Switch Configuration with Chalet

For ExtremeXOS 21.x and Later

121144-05 Rev AD
April 2024

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/about-extreme-networks/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/

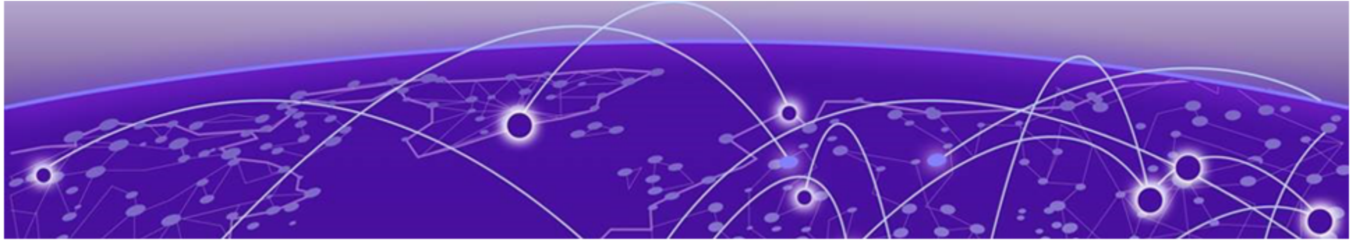
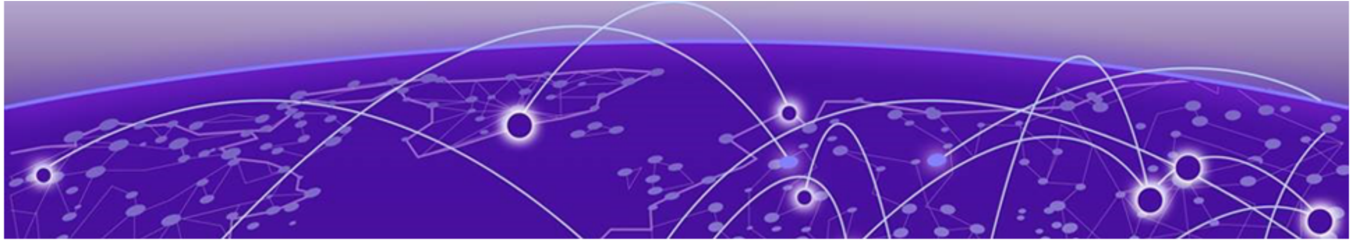


Table of Contents



Preface

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 Extreme Networks 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 *enter* and *type*	When you see the word *enter* 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 *type*.
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 italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
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.
italic text	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, *member*[*member*...].
\	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.

Send Feedback

The User Enablement 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, email us at documentation@extremenetworks.com.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.

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 2800. 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.

Related Publications

ExtremeXOS Publications

To access ExtremeXOS publications, open https://www.extremenetworks.com/support/documentation/extremexos-30-6/ and select the desired software version in the upper-right corner.

- *ExtremeXOS User Guide*
- *ExtremeXOS Command Reference Guide*
- *ExtremeXOS Feature License Requirements*
- *ExtremeXOS Release Notes*

ExtremeCloud IQ - Site Engine Publications

To access ExtremeCloud IQ - Site Engine publications, open https://www.extremenetworks.com/support/documentation/extreme-management-center-8-4/ and select the desired software version in the upper-right corner.

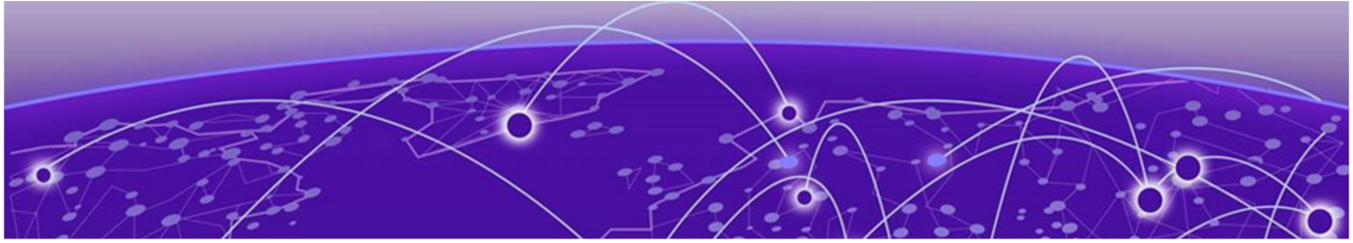
- *Extreme Management Center User Guide*

Other Publications

- *ACL Solutions Guide*
- *Using AVB with Extreme Switches*

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/open-source-declaration/.



About Chalet

Chalet is a web-based user interface for setting up and viewing information about a switch. Chalet removes the need to know and remember commands in a CLI environment. Viewable on desktop and mobile with a quick login and intuitive navigation, Chalet features an Quick Setup mode for configuring a switch in a few simple steps. Basic data surrounding port utilization, power, and *QoS (Quality of Service)* are available, and more advanced users can configure multiple VLANs, create Access Control Lists (ACLs), and configure Audio Video Bridging (AVB).

Chalet is packaged with ExtremeXOS release 15.7.1 and later for all platforms, so there's nothing extra to download or install. Chalet can be launched in any modern web browser and does not depend on any outside resources to work, including Java Applets, Adobe Flash, or dedicated mobile applications.

Note
The screens shown in this guide were captured from a variety of Extreme Networks switches. The information displayed on the screen will vary depending on the switch being used.

Browser Support

Chalet is supported on all modern, standards-compliant browsers, including:

- Internet Explorer 8.0 and later
- Mozilla Firefox 3.0 and later
- Microsoft Edge (Windows 10)
- Chrome
- Safari
- Opera

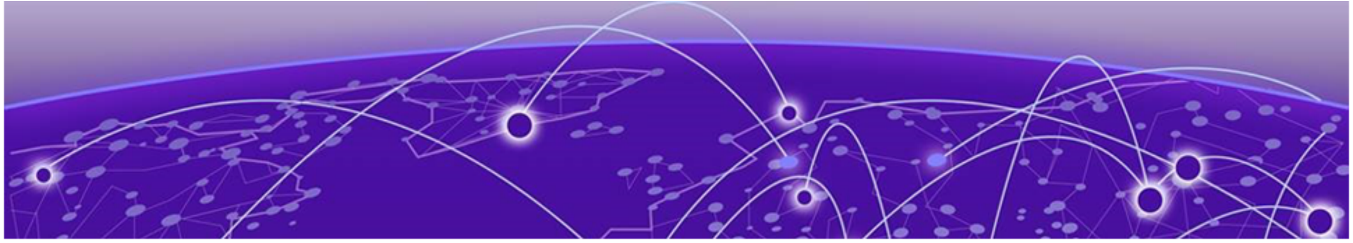
Chalet Features

Chalet helps you interact with the switch outside of a CLI environment and allows you to easily:

- Configure the switch for the first time without the use of a console cable.
- Create and upload files to and from the switch.
- Install software images and modules directly on the switch.

- View status and details of the switch and its slots and ports.
- Analyze power efficiency of power supplies, fans, and *PoE (Power over Ethernet)* ports.
- Create VLANs and *ACL (Access Control List)* policies.
- Enable and disable multiple features, including *QoS*, auto-negotiation, and flooding.
- View recent system events.
- View device topology (stacked switches only).
- Manage users, including defining global and individual security policies.

Note
Beginning with version 31.4, access to the switch through Chalet is limited to only Admin users. Read-only users do not have access to the switch through the Chalet interface. This restriction is included due to security concerns.



Getting Started with Chalet

This section describes how to:

- Set up the switch to use Chalet
- Log in to Chalet
- Configure basic switch settings

Setting up the Switch with a Management Port

After removing the switch from the box, you would normally connect the switch using a console cable and log in directly to set it up for the first time. With Chalet, you can avoid doing this by plugging a cable into the MGMT port and letting the switch self-compute its IP address, which you will use to log into Chalet.

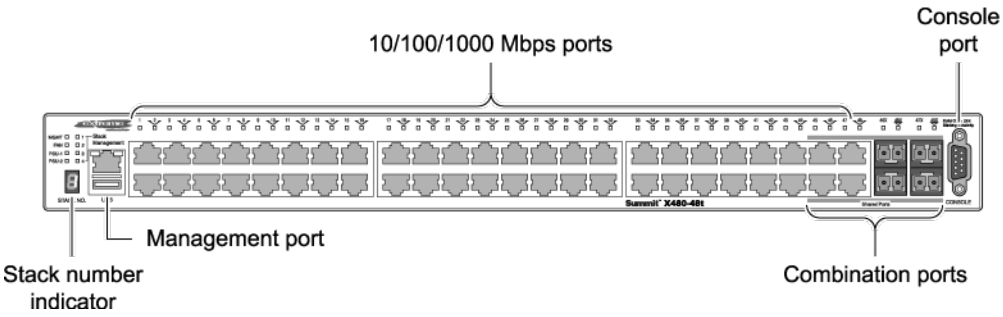
Important
This set up does not apply to most ExtremeSwitching 5320 models or the ExtremeSwitching X435-8T and X435-8P. Instead, a management IP must be configured for these models. See the "Managing the Switch" chapter in the ExtremeXOS *User Guide* for configuration options for switches with no management port.

Note
The ExtremeSwitching 5320-24T-4X-XT and 5320- 24T-24S-4XE-XT models have a front panel MGMT port.

Zero Touch Provisioning (also known as Auto Provisioning) is enabled in ExtremeXOS 15.7 by default and directs this self-assigning behavior.

To get started:

1. Follow unpacking and site location instructions in the hardware manual.
2. Connect a cable to the management (MGMT) port.
3. Find the switch's IP address using one of the following ways to get this information.
    - If you have a switch with a stack number indicator window, the self-assigned IP address will scroll one digit at a time in this window. Enter this address in a web browser to log in to Chalet.



Note
Self-assigned addresses start with 169.254.x.x.

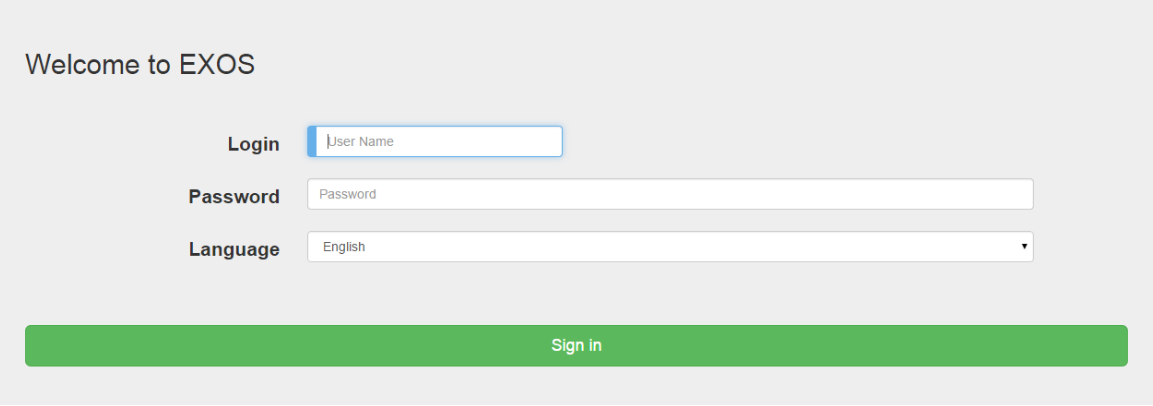
- If your switch does not have a stack number indicator window, you can get the IP address by taking the last two number/letter groups from the MAC adddress (printed on the switch label) and appending them to `0xa9fe` (these are the HEX characters for 169.254). For example, if the last four characters of the switch's MAC address are E9 and EE, the login URL will be `http://0xa9fee9ee`.
- The last option option is to convert the last two number/letter groups from the MAC adddress into decimal using a hex-to-decimal converter (such as www.binaryhexconverter.com/hex-to-decimal-converter). In our example, E9 and EE are converted to 233 and 238, respectively. Append these two numbers to the end of the base 169.254 IP address in order to log in to Chalet.

Logging In

1. To log in to the switch, enter the server's IP address (or HEX characters) in the browser window.

   If you do not know the switch's IP address, use one of the options in step 3 on page 11.

   When you've connected to the switch, the login screen displays.


Welcome to EXOS

Login: User Name

Password: Password

Language: English

2. Enter the user name and password. The default admin user name is 'admin' with no password.

   Note
   To create additional accounts after setup, see Adding Users on page 74.

3. (Optional) Select your preferred language from the **Language** drop-down.

   Note
   English is the default unless your browser's default language is different.

4. Click **Sign in**.

   The **Quick Setup** page displays automatically during first time setup when logging in with the 169.254.xx.xx address. Otherwise, the Dashboard displays.

   Note
   You will be logged out of your session after 10 minutes of inactivity. To change the default idle timeout settings, see Configuring Chalet Settings on page 48.

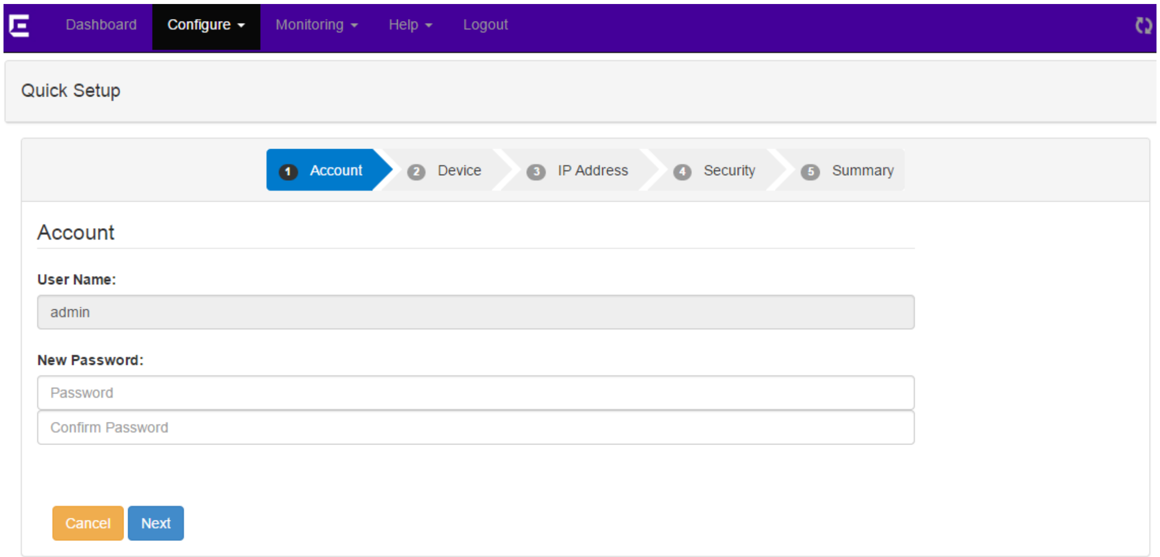
Using the **Quick Setup** Wizard

Note
Only the admin account can configure the switch.

The **Quick Setup** is similar to configuring the switch using a console cable, just with a web interface.

1. After logging in with the 169.254.xx.xx IP address, you are automatically directed to the **Quick Setup**. Otherwise, select **Configure** > **Quick Setup** from the top navigation.

2. On the **Account** page, provide a password for the admin account (this is strongly recommended). On the initial configuration, leave the old password field blank (by default the admin password is not set), fill in the new **Password** and **Confirm** fields, and then click **Next** to continue.



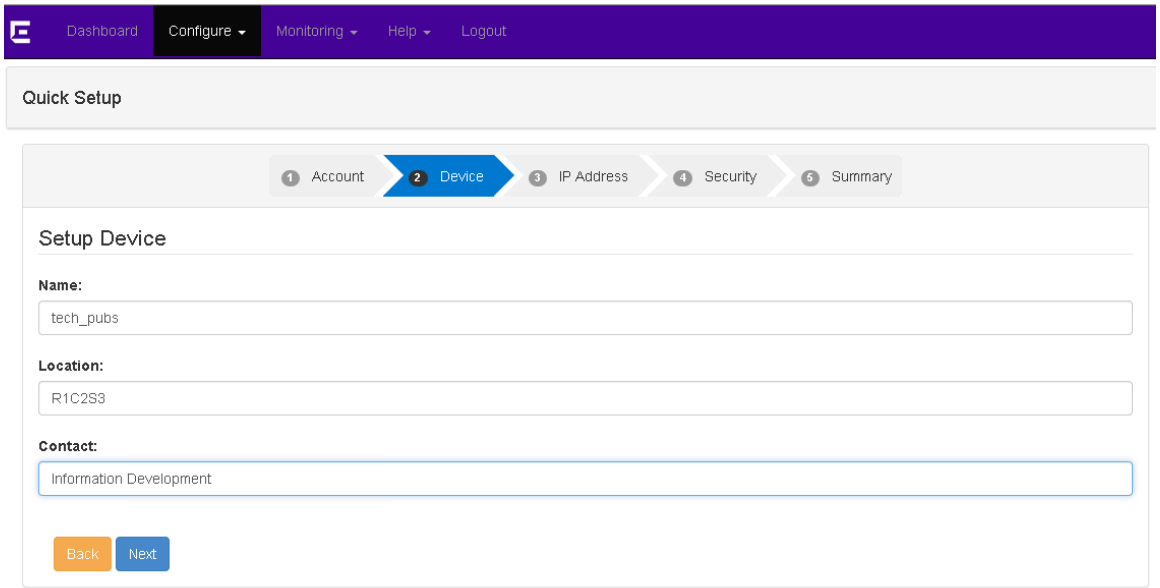
Account

User Name: admin

New Password:

3. On the **Device** page, enter the following information and click **Next** to continue:

- Name: Provide a unique name for the device.
- Location: Enter the device's location.
- Contact: Enter the name or phone number of the person or team responsible for this device.



Setup Device

Name: tech_pubs

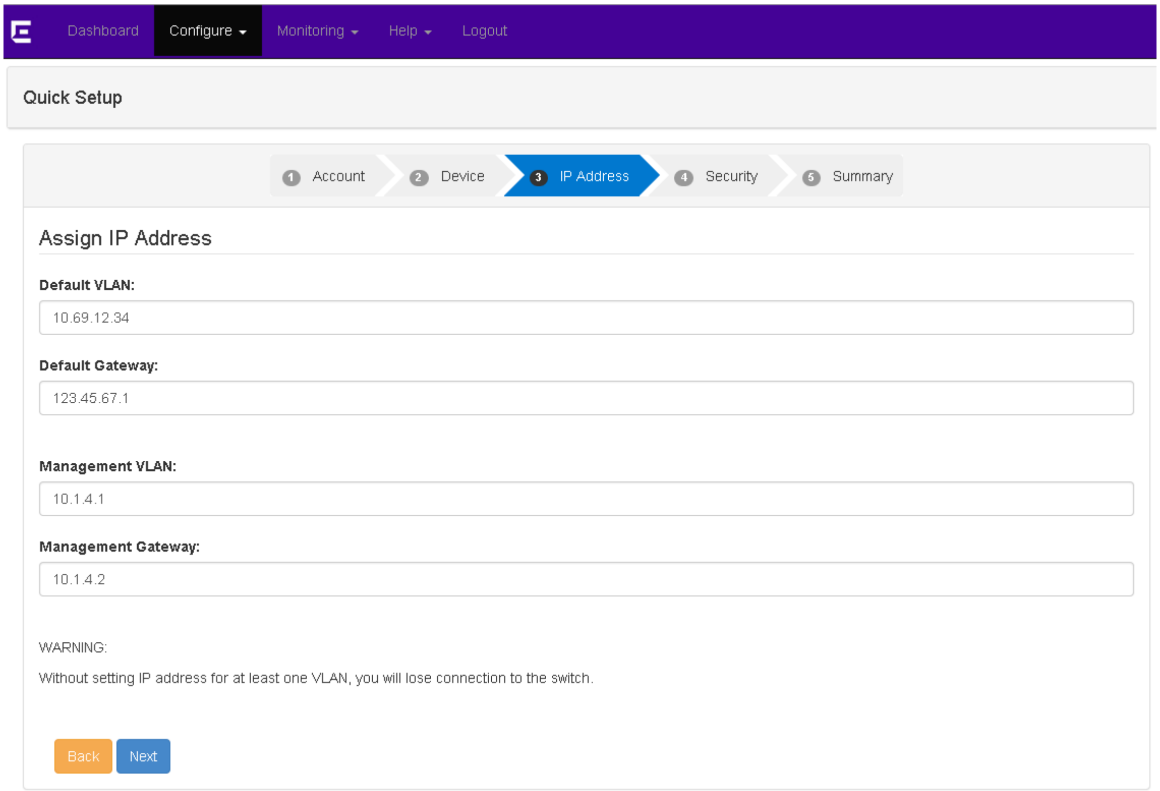
Location: R1C2S3

Contact: Information Development

4. On the **IP Address** page, assign IP addresses for the following and click **Next** to continue:

- Default *VLAN (Virtual LAN)*
- Default Gateway

- Management VLAN
- Managemenet Gateway



Assign IP Address

Default VLAN: 10.69.12.34

Default Gateway: 123.45.67.1

Management VLAN: 10.1.4.1

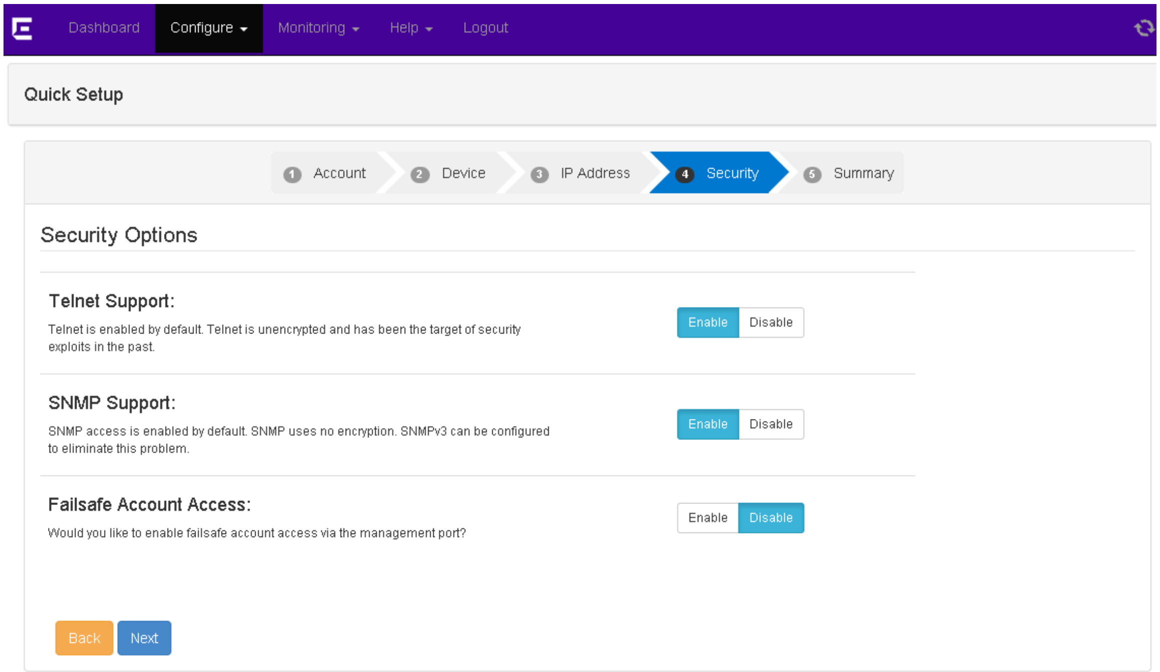
Management Gateway: 10.1.4.2

WARNING:

Without setting IP address for at least one VLAN, you will lose connection to the switch.

5. On the **Security** page, you can enable or disable Telnet, *SNMP (Simple Network Management Protocol)*, and failsafe account access.

   If you are unsure, leave the default and click **Next** to continue. You can always enable or disable these features later.



Security Options

Telnet Support:

Telnet is enabled by default. Telnet is unencrypted and has been the target of security exploits in the past.

[✓ Enable] Disable

SNMP Support:

SNMP access is enabled by default. SNMP uses no encryption. SNMPv3 can be configured to eliminate this problem.

[✓ Enable] Disable

Failsafe Account Access:

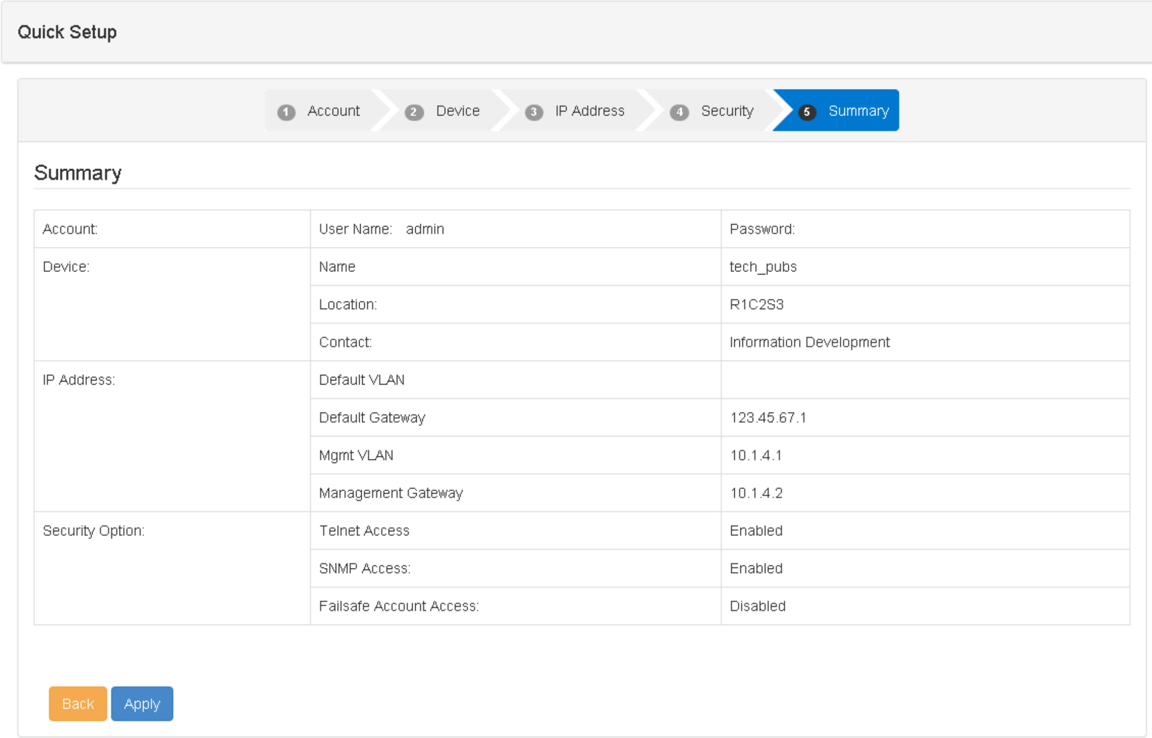
Would you like to enable failsafe account access via the management port?

Enable [✓ Disable]

Note

If you are using (or plan to use) an external network management system such as NetSight or Ridgeline, SNMP must be enabled.

6. At the **Summary** page, click **Apply** to save the configuration.



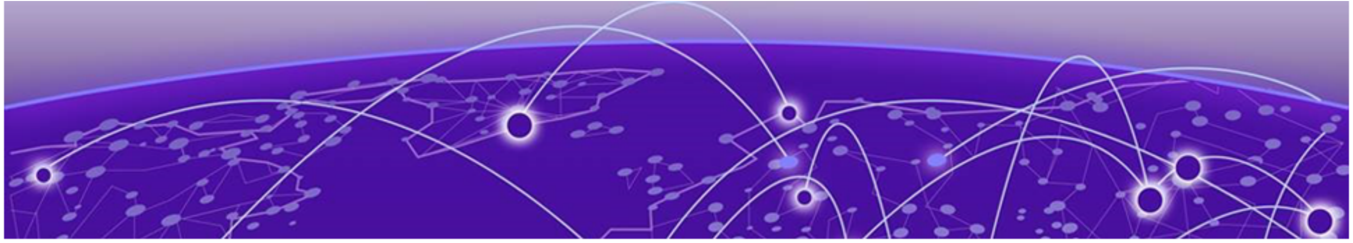
Summary

Account:	User Name: admin	Password:
Device:	Name	tech_pubs
	Location:	R1C2S3
	Contact:	Information Development
IP Address:	Default VLAN	
	Default Gateway	123.45.67.1
	Mgmt VLAN	10.1.4.1
	Management Gateway	10.1.4.2
Security Option:	Telnet Access	Enabled
	SNMP Access:	Enabled
	Failsafe Account Access:	Disabled

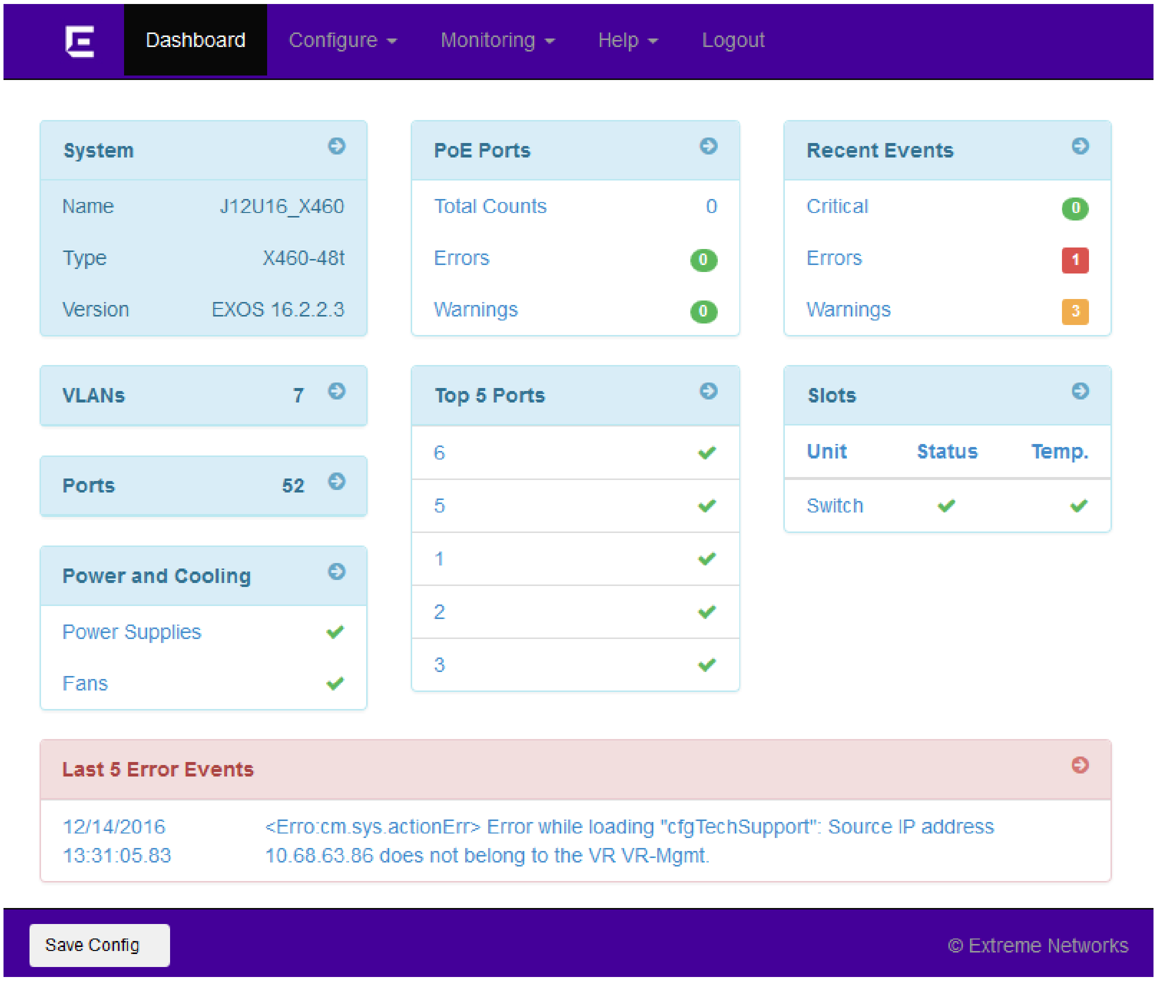
You are directed back to the Dashboard. If you have configured anything incorrectly, you will see a pop-up warning dialog.

7. Next, change the IP address of the management workstation to the same IP subnet as the switch (the IP address you assigned during Quick Setup).

You can now log in to Chalet with the switch's newly assigned IP address.



Chalet Dashboard



System

Name	J12U16_X460
Type	X460-48t
Version	EXOS 16.2.2.3

PoE Ports

Total Counts	0
Errors	0
Warnings	0

Recent Events

Critical	0
Errors	1
Warnings	3

VLANs 7

Ports 52

Power and Cooling

Power Supplies	✓
Fans	✓

Top 5 Ports

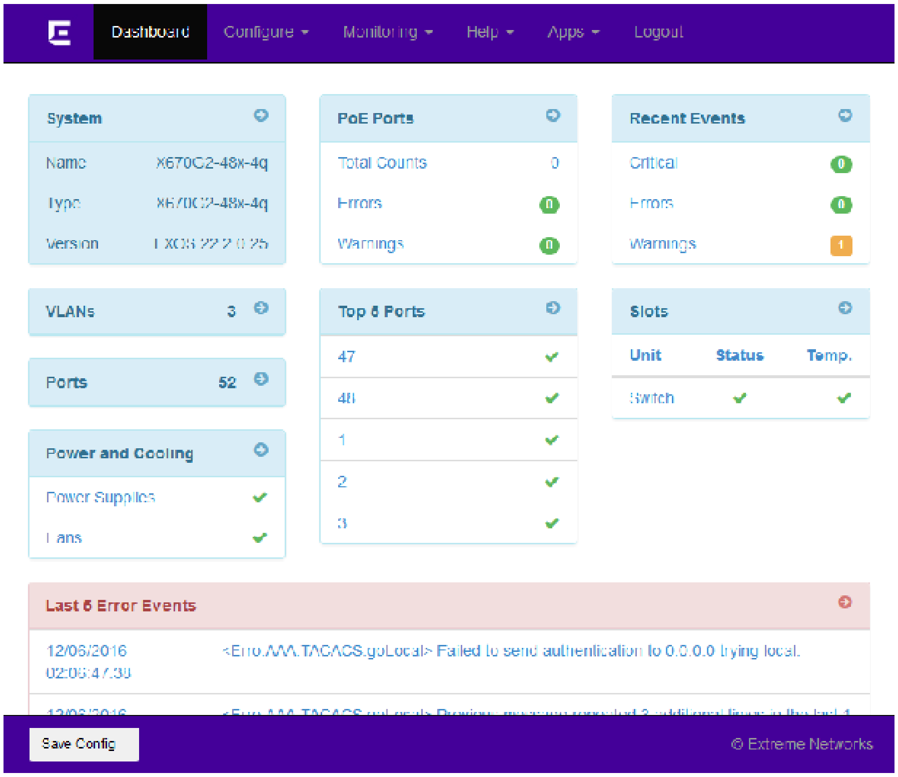
6	✓
5	✓
1	✓
2	✓
3	✓

Slots

Unit	Status	Temp.
Switch	✓	✓

Last 5 Error Events

12/14/2016 13:31:05.83	<Erro:cm.sys.actionErr> Error while loading "cfgTechSupport": Source IP address 10.68.63.86 does not belong to the VR VR-Mgmt.



System

Name	X670G2-48x-4q
Type	X670G2-48x-4q
Version	EXOS 22.2.0.25

PoE Ports

Total Counts	0
Errors	0
Warnings	0

Recent Events

Critical	0
Errors	0
Warnings	1

VLANs 3

Ports 52

Power and Cooling

Power Supplies	✓
Fans	✓

Top 5 Ports

47	✓
48	✓
1	✓
2	✓
3	✓

Slots

Unit	Status	Temp.
Switch	✓	✓

Last 5 Error Events

12/06/2016 02:06:47.38	<Erro:AAA.TACACS.goLocal> Failed to send authentication to 0.0.0.0 trying local.
12/06/2016	<Erro:AAA.TACACS.goLocal> Previous message repeated 3 additional times in the last 1

The **Dashboard** is the home page for Chalet and displays the following information:

System Information

Switch type and model information, including the ExtremeXOS version the switch is running. Clicking this table takes you to the **Switch Information** page.

VLANs

The number of VLANs currently configured. Clicking this table takes you to the **VLAN List** page.

Ports

The number of configured ports. Clicking this table takes you to the **Ports** page.

Power and Cooling

List of power supplies and fans, including status of installation and operation. Clicking this table takes you to the **Power and Cooling** page.

PoE Ports

A list of configured *PoE (Power over Ethernet)* ports. Not all switches are capable of PoE or may have inline-power disabled. Clicking this link takes you to the **PoE Port List** page.

Top 5 Ports

A list of the five most active ports. Clicking this table takes you to the **Ports** page.

Recent Events

The number of Warning, Critical, and Error messages from the last 48 hours of the **Event Log**.

Slots

Status of installed slots. Clicking this table directs you to the **Devices** page.

Last 5 Error Events

A list of the most recent error events. Clicking this table takes you to the **Event Log** page.

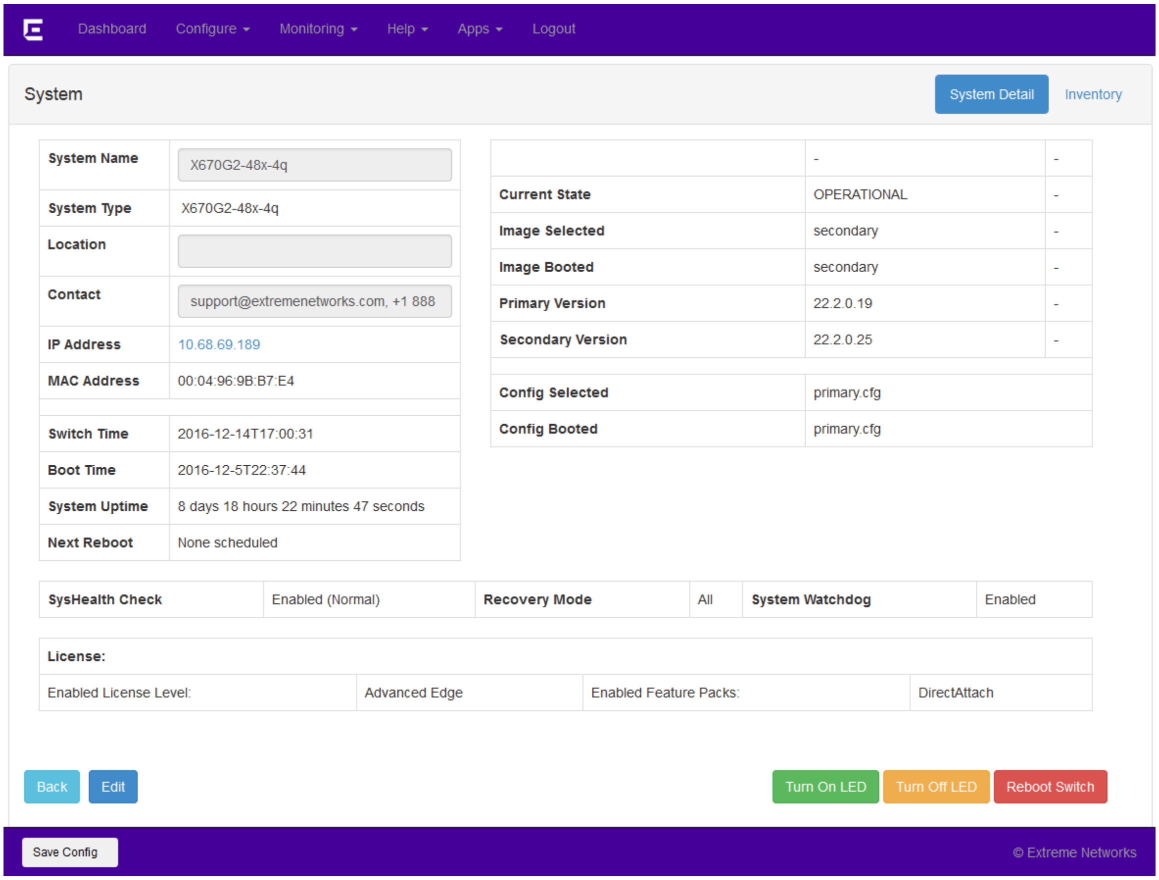
The following sections describe the pages and tabs that are only accessible from the Dashboard. Pages accessible from the navigation menu are described in the Configuration and Monitoring sections.

Note

When the 🔄 displays in the header, Chalet is updating. This happens when changes are being made or data is being retrieved from or sent to the switch. Chalet automatically updates every three minutes even if no changes have been made.

System Information

Clicking the **System Information** table from the Dashboard takes you to the **System Detail** page.



System Name	X670G2-48x-4q
System Type	X670G2-48x-4q
Location	
Contact	support@extremenetworks.com, +1 888
IP Address	10.68.69.189
MAC Address	00:04:96:9B:B7:E4
Switch Time	2016-12-14T17:00:31
Boot Time	2016-12-5T22:37:44
System Uptime	8 days 18 hours 22 minutes 47 seconds
Next Reboot	None scheduled

	-	-
Current State	OPERATIONAL	-
Image Selected	secondary	-
Image Booted	secondary	-
Primary Version	22.2.0.19	-
Secondary Version	22.2.0.25	-
Config Selected	primary.cfg	
Config Booted	primary.cfg	

SysHealth Check	Enabled (Normal)	**Recovery Mode**	All	**System Watchdog**	Enabled

License:			
Enabled License Level:	Advanced Edge	Enabled Feature Packs:	DirectAttach

This page displays detailed information about the switch, eliminatinating the need to enter multiple "show" commands (such as `show switch`, `show licenses`, and `show version`) on the switch to get the same information.

The following buttons are present on this page:

- **Edit**—Edit the System Name, Location, and Contact person. Click **Apply** to save your changes, **Restore** to go restore the default settings, or **Back** to return to the Dashboard.
- **Turn On LED**—Turn on the switch's LED panel to find the switch in a rack. The lights flash across the front of the switch from high to low. This is equivalent to running the command `enable led locator`.
- **Turn Off LED**—Turn off the switch's LED panel. This is equivalent to issuing the command `disable led locator`.
- **Reboot Switch**—Reboot the switch.

Clicking the **Inventory** tab displays the number of slots, their serial numbers, Boot ROM versions, and ExtremeXOS software version.

PoE Port List

Clicking the **PoE Ports** table from the Dashboard takes you to the **PoE Port List** (defaulting to the **Basic** tab).

Note

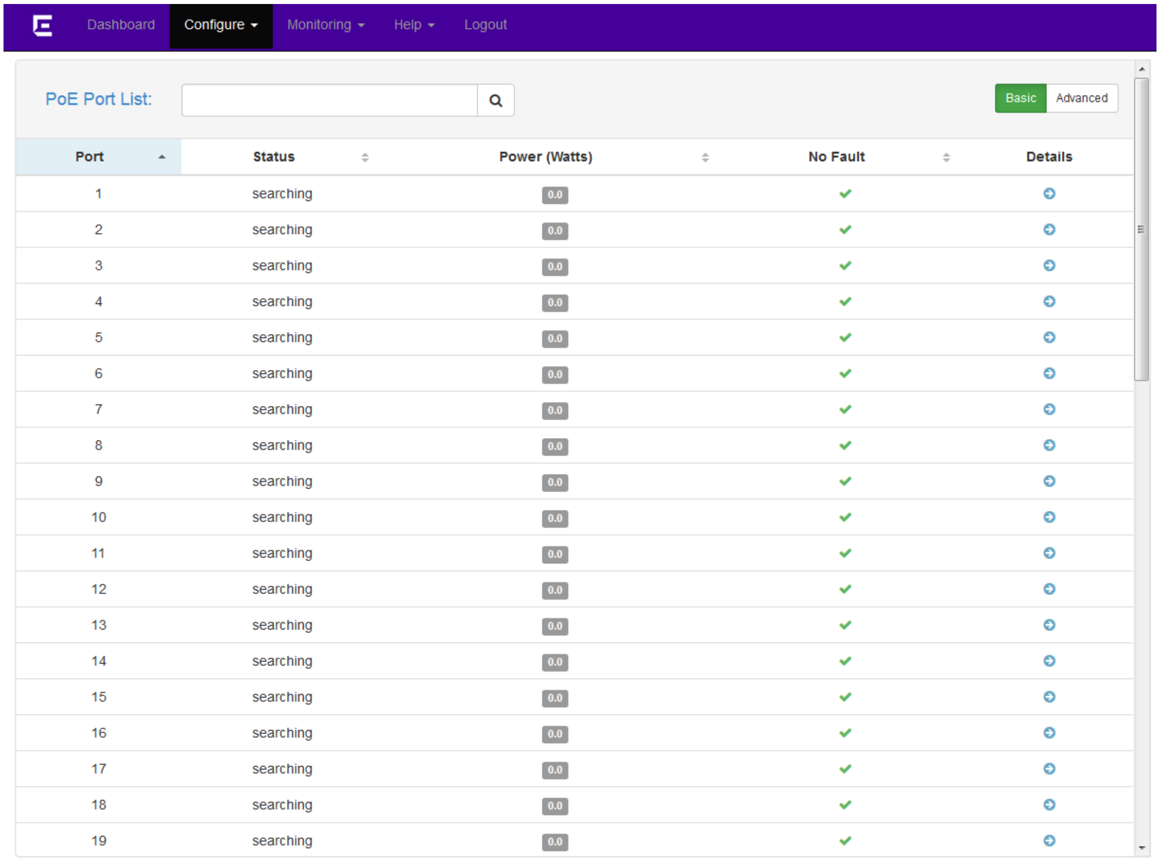
It is not possible to detect if *PoE* ports are present, so if you see the following message, either your switch is not PoE-capable or inline power is disabled.

```
No Power Over Ethernet ports were found on this switch. This switch may not be
capable of PoE or may have inline-power disabled.
```

If your switch *is* PoE-capable, issue the command `enable inline-power ports [`**`all`**` | `*`port_list`*`]` from the CLI.

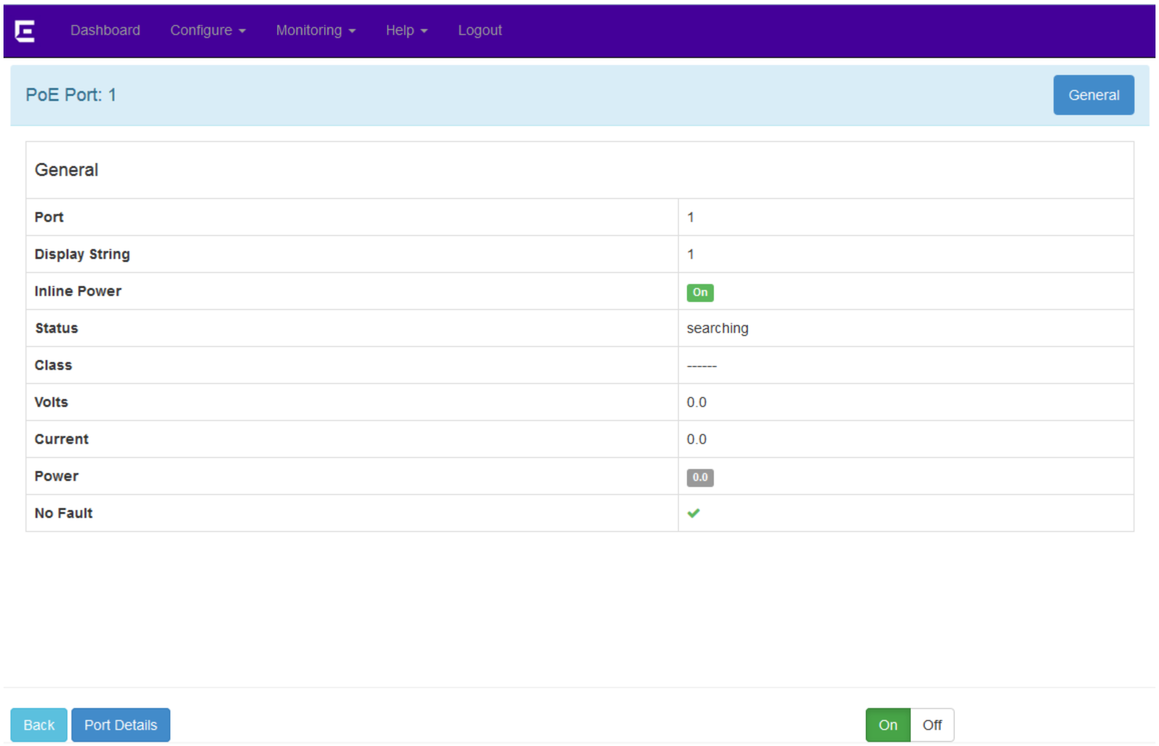
This screen shows which ports are enabled with PoE, listed in numerical order by default. The table also shows their PoE status, power (in Watts), and No Fault state, which are helpful when troubleshooting power issues. The information shown is the equivalent output of the `show inline-power info` command.

To easily see which ports are delivering power, type `delivering` in the search bar.



Port	Status	Power (Watts)	No Fault	Details
1	searching	0.0	✓	➔
2	searching	0.0	✓	➔
3	searching	0.0	✓	➔
4	searching	0.0	✓	➔
5	searching	0.0	✓	➔
6	searching	0.0	✓	➔
7	searching	0.0	✓	➔
8	searching	0.0	✓	➔
9	searching	0.0	✓	➔
10	searching	0.0	✓	➔
11	searching	0.0	✓	➔
12	searching	0.0	✓	➔
13	searching	0.0	✓	➔
14	searching	0.0	✓	➔
15	searching	0.0	✓	➔
16	searching	0.0	✓	➔
17	searching	0.0	✓	➔
18	searching	0.0	✓	➔
19	searching	0.0	✓	➔

To see more details about a port, click the ➔ to the right. You are directed to the PoE Port details screen. This is the same information displayed in the **Advanced** tab.



General

Port	1
Display String	1
Inline Power	On
Status	searching
Class	------
Volts	0.0
Current	0.0
Power	0.0
No Fault	✓

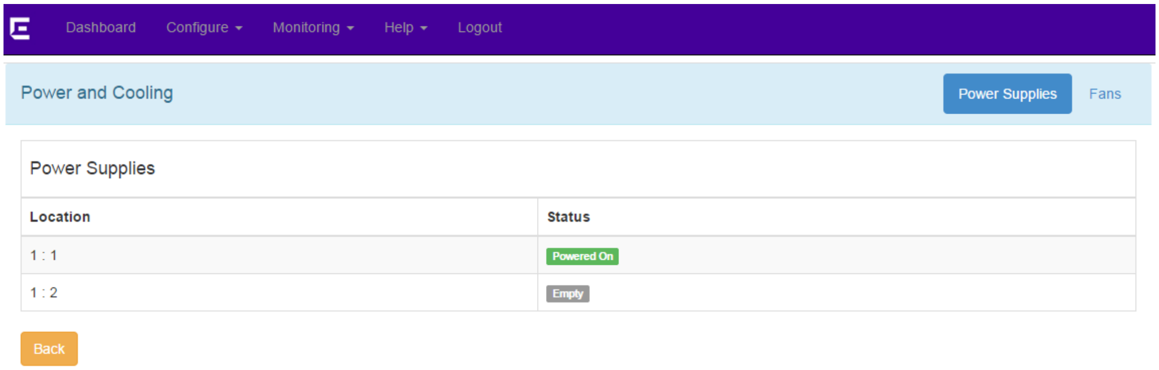
To enable or disable PoE on an individual port. click **On** or **Off** buttons at the bottom of the screen. These buttons perform the same functionality as the `enable inline-power ports` and `disable inline-power ports` commands.

Note
The port's class defines how much power the port is allowed and how the switch can get to it.

To view additional information about the port, click the **Port Details** button. This will direct you to the editable **Port Details** page. For more information about editing port information, see Configuring Ports on page 28.

Power and Cooling

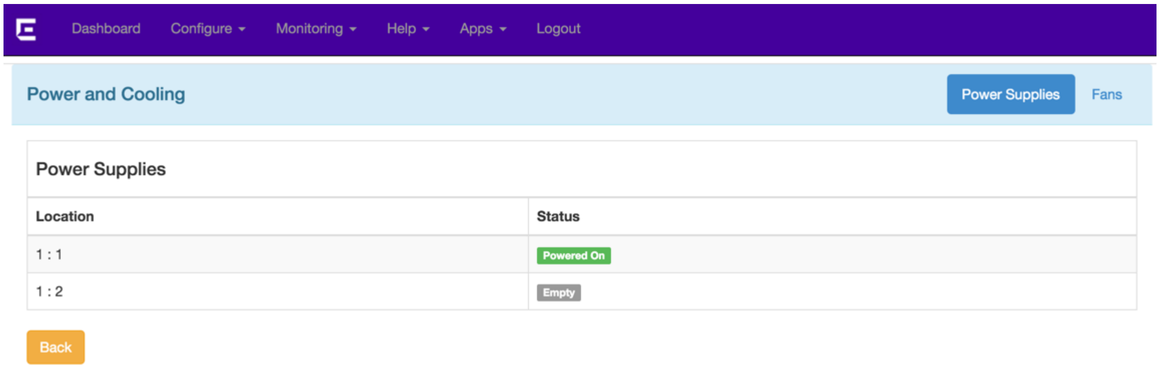
Clicking the **Power and Cooling** table from the Dashboard takes you to the **Power Supplies** page. This screen shows the status of the installed power supplies.



Power and Cooling

Power Supplies

Location	Status
1 : 1	Powered On
1 : 2	Empty



Power and Cooling

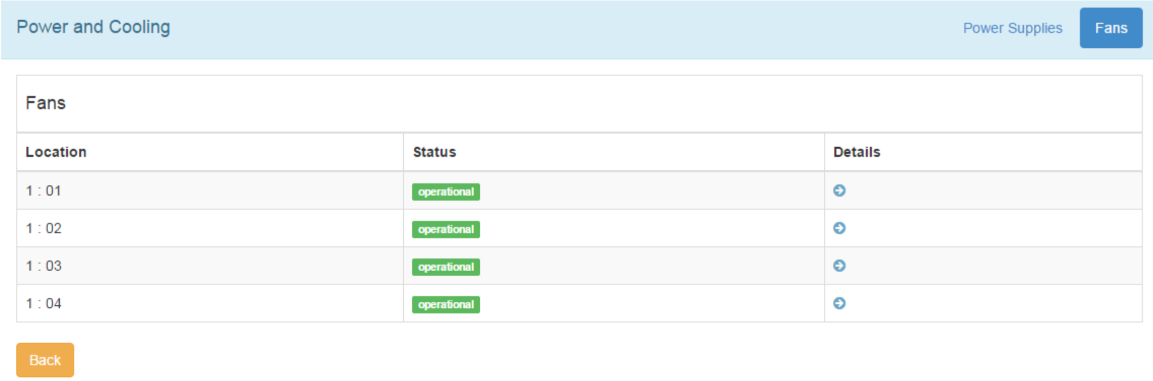
Power Supplies

Location	Status
1 : 1	Powered On
1 : 2	Empty

The Status column will change based on the switch platform:

- P (stacked switches)
- Powered on (Summits)
- Empty or " - "

Clicking the **Fans** tab displays the location and status of installed fans. Clicking the ➔ to the right displays more details about the fan, including number of fans, revision number, temperature, and speed.



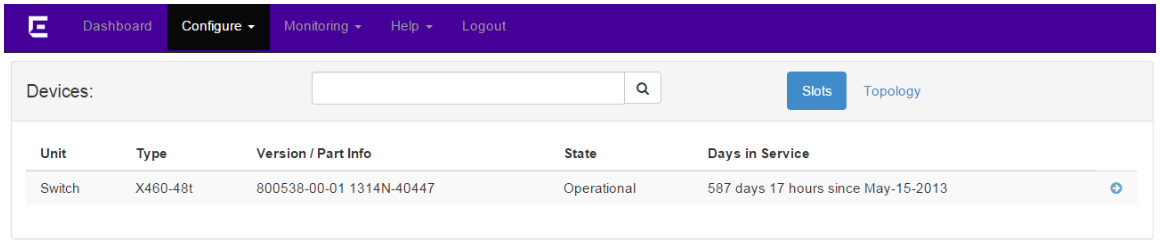
Power and Cooling

Fans

Location	Status	Details
1 : 01	operational	➔
1 : 02	operational	➔
1 : 03	operational	➔
1 : 04	operational	➔

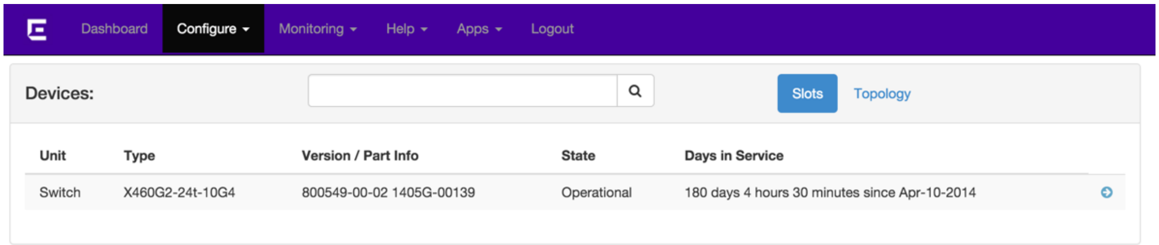
Slots

Clicking the **Slots** table on the Dashboard takes you to the **Devices** page. This page shows the switch name, type, version and part number, current state, and days in service.



Devices:

Unit	Type	Version / Part Info	State	Days in Service
Switch	X460-48t	800538-00-01 1314N-40447	Operational	587 days 17 hours since May-15-2013



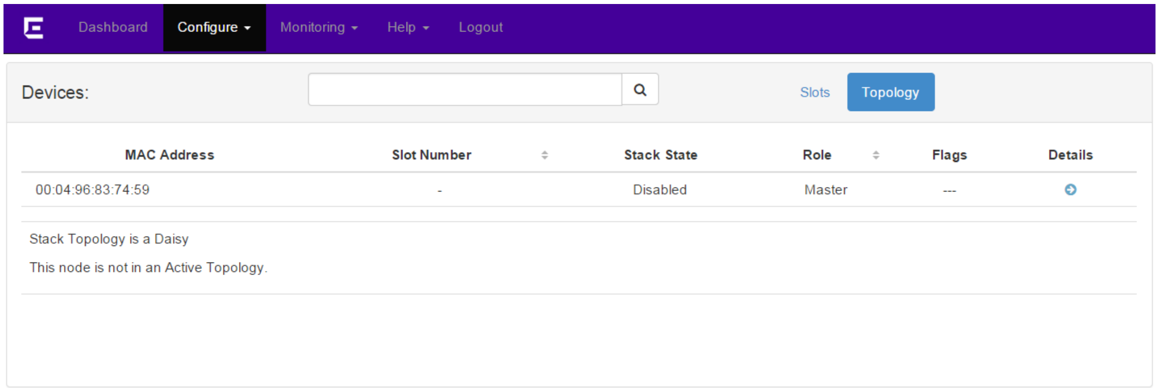
Devices:

Unit	Type	Version / Part Info	State	Days in Service
Switch	X460G2-24t-10G4	800549-00-02 1405G-00139	Operational	180 days 4 hours 30 minutes since Apr-10-2014

Clicking the **Topology** tab displays the type of topology (daisy, ring, etc.), and whether the topology is active. For each node in the stack, you are also provided the MAC address, stack state, role (Master/Slave), and any flags present.

Note
Topology information is available only on stacked switches.

Clicking the ➔ to the right provides further details details about the slot. You can also turn the slot's LEDs on and off, but the information shown is not editable.

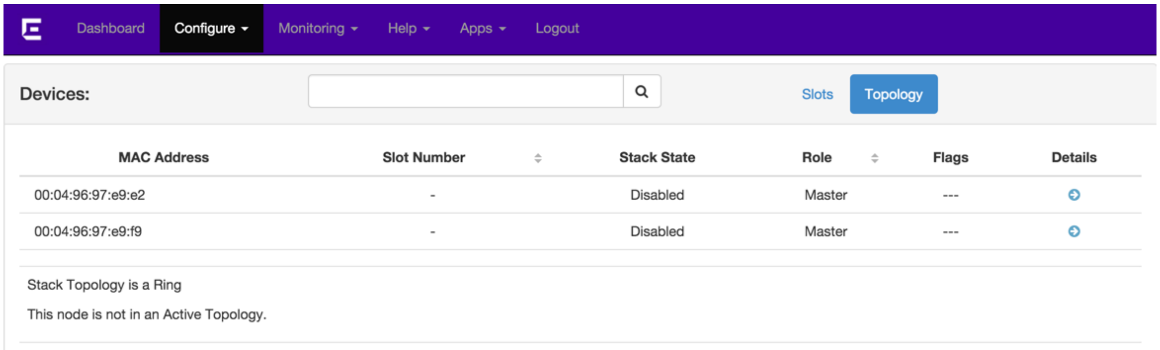


Devices:

MAC Address	Slot Number	Stack State	Role	Flags	Details
00:04:96:83:74:59	-	Disabled	Master	---	➔

Stack Topology is a Daisy

This node is not in an Active Topology.



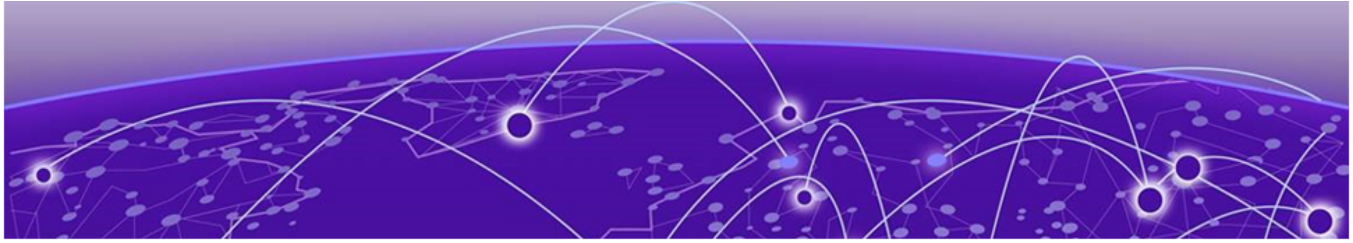
Devices:

MAC Address	Slot Number	Stack State	Role	Flags	Details
00:04:96:97:e9:e2	-	Disabled	Master	---	➔
00:04:96:97:e9:f9	-	Disabled	Master	---	➔

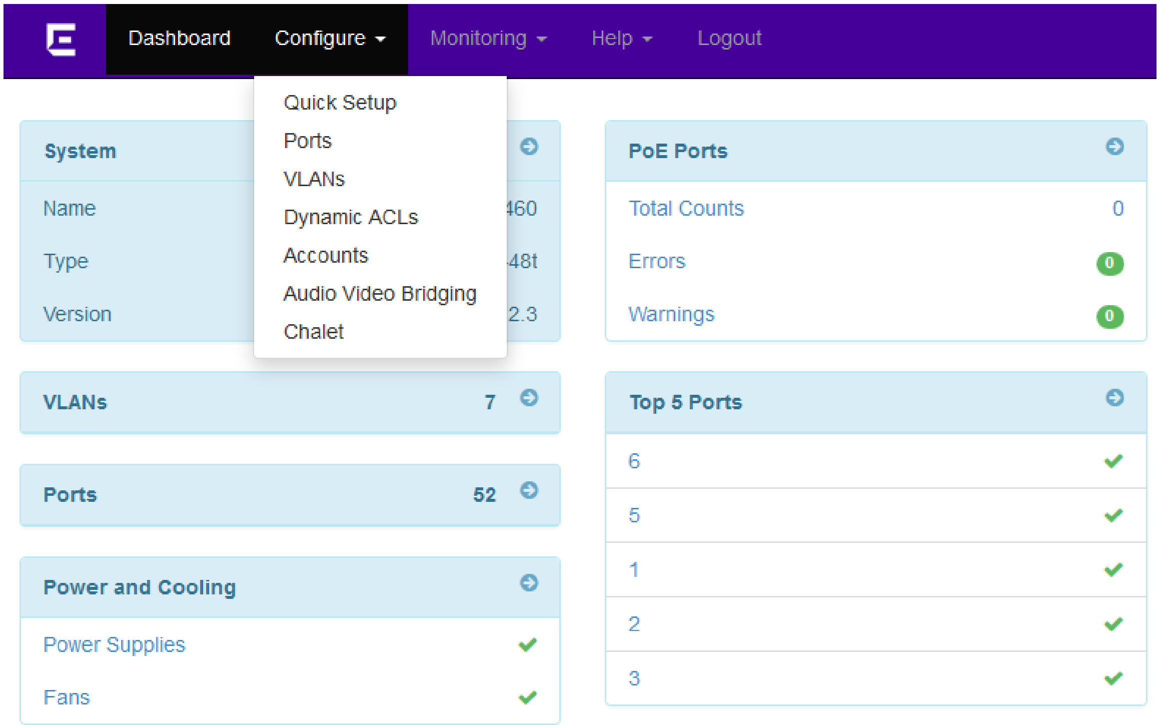
Stack Topology is a Ring

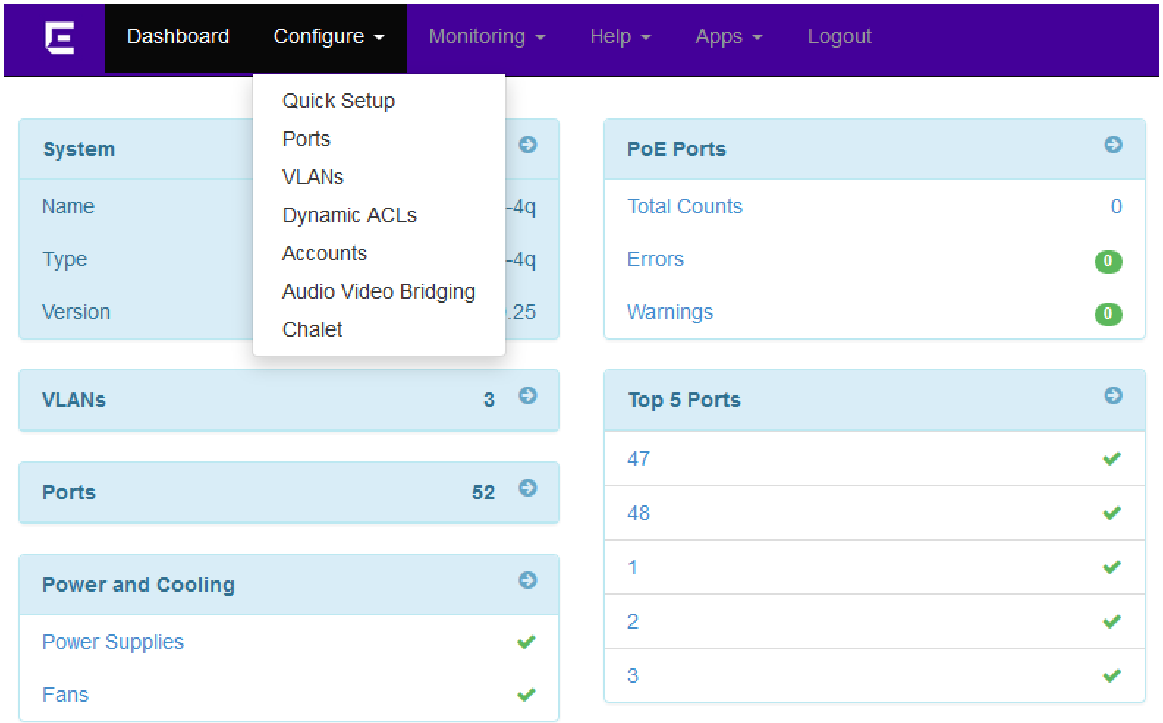
This node is not in an Active Topology.

Clicking the ➔ to the right provides further details details about the slot topology.



Configuring a Switch in Chalet





The **Configure** menu allows administrators to configure:

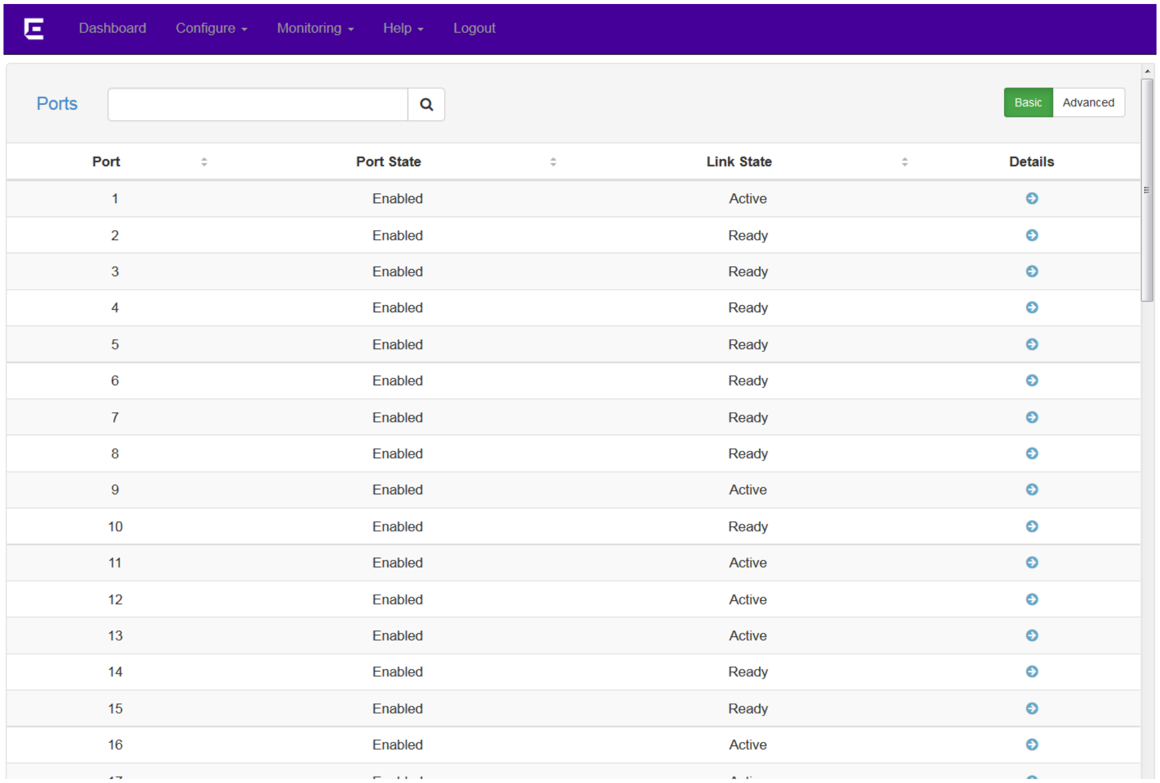
- Ports: Configure port details, including *QoS (Quality of Service)* profiles and VLANs.
- VLANs: Create and delete VLANs, and assign ports.
- Dynamic ACLs: Create *ACL (Access Control List)* policies on the switch.
- Accounts: Manage user accounts and set password policies.

- Audio Video Bridging: Enable AVB.
- Chalet: Configure settings in Chalet, including session idle timeout.

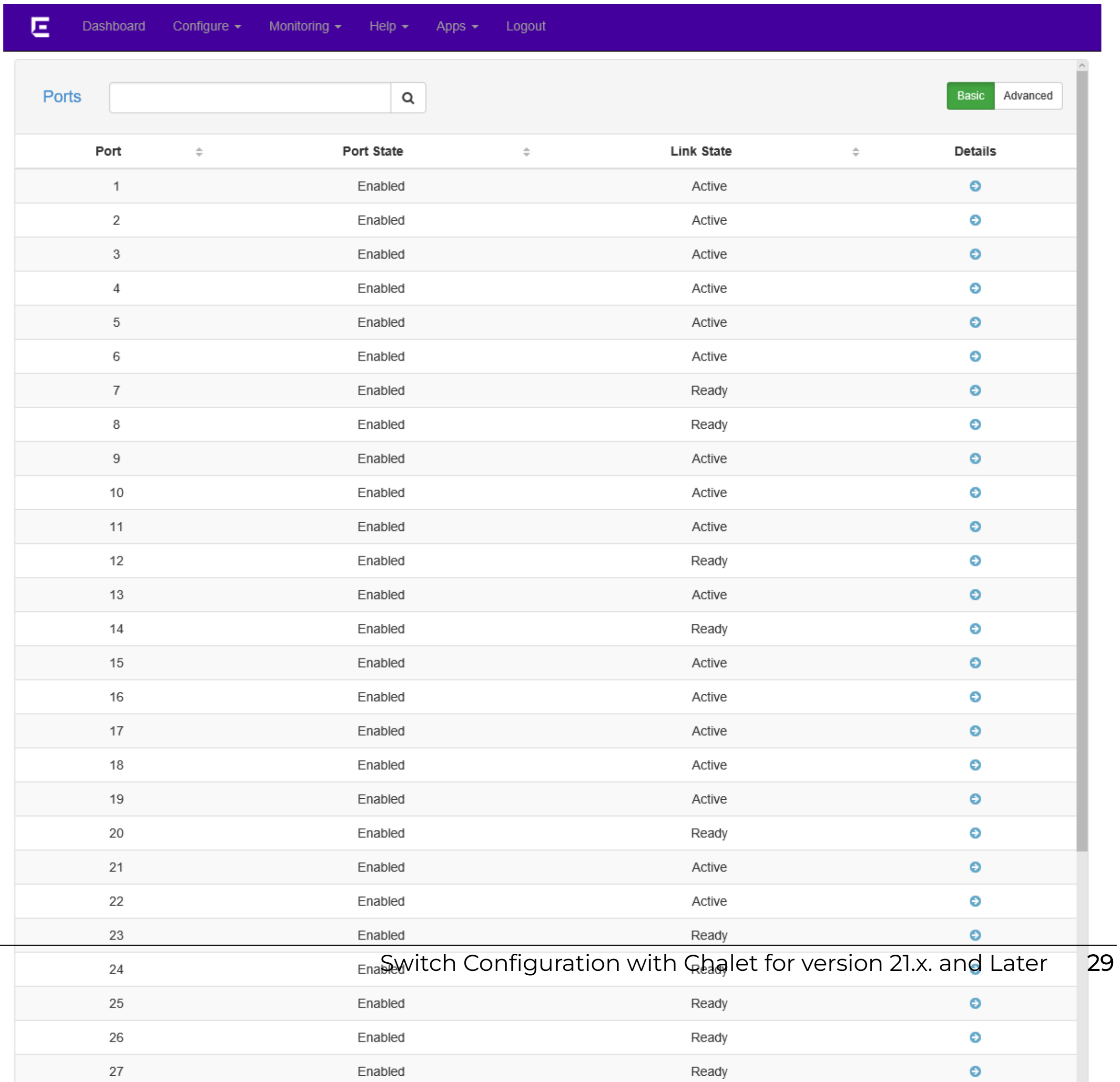
Configuring Ports

Port information displays automatically after clicking the **Ports** table from the Dashboard, or selecting **Configure** > **Ports**.

On the **Basic** tab, the table displays each port and its port and link states. The **Advanced** tab provides flags, link speed, duplex mode, and auto negotiation state.



Port	Port State	Link State	Details
1	Enabled	Active	➔
2	Enabled	Ready	➔
3	Enabled	Ready	➔
4	Enabled	Ready	➔
5	Enabled	Ready	➔
6	Enabled	Ready	➔
7	Enabled	Ready	➔
8	Enabled	Ready	➔
9	Enabled	Active	➔
10	Enabled	Ready	➔
11	Enabled	Active	➔
12	Enabled	Active	➔
13	Enabled	Active	➔
14	Enabled	Ready	➔
15	Enabled	Ready	➔
16	Enabled	Active	➔
17	Enabled	Active	➔

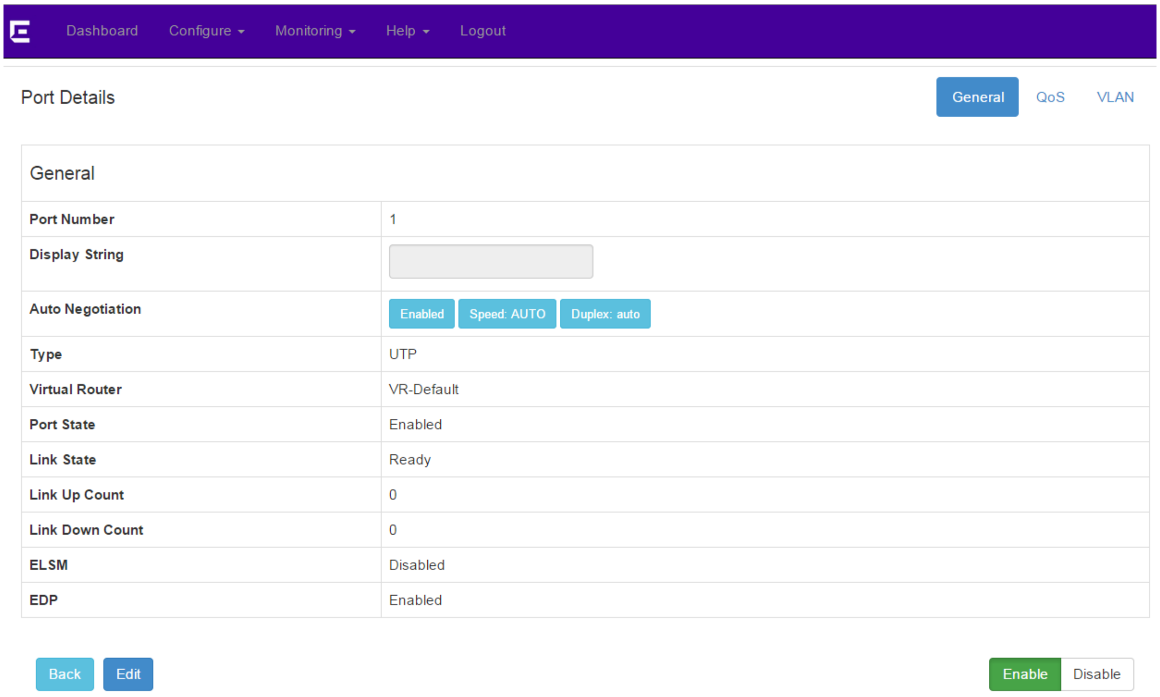


Port	Port State	Link State	Details
1	Enabled	Active	➔
2	Enabled	Active	➔
3	Enabled	Active	➔
4	Enabled	Active	➔
5	Enabled	Active	➔
6	Enabled	Active	➔
7	Enabled	Ready	➔
8	Enabled	Ready	➔
9	Enabled	Active	➔
10	Enabled	Active	➔
11	Enabled	Active	➔
12	Enabled	Ready	➔
13	Enabled	Active	➔
14	Enabled	Ready	➔
15	Enabled	Active	➔
16	Enabled	Active	➔
17	Enabled	Active	➔
18	Enabled	Active	➔
19	Enabled	Active	➔
20	Enabled	Ready	➔
21	Enabled	Active	➔
22	Enabled	Active	➔
23	Enabled	Ready	➔
24	Enabled	Ready	➔
25	Enabled	Ready	➔
26	Enabled	Ready	➔
27	Enabled	Ready	➔

To change a port's details:

1. Click the ➔ for the port you wish to edit.

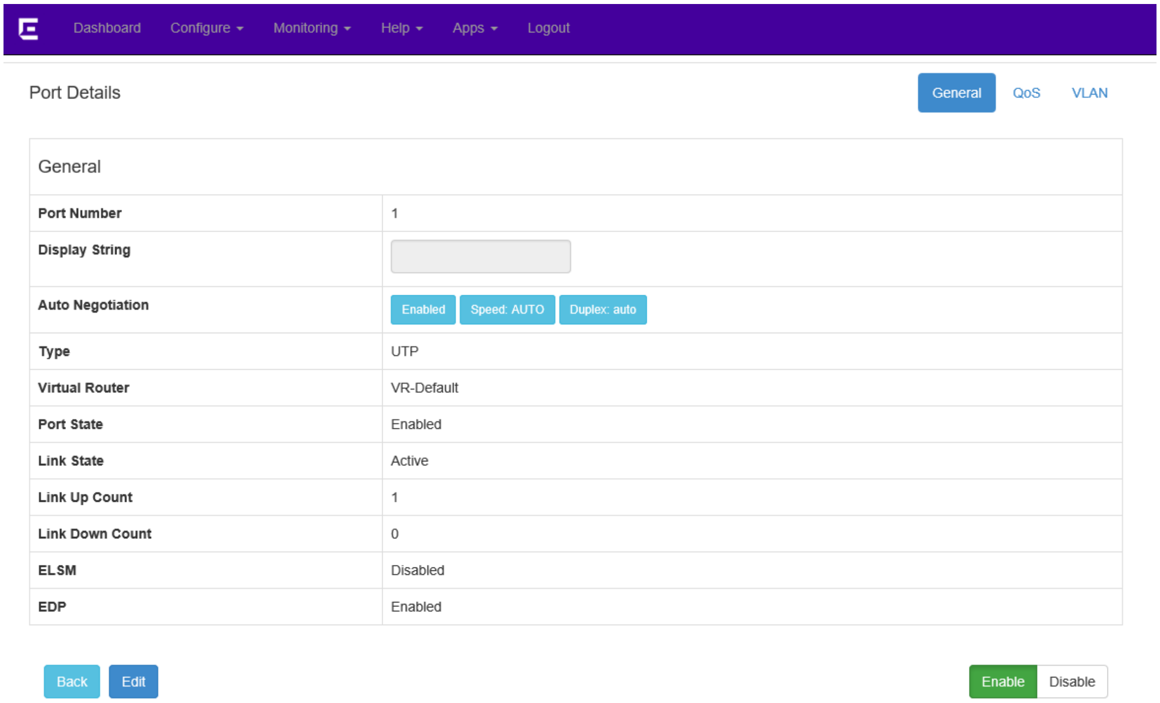
   You are directed to the **Port Details**, **General** tab, where you can edit basic information about the port. Clicking the QoS, or VLAN tabs allow you to create and edit additional information about the port.



Port Details

General

Port Number	1
Display String	
Auto Negotiation	Enabled Speed: AUTO Duplex: auto
Type	UTP
Virtual Router	VR-Default
Port State	Enabled
Link State	Ready
Link Up Count	0
Link Down Count	0
ELSM	Disabled
EDP	Enabled



Port Details

General

Port Number	1
Display String	
Auto Negotiation	Enabled Speed: AUTO Duplex: auto
Type	UTP
Virtual Router	VR-Default
Port State	Enabled
Link State	Active
Link Up Count	1
Link Down Count	0
ELSM	Disabled
EDP	Enabled

2. Click **Edit** to change the following information:
    - Display String—A string of up to 255 characters that displays on all `show port` commands. Some characters such as <, >, ?, & are not permitted, as they have special meanings.
    - Auto Negotiation
        - If Auto Negotiation is Enabled, the Speed and Duplex will display "AUTO".
        - Click **Disable** to disable Auto Negotiation and set Speed and Duplex manually.
3. To save your changes, click **Apply**. If you do not want to save, choose one of the following options:
    - Click **Restore** to cancel your changes.
    - Click **Back** to return to the **Ports** page.
4. To disable the port entirely, click **Disable** at the bottom of the screen. To re-enable the port, click **Enable**.

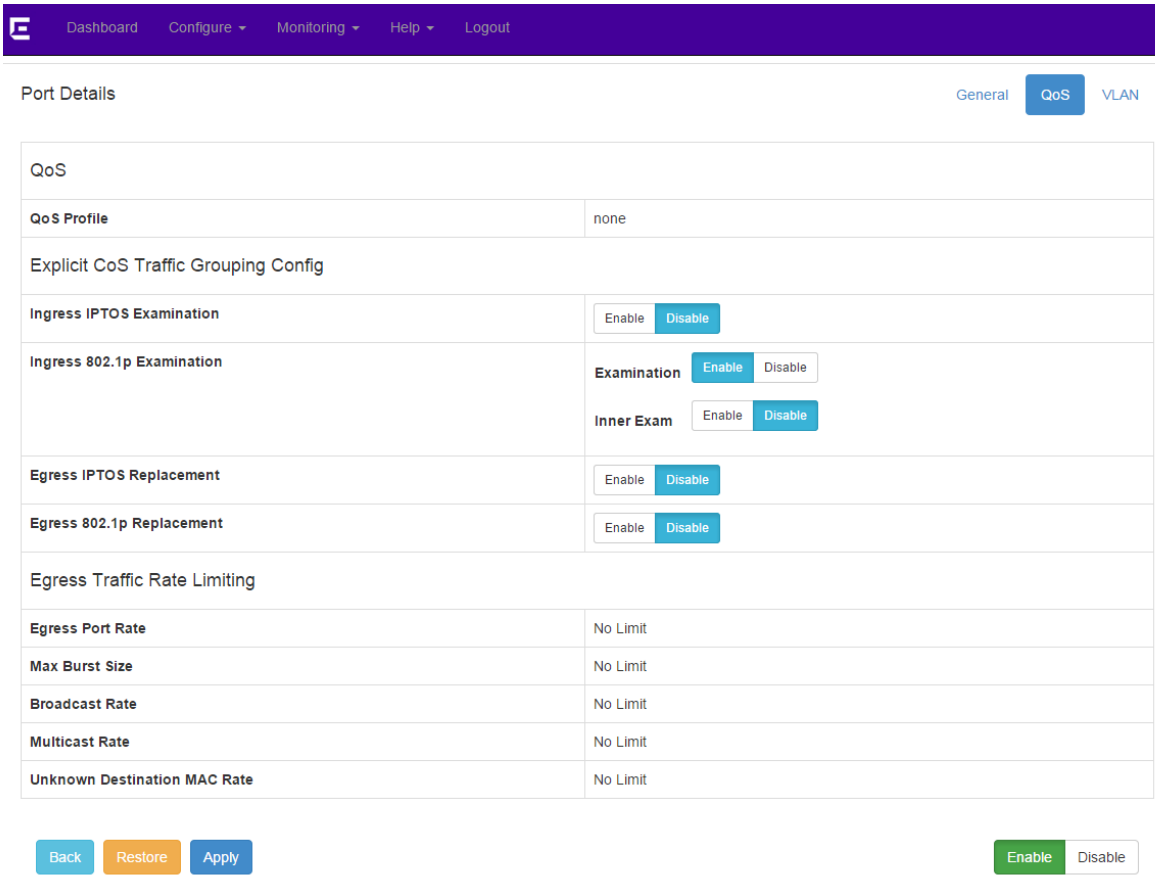
Port Details -- QoS

The **Quality of Service** tab allows you to enable or disable the following traffic groups on a per-port basis:

- Ingress IPTOS Examination
- Ingress 802.1p Examination, both Examination and Inner Exam.

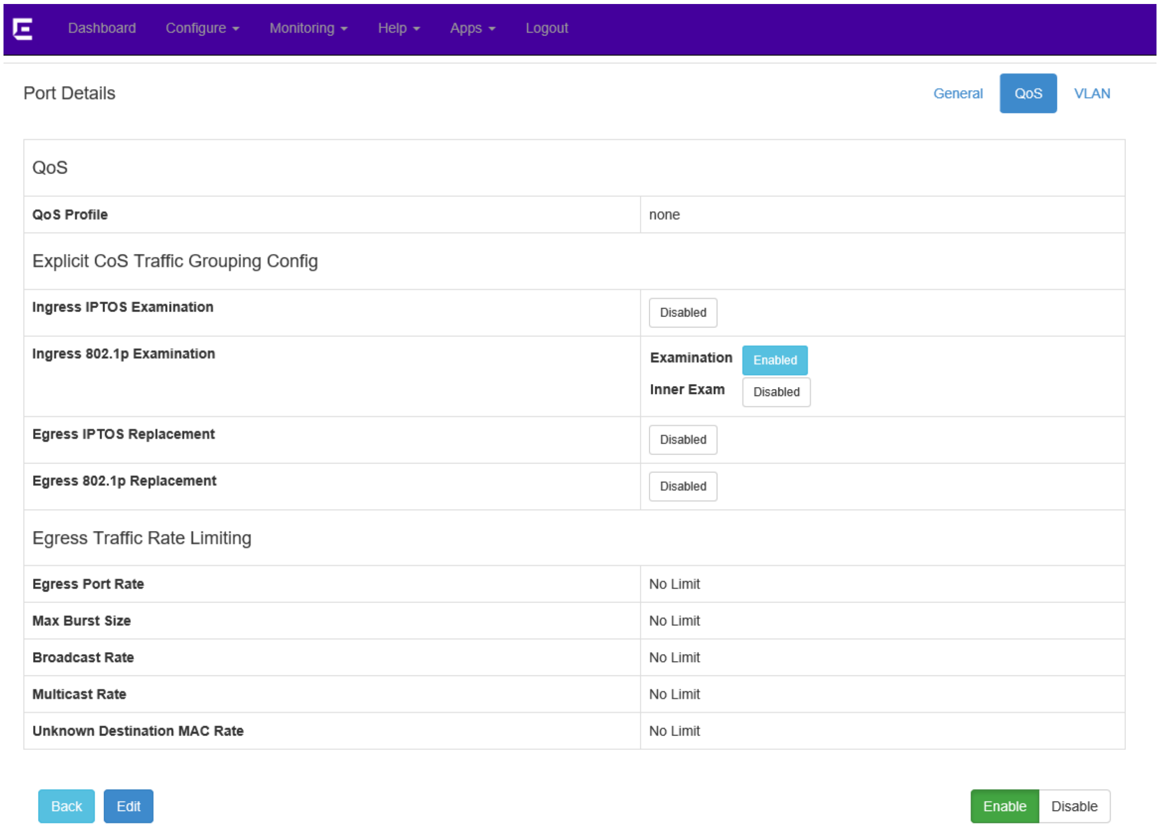
Note
These items are mutually exclusive.

- Egress IPTOS Replacement
- Egress 802.1p



Port Details

QoS	
QoS Profile	none
Explicit CoS Traffic Grouping Config	
Ingress IPTOS Examination	Enable [✓ Disable]
Ingress 802.1p Examination	**Examination** [✓ Enable] Disable **Inner Exam** Enable [✓ Disable]
Egress IPTOS Replacement	Enable [✓ Disable]
Egress 802.1p Replacement	Enable [✓ Disable]
Egress Traffic Rate Limiting	
Egress Port Rate	No Limit
Max Burst Size	No Limit
Broadcast Rate	No Limit
Multicast Rate	No Limit
Unknown Destination MAC Rate	No Limit



Port Details

QoS	
QoS Profile	none
Explicit CoS Traffic Grouping Config	
Ingress IPTOS Examination	Disabled
Ingress 802.1p Examination	**Examination** Enabled **Inner Exam** Disabled
Egress IPTOS Replacement	Disabled
Egress 802.1p Replacement	Disabled
Egress Traffic Rate Limiting	
Egress Port Rate	No Limit
Max Burst Size	No Limit
Broadcast Rate	No Limit
Multicast Rate	No Limit
Unknown Destination MAC Rate	No Limit

When finished, click **Apply** to save your changes. Otherwise:

- Click **Restore** to cancel your changes.
- Click **Back** to return to the **Ports** page.

To disable the port entirely, click **Disable** at the bottom of the screen. To re-enable the port, click **Enable**.

To assign or change the *QoS* Profile, refer to Configuring VLANs on page 35.

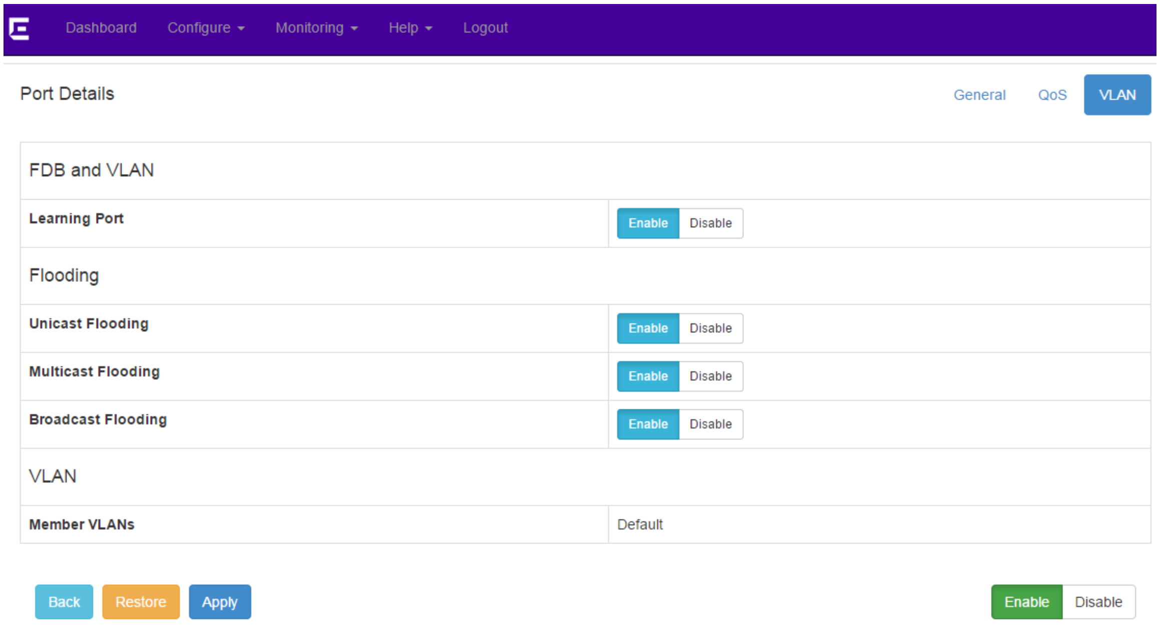
Note
QoS Profiles must be created before you can assign ports. For more information, see "Configuring QoS" in the *ExtremeXOS User Guide*.

Port Details -- VLAN

On the **VLAN** tab, you can enable or disable the following on a per-port basis:

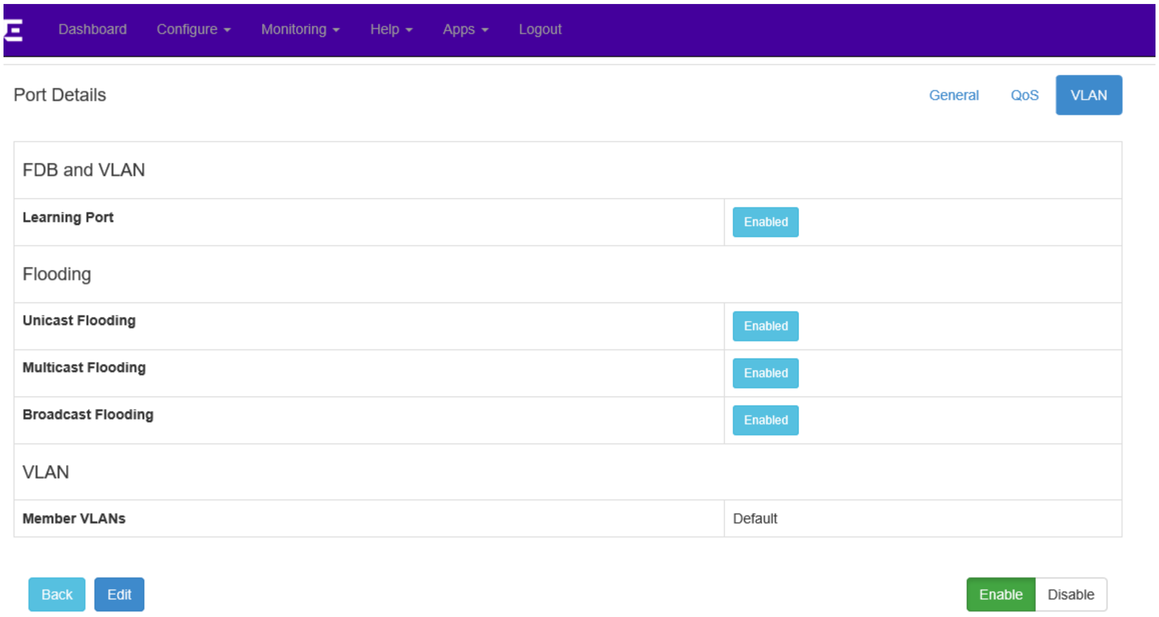
- *FDB (forwarding database)* Learning Port
- Unicast Flooding
- Multicast Flooding
- Broadcast Flooding

This page also displays what *VLAN (Virtual LAN)* this port belongs to. To edit this, continue to Configuring VLANs on page 35.



Port Details

FDB and VLAN	
Learning Port	Enable Disable
Flooding	
Unicast Flooding	Enable Disable
Multicast Flooding	Enable Disable
Broadcast Flooding	Enable Disable
VLAN	
Member VLANs	Default



Port Details

FDB and VLAN	
Learning Port	Enabled
Flooding	
Unicast Flooding	Enabled
Multicast Flooding	Enabled
Broadcast Flooding	Enabled
VLAN	
Member VLANs	Default

When finished, click **Apply** to save your changes. Otherwise:

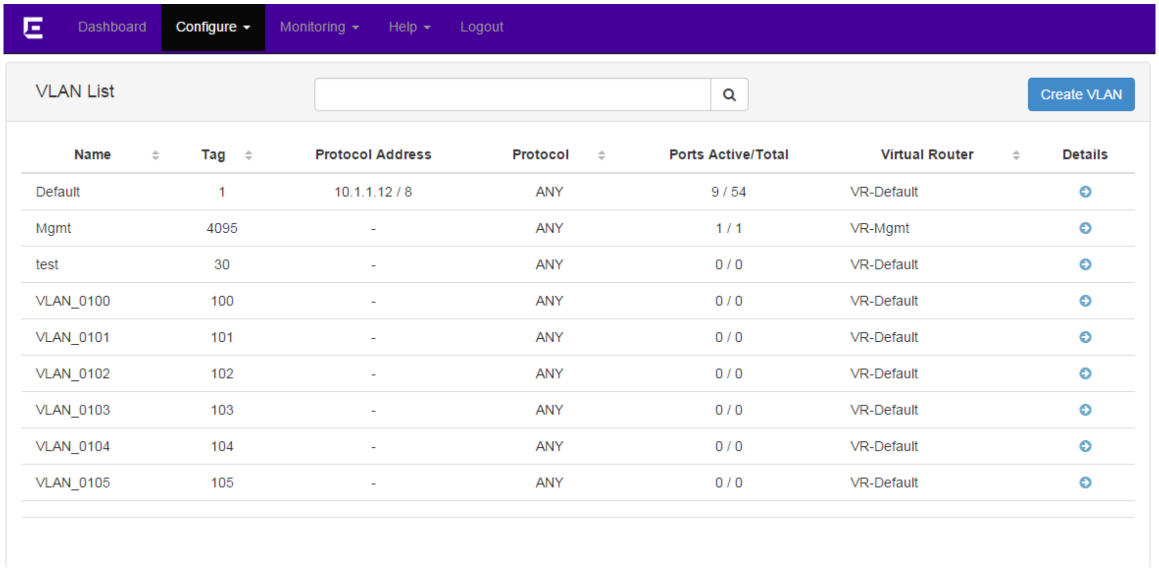
- Click **Restore** to cancel your changes.
- Click **Back** to return to the **Ports** page.

To disable the port entirely, click **Disable** at the bottom of the screen. To re-enable the port, click **Enable**.

Configuring VLANs

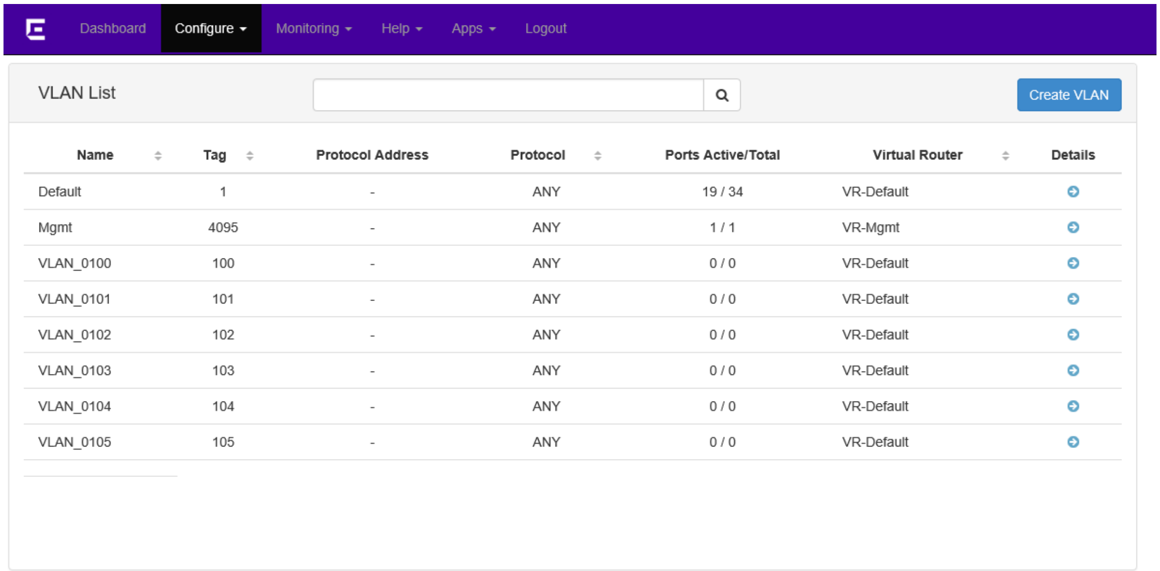
Chalet allows you to create and configure *VLAN*s, tag them, and assign ports and *QoS* profiles. After clicking the **VLANs** table from the Dashboard, or after selecting **Configure** > **VLAN**, you are directed to the **VLAN List** page.

Note
Assigning VLANs into VRs is not currently supported in Chalet. Any VLANs that are created are assigned to *VR-Default* automatically. To create a VLAN in a different VR, create them through the CLI (see the `create vlan` command in the *ExtremeXOS Command Reference Guide*).



VLAN List

Name	Tag	Protocol Address	Protocol	Ports Active/Total	Virtual Router	Details
Default	1	10.1.1.12 / 8	ANY	9 / 54	VR-Default	➡
Mgmt	4095	-	ANY	1 / 1	VR-Mgmt	➡
test	30	-	ANY	0 / 0	VR-Default	➡
VLAN_0100	100	-	ANY	0 / 0	VR-Default	➡
VLAN_0101	101	-	ANY	0 / 0	VR-Default	➡
VLAN_0102	102	-	ANY	0 / 0	VR-Default	➡
VLAN_0103	103	-	ANY	0 / 0	VR-Default	➡
VLAN_0104	104	-	ANY	0 / 0	VR-Default	➡
VLAN_0105	105	-	ANY	0 / 0	VR-Default	➡



VLAN List

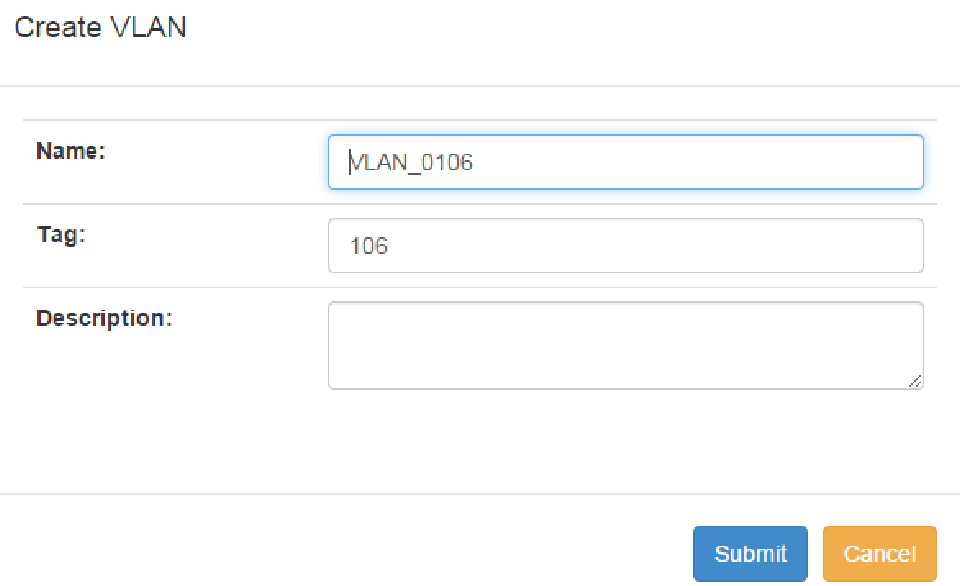
Name	Tag	Protocol Address	Protocol	Ports Active/Total	Virtual Router	Details
Default	1	-	ANY	19 / 34	VR-Default	➡
Mgmt	4095	-	ANY	1 / 1	VR-Mgmt	➡
VLAN_0100	100	-	ANY	0 / 0	VR-Default	➡
VLAN_0101	101	-	ANY	0 / 0	VR-Default	➡
VLAN_0102	102	-	ANY	0 / 0	VR-Default	➡
VLAN_0103	103	-	ANY	0 / 0	VR-Default	➡
VLAN_0104	104	-	ANY	0 / 0	VR-Default	➡
VLAN_0105	105	-	ANY	0 / 0	VR-Default	➡

This page displays a list of all VLANs in alphabetical order, but the list can be sorted by any column or filtered using the search bar.

Clicking the ➡ to the right of a VLAN displays the Assign Ports page.

To create a new VLAN:

1. Click the **Create VLAN** button.



Create VLAN

Name:	VLAN_0106
Tag:	106
Description:	

2. In the pop-up dialog, provide a name for the VLAN. This is required.
3. Provide a VLAN tag and description, if desired.
4. Click **Submit**.

   You are directed back to the **VLAN List** page, with the new VLAN listed.

5. To edit the details of the VLAN, click the ➔ to the right.

   The **VLAN Details** page displays, showing the **General** tab by default.

   On this page, you can edit every field with a drop-down menu or a text field.

6. To save your edits, click **Apply**. If you do not want to save, choose one of the following options:
   - Click **Restore** to cancel your edits.
   - Click **Back** to return to the **VLAN List** page.
   - Click **Delete** to delete the VLAN and return to the **VLAN List** page.

To assign ports to the new VLAN, refer to Assigning Ports to VLANs on page 36.

Assigning Ports to VLANs

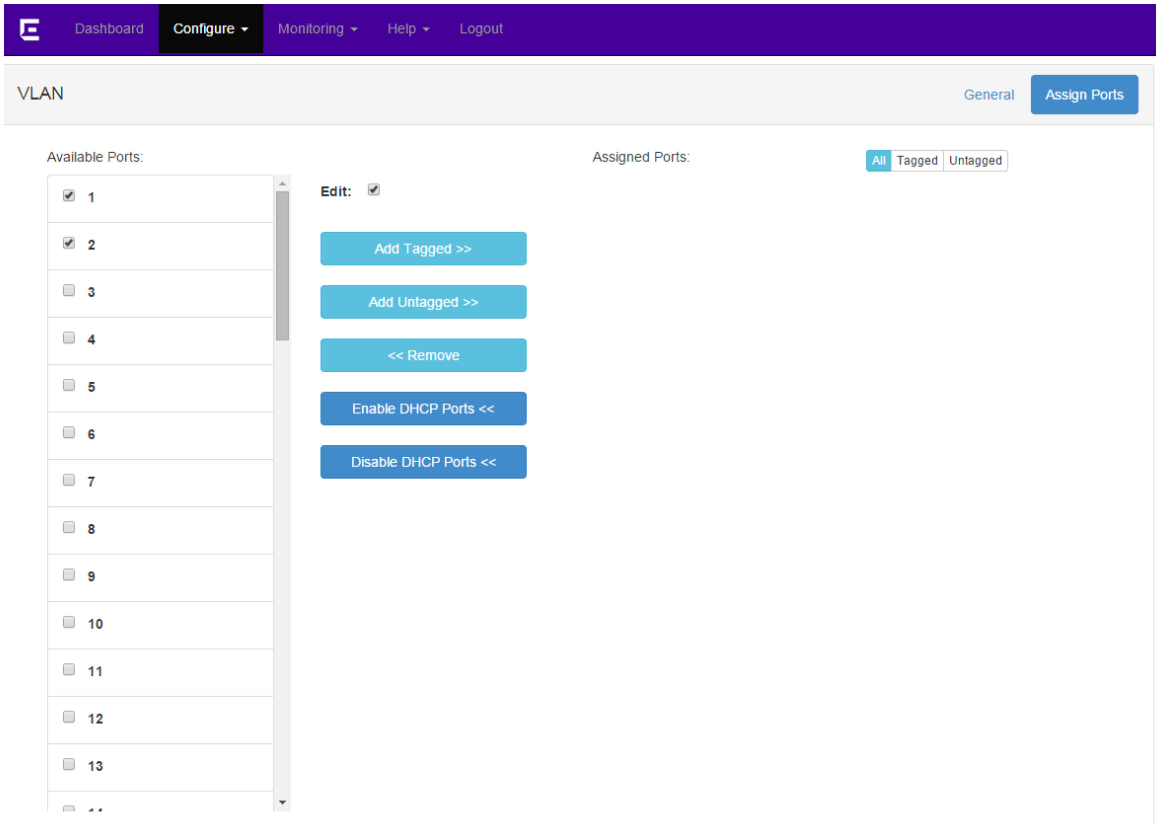
Assigning tagged and untagged ports to a *VLAN* is simple and quick with Chalet.

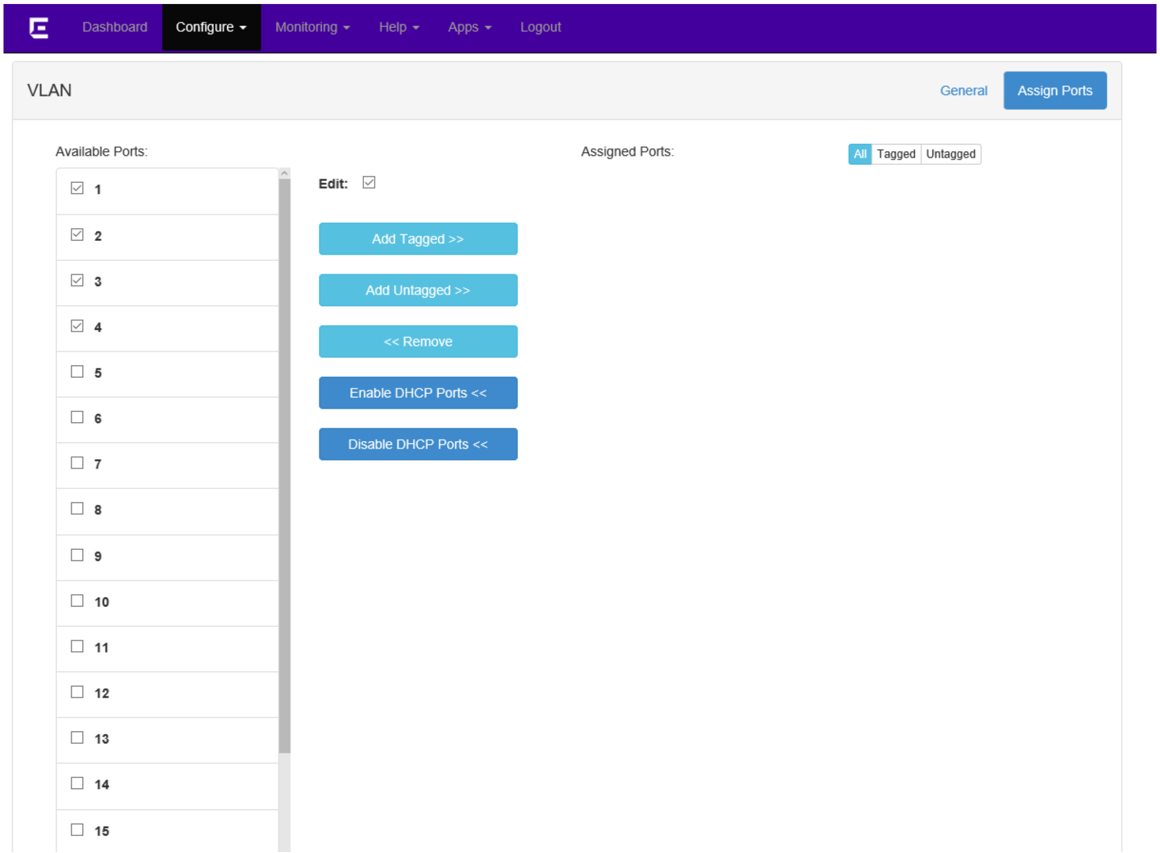
1. To begin, select **Configure** > **VLAN**, and then click the ➔ next to the VLAN you wish to assign ports to.

   The **General** tab displays.

2. Select the **Assign Ports** tab, and then select the **Edit** checkbox. This stops the refresh timer so the switch will not update during this configuration.

   The Available Ports list and buttons become active.


Dashboard
Configure
Monitoring
Help
Logout
VLAN
General
Assign Ports
Available Ports:
Assigned Ports:
All
Tagged
Untagged
Edit: ☑
☑ 1
☑ 2
☐ 3
☐ 4
☐ 5
☐ 6
☐ 7
☐ 8
☐ 9
☐ 10
☐ 11
☐ 12
☐ 13
Add Tagged >>
Add Untagged >>
<< Remove
Enable DHCP Ports <<
Disable DHCP Ports <<


Dashboard
Configure
Monitoring
Help
Apps
Logout
VLAN
General
Assign Ports
Available Ports:
Assigned Ports:
All
Tagged
Untagged
Edit: ☑
☑ 1
☑ 2
☑ 3
☑ 4
☐ 5
☐ 6
☐ 7
☐ 8
☐ 9
☐ 10
☐ 11
☐ 12
☐ 13
☐ 14
☐ 15
Add Tagged >>
Add Untagged >>
<< Remove
Enable DHCP Ports <<
Disable DHCP Ports <<

3. Select the check boxes next to the ports you wish to assign, and then click **Add Tagged** or **Add Untagged**

   The ports move to the "Assigned Ports" area on the right.
4. To remove ports from the VLAN, select the ports from the Assigned Ports area and then click **Remove**.
5. When finished, clear the **Edit** checkbox to restart the refresh timer.
6. Click **Save Config** to save your changes.
7. To confirm that your changes have been made to the switch, click ➔.

   You are directed to the **Port Details** page.
8. Click the **VLAN** tab to see that the Member VLANs field has been updated.

To enable *DHCP (Dynamic Host Configuration Protocol)* on the assigned ports, refer to Enabling DHCP on page 38.

Enabling DHCP

If desired, Chalet allows you to configure the *DHCP* server included in the switch, including the IP address range, IP address lease, and multiple DHCP options. For more information about this feature, see the "DHCP Server" section of the *ExtremeXOS User Guide*.

You must first assign ports to VLANs (see Assigning Ports to VLANs on page 36) before you can enable DHCP on the ports.

1. To begin, select **Configure** > **VLAN**, and then click the ➔ next to the *VLAN* you wish to enable DHCP on.

   The **General** tab displays.
2. Click **Edit**.
3. Assign IP address ranges. The Primary IP on the VLAN is required.

   Note
   DHCP IP ranges must be in the same subnet.
4. Click **Apply** to save your changes.
5. Select the **Assign Ports** tab.
6. Select the **Edit** checkbox. This stops the refresh timer so the switch will not update during this configuration.
7. Select the ports you just added and then click **Enable DHCP Ports**.
8. When finished, clear the **Edit** checkbox to restart the refresh timer.
9. Click **Save Config** to save your changes.
10. To confirm your changes, return to the **General** tab. The **DHCP Ports** area will display the ports enabled with DHCP.
11. To disable DHCP ports, return to the **Assign Ports** tab and select the **Edit** checkbox.
12. Select the ports from the Assigned Ports area and then click **Disable DHCP Ports**.
13. When finished, clear the **Edit** checkbox to restart the refresh timer.
14. Click **Save Config** to save your changes.

15. To confirm your changes, return to the **General** tab to see the updated **DHCP Ports** area.

Configuring Dynamic ACLs

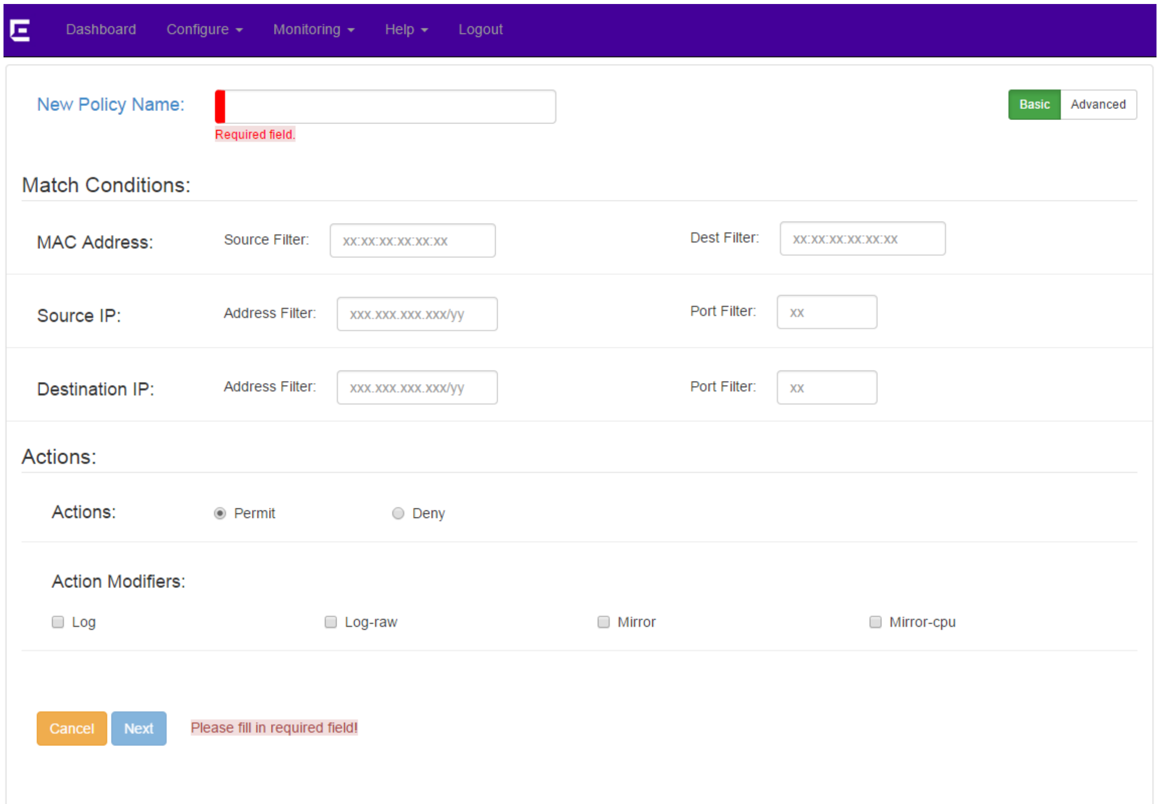
The **Dynamic Access Control Lists** page allows you to create dynamic rules for *ACL*s and is equivalent to entering the command `create access-list` *`dynamic_rule conditions actions`* `{`**`non_permanent`**`}` with its different variables.

> Note
> For more information, refer to the *ACL Solutions Guide* or the ACLs section of the *ExtremeXOS User Guide*.

1. Select **Configure** > **Dyanmic ACL**.

   Any current ACLs on the switch will be listed in a searchable table.
2. Click the **Create Policy** button.

   A new screen displays showing the match conditions and actions (defaulted to the **Basic** tab). Clicking the **Advanced** tab shows more configuration options.



New Policy Name:

Required field.

Match Conditions:

MAC Address: Source Filter: xx:xx:xx:xx:xx:xx Dest Filter: xx:xx:xx:xx:xx:xx

Source IP: Address Filter: xxx.xxx.xxx.xxx/yy Port Filter: xx

Destination IP: Address Filter: xxx.xxx.xxx.xxx/yy Port Filter: xx

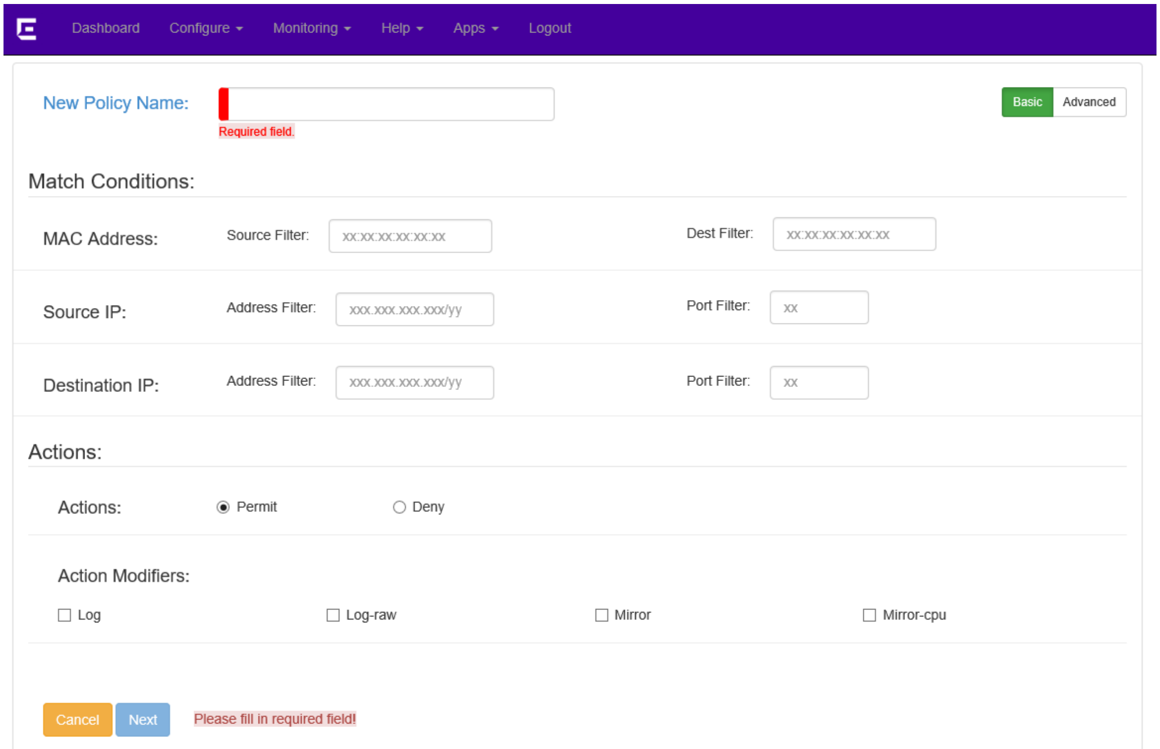
Actions:

Actions: ● Permit ○ Deny

Action Modifiers:

□ Log □ Log-raw □ Mirror □ Mirror-cpu

Please fill in required field!



New Policy Name:

Required field.

Match Conditions:

MAC Address: Source Filter: xx:xx:xx:xx:xx:xx Dest Filter: xx:xx:xx:xx:xx:xx

Source IP: Address Filter: xxx.xxx.xxx.xxx/yy Port Filter: xx

Destination IP: Address Filter: xxx.xxx.xxx.xxx/yy Port Filter: xx

Actions:

Actions: ● Permit ○ Deny

Action Modifiers:

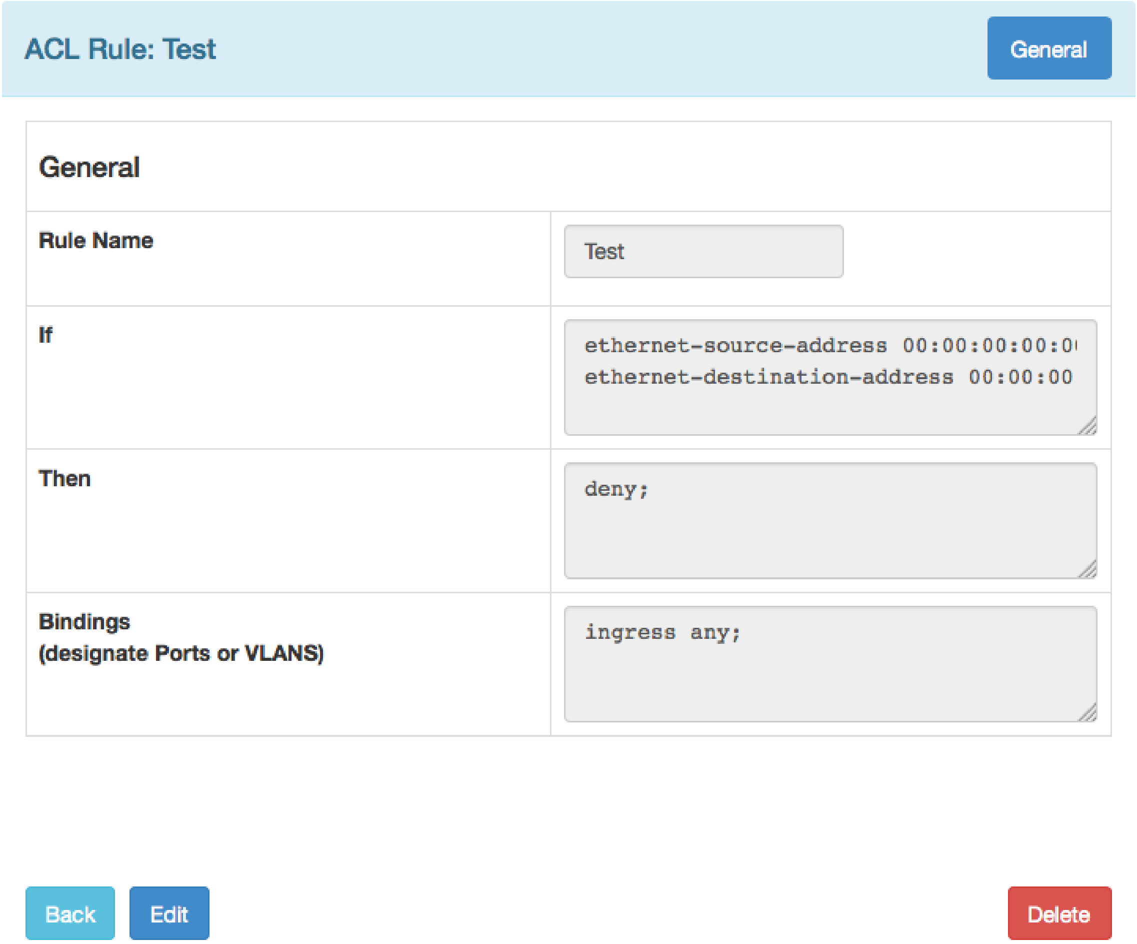
□ Log □ Log-raw □ Mirror □ Mirror-cpu

Please fill in required field!

3. Give the policy a name and provide IP addresses and actions. When complete, click **Next**.
4. On the **ACL Rule: <policy name>** page, complete the **If** area by entering the enternet-source and ethernet-destination addresses.

5. Complete the **Then** field (`deny;` is common here).
6. In the **Bindings** area, determine where this policy will be used—VLANs, ports, or both, and egress or ingress.

   The following examples show ACLs applying the to VLANs and Ports using `ingress any;` and `egress any;`



ACL Rule: Test

General

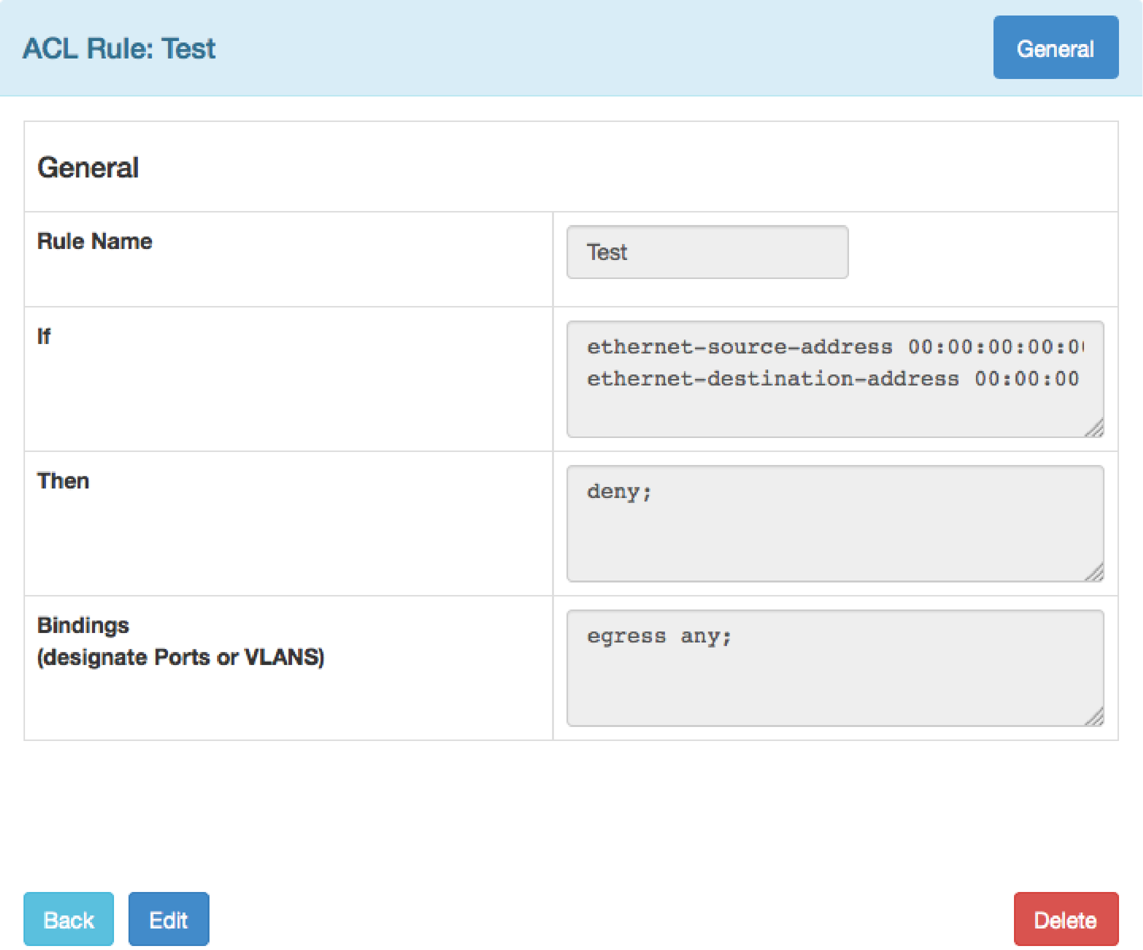
Rule Name	Test

If	`ethernet-source-address 00:00:00:00:0`
	`ethernet-destination-address 00:00:00`

Then	`deny;`
Bindings (designate Ports or VLANS)	`ingress any;`

To create this ACL in the CLI, you would use the following commands:

```
create access-list Test
    "ethernet-source-address 00:00:00:00:00:01 ;
    ethernet-destination-address 00:00:00:00:00:02 ;"
    " deny  ;" application "Cli"
configure access-list add Test last priority 0 zone SYSTEM any ingress
```



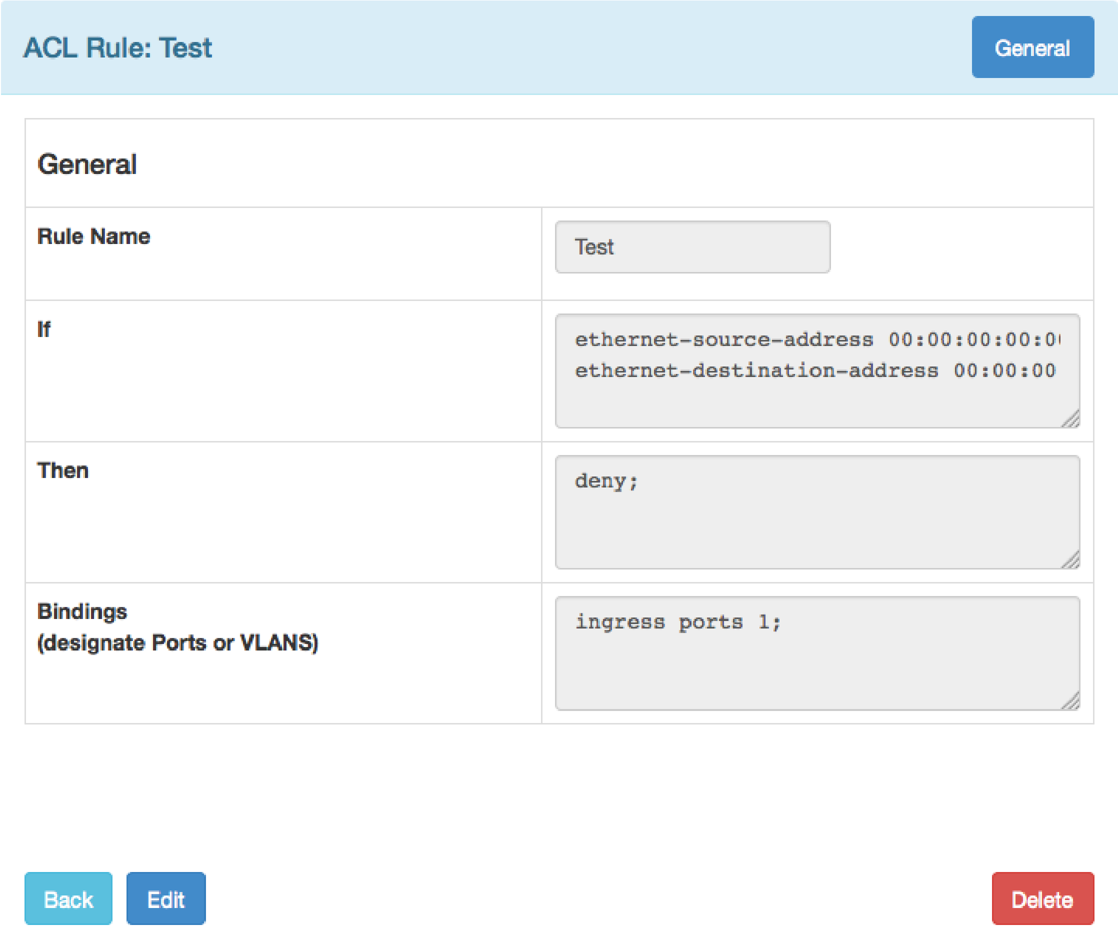
General

Rule Name	Test
If	ethernet-source-address 00:00:00:00:0 ethernet-destination-address 00:00:00
Then	deny;
Bindings (designate Ports or VLANS)	egress any;

To create this ACL in the CLI, you would use the following commands:

```
create access-list Test
    "ethernet-source-address 00:00:00:00:00:01 ;
    ethernet-destination-address 00:00:00:00:00:02 ;"
    " deny  ;" application "Cli"
configure access-list add Test last priority 0 zone SYSTEM any egress
```

The following ACL examples apply bindings to only ports on ingress and egress. For Summit platforms, use the port number only; for SummitStack and chassis, use the slot:port format.

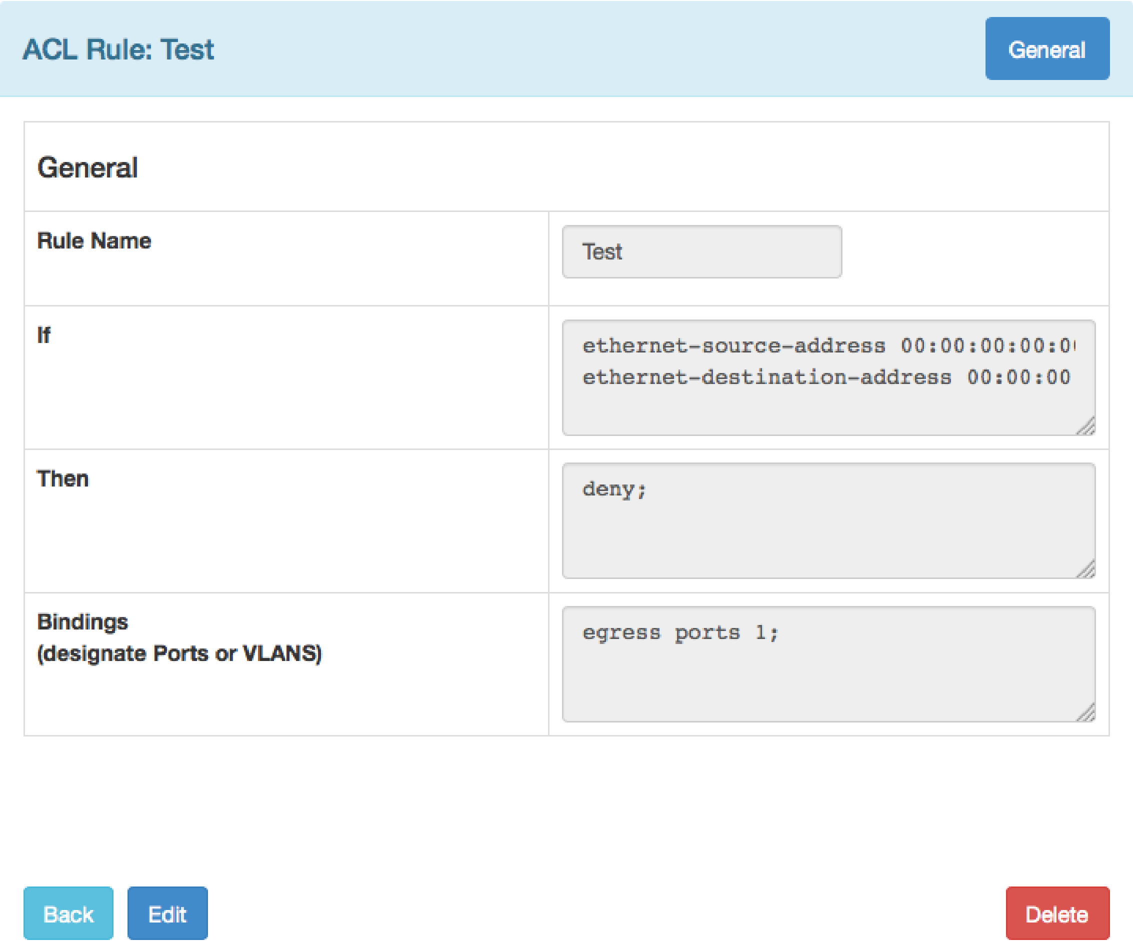


General

Rule Name	Test
If	ethernet-source-address 00:00:00:00:0 ethernet-destination-address 00:00:00
Then	deny;
Bindings (designate Ports or VLANS)	ingress ports 1;

To create this ACL in the CLI, use the following commands:

```
create access-list Test
    " ethernet-source-address 00:00:00:00:00:01 ;
    ethernet-destination-address 00:00:00:00:00:02 ;"
    " deny  ;" application "Cli"
configure access-list add Test last priority 0 zone SYSTEM ports 1 ingress
```



ACL Rule: Test

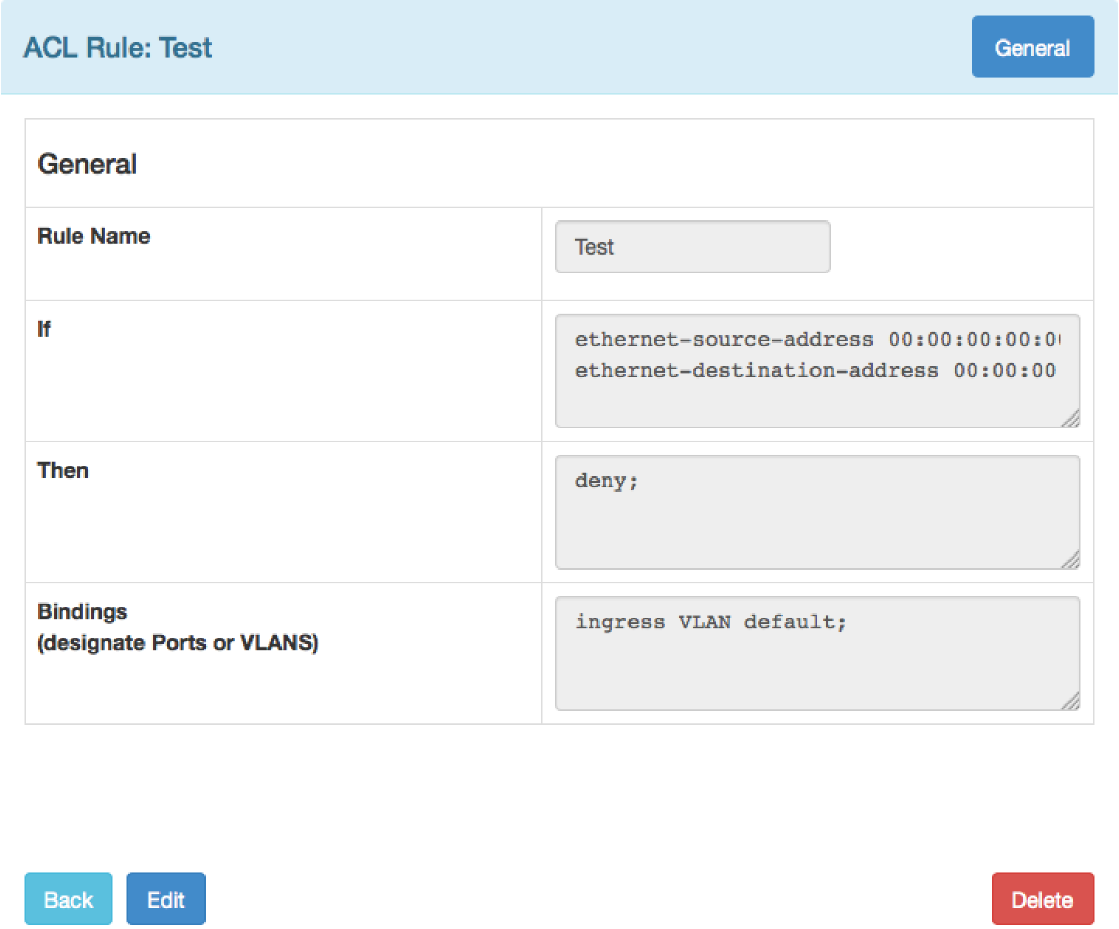
General

Rule Name	Test
If	ethernet-source-address 00:00:00:00:0 ethernet-destination-address 00:00:00
Then	deny;
Bindings (designate Ports or VLANS)	egress ports 1;

To create this ACL in the CLI, use the following commands:

```
create access-list Test
    " ethernet-source-address 00:00:00:00:00:01 ;
    ethernet-destination-address 00:00:00:00:00:02 ;"
    " deny  ;" application "Cli"
configure access-list add Test last priority 0 zone SYSTEM ports 1 egress
```

The following example ACLs apply bindings to ports on a specific *VLAN* on ingress and egress (assuming the VLAN has been created previously). These examples use the Default VLAN.

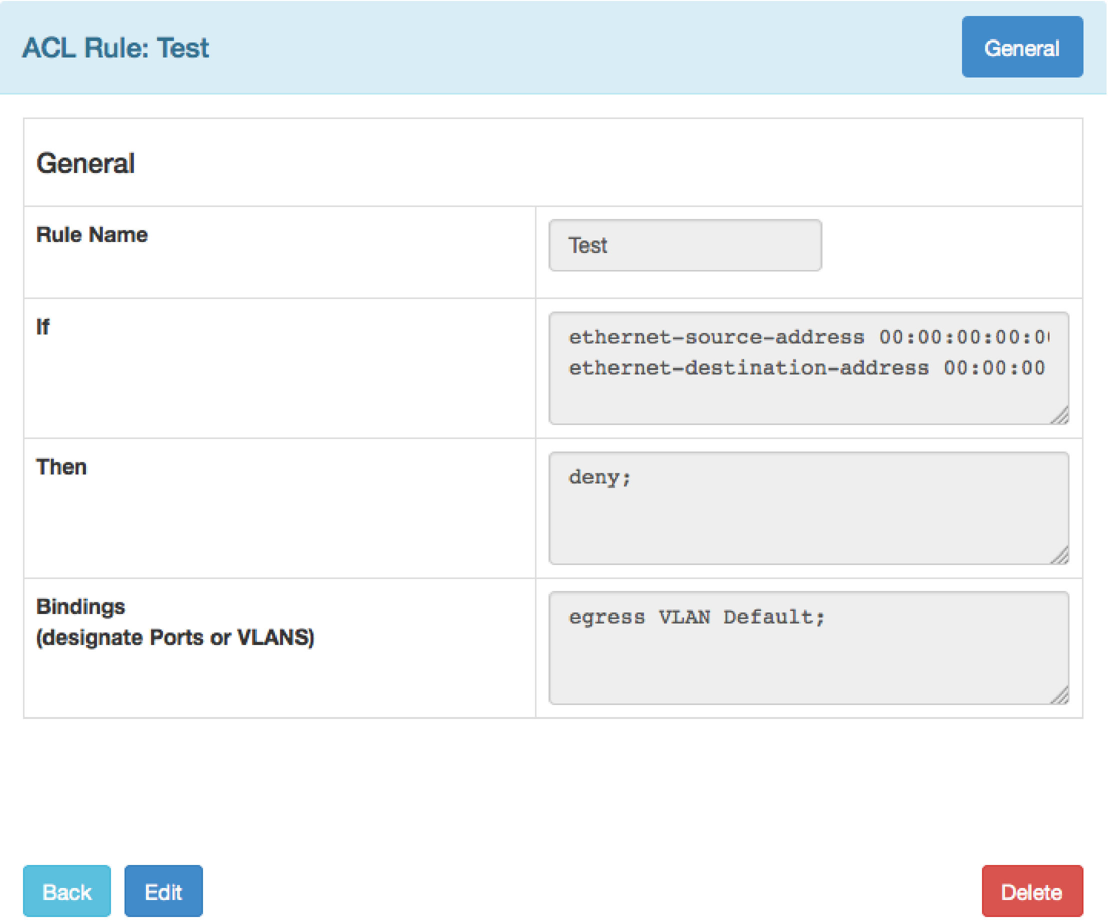


General

Rule Name	Test
If	ethernet-source-address 00:00:00:00:0 ethernet-destination-address 00:00:00
Then	deny;
Bindings **(designate Ports or VLANS)**	ingress VLAN default;

To create this ACL in the CLI, use the following commands:

```
create access-list Test
    " ethernet-source-address 00:00:00:00:00:01 ;
    ethernet-destination-address 00:00:00:00:00:02 ;"
    " deny  ;" application "Cli"
configure access-list add Test last priority 0 zone SYSTEM vlan Default ingress
```



General

Rule Name	Test
If	ethernet-source-address 00:00:00:00:0 ethernet-destination-address 00:00:00
Then	deny;
Bindings (designate Ports or VLANS)	egress VLAN Default;

To create this ACL in the CLI, use the following commands:

```
create access-list Test
    " ethernet-source-address 00:00:00:00:00:01 ;
    ethernet-destination-address 00:00:00:00:00:02 ;"
    " deny  ;" application "Cli"
configure access-list add Test last priority 0 zone SYSTEM vlan Default egress
```

7. Click **Apply** to complete the policy setup, or click **Delete** to start over.

When the ACL is complete, you are returned to the **Dynamic Access Control Lists** screen, where your new policy will be displayed.

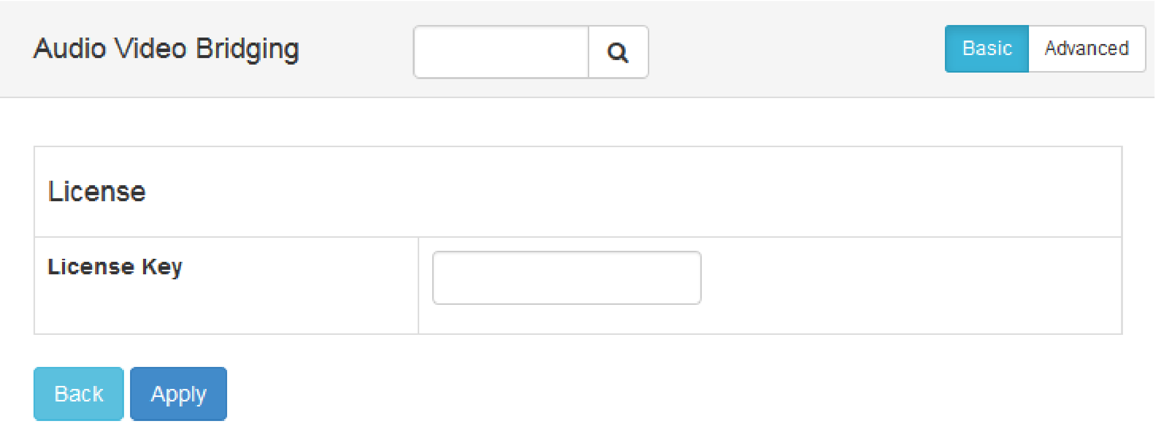
Configuring Audio Video Bridges

Chalet allows you to enable or disable the Audio Video Bridging (AVB) feature to the switch and all ports, and is the equivalent of issuing commands `enable avb` and `enable avb ports [`*`port_list`*` | `**`all`**`]` (and their equivalent disable commands). Transmitter and receiver devices must be set up before enabling AVB.

Note
AVB is only supported on a few Summit platforms. For more information, refer to the *Using AVB with Extreme Switches* guide and the "AVB" section of the *ExtremeXOS User Guide*.

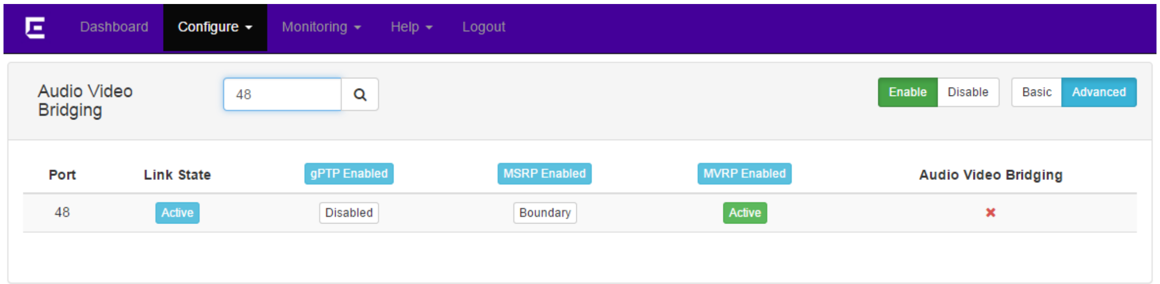
To enable AVB from Chalet, your switch must be AVB-capable and you must have an existing license. Follow the instructions below to enter the license key and configure the feature.

1. Select **Configure** > **Audio Video Bridging**.

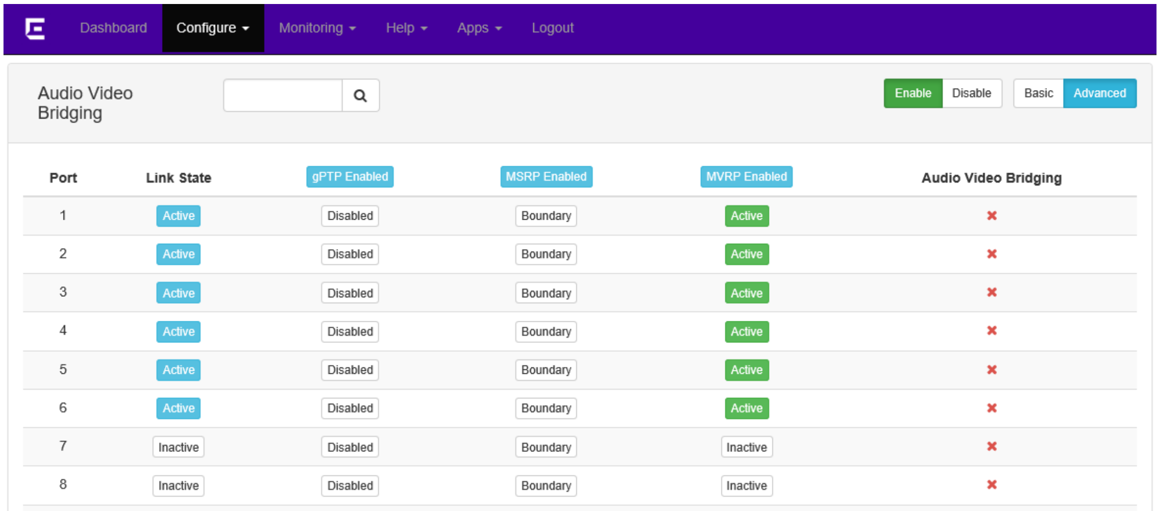


2. Enter the AVB license key and click **Apply**.

   Chalet pushes the license information the switch. Once complete, the page refreshes and displays a list of ports.



Port	Link State	gPTP Enabled	MSRP Enabled	MVRP Enabled	Audio Video Bridging
48	Active	Disabled	Boundary	Active	✖



Port	Link State	gPTP Enabled	MSRP Enabled	MVRP Enabled	Audio Video Bridging
1	Active	Disabled	Boundary	Active	✖
2	Active	Disabled	Boundary	Active	✖
3	Active	Disabled	Boundary	Active	✖
4	Active	Disabled	Boundary	Active	✖
5	Active	Disabled	Boundary	Active	✖
6	Active	Disabled	Boundary	Active	✖
7	Inactive	Disabled	Boundary	Inactive	✖
8	Inactive	Disabled	Boundary	Inactive	✖

Note

If you see ✖ next to a port, AVB is not functioning on that port. A receiver and transmitter must be properly set up for AVB to function.

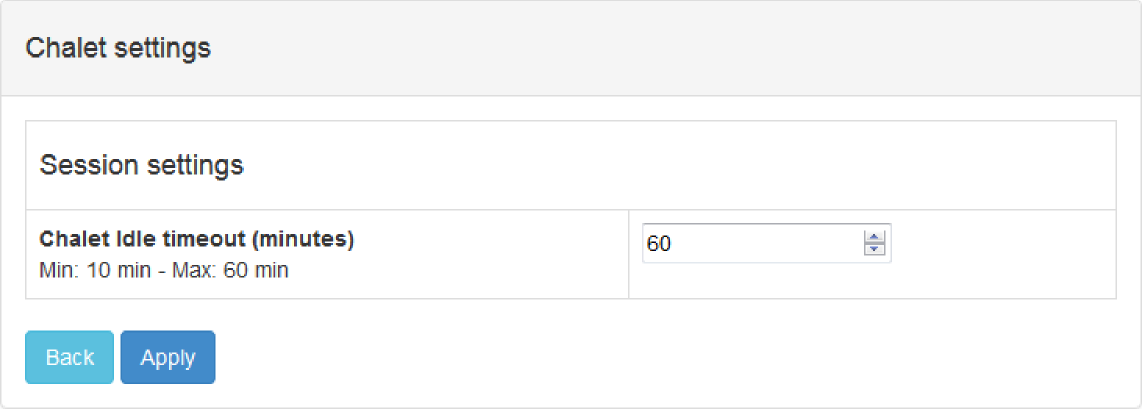
3. Click the **Advanced** tab to see enable/disable information for gPTP, MSRP, and MVRP.

Configuring Chalet Settings

You can configure Chalet's settings, including session idle timeout for the user currently logged in. There is no global setting, so each user will set their individual preferences from this screen.

> Note
> Your browser will store this value so you do not have to set the idle timeout each time you log in. However, if you switch browsers, you will need to configure this setting for the new browser.

1. Select **Configure** > **Chalet**.
2. From the **Session settings** area, type the number of minutes your session will last. The default is 10 minutes.
3. Click **Apply** and then **Save Config**.



Chalet settings

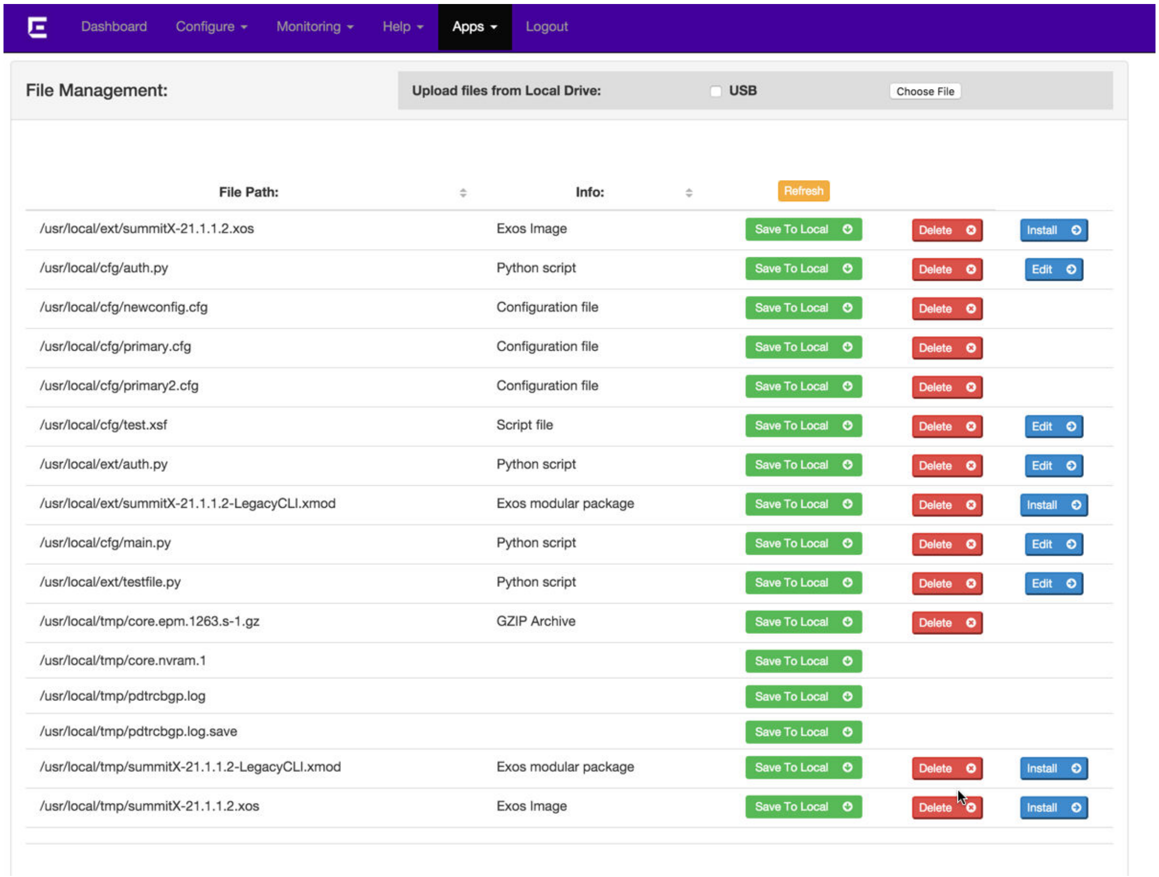
Session settings

Chalet Idle timeout (minutes)
Min: 10 min - Max: 60 min

60

Using the File Manager App

The File Manager application is new for the ExtremeXOS 21.1 release. This app allows you to upload and manage from your local drive or a USB drive plugged into the switch, and then install or configure them directly on the switch. You can also move files from the switch to your local drive with the **Save to Local** button.



File Management:

Upload files from Local Drive: □ USB Choose File

File Path:	Info:	Refresh		
/usr/local/ext/summitX-21.1.1.2.xos	Exos Image	Save To Local	Delete	Install
/usr/local/cfg/auth.py	Python script	Save To Local	Delete	Edit
/usr/local/cfg/newconfig.cfg	Configuration file	Save To Local	Delete	
/usr/local/cfg/primary.cfg	Configuration file	Save To Local	Delete	
/usr/local/cfg/primary2.cfg	Configuration file	Save To Local	Delete	
/usr/local/cfg/test.xsf	Script file	Save To Local	Delete	Edit
/usr/local/ext/auth.py	Python script	Save To Local	Delete	Edit
/usr/local/ext/summitX-21.1.1.2-LegacyCLI.xmod	Exos modular package	Save To Local	Delete	Install
/usr/local/cfg/main.py	Python script	Save To Local	Delete	Edit
/usr/local/ext/testfile.py	Python script	Save To Local	Delete	Edit
/usr/local/tmp/core.epm.1263.s-1.gz	GZIP Archive	Save To Local	Delete	
/usr/local/tmp/core.nvram.1		Save To Local		
/usr/local/tmp/pdtrcbgp.log		Save To Local		
/usr/local/tmp/pdtrcbgp.log.save		Save To Local		
/usr/local/tmp/summitX-21.1.1.2-LegacyCLI.xmod	Exos modular package	Save To Local	Delete	Install
/usr/local/tmp/summitX-21.1.1.2.xos	Exos Image	Save To Local	Delete	Install

Uploading and Editing Files

You can upload files directly to the switch from your local. You can upload any file that the switch can read, including configurations, policies, Python fies, and scripts. This is especially helpful when wanting to transfer files to another switch.

Note

File storage locations are:

- `/usr/local/ext`—Files uploaded to the USB drive plugged into the switch.
- `user/local/cfg`—Scripts and configuration files uploaded to the switch.
- `/usr/local/tmp`—XMOD and XOS images sent directly to the switch

You can also upload ExtremeXOS images and XMODs for upgrades and maintenance. For more information, see Upgrading ExtremeXOS Using the File Manager on page 51.

1. If uploading a file to a USB drive on the switch, select the **USB**.

   Note

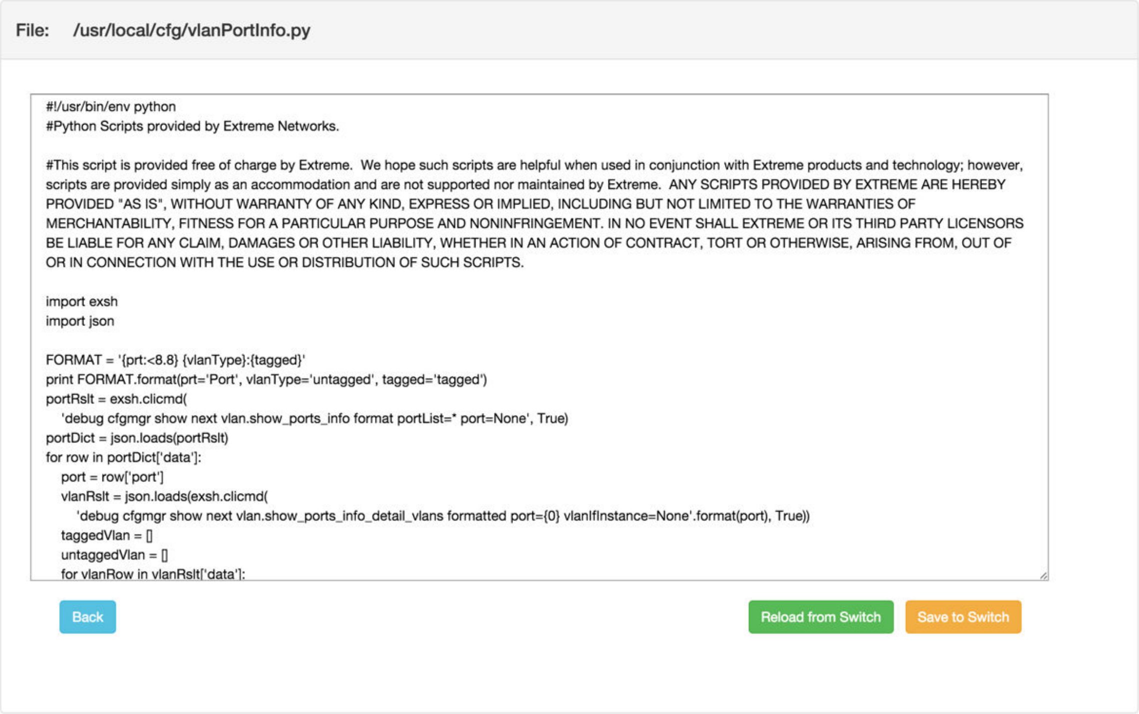
   If no USB drive is present, the checkbox is not visible.

2. Click the **Browse** button to add the file.

   Note
   File upload is slower over wireless connections.

3. To edit a configuration file or script directly, click **Edit** next to the file.

   The file editor page displays.



File: /usr/local/cfg/vlanPortInfo.py

```
#!/usr/bin/env python
#Python Scripts provided by Extreme Networks.

#This script is provided free of charge by Extreme.  We hope such scripts are helpful when used in conjunction with Extreme products and technology; however,
scripts are provided simply as an accommodation and are not supported nor maintained by Extreme.  ANY SCRIPTS PROVIDED BY EXTREME ARE HEREBY
PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL EXTREME OR ITS THIRD PARTY LICENSORS
BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF
OR IN CONNECTION WITH THE USE OR DISTRIBUTION OF SUCH SCRIPTS.

import exsh
import json

FORMAT = '{prt:<8.8} {vlanType}:{tagged}'
print FORMAT.format(prt='Port', vlanType='untagged', tagged='tagged')
portRslt = exsh.clicmd(
    'debug cfgmgr show next vlan.show_ports_info format portList=* port=None', True)
portDict = json.loads(portRslt)
for row in portDict['data']:
    port = row['port']
    vlanRslt = json.loads(exsh.clicmd(
        'debug cfgmgr show next vlan.show_ports_info_detail_vlans formatted port={0} vlanIfInstance=None'.format(port), True))
    taggedVlan = []
    untaggedVlan = []
    for vlanRow in vlanRslt['data']:
```

4. When editing is complete, you can:

   - **Save to Switch**—Takes the content of the current window and saves it to the switch, replacing the existing file.
   - **Reload from Switch**—Pulls what is currently saved on the switch and replaces the content in the current window.

Getting 'show tech' Output for Customer Support

If you are consulting with Extreme Networks Customer Support, you may be asked to send output from the `show tech` command.

To do this in Chalet:

1. Navigate to **Apps** > **File Manager**.
2. Click **Save Show Tech Output To Local Drive**.

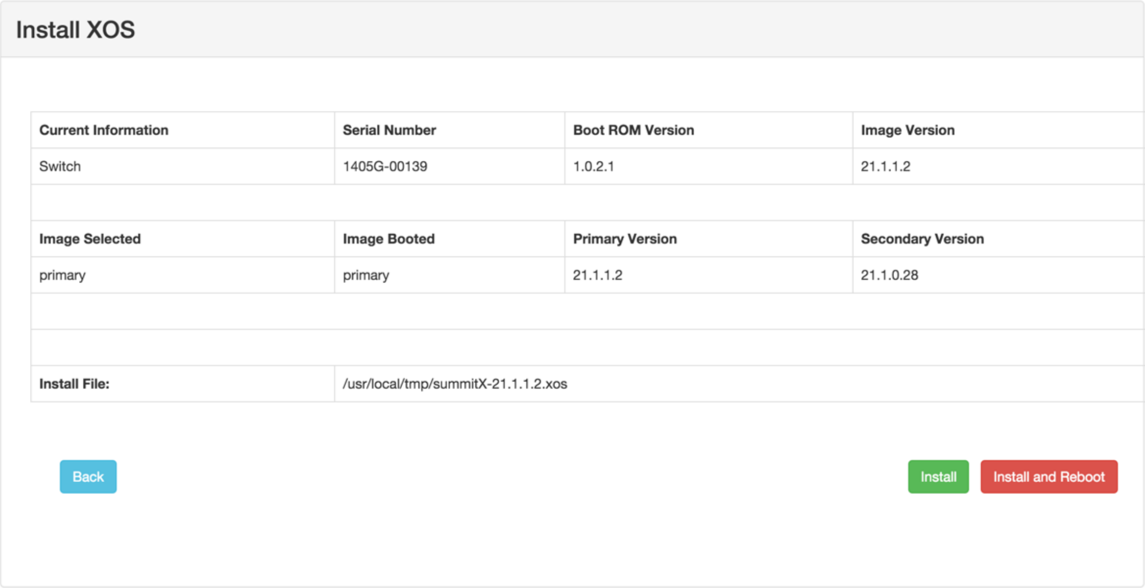
   The switch will generate the output and provide a zipped text file, which you can then forward to Customer Support.

Upgrading ExtremeXOS Using the File Manager

You can upgrade your ExtremeXOS 21.x and later image with Chalet's File Manager app.

> Note
>
> You cannot upgrade the ExtremeXOS image on ExtremeSwitching 5320, 5420 and X435 series switches using Chalet due to their limited storage capacity. To upgrade 4120, ExtremeSwitching 5320, 5320 extended temperature, 5420 and X435 series switches, use the CLI interface. For information about upgrading ExtremeXOS using the CLI interface, see the *ExtremeXOS User Guide*.

1. Upload the ExtremeXOS image or XMOD file (see Uploading and Editing Files on page 49).
2. To install, choose your installation method:
   - **Install**—Installs the image on the inactive partition.
   - **Install and Reboot**—Replaces the image on the inactive partition, saves the configuration, and then reboots the switch.

   Install XOS

Current Information	Serial Number	Boot ROM Version	Image Version
Switch	1405G-00139	1.0.2.1	21.1.1.2
Image Selected	**Image Booted**	**Primary Version**	**Secondary Version**
primary	primary	21.1.1.2	21.1.0.28
Install File:	/usr/local/tmp/summitX-21.1.1.2.xos		

   If the image fails to install, delete the file, upload it again, and try to install it again. For further help, .
3. After rebooting the switch, confirm that the booted image displayed on the Dashboard has changed.

Configuring MLAG with the ezMLAG2 Wizard

The ezMLAG2 wizard, which is new for ExtremeXOS 21.1, was created to simplify the configuration of *MLAG (Multi-switch Link Aggregation Group)* peers and devices. It also helps prevent users from configuring MLAGs that should not be done between peer switches.

Note

The multi-switch link aggregation group (MLAG) feature allows you to combine ports on two switches to form a single logical connection to another network device. MLAG requires two ExtremeXOS switches interconnected by an Inter-Switch Connection (ISC). These connected peers can then monitor the health of the ISC using a keep-alive protocol that periodically sends health-check messages. If the ISC link alone goes down when the remote peer is alive, both the MLAG peers forward the south-bound traffic, resulting in duplication of traffic. However, this does not create a traffic loops. For more information about MLAG, see "Configuring Slots and Ports on a Switch" in the *ExtremeXOS User Guide*.

ezMLAG2 Limitations and Restrictions

- ezMLAG2 only runs on ExtremeXOS 21.x and later.
- Only administrator accounts can use the ezMLAG2 wizard. Viewing *MLAG* setup will be added to user level accounts in a future release.
- Chassis are not supported in ExtremeXOS 21.x.
- Stacking is not currently supported.
- Two tier is not currently supported.
- Only two peers can be configured at a time. You can connect to the next set of switches if needed.
- If an MLAG configuration already exists, only maintenance tasks can be performed. (Currently it is a summary of the current configuration. Future releases will have more functionality.)
- VLANs on MLAG devices must be configured through the CLI.

MLAG Configuration Overview

The ezMLAG2 wizard:

- Discovers ISC links.
- Creates the ISC VLAN and VR for the ISC *VLAN*. (Different configurations and VRF configuration are possible in future releases.)
- Creates the ISC VLAN IP address, which is computed from the switch MAC and uses a link local address.
- Sets up the *LAG (Link Aggregation Group)* on the ISC port and adds it to the ISC VLAN.
- Creates MLAG peers.
- Discovers MLAG devices and LAGs.
- Enables MLAG on a set of ports to MLAG devices.
- Adds VLANs to an MLAG ID.
- Provides a summary of what VLANS belong to switch set of MLAG ports.

Pre-Configuration Setup

Before you begin configuring MLAG with Chalet, ensure that:

- LAGs are pre-configured on the MLAG devices (servers/switches) prior to running the ezMLAG2 wizard. LACP needs to be configured if you plan to use LACP discovery.
- Peer switches start with no configuration before using the ezMLAG2 app.

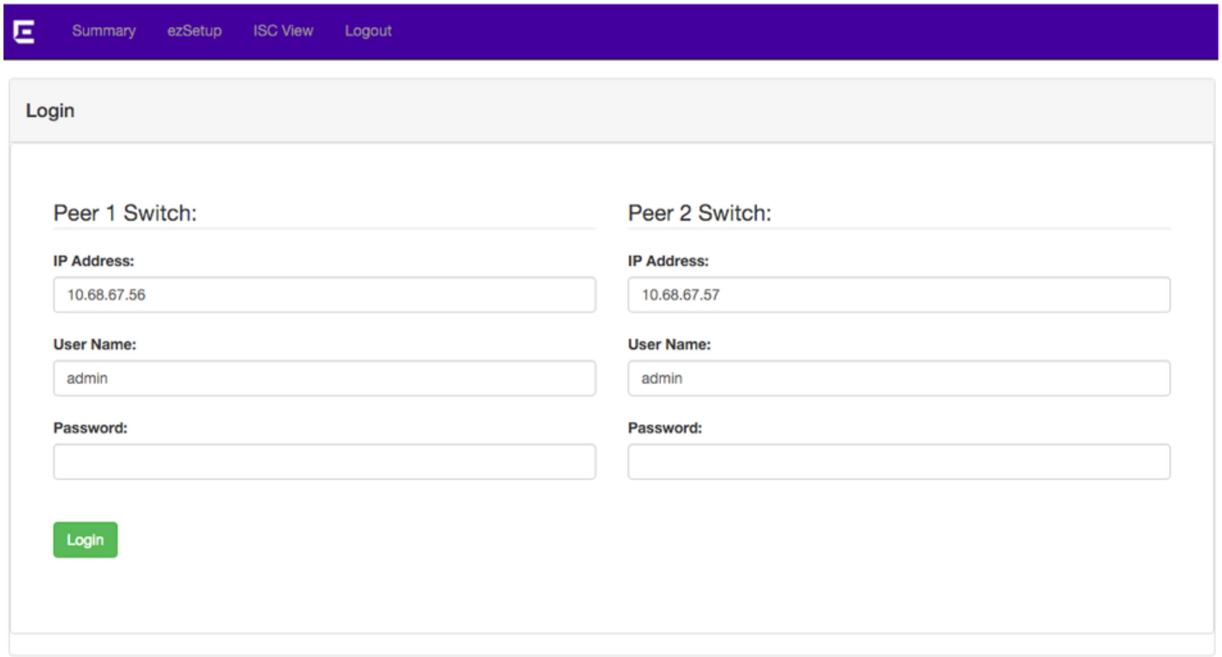
ezMLAG Wizard Configuration Process

1. Log in to each peer (see Getting Started with the ezMLAG App on page 53).
2. Once past the requirements check, the ISC ports are auto-discovered using *EDP (Extreme Discovery Protocol)*, and you will be asked to either accept the discovered ports or make modifications to them. Then ezMLAG2 will use those ports as part of the MLAG configuration (see Setting up ISC Ports on page 57).
3. Select the discovery protocol -- either LACP (recommended) or -- and enable MLAG on discovered ports (see Discovering Devices on page 59).*EDP*
4. Finally, add VLAN tags to the selected ports, either manually or automatically (see Adding VLANs to MLAG Devices on page 63).
5. MLAG is now configured. Confirm information on the Summary page (see MLAG Summary on page 64).

Getting Started with the ezMLAG App

1. Select **Apps** > **ezMLAG2**.

   The **Login** screen displays.



Login

Peer 1 Switch:

IP Address: 10.68.67.56

User Name: admin

Password:

Peer 2 Switch:

IP Address: 10.68.67.57

User Name: admin

Password:

2. Complete the IP Address, User Name, and Password fields for Peer 2, as the information for Peer 1 will be automatically populated with the administrator account you used to access Chalet.
3. Click **Login**.

After logging in, Chalet sends the following commands to the switch to help prevent loops that may occur in the default VLAN during device discovery:

```
configure stpd s0 mode dot1w
enable stpd s0
enable edp port all
```

Note
EDP is enabled because it is needed for device discovery later in the process.

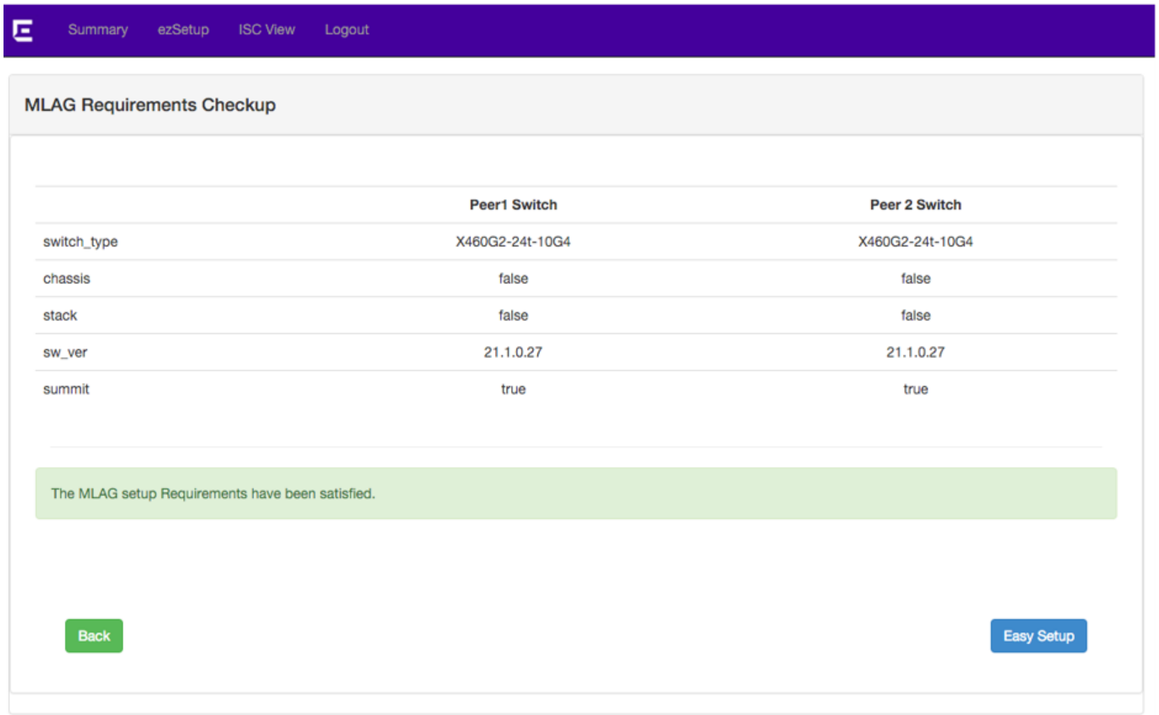
Chalet performs a requriements check to ensure the peers are optimized for MLAG.

MLAG Requirements Check

After logging in, Chalet performs a requirements check to ensure MLAG can be set up between the two peers. The requirements check is based on the recommendations found in the *ExtremeXOS User Guide*.

- MLAG peer switches must be of the same platform family.
- With standalone switches, we strongly recommend that MLAG peers be the same switch type.
- MLAG peers should run the same version of ExtremeXOS for proper functioning. To upgrade your switches, see Upgrading ExtremeXOS Using the File Manager on page 51.
- Chassis are not currently supported (specifically in ExtremeXOS 21.1) Chalet must ensure they are not peers.
- If Chalet finds any of these, you will be warned on what can and cannot be done.

If the requirements are satisfied, click **Easy Setup** to continue.



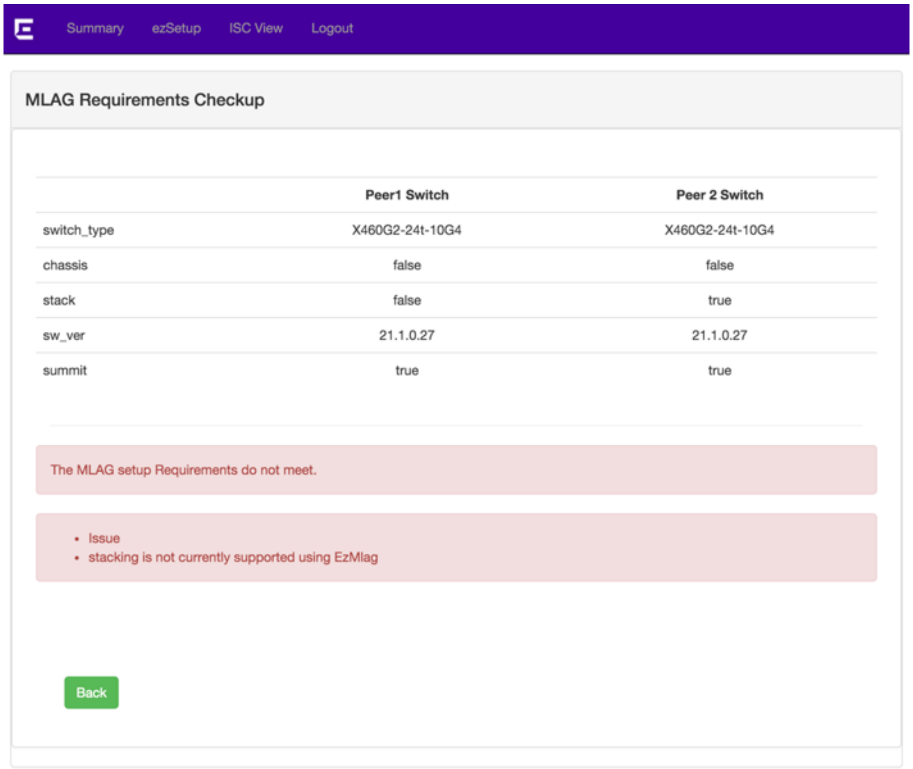
MLAG Requirements Checkup

	Peer1 Switch	Peer 2 Switch
switch_type	X460G2-24t-10G4	X460G2-24t-10G4
chassis	false	false
stack	false	false
sw_ver	21.1.0.27	21.1.0.27
summit	true	true

The MLAG setup Requirements have been satisfied.

Figure 1: Successful Requirements Check

The following image shows that stacking is enabled on one or both peers, so MLAG cannot be configured. Click **Back** to return to the **Dashboard**.



MLAG Requirements Checkup

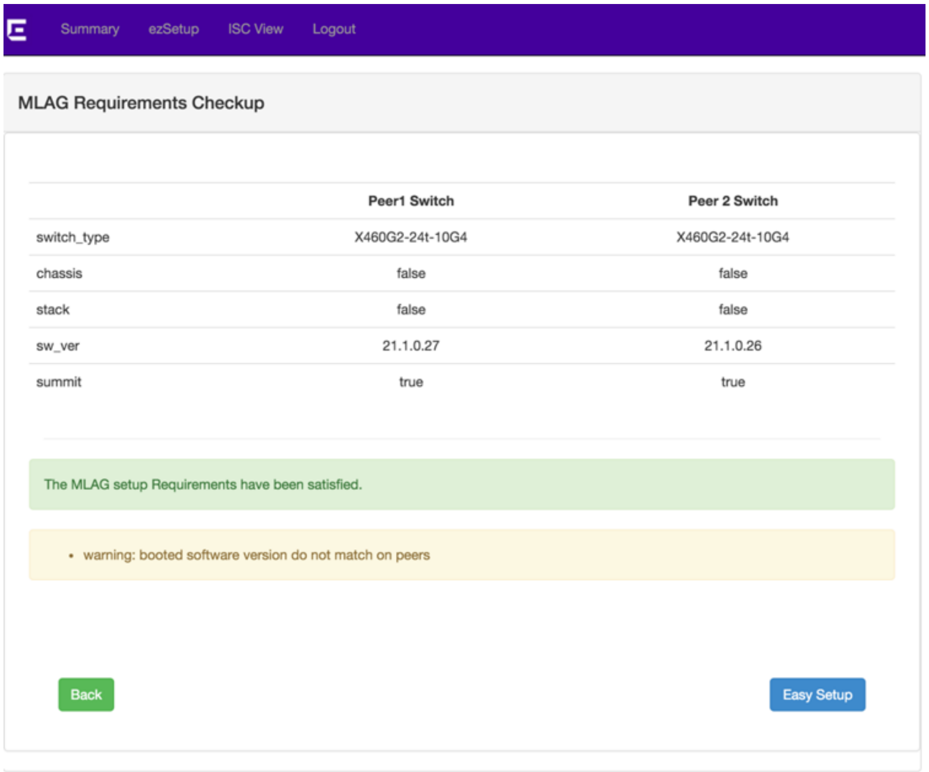
	Peer1 Switch	Peer 2 Switch
switch_type	X460G2-24t-10G4	X460G2-24t-10G4
chassis	false	false
stack	false	true
sw_ver	21.1.0.27	21.1.0.27
summit	true	true

The MLAG setup Requirements do not meet.

- Issue
- stacking is not currently supported using EzMlag

Figure 2: Failed Requirements Check

Although the peers do not share the same ExtremeXOS version, you can still configure MLAG with the wizard. To continue, click **Easy Setup**.



MLAG Requirements Checkup

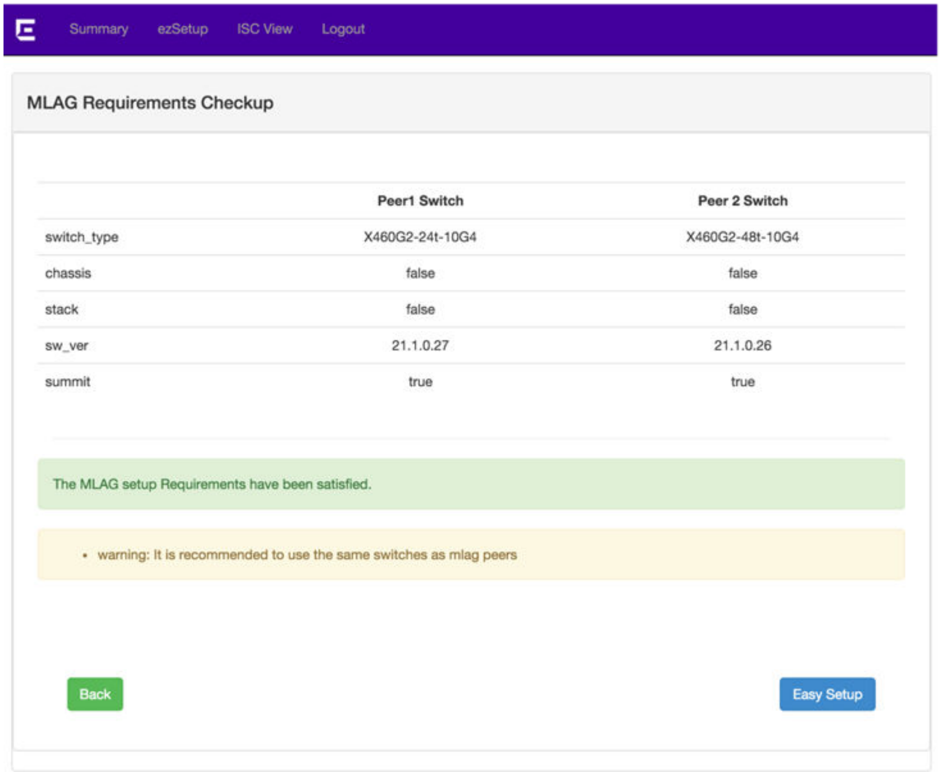
	Peer1 Switch	Peer 2 Switch
switch_type	X460G2-24t-10G4	X460G2-24t-10G4
chassis	false	false
stack	false	false
sw_ver	21.1.0.27	21.1.0.26
summit	true	true

The MLAG setup Requirements have been satisfied.

- warning: booted software version do not match on peers

Figure 3: Example Warning: Software Mismatch

Although the peers are not the same switch type, you can still configure MLAG with the wizard. To continue, click **Easy Setup**.



MLAG Requirements Checkup

	Peer1 Switch	Peer 2 Switch
switch_type	X460G2-24t-10G4	X460G2-48t-10G4
chassis	false	false
stack	false	false
sw_ver	21.1.0.27	21.1.0.26
summit	true	true

The MLAG setup Requirements have been satisfied.

- warning: It is recommended to use the same switches as mlag peers

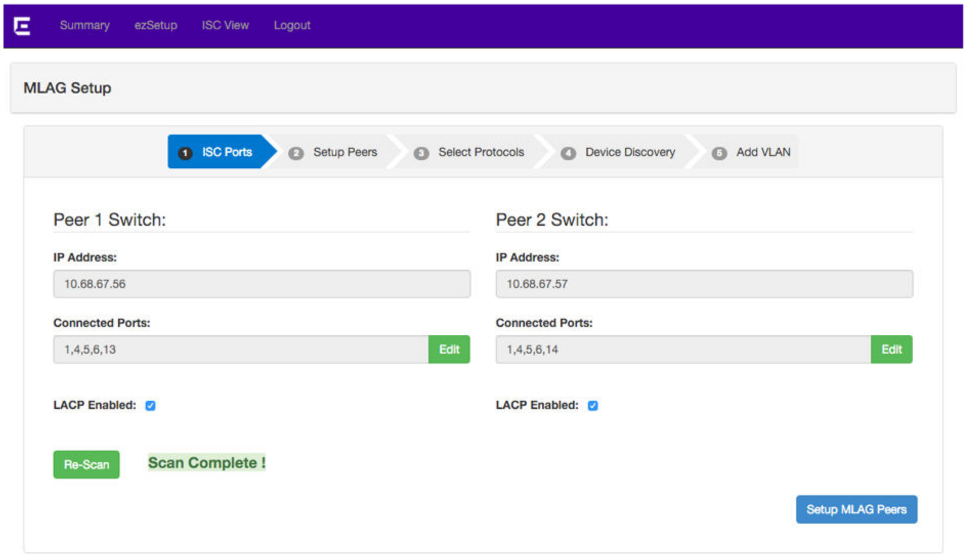
Figure 4: Example Warning: Switch Model Mismatch

Setting up ISC Ports

Using *EDP*, the ports connected between the peers will be automatically discovered. You can then edit which ports are used to construct the ISC.

1. Chalet discovers the ports between the connected ports and populates them on the **ISC Ports** page.

   Note
   We recommend using LACP for this ISC *LAG*.



MLAG Setup

Peer 1 Switch:

IP Address: 10.68.67.56

Connected Ports: 1,4,5,6,13

LACP Enabled: ☑

Scan Complete !

Peer 2 Switch:

IP Address: 10.68.67.57

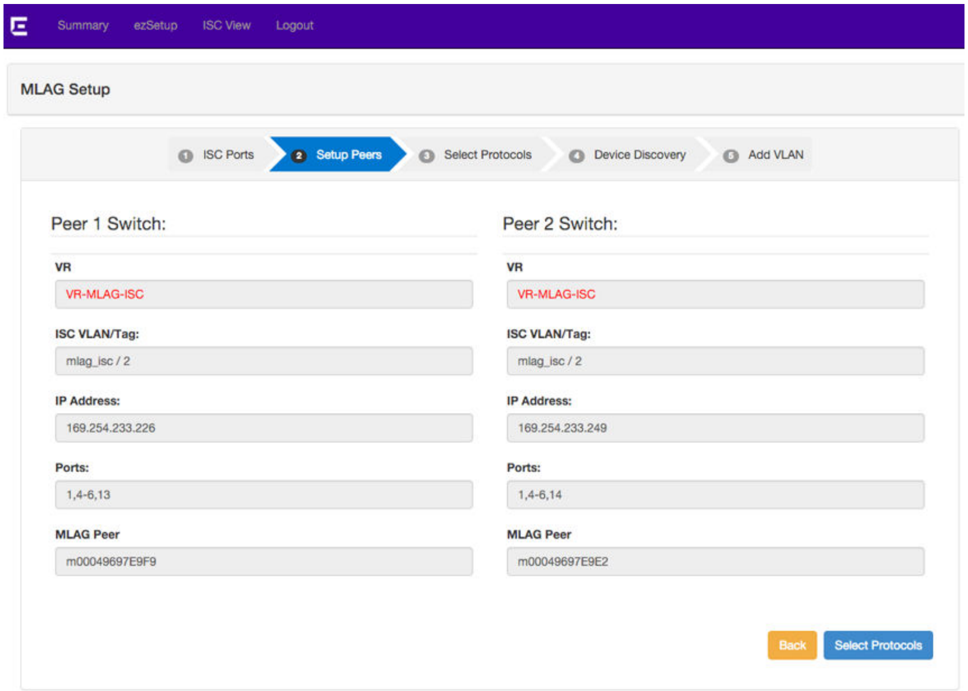
Connected Ports: 1,4,5,6,14

LACP Enabled: ☑

- To edit or add ports, click **Edit**.
- To re-scan for connected ports, click **Re-Scan**.

2. When you are satisfied with the chosen ISC ports, click **Setup MLAG Peers**.

   The **Setup Peers** page displays.



MLAG Setup

Peer 1 Switch:

VR: VR-MLAG-ISC

ISC VLAN/Tag: mlag_isc / 2

IP Address: 169.254.233.226

Ports: 1,4-6,13

MLAG Peer: m00049697E9F9

Peer 2 Switch:

VR: VR-MLAG-ISC

ISC VLAN/Tag: mlag_isc / 2

IP Address: 169.254.233.249

Ports: 1,4-6,14

MLAG Peer: m00049697E9E2

Clicking **Setup MLAG Peers** pushes the following configuration to both peers. If a *virtual router (VR)* is used for the ISC, the ISC ports are removed from any *VLAN*s they may be associated with. The next available tag between both peers is used for the ISC VLAN tag, which in this example is 2.

```
## Peer 1 ##
configure vlan default delete port 1, 4-6, 13
configure Vr VR-Default delete ports 1, 4-6, 13
```

```
enable sharing 1 grouping 1, 4-6, 13 algorithm address-based custom lacp
create vr "VR-MLAG-ISC"
create vlan "mlag_isc" vr VR-MLAG-ISC
configure vlan mlag_isc tag 2
configure vlan mlag_isc add ports 1 tagged
configure vlan mlag_isc ipaddress 169.254.233.226 255.255.0.0

create mlag peer "m00049697E9F9"
configure mlag peer "m00049697E9F9" ip address 169.254.233.249 vr VR-MLAG-ISC

## Peer 2 ##
configure vlan default delete port 1, 4-6, 14
configure Vr VR-Default delete ports 1, 4-6, 14
enable sharing 1 grouping 1, 4-6, 14 algorithm address-based custom lacp
create vr "VR-MLAG-ISC"
create vlan "mlag_isc" vr VR-MLAG-ISC
configure vlan mlag_isc tag 2
configure vlan mlag_isc add ports 1 tagged
configure vlan mlag_isc ipaddress 169.254.233.249 255.255.0.0

create mlag peer "m00049697E9E2"
configure mlag peer "m00049697E9E2" ip address 169.254.233.226 vr VR-MLAG-ISC
```

3. Click **Select Protocols** to continue.

Discovering Devices

You can now choose the discovery method used to find MLAG devices plugged into your configured peers. The discovery converts ports to single-link LAGs and adds LACP to any active ports in the Default *VLAN*. Although this does change existing port configurations, this is the most accurate way to determine which ports are connected to LAGs.

Note
Ports not in the Default VLAN are unaffected by this discovery and may not be detected.

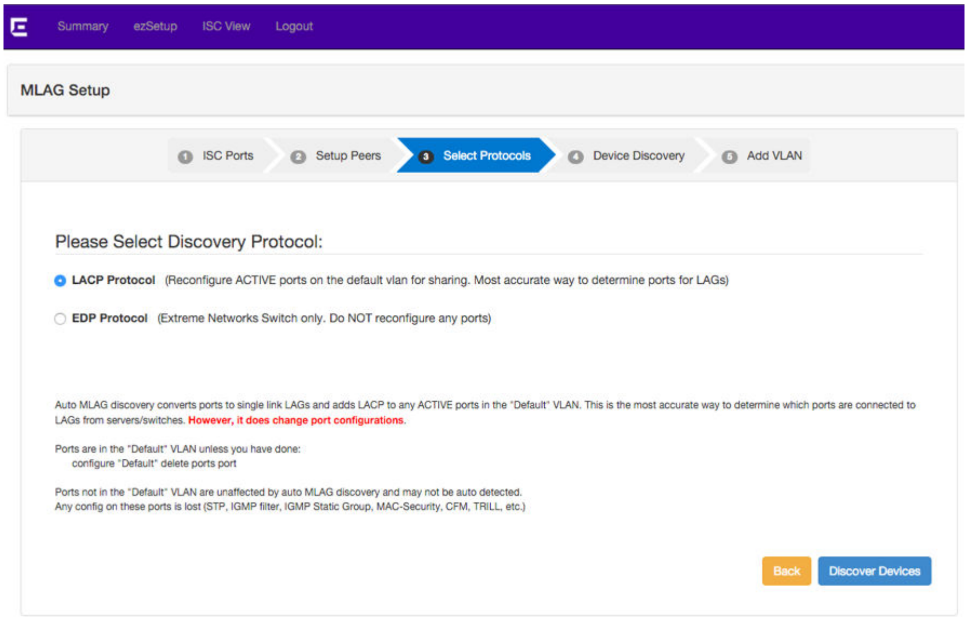
Caution
Any existing configuration on these ports will be lost during discovery. This includes *STP (Spanning Tree Protocol)*, *IGMP (Internet Group Management Protocol)* filter, *IGMP* Static Group, MAC Security, CFM, TRILL, etc.

1. Select the discovery method you want to use:
   - LACP Protocol (use steps 2 on page 60 through 5 on page 62).

     Note
     Load shares must already be configured on the MLAG devices and LACP must be enabled.

   - *EDP* (use steps 6 on page 62 through 7 on page 63).

     Note
     If EDP is chosen as the discovery method, it will only work with Extreme Networks switches.



Please Select Discovery Protocol:

● **LACP Protocol** (Reconfigure ACTIVE ports on the default vlan for sharing. Most accurate way to determine ports for LAGs)

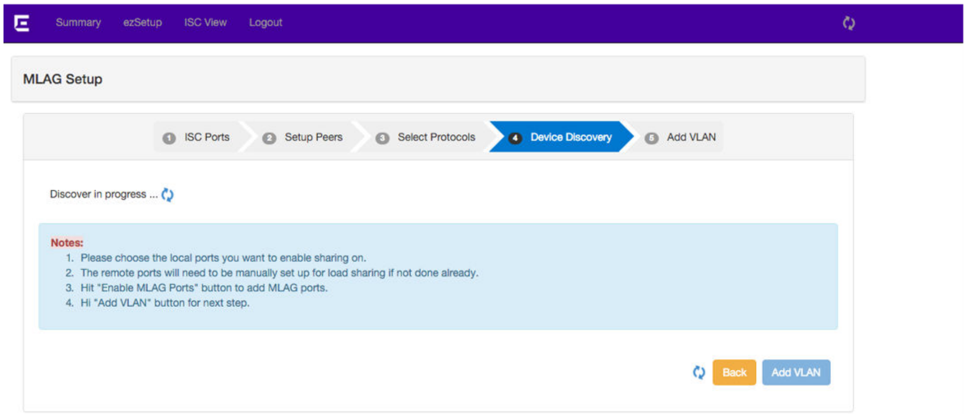
○ **EDP Protocol** (Extreme Networks Switch only. Do NOT reconfigure any ports)

Auto MLAG discovery converts ports to single link LAGs and adds LACP to any ACTIVE ports in the "Default" VLAN. This is the most accurate way to determine which ports are connected to LAGs from servers/switches. **However, it does change port configurations.**

Ports are in the "Default" VLAN unless you have done:
configure "Default" delete ports port

Ports not in the "Default" VLAN are unaffected by auto MLAG discovery and may not be auto detected.
Any config on these ports is lost (STP, IGMP filter, IGMP Static Group, MAC-Security, CFM, TRILL, etc.)

2. Click **Discover Devices** to begin.



Discover in progress ...

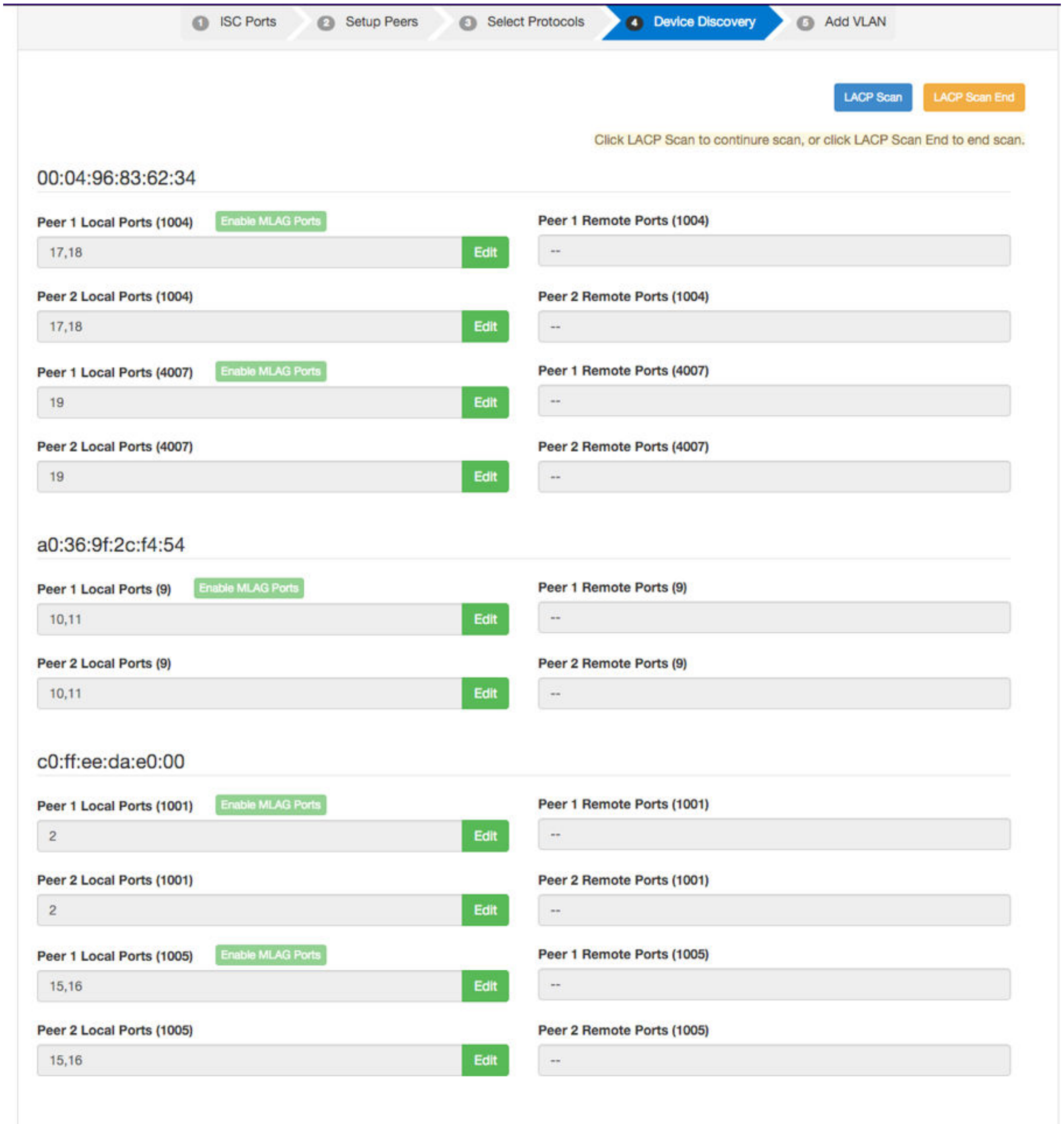
Notes:

1. Please choose the local ports you want to enable sharing on.
2. The remote ports will need to be manually set up for load sharing if not done already.
3. Hit "Enable MLAG Ports" button to add MLAG ports.
4. Hi "Add VLAN" button for next step.

3. For LACP discovery: Click **LACP Scan** to continue.

   Note
   It could take 10–30 seconds for LACP information to be transferred. Please wait 30 seconds for remote MLAG devices to show before re-scanning (with the **LACP Scan** button).

   All the discovered devices display. If no devices display, you can re-scan. If nothing displays after the second time, the remote MLAG device may not have LACP enabled on the loadshare.



Click LACP Scan to continure scan, or click LACP Scan End to end scan.

00:04:96:83:62:34

Peer 1 Local Ports (1004): 17,18
Peer 1 Remote Ports (1004): --
Peer 2 Local Ports (1004): 17,18
Peer 2 Remote Ports (1004): --
Peer 1 Local Ports (4007): 19
Peer 1 Remote Ports (4007): --
Peer 2 Local Ports (4007): 19
Peer 2 Remote Ports (4007): --

a0:36:9f:2c:f4:54

Peer 1 Local Ports (9): 10,11
Peer 1 Remote Ports (9): --
Peer 2 Local Ports (9): 10,11
Peer 2 Remote Ports (9): --

c0:ff:ee:da:e0:00

Peer 1 Local Ports (1001): 2
Peer 1 Remote Ports (1001): --
Peer 2 Local Ports (1001): 2
Peer 2 Remote Ports (1001): --
Peer 1 Local Ports (1005): 15,16
Peer 1 Remote Ports (1005): --
Peer 2 Local Ports (1005): 15,16
Peer 2 Remote Ports (1005): --

Note
Ports are grouped based on their remote device. The number next to each set of ports is the LACP partner key.

4. If you are satisfied with the scan, click **LACP Scan End**.

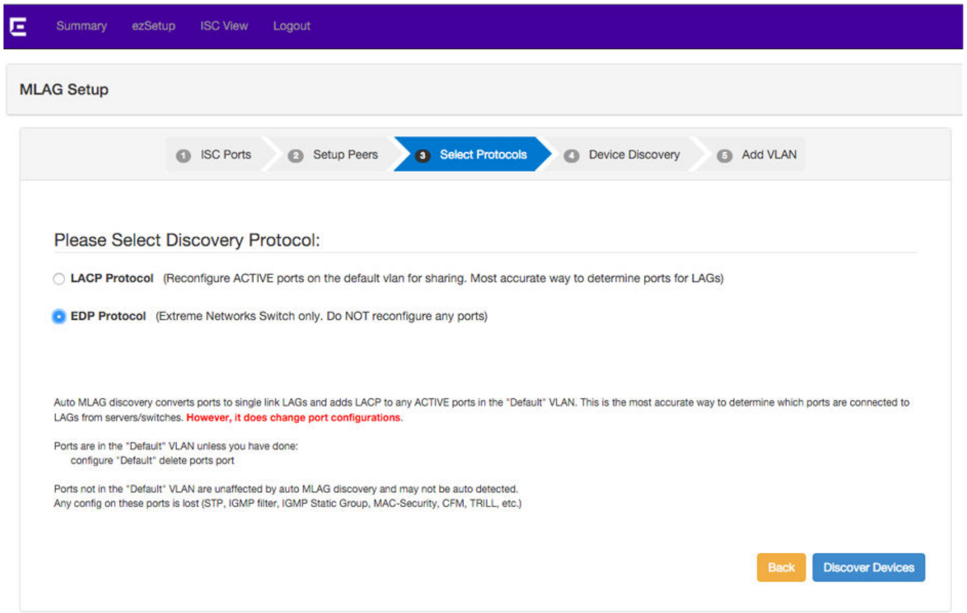
   Chalet will grey out the **Enable MLAG Ports** button until the scan is ended.
5. Click **Enable MLAG Ports** beside each port group you want enabled with MLAG.

   > Note
   > Each port group can be edited if the discovered ports are not acceptable.

   Assuming **Enable MLAG Ports** was clicked for each MLAG device, Chalet pushes the following configuration to each peer:

```
## Peer 1 ##
configure vlan default delete port 2,10-11,15-19
enable sharing 17 grouping 17-18 algorithm address-based custom lacp
enable sharing 19 grouping 19 algorithm address-based custom lacp
enable sharing 10 grouping 10-11 algorithm address-based custom lacp
enable sharing 2 grouping 2 algorithm address-based custom lacp
enable sharing 15 grouping 15-16 algorithm address-based custom lacp
enable mlag port 2 peer "m00049697E9F9" id 4enable mlag port 10 peer "m00049697E9F9"
id 3
enable mlag port 15 peer "m00049697E9F9" id 5enable mlag port 17 peer "m00049697E9F9"
id 1
enable mlag port 19 peer "m00049697E9F9" id 2

## Peer 2 ##
configure vlan default delete port 2,10-11,15-19
enable sharing 17 grouping 17-18 algorithm address-based custom lacp
enable sharing 19 grouping 19 algorithm address-based custom lacp
enable sharing 10 grouping 10-11 algorithm address-based custom lacp
enable sharing 2 grouping 2 algorithm address-based custom lacp
enable sharing 15 grouping 15-16 algorithm address-based custom lacp
enable mlag port 2 peer "m00049697E9E2" id 4
enable mlag port 10 peer "m00049697E9E2" id 3
enable mlag port 15 peer "m00049697E9E2" id 5
enable mlag port 17 peer "m00049697E9E2" id 1
enable mlag port 19 peer "m00049697E9E2" id 2
```

6. For EDP discovery: select **EDP Protcol** and then click **Discover Devices**.



Please Select Discovery Protocol:

○ **LACP Protocol** (Reconfigure ACTIVE ports on the default vlan for sharing. Most accurate way to determine ports for LAGs)

● **EDP Protocol** (Extreme Networks Switch only. Do NOT reconfigure any ports)

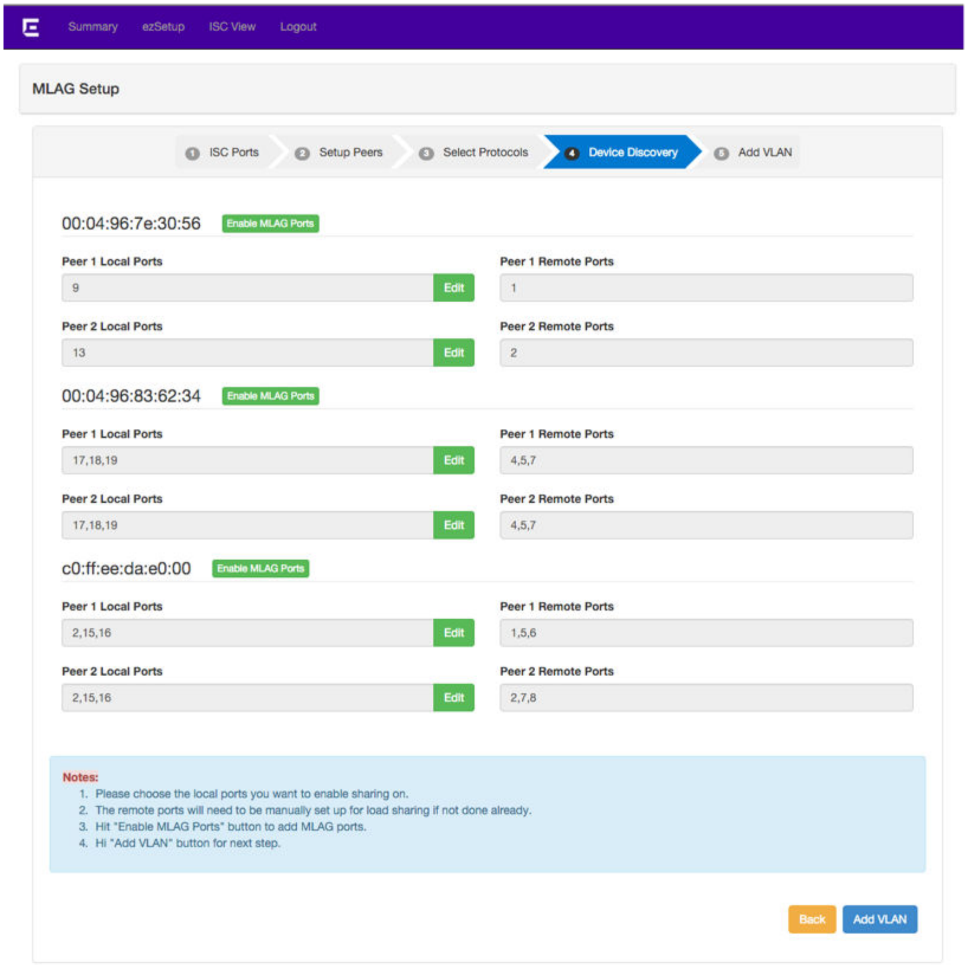
Auto MLAG discovery converts ports to single link LAGs and adds LACP to any ACTIVE ports in the "Default" VLAN. This is the most accurate way to determine which ports are connected to LAGs from servers/switches. **However, it does change port configurations.**

Ports are in the "Default" VLAN unless you have done:
configure "Default" delete ports port

Ports not in the "Default" VLAN are unaffected by auto MLAG discovery and may not be auto detected.
Any config on these ports is lost (STP, IGMP filter, IGMP Static Group, MAC-Security, CFM, TRILL, etc.)

EDP discovery has no way of knowing which LAGs you want on the remote LAG device, so all ports found on the device will be grouped together.

Note
Each port group can be edited if the discovered ports are not acceptable.



MLAG Setup

00:04:96:7e:30:56

Peer 1 Local Ports: 9
Peer 1 Remote Ports: 1
Peer 2 Local Ports: 13
Peer 2 Remote Ports: 2

00:04:96:83:62:34

Peer 1 Local Ports: 17,18,19
Peer 1 Remote Ports: 4,5,7
Peer 2 Local Ports: 17,18,19
Peer 2 Remote Ports: 4,5,7

c0:ff:ee:da:e0:00

Peer 1 Local Ports: 2,15,16
Peer 1 Remote Ports: 1,5,6
Peer 2 Local Ports: 2,15,16
Peer 2 Remote Ports: 2,7,8

Notes:

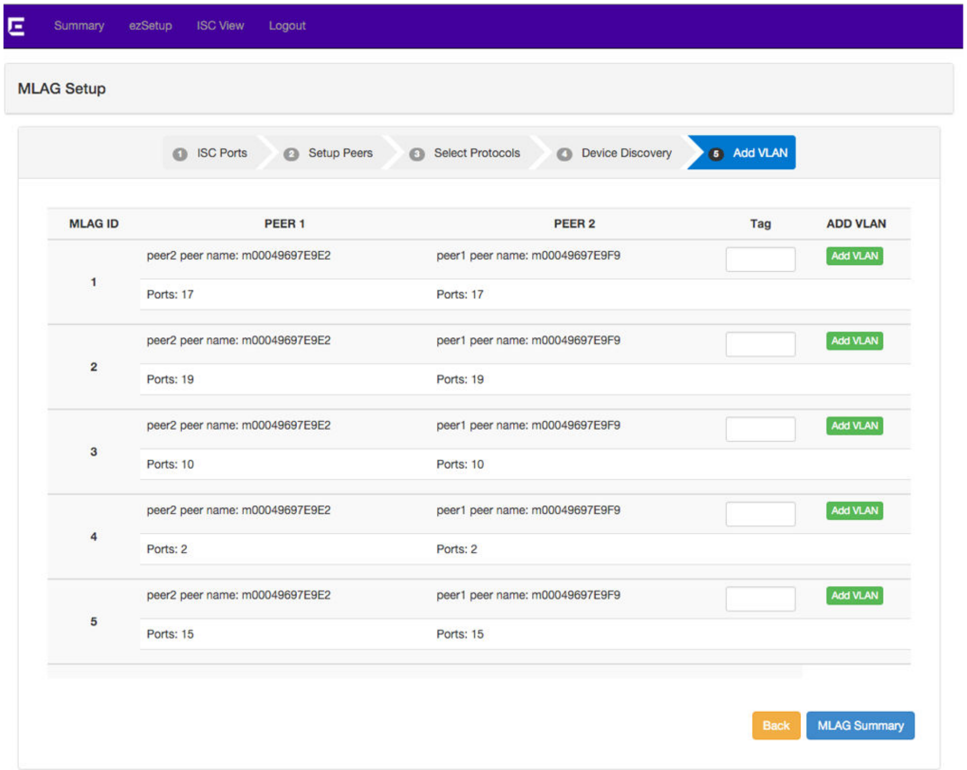
1. Please choose the local ports you want to enable sharing on.
2. The remote ports will need to be manually set up for load sharing if not done already.
3. Hit "Enable MLAG Ports" button to add MLAG ports.
4. Hi "Add VLAN" button for next step.

7. Click **Enable MLAG Ports** beside each port group you want enabled with MLAG.
8. When finished, click **Add VLAN**.

Adding VLANs to MLAG Devices

Chalet will now add VLANs to the MLAG ID set up previously, which will create a VLAN and tag, add the ports on the MLAG device, and add the ISC port.

1. For each port group on the peers, you can add VLANs to the MLAG one of two ways:
    - **Add VLAN**—the next available VLAN tag on both peers will be used.
    - **Tag** text box—add the desired VLAN tag manually.



MLAG ID	PEER 1	PEER 2	Tag	ADD VLAN
1	peer2 peer name: m00049697E9E2 Ports: 17	peer1 peer name: m00049697E9F9 Ports: 17		Add VLAN
2	peer2 peer name: m00049697E9E2 Ports: 19	peer1 peer name: m00049697E9F9 Ports: 19		Add VLAN
3	peer2 peer name: m00049697E9E2 Ports: 10	peer1 peer name: m00049697E9F9 Ports: 10		Add VLAN
4	peer2 peer name: m00049697E9E2 Ports: 2	peer1 peer name: m00049697E9F9 Ports: 2		Add VLAN
5	peer2 peer name: m00049697E9E2 Ports: 15	peer1 peer name: m00049697E9F9 Ports: 15		Add VLAN

Assuming **Add VLAN** was clicked for MLAG ID "1," Chalet will create the VLAN on both peers, add the *LAG* to the MLAG device, and add the ISC ports to the VLAN. VLANs created using the wizard are prefixed with `auto_mlag`*`tag`*.

In this example, Chalet pushes the following configuration to each peer:

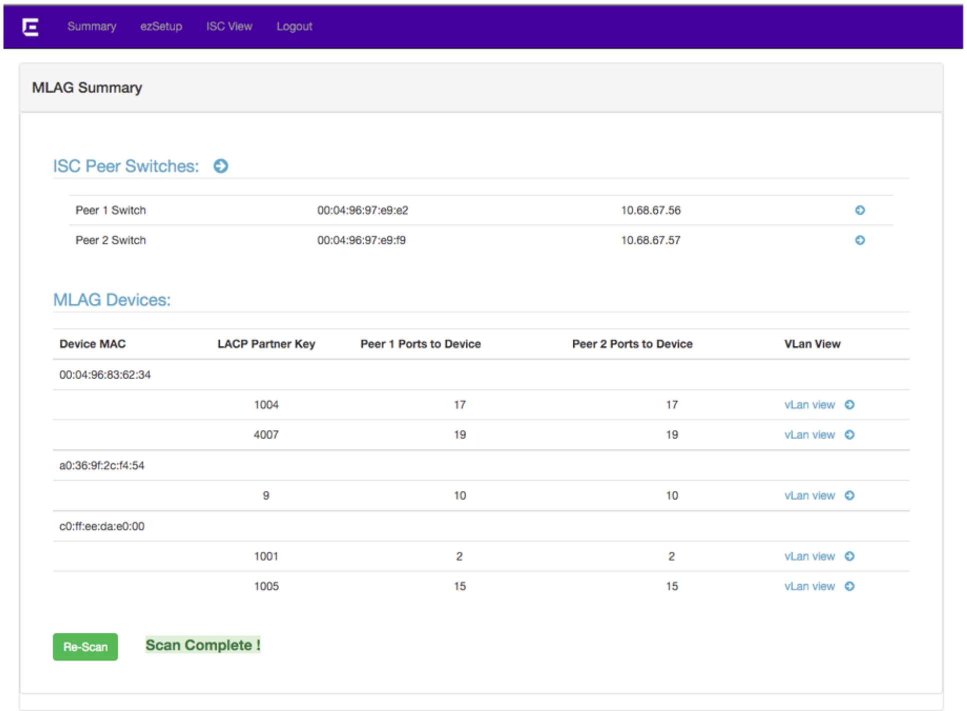
```
## Peer 1 ##
create vlan "auto_mlag3"
configure vlan auto_mlag3 tag 3
configure vlan auto_mlag3 add ports 1,17 tagged

## Peer 2 ##
create vlan "auto_mlag3"
configure vlan auto_mlag3 tag 3
configure vlan auto_mlag3 add ports 1,17 tagged
```

2. You can add as many VLANs as needed.
3. When finished, click **MLAG Summary**.

MLAG Summary

The **MLAG Summary** page displays:

- Detected *MLAG* devices.
- Ports on the MLAG peers that go to the connected MLAG device.
- Which VLANs have the MLAG ports.



MLAG Summary

ISC Peer Switches:

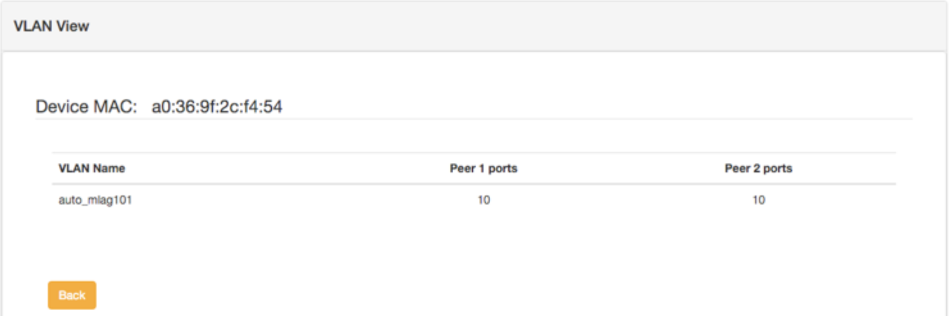
Peer 1 Switch	00:04:96:97:e9:e2	10.68.67.56
Peer 2 Switch	00:04:96:97:e9:f9	10.68.67.57

MLAG Devices:

Device MAC	LACP Partner Key	Peer 1 Ports to Device	Peer 2 Ports to Device	VLan View
00:04:96:83:62:34				
	1004	17	17	vLan view
	4007	19	19	vLan view
a0:36:9f:2c:f4:54				
	9	10	10	vLan view
c0:ff:ee:da:e0:00				
	1001	2	2	vLan view
	1005	15	15	vLan view

Scan Complete !

Clicking on the **vLan view** provides additional detail on a new page:

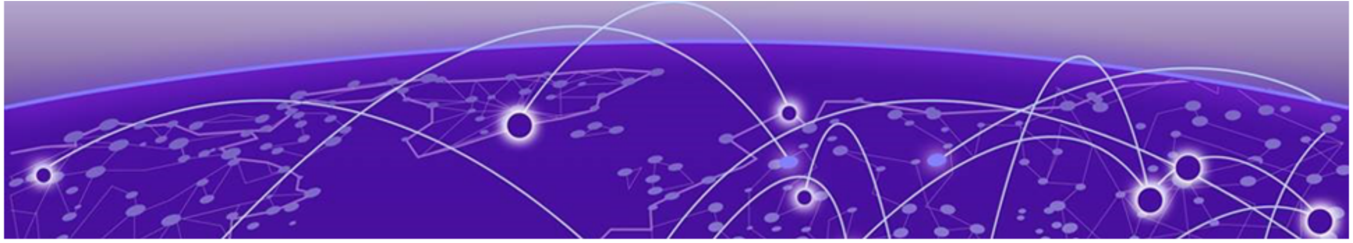


VLAN View

Device MAC: a0:36:9f:2c:f4:54

VLAN Name	Peer 1 ports	Peer 2 ports
auto_mlag101	10	10

Use the top navigation menu to return to the **Dashboard**.



Monitoring a Switch

Chalet's monitoring features allow you to view:

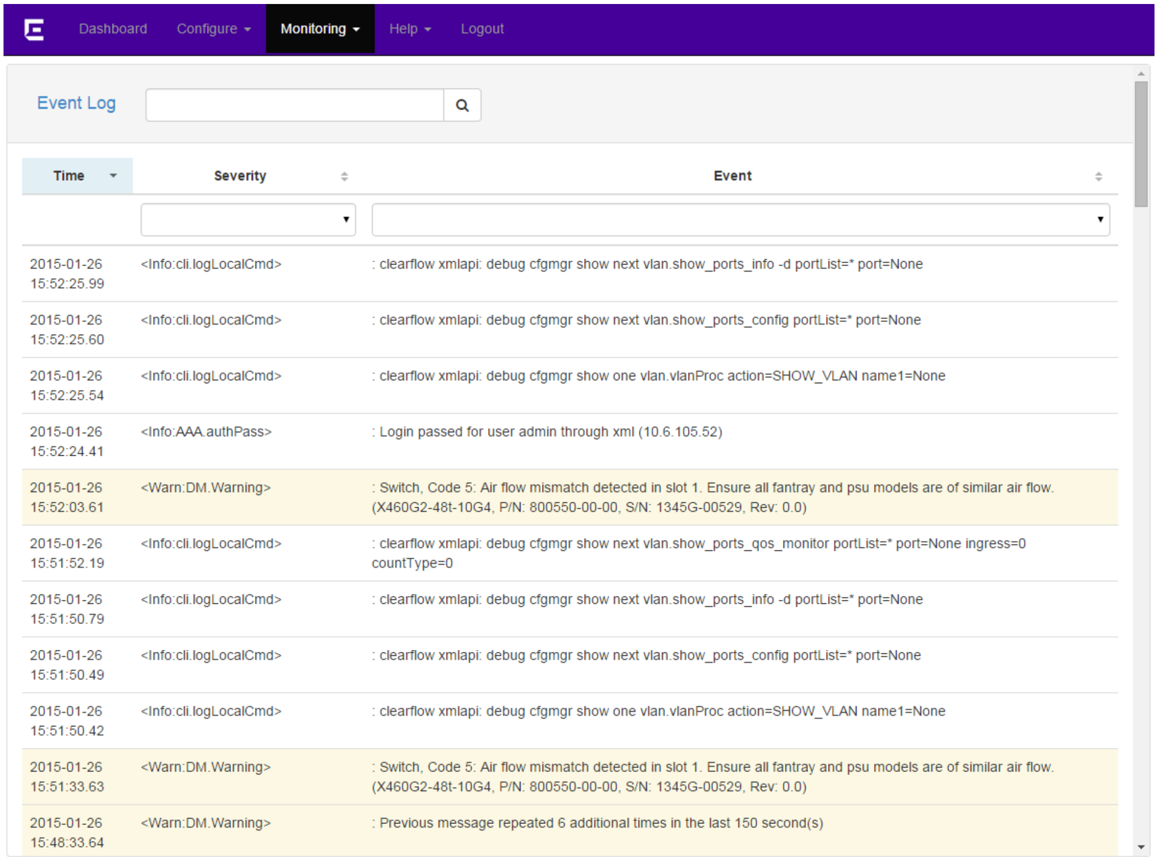
- Event logs by time, date, severity, and event detail.
- System processes and CPU performance by ExtremeXOS feature.
- Port utilization by Percent, Bytes, and Packets.
- Port Quality of Service for each profile (QP1–QP8) by Bytes or Packets and Ingress or Egress.
- User sessions on the switch.

Monitoring Events

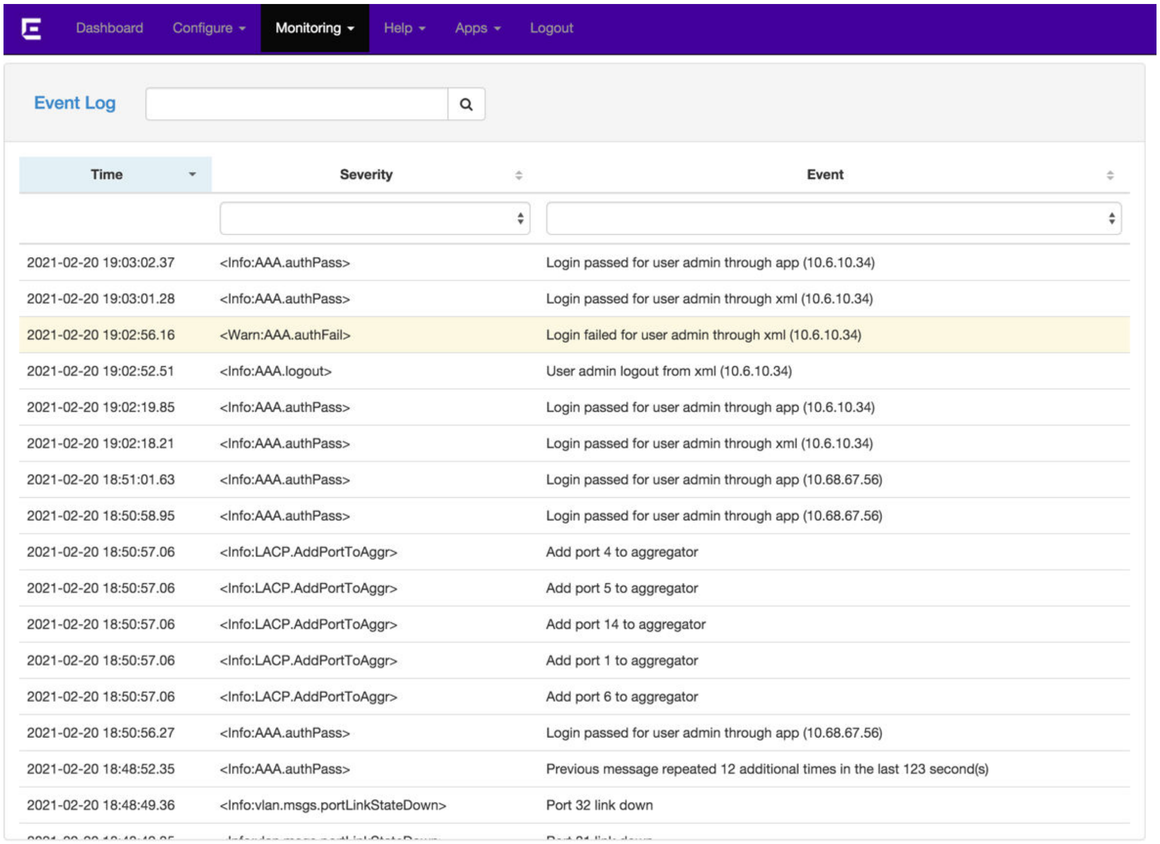
The Dashboard shows the number of recent Critical events, Errors, and Warnings, along with listing the last five errors. To get more information about these events, click anywhere in either of these tables (or select **Monitoring** > **Event Log**).

The **Event Log** screen displays a searchable and sortable list that displays the following for each event:

- Date and time
- Severity
- Event details



Time	Severity	Event
2015-01-26 15:52:25.99	<Info:cli.logLocalCmd>	: clearflow xmlapi: debug cfgmgr show next vlan.show_ports_info -d portList=* port=None
2015-01-26 15:52:25.60	<Info:cli.logLocalCmd>	: clearflow xmlapi: debug cfgmgr show next vlan.show_ports_config portList=* port=None
2015-01-26 15:52:25.54	<Info:cli.logLocalCmd>	: clearflow xmlapi: debug cfgmgr show one vlan.vlanProc action=SHOW_VLAN name1=None
2015-01-26 15:52:24.41	<Info:AAA.authPass>	: Login passed for user admin through xml (10.6.105.52)
2015-01-26 15:52:03.61	<Warn:DM.Warning>	: Switch, Code 5: Air flow mismatch detected in slot 1. Ensure all fantray and psu models are of similar air flow. (X460G2-48t-10G4, P/N: 800550-00-00, S/N: 1345G-00529, Rev: 0.0)
2015-01-26 15:51:52.19	<Info:cli.logLocalCmd>	: clearflow xmlapi: debug cfgmgr show next vlan.show_ports_qos_monitor portList=* port=None ingress=0 countType=0
2015-01-26 15:51:50.79	<Info:cli.logLocalCmd>	: clearflow xmlapi: debug cfgmgr show next vlan.show_ports_info -d portList=* port=None
2015-01-26 15:51:50.49	<Info:cli.logLocalCmd>	: clearflow xmlapi: debug cfgmgr show next vlan.show_ports_config portList=* port=None
2015-01-26 15:51:50.42	<Info:cli.logLocalCmd>	: clearflow xmlapi: debug cfgmgr show one vlan.vlanProc action=SHOW_VLAN name1=None
2015-01-26 15:51:33.63	<Warn:DM.Warning>	: Switch, Code 5: Air flow mismatch detected in slot 1. Ensure all fantray and psu models are of similar air flow. (X460G2-48t-10G4, P/N: 800550-00-00, S/N: 1345G-00529, Rev: 0.0)
2015-01-26 15:48:33.64	<Warn:DM.Warning>	: Previous message repeated 6 additional times in the last 150 second(s)



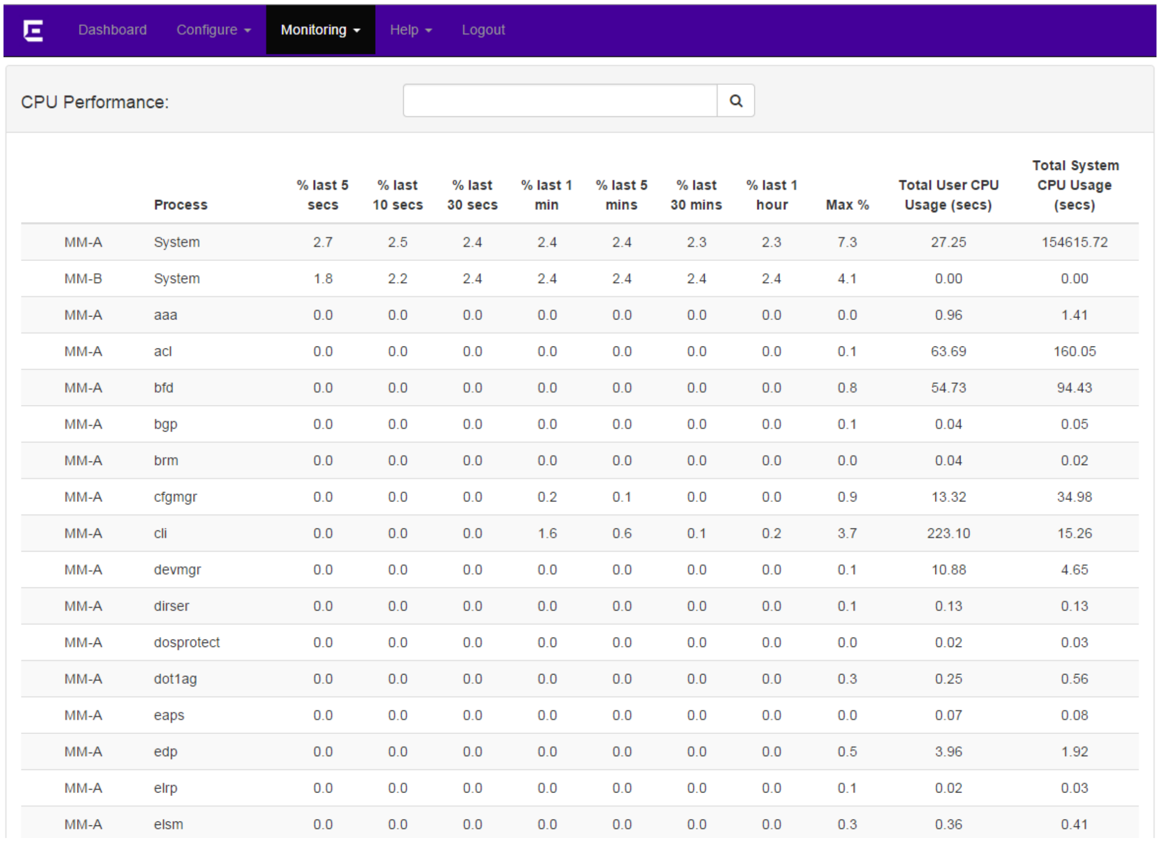
Time	Severity	Event
2021-02-20 19:03:02.37	<Info:AAA.authPass>	Login passed for user admin through app (10.6.10.34)
2021-02-20 19:03:01.28	<Info:AAA.authPass>	Login passed for user admin through xml (10.6.10.34)
2021-02-20 19:02:56.16	<Warn:AAA.authFail>	Login failed for user admin through xml (10.6.10.34)
2021-02-20 19:02:52.51	<Info:AAA.logout>	User admin logout from xml (10.6.10.34)
2021-02-20 19:02:19.85	<Info:AAA.authPass>	Login passed for user admin through app (10.6.10.34)
2021-02-20 19:02:18.21	<Info:AAA.authPass>	Login passed for user admin through xml (10.6.10.34)
2021-02-20 18:51:01.63	<Info:AAA.authPass>	Login passed for user admin through app (10.68.67.56)
2021-02-20 18:50:58.95	<Info:AAA.authPass>	Login passed for user admin through app (10.68.67.56)
2021-02-20 18:50:57.06	<Info:LACP.AddPortToAggr>	Add port 4 to aggregator
2021-02-20 18:50:57.06	<Info:LACP.AddPortToAggr>	Add port 5 to aggregator
2021-02-20 18:50:57.06	<Info:LACP.AddPortToAggr>	Add port 14 to aggregator
2021-02-20 18:50:57.06	<Info:LACP.AddPortToAggr>	Add port 1 to aggregator
2021-02-20 18:50:57.06	<Info:LACP.AddPortToAggr>	Add port 6 to aggregator
2021-02-20 18:50:56.27	<Info:AAA.authPass>	Login passed for user admin through app (10.68.67.56)
2021-02-20 18:48:52.35	<Info:AAA.authPass>	Previous message repeated 12 additional times in the last 123 second(s)
2021-02-20 18:48:49.36	<Info:vlan.msgs.portLinkStateDown>	Port 32 link down

This screen provides the same information as issuing the `show log` command. For more information about system events, refer to the *ExtremeXOS User Guide*.

Monitoring System Performance

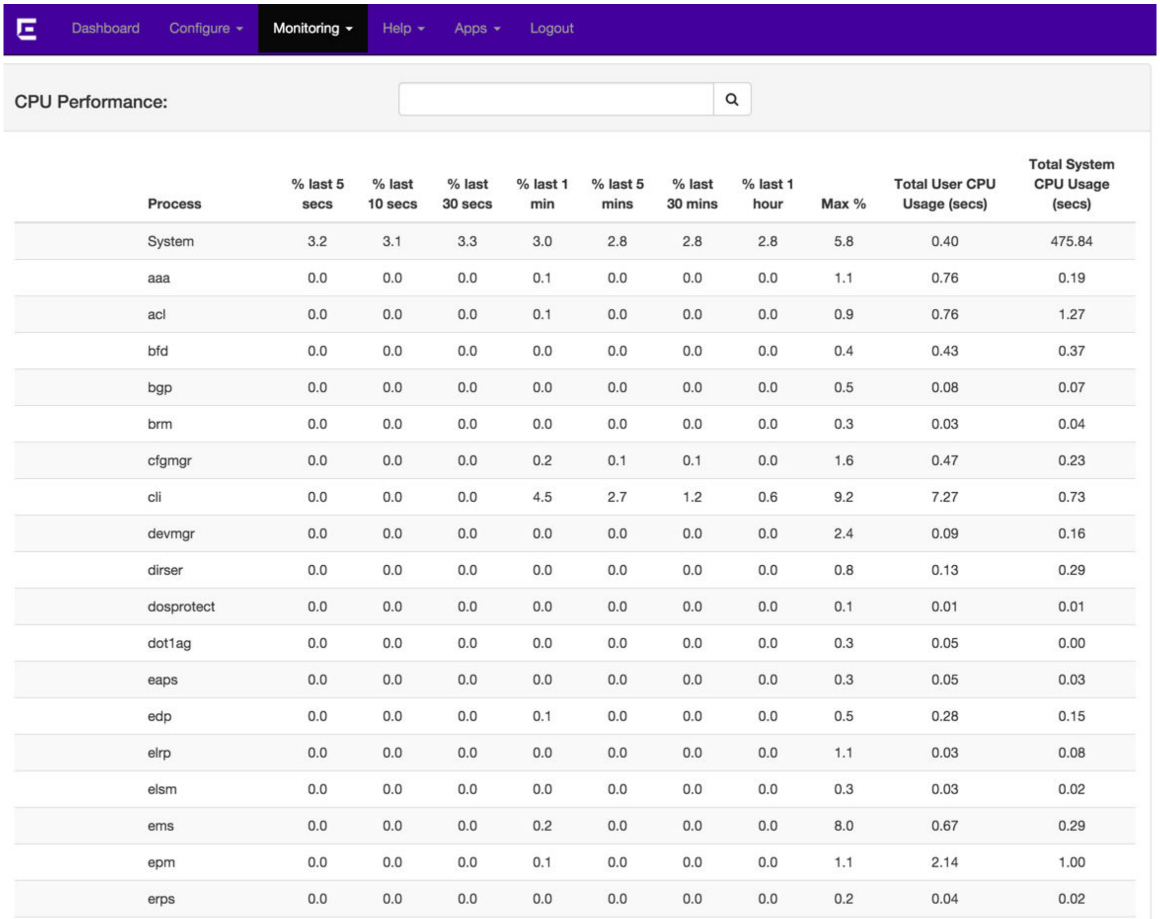
Select **Monitoring** > **System** directs you to the **CPU Performance** page.

The table shows each switch's performance over the last hour in a few pre-determined increments. Nothing on this page is editable, but the information can be filtered using the search bar.



CPU Performance:

	Process	% last 5 secs	% last 10 secs	% last 30 secs	% last 1 min	% last 5 mins	% last 30 mins	% last 1 hour	Max %	Total User CPU Usage (secs)	Total System CPU Usage (secs)
MM-A	System	2.7	2.5	2.4	2.4	2.4	2.3	2.3	7.3	27.25	154615.72
MM-B	System	1.8	2.2	2.4	2.4	2.4	2.4	2.4	4.1	0.00	0.00
MM-A	aaa	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.96	1.41
MM-A	acl	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1	63.69	160.05
MM-A	bfd	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.8	54.73	94.43
MM-A	bgp	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1	0.04	0.05
MM-A	brm	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.04	0.02
MM-A	cfgmgr	0.0	0.0	0.0	0.2	0.1	0.0	0.0	0.9	13.32	34.98
MM-A	cli	0.0	0.0	0.0	1.6	0.6	0.1	0.2	3.7	223.10	15.26
MM-A	devmgr	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1	10.88	4.65
MM-A	dirser	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1	0.13	0.13
MM-A	dosprotect	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.02	0.03
MM-A	dot1ag	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.3	0.25	0.56
MM-A	eaps	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.07	0.08
MM-A	edp	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.5	3.96	1.92
MM-A	elrp	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1	0.02	0.03
MM-A	elsm	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.3	0.36	0.41



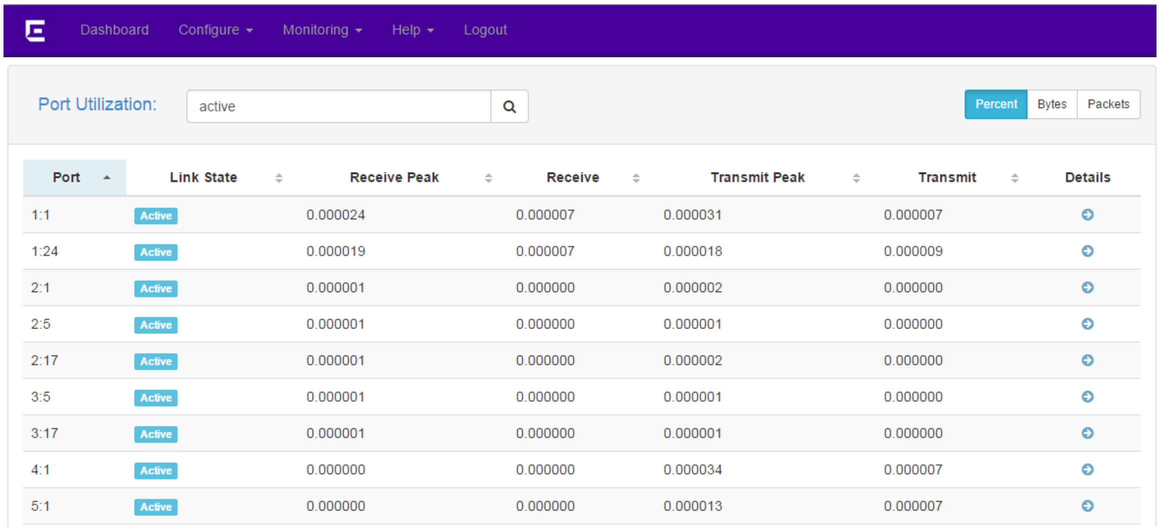
CPU Performance:

Process	% last 5 secs	% last 10 secs	% last 30 secs	% last 1 min	% last 5 mins	% last 30 mins	% last 1 hour	Max %	Total User CPU Usage (secs)	Total System CPU Usage (secs)
System	3.2	3.1	3.3	3.0	2.8	2.8	2.8	5.8	0.40	475.84
aaa	0.0	0.0	0.0	0.1	0.0	0.0	0.0	1.1	0.76	0.19
acl	0.0	0.0	0.0	0.1	0.0	0.0	0.0	0.9	0.76	1.27
bfd	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.4	0.43	0.37
bgp	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.5	0.08	0.07
brm	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.3	0.03	0.04
cfgmgr	0.0	0.0	0.0	0.2	0.1	0.1	0.0	1.6	0.47	0.23
cli	0.0	0.0	0.0	4.5	2.7	1.2	0.6	9.2	7.27	0.73
devmgr	0.0	0.0	0.0	0.0	0.0	0.0	0.0	2.4	0.09	0.16
dirser	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.8	0.13	0.29
dosprotect	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1	0.01	0.01
dot1ag	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.3	0.05	0.00
eaps	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.3	0.05	0.03
edp	0.0	0.0	0.0	0.1	0.0	0.0	0.0	0.5	0.28	0.15
elrp	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.1	0.03	0.08
elsm	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.3	0.03	0.02
ems	0.0	0.0	0.0	0.2	0.0	0.0	0.0	8.0	0.67	0.29
epm	0.0	0.0	0.0	0.1	0.0	0.0	0.0	1.1	2.14	1.00
erps	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.2	0.04	0.02

Monitoring Port Utilization

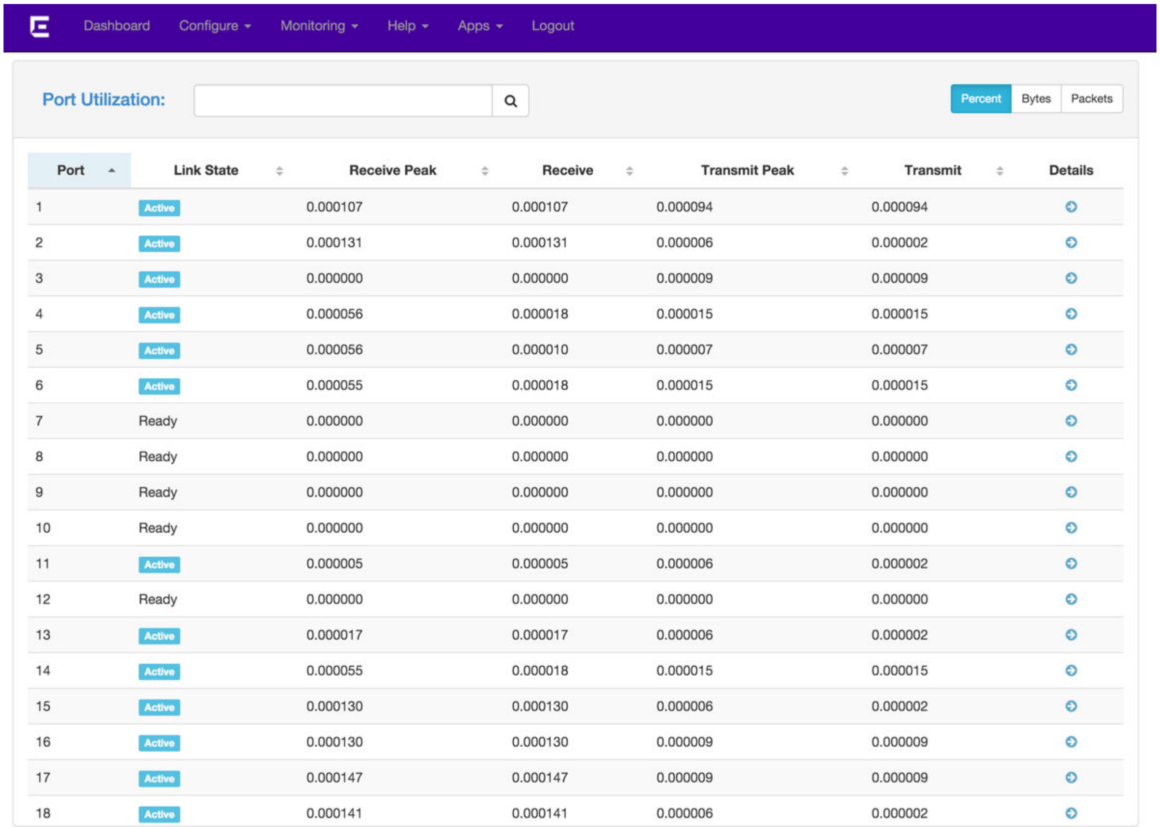
Clicking **Monitoring** > **Port Utilization** provides a summary of all ports with their link states and receive and transmit details that can be viewed in Percent, Bytes, or Packets. The table can be sorted by any column or filtered using the search bar.

The information shown cannot be edited, but you can view more information about the port by clicking the ➔ to the right. This will take you to the **Port Details** screen, where you can configure ports).



Port Utilization: active

Port	Link State	Receive Peak	Receive	Transmit Peak	Transmit	Details
1:1	Active	0.000024	0.000007	0.000031	0.000007	➔
1:24	Active	0.000019	0.000007	0.000018	0.000009	➔
2:1	Active	0.000001	0.000000	0.000002	0.000000	➔
2:5	Active	0.000001	0.000000	0.000001	0.000000	➔
2:17	Active	0.000001	0.000000	0.000002	0.000000	➔
3:5	Active	0.000001	0.000000	0.000001	0.000000	➔
3:17	Active	0.000001	0.000000	0.000001	0.000000	➔
4:1	Active	0.000000	0.000000	0.000034	0.000007	➔
5:1	Active	0.000000	0.000000	0.000013	0.000007	➔



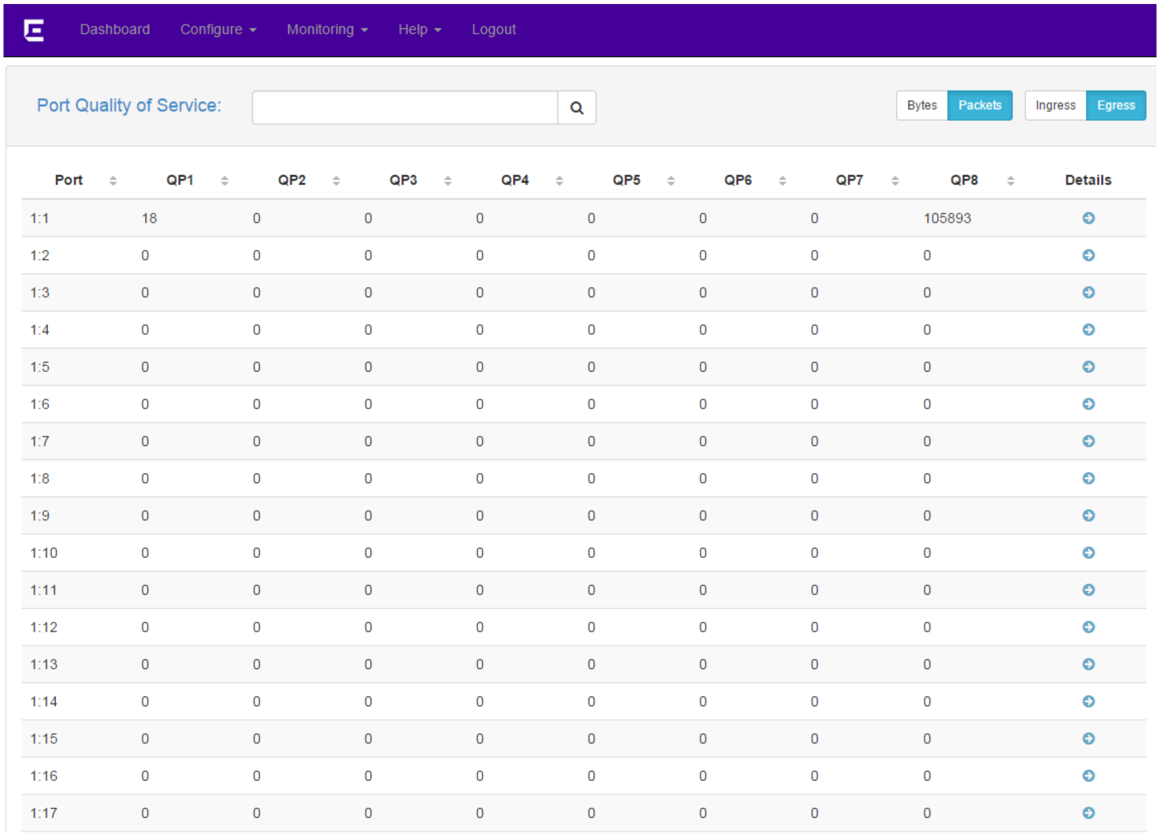
Port Utilization:

Port	Link State	Receive Peak	Receive	Transmit Peak	Transmit	Details
1	Active	0.000107	0.000107	0.000094	0.000094	➔
2	Active	0.000131	0.000131	0.000006	0.000002	➔
3	Active	0.000000	0.000000	0.000009	0.000009	➔
4	Active	0.000056	0.000018	0.000015	0.000015	➔
5	Active	0.000056	0.000010	0.000007	0.000007	➔
6	Active	0.000055	0.000018	0.000015	0.000015	➔
7	Ready	0.000000	0.000000	0.000000	0.000000	➔
8	Ready	0.000000	0.000000	0.000000	0.000000	➔
9	Ready	0.000000	0.000000	0.000000	0.000000	➔
10	Ready	0.000000	0.000000	0.000000	0.000000	➔
11	Active	0.000005	0.000005	0.000006	0.000002	➔
12	Ready	0.000000	0.000000	0.000000	0.000000	➔
13	Active	0.000017	0.000017	0.000006	0.000002	➔
14	Active	0.000055	0.000018	0.000015	0.000015	➔
15	Active	0.000130	0.000130	0.000006	0.000002	➔
16	Active	0.000130	0.000130	0.000009	0.000009	➔
17	Active	0.000147	0.000147	0.000009	0.000009	➔
18	Active	0.000141	0.000141	0.000006	0.000002	➔

Monitoring Quality of Service

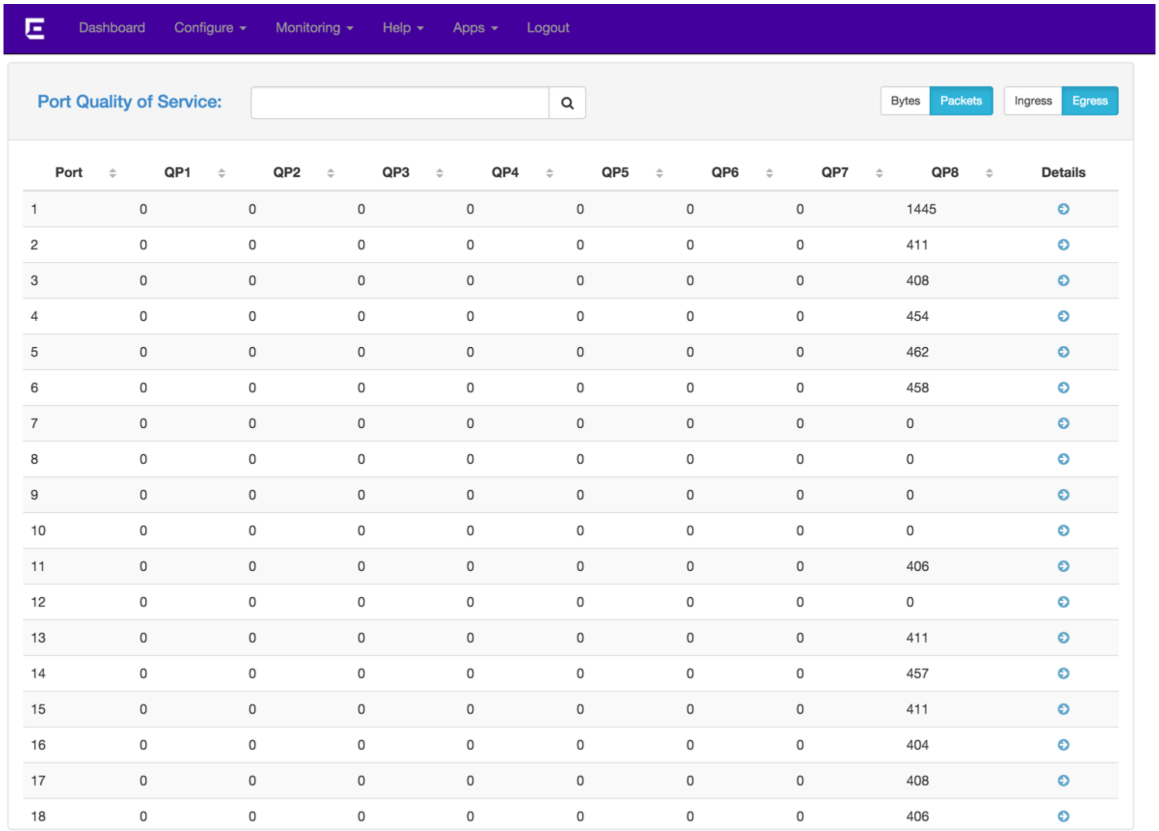
Clicking **Monitoring** > **Quality of Service** provides a summary of *QoS (Quality of Service)* profiles and the packets or bytes on each port, and is equivalent to entering the `show ports` **`qosmonitor`** command.

The QoS information shown cannot be edited, but you can rearrange the data by Bytes or Packets and Ingress or Egress. You can also sort by column or use the search bar to filter the results.



Port Quality of Service:

Port	QP1	QP2	QP3	QP4	QP5	QP6	QP7	QP8	Details
1:1	18	0	0	0	0	0	0	105893	➔
1:2	0	0	0	0	0	0	0	0	➔
1:3	0	0	0	0	0	0	0	0	➔
1:4	0	0	0	0	0	0	0	0	➔
1:5	0	0	0	0	0	0	0	0	➔
1:6	0	0	0	0	0	0	0	0	➔
1:7	0	0	0	0	0	0	0	0	➔
1:8	0	0	0	0	0	0	0	0	➔
1:9	0	0	0	0	0	0	0	0	➔
1:10	0	0	0	0	0	0	0	0	➔
1:11	0	0	0	0	0	0	0	0	➔
1:12	0	0	0	0	0	0	0	0	➔
1:13	0	0	0	0	0	0	0	0	➔
1:14	0	0	0	0	0	0	0	0	➔
1:15	0	0	0	0	0	0	0	0	➔
1:16	0	0	0	0	0	0	0	0	➔
1:17	0	0	0	0	0	0	0	0	➔



Port Quality of Service:

Port	QP1	QP2	QP3	QP4	QP5	QP6	QP7	QP8	Details
1	0	0	0	0	0	0	0	1445	➔
2	0	0	0	0	0	0	0	411	➔
3	0	0	0	0	0	0	0	408	➔
4	0	0	0	0	0	0	0	454	➔
5	0	0	0	0	0	0	0	462	➔
6	0	0	0	0	0	0	0	458	➔
7	0	0	0	0	0	0	0	0	➔
8	0	0	0	0	0	0	0	0	➔
9	0	0	0	0	0	0	0	0	➔
10	0	0	0	0	0	0	0	0	➔
11	0	0	0	0	0	0	0	406	➔
12	0	0	0	0	0	0	0	0	➔
13	0	0	0	0	0	0	0	411	➔
14	0	0	0	0	0	0	0	457	➔
15	0	0	0	0	0	0	0	411	➔
16	0	0	0	0	0	0	0	404	➔
17	0	0	0	0	0	0	0	408	➔
18	0	0	0	0	0	0	0	406	➔

For more information about a particular port, click the ➔ to the right. This will take you to the **Port Details** screen (see Port Details -- QoS on page 31).

Note
QoS Profiles must be created before you can assign ports. For more information, see "Configuring QoS" in the *ExtremeXOS User Guide*.

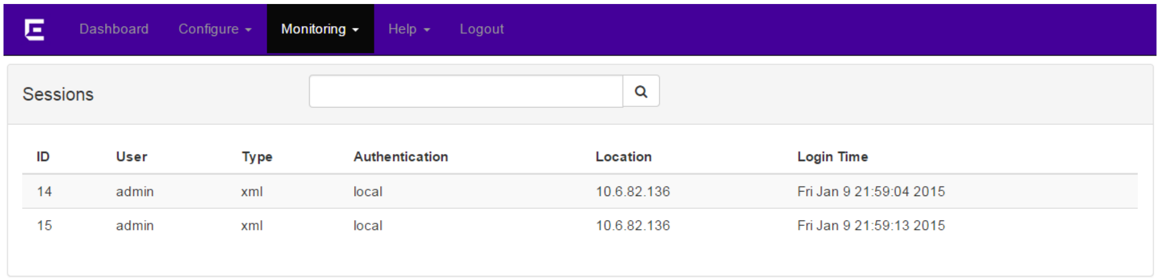
Monitoring User Sessions

The **Sessions** page shows all current sessions in chronological order, including the user name, the type of user (XML, SSH, or Telnet), the authentication, location (IP address), and login date/time stamp.

To view the session list, select **Monitoring** > **Session**.

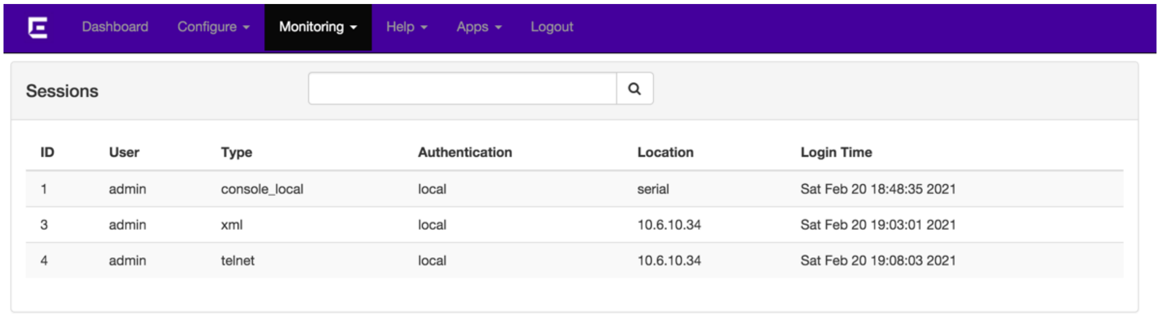
Note
Every time a user refreshes the web browser, a duplicate session is created. Currently, Chalet does not allow administrators to clear duplicate or rogue sessions for other users. To clear your own session, click **Logout** in the navigation menu.

Note
A maximum of six XML session are allowed per device.



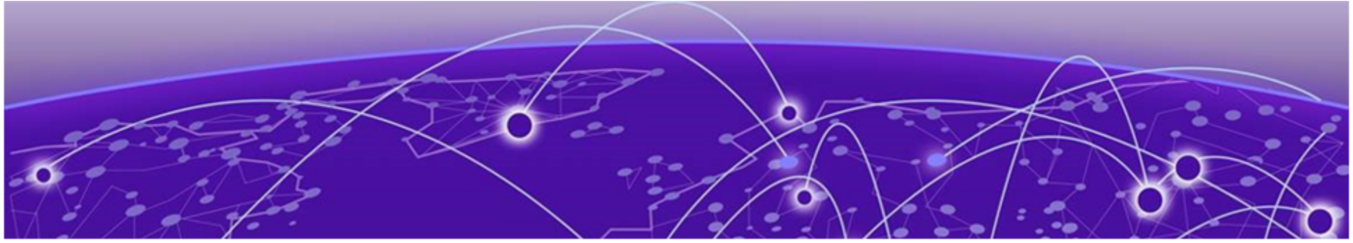
Sessions

ID	User	Type	Authentication	Location	Login Time
14	admin	xml	local	10.6.82.136	Fri Jan 9 21:59:04 2015
15	admin	xml	local	10.6.82.136	Fri Jan 9 21:59:13 2015



Sessions

ID	User	Type	Authentication	Location	Login Time
1	admin	console_local	local	serial	Sat Feb 20 18:48:35 2021
3	admin	xml	local	10.6.10.34	Sat Feb 20 19:03:01 2021
4	admin	telnet	local	10.6.10.34	Sat Feb 20 19:08:03 2021



Managing Accounts

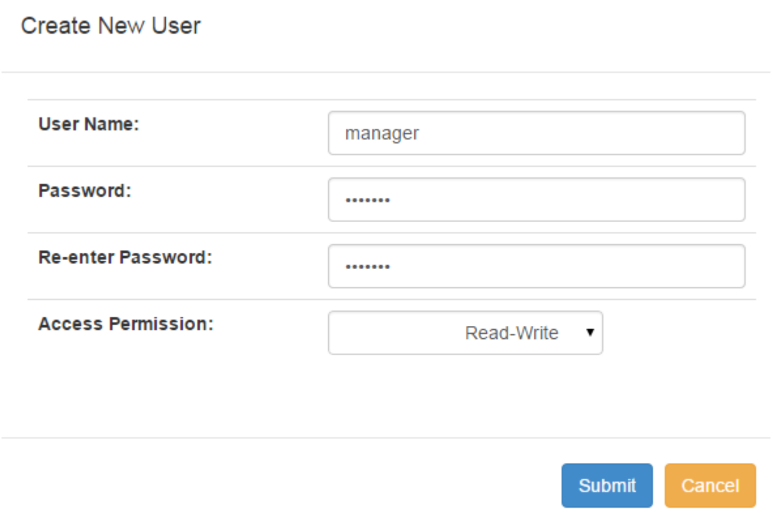
From the **User Detail** page (**Configure** > **Accounts**), administrators can:

- Add users.
- Delete users.
- Change user passwords.
- Set global and individual password policies.
- Set *RADIUS (Remote Authentication Dial In User Service)* and TACACS authentications.

Adding Users

Administrators can add multiple users that have either read-only or read-write access. To add a new user:

1. Click **Configure** > **Accounts** to display the user list.
2. Click the **New User** button.



Create New User

User Name:	manager
Password:	•••••••
Re-enter Password:	•••••••
Access Permission:	Read-Write ▾

3. In the pop-up dialog, enter the user name amd password, confirm the password, and select the permission level.

   Note
   If a global password policy is set, you will be notified if the password you choose does not conform to this policy.

4. Click **Submit** to finish.

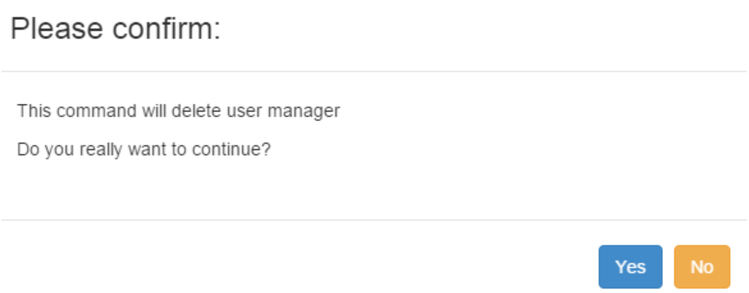
   The page refreshes to show the new user.

Deleting Users

To delete a user:

1. Click **Configure** > **Accounts** to display the user list.
2. Click the ➡ icon on the row of the user you wish to delete.

   The **User Detail** page appears.
3. Click the **Delete User** button and confirm the deletion in the resulting dialog.



Please confirm:

This command will delete user manager

Do you really want to continue?

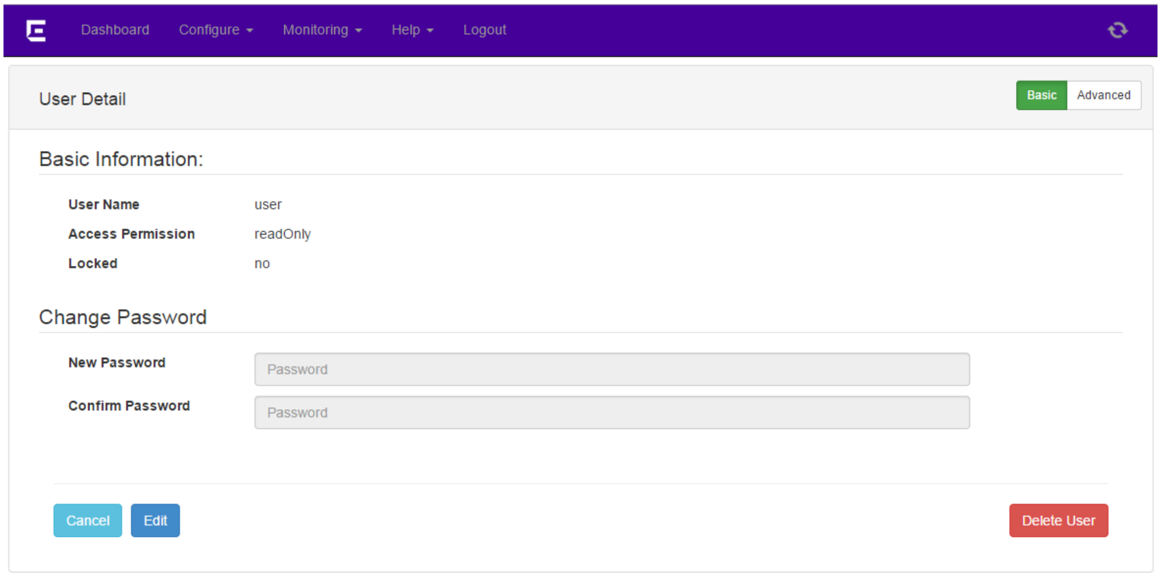
Changing User Passwords

To change a user's password:

1. Click **Configure** > **Accounts** to display the user list.
2. Click the ➡ icon on the row of the desired user.

   The **User Detail** page appears.
3. Click **Edit**.

   The Change Password area becomes editable.



User Detail

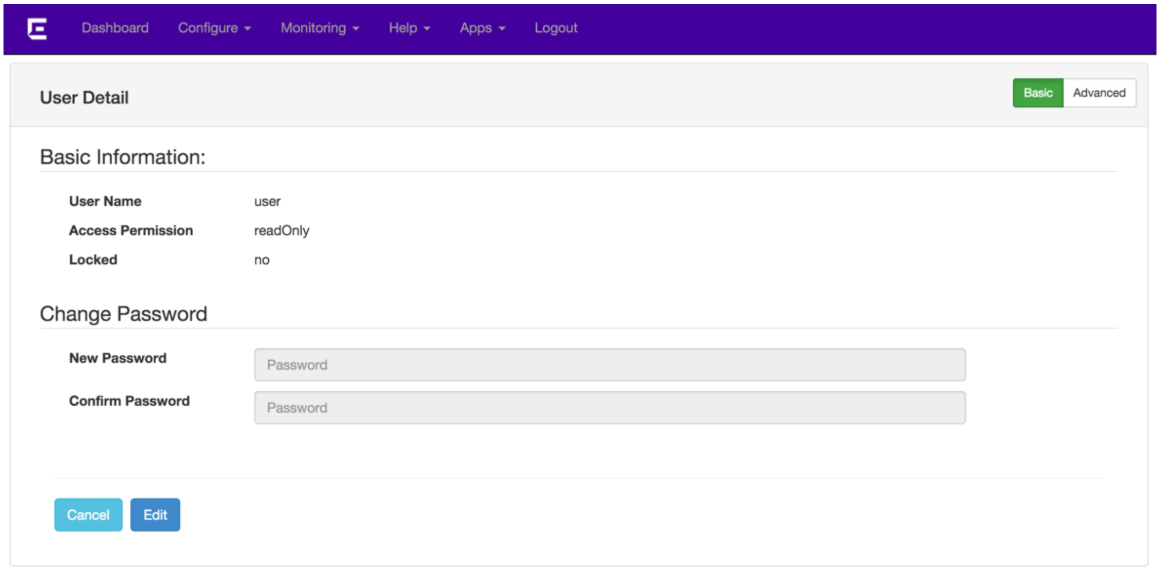
Basic Information:

User Name	user
Access Permission	readOnly
Locked	no

Change Password

New Password: Password

Confirm Password: Password



User Detail

Basic Information:

User Name	user
Access Permission	readOnly
Locked	no

Change Password

New Password: Password

Confirm Password: Password

4. Enter a new password and confirm it, and then click **Apply**.

> Note
> If you have set a global password policy, the new password must conform to the new policy.

5. If you want to create a separate password policy *for just this user*, click the **Advanced** button and complete the following information:
   - Maximum Age (days)—Maximum password age, in days. For example, if you enter `60`, users will be required to set a new password in 60 days.
   - Minimum Length—Set a minimum password length.
   - History Limit—Set the number of new passwords before a user can reuse an older password. For example, if you enter `3`, the user must create three new passwords until a former password can be reused.

- Character Validation—Enforce passwords that have *at least two* of each of the following:
  - upper case letters
  - lower case letters
  - numbers
  - special character

  For example: `P@Sw04d!`
- Lockout on Login Failures—Lock the user out after three unsuccessful login attempts.

6. When finished, click **Save Config**.

Account Security

To add greater security to accounts created on the switch, you can:

- Set a Global Password Policy
- Configure RADIUS
- Configure TACACS

Note
Command usage that should be restricted for a user account by TACACS or RADIUS with CLI authorization enabled may not occur when users are logged in by Chalet or when using the XML API directly. To use Chalet securely, create only read-only users on the switch, and then access Chalet with those user accounts.

Setting a Global Password Policy

Chalet allows you to set a password policy for all users to enhance security. To set up the global password policy:

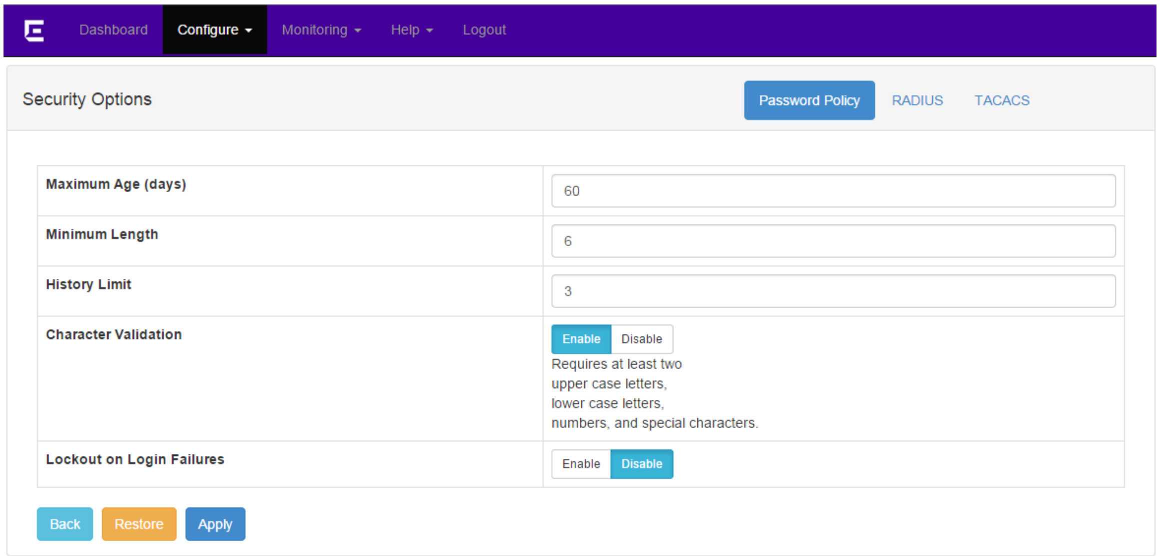
1. Click **Configure** > **Accounts**.
2. Click the **Security Options** button, and then click **Edit** on the **Password Policy** tab.

   The grayed-out fields become editable.
3. You can set great security for account passwords by setting any of the following:
   - Maximum Age (days)—Maximum password age, in days. For example, if you enter `60`, users will be required to set a new password in 60 days.
   - Minimum Length—Set a minimum password length.
   - History Limit—Set the number of new passwords before a user can reuse an older password. For example, if you enter `3`, the user must create three new passwords until a former password can be reused.
   - Character Validation—Enforce passwords that have *at least two* of each of the following:
     - upper case letters
     - lower case letters

- numbers
- special character

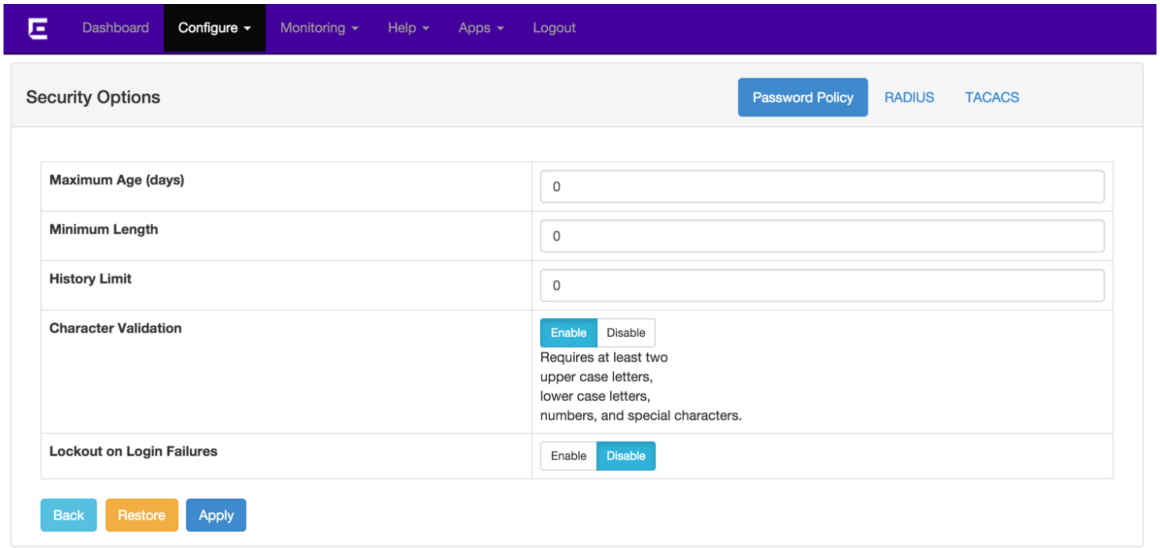
For example: `P@Sw04d!`

- **Lockout on Login Failures**—Lock the user out after three unsuccessful login attempts.



Security Options

Maximum Age (days)	60
Minimum Length	6
History Limit	3
Character Validation	[✓ Enable] Disable Requires at least two upper case letters, lower case letters, numbers, and special characters.
Lockout on Login Failures	Enable [✓ Disable]



Security Options

Maximum Age (days)	0
Minimum Length	0
History Limit	0
Character Validation	[✓ Enable] Disable Requires at least two upper case letters, lower case letters, numbers, and special characters.
Lockout on Login Failures	Enable [✓ Disable]

4. Click **Apply** when finished.

   All new account password must meet these requirements unless the security options are removed.

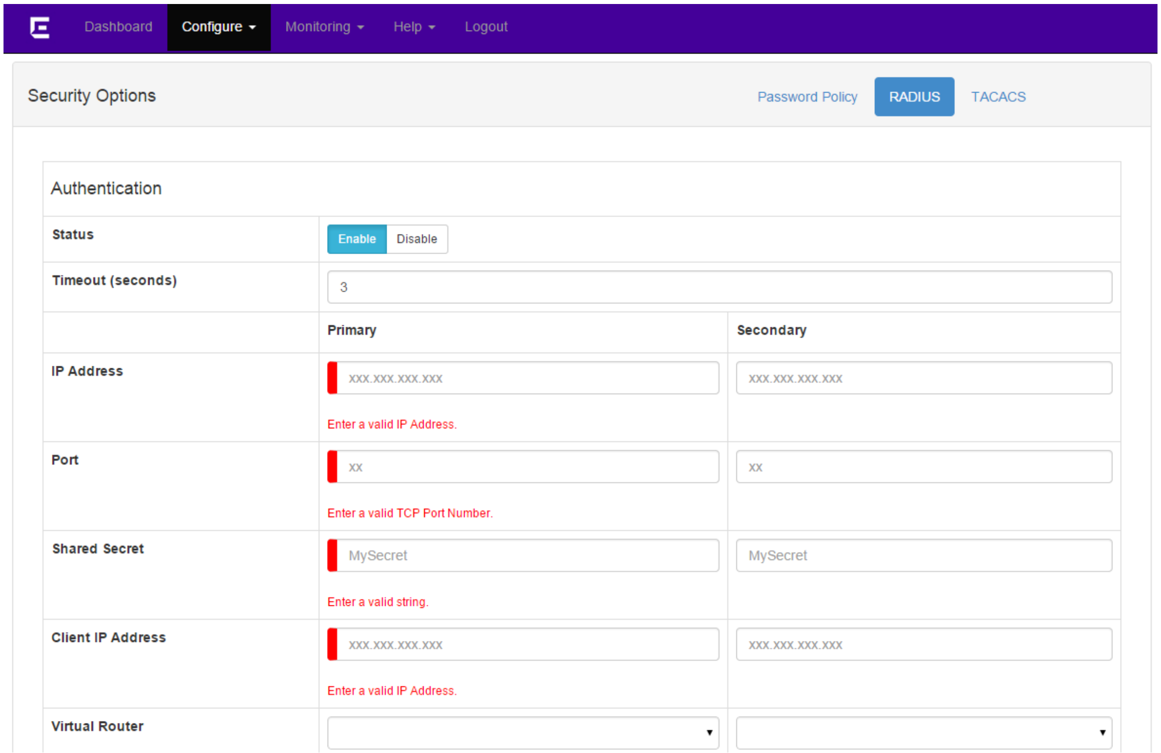
Configuring RADIUS

You can enable and configure *RADIUS* on the switch in one Chalet screen instead of entering multiple comands on the CLI. For more information about configuring RADIUS, see the "Security" section of the *ExtremeXOS User Guide*.

To configure RADIUS:

1. Click **Configure** > **Accounts** to display the user list.
2. Click the **Security Options** tab.
3. Click the **RADIUS** tab.
4. Click **Edit** at the bottom of the page.

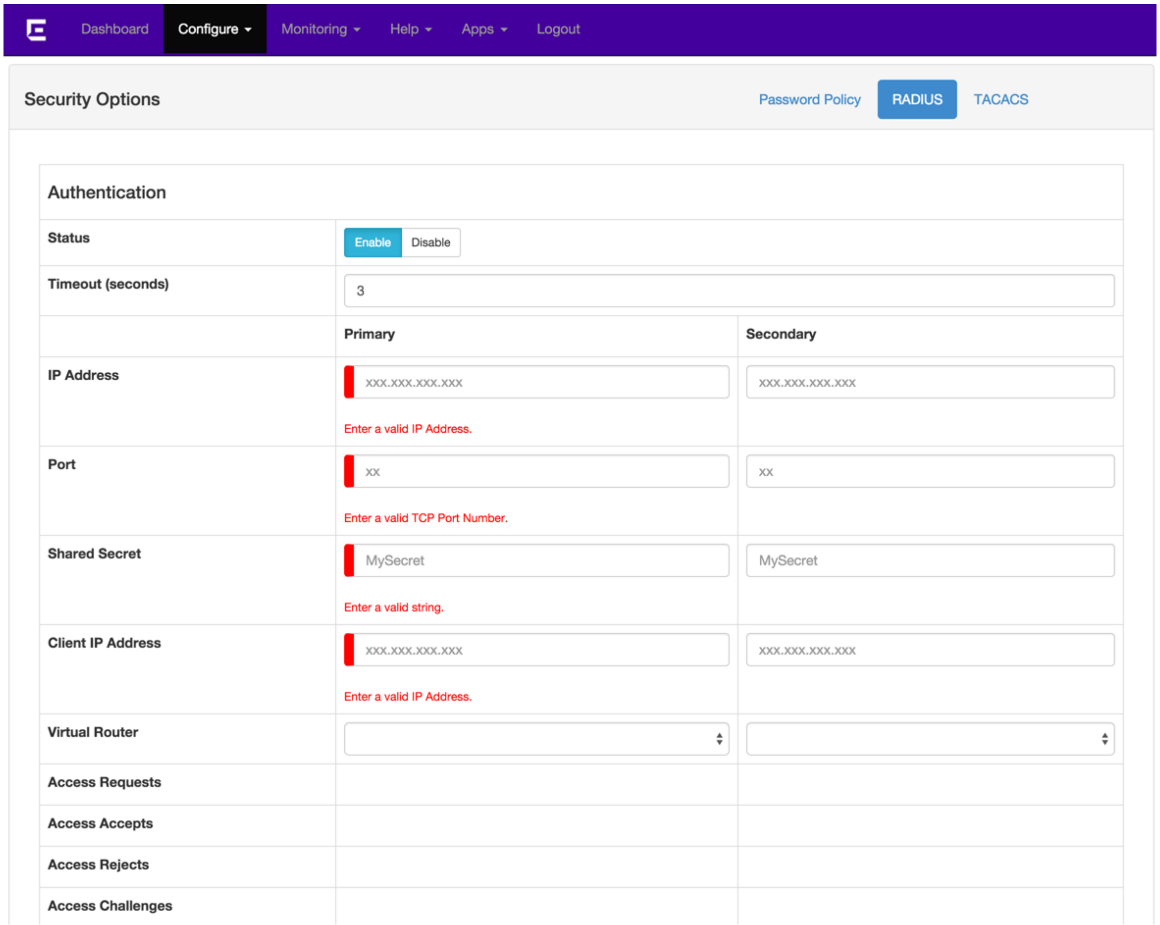
5. To enable RADIUS, click the **Enable** button in the Status field.



Security Options

Authentication

Status	Enable Disable	
Timeout (seconds)	3	
	Primary	Secondary
IP Address	xxx.xxx.xxx.xxx Enter a valid IP Address.	xxx.xxx.xxx.xxx
Port	xx Enter a valid TCP Port Number.	xx
Shared Secret	MySecret Enter a valid string.	MySecret
Client IP Address	xxx.xxx.xxx.xxx Enter a valid IP Address.	xxx.xxx.xxx.xxx
Virtual Router		



Security Options

Authentication

Status	Enable Disable	
Timeout (seconds)	3	
	Primary	Secondary
IP Address	xxx.xxx.xxx.xxx Enter a valid IP Address.	xxx.xxx.xxx.xxx
Port	xx Enter a valid TCP Port Number.	xx
Shared Secret	MySecret Enter a valid string.	MySecret
Client IP Address	xxx.xxx.xxx.xxx Enter a valid IP Address.	xxx.xxx.xxx.xxx
Virtual Router		
Access Requests		
Access Accepts		
Access Rejects		
Access Challenges		

6. Supply the information in the required fields.

   Note
   For the Shared Secret field, enter the *unencrypted* (plain text)

   secret, not the encrypted version. The switch will encrypt the shared secret for you.

   Note
   For the Client IP Address field, you must choose an IP interface existing on the switch so it is contained within the virtual router.

7. When finished configuring RADIUS, click **Save Config**.

To unconfigure this feature (by pushing down the "unconfigure" commands to the switch), you must remove all the text in any configured fields, disable the feature, and then apply and save your changes.

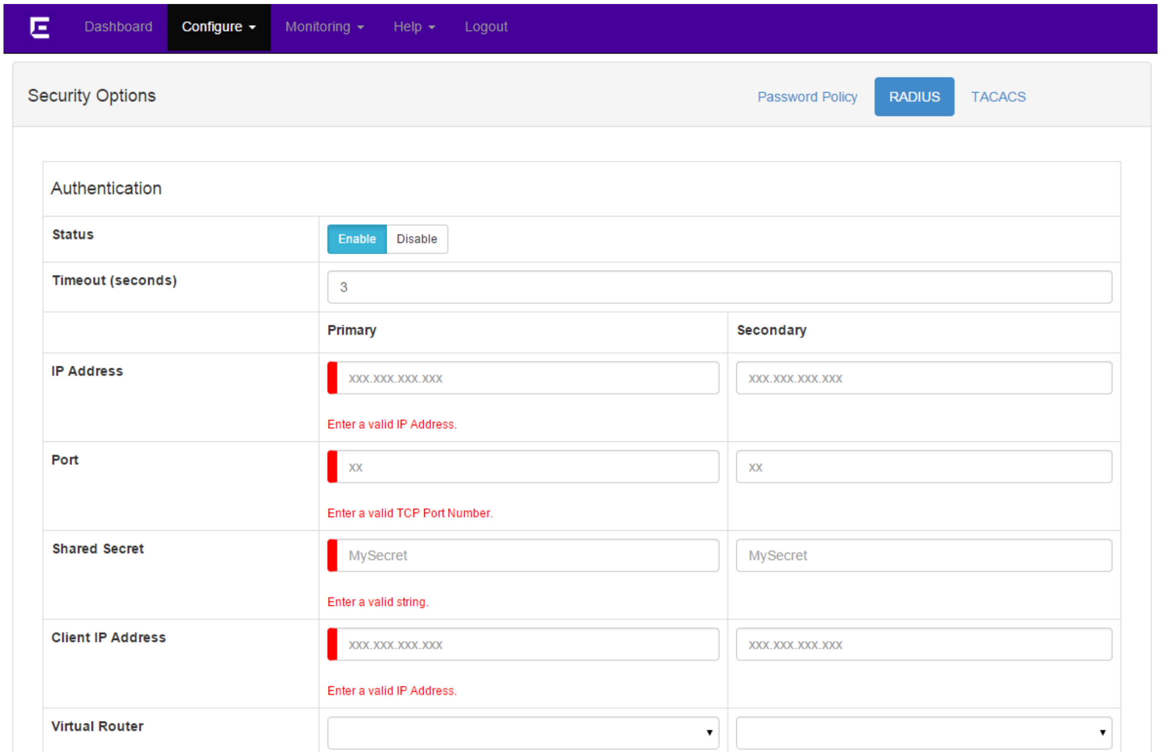
Configuring TACACS

You can enable and configure TACACS on the switch in one Chalet screen instead of entering multiple comands on the CLI. For more information about TACACS, see the "Security" section of the *ExtremeXOS User Guide*.

To configure TACACS:

1. Click **Configure** > **Accounts** to display the user list.
2. Click the **Security Options** tab.
3. Click the **TACACS** tab.
4. Click **Edit** at the bottom of the page.

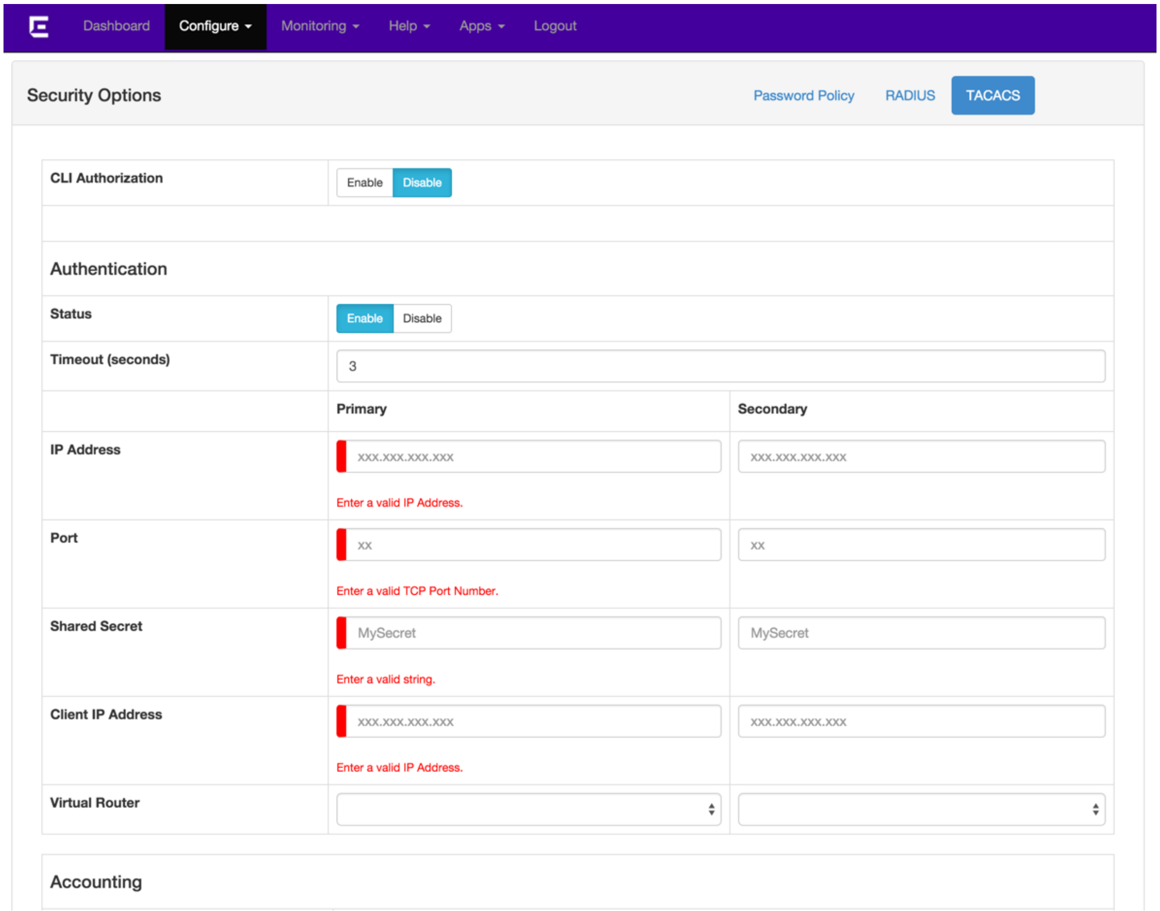
5. To enable TACACS, click the **Enable** button in the Status field.



Security Options

Authentication

Status	Enable [✓] Disable	
Timeout (seconds)	3	
	Primary	Secondary
IP Address	xxx.xxx.xxx.xxx Enter a valid IP Address.	xxx.xxx.xxx.xxx
Port	xx Enter a valid TCP Port Number.	xx
Shared Secret	MySecret Enter a valid string.	MySecret
Client IP Address	xxx.xxx.xxx.xxx Enter a valid IP Address.	xxx.xxx.xxx.xxx
Virtual Router		



Security Options

CLI Authorization	Enable [✓ Disable]

Authentication

Status	Enable [✓] Disable	
Timeout (seconds)	3	
	Primary	Secondary
IP Address	xxx.xxx.xxx.xxx Enter a valid IP Address.	xxx.xxx.xxx.xxx
Port	xx Enter a valid TCP Port Number.	xx
Shared Secret	MySecret Enter a valid string.	MySecret
Client IP Address	xxx.xxx.xxx.xxx Enter a valid IP Address.	xxx.xxx.xxx.xxx
Virtual Router		

Accounting

6. Supply the information in the required fields.
7. When finished configuring TACACS, click **Save Config**.

To unconfigure this feature (by pushing down the "unconfigure" commands to the switch), you must remove all the text in any configured fields, disable the feature, and then apply and save your changes.

Glossary

ACL

An Access Control List is a mechanism for filtering packets at the hardware level. Packets can be classified by characteristics such as the source or destination MAC, IP address, IP type, or QoS queue. Once classified, the packets can be forwarded, counted, queued, or dropped.

ad hoc mode

An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an AP.

ARP

Address Resolution Protocol is part of the TCP/IP suite used to dynamically associate a device's physical address (MAC address) with its logical address (IP address). The system broadcasts an ARP request, containing the IP address, and the device with that IP address sends back its MAC address so that traffic can be transmitted.

ATM

Asynchronous Transmission Mode is a start/stop transmission in which each character is preceded by a start signal and followed by one or more stop signals. A variable time interval can exist between characters. ATM is the preferred technology for the transfer of images.

BSS

Basic Service Set is a wireless topology consisting of one access point connected to a wired network and a set of wireless devices. Also called an infrastructure network. See also *IBSS (Independent Basic Service Set)*.

Chalet

Chalet is a web-based user interface for setting up and viewing information about a switch, removing the need to enter common commands individually in the CLI.

CHAP

Challenge-Handshake Authentication Protocol is one of the two main authentication protocols used to verify a user's name and password for PPP Internet connections. CHAP is more secure because it performs a three-way handshake during the initial link establishment between the home and remote machines. It can also repeat the authentication anytime after the link has been established.

CLI

Command Line Interface. The CLI provides an environment to issue commands to monitor and manage switches and wireless appliances.

Data Center Connect

DCC, formerly known as DCM (Data Center Manager), is a data center fabric management and automation tool that improves the efficiency of managing a large virtual and physical network. DCC provides an integrated view of the server, storage, and networking operations, removing the need to use multiple tools and management systems. DCC automates VM assignment, allocates appropriate network resources, and applies individual policies to various data objects in the switching fabric (reducing VM sprawl). Learn more about DCC at http://www.extremenetworks.com/product/data-center-connect/.

DHCP

Dynamic Host Configuration Protocol allows network administrators to centrally manage and automate the assignment of IP addresses on the corporate network. DHCP sends a new IP address when a computer is plugged into a different place in the network. The protocol supports static or dynamic IP addresses and can dynamically reconfigure networks in which there are more computers than there are available IP addresses.

DoS attack

Denial of Service attacks occur when a critical network or computing resource is overwhelmed so that legitimate requests for service cannot succeed. In its simplest form, a DoS attack is indistinguishable from normal heavy traffic. ExtremeXOS software has configurable parameters that allow you to defeat DoS attacks.

DSSS

Direct-Sequence Spread Spectrum is a transmission technology used in Local Area Wireless Network (LAWN) transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission. (Compare with *FHSS (Frequency-Hopping Spread Spectrum)*.)

EAP-TLS/EAP-TTLS

EAP-TLS Extensible Authentication Protocol - Transport Layer Security. A general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards.

IEEE 802.1x specifies how EAP should be encapsulated in LAN frames.
In wireless communications using EAP, a user requests connection to a WLAN through an access point, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS The server asks the access point for proof of identity, which the access point gets from the user and then sends back to the server to complete the authentication.

EAP-TLS provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys.

EAP-TTLS (Tunneled Transport Layer Security) is an extension of EAP-TLS to provide certificate-based, mutual authentication of the client and network through an encrypted tunnel, as well as to generate dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
(See also *PEAP (Protected Extensible Authentication Protocol)*.)

EDP

Extreme Discovery Protocol is a protocol used to gather topology information about neighboring Extreme Networks switches.

ESRP

Extreme Standby Router Protocol is an Extreme Networks-proprietary protocol that provides redundant Layer 2 and routing services to users.

Extreme Defender for IoT

Extreme Defender for IoT provides unique in-line security for mission critical and/or vulnerable IoT devices. Placed between the IoT device and the network, the Defender for IoT solution helps secure and isolate IoT devices protecting them from internal and external hacking attempts, viruses, malware and ransomware, DDoS attacks, and more. Designed to be simple and flexible, Defender for IoT can be deployed over any network infrastructure to enable secure IoT management without significant network changes.

The solution is comprised of the Extreme Defender Application Software and the Defender Adapter (SA201) or AP3912i access point. ExtremeCloud Appliance is the supported platform for the Extreme Defender Application.

For more information, see https://www.extremenetworks.com/product/extreme-defender-for-iot/.

Extreme Management Center

Extreme Management Center (ExtremeCloud IQ - Site Engine), formerly Netsight™, is a web-based control interface that provides centralized visibility into your network. ExtremeCloud IQ - Site Engine reaches beyond ports, VLANs, and SSIDs and provides detailed control of individual users, applications, and protocols. When coupled with wireless and Identity & Access Management products, ExtremeCloud IQ - Site Engine becomes the central location for monitoring and managing all the components in the infrastructure. Learn more about ExtremeCloud IQ - Site Engine at http://www.extremenetworks.com/product/management-center/.

ExtremeAnalytics

ExtremeAnalytics™, formerly Purview™, is a network powered application analytics and optimization solution that captures and analyzes context-based application traffic to deliver meaningful intelligence about applications, users, locations, and devices. ExtremeAnalytics provides data to show how applications are being used. This can be used to better understand customer behavior on the network, identify the level of user engagement, and assure business application delivery to optimize the user experience. The software also provides visibility into network and application performance allowing IT to pinpoint and resolve performance issues in the infrastructure whether they are caused by the network, application, or server. Learn more about ExtremeAnalytics at http://www.extremenetworks.com/product/extremeanalytics/.

ExtremeCloud Appliance

The ExtremeCloud Appliance is a next generation orchestration application offering all the mobility services required for modern unified access deployments. The ExtremeCloud Appliance extends the simplified workflows of the ExtremeCloud public cloud application to on-prem/private cloud deployments.

The ExtremeCloud Appliance includes comprehensive critical network services for wireless and wired connectivity, wireless device secure onboarding, distributed and centralized data paths, role-based access control through the Application Layer, integrated location services, and IoT device onboarding through a single platform.

Built on architecture with the latest technology, the embedded operating system supports application containers that enable future expansion of value added applications for the unified access edge. Learn more about ExtremeCloud Appliance at https://www.extremenetworks.com/product/extremecloud-appliance/.

ExtremeCloud

ExtremeCloud is a cloud-based network management Software as a Service (SaaS) tool. ExtremeCloud allows you to manage users, wired and wireless devices, and applications on corporate and guest networks. You can control the user experience with smarter edges – including managing QoS, call admission control, secure access policies, rate limiting, multicast, filtering, and traffic forwarding, all from an intuitive web interface. Learn more about ExtremeCloud at http://www.extremenetworks.com/product/extremecloud/.

ExtremeCloud™ IQ

ExtremeCloud™ IQ is an industry-leading and visionary approach to cloud-managed networking, built from the ground up to take full advantage of the Extreme Networks end-to-end networking solutions. ExtremeCloud IQ delivers unified, full-stack management of wireless access points, switches, and routers and enables onboarding, configuration, monitoring, troubleshooting, reporting, and more. Using innovative machine learning and artificial intelligence technologies, ExtremeCloud IQ analyzes and interprets millions of network and user data points, from the network edge to the data center, to power actionable business and IT insights, and deliver new levels of network automation and intelligence. Learn more about ExtremeCloud IQ at https://www.extremenetworks.com/extremecloud-iq/.

ExtremeControl

ExtremeControl, formerly Extreme Access Control™ (EAC), is a set of management software tools that use information gathered by a hardware engine to control policy to all devices on the network. The software allows you to automate and secure access for all devices on the network from a central dashboard, making it easier to roll out security and identity policies across the wired and wireless network. Learn more about ExtremeControl at https://www.extremenetworks.com/product/extremecontrol/.

ExtremeSwitching

ExtremeSwitching is the family of products comprising different switch types: **Modular** (X8 and 8000 series [formerly BlackDiamond] and S and K series switches); **Stackable** (X-series and A, B, C, and 7100 series switches); **Standalone** (SSA, X430, and D, 200, 800, and ISW series); and **Mobile Backhaul** (E4G). Learn more about ExtremeSwitching at http://www.extremenetworks.com/products/switching-routing/.

ExtremeWireless

ExtremeWireless products and solutions offer high-density WiFi access, connecting your organization with employees, partners, and customers everywhere they go. The family of wireless products and solutions includes APs, wireless appliances, and software. Learn more about ExtremeWireless at http://www.extremenetworks.com/products/wireless/.

ExtremeXOS

ExtremeXOS, a modular switch operating system, is designed from the ground up to meet the needs of large cloud and private data centers, service providers, converged enterprise edge networks, and everything in between. Based on a resilient architecture and protocols, ExtremeXOS supports network virtualization and standards-based SDN capabilities like VXLAN gateway and OpenStack Cloud orchestration. ExtremeXOS also supports comprehensive role-based policy. Learn more about ExtremeXOS at http://www.extremenetworks.com/product/extremexos-network-operating-system/.

FDB

The switch maintains a database of all MAC address received on all of its ports and uses this information to decide whether a frame should be forwarded or filtered. Each forwarding database (FDB) entry consists of the MAC address of the sending device, an identifier for the port on which the frame was received, and an identifier for the VLAN to which the device belongs. Frames destined for devices that are not currently in the FDB are flooded to all members of the VLAN. For some types of entries, you configure the time it takes for the specific entry to age out of the FDB.

FHSS

Frequency-Hopping Spread Spectrum is a transmission technology used in Local Area Wireless Network (LAWN) transmissions where the data signal is modulated with a narrowband carrier signal that 'hops' in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. This technique reduces interference. If synchronized properly, a single logical channel is maintained. (Compare with *DSSS (Direct-Sequence Spread Spectrum)*.)

IBSS

An IBSS is the 802.11 term for an ad hoc network. See *ad hoc mode*.

IGMP

Hosts use Internet Group Management Protocol to inform local routers of their membership in multicast groups. Multicasting allows one computer on the Internet to send content to multiple other computers that have identified themselves as interested in receiving the originating computer's content. When all hosts leave a group, the router no longer forwards packets that arrive for the multicast group.

LAG

A Link Aggregation Group is the logical high-bandwidth link that results from grouping multiple network links in link aggregation (or load sharing). You can configure static LAGs or dynamic LAGs (using the LACP).

MIC

Message Integrity Check (or Code), also called ‘Michael’, is part of WPA and TKIP. The MIC is an additional 8-byte code inserted before the standard 4-byte ICV appended in by standard WEP to the 802.11 message. This greatly increases the difficulty in carrying out forgery attacks.
Both integrity check mechanisms are calculated by the receiver and compared against the values sent by the sender in the frame. If the values match, there is assurance that the message has not been tampered with.

MLAG

The Multi-switch Link Aggregation Group feature allows users to combine ports on two switches to form a single logical connection to another network device. The other network device can be either a server or a switch that is separately configured with a regular LAG (or appropriate server port teaming) to form the port aggregation.

netmask

A netmask is a string of 0s and 1s that mask, or screen out, the network part of an IP address, so that only the host computer part of the address remains. A frequently-used netmask is 255.255.255.0, used for a Class C subnet (one with up to 255 host computers). The ".0" in the netmask allows the specific host computer address to be visible.

PEAP

Protected Extensible Authentication Protocol is an IETF draft standard to authenticate wireless LAN clients without requiring them to have certificates. In PEAP authentication, first the user authenticates the authentication server, then the authentication server authenticates the user. If the first phase is successful, the user is then authenticated over the SSL tunnel created in phase one using EAP-Generic Token Card (EAP-GTC) or Microsoft Challenged Handshake Protocol Version 2 (MSCHAP V2). (See also *EAP-TLS/EAP-TTLS*.)

PoE

The Power over Ethernet standard (IEEE 802.3af) defines how power can be provided to network devices over existing Ethernet connections, eliminating the need for additional external power supplies.

QoS

Quality of Service is a technique that is used to manage network resources and guarantee a bandwidth relationship between individual applications or protocols. A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services. Achieving the required QoS becomes the secret to a successful end-to-end business solution.

RADIUS

RADIUS is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. With RADIUS, you can track usage for billing and for keeping network statistics.

SNMP

Simple Network Management Protocol is a standard that uses a common software agent to remotely monitor and set network configuration and runtime parameters. SNMP operates in a multivendor environment, and the agent uses MIBs, which define what information is available from any manageable network device. You can also set traps using SNMP, which send notifications of network events to the system log.

SSL

Secure Socket Layer is a protocol for transmitting private documents using the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. SSL uses the public-and-private key encryption system, which includes the use of a digital certificate. SSL is used for other applications than SSH, for example, OpenFlow.

STP

Spanning Tree Protocol, defined in IEEE 802.1d, used to eliminate redundant data paths and to increase network efficiency. STP allows a network to have a topology that contains physical loops; it operates in bridges and switches. STP opens certain paths to create a tree topology, thereby preventing packets from looping endlessly on the network. To establish path redundancy, STP creates a tree that spans all of the switches in an extended network, forcing redundant paths into a standby, or blocked, state.

STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail. If STP costs change, or if one network segment in the STP becomes unreachable, the spanning tree algorithm reconfigures the STP topology and re-establishes the link by activating the standby path.

syslog

A protocol used for the transmission of event notification messages across networks, originally developed on the University of California Berkeley Software Distribution (BSD) TCP/IP system implementations, and now embedded in many other operating systems and networked devices. A device generates a messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.
syslog uses the UDP as its underlying transport layer mechanism. The UDP port that has been assigned to syslog is 514. (RFC 3164)

virtual router

In the Extreme Networks implementations, virtual routers allow a single physical switch to be split into multiple virtual routers. Each virtual router has its own IP address and maintains a separate logical forwarding table. Each virtual router also serves as a configuration domain. The identity of the virtual router you are working in currently displays in the prompt line of the CLI. The virtual routers discussed in relation to Extreme Networks switches themselves are not the same as the virtual router in VRRP.

In VRRP, the virtual router is identified by a virtual router (VRID) and an IP address. A router running VRRP can participate in one or more virtual routers. The VRRP virtual router spans more than one physical router, which allows multiple routers to provide redundant services to users.

VLAN

The term VLAN is used to refer to a collection of devices that communicate as if they are on the same physical LAN. Any set of ports (including all ports on the switch) is considered a VLAN. LAN segments are not restricted by the hardware that physically connects them. The segments are defined by flexible user groups you create with the CLI.

VR-Default

This virtual router is part of the embedded system in Extreme Networks switches. VR-Default is the default VR on the system. All data ports in the switch are assigned to this VR by default; you can add and delete ports from this VR. Likewise, VR-Default contains the default VLAN. Although you cannot delete the default VLAN from VR-Default, you can add and delete any user-created VLANs. One instance of each routing protocol is spawned for this VR, and they cannot be deleted. (Referred to as VR-2 in earlier ExtremeXOS software versions.)