



# Extreme Defender Application User Guide

*Version 3.31*

Copyright © 2019 Extreme Networks, Inc. All rights reserved.

## 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](http://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](http://www.extremenetworks.com/support/policies/software-licensing)

# Table of Contents

---

<b>Preface</b> .....	<b>4</b>
Text Conventions.....	4
Documentation and Training.....	4
Providing Feedback to Us.....	5
Getting Help.....	5
<b>Chapter 1: Welcome to Extreme Defender Application</b> .....	<b>7</b>
Get Started with Extreme Defender Application.....	7
Install Extreme Defender Application.....	8
Generate API Key.....	11
Upload the API Key File.....	12
Run Defender Application.....	13
Configuration Wizard.....	13
Navigate the User Interface.....	15
<b>Chapter 2: Overview</b> .....	<b>17</b>
Add a New Dashboard.....	17
Modify a Dashboard.....	18
Widgets.....	18
<b>Chapter 3: Inventory</b> .....	<b>19</b>
Inventory Device Status.....	19
View Inventory Details.....	20
Group Protected Devices from the Inventory List.....	21
Throughput Tab.....	21
Usage Tab.....	22
<b>Chapter 4: Protected Devices</b> .....	<b>24</b>
Protected Device Status.....	25
View Protected Device Details.....	25
Group Devices from the Protected Devices List.....	27
Movements Tab.....	28
Policy Generator.....	28
<b>Chapter 5: Policy</b> .....	<b>36</b>
Roles.....	36
Groups.....	37
<b>Chapter 6: Administration</b> .....	<b>39</b>
Activation.....	39
Accounts.....	42
Licensing.....	45
Preferences.....	46
<b>Glossary</b> .....	<b>48</b>
<b>Index</b> .....	<b>50</b>





# Preface

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

## 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.
<i><b>New!</b></i>	New Content	Displayed next to new content. This is searchable text within the PDF.

**Table 2: Text Conventions**

Convention	Description
<code>Screen displays</code>	This typeface indicates command syntax, or represents information as it appears on the screen.
The words <b>enter</b> and <b>type</b>	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.”
<b>[Key]</b> names	Key names are written with brackets, such as <b>[Return]</b> or <b>[Esc]</b> . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press <b>[Ctrl]+[Alt]+[Del]</b>
<i>Words in italicized type</i>	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/](http://www.extremenetworks.com/documentation/)

Archived Documentation (for earlier versions and legacy products)

[www.extremenetworks.com/support/documentation-archives/](http://www.extremenetworks.com/support/documentation-archives/)

Release Notes	<a href="http://www.extremenetworks.com/support/release-notes">www.extremenetworks.com/support/release-notes</a>
Hardware/Software Compatibility Matrices	<a href="https://www.extremenetworks.com/support/compatibility-matrices/">https://www.extremenetworks.com/support/compatibility-matrices/</a>
White papers, data sheets, case studies, and other product resources	<a href="https://www.extremenetworks.com/resources/">https://www.extremenetworks.com/resources/</a>

## 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/](http://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](mailto: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:

<b>Extreme Portal</b>	Search the GTAC (Global Technical Assistance Center) knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
<b>The Hub</b>	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.
<b>Call GTAC</b>	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: <a href="http://www.extremenetworks.com/support/contact">www.extremenetworks.com/support/contact</a>

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](http://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

Get Started with Extreme Defender Application  
Install Extreme Defender Application  
Generate API Key  
Upload the API Key File  
Run Defender Application  
Configuration Wizard  
Navigate the User Interface

Extreme Defender Application provides security management 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.

Extreme Defender Application is installed as a container application on the ExtremeCloud Appliance. The application runs and is upgraded independently from the appliance. Before accessing Extreme Defender Application, you must generate an API key from ExtremeCloud Appliance and upload it to the appliance. Subsequent upgrades can use the previously installed API key file.

For more information about *REST API Access for Docker Container Applications* see <https://extremenetworks.com/documentation/extremecloud-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.

## Related Links

[Get Started with Extreme Defender Application](#) on page 7

[Install Extreme Defender Application](#) on page 8

[Configuration Wizard](#) on page 13

[Navigate the User Interface](#) on page 15

[Sites in Extreme Defender Application](#) on page 40

[Activation](#) on page 39

[Policy Generator](#) on page 28

[Administration](#) on page 39

## **NEW!** Get Started with Extreme Defender Application

The following is the basic workflow for setting up Extreme Defender Application:

- 1 From ExtremeCloud Appliance, go to **Administration > Applications** and install Extreme Defender Application.
- 2 From ExtremeCloud Appliance, generate an API key and upload it for the Extreme Defender Application.
- 3 When you access Defender for the first time, the application runs the Defender Initial Configuration Wizard.
- 4 (Optional) From ExtremeCloud Appliance, clone the default Defender site `DFNDR_SITE` to create additional sites if necessary.
- 5 (Optional) From ExtremeCloud Appliance, create additional adoption rules if necessary.
- 6 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](#). For deployment information specific to Extreme Defender Application, refer to the [Extreme Defender for IoT Solution Deployment Guide](#).
- 7 (Optional) The Defender wizard automatically onboards managed devices. You can optionally pre-register managed devices to sites other than the default site. From Extreme Defender Application, go to **Administration > Activation**.
- 8 Run Policy Generator.
  - a From Extreme Defender Application, go to **Protected Devices**.
  - b Select an onboarded, active device.
  - c Select the **Policy Generator** tab.

### Related Links

- [Install Extreme Defender Application](#) on page 8
- [Configuration Wizard](#) on page 13
- [Sites in Extreme Defender Application](#) on page 40
- [Activation](#) on page 39
- [Policy Generator](#) on page 28

## Install Extreme Defender Application

### Note




Before you can access Extreme Defender Application you must install ExtremeCloud Appliance and generate an API key for access to Extreme Defender Application. For more information, refer to <https://extremenetworks.com/documentation/extremecloud-appliance>. We offer installation guides, an installation video, and information about *REST API Access for Docker Container Applications* in the ExtremeCloud Appliance User Guide.

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 Log into ExtremeCloud Appliance as a full administrator.
- 2 Go to **Administration > Applications**.
- 3 Select  to add an application to ExtremeCloud Appliance.
- 4 Install from a local **File** or docker hub **Registry**.
- 5 To install directly from the docker hub, select **Registry**, then **OK**. Or,
- 6 To install a local file, select **File > Upload**.
- 7 Navigate to the docker file and select **Open**.
- 8 Select **OK**.

The application is uploaded and installed on ExtremeCloud Appliance.

Before accessing Extreme Defender Application, generate an API key file in ExtremeCloud Appliance.

#### Related Links

- [Generate API Key](#) on page 11
- [Get Started with Extreme Defender Application](#) on page 7
- [Upgrade an Application](#) on page 9
- [Uninstall an Application](#) on page 9
- [Defender Application in an Availability Pair](#) on page 10




## Upgrade 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

- [Install Extreme Defender Application](#) on page 8
- [Uninstall an Application](#) on page 9



## Uninstall 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

[Install Extreme Defender Application](#) on page 8

[Upgrade an Application](#) on page 9

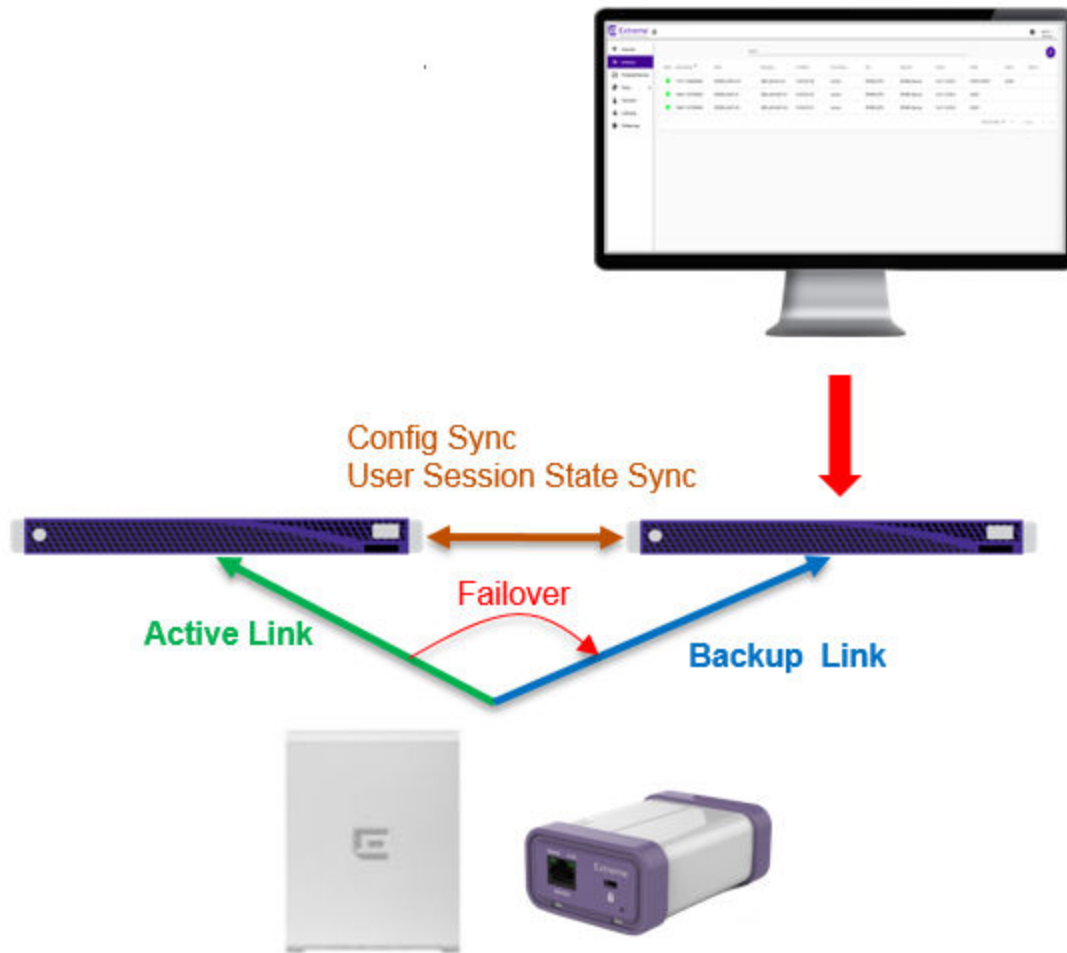
## Defender Application in an Availability Pair

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**

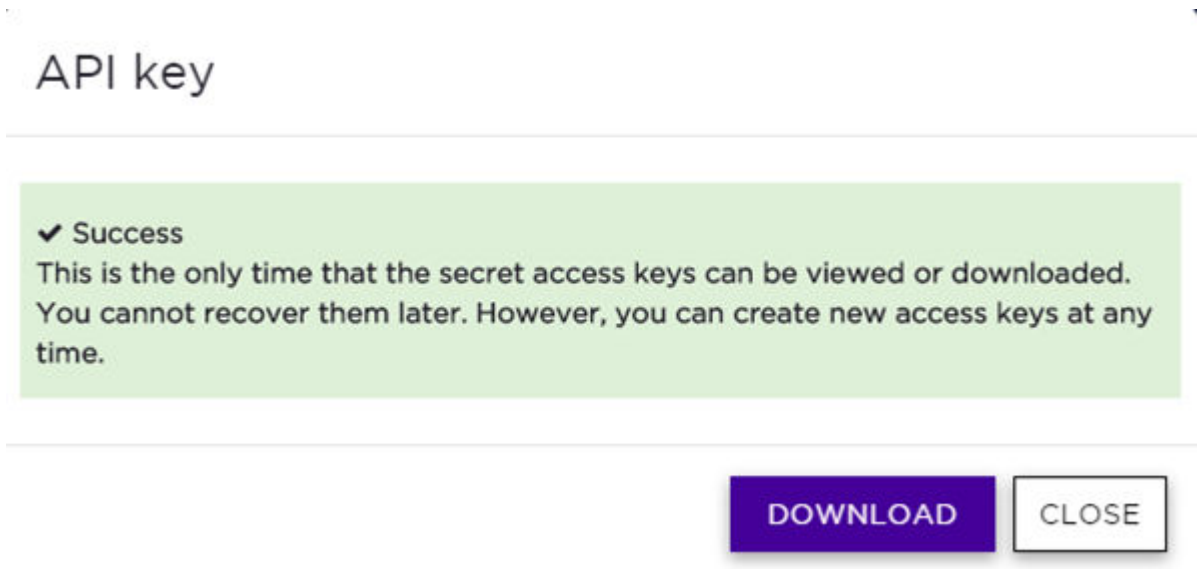
## **NEW!** Generate API Key

To generate an API key in ExtremeCloud Appliance:

- 1 Log into ExtremeCloud Appliance with administrator credentials.
- 2 Go to **Administration > Accounts**.
- 3 Select a user account.

- From the API Keys field, select **Generate New API Key**.

The key is generated. The **API Key** dialog displays.



**Figure 2: API Key dialog**

- To download the API key as a .json file, select **Download**.  
Download the key immediately. If you select **Close**, you will not be able to access the key. You can generate additional keys at any time.
- After you download the key, select **Close**.



#### Related Links

[Upload the API Key File](#) on page 12

## **NEW!** Upload the API Key File

Associating an API key file (configuration file) with Extreme Defender Application allows Defender access to the ExtremeCloud Appliance REST API. Before you can perform this task, generate the API key file.

To upload a generated API key file:

- Log into ExtremeCloud Appliance with full administrator credentials.
- Go to **Administration > Applications** and select .
- Select the **Configuration Files** tab.
- Select **api-keys.json**, and then select the upload icon .
- Upload the API key file one of the following ways:
  - Click the **Choose File** box and navigate to the downloaded API key file.
  - Drag and drop the downloaded API key file onto the **Choose File** box.

The API key file displays in the **Configuration Files** list.

You are now ready to access Extreme Defender Application.

#### Related Links

[Run Defender Application](#) on page 13

[Generate API Key](#) on page 11


## Run Defender Application

---







Before you run Extreme Defender Application, you must do the following:

- 1 Download and install the Defender docker file.
- 2 Generate an API key and upload the API key file to Defender.

To run the Extreme Defender Application:

- 1 Go to **Administration > Applications**.
- 2 Select  to start the application.

The following describes the available application actions:

-  — Install new application.
-  — 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/apps/defender` into the URL field.

#### Related Links

[Configuration Wizard](#) on page 13

## Configuration Wizard

---

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 ▼

Default Site  
DFNDR\_SITE

Create auto-provisioning rules for new access-points

Enable Wireless Radios on 3912 Access-Points

Run Setup

### Figure 3: 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 (Optional) You can rename the default Defender site.
- 3 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.
- 4 Check **Enable Wireless Radios on 3912 Access-Points**.  
Enable this option to allow wireless clients onto your network.
- 5 Select **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:

- |                        |   |
|------------------------|---|
| <b>1 site</b>          | DFNDR_SITE. You can specify a unique name.  |
| <b>2 device groups</b> | <ul style="list-style-type: none"> <li>• DFNDR_Devices for AP3912i access points.</li> <li>• DFNDR_SA201_Devices for SA201 adapters.</li> </ul> |

1 network service	DFNDR_Service
2 adoption rules	One rule for each device group.
2 device group configuration Profiles	<ul style="list-style-type: none"> <li>• DFNDR_SA201 for wired SA201 adapters</li> <li>• DFNDR for wireless AP3912i access points.</li> </ul>
1 RF Profile	DFNDR_ACS
2 policy roles	<ul style="list-style-type: none"> <li>• DFNDR_DenyAll denies all traffic by default action.</li> <li>• DFNDR_PolicyGeneration – Has a contain to VLAN default action and is associated with a Bridged at AP untagged topology.</li> </ul>

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

#### Related Links

[Sites in Extreme Defender Application](#) on page 40

[Roles](#) on page 36

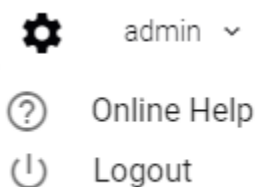
## Navigate the User Interface

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.
- **Administration.** Perform system administration including managing accounts, configuring tagging, activating devices, licensing, and configuring system preferences.

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




**Figure 4: Defender Admin Menu**

Additionally, select  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.

Select  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

## Add a New Dashboard Modify a Dashboard Widgets

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

## Add a New Dashboard

Create additional dashboards to organize data.

To add a new dashboard:

- 1 From the default dashboard, select the plus sign.
- 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 Select  to save the dashboard.

### Related Links

[Modify a Dashboard](#) on page 18


[Widgets](#) on page 18

## Modify a Dashboard

---

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

To modify a dashboard:

- 1 Go to **Overview**.  
The **Default** dashboard is displayed.
- 2 Select the **Widgets** tab to view the list of available widgets.
- 3 Drag and drop a widget on to the dashboard.
- 4 To delete a widget report, select .

### Related Links

[Widgets](#) on page 18

[Add a New Dashboard](#) on page 17

## 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:

<b>Device Vendors</b>	The number of protected devices by device vendor.
<b>Devices by Throughput</b>	The top protected devices by throughput (kilobits per second).
<b>Throughput</b>	Network throughput (kilobits per second) in 10-minute intervals.
<b>Usage</b>	Network usage (RxBytes and TxBytes) in 10-minute intervals.
<b>AP and Adapter Status</b>	<p>Graphs the number of APs or adapters by status. Valid status values are:</p> <ul style="list-style-type: none"> <li>• Green — In-Service. Device has discovered ExtremeCloud Appliance and is providing service.</li> <li>• Yellow — In-Service Trouble. Device has discovered ExtremeCloud Appliance but it is not a member of a device group.</li> <li>• Grey — Unknown. Device is added to ExtremeCloud Appliance but the device has never discovered ExtremeCloud Appliance .</li> <li>• Red — Critical. After being Active, Discovered, and On-boarded, associated device is no longer connected to ExtremeCloud Appliance.</li> </ul>

### Related Links

[Add a New Dashboard](#) on page 17

[Modify a Dashboard](#) on page 18

# 3 Inventory

---

**Inventory Device Status**

**View Inventory Details**

**Group Protected Devices from the Inventory List**

**Throughput Tab**

**Usage Tab**

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
- Name
- Asset ID
- Description
- Tag
- IP Address
- Site
- Networks
- Version
- Model

Select  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 16

[Inventory Device Status](#) on page 19





[View Inventory Details](#) on page 20

---

## 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.

## View Inventory Details

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

- 1 Go to **Inventory** and select a device from the list.
- 2 You have the option to provide the following information:

**Asset ID** Provide the Asset ID of the device. This is an arbitrary ID intended for device tracking.

## Available Details

The following additional information is provided for each device:

- Name
- Description
- Status
- Serial Number
- MAC Address
- IP Address
- Gateway
- Hardware Type
- Version
- Site
- Networks
- Wired Clients
- Wireless Clients
- Tag — You have the option to select a tag from the list. Associating a tag with a device can control which users see the device. Tags can also be assigned when setting up user accounts.
- Number of Protected Devices associated with the selected device. (Available for the AP3912i only):
  - Number of Wired Devices
  - Number of Wireless Devices
- Assigned group for the protected device.

## Available Tabs

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.

Select  to refresh the chart data.

### Related Links

- [Throughput Tab](#) on page 21
- [Usage Tab](#) on page 22
- [Group Protected Devices from the Inventory List](#) on page 21
- [Inventory](#) on page 19
- [Manage Tags](#) on page 43
- [Account Tagging](#) on page 44

## Group 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 Select **Save**.



### Note

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

### Related Links


- [Group Devices from the Protected Devices List](#) on page 27
- [Manage Groups](#) on page 37

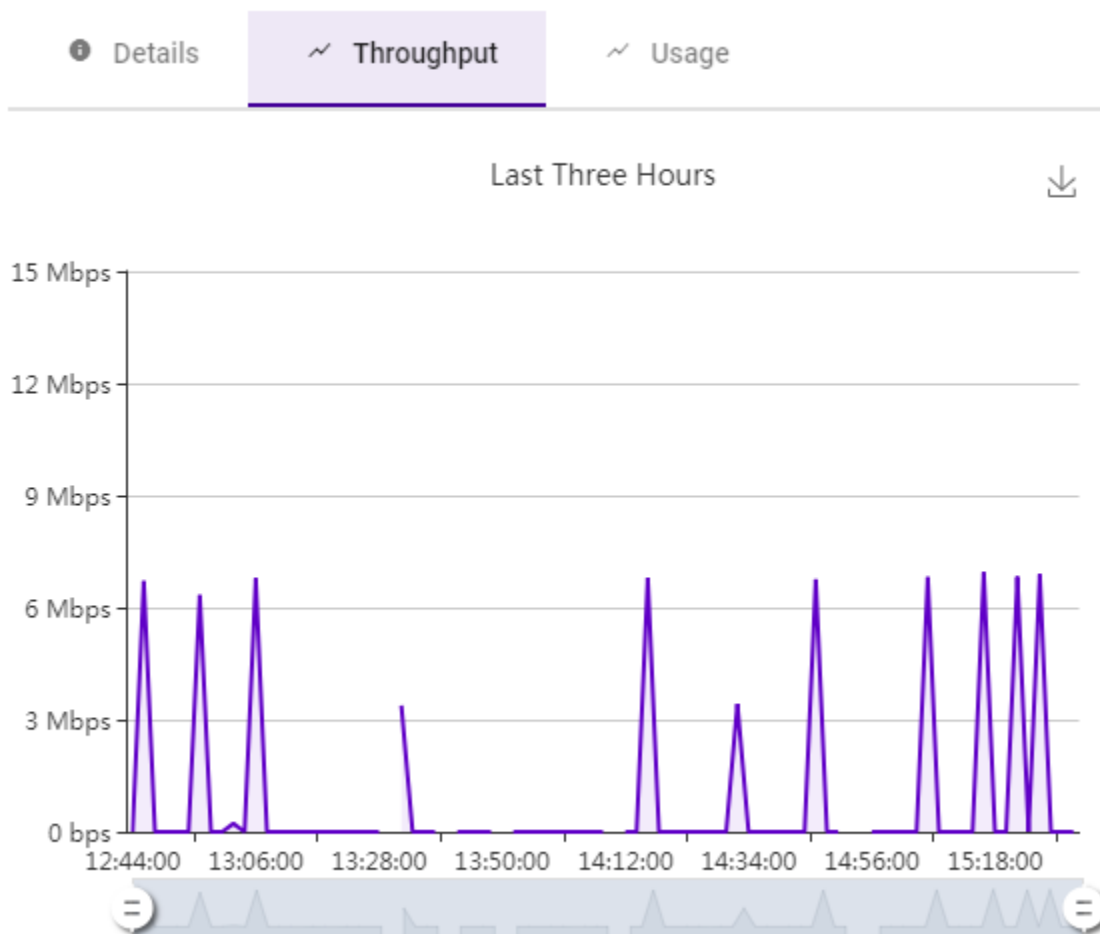
## Throughput Tab

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. Select  to refresh the chart on demand.


Select  to download the chart in .png format.




**Figure 5: AP Inventory Device Throughput (Mbps)**

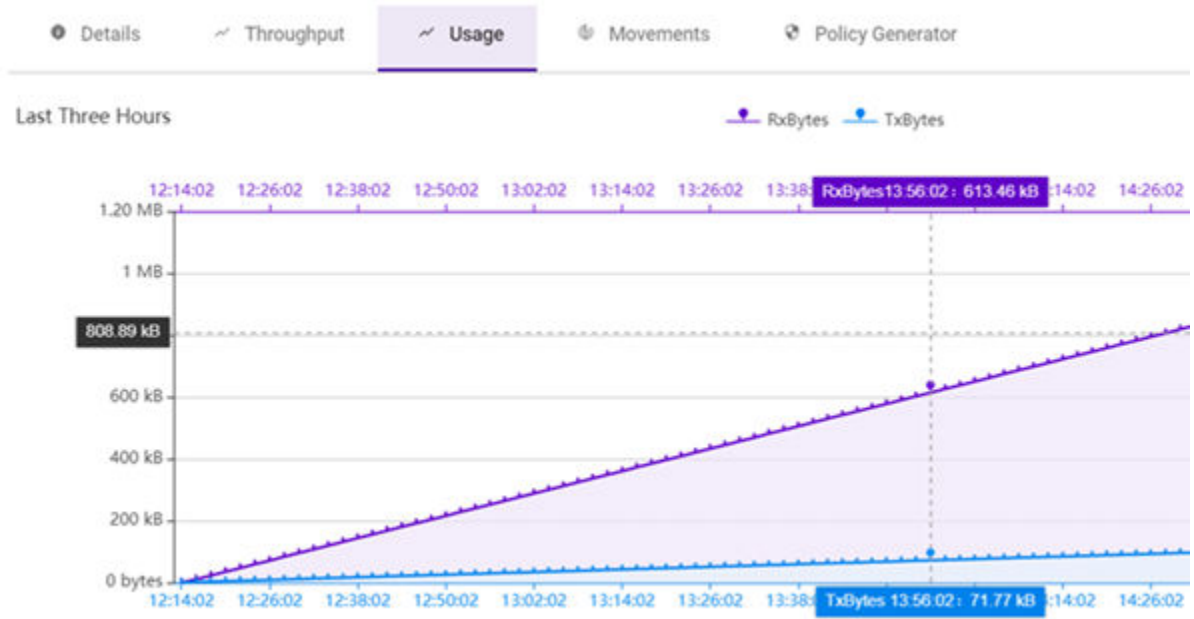
## Usage Tab

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. Select  to refresh the chart on demand.

Select  to download the chart in .png format.

The **Usage** tab is available from both the **Inventory Details** page and the **Protected Device** Details page.



**Figure 6: Protected Device Usage**

# 4 Protected Devices

Protected Device Status

View Protected Device Details

Group Devices from the Protected Devices List

Movements Tab

Policy Generator

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
- Licensed
- Name
- Asset ID
- IP Address
- Site
- Assigned Group
- Assigned Role
- Service
- Host Name
- Last Seen
- AP/Adapter

Select  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 16

[View Protected Device Details](#) on page 25










[Group Devices from the Protected Devices List](#) on page 27

## 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: <ul style="list-style-type: none"> <li>Discovered ExtremeCloud Appliance</li> <li>On-boarded with a policy role</li> <li>Actively sending data.</li> </ul>
	Not On-board. Device: <ul style="list-style-type: none"> <li>Discovered ExtremeCloud Appliance</li> <li>Actively sending data</li> <li>Not on-boarded. To on-board a Protected Device, add it to a group that has an assigned policy role.</li> </ul>
	Inactive. Device: <ul style="list-style-type: none"> <li>On-boarded with a policy role.</li> <li>Not actively sending data.</li> </ul>
	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

[Group Devices from the Protected Devices List](#) on page 27

## View 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.
- 2 You have the option to provide the following information:

**Name** Provide a name for a protected device.

**Description** Provide a description of the protected device.

**Asset ID** Provide the Asset ID of the protected device. This is an arbitrary ID intended for device tracking.

## Available Details

The following additional information is provided for each protected device:

- Status (For active protected devices only)
- Licensed
- Last Seen
- Device Type
- Manufacturer
- Host Name
- MAC Address
- IP Address
- AP/Adapter Name
- AP/Adapter Serial Number
- Group (For active protected devices only)
- Assigned Role (For active protected devices only)
- Last Assigned Group (For archived protected devices only)
- Last Assigned Role (For archived protected devices only)

## Available Tabs

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
- Name of source AP
- Name 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.

Select  to refresh the device and chart data.

### Related Links

[Throughput Tab](#) on page 21


[Usage Tab](#) on page 22

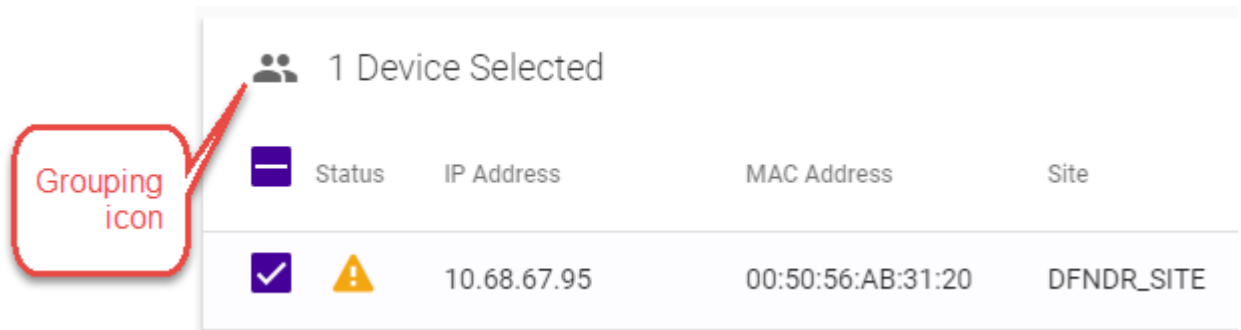
[Movements Tab](#) on page 28

[Policy Generator](#) on page 28

## Group 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:

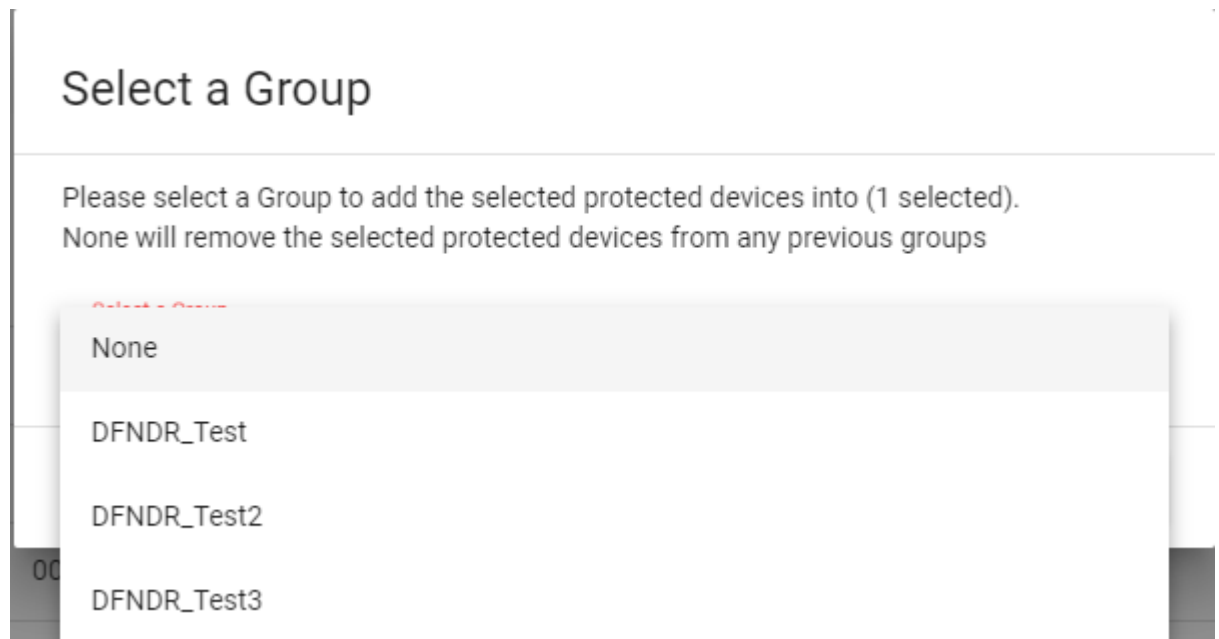
- 1 Go to **Protected Devices**.
- 2 Select the check box for one or more devices.
- 3 Select the group icon 



**Figure 7: 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.



**Figure 8: Selecting a Group**

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

- 5 Select **OK**.

**Note**

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

**Related Links**

[Group Protected Devices from the Inventory List](#) on page 21

[Manage Groups](#) on page 37

## Movements Tab

As protected devices get moved from one location to another, you can track and manage information about the specific device location.

- 1 Go to **Protected Devices** and select a device from the list.
- 2 Select the **Movements** tab.
- 3 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
- Name of source AP
- Name 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 16

[Policy Generator](#) on page 28

## 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.

**Note**

Only users with Full Admin access can run Policy Generator.

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, and configures policy rules based on the contents of the .pcap file. You edit the generated role, providing a unique name and modifying the generated rules if necessary, then save the generated role. For more information, see [Run Policy Generator](#) on page 29.

**Note**

A copy of DFNDR\_PolicyGeneration role is created temporarily for the duration of the packet capture. This temporary role is automatically deleted after the packet capture is completed.

Defender supports up to 10 simultaneous PCAP sessions.

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**

[Run Policy Generator](#) on page 29

[L2 Rules](#) on page 32

[Configure L3 and L4 Rules](#) on page 33

[Allow DNS, DHCP, and Well-Known Port Traffic Automatically](#) on page 34

**Run Policy Generator**

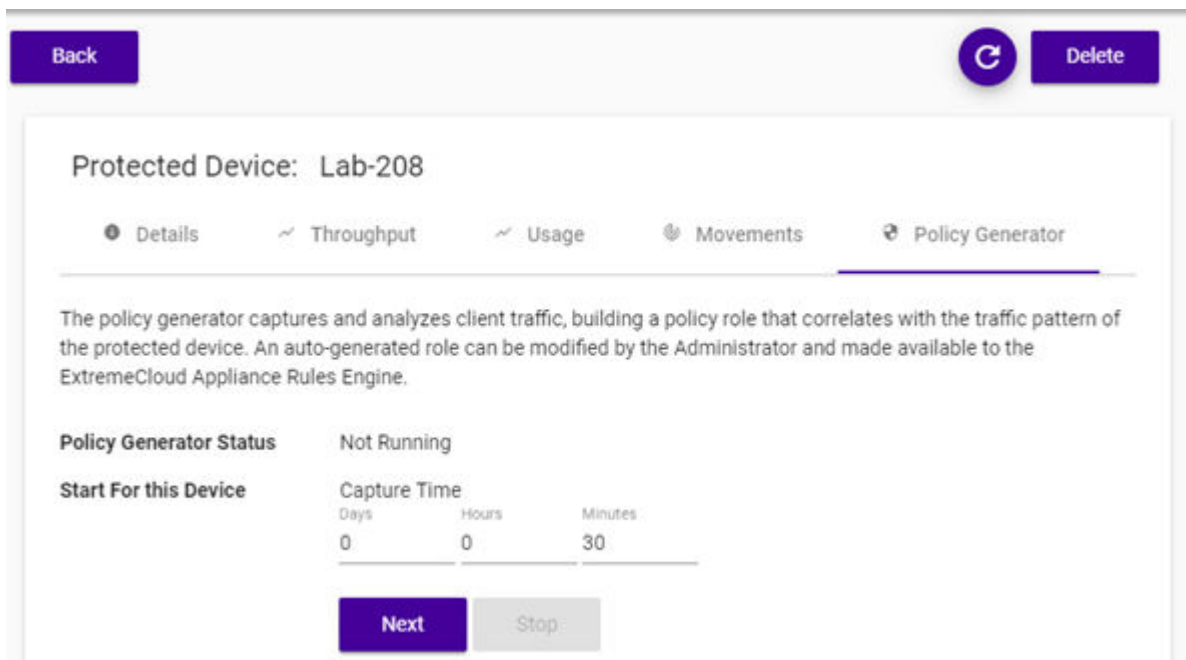
Access Policy Generator from an active protected device on the **Protected Devices** list.

**Note**

Only users with Full Admin access can run Policy Generator. 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 select a device with a status of Active (on-boarded).

- 2 Select the **Policy Generator** tab.



**Figure 9: 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 Select **Next**.
- 5 Select a VLAN ID for the VLAN that the protected device belongs to, and select **Start**.

Figure 10 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 10: Protected Device in Capture Mode**

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

- 7 Provide a name for the generated role using the DFNDR\_ prefix.

You can edit the generated Layer 3 and Layer 4 rules. You can also create new Layer 2-7 rules before saving the generated role.



#### Note

Once you have saved the generated role, you cannot modify or create new rules.

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

#### Related Links

[Policy Generator](#) on page 28

[L2 Rules](#) on page 32

[Configure L3 and L4 Rules](#) on page 33

[L7 Rules](#) on page 33

[Allow DNS, DHCP, and Well-Known Port Traffic Automatically](#) on page 34

## Modify 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.

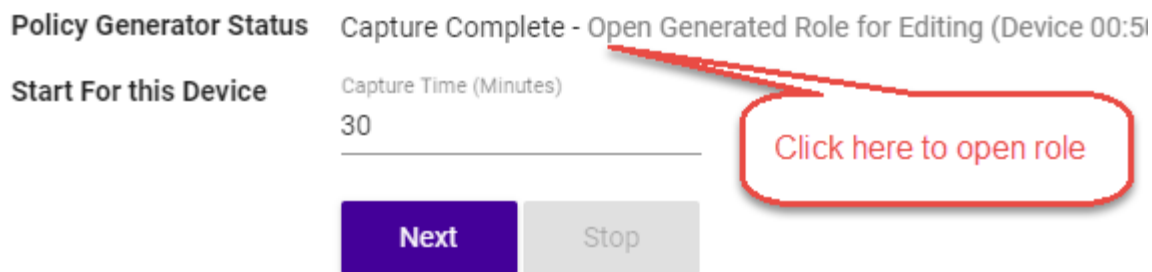


#### Note

New rules can be created for auto-generated roles in Extreme Defender Application before you save the generated role. Once you have saved the generated role, you cannot modify or create new rules.

To modify a generated role, take the following steps:

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



**Figure 11: 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
- 4 Provide a VLAN ID.
- 5 Modify or add rules as necessary before saving the role.

### Related Links

- [L2 Rules](#) on page 32
- [Configure L3 and L4 Rules](#) on page 33
- [L7 Rules](#) on page 33

### L2 Rules

Once auto generation completes, you open the generated role for editing. At this point, you can create Layer 2 rules (before you save the generated role).



#### Note

Once you have saved the generated role, you cannot modify or create new rules.

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

- 1 Go to **Policy > Roles** and select a role.
- 2 Select the drop-down arrow next to the L2 Rules pane and select **New**.
- 3 The following rule parameters display:

<b>Name</b>	Provide a name for the rule.
<b>Action</b>	Determines access control action for the rule. Valid values are: <ul style="list-style-type: none"> <li>• Allow - Packets contained to role's default action's VLAN/topology</li> <li>• Deny - Any packet not matching a rule in the policy is dropped.</li> <li>• Containment VLAN - A topology to use when a network is created using a role that does not specify a topology.</li> </ul>
<b>MAC Address Type</b>	Any MAC indicates no filtering on MAC Address. User Defined MAC displays a MAC Address field. Provide a specific MAC Address.

- 4 Select **Save** to save the role after creating and editing rules.  
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

- [Modify Policy Generator Roles](#) on page 31
- [Configure L3 and L4 Rules](#) on page 33
- [L7 Rules](#) on page 33



## Configure L3 and L4 Rules

For auto-generated roles that create Layer 3 and 4 rules, you can modify the rules and create new rules before saving the role.



### Note

Once you have saved the generated role, you cannot modify or create new 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:

<b>Name</b>	Provide a name for the rule.
<b>Action</b>	Determines access control action for the rule. Valid values are: <ul style="list-style-type: none"> <li>• Allow - Packets contained to role's default action's VLAN/topology</li> <li>• Deny - Any packet not matching a rule in the policy is dropped.</li> <li>• Containment VLAN - A topology to use when a network is created using a role that does not specify a topology.</li> </ul>
<b>Protocol</b>	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: <ul style="list-style-type: none"> <li>• 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.</li> <li>• A specific protocol from the list.</li> </ul>
<b>IP Subnet</b>	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: <ul style="list-style-type: none"> <li>• User Defined. Specify the destination IP address and mask. Use this option to explicitly define the IP/subnet aspect of the rule.</li> <li>• Any IP - Maps the rule to the associated Topology IP address.</li> <li>• Select a specific subnet value - Select to map the rule to the associated topology segment definition (IP address/mask).</li> </ul>
<b>Port Type</b>	The port type associated with the defined rule. Traffic from this port is subject to the defined rule. Valid values are: <ul style="list-style-type: none"> <li>• User Defined, then type the port number. Use this option to explicitly specify the port number.</li> <li>• A specific port type.</li> </ul>
<b>Port Number/Range</b>	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

[Modify Policy Generator Roles](#) on page 31

[L2 Rules](#) on page 32

[L7 Rules](#) on page 33

**NEW!** L7 Rules

Once auto generation completes, you open the generated role for editing. At this point, you can create Layer 7 rules (before you save the generated role).

**Note**

Once you have saved the generated role, you cannot modify or create new rules.

To configure an OSI Layer 7 rule that restricts or limits network traffic:

- 1 Go to **Policy > Roles** and select a role.
- 2 Select the drop-down arrow next to the L7 Rules pane and select **New**.
- 3 The following rule parameters display:

**Name** Rule name.

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

- Allow
- Deny

**Application Group** Internet applications are organized in groups based on the type or purpose of the application. After you select an Application Group, the Application Name drop-down is populated with application names that are part of the specified group.

**Application Name** Names of applications that are a member of the specified group.

**Related Links**

[Modify Policy Generator Roles](#) on page 31

[L2 Rules](#) on page 32

[Configure L3 and L4 Rules](#) on page 33

*Allow 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 28



# 5 Policy

## Roles Groups

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 36

[Groups](#) on page 37

## 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 28

## 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

[Manage Groups](#) on page 37

[Policy Group Settings](#) on page 37

## Manage 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, select **Add** and configure the [Policy Group Settings](#).
- To remove one or more MAC addresses from the group, select the group and then select  next to the MAC Address row you want to remove.
- To delete a group, select the group and then select **Delete**.

### Related Links

[Policy Group Settings](#) on page 37

[Group Protected Devices from the Inventory List](#) on page 21

[Group Devices from the Protected Devices List](#) on page 27

## 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 37

[Manage Groups](#) on page 37

[Roles](#) on page 36



# 6 Administration

Activation  
Accounts  
Licensing  
Preferences

Perform system administration including managing accounts, configuring tagging, activating devices, licensing, and configuring system preferences.

## Related Links

[Activation](#) on page 39  
[Manage Tags](#) on page 43  
[Accounts](#) on page 42  
[Licensing](#) on page 45  
[Preferences](#) on page 46

## Activation

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

### Note



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](#).

For deployment information specific to Extreme Defender Application, refer to the [Extreme Defender for IoT Solution Deployment Guide](#).

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.

You can also specify the site during device activation from within Extreme Defender Application.

## Related Links

[Sites in Extreme Defender Application](#) on page 40  
[Scan a QR Code](#) on page 40  
[Manual Onboarding](#) on page 41

[Use a CSV File](#) on page 41

[Configuration Wizard](#) on page 13

## **NEW!** Sites in Extreme Defender Application

The option to create auto-provisioning rules for new access points in the **Initial Configuration Wizard** automates the process of adding the SA201 adapter or AP3912i to Extreme Defender Application. Upon connecting an SA201 adapter or AP3912i device to the network, the device discovers ExtremeCloud Appliance, and is automatically assigned to its associated device group under the default site name "DFNDR\_SITE". (You can provide a unique site name.)

Each device group within the site must contain devices of the same model. The default name for device groups that hold AP3912i access points is `DFNDR_Devices`. The default name for device groups that hold Defender adapters is `DFNDR_SA201_Devices`. These specific device group names are required for Defender devices.



### Note

Do not modify device group names.

It is possible to create additional sites with device groups on ExtremeCloud Appliance for your Defender devices. However, the device groups within each site must have the default device group names. A best practice is to clone the default Defender site. This will ensure that you have device groups with the required name for each device type.



### Note

When adding a new SA201 adapter or AP3912i device to your network, ExtremeCloud Appliance upgrades images to the baseline version that is associated with the ExtremeCloud Appliance release version. Allow newly connected devices time to start, upgrade, and then restart.

Upon discovery of ExtremeCloud Appliance, if the Defender devices are not assigned to the correct site and device group, verify the device group names. For more information, refer to the following topics in the [ExtremeCloud Appliance User Guide](#) or Online Help:

- *Sites Overview*
- *Modifying Site Configuration*

## Scan a QR Code

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

- 1 Go to **Administration > 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 **Provision a new Access Point or Adapter** dialog opens.



- 4 Select from the list of configured sites in ExtremeCloud Appliance. When you select **Default**, the site is assigned using the Defender adoption rules present on ExtremeCloud Appliance. This is the default value.



#### Note

Before selecting a site for device provisioning, the site and device groups must be configured on ExtremeCloud Appliance. For more information about sites and device groups for Defender devices, refer to [Sites in Extreme Defender Application](#) on page 40.

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

#### Related Links

[Activation](#) on page 39

## Manual Onboarding

To manually provision an access point or adapter:

- 1 Go to **Administration > Activation** and select **Manual Onboarding**.
- 2 Configure the following parameters:

**Serial Number** The serial number of the AP or adapter.

**Model** Select from the list of supported device models.

**Site** Select from the list of configured sites in ExtremeCloud Appliance. When you select **Default**, the site is assigned using the Defender adoption rules present on ExtremeCloud Appliance. This is the default value.



#### Note

Before selecting a site for device provisioning, the site and device groups must be configured on ExtremeCloud Appliance. For more information about sites and device groups for Defender devices, refer to [Sites in Extreme Defender Application](#) on page 40.

**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 39

[Sites in Extreme Defender Application](#) on page 40

## Use a CSV File

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

- 1 Go to **Administration > Activation** and do one of the following:
  - Select 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 select **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, site
1701Y-1248300023, AP3912i-FCC, TestAp, "description1", DFNDR_Area51
1701Y-1248300024, AP3912i-FCC, TestAp1, "description2", DFNDR_Area61
```

#### Note



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

If you do not specify a site value, Defender places the devices in the appropriate default Defender device group.

#### Related Links

[Activation](#) on page 39

[Sites in Extreme Defender Application](#) on page 40

## NEW! Accounts

It is possible to create user accounts that are local to Extreme Defender Application. Log into Defender as a Full Admin. Then, create and manage user accounts from the **Administration > Accounts** page.

Extreme Defender Application supports the following account types:

- Full** An admin account with full access to the Extreme Defender Application. The Full-Admin has access to all functionality in Extreme Defender Application, and the account is synced in a High Availability Pair of appliances. A Full-Admin can accomplish the following tasks in Extreme Defender Application:
- Create accounts
  - Run Auto Policy Generator
  - Install and manage product licenses
  - Create and manage policy roles
  - Create and manage account tags



#### Note

A user with **Full** admin access does not have access to ExtremeCloud™ Appliance configuration.

- User** An admin account with limited access to Extreme Defender Application functionality. A person with **User** access can accomplish the following tasks:
- View and create dashboards.
  - View and interact with items on the **Inventory List**.
  - View and interact with items on the **Protected Devices List**. It is possible to restrict access to devices that are assigned to a user category.
- Read-Only** Read-only access to the Extreme Defender Application. It is possible to restrict read-only access to devices that are assigned to a user category.

ExtremeCloud Appliance users have access to Extreme Defender Application.

#### Related Links

[Manage Accounts](#) on page 43

## **NEW!** Manage Accounts

A user with Full access to Extreme Defender Application can create, modify, and delete user accounts.

### *Create a User Account*

- 1 Go to **Administration > Accounts > Add**.
- 2 Configure the following parameters:

<b>Name</b>	User name for this account.
<b>Password</b>	Password for this account.
<b>Confirm Password</b>	Enter password again to confirm.
<b>Access</b>	User access level. Valid values are: <ul style="list-style-type: none"> <li>• Full</li> <li>• User</li> <li>• Read-Only</li> </ul>

See [Accounts](#) on page 42 for a complete description of each access level.

<b>Tags</b>	Categories used to filter the content that a user can manage. For more information, see <a href="#">Account Tagging</a> on page 44.
-------------	---

- 3 Select **Save**.



#### **Note**

Extreme Defender Application has a limit of 100 user accounts.

### *Modify a User Account*

- 1 Go to **Administration > Accounts** and select a user account from the list.
- 2 Modify the account settings. For a description of each setting, see [Create a User Account](#) on page 43.

### *Delete a User Account*

- 1 Go to **Administration > Accounts** and select a user account from the list.
- 2 Select **Delete**.

### Related Links

[Accounts](#) on page 42

[Account Tagging](#) on page 44

## **NEW!** Manage Tags

Use tags to control which devices a user can manage in Extreme Defender Application. Administrators define a list of tags on the **Administration** workbench, then use those tags when creating user accounts and configuring devices on the **Inventory** list. When tags are used, users are limited to devices and device reports that use the tags that match their user account.

Tagging is an optional feature that facilitates device filtering in Extreme Defender Application. If tags are not used on a user account, that user can see all devices, and a device that is not tagged can be viewed by all users.

### *Add a Tag*

To add a tag to Extreme Defender Application:

- 1 Go to **Administration > Accounts > Tags > Add**.
- 2 Provide a name for the tag and select **Save**.

The tag is added to the list on the **Tags** tab.

### *Delete a Tag*

To delete a tag from Extreme Defender Application:

- 1 Go to **Administration > Accounts > Tags**.
- 2 Select the check box next to the tag and select **Delete**.

### Related Links

[Account Tagging](#) on page 44

[View Inventory Details](#) on page 20

## **NEW!** Account Tagging

Use tags when setting up a user account to control which devices a user can manage in Extreme Defender Application. A user account with an assigned tag can manage access points and adapters with the same tag. When the tags on the user account match the tags on the AP or adapter, the user can do the following:

- Manage the protected devices associated with each tagged AP or adapter
- View the following statistical information for each tagged AP or adapter:
  - Protected Device Vendors
  - Top Protected Devices by Throughput
  - 3912 Status
  - SA201 Status

You can assign up to three tags per user account. Extreme Defender Application supports no more than 200 tags per application instance.

The following rules apply to user account tagging and user access:

- When a user account is tagged, the user can manage APs and adapters with no tags, or manage devices with the same tags that are specified on the user account.
- Users with no assigned tags can manage all APs and adapters.
- ExtremeCloud Appliance admin users can manage all APs and adapters.
- ExtremeCloud Appliance read-only users can view the following limited information in Extreme Defender Application:
  - Dashboard widgets
  - AP or adapter information
  - Protected Device information

#### Related Links

[Manage Tags](#) on page 43

[View Inventory Details](#) on page 20

## 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 **Administration > Licensing**.
- 2 Enter one or more license keys in the **License Key** field and click **Apply**.

The screenshot shows the Extreme Defender Application Licensing Page. The navigation menu on the left includes Overview, Inventory, Protected Devices, Policy, and Administration. The Administration menu is expanded, showing Activation, Accounts, Licensing (selected), and Preferences. The main content area displays a table with the following data:

Licenses	
Maximum Supported Protected Devices:	1000
Total Licenses:	10
Used Licenses:	7
Available Licenses:	3

An 'Apply' button is located at the bottom right of the table.

**Figure 12: Defender Application Licensing Page**

Figure 12 shows that the maximum number of devices this Extreme Defender Application can protect is 1000. This instance has a total of 10 licenses. 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.


## Preferences

Customize the Extreme Defender Application from the **Preferences** workbench.

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

**Table 6: 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 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

---

## A

- accounts
  - create 43
  - edit 43
- activation for devices 39
- adapter provisioning 39
- adding 17
- administration 39
- AP provisioning 39
- API key
  - generating 11
  - using with Defender 12
- application upgrading 9
- application, uninstalling 9
- Availability Pair 10

## C

- conventions
  - notice icons 4
  - text 4
- csv file 41, 42

## D

- dashboard 17
- Defender, running 13
- device activation 39
- device grouping 21, 27
- device groups 40
- device status 19
- documentation
  - feedback 5
  - location 4, 5

## F

- filter user content 43, 44

## G

- getting started 7
- grouping devices 21, 27
- groups 37

## I

- installing Defender 8
- Inventory
  - throughput 21
  - usage 22
- Inventory details 20
- Inventory List 19

## L

- Layer 2 rules 32
- Layer 3 and 4 rules 33
- Layer 7 rules 33
- licensing 45

## M

- Movement tab 28

## O

- onboarding by csv file 41, 42
- onboarding by QR code 40
- onboarding, manually 41
- Open Source Declaration 4, 5
- OSI Layer 3 and 4 rules 33
- Overview dashboard 17

## P

- policy definition 36
- policy generator
  - modifying roles 31
  - running 29
- policy group settings 37
- policy groups 37
- preferences, user interface 46
- Protected Device
  - details 25
  - throughput 21
  - usage 22
- protected devices 24
- Protected Devices, status 25
- provisioning APs and adapters 39

## Q

- QR code scanning 40

## R

- roles
  - policy generator 28, 29
- rules, allowing DNS, DHCP, and well-known port traffic 34
- rules, configuring OSI Layer 3 and 4 rules 33
- rules, OSI Layer 2 rules 32
- rules, OSI Layer 7 rules 33

## S

- sites 40
- support, see technical support

**T**

tagging accounts 44  
tags, managing 43  
technical support  
    contacting 5, 6  
Throughput tab 21  
tracking device movement 28

**U**

Usage tab 22

**W**

widgets 18