ExtremeCloud IQ Universal Switch Deployment

User Guide

August 2023

Table of Contents

Preface

Read the following topics to learn about:

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

Text Conventions

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

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

Table 1: Notes and warnings

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

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words *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 white papers, data sheets, and case studies

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

Help and Support

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

Extreme Portal

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

The Hub

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

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 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 Information Development team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, do either of the following:

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

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

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 allowing 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*

Familiarize yourself with the ExtremeCloud IQ deployment process steps here.

> **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.
> - Ignore the **Change the Network Operating System** task as that does not pertain to non-Universal switches.
> - Make sure all devices operate with the latest firmware and operating system.

Deployment Process Overview

The following list comprises the steps to follow to deploy Universal switches for interaction with ExtremeCloud IQ.

> **Note**
> It is assumed that you have already 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. Make sure you have proper outbound access allowed on your firewall from the switch in order to connect to the cloud. Refer to Configure Firewall Access on page 12.
3. On-board switches by adding their serial numbers to your ExtremeCloud IQ account.

   > **Note**
   > ExtremeCloud IQ automatically discovers the devices as long as the devices have been added to your ExtremeCloud IQ account. You can save some time by connecting your switches to the network first. This way, you can onboard your switches in ExtremeCloud IQ, and while you are creating your configuration, your switches will discover ExtremeCloud IQ in the background. By the time you define your configuration settings, your switches will be ready to be updated with their new configuration.

4. If necessary, 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 the following components:
   - A switch template
   - Additional settings like DNS, NTP, SNMP, and Syslog

   > **Note**
   > If you need to configure a switch feature not supported within a Network Policy, switch template, or device-level configuration, add that feature via the Supplemental CLI, (Refer to Configure Supplemental CLI on page 33). 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 43.

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

About This Task

Before you can onboard your devices, if you have not already done so, you must create an ExtremeCloud IQ account.

Procedure

1. Visit 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. It's 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

About This Task

In order to connect to the cloud, you need to configure proper firewall access.

Procedure

1. On the mail ExtremeCloud page, select the icon next to your user information in the top right corner of the page.
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 here.

Deploy Devices to the Cloud

About This Task

Use this task to set up a new ExtremeCloud IQ network. If you are a first-time user, you will see the **Welcome to ExtremeCloud IQ** onboarding panel at right side 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. Perform the following steps to onboard devices and manage them.

Procedure

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**.

What to Do Next
Assign a location to a device.

Create a Topology Map

Before You Begin

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

About This Task

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. Use this list for the following steps.

Procedure

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**.

Results
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

Before You Begin

Onboard the device to ExtremeCloud IQ.

About This Task

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.

Procedure

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**.

Results

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

About This Task

This is a simplified procedure to add real devices to your existing network with existing locations.

Procedure

1. From the **Devices List** on the main page, select **+** > **Quick Add Devices**
2. For **Device Type**, select **Real**.
3. For **Entry Type**, select **Manual** and enter the device serial number.

   You can also select **CSV Import** and import a `.csv` file with a list of device serial numbers.

   a. For the **Device OS**, choose **Switch Engine** or **Fabric Engine** before you can onboard a Universal Hardware Switch.
4. Select your location from the pick list.

   > **Note**
   > You cannot create a new location in the **Quick Add** process. You must select an existing location.

5. Select **Add Devices**.

Results
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 familiarize yourself 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	Full Description
	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.
	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.
	Unknown State	Device is in an unknown state. **Cause**: This condition can arise when the indicators are ambiguous, indeterminate, 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.
	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.

Table 4: Device Status Icons (continued)

Icon	Icon Name	Full Description
	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.
	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 reason 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.
	Managed by ExtremeIoT	Device is provisioned to function with ExtremeIoT.
	Monitoring Unassociated Clients	Device is using presence analytics to monitor client devices that are not associated to the network, such as passers by.
	Switch Stack (Closed)	Device is a switch stack, but the stack is collapsed visually and displays as a single device.
	Switch Stack (Open)	Device is a switch stack, and the stack is expanded visually to reveal 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.

Table 4: Device Status Icons (continued)

Icon	Icon Name	Full Description
	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.
	VPN Server - Tunnel Up	Device is functioning as a VPN server and the VPN tunnel is up, healthy, and operating properly.
	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.
	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.
	VPN Client - Tunnels Up	Device is functioning as a VPN client and the VPN tunnel is up, healthy, and operating properly.
	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.

Table 4: Device Status Icons (continued)

Icon	Icon Name	Full Description
	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.
	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.
	Extreme Cloud Appliance Cluster (Closed)	Device is a logical cluster of appliances, but the cluster is collapsed visually to appear as a single device.
	Extreme Cloud 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 43.

> **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

About This Task

Network Policy configuration applies to multiple devices. If you want to customize only one device, see Configure Device-Specific Settings on page 43.

Procedure

1. Navigate 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. Enter an optional **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

About This Task

The following configuration settings are the only settings applicable to switches. All other settings displayed in this section are applicable to wireless products only. Choose which default routing instance will be used for NTP, DNS, Syslog and SNMP.

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

Procedure

1. Navigate to **Configure** > **Network Policies**.
2. Select the existing network policy and **Edit**.
3. Configure a DNS Server on page 34.
4. Configure an NTP Server on page 35.
5. Configure an SNMP Server on page 35.
6. Configure a Syslog Server on page 36.
7. Configure Device Credentials on page 45
8. Configure LLDP and CDP Settings on page 38.

> **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.

9. Select **Save**.

Configure Switch Common Settings

About This Task

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

Procedure

1. 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.
2. For the remainder of the configuration options, see Perform Device Configuration on page 22.

Port Type Settings

Use **Port Types** to manage Switch Engine (EXOS) and Fabric Engine (VOSS) SKU port types within the network policy. View, create, edit, clone and delete switch port types from the **Port Types** menu item under **Switch Settings**. Use the plus sign to add a new port type. See here for more information about port type configuration.

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

The table displays information about the port device family, usage, status, and VLAN. For the **Used by** column, hover over, select the number (Total number of usages), and the Device configuration, Device Template, and Network Policy this port type is being used in displays on the right. For example:

- Device Template
- 2ndSlot_5720_copied
- AVM-5720-Stack-2
- Network Policy
- Edge_IOT_Policy

Other columns display based on a filter that enables you to view Switch Engine, EXOS or Fabric Engine, VOSS, or both.

Configure a Device Template

About This Task

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.

Procedure

1. Navigate to **Configure** > **Network Polices** > **the existing network policy** > **Switch Settings** > **Switch Template**.
2. To create a new template based on an existing switch template, use the **Select** icon.
3. In the new dialog box, scroll to an existing Universal device template, for example, **Fabric Engine 5520-24T**.
4. Select **Copy**.
5. Enter a name for this cloned copy.
6. To create a brand new template not based on an existing default, select the add icon.
7. Select a device type from the drop-down, for example, `Switch Engine 5320-24T-8XE`.
8. Enter a name for the new template, for example, `TEST_5320`.
9. Select **Save**.

   The new or cloned template displays on the network policy's **Switch Template** page.
10. Select the template to display the **Device Template** configuration page.

What to Do Next
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

Before You Begin

Create a network policy and Device Template.

About This Task

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 SwitchEngine, 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.

Procedure

1. Navigate to **Configure** > **Network Polices** > **the existing network policy** > **Switching** > **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 24.

4. For **IGMP Settings**, if necessary, 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 to configure ELRP client periodic packet transmission for VLAN(s) assigned to a port type to detect and prevent loops.

    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.

7. 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.

8. For **PSE Settings**, toggle to **On** to configure maximum power thresholds to generate alerts to ExtremeCloud IQ about exceeding maximum power levels.

9. 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.

What to Do Next

Proceed to Port Configuration.

Configure STP Settings

About This Task

Use this task to configure Spanning Tree settings.

Procedure

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.
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 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 :

*   Aggregated Ports (Switch Engine devices only) must be the same type and support the same maximum speed.
*   Copper ports must be of the same speed type.
*   Selected ports with different maximum speed types cannot 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**
- **Port Settings**
- **STP**
- **Storm Control**
- **MAC Locking**
- **Voice**
- **ELRP**
- **PSE**

> **Note**
> 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.

About This Task

To create ports in bulk, follow these steps.

Procedure

1. 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 different templates for the same switch SKU are required to be created with different VIMs, then a classification rule can be created to assign the same template SKU with different VIM options to different devices. For more information about classification rules, see Configure a Classification Rule on page 29.

   d. Select one or more of these VIM ports and continue to **Step 3**.
3. Enter a **Port Type** name.
4. Toggle **Port Status On** or **Off**.
5. 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.

6. In the **Port Usage Settings** section, 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.

7. 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 28.

   > **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.

8. 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 28.

   > **Note**
   > For Switch Engine the **all** keyword can be used. Using **all** will automatically tag VLAN ID's to the ports that are also defined within other *port types* assigned to the Switch Engine device.

9. For **Allowed VLANS**, enter a specific number or leave the **All** default.

10. For **Phone with Data Port** (Voice): This option offers additional LLDP and 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 enable **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**.

    • **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.

11. 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.

12. 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.
- **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.

13. 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.
- **TCP-SYN**: Select to include TCP-SYN flood traffic.
- **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.

14. 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** it is set to clear first arrival MAC's, with the option to retain MAC's. We also have the option to take action when MAC's are aged out.

> **Note**
> MAC Locking must also be enabled on a per-port basis within a port type.

15. For **ELRP**, toggle to **ON** to enable ELRP per port (disabled by default).
16. For **PSE**, select an existing profile or select the plus sign to add a new one.

     See Configure PSE Parameters on page 30.
17. Toggle **POE Status** to the required setting.
18. Select **Save Port Type**.

Configure VLAN Settings

About This Task

Use these steps to configure VLAN settings on the **Port Configuration** page.

Procedure

1. Select the add icon.
2. Enter the name of the new VLAN.
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. Select **Apply VLAN to devices for classification** to create VLANs that you can apply to specific devices based on their location.
5. Select the plus sign.
6. Enter the new VLAN ID.
7. Select **Add** to add the ID 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 29 for more information.
9. Select **Link**.
10. Enter 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. Enter an optional description.
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

About This Task

Use this task to create a classification rule associated with a network policy.

- 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 a switch.
- Configure **IP Subnet** classification rules to assign a match type that contains or does not contain a specific IP subnet associated with a switch(s).
- Configure **IP Range** classification rules to assign a match type that contains or does not contain a specific IP range associated with a switch(s).

Procedure

1. Select the plus sign in the **Classification Rules** column to add a new classification rule.
2. Enter a name for the rule.
3. Enter an optional description.
4. Select the plus sign and the rule type to configure.
5. 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.
6. 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 30.
   c. Select **Save Rule**.
7. 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**.

8. 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**.

9. 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**.

10. 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.

11. Select **Save Rule**.

Add a Cloud Config Group

About This Task

Cloud config groups enable administrators to create network-level policies that can be replicated for multiple network roll-out scenarios. Use this task to create a new group.

Procedure

1. Select the add icon.
2. Enter a name for the new group.
3. Enter an optional description.
4. Select real and 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**.

5. Select **Save Cloud Config Group**.

Configure PSE Parameters

About This Task

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

Procedure

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. Enter an optional description.
7. Select **Save**.

Aggregate Ports

About This Task

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.

Procedure

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**.

Configure Ports Individually

Before You Begin

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

About This Task

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

Procedure

1. Select a **Port Type** from the dropdown 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 25.

   > **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.

Configure Advanced Settings

About This Task

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.

Procedure

1. From the Device Template's configuration page, select **Advanced Settings**.
2. Toggle **ON Upgrade device firmware upon device authentication**.
3. Select your preferred update option.

   > **Note**
   > If the selected firmware is already at the latest or defined firmware, then the upgrade device firmware action will not occur.

4. Toggle **ON Upload configuration automatically**.

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

Configure Supplemental CLI

Before You Begin

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

About This Task

Use this task to update CLI commands to 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.

Procedure

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. Enter an optional 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

About This Task

Procedure

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 39.

Configure a DNS Server

About This Task

The DNS (Domain Name System) 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. Perform the following steps 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.

Procedure

1. Choose to use an existing DNS Server Setting, or proceed to the next step.
2. Enter a name for the server.
3. Enter an optional **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 29.

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

About This Task

Extreme Networks devices typically obtain the time and date for their internal clocks from an NTP server.

Procedure

1. Toggle the NTP Server function to **ON**.
2. Choose to use an existing NTP Server Setting, or proceed to the next step.
3. Enter a new NTP Server name.
4. Enter an optional description.
5. For **HiveOS Device Sync Interval**, set a polling interval for devices to use for internal clock synchronization.
6. For **Switch Sync Interval**, choose a polling interval to apply to Fabric Engine switches.
7. Select an existing NTP server from the table or use the add icon to create a new host name or IP address.
8. Repeat the procedure to add more NTP servers to the profile.

    The second entry becomes the secondary NTP server, and so forth. Because NTP servers are accessed in order from the top according to their position in the profile, you can use the up and down arrows to rearrange them if necessary.
9. To **apply NTP 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 29.
10. Select **Save NTP Server**.
11. If you are ready to deploy the network policy, select **Next** or continue to the next Management server.

Configure an SNMP Server

About This Task

SNMP (Simple Network Management Protocol) 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.

Complete the following steps to configure an SNMP server profile.

Procedure

1. Toggle the SNMP Server function to **ON**.
2. Choose to use an existing SNMP Server Setting, or proceed to the next step.
3. Select the add icon.

4. Enter a name for the server.

5. Enter a brief description for the server.

6. Enter the contact information of the SNMP server admin so they can be contacted if necessary.

   This can be an email address, telephone number, physical location, or a combination.

7. To add the SNMP server to the table, select the add icon.

8. 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 be able to access the devices. To permit management access from a single SNMP server, choose an IP address or host name that defines just 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 **New** and define one.

9. Select the version of SNMP that is running on the management station you intend to use from the drop-down list.

10. From the **Operation** drop-down list, 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.

11. In the **Community** field (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 only accept queries from management stations that send the correct community string.

12. Select **Save SNMP Server**.

    Repeat this procedure to add up to three SNMP servers to the profile.

13. To **apply SNMP 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 29.

14. Select **Save SNMP Server**.

Configure a Syslog Server

About This Task

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 35.

Procedure

1. Toggle the Syslog Server function to **ON**.
2. Choose to use an existing Syslog Server Setting, or proceed to the next step.
3. Enter a name for the server.
4. Enter an optional description.
5. For **Non-IQ Syslog Facility**, select a syslog facility to categorize messages sent to syslog from non-IQ Engine devices.
6. Select the expand arrow to expand the **Syslog Group**.

   Syslog groups organize messages by category and limit the number of messages sent based on severity level.
7. Assign a minimum severity level to each group from the drop-down lists.

   Messages below the assigned level will not be sent from the AP to the syslog server.
8. If you must make PCI DSS compliance reports, leave that check box selected or clear the check box if the servers are on an external network outside the firewall.
9. Select the plus sign to add a syslog server.
10. Select an existing syslog IP Address or host name, or use the add icon to create a new IP Address or host name.
11. 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.
12. 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.

13. 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 29.
14. Select **Save Syslog Server**.

Configure LLDP and CDP Settings

Before You Begin

To enable LLDP/CDP for a port, ensure that LLDP/CDP is enabled under both the policy level and port level configuration.

About This Task

Extreme Networks devices can advertise LLDP data and receive, cache, and display both LLDP and CDP data. However, they do not advertise CDP data. You can use LLDP and CDP data to help debug network issues. For example, the CDP data can be used when debugging VLAN issues on Cisco switches.

Use the following procedure to enable devices to receive and cache LLDP advertisements, and to advertise their own data through LLDP.

Procedure

1. Navigate to **Configure** > **Common Objects** > **Network** > **LLDP/CDP**.
2. Select the plus sign.
   Alternately, you can edit an existing profile.
3. Enter a name for the profile.
4. Enter an optional description.
5. Select whether to enable LLDP on access ports.

   > **Note**
   > LLDP is enabled on other port types by default.

6. Select whether to receive, cache, and display LLDP advertisements from other network devices but to not advertise data.
7. Define the maximum number of LLDP entries from neighboring network devices that a device can store in its cache.
8. Set the length of time that the device instructs neighboring devices to retain the LLDP advertisements it sends them.
   You might want to increase this setting while engaged in troubleshooting a network issue and decrease it if there is a need to reduce overall network traffic.
9. Set the interval for sending LLDP advertisements to neighboring network devices.
10. Set a maximum power level that devices can request in LLDP advertisements to avoid requests for more power than the switch can provide.
11. Enter the amount of time you want the interface to wait before initializing LLDP.
12. Enter the number of advertisement LLDP frames to send when the connected device (such as an IP phone) starts up or is discovered.
13. Select whether to enable devices to receive and cache CDP advertisements.

    > **Note**
    > You can enable devices to support both LLDP and CDP concurrently.

14. Select whether to enable CDP on access ports.
15. Define the maximum number of CDP entries that a device can store in its cache from neighboring network devices.

16. Select **SAVE**.

Deploy a Network Policy

Before You Begin

Create a complete network policy configuration.

About This Task

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.

Procedure

1. Navigate **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 optionally 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**.

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 40.
- To manually create switch stacks, see Configure a Switch Engine Device Switch Stack on page 41

Instantly Create a Switch Engine Device Stack

Before You Begin

To instantly create a stack, onboard the switches into ExtremeCloud IQ via the ExtremeCloud IQ MobileApp. Unbox the switches, connect the stacking/power/uplink cables, and push the **Mode** button until the **STK LED** lights up. Depress the **Mode** button for at least 5 seconds. All of the front panel ports LED will flash. The stack forms automatically, all the slots reboot, and ExtremeCloud IQ detects the newly formed stack.

About This Task

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

Procedure

1. Navigate to **Manage** > **Devices**.
2. Find the new stack in the **Devices List** and select its checkbox.
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 dropdown.
6. Select **Assign**.

Results

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 43.

Configure a Switch Engine Device Switch Stack

About This Task

A stack is two or more Switch Engine devices inserted into slots and cabled together. When onboarding stacks, you will 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 will carry 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.

Procedure

1. If not already there, select **Configure** > **Network Polices**, the existing network policy, and the **Device Template** tab.
2. To create a template based on an existing default template, use the **Select** icon to create a new template.
3. In the new dialog box, scroll to an existing switch stack device template, for example, **Switch Engine 5320-Series-Stack**.
4. Select **Copy**.
5. Enter a name for this cloned copy.
6. To create a brand new template not based on an existing default, select the add icon.
7. Enter a name for the new template.
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 21.

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

11. Save the configuration.

Results

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.

What to Do Next

For any post-configuration switch stack issues, see Switch Stack Issues on page 57. 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 40.

Configure Device-Specific Settings

ExtremeCloud IQ allows you 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, use the **Actions** button from the Device List. To configure settings at the network policy level, see Configure the Network Policy on page 19.

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 43.
- **Port Configuration**: edit port types, STP, Storm, and PSE settings. See Configure Device Ports on page 45.
- **Device Credentials** (Switch Engine devices only): assign or change network administrator credentials and administrator assignments. See Configure Device Credentials on page 45.
- **SSH**: temporarily enable SSH in order to troubleshoot the device. See Configure SSH on page 46.

Configure Devices

About This Task

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.

Procedure

1. Navigate 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 21.
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

Before You Begin

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

About This Task

Use this task to override a network policy and make device-level changes to management server settings for a device. The changes only affect 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 management servers page does not display until you apply the network policy to both single switches and stacks.

Procedure

1. Select **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.

Configure Device Ports

About This Task

You can configure port 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 25.
> - For 5520/5720 Universal Switches, VIM and partition mode are configurable at the device level.
> - LLDP/CDP, MAC locking, and STP Priority, Forwarding Delay, and Max Age are configurable at the device level.

Procedure

1. Go to **Manage** > **Devices**.
2. Select a device **Host Name** to see a details panel for that device.
3. Select the **Configuration** tab.
4. Select **Port Configuration**.
5. Select **Unlock** to enable device-level configuration changes.
6. Select **Port Details**, and edit any field that is not selectable.
7. Select **Port Settings**, and edit any field that is not selectable.
8. Select **STP**, and edit any field that is not selectable.
9. Select **Storm Control**, and edit any field that is not selectable.
10. Select **PSE**, and edit any field that is not selectable.
11. Select **Save Configuration**.
12. To revert back to the network policy:
    a. From the **Devices** list, select the check box for this device.
    b. From the **Actions** drop-down menu, use the **Revert Device Template to Device Defaults** option.

Configure Device Credentials

Before You Begin
You need to 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**.

About This Task

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.

Procedure

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 Begin

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.

About This Task

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 the following steps 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).

Procedure

1. Navigate 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.

Push the Device-Level Configuration to the Device

Before You Begin

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.

About This Task

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. ExtremeCloud IQ also allows you to 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.

Procedure

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 and Fabric Engine 8.9 installed on the switches.

Clone A Device

About This Task

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

> **Note**
> Licensing is not cloned.

Procedure

1. Select the check box for the device in the **Device List**.
2. Select **Actions**.
3. Select **Clone Device**.
4. If the device has already been **Onboarded**, proceed to Step 5. Under **Replacement Device**, if the device is not yet **Onboarded**, select **Quick Onboard**, enter its serial number and proceed to **Step 6**.

   > **Note**
   > After you select **Clone** in **Step 6**, ExtremeCloud IQ waits 30 seconds for the device to be onboarded. If it is not onboarded within that time period, Extreme Cloud IQ manually creates the device. This enables the device to be onboarded through the clone process.

5. Under **Replacement Serial Number**, select the appropriate device serial number.
6. For the **Device OS**, choose **Switch Engine** or **Fabric Engine** before you can onboard a Universal Hardware Switch.
7. Select **Clone**.
8. On the next dialogue select **Yes**.
9. Select **Perform Update** to push the configuration to all selected cloned devices.

Monitor Switches

The Monitor **Overview** tab is the default display that provides 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, this timeline displays data for the last 24 hours, but you can change the time range by Day, Week, or Month, and for 1, 2, 4, 8, and 24 hour durations.

- 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**, use the **Bounce Port** button to reset the port. A green port is connected. A grayed-out port is disconnected. A red port was disconnected by the 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 58.

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

Use the remaining Monitor tabs to view the following:

- **Client**: the details of the clients connected to the device. See Clients on page 50.
- **Diagnostics**: the diagnostic details for ports. See Diagnostics on page 50.
- **Events**: events that occur in the network for the selected device. See Events on page 50.
- **Alarms**: events that can indicate network issues for a specific device which require Admin interaction. See Alarms on page 51.

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 the diagnostics details timeline 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 the timeline to change it.

> **Note**
> Select **=** at the bottom right of this timeline to print it or to download it 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 an alarm or event. The following can be displayed: Major, Info, and Clear.
- **Category**: Indicates how ExtremeCloud IQ was notified of the alarm or event. Available categories are CAPWAP, channel power, state change, client connection down, and client connection change.
- **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

ExtremeCloud IQ also allows you to upgrade the device software images in two ways:

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

Follow these instructions.

Update the Device Software Images

About This Task

Use this task to update the device software.

Procedure

1. Select the device(s) to update in the Devices List.
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:

- 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 12.

- Ping the device or initiate a TraceRoute from within ExtremeCloud IQ. Refer to Establish CLI Access from ExtremeCloud IQ on page 55.

- 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 55.

- 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 56.

- **Incorrect VLAN or Trunk**: Refer to VLAN or Trunk Issues on page 57.

- Switch Stack Issues: Refer to Switch Stack Issues on page 57.

- Switch Communication Issues: Refer to IQAgent and Switch Communication Issues on page 57.

- 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 58.

- Audit Logs: Access these at **Global Settings** > **Logs** > **Audit Logs**
- Configuration Events: Access these at **Manage** > **Devices** > **[select device]** > **Monitor** > **Events** > **Configuration Events**

Establish CLI Access from ExtremeCloud IQ

About This Task

Use this feature 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.

Procedure

1. Navigate 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

About This Task

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.

Procedure

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

What to Do Next

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)

About This Task

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 to allow remote devices to be power-cycled. The **Restart PSE** utility affects only inline power.

Procedure

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

Device Update Failure

About This Task

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 33). 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.

Procedure

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 47.
5. If you still get an error, reset the device.

   See Reset the Device to Default Settings on page 55.

VLAN or Trunk Issues

About This Task

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 need to 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 47 for out-of-sync issues.

Procedure

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 that port's configuration.

Switch Stack Issues

About This Task

When onboarding stacks, you will 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.

Procedure

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

Familiarize yourself with IQAgent.

About This Task

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.

Procedure

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 can't 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

Before You Begin

Follow all previous troubleshooting steps in this chapter.

About This Task

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

Procedure

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.

NEW! Resolving Configuration Discrepancies in ExtremeCloud IQ

About This Task

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 on-boarding, 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 the following procedure to correct out-of-sync configurations in ExtremeCloud IQ and maintain a consistent and accurate configuration across managed switches.

Procedure

Accessing Configuration Status in the ExtremeCloud IQ user interface

1. Log in to ExtremeCloud IQ using appropriate credentials.
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.

Reviewing Configuration Discrepancies

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.

Understanding Available Options

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.

Initiating Configuration Sync

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.