



Extreme Defender Application User Guide

Version 3.41

9036708-00 Rev AA
May 2020



Copyright © 2020 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, see: www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

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



Table of Contents

| | |
|--|-----------|
| Preface..... | 5 |
| Text Conventions..... | 5 |
| Documentation and Training..... | 7 |
| Providing Feedback..... | 7 |
| Getting Help..... | 7 |
| Subscribe to Service Notifications..... | 8 |
| Welcome to Extreme Defender Application..... | 9 |
| Get Started with Extreme Defender Application..... | 10 |
| Install Extreme Defender Application..... | 11 |
| Upgrade an Application..... | 11 |
| Uninstall an Application..... | 12 |
| Defender Application in an Availability Pair..... | 12 |
| Generate API Key..... | 13 |
| Upload the API Key File..... | 14 |
| Run Defender Application..... | 15 |
| Configuration Wizard..... | 15 |
| Navigate the User Interface..... | 17 |
| Search Facility..... | 18 |
| Overview..... | 19 |
| Add a New Dashboard..... | 19 |
| Modify a Dashboard..... | 20 |
| Widgets..... | 20 |
| Inventory..... | 22 |
| Inventory Device Status..... | 23 |
| View Inventory Details..... | 23 |
| Available Details..... | 23 |
| Available Tabs..... | 24 |
| Group Protected Devices from the Inventory List..... | 24 |
| Throughput Tab..... | 24 |
| Usage Tab..... | 25 |
| Protected Devices..... | 27 |
| Protected Device Status..... | 28 |
| View Protected Device Details..... | 29 |
| Available Details..... | 29 |
| Available Tabs..... | 29 |
| Group Devices from the Protected Devices List..... | 30 |
| Movements Tab..... | 31 |
| Policy Generator..... | 32 |
| Run Policy Generator..... | 33 |

| | |
|---|-----------|
| Modify Policy Generator Roles..... | 35 |
| Alarms..... | 39 |
| Active Alarms..... | 39 |
| Alarm Log..... | 40 |
| Configure Alarm Settings..... | 41 |
| Logs..... | 43 |
| Policy..... | 45 |
| Roles..... | 45 |
| Groups..... | 46 |
| Manage Groups..... | 46 |
| Policy Group Settings..... | 46 |
| Administration..... | 48 |
| System..... | 48 |
| Configure Email Notification Server..... | 48 |
| UI Settings..... | 49 |
| Defender Configuration Back Up and Restore..... | 49 |
| Setup Wizard for Configuration Reset..... | 50 |
| Activation..... | 52 |
| Sites in Extreme Defender Application..... | 53 |
| Scan a QR Code..... | 53 |
| Manual Onboarding..... | 54 |
| Use a CSV File..... | 54 |
| Accounts..... | 55 |
| Manage Accounts..... | 56 |
| Manage Tags..... | 57 |
| Account Tagging..... | 57 |
| Licensing..... | 58 |
| Glossary..... | 60 |
| Index..... | 63 |



Preface

This section describes the text conventions used in this document, where you can find additional information, and how you can provide feedback to us.

Text Conventions

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

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

Table 1: Notes and warnings




| Icon | Notice type | Alerts you to... |
|---|-------------|---|
|  | Tip | Helpful tips and notices for using the product. |
|  | Note | Useful information or instructions. |
|  | Important | Important features or instructions. |

Table 1: Notes and warnings (continued)



| Icon | Notice type | Alerts you to... |
|---|-------------|--|
|  | Caution | Risk of personal injury, system damage, or loss of data. |
|  | Warning | Risk of severe personal injury. |

Table 2: Text

| Convention | Description |
|--|---|
| screen displays | This typeface indicates command syntax, or represents information as it appears on the screen. |
| The words <i>enter</i> and <i>type</i> | When you see the word <i>enter</i> 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 <i>type</i> . |
| Key names | Key names are written in boldface, for example Ctrl or Esc . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del |
| Words in <i>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. |
| NEW! | New information. In a PDF, this is searchable text. |

Table 3: Command syntax

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

Documentation and Training

Find Extreme Networks product information at the following locations:

[Current Product Documentation](#)

[Release Notes](#)

[Hardware/software compatibility matrices](#) for Campus and Edge products

[Supported transceivers and cables](#) for Data Center products

[Other resources](#), like white papers, data sheets, and case studies

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

Providing Feedback

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

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

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

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

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

Getting Help

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

[Extreme Portal](#)

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

[The Hub](#)

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

[Call GTAC](#)

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

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

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

Subscribe to 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 (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. Select **Submit**.



Welcome to Extreme Defender Application

[Get Started with Extreme Defender Application](#) on page 10

[Install Extreme Defender Application](#) on page 11

[Generate API Key](#) on page 13

[Upload the API Key File](#) on page 14

[Run Defender Application](#) on page 15

[Configuration Wizard](#) on page 15

[Navigate the User Interface](#) on page 17

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.

With Extreme Defender Application, you can:

- Configure alarms that indicate device status and receive email notification when an alarm is triggered.
- Back up and restore your Defender configuration.
- Keep track of administrator system activity using the Defender audit log feature.

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 Topics

[Get Started with Extreme Defender Application](#) on page 10

[Install Extreme Defender Application](#) on page 11

- [Configuration Wizard](#) on page 15
- [Navigate the User Interface](#) on page 17
- [Sites in Extreme Defender Application](#) on page 53
- [Activation](#) on page 52
- [Alarms](#) on page 39
- [Logs](#) on page 43
- [Policy Generator](#) on page 32
- [Administration](#) on page 48

Get Started with Extreme Defender Application

Extreme Defender Application is installed as a container application on ExtremeCloud Appliance. The application runs and is upgraded independently from the appliance. [Table 4](#) outlines the appliance support matrix for Extreme Defender Application.

Table 4: Extreme Defender Application Support for ExtremeCloud Appliance

| Extreme Defender Application | ExtremeCloud Appliance |
|------------------------------|--------------------------|
| Version 3.41 | Version 4.76.04 or later |
| Version 3.31 | Version 4.56 or later |

The following is the basic work flow 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 Configuration 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 Topics

- [Install Extreme Defender Application](#) on page 11

[Configuration Wizard](#) on page 15
[Sites in Extreme Defender Application](#) on page 53
[Activation](#) on page 52
[Policy Generator](#) on page 32

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 Defender. 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 Portal](#). Then, use the following procedure to install Defender 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.

9. Generate an API key on ExtremeCloud Appliance and associate it with the application before running the application.

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

Related Topics

[Generate API Key](#) on page 13
[Get Started with Extreme Defender Application](#) on page 10
[Upgrade an Application](#) on page 11
[Uninstall an Application](#) on page 12
[Defender Application in an Availability Pair](#) on page 12

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 Topics

[Install Extreme Defender Application](#) on page 11

[Uninstall an Application](#) on page 12

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 Topics

[Install Extreme Defender Application](#) on page 11

[Upgrade an Application](#) on page 11

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>.

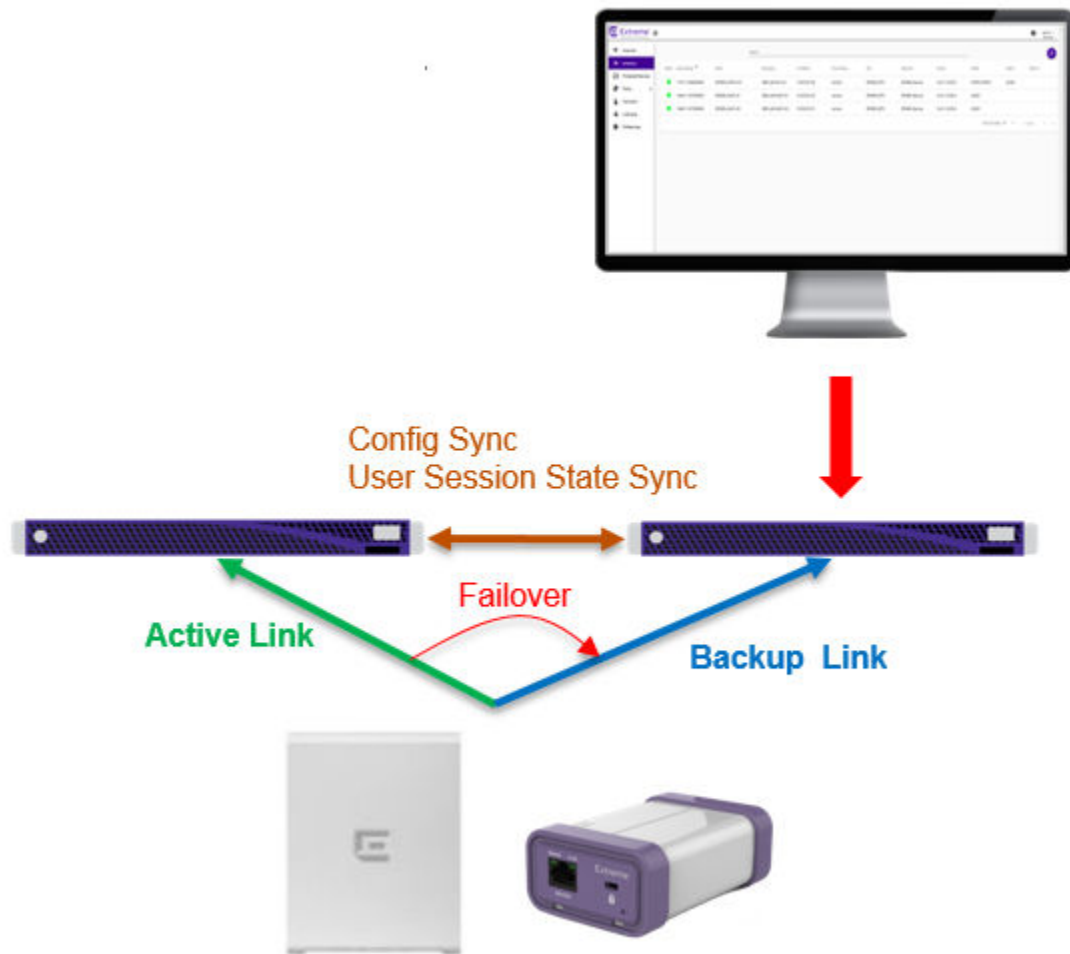


Figure 1: ExtremeCloud Appliance Availability Pair with Extreme Defender Application

Generate API Key



Note

When running more than one ExtremeCloud Appliance application that uses an API key file, you need only one generated API key.

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

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

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

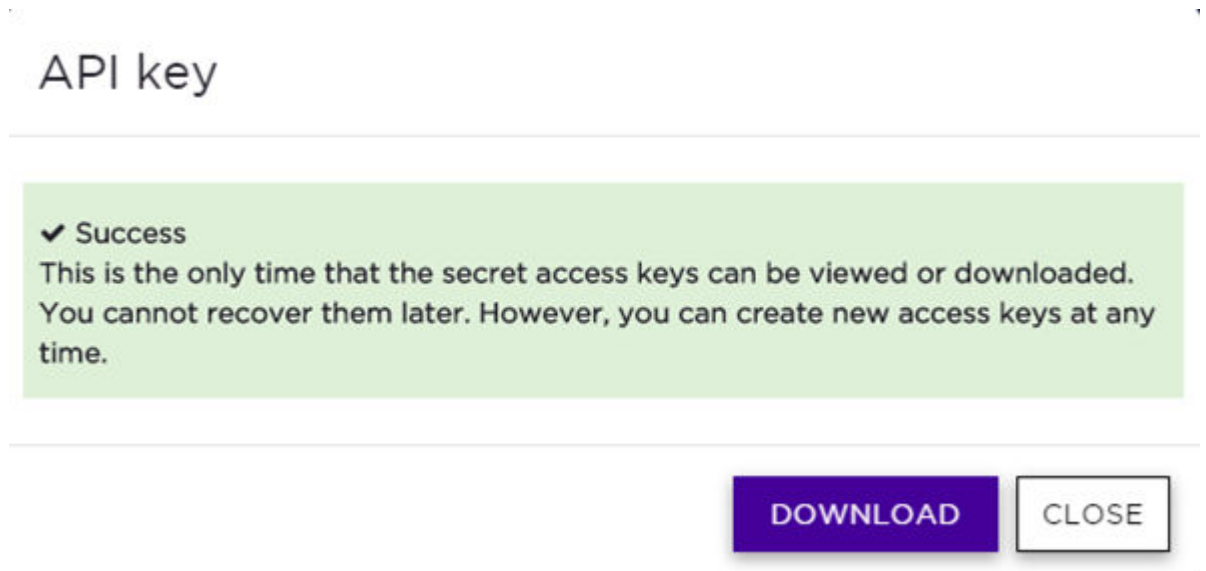


Figure 2: API Key dialog

5. 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.
6. After you download the key, select **Close**.

Related Topics

[Upload the API Key File](#) on page 14

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.



Note

When running more than one application that uses an API Key file, you need only one generated API Key.

To upload a generated API key file:

1. Log into ExtremeCloud Appliance with full administrator credentials.
2. Go to **Administration > Applications** and select .
3. Select the **Configuration Files** tab.
4. Select **api-keys.json**, and then select the upload icon .

5. 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 Topics

[Run Defender Application](#) on page 15


[Generate API Key](#) on page 13

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.

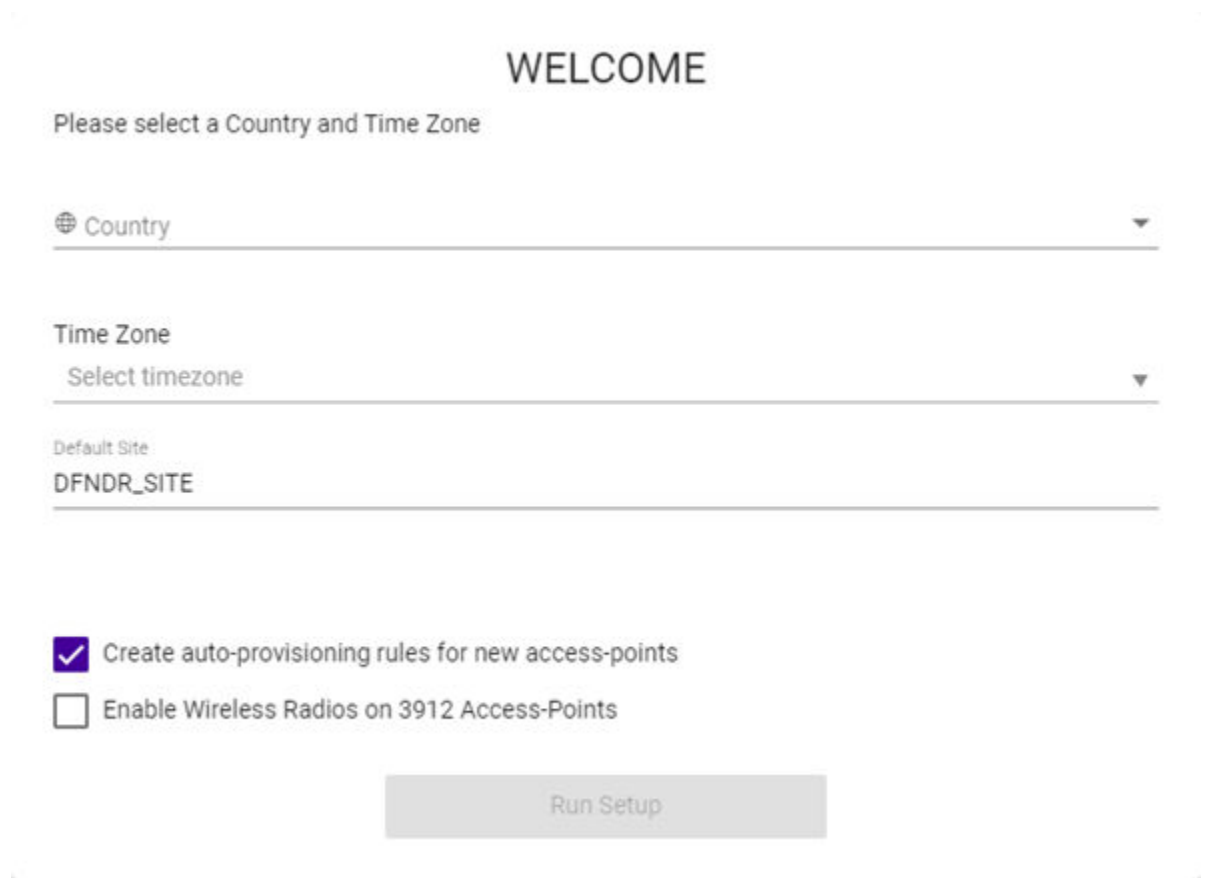
Additionally, the Extreme Defender Application user interface can be accessed using the HTTPS protocol on the TCP port 5825. For example, if your ExtremeCloud Appliance has the IP address 192.168.10.10, you can manage Extreme Defender Application in a browser by typing `https://192.168.10.10:5825/apps/defender`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

Related Topics

[Configuration Wizard](#) on page 15

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 Configuration 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

DFNDR_SITE. You can specify a unique name.

2 device groups

- `DFNDR_Devices` for AP3912i access points.
- `DFNDR_SA201_Devices` for SA201 adapters.

1 network service

`DFNDR_Service`

2 adoption rules

One rule for each device group.

2 device group configuration Profiles

- `DFNDR_SA201` for wired SA201 adapters
- `DFNDR` for wireless AP3912i access points.

1 RF Profile

`DFNDR_ACS`

2 policy roles

- `DFNDR_DenyAll` denies all traffic by default action.
- `DFNDR_PolicyGeneration` — Has a contain to VLAN default action and is associated with a Bridged at AP untagged topology.

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

Related Topics

[Sites in Extreme Defender Application](#) on page 53

[Roles](#) on page 45

[Setup Wizard for Configuration Reset](#) on page 50

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.
- **Alarms.** Event management for Protected Devices and for APs and SA201 adapters. Alarms indicate device status.
- **Logs.** An audit history of administrator modifications for Extreme Defender Application.
- **Policy.** View policy groups and roles associated with your network.
- **Administration.** Perform system administration including managing accounts, configuring tagging, activating devices, licensing, and configuring email notification and 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.

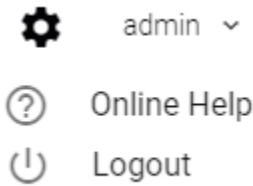



Figure 4: Defender Admin Menu

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.



Overview

[Add a New Dashboard on page 19](#)

[Modify a Dashboard on page 20](#)

[Widgets on page 20](#)

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 Topics


[Modify a Dashboard](#) on page 20

[Widgets](#) on page 20

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 Topics

[Widgets](#) on page 20

[Add a New Dashboard](#) on page 19

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

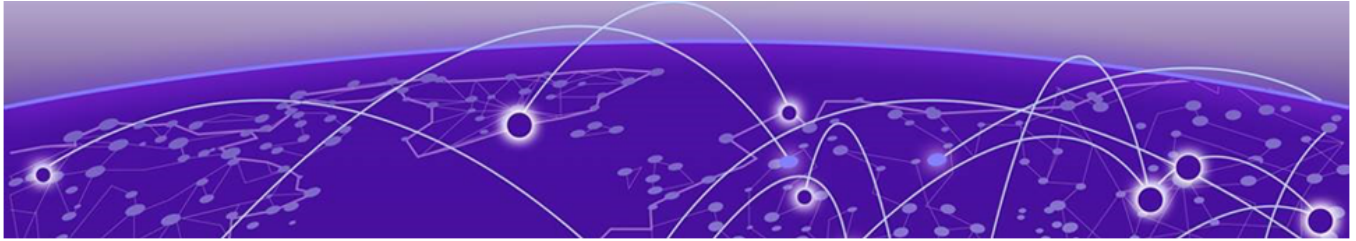
Graphs the number of APs or adapters by status. Valid status values are:

- 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 Topics

[Add a New Dashboard](#) on page 19

[Modify a Dashboard](#) on page 20



Inventory

[Inventory Device Status](#) on page 23

[View Inventory Details](#) on page 23


[Group Protected Devices from the Inventory List](#) on page 24

[Throughput Tab](#) on page 24

[Usage Tab](#) on page 25

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

To manually refresh the page, select .

To customize the number of records displayed per page, select **Items Per Page**. Valid values are:

- 5
- 10
- 25
- 100
- 500

Related Topics

[Search Facility](#) on page 18





[Inventory Device Status](#) on page 23

[View Inventory Details](#) on page 23

Inventory Device Status

The following describes each device status on the **Inventory List**.

Table 5: 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 Topics

[Throughput Tab](#) on page 24

[Usage Tab](#) on page 25

[Group Protected Devices from the Inventory List](#) on page 24

[Inventory](#) on page 22

[Manage Tags](#) on page 57

[Account Tagging](#) on page 57

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 Topics


[Group Devices from the Protected Devices List](#) on page 30

[Manage Groups](#) on page 46

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.

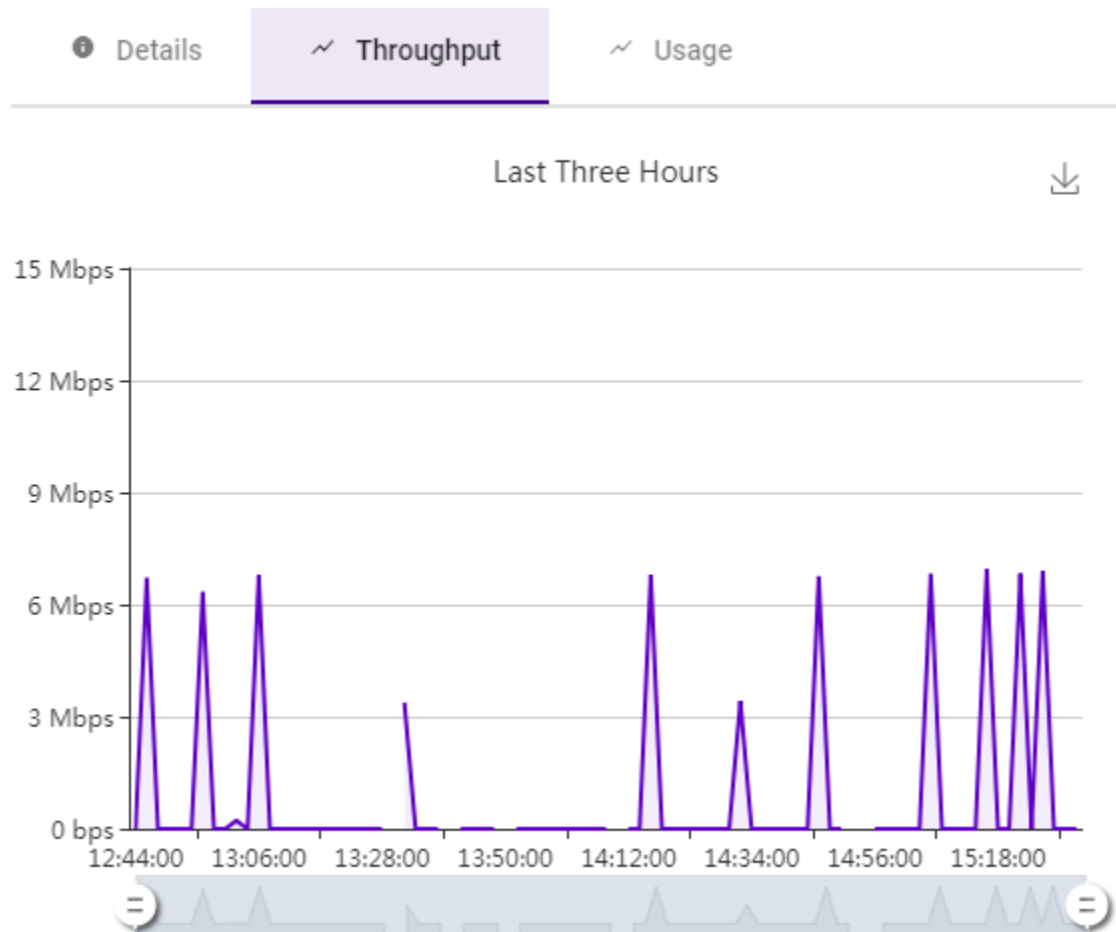




Figure 5: AP Inventory Device Throughput (Mbps)

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.

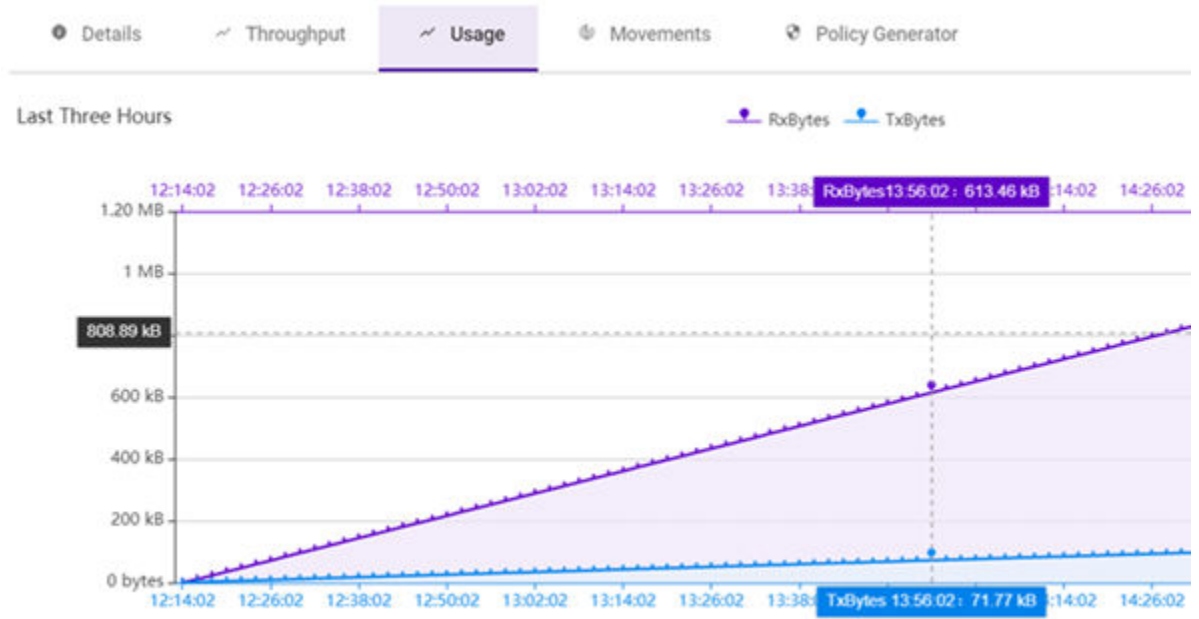
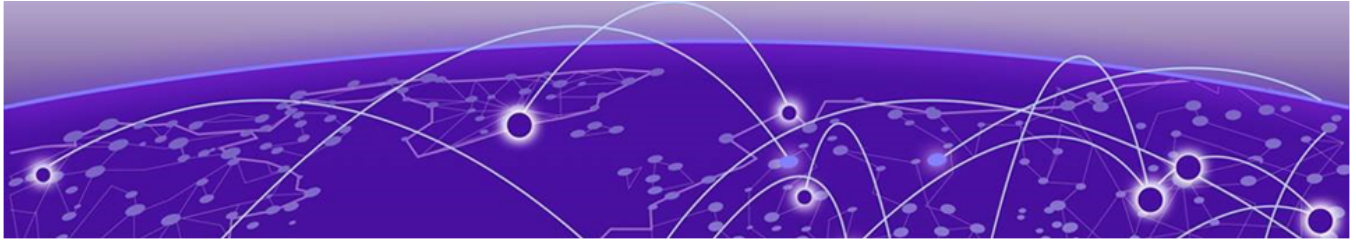


Figure 6: Protected Device Usage



Protected Devices

[Protected Device Status](#) on page 28

[View Protected Device Details](#) on page 29

[Group Devices from the Protected Devices List](#) on page 30

[Movements Tab](#) on page 31

[Policy Generator](#) on page 32

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



Note

It may be necessary to refresh the **Protected Devices List** to sync the Defender clients with ExtremeCloud Appliance.

To manually refresh the page, select .

To customize the number of records displayed per page, select **Items Per Page**. Valid values are:

- 5
- 10
- 25
- 100
- 500

Related Topics

[Search Facility](#) on page 18








[View Protected Device Details](#) on page 29

[Group Devices from the Protected Devices List](#) on page 30

Protected Device Status

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

Table 6: Protected Device Status

| Status | Description |
|---|---|
|  | Active. Device has the following: <ul style="list-style-type: none"> • Discovered ExtremeCloud Appliance • On-boarded with a policy role • Actively sending data. |
|  | Not On-board. Device: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 Topics

[Group Devices from the Protected Devices List](#) on page 30

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 Topics

[Throughput Tab](#) on page 24


[Usage Tab](#) on page 25

[Movements Tab](#) on page 31

[Policy Generator](#) on page 32

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 .

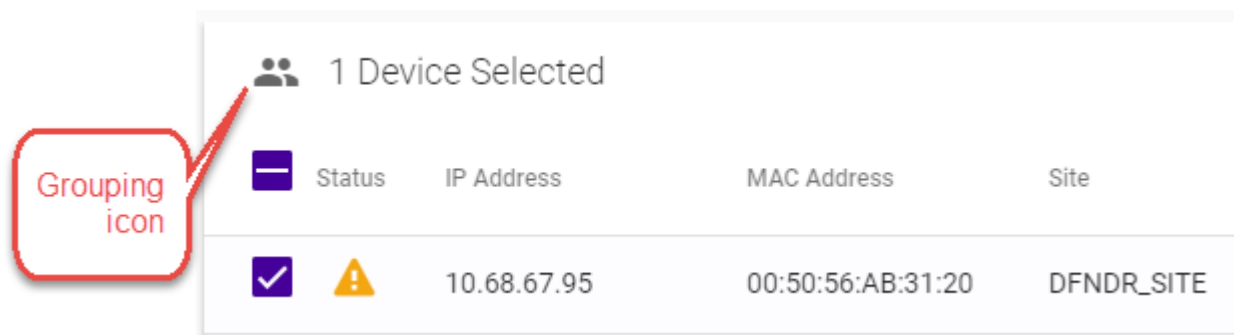


Figure 7: Select a Policy Group for Protected Device

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.

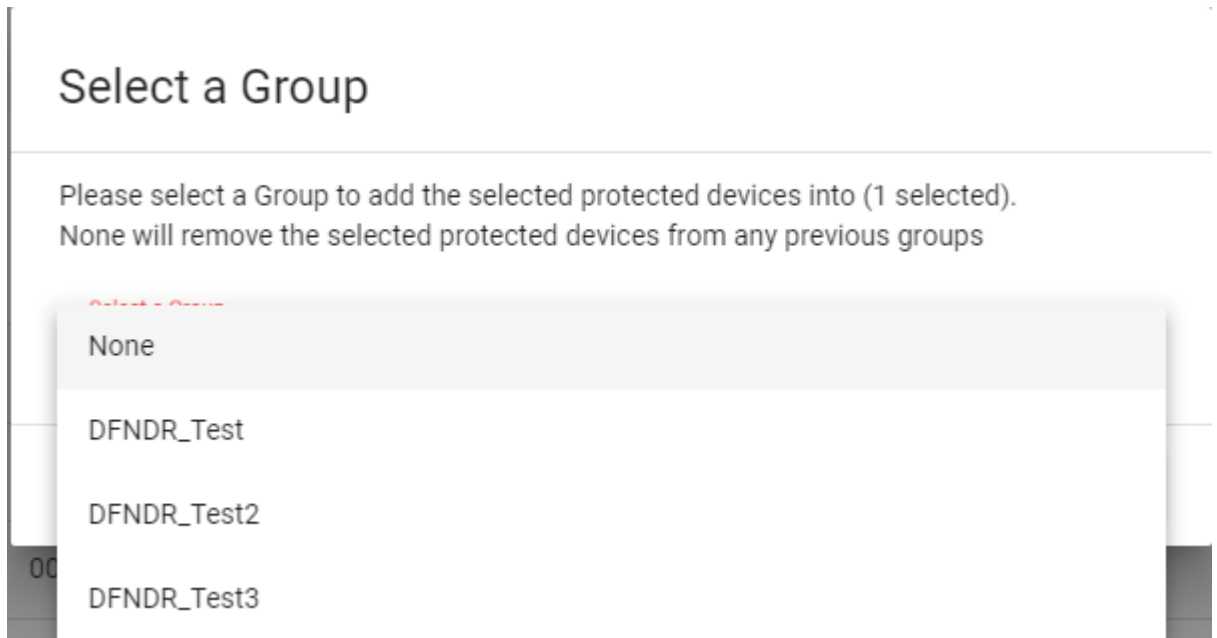


Figure 8: Selecting a Group

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 Topics

[Group Protected Devices from the Inventory List](#) on page 24

[Manage Groups](#) on page 46

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

To customize the number of records displayed per page, select **Items Per Page**. Valid values are:

- 5
- 10
- 25
- 100
- 500

Related Topics

[Search Facility](#) on page 18

[Policy Generator](#) on page 32

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 33.



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 Topics

[Run Policy Generator](#) on page 33

[L2 Rules](#) on page 36

[Configure L3 and L4 Rules](#) on page 36

[Allow DNS, DHCP, and Well-Known Port Traffic Automatically](#) on page 38

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.

Protected Device: Lab-208

Details Throughput Usage Movements **Policy Generator**

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 |

Next Stop

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 Topics

[Policy Generator](#) on page 32

[L2 Rules](#) on page 36

[Configure L3 and L4 Rules](#) on page 36

[L7 Rules](#) on page 37

[Allow DNS, DHCP, and Well-Known Port Traffic Automatically](#) on page 38

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.

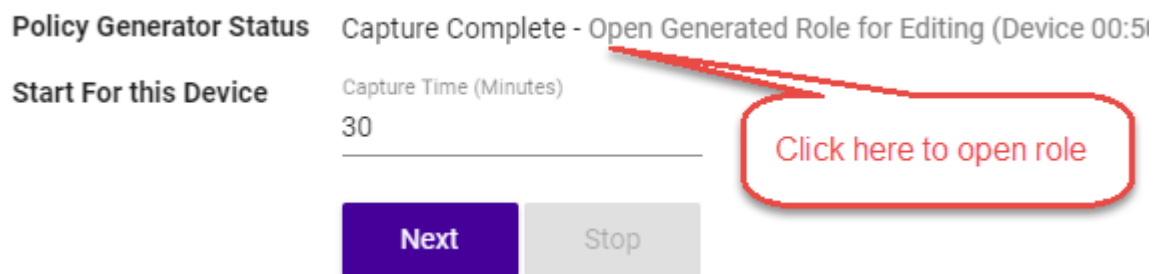


Figure 11: Open Generated Role

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 Topics

[L2 Rules](#) on page 36

[Configure L3 and L4 Rules](#) on page 36

[L7 Rules](#) on page 37

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:

Name

Provide a name for the rule.

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.

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 Topics

[Modify Policy Generator Roles](#) on page 35

[Configure L3 and L4 Rules](#) on page 36

[L7 Rules](#) on page 37

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:

Name

Provide a name for the rule.

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 Topics

[Modify Policy Generator Roles](#) on page 35

[L2 Rules](#) on page 36

[L7 Rules](#) on page 37

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 Topics

[Modify Policy Generator Roles](#) on page 35

[L2 Rules](#) on page 36

[Configure L3 and L4 Rules](#) on page 36

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.

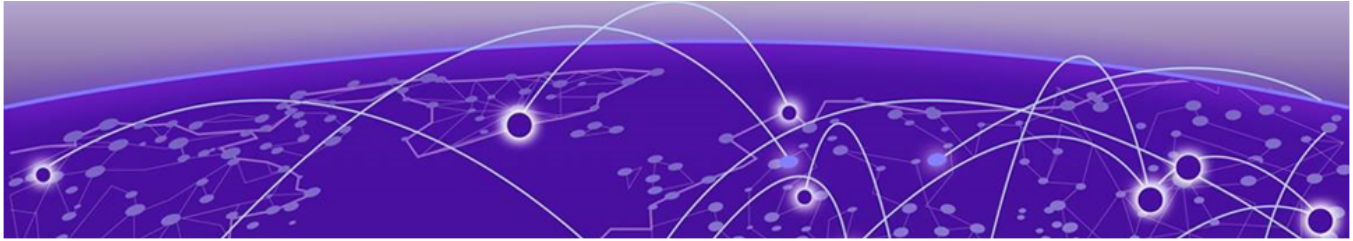


Note

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

Related Topics

[Policy Generator](#) on page 32



NEW!

Alarms

[Active Alarms](#) on page 39

[Alarm Log](#) on page 40

[Configure Alarm Settings](#) on page 41

Configure alarms for Protected Devices and for access points and SA201 adapters from Extreme Defender Application. Alarms indicate the device status:

- Active Alarm indicates that a device is not operating.
- Ready Alarm indicates that a device is operating.

You can configure the level of severity for each alarm and set up email notification.

Go to the **Alarms** workbench to do the following:

- View Active Alarms
- View the Alarm Log
- Configure Alarm Settings

Related Topics

[Active Alarms](#) on page 39

[Alarm Log](#) on page 40

[Configure Alarm Settings](#) on page 41

[Configure Email Notification Server](#) on page 48

NEW! Active Alarms

Active Alarms indicate that a device is Down. Alarms are configured for both Protected Devices and Inventory Devices (the AP3912 access points and the SA201 adapters). When Defender receives a Down event, it populates the Active Alarms table. When Defender receives an Up event, it removes the Active Alarm from the table. A Ready alarm indicates that an Up event is received.

To view Active Alarms, go to **Alarms > Active Alarms**.

Clear

Select  to remove the alarm from the **Active Alarms** list. Clearing the alarm removes the alarm from your list view. It does not indicate a change in device status.

Severity

Severity of the configured alarm. Specify this value when configuring the alarm. The severity setting is determined by how important the alert is to you. The severity level is displayed in the Active Alarms, Alarm Logs, and in the email notification. Valid values are:

- High
- Medium
- Low


Description

- Type of device: Protected Device, AP, or adapter
- Device Name
- Status of the device

Time

Date and Time of the event.

Use the **Search** field to find a specific alarm instance.

To manually refresh the page, select .

To customize the number of records displayed per page, select **Items Per Page**. Valid values are:

- 5
- 10
- 25
- 100
- 500

Related Topics

[Alarms](#) on page 39

[Alarm Log](#) on page 40

[Configure Alarm Settings](#) on page 41

[Configure Email Notification Server](#) on page 48

NEW! Alarm Log

The **Alarm Log** provides a history of alarms for Protected Devices and Inventory Devices (AP3912 access points and SA201 adapters). To view the **Alarm Log**, go to **Alarms > Alarm Log**.

The following information is available on the **Alarm Log** page:

Severity

Severity of the configured alarm. Specify this value when configuring the alarm. The severity setting is determined by how important the alert is to you. The severity level is displayed in the Active Alarms, Alarm Logs, and in the email notification. Valid values are:

- High
- Medium

- Low

Description

- Type of device: Protected Device, AP, or adapter
- Device Name
- Status of the device

Time

Date and Time of the event.

To find a specific alarm instance, use the **Search** field.

To manually refresh the page, select .

To customize the number of records displayed per page, select **Items Per Page**. Valid values are:

- 5
- 10
- 25
- 100
- 500

Related Topics

[Alarms](#) on page 39

[Active Alarms](#) on page 39

[Configure Alarm Settings](#) on page 41

NEW! Configure Alarm Settings

Configure alarms for devices in a Down state and devices in an Up state. Alarms in Extreme Defender Application alert you to when a Protected Device or managed device (AP3912 access point or SA201 adapter) is operating or not operating. From the **Settings** tab, configure alarm severity and email notification for each alarm type:

1. Go to **Alarms > Settings**.

There is an alarm type for APs and adapters and an alarm type for Protected Devices.

2. Configure the following:

Severity

Severity of the configured alarm. Specify this value when configuring the alarm. The severity setting is determined by how important the alert is to you. The severity level is displayed in the Active Alarms, Alarm Logs, and in the email notification. Valid values are:

- High
- Medium
- Low

Email

Select **Email** to receive email notification about the alarm for APs and adapters, and the alarm for Protected Devices.

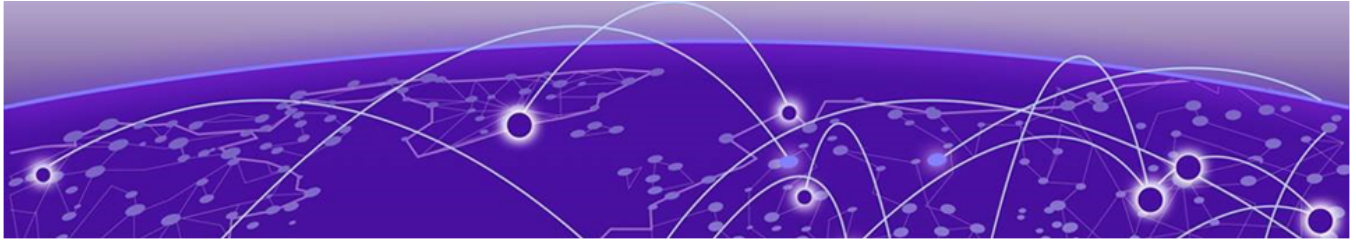
**Note**

Before you can receive email notification, you must configure an Email Notification Server.

- For email notification that a device is not operating, select **Email** next to **Active**.
- For email notification that a device is operating, select **Email** next to **Ready**.

Related Topics

[Configure Email Notification Server](#) on page 48



NEW!

Logs

The **Logs** page provides an audit history of system events for Extreme Defender Application. To view the audit log, go to **Logs**.

To configure the beginning and ending dates for the audit log, select the **From** and **To** fields. Selecting **From** and **To** displays a calendar, from where you can select the beginning and ending dates for the audit log.

The audit log consists of administrator configuration changes, including changes to the following:

- Roles
- Policies
- Groups
- Configuration back up and restore activity
- Managed device attributes and licensing
- Managed accounts and tags
- Device onboarding
- Notification server settings
- Alarm settings
- Policy Generator

The audit log records the date and time of the change, who made the change, and what was changed. The following information is available on the **Logs** page:

Time

Date and Time of the change.


User

User ID of the Extreme Defender Application user who made the change.

Message

Description of the change. Name of the AP, adapter, or client is displayed. If the device does not have a name, the device MAC Address is displayed.

Use the **Search** field to find a specific log instance.

To manually refresh the page, select .

To customize the number of records displayed per page, select **Items Per Page**. Valid values are:

- 5
- 10
- 25
- 100
- 500

The Log maintains a maximum of 1000 records. After the maximum number of records is reached, the oldest records are dropped to maintain the 1000 record capacity.



Policy

[Roles](#) on page 45

[Groups](#) on page 46

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

Related Topics

[Roles](#) on page 45

[Groups](#) on page 46

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 Topics

[Policy Generator](#) on page 32

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 Topics

[Manage Groups](#) on page 46

[Policy Group Settings](#) on page 46

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 Topics

[Policy Group Settings](#) on page 46

[Group Protected Devices from the Inventory List](#) on page 24

[Group Devices from the Protected Devices List](#) on page 30

Policy Group Settings

Configure the following settings to create a new policy group:

Table 7: 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 Topics

[Groups](#) on page 46

[Manage Groups](#) on page 46

[Roles](#) on page 45



Administration

[System](#) on page 48

[Activation](#) on page 52

[Accounts](#) on page 55

[Licensing](#) on page 58

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

Related Topics

[System](#) on page 48

[Activation](#) on page 52

[Manage Tags](#) on page 57

[Accounts](#) on page 55

[Licensing](#) on page 58

System

Perform Extreme Defender Application system configuration from the **Administration** workbench. Go to **Administration > System** to configure system settings.

Related Topics

[Configure Email Notification Server](#) on page 48

[UI Settings](#) on page 49

[Defender Configuration Back Up and Restore](#) on page 49

[Setup Wizard for Configuration Reset](#) on page 50

NEW! Configure Email Notification Server

Before you can receive email notification about alarms, you must configure an email server.



Note

Only one email address and SMTP server is supported at a time.

1. Go to **Administration > System > Notification**.
2. Configure the following parameters:

Delivery Address

Email address that will accept alarm notifications.

SMTP Server

Address of the SMTP Server that has the email account specified in **Delivery Address**.

Port

The Port numbers associated with your service provider for the specified protocol. Example port numbers for a mail submission agent are:

- **465** (for protocol Secure Sockets Layer (SSL))
- **587** (for protocol Transport Layer Security (TLS))

User Name

User Name for the specified SMTP Server, indicated above.

Password

Password for the specified SMTP Server, indicated above.

Security

Security protocol. Valid values are:

- None
- SSL
- TLS



Note

The Port number (indicated above) must correspond to the security protocol that is specified.

Related Topics

[Configure Alarm Settings](#) on page 41


UI Settings

Customize the Extreme Defender Application user interface settings.

Go to **Administration > System > UI Settings** and configure the following settings:

Table 8: Defender User Interface 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 **UI Settings** page.

NEW! Defender Configuration Back Up and Restore

To back up the Extreme Defender Application, take the following steps:

1. Go to **Administration > System > Back Up/Restore**.
2. To download a Defender configuration backup file, select **Back Up to Local**.
The Defender configuration file is downloaded to your local Downloads folder. File name format: *defender_appliance_ip_address_or_host_name_date_build_number*.
3. To restore the Defender configuration from a backup file:
 - a. Select **Restore from Local**.
 - b. Navigate to the Defender backup file.
 - c. Select **Open**.
 - d. Select **Upload File**.

NEW! Setup Wizard for Configuration Reset

After you install Extreme Defender Application and run the application for the first time, the Configuration Wizard opens, prompting you for initial setup. The Configuration Wizard creates a default Defender configuration: a site, device groups, and configuration elements that are visible in the underlying ExtremeCloud Appliance.

In the event that you need to recreate the Defender default configuration without reinstalling Extreme Defender Application, you have the option to re-run the Configuration Wizard from the **Administration** workbench. Use this tool to create a new default Defender configuration on ExtremeCloud Appliance.



Note

Regardless of the Defender site name, all Defender device groups have the same hard-coded names:

- `DFNDR_Devices` for AP3912i access points.
- `DFNDR_SA201_Devices` for SA201 adapters.

The Configuration Wizard looks for these hard-coded names. The wizard runs when there are no existing device groups on ExtremeCloud Appliance with these hard-coded names.


Before running the Configuration Wizard, you must delete these device groups or rename them on ExtremeCloud Appliance.



Note

It is a best practice to manually delete the DFNDR sites from ExtremeCloud Appliance before running the Defender Configuration Wizard.

To run the Configuration Wizard reset tool:

1. Go to **Administration > System > Setup**.
2. Select .

The Configuration Wizard dialog displays.

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 12: Defender Configuration Wizard

3. Specify the configuration parameters and select **Run Setup**.

The ExtremeCloud Appliance configuration is updated to re-create the set of default configuration elements related to the Defender (DFNDR) operation.

The Configuration 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

`DFNDR_SITE`. You can specify a unique name.

2 device groups

- `DFNDR_Devices` for AP3912i access points.
- `DFNDR_SA201_Devices` for SA201 adapters.

1 network service

`DFNDR_Service`

2 adoption rules

One rule for each device group.

2 device group configuration Profiles

- DFNDR_SA201 for wired SA201 adapters
- DFNDR for wireless AP3912i access points.

1 RF Profile

DFNDR_ACS

2 policy roles

- DFNDR_DenyAll denies all traffic by default action.
- DFNDR_PolicyGeneration — Has a contain to VLAN default action and is associated with a Bridged at AP untagged topology.

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

Related Topics

[Configuration Wizard](#) on page 15

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 Topics

[Sites in Extreme Defender Application](#) on page 53

[Scan a QR Code](#) on page 53

[Manual Onboarding](#) on page 54

[Use a CSV File](#) on page 54

[Configuration Wizard](#) on page 15

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 53.

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

Related Topics

[Activation](#) on page 52

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 53.

Name

Unique name for the AP or adapter.

Description

Text description of the AP or adapter.

3. Click **Add Device**.

Related Topics

[Activation](#) on page 52

[Sites in Extreme Defender Application](#) on page 53

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 Topics

[Activation](#) on page 52

[Sites in Extreme Defender Application](#) on page 53

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 Topics

[Manage Accounts](#) on page 56

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:

Name

User name for this account.

Password

Password for this account.

Confirm Password

Enter password again to confirm.

Access

User access level. Valid values are:

- Full
- User
- Read-Only

See [Accounts](#) on page 55 for a complete description of each access level.

Tags

Categories used to filter the content that a user can manage. For more information, see [Account Tagging](#) on page 57.

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 56.

Delete a User Account

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

Related Topics

[Accounts](#) on page 55

[Account Tagging](#) on page 57

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 Topics

[Account Tagging](#) on page 57

[View Inventory Details](#) on page 23

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 Topics

[Manage Tags](#) on page 57

[View Inventory Details](#) on page 23

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**.

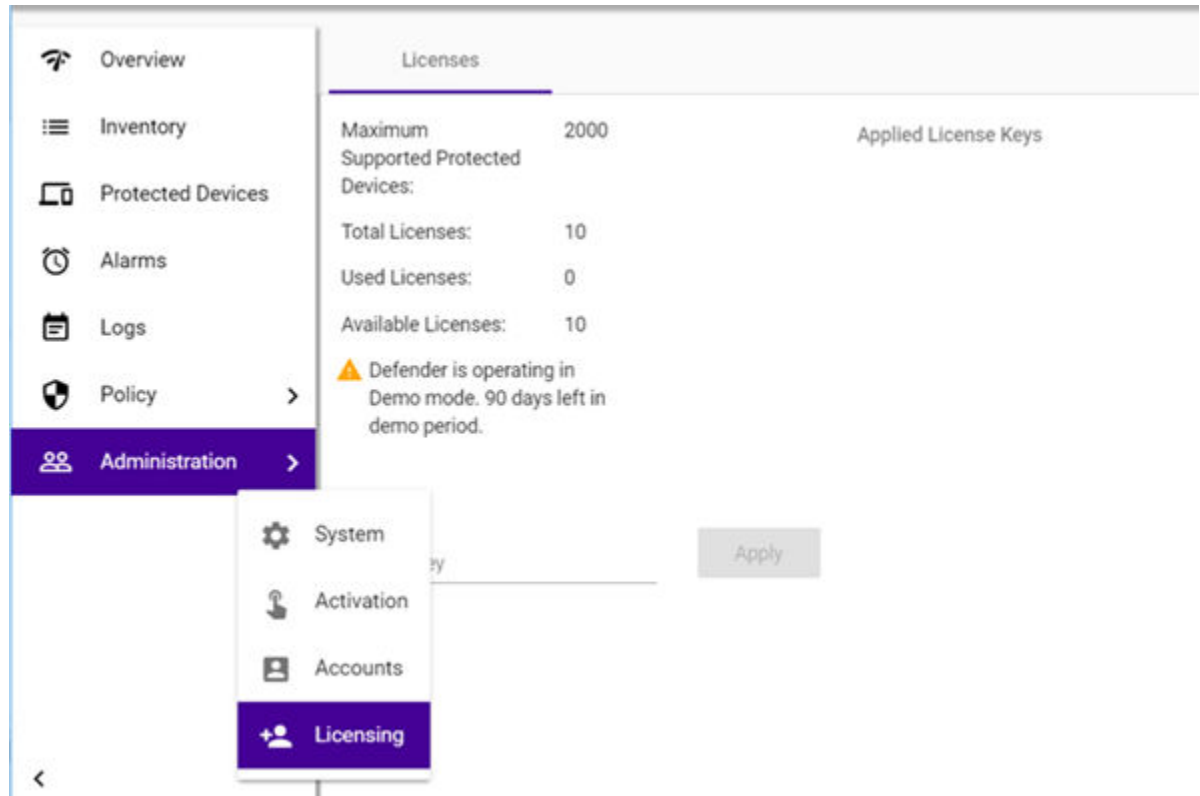


Figure 13: Defender Application Licensing Page

Figure 13 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.



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 Defender for IoT

Extreme Defender for IoT provides unique in-line security for mission critical and/or vulnerable IoT devices. Placed between the IoT device and the network, the Defender for IoT solution helps secure and isolate IoT devices protecting them from internal and external hacking attempts, viruses, malware and ransomware, DDoS attacks, and more. Designed to be simple and flexible, Defender for IoT can be deployed over any network infrastructure to enable secure IoT management without significant network changes.

The solution is comprised of the Extreme Defender Application Software and the Defender Adapter (SA201) or AP3912i access point. ExtremeCloud Appliance is the supported platform for the Extreme Defender Application.

For more information, see <https://www.extremenetworks.com/product/extreme-defender-for-iot/>.

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/>.

ExtremeAnalytics

ExtremeAnalytics™, 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. ExtremeAnalytics 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 ExtremeAnalytics at <http://www.extremenetworks.com/product/extremeanalytics/>.

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/>.

ExtremeCloud™ IQ

ExtremeCloud™ IQ is an industry-leading and visionary approach to cloud-managed networking, built from the ground up to take full advantage of the Extreme Networks end-to-end networking solutions. ExtremeCloud IQ delivers unified, full-stack management of wireless access points, switches, and routers and enables onboarding, configuration, monitoring, troubleshooting, reporting, and more. Using innovative machine learning and artificial intelligence technologies, ExtremeCloud IQ analyzes and interprets millions of network and user data points, from the network edge to the data center, to power actionable business and IT insights, and deliver new levels of network automation and intelligence. Learn more about ExtremeCloud IQ at <https://www.extremenetworks.com/extremecloud-iq/>.

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 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 56
 - edit 56
- activation for devices 52
- active alarms 39
- adapter provisioning 52
- administration 48
- alarm log 40
- alarm settings 41
- alarms
 - active alarms 39
 - alarm log 40
 - configure alarms 41
- AP provisioning 52
- API key
 - generating 13
 - using with Defender 14
- applications
 - uninstalling 12
 - upgrading 11
- Availability Pair 12

B

- back up configuration 49, 50

C

- Configuration Wizard 15, 50
- conventions
 - notice icons 5
 - text 5
- csv file 54, 55

D

- dashboard
 - adding 19
- Defender, running 15
- device activation 52
- device grouping 24, 30
- device groups 53
- device status 23
- documentation
 - feedback 7
 - location 7

E

- email notification 48

F

- feedback 7
- filter user content 57

G

- getting started 10
- grouping devices 24, 30
- groups 46

I

- installing Defender 11
- Inventory
 - throughput 24
 - usage 25
- Inventory details 23
- Inventory List 22

L

- Layer 2 rules 36
- Layer 3 and 4 rules 36
- Layer 7 rules 37
- licensing 58
- Logs screen 43

M

- Movement tab 31

N

- notices 5

O

- onboarding by csv file 54, 55
- onboarding by QR code 53
- onboarding, manually 54
- OSI Layer 3 and 4 rules 36
- Overview dashboard 19

P

- policy definition 45
- policy generator
 - modifying roles 35
 - running 33
- policy group settings 46
- policy groups 46
- Protected Device
 - details 29
 - throughput 24
 - usage 25
- protected devices 27
- Protected Devices, status 28
- provisioning APs and adapters 52

Q

- QR code scanning 53

R

- restore configuration 49, 50
- roles
 - policy generator 32, 33
- rules, allowing DNS, DHCP, and well-known port traffic 38
- rules, configuring OSI Layer 3 and 4 rules 36
- rules, OSI Layer 2 rules 36
- rules, OSI Layer 7 rules 37

S

- Setup Wizard 15, 50
- sites 53
- support, see technical support
- system settings 48

T

- tagging accounts 57
- tags, managing 57
- technical support
 - contacting 7, 8
- Throughput tab 24
- tracking device movement 31

U

- Usage tab 25
- user interface settings 49

W

- warnings 5
- widgets 20