# ExtremeIOT Essentials User Guide

Version 2.0

9037044-00 RevAA
June 2021

## Legal Notice

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

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

## Trademarks

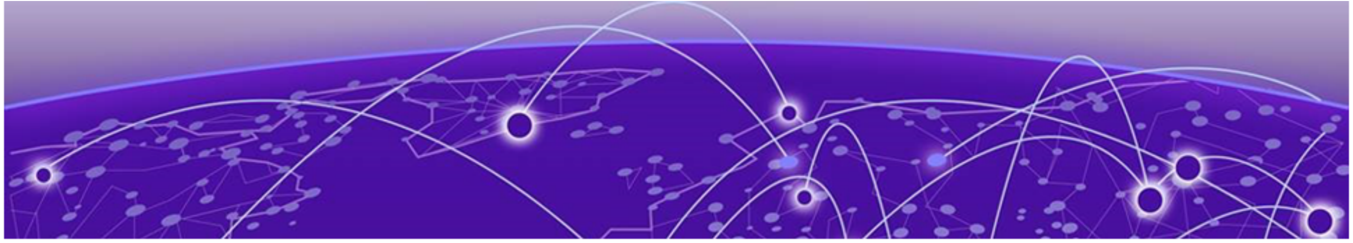
Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

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

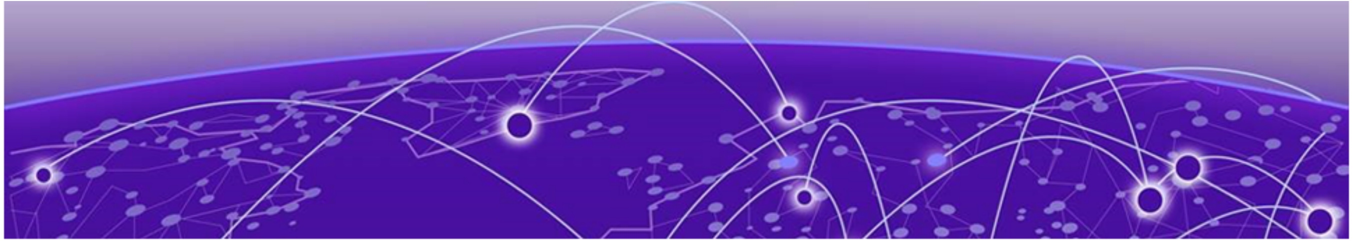
For additional information on Extreme Networks trademarks, see: www.extremenetworks.com/company/legal/trademarks

## Open Source Declarations

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



# Table of Contents



# Preface

Read the following topics to learn about:

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

## Text Conventions

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

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

**Table 1: Notes and warnings**

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

**Table 2: Text**

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

**Table 3: Command syntax**

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

## Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation

Release Notes

Hardware and software compatibility for Extreme Networks products

Extreme Optics Compatibility

Other resources such as white papers, data sheets, and case studies

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

# Getting Help

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 2826. 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.

# Providing Feedback

The Information Development team at Extreme Networks has made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you. We welcome all feedback, but we especially want to know about:

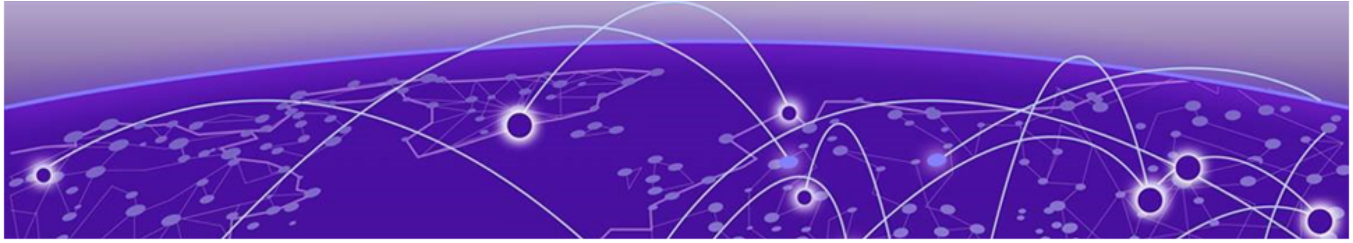
- Content errors, or confusing or conflicting information.

- Improvements that would help you find relevant information in the document.
- Broken links or usability issues.

If you would like to provide feedback, you can do so in three ways:

- In a web browser, select the feedback icon and complete the online feedback form.
- Access the feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

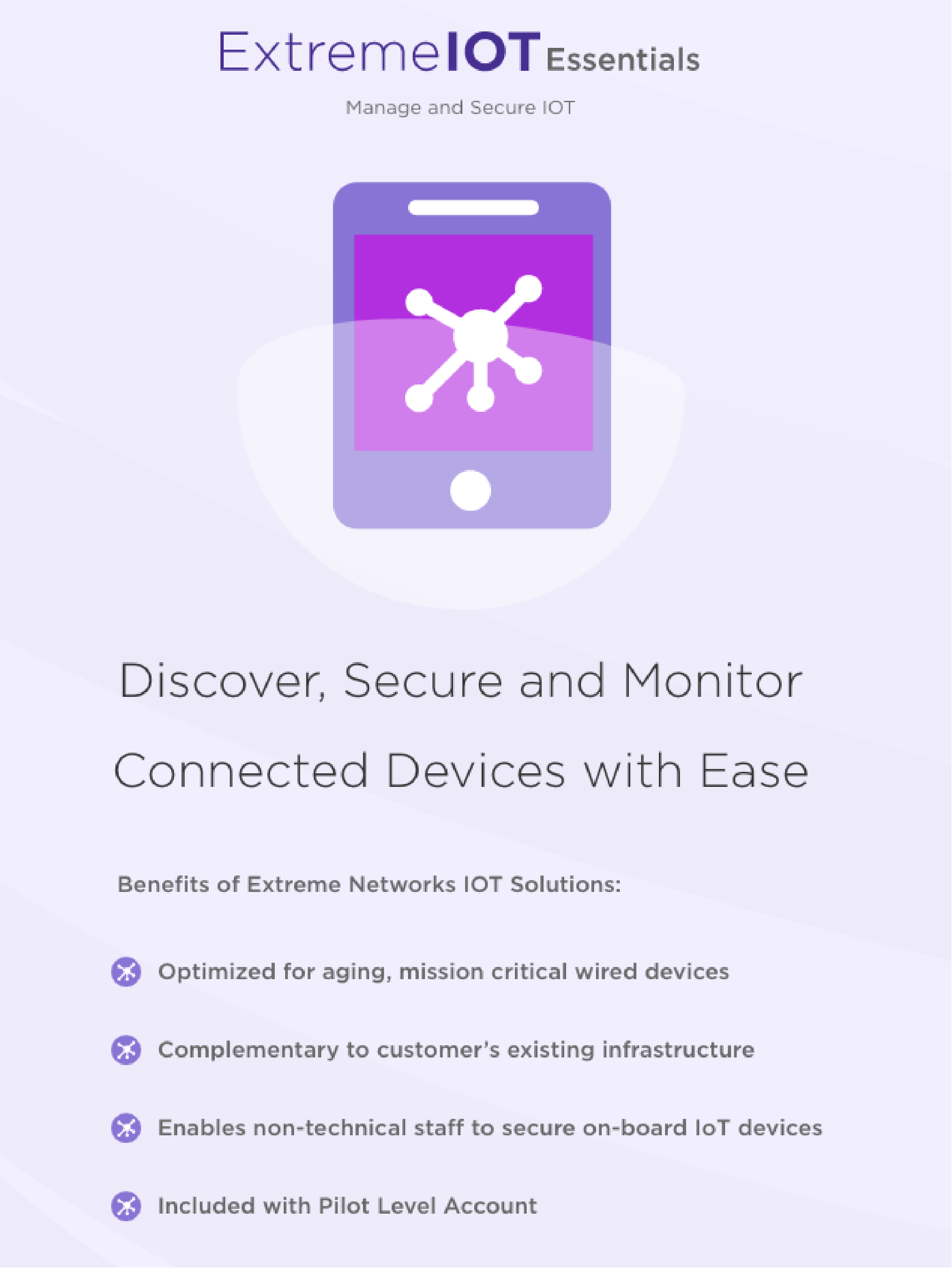
Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.



# Accessing ExtremeIOT Essentials from ExtremeCloud IQ Connect

ExtremeIOT Essentials is part of the ExtremeCloud IQ Essentials product offering that is supported with an ExtremeCloud™ IQ Pilot level account. From an ExtremeCloud IQ Connect account, select the ExtremeIOT Essentials icon to enter your Pilot subscription details or to start a 30-day trial license for a Pilot subscription. Using the 30-day trial license, you can explore the features of ExtremeIOT Essentials for 30 days.

Note
You must be an Admin user to subscribe to an ExtremeCloud IQ Pilot level account.



ExtremeIOT Essentials

Manage and Secure IOT

Discover, Secure and Monitor Connected Devices with Ease

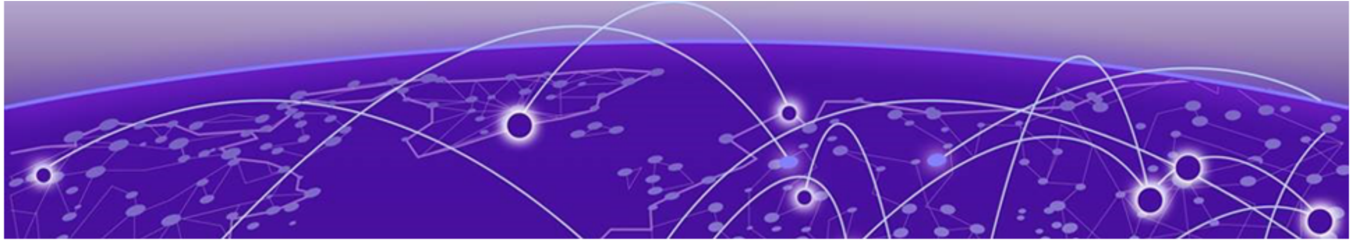
Benefits of Extreme Networks IOT Solutions:

- Optimized for aging, mission critical wired devices
- Complementary to customer's existing infrastructure
- Enables non-technical staff to secure on-board IoT devices
- Included with Pilot Level Account

**Figure 1: Subscribe to ExtremeCloud IQ Pilot**

Related Topics

ExtremeIOT Essentials on page 10



# ExtremeIOT Essentials

ExtremeIOT Essentials (ExtremeIOT) provides security management with a simplified configuration workflow, plus traffic and application visibility of connected end devices. It also enables the centralized creation of policies that define network and security settings for groups of IoT devices.

Note
ExtremeIOT is intended for the protection of wired IoT end devices. The ExtremeIOT Setup creates configuration for wired devices. However, Administrators can create additional wireless networks through ExtremeCloud IQ.

ExtremeIOT is a feature set designed to help you manage IoT devices within ExtremeCloud IQ. Configuration is simplified, stepping you through network policy configuration that is associated with the device. Your network policy includes a device template and a port type definition that both can be reused across all of your devices. The port type definition provides default deny all access to connecting clients. By default, the port type denies access to all connecting clients unless you assign clients to policy groups whose associated user profiles grant them more privileged access.

Access to ExtremeIOT functionality is dependent on your ExtremeCloud IQ user access level. The following lists the ExtremeCloud IQ access levels and describes the ExtremeIOT access permissions for each level:

- **Administrator** and **Operator** — Full administrative access to create and modify ExtremeIOT.
- **Application Operator** — Assigned to a specific ExtremeCloud IQ application. ExtremeIOT Application Operators can create and modify ExtremeIOT policy groups and assign clients to a group.
- **Monitor**, **Help Desk**, **Observer** — Read-only access to ExtremeIOT.
- **Guest Management** — Cannot access ExtremeIOT.

Note
ExtremeIOT functionality requires that you have an ExtremeCloud™ IQ Pilot license.

After onboarding your devices, select the ExtremeIOT tab or icon . You are now in the ExtremeIOT View where you can configure and manage your AP302W and AP150W devices.

The following options are available from the ExtremeIOT menu:

Dashboard

Monitor your network activity and performance on the Dashboard. The dashboard provides a graphical representation of information related to protected devices. Depending on the report, the widget represents historical data or a combination of historical and the latest data from shared memory.

Devices

List of supported ExtremeIOT access points. The ExtremeIOT view displays data for ExtremeIOT capable devices only. The AP302W and AP150W are currently supported by ExtremeIOT.

Clients

List of IoT clients attached to any of the managed devices in ExtremeIOT.

User Profiles

A user profile is a policy role that determines a client's access to the network. Define firewall rules to provide unique treatment of packet types when a user profile is applied.

Policy Groups

Policy groups map a defined user profile to a set of clients. A user profile is a set of network access services that can be applied at various points in a policy-enabled network. All clients in a policy group are subject to the rules defined in the user profile.

Related Topics

ExtremeIOT Configuration Steps on page 12

## Launching QuickStart

When you first log into ExtremeCloud IQ, the QuickStart wizard prompts you to add devices and walks you through an initial ExtremeCloud IQ configuration. It is a best practice for ExtremeIOT Administrators to skip the wizard and add devices manually.

The wizard encourages the creation of network policy for ExtremeCloud IQ, which is separate from ExtremeIOT configuration. ExtremeIOT configuration is handled within ExtremeIOT. After the ExtremeIOT Administrator adds a device, they assign it to ExtremeIOT. Assignment automates the creation of ExtremeIOT configuration through the ExtremeIOT Setup.

Note

The ExtremeIOT best practice is to add ExtremeIOT devices manually through **Quick Add Device**. Go to **Manage** > **Devices** > **Add** > **Quick Add Device**. For each AP, specify the Device Type, Device Model, and Serial Number. For more information, see Add Devices.

For detailed information about the QuickStart Wizard, see Launching the QuickStart and Device Onboarding Wizards.

## ExtremeIOT Configuration Steps

The following is the basic workflow for setting up ExtremeIOT:

Note
Users with Full Administrator access to ExtremeIOT have complete configuration capabilities. Application Operators have *restricted* access to the ExtremeIOT configuration options, and users with Monitor access have *read-only* access.

1. When you first log into ExtremeCloud IQ, the QuickStart wizard prompts you to add devices and walks you through an initial ExtremeCloud IQ configuration. It is a best practice for ExtremeIOT Administrators to skip the wizard and add devices manually.

   Initially, ExtremeIOT devices are listed under **ExtremeIOT** > **Devices** as *Unassigned*. Devices in an Unassigned state, are not being protected by ExtremeIOT.
2. To assign and configure your devices for ExtremeIOT, do one of the following:
   - From the **Actions** menu, change the ExtremeIOT status to **Assigned**
   - Run ExtremeIOT Setup on the device.

   For simplicity, a best practice is to reuse a network policy and its device template and port type definition whenever possible.
3. Configure a user profile that determines client access to the network.

   User profiles define a set of firewall rules, defined in a specific order, that determine whether client traffic is permitted or denied. By default, all traffic is denied. To allow traffic to or from a client, configure rules that allow traffic based on filter criteria.
4. Configure a policy group that includes a user profile mapping.
5. From the **Clients List**, assign a policy group to one or more clients.

   All clients in the policy group are subject to the rules defined in the mapped user profile.

Your devices and associated clients are protected by ExtremeIOT.

Related Topics

Device Actions on page 17
User Profiles on page 27
Policy Groups on page 31
Assign Client to Policy Group on page 24

## Configuring Column Display

Configure column display on a list screen. Column selection, column order, and column width are all persistent.

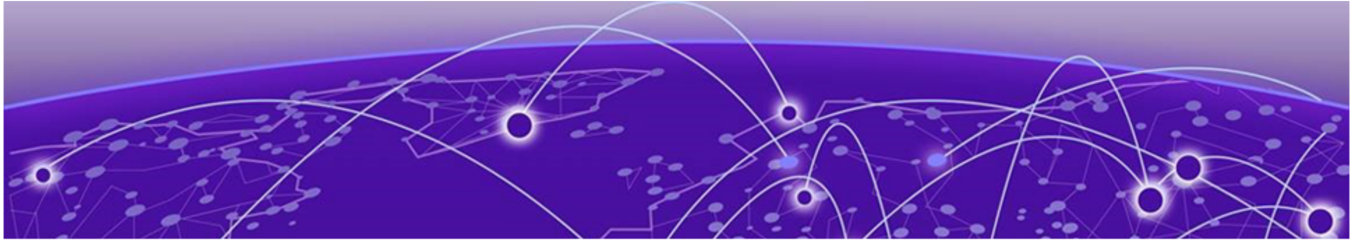
1. Select ✎ to display the list of columns.
2. Select a column to display. Or, clear the check mark to hide the column.

   Note
   To save space, some columns are hidden by default. To customize the list screen, select the columns to be displayed. Configure the AP and Client list screens to fit your needs.

3. To revert back to the default column settings, select **Clear Filter**.

   Your customized column selections are cleared and the default column selections display.
4. To customize the column order, select column headings and drag left and right.
5. To modify the column width, select the column border and drag left and right.

You can also export the data to a csv file. Select **Export all Data to CSV** or **Export Visible Data to CSV**. A spreadsheet with data is created in your Downloads folder.



# Dashboard

Monitor your client connections on the **Dashboard**. The dashboard offers a summary view of all IoT (Internet of Things) client connections. Depending on the selected time range, the widget represents historical data or a combination of historical and the latest data from shared memory.

> Note
> Dashboard statistics display for wired devices and associated clients that are managed by ExtremeIOT and meet the specified time range and filter criteria. Reports can be easily downloaded.

Select ▼ to filter the data that is displayed on the ExtremeIOT dashboard. You can filter on the following criteria:

- Client — OS Types
- Device — Network Policies
- User — User Profiles

Save your filters for repeated use.

ExtremeIOT offers a dashboard that displays the following information:

Time Range

Select a time range: **Day**, **Week**, or **Month**.

- **Day** displays data in hourly intervals. The last 1 hour, 4 hours, 8 hours, or 24 hours.
- **Week** displays data in daily intervals. The last 1 day, 2 days, or 7 days.
- **Month** displays data in larger daily intervals. The last 7 days, 14 days, 30 days, or 90 days.

The timeline appears at the top of the Dashboard. Drag the timeline handles to see data for a specific period. The data that is displayed in the timeline is automatically updated as you drag the handles.

Number of Clients

Displays the number of connected clients.

Summary: Total Application Usage

Displays application usage by device type. Select a device type to display charted usage data. Possible devices are:

- APs
- Client Devices

Top Application Groups

Displays Top Application Group with the data usage percentage associated with that Top Application Group. Also listed are the number of applications in the top group and the top application.

- To download a report, select ⤓.

### Top Applications

Displays top applications with data usage percentage and number of clients.

- Displays top 20 or top 100 depending on the selected option: **Top 20** or **Top 100**.
- To download a report, select ⤓.

### Top Usage

Displays clients, data usage, and the number of applications.

- Displays top 20 or top 100 depending on the selected option: **Top 20** or **Top 100**.
- To download a report, select ⤓.

### Wired Clients by OS

Displays data for wired clients by operating system.

- To download a report, select ⤓.

### Top Wired Clients

Displays data for wired ports, including usage and host name.

- Displays top 20 or top 100 depending on the selected option: **Top 20** or **Top 100**.
- To download a report, select ⤓.

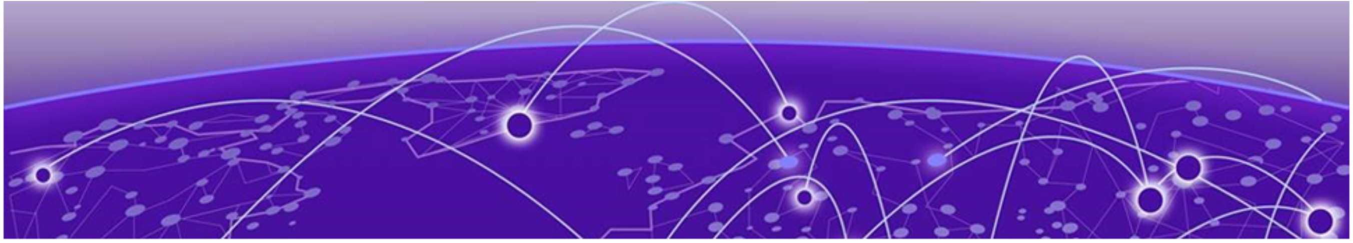
### Top Access Points by Usage or Client Count

Displays top access points based on data usage or client count.

- Select **Access Points**.
- Select **Usage** for data usage per AP.
- Select **Client** for client count per AP.

> Note
>
> - This report does not include application traffic.
> - Graphic display – Bubble size represents amounts graphically.

- To download a report, select ⤓.



# Devices

The **Device List** displays the devices that are ExtremeIOT capable. The AP302W and AP150W access points are supported by ExtremeIOT.

Highlights on the **Device List**:

- Assigned to ExtremeIOT. Indicates that a device is assigned to an ExtremeIOT network policy. Assigned devices are considered protected and all associated clients are protected by the ExtremeIOT network policy (based on your network policy configuration).

  An ExtremeIOT capable device is assigned to ExtremeIOT by assigning it an ExtremeIOT Network Policy from ExtremeIOT Settings.

  Unassigned devices have not been assigned an ExtremeIOT network policy.

  Dashboard statistics display for wired devices with the ExtremeIOT Assigned status.
- Status. Device status includes:
  - Connection Status shows the connection status of the access point indicated by the icon colors:

    ☁ indicates that there is a current connection with ExtremeCloud IQ.

    ☁ indicates that there is no current connection with ExtremeCloud IQ.
  - ✓. Configuration Audit Status indicates that the ExtremeIOT configuration is in sync with ExtremeCloud IQ.
  - ▢. Configuration Mismatch indicates that the ExtremeIOT configuration is not in sync with ExtremeCloud IQ.

    The ExtremeIOT configuration on your device must stay in sync with any ExtremeIOT configuration changes you make in ExtremeCloud IQ. Deploy the changes to the device for it to take effect. From the **Device List**, select **Update Devices**.
  - IOT indicates that this AP is managed by ExtremeIOT.
- Host Name. Displays the host name of the device.

Select this link to display device details and related statistics. For more information, see Using the Device 360 View.

- Policy. Indicates the network policy associated with this device.

  When no policy is assigned, select **Assign Policy** to display the Network Policy dialog and assign a policy.
- MAC Address. Displays the MAC Address for the device.

  Select this link to display device details and related statistics. For more information, see Using the Device 360 View.
- Location. A Location identifies a single site or multiple sites within a network, representing separate geographical locations. For example, offices in different cities or offices in different campuses within one city.

  For more information about configuring Locations, see Insights Network 360 Plan View.
- Updated On. Indicates the date and time of the last device configuration update.

  A progress status bar displays as the device is updating.
- Filter Criteria. Filter data for devices based on location, network policy, connection state, audit status, management state, ExtremeIOT state, software version, cloud configuration group and user profile.

  Filter criteria is specific to the ExtremeIOT view. If required, select **More** to see all available items, or select **Less**.

  For more information, see My Filter Side Bar.
- Assign Location. You can assign one or more devices to a floor plan after you upload or create a floor plan in ExtremeCloud IQ.
- Clients. Shows the total number of wired and wireless clients connected to the access point.

  Note
  The **ExtremeIOT** > **Clients view** only shows clients protected by ExtremeIOT.

Related Topics

Device Actions on page 17
Network Policy Settings on page 18
Update Devices on page 20
Assign Location on page 22
Configuring Column Display on page 12

# Device Actions

ExtremeCloud IQ Administrator/Operators can take the following actions against one or more devices from the **Device List**:

ExtremeIOT Setup

You can change the **ExtremeIoT Configuration** for a device in one of the following ways:

- Go to the **Policy** column of an Unassigned device and select **Assign**.
- Select a device, then select **Actions** > **ExtremeIoT Setup**.
- Go to **ExtremeIoT** > **Devices** > **Change ExtremeIoT Status** > **Assigned**.
- Go to **Manage** > **Devices** > **Assign Network Policy**, and select an ExtremeIOT network policy.

Change ExtremeIOT Status

Change a selected device status from Assigned to Unassigned. Select **Actions** > **Change ExtremeIoT Status**.

Change a selected device status from Unassigned to Assigned. Select **Actions** > **Change ExtremeIoT Status**.

Note
Unassigned devices and their associated clients are not protected by ExtremeIOT.

Assign Location

A Location identifies a single site or multiple sites within a network, representing separate geographical locations. For example, offices in different cities or offices in different campuses within one city. Configure Locations in ExtremeCloud IQ. Then, Assign a Location for the selected ExtremeIOT devices. Select **Assign** from the **Location** column, or select a device, then select **Actions** > **Assign Location**.

For more information about configuring Locations, see Insights Network 360 Plan View.

## Network Policy Settings

Assign one or more devices to an existing ExtremeIOT network policy or create a new network policy. Policy settings display when you clear the **Use Existing Policy** check box. A network policy consists of **Device Template Settings**. The **Device Template Settings** include **Wired Port Type Settings**.

Note
For simplicity, a best practice is to reuse a network policy and its device template and port type definition whenever possible.

When creating new entities, a best practice is to use a naming convention that will easily identify the purpose of a configuration entity. For example, ExtremeIOT default configuration entities are named with the following convention: `XIOT_<entity type initials>`.

Use Existing Policy

Select this option to use an existing ExtremeIOT network policy.

Select **Edit Policy** to modify the existing network policy.

Note
The edit feature is available when a template is not present.

Clear the **Use Existing Policy** option to create a new network policy.

Subsequent **Device Template Settings** and **Wired Port Type Settings** are associated with the new network policy.

Policy Name

Specify a new network policy name.

Device Timezone

Select a timezone for the new network policy. This is the timezone of the AP.

Use existing Device Template

Select this option to use an existing ExtremeIOT device template in the new network policy. Clear this option to create a new device template.

Note
When you select both AP150W and AP302W on the Device list, ExtremeIOT presents both device templates. Configure each device template respectively.

Template Name

Specify a new device template name.

Country Code

Define the regulatory country for the APs associated with the new device template. The regulatory domain of the AP must match the Country code.

Note
It is not necessary to specify a country code in regions that support a single country code (such as the United States and Canada). Customers that receive world-mode AP devices have the option to apply the appropriate country code through the device template or manually assign the country code during the onboarding process.

Use existing Port Type

Select this option to use an existing ExtremeIOT wired port type in the new device template. Clear this option to create a new wired port type.

Note
It is a best practice to use one port type for all devices when possible. However, a single port type supports up to 128 wired clients. If you have more than 128 wired clients, create another network policy, device template, and port type.

If you want to use ExtremeIOT with more than 128 wired clients, use the ExtremeIOT Setup wizard to create different configurations for different subset of devices. A wired client, when moved from one device to another, will get the same authorization settings if the devices share the same configuration.

Port Type Name

Specify a new wired port type name.

Note
The **Port Type Name** option is available only if the default **Use Existing Port Type** check box is cleared.

When you create a new port type, ExtremeIOT generates the default user profile. The user profile and its associated MAC firewall policies are aimed at denying all traffic.

- Default user profile:
  - XIOT_UP_DENY_ALL
- Default MAC firewall policies:
  - XIOT_MAC_DENY_ALL_IN
  - XIOT_MAC_DENY_ALL_OUT

Related Topics

User Profiles on page 27

### ExtremeIOT Default Configuration

The ExtremeIOT Setup walks you through configuring a network policy, device template, and wired port type definition. After you have saved the ExtremeIOT Setup, the wizard creates the following elements for specific use with ExtremeIOT:

Network Policy:

- User-specified device template
- User-specified wired port type.
  - The port type is automatically assigned to the wired interfaces (ETH1, ETH2, and ETH3) of the device template.
  - The port type does not use an authentication method.
  - The port type automatically uses the default user profile XIOT_UP_DENY_ALL, denying all traffic to and from the wired IoT device for enhanced security.

ExtremeCloud IQ Common Objects:

- User Profile
  - ExtremeIOT
    - XIOT_UP_DENY_ALL

## Update Devices

The ExtremeIOT configuration on your device must stay in sync with any ExtremeIOT configuration changes you make in ExtremeCloud IQ. Deploy the changes to the device for it to take effect. From the **Device List**, select **Update Devices**.

Note
Devices must be in Connected status to update configuration.

The following icons indicate the configuration status of an ExtremeIOT device:

- ✓. Configuration Audit Status. This icon indicates that the ExtremeIOT configuration is in sync with ExtremeCloud IQ.
- !. Configuration Mismatch. This icon indicates that the ExtremeIOT configuration on the device is not in sync with ExtremeCloud IQ. To sync the configuration with ExtremeCloud IQ, select the device and select **Update Devices**.

A best practice is to make the following configuration updates within ExtremeIOT:

- Network policy settings
- Device template settings
- Port Type settings
- User Profile settings
- Policy Group assignment

Select **Update Devices** after you modify ExtremeIOT configuration.

Although ExtremeIOT device configuration must be handled from the Network Policy Settings within ExtremeIOT, it is possible to edit certain aspects of the configuration from outside ExtremeIOT.

You can make the following changes to a network policy from outside of ExtremeIOT:

- Associate a new or existing SSID to an ExtremeIOT network policy.

  This is useful if you have existing IOT-capable devices that are already deployed and providing service. You can assign these devices to the ExtremeIOT network policy.
- Associate a new or existing port type to one or more ports of an ExtremeIOT device template.

  This is useful to support existing wired clients with more sophisticated authentication and authorization settings.

  Note
  Port type modifications outside of ExtremeIOT are limited to: name, description, port-status, default-user profile, and traffic-filter management settings. User authentication or authorization settings cannot be changed.

Select **Update Devices** after you modify ExtremeIOT configuration outside of ExtremeIOT.

Related Topics

Perform a Device Configuration Update on page 21

Devices on page 16

## Perform a Device Configuration Update

To update a device configuration:

1. Go to **ExtremeIoT** > **Devices**.
2. Select a device, then select **Device Update**.
3. Select **Update Network Policy and Configuration**, then select one of the following:
   - **Delta Configuration Update** — Update device with changed configuration.
   - **Complete Configuration Update** — Update device with all configurations. Used to reset device to ExtremeCloud IQ configuration settings.

     Caution
     When you perform a complete configuration update, the device is rebooted, impacting network service.
4. To save your update selection as the default selection, select **Save as Defaults**.

5. To update the selected devices, select **Perform Update**.

Related Topics

Update Devices on page 20

## Assign Location

You can assign one or more devices to a floor plan after you upload or create a floor plan in ExtremeCloud IQ. For more information on floor plans, see Insights Network 360 Plan View.

To assign or change the location for one or more devices:

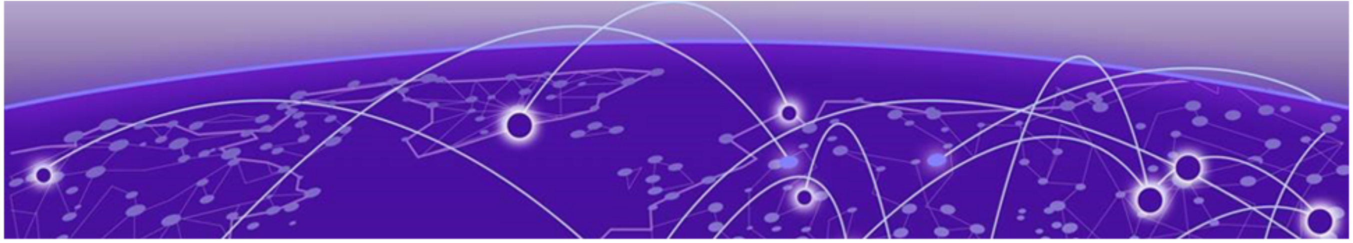
1. Go to **ExtremeIoT** > **Devices**.
2. Select one or more devices.
3. Select **Actions** > **Assign Location**.

   Or, for a single device assignment, select the **Assign** link from the Locations column for the selected device.
4. From the **Assign Devices** dialog, select the plus signs in the Global View, navigating down to the Floor Level.
5. Select a floor and select **Assign**.

   You cannot assign a device to a building directly. Instead, assign the device to a floor within the building in the hierarchy.

Related Topics

Devices on page 16



# Clients

View a list of clients that are managed by ExtremeIOT from the ExtremeIOT **Client List**. You can view clients connected in Real Time or Historical View. Real Time clients are clients currently connected to ExtremeIOT. Historical View provides information about clients connected in the past.

Clients are displayed on the Client List based on the following factors:

- Filter criteria:
  - Device Location
  - Client Operating System
  - User Profile
- Selected time range: current or historical

Only clients connected to an ExtremeIOT device are displayed here. (The port type must be ExtremeIOT defined.)

When displaying clients in **Real Time**, you can assign a client to an existing policy group. Select the check box next to the client and select **Assign Policy Group**.

When displaying The **Historical View**, select a Time Range. Valid values are:

- **Day**. List of clients connected in the last day. View data in the following hourly ranges:
  - 1 hour
  - 4 hours
  - 8 hours
  - 24 hours
- **Week**. Clients connected in the last week. View data in the following ranges:
  - 1 day
  - 2 days
  - 7 days
- **Month**. Clients connected in the last month. View data in the following ranges:
  - 7 days
  - 14 days

- 30 days
- 90 days

## Assign Client to Policy Group

Before you can assign a client to a policy group, you must configure a user profile and a policy group.

Policy groups map a defined user profile to selected clients. A user profile is a set of network access services that can be applied at various points in a policy-enabled network. All clients in a policy group are subject to the rules defined in the user profile.

To assign a policy group to one or more clients:

1. Go to **ExtremeIOT** > **Clients**.
2. Select one or more clients.
3. Select **Assign Policy Group**.
4. Select a group from the list of configured policy groups.
5. Select **Assign**.

The selected clients are now subject to the policy rules defined in the user profile that is associated with the policy group.

Related Topics

Remove Client from Policy Group on page 24

## Remove Client from Policy Group

How to remove a client from a policy group.

### Real Time View

To remove a client from a Real Time view policy group:

1. Go to **ExtremeIOT** > **Clients**.
2. Select **Real Time**.
3. Select one or more clients.
4. Select **Assign Policy Group** > **None**.

The client MAC address is removed from all port types, whether real time or historical, from all policy groups.

### Historical View

For inactive clients in the Historical view:

1. Go to **ExtremeIOT** > **Clients**.
2. Select **Historical**.
3. Select one or more clients.
4. Select **Unassign Policy Group**.

The client MAC address is removed from all port types that are no longer active from all policy groups. For greater control over specific client MAC address / port type combinations, the Administrator can manually delete them from the policy group.

Related Topics

Assign Client to Policy Group on page 24

## Client Details

To display session details about a client:

1. Go to **Clients**.
2. From the **MAC** column, select the MAC Address for the client.
3. Select a Time Range and data interval.

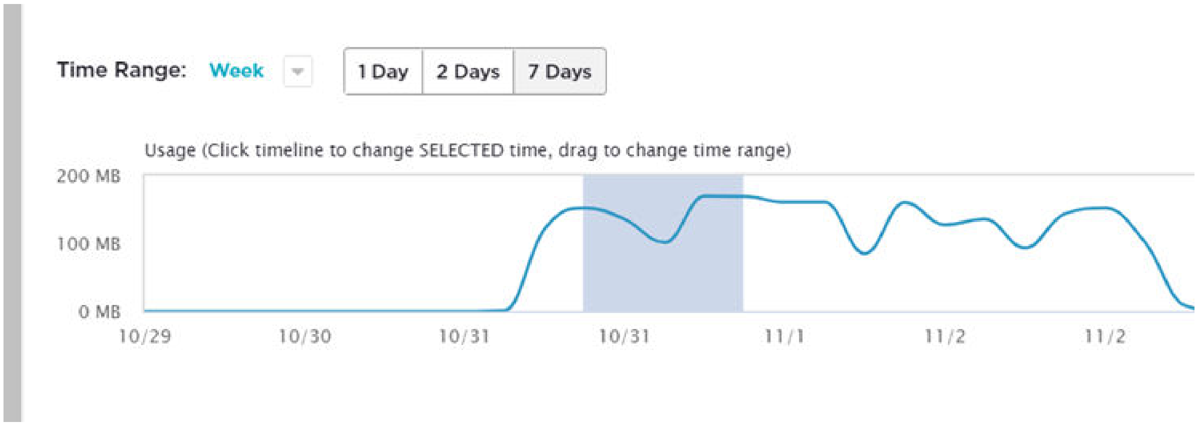


**Figure 2: Client Details Time Range**

Time Range

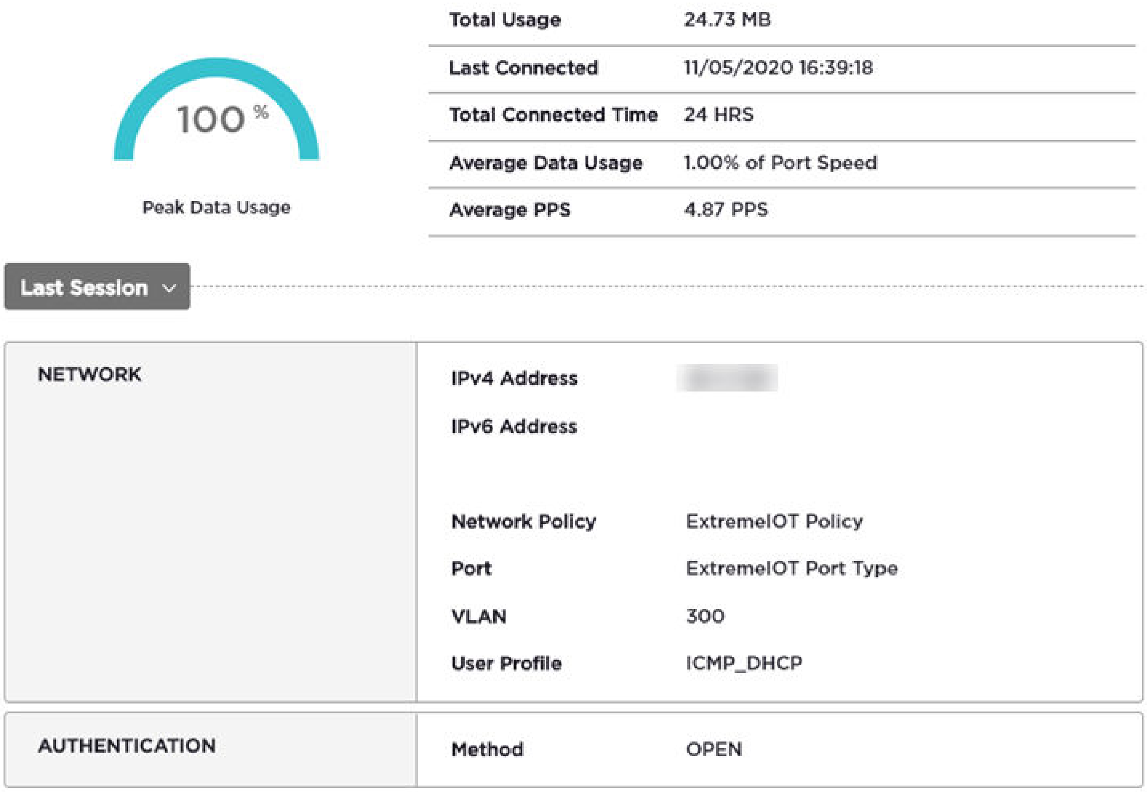
Select a time range: **Day**, **Week**, or **Month**.

- **Day** displays data in hourly intervals. The last 1 hour, 4 hours, 8 hours, or 24 hours.
- **Week** displays data in daily intervals. The last 1 day, 2 days, or 7 days.
- **Month** displays data in larger daily intervals. The last 7 days, 14 days, 30 days, or 90 days.

The timeline appears at the top of the page. Click and drag on the timeline to select a specific period. The session details that display are automatically updated as you highlight a selection on the timeline.

The following session information displays:

- Total Usage
- Last Connected
- Total Connected Time
- Average Data Usage
- Average PPS



| | |
|---|---|
| Total Usage | 24.73 MB |
| Last Connected | 11/05/2020 16:39:18 |
| Total Connected Time | 24 HRS |
| Average Data Usage | 1.00% of Port Speed |
| Average PPS | 4.87 PPS |

NETWORK

| | |
|---|---|
| IPv4 Address | [redacted] |
| IPv6 Address | |
| Network Policy | ExtremeIOT Policy |
| Port | ExtremeIOT Port Type |
| VLAN | 300 |
| User Profile | ICMP_DHCP |

AUTHENTICATION

| | |
|---|---|
| Method | OPEN |

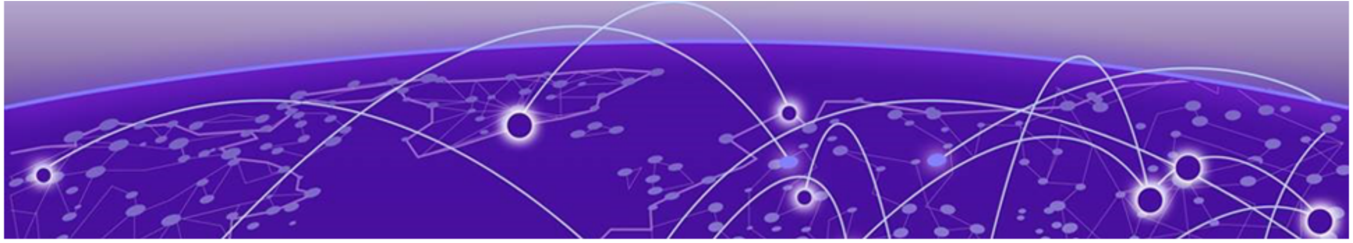
**Figure 3: Client Details**

**Last Session Details:**

- Network:
  - IPv4 Address
  - IPv6 Address
  - Network Policy
  - Port
  - VLAN
  - User Profile
- Authentication Method. All ExtremeIOT client ports are open.

Related Topics

Dashboard on page 14



# User Profiles

A user profile is a policy role that determines a client's access to the network. Define firewall rules to provide unique treatment of packet types when a user profile is applied. The default user profile for an ExtremeIOT port type is XIOT_UP_DENY_ALL, which denies all traffic to and from all connected clients. To grant clients greater network access, you need to create a user profile that allows network traffic, then associate it with a policy group assigned to the clients.

The following default profiles are available:

- ExtremeIOT
    - XIOT_UP_DENY_ALL

From the **User Profiles** page, you can add, edit, clone, and delete a profile:

- To add a user profile, select **Add** and configure the profile settings.
- To edit a user profile, select a profile from the list, then select ✎, and modify the profile settings.
- To clone a user profile, select a profile from the list, then select ⧉, and provide a name for the cloned profile.
- To delete a user profile, select a profile from the list, then select 🗑.

Related Topics

User Profile Settings on page 27

Create an Allow User Profile on page 28

## User Profile Settings

ExtremeIOT by definition, denies all traffic to protected IoT clients. The ExtremeIOT Setup wizard creates the following default user profile to protect assigned IoT devices. The default user profile includes the default firewall rules:

- Default user profile:
    - XIOT_UP_DENY_ALL
- Default MAC firewall policies:
    - XIOT_MAC_DENY_ALL_IN
    - XIOT_MAC_DENY_ALL_OUT

A best practice is to use these default policies to protect the client IoT devices.

To add a new user profile, configure the following settings:

User Profile Name

Name of the user profile.

Connect to

Connect to a VLAN or a VLAN Group. Select from the list.

- Select ☰ to select from the list.

Refer to the ExtremeCloud IQ Online Help for information about the following user profile configuration settings:

- Security
- Traffic Tunneling
- QoS
- Availability Schedule
- Client SLA
- Date/Time Limit

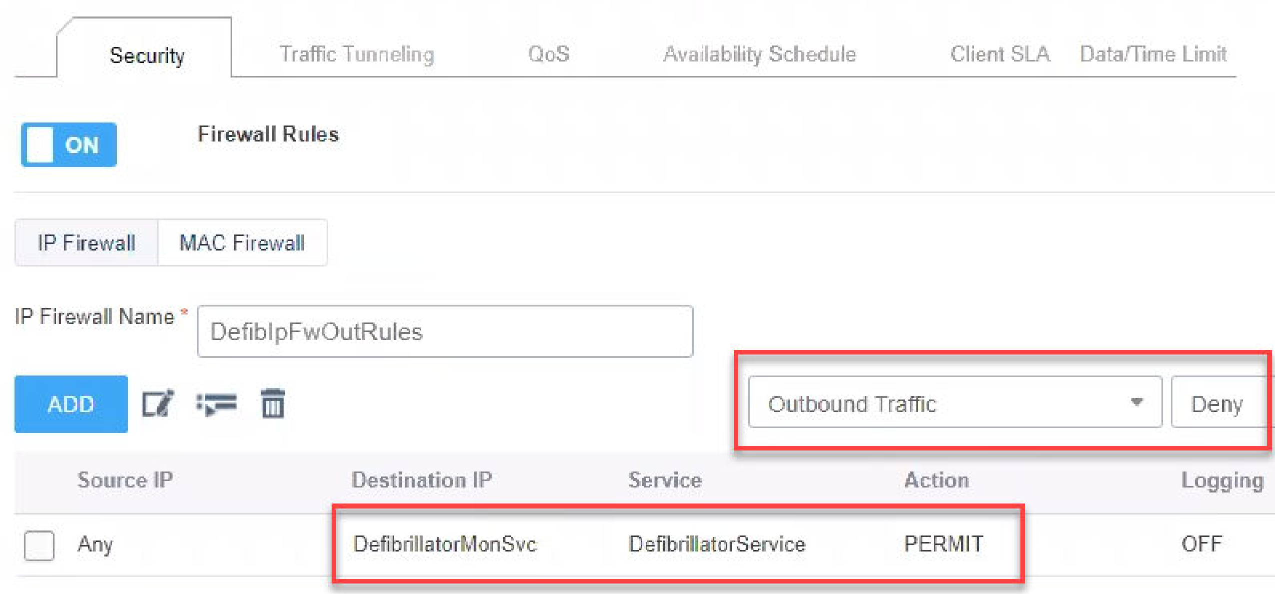
## Create an Allow User Profile

The ExtremeIOT default configuration uses a deny all user profile by default. This is to protect IoT clients from all network traffic. You may need to create additional user profiles that allow user traffic. For example, a defibrillator machine may need to allow traffic to a monitoring device.

To create a user profile that allows traffic:

1. Go to **ExtremeIOT** > **User Profiles** > **Add**.
2. Provide a Profile Name.
   - `DefibrillatorUserProfile`
3. Select the **Security** tab and select the **On/Off** button.

4. Create and IP Firewall Rule that restricts all outbound traffic except traffic destined to the defibrillator monitor service using the protocol `DefibrillatorService`.



IP Firewall Name * DefibIpFwOutRules

Outbound Traffic Deny

| | Source IP | Destination IP | Service | Action | Logging |
|---|---|---|---|---|---|
| □ | Any | DefibrillatorMonSvc | DefibrillatorService | PERMIT | OFF |

5. Select **Save User Profile**.

After you have created the user profile:

1. Create a policy group.
   a. Go to **ExtremeIOT** > **Policy Groups** > **Add**.
   b. Configure the Policy Group Name.
2. Associate the user profile `DefibrillatorUserProfile` to the policy group.
3. Assign selected clients to the policy group.
4. Deploy configuration changes to the device.

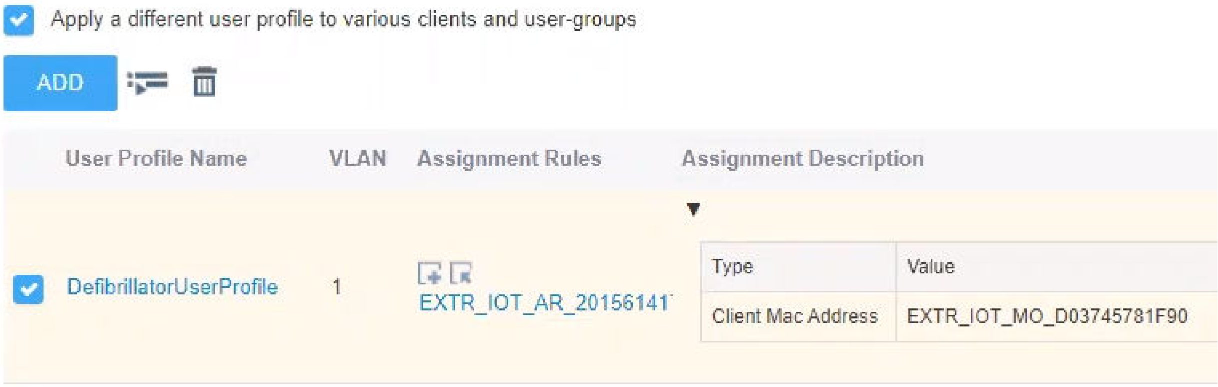
   Go to the **Devices List**, select the device, and select **Update Devices**.

After the device configuration is updated, you can verify which user profile is configured.

Go to **ExtremeIOT** > **Clients** to see the updated value in the **User Profile** column.

An Administrator can verify the user profile assignment:

1. Go to **Configure** > **Network Policies**.
2. Select the device template.
3. Under **Wired Interfaces**, select ✎ to edit the port.
4. Scroll down to the **User Access Settings**, select the **Assignment Description** field, and notice that the `DefibrillatorUserProfile` is selected for the selected client.



☑ Apply a different user profile to various clients and user-groups

| | User Profile Name | VLAN | Assignment Rules | Assignment Description |
|---|---|---|---|---|
| ☑ | DefibrillatorUserProfile | 1 | EXTR_IOT_AR_20156141 | Type: Client Mac Address<br>Value: EXTR_IOT_MO_D03745781F90 |

**Figure 4: User Profile that allows traffic**

Related Topics

- Policy Groups on page 31
- User Profiles on page 27
- Assign Client to Policy Group on page 24
- Update Devices on page 20

# Policy Groups

Policy groups map a defined user profile to a set of clients. A user profile is a set of network access services that can be applied at various points in a policy-enabled network. All clients in a policy group are subject to the rules defined in the user profile.

ExtremeIOT **Policy Groups** page displays all ExtremeIOT policy groups. You can create a new group and edit a group. You can also remove individual clients, all clients connected on a port type, or delete the group altogether.

To add a new group, select **Add** and configure the following group settings:

- Policy Group Name
- User Profile. Associate a user profile with the policy group.

> Note
> All clients associated with the policy group are assigned the specified user profile.

To edit a group, select the group and then select ✎.

To delete a group, select the group and then select 🗑.

Related Topics

Policy Group Settings on page 31

User Profile Settings on page 27

## Policy Group Settings

Configure the following policy group settings:

> Note
> ExtremeIOT Administrators can modify policy group settings.

Policy Group Name

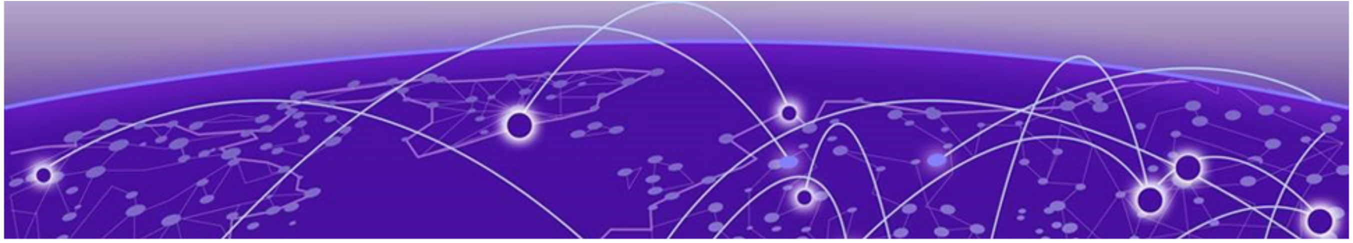
Name of the policy group.

User Profile

User profile associated with the policy group.

### Port Type to Client Mapping

Port Type for the connected client.



# Index