



Extreme Visibility Manager Administration and User Guide

6.1.0

9037155-00 Rev AA
September 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

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/>



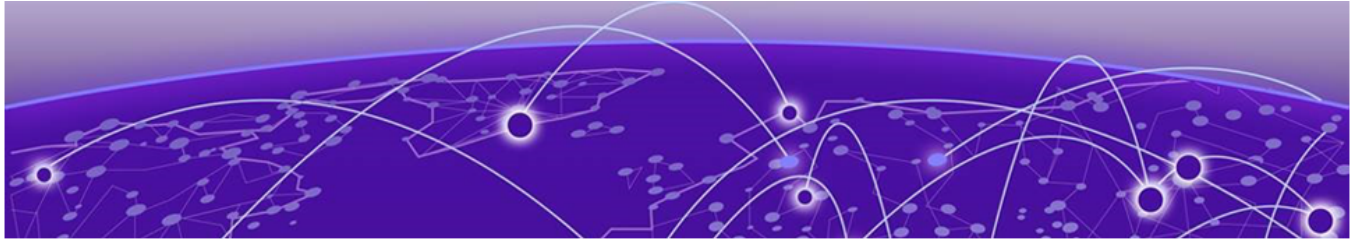
Table of Contents

Preface	7
Text Conventions.....	7
Documentation and Training.....	8
Help and Support.....	9
Subscribe to Product Announcements.....	9
Send Feedback.....	9
What's New In This Document	11
Getting Started	13
Extreme Visibility Manager Functions.....	13
Packet Broker Functions.....	15
Visibility Manager Deployment Model.....	16
Visibility Manager Microservices.....	19
Supported Devices and Software.....	22
Log in to Visibility Manager.....	22
The User Interface.....	23
Typical Device Configuration Workflow.....	25
The Library.....	26
Managing the System	27
Verify the System and Services.....	27
Microservice Logs.....	29
View System Logs.....	29
View User Logs.....	30
View System Monitoring Logs.....	31
TACACS+ Support.....	32
Configure TACACS+ for Web Interface Access.....	32
Configure TACACS+ for Device Access.....	33
Manage TACACS+ Authentication for Web Interface Access.....	33
Manage TACACS+ Authentication for Device Access.....	34
Map a TACACS+ Role.....	34
Change a TACACS+ Configuration.....	35
Change a Secret Key.....	35
Delete a TACACS+ Configuration.....	36
Delete a Mapped Role.....	36
User Roles.....	37
Add a User.....	37
Change a Password.....	38
Change a User Role.....	38
Delete a User.....	38
View the Logged-In User.....	39

Managing Device Types and Versions.....	40
Device Types and Versions.....	40
Add a Device Type File.....	41
Delete a Device Type File.....	41
View Device Type Files.....	41
Managing Devices.....	42
Add Devices	42
Create a Device Definition File.....	44
Delete a Device.....	45
Export the Device Configuration.....	45
Refresh Device Configuration.....	46
Save the Running Configuration of SLX and MLX Devices.....	46
Packet Capture.....	47
Start a PCAP on Extreme 9920 Devices.....	47
Start a PCAP on SLX Devices.....	47
Stop a PCAP.....	48
Clear Device Counters.....	49
Slot-Level Device Configuration.....	50
Configure MLX Device Slots.....	51
Upgrade Device Firmware.....	51
Delete a Firmware Upgrade Status.....	52
Reboot a Device After a Firmware Upgrade.....	52
Search, Group, and Sort Devices.....	52
Device Credentials.....	53
Monitoring Device Health and Statistics.....	54
Supported Device and Health Statistics.....	54
Device statistics.....	54
Device health management	55
View Statistics in a Device Dashboard.....	55
Create and Populate a Custom Dashboard.....	57
Delete a Custom Dashboard.....	57
View the Device Inventory.....	58
Download the Device Inventory.....	58
View Device Logs.....	59
Managing Device Ports and Port Channels.....	60
Create a Port Channel.....	60
Change a Port Channel.....	61
Delete a Port Channel.....	61
Configure Port Properties.....	62
Managing Egress and Egress Mirrors.....	64
Create Egress for SLX and MLX Devices.....	64
Create Egress for 9920 Devices.....	65
Configure a Traffic Mirror for 9920 Devices.....	65
Change an Egress or Mirror Configuration.....	66
Delete an Egress or Mirror Configuration.....	66
Managing Egress Groups.....	67
Create an Egress Group.....	67

Change an Egress Group.....	68
Delete an Egress Group.....	68
Managing Ingress Groups.....	69
Create an Ingress Group for an SLX or MLX Device.....	69
Create an Ingress Group for a 9920 Device.....	70
Change an Ingress Group.....	71
Delete an Ingress Group.....	71
Managing Policy Rule Matches.....	72
Create a Policy Rule Match for a Device.....	72
Create an MLX UDA Match for a Device.....	75
Create an SLX UDA Match for a Device.....	76
Create a Policy Rule Match in the Library.....	77
Create an MLX UDA Match in the Library.....	79
Create an SLX UDA Match in the Library.....	80
Change a Policy Rule Match.....	80
Import a Policy Rule Match to a Device.....	81
Export a Policy Rule Match.....	81
Clone a Policy Rule Match.....	81
Delete a Policy Rule Match.....	82
Search Policy Rule Matches.....	82
Managing Policies.....	83
Create an Egress Policy for a Device.....	83
Create an Ingress Policy for a Device.....	84
Create a Policy in the Library.....	85
Change a Policy.....	86
Import a Policy to a Device.....	86
Export a Policy.....	87
Clone a Policy.....	87
Delete a Policy.....	87
Search Policies.....	88
Managing User-Defined ACL Profiles.....	89
Create an MLX UDA Profile.....	89
Create an SLX UDA Profile.....	89
Change a UDA Profile.....	90
Clone a UDA Profile.....	90
Delete a UDA Profile.....	90
Search UDA Profiles.....	91
Managing Tunnels.....	92
Create a Tunnel.....	92
Change a Tunnel.....	93
Delete a Tunnel.....	93
Managing Locations.....	94
Upload a Location Definition File.....	94
Delete a Location.....	94
Search Locations.....	95
Rule and Functionality Mapping.....	96

MLX to Visibility Manager mapping.....	97
Extreme 9920 to Visibility Manager mapping.....	100
SLX to Visibility Manager mapping.....	104



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> .
Key names	Key names are written in boldface, for example Ctrl or Esc . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
Words in <i>italicized type</i>	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.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
<i>italic text</i>	Italic text indicates variable content.
[]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ x y z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	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/.

Help and Support

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

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.

Send Feedback

The Information Development team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, 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.
- Broken links or usability issues.

To send feedback, do either of the following:

- Access the feedback form at <https://www.extremenetworks.com/documentation-feedback/>.
- Email us at 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

The following table describes changes to this guide for the Extreme Visibility Manager 6.1.0 software release.

Table 4: Summary of changes

Feature	Description	Topic
IPv6	Support for devices with IPv6 addresses.	<ul style="list-style-type: none"> • Add Devices on page 42 • Create a Device Definition File on page 44
TACACS+	Support for TACACS+ for user authentication.	<ul style="list-style-type: none"> • TACACS+ Support on page 32 • Configure TACACS+ for Web Interface Access on page 32 • Configure TACACS+ for Device Access on page 33 • Map a TACACS+ Role on page 34 • Manage TACACS+ Authentication for Web Interface Access on page 33 • Change a TACACS+ Configuration on page 35 • Change a Secret Key on page 35 • Delete a TACACS+ Configuration on page 36 • Delete a Mapped Role on page 36
PCAP	Support for packet capture on SLX devices.	Start a PCAP on SLX Devices on page 47
UDA	Support for creating UDA profiles for SLX and MLX devices.	Managing User-Defined ACL Profiles on page 89
Configuration export	Support for exporting device configuration from an SLX or MLX device to an Extreme 9920 device.	Export the Device Configuration on page 45
SNMPv3	Support for discovering devices through SNMPv3.	<ul style="list-style-type: none"> • Add Devices on page 42 • Create a Device Definition File on page 44

Table 4: Summary of changes (continued)

Feature	Description	Topic
Running configuration	The feature once known as <i>persist configuration</i> is now called <i>save running configuration</i> .	Save the Running Configuration of SLX and MLX Devices on page 46
Custom dashboards	Support for deleting a custom dashboard.	Delete a Custom Dashboard on page 57
User logs	Support for viewing user log-in and log-out transactions.	View User Logs on page 30
System monitoring logs	Support for viewing system-generated alerts related to infrastructure resources and node health.	View System Monitoring Logs on page 31
Counters	Support for deleting specific counters.	Clear Device Counters on page 49
Inventory	Support for retrieving and viewing device details such as chassis and line card information.	<ul style="list-style-type: none"> • View the Device Inventory on page 58 • Download the Device Inventory on page 58
Location	Support for deleting locations.	Delete a Location on page 94
Egress interface	Support for VxLAN mirroring to an egress interface.	Configure a Traffic Mirror for 9920 Devices on page 65
Ingress group for Extreme 9920	Support for configuring inner and outer tunnels and associating a mirror.	Create an Ingress Group for a 9920 Device on page 70
Device slot configuration	Support for updating the slot configuration for MLX devices.	Slot-Level Device Configuration on page 50
Log filtering	Support for filtering the lists of system and device logs.	<ul style="list-style-type: none"> • View System Logs on page 29 • View Device Logs on page 59
Loopback	Support for configuring a loopback interface on SLX or MLX devices.	<ul style="list-style-type: none"> • Create a Port Channel on page 60 • Configure Port Properties on page 62
Firmware upgrade	Support for upgrading the firmware of a managed device.	<ul style="list-style-type: none"> • Upgrade Device Firmware on page 51 • Delete a Firmware Upgrade Status on page 52 • Reboot a Device After a Firmware Upgrade on page 52



Getting Started

[Extreme Visibility Manager Functions](#) on page 13

[Packet Broker Functions](#) on page 15

[Visibility Manager Deployment Model](#) on page 16

[Visibility Manager Microservices](#) on page 19

[Supported Devices and Software](#) on page 22

[Log in to Visibility Manager](#) on page 22

[The User Interface](#) on page 23

[Typical Device Configuration Workflow](#) on page 25

[The Library](#) on page 26

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 15.

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

Table 5: 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 Managing Device Ports and Port Channels on page 60.
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 Create Egress for SLX and MLX Devices on page 64 and Create Egress for 9920 Devices on page 65.
Egress group	A set of interfaces and ports on which traffic is forwarded after a policy is applied. For more information, see Create an Egress Group on page 67.
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 Managing Ingress Groups on page 69.
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 Create a Policy Rule Match for a Device on page 72.
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 Create an Ingress Policy for a Device on page 84.
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 Create an Egress Policy for a Device on page 83.

Table 5: Managed objects (continued)

Object	Description
User-defined access list (UDA)	The UDA profiles for SLX and MLX devices. For more information, see Managing User-Defined ACL Profiles on page 89.
Transport tunnel termination and encapsulation	The GRE or ERSPAN tunnels to associate with ingress groups or egress. For more information, see Create a Tunnel on page 92.

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 6: 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 Create a Policy Rule Match for a Device on page 72.
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 6: Packet broker functions (continued)

Function	Description
Transport tunnel termination	<ul style="list-style-type: none">• GRE (Generic Routing Encapsulation). Creates a tunnel that encapsulates (or wraps) packets that use one type of protocol inside packets that use a different protocol.• ERSPAN (Encapsulated Remote Switched Port Analyzer): Creates a tunnel that mirrors traffic from source ports for delivery to destination ports on a different device.
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, 6.1.0](#) 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.

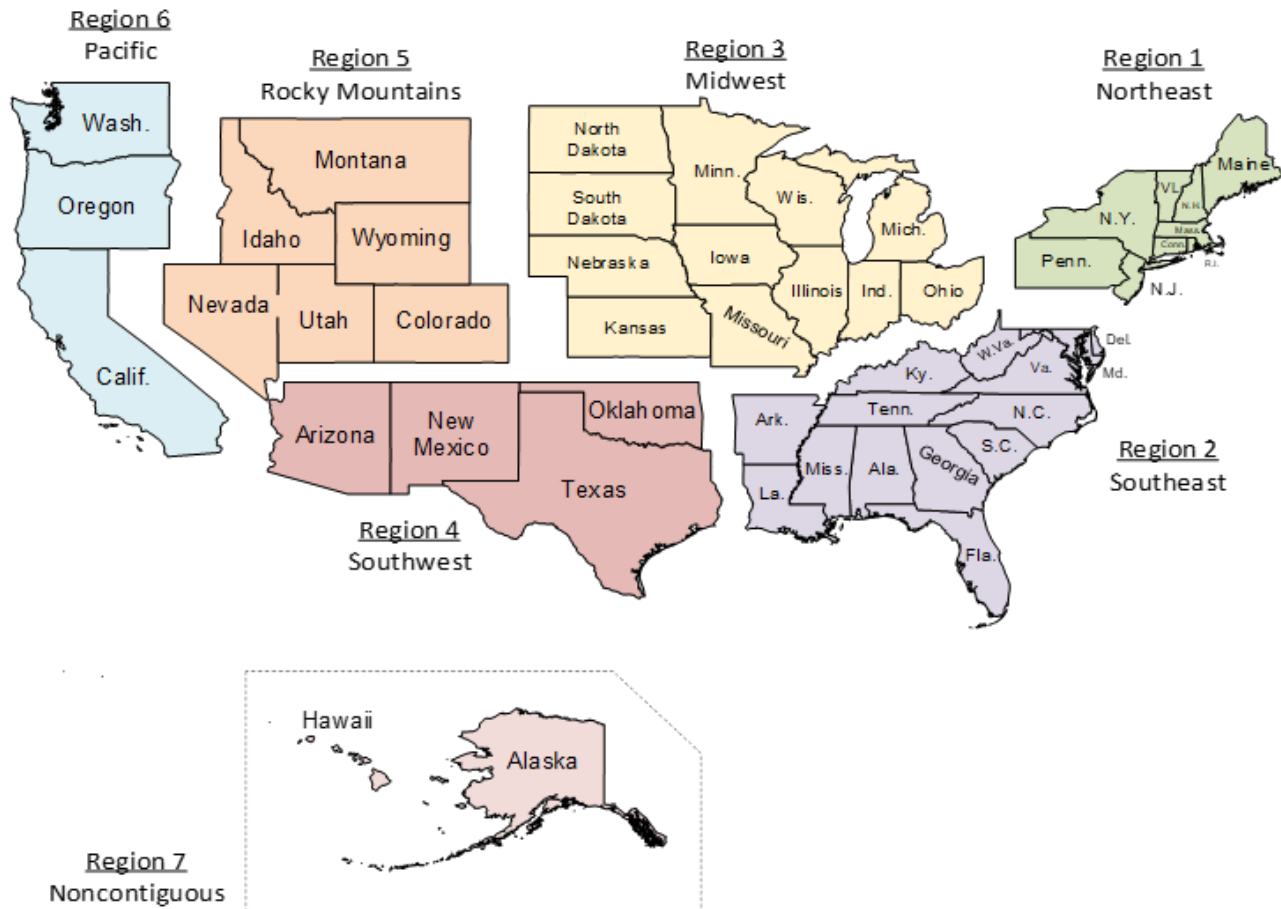


Figure 1: Regions and zones

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.

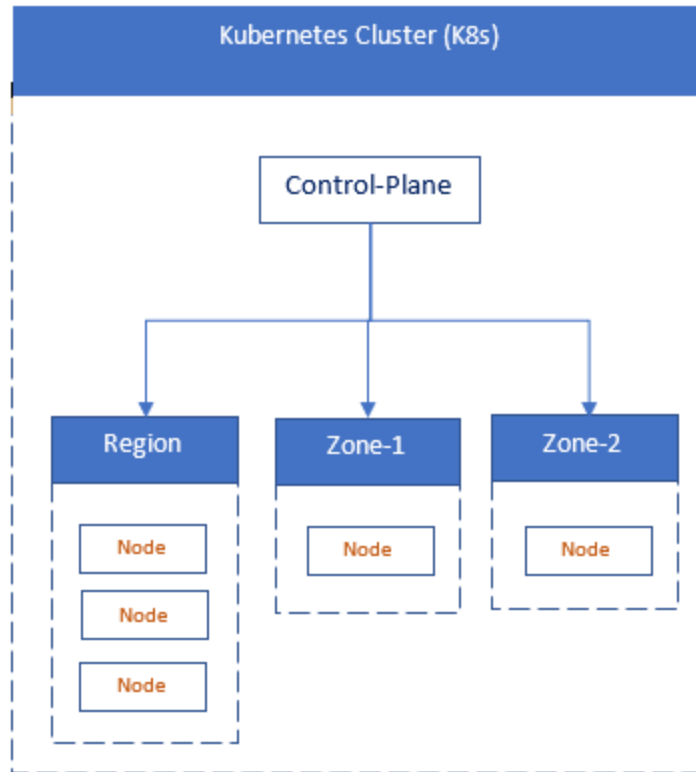


Figure 2: Cluster architecture

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

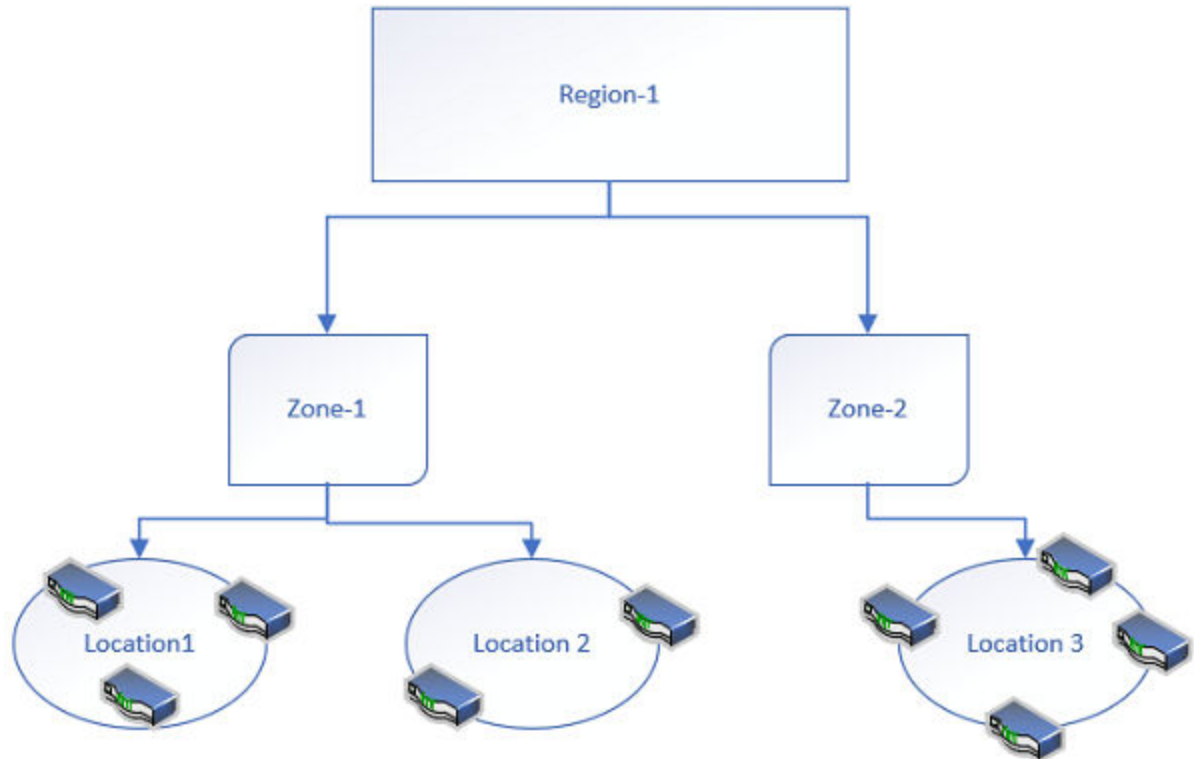


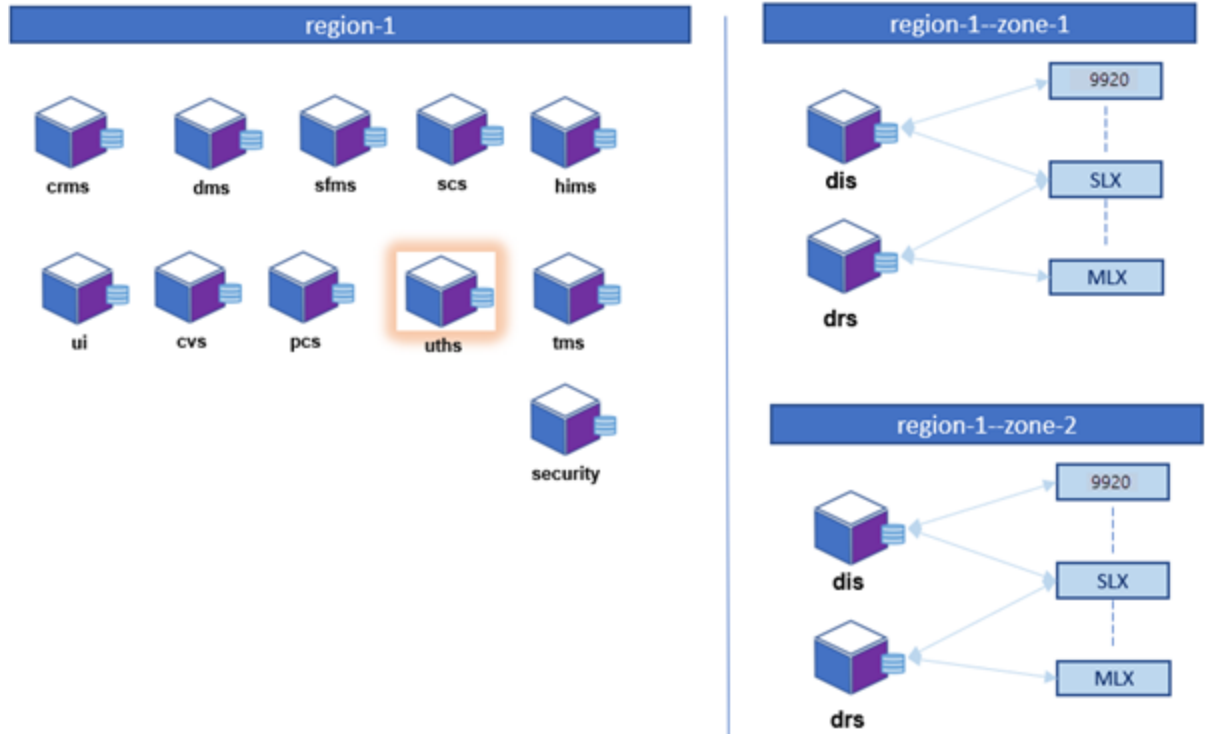
Figure 3: Zone architecture

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, 6.1.0](#).

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 29.

Table 7: Microservice functions

Microservice	Description
Cluster Resource Management Service (CRMS)	<ul style="list-style-type: none"> • Manages resources by providing unique identities for devices and configuration • Receives REST calls from the CVS to update the DTV message • Performs a lookup in the database to verify if the DTV is updated • Dynamically deploys microservices the zone nodes • Upgrades each microservice in a regional cluster • Maintains the location details for all microservices
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 7: Microservice functions (continued)

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

Table 7: 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"> • Maintains user transaction histories for audit trails on user activity • Provides progress on user actions through the Notification service in the user interface • Receives user transaction information from the DIS and the DRS

Supported Devices and Software

Extreme Visibility Manager supports several devices and their software.

Table 8: Supported devices and software

Visibility Manager Version	Supported Device	Supported Device Software
6.1.0	Extreme 9920	Extreme 9920 software with the NPB application, version 21.1.1.0.
6.0.0	Extreme 9920	Extreme 9920 software with the NPB application, version 21.1.0.x.
6.0.0, 6.1.0	ExtremeRouting MLX series	NetIron 6.3.00d
6.0.0, 6.1.0	ExtremeSwitching SLX 9140	<ul style="list-style-type: none"> • SLX-OS 18s.1.03a • SLX-OS 18s.1.03b • SLX-OS 18s.1.03c
6.0.0, 6.1.0	ExtremeSwitching SLX 9240	<ul style="list-style-type: none"> • SLX-OS 18s.1.03a • SLX-OS 18s.1.03b • SLX-OS 18s.1.03c

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.

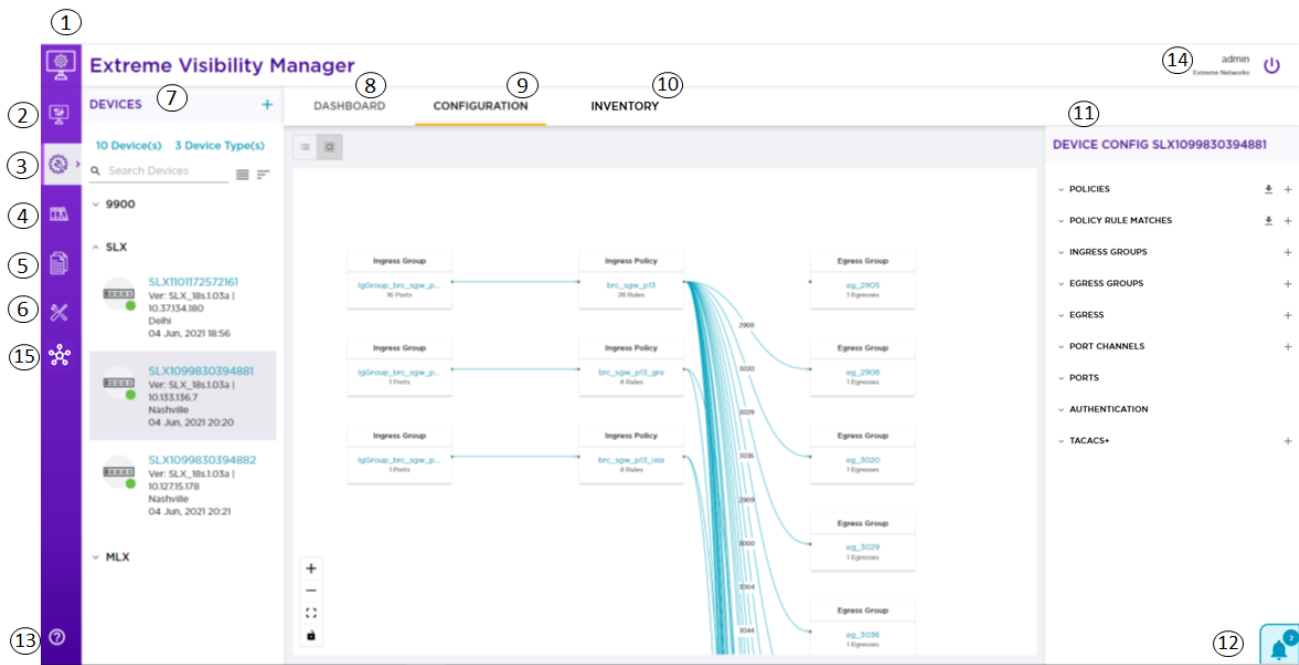


Figure 4: Visibility Manager user interface

Table 9: 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 Dashboard tab.
3	Configure page	Provides access to the Devices pane; the Dashboard, Configurations, and Inventory tabs; the Device Config menu; and configuration notifications.
4	Library page	Provides access to configured matches, policies, and UDA (user-defined ACL) profiles. From here, you can create matches, policies, and profiles (for MLX and SLX devices only), and then export them, clone them, edit them, and delete them.
5	Logs page	Provides access to information about all system logs and user logs, including device ID, IP address, and current and previous values.

Table 9: User interface descriptions (continued)

Legend	Interface Area	Description
6	Settings page	Provides access to settings for users, profile, AAA, and location. From here, you can perform such tasks as the following: <ul style="list-style-type: none"> • Add and delete users • Update user passwords • Add TACACS+ connection details • Enable remote authentication • View the logged-in user • Add location definition files
7	Devices pane	Displays the list of all discovered devices. From here, you can perform the following tasks: <ul style="list-style-type: none"> • Add devices and device types • Sort and group devices • Export and refresh device configurations • View device logs • Clear device counters • Configure packet captures • Persist the configuration of SLX and MLX devices
8	Dashboard tab	Provides access to device-specific, real-time statistics for interfaces, policies, and system usage.
9	Configurations 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	Inventory tab	Provides physical details for the selected device. Details vary by device type and can include some or all of the following: <ul style="list-style-type: none"> • Chassis, including type and serial number • Line card, including name and up time • Health, including system uptime and BIOS version • Thermal, including sensor name and current temperature • Fan, including status and speed • PSU, including name and status • LED, including name and state • Port, including slot number and admin status

Table 9: User interface descriptions (continued)

Legend	Interface Area	Description
11	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"> • Change port properties • Manage port channels • Manage policy rule matches • Manage egress groups and policies • Manage ingress groups and policies • Manage tunnels Is displayed in the interface after you discover a device.
12	Notifications	Displays a list of confirmation and error notifications for every configuration action you perform.
13	Help	Provides access to version information and help for the application.
14	Logout	Logs you out of the application.
15	Device Hub	Provides access to the firmware upgrade feature.

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 10: Configuration workflow

Configuration task	Described in
Add the Device Type Version Capability (DTVC) file	Add a Device Type File on page 41
Add devices	Add Devices on page 42
Add port channels and configure ports	Create a Port Channel on page 60 Configure Port Properties on page 62
Add egress	Create Egress for SLX and MLX Devices on page 64
Add egress groups and ingress groups	Create an Egress Group on page 67 Create an Ingress Group for an SLX or MLX Device on page 69
Add policy rule matches	Create a Policy Rule Match for a Device on page 72
Add policies	Create an Egress Policy for a Device on page 83 Create an Ingress Policy for a Device on page 84
Add tunnels	Create a Tunnel on page 92

The Library

The library provides access to policy rule matches, policies, and user-defined ACL (UDA) profiles (for SLX and MLX devices only).

Matches

A policy rule match identifies the parts of a packet header that a rule targets, such as the source port or the payload length. On the Matches page, you can see matches and their associated device type, rule type, and number of rules. The page provides access to match-related functions such as creating, exporting, cloning, and deleting. For more information, see [Managing Policy Rule Matches](#) on page 72.

Policies

Ingress and egress policies define the actions to apply to inbound and outbound packets. On the Policies page, you can see policies and their associated device type, policy type, and number of rules. The page provides access to policy-related functions such as creating, exporting, cloning and deleting. For more information, see [Managing Policies](#) on page 83.

UDA

A complete MLX or SLX UDA consists of a UDA profile and a UDA match. On the UDA page, you can see UDA profiles and their associated device type. Use the Matches page to work with UDA matches. The UDA page provides access to profile-related functions such as creating, cloning, and deleting. For more information, see [Managing User-Defined ACL Profiles](#) on page 89.



Managing the System

[Verify the System and Services](#) on page 27

[Microservice Logs](#) on page 29

[View System Logs](#) on page 29

[View User Logs](#) on page 30

[View System Monitoring Logs](#) on page 31

[TACACS+ Support](#) on page 32

[User Roles](#) on page 37

[Add a User](#) on page 37

[Change a Password](#) on page 38

[Change a User Role](#) on page 38

[Delete a User](#) on page 38

[View the Logged-In User](#) on page 39

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 11: 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

System logs describe 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

1. In the Navigation menu, select **Logs > System**.
2. To filter the list of logs by a specific device ID or component, take the following steps.
 - a. In the **Device ID** field, enter the complete ID that you want to find.
 - b. In the **Component** field, enter some or all of the component name that you want to find.
 - c. Select **Filter**.

View User Logs

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

About This Task

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

Table 12: User logs

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

Table 12: User logs (continued)

Log Type	Information Provided
Device Type	<ul style="list-style-type: none"> • User name • Action, such as add, update, or delete a DTVC file • Device type • Device type version • Location • Status, such as success or failed • Error message to explain a failure • Date
User Login	<ul style="list-style-type: none"> • User name • Action, such as log in or log out • User role • Log in time • Whether the action was successful

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**.
5. To view user transactions related to logging in, select **User Login**.

View System Monitoring Logs

System monitoring logs describe system-generated alerts related to infrastructure resources and node health.

About This Task

System monitoring logs provide the following information.

- Alert type and description
 - HostHighCPULoad: The CPU load on the host is greater than 80%.
 - HostOutOfMemory: The available memory on the host is less than 10%.
 - MongoDBClusterDown: The cluster is down and unable to connect.
 - MongoDBClusterUnhealthy: The cluster has no more than one member in a running state.
 - MongoDBReplicationLag: Replication lag is greater than 10 seconds.
 - PostgreSQLClusterUnhealthy: The cluster has no more than one member in a running state.
 - PostgreSQLReplicationUnhealthy: Replication is not working or is not configured.
- Severity
- Status
 - Firing: The component requires attention. Alerts are displayed on the System Monitoring Logs page when events have been sustained for three minutes.

- Resolved: The issue was resolved manually or automatically.
- Date

Procedure

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

TACACS+ Support

TACACS+ is an external authentication server used for verifying user credentials.

The TACACS+ (Terminal Access Controller Access-Control System Plus) protocols support environments that are configured for authentication, authorization, and accounting (AAA) services. When TACACS+ is configured through the Visibility Manager interface, TACACS+ users can log in to Visibility Manager interface.

Visibility Manager supports TACACS+ authentication in the following ways.

- Visibility Manager supports up to four TACACS+ servers for authentication purposes and contacts them in the order in which they were configured. When one server is unreachable, failover to the next server can occur.
- The user roles specified in the TACACS+ server configuration can be one of the following.
 - One of the supported Visibility Manager roles, System Admin and Network Operator. For more information, see [User Roles](#) on page 37.
 - A local TACACS+ role that you can map to Visibility Manager. For more information, see [Map a TACACS+ Role](#) on page 34.
- If TACACS+ authentication fails because an unsupported or unmapped role was assigned, the Network Operator role is assigned by default.
- Remote authentication must be enabled. For more information, see [Manage TACACS+ Authentication for Web Interface Access](#) on page 33. If remote authentication is not enabled, only local authentication is used.
- If remote authentication fails, Visibility Manager attempts to use local authentication, which is successful only if the user is in the Visibility Manager database.
- The secret key configured for Visibility Manager must be the same as the secret key from the TACACS+ server configuration file. Authentication fails if the two values do not match.
- Visibility Manager supports two TACACS+ authentication protocols.
 - **CHAP**: Challenge Handshake Authentication Protocol
 - **PAP**: Password Authentication Protocol

Configure TACACS+ for Web Interface Access

You can add TACACS+ connection details so that TACACS+ users can sign in to the Visibility Manager interface.

Procedure

1. In the Navigation menu, select **Settings > AAA**.
2. Select **Add TACACS+**.
3. In the **Host** field, enter the IPv4 or IPv6 address of the TACACS+ server, in CIDR format.

4. In the **Authentication Port** field, enter the TCP port used for authentication.
The default authentication port is 49.
5. In the **Secret Key** field, enter the shared secret that enables messages between the client and the TACACS+ server.
The value you enter must match the shared secret in the TACACS+ server configuration file.
6. In the **Protocol** field, select one of the following authentication protocols.
 - **CHAP**: Challenge Handshake Authentication Protocol
 - **PAP**: Password Authentication Protocol
7. Save (✓) your selections.
The AAA page displays the new configuration.

Configure TACACS+ for Device Access

You can add TACACS+ connection details so that TACACS+ users can sign in to a device using such methods as SSH or Telnet.

Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device you want to configure.
3. Select the **Configurations** tab.
4. In the Device Config menu, select **Add TACACS+**.
5. In the **Host** field, enter the IPv4 or IPv6 address of the TACACS+ server, in CIDR format.
6. In the **Secret** field, enter the shared secret that enables messages between the client and the TACACS+ server.
The value you enter must match the shared secret in the TACACS+ server configuration file.
7. Save (✓) your selections.

Manage TACACS+ Authentication for Web Interface Access

For support of the TACACS+ servers you have configured, you must enable TACACS+ authentication.

Before You Begin

Configure at least one TACACS+ server. For more information, see [Configure TACACS+ for Web Interface Access](#) on page 32.

Procedure

1. In the Navigation menu, select **Settings > AAA**.
2. To activate the feature, slide the **Enable** button to the right.
3. To deactivate the feature, slide the **Enable** button to the left.
Deactivating the feature automatically enables local authentication.

Manage TACACS+ Authentication for Device Access

For support of the TACACS+ servers you have configured, you must enable TACACS+ authentication.

Before You Begin

Configure at least one TACACS+ server. For more information, see [Configure TACACS+ for Device Access](#) on page 33.

About This Task

An Extreme 9920 device has no default value for authentication in its running-configuration file, so you must explicitly enable TACACS+ authentication when you add a TACACS+ server. The default authentication value for SLX and MLX devices is always local, so you explicitly change the authentication to TACACS+ when you add a TACACS+ server.

Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device you want to configure.
3. Select the **Configurations** tab.
4. (9920 only) To enable TACACS+ authentication, take the following steps.
 - a. In the Device Config menu, select **Add Authentication**.
 - b. In the **Authentication Type** field, select **TACACS**.
 - c. To allow the device to use local authentication if TACACS+ authentication fails, select **Local Auth Fallback**.
 - d. Save (✓) your selections.
5. (9920 only) To remove TACACS+ authentication, take the following steps.
 - a. In the Device Config menu, expand **Authentication** and select **Delete Authentication**.
6. (SLX and MLX only) To change authentication from local to TACACS+, take the following steps.
 - a. In the Device Config menu, expand **Authentication** and select **Local**.
 - b. In the **Authentication Type** field, select **TACACS**.
 - c. To allow the device to use local authentication if TACACS+ authentication fails, select **Local Auth Fallback**.
 - d. Save (✓) your selections.
7. (SLX and MLX only) To change authentication from TACACS+ to local, take the following steps.
 - a. In the Device Config menu, expand **Authentication** and select **TACACS**.
 - b. In the **Authentication Type** field, select **Local**.
 - c. Save (✓) your selections.

Map a TACACS+ Role

You can map a local TACACS+ role to one of the built-in Visibility Manager roles.

Procedure

1. In the Navigation menu, select **Settings > AAA**.
2. Select **Add TACACS+ Role**.
3. In the **XVM Role** field, select the role to which you want to map the local TACACS+ role.

4. In the **TACACS+ Role** field, enter the name of the local role.
5. Save (✓) your selections.

The AAA page displays the new mapping.

Change a TACACS+ Configuration

You can change the configuration for access to a device and for access to the Visibility Manager interface.

Procedure

1. To change the configuration for access to the interface, take the following steps.
 - a. In the Navigation menu, select **Settings > AAA**.
 - b. In the TACACS+ section, select **Edit TACACS+** for the configuration that you want to change.
 - c. Complete the **Host**, **Authentication Port**, and **Protocol** fields as described in [Configure TACACS+ for Web Interface Access](#) on page 32.
 - d. Save (✓) your selections.

The AAA page displays the changed configuration.
2. To change the configuration for access to a device, take the following steps.
 - a. In the Navigation menu, select **Configure**.
 - b. In the Devices panel, select the device you want to configure.
 - c. Select the **Configurations** tab.
 - d. In the Device Config menu, expand **TACACS+** and select the IP address of the TACACS+ server you want to configure.
 - e. Complete the **Host** and **Secret** fields as described in [Configure TACACS+ for Device Access](#) on page 33.
 - f. Save (✓) your selections.

Change a Secret Key

You can change the secret key for access to a device and for access to the Visibility Manager interface.

About This Task

If you change the shared secret in the TACACS+ server configuration file, you must also change the secret key in Visibility Manager.

Procedure

1. To change the secret key for access to the interface, take the following steps.
 - a. In the Navigation menu, select **Settings > AAA**.
 - b. In the TACACS+ section, select **Update Secret Key** for the configuration that you want to change.
 - c. In the **New Secret Key** field, enter the shared secret from the TACACS+ configuration file.
 - d. Save (✓) your selections.
2. To change the secret key for access to a device, take the following steps.
 - a. In the Navigation menu, select **Configure**.
 - b. In the Devices panel, select the device you want to configure.

- c. Select the **Configurations** tab.
- d. In the Device Config menu, expand **TACACS+** and select the IP address of the TACACS+ server you want to configure.
- e. In the **Secret** field, enter the shared secret from the TACACS+ configuration file.
- f. Save (✓) your selections.

Delete a TACACS+ Configuration

You can delete a configured TACACS+ host for a device and you can delete the TACACS+ configuration for access to the Visibility Manager interface.

Procedure

1. To delete the configuration for access to the interface, take the following steps.
 - a. In the Navigation menu, select **Settings > AAA**.
 - b. In the TACACS+ section, select **Delete TACACS+** for the configuration that you want to delete.
2. To delete a TACACS+ host for a device, take the following steps.
 - a. In the Navigation menu, select **Configure**.
 - b. In the Devices panel, select the device you want to configure.
 - c. Select the **Configurations** tab.
 - d. In the Device Config menu, expand **TACACS+**.
 - e. Select **Delete TACACS+ Host** for the IP address of the host you want to delete.

Delete a Mapped Role

When you delete a mapped role, TACACS+ users with that local role cannot log in to Visibility Manager.

Procedure

1. In the Navigation menu, select **Settings > AAA**.
2. In the TACACS+ Role Mapping section, select **Delete** for the mapping that you want to delete.

User Roles

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

Table 13: 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"> • Add and view device types and devices • Add and view device configuration and DTVC files • Add and view custom dashboards • Configure and View built-in dashboards • Configure TACACS+ for Visibility Manager and for devices • Add and view users • Change user passwords • Change user roles • View location details • Configure and view the library • View event notifications • Sort device lists <p>The default Visibility Manager user, <code>admin</code>, 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"> • View device types and devices • View device configuration and DTVC files • View custom and built-in dashboards • Add and view users • Change own password • View users • View location details • View the library • View event notifications • Sort device lists

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 37.
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 37.
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 40

[Add a Device Type File](#) on page 41

[Delete a Device Type File](#) on page 41

[View Device Type Files](#) on page 41

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, 6.1.0](#).

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 41.

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, 6.1.0](#).

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 42

[Create a Device Definition File](#) on page 44

[Delete a Device](#) on page 45

[Export the Device Configuration](#) on page 45

[Refresh Device Configuration](#) on page 46

[Save the Running Configuration of SLX and MLX Devices](#) on page 46

[Packet Capture](#) on page 47

[Clear Device Counters](#) on page 49

[Slot-Level Device Configuration](#) on page 50

[Upgrade Device Firmware](#) on page 51

[Search, Group, and Sort Devices](#) on page 52

[Device Credentials](#) on page 53

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 (discover) 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 41.

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](#).

To be able to discover MLX or SLX devices with SNMPv3 credentials, configure the SNMPv3 user name, authorization protocol and password, and privacy protocol and password on those devices.

A device can be managed by only one instance of Visibility Manager. Before adding a device, ensure that it is deleted from any other Visibility Manager instance that is managing it.

About This Task

This topic describes device discovery for the following scenarios.

- SLX, MLX, and Extreme 9920 devices with no device credentials
- Extreme 9920 devices with user name and password credentials
- SLX and MLX devices with SNMPv2c credentials
- SLX and MLX devices with SNMPv3 credentials

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 one device, complete the following fields.
 - a. In the **IP Address** field, enter the IPv4 or IPv6 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. To discover the device with no credentials, skip to step 5 on page 43.
 - e. To discover the device with credentials, select **Additional Fields** and complete the following fields as appropriate.

Field	Device	Protocol	Description
Username, Password	All	None	Does not need to be the user name and password of the default user.
SNMP Version	SLX, MLX	SNMPv2c, SNMPv3	Select v2c or v3 .
Community String	SLX, MLX	SNMPv2c	Enter <code>default</code> if public or enter the community string if not public.
SNMP Username	SLX, MLX	SNMPv3	Up to 32 characters.
Auth Protocol	SLX, MLX	SNMPv3	Select MD5 or SHA . ¹
Auth Password	SLX, MLX	SNMPv3	For MD5, between 8 and 16 characters. For SHA, between 8 and 20 characters.
Privacy Protocol	SLX, MLX	SNMPv3	Select DES or AES . ²
Privacy Password	SLX, MLX	SNMPv3	Between 8 and 16 characters.

5. Select **Add**.

¹ MD5 (Message Digest Algorithm) and SHA (Secure Hash Algorithm)

² DES (Data Encryption Standard) and AES (Advanced Encryption Standard)

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. Each row in the CSV file has a variation of the following format. Field numbers 10 through 14 apply to SNMPv3 only.

```
<IPAddresses>,<DeviceType>,<DeviceVersion>,<Location>,<ConfigProtocol>,<DiscoveryProtocol>,<UserName>,<Password>,<CommunityString>,<SNMPUserName>,<AuthProtocol>,<AuthPassword>,<PrivacyProtocol>,<PrivacyPassword>
```

Table 14: Field descriptions

Field Number	Field	Description
1	IPAddresses	One or more IPv4 or IPv6 addresses, separated by commas.
2	DeviceType	SLX, MLX, or 9900.
3	DeviceVersion	The version of the operating system on the device in the following format: <device-type>_<version>. For example: SLX_18s.1.03a.
4	Location	One of the locations in the locations.csv file. For more information, see the Extreme Visibility Manager Deployment Guide, 6.1.0 .
5	ConfigProtocol	SSH
6	DiscoveryProtocol	SNMP
7	UserName	Credentials for accessing the device, and not necessarily the credentials of the default user.
8	Password	Credentials for accessing the device, and not necessarily the credentials of the default user.
9	CommunityString	(SNMPv2 only) Enter default or enter the community string if not public. (SNMPv3 only) Enter snmpv3.
10	SNMPUserName	(SNMPv3 only) Up to 32 characters.
11	AuthProtocol	(SNMPv3 only) MD5 or SHA.
12	AuthPassword	(SNMPv3 only) For MD5, between 8 and 16 characters. For SHA, between 8 and 20 characters.

Table 14: Field descriptions (continued)

Field Number	Field	Description
13	PrivacyProtocol	(SNMPv3 only) DES or AES
14	PrivacyPassword	(SNMPv3) Between 8 and 16 characters.

Procedure

1. Create a CSV file with a file name of your choosing.
2. Add content to the file in the described format.
3. Save the CSV file to a location that is accessible from the Visibility Manager user interface.

Example

Sample entries with SNMPv2 credentials.

```
2620:100:c:fe08::110,SLX,SLX_18s.1.03a,Duff,SSH,SNMP,admin,password,default
2620:100:c:fe08::111,MLX,MLX_v6.3.00bd,Duff,SSH,SNMP,admin,admin,default
10.37.128.70,SLX,SLX_18s.1.03a,Duff,SSH,SNMP,admin,password,default
```

Sample entries with SNMPv3 credentials.

```
10.37.128.249,MLX,MLX_v6.3.00bd,Duff,SSH,SNMP,admin,admin,snmpv3,xvmuser,
SHA,shapass12,DES,despass12

10.37.128.72,SLX,SLX_18s.1.03a,Duff,SSH,SNMP,admin,password,snmpv3,xvmuser,SHA,
shapass12,DES,despass12
```

Delete a Device

You can remove one or more devices from Visibility Manager.

Procedure

1. In the Navigation menu, select **Configure**.
2. To delete multiple devices, take the following steps.
 - a. In the Devices panel, select **Device(s)**.
 - b. Select the devices to delete.
 - c. Select **Delete**.
3. To delete one device, right-click the device and select **Delete Device**.

Export the Device Configuration

You can export the configuration of an SLX or MLX device to an Extreme 9920 device.

About This Task

In general, the following configuration is exported:

- Policy rule matches (IPv4, IPv6 and L2 only)
- Policies
- Ingress group

- Egress
- Egress group

The following configuration items are not exported. These items appear in red text on the Export Configuration page.

- Special characters such as %, {, }, \, and = are not supported on the Extreme 9920 device. Policies and rule matches are not exported when the names of those items contain special characters.
- User-defined access lists (UDA) are not supported on the Extreme 9920 device and are not exported.

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.

The configuration of the source device is displayed.

Items in red text will not be exported.

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

5. Select all required ports.
6. Save (✓) your selections.

The configuration is exported to the destination device.

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**.

Save the Running Configuration of SLX and MLX Devices

You can save the running configuration of SLX and MLX devices to Visibility Manager.

Procedure

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

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

Packet Capture

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

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

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.

For more information, see the following topics:

- [Start a PCAP on Extreme 9920 Devices](#) on page 47
- [Start a PCAP on SLX Devices](#) on page 47
- [Stop a PCAP](#) on page 48

Start a PCAP on Extreme 9920 Devices

PCAP information from a 9920 device is displayed 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 **Start**.
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, from 1 to 8,000.

Packet capture stops when the selected number of packets has been captured.

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.

Start a PCAP on SLX Devices

PCAP information from an SLX device is captured in a file that you can download.

Before You Begin

Because PCAP for SLX devices is supported on only one port at a time, you must stop an existing PCAP before you can begin a new one. For more information, see [Stop a PCAP](#) on page 48.

About This Task

Every SLX packet capture overwrites the previous PCAP file.

Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, right-click an SLX device and select **Packet Capture**.
3. Select **Configure Port Capture**.
4. Select **Start**.
5. In the **Port** field, select a port on which to capture packets.
6. Select whether to collect **Ingress** packets or **Egress** packets.
7. In the **Packet Count** field, select the number of packets that you want to capture, from 1 to 8,000.

Packet capture stops when the selected number of packets has been captured.

8. Select **Add**.
The capture configuration is displayed on the right.
9. Save (✓) your changes.
The Packet Capture page displays the PCAP file.
10. To download the file when the PCAP is complete, take the following steps.
 - a. Select **Download**.
 - b. In the **Host IP** field, enter the IP address of a device that is accessible from the SLX device.
 - c. In the **User Name** and **Password** fields, provide the device credentials.
 - d. In the **Path** field, provide the download file path.
 - e. In the **Filename** field, provide a name for the file.
This optional step allows you to provide a user-friendly file name.
 - f. Save (✓) your changes.

Stop a PCAP

For SLX devices, you must stop the existing PCAP before you can begin a new one. 9920 devices support up to 10 running PCAPs before you need to delete one, although you do not need to reach the limit of 10 before deleting a PCAP.

Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, right-click a device and select **Packet Capture**.
3. Select **Configure Port Capture**.
The configuration for the running PCAPs are displayed on the right.
4. Select the PCAP that you want to stop.
5. Select **Stop**.
6. Save (✓) your changes.

Clear Device Counters

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

About This Task

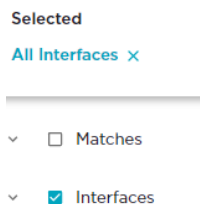
Counters track the number of times a certain event or process occurs. Counters increase over time and you can delete them as needed. For all devices, you can clear all counters of a selected type. For some devices, you can also clear specific counters of a selected type.

Table 15: Support for clearing counters

	9920	SLX	MLX
Clear all counters	<ul style="list-style-type: none"> • Interface • Match • Egress group • Ingress group • Egress • Ingress policy • Egress policy • Transport tunnel • Tunnel encapsulation 	<ul style="list-style-type: none"> • Interface • Match 	<ul style="list-style-type: none"> • Interface • Match
Clear specific counters	<ul style="list-style-type: none"> • Interface • Match • Egress group • Ingress group • Egress • Ingress policy • Egress policy • Transport tunnel • Tunnel encapsulation 	<ul style="list-style-type: none"> • Interface • Match 	<ul style="list-style-type: none"> • Interface

Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, right-click a device and select **Clear Counters**.
3. To clear all counters of one type, select the check box for that type.



- To clear specific counters of one type, expand the type and select the check boxes for the counters.

Selected

3 Interfaces x

∨ Matches

∧ Interfaces

🔍 Search Interfaces

Ethernet 0/1

Ethernet 0/2

Ethernet 0/3

Ethernet 0/4

- Save (✓) your selections.

Reports in the dashboards are updated to reflect your selections.

Slot-Level Device Configuration

You can view and update the configuration of the slots for a selected MLX device.

For a selected processor of the selected device, you can change the slot configuration for header stripping, packet slicing, and packet length matching. All available slots are displayed in the Visibility Manager user interface in the Device Config menu.

∨ AUTHENTICATION

∨ TACACS+

∧ SLOTS

[Slot 1](#)

[Slot 2](#)

[Slot 3](#)

You can refresh the configuration of a selected device to update the list of slots. For more information, see [Refresh Device Configuration](#) on page 46.

In the list, each instance of a slot is a link that opens the configuration page. The right side of the page displays the current configuration for each processor in the device.

The screenshot shows a configuration window titled "Slot : Slot 1". On the left, there are three sections: "PROCESSOR" with a "Processor*" dropdown; "HEADER STRIPPING" with a "Headers" dropdown; and "PACKET SLICING" with "Truncate Egress Ports" and "Truncate Size" dropdowns. At the bottom of this panel are "CLEAR" and "ADD" buttons. On the right, there is a "Search Config" search bar and a list of configurations. "PROCESSOR 1" has "Headers: BR802.VN1AG", "Truncate Egress Ports: ethernet 1/1", and "Truncate Size: 90". "PROCESSOR 2" has "Headers: BR802", "Truncate Egress Ports: ethernet 1/1", and "Truncate Size: 90". Each configuration entry has edit and delete icons.

Configure MLX Device Slots

You can change the slot configuration for header stripping, packet slicing, and packet length matching.

Before You Begin

If necessary, refresh the list of slots. For more information, see [Refresh Device Configuration](#) on page 46.

Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device you want to configure.
3. Select the **Configurations** tab.
4. In the Device Config menu, expand **Slots** and select the slot you want to configure.
5. In the **Processor** field, select the processor you want to update.
6. In the **Header Stripping** field, select one or more headers to strip.
7. In the **Packet Slicing** fields, select one or more egress ports and then select a value to represent the maximum packet size after slicing.
The final packet size will be less than or equal to this value.
8. Select **Add** to save your changes.
9. Repeat steps 5 on page 51 through 8 to change the configuration of other processors on the device.
10. Save (✓) your selections.

Upgrade Device Firmware

You can upgrade the firmware version of a managed device from the Visibility Manager user interface.

About This Task

The version to which you are upgrading the firmware must be represented in the DTVC file for the related device. For more information, see [Device Types and Versions](#) on page 40.

Procedure

1. In the Navigation menu, select **Device Hub > Firmware Upgrade**.
2. Select **Configure Firmware Upgrade**.

3. In the **Device Type** field, select the type of device to upgrade.
4. In the **Location** field, select the device location.
5. In the **Devices** field, select one or more devices to upgrade.
6. Select **Reboot** to reboot the device after upgrade.

**Note**

Rebooting is mandatory for 9920 devices. Rebooting is optional for SLX and MLX devices.

7. In the **IP Address** field, enter the IP address of the remote server where the firmware image is located.
8. In the **Absolute Path** field, enter the complete file path to the location of the firmware image. The following are sample file paths for the various supported device firmware images.

9920 (absolute path to the binary file): `/root/TierraOS-<version>-NPB.bin`

SLX (absolute directory path where supported image files are located): `/root/slxos18s.1.03/slxos18s.1.03a`

MLX (path to the manifest file): `XMR-MLX/MLX_npb_06200_mnf.txt`

9. In the **Username** and **Password** fields, enter the credentials for the remote server.
10. Save (✓) your selections.
Firmware upgrade begins and the device state changes to maintenance mode. You cannot perform any configuration operations during this time. Firmware upgrade takes several minutes and you can see the progress of the upgrade in the Upgrade Status table on the Firmware Upgrade page.

Delete a Firmware Upgrade Status

The statuses of all firmware upgrades remain in the Visibility Manager database until you delete them.

Procedure

1. In the Navigation menu, select **Device Hub > Firmware Upgrade**.
2. In the Upgrade Status table, select the row for the status that you want to delete.
3. Select **Delete**.

Reboot a Device After a Firmware Upgrade

You can manually reboot an SLX or MLX device after a firmware upgrade.

Procedure

1. In the Navigation menu, select **Device Hub > Firmware Upgrade**.
2. In the Upgrade Status table, select the row for the SLX or MLX device that you want to reboot.
3. Select **Reboot**.

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.

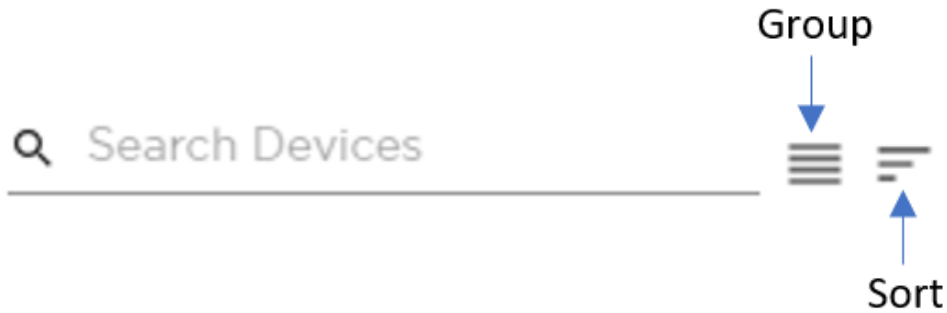


Figure 5: Search, group, and sort

Procedure

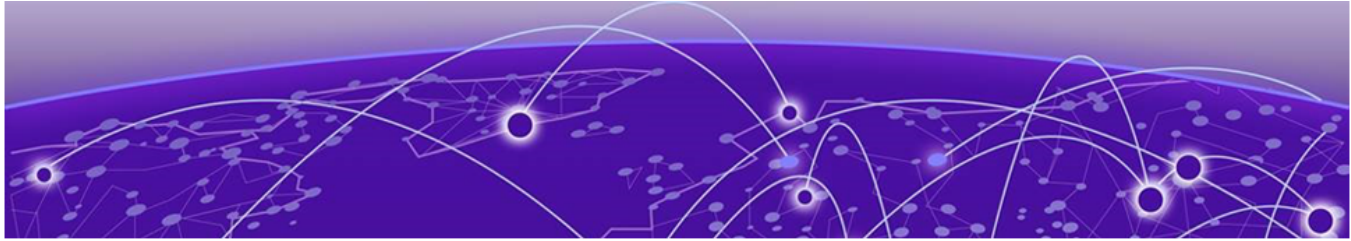
1. In the Navigation menu, select **Configure**.
2. To search for a device, enter a device attribute in the **Search Devices** field.
For example, enter a device name.
As you begin typing, the list is filtered to match your search word or phrase.
3. To group devices, select **Group > Group By Location** 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 54](#)

[View Statistics in a Device Dashboard on page 55](#)

[Create and Populate a Custom Dashboard on page 57](#)

[Delete a Custom Dashboard on page 57](#)

[View the Device Inventory on page 58](#)

[Download the Device Inventory on page 58](#)

[View Device Logs on page 59](#)

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 19.

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 16: 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

Table 16: Supported statistics by device type (continued)

Statistic	9920	SLX	MLX
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 54. 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.

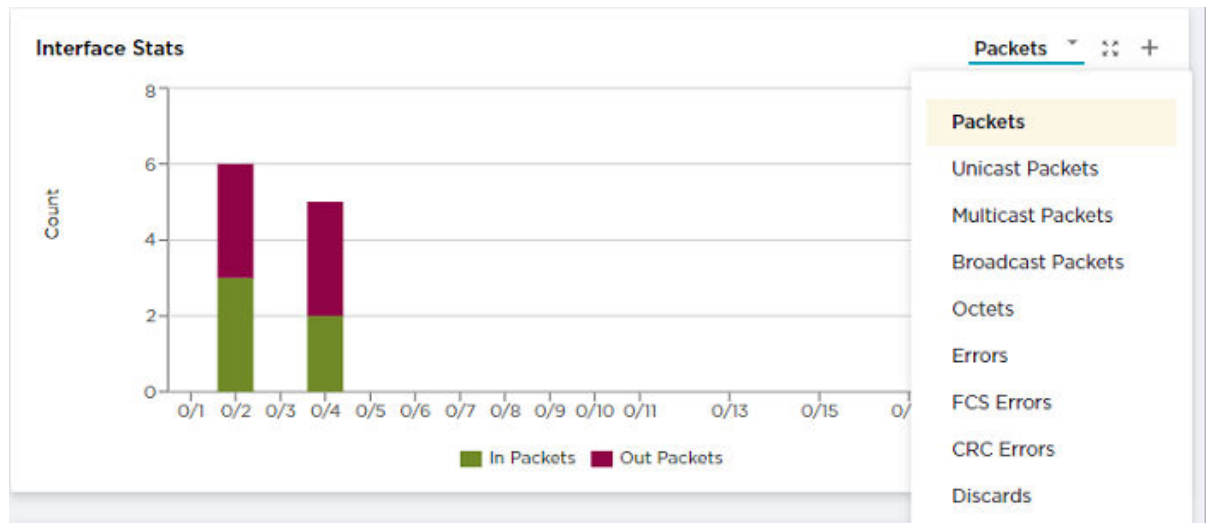


Figure 6: Statistics list

- 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.

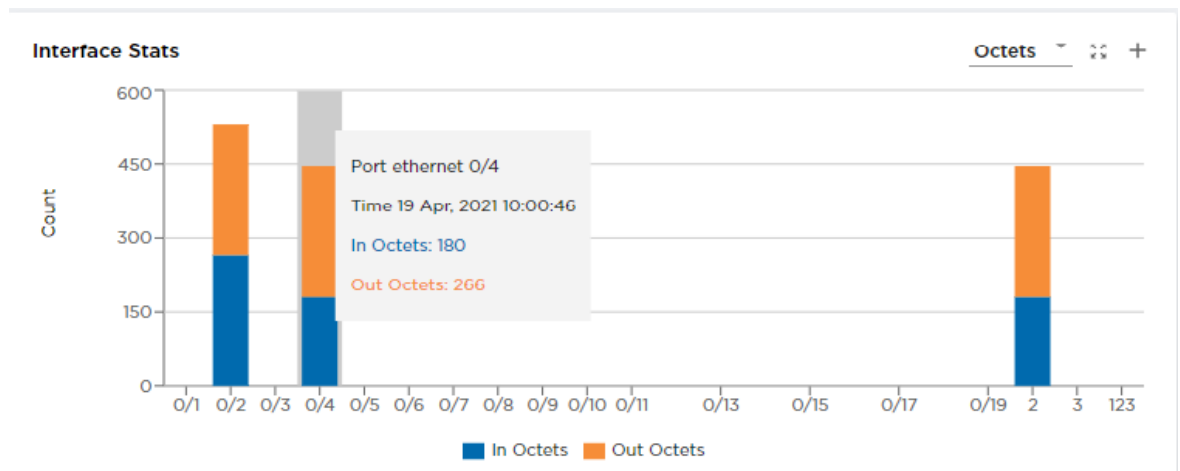


Figure 7: Statistics details

- 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 57.

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 55.
 - 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 57 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.

Delete a Custom Dashboard

You can delete any custom dashboard.

Procedure

1. In the Navigation menu, select **Dashboard**.
2. Select the **Dashboards** link.

The Manage Dashboards page opens.
3. Select **Delete Dashboard** for the dashboard you want to delete.

View the Device Inventory

The Inventory tab displays device details, such as chassis and line card.

About This Task

Device details are displayed in cards by information type, which varies by the device you select. Different devices provide different information. Device details can include some or all of the following:

- Chassis, including type and serial number
- Line card, including name and up time
- Health, including system uptime and BIOS version
- Thermal, including sensor name and current temperature
- Fan, including status and speed
- PSU, including name and status
- LED, including name and state
- Port, including slot number and admin status

Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices pane, select a device.
3. Select the **Inventory** tab.

The lists of details vary by device. The following is an example.

DASHBOARD CONFIGURATIONS **INVENTORY**

The screenshot displays the Inventory tab with the following sections:

- Chassis Information:** Name: MLX9 9-slot, Last Updated: 16 Aug, 2021 15:09, Type: MLX9 9-slot, Serial Number: 0G92529L00C, Part Number: 4P-1000962-04.
- Line Card Information:** LINECARD-1, Name: linecard-1, Last Updated: 16 Aug, 2021 15:09, Type: 8P-MLX-10Gx20 3D-port 1/10/5GE, Serial Number: -, Part Number: -, Firmware Revision: -.
- Fan Information:** FAN UNIT A-1, Name: Fan Unit A-1, Last Updated: 16 Aug, 2021 15:09, Status: OK, Speed: LOW (50%), FAN UNIT A-2, FAN UNIT B-1.
- PSU Information:** PS UNIT 1, Name: PS Unit 1, Last Updated: 16 Aug, 2021 15:09, Type: -, Status: not present, PS UNIT 2, PS UNIT 3.
- Port Information:** SLOT-1 table with columns: NAME, ADMIN STATUS, OPER STATUS, ENABLED, SPEED.

NAME	ADMIN STATUS	OPER STATUS	ENABLED	SPEED
ethernet 1/1	UP	UP	TRUE	UNKNOWN
ethernet 1/2	UP	UP	TRUE	UNKNOWN

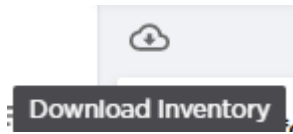
Download the Device Inventory

You can download a device's inventory to a spreadsheet.

Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices pane, select a device.
3. Select the **Inventory** tab.

4. In the upper left corner of the tab, select **Download Inventory**.



A file in .xlsx format is downloaded to your device.

View 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 the logs for a device, take the following steps.

Procedure

1. In the Navigation menu, select **Configure**.
2. Right-click the device and select **View Logs**.
3. To filter the list of logs by a specific message or severity level, take the following steps.
 - a. In the **Message** field, enter some or all of the message text that you want to find.
 - b. In the **Severity** field, enter the full text of the severity level that you want to find.
 - c. Select **Filter**.



Managing Device Ports and Port Channels

[Create a Port Channel on page 60](#)

[Change a Port Channel on page 61](#)

[Delete a Port Channel on page 61](#)

[Configure Port Properties on page 62](#)

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. Only static LAG is supported. The **LACP** option is grayed out and unselected. The **Static** option 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. Select the **Configurations** tab.
4. In the Device Config menu, select **Add Port Channel**.
5. In the **Port Channel ID** field, enter a unique numeric ID.
No two port channels can have the same ID.
6. In the **Lag Speed** field, select the speed for the ports that you will select in step 8.
7. In the **Description** field, provide enough information to help you identify the port channel.

8. 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 6. 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 6 on page 60.

9. (SLX and 9920 only) In the **MTU** field, select the maximum transmission unit for packets that pass through the ports in the channel.
10. (MLX only) In the **Primary Port** field, select one of the port channels you selected in the **Ports** field.
11. In the **Minimum Link** field, select or enter the minimum number of interfaces that the port channel requires to be active.
12. (9920 only) 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.

13. 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.

14. (MLX and SLX only) Select **Loopback** to configure the port channel as a loopback interface.

A loopback is a virtual interface that a device uses to communicate with itself. A loopback interface cannot be used as an egress interface.

15. (SLX only) Select **Truncation Profile** to slice an incoming packet on the loopback interface based on the specified frame size.
 - a. In the **Profile Name** field, enter a name for the truncation profile.
 - b. In the **Frame Size** field, enter a value to represent the maximum packet size after truncation.

The final packet size will be less than or equal to this value.

16. 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 **Configurations** 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 60 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 **Configurations** 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, port breakout, header stripping, and Link Fault Signaling.

About This Task



Note

(SLX only) If the port you are configuring is part of a port channel, do not change the **MTU** or the **Port Speed** values from the Visibility Manager interface.

Procedure

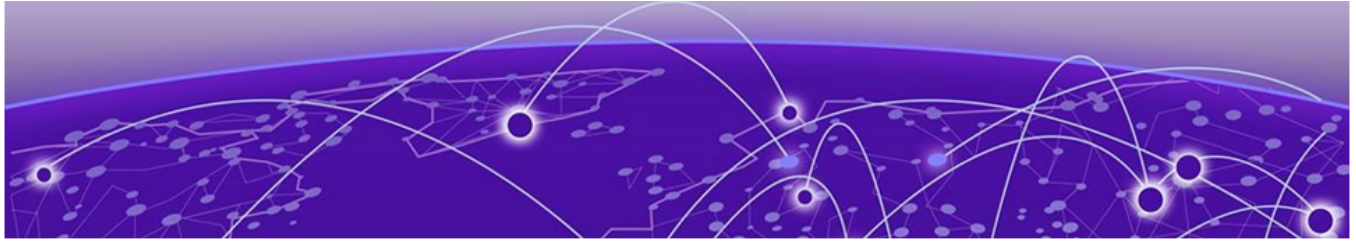
1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device for which you want to configure a port.
3. Select the **Configurations** tab.
4. In the Device Config menu, expand **Ports**.
5. Select a port to display a list of properties.
6. In the **Description** field, provide new information.
7. In the **Port Speed** field, select a different speed.
8. In the **MTU** field, select the maximum transmission unit for packets that pass through the port.
9. (MLX and SLX only) In the **Headers** field, select one or more types of header to strip.
10. (SLX and 9920 only) 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 the port.
 - **None**
11. 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.
12. (9920 only) To enable communication between two Ethernet devices, select **Link Fault Signaling**.

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.

Link Fault Signaling is a physical layer protocol that enables a port to report fault conditions on inbound and outbound ports.

13. 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.
14. (MLX and SLX only) Select **Loopback** to configure the port as a loopback interface.
A loopback is a virtual interface that a device uses to communicate with itself. A loopback interface cannot be used as an egress interface.
15. (SLX only) Select **Truncation Profile** to slice an incoming packet on the loopback interface based on the specified frame size.
 - a. In the **Profile Name** field, enter a name for the truncation profile.
 - b. In the **Frame Size** field, enter a value to represent the maximum packet size after truncation.
The final packet size will be less than or equal to this value.
16. Save (✓) your selections.



Managing Egress and Egress Mirrors

[Create Egress for SLX and MLX Devices](#) on page 64

[Create Egress for 9920 Devices](#) on page 65

[Configure a Traffic Mirror for 9920 Devices](#) on page 65

[Change an Egress or Mirror Configuration](#) on page 66

[Delete an Egress or Mirror Configuration](#) on page 66

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

Create Egress for SLX and MLX Devices

Egress is a combination of ports, port channels, and precedence.

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 60.

About This Task

When you create the egress, you assign a name, select a port and port channel, and then assign precedence. Egress can 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 **Configurations** tab.
4. In the Device Config menu, select **Add Egress**.
5. In the **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. Repeat step 6 through 8 to create all necessary port and precedence combinations.
10. Save (✓) your selections.

Create Egress for 9920 Devices

Egress is a combination of ports, port channels, precedence, and an associated egress policy.

Before You Begin

If necessary, create a port channel. For more information, see [Create a Port Channel](#) on page 60.

If necessary, create an egress policy. For more information, see [Create an Egress Policy for a Device](#) on page 83.

About This Task

Egress can 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 **Configurations** tab.
4. In the Device Config menu, select **Add Egress/Mirror**.
5. Select **Egress**.
6. In the **Name** field, enter a name.
The egress cannot have the same name as an egress group.
7. In the **Port/Port Channel** field, select an egress port or port channel.
8. 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.
9. Select **+** to add your selections.
10. In the **Egress Policy** field, select the policy to associate with the egress.
11. Save (✓) your selections.

Configure a Traffic Mirror for 9920 Devices

You can mirror VxLAN traffic to a mirror port interface.

About This Task

The mirror is used in the outer tunnel configuration for an ingress group. This process ensures that the designated mirroring destination receives the same traffic as the egress port.

Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the device you want to configure.
3. Select the **Configurations** tab.
4. In the Device Config menu, select **Add Egress/Mirror**.
5. Select **Mirror**.
6. In the **Name** field, enter a name for the configuration.
7. In the **Port** field, select the mirroring destination port.
8. Save (✓) your selections.

Change an Egress or Mirror Configuration

You can change the parameters of the configuration.

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 **Configurations** tab.
4. To change an egress configuration for SLX and MLX devices, take the following steps.
 - a. In the Device Config menu, expand **Egress** and select the item that you want to change.
 - b. Complete the fields as described in [Create Egress for SLX and MLX Devices](#) on page 64.
5. To change an egress or mirror configuration for 9920 devices, take the following steps.
 - a. In the Device Config menu, expand **Egress/Mirror** and select the item that you want to change.
 - b. Complete the fields as described in [Create Egress for 9920 Devices](#) on page 65 or [Configure a Traffic Mirror for 9920 Devices](#) on page 65.

Delete an Egress or Mirror Configuration

You can delete the 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 an egress.
3. Select the **Configurations** tab.
4. To delete an egress configuration for SLX and MLX devices, take the following steps.
 - a. In the Device Config menu, expand **Egress**.
 - b. Select **Delete Egress** for the item that you want to delete.
5. To delete an egress or mirror configuration for 9920 devices, take the following steps.
 - a. In the Device Config menu, expand **Egress/Mirror**.
 - b. Select **Delete Egress** for the item that you want to delete.



Managing Egress Groups

[Create an Egress Group on page 67](#)

[Change an Egress Group on page 68](#)

[Delete an Egress Group on page 68](#)

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 Egress for SLX and MLX Devices](#) on page 64.

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 **Configurations** 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. (MLX only) In the **nHop Type** field, select the next hop domain type: **TVF** (transparent VLAN flooding) or **VLAN**.
 - If you selected TVF, continue with step 8.
 - If you selected VLAN, continue with step 7.
7. (MLX only) In the **nHop Value** field, provide the VLAN ID.
8. In the **Egress List** field, select at least one egress to associate with the group.
9. 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 **Configurations** 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 67.

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 **Configurations** 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 for an SLX or MLX Device on page 69](#)

[Create an Ingress Group for a 9920 Device on page 70](#)

[Change an Ingress Group on page 71](#)

[Delete an Ingress Group on page 71](#)

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

Create an Ingress Group for an SLX or MLX Device

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

Before You Begin

If necessary, create the port channel to associate with the ingress group. For more information, see [Create a Port Channel](#) on page 60.

If necessary, create the ingress policy to associate with the ingress group. For more information, see [Create an Ingress Policy for a Device](#) on page 84.

(MLX only) If necessary, create a UDA profile to associate with the ingress group. For more information, see [Create an MLX UDA Profile](#) on page 89.

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 you want to configure.
3. Select the **Configurations** tab.
4. In the Device Config menu, select **Add Ingress Group**.
5. In the **Name** field, enter a name for the group.
6. In the **Ports/Port Channels** field, select at least one port or port channel for the group.
7. In the **Policy Name** field, select the ingress policy to associate with the group.
8. (MLX only) In the **UDA Profile** field, select a UDA profile to associate with the group.

You must select a profile if the policy (in the **Policy Name** field) contains a UDA match. If you do not select a profile, your ingress group configuration will fail.

9. Save (✓) your selections.

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

Create an Ingress Group for a 9920 Device

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

Before You Begin

If necessary, create the port channel to associate with the ingress group. For more information, see [Create a Port Channel](#) on page 60.

If necessary, create the ingress policy to associate with the ingress group. For more information, see [Create an Ingress Policy for a Device](#) on page 84.

If necessary, create a mirror for the outer tunnel. For more information, see [Configure a Traffic Mirror for 9920 Devices](#) on page 65.

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 you want to configure.
3. Select the **Configurations** tab.
4. In the Device Config menu, select **Add Ingress Group**.
5. In the **Name** field, enter a name for the group.
6. In the **Ports/Port Channels** field, select at least one port or port channel for the group.
7. In the **Tunnel Type** field, select the type of tunnel for the incoming traffic: GRE, GTPU, VXLAN, NVGRE, or IPIP.
8. 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.
9. 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
10. In the **Policy Name** field, select the ingress policy to associate with the group.
11. (Optional) If you selected a tunnel type in step 7 on page 70, configure the inner tunnel.
 - Destination IP:** The IPv4 or IPv6 address of the device that is to receive the packets.
 - Destination Mask:** The mask or prefix length for the destination IP address.
 - Source IP:** The IPv4 or IPv6 address of the device that sends the packets.
 - Source Mask:** The mask or prefix length for the source IP address.

- (Optional) If you selected a tunnel type in step 7 on page 70, configure the outer tunnel.

The outer tunnel configuration supports IPv4 addresses only.

Outer Tunnel Type: The type of tunnel for the incoming traffic: VXLAN.

Outer Tunnel ID: A value that represents the tunnel ID.

Outer Destination IP: The IPv4 address of the device that is to receive the packets.

Outer Destination Mask: The mask for the destination IP address.

Outer Source IP: The IPv4 address of the device that sends the packets.

Outer Source Mask: The mask for the source IP address.

Mirror: The mirror you configured in [Configure a Traffic Mirror for 9920 Devices](#) on page 65.

- Save (✓) your selections.

The Configurations 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

- In the Navigation menu, select **Configure**.
- In the Devices panel, select the device for which you want to change an ingress group.
- Select the **Configurations** tab.
- In the Device Config menu, expand **Ingress Groups**.
- In the list of groups, select the group that you want to change.
- Follow the instructions in [Create an Ingress Group for an SLX or MLX Device](#) on page 69 to add, change, or delete the parameters in the group.

Delete an Ingress Group

You can delete an ingress group from a device.

Procedure

- In the Navigation menu, select **Configure**.
- In the Devices panel, select the device for which you want to delete an ingress group.
- Select the **Configurations** tab.
- In the Device Config menu, expand **Ingress Groups**.
- 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 72](#)
- [Create an MLX UDA Match for a Device on page 75](#)
- [Create an SLX UDA Match for a Device on page 76](#)
- [Create a Policy Rule Match in the Library on page 77](#)
- [Create an MLX UDA Match in the Library on page 79](#)
- [Create an SLX UDA Match in the Library on page 80](#)
- [Change a Policy Rule Match on page 80](#)
- [Import a Policy Rule Match to a Device on page 81](#)
- [Export a Policy Rule Match on page 81](#)
- [Clone a Policy Rule Match on page 81](#)
- [Delete a Policy Rule Match on page 82](#)
- [Search Policy Rule Matches on page 82](#)

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 described in this procedure.

This topic does not describe the process for creating matches for SLX and MLX UDAs. For more information, see [Create an SLX UDA Match for a Device](#) on page 76 and [Create an MLX UDA Match for a Device](#) on page 75.

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 **Configurations** tab.
4. In the Device Config menu, select **Add Policy Rule Match**.
5. In the **Name** field, enter a unique 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 75.

The items in this section vary by your selection in the **Protocol** field. The following list 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 the 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 IPv4 or IPv6 address of the device that sends the packets.

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

Destination IP: The IPv4 or IPv6 address of the device that is to receive the packets.

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 in this section vary by your selection in the **Protocol** field. The following list 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.

The items in this section vary by your selection in the **Protocol** field. The following list describes all possible selections.

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 an MLX UDA Match for a Device

When you create an MLX UDA match, you select the match parameters and actions to perform on the matched parameters.

About This Task

A UDA match can contain one or more sets of parameters and actions. Each set of parameters and actions is a rule in the match.

Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the MLX device for which you want to add a UDA profile.
3. Select the **Configurations** tab.
4. In the Device Config menu, select **Add Policy Rule Match**.
5. In the **Name** field, enter a unique name for the match.
6. In the **Type** field, select **UDA**.

7. In the **UDA** field, select the UDA profile to associate with the match.
8. In the **Sequence** field, enter a value to represent the order in which the match performs the selected actions on the targeted matches.
9. In the **VLAN** field, enter the VLAN ID that you want to target.
10. In the rest of the Match section, complete each field, including a mask for each item.
The items that appear in the Match section vary by the items in the selected UDA profile.
11. In the Action section, select one or more actions to perform on the targeted matches.
 - Drop** to drop the packet
 - Log** to add the transaction to the Visibility Manager log.
12. Select **Add**.
The match parameters (the new rule) appear in the pane on the right.
13. Save (✓) your selections.

Create an SLX UDA Match for a Device

An SLX UDA match is a set of match parameters and masks and the action to perform on the targeted items in the UDA profile.

Before You Begin

Create a UDA profile to associate with the match. For more information, see [Create an SLX UDA Profile](#) on page 89.

About This Task

A UDA match can contain one or more sets of parameters and actions. Each set of parameters and actions is a rule in the match.

Procedure

1. In the Navigation menu, select **Configure**.
2. In the Devices panel, select the SLX device for which you want to create a match.
3. Select the **Configurations** tab.
4. In the Device Config menu, select **Add Policy Rule Match**.
5. In the **Name** field, enter a unique name for the match.
6. In the **Type** field, select **UDA**.
7. In the **UDA** field, select the UDA profile to associate with the match.
8. In the **Sequence** field, enter a value to represent the order in which the match performs the selected actions on the items in the profile.
9. In the rest of the Match section, complete each field, including a mask for each item.
The items that appear in the Match section vary by the items in the selected UDA profile.
10. In the Action section, select one or more actions to perform on the profile items.
 - Count** to keep track of the number of packets that match the policy rule
 - Drop** to drop the packet
 - Log** to add the transaction to the Visibility Manager log.
11. Select **Add**.
The match parameters (the new rule) appear in the pane on the right.

12. Repeat steps 8 on page 76 through 11 until you have added all the rules you need.
13. To remove a rule from the match, select **Delete** for that rule in the Rules panel on the right.
14. To change a rule, select **Edit** for that rule in the Rules panel and make your changes.
15. 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

This topic does not describe the process for creating matches for SLX and MLX UDAs. For more information, see [Create an SLX UDA Match in the Library](#) on page 80 and [Create an MLX UDA Match in the Library](#) on page 79.

Procedure

1. In the Navigation menu, select **Library > Match**.
2. Select **Add Match**.
3. In the **Name** field, enter a unique name for the match.
4. In the **Type** field, select whether the match applies to IPv4, IPv6, or L2.

5. 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 7 on page 79.

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 IPv4 or IPv6 address of the device that sends the packets.

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

Destination IP: The IPv4 or IPv6 address of the device that is to receive the packets.

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.

- 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 list 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.

- 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.

- Select **Add**.

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

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

Create an MLX UDA Match in the Library

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

Procedure

- In the Navigation menu, select **Library > Match**.
- Select **Add Match**.
- In the **Name** field, enter a unique name for the match.
- In the **Device Type** field, select **MLX**.
- In the **Type** field, select **UDA**.
- In the **Sequence** field, enter a value to represent the order in which the match performs the selected actions on the targeted matches.
- In the **VLAN** field, enter the VLAN ID that you want to target.
- In the rest of the Match section, complete each field, including a mask for each item.
The items that appear in the Match section vary by the items in the selected UDA profile.
- In the Action section, select one or more actions to perform on the targeted matches.

Drop to drop the packet

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. Save (✓) your selections.

Create an SLX UDA Match in the Library

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

Before You Begin

Create a UDA profile to associate with the match. For more information, see [Create an SLX UDA Profile](#) on page 89.

Procedure

1. In the Navigation menu, select **Library > Match**.
2. Select **Add Match**.
3. In the **Name** field, enter a unique name for the match.
4. In the **Device Type** field, select **SLX**.
5. In the **Type** field, select **UDA**.
6. In the **UDA** field, select the UDA profile to associate with the match.
7. In the **Sequence** field, enter a value to represent the order in which the match performs the selected actions on the items in the profile.
8. In the rest of the Match section, complete each field, including a mask for each item.
The items that appear in the Match section vary by the items in the selected UDA profile.
9. In the Action section, select one or more actions to perform on the profile items.
 - Count** to keep track of the number of packets that match the policy rule
 - Drop** to drop the packet
 - 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 on page 80 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.

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 **Configurations** 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 72 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 72 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 **Configurations** 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 72 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 **Configurations** 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. Perform step 1 to delete the match from any associated device.
 - b. In the Navigation menu, select **Library > Match**.
 - 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 83](#)
- [Create an Ingress Policy for a Device on page 84](#)
- [Create a Policy in the Library on page 85](#)
- [Change a Policy on page 86](#)
- [Import a Policy to a Device on page 86](#)
- [Export a Policy on page 87](#)
- [Clone a Policy on page 87](#)
- [Delete a Policy on page 87](#)
- [Search Policies on page 88](#)

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 a policy rule match to associate with the policy. For more information, see [Create a Policy Rule Match for a Device](#) on page 72.

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.



Note

This topic applies only to Extreme 9920 devices.

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 **Configurations** tab.
4. In the Device Config menu, select **Add Policy**.
5. In the **Name** field, enter a unique name for the policy.

An egress policy cannot have the same name as an ingress policy or another egress policy.

6. In the **Policy Type** field, select **Egress Policy**.

7. Select the **Sequence** in which to apply the rule.
8. 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.
9. In the **Packet Slicing** field, enter a value to represent the maximum packet size after slicing.
The final packet size will be less than or equal to this value.
10. 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.
11. In the **VLAN** field, select the VLAN ID to target the VLAN tag in the egress packet.
12. To remove the outer tunnel headers from the packet, select **Decap**.
13. 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.
14. Select **Add**.
The rule parameters appear in the pane on the right.
15. Repeat steps 7 through 14 until you have added all the rules you need.
16. 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 72.

Create an egress group to associate with the policy. For more information, see [Create an Egress Group](#) on page 67.

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 **Configurations** tab.
4. In the Device Config menu, select **Add Policy**.
5. In the **Name** field, enter a unique name for the policy.
An ingress policy cannot have the same name as an egress policy or another ingress policy.

6. In the **Policy Type** field, select **Ingress Policy**.
7. Select the **Sequence** in which to apply the rule.
8. Select a policy rule **Match**.



Note

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 once per policy.

(MLX only) Do not apply an L2 rule match and a UDA rule match in the same policy. Doing so causes the related ingress group to fail.

(MLX only) If you add a UDA rule match to a policy that is associated with an ingress group, ensure that you first apply the associated UDA profile to that group. For more information, see [Create an Ingress Group for an SLX or MLX Device](#) on page 69.

9. In the **Egress Group** field, select the group to associate with the policy.
10. (MLX and 9920 only) In the **Packet Slicing** field, enter a value to represent the maximum packet size after slicing.
The final packet size will be less than or equal to this value.
11. (SLX only) In the **Truncation Profile** field, select a profile that you created for a port or port channel.
For more information, see [Create a Port Channel](#) on page 60 or [Configure Port Properties](#) on page 62.
12. 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
13. 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.

14. Select **Add**.
The rule parameters appear in the pane on the right.
15. Repeat steps 7 through 14 until you have added all the rules you need.
16. 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 83 or [Create an Ingress Policy for a Device](#) on page 84.

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 **Configurations** 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 84 or [Create an Egress Policy for a Device](#) on page 83 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 84 or [Create an Egress Policy for a Device](#) on page 83 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 **Configurations** 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 84 or [Create an Egress Policy for a Device](#) on page 83 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

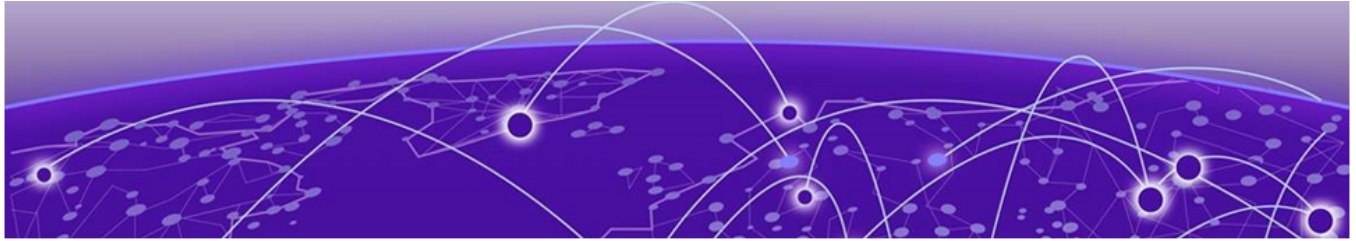
1. To delete a policy from a device, take the following steps.
 - a. Remove the policy from any associated ingress group. For more information, see [Change an Ingress Group](#) on page 71.
 - b. In the Navigation menu, select **Configure**.
 - c. In the Devices panel, select the device for which you want to delete a policy.
 - d. Select the **Configurations** 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 71.
 - 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 ACL Profiles

[Create an MLX UDA Profile on page 89](#)

[Create an SLX UDA Profile on page 89](#)

[Change a UDA Profile on page 90](#)

[Clone a UDA Profile on page 90](#)

[Delete a UDA Profile on page 90](#)

[Search UDA Profiles on page 91](#)

The topics in this section describe how to create, change, clone, delete, and search user-defined access list (UDA) profiles.

A complete MLX or SLX UDA consists of a UDA profile and a UDA match. For information about creating MLX and SLX UDA matches, see [Managing Policy Rule Matches](#) on page 72.

Create an MLX UDA Profile

For MLX devices, you can create a UDA profile in the library.

Procedure

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

An offset indicates the index of the received packet. For example, an offset of 0 indicates the first byte of the received packet.

6. Save (✓) your selections.

Create an SLX UDA Profile

A UDA profile can be associated with a UDA match.

Procedure

1. In the Navigation menu, select **Library > UDA**.
2. Select **Add UDA**.
3. In the **Name** field, enter a unique name for the UDA profile.
4. In the **Device Type** field, select **SLX**.

5. Define the header fields that are required for a match.

The header fields you select constitute the header stack. As you select header types and header fields, additional header selections become available. The additional selections vary based on your header choices.

- a. In the **Header 0 Ethernet - Ethernet** row, select the field that is required for a match and then click **+** to add your selection.
 - b. In the **Header 1** row, select the type and field that are required for a match and then click **+** to add your selection.
Your selections determine whether a Header 2 row is displayed.
 - c. Make selections in the Header 2 row and in all subsequent rows until no more rows are available or until your header stack is complete.
6. Save (✓) your selections.

Change a UDA Profile

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

Procedure

1. In the Navigation menu, select **Library > UDA**.
2. Select **Edit** for the UDA that you want to change.
3. Follow the instructions for the type of UDA you are changing.
 - [Create an MLX UDA Profile](#) on page 89
 - [Create an SLX UDA Profile](#) on page 89

Clone a UDA Profile

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

Procedure

1. In the Navigation menu, select **Library > UDA**.
2. Select **Clone** for the profile that you want to copy.
3. Follow the instructions for the type of profile you are cloning.
 - [Create an MLX UDA Profile](#) on page 89
 - [Create an SLX UDA Profile](#) on page 89

Delete a UDA Profile

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

Procedure

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

Search UDA Profiles

You can search for a user-defined access list (UDA) profile 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 92](#)

[Change a Tunnel on page 93](#)

[Delete a Tunnel on page 93](#)

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 and then associate that group with an ingress policy. For more information, see [Create an Ingress Group for an SLX or MLX Device on page 69](#).



Note

This feature applies to Extreme 9920 devices only.

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 **Configurations** 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 IPv4 or IPv6 address of the device that sends the packets.
9. In the **Destination IP** field, enter the IPv4 or IPv6 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 device 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 **Configurations** 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 92 to change the tunnel configuration.

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 **Configurations** 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 94

[Delete a Location](#) on page 94

[Search Locations](#) on page 95

The topics in this section explain how to add, delete, and search for locations.

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, 6.1.0](#).

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.

Delete a Location

When you delete a location, the Device Type Version Capabilities (DTVC) and all discovered device configurations for that location are also deleted.

About This Task

If you delete all locations in a zone, the zone is deleted from the Visibility Manager infrastructure (the pods running in that zone are removed). However, the zone virtual machine (VM) is not deleted from the Kubernetes cluster. Because the VM remains in the cluster, you can replace the zone by adding a locations definition file that includes the zone.

Procedure

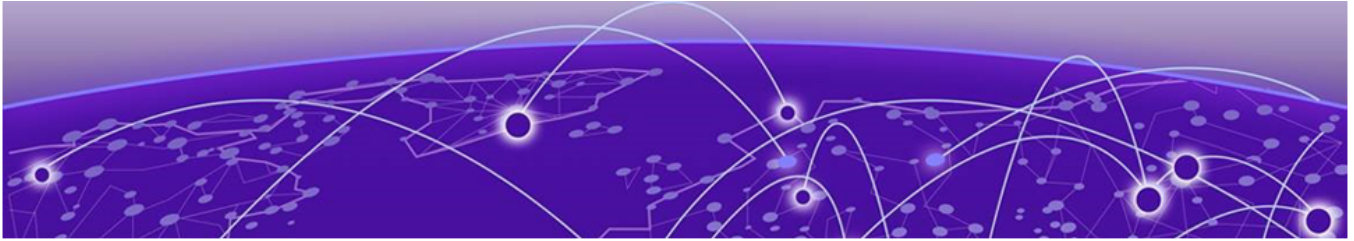
1. In the Navigation menu, select **Settings > Location**.
2. Select a location to delete.
Each row represents a location. You can select multiple locations.
3. Select **Delete**.

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 17: Rule mapping

Rule	MLX path	XVM path
Policies per device		
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'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	
Interfaces per device		
Bind policies to interfaces	Device[]/Slots[]/Device-id[]/Ports[]/Policy	/ingress/Policy bind[name]
Port channels per device		
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 mode.	Device[]/vlans[]/vlan/<load-balancing>	/egress/Port-channel[]

Table 18: Advanced rule mapping for global features

MLX I	MLX E	XVM I	XVM E	Rule	MLX path	XVM path
802.1BR header stripping: 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>
802.1BR header bypass: 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>
VN-tag header stripping: 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>
VN-tag header bypass: 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>
VN-tag and 802.1BR preservation: TBD						
Supported	Not supported	Supported	Supported			
VxLAN header stripping: 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>
NVGRE header stripping: 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>
GTP de-encapsulation: Remove the outer IP, the outer UDP header, and the GTP header from GTP-U packets						

Table 18: 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>
Packet slicing (packet truncation)						
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 19: Rule mapping

Rule	9920 path	XVM path
Ingress port bind		
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
Ingress policies		
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
Egress policies		
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 19: Rule mapping (continued)

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

Table 20: Advanced rule mapping for global features

9920 I	9920 E	XVM I	XVM E	Rule	9920 path
802.1 BR header stripping					
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>
VN-tag header stripping					
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>
VxLAN header stripping					
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>
NVGRE header stripping					
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>
GTP decapsulation					
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 20: 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 21: Rule mapping

Rule	SLX path	XVM path
Policies per device		
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'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	
Interfaces per device		
Bind policies to interfaces	Device[]/Ports[]/npb_bind	/ingress/Policy bind[name]

Table 22: Advanced rule mapping for global features

SLX I	SLX E	XVMI	XVME	Rule	SLX path	XVM path
802.1BR header stripping: 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>
VN-tag header stripping: 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>
VxLAN header stripping: 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>
NVGRE header stripping: 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>
GTP de-encapsulation: 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>
MPLS stripping: 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>