ExtremeCloud IQ (New) v25.5.0 User Guide

Comprehensive Management and Usage Instructions

9039466-00 Rev AA
October 2025

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/

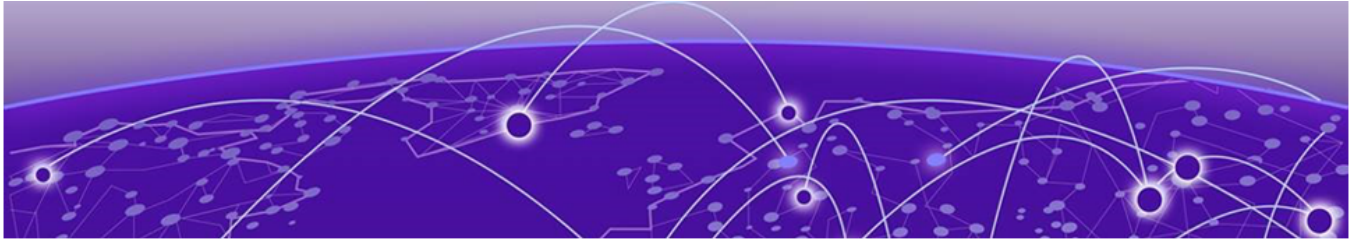
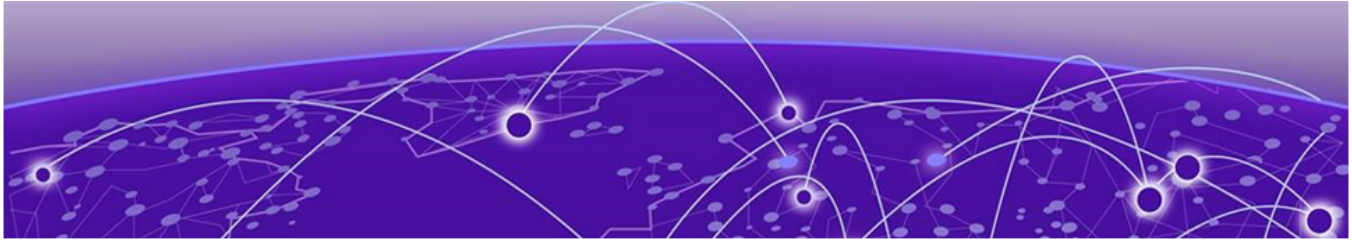


Table of Contents



Abstract

This user guide for ExtremeCloud™ IQ (New) version 25.5.0 provides comprehensive technical documentation for configuring, managing, and monitoring the Extreme Networks cloud-driven networking platform. Designed for IT professionals, the guide supports full-stack management of access points, switches, and SD-WAN using machine learning for automation, analytics, and operational intelligence. It details advanced configuration procedures for wireless and wired interfaces, including MU-MIMO, SDR, VLANs, LLDP/CDP, DHCP services, and Layer 2 IPsec VPNs. The guide includes step-by-step instructions for onboarding devices, deploying firmware, managing network policies, SSIDs, user profiles, and troubleshooting tools such as real-time packet capture, roaming trail visualization, and CLI diagnostics. Monitoring capabilities include RF heat maps, topology views (Access, FloorPlan, Geographic), and Device 360° insights. New features in this release include enhanced support for Hotspot 2.0, expanded Bonjour Gateway configuration, and improved device-level overrides. The document also covers alert management, role-based access, API integrations, and supplemental CLI configurations, ensuring secure and scalable network operations across diverse deployment 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.

Welcome to ExtremeCloud IQ (New)

ExtremeCloud IQ is an industry-leading approach to cloud-driven networking, designed to take full advantage of Extreme Networks end-to-end networking solutions.

ExtremeCloud IQ (New) offers the following:

- Unified, full-stack management of access points, switches, and SD-WAN
- Innovative ML technologies to analyze and interpret millions of network and user data points from the edge to the data center
- Network automation and intelligence to streamline operations

Important
For information about browser support and resolution settings, see Browser Support and Display Settings on page 15.

Note
During the customer onboarding process, Extreme Platform ONE Networking automatically creates the **Organization** for sites. The **Organization** name is the same as the **Company** name that you provided for your account.

ExtremeCloud IQ (New) consists of the following major sections:

- Navigation pane
- Content pane

Unified Login Page

The Extreme Networks unified login page grants access to applications based on licenses and simplifies migration. Customers having only Extreme Platform ONE Standard Networking licensed devices or a mix of Platform ONE Standard Networking and ExtremeCloud IQ Pilot licensed devices are directed to Extreme Platform ONE Networking. From there, you can navigate to ExtremeCloud IQ (Classic) from the 9-dot application menu, ensuring access to all ExtremeCloud IQ (Classic) features.

Extreme Platform ONE Networking licenses do not provide access to ExtremeCloud IQ (New). ExtremeCloud IQ (New) is available for customers having only ExtremeCloud IQ Pilot licenses and provides a limited subset of Extreme Platform ONE Networking features. ExtremeCloud IQ (New) customers can open ExtremeCloud IQ (Classic) from the 9-dot menu.

For more information about other applications and the 9-dot menu, see Extreme Applications and the 9-dot Menu on page 19.

Related Links

Extreme Applications and the 9-dot Menu on page 19

Extreme Applications and the 9-dot Menu on page 19

Log in to ExtremeCloud IQ (New)

Use this task to log in to ExtremeCloud IQ (New).

Note
Available widgets, menu selections, and action permissions depend on your role. For more information, see Role-Based Feature Access.

1. In a web browser, go to https://extremeplatformone.com, and enter your ExtremeCloud IQ credentials.

   Note
   If you don't have an existing ExtremeCloud IQ account, see Create an Extreme Platform ONE Networking Account on page 15.

2. Select **Log In**

   Note
   If you are an ExtremeCloud IQ customer and you have only ExtremeCloud IQ Pilot licenses, ExtremeCloud IQ (New) opens. If you have a mix of Pilot and Extreme Platform ONE Standard Networking subscriptions, or all Platform ONE Standard Networking subscriptions, Extreme Platform ONE Networking opens.

3. In the **Select a Network** dialog, select the account that you want to log in to.

   This dialog appears only if you have multiple accounts. After you log in, you can switch to another account. For more information, see Switch Accounts on page 13.

NEW! Switch Accounts

Use this task to switch accounts after log in.

1. On the ExtremeCloud IQ (New) banner, select  .
2. (Optional) If you have previously hidden some accounts, and want to see them again, select **Show Hidden Accounts**.
3. (Optional) To search for an account by name, start typing in the **Search** bar.
4. In the **Select a Network** dialog, select another account.

5. (Optional) To toggle visibility for an account, mouseover the account and select the corresponding icon:
   - To stop hiding a previously hidden account, select  .
   - To hide an account, select  .
6. (Optional) To favorite an account, mouseover the account and select  .

Forgotten Password

If you forget your password, you can reset it while logging in to ExtremeCloud IQ (New).

Use this task to reset a forgotten password.

1. In the **Log In** dialog, select **Forgot Password?**
2. In the **Forgot Password** dialog, type your **Business Email** (the email address for your account).
3. Select **Send Password Reset Link.**
4. Open your email and select the reset password link.
5. Follow the instructions to reset your password.

Change Password

Use this task to change your password.

1. In the upper-right of the page, select **<your initials>** > **Profile**, and the select **Change Password**.
2. In the dialog, complete following steps:
   a. In the **Current Password** field, type your current password.
   b. In the **New Password** field, type the new password.
   c. In the **Confirm Password** field, retype the new password.
   d. Select **Save**.

Log in with Single Sign-On

SSO simplifies the login process, so you can log in to ExtremeCloud IQ (New) using credentials from an existing SAML-enabled identity provider (IdP).

Key features of SSO:

- **Unified Access**: Log in once and gain access to integrated services without repeated logins.
- **Improved Security**: Use a single, strong password to reduce the risk of security breaches associated with weak or reused passwords, enforce multi-factor authentication based on your IdP policies, and deny administrative access to ExtremeCloud IQ (New) by removing users from the IdP.

Use this task to log in to ExtremeCloud IQ (New) using your SSO credentials.

1. In a web browser, go to `https://extremeplatformone.com`, and then select **Log in with SSO**.

2. Enter your email address, and then select **Log in with SSO**.

   Note
   When you log in with SSO for the first time, you must first select your organization from the list, and then follow the prompts. If you encounter difficulty during configuration, contact your ExtremeCloud IQ (New) administrator to determine whether your account can be configured for SSO.

3. Select your organization.
4. Enter your **Password**, and then select **Sign in**.

   Note
   If you can't remember your password, select **Forgot my password** to reset it.

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 **Create Account**.
2. In the **Create an Account** dialog, type your **Business Email**, and then select **Continue**.
3. Select **Continue**.
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.

Browser Support and Display Settings

Note
ExtremeCloud IQ (New) does not support 32-bit browsers.

Desktop Browsers

ExtremeCloud IQ (New) supports the latest 64-bit versions of the following desktop browsers:

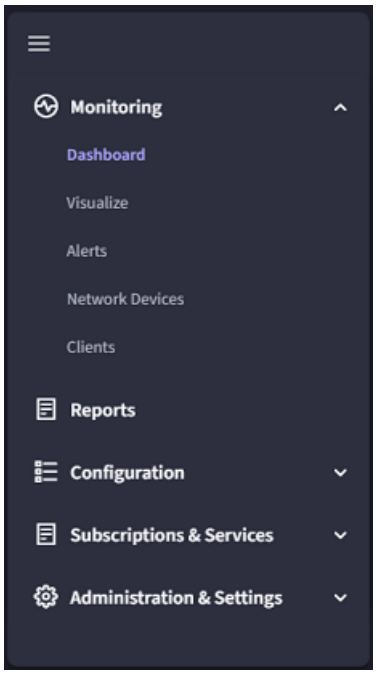
- Chrome
- Edge
- Firefox
- Opera
- Safari

Microsoft Internet Explorer is not supported.

Display Settings

ExtremeCloud IQ (New) supports display resolutions of 1280 x 1024 or higher.

Navigation Pane



Note
Select to toggle the navigation pane on and off.

Use the navigation pane to access the following work benches and content:

- **Workspace**
- **Monitoring**
  - Dashboard
  - Visualize
  - Alerts

    - Network Devices
    - Clients
- **Reports**
- **Configuration**
    - Sites
    - Network
- **Subscriptions & Services**
    - Subscriptions & Licensing
    - Contracts
    - Inventory
- **Administration and Settings**
    - Access Management
    - Alerts
    - External Notifications
    - Backup and Restore
    - Integrations
    - Logs

Content Pane

The ExtremeCloud IQ (New) content pane displays information related to your navigation pane selection.

Table 4 through Table 9 on page 22 describe fields and columns available in the content pane.

Table 4: Standard Icons

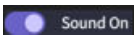
Icon	Description
Notification Bell 	Receive notifications for device, security, performance, and operational activities. When you select the bell icon, a panel displays the following: • **Go to Notification Center** button • **Sound On** toggle  : to hear notification alerts • The following tabs: ◦ All: displays all notifications ◦ Critical: displays critical notifications ◦ Non-Critical: displays non-critical notifications ◦ Information: displays relevant information • **Eye** Icon  **:** displays the total number of unread notifications Select **Go to Notification Center** to do the following: • View notifications from the last 24 hours, last week, last month and last quarter • Select **Generate Report** to download a list of notifications in .csv format • Use the **Search** field to quickly find notifications • Select a particular notification to view the following details about that notification: ◦ Site ◦ Device ◦ Severity ◦ Category ◦ Description ◦ Aggregation count, if applicable ◦ Time stamp
Profile Icon 	Select your initials at the top right corner of the screen to view the following: • Name and email address • Profile icon • About Extreme Platform ONE Networking displays the release version for each software component • Sign Out The **Profile** icon displays your name, login details, and multi-factor authentication (MFA). You can modify your name and password from this menu. **Note:** To show passwords on the screen, select  . You can choose a light or dark theme for your administrative environment.

Table 4: Standard Icons (continued)

Icon	Description
Extreme Applications 	Displays all applications available in ExtremeCloud IQ (New) for trial. • ExtremeCloud™ IQ • Universal ZTNA • ExtremeCloud SD-WAN • Extreme Intuitive Insights
Resource Center icon 	The **Resource Center** icon expands to show the following menu options: • Share Your Feedback • Product Tours • User Guide • Release Notes • Legal Summary • Contact Sales Team Each selection opens an external site, from which you can add feedback or obtain product-related information.
 Download	You can download data and export in .csv format. Use the Filter option to tailor your content to specific views.
 Refresh icon	Refreshes the screen and displays the latest information

Extreme Applications and the 9-dot Menu

The following table lists the applications available on the ExtremeCloud IQ (New) 9-dot menu, according to license type, including applications available for trial.

Table 5: ExtremeCloud IQ 9-dot menu

License types	Available applications	Available for trial
Pilot	ExtremeCloud IQ (Classic)	• Extreme Platform ONE Networking • Extreme Platform ONE Security • ExtremeCloud SD-WAN

Common Functionality

The ExtremeCloud IQ (New) user interface offers the following common functions across the platform:

- Select the information icon for more information.
- Use the **Search** field to find and display information based on the criteria that you enter.

- Tables:
  - 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.[1]
  - Select a column header to sort column data in ascending or descending order.[2]
  - Select **Columns** to add, remove, and reorder the columns.[1]
  - Select **Filters** to narrow your search. You can filter by column or by selecting the **Filter** button and using check boxes.[2]
  - **Filters Applied:** indicates that the data is filtered. To remove filtered data, select **X**.[2]
  - **Page Size:** Specify the number of rows to display per page.

[1] You cannot move the primary column.

[2] Unavailable for the **Dashboard** > **Sites** table.

Table 6: Monitoring View

Left Navigator Menu	Description
Dashboard	The **Dashboard** provides an overview of the network.
Visualize	For a description of all icons on the Visualize screen see, Visualize → Quick Navigation.
Alerts	The **Alerts** screen consists of the following features icons and details: • Date and Time Picker: Displays alerts for up to 30 days • **Refresh Alert**: Displays the most recent alerts • **Export to CSV**: Downloads alerts in a CSV file • **Acknowledge**: Indicates that the alert was read and understood Alerts detect, record, and report details of a specific event.

Table 6: Monitoring View (continued)

Left Navigator Menu	Description
Network Devices	The **Network Devices** page displays all devices for selected locations. You can manage the devices from this page.
Client & Users	The **Client & Users** screen provides an overview of clients and users.

Table 7: Configuration

Navigation pane	Description
Sites	The Sites page consists of the following features icons and details: • **Import Site Tree:** Drag & Drop or browse files in xml format. • **Add Site Group:** Add a site group to manage multiple sites. To add a site group see, Add a Site Group. • **Add Site:** Add a site and connect site groups to the site. To add a site see, Add a Site. • Select the overflow menu ⋮ at the end of each row to do one of the following: ◦ Add a building. ◦ Move a site. ◦ Export the plan in .xml or .tar format. ◦ Edit a site. ◦ Delete a site.

Table 8: Subscriptions & Services

Navigation pane	Description
Subscriptions	The **Subscriptions & Licenses** page includes the following features icons and details: • **Customer Unique Identifier (CUID)**: Use your CUID to purchase licenses and get access to your license pool. • **Linked to Extreme Portal:** A green status means you are connected to the Extreme Portal where you can access training, knowledge articles, forums, log support cases, and access to information about owned assets. • **Not Linked to Extreme Portal:** A red status indicates that you have lost connection. • **Unlink my Extreme Portal Account:** Removes the link to your Extreme Portal Account from Extreme Platform ONE Networking.

Table 8: Subscriptions & Services (continued)

Navigation pane	Description
	Caution: Do not **Unlink** your account without specific direction from Extreme Network Support personnel. • **Synchronize Subscriptions:** Synchronizes information from the license management server. **Note:** It can take up to 5 minutes to synchronize the license data. • **Search:** Search by description, entitlement status, and product. • **Status:** ◦ Green: Everything is good ◦ Yellow: A non-urgent issue ◦ Red: Requires immediate action • **Description:** Indicates the total number of subscriptions associated with a license. This number includes all active, inactive, and expired subscriptions. To view details about individual subscriptions, select the number next to the subscription. • **Entitlement:** Displays product entitlement. • **Product** Displays the product name. • **Total:** Displays the total number of licenses you have purchased. • **Active:** Displays the total number of licenses in use. • **Available:** The total number of licenses minus in use licenses.

Table 9: Administration and Settings

Navigation pane	Description
Access Management	The **Access Management** page provides the following functionality to create and view user access: • Internal Users • External Users • Single Sign-On • Credential Groups Select each section to view additional details. Icons and buttons: • **Create New User:** Add an internal or external user to your account. To create a new user see, Create a New User. • **Search:** Do searches based on column data.

Table 9: Administration and Settings (continued)

Navigation pane	Description
	• Select the overflow menu ⋮ at the end of the row to do one of the following: ◦ Edit ◦ Disable ◦ Delete Single Sign-On: **Note:** Only a **Super Admin** can enable SSO. To add an IdP profile on the **Single Sign On Identity Provider (IdP) Profile** page, select **Add IdP Profile**. Follow the steps to create the IdP profile and configure it with an IdP provider.
Alert Policies	The **Alert Policies** screen provides the following functions: • Configure a Global policy that impacts the full network. • Configure a Site policy that impacts a specific network site.
External Notifications	The **Notification Configuration** screen and the **Alert Notifications** tab consists of the following sections: • Email Recipients • Webhooks • ServiceNow Accounts Icons and buttons: • **Search Recipients:** Search based on column data • **Add Email Recipients:** Add new email recipients. • **Refresh** icon: Refreshes the screen and displays the latest notifications . • **Filters:** Filter notifications by the following: ◦ All ◦ Verified ◦ Not Verified • **Add Webhooks:** Add a new webhook for automatic alert notifications. • Select the overflow menu ⋮ at the end of the row to do one of the following: ◦ Edit ◦ Delete • **Add ServiceNow Accounts:** Add a new ServiceNow Account for automatic alert notifications.

Table 9: Administration and Settings (continued)

Navigation pane	Description
Backup & Restore	**Backup & Restore** provides the following functions: • VIQ management • Default device passwords In addition, you can perform the following actions: • View backup history • Export VIQ settings • Import VIQ settings
Integration	**Integration** provides the ability to use APIs to customize ExtremeCloud IQ (New).
Logs	**Audit logs** contains all changes made by users and applications. The **Audit Logs** screen consists of the following icons and buttons: • **Search:** Search based on column data. • **Date and Time Picker:** Displays activities for up to 30 days.

Navigation pane	Description
Access Management	The **Access Management** page provides the following functionality to create and view user access: • Internal Users • External Users • Single Sign-On • Credential Groups Select each section to view additional details. Icons and buttons: • **Create New User:** Add an internal or external user to your account. To create a new user see, Create a New User. • **Search:** Do searches based on column data. • Select the overflow menu ⋮ at the end of the row to do one of the following: ◦ Edit ◦ Disable ◦ Delete Single Sign-On: **Note:** Only a **Super Admin** can enable SSO. To add an IdP profile on the **Single Sign On Identity Provider (IdP) Profile** page, select **Add IdP Profile**.

Navigation pane	Description
	Follow the steps to create the IdP profile and configure it with an IdP provider.
Alert Policies	The **Alert Policies** screen provides the following functions: • Configure a Global policy that impacts the full network. • Configure a Site policy that impacts a specific network site.
External Notifications	The **Notification Configuration** screen and the **Alert Notifications** tab consists of the following sections: • Email Recipients • Webhooks • ServiceNow Accounts Icons and buttons: • **Search Recipients:** Search based on column data • **Add Email Recipients:** Add new email recipients. • **Refresh** icon: Refreshes the screen and displays the latest notifications . • **Filters:** Filter notifications by the following: ◦ All ◦ Verified ◦ Not Verified • **Add Webhooks:** Add a new webhook for automatic alert notifications. • Select the overflow menu  at the end of the row to do one of the following: ◦ Edit ◦ Delete • **Add ServiceNow Accounts:** Add a new ServiceNow Account for automatic alert notifications.
Backup & Restore	**Backup & Restore** provides the following functions: • VIQ management • Default device passwords In addition, you can perform the following actions: • View backup history • Export VIQ settings • Import VIQ settings

Navigation pane	Description
Integration	**Integration** provides the ability to use APIs to customize ExtremeCloud IQ (New).
Logs	**Audit logs** contains all changes made by users and applications. The **Audit Logs** screen consists of the following icons and buttons: • **Search:** Search based on column data. • **Date and Time Picker:** Displays activities for up to 30 days.

Pagination

ExtremeCloud IQ (New) supports pagination in all pages that show detailed data.

Select the required **Page Size** (**20**, **50**, **100**) to specify the number of entries in a table.

- The default page size is 20.
- Use the **Previous** (**<**) and **Next** (**>**) icons to scroll through the list.

Limitation:

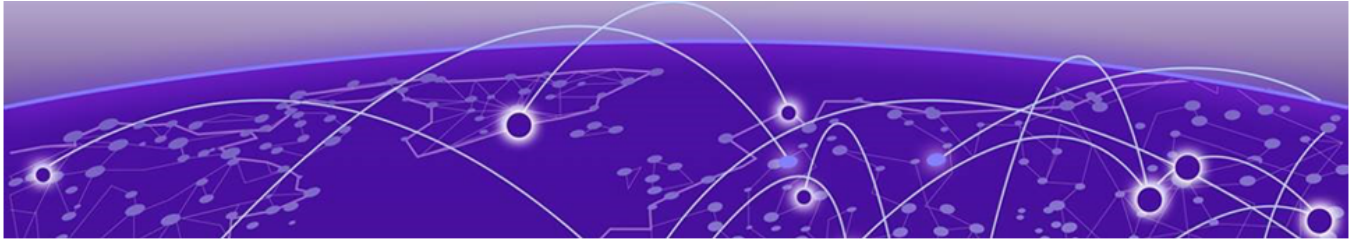
The user interface shows incorrect data on the previous page when you scroll through list pages after applying filters.

Choose a Theme

Use this task to choose a light or dark theme for your administrative environment. This task requires you to be logged in to your account.

1. Select your **Profile** (initials), and then select **Theme**.
2. Depending on your preference, select either **Light** or **Dark**.

   You can repeat these steps to switch between light and dark themes.



Monitoring

In the navigation pane, expand **Monitoring** and select one of the following options:

- **Dashboard**: Provides an overview of the network performance.
- **Visualize**: Presents a summary view of traffic on your network and the number of access points, routers, and switches. It also indicates the number of unique wired and wireless devices on your network and supports router attributes.
- **Alerts**: View and manage alerts.
- **Network Devices**: View managed and unmanaged devices.
- **Clients**: View and manage clients and users.

Dashboard

Dashboard uses the following widgets to provide an overview of the network performance for selected sites:

- Alerts
- Usage & Capacity
- Device Status
- Client Health
- Device Health

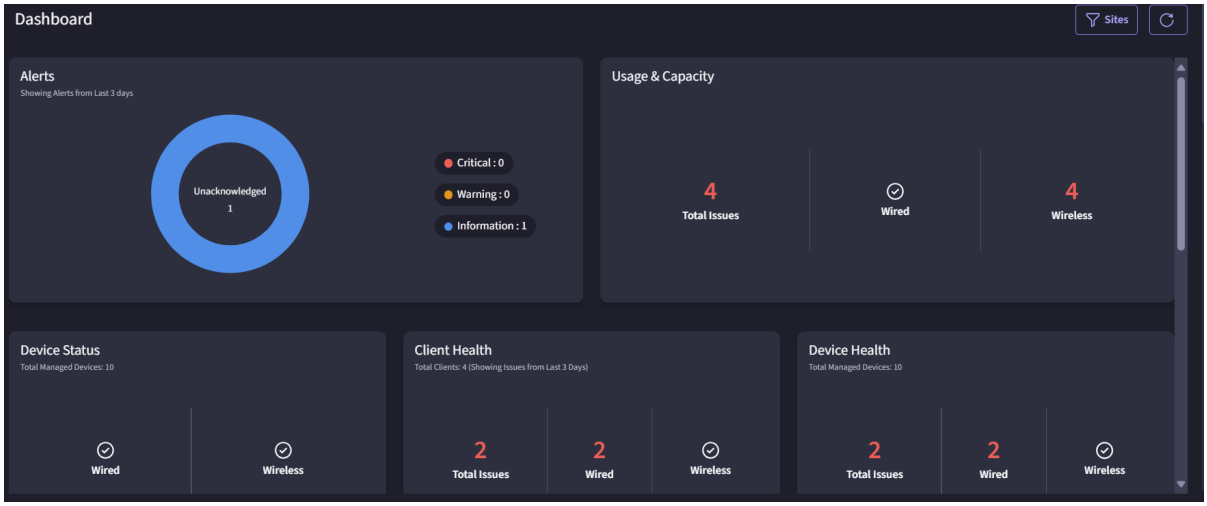


Figure 1: Dashboard

Use the **Sites** filter to select sites and filter the view.

Note
If you have access to only one site, the **Sites** filter is not present.

To display the timestamp for the last update, hover over .

To refresh the data, select .

To customize the **Sites** table view, select . You can choose which columns to display, the column order, and the number of results per page.

Visualize

Visualize provides a comprehensive overview of network performance and geographical location. For information about geographical location support, see Geographic View on page 33.

Customize the Visualize View

Use **Quick Navigation** to navigate to different levels of the network hierarchy. The following table lists and describes the **Quick Navigation** icons and other options for customizing the view.

Table 10: Visualize icons

Icon	Name	Description
Quick Navigation		
	Quick Navigation	Displays the different levels of the network hierarchy and shows the device count for each location. Use **Quick Navigation** to customize your display by location, building, and floor. To highlight the devices on the topology map for the selected location, hover over the devices in **Quick Navigation**.
	Group	Indicates a group of sites. Expand this element to see the sites.

Table 10: Visualize icons (continued)

Icon	Name	Description
	Site	Indicates a site. A blue icon indicates limited features and a purple icon indicates full features. Select **Unlock Full Features** to remove limitations by allocating Platform ONE licenses.
	Building	Indicates a building. A blue icon indicates limited features and a purple icon indicates full features. Select **Unlock Full Features** to remove limitations by allocating Platform ONE licenses.
	Floor	Indicates a floor.
	Floor plan	Indicates that a floor plan exists for the corresponding floor.
	Search	Indicates the search field for the **Quick Navigation**. To begin, start typing in the search field.
	3-dot menu	Provides the following options for the topology map: • Collapse All • Expand All • Hide All Borders • Show All Borders • Floor Layouts: ◦ U-Shaped ◦ Grid • Device Layouts: ◦ Stacked ◦ Spread ◦ Grid ◦ Hierarchical • Density ◦ Very Sparse ◦ Sparse ◦ Dense ◦ Very Dense • Initiate Discovery • Show Masked Devices and Links The 3-dot menu options vary for different levels of the network hierarchy.
General Visualization Options		
	Topology Locked	Indicates that the topology map is locked. Select to unlock the topology map.

Table 10: Visualize icons (continued)

Icon	Name	Description
	Topology Unlocked	Indicates the topology map is unlocked. When the map is unlocked, you can toggle **Autosave**. Select to lock the topology map.
	Zoom In	Zooms in the topology map.
	Zoom Out	Zooms out the topology map.
	Legend	Opens the legends used to describe the symbols used in topology maps.
	Open Minimap	Opens the minimap.
	Close Minimap	Closes the minimap.
	Fit View	Adjusts the magnification for the topology map view to display the entire map.
	Geographic	Provides options to select, or change between, the **Geographic** and **Access** views.
	Refresh Topology	Refreshes the topology map.
	Search	Search for **Devices** by name, IP, MAC, host name, or serial number.
	Filter	Filters the topology map view based on tags. **Note:** Filter settings and view are persistent.
	Settings	Opens the following topology map settings: • Display options • Manage
	Inspector Panel Control Button	Displays the **Inspector** panel for more information about selected elements and services.

Visualize Topology Maps

Visualize supports the following topology maps:

- **Access** view
- **FloorPlan** view
- **Geographic** view

Select  to open the view selector and change the topology map view.

Topology Legends

The following images show the symbols used in the **Geographic** layer and **Access** views.

Note

The **Service Nodes** legend and the **STP Blocked Port** legend entry ( ) are visible only in the legend for a split view with the Service and Physical layers.

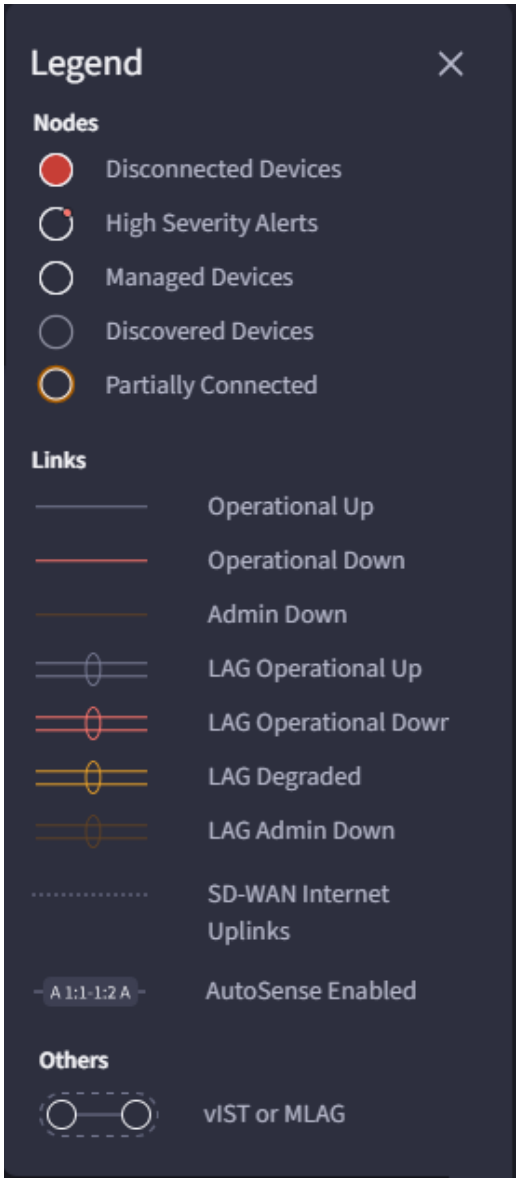


Figure 2: Access view topology legend

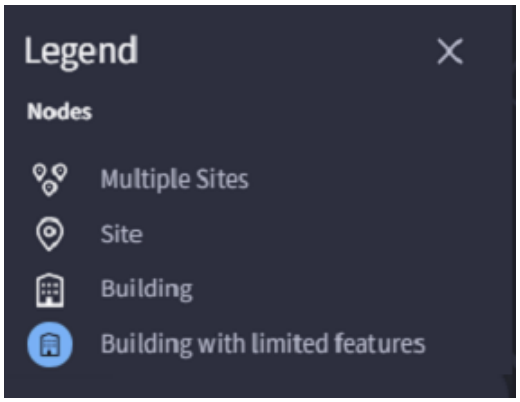


Figure 3: Geographic layer topology legend

Geographic View

The Geographic view is the default view in Visualize. The Geographic view supports the following functions:

- View sites
- Zoom-in up to the building level
- Zoom-out collapses the building level into sites
- Show links between buildings and sites

Note

- Geographic view requires graphics acceleration. For more information about how to enable this feature for your browser, see the Help for your browser.
- When you select a floor, the Geographic view shows the building location and filters devices to the selected floor.
- Hover your cursor over a site on the map to view details such as the number of sites or buildings, number of sites and buildings with alerts, and number of critical alerts.
- The current release supports alerts only from wireless devices in Geographic view.

FloorPlan View

From the **FloorPlan** view, you can view Radio Frequency (RF) network heat maps. RF maps use a color spectrum, ranging from warm to cool, to illustrate real-time device signal strength throughout a building floor plan. Warm colors represent a stronger signal strength. Cool colors represent a weaker signal strength.

ExtremeCloud IQ (New) supports the following map type views:

- Wi-Fi Map

- IoT Map

Note
Maps generated within the **Manage** > **Planning** section in ExtremeCloud IQ are visible in RF Maps.

With ExtremeCloud IQ (New) RF Maps, you can:

- Rotate the heat map.
- View device details or perform actions on a selected device (including uploading installation photos).
- View the summary details of clients connected to an AP (including Client 360º details, roaming paths, and authenticating).
- View the heat map in 3D.
- Filter devices by client connection type.
- Adjust thresholds.
- Change color schemes.

Use this task to view real-time network data coverage.

1. Go to **Monitoring** > **Visualize**, and then select .
2. From **Quick Sites Navigation**, select a floor.

Note
Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

Note
The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 130.

3. From the view selector, select **Views** > **FloorPlan**.
4. From the floor plan view pane, select **Map Type**.
5. To view the heat map for Wi-Fi devices, select **Wi-Fi**, configure the Wi-Fi map type settings in Table 11.

Table 11: Wi-Fi Map Types

Map Type	Radio Frequency
RSSI	2.4 GHz, 5 GHz, or 6 GHz
Coverage Overlap	2.4 GHz, 5 GHz, or 6 GHz
SNR	2.4 GHz, 5 GHz, or 6 GHz
Channel	All frequencies: 2.4 GHz, 5GHz, and 6 GHz
Interference	2.4 GHz, 5 GHz, or 6 GHz
Co-channel Interference	2.4 GHz, 5 GHz, or 6 GHz

6. To view the heat map for IoT devices, select **IoT**, configure the IoT map settings in Table 12.

Table 12: IoT Map Settings

Map Type	Radio Frequency
RSSI	2.4 GHz

Note
IoT heat maps support **2.4 GHz** radio frequencies only.

7. To rotate the map, from the top right corner, select and drag the slider.

Note
Select the arrow icon to reset the map rotation.

8. To view device details or perform actions, select a device on the map.
9. To view asset details for the clients connected to an AP, select the purple halo above the AP.
   - The purple halo shows the number of connected clients.
   - From the **Asset** pop-up window, select a **Hostname** to view client **Summary** and **Actions**:
     - The **Summary** tab displays the Host Name, OS, Uptime, IP Address, MAC Address, Connected to, VLAN, SSID, Captive Web Portal, User, User Profile, Radio, and Channel information for the selected client.
     - From the **Actions** tab:
       - To access Client 360° details, select **Client 360° View**. This opens a new pop-up window displaying the Client 360° information. To return to the client summary, close the pop-up window.
       - To view the roaming trail of the client, select **Client Roaming**. For more information, see View Client Roaming Trail on page 44.
       - Select **Deauthenticate** to disconnect the client from the access point.
10. Right-click an AP to:
    - **Show Coverage**: Updates the heat map to show the coverage from the single AP. To reset and see coverage from all APs, select **Show Coverage** again.
    - **Hide Device**: Hides the device from the heat map without removing it from the network. To show the device, see View Device Inventory on page 47.

Note
Hiding a device from the RF Map requires administrator privileges.

11. For Channel Wi-Fi map types:
    - To view the number of connected clients per AP, select  .
    - To view the number of clients per radio frequency for each AP, select  .
12. Select **3D** to view a three-dimensional representation of the heat map.
    This view allows users to visualize how signals propagate through different areas, including floors and walls, offering a more comprehensive understanding of network

coverage and potential dead zones. This helps to optimize placement of access points and improve overall network performance.

When viewing a heat map in 3D, you can:

- Select to stop the rotation. Select to start the rotation.
- Select and to zoom in and out.
- Select and drag the slider to adjust the angle of the map.

Note
Select **2D** to return to the default map view.

13. To filter devices on the map by their connection type, select one of the following icons:
    - : All
    - : Wi-Fi
    - : Thread
14. To set Wi-Fi coverage thresholds, configure the threshold values in Table 13, select , and then select **Apply**.

    Thresholds provide a visual to see where coverage is optimal, acceptable, and where improvements are needed.

Table 13: Wi-Fi Coverage Threshold Settings

Threshold	Description
Excellent	Above the set threshold, for example -30 dBm, the signal is considered excellent.
Good	Near the set threshold, for example -67 dBm, the signal is considered good.
Medium	Near the set threshold, for example 72 dBm, the signal is considered medium.
Poor	Below the set threshold, for example -90 dBm, the signal is considered poor.

15. To change the color scheme, select and then select a new color scheme.

Note
The **Select Color Map** icon might display different colors, depending on the last color scheme selected.

16. To zoom in and out, select **+** and **-**, or scroll the mouse wheel. Select and drag the map to move within the window.

Note
When you zoom in or out, the scale of the RF Map changes in real time below the zoom icons. The scale represents the relationship between the displayed area on the RF Map and the original map scale.

Related Links

Import a Third-Party RF Map on page 48
Edit an RF Map on page 50
Device Summary and Actions Menu on page 37
View Device Inventory on page 47
View Antenna Patterns on page 49

Device Summary and Actions Menu

In a Radio Frequency (RF) Map, select a device to display device summary information and a list of available actions.

AP Device Summary

The **Summary** tab displays the following information for a selected AP device:

- Connected status: Offering the number of Days, Hours, Minutes, and Seconds a device has been connected.
- AP Name
- Model, and OS Version
- Network Policy associated with the device
- SSIDs: Network SSIDs associated with the device
- AP Installation Height:
  - AP Installation Height
  - Accuracy Range for Installation Height (6GHz Only)
  - Elevation
  - Azimuth
  - Height from Ground (6GHz Only)
  - Accuracy Range from Ground (6GHz Only)

  Note
  To update any AP Installation Height parameter, select the corresponding field, input the new value, and then select **Save**.

- Wi-Fi 0, Wi-Fi 1, and Wi-Fi 2 details:
  - Radio Mode
  - Power
  - Channel
  - Channel Width
  - Frequency
  - Number of Clients
  - Mode
- Installation Photos: Upload photos or videos of the device installation. For better performance, limit the image file (.png, .jpg) to less than 500 KB and limit the video file (.mp4, .mov.) to less than 5MB.

Switch Device Summary

The **Summary** tab displays the following information for a selected switch device:

- Connected status: Offering the number of Days, Hours, Minutes, and Seconds a device has been connected.
- Hostname/SysName: Select to view device details.
- Model
- Network Policy associated with the device
- IP Address, System MAC Address, OS Version, and Make of the device
- Installation Photos: Upload photos or videos of the device installation. For better performance, limit the image file (.png, .jpg) to less than 500 KB and limit the video file (.mp4, .mov.) to less than 5MB.

Actions

From the **Actions** tab, you can perform the following actions on a selected device:

- Locate a Device.
- Reboot a Device.
- Perform a VLAN Probe.
- Reset a Device to Factory Defaults.
- Upgrade Device Firmware.
- Configure AP Radio and Power Settings.

Related Links

FloorPlan View on page 33

Locate a Device

Using a visual cue helps you quickly identify the exact position of a selected device within the mapped area. 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 selected device.

1. Go to **Monitoring** > **Visualize**, and then select  .
2. From **Quick Sites Navigation**, select a floor.

   Note
   Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

   Note
   The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 130.

3. From the view selector, select **Views** > **FloorPlan**.
4. Select a connected device from the floor plan, and then select **Actions**.

5. Select **Locate AP (blinking lights)** or **Locate Switch**, and then configure the Locate Device settings in Table 14.

Table 14: 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**.

6. Select **Submit**.

Related Links

FloorPlan View on page 33
Device Summary and Actions Menu on page 37

Reboot the Selected Device

Use this task to restart the selected device.

Important
The current configuration is not automatically saved. Restarting momentarily disconnects any connected clients.

1. Go to **Monitoring** > **Visualize**, and then select .

2. From **Quick Sites Navigation**, select a floor.

   Note
   Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

   Note
   The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 130.

3. From the view selector, select **Views** > **FloorPlan**.
4. Select a connected device from the floor plan, and then select **Actions** > **Reboot**.
5. Select **Yes** to confirm.

Related Links

FloorPlan View on page 33
Device Summary and Actions Menu on page 37

VLAN Probe from RF Maps

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. Go to **Monitoring** > **Visualize**, and then select .
2. From **Quick Sites Navigation**, select a floor.

   Note
   Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

   Note
   The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 130.

3. From the view selector, select **Views** > **FloorPlan**.
4. Select a connected device from the floor plan, and then select **Actions**.

5. Select **VLAN Probe**, and then configure the VLAN Probe settings in Table 15.

Table 15: 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`.
Probe Retries	The number of attempts made to send a probe to verify the status of a VLAN.
Timeout	The timeout from 5 to 60 seconds to specify how long to wait for a reply from each probe.

6. Select **Start** to start a probe.
7. Select **Stop** to stop a probe before it is complete.

Related Links

FloorPlan View on page 33
Device Summary and Actions Menu on page 37

Reset a Device to Factory Defaults

Use this task to reset the selected device to the default configuration. If you select **Yes** to acknowledge the warning message, the operation restores factory settings and reboots the device.

Important
This operation removes all existing settings from the selected device and resets the device to a factory default configuration state. The device reconnects to ExtremeCloud IQ (New) as a new device.

1. Go to **Monitoring** > **Visualize**, and then select .
2. From **Quick Sites Navigation**, select a floor.

Note
Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

Note
The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 130.

3. From the view selector, select **Views** > **FloorPlan**.
4. Select a connected device from the floor plan, and then select **Actions** > **Reset to factory defaults**.
5. Select **Yes** to confirm.

Related Links

FloorPlan View on page 33
Device Summary and Actions Menu on page 37

Upgrade Device Firmware

Use this task to manually upgrade firmware for a selected device from an RF Map.

Note
LLDP is on by default in ExtremeCloud IQ (New). With IQ Engine Release 10.7.5 and later, LLDP is on by default. If LLDP is disabled in the network policy, upgrading to 10.7.5 or later enables LLDP until after you perform a configuration update.

1. Go to **Monitoring** > **Visualize**, and then select .
2. From **Quick Sites Navigation**, select a floor.

Note
Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

Note
The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 130.

3. From the view selector, select **Views** > **FloorPlan**.
4. Select a connected device from the floor plan, and then select **Actions** > **Upgrade firmware**.
5. In the **Device Update** dialog box, select an update type.

Table 16: Update AP Device Settings

Field	Description
Update Network Policy and Configuration:	
Delta Configuration Update	To update only the configuration changes for the selected device, select **Delta Configuration Update**. ExtremeCloud IQ (New) only updates the device deltas. This action avoids a device reboot.
Complete Configuration Update	If a full update is required, select **Complete Configuration Update**. Used to reset the selected AP to ExtremeCloud IQ (New) configuration settings. **Note:** Only supported on devices running HOS or IQE Firmware.
Upgrade IQ Engine and Extreme Network Switch Images:	
Upgrade to the latest version	Upgrade to the latest firmware version.

Table 16: Update AP Device Settings (continued)

Field	Description
Upgrade to the specific version	Select a **Model** to upgrade, and then select the **Version** to upgrade. To add a new version (local image), select **Add/Remove**: • To add a new local image, select +, and then select **Choose** to upload an image file from your computer. **Note:** The format for an image file name must be *.stk, *.xos, *.voss *.tgz, *.img, or *.img.S. The file name cannot contain spaces and must not exceed 64 characters. • To delete an existing local image, select an image, and then select 🗑. • Select **Close**. Select **View Release Notes** to access the Online Help system and see the latest release notes.
(Optional) Upgrade even if the versions are the same	Force an upgrade to the same version as the current version.
Activation Time for Extreme Networks Devices Running Images:	
Activate at next reboot (requires rebooting manually)	Activation takes affect the next time the AP reboots.
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.

Table 17: Update Switch Device Settings

Field	
Update Network Policy and Configuration:	
Reboot and revert Extreme Networks switch configuration if IQAgent is unresponsive after configuration update.	**Note:** Not supported on Dell/SR.
Perform delta configuration update and resolve local device configuration which is out of sync with Extreme Platform ONE Networking.	
Upgrade IQ Engine and Extreme Network Switch Images	

6. To update the selected device immediately, select **Perform Update**.
7. To save the settings for future use, select **Save as Defaults**.

Related Links

Import a Third-Party RF Map on page 48
Edit an RF Map on page 50

Configure AP Radio and Power Settings

Use this task to configure AP radio and power settings.

1. Go to **Monitoring** > **Visualize**, and then select .
2. From **Quick Sites Navigation**, select a floor.

   Note
   Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

   Note
   The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 130.

3. From the view selector, select **Views** > **FloorPlan**.
4. Select a connected device from the floor plan, and then select **Actions** > **Radio and Power configuration**.
5. Select a Wi-Fi interface, configure the radio and power settings in Table 18, and then select **Apply**.

Table 18: Radio and Power Configuration Settings

Field	Description
Radio Status	Toggle the **Radio Status**.
Channel	Select a specific channel. Select **Auto** to have ExtremeCloud IQ (New) select the channel.
Transmission Power	Set the transmission power for the selected device (1 to 20 dBm). Select **Auto** to have ExtremeCloud IQ (New) select the transmission power.

Related Links

FloorPlan View on page 33
Device Summary and Actions Menu on page 37

View Client Roaming Trail

Viewing the client roaming trail to an access point (AP) on a real-time map has the following benefits:

- **Troubleshoot Connectivity Issues**: Identify areas where the client might be experiencing weak signals or frequent disconnections.
- **Optimize Network Performance**: Understand the movement patterns to adjust the placement of APs to ensure better coverage and reduce dead zones.
- **Monitor Security**: Detect any unusual or unauthorized movements within the network, which could indicate potential security threats.

Use this task to view the roaming trail of a selected AP client from a real-time map.

1. Go to **Monitoring** > **Visualize**, and then select .

2. From **Quick Sites Navigation**, select a floor.

   Note
   Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

   Note
   The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 130.

3. From the view selector, select **Views** > **FloorPlan**.
4. Select the purple halo above a device.

   The purple halo shows the number of connected clients on the device.
5. From the **Inventory** list, select an available **Hostname**, and then select **Actions** > **Client Roaming**.

   A split window opens:

   - **Left Pane**: This pane displays the map and shows how the client roamed.
   - **Right Pane**: This pane displays the roaming view details, including the Client Name, Roaming Time, and surrounding APs.
6. To view the roaming trail, from the right pane, select **Play**.

   Note
   By default, the roaming view displays client roaming details for the previous hour.

   The roaming trail plays within the top map pane, showing where the client roamed and how long it took:

   - A **green** roaming trail signifies a good roam (less than one second).
   - A **red** roaming trail signifies a slow roam (longer than one second).
7. To narrow the roaming time frame, from the right pane, select the **Date & Time Range**.

   a. Select a **Start Date** and **End Date**.
   b. Select a **Start Time** and **End Time**.
   c. Select **Done**.

   To reset to the default time frame, select **Reset to Default**.
8. To exit the roaming view and return to the real-time map, select **X**.

Related Links

FloorPlan View on page 33

Real-Time Troubleshooting

Real-Time Troubleshooting is designed to monitor and diagnose client-side issues as they occur in real-time. This functionality is supported on the following devices: AP3000, AP3000/X, AP5010, and AP5050U/D.

Real-time client monitoring displays the following insights into client-side issues, allowing for prompt identification and resolution:

- **RSSI (Received Signal Strength Indicator)**: Measures the power level that a device receives from an access point.
- **SNR (Signal-to-Noise Ratio)**: Indicates the quality of the signal relative to background noise.
- **Usage**: Tracks the bandwidth consumption of connected devices.
- **Tx (Transmit) and Tx Retries**: Monitors the number of packets sent and the number of retransmissions required.
- **Rx (Receive) and Rx Retries**: Tracks the number of packets received and the number of retransmissions required.

Client Statistics displays the number of data packets transmitted and retried. **Packet Stream** displays the control packets used to manage the network.

You can run Real-Time Troubleshooting simultaneously on up to 10 access points. This capability is particularly useful for identifying and addressing roaming issues, where clients move between different access points.

By leveraging Real-Time Troubleshooting, network administrators can gain a comprehensive view of network performance and client behavior, enabling them to quickly address any issues that arise.

Use this task to begin Real-Time Troubleshooting.

1. Go to **Monitoring** > **Visualize**, and then select .
2. From **Quick Sites Navigation**, select a floor.

   Note
   Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

   Note
   The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 130.

3. Select the purple halo above a device.

   The purple halo shows the number of connected clients on the device.
4. From the Inventory list, select an available **Hostname**, and then select **Actions** > **Real-Time Troubleshooting**.
5. Select a **client from this site (Hostname of MAC)**.
6. Select **one or more APs to track the client**, up to a maximum of 10.
7. Select one of the following **Packet Stream** options:
   - All
   - Data Frames
   - Management Frames

8. Select **Start**.

   Note
   Starting up Real-Time Troubleshooting services typically takes about 10-20 seconds.

9. Select **Client Statistics** to see the following detailed information about the transmission (Tx) and reception (Rx) of packets:
   - **Tx Packets**: The number of packets sent from the source device
   - **Rx Packets**: The number of packets received by the destination device
   - **Tx Retries**: The number of times packets had to be retransmitted due to errors or failures in the initial transmission
   - **Rx Retries**: The number of times packets had to be re-received due to errors or failures in the initial reception
   - **Total Packets**: The total number of packets sent and received
   - **Total Retries**: The total number of retransmissions and re-receptions due to errors
   - **Total Data Usage**: The overall amount of data transmitted and received, in bytes
10. Select **Packet Stream** to see the following details for each packet:
    - **Time**: The timestamp indicating when the packet was captured
    - **Serial Number**: A unique identifier assigned to each packet for tracking purposes
    - **Source**: The IP address or hostname of the device that sent the packet
    - **Destination**: The IP address or hostname of the device intended to receive the packet
    - **Protocol**: The communication protocol used by the packet
    - **Length**: The size of the packet in bytes
11. Select **Stop** to end Real-Time Troubleshooting.

View Device Inventory

Inventory displays a list of **Access Points**, **Switches**, or **Clients** currently being monitored on an RF Map.

The **Access Points** and **Switches** asset lists provide the following details about each device:

- **Hostname**: The name assigned to the device
- **Status**: The current operational state of the device
- **IP Address**: The unique network address assigned to the device
- **Show/Hide**: An option to toggle the visibility of the device on the heat map, allowing for a more customized and focused view of the real-time status of your network

The **Clients** asset list provides the following details about each device:

- **Hostname**: The name assigned to the device
- **MAC Address**: The unique identifier assigned to the device
- **IP Address**: The unique network address assigned to the device
- **Type**: Filter by different client types

Use this task to toggle the visibility of **Access Points** and **Switches** and filter **Client** types on a selected heat map.

1. Go to **Monitoring** > **Visualize**, and then select .
2. From **Quick Sites Navigation**, select a floor.

   Note
   Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

   Note
   The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 130.

3. From the view selector, select **Views** > **FloorPlan**.
4. Select .

   Note
   Use the **Search** field to find a specific device.

5. Select an Asset type:
   - Access Points
   - Switches
   - Clients
6. Select a **Hostname** to view device summary and available actions. For more information, see Device Summary and Actions Menu on page 37.
7. To hide an **Access Point** or **Switch**, deselect the corresponding checkbox.
8. To show a hidden **Access Point** or **Switch**, select the corresponding checkbox.

Import a Third-Party RF Map

ExtremeCloud IQ (New) supports the following third-party RF Maps:

- Ekahau
- Hamina

Use this task to import a third-party RF Map.

1. Go to **Monitoring** > **Visualize**, and then select .

2. From **Quick Sites Navigation**, select a floor.

   Note
   Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

   Note
   The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 130.

3. From the view selector, select **Views** > **FloorPlan**.
4. Select .
5. To import a floor map from Ekahau, select **Import Ekahau**:
   a. Select **Choose**, then browse to your local folder, select a .esx floor plan, and then select **Open**.

      Note
      Use the **serialNumber** tag to import devices with your floor plan.

   b. Select **Next**.
   c. From **Import floors**, select a **Building** from the drop down list.

      Note
      With RF Maps you can only import building floors. To import a site, site folder, or a building, go to **Configuration** > **Sites**.

   d. If the configuration is custom, select the **Import Custom AP Configuration** checkbox.
   e. Select one or more floor plans.
   f. To move a single floor plan, double-click the selected plan.
   g. To move more than one plan, select the applicable arrow.
   h. Select **Import**.
6. To import a floor map from Hamina, select **Import Hamina**:
   a. Log in to your active Hamina account and select **Export**.
   b. Select **Extreme Networks** and follow the instructions.
   c. Select **Export**.

   Your floor map now displays APs in the correct building on the correct floor.

Related Links

FloorPlan View on page 33
Edit an RF Map on page 50

View Antenna Patterns

Antenna Patterns allow users to visualize the coverage and performance of devices on the heat map. This visualization is essential for optimizing network design and troubleshooting connectivity issues.

The antenna patterns display how the antenna radiates energy in different directions and frequencies, including:

- Azimuth Plane: A top-down view of the radiation pattern, illustrating how the signal spreads out horizontally. It helps in understanding the coverage area and signal strength in different directions around the device.
- Elevation Plane: A side view of the radiation pattern, illustrating how the signal spreads out vertically. It helps in understanding the coverage area and signal strength above and below the device.
- Frequency Band: Along with Azimuth and Elevation planes, displays the radiation pattern for the 2.4 GHz, 5 GHz, and 6 GHz frequency bands for wireless devices.

These patterns help network administrators visualize and optimize device placement to ensure even and effective coverage.

Use this task to view antenna patterns.

1. Go to **Monitoring** > **Visualize**, and then select .
2. From **Quick Sites Navigation**, select a floor.

   Note
   Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

   Note
   The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 130.

3. From the view selector, select **Views** > **FloorPlan**.
4. Select .

   Note
   Use the **Search** field to find a specific device.

5. Select a device tab.

Edit an RF Map

An RF Map provides a visual representation of device signal strength across a floor plan. By editing the RF Map, you can identify areas with weak coverage, interference, and dead zones. This information helps network administrators optimize device placement and improve overall network performance.

ExtremeCloud IQ (New) supports the following RF Map editing functions:

- Draw Inner Walls
- Add a Device to a Floor Plan
- Move a Device to a New Location on a Floor Plan
- Remove a Device from a Floor Plan

- Adjust Layer Opacity
- Resize the Heat Map

Use this task to edit an RF Map.

1. Go to **Monitoring** > **Visualize**, and then select .
2. From **Quick Sites Navigation**, select a floor.

Note
Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

Note
The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 130.

3. From the view selector, select **Views** > **FloorPlan**.
4. Select .
5. To draw inner walls:
   a. Select **Walls**.
   b. Select a wall type. See Table 19 for wall type descriptions.

Table 19: Floor Plan Wall Types

Wall Color	Description
	Bookshelf 5dB
	Cubicle 2dB
	Dry Wall 3dB
	Brick Wall 5dB
	Concrete 15dB
	Elevator Shaft 10dB
	Thin Door 4dB
	Thick Door 10dB
	Thin Window 1dB

Table 19: Floor Plan Wall Types (continued)

Wall Color	Description
	Thick Window 6dB
Add Custom Material	Create a new custom material by entering a **Name**, specifying the **Attenuation** (in dB), and selecting a **Color**. Select **Apply** to use this new material type. Delete an existing custom material by selecting the material and pressing the **Delete** key on your keyboard. **Note:** Custom materials can only be deleted after all associated references to the them have been removed.

c. Select each corner of an inner wall on the floor plan to draw a wall boundary.
d. When you reach the end of the wall boundary, double-click the last corner to complete the wall.

Note
Right-click on a wall to change its type or delete it.

e. To disable the pen tool, press the **ESC** key on your keyboard.

6. To add a device to the floor plan, select **Devices**:
   a. Select a device, or use the **Search** field to find a device.
   b. Hover over the floor map and select the desired location to add the device to the floor plan.

Note
Only devices that are not associated with the floor plan are displayed.

7. To move a device to a new location on the floor plan, select **Devices**, and then select a device and drag it to the desired location.
8. To remove a device from the floor plan, select **Devices**, right-click the device, and then select **Remove Device**.

Note
The removed device displays in the **Devices** list.

9. To adjust the opacity of the heat map layers, select **Layers** and adjust the opacity slider bar to make a layer more or less transparent.

Note
As you adjust the slider bar, the layer opacity changes on the map in real time.

10. To resize the heat map, follow these steps:
    a. Select **Recalibrate**.
    b. Select your starting point on the map.

c. Select again to close the line.
d. Add a measurement (in feet) for the line distance, and then press **Enter**.

11. To return to the heat map, select **Exit**.

Related Links

FloorPlan View on page 33
Import a Third-Party RF Map on page 48

Access View

The **Access** view shows per floor view of edge devices such as access points, phones, and cameras connected to a device in a building. The view in the content pane depends on your selection in the navigation pane, as follows:

- If you select a site or group of sites, the content pane displays the first building belonging to the selected site or group of sites.
- If you select a building, the content pane displays the edge devices and connections for that building.
- If you select a floor, the content pane displays the edge devices and connections for that building, and focus is set to the selected floor.

The content pane displays the following devices (expanded) for the **Access** view:

- APs assigned to the selected floor or building
- If the LLDP Neighbors feature is enabled:
  - LLDP-discovered devices connected to switches on the selected floor or in the selected building
  - Cameras connected to switches on the selected floor or building
  - Phones connected to switches on the selected floor or building
  - Other devices connected to switches on the selected floor or building
- Existing links between switches that appear in the content pane

You can hover over an edge device or select it to view the details.

Device Discovery

Visualize supports managed APs, VOSS (Fabric Engine), and EXOS (Switch Engine) devices.

Use **Visualize** to view and manage all devices onboarded through common onboarding services, including switch stacks. **Visualize** view generates a topology map of all

managed on-boarded devices by analyzing data from the LLDP protocols (physical) and Intermediate System to Intermediate System (IS-IS) logical tables.

Table 20: Device Discovery based on LLDP

Adjacency	Description
Physical	Extreme Platform ONE Networking uses physical network connections to generate LLDP Neighborship from the devices.
Logical	Extreme Platform ONE Networking uses logical network connections to generate LLDP Neighborship, ISIS tables, and SD-WAN data.
Third-Party Devices	Special LLDP TLVs discover third-party devices, such as cameras, IoT devices, and sensors, and show them as attached devices on the topology map.

Device Group

The **Visualize** view leverages site-group and site hierarchy in Extreme Platform ONE Networking for the auto-creation of groups during the device onboarding process. Sites and site groups appear in groups on topology maps.

The topology map is a persistent view. The following map characteristics persist after you log out and log back in:

- Layout changes
- Hierarchical level
- User-defined details

Initiate Device Discovery

Use this task to add devices onboarded through ExtremeCloud IQ or Extreme Platform ONE Networking to the Visualize topology map.

1. Go to **Monitoring** > **Visualize** and select .
2. Select , and then select **Expand All**.
3. Locate the required building.
4. Select for the building, and then select **Initiate Discovery**.

   After a successful device discovery, a notification message with a **Refresh** button opens.
5. To refresh the topology map, from the **Success** notification, select **Refresh**.

View Inspector Panel

Use this task to view the **Inspector** panel.

1. Go to **Monitoring** > **Visualize**.
2. To view the **Inspector** panel for the selected site, building, floor, or group of devices, select .

View and Acknowledge Alerts

You can use **Quick Navigation** to navigate to critical alerts by location on the topology map.

Use this task to view and acknowledge alerts.

1. Go to **Monitoring** > **Visualize**.
2. Use **Quick Navigation** to navigate to critical alerts by site, building, or floor.
3. Select a location with critical alerts.
4. To open the **Inspector** panel, select a device.
5. To view alerts, select the **Alerts** tab in the **Inspector** panel.
6. Select an alert from the **Top 3 Alerts** list to view and acknowledge.
7. Select **Acknowledge** to mark the alert as reviewed.

View the Device Inspector Panel

Use this task to view the **Device Inspector** panel.

1. Go to **Monitoring** > **Visualize** and select a view or layer.
2. To view device-specific information, select a device in the topology map.

   The device-specific inspector window opens. You can expand or collapse the device information for a focused view in each tab.

   The following actions are available from the 3-dot menu:

   - Reboot
   - VLAN Probe
   - Assign Location
   - Configure Device
   - Configure Fabric
   - Update Device

View Device 360°

Use this task to open Device 360° from the **Visualize** view.

1. Go to **Monitoring** > **Visualize**.
2. To open the **Device Inspector** panel, select a managed device in the content pane.
3. In the **Device Inspector** panel, select  .

   Available information depends on the device selected and the connection type (wired or wireless). For more information, see the following topics:

   Wired Devices

   - Overview on page 104
   - Clients on page 105
   - Port Stats on page 106
   - Services/VLANs on page 107

- Routing on page 108
- Events on page 109

Wireless Devices

- Overview on page 104
- Wireless Interface on page 114
- Wired Interface on page 114
- Clients on page 114
- Alerts on page 115

AutoSave Device Layout and Density

Use this task to enable the autosave feature for device layout and density in the Access view.

1. Select to unlock device layout and density.
2. Enable the **AutoSave** option.
3. Go to , and select a floor.
4. Select for the floor, and then choose the required **Device Layout** and **Density** options for the topology map:

   Device Layout :

   - Stacked
   - Spread
   - Grid
   - Hierarchical

   Density:

   - Very Sparse
   - Sparse
   - Dense
   - Very Dense

Search an Element

You can search the network for configured VLANs, L2, and L3 services. **Visualize** can display five global services on the topology map. You can select or switch between these global services to view the topology map.

Use this task to search an element in the network topology map.

1. Go to **Monitoring** > **Visualize**.
2. Select .

3. Select the required filter keyword for searching:
   - Devices
   - Services
   - VLANs
4. Type a **Device Name** in the **Search** field.

   All devices with the specified search value open in the global view.

Settings

Select ⚙ to configure topology map settings in the **Visualize** view.

Configure the Display Options

Use this task to configure display options for Visualize topology maps.

Note
The display options are user-specific.

1. Go to **Monitoring** > **Visualize** and select ⚙.
2. Select **Display Options**.
3. Select the **Access** layer options:
   - **Device Labels**: **Name**, **IP**, or **Type** (Select any two.)
   - **LLDP Neighbors** (devices with LLDP and Fabric Attach capabilities):

     You can expand or collapse **Display LLDP Options** to view and edit the list of LLDP devices:
     - Discovered APs
     - Cameras
     - Phones
     - Others (LLDP devices without any capabilities set)

       Note
       To include all types of devices without LLDP capabilities, select **Others**. This option is disabled by default.
4. Select **Apply Settings**.

Manage

The following capabilities are available on the **Settings** > **Manage** tab for all views and layers, except **Geographic**.

- Select **Save User Settings** to save display options, filters, expand/collapse state of **Quick Navigation**, topology focus, zoom level, border state, device types settings, and the breadcrumb path.
- Select **Restore Settings** to restore and apply the saved display options, filters, and border settings.
- Select **Manage Tags** to view tags.

Tags

Apply **Tags** to managed resources in the **Visualize** view. The tags act as labels and help in easy filtering of the devices in maps.

Table 21: Tag types

Tag Type	Description
Default Tag	Default tags are auto assigned during device discovery based on predefined criteria. These tags are created based on switch type, location, model, VLAN, VRF, L2 service, and L3 service. The default tags are read-only and cannot be altered or deleted. The system automatically assigns **Provisional** tags to masked devices.
Manual Tag	Manual tags are labeled by the user. Types of manual tags: • Policy based • Non-policy based

User Roles Supported in Visualize View

Visualize view supports the following user roles:

Table 22: Supported user roles

User Role	Description
Administrator	Administrators have read-write access to Visualize view. They can create and manage all administrator users and licenses through Visualize view.
BizSecOps	BizSecOps have read-write access, but cannot manage accounts and licensing.
BizOps	BizOps have no access to Visualize view.
Observer	Observers have read-only access to Visualize view.

For more information about roles, see Role-Based Access on page 329.

Alerts

The **Alerts** view provides a comprehensive overview of network alerts, allowing operators to detect, record, and report specific events. It evaluates performance metrics and reports occurrences where specific criteria are met. Alerts can be filtered by time range, severity, status, site, and source.

Users can receive alert notifications through email or Webhooks.

Manage Alerts

The **Alerts** view offers widgets such as **Severity**, **Category**, **Top 3 Alerts**, and **Application** to filter the list of alerts raised during the specified time range.

Go to **Monitoring** > **Alerts**.

You can use widgets to filter the list of alerts raised during the specified time range.

Select **Alert Policies** to view and manage global and site policies.

Note
Site policies take precedence over global policies.

Alert Details

By default, the **Alerts** page displays information about alerts raised at all sites for the last 24 hours. You can filter the **Alert Details** list using the following methods:

- Use the **Time Range** controls to specify a time range, within the last 30 days, for which you want to view alerts.
- Use the **Severity** filter to view alerts based on specific severity:
  - Critical - Red
  - Major, Minor, and Warning - Orange
  - Info - Blue
- Use the **Status** drop-down list to view **All** (default), **Acknowledged**, or **New** alerts.
- Use the **Sites** filter to view alerts associated with a specific site.
- Use the interactive device host name in the **Source** column for more information about the alert.
- Use the **Refresh Alerts** button to view the most recent alerts.
- Use the **Export to CSV** button to download the alert data in `.csv` format.

Note
The column filter settings do not persist.

Use the Filter Side Bar

Use the filter sidebar to customize the information shown in the **Devices** list and other **Alerts** view tables. You can save and reuse custom-defined filters. Saved filters are displayed in the saved filters section.

The Filter icon changes depending on whether a filter is applied.

View and Acknowledge Alert

1. Go to **Monitoring** > **Alerts**.
2. Navigate to alerts by **Severity**, **Category**, **Top 3**, or **Application**.
3. Select an alert from the list to view and acknowledge.
4. Select **Acknowledge** to mark the alert as reviewed.

Add a Site Policy

Use this task to add a site policy.

1. Go to **Administration & Settings** > **Alert Policies**, and select **Site Policies**.
2. Select **Add Site Policy**.
3. Complete the following:
   - Provide the **Alert Policy Name**.
   - Select **Sites**.
4. Select **Next**.
5. Select an **Alert Rule** and optionally edit, enable, or disable the rule parameters.
6. Select **Apply Rules**.
7. To edit or delete the site policy, from the 3-dot menu, select **Edit** or **Delete**.

Network Devices

Network Devices is a centralized location for monitoring both wired and wireless network devices. It provides detailed insights into the performance, health, and usage of each device, helping you maintain optimal network functionality. From here, you can:

- Device Status: Check if devices are connected, disconnected, or encountering problems.
- Device Health: Evaluate performance metrics such as CPU Usage, Memory Usage, and PoE Usage.
- Usage & Capacity: Understand bandwidth consumption, data transfer rates, and storage utilization.
- **Sites**: If you have access to multiple sites, select **Sites** to filter the network devices associated with a specific site.
- Onboard: Devices can be onboarded to the network using a manual or bulk onboard method.
- Upgrade Firmware: Manually upgrade firmware for selected devices.
- **Firmware Upgrade History**: 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**.

- **Download XLSX Template**: Select ⋮ to download device list data to an XLSX spreadsheet.
- **Update Device Data**: Select ↻ to refresh and update device data.
- **Download**: Select ⬇ to download the table data as a CSV file.

Device Status

The **Monitoring** > **Network Devices** > **Device Status** window provides resources to facilitate device management. These resources include:

- **Device Status Indicators**: Under the **Status** column in the device list, icons appear that are designed to provide useful device status information. Multiple status icons can be associated with a device. Hover over any icon to view a label indicating what the icon represents. For a description of each icon that can appear in the device list, see Device Status Icons.
- **All**: Displays all devices.
- **Wired**: Displays only wired devices.
- **Wireless**: Displays only wireless devices.
- **Device Management**: Select at the end of a row in the device list to perform actions on a device.

> **Note**
> To perform actions on multiple devices, select the devices to configure, and then select **Actions**.

> **Note**
> To download the table data as a CSV file, select .

Wired

Select **Wired** to filter a list of wired devices.

The Wired table displays the following information:

- Status
- Clients **
- Cloud Config Group **
- Network Policy Template **
- Device *
- Location
- Uptime
- MAC Address *
- Serial Number
- Management IP
- Default Gateway
- FW Upgrade On
- Operating System
- Firmware
- Model
- Network Policy
- IPv6

***** Select to view additional details.

****** Select **Show Additional Data** to view.

Wireless

Select **Wireless** to filter a list of wireless devices.

The Wireless table displays the following information:

- Status
- Clients **
- Cloud Config Group **
- Network Policy Template **
- Device *
- Location
- Uptime
- MAC *
- Serial Number
- Management IP
- Default Gateway
- FW Upgrade On
- Operating System
- Firmware
- Model
- Network Policy
- IPv6
- Country Code
- Managed By
- Wi-Fi 0 **
  - Channel
  - Power
  - Radio
- Wi-Fi 1 **
  - Channel
  - Power
  - Radio
- Wi-Fi 2 **
  - Channel
  - Power
  - Radio

***** Select to view additional details.

****** Select **Show Additional Data** to view.

Device Management Overview

From the **Monitoring** > **Network Devices** > **Device Status** > **3-dot Menu** (⋮), you can perform a number of actions on a device. The available actions depend on the device type selected.

Note

- Not all actions are available for all device types. Most device options are unavailable for an unmanaged device. To change the management status of your device, select **Change Management Status** > **Manage**.
- To perform actions on multiple devices, select the devices to configure, and then select **Actions**.

.

- **Advanced**:
  - **Change Device Mode**: Change the device mode from AP device to Router.

    Note

    - To configure an AP device as a router, the associated network policy must have both wireless and routing activated.
    - The following features are not supported: SDWAN, URL filtering, USB modem, private client group, and client mode.
    - The device must complete a full configuration update for the mode change to take effect.

  - **Advanced** > **Change OS to WiNG**: Change the operating system of the selected devices to WiNG.

    Important
    Changing the OS reboots the device and permanently erases the existing configuration. The new OS reverts to factory default settings.

  - **Advanced** > **SSH Access**: Select an available runtime to temporarily access your network remotely to troubleshoot the selected device. Select **Start** to begin an SSH session.

    Note
    SSH must be enabled to run an SSH session on the selected device. For more information, see Configure SSH on page 90.

  - **Thread Commissioner** (AP5010/AP5020 only): Enter a runtime to temporarily access your network remotely, and then select **Start**. The Thread Commissioner securely screens endpoint devices attempting to join the Thread network. To

define the behavior of the Thread Commissioner, see Configure the Thread Commissioner on page 262.

Note
If another AP is already running as the Commissioner on this Thread network, a warning message displays prompting the user to stop the current Commissioner or wait for it to automatically shutdown. If Thread is not enabled on the AP, or if configuration changes have not been deployed, the operation fails and a related error message displays.

- **Assign Country Code**: Select a country code for a managed device from the drop-down list. The country code defines the device radio channels and power limitations for the country in which the device operates. For devices used in the United States, the region code is reset to **FCC** and the country code is preset to **United States**. Select **Save** to reboot the selected devices.
- **Assign to Cloud Config Group**: Add the selected devices to an existing **Cloud Config Group** (CCG). In the **Assign to a Cloud Config Group** panel, select a CCG to assign to the selected devices, and then select **Assign**. To create a new CCG, see Add a Cloud Config Group on page 291.
- **Assign Location**: Assign a location to the selected devices.
- **Assign Network Policy**: Assign an existing network policy to the device.

  Note
  This action replaces existing associated policies with the newly selected policy.

- **Change Management Status**: Indicates the management status of the selected devices. Select **Manage** or **Unmanage**.

  Note
  The **Change Management Status** menu option is now available for Site Engine and devices managed by Site Engine. If Site Engine status is **Unmanaged**, the status for both Site Engine and devices managed by Site Engine is **Unmanaged**.

- **Clear Audit Mismatch**: Occasionally, there can be a mismatch between the configuration database and the device-level configuration database. If this occurs, perform this action.
- **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. For wireless devices, see Configure Wireless Devices.
- **Delete**: Delete the selected device from the network.
- **Locate Device**: Trigger a visual cue to quickly identify the exact position of a selected device. For more information, see Locate Device on page 65.
- **Reboot**: Reboot devices after uploading a configuration. Rebooting momentarily disconnects any associated clients from the SSID, which could be disruptive.

- **Reset to Default**: Reset the device to factory defaults.

  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.

- **Revert Device to Template**: Select to return the device settings to the network policy template. This removes any device-level configuration settings.
- **Update Devices**: Update network policy and configuration for the selected devices. Select any of the following options, and then select **Update**:
  - Reboot & revert Extreme Networks switch configuration if IQ Agent is unresponsive after configuration update.
  - Perform delta configuration update and resolve local device configuration which is out of sync.
  - Save as default.
- **Upgrade Firmware**: Manually upgrade firmware for a selected device. For more information, see Upgrade Firmware Settings on page 67.
- **Utilities**:
  - **Diagnostics**: Select a diagnostic method to run CLI commands on the device for basic network connectivity checks, status monitoring, and function diagnostics. For a full list of CLI commands, see Diagnostics CLI Commands on page 68.
  - **Initiate RADIUS Test**: Send a RADIUS request from the device to an authentication or accounting server. For more information, see Perform a RADIUS Test on page 66.
  - **Spectrum Intelligence**:
  - **VLAN Probe**: Locates available VLANs for the selected device. When the VLAN probe completes, a table displays the client name, MAC address, available VLANs, unavailable VLANs, and their status. For more information, see VLAN Probe on page 112.

NEW! 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 23.

Table 23: 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**.

NEW! Perform a RADIUS Test

The RADIUS Test tool tests network connectivity between a device acting as a RADIUS authenticator (RADIUS client) and RADIUS authentication server, which can be an Extreme Networks RADIUS server, or an external RADIUS authentication or accounting server.

Use this task to test the connectivity between a RADIUS authenticator and a RADIUS server.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select ⋮ at the end of a connected device row, and then select **Utilities** > **Initiate RADIUS Test**.
3. Select a **RADIUS Client** from the drop-down list.
   This is the device from which the **RADIUS Access-Request** or **Accounting-Request** message is sent.
4. Select the type of RADIUS server that you want to test.
   - To test connectivity to an Extreme Networks RADIUS server, choose **Local Server**, and then select a server from the drop-down list.
   - To test connectivity to an external RADIUS authentication or accounting server, select **External Server**, and enter the IP address of the server.

5. Select either **RADIUS Authentication Server** or **RADIUS Accounting Server**.

   If you select an authentication server, you must also enter supplicant credentials (a user name or barcode, and a password or PIN) for a valid user account on the RADIUS authentication server. You can also enter a user name and password that do not match an account on the RADIUS server.
6. Select **Test**.

Results appear under **Test Result**. A successful test result is shown below.

```
RADIUS server is reachable. Get attributes from RADIUS server: User-Group-ID:0=13; VLAN-ID:1=1; Session-Timeout=1800
```

Upgrade Firmware Settings

Table 24: Upgrade Firmware Settings

Field	Description
Upgrade IQ Engine and Extreme Networks Switch Engines	
Upgrade to the latest version	Upgrade to the latest firmware version.
Upgrade to a specific version	Select a **Model** to upgrade, and then select the **Version** to upgrade. To add a new version (local image), select **Local Image Management**: • To add a new local image, select +, and then select **Choose** to upload an image file from your computer. **Note:** The format for an image file name must be *.stk, *.xos, *.voss *.tgz, *.img, or *.img.S. The file name cannot contain spaces and must not exceed 64 characters. • Select **Close**. Select **View Release Notes** to access the Online Help system and see the latest release notes.
(Optional) Upgrade even if the versions are the same	Enforce an upgrade to the same version as the current version.
(Optional) Enable distributed image upgrade (APs only)	Designate the AP as the server to download the firmware image. This AP then distributes the firmware to other APs in the network.
Activation Time for Extreme Networks Device Running Images	
Activate at next reboot (required manual reboot)	Activation takes affect the next time the device reboots.
Activate after xx seconds	The delay before activation, in seconds.

NEW! 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 25 on page 68, 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 25: 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 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.
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.

Table 25: CLI Commands (continued)

CLI Command	Description
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.

Configure Wired Devices

After you select ⋮ at the end of a wired device row, and then select **Configure** > **Device**, you can create or modify the following:

- 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.
- Switch Port 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 Override Supplemental CLI on page 91.

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 93.

Related Links

Device Management Servers on page 71
Configure Wired Devices on page 69

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.

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.

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**.

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, then select **SAVE CONFIGURATION**.

   The changes only apply at the device level. for more information about management server configuration.

   For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 93.

Related Links

Configure Switch Ports and VLAN on page 72
Configure Wired Devices on page 69

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. Select ⋮ at the end of a device row, and then select **Configure** > **Device**.
3. Under the **Configuration** menu, select **Port / VLAN Configuration**.
4. Select **Unlock** to enable switch-level configuration changes.
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.

   For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 93.
7. To revert back to the network policy switch template, select **Revert to Network Policy**.

Related Links

Configure Wired Device Credentials on page 73
Configure Wired Devices on page 69

Configure Wired Device Credentials

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 93.

Related Links

Configure Wired Devices on page 69

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 26: 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 93.

Related Links

Routing Configuration on page 74
Configure Wired Devices on page 69

Routing Configuration

The device must have an IPv4 interface configured. For more information, see Interface Configuration on page 73.

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 27.

Table 27: 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 93.

Related Links

Configure Wired Devices on page 69

Configure Wireless Devices

After you select a **Wireless** from the Device List, you can create or modify the following:

- Wireless Device Configuration: Edit device details such as the host name, the description, the device function, IP addresses, and VLAN assignments.
- Wireless Interface Settings: View the default template settings and control actions for the Wireless (Wi-Fi) and Wired (Ethernet) ports. You can edit any field that is selectable.
- Wireless Device Credentials: Assign or change network administrator credentials and administrator assignments, and configure CAPWAP and Shared Key settings.
- Configure Netdump: Enable an unresponsive AP to automatically save a core dump file to a TFTP server on the network the next time it boots.
- DHCP Server and Relay: For a small network, configure and enable a DHCP server on a device to provide network settings dynamically to clients.
- Neighboring Devices: Define a list of neighbor access points that will collaborate in the Layer 3 roam process.

- Bonjour Gateway Settings: Choose the AP you want to act as your Bonjour Gateway Designated Device (BDD) at the device level.
- Troubleshooting: Enable Client Monitor so devices can detect client issues, and report client connection activities and problems to ExtremeCloud IQ (New).

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

Wireless Device Configuration

It is a best practice to configure devices using a device template. However, you can override the device template settings for a specific device.

Use this task to configure the settings for a specific wireless 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 **Configuration** menu, select **Device Configuration**.
4. Configure **Device Details** settings in Table 28.

Table 28: Device Details Settings

Field	Description
Host Name	Type a unique host name for the device. It can contain up to 32 characters and can include spaces.
Description	Optional description for the device.
Mgt0 MAC Address	This is the Node ID and is listed on the printed label located on each device.
Device Model	The hardware model of the configured device.
Device Function	This describes the main function of the device. For example, AP.
IQ Engine	Lists the IQ Engine firmware version currently installed on the AP.
SNMP Location	The SNMP location name, for example `headquarters, building 1`.

5. Configure **Network Details** settings:
   - **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.

6. Configure **Management Interface (Mgt0)** settings:
   a. Select **Static Address** to enter a static address for this interface, and then configure the settings in Table 29.

Table 29: Static Address Settings

Field	Description
IPv4 Address	The IPv4 address you want the device to use for the mgt0 interface.
Subnet Mask	The appropriate netmask for the subnet to which the mgt0 interface connects.
Default Gateway	The address through which the device (and its connected hosts) can reach the Internet.

   b. Select **Dynamic Address Configuration (DHCP) Client** to have an address automatically assigned by DHCP, and then configure the settings in Table 30.

Table 30: Dynamic Address Configuration (DHCP) Settings

Field	Decription
Use DHCP only to set IP Address (IPv4 only)	Enable or disable this function.
Advanced DHCP Options (IPv4 only)	Select to display or hide this section. Configure the following settings: • **DHCP Timeout**: Enter the amount of time (in seconds) that the device waits for a response from the DHCP server before assigning itself a static IP address. By default, the timeout for reverting to a static address is 20 seconds. You can change the timeout from 0 to 3600 seconds (1 hour). A timeout of 0 means that the device continues trying to obtain network settings through DHCP indefinitely. • **Automatically Generate Interface IP Settings**: ◦ **IP Prefix**: The Extreme Networks device automatically switches to this IP address if it cannot obtain settings through DHCP. You can also enter an IPv6 address. ◦ **Subnet Mask**: Enter the netmask for the subnet to which the mgt0 interface connects. • **Static Fallback IP Settings**: ◦ **Static IP Address**: Enter the IP address you want the device to use if it cannot contact the DHCP server. You can also enter an IPv6 address. ◦ **Subnet Mask**: Enter the appropriate netmask for the subnet to which the mgt0 interface connects. ◦ **Default Gateway**: The address through which the device (and its connected hosts) can reach the Internet.

   c. Enter the **Management VLAN** for this interface.
   d. Enter the **Native VLAN** for this interface.
   e. Select **Override MGT0 MTU** to manually enter an MTU, ranging from 100-1500 Bytes (the default value is 1500 Bytes).

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 Override Supplemental CLI on page 91.

   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 **Override Disable WebUI in the network policy** to disable the local web user interface on an IQ Engine device to improve system security, without disabling the associated captive web portal.

   If you configured **WebUI** in the network policy, you can disable it for this device here.
9. For **Deployment Mode**, select **Pre-Provisioned** or **Production** to indicate whether the device has been pre-provisioned.
10. (AP5010 only) Enable **POE Profile Override**, select the override option from the dropdown, and hover over the **i** icon to view the corresponding override table.
11. Select **Save Device Configuration**.

    For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 93.

Related Links

Wireless Interface Settings on page 78
Configure Wireless Devices on page 75

Wireless Interface Settings

Use this task to view **Device Template Default Settings** and control actions for Wireless (Wi-Fi) and Wired (Ethernet) ports.

Note
Changes made here are at the device level, which overrides the network policy template for the device only. The Network Policy remains unchanged.

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 **Interface Settings**.
4. For **Wireless Interfaces**, select either the **WiFi0**, **WiFi1**, **WiFi2**, **BLE**, or **IoT0** tab.

   Note
   The **IoT0** tab is supported on AP5010/AP5020 models.

5. To configure **WiFi0**, **WiFi1**, **WiFi2**, or **IoT0**, see Wi-Fi Settings on page 79.
6. To configure **BLE**, go to **Configuration** > **Network** > **Network Policy** > **Wireless** > **Application Management** > **BLE Service**.
7. For **Wired Interfaces**, see Configure Wired Interfaces Settings on page 81.

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

8. To configure **Electronic Shelf Label**, toggle **Enable ESL** to **ON**, and then Configure Electronic Shelf Label Settings.
9. Select **Save Interface Settings**.

   For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 93.

Related Links

Configure Wireless Device Credentials on page 82
Configure Wireless Devices on page 75

Wi-Fi Settings

Table 31: Radio Status Settings

Field	Description
Radio Status	Set to **On**.
Radio Profile—or IoT Profile, if applicable	Select a profile from the drop-down list. You can also add a new Radio Profile or IoT Profile here, or clone and modify an existing profile. **Note:** Only the AP510C, AP510CX, AP550, AP650, AP650X, AP305C, AP305CX, AP302W, AP4000, AP5010, AP3000/X, AP410C, AP460C, AP460S6C, and AP460S12C models support MU-MIMO on its Wi-Fi0 interface.
Radio Usage	Select the usage type: • **Client Mode**: Select to configure a device for AP client mode radio usage, and to configure advanced features such as **Port Forwarding Rules** and **DHCP Server** settings. Select a **Client Mode Profile**. If required, you can configure a new Client Mode Profile, or edit an existing profile. • **Client Access**: Select for normal client operation. • **Backhaul Mesh Link**: Select for wireless portal and mesh backhaul operation. • **Sensor**: Select for presence operation.
Enable SDR (Software Defined Radio)	Enable and then select an **SDR Profile** from the drop-down list. You can also add a new profile here or modify an existing profile.
Channel	Select a channel. If you select **Auto**, ExtremeCloud IQ (New) selects the channel for you.

Table 31: Radio Status Settings (continued)

Field	Description
Override channel exclusion setting in radio profile	Enable, and then select activated channels to manually exclude them from the radio profile.
Transmission Power	Activate to manually set the transmission power. Select **Manual**, and then use the slider to select a dBm setting.
Enable client transmission power control (802.11h)	Activate to manually enable client transmission power control (802.11h). Select **Manual** and use the slider to select a dBm setting.

Table 32: Enable Presence Analytics Settings

Field	Description
Enable Presence Analytics	Toggle to **On** to modify device presence analytics settings.
Name	Automatically populates with the name of the Network Policy.
Trap Interval	The interval (in seconds) that the presence sensor reports data to ExtremeCloud IQ (New).
Aggregate Time	The interval (in seconds) for the period during which aggregation occurs for the presence profile.
Aging Time	The aging time (in seconds) for a given presence profile.

Table 33: SSID Settings

Field	Description
SSID Name (Policy)	The current SSID name.
Status	Toggle the SSID status to **On** or **Off**.
Override SSID Broadcast Name	Change the SSID broadcast name for the device.
Override PSK Password	Change the PSK password for the device.
Reassign CWP	Select a new CWP from the drop-down list.
	Hover and select **Revert** to revert device-specific SSID settings to their default values.

Related Links

Wireless Interface Settings on page 78

Configure Wired Interfaces Settings

Table 34: Wired Interfaces Settings

Field	Description
Interface	The software representation of the physical port.
State	Indicates if the port is enabled or disabled.
Port Type	The interface port type. This field is read only.
Native VLAN	The native (untagged) VLAN assigned to frames that do not have any 802.1Q VLAN tags in their headers.
Allowed VLANs	The VLANs, including the native VLAN, that you want the trunk port to permit. You can list the VLANs individually, separated by commas, or as a range of VLANs using a hyphen. Alternatively, you can enter the word **all** in this field to support all existing VLANs previously configured in the network policy (the default).
Fabric Attach	1. Select , and then enter a **Name** and **Description** for the Fabric Attach. 2. For each VLAN, select , and then enter the device's associated **VLAN ID** and **I-SID**. 3. Select a VLAN from the list, and then select to remove the VLAN from the Fabric Attach. 4. Select **Save**.
Transmission Type	Select one of the following options: • **Auto**: The switch negotiates the best common duplex mode 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.
Speed	The speed the Ethernet port uses to communicate with the connected device.
Green Ethernet (AP4020 and AP5020 Only)	Select for AP5020 devices to allow physical layer transmitters to consume less power when they are in a state of idleness or low data activity.
LLDP	Select for devices to advertise identities, status, and capabilities to each other. Devices can transmit data about themselves and receive transmitted data from other devices, but they cannot solicit and retrieve data from other devices.
CDP	Select for devices to advertise an IP address that can send and receive SNMP traps.

Table 34: Wired Interfaces Settings (continued)

Field	Description
MCast Filter	Select to enable Multicast Rate Limiting on the interface for multicast/ broadcast traffic.
Multicast Rate Limit	Set the maximum rate (in Kbs) for incoming multicast traffic for the interface.

Related Links

Wireless Interface Settings on page 78

Configure Electronic Shelf Label Settings

Table 35: Electronic Shelf Label Settings

Field	Description
Server	The name of the server that manages Electronic Shelf Label (ESL) communication and data updates.
State	The current operational status of the ELS device.
Port Type	The network port type used for communication.
Native VLAN	The assigned VLAN ID.

Related Links

Wireless Interface Settings on page 78

Configure Wireless Device Credentials

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 an AP. Device-level credentials offer access to APs through Telnet, SSH, or console connections.

Note
At this level, you are making changes to the selected AP only. These changes always override the network policy configurations.

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.

Use this task to configure wireless device credentials.

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. Configure the **Primary CAPWAP Server** and **Secondary CAPWAP Server** connections.

   You can select an existing CAPWAP server from the drop-down list, or select the add icon to define a new server.
7. Configure a **Shared Key for Authentication Passphrase**.
8. Select **Save Device Credentials**.

   For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 93.

Related Links

Configure Netdump on page 83
Configure Wireless Devices on page 75

Configure Netdump

You must perform a full configuration update for each device on which you want to enable netdump.

If an AP or switch becomes non-responsive, you can enable it to automatically save a core dump file to a TFTP server on the network the next time it boots. You can provide this file to Support to assist in diagnosing the issue. To configure a device to save a core dump file to a TFTP server, complete the following 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 **Configure Netdump**.
4. Select the check box to **Enable Netdump**.
5. Configure the **Update Settings** in Table 36.

Table 36: Netdump Update Settings

Field	Description
TFTP server for saving netdump files	The IP address of the TFTP server where you want the device to send the core file.
Netdump filename to save	The name of the netdump file.
VLAN for reaching the TFTP server	The VLAN of the interface the device will use to send the netdump file to the TFTP server.
Native VLAN of the local Extreme Networks device	The native VLAN of the device.

6. Select **DHCP** to have the device bootloader use DHCP to obtain an IP address at startup.

7. Select **Static** to use a static IP and configure the network settings in Table 37 that the bootloader must use to connect to the network:

Table 37: Update Static IP Settings

Field	Description
Address of local Extreme Networks device	The IP address of the reporting device.
Netmask of local Extreme Networks device	The netmask for the reporting device.
Gateway for reaching the TFTP server	The IP address of the TFTP server.

8. Select **SAVE NETDUMP CONFIGURATION**.

   For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 93.

The device will send a core dump file to the TFTP server the next time it reboots.

Related Links

Configure DHCP Server and Relay Settings on page 84
Configure Wireless Devices on page 75

Configure DHCP Server and Relay Settings

For small networks that do not already have a DHCP server, you can configure and enable a DHCP server on an Extreme Networks device to provide network settings dynamically to clients. After you configure one hive member as a DHCP server, the other hive members forward the DHCPDISCOVERY and DHCPREQUEST messages to their neighbors. The device you use as the DHCP server must be a portal.

When all hive members are in the same subnet and all devices in that subnet are on a single VLAN, you only need to configure the DHCP server device with a pool of IP addresses it can draw from when responding to DHCP client requests. When some hive members are in a different subnet from the DHCP server, you must also configure those devices to forward DHCP traffic to the IP address of the DHCP server. In this case, the other devices act as DHCP relay agents.

Use this task to configure both DHCP servers and relay agents.

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 **Additional Settings** menu, select **DHCP Server and Relay**.
4. Select ✚ to add or ✎ to edit, and then configure the settings in Table 38.

Table 38: DHCP Server and Relay Settings

Field	Description
Name	A unique identifier for the DHCP configuration profile.
Description	A brief summary for the configuration profile.

Table 38: DHCP Server and Relay Settings (continued)

Field	Description
Platform Supported	The device models or operating systems the configuration is compatible with.
Interface	The network interface through which DHCP services are provided or relayed.
Service	Defines whether the device acts as a DHCP Server or Relay Agent. The DHCP relay enhancement supports deployments when a centralized DHCP server (for example, at corporate headquarters) is used. When you enable DHCP Relay, the DHCP server feature on devices is disabled so that routers redirect DHCP service requests to the centralized DHCP server

5. Enable or disable **Set the DHCP server as authoritative**.

   If this DHCP server is the only one on your network, it contains a record of the valid IP numbers on the network. If a client tries to register with an invalid IP address (for example, if a client device still has an active lease with another network), an authoritative DHCP server denies access to that client.
6. Enable **Use ARP to check for IP address conflicts** when this DHCP server uses ARP to check for IP address conflicts on the network before assigning an IP address to a DHCP client.
7. Select **Enable NAT Support** if this DHCP server uses NAT.
8. For **IP Pool**, define the IP address pool from which the DHCP server draws IP addresses when making assignments.
   a. Select to add a new IP pool.
   b. Enter the **Start IP Address** and **End IP Address**.
   c. Select **Add**.
9. For **IP Binding**
   a. Select to add a new IP Binding.
   b. Enter the**IP Address** and **MAC Address**.
   c. Select **Add**.
10. To configure each of the required parameters that the DHCP server returns to clients along with an IP address, configure the DHCP Server Options Settings on page 86.
11. To define custom DHCP options to provide additional network settings to connected clients, see Configure Custom DHCP Options on page 86.
12. Select **Save**.

    For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 93.

Related Links

Configure Neighboring Devices on page 87
Configure Wireless Devices on page 75

DHCP Server Options Settings

Table 39: DHCP Server Options Settings

Field	Description
Default Gateway	The IP address of the default gateway for the subnet to which the address in the IP pool belong.
DNS Server1 IP	The primary DNS server IP address for the clients to contact when resolving domain names to IP addresses.
DNS Server2 IP	The secondary DNS server IP address for clients to contact when resolving domain names to IP addresses.
DNS Server3 IP	The tertiary IP address for clients to contact when resolving domain names to IP addresses.
POP3 Server IP	The POP3 server IP address.
SMTP Server IP	The SMTP server IP address.
WINS Server1 IP	The primary WINS server IP address.
WINS Server2 IP	The secondary WINS server IP address
Lease Time	The length of time for the DHCP lease to last.
Netmask	The subnet to which the addresses in the IP pool belong.
Domain Name	The DNS name resolution domain name to assign to DHCP clients.
MTU	The path MTU aging timeout in seconds.
NTP Server1 IP	The primary NTP server IP address for DHCP client clock synchronization.
NTP Server2 IP	The secondary NTP server IP address for DHCP client clock synchronization.
Log Server IP	The log server IP address for DHCP clients.

Related Links

Configure DHCP Server and Relay Settings on page 84

Configure Custom DHCP Options

Create or modify **DHCP Server and Relay settings**.

Use this task to define custom DHCP options to provide additional network settings to connected clients.

1. Select .
2. Enter a custom **Number** from 2 to 5, 8 to 14, 16 to 25, 27 to 41, 43, 45 to 50, 52 to 57, 60 to 68, 71 to 224, 227, 228, or 232 to 254.

3. Select the **Type** of data that the option provides:
   - **Integer**: (0-2,147,483,547)
   - **IP Address**: (Four octets for an IP address or eight groups of two octets each for an IPv6 address.)
   - **String**: (1-255 characters)
   - **Hex**: (1-254 hexadecimal digits)
4. Enter the **Value** for the data.
5. Select **Add**.

Related Links

Configure DHCP Server and Relay Settings on page 84

Configure Neighboring Devices

Roaming Threshold helps control the number of tunnels an AP can accept during layer 3 roaming operations.

Manually add a **Neighbor** to define a Hive neighbor in the case where the APs cannot hear over the air and they are in different management subnets (which is how they ordinarily learn of each other.) Bonjour Gateway piggybacks on this functionality to learn of APs in other management subnets that cannot be heard over the air.

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 **Additional Settings** menu, select **Neighboring Devices**.
4. Select a **Roaming Threshold** value from the drop-down list to set the volume of traffic that the selected neighbors will accept through GRE (Generic Routing Encapsulation) tunnels to support Layer 3 roaming.

   This option gives hive members the ability to push tunnels to other members for better tunnel load balancing. For example, if one AP near an entrance gets overloaded with tunnels, you can lower its threshold to medium or low so that more tunnels terminate on other APs.

   Note
   This setting only takes effect when the APs function as portals and Layer 3 roaming is enabled.

5. Select to manually add a Layer 3 roaming or Bonjour gateway neighboring Extreme Networks device.
6. Select an **Available Neighbor** device from the drop-down list and select **Add**.

   Note
   You can add any or all of the Layer 3 roaming and Bonjour gateway neighboring Extreme Networks devices by repeating the previous two steps.

7. To remove a manually configured neighboring device, select a device, and then select .

8. Select **Save Neighboring Devices**.

   For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 93.

Related Links

Configure Bonjour Gateway Settings on page 88
Configure Wireless Devices on page 75

Configure Bonjour Gateway Settings

Define Bonjour Gateway settings in the network policy.

Use this task to choose the wireless device you want to act as your Bonjour Gateway Designated Device (BDD) at the device level. If possible, use the newest model device you have in a low traffic area.

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 **Additional Settings** menu, select **Bonjour Gateway Settings**.
4. Set the **Priority** for the wireless device you want to use as your BDD to around 250.

   By default, every AP is set an automatic priority level (10-20) for the Bonjour service. The AP with the highest priority setting acts as the Bonjour Gateway. The MAC address is used if the priority is the same on all APs.
5. To modify the realm name, select **Override the default real name** and set the **Realm Name**.

   Note
   A realm name is automatically generated by placing this device on a map (the auto-generated name is the building name). Modifying the realm name here overwrites the auto-generated realm name.

6. Select **Save Bonjour Gateway Settings**.

   For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 93.

Push a complete configuration to the BDD, followed by a **Delta** update to all other APs.

Related Links

Troubleshooting on page 88
Configure Wireless Devices on page 75

Troubleshooting

Use this task to enable Client Monitor so devices can detect client issues, and report client connection activities and problems to ExtremeCloud IQ (New).

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 **Additional Settings** menu, select **Troubleshooting**.
4. Toggle **Enable Client Monitor** to **On**.

5. Select to configure a new Client Monitor Policy, see Client Monitor Profile Settings on page 89, and then click **Save**.

   Note
   Select the client monitor profile name to edit the profile.

6. Select to select an existing client monitor policy.
7. Select **X** to use the SSID client monitor policy.
8. For wireless devices that support Dynamic Packet Capture, toggle **Enable Packet Capture** to **On**.

   Note
   If the AP model supports Dynamic Packet Capture, a small packet capture of the event is appended to the client monitor record. Dynamic Packet Capture is supported on the following models:
   - AP3000, AP3000X, or AP5010 running 10.6.7 or higher
   - AP5020 running 10.7.1 or higher
   - AP4020 running 10.8.1 or higher

9. Select **Save Troubleshooting**.

   For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 93.

Related Links

Configure SSH on page 90
Configure Wireless Devices on page 75

Client Monitor Profile Settings

Table 40: Client Monitor Profile Settings

Field	Description
Name	Type a name to identify the Client Monitor Profile policy.
Association Problem	
Trigger Times	Set the number of times an association problem can be triggered, between 1 and 10.
Report Interval	Set the interval between reporting an association problem, between 30 and 3600 seconds.
Authentication Problem	
Trigger Times	Set the number of times an authentication problem can be triggered, between 1 and 10.
Report Interval	Set the interval between reporting an authentication problem, between 30 and 3600 seconds.
Networking Problem	

Table 40: Client Monitor Profile Settings (continued)

Field	Description
Trigger Times	Set the number of times a network problem can be triggered, between 1 and 10.
Report Interval	Set the interval between reporting a network problem, between 30 and 3600 seconds.

Related Links

Troubleshooting on page 88

Configure SSH

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

ExtremeCloud IQ (New) 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 enable SSH on a wireless 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 **Additional Settings** menu, 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.

Related Links

Configure Wireless Devices on page 75

Override Supplemental CLI

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**.

You can save supplemental CLI objects that contain CLI commands and then automatically update devices each time you update the network policy. On the **Device** page, you can keep the supplemental CLI object in the network policy and append another supplemental CLI object to the end of the running configuration list. If the supplemental CLI is appended to the delta configuration and the supplemental CLI portion fails device update, only the supplemental CLI regenerates for subsequent device updates.

If you use CLI to manage features that are not configured in the user interface, you can choose to override the user interface (or to override the CLI), benefiting deployments that rely on overly complex CLI objects.

Use this task to override supplement CLI from network policy supplement CLI.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select at the end of a device row, and then select **Configure** > **Device**.
3. Select **Override Supplement CLI from network policy Supplement CLI**.
4. Select an existing supplemental CLI object, or select to add, or to edit a supplemental CLI object. For more information, see Add a Supplemental CLI Object on page 91.
5. Select **Save Configuration**.

   For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 93.

   Note
   To avoid an unnecessary system reboot, select **Delta Configuration Update**. ExtremeCloud IQ (New) 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`**.

Related Links

Add a Supplemental CLI Object on page 91

Add a Supplemental CLI Object

Before you can use the supplemental CLI tool, you must first enable Supplemental CLI. Go to **Administration & Settings** > **Backup & Restore**, and then enable **Supplemental CLI**.

You can save supplemental CLI objects containing CLI commands, and ExtremeCloud IQ (New) can then automatically update them for devices, each time you update the network policy.

Note

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

Use the following task to create CLI objects.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select at the end of a device row, and then select **Configure** > **Device**.
3. Go to **Configure** > **Common Objects** > **Basic** > **Supplemental CLI Objects**.
4. Select **Override Supplement CLI from network policy Supplement CLI**.
5. To add a new supplemental CLI object, or select to add, or to edit.
6. Enter a **Name** and an optional **Description**.
7. Enter the CLI commands.
   - Enter multiple CLI commands, one command per line, not exceeding a maximum total of 8192 characters. Limit CLI commands to configuration commands. Exclude Show or other commands used to display information.
   - You can use CLI commands that contain IP and VLAN objects: **`${ip:ip_object_name}`** and **`${vlan:vlan_object_name}`**.
   - You must perform a complete configuration update each time commands are appended to device configurations.
   - If supplemental CLI is added to device-level configuration, then device-level supplemental CLI takes precedence.
8. Select **SAVE** and perform a configuration update each time you append commands to device configurations.

   Note
   To avoid an unnecessary system reboot, select **Delta Configuration Update**. ExtremeCloud IQ (New) 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`**.

Related Links

Override Supplemental CLI on page 91

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 41: 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 ExtremeCloud IQ (New).

Table 42: 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 ExtremeCloud IQ (New) 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.

Device Status Icons

Table 43: 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**.
	Anchor AP	Device is set as an anchor.
	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.
	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.

Table 43: Device Status Icons (continued)

Icon	Icon Name	Description
	Configuration Audit Mismatch	The network policy configuration does not match the current running configuration. Cause: The Configuration Audit Mismatch icon is visible on devices between the time that network policy changes are saved and the time that the altered network policy is uploaded to the device. Action: Upload the network policy to the device. 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.
	Configuration Rollback	Device could not establish a connection to ExtremeCloud IQ after the configuration update. Device configuration rolled back to the last known good connection and the **Updated** status column displays `Device update failed`.
	Connected Device	Device is actively communicating with ExtremeCloud IQ (New).
	Device Update Unsuccessful	Device did not accept the OS or configuration upload. Cause: There are many reasons for an unsuccessful update, but the most common include network connectivity or connection status changes, or the device rejected the command it received. Action: Hover over the update message in the Updated column to view the reason message describing the likely error condition. Ensure that the device is properly powered, that there is appropriate network connectivity, and that common causes listed here are not the issue.

Table 43: Device Status Icons (continued)

Icon	Icon Name	Description
	Digital Twin	Device is a simulated device.
	Disconnected Device	Device is not actively communicating with ExtremeCloud IQ (New). Cause: The device might be physically disconnected from the network or powered off. This condition also occurs if there are interruptions in the network between the device and ExtremeCloud IQ (New) 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.
	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.

Table 43: Device Status Icons (continued)

Icon	Icon Name	Description
	Locally Managed (No ExtremeCloud IQ)	Device or its management platform are not visible in ExtremeCloud IQ. Cause: This is not always an error condition, but it can indicate a status communication problem. In this case, the device is functioning properly, so there is no disruption in network performance; instead, the status communication is disrupted so that ExtremeCloud IQ is unaware of the status. Action: First, ensure that the device is functioning properly to rule out problems with the device. Next, ensure that there are no logical barriers between the device and ExtremeCloud IQ. Afterward, ensure that any applications that lie in the communication path are receiving, processing, and sending data appropriately.
	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 ExtremeCloud IQ (New). 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.
	RadSec Proxy Server	Device is acting as a RadSec proxy server. This service optimizes some authentication functions, especially for cloud authentication, such as cloud PPSK and cloud RADIUS.
	Rogue AP Mitigation	Device is actively mitigating a rogue access point. Refer to the information provided by your security management platform.
	Sensor Mode - Interface Active	Device is functioning as a sensor and the monitoring interface is active and monitoring the RF environment.
	Sensor Mode - Interface Inactive	Device is functioning as a sensor, but the monitoring interface is not active and is not monitoring the RF environment.

Table 43: Device Status Icons (continued)

Icon	Icon Name	Description
	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.
	Thread Commissioner Running	The AP is designated Commissioner in the IoT Thread network.
	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 43: 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 ExtremeCloud IQ (New). 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 ExtremeCloud IQ (New). 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 ExtremeCloud IQ (New). 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 43: 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 ExtremeCloud IQ (New). In addition, ensure that there is connectivity and communication between the VPN server and clients.

Device Health

Go to **Monitoring** > **Network Devices** > **Device Health**.

Note
To download the table data as a CSV file, select .

Wired

Select **Wired** to filter a list of wired devices.

When **Show Summary** is enabled, health widgets display CPU Usage Issues, Memory Usage Issues, PoE Usage Issues, Temperature Issues, Fan Issues, and Power Supply Issues.

The Wired table displays the following information:

- Device *
- Location
- CPU Usage %
- Memory Usage %
- PoE Usage %
- Temperature°C
- Fan Status *
- Power Supply *

***** Select to view additional details.

Wireless

Select **Wireless** to filter a list of wireless devices.

When **Show Summary** is enabled, health widgets display CPU Usage Issues, Memory Usage Issues, and PoE Usage Issues.

The Wireless table displays the following information:

- Device *
- Location
- CPU Usage %
- Memory Usage %
- PoE Usage
- Channel Change
- WiFi Reboots
- Unicast/Multicast/Broadcast
- Eth 0%
- Eth 1%

***** Select to view additional details.

Usage & Capacity

Go to **Monitoring** > **Network Devices** > **Usage & Capacity**.

Note
To download the table data as a CSV file, select .

Wired

Select **Wired** to filter a list of wired devices.

When **Show Summary** is enabled, usage and capacity widgets display Usage Utilization, Wired Throughput, and Wire Congestion.

The Wired table displays the following information:

- Device *
- Location
- Clients
- Total Bandwidth Utilized (Bytes)
- Total Throughput (Rx Packets per Second)
- Total Throughput (Tx Packets per Second)
- Total Unicast (Packets %)
- Total Multicast (Packets %)
- Total Broadcast (Packets %)
- Total Queue Congestion (# of Packets)

***** Select to view additional details.

Wireless

Select **Wireless** to filter a list of wireless devices.

When **Show Summary** is enabled, usage and capacity widgets display Excessive Channel Utilization, Excessive Retries, and Excessive Packet Loss.

The Wireless table displays the following information:

- Device *
- Location
- Clients
- MAC Address *
- Packet Loss %
- Channel Utilization %
- Retries
- Unicast/Multicast/Broadcast
- Noise (dBm)
- Interference %

***** Select to view additional details.

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 44.

Table 44: 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**.

Upgrade Network Device Firmware

Use this task to upgrade firmware for selected devices.

1. Select **Upgrade Firmware**.
2. Select a **Device Type** and **Device Management** (Cloud Managed is the default).

   Note
   You can filter the device list by using the **Search** field to quickly locate specific devices.

3. Select the devices for firmware upgrade, and then select **Next**.
4. Select a **Firmware Version** for each device, and then select **Next**.

   Note
   - Firmware upgrades are available only for connected and managed devices.
   - The **Vulnerabilities Fixed** column displays all fixed security vulnerabilities data associated with your selection.

5. Confirm the **Review Summary**, and then select a **Firmware Update 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.

6. 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**.

Device View

The device view provides a comprehensive overview of the selected device's specifications and current status.

Select a **Device** name from the table. The **Device Details** window displays detailed information for the Wired or Wireless device.

Select **Actions** to perform specific tasks on the selected device. For more information, see Device Actions Menu on page 116.

Wired Device View

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

- Connection Status
- Device Image
- Device Location
- VLAN Probe
- 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
- Overview
- Clients
- Port Stats
- Services/VLANs
- Routing
- Events
- Alerts on page 109

Note

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 **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, and PoE Usage.
- 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

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

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.

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:

- The **Events** table lists the following details:
  - Timestamp
  - Severity
  - Category
  - Description

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

NEW! 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).
- 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
  - Category
  - Source
  - Timestamp

Note
Select to export filtered alerts.

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

Wireless Device View

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

- Connection Status
- Device Image
- Floor Map (if available)
- Device Location
- Installation Reports
- Installation Media Gallery: Select to upload an image (.png or .jpg less than 500KB) or video (.mp4 or .mov less than 5MB) file.
- Actions on page 110
- Overview on page 113
- Wireless Interface on page 114
- Wired Interface on page 114
- Clients on page 114
- Events on page 115
- Alerts on page 115

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

Actions

From the **Actions** menu you can perform the following actions for the selected device:

- Reboot on page 110
- Reset Factory Settings on page 110
- Upgrade Firmware on page 111
- Locate on page 112
- VLAN Probe on page 112

Reboot

To restart a connected device, select **Reboot**, and then select **Yes** to confirm. Restarting momentarily disconnects any connected clients.

Note
The current configuration will not be saved before the reboot.

Reset Factory Settings

To reset the selected device to their default configuration, select **Reset Factory Settings**, and then 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

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

1. Select **Upgrade firmware**.
2. In the **Device Update** dialog box, select an upgrade type.

Table 45: Update AP Device Settings

Field	Description
Upgrade IQ Engine and Extreme Network Switch Images:	
Upgrade to the latest version	Upgrade to the latest firmware version.
Upgrade to the specific version	Select a **Model** to upgrade, and then select the **Version** to upgrade to from the drop-down list. To add a new version (local image), select **Add/ Remove**: • To add a new local image, select +, and then select **Choose** to upload an image file from your computer. **Note:** The format for an image file name must be *.stk, *.xos, *.voss *.tgz, *.img, or *.img.S. The file name cannot contain spaces and must not exceed 64 characters. • To delete an existing local image, select an image, and then select 🗑. • Select **Close**. Select **View Release Notes** to access the Online Help system and see the latest release notes.
(Optional) Upgrade even if the versions are the same	Enforce an upgrade to the same version as the current version.
(Optional) Enable distributed image upgrade (APs only)	Designate the AP as the server to download the firmware image. This AP then distributes the firmware to other APs in the network.
Activation Time for Extreme Networks Devices Running Images:	
Activate at next reboot (requires manual reboot)	Activation takes affect the next time the AP is rebooted.
Activate after xx seconds	The delay before activation, in seconds.

3. Confirm the **Review Summary**, and then 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**.

Locate

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

1. Select **Locate**, and then configure the **Locate Device** settings in Table 46.

Table 46: Locate Device Settings

Field	Description
LED Color	Select one of the following blinking light colors to set the color that the locator light will flash to help you find the AP: • Amber • White • Off
Blink Mode	Select one of the following blinking modes to set the speed at which the locator light will flash to help you find the AP: • Fast • Slow • Steady

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

2. Select **Submit**.

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 47.

Table 47: 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.

Overview

Overview displays the following information about the selected device:

- At the top of the page, the **Connection Chain** diagram shows how the device connects to the internet and to ExtremeCloud IQ (New).
- The following widgets appear below the connection chain diagram:
  - Device Health
  - Connectivity Issues
  - Excessive Packet Loss

  Note
  The selected time period applies to the widgets as well as the connection chain diagram.

- System Information for the selected device.

Wireless Interface

Wireless Interface provides the following information about the selected wireless device:

- An interactive timeline graph displaying channel utilization and connected clients. Select a **Radio** (Wi-Fi 0, Wi-Fi 1, or Wi-Fi 2) and **Filter by** Channel Utilization % and Connected Client.
- Summary information tables for **Wi-Fi 0**, **Wi-Fi 1**, and **Wi-Fi 2**.
- **Channel Utilization Interface** widgets.
- The **Surrounding Access Points** table provides details about surrounding APs.

Wired Interface

Wired Interface provides the following interface details about the selected wireless device:

- Status
- Interface
- Port
- Speed
- Tx Bytes
- Rx Bytes
- Tx Errors
- Rx Errors
- Tx Drops
- Rx Drops

Clients

Clients provides the following information about the selected wireless device:

- An interactive timeline graph shows the number of clients connected to the current device, for the specified time frame. By default, the data capture time frame is 24 hours.

  You can select any point along the timeline in the graphic to display details only for connected clients at 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.
- **Client Statics** displays the following widgets:
  - Total Clients within selected time range: Displays the number of clients.
  - Clients with poor health: Displays the number of clients.
  - Total Unique Clients: Displays
- A table lists the following details about the clients that are connected during the specified time range:
  - Connection Status
  - Client
  - Site
  - SNR
  - RSSI
  - Frequency
  - Channel Utilization %
  - Association Issues
  - Authentication Issues

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

NEW! Events

Events displays the following information about the selected device:

- An interactive timeline graph, from which you can:
  - View and filter **Critical**, **Major**, **Minor**, **info**, and **Clear**.
  - 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
- A table lists the following details:
  - **Timestamp**: The time that the event occurred.
  - **Severity**: Identifies the event as major, informational, or cleared.
  - **Category**: The type of event, for example, status or threshold changes.
  - **Description**: A brief explanation of the event.
  - **Host Name**: The host name of the device on which the event occurred.
  - **Device MAC**: The MAC address of the device that reported the event.
  - **Client MAC**: The MAC address of the client that reported the event.

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 **Source** from the list (Critical Alerts, Warning Alerts, and Information Alerts).
- 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
  - Info
- A table lists the following alert details during the specified time range:
  - Alert Name
  - Summary
  - Category
  - Source
  - Timestamp

- Severity
- Status

Note
Select to export filtered alerts.

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

Device Actions Menu

In **Network Devices** > **Device Status**, select a device 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 Factory Setting**: 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. Select a **Firmware Version**, and then select **Upgrade Firmware**.
- **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**: Configure the selected device. See, Device Management Overview on page 63.

Clients

The **Clients** page provides a list of wired and wireless clients, users, and applications.

Monitor Clients

The **Clients** tab provides list of wired and wireless devices. You can filter the client list for the selected site.

For more information on performing actions on the clients from the 3-dot menu, see Client Three-dot Menu on page 118.

The Wired table displays the following information:

- Connection Status
- Client
- Location
- IPv4
- Port Number/Switch Name
- VLAN
- Operating System
- MAC
- Username
- Instant Port Profile
- Total Congestion
- Total Unicast
- Total Multicast
- Total Broadcast
- Total Port Errors
- IPv6

When you select a device and enter the device details page you can select one of the following tabs:

- Overview
- Client Trail on page 118
- Troubleshooting for Wireless on page 118

Overview

In the **Wireless** section, when **Show Summary** is enabled, widgets display Connectivity Issues, Roaming Issues, and Frequency Distribution.

The Wireless table displays the following information:

- Connection Status
- Client
- Location
- SNR
- RSSI
- Frequency
- Airtime %
- Association Issues
- Authentication Issues
- Network Issues
- Roaming Issues
- IPv4
- Connected To
- SSID
- VLAN
- Last Session Start Time
- Operating System
- MAC
- User Name
- Authentication
- Encryption
- User Profile
- Alias
- Category Assignment
- IPv6
- Client Retries
  - Tx Retries
  - Rx Retries

Client Trail

The **Client Trail** tab on the **Wireless Clients** page provides an view of the following:

- Roaming Trail
  - Timestamp
  - From
  - To
  - Roam Duration
  - Status
- Connectivity Experience
  - Timestamp
  - AP Name
  - SSID
  - Association
  - Authentication
  - DHCP
  - DNS
  - Default Gateway ARP

The **Client Trail** tab on the **Wired Clients** page provides an view of the following:

- Timestamp From
- Timestamp To
- Duration
- Device Name
- Port
- Speed
- Duplex

Troubleshooting for Wireless

The **Troubleshooting** tab on the **Clients** page provides an view of the **Troubleshooting Sessions**. The table displays the Timestamp, Description, Initiated by, and Status.

Client Three-dot Menu

From the three-dot menu on the **Client** tab, you can complete the following actions:

- Wireless:
  - Change Client Alias on page 119
  - Disconnect Client on page 120 or Clients (Bulk)
  - Manage Real Time Statistics on page 119
- Wired:
  - Show Endpoint to Endpoint
  - Port Bounce
  - Cable Test

Change Client Alias

Use this task to change a client alias.

1. Go to **Monitoring** > **Clients**.
2. Select one or several clients and select the three dot menu and select **Change Client Alias** .
3. Add a new client alias in the field and select **Save**.
4. For bulk client alias changes, add a new client alias and select **Yes**.

Manage Real Time Statistics

Use this task to manage Real Time Statistics for wireless clients.

1. Go to **Monitoring** > **Clients**.
2. Select one or several clients and select the three dot menu and select **Real Time Statistics** and configure the settings in Table 48.

Table 48: Real Time Statistics Configuration Settings

Field	Descriptions
Client	Select a client.
Select **Start** or **Stop**.	
Select an AP from the drop-down list.	
Packet Stream	Select one of the three options: • All • Data Frames • Management Frames

3. Select **Close**.

Client Actions

From the **Actions** menu on the **Client Overview** tab, you can complete the following actions:

- Wireless:
  - Troubleshoot Connectivity on page 120
  - Disconnect Client on page 120
- Wired:
  - Show Endpoint to Endpoint on page 120
  - VLAN Probe on page 112
  - Port Bounce
  - Cable Test

Troubleshoot Connectivity

Use this task to troubleshoot client connectivity.

1. Go to **Actions** > **Troubleshoot Connectivity** and configure the settings in Table 49.

Table 49: Troubleshooting Settings

Field	Description
Selected Client	Shows selected client.
Description (Optional)	You can add a description.
Select APs from the list below	Search for a specific client or select a client from the list.

2. Select **Start**.

Disconnect Client

Use this task to disconnect a client.

1. Go to **Actions** > **Disconnect Client**.
2. To temporarily disconnect the select client, select **Yes**.

Show Endpoint to Endpoint

Use this task to show endpoint to endpoint.

1. Go to **Actions** > **Show endpoint to endpoint** and configure the settings.
2. Select the **Physical** or **Fabric** layer as required.
3. Right-click a device in the topology map and select **Show Endpoint-to-Endpoint Service/VLAN**.
4. Select the second device from the list of devices to view the endpoint-to-endpoint service mapping.

5. Select **Select End Point**.
   The lists of services available on the selected endpoints opens.

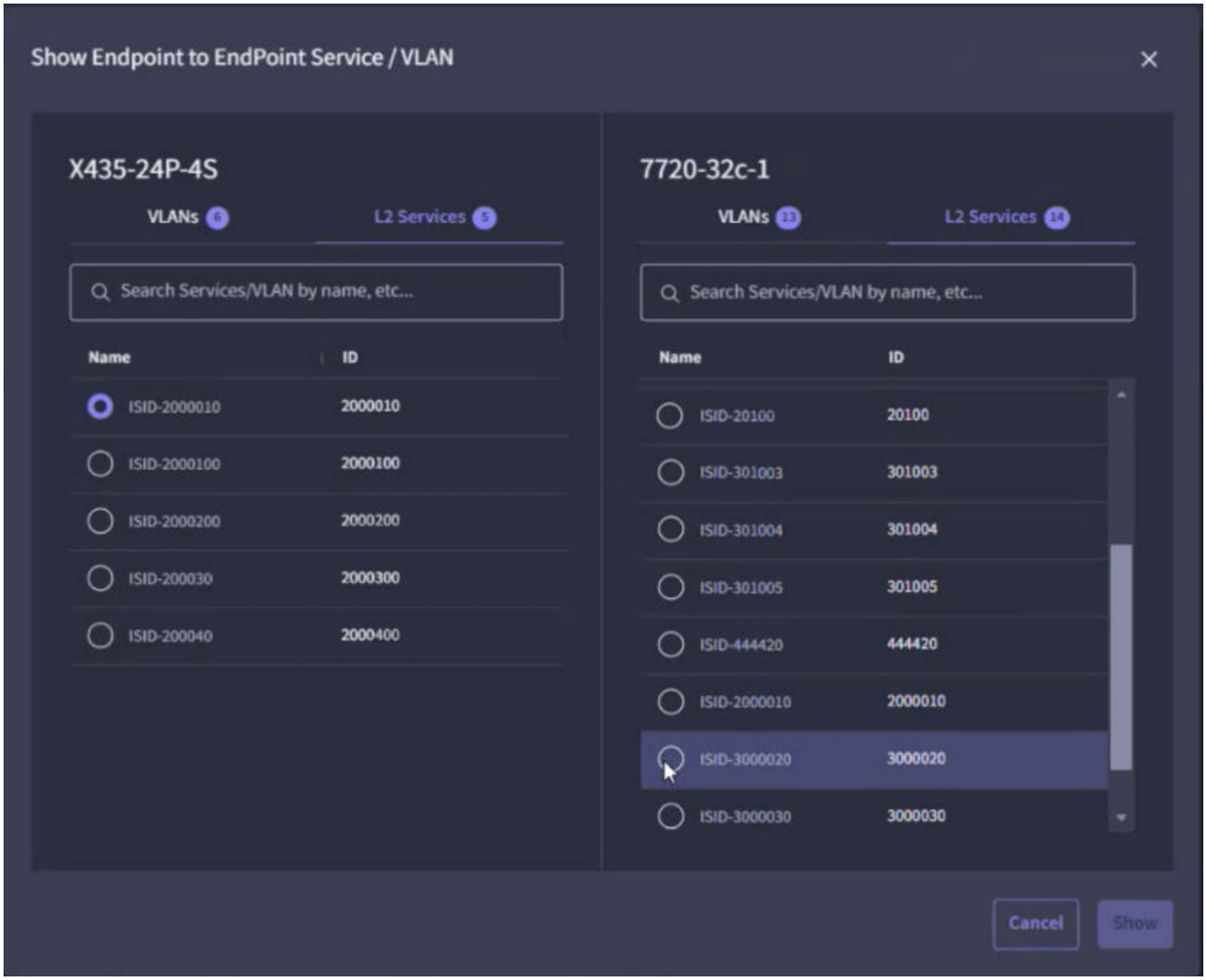


Figure 4: Endpoint Services

6. Select a service from each of the lists.

7. Select **Show**.

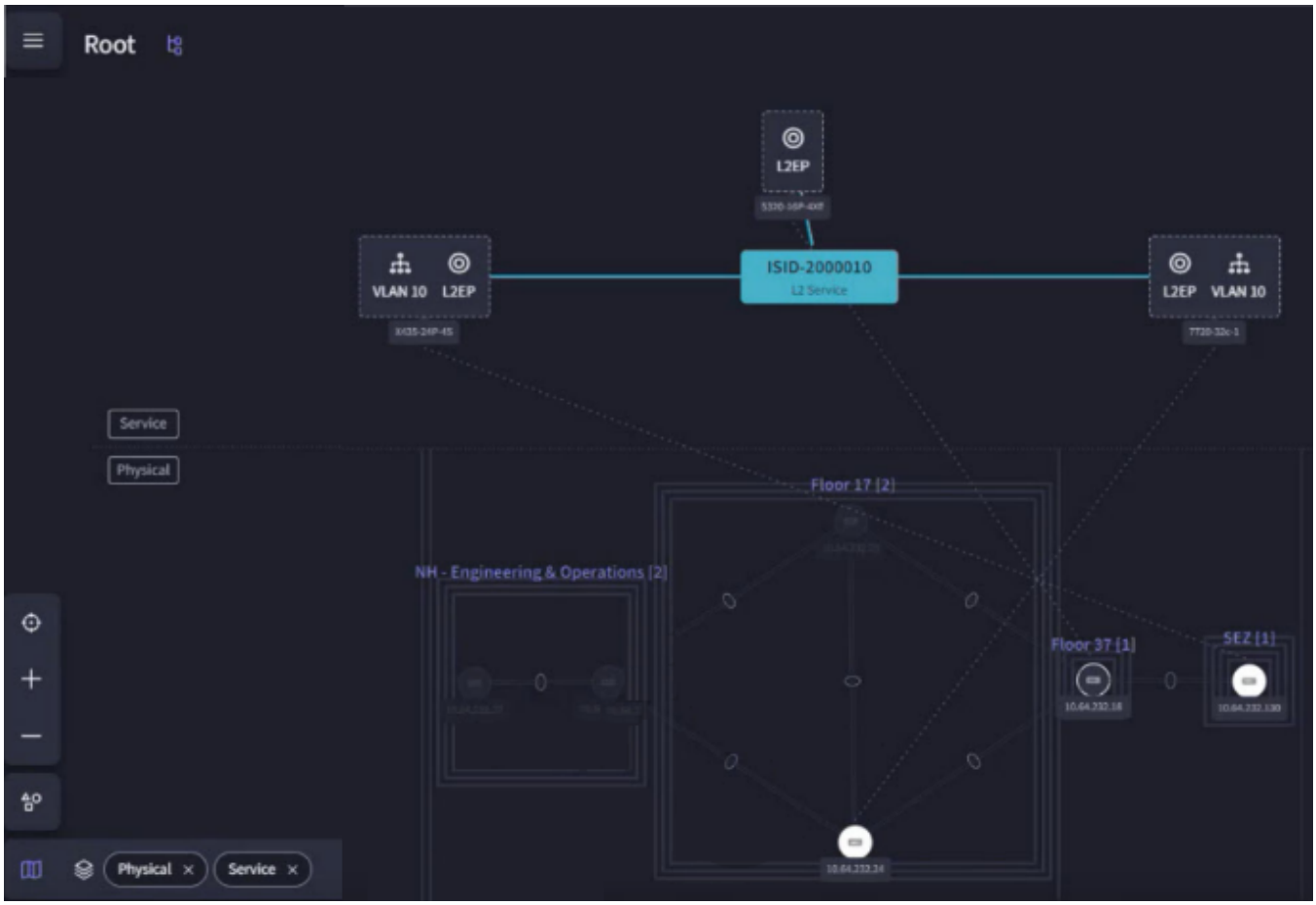


Figure 5: Endpoint to Endpoint Configuration Path

ExtremeCloud IQ (New) displays the Endpoint to Endpoint configuration path for the selected device.

8. Select the highlighted service on the topology map to view the endpoint-to-endpoint summary in the inspector panel.
9. In the inspector panel, select **Close ETE Service View** to exit the endpoint-to-endpoint service view.

Monitor Users

In the **Users** section, enable **Show Summary** to display the following widgets:

- User Type
- Data Usage
- Connected Users

The Users table displays the following information:

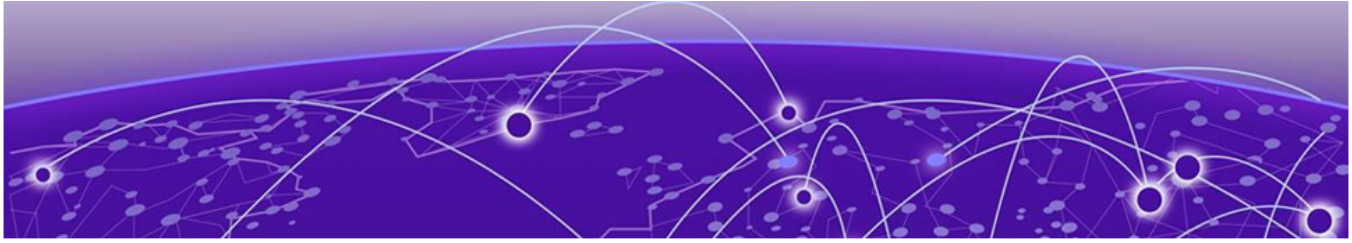
- Status
- Location

- User Name
- Email Address
- User Group
- Clients
  - Wired
  - Wireless
- Data Usage (in GB)
- Source
- Session Duration
- Expires

Monitor Applications

The Applications table displays the following information:

- Application
- Category
- Data Usage
  - Generated Traffic
  - %Used
- #Clients
- #Users



NEW! Reports

Generate Reports on page 124
View and Customize Reports on page 124

The **Reports** > **On-demand Analytics** page provides details about your network and how well it is functioning. The available types of analytics are:

- **Clients** >
  - **Max Concurrent Clients Over Time**
  - **Client Quality Score Over Time**
  - **Wireless Clients By OS**
  - **Unique Clients Over Time By SSID**
  - **Client Sessions Over Time**
  - **Clients By OS**
  - **Unique Wi-Fi Clients Over Time**
  - **Client Airtime Usage Over Time**
- **Application Usage** > **Whole App Traffic Volume**
- **Device** > **Devices By Clients Over Time**

Generate Reports

Use this task to generate reports for one or more analytics types.

1. Select one or more of the analytics types.
2. Select **Generate Analytics**.

   On-demand Analytics generates a report for each selected analytics type.
3. (Optional) To add or remove analytics types, select  .

Related Links

View and Customize Reports on page 124

View and Customize Reports

On-demand Analytics displays the reports for the analytics types that you selected.

1. Scroll through the reports, or select a category: **Clients**, **Application Usage**, or **Device**.

2. Mouseover a line on a graph to see the value and timestamp for a particular point on the timeline.
3. Use the filter menus to further customize the reports.

   You can filter according to the following criteria:

   - Location
   - Date and Time Range
   - Radio Bands
   - SSID
4. To reset the filters, select **Clear**.
5. To download the generated reports, select  and choose the file format (PDF or XLSX).

Related Links

Generate Reports on page 124

Configuration | Sites

Sites on page 126

Use **Sites** to plan your network by adding locations, buildings, and floors. Place simulated devices to determine where you might need to add or redistribute devices for the best wireless network capability.

Note
During the customer onboarding process, Extreme Platform ONE Networking automatically creates the **Organization** for sites. The **Organization** name is the same as the **Company** name that you provided for your account.

Sites

The Visualize view leverages site groups and site hierarchy in ExtremeCloud IQ (New) for creating groups during the device onboarding process. The site groups and sites appear as groups on the map.

ExtremeCloud IQ (New) adds devices that are not mapped to a specific site or floor to the **Default Site** in Visualize view. You can map locations to these devices using ExtremeCloud IQ (New) or keep them in the **Default Site**.

Select the **Default Site** to open the details panel. The **Summary** tab displays a list of devices that are not mapped to a specific site or floor.

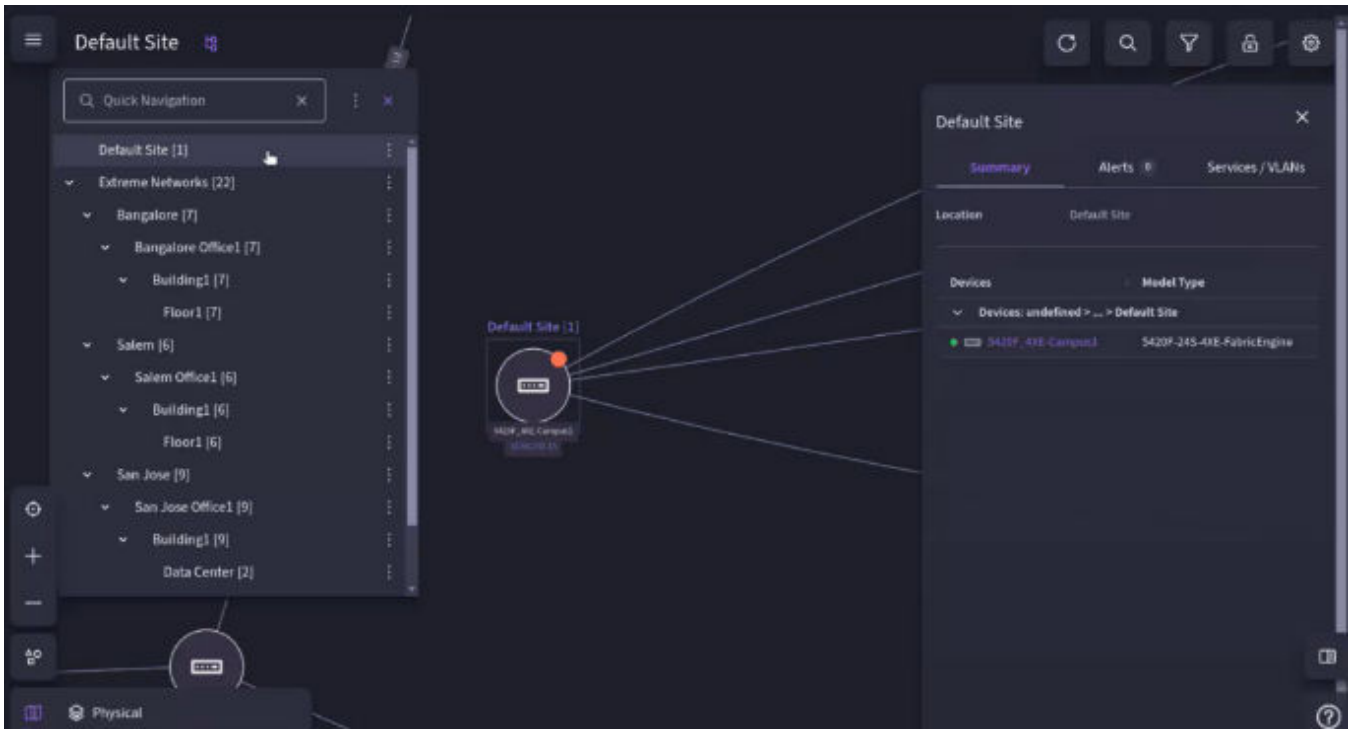


Figure 6: Details panel for the Default Site

The Visualize view supports the following location hierarchy:

Site Group

Site groups are optional folders into which you can organize sites. Two levels of site groups are permitted. Site group names must be unique within the organization.

Site

Sites are a mandatory component of the location hierarchy. A site is the parent container for buildings and can include multiple buildings.

Sites are parent containers for buildings and serve the following purposes:

- Column picker
- Configuration applicability
- Monitoring unit
- Troubleshooting and health score unit

Site names must be unique within the organization. A site cannot belong to more than one site group.

Select to open the Column Picker and select the table columns to include in the Device list view. The options available to choose from depends on the current view.

Building

Buildings are physical premises with addresses. A building is the parent container for floors and must be associated with a site.

Building names must be unique within the parent site.

Floor

Floors are physical subdivisions of buildings.

Floor names must be unique within the parent building.

Import a Site Tree

Use this task to import a site tree to your network plan.

Note
This feature is available only if the site tree is empty.

1. Go to **Configuration** > **Sites** and select **Import Site Tree**.
2. Select **Browse Files** or drag and drop the the site tree file.

   The files must be in .xml format.
3. Select **Import**.

Add a Site

Use this task to add a new site to your network plan.

1. Go to **Configuration** > **Sites** and select **Add Site**.

   Alternatively, to add a site to an existing site group, select ⋮ and choose **Add Site**.
2. Type a **Name** for the new site.
3. Select the **Country**.
4. To add the new site group to an existing group, select an existing parent site group from the **Association** list.
5. (Optional) Enter the address manually, use GPS coordinates, or select the location on the map.
6. Select **Save**.

Add a Site group

Use this task to add a new site group folder to your network plan.

1. Go to **Configuration** > **Sites** and select **Add Site Group**.

   Alternatively, select ⋮ for the corresponding parent group, and then choose **Add Site Group**.
2. Type a **Name** for the new site group.
3. (Optional) Add the **Description** text.
4. To add the new site group to an existing group, select an existing parent site group from the **Association** list.
5. Select **Save**.

Add a Building

Your network hierarchy must contain at least one site with the country code defined, before you can add buildings and floors.

Use this task to add a new building to your network plan, and to upload building perimeters and floor plan images. Visualize view stores the images in the image library for future use.

1. Go to **Configuration** > **Sites**, and select the corresponding ⋮ button for a site.
2. Select **Add Building**.
3. Type a **Name** for the building.
4. Type the building **Address**.

   Alternately, use Google Maps search to automatically populate the address. If you manually adjust the marker on the map, the address updates automatically.

   While sites do not require addresses, buildings must have addresses.
5. Select **Save**.

NEW! Move a Building

Use this task to move a building from one site, to another indoor site.

1. Go to **Configuration** > **Sites**.
2. Locate and expand the site that includes the building that you want to move.
3. Locate the building and select ⋮ > **Move**.
4. In the dialog, from the **Associated With** menu, select the destination site.

   Note
   Moving a building to an outdoor site is not supported.
   Building names must be unique. If a building with the same name exists in the target site, ExtremeCloud IQ (New) prompts you to rename the building before the move.
5. Select **Move**.

Add a Floor

Use this task to add a floor to a building.

1. Go to **Configuration** > **Sites**, and select the corresponding ⋮ button for a building.
2. Select **Add Floor**.
3. Type a **Name** for the floor.
4. From the **Environment** menu, choose the environment type that most closely matches your installation.
5. For **Floor Attenuation (in dB)** menu, type or use the arrows to select the noise level for the floor.

6. Specify the **AP Installation Height** (distance from the floor to the mounting point) of the APs on the floor.

   If the height varies from AP to AP, enter the average height. This setting has a minimal effect on location estimates except for sites such as warehouses where the height of ceilings or high crossbeams is substantial.
7. Specify the unit of measurement: feet or meters.
8. To provide more information for AFC, turn on **Supports AFC (6GHz)** and do the following:
   a. For **AP Installation Height**, specify the **Accuracy Range % (+/-)**.
   b. Specify the **Height from Ground** (distance from the ground to the mounting point) of the APs on the floor.
   c. For **Height from Ground**, specify the **Accuracy Range % (+/-)**.
9. Select **Upload Floor Plan** and choose an image from the Library, or upload a new image.

   For more information, see Upload a Floor Plan on page 130.
10. Verify the name of the building in the **Association** list.
11. Select **Save**.

Related Links

Upload a Floor Plan on page 130

Upload a Floor Plan

Use this task to upload a floor plan to an existing floor, or while creating a new floor.

Extreme Platform ONE Networking supports the jpg and png image formats with an image resolution of 8K.

1. Go to **Configuration** > **Sites** and expand the **Site** and the **Building**, to which you want to add a floor plan.
2. For an existing floor, select  .

   If you're adding a new floor, select **Upload Floor Plan**.
3. Choose **Upload New**.

   Alternatively, select **Choose from Library**, select an image, and then click **Select**.
4. Drag and drop image files into the window, or select **Browse Files** to locate and select the image files.
5. To overwrite files with duplicate names, select **Override floor plan images with same names**.
6. Select **Next**.
7. Select and drag the image border to crop the image.
8. Select **Next**.
9. Select Point A and drag to Point B to set the scale for the floor plan.
10. Select **Done**.

Edit a Site

Use this task to edit a site, site group, building, or floor in your network plan.

1. Go to **Configuration** > **Sites**.
2. Select ⋮ associated with the site to modify it.
3. Select **Edit** and modify the fields as needed.
4. Select **Save**.

Move a Site

Use this task to move a site to a new location.

1. Go to **Configuration** > **Sites**.
2. Select ⋮ associated with the site to move it.
3. Select **Move**.
4. To move the site to an existing group, select an existing parent site group from the Association list.
5. Select **Move**.

Export a Floor Plan

Use this task to export a floor plan.

1. Go to **Configuration** > **Sites**.
2. Select ⋮ associated with the floor to export it.
3. Select **Export**.

   The floor plan is exported into .xml or .tar format.
4. Select **Export**.

Clone a Building

Use this task to clone a building.

1. Go to **Configuration** > **Sites**.
2. Select ⋮ associated with the building to clone it.
3. Select **Clone**.
4. Type a **Name** for the new building.
5. To add the new building an existing group, select an existing parent site group from the Association list.

Delete a Site

Use this task to delete a site.

1. Go to **Configuration** > **Sites**
2. Select ⋮ for the site.

3. Select **Delete**.

   If an object is in use, a pop-up window asks you to delete the references first. The default response is **Cancel**. To delete the object anyway, provide the randomly generated code to delete the location object.

   Warning
   Deleting objects with references can result in orphaned objects and other issues.

Related Links

Delete a Building or a Floor on page 132

Delete a Building or a Floor

Use this task to delete a building or a floor.

1. Go to **Configuration** > **Sites**.
2. Expand the site for which you want to delete a building or floor.
3. Select for the building or floor.

   You can select multiple buildings or floors to delete at once.

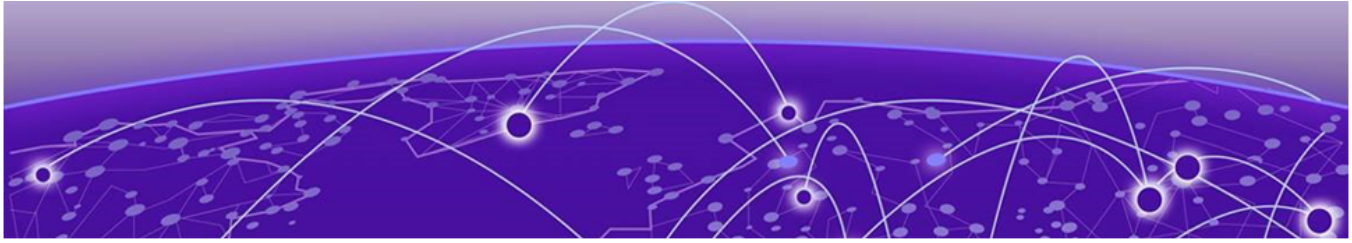
4.
5. Select **Delete**.

   If an object is in use, a pop-up window asks you to delete the references first. The default response is **Cancel**. To delete the object anyway, provide the randomly generated code to delete the location object.

   Warning
   Deleting objects with references can result in orphaned objects and other issues.

Related Links

Delete a Site on page 131



Configuration | Network

A network policy is a combination of configuration settings that can be applied to multiple APs, switches, and routers that share a common characteristic, such as being located at the same site or working together to connect multiple remote sites through VPN tunnels. The type of network policy depends on whether your deployment consists of only wireless AP devices, only switches, only routers, or any combination of these devices. One of the strengths of creating a single policy for multiple device types is that you might only need one unified policy for all your devices. The policy can include one or more SSIDs, device templates, and port types, as well as other configuration elements for networking, including management services such as QoS and VPN tunneling. The policy items are as follows:

- **Policy Details**: Select the policy type: **Wireless** (APs), **Switching** (Universal switches), or both. See Configure Policy Settings on page 135.
- Standard Wireless Networks: Define the wireless network (SSID) and the bands on which to broadcast each SSID, plus SSID usage (authentication, including RADIUS configuration), user access, and additional settings.

- Device Templates: Configure Access Point and Switch device templates.
- Deploy Policy: Push the configuration to your network devices.

Note

- The assigned **Access Scope** determines an administrator's access to **Common Objects**. Administrators without global access can see and work only with policy objects created for the sites to which they are assigned.
- Only Switch Engine/EXOS devices support common switch settings, templates, and port types.

Related Links

Add a Network Policy on page 134
Configure Policy Settings on page 135
Configure the SSID for a Standard Wireless Network on page 165
Configure Device Templates on page 239
Deploy a Network Policy on page 164

Add a Network Policy

This topic guides you through the basic steps to provide clients with network access via Extreme Networks devices. This process assumes that APs and routers have been deployed and have established secure CAPWAP connections with ExtremeCloud IQ (New). Switches do not use CAPWAP connections. Extreme Networks routers and APs run IQ Engine and communicate with ExtremeCloud IQ (New) using CAPWAP on UDP port 12222 or CAPWAP-over-HTTP on TCP port 80. This is true whether they communicate with ExtremeCloud IQ (New) on premises or in the cloud. Other supported devices communicate with ExtremeCloud IQ (New) using HTTPS on TCP port 443.

Sequential workflow tabs at the top of the page define the network policy configuration process. These tabs are: **1 Policy Details**, **2 Wireless**, **3 Switching/Routing**, and **4 Deploy Policy**. The selected tab is highlighted.

Use this task to add a new network policy.

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

   You can display network policies in a list ( ) or in a thumbnail ( ) format.
2. Select from the list view, or select **Add Network Policy** from the thumbnail view.
3. In the **New Policy** window, select a policy type: (Wireless, Switching/Routing, SR/Dell Switching, Branch Routing, or any combination, including all them).
4. Type a **Policy Name**.
5. (Optional) Type a **Description**.
6. Enable or disable **Presence Analytics**.

   Enable this option to collect customer behavior data. After you enable it, go to the **2 Wireless** workflow step, and from the left navigation bar, under **Application Management**, select **Presence Analytics**. This is where you configure analytics settings, such as trap interval, aging time, and aggregate time.

7. Select **SAVE**.
8. Configure Policy Settings on page 135, as required.
9. Select **NEXT**.

   The highlighted tab changes from **1 Policy Details** to **2 Wireless**, **3 Switching/ Routing**, **4 SR/Dell Switching**, **5 Branch Routing** and **6 Deploy Policy**, depending on your configuration choices.

After you have configured the network policy, Deploy a Network Policy on page 164.

Related Links

Configure Policy Settings on page 135
Deploy a Network Policy on page 164

Configure Policy Settings

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

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

1. Go to **Configuration** > **Network**.
2. Select an existing network policy, and then select , or to add a new one, select . to create a new policy.
3. Configure the **Policy Settings**.
   a. Configure DNS Server Policy Settings on page 136.
   b. Configure NTP Server Policy Settings on page 137.
   c. Configure SNMP Server Policy Settings on page 139.
   d. Configure Syslog Server Policy Settings on page 141.
   e. Configure Device Credentials Policy Settings on page 143.
   f. Configure the Device Time Zone on page 143.
   g. Configure HIVE Policy Settings on page 144.
   h. Configure Management and Native VLAN Policy Settings on page 147.
   i. Configure IP Tracking Policy Settings on page 149.
   j. Configure LLDP/CDP Policy Settings on page 151.

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

4. Configure the **Management Settings**.
   a. Configure Management Options on page 152.
   b. Configure Traffic Filters Policy Settings on page 162.
   c. Configure MGT IP Filter Policy on page 163.

5. Select **SAVE**.
6. Select **Policy**, and then select **NEXT**.

Related Links

Configure Classification Rules for a Device Template on page 289

Configure DNS Server Policy Settings

DNS is a critical service for ExtremeCloud managed devices and is required to permit each device to connect to and communicate with ExtremeCloud IQ (New) and related services.

Out of the box, and by default, unconfigured APs and switches find the DNS server to use from your DHCP server.

Note
For APs — If your DHCP server does not advertise a DNS server, the AP will instead use the following DNS servers from OpenDNS:

- 208.67.222.222
- 208.67.220.220

The usability of OpenDNS servers can vary depending on the country. Consult OpenDNS documentation for information on excluded countries.

Either your DHCP-defined DNS server or the two default DNS servers must be reachable outbound on UDP port 53 by each device connecting to ExtremeCloud IQ (New).

The DNS server settings defined in this part of the network policy configuration workflow are written to the configuration of your managed device after initial connection.

Note
If enabled, these DNS server settings will override the default DNS behaviors of your managed device. The DNS servers defined here must be reachable from your managed devices on outbound UDP port 53.

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

1. Go to **Configuration** > **Network**.
2. Select an existing network policy, and then select , or to add a new one, select . to create a new policy.
3. From the **Policy Settings** menu, select **DNS Server**.
4. Toggle the **DNS Server** setting to **ON**.
5. (Optional) To use existing DNS server settings, choose a DNS object from the menu.
6. Configure the DNS Server Settings on page 137.

7. To add a new DNS server, select .
   a. Type the IP address of the new DNS server.
   b. 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.
8. If you want to use classification, select **Apply DNS servers to devices via classification**.
9. Select **SAVE DNS SERVER**.

Related Links

DNS Server Settings on page 137
Configure Policy Settings on page 135

DNS Server Settings

Table 50: Settings for DNS server profiles

Setting	Description
Name	(Required) Type a **Name** for the default DNS server.
Domain Name	Type a **Domain Name** for the default DNS server.
Description	Type a description for the default DNS server. Although optional, entering a description is helpful for troubleshooting and for identifying the DNS server.

Related Links

Configure DNS Server Policy Settings on page 136

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 ExtremeCloud IQ (New) and related services and to ensure alerts and events have the correct timestamp.

Out of the box, and by default, Extreme Networks access points (APs) and switches try to contact the NTP server assigned by your DHCP server. If your DHCP server does not advertise an NTP server, the device will automatically attempt 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 ExtremeCloud IQ (New).

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.

The NTP server settings defined in this part of the network policy configuration workflow for the configuration of your managed device after initial connection.

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

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

1. Go to **Configuration** > **Network**
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 139.
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**.

      ExtremeCloud IQ (New) 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**.
9. Select **SAVE NTP SERVER**.

Related Links

NTP Server Settings on page 139
Configure Policy Settings on page 135

NTP Server Settings

Table 51: 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.

Related Links

Configure NTP Server Policy Settings on page 137

Configure SNMP Server Policy Settings

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**
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 140.
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. If you want to use classification, select **Apply SNMP servers to devices via classification**.
16. Select **SAVE SNMP SERVER**.

Related Links

SNMP Server Settings on page 140
Configure Policy Settings on page 135

SNMP Server Settings

Table 52: 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 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 52: 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.

Related Links

Configure SNMP Server Policy Settings on page 139

Configure Syslog Server Policy Settings

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**
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 Syslog Server Settings on page 142.
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**.
13. Select **SAVE SYSLOG SERVER**.

Related Links

Syslog Server Settings on page 142
Configure Policy Settings on page 135

Syslog Server Settings

Table 53: 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.
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.

Related Links

Configure Syslog Server Policy Settings on page 141

Configure Device Credentials Policy Settings

ExtremeCloud IQ (New) uses device credentials for remote access to devices through Telnet, SSH, or console connections. If you do not configure the Administrator and Read Only Administrator accounts, global device management settings apply.

Note
If you configure a new administrator account, the new account replaces the default account.

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

1. Go to **Configuration** > **Network**.
2. Select an existing network policy, and then select , or to add a new one, select ..
3. For **Policy Settings**, select **Device Credentials**.
4. Configure the following settings:

Table 54: Device Credentials

Setting	Description
Administrator Account	
Admin Name	Type the name of the **Administrator** account.
Password	Type the password for the **Administrator** account.
Show Password	Select the check box to show the password.
Read Only Administrator	
Admin Name	Type the name of the **Read Only Administrator** account.
Password	Type the password for the **Read Only Administrator** account.
Show Password	Select the check box to show the password.

5. Select **SAVE**.

Related Links

Configure Policy Settings on page 135

Configure the Device Time Zone

This task is part of the network policy configuration workflow. Use this task to configure the **Device Time Zone** for a network policy.

1. Go to **Configuration** > **Network**.
2. Select an existing network policy, and then select , or to add a new one, select ..
3. From the **Policy Settings** menu, select **Device Time Zone**.

4. From the **Time Zone** menu, select a time zone.
5. If you want to use classification, select the **Apply time zone to devices via classification** check box.
6. Select **SAVE**.

Related Links

Configure Policy Settings on page 135

Configure HIVE Policy Settings

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

1. Go to **Configuration** > **Network**.
2. Select an existing network policy, and then select , or to add a new one, select . to create a new policy.
3. From the **Policy Settings** menu, select **HIVE**.
4. (Optional) To use existing HIVE settings, choose a HIVE object from the menu.
5. Configure the HIVE Profile Settings on page 144.
6. Apply MAC filters to restrict devices that can join the hive.

   You can select existing filters from the table or add new filters.
7. From the menu, choose the default action (**Permit** or **Deny**) for devices that have a MAC address or OUI that does not match the selected MAC filter.
8. Select **SAVE**.

Related Links

Configure Policy Settings on page 135
HIVE Profile Settings on page 144

HIVE Profile Settings

Table 55: HIVE profile settings

Setting	Description
Name	Type a **Name** for the new profile.
Hive Control Traffic Port	Type the port number for Hive traffic control. Hive communications operate at Layers 2 and 3. The default port number for Layer 3 hive communications and for roaming-related traffic is UDP 3000. If a different service on your network is already using port 3000, you can change this to any number from 1024 to 65535, as long as the new setting is at least 50 greater or less than the current setting. For example, if the current port number is 3000, you can set a new port number higher than 3050.
Description	(Optional) Type a description for the new profile. Although optional, entering a description is helpful for troubleshooting and for identifying the profile.

Table 55: HIVE profile settings (continued)

Setting	Description
Alarms	
CAPWAP Delay Alarms	Toggle the setting **ON** or **OFF**.
Security	
Encryption Protection	Toggle the setting **ON** or **OFF**. Disable **Encryption Protection** to have ExtremeCloud IQ derive a default password from the hive name.
Encryption Password	Choose between **Auto Generate** and **Manual**. Hive members use this password to authenticate to each other over the wireless backhaul link using WPA-PSK CCMP (AES). To see the password that you entered, clear the **Shared Secret** > **Show Password** check box.
MAC-based DoS Prevention Rules	Select **Hive** or **Client**, and modifying the settings in the dialog box. Extreme Networks devices ship with the default hive- and SSID-lever DoS detection settings for a number of frame types that are commonly used when launching DoS attacks. You can raise the thresholds to avoid receiving too many false alarms or lowering them to receive more alarms indicative of spikes in certain types of traffic. • **DoS prevention rules for hives** apply to wireless traffic from all radios that might reach the backhaul or access channel from wireless clients or nearby access points broadcasting on the same channel. You can define settings to detect DoS attacks on the radio channels that a device uses for hive communications and for SSID access traffic. • **DoS prevention rules for clients** apply to traffic originating from a single neighboring radio. The source might be a neighbor member or a nearby device outside the network that is broadcasting on the same channel the Extreme Networks device is using for its wireless backhaul communications, or for SSID access traffic. For both types of rules, you can change the alarm thresholds and enable or disable settings for each DoS Detection type: Probe Requests and Responses, (Re) Associations, Association and Disassociation Requests and Responses, Authentication and Deauthentication, and EAP over LAN (EAPoL). Wireless clients periodically send probe requests to see if any access points are within range. The threshold determines the number of messages per minute required to trigger an alarm about a possible DoS attack. The alarm interval determines the length between repeated alarms when the number of messages continues to exceed the threshold.
Wireless Mesh Settings	

Table 55: HIVE profile settings (continued)

Setting	Description
Request to Send Threshold	Type a value in bytes. This is the maximum frame size in bytes that requires the device to first send an request to send (RTS (request to send) message before sending a large frame. The default setting is 2346 bytes.
Fragment Threshold	Type a value in bytes. This is the maximum IEEE 802.11 frame size in bytes that the device uses when sending control traffic over the wireless backhaul link to other members. If the device needs to send a frame that is larger, it first breaks it into smaller fragments. The default setting is 2346 bytes.
Require minimum wireless signal strength for creating wireless mesh	Select the check box to require a minimum wireless signal strength for creating wireless mesh, and configure the related settings.
Signal Strength Threshold	Use the slider to specify a signal strength between 90 dBm and - 55 dBm. This value is the minimum signal strength required to enable members to form a wireless backhaul link. The default is -80 dBm.
Polling Interval	Type a value for the time interval from 1 to 60 minutes for polling the signal strength of neighboring members. A lower interval increases traffic on the network slightly, especially in environments where there are lots of members, however it also increases the responsiveness of members to changes in signal strength. A higher interval reduces responsiveness to signal strength changes, which can be preferable in an environment where severe and frequent signal strength fluctuations would cause members to continually drop and re-establish connections. The default is every 60 seconds.
Client Roaming > **Detect neighbor devices**	
Devices send keepalive heartbeats every	Type a value and select a unit of time from the menu to set the interval between keepalive heartbeats. The default is 10 seconds, and the range is 5 to 360,000 seconds (100 hours). To calculate the length of time, multiply the keepalive interval by the number of missed keepalives. Using the default settings, 10 seconds (interval) x 5 (missed keepalives), a neighbor ages out after 50 seconds.
Remove neighbor if the number of missed keepalive heartbeats exceeds	Type the number of the number of missed heartbeats before ExtremeCloud IQ removes a neighbor.
Client Roaming > **Share connected client information (Roaming cache)**	
Devices send client information every	Type a value and select a unit of time from the menu to specify how often devices send client information. The default is 60 seconds.

Table 55: HIVE profile settings (continued)

Setting	Description
Remove cached client information when absent from updates after	Type the number of missed updates, after which ExtremeCloud IQ deletes cached client information for the affected client.
Update all hive members within radio range, including Layer 3 neighbors	Select the check box to update all hive members within radio range, including Layer 3 neighbors.
Update hive members in the same subnet and VLAN.	Select the check box to update hive members in the same subnet and VLAN.
IP Address Preference	
Use IP address type first with	(Required) From the menu, select **IPv4** or **IPv6**.

Related Links

Configure HIVE Policy Settings on page 144

Configure Management and Native VLAN Policy Settings

This task is part of the network policy configuration workflow. Use this task to configure **Management and Native VLAN** policy settings for a network policy.

1. Go to **Configuration** > **Network**.
2. Select an existing network policy, and then select , or to add a new one, select ..
3. From the **Policy Settings** menu, select **Management and Native VLAN**.
4. Select an **MGT Interface VLAN** and choose an existing object, or to add a new one, select ..
5. For a new **MGT Interface VLAN**, configure the settings.
   a. Type a **Name** for the new VLAN object.
   b. Type a **VLAN ID** for the new VLAN object.
   c. If you want to use classification, select **Apply VLANs to devices using classification**.

      See Configure Classification Rules on page 148.
6. Select an **Native (Untagged) VLAN***For IQ Engine devices only* and choose an existing object, or to add a new one, select ..
7. For a new **Native (Untagged) VLAN**, configure the settings.
   a. Type a **Name** for the new VLAN object.
   b. Type a **VLAN ID** for the new VLAN object.
   c. If you want to use classification, select **Apply VLANs to devices using classification**.

      See Configure Classification Rules on page 148.
8. Select **SAVE VLAN**.

Related Links

Configure Classification Rules on page 148

Configure Policy Settings on page 135

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.

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

- 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.

This task is part of the network policy configuration workflow. Use this task to create a classification rules object. ExtremeCloud IQ (New) supports multiple classification rules for DNS servers, VLANs, RADIUS servers, device templates, user groups, and private client groups (PCGs).

1. Go to Go to **Configuration** > **Network**.
2. Select an existing rule, and then select , or to add a new one, select .
3. Enter a **Name** for the rule.
4. (Optional) Enter a **Description** for the rule.
5. Select , and then choose the rule type to configure.

   Choose from the following rule types:

Table 56: 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**.

Table 56: Rule types (continued)

Selected rule type	Do this
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**.

6. Select **SAVE RULE**.

Related Links

Add a Cloud Config Group on page 291

Configure IP Tracking Policy Settings

This task is part of the network policy configuration workflow. Use this task to configure **IP Tracking** policy settings for a network policy.

1. Go to **Configuration** > **Network**.
2. Select an existing network policy, and then select , or to add a new one, select . to create a new policy.
3. From the **Policy Settings** menu, select **IP Tracking**.
4. Toggle the **IP Tracking** setting to **ON**.
5. Select a tracking group and use the single-arrow controls to move it from **Available IP Tracking Groups** to **Selected IP Tracking Groups**, or vice versa.

   Use the double-arrow controls to move all of the tracking groups.

6. To add a new IP tracking group, select **ADD ANOTHER IP TRACKING GROUP**, and then configure the IP Tracking Group Settings on page 150.
7. Select **SAVE**.

Related Links

IP Tracking Group Settings on page 150
Configure Policy Settings on page 135

IP Tracking Group Settings

Table 57: Settings for IP Tracking Groups

Setting	Description
Name	Type a **Name** for the group.
Description	(Optional) Type a **Description** for the group. Although optional, entering a description is helpful for troubleshooting and for identifying the group.
Connectivity	Select either **Backhaul Connectivity Tracking for APs** or **WAN Interface Connectivity Tracking for APs**.
Enable IP Tracking	To activate this IP tracking group, select the check box. Clear the check box to exclude the group from **Available IP Tracking Groups**.
Track the Following Targets	
IP Addresses	Enter up to four IP addresses, separated by commas. If you are also tracking the default gateway, enter up to three IP addresses.
Default Gateway	If the IP addresses use the default gateway, select **Default Gateway**. Otherwise, clear the check box.
Take action when	From the menu, select a condition for which to take action. Choose between **All targets become unresponsive** and **A single target becomes unresponsive**.
Tracking Interval	(Required) Type the tracking interval for this group. Default: 6
Tracking Retries	(Required) Type the number of retries before taking action for an IP address failure. Default: 3
Actions to take when target becomes unresponsive	
Enable the virtual access console	Select the check box to take this action when the target is unresponsive.
Disable all active SSIDs	Select the check box to take this action when the target is unresponsive.
Start the backhaul (mesh) failover procedure	Select the check box to take this action when the target is unresponsive.

Related Links

Configure IP Tracking Policy Settings on page 149

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 ExtremeCloud IQ (New). 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**.
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 151.

Related Links

Configure Policy Settings on page 135
LLDP and CDP Settings on page 151

LLDP and CDP Settings

Table 58: 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.

Table 58: Settings for LLDP and CDP (continued)

Setting	Description
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.

Related Links

Configure LLDP/CDP Policy Settings on page 151

Configure Management Options

After you enable **Management Options** in the network policy, you can re-use an existing **Management Options** object, or configure the settings manually.

This task is part of the network policy configuration workflow. Use this task to configure **Management Options** for a network policy.

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

2. Select an existing network policy, and then select , or to add a new one, select . to create a new policy.
3. From the **Management Settings** menu, select **Management Options**.
4. Toggle the **Management Options** setting to **ON**.
5. To reuse existing management options settings, select **Re-use MGT IP Filter**, and then select an existing **Management Option**.
6. Enter a **Name**.
7. (Optional) Enter a **Description**.

   Although optional, entering a description is helpful for troubleshooting and for identifying the **Management Options** object.
8. Configure the settings for Management Options on page 153.
9. Select **SAVE**.

Related Links

Management Options on page 153
Configure Policy Settings on page 135

Management Options

Use these settings to control how administrators authenticate and how they access the devices they manage. You can configure global and device-level settings. For example, you can enable or disable the reset button and console port, enable or disable proxy ARP requests and replies, enable APs and routers to forward broadcasts and multicasts between SSIDs, and a variety of other options such as adjusting LED brightness, and setting temperature alarms.

Forwarding Engine Control Management Options

The forwarding engine controls the type of traffic being forwarded between interfaces, between GRE tunnels, and sets logging features.

Table 59: Forwarding Engine Control Settings

Setting	Description
Forwarding Engine Control	
GRE Tunneling Selective Multicast Forwarding	Select one of the following options: • **Block All**—Prohibits forwarding multicast and broadcast traffic through tunnels. • **Allow All**—Enables forwarding multicast and broadcast traffic through tunnels. ExtremeCloud IQ (New) devices can selectively block or permit broadcast and multicast traffic through GRE tunnels to reduce traffic congestion. You can filter using a blocked list that blocks the forwarding of all broadcast and multicast traffic through GRE tunnels (or blocks all except to a few select destinations) or using an allow list that permits all broadcast and multicast traffic through GRE tunnels (or allows all, except to a few destinations).

Table 59: Forwarding Engine Control Settings (continued)

Setting	Description
Exception IP List	Add an entry (destination IP Address and Netmask) to the **Exception IP List**. Type the values, and then select **ADD**.
Service Control	
Limit MAC Sessions per Station	Select **Limit MAC Sessions per Station** to enable the feature, and then type the maximum number of (Layer 2 sessions) that can be created to or from a station. By default, devices do not enforce MAC or IP session limits per station. By default, devices do not enforce IP session limits per station.
Limit IP Sessions per Station	Select **Limit IP Sessions per Station** to enable the feature, and type the maximum number of sessions per station. This feature enables a device to monitor the TCP MSS (maximum segment size) option in TCP SYN and SYN-ACK messages for traffic that the device is going to pass through GRE tunnels (for Layer 3 roaming and static identity-based tunnels) and GRE-over-IPsec tunnels (for IPsec VPN tunnels). The device can then notify the sender to adjust the TCP MSS value if it exceeds a maximum threshold.
Enable TCP Maximum Segment Size	Select **Enable TCP Maximum Segment Size** to enable the feature, and then type the maximum segment size. When establishing a TCP connection, neither end is aware of the packet processing done by network forwarding equipment in between. For example, if a device has to send traffic through an IPsec VPN tunnel, then it adds a GRE header, IPsec header, and possibly a UDP header for NAT-Traversal to each packet. Since the additional headers expand packet size, the device is forced to fragment them, which increases packet processing and slows down throughput. To avoid fragmentation, the device can adjust the MSS (maximum segment size) value inside the initial SYN packet to provide room for the additional headers. The default thresholds are 1414 bytes for GRE tunnels and 1336 bytes for GRE-over-IPsec tunnels and are based on encapsulation overhead of the corresponding tunnel type and the maximum transmission unit (MTU) for the mgt0 interface, which is 1500 bytes by default. If you change the MTU and use "auto" for the TCP MSS option, the device automatically readjusts the TCP MSS thresholds.)
DHCP Option 82: Replace MAC Address with Hostname	To switch between MAC address and Hostname for DHCP option 82,enable **DHCP Option 82: Replace MAC Address with Hostname**. The default is MAC address.

Table 59: Forwarding Engine Control Settings (continued)

Setting	Description
ARP Shield	Enable **ARP Shield** to prevent Man-In-the-Middle attacks by client devices attempting to impersonate critical network resources on the network such as a network gateway or DNS server through an ARP poisoning attack. ARP Shield should not be used if any clients on the network are assigned static IP addresses. ARP Shield is disabled by default and can only be enabled on access points running IQ Engine 6.8.1 and above. Enabling ARP Shield is not enforced on access points running IQ Engine 6.5, switches, routers, or Virtual Gateway appliances.
DHCP Shield	Disable **DHCP Shield** to turn off the built-in ability for IQ Engine to prevent attached clients from impersonating a DHCP server. In the default enabled state, connected clients are blocked from responding to DHCP server discovery or IP lease requests. When disabled, connected clients can respond to DHCP discovery or IP lease requests. DHCP Shield is enabled by default on access points running IQ Engine 6.8.1 and above. Disabling DHCP Shield results in no changes to access points running IQ Engine 6.5, switches, routers, or Virtual Gateway appliances.
Proxy ARP	**Proxy ARP** requests enable learning MAC addresses and proxy replies to ARP requests. Select one of the following slider bar options: • **Disabled**: Not recommended. Disabling turns off all proxy ARP handling capabilities. It increases air time utilization by having to send ARPs to clients in the roaming cache. Use for troubleshooting only. When diagnosing a network issue, you might need to permit ARP requests and replies between wireless clients and network devices (such as the default gateway) to flow directly across the device without proxy. • **Legacy**: Not recommended, but is available for legacy Wi-Fi 4 APs. • **Enhanced**: Preferred and is the highest level of adoption. Supported on Wi-Fi 5 APs and newer. Does not support ARP suppression for devices not in the roaming cache. Wired clients can flood the air with ARPs. • **ARP Suppression**: Recommended, but support is limited to AP3000, AP5010, and AP5050. Protects airtime from overuse by unneeded ARP traffic.

Table 59: Forwarding Engine Control Settings (continued)

Setting	Description
Disable Inter SSID Flooding	Select **Disable Inter SSID Flooding** to prohibit a device from forwarding traffic that it receives from clients in one SSID to clients associated with the same device in another SSID. Instead, such traffic must first cross the device from an interface in access mode to an interface in backhaul mode. From there, the traffic might pass through an internal firewall that performs deep-packet inspection, URL filtering, or antivirus checking, and other operations, before sending the traffic back across the device to reach the clients in the destination SSID.
Disable WebUI Without Disabling CWP	Select **Disable WebUI Without Disabling CWP** to disable the local web user interface on a device to improve system security without disabling the associated captive web portal.
Enable legacy HTTP redirect	Select **Enable legacy HTTP redirect** to enable redirects to legacy HTTP sites. **Note:** Extreme Networks recommends HTTPS for best security. This option is provided for legacy clients, for which HTTPS is not suitable.
Global Logging Options for Firewall Policies	
Log	Select the corresponding check boxes to enable the generation of logs for the following scenarios: • **Drop packets that are denied by IP or MAC firewall policies** • **The first packets of the session destined for the Extreme Networks device itself**
Drop	Select the corresponding check boxes to enable the generation of logs for the following scenarios: • **Fragmented IP Packets** • **All non-management traffic destined for the Extreme Networks device itself**

System Settings Management Options

Use the settings in this section to adjust various device-level functions, including device health alarm thresholds, VoIP features, and client OS detection types. Miscellaneous settings cover reset, console, PoE, and data collection features.

Table 60: System Settings

Setting	Description
LED Brightness	Set the device status LED brightness level. Select an option from the menu: **Bright**, **Soft**, **Dim**, or **Off**.
Temperature Alarm Threshold	Specify the ambient celsius temperature threshold that triggers an alarm.

Table 60: System Settings (continued)

Setting	Description
Fans Underspeed Alarm Threshold	Specify the minimum RPM operating speed for fans. Speeds below this value trigger an alarm.
Call Admission Control	To enable **Call Admission Control**, toggle the setting to **ON**. If enabled, devices monitor VoIP traffic to determine if there is enough available airtime for new VoIP calls.
Airtime per Second	Set the amount of airtime reserved for VoIP traffic. Decreasing the amount of reserved airtime for VoIP traffic frees more airtime for traffic other than VoIP. This can be useful if there are only a few VoIP users on the WLAN. For a high number of VoIP users, increase the amount of reserved airtime. Type a value in microseconds. By default, a device reserves 500 milliseconds of airtime per second for all VoIP calls. You can change the reserved airtime per second for VoIP from 100 to 1000 milliseconds per second.
Guaranteed Airtime for Roaming Clients	Set the percentage of airtime that a device reserves on the access interface for receiving VoIP calls from roaming clients. Type a value as a percentage (%). By default, a device guarantees 20% of the reserved VoIP airtime for VoIP calls from roaming clients. You can change the percent of guaranteed airtime for roaming clients from 0% to 100%. Consider lowering the percent if VoIP users rarely roam, and raising the setting if roaming often occurs. Because VoIP traffic from a roaming client belongs to an existing session, the device to which the client roams always accepts it. If there is not enough airtime available in the guaranteed roaming reserve, the device deducts available airtime from the relevant user profile.
OS Detection	Enable devices to detect the OS of client devices based on a combination of DHCP option 55 contents and the contents of the HTTP headers. To enable, set the toggle to **ON**. The following detection methods are available: • **Use DHCP option 55 contents**: Select to use the DHCP option 55 parameter list. • **Use HTTP user agent IDs**: Select to use the contents of the HTTP user agent ID within the HTTP headers. • **Use both detection methods (DHCP=primary method, HTTP=secondary method)**: Select to use both the DHCP option 55 parameter list and the HTTP user agent information to identify the client operating system. When you select this option, devices first check the contents of the DHCP option 55 parameter list. If it finds no match, then the device examines the HTTP header for the HTTP user agent ID to determine the operating system. If no match is found in either pass, then ExtremeCloud IQ displays **unknown** as the client OS.

Table 60: System Settings (continued)

Setting	Description
Disable Reset Button	Disable the reset button on the front panel of the chassis to prevent non-administrators from using it to reset the device to its default settings or to a bootstrap configuration. Select the check box.
Disable Console Port	Disable the functionality of the console port on a device to block all administrative access through that port. Select the check box. Disabling the console port on a device that is deployed in a publicly accessibly location is a good security precaution. Disabling the console port means that all administrative access must flow over the network, and if there are any connectivity issues with the network or if the device is configured to use only DHCP to get an IP address and cannot get its network settings from a DHCP server, attempts to log in to the device fail. **Note:** Disabling the console port means that all administrative access must flow over the network, and if there are any connectivity issues with the network or if the device—if configured to use only DHCP to get an IP address—cannot get its network settings from a DHCP server, you will not be able to log into the device.

Table 60: System Settings (continued)

Setting	Description
Enable Smart PoE	To enable Smart PoE, select the check box. Smart PoE lets an AP230, AP320 or AP340 adjust power consumption automatically based on the current power supply. The AP230 and AP320 support PoE on the ETH0 interface. The AP340 supports PoE on both its ETH0 or ETH1 interfaces, and can simultaneously draw power through either one or both. Using Smart PoE, an AP can detect if there are power injectors connected to one or both of its Ethernet ports and how many watts are available for each PoE channel. The AP uses this information to manage its internal use of power resources based on the currently available power level as follows: • 20 W or higher: No adjustments are needed when the power level is 20 W or higher. • 18 - 20 W: The device disables the ETH1 interface. • 15 – 18 W: The device switches from 3x3 MIMO (Multiple In, Multiple Out) to 2x3. • 13.6 - 15 W: In rare cases when the power drops between 13.6 and 15 W and further power conservation is necessary, the device reduces the speed on its active Ethernet interface from 10/100/1000 Mbps to 10/100 Mbps. • 0 - 13.6 W: If there is a problem with the PoE switch or Ethernet cable and the power falls between 0 and 13.6 W, the device disables its wireless interfaces and returns its ETH0 and ETH1 interfaces to 10/100/1000 Mbps speeds. **Note:** When using smart PoE, the maximum power consumption setting must be set to **No limitation** (the default). Manually setting the PoE maximum power consumption level to anything else overrides smart PoE and essentially disables it.
Enable PCI Wireless Control Data Collection	Enable this feature to collect data about MAC DoS, IP DoS, and MAC filter violations in PCI compliance reports. Select the check box.
Accept ICMP Redirect Message	Enable this feature to accept ICMP redirect messages from routers on their subnet. Select the check box. By default, devices reject ICMP redirects because crafted ICMP redirect messages can be maliciously used to cause a victim host to send traffic to an attacker's host or even back to the victim itself, which is what occurs during a WinFreeze attack. However, you can enable this feature if you believe that your network is safe from such threats and you want multiple routers on the local subnet to be able to update the routing table on devices.

Table 60: System Settings (continued)

Setting	Description
Report client information gathered from captive web portals	Enable this feature to require devices to forward client information (such as name and email address) to ExtremeCloud IQ (New), where the information is logged as an event. Select the check box.
Hostname in Beacon	Activate iBeacon for or APs that have internal iBeacon transmitters and that belong to a network policy. Slide the toggle to **ON**. To use this setting, you must first define the iBeacon service in the associated network policy and then turn it on via the **Device Management** page.

Authentication Settings Management Options

Authentication settings specify the database location for storing administrator accounts, and control authentication for administrators.

Table 61: Authentication Settings

Setting	Description
Extreme Networks Device Admin Authentication	Specify the location of the database storing administrator accounts with which the AP authenticates administrators when they log in. Choose one of the following options: • **Local**—Stores admin accounts locally on the APs. • **RADIUS**—Stores admin accounts remotely on RADIUS authentication servers. • **Both**—Stores admin accounts both locally and remotely. If one or more RADIUS servers are already in place, for convenience and security, you can keep all the accounts there and configure the AP to look up administrators on those servers. **Note:** Be careful about using the RADIUS option. If all the AP admin accounts are on a RADIUS server and the device cannot connect to it, attempts by administrators to log in to the device fail. If there is no central RADIUS server containing a user database, or if you prefer to keep the admin accounts locally on the AP, select **Local**. To use accounts located on an external RADIUS server and locally on the device, select **Both**. In this case, the device authenticates administrators by first checking accounts on the external RADIUS servers specified in the RADIUS profile, and then by checking accounts stored on the local database second.
Private PSK Server Auto-Save Interval	Type the length of time that a device acting as a private PSK server automatically saves its list of private PSK-to-client MAC address bindings to flash memory. Depending on how frequently the server is binding private PSKs to client MAC addresses, you can make the interval as short as 60 seconds or as long as 3600 seconds (1 hour).
MAC Address Format	Define the **MAC Address Format**: • **Delimiter**—Choose the type of delimiter: Colon (:), Dash (-), or Dot (.). • **Style**—Choose **No delimiters**, **Two delimiters**, or **Five delimiters**. • **Case Sensitivity**—Choose between **Lower Case** and **Upper Case**. Some servers only accept MAC addresses in a particular format. These parameters control MAC authentication for local users on an Extreme Networks RADIUS server. For

Table 61: Authentication Settings (continued)

Setting	Description
	example, if you set case sensitivity as lower case and store local users with upper case MAC addresses for their user names and passwords, MAC authentication checks fail. By default, a device formats MAC addresses using lower case without any delimiter; for example: 0016cF8d55bc. You can reformat this address by making the following selections: Colon, no delimiter, upper case: 0016CF8D55BC Colon, two-delimiter, upper case: 0016:CF8D:55BC Colon, five-delimiter, upper case: 00:16:CF:8D:55:BC Dash, five-delimiter, upper case: 00-16-CF-8D-55-BC Dot, five-delimiter, upper case: 00.16.CF.8D.55.BC

Related Links

Configure Management Options on page 152

Configure Traffic Filters Policy Settings

After you enable **Traffic Filter** in the network policy, you can re-use an existing Traffic Filter object, or configure the settings manually.

This task is part of the network policy configuration workflow. Use this task to configure **Traffic Filter** policy settings for a network policy.

1. Go to **Configuration** > **Network**.
2. Select an existing network policy, and then select , or to add a new one, select ..
3. From the **Management Settings** menu, select **Traffic Filter**.
4. Toggle the **Traffic Filter** setting to **ON**, and configure the settings.
5. (Optional) To use an existing filter, select **Re-use Traffic Filter Settings**, , and then choose an existing filter.
6. Configure the Traffic Filter Settings on page 162.
7. Select **SAVE**.

Related Links

Traffic Filter Settings on page 162
Configure Policy Settings on page 135

Traffic Filter Settings

Table 62: Settings for Traffic Filters

Setting	Description
Name	Type a **Name** for the new Traffic Filters object.
Description	Type a **Description** for the new Traffic Filters object.

Table 62: Settings for Traffic Filters (continued)

Setting	Description
IQ Engine APs, Routers and Switches	
Control the following types of traffic to devices	Select the corresponding check boxes to enable the selected types of traffic. • **Enable SSH**: Permit an SSH connection to the mgt0 interface. By default, SSH is enabled. • **Enable Telnet**: Permit a Telnet connection to the mgt0 interface. By default, Telnet traffic is disabled. • **Enable Ping**: Permit ICMP echo requests (pings) to reach the mgt0 interface. By default, pinging mgt0 is allowed. • **Enable SNMP**: Permit an SNMP connection to the mgt0 interface. By default, SNMP is disabled. • **Enable Inter-station Traffic**: (Only for APs) Permit inter-station traffic between APs.
Non-IQ Engine Switches (Dell & Extreme Networks)	
Control the following types of traffic to devices	Select the corresponding check boxes to enable the selected types of traffic. • **Enable Telnet**: Permit a Telnet connection to the mgt0 interface. By default, Telnet traffic is disabled. • **Enable Ping**: Permit ICMP echo requests (pings) to reach the mgt0 interface. By default, pinging mgt0 is allowed. Does not apply to N1100 series devices.

Related Links

Configure Traffic Filters Policy Settings on page 162

Configure MGT IP Filter Policy

After you enable MGT IP Filter in the network policy, you can reuse an existing MGT IP Filter object, or configure the settings manually.

This task is part of the network policy configuration workflow. Use this task to configure **MGT IP Filter** policy settings for a network policy.

1. Go to **Configuration** > **Network**.
2. Select an existing network policy, and then select , or to add a new one, select ..
3. From the **Management Settings** menu, select **MGT IP Filter**.
4. Toggle the **MGT IP Filter** setting to **ON**.
5. To use an existing filter, select **Re-use MGT IP Filter** and then select an existing filter.
6. Configure the MGT IP Filter Settings on page 164.
7. To add a new IP Object, select **Add Another IP Object**, configure the settings, and then select **SAVE SUBNET**.

   See MGT IP Filter Settings on page 164.
8. Select **SAVE MGT IP FILTER**.

Related Links

MGT IP Filter Settings on page 164
Configure Policy Settings on page 135

MGT IP Filter Settings

Table 63: Settings for MGT IP Filters

Setting	Description
Name	Type a **Name** for the filter.
Description	(Optional) Type a **Description** for the filter. Although optional, entering a description is helpful for troubleshooting and for identifying the filter.
Permitted Management Traffic Source	
Available IP Objects	IP objects in this list are preconfigured. To add to the list, select **ADD ANOTHER IP OBJECT**. See Table 64 on page 164. Select an IP address in the **Available IP Objects** column, and then select the single arrow (**>**) to move it to the **Selected IP Objects** column. Use the double arrow **>>** to move all available IP addresses.
Selected IP Objects	IP objects in this list are the IP addresses from which administrators can access the devices. Select an IP address in the **Selected IP Object** column, and then select the single arrow (**>**) to move it to the **Available IP Objects** column. Use the double arrow **>>** to move all available IP addresses.

Table 64: Settings for IP Objects

Setting	Description
Name	(Required) Type a **Name** for the new IP object.
Subnet	(Required) Type the new **IP Address** and **Subnet**.

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. ExtremeCloud IQ (New) 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**.
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.

   When ExtremeCloud IQ (New) updates the IQ Engine firmware for multiple, same-model APs, it can send the first upgrade to one device and enable the other devices using the same firmware to get their image from that first updated (seed) device.
7. Select **PERFORM UPDATE**.

Related Links

Configuration | Network on page 133

Configure the SSID for a Standard Wireless Network

A network policy can include one or more wireless networks, commonly referred to as SSIDs. A wireless network SSID is an alphanumeric string that identifies a wireless network, including the set of authentication and encryption services that wireless clients and access point devices use to communicate with each other over the network.

This task is part of the network policy configuration workflow. Use this task to configure an SSID for a standard wireless network.

1. Go to **Configuration** > **Network**.
2. Select an existing network policy, and then select , or to add a new one, select ..
3. Select **2 Wireless**.
4. (Optional) Select **Assign SSIDs using Classification Rules**.
   a. To add a classification rule, select .
   b. To specify an existing classification rule, select .

For more information, see Configure Classification Rules on page 148

Note
If you have more than 16 SSIDs, the check box appears dimmed. To enable the check box, reduce the number of SSIDs to fewer than 16.

5. Select an existing SSID and then select , or to add a new one, select ..
6. Type a **Name** for the wireless network SSID.

   ExtremeCloud IQ (New) and IQ Engine use this name to group all the settings related to this wireless network, such as required and optional data rates, DoS policies, MAC filters, and the broadcast SSID.
7. Type a **Broadcast Name** for this wireless network, or accept the one automatically derived from the SSID name.

   Clients discover this broadcast name from beacons and probe responses.
8. Select SSID radio broadcast bands:
   - **Wi-Fi 0 Radio (2.4 GHz or 5 GHz)**: Broadcast the SSID based on the configuration of the Wi-Fi 0 radio.
   - **Wi-Fi 1 Radio (5 GHz only)**: Broadcast the SSID on the Wi-Fi 1 radio operating in the 5 GHz band. Most Extreme Networks devices have two radios: radio 1 is bound to Wi-Fi 0 and radio 2 is bound to Wi-Fi 1. Radio 1 generally operates in the 2.4 GHz band but can also operate in the 5 GHz band on some models. Radio 2 operates in the 5 GHz band.

     Note
     Mapping an SSID to both radio types is a good approach if the devices need to work with some wireless clients that only support 802.11n/b/g, and others that only support 802.11ac/n/a/ac/x. In this case, both Wi-Fi 0 and Wi-Fi 1 must be in access mode or dual mode. If hive members need to support wireless backhaul communications with each other and you want both interfaces to provide client access, then one of the wireless interfaces must be able to provide both access and backhaul links.

   - **Wi-Fi 2 Radio (6 GHz only)**: This option currently supports only Enterprise WPA3, Personal WPA3, and Open Enhanced. After you select this check box, a message reminds you that WiFi2 supports only 6Ghz band for client access. The configuration menu shows only options applicable to 6Ghz.

9. Select an authentication method and configure the settings.

Table 65: Authentication methods

Method	Configuration
SSID Authentication	• Select **Enterprise WPA/WPA2/WPA3** to require users to authenticate by using a certificate or entering a username and password, and validating against a RADIUS server. Only WPA3 is supported for 6 GHz devices. See Configure Enterprise SSID Authentication on page 178. • Select **Personal WPA/WPA2/WPA3** to require users to enter a shared passphrase to authenticate. Only Personal WPA3 is supported for 6 GHz devices. See Configure Personal SSID Authentication on page 184. • Select **Private Pre-Shared Key** to allow the use of multiple passphrases on a single SSID. See Configure Private Pre-Shared Key SSID Authentication on page 188. • Select **Open** (not available for 6 GHz) so users do not use any form of authentication, but can be directed to a captive web portal before they can access other network resources. • Select **Enhanced Open** (available only for 6 GHz devices) to provide improved data privacy in open Wi-Fi networks, such as Wifi hotspots and guest WLANs. **Note:** For security reasons, WEP configuration is no longer available in the UI. If you require WEP for business continuity purposes, you can enable it via Supplemental CLI.
MAC Authentication	See Configure MAC Authentication on page 177.

10. For an Enterprise or Personal SSID, configure the **Protected Management Frames** settings.

Note

Available settings depend on the **Key Management** selection (WPA, WPA2, or WPA3).

Table 66: Protected Management Frames Settings

Setting	Description
802.11w	Toggle **802.11w** to **ON** to prevent forgery and retransmission of management frames.
Use of 802.11w is	If you select a WPA3 level of security, 802.11w is enabled by default at a Mandatory level. The menu and check box appear dimmed. If you select a WPA3 level of security with Transition Mode enabled, 802.11w will be enabled as Optional.

Table 66: Protected Management Frames Settings (continued)

Setting	Description
Use 802.11w protection for broadcasts/ multicasts	If you select WPA2 level of security, 802.11w is disabled by default, with option to enable.
Enable Beacon Protection	Enhances Wi-Fi security by safeguarding beacon frames against tampering. **Note: Enable Beacon Protection** is supported on AP4020/AP5020 only.

11. To create a captive web portal for open authentication, see:
    - Customize and Preview Cloud-based Captive Portal Settings on page 198
    - Customize and Preview Device-based Captive Web Portal Settings on page 191
    - Import Captive Web Portal HTML Files on page 199
12. If you intend to authenticate via RADIUS servers, either select an existing **Default RADIUS Server Group** from the current list or select the plus sign to add a new group.

    See Configure RADIUS Server Settings on page 202 to add a wireless network (SSID)-specific RADIUS object. See Configure an External RADIUS Server on page 203 to add an external RADIUS common object.

    To use classification, select **Apply RADIUS server groups to devices via classification**.
13. If you intend to authenticate via user groups (Enterprise only), turn on **Authentication with ExtremeCloud IQ Authentication Service**.
14. If you intend to use Zero Trust Network Access (ZTNA), turn on **Authentication with Extreme Platform ONE Security**.

    Note
    Authentication with ExtremeCloud IQ Authentication Service and **Authentication with Extreme Platform ONE Security** are mutually exclusive settings.

15. Select an existing user group from the list, or select + and configure the settings.

    See Cloud User Group Settings on page 169 and Local User Group Settings on page 171.
16. Use the existing **Default User Profile**, select a profile from the list, or select + and configure the settings..

    See Add a User Profile on page 174.
17. (Optional) Under **User Access Settings**, select the **Apply a different user profile to various clients and user groups** check box.

    See Apply Different User Profiles to Clients and User Groups on page 227.
18. To customize the **SSID Availability Schedule**, select the **Restrict the availability of this SSID to selected schedules** check box to enable SSID schedules.
19. Select **Customize**.

    To create a new schedule, select +, and see Schedule Settings on page 226.

20. To customize **Advanced Access Security Controls**, see Customize Advanced Access Security Controls on page 228.
21. To customize **Optional Settings** (not available for 6 GHz), see Customize Wireless Network Optional Settings on page 231.
22. Toggle **Client Monitor ON** (default) to enable a device to detect client issues, and report client connection activities and problems to ExtremeCloud IQ (New).
23. Toggle **Client Monitor ON** (default) to
24. Select **SAVE**.

Continue configuring the network policy.

Related Links

Configure Classification Rules on page 148
Configure Enterprise SSID Authentication on page 178
Configure Personal SSID Authentication on page 184
Configure Private Pre-Shared Key SSID Authentication on page 188
Customize and Preview Cloud-based Captive Portal Settings on page 198
Customize and Preview Device-based Captive Web Portal Settings on page 191
Import Captive Web Portal HTML Files on page 199
Configure MAC Authentication on page 177
Configure RADIUS Server Settings on page 202
Configure an External RADIUS Server on page 203
Cloud User Group Settings on page 169
Local User Group Settings on page 171
Apply Different User Profiles to Clients and User Groups on page 227
Schedule Settings on page 226
Customize Advanced Access Security Controls on page 228
Customize Wireless Network Optional Settings on page 231

Cloud User Group Settings

When you configure a user group for an Enterprise 802.1X SSID, the password database always resides in the cloud. For a user group for a Private Pre-Shared Key (PPSK) SSID, the password database can reside in the cloud or on all SSID APs. The following settings are available when you configure a cloud-based user group.

Table 67: Settings for Cloud User Groups

Setting	Description
User Group Name	Type a name for the user group.
Password DB Location	Select **Cloud** for a cloud-resident password database.
Password Type	Select **PPSK** or **RADIUS**.
Description	Type an optional **Description** for the user group.

Table 67: Settings for Cloud User Groups (continued)

Setting	Description
Enable CWP Register	Select **Enable CWP Register** to require users in this user group to log in using a captive web portal. Available only if a captive web portal is enabled for this SSID.
PCG Use	(Optional) Available only for the PPSK password type. Select **Enable use for Private Client Group**.
Password Settings	
Generate Password Using	(Required) Select any combination of characters that you want to include in the password: **Letters**, **Numbers**, and **Special Characters**.
Enforce the use of	Select one of the password enforcement options from the menu: • **All selected character types** • **Any selected character types** • **Only one character type**
PSK Generation Method	Available only for the PPSK password type. Select **Password Only** or **User String Password** from the menu. With the **User String Password** option, you can include the user name and a string of characters in front of the generated Private PSKs. If the password generation method is **Password Only**, then the PPSK password can be between eight and 63 characters. If the generation method is **User + String + Password**, the maximum passphrase for the Private PSK can be between eight and 31 characters.
Generated Password Length	Select the length for automatically-generated passwords for this user group. Range: 8–63
Concatenating String	Available only for the **User String Password** PSK Generation Method. Range: 0–8 Use this string to generate PPSKs as User name + Character String + Password. For example, if you enter `Extreme`, as the string, then the generated PPSKs are **<User name>Extreme<Password>**.
Expiration Settings	

Table 67: Settings for Cloud User Groups (continued)

Setting	Description
Account Expiration	Select one of the options from the menu: • **Never Expire** • **Valid During Dates** Use the calendar and time controls to specify the **Start** and **End** dates and times. • **Valid For Time Period** Specify the time period for which the password is valid after **ID Creation** or **First Login**. Type the number of **hours**, **days**, or **weeks**. Select the unit of time and the **after**-condition from the menus. Optionally, select **Renew user credentials**. To delete credentials after a specific time period, select **Delete credentials after**, type a value, and then select the unit of time from the menu. • **Daily** Use the **Start** and **End** controls to specify the daily time period.
Action at Expiration	Not available for accounts set to never expire. Select **Access Rejected** to have ExtremeCloud IQ (New) block users from renewing their credentials. Select **Show Expiration Message** to have ExtremeCloud IQ (New) present to users an on-screen prompt that they can use to renew their credentials.
Delivery Settings	
Deliver Access Key by	Select the methods for delivery of the access key. Select one or both: • **Text Messages (SMS)** • **Email** Use the menus to select an email template for each method.

Related Links

Configure the SSID for a Standard Wireless Network on page 165

Local User Group Settings

When you configure a user group for an Enterprise 802.1X SSID, the password database always resides in the cloud. For a user group for a Private Pre-Shared Key (PPSK) SSID,

the password database can reside in the cloud or local on all SSID APs. The following settings are available when you configure a cloud-based user group.

Table 68: Settings for Local User Groups

Setting	Description
User Group Name	Type a name for the user group.
Password DB Location	Select **Local** to store login credentials on all APs using this SSID. You must select **Local** to create a private client group in this user group. See Classification Rules Overview.
Password Type	Select **PPSK** or **RADIUS**.
Description	Type an optional **Description** for the user group.
Set the maximum number of clients per private PSK	(Optional) Available only for the PPSK password type. Select **Set the maximum number of clients per private PSK** to set per-user PPSK limits for different users in the same wireless network (SSID). Because you can set per-user PPSK limits for different users in the same SSID, you no longer need to configure an SSID for each user group (for instance, with three devices per employee). You can set multiple per-user PPSK limits can be set in the same (SSID). Range: 0-15, 0 = no limit
PCG Use	(Optional) Available only for the PPSK password type. Select **Enable use for Private Client Group**.
PPSK Classification Use	(Optional) Available only for the PPSK password type. Select **Enable user for PPSK Classification only** to create a single SSID and distribute unique guest passwords for each location. Use this option with a **Private Pre-Shared Key** SSID Authentication network policy. See Configure Private Pre-Shared Key SSID Authentication on page 188 for more information.
Password Settings	
Generate Password Using	(Required) Select any combination of characters that you want to include in the password: **Letters**, **Numbers**, and **Special Characters**.
Enforce the use of	Select one of the password enforcement options from the menu: • **All selected character types** • **Any selected character types** • **Only one character type**

Table 68: Settings for Local User Groups (continued)

Setting	Description
PSK Generation Method	Available only for the PPSK password type. Select **Password Only** or **User String Password** from the menu. With the **User String Password** option, you can include the user name and a string of characters in front of the generated Private PSKs. If the password generation method is **Password Only**, then the PPSK password can be between eight and 63 characters. If the generation method is **User + String + Password**, the maximum passphrase for the Private PSK can be between eight and 31 characters.
Generated Password Length	Select the length for automatically-generated passwords for this user group. Range: 8–63
Concatenating String	Available only for the **User String Password** PSK Generation Method. Range: 0–8 Use this string to generate PPSKs as User name + Character String + Password. For example, if you enter `Extreme`, as the string, then the generated PPSKs are **<User name>Extreme<Password>**.
Expiration Settings	
Require Authentication After	To force re-authentication after a session is inactive for some time, select **Require Authentication After** and enter a time in the minutes field.
Account Expiration	Select an option from the menu: • **Never Expire** • **Valid During Dates** (Available only for PPSK.) Use the calendar and time controls to specify the **Start** and **End** dates and times.
Action at Expiration	Not available for accounts set to never expire. Select **Access Rejected** to have ExtremeCloud IQ (New) block users from renewing their credentials. Select **Show Expiration Message** to have ExtremeCloud IQ (New) present to users an on-screen prompt that they can use to renew their credentials.
Delivery Settings	
Deliver Access Key by	Select the methods for delivery of the access key. Select one or both: • **Text Messages (SMS)** • **Email** Use the menus to select an email template for each method.

Related Links

Configure the SSID for a Standard Wireless Network on page 165

Add a User Profile

Configure an SSID for a standard wireless network. See Configure the SSID for a Standard Wireless Network on page 165.

User profiles define user traffic settings on APs. After a user associates with a device, the device assigns the user to a user profile. The device can make this assignment dynamically from attributes returned by a RADIUS authentication server or statically by using the default user profile set.

This task is part of the SSID configuration workflow. Use this task to add a user profile for an SSID, as part of a network policy.

1. While configuring an SSID, go to **User Access Settings** > **Default User Profile**.
2. To add a new user profile, select .
3. Type a **Name** for the profile.
4. For **Connect to**, select **VLAN** or **VLAN Group**.
5. To select an existing VLAN or VLAN group, select and choose an existing object, or to add a new one, select .

   See Configure VLAN Settings on page 213 for more information.
6. On the **Security** tab, apply IP or MAC firewall rules.

   For more information, see Configure User Profile Security on page 215.
7. On the **Traffic Tunneling** tab, enable generic routing encapsulation (GRE) traffic tunneling for a user profile.

   For more information, see Configure User Profile Traffic Tunneling on page 219.
8. On the **QoS** tab, set rate limits and traffic forwarding rules for each traffic class.

   For more information, see Configure User Profile QoS on page 223.
9. On the **Availability Schedule** tab, define user profile availability for specific dates, days, and times.

   For more information, see Configure an Availability Schedule on page 225.
10. On the **Client SLA** tab, enable devices to monitor client throughput and take action if the actual throughput is below the targeted minimum level.

    For more information, see Configure User Profile Client SLA on page 226.
11. On the **Date/Time Limit** tab, configure access restrictions for users based on the user's assigned profile.

    For more information, see Configure User Profile Access Restrictions on page 227.
12. Select **Save User Profile**.

Related Links

Configure VLAN Settings on page 213
Configure User Profile Security on page 215
Configure User Profile Traffic Tunneling on page 219
Configure User Profile QoS on page 223
Configure an Availability Schedule on page 225
Configure User Profile Client SLA on page 226
Configure User Profile Access Restrictions on page 227

SSIDs

An SSID is an alphanumeric string that identifies a wireless or guest network. For information about adding wireless networks, see Configure the SSID for a Standard Wireless Network on page 165.

To view the list of configured SSIDs, go to Go to **Configuration** > **Network**, choose an existing network policy, and then select **2 Wireless**.

The SSID table displays the following information about your network SSIDs:

- **SSID Name**: The name assigned to an SSID when it was created. This is the name that APs advertise in beacons (unless the SSID is in stealth mode) and respond to during client probes.
- **SSID Broadcast Name**: This name can be the same as the SSID Name.
- **Access Security**: The method that the SSID uses to secure network access.
- **VLAN**: The VLAN to which this SSID is assigned.
- **Default User Profile**: The user profile that is assigned to this SSID.
- **Used By**: Displays the number of APs and network policies that use this SSID. Hover over any non-zero number to see details.

Related Links

Configure the SSID for a Standard Wireless Network on page 165

SSID Usage in Standard Wireless Networks

As part of configuring a standard wireless network, you must determine how authentication takes place. You can choose SSID authentication or MAC authentication. MAC Authentication is typically used to support legacy clients.

Note
Client mode radios use only PSK or Open SSID authentication.

SSID Authentication

SSID Authentication offers the following types of access security methods:

- **Enterprise WPA/WPA2/WPA3** requires users to authenticate by entering a user name and password, validated against a RADIUS server. Only WPA3 is supported for 6 GHz devices. See Configure Enterprise SSID Authentication on page 178.
- **Personal WPA/WPA2/WPA3** requires users to enter a shared PPSK to authenticate. Only Personal WPA3 is supported for 6 GHz devices. See Configure Personal SSID Authentication on page 184.
- **Private Pre-Shared Key** requires users to authenticate by entering a PPSK unique to each user (not available for 6 GHz). See Configure Private Pre-Shared Key SSID Authentication on page 188.
- **OPEN** (not available for 6 GHz) or **Enhanced Open** does not require users to use any form of authentication, but can direct them to a captive web portal before they can access other network resources. **Enhanced Open** is available only for 6 GHz devices.

MAC Authentication

In Extreme Networks, MAC authentication works by checking a client MAC address against a RADIUS server. The RADIUS server, or an external database with which the RADIUS server communicates, must have an entry with the client MAC address as both user name and password. If the client MAC address matches the entry, it is authenticated, and the AP allows it to access the network as determined by the user profile.

MAC authentication can provide an additional or sole means of authentication. If an SSID employs MAC authentication with another type of access control—PPSK or a captive web portal—MAC authentication occurs first. If it is successful, the AP continues with the rest of the authentication procedure. Otherwise, the authentication process stops, the AP denies network access to the client, and the AP disassociates the client. If you enable MAC authentication and use an open SSID, then MAC authentication becomes the sole means of access control. See Configure MAC Authentication on page 177.

Related Links

Configure the SSID for a Standard Wireless Network on page 165

Configure Private Client Group Options

First, Configure Private Pre-Shared Key SSID Authentication on page 188.

This task is part of the network policy configuration workflow. Use this task to to configure the options for Private Client Groups.

1. On the **2 Wireless** page for the policy, under **SSID Usage**, select **Private Pre-Shared Key**.
2. Select **Private Group Options**.
3. Select **AP-Based** or **Key-Based**.

   AP-Based PCG mode requires a unique user and shared keys. This mode supports common shared devices within personal network spaces. It also requires room assignments for AP anchoring and traffic tunneling.

   Key-Based PCG requires one password used by the entire device group. Key-based PCG does not require room assignments for AP anchoring and traffic tunneling.

4. If you selected **Key-Based**, select the following **Private Client Groups Traffic Filtering** options as required.
   - **Enable Broadcast Filtering**: When selected, broadcast frames are not propagated beyond the current PCG domain.
   - **Enable Multicast Filtering**: When selected, multicast frames are not propagated beyond the current PCG domain.
     - **Enable MDNS** (multicast DNS) Filtering—When applied, multicast DNS frames are not forwarded outside the PCG domain.
     - **Enable SSDP** (Simple Service Discovery Protocol)—When enabled, SSDP frames are not forwarded outside of the PCG domain.

   When you select **Multicast Filtering**, both mDNS and SSDP filtering are auto-selected. If you do not select **Multicast Filtering**, you can independently select mDNS and SSDP filtering. This capability depends solely on site requirements.

Related Links

Configure Private Pre-Shared Key SSID Authentication on page 188
Configure the SSID for a Standard Wireless Network on page 165

Configure MAC Authentication

Create a standard wireless network (SSID).

MAC authentication checks a client MAC address against a RADIUS server, and can provide an additional, or sole means of authentication. If an SSID employs MAC authentication with another type of access control, such as PPSK, PSK, or a captive web portal, MAC authentication occurs first. If it is successful, the AP continues the authentication procedure. Otherwise, the authentication process stops, the AP denies network access to the client, and the AP disassociates the client. If you enable MAC authentication and use an OPEN SSID, then MAC authentication becomes the sole means of access control.

This task is part of creating or editing a network policy. Use this task to configure an MAC authentication.

1. Go to Go to **Configuration** > **Network**.
2. Select **MAC Authentication**, and then toggle the setting to **On**.
3. Select an **Authentication Protocol** to determine how the AP forwards authentication requests from users to an external RADIUS or Active Directory server:

   PAP: The AP sends an unencrypted password to the RADIUS server.

   Note
   When **Authentication with ExtremeCloud Universal ZTNA** is enabled in the SSID authentication settings, PAP is the only option. For more information, see Configure the SSID for a Standard Wireless Network on page 165.

   CHAP or MS CHAP V2: The AP sends the result of an operation it performs on the password, instead of the password itself, to the RADIUS or Active Directory authentication server. The authentication server performs the same operation, and then compares the results to see if they match.

4. Select , and choose an existing RADIUS Server Group, or to add a new one, select .

   For more information, see Configure an AAA Server Profile on page 205

Continue configuring a standard wireless network.

Related Links

Configure an AAA Server Profile on page 205

Configure Enterprise SSID Authentication

First, create a standard wireless network policy. For more information, see Configure the SSID for a Standard Wireless Network on page 165.

This task is part of the network policy configuration workflow. Use this task to configure the **SSID AUTHENTICATION** options for Enterprise SSID authentication.

1. On the **2 Wireless** page for the policy, select to add a new one.

   Alternatively, select an existing Enterprise SSID to edit.
2. Under **SSID Usage** > **SSID Authentication**, select **Enterprise**.

   This option requires users to authenticate by entering a user name and password, which the system checks against a RADIUS authentication server.
3. (Optional) Enable Hotspot 2.0 support.

   IQ Engine v10.7.4 is required. For more information, see Configure a Hotspot on page 179.
4. Select the required **Key Management** from the menu, or keep the default value.

   Key Management options:

   - **WPA3-802.1X** uses 128-bit encryption and automatically enables 802.11w Protected Management Frames, found in the **Advanced Access Security Settings** section of the Wireless Network configuration. If all wireless clients support WPA3, it is a better choice than WPA2.
   - **WPA2-802.1X** supports PMK caching and preauthentication (WPA does not). If the wireless clients support WPA2, it is the better choice over WPA. If you have a lot of legacy clients connecting to the network, WPA2 is a good choice.
   - **WPA-802.1X** does not support PMK caching or preauthentication. However, if you know that all the clients that are going to use this SSID were released before IEEE 802.11i was ratified in 2004 and only support WPA (not WPA2), this option allows the Extreme Networks devices to support them.

   The **Encryption Method** is **CCMP (AES)**. Counter Mode-Cipher Block Chaining Message Authentication Code Protocol (CCMP) uses AES (Advanced Encryption Standard) encryption. CCMP provides message integrity by combining counter mode with CBC (cipher block chaining) to produce a MAC (message authentication code).

5. Toggle **Transition Mode if Applicable** on.

   802.11w settings might have been changed. See Customize Advanced Access Security Controls on page 228 to confirm.

   Important
   Transmission mode with Auto Protected Frame Management across all radios (including 6 GHz) requires IQ Engine 10.7.3. If you push the Auto setting to an AP with IQ Engine below 10.7.3, the AP defaults to the best available 802.11w setting available, and Protected Management Frames is set to **Mandatory**.

   For more information, see Transition Mode Overview on page 186.
6. Select **SAVE**.

Related Links

Configure the SSID for a Standard Wireless Network on page 165

Configure a Hotspot

IQ Engine v10.7.5 or later is required.

Note
AP3000, AP5010, and AP5050 models support Hotspot 2.0.

Hotspot 2.0, also called Wi-Fi Certified Passport, is a standard for public access Wi-Fi that provides seamless and secure roaming among Wi-Fi networks and between Wi-Fi and cellular networks.

This task is part of the network policy configuration workflow. Use this task to configure a hotspot for an Enterprise SSID.

1. On the **2 Wireless** page for the policy, select an existing **Enterprise** SSID, or select to add a new one.
2. From the **Hotspot** list, select **Enabled**.
3. From the **Hotspot Profile** list, select an existing profile, or select to add a new one.
4. On the **Hotspot Identification** tab, configure the settings to identify the hotspot.

   For more information, see Hotspot Identification on page 180.
5. On the **SP Identification** tab, select an existing Service Provider Profile from the list, or select and configure the settings.

   For more information, see Service Provider Identification on page 181.
6. On the **Network Characteristics** tab, configure the settings.

   For more information, see Network Characteristics on page 183.
7. On the **Online Signup** tab, configure the settings.

   For more information, see Online Signup on page 184.
8. Select **SAVE**.

Related Links

Hotspot Settings on page 180

Hotspot Settings

Hotspot Identification

On the **Hotspot Identification** tab, configure the settings to uniquely identify the hotspot and specify the languages for the venue.

Table 69: Hotspot Identification settings

Setting	Description
Name	(Required) Type a name for the hotspot.
HESSID	(Required) Type the Homogenous Extended Service Set Identifier (HESSID) for the Hotspot 2.0 network. One SSID can be used across multiple WLANs (BSS). A Beacon with the same {HESSID, SSID} pair belongs to same WLAN. The {HESSID, SSID} pair must be unique for each WLAN. By default, the HESSID is the MAC address of the controller Ethernet port. Hotspots can have the same HESSID as long as the SSID is unique. If you configure the HESSID manually, we recommend using an AP BSSID as the HESSID. In a mobility domain, manually configure the HESSID to a unique value, to differentiate it from the value used in the WLAN of the controller.
Domain	(Required) Type the Fully-Qualified Domain Name (FQDN) for the Hotspot 2.0 network. (Default: empty string) Domain names in the domain name list might contain sub-domains. If the FQDN of the service provider is not in the domain name list but is in the realm list, mobile devices that use that service provider are considered to be roaming.
Venue Info	Describe the venue. From the lists of predefined values, first select the category of the venue, and then select the subtype. **Example:** Institutional, Hospital Select +, configure the settings, and then select **ADD**.
Operator Name	(Required) Type the name of the venue operator.
Venue Name	(Required) Type the name of the venue.
Language	(Required) Select a language from the list. You can configure up to four languages for each venue.

Service Provider Identification

On the **SP Identification** tab, configure the settings to identify the service provider and configure authentication. Select existing **Service Provider Profiles**, or select + to add a new Service Provider Profile.

Note
Keep your DNS server records up to date so that mobile devices can resolve the server domain names (FQDN).

Mobile devices with a SIM or USIM credential, can obtain a realm from the hotspot NAI Realm list. While hotspot access usually requires 3GPP credentials, a targeted NAI home query is an efficient alternative approach. The device connection manager compares the realm information from the list to the information stored on the device. The connection manager uses the preconfigured user preferences and policy from the mobile device to make a decision between a hotspot AP or a non-hotspot AP, if both are available.

Table 70: Service Provider Profile Settings

Setting	Description
NAI Realm: The Network Access Identification (NAI) Realm list is a list of realms that can be successfully authenticated. Each realm may have up to four supported EAP methods. • Add all realms that can authenticate the login credentials or certificate credentials of a mobile device, including the realms of all roaming partners that are accessible from the hotspot AP. Include the realm of the home service provider. • Add a realm for the PLMN ID. This is the cellular network identity based on public land mobile network (PLMN) information. Select + and configure the settings.	
Realm	(Required) Type the Fully-Qualified Domain Name (FQDN) of the service provider. Wildcards are supported for realm. For example, you can enter *.extreme.area120.com, instead of entering specific realms.
EAP Method	From the list, select the Extensible Authentication Protocol (EAP) authentication type. Mobile devices provisioned to authenticate against the home service provider do not require the EAP methods configured for the NAI Realm List.
Description	Type a description for the realm. Although optional, descriptions can be helpful when you are troubleshooting your network.
Roaming Consortium: Use roaming consortium authentication when you do not know all the authenticated realms. Using identifiers unique to the organization in the beacon is a battery-efficient roaming method because ANQP queries are not required. Select +, configure the settings for the Roaming Consortium, and then select **ADD**.	

Table 70: Service Provider Profile Settings (continued)

Setting	Description
Consortium	(Required) Type the Roaming Consortium Organization Identifier (RCOI). Specify up to eight identifiers unique to the organization that are part of the MAC address.
Description	Type a description for the consortium. Although optional, descriptions can be helpful when you are troubleshooting your network.
3GPP CellularNetwork: Create a list of cellular network IDs in the form of mobile country code (MCC), mobile network code (MNC). This list establishes whether an AP has a roaming arrangement with the 3GPP service providers. Select ✚, configure the settings for a 3rd Generation Partnership Project (3GPP) mobile network, and then select **ADD**.	
MCC	(Required) Type the mobile country code (MCC).
MNC	(Required) Type the mobile network code (MNC).
Description	Type a description for the 3GPP mobile network. Although optional, descriptions can be helpful when you are troubleshooting your network.
Advanced Settings	Select the arrow to expand this section and configure the following settings: • **NAI Realm** • **Roaming Consortium** • **3GPP CellularNetwork** **Note:** Advanced Settings override the corresponding settings in the associated Service Provider profiles.

Network Characteristics

On the **Network Characteristics** tab, configure network settings to specify the type of access network, IP address type availability, WLAN metrics, and connection capabilities.

Table 71: Network Characteristics settings

Setting	Description
Access Network: From the list, select the type of access network: • **Private network**—An enterprise network with user accounts. • **Private network with guest access**—An enterprise network providing guest access. • **Chargeable public network**—(Default) Open to anyone but access requires payment. • **Free public network**—An open network, free of charge but may still require acceptance of terms of use (and may involve OSU servers with a captive portal).	
DGAF	Select **DGAF** to enable Downstream Group Addressed Forwarding for the access network. If enabled, the system forwards all downlink wireless broadcast ARP and multicast packets. (Default: disabled)
IP Address Type Availability: Mobile devices use information about IP address type availability to make network selection decisions. Select the level of restriction for each network type.	
IPV4	From the list, select the type of IPV4 address: • Not Available • Public • Port Restricted • Single NAT • Double NAT • Port Restricted Single NAT • Port Restricted Double NAT • Unknown
IPV6	From the list, select the type of IPV6 address: • Not Available • Available • Unknown
WLAN Metrics: Mobile devices use the WAN Metrics settings to make network selection decisions. The mobile device can determine whether necessary throughput is available from the hotspot before connecting. If the mobile device receives indication that the basic service set (BSS) is at capacity, the device will not associate with that AP.	
Link Status	From the list, select a status. (Up, Down, or Test)
Downlink Speed	Specify the download speed in kbps.
Uplink Speed	Specify the upload speed in kbps.
Connection Capability: Select , configure the settings, and then select **ADD**. Mobile devices use connection capability information to make network selection decisions by determining which services are blocked or supported at the hotspot.	
Protocol	From the list, select the network protocol.

Table 71: Network Characteristics settings (continued)

Setting	Description
Port Number	Type the port number.
Status	From the list, select a status. (Open, Closed, or Unknown)

Online Signup

With Online Signup (OSU), users who are not part of the provider network can manually connect to the hotspot. This feature also provides added security for users who want to connect anonymously.

From the **Network Authentication Type** list, select an authentication method and configure the settings.

Table 72: Online Signup settings

Setting	Description
Acceptance of Terms and Conditions—Redirection occurs after the user accepts the Terms and Conditions.	
Online Sign up—Authentication supports online enrollment.	
OSU SSID	Type the SSID for the online signup service.
CWP (Captive Web Portal)—Redirection occurs after the CWP authenticates the user.	
Redirection URL	Type the HTTP or HTTPS address for automatic redirection after authentication.

Related Links

Configure a Hotspot on page 179

Configure Personal SSID Authentication

First, create a standard wireless network policy. For more information, see Configure the SSID for a Standard Wireless Network on page 165.

This task is part of the network policy configuration workflow. Use this task to configure the **SSID AUTHENTICATION** options for Personal SSID authentication.

1. On the **2 Wireless** page for the policy, select **Personal** SSID Authentication.

   This option requires all users to authenticate by entering the same pre-shared key.

2. Choose one of the following **Key Management** options:
   - Select **WPA3 (SAE)** to negotiate using WPA3 with clients. If all the wireless clients support WPA3, it is a better choice than WPA2.
   - Select **WPA2-(WPA2 Personal)-PSK** to use WPA2 for key management.
   - Select **WPA-PSK** to use WPA for key management. WPA does not support PMK caching or pre-authentication, but if the clients were released before IEEE 802.11i was ratified and they support WPA (not WPA2), this option allows the Extreme Networks devices to support them.

   Note
   For more information, see Transition Mode Overview on page 186.

3. Choose one of the following **Method** options:
   - **HNP/H2E** (default): Enable both Hunting and Pecking (HNP) and Hash to Element (H2E).
   - **H2E**: Set the H2E method as the privacy method for the WLAN on all radios (2.4 GHz, 5 GHz and 6 GHz). This option applies only to 6E capable devices (AP4000, AP5010, AP5020, AP5050, AP3000, and 11ax portfolio).

     Note
     Ensure that networks defined with the option **H2E** are assigned to configuration Profiles of supported devices (AP4000, AP5010, AP5020, AP5050, AP3000, and 11ax portfolio).

   - **HNP**: Set the HNP method as the privacy method for the WLAN on all radios (2.4 GHz, 5 GHz and 6 GHz).
   - Select the **Enable AKM-24 (WiFi 7 Only)** checkbox to ensure compatibility and compliance with 802.11be.

     Note
     Applies only to AP4020 and AP5020 devices.

4. Select an **Encryption Method**.

   The **Encryption Method** for WPA3 and WPA2 is **CCMP (AES)**. Counter Mode-Cipher Block Chaining Message Authentication Code Protocol (CCMP) uses AES (Advanced Encryption Standard) encryption. CCMP provides message integrity by combining counter mode with CBC (cipher block chaining) to produce a MAC (message authentication code).

   Note
   When the SSID is configured for WPA3 (SAE), the encryption method is always set to 128-bit encryption.

   The **Encryption Method** for WPA-PSK is **TKIP**. Temporal Key Integrity Protocol (TKIP), uses RC4 as its cipher and provides a rekeying mechanism. TKIP ensures that every data packet is sent with a unique encryption key, which is a combination of an Interim Key/Temporal Key and a Packet Sequence Counter. TKIP provides more secure encryption than Wired Equivalent Privacy (WEP), and works on older or legacy WEP hardware with minor upgrades.

   Note
   ExtremeCloud IQ supports TKIP only for AP3000, AP3000X, AP4000, AP5010, AP5050D, AP5050U models.

5. Select an **SAE Group**.
6. Toggle **Transition Mode if Applicable** on.

   Note
   When enabled with 6 GHz: PMF is optional for 2.4 GHz and 5 GHz, but mandatory for 6 GHz. Requires IQ Engine version 10.8r4 or higher.

   For more information, see Transition Mode Overview on page 186.
7. For **Key Value**, enter the pre-shared key and **Confirm** it.

   The **Key Type** is **ASCII Key**.
8. (Optional) To show the **Key Value**, select **Show Password**.
9. Select **SAVE**.

Related Links

Configure the SSID for a Standard Wireless Network on page 165

Transition Mode Overview

Transition Mode eases the transition from WPA2 to WPA3 Wi-Fi security by connecting newer client hardware with the latest security standards, and permitting legacy client devices to access the same SSID using older standards.

Important
Transmission mode with Auto Protected Frame Management across all radios (including 6 GHz) requires IQ Engine 10.7.3. If you push the Auto setting to an AP with IQ Engine below 10.7.3, the AP defaults to the best 802.11w setting available, and Protected Management Frames is set to **Mandatory**.

There are three distinct types of transition modes, each functioning in its own unique way:

- **Open to Enhanced Open (OWE)**: Supports both OWE and open standards. Newer devices can connect using OWE, while older client devices can connect without encryption. This is provided through two distinct SSIDs: a visible open network and a similarly-named hidden OWE network. All clients attempt to join the visible open network, but clients that support OWE receive an an information element in the open network SSID probe response to join the hidden OWE network instead.
- **WPA2/WPA3 Personal** (PSK to SAE): Supports both WPA2 and WPA3 on a single passphrase protected SSID. Devices supporting WPA3 can connect using WPA3 with SAE, while older devices can still connect using WPA2 with PSK. 802.11w (Protected Frame Management, or PMF) is set to optional on these SSIDs, enabling newer clients to use Protected Frames, while older clients do not.
- **WPA2/WPA3 Enterprise**: Supports both WPA2-Enterprise and WPA3-Enterprise on the same SSID. While all clients use the same backwards-compatible encryption (AES 128), 802.11w is set to Optional on these SSIDs. Newer clients use PMF, while older clients do not.

Transition Mode is only supported on the legacy radio bands (2.4 and 5 GHz), while 6 GHz networks are required to use the newer security standards. To simplify the adoption and use of the same SSIDs across all radios, ExtremeCloud IQ intelligently applies PMF settings on an SSID within an Enterprise network, based on the selected security and radio settings.

Table 73: Transition Mode Security and Radio Settings

	Transition Mode	2.4/5 GHz Enabled	6 GHz Enabled	802.11w Setting
WPA2-Enterprise	N/A	Yes	N/A	Off
WPA3-Enterprise	No	Yes	No	Mandatory
WPA3-Enterprise	Yes	Yes	No	Optional
WPA3-Enterprise	No	Yes	Yes	Mandatory
WPA3-Enterprise	Yes	Yes	Yes	Auto*

Note
*Auto 802.11w requires IQ Engine 10.7.3 or newer.

Related Links

Configure the SSID for a Standard Wireless Network on page 165
Configure Enterprise SSID Authentication on page 178
Configure Personal SSID Authentication on page 184

Configure Private Pre-Shared Key SSID Authentication

First, create a standard wireless network policy. For more information, see Configure the SSID for a Standard Wireless Network on page 165.

A PPSK is a unique pre-shared key assigned to a user rather than to an SSID. With this approach, you can assign different PPSKs and user profiles to different users on the same SSID. If a user is no longer permitted to use the WLAN or a wireless client becomes lost, stolen, or compromised, you can revoke just that user's PPSK without having to reconfigure the PPSKs on all the other clients.

Note
ExtremeCloud IQ Connect does not support Private Pre-Shared Keys.

This task is part of the network policy configuration workflow. Use this task to configure Private Pre-Shared Key SSID authentication options.

1. On the **2 Wireless** page for the policy, under **SSID Usage**, select **Private Pre-Shared Key**.

   Private Pre-Shared Key SSID authentication uses WPA2-(WPA2 Personal)-PSK for **Key Management**.

   The **Encryption Method** for WPA2-(WPA2 Personal)-PSK is **CCMP (AES)**. Counter Mode-Cipher Block Chaining Message Authentication Code Protocol (CCMP) uses AES (Advanced Encryption Standard) encryption. CCMP provides message integrity by combining counter mode with CBC (cipher block chaining) to produce a MAC (message authentication code).
2. Select **Set the maximum number of clients per private PSK**, and then type the maximum number of simultaneous clients allowed for each PPSK user. (Range: 1 through 15, or type 0 for an unlimited number.)

   Note
   Setting the maximum number of clients per PPSK in the user group to a custom (non-zero) value overrides this setting in the SSID.

3. Select **MAC binding**, and then select an Extreme Networks AP from the menu to define it as a PPSK server.

   When you enable this option, an Extreme Networks AP functions as a PPSK server and automatically binds MAC addresses to PPSKs. When the first client authenticates with a PPSK, the PPSK server creates an internal MAC address-to-PPSK binding list for it. If a second client authenticates with the same PPSK, the server automatically binds its MAC address to the PPSK and adds it to the list—if allowed by the configuration. You can configure a PPSK server to bind up to five MAC addresses to one PPSK so users can submit the same PPSK for all their smart phones, tablets, PCs, and other clients.

   Note
   Only APs that you previously configured with static network settings appear in the PPSK server list.

   A PPSK server stores PPSK users, binds multiple client MAC addresses to a PPSK, and automatically updates and tracks PPSK-to-MAC address bindings. The AP must be at the site location defined in the network policy. Extreme Networks APs (PPSK authenticators) at the same site contact this server when checking and requesting a user-submitted PPSK binding to the client MAC address.

4. To configure **Private Client Group Options**, see Configure Private Client Group Options on page 176.
5. Select **PPSK Classification Options** to use this network policy with associated local user groups.

Related Links

Configure Private Client Group Options on page 176
Configure the SSID for a Standard Wireless Network on page 165

Configure a Client Mode AP Profile using a Wired Connection and a Device Template

There must be at least one client mode profile configured before you can define a LAN-side AP radio for client mode.

You can set a radio on some AP models to client mode, which enables the AP to connect to existing open and PSK wireless networks, including third-party networks as a generic BYOD client. The method described here is recommended because it is often the fastest way to perform this task.

This task is part of the network policy configuration workflow. Use this task to configure a Client Mode Profile as part of an SSID for a network policy.

1. Go to **Configuration** > **Network**.
2. Select an existing network policy, and then select , or to add a new one, select ..
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.

4. Configure a client mode AP device template.
   a. From the **Wireless** > **Configuration Settings** menu, select **AP Template**.
   b. Select +, and then select an AP model to use as the client mode AP.
   c. Type a **Template Name**.
   d. Configure the WAN-side backhaul (WiFi0 or WiFi1) radio for **Backhaul Mesh Link**.
   e. Select **Client Mode** for the LAN-side client mode radio (WiFi0 or WiFi1).
   f. Select an existing client mode **Radio Profile** for the LAN-side client mode radio.
   g. Select **SAVE TEMPLATE**.
5. Add an Open, or PSK SSID, without a captive web portal.

   For more information, see SSID Usage in Standard Wireless Networks on page 175.

Related Links

SSID Usage in Standard Wireless Networks on page 175

Captive Web Portals

Extreme Networks supports two types of captive web portal (CWP):

- AP hosted portals on built-in web servers
- Extreme Networks hosted portals on cloud web servers

AP hosted portals support several user registration types (user authentication, self-registration to provide user data, use policy acceptance, self-registration to obtain a PPSK) plus an extensive set of configuration options. Cloud server hosted portals support two registration options: users can register by authenticating with their social media credentials or by requesting and submitting a PIN. A cloud-based CWP also has a simpler set of configuration options.

After defining a CWP, you must take one of two actions for your changes to take effect:

- For an AP hosted CWP, upload the configuration, web page files, and certificates (for secure communications using HTTPS) to your devices.
- For a cloud-based CWP, upload the configuration to your devices. ExtremeCloud IQ automatically stores the web page files and certificates in the cloud.

Note
To remove an existing login button that has already been deployed, you must resave the CWP and the Network Policy, and then redeploy the respective network policy to the device.

ExtremeCloud IQ can include multiple CWPs.

Related Links

Customize and Preview Cloud-based Captive Portal Settings on page 198
Customize and Preview Device-based Captive Web Portal Settings on page 191
Import Captive Web Portal HTML Files on page 199

Customize and Preview Device-based Captive Web Portal Settings

To configure a device-based captive web portal (CWP), you must first create a wireless network SSID with **Enterprise 802.1X** access security.

To join the SSID, users enter a user name and password, which are checked against a RADIUS server. When they open a web browser, the captive web portal opens to the **Use Policy Acceptance** (UPA) page. After the user agrees to the UPA, the AP allows them to access the rest of the network as determined by settings in the user profile applied to them.

This task is part of the network policy configuration workflow. Use this task to configure a device-based captive web portal.

1. Go to **Configuration** > **Network**.
2. Select an existing policy with open access security, and then select , or to add a new one, select ..
3. On the **Wireless** tab, select an existing SSID, and then select , or to add a new one, select ..
4. In the **SSID Usage** section, toggle **Enable Captive Web Portal** to **ON**.
5. Select **Captive Web Portal**, and then select the features.

Table 74: CWP features

Feature	Description
User Auth on Captive Web Portal	Authenticates users on the splash page.
Enable Self-Registration	Enables user registration on the splash page. **Note:** The **First Name** and **Last Name** fields cannot contain the following characters: $,`,<,>,+, and #.
Return Aerohive Private PSK	Issues a Private PSK for the user.
Enable UPA	Enables the display of the **Use Policy Acceptance** page.
Choose Authentication Type:	(This setting is not available if Self-Registration is enabled.) Authenticate using either a Radius Server, or redirect to an external URL.

6. Select **SELECT** to use an existing CWP, or select **ADD**.
7. Enter a **Name** for the CWP.
8. If you selected **Return Aerohive Private PSK**, configure the **PPSK Settings**.

Table 75: PPSK settings

Setting	Description
Choose Access SSID (Private PSK)	Select an access SSID from the menu.
Choose a PPSK Server	Select a PPSK server from the menu.

9. Select **CUSTOMIZE AND PREVIEW** > **CUSTOMIZATION AND PREVIEW**.

   Alternatively, you can import HTML files. See Import Captive Web Portal HTML Files on page 199.
10. Preview and Customize the Landing Page on page 196.
11. Preview and Customize the Use Policy Acceptance Page on page 197.
12. Preview and Customize the Success Page on page 197.
13. Preview and Customize the Error Page on page 197.
14. Enable or disable the **Success Page**.
15. Enable or disable **Redirect clients after a successful login attempt**.

    When enabled, ExtremeCloud IQ (New) sends successful clients to either the login page or to a specified URL.
16. Enable or disable the **Failure Page**, and choose the page to display the failure message.

    When enabled, ExtremeCloud IQ (New) displays the failure message on either the login page or the standard failure page. See Preview and Customize the Error Page on page 197.
17. Enable or disable **Redirect clients after a failed login attempt**.

    When enabled, ExtremeCloud IQ (New) sends unsuccessful clients to either the login page or to a specified URL.
18. Configure the default language, and additional languages.

Table 76: Supported languages

Setting	Description
Default Language	Select the **Default Language** from the menu.
Support Additional Languages	Select the additional languages you intend to support.

    ExtremeCloud IQ (New) adds the files required for the selected languages to the default CWP directory when you save the CWP.
19. Expand the **Advanced Configuration** section, and configure the settings.

Table 77: Advanced configuration settings

Setting	Description
Session Timer	Select **Display session timer alert before session expires** to display the session timer in the client browser. The timer shows the login status for the registered client, the time remaining in the session, and the elapsed time. You can choose to display the timer alert 5, 15, or 30 minutes before the session expires.
Network Settings	Select **Use default settings** to use the default IP address and netmask for the interface hosting the SSID with the captive web portal, or an admin-defined IP address and netmask. Select **Customize** to enter an IP address and netmask for each of the interfaces. You can use IPv4 or IPv6 addresses.

Table 77: Advanced configuration settings (continued)

Setting	Description
DHCP and DNS servers > **Use external servers**	
Use external servers	Select **Use external servers** to forward DHCP and DNS traffic from unregistered clients to external servers on the network. When enabled, unregistered and registered clients must be assigned to the same VLAN.
Override the VLAN ID used during registration	Select **Override the VLAN ID used during registration** and choose a previously defined VLAN ID from the drop-down list to assign to clients before and during the registration process. Select + to add a new VLAN ID.
DHCP and DNS servers > **Use Extreme Network Devices**	
Use Extreme Networks Devices	Select **Use Extreme Network Devices** to forward DHCP and DNS traffic from unregistered clients to internal servers on the AP hosting the CWP. When enabled, unregistered and registered clients can be assigned to the same VLAN or to different VLANs, because unregistered clients use DHCP and DNS servers on the AP, and registered clients use servers on the network. Note: When the client of a previously unregistered guest first associates with the Guest Access SSID, the AP acts as a DHCP server, DNS server, and web server. Client network access is limited to the AP with which it is associated, and the client browser redirects to a registration page. After the guest registers, the AP stores the client MAC address as a registered client and allows the guest to access external servers.
Lease Time	Type the length of the DHCP lease assigned to the quarantined client of an unregistered guest, and choose the unit of time measure from the menu. DHCP clients typically renew at the midpoint of the lease. After the client successfully registers, the AP allows the next DHCP lease request to pass to an external DHCP server. Keeping the lease short allows the client to obtain new network settings soon after registering.

Table 77: Advanced configuration settings (continued)

Setting	Description
Renewal Response	From the menu, choose how you want the AP to respond to a DHCP lease renewal request for a nonexistent lease. • **Renew-NAK-Broadcast**: By default, the AP responds by broadcasting DHCPNAK messages. Choosing either this option or the unicast DHCPNAK option can accelerate the transition to an external DHCP server on the network, or back to a quarantined address after the client logs out or the session times out. • **Renew-NAK-Unicast**: Choose to have the AP respond by sending unicast DHCPNAK messages. Sending unicast messages can reduce traffic on the network; however, broadcasting the DHCPNAK is safer in environments where there is a large and uncontrollable variety of clients. • **Keep Silent**: Choose to have the AP ignore the renewal request completely and enable the external DHCP server to respond. With this approach, the transition between DHCP servers can be slightly longer.
Web Servers	
Registration Period	Set the length of time that a registered client with an active session remains registered. Type a value and choose the unit of time measure from the menu. If the client closes one session and later starts a new one while the AP still has a roaming cache entry for that client (one hour by default), the client does not have to register with the captive web portal again. If the client closes a session and starts a new session after the roaming cache entry has been removed, the client must complete the registration process again, even if the new session begins within the registration period.
Domain Name	Type the same domain name as the CN (common name) value in the server certificate that the CWP uses for HTTPS. The domain name must be a valid domain name that a DNS server can resolve to the IP address of the interface hosting the CWP. This option allows you to use a server certificate from a CA that supports domain names as CNs, but not IP addresses. **Note:** If the CN has a wildcard domain name that can match multiple valid domain names, enter one of the valid domain names instead of selecting **Override Web server domain name with CN value in the certificate**. For example, if the CN is *.aerohive.com, then you can enter something like `cwp.aerohive.com` in the Web Server Domain Name field, and the clients' browsers will not show a security warning when they make an HTTPS connection to the captive web portal.
Security	

Table 77: Advanced configuration settings (continued)

Setting	Description
Enable HTTPs	Select **Enable HTTPs** to enable HTTPS on the CWP.
HTTPS certificate	Select **Default-CWPCert.pem** for preloaded CWPs. The AP hosting the CWP then uses HTTPS to secure traffic between the client and its CWP server. The certificate file must have the following properties: • The file format must be PEM (Privacy Enhanced Mail). • It must contain a server private key stored in an unencrypted format. • It must contain a server certificate concatenated to the private key.
Override Web server domain name with CN value in the certificate	Select to replace the Web server domain name with the common name value in the certificate.
Client Redirection	
Use HTTP 302	Select **Use HTTP 302** to redirect code as the redirection method instead of JavaScript. This option is useful for clients accessing the network with mobile browsers.
Introduce a delay before redirecting after a successful login attempt	Specify how long the CWP displays the success page before initiating the redirection. Type a value in seconds.
Introduce a delay before redirecting after a failed login attempt	Specify how long the CWP displays the failure page before initiating the redirection. Type a value in seconds. **Note:** This redirection differs from that in the **Captive Web Portal Failure Page Settings** section, which the AP applies after a failed log in attempt.
Prevent the Apple CNA (Captive Network Assistant) application from requesting credentials	Select **Prevent the Apple CNA (Captive Network Assistant) application from requesting credentials** to bypass the Apple CNA application for redirect actions.

20.To create a walled garden, select , and configure the settings.

Table 78: Walled garden settings

Setting	Description
Service Type	Select one of the following options: • **Web**: Permit client access only to the World Wide Web. • **All**: Permit client access to the World Wide Web and all other servers. • **Advanced**: Permit client access only to the admin-defined IP object or host name. If you selected **Web** or **All**, paste IP addresses or host names separated by commas into the **Service Type** text box. Then select **ADD**. If you selected **Advanced**, configure the settings, and then select **ADD**.
IP Object/Host Name	Enter an IP object or host name of the external web server. Choose a previously-defined IP address or host name from the menu, enter a new IP address or domain name, or select and define a new one.
Service	Select the service from the menu: Web, All, or Protocol.
Protocol Number	(Protocol service only) Type a protocol number (from 0 to 255).
Port	(Protocol service only) Type a port number to define the type of service you want to permit.

21. Select **SAVE CWP**.

Return to the **Wireless Network** page to complete the network policy configuration.

Related Links

Import Captive Web Portal HTML Files on page 199
Configure the SSID for a Standard Wireless Network on page 165

Preview and Customize the Landing Page

This task is part of Customize and Preview Device-based Captive Web Portal Settings on page 191. Use this task to preview and customize the landing page for a device-based captive web portal.

1. Select **LANDING PAGE** to preview the landing page.
2. Select **CUSTOMIZE** to modify the landing page colors, logo, language, and message text.
3. Select **SAVE CUSTOMIZATION**.
4. Select the corresponding check boxes to enable fields and to specify which fields are required.
5. Select **SAVE CONFIGURATION**, or select **USE POLICY ACCEPTANCE**.

Next, Preview and Customize the Use Policy Acceptance Page on page 197.

Related Links

Customize and Preview Device-based Captive Web Portal Settings on page 191
Preview and Customize the Use Policy Acceptance Page on page 197

Preview and Customize the Use Policy Acceptance Page

This task is part of Customize and Preview Device-based Captive Web Portal Settings on page 191. Use this task to preview and customize the use policy acceptance page for a device-based captive web portal.

1. Select **USE POLICY ACCEPTANCE** to preview the page that displays the use policy.
2. Select **CUSTOMIZE** to modify the page colors, logo, language, and message text.
3. Select **SAVE CUSTOMIZATION**.
4. Select **SAVE CONFIGURATION**, or select **SUCCESS PAGE**.

Next, Preview and Customize the Success Page on page 197

Related Links

Customize and Preview Device-based Captive Web Portal Settings on page 191
Preview and Customize the Success Page on page 197

Preview and Customize the Success Page

This task is part of Customize and Preview Device-based Captive Web Portal Settings on page 191. Use this task to preview and customize the success page for a device-based captive web portal.

1. Select **SUCCESS PAGE** to preview the page that appears after a successful login.
2. Select **CUSTOMIZE** to modify the page colors, logo, language, and message text.
3. Select **SAVE CUSTOMIZATION**.
4. Select **SAVE CONFIGURATION**, or select **ERROR PAGE**.

Next, Preview and Customize the Error Page on page 197.

Related Links

Customize and Preview Device-based Captive Web Portal Settings on page 191
Preview and Customize the Error Page on page 197

Preview and Customize the Error Page

This task is part of Customize and Preview Device-based Captive Web Portal Settings on page 191. Use this task to preview and customize the error page for a device-based captive web portal.

1. Select **ERROR PAGE** to preview the page that appears after an unsuccessful login.
2. Select **CUSTOMIZE** to modify the page colors, logo, language, and message text.
3. Select **SAVE CUSTOMIZATION**.
4. Select **SAVE CONFIGURATION**.

Related Links

Customize and Preview Device-based Captive Web Portal Settings on page 191

Customize and Preview Cloud-based Captive Portal Settings

To configure a cloud-based captive web portal (CWP), you must first create a wireless network SSID with **Open** access security. For more information, see Captive Web Portals on page 190.

Extreme Networks provides two types of cloud-hosted CWPs. One controls network access by leveraging user credentials in social media services like Google and LinkedIn. The other type authenticates users by requiring them to enter a PIN, which is sent to them by email, to gain network access. Both CWP types are available in ExtremeCloud IQ (New).

This task is part of the network policy configuration workflow. Use this task to configure a cloud-based CWP.

1. Go to **Configuration** > **Network**.
2. Select an existing policy with open access security, and then select , or to add a new one, select ..
3. On the **Wireless** tab, select an existing SSID, and then select , or to add a new one, select ..
4. In the **SSID Usage** section, toggle the **Enable Captive Web Portal** setting **ON**.
5. Select **Cloud Captive Web Portal**.
6. To use social media services, select **Social Login**, or to require a PIN for logging in, select **Request a PIN**.

   If you require a PIN, ExtremeCloud IQ (New) sends a randomly generated PIN to authenticate the user.
7. Select an existing CWP or select **ADD**.
   a. If you selected **ADD**, enter a new **Name** for the CWP.
   b. Enter the length of time that the PIN remains valid.

      The validity period begins when ExtremeCloud IQ (New) receives the PIN request and can last from 1 to 24 hours.
   c. Enter an email address where you want ExtremeCloud IQ (New) to send daily reports about successfully authenticated users on this CWP.

      Each report is in CSV format and shows the login time (in UTC, or universal coordinated time) when the user submitted a PIN, the user name, and the MAC address of the client device used for the connection. ExtremeCloud IQ (New) sends a separate email for when there are no entries to report.
   d. Set the hour and minute when ExtremeCloud IQ (New) generates a daily report of successful user authentications.

      ExtremeCloud IQ (New) reports the time in UTC, and the report contains events for the previous 24 hours.
   e. Use the default CWP without customization, or toggle **Customize** to **ON** and select **PIN-Login-Example** to export the necessary files.
   f. Modify the files and import them in the **New Captive Web Portal** window.
   g. Select **Upload/Remove**, navigate to the files on your system and upload them.

h. Select **Done**.
i. Select the files you want to use for the **Login** and **Success** pages, and then select **SAVE CWP**.

   The imported files are immediately saved to ExtremeCloud IQ (New).

> **Note**
> If you previously completed the configuration with default files and uploaded the network policy to your APs, you do not need to upload the configuration again.
>
> If the customized files have the same name as the default files, the custom files overwrite the default files after import to ExtremeCloud IQ (New).

8. Select **Use a different captive web portal for various clients** to use other CWPs for different clients based on device classification and classification rules.
9. Select **Select a Classification Rule** to choose an existing rule, and then select **Link**.

   To add a new classification rule, select **Add a Classification Rule** and complete the steps. For more information, see Configure Classification Rules for a Device Template on page 289.

Return to the Wireless Network page to complete the network policy configuration.

Related Links

Configure Classification Rules for a Device Template on page 289
Configure the SSID for a Standard Wireless Network on page 165

Import Captive Web Portal HTML Files

To import an HTML file for a captive web portal (CWP), you must first create a wireless network SSID and enable CWP.

This task is part of the network policy configuration workflow. Use this task to to import an HTML file for your captive web portal configuration.

> **Note**
> **Import HTML** overrides the settings that are configured in **Customize and Preview**.

1. Go to **Configuration** > **Network**.
2. Select an existing policy, and then select , or to add a new one, select ..
3. On the **Wireless** tab, select an existing SSID, and then select , or to add a new one, select ..
4. In the **SSID Usage** section, toggle the **Enable Captive Web Portal** setting **ON**.
5. Select **Captive Web Portal**.
6. On the **New Captive Web Portal** page, select **IMPORT HTML**.
7. Select **UPA-Example** to download a template that you can modify.
8. Select an existing **Web File Directory**, or select **Create** and type a new file directory name.

9. Select **Upload/Remove**, navigate to the files on your system and upload them.
10. Select **DONE**.
11. Select a file to use for the **Login Page**.
12. Select a file to use for the **Success Page**.
13. (Optional) Select **Redirect clients after a successful login attempt**.
14. Select the files you want to use for the **Login** and **Success** pages, and then select **SAVE CWP**.

    There is no need for a failure page because error messages appear on the **Login** page rather than requiring navigation to a separate page. ExtremeCloud IQ (New) immediately saves the imported files.

Note
If you previously completed the configuration with default files and uploaded the network policy to your APs, you do not need to upload the configuration again.

If the customized files have the same name as the default files, the custom files overwrite the default files after import to ExtremeCloud IQ (New).

Return to the **Wireless Network** page to complete the network policy configuration.

Related Links

Configure the SSID for a Standard Wireless Network on page 165

RADIUS Authentication

RADIUS authentication is for use by Enterprise WPA/WPA2 802.1X and WEP 802.1X SSIDs, MAC authentication, and captive web portals that require user authentication. Extreme Networks devices use the wireless network (SSID) RADIUS server group for RADIUS lookups, unless there is a classification rule directing them to a different group based on location or other parameters. The servers in the group can be external RADIUS servers, Extreme Networks RADIUS servers, Extreme Networks proxy servers, or a combination of these three types.

Note
The WEP protocol is no longer effective for securing wireless networks. For security reasons, WEP configuration is no longer available in the UI. If you require WEP for business continuity purposes, you can enable it via Supplemental CLI.

Related Links

Configure a RADIUS Server Group on page 201
Configure RADIUS Server Settings on page 202
Configure an External RADIUS Server on page 203
Configure an Extreme Networks RADIUS Server on page 205
Configure a RADIUS Proxy Server Realm on page 211
Add an Active Directory Server on page 208

Add an LDAP Server on page 209

Configure a RADIUS Server Group

You must first create a wireless network SSID with **Enterprise 802.1X (WPA/WPA2/WPA3)** access security. This option requires users to authenticate themselves by entering a user name and password, which are checked against a RADIUS authentication server.

RADIUS servers offer two different types of services:

- Authentication for user credentials (usually on port 1812)
- Accounting (logging) (usually on port 1813)

Extreme Networks devices use the default wireless network (SSID) RADIUS server group, which can include up to four RADIUS servers, for RADIUS lookups, unless there is a device classification rule directing them to a different RADIUS server group. The servers in the group can be external RADIUS servers, Extreme Networks A3 RADIUS servers, Extreme Networks RADIUS servers, Extreme Networks proxy servers, or a combination of these four types.

Security for RADIUS servers uses simple passwords. Configure one password on the server, and the other on each of the clients.

This task is part of the network policy configuration workflow. Use this task to to configure a RADIUS server group for an SSID, as part of a network policy.

1. Go to **Configuration** > **Network**.
2. Select an existing policy, and then select , or to add a new one, select ..
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. In the **Authentication Settings** section, toggle the **Authentication with ExtremeCloud IQ Authentication Service** setting **OFF**.

   The **Authenticate via RADIUS Server** section becomes available.
5. To add an existing RADIUS server group, select and choose an existing object, or to add a new one, select .
6. Type a **RADIUS Server Group Name**.
7. (Optional) Type a **RADIUS Server Group Description**.

   Although optional, descriptions can be helpful when you are troubleshooting your network.
8. Configure the RADIUS server settings for IQ Engine devices.

   See Configure RADIUS Server Settings on page 202.
9. Depending on the type of server that you want to add, select one of the following tabs:

Tab	Configuration task
EXTERNAL RADIUS SERVER	Configure an External RADIUS Server on page 203
EXTREME NETWORKS A3	Configure an Extreme Networks A3 Server on page 204

Tab	Configuration task
EXTREME NETWORKS RADIUS SERVER	Configure an Extreme Networks RADIUS Server on page 205
EXTREME NETWORKS RADIUS PROXY	Configure an Extreme Networks RADIUS Proxy on page 211

Select up to four existing servers to add to your wireless network (SSID) RADIUS server group.

10. Select **SAVE RADIUS**.

Note
In addition to those set by you, or by default, Extreme Networks APs report updated DHCP-snooped IP addresses of associated clients to the RADIUS server asynchronously, or as soon as the information is available.

Related Links

Configure RADIUS Server Settings on page 202

Configure RADIUS Server Settings

First begin configuring a RADIUS server group. See Configure a RADIUS Server Group on page 201.

This task is part of the network policy configuration workflow. Use this task to configure RADIUS server settings for IQ Engine devices for a RADIUS server group, as part of a network policy.

1. On the **Configure RADIUS Servers** page, select  and configure the following settings:

Setting	Description
Retry Interval	Specify the time between retries for an unresponsive primary RADIUS server Access-Request. The device retries the primary server after the interval elapses, even if the current backup server is responding. Range: 60–100000000 (seconds) Default: 600 **Note:** Do not enter commas in this field. Enter 100,000,000 as 100000000.
Accounting Interim Update Interval	Specify the interval for sending RADIUS accounting updates to report the client session status and cumulative length. Range: 10–100000000 (seconds) Default: 600 **Note:** Do not enter commas in this field. Enter 100,000,000 as 100000000.

Setting	Description
Permit Dynamic Change Of Authorization Messages (RFC 3576)	Enable the RADIUS server to dynamically change the authorization for a user, or to disconnect a user per RFC 3576. When you enable this parameter, devices acting as RADIUS authenticators can accept unsolicited disconnect and Change of Authorization (CoA) messages from a RADIUS authentication server, such as GuestManager, per RFC 3576. Disconnect messages terminate a user session immediately, and CoA messages modify session authorization attributes such as VLANs and user profile IDs.
Inject Operator-Name attribute	Select to include the Operator-Name attribute in the Access-Request and Accounting-Request messages that the Extreme Networks RADIUS authenticators send to the RADIUS authentication server. The attribute value is the domain name suffix of the Extreme Networks authenticator, usually assigned by DHCP, and helps to identify the authentication requests source. Providing source information like this can aid in troubleshooting authentication problems.
Message Authenticator attribute	The Message Authenticator attribute is an HMAC-MD5 checksum of the entire Access-Request packet, containing the Type, ID, Length, and Authenticator field, using the shared secret as the key. This ensures the authenticity and integrity of the packet. ExtremeCloud IQ uses this attribute to authenticate RADIUS server replies, and to encrypt passwords.
Override default failover settings	Select this option to override the default RADIUS server failover and retry interval. The retry interval is the number of seconds between RADIUS server requests. Select **Aggressive** or **Custom (Range 1-5)**. Set the **First retry interval**. (Default: 1) Set the **Max-retries** value, which is the maximum number or retries, before failing over to a configured backup RADIUS server. (Default: 3)

2. Select **SAVE RADIUS SETTINGS**.

Finish configuring the RADIUS server group.

Related Links

Configure a RADIUS Server Group on page 201

Configure an External RADIUS Server

First begin configuring a RADIUS server group. See Configure a RADIUS Server Group on page 201.

To add an external RADIUS server, you require the IP address, authentication port number, and the shared secret for the RADIUS server.

This task is part of the network policy configuration workflow. Use this task to configure a RADIUS server for a RADIUS server group, as part of a network policy.

1. On the **Configure RADIUS Servers** page, select **EXTERNAL RADIUS SERVER**.
2. Select an existing server, or select .
3. Type a **Name** for the server.
4. (Optional) Type a **Description** for the server.
5. Select the **IP/Host Name** for the server.

   If you do not see the IP address that you need, select to define a new one (IPv4 or IPv6).

   If the address object is a host name, ensure that the devices can resolve it to an IP address. If you configure a domain name for the devices, or if the devices dynamically receive a domain name through DHCP, and the RADIUS server belongs to the same domain, the RADIUS server name can be just the host name without the domain name. If the RADIUS server belongs to a different domain, the address object must be the fully qualified domain name (FQDN): the host name + the domain name.
6. For **Server Type**, choose the RADIUS server role:
   - **Authentication**: As an authentication server, the RADIUS service requests that the client device demonstrate its identity.
   - **Port**: Set the RADIUS authentication port.
   - **Accounting**: As an accounting server, the RADIUS service tracks client-server session details.
   - **Port**: Set the RADIUS accounting port number.
7. Type the **Shared Secret** for authenticating communications with the RADIUS server.
8. (Optional) Select **Show Password**.
9. Select **SAVE EXTERNAL RADIUS**.

Finish configuring the RADIUS server group.

Related Links

Configure a RADIUS Server Group on page 201

Configure an Extreme Networks A3 Server

You must have existing A3 RADIUS server services.

First, begin configuring a RADIUS server group. See Configure a RADIUS Server Group on page 201.

This task is part of the network policy configuration workflow. Use this task to configure an A3 server for a RADIUS server group, as part of a network policy.

1. On the **Configure RADIUS Servers** page, select **EXTREME NETWORKS A3**.
2. Select an existing server, or select .
3. Type a **Name** for the server.
4. (Optional) Type a **Description**.
5. Enter the **IP/Hostname** of the server.

6. Accept the defaults or enter specific **Server Type** ports.
7. Type the **Shared Secret** for authenticating communications with the A3 server.
8. (Optional) Select **Show Password**.
9. Select **SAVE EXTREME NETWORKS A3**.

Finish configuring the RADIUS server group.

Related Links

Configure a RADIUS Server Group on page 201

Configure an Extreme Networks RADIUS Server

First begin configuring a RADIUS server group. See Configure a RADIUS Server Group on page 201.

Extreme Networks devices can serve as RADIUS authentication servers and respond to 802.1X requests from other Extreme Networks devices acting as RADIUS authenticators. The Extreme Networks RADIUS server can store user accounts locally, or check user login credentials against user accounts stored externally on the following user database servers: Active Directory, or LDAP.

This task is part of the network policy configuration workflow. Use this task to configure an Extreme Networks RADIUS server for a RADIUS server group, as part of a network policy.

1. On the **Configure RADIUS Servers** page, select **EXTREME NETWORKS RADIUS SERVER**.
2. Select a **User Database Type** from the menu.
3. Select an existing server, or select  .
4. Select the devices to configure.
5. Configure the AAA Server Profile.

   See Configure an AAA Server Profile on page 205.

Related Links

Configure an AAA Server Profile on page 205

Configure an AAA Server Profile

First, configure an Extreme Networks RADIUS Server. See Configure an Extreme Networks RADIUS Server on page 205.

Extreme Networks devices can serve as RADIUS authentication servers and respond to 802.1X requests from other Extreme Networks RADIUS authenticators. The Extreme Networks RADIUS server can store user accounts locally or check user login credentials against user accounts stored externally on Active Directory or LDAP (lightweight directory access protocol) user database servers.

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

1. On the **Wireless** tab, select **Add Radius Server Group**.

2. Select **EXTREME NETWORKS RADIUS SERVER**.
3. Type a **RADIUS Server Group Name**.
4. Type an optional **RADIUS Server Group Description**.
5. Select the **User Database** type.
   - **Active Directory**: Select to enable an Extreme Networks RADIUS server to interoperate with an Active Directory server.
   - **LDAP Server**: Select to direct user account look-ups to one or more LDAP servers.
   - **Local Database**: Select to enable an Extreme Networks device to support authentication for local user groups.
6. Select the corresponding check boxes for the devices that you want to configure.
7. Select **CREATE NEW** to add a new AAA server profile.

   Alternately, select **USE EXISTING**, and then select an AAA server profile from the list.
8. Type a **Profile Name**.
9. Type an optional **Profile Description**.
10. Select the **User Database** type: **Active Directory**, **LDAP Server**, or **Local Database**.

    Available configuration options depend on the type of database that you select.
11. Type a **User Group Attribute**, and then select , and choose an existing user group.
12. Expand the **Additional Settings** section, and then enter the number of seconds for each response scenario.

    The **Additional Settings** section is not available for local databases.
13. Select **Enable Caching of Credentials** to improve performance across WAN links.
14. Type the number of seconds to retain the credential cache.
15. Complete the database-specific configuration options as follows:

User database type	Configuration
Active Directory	See Add an Active Directory Server on page 208.
LDAP Server	See Add an LDAP Server on page 209.
Local Database	The Extreme Networks device that authenticates users directly, maintains the user database locally.

16. Select **Security Options**, and then Configure AAA Server Security Options on page 207.
17. Select **Approved RADIUS Clients**, and then Add Approved RADIUS Clients on page 212.
18. Select **SAVE RADIUS SERVER**.

Continue configuring the RADIUS server profile.

Related Links

Configure an Extreme Networks RADIUS Server on page 205
Add an Active Directory Server on page 208
Add an LDAP Server on page 209
Configure AAA Server Security Options on page 207
Add Approved RADIUS Clients on page 212

Configure AAA Server Security Options

Configure an Extreme Networks device as a RADIUS Server.

This task is part of the network policy configuration workflow. Use this task to add increased security to the AAA Server Profile. For more information, see Configure an AAA Server Profile on page 205.

Note
Default certificates are intended to be used for testing only.

1. Select an **Authentication Protocol** from the drop-down list.
   - **TLS** requires mutual authentication using client-side certificates. With a client-side certificate, a compromised password is not enough to break into TLS-enabled systems because the intruder still needs the client-side certificate. A password is only used to encrypt the client-side certificate for storage. Credentials are used for a one-time certificate enrollment. The certificate is sent to the RADIUS server for authentication.
   - **PEAP** encapsulates EAP within a potentially encrypted and authenticated TLS tunnel. The user must enter their credentials, which are sent to the RADIUS Server that verifies the credentials, and authenticates them for network access.
   - **TTLS** extends TLS. The client can, but does not have to, be authenticated via a CA-signed PKI certificate to the server. This greatly simplifies the setup procedure since a certificate is not needed for every client.
   - **LEAP** uses dynamic WEP keys and mutual authentication between the client and RADIUS server. Uses an authentication protocol in which user credentials are not strongly protected and are easily compromised. Users who absolutely must use LEAP should do so with sufficiently complex passwords.

     Note
     The WEP protocol is no longer effective for securing wireless networks. For security reasons, WEP configuration is no longer available in the UI. If you require WEP for business continuity purposes, you can enable it via Supplemental CLI.

   - **MD5** offers minimal security, is vulnerable to dictionary attacks, and does not support key generation. This method is commonly used in a trusted network.
2. Select a **Default Authentication Protocol** from the drop-down list.
3. Select the default certification authority digital certificate type.
4. Select the default server digital certificate type.
5. Select whether to verify the server certificate file.
6. Enter the client key file password.
7. Select whether to **Check common name in certificate against the user for TLS authentication**.
8. Select the authentication that has been assigned to a user.

9. If you **Enable Authentication**, the recommended value for the **Age Timeout for Active Session** is three times the value of the **Accounting Interim Update Interval** in the RADIUS Client.

   For example, if the Accounting Interim Update Interval is set to 600 seconds, set the Age Timeout for Active Session to 1800 seconds.

Continue configuring the server.

Add an Active Directory Server

First, configure an AAA server profile. See Configure an AAA Server Profile on page 205.

This task is part of the network policy configuration workflow. Use this task to add an Active Directory (AD) database to an Extreme Networks device acting as a RADIUS Server.

1. For Step 3, on the **Configure RADIUS Servers** page, to add an existing AD server, select and choose an existing object, or to add a new one, select .
2. Type a **Name** for the AD server.
3. Type the name of the **Domain**, to which the RADIUS authentication server and the AD server both belong.

   (Range: 1–64 characters). Include parent domains, such as .com, .net, and .org.
4. Select **Auto** or **Manual**.

Setting	Description
Auto	ExtremeCloud IQ (New) automatically populates the Active Directory Server and the base distinguished name (BaseDN) parameters. Go to Step 9 on page 209.
Manual	Go to Step 5.

5. From the drop-down list, choose a previously-defined IP object or host name for the **Active Directory Server** that contains the user accounts the RADIUS authentication server will authenticate.

   If you do not see the one that you need listed, select **New** and enter an IP object or host name.
6. Type the **BaseDN**—The starting point for directory server searches, and the point in the directory tree structure where the server stores user accounts.
7. Type a **Short Domain Name**.
8. Type the **Realm** name that corresponds to the user account location, which is often the same as the domain name.

9. Set the organizational unit (OU) where the Extreme Networks RADIUS server has privileges to add itself as a computer in the domain or leave it blank.

   Note
   By default, the RADIUS server attempts to add itself into **Computers** unless you specify a computer-ou here. If you do not want to give a device access to the Computers container, you can create your own OU and give the device user permissions to create computers (that is, to add itself) to the specified OU. For example, the computer OU might be `wireless/APs`.

10. Select **Enable TLS Encryption** to encrypt the user look-up requests that the Extreme Networks RADIUS server sends to the Active Directory server.
11. Select **NEXT**.
12. Select an existing **DNS Server**, or select to create a new one.
13. Select **NEXT**.

Continue configuring the RADIUS server.

Related Links

Configure an AAA Server Profile on page 205

Add an LDAP Server

First, configure an AAA server profile. See Configure an AAA Server Profile on page 205.

This task is part of the network policy configuration workflow. Use this task to add an Lightweight Directory Access Protocol (LDAP) database to an Extreme Networks device acting as a RADIUS Server.

1. On the **Configure RADIUS Servers** page, to use an existing LDAP server, select and choose an existing object, or to add a new one, select .
2. Configure the settings.

   See LDAP Server Settings on page 209

Continue configuring the RADIUS server.

Related Links

LDAP Server Settings on page 209
Configure an AAA Server Profile on page 205

LDAP Server Settings

Table 79: Settings for LDAP servers

Setting	Description
Name	Type a **Name** for the new or cloned server.
LDAP Server	Specify an **IP Address** or **Host Name**. Select and choose an existing object, or to add a new one, select ..

Table 79: Settings for LDAP servers (continued)

Setting	Description
Description	(Optional) Although optional, entering a description is helpful for troubleshooting and for identifying the server.
RADIUS User Base DN	Type the RADIUS user base distinguished name, or the starting point for directory server searches, such as cn=visitors, and the point in the directory tree structure under which the server stores user accounts in its database. **Note:** ExtremeCloud IQ (New) supports up to 2000 users per user group. For more than 2000 users, you must separate the users into different user groups.
Bind DN Name	Type the LDAP client distinguished name used during the authentication part of an LDAP session, such as cn=users, cn=students, dc=southamerica, ou=student, and ou=school.
Bind DN Password	Type the password for the LDAP client distinguished name for use during the authentication part of an LDAP session.
Show Password	Select **Show Password** to see the password.
Communication	Select **LDAP** or **LDAPS** for the required communication protocol.
Optional Settings	
Filter Attribute	Enter required **Filter Attribute** for searching for elements below the baseObject.
Strip realm name from filter	Select the check box to disable the realm, which is commonly appended to a user name and delimited with an @ sign, from the filter.
Destination Port	(Required) Enter the LDAP server **Destination Port**.
TLS Authentication/ Encryption	Select the check box to enable Transport Layer Security authentication and encryption, and configure the settings.
TLS Authentication/Encryption	
CA Certificate File	(Required) Select the default certification authority digital certificate type from the list.
LDAP Client Certificate	(Required) Select the default LDAP client digital certificate type from the list.
Client Key File	(Required) Select the default client key digital certificate type from the list.
Key File Password	Type the client key file password.

Table 79: Settings for LDAP servers (continued)

Setting	Description
Show Password	Select the check box to see the password.
Verify Server	Choose how often the Extreme Networks device checks the relationship between a certificate and its server: • **Try** (on first authorization or authentication) • **Never** • **Demand** (as required, on demand)

Configure an Extreme Networks RADIUS Proxy

First begin configuring a RADIUS server group. See Configure a RADIUS Server Group on page 201.

This task is part of the network policy configuration workflow. Use this task to to configure an Extreme Networks device as a RADIUS proxy server.

1. On the **Configure RADIUS Servers** page, select **EXTREME NETWORKS RADIUS PROXY**.
2. Select the device to configure as a proxy.
3. Type a **Name** for the proxy.
4. Type a **Description**.

   Although optional, descriptions can be helpful when you are troubleshooting your network.
5. For the **Realms** section, see Configure a RADIUS Proxy Server Realm on page 211.
6. For the **Approved RADIUS Clients** section, see Add Approved RADIUS Clients on page 212.
7. For the **Realm Settings** section, see Configure Realm Settings on page 213.
8. Select **SAVE RADIUS PROXY**.

Related Links

Configure a RADIUS Server Group on page 201
Configure a RADIUS Proxy Server Realm on page 211
Add Approved RADIUS Clients on page 212
Configure Realm Settings on page 213

Configure a RADIUS Proxy Server Realm

First configure an Extreme Networks Device as a RADIUS proxy server. See Configure an Extreme Networks RADIUS Proxy on page 211.

You can add a postfix notation realm after a user name, separated by an “@” symbol, and the result resembles an email address domain name. Or you can add a prefix notation realm before a user name, with a backslash “\” separator. User names can also include multiple realms, for example `domain1.com\username@domain2.com` is a valid user name with two realms. Realms can be arbitrary text and do not need to contain real domain names, even though they can look like domains.

This task is part of the network policy configuration workflow. Use this task to configure realms for a RADIUS proxy.

1. On the **Configure RADIUS Servers** page, select **REALMS**.
2. Select **ADD A RADIUS SERVER GROUP** to display and configure the settings.

   See Configure a RADIUS Server Group on page 201.
3. Configure **Required Realms**.
   a. Select the **Default Realm** from the menu.
   b. Select **Strip the realm name from the proxied access requests** to remove the realm name from proxied access requests.
   c. Select the **RADIUS Server Group** from the menu.
4. To create a realm, select an existing realm and then select , or to add a new one, select .
   a. Type the **Realm Name**.
   b. Select a RADIUS server group from the menu.
   c. Select **Strip the realm name from the proxied access requests** to remove the realm name from proxied access requests.
   d. Select **ADD**.
5. Select **SAVE RADIUS PROXY**.

Continue configuring the proxy server.

Related Links

Configure an Extreme Networks RADIUS Proxy on page 211
Configure a RADIUS Server Group on page 201

Add Approved RADIUS Clients

Configure an Extreme Networks device as a RADIUS proxy server. See Configure an Extreme Networks RADIUS Proxy on page 211.

This task is part of the network policy configuration workflow. Use this task to add one or more approved RADIUS clients to each configured realm associated with a RADIUS proxy server.

1. On the **Configure RADIUS Servers** page, select **APPROVED RADIUS CLIENTS**.
2. Select .
3. To use an existing **IP/Host Name/Network** for a client, select and choose an existing object, or to add a new one, select .
4. Type the associated **Shared Secret** (password).
5. To see the password, select **Show Password**.
6. (Optional) Type a **Description**.

   Although optional, entering a description is helpful for troubleshooting and for identifying the approved RADIUS client list.
7. Select **ADD**.
8. Select **SAVE RADIUS PROXY**.

Next, see Configure Realm Settings on page 213.

Related Links

Configure an Extreme Networks RADIUS Proxy on page 211
Configure Realm Settings on page 213

Configure Realm Settings

Configure an Extreme Networks device as a RADIUS proxy server and create a realm.

- Configure an Extreme Networks RADIUS Proxy on page 211
- Configure a RADIUS Proxy Server Realm on page 211

This task is part of the network policy configuration workflow. Use this task to optimize the realm settings for a RADIUS proxy.

1. On the **Configure RADIUS Servers** page, select **REALM SETTINGS**.
2. Select a **User and Realm Name** format:
   - NAI (Network Access Identifier)—The standard syntax is `user@realm`.
   - Windows NT Domain—The standard syntax is `user1@example.com`.
   - SPN (service principal name)—The standard syntax is `serviceclass/host`.
   - AUTO—Extreme automatically applies a format.
3. Type the **Retry Delay**—The time interval between retries.
4. Type the **Retry Count**—The number of retries before declaring failure.
5. Type the **Dead Time**—The time elapse (in seconds) before declaring failure.
6. Select **Inject Operator-Name Attribute**.

   If you do not want to inject an operator-named attribute, clear the check box.
7. Select **SAVE RADIUS PROXY**.

Finish configuring the RADIUS proxy.

Related Links

Configure an Extreme Networks RADIUS Proxy on page 211
Configure a RADIUS Proxy Server Realm on page 211

Configure VLAN Settings

This task is part of the SSID configuration workflow. Use this task to set the default user profile and configure the VLAN settings.

1. Go to **Configuration** > **Network**
2. Select an existing network policy, and then select , or to add a new one, select .
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. Select an existing SSID and then select , or select .
5. Scroll to **User Access Settings**, select the **Default User Profile**, and configure the settings.
   - To edit the selected **Default User Profile**, select the link and configure the settings.

Typically, the default VLAN is 1.

Note
The user profile **default-profile** cannot be edited directly. If this profile is assigned to your wireless network, you must either select a different profile or create a new one to configure the settings.

- To choose a new default user profile, select menu.
- To create a new user profile, select .

Table 80: User profile settings

Setting	Description
User Profile Name	Type a **User Profile Name**.
Connect to	a. Select **VLAN** or **VLAN Group**. b. Select and choose an existing object, or to add a new one, select . . For more information, see VLAN Object Settings on page 215 and VLAN Group Object Settings on page 215. To edit an existing VLAN object, select it and then select .
SECURITY	See Configure User Profile Security on page 215.
TRAFFIC TUNNELING	See Configure User Profile Traffic Tunneling on page 219.
QOS	See Configure User Profile QoS on page 223.
AVAILABILITY SCHEDULE	See Configure an Availability Schedule on page 225.
CLIENT SLA	See Configure User Profile Client SLA on page 226.
DATA/TIME LIMIT	See Configure User Profile Access Restrictions on page 227.

6. Select **SAVE USER PROFILE**.

Continue the SSID configuration.

Related Links

VLAN Group Object Settings on page 215
Configure Classification Rules for a Device Template on page 289

VLAN Object Settings

Configure the following settings, and then select **SAVE VLAN**.

Table 81: Settings for VLANs

Setting	Definition
Name	(Required) Type a name for the new VLAN.
VLAN ID	(Required) Type an ID for the new VLAN.
Apply VLANs to devices using classification	Select **Apply VLAN to devices for classification** to create VLANs that you can apply to specific devices based on their location.

Related Links

Configure VLAN Settings on page 213

VLAN Group Object Settings

VLAN groups combine multiple VLANs as a single common object. Configure the following settings, and then select **SAVE**.

Table 82: Settings for VLAN group objects

Setting	Definition
Name	(Required) Type a name for the new VLAN group object.
VLANs	(Required) Specify individual VLANs or ranges. Indicate a range with a hyphen. Separate VLAN entries with commas, for example, 1-30, 100-200, 500. Range: 1–4094
Description	(Optional) Type a description to identify the VLAN group. Although optional, descriptions can be helpful when you are troubleshooting your network.

Related Links

Configure VLAN Settings on page 213

Configure User Profile Security

Use this task to apply IP or MAC firewall rules to a user policy.

1. On the **SECURITY** tab, turn on **Firewall Rules**.
2. To redirect a user device to an external web site, select **IP Firewall** and complete the following steps:
   a. Select .
   b. Type a **Name** for the firewall rule.
   c. Select whether this firewall rule is for **Inbound Traffic** or **Outbound Traffic**.

d. Select whether this firewall rule is used to **Permit** or **Deny** traffic.

Permit enables traffic to traverse the firewall. **Deny** prevents the device from allowing traffic inside the firewall.

e. Select an existing IP firewall rule or select to create a new rule.

See Add IP Firewall Policies on page 216.

3. To determine how the device manages traffic based on source and destination IP addresses, select **MAC Firewall** and complete the following steps:
   a. Enter a name for the firewall rule.
   b. Select whether this firewall rule is for **Inbound Traffic** or **Outbound Traffic**
   c. Select whether this firewall rule is used to **Permit** or **Deny** traffic.
   d. Select an existing MAC Firewall Rule or select the plus sign to create a new rule.

See Add MAC Firewall Policies on page 218.

4. Continue configuring the user profile, or select **SAVE USER PROFILE**.

Related Links

Add IP Firewall Policies on page 216
Add MAC Firewall Policies on page 218
Configure VLAN Settings on page 213

Add IP Firewall Policies

Use this task to create IP firewall policy objects and rules that determine how the device manages traffic based on network or application services, and source and destination IP addresses.

1. Select an existing IP firewall policy rule, and then select , or to add a new one, select .
2. Enter a **Name** for the new policy.
3. Enter an optional **Description**.
4. Select to add a new rule.
5. Select one or more network or application services.

   Network Service objects identify Layer 4 traffic by protocol and port number. Extreme Networks provides a number of predefined services. Select the add icon to create a new network service. For more information, see Configure Network Services on page 217.

   a. Choose either **Network Services** or **Application Services**.

   You cannot select both.

   b. Select up to 100 items.
   c. Select **Add Service**.
6. Select a source IP address, host name, network, or **Any** from the drop-down list, or select **New** to add a new IP address, host name, or network.
7. Select a destination IP address, host name, network, or **Any** from the drop-down list, or select **New** to add a new IP address, host name, or network.

8. Select the action the device performs when it receives traffic matching the source address-destination address-service.
   The firewall can perform the following actions:
   - **Permit**: Allows traffic to traverse the firewall.
   - **Deny**: Blocks traffic from traversing the firewall.
   - **Drop traffic between stations**: Drops traffic between stations if both stations are associated with one or more members of the same hive. This setting applies to unicast, broadcast, and multicast traffic that the device receives on an interface in access mode.
   - **NAT**: Translates the source IP address of a packet permitted to traverse the firewall to that of the mgt0 interface on the device.
9. Choose one of the following logging options from the drop-down list:
   - **Off**: Disables logging for packets and sessions that match the IP firewall policy rule.
   - **Session Initiation**: Log details about a session created after passing an IP firewall policy lookup.
   - **Session Termination**: Log details about a session matching an IP firewall policy termination.
   - **Both**: Log details after initiating and terminating a session.
10. Select **Save**.

As you continue to add rules to a policy, each subsequent rule is positioned at the bottom of the list. Use the up and down arrows in the rules table to rearrange the position of rules to determine their application order.

Related Links

Configure Network Services on page 217

Configure Network Services

Network service objects identify Layer 4 traffic by protocol and port number. ExtremeCloud IQ (New) provides some predefined services and you can create custom network services to use when defining firewall policies, and QoS traffic classification and marking policies.

The Network Services table displays the following information about predefined and custom network service objects:

- **Name**: The name of the network service object.
- **Protocol Number**: The type of protocol (followed by its standard protocol number) that the service uses. Predefined services use the following protocols:
  - 1 : ICMP (Internet Control Message Protocol)
  - 6: TCP (Transmission Control Protocol)
  - 17: UDP (User Datagram Protocol)
  - 89: OSPF (Open Shortest Path First)
  - 119: SVP (SpectraLink Voice Priority)
- **Port Number**: The standard destination port number of the service. The receiving device uses the port number to map the service to a particular processor.

- **Service Idle Timeout**: The amount of time (in seconds) after which the device terminates an inactive session using this service. (For IP firewall policies, this field is only supported by APs.)
- **ALG Type**: An ALG (application layer gateway) links certain port numbers to a service so that the device can apply the proper QoS (Quality of Service) and firewall policies. For example, the TFTP service has a control stream and data stream that each use different port numbers. The port number for the TFTP control stream is static (port 69 by default), but the port number for the TFTP data stream is dynamic and is negotiated within the control session. The TFTP ALG links these two streams together logically so that the device can apply the proper QoS and firewall policies to both TFTP streams. You can apply different QoS settings to the TFTP control and data sessions, for example, to ensure high reliability but tolerate high latency, or to ensure accept a medium level of reliability but require low latency.
- **Description**: An optional description for the object. Descriptions can be very useful when troubleshooting or managing a complex network.
- **Virtual IQ** : The name of the Virtual IQ (virtual ExtremeCloud IQ) to which the service belongs. All predefined services are marked as global to indicate that they belong to all Virtual IQs. This column only appears when you are logged in to "All Virtual IQs" with super-user privileges.

Use this task to configure a network service:

1. Select  .
2. Enter a name for the service.
3. Select a service idle timeout (for APs and routers only).

   This is the amount of time (in seconds) after which the device terminates an inactive session using this service.
4. Select an IP Protocol number.

   The number of the protocol the service will use. Predefined services appear in the drop-down list, or you can configure a custom protocol.
5. Enter the standard destination port number of the service.

   For services that use TCP or UDP, you must set a destination port number, which the receiving device uses to map the service to a specific processor. When you use a custom protocol, a destination port number is not required because the receiving device can use the protocol to map the service to the appropriate processor.
6. Select an ALG type from the drop-down list.

   ALG is supported for APs and routers only. If the service must use an ALG, select DNS, FTP, HTTP, SIP, or TFTP, from the drop-down list. Otherwise, leave this field empty.

Related Links

Add IP Firewall Policies on page 216

Add MAC Firewall Policies

MAC firewall policies determine how the device manages traffic based on source and destination IP addresses, and the actions (permit or deny) the device can take. When the policy contains multiple rules, the order of the rules affects how they are applied. Use this task to create a new rule.

Use this task to add MAC firewall policy objects and rules.

1. Select an existing IP firewall policy and then select , or to add a new one, select .
2. Enter a **Name** for the new policy.
3. Enter an optional **Description**.
4. Select to add a new rule.
5. For **Source MAC**, select **Any**, an existing MAC OUI or the plus sign.

   If you choose to add a new **Source MAC**, select **MAC Address** or **MAC OUI** and perform the following:

   a. Enter a new name.
   b. Enter the **MAC Address** or **MAC OUI**.
6. For **Destination MAC**, select **ANY**, an existing MAC OUI or the plus sign.

   If you choose to add a new **Source MAC**, select **MAC Address** or **MA OUI** and do the following:

   a. Enter a new name.
   b. Enter the **MAC Address** or **MAC OUI**.
7. Select the action the device performs when it receives traffic matching the source address-destination address-service.

   The firewall can perform the following actions:

   - **Permit**: Allows traffic to traverse its firewall.
   - **Deny**: Blocks traffic from traversing its firewall.
8. Choose one of the following logging options from the drop-down list:
   - **Off**: Disable logging for packets and sessions that match the MAC firewall policy rule.
   - **Session Initiation**: Log session details about a session created after passing a MAC firewall policy lookup.
   - **Session Termination**: Log session details about a session matching a MAC firewall policy termination.
   - **Both**: Log session details after initiating and terminating a session.
9. Select **Save**.

As you continue to add rules to a policy, each new rule is positioned at the bottom of the list. Use the up and down arrows in the rules table to rearrange the position of rules to determine their application order.

Related Links

Configure User Profile Security on page 215

Configure User Profile Traffic Tunneling

You can enable the following types of GRE traffic tunneling for new and existing user profiles:

Layer 3 Roaming

Adjusts roaming thresholds so that a device disassociates with a wireless client that has roamed to it from another subnet and has either been idle for a period of time, or for which traffic is below a specified threshold.

Identity-Based Traffic Tunneling
: Tunnels guest traffic directly to the network.

Standard GRE Tunneling
: Tunnels traffic to non-Extreme Networks tunnel endpoints.

Tunnel Concentrator
: Tunnels traffic to Extreme Networks Tunnel Concentrator.

Use this task to configure traffic tunneling for a user profile.

1. On the **TRAFFIC TUNNELING** tab, turn on **Traffic Tunneling (GRE)**.
2. Select an existing profile from the **Re-use Tunnel Policy** menu, and then select the type of tunneling.
3. For **Layer 3 Roaming**:
   a. Specify a time period between 10 and 600 seconds.
   b. Specify a threshold number between 0 and 2147483647 packets per minute.
4. For **Identity-Based Traffic Tunneling**:
   a. For the **Tunnel Source**, select a subnet from the drop-down list, or add a new subnet.
   b. For **Tunnel Destination**, choose an IP address or host name from the drop-down list or add a new address or host name.
   c. For **Tunnel Authentication**, type the password the AP uses to authenticate to the GRE termination point.
5. For **Standard GRE Tunneling**:
   a. For **Tunnel Destination**, choose an IP address or host name from the drop-down list or add a new address or host name.
   b. If you select **Tunnel Mode dot1q**, type, select, edit, or add the 802.1Q native VLAN ID.

      To add a VLAN ID, see Configure VLAN Settings on page 213.
   c. If you select **Tunnel Mode Access Mode**, type, select, edit, or add the VLAN ID.

      To add a VLAN ID, see Configure VLAN Settings on page 213.
6. For **Tunnel Concentrator**, select the **Tunnel Destination**.

   You can add a new Tunnel Concentrator service, or edit an existing instance. For more information, see Single Tunnel Concentrator Services Settings on page 221 and Redundant Tunnel Concentrator Services Settings on page 222.
7. Continue configuring the user profile, or select **SAVE USER PROFILE**.

Related Links

Configure VLAN Settings on page 213
Single Tunnel Concentrator Services Settings on page 221
Redundant Tunnel Concentrator Services Settings on page 222

Single Tunnel Concentrator Services Settings

Table 83: Single Tunnel Concentrator

Field	Description
Name	**(Required)** Type a name to identify the new Tunnel Concentrator service.
Description	**(Optional)** Provide a description that might be helpful when troubleshooting.
Single Tunnel Concentrator	**(Required)** Select this option to create a single Tunnel Concentrator without redundancy.
Tunnel IP Address/CIDR	**(Required)** Type the IP Address for the tunnel (CIDR).
Gateway	**(Optional)** Type the IP address of the gateway.
Native VLAN ID	**(Required)** Type the Native VLAN ID. The Native VLAN is untagged.
Device Tunnel Concentrator	**(Required)** Select a Tunnel Concentrator from the menu.
Tunnel Port	**(Required)** Select a port from the menu.
VLAN ID	**(Required)** Type the VLAN ID. **(Optional)** For an untagged VLAN, select the corresponding check box.
Bridge Port	**(Required)** Select a bridge port for the tunnel from the menu.
To add or edit broadcast or multicast control for the Tunnel Concentrator service, select **Broadcast/Multicast Control**.	
Add New Rule	Select **Add New Rule** and type an IP address to permit.
Add Pre-defined Rule	Select and choose a pre-defined rule from the menu.
Block Non- Essential Broadcast	Select or clear the check box. Essential Broadcasts are ARP and DHCP
ARP Proxy	Select or clear the check box. **Caution:** Disabling the **ARP Proxy** option can lead to undesired traffic.

Related Links

Configure User Profile Traffic Tunneling on page 219

Redundant Tunnel Concentrator Services Settings

Table 84: Redundant (Primary and Backup) Tunnel Concentrators

Field	Description
Name	(Required) Type a name to identify the new Tunnel Concentrator service.
Description	(Optional) Provide a description that might be helpful when troubleshooting.
Redundant Tunnel Concentrator	(Required) Select this option to create a redundant Tunnel Concentrator.
Tunnel IP Address/CIDR	(Required) Type the IP Address for the tunnel (CIDR).
Gateway	(Optional) Type the IP address of the gateway.
VRRP Router ID	(Required) Type the ID for the VRRP router. ExtremeCloud IQ configures the same VRRP Router ID for both the primary and backup Tunnel Concentrators (range 1-255). The **VRRP Router ID** must be different for each cluster of VRRP devices.
Native VLAN ID	(Required) Type the Native VLAN ID. The Native VLAN is untagged.
Device Tunnel Concentrator	(Required—Primary and Backup) Select a primary Tunnel Concentrator from the menu. Select a backup Tunnel Concentrator from the menu.
Tunnel Port	(Required—Primary and Backup) Select a port for the tunnel from the menu for the primary Tunnel Concentrator from the menu. Select a port for the tunnel from the menu for the backup Tunnel Concentrator from the menu.
VLAN ID	(Required—Primary and Backup) Type the VLAN ID for the primary and for the backup Tunnel Concentrators. (Optional) For an untagged VLAN, select the corresponding check box.
IP Address	(Required—Primary and Backup) Type the IP address for the primary and the backup Tunnel Concentrators.

Table 84: Redundant (Primary and Backup) Tunnel Concentrators (continued)

Field	Description
Bridge Port	(Required—Primary and Backup) Select a bridge port for the tunnel from the menu for the primary Tunnel Concentrator. Select a bridge port for the tunnel from the menu for the backup Tunnel Concentrator.
To add or edit broadcast or multicast control for the Tunnel Concentrator service, select **Broadcast/Multicast Control**.	
Add New Rule	Select **Add New Rule** and type an IP address to permit.
Add Pre-defined Rule	Select and choose a pre-defined rule from the menu.
Block Non- Essential Broadcast	Select or clear the check box. Essential Broadcasts are ARP and DHCP
ARP Proxy	Select or clear the check box. **Caution:** Disabling the **ARP Proxy** option can lead to undesired traffic.

Related Links

Configure User Profile Traffic Tunneling on page 219

Configure User Profile QoS

Extreme Networks devices can apply QoS to traffic originating from members of user profiles to prioritize traffic by category, set rate limits and traffic forwarding rules for each traffic class, and set the maximum traffic forwarding rate and scheduling weight at two levels: for individual users in a user profile and for all users to whom the user profile applies. Through the rate control and queuing profile, you define QoS policing rates and scheduling weights at the individual user level. In the **QoS** section in a user profile configuration, you define the rates and weights at the user profile level. Through the combined configuration of forwarding mechanisms and rate limits, you control how a device schedules traffic forwarding.

1. On the **QOS** tab, turn on **Quality of Service (QoS)**.
2. Configure the **Rate Limit per User Profile per AP** to set the aggregate rate limit for all the users in the user profile.
3. Select **Manage Rate Limit per Client**.
   a. Set the **Rate Limit Per Client** from 0 to 2000 Mbps (0-2000000 Kbps).
   b. Set a weight percentage for each of the seven traffic classes in **Traffic Queue Management Per User per AP**, and set other details as required.
   c. Select **Save**.

4. Type the **Scheduling Weight**.

   Note
   Devices forward traffic of a higher class and greater weight faster than traffic of a lower class and lesser weight.

5. Select a QoS classification system from the **Mark outgoing traffic using** list.

   Extreme Networks devices can apply priority and class mappings to outgoing traffic based on either of the standard QoS classification systems.
6. To add a marker map, see Configure Marker Maps on page 224.
7. Continue configuring the user profile, or select **SAVE USER PROFILE**.

Related Links

Configure Marker Maps on page 224
Configure VLAN Settings on page 213

Configure Marker Maps

For outgoing traffic, you can define marker maps to map classes to priority numbers in standard classification systems (802.11e, 802.1p, and DSCP). After you define classifier and marker maps, you then define classifier and marker profiles that enable one or more of the methods defined in the maps. Finally, you associate those profiles with SSIDs or interfaces to apply the mappings to traffic arriving at or exiting those interfaces.

Use the following procedures to configure marker maps for outgoing traffic. When you configure marker maps at the network policy level, you can reuse existing maps. Select the list, and in the dialog box, select the check box of a map and choose Select. All fields are automatically populated with the information for the selected map.

Note
Deleting a marker map from the Location Server dialog box also deletes it from the Common Objects list. You can only delete a marker map if no other configuration object is using it. to see a list of configuration objects that reference a marker map, hover over the number in the Used By column for that map in the Marker Maps window in the Common Objects section.

1. Select an existing map, and then select , or to add a new one, select .
2. Enter a **Name** for the marker map.
3. Enter an optional **Description** for the map.

4. On the **802.1p Markers** tab, toggle **802.1p Markers** to **On**.

   The QoS marking table shows the mapping of classes to WMM® (Wi-Fi Multimedia™) queues and the 802.1p classification system (marked in the L2 frame header in Ethernet frames). You can modify these mappings if necessary.

   Extreme Network devices automatically include 802.11e priority marking in the L2 headers of wireless frames, so it is not included here as a configurable option.

   Depending on the classification systems used in the surrounding network, select the appropriate check boxes to map classes to one or both systems for outgoing traffic. A network policy can reference just one marker map.
5. On the **Diffserv** tab, toggle **Diffserv** to **On**.

   The QoS marking table shows the mapping of classes to WMM® (Wi-Fi Multimedia™) queues and the DiffServ codepoint marking system (marked in the L3 packet header) on outgoing packets. You can modify these mappings if necessary.

   Note
   If both 802.1p and DiffServ are enabled, only DiffServ takes effect.

Related Links

Configure User Profile QoS on page 223

Configure an Availability Schedule

Begin to Configure VLAN Settings on page 213.

You can make the user profile available for specific dates, days, and times by assigning defined availability schedules to the profile. Profile members can access the network through the device only during these scheduled times. When the user profile is inactive, the device blocks access to the network.

Use this task to enable the Availability Schedule feature and configure the settings when creating a user profile as part of a network policy.

1. On the **AVAILABILITY SCHEDULE** tab, turn on **Availability Schedule**.
2. Select and configure the settings.

   See Schedule Settings on page 226.
3. Continue configuring the user profile, or select **SAVE USER PROFILE**.

   Note
   To apply your SSID availability schedule to a wireless network, you must activate it in the **Additional Settings** section of the Standard Wireless Networks configuration page. See Configure Enterprise SSID Authentication on page 178.

Related Links

Schedule Settings on page 226
Configure Enterprise SSID Authentication on page 178
Configure VLAN Settings on page 213

Schedule Settings

Table 85: Settings for a One Time Schedule

Setting	Description
Name	Type a name for the schedule.
Description	(Optional) Type a description for the schedule.
One Time	Select to apply this schedule one time only.
Start Time	Use the **Start** and **Time** controls to specify the starting date and time for the schedule.
End Time	Use the **End** and **Time** controls to specify the end date and time for the schedule.

Table 86: Settings for a Recurring Schedule

Setting	Description
Name	Type a name for the schedule.
Description	(Optional) Type a description for the schedule.
Recurring	Select to apply this schedule on an ongoing basis.
Recurrence	Select **Every Day**, or select **From** and use the menus to select the day of the week to start, and the day to end the recurrence.
Limit recurrence between	Select the check box to apply the schedule to a specific date range. Use the controls to specify the start and end dates.

Related Links

Configure an Availability Schedule on page 225

Configure User Profile Client SLA

Service-level agreements (SLAs) are contracts that specify the performance parameters within which a network service is provided.

Extreme Networks devices monitor client throughput and take action if the actual throughput is below the defined target minimum level. Use this task to enable client SLA settings for the user profile.

1. On the **CLIENT SLA** tab, turn on **Client SLA**.
2. Use the **Targeted minimum throughput** slider bar to adjust the minimum throughput level.
3. Select **Log** to generate a log entry about the performance sentinel violation.
4. Select **Boost Airtime** to increase the airtime available to clients so they can reach their targeted minimum throughput level.

5. Select both **Log** and **Boost Airtime** to combine the previous two actions.

Note
Using just the Log option to see if wireless clients throughout the corporate network are SLA-compliant is useful even without the Boost Airtime option. When clients do not get the expected level of throughput, you can see the results in graphs in the ExtremeCloud IQ (New) SLA reports. For Extreme Networks devices with non-compliant clients, you can drill down in the graph to see an SLA report for each client and determine why it is not meeting the SLA. If you conclude that the devices are oversubscribed, you can add more devices in that area to improve client throughput.

6. Continue configuring the user profile, or select **SAVE USER PROFILE**.

Related Links

Configure VLAN Settings on page 213

Configure User Profile Access Restrictions

Use this task to configure access restrictions (date and time limits) for users based on their assigned user profiles. This is particularly helpful when you manage non-employee guest users, such as visitors, VIPs, and contractors.

1. On the **DATA/TIME LIMIT** tab, turn on **Access Restrictions**.
2. Select **Time Limit**.
   a. Select the limit in minutes, hours, days, or weeks (the number of minutes in a number of hours, or hours in days, or days in weeks).
   b. Select how to define an hour (either a fixed or rolling time window).
3. Select **Data Usage Limit**.
   a. Configure a data usage limit (in MB or GB).
   b. Limit the duration to days, weeks, or months.
   c. Select how a day is measured (either a fixed or rolling time window).
4. Continue configuring the user profile, or select **SAVE USER PROFILE**.

Related Links

Configure VLAN Settings on page 213

Apply Different User Profiles to Clients and User Groups

Before you can apply different user profiles, configure the SSID for the network. For more information, see Configure the SSID for a Standard Wireless Network on page 165.

With user-profile assignment rules, you can assign clients to user profiles that match all configured conditions. The available conditions are as follows:

- Advanced Guest Policy
- Client OS Type
- Client MAC Address
- Client Location

- Schedule
- Cloud Config Group

This task is part of the network policy configuration workflow. Use this task to apply different user profiles to clients and user groups as part of a network policy.

1. Go to **Configuration** > **Network**.
2. Select an existing policy, and then select , or to add a new one, select .
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. Under **User Access Settings**, select **Apply a different user profile to various clients and user groups**.
5. To choose an existing user profile, select and choose an existing object, or to add a new one, select .
6. To add an existing user profile assignment rule, select .
   a. Select one of the existing rules.
   b. Select **Link**.
7. (Optional) To add a new user profile assignment rule, select .
   a. Type a **Name** for the user profile assignment rule.
   b. Type a **Description**.
   c. Select , and choose a category.
   d. Complete the configuration for the selected category.

   See Configure Classification Rules on page 148.

   You can add multiple assignment rules to create more granular control.
8. Select **SAVE**.

Related Links

Configure the SSID for a Standard Wireless Network on page 165
Configure Classification Rules on page 148

Customize Advanced Access Security Controls

This task is part of the network policy configuration workflow. Use this task to configure and manage the cryptographic keys used to encrypt Wi-Fi traffic during the four-way handshake authentication process between an AP and clients, and to manage and set up Pairwise Transient Keys.

1. Go to **Configuration** > **Network**.
2. Select an existing policy, and then select , or to add a new one, select ..
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. Select an existing SSID, and then select , or to add a new one, select ..
5. Expand the **Additional Settings** section.
6. For **Advanced Access Security Controls** (802.11w, Authentication timeout options), select **CUSTOMIZE**.

7. Configure the settings:

Table 87: Settings for Advanced Access Security Controls

Setting	Description
Advanced Authentication Options	
Generate new Group Master Key (GMK) after	Type the time interval, after which the system generates a new GMK. Select the unit of time (seconds, minutes, hours, or days) from the list. The GMK is a large random number that an Extreme Networks device chooses. From the GMK, the device derives a GTK (Group Temporal Key), which it then sends to all associated clients within EPOL-key messages. The Extreme Networks device and clients use the GTK to encrypt and decrypt broadcast or multicast traffic transmitted between themselves.
Generate New Group Temporal Key (GTK) after	Type the time interval, after which the system generates a new GTK. Select the unit of time (seconds, minutes, hours, or days) from the list. The wireless client and Extreme Networks device use a GTK to encrypt to and decrypt broadcast and multicast traffic transmitted between themselves. A GTK is a temporal key that an Extreme Networks device derives from a GMK (Group Master Key) by performing a cryptographic hash on the concatenation of the GMK, a nonce, and the MAC address of the Extreme Networks device. The Extreme Networks device then sends the GTK to all associated clients within EAPOL-Key messages.
GTK Timeout Period	Type the time interval (in Milliseconds) that the device waits for client replies during the handshake process. To accommodate clients that have shorter or longer timeout values, you can change this to a value from 100 (the standard timeout value) to a maximum of 8000 milliseconds.
Number of GTK Retries	Type the maximum number of times the device will retry sending GTK messages.
Generate a new Pairwise Transient Key (PTK) after	Select to enable PTK rekeying, and enter a value between 10 and 50,000,000 seconds (~231 days). If you enable PTK rekeying, an interval between 2 and 10 minutes (120 and 600 seconds) is the best practice recommendation, which is short enough to thwart the known TKIP exploit. Enable this option only if you know that the clients using the SSID support it. In addition, you might need to configure PTK rekeying on the clients. **Note:** There is a flaw in TKIP that allows an attacker to decrypt unicast packets sent from an access point to a wireless client, and then send the client-forged packets, possibly with the purpose of poisoning ARP or DNS caches. If you cannot transition to AES-CCMP—which is not susceptible to this attack—you can mitigate attacks against TKIP-encrypted data by setting the PTK (pairwise transient key) to rekey at short intervals.

Table 87: Settings for Advanced Access Security Controls (continued)

Setting	Description
PTK timeout period	Type the interval (in Milliseconds) that the device waits for client replies during the four-way handshake in which they derive a PTK for encrypting and decrypting unicast traffic. To accommodate clients that have shorter or longer timeout values, you can change the value from 100 milliseconds (the standard timeout value) to a maximum of 8000 milliseconds.
Number of PTK retries	Type the maximum number of times the device will retry sending PTK messages.
Replay window	Type a window size, within which the device accepts replies to previously sent messages during four-way handshakes. 0 indicates that the device does not accept any messages other than a reply to the last message that it sent. You might want to accept replies to previously sent messages if there are clients that reply more slowly than the device retries sending it messages.
Local TKIP Countermeasure	(Available only when the encryption method is Auto-TKIP or CCMP (AES) or TKIP) Select to enable the deauthentication of all clients when the local device detects message integrity check failures during TKIP operations. If one key fails an integrity check, the discovery of such a failure suggests that other keys in current use might also be compromised. The cautious security stance is to deauthenticate all clients and stop using all existing keys immediately. When clients reauthenticate, they use newly generated pairwise and group primary and temporal keys. If this feature is disabled, the device continues to use existing keys and maintain currently connected clients after detecting MIC failures.
Remote TKIP Countermeasure	(Available only when the encryption method is Auto-TKIP or CCMP (AES) or TKIP) Select to deauthenticate all previously authenticated clients when a client reports MIC failures during TKIP operations. The distinction between the local and remote countermeasure options is where the discovery occurs: • Local—A device discovered the failure. • Remote—A client discovered and reported the failure.
Enable to refresh the GTK only when the rekey period elapses.	To disable GTK refresh when either the rekey period elapses or a client disassociates from the SSID, clear the check box.

8. Select **SAVE**.

Customize Wireless Network Optional Settings

Complete the Add a Network Policy on page 134 task.

When configuring an SSID, you can configure and apply radio rates, DoS prevention settings, traffic filters, and other options.

Use this task to configure the **Optional Settings** for a standard wireless network.

1. Go to **Configuration** > **Network**.
2. Select an existing policy, and then select , or to add a new one, select ..
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. Go to **Additional Settings** > **Optional Settings**, and then select **CUSTOMIZE**.
5. Customize Radios and Rates Settings on page 231.
6. Customize DoS Prevention Settings on page 232.
7. Customize Traffic Filters on page 233.
8. Customize the User Profile Application Sequence on page 233.
9. Customize Voice Enterprise Options on page 234.
10. Customize Wi-Fi Multimedia™ on page 235.
11. Customize Broadcast and Multicast Handling Settings on page 236.
12. Customize Client Related Network Settings on page 237.
13. Customize Other Options on page 238.
14. Select **SAVE OPTIONAL SETTINGS**.

Customize Radios and Rates Settings

Complete the Add a Network Policy on page 134 task.

By default, Extreme Networks devices advertise support for all rates. By setting specific rates, you can restrict access to just those clients that can support them. Use these controls to force clients to connect at higher data rates on an SSID, which can help increase average data transfer rates.

1. Go to **Configuration** > **Network**.
2. Select an existing policy, and then select ..
3. Select **NEXT** to open the **Wireless Network** page.
4. Go to **Additional Settings** > **Optional Settings**, and then select **CUSTOMIZE**.
5. Go to the **Radios and Rates** section.
6. Select a radio frequency and configure the basic (mandatory) and optional data rates per SSID.
7. Select **SAVE RATE SETTING**.
8. Repeat steps 6–7 for each radio frequency.

Continue customizing **Optional Settings** in the **Wireless Networks** configuration window. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Related Links

Add a Network Policy on page 134
Customize Wireless Network Optional Settings on page 231

Customize DoS Prevention Settings

Complete the Add a Network Policy on page 134 task.

This task is part of a series for configuring the **Optional Settings** for a standard wireless network. Use this task to customize settings for broadcast and multicast handling. Use this task to configure defensive settings to protect against Denial of Service (DoS) attacks, and configure SSID access filters based on MAC addresses.

1. Go to **Configuration** > **Network**.
2. Select an existing policy, and then select .
3. Select **NEXT** to open the **Wireless Network** page.
4. Go to **Additional Settings** > **Optional Settings**, and then select **CUSTOMIZE**.
5. Go to the **MAC-based Dos Prevention rules for** section.
6. Select an option and configure the settings.
   - **SSID**—Select to protect against DoS attacks at the MAC layer (Layer 2) on the radio channel that an AP uses for SSID access traffic. The settings for an SSID apply cumulatively to the total amount of Layer 2 traffic that an AP receives on the access channel for the SSID.
   - **Client**—Select to protect against DoS attacks at the MAC layer (Layer 2) on the radio channel that an AP uses for SSID access traffic. The settings in the MAC DoS configuration object apply to the total amount of Layer 2 traffic that an AP receives on the access channel for the SSID from a single MAC address.
7. Under **IP-based Dos Prevention rules for**, select **SSID** and configure the settings. This configuration protects against Denial of Service attacks at the IP layer (Layer 3) on the radio channel that an AP uses for SSID access traffic.

   The settings in the IP DoS configuration object apply cumulatively to the total amount of Layer 3 traffic that an AP receives on the access channel for the SSID.
8. **Enable MAC-Based filters** and select an option for the **Default Action**.
   - **Permit**—Enable traffic from clients that do not match one of the selected filters.
   - **Deny**—Block traffic from clients that do not match any of the selected MAC filters.

   This step makes the **Add MAC-Based Filters** section available.
9. Add Mac-based filters.
   a. Scroll to the **Add MAC-Based Filters** section, and and then select .
   b. Specify a MAC or a MAC Oui.
      - Select and choose an existing MAC or MAC Oui.
      - Select to add a new **MAC Address**, or **MAC Oui**.
   c. Select an **Action** from the menu.
   d. Select **ADD**.

Continue customizing **Optional Settings** in the **Wireless Networks** configuration window. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Related Links

Add a Network Policy on page 134
Customize Wireless Network Optional Settings on page 231

Customize Traffic Filters

Complete the Add a Network Policy on page 134 task.

Select traffic filters to control which management and diagnostic services an AP may receive, and whether to allow traffic between clients connected to the AP.

This task is part of a series for configuring the **Optional Settings** for a standard wireless network. Use this task to customize optional traffic filter settings.

1. Go to **Configuration** > **Network**.
2. Select an existing policy, and then select .
3. Select **NEXT** to open the **Wireless Network** page.
4. Go to **Additional Settings** > **Optional Settings**, and then select **CUSTOMIZE**.
5. Go to the **Traffic Filters** section.
6. Select or clear the following check boxes to permit or deny specific types of management and diagnostic access to the mgt0 interface, or to enable traffic between clients connected to the AP.
   - **Enable SSH**
   - **Enable Telnet**
   - **Enable Ping**
   - **Enable SNMP**
   - **Enable Inter-station Traffic**

   Note
   When an Ethernet interface is in access mode, stations can communicate directly with each other without sending traffic through the AP. In this case, the AP cannot control their traffic. However, the AP can block traffic between stations connected to an Ethernet interface and stations connected to a wireless interface through an SSID.

Continue customizing **Optional Settings** in the **Wireless Networks** configuration window. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Related Links

Add a Network Policy on page 134
Customize Wireless Network Optional Settings on page 231

Customize the User Profile Application Sequence

Complete the Add a Network Policy on page 134 task.

You can specify which profile you want to apply to user traffic. By default, an AP applies user profiles in the following order (the last one is the profile that the AP ultimately applies to user traffic):

- First, the AP applies the user profile indicated by attributes returned by a RADIUS server performing MAC authentication.
- Second, the AP applies the user profile specified in an SSID for traffic management. This overrides the first user profile.

- Third, the AP applies the user profile indicated by attributes returned from a RADIUS server when a captive web portal requires user authentication. This user profile overrides both the first and second profiles.

To give priority to a user profile by applying it later in the sequence, reorder the profiles.

This task is part of a series for configuring the **Optional Settings** for a standard wireless network. Use this task for configurations with different SSID components referencing different user profiles.

1. Go to **Configuration** > **Network**.
2. Select an existing policy, and then select .
3. Select **NEXT** to open the **Wireless Network** page.
4. Go to **Additional Settings** > **Optional Settings**, and then select **CUSTOMIZE**.
5. Go to the **Choose User Profile Application Sequence** section, and then use the arrows to change the application sequence.

Continue customizing **Optional Settings** in the **Wireless Networks** configuration window. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Related Links

Add a Network Policy on page 134
Customize Wireless Network Optional Settings on page 231

Customize Voice Enterprise Options

Complete the Add a Network Policy on page 134 task.

Navigate to **Optional Settings CUSTOMIZE** under **Additional Settings** in the **Configure Standard Wireless Networks** window.

This task is part of a series for configuring the **Optional Settings** for a standard wireless network. Use this task to customize Voice Enterprise options.

Note
To enable Voice Enterprise or 802.11r, the SSID must be configured to use WPA2 key management.

1. Go to Go to **Configuration** > **Network**.
2. Select an existing policy, and then select .
3. Select **NEXT** to open the **Wireless Network** page.
4. Go to **Additional Settings** > **Optional Settings**, and then select **CUSTOMIZE**.
5. Go to the **Voice Enterprise** section.
6. Select an option.
   - **Enable Voice Enterprise**—Select to enable all options that are required for full voice enterprise support.

- **Custom**—Select and choose one of the following options:
  - **Enable 802.11k**: (Radio Resource Measurement of Wireless LANs): Select to enable the devices to monitor the RF environment and network performance to help manage network usage and client roaming.
    - **Enable dualband neighbor list**: Select to enable APs to monitor 2.4 GHz, 5 GHz, and 6 GHz bands at the same time to widen the search for a less-loaded AP channel.
    - **Max. neighbor APs**: Set the maximum neighbor APs to send to the client to reduce the computational resources required for 802.11k handover.
  - **Enable 802.11v**: (IEEE 802.11 Wireless Network Management): Select to enable network devices and clients to share information such as location and neighbor information.
  - **Enable forced disassociation**: Select to enable APs to send disassociate or deauthenticate frames for a variety of reasons per 802.11v.
  - **Disassociate after**: (If forced disassociation is enabled.) Range: 0 to 5 seconds.
  - **SNR Checking**: (If forced disassociation is enabled.) Select to enable APs to consider signal-to-noise ratio to determine when to disassociate.
    - **Disassociate the Client**: : (If forced disassociation and SNR checking are enabled.) Select to enable APs to send disassociation frames to client devices.
    - **BSSID Transition Request**: (If forced disassociation and SNR checking are enabled.) Select to enable APs to send BSSID transmission management request frames to client devices.
  - **SLA Checking**: (If forced disassociation is enabled.) Select to enable Extreme Networks APs to consider service level agreement performance thresholds to determine when to disassociate.
    - **Disassociate the Client**: : (If forced disassociation and SLA checking are enabled.) Select to enable APs to send disassociation frames to client devices.
    - **BSSID Transition Request**: (If forced disassociation and SLA checking are enabled.) Select to enable APs to send BSSID transmission management request frames to client devices.
  - **Enable 802.11r**: (Fast BSS Transition): Select to optimize roaming by forcing stations to forward QoS state and encryption keys preemptively.

Continue customizing **Optional Settings** in the **Wireless Networks** configuration window. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Related Links

Add a Network Policy on page 134
Customize Wireless Network Optional Settings on page 231

Customize Wi-Fi Multimedia™

Complete the Add a Network Policy on page 134 task.

Enable Wi-Fi Multimedia™ (WMM) to prioritize network traffic according to the settings.

This task is part of a series for configuring the **Optional Settings** for a standard wireless network. Use this task to enable WMM and customize the settings.

1. Go to **Configuration** > **Network** .
2. Select an existing policy, and then select .
3. Select **NEXT** to open the **Wireless Network** page.
4. Go to **Additional Settings** > **Optional Settings**, and then select **CUSTOMIZE**.
5. Go to the **WMM** section, and then select **Enable WMM**.
6. Select and clear the following check boxes as required:
   - **Voice**—Select to enable admission control algorithms for voice traffic.
   - **Video**—Select to enable admission control algorithms for video traffic.
   - **Enable Unscheduled Automatic Power Save Delivery**—Select to enable stations to request queued traffic at any time, rather than receiving queued traffic scheduled with the beacon.

Continue customizing **Optional Settings** in the **Wireless Networks** configuration window. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Related Links

Add a Network Policy on page 134
Customize Wireless Network Optional Settings on page 231

Customize Broadcast and Multicast Handling Settings

Complete the Add a Network Policy on page 134 task.

To reduce unnecessary airtime usage for multicast transmissions, a device can convert multicast frames to unicast frames under certain conditions or at all times, and can drop multicast frames when there are no group members present to receive them. Unicast traffic can increase the reliability of video delivery. If a wireless client does not receive a unicast frame and does not reply with an ACK, the AP will retransmit. Multicast traffic does not support wireless frame delivery confirmation.

This task is part of a series for configuring the **Optional Settings** for a standard wireless network. Use this task to customize settings for broadcast and multicast handling.

1. Go to **Configuration** > **Network**.
2. Select an existing policy, and then select .
3. Select **NEXT** to open the **Wireless Network** page.
4. Go to **Additional Settings** > **Optional Settings**, and then select **CUSTOMIZE**.
5. Go to the **Broadcast and Multicast Handling** section, and then select one of the following **Convert IP Multicast to Unicast** options:
   - **Auto**: The device is enabled to convert multicast frames to unicast when the channel utilization or membership count conditions are met.
   - **Always**: The device makes the conversion unconditionally.
   - **Disable**: The device does not use the multicast-to-unicast conversion feature, but instead follows the standard 802.11 behavior for sending multicast frames.
6. Set the **Channel Utilization Threshold** from 1 to 100%.

7. Set the **Membership Count Threshold** from 1 to 30.
8. Select **Enable Non-Essential Broadcast Filtering** to reduce unnecessary broadcast and multicast traffic forwarding (such as AMRP, HSRP, LLC, and STP) from APs with no registered listeners.
9. Select **Enable Multicast Drop** to drop multicast and broadcast traffic, excluding frames for any of the selected protocols. With the exception of **MDNS**, by default, all protocols are selected and are therefore included in multicast and broadcast traffic. To exclude protocols in multicast and broadcast traffic, proceed as follows:
   - **DHCPv4**: Clear the check-box to drop Dynamic Host Configuration Protocol version 4.
   - **DHCPv6**: Clear the check box to drop Dynamic Host Configuration Protocol version 6.
   - **ARP**: Clear the check box to drop Address Resolution Protocol.
   - **IGMP-query**: Clear the check box to drop Internet Group Management Protocol queries.
   - **IPv6-Discovery**: Clear the check box to drop Internet Control Message Protocol router discovery messages.
   - **MDNS**: This check box is not selected by default and is therefore preset to drop multicast DNS frames. Select this check box to **include** multicast DNS frames in multicast and broadcast traffic.

Continue customizing **Optional Settings** in the **Wireless Networks** configuration window. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Related Links

Add a Network Policy on page 134
Customize Wireless Network Optional Settings on page 231

Customize Client Related Network Settings

Complete the Add a Network Policy on page 134 task.

Use this task to define client usage parameters that control how devices in the SSID transmit data, how neighboring devices exchange information with each other, and the maximum number of clients that the SSID supports.

1. Go to **Configuration** > **Network**.
2. Select an existing policy, and then select .
3. Select **NEXT** to open the **Wireless Network** page.
4. Go to **Additional Settings** > **Optional Settings**, and then select **CUSTOMIZE**.
5. Go to the **Client Related Network Settings** section, and then configure the settings:
   - **Maximum client limit**: Set the maximum number of clients that can associate with an SSID on a device.
   - **EAP Timeout** (Enterprise Security Mode Only): During the 802.1x authentication phase, in the event of an EAP retry due to packet loss or lack of response from the client, the AP can retry the EAP request. Some clients cannot properly handle fast retry timers, so this might need adjustment to facilitate fast recovery for bad RF environments.

- **RTS threshold**: The RTS (request-to-send) threshold indicates the minimum packet size to trigger an RTS/CTS (request-to-send/clear-to-send) exchange. The purpose of this exchange is to reserve the medium and thereby reduce collision interference.
- **Fragment threshold**: The fragment threshold indicates the minimum packet size to begin fragmenting packets before transmitting them. If there is a high level of interference, smaller packet sizes can reduce the need to retransmit packets and improve performance.
- **DTIM settings**: Extreme Networks devices include delivery traffic indication messages (DTIM) in beacons at scheduled intervals. DTIMs are included in beacons according to the DTIM period that you set. Increase the DTIM setting to improve battery life or shorten it to deliver buffered broadcast and multicast traffic more frequently.
- **Inactive client ageout**: Set the length of time to age out and automatically disassociate inactive clients.
- **EAP Retries** (Enterprise Security Mode Only): After the EAP timeout, authentication fails and the client tries to reconnect per this value.
- **Roaming cache update interval**: An Extreme Networks AP updates its neighbors about its currently associated clients. Neighboring APs use this information to update their roaming caches—if necessary—with the most up-to-date client information from their neighboring APs.
- **Roaming cache ageout**: By default, an Extreme Networks device removes an entry from its roaming cache if it is absent from 60 consecutive updates from a neighbor. You can change the number of times an entry must be absent.

Continue customizing **Optional Settings** in the **Wireless Networks** configuration window. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Related Links

Add a Network Policy on page 134
Customize Wireless Network Optional Settings on page 231

Customize Other Options

Complete the Add a Network Policy on page 134 task.

This task is part of a series for configuring the **Optional Settings** for a standard wireless network. Use this task to customize the **Other Options**.

1. Go to **Configuration** > **Network**
2. Select an existing policy, and then select .
3. Select **NEXT** to open the **Wireless Network** page.
4. Go to **Additional Settings** > **Optional Settings**, and then select **CUSTOMIZE**.
5. Select **Ignore broadcast probe request** to enable Extreme Networks devices hosting this SSID to ignore probe requests from wireless clients.

6. Select **Hide SSID (Stealth mode)** to enable a simple but ineffective method to secure a wireless network; it hides the SSID (Service Set Identifier).

   Note
   This method provides very little protection against anything but the most casual intrusion efforts.

7. Select **FTM(11mc) Responder Support** to enable client devices to determine their distance from the AP.

   If the civic address, latitude, longitude, or altitude of the AP is configured, the AP advertises this information in the beacon.

   Note
   Enabling FTM (Fine Timing Measurement) 11mc causes a radio reset.

8. Select **Enable enhanced RNR** to enhance roaming for 6 GHz clients, or clear the check box to turn off this feature.

   If you select **Broadcast SSID Using** > **6 GHz radio**, ExtremeCloud IQ (New) enables this feature by default. To disable the feature, turn off the 6 GHz radio.

9. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Finish configuring the network policy.

Related Links

Add a Network Policy on page 134
Customize Wireless Network Optional Settings on page 231

Configure Device Templates

Create or configure an existing network policy.

Use a device template to configure default port settings and other device functions for a specific Extreme Networks model using a visual diagram of the physical ports. After you configure a device template, you can:

- Assign various port types to the device ports, then apply the device template configuration settings to large numbers of devices of the same type.
- Apply different device templates to other devices in the same network policy.

Note
Each network policy has only one template corresponding to each device model. To update devices with different configurations for the same model, you must create a new network policy or modify an existing policy and then configure a new template.

1. To add an AP template to the network policy, select **2 Wireless** in the workflow and proceed to Configure AP Templates on page 240.
2. To add a switch template to the network policy, select **3 Switching** in the workflow and proceed to Configure Switch Templates on page 269.

   For legacy and Dell switch models, select **4 SR/Dell Switching** in the workflow.

Continue configuring the network policy.

Related Links

Configure AP Templates on page 240
Configure Switch Templates on page 269

Configure AP Templates

Create a network policy for the APs. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.

Create AP device templates with default settings for all APs, and settings that ExtremeCloud IQ (New) applies when APs are onboarded. You can then modify the default AP settings individually, as required. AP templates enable quick AP deployment, with most of the port settings already applied by the associated template. Some devices have extra possible configuration options, depending on the device model.

Use this task to configure an AP device template as part of a network policy.

1. On the **2 Wireless** page, select **Configuration Settings** > **AP Template**.
2. Select an existing AP Template, and then select , or to add a new one, select .

   To delete the selected template, select .
3. For a new template, type a **Name**, and for an existing template, edit as required.
4. Select the ports or interface icons on the template graphic.
   a. To select all of the ports and interfaces, choose **Select All Ports**.
   b. To deselect all of the ports and interfaces, select **Deselect All Ports**.
5. To **Assign** an Ethernet port profile, see Assign an Ethernet Port Profile on page 240.
6. To configure **Wireless Interfaces**, see Configure Wireless Interfaces for an AP Template on page 242.
7. To configure **Wired Interfaces**, see Configure Wired Interfaces for an AP Template on page 264.
8. To configure **SES-imagotag**, see Electronic Shelf Labeling on page 266.
9. To configure **Advanced Settings**, see Configure AP Device Template Advanced Settings on page 268.
10. Select **SAVE TEMPLATE**.

Continue configuring the network policy.

Related Links

Configure Device Templates on page 239

Assign an Ethernet Port Profile

An Ethernet port profile lets you manage a variety of features such as port status (on or off), port usage (bridge access, bridge 802.1Q, or uplink), wired connectivity, and MAC authentication.

This task is part of the network policy configuration workflow. Use this task to assign a port profile to device ports.

1. Select an existing AP Template, and then select , or to add a new one, select . to create a new template.
2. To assign an existing port profile, select one or more Ethernet ports on the AP template graphic.
   a. Select **Assign**.
   b. Select **Choose Existing**.
   c. Choose any of the options from the **Port Type Assignment** list, and select **Save**.
3. To create a new port profile, select **Create New**.
   a. Type a **Port Name** for the port type.
   b. (Optional) Type a **Description** for the port profile.
   c. Select the **Port Usage** type:
      - **Uplink Port**: Use to connect the AP to the WAN.
      - **Access Port**: Use for an AP in client access mode, connected to a forwarding device like a switch that supports multiple VLANs.
      - **Trunk Port**: Use to connect the AP in bridge mode to a forwarding device, such as a switch that supports multiple VLANs.
4. For **Wired Connectivity**, enable **User Authentication**.
5. See Configure an External RADIUS Server on page 203 if you are not selecting an existing RADIUS Server Group.
6. Enable **MAC Authentication**, see Configure MAC Authentication on page 177.
7. For **QoS Settings**, see Configure Marker Maps on page 224.
8. For **User Access Settings**, to add a new User Profile, see Add a User Profile on page 174.
9. For **Traffic Filter Management**, see Configure Traffic Filters Policy Settings on page 162.
10. For **Port Settings**, see Configure LLDP/CDP Policy Settings on page 151.
11. For **Storm Control Settings**, see Configure Storm Control on page 284.

Continue configuring the AP template.

Related Links

Configure Port Types on page 287

Enable STP—Device Configuration

Note
Switch templates are supported only for Switch Engine and Extreme XOS devices.

Use this task to enable STP and configure the settings for a switch template.

1. Go to **Configure** > **Common Objects** > **Policy** > **Switch Template**.
2. Select an existing template, and then select , or select +
3. From the **Configuration** menu, select **Device Configuration**.

4. Toggle **STP (Spanning Tree Protocol)** to **ON**.
5. Select the STP Mode:
   - **STP**—The initial version of this protocol uses a single tree without regard to VLAN. After convergence (30-50 seconds), only the root bridge sends configuration Bridge Protocol Data Units (BPDUs).
   - **RSTP (Rapid STP)**—Like STP, RSTP uses single tree without regard to VLAN. After convergence (a few millisecond to 6 seconds), all switches send BPDUs every 2 seconds.
   - **MSTP (Multiple STP)**—Multiple Spanning Tree Protocol (MSTP) can map a group of VLANs into a single Multiple Spanning Tree instance (MSTI). Configure the MSTP settings.
6. Select a **Priority** for STP from the drop-down list.
7. Configure the **STP Timers**:
   - **Forward Delay**—This is the time the switch spends in the listening and learning state. The default is 15 seconds, and the range is 4 to 30 seconds.
   - **Max Age**—This is the maximum time period before a bridge port saves configuration BPDU information. The default is 20 seconds, the range is 6 and 40 seconds.
8. Select **SAVE**.

Continue configuring the Ethernet port.

Configure Wireless Interfaces for an AP Template

This task is part of the network policy configuration workflow. Use this task to Use this task to configure the Wi-Fi 0, Wi-Fi 1, Wi-Fi 2, and IoT0 ports for an AP template, as part of a network policy.

1. Select a **Device Model**, and then select an existing **Template**, or a default template.
2. Scroll down to the **Wireless Interfaces** section.
3. Select an **Operating Mode**.
   - Mode 1: 2.4 GHz / 5 GHz (Full) / 6 GHz — Tri-Radio
   - Mode 2: Tri-Radio / 5GHz (Full) / 6 GHz — Full Band with Scan
   - Mode 3: 5 GHz (Low) / 5 GHz (High) / 6 GHz — Dual 5 GHz with 6 GHz
   - Mode 4: Tri-Radio / 5 GHz (Full) / 2.4 GHz — DBDC
   - Mode 5: 5 GHz (Low) / 5 GHz (High) / 2.4 GHz — Dual 5 GHz with 2.4 GHz
   - Mode 6: 6 GHz (Low) / 5 GHz (Full) / 6 GHz (High) — Dual 6 GHz with 5 GHz
4. Select either the **WiFi0**, **WiFi1**, **WiFi2**, or **IoT0** tab.

   Note
   The **IoT0** tab applies only to AP5010/AP5020 models.

5. Set the **Radio Status** to **On**.
6. Select a **Radio Profile**—or an **IoT Profile** if applicable.

   You can also add a new Radio Profile or IoT Profile here, or clone and modify an existing profile.

7. Select the **Radio Usage** type.
   - Select **Client Mode** to configure a device for AP client mode radio usage, and to configure advanced features such as **Port Forwarding Rules** and **DHCP Server** settings. Choose a **Client Mode Profile** from the drop-down list. If required, you can configure a new Client Mode Profile or edit an existing profile.
   - Select **Client Access** for normal client operation. Optionally, select **Backhaul Mesh Link** for wireless portal and mesh backhaul operation.
   - Select **Sensor** for presence operation.
8. Continue configuring the AP template, or select **Save Interface Settings**.

Related Links

Configure AP Templates on page 240
Configure a Radio Profile on page 244
Configure IoT Profile Settings on page 258
Configure a Client Mode Profile on page 243

Radio Profiles

A radio profile contains settings for the radios in APs. The radios generally operate in two frequency bands: radio 1 (WiFi0) operates at 2.4 GHz, and radio 2 (WiFi1) operates at 5 GHz. WiFi2 supports only the 6 GHz band for client access. The number of radios and frequency bands supported vary by AP model.

In the **Radio Profiles** window, you can view, add, modify, and delete radio profile settings. You can also modify radio profile settings when you configure a device template. See Configure Device Templates on page 239.

The **Radio Profiles** table displays the following information:

- **Radio Profile Name**: The name assigned to a profile when it was created. It is a convenient reference when assigning radio profiles to the WiFi0 and WiFi1 interfaces for an AP.
- **Applied to Radio**: 2.4 GHz, 5 GHz, or 6 GHz.
- **Radio Mode**: 802.11a, a/n, ac, b/g, g/n, ax, or be.
- **Used By**: Shows the number of devices associated with this radio profile. Hover over any non-zero number in this column to see the associated device templates.

Related Links

Configure Device Templates on page 239
Configure a Radio Profile on page 244
Configure Wireless Interfaces for an AP Template on page 242

Configure a Client Mode Profile

This task is part of the network policy configuration workflow. Use this task to configure a Client Mode Profile as part of a network policy.

1. While configuring **Radio Usage**, select an existing Client Mode Profile, and then select  , or to add a new one, select  .
2. Type a **Client Mode Profile Name**.

3. (Optional) Type a **Description**.

   Although optional, descriptions can be helpful when you are troubleshooting your network.
4. The **Enable Local Web Page** option is enabled by default.

   The client mode AP activates a local SSID portal web page, which includes choices to select and connect the client mode AP WAN-side radio to a WAN Wi-Fi network. Clear this check box to configure other options for this profile.
5. Choose one of the following DHCP server options:
   - In the **DHCP Server Scope** field, enter the first IP address of the DHCP server range. The first IP address in this range is the IP address used to display the client mode SSID portal web page. Make a note of this first IP address for later reference.
   - In the **DHCP Server Scope** field, enter a single IP address to reserve a specific client (MAC address) to an IP. A DHCP reservation is a permanent IP address assignment. It is a specific IP address within a DHCP scope that is permanently reserved for a specific DHCP client. DHCP reservations on the AP support security on the local side of the Network Address Translation (NAT) and ensure that the client IP address does not change.
   - Set the **Advanced DHCP Server** slider button to **On**, then choose a pre-configured **DHCP Server and Relay** agent.
6. Toggle **Enable Port Forwarding** to **ON**, and then configure **Port Forwarding Rules** as follows:
   a. Select the plus sign to add a new port forwarding rule.
   b. Enter a description of how this rule is to be used (optional).
   c. Select a number for the outside port in the range of 1025-65535 (reserved ports cannot be used).
   d. Select a number for the local port in the range of 1-65535.
   e. Select **TCP**, **UDP**, or **Both** from the **Protocol** drop-down list.
   f. Select a **Host IP Address** for the internal device from the drop-down list, or select the plus sign to add a new address.
   g. Select **Add**.
7. Select **SAVE**.

Related Links

Configure Wireless Interfaces for an AP Template on page 242

Configure a Radio Profile

Use this task to create or edit a radio profile for 2.4 GHz, 5 GHz or 6 GHz device interfaces. For more information about radio profiles, see Radio Profiles on page 243.

Note
Extreme Networks provides defaults for each item in this section. The following steps are optional, except for the required radio profile **Name**.

1. In the device template, select **Device Configuration** and expand **Wireless Interfaces.**.
2. Select the radio (2.4 GHz, 5 GHz, or 6 GHz).

3. Select an existing **Radio Profile**, and then select , or to add a new one, select ..
4. Type the radio profile **Name**.
5. Type a **Description**.

   Although optional, descriptions can be helpful when you are troubleshooting your network.
6. Select the desired 802 specification from the **Support Radio Modes** menu.
7. Select a **Supported Power Mode**.

   Note
   Only applicable to AP5020/AP4020 and future WiFi 7 APs.
8. To set the optimal maximum power level, enter a value for **Maximum Transmit Power**.
9. To set the minimum power level, enter a value for **Transmission Power Floor**.
10. To set the maximum value to which the radio power can drop below the current power level, type a value for **Transmission Power Drop**.
11. To set the maximum number of wireless clients that can use the radio, type a value for **Maximum Number of Clients**.

    (Default: 100, Range: 1-255)

    A lower value permits fewer concurrent connections to the AP and provides a higher quality of service. A high number of concurrent connections to a radio might affect the quality of service. While 100 might be a bit high for a classroom setting, higher values are suitable for larger public spaces, such as cafeterias or gymnasiums. A higher setting is appropriate for APs that serve dense outdoor areas with frequent connections that quickly roam to other areas.
12. Select **SAVE RADIO PROFILE**.

Now that you have completed the basic configuration, you can modify the advanced radio profile settings. Remember to select **SAVE RADIO PROFILE** after changing the **Advanced Settings**.

Related Links

Radio Profiles on page 243
Configure Neighborhood Analysis on page 246
Channel Selection on page 246
Configure Dynamic Channel Switching on page 249
Optimize Radio Usage on page 250
Configure Radio Settings on page 252
Configure Backhaul Failover on page 254
Configure an Outdoor Deployment on page 255
Configure RF Interface Reports on page 255
Configure Client SLA Definitions on page 256
Configure WMM QoS Settings on page 257
Configure Sensor Mode Scan Settings on page 258
Configure IoT Profile Settings on page 258

Configure Neighborhood Analysis

First, Configure a Radio Profile on page 244.

Using background scanning, an AP divides a full background channel scan into several shorter partial scans so they do not interfere with the beacons sent by the AP. The scan takes less time than the beacon interval (100 TU by default), and is spread out over multiple beacon intervals until the AP scans all available channels. Full scans occur at admin-defined intervals, with a default of 10 minutes.

This task is part of the Radio Profile configuration workflow. Use this task to configure neighborhood analysis (background scanning) settings.

Note
Extreme Networks provides defaults for each item in this section. The following steps are optional.

1. In the device template, select **Device Configuration** and expand **Wireless Interfaces.**.
2. Select the radio (2.4 GHz, 5 GHz, or 6 GHz).
3. Select an existing **Radio Profile**, and then select , or to add a new one, select ..
4. In the **Neighborhood Analysis** section, toggle **Background Scan** to **ON**.
   Background scanning is necessary for WIPS and Layer 3 roaming to function.
5. Set the interval between background scans of all radio channels.
   Perform Background Scan Every: The range is 1 to 1440 minutes (24 hours).
6. For **Skip Background Scan When**, specify when to skip background scans:
   - Select **Clients are connected** to enable an AP with connected clients to scan channels.
   - Select **Connected clients are in power save mode** to enable an AP to scan channels when connected clients are in power save mode.
   - Select **Network traffic with voice priority is detected** to prevent an AP from performing a background scan when voice traffic is detected.

   Voice traffic takes priority and is the least forgiving of slow or degraded connections.
7. Select **SAVE RADIO PROFILE**.

Related Links

Configure Channel Selection on page 248
Configure a Radio Profile on page 244

Channel Selection

2.4 GHz Radio Settings

The 2.4 GHz radio has between 11 and 14 channels, depending on the country code, but only three are completely non-overlapping (channels 1 - 6 - 11). Most wireless vendors recommend choosing one of the non-overlapping channels to avoid interference. However, in some cases, especially in very dense deployments, it can be better to use four channels, particularly in European countries where there are more channels available.

You can set the channel model as three or four channels, depending on the selected region (USA or Europe). When you select Europe, you can modify the channel choices and set a different combination of channels. If you disable limiting channel selection, the AP uses Advanced Channel Selection Protocol (ACSP) to determine the best among all available channels in its region, using data about channel utilization, interference, CRC errors, noise floor, and the number of neighbors and their signal strength. The AP then selects the best channel available.

5 GHz Radio Settings

The 5 GHz radio mode is 802.11a, 802.11n, or 802.11ac. One of the key features in the 802.11n and 802.11ac standards is channel bonding, in which the radio bonds two or four adjacent 20-MHz channels into one 40-MHz or 80-MHz channel to increase the transmit data bandwidth. Unlike the 2.4 GHz radio band, the 5 GHz band has enough space for channel bonding. When you enable channel bonding on an AP whose region code is **FCC** and choose **40 MHz** or **80 MHz**, ACSP automatically chooses the primary channel based on the current RF environment and optimizes channel usage.

You can also use channel bonding in the European Community in conjunction with Dynamic Frequency Selection (DFS), which makes channels 52-64 and 100-140 available in addition to channels non-DFS channels 36-48. Without DFS enabled, channel bonding is not recommended for client access in the European Community because only the Unlicensed National Information Infrastructure (U-NII) lower band would be available (5.15-5.25 GHz; bandwidth: 100 MHz; channels 36 - 40 - 44 - 48) and there would not be enough space for three non-overlapping 40-MHz channels.

Note
The DFS option only takes effect when the AP is configured with the country code of a country complying with European Telecommunications Standards Institute (ETSI) or Federal Communications Commission (FCC) regulations. All Extreme Networks APs are certified to use DFS channels in the ETSI region and all are certified for the FCC region.

The 5-GHz radio frequency spectrum is partitioned U-NII bands. Extreme Networks devices support the following:

- U-NII Low: 5.15-5.25 GHz (bandwidth: 100 MHz; available in the U.S. and E.C.)
- U-NII Upper: 5.725-5.85 GHz (bandwidth: 125 MHz; available in the U.S.)

Note
When a hive contains some APs that do not support channel bonding and others that do, the dynamic channel selection process works as follows:

- Channel selection for backhaul mode: The APs that support only 20-MHz channels converge on the control channel that the other members use as part of their 40-MHz channel.
- Channel selection for access mode: The APs that support only 20-MHz channels avoid choosing either the control channel or extension channel that the other members are using as part of their 40-MHz channels.

6 GHz Radio Settings

Wi-Fi 6 is the next generation of Wi-Fi based on 802.11ax HE (high efficiency) technology. Currently, AP3000, AP4000, AP4020 and AP5000 devices support Wi-Fi 6 on 160 MHz channels.

Wi-Fi 7 is a tri-radio based on 802.11be technology on 320 MHz channels. Currently, only AP5020 devices support Wi-Fi 7 across three bands - 2.4 GHz (4x4:4), 5 GHz (4x4:4), and 6 GHz (4x4:4).

Related Links

Configure Channel Selection on page 248

Configure Channel Selection

First, Configure a Radio Profile on page 244.

This task is part of the Radio Profile configuration workflow. Use this task to make changes to the device channel width. The available settings depend on the **Supported Radio Mode** that you selected in the basic configuration section.

Note
Extreme Networks provides defaults for each item in this section. The following steps are optional.
Channel selection is dimmed and set to **Auto**. Perform channel selection at the device level.

1. In the device template, select **Device Configuration** and expand **Wireless Interfaces.**.
2. Select the radio (2.4 GHz, 5 GHz, or 6 GHz).
3. Select an existing radio profile, and then select , or to add a new one, select ..
4. Specify the **Channel Width and Exclusions**.
   a. To customize the display, select and clear the check boxes as desired:
      - **Show UNII Groups**
      - **Show Frequency Markers**
      - **Show Primary Channels**
      - **Show Preferred Scan Channels (PSC)**
5. To manually exclude channels, select a specific channel.
6. Enable **Dynamic Frequency Selection** to help maintain a balance between Wi-Fi performance and avoid interference with essential radio services.

   Note
   Dynamic Frequency Selection (DFS) settings do not apply to AP121, AP141, AP330, and AP350 access points that were shipped after 2 June 2016 and operate in the FCC domain.

   a. Select **Enable manual channel selection return** to return the affected radio to its original statically assigned DFS channel after a DFS event.

b. Select **Enable ZeroWait DFS** to dedicate a single antenna chain to quickly identify a usable DFS channel. With ZeroWait DFS enabled, a 4x4 AP become a 3x3 AP.

Note
ZeroWait DFS is only available for 3- or 4-stream APs.

c. Select **Enable Background Scan** to enable DFS to run background scans.

7. To manually set **Transmission Power**, select **Manual** and then use the slider to select a dBm setting.
8. Enable **Enable client transmission power control (802.11h)**.
9. To manually enable client transmission power control (802.11h), use the slider to select a dBm setting.
10. Enable **Limit Channel Selection** to limit channel selection to non-overlapping channels.
    a. Select the operating **Region** for the device from the drop-down list.
    b. For **Channel Model**, select 3 channels for USA and 4 channels for Europe.
    c. For **Limit Channel Selection**, USA defaults are 1, 6, and 11, and European defaults are 1, 5, 9.
11. Enable **Use the last known power and channel during the AP boot up process**.
12. Select **SAVE RADIO PROFILE**.

Related Links

Channel Selection on page 246
Configure Dynamic Channel Switching on page 249
Configure a Radio Profile on page 244

Configure Dynamic Channel Switching

This task is part of the Radio Profile configuration workflow. Use this task to enable Dynamic Channel Switching (DCS) to select and switch channels based on specified criteria.

1. In the device template, select **Device Configuration** and expand **Wireless Interfaces.**.
2. Select the radio (2.4 GHz, 5 GHz, or 6 GHz).
3. Select an existing radio profile, and then select , or to add a new one, select ..
4. Expand **Advanced Settings** and toggle **Dynamic Channel Switching** to **ON**.
5. Select **Automatically select and switch channels during specified time interval**.
    a. In the **From** field, enter the start time for the interval.
    b. In the **To** field, enter the end time for the interval.

c. In the **Do not switch channels if the number of connected clients exceeds** field, specify the number of connected clients.

   If the number of associated clients is equal to or less than the specified value, and if the AP finds a better channel, it can switch to a new channel. Associated clients lose their connections and must reconnect. If the number of clients exceeds the value, the AP does not switch to a new channel. When a client de-authenticates during the scheduled time range, the AP checks the number of clients against the value. If the number of clients does not exceed the value, the AP switches channels. If the number of clients still exceeds the value, the AP does not change channels.

6. Select **Switch channels anytime if RF interference exceeds the threshold**.
   a. In the **Interference Threshold** field, enter the value (%).
   b. In the **CRC Error Threshold** field, enter the value (%).
   c. Select **Do not switch channels if clients are connected**.
7. Select **SAVE RADIO PROFILE**.

Related Links

Optimize Radio Usage on page 250
Configure Dynamic Channel Switching on page 249

Optimize Radio Usage

First, Configure a Radio Profile on page 244.

Management frames such as beacons, and probe and association requests and responses, consume airtime that might otherwise be used to transmit user data.

This task is part of the Radio Profile configuration workflow. Use this task to minimize management traffic by using higher data rates, and suppressing and reducing probe and association responses under certain circumstances.

Note
Use caution when configuring radio optimization settings. When device configuration limits specific clients, there is a risk that end user clients will deny access to the WLAN. Extreme Networks provides default values for each setting. Modifying the radio configuration is optional and should be done with caution.

1. In the device template, select **Device Configuration** and expand **Wireless Interfaces.**.
2. Select the radio (2.4 GHz, 5 GHz, or 6 GHz).
3. Select an existing radio profile, and then select , or to add a new one, select ..
4. Choose **High data rates** to transmit management frames at the highest basic data rate specified in an SSID or **Low data rates** to use the lowest basic data rate.
5. Select **Suppress successive requests within the same beacon interval** to enable APs to suppress responses to repeated probe requests from the same client received within a single beacon interval.

6. Select **Suppress response to broadcast probes by** to reduce responses to broadcast probe requests by enabling only one of several SSIDs to respond, in rotation, or reduce responses from specific client device types.

   With this feature enabled, select a suppression method:

   a. Select **Allowing only one SSID to respond at a time** to enable a single SSID to respond at a time.
   b. For **Reducing responses to certain client device types** add a new MAC OUI.

   See Configure a MAC Object and MAC OUI on page 251.

   Note
   When high-density WLAN optimization is enabled, the suppression setting is disabled by default.

7. Enable **Band Steering** and select a mode from the menu.
8. Use the slider to set the **Allowed percentage distribution of 2.4 and 5.0 GHz clients**.
9. Enable **Client Load Balancing** and configure the threshold settings.

Table 88: Load balance clients based on

Airtime	Number of clients
Ignore probe and association requests per device when threshold exceeds: • CRC Error Rate • RF Interference • Average Airtime Per Client	Ignore probe and association requests from clients associated with other Extreme Networks devices until: • Anchor Period Elapses • Query neighbors about client load every
Ignore probe and association requests from clients associated with other Extreme Networks devices until: • Anchor Period Elapses • Query neighbors about client load every	

10. Enable **Radio Load Balancing** and specify the **Number of Connection Attempts**.
11. Enable **Weak Signal Probe Request Suppression** and specify the **Signal-to-Noise Threshold** in dB.
12. Enable **Safety Net** and specify the time elapse, in seconds or minutes, before a device responds again to association requests after an overload incident.
13. Configure Configure Radio Settings on page 252.
14. Select **SAVE RADIO PROFILE**.

Related Links

Configure a MAC Object and MAC OUI on page 251
Configure Radio Settings on page 252
Configure a Radio Profile on page 244

Configure a MAC Object and MAC OUI

A MAC address is a 48-bit number typically written in hexadecimal notation that provides a unique address for each client device. An OUI is the first 24 bits of a MAC

address. After a MAC object is assigned to a device, it can be grouped to a specific hive. In a MAC firewall policy rule, you can determine which traffic to permit or deny based on the source or destination MAC address. In QoS traffic classification and marking policies, you can prioritize traffic based on the OUI.

Use this task to configure a MAC object and MAC OUI.

1. Select .
2. Select **MAC Address**.
3. Type a **Name**.
4. Type the **MAC Address**.
5. Select **SAVE**.
6. Select .
7. Select **MAC OUI**.
8. Type a **Name**.
9. Type the first six digits of the Mac address, for the **MAC OUI**.
10. Select **SAVE**.

Related Links

Optimize Radio Usage on page 250

Configure Radio Settings

First, Configure a Radio Profile on page 244.

You can configure whether you want to use long or short preambles, adjust the beacon period (or interval), and enable the detection of spoofed BSSIDs. For more information about radio settings, see Radio Settings on page 253.

This task is part of the Radio Profile configuration workflow. Use this task to configure the radio settings.

Note
Extreme Networks provides defaults for each item in this section. The following steps are optional.

1. Select the radio (2.4 GHz, 5 GHz, or 6 GHz).
2. Select an existing radio profile, and then select , or to add a new one, select ..
3. Expand the **Advanced Settings** section.
4. Select **Auto (Short/Long)** to enable support for short preambles or **Long** to disable short preamble support.
5. Set the period during which APs send beacons.
6. Set the Guard Interval to 800 nanoseconds by deselecting **Enable Short Guard Interval**.
7. To no longer combine data frames into larger frames before transmission, clear the check box for **Enable MAC Aggregate Protocol Data Units**.
8. Select **Enable Frame Burst** so a wireless client will transmit a burst sequence of up to three packets without releasing control of the transmission medium.

9. Select **Enable Transmit Beamforming** to improve data transfer rates for directional signal transmission processing.
10. Select **Enable MU-MIMO** to enable multiple users to receive data using different simultaneous spatial streams from an AP transmit radio chain.
11. If you selected **Enable MU-MIMO**, set **Station Receive Chain** to **Auto** or **1**, which is the chain the AP uses to receive data from the wireless client.
12. If you are using 802.11ax radios, enable **ODFMA**.
13. If you selected **Enable ODFMA**, select **Uplink** or **Downlink**.
14. If you are using 802.11ax radios, enable **BSS Coloring**.
15. If you selected **Enable BSS Coloring**, enter the numerical value of the new BSS color the AP will transmit after surpassing the beacon threshold.
16. Select **Enable Target Wake Time** to enable an AP to minimize medium contention between stations, and to reduce the required amount of **time** that a station in the power-save mode needs to be **awake**.
17. Select **SAVE RADIO PROFILE**.

Related Links

Configure a Radio Profile on page 244

Radio Settings

Preambles

When you enable short preambles, the AP broadcasts support of short preambles and attempts to negotiate using them with clients. If a client also supports short preambles, the client and AP agree to use them. If a client only supports long preambles, then the AP automatically adjusts to accommodate it, and they agree to use long preambles instead. When you select long preambles, the AP and client both agree to use long preambles. Although a short preamble saves time and improves throughput, a long preamble allows more time for the receiver to tune into and synchronize with the transmitting radio, providing additional decoding accuracy in noisier environments.

Beacon Periods

APs broadcast beacons to all clients within range, and by default, send beacons every 100 TUs (approximately 10 times per second). If APs are in an area with lots of background noise, you might want to add more time between beacon broadcasts, or set an interval from 40 to 3500 TUs (about 24 times per second to about every 3.5 seconds).

Guard Intervals

A guard interval is the amount of time between transmissions to ensure that they do not collide. The default is 800 nanoseconds, which is still suitable for large areas, such as warehouses or outdoors, where the distances between points of reflection are great. For smaller areas, such as office spaces, you can use a shorter interval of 400 nanoseconds. Enabling this option in the right environment can improve data rates.

Aggregate MAC Protocol Data Unit (AMPDU)

AMPDU transmissions reduce overhead when the transmission channel is busy. When AMPDU is enabled, the AP combines data frames into fewer, larger frames before

transmission, and recognizes the format of larger frames when it receives them. Generally, enabling AMPDU increases performance.

Frame Bursts

Frame bursts enable a wireless client to transmit data at a higher throughput by using the inter-frame wait intervals to burst a sequence of up to three packets without releasing control of the transmission medium.

BSS Colors

A basic service set (BSS) is the cornerstone topology of any 802.11 network. The communicating devices that make up a BSS consist of one access point radio with one or more client stations. The BSS color is a numerical identifier of the BSS. 802.11ax radios are able to differentiate between BSSs using BSS color identifiers when other radios transmit on the same channel. If the color is the same, this is considered to be an intra-BSS frame transmission. In other words, the transmitting radio belongs to the same BSS as the receiver. If the detected frame has a different BSS color from its own, then the station considers that frame as an inter-BSS frame from an overlapping BSS.

Related Links

Configure Radio Settings on page 252

Configure Backhaul Failover

First, Configure a Radio Profile on page 244.

When **Backhaul Failovers** are enabled, the AP forms a mesh link with other hive members and can failover backhaul communications from Eth0 to a wireless interface if the Ethernet link goes down.

Note
Extreme Networks provides defaults for each item in this section. The following steps are optional.

This task is part of the Radio Profile configuration workflow. Use this task to configure backhaul failover.

1. In the device template, select **Device Configuration** and expand **Wireless Interfaces.**.
2. Select the radio (2.4 GHz, 5 GHz, or 6 GHz).
3. Select an existing radio profile, and then select , or to add a new one, select ..
4. Enable **Backhaul Failover**.
5. Configure the following settings to define when to failover the backhaul link from Ethernet to wireless, and when to return the backhaul to Ethernet:
   a. In **Switch to Wireless Backhaul**, set how long the Ethernet link must be down to trigger a failover to the wireless link.
   b. In **Revert Back to Wired Backhaul**, set how long the Ethernet link must be up before the AP returns backhaul communications to Ethernet.

      Use the menu to specify the time in seconds or minutes.
6. Select **SAVE RADIO PROFILE**.

Related Links

Configure an Outdoor Deployment on page 255
Configure a Radio Profile on page 244

Configure an Outdoor Deployment

First, Configure a Radio Profile on page 244.

You can configure outdoor APs to communicate wirelessly with each other across a great distance by using a directional antenna for the backhaul link, while continuing to use omnidirectional antennas for access. However, you must make some adjustments to the radios to accommodate the longer transmission intervals. A Wi-Fi radio expects to receive an ACK for every transmitted Unicast frame. If it does not receive an ACK, it retransmits the frame. If the distance between the transmitter and receiver is too great, the ACK timeout period elapses before the ACK from the receiver reaches the transmitter, causing the transmitter to retransmit frames repeatedly until concluding that the frames are not reaching their target.

This task is part of the Radio Profile configuration workflow. Use this task to define the ACK timeout range between APs. By increasing the range, the radio increases the ACK timeout period accordingly.

1. In the device template, select **Device Configuration** and expand **Wireless Interfaces.**.
2. Select the radio (2.4 GHz, 5 GHz, or 6 GHz).
3. Select an existing radio profile, and then select , or to add a new one, select ..
4. Set a distance (between 300 and 10,000 meters) over which to support the radio.
5. Select **SAVE RADIO PROFILE**.

Related Links

Configure RF Interface Reports on page 255
Configure a Radio Profile on page 244

Configure RF Interface Reports

First, Configure a Radio Profile on page 244.

ExtremeCloud IQ can periodically poll APs and collect RF interface-related data. ExtremeCloud IQ forces APs to adopt a shorter polling interval if CRC error, channel interference, or short-term polling thresholds are exceeded.

Note
Extreme Networks provides defaults for each item in this section. The following steps are optional.

This task is part of the Radio Profile configuration workflow. Use this task to configure RF interference reports.

1. In the device template, select **Device Configuration** and expand **Wireless Interfaces.**.
2. Select the radio (2.4 GHz, 5 GHz, or 6 GHz).

3. Select an existing radio profile, and then select , or to add a new one, select ..
4. Set the level of CRC errors for polling.

   The default threshold is 20% for 802.11g/n, and 35% for 802.11a and 802.11ac. The range is from 15 to 60%.
5. Set the level of channel interference for polling.

   The default threshold is 20% for 802.11g/n, and 35% for 802.11a and 802.11ac. The range is from 15 to 60%.
6. Set the short-term average for polling.

   The range is 5 to 30 minutes.
7. Select **SAVE RADIO PROFILE**.

Related Links

Configure Client SLA Definitions on page 256
Configure a Radio Profile on page 244

Configure Client SLA Definitions

First, Configure a Radio Profile on page 244.

For each radio mode (or phymode)—11a, 11b, 11g, 11n, 11ac, 11ax—there are default settings for bit rate, success rate, and usage.

In most cases, the AP and client use several different rates to transmit and receive packets, changing rates as factors such as RSSI and packet loss change. To determine a common mid point to which various client scores can be compared, ExtremeCloud IQ provides three settings for each phymode:

Rate: This setting defines the transmission bit rated used by clients with healthy connectivity. For 80211a/b/g, rates are Mbps. For 802.11n, the rates are Mbps and modulation coding scheme (MCS).

Success: This setting defines the percentage of packets that you expect clients with healthy connectivity to transmit successfully (without retries) at the defined rate.

Usage: This setting defines the percentage of time that clients with healthy connectivity will transmit at the defined rate. The aggregated usage for the two bit rates must be equal to or less than 100%.

Note
To counter traffic congestion from clients with otherwise healthy Tx/Rx bit rates, APs can monitor client throughput and report SLA status to ExtremeCloud IQ. APs can also dynamically increase the amount of airtime for clients with a significant backlog of queued packets and improved throughput.

This task is part of the Radio Profile configuration workflow. Use this task to configure the client SLA definitions.

1. In the device template, select **Device Configuration** and expand **Wireless Interfaces.**.
2. Select the radio (2.4 GHz, 5 GHz, or 6 GHz).

3. Select an existing radio profile, and then select , or to add a new one, select .
4. To use the default settings, select one of the three options: **High Density (performance-oriented)**, **Normal Density**, or **Low Density (coverage-oriented)**.

   Alternately, to customize the settings for each option, select **CUSTOMIZE** and configure the settings on each tab.
5. Select **SAVE RADIO PROFILE**.

Related Links

Configure WMM QoS Settings on page 257
Configure a Radio Profile on page 244

Configure WMM QoS Settings

First, Configure a Radio Profile on page 244.

Wi-Fi Multimedia (WMM) classifies traffic into Voice, Video, Best-effort, and Background access categories, and provides mechanisms to prioritize each category at differing levels. **Contention Window Minimum**, **Contention Window Maximum**, and **AIFS** work together to determine the back-off time for each category. The first two define the minimum and maximum contention window parameters. When there is contention for access to the wireless medium, the AP calculates a random value between these two parameters. The higher the values, the longer the AP will back off during periods of access contention, resulting in longer delays for that traffic category. The lower the values, the shorter the back-off period, with shorter delays for traffic delivery. The AP adds the fixed arbitration interframe space (AIFS) back-off value to the first two values. The higher the setting, the longer the AP backs off, and the longer traffic is delayed during times of contention. The smaller the setting, the less time the AP backs off, resulting in shorter delays.

This task is part of the Radio Profile configuration workflow. Use this task to configure Wi-Fi Multimedia.

1. In the device template, select **Device Configuration** and expand **Wireless Interfaces.**.
2. Select the radio (2.4 GHz, 5 GHz, or 6 GHz).
3. Select an existing radio profile, and then select , or to add a new one, select ..
4. If necessary, modify the default settings in the **Contention Window Minimum**, **Contention Window Maximum**, and **AIFS** columns.
5. If necessary, modify the default setting in the **TXOP Limit** column to determine how long bursts of traffic last before relinquishing the medium.
6. Set the **No ACK** flag to inform the recipient not to send ACKs of the frames it receives, which is useful for the video category where lost packets in streaming video go unnoticed, and retransmissions are unnecessary.
7. Select **SAVE RADIO PROFILE**.

Related Links

Configure Sensor Mode Scan Settings on page 258
Configure a Radio Profile on page 244

Configure Sensor Mode Scan Settings

First, Configure a Radio Profile on page 244.

These settings determine how your APs behave during the scanning process. You can specify how long a device scans each channel and which channels to scan.

Note
Dwell time defines how long the radio transmits on a specific channel frequency to scan client probe requests before moving to the next channel in the sequence. For presence data collection, setting the dwell time above the default value raises the throughput of data collected on each channel. Setting the minimum dwell time below the default value reduces latency but also reduces the throughput of data collected on each channel.

This task is part of the Radio Profile configuration workflow. Use this task to configure scan settings for sensor mode.

1. In the device template, select **Device Configuration** and expand **Wireless Interfaces.**
2. Select the radio (2.4 GHz, 5 GHz, or 6 GHz).
3. Select an existing radio profile, and then select , or to add a new one, select .
4. If necessary, modify the **Dwell Time**.
5. Deselect **Scan All Channels** and set individual channel numbers to collect client probe request data.
6. Select **SAVE RADIO PROFILE**.

Related Links

Configure a Radio Profile on page 244

IoT Profiles

The IoT (Internet of Things) is a network of interconnected smart devices. Smart devices are embedded with software, sensors, and network connectivity that enables them to collect and share data. The smart devices communicate with each other and with other internet-enabled devices, like smartphones and gateways, creating a vast network of interconnected devices that can exchange data and perform a variety of tasks autonomously.

ExtremeCloud IQ (New) uses IoT profiles to support IoT applications.

Related Links

Configure IoT Profile Settings on page 258
Configure the Thread Commissioner on page 262

Configure IoT Profile Settings

First, Configure a Radio Profile on page 244.

This task is part of the Radio Profile configuration workflow. Use this task to configure an AP5010/AP5020 to function as a backbone border router in a thread network, as part of a network policy.

1. In the device template, select **Device Configuration** and expand **Wireless Interfaces.**

2. Select the **IoT0** tab.
3. Toggle **Radio Status** to **ON**.
4. Select an existing profile, and then select , or to add a new one, select .
5. Configure the settings as described in Table 89 on page 259 or Table 90 on page 260.
6. Select **Save**.
7. (Optional) Select **Customize** to Configure the Thread Commissioner on page 262.

Related Links

IoT Profile Settings on page 259
Configure the Thread Commissioner on page 262

IoT Profile Settings

- Thread Profile Settings (Single IoT Application)
- Thread Profile Settings (Multiple IoT Applications)

Table 89: Thread Profile Settings (Single IoT Application)

Setting	Description
Name	Enter a **Name** for the profile.
IoT Application(s) Supported	Select **Single** from the menu.
Function	The default is **Thread**.
Application	The default is **Thread Gateway**.
Network Name	Enter a **Network Name** for the Thread network of an AP. Each AP participates in a Thread network identified with the PAN ID and EXT PAN ID configured for the Thread Profile.
Network Key	Enter the **Network Key** used to encrypt communication between devices in a Thread network.
PAN ID	The **PAN ID** (Personal Area Network Identifier) identifies the Thread network of the AP. Enter a 16-bit value for use in RF data transmissions between devices in a Thread network.
EXT PAN ID	Enter a 64-bit value for use in RF data transmissions between devices in a Thread network. The **EXT PAN ID** must be unique. It is used for a more specific network identification.
Channel	Choose an IEEE 802.15.4 AP **Channel** number from the drop-down list (11-26). The default is channel 15. Note: Thread channel 25 is only supported if the country supports IEEE 802.11 channels 12, 13, or 14. Thread channel 26 is only supported if the country supports IEEE 802.11 channels 13 or 14.

Table 89: Thread Profile Settings (Single IoT Application) (continued)

Setting	Description
Default User Profile	Set the default VLAN user profile. Select an existing user profile to associate with this VLAN or create a new profile. To create a new user profile, see Add a User Profile on page 174. **Note:** Currently, only the VLAN of the associated User Profile is configured by the IoT profile.
Enable NAT64	**Enable NAT64** allows an AP to perform IPv6 to IPv4 translations between the Thread and backbone networks. This option is selected by default.
Add domain to upstream DNS queries	To append the domain name to the host name before forwarding the DNS query, select **Add domain to upstream DNS queries**.

Table 90: Thread Profile Settings (Multiple IoT Applications)

Setting	Description
Name	Enter a **Name** for the profile.
IoT Application(s) Supported	Select **Multiple** from the menu.
BLE Beacon	
Application	Select the corresponding check boxes for the applications that you want to configure: **iBeacon**, and **Eddystone-url**.
iBeacon	Edit the settings as required and select **SAVE**.
Eddystone-url Beacon	Edit the settings as required and select **SAVE**.
BLE Scan	
Application	Select the corresponding check boxes for the applications that you want to configure: **iBeacon**, **Eddystone-url**, and **Generic**.
Destination	Select **Cloud Reporting**, **Batch Reporting**, or both. Specify the interval in seconds. For **Batch Reporting**, specify the destination URL. To remove duplicate entries reported for the **Batch Reporting** interval, keeping only the latest entry for each BLE tag, toggle **Remove Duplicates** to **ON**. **Note:** ExtremeCloud IQ always removes duplicate entries for **Cloud Reporting**.
iBeacon Filter	Edit the settings as required and select **SAVE**.

Table 90: Thread Profile Settings (Multiple IoT Applications) (continued)

Setting	Description
Eddystone-url Beacon Filter	Edit the settings as required and select **SAVE**.
Generic Filter	Edit the settings as required and select **SAVE**. **Note:** If you select Custom for the **Vendor**, type the **Company Name** and the **Company ID**.

Related Links

Configure IoT Profile Settings on page 258

Thread Application

Thread is an IP-based, low-power wireless protocol designed to facilitate connecting to and controlling IoT devices. Thread uses a mesh architecture, which supports more efficient and robust networking.

Elements of a Thread network include the following:

- Thread Router
  - Manages communication between devices within the Thread network.
  - Maintains a routing table to promote the efficient routing of messages.
  - Generally has no ability to communicate with networks outside the Thread network.
- Border Router
  - Extends the capabilities of a Thread Router to allow communication with networks outside the Thread network.
  - Acts as a gateway to external networks.
  - Performs NAT (Network Address Translation) to facilitate communication between external networks and the Thread network.
- Backbone Border Router
  - Extends the capabilities of a Border Router to allow communication between the Thread network and backbone networks.
  - Supports fail-over mechanisms to ensure network resilience.
  - Generally supports higher capacity and greater speeds compared to regular routers for faster and more reliable communication with external networks.

With ExtremeCloud IQ (New), assign an IoT Thread profile to an AP5010/AP5020 wireless interface to have the device function as a BBR (Backbone Border Router).

Note

ExtremeCloud IQ (New) IoT Thread application is supported on AP5010/AP5020 only.

IoT Thread is not supported on simulated devices.

With ExtremeCloud IQ (New), the BBRs in the network negotiate and together elect one PBBR (Primary Backbone Border Router). The PBBR routes traffic between the Thread network and the Backbone network.

Although there can be multiple BBRs in a Thread network, only one can be PBBR at any time. The others act as secondary BBRs. If the PBBR is unreachable, failover occurs to a negotiated secondary BBR, which then becomes the new PBBR.

The IoT Thread profile allows for:

- Specifying key properties of the Thread network, such as its name, network key, PAN ID, Extended PAN ID, channel, and whether or not to enable NAT64.
- Optionally, you can specify the behavior of the Commissioner for the Thread network, including its credentials, timeout, and list of allowed devices.
- Optionally, you can configure the Default User Profile to be associated with the IoT Thread profile by applying only the VLAN.

Consider the following:

- IoT Thread profile configuration automatically takes precedence over BLE configuration. If BLE is configured and deployed, and later IoT Thread is configured and deployed, BLE becomes disabled and IoT Thread is enabled. If BLE configuration exists but has yet to be deployed, and then later IoT configuration is done and deployed, only the IoT configuration is pushed to the AP.
- Only one Commissioner can be active at any given time in a Thread network.

Related Links

IoT Profiles on page 258
Configure IoT Profile Settings on page 258
Configure the Thread Commissioner on page 262

Configure the Thread Commissioner

First, Configure IoT Profile Settings on page 258.

Use this task to define the behavior of the Thread Commissioner role, which can later be assigned to an AP5010/AP5020. The Thread Commissioner securely screens endpoint devices attempting to join the Thread network. The Commissioner uses an Allow List to identify the IoT endpoint devices which have permission to join the Thread network.

Note
Only one Commissioner can be active at any given time in a Thread network.

1. Select an existing Thread Application profile, and then select , or to add a new one, select .
2. Scroll down to **Commissioner**, and select **CUSTOMIZE**.
3. (Optional) Type the **Commissioner Credential** consisting of 6 to 250 alphanumeric characters.

4. (Optional) Set the **Commissioner Timeout** to a value in the range of 1-2000000 seconds.

   This value represents the ideal or known amount of time it takes for all the IoT endpoint devices defined in the Allow List to join the Thread network. The default is 120 seconds.

   Note
   If all of the IoT endpoint devices defined in the Allow List have joined the network but the Commissioner is still running because the Timeout value is set too high, you can force the Commissioner to stop running.

5. Under **Allow List of Thread-End Devices**, choose from the following actions:
   - Add devices to the Allow List either manually or in bulk, or using a combination of both methods.
     - To add devices manually, proceed to step 6 on page 263.
     - To add devices in bulk, proceed to step 7 on page 264.

     Note
     This method is available only after the Thread profile is saved.

   - Edit a device entry in the Allow List. Select the target entry, then select .

     Edit the entry according to steps 6.b on page 263 and 6.c on page 263, then select **Save**. When editing is complete, proceed to step 8 on page 264.
   - Delete entries in the Allow List. Select one or more entries, then select . Proceed to step 8 on page 264.
   - Download the entries in the Allow List to a csv file. Select .
   - Search for an entry in the Allow List. Enter a Joiner ID or PSK ID in the search field, then select .
6. Optionally, add devices to the **Allow List** manually, as follows:
   a. Select .
   b. In the **Joiner ID** field, enter a value consisting of 16 hex digits (excluding 16 "F"s) representing the device's EUI-64 (64-bit Extended Unique Identifier). Alternatively, enter * to admit any joiner.
   c. In the **Pre-Shared-Key for Device (PSKd)** field, enter a value for the shared password in the range of 6-32 alphanumeric characters (0-9, upper-case A-Y, excluding I, O, Q, and Z).
   d. Select **Add**.
   e. Repeat steps 6.a on page 263 through 6.d for each device added.
   f. Proceed to step 8 on page 264.

7. Optionally, add devices in bulk. Select **Import** to upload a csv file containing the device details. From the **Import Allow List of Thread End-Devices** window, choose from the following actions:
   - Deselect the **Delete all Allow List entries prior to import** check box to append the IoT device entries in a csv file to the existing Allow List. By default, this option is selected, resulting in the removal of existing Allow List entries before device entries in a csv file are imported.
   - Select **Download an example CSV import file** to view the required format of device entries to successfully import the list.
   - Drag to the **Choose File** field a csv file containing device entries to be imported, or select **Choose** to upload a locally stored csv file.
   - Select **Submit** to upload and add the device entries from the csv file to the Allow List, or select **Close** to exit the window.
8. To save the settings, select **Save**, or select **Cancel** to close the window without saving settings.

To assign the Thread Commissioner role to an AP, go to **Manage** > **Devices** < *select an AP5010 or AP5020*> **Actions** > **Start Thread Commissioner**. If necessary, you can select **Stop Thread Commissioner** and reassign the Commissioner role to another AP.

Related Links

Configure IoT Profile Settings on page 258

Configure Wired Interfaces for an AP Template

Create or edit an AP template.

This task is part of the network policy configuration workflow. Use this task to configure wired interfaces on the AP.

1. Select a **Device Model**, and then select an existing **Template**, or a default template.
2. Scroll down to the **Wired Interfaces** section.
3. To activate an Ethernet port, toggle the **Interface State** to **ON**.
4. Select one of the following **Port Types**:
   - **Uplink Port**: Use when connecting the AP to the WAN. Use when dynamic trunk port configurations are desired. The Uplink Port automatically translates SSDI configurations as well as global native and Management ports to reduce the need for static trunk port configurations.
   - **Access Port**: Use when the AP is working in client access mode and is connected to a forwarding device, such as a switch that supports multiple VLANs.
   - **Trunk Port**: Use when connecting the AP in bridge mode to a forwarding device, such as a switch that supports multiple VLANs.
5. For **Native VLAN (read only)**: The native (untagged) VLAN assigned to frames that do not have any 802.1Q VLAN tags in their headers.

   By default, Extreme Networks devices use VLAN 1 as the native VLAN. To apply VLANs to devices using classification (uplink port only; not trunk ports), highlight the Ethernet port icons and see Configure Classification Rules for a Device Template on page 289.

6. For **Allowed VLANs (read only)**: Enter the VLANs—including the native VLAN—that you want the trunk port to permit.

   You can list the VLANs individually, separated by commas, or as a range of VLANs using a hyphen. Alternatively, you can enter the word `all` in this field to support all existing VLANs previously configured in the network policy (the default). To apply VLANs to devices using classification (uplink port only; not trunk ports), highlight the Ethernet port icons and see Configure Classification Rules for a Device Template on page 289.
7. For **Fabric Attach**: Select the add icon, enter the device's associated **VLAN ID** and select its **I-SID#** from the drop down.

   Use this field to configure a device connected to an existing Fabric Connect network. The device must already be physically connected to the Fabric Connect switch.
8. For **Transmission Type**, select one of the following:
   - **Auto**: The switch negotiates the best common duplex mode 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.
9. Select the **Speed** the Ethernet port uses to communicate with the connected device.
10. Select **Green Ethernet** for AP4020 and AP5020 devices to enable Energy-Efficient Ethernet (EEE).

    The IEEE 802.3az standard, also known as EEE, introduces enhancements that enable physical layer transmitters to reduce power consumption during periods of idleness or low data activity. By enabling EEE, the network port can switch between active mode (during data transmission) and idle mode (when there is no Ethernet traffic), thereby consuming less power during idle or low activity states.
11. Select **LLDP** for devices to advertise their identities, status, and capabilities to each other.

    Devices can transmit data about themselves and receive transmitted data from other devices, but they cannot solicit and retrieve data from other devices.
12. Select **CDP** for devices to advertise an IP address that can send and receive SNMP traps.
13. Select **MCast Filter** to enable Multicast Rate Limiting on the interface for multicast/broadcast traffic, and configure **Multicast Rate Limit** to set the maximum rate (in Kbs) for incoming multicast traffic for the interface.
14. Optionally, set **USBNET** to **On** to activate the USB Port, and configure the **VLAN**.

    Note
    By default, the USB port will provide power when the AP is powered by 802.3 at the power source. If USBNET is enabled, it will be configured as an access port. The USBNET interface can be configured only for IQ Engine version 10.2r4 and later.

Continue configuring the AP template.

Electronic Shelf Labeling

Electronic Shelf Labeling (ESL) consists of the following components:

- ESL tags, which are 2.4 GHz RF-based battery powered devices
- An ESL communicator used to communicate with the ESL tags
- A server that provides the configuration and updates to the ESL tags

The following access points support Electronic Shelf Labeling:

- AP305C
- AP410C
- AP4020
- AP5010
- AP5020

Configure ESL on a device template or as an individual AP override.

Note
Consider the following for the ESL support.

- An ESL Server behind a NAT (Network Address Translation) or firewall is not supported.
- Do not make configuration changes during ESL programming and setup.

Related Links

Electronic Shelf Labeling Setup on page 266
Configure Electronic Shelf Labeling in a Device Template on page 267
Configure Electronic Shelf Labeling as a Device Override on page 267

Electronic Shelf Labeling Setup

Use this task to enable Electronic Shelf Labeling (ESL).

1. Prepare the AP device:
   a. Ensure that the access point is getting 3AT/3AT+ power.
   b. Connect ESL communicator to access point USB port.
   c. Ensure that the LED on the ESL communicator is red.
2. In ExtremeCloud IQ (New), Configure Electronic Shelf Labeling in a Device Template on page 267 or Configure Electronic Shelf Labeling as a Device Override on page 267 for a supported AP model.

   The following access points support Electronic Shelf Labeling:

   - AP305C
   - AP410C
   - AP4020
   - AP5010
   - AP5020

3. Ensure that the LED on the ESL communicator is amber.

Important
Troubleshooting Tips:

No LED light on ESL communicator

Check the power supply. The AP requires 3AT/3AT+ power supply to work with a USB port.

The LED continues to be red

Check the AP logs to verify that ThinAP2 has started.

The LED continues to be Amber

Check the IP address of AP, the AP-ID, and the connectivity between the AP and the ESL server.

Related Links

Electronic Shelf Labeling on page 266
Configure Electronic Shelf Labeling in a Device Template on page 267
Configure Electronic Shelf Labeling as a Device Override on page 267
Electronic Shelf Labeling Settings on page 268

Configure Electronic Shelf Labeling in a Device Template

Use this task to configure Electronic Shelf Labeling (ESL) in the device template.

1. Select an AP template for one of the supported AP models.

   The following access points support Electronic Shelf Labeling:

   - AP305C
   - AP410C
   - AP4020
   - AP5010
   - AP5020
2. Scroll down to the **Electronic Shelf Labeling** section and select **Enable Imagotag**.
3. Configure the Electronic Shelf Labeling Settings on page 268.

Related Links

Configure AP Templates on page 240
Electronic Shelf Labeling Settings on page 268

Configure Electronic Shelf Labeling as a Device Override

Use this task to configure Electronic Shelf Labeling as a device override.

1. From **Network Devices**, select a supported AP model.

   The following access points support Electronic Shelf Labeling:

   - AP305C
   - AP410C
   - AP4020

- AP5010
- AP5020

2. From the left pane, expand **Action** and select **Configure Device**.
3. In the **CONFIGURATION** section, select **Interface Settings**.
4. Scroll down to the **Electronic Shelf Labeling** section and select **Enable ESL**.
5. Configure the Electronic Shelf Labeling Settings on page 268.

Related Links

Electronic Shelf Labeling Settings on page 268

Electronic Shelf Labeling Settings

Configure the following settings for Electronic Shelf Labeling (ESL) support:

Server

The IP address of the ESL server.

Channel

The RF channel used for ESL communications. Set the channel to **Managed (Auto)** to have ExtremeCloud IQ (New) select the communications channel.

Port

The port associated with the defined rule. To explicitly specify a port number, type the port number in this field. Traffic from this port is subject to the defined rule.

VLAN

The VLAN used to route ESL traffic.

Related Links

Configure Electronic Shelf Labeling in a Device Template on page 267
Configure Electronic Shelf Labeling as a Device Override on page 267
Electronic Shelf Labeling on page 266

Configure AP Device Template Advanced Settings

ExtremeCloud IQ can update device firmware and reboot the device during onboarding.

Use this task to configure **Advanced Settings** for an AP device template.

1. In the device template, select **Advanced Settings**.
2. To upgrade the device firmware when onboarding, toggle **Upload device firmware upon device authentication** to **ON** .

   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.

     If you choose this option, select the firmware version. To manage the list of firmware versions, select **ADD/REMOVE**.

3. To **Reboot after uploading**, toggle the setting **ON**.

   Note
   As a best practice, disable the reboot option when deploying devices in a meshed environment.

4. For **Antenna Location Type**, select a location.

   Note
   - You must have IQ Engine Version 10.2.2 or higher. The 6 GHz radio is supported Low Power Indoor (LPI) only.
   - Antenna Location Type does not apply to AP5020.
   - Because different radio tables are used, a full config push is required.

5. For **Supplemental CLI**, see Configure Supplemental CLI on page 288.
6. Select a **Country Code** from the menu.

   Note
   For Legacy World and EU SKU devices, the template country code assignment only takes place when a device is initially onboarded.

7. Enable **Override MGT0 MTU** to manually enter a maximum transmission unit (MTU) value, ranging from 100-1500 Bytes. Default value is 1500 Bytes.
8. Enable **POE Profile Override** (AP5010 only), and select the override option from the menu.

   Hover over the **i** to view the corresponding override table.
9. Select **SAVE TEMPLATE**.

Related Links

Configure Supplemental CLI on page 288
Configure AP Templates on page 240

Configure Switch Templates

You can create a switch template during the network policy creation process, or at the device level after you have a network policy in place. Device-level changes to a switch template override settings in the network policy.

Create a network policy for the switch model. After you save the **Policy Details**, select **3 Switching/Routing**.

A switch template is a visual depiction of the physical ports on a switch. Configure how ports function by assigning port types and port usage settings to the template, and then applying the template to managed switches. The following steps describe how to create a switch template inside the network policy creation workflow.

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

This task is part of the network policy configuration workflow. Use this task to configure a switch template as part of a network policy.

1. On the **3 Switching/Routing** page, select **Configuration Settings** > **Switch Templates**.
2. To edit an existing switch template, select the corresponding link in the table, or to add a new template, select and select the switch model.
3. Type a **Name** for the template.
4. To make changes to the device configuration, enable **Override Policy Common Settings**.
5. For STP Configuration, see Configure Switch STP Settings on page 271.
6. 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.

7. Enable **IGMP Snooping** and configure the settings.
   - **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.
8. For **Extreme Loop Recovery Protocol Settings**, select to configure ELRP client periodic packet transmission for VLANs assigned to a port type to detect and prevent loops.

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

   Note
   ELRP must also be enabled within the switch template.

9. Enable **DHCP Snooping**, and select **Enable drop rogue DHCP Packets action**

   Ports configured as trusted do not apply the drop action. By default, port types configured as Trunk Port are trusted.
10. 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.
11. For **PSE Settings**, toggle to **On** to configure maximum power thresholds to generate alerts to ExtremeCloud IQ about exceeding maximum power levels.

12. Select **Enable Flow Control** to manage the port data receive transmission rate.
13. For **Management Interface Settings**, select one of the following options:
    - **Infer from device** (Switch Engine/EXOS): Select when the switch supplies the management interface.
    - **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.
14. For the **Port Configuration** section, see the following:
    - To configure **Instant Port Profile**, see Configure an Instant Port Profile on page 272.
    - To **Configure Ports in Bulk**, see Create a New Port Type on page 277
    - To **Configure Ports Individually**, see Configure Individual Ports on page 280
15. For **Supplemental CLI**, see Configure Supplemental CLI on page 288.
16. For **Advanced Settings**, see Configure Switch Device Template Advanced Settings on page 286.
17. Select **Save**.

Configure Switch STP Settings

Before you begin this task, create or modify a switch template.

By default, STP is disabled. Use this task to toggle it on and configure the settings. Extreme Networks recommends that you enable STP.

1. Toggle **STP (Spanning Tree Protocol)** to **ON**, and select one of the following modes:

   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: 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: Can map a group of VLANs into a single multiple spanning tree instance (MSTI). MSTP uses BPDUs to exchange information between spanning-tree compatible devices, to prevent loops in each MSTI by selecting active and blocked paths.
2. Select the **STP Bridge Priority**.

   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 parameters for **STP Timers**:

   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.

Instant Port Profiles

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

To configure IPP, perform the following tasks:

- Create an Instant Port Profile
- Create Instant Port Device Type

Related Links

Configure an Instant Port Profile on page 272
Configure an Instant Port Device Type on page 273

Configure an Instant Port Profile

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

1. On the switch template page, select **Port/VLAN Configuration** and then 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  .
2. Configure the Instant Port Profile Settings on page 272.

Related Links

Instant Port Profile Settings on page 272

Instant Port Profile Settings

Configure the following Instant Port Profile (IPP) settings.

Table 91: IPP Settings

Field	Description
Name	Type a **Name** for the IPP.
Description	Type a **Description** for the IPP.
Non-Forwarding VLAN	From the menu, select a VLAN to detect attached devices; this VLAN does not forward traffic. The non-forwarding VLAN cannot be utilized within a port type assigned to the switch.

Table 91: IPP Settings (continued)

Field	Description
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.
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 274.

Related Links

Instant Port Profiles on page 272
Configure an Instant Port Profile on page 272
Configure an Instant Port Device Type on page 273
IPP Device Type Settings on page 274

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, ExtremeCloud IQ (New) 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 274.
3. Select **Save** to commit changes, or select **Cancel**.

Related Links

Configure an Instant Port Profile on page 272

IPP Device Type Settings

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

Table 92: 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 92: 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 92: 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. • Select to edit a custom VLAN.
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. • 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...).

Table 92: IPP Device Type Settings (continued)

Field	Description
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. • 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. • Select to edit a custom Data VLAN.
STORM CONTROL tab	
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.

Related Links

Configure an Instant Port Device Type on page 273

Create a New Port Type

Create or modify a port type.

Use this task to create ports in bulk.

1. Either under **Create Ports in Bulk**, select one or more ports and select **Assign > Create New** or select (next to **Port Type** under **Configure Ports Individually**).
2. If this template applies to a 5570 or 5520 switch, define the VIM Port Channelization ports.
   a. Under **Configure Ports in Bulk**, select **Select VIM**.
   b. For a 5570 switch, select **VIM-6YE** or **VIM-2CE**.

c. For a 5520 switch, select **VIM-4X**, **VIM-4XE**, or **VIM-4YE**.

Note
If different templates for the same switch SKU are required to be created with different VIMs, then a classification rule can be created to assign the same template SKU with different VIM options to different devices. See Configure Classification Rules for a Device Template on page 289 for more information about classification rules.

d. Select one or more of these VIM ports and continue to Step 3.

3. Type a **Name**.
4. (Optional) Edit the associated **Description**.
5. Toggle the port **ON** or **OFF**.
6. In the **Port Usage Settings** section, select one of the following port types:
   - **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.
7. Select **Next**.
8. Select an existing VLAN or select the add icon to add a new one.

   To add a new VLAN, see Configure VLAN Settings on page 213.
9. Select **Next**.
10. Set authentication options for switches with Instant Secure Port enabled. By default User Authentication (802.1x) and MAC authentication will set the reauthentication period to 3600 seconds. Instant Secure Port Profile must be enabled within the network policy and switch template. For **Instant Secure Port Authentication Settings**:
    - **User Authentication**: Turn **On** for wired devices, such as printers, servers, and end-user computers.
    - **MAC Authentication**: Turn **On** for legacy devices that use MAC addresses as the user name and password to authenticate clients.
      - **Authentication Protocol**: Select the authentication protocol that determines how the port forwards requests to the RADIUS or Active Directory server. Valid values are PAP, CHAP, and MS Chap V2.

        With PAP, the port sends an unencrypted password to the RADIUS server. With CHAP or MS CHAP V2, instead of sending a password, the port and the authentication server perform the same operation on the password, the server compares the results to determine if the results match.
11. Select **Next**.
12. Add RADIUS Servers under **RADIUS Settings** to use this form of user authentication.

    Either select an existing **RADIUS Server Group** or select the add icon to add a new one. See Configure an External RADIUS Server on page 203.
13. For **Authentication Method Priority**, use the up or down arrows to determine the authentication method use order.

14. For **QoS Settings**, toggle **On** to create custom settings.

    Select the 802.1p classification system (marked in the L2 frame header in Ethernet frames) or the DiffServ codepoint marking system (marked in the L3 packet header) on outgoing packets from the drop-down list. See Configure Marker Maps on page 224.
15. Select **Next**.
16. For **Transmission Settings**, configure the following:
    - **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.
    - **Transmission Speed**: Choose the speed the switch port uses to communicate with the connected device.
    - **Debounce Timer**: Select the amount of time the switch does not register another input.
    - **CDP Receive**: Enables the switch to receive and parse the information within Cisco CDP frames.
    - **Auto MDIX**: Automatically detects the required cable connection type (straight through or crossover) and configures the connection appropriately.
    - **LLDP Transmit**: Enables the switch to transmit LLDPDU frames.

      Note
      Instant Port will not function correctly if LLDP Transmit is disabled, especially if LLDP-based matching is part of the Device Type Profile.

    - **LLDP Receive**: Enables the switch to receive LLDPDU frames.
17. Select **Next**.
18. For **STP**:
    - **STP Enabled**: 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 does 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 disables itself upon reception of a BPDU. The port enters the error-disabled state, and is removed from the active topology.
      - **Filter** - Controls whether a port explicitly configured as Edge transmits and receive BPDUs. You must select this option for Fabric Engine switches.
      - **Disabled** - Turns off BPDU Protection.
    - **Priority**: When this port is an STP edge port, select a port priority for STP from the drop-down list.
19. Select **Next**.

20. For **Storm Control**:
    - **Broadcast**: Select to include traffic that is forwarded to all destinations simultaneously.
    - **Unknown Unicast**: Select to include traffic whose destination address does not appear in the forwarding database.
    - **Multicast**: Select to include traffic whose destination is a multicast address.
    - **TCP-SYN**: Select to include TCP-SYN flood traffic.
    - **Thresholds**: Select **Byte Based** or **Packet Based**.
    - **Rate Limit Type**: Select **Kbps** (kilobytes per second) or **Percentage** if you selected **Byte Based** and **PPS** (packets per second) if you selected **Packet Based**.
    - **Rate Limit Value**: Enter when the switch should discard traffic of the selected types.
21. For **MAC Locking**, enable the per port type with the option to specify **Maximum First Arrival Limit** and specify the **Link Down Action**.

    By default, **Link Down Action** it is set to clear first arrival MACs, with the option to retain MAC's. We also have the option to take action when MACs are aged out.
22. Select general **ELRP Settings** and configure the settings:
    - 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.
23. Select **SAVE**.
24. For device-level ELRP interface options, select the specific interface check box and toggle **ELRP Enabled** to enable ELRP per port or toggle **ELRP Exclude** to exclude ELRP.
25. For **PSE**, select an existing profile or select the plus sign to add a new one.

    See Configure PSE on page 286.
26. Review all the port settings in the **Summary** section and select **Save** when complete.

Configure Individual Ports

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 **Port/VLAN Configuration**.
2. For **Port Name & Usage** and **VLAN**, see Configure Port Details on page 281.
3. For **Instant Secure Port Settings**, see Configure Authentication on page 282.
4.
5. For **Transmission Settings**, see Configure Transmission Settings on page 282.
6. For **STP**, see Configure STP Settings on page 283.
7. For **Storm Control**, see Configure Storm Control on page 284.

8. For **PSE**, see Configure PSE on page 286.
9. 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 280.

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 288.
- **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.

Related Links

Configure Individual Ports on page 280
Configure Authentication on page 282

Configure Authentication

First configure the **Port Name & Usage** and **VLAN** tabs. See Configure Port Details on page 281.

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 282.

Related Links

Configure Port Details on page 281
Configure Transmission Settings on page 282

Configure Transmission Settings

First, Configure Authentication on page 282.

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 283.

Related Links

Configure Authentication on page 282
Configure STP Settings on page 283

Configure STP Settings

First Configure Transmission Settings on page 282.

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 284.

Related Links

Configure Transmission Settings on page 282
Configure Storm Control on page 284

Configure Storm Control

First Configure STP Settings on page 283.

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 284.

Related Links

Configure STP Settings on page 283
Configure MAC Locking on page 284

Configure MAC Locking

First, configure Configure Storm Control on page 284.

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 93: 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 285.

Related Links

Configure Storm Control on page 284
Configure ELRP on page 285

Configure ELRP

First, Configure MAC Locking on page 284.

Extreme Loop Recovery Protocol (ELRP) is a loop protection mechanism designed to detect and prevent loops. In ExtremeCloud IQ (New) 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.

Related Links

Configure MAC Locking on page 284
Configure PSE on page 286

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.**

Related Links

Create a New Port Type on page 277

Configure Switch Device Template Advanced Settings

Create or edit a switch template.

ExtremeCloud IQ can update device firmware and reboot the device during onboarding.

1. Select the **Advanced Settings** tab.

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 288.

Complete configuring the device template.

Configure Port Types

After you select ports in a new device template, you must assign a port type. For AP ports, select **Choose Existing** or **Create New**. For switch ports, select from **Choose Existing**, **Create New**, or **Advanced Actions > Aggregate**.

Note
Only Switch Engine and Extreme XOS support port types.

For 1- and 2-port APs, there are three port types:

- **Bridge-Access ports** connect to individual hosts. You can configure captive web portal access, MAC authentication via a RADIUS server, change the user profile, and configure traffic management.
- **Bridge-802.1Q ports** provide network access through forwarding devices and support multiple VLANs. You can change the default user profile and manage incoming traffic.
- **Uplink Ports** act as WAN uplinks. You can change the default user profile and configure traffic control settings.

For 24- and 48-port switch templates there are three port types:

- **Access Ports** are connected to individual hosts such as printers, servers, and end user computers. A VLAN ID tag is added to the frame before it is forwarded using the 802.1Q tagging protocol. You can enable User Authentication or MAC Authentication, and configure QoS settings, Client Detection and VLAN ID.
- **Phone Data Ports** are used for voice transmission.
- **Trunk Port frames that are not VLAN-aware**. Frames are in a native VLAN (default) or Management VLAN.

You can also configure ports at the device level. Port settings that you configure there override any settings you make in the network policy device template.

Use this task to configure port types as part of a network policy.

1. Select an existing device template, and then select , or to add a new one, select ..

2. To assign an existing port type, select the port and then select **Assign**.
3. To create a new port type and assign it to a port at the same time, select an interface port, then select **Assign** > **Create New**.
4. Type a **Name** for the port type.
5. (Optional) Type a brief **Description** for the port type.
6. Turn the port off or on.
7. Select **Save**.

Related Links

Assign an Ethernet Port Profile on page 240

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. Toggle **LACP (Link Aggregation Control Protocol)** to **ON**.

   If LACP (Link Aggregation Control Protocol) is disabled, ExtremeCloud IQ (New) creates a static LAG.
3. Use the arrows to add or remove ports from the LAG.
4. Select the **Master Port**.
5. Select a **Port Load Balancing** option.

Configure Supplemental CLI

First, enable Supplemental CLI in ExtremeCloud IQ. Go to **Global Settings** > **VIQ Management**, and toggle **Supplemental CLI** to **ON**.

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

To avoid an unnecessary system reboot, select **Delta Configuration Update**. ExtremeCloud IQ (New) 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. Select an existing Supplemental CLI object, and then select , or to add a new one, select .

2. Type a **Name**.
3. (Optional) Type an optional **Description**.

   Although optional, descriptions can be helpful when you are troubleshooting your network.
4. 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.
5. Select **SAVE TEMPLATE**.

Related Links

Configure AP Device Template Advanced Settings on page 268
Configure the SSID for a Standard Wireless Network on page 165

Configure Classification Rules for a Device Template

Before you can add classification rules to a network policy, you must add a default AP device template and a location for the target AP. Also, create cloud config groups, IP addresses, and IP subnets.

You can create classification rules as part of a network policy or as a common object. Use this task to create classification rules associated with a network policy. ExtremeCloud IQ (New) supports multiple classification rules for DNS servers, VLANs, RADIUS servers, device templates, user groups, and private client groups (PCGs).

- 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.

This task is part of the network policy configuration workflow. Use this task to configure classification rules for a device template, as part of a network policy.

1. Go to **Configuration** > **Network**.
2. Select an existing policy, and then select , or to add a new one, select ..
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. From the **Configuration Settings** menu, select **AP Template**.

5. Select and choose the desired default template.

   Default templates apply to all of the devices of the selected template type that do not have a matching classification rule.
6. Select , and then select the desired device template.

   Classification rules templates apply only to the devices of the selected template type that match the rules.
7. Type the new **Template Name**.
8. Select **SAVE TEMPLATE**.

   The new template appears in the table, in the main AP template window. The **Classification Rules** column for the template contains the controls for configuring classification rules.
9. To assign an existing classification rule, in the **Classification Rules** column, select .
   a. Select an existing classification rule.
   b. Select **Link**.
10. To create and assign a new classification rule, in the **Classification Rules** column, select .
    a. Type a **Name** for the rule.
    b. Type a **Description**.

       Although optional, entering a description is helpful for troubleshooting and for identifying the rule.
    c. Select , and then select the rule category to configure.

       Choose from the following rule categories:

Table 94: Rule categories

Selected rule category	Do this
Device Location	i. Drill down until you reach the location level at which the device resides. ii. Select **Select**. The location appears in the **Classification Rules** table.
Cloud Config Group	i. Select the **Match Type**. ii. To use an existing group, select and choose an existing object, or to add a new one, select . For more information, see Add a Cloud Config Group on page 291. iii. Select **CLOUD CONFIG GROUP**. iv. Select **CONTINUE**.
IP Address	i. From the **Match Type** menu, select **Contains** or **Does Not Contain**. ii. To use an existing IP address, select and choose an existing object, or to add a new one, select . menu. iii. Select **SAVE IP**. iv. Select **CONTINUE**.

Table 94: Rule categories (continued)

Selected rule category	Do this
IP Subnet	i. From the **Match Type** menu, select **Contains** or **Does Not Contain**. ii. To use an existing IP subnet, select and choose an existing object, or to add a new one, select . iii. Select **SAVE SUBNET**. iv. Select **CONTINUE**.
IP Range	i. From the **Match Type** menu, select **Contains** or **Does Not Contain**. ii. To use an existing IP range, select and choose an existing object, or to add a new one, select . iii. Select **SAVE IP**. iv. Select **CONTINUE**.

11. 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.

    ExtremeCloud IQ (New) 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.
12. Select **SAVE RULE**.

Related Links

Add a Cloud Config Group on page 291

Add a Cloud Config Group

Before you begin, configure devices to associate with the cloud configuration groups.

Use cloud configuration groups to create network-level policies that can be replicated for multiple network roll-out scenarios. Use this task to create a new cloud config group as part of a network policy.

1. Type a **Name** for the new group.
2. (Optional) Type a **Description** for the new group.
3. Select real and simulated devices to have their host names shown 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. Selec t**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**.

Related Links

Configure Classification Rules for a Device Template on page 289
Configure the SSID for a Standard Wireless Network on page 165

Fabric Attach

Fabric Attach is a software-based feature that automates the connection to the Fabric Connect environment, enabling devices and their associated end-points to be quickly mapped to the appropriate virtualized Fabric Connect service.

Provisioning a non-fabric AP to the Fabric Connect network is as easy as taking the Fabric Attach-enabled AP out of the box and physically connecting it to a Fabric Connect-enabled switch. The Fabric Attach device then automatically configures itself with the appropriate management VLAN, preparing itself for the dynamic extension of virtualized fabric services on behalf of its connected end-point devices or users. This can speed the deployment of edge devices to the Fabric Connect environment since no manual configuration is required, and can be especially valuable at locations where networking skills are at a premium, such as remote offices.

ExtremeCloud IQ (New) APs support the following functions:

- Discover the Fabric Attach Server upon start up.
- Receive management VLAN configuration from the Fabric Attach Server, if discovered.
- Configure received management VLAN on the Management interface and Ethernet interface of the AP.
- Establish the management plane communication path to ExtremeCloud IQ (New).
- Support Native VLAN Tagging on the Management interface.

ExtremeCloud IQ APs do not support the following functions:

- Get VLAN to I-SID Mapping from ExtremeCloud IQ (New) as a management command.
- Configure the Fabric Attach Server port with VLAN to I-SID mapping.
- Establish data plane communication path for every configured VLAN.

Related Links

Configure Fabric Attach on page 292

Configure Fabric Attach

Before you begin, physically connect the device to a Fabric Connect-enabled switch. To perform the following task, you require the device VLAN ID and I-SID number.

For more information about Fabric Attach, see Fabric Attach on page 292.

This task is part of the network policy configuration workflow. Use this task to configure Fabric Attach for a device connected to an existing Fabric Connect network.

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

2. Select an existing network policy, and then select , or to add a new one, select .
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. Select an existing **Device Template** to edit, or select .
5. Scroll down to the **Wired Interfaces** section.
6. To use an existing **Fabric Attach** profile, and choose an existing object, or to add a new one, select .
7. Type a **Name** for the new profile.
8. (Optional) Type a description for the new profile.
   Although optional, descriptions can be helpful when you are troubleshooting your network.
9. Select to add a VLAN.
10. Type the associated **VLAN ID** for the device.
11. Select the **I-SID#** for the device from the drop down.
12. Select **SAVE**.

Related Links

Fabric Attach on page 292
Configure the SSID for a Standard Wireless Network on page 165

Configure Device Data Collection and Monitoring Options

First, create a network policy.

This task is part of the network policy configuration workflow. Use this task to set the following data collection and monitoring options:

- **Application Visibility and Control (AVC)**: AVC gives you information that can help you manage network traffic and applications. AVC detects the application-layer contents of the frame to determine the application or protocol that is transmitting the data. ExtremeCloud IQ (New) can then track the amount of data being transmitted by a particular application or protocol.
- **Device Wireless Activity Thresholds**: Set activity threshold limits above which event alarms are generated.
- **Client Wireless Activity Thresholds**: These alarms identify when violations occur that affect the wireless health of a client as reported in SLA reports for non-compliant clients. To trigger more alarms, lower thresholds. To reduce the number of alarms, increase thresholds.
- **Kernel Diagnostic Data Recorder (KDDR)**: KDDR logs capture run-time statistical data about unexpected events for Extreme Networks devices. Extreme Networks Support analyzes the content of these binary log files for troubleshooting.
- **Automatic Synthetic Traffic Generation**: Some of the Client 360°, Device 360°, and Network 360° monitoring capabilities require synthetic traffic generation.

1. Go to **Configuration** > **Network**.
2. Select an existing policy, and then select , or to add a new one, select ..
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. From the **Application Management** menu, select **Device Data Collection And Monitoring**.

5. Toggle the **Application Visibility and Control** setting **ON** to detect frame application-layer contents.
6. Toggle the **Statistics Collection** setting **ON** to record wireless activity statistics between the device and connected clients.
7. To change the data collection interval, select the number of minutes from the menu.
8. For **Device Wireless Activity Thresholds**, type values for the following fields:
   - **CRC error rate exceeds**: The point at which the percent of CRC errors in received wireless frames during the collection interval is considered to be excessive.
   - **Tx drop rate exceeds**: The point at which the percent of transmitted wireless unicast frames that a device drops during the collection interval is considered excessive. A transmitted wireless frame is dropped when the device tries to transmit the same unicast frame a maximum number of times without receiving an acknowledgment from the intended recipient.
   - **Rx drop rate exceeds**: The point at which the percent of dropped wireless frames during collection interval is considered excessive. A device might drop wireless frames on its ingress Wi-Fi interface for several reasons, such as the arrival of duplicate frames or frames that cannot be decrypted.
   - **Tx retry rate exceeds**: The point at which the percent of retransmitted wireless frames during the collection interval is considered excessive. A device tries to resend a unicast frame if the first effort does not elicit an acknowledgment from its intended recipient.
   - **Airtime Consumption exceeds**: The point at which the percent of transmitted and received airtime usage for a wireless interface during the collection interval exceeds the maximum airtime consumption threshold.
9. For **Client Wireless Activity Thresholds**, type values for the following fields:

   Tx drop rate exceeds: Indicates the point at which the percent of wireless unicast frames that a device drops during transmission to the same client during the statistics collection interval is considered excessive.

   Rx drop rate exceeds: Indicates the point at which the percent of dropped wireless frames received from the same client during the statistics collection interval is considered excessive.

   Tx retry rate exceeds: Indicates the point at which the percent of retransmitted wireless frames to the same client during the collection interval is considered excessive.

   Airtime Consumption exceeds: Indicates the point at which the percent of airtime that a device consumes while transmitting traffic to and receiving traffic from the same client during the collection interval is considered excessive.
10. Toggle the **Kernel Diagnostic Data Recorder** setting **ON** to capture run-time statistical data about unexpected events.
11. For **Automatic Synthetic Traffic Generation**:
    a. Enable **RADIUS Authentication** to create synthetic traffic.
    b. Toggle the **Check Radius service connectivity via Status-Server** setting **ON** to check RADIUS service connectivity.

       Ensure that **Status-Server** is enabled on the RADIUS server.

c. Adjust the check **Interval** if necessary.

Related Links

Configure the SSID for a Standard Wireless Network on page 165

Configure the BLE Service

First, configure a network policy.

Consider the following:

- The BLE Service settings configured in this task apply to the Device template associated with the network policy. You can override the settings configured here, and also configure device-level settings, by going to **Manage** > **Devices** > **Configure** > **Interface Settings** > **Wireless Interfaces** > **BLE Service**.
- IoT Thread profile configuration automatically takes precedence over BLE configuration. If BLE is configured and deployed, and later IoT Thread is configured and deployed, BLE becomes disabled and IoT Thread is enabled. If BLE configuration exists but has yet to be deployed, and then later IoT configuration is done and deployed, only the IoT configuration is pushed to the AP.

You can configure the embedded BLE transmitter in APs. As transmitters, these beacons broadcast numerical advertisements that trigger an action on Bluetooth-enabled devices that come within range. For example, an app running on a mobile device might react to a BLE signal by displaying welcome messages, sale announcements, or coupons.

This task is part of the network policy configuration workflow. Use this task to configure the iBeacon service for a network policy.

1. Go to **Configuration** > **Network**.
2. Select an existing policy, and then select , or to add a new one, select .
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. From the **Application Management** menu, select **BLE Service**.
5. Toggle the **BLE Services** setting **ON**.
6. Type a **Service Name**.
7. (Optional) Type a **Description**.

   Although optional, entering a description is helpful for troubleshooting and identification.

8. For **BLE Scan**, select **iBeacon** or **Generic** or both, and then configure the **Destination** settings.

Table 95: Destination settings

Setting		Description
Cloud Reporting (iBeacon scan only)		Toggle **ON** to enable Cloud Reporting for the device. Deselect to disable Cloud Reporting for the device. Cloud Reporting provides real-time analytics and insights into the performance and usage of your BLE network. Use this feature to monitor key metrics, track user interactions, and optimize BLE for maximum efficiency.
	Interval	Specify an interval value between 10-1200 seconds to determine how often iBeacon transmits to ExtremeCloud IQ (New). The default value is 60 seconds.
Batch Reporting (Required for Generic BLE scan)		Toggle **ON** to submit iBeacon reports in batch files. Batch Reporting compiles and analyzes large sets of iBeacon interaction data at scheduled intervals. This feature is ideal for generating periodic reports and gaining insights into long-term trends and patterns.
	Interval	Specify an interval value between 10-60 seconds to determine how often iBeacon transmits batch file reports. The default is 10 seconds.
	URL	Type the destination URL to submit batch file reports.
Ignore Duplicates		Enable this feature to remove duplicate entries automatically, within the specified time interval.
Secure Connection		Toggle **ON** and specify the credentials to secure the data flow to your server.
Token renewal setting		
	Client ID	Specify the unique identifier assigned to the client application. (String, 10-255 characters)
	Client Secret	Specify the confidential key used to authenticate the client. (String, 10-255 characters)
	Show Password	Select the check box to show the password (Client Secret).
	Token URL	Specify the API URL where the client sends requests to obtain or refresh access tokens. (String, valid URL format, max 255 characters)

9. Configure the **iBeacon Filter** settings (iBeacon Filter only).

Table 96: iBeacon Filter settings

Setting	Description
Min RSS(dBm)	The minimum Received Signal Strenth (RSS) value used for filtering iBeacon signals. RSS is measured in dBm (decibels relative to 1 milliwatt).
UUID	The iBeacon unique identifier. If your organization already has a UUID number, type it in the **iBeacon UUID** field. UUID format: 32 hexadecimal (base 16) digits, displayed in five groups separated by hyphens, in the form 8-4-4-4-12 for a total of 36 characters (32 alphanumeric and four hyphens). For example: 123e4567-e89b-12d3-a456-426655440000 You can also automatically create a UUID with an online UUID generator, such as the one at https://www.uuidgenerator.net/.

10. Configure the **Generic Filter** settings (Generic Filter only).

Table 97: Generic Filter settings

Setting		Description
Min RSS(dBm)		The minimum Received Signal Strength (RSS) value used for filtering generic signals. RSS is measured in dBm (decibels relative to 1 milliwatt).
Vendor		Select **Any**, **CHORUS**, or **Custom**.
	Any	Select **Any** to accept all beacons.
	Chorus	Select **Chorus** to auto-populate the settings for this vendor, and then select **ADD**.
	Custom	Select **Custom**, type the **Name** and **Company Id** of the vendor, and then select **ADD**. You can specify an ID for up to five vendors.

11. Select **Save**.

Related Links

Configure the SSID for a Standard Wireless Network on page 165

Configure Presence Analytics

First, configure a network policy.

Note

It is not necessary to change the default values if devices are connected over faster links.

Adjust these settings to accommodate situations where devices are connected over slower links and where the data must be aggregated at different rates.

This task is part of the network policy configuration workflow. Use this task to specify how frequently APs send data to ExtremeCloud IQ (New).

1. Go to **Configuration** > **Network**.
2. Select an existing policy, and then select , or to add a new one, select ..
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. From the **Application Management** menu, select **Presence Analytics**.
5. Toggle the **Enable Presence Analytics** setting **ON**.
6. Type a **Name**.
7. (Optional) Type a **Description**.

   Although optional, entering a description is helpful for troubleshooting and for identification.
8. For **Trap Interval**, specify (in seconds) how often the presence sensor reports data to ExtremeCloud IQ.

   Lowering this interval below 15 seconds pushes data faster but also increases network traffic. Raising this interval above 15 seconds pushes data at a slower rate and decreases network traffic.
9. Specify the **Aging Time** (in seconds) for a given presence profile.
10. Specify the **Aggregate Time** interval (in seconds) for the set period during which aggregation occurs for the presence profile.

Related Links

Configure the SSID for a Standard Wireless Network on page 165

Configure WIPS

This task is part of the network policy configuration workflow. Use this task to enable and configure the Extreme Networks Wireless Intrusion Prevention System (WIPS), as part of a wireless network policy.

1. Go to **Configuration** > **Network**.
2. Select an existing network policy, and then select , or to add a new one, select ..
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. From the **Application Management** menu, select **WIPS**.
5. Toggle **WIPS** to **ON**, and configure the settings.

   For more information, see WIPS Policy Settings on page 299.

   To reuse WIPS settings, select and choose a WIPS policy object.
6. Select **SAVE**.

Related Links

WIPS Policy Settings on page 299
Configure the SSID for a Standard Wireless Network on page 165

WIPS Policy Settings

Table 98: Settings for WIPS policy

Setting	Description
Name	Type a **Name** for the new policy.
Description	(Optional) Type a **Description**. Although optional, descriptions can be helpful when you are troubleshooting your network.
AirDefense Essentials	Toggle **AirDefense Essentials** to **OFF** to disable it, and then select **Save**. By default, **AirDefense Essentials** is **ON** (enabled). To **Allow change of operating channel for air-termination**, select the check box.
Rogue Access Point Detection	
Rogue Access Point Detection (Legacy)	Toggle **Rogue Access Point Detection (Legacy) ON** to enable the feature.
Determine if detected rogue APs are connected to your wired (backhaul) network	Use **Determine if detected rogue APs are connected to your wired (backhaul) network** in combination with other WIPS techniques to determine if a detected rogue AP is in the same network as compliant APs. An Extreme Networks AP builds a MAC learning table from source MAC addresses in the broadcast traffic it receives from devices in its Layer 2 broadcast domain. When an AP running XOS 5.0r2 or later detects a rogue AP through any of the rogue detection mechanisms in the WIPS policy, it checks the MAC learning table for an entry within a 64-address range above or below the BSSID of the invalid SSID. If there is a match, it is assumes that both MAC addresses belong to the same device. Because one of its addresses is in the MAC learning table, the rogue is considered to be in the same backhaul network as the detecting AP, and **In Net** displays in the **In Network** column for that rogue in the list of rogue APs.
Detect rogue access points based on their MAC OUI	Select the check box to enable detection of rogue APs based on MAC OUI.
Select MAC OUIs of wireless devices that are permitted in the WLAN	Create an allow list of wireless devices allowed on the WLAN, according to MAC OUI. To use an existing MAC OUI, select and choose an existing object, or to add a new one, select . Select **ADD**.

Table 98: Settings for WIPS policy (continued)

Setting	Description
Detect rogue access points based on hosted SSIDs and encryption type	Select the check box to enable detection of rogue APs based on hosted SSIDs and the encryption type. Select +, and then choose one of the following: For example, if you have a network security policy that requires all SSIDs to use Enterprise 802.1x, any valid SSID using Enterprise 802.1x makes the access point hosting it valid. An access point is categorized as a rogue if it hosts an SSID using WEP or no encryption at all. • **Select an SSID**—Select the SSID from the menu. • **Enter an SSID Name**—Type the SSID name. Select **Check the type of encryption used by this SSID**, and then select the type of encryption from the list. Otherwise, clear the check box. Select **ADD**.
Detect if wireless clients have formed an ad hoc network to identify rogue clients	Toggle **Detect if wireless clients have formed an ad hoc network to identify rogue clients ON** to enable the feature. Select **Enable rogue client reporting** and type the number of seconds, after which disconnected rogue APs drop from the reports.
Rogue Mitigation	
Mitigation Mode	Select one of the following: • **Manual**: Manually mitigate rogue APs and their clients. In manual mode, you must periodically check for rogue APs and their clients on the heat map pages in your network hierarchy. **Note:** Use caution when mitigating a suspected rogue AP. If your WLAN is within range of other neighboring wireless networks, the access point that might initially be considered a rogue AP, along with its clients, might be valid in another WLAN. • **Automatic**: APs automatically mitigate rogue APs and their clients, starting and stopping the mitigation process without any administrator involvement. **Note:** Use only the automatic mode for rogue APs that are in-network (in the backhaul network of your organization). Otherwise, automatic mitigation can impact the normal operation of valid APs belonging to a nearby business by blocking their wireless clients from connecting to their APs. Reference the appropriate FCC regulations that prohibit Wi-Fi blocking in these cases.

Table 98: Settings for WIPS policy (continued)

Setting	Description
Detect and Mitigate rogue clients every	After you enable rogue detection on an AP, it scans detected rogue APs for clients during the period that you specify. If you manually start mitigation against a rogue, the AP not only continues scanning for clients during this period, it also sends deauthentication frames to the rogue AP and to any detected clients during the same period. For example, if you leave this at the default setting of 1 second, the AP checks for rogues and attacks them every second. Each time an AP checks if there are clients associated with a detected rogue, it must switch channels for about 80 milliseconds (unless it happens to be using the same channel as the rogue). To minimize channel switching, choose an AP that is on the same channel as the rogue to perform the mitigation. The Rogue AP list shows which channel the rogue is using. If none of the APs are using the same channel, choose the one with the fewest clients. Finally, if all the APs are busy and on different channels from the rogue, consider reducing the amount of channel switching by increasing the period so that the associated client check occurs less frequently. You can change the duration from 1 to 600 seconds (10 minutes).
Repeat mitigation for detected rogue clients	Specify how many consecutive periods to spend attacking a rogue AP and its clients before allowing client inactivity to stop and commence a countdown to end the mitigation. If you use the default settings for both the length of the mitigation period and the consecutive number of periods, an attack lasts for 60 seconds before stopping because of client inactivity. The range is from 0 to 2,592,000 seconds (30 days). A value of 0 means that mitigatory APs send deauthentication frames for the entire amount of time that a mitigation effort is in effect.
Limit mitigation efforts per rogue AP to	The maximum length of time that an attack against a rogue AP can last. If the length of client inactivity does not cause the attack to be suspended or if you do not manually stop the attack, the AP stops it after this time limit elapses. The default duration is 14,400 seconds (4 hours), which means that an AP continues checking for clients of a detected rogue for up to four hours and mitigates them if it finds them. The mitigation might stop sooner if the period of client inactivity lasts long enough to stop it. You can change the maximum time limit between 0 and 2,592,000 seconds (30 days). In cases where the response time to detect a rogue AP would be greater than the default duration of four hours, consider increasing the duration to enable more time to locate the AP before ending the mitigation process. A value of 0 means that the client detection and mitigation continues indefinitely, unless the client inactivity period elapses.

Table 98: Settings for WIPS policy (continued)

Setting	Description
Stop mitigation if no client activity is detected in	Set the period of time to stop the mitigation process if the AP no longer detects that clients are associated with the rogue AP. During this time, the AP stops sending DoS attacks but continues checking if any clients form new associations with the targeted AP. If the AP detects any associated clients before this period elapses, it sends a deauthentication flood attack and resets the counter. If there are no more clients associated with the AP after this period, the AP stops the mitigation process even if there is still time remaining in the maximum time limit.
Max number of mitigator APs per rogue AP	(Applies only to automatic mode.) For automatic mitigation, hive members choose one AP to be the arbitrator, which is the one to which all the detector APs send reports. The arbitrator AP also determines which detector APs perform mitigation. When they start, they become mitigatory APs. Set the number of mitigatory APs that the arbitrator AP can automatically assign to attack a rogue AP and its clients. If you set the maximum as 0, all the detector APs can be assigned to perform rogue mitigation.

Related Links

Configure WIPS on page 298

Configure a Location Server

This task is part of the network policy configuration workflow. Use this task to enable and configure a location server as part of a network policy.

1. Go to **Configuration** > **Network**.
2. Select an existing network policy, and then select , or to add a new one, select ..
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. From the **Application Management** menu, select **Location Server**.
5. Toggle **Location Server** to **ON**, and configure the settings, or select and choose an existing location server.

Table 99: Location server settings

Setting	Description
Name	(Required) Type a **Name** for the location server.
Description	Type a **Description** for the location server. Although optional, descriptions can be helpful when you are troubleshooting your network.

Table 99: Location server settings (continued)

Setting	Description
Client Location Tracking	Toggle the setting **ON** to enable tracking. Enable this setting to track the location of currently associated client, rogue APs, and devices carrying RFID (radio frequency identification) tags.
Track Client Location Using	Choose one of the options: • Extreme Networks Location Server • AeroScout Location Server • Tazmen Sniffer Protocol (Ekahau, etc...)

Related Links

Configure the SSID for a Standard Wireless Network on page 165

Install CA Certificates

This task is part of the network policy configuration workflow. Use this task to install CA certificates as part of a network policy.

1. Go to **Configuration** > **Network**.
2. Select an existing network policy, and then select , or to add a new one, select .
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. From the **Application Management** menu, select **Certificates**.
5. Toggle **Install CA Certificates** to **ON**.
6. Select , and then choose a WIPS policy object from the menu.
   If the menu is empty, or does not contain the entry that you want, select to open the **Certificate Management** page.

Related Links

Configure the SSID for a Standard Wireless Network on page 165

Configure a Layer 2 IPsec VPN Service

Layer 2 IPsec VPN is a logical extension of the Layer 2 broadcast domain across an IPsec VPN tunnel. After configuration, it is available for use in multiple network policies.

Note
A Layer 2 VPN server on an AP can terminate a maximum of 128 tunnels. A Layer 2 VPN Gateway Virtual Appliance can terminate up to 1024 tunnels.

Because the NAT mechanism on the device involves both the source IP address and source port number, wireless clients can only send TCP or UDP traffic. Note that the clients will be unable to ping local servers because ICMP does not use port numbers.

When a wireless client associates with a device, the device applies a user profile to traffic from that client. If the device is a VPN client with a user profile tunnel policy, the device tunnels that traffic back to a VPN server at the primary site. The clients receive

network settings from a DHCP server at the primary site, query DNS servers at the primary site for domain name resolution, and access other network servers through the tunnel to any site in the VPN network.

Layer 2 IPsec VPNs tunnel traffic between APs functioning as VPN clients at remote sites and a VPN Gateway Virtual Appliance or Extreme Networks APs functioning as VPN servers at the corporate site, providing Layer 2 extensions of the main network. You can define at least one VPN server or two for redundancy. Each VPN client must belong to the same management network as the VPN server and build a GRE (Generic Routing Encapsulation) tunnel between the client and server. DHCP traffic is also tunneled, so clients receive IP addresses from the DHCP server at the corporate site just as if they were on the primary network.

This task is part of the network policy configuration workflow. Use this task to configure a new Layer 2 IPsec VPN service as part of a network policy.

1. Go to **Configuration** > **Network**.
2. Select an existing network policy, and then select , or to add a new one, select ..
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. From the **Network Services** menu, select **Layer2 IPsec VPN Services**.
5. Toggle **Layer 2 IPsec VPN Service** to **ON**.
6. To use an existing service, select and choose an existing object, or to add a new one, select .
7. Configure the Layer 2 VPN Services Settings on page 304.

Related Links

Layer 2 VPN Services Settings on page 304
Configure the SSID for a Standard Wireless Network on page 165

Layer 2 VPN Services Settings

Table 100: Settings for Layer 2 VPN services

Setting	Description
Name	Type a name for the service.
Description	(Optional) Type a description. Although optional, descriptions can be helpful when you are troubleshooting your network.
Device VPN Server and Device VPN Client Settings	
Single Device VPN Server	Select **Single Device VPN Server** if you are not implementing redundant VPN servers.
Redundant Device VPN Servers	Select **Redundant Device VPN Servers** to configure a redundant VPN server. Configure the settings for **Device VPN Server 1** and **Device VPN Server 2**.
Device VPN Server	Select an AP with Layer 2 IPsec VPN services enabled.

Table 100: Settings for Layer 2 VPN services (continued)

Setting	Description
Server Public IP Address	Auto-populated based on the selected VPN server settings. To change this setting, type the IP address of a VPN server that VPN clients can reach across the network. Note: If the VPN server is behind a NAT device, enter the address of the MIP address on the NAT device. If there is no NAT device in front of the VPN server, enter the mgt0 IP address of the server.
Server MGT0 IP Address	Auto-populated and read-only.
Server MGT0 Default Gateway	Auto-populated and read-only.
Client Tunnel IP Address Pool Start	Type the first IP address of the range of addresses that the VPN server assigns to tunnel interfaces on VPN clients during the Xauth phase of tunnel setup. As a best practice, put this address pool in the same subnet as the VPN server mgt0 interface, and the same subnet as the addresses that the DHCP server assigns to wireless clients through the tunnel. If the tunnel interfaces are in a different subnet, you must define a route the VPN server default gateway router uses to forward traffic destined for the tunnel interface, and traffic destined for the wireless clients to the VPN server mgt0 interface.
Client Tunnel IP Address Pool End	Type the IP address at the end of the range of IP addresses in the address pool.
Client Tunnel IP Address Pool Netmask	Type the netmask that defines the subnet to which the tunnel interfaces belong.
Device VPN Client DNS Server	Select the DNS server IP address or host name object that VPN clients use to resolve domain names, or select ✚ to define a new one.
User Profiles for Traffic Management ExtremeCloud IQ displays a list of available user profiles, for which traffic can be forwarded through the Layer 2 IPsec VPN tunnel or forwarded without tunneling.	
VPN Tunnel Mode	In the **VPN Tunnel Mode** column, select **Enable** to enable VPN clients to tunnel traffic for specific user profiles.
Tunnel All Traffic	To tunnel all client traffic, select **Tunnel All Traffic**.
Split Tunnel	To enable split mode tunneling, select **Split Tunnel**.

Related Links

Configure a Layer 2 IPsec VPN Service on page 303

NEW!

Configuration | User Management

Note
The topics in this chapter apply to ExtremeCloud IQ user management.

Create user groups for a selected network policy or all network policies. Add users and assign them to existing user groups, or add users when you create a user group. User groups define password settings such as, type, complexity, database location, and expiration settings.

Note
For existing user groups, settings related to passwords are unavailable for editing. To modify these settings, you must create a new user group.

Assign a user group to a specific SSID to control access and network policy for users. Associate a user group with a user profile to define network access parameters, including VLAN assignment, firewall policies, QoS, and traffic tunneling.

Related Links

Add a User Profile on page 174

Add a User

Note
You must first create the user group to which you want to assign the user. You cannot edit the user group for an existing user.

Use this task to add a new user and assign an existing user group.

1. Go to **Configuration** > **Network**.
2. On the **Network Configuration / Network Policies** page, select , and then go to **User Management** > **Users**.
3. Select and then configure the user settings.
4. Select **SAVE**.

Related Links

User Settings on page 307

User Settings

Table 101: Settings for new user accounts

Setting	Description
Create account in user group	(Required) Select a user group from the menu.
Name	Type the name of the user. This name appears in messages sent to the email address in the **Deliver Password** section. The email message, which contains login credentials and wireless connection instructions, begins with **`Welcome <this_name>`**. **Note:** Required only if you select **Name** from the **User Name** menu.
Organization	Type the name of the organization for the user. For permanent users, leave this field empty.
Purpose of Visit	Type the purpose of the user's visit. For permanent users, leave this field empty.
Email Address	Type the user's email address. **Note:** Required only if you select **Name** from the **User Name** menu.
Phone Number	Type the user's phone number, and use the menu to set the international dialing code. **Note:** Required only if you select **Phone Number** from the **User Name** menu.

Table 101: Settings for new user accounts (continued)

Setting	Description
User Name	From the menu, select a field to use as the **User Name**. Choose from the following options: • **Name** • **Email Address** • **Phone Number** • **Other** If you select **Other**, type a user name for the account. Example: jsmith
Password	(Required) Type a password, or select **Generate** to automatically generate a password for the user. To see the password, select **Show Password**. **Note:** For either method, the password must conform to the password rules configured for the associated user group.
Description	(Optional) Type a description for the user account.
Deliver Password	Select a password delivery method: • **Email Address** Type the email address for the user in the corresponding field. The auto-populates if you already entered an email address. This option is available only if you previously selected **Email** in the **Delivery Settings** section of the user group configuration. • **Text Message** Type the cell phone number for the user in the corresponding field. This option is available only if you previously selected **Text Messages (SMS)** in the **Delivery Settings** section of the user group configuration.

Related Links

Add a User on page 306

Bulk Create Users

You must first create the user group to which you want to assign the users.

Use this task to bulk-create and add users to an existing user group.

1. Go to **Configuration** > **Network**.
2. On the **Network Configuration / Network Policies** page, select , and then go to **User Management** > **Users**.

3. Select **Bulk Create** and configure the settings.

   See Bulk Create Settings on page 309.
4. Select **SAVE**.

Related Links

Bulk Create Settings on page 309
Add a User Group on page 309

Bulk Create Settings

Table 102: Settings for the bulk creation of users

Setting	Description
Create account in user group	Select a user group from the menu.
Username Prefix	Type a prefix for the user names. Bulk-created user names include this prefix for each user name, starting with 1. For instance, if the user name prefix is 1250, the first bulk-created user is 12501, the second user is 12502, and so on.
Number of Accounts	Type the number of users to add. Range: 1–1000
Email User Account info to	Type the email address to which you want ExtremeCloud IQ (New) to send the user credentials.

Related Links

Bulk Create Users on page 308
Bulk Add Users to a User Group on page 310

Add a User Group

ExtremeCloud IQ (New) supports user groups for Private Pre-Shared Key (PPSK) users and RADIUS users. Administrators and NetSecOps can configure ExtremeCloud IQ (New) user groups with limited access privileges for VIPs and non-employees such as guests, visitors, and contractors who request network access.

Create user groups before you add users. You can add new users to existing user groups, or add new users when you create user groups.

Use this task to create a user group.

1. Go to **Configuration** > **Network**.
2. On the **Network Configuration / Network Policies** page, select , and then go to **User Management** > **User Groups**.
3. Select , and then configure the settings.

   For a cloud-based user group, see Cloud User Group Settings on page 169.

   For a local user group, see Local User Group Settings on page 171.
4. Select **SAVE**.

Related Links

Cloud User Group Settings on page 169
Local User Group Settings on page 171

Add a User to a User Group

You must first create the associated user group.

Use this task to add a single user by editing an existing user group.

1. Go to **Configuration** > **Network**.
2. On the **Network Configuration / Network Policies** page, select , and then go to **User Management** > **User Groups**.
3. Select an existing user group, and then select , or to add a new one, select ..
4. Expand the **Add Users** section.
5. Select and then configure the settings.
   See User Settings on page 307.
6. Select **DONE**.

Related Links

User Settings on page 307

Bulk Add Users to a User Group

You must first create the user group to which you want to assign the users.

Use this task to bulk-add users to an existing user group, or while creating a new user group.

1. Go to **Configuration** > **Network**.
2. On the **Network Configuration / Network Policies** page, select , and then go to **User Management** > **User Groups**.
3. Expand the **Add Users** section.
4. Select **Bulk Create** and configure the settings.
   See Bulk Create Settings on page 309.

   ExtremeCloud IQ (New) saves your changes, creates the requested user accounts, and emails the bulk-created login credentials to the email addresses in the CSV file. The CSV file contains the SSID, user ID, user name, user group, access key, and expiration date for each bulk-created user.
5. Select **DONE**.

Related Links

Bulk Create Settings on page 309

Configure a Private Client Group

Create a Private Pre-shared Key (PPSK) standard wireless network. Enable **Private Client Group Options** and configure the settings. See Configure Private Pre-Shared Key SSID Authentication on page 188.

After you enable Private Client Groups (PCGs), you can designate them as using one of two main operating modes:

- **AP-based** PCG uses unique user and shared keys. This mode supports common shared devices within personal network spaces. It also requires room assignments for AP anchoring and traffic tunneling.
- **Key-based** PCG requires one password used by the entire device group. Key-based PCG does not need room assignments, and no traffic tunneling is used on anchor-based APs.

Note
Each network policy can have only one AP-based PCG wireless network (SSID), one key-based PCG SSID, and any number of non-PCG SSIDs.

Use this task to configure a private client group for a PPSK standard wireless network.

1. Go to **Configuration** > **Network**.
2. On the **Network Configuration / Network Policies** page, select , and then go to **User Management** > **Private Client Groups**.
3. Select a **Network Policy** from the menu.
4. Select **AP-Based Groups** or **Key-Based Groups** and configure the settings.
   a. Toggle the corresponding setting **ON** to enable the feature.
      - **Enable AP-Based Groups**
      - **Enable Key-Based Groups**
   b. (Optional) For AP-based groups, select **Distribute Shared Keys**.
5. Select to add rooms for AP-based groups, or users for key-based groups.
6. Type a name for an AP-based group and then select users from the menus, or for key-based groups select a user from the menu.

   Alternatively, for key-based groups, you can bulk add users by selecting **IMPORT** and uploading a CSV file.
7. Repeat steps 5–6 until you finish adding groups or users.
8. Select **SAVE CHANGES**.

Related Links

Configure Private Pre-Shared Key SSID Authentication on page 188

Unlock Users

ExtremeCloud IQ (New) authenticates PPSK clients against a large list of passwords. Users that repeatedly submit incorrect, deleted, or expired passwords can trigger a DoS attack. To prevent this, ExtremeCloud IQ temporarily puts the MAC address of a client device that repeatedly fails authentication 10 times in 7 minutes (default settings) into a sandbox and blocks future attempts for 30 minutes. For all authentication attempts, ExtremeCloud IQ first checks the client MAC address against the list of locked users in the sandbox.

Use this procedure to unlock users.

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

2. On the **Network Configuration / Network Policies** page, select , and then go to **User Management** > **Locked Users**.
3. Select entries in the locked users list.
4. Select **Unlock**.

Perform a RADIUS Test

The RADIUS Test tool tests network connectivity between a device acting as a RADIUS authenticator (RADIUS client) and RADIUS authentication server, which can be an Extreme Networks RADIUS server, or an external RADIUS authentication or accounting server.

Use this task to test the connectivity between a RADIUS authenticator and a RADIUS server.

1. Go to **Configuration** > **Network**.
2. On the **Network Configuration / Network Policies** page, select , and then go to **User Management** > **RADIUS Test**.
3. Select the type of RADIUS server that you want to test.
   - To test connectivity to an Extreme Networks RADIUS server, choose **Select a Server (local RADIUS)**, and then select a RADIUS server from the drop-down list.
   - To test connectivity to an external RADIUS authentication or accounting server, select **Enter a Server (external RADIUS)**, and enter the IP address of the server in the field.
4. Select a managed device that is acting as a RADIUS authenticator (client) from the drop-down list.

   This is the device from which the **RADIUS Access-Request** or **Accounting-Request** message is sent.
5. Select either **RADIUS Authentication Server** or **RADIUS Accounting Server**.

   If you select an authentication server, you must also enter supplicant credentials (a user name or barcode, and a password or PIN) for a valid user account on the RADIUS authentication server. You can also enter a user name and password that do not match an account on the RADIUS server.
6. Select **Test**.

ExtremeCloud IQ (New) displays the results on the page, under **Test Result**. The following example shows a successful test result.

```
RADIUS server is reachable. Get attributes from RADIUS server: User-Group-ID:0=13; VLAN-ID:1=1; Session-Timeout=1800
```

Unbind a Device

Use this task to unbind a locally-based PPSK from a client device to free up that key or device. You can unbind the client MAC address, the PPSK, or both.

1. Go to **Configuration** > **Network**.
2. On the **Network Configuration / Network Policies** page, select , and then go to **Configure** > **User Management** > **Unbind Device**.

3. Select the method for unbinding from the drop-down list.
   Choose **MAC address**, **PPSK**, or **MAC address and PPSK**.
4. Enter the MAC address, the PPSK, or both.
5. Select **Unbind**.

Subscriptions & Services

Managing your network devices and network topologies with ExtremeCloud IQ (New) is accomplished with applications. Licenses are required for the specialized applications that manage devices and network topologies, such as buildings and sites.

A *subscription* has a start and end date and gives you access to ExtremeCloud IQ (New) application products. A subscription entitles you to an explicit allotment of Extreme Networks licenses for one or more applications to manage the devices, buildings, and outdoor sites in your network. Trial license periods are available to help you decide whether an application addresses your needs, within specific parameters. Such parameters might include dual subscriptions, but trial licenses are granted depending on your license and your eligibility.

It is important to understand the relationship between, subscriptions, and licenses in ExtremeCloud IQ (New):

Contract

A contract is all-encompassing and can include multiple subscriptions and licenses.

Subscription

A subscription defines an explicit number of software-application licenses that enable robust features for managing and viewing devices.

- Licenses associated with the subscription are assigned to devices.
- Some features may require an entire building, outdoor site, or fabric to be covered by Platform ONE licenses only.

License

Licenses are defined and numbered according to subscription terms. Individual licenses are consumed when you allocate them to devices within buildings or outdoor sites. Licenses unlock features specific to the application under license.

Subscriptions Terminology

The following table describes terms commonly used throughout this document and in ExtremeCloud IQ (New).

Table 103: Terminology

Term	Description
Activate	To use a license. When you manually assign a license to a device, or when the system automatically assigns an available license.
License	A license applies to a single device. Licenses are defined and numbered according to subscription terms. For example, you might have four subscriptions (bought at different times) that total 5000 licenses. Allocate licenses to devices to unlock features specific to the application under license. Unlicensed devices are inventory-only.
Purchase	Buy the product or service. For more information about purchasing products or services, contact an official Extreme Networks Partner.
Renew	Extend an existing contract.
Revoke	Return an activated license to the pool of available licenses.
Subscription	Includes a start and end date and provides access to ExtremeCloud IQ (New) application products. A subscription entitles you to an explicit number of Extreme Networks licenses.

Subscriptions & Licensing User Interface Descriptions

Figure 7 shows the elements and features available in the Subscriptions interface. See Table 104 for descriptions of the numbered elements.

Figure 7: Subscriptions & Licensing interface, unfiltered

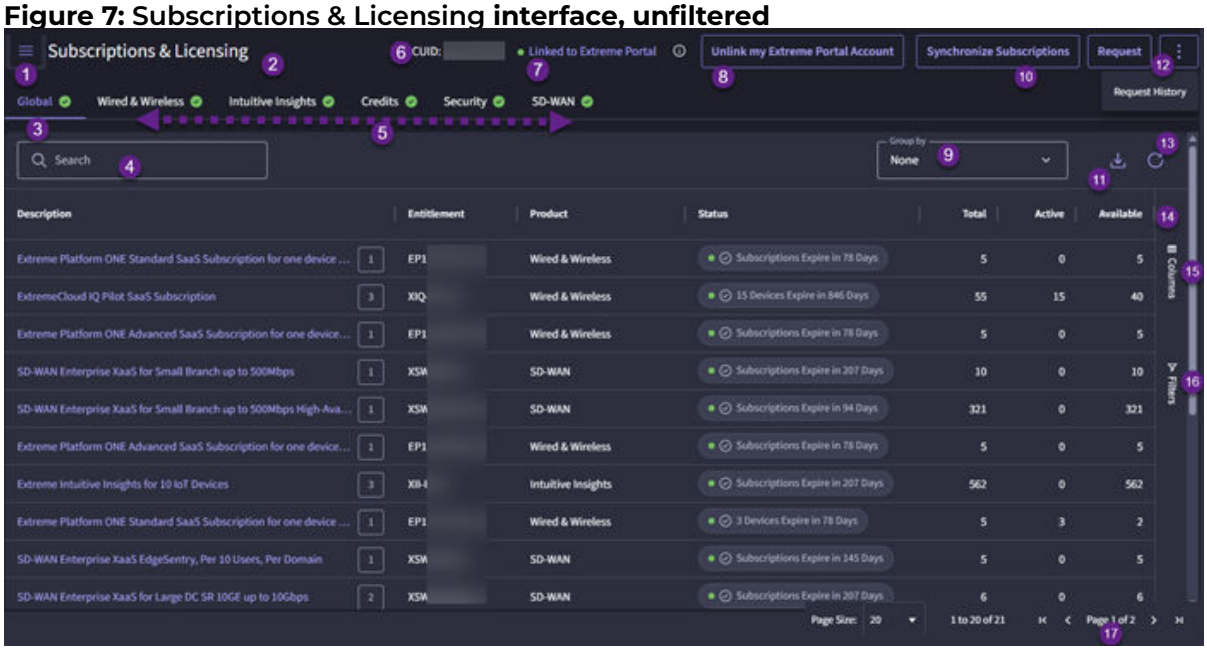


Table 104: Subscriptions & Licensing interface descriptions

Callout	Interface Area	Description
1	Navigation menu	Expand or collapse the ExtremeCloud IQ (New) Navigation menu to provide access to all features of the interface or hide the navigation menu to view more data (image view is collapsed).
2	Page title	Name of your page location within **Subscriptions & Services**
3	Global tab	Display all license pools for all applications when unfiltered
4	Search field	Search all columns in the current data set (not case-sensitive) to filter for specific records, such as License Descriptions, License Type, or Status.
5	Subscriptions & licensing application tabs	Display subscription and licensing detail for each licensed application. The license pool status is indicated by the color dot on the tab, and line-item status is indicated by the same color scheme.
6	CUID	The unique ID associated with the license pool. The CUID is very important when communicating with support personnel.

Table 104: Subscriptions & Licensing interface descriptions (continued)

Callout	Interface Area	Description
7	Extreme Portal Link status	Indicates whether ExtremeCloud IQ (New) is linked to your Portal account. The account must be linked to see content of the license pool
8	Link / Unlink	Toggle the link status between ExtremeCloud IQ (New) and your Extreme Portal account. **Caution:** Use **Unlink** only for troubleshooting when directed by Support personnel.
9	'Group by' filter	Filter by None or Product
10	Synchronize Subscriptions	Synchronize all your Extreme Platform ONE Networking subscriptions
11	Download button	Download table data
12	3-dot menu	Displays action options: • Request History • Request button initiates the License Request process.
13	Refresh button	Refresh data for a current snapshot of table data
14	License counts groups	Shows total licenses, number active, and number still available columns for that license pool; numbers fluctuate as licenses are applied or removed from a device or devices. • **Total** = sum of all licenses available to use today = sum all of the same license type with start date in the past and end date in the future = exclude expired and not yet valid • **Active** = sum of all licenses the customer is using today • **Available** = Total minus Active
15	Columns option	Customize the columns that you see on the page.
16	Filter	Filter the table by Entitlement (license), Application, or Status.
17	Pagination tools	Customize the number of results to show on one page.

Subscriptions and Account Linking

You can use Extreme Platform ONE Networking subscriptions for the following products:

- Extreme Platform ONE Networking
- ExtremeCloud IQ (New)

- ExtremeCloud IQ (Classic)
- ExtremeCloud IQ Controller
- ExtremeCloud Site Engine

To activate the Extreme Platform ONE Networking licenses that you purchased, you must link your Extreme Portal account. For detailed instructions, see the user guide for the specific application.

For Extreme Platform ONE Networking, see Link Your Extreme Portal Account to ExtremeCloud IQ (New) on page 318.

Note
You can link your Extreme Portal account either in Extreme Platform ONE Networking or ExtremeCloud IQ. If either is already linked, new licenses are automatically available for both applications.

Related Links

Link Your Extreme Portal Account to ExtremeCloud IQ (New) on page 318

Link Your Extreme Portal Account to ExtremeCloud IQ (New)

When you log in to ExtremeCloud IQ (New), select **Link the Portal Account** at the prompt, type your Extreme Portal credentials, and then select **Link Extreme Portal Account**.

Use this task to link your ExtremeCloud IQ (New) to the Extreme Portal from the **Subscriptions & Licensing** page.

1. Go to **Subscriptions & Services** > **Subscriptions & Licensing**.
2. Select the **Global** tab.
3. Select **Link Extreme Portal Account** and type your Extreme Portal credentials.

Note
If you are a partner or a distributor and are setting up an Extreme Portal account for a customer, type your Extreme Portal credentials when you link the customer account and the Customer Unique Identifier (CUID). The CUID is included in the customer Welcome Letter.

Synchronize Subscriptions

Subscription synchronization is automated and scheduled by the system, but you can initiate on-demand synchronization.

Use this task if you do not see your new subscriptions and licenses in ExtremeCloud IQ (New). You can synchronize subscriptions only once every 5 minutes.

Important
Do not use **Synchronize Subscription** just to refresh the information in ExtremeCloud IQ (New).

1. Go to **Subscriptions and Services** > **Subscriptions & Licensing**.
2. Select **Synchronize Subscriptions**.

   A 5-minute timer begins. After the timer expires, you can synchronize your subscriptions again, if required.

Examples of Subscriptions & Licensing Detail

Information about licenses and license pools is immediately visible in the **Subscriptions & Licensing** interface, as shown in the following figures. Detail includes license or entitlement, product name, number of days until the license expires, status, and license total, active, and available licenses. Status for each subscription license is indicated by color:

- Green: no problems
- Amber: attention needed, for example:
  - One or more licenses expire in fewer than 60 days and the renewal is not yet in progress
  - Trial is in progress
- Red: immediate attention required, indicating but not limited to the following conditions:
  - The grace period is active
  - One or more licenses expire in fewer than 30 days and the renewal is not yet in progress

Figure 8: Status color indicators

The following figure shows detail about an early warning (amber) for upcoming license expiration.

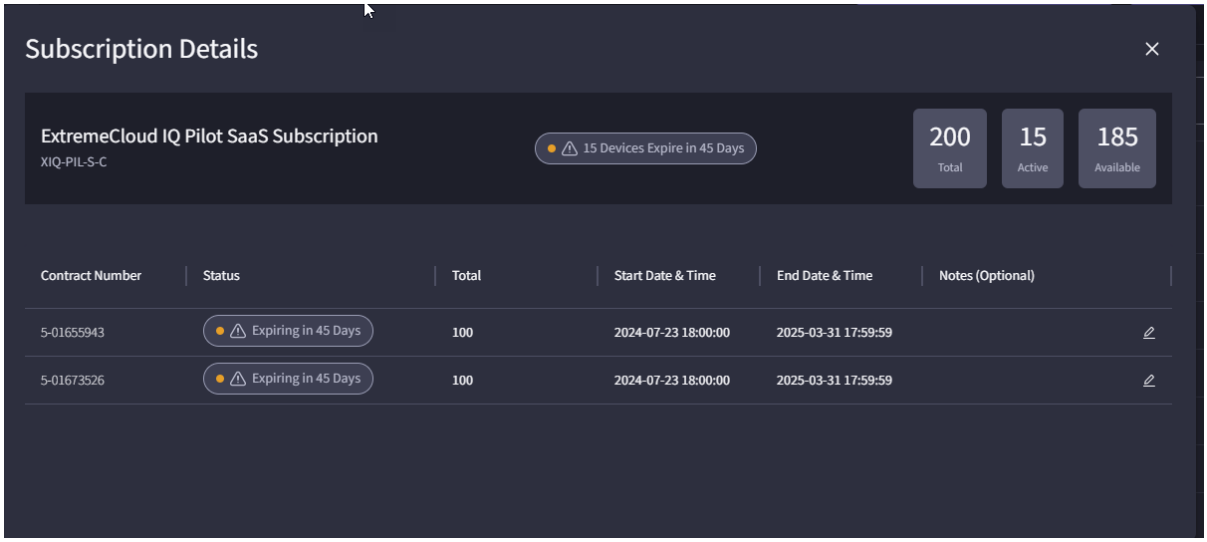


Figure 9: Subscription detail, soon-to-expire status

In the next figure, the urgent status-symbol color (red) indicates an expired legacy entitlement or very soon-to-expire licenses. You can view details for each subscription.

In a similar figure, detail for an soon-to-expire or expired legacy entitlement is visible, indicated by the urgent status-indicator color (red). You can view details for each subscription.

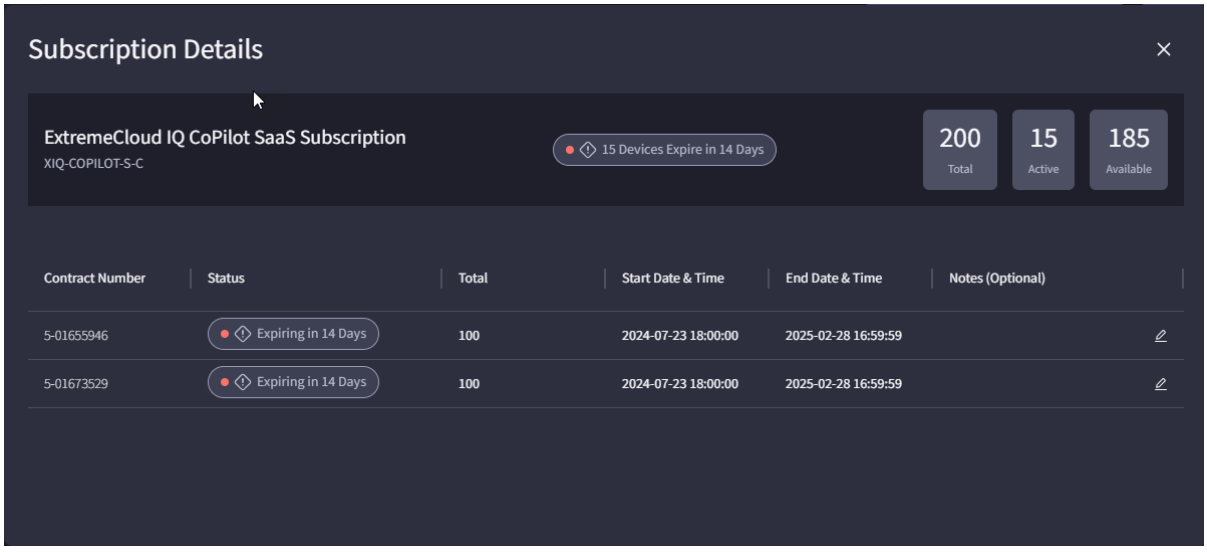


Figure 10: Subscription detail, expired or imminent expiring status

General License Management

You can manage various aspects of licenses in the **Subscriptions & Licensing** interface, including but not limited to requesting more licenses for devices and NAC allocations.

Note
License counts for a pool fluctuate when license usage changes for a product, when a contract or a subscription expires, or when a new subscription order is processed.

View License Pool

A *license pool* is a set of licenses that are available to you. Licenses can have different start dates, end dates, and quantities. You can activate (assign) licenses in the pool when needed and return licenses to the Available pool when you remove them and they are not currently assigned (Active). You can view license expiration status; license type, term start and end date; and the number of licenses total, active, and available. The license counts from the applications appear on the **Subscriptions** page and in the subscription details when you select an individual subscription.

Note
When a license violation state is detected, devices are unmanaged automatically, the **Device License** type value changes to **Not Licensed**, and the lock is released

1. Go to **Subscriptions & Services** and select the desired application tab on the **Subscriptions & Licensing** page.

   All licenses in the pool are available for you to view and page through, if you select the **Global** tab.
2. (Optional) Use the search, group, and filter options to refine the result set and view for a specific license pool or for multiple pools.

   You can view details in the columns.
3. For more information, you can select a line item and view details about the selected subscription or license.

Related Links

Pagination on page 26

Search, Group, and Filter

You can search for an item and organize lists in the **Subscriptions & Licensing** user interface.

You can group records based on the pre-defined criteria that vary for different windows.

Use the **Previous** (**<**) and **Next** (**>**) icons to scroll through the results lists.

Note
Search terms are not case-sensitive.

1. To search for records, start typing a search attribute such as product, license or license type, status, or a complete or phrase or words from a description in the **Search** field.

   To clear the search, select **X** in the **Search** field.
2. To group records in a page, select **Group By** and choose an option.

   The list is organized by the grouping option you selected. Some headings are collapsible, based on the chose option.
3. To filter records in a page, select **Filter** ( ) and choose the filter attribute.

   To clear an individual filter, click **X** for the appropriate filter. To clear all the filters, select **Clear All Filters**.

   The list is organized by the filtering attribute you selected.

Manage NAC Allocations

You can allocate NAC licenses to devices across a license pool according to your needs.

Note
ExtremeCloud Site Engine must be onboarded before you can manage NAC allocations.

1. Go to **Subscriptions & Licensing** and select **Global**.

   You can use the search, group, and filter functionality to find the subscription.

   Note
   The menu selection in this procedure does not appear unless you have one or more NAC subscriptions.

2. At the top right corner of the page, select , and then select **Manage NAC Allocations**.
3. In the **NAC Entitlements Allocation** window, specify the allocation percentage of the license pool to assign to which entity.
4. Select **Save Allocations**.

Activate a License

The following actions activate a license.

- Add a device as managed.

- Enable a licensed application. You may need to apply the license for some licenses (for example, MacSec).

  Note
  Use of some AI Expert agents activates AI Credits.

The following actions revoke a license.

- Unmanage or delete a device.
- Disable a licensed feature. You may need to revoke the license manually for some licenses (for example, MacSec) before you delete the device.

  Note
  Activated AI Credits are automatically revoked monthly.

Pre-provisioning and License Assignment

ExtremeCloud IQ (New) does not assign a license to a device until the device connects to the cloud for the first time. Therefore, you can pre-provision new devices before decommissioning the old ones, even if you do not have enough licenses to cover all the devices. The following example explains how the process works.

Example

AP-A represents the old devices, and AP-B represents the new devices.

AP-A is operational, the **State** is **Managed**, and the device uses a license.

AP-B is not connected to the Internet.

1. Add the serial number for AP-B to ExtremeCloud IQ (New).
2. Assign policy and configure AP-B.

   AP-B does not use a license, and the **State** is **New**.
3. In ExtremeCloud IQ (New), **Unmanage** AP-A.

   AP-A is operational and provides service. Because the State is **Unmanaged**, ExtremeCloud IQ (New) reports the device as **Disconnected**. The system does not collect statistics for the device, and you cannot change the configuration.

   AP-A no longer uses a license.
4. Connect AP-B to the Internet.

   The AP-B **State** changes from **New** to **Managed**, and AP-B uses a license.

Renew a Subscription

Your Extreme Networks partner sends you a renewal quote. You can respond to that quote by renewing a subscription.

Note
Subscription renewal and license renewal are independent actions. Many licenses can be associated with one subscription, but renewing a license isn't linked to renewing the associated subscription.

Use this task to renew a subscription.

1. Send a completed purchase order to your Extreme Networks partner.
2. When the purchase order is processed, subscriptions are added to the license pool for your CUID.

Related Links

Synchronize Subscriptions on page 318

Request a Free Trial

Use the following task to request a free trial from the ExtremeCloud IQ (New) user interface.

1. Go to **Subscriptions & Services** > **Subscriptions & Licensing**, and do one of the following:
   - For , select the **Wired & Wireless** tab, and then select **Extreme Platform ONE Trial** > **Start Trial**.
   - For , select the **Security** tab, and then select **Start Trial**.

   Alternatively, the 9-dot menu in ExtremeCloud IQ (Classic) displays applicable products in the **Available For Trial** section. Select a product link to request the free trial, and go to Step 2.
2. Read the **Terms and Conditions** and **Privacy Policy**, and select the check boxes to continue.

   Signing up for product updates is not required to continue.
3. Select **Accept and Continue**.
4. For **Select Request**, select **Subscriptions**, and then select **Next**.
5. Select the application that you want to trial, and select **Add**.
6. After you finish adding applications to the cart, select **Next**.
7. Type your phone number and optional information, and then select **Next**.
8. Review your request, and then select **Next** to download the request document.
9. Submit the request document to your Extreme Networks partner or contact Sales to submit the request.

Contact Sales

Contact Extreme Networks Sales for information about contracts, subscriptions, and licenses, and for other needs you might have.

1. Go to **Subscriptions & Services** > **Contracts** and select **Contact Sales**.

   The Contact the Extreme Sales Team web page opens.
2. Complete and submit the form.

   Alternatively, see **Other Ways to Get in Touch**, and select another contact option.

   A sales representative will contact you.

Administration & Settings

Access Management

Access Management enables administrators to add users, configure single sign-on for users, or integrate role-based access (RBAC) groups that you configure in an identity provider (IdP). You can:

- Create new users. Add new internal or external user accounts and assign roles to manage their access.
- Implement and assign role-based groups and assign them to sites.
- Allow users to log in with Single Sign-On (SSO) using credentials from an existing SAML-enabled identity provider (IdP).

Role-Mapping Between Extreme Platform ONE Networking and Other Applications

Table 105 and Table 106 on page 327 show the mapping between Extreme Platform ONE Networking roles to those in other applications.

Table 105: Role-Mapping Between Extreme Platform ONE Networking and Other Applications

Extreme Platform ONE Networking	ExtremeCloud IQ (Classic)	ExtremeCloud IQ (New)	Extreme Intuitive Insights
Administrator	Administrator	Administrator	Administrator
NetSecOps	Operator	NetSecOps	NA

Table 105: Role-Mapping Between Extreme Platform ONE Networking and Other Applications (continued)

Extreme Platform ONE Networking	ExtremeCloud IQ (Classic)	ExtremeCloud IQ (New)	Extreme Intuitive Insights
BizOps	Observer	Observer	NA
Observer	Monitor Help Desk Guest Management Application Operator Installer	Observer	NA

Note
The following roles work better in ExtremeCloud IQ (Classic), and do not provide the same experience in ExtremeCloud IQ (New):

- Monitor
- Help Desk
- Guest Management
- Application Operator
- Installer

Table 106: Role-Mapping Between Extreme Platform ONE Networking and Other Applications

Extreme Platform ONE Networking	ExtremeCloud SD-WAN	Extreme Platform ONE Security
Administrator	Administrator	Administrator
NetSecOps	Operator	NetSecOps
BizOps	NA	NA
Observer	Observer	Observer

Note
Extreme Platform ONE Security, was formerly known as Universal ZTNA.

Role-Based Feature Access | Extreme Platform ONE Networking

Table 107: Role-based feature access

Feature	Administrator	NetSecOps	Observer	BizOps
Workspace (Extreme Platform ONE Networking only)	R/W	R/W	Read-only	Read-only
Monitoring				
Dashboard	R/W	R/W	Read-only	Read-only
Visualize	R/W	R/W	Read-only	No access
Alerts	R/W	R/W	Read-only	No access
Network Devices	R/W	R/W	Read-only	No access
Clients	R/W	R/W	Read-only	No access
Configuration				
Sites	R/W	R/W	No access	No access
Network	R/W	R/W	No access	No access
Subscriptions & Services				
Inventory (Extreme Platform ONE Networking only)	R/W	R/W	No access	Read-only
Subscriptions & Licensing	R/W	Read-only	No access	Read-only
Contracts	R/W	Read-only	No access	No access
Administration & Settings				
Access Management	R/W	No access	No access	No access
Alert Policies	R/W	R/W	No access	No access
External Notifications	R/W	R/W	No access	No access
Backup & Restore	R/W	R/W	No access	No access
Integrations	R/W	No access	No access	No access
Logs	R/W	R/W	No access	No access
Extreme AI (Extreme Platform ONE Networking only)				
AI Expert	R/W	R/W	Read-only	Read-only
AI Canvas	R/W	R/W	Read-only	Read-only

Read-only access provides a "view-only" experience without the full functionality reserved for roles with read-write (R/W) access. With read-only access you can customize your view:

- Select the data range and pagination.
- Select which table columns to show.
- Filter and refresh tables.

For most table views, you can export the data to a .CSV file, but you cannot perform actions that require R/W access, such as:

- Download an inventory or configuration template.
- Link or unlink a license account.
- Renew subscriptions.

Users & Roles

You can add multiple users and roles of the following types to ExtremeCloud IQ (New).

- Internal users
- External users

You can also implement single-sign-on via SAML-based identity providers.

Note
Roles for all applications can be assigned only in Extreme Platform ONE Networking. You cannot create or assign roles or custom roles that were previously assigned in individual applications.

Related Links

Role-Mapping Between Extreme Platform ONE Networking and Other Applications on page 326
Role-Based Access on page 329

Role-Based Access

Note
ExtremeCloud IQ (New) user roles cannot be configured in ExtremeCloud IQ (Classic).

Use the following descriptions to determine role assignments.

Administrator

Best for users who need the following:

- Full system-configuration access
- User and access-management capabilities

- Integration and backup management
- Complete administrative control
    - Alerts
    - Licenses
    - Inventory Status
    - Site Health

NetSecOps

Ideal for users who need the following:

- Network device management
- Security policy configuration
- Monitoring and alerting capabilities
- Operational control without user management
    - Alerts (can manage alert policies and acknowledge permissions)
        - Severity
        - Category
        - Top 3 Alerts
        - Application
    - Licenses
    - Inventory Status
    - Site Health

Observer

Appropriate for users who need the following:

- Read-only access to monitoring data
- Dashboard and visualization viewing
- No configuration or administrative access
    - Alerts (no alert policies, no acknowledge permissions)
        - Severity
        - Category
        - Top 3 Alerts
        - Application
    - Site Health

BizOps

Designed for users who need the following:

- Business-focused access to inventory and contracts
- AI Canvas and Agent access for business insights
- Limited operational visibility

Subscription and licensing management

- Licenses
- Inventory Status
- Site Health

Related Links

Security-Specific Roles and Features | Extreme Platform ONE Networking on page 331

Role-Based Feature Access | Extreme Platform ONE Networking on page 328

Security-Specific Roles and Features | Extreme Platform ONE Networking

Extreme Platform ONE Networking security includes the following additional capabilities not available in networking-only deployments.

- Onboarding: Administrator and NetSecOps roles have full access. Observer and BizOps roles have no access.
- Troubleshooting: Administrator and NetSecOps roles have full access. Observer and BizOps roles have no access.
- Policy Management: Includes Security Policies, Users & Devices, Conditions, Network Services, and Applications
- Security Services: Administrator role has full access. NetSecOps role has read access only.

Role-Based Feature Access | Extreme Platform ONE Networking

Table 108: Role-based feature access

Feature	Administrator	NetSecOps	Observer	BizOps
Workspace (Extreme Platform ONE Networking only)	R/W	R/W	Read-only	Read-only
Monitoring				
Dashboard	R/W	R/W	Read-only	Read-only
Visualize	R/W	R/W	Read-only	No access
Alerts	R/W	R/W	Read-only	No access
Network Devices	R/W	R/W	Read-only	No access
Clients	R/W	R/W	Read-only	No access
Configuration				
Sites	R/W	R/W	No access	No access
Network	R/W	R/W	No access	No access
Subscriptions & Services				

Table 108: Role-based feature access (continued)

Feature	Administrator	NetSecOps	Observer	BizOps
Inventory (Extreme Platform ONE Networking only)	R/W	R/W	No access	Read-only
Subscriptions & Licensing	R/W	Read-only	No access	Read-only
Contracts	R/W	Read-only	No access	No access
Administration & Settings				
Access Management	R/W	No access	No access	No access
Alert Policies	R/W	R/W	No access	No access
External Notifications	R/W	R/W	No access	No access
Backup & Restore	R/W	R/W	No access	No access
Integrations	R/W	No access	No access	No access
Logs	R/W	R/W	No access	No access
Extreme AI (Extreme Platform ONE Networking only)				
AI Expert	R/W	R/W	Read-only	Read-only
AI Canvas	R/W	R/W	Read-only	Read-only

Read-only access provides a "view-only" experience without the full functionality reserved for roles with read-write (R/W) access. With read-only access you can customize your view:

- Select the data range and pagination.
- Select which table columns to show.
- Filter and refresh tables.

For most table views, you can export the data to a .CSV file, but you cannot perform actions that require R/W access, such as:

- Download an inventory or configuration template.
- Link or unlink a license account.
- Renew subscriptions.

Create a New User

User access is controlled by the roles you assign. Use this task to add a new internal or external user account and assign roles to manage their site access.

Note
After you create a user account, the new user receives an email prompt to create a password and log in to Extreme Platform ONE Networking. Until the user logs in, their user status remains **Inactive**. When you edit a user account, you can resend the email.

1. Go to **Administration & Settings** > **Access Management**.
2. In the **Users & Roles** area, select one of the following account-types:
   - **Internal Users**: Select this tab to grant access to users within your organization.
   - **External Users**: Select this tab to grant access to users outside of your organization; for example, resellers, distributors, technical support, and sales.

     Caution
     Depending on the role assigned to an External User, that user may have full access or restricted access to all features and assets in Extreme Platform ONE Networking or ExtremeCloud IQ (New). Be cautious and evaluate role-based access options before assigning access to an External User. Provide access to only the minimum necessary resources. Use the Principle of Least Privilege, and add additional capabilities as needed.

3. Select **Create New User**.
4. For an Internal user account, perform the following steps:

   For an External user account, go to step 5 on page 334.

   a. Type the email address for the user and select **Next**.
   b. Configure the Table 109.

Table 109: User configuration settings

Field	Description
Email	Email address, not more than 128 characters.
First Name	First name, not more than 63 characters.
Last Name	Last name, not more than 63 characters.
Extreme Platform ONE	Specify access to Extreme Platform ONE Networking. Includes Security and SD-WAN if applicable.
ExtremeCloud IQ	Specify access for ExtremeCloud IQ. Role options are limited by the **Extreme Platform ONE** role selection above.

Table 109: User configuration settings (continued)

Field	Description
Sites	Specify access to sites. Administrators have access to all sites and locations if a site hierarchy is created. **Note:** It is imperative that you assign users to a site or sites.
Idle Session Timeout	Specify whether to enforce idle session timeout. If you do not specify a time, the user session will not timeout. **Note:** A non-expired timeout configuration overrides any admin-configured timeout. Otherwise, all admin-configured user timeout settings follow those that the admin configured.

c. Select **Save**.

d. You can review the access and roles assigned to the new user by selecting **Internal Users** in the **Users & Roles** area.

5. For an External user account, perform the following steps:

a. Type the external email address and select **Next**.

b. Configure the user's Application Access. Select the user role value for the Primary Role and the Classic Role.

c. **Configure site access** from the role-specific menu choices.

d. (Optional) Select the access duration:

- **Time Dependent:** Select start and end dates (optional). Select the respective drop-down menus to assign workspace and application access, and roles to the external user.
- **Indefinite:** Do not define start and end dates.This means site access is not time-limited until the value changes.

e. Select **Save**.

You can review the access and roles assigned to the new user in the **Users & Roles** area by selecting **External Users** in the **Users & Roles** area.

Related Links

Configure the Idle Session Timeout on page 386

Enable Multi-Factor Authentication

Multi-factor authentication (MFA) is available at the user level.

The system supports mobile apps authentication including Google Authenticator, Microsoft Authenticator, and Twilio.

Use this task to enable user-level MFA.

1. Select your initials in the upper right corner of your screen and select **Profile > Set Up MFA**.

2. Follow these steps to use the authentication APP to enable MFA:
   a. Type your password and select **Submit**.
   b. On the **Set Up Authenticator APP** screen, select an authenticator app and scan the QR code to download the app to your device.

      If you already have an authentication app, select **Skip** to skip this step.
   c. Open the authenticator app on your device and scan the QR code.
   d. In the **Verification Code** field, type the code shown in the authenticator app.
   e. Select **Submit**.
   f. The next time you login, the **Verify Your Identity** screen opens.
   g. Type the security code from the authenticator app and select **Submit**.

   Note
   If you disabled the MFA app and wants to enable it, re-scan the QR code and remove the old account from the app.

3. If you enable email or app MFA, select **Make as Default** for the selected MFA.

   The next time you login, Extreme Platform ONE Networking shows your default MFA.

Edit, Disable, or Delete a User Account

The **Edit** option provides the ability to modify roles, site access, and idle session timeout.

Use this task to edit, disable (suspend), or delete a user account.

1. Go to **Administration & Settings** > **Access Management**.
2. In the **Users & Roles** area, select the **Internal Users** or **External Users** tab.
3. Use search, group, and filter to locate the account.
4. Select the account to change.
5. Select ⋮ for the account, and then select one of the following options:
   - **Edit**. Make changes to the account configuration.
   - **Disable**. Inactivate the account, with the ability to reactivate if desired.
   - **Delete**. Remove the account permanently from the system.
6. Follow the prompts to make your changes, and select **Save**.
7. Select **Save**.

Identity Providers

Identity Providers | Network & Applications

An Identity Provider (IdP) is the source of your users' identities for your organization. Begin by configuring your IdP. You can do this by establishing connections with one of the following IdPs:

- Google Workspace on page 345
- Okta on page 353

The ability to support multiple identity providers (IdPs) within a single tenant is supported for complex identity management needs, such as during cloud service migrations, acquisitions, or ensuring redundancy. It also addresses the growing requirement to manage contractors with separate IdPs securely. This enhancement increases flexibility especially for customers.

For more information, see Support Multiple IdPs on page 364.

Microsoft Entra ID

There are three primary purposes for integrating with an Identity Provider for ExtremeCloud IQ (New). The applications created in the Identity Provider are to be different even if the type is the same, however they can be reused if desired

The purposes are:

- User and User Group Synchronization – Used to make users and user groups available within ExtremeCloud IQ (New) for policy assignment.
- Application Access authentication – Used for logging into the ExtremeCloud IQ (New) Agent or the End User web portal.
- Network Access authentication – Used for 802.1X EAP-TTLS authentication of clients on access points and switches.

Synchronize Users and User Groups with Entra ID

Synchronizing Users and User Groups from Entra ID is required to ensure policies can be applied to users connecting with Entra ID credentials in ExtremeCloud IQ (New). There are two methods available for synchronization:

1. Just in Time (JIT) Synchronization – this method has ExtremeCloud IQ (New) reach into Microsoft Entra ID and pull users and user groups on a polled basis. This method leverages an OIDC application to integrate with the Entra APIs.
2. System for Cross-Domain Identity Management (SCIM) Synchronization – this method has Microsoft Entra ID push users and user groups from Entra into ExtremeCloud IQ (New). This method requires an enterprise application to be set up in Entra ID so that automatic provisioning can be enabled.

Synchronizing Users and User Groups with JIT

For JIT integration, the setup in Entra ID will be completed first, followed by the configuration of ExtremeCloud IQ (New).

Configure JIT in Microsoft Entra ID

Use this task to configure JIT in Microsoft Entra ID.

1. In Microsoft Entra ID go to **Applications** > **App registration** and select **New registration**.
2. Under **Register an application**, name the application appropriately for JIT Integration. Leave the default fields selected and select **Register**.

3. Copy the **Application (client) ID** and **Directory (tenant) ID** for use later. Under **Client Credentials**, select **Add a certificate or secret**.
4. Select **New client secret**. Enter a description if desired and a preferred expiration date of the secret. Once complete, select **Add**.
5. Copy the value of the new secret for use later.
6. Go to **Manage** > **Token Configuration**, select **Add optional claim** and configure the settings in Table 110.

Table 110: Optional Claim Configuration Settings

Field	Description
Token Type	Select the **ID** radio button.
Claim	Select the following from the available list: • email • family_name • given_name • upn
Turn on the Microsoft Graph email, profile permission (required for claims to appear in token).	Enable the toggle if prompted to turn on Microsoft Graph.
Select **Add**.	

7. Select **Add groups claim** and configure settings in Table 111.

Table 111: Group Claim Configuration Settings

Field	Description
Select group types to include in Access, ID, and SAML tokens.	Select **Groups assigned to the application**.
Customize token properties by type	Select **Group ID**.
Select **Add**.	

8. Go to **Manage** > **API permissions** and select **Add a permission**.
9. Select **Microsoft Graph** and configure the settings in Table 112.

Table 112: Microsoft Graph Configuration Settings

Field	Description
What type of permissions does your application require?	Select the **Application permissions**.
Select permissions	Filter on text of the permission needed and select it from the drop-down list. The following permissions are required: • User.Read.All • Group.Read.All • GroupMember.Read.All

Table 112: Microsoft Graph Configuration Settings (continued)

Field	Description
Select **Add permissions** and the **Configured permissions** window is displayed.	
Configured permissions	Select **Grant admin consent for <Company Name>**.

10. Go to **Overview**, scroll to the bottom, and select **Go to Enterprise applications**.
11. Go to **Manage** > **Properties**, set **Assignment required?** to **Yes**, and select **Save**.
12. Go to **Manage** > **Users and groups**, and select **Add user/group**.
13. Assign all groups that should be leveraged in ExtremeCloud IQ (New).

Configure ExtremeCloud IQ (New) JIT

Use this task to configure the Sync IDP profile in ExtremeCloud IQ (New).

1. Log into your ExtremeCloud IQ (New) tenant.
2. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.
3. Select **Add IDP Profile** and configure the settings in Table 113.

Table 113: JIT for Microsoft Entra ID Configuration Settings

Field	Description
Set Up IdP	Select **Sync Users and User Groups** from the Purpose drop-down list.
Approved Domains	If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains**
Select Identity Provider	Select **Microsoft Entra ID** from the **Identity Provider** drop-down list.
Setup Guidelines	Select **JIT (Just in Time)** for the **Sync Using** drop-down list.
	Paste the copied credentials from Microsoft Entra ID: • Client ID • Client Secret • Tenant ID

4. To complete the setup, select **Save**.

A dynamic sync workflow will be schedule automatically. To force a sync, go to **Access ManagementIdentity providers**, select ⋮ and select **Sync Now** .

Synchronizing Users and User Groups with SCIM

For SCIM integration, the setup in ExtremeCloud IQ (New) will be completed first, followed by the configuration of Microsoft Entra ID.

Configure ExtremeCloud IQ (New) SCIM for Microsoft Entra ID

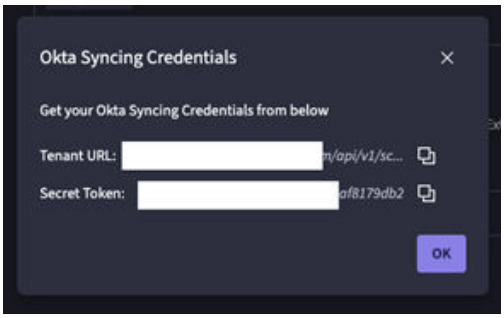
Use this task to configure ExtremeCloud IQ (New) SCIM for Microsoft Entra ID.

1. In ExtremeCloud IQ (New), go to **Access Management** > **Administration & Settings** > **Identity Providers** and select **Network & Applications**.
2. To create a new profile, select the **Add IdP Profile** and configure the settings in Table 114.

Table 114: SCIM for Microsoft Entra ID Configuration Settings

Field	Description
Set Up IdP	Select **Sync Users and User Groups** as the **Purpose** from the drop-down list.
Approved Domains	If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains**.
Select Identity Provider	Select **Microsoft Entra ID** from the **Identity Provider** drop-down list.
Setup Guidelines	Select **SCIM (System for Cross-domain Identity Management)** for the **Sync Using** drop-down list.

3. Select **Save**.
4. Once saved, from the 3-dot menu, select **Edit**.
5. In the **Edit** window, select **Entra Syncing Credentials**.
6. In the **Entra ID Syncing Credentials** window, save the **Tenant URL** and **Secret Token** for use within Entra ID.



Synchronize Users and User Groups using SCIM Provisioning

Using SCIM to push Users and User Groups into ExtremeCloud IQ (New) requires the creation of an Enterprise Application in Entra ID. Use this task to configure System for Cross-domain Identity Management (SCIM) provisioning in Microsoft Entra ID.

1. Log in to Microsoft Entra ID and go to **Enterprise application** > **New application**.
2. Select **Create your own application**. Name the application with Provisioning in the title so that it can be easily located. Select the **Non-gallery** option.
3. Select **Properties** for the application and toggle **Assignment Required** to **Yes** and **Visible to Users** to **No**, then select **Save**.
4. Select **Users and groups** and assign the User groups that should be included in ExtremeCloud IQ (New).
5. Go to **Manage** > **Provisioning** and select **New configuration**.

6. Under **Admin Credentials**, paste the **Tenant URL** and **Secret Token** that were previously copied from ExtremeCloud IQ (New). Select **Test Connection** and on resulting success, select **Create**.
7. Select **Provision Microsoft Entra ID Users**.
8. On the **Attributes Mapping** page and complete the following:
   a. Under **Source Object Scope**, select **All records**.
   b. Select **Add new filter group**.
   c. In **Add Scoping Filter**, select **mail** as the source attribute. The mail attribute needs to exist for the user to be imported into ExtremeCloud IQ (New). If the desire is to only have corporate email accounts imported into ExtremeCloud IQ (New), matching on the email extension for the organization will work. For this example, select **INCLUDES** as the operator and the email domain as the clause value.
   d. Name the scoping filter and select **Apply**.
   e. In the resulting screens, select **Apply** and **Save** to save the filter to the provisioning profile.
9. Go to **Overview**, select **Start Provisioning** to begin the provisioning process.
10. Provisioning can take up to an hour to start. If desired **Provision on Demand** can be selected from the **Provisioning Overview** to immediately start a provisioning cycle.
11. Select the group or users to provision at that moment.
12. In ExtremeCloud IQ (New) the users and user groups should now be available in the **Policy** > **Users & Devices** > **Users** section. If the users or user groups do not show up, review errors or messages in Entra ID for why the provisioning failed.

Network Access with Microsoft Entra ID

If user-based 802.1X EAP-TTLS network authentication is going to be used with Microsoft Entra ID, a separate application is required to be created that bypasses MFA as 802.1X does not have a native method to provide real-time multi-factor authentication prompt. This can only be done with an OpenID Connect (OIDC) Application.

If EAP-TLS (Certificate-based authentication) is going to be the only source of 802.1X user and device authentication, this setup is not required.

Configure Microsoft Entra ID

Use this task to configure Microsoft Entra ID for Network Access.

1. In Microsoft Entra ID go to **Applications** > **App registration** and select **New registration**.
2. Under **Register an application**, name the application appropriately for the Network Access Integration. Leave the default fields selected and select **Register**.
3. Copy the **Application (client) ID** and **Directory (tenant) ID** for use later. Under **Client Credentials**, select **Add a certificate or secret**.
4. Select **New client secret**. Enter a description if desired and a preferred expiration date of the secret. Once complete, select **Add**.
5. Copy the value of the new secret for use later.
6. Go to **Manage** > **API permissions** and select **Grant admin consent for <Company Name>**.

Configure ExtremeCloud IQ (New) for Entra ID

Use this task to configure ExtremeCloud IQ (New) for Entra ID.

1. Log into your ExtremeCloud IQ (New) tenant.
2. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.
3. Select **Add IdP Profile** and configure the settings in Table 115.

Table 115: Entra ID IdP Profile Configuration Settings

Field	Description
Set Up IdP	Select **Network Access** from the Purpose drop-down list.
Approved Domains	If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains**
Select Identity Provider	Select **Microsoft Entra ID** from the **Identity Provider** drop-down list.
Setup Guidelines	Paste the copied credentials from Microsoft Entra ID: • Client ID • Client Secret • Tenant ID

4. To complete the setup, select **Save**.

Disable MFA using a conditional Access Policy for Entra ID

Network Authentication requires that multi-factor authentication be disabled for an Entra ID application when using EAP-TTLS. If Entra ID premium is used, a rule can be created to exclude this only for the Network Access OIDC application. If Entra ID premium is not in use, this must be disabled for all users. For more information on Conditional Access Policies, refer to Microsoft documentation here: https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview

1. Log in to Microsoft Entra ID.
2. Go to **Manage** > **Properties** and configure the settings.
   a. Select **Manage Security defaults**.
   b. Disable the toggle **Disabled** and select **Save**.
3. Go to **Identity** > **Protection** > **Conditional Access** and configure the settings in Table 116.

Table 116: Conditional Access Configuration Settings

Field	Description
User ad groups	Select **All users**.
Cloud apps or actions	Under **Exclude** select the OIDC app created earlier in the **Select excluded cloud apps**.

Table 116: Conditional Access Configuration Settings (continued)

Field	Description
Grant	Select **Grant access** and check **Require multi-factor authentication** and any other settings your organization requires.
Enable policy	Set to **On**.
Select **Create**.	

Application Access with Microsoft Entra ID

Application access for users can be authenticated via Microsoft Entra ID in two ways: OpenID Connect (OIDC) or SAML. The setup process is different in Entra ID depending on the type of integration being leveraged.

Application Access using Open ID Connect (OIDC)

For OIDC integration, the setup in Entra ID will be completed first, followed by the configuration of ExtremeCloud IQ (New). A Redirect URI will be needed from ExtremeCloud IQ (New).

1. Go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Users**.
2. To create a new profile, select **Add IdP Profile** and configure the settings in Table 117.

Table 117: Entra ID Application Access OIDC IdP Profile Configuration Settings

Field	Description
Set Up IdP	Select **Application Access** from the Purpose drop-down list.
Approved Domain	If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**.
Select Identity Provider	Select **Microsoft Entra ID** from the Identity Provider drop-down list.
Application Access	Select **OpenID Connect** from the Single Sign-On drop-down list.
Setup Redirect URIs	Copy the Redirect URI.

3. Select **Cancel**.

Configure Microsoft Entra ID Application Access

Use this task to configure Microsoft Entra ID Application Access.

1. In Microsoft Entra ID go to **Applications** > **App registration** and select **New registration**.
2. Under **Register an application**, name the application appropriately for the Application Access Integration. Leave the default fields selected and select **Register**.
3. Select **Add a Redirect URI**.
4. Select **Add a platform** followed by **Web**.

5. Enter one of the Redirect URIs that was previously copied from ExtremeCloud IQ (New) and select **Configure**.
6. Select Add URI and paste in the second Redirect URI that was copied from ExtremeCloud IQ (New). Select **Save**.
7. Copy the **Application (client) ID** and **Directory (tenant) ID** for use later. Under **Client Credentials**, select **Add a certificate or secret**.
8. Select **New client secret**. Enter a description if desired and a preferred expiration date of the secret. Once complete, select **Add**.
9. Copy the value of the new secret for use later.
10. Go to **Manage** > **API permissions** and select **Grant admin consent for <Company Name>**.

Configure ExtremeCloud IQ (New) for Microsoft Entra ID Application Access

Use this task to configure ExtremeCloud IQ (New) for Microsoft Entra ID Application Access.

1. Log into your ExtremeCloud IQ (New) tenant.
2. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Application**.
3. Select **Add IdP Profile** and configure the settings in Table 118.

Table 118: Entra ID Application Access IdP Profile Configuration Settings

Field	Description
Set Up IdP	Select **Application Access** from the Purpose drop-down list.
Approved Domains	If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains**
Select Identity Provider	Select **Microsoft Entra ID** from the **Identity Provider** drop-down list.
Secure Application Access	Under **Single Sign-On Method**, select **OpenID Connect**.
Setup Extreme Platform One Security	Paste the copied credentials from Microsoft Entra ID: • Client ID • Client Secret • Tenant ID

4. To complete the setup, select **Save**.

Microsoft Entra ID Application Access using SAML

For SAML integration, the preparation in ExtremeCloud IQ (New), followed by the configuration in Entra ID, and a finalization in ExtremeCloud IQ (New).

Configure ExtremeCloud IQ (New) Microsoft Entra ID SAML Preparation

Prior to configuring the SAML application in Microsoft Entra ID, an Identifier and Reply URL will be needed from ExtremeCloud IQ (New).

1. In ExtremeCloud IQ (New), go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Users**.
2. To create a new profile, select **Add IdP Profile** and configure settings in Table 119.

Table 119: Microsoft Entra ID SAML Preparation Configuration Settings

Field	Description
Set Up IdP	Select **Application Access** from the Purpose drop-down list.
Approved Domain	If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**.
Select Identity Provider	Select **Microsoft Entra ID** from the Identity Provider drop-down list.
Single Sign-On Method	Select **SAML**.
Setup Up SSO in Microsoft Entra ID	Copy the Identifier and the Reply URL.

Note
Leave this page open. If it is canceled, the Identifier will change, and this will need to be updated in the Microsoft Entra ID application.

3. Select **Save**.

Configure Microsoft Entra ID SAML

Use his task to configure Microsoft Entra ID SAML.

1. Log in to Microsoft Entra ID and go to **Enterprise application** > **New application**.
2. Select **Create your own application**. Name the application so that it can be easily located. Select the **Non-gallery** option.
3. Go to **Manage** > **Single Sign-On** and select SAML.
4. Under **Basic SAML Configuration** select **Edit**.
5. Select **Add identifier** and paste in the Identifier from ExtremeCloud IQ (New) then select **Add reply URL** and paste in the **Reply URL** that was previously copied. Select **Save**.
6. When prompted to test the integration, select **No, I'll test later**.
7. Further down the SAML application, download the SAML Certificate in Base64 format. Copy the Login URL and the Microsoft Entra Identifier.

Configure ExtremeCloud IQ (New) Microsoft Entra ID SAML Finalization

Use this task to complete the final Microsoft Entra ID SAML configuration in ExtremeCloud IQ (New).

In the **Application Access IdP** screen that was left open, paste in the Login URL, the Microsoft Entity ID Identifier, and upload the certificate that was downloaded. Select **Save**.

Note
If this page was canceled, the Identifier will need to be updated in the Microsoft Entra ID application.

Google Workspace

There are three primary purposes for integrating with an Identity Provider for ExtremeCloud IQ (New). The applications created in the Identity Provider are to be different even if the type is the same, however they can be reused if desired.

The purposes are:

- User and User Group Synchronization – Used to make users and user groups available within ExtremeCloud IQ (New) for policy assignment.
- Application Access authentication – Used for logging into the ExtremeCloud IQ (New) Agent or the End User web portal.
- Network Access authentication – Used for 802.1X EAP-TTLS authentication of clients on access points and switches.

Synchronize Users and Groups with Google Workspace

User and User Group synchronization is performed using the Directory APIs in Google Workspace. They are retrieved on a polled basis from ExtremeCloud IQ (New).

Configure Google Workspace

Use this task to synchronize user and user groups using Google Workspace.

1. Log into Google Cloud via https://console.cloud.google.com.
2. To create a new project, from the drop-down menu at the top of the screen and select **New Project**.
3. Name the project appropriately and select **Create**.
4. Under **Quick Access**, select **APIs & Services**.
5. Select **ENABLE APIS AND SERVICES**.
6. In the search field, enter and select **Admin SDK AP**.
7. Select **ENABLE**.
8. Go to **APIS and SERVICES** > **Credentials**.
9. Select **CREATE CREDENTIALS** and from the drop-down select **Service account**.
10. Enter a service account name to use for the syncing. Select **CREATE AND CONTINUE**, then leave the optional fields blank.
11. Select **DONE**.
12. Select the newly created service account. Copy the Email and Unique ID to be used in later steps and select **KEYS**.
13. From the **ADD KEY** drop-down menu, select **Create new key**.

14. In the **Create Private Key** screen, select JSON as the key type and **CREATE**. This will download the private key to be used.

> **Note**
> If an error is received here due to a permissions issue, see <enter a link to the new security topic>. This restriction appears for newly created Google Cloud Accounts.

15. In the Google Admin Console, go to **Security** > **Access and data control** > **API controls** and select **MANAGE DOMAIN WIDE DELEGATION**.
16. Under **API clients**, select **Add new** and configure the settings in Table 120.

Table 120: API Client Configuration Settings

Field	Description
Client ID	Enter the Unique ID that was previously copied from the Service Account entry.
OAuth Scopes	https://www.googleapis.com/auth/admin.directory.user https://www.googleapis.com/auth/admin.directory.group.member https://www.googleapis.com/auth/admin.directory.group https://www.googleapis.com/auth/admin.directory.user.alias

17. Select **AUTHORIZE.**
18. Go to **Account** > **Admin roles**.
19. If no User and User Group with read privileges appears, select **Create role** and configure the settings in Table 121.

Table 121: Role Configuration Settings

Field		Description
Role Info	Name	Enter a group name.
	Description (Optional)	Enter a role description.
Select **CONTINUE**.		
Select Privileges	Users	Within this group select **Read**.
	Groups	
Select **CONTINUE**.		
Review Admin API Privileges	The review screen confirms that Read privileges are allowed for API calls for Users and Groups.	
Select **CREATE ROLE**.		

20. If the role was just created, select Assign service accounts. If not, select **Assign role** > **Assign service accounts**.
21. Enter the email of the service account, select **ADD** then **ASSIGN ROLE**.
22. Go to **Account** > **Account Settings** and copy the customer ID of Google Workspace.

Configure ExtremeCloud IQ (New) for Google Workspace

Use this task configure ExtremeCloud IQ (New) for Google Workspace.

1. Log into your ExtremeCloud IQ (New) tenant.
2. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.
3. Select **Add IDP Profile** and configure the settings in Table 122.

Table 122: Google Workspace IdP Profile Configuration Settings

Field	Description
Set Up IdP	Select **Sync Users and User Groups** from the Purpose drop-down list.
Approved Domains	If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains**
Select Identity Provider	Select **Google Workspace** from the **Identity Provider** drop-down list.
Setup Guidelines	Upload the private key JSON file that was downloaded from Google Cloud Console and paste in the Customer ID that was saved from the Google Admin Console.

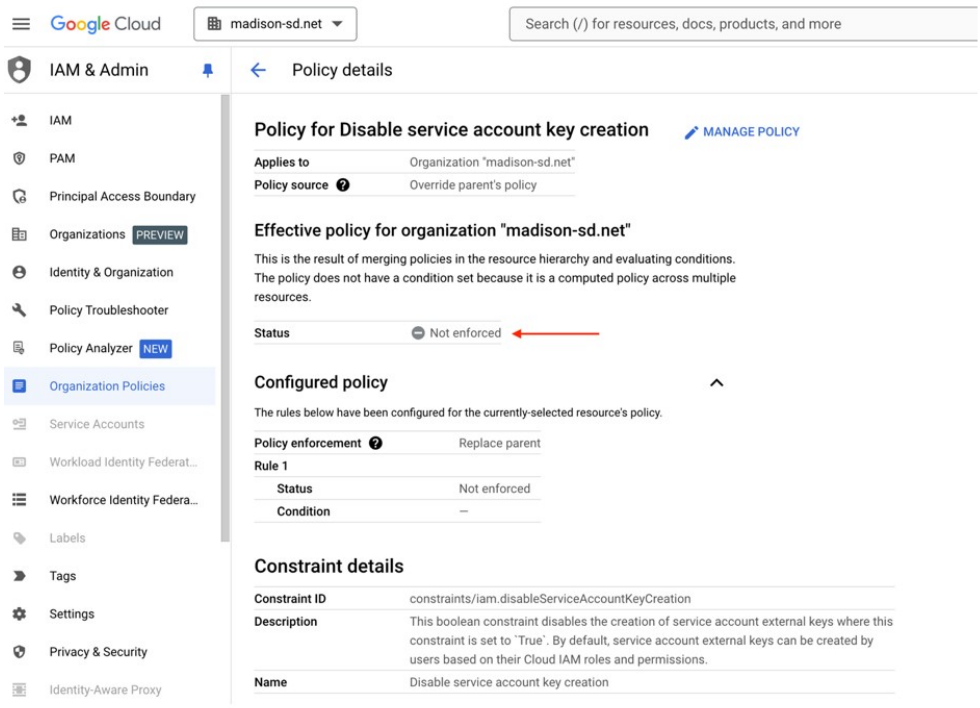
4. To complete the setup, select **Save**.

Adjust Security Defaults for Google Workspace

In cases where a newer Google Workspace or Google Cloud Platform instance was created, security defaults may be enabled so that the administrator cannot download keys for service accounts. If this is the case, use this task to adjust security defaults for Google Workspace.

1. Log into Google Cloud via https://console.cloud.google.com.
2. From the top left, if you are already in a project, select the parent project from the drop-down list.
3. Go to **IAM & Admin** > **IAM**.
4. Under **IAM**, ensure that your account has an Organization Policy Administrator. If it does not, select Edit (pencil icon) next to your account to edit the roles. If your account isn't listed here, to add it select **GRANT ACCESS** and configure settings:
   a. Within the **Edit** window, select **Add Another Role**.
   b. Select the **Organization Policy Administrator** condition from the drop-down list.
   c. Select **SAVE**.
5. Once the roles are set, go to **Organization Policies** > **IAM & Admin**.
6. In the Organization Policies, search for iam.disableServiceAccountKeyCreation. Select edit to make updates.
7. Select **MANAGE POLICY**.
8. Select **Override the parent's policy**. Then edit or create a rule to set the enforcement to **Off**. Finish by selecting the **SET POLICY**.

A successful configuration should look similar to the below screenshot. The creation and download of a private key for a service account should now be successful.



Network Access with Google Workspace

If user-based 802.1X EAP-TTLS network authentication is going to be used with Google Workspace, an Secure LDAP integration is required to be created.

If EAP-TLS (Certificate-based authentication) is going to be the only source of 802.1X user and device authentication, this setup is not required.

Configure Google Workspace for Network Access

Use this task to configure Google Workspace for Network Access.

1. Log into the Google Admin Console and under **Apps** select **LDAP**.
2. Select **Add Client** and configure the settings in Table 123.

Table 123: Client Configuration Settings

Section	Field	Description
Client Details	LDAP client name	Enter a client name.
Select **Continue**.		
Access permissions	Verify user credentials	Select **Entire domain (madison-sd net)**.
	Read user information	Select **Entire domain (madison-sd.net)**.
Select **ADD LDAP CLIENT**.		

3. In the resulting page, once the certificate is done generating, download it and save it for use in ExtremeCloud IQ (New). Select **Continue to Client Details**.

4. By default, the LDAP client is not enabled. To enable it, select the drop-down list under **Service Status**.
5. Select **ON for everyone**.

Configure ExtremeCloud IQ (New) for Google Workspace Network Access

Use this task to configure ExtremeCloud IQ (New) for Google Workspace Network Access.

1. Log into your ExtremeCloud IQ (New) tenant.
2. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.
3. Select **Add IDP Profile** and configure the settings in Table 124.

Table 124: Google Workspace Network Access IdP Profile Configuration Settings

Field	Description
Set Up IdP	Select **Network Access** from the Purpose drop-down list.
Approved Domains	If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains**.
Select Identity Provider	Select **Google Workspace** from the **Identity Provider** drop-down list.
Setup ExtremeCloud IQ (New)	Upload the saved Secure LDAP configuration from Google Admin Console.

4. To complete the setup, select **Save**.

Application Access with Google Workspace

Application access for users can be authenticated via Google Workspace in two ways: OpenID Connect (OIDC) or SAML. The setup process is different in Okta depending on the type of integration being leveraged.

Configure Application Access using Open ID Connect (OIDC)

For OIDC integration, the setup in Google Workspace will be completed first, followed by the configuration of ExtremeCloud IQ (New). A Redirect URI will be needed from ExtremeCloud IQ (New).

1. Go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.
2. To create a new profile, select **Add IdP Profile** and configure settings in Table 125.

Table 125: OIDC Application Access IdP Profile Settings

Field	Description
Set Up IdP	Select **Application Access** from the Purpose drop-down list.
Approved Domain	If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**.

Table 125: OIDC Application Access IdP Profile Settings (continued)

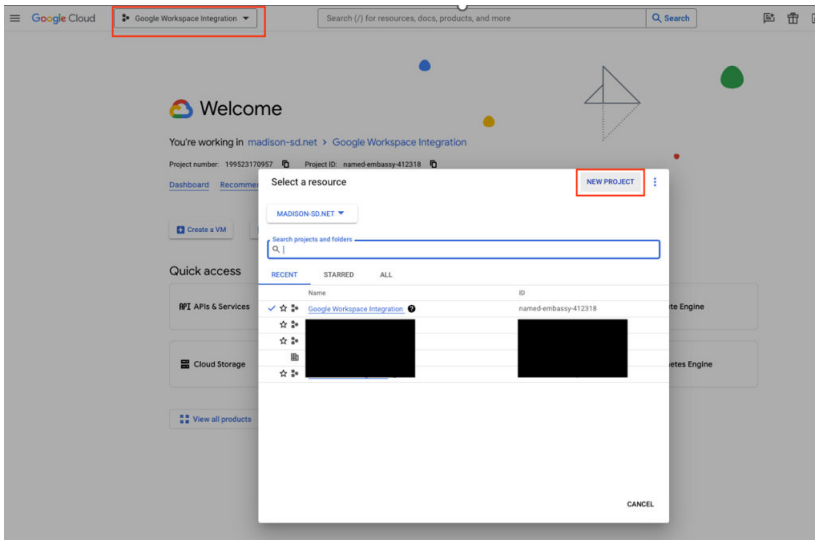
Field	Description
Select Identity Provider	Select **Google Workspace** from the Identity Provider drop-down list.
Application Access	Select **OpenID Connect** from the Single Sign-On drop-down list.
Setup Redirect URIs	Copy the Redirect URI.

3. Select **Cancel**.

Set up Google Workspace with Open ID Connect

Use this task set up Google Workspace with Open ID Connect (OIDC) in Google Cloud (GCP).

1. Log in to Google Cloud using https://console.cloud.google.com.
2. To create a new project:
   a. From the drop-down menu at the top of the screen, select **NEW PROJECT**.



   b. Enter a name in the **Project Name** field and select **CREATE**.
   c. Select the newly created Project, then from the left navigation screen select **VIEW ALL PRODUCTS**.
   d. Under the **All products**, select **Google Auth Platform**.
   e. Select **GET STARTED**.
   f. In the **App Information** section, enter the App Name, select a User support email from the drop-down list then select **Next**.
   g. In the **Audience** section, select **Internal** and then select **Next**.
   h. Under **Contact Information**, enter an email address and select **NEXT**.
   i. Finally, agree to the User Data Policy and select **CREATE**.

3. Go to **Overview**, select **CREATE OAUTH CLIENT** and configure the settings in Table 126.

Table 126: OAuth Client Configuration Settings

Section	Field	Description
CREATE OAuth client ID	Application Type	Select **Web application** from the drop-down list.
	Name	Name the OAuth client.
Authorized redirect URIs	URIs 1	Create two entries and paste the two Redirect URIs that were previously copied from ExtremeCloud IQ (New).
	URIs 2	
Select **Create**.		

4. Under **OAuth 2.0 Client IDs**, select the newly created client.
5. Under **Additional information**, copy the **Client ID** and **Client secret**.

Configure Application Access with Google Workspace for SAML

For SAML integration, the preparation in ExtremeCloud IQ (New), followed by the configuration in Google Workspace, and a finalization in ExtremeCloud IQ (New).

Prepare ExtremeCloud IQ (New) SAML

Prior to configuring the SAML application in Google Workspace, an Identifier and Reply URL will be needed from ExtremeCloud IQ (New).

Use this task to prepare ExtremeCloud IQ (New) for SAML application access.

1. In ExtremeCloud IQ (New), go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.
2. To create a new profile, select **Add IdP Profile** and configure the settings in Table 127.

Table 127: SAML IdP Profile Configuration Settings

Field	Description
Set Up IdP	Select **Application Access** from the Purpose drop-down list.
Approved Domain	If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**.
Select Identity Provider	Select **Google Workspace** from the Identity Provider drop-down list.
Single Sign-On Method	Select **SAML**.
Setup Up SSO in Microsoft Entra ID	Copy the Identifier and the Reply URL.

Note
Leave this page open. If it is canceled, the Identifier will change, and this will need to be updated in the Google Workspace application.

3. Select **Save**.

Configure Google Workspace SAML Application Access

Use this task to configure Google Workspace for SAML Application Access.

1. Log into the Google Admin Console and go to **Apps** > **Web and mobile apps**.
2. From the **Add app** drop-down list, select **Add custom SAML app** and configure the settings in Table 128.

Table 128: SAML Application Access Configuration Settings

Section	Field	Description
App details	App name	Name the App.
Select **Continue**.		
Google Identity Provider Details	SSO URL	Under **Option 2** copy the SSO URL and Entity ID.
	Entity ID	
	Certificate	Download certificate.
Select **Continue**.		
Service provider details	ACS URL	Paste in the **ACS URL** and **Entity ID** that was previously copied from ExtremeCloud IQ (New).
	Entity ID	
Name ID	Name ID format	Set the **Name ID format** to **EMAIL**.
	Name ID	Set the **Name ID** to **Basic Information** > **Primary email**.
Select **Continue**.		
Attribute Mapping	Select **ADD MAPPING**.	
	First name	Enter **first_name**.
	Last name	Enter **last_name**.
	Primary email	Enter **email**.
Select **FINISH**.		

Configure ExtremeCloud IQ (New) Google Workspace SAML Finalization

Use this task to complete the final Google Workspace SAML configuration in ExtremeCloud IQ (New).

In the **Application Access IdP** screen that was left open, paste in the SSO URL, the Entity ID Identifier, and upload the certificate that was downloaded. Select **Save**.

Note
If this page was canceled, the Identifier will need to be updated in the Google Workspace application.

Okta

The ExtremeCloud IQ (New) API Service Integration provides a secure, scalable interface to access your Okta directory without requiring individual user credentials. This integration is primarily designed for automated synchronization of users and groups, ensuring consistent and centralized identity management across the ExtremeCloud IQ (New) environment.

Synchronize Users and User Groups with Okta

Synchronizing Users and User Groups from Okta is required to ensure policies can be applied to users connecting with Okta credentials in ExtremeCloud IQ (New). There are two methods available for synchronization:

1. Just in Time (JIT) Synchronization – this method has ExtremeCloud IQ (New) reach into Okta and pull users and user groups on a polled basis. This method leverages an OIDC application to integrate with the Okta APIs.
2. System for Cross-Domain Identity Management (SCIM) Synchronization – this method has Okta push users and user groups from Okta into ExtremeCloud IQ (New). This method requires an enterprise application to be set up in Entra ID so that automatic provisioning can be enabled.

Synchronizing Users and User Groups with JIT

For JIT integration, the setup in Okta will be completed first, followed by the configuration of ExtremeCloud IQ (New).

Configure Okta JIT

Use this task to configure Okta for JIT.

1. In the Okta administrator portal, go to the **Applications** > **API Service Integrations**.
2. Select **Add Integration**.
3. From the list, select **Extreme Platform ONE Security API Service**, then select **Install and Authorize**.

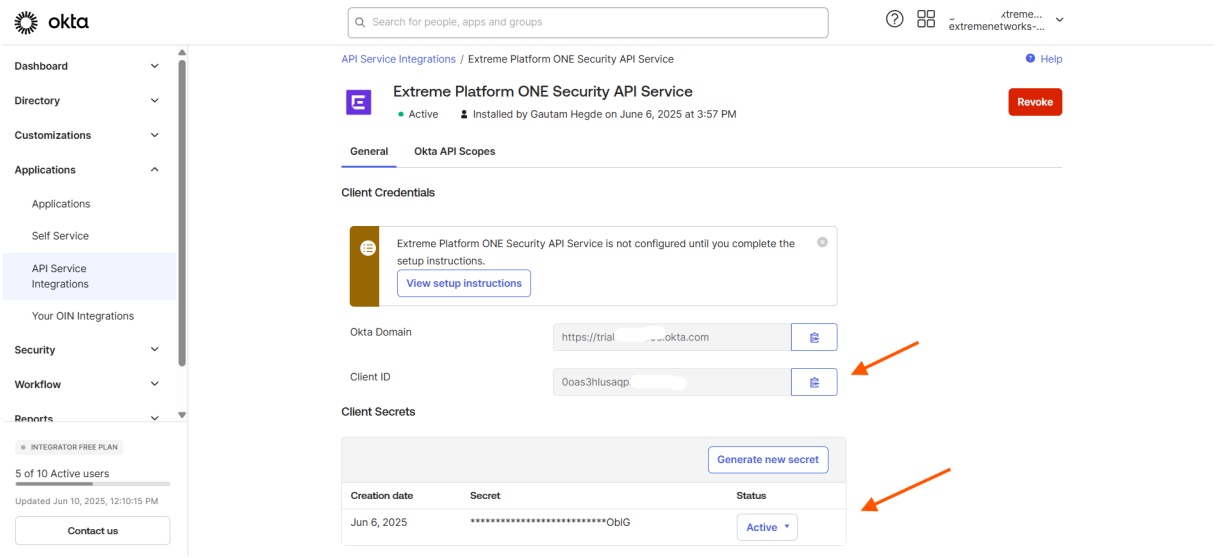
   The following API scopes are automatically applied:

   - `okta.users.manage`
   - `okta.apps.manage`
   - `okta.groups.manage`
4. To copy the Client Secret, when prompted, select **Copy to clipboard**.

   Note
   The Client Secret is only shown once. Ensure it is copied and stored securely.

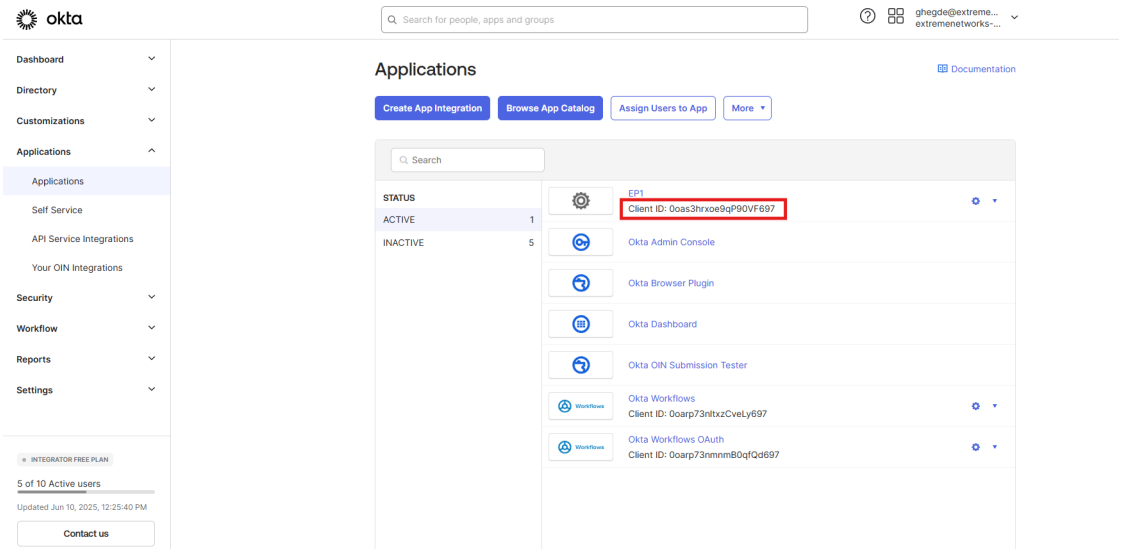
5. Select **Done**.

6. Copy and securely store the following:

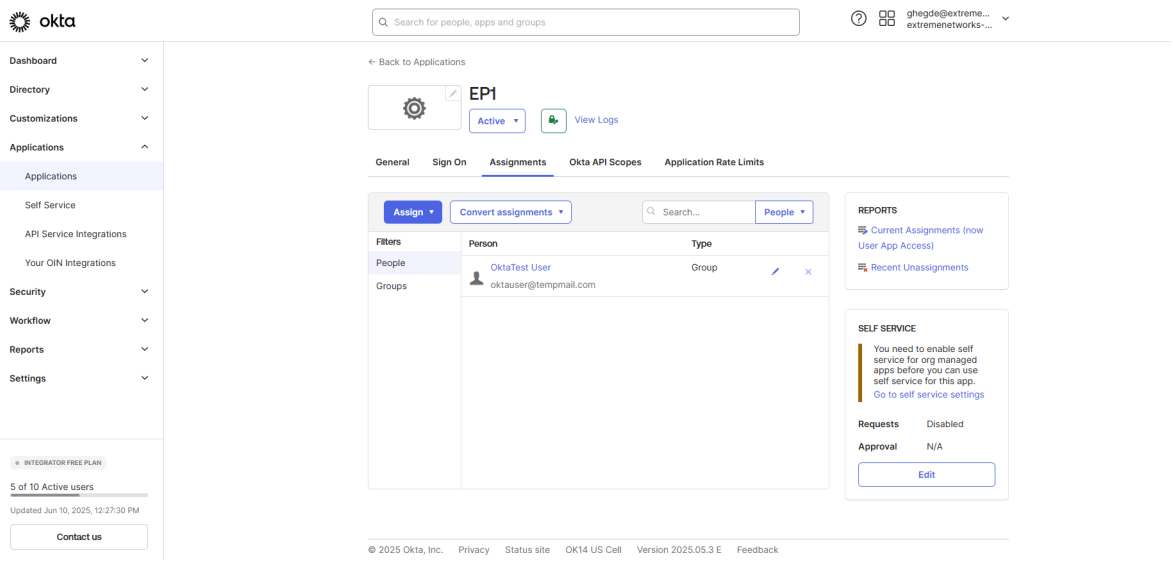


- Okta Org Domain (without the https prefix. e.g. trial-4343365.okta.com)
- API Service Client ID

7. Under **Assignments**, locate and copy the Client ID of the OIDC application you wish to sync users and groups.



Note
Reference the image below oktauser@tempmail.com is assigned to OIDC App which will be synced after successful setup.



Configure Extreme Platform ONE Security JIT

Use this task to configure the Sync IdP profile in ExtremeCloud IQ (New).

1. Log into your ExtremeCloud IQ (New) tenant.
2. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.
3. Select **Add IdP Profile** and configure the settings in Table 129.

Table 129: JIT IdP Profile Configuration Settings

Field	Description
Set Up IdP	Select **Sync Users and User Groups** from the Purpose drop-down list.
Approved Domains	If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains**
Select Identity Provider	Select **Okta** from the **Identity Provider** drop-down list.
Setup Guidelines	Select **JIT (Just in Time)** for the **Sync Using** drop-down list.
	Paste the copied credentials from Okta: • API Service Client ID • API Service Client Secret Key • Application Access Client ID • Org Domain

4. To complete the setup, select **Save**.

A dynamic sync workflow will be schedule automatically. To view synced users and groups, go to **Policy** > **Users & Devices**.

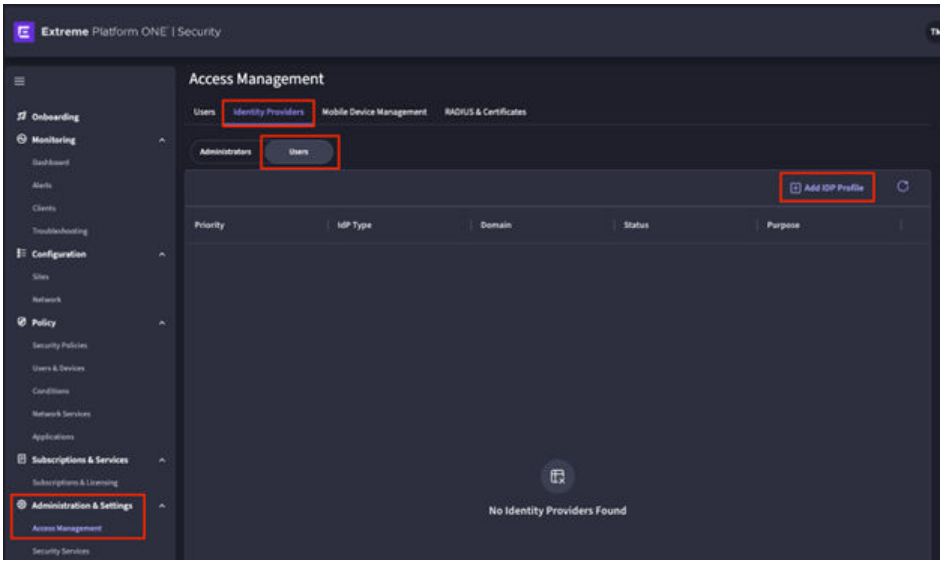
Synchronizing Users and User Groups with SCIM

For SCIM integration, the setup in ExtremeCloud IQ (New) will be completed first, followed by the configuration of Okta.

Configure ExtremeCloud IQ (New) SCIM

Use this task to configure ExtremeCloud IQ (New) SCIM for Okta.

1. In ExtremeCloud IQ (New), go to **Access Management** > **Administration & Settings** > **Identity Providers** and select **Network & Applications**.



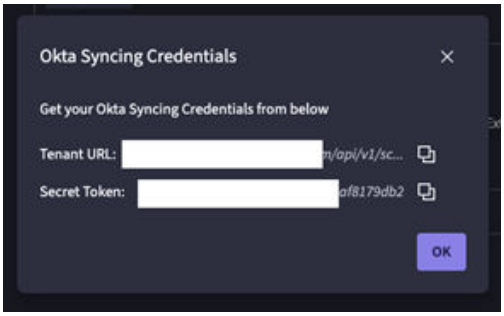
2. To create a new profile, select the **Add IdP Profile** and configure the settings in Table 130.

Table 130: Okta SCIM IdP Profile Configuration Settings

Field	Description
Set Up IdP	Select **Sync Users and User Groups** as the **Purpose** from the drop-down list.
Approved Domains	If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains**.
Select Identity Provider	Select **Okta** from the **Identity Provider** drop-down list.
Setup Guidelines	Select **SCIM (System for Cross-domain Identity Management)** for the **Sync Using** drop-down list.

3. Select **Save**.
4. Once saved, from the 3-dot menu, select **Edit**.
5. In the **Edit** window, select **Okta Syncing Credentials**.

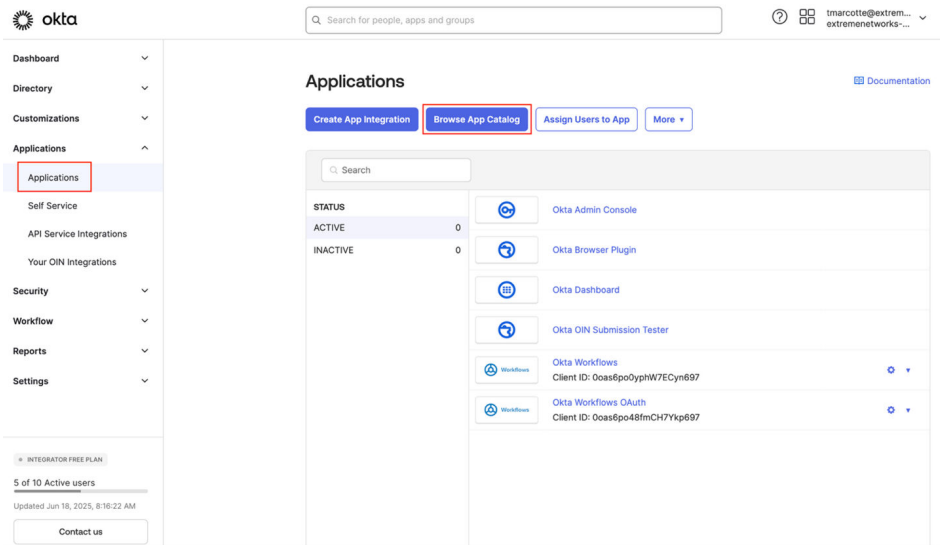
6. In the **Okta Syncing Credentials** window, save the **Tenant URL** and **Secret Token** for use within Okta.



Configure Okta SCIM

Use this task to configure Okta SCIM.

1. In the Okta administrator portal, go to the **Applications** > **Browse App Catalog**.



2. In the search field, enter and select **(OAuth Bearer Token) Governance with SCIM 2.0**.
3. Select **Add Integration**.
4. On the **General Settings** tab, in the **Application label** field, enter **Extreme Platform ONE Security - SCIM** and select **Next**.
5. On the **Sign-On Options** tab, scroll to the bottom and select **Done**. No additional information needs to be added for the SCIM integration.
6. In the new application, select the **Provisioning** > **Configure API Integration** and configure the settings in Table 131.

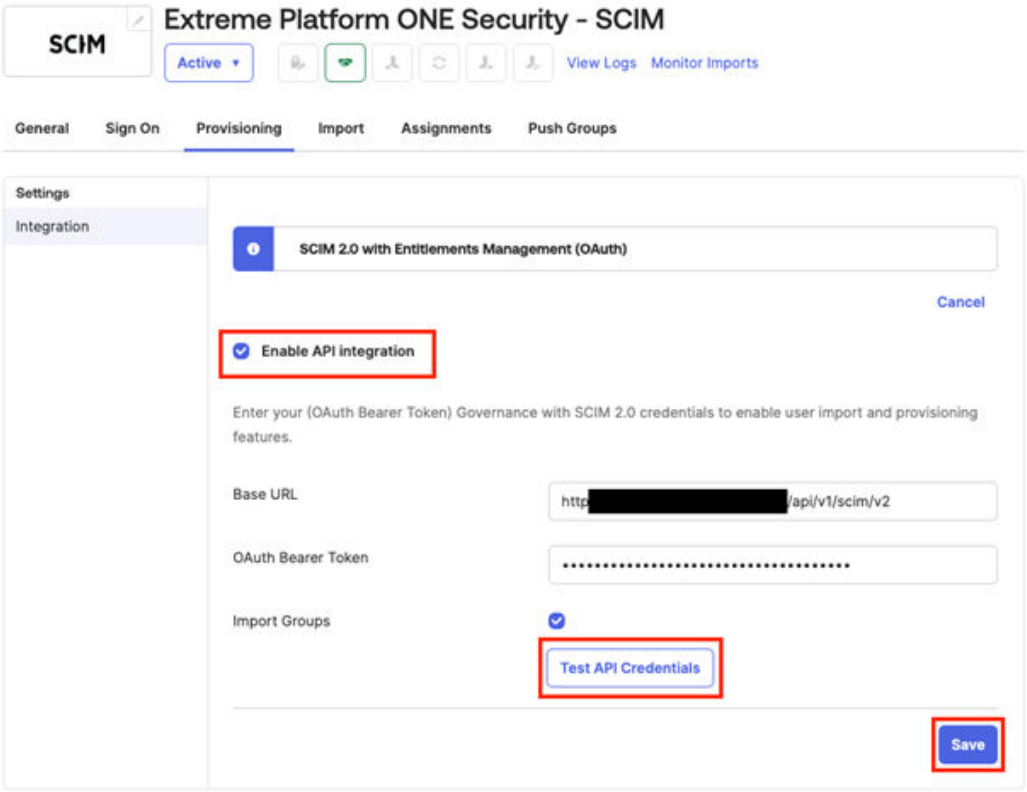


Table 131: API Integration Configuration Settings

Field	Description
Enable API Integration	Select this option.
Base URL	Paste in the Tenant URL that was saved from ExtremeCloud IQ (New).
OAuth Bearer Token	Paste the Secret Token that was saved from ExtremeCloud IQ (New).

7. Select **Test API Credentials**.

Note
If the credentials do not verify successfully, ensure there are not typos in the Tenant URL or Secret Token from the **IdP Profile** entry in ExtremeCloud IQ (New).

8. Upon successful verification, select **Save** and configure the settings in Table 132.

Table 132: API Configuration Settings

Field	Description
Create Users	Enable this option.
Update User Attributes	Enable this option.
Deactivate Users	Enable this option.

9. Select **Save**.
10. Go to **Assignments** > **Assign** and select **Assign to Groups** from the drop-down list.
11. Select **Assign** next to the groups that should be included with the synchronization into ExtremeCloud IQ (New).

    Note
    When assigning groups, do not change any defaults. Once you have selected the assign option, when prompted select **Save and Go Back**.

12. On the **Push Groups** tab, from the **Push Groups** drop-down list, select **Find groups by name**.
13. In the **Search** field enter the name of the group and select **Save** or **Save & Add Another** to add multiple. Repeat this action for each group that should be synchronized with ExtremeCloud IQ (New).
14. To view or change the status of the groups, go to the **Push Groups** tab. To force a push, select **Active** and select **Push now** from the drop-down list.

The users and user groups are now available in ExtremeCloud IQ (New) under **Policy** > **Users & Devices** > **Users**. If the user or group is not displayed, review errors or messages in Okta for the push failed description.

Network Access with Okta

If user-based 802.1X EAP-TTLS network authentication is going to be used with Okta, a separate application is required to be created that bypasses MFA as 802.1X does not have a native method to provide real-time multi-factor authentication prompt. This can only be done with an OpenID Connect (OIDC) Application.

Configure ExtremeCloud IQ (New) for Okta OIDC

Use this task to configure ExtremeCloud IQ (New).

1. In ExtremeCloud IQ (New), go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.
2. To create a new profile, select **Add IdP Profile** and configure the settings in Table 133.

Table 133: Okta OIDC IdP Profile Configuration Settings

Field	Description	
Set Up IdP	Select **Network Access** from the Purpose drop-down list.	
Approved Domain	If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**.	
Select Identity Provider	Select **Okta** from the Identity Provider drop-down list.	
Set Up Extreme Platform ONE Security	Client ID	Paste in the Client ID, Client Secret, and Tenant ID previously copied in Okta.
	Client Secret	
	Org Domain	

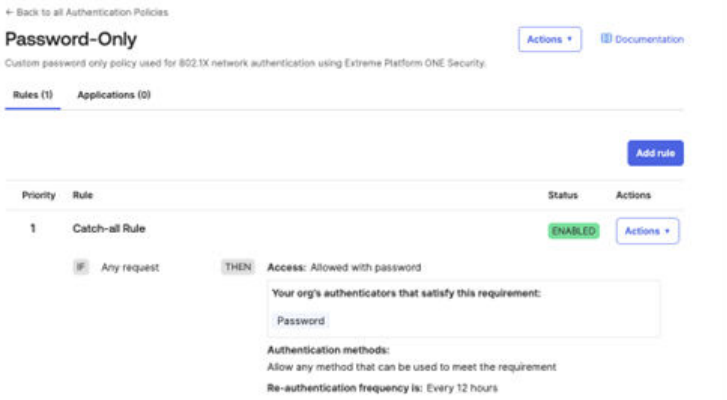
3. Select **Save**.

Configure Okta OIDC

Use this task to configure OIDC for Okta.

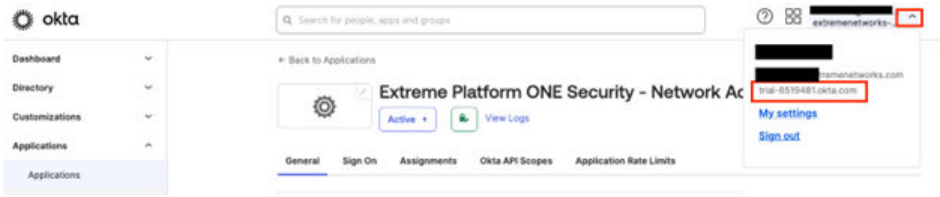
1. In the **Create a new app integration** window select **OIDC – OpenID Connect** as the sign-in method. For Application type select **Native Application** and then **Next**.
2. In **New Native App Integration** window, name the application appropriately. Under **Grant Type** select **Advanced** and under **Other Grants**select **Resource Owner Password**.
3. Within the redirect URI sections maintain default settings. Under **Assignments**, if there is a preference it can be used, however access is granted based on the policies in ExtremeCloud IQ (New). If there is no preference, under **Controlled access** select **Allow everyone in your organization to access**. Leave the checkbox for **Enable immediate access with Federation Broker Mode** enabled. Select **Save**.
4. Under **General**, under **Client Authentication** select **Client secret**. Select **Require PKCE as additional verification** and select **Save**.
5. To create a password-only authentication policy in Okta that is attached to this new application, go to **Security** > **Authentication Policies** and select **Add a policy**.
6. In the **Add Authentication Policy** window, enter a policy name and description. Select **Save**.
7. Within the Password-Only authentication policy, under **Catch-all Rule** select **Edit** from the **Actions** drop-down list.
8. Within the **IF** section maintain default settings. Under **THEN** update the **User must authenticate with** to **1 factor type - Password** from the drop-down list and select **Save**.

   Once saved, the Authentication Policy should look similar to below:



9. Go to **Applications**, select the Network Access Application previously created and do the following:
   a. Under **Sign One** > **User authentication** select **Password-Only** from the **Authentication policy** drop-down list.
   b. Select **Save**.
   c. Under **General** copy the generated Client ID and Client Secret.

10. If the Org Domain of the Okta tenant is required, select **Profile** and copy the tenant name.



Application Access with Okta

Application access for users can be authenticated via Okta in two ways: OpenID Connect (OIDC) or SAML. The setup process is different in Okta depending on the type of integration being leveraged.

Application Access using Open ID Connect (OIDC)

Prior to configuring the OIDC application in Okta, a Redirect URI will be needed from ExtremeCloud IQ (New).

1. Go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.
2. To create a new profile, select **Add IdP Profile** and configure the settings in Table 134.

Table 134: Okta OIDC Application Access IdP Profile Configuration Settings

Field	Description
Set Up IdP	Select **Application Access** from the Purpose drop-down list.
Approved Domain	If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**.
Select Identity Provider	Select **Okta** from the Identity Provider drop-down list.
Application Access	Select **OpenID Connect** from the Single Sign-On drop-down list.
Setup Redirect URIs	Copy the Redirect URI.

3. Select **Cancel**.

Configure Okta OIDC for Application Access

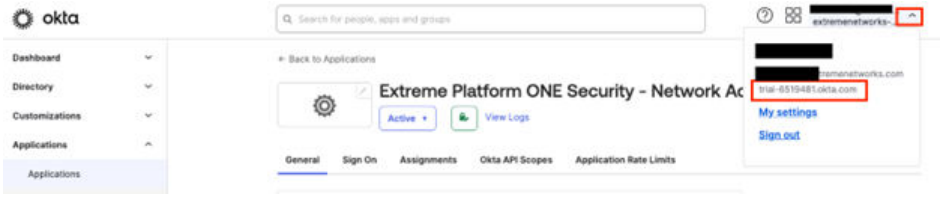
Use this task to configure Okta OIDC for Application Access.

1. In the Okta administrator portal, go to **Applications** then select **Create App Integration** and configure the settings. In the resulting window, select OIDC – OpenID Connect as the sign-in method. For **Application type** select **Web Application** and then **Next** and configure the settings in Table 135.

Table 135: Web Application Configuration Settings

Field	Description
Sign-in method	Select **OIDC – OpenID Connect**.
Application Type	Select **Web Application**.

2. Select **Next**.
3. In the **New Web App Integration** window, enter a new integration name in the the **App Integration name** field and select **Client Credentials** under **Grant Type**.
4. Under **Sign-in redirect URIs**, paste the redirect URI saved when starting to create the application in ExtremeCloud IQ (New).
5. Leave the **Sign-out redirect URIs** and **Trusted Origins** to their defaults or clear them as they are not needed.
6. Under **Assignments** if there is a preference it can be used, however access is granted based on the policies in ExtremeCloud IQ (New). If there is no preference, select the **Allow everyone in your organization to access** option under **Controlled access**. Disable the checkbox for Enable immediate access. Select Save.
7. Disable the checkbox for **Enable immediate access with Federation Broker Mode** and select **Save**.
8. Under the **General** tab, copy the generated Client ID and Client Secret.
9. If the Org Domain of the Okta tenant is required, select **Profile** and copy the tenant name.



Configure ExtremeCloud IQ (New) for Okta OIDC Application Access

Use this task to configure ExtremeCloud IQ (New).

1. In ExtremeCloud IQ (New), go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Network and Applications**.
2. To create a new profile, select **Add IdP Profile** and configure the settings in Table 136.

Table 136: Idp Profile Settings

Field	Description	
Set Up IdP	Select **Application Access** from the Purpose drop-down list.	
Approved Domain	If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**.	
Select Identity Provider	Select **Okta** from the Identity Provider drop-down list.	
Single Sign-On Method	Select **OpenID Connect**.	
Set Up Extreme Platform ONE Security	Client ID	Paste in the Client ID, Client Secret, and Tenant ID previously copied in Okta.

3. Select **Save**.

Configure Okta SAML

Use this task to configure Okta SAML.

1. In the Okta administrator portal, go to the **Applications** then select **Browse App Catalog**.

2. Search for **(OAuth Bearer Token) Governance with SCIM 2.0**. Select the app, then **Add Integration**.
3. Under **Application label** enter **Extreme Platform ONE Security – SAML** and select **Next**.
4. Under **Sign On Options**, expand the Attributes under SAML 2.0 and configure the settings in Table 137.

Table 137: SAML 2.0 Configuration Settings

Field	Description
First Name	user.firstName
Last Name	user.lastName
Email	user.email
UserName	user.username

5. Under **SAML 2.0**:
   a. Expand **Metadata details**.
   b. Copy the Sign on URL and the Issuer for use in ExtremeCloud IQ (New).
   c. Download the Signing Certificate.
   d. Under **Advanced Sign-on**, paste the copied Reply URL Advanced Sign-on Settings section, paste the Reply URL previously copied from ExtremeCloud IQ (New) into the ACS URL field and the Identifier previous copied into Audience URI field.
   e. Select **Done**.
6. Under **Assignments**, select **Assign to Groups** from the Assign drop-down list.
7. Select specific users or groups and select **Done**.

   All users are now displayed as assigned to the application.

Configure ExtremeCloud IQ (New) SAML for Okta

Use this task configure ExtremeCloud IQ (New) SAML for Okta.

1. In ExtremeCloud IQ (New), go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.
2. To create a new profile, select **Add IdP Profile** and configure the settings in Table 138.

Table 138: SAML for Okta Configuration Settings

Field	Description
Set Up IdP	Select **Application Access** from the Purpose drop-down list.
Approved Domain	If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**.
Select Identity Provider	Select **Okta** from the Identity Provider drop-down list.
Single Sign-On Method	Select **SAML**.

Table 138: SAML for Okta Configuration Settings (continued)

Field	Description	
Setup Extreme Platform ONE Security	Login URL	Paste in the Sign On URL in Okta.
	Okta Identifier	Paste in the Issuer from Okta.

3. Select **Save**.

Support Multiple IdPs

Use this task to support and prioritize multiple IdP with a single tenant.

1. Log into your ExtremeCloud IQ (New) tenant.
2. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.
3. To prioritize IdPs, select and drag the Idps in the correct order or the checkbox next to an Idp and from the select and select **Move to the top** or **Move to the bottom**from the drop-down list.
4. In the IdP Priority popup message, select **Save**.

Identity Providers | Management

You can configure one or more identity providers (IdPs) to implement role-based access and single sign-on (SSO) functionality.

An IdP profile defines how ExtremeCloud IQ (New) interacts with an external IdP for user authentication. By creating an IdP profile, you allow your system to authenticate users for the defined domain, governed by the role and site-assignment rules in the IdP profile.

The following IdPs are supported by ExtremeCloud IQ (New):

- Generic SAML Server
- Active Directory Federation Service (ADFS)
- Ping
- Okta
- Microsoft Entra ID
- OneLogin
- Auth0

From **Administration & Settings** > **Access Management** > **Identity Providers** > **Management**, you can perfom the following actions:

- Add an IdP profile to your network. See Add an Identity Provider Profile on page 365.

- Locate the IdP profile from the list, select ⋮ from the corresponding row, and then select one of the following actions:
  - **Edit**: Manage an existing IdP profile. Configure IdP Profile Settings, and then select **Save Changes**.
  - **Disable**: Disable an existing IdP profile. Select **Disable** a second time to confirm.

    Note
    Disabling an IdP profile will make it temporarily inactive.
  - **Enable**: Enable an existing IdP profile.
  - **Delete**: Delete an existing IdP profile. Select **Delete** a second time to confirm.

    Note
    Deleting an IdP profile permanently removes it from the system.

Note
As a prerequisite to adding an IdP to Extreme Platform ONE Networking, you must configure your IdP before you begin.

Add an Identity Provider Profile

You add an identity provider profile to begin the workflow that integrates an IdP with your application to enable single sign-on (SSO) authentication for your ExtremeCloud IQ (New) users. SSO authentication can be used with both IdP- and SP-initiated SSO.

Important
This task is part of a larger workflow. It is important to complete all steps in order. Skipping steps can result in incomplete configurations and require you to repeat parts of the process.

Use this task to add an IdP profile to your network.

1. Go to **Administration & Settings** > **Access Management**, and then select **Identity Providers**.
2. Select **+ Add IdP Profile**.
3. Select an IdP **Provider**, and then select **Next**.
4. Configure the following **IdP Profile Information**, and then select **Next**:
   - **Domain**: Enter a fully qualified domain name (FQDN) based on the identity provider you selected in the preceding step.
   - **Description** (optional): Enter a description of up to 64 characters.
5. Configure IdP Connection Metadata, and then select **Next**.
6. Map User Profile Attributes, and then select **Save**.
7. Export/Import SP Connections on page 369, and then select **Done** to save the IdP profile.

Related Links

Integrating with Microsoft Entra ID on page 373

Integrating with Okta on page 378

Configure IdP Connection Metadata

Identity Provider (IdP) Metadata provides structured information that is used to configure and establish a connection between an IdP and a Service Provider (SP) in a SAML (Security Assertion Markup Language) environment. This metadata includes details such as the following:

- **IdP Entity ID**: A unique identifier for an IdP used to identify the IdP to an SP.
- **SSO URLs**: Endpoints where the SP sends authentication requests.
- **Binding Methods**: Methods for communication between the IdP and SP.
- **Certificates**: Used for signing and encrypting SAML assertions.

Important
This task is part of a larger workflow. It is important to complete all steps in order. Skipping steps can result in incomplete configurations and require you to repeat parts of the process.

Metadata can be provided as a file (Import Metadata), as URL (Import from URL), or you can Enter Metadata Manually.

Import Metadata

1. Select **Import From Metadata**.
2. Select **Browse Files**, then select the metadata file from your local folder.
3. Configure any missing settings that are specific to the selected IdP. For more information, see IDP Metadata Settings Descriptions.
4. Click **Next** to map user profile attributes.

Note
If there is a problem uploading your file, check the file format and then try again. For further assistance, reach out to the Support Center.

Import from URL

1. Select **Import From URL**.
2. Type or paste an **IdP Metadata URL**, and then select **Import**.

Note
If the import was not successful, clear the URL and try again.

3. Configure any missing settings that are specific to the selected IdP. For more information, see IDP Metadata Settings Descriptions.
4. Click **Next** to map user profile attributes.

Enter Metadata Manually

1. Select **Manually Enter**.
2. Configure the IdP metadata settings that are described in IDP Metadata Settings Descriptions.

3. Click **Next** to map user profile attributes.

Table 139: IDP Metadata Settings Descriptions

Setting	Description
IdP Entity ID	The IdP unique identifier URL. URLs must begin with `https`.
SSO Binding	Select **HTTP POST** to send messages within the body of an HTTP POST request. Select **HTTP Redirect** to send encoded messages as query parameters in the URL of an HTTP GET request.
SSO URL	The endpoint where SSO authentication requests are sent. URLs must begin with `https`.
SSO Request	Select **SSO Request** to enhance SSO security. By signing the SSO request, you ensure its authenticity and integrity, confirming that it has not been tampered with.
SLO Binding	Single Logout (SLO) allows users to sign out from multiple applications or services with a single action. Select **HTTP POST** to send messages within the body of an HTTP POST request. Select **HTTP Redirect** to send encoded messages as query parameters in the URL of an HTTP GET request.
SLO URL	The endpoint where logout requests are sent to start the SLO process. This URL ensures that when a user logs out from one service, they are also logged out from all connected services. URLs must begin with `https`.
SLO Response URL	The endpoint where the Service Provider (SP) sends logout response messages after receiving a logout request from the IdP. This URL is used to confirm the completion of the SLO process. URLs must begin with `https`.
Verification Certificate	The digital certificate used to verify the authenticity and integrity of messages exchanged between the IdP and SPs. Select an existing certificate from the drop-down list, or Import a new certificate.

Import Verification Certificates

1. Select **Import Certificates**.
2. Drag and drop the certificate or browse to upload it to the **Verification Certificates** area.
3. Click **Next**.

Related Links

Add an Identity Provider Profile on page 365

Map User Profile Attributes

You must map the appropriate User Profile Attributes to the SAML Attributes sent from the IdP. These strings must be created and be in sync with both IdP and SP.

Note
To generate the SP Metadata required to complete the IdP SAML configuration, the SAML strings cannot be configured on the IdP until the ExtremeCloud IQ (New) workflow is completed. You must complete the ExtremeCloud IQ (New) workflow first. If you do not know the SAML Attribute Strings, add place holder data to save and complete the configuration.

Use this task to map user profile attributes to SAML profile attributes when you add a new IdP profile.

Important
This task is part of a larger workflow. It is important to complete all steps in order. Skipping steps can result in incomplete configurations and require you to repeat parts of the process.

1. Configure the following SAML attributes:
   - **First Name**: The URL or endpoint where the IdP provides the user's given name. For example, `https://schemas.xmlsoap.org/ws/2005/05/identity/ claims/givenname`
   - **Last Name**: The URL or endpoint where the IdP provides the user's family name or surname. For example, `https://schemas.xmlsoap.org/ws/2005/05/identity/ claims/surname`
   - **Email**: The URL or endpoint where the IdP provides the user's email address. For example, `https://schemas.xmlsoap.org/ws/2005/05/identity/ claims/surname`
   - **IdP Group**: The URL or endpoint where the IdP provides the user's group memberships. For example, `https://schemas.microsoft.com/ws/2008/06/identity/ claims/groups`

   Note
   Default SAML attributes are automatically populated based on the selected IdP type.

2. (Optional) To add a new group mapping, select **+ Add a Group Mapping** and configure the settings in Table 140. Repeat this step to add as many group mappings as needed.

Table 140: Group Mapping Settings

Field	Description
IdP Group	The IdP group name.
Primary Role	Select the **Primary Role** for this group from the list. The corresponding **Classic Role** populates based on the selected primary role.

Table 140: Group Mapping Settings (continued)

Field	Description
Classic Role	**Note:** Hover over ⓘ for information about access and access limitations for each role type. The **Primary Role** determines the scope of access for the group.
Sites	Assign site access for the group: • To give the group access to all sites, toggle the setting to **All**. **Note:** When the primary role is set to Administrator, **Sites** is set to **All** by default and cannot be modified. • To give the group access to specific sites, from the sites drop-down list, select one or more sites from the tree menu, and then select **Done**. **Note:** This feature is only available if the VIQ has created sites. If no sites have been created within the VIQ, the default VIQ site is assigned to the IdP group.
• Select 🗑 to delete a group map. • Select ⠿ and drag the row to reorder the group mappings. The first group that the user matches the rule, in the order, the process stops. Rules are enforced top down. Once a user is in the first group in a rule, the remaining groups in that rule are ignored for that user.	

3. When there is no available group map, select one of the following options to define ExtremeCloud IQ (New) behavior:
   a. **Deny user login**: Restrict user login access.
   b. **Allow user login and assign a default role and sites**: Assign user roles and site access permissions. See Group Map Settings.
4. Select **Save** to Export/Import SP Connections on page 369.

Related Links

Add an Identity Provider Profile on page 365

Export/Import SP Connections

After mapping user profile attributes, export the SP metadata and import it to the IdP to complete the configuration.

Important
This task is part of a larger workflow. It is important to complete all steps in order. Skipping steps can result in incomplete configurations and require you to repeat parts of the process.

Use this task to export or import SP connections.

1. Obtain SP connection information:
   - Select **Download SP Metadata** for IdPs that support Metadata files.
   - To manually add SP metadata into the IdP, copy the URL to your clipboard, and then paste it into your IdP. Repeat this process for each URL.
   - Select **Download Signing Certificate** to acquire the signing certificate.
2. Select **Done**.

Related Links

Add an Identity Provider Profile on page 365

Manage IdP Profile Settings

Field	Description
Purpose	Defines the purpose of the IdP within your network.
Last Updated	Indicates the last time the IdP profile was updated.
Configuration Status	The configuration status of the IdP profile.
Disable	Select to disable the IdP profile. Select **Disable** a second time to confirm. **Note:** Disabling an IdP profile will make it temporarily inactive.
Enable	Select to enable the IdP profile.
Delete	Select to delete the IdP profile. Select **Delete** a second time to confirm. **Note:** Deleting an IdP profile permanently removes it from the system.

IdP Profile Information

Field	Description
Domain	The domain used by the IdP to manage and authenticate user identities.
Description	A brief summary of the IdP profile.

IdP Connection

Field	Description
IdP Entity ID	The IdP unique identifier URL. URLs must begin with `https`.
SSO Request	Select **SSO Request** to enhance SSO security. By signing the SSO request, you ensure its authenticity and integrity, confirming that it has not been tampered with.

Field	Description
SSO Binding	Select **HTTP POST** to send messages within the body of an HTTP POST request. Select **HTTP Redirect** to send encoded messages as query parameters in the URL of an HTTP GET request. Data is visible in the URL and is limited by the maximum URL length supported by browsers and servers.
SSO URL	The endpoint where SSO authentication requests are sent. URLs must begin with `https`.
SLO Binding	Single Logout (SLO) allows users to sign out from multiple applications or services with a single action. Select **HTTP POST** to send messages within the body of an HTTP POST request. Select **HTTP Redirect** to send encoded messages as query parameters in the URL of an HTTP GET request.
SLO URL	The endpoint where logout requests are sent to start the SLO process. This URL ensures that when a user logs out from one service, they are also logged out from all connected services. URLs must begin with `https`.
SLO Response URL	The endpoint where the Service Provider (SP) sends logout response messages after receiving a logout request from the IdP. This URL is used to confirm the completion of the SLO process. URLs must begin with `https`.
Verification Certificates	The digital certificates used to verify the authenticity and integrity of messages exchanged between the IdP and SPs. Select **Show Certificates** to view valid certificates. To update the verification certificates for this IdP profile, select **Manage Certificates**. For more information, see Manage IdP Profile Certificates.

Attribute Mapping

Field	Description
First Name	The URL or endpoint where the IdP provides the user's given name.
Last Name	The URL or endpoint where the IdP provides the user's family name or surname.
Email	The URL or endpoint where the IdP provides the user's email address.

Field	Description
Group	The URL or endpoint where the IdP provides the user's group memberships.
Group Mapping	Specifies how group names from the IdP are translated, or mapped, to the corresponding group names in ExtremeCloud IQ (New): • Select **Add a Group Mapping** to add a new group map row. • Select the **IdP Group**, **Primary Role**, **Classic Role**, and **Site(s)** for each group name map. For more information, see Group Map Settings. • Select to delete a group map. • Select and drag the row to reorder the group mappings. The first group that the user matches the rule, in the order, the process stops. Rules are enforced top down. Once a user is in the first group in a rule, the remaining groups in that rule are ignored for that user. Determine what action ExtremeCloud IQ (New) should take when there is no available group map: • **Deny User Login**: Restrict user login access. • **Allow user login and assign a default user group**: Assign user roles and site access permissions. For more information, see Group Map Settings.

Extreme Cloud(SP) Connection

To obtain SP connection information:

- Select **Download SP Metadata** for IdPs that support Metadata files.
- To manually add SP metadata into the IdP, copy the URL to your clipboard, and then paste it into your IdP. Repeat this process for each URL.
- Select **Download Signing Certificate** to acquire the signing certificate.

Manage IdP Profile Certificates

Identity Provider (IdP) profile certificates are essential for securing communication between the IdP and Service Providers (SPs). Properly managing these certificates is key to maintaining the integrity and trustworthiness of your Single Sign-On (SSO) environment.

From the **Certificates** window for an IdP profile, you can:

- View a list of certificates associated with the IdP profile to view details, including certificate provider, days remaining, valid from date, valid to date, and fingerprint.
- Make active certificates inactive.
- Import a new certificate to the IdP profile.

Use this task to ensure your IdP profile certificates are correctly configured and up-to-date.

1. Go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Management**.
2. Locate the IdP profile from the list, select ⋮ from the corresponding row, and then select **Edit**.
3. Expand **IdP Connection**, and then select **Manage Certificates**.
   a. To add a new certificate, select **Import New Certificate**, and then select **Browse Files** to browse to your local folder and select the certificate.
   b. To deactivate a certificate, select ⋮, and then select **Make Inactive**.
   c. To delete a certificate, select ⋮, and then select **Delete**.

   Note
   If only one certificate is listed, you cannot delete the last valid certificate.

4. Select **Certificates for** the IdP you selected to return to the **Management** IdP profile list.

Integrating with Microsoft Entra ID

1. Create a New Enterprise Application in Entra ID:
   a. From the Azure Portal, under **Azure services**, select **Enterprise applications**.
   b. From the Enterprise Applications, select **New application** > **Create your own application**.

      The **Create your own application** dialog displays.
   c. Provide the application name, select **Integrate any other application you don't find in the gallery (Non-Gallery)**, and then select **Create**.

      The application **Overview** page opens.
2. Assign Users and Groups in Entra ID:

   Important
   User groups must be created in the IdP before you can map the user roles in ExtremeCloud IQ (New).

   a. From the application **Overview** page, select **Assign Users and Groups**, and then select **Add user/group**.

      The **Add Assignment** page opens.
   b. From the left pane, select the link under **Users and groups**.

      Azure displays ExtremeCloud IQ (New) required user group.

c. Select the check box for each ExtremeCloud IQ (New) required user group, and then click **Select**.

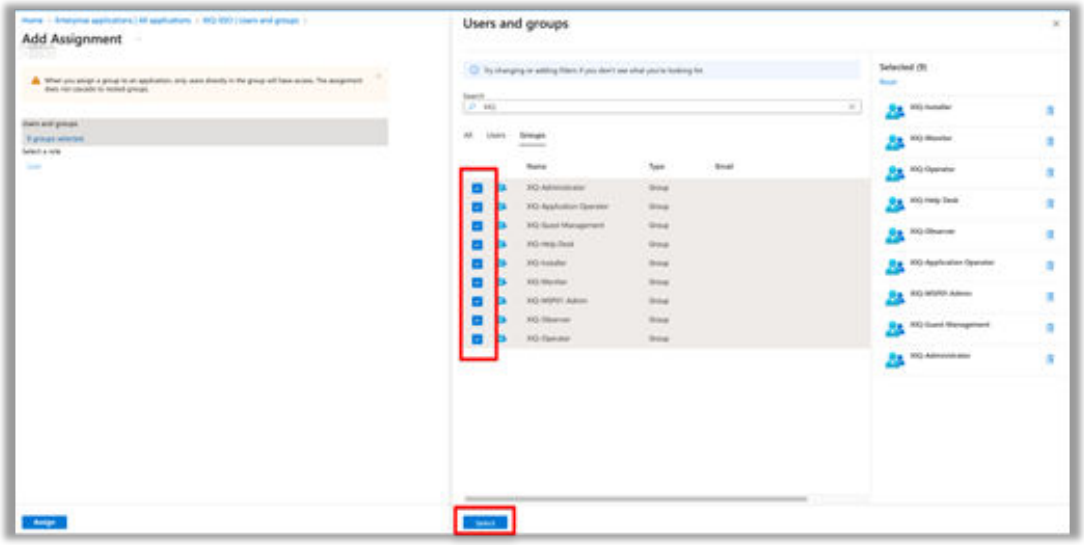


Figure 11: Azure - Assigning ExtremeCloud IQ (New) User Groups to an Azure User Role

d. Select **Assign**.

The selected groups are mapped to the selected role. Azure displays the selected groups on the **Users and Groups** page.

Note
Only users assigned to the defined groups have access to the defined roles in ExtremeCloud IQ (New).

3. Select SAML as the Single Sign-On Method in Entra ID:
   a. From the application **Overview** page, navigate to **Manage** > **Single sign-on**, and then select **Get Started**.
   b. Select the **SAML** single sign-on method.
   c. On the **Set Up Single Sign-On with SAML** page, from the **Basic SAML Configuration** section, select **Edit**.
   d. For **Identifier (Entity ID)**, select **Add identifier** and provide a temporary URL.

   For example: `https://temp_ID`
   e. For **Reply URL (Assertion Consumer Service URL)**, select **Add reply URL** and add a temporary reply URL.

   For example: `https://temp_reply`
   f. Select **Save**.

4. Import Entra ID Metadata to Extreme Platform ONE Networking:

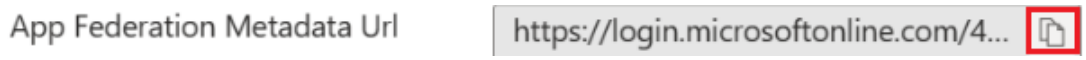
   To see Identity Provider (IdP) profile settings, log in to ExtremeCloud IQ (New) using the Global Data Center (GDC) SSO URL. For example, `https://extremeplatformone.com`.

   Note
   Single Sign-on integration can only be configured by ExtremeCloud IQ (New) users with Administrator permissions in their home account (VIQ). External administrators cannot access the IdP profile configuration page when administering other customer accounts.

   a. From *ExtremeCloud IQ (New)*, go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Management**.
   b. Select **Add IdP Profile**.
   c. Select the **Microsoft Entra ID** provider, and then select **Next**.
   d. Enter the Fully Qualified **Domain** name of the Azure Tenant and optional **Description**.

      Note
      You can only define a single domain name per IdP Profile. If your IdP supports multiple domains, you must create a separate IdP Profile for each domain.

   e. Select **Next**.
   f. Select **Import From URL** to import the data from the App Federation Metadata URL.
   g. From the *Azure Enterprise Application*, scroll down to Section 3: SAML Certificates, and select the **App Federation Metadata Url** copy to clipboard icon.

   h. In *ExtremeCloud IQ (New)*, paste the URL string into the **Enter URL** field, and then select **Import**.

      After importing, the fields in the **IdP Connection** tab display automatically including the Verification Certificate.
   i. Select **Next**.

5. Map Extreme Platform ONE Networking User Profile Attributes to SAML Attributes for Entra ID:

   In *ExtremeCloud IQ (New)*, you must map the appropriate **User Profile Attributes** to the **SAML Attributes** sent from the IdP. For more information, see Map User Profile Attributes on page 367.

Table 141 includes the required strings for integration with Entra ID.

Table 141: ExtremeCloud IQ (New)- Required Strings for Microsoft Entra

User Profile Attribute	SAML Attribute
First Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
Last Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
Email	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/email
Group	http://schemas.microsoft.com/ws/2008/06/identity/claims/groups

6. Map Extreme Platform ONE Networking Group to Roles for Entra ID:

   ExtremeCloud IQ (New) roles must be mapped based on the user group membership that is created in Entra ID to enforce authorization.

   In ExtremeCloud IQ (New), enter the exact **IdP Group** name from Entra ID (for example, EP1-Operator), and then select the corresponding role. For more information, see Add a Group Mapping.

   Important
   The Operator, Monitor, Help Desk, Installer, or Observer RBAC roles require the definition of one or more sites to gain visibility over managed devices. In the rule definition for those roles, specify one or more sites in the rules. Failure to do so will lead to the administrator being unable to view any devices after login. Administrator and Guest Management roles do not leverage sites, and will ignore any site definition in the rule.

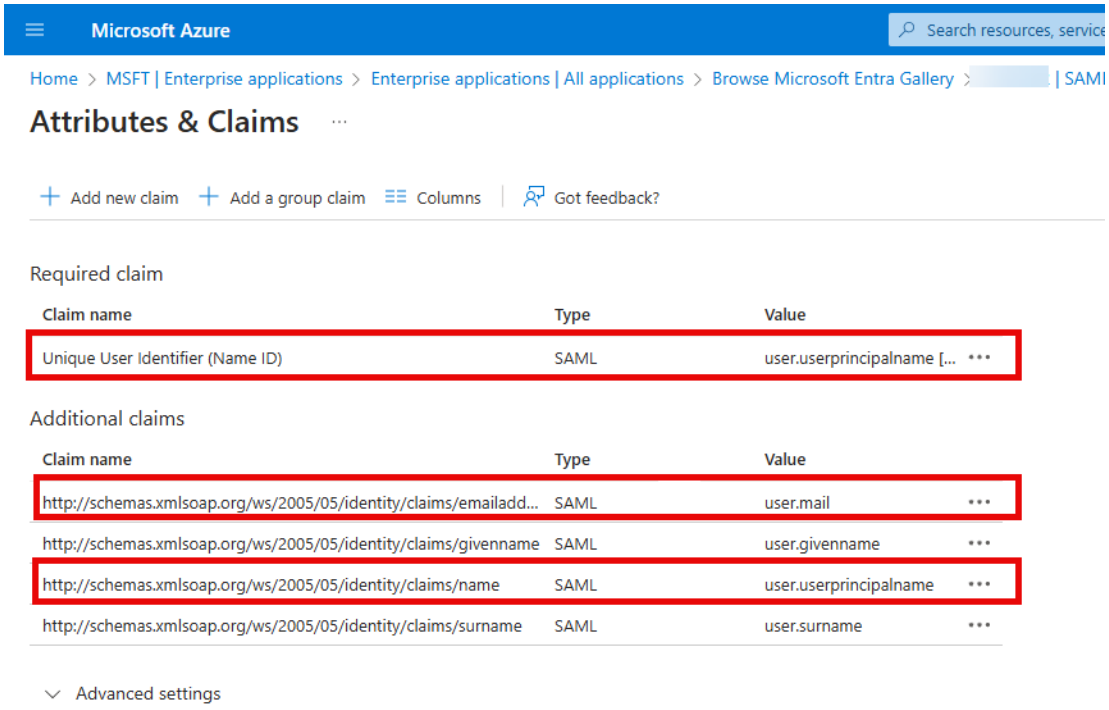
7. Export SP Metadata and Import into Entra ID:
   a. After saving the completed **Add IdP Workflow** in *ExtremeCloud IQ (New)*, download the SP metadata. For more information, see Export/Import SP Connections on page 369.
   b. In the *Microsoft Azure* application, on the **SAML-based Sign-on** page, select **Upload metadata file**, navigate to the saved exported file from ExtremeCloud IQ (New), and then select **Add**.
   c. Confirm that the imported data is correct, and then select **Save**.

      Note
      When prompted to test the application, select **No I'll test later**.

8. Map Entra ID Security Groups to Extreme Platform ONE Networking Roles:

   Configure the SAML attribute strings required to map the Entra ID security groups to the ExtremeCloud IQ (New) Role-Based Access Control (RBAC) roles for authorization.

   a. In the *Microsoft Azure* application, in Section 2: **Attributes & Claims**, select **Edit**.
   b. Under **Additional Claims**, perform the following steps to adjust the default claims:
      i. Select the **Unique User Identifier (Name ID)** row, change the **Value** field to `user.mail`, and then select **Save**.
      ii. In the **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress** row, select ••• , and then select **Delete**.
      iii. Select the **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name** row, change the **Name** field to `email`, and then select **Save**.



   c. To add a group claim, from the Attributes and Claims page, select **Add a group claim**.
   d. Select **Groups assigned to the application**.
   e. From the **Source attribute** list, select **Cloud-only group display names**.

9. Entra ID Test - SP Initiated:

   a. Browse to the **GDC Login** page `https://extremeplatformone.com`, and then select **Log In with SSO**.
   b. Enter the email address of the IdP account and complete the IdP login process.

      The browser is redirected to the Microsoft Login Portal. After a successful sign in, the browser redirects to the ExtremeCloud IQ (New) default view. The ExtremeCloud IQ (New) Audit Logs include the login action.

10. Entra ID Test - IdP Initiated:

    After the integration is complete, test the application.

    a. Go to the Azure main Single Sign On page for the XIQ-SSO application.
    b. Scroll down to the **Test single sign-on with XIQ-SSO** section, and then select **Test**.
    c. Select **Test sign in**, and then sign in to the Microsoft Login Portal.

       After a successful login, you are redirected to the ExtremeCloud IQ (New) default view. The ExtremeCloud IQ (New) Audit Logs include the login action.

Integrating with Okta

1. Navigate to the Okta Admin Portal:
   a. Browse to `https://login.okta.com`, and then log in to your Okta Organization with an account with the necessary Administrator permissions to create user, groups, SAML applications, and Authentication Policies.
   b. From the Okta Dashboard page, select **Admin**.

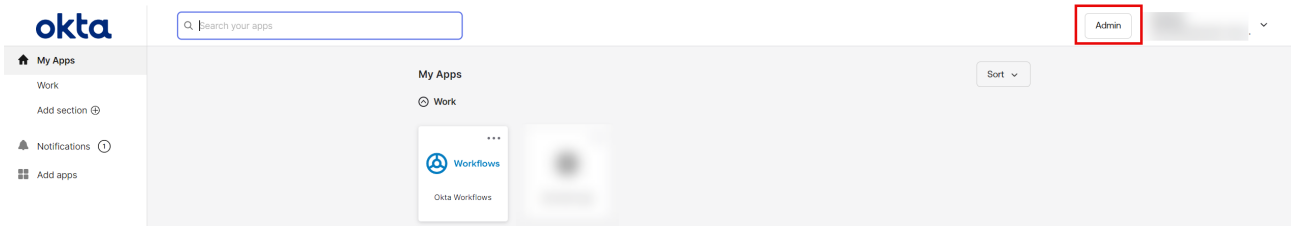


Figure 12: Okta - Dashboard and Link to the Admin Portal

2. Create a New SAML Application and Define User Group Mappings in Okta:

   Note
   You must create the user groups in the IdP before you can map the user roles in ExtremeCloud IQ (New).

   a. From *Okta*, navigate to **Applications** > **Applications**, and then select **Create App Integration**.
   b. Select **SAML 2.0**, and then select **Next**.
   c. Enter an **App name**, and then select **Next**.
   d. In the **SAML Settings** section, enter temporary URLs as a placeholder that will be updated later for the following fields:
      - **Single sign-on URL**: `https://replaceme`
      - **Audience URI (SP Entity ID)**: `https://replaceme`
   e. Scroll down to the **Attribute Statements** section.
   f. Set **Name** to `user.email` and the corresponding **Value** to `user.email`, and then select **Add Another**.
   g. Set **Name** to `user.firstName` and the corresponding **Value** to `user.firstName`, and then select **Add Another**.
   h. Set **Name** to `user.lastname` and the corresponding **Value** to `user.lastname`.

i. Scroll down to the **Group Attributes** section:
   i. Set **Name** to `user.group`.
   ii. Set the corresponding **Filter** to `Matches regex`, and then set the **Value** to `.*` (a period followed by an asterisk).
j. Select **Next**.
k. On the **Help Okta Support understand how you configured this application** page, set **App Type**, and then select **This is an internal app that we have created**.
l. Select **Finish**.

3. Assign Users and Groups in Okta:
   a. Select the **Assignments** tab.
   b. Select **Assign**, and then select **Assign to Groups**.
   c. For each group you want to permit authentication to ExtremeCloud IQ (New) with SSO login, select **Assign** next to the Group Name.

      Note
      For each group that you permit, ensure the Group is set to **Assigned**.

   d. Select **Done**.
4. Create New Password Authentication Policy in Okta:

   When a user logs in to ExtremeCloud IQ (New) using SSO with Okta, the user must follow the rules defined in the Okta Authentication Policy. You can assign your new SAML application to use one of Okta's out-of-the box Authentication policies. By default, your SAML application uses the **Any Two Factors** Authentication Policy, which has been successfully tested with ExtremeCloud IQ (New).

   a. From the **Navigation Pane**, go to **Security** > **Authentication Policies**, and then select **Add a policy**.
   b. Enter a **Name**, and then select **Save**.

      You will be directed to the Rules tab of your new Authentication Policy, where we will modify the rules associated with the existing Catch-all Rule policy.
   c. For the **Catch-all Rule**, select **Actions**, and then select **Edit**.
   d. Scroll down to the **Then** section, for **AND User must authenticate with**, select **Password** from the list.
   e. For **Prompt for authentication**, select **Every time user signs in to resource**.
   f. Select **Save**.
   g. Select the **Applications** tab, and then select **Add app**.
   h. Find the SAML Application you created in Step 2, and then select **Add** for the associated row.
   i. Select **Done** to close the app assignment dialog box.
5. Export Metadata for your Okta SAML Application:
   a. From the **Navigation Bar**, go to **Applications** > **Applications**.
   b. Select the SAML Application you created in Step 2, and then select the **Sign On** tab.
   c. In the **Metadata Details** section, you will see the **Metadata URL**. Select **Copy** and retain the URL for use in the next step.

6. Create IdP Profile, Import Metadata, and Edit Settings in Extreme Platform ONE :

   Note
   Single Sign-on integration can only be configured by ExtremeCloud IQ (New) users with Administrator permissions in their home account (VIQ). External administrators cannot access the SSO configuration page when administering other customer accounts.

   a. In ExtremeCloud IQ (New), go to **Administration & Settings** > **Access Management**, and then select **Identity Providers**.
   b. Select **+ Add IdP Profile**.
   c. From the **Provider** drop-down list, select **Okta**.
   d. Configure the following **IdP Profile Information**, and then select **Next**:
      - **Domain**: Enter a fully qualified domain name (FQDN) for which you want to provide single-sign on.
      - **Description** (optional): Enter a description of up to 64 characters.

      Note
      You can only define a single domain name per integration. If your IdP supports multiple domains, you must create a separate IdP profile for each domain.

   e. Select **Import from URL**.
   f. In the **ISP Metadata URL** field, paste the URL captured in Step 5, and then select **Import**.

      After successful import, metadata from Okta displays.

      Note
      There might be some critical elements not included in the Okta metadata. If the SLO URL and SLO Response URL fields are blank, enter placeholder values in each field, which we can update in a subsequent step.

   g. To supply the placeholder values, copy the **SSO URL** and paste the value into the **SLO URL** and **SLO Response URL** fields.

h. From the **Choose Certificates** list, ensure the certificate that was included in the Metadata import is selected, and then select **Continue**.

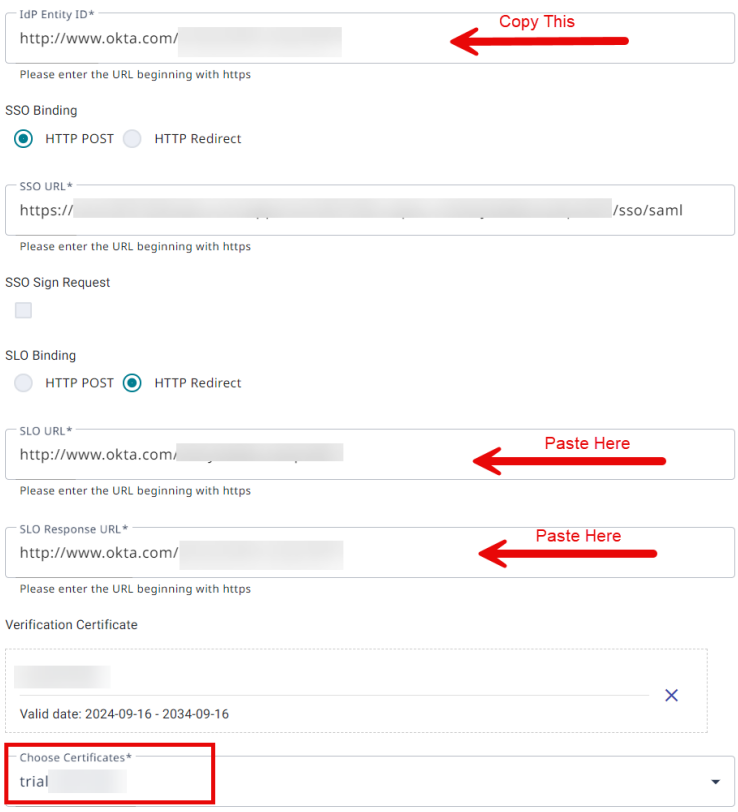


Figure 13: Extreme Platform ONE - Placeholder Values for Single Logout

i. On the **Attribute Mapping** page, enter the following values:

- **First Name**: `user.firstName`
- **Last Name**: `user.lastName`

j. Select **Add a group name mapping** for each Okta group to map to an ExtremeCloud IQ (New) role.

k. In the **IdP group** field, enter the name of your Okta group, and then select the ExtremeCloud IQ (New) role to map any users in the group.

Add additional mappings as needed.

Note
Each of the values for First Name, Last Name, and Group Name are case sensitive. Ensure that what you enter here exactly matches the information in Okta. The list is applied from top to bottom, with the first match taking precedence. If a user belongs to multiple groups listed here, they will be assigned the EP1 role based on the order you specify.

l. When there is no available group map, select one of the following options to define ExtremeCloud IQ (New) behavior:
   i. **Deny user login**: A user that successfully logs into ExtremeCloud IQ (New) with their Okta credentials, but is not in an Okta group mapped to EP1 RBAC role, is denied access to the application.
   ii. **Allow user login and assign a default role and sites**: A user that successfully logs into ExtremeCloud IQ with their Okta credentials, but is not in an Okta group mapped to XIQ RBAC role, is mapped to the role defined here. See Group Map Settings.

m. Select **Save**.

Important
The Operator, Monitor, Help Desk, Installer, or Observer RBAC roles require the definition of one or more sites to gain visibility over managed devices. In the rule definition for those roles, specify one or more sites in the rules. Failure to do so will lead to the administrator being unable to view any devices after login. Administrator and Guest Management roles do not leverage sites, and will ignore any site definition in the rule.

7. Modify Okta SAML Application Metadata with ExtremeCloud IQ (New) Settings:

   For this step, we recommend having ExtremeCloud IQ (New) and Okta open in separate tabs, as you will select data from your new IdP profile in ExtremeCloud IQ (New) and copy it over to your SAML application in Okta.

   a. In **Okta**:
      i. Browse to your Admin Portal, navigate to **Applications** > **Applications**, and then select your SAML application.
      ii. From the **General** tab, scroll down to **SAML Settings**, and then select **Edit**.
      iii. Select **Next**, and then select the **Configure SAML** tab.
   b. In **Extreme Platform ONE Networking**:
      i. From **Administration & Settings** > **Access Management** > **Identity Providers** > **Management**, in the row for your IdP profile completed in Step 6, select ⋮, and then select **Edit**.
      ii. Navigate to **Extreme Cloud (SP) Connection**, and then select **Download Certificate** to save the file to your computer.
      iii. Copy the **SP Entity ID** value from ExtremeCloud IQ (New) and copy it to the **Audience URI (SP Entity ID)** field in Okta.
      iv. Copy the **ACS URL** value from ExtremeCloud IQ (New) and copy it to the **Single Sign-On URL** field in Okta.

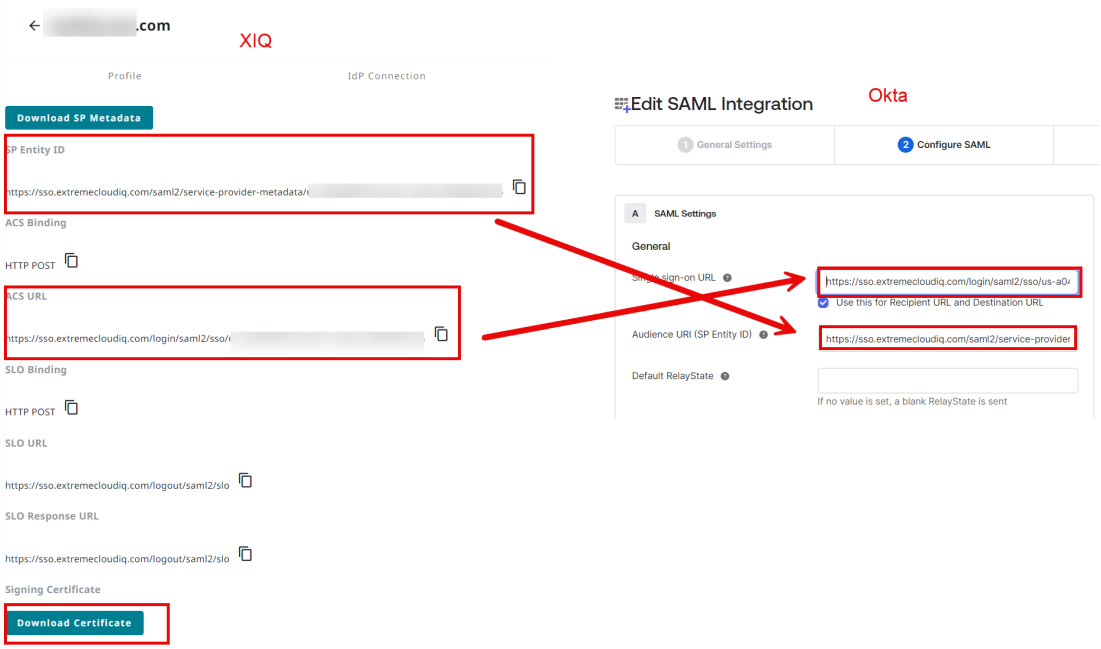


Figure 14: Okta - Replace Temporary Data for Single Sign-On URL and Audience URI

c. In **Okta**:

   i. Under **SAML Settings** > **General**, select **Show Advanced Settings**.

   ii. For **Signature Certificate**, select **Browse files**.

   iii. Select **All Files**, navigate to find the certificate file you downloaded in the previous step, select the certificate, and then select **Open** to upload the ExtremeCloud IQ (New) certificate.

   iv. Select **Enable Single Logout**.

   v. Copy the **SLO URL** value from ExtremeCloud IQ (New) and copy it to the **Single Logout URL** field in Okta.

   vi. Copy the **SP Entity ID** value from ExtremeCloud IQ (New) and copy it to the **SP Issuer** field in Okta.

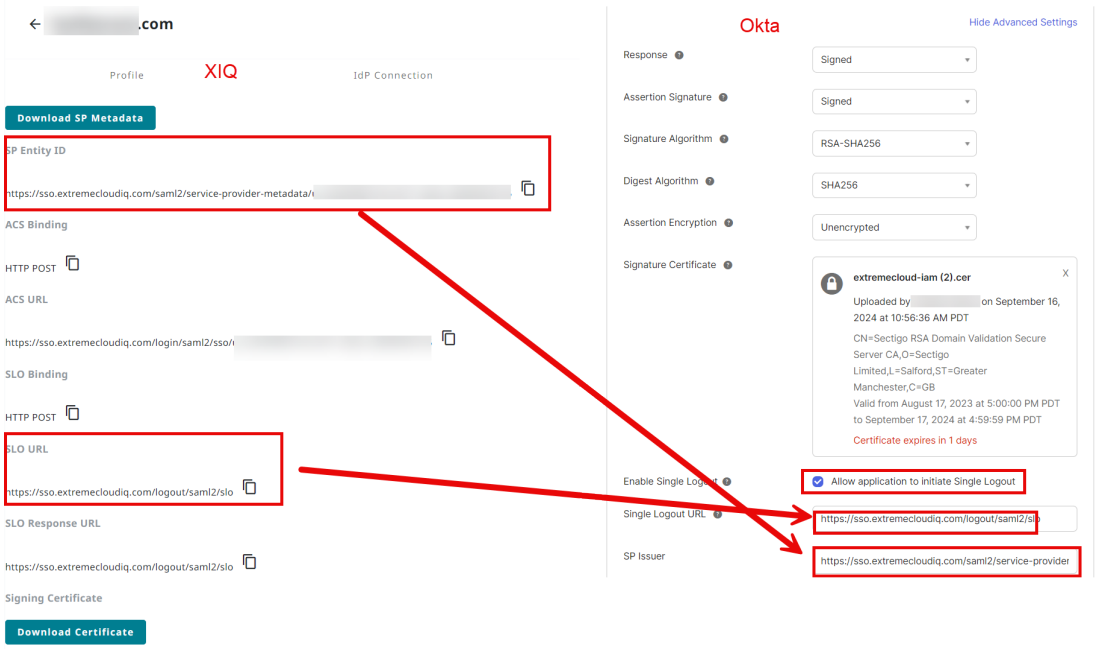


Figure 15: Okta - Single Logout Setting Definition

vii. Select **Next**, and then select **Finish**. Click to view your SAML application again.
viii. Select the **Sign On** tab, and in the **SAML 2.0** section, select **More Details**.
ix. Next to the **Single Logout URL** field, select **Copy**.

Use this URL to replace the placeholder text we submitted earlier.

d. In ExtremeCloud IQ (New):
   i. Return to the **IdP Connection** section of your IdP profile and paste that value into the **SLO URL** and **SLO Response URL** fields, replacing your placeholder values.
   ii. Select **Save Changes**.

The integration is now complete.

8. Okta Test - SP Initiated:
   a. Browse to the GDC Login page, and then select **SSO**.
   `https://extremeplatformone.com`
   b. Enter the email address of the IdP account and complete the IdP login process.
   The browser is redirected to the Okta Login Portal. After a successful sign in, the browser redirects to the ExtremeCloud IQ (New) default view.
9. Okta Test - IdP Initiated:
   After the integration is complete, test the application.
   a. Log in to your Okta Organization at `https://login.okta.com` with a user account that has been granted access to the SAML application.
   b. From the Okta Dashboard page, select your SAML application, and then from the right pane select **Launch App**.
   The browser redirects to the Okta Login Portal.

c. Enter your **Username** and **Password**, and then select **Verify**.

After a successful login, you are redirected to the ExtremeCloud IQ (New) default view.

NEW! Credential Distribution Groups

You can create credential groups in Extreme Platform ONE Networking to define access to multiple users who share similar access privileges.

NEW! *Create a New Credential Distribution Group*

Use this task to create a new credential distribution group.

1. Go to **Administration & Settings** > **Access Management** > **Credential Groups**.
2. Select **Create New Group** and configure the settings:

Table 142: Credential Distribution Group settings

Setting	Description
Group Name	(Required) Type a name for the group.
Admin Account	Required) From the menu, choose **Active Directory User** or **Guest Management Role User**.
Member of	For **Active Directory User** only: Type the name of the Active Directory user group for the account.
Guest Management User	For **Guest Management Role User** only: the system automatically specifies **Guest Management User**.
Add New Member Field (Optional)	If the account is a member of multiple groups, type the name of the first group, select **Add New Member Field**, and type the name of the next group.
Enable User Groups	To add existing user groups to this credential distribution group, select **Enable User Groups**. Then choose **Select All**, or select the check boxes for individual user groups.
Registration Operation	Select **Email Approval**.
Credential Restriction	Select **Restrict The Number of Credentials Per Employee**, and then enter the number of credentials that group members can distribute.

3. Select **Add**.

Configure the Idle Session Timeout

Use this task to specify the idle period, after which an inactive session automatically times out, for all user accounts with **Enforce Idle Session Timeout** enabled. See Create a New User on page 333.

Note
If a user account has **Enforce Idle Session Timeout** disabled, sessions for that account do not time out. To change this setting, edit the user account.

1. Go to **Administration & Settings** > **Access Management**, and then select the **Access Settings** tab.
2. Select **Timeout Duration**, and select the hour and minutes for duration from the **HH** and **MM** menus, respectively.
3. Select **Save**.

Related Links

Create a New User on page 333
Edit, Disable, or Delete a User Account on page 335

Alert Policies

Learn about Extreme Platform ONE Security alerts.

Global Policy

Use the **Global Policy** screen to enable or disable **Alert Rules**, and edit alert rule parameters.

The alert rule categories are **ExtremeCloudIQ**, **Extreme Vendor Specific**, Extreme Platform ONE Security, and **ExtremeCloud SD-WAN**. Select a rule category to see alert rules for that type. Alert rule parameters can be enabled or disabled by selecting the alert rule, then toggle the enable/disable radio button for the event or metric. To edit alert rule parameters, select for the rule.

Site Policy

Add a Site Policy

Use this task to add a site policy.

1. Go to **Administration & Settings** > **Alert Policies**, and select **Site Policies**.
2. Select **Add Site Policy**.
3. Complete the following:
   - Provide the **Alert Policy Name**.
   - Select **Sites**.
4. Select **Next**.
5. Select an **Alert Rule** and optionally edit, enable, or disable the rule parameters.

6. Select **Apply Rules**.
7. To edit or delete the site policy, from the 3-dot menu, select **Edit** or **Delete**.

External Notifications

Go to **Administration and Settings** > **External Notifications** to access the following:

- Recipients on page 387
- Rules on page 388

Recipients

Go to **Administration and Settings** > **External Notifications** > **Recipients** to do the following:

- Add Email Recipient on page 387
- Add Webhook on page 387
- Add ServiceNow Account on page 388

Add Email Recipient

Use this task to add email recipients.

1. Go to **Administration and Settings** > **External Notifications.** > **Recipients** select **Email Recipients**:
2. Type in the **Search** field to view specific email recipients.
3. Apply the following filters for email recipients:
   - All
   - Verified
   - Not Verified
4. To add a new email recipient:
   a. Select **Add Email Recipient**.

      By default, **Select All** is selected for severity, application, sites and policy drop down values.
   b. If a site-specific policy is available and a user selects **Global Policy** to generate an email notification, the system does not send a notification.

      The system only uses the site-specific policy to send notifications.
   c. If there is no site-specific policy, and a user selects **Global Policy** to generate an email notification, the system sends a notification.
   d. Select the **Enable Notifications** toggle.
   e. Select **Save**.

Add Webhook

Use this task to add Webhooks.

1. Go to **Administration and Settings** > **External Notifications.** > **Recipients** select **Webhooks**:
2. Type in the **Search** field to view specific Webhook alerts.

3. To add a webhook alert, select **Add Webhook** and configure the settings in Table 143.

Table 143: Webhook Alerts Configuration Settings

Field	Enter
POST URL	Enter a valid URL
Access Token (optional)	Provide access token details.
Sites	Select at least one site or all sites.
Applications	Select at least one application or all applications.
Severity	Select at least one severity or all severity levels.
Alert Policy	Select at least one alert policy or all alert policies.

   a. Select the **Enable Notifications** toggle.
   b. Select **Save**.

Add ServiceNow Account

Use this task to add a ServiceNow account.

1. Go to **Administration and Settings** > **External Notifications.** > **Recipients** select **ServiceNow**:
2. Type in the **Search** field to view specific ServiceNow alerts.
3. To add a ServiceNow alert, select **Add Account** and configure the settings in Table 144.

Table 144: Add ServiceNow Alerts Configuration Settings

Field	Description
ServiceNow Email	Enter a valid email address
Sites	Select at least one site or all sites.
Applications	Select at least one application or all applications.
Severity	Select at least one severity or all severity levels.
Alert Policy	Select at least one alert policy or all alert policies.

   a. Select the **Enable Notifications** toggle.
   b. Select **Save**.

Rules

Go to **Administration and Settings** > **External Notifications** > **Rules** to do the following:

- Add a Rule for Subscriptions on page 389
- Add a Rule for Contracts on page 389

Add a Rule for Subscriptions

Use this task to add a rule for subscriptions.

1. Go to **Administration and Settings** > **External Notifications** > **Rules** select **Subscriptions**:
2. Type in the **Search** field to view specific rules.
3. Select **Add Rule** and configure the settings in Table 145.

Table 145: Subscription Rule Configuration Settings

Field	Enter
Rule Name	Enter a rule name.
Applications	Select the checkboxes for the applications that apply from the drop-down menu.
Timeline Rules	Select the checkboxes for the timeline rules that apply from the drop-down menu.
Event Rules	Select the checkboxes for the event rules that apply from the drop-down menu.

4. Select **Save**.

Add a Rule for Contracts

Use this task to add a rule for contracts.

1. Go to **Administration and Settings** > **External Notifications** > **Rules** select **Contracts**:
2. Type in the **Search** field to view specific rules.
3. Select **Add Rule** and configure the settings in Table 146.

Table 146: Contracts Rule Configuration Settings

Field	Enter
Rule Name	Enter a rule name.
Timeline Rules	Select the checkboxes for the timeline rules that apply.

4. Select **Save**.

Backup & Restore

The **Backup & Restore** screen consists of the following major sections:

- VIQ Management
- Default Device Password

VIQ Management

The **VIQ Management** screen supports the following functions:

- Manually back up and restore Virtual IQ account data.
- Delete data to reset the Virtual IQ database.
- SSH Availability.

- Supplemental CLI.
- AP Out-of-the-box Wireless Onboarding.
- Import and Export VIQ data.

Use this task to manage the Virtual IQ.

1. Go to **Administration & Settings** > **Backup & Restore** > **VIQ Management**.
2. To perform a manual backup, select  , and then select **Backup VIQ**.

   To ensure data integrity, activities are suspended in the VIQ during both the backup and the restore process. When a backup is complete, the backup event is added to the Backup History table at the bottom of the page.
3. To restore a backup, choose a backup file from the **Backup History** table, and then select **Restore**.
4. To delete the VIQ database, select  , and then select **Reset VIQ**.

   This step resets the VIQ to its initial state before configuration and the addition of inventory.
5. Toggle **SSH Availability** to **ON**.

   Enabling SSH availability potentially gives others direct access to your devices while SSH access is available. While active, SSH Availability exposes your device to the public Internet through an SSH proxy, protected only by the device administrator credentials, as SSH FTP assumes that it is run over a secure channel.
6. Toggle **Supplemental CLI** to **ON**.

   Use the Supplemental CLI tool to append CLI commands to a network policy when you upload the configuration to managed devices.
7. To enable the VIQ to permit APs to respond to mesh-join requests, slide the **AP Out-of-the-box Wireless Onboarding** toggle to **ON**.

   This setting permits or prohibits AP responses to mesh-join requests. When this setting is off, the Virtual IQ prohibits managed APs from responding even if the serial number of the requesting AP is listed in the Virtual IQ.
8. To export VIQ data:
   a. Select **Export VIQ**.
   b. (Optional) Provide **Export Timeout (in minutes)**.
   c. Select **Export**.
9. To import VIQ data:
   a. Select **Import VIQ**.
   b. Select **Import VIQ from ExtremeCloud IQ**.
   c. Either drag the .tar.gz file or select **Browse Files** to navigate to the location of the file and select it.
   d. Complete the following Optional Settings:

   - Enable or disable **Resend Cloud PPSK/RADIUS password via Email/SMS**
   - Provide **Import Timeout** (in minutes)

- Instructions on handling errors during VIQ import: **Abort the import operation** or **Continue the import Operation**.
- Select **Import**.

Set Default Device Password

The device default password is applied to devices when their network policies are uploaded. Use this task to set the default device password.

1. Go to **Backup & Restore** > **Default Device Password**.
2. For **Default Password**, enter the password the administrator uses to log in to a new device.

   The password must be an alphanumeric string containing at least one number and one uppercase character, and cannot be the same as the user name or a previously used password.
3. For EXOS and VOSS switches, select **Enable device management settings for Switch Engine (EXOS)/Fabric Engine (VOSS) switches**.

   Enable this setting to set device credentials at the device level for these switch series.
4. (Optional) Select **Change Password**.

Integrations

Integrations provides administrators with tools to create and manage API keys. The **Integrations** table displays the following information for the API keys that have been added to ExtremeCloud IQ (New):

- **Name**: The name of the API key.
- **Expire At**: The expiration date of the API key.
- **Key Hash**: A partial representation of the API key used for reference without exposing the full key.
- **Description**: A short description of the API key.

To Create a New API Key on page 391, select **Create New API Key**. To edit an existing API key, select ⋮ at the end of the corresponding row, and then select **Edit Key**. To delete an API key, select **Delete Key**.

Note
Once a key is generated it cannot be modified.

Create a New API Key

Use this task to create a new API key.

1. Go to **Administration & Settings** > **Integrations** > **Create New API Key**.

2. Configure the settings in Table 147.

Table 147: API Key Settings

Field	Description
Name	A descriptive label to identify the API key.
Description	A short description of the API key.
Expiration Date	The date the API key automatically becomes inactive.

3. Select **Generate Key**.
4. Select **Copy API Key**, and then select **Close**.

Important
Make sure to copy your API key now. For security reasons, you won't be able to see it again once you close the window.

Related Links

Integrations on page 391

Logs

Use logs to detect anomalies in the system and track past activity.

Logs capture the following activities:

- **Audit Logs**
  - Administrative activity: For example, creating or deleting a user account or changing, suspending, or deleting role-based user access.
  - Data access and modification: When a user views, creates, or modifies data
  - User denials or login failures: Captures when a user is unable to login to a system due to invalid credentials or is denied access to resources such as a specific URL
  - System changes: Captures system activity. Audit logs must be compliant with all Extreme Network standards, for example, HIPPA, PCI, NIST.
- **GDPR Logs**

  The General Data Protection Regulation (GDPR) audit log displays information about download tasks performed on client data, and deletion tasks performed on user, client, and admin data to support compliance with GDPR requirements for EU citizens. Use this log to track actions that are currently being processed, that are complete, or that have failed.
- **Authentication Logs**

  The Authentication Logs table displays information about successful authentication attempts involving cloud-based PPSK and RADIUS users, and users authenticating through a cloud-hosted captive web portal using either social log in credentials or a PIN. The table includes authentication events for the time range that you define using the Start, End, and Time controls at the top of the page. Search for a specific client or user name in the Search field above the table.
- **Accounting Logs**

The Accounting Logs table displays information about cloud-based PPSK and RADIUS user sessions on your network. The table includes authentication events for the time range that you define using the Start, End, and Time controls at the top of the page. Use the Search field above the table to search for a specific client or user name.

- Event Logs

  The Event Logs table displays information about events on devices on the network.

- Security Logs

  The Security Logs table displays detailed information about security-related events within the network.

Use this task to work with logs.

1. Log into ExtremeCloud IQ (New).
2. Go to **Administration and Settings** > **Logs.**
3. Select the **Log** and **Date** and **Time** pickers to do the following:
   - View logs for up to 30 days.
   - View logs for last week, last month or last quarter.
   - Select an end time.
   - Reset to default.
   - Use arrows to select a specific month.
   - To view a logs for a specific date, select the date directly from the calendar.
4. You can also search and filter by column heading.
5. Select the **Date/Time** column to sort in ascending or descending order.
6. Select **Column** to add, hide, and reposition columns on the screen.
7. To refresh the screen and get the latest audit logs, select  .