ExtremeCloud Appliance Deployment Guide

Version 4.76.04

9036571-03 Rev AC
October 2020

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

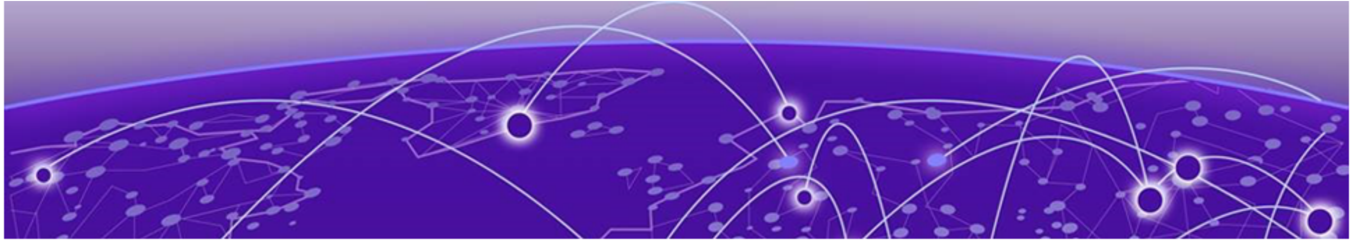
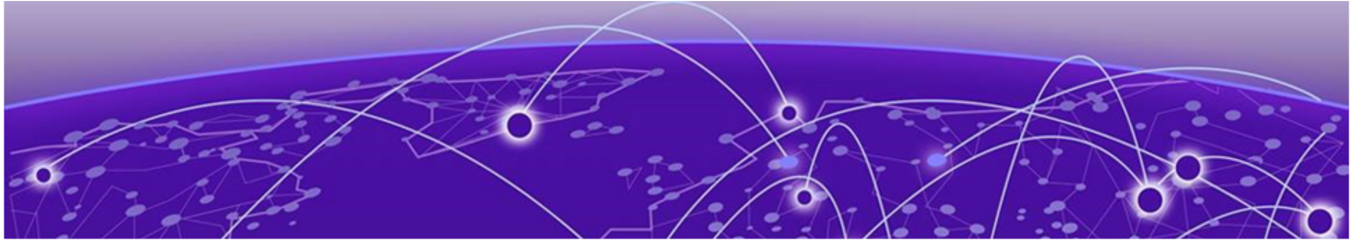


Table of Contents



Preface

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

Conventions

This section discusses the conventions used in this guide.

Text Conventions

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

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

Table 1: Notes and warnings

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

Table 1: Notes and warnings (continued)

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

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it appears on the screen.
The words *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 in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
Words in 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.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

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

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes
Hardware/software compatibility matrices for Campus and Edge products
Supported transceivers and cables for Data Center products
Other resources, like white papers, data sheets, and case studies

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

Providing Feedback

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

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

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

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

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

Getting Help

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

Extreme Portal

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

The Hub

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

Call GTAC

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

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

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

Subscribe to Service Notifications

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

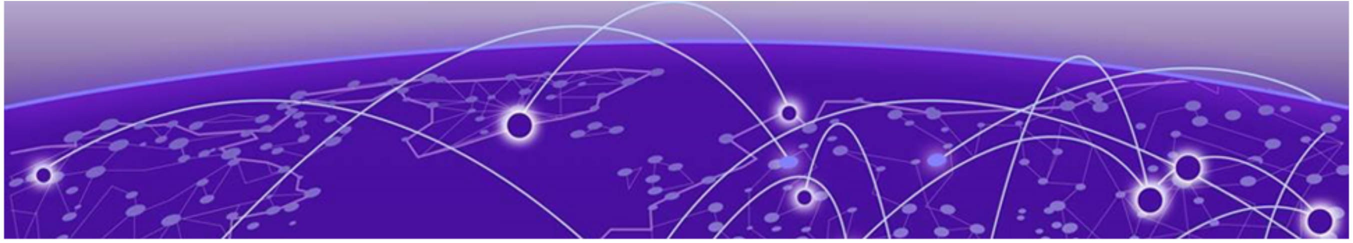
1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form (all fields are required).
3. Select the products for which you would like to receive notifications.

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

4. Select **Submit**.

AP Regulatory Information

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



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.

VE6120H Virtual Appliance

ExtremeCloud Appliance offers a new platform model. The VE6120H for Microsoft Hyper-V offers elasticity with support for small, medium, and large deployments:

- Uses the same licensing procedure as the VE6120.
- Is entitled per the 30324/30326 activation keys.

- Accepts the same capacity keys as the hardware model E2120.
- Supported on Windows Server 16 (minimal support). The lowest supported VMBUS is version 3.0.

> Note
> VE6120H, VE6120, and VE6125 use separate .ova files. You cannot upgrade from one VM model to another.
>
> **Virtual Machine Upgrade File Formats:**
>
> - VE6120 — .dle
> - VE6120H — .spe
> - VE6125 — .rse

Requirements for the ExtremeCloud Appliance VE6120H model are listed in Supported Appliance Specifications on page 12.

For installation information, see *VE6120H Virtual Appliance Installation Guide Microsoft Hyper-V Platform* at https://extremenetworks.com/documentation/extremecloud-appliance.

Related Topics

Supported Appliance Specifications on page 12

VE6125 Virtual Appliance

ExtremeCloud Appliance offers a new platform model. The VE6125 targets extra large deployments of up to 4000 access points. The larger capacity offers support for customers wanting to manage a large deployment from a virtual installation. The new VE6125 X-Large configuration provides capacity parity with the E2120. Customers with large installations of up to 4000 APs have the option to manage their infrastructure via a pair of hardware appliances, the E2120 or in virtual configuration options, the VE6125:

- Requires a VMWare Enterprise license.
- Uses the same licensing procedure as the VE6120.
- Is entitled per the 30324/30326 activation keys.
- Accepts the same capacity keys as the hardware model E2120.

> Note
> VE6120H, VE6120, and VE6125 use separate .ova files. You cannot upgrade from one VM model to another.
>
> **Virtual Machine Upgrade File Formats:**
>
> - VE6120 — .dle
> - VE6120H — .spe
> - VE6125 — .rse

Requirements for the ExtremeCloud Appliance VE6125 model are listed in Supported Appliance Specifications on page 12.

For installation information, see *VE6120/VE6125 Virtual Appliances Installation Guide VMware® Platform* at https://extremenetworks.com/documentation/extremecloud-appliance.

Related Topics

Supported Appliance Specifications on page 12

Supported Appliance Specifications

ExtremeCloud Appliance supports the following virtual appliances:

- VE6120
- VE6120H for Microsoft Hyper-V
- VE6125

And the following hardware appliances:

- E1120
- E2120
- E3120

Requirements for each ExtremeCloud Appliance model are listed below.

Table 4: Virtual ExtremeCloud Appliances (VE6120 and VE6125)

Extreme Application	VE6120			VE6125
	Small	**Medium**	**Large**	**X-Large**
Total APs managed in Standalone mode	50	250	500	2000
Additional APs supported in high-availability mode	50	250	500	2000
Total managed APs per Appliance Pair	100	500	1000	4000
Total Switches managed per Appliance	50/100	100/200	200/400	200/400
Total simultaneous users in Standalone mode	1,000	4,000	8,000	16000
Additional simultaneous users in high-availability mode	1,000	4,000	8,000	16000
Total Simultaneous Users per Appliance Pair	2,000	8,000	16,000	32000
Hardware Requirements				
CPU	4 (4 distinct physical cores or 2 cores with hyper-threading)	6	8	32 (physical or hyper-threading cores)
RAM (GB)	8	16	24	32
Hard Disk (GB)	80	80	80	512

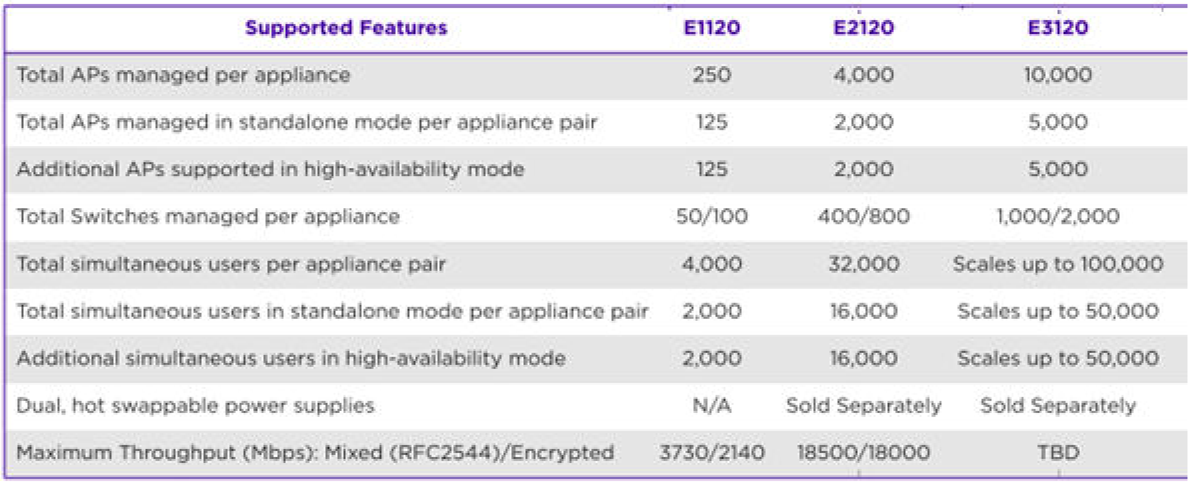
Table 4: Virtual ExtremeCloud Appliances (VE6120 and VE6125) (continued)

Extreme Application	VE6120			VE6125
2x1Gbps Host (Open/Secure Mbps)	1,870/1,870	1,870/1,870	1,870/1,870	
2x10 Gbps Host (Open/Secure Mbps)	10,800/5,100	10,800/5,100	10,800/5,100	

- 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. VE6120 supports VMware ESXi 5.1 or higher. VE6125 supports VMware ESXi 5.5 or higher.
- A VMware Enterprise license is required for the VE6125.

Table 5: Virtual ExtremeCloud Appliances VE6120H

Extreme Application	VE6120H		
	Small	**Medium**	**Large**
Total APs managed in Standalone mode	50	250	500
Additional APs supported in high-availability mode	50	250	500
Total managed APs per Appliance Pair	100	500	1000
Total Switches managed per Appliance	50/100	100/200	200/400
Total simultaneous users in Standalone mode	1,000	4,000	8,000
Additional simultaneous users in high-availability mode	1,000	4,000	8,000
Total Simultaneous Users per Appliance Pair	2,000	8,000	16,000
Hardware Requirements			
CPU	4 (4 distinct physical cores or 2 cores with hyper-threading)	6	8
RAM (GB)	8	16	24
Hard Disk (GB)	80	80	80



Supported Features	E1120	E2120	E3120
Total APs managed per appliance	250	4,000	10,000
Total APs managed in standalone mode per appliance pair	125	2,000	5,000
Additional APs supported in high-availability mode	125	2,000	5,000
Total Switches managed per appliance	50/100	400/800	1,000/2,000
Total simultaneous users per appliance pair	4,000	32,000	Scales up to 100,000
Total simultaneous users in standalone mode per appliance pair	2,000	16,000	Scales up to 50,000
Additional simultaneous users in high-availability mode	2,000	16,000	Scales up to 50,000
Dual, hot swappable power supplies	N/A	Sold Separately	Sold Separately
Maximum Throughput (Mbps): Mixed (RFC2544)/Encrypted	3730/2140	18500/18000	TBD

Figure 1: ExtremeCloud Appliance Hardware

Related Topics

VE6120H Virtual Appliance on page 10

VE6125 Virtual Appliance on page 11

Discovery and Registration

Wireless devices (APs and SA201 adapters) discover the IP address of ExtremeCloud Appliance 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.

Discovery Process for APs and Adapters in a Centralized Site

Note

The following process outlines device discovery and registration for AP39xx, AP4xx, and AP5xx access points, and SA201 adapters, in a Centralized site.

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.

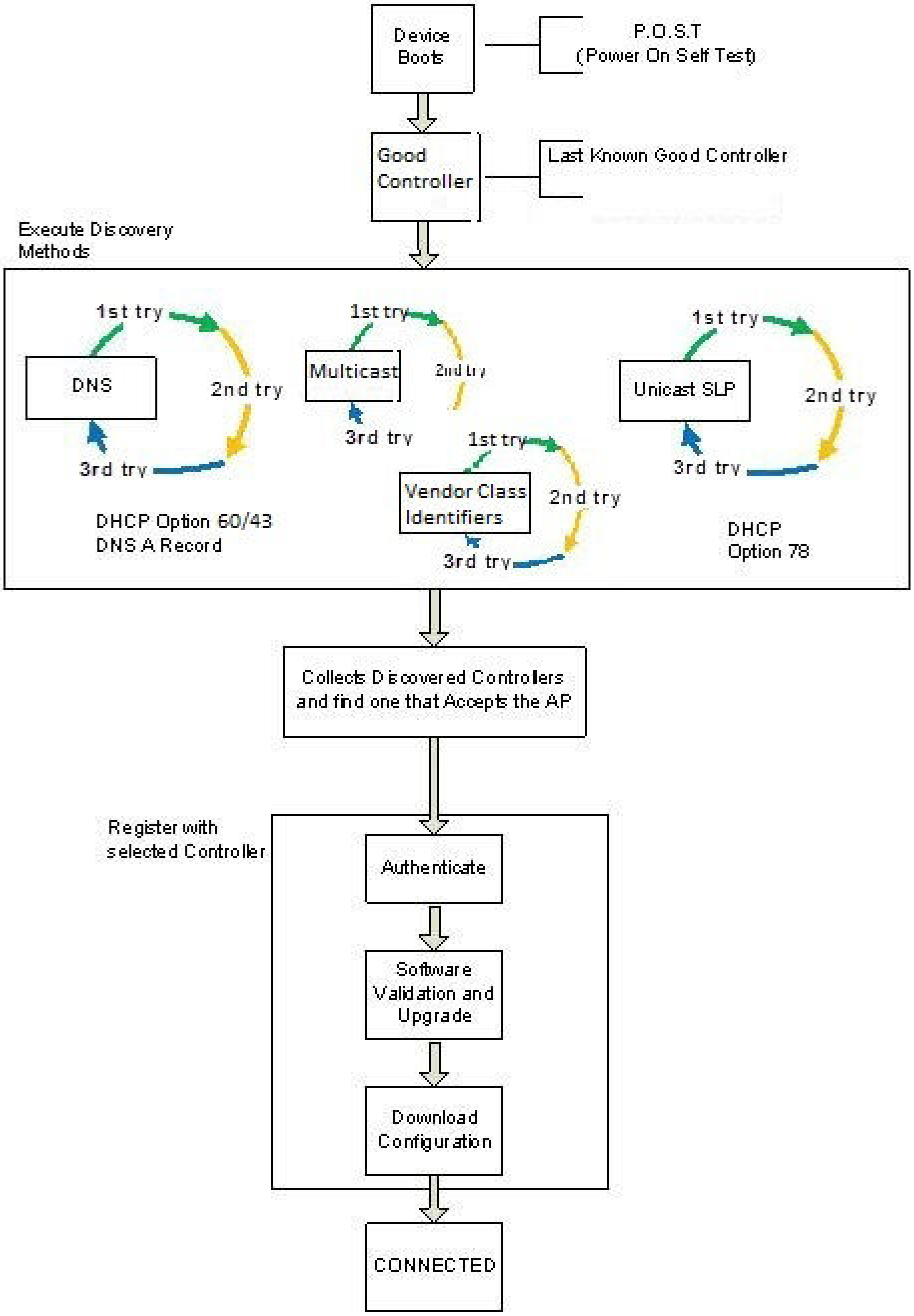

Device Boots
P.O.S.T (Power On Self Test)
Good Controller
Last Known Good Controller
Execute Discovery Methods
1st try
2nd try
3rd try
DNS
DHCP Option 60/43
DNS A Record
Multicast
Vendor Class Identifiers
Unicast SLP
DHCP Option 78
Collects Discovered Controllers and find one that Accepts the AP
Register with selected Controller
Authenticate
Software Validation and Upgrade
Download Configuration
CONNECTED

Figure 2: Discovery Process for devices in a Centralized site

Discovering Centralized Site APs and Adapters

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

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

1. 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 model. Also, configure the DHCP server with the IP addresses of the controllers.
2. 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.
3. 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.
4. 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.

Discovery Process for WiNG APs in a Distributed Site

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.

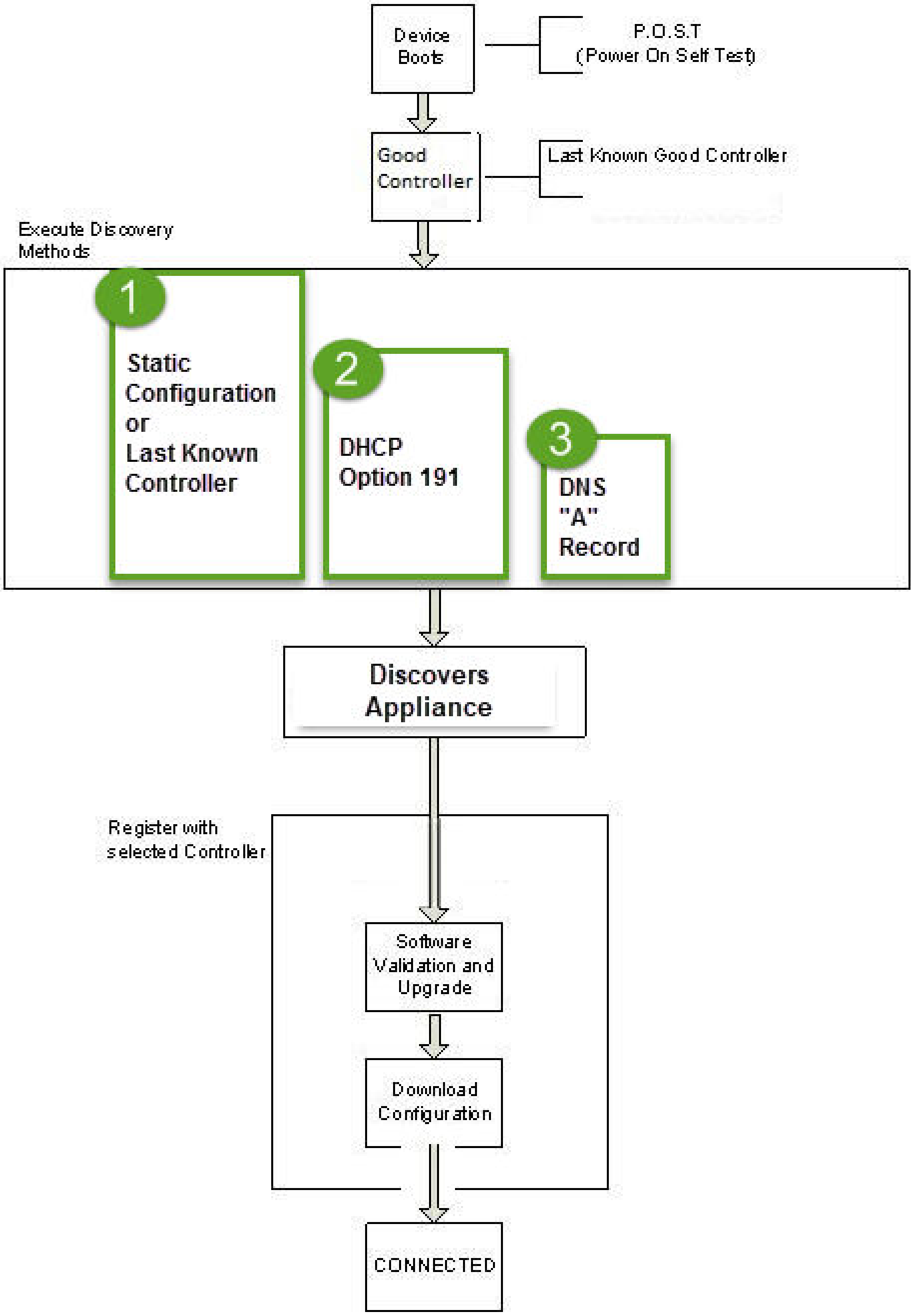

Device Boots
P.O.S.T (Power On Self Test)
Good Controller
Last Known Good Controller
Execute Discovery Methods
1
Static Configuration or Last Known Controller
2
DHCP Option 191
3
DNS "A" Record
Discovers Appliance
Register with selected Controller
Software Validation and Upgrade
Download Configuration
CONNECTED

Figure 3: Discovery Process for WiNG APs in a Distributed Site

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.

802.11ax AP Operational Modes

Prior to deploying your APs to an ExtremeCloud Appliance, know your network site type: Centralized or Distributed. Deploy AP models that are supported by the site. AP39xx, AP4xx, and AP5xx are supported on a Centralized site. AP8xx, AP7xx, and AP5xx are supported on a Distributed site.

The AP5xx access points are supported on either a Distributed or Centralized site. The AP operates in a single mode, which is determined at discovery. If you deploy the AP5xx in a network with a Distributed site, it will assume the Distributed AP mode. If you deploy the AP in a network with a Centralized site, it will assume the Centralized AP mode. Moving the 802.11ax APs between sites of different types from ExtremeCloud Appliance is supported. The AP assumes the operational mode of its assigned site, provided that you have configured the necessary DHCP options.

You can assign APs manually from the AP list. Select APs of the same model type, then from the **AP Actions** button, select **Assign to site**.

Note
Initially, the AP5xx will always assume the operational mode of the site to which it is deployed. However, you can move an AP5xx between sites of different types within ExtremeCloud Appliance.

Related Topics

Options for AP Discovery with Dual Operation Modes on page 25

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 **Administration** > **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 Topics

Discovering Switches on page 20
Switch Discovery in an Availability Pair on page 21

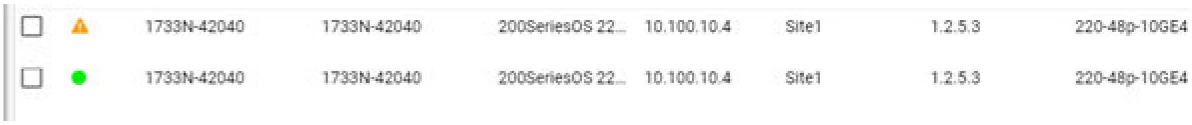
Discovering Switches

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.



□	⚠	1733N-42040	1733N-42040	200SeriesOS 22...	10.100.10.4	Site1	1.2.5.3	220-48p-10GE4
□	●	1733N-42040	1733N-42040	200SeriesOS 22...	10.100.10.4	Site1	1.2.5.3	220-48p-10GE4

Figure 4: ExtremeCloud Appliance: Switch States During Discovery

Related Topics

Switch Discovery in an Availability Pair on page 21

Switch Discovery Process on page 19

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 Topics

Switch Discovery Process on page 19

Discovering Switches on page 20

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.

Note
The following access points are supported in both a Centralized and Distributed site:

- AP505i
- AP510i/e
- AP560i/h

Centralized sites support the following AP39xx models:

- AP410i/e
- AP460i/e
- 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

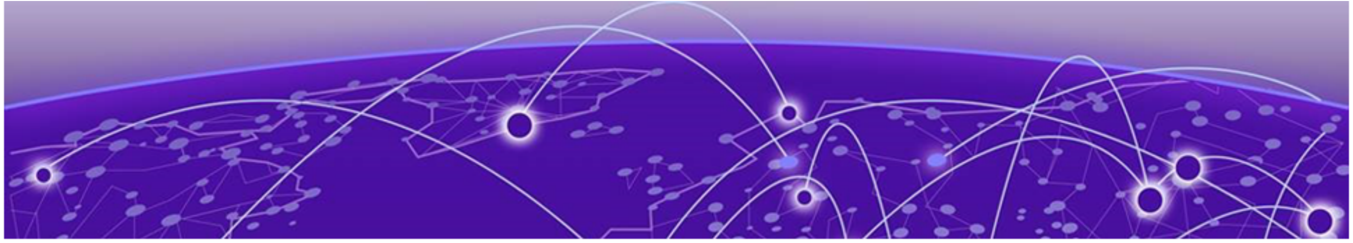
The most simple site configuration allows for one device group for each AP/adapter model, selecting the default configuration profile and the default RF Management profile for that model.

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.



Configuring DHCP, NPS, and DNS Services

This chapter describes how to configure DHCP 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 24
- NPS Service Configuration on page 48
- DNS Service Configuration on page 53

DHCP Service Configuration

Before you can configure the DHCP 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 24
- Configuring DHCP on a Red Hat Linux Server on page 44

Configuring DHCP on Windows Server 2012 R2

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

DHCP options provide specific configuration and service information to DHCP clients. The options described here are specific to pointing an AP to its adopter and setting the correct MINT link level. The option value you configure is specific to your network site type.

When you configure DHCP for ExtremeCloud Appliance, include one of the following options depending on your site type:

- The 078 SLP DA Option for access points on a Centralized site.
- The 191 Option for access points on a Distributed site.

Note
When deploying AP5xx that supports both operation modes, best practice is to configure both Centralized site and Distributed site adoption options.

A scope is a collection of IP addresses meant to be distributed by the DHCP server to the client devices on a subnet.

Enable the DHCP Option for every scope you define. The the DHCP Option is used by:

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

You have the option to configure DHCP at the server IPv4 node. Options configured at the server node apply to all scopes within that node.

Note
Go to http://support.microsoft.com for instructions on how to install DHCP.

Related Topics

Add a New DHCP Scope on page 26
Configure DHCP Server Options on page 34

Options for AP Discovery with Dual Operation Modes

The ExtremeWireless AP5xx offers operation modes that can be supported in either a Centralized site or a Distributed site. The access points assume their operation mode upon site discovery. When configuring infrastructure for discovery adoption for AP5xx, best practice is to configure adoption methods for both a Centralized site and a Distributed site. Therefore, if you opt to move an 802.11ax access point later to a different site (from within ExtremeCloud Appliance) the DHCP options are already configured to support the new site.

In particular, configure both DHCP options for installations that plan to support dynamically swapping AP adoption modes between Centralized and Distributed sites. As the AP switches personalities it needs support for the corresponding discovery options.

When configuring an availability pair, define the IP address for each ExtremeCloud Appliance under the discovery options.

Discovery options:

DHCP

- Option 78: Applicable only to Centralized mode. Points to SLP DA, which is typically instantiated within the appliance itself.

- Option 43/60: Applicable to both modes. Can point directly to the appliance, but would require double encoding of code points for Centralized (01) and Distributed (191). DHCP Server may not allow overload.
- Option 191, 192: Applicable to Distributed mode only. Points to ExtremeCloud Appliance

For AP5xx access points, best practice is to configure both Option78 and Option 191 or 192.

DNS

- Controller.<> : Applicable only in Centralized mode. Resolves to the appliance IP address.
- Wing-wlc.<domain>: Applicable only in Distributed mode: Resolves to the appliance IP address.

For DNS assistance, configure both Controller and WiNG-WLC resolutions to resolve to the appliance.

Multicast

- SLP Multicast: Applicable only for Centralized mode.
- MINT Multicast: Not supported as an adoption method for ExtremeCloud Appliance.

> Note
> The Multicast-based discovery method is not recommended for installation sites requiring dual role or Distributed operation. As APs switch roles, they consider the available information source (DNS, DHCP) to re-establish connection to the managing appliance.

Related Topics

802.11ax AP Operational Modes on page 19

Add a New DHCP Scope

Add a scope for the DHCP service.

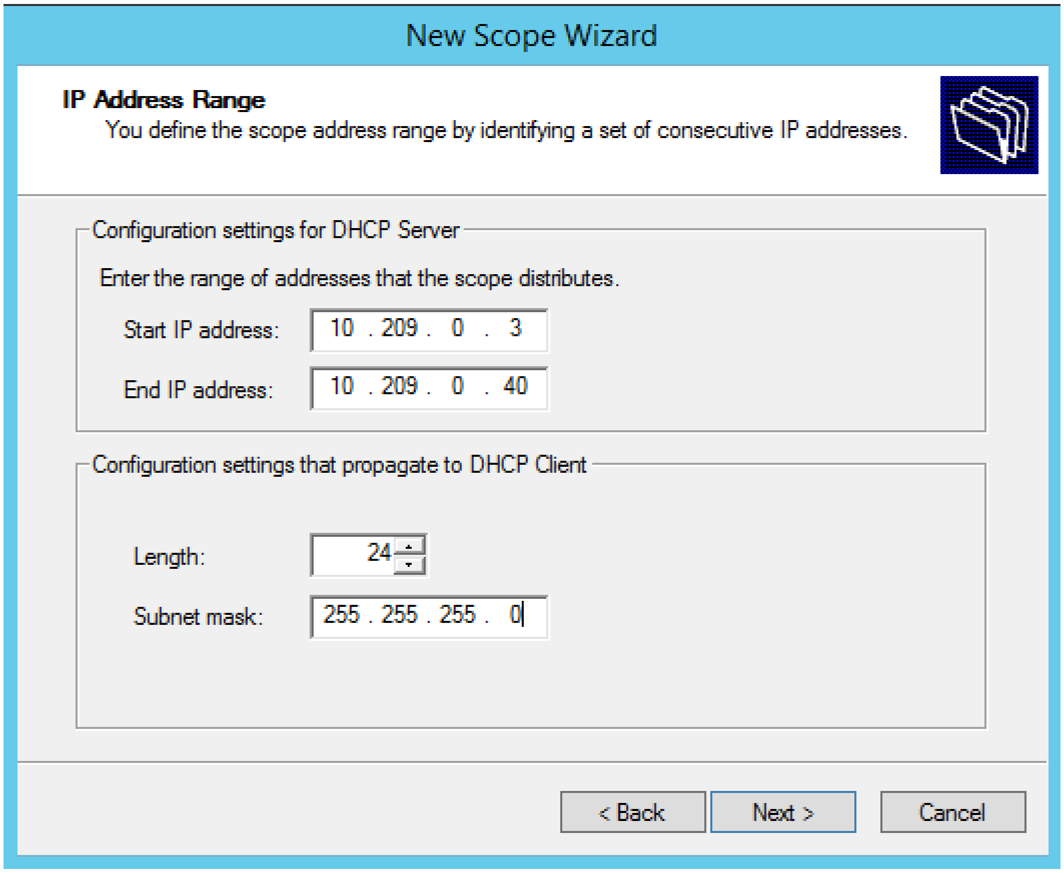
To configure DHCP on Windows Server 2012 R2:

1. Select **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 select **New Scope**.
3. Select **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. Select **Next**.

   The **IP Address Range** window is displayed.



New Scope Wizard

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address: 10 . 209 . 0 . 3

End IP address: 10 . 209 . 0 . 40

Configuration settings that propagate to DHCP Client

Length: 24

Subnet mask: 255 . 255 . 255 . 0

Figure 5: 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. Select **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. Select **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.

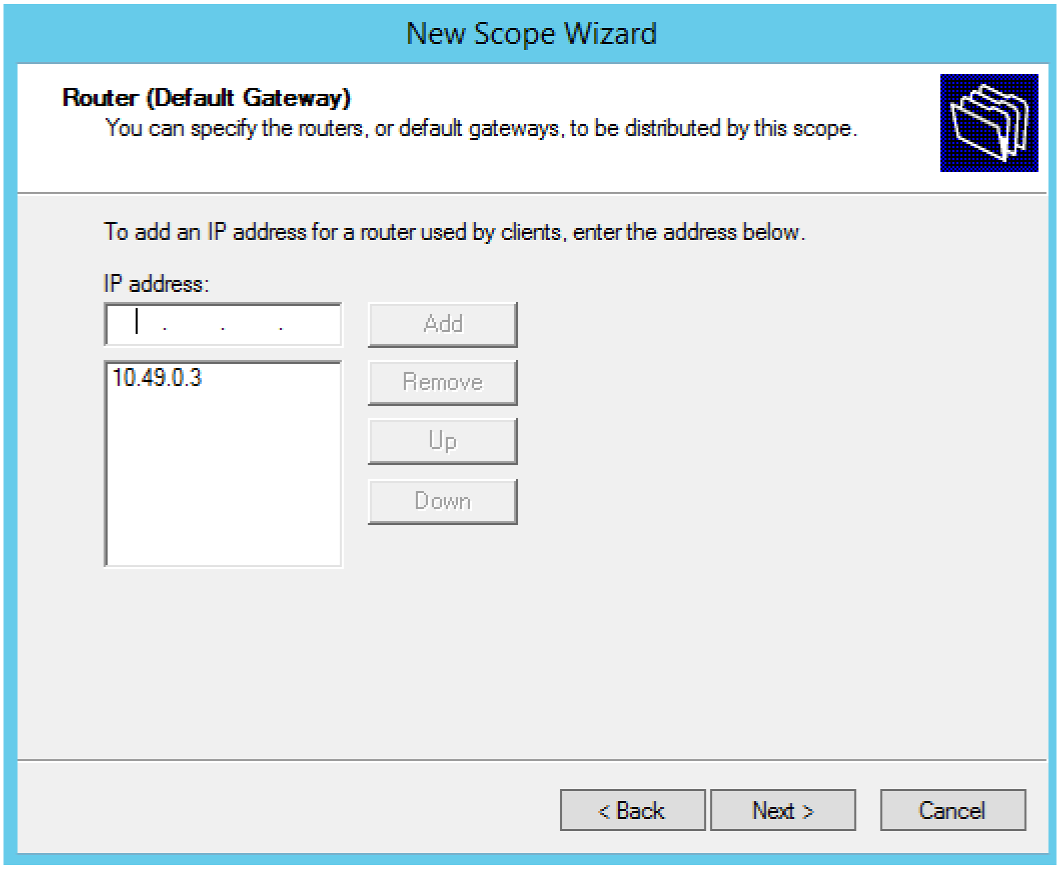
11. In the Days, Hours and Minutes text box, type the lease duration.

    You must use the Lease Duration as specified by your network administrator.
12. Select **Next**.

    The **Configure DHCP Options** window displays.
13. Select **Yes, I want to configure these options now**, and then select **Next**.

    The **Router (Default Gateway)** window displays.
14. In the IP address text box, type the network's default gateway and select **Add**.

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



New Scope Wizard

Router (Default Gateway)

You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

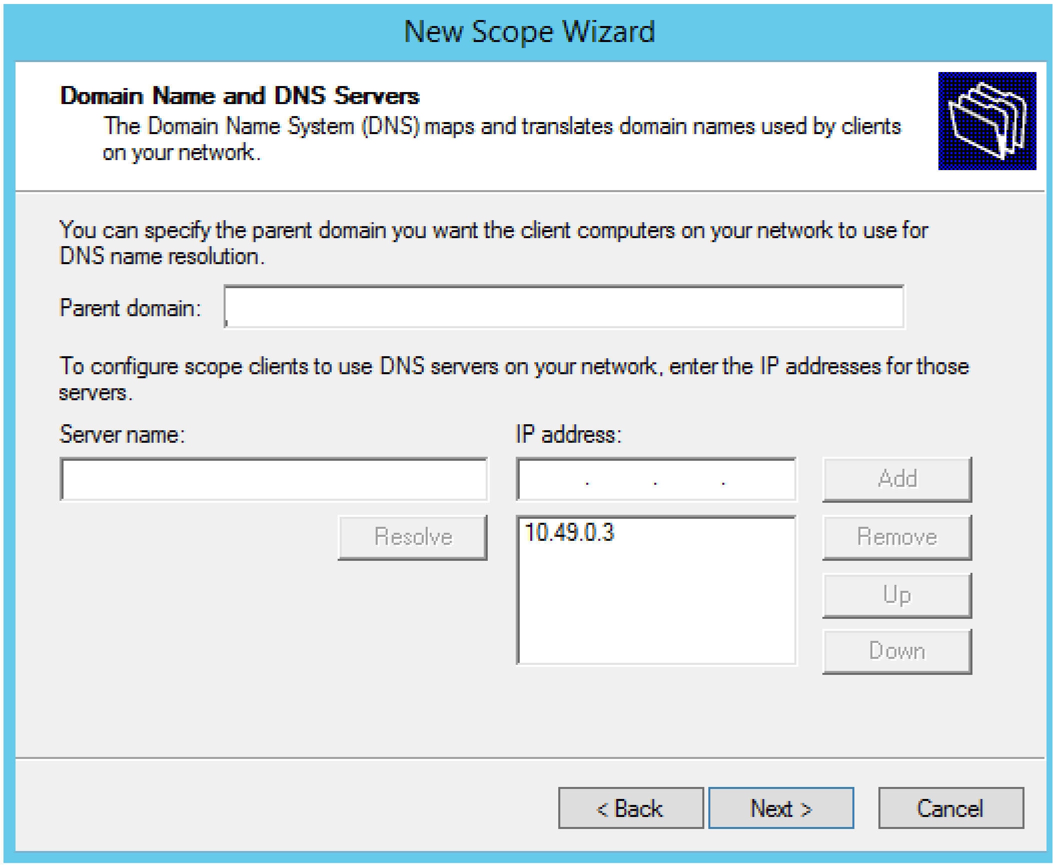
IP address:

10.49.0.3

Figure 6: Router Default Gateway

15. Select **Next**.

    The **Domain Name and DNS Servers** window displays.



New Scope Wizard

Domain Name and DNS Servers

The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:

IP address:

10.49.0.3

Figure 7: 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 select **Add**.
19. Select **Next**.

    The **WINS Servers** window displays.
20. Select **Next**.

    The **Activate Scope** window displays.
21. Select **Yes, I want to activate this scope now**, and select **Next**.

    The wizard displays the following message:
    ```
    You have successfully completed the New Scope wizard.
    ```
22. Select **Finish**.

Related Topics

Create New DHCP Options on page 30

Create New DHCP Options

When you configure DHCP for ExtremeCloud Appliance, create one of the following options that depend on your site type:

- The 078 SLP DA Option for access points on a Centralized site.
- The 191 Option for access points on a Distributed site.

Note
You can create the DHCP options at the scope level or at the server IPv4 node. When you configure DHCP options at the server node, the options apply to all scopes under that node.

1. From the IPv4 node, right-click and select **Set Predefined Options**.

   The **Predefined Options and Values** dialog displays.
2. Option Class is **DHCP Standard Options**.
3. Select **Add**.

   The **Option Type** dialog displays.
4. Refer to the related information for each option.

Related Topics

Creating Option 78 on page 32
Creating Option 191 on page 30

Creating Option 191

ExtremeWireless WiNG APs use DHCP Option 191 to find and adopt to ExtremeCloud Appliance. To configure Option 191 on DHCP server, take the following steps:

1. Go to **Start** > **Administrative Tool** > **DHCP**.
2. Right-click the server node, and select **Set predefined options**.
3. Select **Add**, and configure the following parameters:

   Name

   Provide a name for the option, for example **191 Distributed Discovery**.

   Data Type

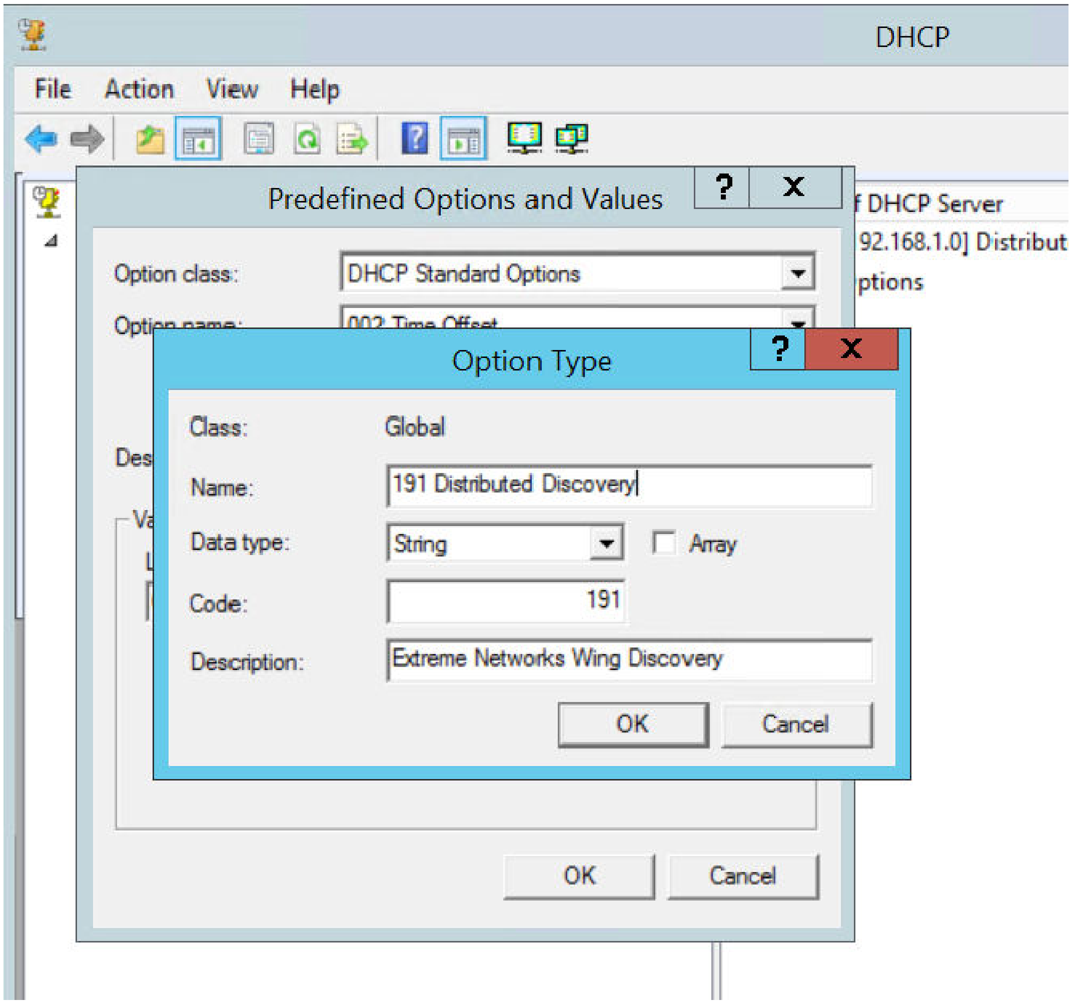
   Set the data type to **String**

   Code

   191

   Description

   Optional description. For example, `Extreme Networks Wing Discovery`.



Predefined Options and Values

Option class: DHCP Standard Options

Option name: 002 Time Offset

Option Type

Class: Global

Name: 191 Distributed Discovery

Data type: String □ Array

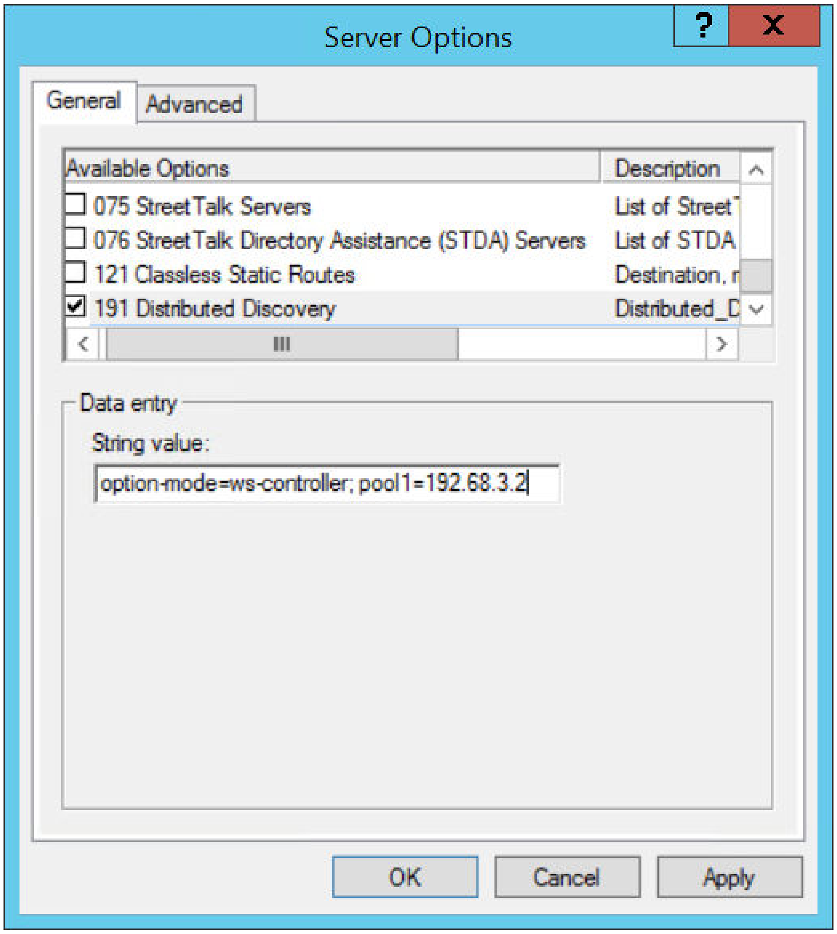
Code: 191

Description: Extreme Networks Wing Discovery

Figure 8: Create DHCP Option 191

4. Select **OK**.
5. Enter the string value for option 191

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



Available Options	Description
□ 075 StreetTalk Servers	List of Street
□ 076 StreetTalk Directory Assistance (STDA) Servers	List of STDA
□ 121 Classless Static Routes	Destination, r
☑ 191 Distributed Discovery	Distributed_D

String value: option-mode=ws-controller; pool1=192.68.3.2

Figure 9: DHCP Option 191 String Value

Related Topics

Creating Option 78 on page 32

Configure DHCP Server Options on page 34

Creating Option 78

To create Option 78 for a Centralized site:

1. Go to **Start** > **Administrative Tool** > **DHCP**.
2. Right-click the server node, and select **Set predefined options**.
3. Select **Add**, and configure the following parameters:

Name

Provide a name for the option, for example **SLP DA**.

Data Type

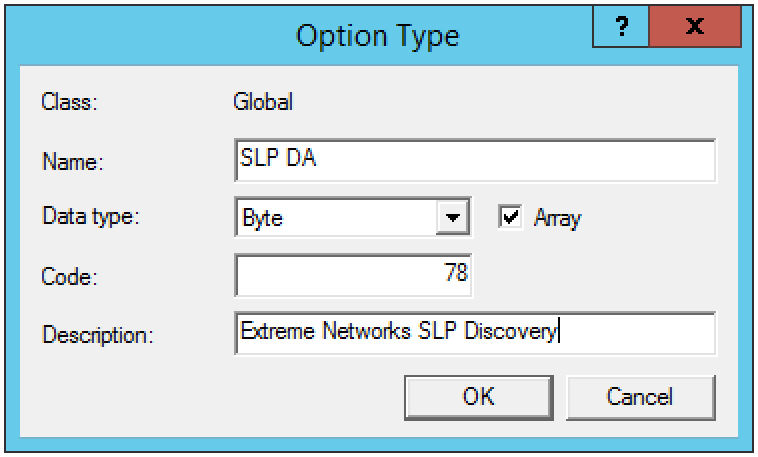
Set the data type to **Byte** and select the **Array** check box.

Code

78

Description

Optional description. For example, `Extreme Networks SLP Discovery`.



Option Type

Class: Global

Name: SLP DA

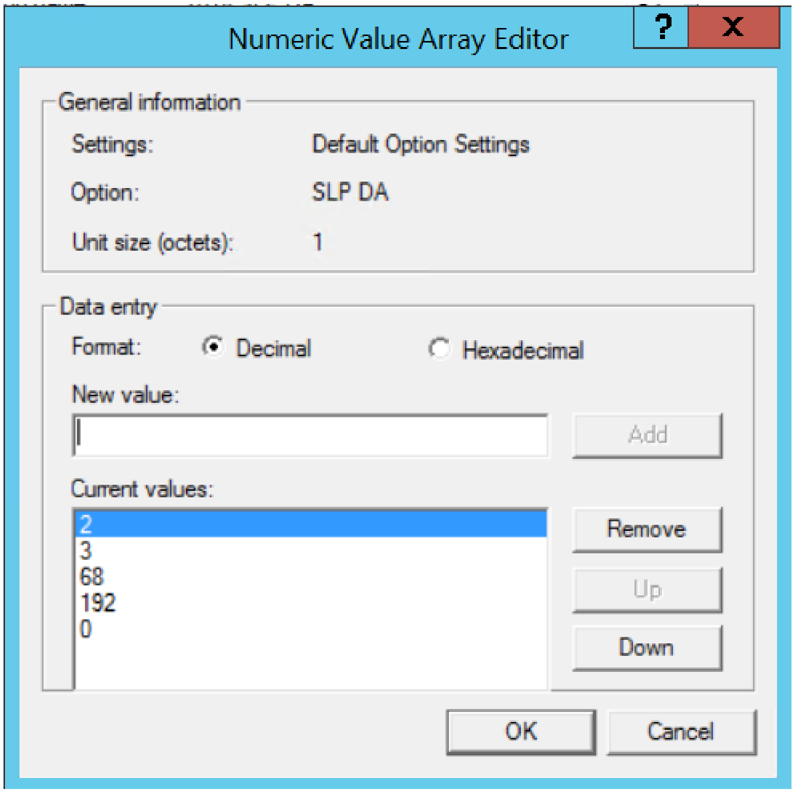
Data type: Byte ☑ Array

Code: 78

Description: Extreme Networks SLP Discovery

Figure 10: Option Type

4. Select **OK**.
5. Select **Edit Array** and enter the IP address per octet.



Numeric Value Array Editor

General information

Settings: Default Option Settings

Option: SLP DA

Unit size (octets): 1

Data entry

Format: ● Decimal ○ Hexadecimal

New value:

Current values:

2
3
68
192
0

Figure 11: DHCP Option 78 Array Decimal Values

6. Select **OK**.

Related Topics

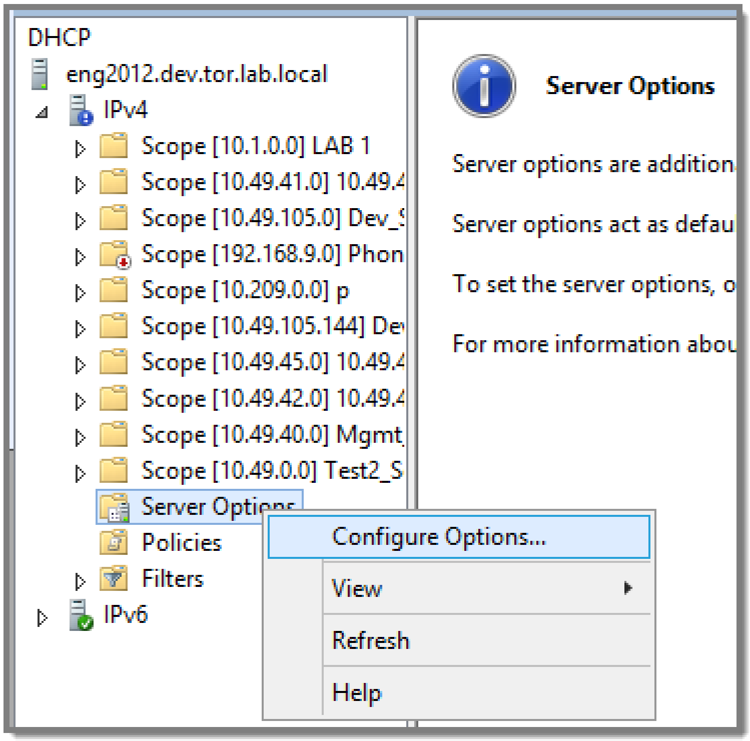
Creating Option 191 on page 30

Configure DHCP Server Options on page 34

Configure DHCP Server Options

Configure the DHCP Option that you created under Create New DHCP Options on page 30. Configuring this option for the server, automatically includes the scope.

1. From the **IPv4** node, expand the tree.
2. Right-click **Server Options** and select **Configure Options**.



Server options are addition

Server options act as defau

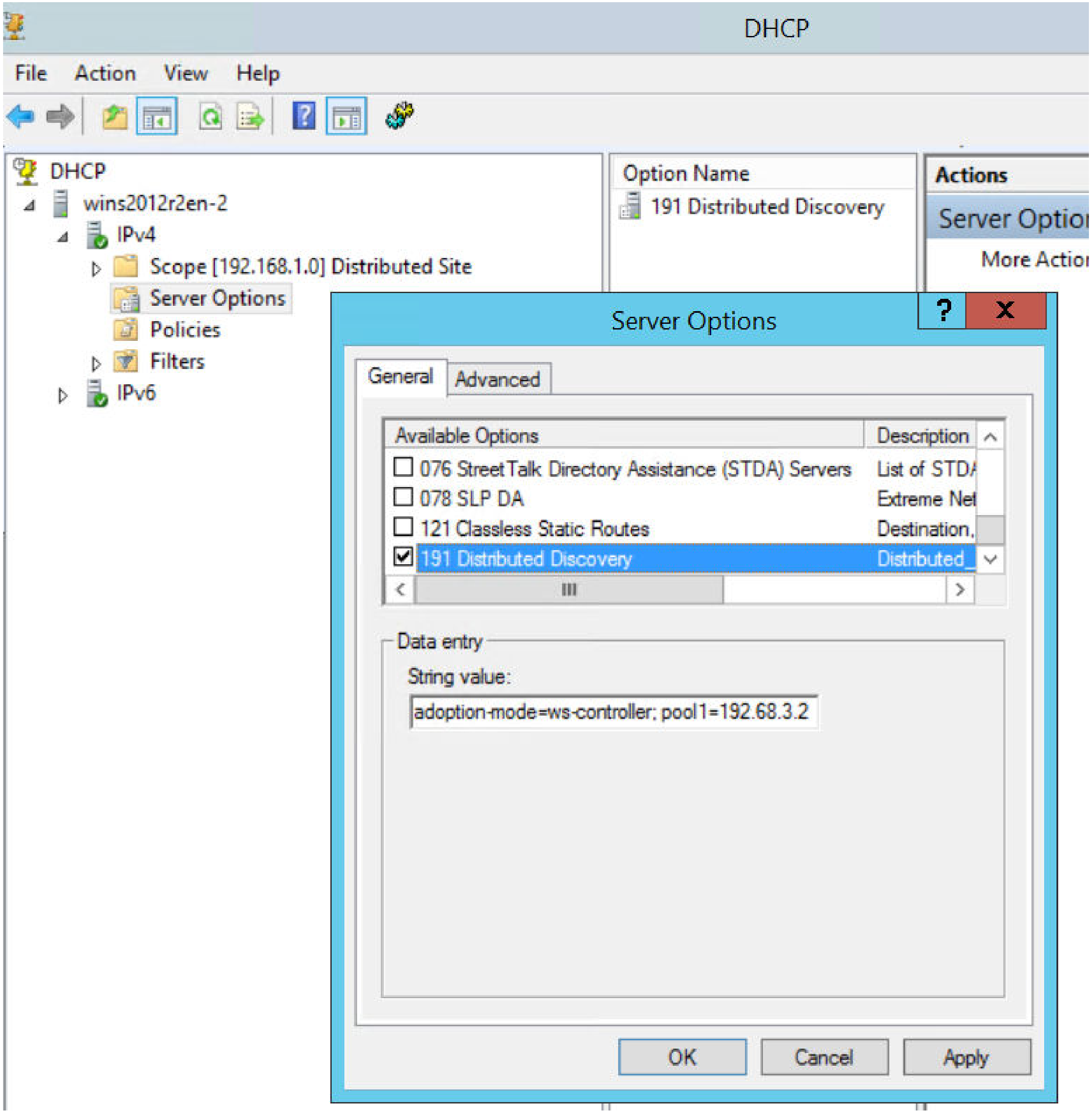
To set the server options, o

For more information abou

Figure 12: Configure Options

The **Server Options** dialog displays.

3. From the **General** tab, select the DHCP option you just created. Possible values are:
   - 191 Distributed Discovery
   - 078 SLP DA



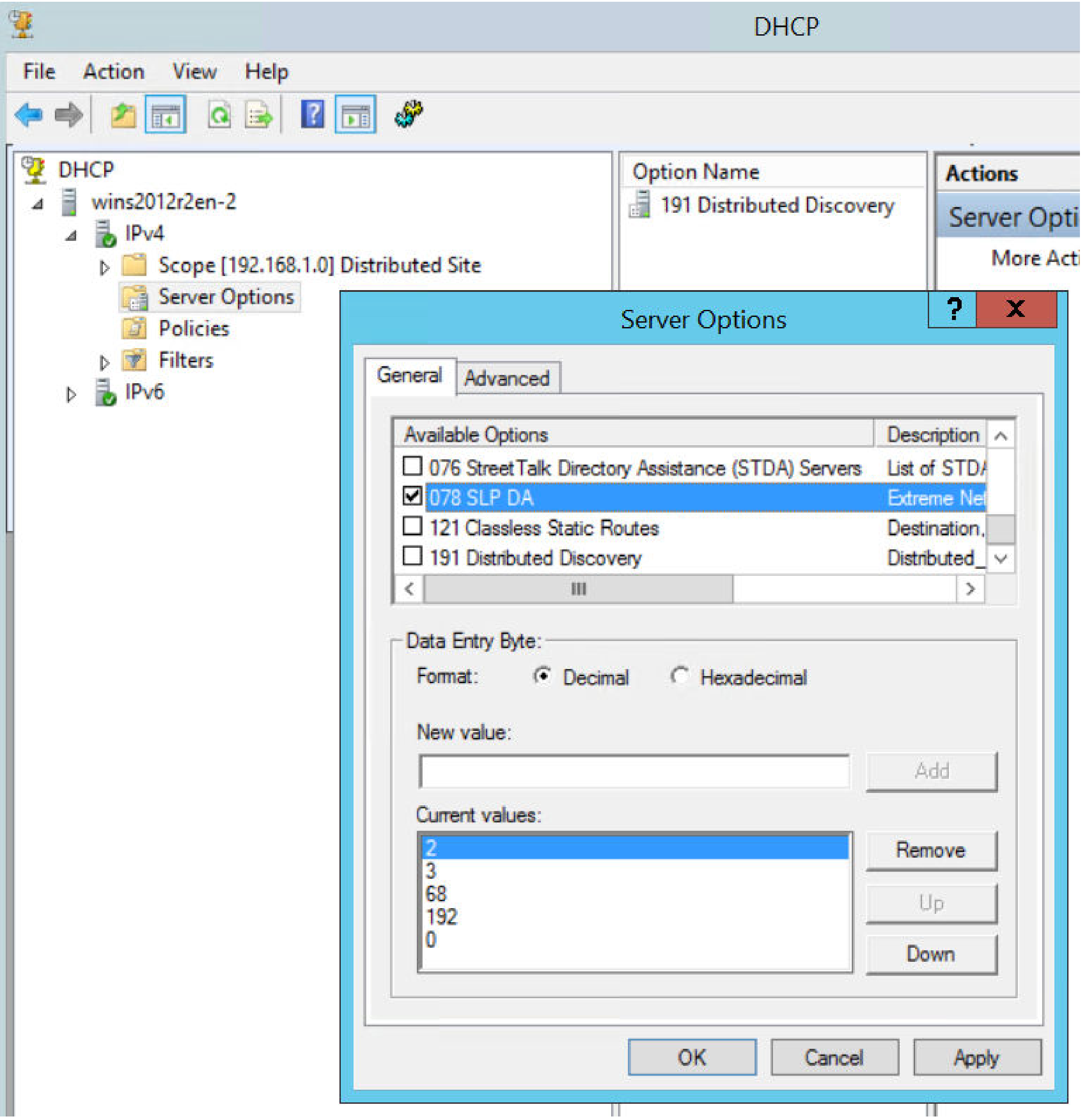
Available Options	Description
☐ 076 StreetTalk Directory Assistance (STDA) Servers	List of STDA
☐ 078 SLP DA	Extreme Net
☐ 121 Classless Static Routes	Destination,
☑ 191 Distributed Discovery	Distributed_

Data entry

String value:

adoption-mode=ws-controller; pool1=192.68.3.2

Figure 13: Configure Server Option 191



DHCP
- wins2012r2en-2
  - IPv4
    - Scope [192.168.1.0] Distributed Site
    - Server Options
    - Policies
    - Filters
  - IPv6

Option Name
191 Distributed Discovery

Available Options	Description
□ 076 StreetTalk Directory Assistance (STDA) Servers	List of STDA
☑ 078 SLP DA	Extreme Ne
□ 121 Classless Static Routes	Destination,
□ 191 Distributed Discovery	Distributed_

Data Entry Byte:

Format: ● Decimal ○ Hexadecimal

New value:

Current values:

2
3
68
192
0

Figure 14: Configure Server Option 078

4. Verify the configured Data entry values for the selected option and select **OK**.

   In a Centralized site, the wireless APs use the SLP DA to discover the ExtremeCloud Appliance. The mobility agents use the SLP DA to discover the mobility manager. 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 IP address 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.

Related Topics

Creating Option 78 on page 32

Creating Option 191 on page 30

Configuring Vendor Class on Windows Server 2012 R2

This section describes the Vendor Class Identifier on a Microsoft DHCP server for ExtremeCloud Appliance discovery. In the discovery process, the DHCP server returns vendor-specific information to the client. When an AP requests vendor specific information, the DHCP server sends the appliance IP addresses in Option 43 to the AP.

- Vendor Class Identifier (VCI)
  - The VCI for an ExtremeWireless AP39xx is `HiPath <AP model name>`. For example, the VCI for the ExtremeWireless AP3965e is `HiPath AP3965`.
  - The VCI for an ExtremeWireless WiNG AP is `WingAP.<AP model name>` . For example, the VCI for the ExtremeWireless WiNG AP505i is `WingAP.<AP505>` and AP410i is `WingAP.<AP410>`.
  - The VCI for the SA201 adapter is `HiPath SA201`.
- Option 43 sub-option code:
  - The option 43 sub-option code:
    - ExtremeWireless APs supported in a Centralized site is `type 1 (0x1)`.
    - ExtremeWireless APs supported in a Distributed site is 191.
- IP addresses of ExtremeCloud Appliance.

To configure VCI, take the following steps:

1. From the IPv4 node, right-click and select **Define Vendor Classes**.

   The **DHCP Vendor Classes** dialog displays.
2. Select **Add**.

Configuring Option 43

How to configure Option 43 on Windows Server 2012 R2.

Create Vendor Class

To create a vendor class using the Windows Server 2012 R2 DHCP, IPv4 server utility:

1. Go to **Start** > **Administrative Tool** > **DHCP**.
2. Right-click the server node, and select **Define Vendor Classes**.

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

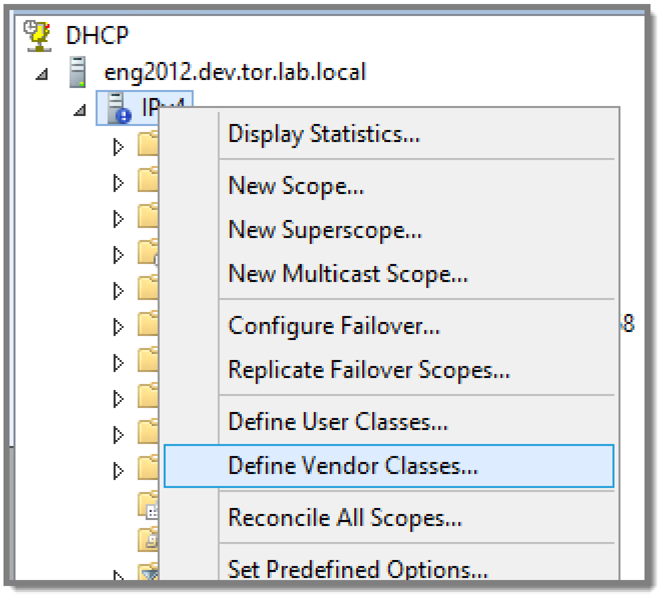
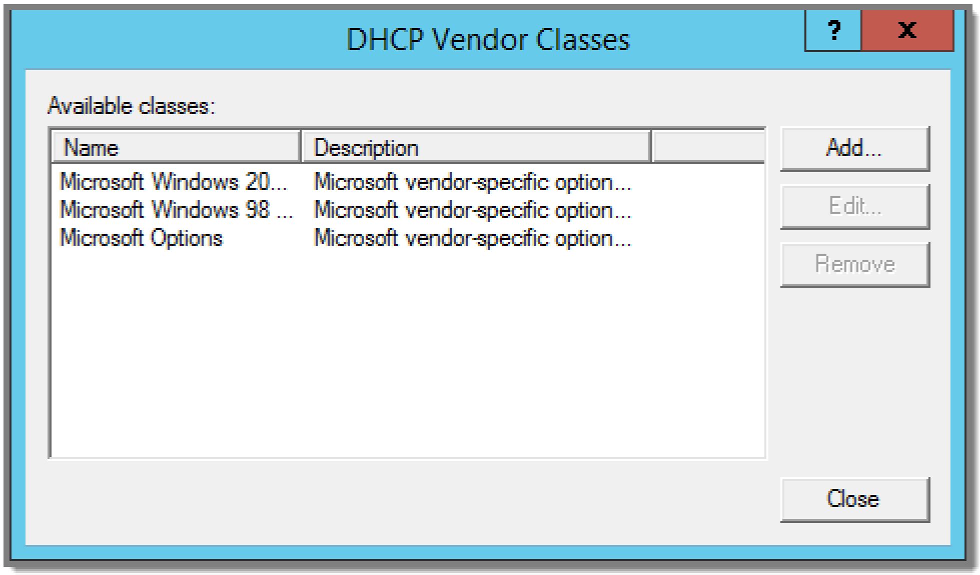


Figure 15: Define Vendor Classes

The **DHCP Vendor Classes** window displays.



Name	Description
Microsoft Windows 20...	Microsoft vendor-specific option...
Microsoft Windows 98 ...	Microsoft vendor-specific option...
Microsoft Options	Microsoft vendor-specific option...

Figure 16: DHCP Vendor Classes

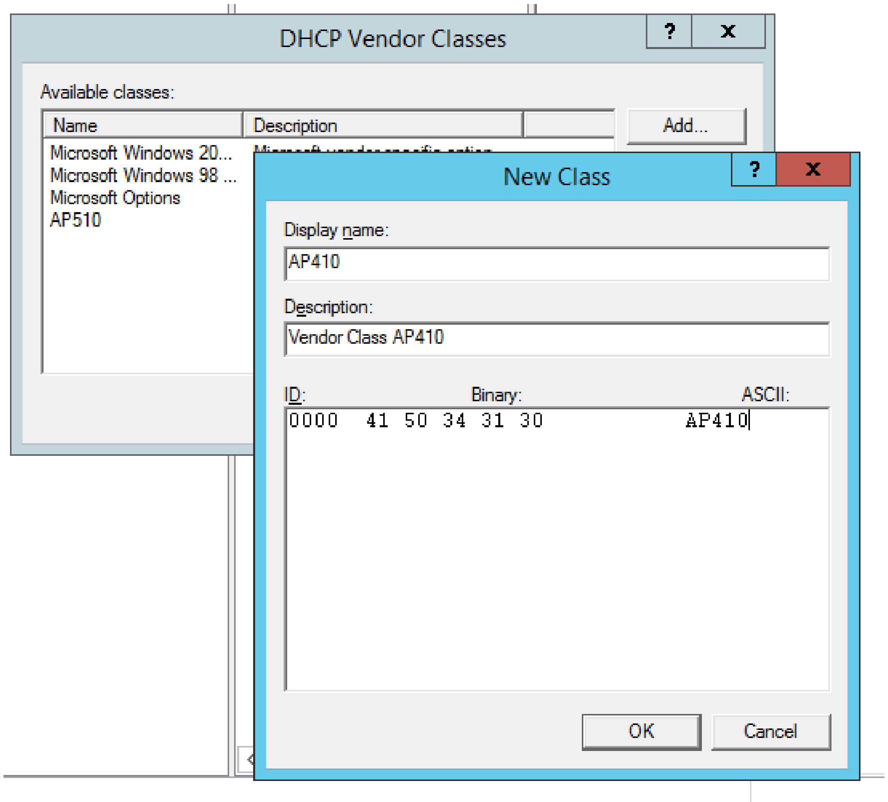
3. To create the new class, select **Add**.

   The **New Class** dialog displays.

4. Provide a Display Name and Description for the vendor class.

5. Select the ASCII field and type the VCI for the specific AP. For example, type **AP410** for an AP410i.

   The ID and Binary values are populated.



Name	Description
Microsoft Windows 20...	
Microsoft Windows 98 ...	
Microsoft Options	
AP510	

Display name: AP410

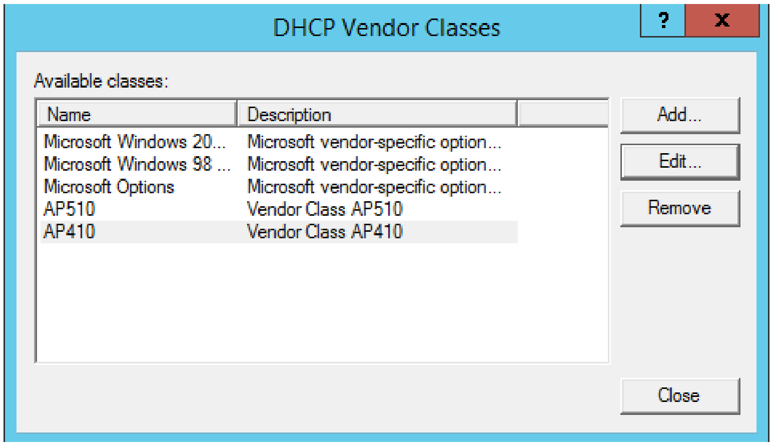
Description: Vendor Class AP410

```
ID:      Binary:                 ASCII:
0000   41 50 34 31 30            AP410
```

Figure 17: VCI AP410

6. Select **OK**.

   The new class is created.



Name	Description
Microsoft Windows 20...	Microsoft vendor-specific option...
Microsoft Windows 98 ...	Microsoft vendor-specific option...
Microsoft Options	Microsoft vendor-specific option...
AP510	Vendor Class AP510
AP410	Vendor Class AP410

Figure 18: Vendor Classes

7. Select **Close**.

Configure Vendor Class

Configure the vendor class that you just created under Create Vendor Class on page 37.

1. Go to **Start** > **Administrative Tool** > **DHCP**.
2. Right-click the server node, and select **Set predefined options**.

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

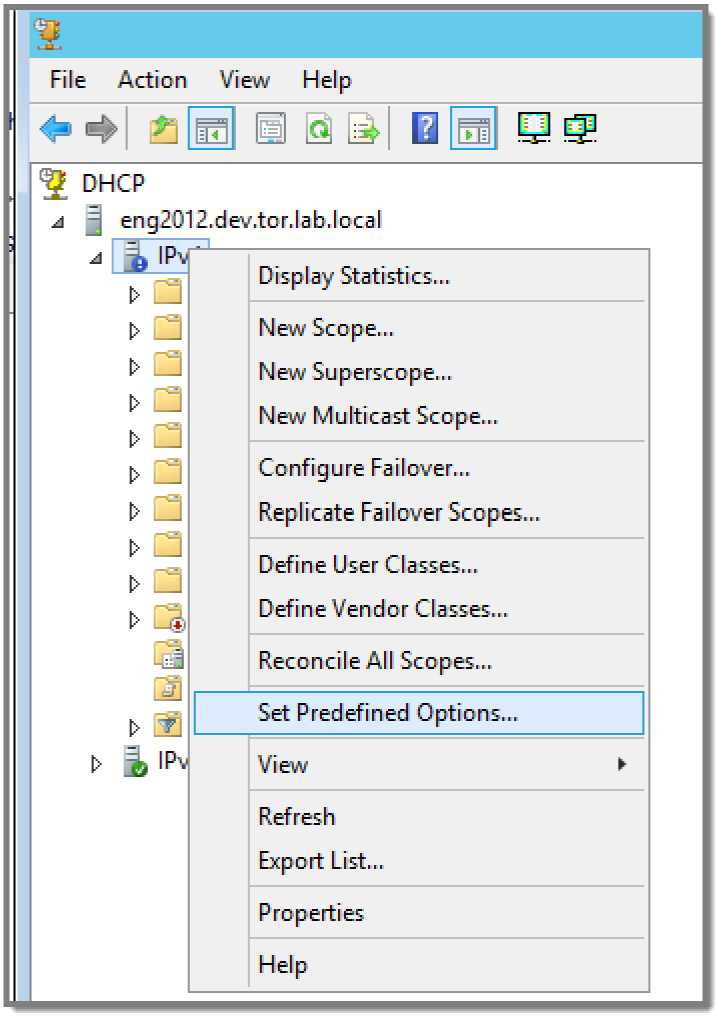
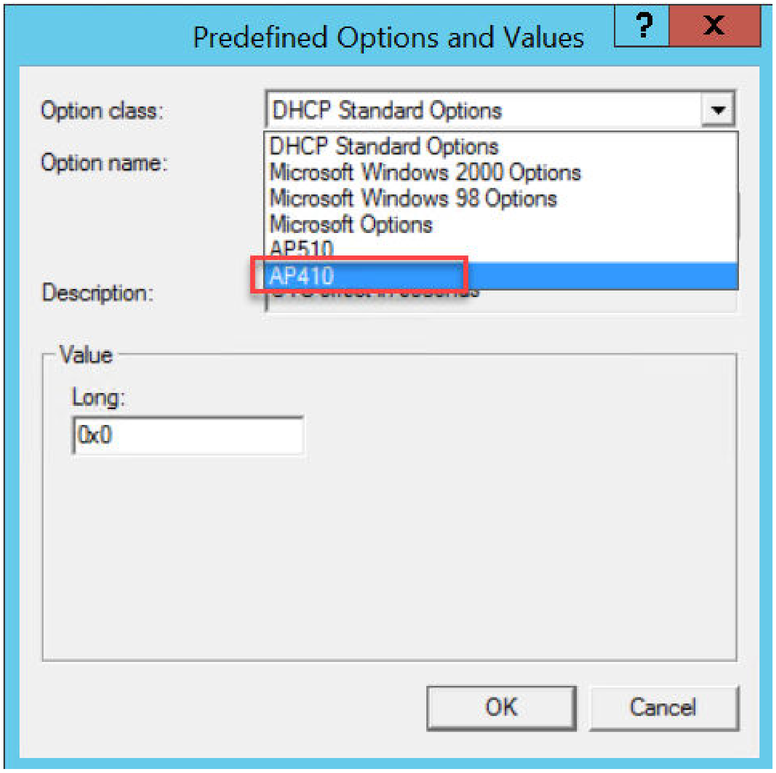


Figure 19: Set Predefined Options



Predefined Options and Values

Option class: DHCP Standard Options

Option name:

Description:

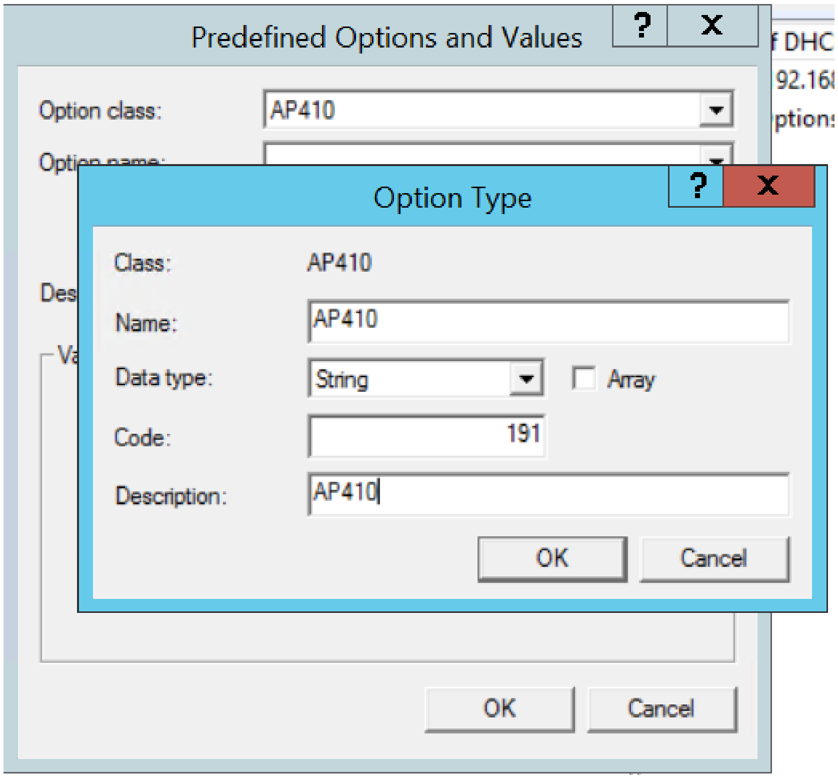
Value

Long: 0x0

Figure 20: Predefined Options and Values

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

   The **Option Type** window displays.



Predefined Options and Values

Option class: AP410

Option Type

Class: AP410

Name: AP410

Data type: String □ Array

Code: 191

Description: AP410

Figure 21: Option Type

4. Configure the following parameters:

   Name

   Name of the VCI option.

   Data Type

   Select one of the following:

   - Centralized Site — **Byte** and select **Array**
   - Distributed Site — **String**

   Code

   Enter one of the following:

   - Centralized site — sub-option value **1**
   - Distributed site — sub-option value **191**

   Note

   When both options are configured, the AP may first adopt to a Distributed site. However, you can control site adoption in ExtremeCloud Appliance using automatic adoption rules, or you can manually move an AP to a specific site.

   Description

   (Optional) Enter a description.

5. Select **OK**.

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

6. Select **OK**.

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

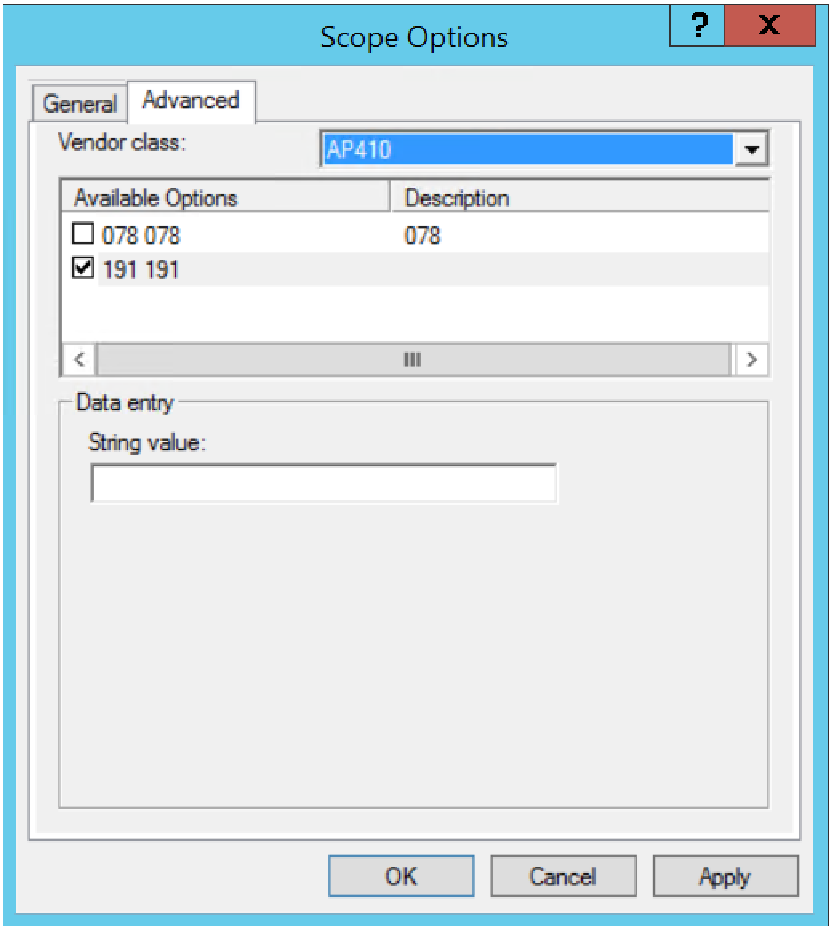
Configuring Server Options

Associate the Vendor Class Identifier option with each DHCP scope.

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

   The **Scope Options** window displays.

2. Click the **Advanced** tab.



Scope Options

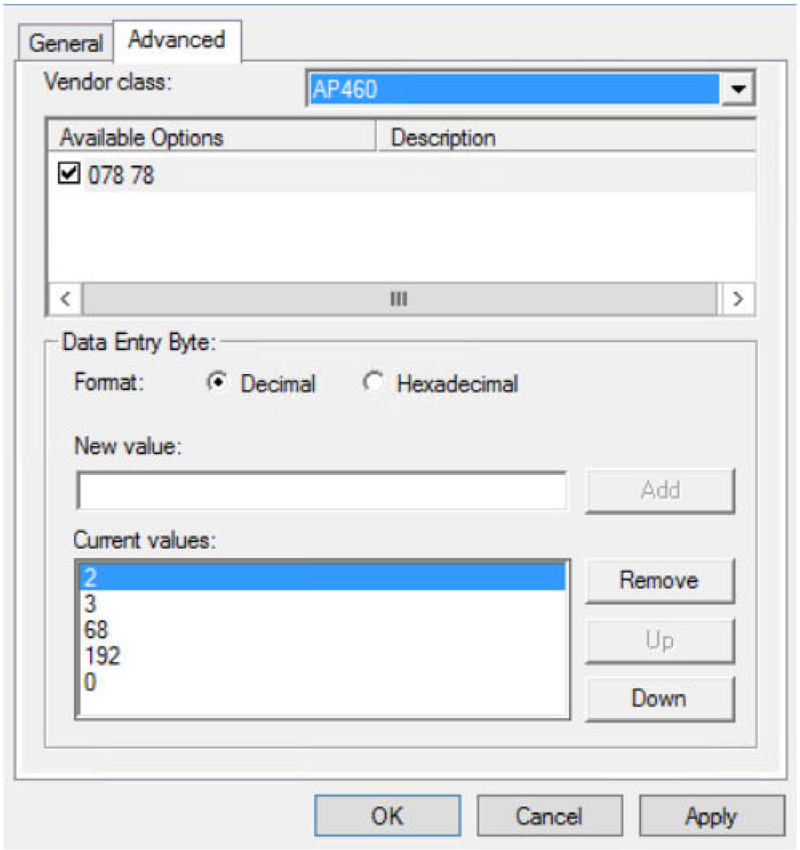
Vendor class: AP410

Available Options	Description
□ 078 078	078
☑ 191 191	

Data entry

String value:

Figure 22: Vendor Class Option 191



Vendor class: AP460

Available Options

☑ 078 78

Format: ● Decimal ○ Hexadecimal

Current values:

2
3
68
192
0

Figure 23: Vendor Class Option 078

Vendor Class

Select the vendor class that you plan to use. For example, AP410 or AP460.

Available Options

Select a predefined sub-option to assign. The option must be checked and highlighted to display Data Entry options.

Data Entry

(Option 078 Only) Enter the controller IP addresses to return to the APs. This is a comma-delimited list.

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 APs in a Centralized site.

option slp-directory-agent true 10.209.0.1, 10.209.0.3;

### SLP option 191 for ExtremeWireless WiNG AP (Distributed site)
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 or adapter is HiPath <AP model name>. For example, the ExtremeWireless AP3912 is **HiPath AP3912** and the SA201 adapter is **HiPath SA201**.
- 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;
```

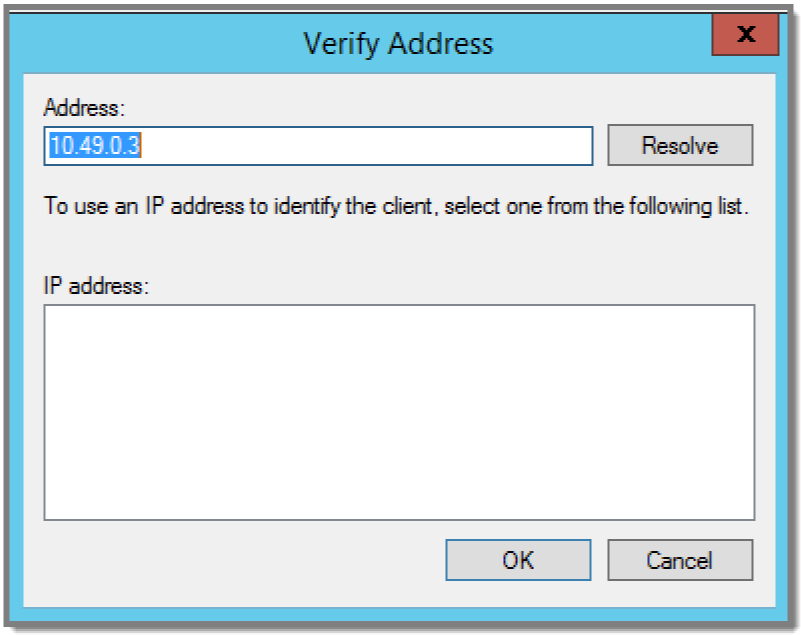
2. Restart the DHCP server.

```
[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**.



Verify Address

Address:

10.49.0.3

To use an IP address to identify the client, select one from the following list.

IP address:

Figure 24: Verify Address

   a. Click **Resolve**.

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

   b. 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 RADIUS 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:

- Add a New Network Policy on page 48
- Configuring the ExtremeCloud Appliance as an NPS Client on page 47

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

Related Topics

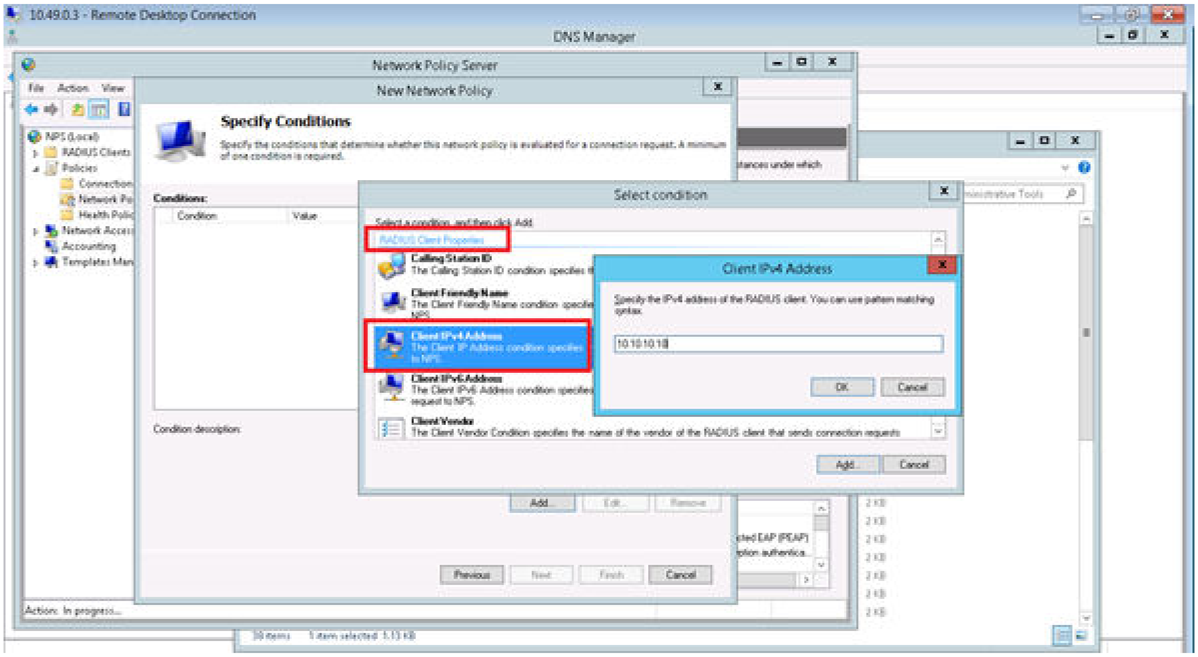
Create Condition: Client IPv4 Addresses on page 48

Create Condition: Windows Groups on page 50

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**.



Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

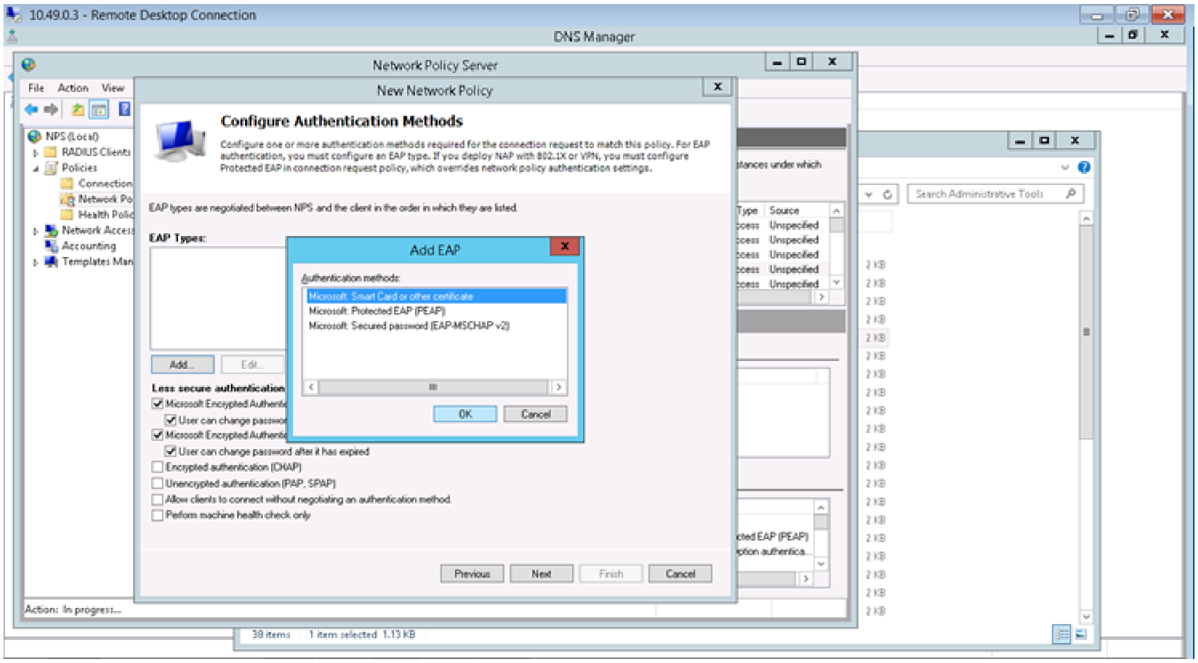
Select a condition, and then click Add.

Client IPv4 Address: Specify the IPv4 address of the RADIUS client. You can use pattern matching syntax.

10.10.10.10

Figure 25: 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**.



Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

EAP types are negotiated between NPS and the client in the order in which they are listed.

Authentication methods:
- Microsoft: Smart Card or other certificate
- Microsoft: Protected EAP (PEAP)
- Microsoft: Secured password (EAP-MSCHAP v2)

Less secure authentication methods:
- ☑ Microsoft Encrypted Authentication
- ☑ User can change password
- ☑ Microsoft Encrypted Authentication
- ☑ User can change password after it has expired
- ☐ Encrypted authentication (CHAP)
- ☐ Unencrypted authentication (PAP, SPAP)
- ☐ Allow clients to connect without negotiating an authentication method
- ☐ Perform machine health check only

Figure 26: Add EAP

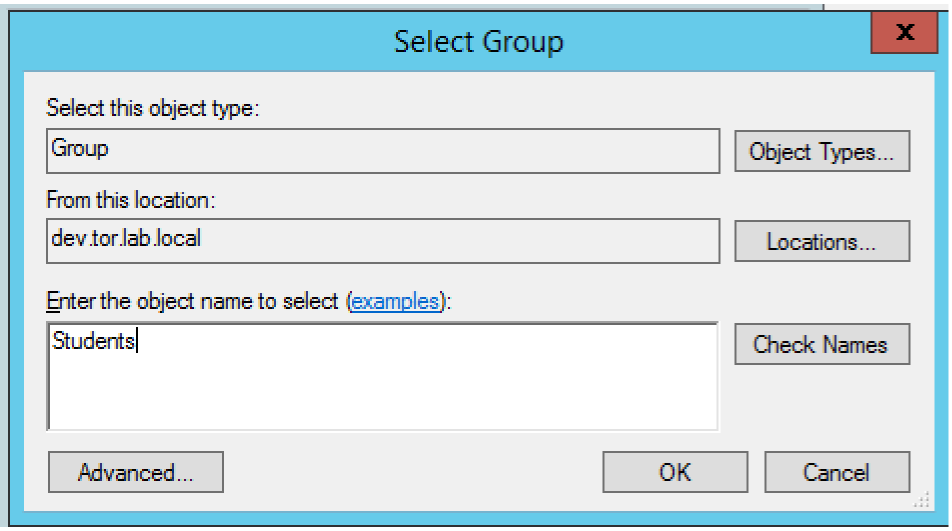
7. Click **Next**.
8. Configure the Idle Timeout and click **Next**.
9. Configure the Radius Attributes and click **Next**.
10. Click **Finish**.

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.



Select Group

Select this object type:
Group

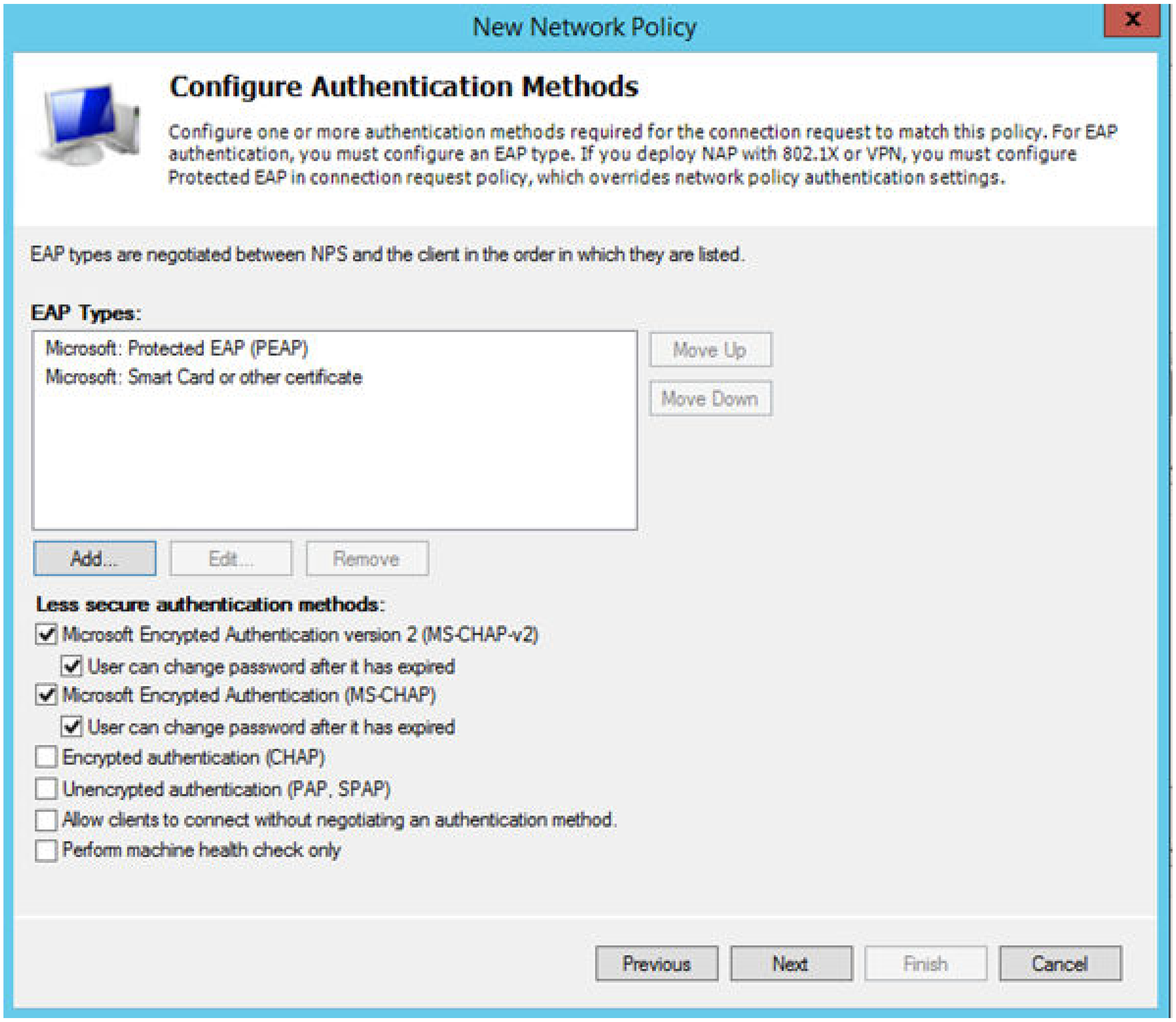
From this location:
dev.tor.lab.local

Enter the object name to select (examples):
Students

Figure 27: 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**.



New Network Policy

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Microsoft: Protected EAP (PEAP)
Microsoft: Smart Card or other certificate

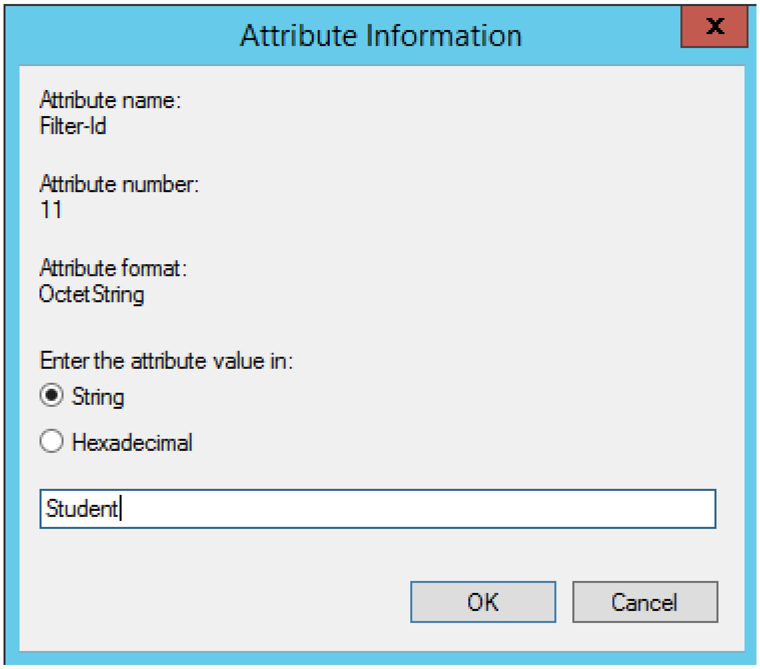
Less secure authentication methods:

☑ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
☑ User can change password after it has expired
☑ Microsoft Encrypted Authentication (MS-CHAP)
☑ User can change password after it has expired
□ Encrypted authentication (CHAP)
□ Unencrypted authentication (PAP, SPAP)
□ Allow clients to connect without negotiating an authentication method.
□ Perform machine health check only

Figure 28: 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.



Attribute name:
Filter-Id

Attribute number:
11

Attribute format:
OctetString

Enter the attribute value in:

● String

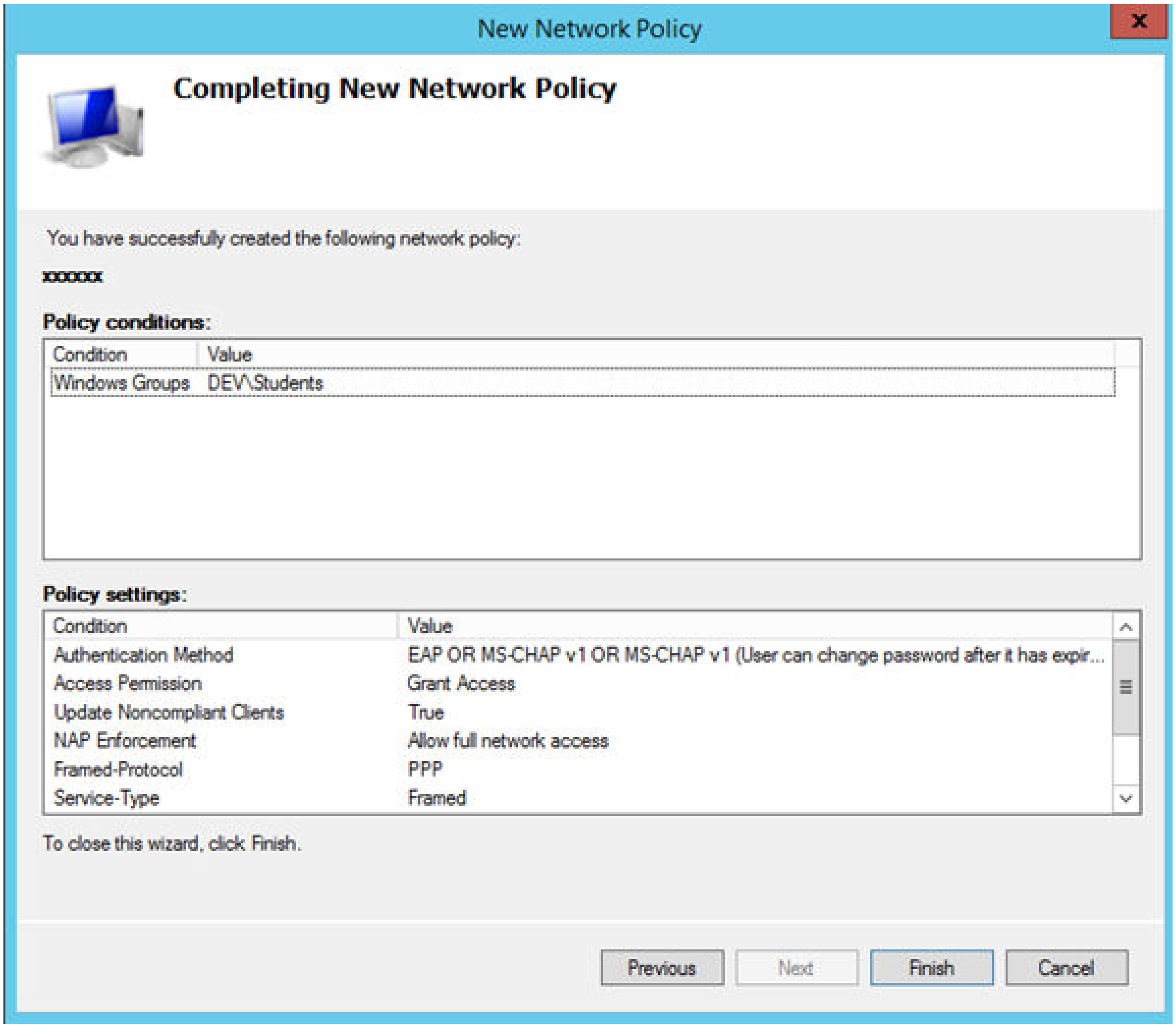
○ Hexadecimal

Student

Figure 29: Attribute Information

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

18. Click **Next**.



New Network Policy

Completing New Network Policy

You have successfully created the following network policy:

xxxxxx

Policy conditions:

Condition	Value
Windows Groups	DEV\Students

Policy settings:

Condition	Value
Authentication Method	EAP OR MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expir...
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

To close this wizard, click Finish.

Figure 30: 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.

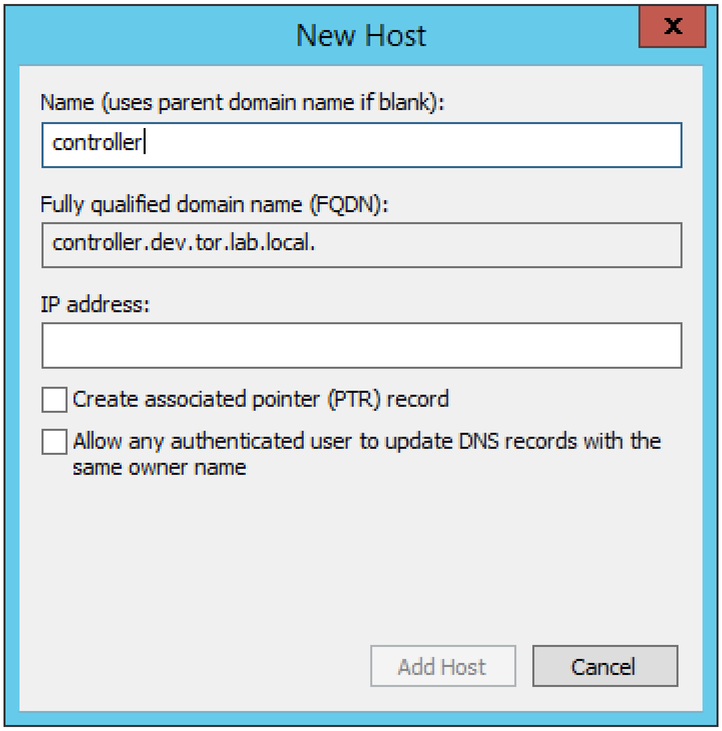
The instructions here are limited to Configuring DNS for Wireless APs Discovery.

For configuration on Linux, see Configuring DNS on a Linux Server on page 55.

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.

   New Host

   Name (uses parent domain name if blank):

   controller

   Fully qualified domain name (FQDN):

   controller.dev.tor.lab.local.

   IP address:

   □ Create associated pointer (PTR) record

   □ Allow any authenticated user to update DNS records with the same owner name

   Figure 31: 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 DHCP 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; };
```

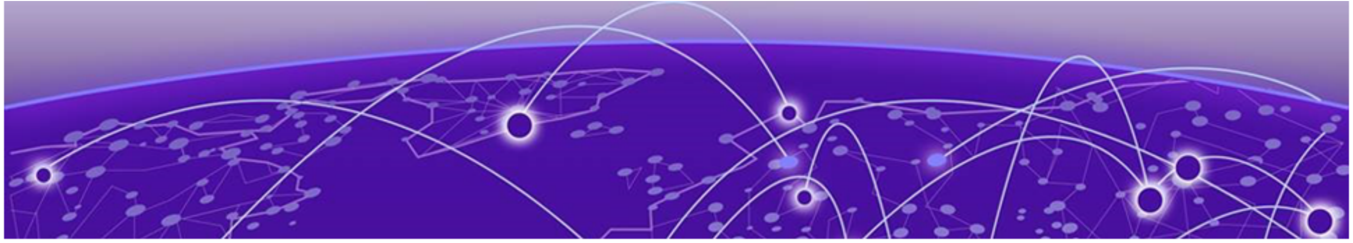
4. Confirm that DNS service is running.

```
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
```



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 **Configure** > **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 **Configure** > **Sites** and select a site. Then, select **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.

   - A Centralized site supports the following AP models:
     - AP39xx supporting ACS Policy for RF Management
     - AP5xx.

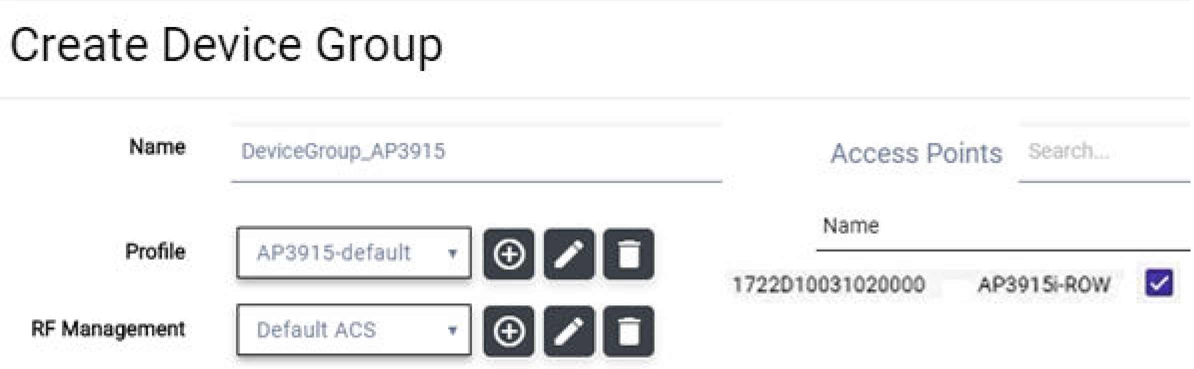
       Note
       AP5xx currently require manual channel plan configuration when used in a Centralized site. Go to **Configure** > **Devices** > **Access Points** and select an AP5xx model. For more information, see *Configure AP Radio Settings* in the *User Guide*

   - Default Smart RF supports APs in a Distributed site (AP7xxx, AP8xxx, and AP5xx).

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**.



Create Device Group

Name: DeviceGroup_AP3915

Profile: AP3915-default

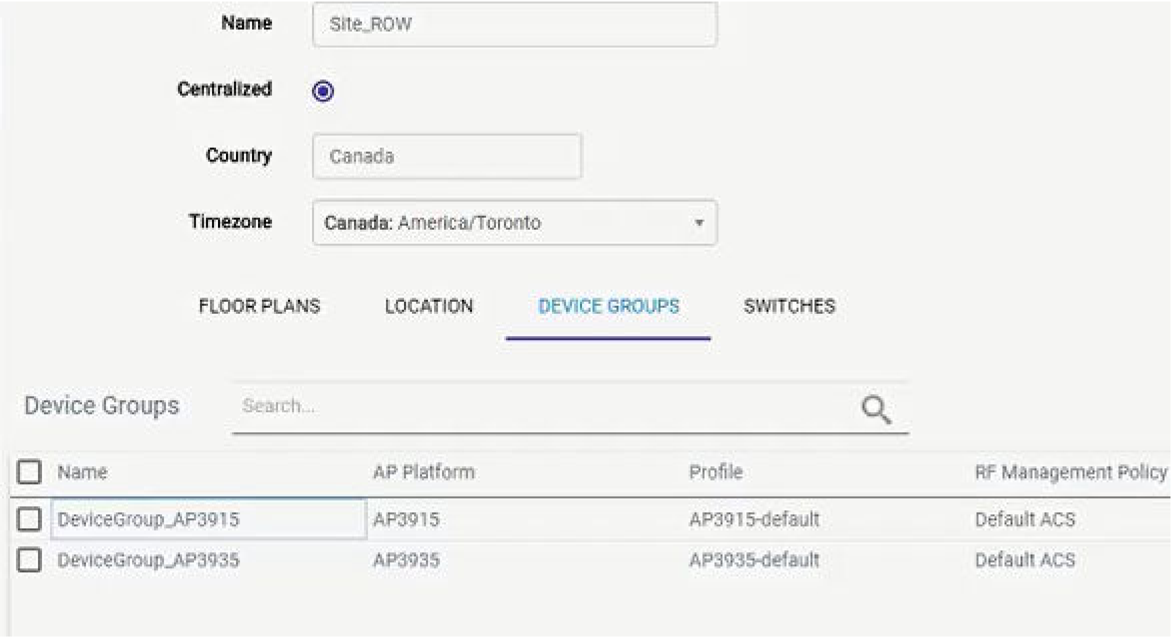
RF Management: Default ACS

Access Points

Name		
1722D10031020000	AP3915i-ROW	☑

Figure 32: 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.



Name: Site_ROW

Centralized: ●

Country: Canada

Timezone: Canada: America/Toronto

Device Groups

□	Name	AP Platform	Profile	RF Management Policy
□	DeviceGroup_AP3915	AP3915	AP3915-default	Default ACS
□	DeviceGroup_AP3935	AP3935	AP3935-default	Default ACS

Figure 33: Centralized Site with Two Device Groups

Next, configure an internal captive portal.

Related Topics

Configuring an Internal Captive Portal on page 59

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** > **RADIUS Servers** > **Add** 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.
4. Click **Save**.

Next, specify a network topology.

Related Topics

Specifying B@AC Network Topology on page 60

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 **Configure** > **Policy** > **VLANS** > **Add** and configure the following parameters:

   Name

   test1

   Mode

   Bridged@AC

   VLAN ID

   Specify a valid VLAN ID.

   Port

   If the Mode is Bridged@AC, specify a data port.

   Layer 3

   If the Mode is Bridged@AC, provide the following Layer 3 parameters:

   - IP Address
   - CIDR
   - FQDN
   - DHCP.

     Select **Relay**, then click **Configure** to enter the DHCP Relay Server IP address.
   - Enable Device Registration. Indicates that the wireless AP or switch can us this port for discovery and registration.
   - Mgmt traffic. Indicates that this port will be used to manage traffic. Enable **Mgmt Traffic** to access the ExtremeCloud Appliance user interface through this port.
2. Click **Save**.

Next, add a network.

Related Topics

Configuring a Captive Portal Network on page 61

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 **Configure** > **Networks** > **WLANs** > **Add** and configure the following parameters:

   Network Name

   test1-ICP

   SSID

   test1-ICP

   Status

   Enable or disable the network service. Disabling the network service shuts off the service but does not delete it.

   Auth Type

   Select **WPAv2 - Personal (PSK)** then select **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 **Proxy RADIUS (Failover)**.
   - Primary RADIUS. This is the RADIUS server we configured. Enter the IP address. You have the option to add 1-3 failover RADIUS servers.
   - Default VLAN = **test1**. This is the B@AC VLAN we created.

   Default Auth Role

   The default network policy roles for an authenticated client. Select the plus sign to create a new 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:

   a. Configure the role under **Configure** > **Policy** > **Roles** and indicate that it is the Default Auth Role here.
   b. Go to **Onboard** > **Rules** and edit a policy rule, specifying **Default Auth Role** in the Accept Policy field.

   Default VLAN

   The default network topology. A topology can be thought of as a VLAN (Virtual LAN) with at least one egress port, and optionally include: sets of services, exception filters, and multicast filters. Examples of supported topology modes are Bridged at AP and Bridged at AC. Select a VLAN from the list.

2. Select **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 Topics

Working with Internal Captive Portal Engine Rules on page 62

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.

   a. Select the rule **Web Authenticated LOC: Network: Test1- ICP** and click ✎ to edit.
   b. 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 Topics

Editing Device Group Profile for Network and Role on page 62

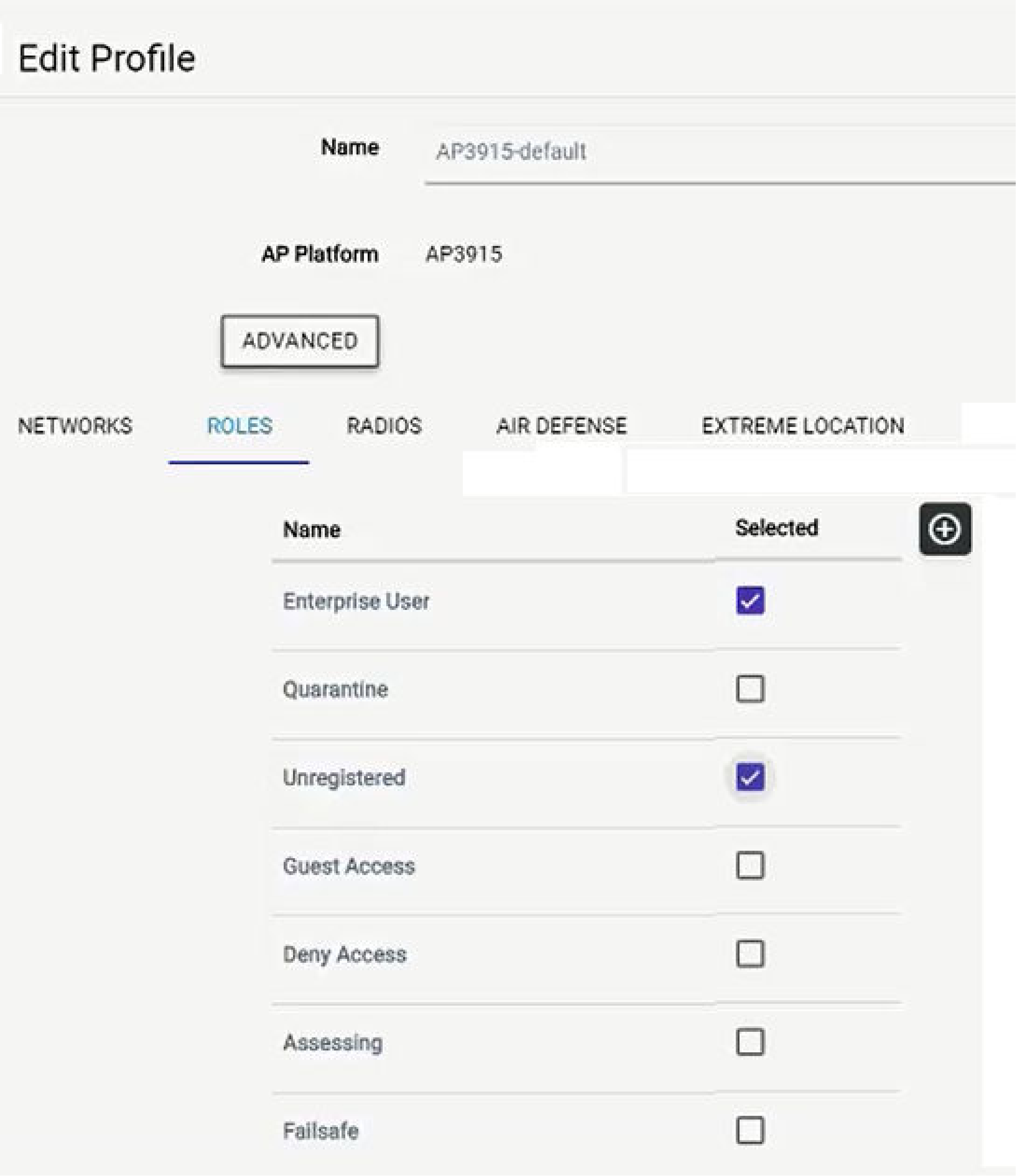
Editing Device Group Profile for Network and Role

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

1. Go to **Configure** > **Sites** and select a site.
2. Click **Device Groups**.
3. Select **DeviceGroup_AP3915**.

4. Beside the Profile field, 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.



Edit Profile

Name: AP3915-default

AP Platform: AP3915

Name	Selected
Enterprise User	☑
Quarantine	□
Unregistered	☑
Guest Access	□
Deny Access	□
Assessing	□
Failsafe	□

Figure 34: 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.

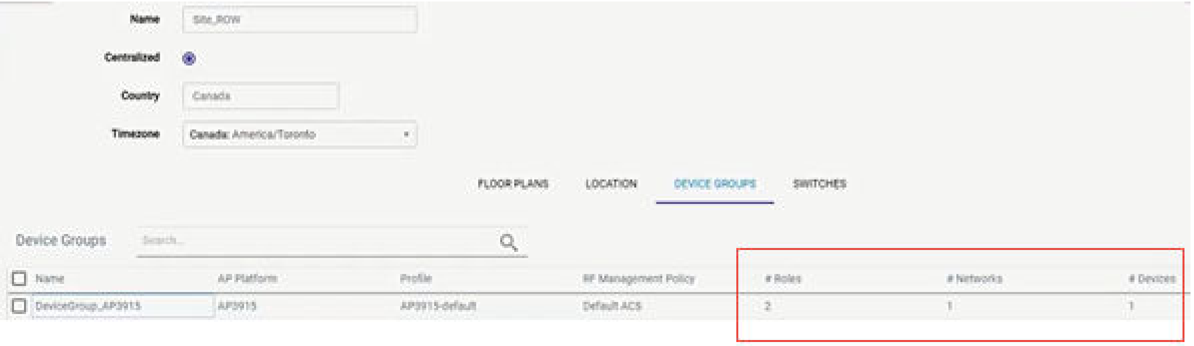
> Note
> The supported profile options depend on the AP Platform definition.

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



Name: Site_ROW

Centralized: ●

Country: Canada

Timezone: Canada: America/Toronto

□ Name	AP Platform	Profile	RF Management Policy	# Roles	# Networks	# Devices
□ DeviceGroup_AP3915	AP3915	AP3915-default	Default ACS	2	1	1

Figure 35: Centralized Site with Device Group

Next, configure adoption rules.

Related Topics

Creating Adoption Rules on page 65

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 **Configure** > **Adoption** > **Add**.
2. To create a rule for access points, select **AP**.
3. Select an Action.
4. Select a site and device group.
5. Specify a filter and select ⊕. The following are available parameters:

   IP Address/CIDR

   Filter the APs or switches by IP address, adopting APs into the specified device group based on their IP address. CIDR field is used along with IP address field to find the IP address range.

   For switch adoption rules, specify the management IP address.

   Host Name

   Filter the APs by host name, adopting APs into the specified device group based on their host name. This field matches on sub strings.

   For switch adoption rules, use the system name. The full host or system name is not required for a match.

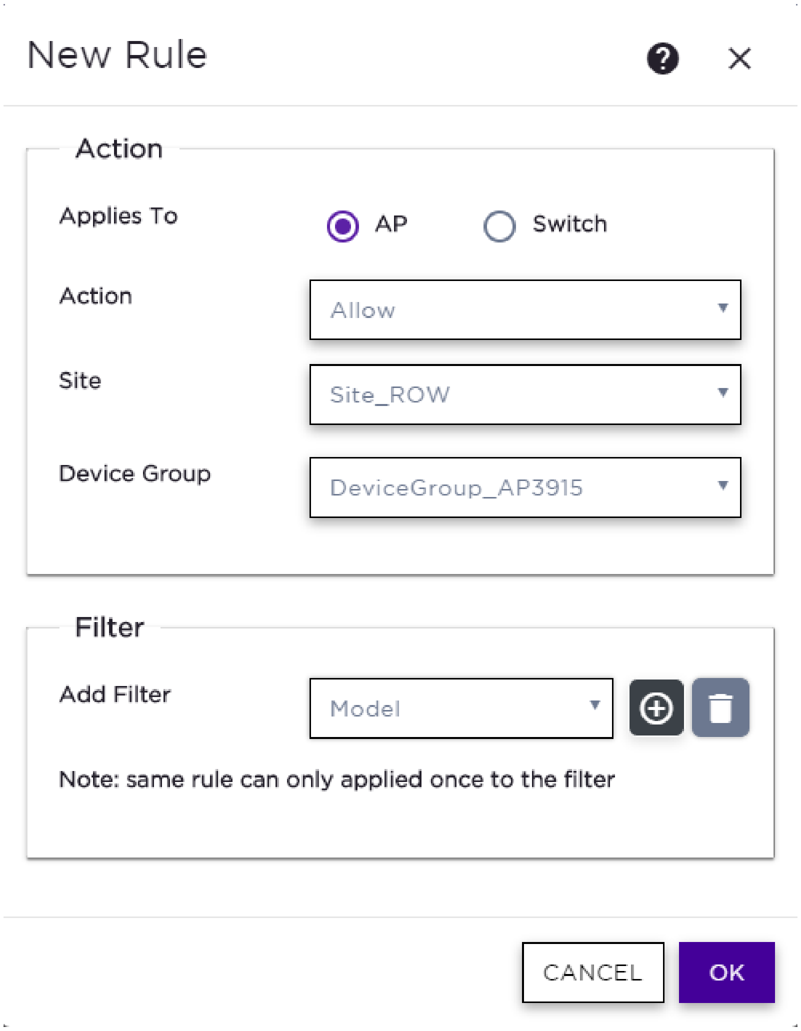
   Model

   Model number on the device. This field matches on sub strings. The full model number is not required for a match.

   Serial Number

Serial number on the device. Serial number requires an *exact* string match.

Note
Each filter value can only be applied once to a single rule.


New Rule

Action

Applies To ● AP ○ Switch

Action: Allow

Site: Site_ROW

Device Group: DeviceGroup_AP3915

Filter

Add Filter: Model

Note: same rule can only applied once to the filter

Figure 36: Create Adoption Rule

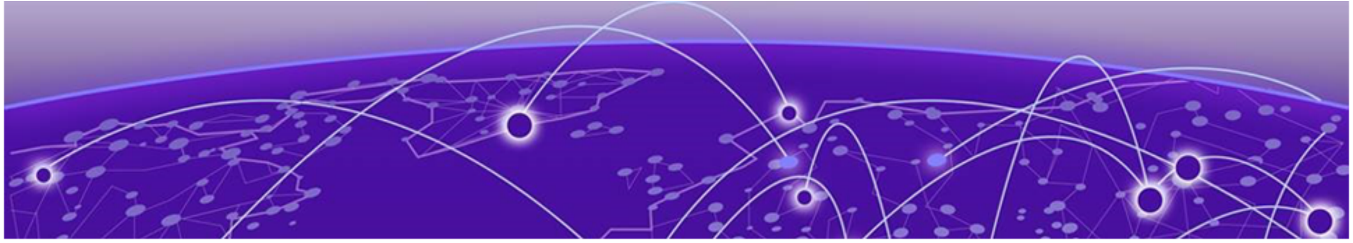
6. Select **OK**.
7. From the **Adoption Rules** page, select **Save**.

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

For more information on adoption rules, including Pattern-Based adoption and device redirection, see the *ExtremeCloud Appliance User Guide*.



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

   For more information, see Specifying B@AC Network Topology on page 60.

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

   Network Name

      Test2-AAA

   SSID

      Test2-AAA

   Status

      Enable or disable the network service. Disabling the network service shuts off the service but does not delete it.

Auth Type

WPA2 Enterprise 802.1x/EAP

AAA Policy

Local On-boarding

This option is not displayed for WLAN Networks that do not require authentication or authorization. The value **Local Onboarding** refers to RADIUS requests that are directed through the ExtremeCloud Appliance. Local Onboarding is the default value for WLAN Networks configured for Internal Captive Portal. AAA Policy can only be configured for WLAN Networks requiring MACAUTH, External Captive Portal, or EAP.

To use AAA Policy to bypass ExtremeCloud Appliance, create a policy with RADIUS servers and a NAS IP address, then specify the policy here. To get started, go to **Configure** > **AAA Policy** > **Add**. For more information, see the *ExtremeCloud Appliance User Guide* or *Online Help*.

Authentication Method

Default

Default AAA Authentication Method

Local

LDAP Configuration

None

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**.

> Note
> To activate the **Scheduling** button and schedule when network services are enabled, install the Extreme Scheduler Application on ExtremeCloud Appliance. For more information, see the *ExtremeCloud Appliance User Guide*.

Next, work with engine rules.

Related Topics

Creating an Engine Rule on page 69

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 Topics

Creating a Policy Role on page 70

Creating a Policy Role

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

To create a new policy role:

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

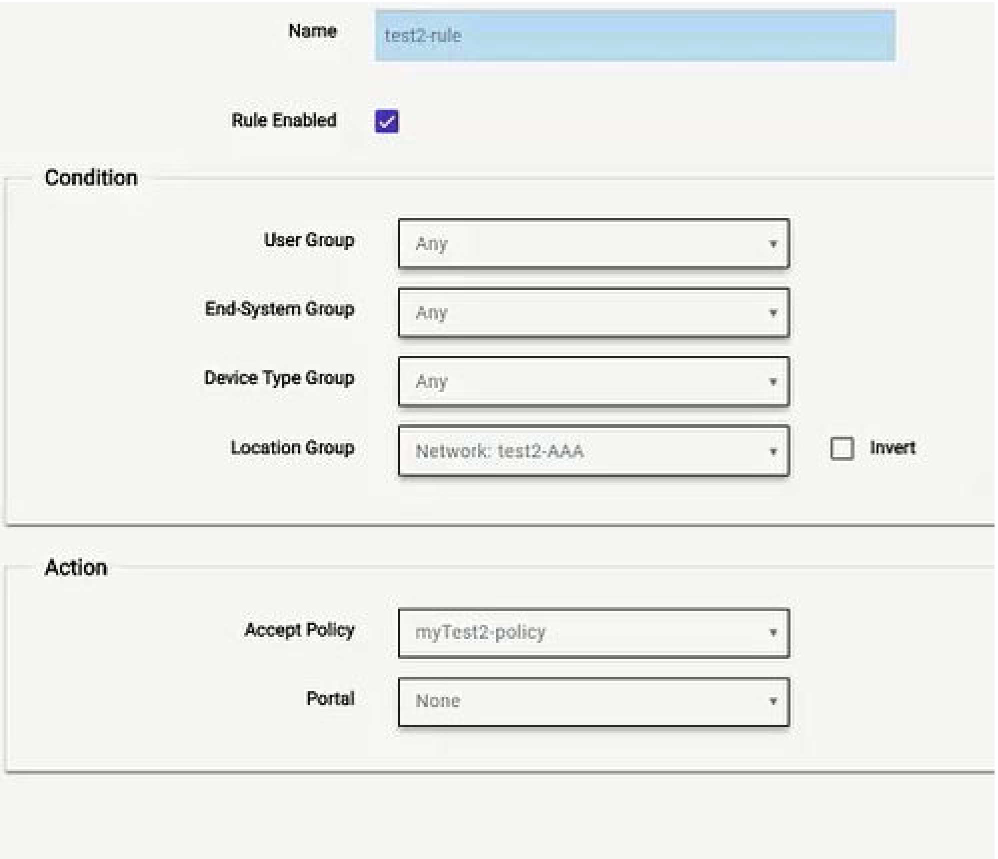
   Name

   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**.



Name: test2-rule

Rule Enabled ☑

Condition

User Group: Any

End-System Group: Any

Device Type Group: Any

Location Group: Network: test2-AAA □ Invert

Action

Accept Policy: myTest2-policy

Portal: None

Figure 37: 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 Topics

Applying a AAA Network and Role to the Device Group on page 71

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 **Configure** > **Sites** and select the site.
2. Select **Device Groups** tab.
3. Select **DeviceGroup_AP3915**.
4. Beside the Profiles field, select ✎ to edit the profile AP3915-default.
5. From the **Networks** tab, assign a radio to network **test2-AAA**.

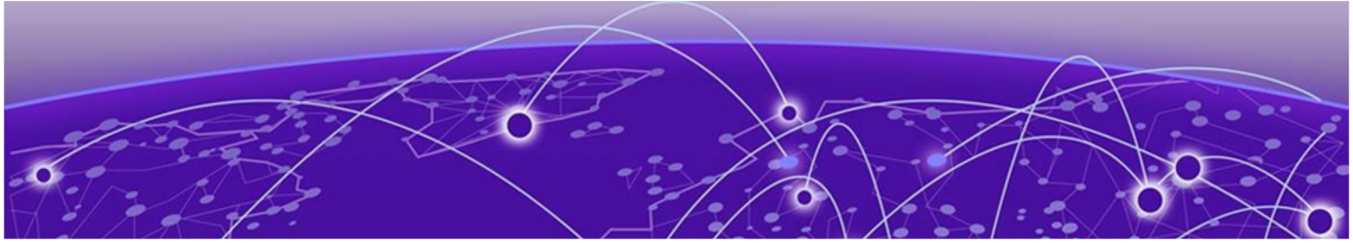
   This is the AAA network we created.

6. 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
7. Click **Save** to save the profile settings.
8. Click **Close** to close **DeviceGroup_AP3915**.

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

Related Topics

Creating Adoption Rules on page 65



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 **Configure** > **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 **Configure** > **Sites** and select a site. Then, select **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.

   - A Centralized site supports the following AP models:
     - AP39xx supporting ACS Policy for RF Management
     - AP5xx

     Note

     AP5xx currently require manual channel plan configuration when used in a Centralized site. Go to **Configure** > **Devices** > **Access Points** and select an AP5xx model. For more information, see *Configure AP Radio Settings* in the *User Guide*.

   - Default Smart RF supports APs in a Distributed site (AP7xxx, AP8xxx, and AP5xx).

   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 Topics

Configuring an Internal Captive Portal on page 59

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 **Configure** > **Policy** > **VLANS** > **Add** 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 Topics

Configuring B@AP Captive Portal Network for a Distributed Site on page 75

Configuring External Captive Portal Network on page 140

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 75.

Note

Distributed sites only support B@AP VLAN topology.

To create an Internal captive portal network with WPAv2 PSK privacy:

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

   Network Name

   ICP_B@AP_Distributed

   SSID

   ICP_B@AP_Distributed

   Status

   Enable or disable the network service. Disabling the network service shuts off the service but does not delete it.

   Auth Type

Select **WPA2 - Personal (PSK)** then select **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 **Proxy RADIUS (Failover)**.
- Primary RADIUS. This is the RADIUS server we configured. Enter the IP address. You have the option to add 1-3 failover RADIUS servers.
- Default VLAN = **B@AP Untagged**. This is the B@AP VLAN we configured under Specifying B@AP Network Topology on page 75.

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:

a. Configure the role under **Configure** > **Policy** > **Roles** and indicate that it is the Default Auth Role here.
b. 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. Select **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.

a. Select the rule **Web Authenticated LOC: Network: Test1- ICP** and click ✎ to edit.
b. 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 Topics

Editing Device Group Profile for Network and Role on page 62

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 **Configure** > **Adoption** > **Add** and select the site and device group, or filter from the following parameters:

   IP Address/CIDR

   Filter the APs or switches by IP address, adopting APs into the specified device group based on their IP address. CIDR field is used along with IP address field to find the IP address range.

   For switch adoption rules, specify the management IP address.

   Host Name

   Filter the APs by host name, adopting APs into the specified device group based on their host name. This field matches on sub strings.

   For switch adoption rules, use the system name. The full host or system name is not required for a match.

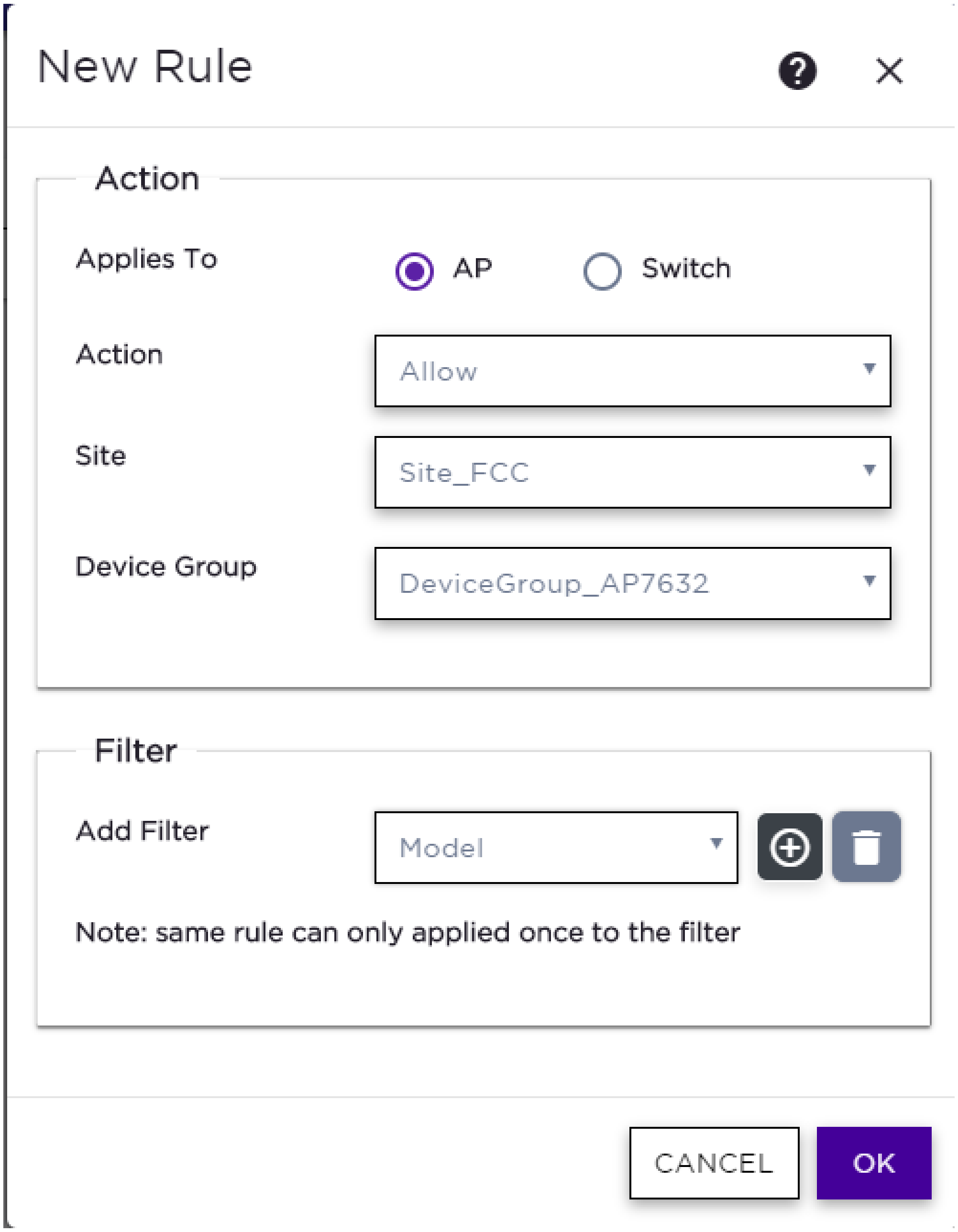
   Model

   Model number on the device. This field matches on sub strings. The full model number is not required for a match.

   Serial Number

   Serial number on the device. Serial number requires an *exact* string match.

   Note
   Each filter value can only be applied once to a single rule.



New Rule

Action

Applies To ● AP ○ Switch

Action: Allow

Site: Site_FCC

Device Group: DeviceGroup_AP7632

Filter

Add Filter: Model

Note: same rule can only applied once to the filter

Figure 38: Create Adoption Rule

2. Select **OK**.
3. From the **Adoption Rules** page, select **Save**.

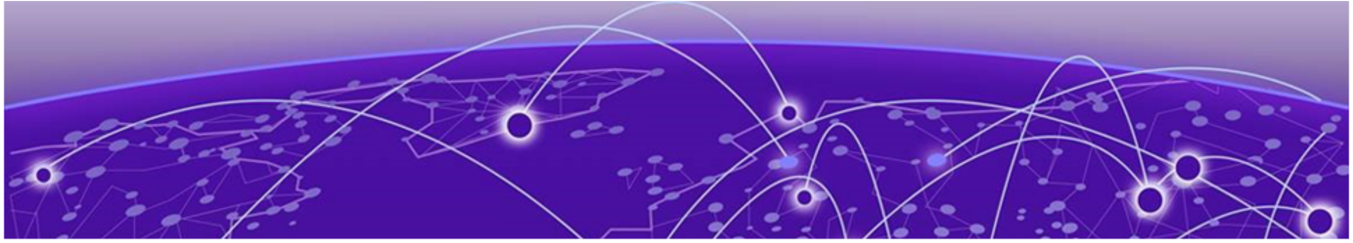
All AP7632 access points will be automatically added to **DeviceGroup_AP7632** within **Site_FCC** upon registration with ExtremeCloud Appliance.

Note

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

- AP model number
- Configuration Profile
- RF Management Profile

For more information on adoption rules, including Pattern-Based adoption and device redirection, see the *ExtremeCloud Appliance User Guide*.



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 ExtremeWireless APs:
  - AP410i/e
  - AP460i/e
  - 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.

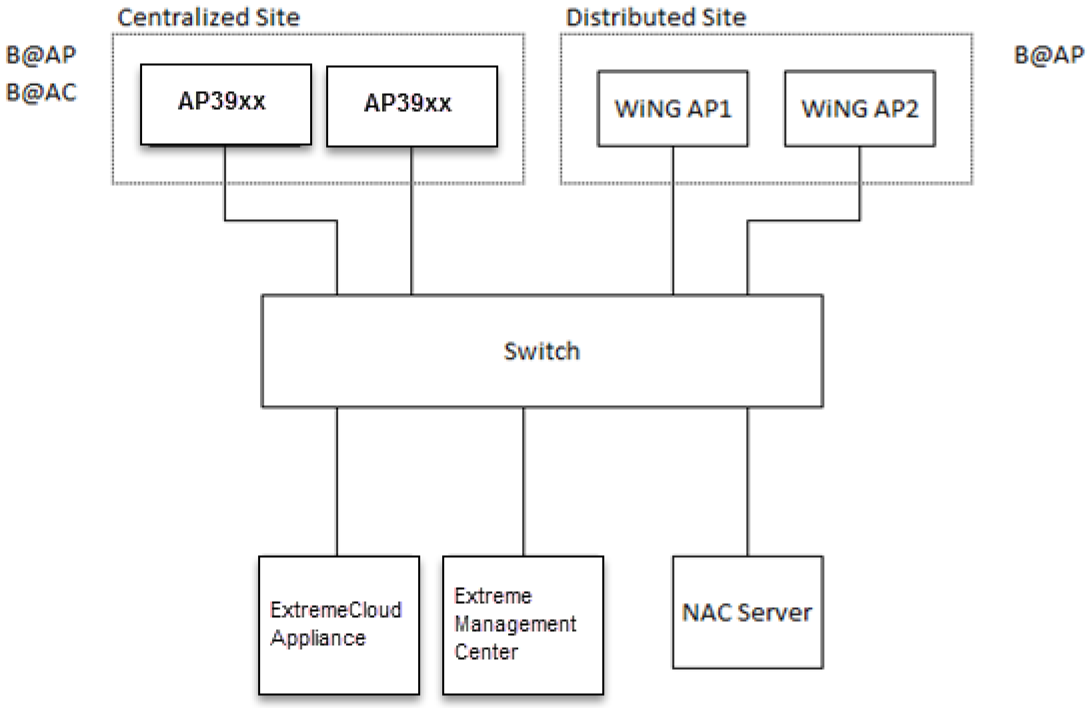


Figure 39: External NAC Server / ExtremeCloud Appliance Setup

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 (XMC) OneView page or launch the XMC console.
2. Add the external NAC server and the ExtremeCloud Appliance esa0 interface as devices to be managed by XMC.
   - Open NAC Manager using either OneView or the XMC console.
   - Add the external NAC server as an appliance to be managed.
     a. Go to **Switches** > **Add Switch**.
     b. Select the ExtremeCloud Appliance esa0 interface
     c. 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 Topics

Configuring an MBA Network on page 83

Configuring a AAA Network on page 84

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 **Configure** > **Sites** and select a site.
   - Click the **Device Groups** tab and select a device group.
   - Beside the Profile field, click ✎ 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 **Configure** > **Sites** and select a site.
   - Click the **Device Groups** tab and select a device group.
   - Beside the Profile field, click ✏ 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 Topics

Configuring an MBA Network on page 86

Configuring a AAA Network on page 87

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 **Configure** > **Sites** and select a site.
    - Click the **Device Groups** tab and select a device group.
    - Beside the Profile field, click ✎ 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 a AAA 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:

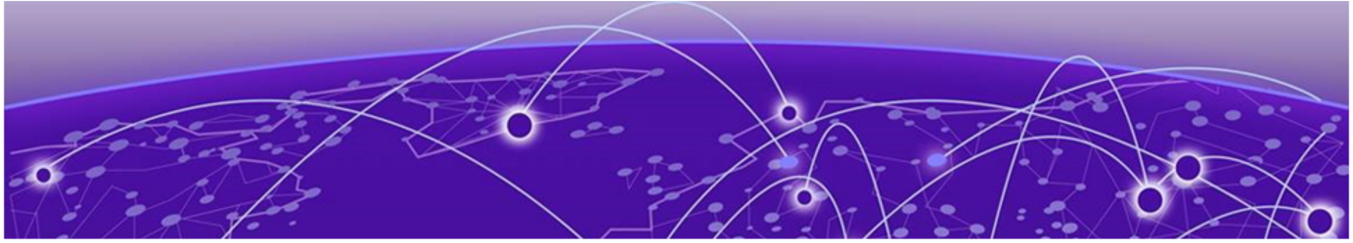
8. Assign the network created previously and its Default Auth Role to either a Centralized or Distributed site and save.

   - Go to **Configure** > **Sites** and select a site.
   - Click the **Device Groups** tab and select a device group.
   - Beside the Profile field, click ✏ 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.



NEW!

External Captive Portal on a Third-Party Server

ExtremeCloud Appliance supports integration with an External Captive Portal (ECP) on a third-party server.

An ECP is a web server that hosts a site that allows users to authenticate to the network. When the web server is not hosted on ExtremeCloud Appliance, the captive portal is considered a third-party ECP. ExtremeCloud Appliance intercepts and redirects the user's HTTP messages to the ECP web server.

ECP authentication involves filtering traffic of unauthenticated clients. When the client sends HTTP traffic, its browser is redirected to a website where the client's user can authenticate. The website is referred to as an ECP because it is located outside ExtremeCloud Appliance (which also offers an 'internal' captive portal). The ECP authenticates the user in whatever way it sees fit, and then tells ExtremeCloud Appliance or the AP whether the user is authenticated and what policy to apply to the user's session.

All interactions with the ECP are initiated by the user. The enterprise allows staff and guests to egress through port 80 on the firewall to use the third-party ECP.

We will discuss how to configure and program the ECP to interact with ExtremeCloud Appliance. This includes details about the message sequence that occurs when a client authenticates through an ECP. The following authentication flows are supported:

- A simplified flow in which ExtremeCloud Appliance accepts instructions from the ECP relayed through the client web browser.
- A more complex flow in which ExtremeCloud Appliance invokes RADIUS authentication to confirm the apparent authentication status of the client.

Firewall Friendly External Captive Portal Flow of Events

Typically, the third-party server is on the other side of a firewall from ExtremeCloud Appliance. Integrating with a third-party server through a firewall is illustrated in Figure 40 on page 91. The main participants in the deployment scenario are:

- The client being authenticated ('user').
- The ExtremeCloud Appliance that manages the AP that the user is communicating through.
- The firewall between the user and ExtremeCloud Appliance on one side and the ECP on the other.
- The ECP that performs the actual authentication.

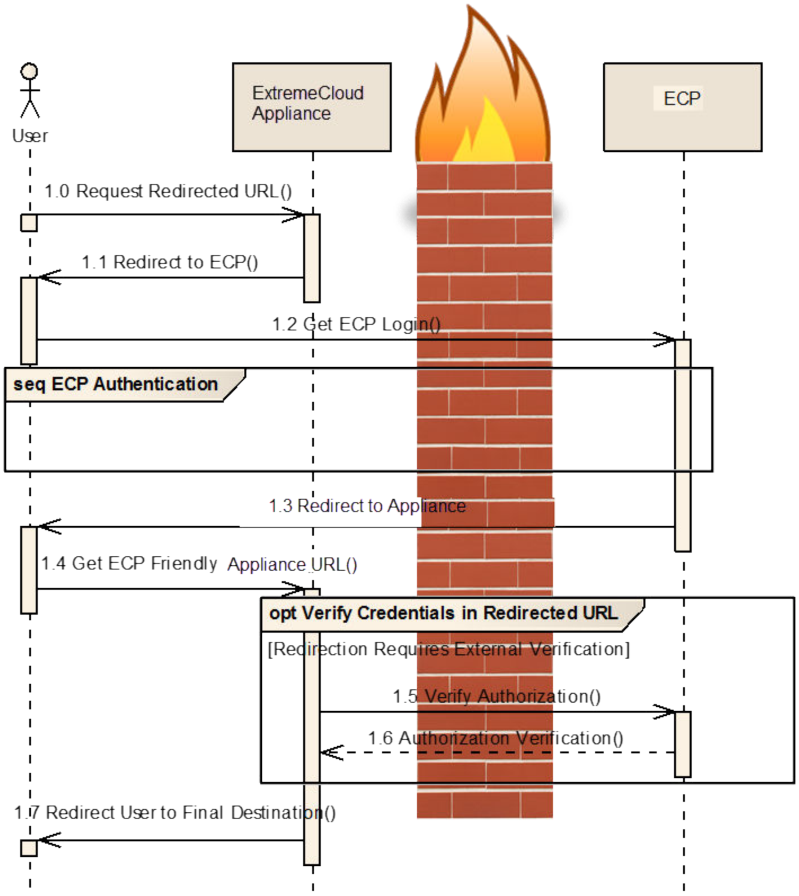

User
ExtremeCloud Appliance
ECP
1.0 Request Redirected URL()
1.1 Redirect to ECP()
1.2 Get ECP Login()
seq ECP Authentication
1.3 Redirect to Appliance
1.4 Get ECP Friendly Appliance URL()
opt Verify Credentials in Redirected URL
[Redirection Requires External Verification]
1.5 Verify Authorization()
1.6 Authorization Verification()
1.7 Redirect User to Final Destination()

Figure 40: Firewall Friendly ECP Event Flow with ExtremeCloud Appliance

FF-ECP on ExtremeCloud Appliance

The following numbered list corresponds to the numbers illustrated in Figure 40 on page 91.

1.0 - When the user sends HTTP traffic, ExtremeCloud Appliance spoofs the destination web server.

1.1 - Traffic is redirected to the ECP. ExtremeCloud Appliance tells the client's browser that the resource it is requesting has temporarily been moved to another server (the ECP) .

ExtremeCloud Appliance adds parameters to the redirection, for example: the user's MAC address, the BSSID, or AP location, and AP Ethernet MAC. All available parameters are encoded into the URL request. The client's browser typically follows the redirection automatically. The redirection contains the query parameters added by ExtremeCloud Appliance.

1.2 - Because the ECP is located on a third-party server, the user's request must be forwarded through the enterprise firewall. Most companies allow requests for port 80 to pass through the firewall. Typically, the firewall also serves as a Network Address Translation (NAT). The NAT records the state of the connection, replaces the IP address in the request, and forwards it to the ECP.

When the ECP receives the redirected request, it typically replies with a web page. The client's browser sends subsequent requests to the ECP to retrieve additional content needed to render the page. If NAT is present, and the firewall allows it, the client establishes direct connection with the ECP web server, which serves the user experience and any necessary transactions related to the captive portal experience (including login, credentials collection, and validation).

ExtremeCloud Appliance is not involved in this interaction, except to forward traffic between the ECP and the client. The interaction can be as simple or complex as necessary (represented by the box labeled *seq ECP Authentication*).

1.3 - The ECP changes the client's authentication state and role. Once the server completes the captive portal workflow, the server responds to the client, instructing the client to redirect to ExtremeCloud Appliance. The status of the ECP authentication (and possibly credentials needed to have ExtremeCloud Appliance perform final authentication of the registering client) are encoded within the response message. You can display a set of terms and conditions on the ECP web page that the user must accept before a more liberal access control role is assigned.

1.4 - The client's browser usually follows the redirection URI automatically. Assuming the URI passes basic validation, the flow proceeds in one of two ways: If the URI contains a signature (secure hash) and the hash is verified by ExtremeCloud Appliance, the appliance accepts the user as authenticated. If the URI contains the name of an access control role defined on ExtremeCloud Appliance, it applies that role to all traffic that the client sends subsequently.

1.5 and 1.6 - If the URI is unsigned and contains a user name and password, then ExtremeCloud Appliance attempts to authenticate the user against a RADIUS server. The WLAN Service that redirects to the ECP must have at least one RADIUS server configured for authentication or an error is reported.

(Optional) If the ECP returns the credentials of the registered client (with the expectation that the appliance will perform final user authentication based on those parameters), the administrator can configure ExtremeCloud Appliance with the address and the shared secret of at least one RADIUS authentication server. Instructions on how to configure a RADIUS server for a network using captive portal authentication is documented in the*ExtremeCloud Appliance User Guide* located in the Extreme Networks documentation portal: https://extremenetworks.com/documentation/extremecloud-appliance.

The response from the RADIUS server may also contain attributes, such as maximum session duration, the VLAN to which the client's traffic is assigned, and the name of an access control role to apply to the traffic the client sends subsequently. If the attributes in the response are valid, ExtremeCloud Appliance applies them to the user session.

If no specific role is returned by the RADIUS server, then ExtremeCloud Appliance applies the Authorized role that is defined in the network configuration.

Once the user is authenticated, it is assigned to a new role that does not redirect its HTTP traffic to the ECP. The client's assigned role is enforced and access is granted or restricted based on the rules defined in the Policy role. Because this is a function of the role that the client gets assigned to, it is up to the ExtremeCloud Appliance administrator to define the authenticated role appropriately. The administrator can configure ExtremeCloud Appliance to steer the client back to the initially intended URL, or redirect the client to a specific URL.

1.7 - Assuming the client is authenticated, it has internet access to the extent allowed by the authenticated role to which it is assigned.

Configure the Firewall

Configure the firewall to enable clients that are behind the firewall to forward traffic to port 80 destination on the insecure side of the firewall. Most sites configure this behavior by default. A firewall friendly ECP can require the firewall to allow ExtremeCloud Appliance to forward RADIUS requests (UDP) to an external server (typically at port 1812).

Configure an External Captive Portal

The External Captive Portal (ECP) is, essentially, a web server that runs an application allowing clients to change their authentication state, by providing credentials, credit card details, demographic information about themselves or acknowledging terms and conditions. The application can be written in any language the ECP provider chooses. The ExtremeCloud Appliance web applications are implemented in PHP, but they will interact with any programming language or library on the ECP or client that can generate valid HTTP.

If the ECP expects the controller to sign redirection responses, it is critical that the real time clocks on ExtremeCloud Appliance and the ECP are synchronized. Signed redirection responses include timestamps to protect against replay attacks. Trust the redirection responses only for a limited period of time.

The easiest way to do this is to configure both ExtremeCloud Appliance and the ECP to use Network Time Protocol (NTP) to manage the clock. The time zone needs to be set correctly, both on the ECP and on the appliance. On ExtremeCloud Appliance, go to **Administration** > **System** > **Network Time** to configure NTP.

The timestamps in signed redirection responses are in UTC (Coordinated Universal Time). There is no need for ExtremeCloud Appliance to know the ECP’s time zone and no need for the ECP to know the appliance’s time zone.

The signing algorithm is a slight variation on Amazon Web Service’s (AWS) algorithm for signing requests using query string parameters. At this time AWS makes an SDK available that includes implementations of the signing algorithms in several different languages (notably Java and PHP). It may be helpful to obtain and use this SDK rather than re-implement the signing algorithm from scratch.

Understand Processing Performed by the ECP

The ECP must receive HTTP/HTTPS redirection from ExtremeCloud Appliance, provide means for a client to become authorized, and finally redirect the user back to a web server on ExtremeCloud Appliance.

The script on the ECP that receives redirected requests has two responsibilities:

- Parse the redirection URL and preserve critical parameters for future use.
- Compose the web page that the user fills in to log into the network.

The Redirection URL Sent from ExtremeCloud Appliance

The request for the login page is in the form of an HTTP/HTTPS `GET` request. All the arguments to the request are passed as query strings appended to the URL. Typically, the web server or the back-end runtime system will parse the query strings and make them available to the back-end scripts.

The parameters that are described in Table 6 on page 94 are included in the URL statement sent from ExtremeCloud Appliance. The following parameters are required to be included in the return statement to ExtremeCloud Appliance:

- wlan
- token
- role
- user name
- password

Additional parameters are provided optionally for reporting purposes.

Table 6: Parameters Available on the Redirection URL from ExtremeCloud Appliance to the ECP

Parameter Name	Parameter Value	Required	Notes
ap		No	The AP Name to which the authenticating user has associated.
bssid	Alphanumeric String	No	The BSSID to which the authenticating client has associated. The BSSID is a MAC address belonging to the AP to which the client associated. The BSSID is in the format of six hex digits. The hex digits are “0123456789abcdef”. An example BSSID could be “00026fe9b568”. This is the same value that would be included in the Called-Station-ID field of a RADIUS Access-Request sent on behalf of this client.
ssid	A character string up to 32 bytes long	No	The SSID (Service Set Identifier) to which the client associated. ASCII-encoded hex string.

Table 6: Parameters Available on the Redirection URL from ExtremeCloud Appliance to the ECP (continued)

Parameter Name	Parameter Value	Required	Notes
dest	Alphanumeric string	No	This is the original URL that the client's browser was trying to receive when the request was redirected. The string is URI-encoded. For example, slashes in the URL are replaced by "%2F".
hwc_ip	Numeric String	No	This is the IP address to which clients should be redirected to complete authentication. Typically, an appliance ends up with many IP addresses, but only one of them will map to the WLAN service's ECP implementation. Note: This address may not be accessible directly by the ECP. However, it will be accessible to the client that is being authenticated. This attribute appears in the redirection response from the appliance. A sample hwc_ip address is "10.10.21.6".
hwc_port	ASCII-encoded numeric string	No	This the port on the appliance interface to which the client should be redirected. If ECP support is configured for HTTP then the hwc_port will be "80", otherwise it will be "443". This attribute appears in the redirection response from the appliance.
mac	ASCII-encoded hex string	No	The MAC address of the client that is being authenticated. A client could have multiple MAC addresses. This MAC address is the MAC address of the client's wireless interface that it used to associate to the wireless network. The client MAC address is in the format of six hex digits. The hex digits are "0123456789abcdef". An example "mac" could be "0023149032a8". This is the same value that would be included in the Calling-Station-ID field of a RADIUS Access-Request sent on behalf of this client.
role	Alphanumeric String	Yes	The name of the access control role to which the authenticating client is assigned at the moment of redirection. A best practice is to use the ExtremeCloud Appliance default roles.
sn	ASCII-encoded hex string	No	The serial number of the AP to which the client being authenticated associated. The serial number identifies the AP. It is assigned to the AP at manufacturing time. The serial number is a sequence of hex digits with the 'alphabetic' characters in lower case. "12b2694560000000" is an example of an AP serial number.

Table 6: Parameters Available on the Redirection URL from ExtremeCloud Appliance to the ECP (continued)

Parameter Name	Parameter Value	Required	Notes
token	Alphanumeric String	Yes	An identifier for the user’s wireless session hosted on the appliance that performed the redirection.
vlan	ASCII-encoded decimal number	No	The VLAN ID of the VLAN/topology to which the client is assigned at the moment of authentication. The VLAN ID is a number in the range 1 to 4094. The VLAN ID is the containment VLAN of the default action of the role to which the authenticating client is assigned. A role’s default action does not have to be “contain to VLAN”. If the default action is not “Contain to VLAN” then this attribute will be empty or not present.
vns	Alphanumeric String	No	The name of the Virtual Network Service (VNS) on which the client is authenticating. In ExtremeCloud Appliance,this value is treated as the `ssid-name`.
wlan	ASCII-encoded decimal string	Yes	An internal identifier for the WLAN service on which the client is authenticating. The `wlan` attribute must be present in all redirection responses (and redirected requests) sent by the appliance. The ECP must return the wlan attribute in the redirection back to the appliance that it sends to the authenticating client’s browser.
X-Amz-Algorithm	Alphanumeric String	No	The identifier for the algorithm used to compute the “X-Amz-Signature”. Only present when the appliance is configured to sign the redirection. This attribute must be present when the appliance is configured to sign the redirection. The value of this attribute is “AWS4-HMAC-SHA256” and is not configurable. The signing algorithm and the role of the identifier in it are covered in more detail in section Verifying the Signed Request on page 97.
X-Amz-Credential	Alphanumeric String	No	The identifier for the account whose shared secret was used to compute the “X-Amz-Signature”. Only present when the appliance is configured to sign the redirection. If the appliance is configured to sign the redirection then this field must be present. This is covered in more detail in section Verifying the Signed Request on page 97.

Table 6: Parameters Available on the Redirection URL from ExtremeCloud Appliance to the ECP (continued)

Parameter Name	Parameter Value	Required	Notes
X-Amz-Date	Alphanumeric String	No	This is the time at which the appliance prepared and sent the redirection back to the user's browser. The date and time are in ASCII-encoded UTC. This attribute is present if a time stamp or a signature is requested. It can be used to identify stale or replayed URLs. If the appliance is configured to sign the request this must be included in the redirection response (and the browser's redirected request).
X-Amz-Expires	Numeric String	No	This is the maximum length of time in seconds to trust the request. In other words the web request is only good until X-Amz-Date + X-Amz-Expires. After that time the URL should not be trusted as it is highly likely to have been replayed. This attribute is present only when the appliance is configured to sign the redirection to the ECP, in which case it must be present.
X-Amz-Signature	ASCII-encoded hex string	No	This is the signature computed over some of the HTTP headers and parts of the query string, presented as ASCII encoded-hex. The field is present only when the appliance is configured to sign the request.
X-Amz-SignedHeaders	Alphanumeric String	No	Which of the headers in the HTTP request were included in the input to the calculation of the signature. This is present only when the appliance is configured sign the redirection to the ECP, in which case it must be present.

Verifying the Signed Request

When the controller is configured to include signatures, it is easy for the ECP to ignore them. The ECP simply extracts the information it is interested in from the provided attributes and ignores the rest.

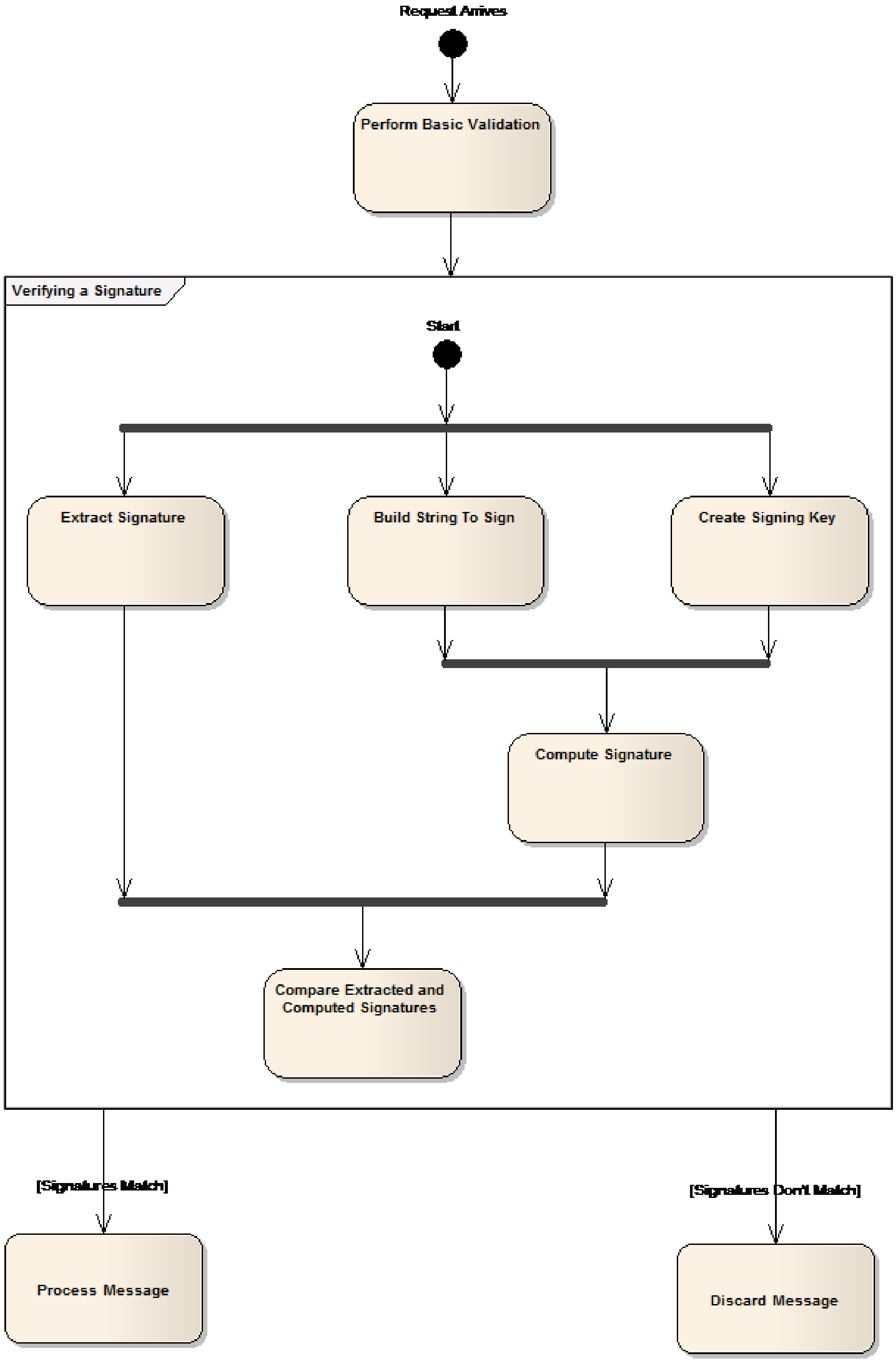
However, it is highly likely that an administrator that enables response signing wants to use the signatures to authenticate the redirected requests it receives. This section covers how to do that. The whole process is shown in Verifying a Signed Request Basic Validation Checks on page 100.

The algorithm used to sign the redirection response (and therefore the redirected request to the ECP) is based on Amazon Web Services API Signature Version 4. AWS documentation refers to this approach as "Pre-signed URLs".

Basic Steps

The basic steps for verifying the signature are:

1. Perform basic validation on the request message (are all required fields present, is the date current?). If these validations fail, there is no point in computing the signature.
2. Extract the signature from the received request.
3. From the received request, construct the string over which the signature will be computed. All but one component of this string come from the query parameters.
4. Generate the signing key. The shared secret is used to generate a signing key and is not itself the signing key.
5. Generate the signature using the signing key and the constructed string.
6. Compare the extracted signature (X-Amz-Signature) to the signature just computed. If they do not match, the request is invalid and should be discarded.


Request Arrives
Perform Basic Validation
Verifying a Signature
Start
Extract Signature
Build String To Sign
Create Signing Key
Compute Signature
Compare Extracted and Computed Signatures
[Signatures Match]
[Signatures Don't Match]
Process Message
Discard Message

Verifying a Signed Request Basic Validation Checks

The following items can be considered when validating the redirect prior to computing the signature:

1. Does the request contain a token parameter, a WLAN parameter, and a destination URL? If not, the request either did not come from the controller or was tampered with en route.
2. If the request contains a timestamp, does the timestamp meet the following requirement:

```
timestamp <= now <= timestamp + x_amz_expires
```

Or if an allowance for clocks being out of sync is made,

```
timestamp - fuzz <= now <= timestamp + x_amz_expires
```

If not, the request is invalid, possibly the result of a user bookmarking the ECP landing page on a previous visit. The request should be rejected or discarded.

1. Are all parameters formatted in accordance with the descriptions?
2. Are all parameters required for the signature present in the request?

The first 1/3 of “verifyAwsUrlSignature” and the private method “validateQueryParms” in section crypt_aws_s4.php on page 154 provide examples of performing these types of checks in PHP.

Extracting the Signature from the Request

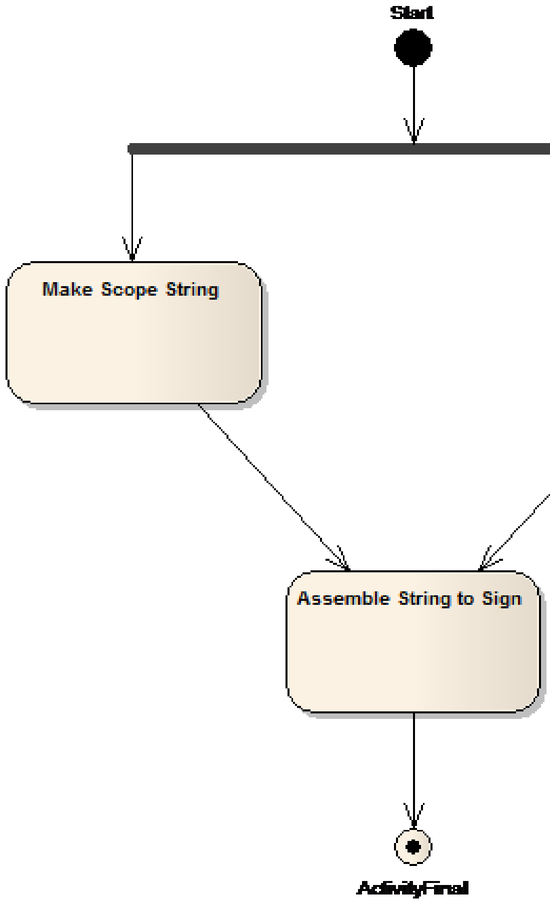
The signature is in the “X-Amz-Signature” query string parameter. Obviously the signature itself can’t be included in the computation of the signature so it must be removed from the request and set aside for later comparison. How the signature is removed from the request will depend on the program language and framework used to implement the external captive portal. The method “simpleaws::verifyAwsUrlSignature” in crypt_aws_s4.php on page 154 illustrates one way to remove the signature when the query parameters are in a PHP array.

Building the String to Sign

Figure 41 shows the main actions required to build the string that will be signed out of the request:

1. Build the scope string.
2. Build a “canonicalized” version of the request.
3. Assemble the scope string, the canonicalized string, and some additional inputs to create the string to sign.

The scope string is easy to build out of a valid request. It is made from parts of the string in the “X-Amz-Credentials” parameter. If the credentials are valid then the scope string can be created by un-escaping the forward slashes it contains (i.e. replace ‘%2f’ with ‘/’), and then taking all the characters to the right of the first forward slash. The scope ends up being the fully qualified credential, less the identity string.



Note

Parts of the Scope

The fully qualified Amazon credential consists of:

- An identity string (the one configured in the controller GUI).
- The date portion of the X-Amz-Date.
- A region string. For a real Amazon application this is one of the geographic service regions defined by Amazon. The service region is not critical for the FF-ECP implementation so it is always set to 'world'.
- A service identifier. The service is always set to 'ecp'.
- The identifier 'aws4_request', which identifies the signature version.

Figure 41: Steps in Building the String to Sign

The canonicalized request string has the format:

```
"GET\n"
.<URL-Path-Component>."\n"
.<URL-Query-Parameters>."\n"
.'host:'.<URL-Host>
."\n\nhost\nUNSIGNED-PAYLOAD";
```

Where:

- `GET` is the request type. For FF-ECP this will always be the literal “GET.”
- `<URL-Path-Component>` is the substring beginning with the ‘/’ at the end of the host or host-plus-port portion of the URL and either the end of the URL or the ‘?’ marking the beginning of the query parameter string. For example, the URL-Path-Component of `https://192.168.18.152:5825/adir/bdir/cdir/resource.htm?x=7&y=gg` is `/adir/bdir/cdir/resource.htm`
- `<URL-Query-Parameters>` is the substring following the ‘?’ character and extending either to the end of the URL or up to but not including the ‘#’ fragment character.
- `<URL-Host>` is the host portion of the URL string. It excludes any port number included in the URL. In the preceding URL, the URL-Host is 192.168.18.152.
- ‘`.`’ is the catenation operator.
- The remaining components are literals that should be added to the string as-is.

Finally the string that will actually be signed is composed as:

```
"AWS4-HMAC-SHA256\n"
.<Date>."\n"
.<scope>."\n"
.sha256(<canonicalized-request-string>)
```

where

- `AWS4-HMAC-SHA256` is a literal identifying the overall signing algorithm being used.
- `<Date>` is the value of the “X-Amz-Date” parameter extracted from the redirected request.
- `<Scope>` is the scope string that was assembled as described above.
- `<canonicalized-request-string>` is the canonicalized request string assembled as described above.
- `sha256()` is a procedure that applies the standard sha256 algorithm to the canonicalized-request-string. Its output should be in the form of a string of lowercase hex digit characters.

Creating the Signing Key

The process for generating signatures uses symmetric key encryption. The controller and the ECP use a shared key (the one configured on the controller’s WLAN Service’s captive portal configuration dialog) and the same encryption algorithm to generate and validate the signature.

The shared key is not used directly. Instead it is used to generate a secure hash (“HMAC”) that is then used as the key to sign the request. The process for creating the key is shown below in Figure 42.

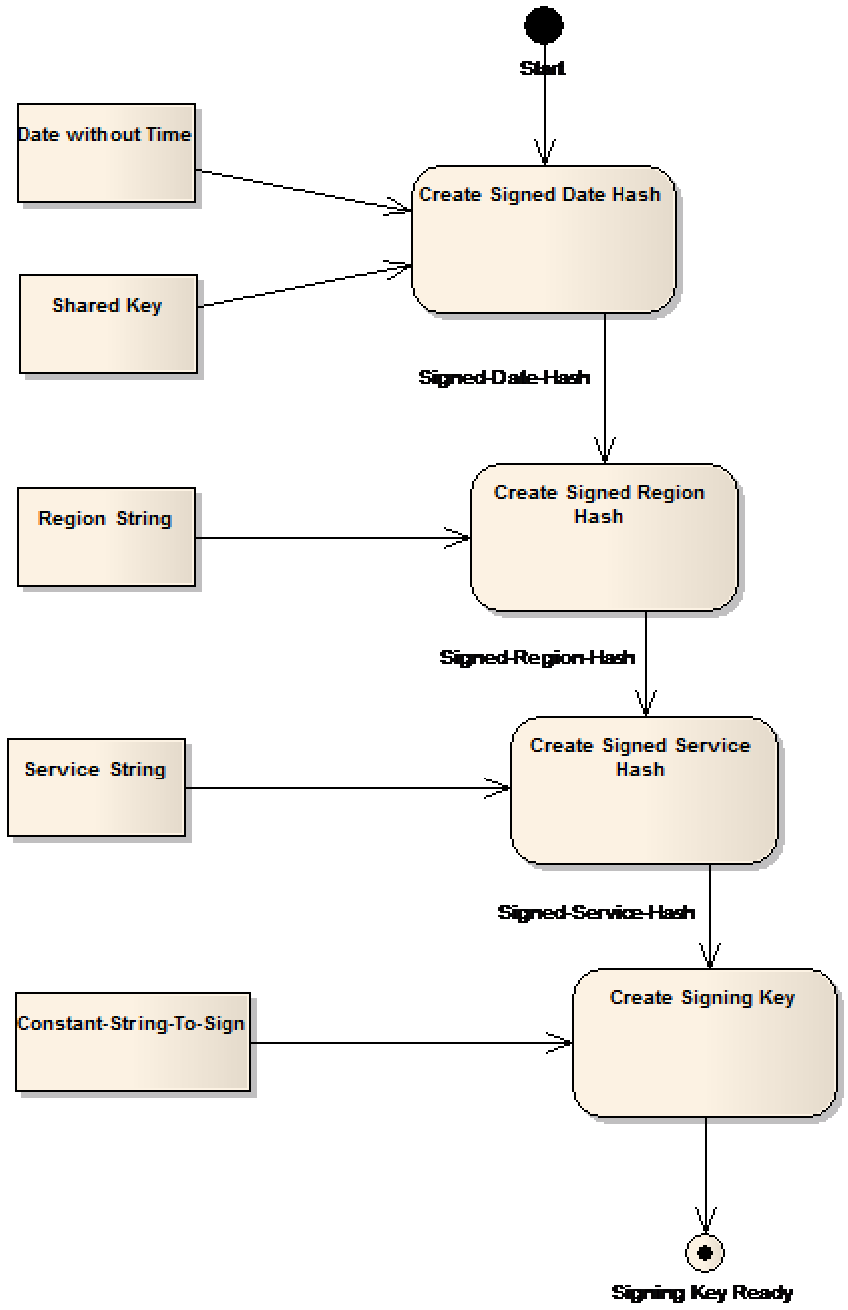


Figure 42: Creating the Signing Key

In the above figure:

1. “Date without Time” is the first 8 characters in the “X-Amz-Date” attribute, which corresponds to the date only in “YYYYMMDD” format.
2. “Shared Key” is the shared key configured on the controller. It is the shared key that is paired with the identity used to create the “X-Amz-Credential” attribute in the redirected request.

3. “Region String” is the region component of the Scope string.
4. “Service String” is the service component of the Scope string.
5. “Constant-String-To-Sign” is the string “aws4_request”.

And each of the “Create...” actions consists of generating a secure HMAC using SHA256 from the inputs. The output secure hash is in binary format (not encoded as a hex character string). The output of each step acts as the signing key for the subsequent step. The signing key for the first step is the shared secret, pre-pended with the literal ‘AWS4’.

Note that for any given identity the correct signing key only needs to be computed once per day. If the calculations are cached the cache should include an entry for the previous day to cope with the request being sent just before midnight UTC. The previous day’s key only needs to be kept for a small overlapping period (perhaps 10 minutes at the most).

Creating the Signature and Verifying the Request

At this point the signature for the request is computed as a secure HMAC using SHA256. The signing key is created as described in Creating the Signing Key and the string to sign is created as described in Building the String to Sign on page 100.

Verifying the signature in the request consists of standard string comparison between the transmitted and computed keys. If they aren’t identical the request is invalid. The client can be sent a web page containing a generic reject message or the request can be discarded silently.

Compose the Login or Splash Screen Page

How you create the login page depends on the programming language and toolset you use. This is largely outside the scope of this document. You can use any programming language that can be used for web development to create an external captive portal.

The content on the login page depends on the overall environment the ECP serves. It can contain as little as terms and conditions and a button to indicate acceptance, or it can contain fields necessary to submit a user ID and password.

The redirected request contains the attributes configured on the ECP configuration dialog. Attributes can be used to decorate the login page, and other information can be input to the authentication process. For example, a user may be considered authenticated only after logging in from one of a specific set of APs.

Approve the Client

Typically, users submit credentials for authentication into an ECP. The credentials are submitted in an HTTP “post”. The post invokes a script on the ECP web server passing the user’s credentials to the script as arguments. Write the script that is adapted to your specific requirements.

The script file can have any name. For this example, the script is named “login.php”. The script can be written in any programming language that supports web development. For this example, the script is written in PHP.

The main job of the “login.php” script is to co-ordinate the client’s browser, the back-end authentication server, and the appliance. The “login.php” script takes the submitted credentials, sends them to an authentication server, and waits for the server's reply. The exact steps taken here depend on the selected programming language, operating system, and the type of authentication server selected.

After the authentication server has verified the user and potentially returned an access control role to assign to the user, the script needs to tell the appliance that the user is authenticated and indicate the role to assign to the user. The ECP informs the appliance by putting the information in the query string of a redirection response. The redirection response sends the client's browser to a web server running on a specific interface and port of the appliance that hosts the client's session. The client's browser normally sends a redirected request immediately and automatically.

The redirection response does not need to be signed. If it is not signed, the appliance does not use the session attributes that are included in the redirected request. Instead, the appliance expects the redirected request to include a user ID and password. These credentials are sent to a RADIUS server in a standard RADIUS Access-Request. The redirected request is considered *invalid* if:

- The redirected request is not signed, and
    - The redirected request does not contain a user ID or password, or
    - The WLAN Service the client is using does not have at least one RADIUS server configured for authentication.

An invalid redirected request is sent to a standard error page. The error page cannot be configured at this time.

Compose the Redirection Response Sending the Browser back to the Appliance

Signing the Redirection to ExtremeCloud Appliance

Signing the redirection response is a similar process to calculating the expected signature for a URL that was received at the ECP. In fact, it is the same algorithm, but the inputs to the algorithm are not taken from the request as the request is under construction.

There are only two steps involved in signing the redirection response from the ECP:

1. Compose the pre-signed redirection URL to be signed.

   This step consists of building the request URL as described in Case 1: When a RADIUS Server Authenticates the Client on page 106 or Case 2: When the ECP is the Final Authority on page 107 but leaving off the `X-Amz-`... parameters that are required for the signature.
2. Sign the URL, adding all parameters to the URL that are required to sign it.

   This step consists of generating the signature, then appending all the `X-Amz-`... parameters used to the URL. This processing is described in Building the String to Sign on page 100, Creating the Signing Key on page 102, and Creating the Signature and Verifying the Request on page 104.

Related Topics

Case 1: When a RADIUS Server Authenticates the Client on page 106

Case 2: When the ECP is the Final Authority on page 107

Case 1: When a RADIUS Server Authenticates the Client

In this scenario, the ExtremeCloud Appliance redirection response includes the following:

- ExtremeCloud Appliance port and IP address or FQDN. The ECP can then cache this information and use it later to compose its redirection response.
- The token and WLAN ID.
- A user name and password that can be treated as the user's RADIUS credentials. These credentials must satisfy the standard requirements for RADIUS User-Name and User-Password attributes.

In order to trigger RADIUS authentication, the redirection response must not be signed.

If the appliance is configured to redirect successfully authenticated clients to their original destination, then the ECP must include in its redirection response, the "dest" parameter that was included in the appliance's redirection response.

The syntax of an unsigned ECP redirect to the appliance is:

```
[http | https]://<controller-IP-address-or-FQDN>{: <port>}/ext_approval.php?
token=<token>&wlan=<wlanid>&username=<userid>&password=<password>{&dest=<dest>}
```

Where

- {...} denotes an optional component of the URL.
- [http | https] is either "http" or "https" depending on how the WLAN service's captive portal is configured.
- :// is the literal string.
- <controller-IP-address-or-FQDN> is the appliance's IP address or Fully Qualified Domain Name. Since the appliance receives the redirect at the default HTTP or HTTPS port it does not need to be included in the redirect.
- {: <port>} is a literal colon, followed by the appliance port to which the client is redirected. The port is optional. Only include it if the port is not port 80 or port 443.
- /ext_approval.php is the literal string. It is the name of the script that is invoked on the appliance when the redirect is received there.
- <token> is the token taken from the redirect to the ECP.
- <wlanid> is the numeric identifier for the client's WLAN Service as taken from the appliance's redirect to the ECP.
- <userid> is the user name the appliance to sends to the RADIUS server to authenticate this user.
- <password> is the password associated with the given user ID.
- <dest> is the original destination the client was trying to reach, as reported in the appliance's redirect to the ECP.

The order of the parameters in the query string is not important.

Examples of the redirection from the ECP to the appliance expressed as a URL are:

```
https://10.21.15.42/ext_approval.php?token= OakRQ7uFYOH5E8dVD4PgvQ!!
&wlan=1&username=argon32&password=6Z*_aL40q!&dest=www.google.com
```

or

```
http://10.21.15.42/ext_approval.php?token= OakRQ7uFYOH5E8dVD4PgvQ!!
&wlan=1&username=argon32&password=6Z*_aL40q!
```

The parameters in the redirection response are summarized in the table below.

Table 7: Parameters in the Redirection to ExtremeCloud Appliance, using RADIUS authentication

Parameter Name	Parameter Value	Mandatory	Notes
wlan	Numeric String	Yes	An identifier for the WLAN Service that the client is using to access the network.
username	Alphanumeric String	Yes	The user ID is mandatory even if the URL is signed. It is used to identify the client in reports and accounting messages, even if it is not used to authenticate the client.
password	Alphanumeric String	Yes	The password is mandatory if the client is to be authenticated using RADIUS. It must be the password that the authenticating RADIUS server associates with the user ID.
dest	URL	Conditional	The dest parameter is required only if the appliance is configured to redirect the client to its original destination. The appliance directs the client's browser to an error page if it is configured to redirect to the original destination and the dest parameter is not returned to the appliance.

Related Topics

Signing the Redirection to ExtremeCloud Appliance on page 105

Case 2: When the ECP is the Final Authority on page 107

Case 2: When the ECP is the Final Authority

If the ECP makes the final authentication and authorization decision, it must sign the redirection response it sends to the client's browser. If it signs the redirection, it can include options that the appliance applies to the authorized client's session, including an access control role and the maximum duration for the client's session. Table 6 on page 94 lists all the parameters that can appear in a signed redirection response from the ECP, and which of them are mandatory in this case.

The syntax of an unsigned ECP redirect to the appliance is:

```
[http | https]://<controller-IP-address-or-FQDN>{: <port>}/ext_approval.php?
token=<token>&wlan=<wlanid>&username=<userid>{&dest=<dest>}{&role=<rolename>}{&opt27=<max-
seconds-duration>}&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=<Scoped-
Credential>&X-Amz-Date=<YYYYMMDDThhmmssZ>&X-Amz-Expires=<duration>&X-Amz-
SignedHeaders=host&X-Amz-Signature=<signature>
```

Where

- {...} denotes an optional component of the URL.
- [http | https] is either "http" or "https" depending on how the WLAN service's captive portal is configured.
- :// is the literal string.
- <controller-IP-address-or-FQDN> is the appliance's IP address or Fully Qualified Domain Name.

- {: <port>} is a literal colon (:), followed by the TCP/IP port number to which the client is redirected. The port is optional. Include it only if the port is not port 80 or port 443.
- /ext_approval.php is the literal string. It is the name of the script that is invoked on the appliance when the redirect is received there.
- <token> is the token taken from the redirect to the ECP.
- <wlanid> is the numeric identifier for the client's WLAN Service as taken from the appliance's redirect to the ECP.
- <userid> is the user name the appliance sends to the RADIUS server to authenticate this user.
- <dest> is the original destination the client was trying to reach, as reported in the appliance's redirect to the ECP.
- <rolename> is the name of a role defined on ExtremeCloud Appliance that will be applied to the remainder of the client's session.
- <max-seconds-duration> is a positive integer representing the maximum duration of the client's session.
- X-Amz-Algorithm=AWS4-HMAC-SHA256 is a literal string embedded in the signed URL.
- <Scoped-Credential> is a credential in the format: <identity>/<YYYYMMDD>/world/ecp/aws4_request.
- <YYYYMMDDThhmmssZ> is the date and time at which the redirection response was sent by the ECP, in ISO 8601 compatible format.
- <duration> is a positive integer indicating the maximum duration after the X-Amz-Date that the request should be honored.
- X-Amz-SignedHeaders=host is a literal string constant.
- <Signature> is the actual signature computed over the redirection response.

The order of the parameters in the query string is not important.

The following is an example of a signed redirection response that assigns the user to a role called "Guest_Access" and limits the session duration to 10 hours:

```
https://10.10.21.6/ext_approval.php?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=BigAuthInc%2F20140729%2Fworld%2Fecp%2Faws4_request&X-Amz-
Date=20140729T153754Z&X-Amz-Expires=60&X-Amz-SignedHeaders=host&dest=http%3A%2F
%2F1.2.3.4%2Fnews.com&opt27=36000&role=Guest_Access&token=T7vb1LdUZmsuY0q9V60Iww
```

```
%21%21&username=test&wlan=1&X-Amz-
Signature=48389399c4b9e237ff64bbbd203a9abe272b8df513dff1eae8202df82ceb2c34
```

Table 8: Parameters that can be included in a Signed Redirection Response from the ECP

Parameter Name	Parameter Value	Mandatory	Notes
dest	URL	Conditional	The <dest> parameter is required only if the appliance is configured to redirect the client to its original destination. The appliance directs the client's browser to an error page if it is configured to redirect to the original destination and the <dest> parameter is not returned to the appliance.
opt27 In the RADIUS protocol option number 27 is the Session-Timeout attribute.	Base 10 Number	No	The maximum amount of time, in seconds, that the current session can last before being terminated. If not specified, the default for the WLAN Service is applied to the authenticated client.
role	Alphanumeric String	No	The name of an access control role defined on ExtremeCloud Appliance. The appliance applies this role to the remainder of the authorized client's session. If a role parameter is not provided, the appliance uses the default authenticated role of the VNS that the authenticated client is accessing.
token	Alpha-numeric String	Yes	An identifier for the user's wireless session hosted on the appliance that performed the redirection.
username	Alpha-numeric String	Yes	The user name is mandatory even if the URL is signed. It is used to identify the client in reports and accounting messages, even if it is not used to authenticate the client.
wlan	Numeric String	Yes	An identifier for the WLAN Service that the client is using to access the network.
X-Amz-Algorithm	Alpha-numeric string	Yes	The identifier for the algorithm used to compute the "X-Amz-Signature". This attribute must be present when the ECP is acting as the final authorizing authority. The value of this attribute is "AWS4-HMAC-SHA256" and is not configurable. The signing algorithm and the role of the identifier in it are covered in more detail in section Verifying the Signed Request on page 97.

Table 8: Parameters that can be included in a Signed Redirection Response from the ECP (continued)

Parameter Name	Parameter Value	Mandatory	Notes
X-Amz-Credential	Alpha-numeric string	Yes	The identifier for the account whose shared secret was used to compute the "X-Amz-Signature". Mandatory if the ECP signs the redirection response in order to act as the final authorizing authority. The credential has the format: `<identity>/<YYYYMMDD>/world/ecp/aws4_request` where: • <identity> is the identity configured for the ECP on the appliance in the WLAN Service's ECP configuration. • <YYYYMMDD> is the year, month, and day extracted from X-Amz-Date. • world/ecp/aws4_request is a constant literal string that scopes the request.
X-Amz-Date	Alpha-numeric string	Yes	This is the date and time at which the appliance prepared and sent the redirection back to the user's browser. The date and time are in ASCII-encoded UTC and has the format: `YYYYMMDDThhmmssZ` This attribute must be present if the ECP signs the redirection response to indicate that it is the final authorizing authority.
X-Amz-Expires	Numeric String	Yes	This is the maximum length of time in seconds that the appliance should trust the redirection response. In other words a signed redirection response from the ECP will be treated as valid only until X-Amz-Date + X-Amz-Expires. This attribute is mandatory if the ECP signs the redirection response.
X-Amz-Signature	ASCII-encoded hex string	Yes	This is the signature computed over some of the HTTP headers and parts of the query string, presented as ASCII encoded-hex. The field must be present if the ECP signs the request in order to act as the final authorizing authority.
X-Amz-SignedHeaders	Alpha-numeric String	Yes	Which of the headers in the HTTP request were included in the input to the calculation of the signature. This is present only when the appliance is configured sign the redirection to the ECP, in which case it must be present.

Related Topics

Signing the Redirection to ExtremeCloud Appliance on page 105

Case 1: When a RADIUS Server Authenticates the Client on page 106

Deploying XMC as External Captive Portal

Deployment Strategy

The following strategy outlines how to configure ExtremeCloud Appliance to integrate with Extreme Management Center (XMC), 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.

   Enable Captive Portal

   Check this option and specify the following parameters:

   Captive Portal Type

   External

   ECP URL

   (http/https)://<access engine fqdn>/static/index.jsp

   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.

   > Note
   > Walled Garden rules are not required for this network. The process of enabling a captive portal on the network automatically creates rules allowing DNS, DHCP, and redirection rules. However, if users are unable to connect to the network, consider creating specific DNS and DHCP Allow rules as a Walled Garden configuration.

```
The following are rule examples:
Unregistered role for ECA_Guest:acfilters# show
Custom AP Filters: disable
filter 1 3 proto udp eth 800 mac any 0.0.0.0/0 port 53 in dst out src allow
filter 2 3 proto udp eth 800 mac any 0.0.0.0/0 port 67 in dst out src allow
filter 3 3 proto any eth any mac any 0.0.0.0/0 all_ports in none out src allow
filter 4 3 proto icmp eth 800 mac any 0.0.0.0/0 type-code 0x0000 0x0000 in dst out
src allow
filter 5 3 proto tcp eth 800 mac any 1.1.1.1/32 all_ports in dst out src allow
filter 6 3 app-signature group "Web Applications" hostname
"fqdn:nac_engine.mynetwork.com" proto any eth 800 mac any 0.0.0.0/0 all_ports in
dst out src allow
filter 7 3 proto tcp eth 800 mac any 0.0.0.0/0 port 80 in dst out none redirect
filter 8 3 proto tcp eth 800 mac any 0.0.0.0/0 port 443 in dst out none redirect
```

   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**.

   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

Authentication Method

RADIUS

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

Default VLAN

Bridged at AP Untagged

2. Select **Advanced** and configure the following parameters:

RADIUS Accounting

Enabled

Pre-authenticated idle timeout

Default value: 300 seconds

Post-authenticated idle timeout

Default value: 1800 seconds

Maximum session timeout

Default value: 0 seconds

End-systems are re-authenticated on ExtremeCloud Appliance, not from the Extreme Management Center Access Control Engine. Therefore, ExtremeCloud Appliance ignores Extreme Management Center re-authentication requests to modify filter-ids (policies). Modification of these timeout values initiates re-authentication from the ExtremeCloud Appliance to the Extreme Management Center Access Control Engine, resulting in modification of the policy/filter-id as expected.

Note

There may be a delay or network interruption on policy changes. Adjust the timeout values if you do not see a timely policy change or if you experience network interruptions during the connection attempts from clients.

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 **Configure** > **Sites** and select a site.
2. Click **Device Groups** tab.
3. Select your configured device group.
4. Beside the Profile field, 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 creates the following:

   - Unregistered role for <network name>

   External Captive Portal networks use the Unregistered role for <network name> by default. We are going to modify this to explicitly configure end system traffic coming from the ExtremeCloud Appliance network. We will create a policy mapping to the Unregistered role for <ECA Network> without actually creating the policy in the NAC policy domain.

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

   Accept Policy

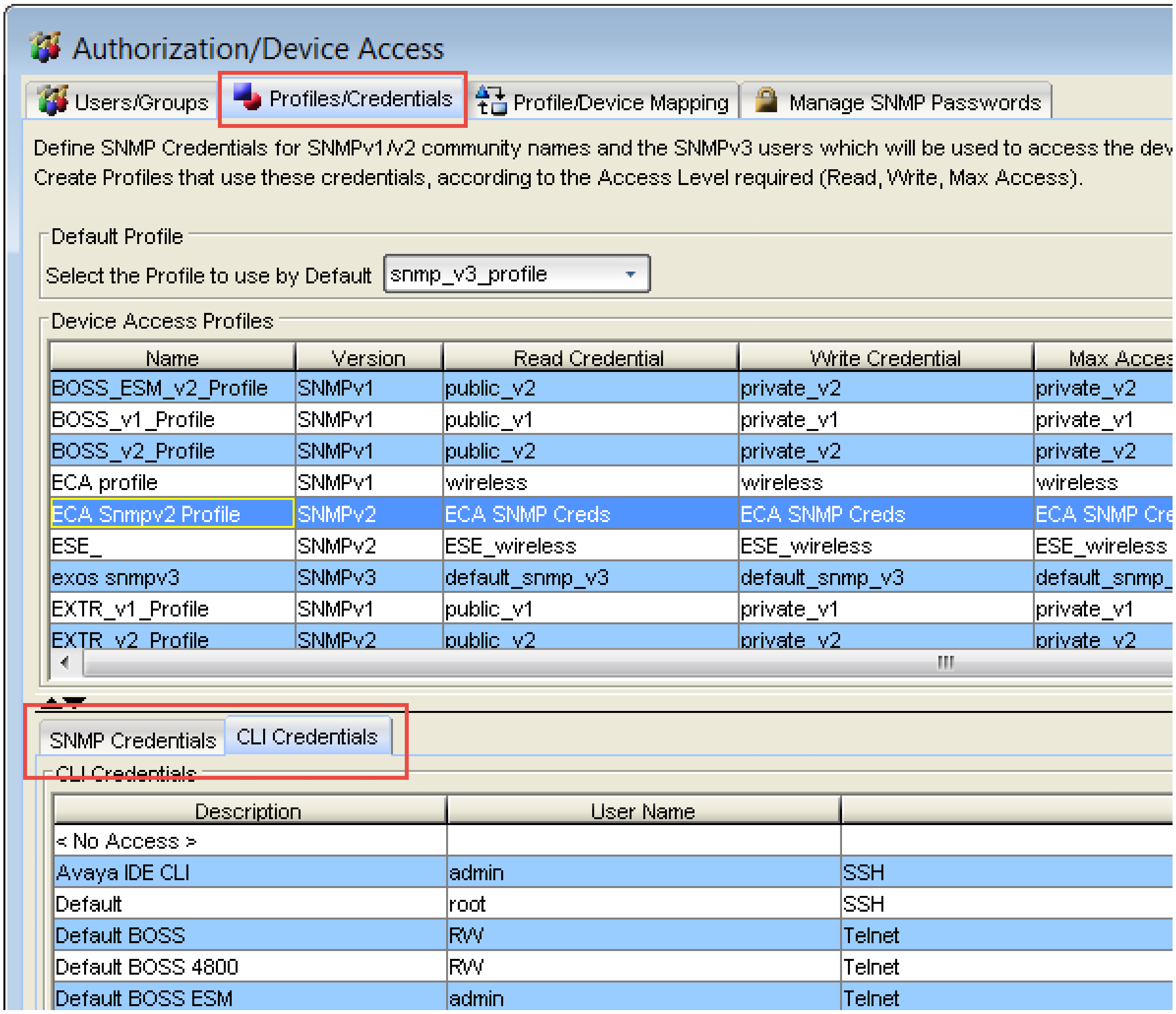
   Pass-Thru External RADIUS
3. Click **Save**.
4. Move the rule to the top of the rule set, if it is not already there.

Adding ExtremeCloud Appliance as a Switch to Extreme Management Center

Configure Extreme Management Center in the NAC Manager thick client.

1. Configure SNMPv2 and CLI credentials.

   Go to NAC Manager **Authorization/Device Access**.



Define SNMP Credentials for SNMPv1/v2 community names and the SNMPv3 users which will be used to access the dev
Create Profiles that use these credentials, according to the Access Level required (Read, Write, Max Access).

Default Profile

Select the Profile to use by Default: snmp_v3_profile

Device Access Profiles

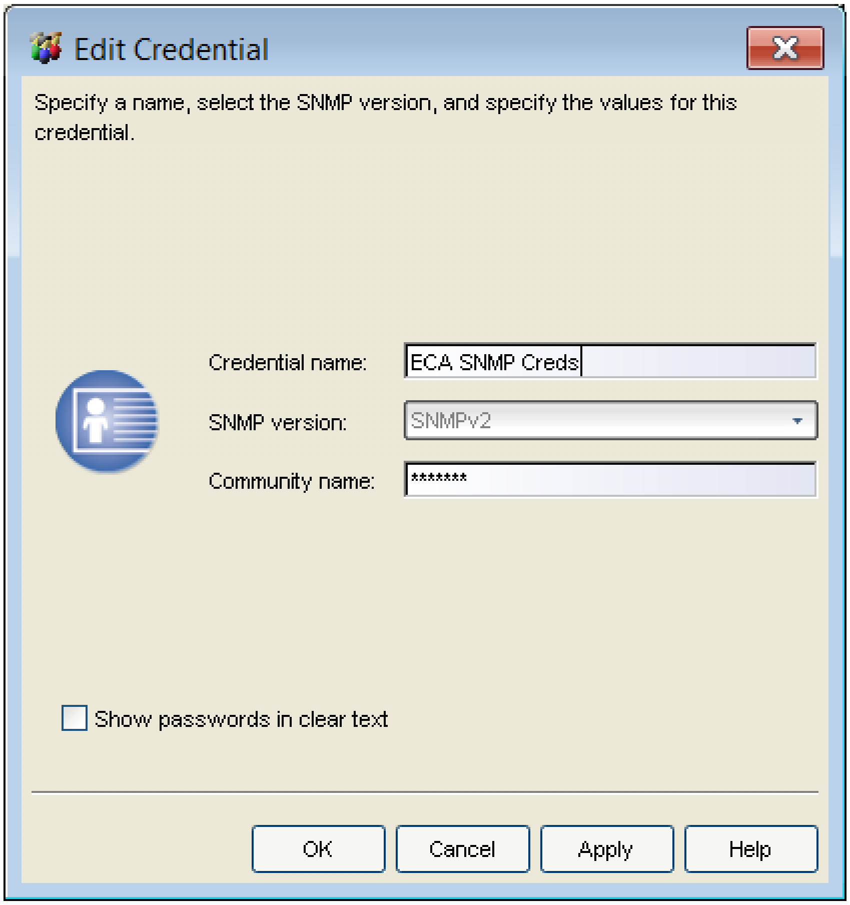
Name	Version	Read Credential	Write Credential	Max Acces
BOSS_ESM_v2_Profile	SNMPv1	public_v2	private_v2	private_v2
BOSS_v1_Profile	SNMPv1	public_v1	private_v1	private_v1
BOSS_v2_Profile	SNMPv1	public_v2	private_v2	private_v2
ECA profile	SNMPv1	wireless	wireless	wireless
ECA Snmpv2 Profile	SNMPv2	ECA SNMP Creds	ECA SNMP Creds	ECA SNMP Cre
ESE_	SNMPv2	ESE_wireless	ESE_wireless	ESE_wireless
exos snmpv3	SNMPv3	default_snmp_v3	default_snmp_v3	default_snmp_
EXTR_v1_Profile	SNMPv1	public_v1	private_v1	private_v1
EXTR_v2_Profile	SNMPv2	public_v2	private_v2	private_v2

CLI Credentials

Description	User Name	
< No Access >		
Avaya IDE CLI	admin	SSH
Default	root	SSH
Default BOSS	RW	Telnet
Default BOSS 4800	RW	Telnet
Default BOSS ESM	admin	Telnet

Figure 43: NAC Manager Authorization/Device Access

2. Click the **Profiles/Credentials** > **SNMP Credentials** and configure SNMPv2 credentials.



Edit Credential

Specify a name, select the SNMP version, and specify the values for this credential.

Credential name: ECA SNMP Creds

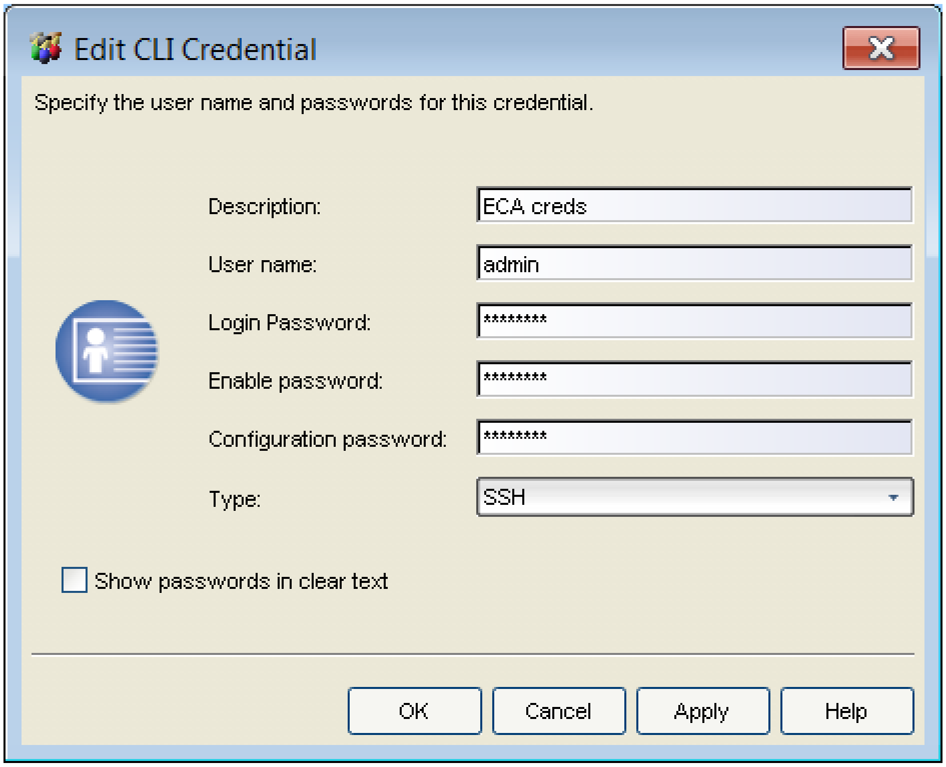
SNMP version: SNMPv2

Community name: *******

□ Show passwords in clear text

Figure 44: SNMPv2 Community

3. Click the **CLI Credentials** tab and configure the CLI credentials.



Edit CLI Credential

Specify the user name and passwords for this credential.

Description: ECA creds

User name: admin

Login Password: ********

Enable password: ********

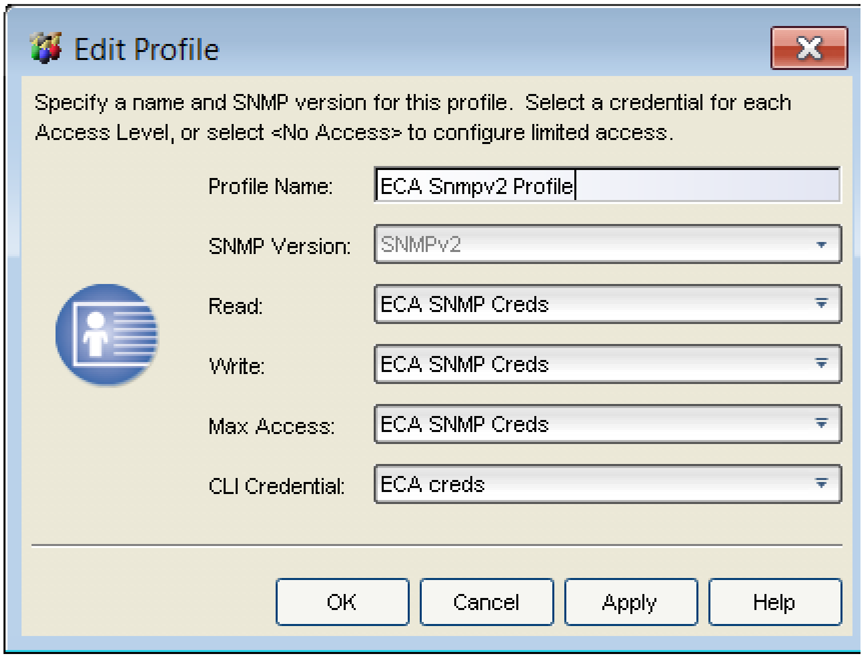
Configuration password: ********

Type: SSH

□ Show passwords in clear text

Figure 45: CLI Credentials

4. Create an ExtremeCloud Appliance SNMP profile, selecting the two credentials.



Edit Profile

Specify a name and SNMP version for this profile. Select a credential for each Access Level, or select <No Access> to configure limited access.

Profile Name: ECA Snmpv2 Profile

SNMP Version: SNMPv2

Read: ECA SNMP Creds

Write: ECA SNMP Creds

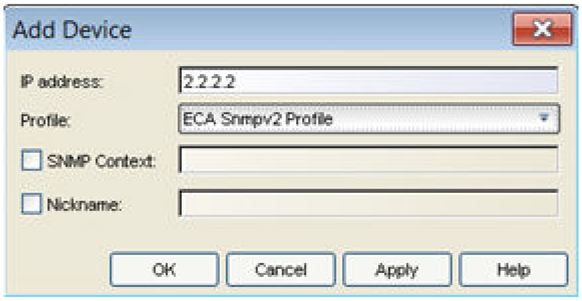
Max Access: ECA SNMP Creds

CLI Credential: ECA creds

Figure 46: ExtremeCloud Appliance SMP Profile

5. Click **Save**.

6. Add the switch to your Access Control Engine.
   a. In NAC Manager, select the Access Control Engine in your configuration.
   b. Click **Switches** > **Add Switch**.
   c. Enter the IP of the ExtremeCloud Appliance, and select the SNMP profile you previously created.



IP address: 2.2.2.2
Profile: ECA Snmpv2 Profile
□ SNMP Context:
□ Nickname:

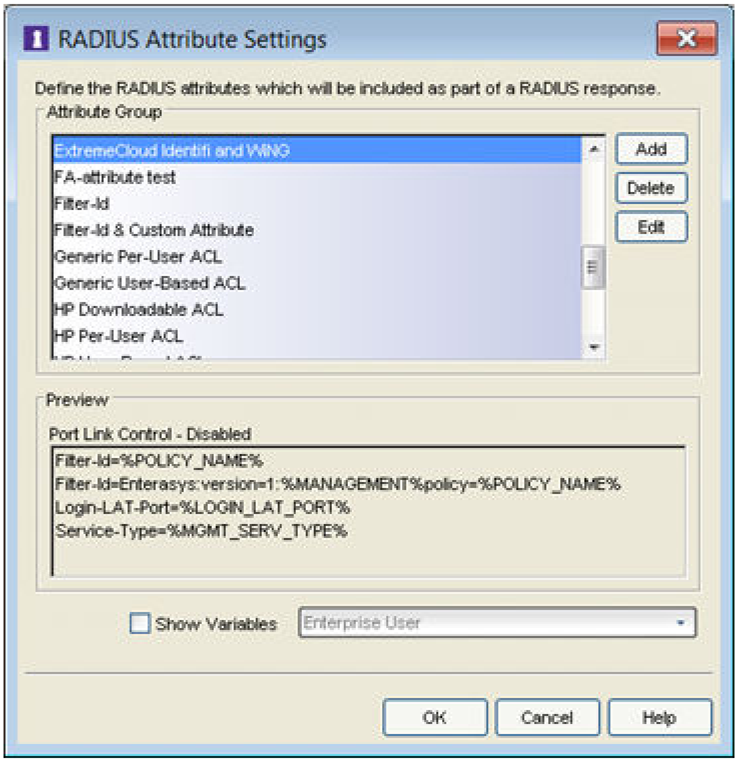
Figure 47: Add Device

7. Click **Apply**.
8. With the switch selected, set the following criteria:
   - 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 (if appropriate for your configuration)
   - Edit Auth Access Type: **Manual RADIUS Configuration**

     Note
     Select the drop-down for **RADIUS Attributes to Send** and select the gear icon beside **Edit RADIUS Attribute Settings**.

   - Select **Extreme Identifi Wireless** and copy the attributes listed in the **Preview** pane.
9. Select **Add** to create a new Attribute Grouping.
   - Name: **ExtremeCloud Identifi and WiNG**
   - Attributes
     - Press **Ctrl-V** to paste in the attributes from Extreme Identifi Wireless.
     - Add the following attribute: `Filter-Id=%POLICY_NAME%`

     Note
     WiNG devices do not accept the Identifi Attribute set and therefore will not set the policy appropriately on ExtremeCloud Appliance when connecting end systems to a WiNG network. Therefore, create an attribute set with all valid values to ensure that the correct policy is applied to both Identifi-connected and WiNG-connected end systems.



Define the RADIUS attributes which will be included as part of a RADIUS response.

Attribute Group

- ExtremeCloud Identifi and WiNG
- FA-attribute test
- Filter-Id
- Filter-Id & Custom Attribute
- Generic Per-User ACL
- Generic User-Based ACL
- HP Downloadable ACL
- HP Per-User ACL

Preview

Port Link Control - Disabled

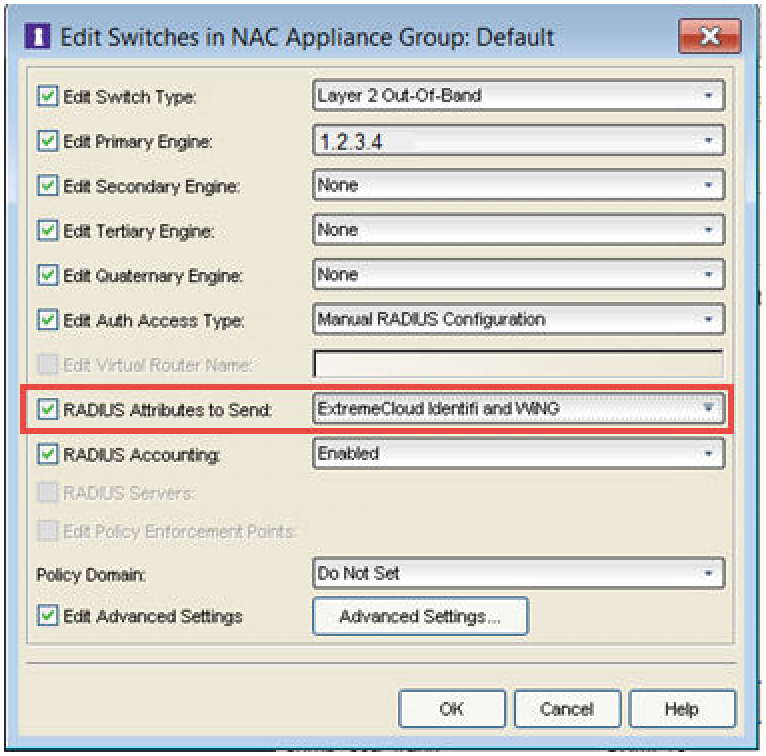
```
Filter-Id=%POLICY_NAME%
Filter-Id=Enterasys:version=1:%MANAGEMENT%policy=%POLICY_NAME%
Login-LAT-Port=%LOGIN_LAT_PORT%
Service-Type=%MGMT_SERV_TYPE%
```

☐ Show Variables   Enterprise User

Figure 48: RADIUS Attribute Settings

10. Click **OK**.

11. From the **RADIUS Attributes to Send** drop-down menu, select the new attribute set for the ExtremeCloud Appliance switch and click **OK**.



Edit Switches in NAC Appliance Group: Default

☑ Edit Switch Type: Layer 2 Out-Of-Band

☑ Edit Primary Engine: 1.2.3.4

☑ Edit Secondary Engine: None

☑ Edit Tertiary Engine: None

☑ Edit Quaternary Engine: None

☑ Edit Auth Access Type: Manual RADIUS Configuration

□ Edit Virtual Router Name:

☑ RADIUS Attributes to Send: ExtremeCloud Identifi and WING

☑ RADIUS Accounting: Enabled

□ RADIUS Servers:

□ Edit Policy Enforcement Points:

Policy Domain: Do Not Set

☑ Edit Advanced Settings

Figure 49: Edit Switch in NAC – ExtremeCloud Appliance

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.

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**.
8. Return to NAC Manager.

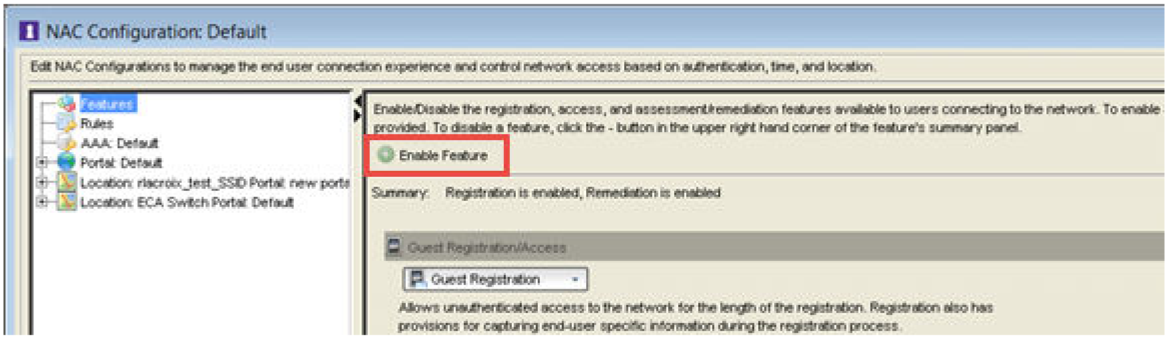
Editing the Extreme Management Center Profile for Policy and Location-Based Services

All policies/filter-ids sent from the NAC server to ExtremeCloud Appliance must also be configured in ExtremeCloud Appliance. If ExtremeCloud Appliance cannot correlate a filter-id to an existing policy in the ExtremeCloud Appliance roles database, the ExtremeCloud Appliance default authenticated roles are applied.

To enable Location Based Services on a NAC server, take the following steps:

1. Go to NAC Manager and select the NAC Appliance Group.
2. Select the **Configuration** tab
3. From the **Configuration** drop-down, click the gear icon next to the NAC Configuration that you are using for your appliance group.

   The NAC Configuration Default dialog displays.


NAC Configuration: Default
Features
Rules
AAA: Default
Portal: Default
Location: rlacroix_test_SSID Portal: new ports
Location: ECA Switch Portal: Default
Enable Feature
Guest Registration/Access
Guest Registration

Edit NAC Configurations to manage the end user connection experience and control network access based on authentication, time, and location.

Enable/Disable the registration, access, and assessment/remediation features available to users connecting to the network. To enable provided. To disable a feature, click the - button in the upper right hand corner of the feature's summary panel.

Summary: Registration is enabled, Remediation is enabled

Allows unauthenticated access to the network for the length of the registration. Registration also has provisions for capturing end-user specific information during the registration process.

Figure 50: NAC Configuration Default

4. Select **Enable Feature**.
5. Select **Allow Location-Based Access**.

   The Location-Based configuration window appears.
6. Select the **Location** drop-down and select **New**.
7. Configure the following parameters:

   Switch

      ExtremeCloud Appliance Switch IP

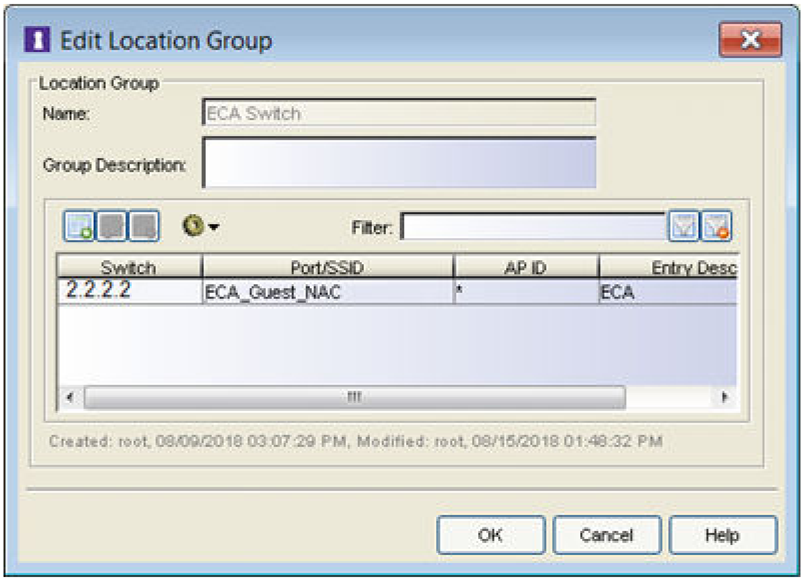
   Interface (optional)

      Select **Wireless** to restrict to a Wireless interface.

   SSIDs

      ExtremeCloud Appliance_Guest (if you want to restrict this to only systems via this SSID)

8. Click **OK**.



Location Group

Name: ECA Switch

Group Description:

Switch	Port/SSID	AP ID	Entry Desc
2.2.2.2	ECA_Guest_NAC	*	ECA

Created: root, 08/09/2018 03:07:29 PM, Modified: root, 08/15/2018 01:48:32 PM

Figure 51: Edit Location Group Dialog

9. Select the network as the location you just created.
10. Select a portal and features you wish to enable for this location.
11. To create a new NAC profile, go to **Access Rules**.
12. From the **Registration Pending Access** column, select **Unregistered**, then select **New**.
13. Configure the following parameters:

Name

ExtremeCloud Appliance Unregistered

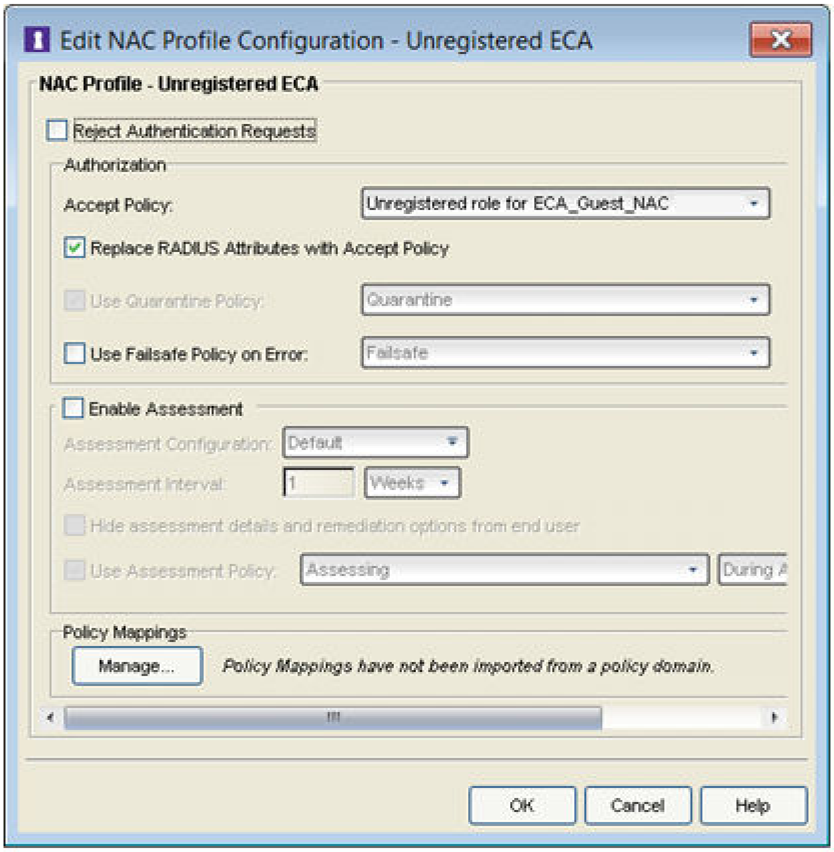
Accept Policy

Unregistered role for ExtremeCloud Appliance_Guest

Replace RADIUS attributes with Accept Policy

Enabled

Note
By default, all unregistered systems get the Unregistered profile/policy. Modify the default profile so all ExtremeCloud Appliance end system traffic explicitly uses the new NAC Profile and the new ExtremeCloud Appliance Unregistered policy that we created for the network, previously.



Edit NAC Profile Configuration - Unregistered ECA

NAC Profile - Unregistered ECA

☐ Reject Authentication Requests

Authorization

Accept Policy: Unregistered role for ECA_Guest_NAC

☑ Replace RADIUS Attributes with Accept Policy

☐ Use Quarantine Policy: Quarantine

☐ Use Failsafe Policy on Error: Failsafe

☐ Enable Assessment

Assessment Configuration: Default

Assessment Interval: 1 Weeks

☐ Hide assessment details and remediation options from end user

☐ Use Assessment Policy: Assessing During A

Policy Mappings

Policy Mappings have not been imported from a policy domain.

Figure 52: NAC Profile Unregistered for ExtremeCloud Appliance

14. Click **OK**.
15. Set the Profile for both **Registration Pending Access** and **Unregistered** to the new NAC Profile: **Unregistered ECA** and click **OK**.
16. Click **OK** again to save the Location-Based Services profile.
17. Go to **NAC Configuration Default** > **Rules** to see the new rules that are specific to the ExtremeCloud Appliance network.

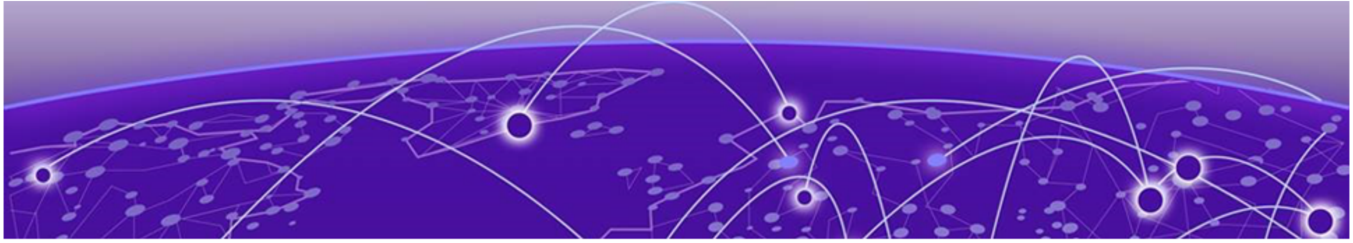
Note

There are multiple registration rules for each registration type, because we have configured both Guest and Authenticated registrations enabled on the portal configuration.

Note

If there is a mismatch in roles between NAC and ExtremeCloud Appliance, force a re-authentication from ExtremeCloud Appliance. The mismatch may be a result of a timing issue. View **Session timeouts** on the network configuration for more information.

If the mismatch persists, confirm that you have used exact syntax on the role configuration. See Creating an Unregistered Policy on Extreme Management Center on page 120 for more information.



Deploying an ExtremeGuest Captive Portal

Deployment Strategy

The following strategy outlines how to configure ExtremeCloud Appliance to integrate with ExtremeGuest™, which houses the external captive portal. The ExtremeGuest server can be assigned from the ExtremeCloud Appliance **Networks Add** page to handle client authentication and accounting. The portal resides on the ExtremeGuest server and ExtremeCloud Appliance initiates the client network connections.

The following outlines how to integrate ExtremeCloud Appliance with ExtremeGuest.

1. Add a site with a device group.
2. Configure one or more ExtremeGuest servers.
3. Configure a captive portal network:
   - Select **Enable Captive Portal** on the network.
   - Select portal type **EGuest**.
   - Specify the ExtremeGuest servers.
4. Modify the configuration profile associated with the device group:
   - Assign the ExtremeGuest network to the device group.
   - Assign the policy roles to the device group.

> Note
> The policy role names must match on both ExtremeGuest and ExtremeCloud Appliance. A simple approach is to create policies on ExtremeGuest with names that match the ExtremeCloud Appliance default policies.

Related Topics

Configure an ExtremeGuest Server on page 125
Configure an ExtremeGuest Captive Portal Network on page 125
Configuration Settings on ExtremeGuest on page 126

Configure an ExtremeGuest Server

Configure up to three ExtremeGuest servers. To configure an ExtremeGuest server. Take the following steps:

1. Go to **Configure** > **ExtremeGuest** and select **Add**.
2. Configure the following parameters:

   IP Address

   Valid IP address of the ExtremeGuest server.

   Name

   Name of the ExtremeGuest server.

   FQDN

   Fully-qualified domain name of the ExtremeGuest server.

   Authentication Timeout Duration (Seconds)

   Determines a timeout value, in seconds, for the RADIUS server connection.

   Authentication Retry Count

   Determines the number of times ExtremeCloud Appliance will attempt to authenticate an end user.

   Authentication Client UDP Port

   User Datagram Protocol (UDP) port number used for client authentication. UDP needs only one port for full-duplex, bidirectional traffic.

   Shared Secret

   The password that is used to validate the connection between ExtremeCloud Appliance and the ExtremeGuest server.

   Mask

   Determines if the Shared Secret or password value is displayed on the user interface. Enable Mask to display dots in place of the Shared Secret or password value. To display the password characters, clear the **Mask** check box.

   Callback User Name

   User ID that Callback Manager uses to access the ExtremeGuest server.

   Callback Password

   The password that Callback Manager uses to access the ExtremeGuest server. The minimum password length is 6 characters.

   Mask

   Determines if the Shared Secret or password value is displayed on the user interface. Enable Mask to display dots in place of the Shared Secret or password value. To display the password characters, clear the **Mask** check box.

Configure an ExtremeGuest Captive Portal Network

To configure an ExtremeGuest captive portal network.

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

Network Name

ECA_EGuest

SSID

ECA_EGuest

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 = **EGuest**
- Select the ExtremeGuest server from the drop-down list of configured servers. The number of server fields depends on the number of configured servers. Configure one portal server and up to two backup servers.
  - Select an icon (⊕, ✎, or 🗑) to manage your servers from here. Select the appropriate check box to indicate that the server handles authentication, accounting, or both. At least one selection is required for each server.
  - Select **Portal** to configure one server as the portal server. If your portal server goes down, you must manually select a backup server as the portal server.

> Note
> Walled Garden rules are not required for this network. The process of enabling a captive portal on the network automatically creates rules allowing DNS, DHCP, and redirection rules. However, if users are unable to connect to the network, consider creating specific DNS and DHCP Allow rules as a Walled Garden configuration.

MAC-based authentication (MBA)

This option is enabled by default. Configure the following parameters:

MBA Timeout Role

Unregistered

Use HTTPS connection

Enable this option if connecting to the server through https.

Default Auth Role

Enterprise User

Default VLAN

Bridged at AP Untagged

Configuration Settings on ExtremeGuest

Configure the following settings on ExtremeGuest to support integration with ExtremeCloud Appliance:

- Policy Role Names — The policy role names must match on both ExtremeGuest and ExtremeCloud Appliance. A simple approach is to create policies on ExtremeGuest with names that match the ExtremeCloud Appliance default policies.

- Configure ExtremeCloud Appliance as the **AAA NAS** (Network Access Server). Use the IP address (or Subnet address) of ExtremeCloud Appliance or the address of the RF Domain Manager.

For more information, see the *ExtremeGuest User Guide* on https://extremenetworks.com/support/documentation.

Hierarchical Visibility for WiNG Appliances

Deployment Strategy

ExtremeCloud Appliance offers unified visibility into Extreme Management Center for existing ExtremeWireless WiNG installations. This option extends the reporting and visibility capabilities of Extreme Management Center to ExtremeWireless WiNG accounts. This offers not only as an alternative to NSight, but supports unified wireless, wired infrastructure and expands other Extreme Networks software offerings, such as ExtremeAnalytics. If you are already leveraging NSight, this solution continues to support that investment. ExtremeCloud Appliance will relay statistics that feed into NSight to keep it's visibility value intact.

APs and appliances running ExtremeWireless WiNG version 5.9.1 or later are supported in this deployment strategy. ExtremeWireless WiNG APs are adopted by the WiNG appliance, and their configuration and statistics are fed through ExtremeCloud Appliance for presentation in Extreme Management Center or NSight.

The ExtremeCloud Appliance Statistics Proxy function leverages the ExtremeWireless WiNG stats connection that typically feeds NSight. The connection may already be in use if you are using the NSight product on the ExtremeWireless WiNG deployment. To support compatibility with the installed base, ExtremeCloud Appliance can relay the stats to feed the NSight (cluster).

You can opt to configure ExtremeCloud Appliance as an external NSight server for an ExtremeWireless WiNG controller or as an additional proxy server between ExtremeWireless WiNG and Extreme Management Center, with or without NSight. When using NSight, the NSight server displays stats from proxy APs along side other AP stats. The ExtremeCloud Appliance is completely transparent to NSight.

Related Topics

Configuring ExtremeCloud Appliance as an External Server on page 129
Configuring ExtremeCloud Appliance as Proxy Server on page 129

Configuring ExtremeCloud Appliance as an External Server

The following outlines how to configure ExtremeCloud Appliance as an external server to NSight.

1. Configure the following parameters on the ExtremeWireless WiNG appliance.

   nsight-policy

   <policy-name>

   server host

   <ECA IP address> using https

   rf-domain

   <rf-domain-name>

2. On ExtremeCloud Appliance, enable **Device Registration** on the Interface that uses the ExtremeCloud Appliance IP address.

   Go to **Administration** > **System** > **Interfaces**. Under **Interfaces**, select the topology and enable **Device Registration**.

Related Topics

Configuring ExtremeCloud Appliance as Proxy Server on page 129

Deployment Strategy on page 128

Configuring ExtremeCloud Appliance as Proxy Server

The following outlines how to configure ExtremeCloud Appliance as a proxy server to utilize Extreme Management Center in an ExtremeWireless WiNG environment. The proxy function provides visibility into metrics of an ExtremeWireless WiNG deployment, by leveraging existing reporting interfaces that feed into Extreme Management Center.

This deployment strategy can be used with or without NSight. If NSight is present, ExtremeCloud Appliance serves as a proxy for the data stream. While NSight controls the data stream, ExtremeCloud Appliance becomes, essentially, a relay.

1. Configure the following parameters on the ExtremeWireless WiNG appliance.

   (Optional) nsight-policy

   <policy-name>

   server host

   <ECA IP address> using https

   rf-domain

   <rf-domain-name>

2. On ExtremeCloud Appliance, enable **Device Registration** on the Interface that uses the ExtremeCloud Appliance IP address.

   Go to **Administration** > **System** > **Interfaces**. Under **Interfaces**, select the topology and enable **Device Registration**.

3. If NSight is part of your deployment strategy, on ExtremeCloud Appliance, configure the IP address of the NSight server.

   Go to **Administration** > **System** > **Setting**. Under **NSight Configure** provide the following:

   Connection

HTTPS

IP Address

IP address of NSight server

Related Topics

Configuring an Availability Pair with WiNG on page 130

Configuring an Availability Pair with WiNG

When deploying an availability pair of appliances, within ExtremeWireless WiNG configuration, configure the server host address for each ExtremeCloud Appliance. From the ExtremeWireless WiNG controller, configure the following parameters:

nsight-policy

<policy-name>

Server host 1

ECA1 (https)

Server host 2

ECA 2 (https)

Note

Each ExtremeCloud Appliance serves as a proxy server to one NSight instance. If one ExtremeCloud Appliance/NSight connection fails, the ExtremeWireless WiNG controller moves to another ExtremeCloud Appliance/NSight connection. ExtremeCloud Appliance does not initiate the change to another NSight. As a result, ExtremeCloud Appliance is not aware of the new NSight IP address. Therefore, the NSight IP address is not synchronized between paired appliances. Configure the NSight IP address separately on each ExtremeCloud Appliance.

Understanding Proxy APs

A proxy AP is an AP that has been adopted by an ExtremeWireless WiNG controller. The AP statistics and configuration are fed from the controller through ExtremeCloud Appliance for display in NSight. Proxy APs and their associated components are all marked as **Proxied** in the ExtremeCloud Appliance:

- **AP List** — APs that are adopted by an ExtremeWireless WiNG controller are listed as Proxied on the ExtremeCloud Appliance **AP** page.
- **Site List** — RF domains associated with the proxy AP are listed as Proxied on the ExtremeCloud Appliance **Sites** page. The Country designation for a site is derived from the AP RF domain. When there are no APs assigned to an RF domain, the Country designation for the site is “Demo Country”.
- **Networks List** — Networks associated with the proxy AP are listed as Proxied on the ExtremeCloud Appliance **Networks** page, and a proxy network displays the network name, SSID, privacy/ encryption and VLAN of the ExtremeWireless WiNG network. The default role is “Enterprise User” for a proxy network.
- **VLAN List** — VLANs associated with the proxy AP are listed as Proxied on the ExtremeCloud Appliance **VLAN** page. A proxy VLAN topology is always "Bridged at AP, tagged". If a network

references a VLAN that is configured in ExtremeCloud Appliance, that existing VLAN is used by the proxy network.

- **Controller List** — ExtremeWireless WiNG proxy controllers configured for NSight are listed in ExtremeCloud Appliance under **Monitor** > **Devices** > **Controllers**. Proxied controllers can be removed from the **Controllers** page. However, if the ExtremeWireless WiNG controller has ExtremeCloud Appliance in its configuration, the ExtremeWireless WiNG controller displays in the list of controllers after each update. Proxy controllers cannot be edited.

All relevant information and statistics for a proxy AP displays in ExtremeCloud Appliance. However, editing and troubleshooting are not available in ExtremeCloud Appliance for a proxy AP or its associated: site, network, or VLAN.

Note
A proxy AP and its associated components can be removed from the ExtremeCloud Appliance. However, as long as the AP is adopted by the ExtremeWireless WiNG controller, the AP, site, network, and VLAN are re-created each time the controller sends an update to ExtremeCloud Appliance.

APs that are adopted by an ExtremeWireless WiNG controller continue to provide data to ExtremeWireless WiNG wizards and dashboards, as well as feed data to ExtremeCloud Appliance.

Related Topics

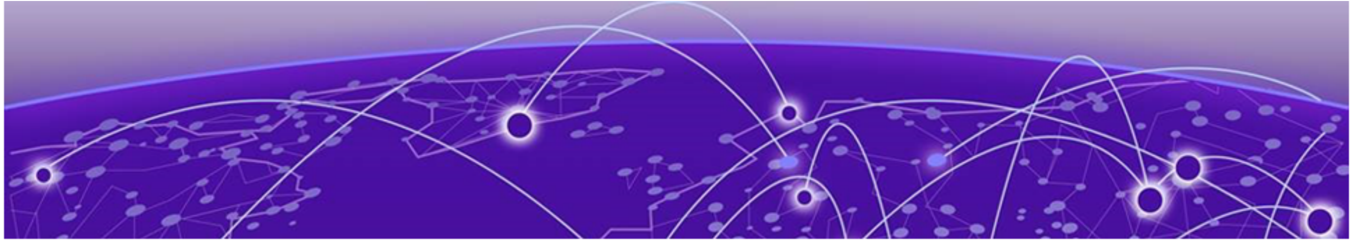
Legacy AP Support on page 131

Legacy AP Support

ExtremeCloud Appliance supports AP proxy for all ExtremeWireless WiNG AP models. AP models that are not supported for local adoption by ExtremeCloud Appliance are displayed as “Legacy AP model” in ExtremeCloud Appliance. However, the proxy AP model is correctly displayed in NSight. All ExtremeWireless WiNG AP widgets are supported on ExtremeCloud Appliance dashboards for legacy AP models.

Understanding Proxy Clients

There is little difference between a wireless client associated with a proxy AP and a locally adopted AP. In ExtremeCloud Appliance, wireless clients, attached to proxy APs, are displayed on the **Clients** page, along side clients of locally adopted APs. ExtremeCloud Appliance widgets and dashboards are available for proxy clients. You cannot delete or disassociate a proxy client from ExtremeCloud Appliance because they are managed by the ExtremeWireless WiNG controller.



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 **Administration** > **System** > **Network Time** and select **NTP**.
2. On the primary ExtremeCloud Appliance, go to **Administration** > **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.

   > Note
   > The Peer IP address must refer to a physical topology of the peer appliance. It can be the IP address of a physical port or the IP address of a Lagged interface. Configuring availability against a service topology such as the IP address (L3) of a Bridged@Controller appliance is not supported.

   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.

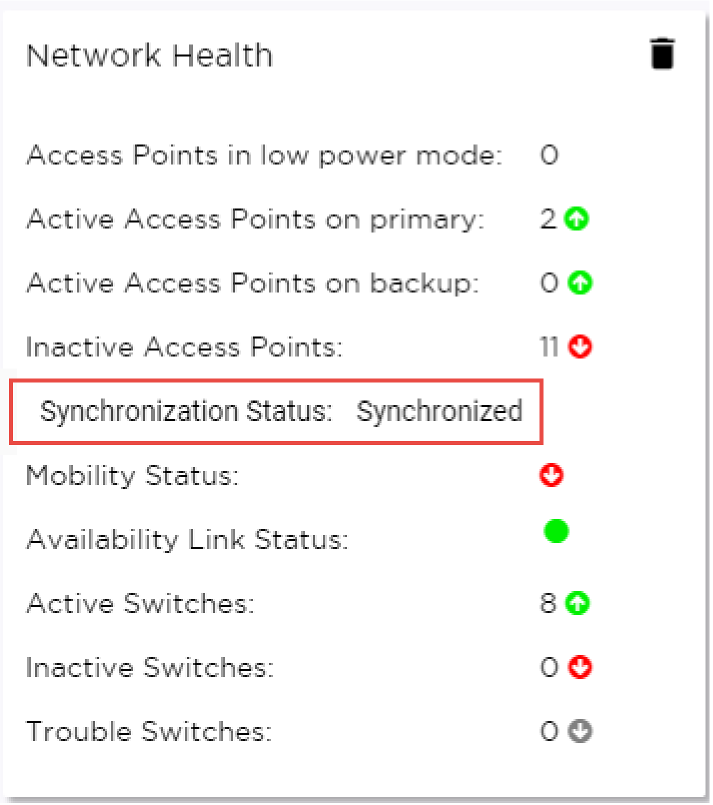
   a. Go to **Dashboard**.

   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.



Network Health

Access Points in low power mode: 0

Active Access Points on primary: 2 ↑

Active Access Points on backup: 0 ↑

Inactive Access Points: 11 ↓

Synchronization Status: Synchronized

Mobility Status: ↓

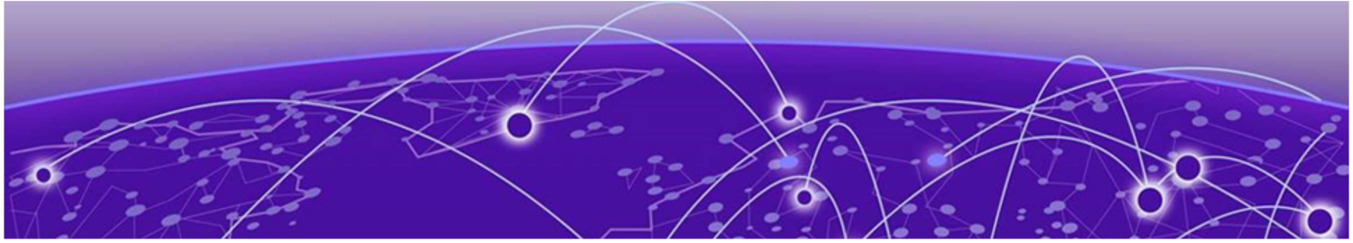
Availability Link Status: ●

Active Switches: 8 ↑

Inactive Switches: 0 ↓

Trouble Switches: 0 ↓

Figure 53: Availability Pair Synchronization Status



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 Topics

Adding a Centralized Site with Device Group on page 57
Adding a Distributed Site on page 73
Configuring an Internal Captive Portal on page 59
Specifying B@AC Network Topology on page 60
Configuring a Captive Portal Network on page 61
Working with Internal Captive Portal Engine Rules on page 62
Configuring the Centralized Site with an AP3915 Profile on page 136
Configuring the Distributed Site and AP7632 Profile on page 136
Creating Adoption Rules on page 65
Deploying an Availability Pair on page 132

Configuring the Centralized Site with an AP3915 Profile

1. Go to **Configure** > **Sites** > **Add** to create a Centralized site.
2. Click **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 Topics

Adding a Centralized Site with Device Group on page 57
Editing Device Group Profile for Network and Role on page 62
Configuring ExtremeLocation on page 137
Configuring AirDefense on page 137

Configuring the Distributed Site and AP7632 Profile

1. Go to **Configure** > **Sites** > **Add** to create a Distributed site.
2. Click **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 Topics

Adding a Distributed Site on page 73
Editing Device Group Profile for Network and Role on page 62
Configuring ExtremeLocation on page 137
Configuring AirDefense on page 137

Configuring ExtremeLocation

Configure the following parameters to integrate the AP with ExtremeLocation.

Table 9: 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.

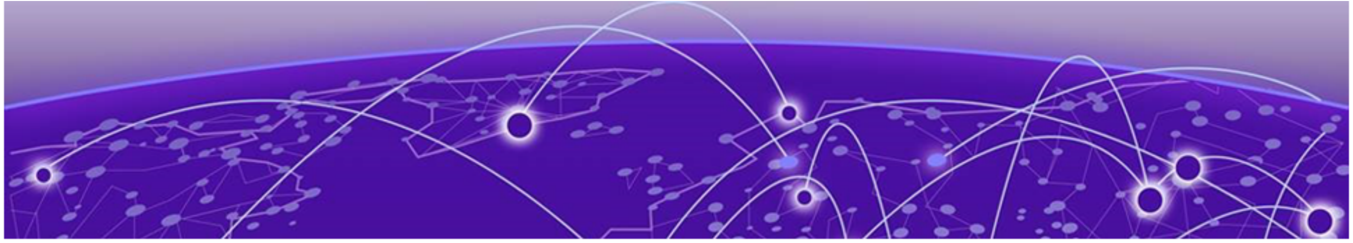
In dedicated sensor mode, the AP operates independently from the ExtremeCloud Appliance while the ExtremeCloud Appliance continues to see the AP and display the AP Role as a dedicated AirDefense sensor. In its role as a dedicated sensor, the AP does not report statistics to the ExtremeCloud Appliance.

Table 10: AirDefense Profile Settings

Field	Description
Name	Name of AirDefense profile.
Add Server 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 **Servers** list. Note: When using the AirDefense Base (add-on container application), provide the IP address of the ExtremeCloud Appliance data port that is reachable by the APs and sensors.

Table 10: AirDefense Profile Settings (continued)

Field	Description
Port	Specify a port for the AirDefense server. The default port is 443 (used with a dedicated external AirDefense Server). Note: When using the AirDefense Base (add-on container application), configure port number to **32032**.
Servers	List of IP addresses for servers. Click 🗑 to remove an IP address from the list.



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 Topics

Deployment Strategy on page 139
Configuring External Captive Portal Network on page 140

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 Topics

Adding a Centralized Site with Device Group on page 57
Adding a Distributed Site on page 73
Specifying B@AP Network Topology on page 75
Configuring External Captive Portal Network on page 140
Creating Adoption Rules on page 65
Deploying an Availability Pair on page 132

Configuring External Captive Portal Network

To configure an External Captive Portal network:

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

Table 11: 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. Maximum 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 11: 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 Auth role is the only supported policy role. • WEP (Static Wired Equivalent Privacy) — Keys for a selected network, that match the WEP mechanism used on the rest of the network. Each AP can participate in up to 50 networks. Specify one WEP key per network. This option is offered to support legacy APs. • 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 Auth role only. • WPA2 Enterprise w/ RADIUS — Supports 802.1X authentication with a RADIUS server, using AES encryption. This method can be used 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. The devices with 802.1X use Default Auth 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. • WPAv3 - Personal with SAE — 128-bit encryption, supported on: ◦ AP4xx running ExtremeWireless WiNG 7.3x. ◦ AP5xx running ExtremeWireless WiNG 7.2x and later. WPAv3 uses a pre-shared key (PSK) and Simultaneous Authentication of Equals (SAE). WPAv3 offers an

Table 11: External Captive Portal Settings (continued)

Field	Description
	augmented handshake and protection against future password compromises. - WPAv3 - Compatibility — Option for mixed deployments of 802.11ax APs and older AP models. If the network is configured with WPAv3-Compatibility (SAE or WPAv2 PSK authentication), 802.11ax APs running ExtremeWireless WiNG 7.2.x or later utilize the WPAv3 - Personal protocol. Older AP models that are not WPAv3 compatible use WPAv2 AES. For more information, see the *ExtremeCloud Appliance User Guide* or *Online Help*.
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	Select **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. Select **Save**.

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

Related Topics

Editing the Device Group Profile for ECP Network on page 142

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 **Configure** > **Sites** and select a site.
2. Click **Device Groups**.

3. Select a device group.
4. Beside the Profile field, 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.

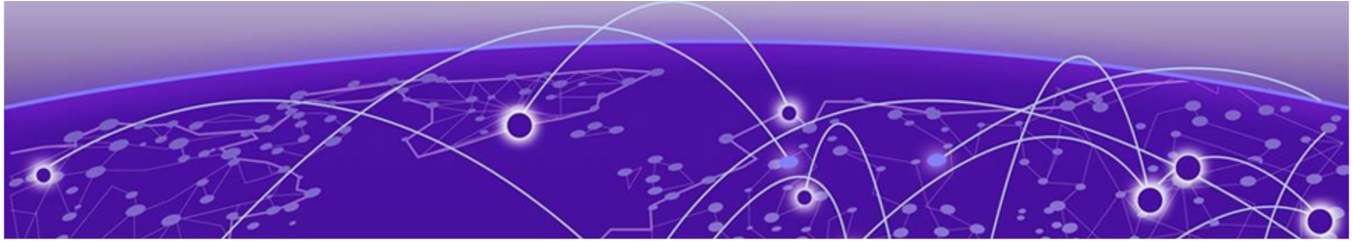
8. Click **Save** to save the profile settings.
9. Click **Close** to close the device group.

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

Related Topics

Creating Adoption Rules on page 65

Deploying an Availability Pair on page 132



PHP External Captive Portal, Controller’s Firewall Friendly API

This appendix contains five files that serve as an example of how to build an External Captive Portal that makes use of the controller’s Firewall-Friendly External Captive Portal Interface. The files presented are:

- net-auth.php

  Receives redirected requests from browsers trying to access web sites, verifies that the redirect was sent from the controller and if so, displays a suitable login page.
- login.php

  This script gets invoked as a consequence of a browser submitting the login form created by net-auth.php. The script authenticates the station in whatever way it likes. If the station is authorized the script selects a maximum session duration and an access control role for the station. It then redirects the station’s browser back to a web server on the controller, using a URI that contains the access control role, the maximum session duration, other data required by the controller, and a signature.
- crypt_aws_s4.php

  This file contains the code that verifies the signatures on received URLs and that signs the URLs that redirect the station back to the controller.
- common_utilities.php

  Utilities used by various ECP scripts
- ffecp-config.php

  Contains the main statically configured parameters that the application uses to verify signed URLs and to create signed URLs.

net-auth.php

```
<?php
  // net-auth.php
  // This is a simple implementation of a script that
  // receives HTTP requests that have been redirected
  // by a controller configured with "Firewall-Friendly
  // External Captive Portal" support enabled.
  // This script is responsible for collecting critical
  // information from the redirection, such as the
  // session token, and for constructing the login page
  // for the user. The script reads the VNS attribute
  // from the redirected request so that the script can
  // display it on the login page.
  //
  // The script expects the controller to sign the
  // redirection response. The script validates the
  // signature. If the signature is valid, it displays
  // the login page. Otherwise, it displays an error page.
  //
  // Assumptions
  // ===========
  // 1. The controller is configured to include its IP address
  //    and port in the redirection URL.
  // 2. The controller is configured to sign its redirection
  //    responses using the Amazon S3 version 4 signature
  //    algorithm (as of May 2014).
  // 3. The controller is configured to include the VNS in its
  // redirection response.
  // 4. This application assumes that the Identity & Shared Key
  // key pairs that it is allowed to use are stored in an associative
  // array. It also assumes that some configuration options such
  // as the 'service' and 'region' are stored in another associative
  // array. Real applications might retrieve this information from
  // a database or configuration file.

  require_once("ffecp_config.php");
  require_once("crypt_aws_s4.php");
  require_once("common_utilities.php");

  // Mainline processing starts here. Utilities are defined after
  // the mainline.
  // 1. Verify that the request has all necessary fields
  // and a valid signature.
  $rc = SimpleAws::verifyAwsUrlSignature(getURL($_SERVER),
   $awsKeyPairs);
  if (SimpleAws::AWS4_ERROR_NONE != $rc) {
      printError(SimpleAws::getAwsError($rc));
      exit;
  }
  // Determines which controller interface to interact with
  if(isset($_REQUEST['hwc_ip']) && isset($_REQUEST['hwc_port'])) {
    //BM IP address and port is enabled
    $hwc_ip = trim($_REQUEST['hwc_ip']);
    $hwc_port = trim($_REQUEST['hwc_port']);
  } else {
    // The controller has not been configured as expected. It did not
    // include its address and port on the redirection URL. This is
    // easy to fix but all this program can do is report the error.
    printError("Controller must be configured to include its IP " .
    "address & port in the request.");
    exit;
  }
  // Collect the data required by the login page and
  // subsequent authentication.
  $dest = isset($_REQUEST['dest']) ? $_REQUEST['dest'] : "";
  $bssid = isset($_REQUEST['bssid']) ? $_REQUEST['bssid'] : "";
  $wlan = isset($_REQUEST['wlan']) ? $_REQUEST['wlan'] : "";
  $vns = isset($_REQUEST['vns']) ? $_REQUEST['vns'] : "";
  $mu_mac = isset($_REQUEST['mac']) ? $_REQUEST['mac'] : "";
  $ap_name = isset($_REQUEST['ap']) ? $_REQUEST['ap'] : "";
```

```
  $token = isset($_REQUEST['token']) ? $_REQUEST['token'] : "";
  if(!tokenCheck($token)) {
      printError("Error: <span style='color:red'>Failed to process the request: incorrect 
token.</span>");
      exit;
  } else if(isset($hwc_port) && !is_numeric($hwc_port)) {
      printError("Error: <span style='color:red'>Failed to process the request: incorrect 
port.</span>");
      exit;
  }else if($mu_mac && !macCheck($mu_mac)) {
      printError("Error: <span style='color:red'>Failed to process the request: incorrect 
client MAC address.</span>");
      exit;
  } else if(!empty($wlan) && !is_numeric($wlan)) {
      printError("Error: <span style='color:red'>Failed to process the request: incorrect 
WLAN.</span>");
      exit;
  }
   //escape the parameters
  $dest =convertUrlParam($dest);
  $bssid = convertUrlParam($bssid);
  $vns = convertUrlParam($vns);
  $ap_name = convertUrlParam($ap_name);
  // 3. Compose the login page and send it to the user. The page
  // is used to store session data. This could have been
  // stored in the user session variable or in cookies.
  print compose_login_page($hwc_ip, $hwc_port, $token, $dest,
           $wlan, $vns, $bssid, $mu_mac, $ap_name);
    // 4. And exit. This script is finished executing.
  exit;
  // End of mainline
  // A function that reconstructs the URL that the
  // station was trying to Get, from the variables
  // generated by the PHP runtime.
  function getURL($data) {
    $ssl = (!empty($data['HTTPS']) && $data['HTTPS'] == 'on') ? true:false;
    $protocol = $ssl ? "https" : "http";
    $port = $data['SERVER_PORT'];
    $port = ((!$ssl && $port=='80') || ($ssl && $port=='443')) ? '' : 
   ':'.$port;
    $host = isset($data['HTTP_HOST']) ? $data['HTTP_HOST'] : 
   $data['SERVER_NAME'] . $port;
    return $protocol . '://' . $host . $data['REQUEST_URI'];
  }
  // This function generates a basic login page containing a form
  // that allows the user to submit credentials back to this
  // server. The page displays the name of the VNS (service) that the user
  // is associated to.
  // A real login page normally has more content. This routine
  // highlights the critical aspects of composing a login page so
  // that when the user submits credentials, all the information
  // that is necessary to manage the user's session is on the page.
  function compose_login_page($hwc_ip, $hwc_port, $token, $dest,
          $wlan, $vns, $bssid, $mu_mac, $ap_name)
   {
     $template = "<!DOCTYPE html>
 <html>
 <head>
   <meta charset=\"ISO-8859-1\">
   <title>Please Login</title>
 </head>
 <body>
   <form id=\"Login\" name=\"Login\" method=\"post\" action=\"login.php\">
     <table border='0' width='800' height='310' cellpadding='0'
```

```
      cellspacing='0'>
      <tr>
        <td colspan=\"3\" height=\"100\">&nbsp;</td>
      </tr>
      <tr>
        <td width='260' height='1' border='0'/>
        <td width='300' height='65'>
          Please login to use '$vns' network.</td>
        <td width='240' rowspan='5'>&nbsp;</td>
      </tr>
      <tr>
        <td align=\"right\"><b>User Name&nbsp;&nbsp;</b>
        </td>
        <td height=\"28\">
          <input type=\"text\" autocomplete=\"off\"
            id=\"userid\" name=\"userid\"
tabindex=\"1\">
        </td>
      </tr>
      <tr>
        <td align=\"right\"><b>Password&nbsp;&nbsp;</b>
        </td>
        <td height=\"28\"><input type=\"password\"
autocomplete=\"off\"
          id=\"passwd\" name=\"passwd\" tabindex=\"2\">
        </td>
      </tr>
      <tr>
        <td><br>
        </td>
        <td height=\"33\" valign=\"bottom\"><input
type=\"submit\"
          style=\"width: 100px\" value=\"Login\"
tabindex=\"3\">
        </td>
      </tr>
    </table>
    <input type=\"hidden\" name=\"hwc_ip\" id=\"hwc_ip\"
value=\"$hwc_ip\"/>
    <input type=\"hidden\" name=\"hwc_port\" id=\"hwc_port\"
value=\"$hwc_port\"/>
    <input type=\"hidden\" name=\"token\" id=\"token\"
value=\"$token\"/>
    <input type=\"hidden\" name=\"dest\" id=\"dest\"
value=\"http://$dest\" />
    <input type=\"hidden\" name=\"wlan\" id=\"wlan\"
value=\"$wlan\" />
    <input type=\"hidden\" name=\"mu_mac\" id=\"mu_mac\"
value=\"$mu_mac\" />
    <input type=\"hidden\" name=\"bssid\" id=\"bssid\"
value=\"$bssid\" />
    <input type=\"hidden\" name=\"ap\" id=\"ap\"
value=\"$ap_name\" />
  </form>
</body>
</html>";
    return $template;
  }
?>
```

login.php

```
<?php
  // login.php
  // This is a simple implementation of a script that
  // receives a user's credentials, authenticates the
  // credentials, selects an access control role for
  // the user, then redirects the user back to the
  // controller using a signed URL containing the selected
  // access control role.
  // This script assumes that the credentials are
  // submitted on the form created by the example script
  // net-auth.php.
  //
  //
  // Assumptions
  // ===========
  // 1. The controller is configured to include its IP address
  //    and port in the redirection URL and the submitted login
  //    form contains that IP address and port. This allows the
  //    ECP to interact with more than one controller.
  // 2. Whether the script uses HTTP or HTTPS in its redirection
  //    response depends on the value of use_https,
  //    which must be defined in php.ini.
  //    If the value of use_https is 1, then the script uses
  //    HTTPS. If the configuration variable has any other value
  //    or is not defined, then the script uses HTTP. In practice,
  //    an actual site is going to settle on using HTTP or HTTPS.
  //    The scripts can then assume that method is being used
  //    rather than looking up the method in php.ini.
  // The use_https is a user-
  // defined variable. It must be created in php.ini by the
  // web server administrator.
  require_once("ffecp_config.php");
  require_once("crypt_aws_s4.php");
  require_once("common_utilities.php");
  // Some local constants
  const EWC_HTTP_REQ = "http://";
  const EWC_HTTPS_REQ = "https://";
  const EWC_REDIRECT_TARGET = "/ext_approval.php?";
  // The mainline begins here. The utilities are defined after the
  // mainline.
  // 1. Collect the parameters submitted on the login form.
  //    Some of these attributes come from hidden fields.
  $hwc_ip = trim($_REQUEST['hwc_ip']);
  $hwc_port = trim($_REQUEST['hwc_port']);
  $dest = trim($_REQUEST['dest']);
  $token = trim($_REQUEST['token']);
  $username = (isset($_REQUEST['userid'])) ?
    trim($_REQUEST['userid']) : "";
  $passwd = (isset($_REQUEST['passwd'])) ?
    trim($_REQUEST['passwd']) : "";
  $wlan = isset($_REQUEST['wlan']) ?
    trim($_REQUEST['wlan']) : "";
  if(!tokenCheck($token)) {
      printError("Error: <span style='color:red'>Failed to process the request: incorrect
token.</span>");
      exit;
  } else if(isset($hwc_port) && !is_numeric($hwc_port)) {
      printError("Error: <span style='color:red'>Failed to process the request: incorrect
port.</span>");
      exit;
  } else if(!empty($wlan) && !is_numeric($wlan)) {
      printError("Error: <span style='color:red'>Failed to process the request: incorrect
WLAN.</span>");
      exit;
  }
  // For this example the maximum duration of any user's
  // session will be 36000 seconds. The session is terminated
  // no later than this time. After the session is terminated,
  // the user can access the network but will be unauthenticated
  // again.
  $max_duration = 36000;
  // 2. Authenticate the user and select an appropriate role.
  //    Selecting the role is optional. If a role is not specified
  //    for the controller, the controller will apply the default
  //    authenticated role of the WLAN Service that the user is
  //    accessing.
  $assigned_role = authenticate($username, $passwd);
  if (false === $assigned_role) {
      // Failed to authenticate the user.
      // Authenticate prints the error message for
      // the browser and exits.
      exit;
  }
  // 3. Tell the controller that the user is authenticated,
  //    and tell it which role to apply to the user.
  //    3.a Build the URL that needs to be signed.
  $pUrl = makeUnsignedUrl($hwc_ip, $hwc_port, isHttps(), $token,
          $username, $wlan, $assigned_role, $dest,
          $max_duration);
  // 3.b Sign the URL. Otherwise, the role and session
  //     duration options will be ignored by the controller.
  $redirection = SimpleAws::createPresignedUrl(
    $pUrl, 'BigAuthInc', $awsKeyPairs['BigAuthInc'],
      $awsConfig['region'], $awsConfig['service'],
      $awsConfig['expires']);
  if (null == $redirection) {
      // Quietly exit. createPresignedUrl has already
      // reported an error to the browser.
    exit;
  }
  header( 'Location: '.$redirection);
  exit;
  // End of mainline.
  // A method that validates the user's credentials and
  // returns the role to apply to the user. In some cases,
  // this routine might also return the maximum session
  // duration in seconds.
  //
  // For purposes of this example, this procedure is
  // not much more than a stub. The stub can be replaced
  // by any authentication method, such as sending access
  // requests to a backend RADIUS server, or performing
  // a lookup in an application credential database.
  function authenticate($userid, $passwd) {
      if (("" == $userid) || ("" == $passwd)) {
          printError("Invalid Userid or Password. ".
                  "Please press the 'Back' button and try again.");
          // If you generate another login page for the user,
          // be sure to copy the hwc_ip address, hwc_port,
          // token and dest attributes from the submitted
          // login form to the login page.
          return false;
      } else {
          // Return the name of a role to be applied
          // to the station. The role must be defined on
          // the controller or it will substitute the
          // default authenticated role of the VNS that the
          // user is logging into.
          // For purposes of this example, assume all
          // authenticated users get the 'Guest_Access' role.
          return "Guest_Access";
      }
  }
  /**
   * A function that decides whether
   * to use HTTP or HTTPS in the redirect to
   * the controller. This example just uses
   * a php.ini user configuration variable
   * to decide.
   */
  function isHttps() {
      if (get_cfg_var('use_https')) {
          if (1 == get_cfg_var('use_https')) {
              $useHttps = true;
          } else {
              $useHttps = false;
          }
      } else {
          $useHttps = false;
      }
      return $useHttps;
  }
  /**
   * A method that assembles an unsigned URL out of the
   * the input from the user's succesful login
   * @param string  $hwc_ip      IP or FQDN of controller
   * @param int     $hwc_port    Port on controller to receive redirection
   * @param bool    $useHttps    Whether the redirect uses HTTP or HTTPS
   * @param string  $token       Identifier for the station's session
   * @param string  $username    The name the station's user logged in with
   * @param int     $wlanid      Identifier for the WLAN the station is using
   * @param string  $assigned_role Name of the access control role to assign
   * @param string  $dest        The URL the station was trying to get to
   * @param int     $max_duration The maximum length of the station's session.
   */
  function makeUnsignedUrl($hwc_ip, $hwc_port, $useHttps, $token,
          $username, $wlanid, $assigned_role, $dest,
          $max_duration) {
       $redirectUrl = ($useHttps ? EWC_HTTPS_REQ : EWC_HTTP_REQ)
          .$hwc_ip;
       if ((80 != $hwc_port) && (443 != $hwc_port)) {
           $redirectUrl .= ":".$hwc_port;
       }
       $redirectUrl .= EWC_REDIRECT_TARGET
          .'token='. rawurlencode($token)
          .'&wlan='.rawurlencode($wlanid)
          .'&username='.rawurlencode($username)
          .(is_not_empty($dest) ?'&dest='.rawurlencode($dest):'')
          .(is_not_empty($assigned_role) ? '&role='.
                  rawurlencode($assigned_role):'')
          .(is_not_empty($max_duration) ?'&opt27='.$max_duration:'');
       return $redirectUrl;
  }
  ?>
```

common_utilities.php

```
<?php
  // A library of utilities that can be used by PHP scripts
  // comprising an external captive portal.
  // A utility that translates error codes to error messages.
  function code_2_message($code, $content_type)
  {
    $errMsgList = array (
      0 =>
      array (
        'label' => 'Invalid',
        'content' => '<span style=\'color:red\'>Empty id /
password not allowed. Please try again.</span>'
      ),
      1 =>
      array (
        'label' => 'Success',
        'content' => 'Success',
      ),
      2 =>
      array (
        'label' => 'Access Fail',
        'content' => '<span style=\'color:red\'>Userid or
password incorrect. Please try again.</span>',
      ),
      3 =>
      array (
        'label' => 'Fail',
        'content' => '<span style=\'color:red\'>A problem has
occurred while trying to validate your userid & password.<br>Please contact
your system administrator.</span>',
      ),
      4 =>
      array (
        'label' => 'Timeout',
        'content' => '<span style=\'color:red\'>A problem has
occurred while trying to validate your userid & password.<br>Please contact
your system administrator.</span>',
      ),
      5 =>
      array (
        'label' => 'RADIUS shared security key fail',
        'content' => '<span style=\'color:red\'>A problem has
occurred while trying to validate your userid & password.<br>Please contact
your system administrator.</span>',
      ),
      6 =>
      array (
        'label' => 'RADIUS internal error',
        'content' => '<span style=\'color:red\'>A problem has
occurred while trying to validate your userid & password.<br>Please contact
your system administrator.</span>',
      ),
      7 =>
      array (
        'label' => 'Max RADIUS login fail',
        'content' => '<span style=\'color:red\'>Too many users
trying to login at the same time.Please try again later.</span>',
      ),
      8 =>
      array (
        'label' => 'Invalid Login parameters',
        'content' => '<span style=\'color:red\'>Userid or
password incorrect. Please try again.</span>',
      ),
      9 =>
      array (
        'label' => 'General failure',
        'content' => '<span style=\'color:red\'>A problem has
occurred while trying to validate your userid & password.<br>Please contact
your system administrator.</span>',
      ),
      14 =>
      array (
        'label' => 'Invalid third party parameters',
        'content' => '<span style=\'color:red\'>Invalid third
party parameters.</span>',
      ),
      15 =>
      array (
        'label' => 'Authentication in progress failure',
        'content' => '<span style=\'color:red\'>Authentication is
in progress.</span>',
      ),
      17 =>
      array (
        'label' => 'Max concurrent session failure',
        'content' => '<span style=\'color:red\'>Login rejected
because the maximum number of concurrent sessions for this set of credentials
has been reached. Please try again later.</span>',
      ),
      18 =>
      array (
        'label' => 'Identified session not found',
        'content' => '<span style=\'color:red\'>Login failed
because could not find a session for the specified identifiers.</span>'
      ),
      99 =>
      array (
        'label' => 'Timeout while trying to authorize a session',
        'content' => '<span style=\'color:red\'>Login failed
because because the controller took too long to authorize the
session.</span>'
      )
      );
      return (isset($errMsgList[$code])) ?
        $errMsgList[$code][$content_type] :
        "Unrecognized error code: ".$code;
  }
  // General purpose error reporting procedure.
  function printError($errorMsg) {
    header('Content-type: text/html; charset=iso-8859-1');
    print
"<html>\n<head><title>Error</title></head><body>\n<p>\n$errorMsg\n</p>\n</bod
y>\n</html>\n";
  }
  // Use base64 url safe encode/decode when dealing
  // with AES-encrypted strings.
  // encode: '+'=>'-', '/' => '_' , '=' => '!'
  function base64_url_encode($input) {
    return strtr(base64_encode($input), '+/=', '-_!');
  }
  // Decode: '-'=>'+', '_' => '/' , '!' => '='
  function base64_url_decode($input) {
    return base64_decode(strtr($input, '-_!', '+/='));
  }
  // xml parsing functions
  function my_xml2array($contents)
  {
    $xml_values = array();
    if (! isset($contents)) {
      return false;
    }
    $parser = xml_parser_create('');
    if(!$parser) {
      return false;
    }
    xml_parser_set_option($parser, XML_OPTION_TARGET_ENCODING,
                  'UTF-8');
    xml_parser_set_option($parser, XML_OPTION_CASE_FOLDING, 0);
    xml_parser_set_option($parser, XML_OPTION_SKIP_WHITE, 1);
    xml_parse_into_struct($parser, trim($contents), $xml_values);
    xml_parser_free($parser);
    if (!$xml_values) {
      return array();
    }
    $xml_array = array();
    $last_tag_ar =& $xml_array;
    $parents = array();
    $last_counter_in_tag = array(1=>0);
    foreach ($xml_values as $data)
    {
      switch($data['type'])
      {
        case 'open':
          $last_counter_in_tag[$data['level']+1] = 0;
          $new_tag = array('name' => $data['tag']);
          if(isset($data['attributes']))
          $new_tag['attributes'] = $data['attributes'];
          if(isset($data['value']) && trim($data['value']))
          $new_tag['value'] = trim($data['value']);
          $last_tag_ar[$last_counter_in_tag[
$data['level']]] = $new_tag;
          $parents[$data['level']] =& $last_tag_ar;
          $last_tag_ar =& $last_tag_ar[
            $last_counter_in_tag[$data['level']]++];
          break;
        case 'complete':
          $new_tag = array('name' => $data['tag']);
          if(isset($data['attributes']))
          $new_tag['attributes'] = $data['attributes'];
          if(isset($data['value']) &&
            trim($data['value']))
          $new_tag['value'] = trim($data['value']);
          $last_count = count($last_tag_ar)-1;
            $last_tag_ar[ $last_counter_in_tag[$data[
'level' ]]++ ] = $new_tag;
          break;
        case 'close':
          $last_tag_ar =& $parents[$data['level']];
          break;
        default:
          break;
      };
    }
    return $xml_array;
  }
  function get_value_by_path($__xml_tree, $__tag_path)
  {
    $tmp_arr =& $__xml_tree;
    $tag_path = explode('/', $__tag_path);
    foreach($tag_path as $tag_name)
    {
      $res = false;
      foreach($tmp_arr as $key => $node)
      {
        if(is_int($key) && $node['name'] == $tag_name)
        {
          $tmp_arr = $node;
          $res = true;
          break;
        }
      }
      if(!$res) {
        return false;
      }
    }
    if( isset($tmp_arr['value']) ) {
      return $tmp_arr['value'];
    } else {
      return null;
    }
  }
  function is_not_empty($string) {
    return (isset($string) && (0 < strlen($string)));
  }
  //check token format
    function tokenCheck($val){
        return preg_match('/^([a-zA-Z0-9-_!]){0,24}$/', $val);
    }
    //check the mac address
    function macCheck($val){
        return preg_match("/^[A-Fa-f0-9]{2}:[A-Fa-f0-9]{2}:[A-Fa-f0-9]{2}:[A-Fa-f0-9]{2}:
[A-Fa-f0-9]{2}:[A-Fa-f0-9]{2}$/", $val);
    }
    //encode the input string to avoid script attack
    function convertUrlParam($input) {
        return htmlentities($input, ENT_QUOTES);
  }
?>
```

crypt_aws_s4.php

Note
The External Captive Portal and ExtremeCloud Appliance must be time synchronized. AWS4 signature includes a time stamp; therefore, both systems must be configured with the correct date and time when using AWS4 signature.

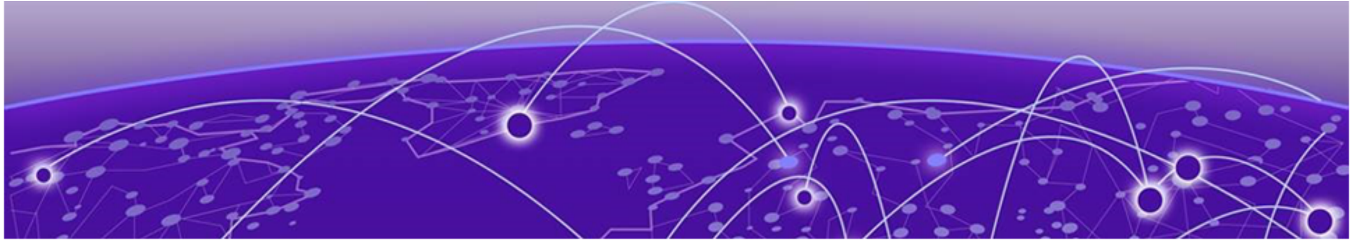
```
<?php
class SimpleAws {
    const     AWS4_ERROR_NONE=0;
    const     AWS4_ERROR_NULL_INPUT=1;
    const     AWS4_ERROR_INPUT_BUFFER_TOO_SMALL=2;
    const     AWS4_ERROR_INVALID_PROTOCOL=3;
    const     AWS4_ERROR_INPUT_URL_TOO_BIG=4;
    const     AWS4_ERROR_INPUT_ID_TOO_BIG=5;
    const     AWS4_ERROR_INPUT_KEY_TOO_BIG=6;
    const     AWS4_ERROR_INVALID_REGION=7;
    const     AWS4_ERROR_INVALID_SIGNATURE=8;
    const     AWS4_ERROR_MISSING_QUERY=9;
    const     AWS4_ERROR_MISSING_QUERY_DATE=10;
    const    AWS4_ERROR_MISSING_QUERY_SIGNED_HEADERS=11;
    const    AWS4_ERROR_MISSING_QUERY_EXPIRES=12;
    const    AWS4_ERROR_MISSING_QUERY_SIGNATURE=13;
    const    AWS4_ERROR_MISSING_QUERY_CREDENTIAL=14;
    const    AWS4_ERROR_MISSING_QUERY_ALGORITHM=15;
    const    AWS4_ERROR_MISSING_QUERY_PARAMS=16;
    const    AWS4_ERROR_MISSING_CRED_PARAMS=17;
   const     AWS4_ERROR_STALE_REQUEST=2001;
   const     AWS4_ERROR_UNKNOWN_IDENTITY=2002;
    const     AWS4_EXTREME_REQUEST="aws4_request";
    const     AWS4_MAX_URL_SIZE= 512;
    const     AWS4_HTTP_REQ = "http://";
    const     AWS4_HTTPS_REQ= "https://";
    const     AWS4_MANDATORY_CRED_PARAMS = 4;
    /**
     * Method to verify the AWS signature based on given full URL address.
         *
     * @param string $pUrl
     * @param array $awsKeyPairs identity, shared secret key pairs
     * @return AWS error code
     */
    public static function verifyAwsUrlSignature($pUrl,
        $awsKeyPairs) {
          // Perform basic validation
        if($pUrl==NULL) {
            return self::AWS4_ERROR_NULL_INPUT;
        }
        if (2*self::AWS4_MAX_URL_SIZE < strlen($pUrl)) {
            return self::AWS4_ERROR_INPUT_URL_TOO_BIG;
        }
        if(stripos($pUrl, self::AWS4_HTTP_REQ)!=0 || stripos($pUrl, self::AWS4_HTTPS_REQ)!
=0) {
            return self::AWS4_ERROR_INVALID_PROTOCOL;
        }
        $urlParams = parse_url($pUrl);
        if (!isset($urlParams['query'])) {
            return self::AWS4_ERROR_MISSING_QUERY;
        }
        $queryParams = explode("&", $urlParams['query']);
        foreach($queryParams AS $el) {
            $arr = explode("=", $el);
            $q[$arr[0]] = $arr[1];
        }
        $valResult = self::validateQueryParms($q);
        if (self::AWS4_ERROR_NONE != $valResult) {
            return $valResult;
        }
        // Done with the basic validations.
        $date = $q['X-Amz-Date'];
        $sign = $q['X-Amz-Signature'];
        $credentVal = rawurldecode($q['X-Amz-Credential']);
        ksort($q);
        // Remove the signature from the list of parameters over
        // which the signature will be recomputed.
        unset($q['X-Amz-Signature']);
        $credentAttrs = explode("/", $credentVal);
        $pKey = $credentAttrs[0];
        if (self::AWS4_MAX_URL_SIZE < strlen($pKey)) {
            return self::AWS4_ERROR_INPUT_KEY_TOO_BIG;
        }
        if(self::AWS4_MANDATORY_CRED_PARAMS > count($credentAttrs)) {
            return self::AWS4_ERROR_MISSING_CRED_PARAMS;
        }
       if (!isset($awsKeyPairs[$pKey])) {
            return self::AWS4_ERROR_UNKNOWN_IDENTITY;
       }
        $scope = $credentAttrs[1]."/".$credentAttrs[2]."/"
         .$credentAttrs[3]."/".$credentAttrs[4];
      $port = $urlParams['port'];
       $host = strtolower($urlParams['host']);
        if($port && (($urlParams['scheme']=='https' && $port !=
         443)||($urlParams['scheme']=='http' && $port != 80))) {
            $host .= ':'.$port;
        }
        $canonical_request = self::getCanonicalFFECPContent($q,
            $host, $urlParams['path']);
        $stringToSign = "AWS4-HMAC-SHA256\n{$date}\n{$scope}\n" .
          hash('sha256', $canonical_request);
        $signingKey = self::getSigningKey($credentAttrs[1], $credentAttrs[2],
            $credentAttrs[3], $awsKeyPairs[$pKey]);
        $mySign = hash_hmac('sha256', $stringToSign, $signingKey);
        if (strcmp($mySign,$sign)){
            return self::AWS4_ERROR_INVALID_SIGNATURE;
        }
        return self::AWS4_ERROR_NONE;
    }
    /**
     * Method to verify that the query parameters contain the elements
     * required in the response to the controller and the ones required to
     * sign the request.
     * @param array $qParams: an associative array in which the key of an
     * entry is the name of a query parameter and the corresponding value
     * is the value of that parameter.
     * @return an AWS_ERROR code.
     */
     private static function validateQueryParms($qParams) {
         if (is_null($qParams)) {
             return self::AWS4_ERROR_MISSING_QUERY;
         }
         if ((!isset($qParams['wlan'])) or (!isset($qParams['token']))
            or (!isset($qParams['dest']))) {
            return self::AWS4_ERROR_MISSING_QUERY_PARAMS;
         }
         if (!isset($qParams['X-Amz-Signature'])) {
             return self::AWS4_ERROR_MISSING_QUERY_SIGNATURE;
         }
         if(!isset($qParams['X-Amz-Algorithm'])) {
             return self::AWS4_ERROR_MISSING_QUERY_ALGORITHM;
         }
         if (!isset($qParams['X-Amz-Credential'])) {
             return self::AWS4_ERROR_MISSING_QUERY_CREDENTIAL;
         }
         if (!isset($qParams['X-Amz-Date'])) {
             return self::AWS4_ERROR_MISSING_QUERY_DATE;
         }
         if (!isset($qParams['X-Amz-Expires'])) {
             return self::AWS4_ERROR_MISSING_QUERY_EXPIRES;
         }
         if (!isset($qParams['X-Amz-SignedHeaders'])) {
             return self::AWS4_ERROR_MISSING_QUERY_SIGNED_HEADERS;
         }
         // The date & expires parameters exist in the request.
         // Verify that the request is not stale or replayed.
         $redirectedAt = DateTime::createFromFormat('Ymd?Gis?',
            $qParams['X-Amz-Date'], new DateTimeZone("UTC"));
         $expires = $qParams['X-Amz-Expires'];
         $now = date_create();
         $delta = $now->getTimestamp() - $redirectedAt->getTimestamp();
         // The following gives some latitude for clocks that are not synched
         if (($delta < -10) or ($delta > $expires)) {
             print("<br>");
             print(date("Y-m-d H:i:sZ", $now->getTimestamp()));
             print("<br>");
```

```
                print("Redirected at: ");
             print(date("Y-m-d H:i:sZ", $redirectedAt->getTimestamp()));
             print("<br>");
                print($now->getTimeZone()->getName());
             print("<br>");
        print($redirectedAt->getTimeZone()->getName());
                print("<br>");
             print($expires);
             print("<br>");
             print($delta);
            return self::AWS4_ERROR_STALE_REQUEST;
         }
         return self::AWS4_ERROR_NONE;
     }
    /**
     * Method to generate the AWS signed URL address
     * @param string $pUrl: the URL that need to be appended with AWS parameters
     * @param string $identity: the AWS identity
     * @param string $sharedSecret: the secret shared with the controller
     * @param string $region:  the region component of the scope
     * @param string $service: the service component of the scope
     * @param int $expires: number of seconds till presigned URL is untrusted.
     * @return URL string with AWS parameters
     */
    public static function createPresignedUrl(
        $pUrl, $identity, $sharedSecret, $region,
        $service, $expires) {
        $urlParams = parse_url($pUrl);
        $httpDate = gmdate('Ymd\THis\Z', time());
        $scopeDate = substr($httpDate, 0, 8);
        $scope = "{$scopeDate}/".$region."/".$service."/".self::AWS4_EXTREME_REQUEST;
        $credential = $identity . '/' . $scope;
        $duration = $expires;
        //set the aws parameters
        $awsParams = array(
            'X-Amz-Date'=>$httpDate,
            'X-Amz-Algorithm'=> 'AWS4-HMAC-SHA256',
            'X-Amz-Credential'=> $credential,
            'X-Amz-SignedHeaders' =>'host',
            'X-Amz-Expires'=> $duration
        );
        parse_str($urlParams['query'],$q);
        $q = array_merge($q, $awsParams);
        ksort($q);
      $port = $urlParams['port'];
       $host = strtolower($urlParams['host']);
        if($port && (($urlParams['scheme']=='https' && $port !=
         443)||($urlParams['scheme']=='http' && $port != 80))) {
            $host .= ':'.$port;
        }
        $canonical_request = self::getCanonicalFFECPContent($q,
         $host, $urlParams['path'], true);
        $stringToSign = "AWS4-HMAC-SHA256\n{$httpDate}\n{$scope}\n" .
            hash('sha256', $canonical_request);
        $signingKey = self::getSigningKey(
                $scopeDate,
                $region,
                $service,
                $sharedSecret
        );
        $q['X-Amz-Signature'] = hash_hmac('sha256', $stringToSign,
                $signingKey);
        $p = substr($pUrl, 0, strpos($pUrl,'?'));
        $queryParams = array();
        foreach($q AS $k=>$v) {
            $queryParams[] = "$k=".rawurlencode($v);
        }
        $p .= '?'.implode('&', $queryParams);
        return $p;
    }
    /**
     * Method to generate the AWS signing key
     * @param string $shortDate: short date format (20140611)
     * @param string $region: Region name (us-east-1)
     * @param string $service: Service name (s3)
     * @param string $secretKey Secret Access Key
     * @return string
     */
    protected static function getSigningKey($shortDate, $region, $service, $secretKey) {
        $dateKey = hash_hmac('sha256', $shortDate, 'AWS4' . $secretKey, true);
        $regionKey = hash_hmac('sha256', $region, $dateKey, true);
        $serviceKey = hash_hmac('sha256', $service, $regionKey, true);
        return  hash_hmac('sha256', self::AWS4_EXTREME_REQUEST, $serviceKey, true);
    }
    /**
     * Create the canonical context for the AWS service
     * @param array $queryHash the query parameter hash
     * @param string $host host name or ip address for the target service
     * @param string $path the service address for the target service
     * @param boolean $encode determine if the query parameter need to be encoded or not.
     * @return string the canonical content for the request
     */
    protected static function getCanonicalFFECPContent($queryHash, $host, $path,
$encode=false) {
        $queryParams = array();
        foreach($queryHash AS $k=>$v) {
            if($encode) {$v = rawurlencode($v);}
        $queryParams[] = "$k=$v";
         }
         $canonical_request = "GET\n"
            .$path."\n"
            .implode('&',$queryParams)."\n"
            .'host:'.$host
            ."\n\nhost\nUNSIGNED-PAYLOAD";
         return $canonical_request;
    }
    /**
     * Create user readable error message
     * @param integer $eid error code after verifying the AWS URL
     * @return string the error message
     */
    public static function getAwsError($eid) {
        $forAws = " for Amazon Web Service request.";
        SWITCH ($eid) {
            case self::AWS4_ERROR_NULL_INPUT:
                $res = "Empty input".$forAws;
            break;
            case self::AWS4_ERROR_INPUT_BUFFER_TOO_SMALL:
                $res = "Input buffer is too small".$forAws;
            break;
            case self::AWS4_ERROR_INVALID_PROTOCOL:
                $res = "Invalid protocol".$forAws;
            break;
            case self::AWS4_ERROR_INPUT_URL_TOO_BIG:
                $res = "Input url is too big".$forAws;
            break;
            case self::AWS4_ERROR_INPUT_ID_TOO_BIG:
                $res = "Input ID is too big".$forAws;
            break;
            case self::AWS4_ERROR_INVALID_REGION:
                $res = "Invalid region".$forAws;
            break;
            case self::AWS4_ERROR_INVALID_SIGNATURE:
                $res = "Invalid signature".$forAws;
            break;
            case self::AWS4_ERROR_MISSING_QUERY:
                $res = "Missing all query parameters".$forAws;
            break;
            case self::AWS4_ERROR_MISSING_QUERY_DATE:
                $res = "Missing query date".$forAws;
            break;
            case self::AWS4_ERROR_MISSING_QUERY_SIGNED_HEADERS:
                $res = "Missing query signed headers".$forAws;
            break;
            case self::AWS4_ERROR_MISSING_QUERY_EXPIRES:
                $res = "Missing query expires".$forAws;
            break;
            case self::AWS4_ERROR_MISSING_QUERY_SIGNATURE:
                $res = "Missing query signature".$forAws;
            break;
            case self::AWS4_ERROR_MISSING_QUERY_CREDENTIAL:
                $res = "Missing query credential".$forAws;
            break;
            case self::AWS4_ERROR_MISSING_QUERY_ALGORITHM:
                $res = "Missing query algorithm".$forAws;
            break;
            case self::AWS4_ERROR_MISSING_QUERY_PARAMS:
                $res = "Missing query parameter".$forAws;
            break;
            case self::AWS4_ERROR_MISSING_CRED_PARAMS:
                $res = "Missing credential parameters".$forAws;
            break;
            case self::AWS4_ERROR_STALE_REQUEST:
                $res = "Invalid request date".$forAws;
            break;
            case self::AWS4_ERROR_UNKNOWN_IDENTITY:
                $res = "Unrecognized identity or identity without a shared secret.";
            break;
            default:
                $res = "Successfully validated".$forAws;
            break;
        }
        return $res;
    }
    /**
     * Return the AWS validation error message
     * @param string $pUrl
     * @return string the error message
     */
    public function getUrlValidationResult($pUrl) {
        $eid = self::verifyAwsUrlSignature($pUrl);
        return self::getAwsError($eid);
     }
  }
?>
```

ffecp-config.php

```
<?php
  // This file contains PHP associative arrays holding the relatively
  // static configuration for this ECP application. A real application
  // might read the data in from an XML or '.ini' file.
  // An associative array of identity => shared secret pairs.
  // This example only uses the first one. Any printable ASCII
  // alphanumeric string can be use for the identity and shared
  // secret so long as both the ECP and the controller use the
  // same pair.
  $awsKeyPairs = array(
      'BigAuthInc'=>'secretferqrer123456667',
      'testingidentity1'=>'secretferqrer123456668',
      'testingidentity2'=>'secretferqrer123456669'
  );
  // Aws Signature-related Configuration
  // Region and service are used to build the scope.
  // Expires is the maximum amount of time the signed URL
  // should be trusted.
  $awsConfig = array(
      'region' => 'world',
      'signature'=> 'v4',
      'service'=>'ecp',
      'expires'=>60
  );
?>
```

N



Glossary

Chalet

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

CLI

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

Data Center Connect

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

Extreme Defender for IoT

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

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

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

Extreme Management Center

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

ExtremeAnalytics

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

ExtremeCloud Appliance

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

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

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

ExtremeCloud

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

ExtremeCloud™ IQ

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

ExtremeControl

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

ExtremeSwitching

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

ExtremeWireless

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

ExtremeXOS

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

Index