ExtremeCloud IQ v24.6.0 Universal Switch Deployment Guide

Configuration, Management, and Best Practices

9038988-00 Rev AA
September 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: https://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/

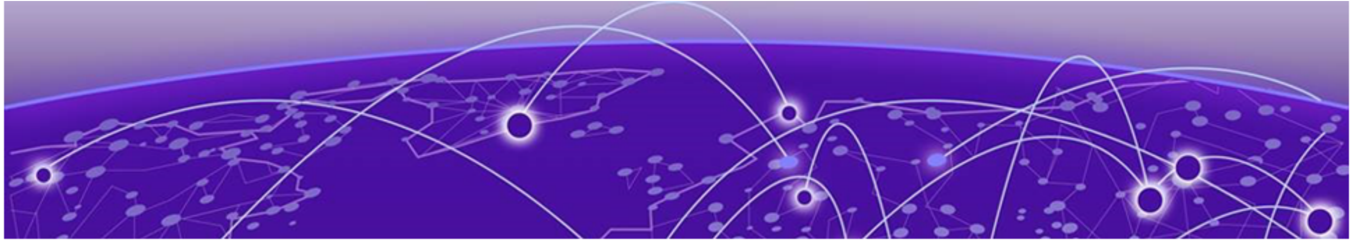
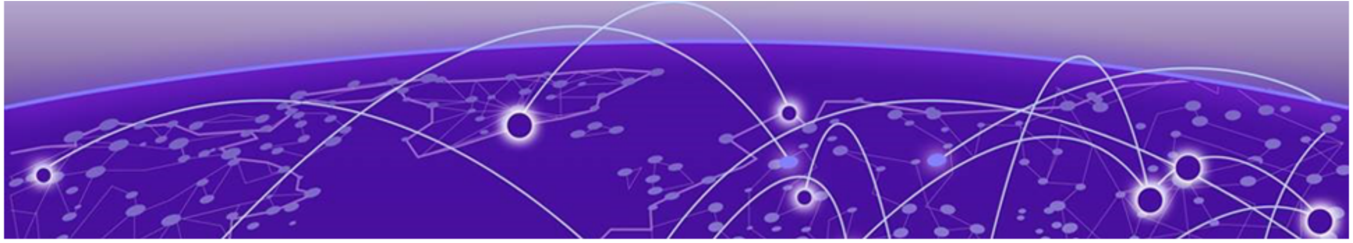
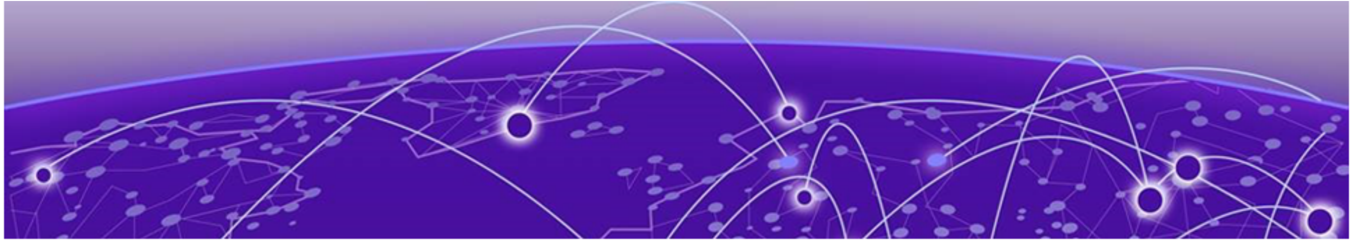


Table of Contents



Abstract

This Deployment Guide for ExtremeCloud IQ Universal Switch version 24.6.0 provides detailed instructions for deploying and managing Extreme Networks Universal Switches using ExtremeCloud IQ. The guide covers connecting switches to the network, configuring firewall access, onboarding switches, creating topology maps, and changing the network operating system between Switch Engine and Fabric Engine. It includes steps for creating and configuring network policies, managing device-specific settings, and monitoring switches. The document also addresses troubleshooting, resolving configuration discrepancies, updating device software, and downloading technical support files. References to CLI commands and other detailed settings are provided for both Switch Engine and Fabric Engine environments.



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.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes
Hardware and Software Compatibility for Extreme Networks products
Extreme Optics Compatibility
Other Resources such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the Open Source Declaration page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the Extreme Networks Training page.

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.

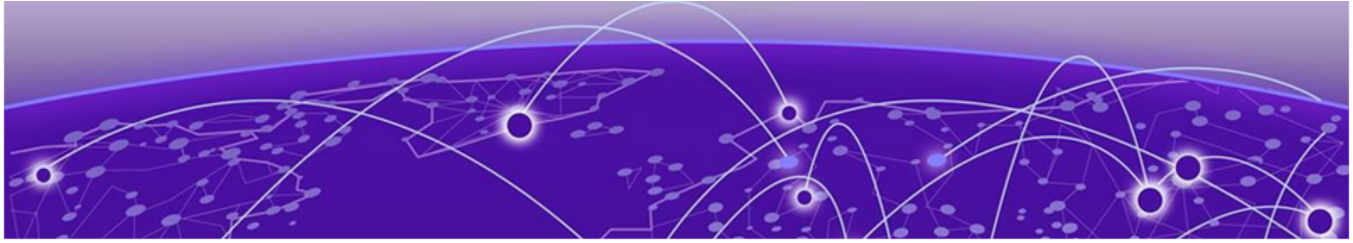
Send Feedback

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.



Overview of Universal Switch Deployment in ExtremeCloud IQ

The Universal hardware platform is a family of high-performance, feature-rich edge, and aggregation switches designed for the next generation digital enterprise. It comes with a dual-persona capability for user choice of the switch Network Operating System (NOS).

- All Universal switches have Switch Engine and Fabric Engine pre-installed and ready to run. After onboarding a switch to ExtremeCloud IQ, you can change the NOS from Switch Engine (the default) to Fabric Engine.
- Support starts from Switch Engine 31.6 and Fabric Engine 8.6.
- A one-year Pilot-level subscription is offered with every Universal device purchase.

This document provides instructions for using ExtremeCloud IQ to configure and monitor the Extreme Networks Universal Switch series. For any CLI information, see the following guides:

- Fabric Engine: *Fabric Engine CLI Commands Reference*
- Switch Engine: *Switch Engine CLI Commands Reference*

For IQ Agent and other Universal Switch operating system information, see the following guides:

- Fabric Engine: *Fabric Engine User Guide*
- Switch Engine: *Switch Engine User Guide*

To become familiar with the ExtremeCloud IQ deployment process steps, see Deploy Universal Switches on page 12.

Note

To use this guide for non-Universal switches:

- **EXOS Devices**: Refer to information geared towards Switch Engine devices.
- **VOSS Devices**: Refer to information geared towards Fabric Engine devices.
- Disregard the **Change the Network Operating System** task as that does not pertain to non-Universal switches.
- Ensure all devices operate with the latest firmware and operating system.

Deploy Universal Switches

Use this task to deploy a Universal Switch to interact with ExtremeCloud IQ.

> Note
> You must already have set up your network in ExtremeCloud IQ, including configuring your buildings, floor plans, locations, etc.

1. Connect the switches to the network and power them up.
2. Ensure you have proper outbound access allowed on your firewall from the switch in order to connect to the cloud. For more information, see Configure Firewall Access on page 15.
3. Onboard switches by adding their serial numbers to your ExtremeCloud IQ account.

   > Note
   > When configuring switch features that are not supported within a **Network Policy**, switch template, or device-level configuration in ExtremeCloud IQ, you must follow these guidelines to avoid unintended behaviors and potential device update failures:
   >
   > a. Supplemental CLI Configuration:
   >   - Use the Supplemental CLI to add unsupported features.
   >   - Ensure that the Supplemental CLI configuration does not overlap with the ExtremeCloud IQ configuration. For more information, see Configure Supplemental CLI on page 42.
   >
   > b. Avoid Overlapping Configurations:
   >   - Do not use SSH proxy, Web CLI, or console access to add configurations that overlap with those managed by ExtremeCloud IQ. Overlapping configurations can cause device update failures when pushed from ExtremeCloud IQ.
   >
   > c. Potential Risks:
   >   - Modifying configurations within CLI while the switch is cloud-managed can lead to unintended behaviors, such as disabling the ExtremeCloud IQ Agent or restarting network tools.
   >   - In the event of a switch crash, manual recovery may be necessary to reconnect the switch to the cloud.
   >
   > By adhering to these guidelines ensures a stable and consistent configuration management process for your cloud-managed switches.

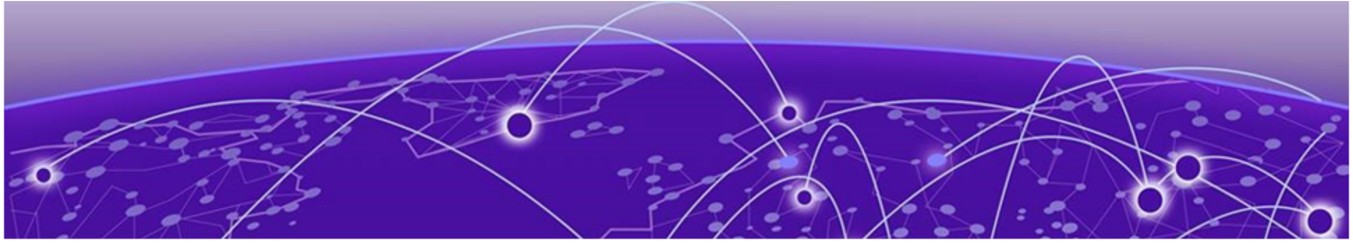
4. (Optional) Change the default Network Operating System from Switch Engine to Fabric Engine.
5. Create topology maps to associate switches with locations.

6. Configure a network policy with a switch template and additional settings (for example, DNS, Syslog, SNMP).

   Note
   To configure a switch feature not supported within a Network Policy, switch template, or device-level configuration, add that feature in the Supplemental CLI, (refer to Configure Supplemental CLI on page 42). The Supplemental CLI must not overlap with the ExtremeCloud IQ configuration. Additional configuration via SSH proxy, Web CLI, or console access must also not overlap with the ExtremeCloud IQ configuration or a **`Device Update Failure`** might occur when you push the overlapping configuration from ExtremeCloud IQ.

7. Deploy the Network Policy.

Note
After you deploy your Network Policy, you have the option to configure specific devices at the device level, which will override the Network Policy for that specific device, and then push these specific configurations to the device. Refer to Configure Device-Specific Settings on page 87.



Onboard Switches

After you create an account, you can use two methods to onboard your devices:

- Quick Add Devices: Use to add devices to an established ExtremeCloud IQ network.
- Deploy Devices to the Cloud: Use for your initial ExtremeCloud IQ setup.

Related Topics

Create an Account on page 14

Create an Account

Before you onboard your devices, you must create an ExtremeCloud IQ account. Use this task to create your account.

1. Go to https://www.extremecloudiq.com.
2. Select **Register for a new account**.
3. Fill in the form, then select **Register**.
4. Select **Setup Password**.
5. Enter the password, then select **Next**.

6. Select one of the following options:
    - **I want to continue with my 30-day trial of ExtremeCloud IQ**: If you do not have an entitlement key for ExtremeCloud IQ but want to try it out, you can choose this option to begin or continue a 30-day ExtremeCloud IQ trial.
    - **I have an ExtremeCloud IQ entitlement key**: Select this option if you have received your ExtremeCloud IQ key and want to begin using it. The key looks something like `QV23E-S81KJ-8BPLV-V1LVC-QUCIX-XXXXX`.
    - **Start with ExtremeCloud IQ Connect**: Select this option to begin using ExtremeCloud IQ Connect, free of charge, which provides you with sufficient tools to configure and manage Extreme Networks devices in common network environments.
7. Accept the end-user license agreement.

Configure Firewall Access

To connect to the cloud, you must configure firewall access. Use this task to configure firewall access.

1. In the top-right corner of the mail ExtremeCloud page, select the icon next to your user information.
2. Select **About ExtremeCloud IQ**.
3. Select the **Firewall Configuration Guide** link.

    For example: https://extremecloudiq.com/support/US_East2.html
4. Use the table to ensure all in-line firewalls enable outbound connections to the listed Extreme cloud services.
5. You can also access this table from the ExtremeCloud IQ Release notes, see https://supportdocs.extremenetworks.com/support/documentation/extremecloud-iq/ .

Deploy Devices to the Cloud

Use this task to set up a new ExtremeCloud IQ network and onboard and manage devices. The first time you log in, the **Welcome to ExtremeCloud IQ** onboarding panel opens to the right of the main window. For subsequent log ins, to see this panel, select the expand arrow in the blue rectangle on the right edge of any window.

1. Name your organization, then select **Continue**.
2. Choose to deploy and manage your devices in the cloud, then select **Let's get started**.
3. Add a Location, then select **Save Location**.
4. Select **Next: Building**.
5. Add a Building, then select **Save Building**.
6. Select **Next: Floor**.
7. Add a Floor, associate it with a building, select an environment from the options, enter the floor attenuation, and the device installation height.

    > Note
    > Select **Choose from Library** to import a floorplan image.

8. Choose to onboard **Real** device.
9. Enter the device serial number.
10. For the **Device OS**, choose **Switch Engine** or **Fabric Engine** before you can onboard a Universal Hardware Switch.
11. Select **Onboard Devices**.
12. Select **Next: Topology**.

Assign a location to a device.

Create a Topology Map

Onboard the device and select **Next: Topology**.

The list at the top of the dialog box shows the locations in your network and the number of devices assigned at each location (in purple), if any. Reference the location list for this task.

1. Select a floor from the location list to display the floor plan.
2. Select one or multiple devices from the list of unassigned devices and drag them to the floor map.

   You can use the type-ahead search box to locate devices or the filter tool to narrow your search.
3. Use the pencil icon to edit the device name.
4. Select **Finish**.

After connection to ExtremeCloud IQ, the device status changes from Red to Green. It can take up to 3 minutes.

Change the Network Operating System

Onboard the device to ExtremeCloud IQ.

Universal switches are preloaded with two Network Operating Systems (NOS): Switch Engine and Fabric Engine. Switch Engine is the default NOS. Use this task to change the current default NOS to Fabric Engine.

1. Select **Manage** > **Devices**.
2. Locate the device in the **Device List** and select it.

   Notice that under **Host Name**, the name extension is Switch Engine. For example, Switch Engine 5520-48W-Switch Engine.
3. Select **Actions** > **Change OS to Fabric Engine**.
4. Select **Yes**.

The **Host Name** now has the Fabric Engine extension. If you select **Actions** again, the option says **Change OS to Switch Engine**.

Quick Add Devices

Use this task to quickly add devices to ExtremeCloud IQ from the **Manage** > **Device List** page.

1. Go to **Manage** > **Devices**.
2. Select +, then select **Quick Add Devices**.
3. Select **Manage your devices directly from the cloud**.
4. For **Device Type**, select **Real** or **Simulated**.

   - For **Real** devices: For **Entry Type**, either select **Manual** and enter device serial numbers in the field, or select **CSV** to import a **.csv** file with a list of device serial numbers or service tags. If you select **Manual**, ExtremeCloud IQ tries to detect your device automatically when you submit the serial numbers and displays the detected device make in a separate field. If it cannot detect the device make from the serial number, it prompts you to select a device make manually.

     Note
     To onboard a Universal Hardware Switch, for the **Device OS**, choose **Switch Engine** or **Fabric Engine**.

     Your CSV file must have at least one field containing serial numbers or service tags. Add a second field for the model numbers of the devices. For example:

     Serial Number:

     01234567890123

     01234567890124

     01234567890125

     Serial Number and Model Number:

     01234567890123, AP3000

     01234567890124, AP410

     01234567890125, AP5050

     Note
     Avoid using spreadsheet applications such as Excel to create or modify a .csv file. Excel formats serial numbers that contain preceding zeros incorrectly. Many applications interpret the serial number as a numeric value, which can cause the preceding zeros to be lost and the value to be represented in scientific notation, requiring you to use special functions or convert the cell content type. Instead, use a text editor that does not format the contents.

   - For **Simulated** devices: In the **Device Model** drop-down list, choose a model, and enter the number of devices to add. Repeat this step to add different models.

- For **Digital Twin** devices: Use to create a simulated Switch Engine Switch. Select `Switch Engine` from the **OS Persona**, then select the **Device Model** and **OS Version**. Proceed to Step 4.

  Note
  You can only add Digital Twin devices if you are also using ExtremeCloud IQ CoPilot.

- For **Simulated** devices: In the **Device Model** drop-down list, choose a model, and enter the number of devices to add. Repeat this step to add different models.
- For **Digital Twin** devices: Use to create a simulated Switch Engine Switch. Select `Switch Engine` from the **OS Persona**, then select the **Device Model** and **OS Version**. Proceed to Step 4.

  Note
  You can only add Digital Twin devices if you are also using ExtremeCloud IQ CoPilot.

5. For **Location**, select a location from the pick list.

   Note
   You cannot create a new location in the Quick Add process; you can select an existing location.

6. (Optional) From the **Policy** menu, select an existing network policy.
7. Select **Add Devices** or **Launch Digital Twin**.

   Note
   To add a device that was previously onboarded using an earlier version of ExtremeCloud IQ or Extreme Management Center, you must first delete the device from the older version. In these instances, you see an alert.

After connection to ExtremeCloud IQ, the device status changes from Red to Green. It can take up to 3 minutes.

Device Management

Use the following table to become familiar with the different symbolic representations in the **Devices List** on the ExtremeCloud IQ landing page. Hover over an icon on the page to display its name, then refer to the table.

Table 4: Device Status Icons

Icon	Icon Name	Description
!	AFC Status	Indicates an AFC issue with the selected device. Status options include **Pending**, **Grace Period**, and **Spectrum Mismatch**. For more information, select the AFC status icon to open the **AFC Wireless** view of the selected device.
☁	Provisioned Device	An administrator has provisioned the device, but the device has not yet communicated with ExtremeCloud IQ. This is an administrative state and does not reflect the actual connection status. To view the actual connection status, you must manually change the management state using the **Actions** > **Change Manage Status** > **Managed Devices** menu option.
☁	Connected Device	Device is actively communicating with ExtremeCloud IQ.
☁	Disconnected Device	Device is not actively communicating with ExtremeCloud IQ. Cause: The device might be physically disconnected from the network or powered off. This condition also occurs if there are interruptions in the network between the device and ExtremeCloud IQ or when there are misconfigured firewalls or ACL rules. Action: Ensure the device is connected to the network and powered on and ensure that communication can occur through logical barriers such as firewalls.
!	Configuration Rollback	Device could not establish a connection to ExtremeCloud IQ after the configuration update. Device configuration rolled back to the last known good connection and the **Updated** status column displays *Device update failed*.
☁	Simulated Device	Device is a simulated device, which possesses only simulated configurations, conditions, and traffic. By contrast, a real device has a physical presence on the network and consumes power and network resources.
?	Undetermined	Device status is undetermined. Cause: This condition can arise when the indicators are ambiguous, unknown, or appear contradictory due to other factors. Action: Begin general troubleshooting procedures to ensure that the device is powered, connected, and is responding to traffic and CLI commands. Ensure that the device is communicating appropriately with network services, such as NTP, DHCP, etc.

Table 4: Device Status Icons (continued)

Icon	Icon Name	Description
⊘	Old OS Personality (Inactive)	Device formerly used another OS persona, which is no longer active. The information in this record pertains to the device when it ran using this OS persona.
✓	Configuration Audit Match	The network policy configuration matches the current running configuration. Select the icon to open a pop-up window detailing the configuration changes that occurred since the last **Update Devices** operation. • Audit tab — lists any modifications made since the previous configuration update. • Delta tab — shows CLI commands that have changed since the previous update. • Complete tab — shows all CLI commands (including the CLI commands in the Delta tab) that form a configuration file. ExtremeCloud IQ uses this file for the next configuration update. After a successful configuration update, the configuration in the Complete tab matches the running configuration. Note: Not applicable for locally managed switches.
ⓘ	Configuration Audit Mismatch	The network policy configuration does not match the current running configuration. Cause: The Configuration Audit Mismatch icon is visible on devices between the time that network policy changes are saved and the time that the altered network policy is uploaded to the device. Action: Upload the network policy to the device. Select the icon to open a pop-up window detailing the configuration changes that occurred since the last **Update Devices** operation. See the Configuration Audit Match icon description for details. Note: Not applicable for locally managed switches.
📋	Configured at Device Level	Device possesses a device-level configuration that is different from the configuration defined in the network policy. This is not an error condition, but this information can be useful when troubleshooting network behavior because device-level configurations supersede device templates and network policy configurations.
!	Device Update Unsuccessful	Device did not accept the OS or configuration upload. Cause: There are many reasons for an unsuccessful update, but the most common include network connectivity or connection status changes, or the device rejected the command it received. Action: Hover over the update message in the Updated column to view the reason message describing the likely error condition. Ensure that the device is properly powered, that there is appropriate network connectivity, and that common causes listed here are not the issue.

Table 4: Device Status Icons (continued)

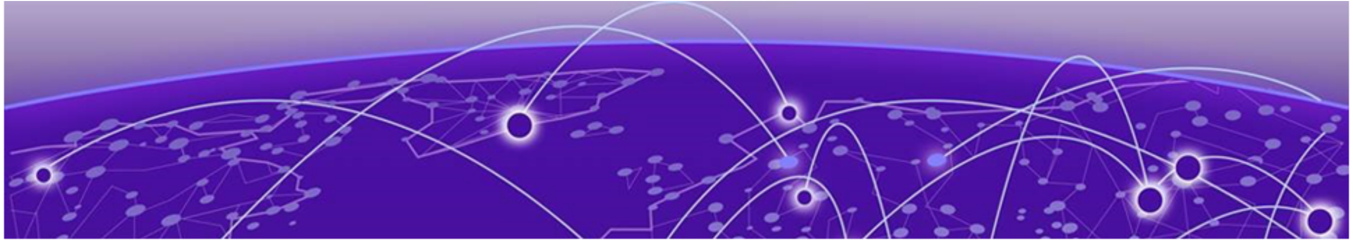
Icon	Icon Name	Description
IOT	Managed by ExtremeIoT	Device is provisioned to function with ExtremeIoT.
	Thread Commissioner Running	The AP is designated Commissioner in the IoT Thread network.
	Monitoring Unassociated Clients	Device is using presence analytics to monitor client devices that are not associated to the network, such as passersby.
	Switch Stack	Device is a switch stack. Select the icon to expand the device list view to include details for the switch stack members.
	Switch Stack Warning	One or more stack member switches is not associated to the master stack node. Cause: One or more member switches within a stack has lost connectivity to the master stack node. This can happen if the member switch is powered off, physically disconnected from the stack, or if there is an issue with the switch itself. Action: Ensure that the switch slot has power and that the stacking cables are properly connected.
	RadSec Proxy Server	Device is acting as a RadSec proxy server. This service optimizes some authentication functions, especially for cloud authentication, such as cloud PPSK and cloud RADIUS.
	Rogue AP Mitigation On	Device is actively mitigating a rogue access point. Refer to the information provided by your security management platform.
	Sensor Mode - Interface Active	Device is functioning as a sensor and the monitoring interface is active and monitoring the RF environment.
	Sensor Mode - Interface Inactive	Device is functioning as a sensor, but the monitoring interface is not active and is not monitoring the RF environment.
⇅	Swap for Real Device	Device is a simulated device that you can exchange for a real device.
	Spectrum Intelligence	Device is functioning as a Spectrum Intelligence monitor, which monitors the RF environment and provides frequency and time domain graphs and heat maps.
S↑	VPN Server - Tunnel Up	Device is functioning as a VPN server and the VPN tunnel is up, healthy, and operating properly.

Table 4: Device Status Icons (continued)

Icon	Icon Name	Description
S↓	VPN Server - Tunnel Down	Device is functioning as a VPN server, but the VPN tunnel is down. If the tunnel is administratively down, then this is not an error condition. Cause: If not administratively down, issues on the client side can cause the tunnel to go down. Additionally, if the client- and server-side configuration do not agree, then a tunnel cannot be built. Action: Consult the VPN troubleshooting tools in ExtremeCloud IQ. You can also ensure that the client device is connected to the network and that the tunnel configurations agree on both ends of the tunnel.
S↑↓	VPN Server - Tunnels Up and Down	Some of the VPN server tunnels are administratively up but operationally down. Cause: VPN client might be down, or unreachable. Action: Ensure that the VPN clients are powered on, connected to the network, and communicating with ExtremeCloud IQ. In addition, ensure that there is connectivity and communication between the VPN server and clients.
C↑	VPN Client - Tunnels Up	Device is functioning as a VPN client and the VPN tunnel is up, healthy, and operating properly.
C↓	VPN Client - Tunnels Down	Device is functioning as a VPN client, but the VPN tunnel is down. If the tunnel is administratively down, then this is not an error condition. Cause: If not administratively down, issues on the server side can cause the tunnel to go down. Additionally, if the client- and server-side configuration do not agree, then a tunnel cannot be built. Action: Consult the VPN troubleshooting tools in ExtremeCloud IQ. You can also ensure that the server device is connected to the network and that the tunnel configurations agree on both ends of the tunnel.
C↑↓	VPN Client - Tunnels Up and Down	Some of the VPN client tunnels are administratively up but operationally down. Cause: VPN server might be down, or unreachable. Action: Ensure that the VPN server is powered on, connected to the network, and communicating with ExtremeCloud IQ. In addition, ensure that there is connectivity and communication between the VPN server and client.
📍	Locally Managed (ExtremeCloud IQ)	Device is managed by a platform that is visible in ExtremeCloud IQ.

Table 4: Device Status Icons (continued)

Icon	Icon Name	Description
📍	Locally Managed (No ExtremeCloud IQ)	Device or its management platform are not visible in ExtremeCloud IQ. Cause: This is not always an error condition, but it can indicate a status communication problem. In this case, the device is functioning properly, so there is no disruption in network performance; instead, the status communication is disrupted so that ExtremeCloud IQ is unaware of the status. Action: First, ensure that the device is functioning properly to rule out problems with the device. Next, ensure that there are no logical barriers between the device and ExtremeCloud IQ. Afterward, ensure that any applications that lie in the communication path are receiving, processing, and sending data appropriately.
●+	ExtremeCloud Appliance Cluster (Closed)	Device is a logical cluster of appliances, but the cluster is collapsed visually to appear as a single device.
●−	ExtremeCloud Appliance Cluster (Open)	Device is a logical cluster of appliances, but the cluster is expanded visually to reveal the cluster members.
◎	Fabric Attach	Device is a member of the Fabric Attach Connect Automation environment and is functioning properly in that context.
◎	Fabric Attach Issue	Device is Fabric Attach capable, but the Fabric Attach (FA) session to the FA server is not established. Cause: This can occur if the communication link between the FA device and server is disrupted or if FA is disabled on the peer switch. Action: Ensure that there is connectivity between FA device and server, and that FA server functionality is enabled on the peer switch.
🎭	Digital Twin	Device is a simulated device.



Configure the Network Policy

A Network Policy is an assembly of configurations that ExtremeCloud IQ deploys to all devices. Because these configurations are set at the network policy level, you can apply them to multiple devices for a similar configuration. The network policy section has a **Switching** section for managing Switch Engine and Fabric Engine templates and settings.

The **SR/Dell Switching** section is separate. The availability of each section depends on the policy type selected on the **Policy Details** page. In contrast, device-level configurations apply only to individual devices. Device-level configurations override network policy-level configuration. For example, you can set a network policy to apply to all 5420 switches, but at the device level, you can customize one 5420 switch in a particular location. For more information about device-level configuration, see Configure Device-Specific Settings on page 87.

Note
Device Management settings do not put the device into device-level configuration mode as each device will likely have a unique setting (unique static IP).

Network Policy configuration options are available under the main **Configure** tab.

Create a Network Policy

Network Policy configuration applies to multiple devices. If you want to customize only one device, see Configure Device-Specific Settings on page 87.

1. Go to **Configure** > **Network Policies** > **Add Network Policy**.
2. If desired, you can deselect **Wireless**, **SR/Dell Switching**, and **Branch Routing** so that only **Switches** is selected for policy type.
3. Enter a **Policy Name**.
4. (Optional) Enter a **Description**.

   Note
   Presence Analytics is a Wireless feature and has no relevance with Universal devices.

5. Select **Save**.
6. Select **(3) Switching** from the breadcrumbs at the top of the page.

Configure Policy Settings

The following configuration settings are the only settings applicable to switches. All other settings displayed in this section are applicable to wireless products only.

- DNS Server
- NTP Server
- SNMP Server
- Syslog Server Settings
- LLDP/CDP

The network policy settings that you configure depend on your requirements. For example, determine which default routing instance to use for NTP, DNS, Syslog, and SNMP for a switch.

This task is part of the network policy configuration workflow. Use this task to configure policy settings.

1. Go to **Configure** > **Network Policies**.
2. Select an existing network policy, and then select ✎, or select + to create a new policy.
3. Configure the **Policy Settings**.
   a. Configure a DNS Server on page 43
   b. Configure an NTP Server on page 44
   c. Configure an SNMP Server on page 45
   d. Configure a Syslog Server on page 47

e. Configure Device Credentials on page 90
f. Configure LLDP/CDP Policy Settings on page 49

> **Note**
> To configure LLDP port configurations on SR22XX, 23XX, VOSS, and EXOS devices, go to the device template or device configuration page. Configuring LLDP from this page can affect APs, XR, and 20XX/21XX switches, along with certain EXOS, VOSS, SR22XX, and 23XX Global LLDP parameters.

4. Select **SAVE**.

Configure Switch Common Settings

This section contains configuration elements applicable to all Switch Engine, EXOS, Fabric Engine, and VOSS switches assigned to a specific network policy.

1. Go to **Configure** > **Network Policies** > **Switching/Routing**.
2. For **Management Servers** (Switch Engine/EXOS only), select **VR-Default** or **VR-mgmt** to apply the correct routing instance to defined network policy DNS, NTP, SNMP, and Syslog server settings.
3. For the remainder of the configuration options, see Perform Device Configuration on page 29.

Port Type Settings

Use the **Port Types** menu to manage Switch Engine (EXOS) and Fabric Engine (VOSS) port types within the network policy.

Go to **Configure** > **Network Policies**, select your device, select **Switching/Routing** > **Switch Settings** > **Port Types** to view, create, edit, clone, and delete switch port types. For more information about port type configuration, see Configure Ports in Bulk on page 32.

To add a port type, select +.

To edit a port type, select the desired port type, and select ✎.

To clone a port type, select the desired port type, and select ⧉.

The Port Types table column display is configurable. The table displays the following columns by default:

- Device Family
- Port Usage
- Port Status
- VLAN
- Used By - Select the entry in the row (Total number of usages) to view the Device configuration, Device Template, and Network Policy where this port type is used.

To add additional, hide, or remove columns, select ▥.

You can filter the port types to view Switch Engine, EXOS or Fabric Engine, VOSS, or both.

To delete a port type, select desired port type, and select 🗑.

Note
You cannot delete a port type if it is currently assigned to a switch associated to any network policy.

VLAN Attributes

Use the VLAN attributes page to define additional configurations on a per-VLAN basis within a network policy. VLAN attributes are applied when the VLAN is defined within an assigned port type or when the VLAN deployment option is enabled. If dynamic VLANs are utilized, then the VLAN deployment option can be enabled within the VLAN attributes page to apply VLAN settings.

Note
A VLAN defined within Instant Port Profiles as Non-Forwarding will not apply VLAN attributes.

To create a new VLAN Attribute:

1. Go to **Configure** > **Network Policies**.
2. Select a network policy.
3. Select **Switch Template** > **Switch Settings** > **VLAN Attributes**.
4. Select +.
5. Configure the following settings:

Table 5: VLAN Attributes

Setting	Description
Use VLAN common object	Select **Use VLAN common object** to automatically update the VLAN NAME and VLAN ID.
Manual	Select **Manual** to customize the following fields: • VLAN ID - The numerical identification number of the VLAN. This can be any currently unused number. • VLAN Name - The name of the VLAN.
IGMP Snooping VLAN Settings	Enable **IGMP Snooping** for switches to identify ports to which multicast group member hosts are attached in order to optimize the distribution of multicast traffic. Note: Enable **Immediate Leave** to remove multicast host immediately when it leaves the group.

Table 5: VLAN Attributes (continued)

Setting	Description
DHCP Snooping VLAN Settings	Enable snooping of DHCP packets and creates a DHCP bindings database of IP to MAC addresses for this VLAN. Choose to enable DHCP Snooping, and the drop rogue DHCP packets action.
VLAN Deployments	With VLAN Deployments, VLAN and VLAN attributes can be created on switches when no port types are assigned with the defined VLAN.
Used By	How many devices use this VLAN. This field is system-generated.

6. Select **Save**.

Configure a Device Template

A device template provides a diagram of the physical ports for a specific Universal device and allows you to specify its functionality. For example, after you configure a device template for a specific device type, you assign its ports to various port types. A port type defines how the ports assigned to it will function. You configure the default port settings and other device functions and apply these settings to large numbers of devices of the same type. If you want to apply different device templates to other devices in the same network policy, you can do so.

You can make use of default templates, which are pre-loaded in ExtremeCloud IQ for every device model. The available template list expands as you create new policies. You can then use the same template for another policy.

If you select a default template, you must copy it by saving it as a new template. This will carry all the settings in the default template and let you customize it as required.

1. Go to **Configure** > **Network Polices** > **the existing network policy** > **Switch Settings** > **Switch Template**.
2. To create a new template based on an existing switch template, from the ☰ menu, scroll to an existing Universal device template, or Stack template, for example, **Switch Engine 5520-24T**.
3. Select **Copy**.
4. Enter a name for this copy.
5. To create a brand-new template not based on an existing default, select +.
6. Select a device type from the drop-down, for example, `Switch Engine 5320-24T-8XE`.
7. Enter a name for the new template, for example, `TEST_5320`.
8. Select **Save**.
9. To clone an existing template, select the check box of the existing template, and select ⧉.
10. Select the template to display the **Device Template** configuration page.

Proceed to Device Configuration.

Note
For the purposes of this document, the configuration instructions that follow apply to creating a device template from scratch, not starting with a cloned default template.

Perform Device Configuration

Create a network policy and device template.

Under **Device Configuration**, you can choose to override settings made under **Common Settings** in a network policy. The Switch Template Override feature allows customers to create and manage switch templates based on common settings for the Switch Engine, ExtremeXOS, Fabric Engine, and VOSS platforms.

These common settings include STP, MAC Locking, IGMP, Extreme Loop Recovery Protocol Settings (ELRP), MTU, PSE, and Management Interfaces (Switch Engine only). The default values for these settings are defined within the common switch settings for each platform type. When you create a new switch template and enable the override option, you can customize device configuration settings that will override the network policy switch common settings. If the override option is disabled, the device configuration will be inherited by the network policy common settings.

Note
If this is a switch stack, repeat this task for each device in the stack.

Use this task to configure device configurations for a specific switch template.

1. Go to **Configure** > **Network Polices** > **the existing network policy** > **Switching/ Routing** > **Switch Settings** > **Switch Templates** and select the template for the device model.
2. Ensure that **Enable Override Policy Common Settings** is set to **ON** to make any changes to device configuration.
3. For **STP Configuration**, see Configure STP Settings on page 31.
4. For **IGMP Settings**, toggle to **On** and make the following selections:
   - **Enable immediate leave**: Instructs the switch to remove a multicast host from the multicast forwarding table immediately upon receipt of a leave-group-membership message.
   - **Suppress redundant IGMP membership reports to optimize traffic**: Suppresses redundant IGMP membership reports from multiple hosts on a subnet. The switch sends a single report to the IGMP router, reducing traffic.
5. For **MAC Locking Settings**, select to control the forwarding database for learned MAC address entries on a port.

   Note
   MAC Locking must also be enabled on a per-port basis.

6. For **Extreme Loop Recovery Protocol Settings**, select **Configure ELRP client periodic packet transmission for VLAN(s) assigned to port type to detect and prevent loops. ELRP must also be enabled within switch template.**

   This option enables an ELRP client and disables a port when a loop is detected on the applied access or trunk VLANs assigned to the port type.

   Note
   ELRP must also be enabled within the switch template.

   Or

   Select **Configure ELRP Port Duration** to enable the ability to define how many seconds a port stays disabled before re-enabling when ELRP detects a loop (15-600 seconds).
7. For **DHCP Snooping Settings**, toggle to **On**, and make the following selection:
   - **Drop Rogue DHCP Packets Action**: Ports configured as **Trusted** will not apply drop action.

   Note
   If VLAN attributes has enabled DHCP Snooping settings, then the VLAN attributes will override the switch template.
8. For **MTU Settings**, enter a maximum transmission unit value for Ethernet interfaces.

   The MTU value determines the largest packet size that can be transmitted through your system.
9. For **PSE Settings**, toggle to **On** to configure maximum power thresholds to generate alerts to ExtremeCloud IQ about exceeding maximum power levels.
10. For **Management Interface Settings** (Switch Engine devices only), select one of the following options:
    - **VLAN Interface**: Select when the management interface is to be supplied by the management VLAN.
      - **Management VLAN**: Enter the VLAN to be used by the switch.
      - **Management IP Settings**: Select to enable DHCP on this interface.

Proceed to Port Configuration.

Configure STP Settings

Use this task to configure Spanning Tree settings.

1. For STP Mode, select one of the following:
   - **STP**: Uses a single spanning tree without regard to VLANs. After convergence, only the root bridge sends configuration BPDUs, and other switches only relay those BPDUs.
   - **RSTP (Rapid STP)**: Uses a single spanning tree without regard to VLANs. After convergence, all switches send BPDUs every two seconds in the event of a physical link failure.
   - **MSTP (Multiple STP)**: Can map a group of VLANs into a single multiple spanning tree instance (MSTI). MSTP uses BPDUs to exchange information between spanning-tree compatible devices, to prevent loops in each MSTI by selecting active and blocked paths. Configure MSTP settings.
2. Select an **STP Bridge Priority** from the drop-down list.

   Every switch taking part in spanning tree has a bridge priority. The switch with the lowest priority becomes the root bridge. If there's a tie, the switch with the lowest bridge ID number wins. The ID number is typically derived from a MAC address on the switch.
3. Set the following **STP Timers** parameters:

   Forward Delay: The time the switch spends in the listening and learning state.

   Max Age: The maximum time before a bridge port saves its configuration BPDU information.

Port and VLAN Configuration

You can configure switch ports in bulk or on an individual basis. If you choose bulk configuration, you can use existing port types or create new ones. You can also configure multiple ports at the same time. The following rules apply to bulk port configuration for:

- Copper ports must be of the same speed type.
- Selected ports with different maximum speeds can now be part of the same aggregation.

Warning messages appear if your port selections do not follow these rules.

The following configuration options are available:

- **Port Details**
- **Instant Secure Port**
- **Port Settings**
- **STP**
- **Storm Control**
- **MAC Locking**
- **Voice**
- **ELRP**

- **PSE**
- **VLAN Attributes**

Note

- BPDU Restrict and BPDU Restrict Recovery settings are found within the STP settings.
- For switch stacks, repeat all applicable port configuration steps for each device in the stack.

Configure Ports in Bulk

Before you begin, create a Switch template.

Use this task to create ports in bulk.

1. Go to **Configure** > **Network Policies** > **existing switch template** > **Configuration** > **Port Configuration**, then under **Configure Ports in Bulk**, select one or more ports and select **Assign** > **Create New**.
2. If this template applies to a 5570 or 5520 switch, you can define VIM Port Channelization ports.
   a. Under **Configure Ports in Bulk**, choose **Select VIM**.
   b. For a 5570 switch, select **VIM-6YE** or **VIM-2CE**.
   c. For a 5520 switch, select **VIM-4X**, **VIM-4XE**, or **VIM-4YE**.

   Note
   If you need to create different templates for different VIMs on the same switch model, you can create a classification rule so that different devices have the same template with different VIM options. For more information about classification rules, see Configure a Classification Rule on page 37.

   d. Select one or more of these VIM ports and continue to Step 3.
3. Configure the port settings.

Table 6: Settings for Port Bulk Configuration

Setting	Description
Port Type	Enter a **Port Type** name.
Port Status	Toggle **Port Status On** or **Off**.
Auto-Sense	Toggle **Auto-Sense On** or **Off** (Fabric Engine device only). **Auto-Sense** detects connected device types and automatically configures specific port settings. Certain port settings are not configurable.

Table 6: Settings for Port Bulk Configuration (continued)

Setting	Description
Port Usage Settings	Select one of the following port types: • **Auto-Sense Enabled**: The only option if previously selected. (Fabric Engine device only) • **Access Port**: Ports connected to individual hosts such as printers, servers, and end-user computers. • **Trunk port (802.1Q VLAN Tagging)**: Ports connected to network forwarding devices that support multiple VLANs on trunk ports. • **Phone with a Data Port**: Ports connected to IP phones, and optionally, to computers cabled to the phones.
Access Port	For an **Access Port**, select an existing VLAN or select the add icon to add a new one. Tag the VLAN to a particular access port to control and monitor switch traffic. To add a new VLAN, see Configure VLAN Settings on page 36. Note: For Switch Engine the **none** keyword is available for entry as a VLAN. Alternatively, a common object VLAN can be created with the VLAN ID using the **none** keyword. Using **none** removes the assignment of the native VLAN from the port.
Trunk Port	For a **Trunk Port**, select an existing **Native VLAN** or select the add icon to add a new one. The native (untagged) VLAN is the VLAN assigned to frames that do not have any 802.1Q VLAN tags in their headers. By default, Extreme Networks devices also use VLAN 1 as the native VLAN. To add a new VLAN, see Configure VLAN Settings on page 36. Note: For Switch Engine the **all** keyword can be used. Using **all** will automatically tag VLAN IDs to the ports that are also defined within other *port types* assigned to the Switch Engine device.
Allowed VLANS	For **Allowed VLANS**, enter a specific number or leave the **All** default.

Table 6: Settings for Port Bulk Configuration (continued)

Setting	Description
Phone with Data Port	For **Phone with Data Port** (Voice): This option offers additional CDP advertisement options within VLAN settings. • **Voice VLAN** (tagged) and **Data VLAN** (untagged) can be specified under the **VLAN Settings** tab. • **LLDP Voice VLAN Options** are disabled by default. When enabled, the default behavior is to also to **Enable LLDP advertisement of 802.1 VLAN ID and port protocol of Voice VLAN**. • If checked, select a value for **Enable LLDP advertisement of med Voice VLAN DSCP Value**. • If checked, select a value for **Enable LLDP advertisement of med Voice Signaling VLAN DSCP Value**. Note: LLDP MED Capabilities are available for Switch Engine for any port usage type. • **CDP Voice VLAN Options** is disabled by default. When enabled, the default behavior is to also enable the following: ◦ **Enable CDP advertisement of Voice VLAN** ◦ **Enable CDP advertisement of power available** Note: If the LLDP/CDP options are enabled, then CDP/LLDP options within **Transmission Settings** are automatically enabled.
Transmission Settings	Under **Port Settings**, for **Transmission Settings**, configure the following: • **Transmission Type**. Valid values are: ◦ **Auto**. Selecting **Auto** causes the switch to negotiate the best possible duplex mode possible with the connected device. ◦ **Full-Duplex**. Selecting **Full-Duplex** forces the switch to communicate with the connected device using full-duplex communication. ◦ **Half-Duplex**. Selecting **Half-Duplex** forces the switch to communicate with the connected device using half-duplex communication. • **Transmission Speed**: Choose the speed the port uses to communicate with the connected device. • **LLDP Transmit**: Enables the switch to transmit LLDPDU frames. • **LLDP Receive**: Enables the switch to receive LLDPDU frames. • **Enable CDP**: Enables the switch to receive and parse the information within Cisco CDP frames. • **Client Reporting**: Enables collection and reporting of learned MAC addresses for the port.

Table 6: Settings for Port Bulk Configuration (continued)

Setting	Description
STP	For **STP**: • **STP Status**: Toggle **ON** to enable STP for the port. • **Edge Port**: Connects to a user terminal or server, instead of other switches or shared network segments. A port configured as an edge port will not cause a loop upon network topology changes. • **BPDU Protection** (Switch Engine devices only): Use the drop-down list to change BPDU protection to guard or filter status. ◦ **Guard** - Controls whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology. ◦ **Disabled** - Turns off BPDU Protection. • Toggle the switch to **On** to enable **BPDU Restrict**. • For **BPDU recovery timeout**, input a time between 60-600 seconds. • **Priority**: When this port is an STP edge port, select a port priority for STP from the drop-down list. • Enter the **Path Cost** (bandwidth) for this port. Note: The port is re-enabled automatically when time expires.
Storm Control	For **Storm Control**: • **Broadcast**: Select to include traffic that is forwarded to all destinations simultaneously. • **Unknown Unicast**: Select to include traffic whose destination address does not appear in the forwarding database. • **Multicast**: Select to include traffic whose destination is a multicast address. • **Thresholds**: **Packet Based** is the default. • **Rate Limit Type**: **PPS** (packets per second) is the default. • **Rate Limit Value**: Enter when the switch should discard traffic of the selected types.
MAC Locking	For **MAC Locking**, enable the per port type with the option to specify **Maximum First Arrival Limit** and specify the **Link Down Action**. By default, **Link Down Action** is set to clear first arrival MACs, with the option to retain MACs. We also have the option to take action when MACs are aged out. Note: MAC Locking must also be enabled on a per-port basis within a port type.

Table 6: Settings for Port Bulk Configuration (continued)

Setting	Description
ELRP	For **ELRP Enabled**, toggle to **ON** to enable ELRP per port (disabled by default). Switch Engine switches support the ability to configure **ELRP Exclude** on a port type which will not allow ELRP to disable the port when ELRP packets are received.
PSE	For **PSE**, select an existing profile or select the plus sign to add a new one. For more information, see Configure PSE Parameters on page 39
POE Status	Toggle **POE Status** to the required setting.

4. Select **Save Port Type**.

Configure VLAN Settings

Use this task to configure VLAN settings on the **Port Configuration** page.

1. Select +.
2. Type a **Name** for the new VLAN object.
3. Enter the VLAN ID for this VLAN.

   Typically, the default VLAN ID is 1.

   > Note
   > You can also create a VLAN ID with a value of `none`. `None` clears the native VLAN from a port. (Switch Engine device only)

4. Enable **DHCP Trusted Port**.
5. Select the **Apply VLAN to devices for classification** check box to create VLANs that you can apply to specific devices based on their location.
6. Select +.
7. Type the new **VLAN ID**, and then select **Add** to add it to the VLAN table.
8. Under **Classification Rules** in the VLAN table, select an existing classification rule, or select the add icon to add a new rule.

   See Configure a Classification Rule on page 37 for more information.
9. Select **Link**.
10. Type a **Name** for the classification rule.

    For easier tracking, you might want to add the locations and device models using this VLAN classification rule (for example, VLAN-AP230-Sunnyvale).
11. (Optional) Type a **Description**.

    Although optional, descriptions can be helpful when you are troubleshooting your network.
12. Select the plus sign to choose the device location.

13. Assign your VLAN profile based on the location of managed devices.

    > Note
    > When selecting a location, drill down to the level where the devices are located. For example, if the devices are located on the floor of a building, select that specific floor.

14. Choose **Select**.
15. Select **SAVE VLAN**.

Configure a Classification Rule

You can create classification rules as part of a network policy or as a common object.

Classification rules are used for consistency across multiple switch templates. Before you create a classification rule, create the switch templates that will associate with the rule:

1. Create a second template of the same device type that uses the same device SKU. For more information, see Configure a Device Template on page 28.
2. Clone the first switch template. For more information, see Configure a Device Template on page 28.

- Configure **Device Location** rules to assign different switch templates or VLANs within a port type to switches assigned to different locations.
- Configure **Cloud Config Groups** (CCGs) to assign a match type that contains or does not contain a specific selection of switches.
- Configure **IP Address** classification rules to assign a match type that contains or does not contain a specific IP address associated with switches.
- Configure **IP Subnet** classification rules to assign a match type that contains or does not contain a specific IP subnet associated with switches.
- Configure **IP Range** classification rules to assign a match type that contains or does not contain a specific IP range associated with switches.

Use this task to create classification rules associated with a network policy. ExtremeCloud IQ supports multiple classification rules for DNS servers, VLANs, RADIUS servers, device templates, user groups, and private client groups (PCGs).

1. Go to **Configure** > **Network Policies**.
2. Select a device.
3. Go to **Configuration** > **Port Configuration**.
4. In the **Configure Ports Individually** section, select + to create a new port.
5. In the VLAN tab, select +.
6. Add a Name, VLAN ID, and select the **Apply VLAN to devices for classification** check box.
7. Select **Add**.

   The new VLAN is added to the VLAN table below.
8. Select + in the **Classification Rules** column to add a new classification rule.
9. Enter a name for the rule.

10. (Optional) Enter a description.
11. Select + and the rule type to configure settings.

Table 7: Classification Rules Settings

Setting	Description
Device Location	If you selected **Device Location**, perform the following steps: a. Open each location level until you reach the level where the device resides. b. Choose **Select**. The location is displayed in the Classification Rule table.
Cloud Config Group	If you selected **Cloud Config Group**, perform the following steps: a. Select the **Match Type**. b. Select an existing group from the drop-down list. To add a new group, select the add icon. For more information, see Add a Cloud Config Group on page 39.
IP Address	If you selected **IP Address**, perform the following steps: a. Select the **Match Type**. b. Select an existing IP address from the drop-down list. To add a new IP address, select the add icon. c. Select **Save IP**.
IP Subnet	If you selected **IP Subnet**, perform the following steps: a. Select the **Match Type**. b. Select an existing IP subnet from the drop-down list. To add a new IP subnet, select the add icon. c. Select **Save Subnet**.
IP Range	If you selected **IP Range**, perform the following steps: a. Select the **Match Type**. b. Select an existing IP range from the drop-down list. To add a new IP range, select the add icon. c. Select **Save IP**.

12. Use the up and down arrows in the **Order** column to define the order in which the location, cloud config group, IP address, IP subnet, and IP range objects appear.

    These objects are considered using a top-down, first-match, stop-on-match method, so if a device is a member of more than one matching object for an element, only the first match is applied.
13. Select **Save Rule**.

Add a Cloud Config Group

Cloud config groups enable administrators to create network-level policies that can be replicated for multiple network roll-out scenarios. When you choose Cloud config groups as your VLAN classification rule use this task to create a new group from the **Port Configuration** page.

1. Select + and enter the group name.
2. (Optional) Enter a description.
3. Search for and select devices to have their host names display in the **Selected Devices** field.

   Note
   You can also import a comma-separated-values (CSV) file including the host names, serial numbers, and optional MAC addresses of other devices.

   a. Select **Import**.
   b. Select the CSV file or drag the CSV file to the **Import Cloud Config Group Members** window.
   c. Select **Submit**.
4. Select **Save Cloud Config Group**.

Configure PSE Parameters

Use this task to configure PSE settings, which define how ports manage the power that they supply to devices.

1. Select the add icon.
2. Enter a name.
3. For **Power Mode**, select **802.3af** or **802.3at**.

   802.3af (PoE) can deliver 15.4 watts over Cat5 cables. **802.3at (PoE+)** can deliver up to 30 watts over Cat 5 cables with 25.5 watts available to devices.
4. For **Power Limit**, limit the available PoE power to a level lower than the maximum allowed by the power mode.
5. Select a **Priority** from the drop-down list:

   Low: If the total powered device (PD) power consumption exceeds the PSE power budget, power output is modified to bring the total consumption back to within the PSE power budget.

   High: When the total PD power consumption exceeds the PSE power budget, power output is modified only after ports with low priority PSE profiles are regulated.

   Critical: When the total PD power consumption exceeds the PSE power budget, power output is shut down last.
6. (Optional) Enter a description.
7. Select **Save**.

Aggregate Ports

This task applies to Switch Engine devices only. You can group individual ports into aggregate ports on 24- and 48-port switches by selecting two or more ports of the same type on the switch template.

1. Select the ports you want to aggregate and under **Configure Ports in Bulk**, select **Assign** > **Advanced Actions** > **Aggregate**.
2. Add or remove ports from the LAG.
3. Select a **Master Port**.
4. For **Port Load Balancing**, select the appropriate hash algorithm.
5. Select **Save Port Type**.

> Note
> You can change the LAG port type after a port has been assigned to a LAG, without having to delete and recreate the LAG.

Configure Ports Individually

Create or modify a Switch Template, then select the **Port Configuration** tab.

Use this task to create an individual port from an existing default port type.

1. Select a **Port Type** from the drop-down menu.
   - **Auto-sense** (Fabric Engine devices only): Detects connected device types and then automatically configures specific port settings. Certain port settings are not configurable when Auto-sense is enabled.
   - **Access Port**: Ports connected to individual hosts such as printers, servers, and end-user computers.
   - **Disabled Port** (N/A)
   - **Onboarding Port** (N/A)
   - **Trunk Port** Ports connected to network forwarding devices that support multiple VLANs on trunk ports.
2. Follow the configuration steps in Configure Ports in Bulk on page 32.

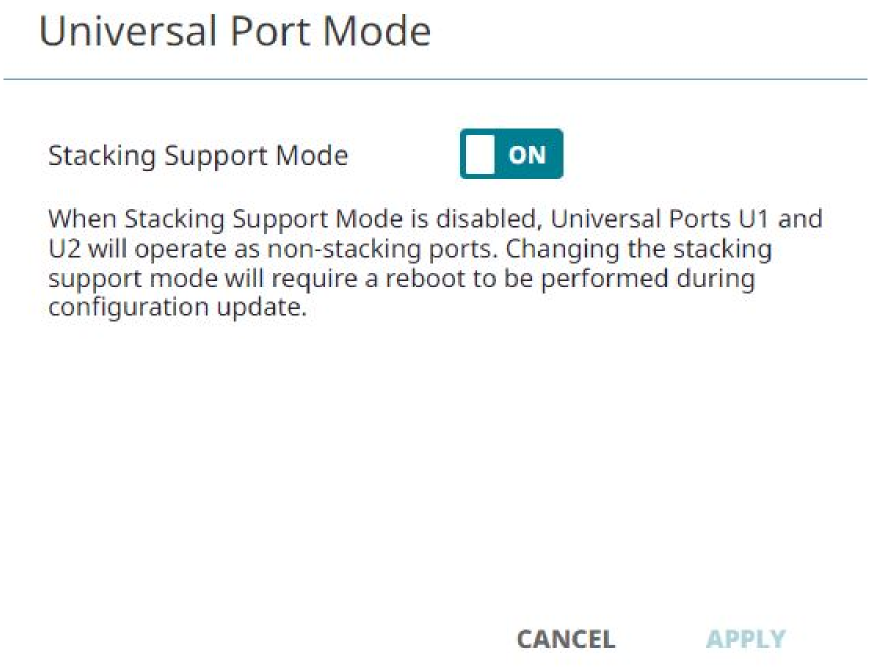
> Note
> You can only aggregate ports when you configure in bulk.

3. After you save the new port, it displays in the table.
4. Select the edit icon to make changes.
5. Remember to save your changes.

Universal Port Stacking Support Mode

Switch Engine 4000 Series hardware allows for the configuration of Universal Port Stacking Support Mode. When Stacking Support Mode is disabled, Universal Ports U1 and U2 operate as non-stacking ports. Once stacking ports are no longer defined as stacking, then all ExtremeCloud IQ supported port configurations apply, including configuration by port type and configurations associated with ports such as Instant Port/Instant Secure Port configurations.

Note
Changing the stacking support mode requires a reboot to be performed during configuration update.



When Stacking Support Mode is disabled, Universal Ports U1 and U2 will operate as non-stacking ports. Changing the stacking support mode will require a reboot to be performed during configuration update.

Figure 1: Universal Port Stacking Support Mode

To Enable or Disable Universal Port Stacking Support Mode:

1. Go to **Configure** > **Network Policies**, to edit or create a new policy.
2. Select **Switch Template**.
3. From the Details page, select **Switching** > **Port/VLAN Configuration**.
4. Select ✎ beside the Universal Ports.
5. Choose your Stacking Support Mode with the **Toggle**.
6. If the device is a Switch Engine 4120 series, additional channelization options appear. Select the Channelization options for both Universal Ports.

   Note
   The default channelization option for 4120 models is 1x100G.

7. Select **Apply**.

   Note
   Universal Port Stacking Support Mode can also be configured at the device-level, within the **Port / VLAN Configuration** page. Device level configuration will override the template configuration.

Configure Advanced Settings

Currently, switch onboarding and firmware/configuration updates require manual steps. Use this task to enable the firmware upgrade option, as well as auto config push, during switch onboarding within the defined template for the switch assigned to the associated network policy. Each can be enabled/disabled together or independently.

1. Go to **Configure** > **Network Policies** > **existing switch template** > **Configuration** > **Advanced Settings**.
2. (Optional) Toggle **ON Upgrade device firmware upon device authentication**.
   a. Select your preferred update option:
      - **Upgrade firmware to the latest version**
      - **Upgrade to the specific device firmware version**

      Note
      If the selected firmware is already at the latest or defined firmware, then the upgrade device firmware action will not occur.
3. (Optional) Toggle **ON Upload configuration automatically**.

   Note
   If upgrade and config push are selected, then the upgrade happens first.

   a. Check **Reboot and revert Extreme Networks switch configuration if IQAgent is unresponsive after configuration update.** check box.

Configure Supplemental CLI

To use the supplemental CLI tool, navigate to **Global Settings** > **VIQ Management**, and enable **Supplemental CLI**.

Use this task to update CLI commands for multiple devices simultaneously from ExtremeCloud IQ. You can save Supplemental CLI objects containing CLI commands, and the commands can then be automatically updated for devices each time you update the network policy. If a supplemental CLI is appended to a delta configuration and the supplemental CLI portion fails device update, only the supplemental CLI will be regenerated for subsequent device updates.

Note

- Limit CLI commands to configuration commands. Exclude **`Show`** or other commands used to display information.
- Do not use Supplemental CLI commands to configure any settings set via the ExtremeCloud IQ GUI as that creates a configuration sync conflict that will result in future **`Device Update Failed`** errors.
- These commands work as a delta mechanism. Every new Supplemental CLI update must only include new commands that you want to run, not ALL commands that you want to have present on the switch at startup. Re-running some commands after already applied can cause future **`Device Update Failed`** errors.

1. Toggle **Supplemental CLI On**.
2. Select existing supplemental CLI objects using the drop-down list next to **Re-use Supplemental CLI Settings**.
3. To add a new supplemental CLI object:
    a. Enter a name.
    b. (Optional) Enter a description.
    c. Enter the CLI commands.
        - Enter multiple CLI commands, one command per line.
        - Use CLI Commands that contain IP and VLAN objects: **`${ip:ip_object_name}`** and **`${vlan:vlan_object_name}`**.
4. Select **Save** and perform a complete configuration update each time you append commands to device configurations.

Configure Management Server Settings

1. To configure policy settings for a Management Server, select the server under **Policy Details** > **Policy Settings**:
    - DNS Server
    - NTP Server
    - SNMP Server
    - Syslog Server
2. Configure the management server and save your changes.
3. Select **Next** to deploy the network policy.

    See also, Deploy a Network Policy on page 51.

Configure a DNS Server

The Domain Name System (DNS) translates human-friendly domain names into IP addresses. You can supply external DNS server IP addresses or use routers to provide proxy DNS services for every local network under their control. The DNS service transparently proxies DNS requests and responses to and from internal or external DNS servers. Use this task to configure a DNS server.

> Note
> Limit the number of DNS servers in your configuration to less than 8.Switch Engine devices can have only 8 DNS servers configured across both VR-Default and VR-Mgmt. Each defined DNS server adds an entry for both VR-Default and VR-Mgmt (a maximum of 4 configured servers in ExtremeCloud IQ fills all 8 slots). The switch can have also pulled DNS Server configuration via DHCP, creating further limitations. If a configuration push tries to configure a 9th DNS server, a `Device Update Failed` error occurs.

1. Choose to use an existing DNS Server Setting, or proceed to the next step.
2. Enter a name for the server.
3. (Optional) Enter a **Domain Name** and **Description**.
4. Select an existing IP address for the device to configure as a DNS server.

   If you do not see the IP address or host name that you need, use the add icon. You can add up to three servers. The first entry becomes the primary server. The secondary entry becomes the secondary server, and so forth. Change their order with the **Order** arrows.
5. To **apply DNS servers to devices via classification**, select an existing classification rule or select the add icon to add a new rule.

   To add a new rule, see Configure a Classification Rule on page 37.
6. Select **Save DNS Server**.
7. If you are ready to deploy the network policy, select **Next** or continue to the next Management server.

Configure an NTP Server

Extreme Networks devices typically obtain the time and date for their internal clocks from an NTP server. Use this task to configure an NTP server.

1. Go to **Configure** > **Network Policies**.
2. Select an existing network policy, and then select ✎, or select +.
3. Or and then select ✎, or select + to create a new policy.
4. From the **Policy Settings** menu, select **NTP Server**.
5. Toggle the **NTP Server** setting to **ON**.
6. (Optional) To use existing NTP server settings, choose an NTP object from the ☰ menu.
7. Configure NTP Server Settings on page 45.
8. To add a new NTP server to the list, select +.
   a. To use an existing NTP server, select it from the ☰ menu.
   b. To add a new NTP server, select +, and then select **IP Address** or **Host Name**.
   c. Type a **Name** for the new IP object.

   d. (Optional) If you want to change your previous selection, select **IP Address** or **Host Name** from the menu.
   e. Select **SAVE IP OBJECT**.
   f. Select **ADD**.

   ExtremeCloud IQ accesses NTP servers in order, from the top down. Use the up and down arrows to rearrange them if necessary.

9. If you want to use classification, select **Apply NTP servers to devices via classification**.
10. Select **SAVE NTP SERVER**.
11. If you are ready to deploy the network policy, select **Next** or continue to the next Management server.

NTP Server Settings

Table 8: Settings for NTP server profiles

Setting	Description
Name	Type a **Name** for the NTP server.
Domain Name	(Optional) Type a **Domain Name** for the NTP server.
Synchronize the device clock with the NTP servers.	1. Type the **HiveOS Device Sync Interval** value (in minutes). 2. From the **Switch Sync Interval**, select a value.

Configure an SNMP Server

Simple Network Management Protocol (SNMP) exchanges information between network devices and one or more central network management stations (referred to in ExtremeCloud IQ as an SNMP server). The devices send traps, which are unsolicited messages, to the management stations on UDP port 162 when events of note occur. Management stations also query monitored devices to check their operational status. The queries are in the form of get commands that management stations send on UDP port 161.

This task is part of the network policy configuration workflow. Use this task to configure an SNMP server.

1. Go to **Configure** > **Network Policies**.
2. Select an existing network policy, and then select ✏, or select + to create a new policy.
3. From the **Policy Settings** menu, select **SNMP Server**.
4. Toggle the **SNMP Server** setting to **ON**.
5. (Optional) To use existing SNMP server settings, choose an SNMP server from the ☰ menu.
6. To add a new SNMP server, select +, and then select **IP Address** or **Host Name**.

   You can add up to three SNMP servers to the profile.

7. Configure SNMP Settings on page 46.
8. (Optional) If you want to change your previous selection, select **IP Address** or **Host Name** from the menu.
9. Select **SAVE IP OBJECT**.
10. Select **ADD SNMP SERVER**.
11. If you want to use classification, select **Apply SNMP servers to devices via classification**.
12. Select **SAVE SNMP SERVER**.

SNMP Settings

Table 9: Settings for SNMP servers

Setting	Description
Name	Type a **Name** for the server.
Description	(Optional) Type a brief **Description** for the server. Although optional, entering a description is helpful for troubleshooting and for identifying the server.
SNMP Contact	Type the **SNMP Contact** contact information for the SNMP server administrator, so they can be contacted if necessary. This can be an email address, telephone number, physical location, or a combination.
Disable to Send traps over CAPWAP	Clear the check box for **Disable to Send traps over CAPWAP** to enable devices to send trap information (events and alarms) to ExtremeCloud IQ over a CAPWAP connection, or leave the box checked to disable this action.
SNMP Server	Select an SNMP server from the drop-down list. Choose the IP address or host name object for the SNMP server or servers that will access the devices. To permit management access from a single SNMP server, choose an IP address or host name that defines only that server. To permit management access from an entire subnet, choose an IP address or host name that defines that subnet. If you do not see the IP address or host name that you need, select **+** and define one.
Version	From the drop-down list, select the version of SNMP that is running on the management station that you intend to use.

Table 9: Settings for SNMP servers (continued)

Setting	Description
Operation	Select the type of activity to permit between the specified SNMP management station and the devices in the network policy to which you will assign this profile. Options include: • **None**: Disable all SNMP activity for the specified management station. • **Get**: Permit GET commands sent from the management station to a device to retrieve MIBs. • **Get and Trap**: Permit the reception of GET commands from the management station and the transmission of traps to the management station. • **Trap**: Permit devices to send messages notifying the management system of events of interest.
Community	For SNMP V2C and V1, enter a text string that must accompany queries from the management station. The community string acts similarly to a password, such that devices accept queries only from management stations that send the correct community string.

Configure a Syslog Server

You can configure syslog server profiles for device log entry storage. The syslog administrator can then sort messages by facility and see all the ones relating to Extreme Networks devices. The administrator can further sort the messages by IP address and by severity.

> Note
> Using NTP to synchronize the time stamp on messages from all syslog clients can ensure that all messages reported to the syslog server appear in their proper chronological order. Otherwise, it can be very difficult to interpret a series of events affecting multiple network devices, such as reconnaissance probes and network intrusion exploits. To further ensure synchronicity, all syslog clients should use the same NTP time server. See Configure an NTP Server on page 44.

1. Go to **Configure** > **Network Policies**.
2. Select an existing network policy, and then select ✎, or select + to create a new policy.
3. From the **Policy Settings** menu, select **Syslog Server**.
4. Toggle the **Syslog Server** setting to **ON**.
5. (Optional) To use existing syslog server settings, choose a syslog server from the ☰ menu.
6. Configure the Syslog Server Settings on page 48.

7. Select the plus sign to add a syslog server.
8. Select an existing syslog IP Address or host name, or use the add icon to create a new IP Address or host name.
9. From the drop-down list, choose the minimum severity level of messages that devices will send to the syslog server.

   Devices send syslog messages for the severity level you choose, plus messages for all of the more severe levels above it.
10. To add another syslog server, select the add icon, and repeat the previous steps.

    Note
    Use the up or down arrows to reorder the list of syslog servers in the table.

11. To **apply Syslog servers via classification**, select an existing classification rule or select the add icon to add a new rule.

    To add a new rule, see Configure a Classification Rule on page 37.
12. Select **Save Syslog Server**.

Syslog Server Settings

Table 10: Settings for Syslog servers

Setting	Description
Name	Type a **Name** for the syslog server.
Description	(Optional) Type a **Description** for the syslog server. Although optional, entering a description is helpful for troubleshooting and for identifying the server.
Syslog Facility	
IQ Engine Syslog Facility	Select an **IQ Engine Syslog Facility** to categorize messages sent to syslog from IQ Engine devices. Because syslog servers can receive messages from many types of network devices, such as routers, firewalls, mail servers, you can designate one of the twelve syslog facilities reserved for local use—Auth, Authpriv, Security, User, and Local0 to Local7—to mark messages from all the devices to which you apply this management service set.
Non-IQ Syslog Facility	Select a **Non-IQ Syslog Facility** to categorize messages sent to syslog from non-IQ Engine devices.

Table 10: Settings for Syslog servers (continued)

Setting	Description
Syslog Group	Select the arrow to expand the **Syslog Group** section, and use the menus to select the log level for each category. • Emergency • Alert • Critical • Error • Warning • Notification • Info • Debug Syslog groups organize messages by category and limit the number of messages sent based on severity level. APs do not send messages that are below the assigned level to the syslog server.
Syslog servers are on the same internal network as the reporting Extreme Networks devices (for PCI DSS compliance)	If you must make PCI DSS compliance reports, select the check box. If the servers are on an external network outside the firewall, clear the check box.
Enable hostname in syslog headers	To add the hostname to the headers for all syslog messages, select the check box.

Configure LLDP/CDP Policy Settings

This task is part of the network policy configuration workflow. Use this task to configure **LLDP/CDP** policy settings for a network policy.

1. Select an existing network policy, and then select ✎, or select + to create a new policy.
2. From the **Policy Settings** menu, select **LLDP/CDP**.
3. Toggle the **LLDP/CDP** setting to **ON**.
4. (Optional) To use existing LLDP/CDP settings, choose an LLDP/CDP object from the ☰ menu.
5. Configure the settings.

   See LLDP and CDP Settings on page 50.
6. Select **SAVE**.

LLDP and CDP Settings

Table 11: Settings for LLDP and CDP

Setting	Description
Name	Type a **Name** for the new LLDP/CDP object.
Description	(Optional) Type a **Description** for the new LLDP/CDP object. Although optional, entering a description is helpful for troubleshooting and for identifying the LLDP/CDP object.
Enable LLDP on access ports	Select the check box to permit LLDP on access ports. Note: LLDP is enabled on other port types by default.
Enable receive only mode.	Select the check box to permit devices to receive, cache, and display LLDP advertisements from other devices, but to not advertise their own data.
LLDP entries to cache	(IQ Engine Only) Type the maximum number of LLDP entries from neighboring network devices that a device can store in its cache.
Neighbors keep Extreme Networks advertisements for	Type the number of seconds for which neighboring devices retain LLDP advertisements. Increase the time while troubleshooting a network issue and decrease it if you need to reduce overall network traffic.
Advertisements Interval	Type the number of seconds between LLDP advertisements sent to neighboring network devices.
Timer Hold	Type a multiple of the advertisements interval. (EXOS/ Switch Engine, VOSS/Fabric Engine, SR22XX/23XX, Dell)
Max power for LLDP advertisements	Select **Use the default max power in IQ Engine** to use the maximum power level that devices can request in LLDP advertisements.
LLDP Initialization Delay Time	Type the length of time that you want the interface to wait before initializing LLDP.
Fast start repeat count	Type the number of advertisement LLDP frames to send when the connected device (such as an IP phone) starts up or is discovered.
CDP (Cisco Discovery Protocol)	Toggle CDP **ON** to enable devices to receive and cache CDP advertisements. Note: You can enable LLDP and CDP concurrently. CDP is a proprietary Data Link Layer protocol developed by Cisco Systems.
Enable CDP on access ports.	Select the check box to permit CDP on access ports. By default, CDP is enabled on other port types.
CDP entries to cache	Type the maximum number of CDP entries that a device can store in its cache.

Deploy a Network Policy

Before you begin, create a complete network policy configuration.

When you create a new network policy or make changes to an existing policy, the final step is to push the policy to the devices that will operate under the policy. ExtremeCloud IQ pushes all configuration uploads as complete uploads. This requires devices to reboot and activate the new configurations.

1. Go to **Configure** > **Network Policies**.
2. Select a policy that is ready to deploy.
3. Select the **Deploy Policy** tab.
4. To upload a network policy to all of the devices in the devices list, select the check box in the top left side of the table header.

   This automatically selects the check boxes for all of the devices.
5. Select **Upload**.
6. To upload your network policy to specific devices only, select the check box for those devices, and then select **Upload**.

   You can filter the devices displayed with the **Assigned**, **Eligible** and **Filtered** options.
7. In the **Device Update** window, select the type of update (**Delta** or **Complete**), whether to update IQ Engine and Extreme Networks switch images, and the activation times for the updated devices.
8. You can select **Reboot and revert Extreme Networks switch configuration if IQAgent is unresponsive after configuration update** under **Update Network Policy and Configuration**.

   Select this option to revert the switch configuration if the device update causes a disconnect between the switch and ExtremeCloud IQ. The switch reboots and reverts to its previous configuration, which enables you to correct any configuration issues and perform a new device update.
9. Select **Perform Update**.

Instant Port Profiles

Instant Port Profiles (IPP) in ExtremeCloud IQ is an automated approach to configuring switch ports based on the connected devices. IPP streamlines the management of network-connected devices, such as access points (AP), security cameras, and VoIP devices by dynamically provisioning the appropriate port configuration automatically.

Some common use cases for IPP are:

- Configure VoIP phones in a dedicated VLAN.
- Configure guest devices in a guest VLAN.
- Combine IoT devices with VoIP in a dedicated VLAN.
- Automate device placement into the correct VLAN for devices with port changes.
- Provision tagged VLANs for devices such as connected AP.

IPP provides the capability to assign specific port profiles to client devices automatically, eliminating the need for manual port configuration by an administrator. When a user connects a device to a switch port, IPP allows the device to identify itself to the network system by its properties. Subsequently, IPP provisions the assigned port configuration, giving the device access to the network.

Create an IPP within the Switching Section of a Network Policy, assign IPP to ports within a switch template, or within the port configuration of a switch at device level configuration.

Some benefits of IPP are:

- Reduced operational costs by automating the configuration of devices.
- Improved security by ensuring that devices are placed in the correct VLANs.
- Improved performance by configuring broadcast suppression for specific devices or device types.

Instant Port Profiles empower administrators to preconfigure switch ports with VLANs, storm control. These configurations are applied automatically when a connected device matches predefined conditions in a profile. Conditions are based on:

- MAC Address (partial or exact matches)
- LLDP Information (system type, MAC)

  IPP allows for custom definitions (device types) and match criteria, enabling automatic VLAN assignment and storm control parameters. IPP offers more granular control over the network configuration based on specific device types.

Device Types and Match Criteria

- Device Types: Custom definitions for types of wired devices.
- Match Criteria:
  - MAC Learning
  - LLDP Src MAC
  - LLDP Capability
  - LLDP MAC + Capability

When a match occurs, action parameters specified in the profile are automatically configured by the system, such as managing devices that move between different switch ports and switches while requiring consistent VLAN and port configurations.

Important
Tagged packets cannot be classified by IPP. For devices expected to send tagged data frames, use only LLDP (Link Layer Discovery Protocol) match configuration.

Wired Device Types

Each wired device type includes configuration that is dynamically applied to the port based on the match criteria. Dynamic configurations may include VLAN assignment and storm control parameters. VLAN configurations assign untagged VLANs based on the client's MAC address or assign tagged VLANs to the port.

Non-Forwarding VLAN

Instant Port Profiles also use a non-forwarding VLAN, defined by the customer. This VLAN is used to initially detect MAC addresses on a switch port, preventing traffic forwarding for untagged traffic until a device type match occurs.

Note
The non-forwarding VLAN cannot be defined within a port type assigned to the switch; it is exclusively used for the Instant Port Profile feature.

Default Port Type

You can select a default port type for an Instant Port Profile. When port parameters cannot be dynamically set by the device type configuration, the default port type settings provide the configuration.

VLAN parameters on the default port type are applied. For example, if the default port type is a phone port and LLDP/CDP parameters are statically defined for the port, LLDP/CDP/MED is not enabled dynamically on the match actions.

Note
Storm control settings are inherited when the non-match action is set to use the default port type, and a device does not match any defined device type.

Instant Port Profile Switch Template Configuration

Choosing a Non-Forwarding VLAN

Choosing a Non-Forwarding VLAN is essential for detecting MAC addresses on switch ports. The non-forwarding VLAN will be used to detect attached devices and will not forward traffic. The non-forwarding VLAN cannot be utilized within a port type assigned to the switch. Only the VLAN attribute **Name** is supported by a non-forwarding VLAN.

Choosing a Default Port Type

Configure the Default Port Type settings, which serve as a baseline for other port configuration parameters. Ports assigned with an Instant Port Profile inherit the selected port type setting such as type, speed, STP, MAC locking, ELRP, and PSE port settings. Storm control settings are inherited when the non-match action is set to use the default port type, and a device does not match a defined device type. See Configure Ports Individually on page 40 for more information on these port types.

Configuring Non-Match Actions

There are two options to choose between for non-match actions when a device does not match any defined device type criteria, including storm control settings:

- Non-forwarding VLAN – Traffic is not forwarded for devices that do not match an assignment rule when non-forwarding VLAN is selected.
- Use Default Port Type VLAN – Selecting the non-match action of the default port type assigns the VLANs associated with the port type.

Defining Match Criteria

Matches are based on the following criteria:

- MAC Learning – Matches the device based on the MAC address learned on the port from untagged traffic. The match can be an exact MAC, OUI based MAC, or custom MAC mask format.
- LLDP Src MAC – Matches the device based on the source MAC of an LLDP PDU. The match can be an exact MAC, OUI based MAC, or custom MAC mask format.
- LLDP Capability – Matches the device based on the LLDP capability from the source LLDP PDU. The LLDP capability is selectable.
- LLDP MAC + Capability – Matches the device based on the source MAC of an LLDP PDU and the LLDP capability from the source LLDP PDU selected.

Device-Level Configuration

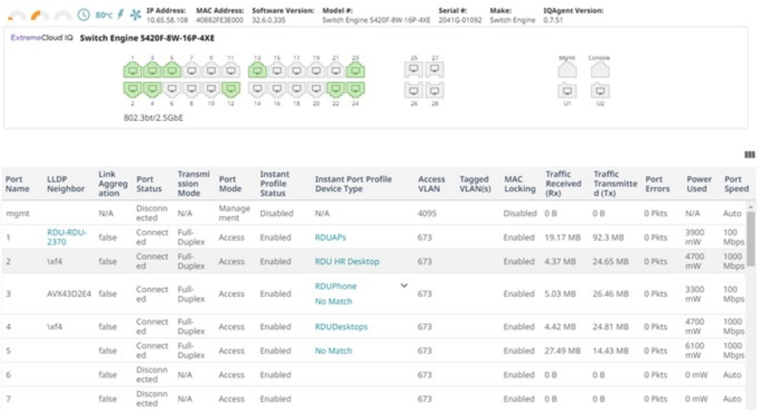
Instant Port Profiles (IPPs) can only be edited at the switch template level. At the device level, you must either select a different IPP or create a new IPP if your current IPP is not configured to your needs.

Choose from the following options for device level configuration of IPP:

- Unlock the device level template and disable or enable IPP per port
- Multi-edit ports and disable or enable IPP
- Create a new IPP from the device level
- Select a different IPP available from the menu, if you wish to deviate from switch template

Two new columns are added to the Device Monitoring page, **Instant Port Profile Status** and **Instant Port Profile Device Type VLAN(s)**.

The matched devices are connected to ports 1-4. These are the device types configured with Instant Port Profiles within the switch template.



80°c

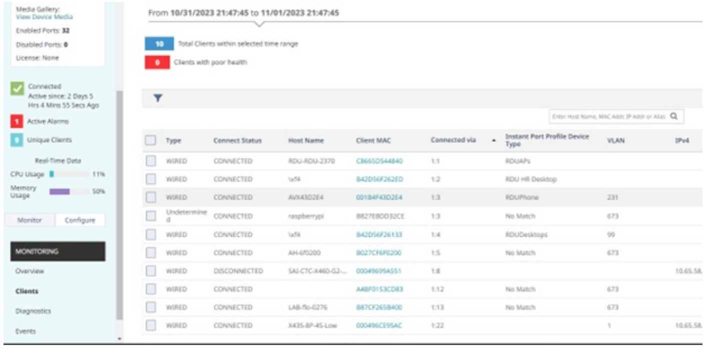
IP Address: 10.65.58.108
MAC Address: 40882FE3E000
Software Version: 32.6.0.335
Model #: Switch Engine 5420F-8W-16P-4XE
Serial #: 2041G-01092
Make: Switch Engine
IQAgent Version: 0.7.51

ExtremeCloud IQ Switch Engine 5420F-8W-16P-4XE

Port Name	LLDP Neighbor	Link Aggregation	Port Status	Transmission Mode	Port Mode	Instant Profile Status	Instant Port Profile Device Type	Access VLAN	Tagged VLAN(s)	MAC Locking	Traffic Received (Rx)	Traffic Transmitted (Tx)	Port Errors	Power Used	Port Speed
mgmt		N/A	Disconnected	N/A	Management	Disabled	N/A	4095		Disabled	0 B	0 B	0 Pkts	N/A	Auto
1	RDU-RDU-2370	false	Connected	Full-Duplex	Access	Enabled	RDUAPs	673		Enabled	19.17 MB	92.3 MB	0 Pkts	3900 mW	100 Mbps
2	\xf4	false	Connected	Full-Duplex	Access	Enabled	RDU HR Desktop	673		Enabled	4.37 MB	24.65 MB	0 Pkts	4700 mW	1000 Mbps
3	AVX43D2E4	false	Connected	Full-Duplex	Access	Enabled	RDUPhone No Match	673		Enabled	5.03 MB	26.46 MB	0 Pkts	3300 mW	100 Mbps
4	\xf4	false	Connected	Full-Duplex	Access	Enabled	RDUDesktops	673		Enabled	4.42 MB	24.81 MB	0 Pkts	4700 mW	1000 Mbps
5		false	Connected	Full-Duplex	Access	Enabled	No Match	673		Enabled	27.49 MB	14.43 MB	0 Pkts	6100 mW	1000 Mbps
6		false	Disconnected	N/A	Access	Enabled		673		Enabled	0 B	0 B	0 Pkts	0 mW	Auto
7		false	Disconnected	N/A	Access	Enabled		673		Enabled	0 B	0 B	0 Pkts	0 mW	Auto

Figure 2: Instant Port Profiles Overview

Check the connected clients in the **Monitoring** page. The Instant Port Profile Device Type column lists all the matched and no match device types connected to physical ports.



Media Gallery: View Device Media
Enabled Ports: 32
Disabled Ports: 0
License: None

Connected
Active since: 2 Days 5 Hrs 4 Mins 55 Secs Ago
1 Active Alarms
9 Unique Clients

Real-Time Data
CPU Usage 11%
Memory Usage 50%

From 10/31/2023 21:47:45 to 11/01/2023 21:47:45

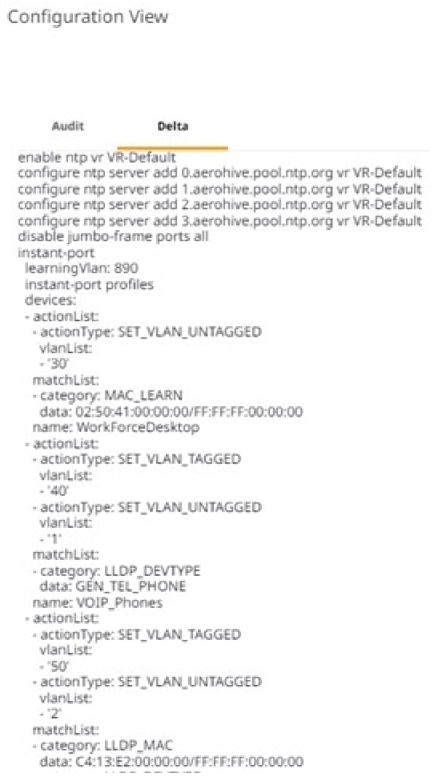
10 Total Clients within selected time range
0 Clients with poor health

□	Type	Connect Status	Host Name	Client MAC	Connected via	Instant Port Profile Device Type	VLAN	IPv4
□	WIRED	CONNECTED	RDU-RDU-2370	C8665O544840	1:1	RDUAPs		
□	WIRED	CONNECTED	\xf4	B42D56F262ED	1:2	RDU HR Desktop		
□	WIRED	CONNECTED	AVX43D2E4	001B4F43D2E4	1:3	RDUPhone	231	
□	Undetermined	CONNECTED	raspberrypi	B827EBDD32CE	1:3	No Match	673	
□	WIRED	CONNECTED	\xf4	B42D56F26133	1:4	RDUDesktops	99	
□	WIRED	CONNECTED	AH-6f0200	B027CF6F0200	1:5	No Match	673	
□	WIRED	DISCONNECTED	SAI-CTC-X460-G2-...	00049699A551	1:8			10.65.58.
□	WIRED	CONNECTED		A4BF0153CD83	1:12	No Match	673	
□	WIRED	CONNECTED	LAB-flo-0276	B87CF265B400	1:13	No Match	673	
□	WIRED	CONNECTED	X435-8P-4S-Low	000496CE95AC	1:22		1	10.65.58.

Figure 3: Instant Port Profiles Monitoring

Instant Port Profiles Delta Configuration Example

A configuration delta is created after an Instant Port Profile is created and applied to a port at the switch template level or device template level.



Configuration View

```
enable ntp vr VR-Default
configure ntp server add 0.aerohive.pool.ntp.org vr VR-Default
configure ntp server add 1.aerohive.pool.ntp.org vr VR-Default
configure ntp server add 2.aerohive.pool.ntp.org vr VR-Default
configure ntp server add 3.aerohive.pool.ntp.org vr VR-Default
disable jumbo-frame ports all
instant-port
 learningVlan: 890
 instant-port profiles
 devices:
 - actionList:
  - actionType: SET_VLAN_UNTAGGED
   vlanList:
   - '30'
  matchList:
  - category: MAC_LEARN
   data: 02:50:41:00:00:00/FF:FF:FF:00:00:00
  name: WorkForceDesktop
 - actionList:
  - actionType: SET_VLAN_TAGGED
   vlanList:
   - '40'
  - actionType: SET_VLAN_UNTAGGED
   vlanList:
   - '1'
  matchList:
  - category: LLDP_DEVTYPE
   data: GEN_TEL_PHONE
  name: VOIP_Phones
 - actionList:
  - actionType: SET_VLAN_TAGGED
   vlanList:
   - '50'
  - actionType: SET_VLAN_UNTAGGED
   vlanList:
   - '2'
  matchList:
  - category: LLDP_MAC
   data: C4:13:E2:00:00:00/FF:FF:FF:00:00:00
```

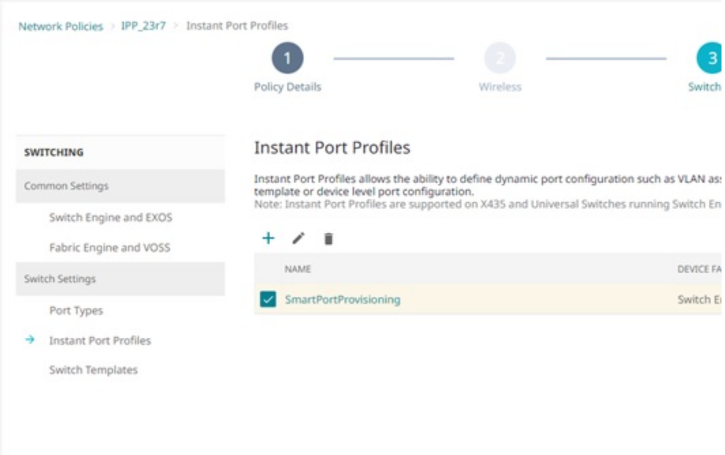
Figure 4: An example IPP configuration delta.

Instant Port Profile Example Workflow

This is an example workflow using the Instant Port Profile feature.

To create a new Instant Port Profile:

1. Navigate to **Network Policy** > **Policy** > **Switching** > **Switch Settings** > **Instant Port Profiles.**



Network Policies > IPP_23r7 > Instant Port Profiles

SWITCHING
Common Settings
Switch Engine and EXOS
Fabric Engine and VOSS
Switch Settings
Port Types
Instant Port Profiles
Switch Templates

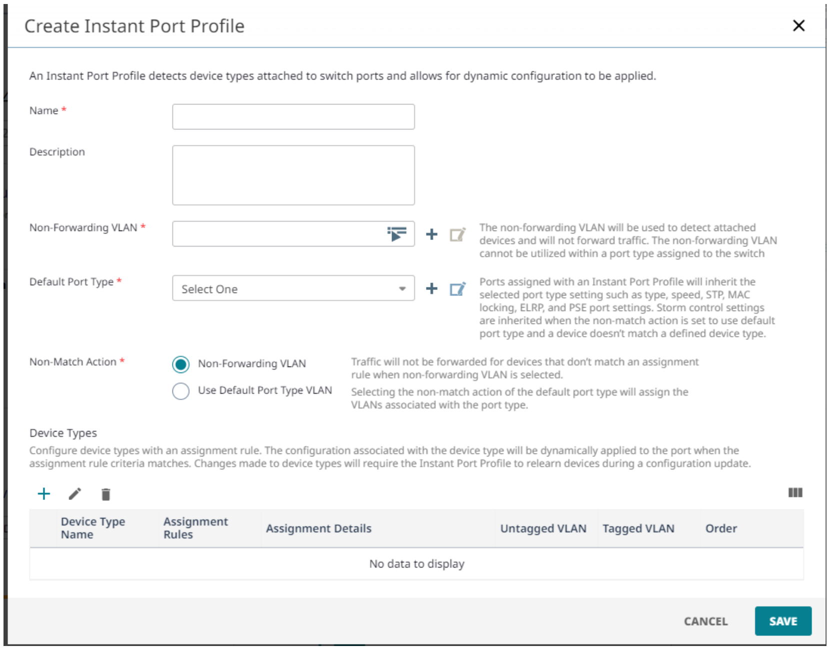
Instant Port Profiles

Instant Port Profiles allows the ability to define dynamic port configuration such as VLAN as template or device level port configuration.
Note: Instant Port Profiles are supported on X435 and Universal Switches running Switch En

	NAME	DEVICE FA
☑	SmartPortProvisioning	Switch E

Figure 5: Instant Port Profiles Switch Template

2. Enter the information for the Non-Forwarding VLAN, Default Port Type, and Non-Match Action. See Instant Port Profile Switch Template Configuration on page 53 for more information about configuring IPP.



Create Instant Port Profile

An Instant Port Profile detects device types attached to switch ports and allows for dynamic configuration to be applied.

Name *

Description

Non-Forwarding VLAN * — The non-forwarding VLAN will be used to detect attached devices and will not forward traffic. The non-forwarding VLAN cannot be utilized within a port type assigned to the switch

Default Port Type * Select One — Ports assigned with an Instant Port Profile will inherit the selected port type setting such as type, speed, STP, MAC locking, ELRP, and PSE port settings. Storm control settings are inherited when the non-match action is set to use default port type and a device doesn't match a defined device type.

Non-Match Action *
● Non-Forwarding VLAN — Traffic will not be forwarded for devices that don't match an assignment rule when non-forwarding VLAN is selected.
○ Use Default Port Type VLAN — Selecting the non-match action of the default port type will assign the VLANs associated with the port type.

Device Types

Configure device types with an assignment rule. The configuration associated with the device type will be dynamically applied to the port when the assignment rule criteria matches. Changes made to device types will require the Instant Port Profile to relearn devices during a configuration update.

Device Type Name	Assignment Rules	Assignment Details	Untagged VLAN	Tagged VLAN	Order
No data to display					

Figure 6: Instant Port Profiles Creation

3. Create, edit, or delete device types.
4. Define device types and their respective match criteria such as MAC learning, LLDP Source MAC, LLDP Capability, or a combination. For a device type to match based

on MAC learning, the rule must be ordered above any LLDP-based assignment rules. This ensures that MAC learning takes precedence, irrespective of LLDP information.

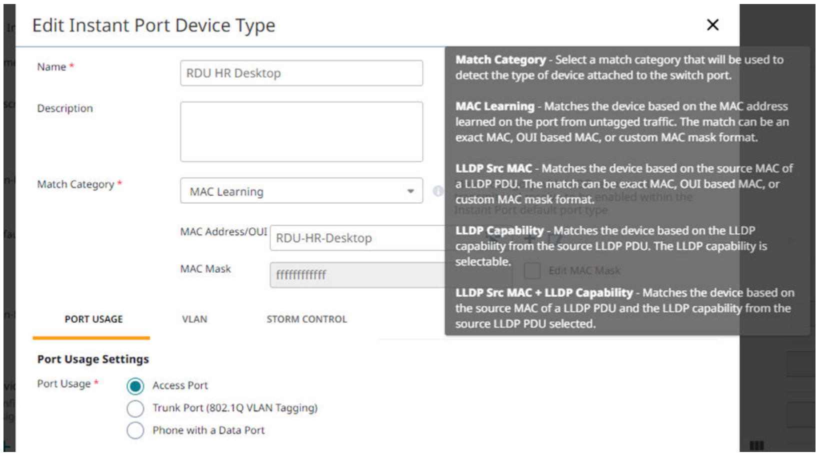
Configure port usage, VLAN, and storm control settings under match criteria for the device type.

The options for port usage are:

- Access Port
- Trunk Port (802.1Q VLAN Tagging)
- Phone with a Data Port

Within the **VLAN Settings** section, untagged VLANs are assigned based on MAC addresses using MAC-based VLANs determined by the selected match category. The system identifies the client MAC addresses for this purpose. However, for traffic with tagged VLANs, no learning or device type matches are conducted.

> **Note**
> The latest device type match on a port for storm control settings will override existing storm control values.



Edit Instant Port Device Type ✕

Name *: RDU HR Desktop

Description:

Match Category *: MAC Learning

MAC Address/OUI: RDU-HR-Desktop

MAC Mask: ffffffffffff

PORT USAGE | VLAN | STORM CONTROL

Port Usage Settings

Port Usage *:
● Access Port
○ Trunk Port (802.1Q VLAN Tagging)
○ Phone with a Data Port

Match Category - Select a match category that will be used to detect the type of device attached to the switch port.

MAC Learning - Matches the device based on the MAC address learned on the port from untagged traffic. The match can be an exact MAC, OUI based MAC, or custom MAC mask format.

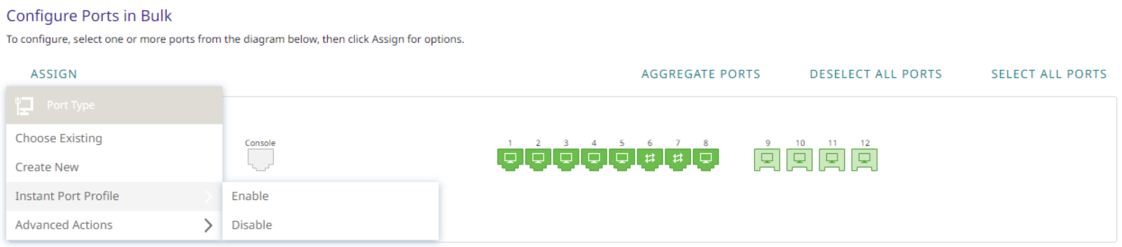
LLDP Src MAC - Matches the device based on the source MAC of a LLDP PDU. The match can be exact MAC, OUI based MAC, or custom MAC mask format.

LLDP Capability - Matches the device based on the LLDP capability from the source LLDP PDU. The LLDP capability is selectable.

LLDP Src MAC + LLDP Capability - Matches the device based on the source MAC of a LLDP PDU and the LLDP capability from the source LLDP PDU selected.

Figure 7: Instant Port Profiles Port Device Type

5. Assign Instant Port profiles to switches within switch templates. Select **Template** > **Port Configuration.** Under **Configure Port Individually** select the existing IPP from the menu.



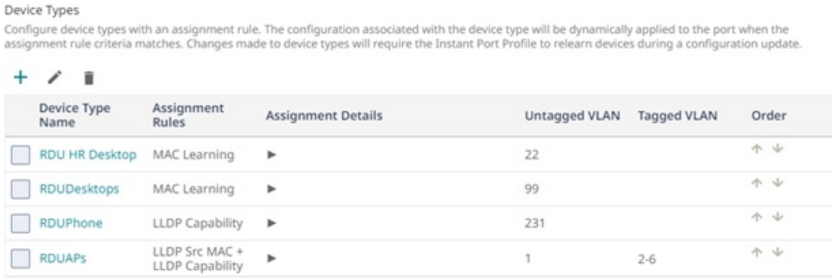
Configure Ports in Bulk

To configure, select one or more ports from the diagram below, then click Assign for options.

Figure 8: Instant Port Profiles Wired Devices

6. For device level management of IPP: Select the desired port(s) by selecting **Assign**, select **Instant Port Profile** > **Enable or Disable.** To override Instant Port Profile settings at the device level:
   a. Navigate to **Manage** > **Devices** > **Configure** > **Port Configuration.**
   b. Override IPP assignments and the ability to enable or disable ports as required.
7. Select **Save** to apply IPP to the switch template.

   For the following example, the below device types are configured using Instant Port Profiles assigned to a switch template.



Device Types

Configure device types with an assignment rule. The configuration associated with the device type will be dynamically applied to the port when the assignment rule criteria matches. Changes made to device types will require the Instant Port Profile to relearn devices during a configuration update.

	Device Type Name	Assignment Rules	Assignment Details	Untagged VLAN	Tagged VLAN	Order
□	RDU HR Desktop	MAC Learning	▶	22		↑ ↓
□	RDUDesktops	MAC Learning	▶	99		↑ ↓
□	RDUPhone	LLDP Capability	▶	231		↑ ↓
□	RDUAPs	LLDP Src MAC + LLDP Capability	▶	1	2-6	↑ ↓

Figure 9: Wired Device Types

Example Deployment Scenario: Optimizing Network for an Office

In an office with diverse network needs, an IT administrator utilizes Instant Port Profiles to automate and optimize network configuration based on the types of devices connected to switch ports.

IPP offers the following advantages:

- Automatically assigns VLANs and applies appropriate settings to switch ports based on connected devices
- Ensure secure and efficient network operation

In this scenario, we define three different device types: Employees, Guests, and Printers. Each device type has specific matching criteria. We will configure VLAN assignments based on these criteria.

- Employees: Devices identified by MAC addresses
- Guests: Devices identified by LLDP information
- Printers: Devices identified by a combination of MAC and LLDP data

Next, configure Instant Port Profiles:

- Create a new Instant Port Profile
- Select a non-forwarding VLAN to detect MAC addresses initially
- Choose a default port type for other configuration parameters
- Define the non-match action, specifying whether to use the default port type configuration or set traffic to non-forwarding

Then configure device types:

- Add or edit device types
- Define matching criteria for each type:
    - For **Employees** specify MAC learning
    - For **Guests** use LLDP Source MAC or LLDP Capability
    - For **Printers** use a combination of MAC and LLDP data

Assign the created Instant Port Profile to switch ports within a template or device-level port configuration override settings.

Optionally, you can override the Instant Port Profile assignment and port enable or disable settings within device-level configuration.

In this scenario, when a device connects to a switch port, IPP will analyze its characteristics:

- If it matches the criteria for **Employees** (based on MAC address), it is assigned to VLAN **X**
- If it matches the criteria for **Guests** (based on LLDP Capability), it is assigned to VLAN **Y**
- If it matches the criteria for **Printers** (based on MAC address and LLDP Capability), it is assigned to VLAN **Z**

Example Deployment Scenario: Unmanaged Switch or Hub with Two Different Devices

In this scenario, we have an unmanaged switch or hub with two different devices connected to the same port. IPP allows us to handle this situation effectively by applying VLAN assignments based on MAC addresses.

First, define device types for each connected device

Next, configure Instant Port Profiles:

- Create a new Instant Port Profile
- Select a non-forwarding VLAN to detect MAC addresses initially
- Choose a default port type for other configuration parameters
- Define the non-match action, specifying whether to use the default port type configuration or set traffic to non-forwarding

Then configure device types:

- Add or edit device types
- Define matching criteria based on the characteristics of each device:
    - **Device 1 (e.g., Laptop)**:
        - Sample MAC Address: 00:1A:2B:3C:4D:5E
        - Dynamic Configuration: Assign VLAN 10 based on the MAC address
    - **Device 2 (e.g., Desktop Computer)**:
        - Sample MAC Address: 00:AA:BB:CC:DD:EE

- Dynamic Configuration: Assign VLAN 20 based on the MAC address.

Assign the created Instant Port Profile to the port where the unmanaged switch or hub is connected.

IPP dynamically assigns VLANs based on the MAC addresses of the two devices connected to the unmanaged switch or hub, allowing them to have different VLAN assignments on the same port.

When both Device 1 and Device 2 are connected to the same port, IPP will dynamically assign VLANs based on their respective MAC addresses. Device 1 will be assigned to VLAN 10, and Device 2 will be assigned to VLAN 20, allowing different VLAN assignments on the same port based on MAC address matching.

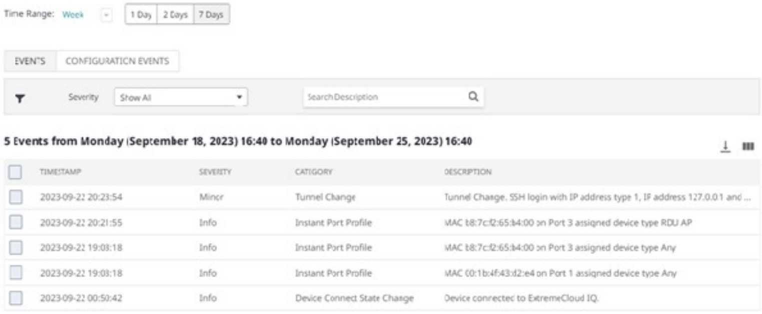
Instant Port Profiles Troubleshooting

When facing issues with IPP, check the audit logs at **Global Settings** > **Logs** > **Audit Logs** for more information.

Check the monitoring page after a match has occurred.

Note
It may take up to 10 minutes for the information to appear.

In the below example, MAC `b8:7c:f2:65:b4:00` on Port 3 is assigned the device type RDU AP and is checked under the IPP category of Events.



5 Events from Monday (September 18, 2023) 16:40 to Monday (September 25, 2023) 16:40

	TIMESTAMP	SEVERITY	CATEGORY	DESCRIPTION
□	2023-09-22 20:23:54	Minor	Tunnel Change	Tunnel Change. SSH login with IP address type 1, IP address 127.0.0.1 and ...
□	2023-09-22 20:21:55	Info	Instant Port Profile	MAC b8:7c:f2:65:b4:00 on Port 3 assigned device type RDU AP
□	2023-09-22 19:03:18	Info	Instant Port Profile	MAC b8:7c:f2:65:b4:00 on Port 3 assigned device type Any
□	2023-09-22 19:03:18	Info	Instant Port Profile	MAC 00:1b:4f:43:d2:e4 on Port 1 assigned device type Any
□	2023-09-22 00:50:42	Info	Device Connect State Change	Device connected to ExtremeCloud IQ.

Instant Port Profile matched device type are checked under **Monitoring** > **Overview**.

Instant Port Profile client MAC addresses are checked under **Monitoring** > **Clients**. Select the client MAC to check the current connection status of the connected client.

Instant Port Profiles Out of Sync

Configuration changes related to LLDP/STP on a port from outside ExtremeCloud IQ when you have configured IPP from inside ExtremeCloud IQ causes out of sync configuration errors.

to resolve out of sync errors, begin by selecting **Update Devices** in the Devices list. Then, in the **Device Update** dialog, select **Perform delta configuration update and**

resolve local device configuration which is out of sync with ExtremeCloud IQ and perform an update.

Hardware and Software Requirements

This feature is supported on the following hardware:

- Switch Engine 5000 and 7000 series
- EXOS x435 ExtremeCloud IQ supported switches

Note
Instant Port Profiles is not supported on Digital Twin.

Instant Port Profiles requires software 32.6.1.5-patch1-2 or later.

Scaling

Instant Port Profiles scales to the following limitations:

- Maximum number of device-types per Instant Port Profile: 20
- Maximum number of actions per device-types: 8
- Maximum number of detections per switch with instant port enabled: 1,000
- Maximum number of device type MAC based VLAN assignment: 1,024

Note
The maximum burst of device type detection such as MAC Learning or LLDP device-detect is 1000. When the queue limit is reached some devices are ignored. If the max limit is reached, a clear FDB or port restart is required.

Instant Secure Port Profiles

Instant Secure Port Profiles (ISPP) in ExtremeCloud IQ enables you to configure user authentication and MAC authentication per port and to specify a RADIUS server to use in conjunction with Universal ZTNA.

Only one Instant Secure Port Profile can be configured per switch, with the ability to enable and disable user authentication and MAC authentication per port.

Specify a RADIUS server configured in the Universal ZTNA/Raas application. Only those Regional Data Centers (RDCs) that support this configuration and users that have a license are able to use ISPP.

An instant secure port profile is created separately from any existing instant port profiles.

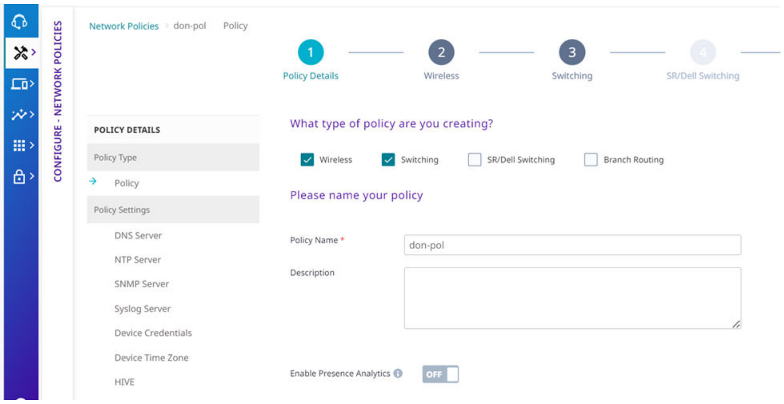
Creating a New Instant Secure Port Profile

> **Note**
> The Instant Secure Port Profile (ISPP) option will only become available when Universal ZTNA is activated.

You must create a network policy.

Use the **Manage** > **Devices** page to see all the devices that have been onboarded to ExtremeCloud IQ. Add the network policy to the desired Switch Engine.

The type must have the **Switching** box checked. Other options like **Wireless** can be checked as needed. The **Policy Name** is a required attribute.



What type of policy are you creating?

☑ Wireless ☑ Switching □ SR/Dell Switching □ Branch Routing

Please name your policy

Policy Name * don-pol

Description

Enable Presence Analytics OFF

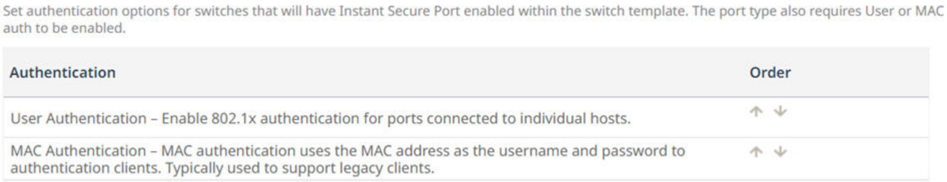
Figure 10: Network Policy Creation

Instant Secure Port Profiles (ISPPs) are created within the Switch Settings subsection of the Network Policy creation and editing page.

To create a new Instant Secure Port Profile:

1. Select ＋.
2. Enter the name for your ISPP. The name is unique within ExtremeCloud IQ but is not pushed to the device.
3. Choose whether to use Unauthenticated VLAN. Unauthenticated VLAN is either a common object or can be created when the profile is created. If the Enable Unauthenticated VLAN is selected, then this VLAN will override the untagged VLAN in the port type and will be used as the Unauthenticated VLAN on the Switch Engine device when the configuration is pushed.

4. Specify the order in which to execute authentication. The order is per profile; therefore the same order is used for the entire Switch Engine device once the configuration is pushed. Use the arrows to change the default order.



Set authentication options for switches that will have Instant Secure Port enabled within the switch template. The port type also requires User or MAC auth to be enabled.

Authentication	Order
User Authentication – Enable 802.1x authentication for ports connected to individual hosts.	↑ ↓
MAC Authentication – MAC authentication uses the MAC address as the username and password to authentication clients. Typically used to support legacy clients.	↑ ↓

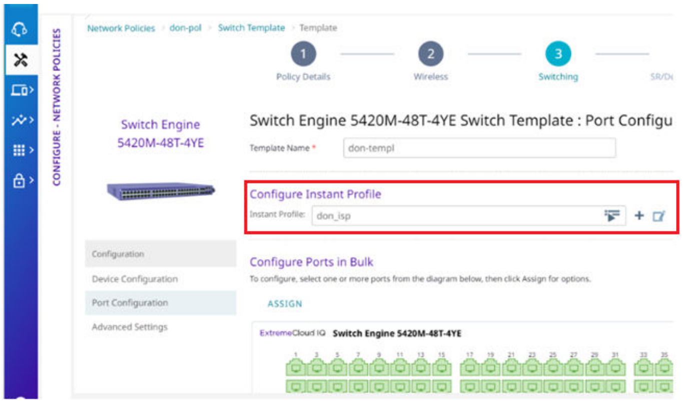
Figure 11: ISPP Authentication Order

5. Pick the RADIUS server for the Instant Secure Profile. Selecting **Use UZTNA RADIUS Cloud configuration** uses either the free cloud RADIUS server set up per RDC, or configured proxy RADIUS servers in the UZTNA application. Select one of the radio buttons to decide which type to use. Further, in the case of proxy RADIUS, you can select up to two proxy RADIUS servers; it is assumed that the ones selected have reached a deployed state after being configured in UZTNA.
6. Select **Save**.

ISPP Configuration from Switch Template

To configure and select an existing Instant Secure Port Profile from within a switch template:

1. Go to **Configure** > **Network Policies** > **Create or Edit a Policy** > **Switching** > **Switch Templates** page.
2. Either edit an existing template, or create a new switch template for a specific Switch Engine device model such as a 5420M-48T-4YE.
3. In the left menu pane select **Port/VLAN Configuration**.
4. If you are creating a new template, supply a template name.
5. Select the Instant Secure Profile from the **Instant Port Profile** list.



Switch Engine 5420M-48T-4YE Switch Template : Port Configu

Template Name * don-templ

Configure Instant Profile

Instant Profile: don_isp

Configure Ports in Bulk

To configure, select one or more ports from the diagram below, then click Assign for options.

Figure 12: Switch Template ISPP Selection

Enable Instant Secure Port Profile on a Port

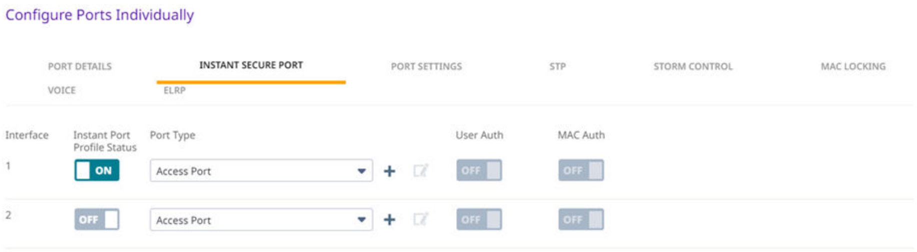
Create the Instant Secure Port Profile (ISPP) switch template, see ISPP Configuration from Switch Template on page 63.

Use this task to enable ISPP on a port.

1. Go to **Configure** > **Network Policies** page.
2. Edit an existing template, or create a new switch template.
3. From the left pane, select **Port/VLAN Configuration**.
4. Enable or disable the Instant Secure Port Profile for any specific ports:
   a. Select the profile to use in the **Port Profile** dropdown menu.
   b. Enable or disable the profile on a port by using the **Instant Profile** toggle switches in the **Configure Ports Individually** section.

   > Note
   > The switch can only have Instant Port or Instant Secure Port enabled, but not both.

5. Enable User Auth or MAC Auth or both.
6. Specify the Port Type, such as Access, Trunk, or Phone:
   a. Create or edit your selected **Port Type**.
   b. Select the Port Usage within the **Port Name & Usage** tab.
7. After all the ports are configured, select **SAVE**.

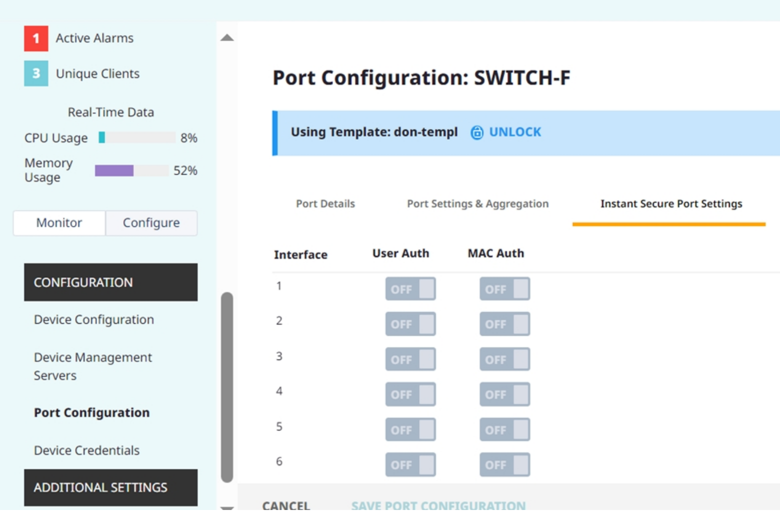


Interface	Instant Port Profile Status	Port Type	User Auth	MAC Auth
1	ON	Access Port	OFF	OFF
2	OFF	Access Port	OFF	OFF

Figure 13: ISPP Individual Port Configuration

Instant Secure Port Profiles Device Level Override

You can override the template parameters within the devices **Port Configuration** page. Use the **LOCK/UNLOCK** option to switch between the inherited template settings and to override at the device level. The device's **Port Configuration** page can be used for stacks, LAGs, channelized ports, and VIMs.



Port Configuration: SWITCH-F

Using Template: don-templ

Interface	User Auth	MAC Auth
1	OFF	OFF
2	OFF	OFF
3	OFF	OFF
4	OFF	OFF
5	OFF	OFF
6	OFF	OFF

Figure 14: Instant Secure Port Profile Device Level

DHCP Snooping

DHCP Snooping enables snooping of DHCP packets and creates a DHCP bindings database of IP to MAC addresses for static and dynamic VLANs.

DHCP servers connected to ports not configured as trusted are deemed to be rogue DHCP servers. This feature allows you to:

- Configure DHCP Snooping for EXOS/Switch Engine globally within a switch template
- Define DHCP snooping actions within the VLAN attributes section
- Enable or disable trusted ports within port types
- Enable dropping of rogue DHCP Packets action for static and dynamic VLANs.

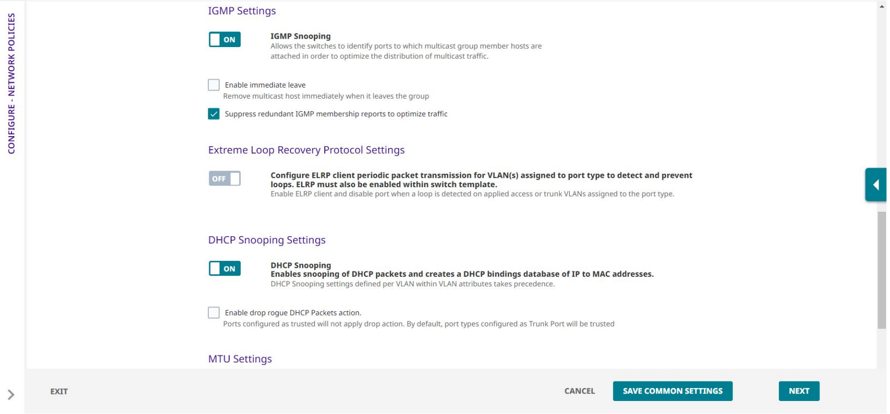
Common use-cases for DHCP Snooping are:

- The ability to configure DHCP Snooping protection on edge switches to prevent rogue DHCP packets from traversing ports.
- The ability to globally enable the feature for all edge switches in specific VLANs assigned to a network policy.
- The ability to support DHCP snooping being disabled using switch template VLAN attributes override or device level configuration override.
- Provide flexibility to enable a trusted port on specific ports where DHCP servers may exist on a switch with mixed ports (untrusted and trusted) for DHCP snooping. Visibility of violations and additional information such as DHCP lease time is also required to be visible when the DHCP snooping feature is enabled.

DHCP Snooping Configuration

Enable DHCP Snooping from the Common Settings of a Network Policy. Go to **Configure** > **Network Policies**, select a policy or add a policy, select **Switching** > **Common Settings**

ExtremeXOS/Switch Engine



IGMP Settings

ON **IGMP Snooping**
Allows the switches to identify ports to which multicast group member hosts are attached in order to optimize the distribution of multicast traffic.

□ Enable immediate leave
Remove multicast host immediately when it leaves the group

☑ Suppress redundant IGMP membership reports to optimize traffic

Extreme Loop Recovery Protocol Settings

OFF **Configure ELRP client periodic packet transmission for VLAN(s) assigned to port type to detect and prevent loops. ELRP must also be enabled within switch template.**
Enable ELRP client and disable port when a loop is detected on applied access or trunk VLANs assigned to the port type.

DHCP Snooping Settings

ON **DHCP Snooping**
Enables snooping of DHCP packets and creates a DHCP bindings database of IP to MAC addresses.
DHCP Snooping settings defined per VLAN within VLAN attributes takes precedence.

□ Enable drop rogue DHCP Packets action.
Ports configured as trusted will not apply drop action. By default, port types configured as Trunk Port will be trusted

MTU Settings

Figure 15: DHCP Snooping Network Policy

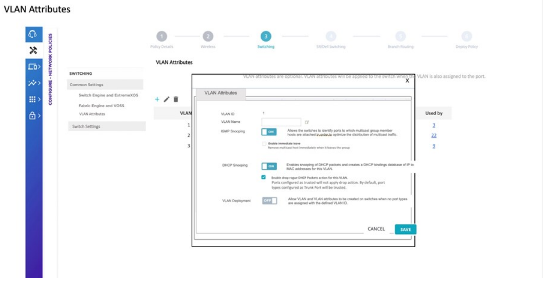
When enabled, ExtremeCloud IQ pushes the DHCP Snooping configuration for all VLANs configured from within ExtremeCloud IQ.

> **Note**
> Trunk ports are configured as trusted by default.

Enable all ports (including trunk ports) for the DHCP Snooping configuration, and the violation action to drop packets enabled.

VLAN Attributes Configuration

Common Settings can be overridden by configuring VLAN specific attributes.



VLAN Attributes

VLAN attributes are optional. VLAN attributes will be applied to the switch when the VLAN is also assigned to the port.

VLAN	Used by
1	3
2	22
3	9

VLAN ID 1

VLAN Name

IGMP Snooping ON Allows the switches to identify ports to which multicast group member hosts are attached in order to optimize the distribution of multicast traffic.

□ Enable immediate leave
Remove multicast host immediately when it leaves the group

DHCP Snooping ON Enables snooping of DHCP packets and creates a DHCP bindings database of IP to MAC addresses for this VLAN.

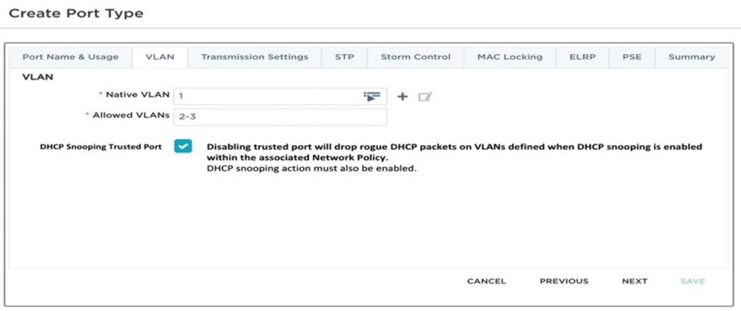
☑ Enable drop rogue DHCP Packets action for this VLAN.
Ports configured as trusted will not apply drop action. By default, port types configured as Trunk Port will be trusted.

VLAN Deployment OFF Allow VLAN and VLAN attributes to be created on switches when no port types are assigned with the defined VLAN ID.

Figure 16: DHCP Snooping VLAN Attributes

Custom Port Types DHCP Snooping Action

By default, all trunk ports on VLANs are trusted, you can override the trusted setting by defining a custom port type and associating the port with device in the template or the device monitoring page.



VLAN

* Native VLAN: 1

* Allowed VLANs: 2-3

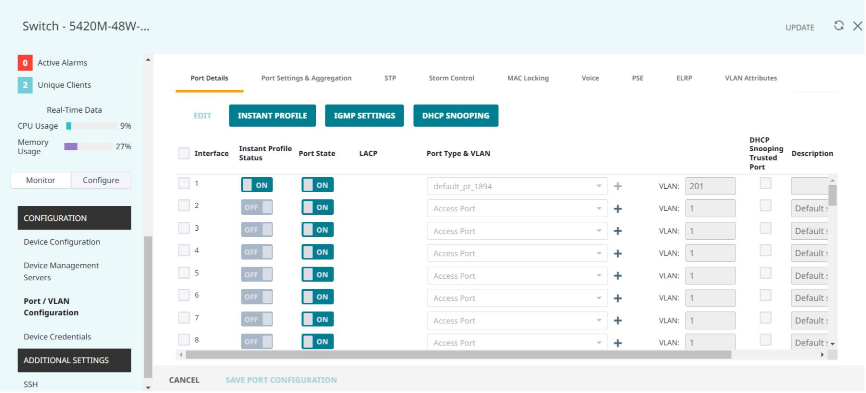
DHCP Snooping Trusted Port ☑

Disabling trusted port will drop rogue DHCP packets on VLANs defined when DHCP snooping is enabled within the associated Network Policy.
DHCP snooping action must also be enabled.

Figure 17: Port / VLAN Configuration

Device Level Override

The device monitoring page override options take precedence over policy, common settings and VLAN attribute configurations. To enable DHCP Snooping on the device level, select the **DHCP Snooping** button and toggle the feature enabled within the **Port/VLAN Configuration** page of the Device Configuration menu.



0 Active Alarms

2 Unique Clients

Real-Time Data

CPU Usage 9%

Memory Usage 27%

□ Interface	Instant Profile Status	Port State	LACP	Port Type & VLAN		DHCP Snooping Trusted Port	Description
□ 1	ON	ON		default_pt_1894	VLAN: 201	□	
□ 2	OFF	ON		Access Port	VLAN: 1	□	Default :
□ 3	OFF	ON		Access Port	VLAN: 1	□	Default :
□ 4	OFF	ON		Access Port	VLAN: 1	□	Default :
□ 5	OFF	ON		Access Port	VLAN: 1	□	Default :
□ 6	OFF	ON		Access Port	VLAN: 1	□	Default :
□ 7	OFF	ON		Access Port	VLAN: 1	□	Default :
□ 8	OFF	ON		Access Port	VLAN: 1	□	Default :

Figure 18: Device Monitoring Override

IGMP Snooping

With IGMP Snooping switches identify which ports multicast group members hosts are associated with to optimize the distribution of multicast traffic.

Some common use-cases for IGMP Snooping are:

- Configuring IGMP Snooping on switches for specific VLANs.
- Enabling the feature globally for all edge switches in specific VLANs assigned to a network policy.
- Supporting IGMP Snooping to be disabled using switch template VLAN attributes override or device-level configuration override.

The IGMP Snooping feature can be configured in multiple locations, in an overriding hierarchy, listed in order of priority:

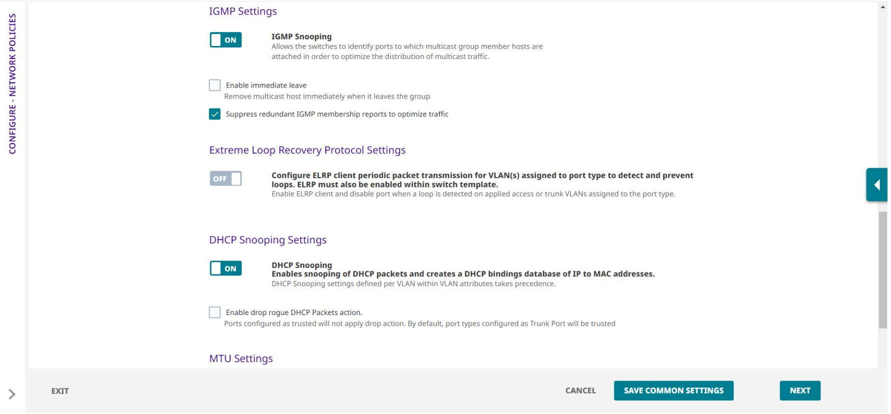
1. Device Specific VLAN configuration
2. VLAN attributes screen

3. Device templates
4. Common settings

When IGMP Snooping is not configured, the higher-level settings take effect. For example, if device-specific VLAN IGMP settings are set to **disabled**, the VLAN attributes settings for the VLAN take effect.

Configure IGMP Snooping

IGMP Snooping can be enabled in the common settings of the network policy.



IGMP Settings

ON **IGMP Snooping**
Allows the switches to identify ports to which multicast group member hosts are attached in order to optimize the distribution of multicast traffic.

□ Enable immediate leave
Remove multicast host immediately when it leaves the group

☑ Suppress redundant IGMP membership reports to optimize traffic

Extreme Loop Recovery Protocol Settings

OFF **Configure ELRP client periodic packet transmission for VLAN(s) assigned to port type to detect and prevent loops. ELRP must also be enabled within switch template.**
Enable ELRP client and disable port when a loop is detected on applied access or trunk VLANs assigned to the port type.

DHCP Snooping Settings

ON **DHCP Snooping**
Enables snooping of DHCP packets and creates a DHCP bindings database of IP to MAC addresses.
DHCP Snooping settings defined per VLAN within VLAN attributes takes precedence.

□ Enable drop rogue DHCP Packets action.
Ports configured as trusted will not apply drop action. By default, port types configured as Trunk Port will be trusted

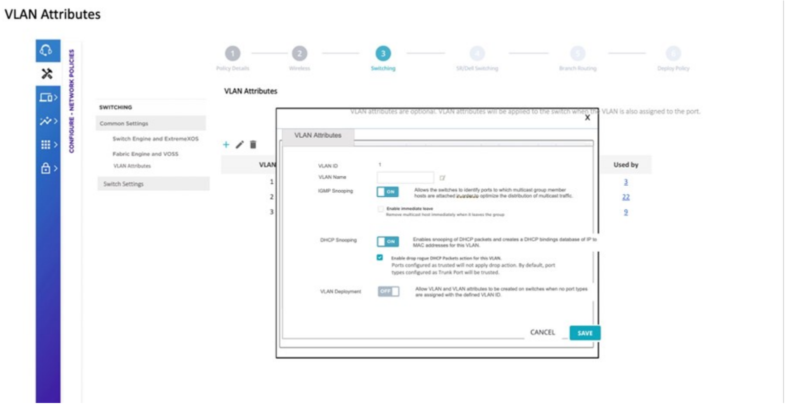
MTU Settings

Figure 19: IGMP Snooping Network Policy

When enabled, ExtremeCloud IQ pushes the IGMP Snooping configuration for all VLANs configured from ExtremeCloud IQ.

VLAN Attributes Configuration

You can override Common Settings by configuring VLAN specific attributes.



VLAN attributes are optional. VLAN attributes will be applied to the switch when the VLAN is also assigned to the port.

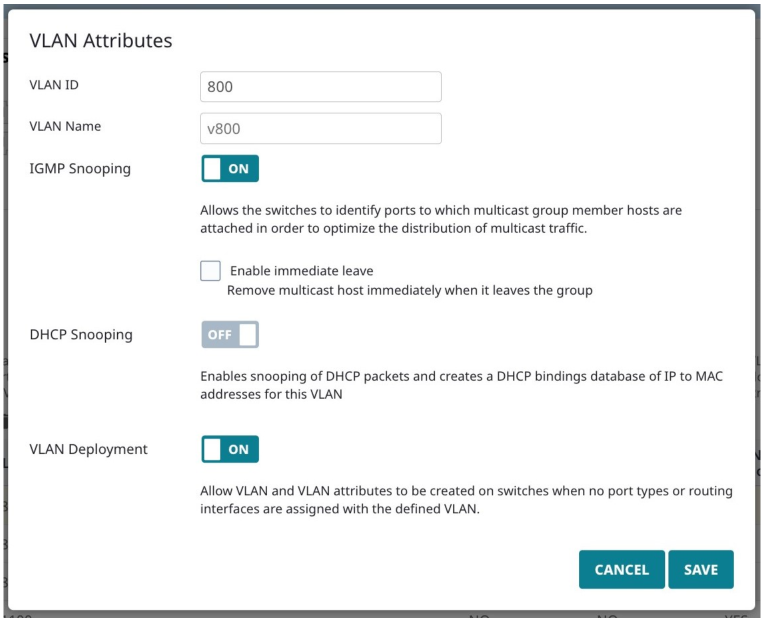
VLAN	Used by
1	3
2	22
3	9

VLAN ID 1
VLAN Name
IGMP Snooping ON Allows the switches to identify ports to which multicast group member hosts are attached in order to optimize the distribution of multicast traffic.
□ Enable immediate leave
Remove multicast host immediately when it leaves the group
DHCP Snooping ON Enables snooping of DHCP packets and creates a DHCP bindings database of IP to MAC addresses for this VLAN.
☑ Enable drop rogue DHCP Packets action for this VLAN.
Ports configured as trusted will not apply drop action. By default, port types configured as Trunk Port will be trusted.
VLAN Deployment OFF Allow VLAN and VLAN attributes to be created on switches when no port types are assigned with the defined VLAN ID.

Figure 20: IGMP Snooping VLAN Attributes

Device Level Override

The device monitoring page override options take precedence over policy, common settings and VLAN attribute configurations. To enable IGMP Snooping on the device level, select the IGMP Snooping button and toggle the feature enabled within the **Port/ VLAN Configuration** page of the devices configuration menu.



VLAN Attributes

VLAN ID: 800

VLAN Name: v800

IGMP Snooping: ON

Allows the switches to identify ports to which multicast group member hosts are attached in order to optimize the distribution of multicast traffic.

□ Enable immediate leave
Remove multicast host immediately when it leaves the group

DHCP Snooping: OFF

Enables snooping of DHCP packets and creates a DHCP bindings database of IP to MAC addresses for this VLAN

VLAN Deployment: ON

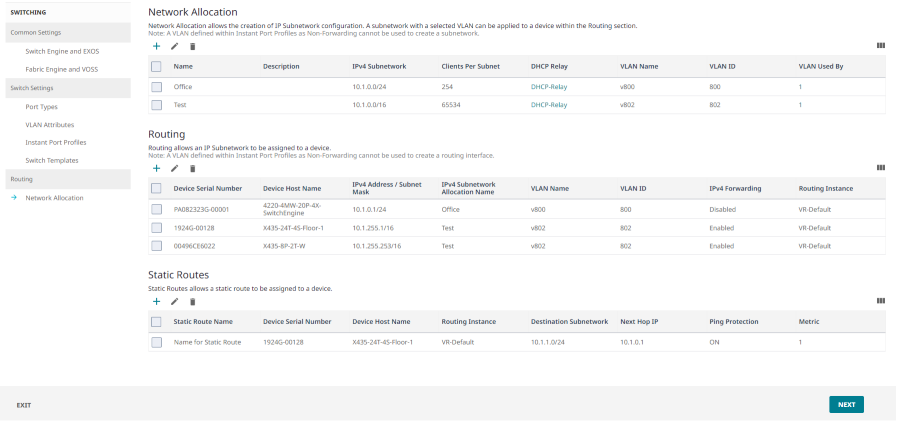
Allow VLAN and VLAN attributes to be created on switches when no port types or routing interfaces are assigned with the defined VLAN.

Figure 21: VLAN Attributes

Routing

The Routing feature in ExtremeCloud IQ allows for configuration of IPv4 forwarding, DHCP Relay, and Static Routing for Universal Hardware running Switch Engine or x435 devices.

Network Allocation within the Network Policy Switching Section allows for an IPv4 Subnetwork to be defined with a VLAN created from VLAN attributes with a defined local IP Address Subnetwork space, IP address of the IPv4 interface, and DHCP Relay Server configuration.



Network Allocation

Network Allocation allows the creation of IP Subnetwork configuration. A subnetwork with a selected VLAN can be applied to a device within the Routing section.
Note: A VLAN defined within Instant Port Profiles as Non-Forwarding cannot be used to create a subnetwork.

□	Name	Description	IPv4 Subnetwork	Clients Per Subnet	DHCP Relay	VLAN Name	VLAN ID	VLAN Used By
□	Office		10.1.0.0/24	254	DHCP-Relay	v800	800	1
□	Test		10.1.0.0/16	65534	DHCP-Relay	v802	802	1

Routing

Routing allows an IP Subnetwork to be assigned to a device.
Note: A VLAN defined within Instant Port Profiles as Non-Forwarding cannot be used to create a routing interface.

□	Device Serial Number	Device Host Name	IPv4 Address / Subnet Mask	IPv4 Subnetwork Allocation Name	VLAN Name	VLAN ID	IPv4 Forwarding	Routing Instance
□	PA082323G-00001	4220-4MW-20P-4X-SwitchEngine	10.1.0.1/24	Office	v800	800	Disabled	VR-Default
□	1924G-00128	X435-24T-4S-Floor-1	10.1.255.1/16	Test	v802	802	Enabled	VR-Default
□	00496CE6022	X435-8P-2T-W	10.1.255.253/16	Test	v802	802	Enabled	VR-Default

Static Routes

Static Routes allows a static route to be assigned to a device.

□	Static Route Name	Device Serial Number	Device Host Name	Routing Instance	Destination Subnetwork	Next Hop IP	Ping Protection	Metric
□	Name for Static Route	1924G-00128	X435-24T-4S-Floor-1	VR-Default	10.1.1.0/24	10.1.0.1	ON	1

Figure 22: Network Allocation

The IPv4 interface assigned to a device allows the ability to define IPv4 forwarding, VLAN loopback, and DHCP relay assignment.

IPv4 Static routes can also be defined with the destination subnetwork, next hop IP, next hop IP ping protection, and metric.

Network Allocation

Network Allocation supports the creation of IP subnetwork configuration. A subnetwork with a selected VLAN can be applied to a device within the Routing section. When entries are added in the Network Allocation table, the Local IP Address

Space field is valid only if it's a subnet address, not a host address. This table allows the user to create subnetworks which will be then used to the configure IP addresses per VLAN in the next table.

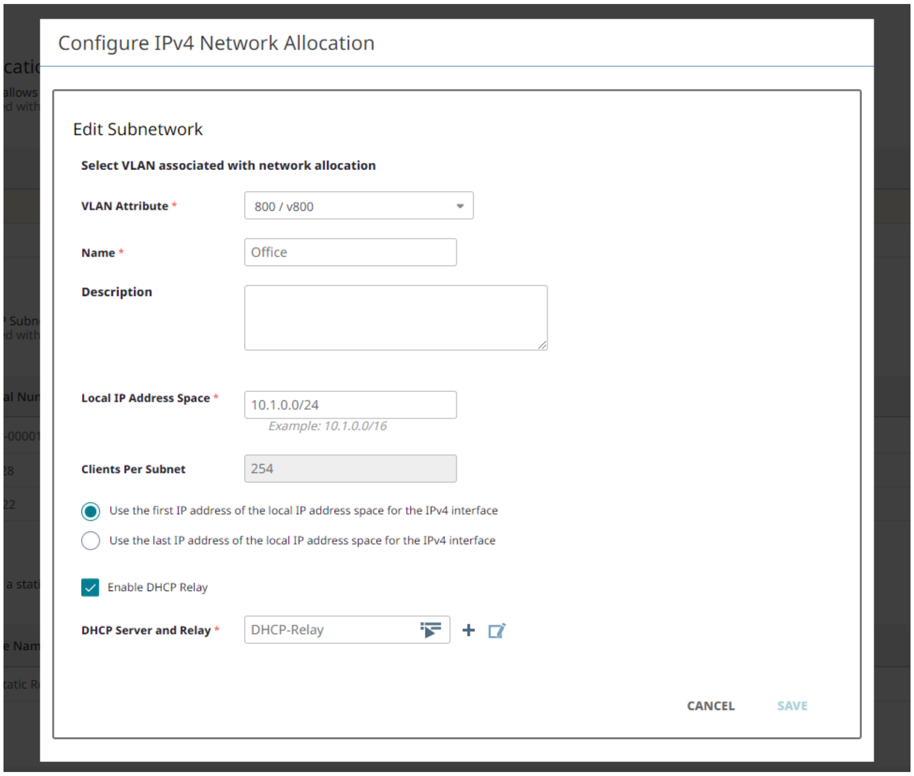
Note
A VLAN defined within Instant Port Profiles as Non-Forwarding cannot be used to create a subnetwork.

On the **Network Allocation** page, you can add, edit, or delete Network Allocation configurations. The table includes the following parameters:

- Name
- Description
- IPv4 Subnetwork
- Clients Per Subnet
- DHCP Relay
- VLAN Name
- VLAN ID
- VLAN Used By

Use this task to configure Network Allocation at the template level.

1. Go to **Configure** > **Network Policies**.
2. Create or select a Network Policy.
3. Select **Switching** > **Routing** > **Network Allocation**.
4. Select + to add or ✎ to edit.



Configure IPv4 Network Allocation

Edit Subnetwork

Select VLAN associated with network allocation

VLAN Attribute * 800 / v800

Name * Office

Description

Local IP Address Space * 10.1.0.0/24
Example: 10.1.0.0/16

Clients Per Subnet 254

● Use the first IP address of the local IP address space for the IPv4 interface

○ Use the last IP address of the local IP address space for the IPv4 interface

☑ Enable DHCP Relay

DHCP Server and Relay * DHCP-Relay

Figure 23: Network Allocation

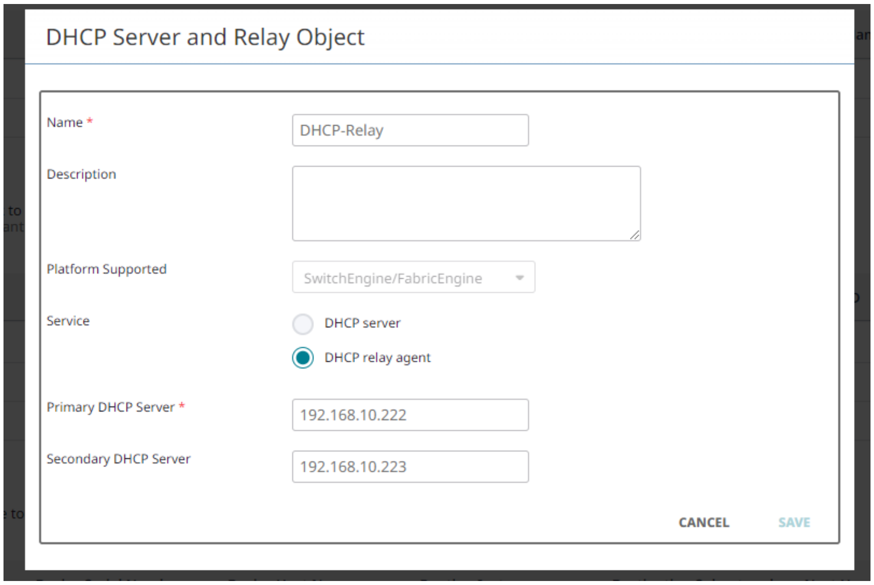
5. Configure the following IPv4 Network Allocation settings:

Table 12: Network Allocation Settings

Setting	Description
VLAN Attribute	A VLAN attribute can be created from within the VLAN attribute section within the Network Policy Switching Section.
Name	The name of your subnetwork.
Description	A description of your subnetwork.
Local IP Address Space	Define the local IP address space using CIDR notation, such as `10.1.0.0/16`. At the template level the IP address must be the valid network address and not a host address within the subnet range you are creating. For more Information, see Template-level IP Address Specifications on page 73.
Clients Per Subnet	Shows the clients per subnet.

Table 12: Network Allocation Settings (continued)

Setting	Description
Select One	- Use the first IP address of the local IP address space for the IPv4 interface - Use the last IP address of the local IP address space for the IPv4 interface
Enable DHCP Relay	Enable DHCP Relay. If enabled, select or create a DHCP Relay Common Object. For more information, see Figure 24.



DHCP Server and Relay Object

Name * DHCP-Relay

Description

Platform Supported SwitchEngine/FabricEngine

Service ○ DHCP server ● DHCP relay agent

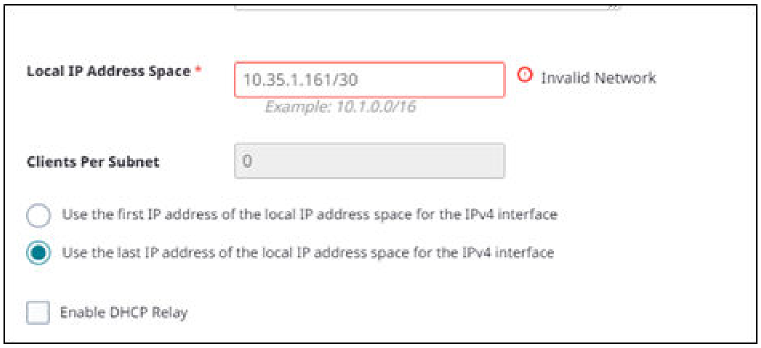
Primary DHCP Server * 192.168.10.222

Secondary DHCP Server 192.168.10.223

Figure 24: DHCP Server and Relay Object

Template-level IP Address Specifications

If 10.35.1.161/30 is the host address, then to create a valid Network Allocation entry in the network policy switch routing section you must introduce 10.35.1.160/30 in the Local IP Address Space field or you will receive an "Invalid Network" error.



Local IP Address Space * 10.35.1.161/30 Invalid Network

Example: 10.1.0.0/16

Clients Per Subnet 0

○ Use the first IP address of the local IP address space for the IPv4 interface

● Use the last IP address of the local IP address space for the IPv4 interface

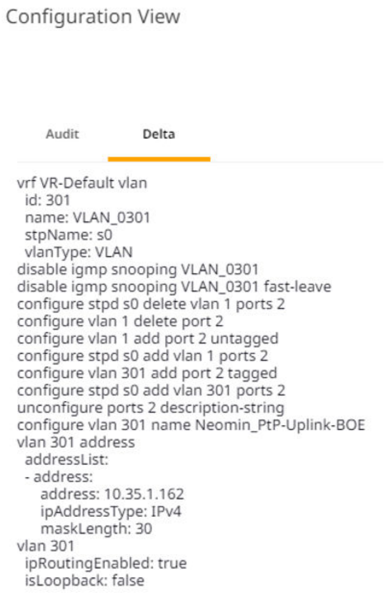
□ Enable DHCP Relay

Figure 25: Error Message

Using 10.35.1.160 will create the following IP Address parameters:

- Network Address (10.35.1.160) - Can be used in the Network Allocation table.
- Usable Host IP Range (10.35.1.161 - 10.35.1.162) - Can be used in the Routing table.
- Broadcast Address (10.35.1.163) - Unable to use for ExtremeCloud IQ or NOS.

When entries are added in a Routing table, the IPv4 Address / Subnet Mask is valid if a host address is used, and this is the IP address that will be configured on the VLAN.



```
vrf VR-Default vlan
  id: 301
  name: VLAN_0301
  stpName: s0
  vlanType: VLAN
disable igmp snooping VLAN_0301
disable igmp snooping VLAN_0301 fast-leave
configure stpd s0 delete vlan 1 ports 2
configure vlan 1 delete port 2
configure vlan 1 add port 2 untagged
configure stpd s0 add vlan 1 ports 2
configure vlan 301 add port 2 tagged
configure stpd s0 add vlan 301 ports 2
unconfigure ports 2 description-string
configure vlan 301 name Neomin_PtP-Uplink-BOE
vlan 301 address
  addressList:
  - address:
      address: 10.35.1.162
      ipAddressType: IPv4
      maskLength: 30
vlan 301
  ipRoutingEnabled: true
  isLoopback: false
```

Figure 26:

Network Allocation - Routing

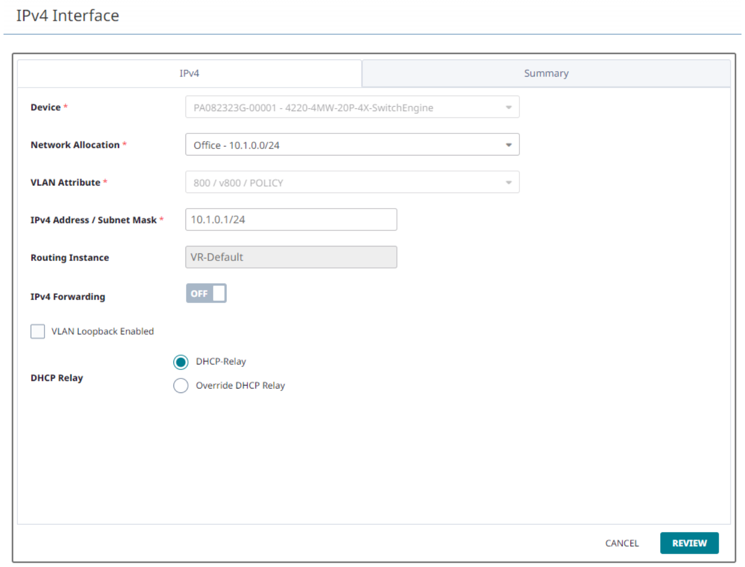
Use routing to assign an IP subnetwork to a device.

> **Note**
> A VLAN defined within Instant Port Profiles as Non-Forwarding cannot be used to create a routing interface.

Use this task to configure routing.

1. Go to **Configure** > **Network Policies**.
2. Create or select a network policy.
3. Select **Switching** > **Routing** > **Network Allocation** and scroll to the Routing table.

4. Select + to add or ✎ to edit.



IPv4 Interface

Device * PA082323G-00001 - 4220-4MW-20P-4X-SwitchEngine

Network Allocation * Office - 10.1.0.0/24

VLAN Attribute * 800 / v800 / POLICY

IPv4 Address / Subnet Mask * 10.1.0.1/24

Routing Instance VR-Default

IPv4 Forwarding OFF

□ VLAN Loopback Enabled

DHCP Relay ● DHCP-Relay ○ Override DHCP Relay

Figure 27: IPv4 Interface

5. Configure the following routing settings:

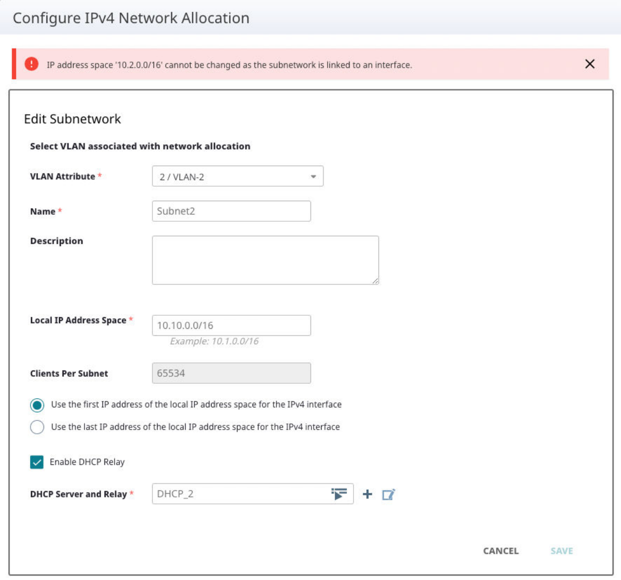
Table 13: Routing Attributes

Field	Description
Device (Mandatory)	Select a Device from the drop-down menu. Only standalone or stack EXOS/ Switch Engine switches with this policy assigned can be selected.
Network Allocation (Mandatory)	Select a Network Allocation from the drop-down menu. Note: You cannot assign a device to the same subnetwork twice or multiple subnetworks referencing the same VLAN ID or subnetworks with overlapping subnet space.
VLAN Attribute (Read-only)	Select a VLAN Attribute from the drop-down menu. Note: This field displays <VLAN ID> / <VLAN name> / <VLAN attribute created from>. For IPv4 interfaces created from a network policy, it will display the VLAN ID and VLAN name from the selected subnetwork and "POLICY" as the source for the VLAN attribute.

Table 13: Routing Attributes (continued)

Field	Description
IPv4 Address / Subnet Mask (Mandatory)	Shows the assigned IP Address, such as `10.1.0.0/16`. Note: IPv4 address must be a host address within the same subnet space as the selected subnetwork.
Routing Instance (Read-only)	Shows the Routing Instance. Note: IPv4 interfaces can only be created within VR-Default.
IPv4 Forwarding	Enables/disables IPv4 forwarding.
VLAN Loopback	**Enable** or **Disable** VLAN Loopback.
DHCP Relay (Read-only)	DHCP Relay configured within the selected subnetwork or allows overriding DHCP Relay from subnetwork with a custom configuration.

6. By selecting a device when creating an IPv4 interface, the routing feature allows you to perform device-level configuration from a network policy. The entries from Routing table generates delta only for those devices selected when the IPv4 interfaces have been created.



Configure IPv4 Network Allocation

IP address space '10.2.0.0/16' cannot be changed as the subnetwork is linked to an interface.

Edit Subnetwork

Select VLAN associated with network allocation

VLAN Attribute * 2 / VLAN-2

Name * Subnet2

Description

Local IP Address Space * 10.10.0.0/16

Example: 10.1.0.0/16

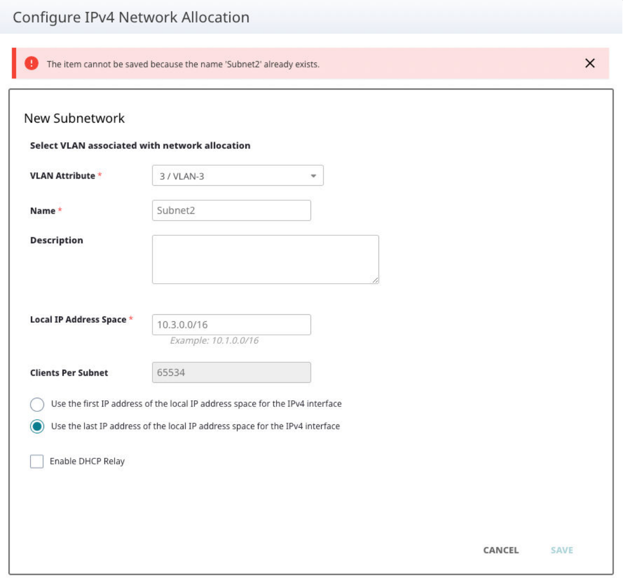
Clients Per Subnet 65534

● Use the first IP address of the local IP address space for the IPv4 interface

○ Use the last IP address of the local IP address space for the IPv4 interface

☑ Enable DHCP Relay

DHCP Server and Relay * DHCP_2



Configure IPv4 Network Allocation

The item cannot be saved because the name 'Subnet2' already exists.

New Subnetwork

Select VLAN associated with network allocation

VLAN Attribute * 3 / VLAN-3

Name * Subnet2

Description

Local IP Address Space * 10.3.0.0/16

Example: 10.1.0.0/16

Clients Per Subnet 65534

○ Use the first IP address of the local IP address space for the IPv4 interface

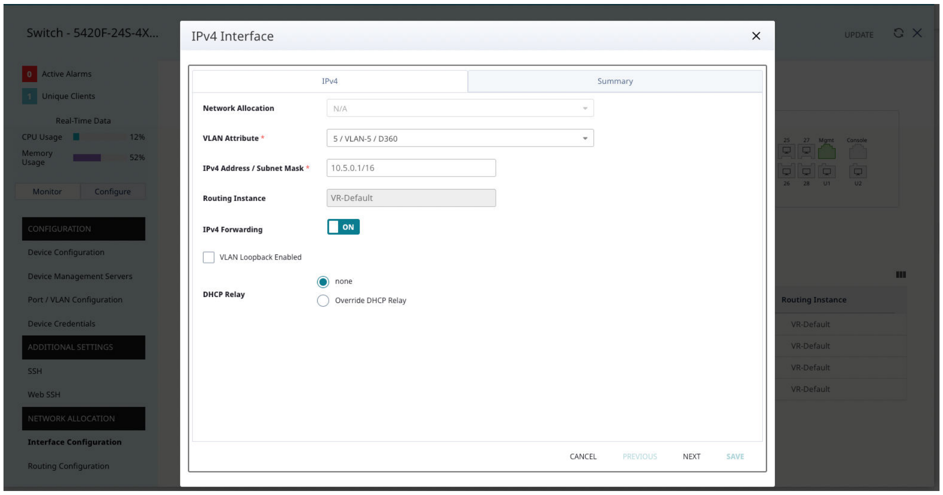
● Use the last IP address of the local IP address space for the IPv4 interface

□ Enable DHCP Relay

7. Device-level IPv4 interface configuration can be performed also from device-level page of each device which has a policy assigned: go to **Manage** > **Devices** and select the supported device. Select **Configure** > **Network Allocation** > **Interface Configuration**.

Note

When creating an IPv4 interface from this page, the Network Allocation field is grayed out, a VLAN attribute must be selected instead. While Port / VLAN Configuration is locked, only VLAN attributes created from the assigned network policy can be selected. VLAN IDs or IPv4 addresses from the same subnetwork can only be configured once to a device.



IPv4 Interface

Network Allocation N/A

VLAN Attribute * 5 / VLAN-5 / D360

IPv4 Address / Subnet Mask * 10.5.0.1/16

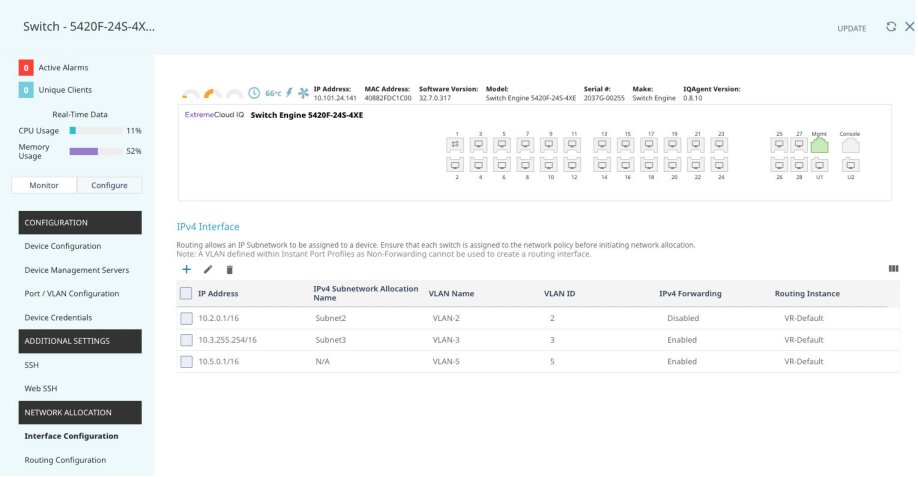
Routing Instance VR-Default

IPv4 Forwarding ON

□ VLAN Loopback Enabled

DHCP Relay ● none ○ Override DHCP Relay

8. All IPv4 interfaces created from a network policy for a specific device are displayed and can be edited also from the device-level page of that device and vice-versa.



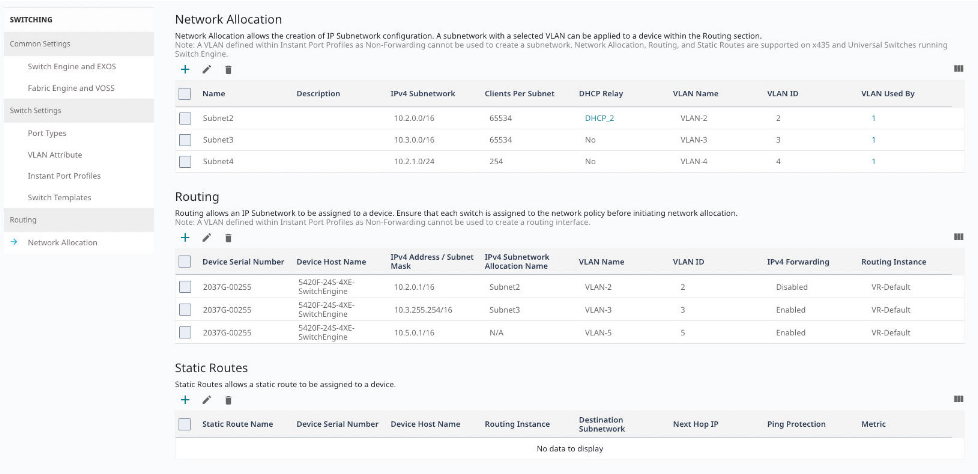
IP Address: 10.101.24.141
MAC Address: 40882FDC1C00
Software Version: 32.7.0.317
Model: Switch Engine 5420F-24S-4XE
Serial #: 2037G-00255
Make: Switch Engine
IQAgent Version: 0.8.10

Switch Engine 5420F-24S-4XE

IPv4 Interface

Routing allows an IP Subnetwork to be assigned to a device. Ensure that each switch is assigned to the network policy before initiating network allocation.
Note: A VLAN defined within Instant Port Profiles as Non-Forwarding cannot be used to create a routing interface.

IP Address	IPv4 Subnetwork Allocation Name	VLAN Name	VLAN ID	IPv4 Forwarding	Routing Instance
10.2.0.1/16	Subnet2	VLAN-2	2	Disabled	VR-Default
10.3.255.254/16	Subnet3	VLAN-3	3	Enabled	VR-Default
10.5.0.1/16	N/A	VLAN-5	5	Enabled	VR-Default



Network Allocation

Network Allocation allows the creation of IP Subnetwork configuration. A subnetwork with a selected VLAN can be applied to a device within the Routing section.
Note: A VLAN defined within Instant Port Profiles as Non-Forwarding cannot be used to create a subnetwork. Network Allocation, Routing, and Static Routes are supported on x435 and Universal Switches running Switch Engine.

Name	Description	IPv4 Subnetwork	Clients Per Subnet	DHCP Relay	VLAN Name	VLAN ID	VLAN Used By
Subnet2		10.2.0.0/16	65534	DHCP_2	VLAN-2	2	1
Subnet3		10.3.0.0/16	65534	No	VLAN-3	3	1
Subnet4		10.2.1.0/24	254	No	VLAN-4	4	1

Routing

Routing allows an IP Subnetwork to be assigned to a device. Ensure that each switch is assigned to the network policy before initiating network allocation.
Note: A VLAN defined within Instant Port Profiles as Non-Forwarding cannot be used to create a routing interface.

Device Serial Number	Device Host Name	IPv4 Address / Subnet Mask	IPv4 Subnetwork Allocation Name	VLAN Name	VLAN ID	IPv4 Forwarding	Routing Instance
2037G-00255	5420F-24S-4XE-SwitchEngine	10.2.0.1/16	Subnet2	VLAN-2	2	Disabled	VR-Default
2037G-00255	5420F-24S-4XE-SwitchEngine	10.3.255.254/16	Subnet3	VLAN-3	3	Enabled	VR-Default
2037G-00255	5420F-24S-4XE-SwitchEngine	10.5.0.1/16	N/A	VLAN-5	5	Enabled	VR-Default

Static Routes

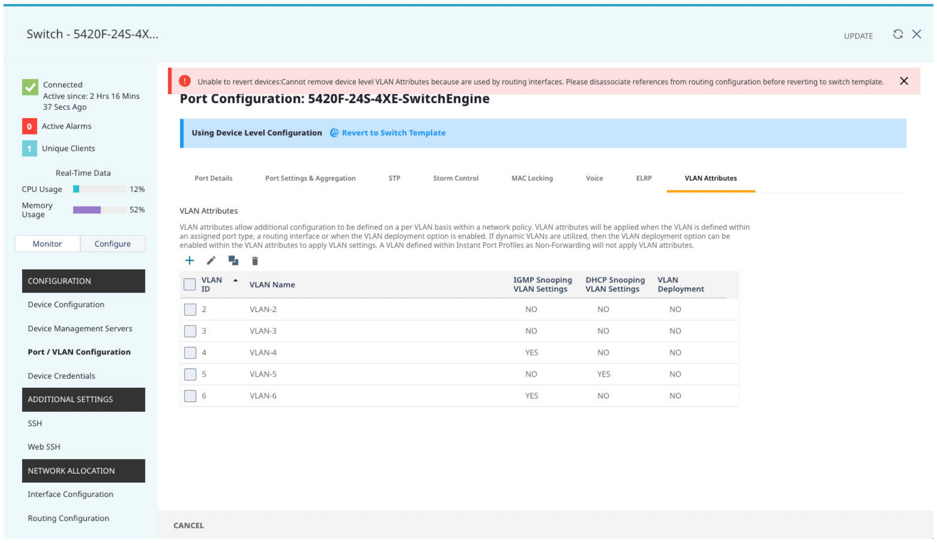
Static Routes allows a static route to be assigned to a device.

Static Route Name	Device Serial Number	Device Host Name	Routing Instance	Destination Subnetwork	Next Hop IP	Ping Protection	Metric
No data to display							

Note

After unlocking Port / VLAN Configuration, when creating IPv4 interfaces from device-level configuration page, only VLAN attributes created from this page can be selected. Even with VLAN attributes configuration unlocked, IPv4 interfaces can be created from a network policy as long as for the VLAN ID of the selected subnetwork, there is a corresponding VLAN attribute in device-level configuration page.

9. Before reverting Port / VLAN Configuration back to the switch template, ensure for all the VLAN IDs of the IPv4 interfaces created while the configuration was unlocked, there are corresponding VLAN attributes within the network policy or the operation won't be allowed.
   When reverting to the switch template configuration, the system will link the IPv4 interfaces to the VLAN attributes defined in the network policy based on the VLAN ID. This process effectively unlinks the interfaces from the VLAN attributes associated with the device-level configuration, allowing for the deletion of those device-level VLAN attributes.



Switch - 5420F-24S-4X...

Unable to revert devices:Cannot remove device level VLAN Attributes because are used by routing interfaces. Please disassociate references from routing configuration before reverting to switch template.

Connected
Active since: 2 Hrs 16 Mins 37 Secs Ago

0 Active Alarms

1 Unique Clients

Real-Time Data

CPU Usage 12%

Memory Usage 52%

Port Configuration: 5420F-24S-4XE-SwitchEngine

Using Device Level Configuration Revert to Switch Template

VLAN Attributes

VLAN attributes allow additional configuration to be defined on a per VLAN basis within a network policy. VLAN attributes will be applied when the VLAN is defined within an assigned port type, a routing interface or when the VLAN deployment option is enabled. If dynamic VLANs are utilized, then the VLAN deployment option can be enabled within the VLAN attributes to apply VLAN settings. A VLAN defined within Instant Port Profiles as Non-Forwarding will not apply VLAN attributes.

□	VLAN ID	VLAN Name	IGMP Snooping VLAN Settings	DHCP Snooping VLAN Settings	VLAN Deployment
□	2	VLAN-2	NO	NO	NO
□	3	VLAN-3	NO	NO	NO
□	4	VLAN-4	YES	NO	NO
□	5	VLAN-5	NO	YES	NO
□	6	VLAN-6	YES	NO	NO

Note
A VLAN defined within Instant Port Profiles as Non-Forwarding cannot be used to create a routing interface, an error message will be displayed when checking delta or before pushing the configuration on the device.

Note
The VLAN defined within Management Interface Settings cannot be used to create a routing interface, an error message will be displayed when trying to create the IPv4 interface. If a VLAN used by an existing IPv4 interface is configured within Management Interface Settings, an error message will be displayed when checking delta or before pushing the configuration on the device.

Note
IPv4 interfaces with IPv4 address in the same subnet as IPv4 address configured from Management Interfaces Settings cannot be created, an error message will be displayed when trying to create the IPv4 interface. When configuring the IPv4 address within Management Interface Settings in the same subnet as an existing IPv4 interface, an error message will be displayed when checking delta or before pushing the configuration on the device.

Note
The management interface defined within Management Interface Settings is displayed as read-only in IPv4 routing interfaces tables from both device-level configuration page and network policy.

Static Routes

Static route configuration in a Network Policy allows you to create one static route entry and assign that static route entry to multiple devices. The device is required to have the corresponding directly connected interface present in the routing section.

If adding a static route configuration at device-level, then the device is still required to have a corresponding directly connected interface present in the device-level routing section.

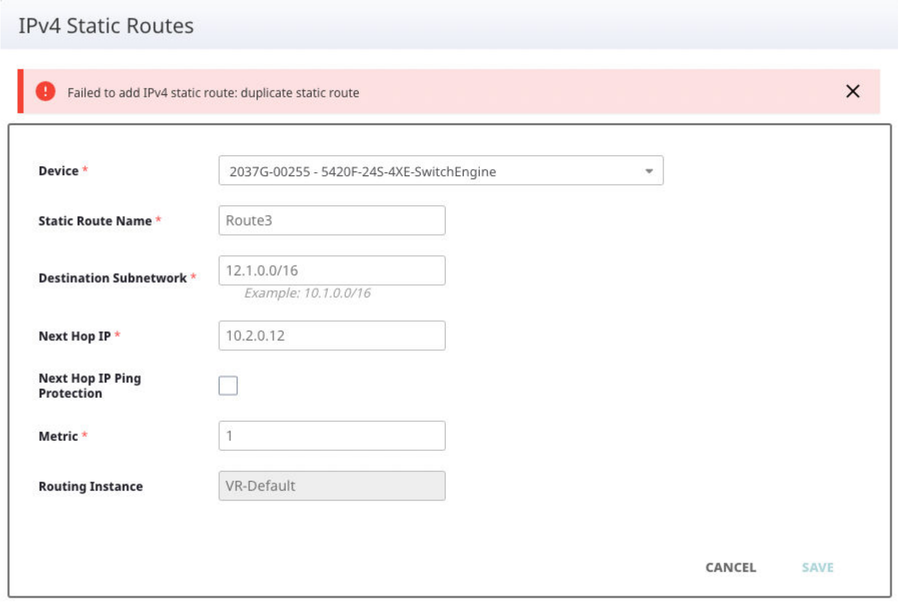
To configure Static Routes:

1. Go to **Configure** > **Network Policies**.
2. Create or select a Network Policy.
3. Select **Switching** > **Routing** > **Network Allocation** and scroll to the Static Routes table.
4. Select + to add or ✎ to edit.
5. Enter the Static Route Attributes according to the table below:

Table 14: Static Route Attributes

Setting	Description
Device (Mandatory)	Select a Device from the **drop-down menu**. Only standalone or stack EXOS/Switch Engine switches having this policy assigned can be selected.
Static Route Name (Mandatory)	Enter the name of the Static Route.
Destination Subnet (Mandatory)	Enter the desired subnet address, such as `10.1.0.0/16`.
Next Hop IP (Mandatory)	Enter the desired IP Address for the next Hop, such as `123.321.132.312`. Must be in the same subnetwork with at least one of the IPv4 interfaces configured for the device. Next hop IP cannot be configured with the same IPv4 address as that of the interface configured for device.
Next Hop IP Ping Protection (Mandatory)	**Enable** or **Disable** Next Hop IP Ping Protection. Note: Enabling Ping Protection will generate a Ping Protection Status tool tip when viewing your device within **Manage** > **Devices** > **Monitoring** > **Routing**.
Metric (Mandatory)	Enter your desired metric value from 1 to 255.
Routing Instance (Read-only)	Shows the Routing Instance. Note: IPv4 static routes can only be created within VR-Default.

You cannot configure the same static route twice for the same device. A static route is defined by the following parameters: destination subnetwork, next hop IP, and routing instance.



IPv4 Static Routes

Failed to add IPv4 static route: duplicate static route

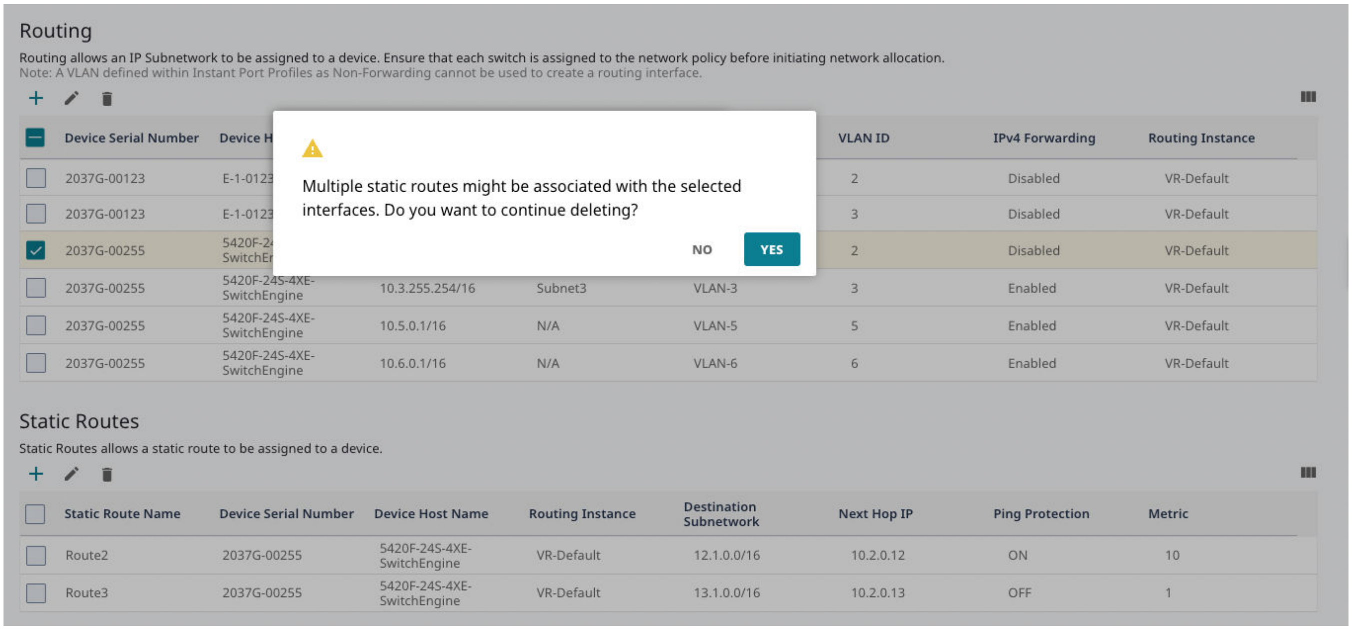
Device *	2037G-00255 - 5420F-24S-4XE-SwitchEngine
Static Route Name *	Route3
Destination Subnetwork *	12.1.0.0/16 Example: 10.1.0.0/16
Next Hop IP *	10.2.0.12
Next Hop IP Ping Protection	□
Metric *	1
Routing Instance	VR-Default

By selecting a device when creating an IPv4 static route, routing feature allows device-level configuration to be performed from a network policy. The entries from Static Routes table will generate delta only for those devices selected when the IPv4 static routes have been created.

6. Device-level IPv4 static route configuration can also be performed also from page of each device which has a policy assigned: go to **Manage** > **Devices** and select the supported device. Select **Configure** > **Network Allocation** > **Routing Configuration**.

Note
All IPv4 static routes created from a network policy for a specific device are displayed and can be edited also from the device-level page of that device and vice-versa.

7. Since every IPv4 static route is linked to an IPv4 interface, when deleting an IPv4 interface all static routes linked to, you must confirm the actions.



Routing

Routing allows an IP Subnetwork to be assigned to a device. Ensure that each switch is assigned to the network policy before initiating network allocation.
Note: A VLAN defined within Instant Port Profiles as Non-Forwarding cannot be used to create a routing interface.

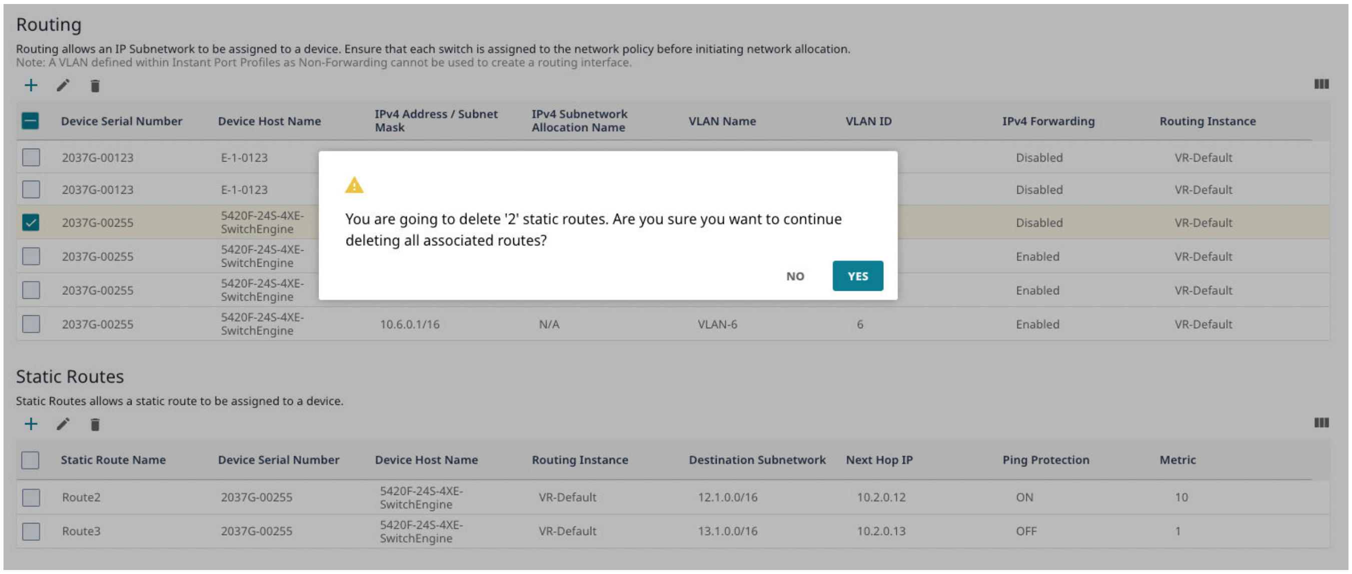
	Device Serial Number	Device H				VLAN ID	IPv4 Forwarding	Routing Instance
□	2037G-00123	E-1-0123				2	Disabled	VR-Default
□	2037G-00123	E-1-0123				3	Disabled	VR-Default
☑	2037G-00255	5420F-24 SwitchEr				2	Disabled	VR-Default
□	2037G-00255	5420F-24S-4XE-SwitchEngine	10.3.255.254/16	Subnet3	VLAN-3	3	Enabled	VR-Default
□	2037G-00255	5420F-24S-4XE-SwitchEngine	10.5.0.1/16	N/A	VLAN-5	5	Enabled	VR-Default
□	2037G-00255	5420F-24S-4XE-SwitchEngine	10.6.0.1/16	N/A	VLAN-6	6	Enabled	VR-Default

Multiple static routes might be associated with the selected interfaces. Do you want to continue deleting?

Static Routes

Static Routes allows a static route to be assigned to a device.

□	Static Route Name	Device Serial Number	Device Host Name	Routing Instance	Destination Subnetwork	Next Hop IP	Ping Protection	Metric
□	Route2	2037G-00255	5420F-24S-4XE-SwitchEngine	VR-Default	12.1.0.0/16	10.2.0.12	ON	10
□	Route3	2037G-00255	5420F-24S-4XE-SwitchEngine	VR-Default	13.1.0.0/16	10.2.0.13	OFF	1



Routing

Routing allows an IP Subnetwork to be assigned to a device. Ensure that each switch is assigned to the network policy before initiating network allocation.
Note: A VLAN defined within Instant Port Profiles as Non-Forwarding cannot be used to create a routing interface.

	Device Serial Number	Device Host Name	IPv4 Address / Subnet Mask	IPv4 Subnetwork Allocation Name	VLAN Name	VLAN ID	IPv4 Forwarding	Routing Instance
□	2037G-00123	E-1-0123					Disabled	VR-Default
□	2037G-00123	E-1-0123					Disabled	VR-Default
☑	2037G-00255	5420F-24S-4XE-SwitchEngine					Disabled	VR-Default
□	2037G-00255	5420F-24S-4XE-SwitchEngine					Enabled	VR-Default
□	2037G-00255	5420F-24S-4XE-SwitchEngine					Enabled	VR-Default
□	2037G-00255	5420F-24S-4XE-SwitchEngine	10.6.0.1/16	N/A	VLAN-6	6	Enabled	VR-Default

You are going to delete '2' static routes. Are you sure you want to continue deleting all associated routes?

Static Routes

Static Routes allows a static route to be assigned to a device.

□	Static Route Name	Device Serial Number	Device Host Name	Routing Instance	Destination Subnetwork	Next Hop IP	Ping Protection	Metric
□	Route2	2037G-00255	5420F-24S-4XE-SwitchEngine	VR-Default	12.1.0.0/16	10.2.0.12	ON	10
□	Route3	2037G-00255	5420F-24S-4XE-SwitchEngine	VR-Default	13.1.0.0/16	10.2.0.13	OFF	1

Note

When editing an IPv4 static route, only Next Hop IP Ping Protection and Metric fields can be changed. To change the other fields, create a new static route after deleting the existing one.

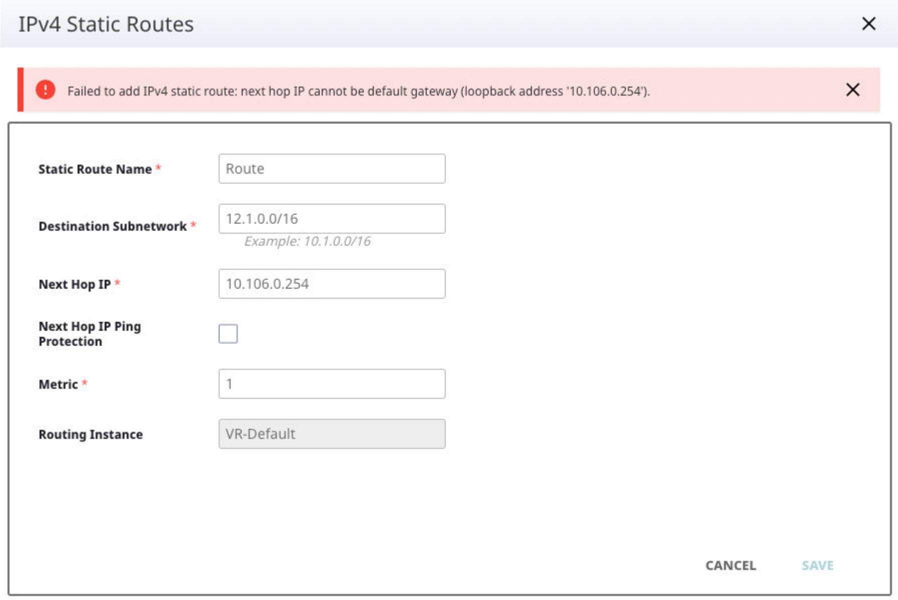
8. When editing an IPv4 interface which is linked to an IPv4 static route (next hop IP of a static route is in the same subnet as the IPv4 address of the routing interface), IPv4 address field cannot be changed anymore. The rationale behind this restriction is to not invalidate existing static routes.

   Note

   The default route defined within Management Interface Settings using Static Address option is displayed as read only in IPv4 static routes tables from both the device-level configuration page and network policy. In the device-level configuration page, the default static route name has a hyperlink to Management Interface Settings from the Device Configuration tab.

   Note

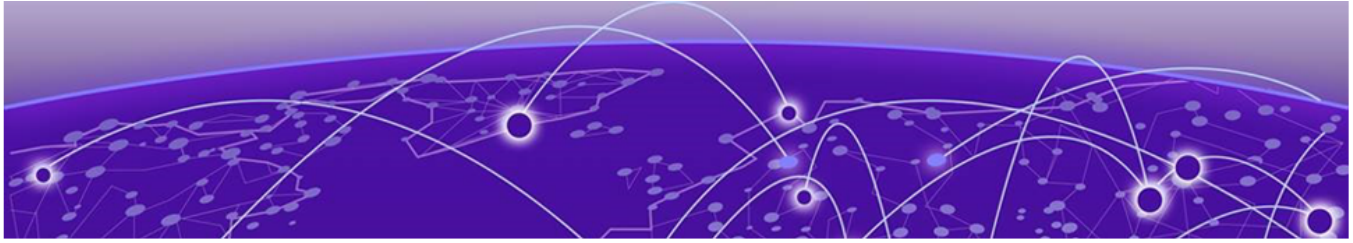
   When creating an IPv4 static route, next hop IP cannot be default gateway defined within Management Interface Settings using Static Address option.



IPv4 Static Routes

Failed to add IPv4 static route: next hop IP cannot be default gateway (loopback address '10.106.0.254').

Static Route Name *	Route
Destination Subnetwork *	12.1.0.0/16 *Example: 10.1.0.0/16*
Next Hop IP *	10.106.0.254
Next Hop IP Ping Protection	□
Metric *	1
Routing Instance	VR-Default



Configure Switch Engine Device Switch Stacks

Stacking is a proven technology commonly used for increasing port density in a wiring closet. It simplifies the management of all the switches within the stack using a single IP address. You can stack up to eight switches. You can create a switch stack for Switch Engine devices only. You can create stacks automatically or manually, as long as they are of the same configuration.

- To automatically create stacks, see Instantly Create a Switch Engine Device Stack on page 84.
- To manually create switch stacks, see Configure a Switch Engine Device Switch Stack on page 85

Instantly Create a Switch Engine Device Stack

To instantly create a stack, onboard the switches into ExtremeCloud IQ using the ExtremeCloud IQ mobile app. Unbox the switches, connect the stacking/power/uplink cables, and push the **Mode** button until the **STK LED** lights up. Hold down the **Mode** button for at least 5 seconds, until all the front-panel port LEDs flash. The stack forms automatically, all the slots reboot, and ExtremeCloud IQ detects the newly formed stack.

Note
In Switch Engine or EXOS, if you are replacing a failed stack member with the same model switch, the replacement slot is handled with the **Replace Stack Members** action. On X440-G2 /5320/5420/5520 stacks, select the stack, and select the **Replace Stack Members** action within **Utilities**. Select the member, enter the serial number, and select **Replace**.

Use this task to instantly configure a Switch Engine stack in ExtremeCloud IQ.

1. Go to **Manage** > **Devices**.
2. Find the new stack in the **Devices List** and select its check box.
3. In the **Template** column, select **Assign/Create Template**.
4. Select the **Create template based on currently selected device.**

5. Select an existing stack template from the drop-down list.
6. Select **Assign**.

The assigned template now displays in the **Policy** column. To make any changes to the individual devices in the stack at the device level, see Configure Device-Specific Settings on page 87.

Configure a Switch Engine Device Switch Stack

A stack is two or more Switch Engine devices inserted into slots and cabled together. When onboarding stacks, you see one entry for each slot when first adding serial numbers.

Use this task to configure a Switch Engine device switch stack. If you select a default template, you must copy it by saving it as a new template. This carries all the settings in the default template and let you customize it as required.

> **Note**
> Do not to make any changes in the default template. Always create a copy and make changes to the cloned version.

1. Go to **Configure** > **Network Polices**, the existing network policy, and the **Device Template** tab.
2. Select an existing Stack Template.
3. Select ⧉ to clone the template.
4. The cloned template requires a new **Save As** name to be entered and the **Clone to policy** to be selected.
5. To create a brand new template not based on an existing default, select +.
6. Enter a name for the new template.
7. To add additional devices to the Stack, select the **Add** button under the **Stack Template Name**.
8. Select **Save**.

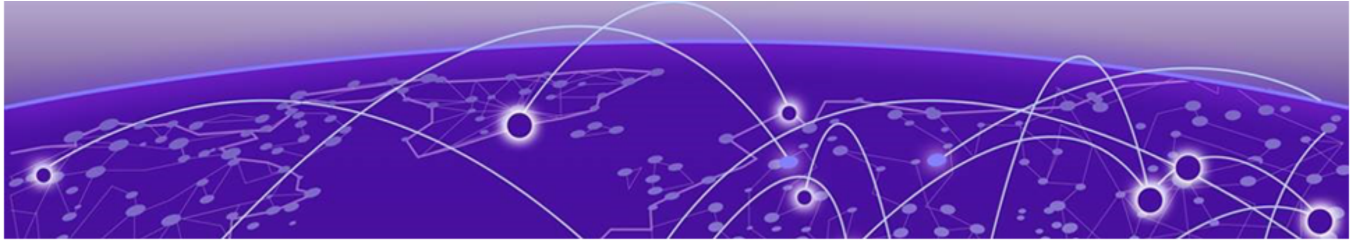
   The new or cloned switch stack template displays on the network policy's **Switch Template** page.
9. Select the template to display the **Device Template** configuration page.
10. Refer to Configure a Device Template on page 28.

    > **Note**
    > Repeat the Device Template configuration steps for each device in the stack.

11. Save the configuration.

After the stack is configured and operational, all slots will consolidate into a single stack object in ExtremeCloud IQ. It can take up to 15 minutes for the slots to consolidate and for ExtremeCloud IQ to recognize all slots as online. You might see a red icon in ExtremeCloud IQ if slots are offline or have not yet onboarded.

For any post-configuration switch stack issues, see Switch Stack Issues on page 106. Now that you have created the switch stack, you can automatically create more if they are configured exactly the same way. See Instantly Create a Switch Engine Device Stack on page 84.



Configure Device-Specific Settings

Use ExtremeCloud IQ to modify switch templates at the device level. Settings made at this level (**Manage** > **Devices** > **`switch_name`** > **Configure**) apply only to the device and override the template settings configured in the network policy. If you undo the device-level settings, the device automatically reverts back to the original network policy and device template configuration. To revert to the settings in the network policy, select **Actions** from above the Device List. To configure settings at the network policy level, see Configure the Network Policy on page 24.

After you select a switch from the Device List, you can create or modify the following for the specific device:

- **Device Configuration**: edit device details such as the host name, the description, the device function, IP addresses, and VLAN assignments. See Configure Devices on page 87.
- **Port Configuration**: edit port types, STP, Storm, and PSE settings. See Configure Device Ports and VLAN on page 89.
- **Device Credentials** (Switch Engine devices only): assign or change network administrator credentials and administrator assignments. See Configure Device Credentials on page 90.
- **SSH**: temporarily enable SSH in order to troubleshoot the device. See Configure SSH on page 91.

Configure Devices

Use this task to make device configuration changes at the device level, which overrides any equivalent settings in the network policy assigned to this device.

1. Go to **Manage** > **Devices**.

2. Select a device hostname to see a details panel for that device.
3. Hover over the icon at the top of the panel to see node type, IP address, host name, and VLAN assignments.
4. Select the **Configuration** tab.
5. Select **Device Configuration**.
6. You can edit any field that is selectable.
7. Use the add icon to create a new device template for this device.

   For information about device template creation, see Configure a Device Template on page 28.
8. Select **Save Configuration**.
9. To revert back to the network policy, from the **Devices** list, select the check box for this device, and from the **Actions** drop-down, use the **Revert Device Template to Device Defaults** option.

Device Management Servers

The **Device Management Servers** page does not appear until you apply a network policy to the device.

Use this task to override a network policy and make device-level changes to management server settings for a device. The changes affect only the specific device, not all devices associated with the network policy. You must **Unlock** before you can configure and save a device level management server configuration. You can use **Revert** to restore the network policy configuration overwrite any changes made at the device level.

Note
DNS Server, NTP Server, SNMP Server, and Syslog Server configurations can be managed at the device level for EXOS and Switch Engine devices after unlock. Not all management server tabs are available for all device types.

For stacks, the unlock and revert action applies to all units/slots within the page. This enables the full stack to revert to the currently assigned network policy. Also, the **Device Management Servers** is not available until you apply the network policy to both single switches and stacks.

1. Go to **Manage** > **Devices**.
2. Select the **HOST NAME** of the device you want to manage.
3. Select **Configure** > **Device Management Servers**.
4. Select **Unlock** from the top banner.

   Changes saved after you unlock the device override the associated network policy.
5. Select each server tab to make any necessary changes to the server settings, then select **SAVE CONFIGURATION**.

   The changes only apply at the device level. See *Configure Management Server Settings* in the *ExtremeCloud IQ Universal Switch Deployment Guide* for more information about management server configuration.
6. To update the device immediately, select **Update**.

7. Select the type of update, and then select **Save as Defaults** to save this option as the default action.
8. To update the device immediately, select **Perform Update**.

Configure Device Ports and VLAN

You can configure port and VLAN configuration details and settings at the device level. Device level settings always override any port configuration settings that were made in the device template for a network policy. You must first **Unlock** this page in order to change the device-specific port configuration. You can also return to the original template configuration with the **Revert** option.

Note

- Only the options available to the specific switch are displayed. For details about each option, see Configure Ports in Bulk on page 32.
- For 5520/5720 Universal Switches, VIM and partition mode are configurable at the device level.
- LLDP/CDP, MAC locking, STP Priority, BPDU Restrict, BPDU Restrict Recovery, Forwarding Delay, VLAN Attributes, and Max Age are configurable at the device level.
- BPDU Restrict and BPDU Recovery settings are found within the STP tab.

Use this task to configure device ports and VLAN details at the device level.

1. Go to **Manage** > **Devices**.
2. Select a switch **Host Name** to see a details panel for that switch.
3. Select the **Configure** tab.
4. Under **Configuration**, select **Port/VLAN Configuration**.
5. Select **Unlock** to enable switch-level configuration changes.
6. Select each tab, and edit any accessible field.
7. Select **Save Port Configuration**.

   Note
   BPDU Restrict and BPDU Restrict Recovery Timeout settings are found within the STP settings.

8. To revert back to the network policy switch template, select **Revert to Switch Template**.
9. To update the device immediately, select **Update**.
10. Select the type of update, and then select **Save as Defaults** to save this option as the default action.
11. To update the device immediately, select **Perform Update**.

VLAN Attributes

Use the VLAN attributes page to define additional configurations on a per-VLAN basis within a network policy. VLAN attributes are applied when the VLAN is defined within an assigned port type or when the VLAN deployment option is enabled. If dynamic

VLANs are utilized, then the VLAN deployment option can be enabled within the VLAN attributes page to apply VLAN settings.

> Note
> A VLAN defined within Instant Port Profiles as Non-Forwarding will not apply VLAN attributes.

To create a new VLAN Attribute:

1. Go to **Configure** > **Network Policies**.
2. Select a network policy.
3. Select **Switch Template** > **Switch Settings** > **VLAN Attributes**.
4. Select +.
5. Configure the following settings:

Table 15: VLAN Attributes

Setting	Description
Use VLAN common object	Select **Use VLAN common object** to automatically update the VLAN NAME and VLAN ID.
Manual	Select **Manual** to customize the following fields: • VLAN ID - The numerical identification number of the VLAN. This can be any currently unused number. • VLAN Name - The name of the VLAN.
IGMP Snooping VLAN Settings	Enable **IGMP Snooping** for switches to identify ports to which multicast group member hosts are attached in order to optimize the distribution of multicast traffic. Note: Enable **Immediate Leave** to remove multicast host immediately when it leaves the group.
DHCP Snooping VLAN Settings	Enable snooping of DHCP packets and creates a DHCP bindings database of IP to MAC addresses for this VLAN. Choose to enable DHCP Snooping, and the drop rogue DHCP packets action.
VLAN Deployments	With VLAN Deployments, VLAN and VLAN attributes can be created on switches when no port types are assigned with the defined VLAN.
Used By	How many devices use this VLAN. This field is system-generated.

6. Select **Save**.

Configure Device Credentials

You must select **Enable Device Management Settings for Switch Engine/EXOS Switches** under **Global Settings**. To do this, under your admin name at the top right of the ExtremeCloud IQ window, select **Global Settings** > **Administration** > **Device Management Settings**.

For Switch Engine devices only, use device credentials to set up login information for root or read-only administrators, change the name and password of the root admin, or add a read-only admin to a device. Device-level credentials offer access to devices through Telnet, SSH, or console connections.

A root admin has complete privileges, which include the ability to add, modify, and delete other administrators, and to reset the configuration. A read-only admin can view settings but cannot add, modify, or delete them. You can require that an admin be prompted for a password before accessing high-level privileged CLI commands.

1. Enter the **Admin Name** for the **Administrator Account**.
2. Create a password for this admin.

   Passwords must contain at least 8 characters, including at least one number, one special character, and one uppercase character.
3. Repeat the previous steps for the **Read Only Administrator**.
4. Select **Save Device Credentials**.
5. To revert back to the network policy, from the **Devices** list, select the check box for this device, and from the **Actions** drop-down, use the **Revert Device Template to Device Defaults** option.

Configure SSH

Before you can configure SSH access on a device, you must first enable SSH Availability. To do this, under your admin name at the top right of the ExtremeCloud IQ window, select **Global Settings** > **SSH Availability** and enable the feature.

ExtremeCloud IQ provides a way to access devices remotely using the SSH protocol by using an SSH proxy server. It is important to remember that while SSH access is available, your device is exposed to public access through an SSH proxy. The device is protected only by the device administrator credentials, because SSH FTP assumes that it is run over a secure channel. Use this task to enable SSH on a device from the device details panel, under **Configuration** > **Additional Settings** > **SSH**.

> Note
> The session is only valid for a single log-in attempt (even if unsuccessful).

1. Go to **Manage** > **Devices**.
2. Select a device hostname to see a details panel for that device.
3. Select **Additional Settings** > **SSH**.
4. Select the length of time that you want SSH to be available for this device.
5. Select **Enable SSH**.

   Provide assisting technicians with the onscreen instructions and device log-in credentials so they can open a session from their external SSH client to the specified IP address and port number of the proxy server.

6. When they are finished, select **Disable SSH**.

   The SSH session remains active for another minute or so and then automatically closes. If more time is required, enable a new SSH session.

Web SSH

ExtremeCloud IQ provides a way to access devices remotely using the SSH protocol from the web interface. Use the following steps access the web SSH:

> Note
> The Web SSH session automatically closes if the wrong username or password is entered.

1. Go to **Manage** > **Devices**.
2. Select a device hostname to see a details panel for that device.
3. Select **Additional Settings** > **Web SSH**.
4. Enter your username and password.
5. Select **Connect**.

Push the Device-Level Configuration to the Device

Perform any necessary configuration changes at the device level. After you save these changes, an exclamation mark displays in the device Status column, indicating the device configuration is now out of sync with the network policy.

Use this task to push any configuration changes made at the device level to the specific device, which will replace the exclamation mark with a green check. With ExtremeCloud IQ you can upgrade the device in two ways:

- Go to **Manage** > **Devices** > **Update Devices** on the Devices List page
- Go to **Manage** > **Devices** > `host_name` > **Update** on the Configure page.

1. Select one or more devices to update in the Devices List.
2. Select **Update Devices**.
3. If on the **Configure** page, select **Update**.
4. Select the option **Perform delta configuration update and resolve local device configuration which is out of sync with ExtremeCloud IQ**.
5. Select **Perform Update**.

   The status icon changes from an exclamation mark to a green check.
6. If you receive an out-of-sync error, hover over the message and review the details to reveal where the local configuration is out of sync.
   a. Match the out-of-sync local configuration within the network policy, switch template, or device level configuration and perform an update device again.

b. If Step a is not successful, select **Perform delta configuration update and resolve local device configuration which is out of sync with ExtremeCloud IQ**.

   Note
   The option **Perform delta configuration update and resolve local device configuration which is out of sync with ExtremeCloud IQ** requires a minimum version of Switch Engine 32.3 or Fabric Engine 8.9 installed on the switches.

Clone A Device

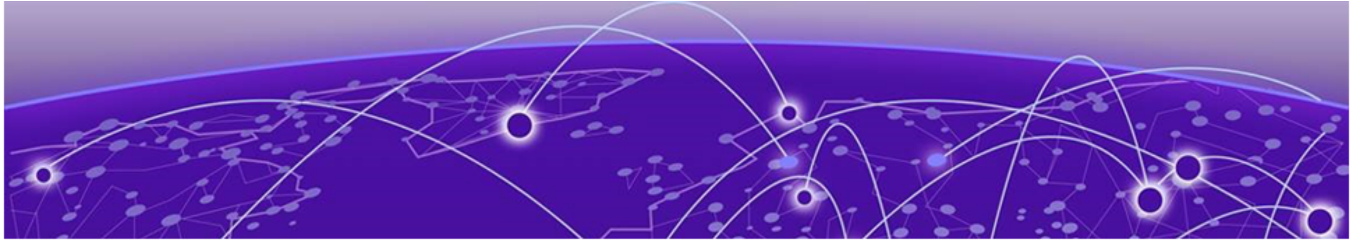
Use this task to apply the existing device-level configuration from one switch to a new switch with the same model. For example, if you need to replace one switch with another, this task describes how to do so and then apply the existing device-level configurations used by the previous switch.

Note
Licensing is not cloned.

1. Go to **Manage** > **Devices** and select the check box for the device in the **Device List**.
2. Select **Actions** > **Clone Device**.
3. (Optional) Select the **Perform full configuration clone** check box to clone additional configurations previously performed through supplemental CLI, SSH proxy, or local console saved on the original device with the same software version (minimum of 32.3.1.11).
4. Under **Replacement Device**, if the device is not yet **Onboarded**, select **Quick Onboard**, enter the device serial number and proceed to **Step 6**.

   If the device has already been **Onboarded**, proceed to **Step 5**.
5. Under **Replacement Serial Number**, select the appropriate device serial number.

   Note
   To onboard a Universal Hardware Switch, for the **Device OS**, choose **Switch Engine** or **Fabric Engine**.
6. Select **Clone**.
7. Select **Yes**.
8. Select **Perform Update** to push the configuration to all selected cloned devices.



Monitor Switches

The Monitor **Overview** tab is the default display that provides information about the overall health of the device. The page starts with the topology overview graphic at the top, followed by the device overall health timeline graph. By default, the timeline displays data for the last 24 hours. You can configure the time range for Day, Week, or Month, and for 1, 2, 4, 8, and 24 hour durations. This page also displays near real-time information for CPU, Memory, and Temperature displayed in widgets.

- Choose **Day** from the **Time Range** drop-down to see the event data in the timeline on an hourly basis.
- Choose **Week** or **Month** to see the data on a daily basis. You can also drag either side of the timeline to change it.
- Select **=** at the bottom right of this timeline to print it or to download it in a variety of file formats.

Hover the cursor over the different icons to display:

- **CPU Usage**
- **Memory**
- **MAC Table Utilization**
- **Last Seen** (uptime)
- **Temperature**
- **Power Supply Status**
- **Fan Status**

In the port graphic section, select an individual port to display its details. Under **Actions**, select the **Bounce Port** button to reset the port.

Port status is indicated as follows:

- Green = Connected
- Grey = Disconnected
- Red = Disconnected by Admin

Use **Run Cable Test** to test the physical cables connected to Switch Engine switch stack ports. See Use Cabletest for Switch Engine Device Duplex or Speed Issues on page 106.

A table of port details and Storm Control parameters follows the port graphic section, followed by the **Active Alarms** overview graphic.

To view the Storm Control parameters, select the **Storm Control** column from the column picker ▥.

Use the remaining Monitor tabs to view the following:

- **Interfaces**: Provides details of the VLAN and IPv4 interfaces. See Interfaces on page 95.
- **Client**: Provides details of the clients connected to the device. See Clients on page 98.
- **Diagnostics**: Displays details of the port diagnostics. See Diagnostics on page 98.
- **Events**: Provides details of the events that occur in the network for the selected device. See Events on page 98.
- **Alarms**: Provides details of alarms that can indicate network issues for a specific device which require Admin interaction. See Alarms on page 99.

Interfaces

Device Details for Interfaces

When you select the host name of an AP from the **Devices list** and then select **Monitor** > **Monitoring** > **Wireless Interfaces or Wired Interfaces**, the following information is displayed (APs only):

- At the top of the **Wireless** main section, you can adjust the time range by Day, Week, or Month, and for 1, 2, 4, 8, and 24 hour durations to view the Wi-fi channel utilization.
- Within the Wi-fi Health table, view the overall, SNR, channel utilization, and association per radio scores for 2.4 GHz, 5 GHz, 6GHz, and combined.
- The Total Clients, Clients with Poor Health, Surrounding BBSSIDs, CPU Usage, and Memory Usage are also displayed with tables for more specific details pertaining to channel utilization and wi-fi.
- The Surround Access Points table at the bottom of the page, displays the following columns:
    - MAC (BSSID)
    - SSID
    - Channel Width (MHz)
    - RSSI
    - Mode
    - Rogue AP / Friendly AP
    - Extreme Networks Device
    - CU (%)

  - CRC
  - # Clients

- At the top of the **Wired** main section, you can adjust the time range by Day, Week, or Month, and for 1, 2, 4, 8, and 24 hour durations to view CPU Usage, Memory Usage, Connected Clients, TX Bytes, RX Bytes, TX Errors, RX Errors, Discards TX, and Discards RX.
- The Total Clients and Number of Ports in Use are also displayed.
- The Interface Details table at the bottom of the page, displays the following columns by default:
  - Status
  - Interface
  - Port Type
  - Connected Clients
  - Speed
  - TX Bytes
  - RX Bytes
  - TX Errors
  - RX Errors
  - TX Drops
  - RX Drops
- Select the column picker ▥ to add additional columns or hide default columns:
  - LLDP Port #
  - LLDP Sys-ID
  - LLDP Sys-Name

When you select the host name of a switch from the **Devices list** and then select **Monitor** > **Monitoring** > **Interfaces** , the following information is displayed (Switches only):

- At the top of the main section, CPU Usage, Memory Usage, MAC Table Utilization, Last Seen time, Temperature, Power Supply Status, Fan Status, IP Address, MAC Address, Software Version, Device Model, Serial Number, Make, and IQAgent Version are all listed.
- The graphic below shows all of the ports on the device. Selecting a port displays more information.
- Within the VLAN tab are the VLAN Name, VLAN ID, Active Ports (Enabled port with VLAN assigned), STP Instance, IGMP Snooping, and DHCP Snooping information columns. Selecting a VLAN within the VLAN tab highlights the ports that are currently assigned.
- Within the IPv4 tab the VLAN Name, VLAN ID, IPv4 Forwarding, Routing Instance, and IP Address / Subnet information columns are displayed. The VLAN can be selected when the row is highlighted. Ports using the VLAN, both tagged and untagged that are actively provisioned, light up to indicate ports using the VLAN. Select a port to display the port name, port status, VLAN untagged/tagged status, and port actions.

Routing

Software version 32.6.2.68 or newer is required.

To monitor IPv4 Routing information:

1. Go to **Manage** > **Devices** and select a device.
2. From the **Device Details** page, select **Monitor** > **Monitoring** > **Routing**.

> Note
>
> You can refresh the IPv4 Routing table by selecting ↻ next to the **Last Polled** time.

The following information is available from the Route Monitor Polling Graph:

- A time range showing total number of routes within a 24 hour time period.
- Route type counts:
  - Direct Routes
  - Static Routes
  - OSPF Routes
  - Total Routes
- The Y axis resizes based on chosen routes.
- The Y axis represents the total number of routes.
- The X axis represents the poll time interval
- Hovering over the graph displays a summary of routes with the given timestamp.

> Note
> Select the graph heading to enable or disable the graph line view.

The following information is available from the IPv4 Routing table:

- Destination Subnetwork
- Next Hop
- VLAN Name
- VLAN ID
- Route Origin
- Status
- Metric
- Route Age
- Route Type Priority
- Routing Instance

You can filter for the Route Origin and Status.

> Note
> Up to 100 IPv4 Routes are visible within the table. For additional visibility use an SSH proxy.

Clients

The **Clients** tab provides details of the clients connected to the device. It includes the type of client, OS, connection status, Host Name, Client MAC address, the VLAN the client is in, and the IP address. Use the filter section to specify what displays in the table. You can also use the **Search** field to find a specific client.

Diagnostics

The **Diagnostics** tab provides detailed diagnostic timelines for ports, which includes transmit and received traffic, and port utilization over time.

By default, this timeline displays data for the last 24 hours, but you can choose from the following other options:

- Day, week, or month.
- 1, 2, 4, 8, and 24 hour durations.

You can also drag either side of a timeline to change it.

The **Port Congestion Pkt Drops** timeline shows the number of packets dropped due to port congestion over time.

Note
Select **=** at the bottom right of these timelines to print or to download them in a variety of file formats.

QoS Statistics

The **QoS Statistics** tab provides detailed diagnostic timelines for QoS Packets, and QoS Packet Congestion, over time.

By default, these timelines display data for the last 24 hours, but you can choose from the following other options:

- Day, week, or month.
- 1, 2, 4, 8, and 24 hour durations.

You can also drag either side of a timeline to change it.

For both QoS timelines, you can select QP 1-8 from the drop-down menu, to view the relevant timeline graph information.

Note
Select **=** at the bottom right of these timelines to print or to download them in a variety of file formats.

Events

A graphic at the top of this window shows the device and its network connections. Events that occur in the network for the selected device are recorded and displayed in this window. Table data is updated hourly. There is an **Events** tab and a **Configuration**

Events tab above the table. Configuration events show only changes to the device configuration, either from inside a network policy, or at the device level.

Use the key-ahead search field to search for an event by description. Use the column picker to customize the categories displayed in the table. By default, Timestamp, Severity, Category, and Description columns are displayed. Optional columns include Host Name, Device MAC, and Client MAC. You can download table data as a .csv file.

Sort the table by the event category using the drop-down list. To control how the information is presented, select any of the column headings. For example, if you want to organize the content by host name, select the **Host Name** heading.

Each alarm or event log entry consists of the following elements:

- **Type**: Indicates if the row represents an alarm or an event.
- **Timestamp**: Indicates the time in the month/day and time-of-day format that the alarm or event occurred.
- **Severity**: Indicates the severity of the alarm or event. The following can be displayed: Critical, Major, Minor, Info, and Clear.
- **Category**: Specifies the issue category that triggered the alarm or event. The following categories are available state change, client connection down, client connection change, static route ping protection, and DHCP rogue MAC detection.
- **Host Name**: The host name of the configured device on which the event occurred.
- **Device MAC**: The MAC address of the device that reported the alarm or event.
- **Client MAC**: The MAC address of the client that reported the alarm or event.

Alarms

Alarms can indicate network issues which require the attention of IT administrators. The following views are available:

- **Alarm Details**– Opens by default and contains a table showing all active alarms.
- **Timeline**– A visual display of alarms that occurred during a period of time that you specify. You can manipulate the timeline to show alarms for a specific time interval.

Note
The default time period for which alarms are displayed in both views is 24 hours.

Use the refresh icon to refresh the data that displays here. The Alarm Details table lists information about all active alarms. Use the column picker to select which columns are displayed. Your column selections are maintained even if you go to another window and return, and when you log out and log in again. Horizontal scrolling is available for this table when there are too many columns to fit in your display window.

Alarm Details default table columns include:

- **Status**: The status of the alarm.
- **Severity**: Major, minor, or informational.

- **Category**: The type of alarm, for example Agent alarm, Device disconnected, or Change OS.
- **Description** :A description of the alarm.
- **Time Raised**: The date and time when the alarm was reported.
- **Action**: Actions that can be taken with this alarm.

The following columns are optional:

- **Time Cleared**: The time that the alarm was cleared.
- **Cleared by**: The name of the person who cleared the alarm.

To remove one or more alarms, or remove redundant entries, select the check box next to the alarm, and then select **Clear Selected Alarms**. Cleared alarms then become events and are displayed in the event log.

To clear multiple alarms at the same time, either select the check box in the table header to select all alarms, select the check boxes individually, or shift-click to select check boxes for multiple alarms. Then select **Clear Selected Alarms**.

The **Alarms Timeline** is a visual indicator of when and how many active alarms have occurred. Select and drag inside the timeline to choose a specific time period within the seven-day time frame. The complete view of the timeline displays up to seven days of information. Select the menu icon to download alarm data. The Alarm Details table displays below the timeline.

Update Device Software

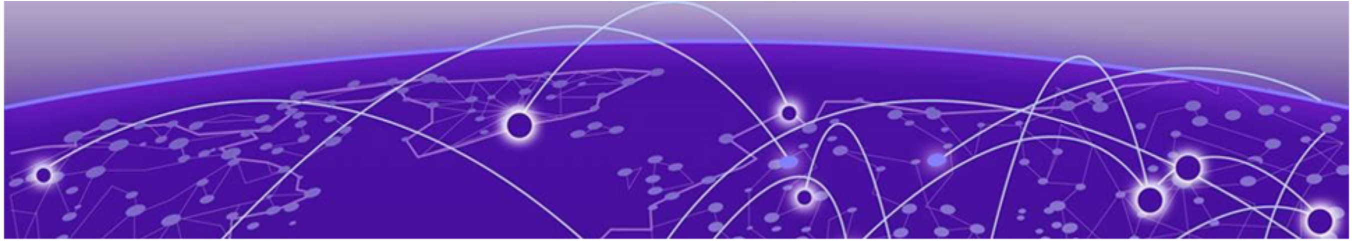
With ExtremeCloud IQ you can upgrade the device software images in two ways:

- Go to **Manage** > **Devices** > **Update Devices**
- Go to **Manage** > **Devices** > `host_name` > **Update**

Update the Device Software Images

Use this task to update the device software.

1. Go to **Manage** > **Devices** and select the check box for each device.
2. Select **Update Devices**.
3. If on the **Configure** page, select **Update**.
4. Select **Update IQ Engine and Switch Images**.
5. To upgrade the selected devices to the latest IQ Engine version on multiple device models, select **Upgrade to the latest version**.
6. For a single device or when you select multiple devices that are all the same device model:
    a. Select **Upgrade to the specific IQ Engine version**.
    b. Choose an image file from the drop-down menu of available IQ Engine releases.
    c. To add a local IQ Engine image to the drop-down list, select **Add/Remove**, and then **Choose**.
7. To update a device to a patch release, or if you have several IQ Engine versions running on the same device model, and you want to upgrade all of them to the same IQ Engine version, select **Upgrade even if the versions are the same**.
8. Select **Perform Update**.



Troubleshoot Switches

In the event you have issues after you onboard and configure your Universal switches, here are some possible areas for further exploration:

- You can have the device blink LED lights to physically show which device is selected. Refer to Locate Device Utility on page 103
- Make sure you have configured proper outbound firewall access. The device needs to be able to access the redirector on TCP 443, a DNS server in order to resolve the redirector IP address from its hostname, and to access an NTP server in order to get the correct time. If this access is not available, the secure connection to the redirector will fail. Refer to Configure Firewall Access on page 15.
- Ping the device or initiate a TraceRoute from within ExtremeCloud IQ. Refer to Establish CLI Access from ExtremeCloud IQ on page 103.
- Reset the device to factory defaults and push a fresh configuration. This also simultaneously resets the ExtremeCloud IQ device configuration. Refer to Reset the Device to Default Settings on page 103.
- Change the Management VLAN to something with no DHCP: As long as you operate with the latest OS code and firmware, this issue auto-corrects during reboot.
- **`Device Update Failed`**: Use your mouse to hover over this error message for more details, then refer to Device Update Failure on page 105.
- **`Incorrect VLAN or Trunk`**: Refer to VLAN or Trunk Issues on page 105.
- Switch Stack Issues: Refer to Switch Stack Issues on page 106.

- Switch Communication Issues: Refer to IQAgent and Switch Communication Issues on page 106.
- Cabletest: Use this tool as a last resort to check switch cables for duplex or speed issues in the event all other troubleshooting methods fail. Refer to Use Cabletest for Switch Engine Device Duplex or Speed Issues on page 106.
- Audit Logs: Access these at **Global Settings** > **Logs** > **Audit Logs**
- Configuration Events: Access these at **Manage** > **Devices** > **[select device]** > **Monitor** > **Events** > **Configuration Events**

Locate Device Utility

Use the Locate Device utility to alter the status LED on APs and Switch Engine devices so that you or an assistant at a remote site can locate the physical device more easily. You can also turn the LED off, which can be useful when an AP is mounted near a projection screen or is in a location where the light can be distracting.

1. Go to **Manage Device** and select a single device.
2. **Utilities** > **Tools**.
3. Select **Locate Device**.
4. Set the LED timeout, between 10-300 seconds.

   Note
   The default timeout is 300 seconds.

5. Select **Submit**.
6. To return the LED to normal operation, select **Return to normal LED operations**.

Establish CLI Access from ExtremeCloud IQ

Use this task to enter CLI commands for the selected device or devices without establishing a console cable connected to the device. For example, you can initiate a remote Ping or TraceRoute to a specific destination from a selected switch.

1. Go to **Manage** > **Devices**.
2. Select a device.
3. Select **Actions** > **Advanced** > **CLI Access**.
4. Enter the command and select **Apply**.

Reset the Device to Default Settings

Use this task to reset a device to factory settings.

Note
When you reset a device to factory defaults, you might create a network loop, depending on your network's topology. After you reset the device, make sure you re-deploy the network policy/template and any associated device-level configuration, and push a fresh update from ExtremeCloud IQ.

1. Go to **Manage** > **Devices**.

2. Select the device(s).
3. Select **Utilities** > **Reset Device to Default** .

Re-deploy the network policy/template and any associated device-level configuration, and push a fresh update from ExtremeCloud IQ.

Restart Power Supply Equipment (PSE)

Use this task to reset the PoE settings on all ports of PoE capable switches. Use the **Restart PSE** utility to power cycle all connected devices, without losing the power allocated to their ports.

Note
The utility immediately disables and then re-enables the ports for remote devices to be power-cycled. The **Restart PSE** utility affects only inline power.

1. Go to **Manage** > **Devices**.
2. Select the one or more devices to restart.
3. Select **Utilities** > **Restart PSE**.

Switch VLAN Probe

The VLAN probe function utilizes DHCP client on the switch to check for and display IP connectivity on a specified VLAN.

Note
The VLAN probe is skipped when the selected VLAN has a static IP address or is DHCP enabled.

Use this task to locate a VLAN in a complex network with multiple VLANs. You can also trigger VLAN probe for a Switch Engine device through the topology map.

To verify the VLAN probe results for a selected device:

1. Go to **Manage** > **Devices** select the associated device.
2. Select **Utilities** > **Tools** > **Switch VLAN Probe**.
3. Configure the following settings:

   VLAN Range

   Indicates the range of VLAN IDs to probe. Enter the start and end values. You can enter up to five ranges, separated by commas, up to a total range of 12. Range numbers cannot overlap. For example, 1,2-7,8,9-12.

   Probe Retries

   Indicates the number of probe retries. Valid values are 1-10.

   Timeout

   (Optional) Indicates how long to wait for a reply from each probe. Valid values are 5 to 60 seconds.
4. Select **Start** to start a probe.
5. Select **Stop** to stop a probe before it is complete.

6. Select **Clear** to clear entries for a probe.

   When the VLAN probe is complete, a table shows the host name, MAC address, available VLANs, unavailable VLANs, and their status.

Device Update Failure

This error indicates that a command on the switch failed to run or produced unexpected output. This can indicate that a manual or Supplemental CLI configuration conflicted with the configuration pushed by ExtremeCloud IQ. (See Configure Supplemental CLI on page 42). When ExtremeCloud IQ encounters this error, it attempts to push the same configuration delta again on the next update unless you create a different configuration.

Hover over this error message for more details.

1. Select the device and manually push the configuration by clicking **UPDATE DEVICES**.
2. If not successful, make a change to the configuration and push it.
3. If not successful, make changes to the device manually until you achieve a successful push.
4. If the device becomes isolated and changes are made to the device, correct an out-of-sync issue. See Push the Device-Level Configuration to the Device on page 92.
5. If you still get an error, reset the device.

   See Reset the Device to Default Settings on page 103.

VLAN or Trunk Issues

It is possible to update the switch into a state where it can no longer reach the cloud, and it becomes isolated. In this scenario, you must access the switch, manually reset it, delete it, and then add it back into ExtremeCloud IQ.

> **Note**
> You can make a change manually to correct the issue, but this can result in the switch configuration becoming out of sync with ExtremeCloud IQ. For information about correcting sync issues, see Push the Device-Level Configuration to the Device on page 92 for out-of-sync issues.

1. Access the device via SSH.
2. Use `unconfigure switch all` to manually reset the switch.
3. Delete the device from ExtremeCloud IQ.
4. Add the device back into ExtremeCloud IQ.
5. During a configuration update, select the **Reboot and Revert Extreme Networks Switch Configuration if IQAgent is unresponsive after configuration update** option.
6. For updates that disconnect a device, reconsider if your last update was appropriate and revisit the configuration for that port.

Switch Stack Issues

When onboarding stacks, you see one entry for each slot when first adding serial numbers. After the stack is configured and operational, all slots will consolidate into a single stack object in ExtremeCloud IQ. It can take up to 15 minutes for the slots to consolidate and for ExtremeCloud IQ to recognize all slots as online. You might see a red icon in ExtremeCloud IQ if slots are offline or have not yet onboarded.

If slots continue to show offline, ensure that all slots are powered and that stacking connections are up and active. CLI verification might be needed if issues persist.

1. Ensure that all slots are powered.
2. Ensure that stacking connections are up and active.
3. Perform CLI verification.

Switch Communication Issues

Before you begin become familiar with IQ Agent.

Here are some basic approaches to troubleshooting communication issues. Note that you can configure IQ Agent to use a specific VR or VLAN for Switch Engine.

1. In IQ Agent:
   a. To check the current status, use **`show iqagent`**.
   b. To discover onboarding issues, use **`show iqagent discovery detail`**.

      Issues that might arise can be that you cannot ping the cloud or resolve host names.
2. Use **`ping extremecloudiq.com`** to check for basic internet connectivity.
3. Use **`ping vr vr-mgmt extremecloudiq.com`** to check for basic internet connectivity if you are using the dedicated management port.
4. Use **`traceroute extremecloudiq.com`** to check where packets are dropped.
5. Use **`traceroute vr vr-mgmt extremecloudiq.com`** to check where packets are dropped if you are using the dedicated management port.
6. Use configure **`iqagent server vr <VR-Mgmt | VR-Default> vlan <vlan_name>`** to configure a specific VR and/or VLAN for IQ Agent to use.

Use Cabletest for Switch Engine Device Duplex or Speed Issues

Follow all previous troubleshooting steps in this chapter.

Use this test for active ports displayed on the **Device Details Monitor** page for Switch Engine switch stacks only.

1. Navigate to **Manage** > **Devices**.
2. Select the device host name.

   The **Device Details Monitor** page displays.
3. Scroll down to the port status graphic.
4. Select an active (green) port.

5. Scroll down to the **Actions** section.
6. Select **Run Cable Test**.
7. Select **OK** to proceed with the test.

    Note
    This test might temporarily interfere with port traffic.

8. If the test failed, checked the physical cable connected to the device.

Resolving Configuration Discrepancies in ExtremeCloud IQ

This section outlines how to correct out-of-sync configurations in ExtremeCloud IQ when configuration parameters on a managed switch have been changed outside the ExtremeCloud IQ user interface. These changes may occur during initial onboarding, troubleshooting, or when an admin is unaware that the switch is cloud-managed. Out-of-sync configurations can cause device updates to fail.

Important
To ensure smooth and consistent network operations, it is crucial to resolve these scenarios.

Out-of-sync configurations occur when modifying configuration parameters directly on the managed switch through the console, SSH proxy, or other remote sessions. Additionally, supplemental CLI managed outside of the ExtremeCloud IQ user interface also affects the configuration synchronization. Dynamic configuration changes of VLANs and or LAGs through other protocols can further affect the consolidation and synchronization of configurations.

Use this task to correct out-of-sync configurations in ExtremeCloud IQ and maintain a consistent and accurate configuration across managed switches.

1. Log in to ExtremeCloud IQ.
2. Navigate to the **Devices** section and select the affected switch from the list of managed devices.
3. Check the **Updated** column.

    If a device fails to update, the **Updated** column displays the ⓘ **Device Update Failed** status.
4. Select the **Device Update Failed** notification to open the **Configuration Events** page.

    Alternately, you can view device configuration events on the **Device** > **Monitor** > **Monitoring** > **Events** > **Configuration Events** page.

    ExtremeCloud IQ displays the specific configuration elements that are out-of-sync between ExtremeCloud IQ and the running configuration on the switch.

5. Choose one of the following options:
   - Override configuration from ExtremeCloud IQ: With this option, the configuration changes made in ExtremeCloud IQ are pushed to the switch, overwriting any discrepancies in the running configuration. The switch configuration aligns with the ExtremeCloud IQ-defined configuration. Click on the **Update** button in the **Device Details** page or select the device and click **Update Device**.
   - Match configuration in ExtremeCloud IQ: With this option, using the CLI, you match the configuration flagged as out of sync with ExtremeCloud IQ, in the assigned switch template or device level configuration.
   - Clear the Audit Mismatch by selecting the device on the **Manage Devices** page, and then choosing **Actions** > **Clear Audit Mismatch**: With this option, no configuration changes are pushed to the switch. This option maintains the current configuration on the switch without affecting the ExtremeCloud IQ configuration.
6. Resolve interdependent conflicts manually before proceeding with a configuration update.
7. After you have selected the appropriate option for each configuration element, initiate the configuration synchronization from ExtremeCloud IQ.

   ExtremeCloud IQ pushes the selected changes to the switch, ensuring that the configurations are aligned.

Download Tech Support File

To help with support related issues, download a technical support file that is gathered from your system.

This action is only supported by one device at a time.

To download the technical support file:

1. Go to **Manage Device** and select a single device.
2. **Utilities** > **Tools**.
3. Select **Get Tech Support File**.
4. Select **Yes** when asked if you want to proceed.
5. Select **Download Tech Support**.