Extreme™
Customer-Driven Networking

Extreme Defender for IoT Solution Deployment Guide

Version 3.31

9036495-00 Rev AA

Published September 2019

Legal Notice

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

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

Trademarks

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

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

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

Open Source Declarations

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

Table of Contents

Preface

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

Conventions

This section discusses the conventions used in this guide.

Text Conventions

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

Table 1: Notice Icons

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

Table 2: Text Conventions

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

Providing Feedback to Us

Quality is our first concern at Extreme Networks, and we have made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

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

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

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

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

Getting Help

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

Extreme Portal	Search the GTAC (Global Technical Assistance Center) knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
The Hub	A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
Call GTAC	For immediate support: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

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

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

Subscribing to Service Notifications

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

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

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

4 Click **Submit**.

Documentation and Training

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

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

Training

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

1 About Extreme Defender for IoT Solution Deployment

The Extreme Defender for IoT solution consists of the following elements for deployment:

- ExtremeCloud™ Appliance
- Extreme Defender Application
- SA201 adapter or AP3912i

The Extreme Defender Application is installed on the ExtremeCloud Appliance docker container platform and provides restricted provisioner / administrator access.

Figure 1: Elements of the Extreme Defender for IoT Solution

This guide provides instructions on how to deploy the Extreme Defender for IoT solution on a network infrastructure, illustrates the deployment options available, and details the tasks required to configure the elements to successfully deploy the solution on a network.

Before You Begin

This guide is based on ExtremeCloud Appliance version 4.36.01 and Extreme Defender Application version 03.01.22 or later.

Before you begin:

- Install ExtremeCloud Appliance version 4.36.01 and obtain an ExtremeCloud Appliance license from the Extreme Networks Support site.

  For more information, see the *Installation video* at https://extremenetworks.com/documentation/extremecloud-appliance.
- You must be familiar with managed device provisioning (SA201 adapter or AP3912i) and policy configuration.

- You must have detailed knowledge of the network switching infrastructure, which may include:
  - Access layer VLAN and IP subnet configuration.
  - Fabric Attach (for Extreme Fabric Connect core infrastructure).
  - Data Center and Application Server access configuration.

Network Deployment Options

You have a choice on how you plan to connect the protected IoT devices to the network. The deployment strategy encompases Extreme Defender Application, ExtremeCloud Appliance (as the supported platform) with an SA201 adapter or AP3912i. The IoT device is connected to the adapter or AP through the appropriate network service. IoT devices can be locally attached to a VLAN at the access layer / edge of the network, or tunneled and encrypted over the network to ExtremeCloud Appliance for access to application servers.

Defender for IoT deployment options:

- Legacy IP solution with local VLAN attachment (not encrypted)
- IPSec Tunnel Overlay solution (encrypted tunnel between managed device and ExtremeCloud Appliance)
- Fabric Connect core with Fabric Attach for automated VLAN and Fabric service attachment.

Determine the device management plane connection to ExtremeCloud Appliance before determining the IoT device service attachment. Choose between Tagged or Untagged management when establishing the management plane between the adapter or AP and ExtremeCloud Appliance at the access switch.

For Legacy IP networks with local VLAN attachment and IPSec Tunnel Overlay solution deployments, use Untagged port configuration on the access switch (any vendor). For Extreme Networks Fabric Connect infrastructures that support Fabric Attach, you can use either Untagged or Tagged port configuration in a fully-automated fashion.

Regardless of the deployment model, ExtremeCloud Appliance with the Defender for IoT solution programs access control with implicit policies to control IoT communications traffic on the network.

Managed Device Attachment

The first step in preparing the network to connect the SA201 adapter or AP3912i to an access layer / wiring closet switch is to determine the VLAN and IP subnet desired for management of the SA201 adapter or AP3912i.

For all networks where Fabric Attach is *not* in use, simply configure the access switch Port VLAN ID (untagged VLAN membership) to the desired VLAN / IP subnet for connection to the network. SA201 adapter or AP3912i use DHCP by default and will primarily attempt to contact ExtremeCloud Appliance using DNS a server to resolve the name “controller.<yourdomain.com>”.

If Fabric Attach is enabled on the Extreme Networks access switch to which the SA201 adapter or AP3912i is connected, there are two options for automating the management plane VLAN ID using Untagged or Tagged frames between the SA/AP and the switch.

ExtremeCloud Appliance discovery options are available: such as DHCP Option 43/60, DHCP Option 78, and SLP. For detailed information, refer to "Discovery and Registration" in the *Extreme Cloud Appliance Deployment Guide* at https://extremenetworks.com/documentation/extremecloud-appliance.

Related Links

Local VLAN Attachment Model on page 9
IPSec Tunnel Overlay Model on page 9
Fabric Connect with Fabric Attach Model on page 10

Local VLAN Attachment Model

Figure 2 illustrates the Local VLAN attach model highlighting the attachment of different IoT device types. IoT device traffic (denoted by different colored lines) is switched at the SA201 adapter or AP3912i directly onto a local VLAN at the access layer switch. IoT traffic is then routed across the network to access respective data center application servers.

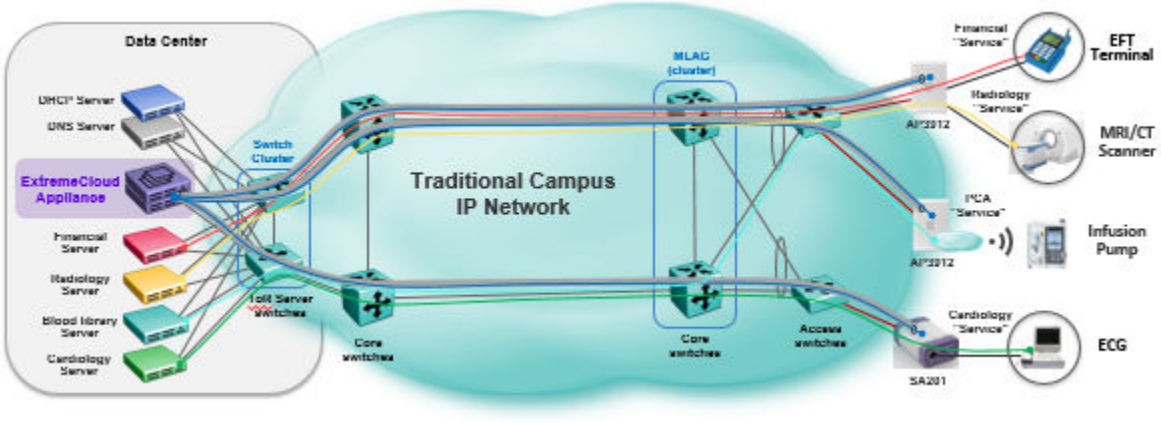


Figure 2: Local VLAN Attachment model

IPSec Tunnel Overlay Model

Figure 3 on page 10 illustrates the IPSec Tunnel Overlay model highlighting the attachment of different IoT device types. IoT device traffic (denoted by different colored lines) is encapsulated at the SA201 adapter or AP3912i into VLAN and then encrypted and forwarded in the IPSec tunnel to the ExtremeCloud Appliance controller. IoT traffic is then decrypted onto an appropriate remote VLAN and switched or routed to access the respective data center application server.

Note

All disparate colored IoT device traffic is shown inside the tunnel with the blue management plane traffic between the SA201 adapter or AP3912i and the ExtremeCloud Appliance. IoT traffic continues on through ExtremeCloud Appliance to the respective application server.

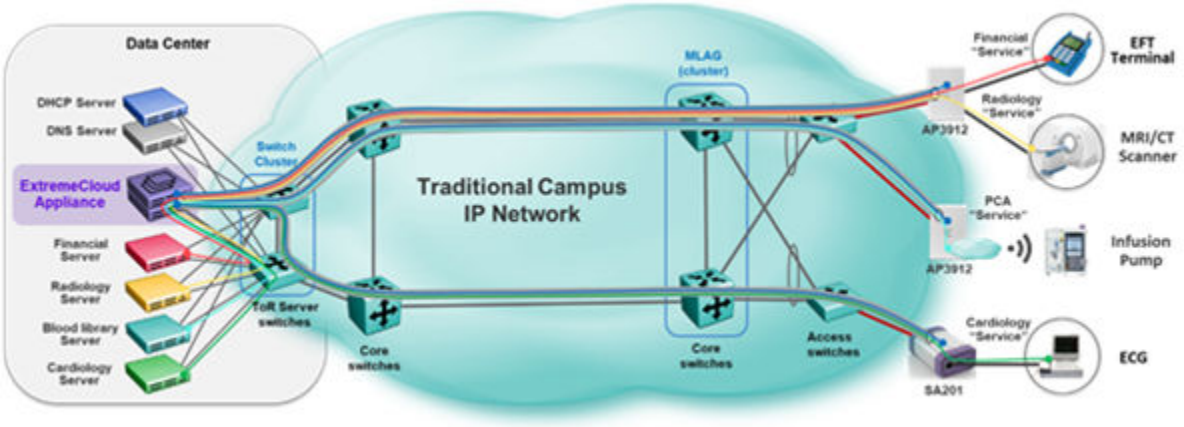


Figure 3: IPSec Tunnel Overlay model

Fabric Connect with Fabric Attach Model

Figure 4 illustrates the Fabric Connect core Fabric Attach model highlighting the attachment of different IoT device types. IoT device traffic is switched at the SA201 adapter or AP3912i directly onto a local VLAN and Fabric service that has been dynamically created by FA based on the security profile for the specific IoT device. IoT traffic is forwarded over the Fabric Connect network in a Layer 2 or Layer 3 virtual service to access respective data center application server.

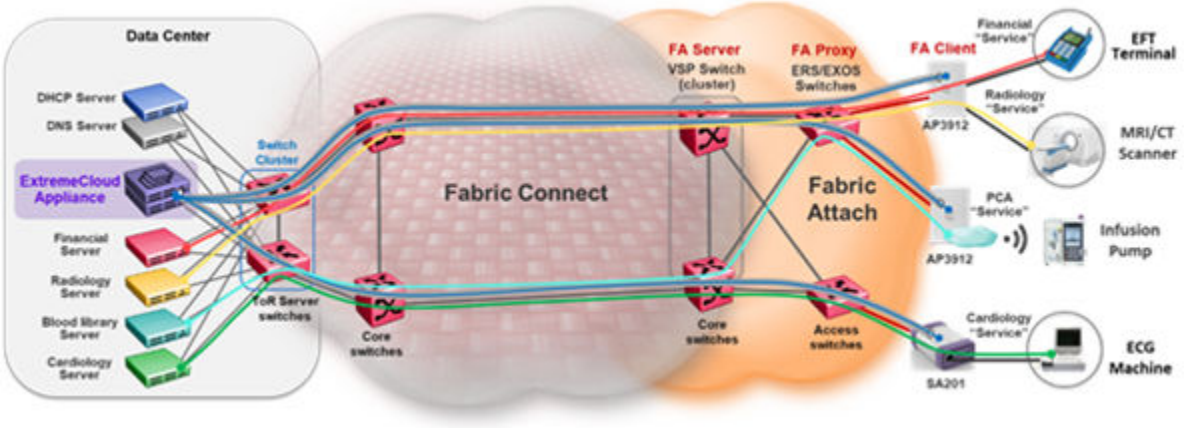


Figure 4: Fabric Connect with Fabric Attach model

2 Download and Install Extreme Defender Application

Download Defender Application

You can find the Defender Application docker app on the Extreme Networks support portal.

1 Log into the Extreme Portal to access the latest version of the Extreme Defender Application Docker app.

2 Go to **Products** > **ExtremeCloud**.

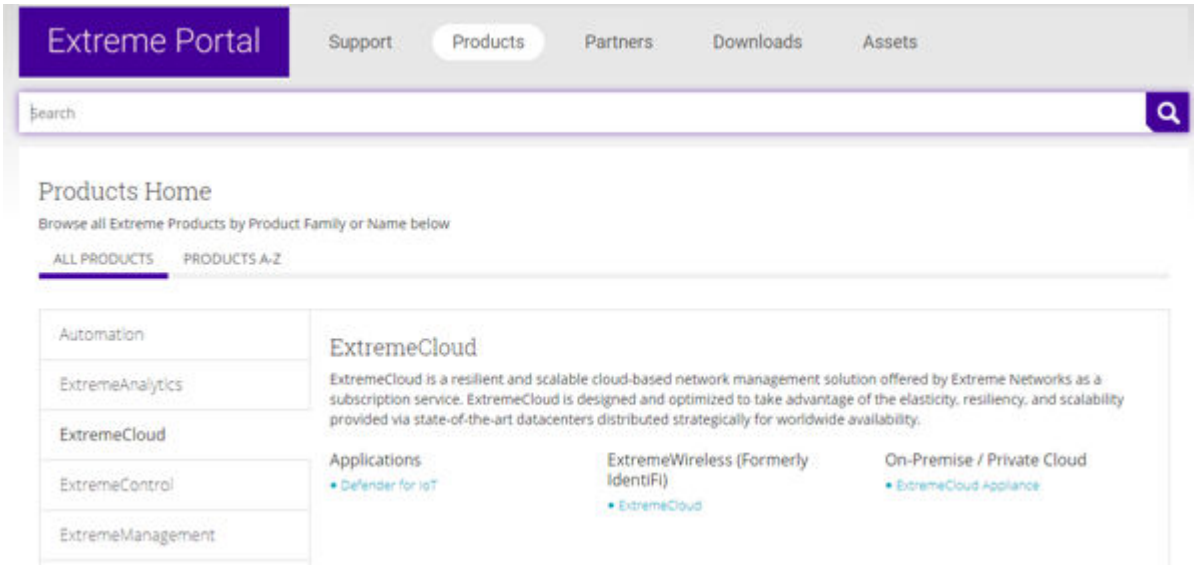


Figure 5: Defender for IoT on the Extreme Networks Support Portal

3 Select **Defender for IoT** for a list of product versions and release notes.

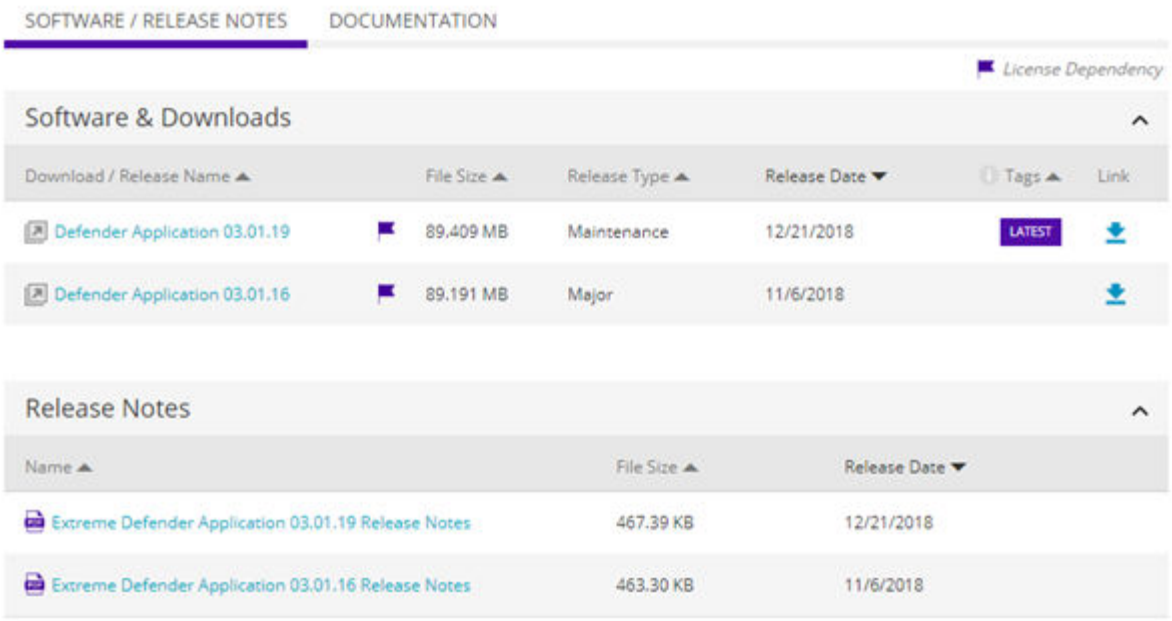


Figure 6: Defender Application downloads and release notes

Install Defender

Note

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

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

From the ExtremeCloud Appliance:

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

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

NEW! Generate API Key

To generate an API key in ExtremeCloud Appliance:

1 Log into ExtremeCloud Appliance with administrator credentials.

2 Go to **Administration** > **Accounts**.

3 Select a user account.

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

The key is generated. The API Key dialog displays.

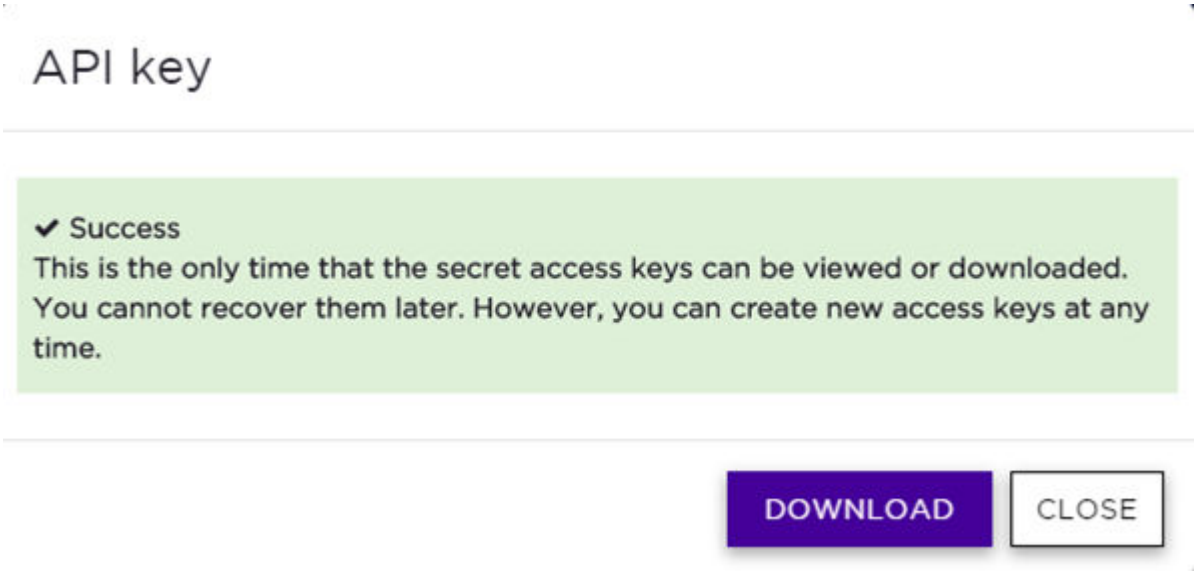


Figure 7: API Key dialog

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 Links

Upload the API Key File on page 13

NEW! Upload the API Key File

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

To upload a generated API key file:

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 Links

Run Defender Application on page 14
Generate API Key on page 12

Run Defender Application

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

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

To run the Extreme Defender Application:

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

   The following describes the available application actions:
   - — Install new application.
   - — Upgrade existing application.
   - — Uninstall application.
   - — Start application.
   - — Stop application.
   - — Show application statistics. Displays dashboard widgets, configuration details, and logs, and it provides console access to the application for troubleshooting.

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

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

Related Links

Configuration Wizard on page 15

Configuration Wizard

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

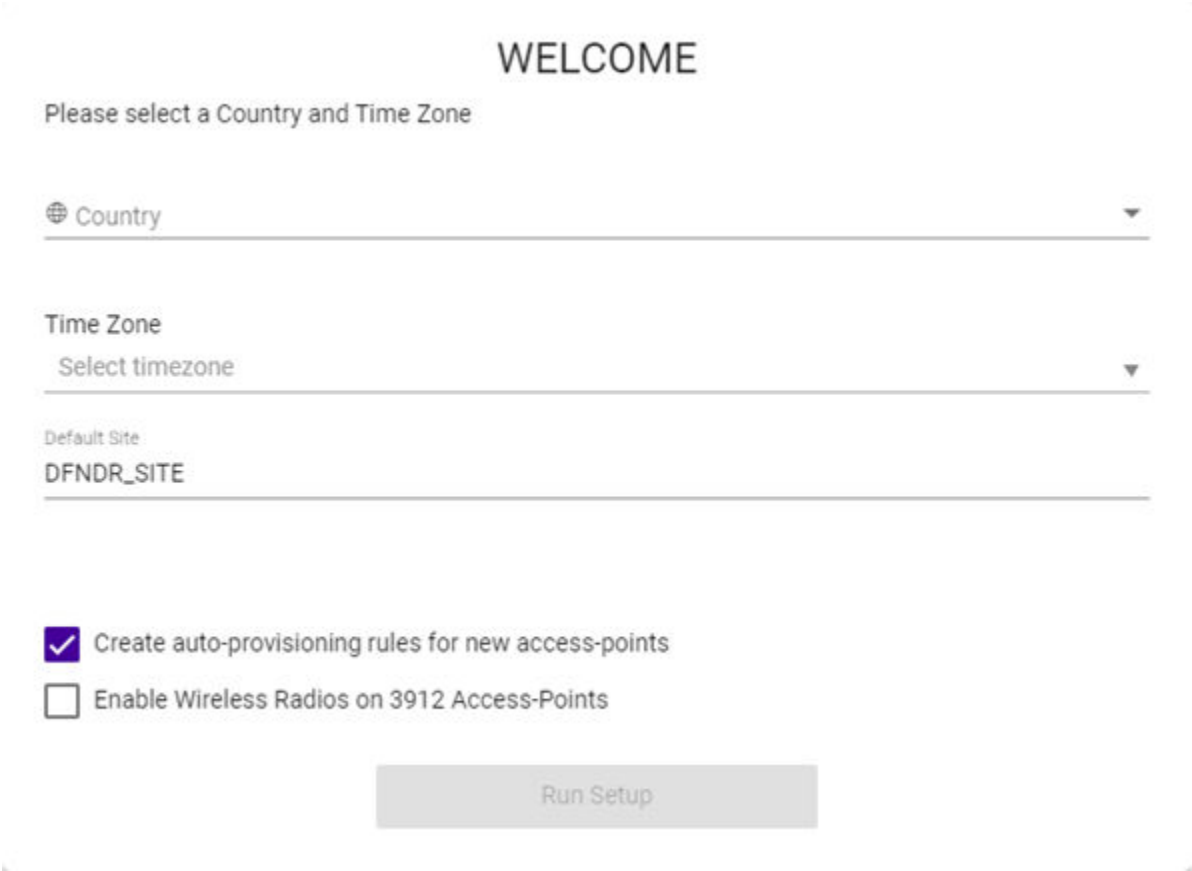


Figure 8: Defender Initial Configuration

Take the following steps:

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

Specify the values that correspond to your AP licensing domain.

2 (Optional) You can rename the default Defender site.

3 Check **Create auto-provisioning rules for new access points**.

This option creates adoption rules for your access points so that your access points are automatically discovered by the appliance. If you do not enable this option, you will have to go to ExtremeCloud Appliance and manually select your access points for provisioning.

4 Check **Enable Wireless Radios on 3912 Access-Points**.

Enable this option to allow wireless clients onto your network.

5 Select **Run Setup**.

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

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.

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**.

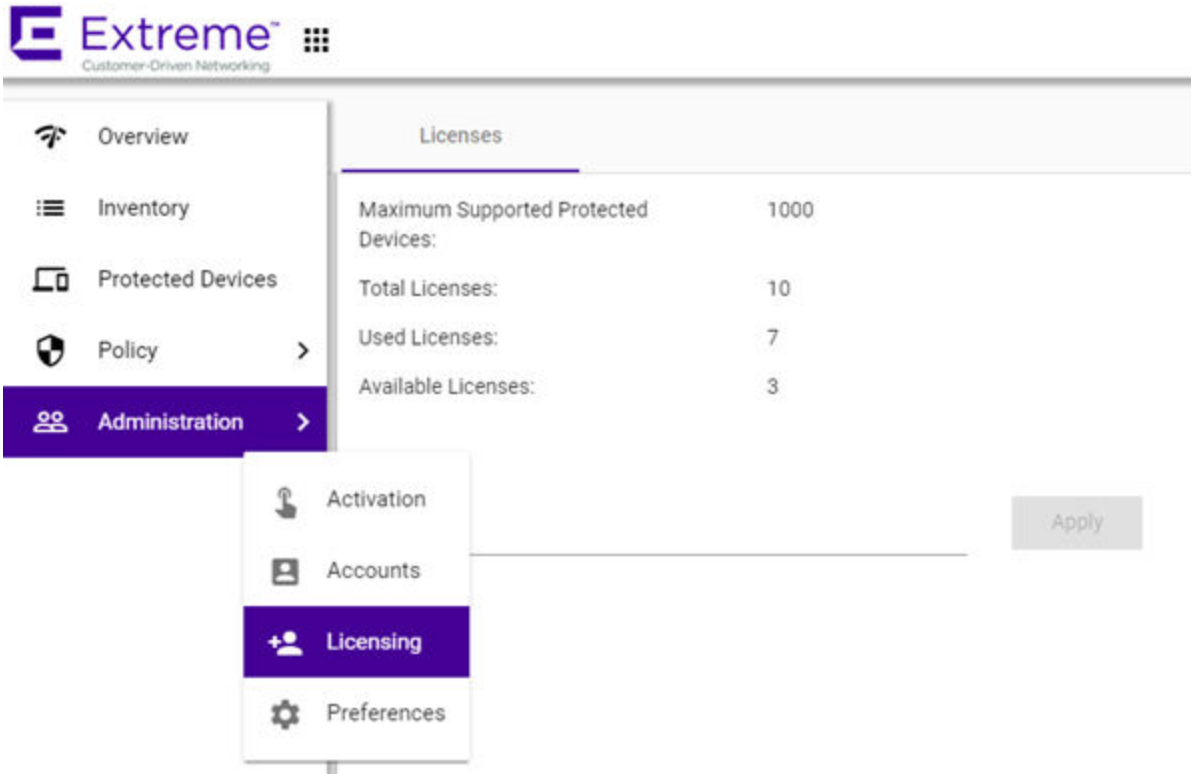


Figure 9: Defender Application Licensing Page

Figure 9 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.

NEW! User 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.

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

For more information on filtering data through the use of tags, see the Extreme Defender Application User Guide.

3 Add Managed Devices

Sites in Extreme Defender Application
Creating Defender Sites in ExtremeCloud Appliance

NEW! Sites in Extreme Defender Application

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

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

Note
Do not modify device group names.

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

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

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

- *Sites Overview*
- *Modifying Site Configuration*

NEW! Creating Defender Sites in ExtremeCloud Appliance

During the device activation process, Extreme Defender Application automatically creates sites and device groups on ExtremeCloud Appliance. The default name for the site is `DFNDR_SITE`. You can create additional Defender sites in ExtremeCloud Appliance and manually specify the site during device activation.

A best practice is to clone the `DFNDR_SITE`, ensuring that you have the proper device groups for each type of device supported in Extreme Defender Application.

To clone a site in ExtremeCloud Appliance:

1 Go to **Configure** > **Sites**.

2 Select the **DFNDR_SITE**.

The site dashboard displays.

3 Select **Clone** and provide a new Site name.

The site is cloned with the default device groups included:

- `DFNDR_Devices` that hold AP3912i devices.
- `DFNDR_SA201_Devices` that hold SA201 adapters.

Select a Site Using QR Code or Manual On-Boarding

When scanning a QR code or manually on-boarding your devices, you can select from a list of configured sites.

To select a site when on-boarding a device:

1 Go to **Administration** > **Activation**.

2 Scan the QR Code or select **Manual Onboarding**.

Note
The QR Code scan populates the device serial number and model. You can select a site.

3 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 19.

Name	Unique name for the AP or adapter.

Description	Text description of the AP or adapter.

Include a Site in the .CSV File

Specify the site in the .csv file to on-board devices to a specific site.

1 Go to **Administration** > **Activation** and do one of the following:
   - Select on the **Browse/Drop CSV** image and navigate to the .csv file.
   - Drag and Drop a .csv file onto the **Browse/Drop CSV** image.

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

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

.csv file format

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

```
serialNumber,hardwaretype,apName,description,site
1701Y-1248300023,AP3912i-FCC,TestAp,"description1",DFNDR_Area51
1701Y-1248300024,AP3912i-FCC,TestAp1,"description2",DFNDR_Area61
```

Note

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

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

Related Links

Sites in Extreme Defender Application on page 19

4 VLAN Configurations

Bridged@AP Configuration
Bridged@AC Configuration
Fabric Attach Configuration

Determine VLAN configuration before connecting an IoT device to the network through an SA201 adapter or AP3912i. Configure VLANs from ExtremeCloud Appliance. The deployment approach for Extreme Defender Application is to apply a role that specifies the VLAN service that the associated IoT device is meant to connect to. Depending on the deployment model, one or more VLAN configuration modes can be configured to achieve the desired service connection model:

- Bridged@AP — Untagged or tagged the VLAN configuration must be assigned to the switch port that the device is connected.

  Bridged@AP requires the access switch to have all desired VLANs to be in place to support any profile pushed to an SA201 adapter or AP3912i. For example, the access switch port must support tagging and any VLAN ID to be used must be a member of that port on the switch side. User traffic can be untagged if the user VLAN is the same as the Defender device VLAN.

  Note
  VLAN 1 can only be used as an untagged configuration. IoT device traffic assigned to VLAN ID 1 will be forwarded as untagged frames to the access switch.

- Bridged@AC — Traffic is tunneled back to ExtremeCloud Appliance and breaks out via a port (typically trunked/tagged) on the appliance. The tunneled traffic is secured with IPSec.

  Bridged@AC allows tagged or untagged user traffic from ExtremeCloud Appliance. Tagging is defined on the ExtremeCloud Appliance VLAN configuration page.

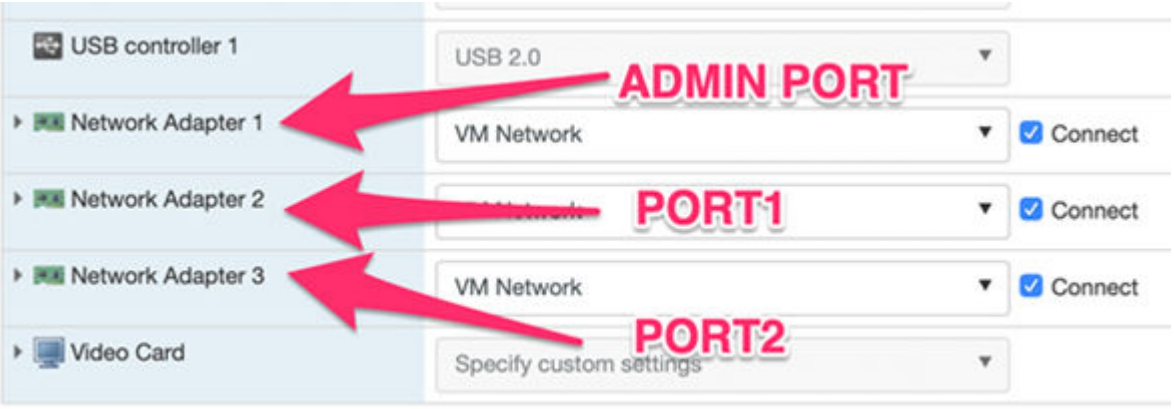


Figure 10: VMWare: Network Adapters connected to ExtremeCloud Appliance

- FabricAttach — Utilize Fabric Attach to automatically configure switch ports that the Defender device is plugged into.

  Note
  A fully-deployed and configured Fabric Attach network is required to implement a Fabric Connect topology.

  With Fabric Attach, you must define the VLAN ID and I-SID (fabric service ID). When Fabric Attach is supported and enabled on the access switch port, the access switch configuration is fully dynamic and automated. All ingress IoT traffic to the access switch is tagged with the VLAN configuration according to the service associated with the policy role. To validate that the network VLANs have been provisioned, from ExtremeCloud Appliance, go to **Configure** > **Policy** > **VLANs**.

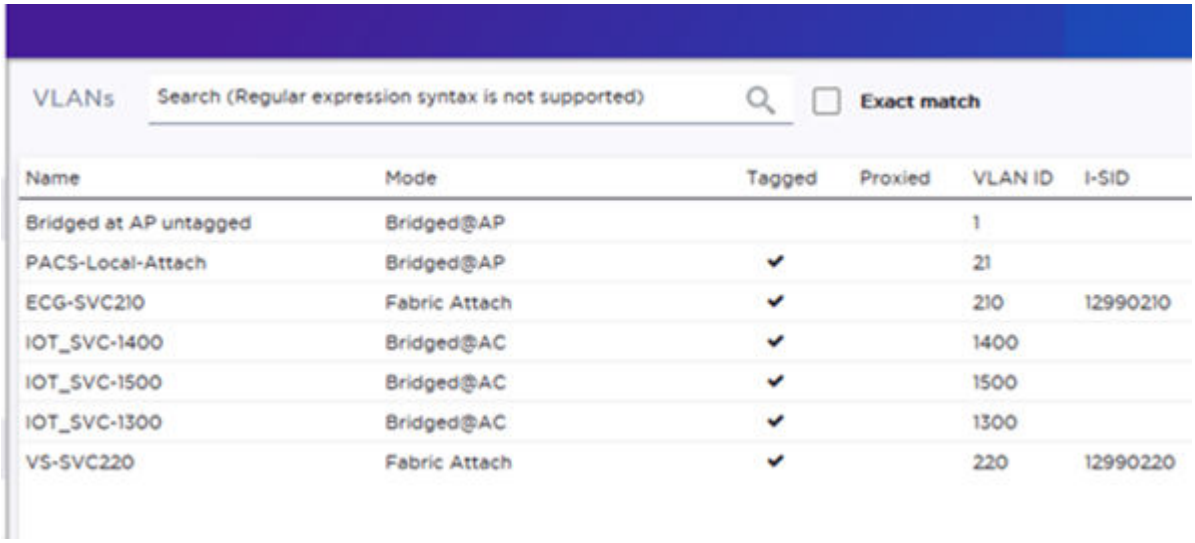


Figure 11: ExtremeCloud Appliance VLAN List

Related Links

Bridged@AP Configuration on page 23
Bridged@AC Configuration on page 24
Fabric Attach Configuration on page 26

Bridged@AP Configuration

To configure a B@AP topology, take the following steps:

1 From ExtremeCloud Appliance, go to **Configure** > **Policy** > **VLANs** and click **Add**.
2 Configure the following parameters:

Name	Provide a unique name for the VLAN.
Mode	Select **Bridged@AP** — Assigned to APs, the AP bridges traffic between its wired and wireless interfaces without involving the ExtremeCloud Appliance. The station's "point of presence" on the wired network for a bridged at AP topology is the AP's wired port.
VLAN ID	Provide a VLAN ID and select **Tagged**. The VLAN ID range is (1 - 4094). 4094 is reserved for Internal VLAN ID. Traffic linked to this service will be Tagged with the VLAN ID.

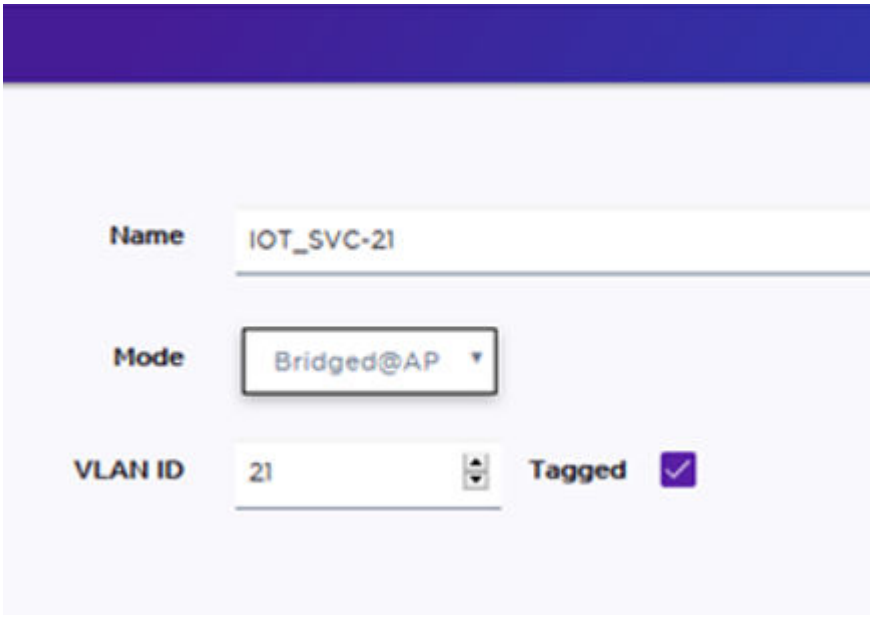


Figure 12: Bridged@AP VLAN Configuration

Using the settings shown in Figure 12, the local access switch must include the following:

- Switch configured with VLAN 21
- Switch port configured to support tagging.

  When the SA201 adapter or AP3912i is using *untagged* management, the access switch port must be configured to support both Untagged and Tagged frames.
- Switch port must be a member of VLAN 21

IoT traffic will be tagged with VLAN ID 21 egressing the SA201 adapter or AP3912i and forwarded into VLAN 21 on the access switch for routing across the IP network to the respective application server.

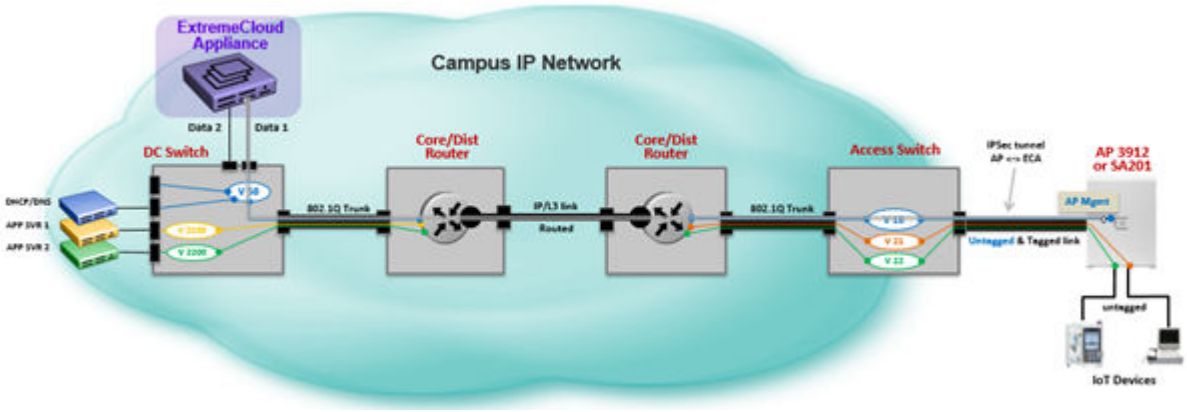


Figure 13: Topology using local VLAN attachment with Bridged@AP

Bridged@AC Configuration

To configure a B@AC topology, take the following steps:

1 From ExtremeCloud Appliance, go to **Configure** > **Policy** > **VLANs** and click **Add**.

2 Configure the following parameters:

Name	Provide a unique name for the VLAN.
Mode	Select **Bridged@AC** — The ExtremeCloud Appliance bridges traffic for the station through its interfaces, rather than routing the traffic. For B@AC, topology the station's "point of presence" on the wired network is the data plane port assigned to the topology.
VLAN ID	Provide a VLAN ID and select **Tagged**. The VLAN ID range is (1 - 4094). 4094 is reserved for Internal VLAN ID. Traffic linked to this service will be tagged with the VLAN ID, then tunneled to the ExtremeCloud Appliance and forwarded to the Data 2 port on ExtremeCloud Appliance. Optionally, you can select Layer 3 and configure an IP address that ExtremeCloud Appliance will use for the Layer 3 presence in the VLAN. DHCP services for the clients (server or relay) can also be enabled.
Port	The port for network traffic bridged at controller (for example, physical ports: Port0, Port1, Port3, Port4).
Layer 3	Check this box when configuring parameters for the network layer (B@AC).

Note
The **Certificates** button displays to configure browser certificates for captive portal security.

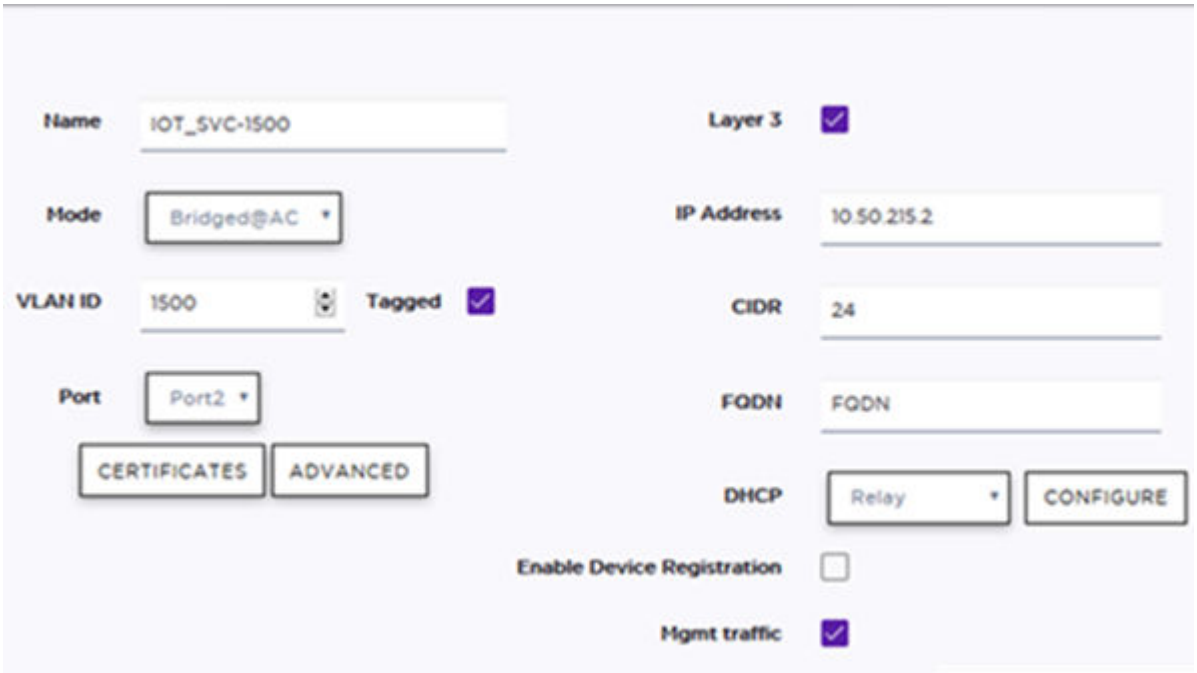


Figure 14: Bridged@AC VLAN Configuration

Using the settings shown in Figure 14, IoT device traffic assigned to a role that is using "IOT_SVC-1500" will be tagged with VLAN 1500 at the SA201 adapter or AP3912i, then tunneled to ExtremeCloud Appliance and forwarded to the remote VLAN with VID1500 tag egressing the Data Port2 on ExtremeCloud Appliance.

3 To configure one or more DHCP servers, next to the DHCP field, click **Configure** and enter the IP addresses of DHCP servers. If multiple servers are available, enter a comma delimited list.

Figure 15: DHCP Server Configuration

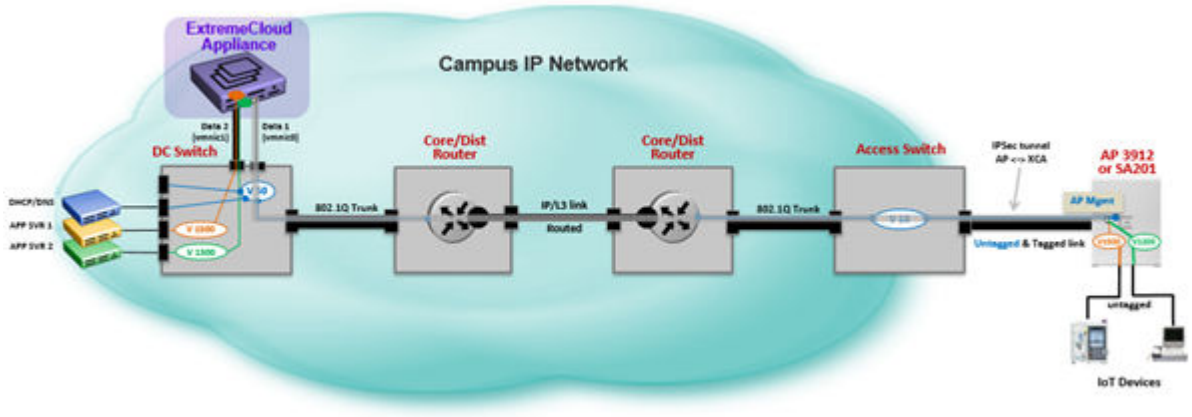


Figure 16: Topology using local VLAN attachment with Bridged@AC

Fabric Attach Configuration

You must create new VLANs from ExtremeCloud Appliance. To configure a Fabric Attach topology, take the following steps:

1 From ExtremeCloud Appliance, go to **Configure** > **Policy** > **VLANs** and click **Add**.

2 Configure the following parameters:

Name	Provide a unique name for the VLAN.
Mode	Select **Fabric Attach** — The FA Client component on the SA201 adapter or AP3912i signals the attached switch running in FA Server or FA Proxy mode, requesting a VLAN/I-SID mapping to the Fabric Connect service (backbone Service Identifier [IEEE 802.1ah]). An FA Client only communicates directly to an FA Server if the switch that it is connected to is running in that mode (VSP or ERS4900/5900). FA assignment requests sent to an FA Proxy switch (ERS or EXOS) rely on the switch to relay the request upstream to the FA server (VSP).
VLAN ID	Provide a VLAN ID and I-SID, and select **Tagged**. The VLAN ID range is (1 - 4094). 4094 is reserved for Internal VLAN ID. The I-SID range is (1-15999999). Traffic linked to this service will be Tagged with the VLAN ID, then forwarded to the fabric service (I-SID).

Fabric Attach signals the VLAN /I-SID binding to the network to dynamically set up this service if it is not already in place. This service can connect as a Virtual Layer 2 service or be connected to a Layer 3 service across the fabric.

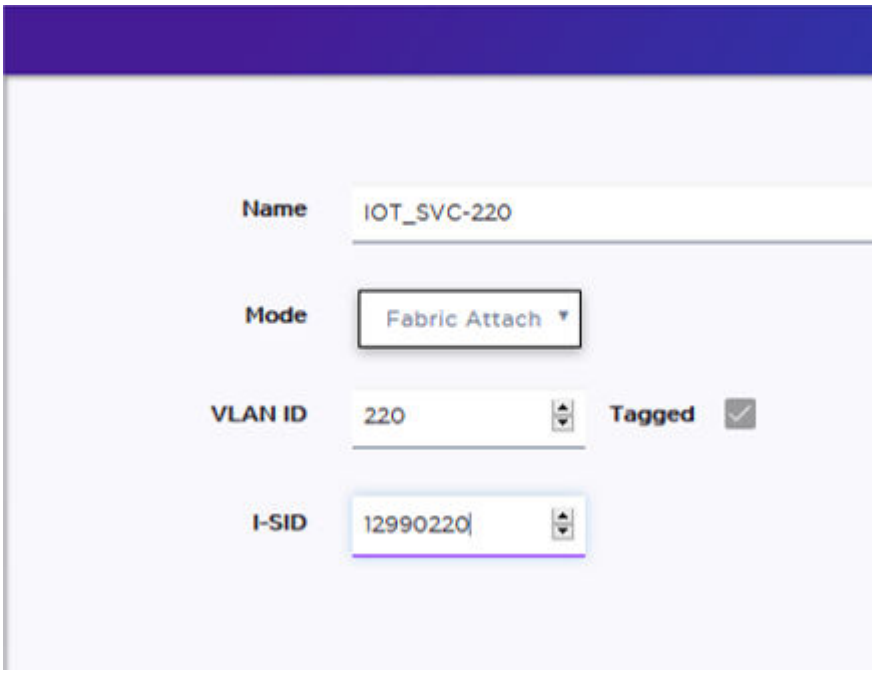


Figure 17: Fabric Attach VLAN Configuration

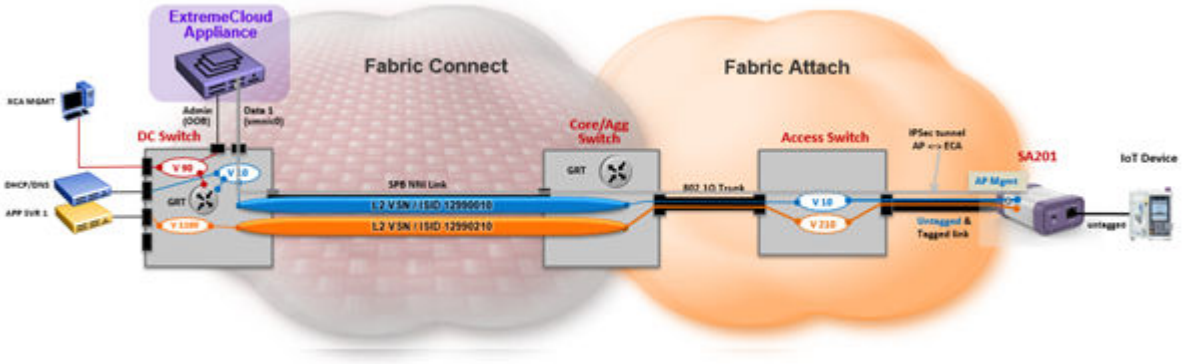


Figure 18: Topology using Fabric Attach mode

5 Creating Policy Roles and Policy Rules for IoT Devices

Automated Policy Generation

Extreme Defender Application provides an automatic Policy Generation tool to assist with the easy creation of policy rules for IoT devices. Any IoT device can be placed into policy generation mode. Packet capture is run for a configured length of time to capture traffic session information in a normalized environment.

Note
Only users with Full Admin access can run Policy Generator.

When the policy generator is running against a Protected Device, that device is placed in the Policy Generation Group that is associated with an `Allow All` policy rule. The device is displayed in the Defender Protected Devices List with a green shield icon that indicates it is being processed by the Policy Generator. When the capture session is complete, you can edit and save capture information as a role and use it as a whitelist policy. The IoT device is only allowed to communicate with other devices or hosts whose traffic matches allowed destination rules within the role.

Extreme Defender Application automated policy generation creates a role with Layer 3 and Layer 4 destination rules in the summarized list. An admin user can modify these rules and create Layer 2 though Layer 7 policy rules in Extreme Defender Application before saving the generated role. Once the role is saved, its rules can no longer be modified.

To manually create policy access control lists, first gather IoT device communication session information by external means, such as: Direct port mirroring on access switches or Remote port/traffic mirroring to a collection device. Packet capture files can be read by applications such as Wireshark or summarized by custom tools, providing a list that can be used to manually create a role in ExtremeCloud Appliance.

Policy roles, rules, and groups can be expanded or modified at any time within ExtremeCloud Appliance.

For more information about policy roles and the Defender Policy Generator, see the *Extreme Defender Application User Guide* at https://extremenetworks.com/documentation/defender-application. For more information about working with policy roles in ExtremeCloud Appliance, see *ExtremeCloud Appliance User Guide* at https://extremenetworks.com/documentation/extremecloud-appliance.

Related Links

Policy Groups and Roles for IoT Devices on page 29

Policy Groups and Roles for IoT Devices

Extreme Defender Application provides an automatic Policy Generation tool to assist with the easy creation of policy rules for IoT devices. 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.

The Extreme Defender Application setup wizard creates policy roles and an access control group for Defender IoT devices. ExtremeCloud Appliance administrators can create additional policy roles and access control groups for further classification of IoT devices. The Extreme Defender Application configuration wizard automatically creates the following:

- `DFNDR_DenyAll` policy role
- `DFNDR_PolicyGeneration Role` policy role
- `DFNDR_PolicyGeneration` access control group

One a role is generated, an admin user can modify generated rules and create Layer 2 though Layer 7 application policy rules in Extreme Defender Application before saving the generated role. Once the role is saved, its rules can no longer be modified.

From ExtremeCloud Appliance, users with Admin privileges can create additional roles containing L2-L7 rules that can apply to specific IoT devices and device groups. Admin users can also create additional access control groups that can further classify common IoT device types.

Note

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

Related Links

Automated Policy Generation on page 28

Create Policy Roles

Policy roles are used to apply a specific set of Layer 2, 3, 4 and 7 filter classifiers against traffic flows to and from IoT devices to control communication. A whitelist approach is used with the Defender for IoT Solution to constrain traffic from an IoT device restricting communications to a specific set of destination application servers or hosts. Therefore, the Default Action `Deny` is used while specifying the service that the IoT device will be connected to. Communications is only permitted for traffic matching the L2-L7 rules within the role. All other non-matching traffic is denied.

Related Links

Manual Role Creation on page 30
Automatic Role Creation on page 30
Example: DICOM Client Whitelist Role on page 31

Manual Role Creation

To create a role manually:

1 Log in to ExtremeCloud Appliance and go to **Configure** > **Policy** > **Roles** > **Add**.

> **Note**
> Roles created for access from the Extreme Defender Application must be named with the DFNDR_ prefix.

2 Configure the following parameters:

Name	Name of the role.
Bandwidth Limit (Optional)	Select this option to allow unlimited bandwidth. Click to set the Class of Service value.
Default Action	Deny. Deny packets that do not match a filter rule or deny packets when a filter rule does not exist. When a packet *does* match the filter rule action Allow, allow packet using the specified VLAN option. Specify either the Default Network VLAN or a configured VLAN.
VLAN ID	VLAN ID to connect IoT devices using this policy role associated with the group.
Associated Profile	Indicates profiles that this role is associated with. Select to modify profile association. To ensure a device profile (SA201 adapter or AP3912i) is selected to support the new role, select . You will also be prompted to select the Associated Profiles when saving the role.

> **Note**
> Associate a role with a configuration Profile. The configuration Profile is associated with the device group. Each AP in the device group makes use of the policy role.

Related Links

Automatic Role Creation on page 30

Automatic Role Creation

The Defender Policy Generator is a tool to assist IT Administrators to capture traffic flow information from an IoT device over a specified length of time and then use the traffic session information to create a whitelist set of filter rules for a new role. The Policy Generator creates a list of “normalized” communication sessions between the IoT device and other hosts, which can then be saved and applied to the IoT device to lock down communications based on the learned session information.

To automatically create a role for an IoT device, take the following steps:

1 Log in to Extreme Defender Application and go to **Protected Devices**.
2 Select an active, on-boarded device by clicking on the IP, MAC or Host name fields in the list.

> **Note**
> The device must be in active, on-boarded status to enable the **Policy Generator** tab.

3 From the Protected Device Detail, select the **Policy Generator** tab.
4 Enter the time in seconds at the **Capture Time** field, then click **Next**.

5 On the Select a VLAN dialog, enter the VLAN service that you wish to run the IoT device traffic capture session in and click **Start**.

While the capture is running, a green shield will appear next to the IoT Protected Device.

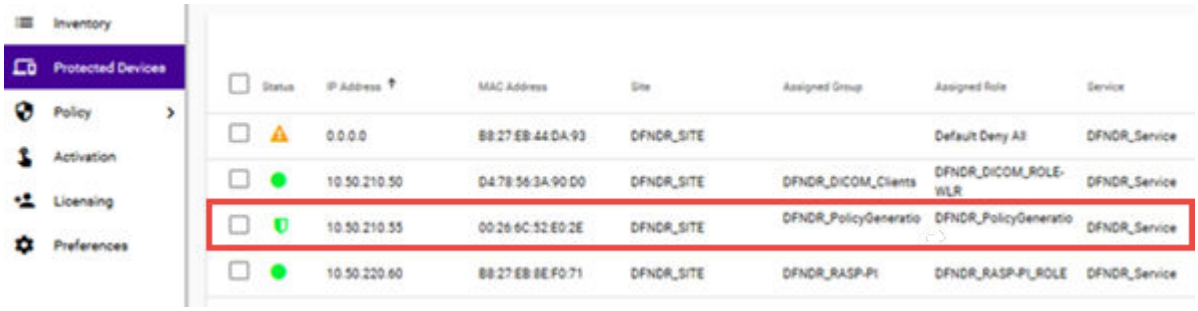


Figure 19: Protected Device List -- Auto Policy Generation

6 When the capture is complete, click **Open Generated Role for Editing**

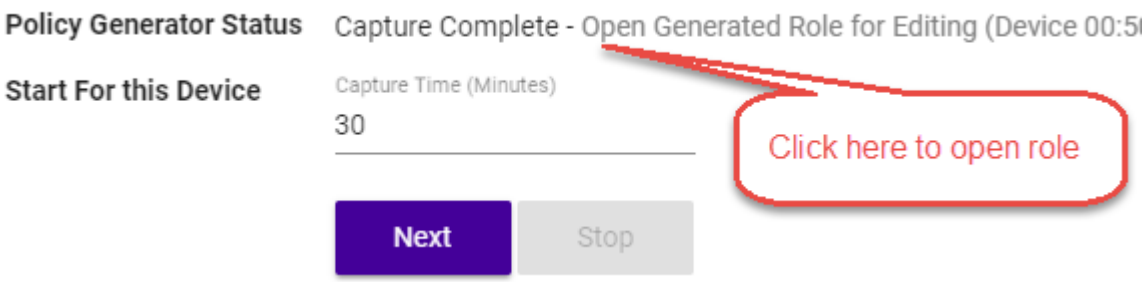


Figure 20: Open Generated Role

7 Before you save the role, you can modify or add new allowed session entries.

Note

Extreme Defender Application automated policy generation creates a role with Layer 3 and Layer 4 destination rules in the summarized list. An admin user can modify these rules and create Layer 2 though Layer 7 policy rules in Extreme Defender Application before saving the generated role. Once the role is saved, its rules can no longer be modified.

Related Links

Manual Role Creation on page 30

Example: DICOM Client Whitelist Role

This topic illustrates how to manually create new roles for a DICOM (Digital Imaging and Communications in Medicine) imaging device. DICOM is a an imaging file format and network protocol.

1 Log in to ExtremeCloud Appliance.

2 Go to **Configure** > **Policy** > **Roles** and select **Add**.

3 Configure the following parameters:

Name	Use an appropriate name that summarizes the rule. The rule name must start with the `DFNDR_` prefix to allow Extreme Defender Application to manage the role.
Default Action	Set the default action to **Deny**.
VLAN ID	Select the VLAN ID to which the DICOM Client must connect.
Associated Profile	Indicates profiles that this role is associated with. Select ✎ to modify profile association. To ensure a device profile (SA201 adapter or AP3912i) is selected to support the new role, select ✎. You will also be prompted to select the Associated Profiles when saving the role.

Note
Associate a role with a configuration Profile. The configuration Profile is associated with the device group. Each AP in the device group makes use of the policy role.

Rules	Select the rule drop-down arrow to edit the full rule options for Classification and Action.

4 Provide an individual Allow action for all new L2-7 rules. If a packet does not match any listed rules, the packet will be denied per the default action.

Select **New** and select the rule row to edit the full rule options for Classification and Action.

The following is an example of a rule allowing DICOM application or protocol between the client device and a Picture Archiving Comms Server (PACS) host.

- Action: Allow
- Protocol: TCP
- PACS host IP address: 10.50.200.10/32
- Port Range: 4242 to 4242

Figure 21: Rule to allow DICOM application or protocol between client device and a (PACS) host

5 Select **New** and select the rule row to edit the full rule options for Classification and Action.

The following is an example of a rule to allow ICMP (Ping) between the DICOM client device and the PACS host IP subnet:

- Action: Allow
- Protocol: ICMP
- PACS host IP subnet: 10.50.200.0/24

Figure 22: Rule to allow ICMP (Ping) between the DICOM client device and the PACS host IP subnet

6 Follow the same steps to add new rules and edit rule configuration information. The following is an example rule to allow DHCP packets to a DHCP Server.

Figure 23: Example rule to allow DHCP packets to a DHCP Server

7 Follow the same steps to add new rules and edit Rule configuration information. The following is an example rule to allow DNS packets to a DNS Server.

Figure 24: Example rule to allow DNS packets to a DNS Server

8 Optionally, add further rules to allow access to other hosts or devices. The following is an example rule to allow HTTP to a specific host from the client IoT device.

Figure 25: Example rule to allow HTTP to a specific host from the client IoT device

9 When all the rules are created, select **Save**. If this is a new role, you are prompted to associate the role with a device configuration Profile. Verify that the correct SA201 adapter or AP3912i configuration Profiles are selected.

The role is now ready to be linked to a Group Profile.

Layer 7 Application Rules

An *application rule* leverages the AP's deep packet inspection (DPI) engine to detect the underlying application to which a frame or flow belongs. The rule then applies access control and quality of service actions to all the traffic associated with the application, not just traffic destined for specific IP addresses or ports. The control actions regulate both access control and traffic engineering (rate limit, marking, and prioritization) for applications and groups.

Using application rules provides greater traffic enforcement against traffic from an IoT device to further constrain and control communications from the device.

Create Layer 7 application rules and configure the Default Action as “Allow”. Because IoT device security is predicated on using a whitelist approach, when you add a Layer 7 application rule, you must add a final set of Deny catchall rules. The Deny rules will deny all traffic other than traffic allowed by the specific L2- L4 rules and the application traffic (L7).

Figure 26 is an example of a whitelist role that is comprised of rules from L3, L4 and L7. This role allows the following:

- DICOM protocol
- DHCP
- DNS
- HTTP to an IP Subnet

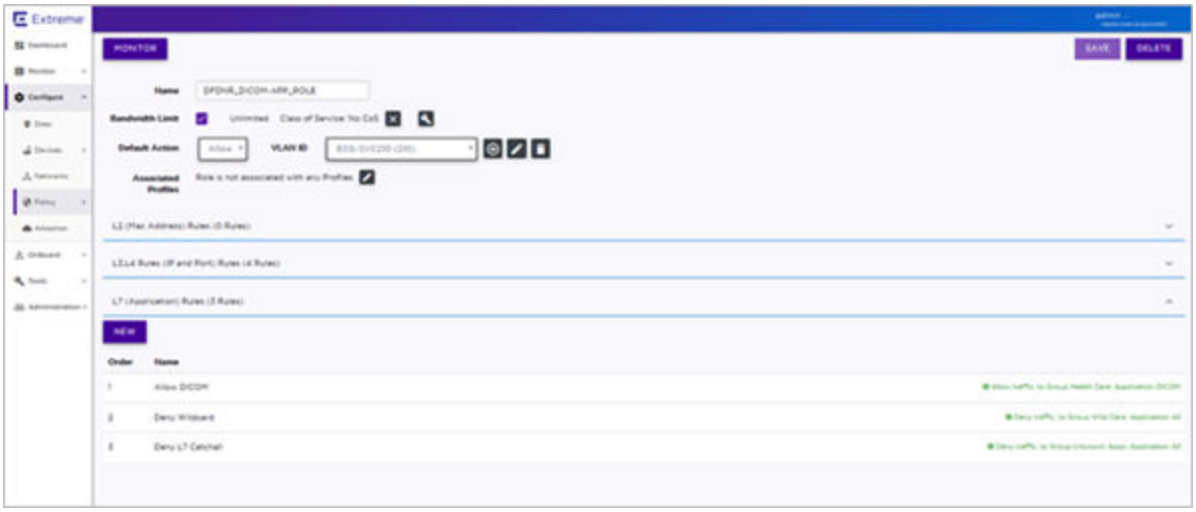


Figure 26: Whitelist role with L3, L4 and L7 rules

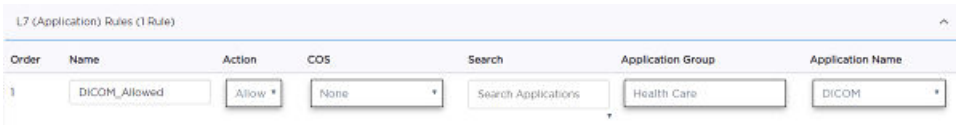


Figure 27: Whitelist rule detail

Related Links

Create Layer 7 Application Rules on page 34

Create Layer 7 Application Rules

1 Log in to ExtremeCloud Appliance.

2 Go to **Configure** > **Policy** > **Roles** and select **Add**.

3 Configure the following parameters:

Name	Use an appropriate name that summarizes the rule.
Default Action	Set the default action to **Allow**.
VLAN ID	Select the VLAN ID to which the DICOM Client must connect.
Associated Profile	Indicates profiles that this role is associated with. Select ✎ to modify profile association. To ensure a device profile (SA201 adapter or AP3912i) is selected to support the new role, select ✎. You will also be prompted to select the Associated Profiles when saving the role.

Note
Associate a role with a configuration Profile. The configuration Profile is associated with the device group. Each AP in the device group makes use of the policy role.

Rules	Expand **L7 Application Rules** section and select **New**.

4 Configure the following for the application rule:

- Rule Name — DICOM APP
- Action — **Allow**
- Search *Healthcare*
- Application Group — Health Care
- Application Name — DICOM

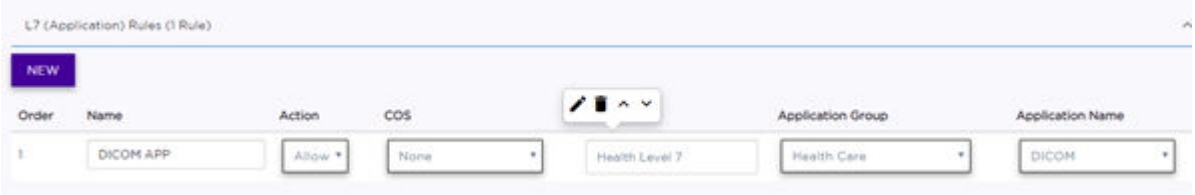


Figure 28: ExtremeCloud Appliance Layer 7 rule configuration

5 Because DICOM is the only allowed application, the next step is to deny all other applications. Click **New** to enter a second L7 rule:

- Rule name — Deny Wild card
- Action — **Deny**
- Application Group — **Wild Card**.

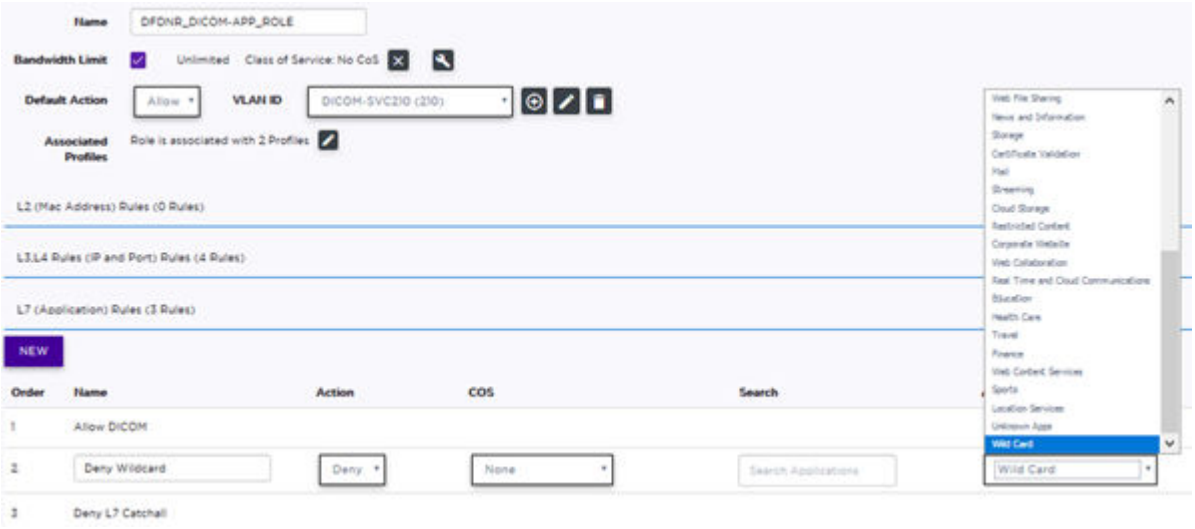


Figure 29: ExtremeCloud Appliance DICOM role with Layer 7 Wild Card rules

6 To catch any other applications whose signatures may not be recognized by ExtremeCloud Appliance, an additional Deny rule for unknown applications is required. Click **New** to enter a third L7 rule:

- Rule Name — Deny Catchall
- Action — **Deny**
- Application Group — **Unknown Apps**

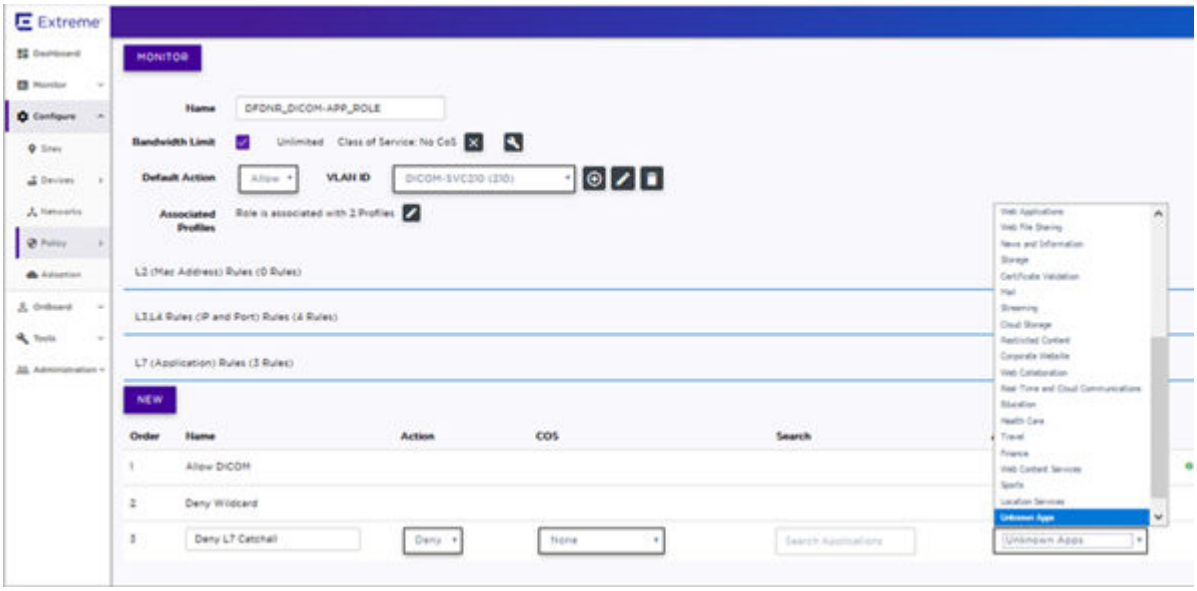


Figure 30: ExtremeCloud Appliance DICOM role with Layer 7 Unknown Apps rules

7 To support selected Layer 3 / 4 rules, expand the L3, L4 (IP and Port) Rules section and select **New**.

For an example of Layer 3 and Layer 4 rules that allow DHCP, DNS for the DICOM Client device, and allow HTTP to a specific IP subnet, see Example: DICOM Client Whitelist Role on page 31.

Note

As L2, L3 or L4 rules precede Layer 7, avoid classifying traffic on a broad basis, which could negate Layer 7 rules. For example, L2; allowing all traffic from a source MAC, or L3/4; allowing UDP and/or TCP with a large or open port range to an IP host.

8 From ExtremeCloud Appliance, create a Group Profile for this role. See Create Onboard Groups in ExtremeCloud Appliance on page 38, then create an Access Control Rule with conditions that link the Group to the created Application Role.

You can also, create a Group Profile within Defender (see Create Onboard Groups in Defender Application on page 39) and associate the DICOM Application based Role to the Group.

Security Profile Creation Workflow

Figure 31 illustrates the process for creating a policy role with filter rules and creating an Onboard Access Control Group that will use the role, resulting in the creation of a security profile. The workflow tasks vary depending on creating the role using the auto policy generator or the manual approach.

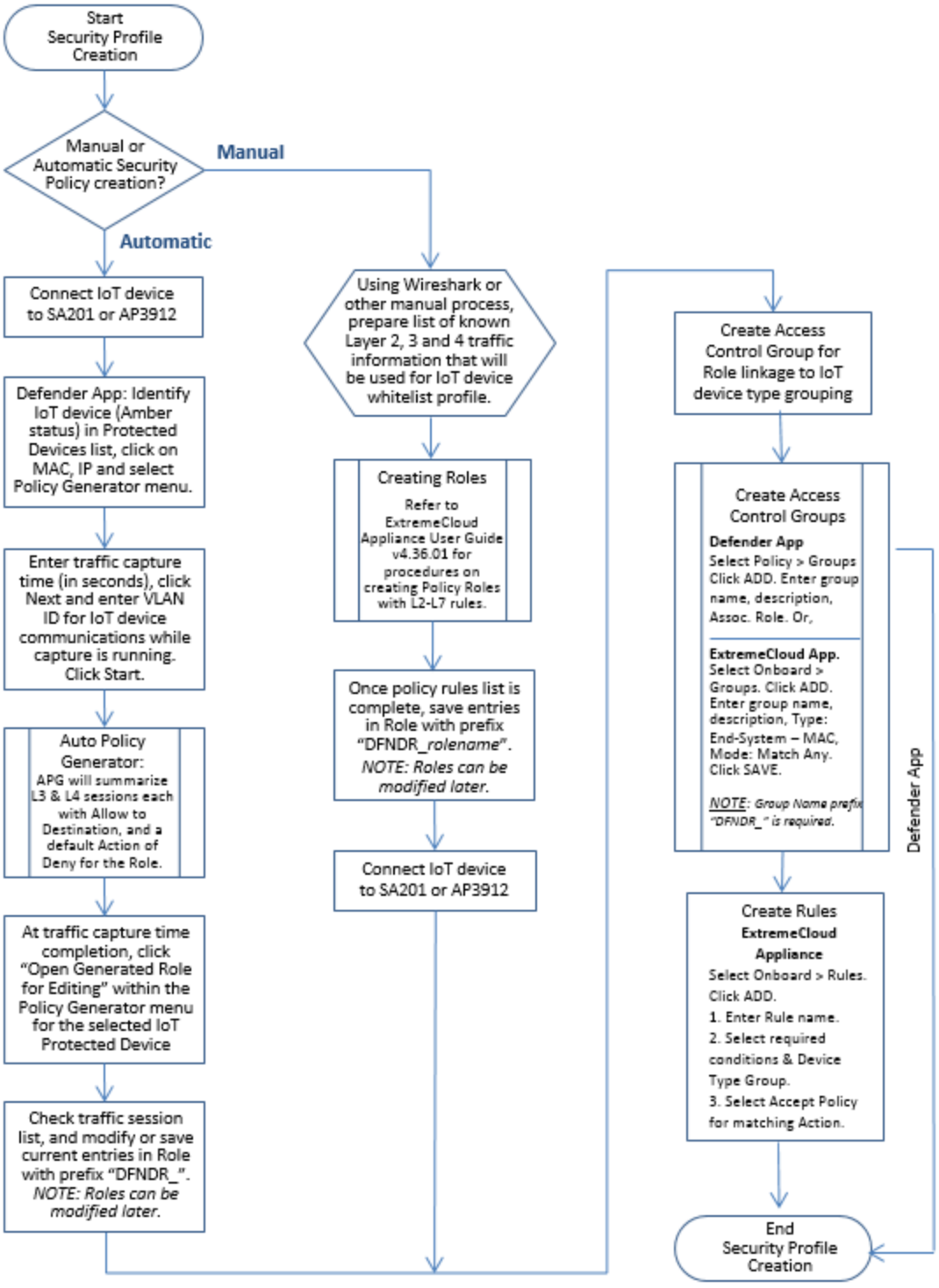


Figure 31: Security Profile Creation Workflow

6 Create Onboard Access Control Groups and Rules

We have created network policy roles under Create Policy Roles on page 29, now we will create access control groups and rules. An access control rule automates the onboarding process. It is comprised of a policy role and an access control group.

An access control group is used to organize mobile clients by various group types, including device type or end system characteristics such as IP address, hostname, or LDAP host group. Configure groups to be used with access control rules. ExtremeCloud Appliance provides a set of default system groups with your installation to simplify the group set up process.

Related Links

Create Onboard Groups in ExtremeCloud Appliance on page 38
Create Onboard Groups in Defender Application on page 39
Create Onboard Rules on page 40

Create Onboard Groups in ExtremeCloud Appliance

To create access control groups or Onboard Groups from ExtremeCloud Appliance, take the following steps:

1 Go to **Onboard** > **Groups** and click **Add**.
2 Configure the following parameters:

Group Name Name of the group.

Description Description of the group.

Group Type Criteria by which the accounts are grouped. Select **End System – MAC**.

This type is used for IoT device MAC authentication to the group where a Defender Group Profile is selected against an IoT device in the Defender Protected Devices list.

Group Mode For End System LDAP Host Groups only. Not applicable here.

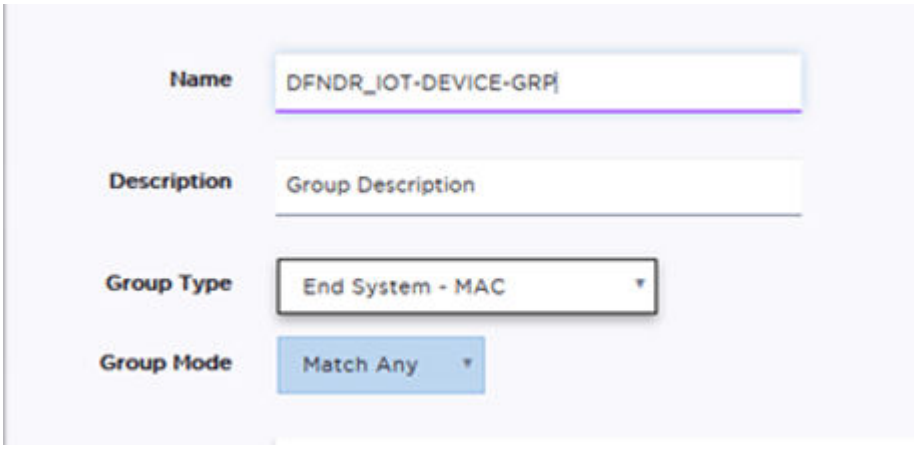


Figure 32: ExtremeCloud Appliance Onboard Group settings

When the MAC of a discovered IoT device is assigned to a Group profile, the MAC address is automatically added to the associated group's list as a *Defender Auto Added MAC*.

Create Onboard Groups in Defender Application

To create access control groups or Onboard groups from Extreme Defender Application, take the following steps:

1 Go to **Policy** > **Groups** and click **Add**.

2 Configure the following parameters:

Group Name	Name of the group.
Description	Description of the group.
Associated Role	Select the role that will apply policy rules to devices that authenticate with this group.

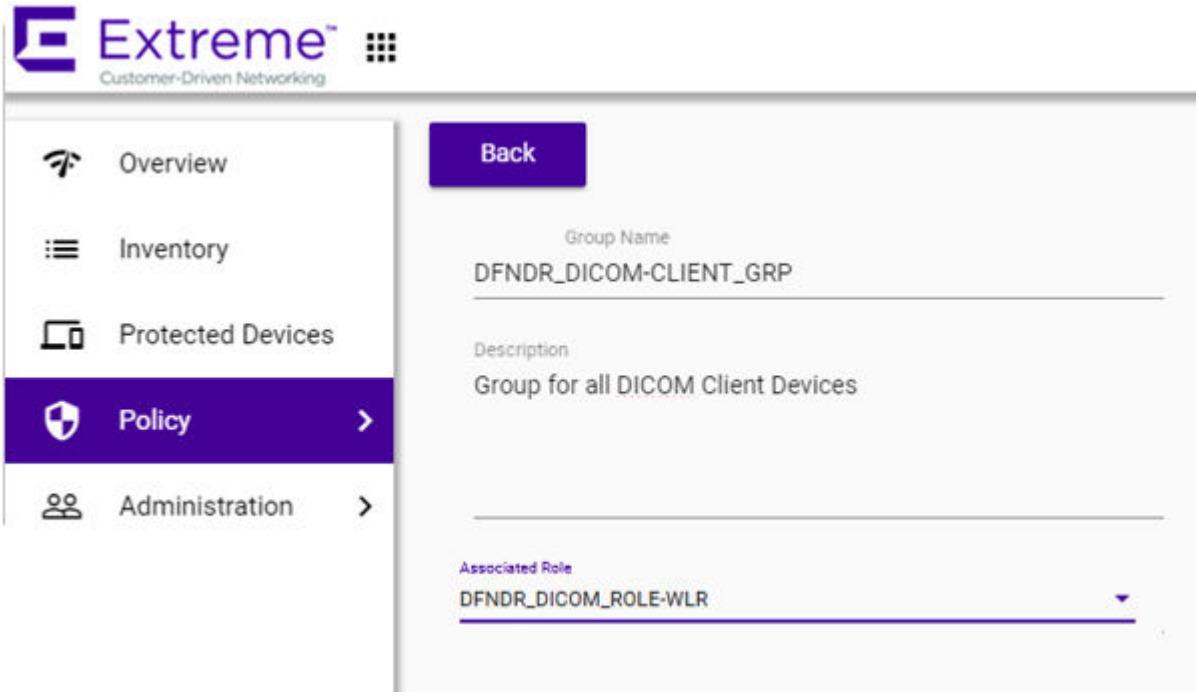


Figure 33: Defender Application Onboard Group configuration

3 Within Extreme Defender Application all groups created and associated to a role automatically create an Access Control Rule within ExtremeCloud Appliance.

To validate, from ExtremeCloud Appliance, go to **Onboard** > **Rules** and view the End-System Rule Conditions linking the Group Profile Policy to the Access Policy.

Name	Conditions	Accept Policy	Portal
Blacklist	End-System is in **Blacklist**	Quarantine	Default
DFNDR_DICOM-CLIENTS-GRP_RULE	End-System is in **DFNDR_DICOM-CLIENTS-GRP**	DFNDR_DICOM_ROLE-WLR	Default
IOT-DEVICE-A_RULE	End-System is in **DFNDR_IOT-DEVICE-GRP** and Location is in **Network: DFNDR_Service**	DFNDR_RASP-PI_ROLE	Default
DFNDR_ECG-PI_RULE	End-System is in **DFNDR_ECG-PI_GRP**	DFNDR_ECG-PI-ROLE-WLR	Default
DFNDR_HEALTHYPI_RULE	End-System is in **DFNDR_HEALTHYPI_GRP**	DFNDR_HEALTHYPI_ROLE-WLR	Default
DFNDR_DICOM-APP_RULE	End-System is in **DFDNR_DICOM-APP_GRP**	DFDNR_DICOM-APP_ROLE	Default
DFNDR_VS-Camera_RULE	End-System is in **DFNDR_VS-Cameras**	DFNDR_VS-Camera_ROLE	Default
EXTR_VS-Cameras	End-System is in **AP3916-Cameras**	VS-Camera_ROLE	Default
DFDNR_RASP-PI	End-System is in **DFNDR_RASP-PI**	DFNDR_RASP-PI_ROLE	Default
DFNDR_PolicyGeneration_RULE	End-System is in **DFNDR_PolicyGeneration**	DFNDR_PolicyGeneration	Default
Default Catchall		Deny Access	Default

Figure 34: ExtremeCloud Appliance Onboard Rules List

Create Onboard Rules

Access Control Rules allow you to apply network access permissions and restrictions based on defined rules. The rules can address network resources, a user's role or purpose in the organization, or the device type that is used to access the network. Network access control is dynamic. End-user network

access can change as group associations change without a network administrator getting involved. For more information, see the *ExtremeCloud Appliance User Guide* at https://extremenetworks.com/documentation/extremecloud-appliance.

After creating a role, you can create a policy group within ExtremeCloud Appliance or Extreme Defender Application.

Note
Access Control Rules need to be manually created only when the role and policy group is manually created from ExtremeCloud Appliance.

To create an Access Control Rule in ExtremeCloud Appliance:

1 Go to **Onboard** > **Rules** and click **Add**.
2 Configure the following parameters:

Name	Name of the rule. This does not require “DFNDR_” prefix
Rule Enabled	Check to enable the rule.
Conditions	Configure the conditions that must be met to allow access for devices associated to specific groups.

User Group	Any
End-System Group	Select group profile.
Device Type Group	Any — unless the system OS is well known.
Location Group	Defender Network Service
Action	

Accept Policy	Select desired role containing L2-L7 rules and service.
Portal	Default

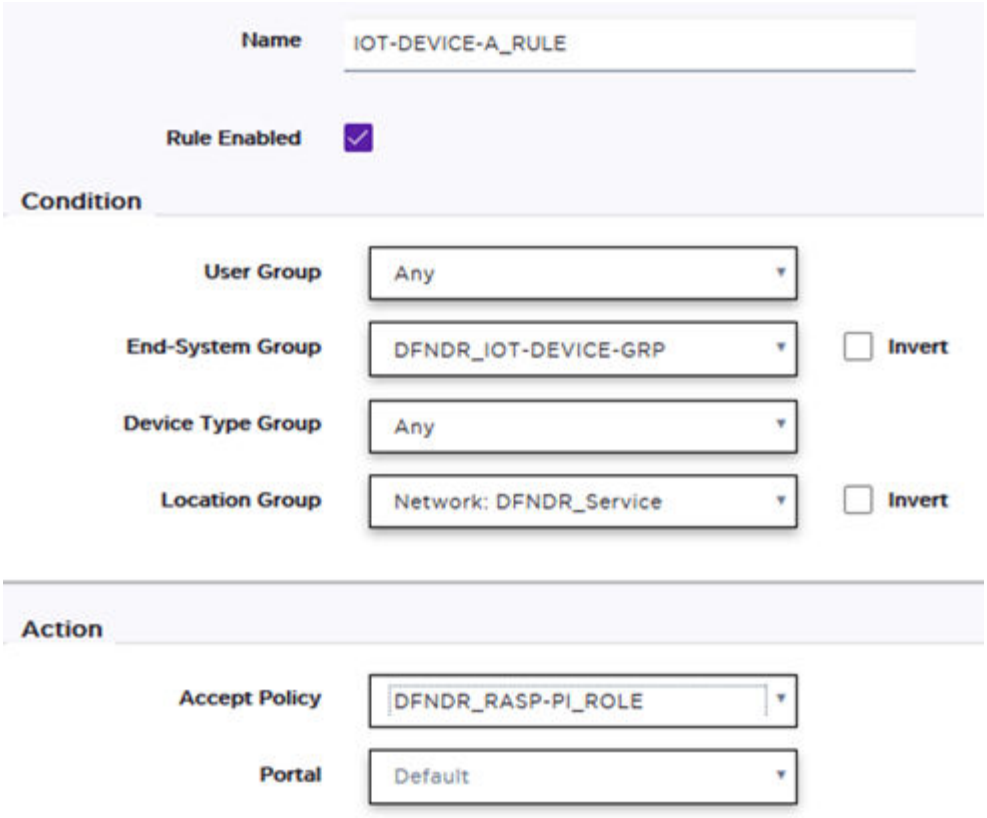


Figure 35: ExtremeCloud Appliance Access Control Rule

3 Click **Save**.

New rule displays in the Onboard Rules list.

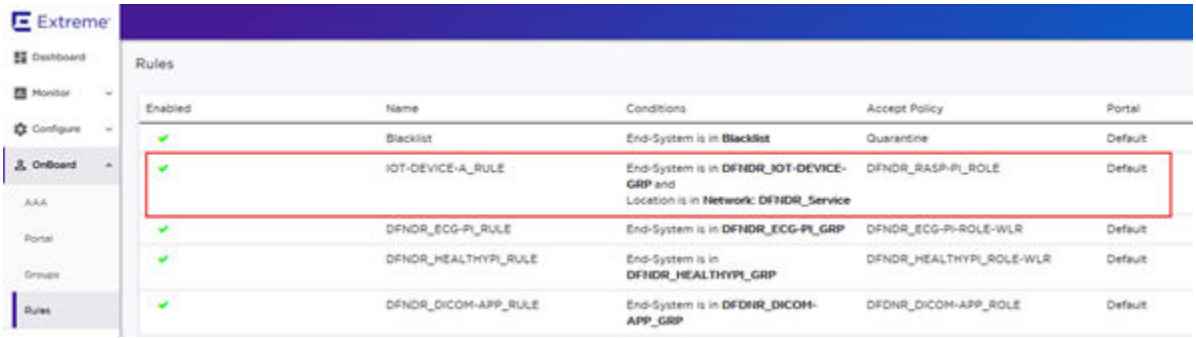


Figure 36: Defender IoT Access Control Rule — ExtremeCloud Appliance

Apply Security Profiles in Extreme Defender Application

Once policy roles and groups are created, we can deploy them with connected IoT devices within Extreme Defender Application. Connect a DICOM Client device to an active SA201 or AP3912 and apply the group security Profile.

1 From the Protected Devices list, select a device check box and click the group icon .

2 From the **Select a Group** drop-down, select the desired group Profile to apply to the DICOM device and click **OK**.

3 (Optional) you can click on the device IP address, MAC address or Host name in the **Protected Devices** list and enter a text description for the device.

4 When Defender has assigned the group profile and policy, from the **Policy** tab, verify the associated group to view the MAC addresses of assigned devices. The MAC address is automatically added to the group when the group profile is assigned to the device.

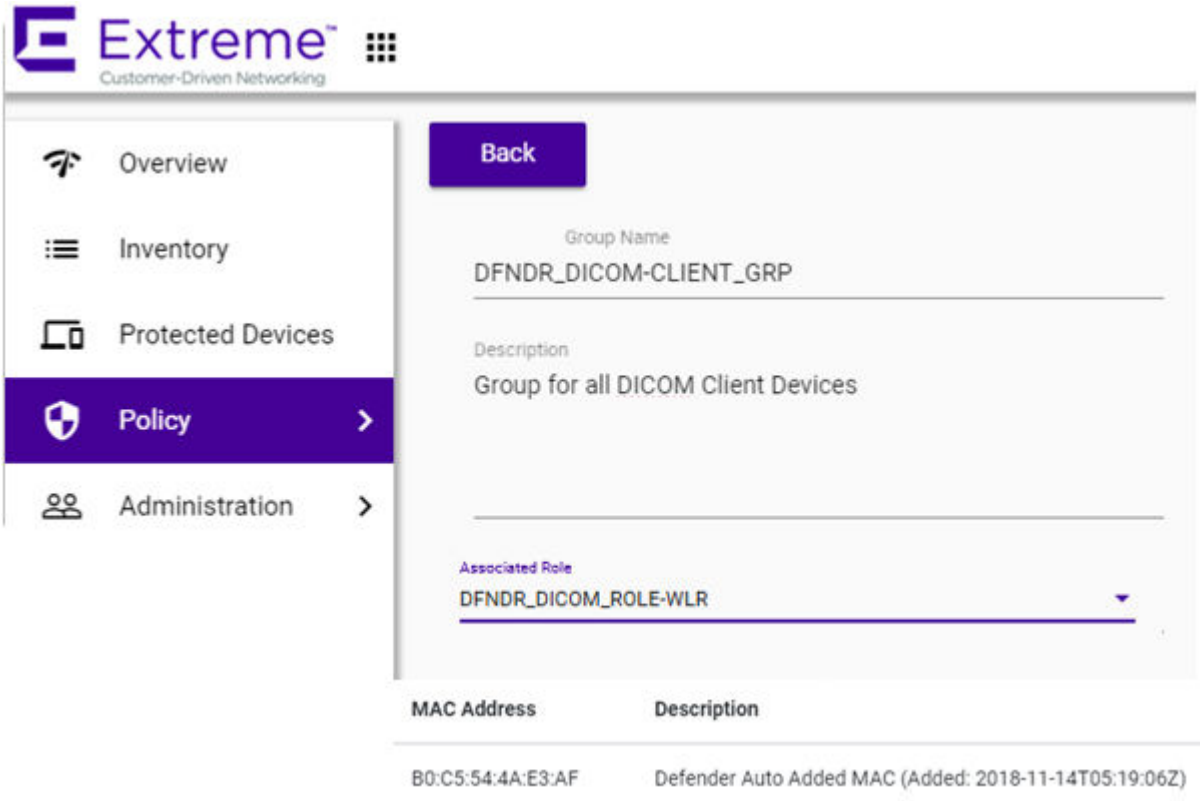


Figure 37: Policy Group with MAC Address included

Selecting group from Device Details

You can also navigate to the group policy assignment for the IoT device by clicking on the device serial number.

1 On the **Inventory** list, click the device Serial Number for the unassigned IoT device (Amber Status).

2 From the **Device Details** view, identify the IoT device and select a group policy to assign to the IoT device.

3 Click **Save**.

The Group policy is now applied.

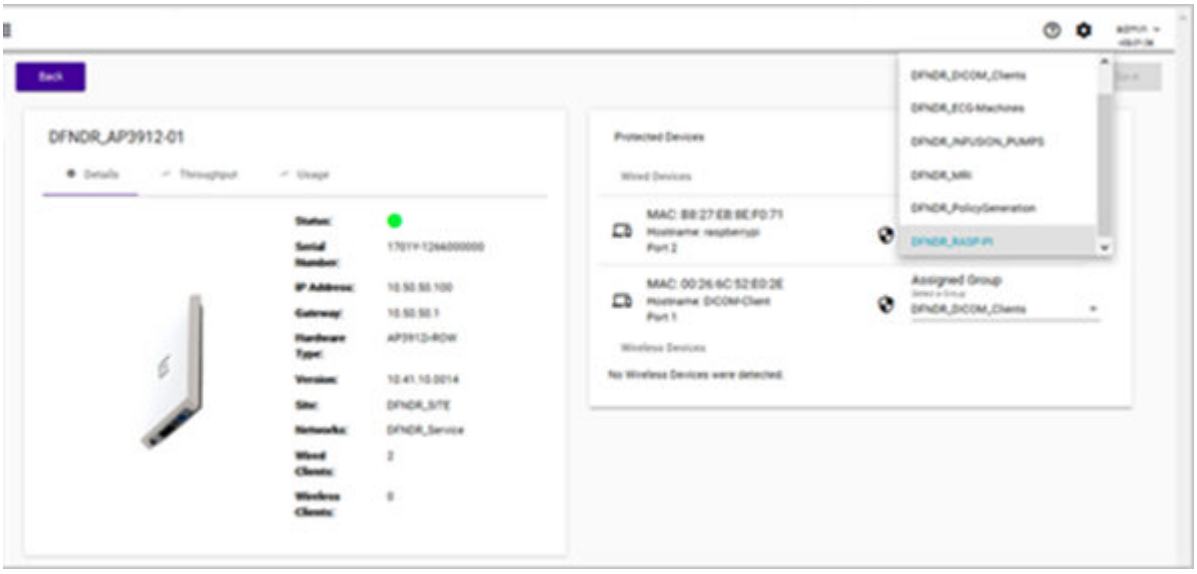


Figure 38: Selecting group from AP3912 Details tab

Figure 39: Selecting group from SA201 Details tab

7 Modify Configuration Profile for Defender Device Groups

The Extreme Defender Application setup wizard automatically creates two adoption rules for an SA201 adapter or AP3912i device. As a result, any SA201 adapter or AP3912i that discovers ExtremeCloud Appliance is automatically onboarded to the appropriate device group under the DFNDR_SITE. You have the option to modify the configuration Profile for the device group in ExtremeCloud Appliance. Take the following steps:

1 Go to **Configure** > **Sites**.
2 Select the DFNDR_SITE and select the **Device Groups** tab.
3 Select the device group.
4 Next to the Profile field, click to edit the profile.
5 Select the **Roles** tab. From the list, select the applicable roles for the SA201 devices in this group.

6 Click **Save**.

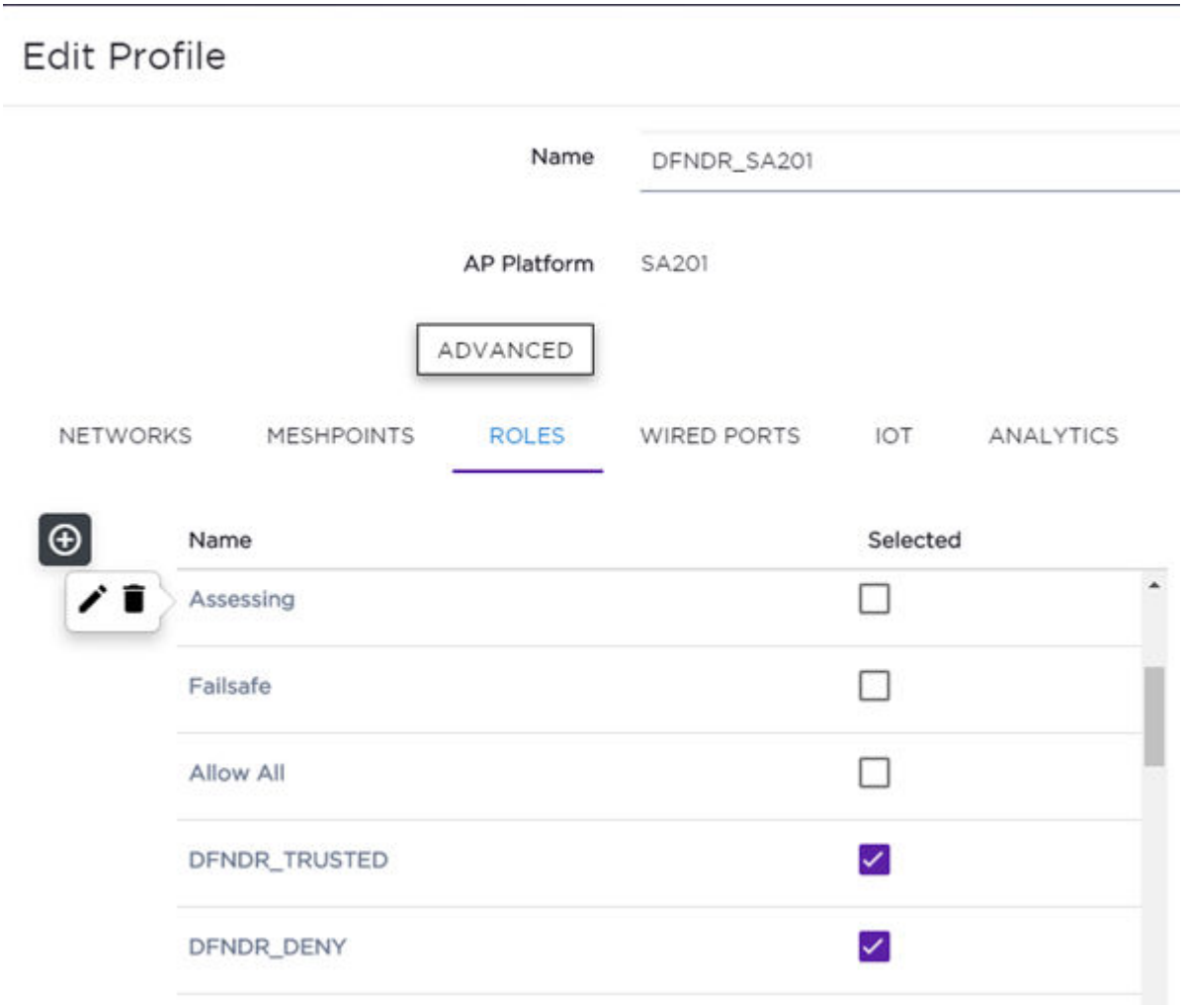
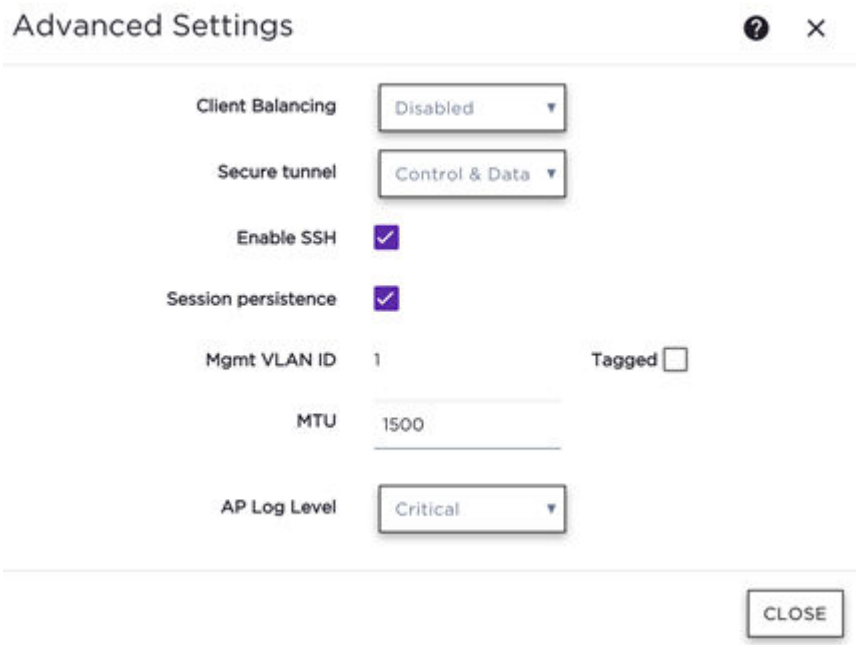


Figure 40: SA201 Device Group Roles tab

7 If required, select the **Wired Ports** tab to set the port speed and duplex of the IoT device side port of an SA201 adapter or AP3912i.

8 From the Edit Profile dialog, click **Advanced** to view additional settings. You can enable **Session persistence** from the Advanced Settings dialog. Session persistence prevents the Defender adapter from rebooting when communication with ExtremeCloud Appliance is lost.

Figure 41: Edit Profile Advanced Settings



You have the option to create additional sites and device groups. For more information, see Sites in Extreme Defender Application on page 19.

For more information about configuration Profiles and device groups, see the ExtremeCloud Appliance Online Help or the *ExtremeCloud Appliance User Guide* at https://extremenetworks.com/documentation/extremecloud-appliance.

Index