Extreme™
Customer-Driven Networking

ExtremeCloud Appliance Deployment Guide

Version 4.26.04

9035971-03

Published February 2019

Legal Notice

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

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

Trademarks

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

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

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

Open Source Declarations

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

Table of Contents

Preface

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

Conventions

This section discusses the conventions used in this guide.

Text Conventions

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

Table 1: Notice Icons

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

Table 2: Text Conventions

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

Documentation and Training

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

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

Training

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

Providing Feedback to Us

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

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

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

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

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

Getting Help

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

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

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

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

Subscribing to Service Notifications

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

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

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

4 Click **Submit**.

AP Regulatory Information

For regulatory information for the ExtremeCloud Appliance supported access point models and appliances, refer to the appropriate *Installation Guide*.

1 About ExtremeCloud Appliance Deployment

Deploying ExtremeCloud Appliance

The Deployment Guide will guide you through the process of deploying your access points using ExtremeCloud Appliance. The instructions will provide a flow of tasks from creating a site, through captive portal and network configuration, to developing adoption rules that will automatically organize your APs into proper device groups upon registration with ExtremeCloud Appliance.

The purpose of the Deployment Guide is to get you up and running quickly, taking you through the full deployment process. If there are concepts or parameter options you do not understand, consult the User Guide or ExtremeCloud Appliance Online Help system for detailed information.

Supported Appliance Specifications

ExtremeCloud Appliance supports the VE6120 virtual appliance and the following hardware appliances:

- E1120
- E2120

Requirements for each ExtremeCloud Appliance model are listed below.

Extreme Application	VE6120 (VMware)		
Network Architecture	**Small**	**Medium**	**Large**
Total APs Managed Per Appliance	100	500	1,000
Total APs Managed in Standard Mode	50	250	500
Additional APs Supported in High-Availability Mode	50	250	500
Total Switches Managed Per Appliance (Standalone/HA)	50/100	100/200	200/400
Total Simultaneous Users Per Appliance	2,000	8,000	16,000
Total Simultaneous Users in Standard Mode	1,000	4,000	8,000
Additional Simultaneous Users in High-Availability Mode	1,000	4,000	8,000
Harware Requirements			
CPU[1]	4	6	8
RAM (GB)	8	16	24
Hard Disk (GB)	80	80	80
Maximum Throughput (Mixed RFC2544)* Open/Encrypted			
2x1Gbps Host	1,870/1,000	1,870/1,800	1,870/1,800
2x10 Gbps Host	5,000/1,870	10,800/5,000	10,800/5,000

Figure 1: Virtual ExtremeCloud Appliance (VE6120)

- Consult VMWare ESXi for minimum host performance requirements for virtual environment. Performance depends on network interface characteristics of underlying host and on utilization on shared interfaces by other virtual appliances.
- Follow VMWare minimum installation requirements. 10 Gbps host recommended for best results. Supports VMware ESXi 6.0 or higher.

Supported Features	E1120	E2120
Total APs Managed Per Appliance	250	4,000
Total APs Managed in Standard Mode	125	2,000
Additional APs Supported in High-Availability Mode	125	2,000
Total Switches Managed Per Appliance (Standalone/HA)	50/100	400/800
Total Simultaneous Users Per Appliance	4,000	32,000
Total Simultaneous Users in Standard Mode	2,000	16,000
Additional Simultaneous Users in High-Availability Mode	2,000	16,000
Dual, Hot Swappable Power Supplies	N/A	Sold Seperately
Maximum Throughput (Mbps):Mixed (RFC2544)/Encrypted	3730/2140	18500/18000
Link Aggregation (Static LAGs)		
2x1Gbps Host	1,870/1,800	1,870/1,800

Figure 2: ExtremeCloud Appliance Hardware

Discovery and Registration

Wireless devices (APs and SA201 adapters) discover the IP address of a controller using a sequence of mechanisms that allow for the possible services available on the enterprise network. The discovery process is successful when the AP/adapter successfully locates a controller to which it can register. Ensure that the appropriate services on your enterprise network are prepared to support the discovery process.

AP39xx and SA201 Discovery Process

Note

ExtremeCloud Appliance supports Extreme Defender Adapter SA201 for the Defender for IoT solution. For more information on Extreme Defender for IoT, refer to documentation located in the Extreme Networks documentation portal: https://extremenetworks.com/documentation/defender-application.

When a wireless device is powered on, it automatically begins a discovery process to determine its own IP address and the IP address of the ExtremeCloud Appliance. When the discovery process is successful, the AP/adapter registers with the ExtremeCloud Appliance.

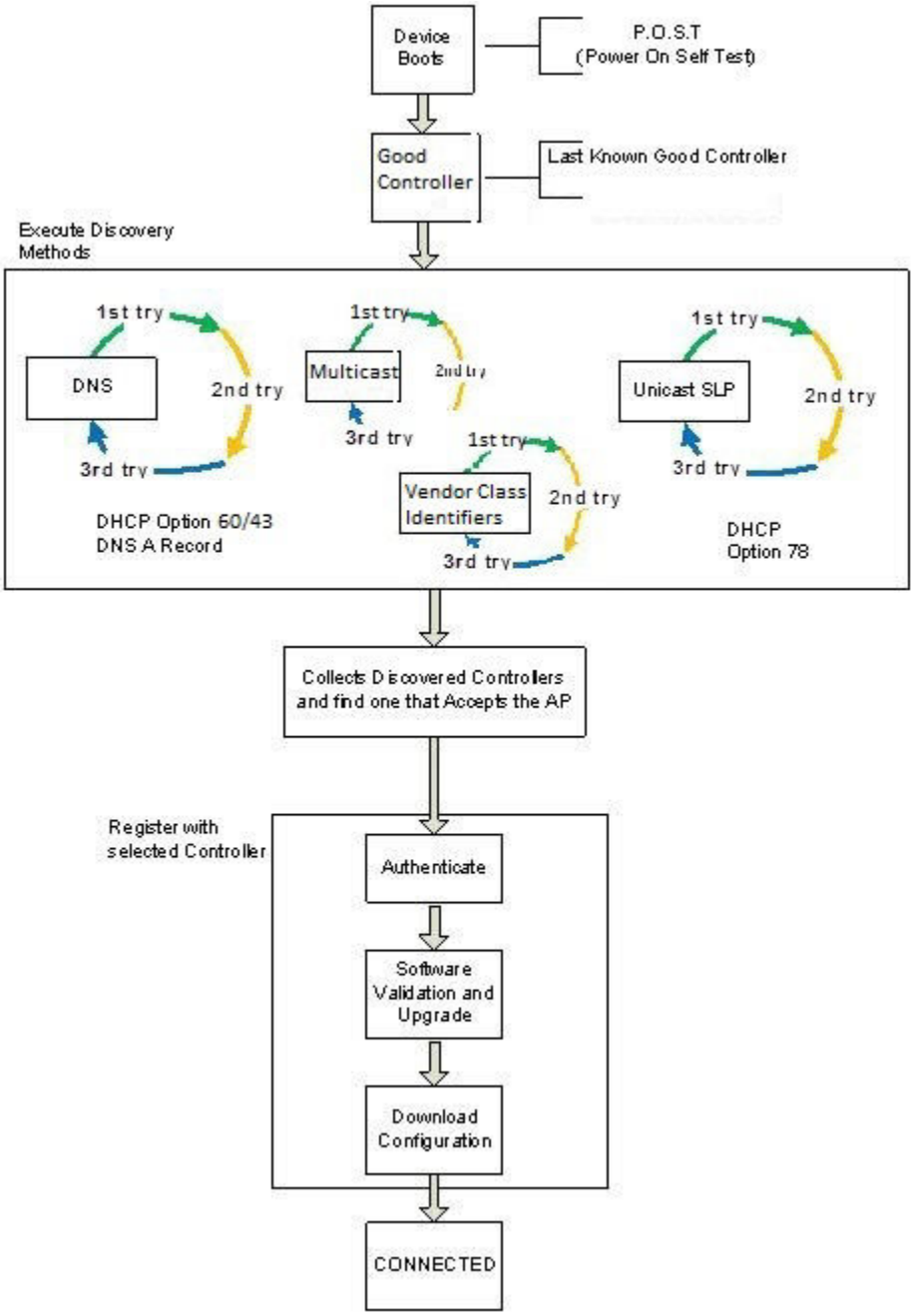


Figure 3: AP39xx and SA201 Discovery Process

Discovering AP39xx Access Points and SA201 Adapters

Take the following steps to find a known controller:

1 Use the IP address of the controller to which the AP last connected successfully.

Once an AP has successfully registered with a controller, it recalls that controller's IP address, and uses that address on subsequent reboots. The AP bypasses discovery and goes straight to registration.

If a known controller cannot be located, take the following steps:

2 Use DHCP Option 60 to query the DHCP server for available controllers. The DHCP server responds to the AP with Option 43, which lists the available controllers.

   For the DHCP server to respond to an Option 60 request from an AP, configure the DHCP server with the vendor class identifier (VCI) for each AP. Also, configure the DHCP server with the IP addresses of the controllers.

3 Use a Domain Name Server (DNS) lookup for the host name Controller.domain-name.

   The AP tries the DNS server if it is configured in parallel with SLP unicast and SLP multicast.

   If you use this method for discovery, place an A record in the DNS server for Controller.*<domain-name>*. The *<domain-name>* is optional, but if used, ensure it is listed with the DHCP server.

4 Use a multicast SLP request to find SLP SAs.

   The AP sends a multicast SLP request, looking for any SLP Service Agents providing the Extreme Networks service.

   The AP tries SLP multicast in parallel with other discovery methods.

5 Use DHCP Option 78 to locate a Service Location Protocol (SLP) Directory Agent (DA), followed by a unicast SLP request to the Directory Agent.

   To use the DHCP and unicast SLP discovery method, ensure that the DHCP server on your network supports Option 78 (DHCP for SLP RFC2610). The APs use this method to discover the controller.

   This solution takes advantage of two services that are present on most networks:

   - **DHCP** — The standard is a means of providing IP addresses dynamically to devices on a network.
   - **SLP** — A means of allowing client applications to discover network services without knowing their location beforehand. Devices advertise their services using a Service Agent (SA). In larger installations, a Directory Agent (DA) collects information from SAs and creates a central repository (SLP RFC2608).

     The controller contains an SLP SA that, when started, queries the DHCP server for Option 78 and if found, registers itself with the DA as service type Extreme Networks. The controller contains a DA (SLPD).

     The AP queries DHCP servers for Option 78 to locate any DAs. The SLP User Agent for the AP then queries the DAs for a list of Extreme Networks SAs.

     Option 78 must be set for the subnets connected to the ports of the controller and the subnets connected to the APs. These subnets must contain an identical list of DA IP addresses.

WiNG AP Discovery Process

When a wireless access point is powered on, it automatically begins a discovery process to determine its own IP address and the IP address of the ExtremeCloud Appliance. When the discovery process is successful, the AP registers with the ExtremeCloud Appliance.

Note

When your environment employs a WiNG appliance or a Cloud appliance entitlement, WiNG APs will discover the WiNG appliance and the Cloud appliance before discovering the ExtremeCloud Appliance. WiNG APs discover WiNG appliances by default.

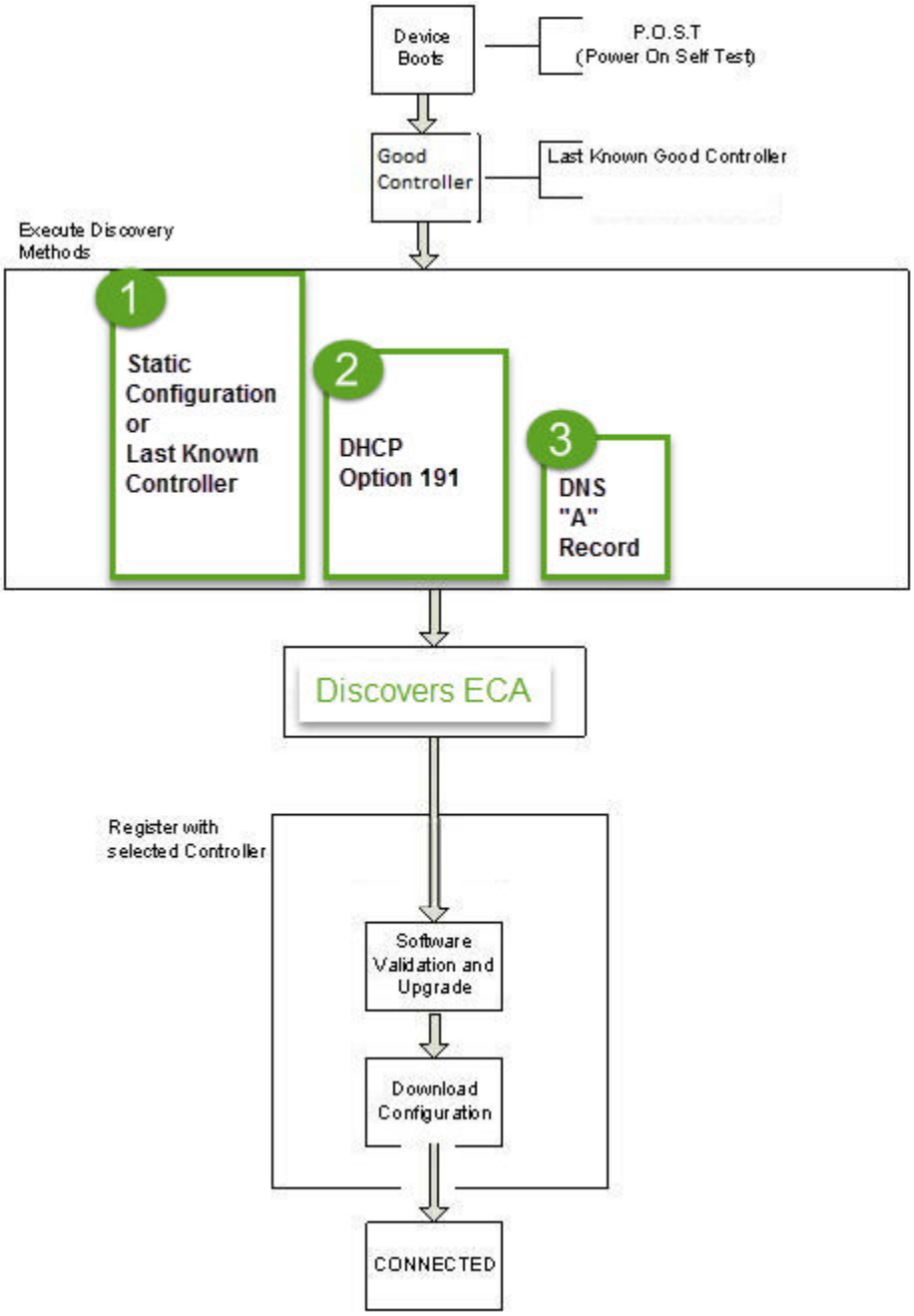


Figure 4: WiNG AP Discovery Process

Discovering WiNG Access Points

1 Use the IP address of the controller to which the AP last connected successfully.
Once an AP has successfully registered with a controller, it recalls that controller's IP address and uses that address on subsequent reboots. The AP bypasses discovery and goes straight to registration.

If a known controller is not available, continue to Step 2.

2 Use DHCP option 191 to locate ExtremeCloud Appliance IP address or FQDN. Option 191 should contain

```
adoption-mode = ws-controller; pool1 = <IP1 | FQDN>
```

Or,

3 Use a Domain Name Server (DNS) lookup for the host name Controller.domain-name.

If you use this method for discovery, place an `"A" record` in the DNS server for Controller.<domain-name>. The <domain-name> is optional, but if used, ensure it is listed with the DHCP server.

Switch Discovery Process

ExtremeCloud Appliance provides support for Management and Statistical services for ExtremeXOS and 200 Series switches. These switches are provisioned with built-in Zero Touch Provisioning (ZTP). ZTP provisioned switches can discover and connect to any of the following Extreme Networks Management Appliances:

- On-premises ExtremeCloud Appliance
- On-premises Extreme Management Center
- ExtremeCloud

Note
Only one appliance at a time can be configured as the Management Appliance.

When the switch is turned on, it automatically starts the Linux process `cloud-connector client`. The cloud-connector client relies on the Default VLAN 1 enabled DHCP client to discover a DHCP server. The default configuration for these switches includes all data ports configured with VLAN 1. Any pre-configured data port can be used to connect to a DHCP Server. Simply provide an IP address and the Domain Name.

After the switch receives an IP address and a Domain Name, it begins the DNS query to find the built-in Extreme Networks Management Appliance Fully-Qualified Domain Name (FQDN):

- `extremecontrol@<domain-name>` for on-premises appliances (ExtremeCloud Appliance or Extreme Management Center).
- `devices.extremenetworks.com` resolved by the Internet Domain Name Servers to the ExtremeCloud IP address.

The cloud-connector tries to resolve these names in an endless round-robin loop. When any of the names are resolved to an IP address, the switch attempts connection to that IP address.

Note

Before connecting a switch to an on-premises Management Appliance:

- Within ExtremeCloud Appliance, configure each physical port to enable device registration:

  1 Go to **Admin** > **System**.
  2 Under **Interfaces** click **Add**.
  3 On the Create New Interface dialog, check **Enable Device Registration**.
- Configure a local DNS server that resolves `extremecontrol@<domain-name>` to the IP address of a ExtremeCloud Appliance physical port that is configured with the **Enable Device Registration** enabled.

Note

Switches that are connected to the internet and can reach the Internet Domain Name servers will attempt to connect to ExtremeCloud.

Related Links

Discovering Switches on page 16
Switch Discovery in an Availability Pair on page 17

Discovering Switches

A switch discovers ExtremeCloud Appliance by resolving the built-in Fully-Qualified Domain Name (FQDN) `extremecontrol@<domain-name>` to an IP address. `<domain-name>` is the domain assigned to the switch by the DHCP server.

To configure switch discovery, add a single `"A" record` for `extremecontrol@<domain-name>` to the local DNS server. If using a public DNS service, add the record to the DNS service. When using the public option, the DNS servers used by the switch must be integrated with the public service.

When the switch discovers ExtremeCloud Appliance, the device status is initially *In-Service-Trouble*. This corresponds to the cloud-connector machine state *Connecting* and is represented in ExtremeCloud Appliance as a yellow triangle.

Once ExtremeCloud Appliance acknowledges the switch configuration, the switch enters the machine state *Running*. This state is represented in ExtremeCloud Appliance with a green circle.

Figure 5: ExtremeCloud Appliance: Switch States During Discovery

Related Links

Switch Discovery in an Availability Pair on page 17
Switch Discovery Process on page 15

Switch Discovery in an Availability Pair

When configuring ExtremeXOS switches in an ExtremeCloud Appliance (ExtremeCloud Appliance) Availability Pair, use an `"A" record` for `extremecontrol@<domain-name>`, providing an IP address for the primary ExtremeCloud Appliance and an IP address for the backup ExtremeCloud Appliance. When the first address fails, the switch attempts the second IP address. If both IP addresses fail, the switch performs a second DNS request. The switch performs the DNS request before sending an HTTPS message and does not use DNS caching.

- If both the primary and backup ExtremeCloud Appliance are up, all configured switches are adopted on the primary ExtremeCloud Appliance, and the switch sends the HTTPS message to the primary ExtremeCloud Appliance only.
- If the primary ExtremeCloud Appliance is down and the backup ExtremeCloud Appliance is up, the switch fails over to the backup. The switch will timeout on the primary IP address and proceed to the secondary IP address. The switch attempts to send the HTTPS message to the primary ExtremeCloud Appliance first because its IP address is first in the DNS reply. That attempt will timeout and the switch will send the second HTTPS to the secondary IP address. The switch continues to send HTTPS messages to both IP addresses. If the primary ExtremeCloud Appliance comes up, the switch sends the HTTP message to the first IP address and does not attempt the second IP address.

Related Links

Switch Discovery Process on page 15
Discovering Switches on page 16

Sites

Use sites to define boundaries for fast roaming and session mobility without interruption. A site represents a physical, geographic area in your network. As the top-level element in the ExtremeCloud Appliance data model, the site runs Sessions Manager and RF Manager functions for all RF Domains in the site.

ExtremeCloud Appliance supports two types of sites: Centralized and Distributed. Each site type supports a unique set of access points. Know the model of your access points before configuring a site. Centralized sites support the following AP39xx models:

- AP3917i/e/k
- AP3916ic
- AP3915i/e
- AP3912i
- AP3935i/e
- AP3965i/e

A Defender site is a Centralized site that supports SA201. It begins with the DFNDR_ prefix.

Distributed sites support the following ExtremeWireless WiNG models:

- AP7522
- AP7532
- AP7562

- AP7612
- AP7632
- AP7662
- AP8432
- AP8533

The licensing domain is defined at the site level. When configuring a site, select the Country value that matches the licensing domain of the APs that comprise the site.

Note
If the licensing domain of your AP does not match the Country assigned to the site, the AP will not display within a device group for possible selection.

Device Groups

The most simple site configuration allows for one device group for each AP/adapter model, selecting the default configuration profile and the default RF Management profile for that model.

A more complex deployment allows for more than one device group per AP model. This makes use of different profile features and/or a unique RF Management profile for each device group. With this more complex deployment, create a device group for any combination of configuration features and RF configurations.

All devices in a device group must share the following:

- AP/adapter model number
- Configuration Profile
- RF Management Profile

You have the option to discover AP/adapters before creating a device group. However, if you create the device group first, discovered devices that match the configuration profile are listed within the Create Device Group dialog, allowing you to simply add each AP/adapter to the device group. Furthermore, if you create a device group and an adoption rule, your newly discovered AP/adapters will be automatically added to the correct device group without your intervention.

2 Configuring DHCP, NPS, and DNS Services

This chapter describes how to configure and DNS (Domain Name System) services on a Windows Server 2012 R2 or Linux server for use by ExtremeWireless Appliance and APs. In addition, the chapter explains how to configure Network Policy Server (NPS) service on Windows Server 2012 R2. Use the configuration processes in this chapter as a reference when configuring services.

Note
Windows Server 2012 R2 or Linux server may have a different configuration process than what is described here. Refer to your manufacturer's documentation for the configuration process that is specific to your server.

This section includes the following procedures:

- DHCP Service Configuration on page 19
- NPS Service Configuration on page 37
- DNS Service Configuration on page 43

DHCP Service Configuration

Before you can configure the service, you must install it on the server. You can configure DHCP on Windows Server 2012 R2 or on a Red Hat Linux server.

This section includes the following procedures:

- Configuring DHCP on Windows Server 2012 R2 on page 19
- Configuring DHCP on a Red Hat Linux Server on page 33

Configuring DHCP on Windows Server 2012 R2

Install either during the initial installation of Windows Server 2012 R2 or after the initial installation is completed.

When you configure DHCP for ExtremeCloud Appliance LAN () solution, you can include 078 SLP DA Option.

You must enable 078 SLP DA Option for every scope you define. A scope is a collection of IP addresses meant to be distributed by the DHCP server to the client devices on a subnet. The SLP DA is used by:

- The Wireless APs to discover the ExtremeCloud Appliance
- The mobility agents to discover the mobility manager.

Note
You may visit http://support.microsoft.com for instructions on how to install DHCP.

Configure DHCP option 43 for ExtremeCloud Appliance discovery when there is a need for a specific AP platform to connect to a specific controller.

For more information, see:

- Creating Option 78 on page 20
- Configuring Option 78 on page 20
- DHCP Option 43 on Windows Server 2012 R2 on page 25

Creating Option 78

To create option 78 as a byte array, perform the following steps:

1. Click **Start** > **Administrative Tool** > **DHCP**
2. Right-click the server node, and select **Set predefined options**.
3. Select **Add**, and type a name for the option, for example "SLP DA".
4. Set the data type to **Byte**, and select the **Array** checkbox.
5. In the Code field, type `78`.
6. Type a description for the option, for example, "Extreme Networks SLP Discovery", and then select **OK**.

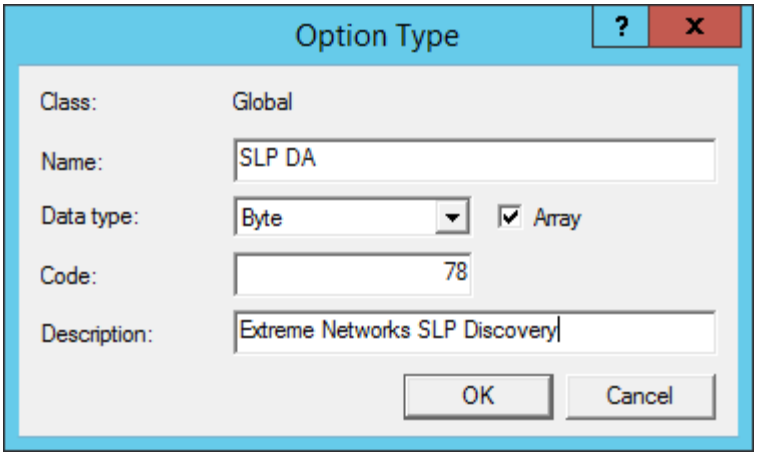


Figure 6: Option Type

Configuring Option 78

To configure on Windows Server 2012 R2:

1. Click **Start** > **Administrative Tool** > **DHCP**.
2. In the console tree, right-click the DHCP server, IPv4 on which you want to create the new DHCP scope, and then click **New Scope**.
3. Click **Next**.

4 In the Name and Description text boxes, type the scope name and description.

This can be any name that you want, but it should be descriptive enough so that you can identify the purpose of the scope on your network.

5 Click **Next**.

The IP Address Range window is displayed.

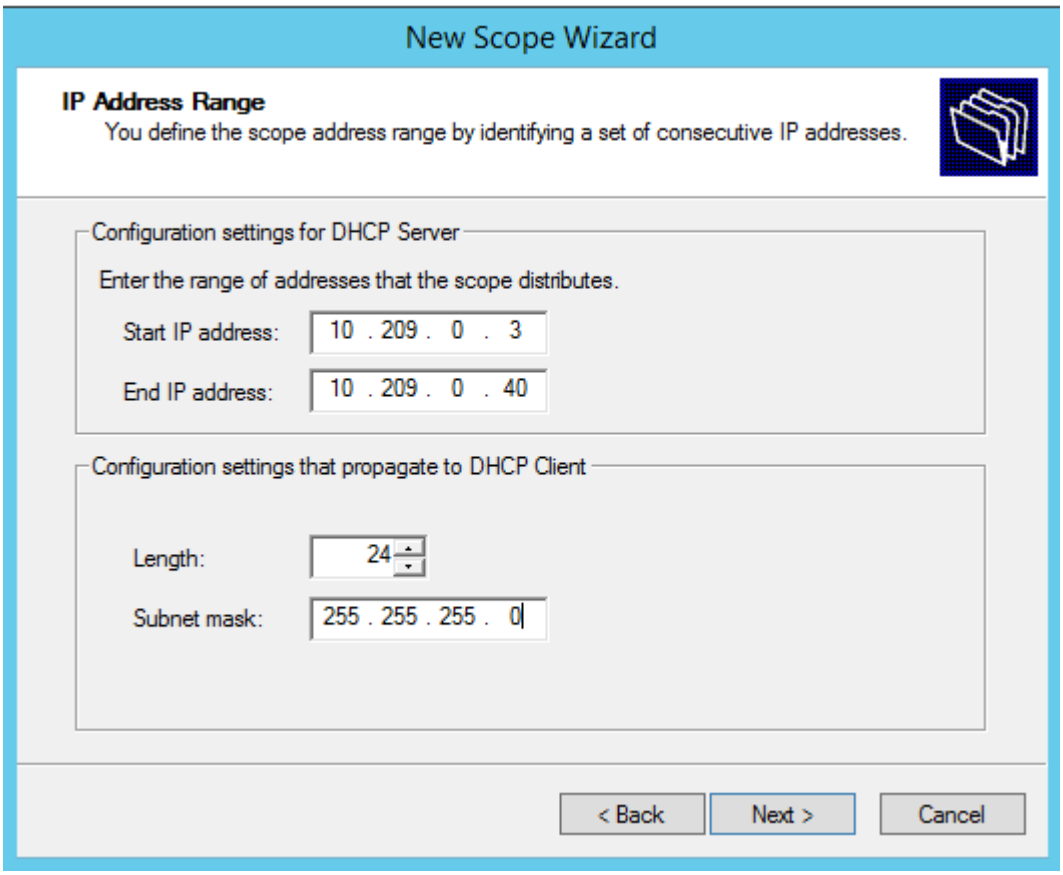


Figure 7: IP Address Range

6 In the Start IP address and the End IP address text boxes, type the start and end of the IP address range that you want to be distributed to the network.

You must use the range provided by your network administrator.

7 In the Length text box, type the numeric value of the subnet mask bits, or in the Subnet mask text box, type the subnet mask IP address.

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address. You must use the Length (or the Subnet mask) provided by your network administrator.

8 Click **Next**.

The Add Exclusions window displays.

9 In the Start IP address and the End IP address text boxes, type the start and end of the IP address range that you want to exclude from the distribution.

You must use the exclusion range provided by your network administrator.

10 Click **Next**.

The Lease Duration window displays.

The DHCP server assigns a client an IP address for a given amount of time. The amount of time for which the IP address can be leased is defined in the Lease Duration window.

11 In the Days, Hours and Minutes text box, type the lease duration.

You must use the Lease Duration as specified by your network administrator.

12 Click **Next**.

The Configure DHCP Options window displays.

13 Select **Yes, I want to configure these options now**, and then click **Next**.

The Router (Default Gateway) window displays.

14 In the IP address text box, type the network's default gateway and click **Add**.

You must use the default gateway provided by your network administrator.

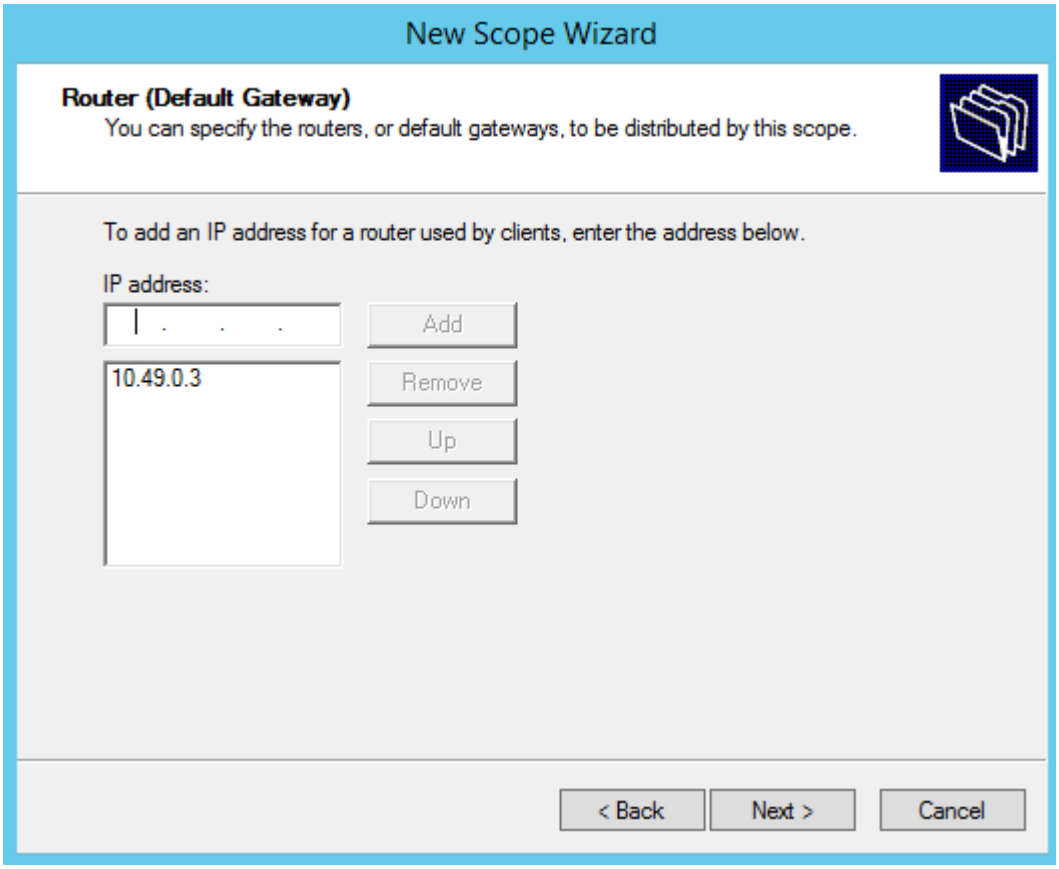


Figure 8: Router Default Gateway

15 Click **Next**.

The Domain Name and DNS Servers window displays.

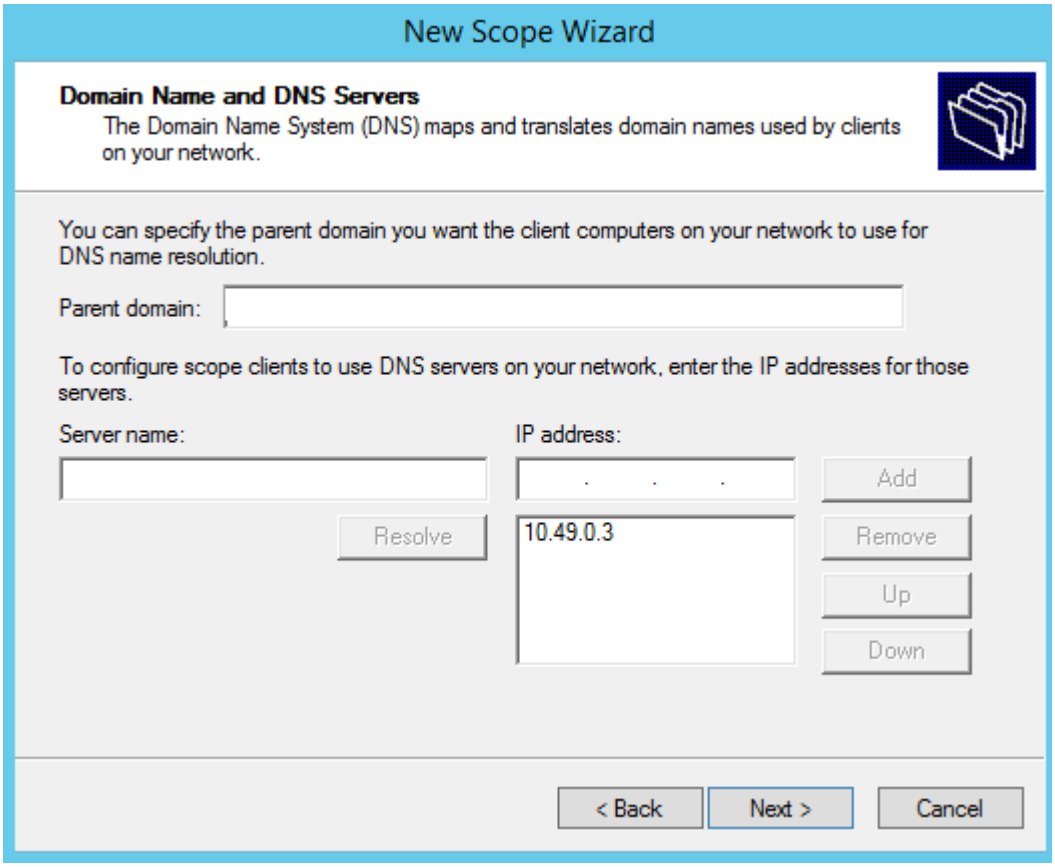


Figure 9: Domain Name and DNS Servers

16 In the Parent domain text box, type your company's domain name.

You must use the Parent Domain provided by your network administrator.

17 In the Server name text box, type your server name.

You must use the server name provided by your network administrator.

18 In the IP address text box, type your server's IP address, and then click **Add**.

19 Click **Next**.

The WINS Servers window displays.

20 Click **Next**.

The Activate Scope window displays.

21 Select **Yes, I want to activate this scope now**, and click **Next**.

The wizard displays the following message:

```
You have successfully completed the New Scope wizard.
```

22 Click **Finish**.

23 Click **Start** > **Administrative Tool** > **DHCP**.

The DHCP console tree displays.

24 Right-click **Server Options** in the tree and select **Configure Options**.

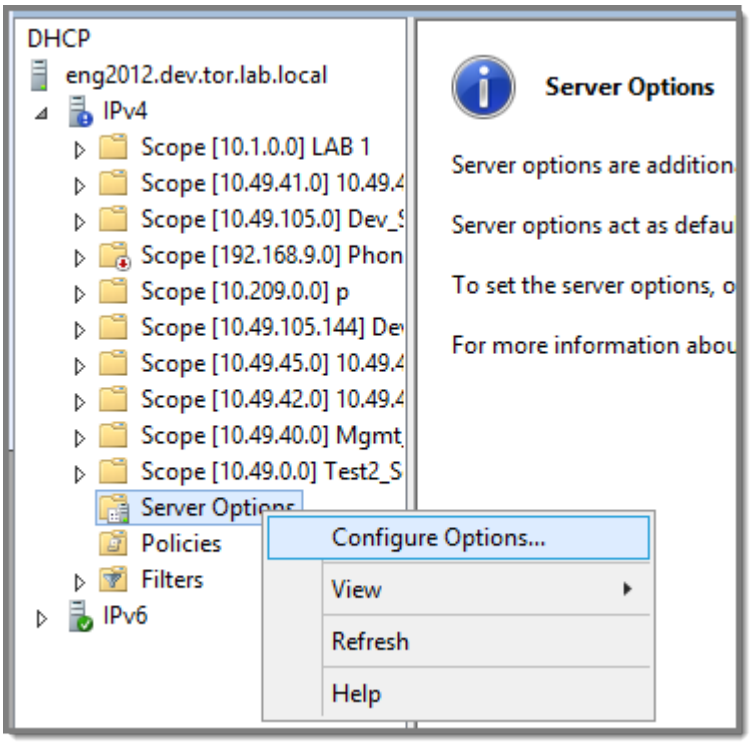


Figure 10: Configure Options

The Server Options dialog displays.

25 On the General tab, enable 078 SLP DA.

26 In the lower pane of the screen, type the dotted decimal values of the SLP DA's IP address.

The Wireless APs use the SLP DA to discover the ExtremeCloud Appliance.

The mobility agents use the SLP DA to discover the mobility manager.

Note

If there is no SLP deployment on the enterprise network, the ExtremeCloud Appliance is configured to act as a DA by default. If you put the appliance's IP address(es) in a DHCP server for Option 78, Wireless APs will interact with the appliance for discovery.

Similarly, the mobility agents also interact with the ExtremeCloud Appliance to discover the mobility manager.

Configuring Option 191 for WiNG APs

When you configure DHCP for ExtremeCloud Appliance LAN solution, include Option 191 for ExtremeWireless WiNG APs. To create option 191, take the following steps:

1 Click **Start** > **Administrative Tool** > **DHCP**

2 Right-click the server node, and select **Set predefined options**.

3 Select **Add**, and type a name for the option, for example `191_Wing_Discovery`.

4 Set the data type to **String Value**.

Note
The Sring Value is `adoption-mode = ws-controller; pool1 = <IP1 | FQDN>`

5 In the Code field, type **191**.

6 Type a description for the option, for example, `Extreme Networks Wing Discovery`, and then select **OK**.

DHCP Option 43 on Windows Server 2012 R2

This section describes how to configure the Microsoft server to use DHCP option 43 for ExtremeCloud Appliance discovery. In the discovery process, the DHCP server returns vendor-specific information to the client as option 43. You must supply the following information to configure DHCP option 43:

- Vendor Class Identifier (VCI) — The VCI for an Extreme Networks AP is HiPath <AP model name>.

  For example, the VCI for the Extreme Networks AP3965e is HiPath AP3965. The following table lists the Vendor Class Identifiers for each Extreme Networks AP model.

Table 3: AP Vendor Class Identifiers

AP Model	Vendor Class Identifier
AP3912i	HiPath AP3912
AP3915i	HiPath AP3915
AP3915e	HiPath AP3915
AP3916ic	HiPath AP3916
AP3917i	HiPath AP3917
AP3917e	HiPath AP3917
AP3935i	HiPath AP3935
AP3935e	HiPath AP3935
AP3965i	HiPathAP3965
AP3965e	HiPath AP3965

- Option 43 sub-option code — The option 43 sub-option code for the Extreme Networks APs is type 1 (0x1).
- IP addresses of ExtremeCloud Appliance

Configuring Option 43

To configure option 43 using the Windows Server 2012 R2 DHCP, IPv4 server utility:

1 In the DHCP server utility, right-click the DHCP server icon and choose **Define Vendor Classes**.

You will create a new vendor class to program the DHCP server to recognize the VCI ExtremeWireless *<AP model name>*.

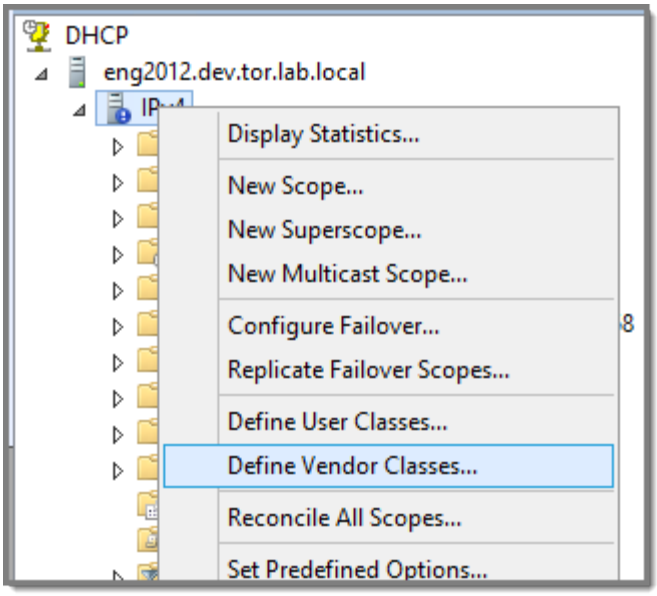


Figure 11: Define Vendor Classes

The DHCP Vendor Classes window displays.

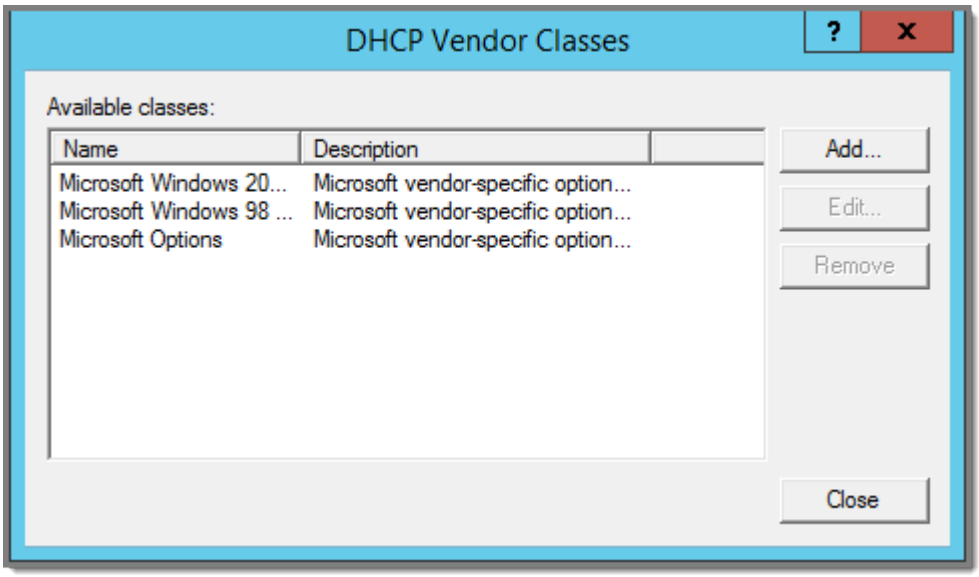


Figure 12: DHCP Vendor Classes

2 Click **Add** to create the new class.

The New Class window displays.

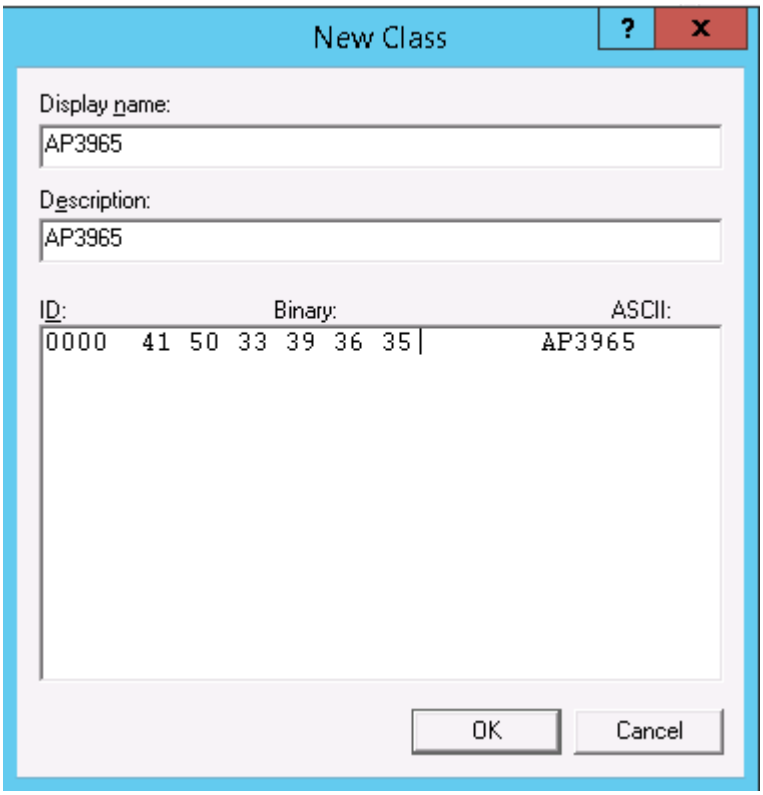


Figure 13: New Class

3 In the Display name field, enter a name. In this example, AP3965 is used as the display name.

4 In the Description field, enter a short description of the vendor class: AP3965.

5 Add the Vendor Class Identifier string. Click the ASCII field, and enter the appropriate value (for example, AP3965).

6 Click **OK**.

The new class is created.

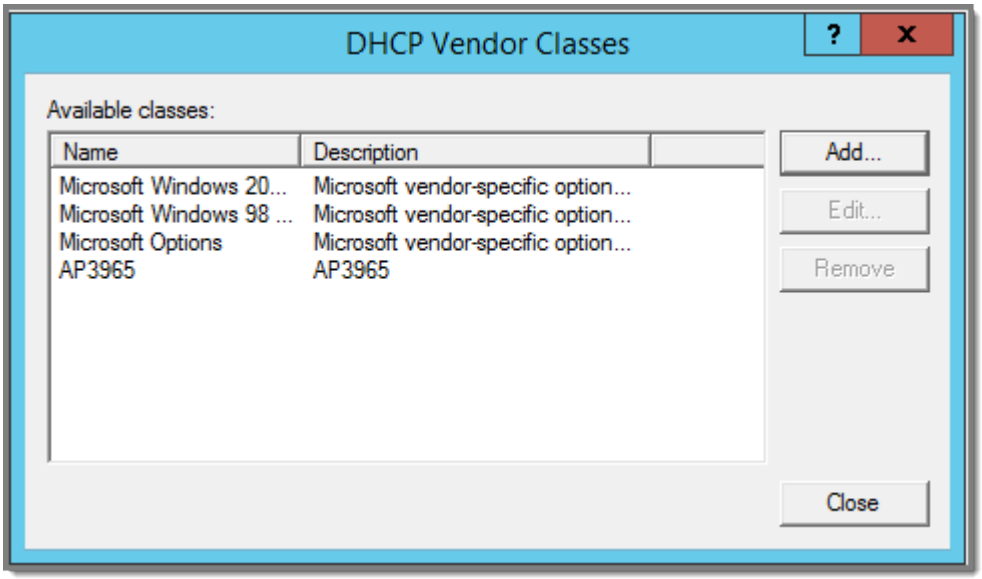


Figure 14: DHCP Vendor Classes

7 Click **Close**.

8 In the DHCP server, IPv4 utility, right-click the server icon and select **Set Predefined Options** to add an entry for the controller sub-option for the newly created vendor class.

The sub-option code type and the data format is used to deliver the vendor specific information to the APs.

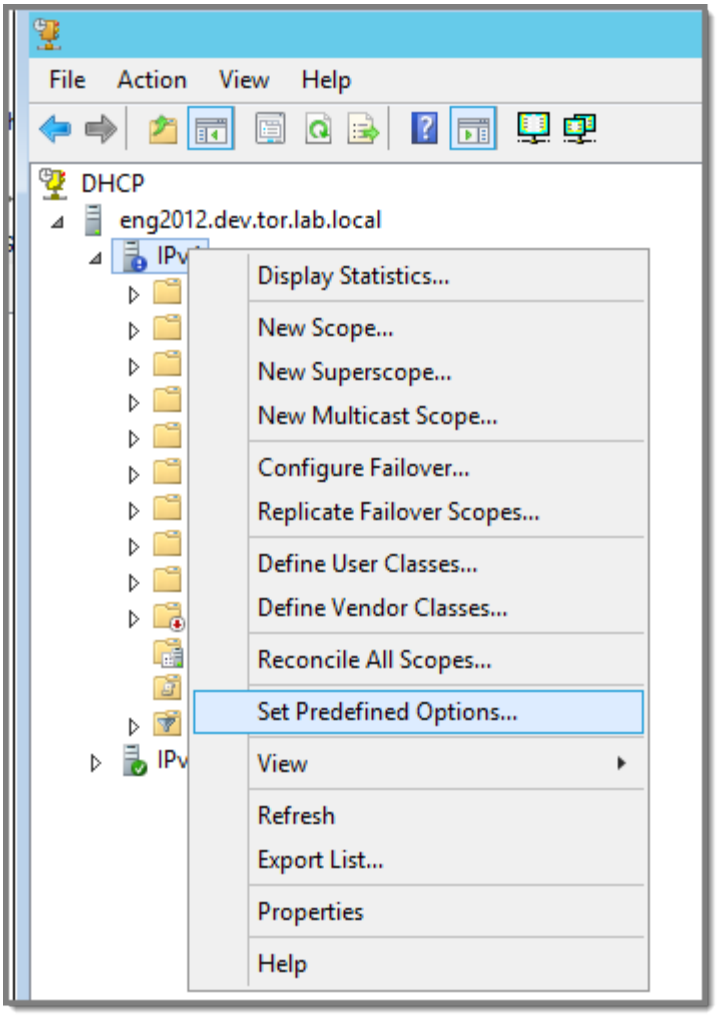


Figure 15: Set Predefined Options

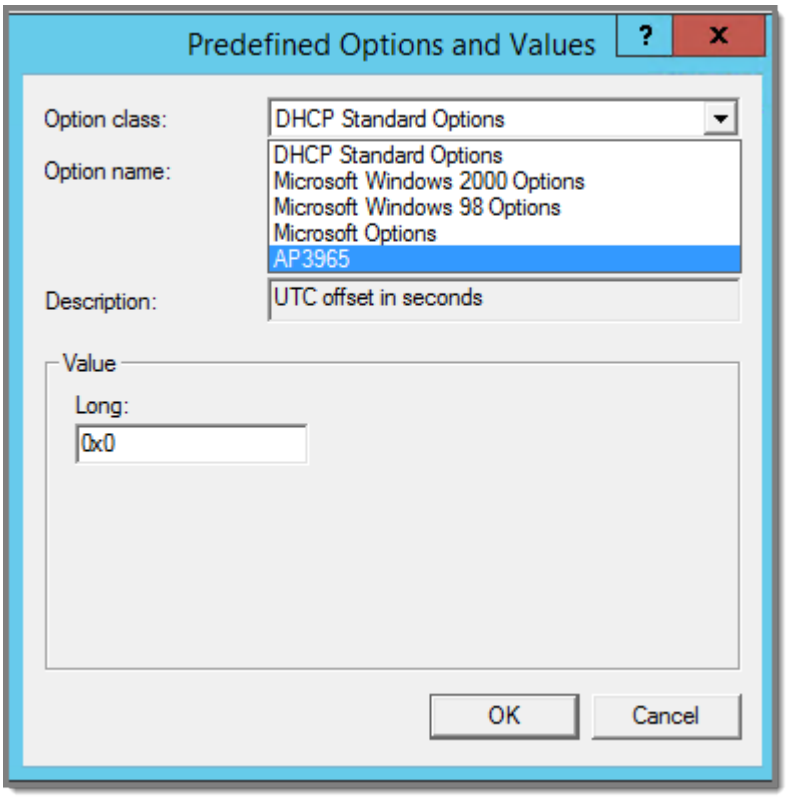


Figure 16: Predefined Options and Values

9 In the Option class field, select the value you configured for the vendor class and click **Add**.

The Option Type window displays.

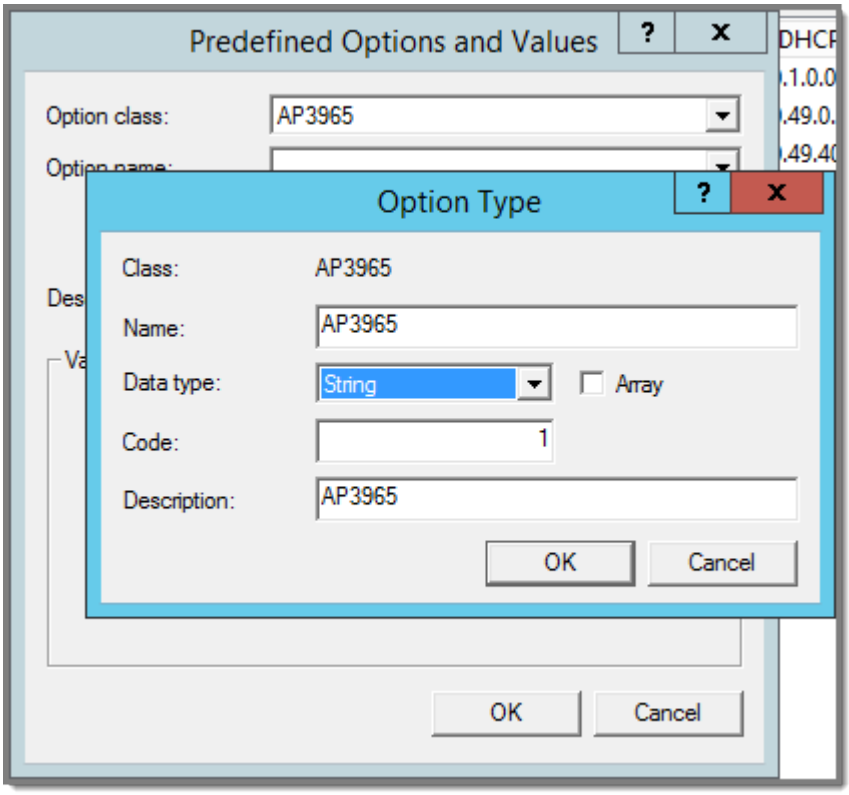


Figure 17: Option Type

10 Enter a value in the Name field.

11 In the Data type field, select **String**.

12 In the Code field, enter the sub-option value `1`.

13 Enter a description in the Description field (Optional).

14 Click **OK**.

The new predefined option is displayed in the Predefined Options and Values window.

15 Click **OK**.

You have created the vendor class and sub-option type needed in order to support controller discovery.

Configuring Server Options

1 In the server utility, right-click the **Server Options** folder under the DHCP scope, and select **Configure Options**.

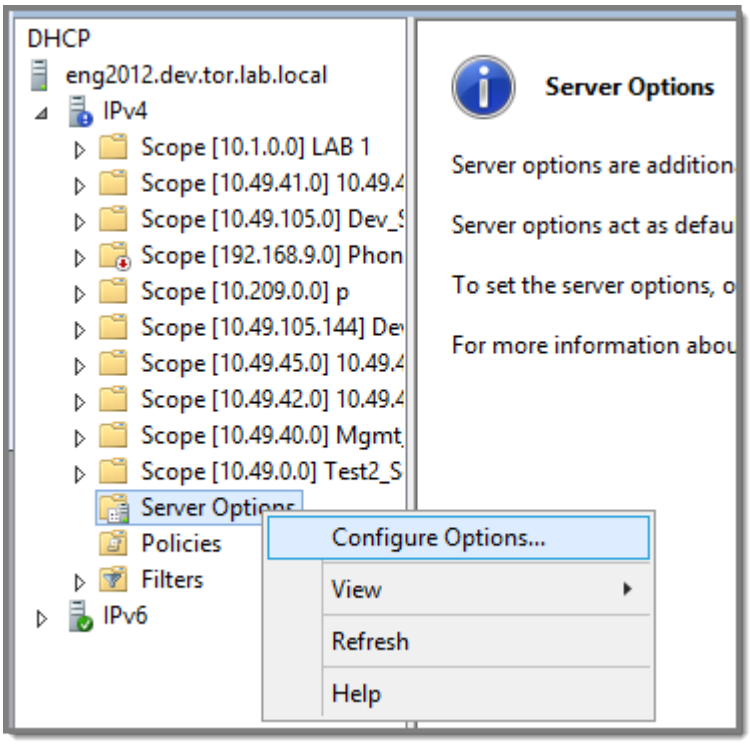


Figure 18: Configure Options

The Server Options window displays.

2 Click the **Advanced** tab and configure the following parameters:

- Vendor Class. Select the vendor class that you plan to use. For example, AP3965.
- Available Options. Select the predefined 001 sub-option to assign to this scope.
- Data Entry. Enter the controller IP addresses to return to the APs. This is a comma-delimited list.

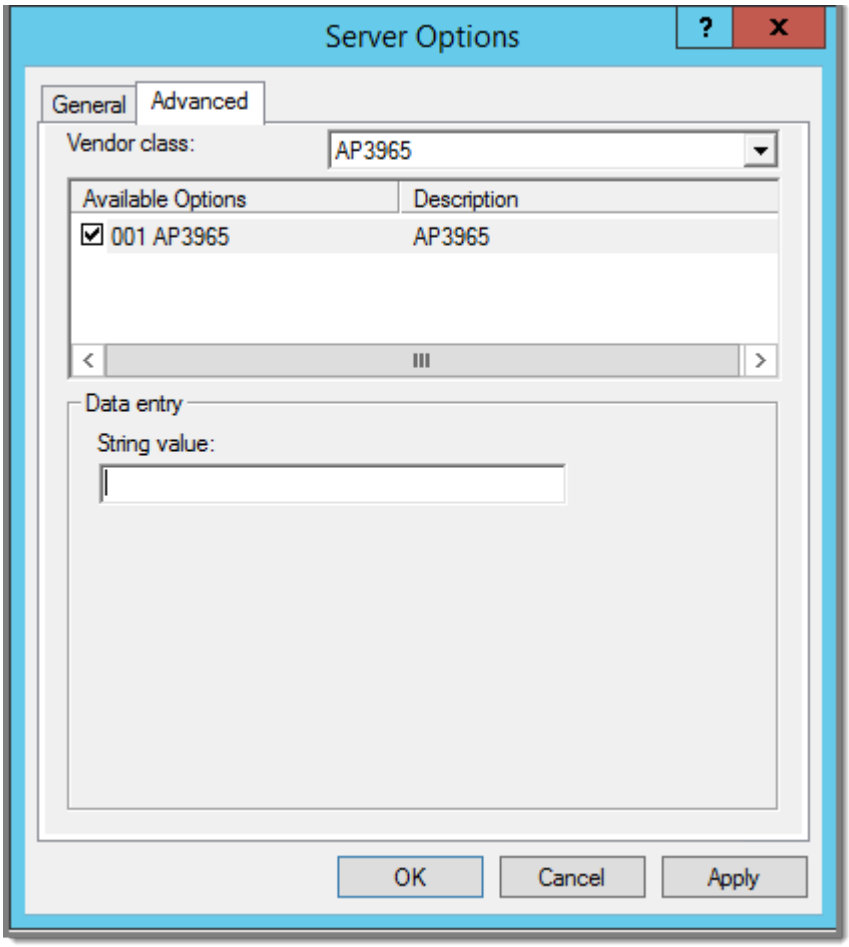


Figure 19: Server Options

3 Click **OK**.

DHCP Option 43 is now configured. This DHCP option is available for all the DHCP scopes that are configured in the DHCP server. When an AP requests vendor specific information, the DHCP server sends the ExtremeCloud Appliance IP addresses in Option 43 to the AP.

Configuring DHCP on a Red Hat Linux Server

You can configure a DHCP server using the configuration file `/etc/dhcpd.conf`.

DHCP also uses the file /var/lib/dhcp/dhcpd.leases to store the client lease database.

The first step in configuring a DHCP server is to create the configuration file that stores the network information for the clients. Global options can be declared for all clients, or options can be declared for each client system.

Option 191 for ExtremeWireless WiNG should be globally defined at the beginning of the DHCP file:

```
option controller-discovery code 191=string;
```

The configuration file can contain any extra tabs or blank lines for easier formatting. The keywords are not case-sensitive and lines beginning with a hash mark (#) are considered comments.

To use the recommended mode, add the following line to the top of the configuration file:

```
ddns-update-style interim;
```

Read the dhcpd.conf man page for details about the different modes.

There are two types of statements in the configuration file:

- Parameters – State how to perform a task, whether to perform a task or what networking configuration options to use to send to the client.
- Declarations – Describe the Topology of the network, describe the clients, provide addresses for the clients, or apply a group of parameters to a group of declarations.

Some parameters must start with the option keyword and are referred to as options. Options configure DHCP options; whereas, parameters configure values that are not optional or control how the DHCP server behaves.

Parameters (including options) declared before a section enclosed in curly brackets {} are considered global parameters. Global parameters apply to all the sections below it.

Note
If you change the configuration file, the changes will not take effect until you restart the DHCP daemon with the command service dhcpd restart.

The following is an example of a DHCP configuration on a Red Hat Linux server.

For Wireless AP Subnet

```
subnet 10.209.0.0 netmask 255.255.255.0 {
option routers 10.209.0.2; ### This is the network's default gateway address.
option subnet-mask 255.255.255.0
option domain-name xyznetworks.ca
option domain-name servers 192.168.1.3, 207.236, 176.11
range 10.209.0.3 10.209.0.40;
default-lease-time 7200000 ###The figures are in seconds.
## SLP option 78 for Extreme Wireless AP39xx

option slp-directory-agent true 10.209.0.1, 10.209.0.3;

### SLP option 191 for ExtremeWireless WiNG AP
option controller-discovery "adoption-mode=ws-controller;pool1=10.48.240.33;
authoritative;
```

Configuring DHCP Option 43 on a Linux Server

This section describes the configurations necessary on the Linux DHCP server to use DHCP option 43 for ExtremeCloud Appliance discovery. Option 43 requires the following information:

- Vendor Class Identifier (VCI) — The VCI for an ExtremeWireless AP is HiPath <AP model name>. Table 3 on page 25 lists the Vendor Class Identifiers for Extreme Networks AP39xx models.

- Option 43 sub-option code — The option 43 sub-option code for the ExtremeWireless APs is type 1 (0x1).
- IP addresses of ExtremeCloud Appliance

To configure the vendor encapsulated option on a Linux server, you must do the following:

- Define an option space.
- Define some options in that option space.
- Provide values for the options.
- Specify that this option space should be used to generate the vendor-encapsulated-options option.
- ExtremeWireless WiNG access points use Vendor Class with Option 191.

To configure DHCP option 43:

1 Modify the dhcp.conf file (modifications are in bold).

```
[root@localhost ~]# vim /etc/dhcpd.conf
authoritative;
ddns-update-style interim;
ignore client-updates;
option space HAP;
option HAP.HWC code 1 = text;

subnet 10.100.1.0 netmask 255.255.255.0 {
range 10.100.1.10 10.100.1.254;
option subnet-mask 255.255.255.0;
option slp-directory-agent false 10.1.100.11;
option domain-name-servers 10.100.1.2;
option domain-name "bpmgmt.com";
option routers 10.100.1.1;
default-lease-time 40000;
}
…
subnet 10.100.4.0 netmask 255.255.255.0 {
range 10.100.4.100 10.100.4.254;
option subnet-mask 255.255.255.0;
option slp-directory-agent false 10.100.4.46, 10.100.4.47;
option domain-name-servers 10.100.1.2;
option domain-name "bpmgmt.com";
option routers 10.100.4.1;
default-lease-time 40000;


Vendor Class for ExtremeWireless APs:

class "HAP" {
match option vendor-class-identifier;
}
subclass "HAP" "AP3935" {
vendor-option-space HAP;
option HAP.HWC "10.100.2.36, 10.100.2.22";


}
Vendor class for ExtremeWireless WiNG APs:


class "WingAP.AP7662"{     ### Vendor class for Wing AP7662
match if substring (option vendor-class-identifier, 0, 17) = "WingAP.AP7662";
option controller-discovery "adoption-mode=ws-controller;pool1=10.48.209.33";
option vendor-class-identifier "WingAP.AP7662";
```

```
}

authoritative;
```

2 Restart the DHCP server.

```
[root@localhost ~]# /etc/init.d/dhcpd restart
```

Configuring the ExtremeCloud Appliance as an NPS Client

1 Click **Start** > **Administrative Tools** > **Network Protocol Server**.

2 Expand **RADIUS Clients and Servers**, right-click **RADIUS Clients**, and then click **New**.

The dialog appears.

3 Configure the following parameters:

- Friendly name. Type the name that you want to assign to the ExtremeCloud Appliance
- Client address (IP or DNS). Type the IP address of the ExtremeCloud Appliance , and then click **Verify**.

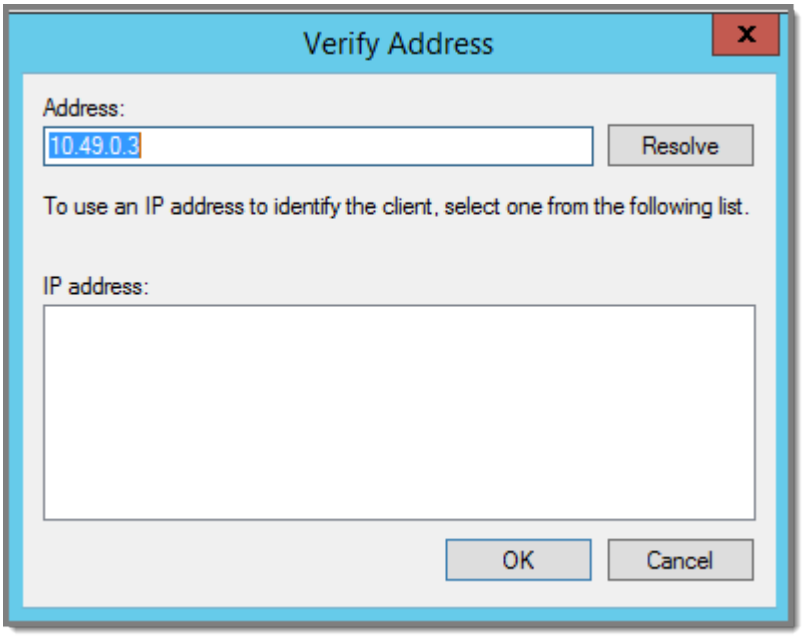


Figure 20: Verify Address

1 Click **Resolve**.

If the IP address is correct, it appears in the Search results text box.

2 Click **OK**.

- Shared Secret. Select a Shared Secret Template (Optional).

You can opt to enter a Shared Secret manually or have NPS generate the Shared Secret.

- Manual. Type a password that both the NPS server and the ExtremeCloud Appliance will use to mutually authenticate. This password is case-sensitive. You can use alpha-numeric characters. You must configure the same shared secret password for the VNS .
- Generate. Click **Generate** to have NPS generate the password. Not all servers support long generated secrets.

4 Click **OK**.

NPS Service Configuration

Microsoft Network Policy Server (NPS) can run as a server. You can use NPS for centralized authentication and accounting of multiple client devices. To install NPS on Windows Server 2012 R2, see http://support.microsoft.com. This section outlines the following configuration procedures:

- Adding a New Network Policy on page 38
- Configuring the ExtremeCloud Appliance as an NPS Client on page 36

Adding a New Network Policy

Create one or more network policies. In this section, we outline how to create two specific policy conditions. Adding policy conditions is optional.

- Create a condition to limit the policy to specific IP addresses.
- Create a condition to limit the policy to a specific group that corresponds to an ExtremeCloud Appliance Role.

To create a new network policy:

1 Click **Start** > **Administrative Tool** > **Network Policy Server**.
2 In the tree view, expand **NPS (Local)**, expand **Policies**, and right-click **Network Policies**.
3 Click **New**
4 Provide a **Policy name**.
   - Type of network access server is **Unspecified**.
   - Do not select **Vendor Specific**
5 Click **Next** to configure a condition if applicable.

Related Links

Create Condition: Client IPv4 Addresses on page 38

Create Condition: Windows Groups on page 39

Create Condition: Client IPv4 Addresses

1 Click **Add** to add a condition.
2 Scroll down to Radius Client Properties and select **Client IPv4 Addresses**.
3 Enter the IP Address of the ExtremeCloud Appliance and click **OK**.

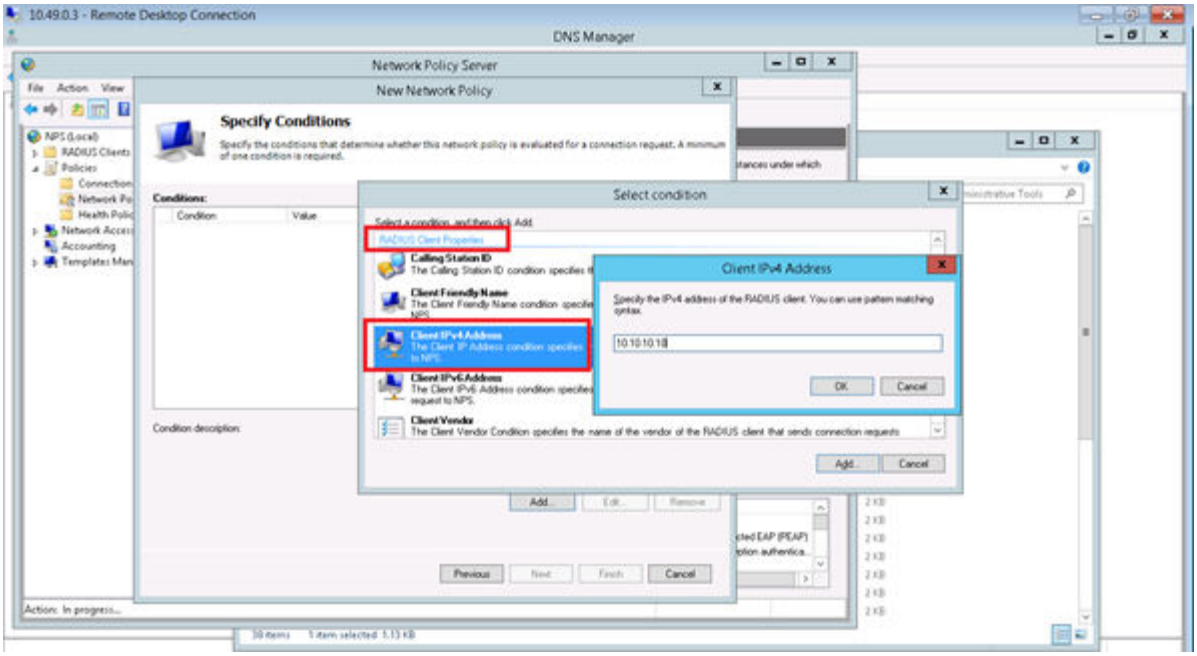


Figure 21: Condition: Client IPv4 Address

4 Click **Next**.

5 On the Specify Access Permission screen, select **Access granted** and click **Next**.

6 On the Configure Authentication Methods screen, click **Add** and select **Microsoft: Smart Card or other certificate**. Then, click **OK**.

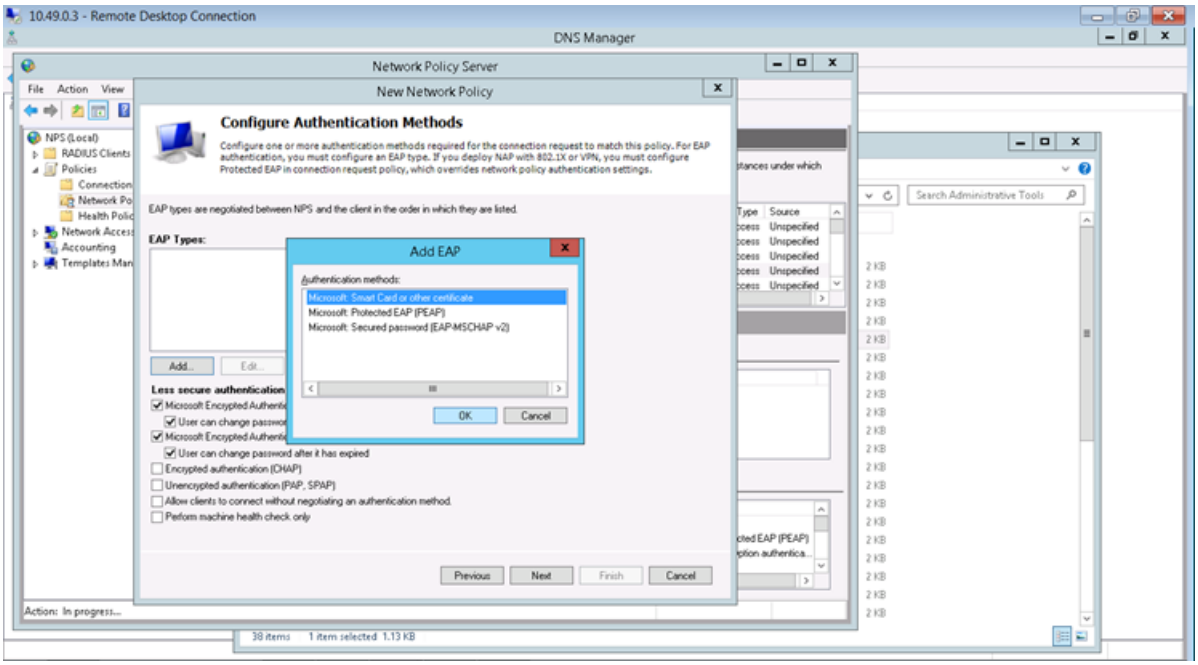


Figure 22: Add EAP

7 Click **Next**.

8 Configure the Idle Timeout and click **Next**.

9 Configure the Radius Attributes and click **Next**.

10 Click **Finish**.

Create Condition: Windows Groups

Create a condition specifying a Windows group to add flexibility to policy management.

1 Click **Add** to add a condition.

2 Select **Windows Groups** and click **Add**.

3 Click **Add Groups**.

The Select Groups dialog appears.

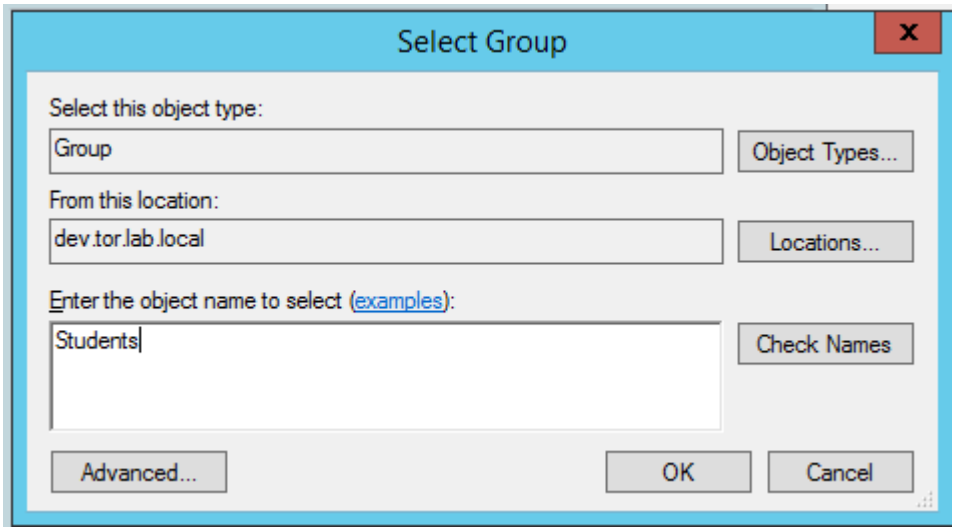


Figure 23: Select Group

4 Type `Group` as the object type.

5 Specify the location.

6 Enter the name of the group. This name must match a configured Active Directory group. You may be prompted to specify the Active Directory Windows group that the group corresponds to.

7 Click **OK**.

8 On the Specify Access Permission screen, specify the level of access permission and click **Next**.

9 On the Configure Authentication Methods screen, click **Add** and select one or more EAP methods. Then, click **OK**.

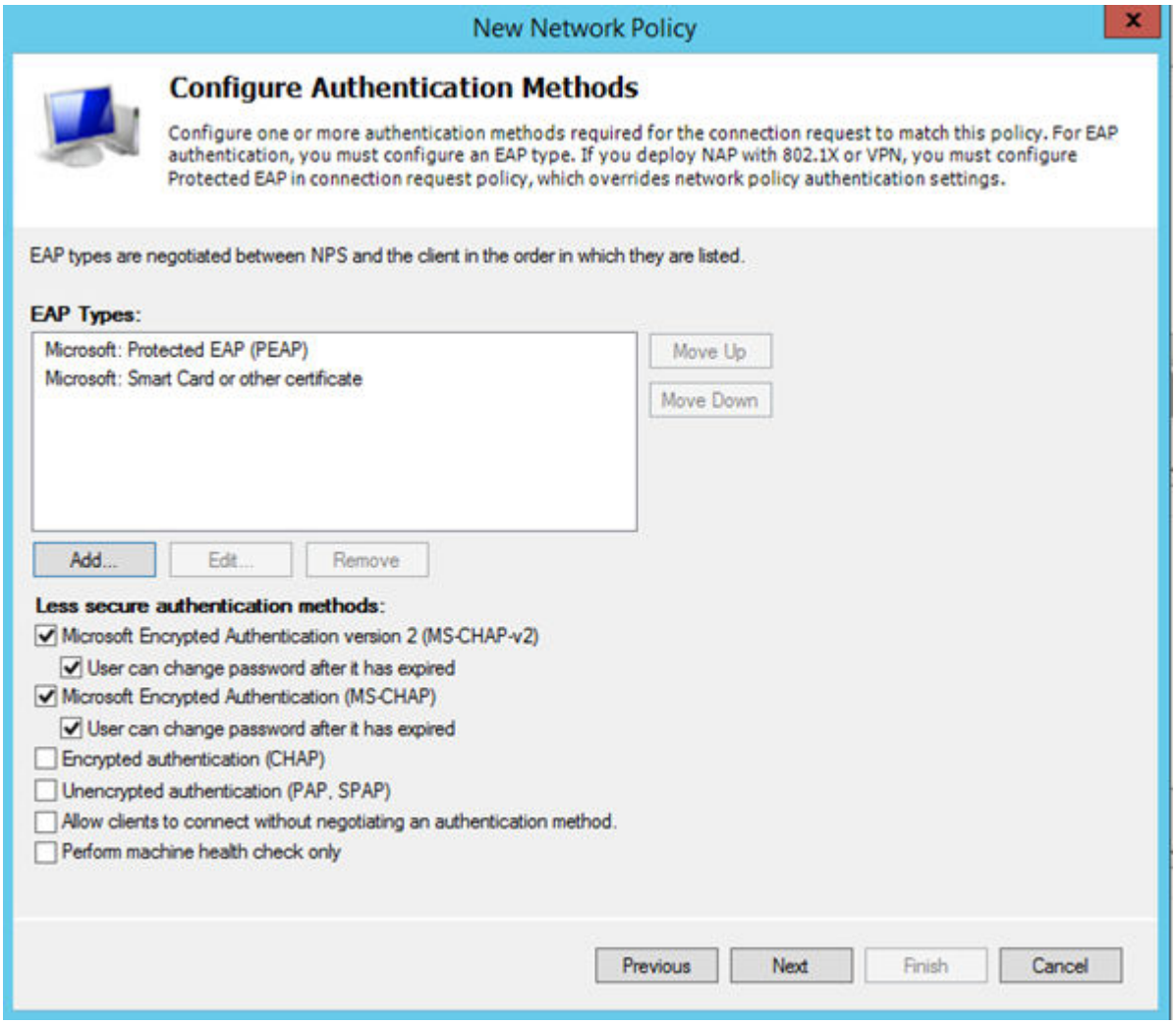


Figure 24: Configure Authentication Methods

10 Click **Next**.

11 Configure the Idle Timeout and click **Next**.

12 Configure the Radius Attributes. As an example, you can set the Filter-Id attribute to a wireless controller role. This will override the default role. The following procedure illustrates how to set the Filter-Id:

13 Click **Add**, select the **Filter-Id** attribute.

14 Click **Add**.

15 Click **Add** again and type the attribute name. The Attribute name is case sensitive and must match the Role on the wireless controller.

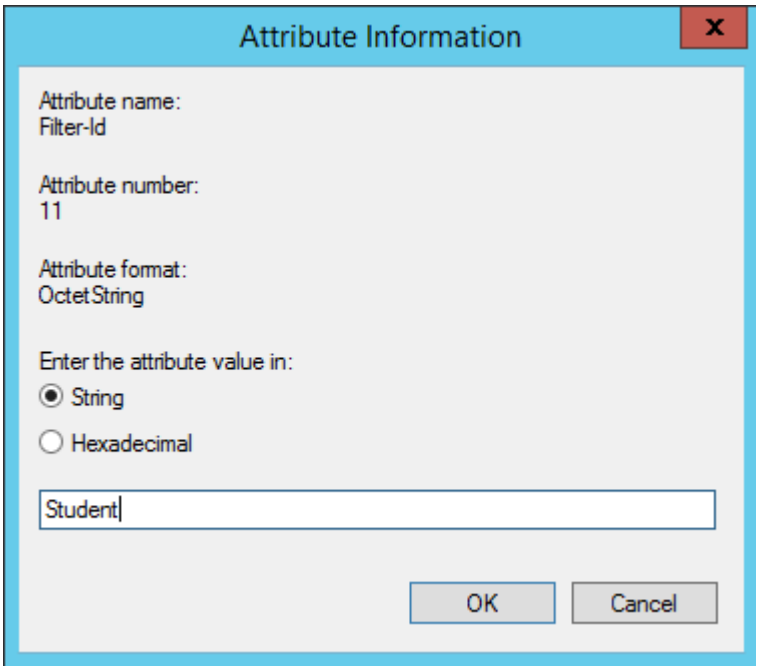


Figure 25: Attribute Information

16 Click **OK**.

17 Click **Close** to close the RADIUS Attribute dialog.

18 Click **Next**.

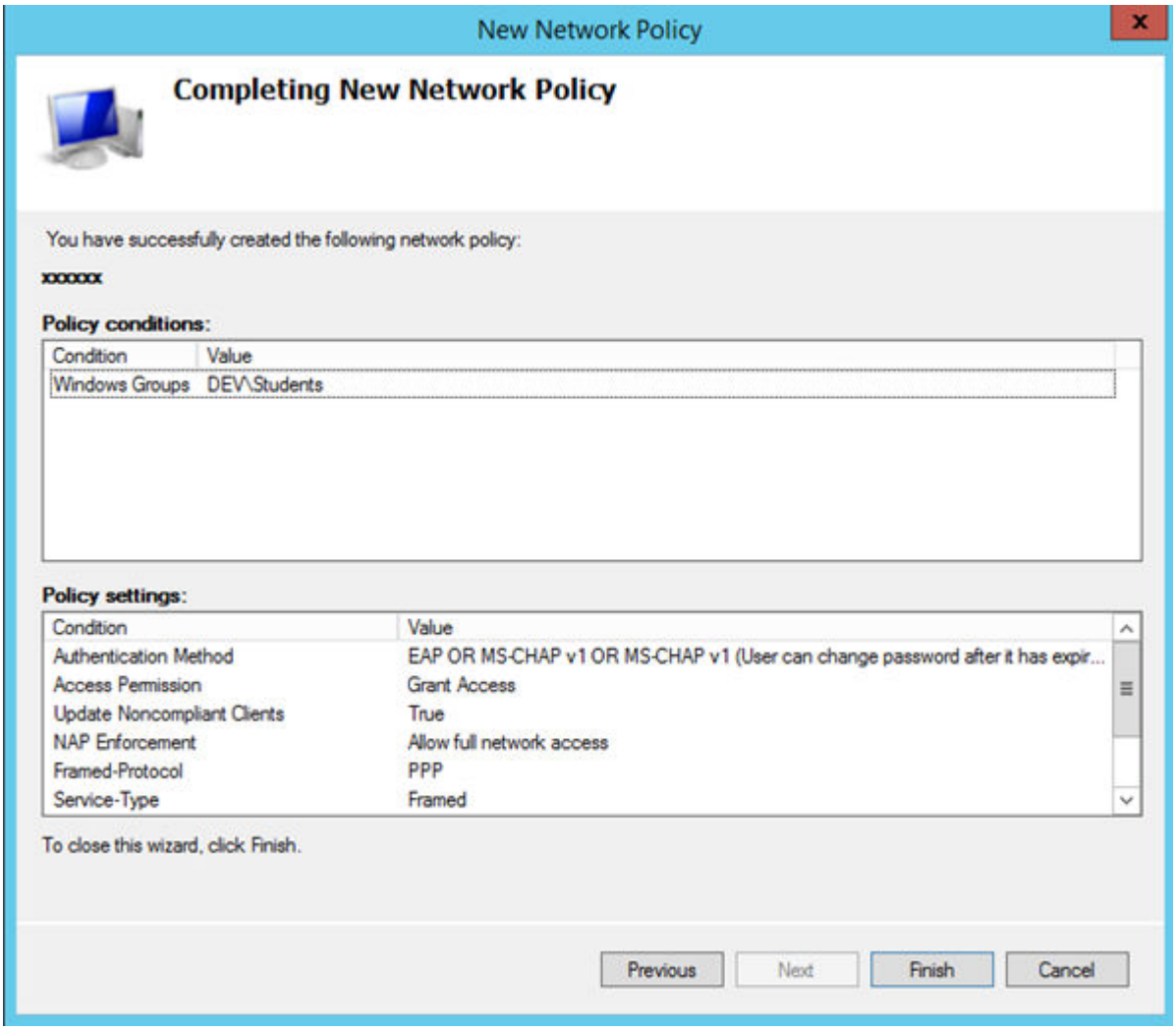


Figure 26: Completing New Network Policy

19 Click **Finish**.

DNS Service Configuration

The domain name system (DNS) stores and associates many types of information with domain names, but most importantly, it translates domain names (computer hostnames) to IP addresses.

You must install DNS on Windows Server 2012 R2 according to the server documentation. Visit http://support.microsoft.com to learn how to install and configure DNS on Windows Server 2012 R2.

The instructions here are limited to Configuring DNS for Wireless APs Discovery.

For configuration on Linux, see Configuring DNS on a Linux Server on page 45.

Configuring DNS for Wireless AP Discovery

1 Click **Start** > **Administrative Tools** > **DNS** .

2 Expand the tree and right-click on a domain.

3 Select **New Host (A or AAA)**.

The New Host window displays.

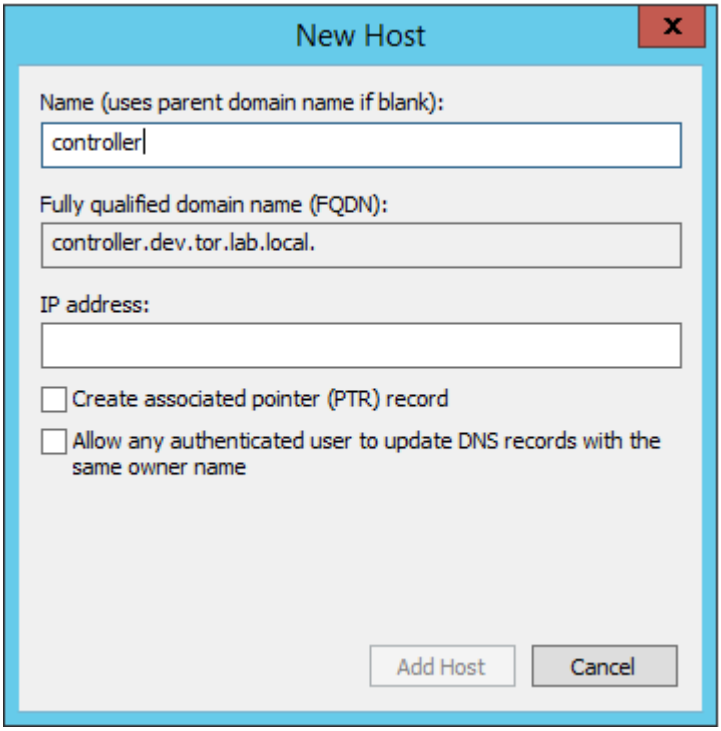


Figure 27: New Host

4 In the Name text box, type *controller*

5 In the IP address text box, type the ExtremeCloud Appliance IP address.

If configuring multiple controllers, create all records with the same name controller, and provide unique IP addresses.

6 Select **Create associated pointer (PTR) record** check box.

This option creates a record for reverse lookup.

Note

ExtremeWireless WiNG APs — Use a Domain Name Server (DNS) lookup for the host name `Controller.<domain-name>`. If you use this method for discovery, place an `"A" record` in the DNS server for Controller.<domain-name>. The <domain-name> is optional, but if used, ensure it is listed with the DHCP server.

7 Click **Add Host**.

The new host is displayed in the right pane of the screen.

8 Click **Done**.

You must now configure the Wireless APs via the ExtremeCloud Appliance.

Configuring DNS on a Linux Server

This section describes the procedure to configure Linux DNS server for ExtremeCloud Appliance IP addresses discovery.

1 Configure the Linux server to include DNS information. In the `/etc/dhcp.conf` file, add domain-name-servers and domain-name DHCP options.

```
subnet 10.2.221.0 netmask 255.255.255.0 {
range 10.2.221.30 10.2.221.130;

option slp-directory-agent true 10.2.221.2;
option subnet-mask 255.255.255.0;
option domain-name-servers 192.168.6.2;
option domain-name "Availability-221.com";
option routers 10.2.221.1;
default-lease-time 40000;
}
```

2 Configure the Linux DNS server to include ExtremeCloud Appliance IP addresses.

Create a file for the domain name configured in dhcp.conf (in this example, "Availability-221.com") as follows at `/var/named/chroot/var/named`.

The name of the file should be the following: `/var/named/chroot/var/named/named.Availability-221.com`

```
/var/named/chroot/var/named/named.Availability-221.com
$TTL 86400
@     IN    SOA   ns1.availability-221.com.     hostmaster.availability-221.com.    (
                            2      ; serial #
                            28800   ; refresh
                            14400   ; retry
                            3600000 ; expire
                            86400   ; ttl
                            )
                IN    NS    ns1.availability-221.com.
Controller      IN    A     10.2.221.2
```

3 Add the domain name to the DNS configuration file (`/var/named/chroot/etc/named.conf`).

```
$//
// a caching only nameserver config
//
options {
/*
 * If there is a firewall between you and nameservers you want
 * to talk to, you might need to uncomment the query-source
 * directive below.  Previous versions of BIND always asked
 * questions using port 53, but BIND 8.1 uses an unprivileged
 * port by default.
 */
// query-source address * port 53;
version "Bind";
recursion no;
directory "/var/named";
};
zone "Availability-221.com" {
       type master;
       file "named.Availability-221.com";
};
zone "0.0.127.in-addr.arpa" {
type master;
file "named.local";
allow-update { none; };
```

4 Confirm that DNS service is running.

```
ps -ef | grep named
named 10023 1 0 Feb18 ? 00:00:00 /usr/sbin/named -u named -t /var/named/chroot
root 7687 7531 0 22:14 pts/982 00:00:00 grep named
```

5 Verify that the domain name is configured properly.

```
nslookup Controller.Availability-221.com
Server:            127.0.0.1
Address:           127.0.0.1#53

Name:  Controller.Availability-221.com
Address: 10.2.221.2
```

3 Centralized Site with a Captive Portal

Deployment Strategy

The following strategy outlines how to create a Centralized site with an internal captive portal:

1 Add a Centralized site with a device group.
2 Configure an internal captive portal.
3 Specify a network topology.
4 Configure a captive portal network.
5 Work with engine rules.
6 Specify the network and role in the device group profile.
7 Create adoption rules.

Adding a Centralized Site with Device Group

Before you create a site, know the following information about your network:

- AP licensing domain
- AP models.

For this deployment scenario, the licensing domain is ROW (Rest of World).

For this deployment scenario, the AP model is AP3915.

1 Go to **Sites** > **Add** and configure the following parameters:

Name	**Site_Row**
Centralized or Distributed	Select **Centralized**, which is supported by AP3915.
Country	Select **Toronto Canada**. This value corresponds to the licensing domain ROW.
Timezone	Canada: America/Toronto

2 Create one or more device groups for the site.

All APs in a device group must share the following:

- AP model number
- Configuration Profile
- RF Management Profile

Go to **Device Groups** > **Add** and configure the following parameters:

Name	DeviceGroup_AP3915
Profile	AP3915-default Select a configuration profile for the AP model. The configuration profile is specific to the AP model.
RF Management	Select **Default ACS**. This option displays after you have selected the configuration profile, because the RF Management options depend on the selected configuration profile. • Default ACS supports AP39xx • Default Smart RF supports AP7xxx and AP8xxx

3 Select from the list of discovered APs.

Auto-discovered APs that match the selected configuration profile display in a list on the Create Device Group dialog.

4 Click **OK**.

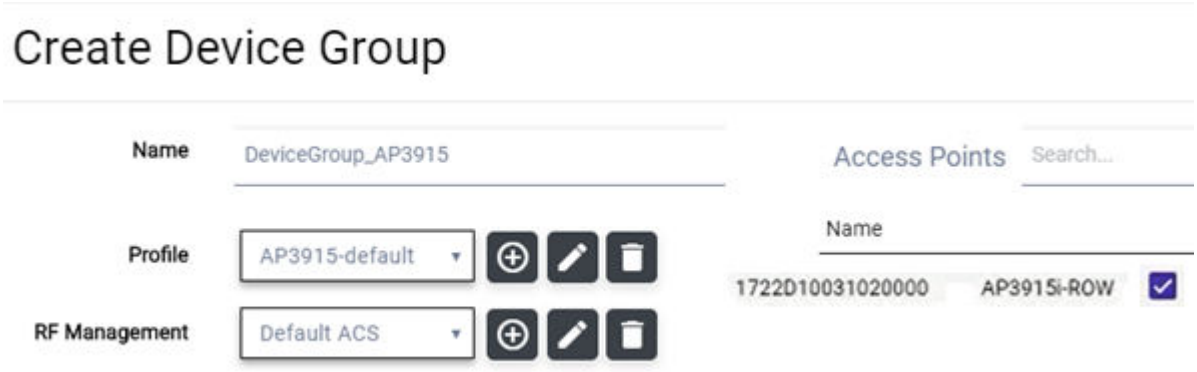


Figure 28: Create Device Group AP3915

5 Click **Save** on the Site page to save the site and device group.

6 **Optional:** Repeat steps 1-5 to create a second device group for AP3935 access points.

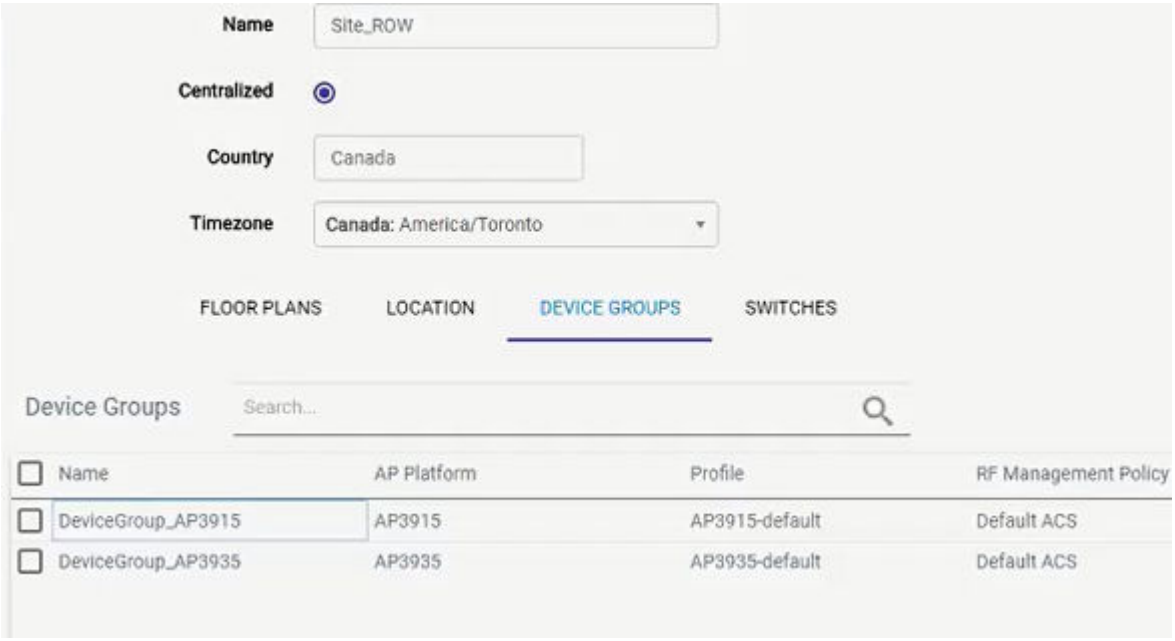


Figure 29: Centralized Site with Two Device Groups

Next, configure an internal captive portal.

Related Links

Configuring an Internal Captive Portal on page 49

Configuring an Internal Captive Portal

Creating a captive portal on ExtremeCloud Appliance that is authenticated with an external RADIUS server.

1 Go to **Onboard** > **Portal** > **Default** and select the portal type.
2 From the Authenticated Portal field, select **Authenticated Web Access** and click **Save**.
3 Go to **Onboard** > **AAA Configuration** > **RADIUS Servers** and configure the following parameters for your RADIUS server.

RADIUS Server IP address	Valid IP address of the RADIUS server.
Shared Secret	Password for the RADIUS server. The value must be at least six characters.

Next, specify a network topology.

Related Links

Specifying B@AC Network Topology on page 49

Specifying B@AC Network Topology

ExtremeCloud Appliance offers a default VLAN that is Bridged@AP, untagged. Each site can only have one untagged VLAN. For this deployment, we will specify Bridged@AC topology.

1 Go to **Policy** > **VLANS** > **Add** and configure the following parameters:

Name	**test1**
Mode	**Bridged@AC**
VLAN ID	Specify a valid VLAN ID.
Port	Specify a data port.
Layer 3	Provide the following Layer 3 parameters: • IP Address • CIDR • DHCP. Select **Relay**, then click **Configure** to enter the DHCP Relay Server IP address.

2 Click **Save**.

Next, add a network.

Related Links

Configuring a Captive Portal Network on page 50

Configuring a Captive Portal Network

Configuring an Internal Captive Portal network with WPAv2 PSK privacy.

Note
Centralized sites support B@AC and B@AP VLAN topology.

1 Go to **Networks** > **Add** and configure the following parameters:

Network Name	**test1-ICP**
SSID	**test1-ICP**
Auth Type	Select **WPAv2 with PSK** then click **Edit Privacy** and enter a password key.
Enable Captive Portal	Check this option and specify the following parameters: • Captive Portal Type = **Internal** • **Default** captive portal is specified. This is the captive portal we configured. • Authentication Method. Select **RADIUS**. • Primary RADIUS. This is the RADIUS server we configured. Enter the IP address. • Default VLAN = **test1**. This is the VLAN we created.

2 Click **Save**.

When a client connects to the network, a captive portal page is presented. The user enters a user name and password. The RADIUS authenticates the user name and password. Captive portal automatically generates two engine rules that define the Accept Policy for a client before authentication and after authentication.

Next, work with the ExtremeCloud Appliance engine rules.

Related Links

Working with Internal Captive Portal Engine Rules on page 51

Working with Internal Captive Portal Engine Rules

When configuring captive portal, the ExtremeCloud Appliance Rules Engine creates default rules for network policy. Use the default rules and modify the Accept Policy when necessary.

1 Go to **Onboard** > **Rules**.

Two new engine rules are displayed:

- Unregistered LOC: Network: Test1- ICP (SSID of network)

  Prior to CP authentication, the client matches this rule and applies the **Accept Policy** of a non-authenticated role.
- Web Authenticated LOC: Network: Test1- ICP (SSID of network)

  Once the client password is authenticated on the RADIUS server, the client matches this rule and applies the **Accept Policy** of the **Enterprise User** role.

  The **Enterprise User** is the default **Accept Policy**.

Alternatively, you can create unique **Accept Policy** roles to be assigned upon authentication.

1 Select the rule **Web Authenticated LOC: Network: Test1- ICP** and click ✎ to edit.
2 From the **Accept Policy** field select a different value.

2 Click **Save**.

Next, modify the device group profile to enable the network and role options we are using.

Related Links

Editing Device Group Profile for Network and Role on page 51

Editing Device Group Profile for Network and Role

Configure a network and be aware of policy roles that you are using before modifying the device group profile.

1 Go to **Sites** and select a site.
2 Click **Configure Site** > **Device Groups**.
3 Select **DeviceGroup_AP3915**.
4 Select ✎ to edit the default profile AP3915-default.
5 From the Networks tab, assign a radio to the network you created.

6 From the Roles tab, select the Accept Policy roles that the Rules Engine is using.

Note

Upon creating an internal captive portal network, the rules engine created two engine rules that make use of the following policies:

- Enterprise User
- Unregistered

External Captive Portal networks use the Unregistered policy by default, there is no user interaction.

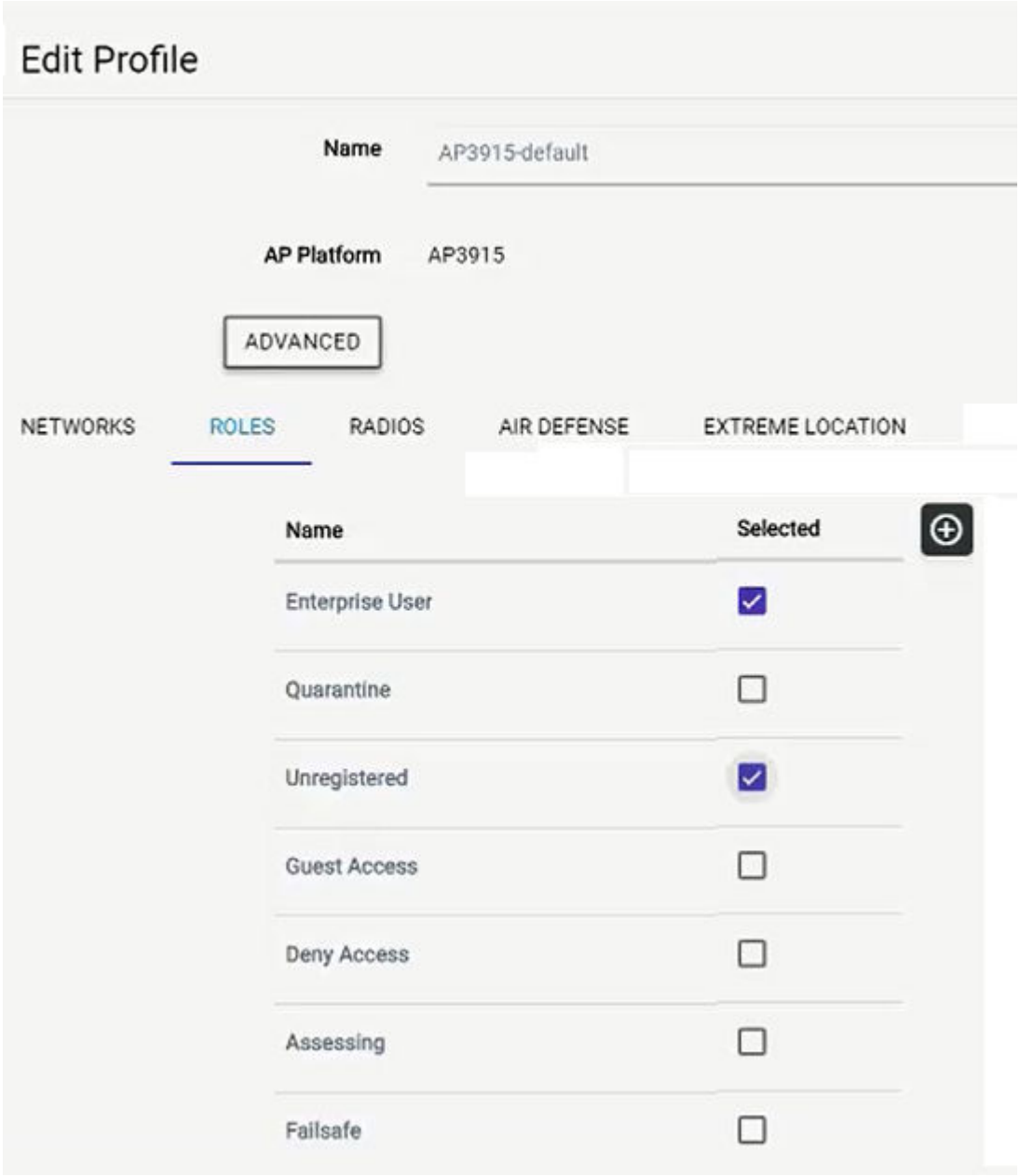


Figure 30: Edit Device Group Profile (Internal Captive Portal)

7 Optionally, you can configure settings from any of the available profile options. All APs in the device group are affected by options configured in the profile.

> **Note**
> The supported profile options depend on the AP Platform definition.

8 Click **Save** to save the profile settings.

9 Click **Close** to close **DeviceGroup_AP3915**

Currently, **Site_ROW** has **DeviceGroup_AP3915** with the following:

- 2 Roles
- 1 Network
- 1 Device

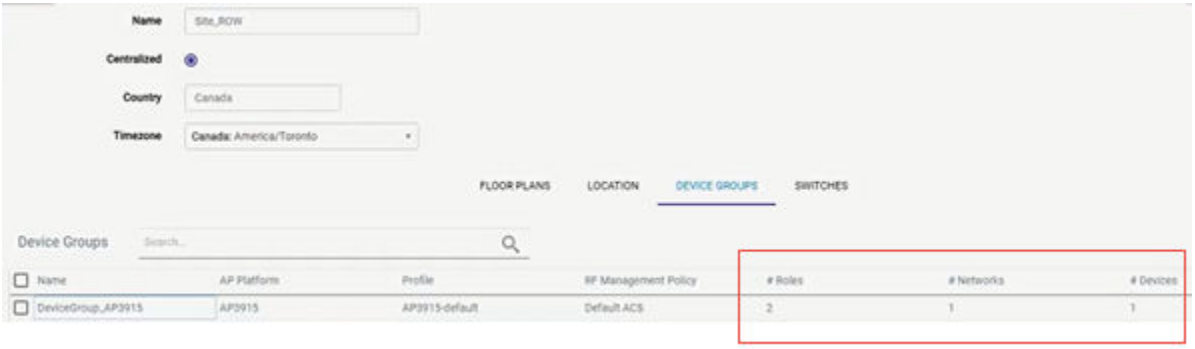


Figure 31: Centralized Site with Device Group

Next, configure adoption rules.

Related Links

Creating Adoption Rules on page 53

Creating Adoption Rules

Configure a site and a device group before creating adoption rules. Adoption rules automatically assign devices to specific device groups upon registration with ExtremeCloud Appliance.

1 Go to **Devices** > **Adoption** > **Add** and configure the following parameters:

Site	Specify the site that will hold the devices. **Site_ROW**
Device Group	Specify the device group that will hold the devices. **DeviceGroup_AP3915**
Model	Specify the AP model of the devices affected by this rule. **AP3915**

2 Alternatively, you could specify other options to define the rule.

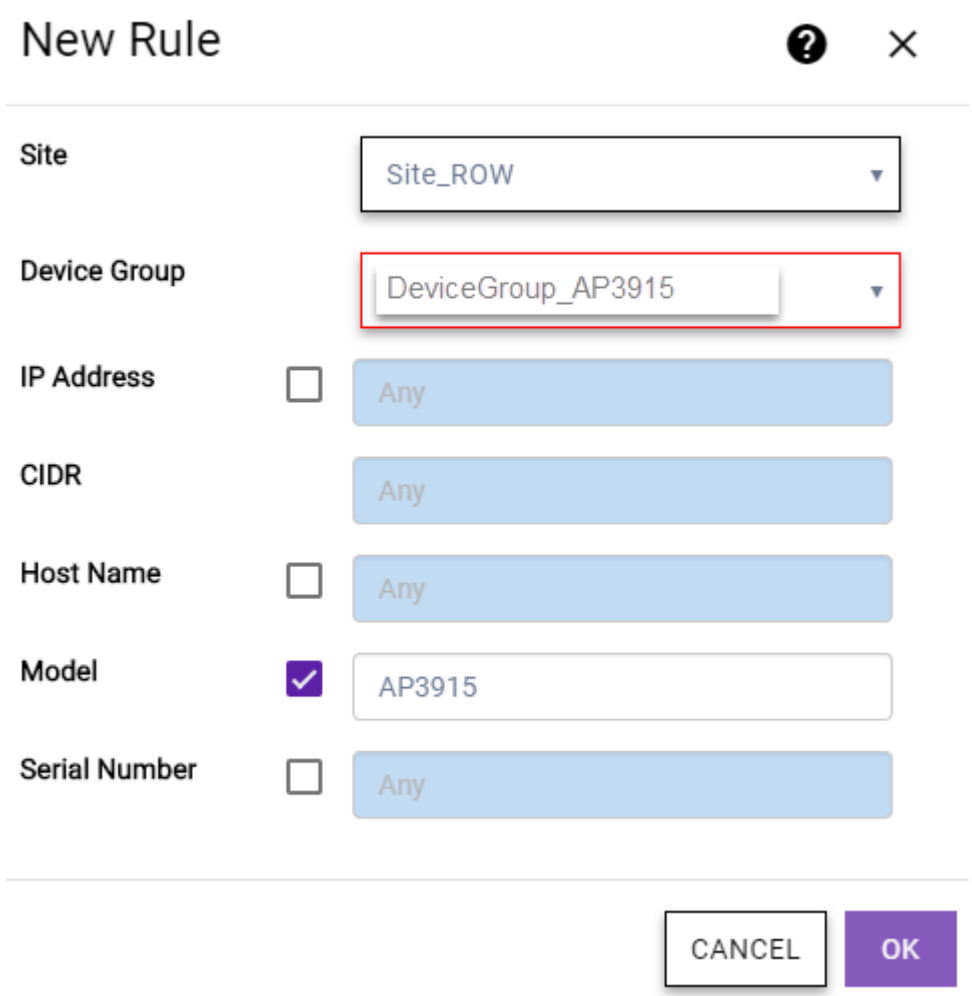


Figure 32: Create Adoption Rule

3 Click **OK**.

4 From the Adoption Rules page, click **Save**.

All AP3915 access points will be automatically added to **DeviceGroup_AP3915** within **Site_ROW** upon registration with ExtremeCloud Appliance.

Note

Be aware that all devices in a device group must share the following:

- AP model number
- Configuration Profile
- RF Management Profile

4 Centralized Site with AAA Network

Deployment Strategy

The following strategy outlines how to create a Centralized site with a AAA network.

1 Add a Centralized site with a device group.
2 Configure a AAA network.
3 Work with engine rules.
4 Create a policy role.
5 Specify the network and role in the device group profile.
6 Create adoption rules.

Configuring a AAA Network

Using the same Centralized site: **Site_ROW** specify a separate tagged VLAN for the AAA Network, defining a different IP address range for the AAA Network.

Note
You can configure more than one network on a single VLAN, but to configure a separate IP address range for the AAA Network, we will create a separate VLAN.

1 Go to **Policy** > **VLAN** > **Add** to create a new VLAN for the AAA Network.

For more information, see Specifying B@AC Network Topology on page 49.

2 Go to **Networks** > **Add** and configure the following parameters:

Network Name	Test2-AAA
SSID	Test2-AAA
Auth Type	WPA2 Enterprise w/RADIUS
Authentication Method	RADIUS
Primary RADIUS	RADIUS server IP address (This is the RADIUS server we configured.)
Default Auth Role	Quarantine
	Defines the default Accept Policy for a client attempting to join the network. When an authenticated client does not meet rule conditions on an 802.1x AAA Network, the default policy role is Quarantine.

Default VLAN	test2 (This is the VLAN we created for the AAA Network.)

3 Click **Save**.

Next, work with engine rules.

Related Links

Creating an Engine Rule on page 56

Creating an Engine Rule

Create a unique engine rule that applies the Enterprise User role upon authentication.

1 Go to **Onboard** > **Rules** > **Add** and configure the following parameters:

Name	test2-rule
Rule Enabled	Select this box to enable the rule.
Location Group	Specify the Test2-AAA Network we created.

2 Select **Enterprise User** as the Accept Policy.

3 Click **Save**.

Next, create a unique policy role that this engine rule will apply upon authentication instead of **Enterprise User**.

Related Links

Creating a Policy Role on page 56

Creating a Policy Role

You can create a policy role that will customize network access.

To create a new policy role:

1 Go to **Policy** > **Roles** > **Add** and configure the following parameters.

Name	**myTest2-policy**
Default Action	Set to **Deny**. The policy rule will deny everything except for the rules we define as allowed.

2 Select the **L3 L4 Rules** section and click **New**.

3 Configure the following rules:

- Allow traffic to subnet 0.0.0.0/0, any protocol, Port DHCP Server (68).
- Allow traffic to subnet 0.0.0.0/0, any protocol, port Port DHCP Client (67).
- Allow traffic to subnet 10.48.51.50/28, any protocol, any port.
- Allow traffic to subnet 10.48.49.9/32, any protocol, any port.

4 Click **Save** to save the policy.

5 Go to **Onboard** > **Rules**.

6 Edit the **test2-rule** Accept Policy. Apply **myTest2-policy** instead of **Enterprise User** policy.

a Highlight **test2-rule** and click ✎.

b From the Accept Policy field, select **myTest2-policy**.

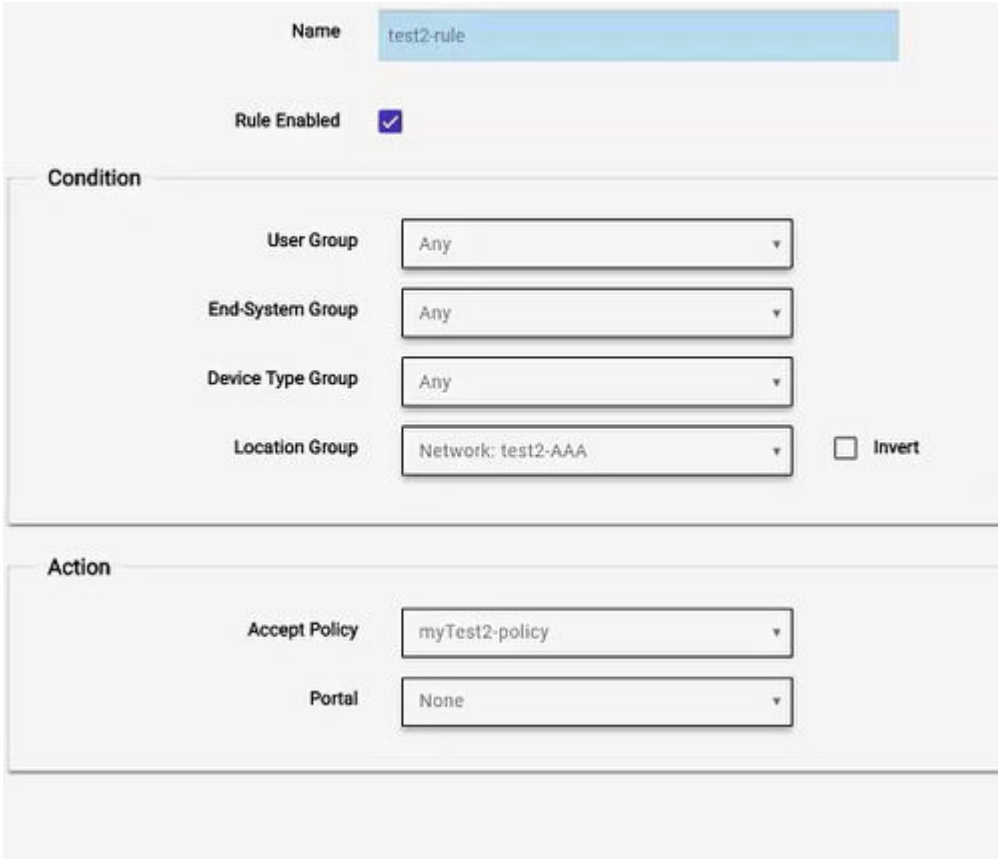


Figure 33: Engine Rule with Unique Policy

7 Click **Save**.

Upon authentication to the network, the client reaches the engine rule **test2-rule**. Client is accepted to the network based on the unique Accept Policy **myTest2-policy**.

Next, enable **myTest2-policy** within the device group profile.

Related Links

Applying a AAA Network and Role to the Device Group on page 57

Applying a AAA Network and Role to the Device Group

Each time you configure a network or specify policy roles, you must enable the network and roles within the device group.

1 Go to **Sites** > **Configure Site** > **Device Groups**.
2 Select **DeviceGroup_AP3915**.
3 Select ✎ to edit the default profile AP3915-default.
4 From the Networks tab, assign a radio to network **test2-AAA**.

This is the AAA network we created.

5 From the Roles tab, select the Accept Policy roles we have configured under the Rules Engine. Quarantine is added to the list of roles.
   - Enterprise User
   - Quarantine
   - Unregistered
   - myTest2-policy
6 Click **Save** to save the profile settings.
7 Click **Close** to close **DeviceGroup_AP3915**.

Next, you have the option to create adoption rules for device group **DeviceGroup_AP3915**.

Related Links

Creating Adoption Rules on page 53

5 Distributed Site with a Captive Portal

Deployment Strategy

The following strategy outlines how to create a Distributed site with a captive portal:

1 Add a Distributed site with a device group.
2 Configure an internal captive portal.
3 Specify a network topology.
4 Configure a captive portal network.
5 Work with engine rules.
6 Specify the network and role in the device group profile.
7 Create adoption rules.

Adding a Distributed Site

Before you create a site, know the following information about your network:

- AP licensing domain
- AP model.

For this deployment scenario, the licensing domain is FCC

For this deployment scenario, the AP model is AP76xx

1 Go to **Sites** > **Add** and configure the following parameters:

Name	**Site_FCC**
Centralized or Distributed	Select **Distributed**, which is supported by AP7632.
Country	Select **United States**. This value corresponds to the licensing domain FCC.
Timezone	**United States:** America/New York

2 Create one or more device groups for the site.

The most simple site configuration allows for one device group for each AP model, selecting the default configuration profile and default RF Management profile for that AP model.

A more complex deployment allows for more than one device group with the same AP model that makes use of different profile features and/or a unique RF Management profile for each device group. With this more complex deployment, create a device group for any combination of configuration features and RF configurations. All APs in a device group must share the following:

- AP model number
- Configuration Profile
- RF Management Profile

Go to **Device Groups** > **Add** and configure the following parameters:

Name	DeviceGroup_AP7632
Profile	AP7632-default Select a configuration profile for the AP model. The configuration profile is specific to the AP model.

RF Management	This option displays after you have selected the configuration profile, because the RF Management options depend on the selected configuration profile.
	• Default ACS supports AP39xx
	• Default Smart RF supports:
	  • AP7522
	  • AP7532
	  • AP7562
	  • AP7612
	  • AP7632
	  • AP7662
	  • AP8432
	  • AP8533
	
	Select **Default Smart RF**.

3 Select from the list of discovered APs.

Auto-discovered APs that match the selected configuration profile display in a list on the Create Device Group dialog.

4 Click **OK**.

5 Click **Save** on the Site page to save the site and device group.

Next, configure an internal captive portal.

Related Links

Configuring an Internal Captive Portal on page 49

Specifying B@AP Network Topology

Distributed sites support B@AP VLAN topology only. ExtremeCloud Appliance offers a default B@AP topology, one per site. You can configure your network with the default B@AP topology or configure another VLAN.

To configure a B@AP topology:

1 Go to **Policy** > **VLANS** and configure the following parameters:

Name	**Bridged at AP Untagged**
Mode	**B@AP**
VLAN ID	Unique VLAN ID

2 Click **Save**.

Next, configure a network.

Related Links

Configuring B@AP Captive Portal Network for a Distributed Site on page 61
Configuring External Captive Portal Network on page 91

Configuring B@AP Captive Portal Network for a Distributed Site

ExtremeCloud Appliance offers a default B@AP topology that you can use for your B@AP network. Or, you can configure a separate B@AP topology. See Specifying B@AP Network Topology on page 60.

Note
Distributed sites only support B@AP VLAN topology.

Creating an Internal Captive Portal network with WPAv2 PSK privacy.

1 Go to **Networks** > **Add** and configure the following parameters:

Network Name	**ICP_B@AP_Distributed**
SSID	**ICP_B@AP_Distributed**
Auth Type	Select **WPAv2 with PSK** then click **Edit Privacy** and enter a password key.
Enable Captive Portal	Check this option and specify the following parameters: • Captive Portal Type = **Internal** • **Default** captive portal is specified. This is the captive portal we configured. • Authentication Method. Select **RADIUS**. • Primary RADIUS. This is the RADIUS server we configured. Enter the IP address. • Default VLAN = **B@AP Untagged**. This is the B@AP VLAN we configured under Specifying B@AP Network Topology on page 60.
Default Auth Role	(Optional) In this scenario, we do not specify a role here. We are using the default **Enterprise User** role. Configure this setting if you want to override the default accept policy role with your own default authentication policy role. By default, **Enterprise User** is the Default Auth Role. To configure a different role as the Default Auth Role: 1 Configure the role under **Policy** > **Roles** and indicate that it is the Default Auth Role here. 2 Go to **Onboard** > **Rules** and edit a policy rule, specifying **Default Auth Role** in the Accept Policy field.

(Edit the Web Authenticated rule for Captive Portal.)

2 Click **Save**.

When a client connects to the network, a captive portal page is presented. The user enters a user name and password. The RADIUS server authenticates the user name and password. Captive portal automatically generates two engine rules that define the Accept Policy for a client before authentication and after authentication.

Next, work with the ExtremeCloud Appliance engine rules.

Working with Captive Portal Engine Rules

When configuring captive portal, the ExtremeCloud Appliance Rules Engine creates two default rules for network policy. Use the default rules and modify the Accept Policy when necessary.

1 Go to **Onboard** > **Rules**.

Two new engine rules are displayed:

- Unregistered LOC: Network: ICP_B@AP_Distributed

  Prior to CP authentication, the client matches this rule and applies the **Accept Policy** of a non-authenticated role.
- Web Authenticated LOC: Network: ICP_B@AP_Distributed

  Once the client password is authenticated on the RADIUS server, the client matches this rule and applies the **Accept Policy** of the **Enterprise User** role.

  The **Enterprise User** is the default **Accept Policy**.

Alternatively, you can create unique **Accept Policy** roles to be assigned upon authentication.

1 Select the rule **Web Authenticated LOC: Network: Test1- ICP** and click ✎ to edit.
2 From the **Accept Policy** field select a different value.

2 Click **Save**.

Next, modify the device group profile to enable the network and role options we are using.

Related Links

Editing Device Group Profile for Network and Role on page 51

Creating Adoption Rules

Configure a site and a device group before creating adoption rules. Adoption rules automatically assign devices to specific device groups upon registration with ExtremeCloud Appliance.

1 Go to **Devices** > **Adoption** > **Add** and configure the following parameters:

Site	Specify the site that will hold the devices. **Site_FCC**
Device Group	Specify the device group that will hold the devices. **DeviceGroup_AP7632**
Model	Specify the AP model of the devices affected by this rule. **AP7632**

2 Alternatively, you could specify other options to define the rule.

3 Click **OK**.

4 From the Adoption Rules page, click **Save**.

All AP7632 access points will be automatically added to **DeviceGroup_AP7632** within **Site_FCC** upon registration with ExtremeCloud Appliance.

Note

Be aware that all devices in a device group must share the following:

- AP model number
- Configuration Profile
- RF Management Profile

6 Configuring an External NAC Server for MBA and AAA Authentication

Deployment Strategy

The following deployment strategy uses an external NAC (Network Access Control) server to authenticate client sessions using MBA and AAA authentication methods. We will configure the “Use Default Auth” and the “Pass Through External RADIUS” Accept Policy actions upon successful user authentications.

For this strategy we are using the following:

- One of the following AP39xx APs:
  - AP3917i/e/k
  - AP3916ic
  - AP3915i/e
  - AP3912i
  - AP3935i/e
  - AP3965i/e
- One of the following ExtremeWireless WiNG APs:
  - AP7522
  - AP7532
  - AP7562
  - AP7612
  - AP7632
  - AP7662
  - AP8432
  - AP8533
- An external NAC server running version 8.1.3 or later, and an Extreme Management Center Server server to manage and configure the NAC server.

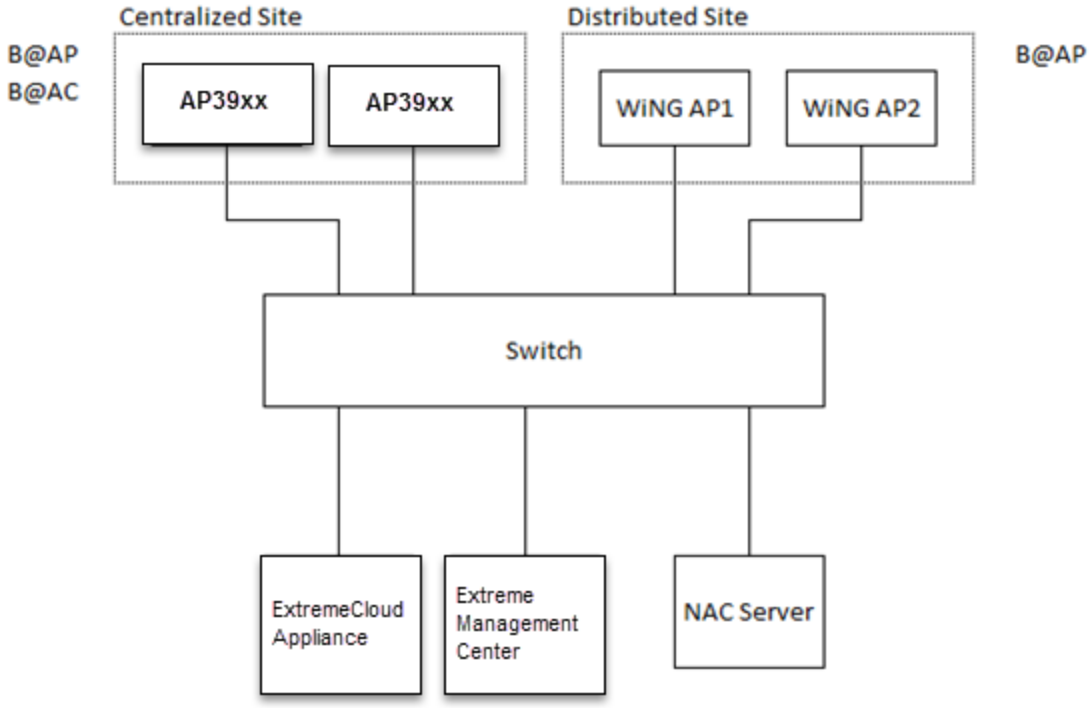


Figure 34: External NAC Server / ExtremeCloud Appliance Setup

Configuring the External NAC Server

Take the following steps to configure the External NAC server:

Extreme Management Center Console

1 Navigate to the Extreme Management Center OneView page or launch the Extreme Management Center console.

2 Add the external NAC server and the ExtremeCloud Appliance esa0 interface as devices to be managed by Extreme Management Center.

- Open NAC Manager using either OneView or the Extreme Management Center console.
- Add the external NAC server as an appliance to be managed.

  1 Go to **Switches** > **Add Switch**.

  2 Select the ExtremeCloud Appliance esa0 interface

  3 Configure the following parameters:

Primary Engine	NAC server
RADIUS Attributes to Send	Edit RADIUS Attribute Settings

3 To edit the RADIUS Attribute settings:

- Select **Add** and provide the Attribute Group name.
- In the Attribute field, enter the following:
  - Filter-Id=%FILTER_NAME%
  - Filter-Id=Enterasys:version=1:%MANAGEMENT%policy=%POLICY_NAME%
  - Login-LAT-Port=%LOGIN_LAT_PORT%
  - Service-Type=%MGMT_SERV_TYPE%

Note
The Attribute Group is configured to ensure that both ExtremeWireless and ExtremeWireless WiNG APs function with the appliance.

4 Save the Attribute Group, then select this group as the option in the **RADIUS Attributes to Send** field.

5 Press **OK**.

NAC Manager

6 Go to **Tools** > **Management**

7 Click **Configuration** > **Advanced NAC Configurations** > **AAA Configurations** > **Local Password Repository** > **Default**.

8 Add a new user.

Click **Add** and configure the following parameters:

- Display Name
- Username
- Password

9 Click **Save**.

10 In the Advanced Configuration window, navigate to **NAC Configurations** > **Rule Components** > **End-System Group**.

11 Add a new **End-System Group**.

Add a new MAC entry for each MAC address of each client that should be successfully authenticated.

12 Click **Save**.

13 In the Advanced Configuration window, navigate to **NAC Configurations** > **Default**.

14 Add a new rule.

From the End-System Group drop-down list, select the End-System Group that you previously created.

15 In the **Profile** drop-down list, select **Default NAC Profile**.

Note
Assuming no prior configuration changes have been made to the Default NAC Profile, it will send an *Enterprise User* Filter-ID.

16 Save the rule and move it up the list, just after the **Assessment Warning** rule.

17 Close the Advanced Configuration window and Enforce the NAC engine.

18 Once the Enforce is successful, close the window.

Network with Default Auth Role

The following procedure outlines how to configure a network and associate it with a Default Auth Role accept policy. The following network types are described:

- MBA Network
- AAA Network

Related Links

Configuring an MBA Network on page 67
Configuring a AAA Network on page 68

Configuring an MBA Network

To create the MBA network associated to a Default Auth Role accept policy. Take the following steps:

1 Configure a RADIUS server for AAA authentication.

- Log in to ExtremeCloud Appliance and go to **Onboard** > **AAA** > **Radius Server** and add a new RADIUS server.
- Configure the following parameters:

Radius Server IP Address	Add the NAC IP address
Shared Secret	Provide the NAC Shared Secret.

Note
To find the Shared Secret of the NAC Manager, go to:
Advanced NAC Configuration Settings > **Global and Appliance Settings** > **Appliance Settings**.

2 Create a new network.

- Enable **MAC-based authentication (MBA)** and choose an appropriate MBA Timeout Role.
- Clear the **Authenticate Locally for MAC** check box.
- Choose **RADIUS** as the Authentication Method and select the NAC added in Step 1 as the Primary RADIUS.
- Select a Default VLAN.

Note
WiNG AP's do not support Bridged@AC VLAN's.

- Click **Save**.

3 Add a new rule.
- From ExtremeCloud Appliance, navigate to **Onboard** > **Rules**.
- Click **Add**.
- In the Location Group drop-down menu, select **Network: <name of your network>**.
- From the Accept Policy field:
  - To configure a Default Auth Role Policy: select **Use Default Auth Role**.
  - To configure a Pass-thru External RADIUS Accept Policy: select **Pass Through External RADIUS**.
- Save the rule.

4 Assign the network created previously and its Default Auth Role to either a Centralized or Distributed site and save. Take the following steps:
- Go to **Sites** and select a site.
- Click **Configure Site**.
- Click the **Device Groups** tab and select a device group.
- Click ✎ on the Profile field to edit the device group profile.
- Go to the **Networks** tab and select the configured network.
- Go to the **Roles** tab and select the configured Default Auth Role.

Finally, associate clients to the SSID of the network. The Access-Request is sent to the external NAC server. The NAC server matches the MAC address of the user with one of the MAC addresses in the End-System Group (that was created earlier) and sends an Access-Accept with a Filter-ID *Enterprise User*. The ExtremeCloud Appliance Access Control engine ignores the Filter-ID and applies the Default Auth Role that was configured under Network Settings.

Configuring a AAA Network

To configure a AAA Network associated to a Default Auth Role accept policy. Take the following steps:

On ExtremeCloud Appliance:

Use the IP address of the external NAC server as the primary RADIUS server.

1 Configure a RADIUS server for AAA authentication.
- Log in to ExtremeCloud Appliance and go to **Onboard** > **AAA** > **Radius Server** and add a new RADIUS server.
- Configure the following parameters:

Radius Server IP Address	Add the NAC IP address
Shared Secret	Provide the NAC Shared Secret.

Note
To find the Shared Secret of the NAC Manager, go to:
Advanced NAC Configuration Settings > **Global and Appliance Settings** > **Appliance Settings**.

2 Create a new network.

Configure the following parameters:

Auth Type	WPA2 Enterprise w/ RADIUS
Authentication Method	RADIUS
Primary RADIUS	IP Address of the External NAC added in Step 1.
Default Auth Role	Select a role other than *Enterprise User*.
Default VLAN	Select a Default VLAN. B@AP *VLAN ID*

Note
ExtremeWireless WiNG AP's do not support Bridged@AC VLAN's.

3 Click **Save**.

4 Create a policy rule.

Go to **Onboard** > **Rules** and configure the following parameters:

Location Group	Network: *<name of your network>*
Accept Policy	• To configure a Default Auth Role Policy, select **Use Default Auth Role**. • To configure a Pass-Through External RADIUS Accept Policy, select **Pass Through External RADIUS**.

5 Click **Save**.

On the NAC Manager:

6 Edit the rule you created on ExtremeCloud Appliance here.

Configure the following parameters:

Authentication Method	802.1x
End-System Group	Any

7 Click **Save** and enforce the NAC.

On ExtremeCloud Appliance:

8 Assign the network created previously and its Default Auth Role to either a Centralized or Distributed site and save.

- Go to **Sites** and select a site.
- Click **Configure Site**.
- Click the **Device Groups** tab and select a device group.
- Click ✎ on the Profile field to edit the device group profile.
- Go to the **Networks** tab and select the configured network.
- Go to the **Roles** tab and select the configured Default Auth Role.

Associate clients to the SSID of the Network, when prompted for the username and password, use the username and password created with the New User. The external NAC server matches the rule you created under New Rule and upon successful authentication sends an Access-Accept and a Filter-ID *Enterprise User*. The ExtremeCloud Appliance Access Control engine ignores the Filter-ID and applies the Default Auth Role that was configured under Network Settings.

Network with Pass-Through External RADIUS

The following procedure outlines how to configure a network and associate it with a Pass-Through External RADIUS accept policy. The following network types are described:

- MBA Network
- AAA Network

Related Links

Configuring an MBA Network on page 70
Configuring a AAA Network on page 71

Configuring an MBA Network

To create the MBA network associated to a Pass-thru External RADIUS accept policy. Take the following steps:

1 Configure a RADIUS server for AAA authentication.

- Log in to ExtremeCloud Appliance and go to **Onboard** > **AAA** > **Radius Server** and add a new RADIUS server.
- Configure the following parameters:

Radius Server IP Address	Add the NAC IP address
Shared Secret	Provide the NAC Shared Secret.

Note
To find the Shared Secret of the NAC Manager, go to:
Advanced NAC Configuration Settings > **Global and Appliance Settings** > **Appliance Settings**.

2 Create a new network.

- Enable **MAC-based authentication (MBA)** and choose an appropriate MBA Timeout Role.
- Clear the **Authenticate Locally for MAC** check box.
- Choose **RADIUS** as the Authentication Method and select the NAC added in Step 1 as the Primary RADIUS.
- Select a Default VLAN.

Note
WiNG AP's do not support Bridged@AC VLAN's.

- Click **Save**.

3 Add a new rule.

- From ExtremeCloud Appliance, navigate to **Onboard** > **Rules**.
- Click **Add**.
- In the Location Group drop-down menu, select **Network: <name of your network>**.
- From the Accept Policy field:
  - To configure a Default Auth Role Policy: select **Use Default Auth Role**.
  - To configure a Pass-thru External RADIUS Accept Policy: select **Pass Through External RADIUS**.
- Save the rule.

4 Assign the network created previously and its Default Auth Role to either a Centralized or Distributed site and save. Take the following steps:

- Go to **Sites** and select a site.
- Click **Configure Site**.
- Click the **Device Groups** tab and select a device group.
- Click ✎ on the Profile field to edit the device group profile.
- Go to the **Networks** tab and select the configured network.
- Go to the **Roles** tab and select the configured Default Auth Role.

Finally, associate clients to the SSID of the network. The Access-Request is sent to the external NAC server. The NAC server matches the MAC address of the user with one of the MAC addresses in the End-System Group (that was created earlier) and sends an Access-Accept with a Filter-ID *Enterprise User*. The ExtremeCloud Appliance applies the *Enterprise User* Role instead of the Default Auth Role that was configured under Network Settings.

Note
The *Enterprise User* role must exist on ExtremeCloud Appliance and must be assigned to the same device group as the client in order to be applied.

Configuring a AAA Network

To create the MBA network associated to a Pass-thru External RADIUS Accept Policy. Take the following steps:

On ExtremeCloud Appliance:

Use the IP address of the external NAC server as the primary RADIUS server.

1 Configure a RADIUS server for AAA authentication.

- Log in to ExtremeCloud Appliance and go to **Onboard** > **AAA** > **Radius Server** and add a new RADIUS server.
- Configure the following parameters:

Radius Server IP Address	Add the NAC IP address
Shared Secret	Provide the NAC Shared Secret.

Note
To find the Shared Secret of the NAC Manager, go to:
Advanced NAC Configuration Settings > **Global and Appliance Settings** > **Appliance Settings**.

2 Create a new network.

Configure the following parameters:

Auth Type	WPA2 Enterprise w/ RADIUS
Authentication Method	RADIUS
Primary RADIUS	IP Address of the External NAC added in Step 1.
Default Auth Role	Select a role other than *Enterprise User*.

Default VLAN	Select a Default VLAN. B@AP *VLAN ID*

Note
ExtremeWireless WiNG AP's do not support Bridged@AC VLAN's.

3 Click **Save**.

4 Create a policy rule.

Go to **Onboard** > **Rules** and configure the following parameters:

Location Group	Network: *<name of your network>*
Accept Policy	• To configure a Default Auth Role Policy, select **Use Default Auth Role**. • To configure a Pass-Through External RADIUS Accept Policy, select **Pass Through External RADIUS**.

5 Click **Save**.

On the NAC Manager:

6 Edit the rule you created on ExtremeCloud Appliance here.

Configure the following parameters:

Authentication Method	802.1x
End-System Group	Any

7 Click **Save** and enforce the NAC.

On ExtremeCloud Appliance:

8 Assign the network created previously and its Default Auth Role to either a Centralized or Distributed site and save.

- Go to **Sites** and select a site.
- Click **Configure Site**.
- Click the **Device Groups** tab and select a device group.
- Click ✎ on the Profile field to edit the device group profile.
- Go to the **Networks** tab and select the configured network.
- Go to the **Roles** tab and select the configured Default Auth Role.

Associate clients to the SSID of the Network, when prompted for the username and password, use the username and password created with the New User. The external NAC server matches the rule you created under New Rule and upon successful authentication sends an Access-Accept and a Filter-ID *Enterprise User*. The ExtremeCloud Appliance Access Control engine applies the *Enterprise User* Role instead of the Default Auth Role that was configured under Network Settings.

Note
The *Enterprise User* role must exist on ExtremeCloud Appliance and must be assigned to the same device group as the client in order to be applied.

7 Deploying Extreme Management Center as External Captive Portal

Deployment Strategy

The following strategy outlines how to configure ExtremeCloud Appliance to integrate with Extreme Management Center, which houses the external captive portal, handling client authentication. The portal resides on the NAC server and ExtremeCloud Appliance handles the client network connections. Traffic connecting to the Guest network will send and receive all RADIUS requests from the externally defined RADIUS server, not from the ExtremeCloud Appliance that processes the request. The NAC server provides RADIUS authentication and authorization and policies that are defined in Extreme Management Center.

The following outlines how to integrate ExtremeCloud Appliance with Extreme Management Center, configuring an External Captive Portal on the NAC server.

1 Add a site with a device group.
2 Configure the network as External Captive Portal.
3 Assign the network to the device group by modifying the configuration profile.
4 Create a RADIUS pass-through rule on ExtremeCloud Appliance.
5 Add ExtremeCloud Appliance to Extreme Management Center as a switch.
6 On NAC, create an Unregistered Policy for the ExtremeCloud Appliance Pass-Through Network.
7 Edit the NAC configuration profile, associating network policy and Location-Based Services.

Configuring an External Captive Portal Network

Configuring an External Captive Portal network with WPAv2 PSK privacy.

1 Go to **Networks** > **Add** and configure the following parameters:

Network Name	**ECA_Guest**
SSID	**ECA_Guest**

Auth Type

Select **WPAv2 with PSK** then click **Edit Privacy** and enter a password key.

> **Note**
> 802.1x authentication is not supported with captive portal.

Enable Captive Portal

Check this option and specify the following parameters:

Captive Portal Type	External
ECP URL	(http/https)://<access engine fqdn or IP address>/static/index.jsp

- This can be the FQDN or IP address of the access engine.
- FQDN should be resolvable by connecting end systems via DNS.
- Full URL of "/static/index.jsp" is required for both standard and mobile captive portal detection and device detection by the access control engine.
- When creating Walled Garden rules, create an L3/L4 rule that allows the IP address of the External NAC.

Identity/ Shared Secret

Use the Shared Secret setting for switches as defined by your Access Control Engine Credentials setting. Right-click on the engine, and select **Engine Settings** The default shared secret is ETS_TAG_SHARED_SECRET..

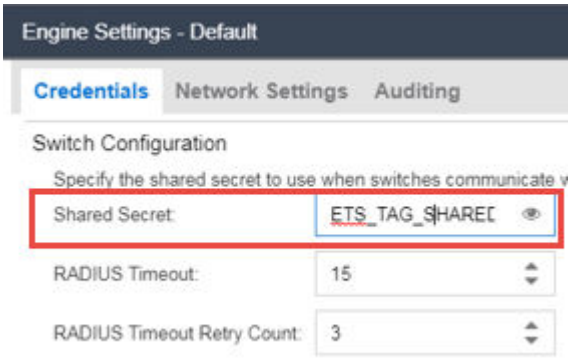


Figure 35: Extreme Management Center Engine Settings Dialog

Use HTTPS

Check this option if using https on the Access Control Engine portal configuration.

Send Successful Login To

Original Destination. Or ,enter the redirection URL here.

MAC-based authentication (MBA)

Enable and configure the following parameters:

MBA Timeout Role	Enterprise User This setting is a failsafe only. It is not used if the proper filter-ids are sent from the Access Control Engine.
Authentication Method	RADIUS • Set the Authentication Method to RADIUS and specify your Access Control Engine's IP (or IP's as primary/ backup in your Extreme Management Center configuration).

	You can also use “Default” here if the primary/backup RADIUS server is in your “Default” AAA configuration. Specify your Access Control Engine's not an off-box RADIUS server (i.e., OpenLDAP or Windows).
Primary RADIUS	IP address of the Access Control Engine. Configure a primary and backup if you have more than one Access Control Engine.
Authenticate Locally for MAC	Must be *Disabled* for external captive portal on the NAC server.
Default Auth Role	Enterprise User This setting is a failsafe only. It is not used if the proper filter-ids are sent from the Access Control Engine.
Default VLAN	Bridged at AP Untagged Use your configured network ExtremeCloud Appliance topology for client access.

2 Click **Advanced** and enable **RADIUS Accounting**.

3 Save the network.

Editing the Configuration Profile for Network and Roles

Configure a network and be aware of policy roles that you are using before modifying the device group profile.

1 Go to **Sites** and select a site.

2 Click **Configure Site** > **Device Groups**.

3 Select your configured device group.

4 Select ✎ to edit the configuration profile.

5 From the Networks tab, assign a radio to the network you created.

6 From the Roles tab, select the appropriate roles that will be applied to the end system during connection/registration/authorization. Typically all roles are selected.

Note

Upon creating an External Captive Portal network, the rules engine created two engine rules that make use of the following policies:

- Enterprise User
- Unregistered

External Captive Portal networks use the Unregistered policy by default. We are going to modify this to explicitly configure end system traffic coming from the ExtremeCloud Appliance network to use a new NAC Profile and a new ExtremeCloud Appliance Unregistered policy that we will create.

7 Click **Save** to save the profile settings.

8 Click **Close** to close the device group.

ExtremeCloud Appliance Default Pass-Through Rule

Create a RADIUS Pass-Through rule on ExtremeCloud Appliance. This rule designates that traffic connecting to the ECA_Guest_NAC network will send and receive all RADIUS requests from the externally defined RADIUS server, not from the ExtremeCloud Appliance that processes the request. This includes filter-ids that are received as attributes. The NAC RADIUS server provides RADIUS authentication and authorization and policies that are defined in Extreme Management Center.

1 On ExtremeCloud Appliance, go to **Onboard** > **Rules** > **Add**.

2 Configure the following parameters:

Name	ECA Guest Rule
Rule Enabled	Check this option to enable the new rule.
Location	ECA_Guest_NAC (Use your network name)
Accept Policy	Pass-Thru External RADIUS

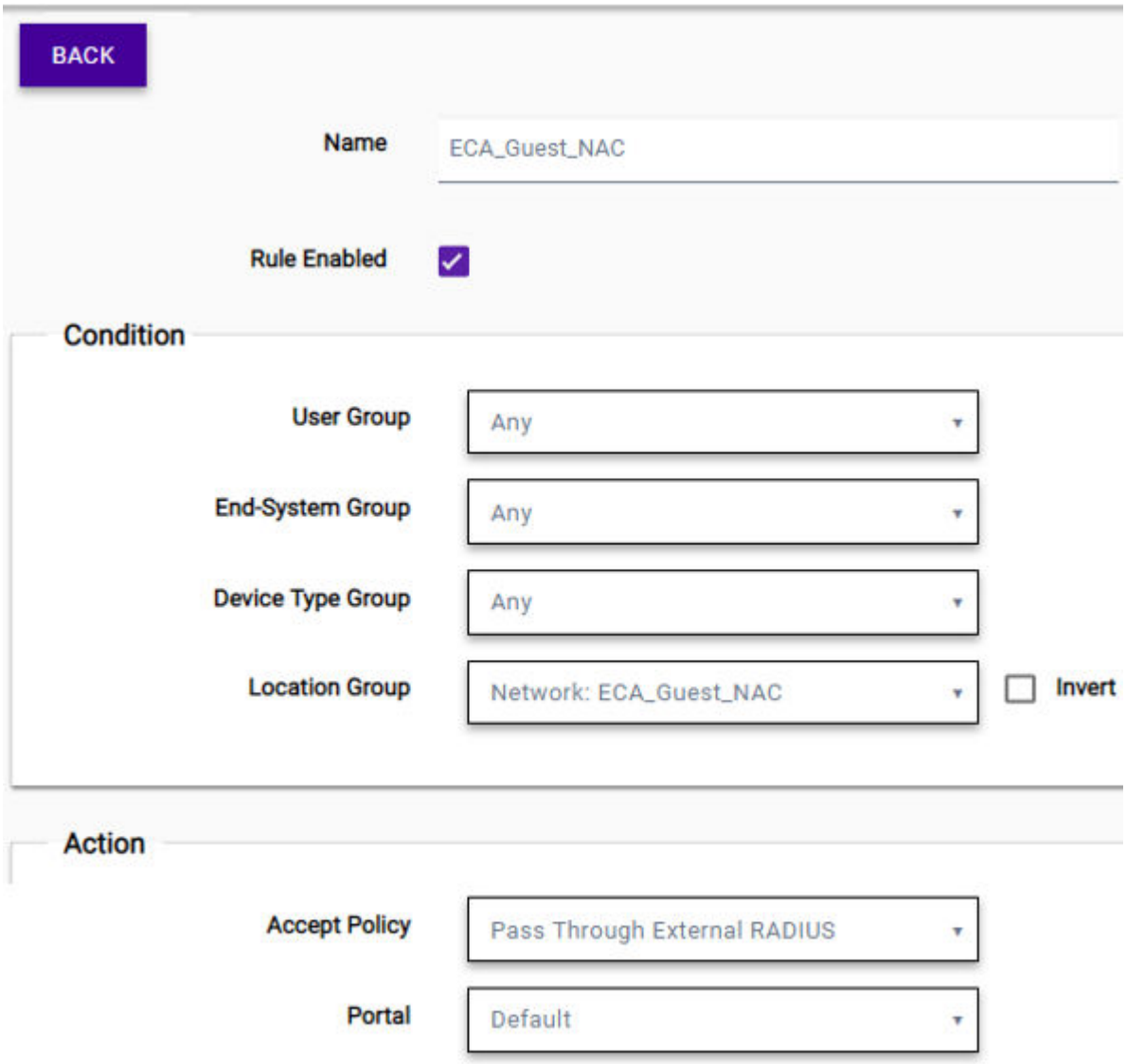


Figure 36: Add Rule Dialog

3 Click **Save**.

4 Move the rule to the top of the rule set, if it is not already there.

Adding external NAC as RADIUS in ExtremeCloud Appliance

1 From ExtremeCloud Appliance, go to **Admin** > **Accounts** > **RADIUS**.

2 Under RADIUS Servers, click **Add** to add the properties of the RADIUS server.

3 Select the RADIUS server row to add a server.

Provide the IP address of the External NAC as the External RADIUS server.

4 Click **Save**.

Adding ExtremeCloud Appliance as a Switch to Extreme Management Center

Use the web client to configure SNMPv2 and CLI credentials.

1 Configure SNMPv2 and CLI credentials using any GUI client via **Authorization** > **Device Access** , or in the **Administration** > **Profiles** section of the Extreme Management Center™ web client.

a Specify the **Community Name**.

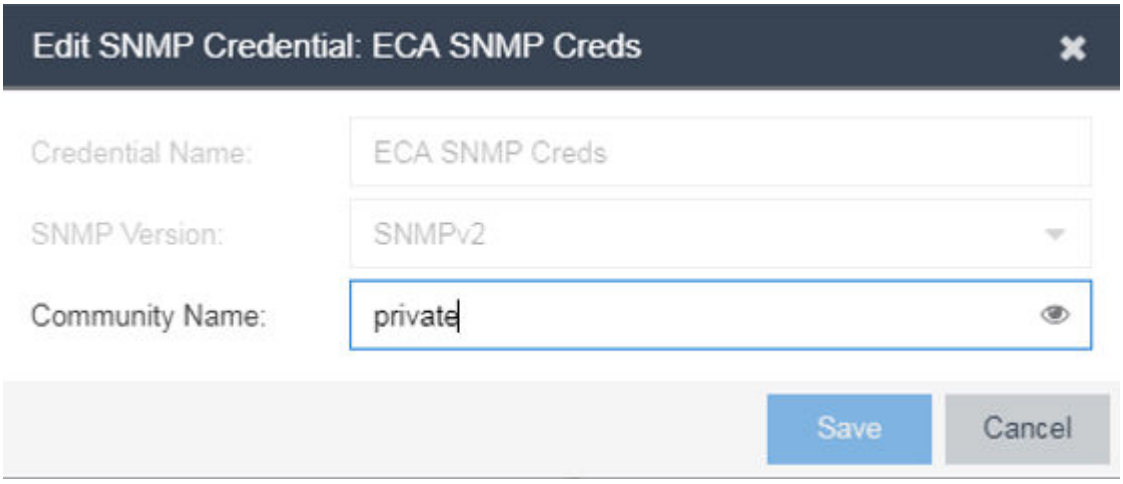


Figure 37: SNMPv2 Private Community

b Provide ExtremeCloud Appliance credentials.

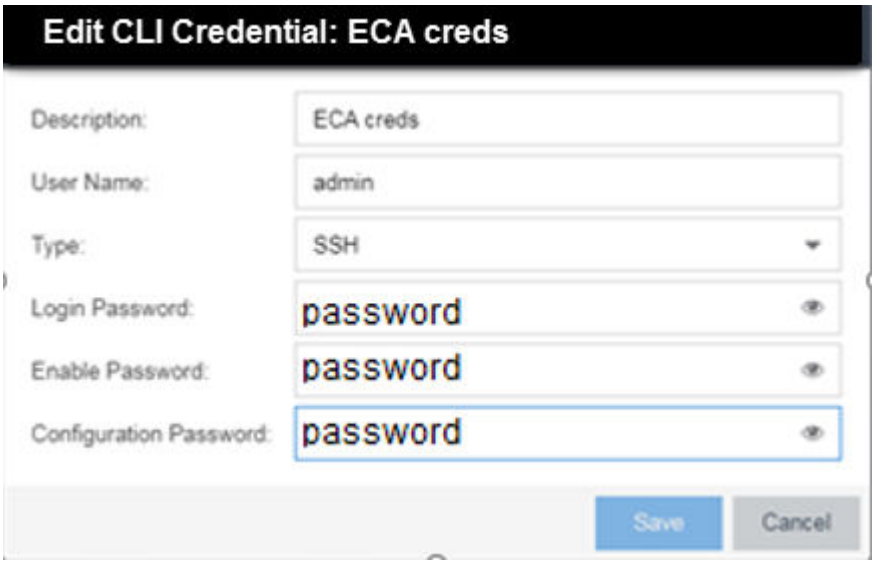


Figure 38: CLI Credentials: admin/admin password

c Create an ExtremeCloud Appliance SNMP profile, selecting the two credentials:

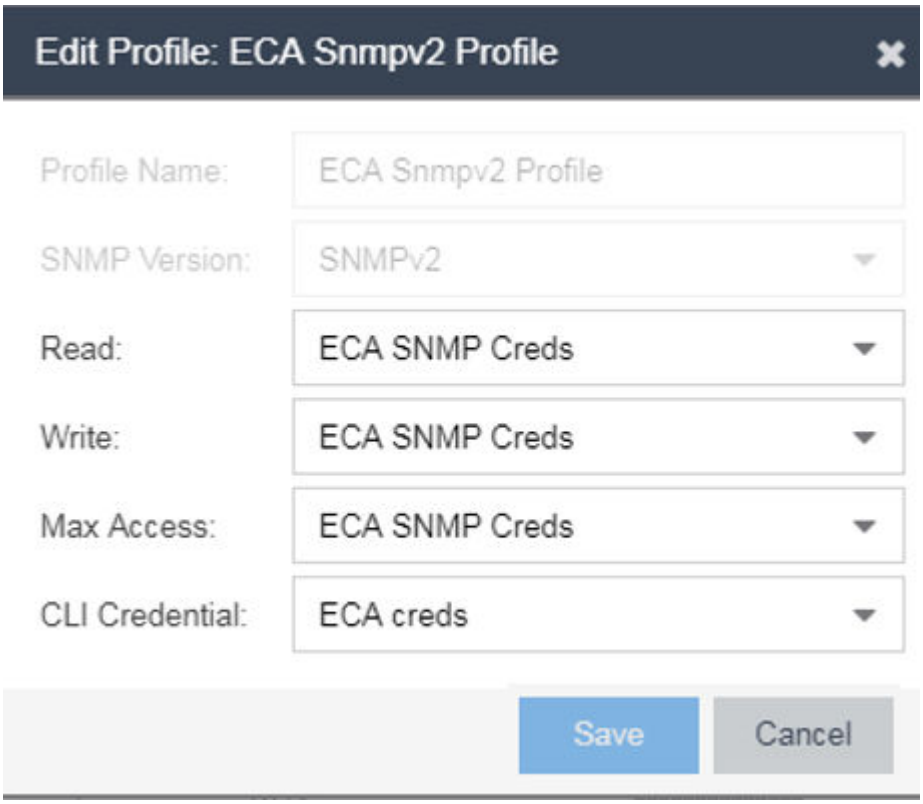


Figure 39: Snmpv2 Profile for ExtremeCloud Appliance

d Click **Save**.

Note
Both SNMPv2 and SNMPv3 are supported.

2 Add the switch to your Access Control Engine.

a From Extreme Management Center, go to **Control** > **Access Control** > **Switches**.

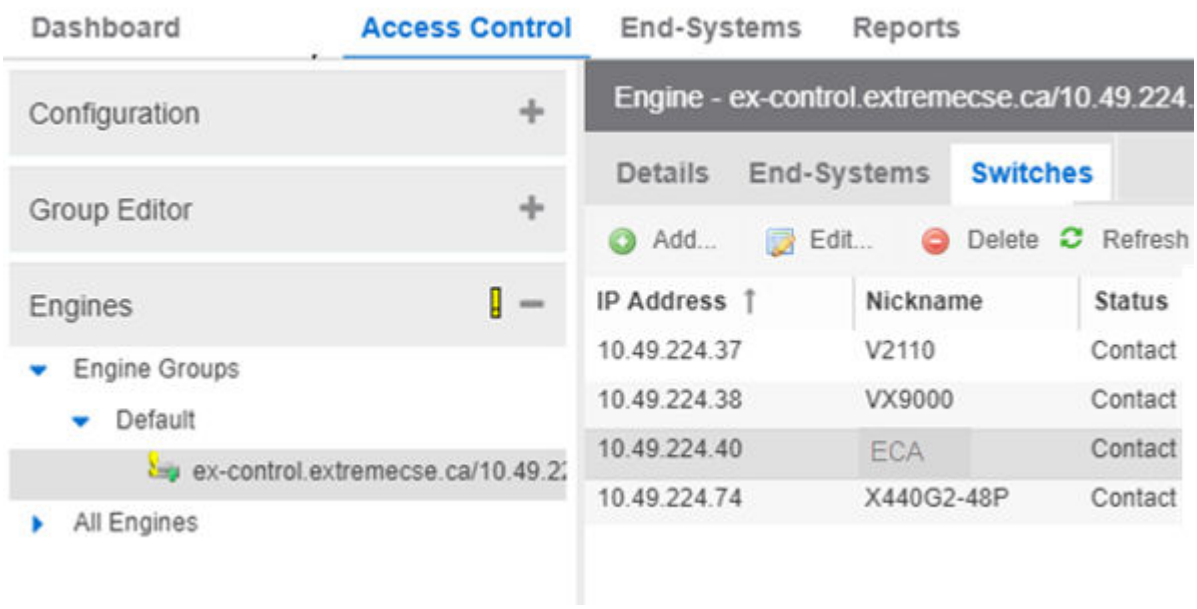


Figure 40: Access Control Switches tab

b Click **Add**.

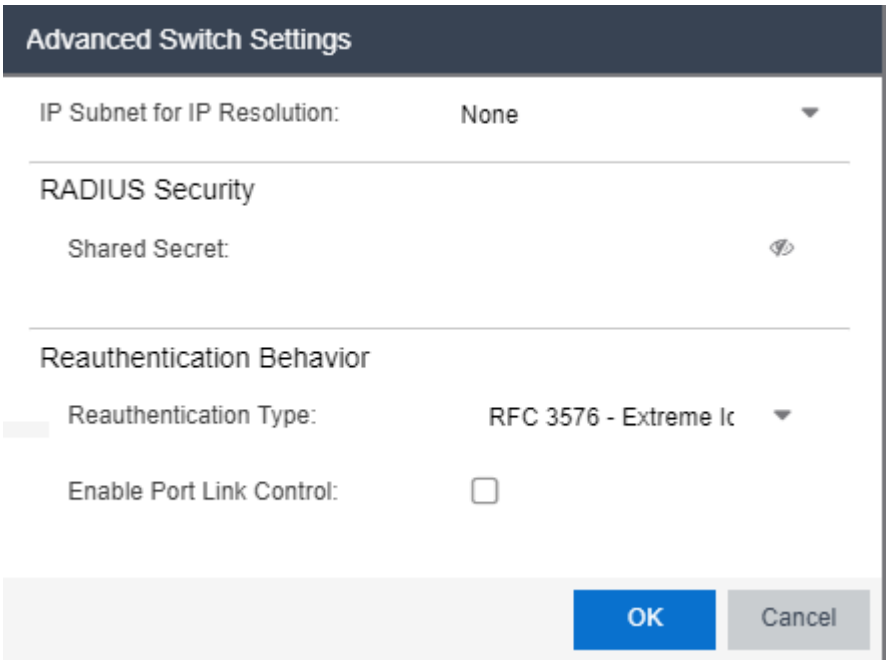
c Expand the tree and navigate to the ECA device.

d Configure the following parameters:

Switch Type	Layer 2 Out-Of-Band
Primary Engine	Select the Access Control Engine that you set as the RADIUS server for the network on the ExtremeCloud Appliance.
Secondary Engine	Optional if appropriate for your configuration.
Edit Auth Access Type	Manual RADIUS Configuration
RADIUS Attributes to Send	Extreme Identifi Wireless

e Click **Advanced settings**.

f Under **Reauthentication Behavior**, select the **Reauthentication Type** value **RFC3576 Extreme identifi Wireless**.



g Click **OK** and then click **Save**.

Creating an Unregistered Policy on Extreme Management Center

Create an unregistered policy on the Extreme Management Center web console. Policy creation is not available in NAC Manager.

1 Go to the Extreme Management Center web client and select **Access Control** > **Policy**.

If you have imported policy domains in your NAC configuration, select the domain your configuration uses. If you have not imported a domain policy configuration, select the Default Policy Domain.

2 Go to **Open Domain** > **Open** > **Manage Domains**.

3 Expand the **Roles** tree.

4 Right-click the **Unregistered** policy and select **Copy**.

5 Go to **Roles** and select **Paste** from the right-click menu.

A new Unregistered policy is pasted into the tree.

6 Rename the new policy to **Unregistered role for ECA_Guest**.

Use *Unregistered role for <network name>* as the name of the policy if not using *ECA_Guest* as your network name.

Note

The role *must* be named *Unregistered role for <NETWORK NAME>*. Use the *Name* of the network and not the SSID of the network. The name must match all characters and spaces exactly.

7 Go to **Open** > **Manage Domain** and select **Save Domain**.

Saving the role automatically creates a profile for this role under the **Access Control** > **Profiles** menu.

Creating a Location-Based, Unregistered Profile and Policy Mapping to the ExtremeCloud Appliance Pass-Through Network

To create a profile and map it to the ExtremeCloud Appliance pass-through network, take the following steps:

1 From the Extreme Management Center web interface, go to **Control** > **Access Control** > **Group Editor** > **Location Group** and click **Add**.

2 Configure the following parameters:

Switches	Select **List** and specify the ExtremeCloud Appliance IP address.
Interface	Wireless

3 Click **Update** and then click **Save**.

4 Go to **Access Control** > **Configuration** > **Profiles**.

5 Select **Policy Mappings** > **Default**.

6 Click **Switch to Advanced**.

7 Find the Unregistered role that was previously created for ExtremeCloud Appliance and click **Edit**.

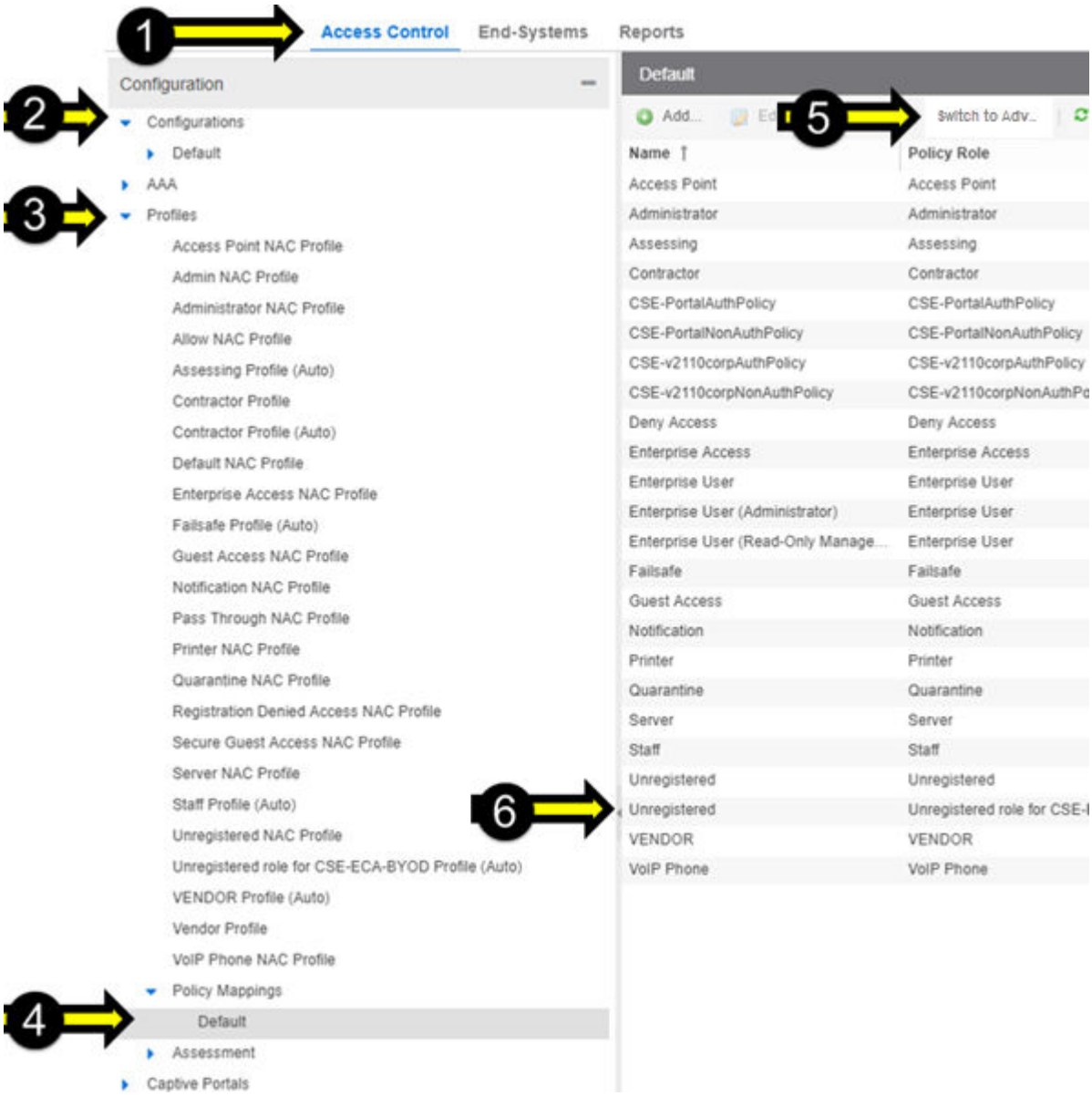


Figure 41: Extreme Management Center Access Control Profiles

8 Modify the **Map to Location** option. Provide the previously created ExtremeCloud Appliance location and click **Save**.

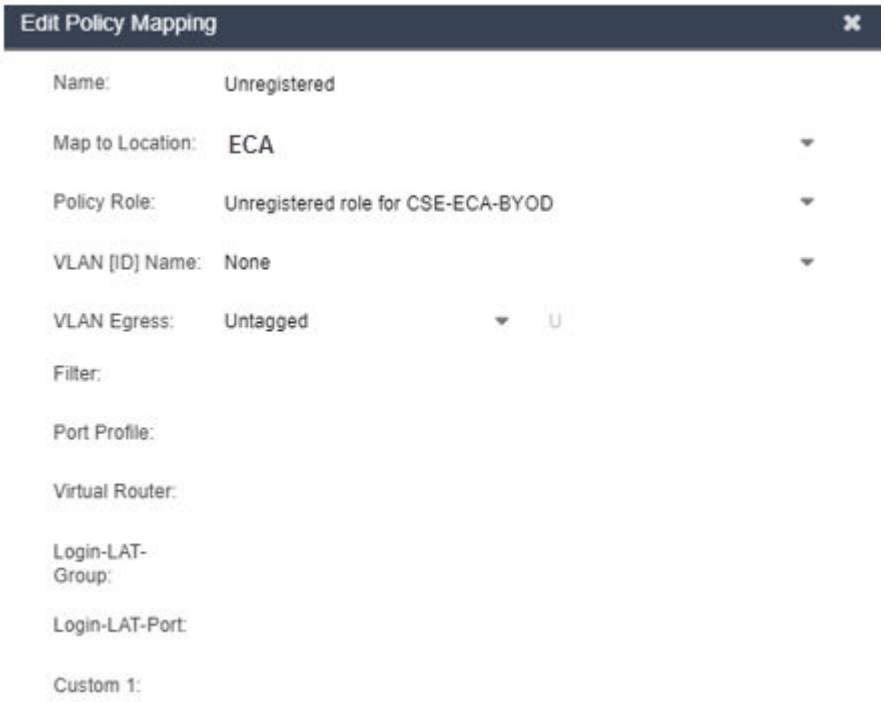


Figure 42: Extreme Management Center Edit Policy Mapping

9 Enforce the NAC engine for the configuration to take effect.

Note

Policies/filter-ids sent from NAC to the ExtremeCloud Appliance must exist under ExtremeCloud Appliance roles . If ExtremeCloud Appliance cannot correlate a filter-id to an existing policy in its own Roles database, the default authenticated roles are applied.

If you see a mismatch in roles between NAC and ExtremeCloud Appliance, force a reauthentication from ExtremeCloud Appliance. This will determine if it is a timing issue. (See **Session timeouts** on the network configuration.)

If the roles still do not match between NAC and ExtremeCloud Appliance, verify that the roles are configured based on the network name (not SSID) and that the syntax and all characters in the roles match. For more information, see Creating an Unregistered Policy on Extreme Management Center on page 81.

8 Deploying an Availability Pair

Deploying an Availability Pair

ExtremeCloud Appliance provides the availability feature to maintain service availability in the event of an outage. The Availability Pair feature allows both AP and Client statistics to be available on both sides of the High Availability configuration.

Before you begin:

1 Enable NTP on both ExtremeCloud Appliance appliances. Go to **Admin** > **System** > **Network Time** and select **NTP**.

2 On the primary ExtremeCloud Appliance, go to **Admin** > **System** > **Availability** and select **Paired**.

3 Configure the following parameters:

Role	Primary
Peer IP Address	The data port IP address of the second ExtremeCloud Appliance.
Auto AP Balancing	Select **Active - Passive** In a Availability Pair, an AP establishes an active tunnel to one appliance and a backup tunnel to the other appliance. The active tunnel is used to pass the client data over tunneled topologies. • In an **Active-Active** configuration, approximately half of the APs establish an active tunnel to the primary appliance. The remaining APs establish an active tunnel to the backup appliance, spreading the load across the Availability Pair. • In an **Active-Passive** configuration, all APs establish an active tunnel to the primary appliance. The secondary appliance is used for failover only. In either configuration, however, most parameters can be configured on either appliance in the availability pair.

4 Click **Save**.

5 On the secondary ExtremeCloud Appliance, select **Paired** and configure the following parameters:

Role	Backup
Pair IP Address	The IP address of the primary ExtremeCloud Appliance.
Auto AP Balancing	Select **Active-Passive**

6 Click **Save**.

7 Go to **Admin** > **Logs** and look for the message `Availability Link established with Peer <ip address>.`

Note
It will take a few minutes for the two ExtremeCloud Appliance configurations to synchronize.

8 To verify synchronization, add a network health widget to the Overview dashboard.

a Go to **Overview**.

b Click to edit the dashboard.

c Select **Widgets**.

d Select **System** and drag **Network Health** onto the dashboard.

The **Synchronization Status** is displayed as part of the Network Health widget.

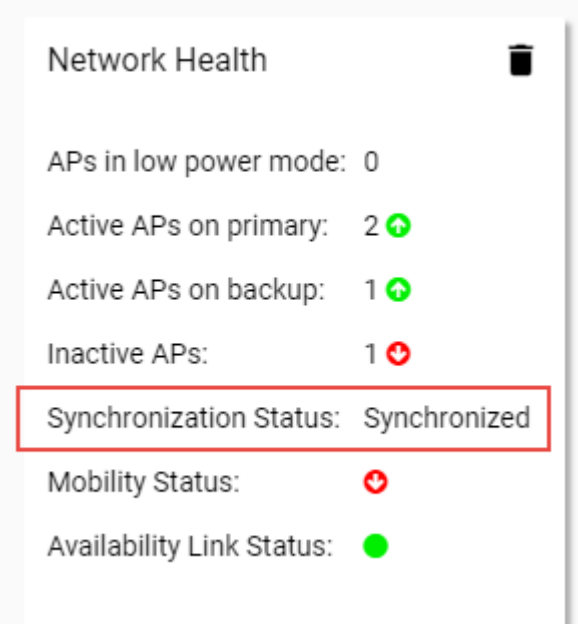


Figure 43: Availability Pair Synchronization Status

9 ExtremeCloud Appliance Pair with ExtremeLocation and AirDefense

Scenario Outline

The following scenario outlines an availability pair of ExtremeCloud Appliance appliances that utilize both ExtremeWireless and ExtremeWireless WiNG access point models. This scenario supports integration with ExtremeLocation and AirDefense products.

This deployment scenario offers the following configuration factors:

- Availability pair of ExtremeCloud Appliance appliances.
- Appliance capacity 32K-100K users
- Local authentication with 802.1x and internal captive portal.
- Both ExtremeWireless and ExtremeWireless WiNG APs are supported.
- ExtremeLocation is provisioned from within ExtremeCloud Appliance and the data is fed from the APs.
- AirDefense is provisioned from within ExtremeCloud Appliance and the data is fed from the APs.

Deployment Strategy

1. Create two sites: A Centralized site with a device group for the AP3915 devices, and a Distributed site with a device group for the AP7632 devices.
2. Configure an internal captive portal.
3. Specify the network topology.
4. Configure a captive portal network.
5. Work with the captive portal engine rules.
6. Go back to each device group in the site and configure the configuration profile.
7. Create adoption rules for each device group.
8. Deploy the availability pair.

Related Links

Adding a Centralized Site with Device Group on page 47
Adding a Distributed Site on page 59

Configuring an Internal Captive Portal on page 49
Specifying B@AC Network Topology on page 49
Configuring a Captive Portal Network on page 50
Working with Internal Captive Portal Engine Rules on page 51
Configuring the Centralized Site with an AP3915 Profile on page 88
Configuring the Distributed Site and AP7632 Profile on page 88
Creating Adoption Rules on page 53
Deploying an Availability Pair on page 85

Configuring the Centralized Site with an AP3915 Profile

1. Go to **Sites** > **Add** to create a Centralized site.
2. Click **Configure Site** > **Device Groups**
3. Select the AP3915 device group.
4. From the Profile field, select the **default AP3915** profile and click to edit the profile.
5. From the Networks tab, select the configured Internal Captive Portal network.
6. From the Roles tab, select the configured policy roles.
7. From the ExtremeLocation tab, configure ExtremeLocation integration.
8. From the AirDefense tab, configure AirDefense integration.

Related Links

Adding a Centralized Site with Device Group on page 47
Editing Device Group Profile for Network and Role on page 51
Configuring ExtremeLocation on page 89
Configuring AirDefense on page 89

Configuring the Distributed Site and AP7632 Profile

1. Go to **Sites** > **Add** to create a Distributed site.
2. Click **Configure Site** > **Device Groups**
3. Select the AP7632 device group.
4. From the Profile field, select the **default AP7632** profile and click to edit the profile.
5. From the Networks tab, select the configured Internal Captive Portal network.
6. From the Roles tab, select the configured policy roles.
7. From the ExtremeLocation tab, configure ExtremeLocation parameters.
8. From the AirDefense tab configure AirDefense parameters.

Related Links

Adding a Distributed Site on page 59
Editing Device Group Profile for Network and Role on page 51
Configuring ExtremeLocation on page 89
Configuring AirDefense on page 89

Configuring ExtremeLocation

Configure the following parameters to integrate the AP with ExtremeLocation.

Table 4: ExtremeLocation Profile Settings

Field	Description
Name	Name of the ExtremeLocation Profile.
Tenant ID	The Tenant ID links the ExtremeCloud Appliance to the tenant, ensuring that your assets cannot inadvertently be deployed on sites that belong to other ExtremeLocation accounts. Any modification made to sites managed by this ExtremeCloud Appliance, such as adding new access points or sites, is tagged by the ExtremeLocation Tenant Account Number automatically. The location Tenant ID is saved to, and retrieved from, the data plane by websocket client, then sent as session data to the ExtremeLocation server once a session is established. The Tenant ID can be up to 32 characters.
Server Address	The FQDN (fully-qualified domain name) of the LocationEngine Server.
Minimum RSS	RSS threshold for reporting location data. Valid values are -90 to -70 dBm.
Report Frequency	Reporting interval in seconds.

Configuring AirDefense

The AP integrates with the AirDefense Service Platform (ADSP), offering an additional profile option that allows the AP to function as an AirDefense sensor or to act as a sensor and retain the ability to forward traffic.

In dedicated sensor mode, the AP operates independently from the ExtremeCloud Appliance while the ExtremeCloud Appliance continues to see the AP and display the AP Role as a dedicated AirDefense sensor. In its role as a dedicated sensor, the AP does not report statistics to the ExtremeCloud Appliance.

Table 5: AirDefense Profile Settings

Field	Description
Name	Name of AirDefense profile.
Add Server IP Address	The IP address of the AirDefense servers. Provide the FQDN or IPv4 string, maximum 255 characters. Enter the IP address, then click ⊕. The IP address is added to the **Server IP Addresses** list.
Server IP Addresses	List of IP addresses for servers. Click 🗑 to remove an IP address from the list.

10 ECP Local Authentication

Scenario Outline

The following scenario outlines an availability pair of ExtremeCloud Appliance appliances with both ExtremeWireless and ExtremeWireless WiNG access point models. This scenario employs an External Captive Portal.

This deployment scenario offers the following configuration factors:

- Availability pair of ExtremeCloud Appliance appliances.
- Appliance capacity 32K-100K users
- MBA with local authentication and External Captive Portal.
- Both ExtremeWireless and ExtremeWireless WiNG APs are supported.

Related Links

Deployment Strategy on page 90
Configuring External Captive Portal Network on page 91

Deployment Strategy

1. Create two sites: A Centralized site with a device group for the AP3915 devices, and a Distributed site with a device group for the AP7632 devices.
2. Configure an External Captive Portal.
3. Specify the network topology.

   Specify **Bridged@AP**. ExtremeWireless APs support both Bridged@AC and Bridged@AP topologies. ExtremeWireless WiNG APs support Bridged@AP only.
4. Configure an External Captive Portal network.
5. Engine Rules: The ExtremeCloud Appliance rules engine generates a default Unauthenticated rule. There is no user interaction required on the ExtremeCloud Appliance. An authenticated rule is generated from the External Captive Portal server. You must define a policy role on ExtremeCloud Appliance that matches the authenticated role on the server. This can be a unique role or default authenticated role like Enterprise User.
6. Go back to each device group and configure the configuration profile. Specify the External Captive Portal network and the ExtremeCloud Appliance authenticated role that matches the ECP server authenticated policy.
7. Create adoption rules for each device group.

8 Deploy the availability pair.

Related Links

Adding a Centralized Site with Device Group on page 47
Adding a Distributed Site on page 59
Specifying B@AP Network Topology on page 60
Configuring External Captive Portal Network on page 91
Creating Adoption Rules on page 53
Deploying an Availability Pair on page 85

Configuring External Captive Portal Network

To configure an External Captive Portal network:

1 Go to **Networks** > **Add**
2 Configure the following parameters:

Table 6: External Captive Portal Settings

Field	Description
Network Name	Enter a unique, user-friendly value that makes sense for your business. Example: Staff
SSID	Enter a character string to identify the wireless network. Must be a maximum of 32 characters. Upper and lowercase allowed. Example: PermanentStaff
Status	Enable or disable the network service. Disabling the network service shuts off the service but does not delete it.

Table 6: External Captive Portal Settings (continued)

Field	Description
Auth Type	Define the authorization type. Valid values are: • Open. Anyone is authorized to use the network. This authorization type has no encryption. The Default Unauth role is the only supported policy role. • WPAv2 with PSK Network access is allowed to any client that knows the pre-shared key (PSK). All data between the client and the AP is AES encrypted using the shared secret. Privacy is based on the IEEE standard, and privacy settings are editable. If MAC-based authentication (MBA) is enabled, you can assign different roles to different devices with a PSK because MBA distinguishes between different devices. If MBA is not enabled, then devices with a PSK use the Default Unauth role only. Privacy Settings: • Protected Management Frames — Management Frames are the signaling packets used in the 802.11 wireless standard to allow a device to negotiate with an AP. PMF adds an integrity check to control packets being sent between the client and the access point. This setting is enabled by default. Valid values are: Enabled. Supports PMF format but does not require it. Disabled. Does not address PMF format. Clients connect regardless of format. Required. Requires all devices use PMF format. This could result in older devices not connecting. • WPA2 key • WPA2 Enterprise w/ RADIUS Supports 802.1x authentication with a RADIUS server, using AES encryption. This is the highest level of network security, particularly when used in conjunction with client certificate-based authentication (EAP-TLS). All 802.1x protocols are supported. Note: MBA and Captive Portal are not supported when using WPA2 Enterprise w/ RADIUS. Privacy Settings: • Protected Management Frames — Management Frames are the signaling packets used in the 802.11 wireless standard to allow a device to negotiate with an AP. PMF adds an integrity check to control packets being sent between the client and the access point. This setting is enabled by default. Valid values are: Enabled. Supports PMF format but does not require it. Disabled. Does not address PMF format. Clients connect regardless of format. Required. Requires all devices use PMF format. This could result in older devices not connecting. • Fast Transition — Provides faster roaming by authenticating the device before roaming occurs. This setting is enabled by default.

Table 6: External Captive Portal Settings (continued)

Field	Description
Enable Captive Portal	Check this option to enable captive portal support on the network service.
Captive Portal Type	Select **External** as the Captive Portal Type.
ECP URL	URL address for the external captive portal.
Walled Garden Rules	Click **Walled Garden Rules** to configure policy rules for the external captive portal.
Identity	Determines the name common to both the ExtremeCloud Appliance and the external Web server if you want to encrypt the information passed between the ExtremeCloud Appliance and the external Web server. Required for signing the redirected URL. If you do not configure the Identity, the redirector on the AP drops the traffic.
Shared Secret	The password that is used to validate the connection between the client and the RADIUS server.
Use HTTPS for connection	Indicates that the connection will be secure with HTTPS.
Send Successful Login To	Indicates destination of authenticated user. Valid values are: • Original Destination. The destination of the original request. • Custom URL. Provide the URL address.
MAC-based authentication (MBA)	Check this option to enable MBA.

3 Click **Save**.

Next, edit the configuration profiles in each device group, specifying the External Captive Portal network.

Related Links

Editing the Device Group Profile for ECP Network on page 93

Editing the Device Group Profile for ECP Network

Configure an ECP network and be aware of the authenticated policy role that you are using before modifying the device group profile.

1 Go to **Sites** and select a site.
2 Click **Configure Site** > **Device Groups**.
3 Select a device group.
4 Select ✎ to edit the default profile AP3915-default.
5 From the Networks tab, assign a radio to the ECP network you created.
6 External Captive Portal networks use the Unregistered policy by default, there is no user interaction. The authenticated policy is configured on the captive portal server. You must specify an authenticated policy on the ExtremeCloud Appliance that will coincide with the authenticated captive portal server policy. For example, from the **Roles** tab, specify **Enterprise User** as the ExtremeCloud Appliance authenticated policy.

7 Optionally, you can configure settings from any of the available profile options. All APs in the device group are affected by options configured in the profile.

Note
The supported profile options depend on the AP Platform definition.

8 Click **Save** to save the profile settings.

9 Click **Close** to close the device group.

Next, configure adoption rules and deploy an availability pair of appliances.

Related Links

Creating Adoption Rules on page 53
Deploying an Availability Pair on page 85

Glossary

Chalet

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

CLI

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

Data Center Connect

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

Extreme Application Analytics

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

Extreme Management Center

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

ExtremeCloud Appliance

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

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

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

ExtremeCloud

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

ExtremeControl

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

ExtremeSwitching

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

ExtremeWireless

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

ExtremeXOS

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

Index

U