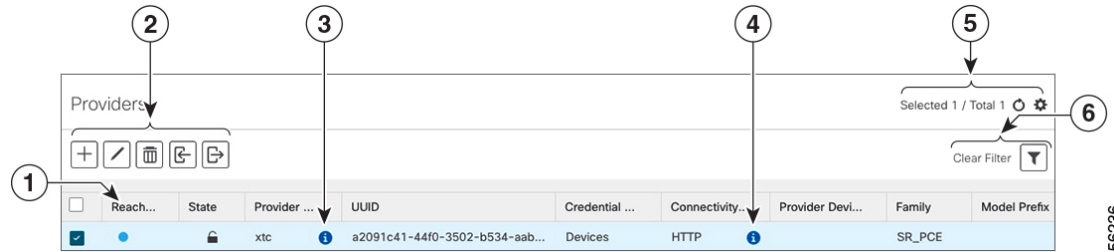
Cisco Crosswork Optimization Engine communicates with SR-PCE and NSO providers. Cisco Crosswork Optimization Engine stores the provider connectivity details and makes that information available to applications.



Note Other providers are available on the UI. However, they are not used by Cisco Crosswork Optimization Engine. They are used by other Cisco Network Automation applications.




From the **Providers** window, you can add a new provider, update the settings configured for an existing provider, and delete a particular provider. To open this window, choose **Inventory Management > Providers**.

Figure 6: Providers window



356236

Item	Description
1	The icon shown next to the provider in this column indicates the provider's Reachability . For more on the icons and how reachability is determined, see Reachability and Operational State, on page 21 .
2	Click to add a provider. See Add Cisco SR-PCE Providers, on page 32 .
	Click to edit the settings for the selected provider. See Edit Providers, on page 41 .
	Click to delete the selected provider. See Delete Providers, on page 41 .
	Click to import new providers or update existing providers from a CSV file. You can also download a CSV file template by clicking this icon. The template includes sample data that you can use as a guide for building your own CSV file. See Import Providers, on page 38 .
4	Click to export a provider to a CSV file. See Export Providers, on page 42 .
	Click next to the provider in the Provider Name column to open the Properties for pop-up window, showing the details of any startup session key/value pairs for the provider.
3	Click next to the provider in the Connectivity Type column to open the Connectivity Details pop-up window, showing the protocol, IP and other connection information for the provider.

Item	Description
5	Click  to refresh the Providers window.
	Click  to choose the columns to make visible in the Providers window (see Set, Sort and Filter Table Data, on page 6).
6	Click  to set filter criteria on one or more columns in the Providers window.
	Click the Clear Filter link to clear any filter criteria you may have set.

Add Cisco SR-PCE Providers

Cisco Segment Routing Path Computation Elements (Cisco SR-PCE) providers supply device discovery, management, configuration-maintenance and route-calculation services to Cisco Crosswork Optimization Engine. At least one SR-PCE provider is required in order to learn and discover SR policies, Layer 3 links, and devices.

Follow the steps below to use the user interface to add up to two instances of Cisco SR-PCE as providers for Cisco Crosswork Optimization Engine.

Before you begin

You will need to:

- Create a credential profile for the Cisco SR-PCE provider (see [Create Credential Profiles, on page 24](#)). This should be a basic HTTP text-authentication credential (currently, MD5 authentication is not supported). If the Cisco SR-PCE server you are adding does not require authentication, you must still supply a credential profile for the provider, but it can be any profile that does not use the HTTP protocol.
- Know the name you want to assign to the Cisco SR-PCE provider. This is usually the DNS hostname of the Cisco SR-PCE server.
- Know the Cisco SR-PCE server IP address.
- Determine whether you want to auto-onboard the devices that Cisco SR-PCE discovers and, if so, whether you want the new devices to have their management status set to **managed** or **unmanaged** when added. For more information, see [Auto-Onboard Property Descriptions, on page 34](#).
- If you plan to auto-onboard devices that the Cisco SR-PCE provider discovers, and set them to a managed state when they are added to the database:
 - Assign an existing credential profile for communication with the new managed devices.
 - The credential profile must be configured with an SNMP protocol.
- If you want to ensure high availability by setting up two Cisco SR-PCE providers and then using them both with Cisco Crosswork Optimization Engine, ensure that you set up two separate Cisco SR-PCE providers with unique names and IP addresses, but having matching configurations (see [Multiple Cisco SR-PCEs, on page 35](#)).

Step 1 From the main menu, choose **Inventory Management > Providers**.

Step 2 Click .


Step 3 Enter the following values for the Cisco SR-PCE provider fields:

a) Required fields:

- **Provider Name:** Name of the SR-PCE provider that will be used in Cisco Crosswork Optimization Engine.
- **Credential Profile:** Select the previously created Cisco SR-PCE credential profile.
- **Family:** Select **SR_PCE**. All other options should be ignored.
- **Protocol:** Select **HTTP**. All other options should be ignored.
- **IPv4 Address:** Enter the IPv4 address of the server.
- **Provider Properties:** Enter one of the following key/value pairs in the first set of fields (see [About Adding Devices, on page 17](#) and [Auto-Onboard Property Descriptions, on page 34](#)):

Property Key	Value
auto-onboard	off
auto-onboard	unmanaged
auto-onboard	managed

If you enter the **auto-onboard/managed** pair:

1. Click the  next to the first set of fields to add a new set.
2. In the new **Property Key** field, enter **device-profile**.
3. In the new **Property Value** field, enter the name of a credential profile that contains SNMP credentials for all the new devices.

b) Optional values:

- **IPv6 Address:** Leave blank. Reserved for future use.
- **Timeout:** The amount of time (in seconds) to wait before timing out the connection to the SR-PCE server. The default is 30 seconds.

Step 4 When you have completed entries in all of the required fields, click **Save** to add the SR-PCE provider.

Step 5 Confirm that the SR-PCE shows a green Reachability status without any errors. You can also view the Events window to see if the provider has been configured correctly.



Note It is not recommended to modify auto-onboard options (**managed/unmanaged/off**) once set. If you need to modify them, do the following:

1. Delete the provider and wait until deletion confirmation is displayed in the Events page.
2. Re-add the provider with the updated auto-onboard option.
3. Confirm the provider has been added with the correct auto-onboard option in the Events page.

What to do next

- If you entered the **auto-onboard/off** pair, navigate to **Inventory Management > Devices** to add a device list (see [Import Devices, on page 44](#)).
- If you opted to automatically onboard devices, navigate to **Inventory Management > Devices** to view the device list. To add more node information such as geographical location details, export the device list (.csv), update it, and import it back. If geographical location data is missing, you will only be able to see device topology using the logical map.

Auto-Onboard Property Descriptions

The following table describes auto-onboard property provider fields.

Field	Description
off	If this option is enabled, you add or import devices manually (typically using a .csv file). When devices are discovered, the device data is recorded in the Cisco SR-PCE database, but is not registered in Crosswork Optimization Engine Inventory Management database.
unmanaged	If this option is enabled, all devices that Cisco SR-PCE discovers will be registered in the Cisco Crosswork Optimization Engine Inventory Management database, with their configured state set to unmanaged . SNMP polling will be disabled for these devices, and no management IP information will be included. To get these devices into the managed state later, you will need to download them as a CSV file (see Export Devices, on page 54), and modify the CSV file to add the SNMP and management IP address information. You can then update the auto-onboarded devices with this information by importing the modified CSV file (see Import Devices, on page 44). You can also assign credential profile by adding them to the device CSV file before import (the credential profiles must already exist).
managed	If this option is enabled, all devices that Cisco SR-PCE discovers will be registered in the Cisco Crosswork Optimization Engine Inventory Management database, with their configured state set to managed . SNMP polling will be enabled for these devices, and Cisco SR-PCE will also report the management IP address (Router ID). You will also need to add a second Provider Properties key/value pair, with the key device-profile and the value being the name of a credential profile for the new devices.



Note If **managed** or **unmanaged** options are set and you want to delete a device later, you must do one of the following:

- Reconfigure and remove the devices from the network before deleting the device from Cisco Crosswork Optimization Engine. This avoids Cisco Crosswork Optimization Engine from rediscovering and adding the device back to Cisco Crosswork Optimization Engine.
- Set auto-onboard to **off**, and then delete the device from Cisco Crosswork Optimization Engine. However, doing so will not allow Cisco Crosswork Optimization Engine to detect or auto-onboard any new devices in the network.

Cisco SR-PCE Reachability Issues

You can find reachability issues raised in the Events table and reachability status in the **Providers** window (see [Get Provider Details, on page 40](#)). If the SR-PCE goes down, all links in the topology will display with the last known state since the SR-PCE cannot send any notification updates. When the SR-PCE becomes reachable again, a message will show in the **Events** window that SR-PCE is reconnected and the topology will be updated accordingly. If you find that the SR-PCE goes down for an extended amount of time, delete the SR-PCE and add it back (when connectivity returns) using the UI.

If you are running into provider reachability problems, you can troubleshoot as follows:

-
- Step 1** Check device credentials.
- Step 2** Ping the provider host.
- Step 3** Attempt a connection using the protocols specified in the connectivity settings for the provider. For an SR-PCE provider, it is typically HTTP and port 8080.
- ```
curl --raw -vN "http://<hostname or ip-address>:8080/topology/subscribe/txt"
curl --raw -vN "http://<username>:<password>@"
```
- Step 4** Check your firewall setting and network configuration.
- Step 5** Check the Cisco SR-PCE host or intervening devices for Access Control List settings that might limit who can connect.
- 

## Multiple Cisco SR-PCEs

You can set up two Cisco SR-PCEs to ensure high availability (HA). The two Cisco SR-PCE providers must have matching configurations, supporting the same network topology. In HA, if the primary SR-PCE becomes unreachable, Cisco Crosswork Optimization Engine uses the secondary SR-PCE to discover the network topology. The network topology will continue to be updated correctly and you can view SR-PCE connectivity events in the Events table. To troubleshoot SR-PCE connectivity issues, see [Cisco SR-PCE Reachability Issues, on page 35](#).

### Configure HA

The following configurations must be done to enable HA when two Cisco SR-PCE providers are added in Cisco Crosswork Optimization Engine. There must be a direct link between both SR-PCE's to enable HA. The PCE IP address of the other SR-PCE should be reachable through this sync link.

Issue the following commands on *each* of the Cisco SR-PCE devices:

Enable the interface:

```
interface <interface><slot>/<port>
ipv4 address <sync-link-interface-ip-address> <subnet-mask>
no shut
```

Enable HA:

```
pce rest sibling ipv4 <other-node-pce-address>
```

Establish a sync link between the two SR-PCEs:

```
router static
address-family ipv4 unicast
<other-node-pce-ip-address>/<subnet-mask-length> <remote-sync-link-ip-address>
```

(Optional) # pce-segment-routing traffic-eng peer ipv4 <other-node-pce-ip-address>

Issue the following command on the PCC:

```
segment-routing traffic-eng pcc redundancy pcc-centric
```

### SR-PCE Delegation

Depending on where an SR policy is created, the following SR-PCE delegation occurs:

- SR-PCE initiated—An SR policy that is configured directly on an SR-PCE device. The source SR-PCE is delegated.
- PCC initiated—An SR policy that is configured directly on a device. The SR-PCE configured with the lowest precedence is the delegated SR-PCE. If precedence is not set, then SR-PCE with the lowest PCE IP address is the delegated SR-PCE. The following configuration example, shows that **10.0.0.1** is assigned a precedence value of 10 and will be the delegated SR-PCE.

```
segment-routing
 traffic-eng
 pcc
 source-address ipv4 10.0.0.2
 pce address ipv4 10.0.0.1
 precedence 10
 !
 pce address ipv4 10.0.0.8
 precedence 20
 !
 report-all
 redundancy pcc-centric
```

- Cisco Crosswork Optimization Engine SR-PCE initiated—An SR policy that is configured using Cisco Crosswork Optimization Engine. SR-PCE delegation is random.




---

**Note** This is the only type of SR policy that Cisco Crosswork Optimization Engine can modify or delete (see [Create and Manage SR Policies, on page 87](#)).

---

### HA Notes and Limitations

- It is assumed that all PCCs are PCEP connected to both SR-PCEs.

- When an SR-PCE is disconnected only from Cisco Crosswork Optimization Engine, the following occur:
  - SR-PCE delegation assignments remain, but the SR-PCE that has been disconnected will not appear in Cisco Crosswork Optimization Engine.
  - You are not able to modify Cisco Crosswork Optimization Engine SR-PCE initiated SR policies if the disconnected SR-PCE is the delegated PCE.
- After an SR-PCE reloads, do the following:
  1. Execute the following command:

```
process restart pce_server
```
  2. Remove the PCE sibling configuration in both SR-PCEs and then add the sibling configuration again.
- In some cases, when an SR policy that was created via the UI is automatically deleted (intentional and expected) from Cisco Crosswork Optimization Engine, a warning message does not appear. For example, if the source PCC is reloaded, the UI created SR policy disappears and the user is not informed.
- In an extreme case where one SR-PCE fails on all links (to PCCs/topology devices) except the up-link to Cisco Crosswork Optimization Engine, then topology information will not be accurate in Cisco Crosswork Optimization Engine. When this happens, fix the connectivity issue or delete both SR-PCEs from the Provider page and re-add the one that is reachable.

## Add Cisco NSO Providers

Cisco Network Services Orchestrator (Cisco NSO) providers supply device management and configuration-maintenance services to Cisco Crosswork Optimization Engine.

Follow the steps below to add through the UI one or more instances of (Cisco NSO) as providers for Cisco Crosswork Optimization Engine. You can also add providers using CSV files (see [Import Providers, on page 38](#)).

### Before you begin

You will need to:

- Create a credential profile for the Cisco NSO provider (see [Create Credential Profiles, on page 24](#)).  
Know the name you want to assign to the Cisco NSO provider.
- Know the Cisco NSO NED device models and driver versions used in your topology.
- Know the Cisco NSO server IP address and hostname.
- Confirm Cisco NSO device configurations (see [Sample Configuration for Devices in Cisco NSO, on page 20](#)).


---

**Step 1** From the main menu, choose **Inventory Management > Providers**.

**Step 2** Click .

**Step 3** Enter the following values for the Cisco NSO provider fields:

- a) Required fields:

- **Provider Name:** The name for the provider that will be used in Cisco Crosswork Optimization Engine.
- **Credential Profile:** Select the previously created Cisco NSO credential profile.
- **Family:** Select **NSO** only.
- **Protocol:** Select **NETCONF** only.
- **Device Key:** Select the method that Cisco NSO uses to identify devices uniquely. This will serve as the way maps the device to Cisco NSO. Choose **NODE\_IP** and other options you wish.
- **IPv4 Address:** Enter the IPv4 address of the Cisco NSO server. If you are using the DNS hostname as the provider name, the IP address is resolved automatically.
- **Port:** Enter the Cisco NSO. The default is **2022**.
- **Model:** Select the model (**Cisco-IOS-XR**, **Cisco-NX-OS**, or **Cisco-IOS-XE**) from the drop-down list and enter its associated NED driver version for each type of device that will be used in the topology. If you have more than one select  to add another supported model.

For more information on fields, see [Import Providers, on page 38](#).

b) Optional values:

- **Timeout:** The amount of time (in seconds) to wait before timing out the connection to the Cisco NSO server. The default is 30 seconds.
- **IPv6 Address:** Leave blank. Reserved for future use.

**Step 4** When you have complete entries in all of the required fields, click **Save** to add Cisco NSO as a provider.

## Import Providers

Complete the steps below to create a CSV file that specifies providers and then import it into Cisco Crosswork Optimization Engine.

Importing providers from a CSV file adds any providers not already in the database, and updates any providers with the same name as an imported provider. For this reason, it is a good idea to export a backup copy of all your current providers before an import (see [Export Providers, on page 42](#)).

**Step 1** From the main menu, choose **Inventory Management > Providers**.

**Step 2** Click  to open the **Import CSV File** dialog box.

**Step 3** If you have not already created a provider CSV file to import:

- Click the **Download sample 'Provider template (\*.csv)' file** link and save the CSV file template to a local storage resource.
- Open the template using your preferred tool. Begin adding rows to the file, one row for each provider.

Use a semicolon to separate multiple entries in the same field. Use two semicolons with no space between them to indicate that you are leaving the field blank. When you separate entries with semicolons, the order in which you enter values is important. For example, if you enter **SSH ; SNMP ; NETCONF ; TELNET** in the **connectivity\_type** field and

you enter **22 ; 161 ; 830 ; 23** in the **connectivity\_port** field, the order of entry determines the mapping between the two fields:

- SSH: port 22
- SNMP: port 161
- NETCONF: port 830
- Telnet: port 23

| Field                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Required or Optional                                                                                      |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <b>Provider Name</b>           | Enter the name for the provider that will be used in Crosswork Optimization Engine. For example: <b>MySRPCE</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Required                                                                                                  |
| <b>Connectivity Type</b>       | Enter the name of the protocol that Crosswork Optimization Engine will use to connect to the provider. For example:<br><b>ROBOT_MSVC_TRANS_HTTP</b> = HTTP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Required                                                                                                  |
| <b>Connectivity IPv4</b>       | Enter the IPv4 address of the provider.<br><br>If you are using the DNS hostname as the <b>provider_name</b> , the IP address is resolved automatically                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Required                                                                                                  |
| <b>Connectivity IPv6</b>       | Leave blank. Reserved for future use                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Optional                                                                                                  |
| <b>Connectivity Port</b>       | Enter the port number to use to connect to the provider's server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Required                                                                                                  |
| <b>Connectivity Timeout</b>    | Enter the amount of time (in seconds) to wait before the connection to the provider times out. The default is 30 seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Optional                                                                                                  |
| <b>Credential Profile Name</b> | Enter the name of the credential profile that Crosswork Optimization Engine will use to connect to the provider. This profile must already exist in the system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Required                                                                                                  |
| <b>Provider Device Key</b>     | Enter the enum value corresponding to the key that the Cisco NSO provider uses to identify devices uniquely. This will serve as the way Crosswork Optimization Engine maps the device to the Cisco NSO provider. Valid values are: <ul style="list-style-type: none"> <li>• <b>ROBOT_PROVDEVKEY_HOST_NAME</b>—If you are using the device hostname as the device ID within NSO, this value must match the hostname that is specified for the device in the inventory.</li> <li>• <b>ROBOT_PROVDEVKEY_NODE_IP</b>—Use this enum value if the NSO device identifier is the IP address for the Node IP value in the CSV file.</li> <li>• <b>ROBOT_PROVDEVKEY_INVENTORY_ID</b>—Use this enum value if the inventory ID is the device identifier for NSO.</li> </ul> | This entry is only required if you are creating or updating a Cisco NSO provider. Otherwise, leave blank. |
| <b>Family</b>                  | Enter <b>ROBOT_PROVIDER_SR_PCE</b> or <b>ROBOT_PROVIDER_SR_NSQ</b> . Do not choose other options as they are reserved for use by other Cisco Network Automation applications.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Required                                                                                                  |

| Field                | Description                                                                                                                                                                                                                                                                                                       | Required or Optional                                                                                         |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| <b>Model Prefix</b>  | If you are adding a Cisco NSO provider: Select the model prefix that matches the NED CLI used by the NSO server. Valid entries are: <b>Cisco-IOS-XR</b> , <b>Cisco-NX-OS</b> , <b>Cisco-IOS-XE</b> .<br><br>For telemetry, only Cisco-IOS-XR is supported.                                                        | Required for Cisco NSO providers only                                                                        |
| <b>Model Version</b> | If you adding a Cisco NSO provider: Enter the Cisco NSO NED driver version used on the server.                                                                                                                                                                                                                    | Required for Cisco NSO providers only                                                                        |
| <b>Properties</b>    | Enter the Cisco SR-PCE appropriate auto-onboard entries:<br><del>auto-onboard: &lt;auto-onboard-property&gt; device-profile: &lt;SR-PCE-credential-profile-name&gt;</del><br>For example:<br><b>auto-onboard:managed;device-profile:cisco</b><br><br>See <a href="#">Add Cisco SR-PCE Providers, on page 32</a> . | This entry is only required if you are creating or updating a Cisco SR-PCE provider. Otherwise, leave blank. |

Be sure to delete the sample data rows before saving the file, or they will be imported along with the data you want. The column header row can stay, as it is ignored during import.

c) When you are finished, save the new CSV file.

**Step 4** Click **Browse** to navigate to the CSV file you just created and then click **Open** to select it.

**Step 5** With the CSV file selected, click **Import**.

The provider information you imported should now be displayed in the **Providers** window.

**Step 6** Resolve any errors reported during the import and check provider details to confirm connection.

## Get Provider Details

Use the **Providers** window to get details about your providers and to check on their reachability.

**Step 1** From the main menu, choose **Inventory Management > Providers**.

For each provider configured in Cisco Crosswork Optimization Engine, the **Providers** window lists information such as the provider's name, universally unique identifier (UUID), associated credential profile, device key, and more, as shown in the figure below.

**Figure 7: Providers Window**




| Rea...                   | Provide... | UUID                       | Credential... | Connect... | Provider D... | Family         | Model Prefix | Model Version |
|--------------------------|------------|----------------------------|---------------|------------|---------------|----------------|--------------|---------------|
| <input type="checkbox"/> | xtc-CE2    | 5841cb3d-92b6-312c-8b7...  | XTC1-CE2      | HTTP       |               | SR_PCE         |              |               |
| <input type="checkbox"/> | xtc-CE4    | 313b3a98-36e8-3ec1-90b...  | XTC1-CE2      | HTTP       |               | SR_PCE         |              |               |
| <input type="checkbox"/> | NSO179     | de20c619-55e8-3f70-84f1... | NSO-Cred      | NETCONF    | NODE_IP       | NSO            | Cisco-IOS-XR | 6.6.2         |
| <input type="checkbox"/> | Syslog     | 6e9a49a1-1054-3758-85c...  | syslog        | SSH        |               | SYSLOG_STOR... |              |               |



**Step 2** The icons in the **Reachability** column indicate whether a provider is reachable via the listed connectivity protocols. For a description of each icon and its meaning, see [Reachability and Operational State, on page 21](#).

Cisco Crosswork Optimization Engine checks provider reachability immediately after a provider is added or modified. Other than these events, Cisco Crosswork Optimization Engine checks SR-PCE reachability about every 10 seconds.

**Step 3** Get additional details for any provider, as follows:

- a) In the **Provider Name** column, click the  to view provider-specific key/value properties.
- b) In the **Connectivity Type** column, click the  to view detailed connectivity information for the provider, such as provider-specific protocol, IP format, IP address, port, and timeout information.
- c) When you are finished, click  to close the details window.

If you are running into Cisco SR-PCE reachability problems, see [Cisco SR-PCE Reachability Issues, on page 35](#).

---

## Edit Providers

When editing provider settings, be aware that a provider can be mapped to many devices.



### Note


- Before making any changes to a provider configuration you should be certain that you understand the full impact of the change. If you are unsure about the potential risk of making a change, contact Cisco services for guidance.
- See [Add Cisco SR-PCE Providers, on page 32](#) before modifying an SR-PCE provider. There are additional steps that must be done when editing an SR-PCE provider.

---

Before editing any provider, it is always good practice to export a CSV backup of the providers you want to change (see [Export Providers, on page 42](#)).

---

**Step 1** From the main menu, choose **Inventory Management > Providers**.

**Step 2** In the **Providers** window, choose the provider you want to update and click .

**Step 3** Make the necessary changes and then click **Save**.

**Step 4** Resolve any errors and confirm provider reachability.

---

## Delete Providers

Follow the steps below to delete a provider.




**Note** If an SR-PCE provider's auto-onboard **managed** or **unmanaged** options are set, you must do one of the following:

- Reconfigure and remove the devices from the network before deleting the device from Cisco Crosswork Optimization Engine. This avoids Cisco Crosswork Optimization Engine from rediscovering and adding the device back to Cisco Crosswork Optimization Engine.
- Set auto-onboard to **off**, and then delete the device from Cisco Crosswork Optimization Engine. However, doing so will not allow Cisco Crosswork Optimization Engine to detect or auto-onboard any new devices in the network.

You are alerted when you try to delete a provider that is associated with one or more devices or credential profiles.

**Step 1** Export a backup CSV file containing the provider you plan to delete (see [Export Providers, on page 42](#)).

**Step 2** Delete the provider as follows:

- From the main menu, choose **Inventory Management > Providers**.
- In the **Providers** window, choose the provider(s) that you want to delete and click .
- In the confirmation dialog box, click **Delete**.

## Export Providers

You can quickly export provider data to a CSV file. This is a handy way to keep backup copies of your provider information.




**Note** You cannot edit a CSV file and then re-import it to update existing providers.

**Step 1** From the main menu, choose **Inventory Management > Providers**.

**Step 2** (Optional) In the **Providers** window, filter the provider list as needed.

**Step 3** Check the check boxes for the providers you want to export. Check the check box at the top of the column to select all the providers for export.

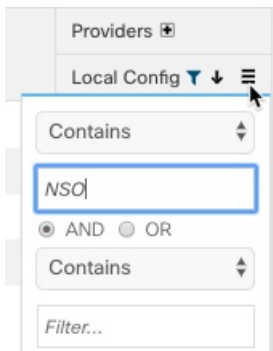
**Step 4** Click . Depending on your browser, you will be prompted to select a path and file name to use when saving the CSV file, or to open it immediately.

## View Devices Assigned to a Provider

To see a list of devices that are assigned to a particular Cisco NSO provider:

- Step 1** From the main menu, choose **Inventory Management > Devices**.
- Step 2** In the **Devices** window, scroll across the table until you find the **Providers** column.
- Step 3** Under the Local Config field, set the filter criteria by selecting the logical operator from the drop down list in the first field, and then enter the Provider name in the second field.

**Figure 8: Filter Providers Column**

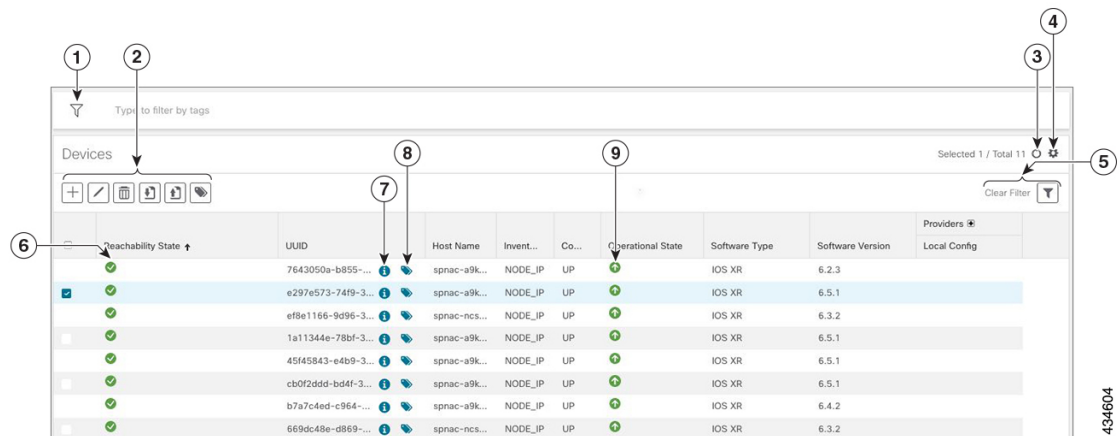


The table displays only the devices with the Provider criteria you entered.












## Manage Devices

The Inventory Management application's **Devices** window (shown below) gives you a consolidated list of all your devices and their status. To view the **Devices** window, select **Inventory Management > Devices**.

**Figure 9: Devices Window**



| Item | Description                                                                                                                                                                                                                                 |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | The <b>Filter by tags</b> field lets you filter the devices by the tags applied to them. Type the name of the tag that has been applied to the device that you are trying to find. See <a href="#">Filter Devices by Tags, on page 53</a> . |

| Item | Description                                                                                                                                                                                                                                                                                                                                                                  |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2    | Click  to add a new device to the device inventory. See <a href="#">About Adding Devices, on page 17</a> .                                                                                                                                                                                  |
|      | Click  to edit the information for the currently selected devices. See <a href="#">Edit Devices, on page 53</a> .                                                                                                                                                                           |
|      | Click  to delete the currently selected devices. See <a href="#">Delete Devices, on page 54</a> .                                                                                                                                                                                           |
|      | Click  to import new devices and update existing devices, using a CSV file. You can also download a CSV file template by clicking this icon. The template includes sample data that you can use as a guide for building your own CSV file. See <a href="#">Import Devices, on page 44</a> . |
|      | Click  to export information for selected devices to a CSV file. See <a href="#">Export Devices, on page 54</a> .                                                                                                                                                                           |
|      | Click  to modify tags applied to the selected devices. See <a href="#">Apply or Remove Device Tags, on page 58</a> .                                                                                                                                                                        |
| 3    | Click  to refresh the Devices list.                                                                                                                                                                                                                                                         |
| 4    | Click  to select which columns to display in the Devices list (see <a href="#">Set, Sort and Filter Table Data, on page 6</a> ).                                                                                                                                                            |
| 5    | Click  to set filter criteria on one or more columns in the Devices list.                                                                                                                                                                                                                 |
|      | Click the <b>Clear Filter</b> link to clear any filter criteria you may have set.                                                                                                                                                                                                                                                                                            |
| 6    | Icons in the <b>Reachability State</b> column show whether a device is reachable or not. See <a href="#">Reachability and Operational State, on page 21</a> .                                                                                                                                                                                                                |
| 7    | Click  to open the <b>Device Details</b> pop-up window, where you can view important information for the selected device. See <a href="#">Get Device Details, on page 51</a> .                                                                                                            |
| 8    | Click  to see all the tags that have been applied to the device. See <a href="#">Manage Tags, on page 56</a> .                                                                                                                                                                            |
| 9    | Icons in the <b>Operational State</b> column show whether a device is operational or not. See <a href="#">Reachability and Operational State, on page 21</a>                                                                                                                                                                                                                 |

## Import Devices

Complete the steps below to create a CSV file that specifies multiple devices and then import it into Cisco Crosswork Optimization Engine.

Importing devices from a CSV file adds any devices not already in the database. The **Update Existing** option overwrites the data in any device record with an Inventory Key Type and device key field value that matches those of an imported device (this excludes the UUID, which is set by the system and not affected by import).

For this reason, it is a good idea to export a backup copy of all your current devices before an import (see [Export Devices, on page 54](#)).




---

**Note** If you plan on using a CSV file to import devices managed by Cisco Network Services Orchestrator (Cisco NSO), you must prepare the CSV following the guidelines given in [Sample Configuration for Devices in Cisco NSO, on page 20](#).

---

**Step 1** From the main menu, choose **Inventory Management > Devices**.

**Step 2** Click  to open the **Import CSV File** dialog box.

**Step 3** If you have not already created a device CSV file to import:

- a) Click the **Download sample 'Device Management template (\*.csv)' file** link and save the CSV file template to a local storage resource.
- b) Open the template using your preferred tool. Begin adding rows to the file, one row for each device.

Use a semicolon to separate multiple entries in the same field. Use two semicolons with no space between them to indicate that you are leaving the field blank. When you separate multiple entries with semicolons, remember that the order in which you enter values in each field is important. For example, if you enter **SSH ; SNMP ; NETCONF ; TELNET** in the **Connectivity Type** field and you enter **22 ; 161 ; 830 ; 23** in the **Connectivity Port** field, the order of entry determines the mapping between the two fields:

- SSH: port 22
- SNMP: port 161
- NETCONF: port 830
- Telnet: port 23

For a list of the fields and the values you can enter, see the "Add New Device" field table in [Add Devices Through the UI, on page 46](#).

Be sure to delete the sample data rows before saving the file, or they will be imported along with the data you want. The column header row can stay, as it is ignored during import.

- c) When you are finished, save the new CSV file.



**Step 4** Click **Browse** to navigate to the CSV file you just created and then click **Open** to select it.

**Step 5** With the CSV file selected, click **Import** to add new devices or **Update Existing** to add or change data to devices already in the system.

**Step 6** Resolve any errors and confirm device reachability.

The device information you imported should be displayed in the **Devices** window within a few minutes (see [Manage Devices, on page 43](#)).

It is normal for devices to show as unreachable or not operational when they are first imported. However, if after 30 minutes they are still displayed as unreachable or not operational, there is an issue that needs to be investigated. To

investigate, select **Inventory Management > Job History** and click on any   you see in the **Status** column. Common issues include failure to ensure the associated credential profile contains the correct credentials. You can test this by

opening a terminal window on the Cisco Crosswork Optimization Engine server and then trying to access the device using the protocol and credentials specified in the associated credential profile.

## Add Devices Through the UI

Follow the steps below to add devices one by one, using the GUI. Under normal circumstances, you will want to use this method when adding one or a few devices only .

### Before you begin

Be sure you have completed the planning steps and setup requirements discussed in [Get Started, on page 9](#), and that the devices themselves have been pre-configured as explained in [Prerequisites for Onboarding Devices, on page 19](#).




- Step 1** From the main menu, choose **Inventory Management > Devices**. The **Devices** window opens.
- Step 2** Click .
- Step 3** Enter values for the new device, as listed in the table below.
- Step 4** Click **Save**. (The Save button is disabled until all mandatory fields are complete.)
- Step 5** (Optional) Repeat to add more devices.

Table 4: Add New Device Window (\*=Required)

| Field              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| * Configured State | The management state of the device. Options are <ul style="list-style-type: none"> <li>• <b>UNMANAGED</b>—Cisco Crosswork Optimization Engine is not monitoring the device.</li> <li>• <b>DOWN</b>—The device is being managed and is down.</li> <li>• <b>UP</b>—The device is being managed and is up.</li> </ul>                                                                                                                                  |
| Reachability Check | Determines whether Cisco Crosswork Optimization Engine performs reachability checks on the device. Options are: <ul style="list-style-type: none"> <li>• <b>ENABLE/REACH_CHECK_ENABLE</b>—Checks for reachability and then updates the Reachability State in the UI automatically.</li> <li>• <b>DISABLE/REACH_CHECK_DISABLE</b>—The device reachability check is disabled.</li> </ul> Cisco recommends that you always set this to <b>ENABLE</b> . |
| Credential Profile | The name of the credential profile assigned to the device and used to access it for data collection and configuration changes. For example: <b>nso23</b> or <b>srpce123</b> .                                                                                                                                                                                                                                                                       |

| Field                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| * <b>Inventory Key Type</b>         | The type of identification key for the device. You must choose one of the available types. In all cases other than <b>UUID</b> , you must enter the corresponding key field with a unique ID value. For example: If you choose <b>HOST_NAME</b> as the * <b>Inventory Key Type</b> , you must fill in the <b>Host Name</b> field with the unique host name of the device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| * <b>Host Name</b>                  | The hostname of the device. Required only if * <b>Inventory Key Type</b> is <b>HOST_NAME</b> . Otherwise, Cisco Crosswork Optimization Engine discovers it and updates it.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Inventory ID</b>                 | Inventory ID value for the device. Required only if * <b>Inventory Key Type</b> is <b>INVENTORY_ID</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>UUID</b>                         | Universally unique identifier (UUID) for the device. If you choose <b>UUID</b> as the * <b>Inventory Key Type</b> , leave this field blank.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Serial Number</b>                | Serial number for the device. Required only if * <b>Inventory Key Type</b> is <b>SERIAL_NUMBER</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Node IP</b>                      | Node IP value for the device. Required only if * <b>Inventory Key Type</b> is <b>NODE_IP</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>MAC Address</b>                  | MAC address for the device. Required only if * <b>Inventory Key Type</b> is <b>MAC</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| * <b>Capability</b>                 | The capabilities that allow collection of device data and that are configured on the device. You must select at least <b>SNMP</b> , as this is a required capability. The device will not be onboarded if <b>SNMP</b> is not configured. Other options are <b>YANG_MDT</b> , <b>TL1</b> , <b>YANG_CLI</b> , and <b>YANG-EPNM</b> . The capabilities you select will depend on the device software type and version.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Tags</b>                         | The available tags to assign to the device.<br><br>Use device tags to group devices for monitoring, and to provide additional information that might be of interest to other users, such as the device's physical location and its administrator's email ID. For more information, see <a href="#">Manage Tags</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Connectivity Details</b>         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Protocol</b>                     | The connectivity protocols used by the device. Choices are: <b>SSH</b> , <b>SNMP</b> , <b>NETCONF</b> , <b>TELNET</b> , <b>HTTP</b> , and <b>HTTPS</b> .<br><br>To add more connectivity protocols for this device, click  at the end of the first row in the <b>Connectivity Details</b> panel. To delete a protocol you have entered, click  shown next to that row in the panel.<br><br>You can enter as many sets of connectivity details as you want, including multiple sets for the same protocol. You must enter details for at least <b>SSH</b> and <b>SNMP</b> . If you do not configure <b>SNMP</b> , the device will not be on-boarded. If you want to manage the device (or you are managing XR devices), you must enter details for <b>NETCONF</b> . <b>TELNET</b> connectivity is optional. |
| * <b>IPv4 Address / Subnet Mask</b> | Enter the device's IPv4 address and CIDR subnet mask.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>IPv6 Address / Subnet Mask</b>   | Enter the device's IPv6 address and subnet mask.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

| Field                                                                                                                                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>* Port</b>                                                                                                                                                               | The port used for this connectivity protocol. Each protocol is mapped to a port, so be sure to enter the port number that corresponds to the <b>Protocol</b> you chose. The standard port assignments for each protocol are: <ul style="list-style-type: none"> <li>• SSH: 22</li> <li>• SNMP: 161</li> <li>• NETCONF: 830</li> <li>• TELNET: 23</li> <li>• HTTP: 80</li> <li>• HTTPS: 443</li> </ul> |
| <b>Timeout</b>                                                                                                                                                              | The elapsed time (in seconds) before communication attempts using this protocol will time out. The default value is 30 seconds. For XE devices using NETCONF, the recommended minimum timeout value is 90 seconds. For all other devices and protocols, the recommended minimum timeout value is 60 seconds.                                                                                          |
| <b>Routing Info</b>                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>ISIS System ID</b>                                                                                                                                                       | The device's IS-IS system ID. This ID identifies the router in an IS-IS topology, and is required for SR-PCE integration.                                                                                                                                                                                                                                                                             |
| <b>OSPF Router ID</b>                                                                                                                                                       | The device's OSPF router ID. This ID identifies the router in an OSPF topology, and is required for SR-PCE integration.                                                                                                                                                                                                                                                                               |
| <b>Streaming Telemetry Config</b>                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Telemetry Interface Source VRF</b>                                                                                                                                       | Name of the VRF in whose context Model Driven Telemetry (MDT) traffic is routed.                                                                                                                                                                                                                                                                                                                      |
| <b>Location</b>                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                       |
| All location fields are optional, with the exception of <b>Longitude</b> and <b>Latitude</b> , which are required for a correct geographical view of your network topology. |                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Longitude, Latitude</b>                                                                                                                                                  | Entries in these fields are recommended. Without <b>Longitude</b> and <b>Latitude</b> values, the topology map's geographical view shows all devices and links bunched together at the same spot. With these values, the map can present the correct geographical location of each device and its links to other nodes.                                                                               |
| <b>Altitude</b>                                                                                                                                                             | The altitude, in feet or meters, at which the device is located. For example, <b>123</b> .                                                                                                                                                                                                                                                                                                            |
| <b>Providers and Access</b>                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Local Config: Device Key and Provider</b>                                                                                                                                | This field is mandatory only when mapping an NSO provider. The Device Key will automatically populate and the Credential Profile appears.<br>For CSV entry, use <code>ROBOT_PROVIDER_LOCAL_CONFIG</code> and enter the Provider name.                                                                                                                                                                 |
| <b>Compute Config: Device Key and Provider</b>                                                                                                                              | (Optional) Provider name used for topology computation. Choose a provider from the list.<br>For CSV entry, use <code>ROBOT_PROVIDER_COMPUTE</code> and enter the Provider name.                                                                                                                                                                                                                       |



### Example

*Figure 10: Add Device Window*

Add New Device



\*Configured State UNMANAGED  
 Reachability Check  
 Credential Profile NSO-Cred  
 \*Inventory Key Type NODE\_IP  
 Host Name  
 Inventory ID  
 UUID  
 Serial Number  
 \*Node IP 172. /  
 Mac Address  
 Capability Select capability  
 Tags Select Tags

Connectivity Details

| Protocol | IPv4 Address / Subnet Mask | IPv6 Address / Subnet Mask | Port | Timeout |
|----------|----------------------------|----------------------------|------|---------|
| NETCONF  | 172. /24                   |                            | 23   | 60      |

Routing Info

IS-IS System ID  
 OSPF Router ID

Streaming Telemetry config

Telemetry Interface Source VRF

Location

Building ABC\_Building  
 Street Cisco123 St  
 City San Jose  
 State CA - California  
 Country United States  
 Region California  
 Zip 95128  
 Latitude  
 Longitude  
 Altitude

Providers and Access

Local Config


Provider NSO179  
 Device Key 172.  
 Credential Profile NSO-Cred

Compute Config

Provider xtc-CE2  
 Credential Profile XTC1-CE2

Save Cancel

## Get Device Details

Whenever you select **Inventory Management > Devices** and display the list of devices, you can click  next to any listed device to get more information about that device. Clicking this icon opens the **Details for DeviceName** pop-up window, as shown in the following example:

*Figure 11: Details for DeviceName Window*

Expand the **Connectivity Details** area at the top of the pop-up window (if it is not already expanded). This area shows the reachability status for all transport types (for help with the icons shown in this area, see [Device and Link Icons, on page 64](#)).

Expand and collapse the other areas of the pop-up window, as needed. Click **X** to close the window.

## Filter Devices by Tags

By creating a tag and assigning it to a particular device, you can easily provide additional information that might be of interest to other users, such as the device's physical location and its administrator's email ID. You can also use tags to find and group devices with the same or similar tags in any window that lists devices.

For help with tagging your devices, see [Apply or Remove Device Tags, on page 58](#). For help with creating and deleting tags, see [Manage Tags, on page 56](#).

To filter devices by tags:

- 
- Step 1** Display the **Devices** window by choosing **Inventory Management > Devices**.
- Step 2** In the **Type to filter by tags** bar at the top of the user interface, type all or part of the name of a tag.
- The **Type to filter by Tags** bar has a type-ahead feature: As you start typing, the field shows a drop-down list of tags that match all the characters you have typed so far. To force the drop-down list to display all available tags, type **\***.
- Step 3** Choose the name of the tag you want to add to the filter. The filter appears in the **Type to filter by tags** filter bar. The table or map shows only the devices with that tag.
- Step 4** If you want to filter on more than one tag:
- Repeat Steps 2 and 3 for each additional tag you want to set as part of the filter.
  - When you have selected all the tags you want, click **Apply Filters**. The table or map shows only the devices with tags that match **all** the tags in your filter.
- Step 5** To clear all tag filters, click the **Clear Filters** link. To remove a tag from a filter containing multiple tags, click the **X** icon next to that tag's name in the filter.
- 

## Edit Devices

Complete the following procedure to update a device's information.

Before editing any device, it is always good practice to export a CSV backup of the devices you want to change (see [Export Devices, on page 54](#)).

- 
- Step 1** From the main menu, choose **Inventory Management > Devices**.
- Step 2** (Optional) In the **Devices** window, filter the list of devices by filtering specific columns.
- Step 3** Check the check box of the device you want to change, then click
- Step 4** Edit the values configured for the device, as needed.
- For a description of the fields you can update, see [Add Devices Through the UI](#).
- Step 5** Click **Save**. (The Save button remains dimmed until all required fields are filled in.)

**Step 6** Resolve any errors and confirm device reachability.

---

## Delete Devices

Complete the following procedure to delete devices.

### Before you begin

- If the auto-onboard **managed** or **unmanaged** options are set for the SR-PCE provider, you should set auto-onboard for the SR-PCE(s) to **off**.
- Confirm that the device is not connected to the network or that it is powered off before deleting the device.



### Note


- If devices are mapped to NSO with MDT capability, and telemetry configuration is pushed, then those configurations will be removed from the device.
  - If auto-onboard is not set to **off**, and it is still functional and connected to the network, the device will be rediscovered as unmanaged as soon as it is deleted.
- 

**Step 1** Export a backup CSV file containing the devices you plan to delete (see [Export Devices, on page 54](#)).

**Step 2** From the main menu, choose **Inventory Management > Devices**.

**Step 3** (Optional) In the **Devices** window, filter the list of devices by entering text in the **Search** field or filtering specific columns.

**Step 4** Check the check boxes for the devices you want to delete.

**Step 5** Click  to change each device's state to ADMIN DOWN or UNMANAGED.

If you want to delete devices in bulk, Cisco recommends that you change the device state in this manner in batches of 50 devices, then complete deletion of these devices before deleting another batch.

**Step 6** Click .

**Step 7** In the confirmation dialog box, click **Delete**.

---


## Export Devices

When you export the device list, all device information is exported to a CSV file. Exporting the device list is a handy way to keep a record of all devices in the system at one time. You can also edit the CSV file as needed, and re-import it to overwrite existing device data.

---

**Step 1** From the main menu, choose **Inventory Management > Devices**.

**Step 2** (Optional) In the **Devices** window, filter the device list as needed.



- Step 3** Check the check boxes for the devices you want to export. Check the check box at the top of the column to select all the devices for export.
- Step 4** Click . Your browser will prompt you to select a path and the file name to use when saving the CSV file, or to open it immediately


## View Device Job History
















Inventory Management collects and stores information about device-related jobs. Follow the steps below to track all create, update and delete activities.

- Step 1** From the main menu, choose **Inventory Management > Job History**. The **Job History** window displays a log of all device-related jobs, like the one shown below.

**Figure 12: Job History Window With Error Details Popup**

Inventory Jobs Total 48  


Clear Filter 

| Start Time               | End Time                 | Status                                                                                                                                                                         | Transaction ID                 | Description                   | User Name |
|--------------------------|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|-------------------------------|-----------|
| Thu Jul 11 2019 00:29:45 | Thu Jul 11 2019 00:29:45 |  Completed                                                                                    | 2df5abfb-a773-44cf-90eb-bb3... | Update 1 Provider(s)          | admin     |
| Thu Jul 11 2019 00:29:37 | Thu Jul 11 2019 00:29:37 |  Completed                                                                                    | a48fc525-294f-401c-931f-6ec... | Insert 1 Credential(s)        | admin     |
| Thu Jul 11 2019 00:29:06 | Thu Jul 11 2019 00:29:06 |  Completed                                                                                    | b2ff90c2-ada7-449b-9e1c-34b... | Insert 1 Provider(s)          | admin     |
| Wed Jul 10 2019 23:54:27 | Wed Jul 10 2019 23:54:27 |  Failed  | f9bbc535-109e-4621-a1c5-c6...  | Delete 7 Tag(s)               | admin     |
| Wed Jul 10 2019 23:51:51 | Wed Jul 10 2019 23:51:51 |  Completed                                                                                  | b6362a8a-7ff9-4d9d-9c6d-d1...  | Insert 1 Tag(s)               | admin     |
| Wed Jul 10 2019 23:30:25 | Wed Jul 10 2019 23:30:25 |  Completed                                                                                  | b34cb396-9077-4561-a294-e...   | Update 8 Node(s) Via CS...    | admin     |
| Wed Jul 10 2019 23:28:32 | Wed Jul 10 2019 23:28:32 |  Completed                                                                                  | 2823a33e-8ce1-499d-89f1-9c...  | Update 1 Node(s)              | admin     |
| Wed Jul 10 2019 23:28:32 | Wed Jul 10 2019 23:28:32 |  Completed                                                                                  | 662ffc8c-4992-4778-a7ba-22b... | Unassign Tags                 | admin     |
| Wed Jul 10 2019 23:28:26 | Wed Jul 10 2019 23:28:26 |  Completed                                                                                  | 180a0b48-cacc-48e2-913c-5a...  | Update 1 Node(s)              | admin     |
| Wed Jul 10 2019 23:22:45 | Wed Jul 10 2019 23:22:45 |  Failed  | 455409d4-f69d-4e8e-951f-4d...  | Insert 2 Provider(s) Via C... | admin     |
| Wed Jul 10 2019 23:14:18 | Wed Jul 10 2019 23:14:18 |  Failed  |                                |                               |           |
| Wed Jul 10 2019 23:14:10 | Wed Jul 10 2019 23:14:10 |  Completed                                                                                  |                                |                               |           |

**Error Details**

[ErrCannotDeleteProvider]: Provider xtc-CE2 is in use and cannot be deleted.

The jobs display in descending order of creation time. The most recent job is shown first. To sort the data in the table, click a column heading. You can toggle between ascending and descending sort order (for more help, see [Set, Sort and Filter Table Data, on page 6](#)).

- Step 2** The **Status** column shows three types of states: completed, failed, and partial. For any failed or partial job, click  shown next to the error for information.

Error information may include `clean-up failure` events as audit messages. These messages indicate that Cisco Crosswork Network Automation configuration objects on the device could not be removed, and will explain why they could not be removed. Users will need to take manual action to remove them. This typically involves deleting any XR telemetry configuration objects with names starting with `CW_`.

# Manage Tags

Use the **Tag Management** window to manage the tags available for assignment to the devices in your network. Tags can provide information such as the device's physical location and its administrator's email ID, and are used to group devices.

To open this window, choose **Inventory Management > Tags** from the main window.

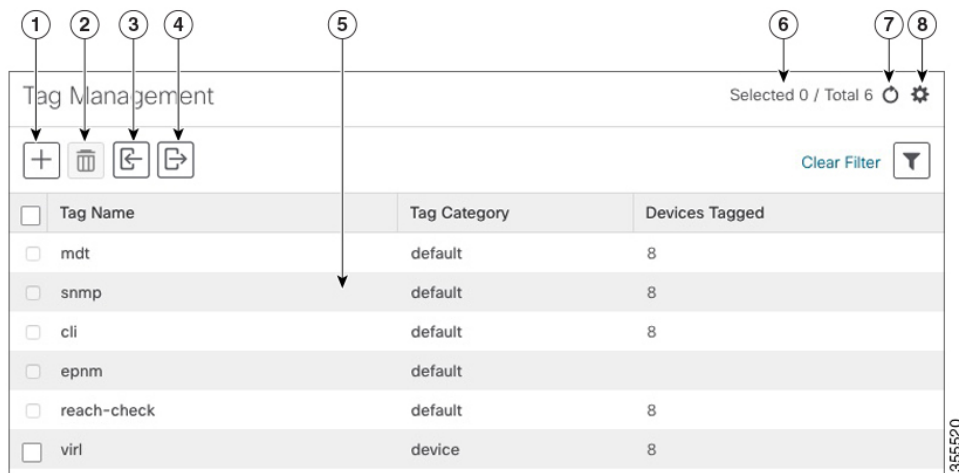


**Note** Cisco Crosswork Optimization Engine automatically creates a default set of tags and assigns them to every device it manages:

- cli
- mdt
- reach-check
- snmp
- clock-drift-check






You cannot select, edit, delete, or manually associate these default tags with any device.

**Figure 13: Tag Management Window**



| Item | Description                                                                        |
|------|------------------------------------------------------------------------------------|
| 1    | Click  to create new device tags. See <a href="#">Create Tags</a> .                |
| 2    | Click  to delete currently selected device tags. See <a href="#">Delete Tags</a> . |



| Item | Description                                                                                                                                                                                                                                                                                                                                                                                   |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3    | Click  to import the device tags defined in a CSV file into Cisco Crosswork Network Automation. See <a href="#">Import Tags, on page 58</a> . You can also download a CSV file template by clicking this icon. The template includes sample data that you can use as a guide for building your own CSV file. |
| 4    | Click  to export a CSV file that lists the tags that are currently configured and their attributes. You can update this file and import it back into Cisco Crosswork Optimization Engine to quickly add or edit multiple tags. See <a href="#">Export Tags, on page 59</a> .                                 |
| 5    | Displays the tags currently available in Cisco Crosswork Optimization Engine and their attributes.                                                                                                                                                                                                                                                                                            |
| 6    | Indicates the number of tags that are currently selected in the table.                                                                                                                                                                                                                                                                                                                        |
| 7    | Click  to refresh the <b>Tag Management</b> window.                                                                                                                                                                                                                                                          |
| 8    | Click  to choose the columns to make visible in the <b>Tag Management</b> window (see <a href="#">Set, Sort and Filter Table Data, on page 6</a> ).                                                                                                                                                          |
|      | Click  to set filter criteria on one or more columns in the <b>Tag Management</b> window.                                                                                                                                                                                                                    |
|      | Click the <b>Clear Filter</b> link to clear any filter criteria you may have set.                                                                                                                                                                                                                                                                                                             |

## Create Tags

You can create as many tags and tag categories as you want.

**Step 1** From the main menu, choose **Inventory Management > Tags**. The **Tag Management** window opens.

**Step 2** Click . The **Create New Tags** pane opens.

**Step 3** In the **Category** area:

- To associate your new tags with an existing category: Choose the category from the drop-down list.
- To associate your new tags with a new category: Click the **New Category** link, enter the new category's name in the text field, and click **Save**.

All the new tags you create after this step will be assigned to the category you selected or created.

**Step 4** In the **Tags** area: Start entering the names of the new tags that you want to create. Press **Return** after you type each tag.

To keep from entering duplicate tags, click the **Show Tags** link. The **Create New Tags** window will list only the tags that already exist in your currently selected category.

**Step 5** When you are finished entering new Tag names, click **Save**.

**What to do next**

Add tags to devices. See [Apply or Remove Device Tags, on page 58](#).


## Import Tags

Complete the steps below to create a CSV file that specifies tags and then import it into Cisco Crosswork Optimization Engine. This is the easiest way to create a lot of new tags and tag categories quickly.

You can create as many tags and tag categories as you want. Tag and tag category names are case-insensitive and can contain up to 128 alphanumeric characters. They cannot contain special characters, symbols, or spaces.

Importing adds any tags not already in the database, and overwrites the data in any tags with the same name as an imported tag. For this reason, it is a good idea to export a backup copy of all your current tags before import (see [Export Tags, on page 59](#)).

**Step 1** From the main menu, choose **Inventory Management > Tag Management**.

**Step 2** Click  to open the **Import CSV File** dialog box.

**Step 3** If you have not already created a provider CSV file to import:

- a) Click the **Download sample 'Tags template (\*.csv)' file** link and save the CSV file template to a local storage resource.
- b) Open the template using your preferred tool. Begin adding rows to the file, one row for each tag. Use a comma to delimit each field within a row. Use a semicolon to separate multiple entries in the same field.

| Field        | Description                                                    | Required or Optional |
|--------------|----------------------------------------------------------------|----------------------|
| Tag Name     | Enter the name of the tag. For example: <b>San Francisco</b> . | Required             |
| Tag Category | Enter the tag category. For example: <b>City</b> .             | Required             |

Be sure to delete the sample data rows before saving the file, or they will be imported along with the data you want. The column header row can stay, as it is ignored during import.

- c) When you are finished, save the new CSV file.

**Step 4** Click **Browse** to navigate to the CSV file you just created and then click **Open** to select it.

**Step 5** With the CSV file selected, click **Import**.

The tags and tag categories that you imported should now be displayed in the **Tag Management** window.

**What to do next**

Add tags to devices. See [Apply or Remove Device Tags, on page 58](#).



## Apply or Remove Device Tags

Tags and their categories are your main tool for grouping devices. Once you have tagged a set of devices with the same tag, they are considered part of a group, and you can manage them more easily.

In order to apply a tag to a device or group of devices, the tag must already exist (see [Create Tags, on page 57](#)).

You can apply a maximum of 15 tags to any one device.

To apply tags to a device or set of devices, do the following:

- 
- Step 1** From the main menu, choose **Inventory Management > Devices**. The **Devices** window opens, showing the list of devices.
  - Step 2** (Optional) If the list is long, click  to set one or more filters and narrow the list to only those devices you want to tag.
  - Step 3** Check the check box next to the device(s) you want to tag. If you select multiple devices, any changes you make will be applied to all the devices you selected.
  - Step 4** From the toolbar, click . The **Modify Tags** window opens, showing the tags currently applied to the device(s) you selected.
  - Step 5** Click in the **Type to autocomplete item** field to display the list of existing tags, or begin typing the name of the tag you want.
  - Step 6** Click on individual tags in the list to add them to the list of tags applied to the device(s). To delete an applied tag, click the X icon shown next to that tag.
- 

## Delete Tags


To delete device tags, do the following:



---

**Note** If the tag is mapped to any devices, then the tag cannot be deleted.


---

- 
- Step 1** Export a backup CSV file containing the tags you plan to delete (see [Export Tags, on page 59](#)).
  - Step 2** From the main menu, choose **Inventory Management > Tag Management**.
  - Step 3** Check the check box next to the tags you want to delete.
  - Step 4** From the toolbar, click .
  - Step 5** The confirmation dialog box will list the number of devices currently using the tag(s) you are about to delete. Click **Delete** to confirm deletion.
- 

## Export Tags

You can quickly export tags and tag categories to a CSV file. This will allow you to keep backup copies of your tags. You can also edit the CSV file as needed, and re-import it to overwrite existing tags. Note that you will need to re-associate devices and tags in some cases.

- 
- Step 1** From the main menu, choose **Inventory Management > Tags**.
  - Step 2** (Optional) In the **Tag Management** window, filter the tag list as needed.

- Step 3** Check the check boxes for the tags you want to export. Check the check box at the top of the column to select all the tags for export.
- Step 4** Click . Depending on your browser, you will be prompted to select a path and file name to use when saving the CSV file, or to open it immediately.
-



## CHAPTER 4

# Visualize the Network

---

Cisco Crosswork Optimization Engine provides a real-time graphical, topological map view of devices, links, and SR policies between them. This section focuses on device and link visualization features, and customizing the topology map.

For information on SR policy management and visualization, see [Visualize and Manage SR Policies, on page 75](#) and [Get Started with Function Packs, on page 129](#)).

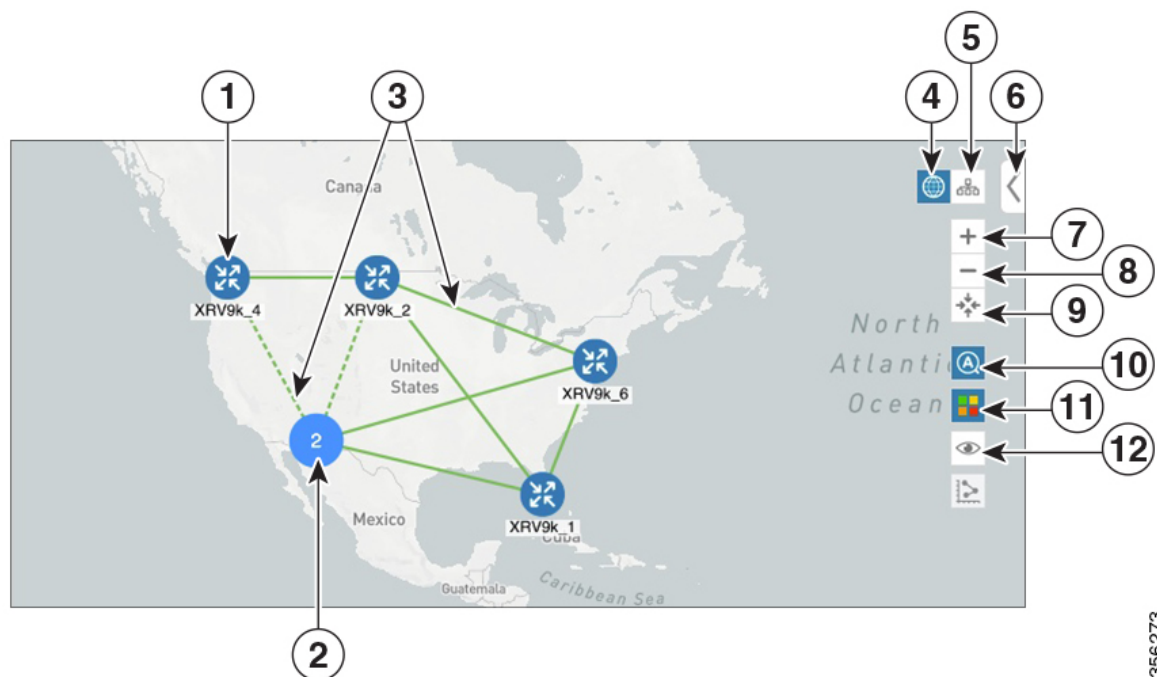
- [Network Topology Map, on page 61](#)
- [Visualize Devices, on page 68](#)
- [Visualize Links, on page 71](#)

## Network Topology Map

The network topology can be displayed on a logical map or a geographical map, where the devices and links are shown in their geographic context. From the map, you can drill down to get detailed information about devices and links.

To get to the topology map, choose **Optimization Engine** from the left navigation bar, and click **SR Policies**.

Figure 14: Network Topology Map - Devices and Links



356273

| Callout No. | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1           | <p><b>Single Device:</b> A blue device icon means the device is reachable; a gray icon means the device is not reachable.</p> <p>To view a device configuration summary, hover the mouse cursor over the device icon. A pop up window displaying the host name, state, node ID, and device type appears.</p> <p>To view device details, click on the device icon. The <b>Device Details</b> window appears to the right. See <a href="#">Get More Information About Devices on the Map, on page 68</a>.</p> |
| 2           | <p><b>Device Cluster:</b> If devices are in close physical proximity, the geographical map shows them as a cluster. The number in the blue circle indicates the number of devices in the cluster. Displaying devices in this manner helps prevent overlap and clutter on the map. In this example, there are two devices in the cluster. Click on the cluster to zoom in and see the individual devices.</p>                                                                                                |
| 3           | <p><b>Links:</b> A solid line indicates a <i>single link</i> between two devices. If there is more than one link between two devices, or between a device and a cluster of devices, the line is shown dashed instead. A dashed line indicates an <i>aggregated link</i> that represents more than one link.</p>                                                                                                                                                                                             |
| 4           | <p><b>Geographical Map:</b> Click this icon to view the geographical map.</p> <p>The geographical map shows single devices, device clusters, links, and SR policies, superimposed on a map of the world. Each device location on the map reflects the device's GPS coordinates (longitude and latitude) as defined in the device inventory.</p>                                                                                                                                                             |

| Callout No. | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5           | <p><b>Logical Map:</b> Click this icon to toggle from the geographical map to the logical map. The logical map shows devices and their links, positioned according to an automatic layout algorithm, ignoring their geographical location. You can change the layout algorithm; see <a href="#">Change the Layout of a Logical Map, on page 65</a>.</p> <p>The logical map displays up to 5000 devices and never displays devices in clusters.</p> <p>If you drill down to the logical map from a geographical cluster at the maximum zoom level, the logical map shows devices that are located in the same location. See <a href="#">Identify the Members of a Cluster, on page 70</a>.</p> |
| 6           | <p><b>Expand/Collapse/Hide Side Panel:</b> Expand or collapse the contents of the side panel. Close the side panel to get a larger view of the topology map.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 7           | <p><b>Zoom In:</b> Click this icon to zoom in on the selected area; for example, to view clustered devices on the geographical map.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 8           | <p><b>Zoom Out:</b> Click this icon to zoom out from a selection area.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 9           | <p><b>Zoom Fit:</b> Lets you automatically scale the map to fit your zoom area.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 10          | <p><b>Auto Zoom:</b> Zooms in on selected SR policies. This option is selected by default. If you uncheck this option, navigate away from the map, and later return to the map; it will revert to the default option.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 11          | <p><b>Bandwidth Utilization:</b> Lets you enable or disable visualization of the bandwidth utilization for the mapped links. See <a href="#">Show Bandwidth Utilization for Links on the Map, on page 73</a>. This option is selected by default. If you uncheck this option, navigate away from the map, and later return to the map; it will revert to the default option.</p>                                                                                                                                                                                                                                                                                                              |
| 12          | <p><b>Custom Map View:</b> Lets you create a named custom view using the settings and layout for your current map, or display a custom view you have created previously. See <a href="#">Create Custom Map Views, on page 66</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Troubleshoot Network Topology Map

If you encounter topology issues, such as topology components not rendering as expected or component data not displaying on the map, Cisco recommends the following:







- If you cannot see geographical map tiles: Make sure your browser has Internet connectivity to your selected geographical map services vendor. The map services vendor and the vendor's URL are set by the system administrator, as explained in [Configure Geographical Map Settings, on page 65](#).
- If your devices are missing from the geographical map: Ensure that latitude and longitude data was included when onboarding your devices, or entered later. Cisco Crosswork Optimization Engine cannot position devices properly on the geographical map without location information.
- Devices that do not have geographical coordinates default to 0° latitude and 0° longitude.
- If your devices are appearing in the wrong location on the geographical map, confirm that you have entered the latitude and longitude values in the correct order via the UI or in the CSV file you uploaded.

- If you are having intermittent problems displaying the map or your devices: Clear your browser cache and try again.




## Device and Link Icons

The following tables describe the icons used to represent device states, link states, and device types in the Cisco Crosswork Optimization Engine user interface.


**Table 5: Device State Icons**

| Icon                                                                                | Description                                                                                                                                                                                                                       |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | The device is reachable.                                                                                                                                                                                                          |
|    | The device is unreachable.                                                                                                                                                                                                        |
|    | The device has an unknown reachability state (its reachability cannot be determined).                                                                                                                                             |
|    | The device is operational.                                                                                                                                                                                                        |
|    | The device is not operational. It is either not up, or unreachable, or both.<br>A number in a circle is shown next to this icon. The number indicates the number of recent errors and can be clicked on to display error details. |
|  | Some connections to the device are down.                                                                                                                                                                                          |




**Table 6: Link State Icons**

| Icon                                                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | Link is down.                                                                                                                                                                                                                                                                                                                                                                                                                     |
|  | Link is up and traffic is passing through it.                                                                                                                                                                                                                                                                                                                                                                                     |
|  | Link is degraded.<br>If some (but not all links) in an aggregated link are down, the aggregated link shows a degraded icon. The link will also show as degraded if only one direction of an L2 or L3 link was discovered instead of both directions. Click the degraded icon to see exactly which link or interface is down.<br>If <i>all</i> links in an aggregated link are down, the connectivity link shows a link down icon. |

**Table 7: Device Icons**

| Icon                                                                                | Description |
|-------------------------------------------------------------------------------------|-------------|
|  | Router      |



| Icon                                                                              | Description                                                 |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------|
|  | Router (unreachable)                                        |
|  | Device is reachable, but is undefined or of an unknown type |
|  | Unreachable device                                          |

## Configure Geographical Map Settings

The geographical map lets you position your network devices on a world map and monitor them within their geographical context. The displayed world map is imported by accessing the map vendor's site over the Internet (online mode). The look of the map will vary depending on the map vendor you choose.

By default, the client machine from where you access Optimization Engine UI is setup to get map tiles from a specific Mapbox URL over internet connection. If required, you can use a different map vendor (such as Google Maps or OpenStreetMap) by providing the appropriate URL. Both of these options require an Internet connection from your client machine.

Cisco Crosswork Optimization Engine administrator privileges are required to change these settings.

- 
- Step 1** From the main menu, choose **Admin > Visualization Settings**.
- Step 2** Click the **Map** tab.
- Step 3** From the **Map Provider** drop-down list, choose one of the following:
- **Mapbox**—Specifies that you want to display the geographical map using the default map provider.
  - **Custom**—Identifies the map tiles source (using an Internet connection). To use a map provider other than Mapbox, you must provide the URL for map tiles access. Be sure to request the exact format of this URL from the map tiles provider.
- Step 4** If you are using a custom map provider, in the **Map Source URL** field, enter the URL for map access.
- Step 5** Click **Save**.
- Step 6** Return to the **SR Policies** page and confirm that the map is displayed correctly.
- 

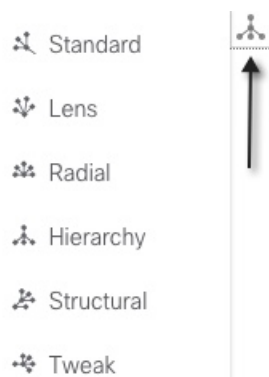
## Change the Layout of a Logical Map

When you open the logical map, it is displayed according to the default standard layout. You can change the layout, but any changes you make will not persist if you close the map. To save your layout changes, create a custom view (see [Create Custom Map Views, on page 66](#)).

- 
- Step 1** From the main menu, choose **Optimization Engine > SR Policies**.
- Step 2** In the top-right corner of the map, toggle from the geographical map view to the logical map view.

**Step 3** In the logical map, click the **System Layouts** icon in the toolbar to access the layout options.

*Figure 15: System Layouts*



**Step 4** Choose one of the predefined options to rearrange the devices and links in the map according to your preference:

- **Standard (default)**—Maintains consistent link length and distributes devices evenly. This ensures that adjacent devices are closer to each other and prevents overlap.
- **Lens**—Positions highly connected devices in the center, and moves less-connected devices out to the edges. This layout is especially useful in large networks.
- **Radial**—Arranges the devices in a circular style around the original subject. Each generation of devices becomes a new concentric ring that orbits the original parent. This layout is useful in networks where each parent has many child devices.
- **Hierarchy**—Displays devices in a family tree, where child devices are shown in horizontal layers underneath their parents.
- **Structural**—Groups devices with similar attributes together in a fan shape. This layout gives you an overview of the clusters in the network.
- **Tweak**—Adjusts the layout as the network evolves. As devices and links are added and removed, the layout adapts itself, allowing you to visualize network changes.

## Create Custom Map Views

When you rearrange the devices and links on a map, your changes are not normally saved. When you open the map later, your map settings are lost.

To easily recreate a useful map layout, you can save it as a named custom view and quickly retrieve it, without having to rearrange the map each time. This is especially useful when managing large networks with many devices.

When you save a custom view, the following settings will be saved:




- Whether it is a geographical or logical map.
- Device positions in the logical map layout.
- Whether bandwidth utilization visualization is enabled or disabled.

- Tag filters that have been applied to the map.

The map zoom level will not be saved.

Your custom map views are not user-specific. It is shared and can be modified by all users using the same Cisco Crosswork Optimization Engine server.

To create custom views:

- 
- Step 1** Choose **Optimization Engine > SR Policies** from the left navigation bar.
- Step 2** Customize the current map view until it contains only the information you want and until the layout meets your needs.
- Step 3** When you have the view the way you want it, click . The **Custom Views** pane opens.
- Step 4** From the pane's toolbar, click . The pane displays a new, blank input field under the **Name** field.
- Step 5** Enter a unique name for the new custom view. When you press Enter, the new custom view appears in the list of custom views under the **Name** field.
- Step 6** When you are finished, click  in the **Custom Views** pane to close it.
- 



#### What to do next

Retrieve, update and delete your custom views as explained in [Manage Custom Map Views, on page 67](#).

## Manage Custom Map Views

You can display, update or delete any of the custom views created using the instructions in [Create Custom Map Views, on page 66](#). This includes custom views created by other Cisco Crosswork Network Automation users.



To manage custom views:

- 
- Step 1** Open the topology map by choosing **Optimization Engine > SR Policies** from the left navigation bar.
- Step 2** Click . The **Custom Views** pane displays a list of existing custom views under the **Name** field.
- Step 3** To display a custom view, find the view you want in the list and then click the selection button next to the view's name in the list. Cisco Crosswork Optimization Engine displays the custom view.
- Step 4** To find a custom view in the list:
- a) Click in the **Name** field above the list.
  - b) Enter text matching the name of the view you want. The **Name** field includes a type-ahead feature: As you type, it will restrict the list of views to those with names that contain all or part of the text you enter. A filter icon indicates that the list is now filtered.
  - c) To use Boolean operators instead of the default "Contains" text match: Click the dropdown menu icon at the right of the **Name** field label and then select the operator you want (for example: "Not Contains" or "Equals").
  - d) To sort the list in ascending or descending alphanumerical order, click the arrow icon next to the **Name** field label.
  - e) To clear the filter, delete your search text.
- Step 5** To update a custom view:
- a) Click  to display the list of custom views.
  - b) Find the view you want in the list and then click the selection button next to the view's name in the list.

- c) Customize the view as needed.
- d) With the list of custom views still displayed, click . Your changes overwrite the previous state of the custom view.

**Step 6**

To delete a custom view:

- a) Click  to display the list of custom views.
  - b) Find the view you want in the list and then click the selection button next to the view's name in the list.
  - c) Click .
  - d) Click the **Delete** button to confirm that you want to delete the custom view.
- 

## Visualize Devices

Cisco Crosswork Optimization Engine displays discovered devices in your network and gives you the ability to access the device via SSH or Telnet. To view link state icons, see [Device and Link Icons, on page 64](#). This section contains the following topics:

- [Get More Information About Devices on the Map, on page 68](#)
- [Access the Device Console, on page 69](#)
- [Identify the Members of a Cluster, on page 70](#)

## Get More Information About Devices on the Map

In the topology map, hover over a device icon to open a popup window with the most important device details: hostname, reachability state, IP address, and type. Click on the device icon to open the **Device Details** pop-up window, where you can view more detailed information about the device and its associated links. The following example shows both details windows.

Click on the device icon to open the **Device Details** pop-up window where you can view more detailed information about the device and its associated links, as in the following example:

Figure 16: Device Details Popups

The screenshot shows the Network Topology interface. On the left, a map displays several network devices. A popup window for device 'cw-ncs-r3' is visible, showing the following details:

- Host Name: cw-ncs-r3
- State: Reachable
- Node IP: 25.1.1.12
- Type: NCS-5500

On the right, the 'Device Details' window is open, showing the following information:

- Summary**
  - Host Name: cw-ncs-r3
  - State:  Reachable
  - Operational State: OK
  - Node IP: 25.1.1.12
  - Civic Address: Newyork, Newyork, United States, North America, 10001
  - Geo Location: Longitude: -73.960745, Latitude: 40.789556
  - Type: NCS-5500
- Connect To Device**
  - Telnet IPv4
  - SSH IPv4
- Last Update**: 2019-Mar-24, 17:30:53 (GMT +02:00)
- Routing**
  - TE router ID: 10.8.8.12
  - ASN: 0

In the **Device Details** window, click on the **Links** tab to see a list of all of the device's links to other devices, as in the following example (see [Get More Information About Links](#), on page 71):

Figure 17: Links Tab of Device Details Window

The screenshot shows the 'Links' tab of the Device Details window. It displays a table titled 'Links on Device' with the following data:



| State                               | Link Type    | A Side Interface       | Z Side Interface       | A Side Utilization       | Z Side Utilization     |
|-------------------------------------|--------------|------------------------|------------------------|--------------------------|------------------------|
| <input checked="" type="checkbox"/> | L3 ISIS IPV4 | GigabitEthernet0/0/0/0 | GigabitEthernet0/0/0/4 | 2.5% (25.26Mbps/1Gbps)   | 35% (350.29Mbps/1Gbps) |
| <input checked="" type="checkbox"/> | L3 ISIS IPV4 | GigabitEthernet0/0/0/1 | GigabitEthernet0/0/0/3 | 63.4% (634.25Mbps/1Gbps) | 37% (370.3Mbps/1Gbps)  |

## Access the Device Console

After drilling down to a device's details from the topology map, you can access the device's CLI command console from the **Device Details** window (see [Get More Information About Devices on the Map](#), on page 68).

### Before you begin

- Depending on your environment, your local machine may not have direct access to your network devices (for example: you cannot ping the device's management address directly from the command line on your local machine). If this is the case, you may need to configure a tunnel. Contact Cisco Services for assistance with this more advanced configuration.
- Be sure you have installed on your client an application that can connect to devices via Secure Shell (SSH) or Telnet.



- 
- Step 1** From the main menu, choose **Optimization Engine > SR Policies**.
- Step 2** In the topology map, click on the icon representing the device to which you want to connect. The **Device Details** window displays its **Details** tab, with the device hostname, reachability state, IP address, and other details.
- Step 3** In the **Connect to Device** field, click the relevant link to connect to the device console via Telnet , or via SSH .
- If you have already defined a default connectivity application that you want to launch, Cisco Crosswork Optimization Engine launches your selected application and attempts to connect to the device. Log into the device and enter the commands you want.
- If you have not defined a default application to launch, your browser will prompt you to select one. Your choices and how they are presented will be appropriate for your client operating system, the applications you have installed, and the connectivity protocol you choose. Select the application you want and, for convenience, make sure that you select the check box indicating that this is your default choice before continuing.
- 

## Identify the Members of a Cluster

When there are multiple devices that are too close to be shown individually at the current Zoom level, they are combined together and shown as a single cluster. The cluster is represented on the geographical map by a circle with a number in its center, indicating the number of devices in the cluster.

Zoom in on a cluster to see the individual devices in the cluster displayed on the map.

If cluster members are very close to each other or in the same location, zooming in will not show the individual devices. In this case, follow these steps to see the individual members of the cluster:

- 
- Step 1** In the geographical map, click . The map zooms in on the cluster area.
- Step 2** Click  again. If you are at the maximum zoom level, the geographical map toggles to the logical map and displays the individual devices in the cluster. When you close the view, you will be switched back to the geographical map.
-

## Visualize Links

Cisco Crosswork Optimization Engine displays the links between devices and gives you the ability to configure and view bandwidth utilization on these links. To view link state icons, see [Device and Link Icons, on page 64](#). This section contains the following topics:

- [Get More Information About Links, on page 71](#)
- [Show Bandwidth Utilization for Links on the Map, on page 73](#)
- [Define Color Thresholds for Link Bandwidth Utilization, on page 73](#)

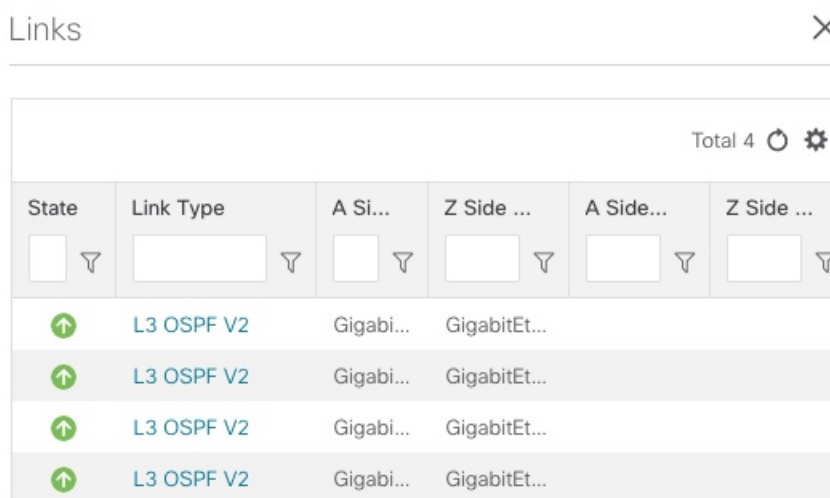
## Get More Information About Links

You can drill down in the topology map to view detailed information about links, using either of these methods:

- Click on an aggregated link (symbolized by a dashed line) to show the individual links in the side panel.
- Click on a single link (solid line) to show the **Link Details** page.

The **Links** page provides information about the configuration and status of all of a device's links, including each link's type, interfaces, and utilization (you can get the same information from the **Links** tab on the **Device Details** window; see [Get More Information About Devices on the Map, on page 68](#)). The **Links** window lists all the underlying links in the aggregation, as in the following example:


**Figure 18: Links Window**



The screenshot shows a window titled "Links" with a close button (X) in the top right corner. Below the title bar, there is a "Total 4" indicator with a refresh and settings icon. The main content is a table with the following columns: State, Link Type, A Si..., Z Side ..., A Side..., and Z Side ... Each column has a filter icon (funnel) to its right. The table contains four rows, all with a green up arrow in the State column and "L3 OSPF V2" in the Link Type column. The interface elements for the first row are as follows:

| State | Link Type  | A Si...   | Z Side ...   | A Side... | Z Side ... |
|-------|------------|-----------|--------------|-----------|------------|
| ↑     | L3 OSPF V2 | Gigabi... | GigabitEt... |           |            |
| ↑     | L3 OSPF V2 | Gigabi... | GigabitEt... |           |            |
| ↑     | L3 OSPF V2 | Gigabi... | GigabitEt... |           |            |
| ↑     | L3 OSPF V2 | Gigabi... | GigabitEt... |           |            |

Use the expand and collapse icons (< and >) to the left of the **Links** title to expand the window to the entire screen, or collapse the window back to its normal size.

Click  to choose the columns to make visible in the **Links** window's table:

- **State**—Displays each link's state: up, down, degraded, and so on (see [Device and Link Icons, on page 64](#)).

- **Link Type**—Displays the type of link. Click on the link type to open the **Link Details** window for the specific link.
- **A Side Device**—Displays the originating device for the link.
- **Z Side Device**—Displays the destination device for the link.
- **A Side Interface**—Displays the originating interface for the link.
- **Z Side Interface**—Displays the destination interface for the link.
- **A Side Utilization**—Displays the percentage of bandwidth consumption on the originating side of the link.
- **Z Side Utilization**—Displays the percentage of bandwidth consumption on the destination side of the link.

You can also use sorts and filters in the **Links** window to focus the table on only the links in which you are interested (see [Set, Sort and Filter Table Data, on page 6](#)).

The **Link Details** window provides information about the configuration and status of a single link, including link type, the link's interfaces, associated adjacent segment IDs, and so on.

**Figure 19: Link Details Window**

Link Details
✕

---

**Summary**

**Name** GigabitEthernet0/0/0/0-GigabitEthernet0/0/0/0

**State** ↑ Up

**Link Type** L3 ISIS IPV4

**ISIS Level** 2

**Last Update** 2019-Jul-14, 15:51:00 (GMT -07:00)

|                    | A Side                 | Z Side                    |
|--------------------|------------------------|---------------------------|
| <b>Node</b>        | P2                     | P1                        |
| <b>Interface</b>   | GigabitEthernet0/0/0/0 | GigabitEthernet0/0/0/0    |
| <b>Adj SID</b>     | 24001 Unprotected      | 24003 Unprotected         |
| <b>Utilization</b> | 0% (1.45Kbps/500Mbps)  | 19.2% (96.24Mbps/500Mb... |
| <b>IGP</b>         | 1                      | 1                         |
| <b>TE</b>          | 1                      | 1                         |
| <b>Delay</b>       | 1                      | 1                         |
| <b>Node IP</b>     | 10.0. [redacted]       | 10.0. [redacted]          |
| <b>Admin Group</b> | 0                      | 34816                     |



## Show Bandwidth Utilization for Links on the Map

In the geographical map and in the logical map, you can enable visualization of the bandwidth utilization for links over which circuits are provisioned. When bandwidth utilization visualization is enabled, links in the map are colored based on the percentage of total bandwidth currently utilized on the link. The utilization value is a percentage calculated by dividing link traffic by link capacity.


In this way, you can easily identify when a link is over-utilized or approaching over-utilization. Bandwidth visualization is enabled by default. The color of the link indicates the percentage of total bandwidth being used by provisioned circuits on the link:

- Green—0–25% usage
- Yellow—25–50% usage
- Orange—50–75% usage
- Red—75–100% usage

You can adjust the thresholds for each color as needed (see [Define Color Thresholds for Link Bandwidth Utilization, on page 73](#)). When visualization is disabled, the links are shown only in blue.

Please note that link bandwidth utilization data can be collected and displayed only if the linked devices are added to and managed in the device inventory.

To enable or disable visualization of bandwidth utilization:

- 
- Step 1** From the main menu, choose **Optimization Engine > SR Policies**.
- Step 2** In the top-right corner of the map, click , which toggles the display of bandwidth utilization. When usage visualization is enabled, the links are shown in green, yellow, orange, or red, depending on their utilization. If you see only blue links, usage visualization is disabled. This option is selected by default. If you uncheck this option, navigate away from the map, and later return to the map; it will revert to the default option.
- 

## Define Color Thresholds for Link Bandwidth Utilization

Cisco Crosswork Optimization Engine comes with a default set of BW Utilization color indicators and % range assignments. You can customize these to meet your needs with the following notes and limitations:

- You can enter values in the "To" ranges. Each row begins automatically from the end of the previous row's range.
- 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 the first row is 0-25%, the second row's range must end with a value greater than 25.
- You cannot use the same color for multiple thresholds. For example, you cannot choose **Green** for both the first and second rows.

Cisco Crosswork Optimization Engine administrator privileges are required to change these settings.

- 
- Step 1** From the main menu, choose **Admin > Visualization Settings**.

- Step 2** Click the **Bandwidth Utilization** tab.
- Step 3** In the **Polling Frequency** field, enter a whole number from 5 to 60. By default, Cisco Crosswork Optimization Engine polls link bandwidth every 5 minutes.
- Step 4** 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% usage
  - Yellow—25–50% usage
  - Orange—50–75% usage
  - Red—75–100% usage
- Step 5** Click **Save**.
-



## CHAPTER 5

# Visualize and Manage SR Policies

---

Cisco Crosswork Optimization Engine visualization provides the most value by giving you the ability to easily view and manage SR policies. By visually examining your network, the complexity of provisioning and managing SR policies is significantly reduced.

This section contains the following topics:

- [SR Policies Topology Map, on page 75](#)
- [SR Policies Table, on page 77](#)
- [SR Policy Configuration Sources, on page 79](#)
- [Visualize SR Policies, on page 80](#)
- [Create and Manage SR Policies, on page 87](#)

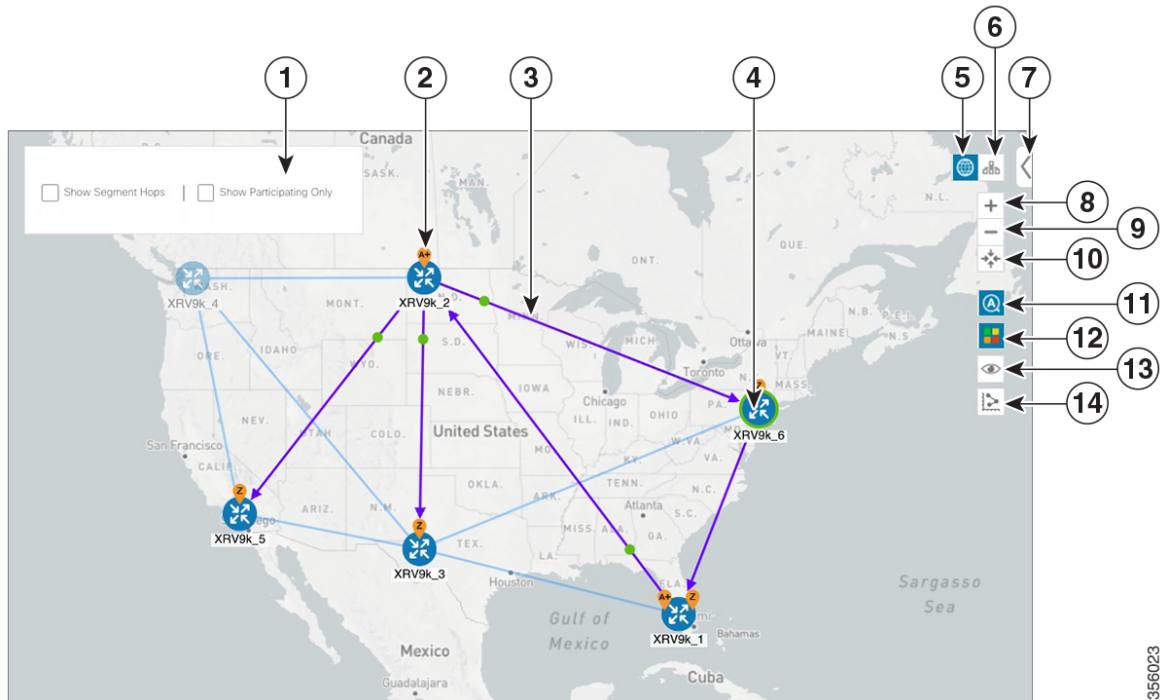
## SR Policies Topology Map

To get to the topology map, choose **Optimization Engine** from the left navigation bar, and click **SR Policies**.

For information on topology issues, or using the map to get information about devices and links, see [Network Topology Map, on page 61](#) and [Troubleshoot Network Topology Map, on page 63](#).

The following figure shows the topology map with SR policies highlighted. See the [Visualize SR Policies Example, on page 80](#) for information on how to select SR policies so that they appear on the topology map/

Figure 20: SR Policies Topology Map



356023

| Callout No. | Description                                                                                                                                                                                                                                                                                                                                               |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1           | Click the appropriate check box to enable the following options: <ul style="list-style-type: none"> <li>• <b>Show Segment Hops</b>—Displays segment hops for the selected explicit SR policies.</li> <li>• <b>Show Participating Only</b>—Displays only links that belong to selected SR policies. All other links and devices disappear.</li> </ul>      |
| 2           | <b>SR Policy Origin and Destination:</b> If both <b>A</b> and <b>Z</b> are displayed in a device cluster, at least one node in the cluster is a source and another is a destination. The <b>A+</b> denotes that there is more than one policy that originates from a node. The <b>Z+</b> denotes that the node is a destination for more than one policy. |
| 3           | <b>SR Policies:</b><br>When SR policies are selected from the <a href="#">SR Policies Table, on page 77</a> , they show as purple directional lines on the map indicating source and destination.<br><br>An adjacency segment ID (SID) is shown as a green dot on a link along the path (—●—).                                                            |
| 4           | A device or device cluster with a green outline (●) indicates there is a node SID associated with that device or a device in the cluster.                                                                                                                                                                                                                 |

| Callout No. | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5           | <p><b>Geographical Map:</b> Click this icon to view the geographical map.</p> <p>The geographical map shows single devices, device clusters, links, and SR policies, superimposed on a map of the world. Each device location on the map reflects the device's GPS coordinates (longitude and latitude) as defined in the device inventory.</p>                                                                                                                                                                                                                                                                                                                                               |
| 6           | <p><b>Logical Map:</b> Click this icon to toggle from the geographical map to the logical map. The logical map shows devices and their links, positioned according to an automatic layout algorithm, ignoring their geographical location. You can change the layout algorithm; see <a href="#">Change the Layout of a Logical Map, on page 65</a>.</p> <p>The logical map displays up to 5000 devices and never displays devices in clusters.</p> <p>If you drill down to the logical map from a geographical cluster at the maximum zoom level, the logical map shows devices that are located in the same location. See <a href="#">Identify the Members of a Cluster, on page 70</a>.</p> |
| 7           | <p><b>Expand/Collapse/Hide Side Panel:</b> Expand or collapse the side panel to see the full and truncated versions of the right-side panel. Close the side panel to get a larger view of the topology map.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 8           | <p><b>Zoom In:</b> Click this icon to zoom in on the selected area; for example, to view clustered devices on the geographical map.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 9           | <p><b>Zoom Out:</b> Click this icon to zoom out from a selection area.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 10          | <p><b>Zoom Fit:</b> Lets you automatically scale the map to fit your zoom area.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 11          | <p><b>Auto Zoom:</b> Zooms in on selected SR policies. This option is selected by default. If you uncheck this option, navigate away from the map, and later return to the map; it will revert to the default option.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 12          | <p><b>Bandwidth Utilization:</b> Lets you enable or disable visualization of the bandwidth utilization for the mapped links. See <a href="#">Show Bandwidth Utilization for Links on the Map, on page 73</a>. This option is selected by default. If you uncheck this option, navigate away from the map, and later return to the map; it will revert to the default option.</p>                                                                                                                                                                                                                                                                                                              |
| 13          | <p><b>Custom Map View:</b> Lets you create a named custom view using the settings and layout for your current map, or display a custom view you have created previously. See <a href="#">Create Custom Map Views, on page 66</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 14          | <p><b>Metrics:</b> Shows IGP, TE, or delay metrics for each link along the SR policy paths (see <a href="#">Show IGP, Delay, and Traffic Engineering Metrics, on page 86</a>).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## SR Policies Table

To get to the **SR Policies** table, choose **Optimization Engine** from the left navigation bar, and click **SR Policies**. You will see the topology map and, to the right of the map, the **SR Policies** table.

Figure 21: SR Policies Table

|                          | Headend | Endpoint | Color | Path Name    | Admin Status | Oper Status | Binding SID | Utilization (Mbps) | Disjoint Group | Last Update                        | Actions                 |
|--------------------------|---------|----------|-------|--------------|--------------|-------------|-------------|--------------------|----------------|------------------------------------|-------------------------|
| <input type="checkbox"/> | PE2     | PE1      | 102   | 102          |              |             | 24011       | 0                  |                | 2019-Jul-12, 22:37:20 (GMT -07:00) | <a href="#">Details</a> |
| <input type="checkbox"/> | PE2     | PE4      | 103   | 103          |              |             | 24013       | 0                  |                | 2019-Jul-12, 22:37:20 (GMT -07:00) | <a href="#">Details</a> |
| <input type="checkbox"/> | PE4     | PE1      | 6600  | bwopt_to_PE1 |              |             | 24011       | 24.55              |                | 2019-Jul-12, 00:16:02 (GMT -07:00) | <a href="#">Details</a> |
| <input type="checkbox"/> | PE3     | PE1      | 6600  | bwopt_to_PE1 |              |             | 24008       | 714.33             |                | 2019-Jul-12, 16:16:12 (GMT -07:00) | <a href="#">Details</a> |
| <input type="checkbox"/> | PE4     | PE2      | 6600  | bwopt_to_PE2 |              |             | 24007       | 587.158            |                | 2019-Jul-12, 00:23:54 (GMT -07:00) | <a href="#">Details</a> |
| <input type="checkbox"/> | PE2     | PE4      | 6600  | bwopt_to_PE4 |              |             | 24007       | 498.643            |                | 2019-Jul-12, 22:38:54 (GMT -07:00) | <a href="#">Details</a> |
| <input type="checkbox"/> | PE1     | PE4      | 105   | u-pe1-pe4    |              |             | 24012       | 0                  |                | 2019-Jul-14, 11:16:36 (GMT -07:00) | <a href="#">Details</a> |
| <input type="checkbox"/> | PE3     | PE2      | 106   | u-pe3-pe2    |              |             | 24011       | 24.701             |                | 2019-Jul-12, 15:50:27 (GMT -07:00) | <a href="#">Details</a> |
| <input type="checkbox"/> | PE4     | PE1      | 104   | u-pe4-pe1    |              |             | 24014       | 0                  |                | 2019-Jul-12, 11:30:28 (GMT -07:00) | <a href="#">Details</a> |

The **SR Policies** table provides the following functions:

- Displays a list of all SR Policies discovered from the network.
- Configure new SR policies.
- Edit SR policies created using Crosswork Optimization Engine (click on **Details** link).



**Note** Only SR policies created from Crosswork Optimization Engine can be modified or deleted on the Crosswork Optimization Engine UI.

- Highlight SR policies on the map when selected from the table.
- View SR policy details (click on **Details** link). See [Get More Information About an SR Policy, on page 98](#).
- Refresh (🔄) the table or policy details (if in the **SR Policy Details** table). You can also view the date and time as to when the last refresh occurred.



**Note** When creating or modifying SR policies, the refresh and auto-refresh functions are disabled in the tables.

The following information is available in the **SR Policies** table:



**Note** Some fields may be blank depending on the SR policy type.

Table 8:

| Column Heading | Description                          |
|----------------|--------------------------------------|
| Headend        | Where the SR policy is instantiated. |
| Endpoint       | The destination of the SR policy.    |

| Column Heading | Description                                                                                                                                                                                                                                                                  |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Color          | A numerical value that distinguishes between two or more policies to the same node pairs (Headend – Endpoint). Every SR policy between a given headed and endpoint must have a unique color.                                                                                 |
| Path Name      | Name of SR policy path.                                                                                                                                                                                                                                                      |
| Admin Status   | Administrative status of the SR policy. This is the status defined by the user.                                                                                                                                                                                              |
| Oper Status    | Operational status of the SR policy. This is the state of the policy as reported by the system. For example, the user can define the Admin status as Up. However, if the policy is operationally down due to some network issues, then the Oper Status will display as Down. |
| Binding SID    | The binding segment is a local segment identifying an SR policy. Each SR policy is associated with a binding segment ID (BSID).                                                                                                                                              |
| Utilization    | Percentage of total bandwidth being used.                                                                                                                                                                                                                                    |
| Disjoint Group | If applicable, the disjoint group the SR policy belongs in.                                                                                                                                                                                                                  |
| Last Update    | Time when the most recent update for the policy was received from the network.                                                                                                                                                                                               |
| Actions        | Click <b>Details</b> to <a href="#">Get More Information About an SR Policy, on page 98</a> .                                                                                                                                                                                |

## SR Policy Configuration Sources

SR Policies discovered and reported by Cisco Crosswork Optimization Engine may have been configured from the following sources:

- SR-PCE initiated—An SR policy that is configured directly on an SR-PCE device.
- PCC initiated—An SR policy that is configured directly on a device.
- Cisco Crosswork Optimization Engine PCE initiated—An SR policy that is configured using Cisco Crosswork Optimization Engine. This is the only type of SR policy that Cisco Crosswork Optimization Engine can modify or delete (see [Create and Manage SR Policies, on page 87](#)).

# Visualize SR Policies

This section describes the visualization features provided in the topology map for SR policies that have been discovered during the onboard of devices or provisioned using Cisco Crosswork Optimization Engine. To create and manage SR policies using Cisco Crosswork Optimization Engine see [Create and Manage SR Policies](#), on page 87.

This section contains the following topics:

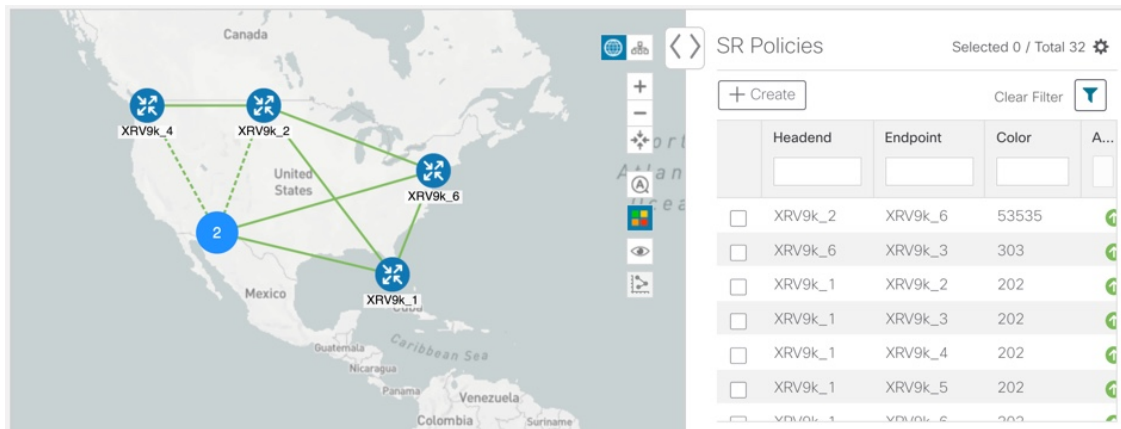
- [Visualize SR Policies Example](#), on page 80
- [Highlight an SR Policy on the Map](#), on page 86
- [Identify Segment Hops](#), on page 86
- [Show IGP, Delay, and Traffic Engineering Metrics](#), on page 86

## Visualize SR Policies Example

Follow the steps in this example to quickly familiarize yourself with a number of SR policy visualization features that are available from the topology map.

In this example, we are using the following geographical map with devices and links that have SR policies configured. SR policies are not yet highlighted in the map.

**Figure 22: Topology Map Example**



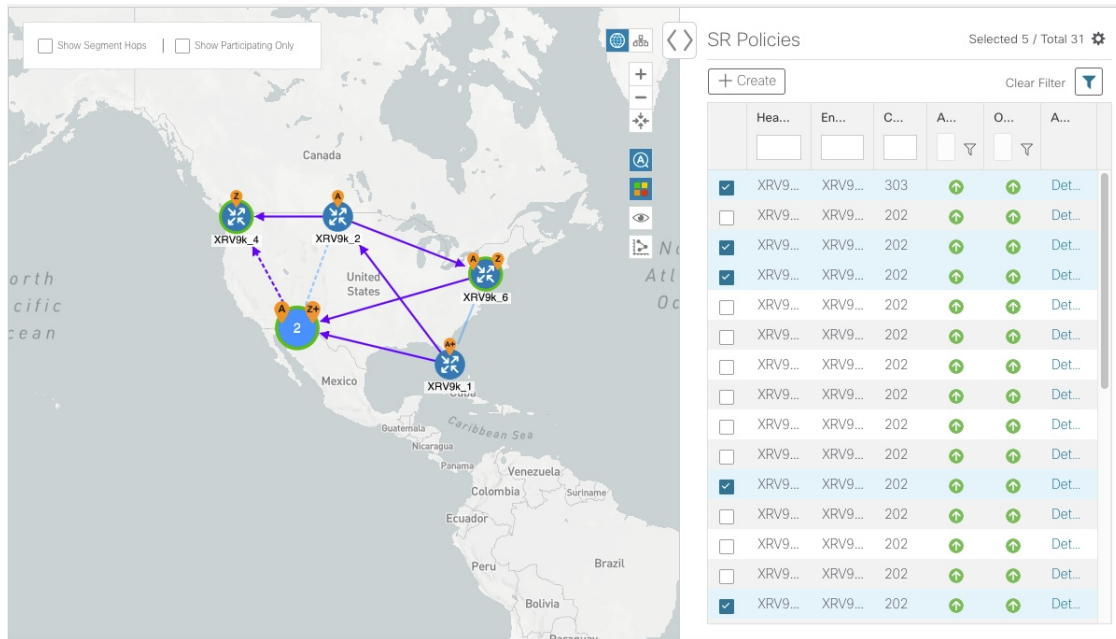
### Before you begin

In this example, we assume that devices and SR policies have already been added to Crosswork Optimization Engine (see [Get Started](#), on page 9).



- Step 1** From the **SR Policies** table, click the checkbox next to the SR policies you are interested in. In this example, there are four SR policies selected.



Figure 23: SR Policy Selection

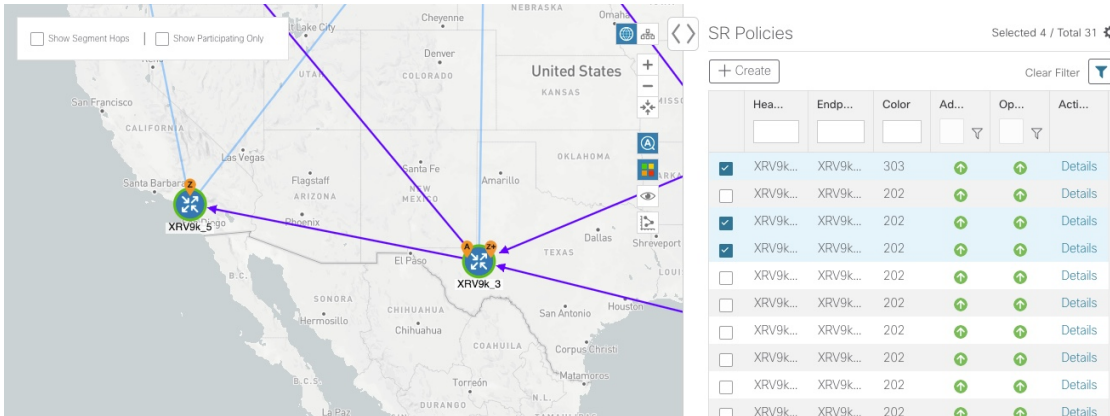


After SR selection, the map displays the following:

- SR policies appear as purple links with arrows that indicate the path direction. Dashed links represent aggregated links.
- XR9k\_1, XR9k\_2, and XR9k\_6 devices are origins for the selected policies. XR9k\_4, XR9k\_6, and devices in the device cluster are destinations for the selected policies. SR policy origin and destination are marked with **A** and **Z**, respectively. If both **A** and **Z** are displayed in a device cluster, at least one device in the cluster is a source and another is a destination. The **A+** denotes that there is more than one policy that originates from a device. The **Z+** denotes that the device is a destination for more than one policy.
-  indicates a device cluster composed of 2 devices within the same general location. This particular device cluster also has a node SID which is indicated by the green outline.
-  indicates XR9k\_4 and XR9k\_6 have node SIDs.

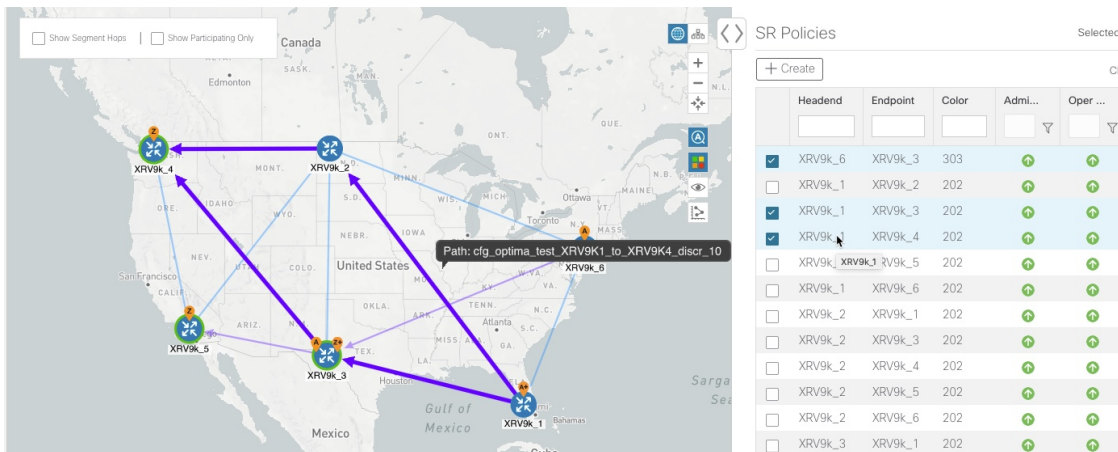
**Step 2** Click on the device cluster to zoom in and see the individual devices (XR9k\_5 and XR9k\_1).

Figure 24: Device Cluster Zoom



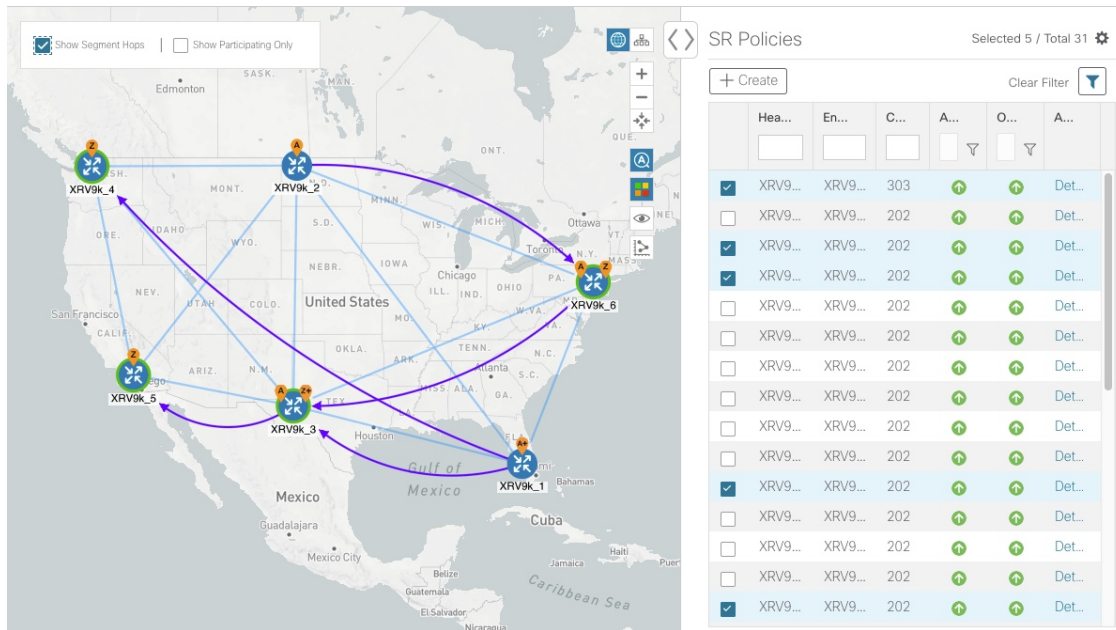
**Step 3** From the **SR Policies** table, *hover* over one of the selected policy names. When you hover on one of the selected SR policy entries, the IGP path of that policy is highlighted on the topology view. In the case of ECMP (Equal Cost Multi-Path) all paths will be highlighted as shown in the example below.

Figure 25: Hover over an SR Policy



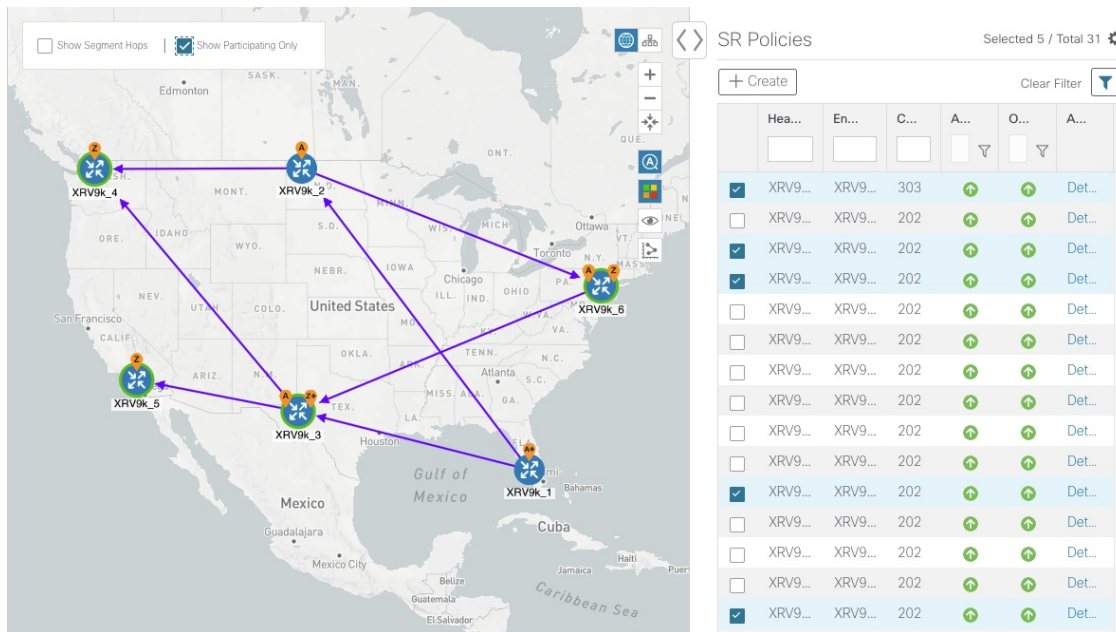
**Step 4** Check the **Show Segment Hops** check box. The segment hops for the selected SR policies are displayed, with curved arrows, instead of the IGP paths.

Figure 26: Segment Hops



**Step 5** Check the **Show Participating Only** check box. All non-participating links and devices disappear. Only participating policies are displayed.

Figure 27: Participating SR Policies




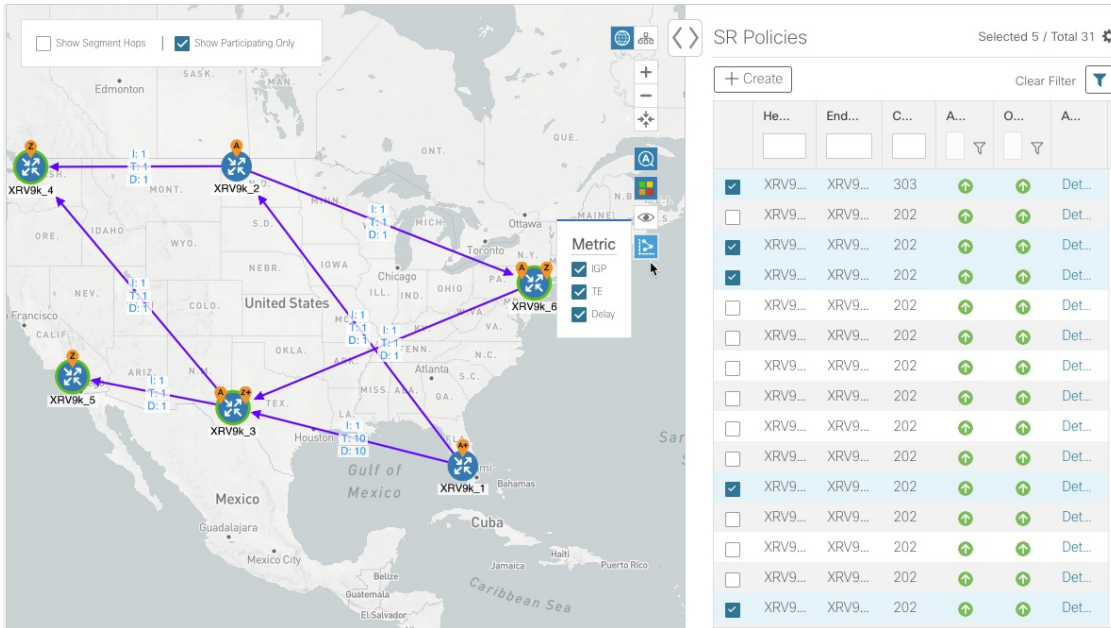
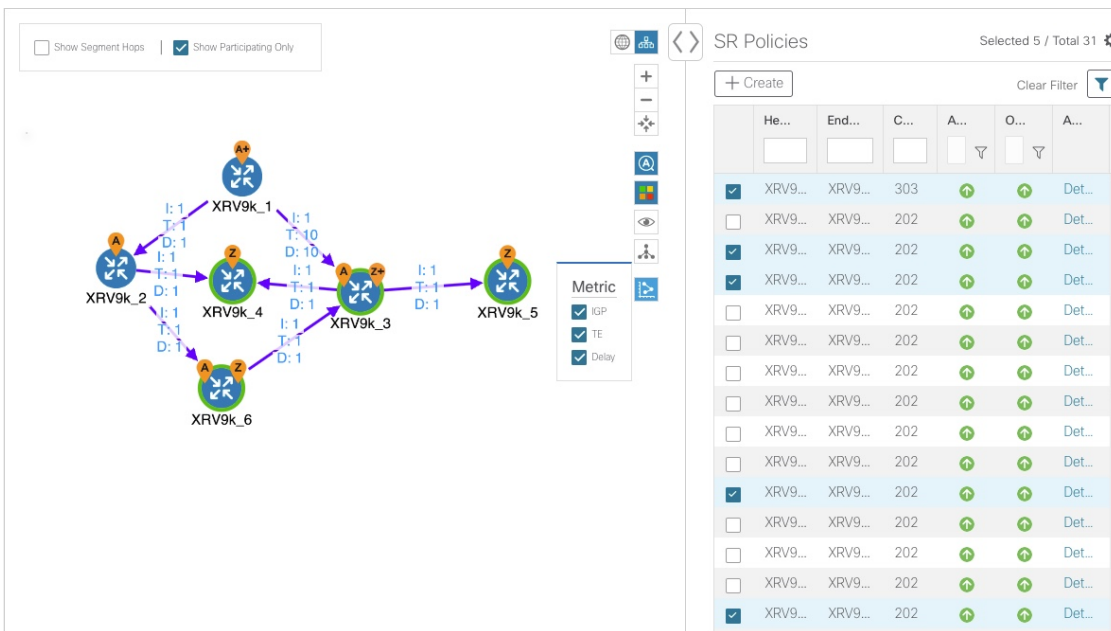
**Step 6** To view the IGP, TE or Delay metrics for each link along a policy's IGP path, select the Metric icon  and click the applicable check boxes. The metric details are displayed for each policy on the map.

Figure 28: IGP, Delay, and TE Metrics



Step 7 Click the logical map icon (🗺️).

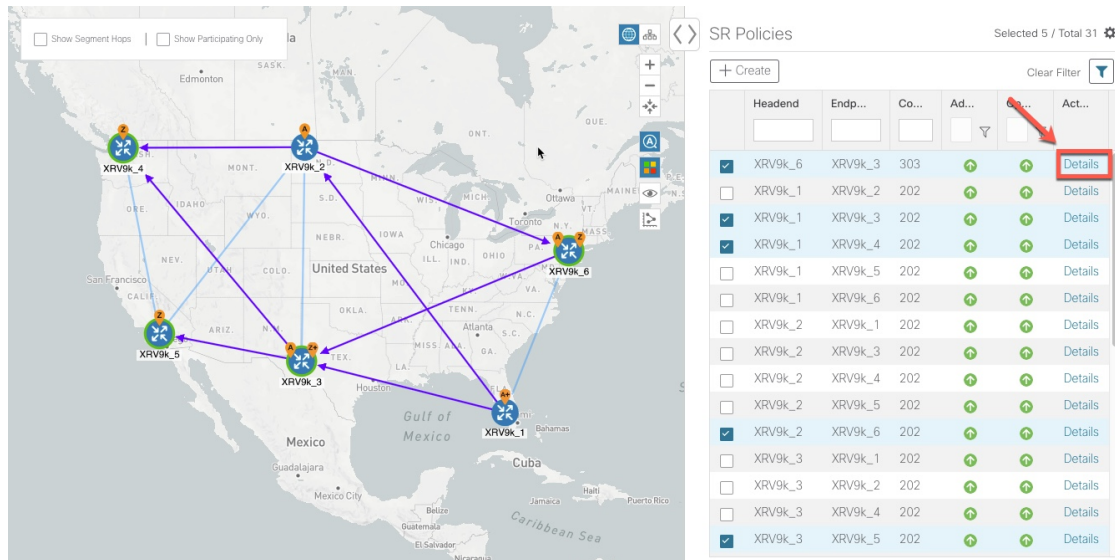
Figure 29: Logical Map



You are able to see the same information (aside from geographical location) that is available on the geographical topology map. You also have the ability to move devices and links on the map to make it easier to view.

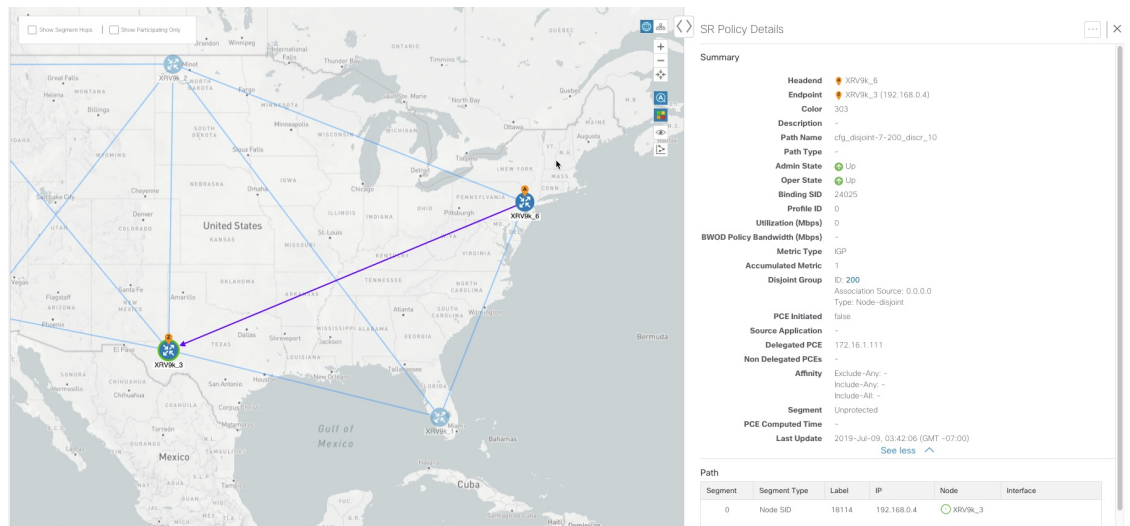
Step 8 To view SR policy details such as disjoint groups, metric type, segment hop information, and so on, click **Details...** from the table.

Figure 30: SR Policy Detail Link



The SR Policy Details page is displayed in the side panel (see [Get More Information About an SR Policy, on page 98](#)). Note that only the selected policy is now highlighted on the topology map.

Figure 31: SR Policy Details



**Note** To return to the SR Policies table, close (X) the current view.

**What to do next**

Provision and manage SR policies. See [Visualize and Manage SR Policies, on page 75](#).

## Highlight an SR Policy on the Map

When many SR policies are displayed on the map, it may be difficult to view a particular SR policy path. To highlight a particular SR policy path on the map, navigate to **Optimization Engine > SR Policies > SR Policies** table, and hover over the SR policy.

| Headend                             | Endpoint | Color   | Admi... | Oper ... |
|-------------------------------------|----------|---------|---------|----------|
| <input checked="" type="checkbox"/> | XRV9k_6  | XRV9k_3 | 303     |          |
| <input type="checkbox"/>            | XRV9k_1  | XRV9k_2 | 202     |          |
| <input checked="" type="checkbox"/> | XRV9k_1  | XRV9k_3 | 202     |          |
| <input checked="" type="checkbox"/> | XRV9k_1  | XRV9k_4 | 202     |          |
| <input type="checkbox"/>            | XRV9k_1  | XRV9k_5 | 202     |          |
| <input type="checkbox"/>            | XRV9k_1  | XRV9k_6 | 202     |          |
| <input type="checkbox"/>            | XRV9k_2  | XRV9k_1 | 202     |          |
| <input type="checkbox"/>            | XRV9k_2  | XRV9k_3 | 202     |          |
| <input type="checkbox"/>            | XRV9k_2  | XRV9k_4 | 202     |          |
| <input type="checkbox"/>            | XRV9k_2  | XRV9k_5 | 202     |          |
| <input type="checkbox"/>            | XRV9k_2  | XRV9k_6 | 202     |          |
| <input type="checkbox"/>            | XRV9k_3  | XRV9k_1 | 202     |          |

## Identify Segment Hops

To view segment hops for selected policies, do the following:

- 
- Step 1** From the **SR Policies** table, select the SR policies you are interested in.
  - Step 2** From the top left box in the topology map, check the **Show Segment Hops** check box. The segment hops for the selected SR policies are displayed, with curved arrows, instead of the IGP paths.
- 

## Show Participating Nodes and Links


To view only the nodes and links that are part of selected SR policies, do the following:

- 
- Step 1** From the **SR Policies** window, select the SR policies you are interested in.
  - Step 2** From the top left box in the topology map, check the **Show Participating Only** check box.
- 

## Show IGP, Delay, and Traffic Engineering Metrics

Each link is assigned a metric value. The distance between two nodes is the sum of all the metric values of links along a path. To view IGP, Delay, or Traffic Engineering (TE) metrics on the topology map:

- 
- Step 1** From the **SR Policies** table, check the checkboxes next to the SR policies you are interested in. The SR policies are highlighted in the topology map.

- Step 2** From the topology map, select the Metric icon  and click the applicable check boxes. The metric details are displayed for each policy on the map.

---

### What to do next

To configure a dynamic SR policy based on one of these metrics, see [Create Dynamic Path SR Policies, on page 91](#).

## Create and Manage SR Policies





This section describes how to provision and manage SR policies using the Cisco Crosswork Optimization Engine UI. The Cisco Crosswork Optimization Engine UI gives you the capability of provisioning SR policies in a variety of methods (explicit, dynamic, and bandwidth constraint driven). As you provision an SR policy, you can select nodes on the topology map and also preview the path before deployment. This greatly reduces the complexity of SR policy management. Before provisioning SR policies, you should understand some basic segment routing configuration concepts (see [Segment Routing, on page 9](#)).

## Configure Affinity Mapping

Affinity of an SR policy is used to specify the link attributes for which the policy has affinity for. It determines which links are suitable to form a path for the policy. It is a 32-bit value, with each bit position (0 - 31) representing a link attribute. Affinity mapping is used to map each bit position or attribute to a color. This makes it easier to refer to link attributes.



- Note** The affinity mapping name is only used for visualization in Cisco Crosswork Optimization Engine. Affinities defined on devices are not collected by Cisco Crosswork Optimization Engine. Define affinity mapping in Cisco Crosswork Optimization Engine with the same name and bits that are used on the device interface. Cisco Crosswork Optimization Engine will only send bit information to SR-PCE during provisioning.

- 
- Step 1** From the main menu choose **Optimization Engine** > **Affinity Mapping**. You can also define affinities while creating a policy ([Create Dynamic Path SR Policies, on page 91](#)) by clicking **Manage Mapping**.
- Step 2** To add a new affinity mapping, click **Create Mapping**.
- Enter the name (color) and the bit it will be assigned to.
  - Click  to save the mapping.
- Step 3** To edit an affinity mapping, click .
- Make the necessary changes. If you want to cancel your changes, click **X**.
  - Click  to save the changes.
- Step 4** To delete an affinity mapping, click .

**Note** You should remove the policy before removing the affinity to avoid orphan policies. If you have removed an affinity associated to an SR policy, the affinity is shown as "UNKNOWN" in the **SR Policy Details** window.

### What to do next

After defining affinities, you can [Create Dynamic Path SR Policies, on page 91](#).

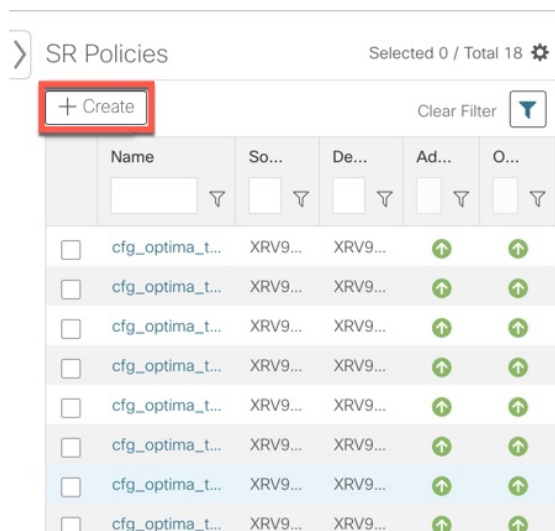
## Create Explicit Path SR Policies

This task creates an SR policy using an explicit path (segments) that you define.

**Step 1** From the main menu, choose **Optimization Engine > SR Policies**.

**Step 2** From the **SR Policies** table, click **+ Create**.

**Figure 32: Create SR Policy**



**Step 3** Enter the following SR policy values:

a) Required fields:

- **Headend**—Where the SR policy is instantiated. Note: You can either select a node (from the map or drop-down list) or enter part of the node name to filter the headend and endpoint node entries.
- **Endpoint**—The destination of the SR policy.
- **IP Address**—After the endpoint is selected, the SID list is populated and you can select the loopback IP address.
- **Color**—A numerical value that distinguishes between two or more policies to the same node pairs (Headend – Endpoint). Every SR policy between a given headed and endpoint must have a unique color. The bit value must match the value that is configured on the device.
- **Path Name**—Enter a name for this SR policy path. SR policy paths from the same headend must be unique. Policy path names are not case sensitive.




b) Optional values:

- **Description**—Enter details or a description of this policy.
- **Explicit Binding SID**—The binding segment is a local segment identifying an SR policy. Each SR policy is associated with a binding segment ID (BSID). The BSID is a local label that is automatically allocated for each SR policy when the policy is instantiated. If you wish to use a specific segment ID, rather than the default one that is automatically assigned, then enter it here.
- **Profile ID**—Identification used to associate an SR policy with a set of features applied to the policy by the headend. It should correspond with a profile configured on the headend.

**Step 4** Under Policy Path, click **Explicit Path**.

**Step 5** Add segments that are part of the SR policy path.

- a) You can either select a node from the drop-down list or enter part of the node name to filter the node list. After a node is selected, the **Select SID** drop-down list is populated with associated prefix and adjacency segment IDs.
- b) Select a segment ID from the **Select SID** drop-down list. The drop-down list contains all available segments. The segment names indicate the associated node and whether it is a prefix or an adjacency segment. The name also includes whether the segment is protected (P) or unprotected (U).
- c) Click **Add**. The segment appears in the table with segment values.
- d) Repeat for each segment you want to add to the SR policy path. To reorder the segment hops, click and drag  next to the segment hop you want to move.

**Note** The segments must be in order or the path will not be created.

Figure 33: Explicit SR Policy Example

New SR Policy \* Required Field

Policy Details

**Headend \***  
XRV9k\_4

**Endpoint \*** XRV9k\_6 **IP Address \*** 192.168

**Color \***  
108

**Description**  
SiteA Services to SiteH Collection

**Explicit Binding SID**

**Profile ID**  
4653

Policy Path

**Path Name \***  
SiteA\_SiteH\_ExpSR

Explicit Path  Dynamic Path  Bandwidth On Demand

Enter values below to add SID to the list \*

Enter node name.. Select IP Add

| Segment | Segment Type | Label | IP     |
|---------|--------------|-------|--------|
| 0       | IGP Adj SID  | 24004 | 10.0.1 |
| 1       | IGP Adj SID  | 24004 | 10.0.1 |
| 2       | IGP Adj SID  | 24001 | 10.0.1 |

Cancel Preview Provision

**Step 6** Click **Preview**. The path is highlighted on the map and policy details are displayed on the right.

Figure 34: Explicit SR Policy Example

| Segment | Segment Type | Label | IP     |
|---------|--------------|-------|--------|
| 0       | IGP Adj SID  | 24004 | 10.0.1 |
| 1       | IGP Adj SID  | 24004 | 10.0.1 |
| 2       | IGP Adj SID  | 24001 | 10.0.1 |

**Step 7** If you are satisfied with the policy path, click **Provision**.

**Step 8** When the policy is provisioned successfully, a window appears with the following options:

- **View SR Policy List**—Displays the **SR Policies** table that lists all SR policies including the one that was just created.
- **Create New**—Allows you to create another SR policy.

**Note** The newly provisioned SR policy may take some time, depending on network size and performance, to appear in the **SR Policies** table. The **SR Policies** table is refreshed every 30 seconds.

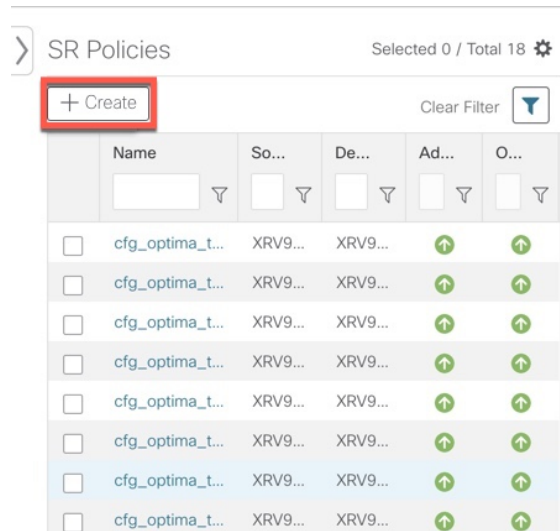
## Create Dynamic Path SR Policies

This task creates an SR policy with a dynamic path. SR-PCE computes a path for the policy based on metrics and path constraints (affinity or disjointness) defined by the user. A user can select from three available metrics to minimize in path computation: IGP, TE, or delay. SR-PCE may also automatically re-optimize the path as necessary based on topology changes.

**Step 1** From the main menu, choose **Optimization Engine > SR Policies**.

**Step 2** From the **SR Policies** table, click **+ Create**.

Figure 35: Create SR Policy

**Step 3** Enter the following SR policy values:

## a) Required fields:

- **Headend**—Where the SR policy is instantiated. Note: You can either select a node (from the map or drop-down list) or enter part of the node name to filter the headend and endpoint node entries.
- **Endpoint**—The destination of the SR policy.
- **IP Address**—After the endpoint is selected, the SID list is populated and you can select the loopback IP address.
- **Color**—A numerical value that distinguishes between two or more policies to the same node pairs (Headend – Endpoint). Every SR policy between a given headend and endpoint must have a unique color.
- **Path Name**—Enter a name for this SR policy path. SR policy paths from the same headend must be unique. Policy path names are not case sensitive.

## b) Optional values:

- **Description**—Enter details or a description of this policy.
- **Explicit Binding SID**—The binding segment is a local segment identifying an SR policy. Each SR policy is associated with a binding segment ID (BSID). The BSID is a local label that is automatically allocated for each SR policy when the policy is instantiated. If you wish to use a specific segment ID, rather than the default one that is automatically assigned, then enter it here.
- **Profile ID**—Identification used to associate an SR policy with a set of features applied to the policy by the headend. It should correspond with a profile configured on the headend.

**Step 4** Under Policy Path, click **Dynamic Path**.**Step 5** Under Optimization Objective, select one of the following:

- **Interior Gateway Protocol (IGP) Metric**—Minimizes total path IGP metric.
- **Traffic Engineering (TE) Metric**—Minimize total path TE metric.

- **Latency**—Minimize total path latency.

**Step 6** Define affinities:

**Note** Affinity constraints and disjointness cannot be configured on the same SR policy.

- **Exclude Any**—Does not traverse interfaces that have any of the specified affinities.
- **Include Any**—Includes only interfaces that have any of the specified affinities.
- **Include All**—Include only interfaces that have all of the specified affinities.
- **Select or Create Mapping**
  - If affinity mappings have been defined, select the applicable value.
  - To create an affinity mapping, click **Create Mapping**.

**Note** For more information, see [Configure Affinity Mapping, on page 87](#).

- **Add Another**—Click this link to add more affinity rules.

**Step 7** (Optional) Define disjointness. For more information on how Cisco Crosswork Optimization Engine handles disjoint policies and what options are supported, see the "Disjointness" section in [Segment Routing, on page 9](#)). Enter the disjoint group ID and subgroup ID. If there are existing SR policies belonging to a disjoint group that you define here, all SR policies that belong to that same disjoint group are shown during Preview.

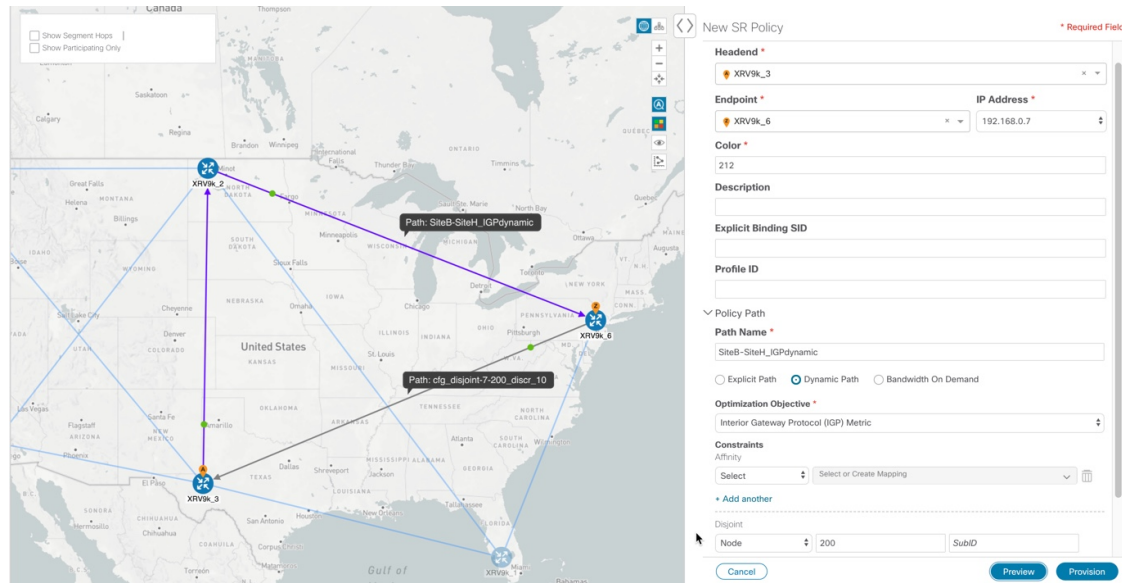
**Note** There cannot be more than two SR policies in the same disjoint group or subgroup.

**Step 8** Under Segments, select one of the following:

- **Protected (Preference)**—Creates an SR policy that will use protected segments (provides a backup path) when available.
- **Unprotected Only**—Creates an SR policy that will only use unprotected segments. This option cannot be used when affinity constraints are defined.

**Step 9** Click **Preview**. The path is highlighted on the map. Note in the following example that all policies belonging to the same disjoint group are displayed.

Figure 36: Dynamic SR Policy and Disjoint Group Policy Preview



**Step 10** If you are satisfied with the policy path, click **Provision**.

**Step 11** When the policy is provisioned successfully, a window appears with the following options:

- **View SR Policy List**—Displays the **SR Policies** table that lists all SR policies including the one that was just created.
- **Create New**—Allows you to create another SR policy.

See the following topics:

- [Configure Affinity Mapping, on page 87](#)
- [Preview Disjoint Policies, on page 94](#)
- [View SR Policies Belonging to a Disjoint Group, on page 97](#)

## Preview Disjoint Policies

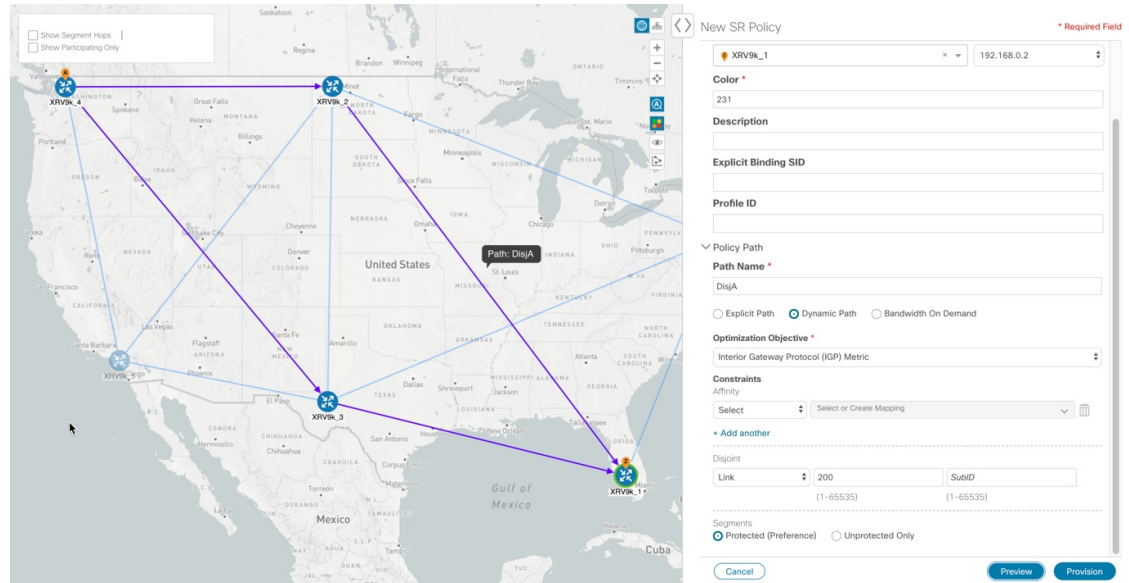
The following example shows how the SR policy provisioning preview feature can be used for disjoint SR policies. Two SR policies will be provisioned with link disjointness. After the first one is provisioned, the preview of the second will show both policies in the map view and how the path of the first would be re-optimized by SR-PCE to make them link disjoint from each other.



**Note** There cannot be more than 2 disjoint policies in the same disjoint group or subgroup

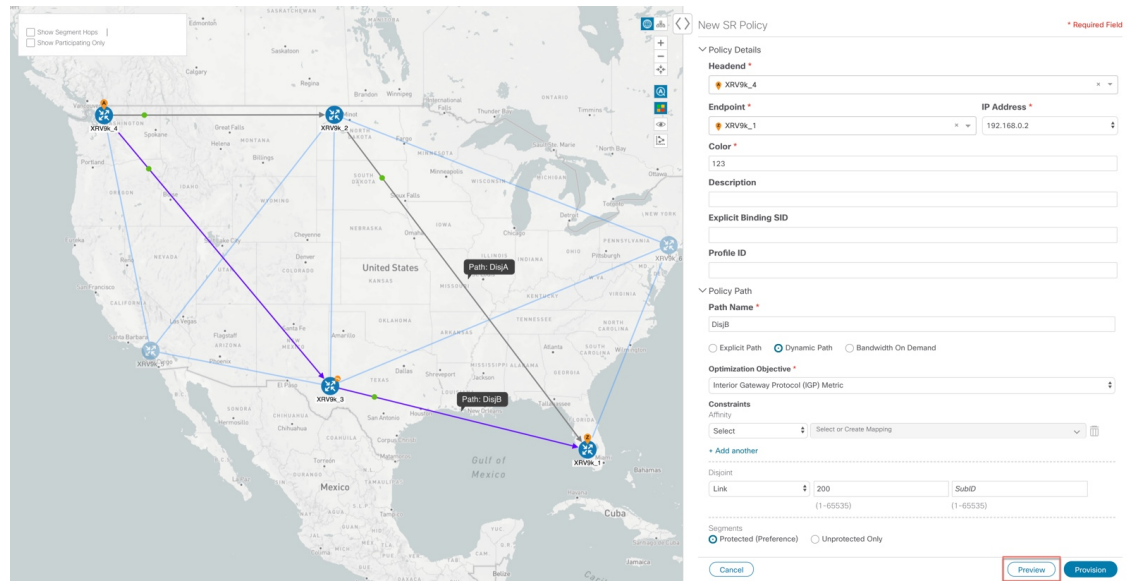
Below is a provisioned dynamic policy (DisjA) belonging to disjoint link group 200. The SR policy has a path that ECMP splits between XRV9k\_4 and XRV9k\_1 as shown in the following figure.

Figure 37: Example: DisjA SR Policy



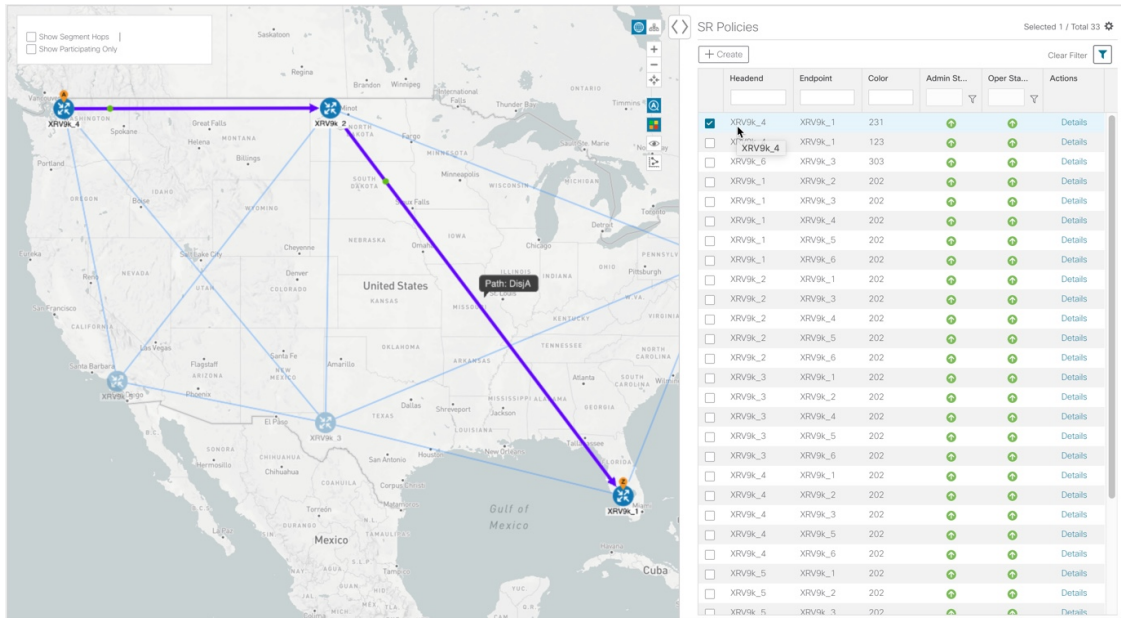
A second policy (DisjB) is now configured in the same disjoint group as the first. When we preview this policy you see both DisjA and DisjB are displayed. You also see the path of DisjA has been reoptimized to ensure both policies are link disjoint. This path change to the existing policy DisjA will be made by SR-PCF if DisjB is provisioned.

Figure 38: Example: Preview Disjoint SR Policies



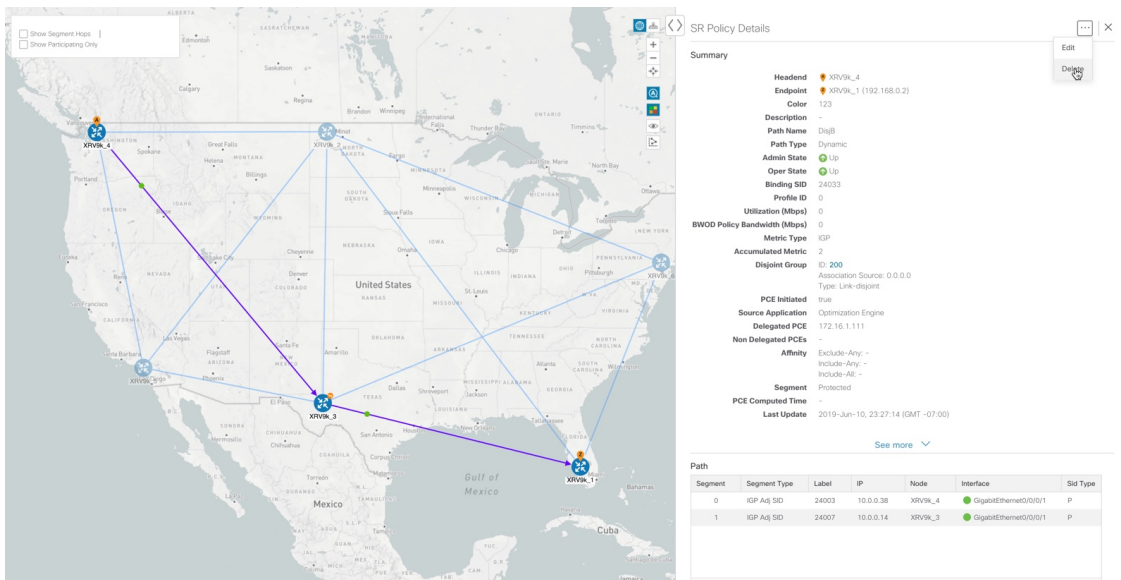
After DisjB is provisioned, we select **View SR Policy List** and check the checkbox next to the DisjA policy to confirm that the path for DisjA has been rerouted.

Figure 39: Example: DisjA SR Policy Rerouted



From the SR Policies table, check the checkbox next to DisjB, and delete it.

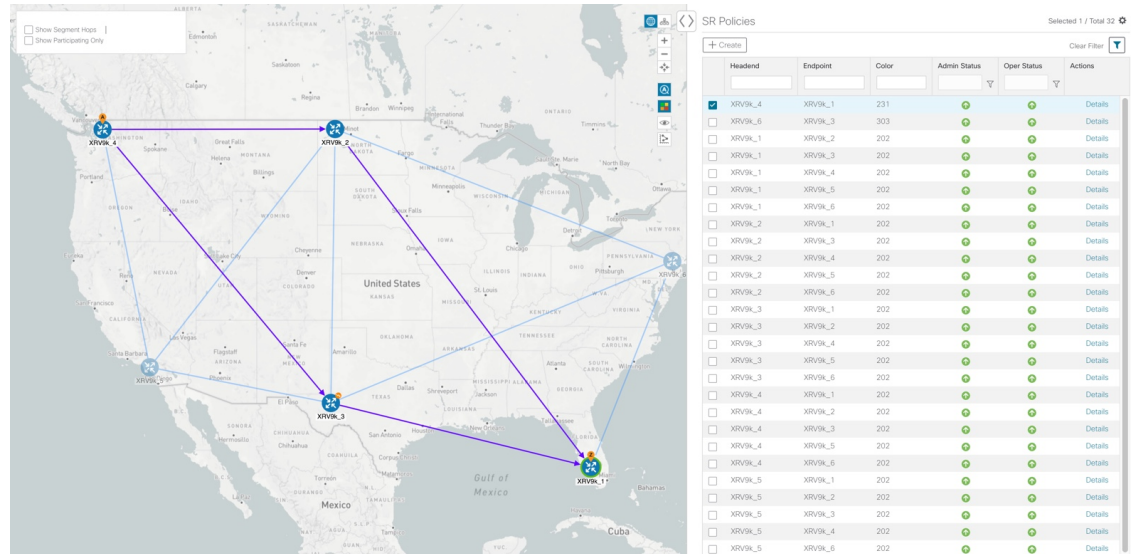
Figure 40: Example: Delete DisjB SR Policy



After a few seconds, display DisjA again. You will see that it has reset itself and shows two paths from XR.



Figure 41: Example: DisjA SR Policy Reset



## View SR Policies Belonging to a Disjoint Group

From the **SR Policy Details** window, click the **Disjoint Group** ID number to view all SR policies that use that disjoint group.

Figure 42: Disjoint Group

Disjoint Group 500 (View All)

SR Policies Selected 0 / Total 3

| Headend | Endpoint | Color | Path Name           | Admin Status | Oper Status | Binding SID | Last Update                       | Utilization... | Disjoint Group | Actions |
|---------|----------|-------|---------------------|--------------|-------------|-------------|-----------------------------------|----------------|----------------|---------|
| XRV9k_1 | XRV9k_5  | 456   | FinSite2_Site5_I... | 🟢            | 🟢           | 24007       | 2019-May-28, 14:00:57 (GMT-07:... | 0              | 500            | Details |
| XRV9k_4 | XRV9k_1  | 423   | FinSite2_Site7_I... | 🟢            | 🟢           | 24011       | 2019-May-28, 13:51:48 (GMT-07:... | 0              | 500            | Details |
| XRV9k_2 | XRV9k_6  | 213   | FinSite4_Site8_I... | 🟢            | 🟢           | 24011       | 2019-May-28, 13:53:13 (GMT-07:... | 0              | 500            | Details |

To go back to the **SR Policy Details** window, click

## Modify SR Policies

To modify an SR policy:

- Step 1** From the main menu, choose **Optimization Engine > SR Policies**.
- Step 2** Expand the **SR Policies** table. You will see a list of SR policies and various information such as source, destination, Admin status, operating status, and so on.
- Step 3** Locate the SR policy you are interested in and click the **Details...** link (under the **Actions** column). You may need to expand the SR Policies table to view the **Actions** column.
- Step 4** From the top-right corner of the **SR Policy Details** window, click

**Note** If the icon is grayed out, the policy cannot be modified for one of the following reasons:

- The policy was not created using the Crosswork Optimization Engine (**SR Policies** table > **Create**).
- The policy was created using the Bandwidth Optimization function pack.

**Step 5** Click **Edit**.

**Step 6** In the **Policy Path** area, modify the values you want to change.

**Step 7** (Optional) Click **Preview** to view visible updates on the topology map.

**Step 8** Click **Update**.

**Step 9** When the policy is updated successfully, a window appears with the following options:

- **View SR Policy List**—Displays the **SR Policies** table that lists all SR policies including the one that was just updated.
- **Create New**—Allows you to create a new SR policy.

---

## Get More Information About an SR Policy

From the **SR Policies** table, locate the SR policy you are interested in and click the **Details...** link (under the **Actions** column). You may need to expand the **SR Policies** table to view the **Actions** column. The SR Policy Details window appears, where you can view more detailed information about the policy and its associated paths. See the following table for field descriptions.

Figure 43: SR Policy Details

SR Policy Details
⋮ ×

---

Summary

- Headend** 📍 XRV9k\_4
- Endpoint** 📍 XRV9k\_6 (192.168.0.7)
- Color** 108
- Description** SiteA Services to SiteH Collection
- Path Name** SiteA\_SiteH\_ExpSR
- Path Type** Explicit
- Admin State** 🟢 Up
- Oper State** 🟢 Up
- Binding SID** 24011
- Profile ID** 4653
- Utilization (Mbps)** 0
- BWOD Policy Bandwidth (Mbps)** 0
- Metric Type** TE
- Accumulated Metric** 0
- Disjoint Group** ID: -  
Association Source: -  
Type: -
- PCE Initiated** true
- Source Application** Optimization Engine
- Delegated PCE** 172.16.1.
- Non Delegated PCEs** -
- Affinity** Exclude-Any: -  
Include-Any: -  
Include-All: -
- Segment** Protected
- PCE Computed Time** -
- Last Update** 2019-Jun-09, 14:43:19 (GMT -07:00)

[See less](#) ^

---

Path

| Segment | Segment Type | Label | IP    | Node    | Interface                                                   | Sid Type |
|---------|--------------|-------|-------|---------|-------------------------------------------------------------|----------|
| 0       | IGP Adj SID  | 24004 | 10.0. | XRV9k_4 | <span style="color: green;">●</span> GigabitEthernet0/0/0/2 | U        |
| 1       | IGP Adj SID  | 24004 | 10.0. | XRV9k_5 | <span style="color: green;">●</span> GigabitEthernet0/0/0/0 | U        |

Table 9: SR Policy Details Fields

| Field              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Headend</b>     | Where the SR policy is instantiated (source).                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Endpoint</b>    | The destination of the SR policy.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Color</b>       | A numerical value that distinguishes between two or more policies to the same node pairs (Headend – Endpoint). Every SR policy between a given headed and endpoint must have a unique color.                                                                                                                                                                                                                                                        |
| <b>Description</b> | (Optional) If provisioned using the Cisco Crosswork Optimization Engine UI, it is the description entered by the user. This may be blank if the user did not enter a description.                                                                                                                                                                                                                                                                   |
| <b>Path Name</b>   | The name of the current active candidate path of the SR policy. For SR policies created using the Cisco Crosswork Optimization Engine UI, it will be the name provided by the user during configuration. For SR policies created through configuration on the headend router, the Path Name will be the base name configured for the policy on the CLI with "cfg_" appended to the beginning and the candidate path preference appended to the end. |

| Field                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Path Type</b>                    | Indicates whether an SR policy created through Cisco Crosswork Optimization Engine is explicit or dynamic.                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Admin State</b>                  | Administrative state is dictated by the user.<br>For example, the user creates an SR policy and does not intentionally shut it down. The Admin State will be UP.                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Oper State</b>                   | Operational state received by the system.<br>For example, the user has configured a policy and so the Admin State is UP. However, due to network issues it is operationally down. In this case, Oper State will display DOWN and Admin State will remain as UP.                                                                                                                                                                                                                                                                                            |
| <b>Binding SID</b>                  | The binding segment is a local segment identifying an SR policy. Each SR policy is associated with a binding segment ID (BSID). The BSID is a local label that is automatically allocated (or explicitly entered during manual provisioning) for each SR policy when the policy is instantiated.                                                                                                                                                                                                                                                           |
| <b>Profile ID</b>                   | Identification used to associate an SR policy with a set of features applied to the policy by the headend. It should correspond with a profile configured on the headend.                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Utilization (Mbps)</b>           | The measured traffic on the SR policy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>BWOD Policy Bandwidth (Mbps)</b> | The bandwidth constraint associated with a policy created through the Bandwidth on Demand function pack.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Metric Type</b>                  | The metric type can be of type TE, IGP, or latency.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Accumulated Metric</b>           | Total metric calculation of the SR policy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Disjoint Group</b>               | If applicable, displays disjointness information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>PCE Initiated</b>                | If the policy was initiated and provisioned by a PCE, the value is <b>True</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Source Application</b>           | Indicates which application created this SR policy. It can be one of the following: <ul style="list-style-type: none"> <li>• <b>Optimization Engine</b>—The policy was provisioned using the Cisco Crosswork Optimization Engine UI.</li> <li>• <b>Bandwidth Optimization</b>—This is a tactical SR policy that was created by the Bandwidth Optimization function pack to remediate traffic congestion. It will be removed when the congestion goes below the configured threshold.</li> </ul> <p>If it is blank, the SR policy was PCC instantiated.</p> |
| <b>Delegated PCE</b>                | The SR policy is delegated to this PCE IP address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Non Delegated PCEs</b>           | PCEs reporting the policy, but not currently delegated.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Affinity</b>                     | Lists any affinity constraints belonging to this policy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Segment</b>                      | Lists whether a dynamic path policy should prefer protected or require unprotected SIDSs                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>PCE Computed Time</b>            | Time when PCE computed the path currently in effect.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Field       | Description                                                                                                                                                                                   |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Last Update | The last time the policy was updated.                                                                                                                                                         |
| Path        | Lists segments that are part of the policy. It gives the following segment information: segment type, label, IP address, associated node, interface, and SID type (Protected or Unprotected). |





## CHAPTER 6

# Perform Administrative Tasks

---

This section contains the following topics:

- [Manage Users](#), on page 103
- [Manage TACACS+ Servers](#), on page 107
- [Define Network Topology Display Settings](#), on page 108
- [Manage Certificates](#), on page 109
- [Manage Cisco Crosswork Network Automation](#), on page 111
- [Security Hardening Overview](#), on page 120

## Manage Users

From the main menu, select **Admin > Users** to display the **User Management** window. Using this window, you can add a new user, edit the settings for an existing user, delete a user from the network, and create user roles.



---

**Note** Before you can create a new user that does *not* have admin-level access to Cisco Crosswork Optimization Engine functionality, you must first create a new role that limits the features they can access. See [Create User Roles](#) for more information.

Only a local admin user can add, update, and delete other local user accounts. A TACACS+ user, regardless of role assigned, will not be able to manage local users.

---

## Administrative Users Created During Installation

During installation, Cisco Crosswork Optimization Engine creates two special administrative IDs:

1. The **virtual machine administrator**, with the username **cw-admin**, and the default password **cw-admin**. Data center administrators use this ID to log in to and troubleshoot the VM hosting the Cisco Crosswork Optimization Engine server.
2. The **Crosswork administrator**, with the username **admin** and the default password **admin**. Product administrators use this ID to log in to and configure the Cisco Crosswork Optimization Engine user interface, and to perform special operations, such as creating new user IDs.

The default password for both administrative user IDs must be changed the first time they are used. You can also change the Crosswork administrator password using the following methods:

- Log in as the admin user and edit the admin user password, as explained in [Edit Users, on page 104](#).
- Enter the following command: `admin(config)# username admin <password>`

## Add Users

Follow the steps below to create a new Cisco Crosswork Optimization Engine user ID.

The user ID's user name must be unique. You cannot create a new user ID with the same user name as an existing user ID.


The special administrative user names **admin** (for administering Cisco Crosswork Optimization Engine) and **cw-admin** (for administering the virtual machine hosting the product) are created during installation and are reserved for those purposes (see [Administrative Users Created During Installation, on page 103](#)).

---

**Step 1** From the main menu, choose **Admin > Users**.

The **User Management** window opens.

If it is not already displayed, click the **User Management** tab.

**Step 2** Click  to open the **Add New User** dialog box.

**Step 3** Enter the following information for the user you are adding:

- **User Name:** Enter the name of the user ID. User Names cannot contain spaces or special characters.
- **First Name** and **Last Name:** Enter the first and last name of the person assigned to this user ID.
- **Password** and **Confirm Password:** Enter the default password for this user ID. The user will be required to change the default password the first time they attempt to log on using it.

**Step 4** From the **Select Role** drop-down at the bottom of the dialog box, choose the role that you want to assign to the user.

See [Create User Roles](#) for more information.


**Step 5** Click **Add**.

---

## Edit Users

Users with administrator privileges can edit any user ID's User Name, First Name, Last Name, and Role.

Administrators cannot change a user's password by editing the user ID. Users can change their passwords by

logging in, clicking , and selecting **Change Password**.


---

**Step 1** From the main menu, choose **Admin > Users**.

The **User Management** window opens.



If it is not already displayed, click the **User Management** tab.


- Step 2** Click on the user ID whose settings you want to update, then click  to open the **Edit User** dialog box.
- Step 3** Make the necessary updates to the user ID.
- Step 4** Click **Update** to save your changes.
- 

## Delete Users

Follow the steps below to delete an existing user ID.

The administrative user IDs **admin** and **cw-admin** created during installation cannot be deleted (see [Administrative Users Created During Installation, on page 103](#)).

---

- Step 1** From the main menu, choose **Admin > Users**.  
The **User Management** window opens.  
If it is not already displayed, click the **User Management** tab.
- Step 2** Click on the user ID you want to delete, then click . The **Delete Username User** dialog displays.
- Step 3** Click **Delete** to confirm deletion.
- 

## Create User Roles


Local users with administrator privileges can create new users as needed (see [Add Users, on page 104](#)).

Users created in this way can perform only the functions or tasks that are associated with the user role they are assigned.

The local **admin** role enables access to all functionality. It is created during installation and cannot be changed or deleted. However, its privileges can be assigned to new local users. Only local users can create or update user roles; TACACS users cannot.

Follow the steps below to create a new user role.

---

- Step 1** From the main menu, choose **Admin > Users**.  
The **User Management** window opens.  
If it is not already displayed, click the **Role Management** tab.
- Step 2** Click  to display the **Add Role** dialog box.
- Step 3** Enter a unique name for the new role and then click **Add**.
- Step 4** Define the user role's privilege settings:
- Check the check box for every API that users with this role can access.

- b) For each API, define whether the user role has **Read**, **Write**, and **Delete** permission by checking the appropriate check box.

**Step 5** When you are finished, click **Save** to create the new role.

To assign the new user role to one or more user IDs, edit the **Role** setting for the user IDs (see [Edit Users, on page 104](#)).

---

## Edit User Roles

Users with administrator privileges can quickly change the privileges of any user role other than the default **admin** role.

---

**Step 1** From the main menu, choose **Admin > Users**.

The **User Management** window opens.

If it is not already displayed, click the **Role Management** tab.

**Step 2** Click on an existing role to select it. The **Role Management** tab displays the user role's settings.

**Step 3** Define the role's settings:

- a) Check the check box for every API that the role can access.
- b) For each API, define whether the role has **Read**, **Write**, and **Delete** permission by checking the appropriate check box.

**Step 4** When you are finished, click **Save** to save your changes.

---

## Clone User Roles

Cloning an existing user role is the same as creating a new user role (see [Create User Roles, on page 105](#)), except that you need not set privileges for it. If you like, you can let the cloned user role inherit all the privileges of the original user role.

Cloning user roles is a handy way to create and assign many new user roles quickly. Following the steps below, you can clone an existing role multiple times. Defining the cloned user role's privileges is an optional step; you are only required to give the cloned role a new name. If you like, you can assign it a name that indicates the role you want a group of users to perform. You can then edit the user IDs of that group of users to assign them their new role (see [Edit Users, on page 104](#)). Later, you can edit the roles themselves to give users the privileges you want (see [Edit User Roles](#)).

---

**Step 1** From the main menu, choose **Admin > Users**.

The **User Management** window opens.

If it is not already displayed, click the **Role Management** tab.

**Step 2** Click on an existing role to select it.


**Step 3** Click  to display the **Clone Role** dialog box.

- Step 4** Enter a unique name for the cloned role and then click **Clone**.
- Step 5** (Optional) Define the role's settings:
- Check the check box for every API that the cloned role can access.
  - For each API, define whether the clone role has **Read**, **Write**, and **Delete** permission by checking the appropriate check box.
- Step 6** Click **Save** to create the newly cloned role.
- 

## Delete User Roles

Users with administrator privileges can delete any user role that is not the default **admin** user role or that is not currently assigned to a user ID. If you want to delete a role that is currently assigned to one or more user IDs, you must first edit those user IDs to assign them to a different user role.

---

- Step 1** From the main menu, choose **Admin > Users**.  
The **User Management** window opens.  
If it is not already displayed, click the **Role Management** tab.
- Step 2** Click on the role you want to delete, to select it.
- Step 3** Click  to display the **Delete Role** dialog box.
- Step 4** Click **Delete** to confirm that you want to delete the user role.
- 

## Manage TACACS+ Servers

In addition to local database authentication, Cisco Crosswork Optimization Engine can use TACACS+ servers to authenticate users. TACACS+ is a security protocol that provides centralized validation of users attempting to access your network. It allows for a single access control server (the TACACS+ daemon) to provide authentication, authorization, and accounting (AAA) services independently of one another.

Local database authorization takes precedence over authorization by TACACS+ server. When adding the TACACS+ server, you can specify the priority value for each instance.

Please note that any operation you do following the instructions in this section will affect all new logins to the Cisco Crosswork Optimization Engine user interface. To minimize session interruption, Cisco recommends that you perform all your TACACS+ changes and submit them in a single session.


## Add a TACACS+ Server

Before adding a TACACS+ server, you will need to know the server's IP address, port number, shared secret, and service name.

---

- Step 1** From the main menu, choose **Admin > AAA**.

The AAA window opens.

**Step 2** Click  to open the **Add Server** dialog box.


**Step 3** Enter the TACACS+ server's settings, then click **Add**.

**Note** Only the server's IP address, port number, shared secret, and service name are required. You can leave the other values blank, as needed.

## Edit a TACACS+ Server

**Step 1** From the main menu, choose **Admin > AAA**.

The AAA window opens.

**Step 2** Click the check box next to the TACACS+ server whose settings you want to update, then click . The **Edit Server** dialog box opens.

**Step 3** Make the necessary changes, then click **Update**.

**Note** You cannot change the value for the **Shared Secret** parameter.


## Delete a TACACS+ Server

**Step 1** From the main menu, choose **Admin > AAA**.

The AAA window opens.

**Step 2** Click the check box next to the TACACS+ server you want to delete.

**Note** You can delete only one TACACS+ server at a time.

**Step 3** Click . The **Delete server-IP-address** dialog box opens.

**Step 4** Click **Delete** to confirm.

## Define Network Topology Display Settings

Cisco Crosswork Optimization Engine administrator privileges are required to configure the display settings that are used by the Network Topology application.

For a description of how to configure these settings, see the following topics:

- [Define Color Thresholds for Link Bandwidth Utilization](#)
- [Configure Geographical Map Settings, on page 65](#)

## Manage Certificates

The Cisco Crosswork Optimization Engine VM-hosted server and its browser-based user interface communicate with each other using SSL certificates exchanged over HTTPS. For details about these protocols, see [SSL Certificates, on page 121](#) and [HTTPS, on page 120](#)

When installed, Cisco Crosswork Optimization Engine secures these interactions using a self-signed TLS certificate. This certificate has a two-year lifespan, after which it expires. If you want to continue using the expired self-signed certificate to secure server/client communications, you will need to regenerate it by following the steps in [Extend Self-Signed Certificate Expiration, on page 110](#)

If you prefer to secure these communications with a user-provided certificate, either purchased from a Certificate Authority (CA) or self-signed by your organization, you can validate and upload it by following the steps in [Substitute a User-Provided Certificate, on page 110](#).

The user-provided certificate must meet the following requirements:

- Cisco Crosswork Optimization Engine supports IP Subject Alternative Name (SAN) server certificates only. The IP address is the primary means to reach the user interface.
- The server will present your user-provided certificates to the browser, so the certificates you supply must be valid both for Cisco and for Cisco Crosswork Optimization Engine.
- It must also include the required fields and field values shown in the following table.

**Table 10: Required User-Provided Certificate Fields and Values**

| Field                      | Description                                   | Value                                                                            |
|----------------------------|-----------------------------------------------|----------------------------------------------------------------------------------|
| <NUMBER OF DAYS>           | Number of days the certificate will be valid. | Must be greater than <b>30</b> days and less than <b>730</b> days (or two years) |
| <COUNTRY>                  | Country (c=)                                  | <b>US</b>                                                                        |
| <STATE>                    | State (sT=)                                   | <b>CALIFORNIA</b>                                                                |
| <LOCATION>                 | Location (l=)                                 | <b>SAN JOSE</b>                                                                  |
| <ORGANIZATION>             | Organization (o=)                             | <b>CISCO SYSTEMS INC</b>                                                         |
| <ORGANIZATIONAL UNIT NAME> | Organizational Unit (ou=)                     | <b>CROSSWORK</b>                                                                 |
| <COMMON NAME>              | Common Name (cn=)                             | The IP address of the Cisco Crosswork Optimization Engine server VM.             |

- The certificate must also have the SAN extension set, with both DNS and IP address keys. The following provides an example of how to generate a self-signed certificate using OpenSSL:

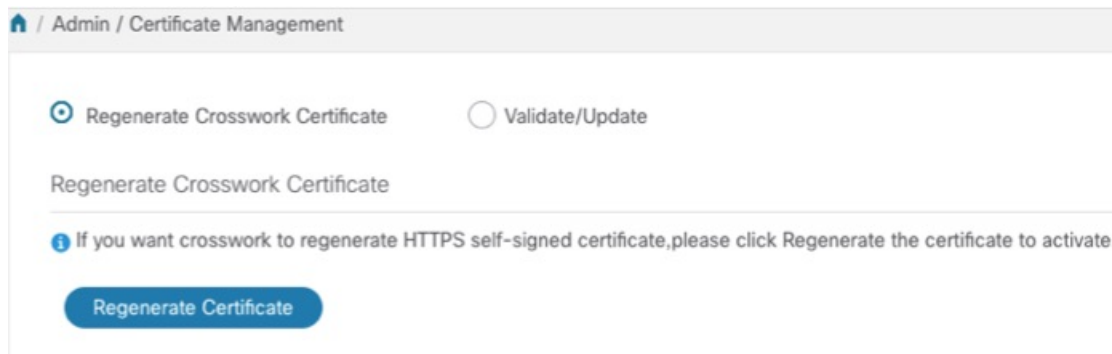
```
/usr/bin/openssl req \
 -x509 \
 -nodes \
 -days 730 \
 -newkey rsa:4096 \
 -keyout "filename.key" \
 -out "filename.crt" \
 -subj "/C=US/ST=CALIFORNIA/L=SAN JOSE/O=CISCO SYSTEMS
INC/OU=CROSSWORK/CN=1.1.1.1" \
 -extensions SAN \
 -config <(cat /etc/ssl/openssl.cnf \
 <(printf "\n[SAN]\nsubjectAltName=DNS:0.0.0.0,IP:1.1.1.1"))
```

## Extend Self-Signed Certificate Expiration

Follow these steps to regenerate the self-signed certificate and extend its lifetime by two years.

**Step 1** From the main menu, select **Admin > Certificate Management**. The **Certificate Management** window appears.

**Step 2** Select the **Regenerate Crosswork Certificate** radio button.



**Step 3** When you are ready, click **Regenerate Certificate**.

When Cisco Crosswork Optimization Engine has finished regenerating the certificate, it displays an alert message indicating that the regeneration operation is successful and you will be logged out. You must log in again to continue using Cisco Crosswork Optimization Engine.

## Substitute a User-Provided Certificate

Follow the steps below to validate and upload a user-provided certificate. The certificate must meet the requirements explained in [Manage Certificates, on page 109](#).

### Before you begin

You must know the names of the user-provided certificate and key files and their locations in your local storage.

- Step 1** From the main menu, select **Admin > Certificate Management**. The **Certificate Management** window appears.
- Step 2** Select the **Validate/Update** radio button.
- Step 3** Use the **Browse** button next to each field to browse to and select the key and certificate files you want to validate and use.

The screenshot shows the 'Admin / Certificate Management' interface. At the top, there are two radio buttons: 'Regenerate Crosswork Certificate' (unselected) and 'Validate/Update' (selected). Below this, the section is titled 'Validate/Update Certificate'. An information icon (i) is followed by the text: 'You can upload new Certificate here. once you upload the files, it will be validated and updated.' There are two input fields: 'Key File\*' with the value 'foo.key' and 'Cert File\*' with the value 'foo.crt'. Each input field has a close button (X) and a 'Browse' button. At the bottom, there are two buttons: 'Validate' (solid blue) and 'Update' (outlined blue).

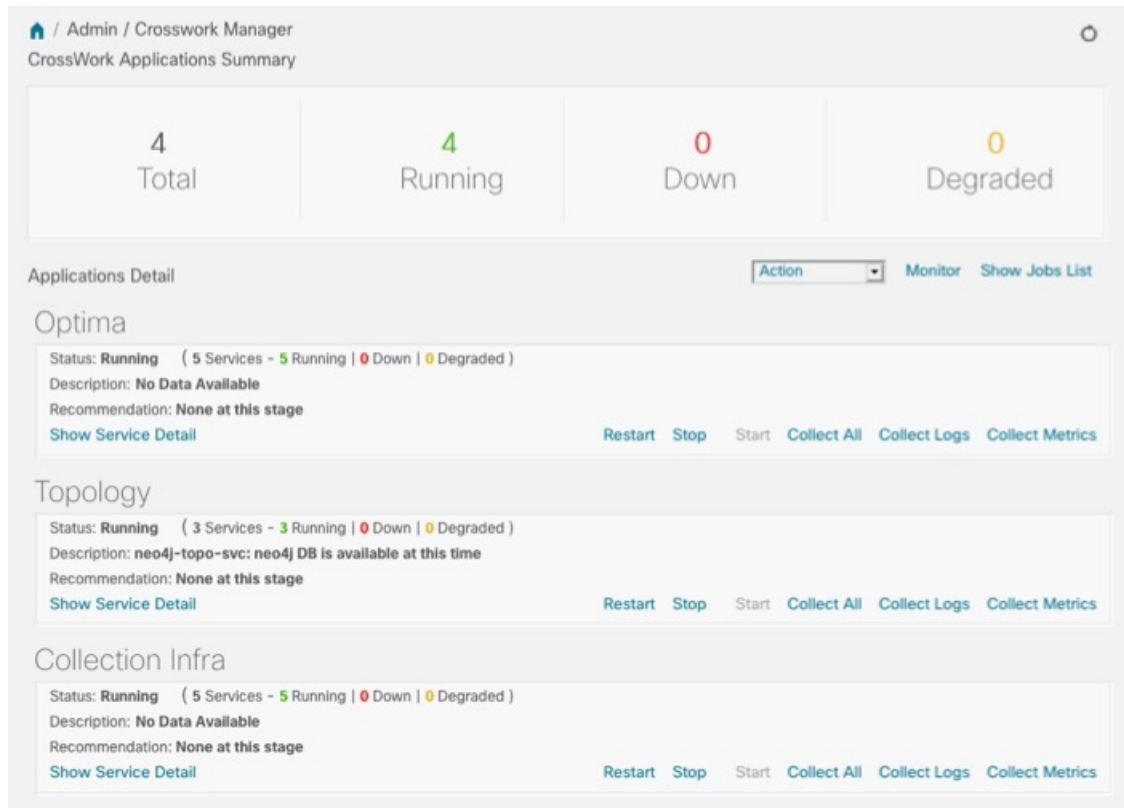
- Step 4** Click **Validate** to validate the certificate and key files.
- Step 5** Click **Update** to replace the existing certificate with the user-provided certificate you have validated.

## Manage Cisco Crosswork Network Automation

The **Crosswork Manager** window gives you consolidated information about the current status of each installed Cisco Crosswork Optimization Engine application and its supporting services. It also supplies tools and information that, with support and guidance from your Cisco Customer Experience account team, you can use to identify, diagnose and fix issues with Cisco Crosswork Optimization Engine.

Select **Admin > Crosswork Manager** to display a **Crosswork Manager** window, with information like the window shown in the following example.

Figure 44: Crosswork Manager Window



The **Crosswork Manager** window has two main views. The **Crosswork Applications Summary** view, at the top of the window, is a dashboard giving you a quick look at the overall health of the system. It displays the total number of Cisco Crosswork Optimization Engine applications currently installed in the system, and how many of that total are **Running**, **Down**, or **Degraded**.

The **Applications Detail** view, below the **Crosswork Applications Summary** view, allows you to:

- View the name and current runtime status of each installed application and its supporting services.
- Get advice about what to do when an application or one of its services has issues.
- Collect logs and metrics on any application or service, or for the system as a whole.
- Stop, start, or restart any application or service.

The **Applications Detail** view, shown in the following figure, is the best way to investigate any system health issues indicated in the **Crosswork Applications Summary**.



Figure 45: Applications Detail View

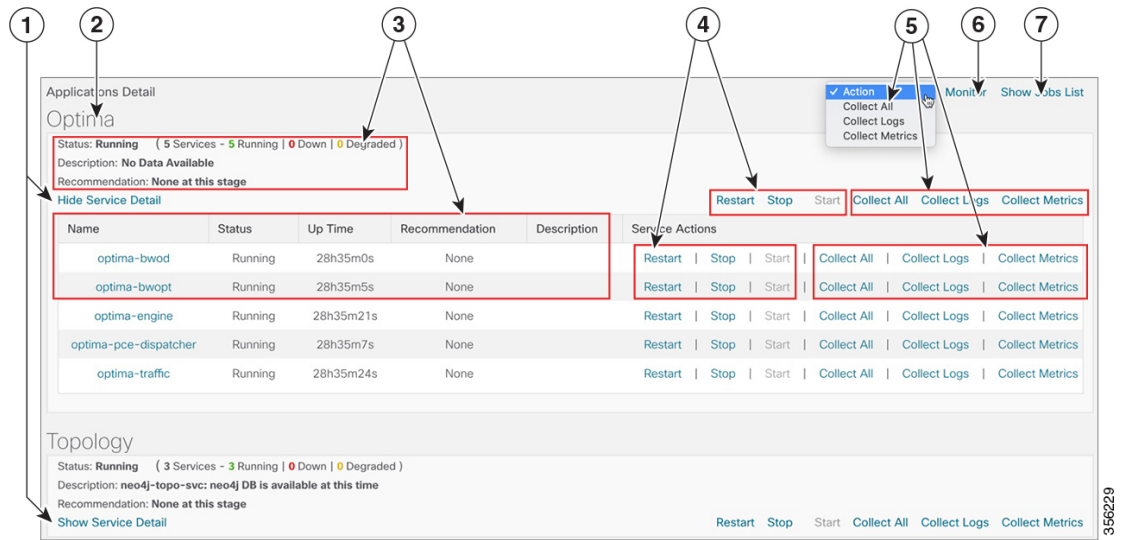


Figure 46: Applications Detail View

| Item | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Click the <b>Show/Hide Service Detail</b> link in each application tile to view the detailed status of the underlying services for that application.                                                                                                                                                                                                                                                                                                                                      |
| 2    | An <b>application tile</b> like this shows the current status of the named application and a summary of the status of that application's services. This includes the total number of services, and how many of those services are Running, Down, or Degraded.                                                                                                                                                                                                                             |
| 3    | Both the <b>application tile</b> and its <b>Service Detail</b> table provide the name, status, description and recommendation for the respective application or service. The Service Detail table also provides service uptime, and you can click on the link in the <b>Name</b> column to see more details about the service, such as its process ID and pod identifier.                                                                                                                 |
| 4    | To control an application or service, click on any of the links in this section of the application tile or Service Detail table. You can click: <ul style="list-style-type: none"> <li>• <b>Restart</b> to restart the application or service.</li> <li>• <b>Stop</b> to stop the application or service.</li> <li>• <b>Start</b> to start the application or service.</li> </ul> See <a href="#">Control Cisco Crosswork Network Automation Applications and Services</a> , on page 119. |

| Item | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5    | <p>To gather logs and metrics for the entire system, or for any application or service, click on any of the "collect" links at the system (in the dropdown menu), application, or service level. You can choose:</p> <ul style="list-style-type: none"> <li>• <b>Collect All</b> to collect both logs and metrics.</li> <li>• <b>Collect Logs</b> to collect only logs.</li> <li>• <b>Collect Metrics</b> to collect only metrics.</li> </ul> <p>See <a href="#">Collect and Share Cisco Crosswork Network Automation Logs and Metrics</a>, on page 118.</p> |
| 6    | <p>Click the <b>Monitor</b> link to monitor individual Cisco Crosswork Optimization Engine functions and features, using analytical dashboards and data gathered over the last 24 hours of run time.</p> <p>See <a href="#">Monitor Cisco Crosswork Network Automation Functions in Real Time</a>, on page 114.</p>                                                                                                                                                                                                                                          |
| 7    | <p>Choosing any of the control or collect actions at the system, application or service level will initiate a job. You can view each job's progress by clicking the <b>Show Jobs List</b> link at the top right corner of the window. You can also use the <b>Show Jobs List</b> to publish collected logs and metrics files, and check on the status of publish jobs you initiate.</p>                                                                                                                                                                      |

## Monitor Cisco Crosswork Network Automation Functions in Real Time

You can monitor the health of Cisco Crosswork Optimization Engine and any of its functions in real time, using a set of monitoring dashboards you can access from the **Crosswork Manager** window.

Cisco Crosswork Optimization Engine uses Grafana to create these dashboards. They give you a graphical view of the product's infrastructure, using metrics collected in its database. You can use these dashboards to diagnose problems you may encounter with individual Cisco Crosswork Optimization Engine applications or their underlying services.

There are multiple monitor dashboards, categorized by the type of functionality they monitor and the metrics they provide, as shown in the following table.

**Table 11: Monitoring Dashboard Categories**

| This dashboard category... | Monitors...                                                                                                                                                                                       |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Optima</b>              | Cisco Crosswork Optimization Engine function pack, traffic, and SR-PCE dispatcher functions.                                                                                                      |
| <b>Topology</b>            | Topology service and database functions.                                                                                                                                                          |
| <b>Collection Infra</b>    | Device-data collection functions. Metrics include telemetry collection latencies, total collection operations, memory and database activity related to telemetry, delayed collections, and so on. |
| <b>Core Infra</b>          | System hardware and communications usage and performance. Metrics include disk and CPU usage, database size, network and disk operations, and client/server communications.                       |

To conserve disk space, Cisco Crosswork Optimization Engine maintains a maximum of 24 hours of collected metric data.

Grafana is an open-source visualization tool. The following provides general information about how to use the Cisco Crosswork Optimization Engine implementation of Grafana. For more information about Grafana itself, see <https://grafana.com> and <http://docs.grafana.org>

---

**Step 1** From the main menu, choose **Admin > Crosswork Manager**.

**Step 2** At the right, just below the **Crosswork Applications Summary** view, click the **Monitor** link, highlighted below.



The Grafana user interface appears within the **Crosswork Manager** window, replacing the **Applications Detail** view.

**Step 3** In the Grafana user interface, click **Home**. Grafana displays the list of monitoring dashboards and their categories, as shown in the following example.

Home / Admin / Crosswork Manager

CrossWork Applications Summary

|            |              |           |
|------------|--------------|-----------|
| 5<br>Total | 5<br>Running | 0<br>Down |
|------------|--------------|-----------|


Action ▼ St

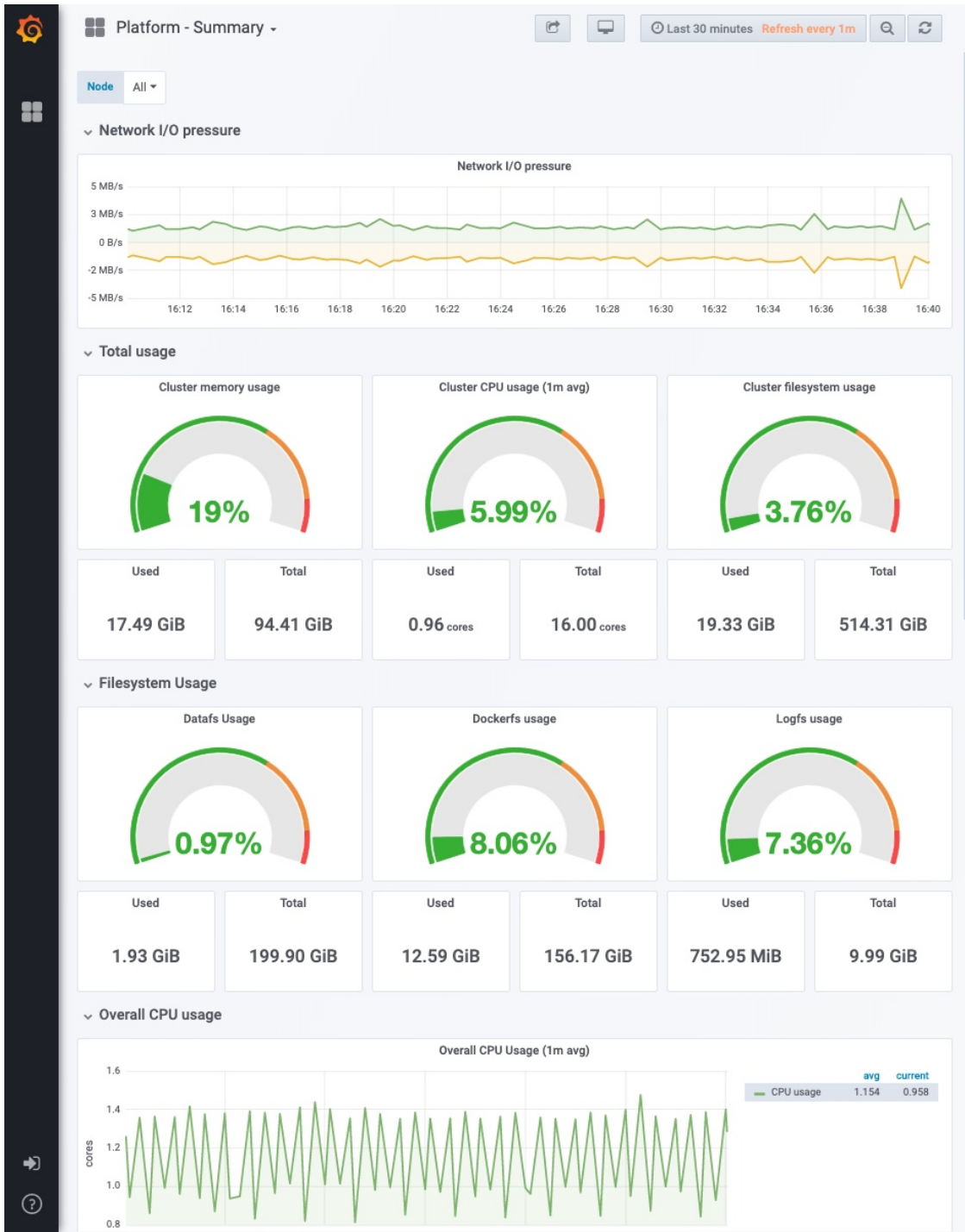
Find dashboards by name

Recent

General

- Change Automation nca
- Collection - Manager collection
- Collection - Pipeline CLI collection
- Collection - Pipeline Kafka collection
- Infra - Etcd infra
- Infra - Kafka infra
- Infra - Nats infra
- Inventory - Manager inventory
- Platform - Metrics platform
- Platform - Pods platform
- Platform - Statefulsets platform
- Platform - Summary kubernetes platform

**Step 4** Click the  icon next to the dashboard you want to view. For example: Clicking on the **Platform - Summary** dashboard displays a view like the one shown in the following figure. For more information on how to use Grafana go to <https://grafana.com>.



## Collect and Share Cisco Crosswork Network Automation Logs and Metrics

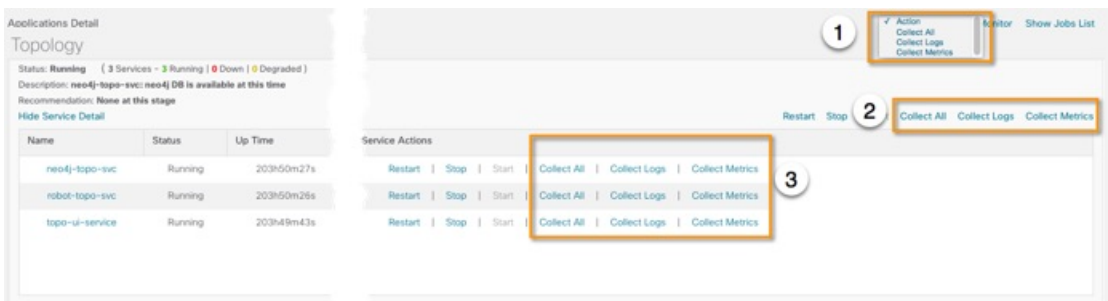
You can collect logs and metrics on multiple levels of Cisco Crosswork Optimization Engine. You can collect logs and metrics for the entire system, for any of its installed application, or for any service supporting an application. You can also choose to collect only logs, only the additional metrics, or both.

Collected logs and metrics are stored in gzipped tar archive files. You can publish these archives to an HTTP or HTTPS server of your choice.

**Step 1** From the main menu, choose **Admin > Crosswork Manager**. The **Crosswork Manager** window displays, with the **Application Detail** section listing all the applications.

**Step 2** Click the option for the collection level and target information you want, as follows:

- To collect for the entire system: From the **Action** drop down on the right, opposite the **Applications Detail** section title, choose **Collect All**, **Collect Logs**, or **Collect Metrics**. See item 1 in the following figure.
- To collect for an application: Scroll to the **Application Detail** tile for the application you want. Then click the **Collect All**, **Collect Logs**, or **Collect Metrics** link on the right, opposite the application's name. See item 2 in the following figure.
- To collect for a service: Scroll to the **Application Detail** tile for the application whose service you want to collect. Click the **Show Service Detail** link for that application. Then click the **Collect All**, **Collect Logs**, or **Collect Metrics** link on the right, opposite the service's name. See item 3 in the following figure.



**Step 3** When you click on the collection option you want, the **Crosswork Manager** window displays a popup message indicating that a job was successfully created and giving the job ID. Click on the **Show Jobs List** link at the right to view the job's progress in the **Crosswork Manager** window's **Jobs List** view, which replaces the **Applications Detail** view.

**Step 4** Wait for the job to complete. When the **Jobs List** view's **Status** column for your job has changed to **JobCompleted**, the **Action** column for the job will show an enabled **Publish** link for the completed job, and the **Description** column will show the file name of the gzipped tar archive file containing the collected information.

| User  | Job Id   | Status       | Job Scope       | Description                        | Action  | Publish Status |
|-------|----------|--------------|-----------------|------------------------------------|---------|----------------|
| admin | 20190506 | JobCreated   | Health-Insights | Job in progress. Progress compl... | Publish | Details        |
| admin | 20190506 | JobCompleted | All             | showtech_all_20190506175107...     | Publish | Details        |

- Step 5** (Optional) Click on the **Publish** link to publish the collected information to an HTTP or HTTPS server, as follows:
- A popup window will prompt you for the destination server host name, the storage path on the server, the port number, and the login user name and password for the server (if required). Enter the server information and click **Publish**.
  - The **Job List** view's **Publish Status** column for the job shows an enabled **Details** link. Click the **Details** link to view a popup window showing the status of the publish job.

- Step 6** When you are finished, click the **Show Application Details** link to re-display the **Applications Detail** view.

## Control Cisco Crosswork Network Automation Applications and Services

Users with administrator privileges can control the runtime status of any Cisco Crosswork Optimization Engine application or service. This can include:

- Stopping a running application or service
- Starting a stopped application or service
- Restarting a running or stopped application or service

Please note that stopping, starting and restarting Cisco Crosswork Optimization Engine applications and services can result in anomalous system behavior and possible data loss. Use these functions only with the supervision of Cisco TAC staff.

- Step 1** From the main menu, choose **Admin > Crosswork Manager**. The **Crosswork Manager** window displays, with the **Application Detail** view listing all the applications.
- Step 2** Display the application or service whose runtime status you want to control:
- To control an application: Scroll to the **Application Detail** tile for the application you want.
  - To control a service: Scroll to the **Application Detail** tile for the application whose service you want to control, then click the **Show Service Detail** link for that application to show its services.
- Step 3** Click on the **Start**, **Stop**, or **Restart** link shown next to the service (item 1 in the following figure) or the application whose runtime status you want to control.

The screenshot displays the 'Topology' section of the Crosswork Manager. It shows a table of services with columns for Name, Status, and Up Time. Below the table, there are two callouts: '1' points to the 'Service Actions' section, and '2' points to the 'Restart', 'Stop', and 'Start' buttons.

| Name            | Status  | Up Time    |
|-----------------|---------|------------|
| neo4j-topo-svc  | Running | 204h39m46s |
| robot-topo-svc  | Running | 204h39m45s |
| topo-ui-service | Running | 204h39m2s  |

Service Actions:

| Service Name    | Restart | Stop | Start | Collect |
|-----------------|---------|------|-------|---------|
| neo4j-topo-svc  | Restart | Stop | Start | Collect |
| robot-topo-svc  | Restart | Stop | Start | Collect |
| topo-ui-service | Restart | Stop | Start | Collect |

**Step 4** Click the **Show Jobs List** link at upper right to view the runtime control job's progress in the **Crosswork Manager** window's **Jobs List** view.

**Step 5** When you are finished, click the **Show Application Details** link to re-display the **Applications Detail** view.

## Security Hardening Overview

Security hardening entails making adjustments to ensure that the following components optimize their security mechanisms:

- infrastructure
- storage system (local or external)

Hardening security requires completion of the following tasks:

- Shutting down insecure and unused ports
- Configuring network firewalls
- Hardening the infrastructure, 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 in this section to secure .

## Core Security Concepts

If you are an administrator and are looking to optimize the security of your 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 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 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.

## Disable Insecure Ports and Services

As a general policy, any ports that are not needed 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 . You can do this by listing the ports that are open and comparing it with a list of ports needed for .

To view a list of all open listening ports:

### Step 1

Log in as a Linux CLI admin user and enter the `netstat -aln` command.

The `netstat -aln` 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. The command returns output similar to the following:

```

[root@vm ~]# netstat -aln
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 0.0.0.0:111 0.0.0.0:* LISTEN
tcp 0 0 127.0.0.1:8080 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN
tcp 0 0 127.0.0.1:25 0.0.0.0:* LISTEN
tcp 0 0 127.0.0.1:10248 0.0.0.0:* LISTEN
tcp 0 0 127.0.0.1:10249 0.0.0.0:* LISTEN
tcp 0 0 192.168.125.114:40764 192.168.125.114:2379 ESTABLISHED
tcp 0 0 192.168.125.114:48714 192.168.125.114:10250 CLOSE_WAIT
tcp 0 0 192.168.125.114:40798 192.168.125.114:2379 ESTABLISHED
tcp 0 0 127.0.0.1:33392 127.0.0.1:8080 TIME_WAIT
tcp 0 0 192.168.125.114:40814 192.168.125.114:2379 ESTABLISHED

```

|     |   |   |                       |                      |             |
|-----|---|---|-----------------------|----------------------|-------------|
| tcp | 0 | 0 | 192.168.125.114:40780 | 192.168.125.114:2379 | ESTABLISHED |
| tcp | 0 | 0 | 127.0.0.1:8080        | 127.0.0.1:44276      | ESTABLISHED |
| tcp | 0 | 0 | 192.168.125.114:40836 | 192.168.125.114:2379 | ESTABLISHED |
| tcp | 0 | 0 | 192.168.125.114:40768 | 192.168.125.114:2379 | ESTABLISHED |
| tcp | 0 | 0 | 127.0.0.1:59434       | 127.0.0.1:8080       | ESTABLISHED |
| tcp | 0 | 0 | 192.168.125.114:40818 | 192.168.125.114:2379 | ESTABLISHED |
| tcp | 0 | 0 | 192.168.125.114:22    | 192.168.125.1:45837  | ESTABLISHED |
| tcp | 0 | 0 | 127.0.0.1:8080        | 127.0.0.1:48174      | ESTABLISHED |
| tcp | 0 | 0 | 127.0.0.1:49150       | 127.0.0.1:8080       | ESTABLISHED |
| tcp | 0 | 0 | 192.168.125.114:40816 | 192.168.125.114:2379 | ESTABLISHED |
| tcp | 0 | 0 | 192.168.125.114:55444 | 192.168.125.114:2379 | ESTABLISHED |

**Step 2** Check the *Cisco Crosswork Optimization Engine Installation Guide* for the table of ports used by Cisco Crosswork Optimization Engine, 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 3** If you have firewalls in your network, configure the firewalls to only allow traffic that is needed for Cisco Crosswork Optimization Engine to operate.

## Harden Your Storage

We recommend that you secure all storage elements that will participate in your installation, such as the database, backup servers, and so on.

- If you are using external storage, contact your storage vendor and your Cisco representative.
- If you are using internal storage, contact your Cisco representative.
- If you ever uninstall or remove , make sure that all VM-related files that might contain sensitive data are digitally shredded (as opposed to simply deleted). Contact your Cisco representative for more information.





## CHAPTER 7

# Configure Collection

---

This section contains the following topics:

- [Collection Service Overview, on page 125](#)
- [Collection Modes, on page 125](#)
- [Prerequisites for Device Telemetry, on page 126](#)
- [List of Supported MIBs and MDT Model, on page 128](#)

## Collection Service Overview

Networks maintain a large amount of data that spans thousands of devices. The Cisco Crosswork Optimization Engine Collection Service collects and manages that flow of data in a multi-vendor environment. The Collection Service leverages existing collection agents and open-source solutions to collect and store data and provides a real-time publish/subscribe model infrastructure to Cisco Crosswork Network Automation applications. The Collection Service is highly scalable in order to meet the performance demands of the Cisco Crosswork Optimization Engine applications.

The Collection Service generates collection orchestration containers that collect streaming endpoint data from devices and push that data to the message bus. The Collection Service is comprised of the following services/processes that run in a collection container:

- Collector Controller—Services requests from applications and manages the collectors
- Telemetry Configuration Server—Interfaces with the devices

The Inventory Manager (also known as the Device Lifecycle Manager, or DLM) is the Cisco Crosswork Optimization Engine device inventory data store, which stores device details such as software version, OS type, device credentials, and capabilities.

Users with administrative privileges can monitor Collection Service status and performance, and start/stop/restart it or its underlying services, using the Cisco Crosswork Optimization Engine user interface. You can also collect logs and performance metrics for this service. For help with these tasks, see [Manage Cisco Crosswork Network Automation, on page 111](#).

## Collection Modes

You may choose one of the following modes for device management collection during installation.

### Single Collection Mode

In single collection mode, only one MDT collector is used for devices. Consider the following information when choosing single collection mode:

- The maximum number of MDT capable devices that can be managed is 500.
- If you do not plan to use Cisco NSO, choose single collection mode. Devices cannot be mapped to Cisco NSO.
- Telemetry configuration will not be automatically pushed by Cisco Crosswork Optimization Engine to devices. You must push the telemetry configuration to devices (see [Prerequisites for Device Telemetry, on page 126](#)).
- The default MDT collector port is 31500.
- Changing from a single collection mode to a multiple collection mode requires the help from a Cisco service representative.

### Multiple Collection Mode

In multiple collection mode, multiple MDT collectors are enabled depending on the number of MDT devices that are added. For the first 500 devices, default 31500 ports will be configured to reach the first MDT collector. The next 500 devices, 31503 ports will be configured to reach the second collector, and so on.



---

**Note** If devices are deleted and then added to Cisco Crosswork Optimization Engine again, then original port assignments will change.

---

Consider the following information when choosing multiple collection mode:

- More than 500 MDT capable devices can be managed.
- You must add a Cisco NSO provider and map devices to it.

## Prerequisites for Device Telemetry

The Cisco Crosswork Optimization Engine Collection Service configures telemetry as needed on the devices enrolled within the service. Telemetry configuration must be done on PCCs or provider edge routers.



---

**Note** Cisco Crosswork Optimization Engine uses the Cisco-IOS-XR-infra-tc-oper YANG module for MDT collection.

---

If an operator configures telemetry directly on the same devices either manually or through some mechanism outside of the Collection Service, the commands must not contain the keyword `cw`. The keyword `cw` is reserved for use by the Collection Service. In particular, the following commands must not contain the keyword `cw` when configured outside of the Collection Service:

```
destination-group
sensor-group
subscription
```

```

sensor-group-id
destination-id

```

For example (invalid telemetry configuration):

```

telemetry model-driven
destination-group CW_1b4ac245d863cf3e787d42bae97f1d18dd300d5e

```

For more information, see the telemetry configuration documentation for your particular device (for example: [Telemetry Configuration Guide for Cisco ASR 9000](#))

If using single collection mode, use only port 31500. If managing more than 500 MDT capable devices and using multiple provider collection mode, you can use other ports. See [Collection Modes, on page 125](#).

### Valid Telemetry Configuration

The following sample output shows a *valid* telemetry configuration on a device when configured outside of the Collection Service. If using a single interface network, then the IP address is the management IP address. In a dual interface network, then the IP address should be the data IP address.

```

telemetry model-driven
destination-group OE_43dc8a5ea99529715899b4f5218408a785e40fce
vrf default
address-family ipv4 192.168.0.3 port 31500
encoding self-describing-gpb
protocol tcp
!
!
destination-group OE_4b3c69a200668b0a8dc155caff295645c684a8f8
vrf default
address-family ipv4 192.168.0.3 port 31500
encoding self-describing-gpb
protocol tcp
!
!
sensor-group OE_43dc8a5ea99529715899b4f5218408a785e40fce
sensor-path Cisco-IOS-XR-infra-tc-oper:traffic-collector/afs/af/counters/tunnels/tunnel
!
sensor-group OE_4b3c69a200668b0a8dc155caff295645c684a8f8
sensor-path
Cisco-IOS-XR-infra-tc-oper:traffic-collector/vrf-table/default-vrf/afs/af/counters/prefixes/prefix
!
subscription OE_43dc8a5ea99529715899b4f5218408a785e40fce
sensor-group-id OE_43dc8a5ea99529715899b4f5218408a785e40fce sample-interval 300000
destination-id OE_43dc8a5ea99529715899b4f5218408a785e40fce
!
subscription OE_4b3c69a200668b0a8dc155caff295645c684a8f8
sensor-group-id OE_4b3c69a200668b0a8dc155caff295645c684a8f8 sample-interval 300000
destination-id OE_4b3c69a200668b0a8dc155caff295645c684a8f8
!

```



**Note** The **sample-interval** can be changed depending on the size of your network. It is defined in milliseconds and determines how fast you want the data to be pushed out.

Confirm that all PCCs or provider edge routers have telemetry configured and report data to Crosswork Optimization Engine. For example, routers should report prefix and tunnel counters:

```
RP/0/RP0/CPU0:PE1#show traffic-collector ipv4 counters prefix
Thu Jul 11 08:32:32.993 UTC
Prefix Label Base rate TM rate State
(Bytes/sec) (Bytes/sec)

192.168.0.1/32 16001 1 0 Active
192.168.0.2/32 16002 1 0 Active
192.168.0.3/32 16003 1 0 Active
192.168.0.4/32 16004 2 0 Active
192.168.0.6/32 16006 501023 501021 Active
192.168.0.7/32 16007 17320774 17320772 Active
192.168.0.8/32 16008 3737825 3737823 Active
192.168.0.9/32 16097 3 0 Active
192.168.0.10/32 16096 2 0 Active
```

```
RP/0/RP0/CPU0:PE1#show traffic-collector ipv4 counters tunnel
Thu Jul 11 08:32:20.746 UTC
Interface Base rate Base rate State
(Packet/sec) (Bytes/sec)

srte_c_102_ep_192.168.0.7 0 0 Active
```

Cisco IOS XR devices that are onboarded through telemetry must have the following configuration settings on the device to ensure that NETCONF and SSH work correctly:

```
ssh server v2
ssh server vrf default
ssh server netconf vrf default
ssh server rate-limit 600
ssh server session-limit 1024
netconf-yang agent ssh
```

Cisco IOS XR devices that are onboarded through SNMP must have SNMP enabled on the device. The following is an example of an SNMP configuration on a Cisco IOS XR device:

```
snmp-server community public RO
```

Please note that, currently, Cisco Crosswork Optimization Engine does not itself support execution of EXEC privilege commands, such as **enable**, on devices. These types of commands must be executed using the device console or other means.

## List of Supported MIBs and MDT Model

The following MIBs are supported:

- IF-MIB
- IP-MIB
- SNMPv2-MIB

The following YANG MDT model is supported:

- Cisco-IOS-XR-infra-tc-oper





## CHAPTER 8

# Get Started with Function Packs

Function packs extend the functionality of Crosswork Optimization Engine. Function packs can be developed to support additional use cases that are not available with the Crosswork Optimization Engine base software package. By leveraging SDKs and APIs, network operators can build additional function packs to support more optimization workflows.

This section describes functions packs that can be purchased with Crosswork Optimization Engine and how to configure and use them. To obtain a Crosswork Optimization Engine function pack license, contact your Cisco representative.

This section contains the following topics:

- [Install Function Packs, on page 129](#)
- [Update Network Configuration for Function Packs, on page 131](#)
- [Bandwidth on Demand, on page 131](#)
- [Bandwidth Optimization, on page 136](#)

## Install Function Packs

To install the Bandwidth on Demand (BWoD) or Bandwidth Optimization function pack, do the following:

### Before you begin

You must have the applicable [Bandwidth on Demand](#) or [Bandwidth Optimization](#) function pack license.

**Step 1** Connect to the Cisco Crosswork Optimization Engine VM via SSH.

**Step 2** Shift to sudo user access (**sudo su**).

**Step 3** (Optional) If you do not know the orchestrator pod name, enter the following command:

```
kubectl get pods -n kube-system | grep robot-orch

robot-orch-5d4d79d549-81zwr 1/1 Running 0 6d
```

In this example, `robot-orch-5d4d79d549-81zwr` is the orchestrator pod name.

**Step 4** Log into the orchestrator pod:

```
kubectl exec -it <pod_name> bash -n kube-system
```

For example:

```
kubectl exec -it robot-orch-5d4d79d549-81zwr bash -n kube-system
```

**Step 5** Open the pod.conf file (`vi /root/pod.conf`) and add the following service names to the "Pods" and "Services" section and save changes.

- optima-bwopt
- optima-bwod

**Figure 47: Example: pod.conf File**

```
namespace : default
pods:
- robot-dlminmgr
- tyk
- helios
- robot-grafana
- neo4j-topo-svc
- robot-topo-svc
- topo-ui-service
- robot-ui
- cas
- optima-traffic
- optima-engine
- optima-pce-dispatcher
- optima-bwopt
- optima-bwod
service:
- robot-dlminmgr
- tyk
- helios
- robot-grafana
- neo4j-topo-svc
- robot-topo-svc
- topo-ui-service
- robot-ui
- topo-ui-service
- cas
- optima-traffic
- optima-engine
- optima-pce-dispatcher
- optima-bwopt
- optima-bwod
```

**Step 6** Update the orchestrator. The update may take up to 30 seconds.

```
robotctl update
Are you sure? [y/n]: y
Operation [update] succeeded
```

**Step 7** Start the function packs:

```
robotctl start optima-bwopt
Are you sure? [y/n]: y
Operation [start,optima-bwopt] is success

#robotctl start optima-bwod
Are you sure? [y/n]: y
Operation [start,optima-bwod] is success
```

**Step 8** Exit and confirm the function packs are running.

```
exit
kubectl get pods
```

You should see `optima-bwod-xxx` and `optima-bwopt-xxx` listed.

**Step 9** Update network configuration. See [Update Network Configuration for Function Packs](#), on page 131.

# Update Network Configuration for Function Packs

The following network configuration parameters must be updated prior to using the Bandwidth on Demand or Bandwidth Optimization function packs.

```
kubectl exec -it optima-engine-55665ff5cb-vvqmqz bash
vi /config/optima-engine.json

{
 "verbosity":60,
 "heartbeat":30,
 "traffic-notification-interval":60,
 "log-toposvc-messages":true,
 "measured-traffic-threshold":0.01,
 "initial-notification-delay":330,
 "use-srtm-policy-traffic":false
}
```

The following parameters can be useful and updated per your preference:

- **measured-traffic-threshold**—Sends traffic update notification if the traffic value has changed at least by the percentage you indicated. This can be any value between 0 (0%) and 1 (100%). In the example above, notification of traffic updates will be sent if the traffic value changes by at least 1% .
- **initial-notification-delay**—The delay in seconds before the first notification goes to function packs after startup.
- **use-srtm-policy-traffic**—Whether to update the policy measured traffic from SRTM. In the example above, it is set to **false**, so policy measured traffic only comes from SNMP.



---

**Note** Function packs rely on telemetry data received from devices. Confirm that devices are configured (see [Prerequisites for Device Telemetry, on page 126](#)).

---

## Bandwidth on Demand

The Bandwidth on Demand (BWoD) function pack provides a bandwidth-aware Path Computation Element (PCE) to derive SR policy paths with requested bandwidth when available. Computed paths are deployed to the network through SR-PCE. BWoD continuously monitors link utilization to ensure no congestion occurs along the path. If conditions change in the network which causes link utilization to exceed the congestion threshold set by the user, BWoD automatically reoptimizes the policy path.

BWoD utilizes a near real-time model of the network along with a demand matrix derived from telemetry-based Segment Routing Traffic Matrix (SRTM) reporting to ensure BWoD policies meet their bandwidth constraints. Users may fine tune the behavior BWoD, affecting the path it computes, through the selection of application options including network utilization threshold (definition of congestion) and path optimization objectives. The BWoD function pack works as a bandwidth-aware PCE for SR policies created through the Crosswork Optimization Engine UI, and for SR policies created through CLI configuration on a headend with delegation to SR-PCE. In the latter case, SR-PCE will subdelegate the SR policy with bandwidth constraint to BWoD for path computation and relay the computed path returned by BWoD to the headend for instantiation.

### Operation Modes

There are two modes of operation for BWoD based on the "Priority" option setting for the application. In non-Priority mode, BWoD takes into account all traffic in the network when computing a path for a SR policy with bandwidth constraint. In this case, BW SR policies compete with all other traffic for resources and may be provided a path that is longer to avoid congestion on links along the shortest path. Note that




---

**Note** In non-Priority mode, BWoD *should not* be enabled at the same time as the Bandwidth Optimization function pack to ensure they do not conflict.

---

The Priority mode allows BWoD to ignore all other traffic in the network that is not flowing through a BWoD SR policy and give its policies priority treatment when computing paths. This means that BWoD policies are only contending for resources with other BWoD policies and will likely take the shortest path unless there are links that include a significant amount of other BWoD traffic.




---

**Note** To mitigate any congestion that may occur by ignoring other traffic, the Bandwidth Optimization application *should* be used in conjunction with BWoD in the Priority mode to shift other traffic away from any hotspots caused by the BWoD traffic.

---

The other traffic may then be sent over alternate (possibly longer) paths to mitigate congestion in this case, while BWoD maintains its policies along the shortest paths.

## Important Notes and Limitation for BWoD

Consider the following notes and limitations when using BWoD:

- If BWoD cannot find a path for a policy that guarantees its requested bandwidth, BWoD will attempt to find a *best effort* path. The best effort path may not meet the requested bandwidth for the policy.
- BWoD temporarily pauses operation whenever the Optimization Engine model is unavailable due to an Optimization Engine restart or a rebuild of the topology from Topology Services. Any requests to BWoD during this time are rejected. When the model becomes available and BWoD receives 2 traffic updates from the Optimization Engine, BWoD will resume normal operation.
- BWoD uses simulated traffic based on measured SRTM data to determine link utilizations for computing BWoD paths. The simulated interface utilization BWoD utilizes should closely align with the SNMP-based interface utilization that is displayed in the Optimization Engine UI. However, due to various factors, including SNMP polling cadence and rate averaging techniques, they may differ at times. This can result in scenarios like a link along a BWoD path appearing to be congested in the UI and BWoD not re-optimizing it.

## Configure Bandwidth on Demand

Do the following to enable and configure Bandwidth on Demand.

### Before you begin

Bandwidth on Demand must be installed (see [Install Function Packs, on page 129](#)).



**Note** If a policy is configured on the router with affinity constraints, they are not considered in the **Bandwidth on Demand** optimization calculation.

- Step 1** From the main menu, choose **Optimization Engine > Function Packs > Bandwidth on Demand**.
- Step 2** From the **Enable** tile, toggle the slider to **True**.  
Notice that each time a tile is updated it turns blue.
- Step 3** Select one of the following **Primary Objectives**:
- **Maximize Available Bandwidth**—Computes an SR policy path maximizing the overall available bandwidth in the network. This setting generally attempts to maximize usable network capacity at the expense of potentially longer paths.
  - **Metric Minimization**—Computes an SR policy path minimizing the metric selected. This setting generally results in the shortest available paths for a metric type.
- Step 4** In the **Link Utilization** tile, enter the congestion constraint (in percentage). When the Bandwidth on Demand application searches a path for the policies being delegated, it will avoid any paths that may exceed the congestion utilization threshold.
- Step 5** In the **Reoptimization Interval** tile, enter the duration (in seconds) after which the paths will be reoptimized if conditions in the network change. This is a count down timer where the BWoD policy will wait to reoptimize until this duration has expired.
- Step 6** In the **Metric Reoptimization Interval** tile, enter the duration (in seconds) after which the paths can be reoptimized for metric optimization. If the bandwidth constraint is still being met, but a shorter IGP or TE path is available, BWoD will not run reoptimization until the timer has expired. This value is meant to dampen frequent path change and reoptimizations in the network.
- Step 7** From the **Priority Mode** tile, toggle the slider to **True** if you have also enabled Bandwidth Optimization. See [Bandwidth on Demand](#), on page 131 for more information on Priority Mode.
- Step 8** Click the **Advanced** tab for more advanced configuration (see the following table for field descriptions).
- Step 9** Click **Commit Changes** to save the configuration.

**Table 12: Advanced Bandwidth on Demand Fields**

| Field                   | Description                                                                           |
|-------------------------|---------------------------------------------------------------------------------------|
| Private New SR Policies | If <b>True</b> , all policies that are created using Bandwidth on Demand are private. |

| Field                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SR Policy Traffic</b>        | <p>Determines the type of bandwidth optimization is performed with each policy.</p> <ul style="list-style-type: none"> <li>• <b>Simulated</b>—Uses the current simulated traffic on the BWoD provisioned SR policies for optimization calculations.</li> <li>• <b>Measured</b>—Uses the current measured traffic of BWoD provisioned SR policies for optimization calculations.</li> <li>• <b>Max Simulated Requested</b>—Uses the maximum value between the current simulated traffic on BWoD provisioned SR policies or the amount of bandwidth requested for optimization calculations.</li> <li>• <b>Max Measured Requested</b>—Uses the maximum value between the current measured traffic on BWoD provisioned SR policies or the amount of bandwidth requested for optimization calculations.</li> </ul> |
| <b>Deployment Timeout</b>       | The time (in seconds) to wait for a PCE dispatcher response.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Update Throttle</b>          | This option is a knob for throttling updates from the Crosswork Optimization Engine. By setting the knob, it tells BWoD to only accept 1 update per x seconds. Set it to 0 to disable the throttle.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Debug Optimizer</b>          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Debug Opt Max Plan Files</b> | The maximum number of debug plan files you would like to save.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Debug Opt</b>                | If <b>True</b> , debug log files will be saved (see <a href="#">Collect and Share Cisco Crosswork Network Automation Logs and Metrics, on page 118</a> ).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

**What to do next**

Create a Bandwidth on Demand SR policy (see [Create Bandwidth on Demand SR Policies, on page 134](#)).

## Create Bandwidth on Demand SR Policies

This task creates a dynamic path steering policy that finds the optimal path that requires a persistent bandwidth and IGP, TE, or delay metrics.

**Before you begin**

You must have the Bandwidth on Demand function pack installed and enabled (see [Install Function Packs, on page 129](#) and [Configure Bandwidth on Demand, on page 132](#)).

**Step 1** From the **SR Policies** table, click **Create**.

**Step 2** Enter the following SR policy values:

a) Required fields:

- **Headend**—Where the SR policy is instantiated. Note: You can either select a node (from the map or drop-down list) or enter part of the node name to filter the headend and endpoint node entries.
- **Endpoint**—The destination of the SR policy.
- **IP Address**—After the endpoint is selected, the SID list is populated and you can select the loopback IP address.

- **Color**—A numerical value that distinguishes between two or more policies to the same node pairs (Headend – Endpoint). Every SR policy between a given headend and endpoint must have a unique color.
- **Path Name**—Enter a name for this SR policy path. SR policy paths from the same headend must be unique. Policy path names are not case sensitive.

b) Optional values:

- **Description**—Enter details or a description of this policy.
- **Explicit Binding SID**—The binding segment is a local segment identifying an SR policy. Each SR policy is associated with a binding segment ID (BSID). The BSID is a local label that is automatically allocated for each SR policy when the policy is instantiated. If you wish to use a specific segment ID, rather than the default one that is automatically assigned, then enter it here.
- **Profile ID**—Identification used to associate an SR policy with a set of features applied to the policy by the headend. It should correspond with a profile configured on the headend.

**Step 3** Under Policy Path, click **Bandwidth On Demand**.

**Note** This option is only available when the Bandwidth on Demand function pack is installed and enabled.

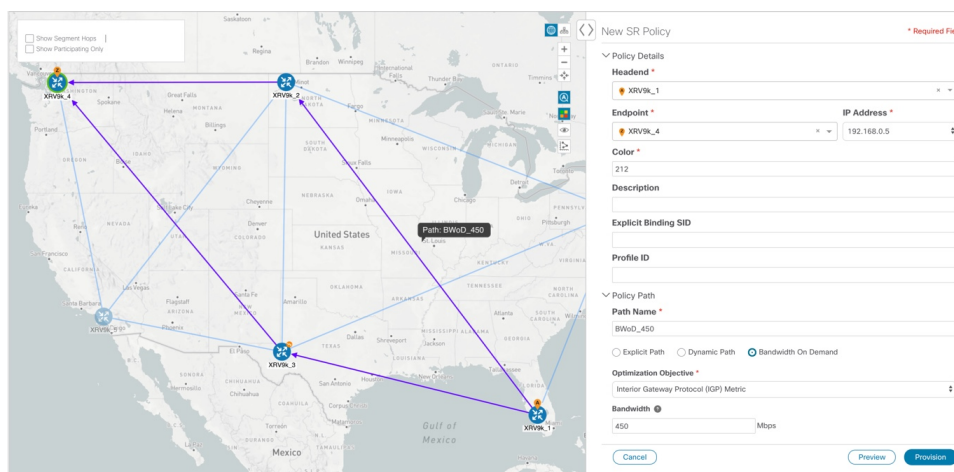
**Step 4** **Optimization Objective**—Depending on the bandwidth constraint chosen (see [Configure Bandwidth on Demand, on page 132](#)), select the specific metric to optimize for Bandwidth on Demand

- **Interior Gateway Protocol (IGP) Metric**—Minimizes total path IGP metric.
- **Traffic Engineering (TE) Metric**—Minimize total path TE metric.
- **Latency**—Minimize total path latency.

**Step 5** **Bandwidth**—Enter the requested bandwidth amount.

**Step 6** Click **Preview**. The path is highlighted on the map.

**Figure 48: Bandwidth on Demand SR Policy Example**



**Step 7** If you are satisfied with the policy path, click **Provision**.

**Step 8** When the policy is provisioned successfully, a window appears with the following options:

- **View SR Policy List**—Displays the **SR Policies** table that lists all SR policies including the one that was just created.
- **Create New**—Allows you to create another SR policy.

## Troubleshoot BWoD

The following are some of the most common error conditions for BWoD and some possible corrective actions that may fix the issue.

*Table 13: Errors*

| Error Event Message                             | Possible Causes and Recommended Corrective Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OptimaModelError                                | <p>The network model used by BWoD from the Optimization Engine is corrupt or is missing key data that is needed to properly support BWoD. Possible causes include network discovery issues or synchronization problems between the Optimization Engine and Topology Services. Try restarting the Optimization Engine pod to rebuild the model.</p> <p>This error can also occur if the time required to discover a policy and add it to the model after it has been deployed exceeds the <b>Deployment Timeout</b> option set for BWoD. The default is 30 seconds which should suffice for small to medium sized networks. However, larger networks may require additional time.</p> |
| NATSTimedOutError                               | <p>The deployment of a bandwidth policy through SR-PCE exceeds the <b>Deployment Timeout</b> option set for BWoD. Increase the <b>Deployment Timeout</b> option to allow for additional time for deployments in larger networks.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Traceback or other errors found in the log file | Please contact your Cisco service representative.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Bandwidth Optimization

The Bandwidth Optimization (BWOpt) function pack provides automated SR policy based tactical traffic engineering capability to detect and mitigate congestion in your network. It achieves this through a real-time view of the network topology overlaid with a demand matrix built through telemetry-based Segment Routing Traffic Matrix (SRTM). BWOpt uses the threshold interface utilization requested by the user and compares it to the actual utilization in the network. When interface congestion is detected by BWOpt, it attempts to shift traffic away from hot spots through the use of tactical traffic engineered SR policies which are deployed to the network via SR-PCE. As network conditions (topology and/or traffic) change over time, BWOpt will continue to monitor interface utilization and manage any tactical SR policies deployed, including changing their paths and/or removing them from the network when deemed no longer necessary.



## Important Notes and Limitations for BWOpt

Consider the following notes and limitations when using BWOpt:

- Only traffic that is not in an SR policy or existing BWOpt SR policy can be rerouted to mitigate congested links. BWOpt will not shift traffic in existing SR policies that it did not create. This may prevent it from being able to mitigate congestion if most of the traffic on the congested link is in non-BWOpt SR policies.
- BWOpt relies on the PCC's autoroute feature to steer traffic into the tactical SR policies it creates. Autoroute is applied to these policies through the proper **Profile ID** option set in BWOpt (to align with configuration on the PCC associating that Profile ID with autoroute feature). This is critical to tactical SR policies shifting traffic away from congested links.
- BWOpt does not support multi-area or multi-level IGP (see "IGP and Inter-AS Support" in the *Cisco Crosswork Optimization Engine Installation Guide*). Autoroute will not properly steer traffic onto inter-area or inter-level tactical SR policies. So, although they can be provisioned, traffic will not use them. Therefore, BWOpt will be ineffective if enabled in this environment.
- BWOpt uses simulated traffic based on measured SRTM data to determine link utilizations and when to mitigate congestion. The simulated interface utilization that BWOpt monitors should closely align with the SNMP-based interface utilization that is displayed in the Optimization Engine UI. However, due to various factors, including SNMP polling cadence and rate averaging techniques, they may differ at times. This can result in scenarios like a link appearing to be congested in the UI and BWOpt not reacting.
- BWOpt only creates tactical SR policies on PCCs that are sources of SRTM telemetry data. Only these nodes (typically provider edge routers) provide the telemetry-based data needed to create simulated traffic demands in the internal model representing the traffic from that node to other PE nodes in the network.
- Only solutions that produce interface utilization below the threshold (set across all interfaces) will be deployed. If BWOpt is unable to mitigate congestion across the entire network, it will not deploy any tactical SR policies and a "Network Congested. BWOpt unable to mitigate." alarm is set. This alarm is unset when congestion either subsides on its own or can be addressed successfully through BWOpt tactical SR policy deployments.
- BWOpt temporarily pauses operation whenever the Optimization Engine model is unavailable due to an Optimization Engine restart or a rebuild of the topology from Topology Services. When this occurs, an alarm indicating this condition is set by BWOpt. During this time, BWOpt will not evaluate congestion in the network. All currently deployed tactical SR policies are maintained, but will not be modified or deleted. As soon as the model becomes available, the alarm is cleared and BWOpt will resume normal operation.

## Configure Bandwidth Optimization

After Bandwidth Optimization is enabled, Cisco Crosswork Optimization Engine monitors all interfaces in the network for congestion based on the configured utilization threshold. When the utilization threshold is exceeded, it automatically deploys tactical policies and moves traffic away from the congested links. When congestion is alleviated, Bandwidth Optimization automatically removes the tactical SR policy.

Do the following to enable and configure Bandwidth Optimization.

### Before you begin

Bandwidth Optimization must be installed (see [Install Function Packs, on page 129](#)).




---

**Note** Bandwidth Optimization should only be enabled (Enable option set to True) together with Bandwidth on Demand if the Bandwidth on Demand "Priority Mode" option is set to True. Otherwise, their actions may conflict resulting in unpredictable behavior.

---


- Step 1** From the main menu, choose **Optimization Engine > Function Packs > Bandwidth Optimization**.
- Step 2** From the **Enable** tile, toggle the slider to **True**.
- Notice that each time a tile is updated it turns blue.
- Step 3** Select one of the following **Optimization Objectives**:
- **Maximize Available Bandwidth**—Leads to preferred paths that result in higher available bandwidth values on interfaces.
  - **Minimize the IGP/TE/Delay**—Leads to preferred paths that result in lower total IGP/TE or Delay metrics..
- Step 4** In the **Color** tile, enter a color value to be assigned to Bandwidth Optimization SR policies.
- Step 5** In the **Utilization Threshold** tile, enter a percentage that represents the interface utilization threshold for congestion. Traffic utilization on any interface exceeding this threshold will trigger Bandwidth Optimization to attempt to mitigate.
- Step 6** In the **Utilization Hold Margin** tile, enter a percentage that represents the utilization below the threshold required of all interfaces to consider removing existing tactical SR policies. For example, if the Utilization Threshold is 90% and the Utilization Hold Margin is 5%, then tactical SR policies deployed by Bandwidth Optimization will only be removed from the network if all interface utilization would be under 85% (90 - 5) without the tactical policy in the network. This serves as a dampening mechanism to prevent small oscillations in interface utilization from resulting in repeated deployment and deletion of tactical SR policies. Utilization Hold Margin must be between 0 and the Utilization Threshold.
- Step 7** In the **Maximum Global Reoptimization Interval** tile, enter the maximum time interval (in minutes) to reoptimize the existing tactical SR policies globally. During a global reoptimization, existing tactical policies may be rerouted or removed to produce a globally more optimal solution. Set to 0 to disable.
- Step 8** From the **Delete Tactical SR Policies when Disabled** tile, toggle the slider to **True** if you want all deployed tactical SR policies deleted when Bandwidth Optimization is disabled.
- Step 9** In the **Profile ID** tile, enter the profile ID that will be assigned to tactical SR policies that are created. Enter 0 if you do not wish to assign a profile ID.
- Step 10** Click the **Advanced** tab for more advanced configuration (see the following table for field descriptions).
- Step 11** Click **Commit Changes** to save the configuration. Cisco Crosswork Optimization Engine begins to monitor network congestion based on the threshold that was configured.
- Note**
- You can easily turn Bandwidth Optimization on or off by toggling the **Enable** slider to **True** or **False**.
  - Click  to view events relating to instantiation and removal of tactical SR policies created by Bandwidth Optimization.
-

Table 14: Advanced Bandwidth on Demand Fields

| Field                                  | Description                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Fix Tactical SR Policy Duration</b> | The minimal time (in seconds) between the creation of a new tactical SR policy to when it can be removed or modified. This serves as a dampening factor to control the rate of change to deployed tactical SR policies.                                                                                                                                                                       |
| <b>Removal Suspension Interval</b>     | The time (in seconds) between any tactical SR policy change to when any tactical SR policy can be removed or modified. This allows SRTM to converge after a tactical SR policy creation, allowing traffic on the policy to be reported accurately.                                                                                                                                            |
| <b>Deployment Timeout</b>              | The maximum time (in seconds) to wait until deployment of tactical SR policies are confirmed.<br>The value assigned should be larger for larger networks to account for the increased processing time needed by SR-PCE to deploy an SR policy. Tactical SR policies not confirmed before this timeout are declared failed and Bandwidth Optimization will disable itself for troubleshooting. |
| <b>Debug Optimizer</b>                 |                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Debug Opt Max Plan Files</b>        | The maximum number of optimizer debug files written to disk.                                                                                                                                                                                                                                                                                                                                  |
| <b>Debug Opt</b>                       | If <b>True</b> , optimizer debug files will be saved to disk in the <b>/tmp</b> dir of the Bandwidth Optimization container.                                                                                                                                                                                                                                                                  |

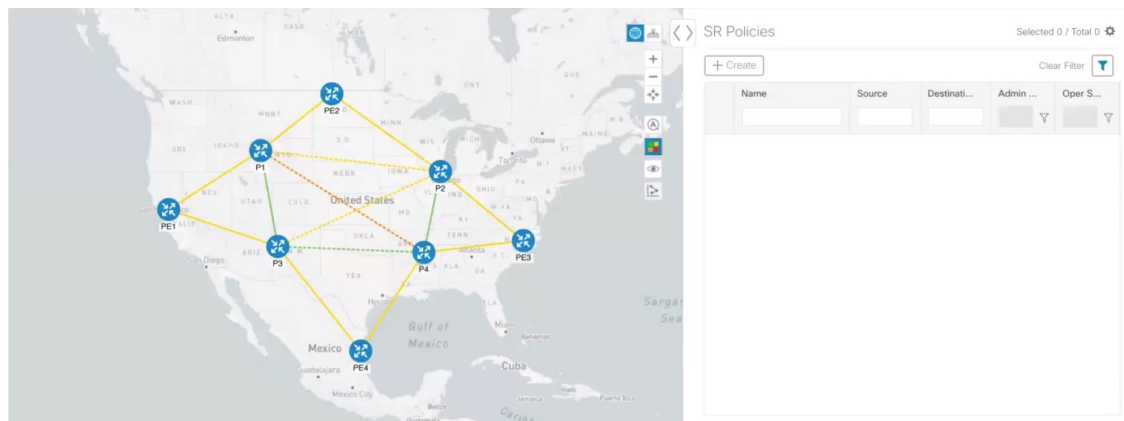
## Bandwidth Optimization Example

In this example, we have configured and enabled Bandwidth Optimization with the following options.

Figure 49: Bandwidth Optimization Configuration

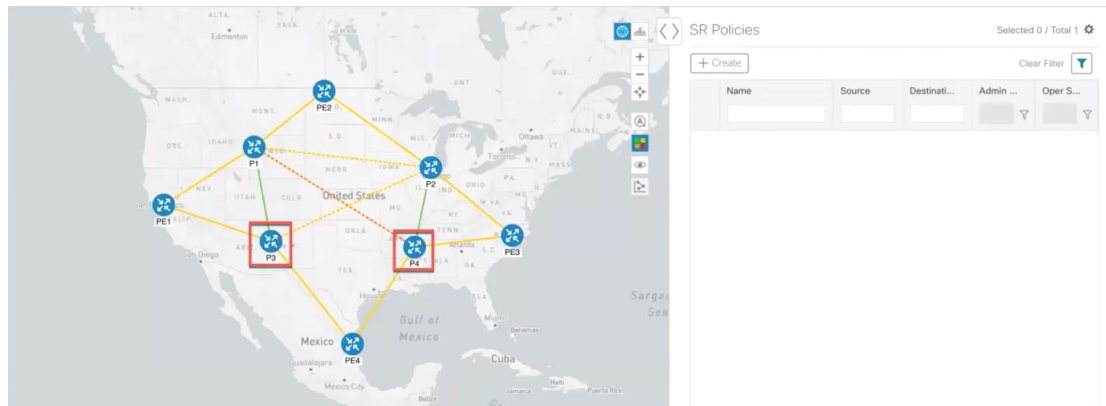
Below is a network with various devices and links that span the United States. Note that there are no SR policies listed in the **SR Policies** window.

Figure 50: Example: Current Network



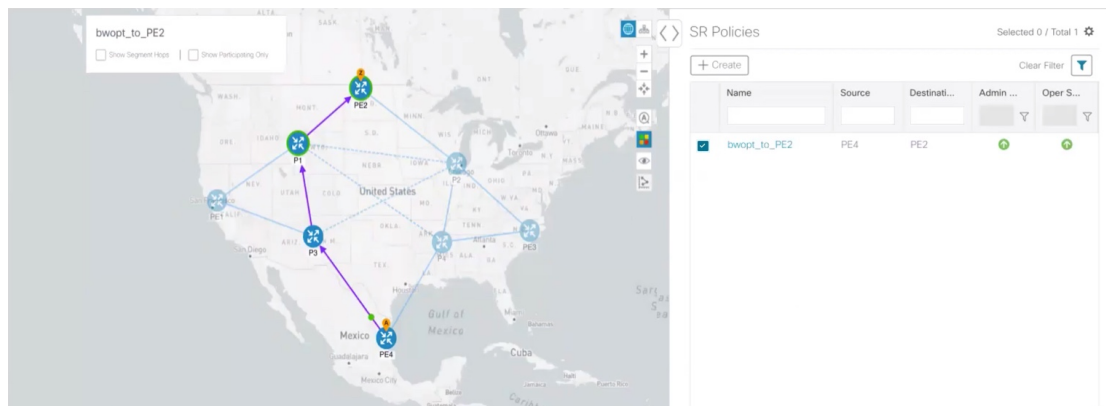
Suppose links between P3 and P4 devices go down. Traffic moves towards other links causing congestion and exceeds the utilization threshold set in Bandwidth Optimization.

**Figure 51: Example: Links Go Down Between P3 and P4**



Bandwidth Optimization recognizes the congestion and immediately calculates and deploys a tactical SR policy. This new tactical SR policy is listed in the **SR Policies** window.

**Figure 52: Example: Tactical SR Policy Deployed**



Cisco Crosswork Optimization Engine continually monitors the network. When the links between P3 and P4 are back up, Cisco Crosswork Optimization Engine will detect that the congestion (based on the criteria set in Bandwidth Optimization) has been mitigated. When the congestion falls under the set utilization threshold minus the utilization hold margin, the tactical SR policy is automatically removed from the network by Bandwidth Optimization.

## Troubleshoot BWOpt

BWOpt disables itself and issues an alarm when specific error conditions occur that hinder its ability to manage congestion properly and may lead to instability. The following table defines some of these conditions and possible causes to investigate. Additional details can be obtained for each error condition by referring to the BWOpt logs.

Table 15: Errors

| Error Event Message                   | Possible Causes and Recommended Corrective Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Optima Engine model error             | <p>The network model used by BWOpt from the Optimization Engine is corrupt or is missing key data that is needed to properly support BWOpt. Possible causes include network discovery issues or synchronization problems between the Optimization Engine and Topology Services. Try restarting the Optimization Engine pod to rebuild the model.</p> <p>This error can also occur if the time required to deploy a tactical policy through SR-PCE, discover it, and add it to the model exceeds the <b>Deployment Timeout</b> option set for BWOpt. The default is 30 seconds which should suffice for small to medium sized networks. However, larger networks may require additional time.</p> |
| PCE Dispatch unreachable              | <p>The deployment of a tactical policy to the network is not confirmed successful before the <b>Deployment Timeout</b> is exceeded. Increase the <b>Deployment Timeout</b> option to allow for additional time for deployments in larger networks.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Unable to deploy a tactical SR policy | <p>A tactical SR policy deployment to SR-PCE was unsuccessful. There could be a variety of reasons for this. BWOpt and/or PCE Dispatch logs can provide some guidance as to the details of the failure. Confirm basic SR policy provisioning capability to the PCC via one of the SR-PCE providers is working.</p>                                                                                                                                                                                                                                                                                                                                                                               |