Extreme™
Customer-Driven Networking

Extreme Defender Application User Guide

Version 3.21

9036374-00 Rev AA

Published July 2019

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, please 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:
www.extremenetworks.com/support/policies/software-licensing

Table of Contents

Preface

This section discusses the conventions used in this guide, ways to provide feedback, additional help, and other Extreme Networks® publications.

Conventions

This section discusses the conventions used in this guide.

Text Conventions

The following tables list text conventions that are used throughout this guide.

Table 1: Notice Icons

Icon	Notice Type	Alerts you to...
👉	General Notice	Helpful tips and notices for using the product.
📌	Note	Important features or instructions.
⚠	Caution	Risk of personal injury, system damage, or loss of data.
⚡	Warning	Risk of severe personal injury.
New!	New Content	Displayed next to new content. This is searchable text within the PDF.

Table 2: Text Conventions

Convention	Description
`Screen displays`	This typeface indicates command syntax, or represents information as it appears 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 with brackets, such as **[Return]** 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.

Documentation and Training

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for earlier versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes
Hardware/Software Compatibility Matrices	https://www.extremenetworks.com/support/compatibility-matrices/
White papers, data sheets, case studies, and other product resources	https://www.extremenetworks.com/resources/

Training

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

Providing Feedback to Us

Quality is our first concern at Extreme Networks, and we have 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 especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team, you can do so in two ways:

- Use our short online feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Please 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.

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: 1-800-998-2408 (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 and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) 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

Subscribing to Service Notifications

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

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form with your information (all fields are required).
3. Select the products for which you would like to receive notifications.

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

4. Click **Submit**.

1 Welcome to Extreme Defender Application

Extreme Defender Application provides security management plus traffic and application visibility of connected end devices. Extreme Defender Application enables the centralized creation of policies that define network and security settings for groups of IoT devices.

Extreme Defender Application is installed as a container application on the ExtremeCloud Appliance. The application runs and is upgraded independently from the appliance.

Extreme Defender Application employs a configuration wizard that handles the following tasks:

- AP3912 and SA201 device adoption
- Site and device group creation
- Adoption rule configuration
- Policy group creation and auto-generation and assignment of policy roles
- Statistical reporting for protected devices.

Installing Extreme Defender Application

> Note
> Before you can install Extreme Defender Application you must install ExtremeCloud Appliance. See https://extremenetworks.com/documentation/extremecloud-appliance for more information.

Download the docker file from the Extreme Networks support site. Then, use the following procedure to install Extreme Defender Application on the ExtremeCloud Appliance.

From the ExtremeCloud Appliance:

1 Go to **Administration** > **Applications**.
2 Click **Add** to create the Configuration Template.

> Note
> ExtremeCloud Appliance offers a pre-configured template for Extreme Defender Application.

3 Click ⊕ to add an application to ExtremeCloud Appliance.
4 Install from a local **File** or docker hub **Registry**.
5 Click **Upload**, select the docker file, and click **Open**.

6 Click **OK**.

The application is uploaded and installed on ExtremeCloud Appliance.

7 Click ▶ to start the application.

The following describes the available application actions:

- ⚙ — Install new application.
- ✎ — Edit Configuration Template.
- ⊡ — Upgrade existing application.
- ⊖ — Uninstall application.
- ▶ — Start application.
- ■ — Stop application.
- ⓘ — Show application statistics. Displays dashboard widgets, configuration details, and logs, and it provides console access to the application for troubleshooting.

From the ExtremeCloud Appliance **Applications** list, select the Extreme Defender Application to display the Defender login screen. Your login credentials will match your ExtremeCloud Appliance credentials.

Additionally, the Extreme Defender Application user interface can be accessed using the HTTPS protocol on the TCP port 5825. For example, if your ExtremeCloud Appliance has the IP address 192.168.10.10, you can manage Extreme Defender Application in a browser by typing `https://192.168.10.10:5825/defender` into the URL field.

Note

When installing Extreme Defender Application on an ExtremeCloud Appliance Availability Pair, the ExtremeCloud Appliance services are supported by High Availability, the Extreme Defender Application is not.

Related Links

Upgrading an Application on page 8

Uninstalling an Application on page 9

Defender Application in an Availability Pair on page 9

Upgrading an Application

Note

Data in Volume storage *will not* be deleted upon application upgrade. However, all data is deleted when the application is uninstalled.

To upgrade an application:

1 Go to **Administration** > **Applications**.

2 To stop the application, select ■ then select **OK**.

3 To begin the application upgrade, select ⊡.

4 Upgrade from a local **File** or Docker hub **Registry**.

5 Select **Upload** and select the Docker file.

6 Select **Open** and select **OK**.

7. Select ▶ to start the application.

Related Links

Installing Extreme Defender Application on page 7

Uninstalling an Application on page 9

Uninstalling an Application

> Note
>
> All application data is deleted when you uninstall an application.

To uninstall an application:

1. Go to **Administration** > **Applications**.
2. To stop the application, select ■.
3. To remove the application, select ⊖.
4. To confirm that you want to uninstall the application, select **OK**.

Related Links

Installing Extreme Defender Application on page 7

Upgrading an Application on page 8

Defender Application in an Availability Pair

Extreme Defender Application is a single installation for an Availability Pair. The underlying ExtremeCloud Appliance is HA capable, but access to the Extreme Defender Application instance may be interrupted.

The following is supported in an Availability Pair:

- Automatic Configuration Sync — Configuration modifications on one appliance are replicated to the peer appliance.
- Automatic User Session Sync — In the case of a failover, the surviving appliance resumes ownership of the session.
- Double Capacity of Pair — In the case of a failover, the surviving appliance can sustain full paired capacity.
- Automatic load balancing of devices.
- Centralized APs maintain active and backup links to each controller. — In case of a failover, the device *activates* the backup link.

For more information about Availability Pair for ExtremeCloud Appliance, refer to *ExtremeCloud Appliance User Guide* located in the documentation portal: https://extremenetworks.com/documentation/extremecloud-appliance.

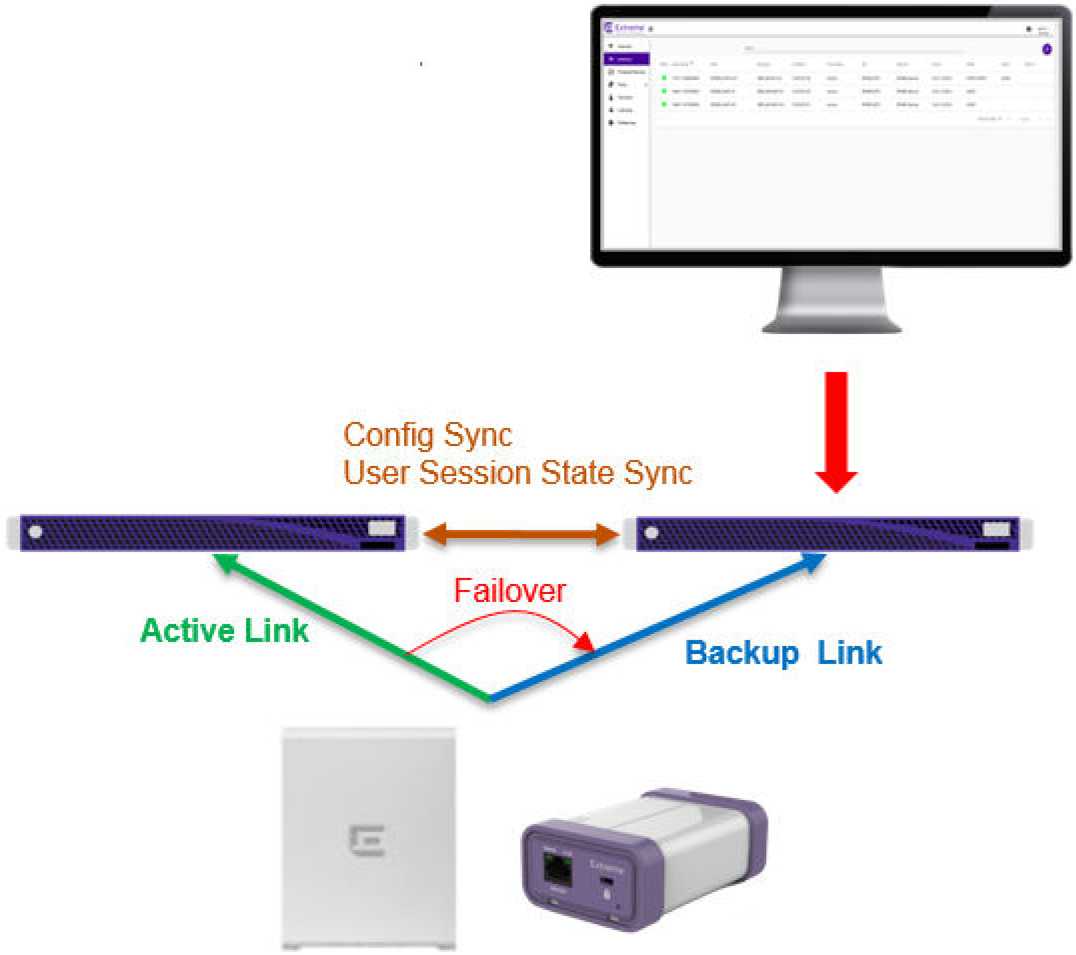
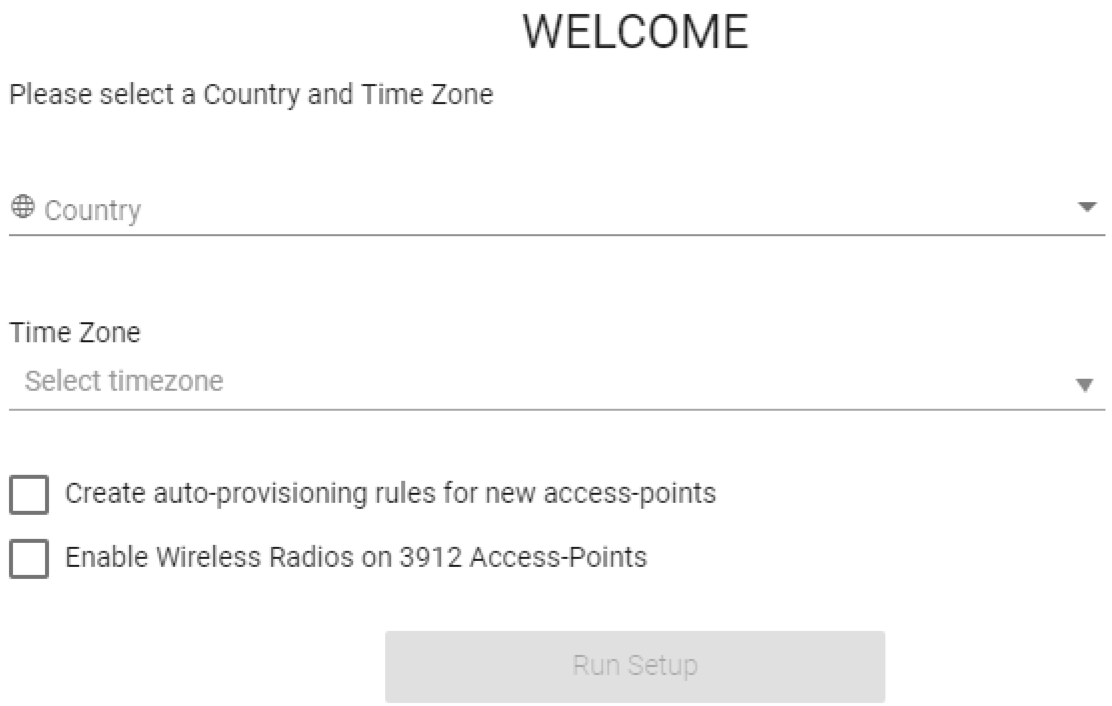


Figure 1: ExtremeCloud Appliance Availability Pair with Extreme Defender Application

Getting Started

When you log in to Extreme Defender Application for the first time, you are prompted with initial configuration options.



WELCOME

Please select a Country and Time Zone

Country

Time Zone

Select timezone

□ Create auto-provisioning rules for new access-points

□ Enable Wireless Radios on 3912 Access-Points

Run Setup

Figure 2: Defender Initial Configuration

Take the following steps:

1. Select a **Country** and **Time Zone** value from the drop-down lists.

   Specify the values that correspond to your AP licensing domain.
2. Check **Create auto-provisioning rules for new access points**.

   This option creates adoption rules for your access points so that your access points are automatically discovered by the appliance. If you do not enable this option, you will have to go to ExtremeCloud Appliance and manually select your access points for provisioning.
3. Check **Enable Wireless Radios on 3912 Access-Points**.

   Enable this option to allow wireless clients onto your network.
4. Click **Run Setup**.

The setup wizard automatically creates default configurations on ExtremeCloud Appliance, specifically for managing SA201 adapter or AP3912i. The default configuration is comprised of the following components:

- 1 site
- 2 device groups
- 1 network service
- 2 adoption rules
- 1 device group configuration Profile
- 2 roles

Each of these components is labeled with the “DFNDR_” prefix, indicating that they are configured for the Extreme Defender Application.

Note
Do not rename the Defender components.

Navigating the User Interface

The Extreme Defender Application user interface is divided into workbenches that correspond to the network administration workflow. The **Overview** is the first workbench. Once the network is up and running, use the Overview dashboard to monitor your network activity and performance.

Extreme Defender Application offers the following workbenches:

- **Overview**. Create multiple dashboards to monitor your protected devices, access points, and adapters.
- **Inventory**. List your access points and adapters and view details about each network device.
- **Protected Devices**. List your protected devices and view details about each protected device.
- **Policy**. View policy groups and roles associated with your network.
- **Activation**. Activates managed devices and access points.
- **Licensing**. Manage product licenses.
- **Preferences**. Configure user interface preferences.

Defender offers a context-sensitive Online Help system. Click the drop-down admin menu on any page to access the topic-based Help System.

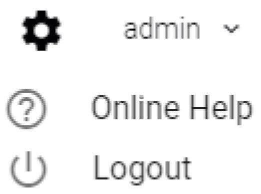


Figure 3: Defender Admin Menu

Additionally, click ? on each dialog to display Help content for that dialog.

The Online Help file organization corresponds to the workbench structure of Extreme Defender Application. The Online Help file offers a Table of Contents, Search Facility, and Index so you can find the information that you need.

Also on the **admin** menu, you will find the **Logout** option.

Click ⚙ on any page to access the Preferences page.

Search Facility

Each list page in Defender offers a search facility so you can easily find what you are looking for based on specific criteria. Regular expression search, including wild cards is not supported.

2 Overview

Monitor your network activity and performance on the Overview dashboard. The Overview dashboard displays widgets that can help you proactively monitor and troubleshoot your network. The dashboard provides a graphical representation of information related to devices, protected devices, and network traffic. Depending on the report, the widget represents historical data or a combination of historical and the latest data from shared memory.

Note
Historical data is persistent after system restarts and software upgrades, but not if the system is restored to the factory defaults or from a backup.

Extreme Defender Application is installed with a default dashboard. You can customize the default dashboard and add additional dashboards with a unique set of widgets. The maximum number of supported dashboards is 10. The Overview dashboard offers the following widgets:

- Device Vendors
- Devices by Throughput
- Throughput
- Usage
- AP Status
- Adapter Status

Adding a New Dashboard

Create additional dashboards to organize data.

To add a new dashboard:

1 From the default dashboard, click the plus sign.

The Layout tab displays.

2 In the **Name** field, enter a name for the dashboard.

3 Select the Widgets tab.

The list of widgets by category is displayed.

4 Expand the list of widgets in each category.

5 Drag and drop a widget onto the dashboard.

6 Click 💾 to save the dashboard.

Related Links

Modifying a Dashboard on page 15

Widgets on page 15

Modifying a Dashboard

You can customize the default dashboard views to fit your network's analytic requirements.

To modify a dashboard:

1. Go to **Overview** and select ✎.
2. Select the Widgets tab to view the list of available widgets.
3. Drag and drop a widget on to the dashboard.

Related Links

Widgets on page 15

Adding a New Dashboard on page 14

Widgets

From the Widgets tab, expand the categories that you want to use. Drag and drop a widget onto the dashboard. The following widget categories are available:

Device Vendors	The number of protected devices by device vendor.
Devices by Throughput	The top protected devices by throughput (kilobits per second).
Throughput	Network throughput (kilobits per second) in 10-minute intervals.
Usage	Network usage (RxBytes and TxBytes) in 10-minute intervals.
AP and Adapter Status	Graphs the number of APs or adapters by status. Valid status values are: • Green — In-Service. Device has discovered ExtremeCloud Appliance and is providing service. • Yellow — In-Service Trouble. Device has discovered ExtremeCloud Appliance but it is not a member of a device group. • Grey — Unknown. Device is added to ExtremeCloud Appliance but the device has never discovered ExtremeCloud Appliance . • Red — Critical. After being Active, Discovered, and On-boarded, associated device is no longer connected to ExtremeCloud Appliance.

Related Links

Adding a New Dashboard on page 14

Modifying a Dashboard on page 15

3 Inventory

The Inventory list allows you to view the inventory of mobile network devices, such as access points and Extreme Defender Adapter hardware (SA201). The Inventory list provides information on the status and the location of the devices. The following information is provided for each device on the Inventory list:

- Status
- Serial Number
- Name
- Description
- IP Address
- Site
- Networks
- Version
- Model

Click ⟳ to manually refresh the page.

Select **Items Per Page** to customize the number of records displayed per page. Valid values are:

- 5
- 10
- 25
- 100
- 500

Related Links

Search Facility on page 13
Inventory Device Status on page 16
Viewing Inventory Details on page 17

Inventory Device Status

The following describes each device status on the Inventory List.

Table 3: Device Status from the Inventory List

Status	Description
🟢	In-Service. Device has discovered ExtremeCloud Appliance and is providing service.
⚠	In-Service Trouble. Device has discovered ExtremeCloud Appliance but it is not a member of a device group.
●	Unknown. Device is added to ExtremeCloud Appliance but the device has never discovered ExtremeCloud Appliance .
🟥	Critical. After being Active, Discovered, and On-boarded, associated device is no longer connected to ExtremeCloud Appliance.

Viewing Inventory Details

Specific details about each device are available from the device **Details** tab. To access the details for each device:

1. Go to **Inventory** and select a device from the list.

   The following information is provided:

   - Device Status
   - Serial Number
   - IP Address
   - Gateway Address
   - Hardware Type
   - Firmware Version
   - Assigned Site
   - Assigned Networks
   - Number of Wired Clients
   - Number of Protected Devices associated with the selected device:
     - Number of Wired Devices
     - Number of Wireless Devices
   - Assigned group for the protected device.
2. Select the **Throughput** tab to display network throughput for the last 3 hours.
3. Select the **Usage** tab to display the Rx and Tx Bytes transmitted in the last 3 hours.

Click ↻ to manually refresh the page.

Related Links

Throughput Tab on page 18

Usage Tab on page 19

Grouping Protected Devices from the Inventory List on page 18

Inventory on page 16

Grouping Protected Devices from the Inventory List

Add Protected Devices to a policy group from the **Inventory** > **Device Details** page or from the Protected Devices list. To add devices to a policy group from the **Inventory** > **Device Details** take the following steps:

1. Go to **Inventory** and select a device.

   The device Details tab displays.
2. If the device has associated Protected Devices, the **Assigned Group** field is displayed.
3. Select a group name from the **Assigned Group** drop-down list.

   To remove a device from a group, select **None**.
4. Click **Save**.

> Note
> To create a new policy group, go to **Policy** > **Groups** > **Add**.

Related Links

Grouping Devices from the Protected Devices List on page 23

Managing Groups on page 32

Throughput Tab

Select the **Throughput** tab to display network throughput for the last 3 hours.

Network Throughput indicates the amount of data in Kilobits per second or Megabits per second that travels through the communication channel at a given time. This is one indication of network speed. The Throughput chart displays data for the last 3 hours. Click ↻ to refresh the chart on demand.

Select ⤓ to download the chart in .png format.

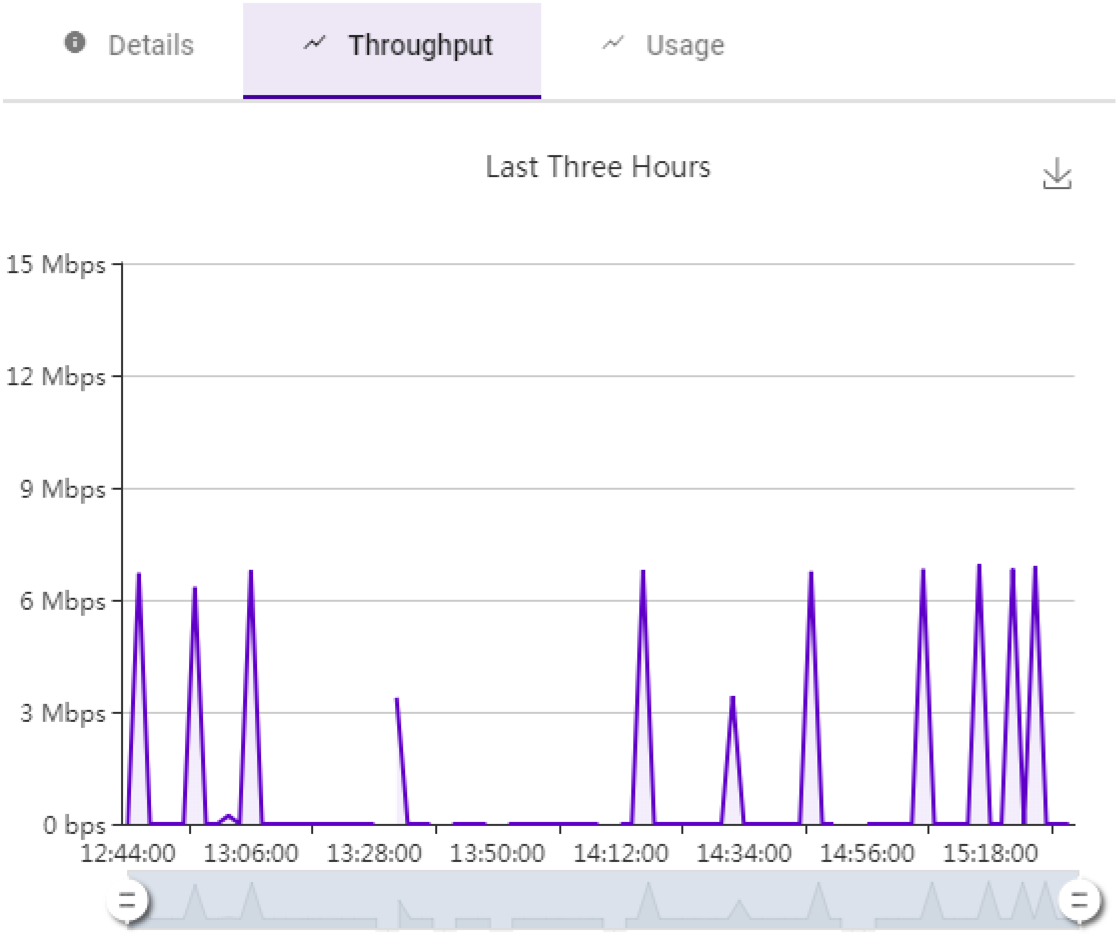


Figure 4: AP Inventory Device Throughput (Mbps)

Usage Tab

Select the **Usage** tab to display the Rx and Tx Bytes transmitted in the last 3 hours.

Network Usage indicates the amount of data in Megabytes or Gigabytes that travels through the communication channel at a given time. Rx refers to bytes *received* by the device. Tx refers to bytes *transmitted* from the managed device (AP/SA201) . This is one indication of network load. The Usage chart displays data for the last 3 hours. Click ⟳ to refresh the chart on demand.

Select ⤓ to download the chart in .png format.

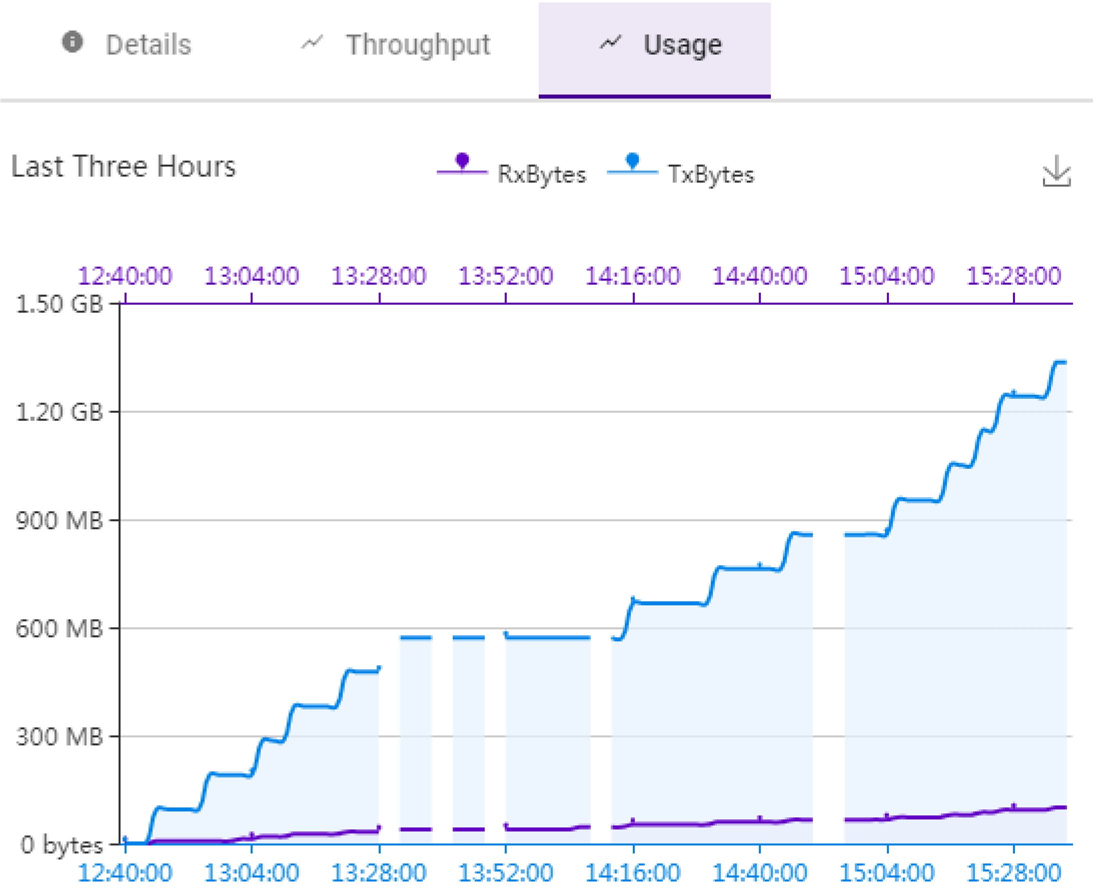


Figure 5: AP Inventory Managed Device Usage

4 Protected Devices

The Protected Devices list allows you to manage attached devices that are protected by the Extreme Defender Application access points and adapter hardware (SA201) . The Protected Devices list provides information on the status and the location of the attached devices.

Display current devices or archived devices by selecting the appropriate option from the drop-down field at the top of the page.

The following information is provided for each device on the Protected Devices list:

- Status
- IP Address
- MAC Address
- Associated Site
- Assigned Group
- Assigned Role
- Service
- Host Name
- Last Seen
- Manufacturer
- AP/Adapter

Click ↻ to manually refresh the page.

Select **Items Per Page** to customize the number of records displayed per page. Valid values are:

- 5
- 10
- 25
- 100
- 500

Related Links

Search Facility on page 13
Viewing Protected Device Details on page 22
Grouping Devices from the Protected Devices List on page 23

Protected Device Status

The following describes each device status on the Protected Devices List.

Table 4: Protected Device Status

Status	Description
🟢	Active. Device has the following: • Discovered ExtremeCloud Appliance • On-boarded with a policy role • Actively sending data.
⚠	Not On-board. Device: • Discovered ExtremeCloud Appliance • Actively sending data • Not on-boarded. To on-board a Protected Device, add it to a group that has an assigned policy role.
●	Inactive. Device: • On-boarded with a policy role. • Not actively sending data.
🟥	Critical. After being Active, Discovered, and On-boarded, associated AP or adapter is no longer connected to ExtremeCloud Appliance.
❗	Archived. Defender archives devices that are no longer present on ExtremeCloud Appliance. The device may have become inactive and aged out of ExtremeCloud Appliance reporting. If the device becomes active again on ExtremeCloud Appliance, the device will move from Archived to Active on Defender.
🛡	Policy Generator runs on a device that is active and on-boarded.
🛡	Policy Generator runs on an inactive device. No policy will be created while the device is inactive. When the device becomes active, the policy will automatically generate.

Related Links

Grouping Devices from the Protected Devices List on page 23

Viewing Protected Device Details

Specific details about each protected device are available from the Protected Device Details page. To access the details for each protected device:

1. Go to **Protected Devices** and select a device from the list.

   The following information is provided:

   - Licensed
   - Status
   - Last Seen

- Device Type
- Manufacturer
- Host Name
- MAC Address
- IP Address
- Associated Access Point
- Assigned Group
- Assigned Role
- Service
- Associated Site

The following tabs provide additional information.

Throughput
Select the **Throughput** tab to display network throughput for the last 3 hours.

Usage
Select the **Usage** tab to display the Rx and Tx Bytes transmitted in the last 3 hours.

Movements
Tracks the movement of protected devices, registering the following information:

- Time of movement
- Event description
- Serial number of source AP
- Serial number of destination AP
- Additional details
- Network SSID

Policy Generator
The policy generator captures and analyzes client traffic, building an Allow policy role that correlates with the traffic pattern of the protected device. An auto-generated role can be modified by the Administrator and made available to the ExtremeCloud Appliance Rules Engine.

2 Select ↻ to refresh the chart data.

Related Links

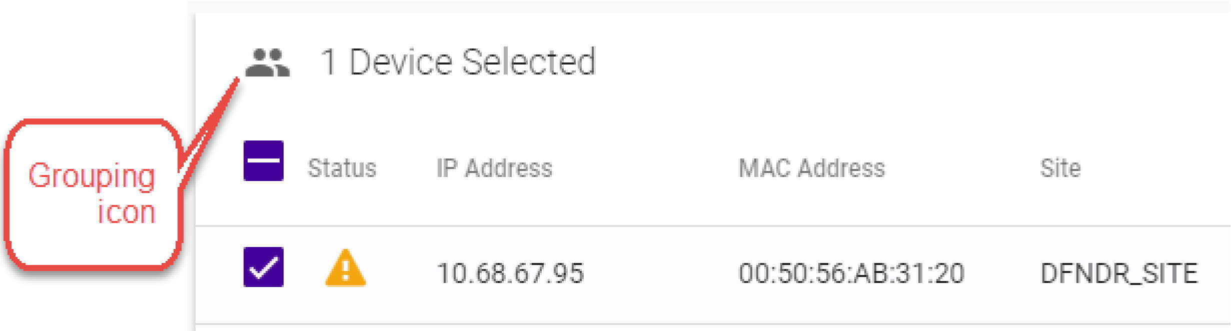
Throughput Tab on page 18
Usage Tab on page 19
Movements Tab on page 25
Policy Generator on page 25

Grouping Devices from the Protected Devices List

Add Protected Devices to a policy group from the Protected Devices list or from the **Inventory** > **Device Details** page. To add devices to a policy group from the Protected Devices list, take the following steps:

1 Go to **Protected Devices**.
2 Select the check box for one or more devices.

3 Click the group icon



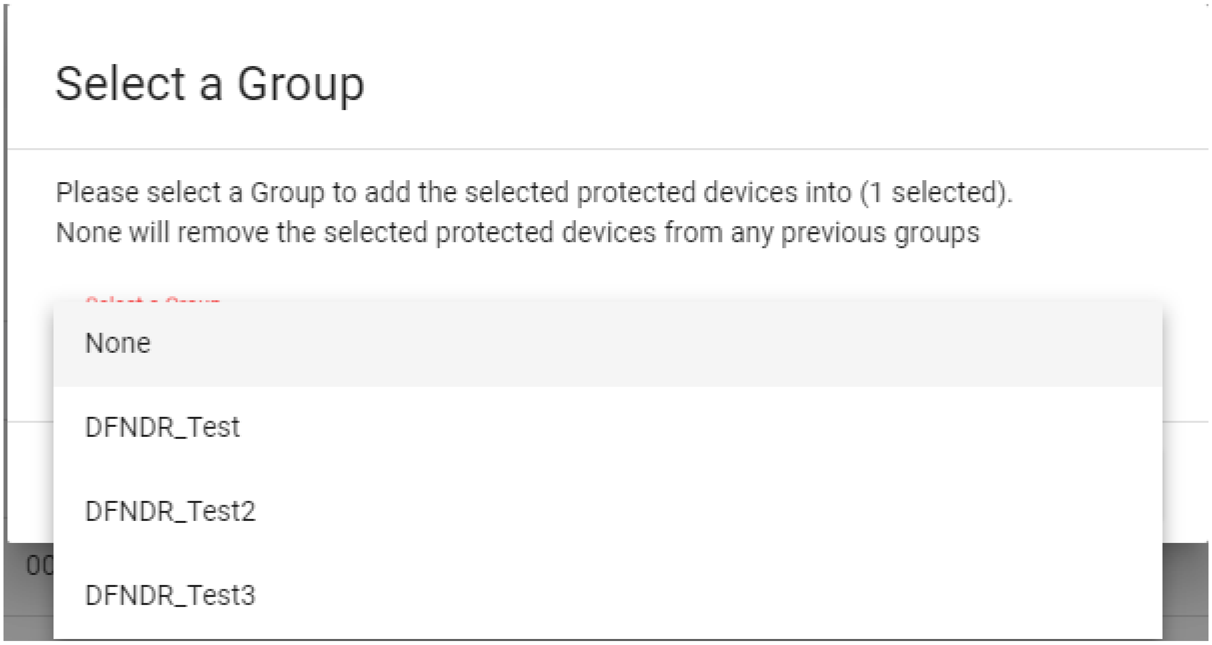
1 Device Selected

☐	Status	IP Address	MAC Address	Site
☑	⚠	10.68.67.95	00:50:56:AB:31:20	DFNDR_SITE

Figure 6: Select a Policy Group for Protected Device

The Select a Group dialog displays.

4 From the **Select a Group** drop-down, select the group name to which the devices will be added.


Select a Group

Please select a Group to add the selected protected devices into (1 selected).
None will remove the selected protected devices from any previous groups

Figure 7: Selecting a Group

To remove a device from a group, select **None**.

5 Click **OK**.

Note
To create a new policy group, go to **Policy** > **Groups** > **Add**.

Related Links

Grouping Protected Devices from the Inventory List on page 18

Managing Groups on page 32

Movements Tab

As protected devices get moved from one location to another, you can track and manage information about the specific device location. Go to **Protected Devices** > **Movements**. Then, specify a date range to display event information for a selected protected device. Each movement record displays the following information:

- Time of event
- Event description
- Serial number of source AP
- Serial number of destination AP
- Additional details
- Network SSID

Select **Items Per Page** to customize the number of records displayed per page. Valid values are:

- 5
- 10
- 25
- 100
- 500

Related Links

Search Facility on page 13

Policy Generator on page 25

Policy Generator

Policy Generator captures and analyzes client traffic, creating a "Deny" policy role as the default action. (The Defender IoT solution is based on whitelist filter rules.) An auto-generated role can be modified by the Administrator and made available to the ExtremeCloud Appliance Rules Engine.

To initiate auto policy generation, allow all traffic up to 14 days, capturing traffic in a .pcap file. The auto generator creates the policy role and policy group of MAC addresses called `DFNDR_PolicyGeneration` and configures policy rules based on the contents of the .pcap file. When you stop policy generation, the auto generator removes the MAC addresses from the `DFNDR_PolicyGeneration` group. Defender supports up to 10 simultaneous PCAP sessions.

Note
Do not rename the Defender components.

Although the Policy Generator engine is run from Extreme Defender Application, the corresponding policies are managed and enforced through the underlying ExtremeCloud Appliance. ExtremeCloud Appliance supports up to a maximum of 64 rules per policy/role definition. The number of policies/roles varies based on the appliance model.

When DHCP and DNS translations are required, policy generator automatically creates rules that allow DHCP and DNS traffic, respectively. Policy generator can also create rules that allow traffic from well-known ports and protocols. You can later remove or modify an auto-generated rule as necessary.

Protected devices of the same type can be attached to a single role regardless of the network location and subnet, but multiple device types cannot share one policy role. Policy roles are enforced on the SA201 adapter or AP3912i for B@AP and Fabric Attach topologies. They are enforced on ExtremeCloud Appliance for B@AC topologies.

Note
Each protected device type must be associated with a different policy role. However, multiple devices of the *same* type can share a single policy role.

Related Links

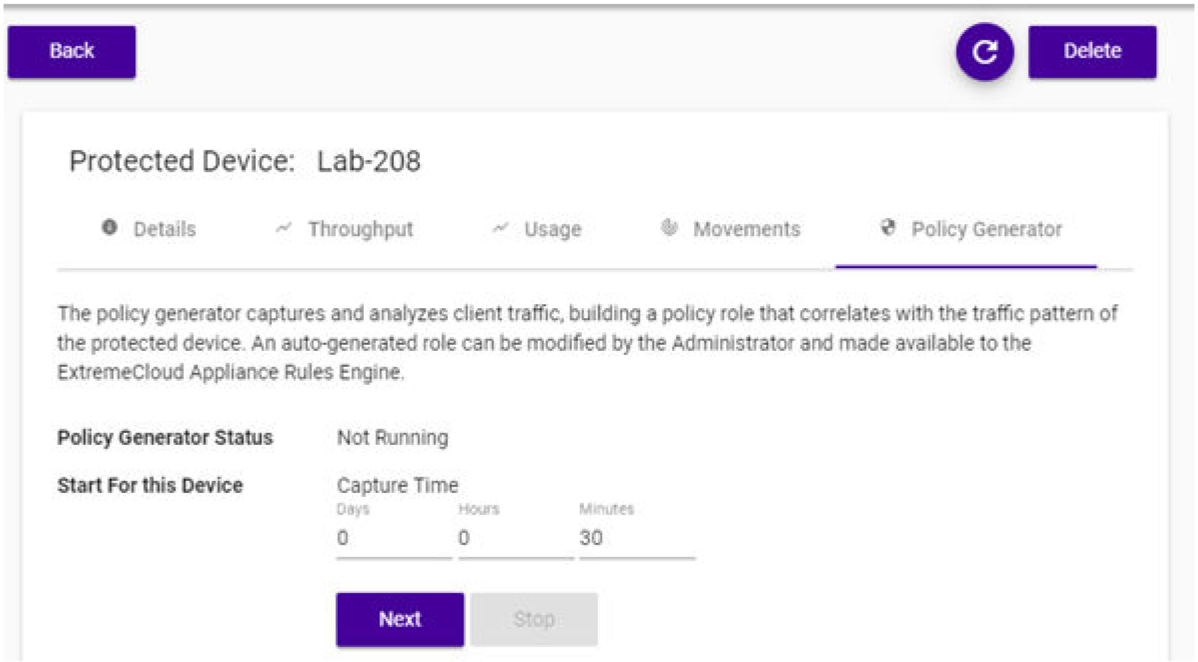
Running Policy Generator on page 26
Configuring L2 Rules on page 28
Configuring L3 and L4 Rules on page 29
Allowing DNS, DHCP, and Well-Known Port Traffic Automatically on page 30

Running Policy Generator

Access Policy Generator from an active protected device on the **Protected Devices** list.

Note
Run one policy generation on an AP at a time. You can run up to 10 concurrent policy generations from Extreme Defender Application.

1 Go to **Protected Devices** and click on a device with a status of Active (on-boarded).
2 Select the **Policy Generator** tab.



Protected Device: Lab-208

The policy generator captures and analyzes client traffic, building a policy role that correlates with the traffic pattern of the protected device. An auto-generated role can be modified by the Administrator and made available to the ExtremeCloud Appliance Rules Engine.

Policy Generator Status Not Running

Start For this Device Capture Time

Days	Hours	Minutes
0	0	30

Figure 8: Policy Generator

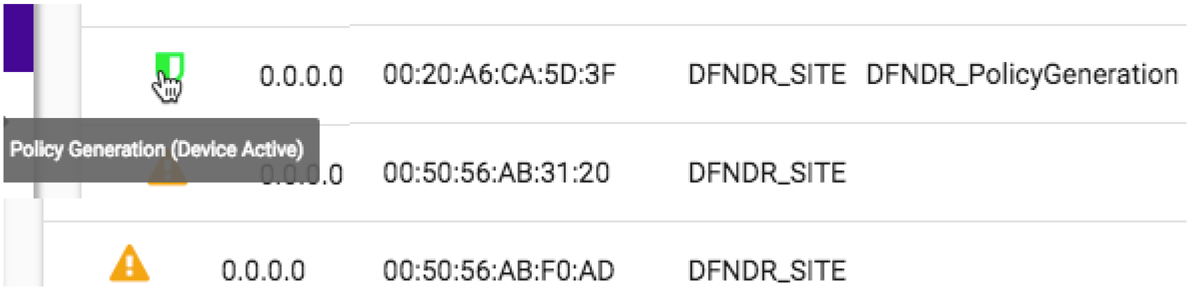
3 From the **Start for this Device** field, specify a capture window in Days, Hours, or Minutes.

- Days. Valid values are 0-14
- Hours. Valid values are 0-23
- Minutes. Valid values are 0-59

4 Click **Next**.

5 Select a VLAN ID for the VLAN that the protected device belongs to, and click **Start**.

Figure 9 is an example of a protected device in the device list that is in capture mode for policy generation:



🟩	0.0.0.0	00:20:A6:CA:5D:3F	DFNDR_SITE	DFNDR_PolicyGeneration
⚠	0.0.0.0	00:50:56:AB:31:20	DFNDR_SITE	
⚠	0.0.0.0	00:50:56:AB:F0:AD	DFNDR_SITE	

Figure 9: Protected Device in Capture Mode

6 When the capture is complete, click **Open Generated Role for Editing** to view and edit the role.

If necessary, click **Stop** to stop the Policy Generator. You can stop the packet capture process and generate a policy based on the packets captured before you clicked **Stop**.

Related Links

Policy Generator on page 25

Configuring L2 Rules on page 28

Configuring L3 and L4 Rules on page 29

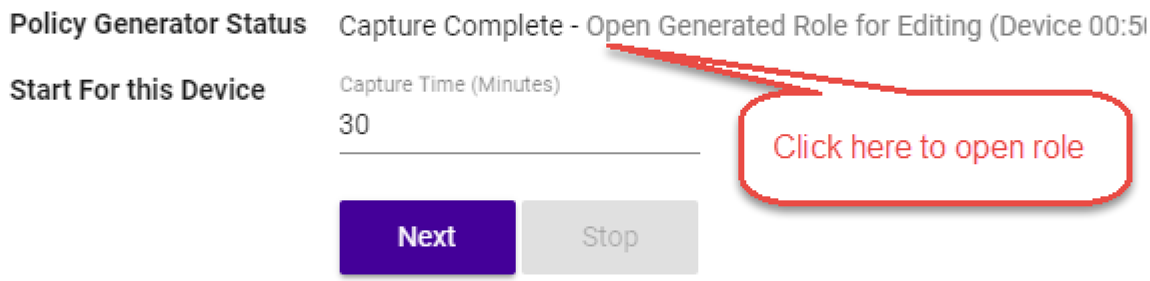
Allowing DNS, DHCP, and Well-Known Port Traffic Automatically on page 30

Modifying Policy Generator Roles

Policy Generator captures and analyzes client traffic, creating a "Deny" policy role as the default action. (The Defender IoT solution is based on whitelist filter rules.) An auto-generated role can be modified by the Administrator and made available to the ExtremeCloud Appliance Rules Engine.

To modify a generated role, take the following steps:

1 Click **Open Generated Role for Editing** to view and edit the role.



Policy Generator Status: Capture Complete - Open Generated Role for Editing (Device 00:5

Start For this Device: Capture Time (Minutes) 30

Click here to open role

Figure 10: Open Generated Role

2 Provide a name for the generated role. All generated roles start with the DFNDR_ prefix.

> Note
> For generated roles, use the DFNDR_ prefix in the role name. You can provide a unique suffix.

3 Select the default action for the generated role.

Valid values are:

- Allow
- Deny
- Contain to VLAN
    - Provide a VLAN ID

4 Add additional rules to the generated role as required.

Related Links

Configuring L2 Rules on page 28

Configuring L3 and L4 Rules on page 29

Configuring L2 Rules

To configure an OSI Layer 2 rule, which filters on MAC Address:

1 Select **New**.

2 Enter a rule name and configure the following parameters:

From User — A packet header includes both a destination IPv4 address and a source IPv4 address. Determine how to filter traffic that flows from the station to the network by defining the destination or the source address as the filter. Options include: Destination (dest), Source (src), and None.

To User — A packet header includes both a destination IPv4 address and a source IPv4 address. Determine how to filter traffic that flows from the network to the station by defining the destination or the source address as the filter. Options include: Destination (dest), Source (src), and None.

Action — Determines access control action for the rule. Valid values are:

- Allow - Packets contained to role's default action's VLAN/topology
- Deny - Any packet not matching a rule in the policy is dropped.
- Containment VLAN - A topology to use when a network is created using a role that does not specify a topology.

MAC Address Type
: Any MAC indicates no filtering on MAC Address. User Defined MAC displays a MAC Address field. Provide a specific MAC Address.

3. Select **Save**.

   All rule types are applied to the policy in top to bottom order. Click the Up or Down arrows to move the rule up or down in the list. The policy is installed on the enforced APs.

Related Links

Modifying Policy Generator Roles on page 27

Configuring L3 and L4 Rules on page 29

Configuring L3 and L4 Rules

To configure an OSI Layer 3 and 4 rule, which filters on IP Address and Port number:

1. Select **New**.

   A new row appears at the bottom of the list.

2. Enter a rule name and configure the following parameters:

From User
: A packet header includes both a destination IPv4 address and a source IPv4 address. Determine how to filter traffic that flows from the station to the network by defining the destination or the source address as the filter. Options include: Destination (dest), Source (src), and None.

To User
: A packet header includes both a destination IPv4 address and a source IPv4 address. Determine how to filter traffic that flows from the network to the station by defining the destination or the source address as the filter. Options include: Destination (dest), Source (src), and None.

Action
: Determines access control action for the rule. Valid values are:

- Allow - Packets contained to role's default action's VLAN/topology
- Deny - Any packet not matching a rule in the policy is dropped.
- Containment VLAN - A topology to use when a network is created using a role that does not specify a topology.

Protocol
: The user defined protocol or protocol type associated with the defined rule. Traffic from this protocol is subject to the defined rule. Valid values are:

- User Defined, then specify a protocol that is not already in the list. Use this option to explicitly specify a protocol that is not listed.
- A specific protocol from the list.

IP Subnet
: Specify the IP address or subnet address associated with the defined rule. Traffic from this address will be subject to the defined rule. Valid values are:

- User Defined. Specify the destination IP address and mask. Use this option to explicitly define the IP/subnet aspect of the rule.
- Any IP - Maps the rule to the associated Topology IP address.
- Select a specific subnet value - Select to map the rule to the associated topology segment definition (IP address/mask).

Port Type
: The port type associated with the defined rule. Traffic from this port is subject to the defined rule. Valid values are:

- User Defined, then type the port number. Use this option to explicitly specify the port number.
- A specific port type.

Port Number/ Range	Specific port number or range of ports.

3. Select **Save**.

   All rule types are applied to the policy in top to bottom order. Click the Up or Down arrows to move the rule up or down in the list. The policy is installed on the enforced APs.

Related Links

Modifying Policy Generator Roles on page 27

Configuring L2 Rules on page 28

NEW!

Allowing DNS, DHCP, and Well-Known Port Traffic Automatically

To allow for DNS and DHCP transactions, Policy Generator detects packet transfers and automatically creates allow rules for this client traffic:

- When the client sends DNS packets during packet capture, Policy Generator creates a rule that allows UDP port 53 to and from the *DNS server* for DNS traffic.
- When the client does not detect DNS packets during packet capture, Policy Generator creates a rule that allows UDP port 53 to and from *any IP address* for DNS traffic.
- Regardless of whether or not the client sends DHCP packets during packet capture, policy generator creates a rule that allows UDP port 67 to and from *any IP address* for DHCP traffic.

Additionally, when the client sends packets with well-known port numbers that are associated with UDP protocols, such as SNMP and NetBIOS, Policy Generator creates rules that allow traffic on those UDP ports.

Note

All auto-generated rules that Policy Generator creates can be modified or deleted from ExtremeCloud Appliance.

Related Links

Policy Generator on page 25

5 Policy

Extreme Defender Application policy definition consists of roles, rules, and group management. You can use default roles and groups or create new ones.

Related Links

Roles on page 31

Groups on page 32

Roles

The Policy Roles list displays all roles available in your Extreme Defender Application network.

Network policies are a set of rules, defined in a specific order, that determine how connections are authorized or denied. If you do not define policy rules for a role, the role's default action is applied to all traffic subject to that role. However, if you require user-specific filter definitions, then the filter ID configuration identifies the specific role that is applied to the user.

Policy definition (Access Control List, Network assignment) are defined by the IT staff through the ExtremeCloud Appliance. Roles with a Prefix of "DFNDR_" are available for policy assignment via the Extreme Defender Application.

By default, Extreme Defender Application creates two policy roles: DenyAll and PolicyGeneration. The DenyAll role denies all traffic by default action. There are no filter rules associated with this role. The PolicyGeneration role, has a Contain to VLAN default action and is associated with a B@AP untagged topology. The Contained to VLAN default action sends any packet not matching a rule to the defined VLAN.

ExtremeCloud Appliance supports up to 256 unique policy roles, depending on the specific appliance model user limitation. The Defender Policy Generator can generate a policy based on traffic patterns associated with a protected device. A user with Administrator access can modify an auto-generated role and make it available to the ExtremeCloud Appliance Rules Engine.

Select a role to view the associated rules in Extreme Defender Application. You can manually add and modify roles from ExtremeCloud Appliance.

Related Links

Policy Generator on page 25

Groups

An access control group is used to organize protected devices by MAC Address. Configure groups to be used with Access Control Rules. Defender provides the default system group PolicyGeneration with your installation to simplify the group set up process.

Related Links

Managing Groups on page 32

Policy Group Settings on page 32

Managing Groups

From the Policy Groups page you can create a new group and search for an existing group. You can also remove MAC addresses from a group or delete the group altogether.

> Note
> Add Protected Device MAC addresses to a group, from the Protected Devices list or from the Inventory list.

To manage groups from the **Policy** workbench:

- Go to **Policy** > **Groups**.
  A list of configured groups displays. From here, you can search for a group or add a new group.
- To add a new group, click **Add** and configure the Policy Group Settings.
- To remove one or more MAC addresses from the group, select the group and click 🗑 next to the MAC Address row you want to remove.
- To delete a group, select the group and click **Delete**.

Related Links

Policy Group Settings on page 32

Grouping Protected Devices from the Inventory List on page 18

Grouping Devices from the Protected Devices List on page 23

Policy Group Settings

Configure the following settings to create a new policy group:

Table 5: Policy Group Settings

Field	Description
Name	Name of the group. Defender groups include the DFNDR_ prefix.
Description	Description of the group.
Associated Role	Policy role that applies to this group. All protected devices that are members of the group are awarded the policy access defined in the associated policy role.

Related Links

Groups on page 32

Managing Groups on page 32

Roles on page 31

6 Activation

From the **Activation** workbench, you can easily add access points and adapters to your network. The devices will be listed in an Unknown status until each device has discovered ExtremeCloud Appliance.

Note

You must configure ExtremeCloud Appliance discovery for your devices before the devices will function in Extreme Defender Application. For information about Configuring DHCP, NPS, and DNS Services for ExtremeCloud Appliance discovery, refer to the *ExtremeCloud Appliance Deployment Guide* located in the documentation portal: https://extremenetworks.com/documentation/extremecloud-appliance.

For deployment information specific to Extreme Defender Application, refer to the *Extreme Defender for IoT Solution Deployment Guide* located here: https://extremenetworks.com/documentation/defender-application.

Extreme Defender Application offers different ways to provision access points and adapters. If you have configured discovery and auto-provisioning, the provisioning process creates a device group for the device type within the DFNDR_SITE. Configure auto-provisioning from the Extreme Defender Application **Welcome** screen.

Related Links

Scanning a QR Code on page 34

Manual Onboarding on page 35

Using a CSV File on page 35

Getting Started on page 10

Scanning a QR Code

You can provision an access point or adapter by QR Code.

1. Go to **Activation**.
2. From the Scan QR Code pane, click **Camera**.
3. Place the QR Code on the device up to the black box for scanning.

   The information provided from the QR Code populates Defender and provisions the APs and adapters.

Related Links

Activation on page 34

Manual Onboarding

To manually provision an access point or adapter:

1 Go to **Activation** and select **Manual Onboarding**.

2 Configure the following parameters:

Table 6: Settings for Manual Provisioning

Field	Description
Serial Number	The serial number of the AP or adapter.
Model	Select from the list of supported device models.
Name	Unique name for the AP or adapter.
Description	Text description of the AP or adapter.

3 Click **Add Device**.

Related Links

Activation on page 34

Using a CSV File

Drag and drop a .csv file to automatically provision an AP or adapter.

1 Go to **Activation** and do one of the following:

- Click on the **Browse/Drop CSV** image and navigate to the .csv file.
- Drag and Drop a .csv file onto the **Browse/Drop CSV** image.

2 Navigate to the .csv file and click **Open**.

The information provided in the .csv file populates Defender and provisions the APs and adapters.

.csv file format

Provide the .csv file in the following format. When using a spreadsheet, the following are the column headings of the spreadsheet.

`serialNumber,hardwaretype,apName,description`

```
1701Y-1248300023,AP3912i-FCC,TestAp,"description1"
1701Y-1248300024,AP3912i-FCC,TestAp1,"description2"
```

Note
Column values are separated by commas. To use commas within the description, use quotes around the full description.

Related Links

Activation on page 34

7 Licensing

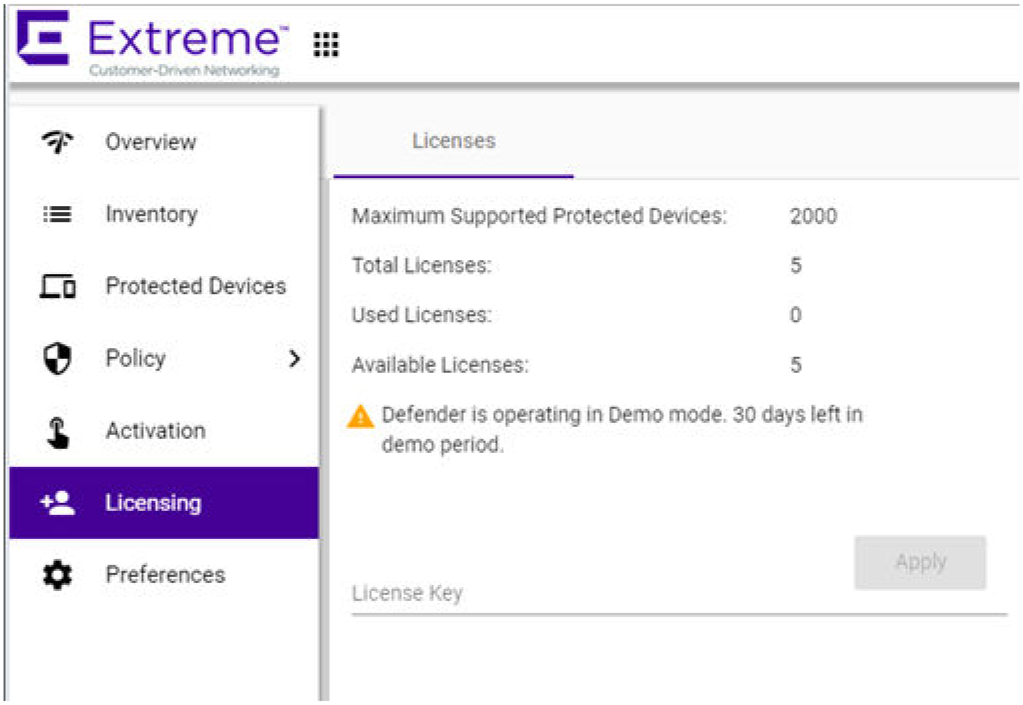
Licensing for the Defender for IoT solution is based on the number of IoT devices being protected by Defender. Extreme Defender Application allows a specific number of protected device licenses. The Licensing page displays the following information:

- Maximum number of supported devices for the appliance model
- Total number of licenses
- Number of licenses currently used
- Number of available licenses.

Note
Extreme Defender Application offers a Demo license that supports up to 10 access points for demonstration purposes. The Demo license period is 90 days.

From the Licensing workbench, apply the Extreme Defender Application license key.

1 Go to Licensing.
2 Enter one or more license keys in the License Key field and click **Apply**.



Maximum Supported Protected Devices: 2000
Total Licenses: 5
Used Licenses: 0
Available Licenses: 5

Defender is operating in Demo mode. 30 days left in demo period.

Figure 11: Defender Application Licensing Page

Figure 11, shows that the maximum number of devices this Extreme Defender Application can protect is 2000. This instance is currently licensed for 5. Devices can be MRI / CT scanner, Infusion pumps, HVAC, printer or any other IoT device.

Note
ExtremeCloud Appliance governs the total number of managed devices and the capacity of managed devices. Log into ExtremeCloud Appliance, then go to **Administration** > **License**. For more information about ExtremeCloud Appliance licensing see the *ExtremeCloud Appliance User Guide* at https://extremenetworks.com/documentation/extremecloud-appliance or see the ExtremeCloud Appliance Online Help.

8 Preferences

Customize the Extreme Defender Application from the Preferences workbench.

Go to **Preferences** and configure the following settings:

Table 7: Defender Preference Settings

Field	Description
Web Session Timeout	Determines the web session inactive window before the session times out. Enter the value as hours : minutes. The range is 1 minute to 168 hours (7 days).

Click ⚙ on any page to access the Preferences page.

Glossary

Chalet

Chalet is a web-based user interface for setting up and viewing information about a switch, removing the need to enter common commands individually in the CLI.

CLI

Command Line Interface. The CLI provides an environment to issue commands to monitor and manage switches and wireless appliances.

Data Center Connect

DCC, formerly known as DCM (Data Center Manager), is a data center fabric management and automation tool that improves the efficiency of managing a large virtual and physical network. DCC provides an integrated view of the server, storage, and networking operations, removing the need to use multiple tools and management systems. DCC automates VM assignment, allocates appropriate network resources, and applies individual policies to various data objects in the switching fabric (reducing VM sprawl). Learn more about DCC at http://www.extremenetworks.com/product/data-center-connect/.

Extreme Application Analytics

EAA, formerly Purview™, is a network powered application analytics and optimization solution that captures and analyzes context-based application traffic to deliver meaningful intelligence about applications, users, locations, and devices. EAA provides data to show how applications are being used. This can be used to better understand customer behavior on the network, identify the level of user engagement, and assure business application delivery to optimize the user experience. The software also provides visibility into network and application performance allowing IT to pinpoint and resolve performance issues in the infrastructure whether they are caused by the network, application, or server. Learn more about EAA at http://www.extremenetworks.com/product/extremeanalytics/.

Extreme Management Center

Extreme Management Center (Management Center), formerly Netsight™, is a web-based control interface that provides centralized visibility into your network. Management Center reaches beyond ports, VLANs, and SSIDs and provides detailed control of individual users, applications, and protocols. When coupled with wireless and Identity & Access Management products, Management Center becomes the central location for monitoring and managing all the components in the infrastructure. Learn more about Management Center at http://www.extremenetworks.com/product/management-center/.

ExtremeCloud Appliance

The ExtremeCloud Appliance, the newest addition to the Smart OmniEdge portfolio, is a next generation orchestration application offering all the mobility services required for modern unified access deployments. The ExtremeCloud Appliance extends the simplified workflows of the ExtremeCloud public cloud application to on-prem/private cloud deployments.

The ExtremeCloud Appliance includes comprehensive critical network services for wireless and wired connectivity, wireless device secure onboarding, distributed and centralized data paths, role-based access control through the Application Layer, integrated location services, and IoT device onboarding through a single platform.

Built on architecture with the latest technology, the embedded operating system supports application containers that enable future expansion of value added applications for the unified access edge. Learn more about ExtremeCloud Appliance at https://www.extremenetworks.com/product/extremecloud-appliance/.

ExtremeCloud

ExtremeCloud is a cloud-based network management Software as a Service (SaaS) tool. ExtremeCloud allows you to manage users, wired and wireless devices, and applications on corporate and guest networks. You can control the user experience with smarter edges – including managing QoS, call admission control, secure access policies, rate limiting, multicast, filtering, and traffic forwarding, all from an intuitive web interface. Learn more about ExtremeCloud at http://www.extremenetworks.com/product/extremecloud/.

ExtremeControl

ExtremeControl, formerly Extreme Access Control™ (EAC), is a set of management software tools that use information gathered by a hardware engine to control policy to all devices on the network. The software allows you to automate and secure access for all devices on the network from a central dashboard, making it easier to roll out security and identity policies across the wired and wireless network. Learn more about ExtremeControl at https://www.extremenetworks.com/product/extremecontrol/.

ExtremeSwitching

ExtremeSwitching is the family of products comprising different switch types: Modular (X8 and 8000 series [formerly BlackDiamond] and S and K series switches); Stackable (X-series and A, B, C, and 7100 series switches); Standalone (SSA, X430, and D, 200, 800, and ISW series); and Mobile Backhaul (E4G). Learn more about ExtremeSwitching at http://www.extremenetworks.com/products/switching-routing/.

ExtremeWireless

ExtremeWireless products and solutions offer high-density WiFi access, connecting your organization with employees, partners, and customers everywhere they go. The family of wireless products and solutions includes APs, wireless appliances, and software. Learn more about ExtremeWireless at http://www.extremenetworks.com/products/wireless/.

ExtremeXOS

ExtremeXOS, a modular switch operating system, is designed from the ground up to meet the needs of large cloud and private data centers, service providers, converged enterprise edge networks, and everything in between. Based on a resilient architecture and protocols, ExtremeXOS supports network virtualization and standards-based SDN capabilities like VXLAN gateway, OpenFlow, and OpenStack Cloud orchestration. ExtremeXOS also supports comprehensive role-based policy. Learn more about ExtremeXOS at http://www.extremenetworks.com/product/extremexos-network-operating-system/.

Index