Extreme Platform ONE Networking v25.7.0 Universal Switch Deployment Guide

Configuration, Management, and Best Practices

9041009-00 Rev AA
February 2026

Legal Notice

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

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

Trademarks

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

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

For additional information on Extreme Networks trademarks, see: https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

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

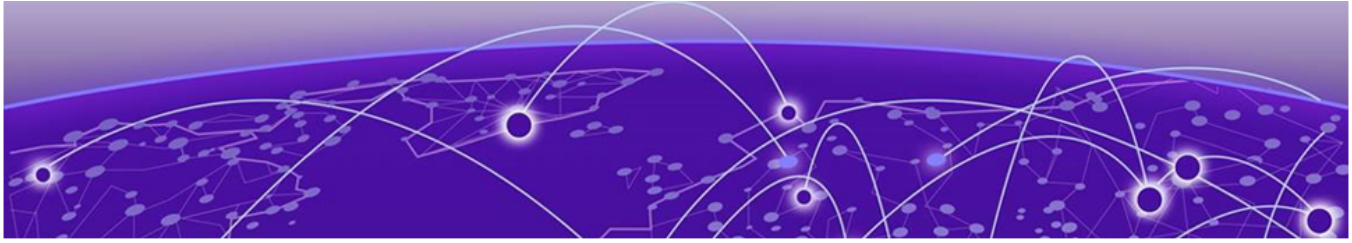
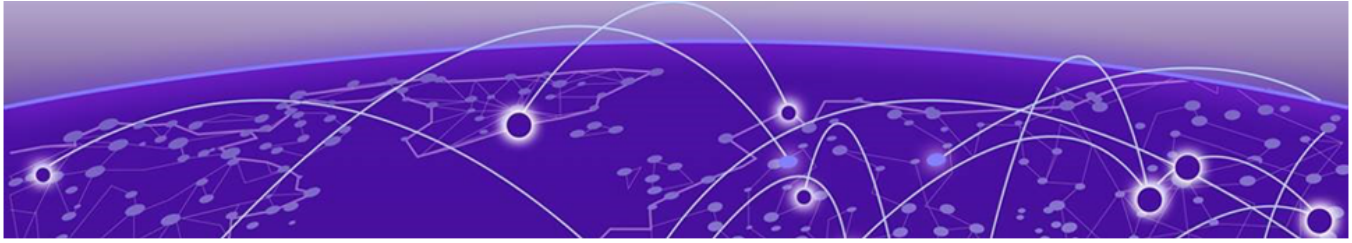


Table of Contents



Abstract

This deployment guide for Extreme Platform ONE Networking version 25.7.0 provides comprehensive technical instruction for configuring, onboarding, and managing Extreme Networks Universal Switches, detailing support for dual persona Switch Engine and Fabric Engine software, required firewall access, account creation, NOS selection, and manual or bulk onboarding workflows. It outlines full network policy construction—including switch templates, common settings, VLAN attributes, Instant Port Profiles, Instant Secure Port Profiles, DHCP/IGMP Snooping, STP, ELRP, MAC locking, PSE, and management server configurations—along with device level overrides, supplemental CLI usage, and template inheritance rules for large scale deployments. Advanced features such as routing configuration, IPv4 subnet allocation, static routes, Auto Sense behavior, SPBM fabric settings, stack creation, and VIM/port channelization support are included to guide administrators through switch specific and multi device implementations. Troubleshooting sections provide targeted procedures for stack issues, VLAN and trunk mismatches, device update failures, switch communication problems, cable testing, diagnostics commands, and resolving out of sync configurations, ensuring reliable operations in enterprise environments. The guide is written for technically proficient network administrators and delivers structured instructions, configuration workflows, operational insights, and best practice guidance for deploying and maintaining Universal Switch infrastructure across diverse network scenarios.

Preface

Read the following topics to learn about:

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

Text Conventions

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

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

Table 1: Notes and warnings

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

Table 2: Text

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

Table 3: Command syntax

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

Documentation and Training

Find Extreme Networks product information at the following locations:

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

Open Source Declarations

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

Training

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

Help and Support

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

Extreme Portal

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

The Hub

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

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

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

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

Subscribe to Product Announcements

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

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

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

Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

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

To send feedback, email us at Product-Documentation@extremenetworks.com.

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

Overview of Universal Switch Deployment in Extreme Platform ONE Networking

Deploy Universal Switches on page 11

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

- All Universal switches have Switch Engine and Fabric Engine pre-installed and ready to run. After onboarding a switch to Extreme Platform ONE Networking, 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 Extreme Platform ONE Networking to configure and monitor the Extreme Networks Universal Switch series. For any CLI information, see the following guides:

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

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

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

To become familiar with the Extreme Platform ONE Networking deployment process steps, see Deploy Universal Switches on page 11.

Note
To use this guide for non-Universal switches:

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

Deploy Universal Switches

Use this task to deploy a Universal Switch to interact with Extreme Platform ONE Networking.

Note
You must already have set up your network in Extreme Platform ONE Networking, including configuring your buildings, floor plans, locations, etc.

1. Connect the switches to the network and power them up.
2. Ensure you have proper outbound access allowed on your firewall from the switch in order to connect to the cloud. For more information, see Configure Firewall Access on page 15.
3. **Network Devices** is a centralized location for monitoring both wired and wireless network devices. Devices can be onboarded to the network using a manual or bulk

onboard method. Onboard switches by adding their serial numbers to your Extreme Platform ONE Networking account.

Note

When configuring switch features that are not supported within a **Network Policy**, switch template, or device-level configuration in Extreme Platform ONE Networking, you must follow these guidelines to avoid unintended behaviors and potential device update failures:

a. Supplemental CLI Configuration:
   - Use the Supplemental CLI to add unsupported features.
   - Ensure that the Supplemental CLI configuration does not overlap with the Extreme Platform ONE Networking configuration.

b. Avoid Overlapping Configurations:
   - Do not use SSH proxy, Web CLI, or console access to add configurations that overlap with those managed by Extreme Platform ONE Networking. Overlapping configurations can cause device update failures when pushed from Extreme Platform ONE Networking.

c. Potential Risks:
   - Modifying configurations within CLI while the switch is cloud-managed can lead to unintended behaviors, such as disabling the ExtremeCloud IQ Agent or restarting network tools.
   - In the event of a switch crash, manual recovery may be necessary to reconnect the switch to the cloud.

By adhering to these guidelines ensures a stable and consistent configuration management process for your cloud-managed switches.

4. (Optional) Change the default Network Operating System from Switch Engine to Fabric Engine.
5. Create Visualize topology maps to associate switches with locations.
6. Configure a network policy with a switch template and additional settings (for example, DNS, Syslog, SNMP).

Note

To configure a switch feature not supported within a Network Policy, switch template, or device-level configuration, add that feature in the Supplemental CLI, (refer to Configure Supplemental CLI on page 60). The Supplemental CLI must not overlap with the Extreme Platform ONE Networking configuration. Additional configuration via SSH proxy, Web CLI, or console access must also not overlap with the Extreme Platform ONE Networking configuration or a **`Device Update Failure`** might occur when you push the overlapping configuration from Extreme Platform ONE Networking.

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 80.

Onboard Switches

Create an Extreme Platform ONE Networking Account

Use this task to create an Extreme Platform ONE Networking account.

Note
With an Extreme Platform ONE Networking account, you have access to ExtremeCloud IQ. The newly created Extreme Platform ONE Networking administrator account is also an ExtremeCloud IQ administrator account.

1. Near the bottom of the **Log In** dialog, select **Register to Get Started**.
2. In the **Create an Account** dialog, type your **Business Email**, and then select **Continue**.

   The system sends an email asking you to verify your email address.
3. Follow the instructions in the email to verify your email address.
4. Provide the following information:
   a. In the fields, type the required information about you, and then select **Continue**.
   b. In the fields, type the required information about your company, and then select **Continue**.
   c. Review and accept the account notices.
5. Select **Create Account**.

   The system sends a registration email to the email address you used to create your account. Follow the link in the email to set up your password and complete the registration process.

   Creating a new Extreme Platform ONE Networking account automatically starts the process of creating an Extreme Portal account. If you do not already have an Extreme Portal account, you will receive an email with instructions to set a password for your new Extreme Portal account. For information about purchasing required licenses and linking to your Extreme Portal account, see *Extreme Platform ONE Networking and ExtremeCloud IQ Licensing Entitlement Guide*.

Configure Firewall Access

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

1. In the top-right corner of the Extreme Platform ONE Networking page, select the icon next to your user information.
2. Select **About Extreme Platform ONE Networking**.
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 Extreme Platform ONE Networking Release notes, see https://supportdocs.extremenetworks.com/support/documentation/ep1-latest-documentation/ .

Change the Network Operating System

Onboard the device to Extreme Platform ONE Networking.

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

1. Select **Monitoring** > **Network 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, 5520-48W-Switch Engine.
3. Select the associated 3-dot menu and select **Change OS to Fabric Engine**.
4. Select **Yes**.

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

Onboard Network Devices

Onboard devices to the network using one of the following methods:

- **Manual**: Manually enter up to 10 serial numbers for devices of the same type.
- **Bulk**: Bulk onboard multiple devices of any type using a CSV file that contains device serial numbers.

Use this task to onboard devices to your network.

1. Select **Onboard**.

2. Configure the applicable Onboard Device Settings in Table 4.

Table 4: Onboard Device Settings

Field	Description
Manual	
Cloud or Locally	Select option.
Device OS	Select a device type.
License Level	Select the license level.
Network Policy (Optional)	Assign the device to an existing network policy.
Location (Optional)	Assign the device to an existing location.
Select **Next**.	
Serial No.	Enter a device serial number. Select  to add additional serial numbers. You can add up to 10 serial numbers from the same platform family.
Select **Next**.	
Generate a Formatted Hostname	Enable the toggle.
Bulk	
Network Policy (Optional)	Assign the device to an existing network policy.
Location (Optional)	Assign the device to an existing location.
Upload File	Select **Browse Files** or drag and drop a CSV file containing device serial numbers. **Note:** Supports .xlsx files only.

3. Select **Onboard**.

Device Status Icons

Table 5: Device Status Icons

Icon	Icon Name	Description
	AFC Status	Indicates an AFC issue with the selected device. Status options include **Pending**, **Grace Period**, and **Spectrum Mismatch**.
	Configuration 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.

Table 5: Device Status Icons (continued)

Icon	Icon Name	Description
	Configuration Audit Match	The network policy configuration matches the current running configuration. Select the icon to open a pop-up window detailing the configuration changes that occurred since the last **Update Devices** operation. • Audit tab — lists any modifications made since the previous configuration update. • Delta tab — shows CLI commands that have changed since the previous update. • Complete tab — shows all CLI commands (including the CLI commands in the Delta tab) that form a configuration file. ExtremeCloud IQ uses this file for the next configuration update. After a successful configuration update, the configuration in the Complete tab matches the running configuration. **Note:** Not applicable for locally managed switches.
	Configuration Audit Mismatch	The network policy configuration does not match the current running configuration. Cause: The Configuration Audit Mismatch icon is visible on devices between the time that network policy changes are saved and the time that the altered network policy is uploaded to the device. Action: Upload the network policy to the device. Select the icon to open a pop-up window detailing the configuration changes that occurred since the last **Update Devices** operation. See the Configuration Audit Match icon description for details. **Note:** Not applicable for locally managed switches.
	Configured at Device Level	Device possesses a device-level configuration that is different from the configuration defined in the network policy. This is not an error condition, but this information can be useful when troubleshooting network behavior because device-level configurations supersede device templates and network policy configurations.
	Configuration Pending	Device is currently offline and will receive its latest assigned configuration once it reconnects to the network.

Table 5: Device Status Icons (continued)

Icon	Icon Name	Description
	Configuration Rollback	Device could not establish a connection to Extreme Platform ONE Networking after the configuration update. Device configuration rolled back to the last known good connection and the **Updated** status column displays `Device update failed`.
	Connected Device	Device is actively communicating with Extreme Platform ONE Networking.
	Device Update Unsuccessful	Device did not accept the OS or configuration upload. Cause: There are many reasons for an unsuccessful update, but the most common include network connectivity or connection status changes, or the device rejected the command it received. Action: Hover over the update message in the Updated column to view the reason message describing the likely error condition. Ensure that the device is properly powered, that there is appropriate network connectivity, and that common causes listed here are not the issue.
	Digital Twin	Device is a simulated device.
	Disconnected Device	Device is not actively communicating with Extreme Platform ONE Networking. 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 Extreme Platform ONE Networking 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.
	ExtremeCloud Appliance Cluster (Closed)	Device is a logical cluster of appliances, but the cluster is collapsed visually to appear as a single device.
	ExtremeCloud Appliance Cluster (Open)	Device is a logical cluster of appliances, but the cluster is expanded visually to reveal the cluster members.
	Fabric Attach	Device is a member of the Fabric Attach Connect Automation environment and is functioning properly in that context.

Table 5: Device Status Icons (continued)

Icon	Icon Name	Description
	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.
	Locally Managed (ExtremeCloud IQ)	Device is managed by a platform other than ExtremeCloud IQ, but it is monitored by ExtremeCloud IQ. For example, other platforms can include 3rd party, ExtremeCloud IQ Site Engine, or ExtremeCloud IQ Controller.
	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.
	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 passersby.
	No Connection	This device has not yet made a connection with Extreme Platform ONE Networking. It can take up to 10 minutes for a device to appear after the initial onboarding process. If the device has not successfully connected after 10 minutes.
	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.

Table 5: Device Status Icons (continued)

Icon	Icon Name	Description
	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.
	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.
	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.
	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.
	Swap for Real Device	Device is a simulated device that you can exchange for a real device.
	Switch Stack	Device is a switch stack.
	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.
	Undetermined	Device status is undetermined. Cause: This condition can arise when the indicators are ambiguous, unknown, or appear contradictory due to other factors. Action: Begin general troubleshooting procedures to ensure that the device is powered, connected, and is responding to traffic and CLI commands. Ensure that the device is communicating appropriately with network services, such as NTP, DHCP, etc.

Table 5: Device Status Icons (continued)

Icon	Icon Name	Description
	VPN Client Server 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 Extreme Platform ONE Networking. 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.
	VPN Client Server Tunnels Up	Device is functioning as a VPN client and the VPN tunnel is up, healthy, and operating properly.
	VPN Client Server 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 Extreme Platform ONE Networking. In addition, ensure that there is connectivity and communication between the VPN server and client.
	VPN Server Turned 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 Extreme Platform ONE Networking. 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.

Table 5: Device Status Icons (continued)

Icon	Icon Name	Description
	VPN Server Turned Up	Device is functioning as a VPN server and the VPN tunnel is up, healthy, and operating properly.
	VPN Server Turned 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 Extreme Platform ONE Networking. In addition, ensure that there is connectivity and communication between the VPN server and clients.

Configure the Network Policy

A Network Policy is an assembly of configurations that Extreme Platform ONE Networking 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 **Wired Devices** section for managing Switch Engine templates and settings. Extreme Platform ONE Networking supports Network Policy and device-level configuration for all supported wired devices.

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 80.

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). Fabric Engine templates are not available within a Network Policy. Fabric Engine devices can be managed at device configuration level only. Legacy switching devices are not supported such as SR/DELL in Extreme Platform ONE Networking.

To view or edit network Policy configuration options, go to **Configuration** > **Network** on the left navigation menu.

Create a Network Policy

Network Policy configuration applies to multiple devices. If you want to customize only one device, see Configure Device-Specific Settings on page 80.

1. Go to **Configuration** > **Network** > **Network Policies** > **Wireless & Switching/Routing**.

2. If desired, you can deselect **Wireless** so that only **Switches** is selected as the policy type.
3. Enter a **Policy Name**.
4. (Optional) Enter a **Description**.

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

5. Select **Save**.
6. Select **Switching/Routing** from the breadcrumbs at the top of the page.

Configure Switch Common Settings

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

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

1. Go to **Configuration** > **Network**.

   Page will default to **Network Policies**. To access **Common Objects** or **User Management**, select from the drop-down list. Go to **Switching/Routing**.
2. For **Management Servers** (Switch Engine/EXOS only), select **VR-Default** or **VR-mgmt** to apply the correct routing instance to defined network policy DNS, NTP, SNMP, and Syslog server settings.
3. For the remainder of the configuration options, see Perform Device Configuration on page 42.

IGMP Snooping

With IGMP Snooping switches identify which ports multicast group members hosts are associated with to optimize the distribution of multicast traffic. IGMP Snooping can be configured in the common settings of the network policy.

When enabled, Extreme Platform ONE Networking pushes the IGMP Snooping configuration for all VLANs configured from Extreme Platform ONE Networking.

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

Some common use-cases for IGMP Snooping are:

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

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

1. Device Specific VLAN configuration
2. VLAN attributes screen
3. Device templates
4. Common settings

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

DHCP Snooping

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

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

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

Common use-cases for DHCP Snooping are:

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

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

On the **Switch Engine and EXOS** screen, under **DHCP Snooping Settings** when the **DHCP Snooping** toggle is enabled, Extreme Platform ONE Networking pushes the DHCP Snooping configuration for all VLANs configured from within Extreme Platform ONE Networking.

Note
Trunk ports are configured as trusted by default.

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

Note
Common Settings can be overridden by configuring the specific **VLAN Attributes Override** toggle.

Custom Port Types DHCP Snooping Action

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

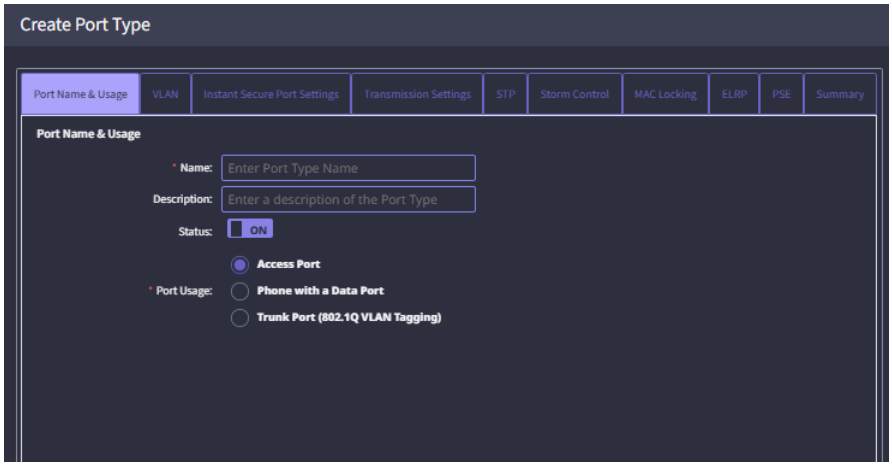


Figure 1: Port / VLAN Configuration

Device Level Override

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

Switch Policy Settings

This section contains switch policy settings.

Port Type Settings

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

Go to **Configuration** > **Network**, select your policy, select **Switching/Routing** > **Switch Settings** > **Port Types** to view, create, edit, clone, and delete switch port types. For more information about port type configuration, see Configure Ports in Bulk on page 45.

To add a port type, select +.

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

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

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

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

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

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

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

VLAN Attributes

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

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

To create a new VLAN Attribute:

1. Go to **Configuration** > **Network**.
2. Select **Switch Template** > **Switch Settings** > **VLAN Attributes**.
3. Select .

4. Configure the settings in Table 6.

Table 6: VLAN Attributes

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

5. Select **Save**.

Instant Secure Port Profiles

Instant Secure Port Profiles (ISPP) in Extreme Platform ONE Networking enables you to configure user authentication and MAC authentication per port and to specify a RADIUS server to use in conjunction with Extreme Platform ONE Security.

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

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

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

Creating a New Instant Secure Port Profile

Note
The Instant Secure Port Profile (ISPP) option will only become available when Extreme Platform ONE Security is activated.

You must create a network policy.

Use the **Configuration** > **Network** page to see all the devices that have been onboarded to Extreme Platform ONE Networking. Add the network policy to the desired Switch Engine.

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

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

To create a new Instant Secure Port Profile:

1. Go to **Monitoring** > **Network Devices**.
2. From the 3-dot menu, select **Configure** > **Device**.
3.
4. Within **Port/VLAN Configuration** select the **Instant Secure Port Profile** tab.
5. Enter the name for your ISPP. The name is unique within Extreme Platform ONE Networking but is not pushed to the device.
6. Choose whether to use Unauthenticated VLAN. Unauthenticated VLAN is either a common object or can be created when the profile is created. If the Enable Unauthenticated VLAN is selected, then this VLAN will override the untagged VLAN in the port type and will be used as the Unauthenticated VLAN on the Switch Engine device when the configuration is pushed.
7. Specify the order in which to execute authentication. The order is per profile; therefore the same order is used for the entire Switch Engine device once the configuration is pushed. Use the arrows to change the default order.
8. Pick the RADIUS server for the Instant Secure Profile. Selecting **Use Extreme Platform ONE Security RADIUS Cloud configuration** uses either the free cloud RADIUS server set up per RDC, or configured proxy RADIUS servers in the Extreme Platform ONE Security application. Select one of the radio buttons to decide which type to use. Further, in the case of proxy RADIUS, you can select up to two proxy RADIUS servers; it is assumed that the ones selected have reached a deployed state after being configured in Extreme Platform ONE Security.
9. Select **Save**.

ISPP Configuration from Switch Template

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

1. Go to **Configuration** > **Network** select **Create or Edit a Policy** > **Switching** > **Switch Templates** page.

2. Either edit an existing template, or create a new switch template for a specific Switch Engine device model such as a 5420M-48T-4YE.
3. Select **Port/VLAN Configuration**.
4. If you are creating a new template, supply a template name.
5. Select the Instant Secure Profile from the **Instant Port Profile** list.

Enable Instant Secure Port Profile on a Port

Create the Instant Secure Port Profile (ISPP) switch template, see ISPP Configuration from Switch Template on page 29.

Use this task to enable ISPP on a port.

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

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

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

Instant Secure Port Profiles Device Level Override

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

Instant Port Profiles

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

Some common use cases for IPP are:

- Configure VoIP phones in a dedicated VLAN.
- Configure guest devices in a guest VLAN.

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

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

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

Some benefits of IPP are:

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

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

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

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

Configure an Instant Port Profile

First, create or modify a switch template as part of a network policy.

Note
To create or modify switch template as part of Common Objects, see the Extreme Platform ONE Networking User Guide.

Use this task to add or edit an Instant Port Profile (IPP) in a switch template.

1. In the switch template, select **Configuration** > **Port/VLAN Configuration**.
2. Choose one of the following actions:
   - To add a new IPP, select .
   - To edit an existing IPP, select , choose the IPP object, and then select .
3. Configure the Instant Port Profile Settings on page 32.

Instant Port Profile Settings

Configure the following Instant Port Profile (IPP) settings.

Table 7: IPP Settings

Field	Description
Name	Type a **Name** for the IPP.
Description	Type a **Description** for the IPP.
Non-Forwarding VLAN	Select to choose a VLAN to detect attached devices; this VLAN does not forward traffic. To add a new non-forwarding VLAN, select , to edit an existing choose a VLAN and then select , enter a **Name** and **VLAN ID**, and then select **SAVE VLAN**. The non-forwarding VLAN cannot be utilized within a port type assigned to the switch.
Default Port Type	From the menu, select the default port type: • **Access Port** - Use for a port connected to an individual host. • **Trunk Port** - Use for a port connected to a forwarding device such as an AP and switch that supports multiple VLANs. Ports assigned to an IPP inherit the selected port type settings, such as type, speed, STP, MAC locking, ELRP, and PSE port settings. To add a new port type, select .
Non-Match Action	Select one of the options: • **Non-Forwarding VLAN**: Does not forward traffic for devices that do not match an assignment rule. • **Use Default Port Type VLAN**: Assigns the VLANs associated with the port type. Storm control settings are inherited when the non-match action is set to use the default port type and the device does not match a defined device type.
Device Types	Add a new **Device Type**, edit or delete an existing **Device Type**. Configure the IPP Device Type Settings on page 33. **Note:** For a device type to match based on MAC learning, the rule must be ordered above any LLDP-based assignment rules. This ensures that MAC learning takes precedence, irrespective of LLDP information.

Configure an Instant Port Device Type

Configure a Network Policy with a switch template and an Instant Port Profile.

The Port Device type profile is part of the Instant Port Profile. When a device connects to a switch port, Extreme Platform ONE Networking uses the criteria defined in the Instant Port device type to determine whether to apply the IPP to the port.

Universal Switches running Switch Engine and x435 models running ExtremeXOS version 32.x or later support the definition of up to 260 Instant Port device types for an IPP.

Use this task to configure device types for use with IPP.

1. In the **Create Instant Port Profile** dialog, under **Device Types**, select .
2. Configure settings.

   See IPP Device Type Settings on page 33.
3. Select **Save** to commit changes, or select **Cancel**.

IPP Device Type Settings

Configure the following Instant Port Profile (IPP) device type settings.

Table 8: IPP Device Type Settings

Field	Description
Name	Type a **Name** for the device type profile.
Description	Optionally, type a **Description** of the device type profile.

Table 8: IPP Device Type Settings (continued)

Field	Description
Match Category	Select a **Match Category**. Options are: • **MAC Learning** - Matches the device based on the MAC address learned on the port from untagged traffic. The match criteria can be an exact MAC, OUI-based MAC, or custom MAC mask format. • **LLDP Src MAC** - Matches the device based on the source MAC of a LLDP PDU. The match criteria can be an exact MAC, OUI-based MAC, or custom MAC mask format. • **LLDP Capability** - Matches the device based on the LLDP capability from the source LLDP PDU. Options are: • **LLDP Src MAC + LLDP Capability** - Matches the device based on the source MAC of a LLDP PDU and the selected LLDP capability from the source LLDP PDU. Note: Instant Port will not function correctly if LLDP Transmit is disabled especially if LLDP-based matching is part of the Device Type profile. If you choose **MAC Learning** or **LLDP Src MAC**, configure the following fields: • **MAC Address/OUI** ◦ Select  and choose a MAC address. ◦ Select  to add a custom **MAC Address** or **MAC OUI**. ◦ Select  to edit a custom MAC Address or MAC OUI. • **MAC Mask** ◦ Enter a custom MAC mask format. ◦ Select the **Edit MAC Mask** check box, then edit the entry in the MAC Mask field. Instant Port uses Link Layer Discovery Protocol (LLDP) as one of its key device matching mechanisms, especially for: • LLDP Source MAC • LLDP Capability • LLDP MAC + Capability If LLDP is disabled on a port: • The switch cannot receive LLDP PDUs from the connected device. • The switch cannot transmit LLDP advertisements, which may be required for devices like VoIP phones to configure themselves (e.g., voice VLAN). • LLDP-based match rules will fail, and the device may fall into the non-match action (e.g., default port type or non-forwarding VLAN). However,LLDP Is Not Required If your Instant Port profile uses MAC-based matching only, then LLDP can be disabled and Instant Port will still work. For example: Match:

Table 8: IPP Device Type Settings (continued)

Field	Description
	Category: MAC OUI: "00:1A:2B" In this case, Instant Port relies on MAC Learning from untagged traffic and does not need LLDP. If you choose **LLDP Capability**, use the drop-down menu to select one of the following options: • Avaya Phone • Gen Tel Phone • Router • Bridge • Repeater • WLAN Access Pt • Docsis Cable Ser • Station Only • Other If you select **LLDP Src MAC + LLDP Capability**, configure the parameters as described above.
PORT USAGE tab	
Port Usage	Select a **Port Usage** option, as follows: • Access Port • Trunk Port (802.1Q VLAN Tagging) • Phone with a Data Port
VLAN tab	
VLAN	This field appears if **Port Usage** is configured as **Access Port**. Choose from the following actions: • Select and choose a VLAN. • Select to add a custom VLAN. Optionally, select the **Apply VLANs to devices using classification** check box. To add a classification rule, select To specify an existing classification rule, select . For more information, see Configure Classification Rules on page 50. • Select to edit a custom VLAN.

Table 8: IPP Device Type Settings (continued)

Field	Description
Native VLAN	This field appears if **Port Usage** is configured as **Trunk Port (802.1Q VLAN Tagging)**. Choose from the following actions: • Select and choose a Native VLAN. • Select to add a custom Native VLAN. Optionally, select the **Apply VLANs to devices using classification** check box. To add a classification rule, select To specify an existing classification rule, select . For more information, see Configure Classification Rules on page 50. • Select to edit a custom Native VLAN.
Allowed VLANs	This field appears if **Port Usage** is configured as **Trunk Port (802.1Q VLAN Tagging)**. Enter the VLAN names using comma delimiters (vlan1,vlan2,vlan3...).
Voice VLAN (tagged)	This field appears if **Port Usage** is configured as **Phone with a Data Port**. Choose from the following actions: • Select and choose a Voice VLAN. • Select to add a custom Voice VLAN. Optionally, select the **Apply VLANs to devices using classification** check box. To add a classification rule, select To specify an existing classification rule, select . For more information, see Configure Classification Rules on page 50. • Select to edit a custom Voice VLAN.
Data VLAN (untagged)	This field appears if **Port Usage** is configured as **Phone with a Data Port**. Choose from the following actions: • Select and choose a Data VLAN. • Select to add a custom Data VLAN. Optionally, select the **Apply VLANs to devices using classification** check box. To add a classification rule, select To specify an existing classification rule, select . For more information, see Configure Classification Rules on page 50. • Select to edit a custom Data VLAN.
STORM CONTROL tab	

Table 8: IPP Device Type Settings (continued)

Field	Description
Broadcast	Select **Broadcast** to include traffic that is forwarded to all destinations simultaneously.
Unknown Unicast	Select **Unknown Unicast** to include traffic whose destination address does not appear in the forwarding database.
Multicast	Select **Multicast** to include traffic whose destination is a multicast address.
Thresholds	The default is **Packet Based**.
Rate Limit Type	The default is **PPS** (packets per second).
Rate Limit Value	Enter (in packets per second) when the switch should discard traffic of the selected types.

Instant Port Profiles Delta Configuration Example

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

Figure 2: An example IPP configuration delta.

Instant Port Profile Example Workflow

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

To create a new Instant Port Profile:

1. Navigate to **Network Policy** > **Policy** > **Switching** > **Switch Settings** > **Instant Port Profiles.**
2. Enter the information for the Non-Forwarding VLAN, Default Port Type, and Non-Match Action.
3. Create, edit, or delete device types.
4. Define device types and their respective match criteria such as MAC learning, LLDP Source MAC, LLDP Capability, or a combination. For a device type to match based on MAC learning, the rule must be ordered above any LLDP-based assignment rules. This ensures that MAC learning takes precedence, irrespective of LLDP information.

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

   The options for port usage are:

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

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

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

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

Example Deployment Scenario: Optimizing Network for an Office

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

IPP offers the following advantages:

- Automatically assigns VLANs and applies appropriate settings to switch ports based on connected devices

- Ensure secure and efficient network operation

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

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

Next, configure Instant Port Profiles:

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

Then configure device types:

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

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

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

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

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

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

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

First, define device types for each connected device

Next, configure Instant Port Profiles:

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

Then configure device types:

- Add or edit device types
- Define matching criteria based on the characteristics of each device:
  - Device 1 (e.g., Laptop):
    - Sample MAC Address: 00:1A:2B:3C:4D:5E
    - Dynamic Configuration: Assign VLAN 10 based on the MAC address
  - Device 2 (e.g., Desktop Computer):
    - Sample MAC Address: 00:AA:BB:CC:DD:EE
    - Dynamic Configuration: Assign VLAN 20 based on the MAC address.

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

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

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

Instant Port Profiles Troubleshooting

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

Check the monitoring page after a match has occurred.

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

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

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

Instant Port Profiles Out of Sync

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

to resolve out of sync errors, to begin select **Update Devices** from the 3-dot menu. Then, in the **Update Devices** dialog, select **Delta Configuration Update** and select **Update**.

Hardware and Software Requirements

This feature is supported on the following hardware:

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

Note
Instant Port Profiles is not supported on Digital Twin.

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

Scaling

Instant Port Profiles scales to the following limitations:

- Maximum number of device-types per Instant Port Profile: 260

  Note
  Device must be running 32.x or higher.

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

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

Configure a Switch Template

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

You can make use of default templates, which are pre-loaded for each 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.

Note
When using a default template, you must **save it as a new template** before making changes. This ensures the original default remains unchanged.

Note
Templates created in one policy can be reused in others, streamlining configuration across your network.

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

Perform Device Configuration

Create a network policy and device template.

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

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

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

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

1. Go to **Configure** > **Network Polices** > **the existing network policy** > **Switching/ Routing** > **Switch Settings** > **Switch Templates** and select the template for the device model.
2. Ensure that **Enable Override Policy Common Settings** is set to **ON** to make any changes to device configuration.
3. For **STP Configuration**, see Configure STP Settings on page 44.
4. For **IGMP Settings**, toggle to **On** and make the following selections:
   - **Enable immediate leave**: Instructs the switch to remove a multicast host from the multicast forwarding table immediately upon receipt of a leave-group-membership message.
   - **Suppress redundant IGMP membership reports to optimize traffic**: Suppresses redundant IGMP membership reports from multiple hosts on a subnet. The switch sends a single report to the IGMP router, reducing traffic.
5. For **MAC Locking Settings**, select to control the forwarding database for learned MAC address entries on a port.

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

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

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

   Note
   ELRP must also be enabled within the switch template.

   Or

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

   Note
   If VLAN attributes has enabled DHCP Snooping settings, then the VLAN attributes will override the switch template.

8. For **MTU Settings**, enter a maximum transmission unit value for Ethernet interfaces.

   The MTU value determines the largest packet size that can be transmitted through your system.
9. For **PSE Settings**, toggle to **On** to configure maximum power thresholds to generate alerts to ExtremeCloud IQ about exceeding maximum power levels.

10. For **Management Interface Settings** (Switch Engine devices only), select one of the following options:
    - **VLAN Interface**: Select when the management interface is to be supplied by the management VLAN.
      - **Management VLAN**: Enter the VLAN to be used by the switch.
      - **Management IP Settings**: Select to enable DHCP on this interface.

Proceed to Port Configuration.

Configure STP Settings

Use this task to configure Spanning Tree settings.

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

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

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

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

Port and VLAN Configuration

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

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

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

The following configuration options are available:

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

Note

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

Configure Ports in Bulk

Before you begin, create a Switch template.

Use this task to create ports in bulk.

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

   Note
   If you need to create different templates for different VIMs on the same switch model, you can create a classification rule so that different devices have the same template with different VIM options.

   d. Select one or more of these VIM ports and continue to **Step 3**.
3. Configure the Table 9.

Table 9: Settings for Port Bulk Configuration

Setting	Description
Name	Enter a port type name.
Description	Enter a description of the port type.

Table 9: Settings for Port Bulk Configuration (continued)

Setting	Description
Status	Toggle **Status On** or **Off**.
Auto-Sense	Toggle **Auto-Sense On** or **Off** (Fabric Engine device only). **Auto-Sense** detects connected device types and automatically configures specific port settings. Certain port settings are not configurable.
Port Usage	Select one of the following port types: • **Auto-Sense Enabled**: The only option if previously selected. (Fabric Engine device only) • **Access Port**: Ports connected to individual hosts such as printers, servers, and end-user computers. • **Trunk port (802.1Q VLAN Tagging)**: Ports connected to network forwarding devices that support multiple VLANs on trunk ports. • **Phone with a Data Port**: Ports connected to IP phones, and optionally, to computers cabled to the phones.
Access Port	For an **Access Port**, select an existing VLAN or select the add icon to add a new one. Tag the VLAN to a particular access port to control and monitor switch traffic. To add a new VLAN, see Configure VLAN Settings on page 49. **Note:** For Switch Engine the **none** keyword is available for entry as a VLAN. Alternatively, a common object VLAN can be created with the VLAN ID using the **none** keyword. Using **none** removes the assignment of the native VLAN from the port.
Trunk Port	For a **Trunk Port**, select an existing **Native VLAN** or select the add icon to add a new one. The native (untagged) VLAN is the VLAN assigned to frames that do not have any 802.1Q VLAN tags in their headers. By default, Extreme Networks devices also use VLAN 1 as the native VLAN. To add a new VLAN, see Configure VLAN Settings on page 49. **Note:** For Switch Engine the **all** keyword can be used. Using **all** will automatically tag VLAN IDs to the ports that are also defined within other *port types* assigned to the Switch Engine device.
Allowed VLANS	For **Allowed VLANS**, enter a specific number or leave the **All** default.

Table 9: Settings for Port Bulk Configuration (continued)

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

Table 9: Settings for Port Bulk Configuration (continued)

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

Table 9: Settings for Port Bulk Configuration (continued)

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

4. Select **Save Port Type**.

Configure VLAN Settings

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

1. Go to **Monitoring** > **Network Devices**.
2. From the 3-dot menu, select **Configure** > **Device**.
3. Select +.
4. Type a **Name** for the new VLAN object.
5. 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)

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

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

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

15. 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.

16. Choose **Select**.
17. Select **SAVE VLAN**.

Configure Classification Rules

Before you can use classification rules, you must create a network location, along with cloud config groups, IP addresses, and IP subnets.

Extreme Platform ONE Networking supports multiple classification rules for DNS servers, VLANs, RADIUS servers, device templates, user groups, and private client groups (PCGs). You can create classification rules as part of a network policy or as a common object.

Important
Classification rules for IP objects are supported only when IP objects are used to create firewall rules.

- Configure **Device Location** rules to assign different DNS and RADIUS servers and different time zones to different physical locations.
- Configure **Cloud Config Groups** (CCGs) to create user passwords which restrict access to private and personal network devices.
- Configure **IP Address** classification rules to associate user groups so they can communicate using their own private networks.
- Configure **IP Subnet** classification rules to support multiple user-group private networks.
- Configure **IP Range** classification rules for multiple user-group private networks.

Use this task to configure classification rules.

1. Select an existing rule, and then select , or to add a new one, select .
2. Enter a **Name** for the rule.
3. (Optional) Enter a **Description** for the rule.

4. Select , and then choose the rule type to configure.

   Choose from the following rule types:

Table 10: Rule types

Selected rule type	Do this
Device Location	a. Drill down until you reach the location level at which the device resides. b. Select **Select**. The location appears in the **Classification Rules** table.
Cloud Config Group	a. Select the **Match Type**. b. Select and choose an existing group, or select . c. Select **CLOUD CONFIG GROUP**. d. Select **CONTINUE**.
IP Address	a. From the **Match Type** menu, select **Contains** or **Does Not Contain**. b. Select and choose an existing IP address, or select . If you do not see the IP address that you want, select **New** to create a new IP address. c. Select **SAVE IP**. d. Select **CONTINUE**.
IP Subnet	a. From the **Match Type** menu, select **Contains** or **Does Not Contain**. b. Select and choose an existing IP subnet, or select menu. If you do not see the IP subnet that you want, select **New** to create a new IP subnet. c. Select **SAVE SUBNET**. d. Select **CONTINUE**.
IP Range	a. From the **Match Type** menu, select **Contains** or **Does Not Contain**. b. Select and choose an existing IP range, or select . If you do not see the IP range that you want, select **New** to create a new IP range. c. Select **SAVE IP**. d. Select **CONTINUE**.

5. Select **SAVE RULE**.

6. 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.

   Extreme Platform ONE Networking uses a top-down, first-match, stop-on-match processing method for these objects. Therefore, if a device is a member of more than one matching object for an element, only the first match applies.

Add a Cloud Config Group

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

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

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

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

Aggregate LAG and LACP Ports

Create or modify a switch template.

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.

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

1. Select the ports you want to aggregate, and then select **AGGREGATE PORTS** .

   Alternatively, select **Assign** > **Advanced Actions** > **Aggregate**.
2. Enter an optional description.
3. Toggle **LACP (Link Aggregation Control Protocol)** to **ON**.

   If LACP (Link Aggregation Control Protocol) is disabled, Extreme Platform ONE Networking creates a static LAG.
4. Use the arrows to add or remove ports from the LAG.
5. Select the **Master Port**.
6. Select a **Port Load Balancing** option.

Configure Individual Ports

First, create or modify a switch template as part of a Network Policy.

Note
For create or modify a switch template as part of Common Objects, see the Extreme Platform ONE Networking User Guide.

Create or modify a switch template, then select from the menu.

Note
To modify an existing port, select the **Port Type** from the list and then select the edit icon. You can edit all port parameters from the **Summary** page.

Use this task to configure or modify settings for individual ports.

Note
To support Stacking Mode for Switch Engine 5320-16P-2MXT-2X switch templates, select the edit button next to the ports and enable to **Stacking Support Mode** toggle.

1. In the switch template, select **Configuration** > **Port/VLAN Configuration**.
2. For **Port Name & Usage** and **VLAN**, see Configure Port Details on page 53.
3. For **Instant Secure Port Settings**, see Configure Authentication on page 54.
4. For **Transmission Settings**, see Configure Transmission Settings on page 55.
5. For **STP**, see Configure STP Settings on page 55.
6. For **Storm Control**, see Configure Storm Control on page 56.
7. For **MAC Locking**, see Configure MAC Locking on page 57
8. For **ELRP**, see Configure ELRP on page 57
9. For **PSE**, see Configure PSE on page 58.
10. Review the settings on the **Summary** tab, and then select **SAVE**

Configure Port Details

Create or modify a switch template, and then open it for configuration. See Configure Individual Ports on page 53.

The **PORT DETAILS** tab of the **Configure Ports Individually** table displays the following information:

- **Interface**: The interfaces available for the switch, such as Eth1/0/1-Eth1/0/52.
- **Port Type**: Indicates the current port usage setting.
- **Enabled**: Indicates whether the port is currently activated.
- **LACP**: Indicates link aggregation control protocol for a member of a link aggregation port group. See Aggregate LAG and LACP Ports on page 52.

- **VLAN**: This column displays the VLAN assigned to the port. Change the VLAN number directly in the VLAN text box.
- **Description**: A brief description of the port.

Tip
These settings appear in the **Info & VLAN** section of the **Summary** tab.

Use this task to configure the settings for a new port, on the **Port Name & Usage** and **VLAN** tabs.

1. Under **Configure Ports Individually**, select the the **Port Details** tab.
2. For the interface that you want to configure:
   - To edit an existing port, select .
   - To configure a new port, select .
3. Configure the settings on the **Port Name & Usage** tab:
   a. Type a **Name** for the new port.
   b. Type a **Description** for the new port.
      Although optional, descriptions can be helpful when you are troubleshooting your network.
   c. Toggle the **Status** to **ON** or **OFF**.
4. Select the **Port Usage** setting:
   - **Access Port**: Ports connected to individual hosts such as printers, servers, and end-user computers.
   - **Phone with a data port**: Ports connected to IP phones, and optionally, to computers cabled to the phones.
   - **Trunk port**: Ports connected to network forwarding devices, such as switches and APs that support multiple VLANs on trunk ports.
5. Select **NEXT** to open the **VLAN** tab.
6. For **VLAN**, select and choose an existing object, or to add a new one, select . to create a new VLAN object.
7. Select **NEXT**, or select the **User Authentication** or **QoS** tab, and continue configuring the port.
8. Select the **Instant Secure Port Settings** tab, and continue configuring the port.

Configure Authentication

First configure the **Port Name & Usage** and **VLAN** tabs.

Tip
These settings appear in the **Authorization** section of the **Summary** tab.

Use this task to configure the authentication settings for a new port, on the **Instant Secure Port Settings** tab.

Note
The **User Authentication** tab is part of the taskflow for older Dell and SR-based devices.

1. Toggle **User Authentication** to **ON** or **OFF**.
2. Toggle **MAC Authentication** to **ON** or **OFF**.
3. Select **NEXT**, or select the **Transmission Settings** tab, and continue configuring the port.

   See Configure Transmission Settings on page 55.

Configure Transmission Settings

First, Configure Authentication on page 54.

Tip
These settings appear in the **Port Settings** section of the **Summary** tab.

Use this task to configure the settings for a new port, on the **Transmission Settings** tab.

1. For **Transmission Type**, select **Auto**, **Half-Duplex**, or **Full-Duplex**.

   Auto causes the switch to negotiate the best possible duplex mode possible with the connected device. **Full-Duplex** forces the switch to communicate with the connected device using full-duplex communication. **Half-Duplex** forces the switch to use half-duplex communication.
2. Select the **Transmission Speed** the switch port uses to communicate with the connected device.
3. To display learned switch port client MAC addresses on ExtremeCloud IQ monitoring screens, select **Client Reporting**.

   When client reporting is disabled, client MAC addresses are not displayed. It is disabled when **CDP Receive** is turned off.
4. To enable Cisco Discovery Protocol (CDP), select **Enable CDP Transmit/Receive**.
5. To enable the switch to transmit LLDPDU frames, select **LLDP Transmit**.
6. To enable the switch to receive LLDPDU frames, select **LLDP Receive**.
7. To enable Link Layer Discovery Protocol-Media Endpoint Discovery, select **Enable LLDP MED Capabilities**.
8. Select **NEXT**, or select the **STP** tab, and continue configuring the port.

   See Configure STP Settings on page 55.

Configure STP Settings

First Configure Transmission Settings on page 55.

Note
Extreme Networks recommends that you enable STP.

Extreme Networks switches can use Spanning Tree Protocol (STP) to activate links with the lowest cost (highest bandwidth), establish backup links where possible, and prevent Layer 2 network loops, which can result in duplicate unicast frames and broadcast storms. Bridge Protocol Data Unit (BPDU) protection is a security feature designed to protect the active STP topology by preventing spoofed BPDU packets from entering the STP domain. BPDU protection is applied to edge ports connected to end-user devices that do not run STP. If an STP BPDU protected port receives packets, this feature disables that port and alerts the network admin.

The BPDU Restrict feature disables the port as soon as a BPDU is received on the BPDU restrict port, blocking the loop. Specify a BPDU recovery timeout, enabling the port after the configured amount of time.

Note
You can enable BPDU Restrict only when Edge port is also enabled.

By default, STP is disabled. Use this task to enable STP and configure the settings for an individual port, on the **STP** tab.

1. Toggle **STP ON**.
2. Toggle **Edge Port ON** so the 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.
3. For **BPDU Protection**, select **Guard** or **Disabled** status.
   - **Guard**: Controls whether a port explicitly configured as Edge disables itself upon reception of a BPDU. The port enters the error-disabled state, and is removed from the active topology.
   - **Disabled**: Turns off BPDU Protection.
4. Select the port **Priority**.

   If Spanning Tree Mode is set to STP, set the port priority to either 0 or 16.
5. Select **NEXT**, or select the **Storm Control** tab, and continue configuring the port.

   See Configure Storm Control on page 56.

Configure Storm Control

First Configure STP Settings on page 55.

Extreme Networks switches can mitigate traffic storms by tracking the source and type of frames to determine whether they are legitimately required. Switches then discard frames that are determined to be the products of a traffic storm. You can apply storm control to broadcast, unknown unicast, and multicast traffic, and configure packet-based or byte-based rate limit thresholds for each interface.

Tip
These settings appear in the **Storm Control** section of the **Summary** tab.

Use the following procedure to configure traffic storm mitigation for an individual port.

1. Select the traffic to include:
   - Select **Broadcast** to include traffic that is forwarded to all destinations simultaneously.
   - Select **Unknown Unicast** to include traffic with a destination address does not appear in the forwarding database.
   - Select **Multicast** to include traffic with a multicast address as a destination.
2. Type the **Rate Limit Value** for discarding traffic of the selected types.
3. Select **NEXT**, or select the **MAC Locking** tab, and continue configuring the port.

   See Configure MAC Locking on page 57.

Configure MAC Locking

First, configure Configure Storm Control on page 56.

Configure MAC locking security to control the forwarding database for learned MAC address entries on a port. You must also enable MAC locking in the switch template.

Use this task to configure the settings for MAC locking.

1. Toggle **MAC Locking Enable** to **ON**, and configure the settings.

Table 11: MAC Locking settings

Setting	Description
Maximum First Arrival	Specify the number of first-arrival MAC addresses allowed to communicate on the port. Range (0-600)
Disable Port	To disable the port when the maximum first arrival limit is exceeded, toggle **Disable Port** to **ON**.
Link Down Action	Select one of the following options: • **Clear first arrival MACs when port link goes down** • **Retain first arrival MACs when port link goes down**
Remove Aged MACs	To remove learned MAC Addresses after they age out from the switch forwarding database, toggle **Remove Aged MACs** to **ON**.

2. Select **NEXT**, or select the **ELRP** tab, and continue configuring the port.

   See Configure ELRP on page 57.

Configure ELRP

First, Configure MAC Locking on page 57.

Extreme Loop Recovery Protocol (ELRP) is a loop protection mechanism designed to detect and prevent loops. In Extreme Platform ONE Networking you can configure ELRP client periodic packet transmission for VLAN(s) assigned to a port type. You must also enable ELRP in the switch template.

Use this task to enable and configure ELRP.

1. Toggle **Enable ELRP client and disable port when a loop is detected on applied access or trunk VLANs assigned to the port type** to **ON**.
2. To prevent the ELRP client port from being disabled, toggle **ELRP Exclude** to **ON**.
3. Select **NEXT**, or select the **PSE** tab, and continue configuring the port.

Configure PSE

Create or modify a switch template.

Tip
These settings appear in the **PSE Settings** section of the **Summary** tab.

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

1. Select an existing PSE profile from the menu, or select .
2. Type a **Name**.
3. For **Power Mode**, select **802.3af** or **802.3at**.

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

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

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

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

   Although optional, descriptions can be helpful when you are troubleshooting your network.
7. Select **SAVE**.
8. Toggle **POE Status** to **ON** or **OFF**.
9. Select **NEXT**, or select the **Summary** tab, and review the settings for the port.
10. Select **SAVE.**

Universal Port Stacking Support Mode

Switch Engine 4000 Series hardware allows for the configuration of Universal Port Stacking Support Mode. When Stacking Support Mode is disabled, Universal Ports U1 and U2 operate as non-stacking ports. Once stacking ports are no longer defined as stacking, then all Extreme Platform ONE Networking supported port configurations

apply, including configuration by port type and configurations associated with ports such as Instant Port/Instant Secure Port configurations.

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

To Enable or Disable Universal Port Stacking Support Mode:

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

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

7. Select **Apply**.

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

Configure Switch Template Advanced Settings

First, create or modify a switch template as part of a network policy.

Note
To create or modify switch template as part of Common Objects, see the Extreme Platform ONE Networking User Guide.

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

1. In the switch template, select **Configuration** > **Advanced Settings**.
2. For **Upgrade device firmware upon device authentication**, select **On** to upgrade the device firmware upon onboarding.

   If you have activated device firmware upgrading, select one of two options:

   - Update firmware to the latest version.
   - Upgrade to a specific device firmware version.

3. To reboot and roll back a device to a previous configuration if there are issues with the template configuration, select **On** for **Upload Configuration Automatically**, followed by the check box below.
4. To use **Supplemental CLI**, select **On**.

   For more information, see Configure Supplemental CLI on page 60.

Complete configuring the device template.

Configure Supplemental CLI

First, enable Supplemental CLI in Extreme Platform ONE Networking. Go to **Administration & Settings** > **Backup & Restore** > **VIQ Management**, and toggle **Supplemental CLI** to **ON**.

Create or modify a switch template as part of a network policy.

Note
To create or modify switch template as part of Common Objects, see the Extreme Platform ONE Networking User Guide.

After you save supplemental CLI objects containing CLI commands, you can update the commands for devices automatically.

To avoid an unnecessary system reboot, select **Delta Configuration Update**. Extreme Platform ONE Networking attempts to update only the configuration deltas. If a full update is required, the system prompts you to select **Complete Configuration Update**. Examples of CLI commands that require a full configuration update are: **`system antenna-type`** and **`system environment`**.

Use this task to configure supplemental CLI (sCLI) objects.

1. In the switch template, select **Configuration** > **Advanced Settings**.
2. Select an existing Supplemental CLI object, and then select  , or to add a new one, select  .
3. Type a **Name**.
4. (Optional) Type an optional **Description**.

   Although optional, descriptions can be helpful when you are troubleshooting your network.
5. Type or paste the **CLI commands** into the field.
   - Enter multiple CLI commands, one command per line, not exceeding a maximum total of 8192 characters.
   - Use CLI Commands that contain IP and VLAN objects: **`${ip:ip_object_name}`** and **`${vlan:vlan_object_name}`**.
   - Perform a complete configuration update each time commands are appended to device configurations.
   - For Dell EMC switches, enter the CLI commands, `enable`, and `config` in the beginning of a sequence of CLI commands.
6. Select **SAVE TEMPLATE**.

Device Management Server Settings

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select at the end of a device row, and then select **Configure** > **Device**.
3. Under the **Configuration** menu, select **Device Management Servers**.
4. Select **Unlock** to enable switch-level configuration changes.

DNS Server Settings

5. Select **DNS Server**.
6. Toggle **DNS Server** to **ON**.

> **Note**
> Use DNS Server for domain name-to-IP address resolution. Extreme Networks devices that are DHCP clients can receive a domain name and DNS Server IP Address through DHCP, although any DNS settings that you enter here override those dynamically applied.

7. Enter a **Domain Name** for the default DNS server.
8. To add a new DNS server, select , and then:
   a. Enter an **IP Address** for the DNS server.
   b. Select a **Routing Instance**.
   c. Select **ADD**.

   You can add up to three servers. The first entry is the primary server. The secondary entry is the secondary server, and the third entry is the tertiary server. Use the arrows in the **Order** column to change the order.
9. To delete a DNS server from the list, select the DNS servers, and then select (delete).

NTP Server Settings

10. Select **NTP Server**.
11. Toggle **NTP Server** to **ON**.

> **Note**
> When enabled, Extreme Networks devices synchronize their time with specified servers. Devices use a manually set time if synchronization is disabled. Fastpath and X435 switches support SNTP, but do not support NTP. Use an NTP server with an IP Address instead of a Fully Qualified Domain Name for VOSS platforms.

12. To add a new NTP server to the list, select .
    a. Enter an **NTP Server**.
    b. Select a **Routing Instance**.
    c. Select **ADD**.
13. To delete an NTP server from the list, select the NTP servers, and then select (delete).

SNMP Server Settings

14. Select **SNMP Server**.
15. Toggle **SNMP Server** to **ON**.
16. Enter an **SNMP Contact** for the default SNMP server.
17. Select an existing SNMP server, and then select , or to add a new one, select .
18. Configure the following SNMP server settings, and then select **ADD SNMP SERVER**:

Table 12: Settings for SNMP servers

Setting	Description
SNMP Server	Type a name for the server.
Version	From the drop-down list, select the version of SNMP that is running on the management station that you intend to use.
Operation	Select the type of activity to permit between the specified SNMP management station and the devices in the network policy to which you will assign this profile. Options include: • **None**: Disable all SNMP activity for the specified management station. • **Get**: Permit GET commands sent from the management station to a device to retrieve MIBs. • **Get and Trap**: Permit the reception of GET commands from the management station and the transmission of traps to the management station. • **Trap**: Permit devices to send messages notifying the management system of events of interest.
Community	For SNMP V2C and V1, enter a text string that must accompany queries from the management station. The community string acts similarly to a password, such that devices accept queries only from management stations that send the correct community string.
Routing Instance	Select the SNMP server routing instance.

Note
Use the arrows in the **Order** column to change the order.

19. To delete an SNMP server from the list, select the SNMP servers, and then select (delete).

Syslog Server Settings

20. Select **Syslog Server**.
21. Toggle **Syslog Server** to **ON**.

Note
When enabled, Extreme Networks devices save the event log entries to the Syslog servers specified.

22. Select a **Syslog Facility**.
23. To add a new Syslog server, select , and then:
    a. Enter a **Syslog IP Address** for the Syslog server.
    b. Select a **Severity** level.
    c. Type the **Port** number.
    d. Select a **Virtual Routing** instance.
    e. Select **ADD**.

    Note
    Use the arrows in the **Order** column to change the order.

24. To delete a Syslog server from the list, select the Syslog servers, and then select (delete).

RADIUS Server Settings

25. Select **RADIUS Server**.
26. Toggle **RADIUS Server** to **ON**.
27. Select one of the following options:

- **Use Extreme Platform ONE RADIUS Cloud Configuration**: Enables the device to use the cloud-based RADIUS configuration provided by UZTNA for authentication.

  Note
  UZTNA is provisioned through the UZTNA application. If UZTNA settings or license is not properly configured, then device authorization may fail.

- **Use Extreme Platform ONE Security RADIUS Proxy Servers**: Enables the device to route RADIUS authentication requests through Extreme Platform ONE Security proxy servers for secure handling and centralized control. Select the **Primary RADSEC Proxy Server** and the **Secondary RADSEC Proxy Server**.

Configure a DNS Server

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

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

1. Enable the **DNS Server** to **ON**.

2. Choose to use an existing DNS Server Setting, or add new.
3. Enter a name for the server.
4. (Optional) Enter a **Domain Name** and **Description**.
5. 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.
6. 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 Classification Rules on page 50.
7. Select **Save DNS Server**.
8. If you are ready to deploy the network policy, select **Next** or continue to the next Management server.

Configure NTP Server Policy Settings

NTP is a critical service for ExtremeCloud managed devices and is required to permit each device to securely connect with Extreme Platform ONE Networking and related services and to ensure alerts and events have the correct timestamp.

By default, Extreme Networks switches try to contact the NTP server assigned by your DHCP server. If your DHCP server does not advertise an NTP server, the device automatically attempts to resolve and connect to the NTP server at `0.aerohive.pool.ntp.org`. Device DNS must be functioning correctly to contact the NTP server.

Either your DHCP-defined NTP server or the default NTP server must be reachable outbound on UDP port 123 by each device connecting to Extreme Platform ONE Networking.

Note
If using a Windows server as your NTP server, your Windows server must synchronize with an upstream NTP server for Extreme APs to trust and accept responses from the Windows NTP server.

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

Note
If enabled, these NTP server settings override the default NTP behaviors of your managed devices. The NTP servers defined here must be reachable from your managed devices on outbound UDP port 123.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing network policy, and then select , or to add a new one, select .
3. For **Policy Settings**, select **NTP Server**.

4. Toggle **NTP Server** to **ON**.
5. To use existing NTP server settings, select , and choose an NTP object.
6. Configure NTP Server Settings on page 65.
7. To add a new NTP server to the list, select .
   a. To use an existing NTP, select , and choose a server.
   b. To add a new NTP server, select , and then select **IP Address** or **Host Name**.
   c. Type a **Name** for the new object.

      You can use the menu to change your previous selection (**IP Address** or **Host Name**).
   d. Select **SAVE IP OBJECT**.
   e. Select **ADD**.

      Extreme Platform ONE Networking accesses NTP servers in order, from the top down. Use the arrows to rearrange them.
8. If you want to use classification, select **Apply NTP servers to devices via classification**.
   a. To add a classification rule, select .
   b. To specify an existing classification rule, select .

   For more information, see Configure Classification Rules on page 50.
9. Select **SAVE NTP SERVER**.

NTP Server Settings

Table 13: Settings for NTP server profiles

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

Configure SNMP Server Policy Settings

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

This task is part of the network policy configuration workflow. Use this task to configure **SNMP Server Policy Settings** for a network policy.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing network policy, and then select , or to add a new one, select ..
3. For **Policy Settings**, select **SNMP Server**.
4. Toggle **SNMP Server** to **ON**.
5. To use existing SNMP server settings, select , and choose an SNMP server.
6. Configure the SNMP Server Settings on page 67.
7. To add a new SNMP server, select , and then select **IP Address** or **Host Name**.

   You can add up to three SNMP servers to the profile.
8. To use an existing SNMP server, select it from the menu.
9. Type a **Name** for the new IP object.

   You can use the menu to change your previous selection (**IP Address** or **Host Name**).
10. Select **SAVE IP OBJECT**.
11. For **Version**, select the version of SNMP that is running on the management station you intend to use.
12. For **Operation**, select the type of activity to permit between the specified SNMP management station and the devices assigned to this profile in the network policy.
    - **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 reception of GET commands from the management station and transmission of traps to the management station.
    - **Trap**: Permit devices to send messages notifying the management system about events of interest.
13. In the Community field (for SNMP V2C and V1), type a text string that must accompany queries from the management station.

    The community string acts similarly to a password, in that devices accept queries only from the management stations that send the correct community string.
14. Select **ADD SNMP SERVER**.
15. (Optional) Select **Apply SNMP servers to devices via classification**.

    a. To add a classification rule, select .

    b. To specify an existing classification rule, select .

    For more information, see Configure Classification Rules on page 50.
16. Select **SAVE SNMP SERVER**.

SNMP Server Settings

Table 14: Settings for SNMP servers

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

Table 14: Settings for SNMP servers (continued)

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

Configure Syslog Server Policy Settings

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. Syslog server settings can be configured as common objects, from within the network policy workflow, and at the device level. Device-level settings override network policy settings.

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, as a best practice, have all syslog clients use the same NTP time server. See Configure NTP Server Policy Settings on page 64.

This task is part of the network policy configuration workflow. Use this task to configure the **Policy Settings** for a Syslog server.

1. Go to **Configuration** > **Network Policies**
2. Select an existing network policy, and then select , or to add a new one, select .
3. For **Policy Settings**, select **Syslog Server**.
4. Toggle **Syslog Server** to **ON**.

5. To use existing syslog server settings, select , and choose a syslog server.
6. Configure the Configure Syslog Server Policy Settings on page 68.
7. To add a new syslog server to the table, select .

   Use the up or down arrows to reorder the list of syslog servers in the table.
8. Select , and choose an existing syslog IP address or host name, or select .
9. For **Severity**, select the log level.
10. Type the **Port** number.
11. Select **ADD**.
12. Select **Assign Syslog servers via Classification**.

    a. To add a classification rule, select .

    b. To specify an existing classification rule, select .

    For more information, see Configure Classification Rules on page 50
13. Select **SAVE SYSLOG SERVER**.

Syslog Server Settings

Table 15: Settings for Syslog servers

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

Table 15: Settings for Syslog servers (continued)

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

Configure LLDP/CDP Policy Settings

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

Note

LLDP is on by default in Extreme Platform ONE Networking. In IQ Engine, LLDP was previously off by default. With IQ Engine Release 10.7.5 and later, LLDP is on by default. This is the new default behavior for all new devices running 10.7.5 and later.

If LLDP is disabled in the network policy, upgrading to 10.7.5 enables LLDP until after you perform a configuration update.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing network policy, and then select , or to add a new one, select .
3. For **Policy Settings**, select **LLDP/CDP**.
4. Toggle **LLDP/CDP** to **ON**.
5. To use existing LLDP/CDP settings, select , and choose an LLDP/CDP object.
6. Configure the LLDP and CDP Settings on page 71.

LLDP and CDP Settings

Table 16: Settings for LLDP and CDP

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

Deploy a Network Policy

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. Extreme Platform ONE Networking pushes all configuration uploads as complete uploads. This action requires devices to reboot and activate the new configurations. Network policies can only be pushed to real devices (not simulated devices).

This task is part of the network policy configuration workflow. Use this task to deploy a network policy.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing policy, and then select , or to add a new one, select ..
3. After you configure the network policy, select the devices to which you want to upload the policy.
   - To automatically select the check boxes for all of the devices, select the check box in the top left of the table header.
   - To upload your network policy to specific devices only, select the corresponding check boxes for those devices.

     Use the **Assigned**, **Eligible**, and **Filtered** controls to customize your view of the devices that appear in the table.
4. Select **UPLOAD**.
5. 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.
6. Select **Enable Distributed Image Upgrade** when WAN speed and traffic usage are concerns.

   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.
7. Select **PERFORM UPDATE**.

Routing

Network Allocation

Network Allocation supports the creation of IP subnetwork configuration. A subnetwork with a selected VLAN can be applied to a device within the Routing section. When entries are added in the Network Allocation table, the Local IP Address Space field is valid only if it's a subnet address, not a host address. This table allows the user to create subnetworks which will be then used to the configure IP addresses per VLAN in the next table.

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

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

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

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

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

5. Configure the following IPv4 Network Allocation settings:

Table 17: Network Allocation Settings

Setting	Description
VLAN Attribute	A VLAN attribute can be created from within the VLAN attribute section within the Network Policy Switching Section.
Name	The name of your subnetwork.
Description	A description of your subnetwork.
Local IP Address Space	Define the local IP address space using CIDR notation, such as `10.1.0.0/16`. At the template level the IP address must be the valid network address and not a host address within the subnet range you are creating.
Clients Per Subnet	Shows the clients per subnet.
Select One	• Use the first IP address of the local IP address space for the IPv4 interface • Use the last IP address of the local IP address space for the IPv4 interface
Enable DHCP Relay	Enable DHCP Relay. If enabled, select or create a DHCP Relay Common Object.

Template-level IP Address Specifications

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

Using 10.35.1.160 will create the following IP Address parameters:

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

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

Static Routes

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

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

To configure Static Routes:

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

Table 18: Static Route Attributes

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

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

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

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

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

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

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

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

Configure a Switch Engine Device Switch Stack

Create a Switch Engine Device Stack on page 78
Creating a New Instant Secure Port Profile on page 78

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

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

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

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

   The new or cloned switch stack template displays on the network policy's **Switch Template** page.
10. Select the template to display the **Device Template** configuration page.
11. Refer to Configure a Switch Template on page 41.

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

12. Save the configuration.

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

For any post-configuration switch stack issues, see Switch Stack Issues on page 127. Now that you have created the switch stack, you can automatically create more if they are configured exactly the same way.

Create a Switch Engine Device Stack

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

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

Use this task to instantly configure a Switch Engine stack in Extreme Platform ONE Networking.

1. Go to **Monitoring** > **Network Devices** and select a device from the list.
2.

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 80.

Creating a New Instant Secure Port Profile

Note
The Instant Secure Port Profile (ISPP) option will only become available when Extreme Platform ONE Security is activated.

You must create a network policy.

Use the **Configuration** > **Network** page to see all the devices that have been onboarded to Extreme Platform ONE Networking. Add the network policy to the desired Switch Engine.

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

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

To create a new Instant Secure Port Profile:

1. Go to **Monitoring** > **Network Devices**.
2. From the 3-dot menu, select **Configure** > **Device**.
3.
4. Within **Port/VLAN Configuration** select the **Instant Secure Port Profile** tab.
5. Enter the name for your ISPP. The name is unique within Extreme Platform ONE Networking but is not pushed to the device.
6. Choose whether to use Unauthenticated VLAN. Unauthenticated VLAN is either a common object or can be created when the profile is created. If the Enable Unauthenticated VLAN is selected, then this VLAN will override the untagged VLAN in the port type and will be used as the Unauthenticated VLAN on the Switch Engine device when the configuration is pushed.
7. Specify the order in which to execute authentication. The order is per profile; therefore the same order is used for the entire Switch Engine device once the configuration is pushed. Use the arrows to change the default order.
8. Pick the RADIUS server for the Instant Secure Profile. Selecting **Use Extreme Platform ONE Security RADIUS Cloud configuration** uses either the free cloud RADIUS server set up per RDC, or configured proxy RADIUS servers in the Extreme Platform ONE Security application. Select one of the radio buttons to decide which type to use. Further, in the case of proxy RADIUS, you can select up to two proxy RADIUS servers; it is assumed that the ones selected have reached a deployed state after being configured in Extreme Platform ONE Security.
9. Select **Save**.

Configure Device-Specific Settings

Use Extreme Platform ONE Networking to modify switch templates at the device level. Settings made at this level (**Monitoring** > **Network Devices** > **Device Status** > **`switch_name`** > **`three dot menu`** > **Configure** > **Device**) apply only to the device and override the template settings configured in the network policy. If you undo the device-level settings, the device automatically reverts back to the original network policy and device template configuration. To revert to the settings in the network policy, select **Actions** from above the Device List. To configure settings at the network policy level, see Configure the Network Policy on page 23.

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

Configure Wired Devices

The following configuration options are offered on the 3-dot menu for each wired device. Select ⋮ > **Configure** > **Device**.

- Device Configuration: Edit device details such as the host name, the description, the device function, IP addresses, and VLAN assignments.
- Device Management Servers: Edit management server settings for a device associated with a network policy.

- Port/VLAN Configuration: Edit switch ports, STP, Storm Control, PSE, and VLAN attributes.

  Note
  Fabric Engine devices support EAPoL, SLPP, and VLAN/ISID configuration with VLAN attributes.

- Device Credentials: Assign or change network administrator credentials and administrator assignments.
- Interface Configuration: Add, edit, or delete interface configurations.
- Routing Configuration: Configure IP4 Static Routes.

After you make changes to the configuration, you must push the configuration changes to the device.

Wired Device Configuration

Making device configuration changes at the wired device level overrides the equivalent settings in the network policy assigned to the device, after you push the updated configuration to the device.

Use this task to make device configuration changes at the device level.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select at the end of a device row, and then select **Configure** > **Device**.
3. Under the **Configuration** menu, select **Device Configuration**.
4. Configure the **Device Details**:
   - **Host Name**: Enter a unique host name for the device. It can contain up to 32 characters and can include spaces.
   - **SNMP Location**: Enter a location name, for example `headquarters, building 1`.
5. Configure the **Network Details**:
   - **Network Policy**: Select a network policy from the drop-down list of existing policies.
   - **Device Template**: Select a device template from the drop-down list of existing templates, or clone an existing template.

     Note
     Fabric Engine devices do not support device templates.

6. Toggle **Management Interface Settings** to **On** or **Off**.

   When enabled, management interface settings specified below are applied and override template-level management interface settings. If disabled, you can apply template settings, or the device will use manually configured management interface settings. Leave disabled when using **Out-Of-Band Management**.

   - **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 **Static Address** or **Dynamic Address Configuration (DHCP) Client** to enable DHCP on this interface.
7. (Optional) Configure **Supplemental CLI**:
   a. **Apply Supplement CLI from network policy switch template**: Include the supplemental CLI object in the network policy and append the selected CLI object from the list. If you select a supplemental CLI object from the list, or create a new one, it is appended to the end of the configuration list, after the supplemental CLI object in the network policy.
   b. **Override Supplement CLI from network policy Supplement CLI**: Enable the network policy to override supplemental CLI objects for the device. For more information, see Configure Supplemental CLI on page 60.

   Note
   Fabric Engine only supports Supplemental CLI from device-level configuration.

   Important
   Before you can configure Supplemental CLI access on a device, you must first enable Supplemental CLI. Go to **Administration & Settings** > **Backup & Restore**, and then enable **Supplemental CLI**.

8. Select **Save Configuration**.

   For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 107.

Device Management Servers

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

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

For stacks, the unlock and revert action applies to all units/slots within the page. This enables the full stack to revert to the currently assigned network policy. Also, the

Device Management Servers is not available until you apply the network policy to both single switches and stacks.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select ⋮ at the end of a device row, and then select **Configure** > **Device**.

   Note
   This action is available only for managed devices. If the device is not currently managed, to change the management status of the device, select **Change Management Status** > **Manage**.

3. Under the **Configuration** menu, select **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:
   - DNS Server
   - NTP Server
   - SNMP Server
   - Syslog Server
   - RADIUS Server (Fabric Engine devices only)

   Note
   DNS Server, NTP Server, SNMP Server, and Syslog Server configurations can be managed at the device level for Switch Engine/EXOS and Fabric Engine/VOSS after unlock. Not all management server tabs are available for all device types. EXTREME PLATFORM ONE RADIUS and EXTREME PLATFORM ONE RADIUS Proxy Servers are supported only for Fabric Engine devices under device management servers. The **RADIUS Server** tab provides a **Use Extreme Platform ONE Security RADIUS Cloud Configuration** toggle.

6. Select **SAVE CONFIGURATION**.

   The changes only apply at the device level.

   For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 107.

Device Management Server Settings

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select ⋮ at the end of a device row, and then select **Configure** > **Device**.
3. Under the **Configuration** menu, select **Device Management Servers**.
4. Select **Unlock** to enable switch-level configuration changes.

DNS Server Settings

5. Select **DNS Server**.

6. Toggle **DNS Server** to **ON**.

   Note
   Use DNS Server for domain name-to-IP address resolution. Extreme Networks devices that are DHCP clients can receive a domain name and DNS Server IP Address through DHCP, although any DNS settings that you enter here override those dynamically applied.

7. Enter a **Domain Name** for the default DNS server.
8. To add a new DNS server, select , and then:
   a. Enter an **IP Address** for the DNS server.
   b. Select a **Routing Instance**.
   c. Select **ADD**.

   You can add up to three servers. The first entry is the primary server. The secondary entry is the secondary server, and the third entry is the tertiary server. Use the arrows in the **Order** column to change the order.
9. To delete a DNS server from the list, select the DNS servers, and then select (delete).

NTP Server Settings

10. Select **NTP Server**.
11. Toggle **NTP Server** to **ON**.

    Note
    When enabled, Extreme Networks devices synchronize their time with specified servers. Devices use a manually set time if synchronization is disabled. Fastpath and X435 switches support SNTP, but do not support NTP. Use an NTP server with an IP Address instead of a Fully Qualified Domain Name for VOSS platforms.

12. To add a new NTP server to the list, select .
    a. Enter an **NTP Server**.
    b. Select a **Routing Instance**.
    c. Select **ADD**.
13. To delete an NTP server from the list, select the NTP servers, and then select (delete).

SNMP Server Settings

14. Select **SNMP Server**.
15. Toggle **SNMP Server** to **ON**.
16. Enter an **SNMP Contact** for the default SNMP server.
17. Select an existing SNMP server, and then select , or to add a new one, select .

18. Configure the following SNMP server settings, and then select **ADD SNMP SERVER**:

Table 19: Settings for SNMP servers

Setting	Description
SNMP Server	Type a name for the server.
Version	From the drop-down list, select the version of SNMP that is running on the management station that you intend to use.
Operation	Select the type of activity to permit between the specified SNMP management station and the devices in the network policy to which you will assign this profile. Options include: • **None**: Disable all SNMP activity for the specified management station. • **Get**: Permit GET commands sent from the management station to a device to retrieve MIBs. • **Get and Trap**: Permit the reception of GET commands from the management station and the transmission of traps to the management station. • **Trap**: Permit devices to send messages notifying the management system of events of interest.
Community	For SNMP V2C and V1, enter a text string that must accompany queries from the management station. The community string acts similarly to a password, such that devices accept queries only from management stations that send the correct community string.
Routing Instance	Select the SNMP server routing instance.

Note
Use the arrows in the **Order** column to change the order.

19. To delete an SNMP server from the list, select the SNMP servers, and then select (delete).

Syslog Server Settings

20. Select **Syslog Server**.
21. Toggle **Syslog Server** to **ON**.

Note
When enabled, Extreme Networks devices save the event log entries to the Syslog servers specified.

22. Select a **Syslog Facility**.

23. To add a new Syslog server, select , and then:
    a. Enter a **Syslog IP Address** for the Syslog server.
    b. Select a **Severity** level.
    c. Type the **Port** number.
    d. Select a **Virtual Routing** instance.
    e. Select **ADD**.

    Note
    Use the arrows in the **Order** column to change the order.

24. To delete a Syslog server from the list, select the Syslog servers, and then select (delete).

RADIUS Server Settings

25. Select **RADIUS Server**.
26. Toggle **RADIUS Server** to **ON**.
27. Select one of the following options:

- **Use Extreme Platform ONE RADIUS Cloud Configuration**: Enables the device to use the cloud-based RADIUS configuration provided by UZTNA for authentication.

  Note
  UZTNA is provisioned through the UZTNA application. If UZTNA settings or license is not properly configured, then device authorization may fail.

- **Use Extreme Platform ONE Security RADIUS Proxy Servers**: Enables the device to route RADIUS authentication requests through Extreme Platform ONE Security proxy servers for secure handling and centralized control. Select the **Primary RADSEC Proxy Server** and the **Secondary RADSEC Proxy Server**.

Configure Switch Ports and VLAN

You can configure switch port configuration details and settings at the device level. Switch-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 to change

the switch-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 5520/5720 Universal Switches, VIM and partition mode are configurable at the device level.
- LLDP/CDP, MAC locking, STP Priority, BPDU Restrict, BPDU Restrict Recovery, Forwarding Delay, VLAN Attributes, and Max Age are configurable at the device level.
- BPDU Restrict and BPDU Recovery settings are found within the STP tab.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. From the 3-dot menu, **Configure** > **Device**.
3. Under the **Configuration** menu, select **Port/VLAN Configuration**.
4. Select **Unlock** to enable switch-level configuration changes.

   Note
   Changes made after unlocking the device will override network policy and switch template configuration.

5. Select each tab, and edit any accessible field.
6. Select **Save Port Configuration**.

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

7. To revert back to the network policy switch template, select **Revert to Network Policy**.

Port/VLAN Configuration Settings

Table 20: Port Details

Field	Description
EDIT	Edit multiple ports at once. Select the ports, then select **EDIT** to apply bulk changes.
Instant Profile	1. Select to choose an existing instant profile. 2. To create a new instant profile, select , and then select **Instant Port Profile** or **Instant Secure Port Profile**. 3. Select **SAVE**. **Note:** Not supported on Fabric Engine devices.

Table 20: Port Details (continued)

Field	Description
IGMP Settings	Toggle to **ON** to enable the switch to identify ports to which multicast group member hosts are attached to optimize the distribution of multicast traffic. When enabled, the following options are available (not supported on Fabric Engine devices): • **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.
DHCP Snooping (non-Fabric Devices)	Toggle **DHCP Snooping** to **ON**, to enable snooping of DHCP packets and create a DHCP bindings database of IP to MAC addresses for static and dynamic VLANs. Optionally, select **Enable drop rogue DHCP Packets action for static and dynamic VLANs**. Ports configured as trusted will not apply drop action. By default, port types configured as Trunk Port will be trusted. **Note:** If VLAN attributes has enabled DHCP Snooping settings, then the VLAN attributes will override the switch template.
DHCP Snooping Global Enable (Fabric Device Only)	Toggle to **ON** to enable DHCP Snooping. **Important:** When DHCP Snooping is enabled, it may disrupt connectivity for authorized DHCP servers connected to a switch port or an uplink port currently in use. Select **YES** to confirm.
Interface	The port or interface identifier on the switch.
Instant Profile Status	Indicates if an instant profile is applied to the port.
Port State	Indicates the current operational state of the port (ON or OFF).

Table 20: Port Details (continued)

Field	Description
LACP	Indicates if Link Aggregation Control Protocol (LACP) is enabled for the port.
Auto-Sense (Fabric Engine only)	Indicates whether Auto-Sense is enabled, allowing the port to automatically detect and configure its role based on the connected device type.
Port Type & VLAN	Specifies the port type (access or trunk) and associated VLAN configuration. To create a new port type, select  .
VLAN	Lists the VLAN assigned to the port.
DHCP Snooping Trusted Port	Indicates if the port is trusted for DHCP snooping to allow DHCP server responses.
Description	A description or label for the port.

Table 21: Port Settings & Aggregation

Field	Description
EDIT	Edit multiple ports at once. Select the ports, then select **EDIT** to apply bulk changes.
MTU Settings	Set the maximum transmission unit value for Ethernet interfaces. The MTU value determines the largest packet size that can be transmitted through your system.
LLDP Settings	Set the following LLDP settings: • **Advertisements Interval**: Type the number of seconds between LLDP advertisements sent to neighboring network devices. • **Timer Hold**: Type a multiple of the advertisements interval. (EXOS/ Switch Engine, VOSS/Fabric Engine, SR22XX/ 23XX, Dell) • **LLDP Initialization Delay Time**: Type the length of time that you want the interface to wait before initializing LLDP. • **Fast start repeat count**: Type the number of advertisement LLDP frames to send when the connected device (such as an IP phone) starts up or is discovered.

Table 21: Port Settings & Aggregation (continued)

Field	Description
Aggregate Selected Ports	Select two or more ports of the same type that you want to aggregate, and then select **Aggregate Selected Ports**. For more information, see Aggregate LAG and LACP Ports on page 52. **Note:** You can only aggregate ports when you configure in bulk.
Interface	The port or interface identifier on the switch.
Transmission Type	Set the **Transmission Type**: • **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.
Speed	Select the speed the port uses to communicate with the connected device.
Flow Control	Select how to manage the receive transmission speed, which enables a feedback mechanism between a transmitting port and the receiving port on the switch.
LLDP—Transmit	Enables the switch to transmit LLDPDU frames.
LLDP—Receive	Enables the switch to receive LLDPDU frames.
LLDP MED Capabilities	Enables LLDP-Media Endpoint Discovery.

Table 21: Port Settings & Aggregation (continued)

Field	Description
CDP	Enables the switch to receive and parse the information within Cisco CDP frames.
Client Reporting	Enables collection and reporting of learned MAC addresses for the port.

Table 22: Instant Secure Port Settings

Field	Description
EDIT	Edit multiple ports at once. Select the ports, then select **EDIT** to apply bulk changes.
Interface	The port or interface identifier on the switch.
User Auth	Toggle to **ON** to enable user authentication.
MAC Auth	Toggle to **ON** to enable MAC authentication.

Table 23: STP

Field	Description
Enable STP	Toggle to **ON** to enable STP and configure the settings for the device. **Note:** Not applicable to Auto-Sense ports on Fabric Engine devices.
EDIT	Edit multiple ports at once. Select the ports, then select **EDIT** to apply bulk changes.
STP for Device	Configure STP settings for the device. For more information, see Configure STP Settings on page 55. **Note:** If Spanning Tree Mode is set to STP, then port priority should be set to either 0 or 16. Any greater value will be ignored and the default STP (802.1D) port priority of 16 will be used.
Interface	The port or interface identifier on the switch.
STP Status	Toggle **ON** to enable STP for the port.

Table 23: STP (continued)

Field	Description
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	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.
BPDU Restrict	Toggle the switch to **ON** to enable BPDU Restrict. **Note:** Not supported on Fabric Engine devices.
BPDU Recovery Timeout	Input a BPDU recovery timeout time between 60-600 seconds.
Priority	When this port is an STP edge port, select a port priority for STP from the drop-down list.
Path Cost	Enter the Path Cost (bandwidth) for this port.

Table 24: Storm Control

Field	Description
EDIT	Edit multiple ports at once. Select the ports, then select **EDIT** to apply bulk changes.
Interface	The port or interface identifier on the switch.
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.

Table 24: Storm Control (continued)

Field	Description
Rate Limit Type	PPS (packets per second) is the default rate limit type.
Value	Enter when the switch should discard traffic of the selected types.

Table 25: MAC Locking

Field	Description
Enable MAC Locking	Toggle to **ON** to enable MAC locking.
EDIT	Edit multiple ports at once. Select the ports, then select **EDIT** to apply bulk changes.
Interface	The port or interface identifier on the switch.
MAC Locking	Toggle **ON** to enable MAC locking for the port.
Max First Arrival Limit	Set the Maximum First Arrival Limit for the port. Select  to revert to the original network policy settings.
Disable Port	Toggle **ON** to disable the port.
Link Down Action	Specify the Link Down Action for the port. By default, Link Down Action is set to clear first arrival MACs, with the option to retain MACs.
Remove Aged MACs	Toggle **ON** to remove MACs when they are aged out for the port.

Table 26: Voice

Field	Description
EDIT	Edit multiple ports at once. Select the ports, then select **EDIT** to apply bulk changes.
Interface	The port or interface identifier on the switch.
LLDP Voice Advertisements	Toggle to **ON** to enable LLDP to advertise voice VLAN information to connected devices for VoIP configuration.
802.1 VLAN and Port Protocol	Select to configure IEEE 802.1 standards for VLAN tagging and port protocol identification for voice traffic.

Table 26: Voice (continued)

Field	Description
Med Voice VLAN DSCP Value	Type the DSCP (Differentiated Services Code Point) value for voice media traffic to prioritize audio streams.
Med Voice Signaling DSCP Value	Type the DSCP value for voice signaling traffic to ensure call setup and control messages are prioritized.
CDP Advertisements	Toggle to **ON** to enable Cisco Discovery Protocol advertisements to share voice VLAN and device information with connected endpoints.
CDP Voice VLAN	Specifies the voice VLAN ID communicated through CDP for VoIP devices.
CDP Power Available	Indicates the amount of PoE (Power over Ethernet) available on the port, advertised via CDP for powered devices.

Table 27: PSE

Field	Description
EDIT	Edit multiple ports at once. Select the ports, then select **EDIT** to apply bulk changes.
PSE Settings for Device	Select to set maximum power thresholds to send alerts to Extreme Platform ONE Networking when exceeding maximum power levels.
Interface	The port or interface identifier on the switch.
POE	Toggle to **ON** to enable POE on the port.
PSE Profile	Select  to choose an existing PSE profile. To create a new PSE profile, select  . For more information, see Configure PSE on page 58.
Power Mode	The POE power mode. 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.

Table 27: PSE (continued)

Field	Description
Power Limit (mW)	The available PoE power limit.
Priority	The power output priority: • **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.

Table 28: ELRP

Field	Description
EDIT	Edit multiple ports at once. Select the ports, then select **EDIT** to apply bulk changes.
ELRP Settings	Configure ELRP settings for the device: • Toggle **Enable ELRP**. • Select the **Enable ELRP for dynamically created VLAN(s)** check box. • Toggle **Configure ELRP Port Duration** and enter the duration in seconds.
Interface	The port or interface identifier on the switch.
ELRP	Toggle to **ON** to enable ELRP on the port.
ELRP Exclude	Toggle to **ON** to exclude ELRP on the port.

Table 29: VLAN Attributes

Field	Description
Create a new, edit, clone, or delete VLAN attributes.	
VLAN ID	The VLAN ID for the VLAN attribute.
VLAN Name	The name of the VLAN.
ISID	The unique service identifier for the VLAN attribute.

Table 29: VLAN Attributes (continued)

Field	Description
IGMP Snooping VLAN Settings	Specifies if IGMP Snooping is enabled for the VLAN attribute.
DHCP Snooping VLAN Settings	Specifies if DHCP Snooping is enabled for the VLAN attribute.
VLAN Deployment	Specifies if VLAN Deployment is enabled for the VLAN attribute.

Table 30: SLPP

Field	Description
EDIT	Edit multiple ports at once. Select the ports, then select **EDIT** to apply bulk changes.
Interface	The port or interface identifier on the switch.
SLPP	Toggle to **ON** to enable Simple Loop Prevention Protocol (SLPP) to detect and prevent Layer 2 loops within the fabric by monitoring packets on VLANs.
Guard Timeout	Specify the time interval (in seconds) before the system re-enables a port after a loop protection event, helping maintain network stability.

Table 31: EAPoL

Field	Description
Enable EAPoL	Toggle to **ON** to enable EAPoL on the device. **Note:** Modifying user authentication port settings will disconnect authenticated clients when a configuration update is performed.
EDIT	Edit multiple ports at once. Select the ports, then select **EDIT** to apply bulk changes.
Interface	The port or interface identifier on the switch.
User Auth	Toggle to **ON** to enable user authentication.
MAC Auth	Toggle to **ON** to enable MAC authentication.

Table 31: EAPoL (continued)

Field	Description
Any Auth MAC MAX	Set the maximum number of authenticated MAC addresses allowed on the port for any authentication method.
802.1X Auth MAC MAX	Set the maximum number of MAC addresses that can be authenticated using 802.1x on the port.
MAC Auth MAC MAX	Set the maximum number of MAC addresses permitted for MAC-based authentication on the port.
EAPoL Re-Authentication—Status	Toggle to **ON** to enable periodic EAPoL re-authentication on the port.
EAPoL Re-Authentication—Period	Set the time interval (in seconds) for performing EAPoL re-authentication when enabled.

Configure Instant Port Profiles

Use this task to configure Instant Port Profiles (IPP) from Network Devices or Network Policies:

Network Devices

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select at the end of a device row, and then select **Configure** > **Device**.
3. Under the **Configuration** menu, select **Port / VLAN Configuration**.
4. From **Port Details**, select **INSTANT PROFILE**.
5. To add a new IPP, select , and then select **Instant Port Profile**.
6. Configure the IPP settings in Table 32 on page 98.
7. Select **Save** to apply the IPP to the device.

Network Policies

8. Go to **Configuration** > **Network**.
9. Select an existing switching/routing network policy.
10. On the **3 Switching/Routing** page, select **Configuration Settings** > **Switch Templates**.
11. In the switch template, select **Configuration** > **Port/VLAN Configuration**.
12. Choose one of the following actions:
    - To add a new IPP, select .
    - To edit an existing IPP, select , choose the IPP object, and then select .
13. Configure the IPP settings in Table 32 on page 98.
14. Select **Save** to apply the IPP to the device template.

IPP Settings

15. Configure IPP settings.

Table 32: Instant Port Profile Settings

Field	Description
Name	Type a **Name** for the IPP.
Description	Type a **Description** for the IPP.
Non-Forwarding VLAN	Select to choose a VLAN to detect attached devices; this VLAN does not forward traffic. To add a new non-forwarding VLAN, select , to edit an existing choose a VLAN and then select , enter a **Name** and **VLAN ID**, and then select **SAVE VLAN**. The non-forwarding VLAN cannot be utilized within a port type assigned to the switch.
Default Port Type	From the menu, select the default port type: • **Access Port** - Use for a port connected to an individual host. • **Trunk Port** - Use for a port connected to a forwarding device such as an AP and switch that supports multiple VLANs. Ports assigned to an IPP inherit the selected port type settings, such as type, speed, STP, MAC locking, ELRP, and PSE port settings. To add a new port type, select .
Non-Match Action	Select one of the options: • **Non-Forwarding VLAN**: Does not forward traffic for devices that do not match an assignment rule. • **Use Default Port Type VLAN**: Assigns the VLANs associated with the port type. Storm control settings are inherited when the non-match action is set to use the default port type and the device does not match a defined device type.
Device Types	Add a new **Device Type**, edit or delete an existing **Device Type**. Configure the IPP Device Type Settings on page 33. **Note:** For a device type to match based on MAC learning, the rule must be ordered above any LLDP-based assignment rules. This ensures that MAC learning takes precedence, irrespective of LLDP information.

Configure Instant Secure Port Profiles

Use this task to configure Instant Secure Port Profiles (ISPP) from Network Devices or Network Policies:

Network Devices

1. Go to **Monitoring** > **Network Devices** > **Device Status**.

2. Select at the end of a device row, and then select **Configure** > **Device**.
3. Under the **Configuration** menu, select **Port / VLAN Configuration**.
4. From **Port Details**, select **INSTANT PROFILE**.
5. Select , and then select **Instant Secure Port Profile**.
6. Configure the Instant Secure Port Profile settings in Table 33 on page 99.
7. Select **Save** to apply the ISPP to the device.
8. Choose whether to use Unauthenticated VLAN. Unauthenticated VLAN is either a common object or can be created when the profile is created. If the Enable Unauthenticated VLAN is selected, then this VLAN will override the untagged VLAN in the port type and will be used as the Unauthenticated VLAN on the Switch Engine device when the configuration is pushed.
9. Specify the order in which to execute authentication. The order is per profile; therefore the same order is used for the entire Switch Engine device once the configuration is pushed. Use the arrows to change the default order.
10. Pick the RADIUS server for the Instant Secure Profile. Selecting **Use Extreme Platform ONE Security RADIUS Cloud configuration** uses either the free cloud RADIUS server set up per RDC, or configured proxy RADIUS servers in the Extreme Platform ONE Security application. Select one of the radio buttons to decide which type to use. Further, in the case of proxy RADIUS, you can select up to two proxy RADIUS servers; it is assumed that the ones selected have reached a deployed state after being configured in Extreme Platform ONE Security.
11. Select **Save**.

Network Policies

12. Go to **Configuration** > **Network**.
13. Select an existing switching/routing network policy.
14. On the **3 Switching/Routing** page, select **Configuration Settings** > **Switch Templates**.
15. In the switch template, select **Configuration** > **Port/VLAN Configuration**.
16. Choose one of the following actions:
    - To add a new ISPP, select .
    - To edit an existing ISPP, select , choose the ISPP object, and then select .
17. Configure the Instant Secure Port Profile settings in Table 33 on page 99.
18. Select **Save** to apply the IPP to the device template.

ISPP Settings

19. Configure ISPP settings.

Table 33: Instant Secure Port Profile Settings

Field	Description
Name	Enter a profile name.
Description	Enter a profile description.

Table 33: Instant Secure Port Profile Settings (continued)

Field	Description
Enable Unauthenticated VLAN	Enable and define an untagged VLAN when the device is unauthenticated. Authentication mode is optional when the Unauthenticated VLAN is enabled.
Authentication	Set authentication options for switches that will have Instant Secure Port enabled within the switch template. The port type also requires User or MAC auth to be enabled. Enabling Instant Secure Port will also enable node alias. Node alias will provide additional data for wired client information such as IP address of the wired client device.
Use Extreme Platform ONE Security RADIUS Cloud Configuration	Define the RADIUS server configuration. If a DHCP assigned IP address is utilized, the DHCP IP address will be used for the RADIUS client IP configuration. If the DHCP assigned IP address changes, then a device update will be required to update the RADIUS client IP configuration. **Note:** If Extreme Platform ONE Security settings or license is not properly configured, then device authorization may fail.
Use Extreme Platform ONE Security RADIUS Proxy Servers	

20.Select **SAVE**.

Configure Wired Device Credentials

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

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

Note
At this level, you are making changes to the selected device only. These changes always override the network policy configurations. To revert to the settings in the network policy, from the **Device List**, select the device host name, and use the **Actions** button.

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. To configure a root admin with full capability, follow these steps:

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select ⋮ at the end of a device row, and then select **Configure** > **Device**.
3. Under the **Configuration** menu, select **Device Credentials**.
4. For an **Administrator Account**, enter the **Admin Name** and **Password**.

   Passwords should contain at least 8 characters, including at least one number, one special character, and one uppercase character.
5. For a **Read Only Administrator**, enter the **Admin Name** and **Password**.

   Passwords should contain at least 8 characters, including at least one number, one special character, and one uppercase character.
6. Select **Save Configuration**.

   For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 107.

Configure SSH

Before you can configure SSH access on a device, you must first enable **SSH Availability**. To do this, select **Administration & Settings** > **Backup & Restore** > **VIQ Management** , and then enable **SSH Availability**.

Extreme Platform ONE Networking provides a way to access devices remotely using the SSH protocol by using an SSH proxy server.

Note
It is important to remember that while SSH access is available, your device is exposed to public access through an SSH proxy. The device is protected only by the device administrator credentials, because SSH FTP assumes that it is run over a secure channel.

Use this task to configure SSH on a device.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select ⋮ at the end of a device row, and then select **Configure** > **Device**.
3. Under **Additional Settings**, select **SSH**.
4. Under **Run Time**, select the length of time that you want SSH to be available for the device.

   Extreme Platform ONE Networking creates an SSH session for the specified length of time between the SSH proxy server and the 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.

Interface Configuration

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

- IP Address
- IPv4 Subnetwork Allocation Name
- VLAN Name
- VLAN ID
- DHCP Relay
- IPv4 Forwarding
- Routing Instance

Use this task to configure the device interface.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select at the end of a device row, and then select **Configure** > **Device**.
3. Under **Network Allocation**, select **Interface Configuration**.
4. Select a port icon on the template graphic to view port details, if available.
5. Select to add, or to edit an Interface.
6. Enter the interface attributes according to the table below:

Table 34: Interface Configuration Attributes

Field	Description
Network Allocation	An IP subnetwork configuration.
VLAN Attribute	A VLAN attribute, which can be created from within the **Network Policy Switching** > **VLAN Attribute** Section.
IPv4 Address / Subnet Mask	The assigned device IP Address.
Routing Instance	The device routing instance.
IPv4 Forwarding	Toggle **ON** to enable IPv4 forwarding.
VLAN Loopback Enable	Select the check box to enable VLAN loopback.
DHCP Relay	To override DHCP Relay, toggle **ON Enable DHCP Relay**. If enabled, enter a **Primary DHCP Server** and an optional **Secondary DHCP Server**.

7. Select **Next**.
8. Confirm **Summary** details, and then select **Save**.

   To go back and make changes, select **Previous**.

9. To delete Interfaces, select the Interface(s) and then select .
10. For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 107.

Routing Configuration

The device must have an IPv4 interface configured. For more information, see Interface Configuration on page 102.

Use this task to configure IP4 Static Routes for the selected device.

1. Go to **Monitoring** > **Network Devices** > **Device Status**..
2. Select at the end of a device row, and then select **Configure** > **Device**.
3. Under the **Network Allocation** menu, select **Routing Configuration**.
4. Select to add or to edit, and then configure the static route settings in Table 35.

Table 35: Static Route Settings

Field	Description
Static Route Name	The name of the Static Route.
Destination Subnet	The desired subnet, such as `10.1.0.0/16`.
Next Hop IP	The desired IP Address for the next Hop, such as `123.321.132.312`.
Next Hop IP Ping Protection	**Enable** or **Disable** Next Hop IP Ping Protection. **Note:** Enabling Ping Protection will generate a Ping Protection Status tool tip when viewing your device within **Monitoring** > **Visualize** > **Wired** > **Routing** **Note:** Not supported for Fabric Engine/ VOSS.
Metric	The desired metric value.
Routing Instance	Shows the Routing Instance.

5. Select **Save**.
6. To delete a static route, select the check box next to the Static Route Name and then select .
7. For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 107.

Push Device-Level Configuration

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

Use this task to push any configuration changes made at the device level to the specific device.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select at the end of a device row, and then select **Configure** > **Device**.

3. Select **Update** and configure the **Device Update** settings for the selected device.

Table 36: Update Wired Device Settings

Field
Update Network Policy and Configuration
Reboot and revert Extreme Networks switch configuration if IQAgent is unresponsive after configuration update.
Perform delta configuration update and resolve local device configuration which is out of sync with Extreme Platform ONE Networking.

Table 37: Update Wireless Device Settings

Field	
Update Network Policy and Configuration	
Delta Configuration Update	Updates only the device delta configuration changes for the selected device. This action avoids a device reboot.
Complete Configuration Update	A full update for the selected device. This resets the selected device to Extreme Platform ONE Networking configuration settings. **Note:** Only supported on devices running HOS or IQE Firmware.
Activation Time for Extreme Networks Devices Running Images:	
Activate at next reboot (requires rebooting manually)	Activation takes affect the next time the AP is rebooted.
Activate after xx seconds	The delay before activation, in seconds.
Activate/reboot on this schedule based on your local system time	Schedule a **Date** and **Time** to activate.

4. To update the selected device immediately, select **Perform Update**, or select **Save as Defaults** to keep these settings for future use.

Configure Fabric Settings

Shortest Path Bridging MAC (SPBM) is a next generation virtualization technology that revolutionizes the design, deployment, and operations of carriers and service providers, along with enterprise campus core networks and the enterprise data center. SPBM provides massive scalability while at the same time reducing the complexity of the network.

Auto-sense is a port-based functionality that supports zero touch capabilities on the switch. Auto-sense dynamically configures the port to act as an IS-IS network-to-network interface (NNI), Fabric UNI (Flex-UNI), Fabric Attach (FA), Fabric Extend, or voice (IP phone) interface, based on the Link Layer Discovery Protocol (LLDP) events. Auto-

sense provides global configuration options for IS-IS authentication, FA authentication, Fabric Extend tunnel creation, and voice configuration for IP phones on the switch.

Note
This feature is available only if the device is in an Extreme Platform ONE Networking-compatible building or outdoor site with full features unlocked. For more information, see *Extreme Platform ONE Networking and ExtremeCloud IQ Licensing Entitlement Guide*.

Use this task to configure fabric settings for devices running Fabric Engine.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select ⋮ at the end of a device row, and then select **Configure** > **Fabric**.
3. Configure the following fabric settings:
   - Global SPBM Settings
   - Auto Sense Settings

   Note
   Toggle **Advanced** to **ON** to view advanced options.
4. To save device fabric settings, see Push Device-Level Configuration on page 107.

Global SPBM Settings

Table 38: Global SPBM Settings

Field	Description
SPBM	
Hostname	Specifies the SPBM system name. Enter a string length from 1 to 255.
System ID	Specifies the SPBM instance ID. **Note:** System ID and Nickname can only be changed together.
Nickname	Specifies a nickname for the SPBM instance globally. Valid value is 2.5 bytes in the format <x.xx.xx>. **Note:** System ID and Nickname can only be changed together.
ISIS Manual Area ID	Specifies the IS-IS manual area. Valid value is 1-26 bytes in the format <xx.xxxx.xxxx...xxxx>. Only one manual area is supported. Use the same manual area across the entire SPBM cloud. For IS-IS to operate, you must configure at least one manual area.
Primary BVLAN	Specifies the primary SPBM B-VLAN to add to the SPBM instance.

Table 38: Global SPBM Settings (continued)

Field	Description
Secondary BVLAN	Specifies the secondary SPBM B-VLAN to add to the SPBM instance.
IP Shortcuts	Toggle **IP Shortcuts** to **ON** to enable the SPBM IP shortcut state. The default is disable. In **IP Source Address**, specify the CLIP interface to use as the source address for SBPM IP shortcuts.
Multicast	Toggle **Multicast** to **ON** to enable IP multicast over SPBM. The default is disabled.
Auto ISID Assignment	Toggle **Auto ISID Assignment** to **ON** to enable automatic allocation to assign and manage ISIDs. In **L2 ISID Offset**, specify the starting index for SID allocation for Level 2 IS-IS routers.
Nickname Server (Advanced Option)	
Nickname Prefix	Specifies the nickname server allocation prefix. x.xx.xx uses the form X.X0.00 from 0.00.00 to F.F0.00. A group, X.X0.00 to X.XF.FF, can provide up to 4,096 nicknames. The default is A.00.00.

Auto Sense Settings

Table 39: Auto Sense Settings

Field	Description
General Assignments	
Onboarding ISID	Specifies the onboarding I-SID used by the auto-sense ports. **Note:** This is an **Advanced** option.
Data ISID	Specifies the data I-SID used by the auto-sense ports.
Wait Interval	Specifies the wait interval, in seconds, for Auto sense to wait for a Link Layer Discovery Protocol (LLDP) neighbor to be detected in the auto-sense wait state before transitioning to the auto sense onboarding state. This configuration is a global configuration that applies to all auto-sense ports. The default value is 35. **Note:** This is an **Advanced** option.
Voice ISID	Specifies the voice I-SID used by auto sense ports.
Voice CVID	Specifies the customer VLAN ID associated with the voice I-SID used by auto-sense ports. Voice C-Vid is configured for tagged voice traffic only. **Important:** You must configure the Auto-sense voice customer VLAN ID along with the auto sense voice I-SID.

Table 39: Auto Sense Settings (continued)

Field	Description
EAPoL Voice LLDP Authentication Bypass	Select to enable the EAPoL LLDP authentication bypass for voice auto sense ports. **Note:** This is an **Advanced** option.
Fabric Attach Assignments	
FA Proxy Management ISID	Specifies the FA proxy management I-SID used by auto sense ports.
FA Proxy Management CVID	Specifies the proxy management client-VLAN ID (C-VID) used by auto sense ports.
FA Proxy No Auth Management ISID	Specifies the proxy no-auth I-SID used by auto sense ports. **Note:** This is an **Advanced** option.
FA WAP Type1 ISID	Specifies the FA WAP type-1 I-SID used by auto sense ports.
FA Camera ISID	Specifies the FA camera I-SID used by auto sense ports.
EAPoL FA WAP Type1 Authentication Bypass	Select to enable the FA EAPoL authentication bypass for Wap-type-1 I-SID used by auto sense ports.
EAPoL FA Camera Authentication Bypass	Select to enable the FA EAPoL authentication bypass for camera I-SID used by auto sense ports.
FA Message Authentication	
FA Message Authentication	Select to enable FA message authentication.
FA Auth Key	Specifies the FA authentication key for the auto sense ports.
Message Authentication IS-IS (Advanced Options)	
ISIS Hello Auth Type	Select an IS-IS hello authentication type.
ISIS Hello Auth Key ID	Specifies the IS-IS authentication key ID for auto sense ports.
ISIS Hello Auth Key	Specifies the IS-IS authentication key for auto sense ports.

Push Device-Level Configuration

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select ⋮ at the end of a device row, and then select **Configure** > **Device**.

3. Select **Update** and configure the **Device Update** settings for the selected device.

Table 40: Update Wired Device Settings

Field
Update Network Policy and Configuration
Reboot and revert Extreme Networks switch configuration if IQAgent is unresponsive after configuration update.
Perform delta configuration update and resolve local device configuration which is out of sync with Extreme Platform ONE Networking.

Table 41: Update Wireless Device Settings

Field	
Update Network Policy and Configuration	
Delta Configuration Update	Updates only the device delta configuration changes for the selected device. This action avoids a device reboot.
Complete Configuration Update	A full update for the selected device. This resets the selected device to Extreme Platform ONE Networking configuration settings. **Note:** Only supported on devices running HOS or IQE Firmware.
Activation Time for Extreme Networks Devices Running Images:	
Activate at next reboot (requires rebooting manually)	Activation takes affect the next time the AP is rebooted.
Activate after xx seconds	The delay before activation, in seconds.
Activate/reboot on this schedule based on your local system time	Schedule a **Date** and **Time** to activate.

4. To update the selected device immediately, select **Perform Update**, or select **Save as Defaults** to keep these settings for future use.

Wired Device View

The **Wired** device view provides a streamlined interface for reviewing device details. Allowing quick access to essential device-specific information.

Select a **Device** name from the table. The **Device Details** window displays the following detailed information for the wired device:

- Connection Status: The current network connectivity status of the device.
- Device Image: A visual representation or model image of the device.
- Device Location: The physical or configured location of the device.
- From the **Actions** menu you can perform actions for the selected device. For more information, see Device View Actions Menu on page 118.

  Note
  Not all actions are available for all devices.

- Installation Media Gallery: Select to upload an image (.png or .jpg less than 500KB) or video (.mp4 or .mov less than 5MB) file.
- Device Details: Key device information.
- Tags: Assigned tags for device categorization. Select **Add Tag** to manually add tags. Tags act as labels and help in easy filtering of the devices.
- Overview: Displays general device information.
- Clients: Lists device client details.
- Port Stats: Displays statistics for all device ports.
- Services/VLANs: Displays configured services and VLAN assignments.
- Routing: Provides routing configuration and status.
- Events: Lists system and device events.
- Alerts: Displays alerts and notifications triggered on the device.

To narrow the time frame, select the **Date & Time Range**, select a **Start Date** and **End Date**, select a **Start Time** and **End Time**, and then select **Done**. Select **Reset to Default** to reset back to the default time frame.

To refine the device list:

- Select and drag the left or right border of the column header to adjust the column width.
- Select and drag the column headers to change the order of the columns.
- Select a column header to sort column data in ascending or descending order.
- Select **Columns** to add, remove, and reorder the columns.
- To refine the list, select **Filter**. The filter sidebar lets you customize what information is displayed in the device list. Available filters vary depending on the window you are in. To see all available options, in the filter area, select a section heading to see more or less items. Select **Reset** to restore the default view.

Select **Actions** to perform specific tasks on the selected device.

Overview

Overview displays the following information about the selected device:

- **Device Health** widgets display:
  - CPU Usage
  - Memory Usage
  - Resource Utilization
  - PoE Usage
  - Temperature
  - Fan Status
  - Power Status

  Note
  To view more information, select a widget.

- From the Port Configuration diagram, select individual ports or enable **Select All Ports** to reveal the following options:
  - Port Bounce
  - PoE Bounce
  - Cable Test
- From the interactive timeline graph:
  - View and filter:
    - Total CPU Utilized
    - Total Memory Utilized
    - Total MAC Table Utilized
    - Temperature
    - Poe Usage Consumed %

        - Fan Status
        - Power Supply Status
    - Select any point along the timeline in the graphic to display details only for that precise time. To customize the time period for graphs, drag inside the timeline. The chart lines are interactive—hover over a line to see more data.
    - Select ☰ to:
        - View in full screen
        - Print chart
        - Download PNG image
        - Download JPEG image
        - Download PDF document
        - Download SVG vector image
- Device widgets display **Usage Utilization**, **Client Health**, and **Wired Throughput**.

Clients

Clients displays the following information about the selected device:

- From the Port Configuration diagram, select individual ports or enable **Select All Ports** to reveal the following options:
    - Port Bounce
    - PoE Bounce
    - Cable Test
- From the interactive timeline graph:
    - View and filter:
        - Clients with Issues
        - Port Congestion
        - Unicast TX/RX
        - Broadcast TX/RX
        - Multicast TX/RX
        - Port Errors TX/RX
    - To narrow the time frame, select the **Date & Time Range**, select a **Start Date** and **End Date**, select a **Start Time** and **End Time**, and then select **Done**. Select **Reset to Default** to reset back to the default time frame.
    - Select any point along the timeline in the graphic to display details only for that precise time. To customize the time period for graphs, drag inside the timeline. The chart lines are interactive—hover over a line to see more data.
- Device widgets display **IP Connectivity Issues**, **Port Congestion**, **Traffic Anomalies**, and **Port Errors**.
- Select **Client Details** to display the following information:
    - Port Number
    - Client
    - MAC

    - Operating System
    - Connection Status
    - IPv4
    - IPv6
    - VLAN
- Select **Client Traffic** to display the following information:
    - Connection Status
    - Client
    - VLAN
    - Port Number
    - Total Congestion (# of Packets)
    - Total Unicast (Packets%)
    - Total Multicast Packets
    - Total Broadcast (Packets%)
    - Total Port Errors

Services/VLANs

Services/VLANs displays the following information about the selected device:

- From the Port Configuration diagram, select individual ports or enable **Select All Ports** to reveal the following options:
    - Port Bounce
    - PoE Bounce
    - Cable Test
- A table lists the following details about the clients that are connected during the specified time range:
    - VLAN Id
    - VLAN Name
    - Total Active Ports
    - Total Tagged Ports
    - STP Instance

Note
You can use the **Search** field to filter the table view.

Port Stats

Port Stats displays the following information about the selected device:

- From the Port Configuration diagram, select individual ports or enable **Select All Ports** to reveal the following options:
    - Port Bounce
    - PoE Bounce

- Cable Test

- From the interactive timeline graph:
  - View and filter:
    - Total TX/RX Bytes
    - Total TX/RX Unicast Pkts
    - Total TX/RX Broadcast Pkts
    - Total TX/RX Multicast Pkts
    - Total Errors
    - Total Queue Congestion
  - Narrow the time frame. Select the **Date & Time Range**, select a **Start Date** and **End Date**, select a **Start Time** and **End Time**, and then select **Done**. Select **Reset to Default** to reset back to the default time frame.
  - Select any point along the timeline in the graphic to display details only for that precise time. To customize the time period for graphs, drag inside the timeline. The chart lines are interactive—hover over a line to see more data.
- Device widgets display **Usage Utilization**, **Wired Throughput**, and **Wired Congestion**.
- The description table lists the following details:

Note
You can use the **Search** field to filter the table view.

Ports Description:

- Port Number
- LLDP Neighbor
- MAC Locking
- Media Type
- Operational Status
- STP Port State
- Transmission Mode
- Link Speed

Port Stats Summary:

- **% Utilization**
  - Port Number
  - % Utilization Rx
  - % Utilization Tx
  - % Utilization MaxRx
  - % Utlization MaxTx
- **In/Out Statistics**:
  - Port Number
  - InOctets
  - OutOctets
  - InUcastPkts
  - OutUcastPkts
  - InBroadcastPkts
  - OutBroadcastPkts
  - InMulticastPkts
  - OutMulticastPkts
  - Port Queue Congestion Count
- **Error**:
  - Port Number

        - Total Aggregated Port Errors Counter
    - **Queue**:

        - Port Number
        - QP0 Pkt Cong | Xmts
        - QP1 Pkt Cong | Xmts
        - QP2 Pkt Cong | Xmts
        - QP3 Pkt Cong | Xmts
        - QP4 Pkt Cong | Xmts
        - QP5 Pkt Cong | Xmts
        - QP6 Pkt Cong | Xmts
        - QP7 Pkt Cong | Xmts
        - QP8 Pkt Cong | Xmts

    Link PoE:
    - Port Number
    - Power Consumed per port, mW

Routing

Routing displays the following information about the selected device:

- From the Port Configuration diagram, select individual ports or enable **Select All Ports** to reveal the following options:
    - Port Bounce
    - PoE Bounce
    - Cable Test
- From the interactive timeline graph:
    - View and filter:
        - Total Routes
        - Direct Routes
        - Static Routes
        - OSPF Routes
        - IS-IS Routes
        - BGP Routes
    - Narrow the time frame. Select the **Date & Time Range**, select a **Start Date** and **End Date**, select a **Start Time** and **End Time**, and then select **Done**. Select **Reset to Default** to reset back to the default time frame.
    - Select any point along the timeline in the graphic to display details only for that precise time. To customize the time period for graphs, drag inside the timeline. The chart lines are interactive—hover over a line to see more data.
- The **IPv4/IPv6 Routing Table** lists the following details:

    - Destination
    - Next Hop
    - VLAN Name
    - VLAN Id
    - Route Origin
    - Status
    - Metric
    - Route Type Priority
    - Routing Instance

- Service Name
- Service ID

Note

- Select **Refresh Routing Table** to update the table with the most current data.
- Use the **Search** field to filter the table view.

Events

Events displays the following information about the selected device:

- From the **Events** interactive timeline graph:
  - View and filter by **Critical**, **Major**, **Minor**, **info**, and **Clear** events.
  - Select any point along the timeline in the graphic to display details only for that precise time. To customize the time period for graphs, drag inside the timeline. The chart lines are interactive—hover over a line to see more data.
  - Select ☰ to:
    - View in full screen
    - Print chart
    - Download PNG image
    - Download JPEG image
    - Download PDF document
    - Download SVG vector image
- The **Events** table lists the following details:
  - Timestamp
  - Severity
  - Component
  - Description

Note
You can use the **Search** field to filter the table view.

Alerts

Alerts provides the following information about the selected wireless device:

- An interactive graph shows the number of alerts raised on the current device, for the specified time frame. By default, the data capture time frame is 24 hours.
  - To customize the graph, select any **Filter by** option from the list (Critical Alerts, Warning Alerts, and Information Alerts).

  - To narrow the time frame, select the **Date & Time Range**, select a **Start Date** and **End Date**, select a **Start Time** and **End Time**, and then select **Done**. Select **Reset to Default** to reset back to the default time frame.
- The **Alerts by Severity** widget displays the total number of **Alerts Raised** for the specified time range, with the colored bands of the arch and color-matched beads below it representing refinements on the basis of **Severity**, as follows:
  - Critical
  - Warning
  - Information
- A table lists the following alert details during the specified time range:
  - Alert Name
  - Summary
  - Severity
  - Status
  - Application
  - Location
  - Category
  - Source
  - Timestamp

  To view alert details, select an **Alert Name**. The **Alert Details** pane displays the following information:
  - Severity
  - Description
  - Detected
  - Source:
    - Name
    - Type
  - Details:
    - Model
    - MAC Address
    - Application
    - Serial Number
    - Admin State
    - IP Address
    - Location

  Note
  Select **Acknowledge** to mark the alert as reviewed. Acknowledging an alert does not resolve the issue, but it signals that the alert has been reviewed. This helps reduce duplicate investigations and allows teams to track which alerts are actively being addressed or have already been acknowledged.
- Select to export filtered alerts.
- You can use the **Search** field to filter the table view.

Audit Logs

Audit Logs provides a detailed record of user actions and configuration changes on the UCP device. Audit logs help administrators track activity for compliance, troubleshooting, and security auditing.

The table lists the following audit log details:

- **Timestamp**: Date and time of the recorded action.
- **Username**: The user who performed the action.

- **Context**: The area or component where the action occurred.
- **Description**: Details of the action performed.

Note

You can use the **Search** field to filter the table view. Select to export the audit logs.

Device View Actions Menu

Upgrade Firmware on page 119

In **Network Devices** > **Device Status**, select a device name from the **Device** column to display a list of available actions.

From the **Actions** menu, you can perform the following tasks on a selected device:

- **Reboot**: Restart the selected device. Select **Yes** to confirm.
- **Reset to Default**: Reset the device to factory defaults. Select **Yes** to confirm.

  Important
  This operation removes existing settings from the selected device and returns it to factory settings. It then reconnects to the cloud as a new device.

- **Upgrade Firmware**: Upgrade device firmware. See, Upgrade Firmware on page 119.
- **Locate**: Locate the physical location of the selected device. Set an **LED Timeout**, and then select **Submit**.

  Note
  To stop the blinking lights used for locating the device, select **Return to Standard LED operations**, and then select **Submit**.

- **VLAN Probe**: Locate available VLANs for the selected device. Configure the VLAN Probe settings, and then select **Start**. To stop a probe before it is complete, select **Stop**.
- **Assigned Location**: Assign a location to the selected device. Select a location, and then select **Submit**.
- **Configure Device**: Perform device-level configuration tasks and update devices. Settings made at this level apply only to the individual device and overrides the template settings configured for the network policy. For wired devices, see Configure Wired Devices.
- **Configure Fabric**: Configure the minimum required Global SPBM and Auto Sense settings to enable SPBM to operate on a wired device.

  Note
  This feature is available only if the device is in an Extreme Platform ONE Networking-compatible building or outdoor site with full features unlocked. For more information, see *Extreme Platform ONE Networking and ExtremeCloud IQ Licensing Entitlement Guide*.

Upgrade Firmware

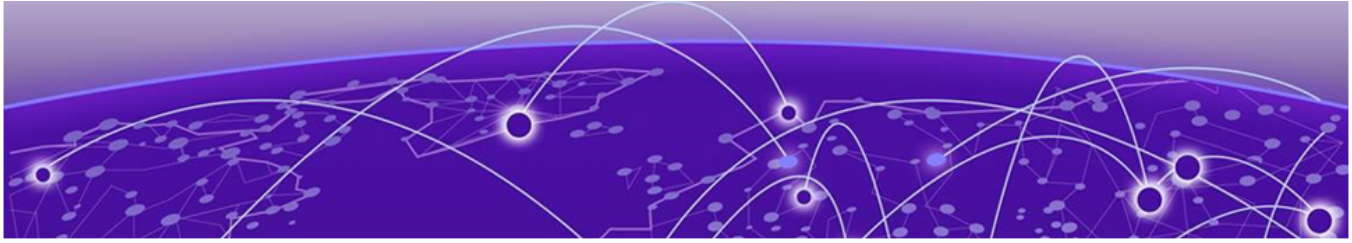
Use this task to manually upgrade firmware for a selected device.

1. Select **Upgrade firmware**.
2. Select a **Firmware Version**.
3. Select a **Firmware Upgrade Schedule**:
   - To update immediately, select **Upgrade Now**, and then select **Upgrade Firmware**.
   - To update at a later time, select **Upgrade Later**, select a **Date & Time** , and then select **Schedule Firmware Update**.

     Note
     Firmware upgrades can be scheduled up to 30 days in advance.

4. Select ⋮ to view **Firmware Upgrade History**. Firmware upgrade activity is stored for a maximum of 30 days.

   Note
   To reschedule a scheduled firmware upgrade:
   - Select a scheduled upgrade, and then select **Reschedule Upgrade**.
   - Select a new **Date & Time**, and then select **Reschedule**.



Switching/XLS Bulk Onboarding Support

Our bulk onboarding process relies on a CSV file format originally developed for wireless access point (AP) onboarding. While functional, this format is narrowly focused and does not adequately support the broader requirements of switching and appliance onboarding.

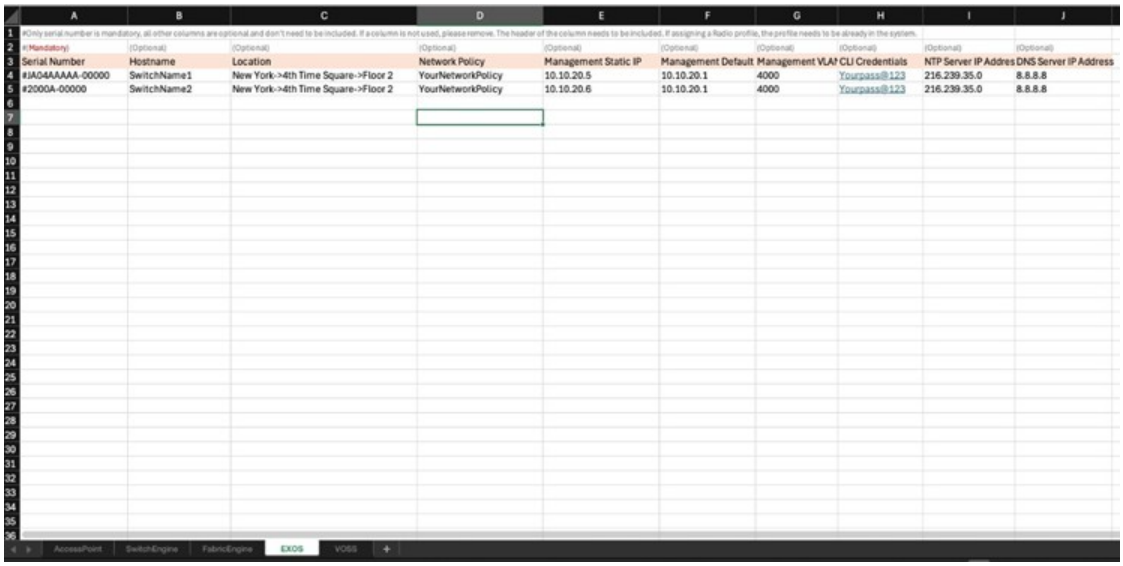
Extreme Platform ONE Networking supports an enhanced **XLSX-based onboarding template**. This new format will support:

- Fabric Configuration
- Switch Engine switches
- Access Points

The XLSX format offers improved structure, better documentation capabilities, and enhanced usability through features like data validation, drop-downs, and multi-sheet organization. This change lays the foundation for a more scalable and maintainable onboarding process across multiple device types.

Switch Engine/EXOS & Fabric Engine/VOSS

- Serial Number
- Hostname
- Location
- Network Policy
- In-Band Management Static IP, DG, VLAN, CLI Creds
- NTP, DNS Server IP



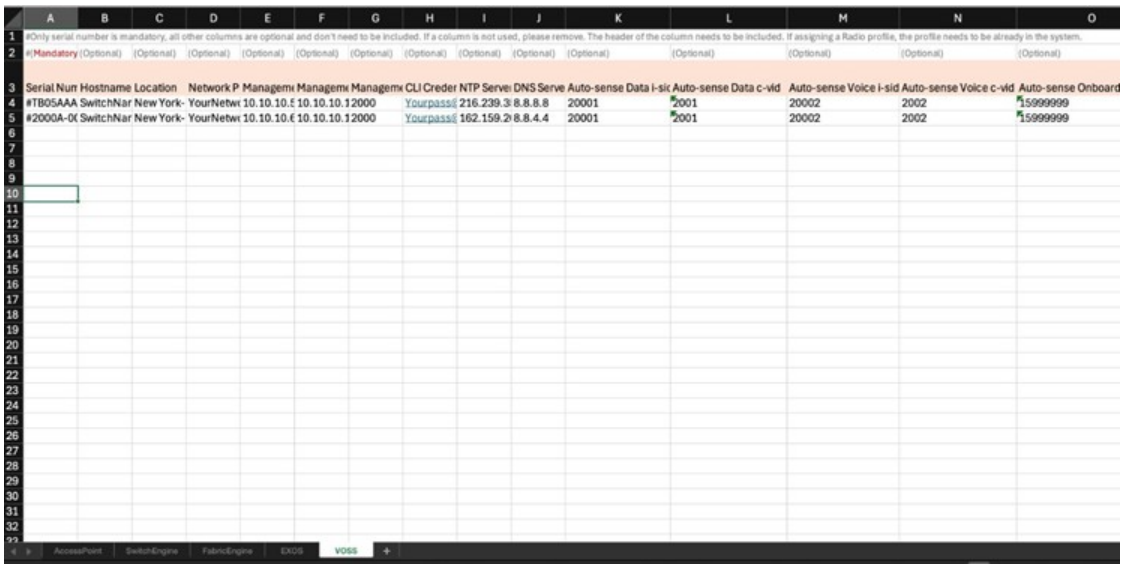
	A	B	C	D	E	F	G	H	I	J
1	#Only serial number is mandatory, all other columns are optional and don't need to be included. If a column is not used, please remove. The header of the column needs to be included. If assigning a Radio profile, the profile needs to be already in the system.									
2	#(Mandatory)	(Optional)	(Optional)	(Optional)	(Optional)	(Optional)	(Optional)	(Optional)	(Optional)	(Optional)
3	Serial Number	Hostname	Location	Network Policy	Management Static IP	Management Default	Management VLA	CLI Credentials	NTP Server IP Addres	DNS Server IP Address
4	#IA04AAAAA-00000	SwitchName1	New York->4th Time Square->Floor 2	YourNetworkPolicy	10.10.20.5	10.10.20.1	4000	Yourpass@123	216.239.35.0	8.8.8.8
5	#2000A-00000	SwitchName2	New York->4th Time Square->Floor 2	YourNetworkPolicy	10.10.20.6	10.10.20.1	4000	Yourpass@123	216.239.35.0	8.8.8.8
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										
17										
18										
19										
20										
21										
22										
23										
24										
25										
26										
27										
28										
29										
30										
31										
32										
33										
34										
35										
36										

AccessPoint | SwitchEngine | FabricEngine | EXOS | VOSS | +

Figure 3: XLS Bulk Onboarding Switch Engine/EXOS Example

Fabric Engine/VOSS Additional Config

- Auto-Sense
- Data I-SID, Voice I-SID, Onboarding I-SID
- FA wap-type, camera i-sid
- FA auth-key, FA message-auth, IS-IS hello-auth
- EAPOL voice LLDP-Auth
- EAPOL FA wap-type, camera auth

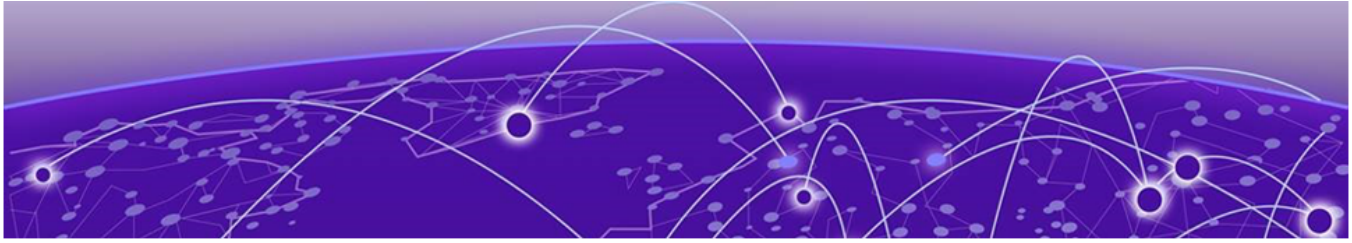


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	#Only serial number is mandatory, all other columns are optional and don't need to be included. If a column is not used, please remove. The header of the column needs to be included. If assigning a Radio profile, the profile needs to be already in the system.														
2	#(Mandatory)	(Optional)	(Optional)	(Optional)	(Optional)	(Optional)	(Optional)	(Optional)	(Optional)	(Optional)	(Optional)	(Optional)	(Optional)	(Optional)	(Optional)
3	Serial Num	Hostname	Location	Network P	Managem	Managem	Managem	CLI Creder	NTP Serve	DNS Serve	Auto-sense Data i-sic	Auto-sense Data c-vid	Auto-sense Voice i-sid	Auto-sense Voice c-vid	Auto-sense Onboard
4	#TB05AAA	SwitchNar	New York-	YourNetwo	10.10.10.5	10.10.10.1	2000	Yourpass@	216.239.3	8.8.8.8	20001	2001	20002	2002	15999999
5	#2000A-0(	SwitchNar	New York-	YourNetwo	10.10.10.6	10.10.10.1	2000	Yourpass@	162.159.2	8.8.4.4	20001	2001	20002	2002	15999999
6															
7															
8															
9															
10															
11															
12															
13															
14															
15															
16															
17															
18															
19															
20															
21															
22															
23															
24															
25															
26															
27															
28															
29															
30															
31															
32															
33															

AccessPoint | SwitchEngine | FabricEngine | EXOS | VOSS | +

Figure 4: XLS Bulk Onboarding Fabric Engine /VOSS Example

Fabric Engine / VOSS will automatically have XLS config pushed when network policy is defined as Fabric Engine / VOSS doesn't support auto provision.



Troubleshoot Switches

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

- You can have the device blink LED lights to physically show which device is selected.
- 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., see Configure Firewall Access on page 15.
- Reset the device to factory defaults and push a fresh configuration. This also simultaneously resets the ExtremeCloud IQ device configuration, see Reset Device Default Settings on page 125.
- 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.
- Switch Stack Issues: See Switch Stack Issues on page 127.
- Switch Communication Issues: See IQAgent and Switch Communication Issues on page 127.
- 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. See Use Cabletest for Switch Engine Device Duplex or Speed Issues on page 128.
- Audit Logs: Access these at **Administration & Settings** > **Logs** > **Audit Logs**

Locate Device

Using a visual cue helps you quickly identify the exact position of a connected device. By triggering the blinking function, you can efficiently manage and troubleshoot your network, ensuring optimal performance and coverage.

Use this task to locate the physical location of a connected device.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select at the end of a connected device row, select **Locate Device**, and then configure the Locate Device settings in Table 42.

Table 42: Locate Device Settings

Device Type	Field	Description
AP	LED Color	Select one of the following blinking light colors to set the color that the locator light flashes to help you find the AP: • Amber • White • Off
AP	Blink Mode	Select one of the following blinking modes to set the speed at which the locator light flashes to help you find the AP: • Fast • Slow • Steady
Switch	LED Timeout	Select a number of seconds between 0 (until disabled) and 604800 (one week).

Note
To stop the blinking lights used for locating the device, select **Return to Standard LED operations**, and then select **Submit**.

3. Select **Submit**.

Diagnostics CLI Commands

From the **Monitoring** > **Network Devices** > **Device Status** > **3-dot Menu** (⋮), select **Utilities** > **Diagnostics** to run one of the CLI commands, listed in Table 43 on page 124, on a device.

Note
For Tunnel Concentrator devices, only the following subset of diagnostics is available:

- Ping
- Show GRE Tunnel
- Show Tunnel Clients
- Show Log

Table 43: CLI Commands

CLI Command	Description
Ping	Have the selected device ping the IP address of its own mgt0 interface (default). You can change the target to any IP address, such as the default gateway, or an address beyond the gateway, such as a DNS server.
Show AFC Data Exchange	Displays details of the last data exchange between the AP and the AFC system, including request parameters, response channels, power limits, and status. **Note:** Available only for AFC Wireless devices.
Show AMRP Tunnel	Displays information about DNXP, INXP, and VPN tunnels, including tunnel type, the peer IP address, and how long the tunnel has been up.
Show ARP Cache	Displays the ARP cache.
Show CPU	Displays total, per user, and per system CPU utilization.
Show DNXP Cache	Displays the DNXP cache, which provides information that the device uses to form an association with a client that has already associated with a DNXP neighbor and that could possibly roam to it.
Show DNXP Neighbors	Displays neighboring hive members in the same or different subnets. This is the equivalent of entering the **`show amrp dnxp neighbor`** command. Hive members use AMRP to support roaming clients. DNXP is a component of AMRP that supports Layer 3 roaming. Hive members in different subnets use DNXP to create tunnels on an as-needed basis between themselves, allowing clients to seamlessly roam between subnets, while preserving their IP address settings, authentication state, encryption keys, firewall sessions, and QoS enforcement settings. Tunnels are not required for clients roaming among members in the same subnet.

Table 43: CLI Commands (continued)

CLI Command	Description
Show GRE Tunnel	Displays packet statistics for client traffic that members send through GRE tunnels between themselves. Extreme Networks devices use GRE tunnels for DNXP, INXP, and wireless VPN.
Show IKE Event	Displays up to 12 recent events during IKE phase 1 and phase 2 negotiations between a VPN client device and VPN server device.
Show IKE SA	Displays the cookies and creation times of SAs (security associations) established during IKE phase 1 negotiations between a VPN client and VPN server. If there are no SAs, the negotiations were either incomplete or unsuccessful. Use this option to check the log messages for more details.
Show IP Routes	Displays the IP routing table.
Show IPsec SA	Displays the SAs established during IKE phase 2 negotiations between a VPN client and VPN server.
Show IPsec Tunnel	View details about the IPsec tunnel including the amount of traffic between the VPN client and servers.
Show Log	Displays the event log for the device.
Show MAC Routes	Displays the MAC routes table.
Show Memory	Displays total, free, used, buffered, and cached memory.
Show Roaming Cache	Displays the roaming cache, which contains MAC addresses and PMKs (pairwise master keys) for wireless clients and MAC addresses for the authenticating devices. This table also includes the user profile ID number of the client and details about the PMK.
Show Running Config	Displays the configuration running on the device.
Show Startup Config	Displays the configuration used by the device on reboot.
Show Version	Displays the version running on the device.

Reset Device Default Settings

Use this task to reset a device to factory settings.

1. Go to **Monitoring** > **Network Devices**.
2. Select the one or more device(s).
3. Select the 3-dot menu and **Reset Device to Default** .

VLAN Probe

The VLAN probe action locates available VLANs for the selected device. When the VLAN probe is complete, a table shows the host name, MAC address, available VLANs, unavailable VLANs, and their status.

Note
The VLAN Probe Utility is also available from the **Device List** for a connected device.

Use this task to verify the VLAN probe results and status of VLAN for selected device.

1. Select **VLAN Probe**, and then configure the VLAN Probe settings in Table 44.

Table 44: VLAN Probe Settings

Field	Description
VLAN Range	The start and end **VLAN Range** to probe. You can enter up to five ranges separated by commas, up to a total range of 12. However, range numbers cannot overlap. For example, `1, 2-7, 8, 8-12`.
Timeout	The timeout from 5 to 60 seconds to specify how long to wait for a reply from each probe.
Probe Retries	The number of attempts made to send a probe to verify the status of a VLAN. **Note:** Probe retries is not supported for switch devices.

2. Select **Start** to start a probe.
3. Select **Stop** to stop a probe before it is complete.

Device Update Failure

This error indicates that a command on the switch failed to run or produced unexpected output. This can indicate that a manual or Supplemental CLI configuration conflicted with the configuration pushed by ExtremeCloud IQ. (See Configure Supplemental CLI on page 60). When Extreme Platform ONE Networking encounters this error, it attempts to push the same configuration delta again on the next update unless you create a different configuration.

Hover over this error message for more details.

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

   See Reset Device Default Settings on page 125.

VLAN or Trunk Issues

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

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

Switch Stack Issues

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

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

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

Switch Communication Issues

Before you begin become familiar with IQ Agent.

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

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

      Issues that might arise can be that you cannot ping the cloud or resolve host names.
2. Use **`ping extremecloudiq.com`** to check for basic internet connectivity.
3. Use **`ping vr vr-mgmt extremecloudiq.com`** to check for basic internet connectivity if you are using the dedicated management port.
4. Use **`traceroute extremecloudiq.com`** to check where packets are dropped.
5. Use **`traceroute vr vr-mgmt extremecloudiq.com`** to check where packets are dropped if you are using the dedicated management port.

6. Use configure **`iqagent server vr <VR-Mgmt | VR-Default> vlan <vlan_name>`** to configure a specific VR and/or VLAN for IQ Agent to use.

Use Cabletest for Switch Engine Device Duplex or Speed Issues

Follow all previous troubleshooting steps in this chapter.

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

1. Navigate to **Monitoring** > **Network 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 can temporarily interfere with port traffic.

8. If the test fails, check the physical cable connected to the device.

Resolving Configuration Discrepancies in Extreme Platform ONE Networking

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

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

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

Use this task to correct out-of-sync configurations in Extreme Platform ONE Networking and maintain a consistent and accurate configuration across managed switches.

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

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

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

   Extreme Platform ONE Networking displays the specific configuration elements that are out-of-sync between Extreme Platform ONE Networking and the running configuration on the switch.
5. Choose one of the following options:
   - Override configuration from Extreme Platform ONE Networking: With this option, the configuration changes made in Extreme Platform ONE Networking are pushed to the switch, overwriting any discrepancies in the running configuration. The switch configuration aligns with the Extreme Platform ONE Networking-defined configuration. Click on the **Update** button in the **Device Details** page or select the device and click **Update Device**.
   - Match configuration in Extreme Platform ONE Networking: With this option, using the CLI, you match the configuration flagged as out of sync with Extreme Platform ONE Networking, 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 Extreme Platform ONE Networking configuration.
6. Resolve interdependent conflicts manually before proceeding with a configuration update.
7. After you have selected the appropriate option for each configuration element, initiate the configuration synchronization from Extreme Platform ONE Networking.

   Extreme Platform ONE Networking pushes the selected changes to the switch, ensuring that the configurations are aligned.

Download Tech Support File

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

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

To download the technical support file:

1. Go to **Network Devices** and select a single device.
2. Select **Action**.
3. Select **Get Tech Support File**.
4. Select **Yes** when asked if you want to proceed.
5. Select **Download Tech Support**.