



# Extreme Visibility Manager Administration and User Guide

6.0.0

9037082-00 Rev AA  
June 2021



Copyright © 2021 Extreme Networks, Inc. All rights reserved.

## Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

## Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: [www.extremenetworks.com/company/legal/trademarks](http://www.extremenetworks.com/company/legal/trademarks)

## Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: <https://www.extremenetworks.com/support/policies/open-source-declaration/>



# Table of Contents

---

<b>Preface.....</b>	<b>6</b>
Text Conventions.....	6
Documentation and Training.....	7
Getting Help.....	8
Subscribe to Product Announcements.....	8
Providing Feedback.....	8
<b>What's New In This Document.....</b>	<b>10</b>
<b>Getting Started.....</b>	<b>11</b>
Extreme Visibility Manager Functions.....	11
Packet Broker Functions.....	13
Visibility Manager Deployment Model.....	14
Visibility Manager Microservices.....	17
Supported Devices.....	20
Log in to Visibility Manager.....	20
The User Interface.....	21
Typical Device Configuration Workflow.....	23
The Library.....	23
<b>Managing the System.....</b>	<b>25</b>
Verify the System and Services.....	25
Microservice Logs.....	27
View System Logs.....	27
View User Logs.....	28
User Roles.....	29
Add a User.....	30
Change a Password.....	30
Change a User Role.....	30
Delete a User.....	31
View the Logged-In User.....	31
<b>Managing Device Types and Versions.....</b>	<b>32</b>
Device Types and Versions.....	32
Add a Device Type File.....	33
Delete a Device Type File.....	33
View Device Type Files.....	33
<b>Managing Devices.....</b>	<b>34</b>
Add Devices.....	34
Create a Device Definition File.....	35
Delete a Device.....	36
Export the Configuration of SLX and MLX Devices.....	36
Refresh Device Configuration.....	36

Persist the Configuration of SLX and MLX Devices.....	36
Configure Packet Capture on the Extreme 9920.....	37
Clear Device Counters.....	37
Search, Group, and Sort Devices.....	38
Device Credentials.....	39
<b>Monitoring Device Health and Statistics.....</b>	<b>40</b>
Supported Device and Health Statistics.....	40
Device statistics.....	40
Device health management .....	41
View Statistics in a Device Dashboard.....	41
Create and Populate a Custom Dashboard.....	43
View Events in Device Logs.....	43
<b>Managing Device Ports and Port Channels.....</b>	<b>45</b>
Create a Port Channel.....	45
Change a Port Channel.....	46
Delete a Port Channel.....	46
Configure Port Properties.....	47
<b>Managing Egress.....</b>	<b>48</b>
Create an Egress.....	48
Change an Egress.....	49
Delete an Egress .....	49
<b>Managing Egress Groups.....</b>	<b>50</b>
Create an Egress Group.....	50
Change an Egress Group.....	50
Delete an Egress Group.....	51
<b>Managing Ingress Groups.....</b>	<b>52</b>
Create an Ingress Group.....	52
Change an Ingress Group.....	53
Delete an Ingress Group.....	53
<b>Managing Policy Rule Matches.....</b>	<b>54</b>
Create a Policy Rule Match for a Device.....	54
Create a Policy Rule Match in the Library.....	56
Change a Policy Rule Match.....	56
Import a Policy Rule Match to a Device.....	57
Export a Policy Rule Match.....	57
Clone a Policy Rule Match.....	57
Delete a Policy Rule Match.....	58
Search Policy Rule Matches.....	58
<b>Managing Policies.....</b>	<b>59</b>
Create an Egress Policy for a Device.....	59
Create an Ingress Policy for a Device.....	60
Create a Policy in the Library.....	61
Change a Policy.....	61
Import a Policy to a Device.....	62
Export a Policy.....	62
Clone a Policy.....	63

Delete a Policy.....	63
Search Policies.....	63
<b>Managing User-Defined ACLs.....</b>	<b>65</b>
Create a UDA.....	65
Change a UDA.....	65
Clone a UDA.....	66
Delete a UDA.....	66
Search UDAs.....	66
<b>Managing Tunnels.....</b>	<b>67</b>
Create a Tunnel.....	67
Change a Tunnel.....	68
Delete a Tunnel.....	68
<b>Managing Locations.....</b>	<b>69</b>
Upload a Location Definition File.....	69
Search Locations.....	69
<b>Rule and Functionality Mapping.....</b>	<b>70</b>
MLX to Visibility Manager mapping.....	71
Extreme 9920 to Visibility Manager mapping.....	74
SLX to Visibility Manager mapping.....	78



# Preface

---

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.






## Text Conventions

---

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as ExtremeSwitching switches or SLX routers, the product is referred to as *the switch* or *the router*.

**Table 1: Notes and warnings**

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

**Table 2: Text**

Convention	Description
screen displays	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words <i>enter</i> and <i>type</i>	When you see the word <i>enter</i> in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says <i>type</i> .
<b>Key</b> names	Key names are written in boldface, for example <b>Ctrl</b> or <b>Esc</b> . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press <b>Ctrl+Alt+Del</b>
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
<b>NEW!</b>	New information. In a PDF, this is searchable text.

**Table 3: Command syntax**

Convention	Description
<b>bold</b> text	Bold text indicates command names, keywords, and command options.
<i>italic</i> text	Italic text indicates variable content.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ <b>x</b>   <b>y</b>   <b>z</b> }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
<b>x</b>   <b>y</b>	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <i>member</i> [ <i>member</i> . . .].
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

## Documentation and Training

Find Extreme Networks product information at the following locations:

[Current Product Documentation](#)

[Release Notes](#)

[Hardware and software compatibility](#) for Extreme Networks products

[Extreme Optics Compatibility](#)

[Other resources](#) such as white papers, data sheets, and case studies

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit [www.extremenetworks.com/education/](http://www.extremenetworks.com/education/).

---

## Getting Help

---

If you require assistance, contact Extreme Networks using one of the following methods:

### Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

### The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

### Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2826. For the support phone number in your country, visit: [www.extremenetworks.com/support/contact](http://www.extremenetworks.com/support/contact)

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

## Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to [The Hub](#).
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

---

## Providing Feedback

---

The Information Development team at Extreme Networks has made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.



- Improvements that would help you find relevant information in the document.
- Broken links or usability issues.

If you would like to provide feedback, you can do so in three ways:

- In a web browser, select the feedback icon and complete the online feedback form.
- Access the feedback form at <https://www.extremenetworks.com/documentation-feedback/>.
- Email us at [documentation@extremenetworks.com](mailto:documentation@extremenetworks.com).

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.



## What's New In This Document

---

Extreme Visibility Manager 6.0.0 differs from previous releases in that it has a new architecture and a new user interface. This document is new for this release.

For information about the features in this release, see the [Extreme Visibility Manager Release Notes, 6.0.0](#).



# Getting Started

---

- [Extreme Visibility Manager Functions](#) on page 11
- [Packet Broker Functions](#) on page 13
- [Visibility Manager Deployment Model](#) on page 14
- [Visibility Manager Microservices](#) on page 17
- [Supported Devices](#) on page 20
- [Log in to Visibility Manager](#) on page 20
- [The User Interface](#) on page 21
- [Typical Device Configuration Workflow](#) on page 23
- [The Library](#) on page 23

The topics in this section describe functions, accessibility, and navigation.

## Extreme Visibility Manager Functions

---

Extreme Visibility Manager (Visibility Manager), a Kubernetes-based microservices application, provides centralized device and policy management as part of the Extreme Visibility solution.

Visibility Manager supports several network packet broker devices. Although devices have different functionality and different configuration methods, Visibility Manager seamlessly interacts with all supported devices for simplified management.

You use Visibility Manager to perform much of the same traffic configuration that you might otherwise perform from the command-line interface of your network packet broker operating system. And then you use Visibility Manager to analyze the traffic for insight into issues such as network usage, load-balancing irregularities, and security threats. For more information, see [Packet Broker Functions](#) on page 13.

Visibility Manager managed objects work together to accomplish most packet broker functions. You configure these objects from the user interface.

**Table 4: Managed objects**

Object	Description
Ports and port channels	The interfaces on which traffic enters and exits the packet broker device. You can associate ports and port channels with ingress groups and egress. For more information, see <a href="#">Create a Port Channel</a> on page 45 and <a href="#">Configure Port Properties</a> on page 47.
Egress	A port or port channel that you associate with an egress policy, which identifies the actions to take on egress traffic. For more information, see <a href="#">Create an Egress</a> on page 48.
Egress group	A set of interfaces and ports on which traffic is forwarded after a policy is applied. For more information, see <a href="#">Create an Egress Group</a> on page 50.
Ingress group	A collection of ports, port channels, and tunnels on which monitored traffic is received. You can select several actions to perform on the incoming traffic and you can associate the ingress group with an ingress policy. For more information, see <a href="#">Create an Ingress Group</a> on page 52.
Policy rule matches	The parts of a packet header that a rule targets, such as the source port or the payload length. One or more rules constitute a match. You associate matches with ingress or egress policies. For more information, see <a href="#">Create a Policy Rule Match for a Device</a> on page 54.
Ingress policy (or route map)	The actions to apply to inbound packets. You can associate policy rule matches and egress groups, and select other actions such as packet slicing and scope shift. For more information, see <a href="#">Create an Ingress Policy for a Device</a> on page 60.
Egress policy (or listener policy)	The actions to apply to outbound packets. You can associate policy rule matches and select other actions such as packet slicing and header stripping. For more information, see <a href="#">Create an Egress Policy for a Device</a> on page 59.

**Table 4: Managed objects (continued)**

Object	Description
User-defined access list (UDA)	The rules and matches created for or reconciled from MLX devices. For more information, see <a href="#">Create a UDA</a> on page 65.
Transport tunnel termination and encapsulation	The GRE or ERSPAN tunnels to associate with ingress groups or egress. For more information, see <a href="#">Create a Tunnel</a> on page 67.

## Packet Broker Functions

A network packet broker aggregates network traffic from multiple ports for forwarding to analysis applications.

When a packet broker is attached to networking devices, a copy of the traffic that passes through the devices is sent to the packet broker. Based on your configuration, the packet broker filters the copied traffic for the data that you want to analyze. The broker then sends the filtered traffic to an analysis application.

In general, packet brokers can perform the following types of actions on copied network traffic.

**Table 5: Packet broker functions**

Function	Description
ACL filtering	Directs network traffic based on Layer 2 to Layer 4 protocol headers
Aggregation	Combines traffic that from multiple ports and directs it to one port or port channel
Decapsulation	Removes the outer tunnel headers from a packet
Header stripping	Removes header tags that are not supported by some visibility applications, including 802.1BR, VN (virtual NIC), VLAN, VXLAN, GTPU, GRE, and IPIP headers
Load balancing	Distributes network traffic among ports in a port channel
Packet slicing	Filters packet headers for the header components that you want to target. For a list of such components, see <a href="#">Create a Policy Rule Match for a Device</a> on page 54.
Replication	Copies network traffic to multiple ports and port channels
Route map forwarding	Redirects Layer 2 and Layer 3 packets to the selected physical or port channel interface

**Table 5: Packet broker functions (continued)**

Function	Description
Transport tunnel termination	<ul style="list-style-type: none"><li>• <b>GRE</b> (Generic Routing Encapsulation). Creates a tunnel that encapsulates (or wraps) packets that use one type of protocol inside packets that use a different protocol.</li><li>• <b>ERSPAN</b> (Encapsulated Remote Switched Port Analyzer): Creates a tunnel that mirrors traffic from source ports for delivery to destination ports on a different device.</li></ul>
Transport tunnel encapsulation	GRE only

## Visibility Manager Deployment Model

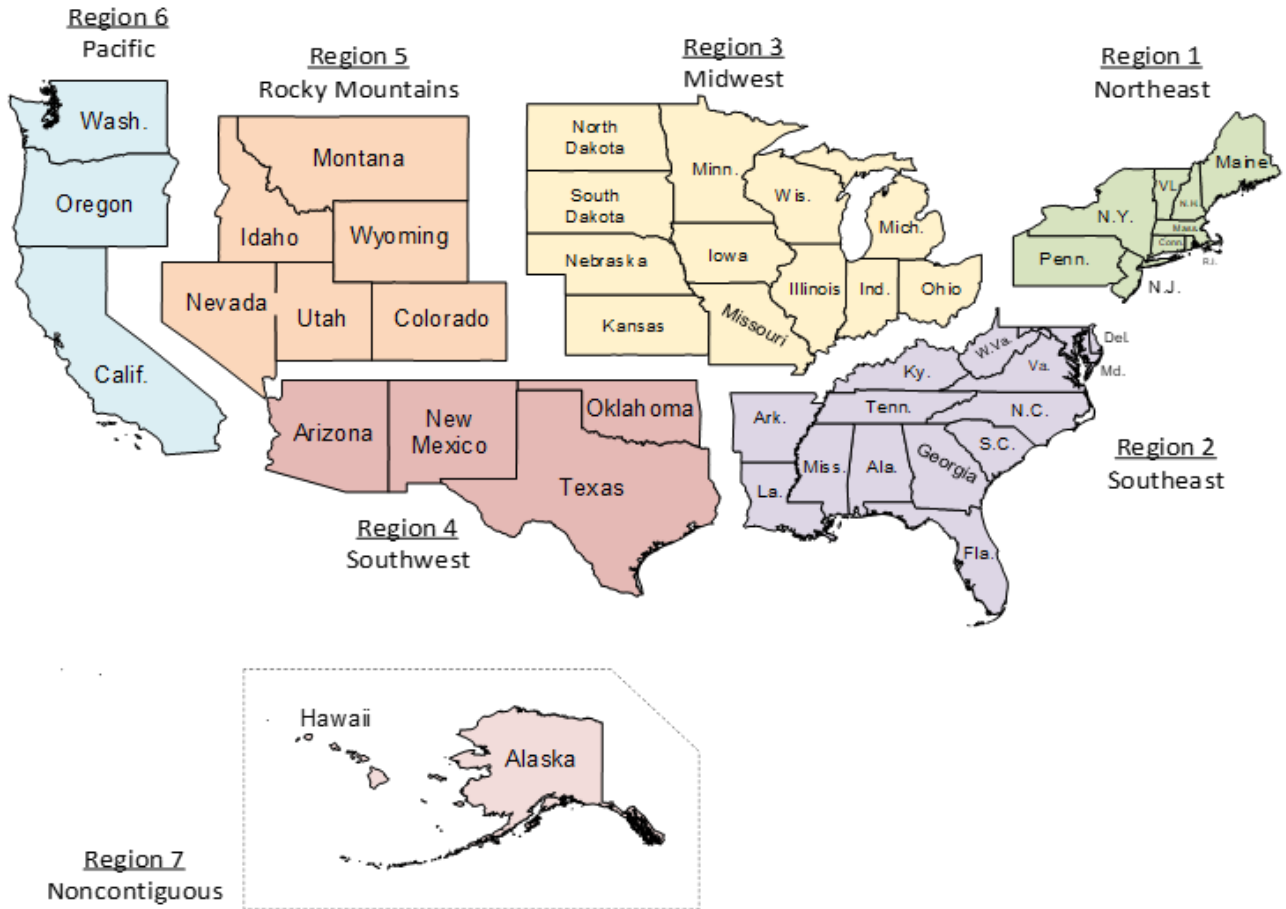
With Visibility Manager, you can manage packet broker devices across multiple data centers and geographic locations.

You can separate your network into regions and further separate regions into zones. A zone is a set of locations (at least one and no more than five) where packet broker devices reside.

**Note**

See the [Extreme Visibility Manager Release Notes, 6.0.0](#) for any limitations on supported regions.

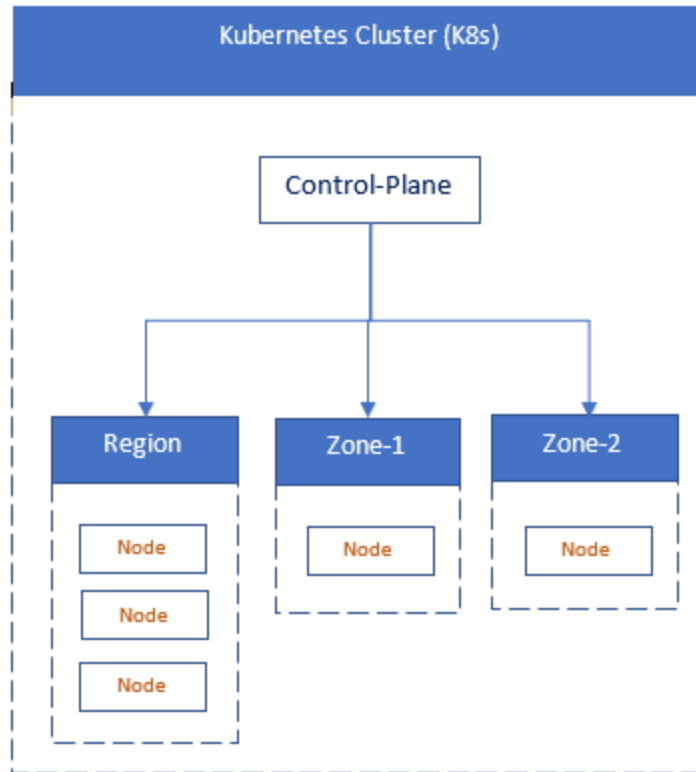
In this example, a map of the United States is separated into seven regions. Each region contains one or more zones. Each zone is a state with a data center.



**Figure 1: Regions and zones**

Each region is a Kubernetes cluster that is managed by a control plane. Having multiple small clusters rather than one large cluster ensures better fault isolation. If one cluster fails, the other clusters provide failover assistance. All clusters are deployed on virtual machines (VMs).

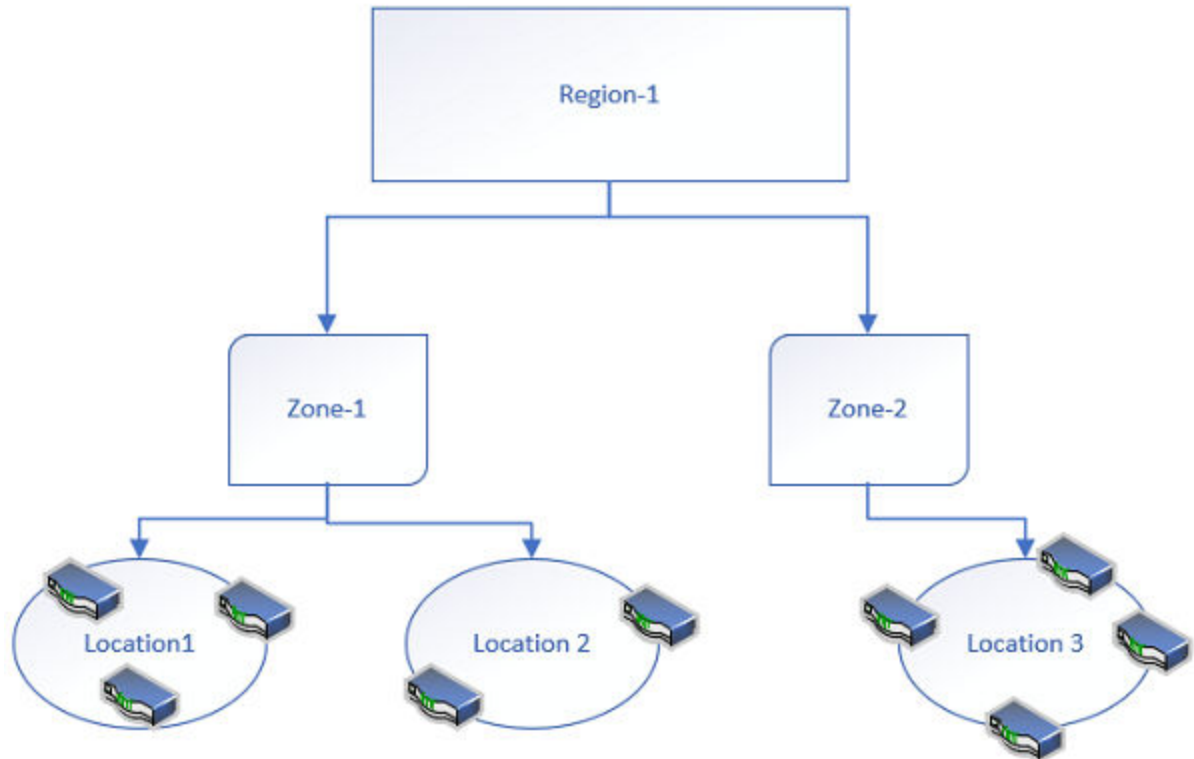
In the following diagram, you can see the Kubernetes cluster, with the control plane, region nodes, and zone nodes.



**Figure 2: Cluster architecture**

In this next diagram, you see how zones can have multiple locations, which tell you where packet broker devices are located.





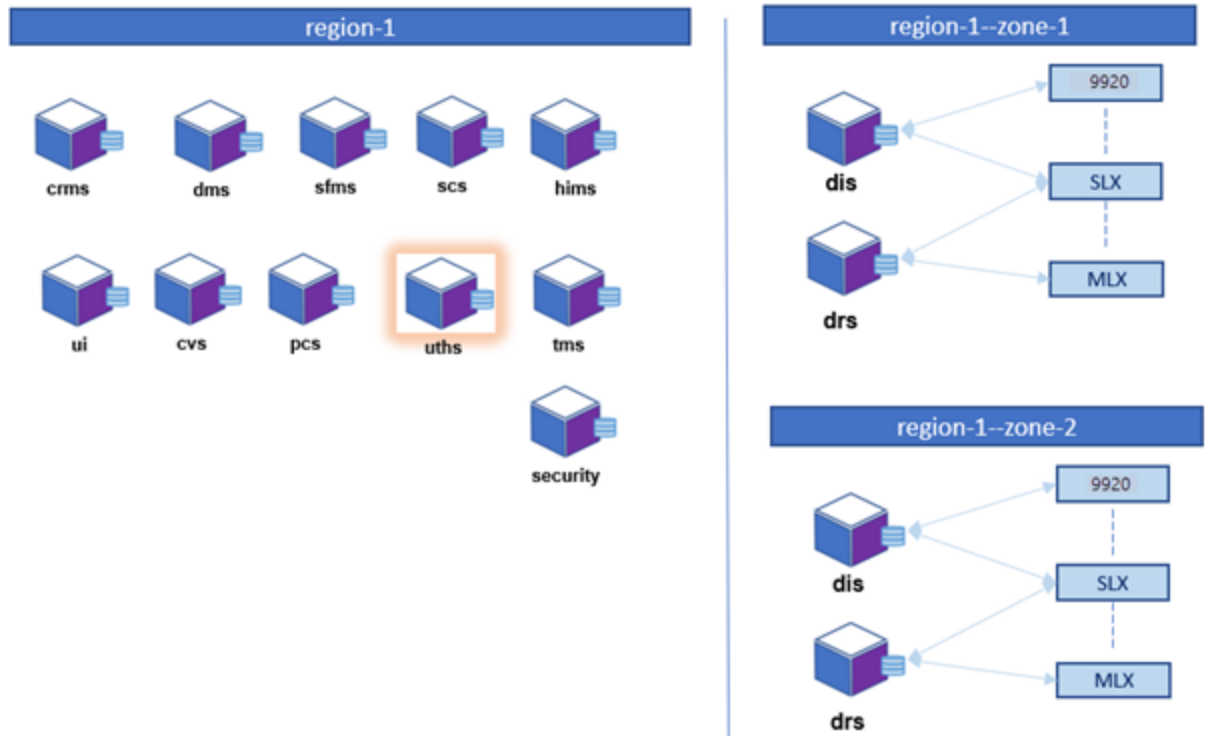
**Figure 3: Zone architecture**

You identify all zones and regions in a CSV file that is incorporated into Visibility Manager during installation. For information about the CSV file and about deploying the control plan, region, and zone VMs, see the [Extreme Visibility Manager Deployment Guide, 6.0.0](#).

## Visibility Manager Microservices

The Visibility Manager microservices work together to provide and control the functionality of the application.

Most of the microservices reside in the region nodes. The DIS and DRS reside in the region and zone nodes and pass information to and from the UTHS.



Logs for each microservice are saved in `/var/log/xvm`. For details, see [Microservice Logs](#) on page 27.

**Table 6: Microservice functions**

Microservice	Description
Cluster Resource Management Service (CRMS)	<ul style="list-style-type: none"> <li>Manages resources by providing unique identities for devices and configuration</li> <li>Receives REST calls from the CVS to update the DTV message</li> <li>Performs a lookup in the database to verify if the DTV is updated</li> <li>Dynamically deploys microservices the zone nodes</li> <li>Upgrades each microservice in a regional cluster</li> <li>Maintains the location details for all microservices</li> </ul>
Configuration Validate Service (CVS)	Supports basic validation for user interface requests and acts as cache and user interface helper
Device Health and Incident Management Service (DHMS)	Monitors and persists device states by collecting syslogs and RASlogs from devices

**Table 6: Microservice functions (continued)**

Microservice	Description
Device Interface Service (DIS)	<ul style="list-style-type: none"> <li>• Manages a site and the devices in that site</li> <li>• Establishes connections with devices</li> <li>• Retrieves and pushes configuration</li> <li>• Streams statistics and events</li> </ul>
Device and Zone Management Service (DMS)	<ul style="list-style-type: none"> <li>• Acts as a gateway between region and zone nodes</li> <li>• Directs messages to the correct zone based on device location</li> <li>• Manages devices on different zones for a region</li> <li>• Receives information about device types, versions, and site details</li> <li>• Maintains a private database to persist device type, device version, and device information</li> </ul>
Device Receive Service (DRS)	<ul style="list-style-type: none"> <li>• Hosts the syslog server and streams syslog messages to the DHMS</li> <li>• Receives telemetry streams from SLX devices and forwards them to the SCS for processing</li> </ul>
Policy Control Service (PCS)	Maintains a library of policies and ACLs that can be reused across multiple devices
Security	Supports the following: <ul style="list-style-type: none"> <li>• Authentication and authorization for secure access of APIs</li> <li>• Local user management</li> <li>• TLS</li> <li>• Local authorization</li> <li>• Certificate management</li> </ul>
Service Function Management Service (SFMS)	<ul style="list-style-type: none"> <li>• Manages and persists device configuration</li> <li>• Intelligently derives service chains for Extreme 9920 devices</li> </ul>
Statistics Collection Service (SCS)	Collects and persists statistics from devices for various device configuration and on physical ports
Transaction Management Service (TMS)	<ul style="list-style-type: none"> <li>• Manages distributed transactions</li> <li>• Ensures consistency of transactions across services</li> <li>• Creates a transaction for every user request</li> <li>• Forwards requests to the DMS</li> </ul>

**Table 6: Microservice functions (continued)**

Microservice	Description
User Interface (UI)	Provides access and functionality for managing and monitoring devices
User Transaction History Service (UTHS)	<ul style="list-style-type: none"> <li>• Maintains user transaction histories for audit trails on user activity</li> <li>• Provides progress on user actions through the Notification service in the user interface</li> <li>• Receives user transaction information from the DIS and the DRS</li> </ul>

## Supported Devices

Extreme Visibility Manager supports several devices and their software.

**Table 7: Supported devices and software**

Device	Supported Software
Extreme 9920	Extreme 9920 software, version 21.1.0.0, with the NPB application
ExtremeRouting MLX series	NetIron 06.3.00d
ExtremeSwitching SLX 9140	SLX-OS 18s.1.03a, SLX-OS 18s.1.03b
ExtremeSwitching SLX 9240	SLX-OS 18s.1.03a, SLX-OS 18s.1.03b

## Log in to Visibility Manager

You access Extreme Visibility Manager from a supported web browser, either Chrome or Firefox.

### Procedure

1. Navigate to the interface at `http://<ip-addr of controlplane node>/login`.
2. Complete the **Username** and **Password** fields.

The default credentials are as follows:

**Username:** admin

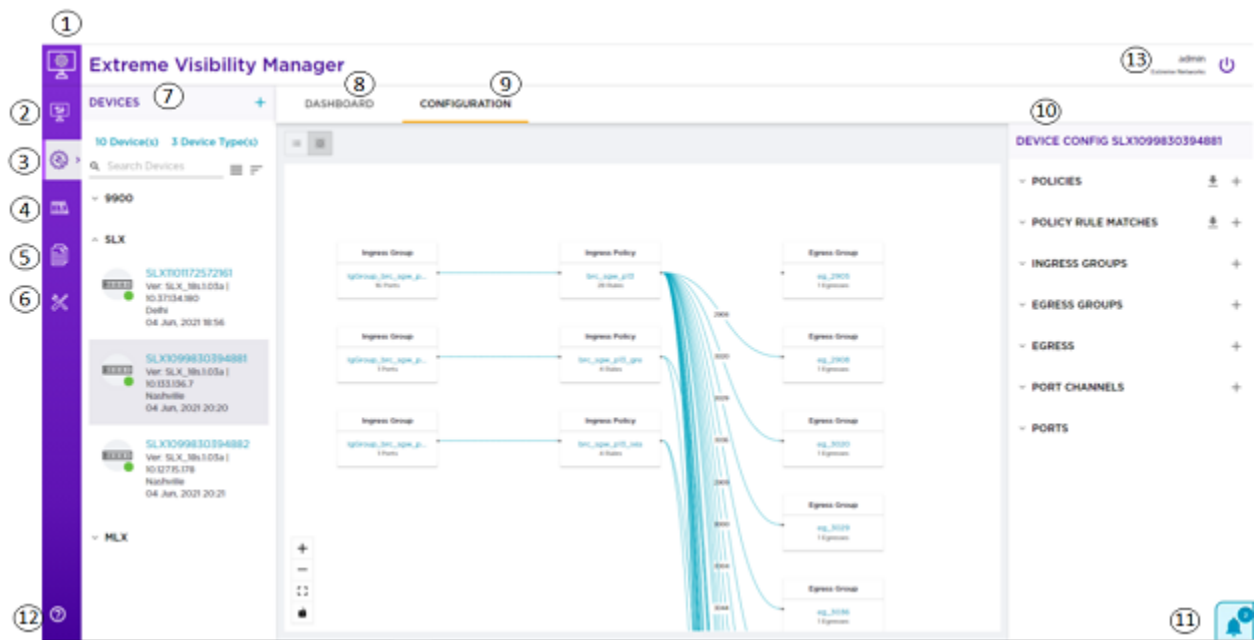
**Password:** password

3. Select **Login**.

If this is your first time logging in, you are prompted to add device types and devices. Otherwise, the user interface opens to the Configure page.

## The User Interface

The Extreme Visibility Manager interface provides access to all system functions.



**Figure 4: User interface**

**Table 8: User interface descriptions**

Legend	Interface Area	Description
1	Navigation menu	Provides access to all pages of the interface.
2	Dashboard page	Provides access to custom dashboards that you create from the built-in reports on the <b>Dashboard</b> tab.
3	Configure page	Provides access to the Devices pane, the Dashboard and Configuration tabs, the Config menu, and configuration notifications.
4	Library page	Provides access to all configured matches, policies, and UDA (User-Defined ACLs). From here, you can add matches and policies, export them, clone them, edit them, and delete them.
5	System Logs page	Provides access to information about all system logs, including device ID, IP address, and current and previous values.

**Table 8: User interface descriptions (continued)**

Legend	Interface Area	Description
6	Settings page	Provides access to settings for users, profile, and location. From here, you can perform the following tasks: <ul style="list-style-type: none"> <li>• Add and delete users</li> <li>• Update user passwords</li> <li>• View the logged-in user</li> <li>• Add location definition files</li> </ul>
7	Devices pane	Displays the list of all discovered devices. From here, you can perform the following tasks: <ul style="list-style-type: none"> <li>• Add devices and device types</li> <li>• Sort and group devices</li> <li>• Export and refresh device configurations</li> <li>• View device logs</li> <li>• Clear device counters</li> <li>• Configure packet captures</li> <li>• Persist the configuration of SLX and MLX devices</li> </ul>
8	Dashboard tab	Provides access to device-specific, real-time statistics for interfaces, policies, and system usage.
9	Configuration tab	Provides a graphical representation of the relationship between groups and policies for the selected device (also known as a <i>service chain</i> ). Is displayed in the interface after a device configuration is reconciled.
10	Device Config menu	Provides access to all configuration settings for the selected device. From here, you can perform the following tasks: <ul style="list-style-type: none"> <li>• Change port properties</li> <li>• Manage port channels</li> <li>• Manage policy rule matches</li> <li>• Manage egress groups and policies</li> <li>• Manage ingress groups and policies</li> <li>• Manage tunnels</li> </ul> Is displayed in the interface after you discover a device.
11	Notifications	Displays a list of confirmation and error notifications for every configuration action you perform.

**Table 8: User interface descriptions (continued)**

Legend	Interface Area	Description
12	Help	Provides access to version information and help for the application.
13	Logout	Logs the current user out of the application.

## Typical Device Configuration Workflow

Configure your devices in the order shown, so that information from one task is available to select in a subsequent task.

**Table 9: Configuration workflow**

Configuration task	Described in
Add the Device Type Version Capability (DTVC) file	<a href="#">Add a Device Type File</a> on page 33
Add devices	<a href="#">Add Devices</a> on page 34
Add port channels and configure ports	<a href="#">Create a Port Channel</a> on page 45 <a href="#">Configure Port Properties</a> on page 47
Add egress	<a href="#">Create an Egress</a> on page 48
Add egress groups and ingress groups	<a href="#">Create an Egress Group</a> on page 50 <a href="#">Create an Ingress Group</a> on page 52
Add policy rule matches	<a href="#">Create a Policy Rule Match for a Device</a> on page 54
Add policies	<a href="#">Create an Egress Policy for a Device</a> on page 59 <a href="#">Create an Ingress Policy for a Device</a> on page 60
Add tunnels	<a href="#">Create a Tunnel</a> on page 67

## The Library

The library provides access to policy rule matches, policies, and user-defined ACLs (UDAs, for MLX devices only).

Matches and rules from managed devices are imported to the library for use by other devices.

### Matches

Policy rule matches in the library can be imported as needed to one or more devices. On the Matches page, you can see matches and their associated device type, rule type, and number of rules.

For every match in the library, you have easy access to several functions: create, export, clone, edit, delete, and search. For more information, see the following topics.

- [Create a Policy Rule Match in the Library](#) on page 56
- [Change a Policy Rule Match](#) on page 56
- [Export a Policy Rule Match](#) on page 57

- [Clone a Policy Rule Match](#) on page 57
- [Delete a Policy Rule Match](#) on page 58
- [Search Policy Rule Matches](#) on page 58

## Policies

Policies in the library can be imported as needed to one or more devices. On the Policies page, you can see policies and their associated device type, rule type, and number of rules.

For every policy in the library, you have easy access to several functions: create, export, clone, edit, delete, and search. For more information, see the following topics.

- [Create a Policy in the Library](#) on page 61
- [Change a Policy](#) on page 61
- [Export a Policy](#) on page 62
- [Clone a Policy](#) on page 63
- [Delete a Policy](#) on page 63
- [Search Policies](#) on page 63

## UDA

The UDAs in the library represent rules and matches from reconciled MLX devices. For every UDA in the library, you have easy access to several functions: create clone, edit, delete, and search. For more information, see the following topics.

- [Create a UDA](#) on page 65
- [Change a UDA](#) on page 65
- [Clone a UDA](#) on page 66
- [Delete a UDA](#) on page 66
- [Search UDAs](#) on page 66





# Managing the System

---

[Verify the System and Services](#) on page 25

[Microservice Logs](#) on page 27

[View System Logs](#) on page 27

[View User Logs](#) on page 28

[User Roles](#) on page 29

[Add a User](#) on page 30

[Change a Password](#) on page 30

[Change a User Role](#) on page 30

[Delete a User](#) on page 31

[View the Logged-In User](#) on page 31

The topics in this section describe how and when to perform system-related functions such as managing users, viewing logs, and verifying the running system.

## Verify the System and Services

---

You can verify the status of the Visibility Manager system and services with four simple commands.

### **About This Task**

Take the following steps on the node that you want to verify.

## Procedure

1. Verify that all system pods are in Running state.

```
# kubectl get pods -A
```

NAMESPACE	NAME	READY	STATUS	RESTARTS	AGE
kube-system	calico-kube-controllers-6fc78cbdf6-w82kf	1/1	Running	0	41d
kube-system	calico-node-2sn2t	1/1	Running	0	41d
kube-system	calico-node-4kc5f	1/1	Running	0	41d
kube-system	calico-node-8nnwv	1/1	Running	0	41d
kube-system	calico-node-kxwk6	1/1	Running	0	41d
xvm	ms-db-1	2/2	Running	0	21d
xvm	ms-db-2	2/2	Running	0	21d
xvm	msgbus-5966d4fc6d-rg4xc	1/1	Running	0	14d
xvm	pcs-ms-56994db6c5-qf8hb	1/1	Running	0	14d
xvm	scs-ms-7d6856ff94-h4rrx	1/1	Running	0	62s
xvm	security-ms-68869cc69b-kccqx	1/1	Running	0	14d
xvm	sfms-ms-57d68dbc9f-4hkvw	1/1	Running	0	14d
xvm	tms-ms-6f65655c46-rt7jd	1/1	Running	0	14d
xvm	traefik-ingress-controller-65b5b58475-hkcdq	1/1	Running	0	14d
xvm	ui-ms-697c6c8899-z6pcn	1/1	Running	0	14d
xvm	uths-ms-555c86f8f4-h9xxj	1/1	Running	0	14d
xvm	zookeeper-deployment-1-7854cf76d-xb5xg	1/1	Running	0	14d

2. Verify that the microservices are present on the node.

```
# kubectl get svc -A
```

NAMESPACE	NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
default	kubernetes	ClusterIP		<none>	443/TCP	41d
kube-system	kube-dns	ClusterIP		<none>	53/UDP,53/TCP,9153/TCP	41d
xvm	crms-svc	ClusterIP		<none>	8090/TCP	14d
xvm	cvs-svc	ClusterIP		<none>	9000/TCP	14d
xvm	dhms-db-svc	ClusterIP		<none>	27017/TCP	14d
xvm	dhms-rest-svc	ClusterIP		<none>	9035/TCP,9030/TCP	14d
xvm	dhms-db-svc	ClusterIP	None	<none>	5000/TCP	14d
xvm	dis-east-zone-svc	LoadBalancer			9010:30136/TCP	14d
xvm	disdb-east-zone-svc	ClusterIP		<none>	27017/TCP	14d
xvm	das-svc	ClusterIP		<none>	9020/TCP	14d
xvm	drs-east-zone-svc	LoadBalancer			514:31646/UDP	21d
xvm	drs-telemetry-east-zone-svc	LoadBalancer			54322:31639/TCP	21d
xvm	eventstore-svc	ClusterIP		<none>	2113/TCP,2112/TCP,1113/TCP,1112/TCP	14d
xvm	kafka	ClusterIP		<none>	9092/TCP	14d
xvm	ms-db-svc	ClusterIP	None	<none>	27017/TCP	21d
xvm	msgbus-svc	ClusterIP		<none>	4222/TCP	14d
xvm	pcs-svc	ClusterIP		<none>	9050/TCP	14d
xvm	scs-rest-svc	ClusterIP		<none>	9060/TCP,9065/TCP	14d
xvm	scsts-db-svc	ClusterIP	None	<none>	5000/TCP	14d
xvm	security-db-svc	ClusterIP	None	<none>	5000/TCP	14d
xvm	security-svc	ClusterIP		<none>	9080/TCP	14d
xvm	sfms-svc	ClusterIP		<none>	9040/TCP	14d
xvm	tms-rest-svc	ClusterIP		<none>	8080/TCP,8081/TCP	14d
xvm	traefik-ingress-service	LoadBalancer		10.2.1.10.70	80:32529/TCP,443:31909/TCP,8080:32636/TCP	14d
xvm	ts-db-svc	ClusterIP	None	<none>	5000/TCP	14d
xvm	ui-svc	ClusterIP		<none>	3000/TCP	14d
xvm	uths-rest-svc	ClusterIP		<none>	9070/TCP,9071/TCP	14d
xvm	zookeeper-svc	ClusterIP		<none>	2181/TCP,2888/TCP,3888/TCP	14d

3. Verify that persistent volumes are in Bound state.

```
# kubectl get pv
```

NAME	CAPACITY	ACCESS MODES	RECLAIM POLICY	STATUS	CLAIM	STORAGECLASS	REASON	AGE
evm-persistent-volume	100Mi	RWO	Retain	Bound	xvm/evm-persistent-volumeclaim	evm-pv		14d
ms-db-storage-0	20Gi	RWO	Retain	Bound	xvm/pv-data-ms-db-0	evm-cs-pv-0		21d
ms-db-storage-1	20Gi	RWO	Retain	Bound	xvm/pv-data-ms-db-1	evm-cs-pv-1		21d
ms-db-storage-2	20Gi	RWO	Retain	Bound	xvm/pv-data-ms-db-2	evm-cs-pv-2		21d
my-local-pv	100Mi	RWX	Retain	Bound	xvm/my-claim	my-local-storage		14d

4. Verify that persistent volume claims are in Bound state.

```
# kubectl get pvc -n xvm
NAME                                STATUS  VOLUME                CAPACITY  ACCESS MODES  STORAGECLASS  AGE
evm-persistent-volumeclaim         Bound  evm-persistent-volume  100Mi     RWO           evm-pv        14d
my-claim                           Bound  my-local-pv           100Mi     RWX           my-local-storage  14d
pv-data-ms-db-0                   Bound  ms-db-storage-0       20Gi     RWO           evm-cs-pv-0     21d
pv-data-ms-db-1                   Bound  ms-db-storage-1       20Gi     RWO           evm-cs-pv-1     21d
pv-data-ms-db-2                   Bound  ms-db-storage-2       20Gi     RWO           evm-cs-pv-2     21d
```

## Microservice Logs

Logs for each microservice are saved in `/var/log/xvm`.



**Tip**

To collect the logs for a particular microservice, first determine which node is running. Then you can find the logs on the running node at the file paths noted in the following table. You can run the `kubect1 get pods -n xvm -o wide` command to find the running node.

**Table 10: Microservice descriptions**

Microservice	Log File Path
Cluster Resource Management Service (CRMS)	<code>/var/log/xvm/crms-ms/*</code>
Configuration Validate Service (CVS)	<code>/var/log/xvm/cvs-ms/*</code>
Device Health and Incident Management Service (DHMS)	<code>/var/log/xvm/dhms-ms/*</code>
Device Interface Service (DIS)	<code>/var/log/xvm/dis-ms/*</code>
Device and Zone Management Service (DMS)	<code>/var/log/xvm/dms-ms/*</code>
Device Receive Service (DRS)	<code>/var/log/xvm/drs-ms/*</code>
Policy Control Service (PCS)	<code>/var/log/xvm/pcs-ms/*</code>
Security	<code>/var/log/xvm/security-ms/*</code>
Service Function Management Service (SFMS)	<code>/var/log/xvm/sfms-ms/*</code>
Statistics Collection Service (SCS)	<code>/var/log/xvm/scs-ms/*</code>
Transaction Management Service (TMS)	<code>/var/log/xvm/tms-ms/*</code>
User Transaction History Service (UTHS)	<code>/var/log/xvm/uths-ms/*</code>

## View System Logs

You can view system logs to understand the status of monitored Extreme 9920 devices.

**About This Task**

System logs, based on gNMI notifications, provide the following information:

- IP address
- Name

- Current and previous states, such as online, offline, or degraded (which indicates that at least one microservice is not in a Running state)
- Date

### Procedure

In the Navigation menu, select **Logs > System**.

## View User Logs

You can view user logs to understand the transactions that a user has performed.

### About This Task

Visibility Manager offers three types of logs related to user transactions: Device, Device Config, and Device Type. These logs provide the following information.

**Table 11: User logs**

Log Type	Information Provided
Device	<ul style="list-style-type: none"> <li>• Action, such as delete or discover a device</li> <li>• IP address</li> <li>• Name</li> <li>• Device type version</li> <li>• Location</li> <li>• Status, such as success or failed</li> <li>• Error message to explain a failure</li> <li>• Date</li> </ul>
Device Config	<ul style="list-style-type: none"> <li>• Action, such as add, update, or delete a configuration</li> <li>• IP address</li> <li>• Name</li> <li>• Type, such as policy match or port channel</li> <li>• Status, such as success or failed</li> <li>• Error message to explain a failure</li> <li>• Date</li> </ul>
Device Type	<ul style="list-style-type: none"> <li>• Action, such as add, update, or delete a DTVC file</li> <li>• Device type</li> <li>• Device type version</li> <li>• Location</li> <li>• Status, such as success or failed</li> <li>• Error message to explain a failure</li> <li>• Date</li> </ul>

### Procedure

1. In the Navigation menu, select **Logs > User**.
2. To view user transactions on devices, select **Device**.

3. To view user transactions related to configuration, select **Device Config**.
4. To view user transactions related to device types, select **Device Type**.

## User Roles

Role-based Access Control (RBAC) determines which functions a user can perform, based on the user's role.

**Table 12: Role definitions**

Role	Functions
System Admin	<p>Users with this role have complete privileges to perform all operations in the system. Privileges include the following:</p> <ul style="list-style-type: none"> <li>• Add and view device types and devices</li> <li>• Add and view device configuration and DTVC files</li> <li>• Add and view custom dashboards</li> <li>• Configure and View built-in dashboards</li> <li>• Add and view users</li> <li>• Change user passwords</li> <li>• Change user roles</li> <li>• View location details</li> <li>• Configure and view the library</li> <li>• View event notifications</li> <li>• Sort device lists</li> </ul> <p>The default Visibility Manager user, admin, has this role.</p>
Network Operator	<p>Users with this role have read-only privileges to all operations in the system, with one exception: logged-in users with this role can change their own passwords. Privileges include the following:</p> <ul style="list-style-type: none"> <li>• View device types and devices</li> <li>• View device configuration and DTVC files</li> <li>• View custom and built-in dashboards</li> <li>• Add and view users</li> <li>• Change own password</li> <li>• View users</li> <li>• View location details</li> <li>• View the library</li> <li>• View event notifications</li> <li>• Sort device lists</li> </ul>

## Add a User

---

Only a user with the System Admin role can add a user.

### Procedure

1. In the Navigation menu, select **Settings > Users**.
2. Select **Add User**.
3. In the **Username** field, enter the user's user name.
4. In the **Password** and **Confirm Password** fields, enter the user's password.
5. In the **Role** field, select **System Admin** or **Network Operator**.

For more information, see [User Roles](#) on page 29.

6. Save (✓) your selections.

## Change a Password

---

Logged-in users can change their own passwords. System Admins can change passwords for all users.

### Procedure

1. (System Admin only) To change any user's password, take the following steps.
  - a. In the Navigation menu, select **Settings > Users**.
  - b. Select **Reset Password** for the relevant user.
  - c. In the **Password** and **Confirm Password** fields, enter the new password.
  - d. Save (✓) your changes.
2. (Logged-in user only) To change your own password, take the following steps.
  - a. In the Navigation menu, select **Settings > Profile**.
  - b. Select **Change Password**.
  - c. In the **Old Password** field, enter the password that you want to change.
  - d. In the **New Password** and **Confirm Password** fields, enter the new password.
  - e. Save (✓) your changes.

## Change a User Role

---

Only a user with the role of System Admin can change the role of another user.

### Procedure

1. In the Navigation menu, select **Settings > Users**.
2. Select **Edit Role** for the relevant user.
3. In the **Role** field, select **System Admin** or **Network Operator**.

For more information, see [User Roles](#) on page 29.

4. Save (✓) your changes.

## Delete a User

---

Only a user with the role of System Admin can delete a user.

### Procedure

1. In the Navigation menu, select **Settings > Users**.
2. Select **Delete User** for the relevant user.

## View the Logged-In User

---

The Profile page identifies the logged-in user.

### Procedure

In the Navigation menu, select **Settings > Profile**.

The user name and role of the logged-in user are displayed.



# Managing Device Types and Versions

---

[Device Types and Versions](#) on page 32

[Add a Device Type File](#) on page 33

[Delete a Device Type File](#) on page 33

[View Device Type Files](#) on page 33

Device types and device type versions information is the basic data that Visibility Manager uses to manage the packet brokers in all of your locations.

The topics in this section explain device types and versions, and show you how to create, add, and delete device type information.

## Device Types and Versions

---

Device types and versions are specified in a Device Type Version Capabilities (DTVC) file, which is an encrypted tar.gz file.

The DTVC file contains all the device type and version information that Visibility Manager needs to manage the related devices. DTVC files for supported devices are included in the `xvm-<version-build>.tar` file from which you extracted the installation files. For more information, see the [Extreme Visibility Manager Deployment Guide, 6.0.0](#).

You can add a DTVC file at any time, and you are prompted to add a DTVC file when you log in to the interface for the first time. For more information, see [Add a Device Type File](#) on page 33.

Visibility Manager propagates the new device type and version information to its database and to all required microservices. Newly added devices are then verified against this collected information. Any device you add must match a device type and version in the database.

Each device type can support one or more device type versions and the capabilities of those versions. Capabilities are generally the features supported by a device.

You can delete a DTVC file, which also deletes the associated versions. This process requires you to remove devices that match the device type versions in the DTVC file you deleted.



---

## Add a Device Type File

---

You can add a device type file at any time, and you are prompted to add one when you log in to the interface for the first time.

### Before You Begin

Obtain the Device Type Version Capabilities (DTVC) file. DTVC files for supported devices are included in the `xvm-<version-build>.tar` file from which you extracted the installation files. For more information, see the [Extreme Visibility Manager Deployment Guide, 6.0.0](#).

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select **Add > Device Types**.
3. Upload the DTVC file in one of the following ways.
  - Drag the file into the **Drag & Drop Device Type-Version Definition** box.
  - Select **Browse** and navigate to the file location.
4. In the **Location** field, select the location associated with the device types in the file you uploaded.
5. Select **Add**.

The device types appear in the Manage Device Types page, which you can see by selecting **Device Types** in the Devices panel.

---

## Delete a Device Type File

---

When you delete a DTVC (Device Type Version Capabilities) file, you delete the device type, all associated versions, and all associated devices.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select **Device Types**.
3. Select one or more DTVC files to delete.
4. Select **Delete**.

---

## View Device Type Files

---

Use the Manage Device Types page to view all uploaded Device Type Version Capabilities (DTVC) files.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select **Device Types**.

The Manage Device Types page displays all uploaded DTVC files and identifies the associated location, discovery protocol, and configuration protocol for each file.



# Managing Devices

---

[Add Devices](#) on page 34

[Create a Device Definition File](#) on page 35

[Delete a Device](#) on page 36

[Export the Configuration of SLX and MLX Devices](#) on page 36

[Refresh Device Configuration](#) on page 36

[Persist the Configuration of SLX and MLX Devices](#) on page 36

[Configure Packet Capture on the Extreme 9920](#) on page 37

[Clear Device Counters](#) on page 37

[Search, Group, and Sort Devices](#) on page 38

[Device Credentials](#) on page 39

The topics in this section describe how to perform device-related tasks such as creating a Device Definition file, adding and deleting devices, refreshing device configurations, enabling packet capture, clearing counters, and creating and viewing dashboards.

## Add Devices

---

You can add devices at any time, and you are prompted to add devices when you log in to the interface for the first time.

### Before You Begin

Upload the Device Type Version Capabilities (DTVC) file associated with the devices you are adding. For more information, see [Add a Device Type File](#) on page 33.

To be able to add multiple devices in bulk, create a Device Definition File, a CSV file that specifies the devices that you want to add. For more information, see [Create a Device Definition File](#).

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select **Add Devices**.
3. To add multiple devices in bulk, upload the CSV file in one of the following ways.
  - Drag the file into the **Drag & Drop Definition File** box.
  - Select **Browse** and navigate to the file location.
4. To add devices one at a time, complete the following fields.
  - a. In the **IP Address** field, enter the IP address of the device.
  - b. In the **Device Type** field, select the DTVC file associated with the device.

- c. In the **Location** field, select the location where the device resides.
  - d. (Optional) To specify credentials for access to the device, select **Additional Fields** and complete the following fields.
    - **Username**, which does not need to be the user name of the default user
    - **Password**
    - **Community String**, which is applicable only for MLX and SLX devices
5. Select **Add**.

## Create a Device Definition File

A Device Definition file (in CSV format) identifies devices by such data as IP address, device type and version, location, and credentials.

### About This Task

You use a Device Definition file to add multiple devices in bulk. The CSV file has the following format, with one row per IP address.

```
<IPAddresses>,<DeviceType>,<DeviceVersion>,<Location>,<ConfigurationProtocol>,<DiscoveryProtocol>,<UserName>,<Password>,<CommunityString>
```

Note the following rules.

- The `IPAddresses` field can contain multiple IP addresses, separated by commas.
- The `DeviceType` field must be one of the following strings: SLX, MLX, or NGNPB.
- The `Location` field must match one of the locations that you specified in the `locations.csv` file. For more information about the `locations.csv` file, see the [Extreme Visibility Manager Deployment Guide, 6.0.0](#).
- The `DeviceVersion` field is the version of the operating system that is installed on the device.
- The `UserName` and `Password` fields are the credentials for accessing the device. These do not need to be the credentials of the default user.
- The `CommunityString` is applicable only for SLX and MLX devices.

### Procedure

1. Create a CSV file with a file name of your choosing.
2. Add content to the file, allowing one row per IP address.

For example:

	A	B	C	D	E	F	G	H	I	J
1	IP Address:	DeviceType:	DeviceVer:	Location	Configura	Discovery	UserName	Password	Community String	
2	10.37.128.	SLX	SLX_18s.1	Duff	SNMP	SSH/CLI	admin	password	default	
3	10.37.138.	NGNPB	NGNPB_v1	Nashville	GNMI	GRPC	admin	rocks	default	
4	10.37.128.	MLX	MLX_v6.3	Las Vegas	SNMP	SSH/CLI	admin	admin	public	
5										

**Figure 5: Device definition CSV**

3. Save the CSV file to a location that is accessible from the Visibility Manager user interface.

---

## Delete a Device

---

You can remove one or more devices from Visibility Manager.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select **Devices**.
3. Select one or more devices to delete.
4. Select **Delete**.

---

## Export the Configuration of SLX and MLX Devices

---

You can export configuration from one device to another.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, right-click the device from which you want to export the configuration.
3. Select **Export Configuration**.
4. In the **To Device** field, select the device to which you want to export the configuration.
5. Select the configuration items that you want to export.

Items flagged with an "i" symbol require the selection of one or more ports before you can export the items.

6. Save (✓) your selections.

---

## Refresh Device Configuration

---

You can use the refresh function to retrieve the latest configuration from a device.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, right-click the device that you want to refresh.
3. Select **Refresh Configuration**.

---

## Persist the Configuration of SLX and MLX Devices

---

You can ensure that Visibility Manager contains the configuration of SLX and MLX devices, which do not support the auto-persistence functionality.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, right-click the device and select **Persist Configuration**.

The configuration is written into the `startup config` file.

---

## Configure Packet Capture on the Extreme 9920

---

The packet capture (PCAP) feature captures live packet data from the traffic that enters and leaves a device and renders the data in a human-readable format.

### About This Task

You can enable PCAP on any physical port on the 9920 device. You can use the data in PCAP files to monitor and analyze network traffic for such information as bandwidth usage, DNS resolution, and even network intrusion.

Ingress packets are captured before any processing occurs, such as actions that are defined by the policies you created. Egress packets are captured after all processing occurs, including header alterations.

As PCAP files are created, Visibility Manager retrieves the information from the 9920 device and displays the information in the Visibility Manager interface.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, right-click a 9920 device and select **Packet Capture**.
3. Select **Configure Port Capture**.
4. Select whether to **Start** or **Stop** a packet capture.
5. In the **Port** field, select a port on which to capture packets.
6. Select whether to collect **Ingress** packets, **Egress** packets, or **Both** types.
7. In the **Packet Count** field, select the number of packets that you want to capture.
8. Select **Add**.

The capture configuration for the selected port is displayed on the right.

9. Repeat steps 4 through 8 as needed to configure PCAPs for more ports.

PCAP configuration is supported for a maximum of 10 ports for the selected device.

10. Save (✓) your changes.

The Packet Capture page displays running PCAPs and PCAP results.

---

## Clear Device Counters

---

You can clear counters for Extreme 9920, MLX, and SLX devices.

### About This Task

Counters track the number of times a certain event or process occurs. Counters increase over time and you can delete them as needed.

For Extreme 9920 devices, you can clear the following counters:

- interface
- ACL
- egress group
- ingress group
- interface

- transport tunnel
- tunnel encapsulation

For MLX and SLX devices, you can clear interface and ACL counters.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, right-click a device and select **Clear Counters**.
3. Select one or more counters to clear.
4. Save (✓) your selections.

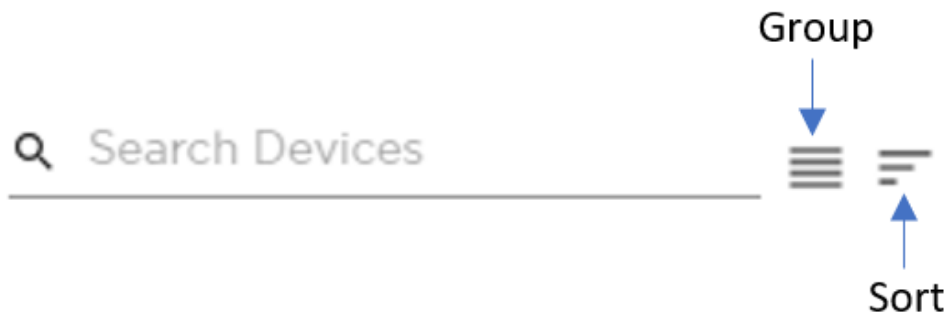
Reports in the dashboards are updated to reflect your selections.

## Search, Group, and Sort Devices

You can search for and organize the devices in the Devices pane.

### About This Task

You can group devices by a common attribute: location or device type. You can sort by device name or by age, with the most recently added device first.



**Figure 6: Search, group, and sort**

### Procedure

1. In the Navigation menu, select **Configure**.
2. To search for a device, enter a device attribute in the **Search Devices** field.  
For example, enter a device name.  
As you begin typing, the list is filtered to match your search word or phrase.
3. To group devices, select **Group > Group By Location** or select **Group > Group by Device Type**.  
The list is organized by the grouping you selected. For example, if you selected Group By Location, the names of all your locations appear in the list. Devices are grouped under each heading. The headings are collapsible.
4. To sort devices, select **Sort > Sort By Recently Added** or select **Sort > Sort By Device Name**.  
The list is organized by the sorting you selected.

## Device Credentials

---

The credentials of monitored devices are stored in the Visibility Manager database.

Credentials for each device are encrypted with a secret key and transferred between Visibility Manager microservices. The microservices store the credentials in the Visibility Manager database.

The Device Interface Service (DIS) uses the secret keys to decrypt the credentials and to establish connections with devices.



# Monitoring Device Health and Statistics

[Supported Device and Health Statistics](#) on page 40

[View Statistics in a Device Dashboard](#) on page 41

[Create and Populate a Custom Dashboard](#) on page 43

[View Events in Device Logs](#) on page 43

The topics in this section describe the device statistics that you can monitor and show you where to view those statistics.

## Supported Device and Health Statistics

You can view real-time device and health statistics in device-specific dashboards and in custom dashboards.

For more information about the services discussed in this topic, see [Visibility Manager Microservices](#) on page 17.

### Device statistics

The Statistics Collection Service (SCS) processes the statistics that are displayed in dashboards. Statistics are obtained from supported devices in the following ways.

- **Extreme 9920 devices:** When a 9920 device is discovered, Visibility Manager uses gNMI to subscribe to the required statistic types. The collected statistics are processed and displayed in dashboards.
- **SLX devices:** When an SLX device is discovered, Visibility Manager is configured as a telemetry collector for streaming statistics. Streamed statistics are processed and displayed in dashboards.
- **MLX devices:** Visibility Manager runs CLI commands periodically to collect statistics, which are processed and displayed in dashboards.

**Table 13: Supported statistics by device type**

Statistic	9920	SLX	MLX
Ingress group	Yes	No	No
Interface	Yes	Yes	Yes
Egress policy	Yes	No	No
Ingress policy	Yes	Yes	Yes
System	Yes	Yes	Yes
Interface summary	Yes	Yes	Yes



## Device health management

The Device Health Monitoring Service (DHMS) runs on the region nodes and controls health management information. It manages device health and informs the other microservices about a device's state. Based on this information, the other microservices update their internal states and respond accordingly. The DHMS also manages syslog and event streams from a device.

- **Syslog:** A device generates logs from different components running on the system. These logs are consumed by the syslog client on the device. Visibility Manager enables syslog configuration when a device is discovered. The Device Receive Service (DRS) hosts the syslog server and streams the syslog messages to the DHMS and Visibility Manager, where the messages are displayed.
- **Events:** Events for Extreme 9920 devices are supported by gNMI subscriptions to the paths of interest. The following events are supported: device state, chassis state, port status, and port-channel status. Events are displayed per device in the dashboards.



### Note

Because SLX and MLX devices do not support gNMI, this functionality is not supported on those devices.

- **Device availability:** Visibility Manager periodically checks for device availability. When a failure occurs or an offline device comes back online, Visibility Manager generates an event and forwards it to internal services. The change in the device state is reflected in the Notification area of the user interface.

## View Statistics in a Device Dashboard

The reports on the Dashboard tab provide real-time, per-device statistics.

### About This Task

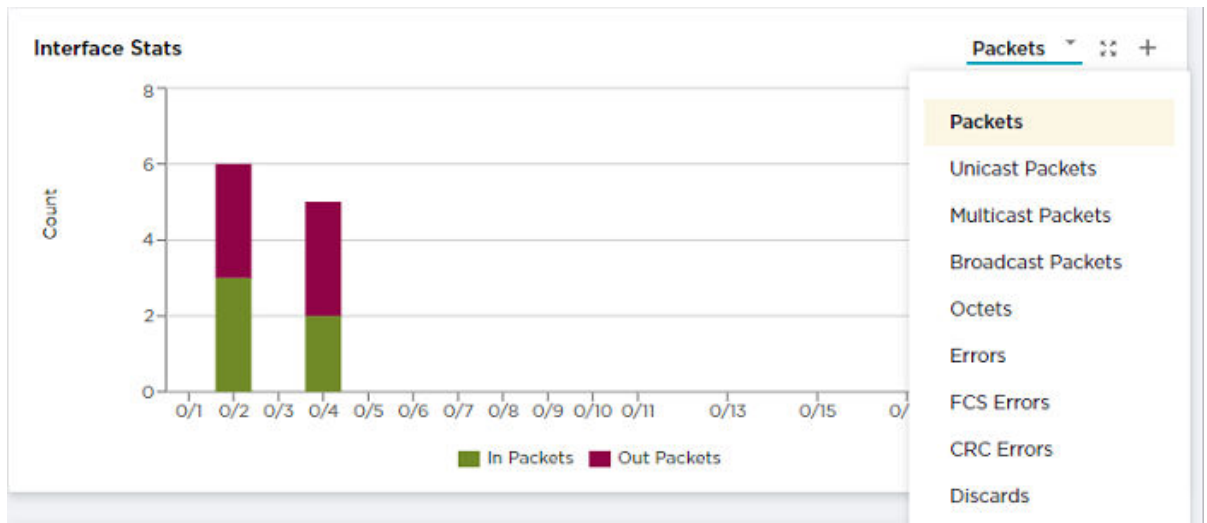
The Dashboard tab becomes available after you add one or more devices. For more information, see [Supported Device and Health Statistics](#) on page 40. Although you cannot change which reports are displayed on the dashboard, you can select the statistics that you want to view and enlarge any report for easier viewing.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device for which you want to view statistics.

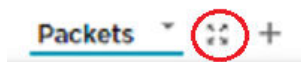
The Dashboard tab displays several default reports.

- To view a different statistic in a report, select the statistic from the list in the upper right corner of the report.

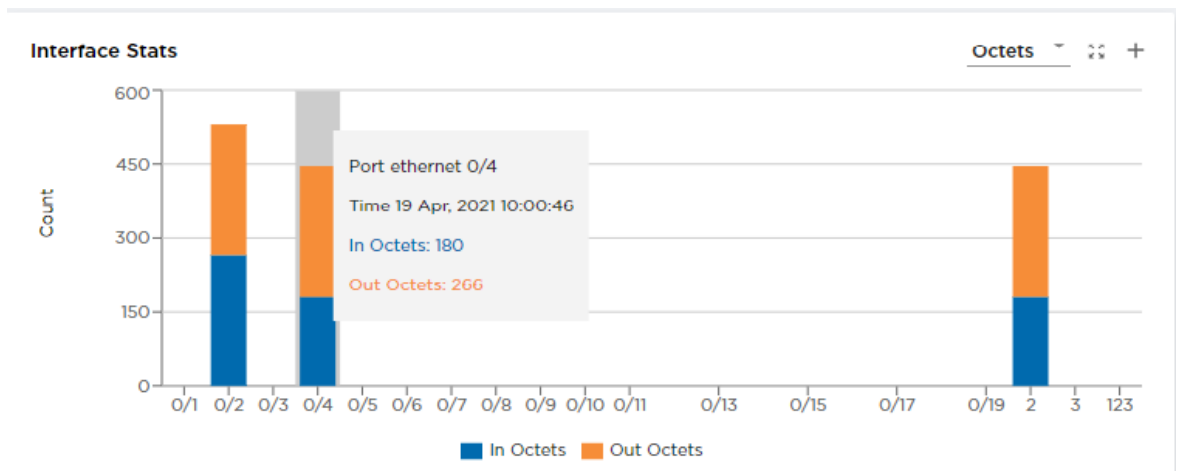


**Figure 7: Statistics list**

- To enlarge a report to the width of the interface, select **Expand** in the report.



- To return a report to its original size, select **Expand** again.
- To view statistics details, hover your cursor over an item in a report.



**Figure 8: Statistics details**

- To add a report to a custom dashboard, select **Add to Dashboard (+)** in the report. Only reports with the + in the upper right corner can be added to a custom dashboard. For more information, see [Create and Populate a Custom Dashboard](#) on page 43.

---

## Create and Populate a Custom Dashboard

---

You can add any report from the device-specific Dashboard tab to your own custom dashboard.

### About This Task

You can create custom dashboards for various purposes. For example, you can create a dashboard that displays the Interface Stats - Summary reports for each device in a zone.

### Procedure

1. Create a custom dashboard.
  - a. In the Navigation menu, select **Dashboard**.
  - b. Select **Add Dashboard**.
  - c. In the **Dashboard Name** field, enter a name for the dashboard.
  - d. Save (✓) your changes.

The new dashboard name is displayed in the Dashboards panel.
2. Add reports to the custom dashboard.
  - a. In the Navigation menu, select **Configure**.
  - b. In the Devices panel, select a device.

The Dashboard tab for that device is displayed. For more information, see [View Statistics in a Device Dashboard](#) on page 41.
  - c. Select **Add to Dashboard** in the report.

Only reports that offer the **Add to Dashboard** tool (+) can be added to a custom dashboard.
  - d. In the **Dashboard** field, select the dashboard to which you want to add the report.

If you have not yet created the custom dashboard, you can do so now by selecting **Create Dashboard**.
  - e. Select all statistics that you want to include on the custom dashboard.
  - f. Save (✓) your changes.
  - g. Repeat steps [2.b](#) on page 43 through [2.f](#) for each report you want to add to the custom dashboard.
3. View the reports in the custom dashboard.
  - a. In the Navigation menu, select **Dashboard**.
  - b. Select the name of the custom dashboard you created.

All reports that you added are displayed.

---

## View Events in Device Logs

---

You can view real-time events in device-specific logs.

### About This Task

Device-specific logs, based on RASlog notifications, provide the following information:

- Host name
- IP address
- Message

- Severity
- Date

To view logs for one device, take the following steps.

**Procedure**

1. In the Navigation menu, select **Configure**.
2. Right-click the device and select **View Logs**.



# Managing Device Ports and Port Channels

---

[Create a Port Channel on page 45](#)

[Change a Port Channel on page 46](#)

[Delete a Port Channel on page 46](#)

[Configure Port Properties on page 47](#)

The topics in this section describe how to create, change, and delete port channels, and describe how to update port configuration.

## Create a Port Channel

---

Port channels, also called Link Aggregation Groups (LAG), are used for load balancing traffic among ports.

### Before You Begin

Remove the MTU configuration from any interface that you plan to add to a port channel.

### About This Task

After you create a port channel, it is available for selection when you create ingress groups and egress.



#### Note

- The fields that are available for creating a port channel vary by the device you are configuring.
- LACP LAG is not supported for Extreme 9920 devices. Only static LAG is supported. The **LACP LAG** field is grayed out and unselected. The **Static LAG** field is grayed out and selected.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device for which you want to create a port channel.
3. In the Device Config menu, select **Add Port Channel**.
4. In the **Port Channel ID** field, enter a unique numeric ID.  
No two port channels can have the same ID.
5. In the **Lag Speed** field, select the speed for the ports that you will select in step 7.
6. In the **Description** field, provide enough information to help you identify the port channel.

7. In the **Ports** field, select at least one port from the list.

The ports in the list will be of the speed that you selected in step 5. A port can be a member of only one port channel. Ports that are not in the list are either already added to another port channel or are operating at a speed that is different from the selection in step 5 on page 45.
8. In the **MTU** field, select the maximum transmission unit for packets that pass through the ports in the channel.
9. In the **Minimum Link** field, select or enter the minimum number of interfaces that the port channel requires to be active.
10. In the **Load Balance Algorithm** field, select a load-balancing method or select **None**.
  - src-dst-ip-l4-port**: The source and destination IP Layer 4 ports method is the default load-balancing method.
  - src-dst-ip-l4-port-tid**: The source and destination IP Layer 4 ports method with tunnel ID.
11. Select **Enable** to change the port channel operating status to Up.

When you select this field, you initiate the **no shutdown** command on the device, which changes the operating status to Up. When the field is not selected, the **shutdown** command runs on the port channel and the operating status changes to Down.
12. Save (✓) your selections.

---

## Change a Port Channel

---

You can change the parameters of a port channel.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device for which you want to change a port channel.
3. Select the **Configuration** tab.
4. In the Device Config menu, expand **Port Channels**.
5. Select the object you want to change.
6. Follow the steps in [Create a Port Channel](#) on page 45 to change the channel parameters.

---

## Delete a Port Channel

---

You can delete a port channel from a device.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device for which you want to delete a port channel.
3. Select the **Configuration** tab.
4. In the Device Config menu, expand **Port Channels**.
5. Select **Delete Port Channel** for the object that you want to delete.

## Configure Port Properties

---

You can change several port properties, including description, port speed, MTU, Forward Error Correction, and Link Fault Signaling.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device for which you want to configure a port.
3. In the Device Config menu, expand **Ports**.
4. Select a port to display a list of properties.
5. In the **Description** field, provide new information.
6. In the **Port Speed** field, select
7. In the **MTU** field, select the maximum transmission unit for packets that pass through the port.
8. In the **Breakout** field, select one of the following:
  - **4x10G**: Configures four 10G breakout interfaces on the port.
  - **4x25G**: Configures four 25G breakout interfaces on a port.
  - **None**
9. In the **Forward Error Correction** field, select one of the following:
  - **Auto-negotiation**: Selects the appropriate algorithm automatically.
  - **FC-FEC**: An algorithm that corrects errors in a block of data, with lower latency than RS-FEC.
  - **RS-FEC**: An algorithm that corrects errors in a block of data, with better error correction than FC-FEC.
  - **Disabled**: Disables the FEC feature.

FEC corrects errors in data without the need for retransmission of the data. Port speed determines which FEC configuration is supported.

  - For 100G ports, RS-FEC, Auto-negotiation, and Disabled are supported.
  - For 25G ports, RS-FEC, FC-FEC, Auto-negotiation, and Disabled are supported.
  - For 40G and 10G ports, only Disabled is supported.
10. To enable communication between two Ethernet devices, select **Link Fault Signaling**.

Link Fault Signaling is a physical layer protocol that enables a port to report fault conditions on inbound and outbound ports.
11. Select **Enable** to change the port operating status to Up.

When you select this field, you initiate the **no shutdown** command on the device, which changes the operating status to Up. When the field is not selected, the **shutdown** command runs on the port and the operating status changes to Down.
12. Save (✓) your selections.



# Managing Egress

---

[Create an Egress on page 48](#)

[Change an Egress on page 49](#)

[Delete an Egress on page 49](#)

The topics in this section explain how to create, change, and delete egress.

## Create an Egress

---

An egress associates ports and port channels with an egress policy.

### Before You Begin

If applicable, create the port channel that you need for the egress. For more information, see [Create a Port Channel](#) on page 45.

Create the egress policy that you need for the egress. For more information, see [Create an Egress Policy for a Device](#) on page 59.

### About This Task

When you create the egress, you assign a name, select a port (or port channel) and its precedence, and then associate your selections with an egress policy. Egress is then available to be associated with the egress groups that you create.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device for which you want to create egress.
3. Select the **Configuration** tab.
4. In the Device Config menu, select **Add Egress**.
5. In the **Egress Name** field, enter a name.

The egress cannot have the same name as an egress group.

6. In the **Port/Port Channel** field, select an egress port or port channel.
7. In the **Precedence** field, select the order of precedence for the port or port channel.

The precedence indicates the priority given to the port or port channel. The lower the number, the higher the priority.

8. Select **+** to add your selections.
9. In the **Egress Policy** field, select the policy to associate with the egress.
10. Save (✓) your selections.



---

## Change an Egress

---

You can change the parameters of an egress.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device for which you want to change an egress.
3. Select the **Configuration** tab.
4. In the Device Config menu, expand **Egress**.
5. Select the egress you want to change.
6. Follow the steps in [Create an Egress](#) on page 48 to change the parameters.

---

## Delete an Egress

---

You can delete an egress from a device.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device for which you want to delete an egress.
3. Select the **Configuration** tab.
4. In the Device Config menu, expand **Egress**.
5. Select **Delete Egress** for the egress that you want to delete.



# Managing Egress Groups

---

[Create an Egress Group on page 50](#)

[Change an Egress Group on page 50](#)

[Delete an Egress Group on page 51](#)

The topics in this section explain egress groups and describe how to create, change, and delete them.

## Create an Egress Group

---

An egress group is a set of interfaces and ports on which traffic is forwarded after a policy is applied.

### Before You Begin

Create the egress to associate with the egress group. For more information, see [Create an Egress](#) on page 48.

### About This Task

When you create an egress group, you assign a name and associate at least one egress. An egress associates an egress port (or port channel) with an egress policy.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device for which you want to create an egress group.
3. Select the **Configuration** tab.
4. In the Device Config menu, select **Add Egress Group**.
5. In the **Name** field, enter a name for the group.  
An egress group cannot have the same name as an egress.
6. In the **Egress List** field, select at least one egress to associate with the group.
7. Save (✓) your selections.

## Change an Egress Group

---

You can add or delete egress in an egress group.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device for which you want to change an egress group.
3. Select the **Configuration** tab.
4. In the Device Config menu, expand **Egress Groups**.

5. Select the group that you want to change.
6. In the **Egress List** field, select (or delete) at least one egress.  
For more information, see [Create an Egress Group](#) on page 50.
7. Save (✓) your selections.

## Delete an Egress Group

---

You can delete an egress group from a device.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device for which you want to delete an egress group.
3. Select the **Configuration** tab.
4. In the Device Config menu, expand **Egress Groups**.
5. Select **Delete Egress Group** for the group that you want to delete.



# Managing Ingress Groups

---

[Create an Ingress Group on page 52](#)

[Change an Ingress Group on page 53](#)

[Delete an Ingress Group on page 53](#)

The topics in this section explain ingress groups and describe how to create, change, and delete them.

## Create an Ingress Group

---

An ingress group is a set of ports and port channels on which monitored traffic is received.

### Before You Begin

If applicable, create the port channel to associate with the ingress group. For more information, see [Create a Port Channel](#) on page 45.

Create the ingress policy to associate with the ingress group. For more information, see [Create an Ingress Policy for a Device](#) on page 60.

### About This Task

Ingress groups classify and apply policies on monitored traffic. After you create an ingress group, the group can be associated with an ingress policy.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device for which you want to create a policy.
3. In the Device Config menu, select **Add Ingress Group**.
4. In the **Name** field, enter a name for the group.
5. In the **Ports/Port Channels** field, select at least one port or port channel for the group.
6. In the **Tunnel Type** field, select the type of tunnel for the incoming traffic: GRE, GTPU, VXLAN, NVGRE, or IPIP.
7. In the **Tunnel ID** field, select or enter a value that represents the tunnel ID.  
This field is not applicable for GRE and IPIP tunnels.
8. In the Advance Scope section, select one of the following actions to apply to the incoming traffic.
  - Decap** to remove the outer tunnel headers from the packet
  - Scope Shift** to move the ACL scope for matching from the outer headers to the inner headers of a tunneled packet
  - None** to perform neither action
9. In the **Policy Name** field, select the ingress policy to associate with the ingress group.

10. Save (✓) your selections.

The Configuration tab displays a graphical representation of the ingress group and its associated policies and egress groups (also known as a service chain).

---

## Change an Ingress Group

---

You can add, change, or delete the parameters of an ingress group.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device for which you want to change an ingress group.
3. In the Device Config menu, expand **Ingress Groups**.
4. In the list of groups, select the group that you want to change.
5. Follow the instructions in [Create an Ingress Group](#) on page 52 to add, change, or delete the parameters in the group.

---

## Delete an Ingress Group

---

You can delete an ingress group from a device.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device for which you want to delete an ingress group.
3. In the Device Config menu, expand **Ingress Groups**.
4. Select **Delete Ingress Group** for the group that you want to delete.



# Managing Policy Rule Matches

---

- [Create a Policy Rule Match for a Device on page 54](#)
- [Create a Policy Rule Match in the Library on page 56](#)
- [Change a Policy Rule Match on page 56](#)
- [Import a Policy Rule Match to a Device on page 57](#)
- [Export a Policy Rule Match on page 57](#)
- [Clone a Policy Rule Match on page 57](#)
- [Delete a Policy Rule Match on page 58](#)
- [Search Policy Rule Matches on page 58](#)

The topics in this section explain policy rule matches and describe how to create, change, import, export, clone, and delete them.

## Create a Policy Rule Match for a Device

---

A policy rule match identifies the parts of a packet header that a rule targets, such as the source port or the payload length.

### About This Task

When you create a policy rule match, you select all parts of a packet header that you want to target and then select the action to perform on the targeted items. These selections are the rules in your match. The match can then be associated with ingress or egress policies. A policy rule match can contain one or more rules.



#### Note

A policy rule match is a device-specific feature. If you have ACLs configured for a device, ACL-related fields are displayed in the Create Match page. These fields are not specified in this procedure.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device for which you want to add a policy rule match.
3. Select the **Configuration** tab.
4. In the Device Config menu, select **Add Policy Rule Match**.
5. In the **Name** field, enter a name for the match.
6. In the **Type** field, select whether the match applies to IPv4, IPv6, or L2.

7. In the Match section, complete the following fields to identify all parts of the packet header that you want to target with the actions you select in step 9 on page 56.

The items that you can select vary by your selection in the **Protocol** field. The following describes all possible selections.

**Protocol:** The protocol that you want to target. If the protocol you want is not in the list, select **None** and provide the ID of the protocol you want in the **Protocol ID** field. Every protocol has a numeric value that is defined by IETF.

**Sequence:** The order in which this rule is performed in the match.

**Protocol ID:** The ID of a protocol that you want to target. Use only when the protocol you want is not available in the **Protocol** field.

**Source IP:** The IP address of the device that sends the packets, in CIDR format.

**Source Mask:** The mask for the source IP address, in the following format: 255.255.255.255.

**Destination IP:** The IP address of the device that is to receive the packets, in CIDR format.

**Destination Mask:** The mask for the destination IP address, in the following format: 255.255.255.255.

**Source Mac:** The MAC address of the device that sends the packets, in the following format: 1111.1111.1111 or 11:11:11:11:11:11. Any alpha characters in the address must be lowercase.

**Source Mac Mask:** The mask for the source MAC address, in the following format: ffff.ffff.ffff or ff:ff:ff:ff:ff:ff. Any alpha characters in the mask must be lowercase.

**Destination Mac:** The MAC address of the device that is to receive the packets, in the following format: 1111.1111.1111 or 11:11:11:11:11:11. Any alpha characters in the address must be lowercase.

**Destination Mac Mask:** The mask for the destination MAC address, in the following format: ffff.ffff.ffff or ff:ff:ff:ff:ff:ff. Any alpha characters in the mask must be lowercase.

**Source Port:** The port through which packets enter the device.

**Source Port End:** The last port in the range of ports through which packets enter the device.

**Destination Port:** The port through which packets leave the device. Valid values range from 1 through 65535.

**Destination Port End:** The last port in the range of ports through which packets leave the device. Valid values range from 1 through 65535.

**IP Payload Length:** The length of the IP packets that you want to target, or the size of the IP payload. Valid values range from 64 through 9000.

**IP Payload Length End:** The last acceptable value of the IP payload. Valid values range from 65 through 9000.

**DSCP:** The value of the Differentiated Services Code Point in the Type of Service field in the header. Valid values range from 0 through 63.

**VLAN:** The VLAN ID. Valid values range from 0 through 4095.

**EtherType:** Identifies the protocol that is encapsulated in the payload. For example, the EtherType value for IPv4 is 0x0800. Valid values range from 1536 through 65536 (numerical), or 0x0600 through 0xffff (hexadecimal), or are one of the following: ARP, IPv4, or IPv6.

**PCP:** The Priority Code Point, a 3-bit field in a VLAN header. Valid values range from 0 through 7.

**Tunnel ID:** The ID number of the tunnel. Valid values range from 1 through 16777215.

8. In the Fragmentation section, select one or more of the following.

The items that you can select vary by your selection in the **Protocol** field. The following describes all possible selections.

**Fragmented:** Targets target fragmented packets.

**Non Fragmented:** Targets non-fragmented packets.

**None:** Targets packets in which the DF (Don't Fragment) flag is set in the IP header.

**Acknowledgment:** Targets packets in which the ACK flag is set in the TCP header.

**Congestion:** Targets packets in which the CWR flag is set in the TCP header.

**ECN-Echo:** Targets packets in which the ECE flag is set in the TCP header.

**Last Packet:** Targets packets in which the FIN flag is set in the TCP header.

**Push:** Targets packets in which the PSH flag is set in the TCP header.

**Reset:** Targets packets in which the RST flag is set in the TCP header.

**Synchronize:** Targets packets in which the SYN flag is set in the TCP header.

**Urgent:** Targets packets in which the URG flag is set in the TCP header.

9. In the Action section, select one or more actions to perform on the targeted items.

**Drop** to drop the packet

**Count** to keep track of the number of packets that match the policy rule

**Log** to add the transaction to the Visibility Manager log.

10. Select **Add**.

The match parameters (the new rule) appear in the pane on the right.

11. Repeat steps 7 through 10 until you have added all the rules you need.
12. To remove a rule from the match, select **Delete** for that rule in the Rules panel on the right.
13. To change a rule, select **Edit** for that rule in the Rules panel and make your changes.
14. Save (✓) your selections.

## Create a Policy Rule Match in the Library

---

Policy rule matches in the library can be imported to a device.

### About This Task

You can create policy rule matches that you store in the library. Matches in the library can be imported as needed to one or more devices.

### Procedure

1. In the Navigation menu, select **Library > Match**.
2. Select **Add Match**.
3. Follow the instructions in [Create a Policy Rule Match for a Device](#) on page 54.

## Change a Policy Rule Match

---

You can add, change, or delete one or more rules in a policy rule match.

### About This Task

You can change a policy rule match for a specific device or change a match in the library.



### Procedure

1. To change a match for a device, take the following steps.
  - a. In the Navigation menu, select **Configure**.
  - b. In the Devices panel, select the device for which you want to change a match.
  - c. Select the **Configuration** tab.
  - d. In the Device Config menu, expand **Policy Rule Matches**.
  - e. In the list of matches, select the match that you want to change.
  - f. Follow the instructions in [Create a Policy Rule Match for a Device](#) on page 54 to add, change, or remove rules in the match.
2. To change a match in the library, take the following steps.
  - a. In the Navigation menu, select **Library > Match**.
  - b. Select **Edit** for the match that you want to change.
  - c. Follow the instructions in [Create a Policy Rule Match for a Device](#) on page 54 to add, change, or remove rules from the match.

Your changes affect all devices that are associated with the match.

## Import a Policy Rule Match to a Device

---

Policy rule matches that you store in the library can be imported as needed to one or more devices.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device for which you want to import a policy rule match.
3. Select the **Configuration** tab.
4. In the Device Config menu, select **Import Match**.
5. Select one or more matches.
6. Select **Import**.

## Export a Policy Rule Match

---

From the library, you can export a policy rule match to selected devices.

### Procedure

1. In the Navigation menu, select **Library > Match**.
2. Select **Export** for the match that you want to export.
3. Select the devices to which you want to export the selected match.
4. Select **Export**.

## Clone a Policy Rule Match

---

From the library, you can clone (copy) a policy rule match to create a new match with the same or similar configuration.

### Procedure

1. In the Navigation menu, select **Library > Match**.

2. Select **Clone** for the match that you want to copy.
3. In the **Name** field, provide a new name for the cloned match.
4. Follow the instructions in [Create a Policy Rule Match for a Device](#) on page 54 to add, change, or remove rules from the match.
5. Save (✓) your selections.

## Delete a Policy Rule Match

---

You can delete a policy rule match from a device or from the library.

### Procedure

1. To delete a policy rule match from a device, take the following steps.
  - a. In the Navigation menu, select **Configure**.
  - b. In the Devices panel, select the device for which you want to delete a policy rule match.
  - c. Select the **Configuration** tab.
  - d. In the Device Config menu, expand **Policy Rule Matches**.
  - e. Select **Delete Match** for the match you want to delete.
2. To delete a policy rule match from the library, take the following steps.
  - a. In the Navigation menu, select **Library > Match**.
  - b. Perform step 1 on page 58 to delete the policy rule match from any associated device.
  - c. Select one or more matches to delete.
  - d. Select **Delete**.

## Search Policy Rule Matches

---

From the library, you can search for a policy rule match by name, device type, rule type, or number of rules.

### Procedure

1. In the Navigation menu, select **Library > Match**.
2. In the **Search Matches** field, type the information you want to find.

For example, to search for a match name that contains the numeric string 65550, type 65550. As you begin typing, the Matches list is filtered to match your search word or phrase.
3. To reset the list, delete the characters in the **Search Matches** field.



# Managing Policies

---

- [Create an Egress Policy for a Device on page 59](#)
- [Create an Ingress Policy for a Device on page 60](#)
- [Create a Policy in the Library on page 61](#)
- [Change a Policy on page 61](#)
- [Import a Policy to a Device on page 62](#)
- [Export a Policy on page 62](#)
- [Clone a Policy on page 63](#)
- [Delete a Policy on page 63](#)
- [Search Policies on page 63](#)

The topics in this section describe how to create, change, import, export, clone, and delete policies.

## Create an Egress Policy for a Device

---

An egress policy (or listener policy) defines the actions to apply to outbound packets.

### Before You Begin

Create the policy rule match to associate with the policy. For more information, see [Create a Policy Rule Match for a Device](#) on page 54.

### About This Task

Take the following steps to define the criteria for a policy. Each set of criteria is a rule. A policy can contain multiple rules.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device for which you want to create a policy.
3. Select the **Configuration** tab.
4. In the Device Config menu, select **Add Policy**.
5. In the **Name** field, enter a name for the policy.
6. In the **Policy Type** field, select **Egress Policy**.
7. In the Rule section, complete the following fields.
  - a. Enter a **Name** for the policy rule.
  - b. Select the **Sequence** in which to apply the rule.

- c. Select a policy **Match**.

If you did not create a policy rule match, select **Create Match** to create the match now.

You cannot use the same policy rule match multiple times in a policy. Rule match usage is limited to one per policy.

8. In the **Packet Slicing** field, select a value to represent the final packet size after slicing, unless the packet is already smaller than the value you select.
9. In the **Header Stripping** field, select one or more tags to strip: 802.1BR, VLAN, or VN (Virtual NIC).  
The 802.1BR and VN tags cannot coexist in the same policy rule action.
10. In the **VLAN** field, select the VLAN ID to target the VLAN tag in the egress packet.
11. To remove the outer tunnel headers from the packet, select **Decap**.
12. To prevent the rule from being used in the policy, select **Deny**.



#### Tip

This option prevents the rule from being used, but does not delete the configuration of the rule. The rule is skipped and is not used to drop a packet. You can reinstate the rule later without having to reconfigure it.

13. Select **Add**.

The rule parameters appear in the pane on the right.

14. Repeat steps 7 through 13 until you have added all the rules you need.
15. Save (✓) your selections.

## Create an Ingress Policy for a Device

An ingress policy (or route map) defines the actions to apply to inbound packets.

### Before You Begin

Create a policy rule match to associate with the policy. For more information, see [Create a Policy Rule Match for a Device](#) on page 54.

Create an egress group to associate with the policy. For more information, see [Create an Egress Group](#) on page 50.

### About This Task

Take the following steps to define the criteria for a policy. Each set of criteria is a rule. A policy can contain multiple rules.


### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device for which you want to create a policy.
3. Select the **Configuration** tab.
4. In the Device Config menu, select **Add Policy**.
5. In the **Name** field, enter a name for the policy.
6. In the **Policy Type** field, select **Ingress Policy**.

7. In the Rule section, complete the following fields.
  - a. Enter a **Name** for the policy rule.
  - b. Select the **Sequence** in which to apply the rule.
  - c. Select a policy **Match**.

If you did not create a policy rule match, select **Create Match** to create the match now.

You cannot use the same policy rule match multiple times in a policy. Rule match usage is limited to one per policy.
8. In the **Egress Group** field, select the group to associate with the policy.
9. In the **Packet Slicing** field, select a value to represent the final packet size after slicing, unless the packet is already smaller than the value you select.
10. In the Advance Scope section, select one of the following:
  - Decap** to remove the outer tunnel headers from the packet
  - Scope Shift** to move the ACL scope for matching from the outer headers to the inner headers of a tunneled packet
  - None** to perform neither action
11. To prevent the rule from being used in the policy, select **Deny**.

 **Tip** This option prevents the rule from being used, but does not delete the configuration of the rule. The rule is skipped and is not used to drop a packet. You can reinstate the rule later without having to reconfigure it.
12. Select **Add**.

The rule parameters appear in the pane on the right.
13. Repeat steps 7 through 12 until you have added all the rules you need.
14. Save (✓) your selections.

## Create a Policy in the Library

---

Policies in the library can be imported to one or more devices.

### Procedure

1. In the Navigation menu, select **Library > Policy**.
2. Select **Add Policy**.
3. Follow the instructions in [Create an Egress Policy for a Device](#) on page 59 or [Create an Ingress Policy for a Device](#) on page 60.

## Change a Policy

---

You can add, change, or delete one or more rules or actions in a policy.

### About This Task

You can change a policy for a specific device or change a policy in the library.

### Procedure

1. To change a policy for a device, take the following steps.
  - a. In the Navigation menu, select **Configure**.
  - b. In the Devices panel, select the device for which you want to change a policy.
  - c. Select the **Configuration** tab.
  - d. In the Device Config menu, expand **Policies**.
  - e. Select the policy that you want to change.
  - f. Follow the instructions in [Create an Ingress Policy for a Device](#) on page 60 or [Create an Egress Policy for a Device](#) on page 59 to add, change, or remove rules or actions in the policy.

**Tip**

To reinstate a rule that is not included in the policy (the **Deny** field is selected), clear the **Deny** field.

2. To change a policy in the library, take the following steps.
  - a. In the Navigation menu, select **Library > Policy**.
  - b. Select **Edit** for the policy that you want to change.
  - c. Follow the instructions in [Create an Ingress Policy for a Device](#) on page 60 or [Create an Egress Policy for a Device](#) on page 59 to add, change, or remove rules or actions in the policy.

**Tip**

To reinstate a rule that is not included in the policy (the **Deny** field is selected), clear the **Deny** field.

Your changes affect all devices that are associated with the policy.

## Import a Policy to a Device

---

Policies that you store in the library can be imported as needed to one or more devices.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device for which you want to import a policy.
3. Select the **Configuration** tab.
4. In the Device Config menu, select **Import Policy**.
5. Select one or more policies.
6. Select **Import**.

## Export a Policy

---

From the library, you can export a policy to selected devices.

### Procedure

1. In the Navigation menu, select **Library > Policy**.
2. Select **Export** for the policy that you want to export.
3. Select the devices to which you want to export the selected policy.

4. Select **Export**.

## Clone a Policy

---

From the library, you can clone (copy) a policy to create a new policy with the same or similar configuration.

### Procedure

1. In the Navigation menu, select **Library > Policy**.
2. Select **Clone** for the policy that you want to copy.
3. In the **Name** field, provide a new name for the cloned policy.
4. Follow the instructions in [Create an Ingress Policy for a Device](#) on page 60 or [Create an Egress Policy for a Device](#) on page 59 to add, change, or remove rules from the policy.
5. Save (✓) your selections.

## Delete a Policy

---

You can delete a policy from a device or from the library.

### Procedure

1. To delete a policy from a device, take the following steps.
  - a. Remove the policy from any associated ingress group. For more information, see [Change an Ingress Group](#) on page 53.
  - b. In the Navigation menu, select **Configure**.
  - c. In the Devices panel, select the device for which you want to delete a policy.
  - d. Select the **Configuration** tab.
  - e. In the Device Config menu, expand **Policies**.
  - f. Select **Delete Policy** for the policy that you want to delete.
2. To delete a policy from the library, take the following steps.
  - a. Remove the policy from any associated ingress group. For more information, see [Change an Ingress Group](#) on page 53.
  - b. Perform step 1 to delete the policy from any associated device.
  - c. In the Navigation menu, select **Library > Policy**.
  - d. Select one or more policies to delete.
  - e. Select **Delete**.

## Search Policies

---

From the library, you can search for a policy by name, device type, policy type, or number of rules.

### Procedure

1. In the Navigation menu, select **Library > Policy**.
2. In the **Search Policies** field, type the information you want to find.

For example, to search for a policy name that contains the numeric string 65550, type 65550. As you begin typing, the Policies list is filtered to match your search word or phrase.

3. To reset the list, delete the characters in the **Search Policies** field.





# Managing User-Defined ACLs

---

[Create a UDA on page 65](#)

[Change a UDA on page 65](#)

[Clone a UDA on page 66](#)

[Delete a UDA on page 66](#)

[Search UDAs on page 66](#)

The topics in this section describe how to manage user-defined access lists (UDAs) for MLX devices.

## Create a UDA

---

You can create a user-defined access list (UDA) in the library.

### About This Task

UDAs are supported only for MLX devices.

### Procedure

1. In the Navigation menu, select **Library > UDA**.
2. Select **Add UDA**.
3. In the **Name** field, enter a name for the UDA.
4. In the **Device Type** field, select the appropriate device.
5. In the four **Offset** fields, select the appropriate offset values.

An offset increases a metric in a routing update for networks that match the access list. It simulates increasing the number of hops between routers. No action is taken for an offset of 0.

6. Save (✓) your selections.

## Change a UDA

---

You can change the parameters of a user-defined access list (UDA).

### Procedure

1. In the Navigation menu, select **Library > UDA**.
2. Select **Edit** for the UDA that you want to change.
3. Follow the instructions in [Create a UDA on page 65](#) to change the parameters.

---

## Clone a UDA

---

You can clone (copy) a user-defined access list (UDA) to create a new UDA with the same or similar configuration.

### Procedure

1. In the Navigation menu, select **Library > UDA**.
2. Select **Clone** for the UDA that you want to copy.
3. Follow the instructions in [Create a UDA](#) on page 65 to configure the UDA.
4. Save (✓) your selections.

---

## Delete a UDA

---

You can delete a user-defined access list (UDA) from the library.

### Procedure

1. In the Navigation menu, select **Library > UDA**.
2. Select one or more UDAs to delete.
3. Select **Delete**.

---

## Search UDAs

---

You can search for a user-defined access list (UDA) by name or device type.

### Procedure

1. In the Navigation menu, select **Library > UDA**.
2. In the **Search UDAs** field, type the information you want to find.  
For example, to search for a name that contains the word 'tap', type tap.  
As you begin typing, the UDAs list is filtered to match your search word or phrase.
3. To reset the list, delete the characters in the **Search UDAs** field.



# Managing Tunnels

---

[Create a Tunnel](#) on page 67

[Change a Tunnel](#) on page 68

[Delete a Tunnel](#) on page 68

The topics in this section explain how to create, change, and delete transport tunnels.

## Create a Tunnel

---

You can configure transport tunnel termination and encapsulation for a device.

### About This Task

You can associate transport tunnel termination with an ingress group. You can apply an ACL or ingress policy based on the ingress group configuration (GRE and ERSPAN tunnel). For more information, see [Create an Ingress Group](#) on page 52.

For traffic that leaves an Extreme 9920 device, you can associate transport tunnel encapsulation with egress. For more information, see [Create an Egress](#) on page 48.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device for which you want to create a tunnel.
3. Select the **Configuration** tab.
4. In the Device Config menu, select **Add Tunnel**.
5. In the **Name** field, enter a name for the tunnel.
6. In the **Type** field, select **Termination or Encapsulation**.
7. In the **Tunnel Type** field, select one of the following.

The options vary by the type you selected in step 6.

- **GRE** (Generic Routing Encapsulation). This type of tunnel encapsulates (or wraps) packets that use a certain protocol inside packets that use a different protocol.
  - **ERSPAN** (Encapsulated Remote Switched Port Analyzer): This type of tunnel mirrors traffic from source ports for delivery to destination ports on a different device.
8. In the **Source IP** field, enter the IP address of the devices that sends the packets.
  9. In the **Destination IP** field, enter the IP address of the device that is to receive the packets.

10. Complete the following fields.

The fields vary by the type you selected in step 6.

- **Source MAC.** The MAC address of the device that sends the packets.
- **Destination MAC.** The MAC address of the device that is to receive the packets.
- **VLAN Tag.** A numeric string that identifies which VLAN a packet belongs to.
- **VLAN PCP.** The Priority Code Point, a 3-bit field in the VLAN header.
- **Egress.** The egress to associate with the tunnel.
- **Source Prefix.** The prefix of the IP address of the devices that sends the packets, in CIDR notation format.
- **Destination Prefix.** The prefix of the IP address of the device that receives the packets, in CIDR notation format.
- **Ingress Groups.** The ingress group to associate with the tunnel.

11. Save (✓) your selections.

---

## Change a Tunnel

---

You can change the tunnel configuration for a device.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device for which you want to change the configuration of a tunnel.
3. Select the **Configuration** tab.
4. In the Device Config menu, expand **Tunnel**.
5. Select the tunnel that you want to change.
6. Follow the steps in [Create a Tunnel](#) on page 67 to configure the tunnel.

---

## Delete a Tunnel

---

You can delete tunnel configuration from a device.

### Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device for which you want to delete a tunnel.
3. Select the **Configuration** tab.
4. In the Device Config menu, expand **Tunnel**.
5. Select **Delete Tunnel** for the tunnel that you want to delete.



# Managing Locations

---

[Upload a Location Definition File](#) on page 69  
[Search Locations](#) on page 69

The topics in this section explain how to add locations.csv files and search locations from the Visibility Manager user interface.

## Upload a Location Definition File

---

The Location Definition file (in CSV format) identifies regions and their associated zones and managed locations.

### About This Task

You created the `locations.csv` file before you installed Visibility Manager because the file plays a part in the installation process. For more information, see [Extreme Visibility Manager Deployment Guide, 6.0.0](#).

After Visibility Manager is installed, you can upload the CSV file to the interface so that you can easily see the zones and locations that are in a particular region.

### Procedure

1. In the Navigation menu, select **Settings > Location**.
2. Select **Add Location**.
3. Upload the `locations.csv` file in one of the following ways.
  - Drag the file into the **Drag & Drop Location Definition File** box.
  - Select **Browse** and navigate to the file location.
4. Save (✓) your changes.

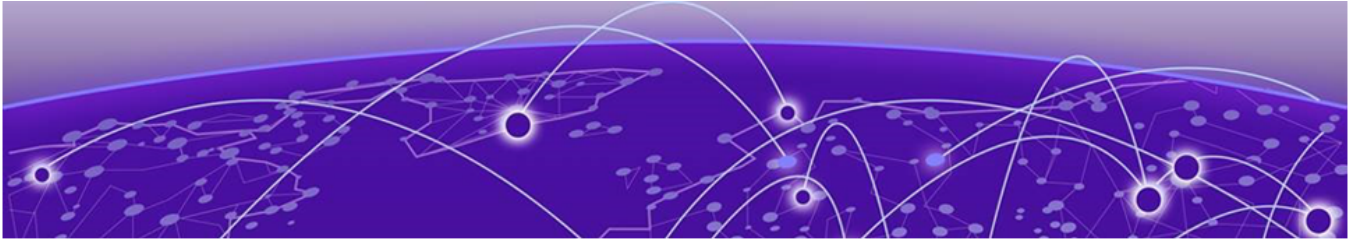
## Search Locations

---

You can search the list of locations for a particular region, zone, or location.

### Procedure

1. In the Navigation menu, select **Settings > Location**.
2. In the **Search Locations** field, type the information you want to find.  
For example, to search for all locations in Las Vegas, type `Las Vegas`.  
As you begin typing, the Locations list is filtered to match your search word or phrase.
3. To reset the list, delete the characters in the **Search Locations** field.



# Rule and Functionality Mapping

---

Extreme Visibility Manager supports multiple devices, which have different functions and configurations related to traffic direction.

The following tables describe how Visibility Manager configuration, policies, and header modification tasks map to the same features on supported devices.

Key for the abbreviations in the following tables:

- MLX I: MLX ingress direction
- MLX E: MLX egress direction
- 9920 I: Extreme 9920 ingress direction
- 9920 E: Extreme 9920 egress direction
- SLX I: SLX ingress direction
- SLX E: SLX egress direction
- XVM I: Visibility Manager ingress direction
- XVM E: Visibility Manager egress direction
- VN-tag: Virtual Network tag
- VxLAN: Virtual Extensible LAN
- NVGRE: Network Virtualization with Generic Routing Encapsulation
- GTP: GPRS (General Packet Radio Service) Tunneling Protocol

## MLX to Visibility Manager mapping

**Table 14: Rule mapping**

Rule	MLX path	XVM path
<b>Policies per device</b>		
Create a policy structure for every route-map name. Index to the policy structure is the route-map name	Device[]/route-map[name]	/Policy[name]
Create a rule structure under policy for every rm-instance indexed by seq-num	Device[]/route-map[name]/rm-instance[seqNum]	/Policy[name]<ingress>/Rule (SeqNum)
For every route-map stanza, a set operation can be mapped to a rule action	Device[]/route-map[name]/rm-instance[seqNum]/action	/Policy[name]<ingress>/Rule (SeqNum)/action
Each route-map can have multiple match criteria on an ACL level related to Layer 2 and Layer 3 headers	Device[]/route-map[name]/rm-instance[seqNum]/X'acl	/Policy[name]<ingress>/Rule(SeqNum)/X(l2/ipv4/ipv6)
	Device[]/route-map[name]/rm-instance[seqNum]/X'aci/match	/Policy[name]/Rule (SeqNum)/X/match
Device[]/route-map[name]/rm-instance[seqNum]/X'aci/action		/Policy[name]<ingress>/Rule (SeqNum)/X/action
<b>Interfaces per device</b>		
Bind policies to interfaces	Device[]/Slots[]/Device-id[]/Ports[]/Policy	/ingress/Policy bind[name]
<b>Port channels per device</b>		
Members of VLANs that are part of a route-map's nexthop are scanned. If port channels are present with load-balancing, apply the same to port channels in the Visibility Manager model.	Device[]/vlans[]/vlan/<load-balancing>	/egress/Port-channel[]

**Table 15: Advanced rule mapping for global features**

MLX I	MLX E	XVM I	XVM E	Rule	MLX path	XVM path
<b>802.1BR header stripping:</b> Strip the 802.1BR header from ingress traffic and send it for processing						
Supported	Not supported	Supported	Supported	Add the decap traffic type for 802.1BR on the ingress port	Device[]/Slots[]/ Device-id[]/ Ports[]/<802.1br strip>	/ingress[]/Traffic/ TrafficDecap<802. 1BR>
<b>802.1BR header bypass:</b> Bypass the 802.1BR header and perform inner header lookup						
Supported	Not supported	Supported	Supported	Add the bypass traffic type for 802.1BR on the ingress port	Device[]/Slots[]/ Device-id[]/ Ports[]/<802.1br bypass>	/ingress[]/Traffic/ TrafficBypass<80 2.1BR>
<b>VN-tag header stripping:</b> Strip the VN-tag from ingress traffic and send it for processing						
Supported	Not supported	Supported	Supported	Add the decap traffic type for the VN-tag on the ingress port	Device[]/Slots[]/ Device-id[]/ Ports[]/<vn-tag strip>	/ingress[]/Traffic/ TrafficDecap<vn- tag>
<b>VN-tag header bypass:</b> Bypass the VN-tag header and perform inner header lookup						
Supported	Not supported	Supported	Supported	Add the bypass traffic type for the VN-tag on the ingress port	Device[]/Slots[]/ Device-id[]/ Ports[]/<vn-tag bypass>	/ingress[]/Traffic/ TrafficBypass<VN -tag>
<b>VN-tag and 802.1BR preservation:</b> TBD						
Supported	Not supported	Supported	Supported			
<b>VxLAN header stripping:</b> Strip VxLAN from ingress traffic and send it for processing						
Supported	Not supported	Supported	Supported	Add the decap traffic type for the VxLAN on the ingress port	Device[]/Slots[]/ Device-id[]/ Ports[]/vxlan strip>	/ingress[]/Traffic/ TrafficDecap<vxla n>
<b>NVGRE header stripping:</b> Strip NVGRE from ingress traffic and send for processing						
Supported	Not supported	Supported	Supported	Add the decap traffic type for NVGRE on the ingress port	Device[]/Slots[]/ Device-id[]/ Ports[]/<nvgre strip>	/ingress[]/Traffic/ TrafficDecap<nvgr e>
<b>GTP de-encapsulation:</b> Remove the outer IP, the outer UDP header, and the GTP header from GTP-U packets						



**Table 15: Advanced rule mapping for global features (continued)**

MLX I	MLX E	XVM I	XVM E	Rule	MLX path	XVM path
Supported	Not supported	Supported	Supported	Add the decap traffic type for GTP on the ingress port	Device[]/Slots[]/ Device-id[]/ Ports[]/<gtp decap>	/ingress[]/Traffic/ TrafficDecap<gtp Decap>
<b>Packet slicing (packet truncation)</b>						
Not supported	Supported	Supported	Supported	Add packet slicing for traffic on the egress port	Device[]/Slots[]/ Device-id[]/ Ports[]<egress>/ <gtp decap>	/egress[]/Traffic/ <packetSlicing>

## Extreme 9920 to Visibility Manager mapping

**Table 16: Rule mapping**

Rule	9920 path	XVM path
<b>Ingress port bind</b>		
Device traffic parameters are mapped to the Visibility Manager model	Device[]/ingress-group/Traffic	/ingress/Traffic
Copy all ingress direction policies per interface	Device[]/ingress-group/rm-bind	/ingress/Policy-bind
<b>Ingress policies</b>		
Create a route-map and subsidiaries, and copy all ingress policies	Device[]/route-map[name]/rm-instance[seqNum]	/Policy[name]<ingress>/Rule[SeqNum]
	Device[]/route-map[name]/rm-instance[seqNum]/action	/Policy[name]<ingress>/Rule[SeqNum]/action
	Device[]/route-map[name]/rm-instance[seqNum]/X'acl	/Policy[name]<ingress>/Rule[SeqNum]/X(12/ipv4/ipv6)
	Device[]/route-map[name]/rm-instance[seqNum]/L2acl/ipv4acl/X'acl/match	/Policy[name]<ingress>/Rule[SeqNum]/X/match
	Device[]/route-map[name]/rm-instance[seqNum]/L2acl/ipv4acl/X'acl/action	/Policy[name]<ingress>/Rule[SeqNum]/X/action
<b>Egress policies</b>		
Create a route-map and subsidiaries, and copy all listener policies	Device[]/Listener-policy[name]/ip-instance[seqNum]	/Policy[name]<Egress>/Rule[SeqNum]
	Device[]/Listener-policy[name]/ip-instance[seqNum]/action	/Policy[name]<Egress>/Rule[SeqNum]/action
	Device[]/Listener-policy[name]/ip-instance[seqNum]/X'acl	/Policy[name]<Egress>/Rule[SeqNum]/X(12/ipv4/ipv6)
	Device[]/Listener-policy[name]/ip-instance[seqNum]/L2acl/ipv4acl/X'acl/match	/Policy[name]<Egress>/Rule[SeqNum]/X/match
	Device[]/Listener-policy[name]/ip-instance[seqNum]/L2acl/ipv4acl/X'acl/action	/Policy[name]<Egress>/Rule[SeqNum]/X/action
Copy all egress direction policies per interface	device/egress-group/egress/Listener-Policy[]	/egress[]/Policy<egress>-bind[]

**Table 16: Rule mapping (continued)**

Rule	9920 path	XVM path
<p><b>Egress encapsulation</b></p> <p>For the egress direction, copy encap to all egress port policies</p>	<p>device/egress-group/egress/TrafficEncap</p>	<p>/egress/Traffic&lt;encap&gt;</p>

**Table 17: Advanced rule mapping for global features**

9920 I	9920 E	XVM I	XVM E	Rule	9920 path
<b>802.1 BR header stripping</b>					
Not supported	Supported	Supported	Supported	Map the listener-policy action to the egress policy rule action of the XVM model	Device[]/Slots[]/Device-id[]/Ports[]/<802.1bR strip>
<b>VN-tag header stripping</b>					
Not supported	Supported	Supported	Supported	Map the listener-policy action to the egress policy rule action of the XVM model	Device[]/Listener-policy[name]/ip-instance[seqNum]/action<vn-tag strip>
<b>VxLAN header stripping</b>					
Supported	Not supported	Supported	Supported	Map the ingress-group VxLAN strip to the ingress traffic decap of the XVM model	Device[]/ingress-group/Ports[]/Traffic/TrafficDecap<vxlan>
<b>NVGRE header stripping</b>					
Supported	Not supported	Supported	Supported	Map the ingress-group VxLAN strip to the ingress traffic decap of the XVM model	Device[]/ingress-group/Ports[]/Traffic/TrafficDecap<nvgre>
<b>GTP decapsulation</b>					
Supported	Not supported	Supported	Supported	Map the ingress-group VxLAN strip to the ingress traffic decap of the XVM model	Device[]/ingress-group/Ports[]/Traffic/TrafficDecap<gtp>

**Table 17: Advanced rule mapping for global features (continued)**

9920 I	9920 E	XVM I	XVM E	Rule	9920 path
Packet slicing					
Supported	Supported	Supported	Supported	Truncation is supported in ingress or egress depending on configuration. Map to the XVM model	Device[]/route-map[name]/rm-instance[seqNum]/action<truncate> or Device[]/Listener-policy[name]/lp-instance[seqNum]/action<truncate>

## SLX to Visibility Manager mapping

**Table 18: Rule mapping**

Rule	SLX path	XVM path
<b>Policies per device</b>		
Create a policy structure for every route-map name. Index to the policy structure is the route-map name	Device[]/route-map[name]	/Policy[name]
Create a rule structure under policy for every rm-instance indexed by seq-num	Device[]/route-map[name]/rm-instance[seqNum]	/Policy[name]<ingress>/Rule (SeqNum)
For every route-map stanza, a set operation can be mapped to a rule action	Device[]/route-map[name]/rm-instance[seqNum]/action	/Policy[name]<ingress>/Rule (SeqNum)/action
Each route-map can have multiple match criteria on an ACL level related to Layer 2 and Layer 3 headers	Device[]/route-map[name]/rm-instance[seqNum]/X'acl	/Policy[name]<ingress>/Rule(SeqNum)/X(12/ipv4/ipv6)
	Device[]/route-map[name]/rm-instance[seqNum]/X'acl/match	/Policy[name]/Rule (SeqNum)/X/match
Device[]/route-map[name]/rm-instance[seqNum]/X'acl/action	/Policy[name]<ingress>/Rule (SeqNum)/X/action	
<b>Interfaces per device</b>		
Bind policies to interfaces	Device[]/Ports[]/npb_bind	/ingress/Policy bind[name]

**Table 19: Advanced rule mapping for global features**

SLX I	SLX E	XVMI	XVME	Rule	SLX path	XVM path
<b>802.1BR header stripping:</b> Strip the 802.1BR header from ingress traffic and send it for processing						
Supported	Not supported	Supported	Supported	Add the decap traffic type for 802.1BR on the ingress port	Device[]/Ports[]<ingress>/<802.1BR strip>	/ingress[]/Traffic/TrafficDecap<802.1BR>
<b>VN-tag header stripping:</b> Strip the VN-tag from ingress traffic and send it for processing						
Supported	Not supported	Supported	Supported	Add the decap traffic type for the VN-tag on the ingress port	Device[]/Slots[]/Device-id[]/Ports[]/<vn-tag strip>	/ingress[]/Traffic/TrafficDecap<vn-tag>
<b>VxLAN header stripping:</b> Strip VxLAN from ingress traffic and send it for processing						
Supported	Not supported	Supported	Supported	Add the decap traffic type for the VxLAN on the ingress port	Device[]/Slots[]/Device-id[]/Ports[]/vxlan strip>	/ingress[]/Traffic/TrafficDecap<vxlan>
<b>NVGRE header stripping:</b> Strip NVGRE from ingress traffic and send for processing						
Supported	Not supported	Supported	Supported	Add the decap traffic type for NVGRE on the ingress port	Device[]/Slots[]/Device-id[]/Ports[]/<nvgre strip>	/ingress[]/Traffic/TrafficDecap<nvgre>
<b>GTP de-encapsulation:</b> Remove the outer IP, the outer UDP header, and the GTP header from GTP-U packets						
Supported	Not supported	Supported	Supported	Add the decap traffic type for GTP on the ingress port	Device[]/Slots[]/Device-id[]/Ports[]/<gtp decap>	/ingress[]/Traffic/TrafficDecap<gtp Decap>
<b>MPLS stripping:</b> Strip the outer headers (MPLS labels, outer L2, and the pseudo-wire control word) to prepare the inner headers and frame payload for forwarding and processing						
Supported	Not supported	Supported	Supported	Add the decap traffic type for MPLS on the ingress port	Device[]/Slots[]/Device-id[]/Ports[]/<mpls strip>	/ingress[]/Traffic/TrafficDecap<mpls strip>