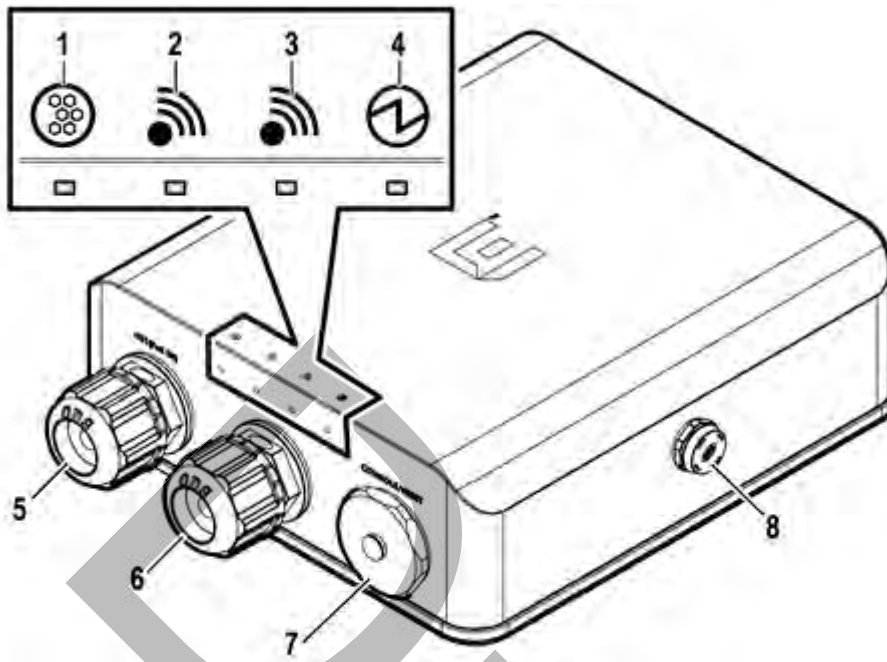


AP3917 LED Indicators

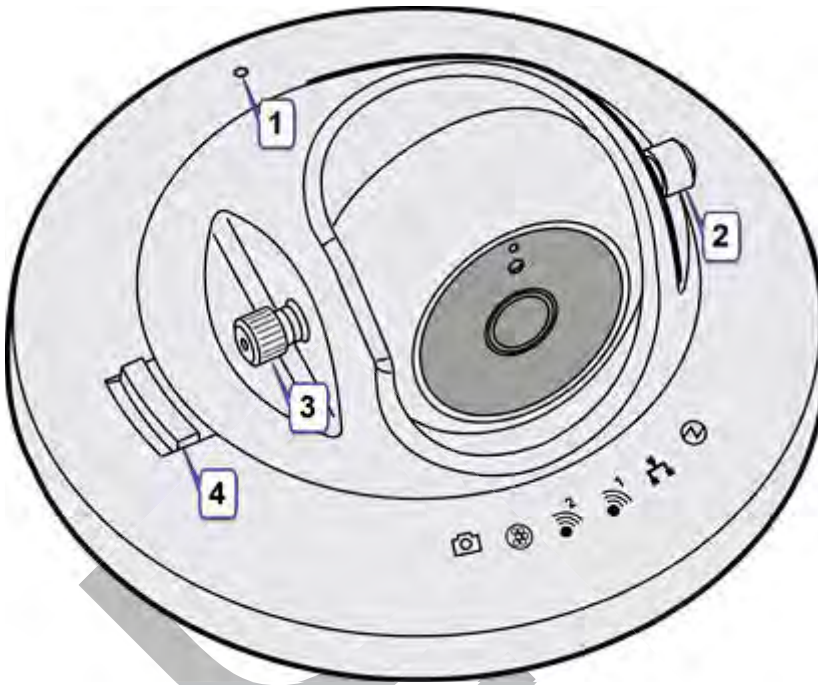
**Figure 59: AP3917i LEDs and Features****Table 26: AP3917 LEDs**

Item	Status Color	Description
1 (IoT Radio) 	Blue	Indicates that the IoT application is running.
2 (5 GHz radio) 	Green	Indicates that the radio is enabled.
3 (2.4 GHz radio) 	Green	Indicates that the radio is enabled.
4 (Status LED) 	Green	Indicates AP is working normally.
	Amber	Indicates System Failure.

Table 27: AP3917 Features

Item	Description
5	Ethernet Port 1 (POE IN)
6	Ethernet Port 2 (Client Port)
7	Console
8	Gore Vent

AP3916 LED Indicators

**Figure 60: Front View of AP3916ic**

The following features are on the front of the AP:

Item	Description
1 - Reset Button	The power reset button is recessed and located on the top of the AP. Use a tool to press the reset button.
2 - Cap	Remove the caps to access the thumbscrews.
3 - Thumbscrew	The thumbscrews let you adjust and set the tilt angle of the camera.
4 - Locking Pin	The locking pin lets you adjust and set the rotational position of the camera.

The following LEDs are located on the top cover of the AP:

Table 28: LEDs

Symbol	Description
	Camera
	IoT (BLE or 802.15.4)

Table 28: LEDs (continued)

Symbol	Description
	Radio 2 (2.4 GHz)
	Radio 1 (5 GHz)
	LAN 1 (Ethernet 1)
	Status

AP3915i LED Indicators

The AP3915i has the following LEDs:

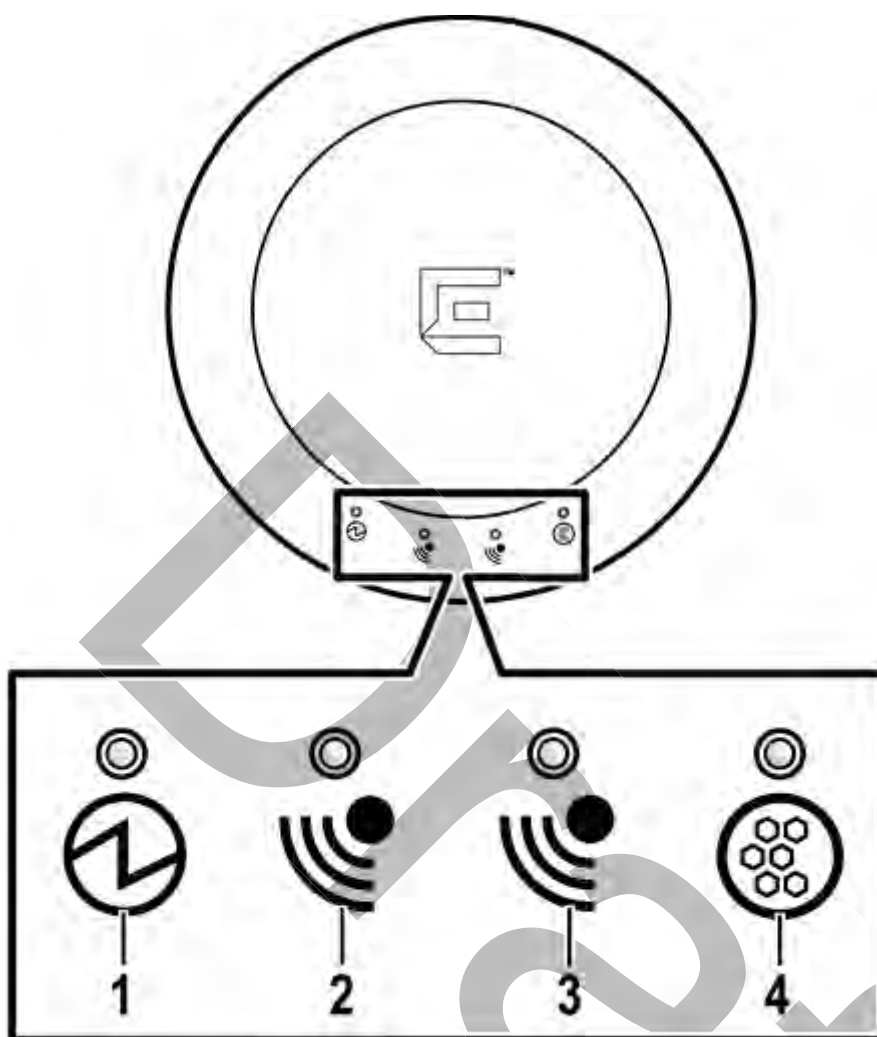


Figure 61: AP3915i LEDs

Table 29: AP3915i LEDs

Item	Status	Description
1 (Status LED) 	Green	Indicates AP is working normally.
	Amber	Indicates System Failure.
2 (2.4 GHz radio) 	Green	Indicates radio is enabled.
3 (5 GHz radio) 	Green	Indicates radio is enabled.
4 (IoT Radio) 	Blue	Indicates IoT application is running.

NEW! AP3915e LED Indicators

AP3915e access points have LED indicators on the front of the box. The LEDs provide the status of the access point indicating on, off, and network activity.

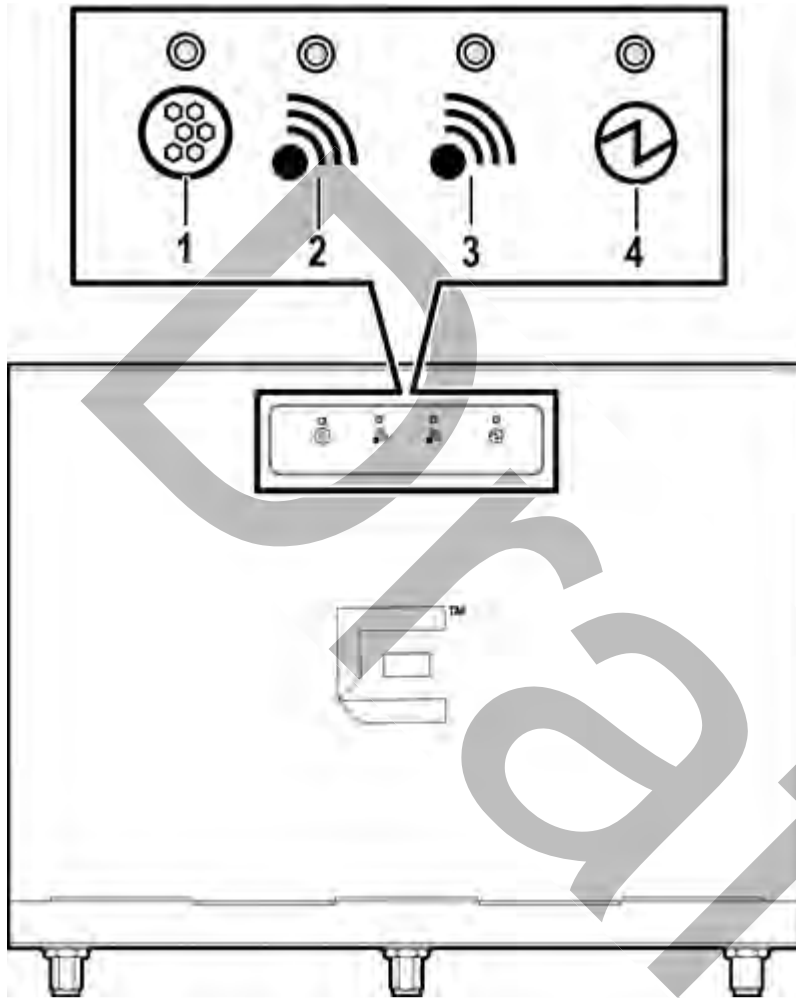


Figure 62: AP3915e Top View

Table 30: AP3915e LED Indicators

Item	Status	Description
1 (IoT Radio) 	Blue	Indicates IoT application is running.
2 (5 GHz radio) 	Green	Radio 1, 5GHz. Indicates radio is enabled.

Table 30: AP3915e LED Indicators (continued)

Item	Status	Description
3 (2.4 GHz radio) 	Green	Radio 2, 2.4GHz. Indicates radio is enabled.
4 (Status LED) 	Green	Indicates AP is working normally.
	Amber	Indicates System Failure.

AP3912 LED Indicators

The AP3912i has six LED indicators. The LEDs provide status information on the current state of the AP3912i.

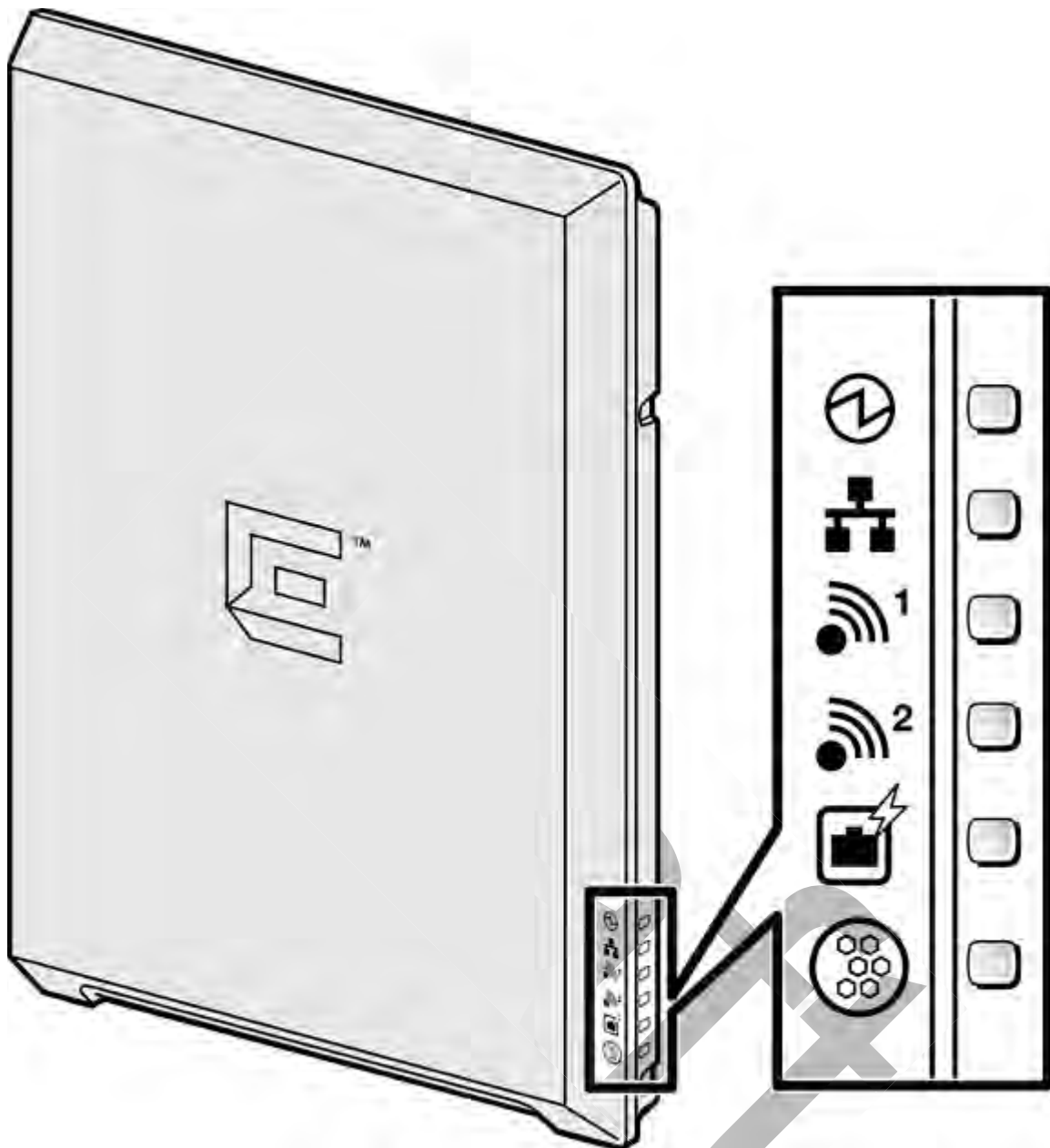


Figure 63: AP3912i LEDs

Table 31: AP3912i LED Status Indicators

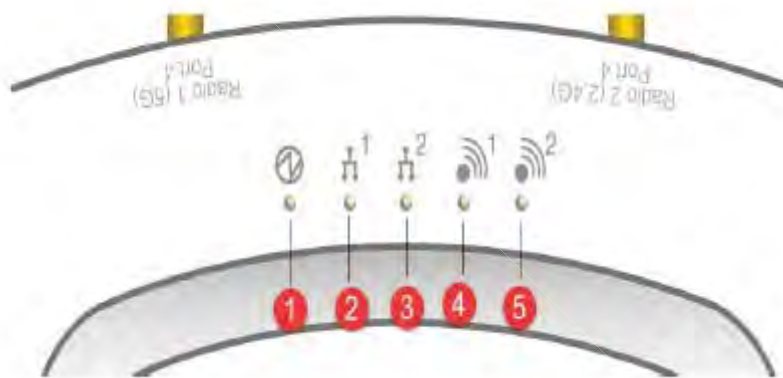
LED	Indicator	Status	Description
1 (Status)		Green	Indicates AP is working normally
		Amber	System failure
2 (Ethernet link state) LAN 1		Amber	Indicates a valid 1Gbps Ethernet link
		Green	Indicates a valid 10Mbps or 100Mbps Ethernet link

Table 31: AP3912i LED Status Indicators (continued)

LED	Indicator	Status	Description
3 (Radio 1)	 1	Green	Indicates Radio 1 is enabled
4 (Radio 2)	 2	Green	Indicates Radio 2 is enabled
5 (PSE Client Port)		Green	Uplink AP port detects AF <i>PoE</i> (<i>Power over Ethernet</i>) source
6 (BLE)		Green	Indicates IoT (BLE or 802.15.4) is enabled

AP3935, AP3965 LED Indicators

The AP3935 and AP3965 provide 5 LED indicators. The LEDs provide status information on the current state of the AP.

**Table 32: LED Indications AP3935 and AP3965**

LED	Status	Description
1 (AP status)	On Green	Indicates that the AP is working normally.
	Flashing Green	Indicates: - running a self test - loading software program
	On Amber	Indicates a CPU/system failure.
2 (Ethernet link state) LAN 1	On Green	Indicates a valid 100Mbps Ethernet link.
	On Amber	Indicates a valid 1Gbps Ethernet link.

Table 32: LED Indications AP3935 and AP3965 (continued)

LED	Status	Description
	Off	Indicates the link is down.
3 (Ethernet link state) LAN 2	On Green	Indicates a valid 100Mbps Ethernet link.
	On Amber	Indicates a valid 1Gbps Ethernet link.
	Off	Indicates the link is down.
4 (Radio 1 (5 GHz) status)	On Green	Indicates Radio 1 is enabled.
	Off	Indicates Radio 1 is not on.
5 (Radio 2 (2.4 GHz) status)	On Green	Indicates Radio 2 is enabled.
	Off	Indicates Radio 2 is not on.

38xx Series Wireless APs

The following AP38xx model access points are supported by ExtremeWireless:

- WS-AP3801i
- WS-AP3805i/e
- WS-AP3865
- WS-AP3825

WS-AP3801i LED Indicators

The WS-AP3801i provides three LED indicators. The LEDs provide status information on the current state of the WS-AP3801i.

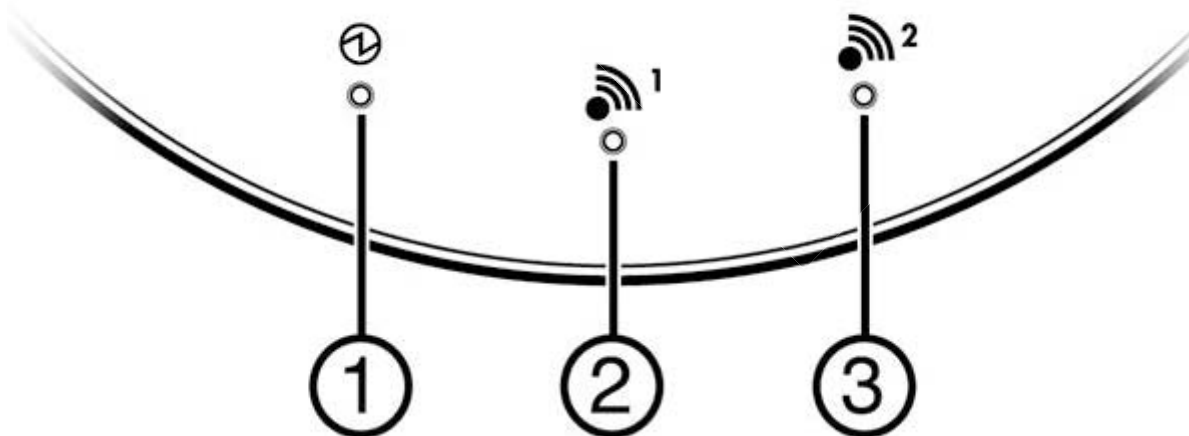
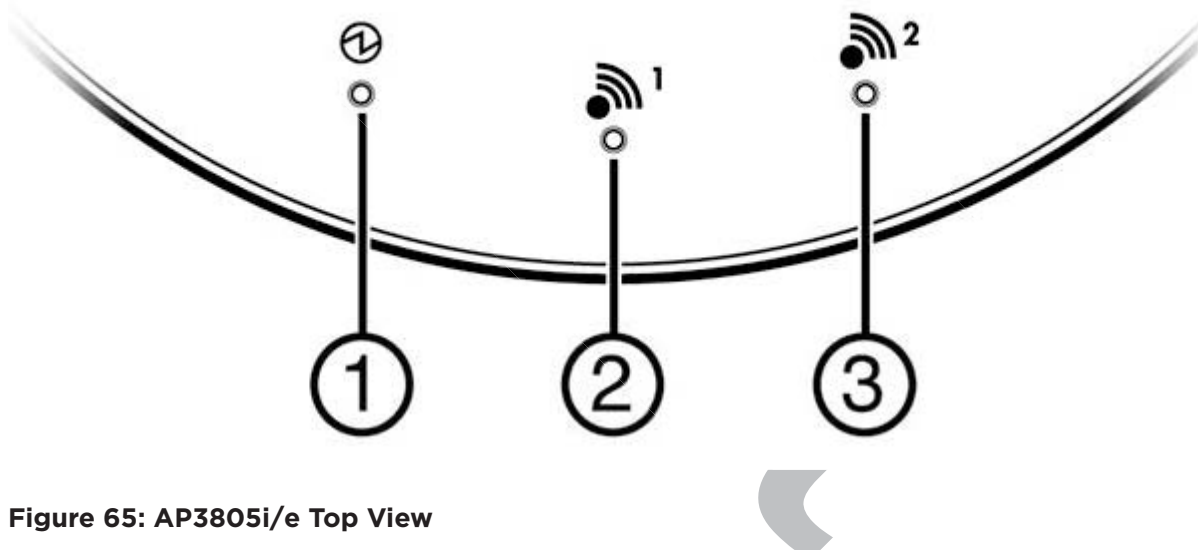
**Figure 64: AP3801i Top View**

Table 33: AP3801i LED Status Indicators

LED	Status	Description
1 (Power)	On Green	Indicates the AP3801 is working normally.
	Flashing Green	Indicates: • running a self test • loading software program
	On Red	Indicates a CPU or system failure.
2 (Radio 1 Status)	On Green	Indicates Radio 1 (5.0 GHz) is enabled.
3 (Radio 2 Status))	On Green	Indicates Radio 2 (2.4 GHz) is enabled.

WS-AP3805i/e LED Indicators

The WS-AP3805i/e provides three LED indicators. The LEDs provide status information on the current state of the WS-AP3805i/e.

**Figure 65: AP3805i/e Top View****Table 34: AP3805i/e LED Status Indicators**

LED	Status	Description
1 (Power)	On Green	Indicates the AP3805 is working normally.
	Flashing Green	Indicates: • running a self test • loading software program
	On Red	Indicates a CPU or system failure.

Table 34: AP3805i/e LED Status Indicators (continued)

LED	Status	Description
2 (Radio 1 Status)	On Green	Indicates Radio 1 (5.0 GHz) is enabled.
3 (Radio 2 Status))	On Green	Indicates Radio 2 (2.4 GHz) is enabled.

WS-AP3865 LED Indicators

The WS-AP3865e has five LED indicators. The LEDs provide status information on the current state of the WS-AP3865e.

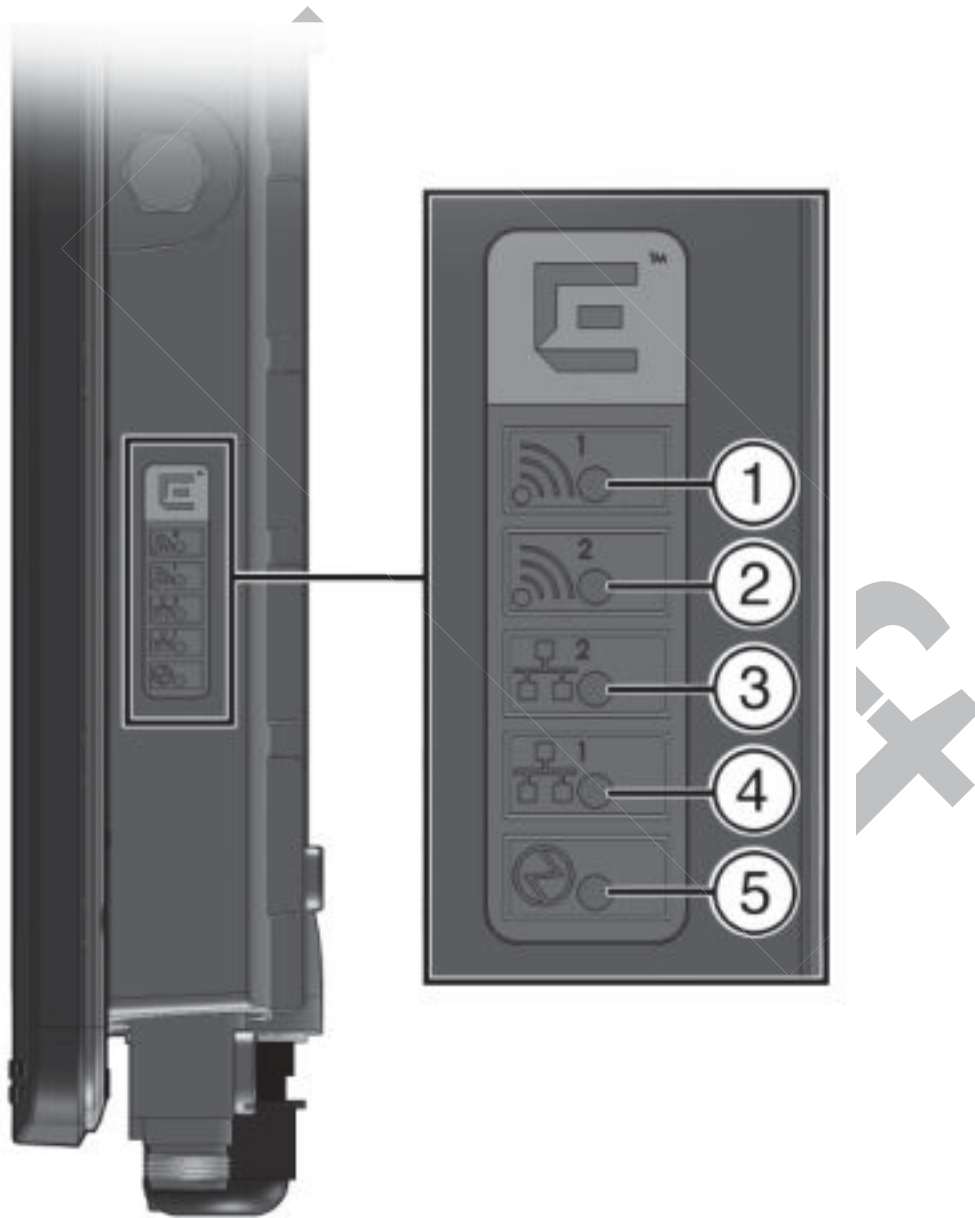
**Figure 66: WS-AP3865e LEDs**

Table 35: WS-AP3865 LED Indications

LED	Status	Description
1 (Radio 1 status)	On Green	Indicates Radio 1 is enabled.
	Off	Indicates Radio 1 is not on.
2 (Radio 2 status)	On Green	Indicates Radio 2 is enabled.
	Off	Indicates Radio 2 is not on.
3 (Ethernet link state) LAN 2	On Green	Indicates a valid 100Mbps Ethernet link.
	On Amber	Indicates a valid 1Gbps Ethernet link.
	Off	Indicates the link is down.
4 (Ethernet link state) LAN 1	On Green	Indicates a valid 100Mbps Ethernet link.
	On Amber	Indicates a valid 1Gbps Ethernet link.
	Off	Indicates the link is down.
5 (AP status)	On Green	Indicates the WS-AP3865 is working normally.
	Flashing Green	Indicates: • running a self test • loading software program
	On Amber	Indicates a CPU/system failure.

WS-AP3825 LED Indicators

The WS-AP3825 has five LED indicators. The LEDs provide status information on the current state of the WS-AP3825.

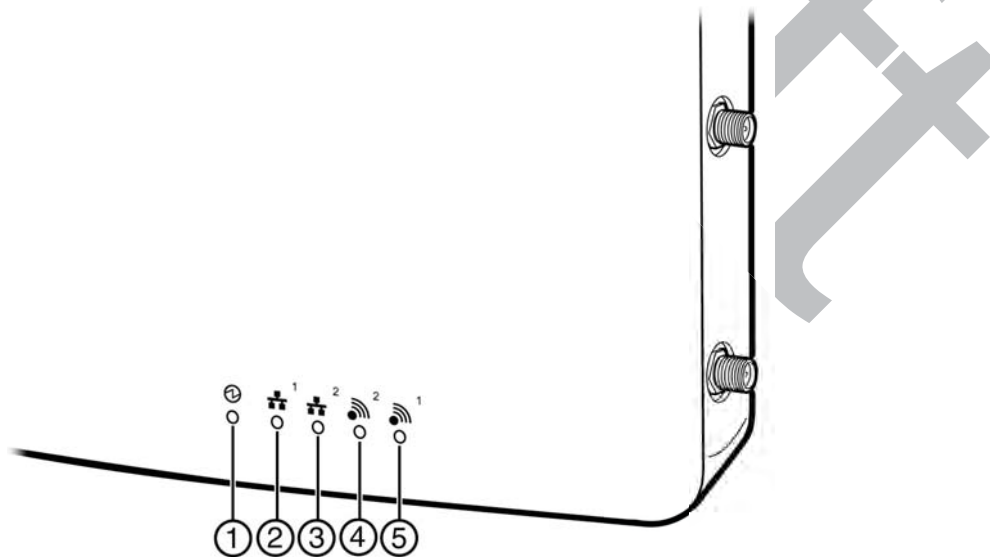
**Figure 67: WS-AP3825 LEDs**

Table 36: WS-AP3825 LED Indications

LED	Status	Description
1 (AP status)	On Green	Indicates the WS-AP3825 is working normally.
	Flashing Green	Indicates: • running a self test • loading software program
	On Amber	Indicates a CPU/system failure.
2 (Ethernet link state) LAN 1	On Green	Indicates a valid 100Mbps Ethernet link.
	On Amber	Indicates a valid 1Gbps Ethernet link.
	Off	Indicates the link is down.
3 (Ethernet link state) LAN 2	On Green	Indicates a valid 100Mbps Ethernet link.
	On Amber	Indicates a valid 1Gbps Ethernet link.
	Off	Indicates the link is down.
4 (Radio 2 status)	On Green	Indicates Radio 2 is enabled.
	Off	Indicates Radio 2 is not on.
5 (Radio 1 status)	On Green	Indicates Radio 1 is enabled.
	Off	Indicates Radio 1 is not on.

37xx Series Wireless APs

The ExtremeWireless AP37xx series are 802.11n APs, with added capacity for intrusion threat detection and prevention capability. The LED indicators on these are described in the following subsections:

- [WS-AP3710 LED Indicators](#) on page 256
- [WS-AP3715 LED Indicators](#) on page 257
- [AP3765/AP3767/W786C LED Status](#) on page 259

WS-AP3705i LED Indicators

The WS-AP3705i provides four LED indicators (see [Figure 68](#)). The LEDs provide status information (see [Table 37](#)) on the current state of the WS-AP3705i.

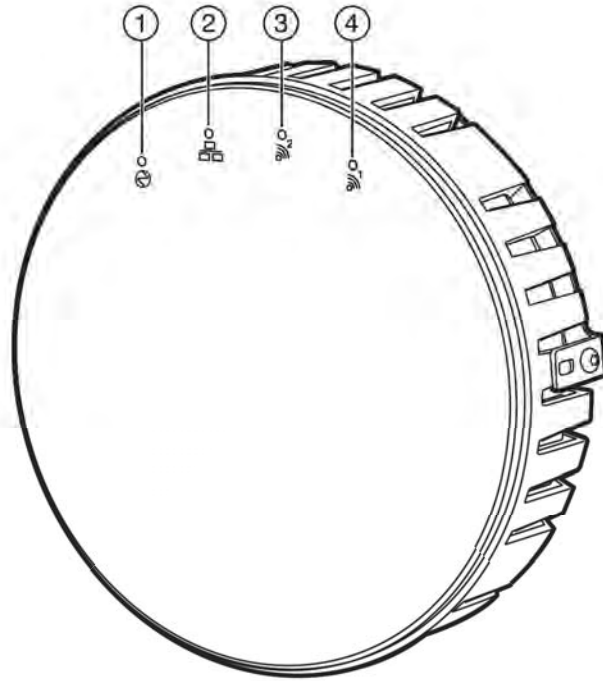


Figure 68: AP3705i Top View

Table 37: AP3705i LED Status Indicators

LED	Status	Description
1 (Power)	On Green	Indicates the AP3705 is working normally.
	Flashing Green	Indicates: • running a self test • loading software program
	On Red	Indicates a CPU or system failure.
2 (Ethernet Link)	On Blue	Indicates a valid 1Gbps Ethernet link.
	On Green	Indicates a valid 100Mbps Ethernet link.
	Off	Indicates the link is down.
3 (Radio 2 Status)	On Green	Indicates Radio 2 (2.4 GHz) is enabled.
4 (Radio 1 Status))	On Green	Indicates Radio 1 (5 GHz) is enabled.

WS-AP3710 LED Indicators

Both models (AP3710i and AP3710e) of the WS-AP3710 have four LED indicators, shown in [Figure 69](#). The LEDs provide status information, described in [Table 38](#) on page 257, on the current state of the WS-AP3710.

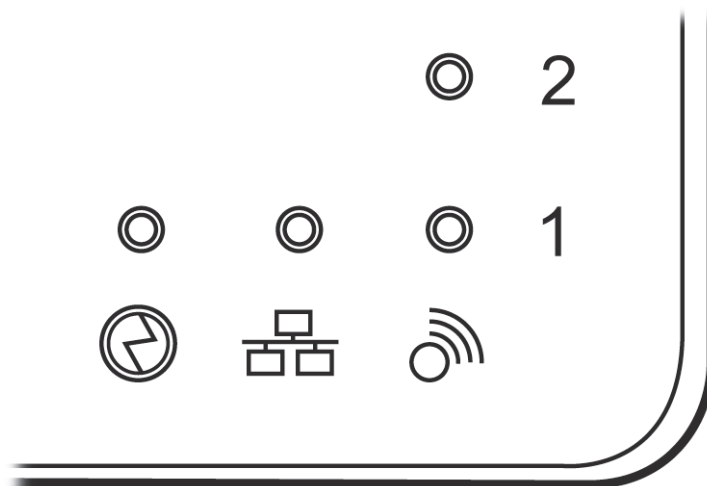


Figure 69: WS-AP3710 LEDs (Front, lower right)

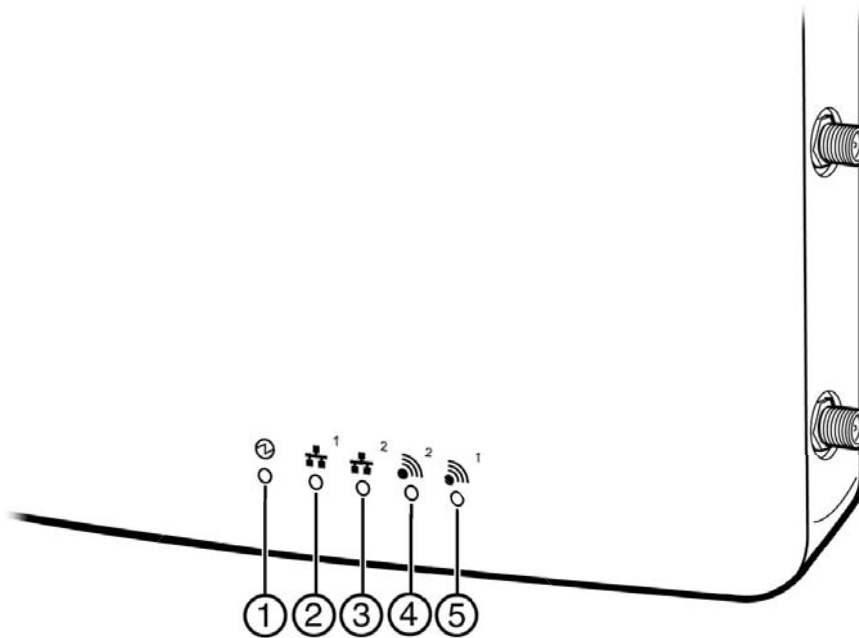
		
Identifies Power Indicator LED	Identifies LAN Indicator LED	Identifies Radio Indicator LEDs

Table 38: WS-AP3710 LED Indications

LED	Status	Description
1 (AP status)	On Green	Indicates the WS-AP3710 is working normally.
	Flashing Green	Indicates: - running a self test - loading software program
	On Red	Indicates a CPU/system failure.
2 (Ethernet link state)	On Green	Indicates a valid 100Mbps Ethernet link.
	On Blue	Indicates a valid 1Gbps Ethernet link.
	Off	Indicates the link is down.
3 (Radio 1 status)	On Green	Indicates Radio 1 is enabled.
4 (Radio 2 status)	On Green	Indicates Radio 2 is enabled.

WS-AP3715 LED Indicators

The WS-AP3715 has six LED indicators, as shown in [Figure 70](#). The LEDs provide status information, described in [Table 39](#) on page 258, on the current state of the WS-AP3715.

**Figure 70: WS-AP3715 LEDs**

 Identifies Power Indicator LED	 Identifies LAN Indicator LED	 Identifies Radio Indicator LEDs
--	--	---

Table 39: WS-AP3715 LED Indications

LED	Status	Description
1 (AP status)	On Green	Indicates the WS-AP3825 is working normally.
	Flashing Green	Indicates: • running a self test • loading software program
	On Amber	Indicates a CPU/system failure.
2 (Ethernet link state) LAN 1	On Green	Indicates a valid 100Mbps Ethernet link.
	On Amber	Indicates a valid 1Gbps Ethernet link.
	Off	Indicates the link is down.
3 (Ethernet link state) LAN 2	On Green	Indicates a valid 100Mbps Ethernet link.
	On Amber	Indicates a valid 1Gbps Ethernet link.
	Off	Indicates the link is down.
4 (Radio 2 status)	On Green	Indicates Radio 2 is enabled.
	Off	Indicates Radio 2 is not on.
5 (Radio 1 status)	On Green	Indicates Radio 1 is enabled.
	Off	Indicates Radio 1 is not on.

AP3765/AP3767/W786C LED Status

The ExtremeWireless AP3765i, W786C, AP3765e, and AP3767e models are nearly identical in appearance (e models have external antenna ports). LED status indicator displays are the same on all three models. The frontal view of the housing cover (see [Figure 71](#)) displays six LEDs. These LEDs provide information on operating status.

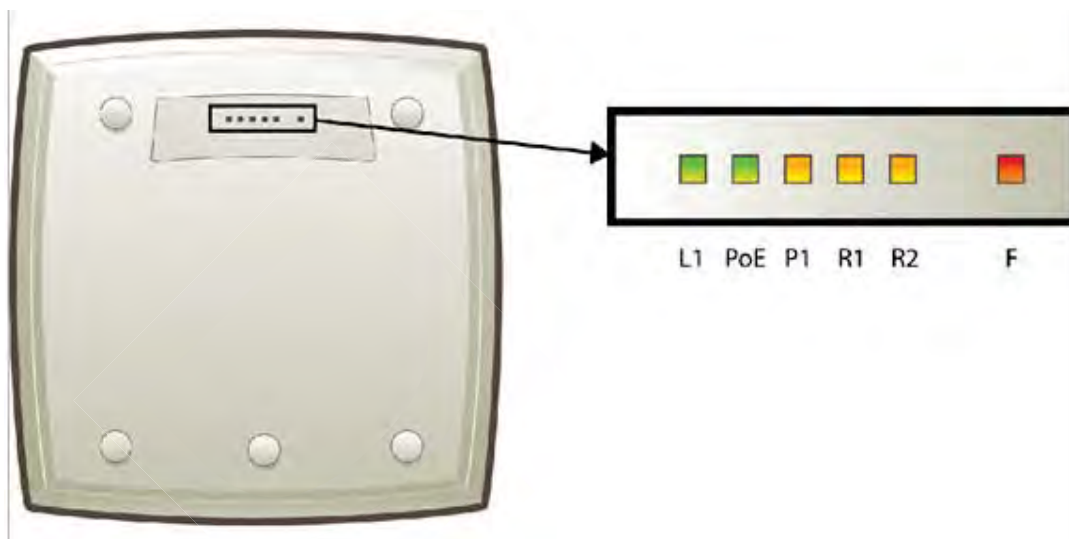


Figure 71: Wireless Outdoor AP3765/AP3767/W786C LEDs

Table 40: AP3765/AP3767 LED Status Indicators

LED	Color	Meaning
L1	Green	Power LED. When on, indicates AP power is sourced from power supply.
PoE	Green	PoE power LED. When on, indicates AP power is sourced from PoE.
P1	Green	Ethernet port 1 LED. When green on, indicates Ethernet port activity. When off, Ethernet is off, WDS is enabled.
R1	Green	WLAN Radio 1 LED. When green on, indicates Radio 1 is active.
R2	Green	WLAN Radio 2 LED When green on, indicates Radio 2 is active.
F	Red	Error LED. When on, indicates error. When off, indicates normal operation, AP connected to controller.

Configuring Wireless AP LED Behavior

You can configure the behavior of the LEDs so that they provide the following information:

Table 41: LED Operational Modes

LED Mode	Information Displayed
Off	Displays fault patterns only. LEDs do not light when the AP is fault free and the discovery is complete.
Normal	Identifies the AP status during the registration process during power on and boot process.
Identify	All LEDs blink simultaneously approximately two to four times every second.

You can configure the AP LED mode when you configure the following:

- An individual AP.
- Multiple APs simultaneously.
- Default AP behavior.

**Note**

You can configure all four AP LED modes if you configure an individual AP or multiple APs simultaneously. If you configure the default AP behavior, the only LED modes available are Off and Normal.

Related Links

[AP Multi-Edit Properties](#) on page 111

[AP Properties Tab - Advanced Settings](#) on page 164

Configuring Operational Mode for One AP

To configure the AP LED operational mode when configuring an individual wireless AP:

- 1 From the top menu, click **AP > APs**.
- 2 In the AP list, click a wireless AP (not the check box).
The **AP Configuration** page displays with the **AP Properties** tab exposed.
- 3 On the **AP Properties** tab, click **Advanced**.
- 4 In the **LED** field, select an LED operational mode.
See [Table 41](#) on page 260 for a description of each option.

Configuring Operational Mode with Multi-Edit

To set the AP LED Operational Mode when using the AP Multi-edit feature:

- 1 From the top menu, click **AP**.
- 2 Select the check box for more than one AP.
- 3 Click **Actions > Multi Edit**.
The **Multi Edit** dialog displays.
- 4 In the LED field, select an LED operational mode.
See [Table 41](#) on page 260 for a description of each option.

Configuring AP Operational Mode Default Behavior

To set the AP LED Operational Mode when configuring default AP behavior:

- 1 From the top menu, click **AP**.
- 2 In the left pane, click **Global > Default Settings**.
- 3 Click the AP tab that corresponds to the type of AP that you want to configure.
- 4 Click **Advanced**. The **Advanced** window displays.

In the LED field, select an LED operational mode. See [Table 41](#) on page 260 for a description of each option.

Draft

5 Configuring Topologies

Topology Overview

Configuring the Admin Port

Configuring a Basic Data Port Topology

Creating a Topology Group

Edit or Delete a Topology Group

Enabling Management Traffic

Layer 3 Configuration

Exception Filtering

Multicast Filtering

Topology Overview

A topology can be thought of as a *VLAN (Virtual LAN)* with at least one egress port, and optionally, sets of services, exception filters and multicast filters.

ExtremeWireless makes use of a number of different topology modes:

- Admin - This is the topology to which the management plane's administration interface is assigned. It is the only topology that can be assigned to the administration interface. The interface must be present at layer 3 to receive management related traffic such as ssh, https and RADIUS. This interface supports IPv4 and IPv6.
- Physical - A physical mode topology is intended to be used for management purposes. A physical topology can also be used to carry station traffic for a "3rd party VNS", a VNS that uses non-Extreme Networks wireless APs. A physical topology can be assigned to any of the data plane ports on the controller.
- Routed - For this type of topology the controller acts as a router between the topology's VLAN and the rest of the network. The controller's data plane ports can be assigned to this type of topology.
- Bridged Traffic Locally at EWC - For this type of topology the controller bridges traffic for the station through its interfaces, rather than routing the traffic. For this type of topology the station's "point of presence" on the wired network is the data plane port assigned to the topology.
- Bridged Traffic Locally at AP - This type of topology is assigned to APs. For this type of topology the AP bridges traffic between its wired and wireless interfaces without involving the controller. The station's "point of presence" on the wired network for a bridged at AP topology is the AP's wired port.



Note

IPv6 is supported for Layer 2 bridging for both B@AC and B@AP topologies.

- Fabric Attach - The Fabric Attach topology type allows an AP to attach to a Shortest Path Bridging (Fabric Connect) Network. The client component on the AP communicates directly with the server on an edge switch (or it can communicate with the server through a proxy) to allow the AP to request VLAN to I-SID (backbone Service Identifier [IEEE 802.1 ah] mappings). The Fabric Attach

topology type is similar to B@AP with the added I-SID parameter. Fabric Attach can be configured on a controller anywhere a B@AP topology can be configured.

Define the following parameters on the **Topologies** configuration page:

- VLAN ID and associated L2 port
- L3 (IP) interface presence and the associated IP address and subnet range
- The rules for using *DHCP (Dynamic Host Configuration Protocol)*
- Enabling or disabling the use of the associated interface for management/control traffic
- Selection of an interface for AP registration
- Multicast filter definition
- Exception filter definition

The controller has two types of Layer 2 ports:

- Admin - which can only be used for management-related purposes. It is connected directly on the management plane of the controller.
- Physical - which can be used for a variety of purposes, including bridging and routing as well as management. The physical ports are directly connected to the controller's data plane, although traffic received at physical ports may be sent up the exception path to the management plane.

At most, one physical topology can be enabled for the multicast support for Routed VNS. This can be configured on the new physical port GUI.

Related Links

[Configuring the Admin Port](#) on page 263

[Fabric Attach Topology](#) on page 269

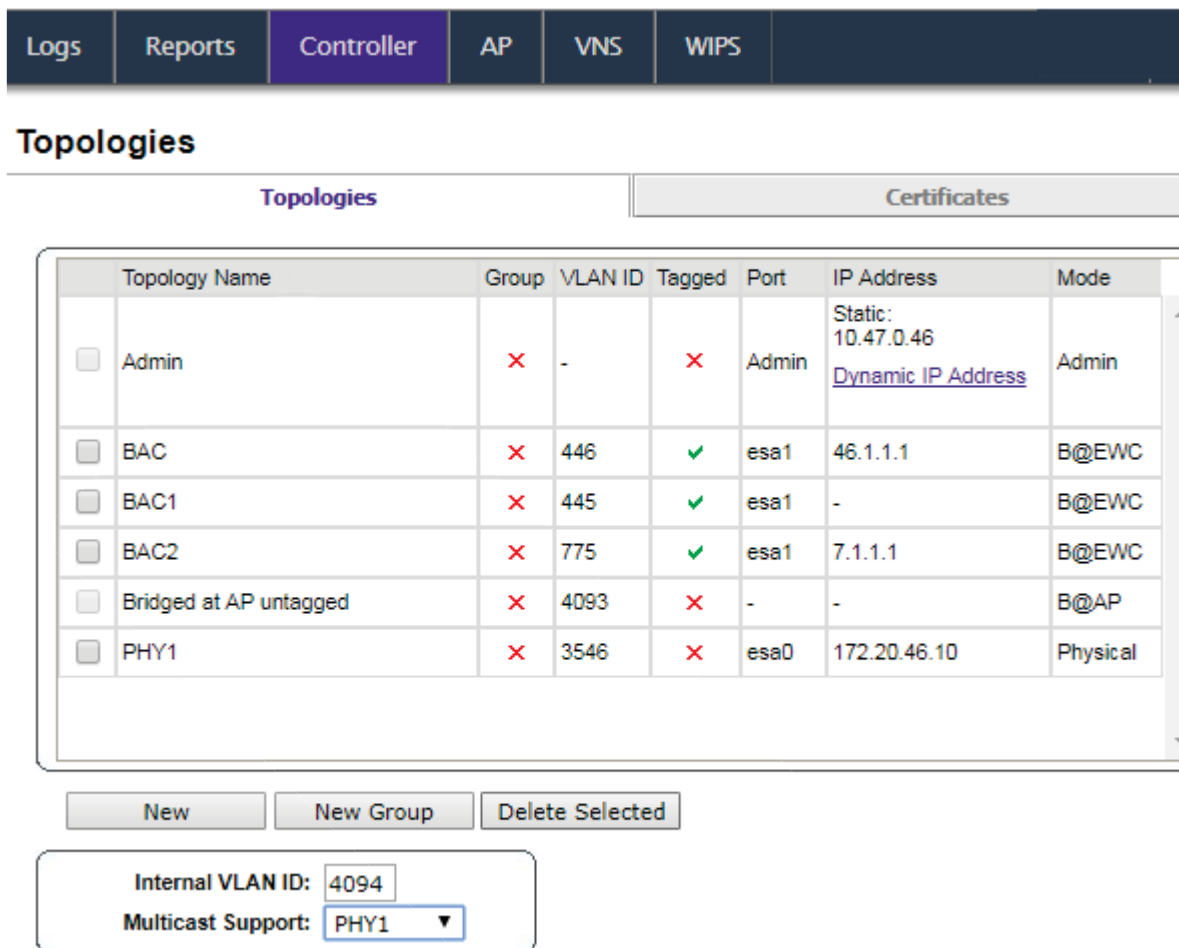
Configuring the Admin Port

The Admin port is a physical ethernet port directly connected to the controller's management plane. It provides a dedicated connection to a secure management *VLAN*. The controller can use the Admin port to interact with RADIUS, *SNMP (Simple Network Management Protocol)*, and Extreme Management Center servers.

- 1 From the top menu, click **Controller**.

- 2 In the left pane, click **Network** > **Topologies**.

The **Topologies** tab is displayed.



Topology Name	Group	VLAN ID	Tagged	Port	IP Address	Mode
☐ Admin	×	-	×	Admin	Static: 10.47.0.46 Dynamic IP Address	Admin
☐ BAC	×	446	✓	esa1	46.1.1.1	B@EWC
☐ BAC1	×	445	✓	esa1	-	B@EWC
☐ BAC2	×	775	✓	esa1	7.1.1.1	B@EWC
☐ Bridged at AP untagged	×	4093	×	-	-	B@AP
☐ PHY1	×	3546	×	esa0	172.20.46.10	Physical

Internal VLAN ID:
 Multicast Support:

Figure 72: Network Topologies

- 3 To change any of the associated Admin parameters, click on the Admin topology entry. The **Edit Topology** dialog appears.

The screenshot shows the 'Edit Topology' dialog box with the title 'Topology: Admin'. It has a 'General' tab selected. On the left, under 'Core', there is a box containing 'Name: Admin' and 'Mode: Admin'. On the right, under 'Layer 3', there is a checked checkbox. Below it, the 'Layer 3 - IPv4' section contains fields for 'Static IP Address' (192.168.14.11), 'Mask' (255.255.255.0), 'MTU' (1500), and 'Gateway' (192.168.14.1). Below that, the 'Layer 3 - IPv6' section contains fields for 'Static IPv6 Address', 'Static IPv6 Gateway', 'Prefix Length' (empty), and 'MTU' (1500). There is also a 'Dynamic IP Address' section with a list box containing '1 fe80:0000:0000:0000:862b:2bff:fe70:b94d'. A 'Refresh' button is at the bottom of the IPv6 section. At the very bottom of the dialog are buttons for 'New', 'Delete', 'Save', and 'Cancel'.

Figure 73: Edit Topology

- 4 Under Core, the Admin port **Name** and **Mode** are not configurable.
- 5 Under Layer 3 - IPv4, the following settings are available:

The **Static IP Address** specifies the address assigned by the administrator.

In the **Mask** field, type the appropriate subnet mask for the IP address (typically, 255.255.255.0).

The **MTU** value specifies the Maximum Transmission Unit or maximum packet size for this topology. The fixed value is 1500 bytes for physical topologies. The maximum MTU can be increased to 1800 bytes by enabling Jumbo Frames support (for more information, see [Setting Up the Data Ports](#) on page 51).

The **Gateway** field specifies the IP address of the default gateway for the Admin port.

- 6 Under Layer 3 - IPv6, the following settings are available:
- The **Static IPv6 Address** field specifies the address assigned by the administrator.
 - The **Static IPv6 Gateway** field specifies the IP address of the default gateway for the Admin port.
 - The **Prefix Length** field specifies the length of the IPv6 prefix. Maximum is 64 bits.
 - The **MTU** value specifies the Maximum Transmission Unit or maximum packet size for this topology. The fixed value is 1500 bytes for physical topologies. The maximum MTU can be increased to 1800 bytes by enabling Jumbo Frames support (for more information, see [Setting Up the Data Ports](#) on page 51).
 - The **Dynamic IP Address** lists the current auto-generated IPv6 addresses assigned to the Admin port.

Note



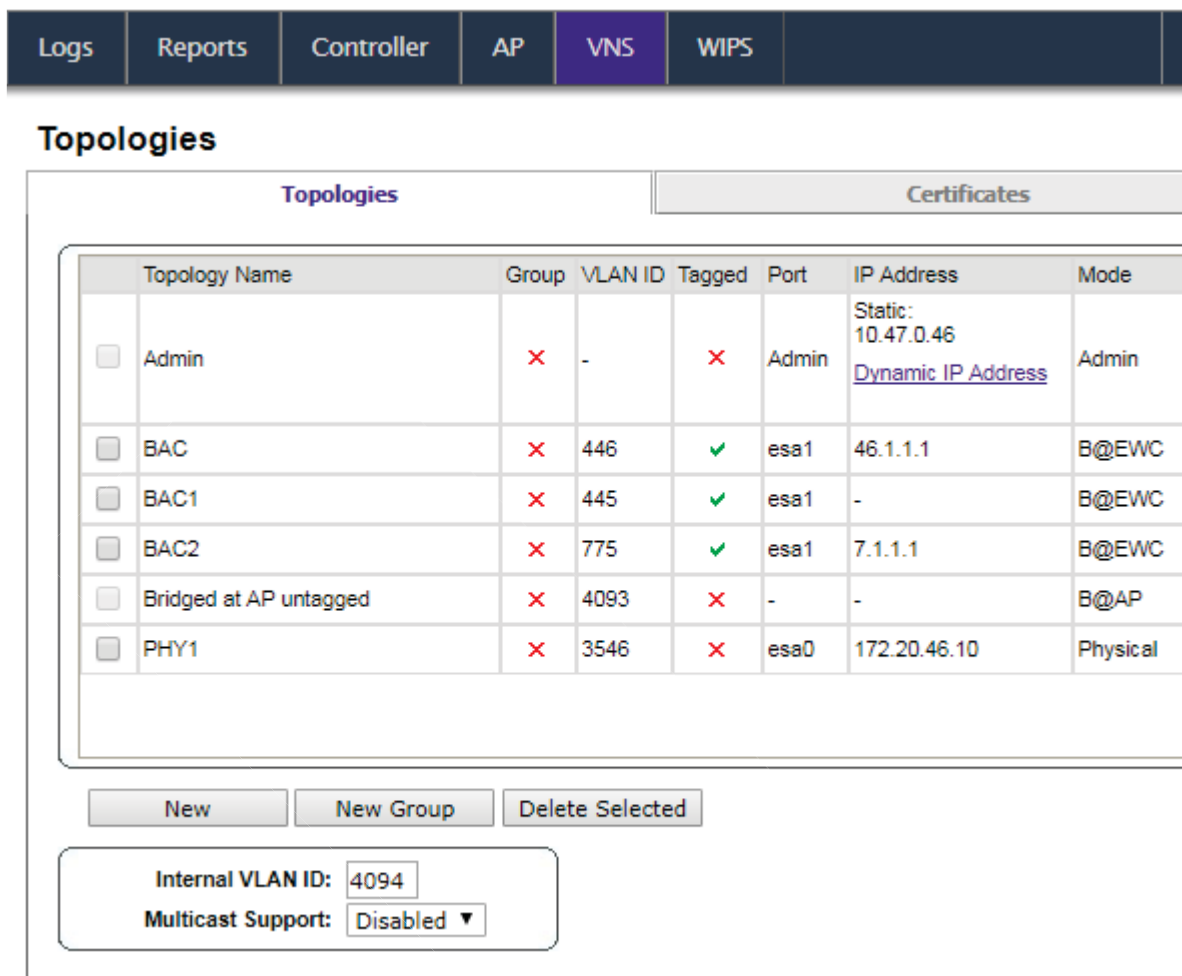
IPv6 supports multiple addresses on the same port including auto-generated addresses such as a link-local address, or an address created by combining the Router Advertisement prefix with the interface ID. Auto-generated addresses generated via the Router Advertisement prefix are dynamic and their availability depends on the existence of the prefix (or lack of) in the Router Advertisement.

- 7 Click **Refresh** to refresh the list of Dynamic IP Addresses and click **Save** .
Or, click **Cancel** to close the **Edit Topology** dialog without saving any changes to the port configuration.

Configuring a Basic Data Port Topology

To configure a basic data port topology:

- 1 From the top menu, click **VNS**. Then, in the left pane, select **Topologies**. The **Topologies** window displays.



Topology Name	Group	VLAN ID	Tagged	Port	IP Address	Mode
☐ Admin	×	-	×	Admin	Static: 10.47.0.46 Dynamic IP Address	Admin
☐ BAC	×	446	✓	esa1	46.1.1.1	B@EWC
☐ BAC1	×	445	✓	esa1	-	B@EWC
☐ BAC2	×	775	✓	esa1	7.1.1.1	B@EWC
☐ Bridged at AP untagged	×	4093	×	-	-	B@AP
☐ PHY1	×	3546	×	esa0	172.20.46.10	Physical

Internal VLAN ID:
 Multicast Support:

Figure 74: Configuring a Topology

- 2 Select the topology to edit or click **New** to create a new topology.
For more information, see [Configuring a Basic Topology](#) on page 267.

Configuring a Basic Topology

To configure a basic topology:

- 1 From the top menu, click **VNS**. Then, in the left pane, select **Topologies**.
The **Topologies** window displays.

- 2 Select the topology to edit or click **New** to create a new topology.

The screenshot shows the VNS configuration interface. At the top is a navigation bar with tabs: Logs, Reports, Controller, AP, VNS (selected), WIPS. Below the navigation bar is the 'Topology:' section. The 'General' tab is active, showing configuration fields for a topology. The 'Core' section has a 'Name' field with the value 'name' and a 'Mode' dropdown set to 'Bridge Traffic Locally at EWC'. The 'Layer 2' section has a 'VLAN Setting' with 'VLAN ID' set to '1' (range 1-4094), radio buttons for 'Untagged' (selected) and 'Tagged', and a 'Port' dropdown set to '-'. The 'Status' section has a 'Synchronize' checkbox checked, with a red note below it: 'Replicated when Synchronize Configuration is enabled'. To the right is the 'Multicast Filters' tab, which is currently inactive, showing 'Layer 3' and 'Layer 3 - IPv4' sections.

Figure 75: Configuring a basic topology

- 3 On the **General** tab, enter a name for the topology in the **Name** field.
- 4 Select a mode of operation from the **Mode** drop-down list. Choices are:
 - **Physical** — VLAN identifier (1 - 4094), with at least one layer 2 member port (no mu associated).
 - **Routed** — Routed topologies do not require Layer 2 configuration (controller internal VLAN identifier from valid range 1- 4094), and Layer 3 configuration. See [Layer 3 Configuration](#) on page 272 for more information.
 - **Bridge Traffic Locally at AP** — Requires Layer 2 configuration. Does not require Layer 3 configuration. Bridge Traffic at the AP VNSs do not require the definition of a corresponding IP address since all traffic for users in that VNS will be directly bridged by the Wireless AP at the local network point of attachment (VLAN at AP port).
 - **Bridge Traffic Locally at EWC** — Requires Layer 2 configuration. May optionally have Layer 3 configuration. Layer 3 configuration would be necessary if services (such as DHCP, captive portal, etc.) are required over the configured network segment, or if controller management operations are intended to be done through the configured interface.
 - **Fabric Attach** — The Fabric Attach topology type is similar to B@AP with the added I-SID parameter. Fabric Attach can be configured on a controller anywhere a B@AP topology can be configured. See **Bridge Traffic Locally at AP**.

- 5 Configure the Layer 2 **VLAN Settings**, depending on the previously selected Mode.
 - For **Physical**, enter a VLAN identifier (2 - 4094), with at least one layer 2 member port (no MU associated).
 - For **Bridge Traffic Locally at EWC**, enter a VLAN identifier (2- 4094) that is valid for your system and enter the port to which this VLAN is attached to, according to the networking deployment model pre-established during planning.
 - For **Bridge Traffic Locally at AP**, enter a VLAN identifier (1 - 4094), 4094 is reserved for Internal VLAN ID.
 - For **Fabric Attach**, enter a VLAN identifier (1 - 4094), 4094 is reserved for Internal VLAN ID and an I-SID (service identifier).
 - Specify whether the VLAN configuration is **Tagged** or **Untagged**.
 - To eliminate ARP Request Broadcast on the Wireless network, select **ARP Proxy**. ARP Proxy applies to traffic for **Bridge Traffic Locally at AP** Topologies. ARP Proxy is configurable per topology.
 - For **Port**, select the Physical (Ethernet) or *LAG (Link Aggregation Group)* data port. For more information, see [Viewing and Changing the L2 Ports Information](#) on page 52.
- 6 (Optional) Provide a netmask in the **Mask** field for topologies that do not support Layer 3. This option makes it possible to add the **Framed-IP-Netmask** attribute to the client RADIUS accounting request packets when the topology does not support Layer 3.
- 7 Click **Save** to save your changes.

These steps are sufficient to create and save a topology. The following configuration options are optional and depend on the mode of the topology.

Related Links

[Layer 3 Configuration](#) on page 272

[Creating a Topology Group](#) on page 270

[Enabling Management Traffic](#) on page 272

Fabric Attach Topology

The Fabric Attach topology type allows an AP to attach to a Shortest Path Bridging (Fabric Connect) Network. The client component on the AP communicates directly with the server on an edge switch (or it can communicate with the server through a proxy) to allow the AP to request VLAN to I-SID (backbone Service Identifier [IEEE 802.1 ah] mappings). The Fabric Attach topology type is similar to B@AP with the added I-SID parameter. Fabric Attach can be configured on a controller anywhere a B@AP topology can be configured.



Note

When Fabric Attach is configured, LLDP (Link Layer Discovery Protocol) is automatically enabled on all APs associated with the topology. The setting cannot be disabled by users.

The switch requires that the VLAN/I-SID mapping is unique per port per switch, therefore only one AP per switch port is allowed. The exception is WDS (Wireless Distribution Service). When using WDS, only the root AP in the mesh has a Fabric Attach client. The root AP handles all VLAN/I-SID mapping for all APs in its mesh.

The controller enforces the unique VLAN/I-SID requirement for each Fabric Attach topology. A single controller supports up to 94 VLAN/I-SID mappings. This is a limit of LLDP.

APs connected to a Fabric-enabled switch automatically use the default management VLAN that is configured on the switch. Moving an AP from a Fabric-enabled switch to a non Fabric-enabled switch requires a factory default reset to connect to the new management VLAN.



Note

In a mobility scenario that includes a local and foreign controller, make sure the Fabric Attach topology configuration is the same on each controller, ensuring that an AP that moves between controllers has the same set of topologies.

Fabric Attach is supported on all AP39xx series access points.

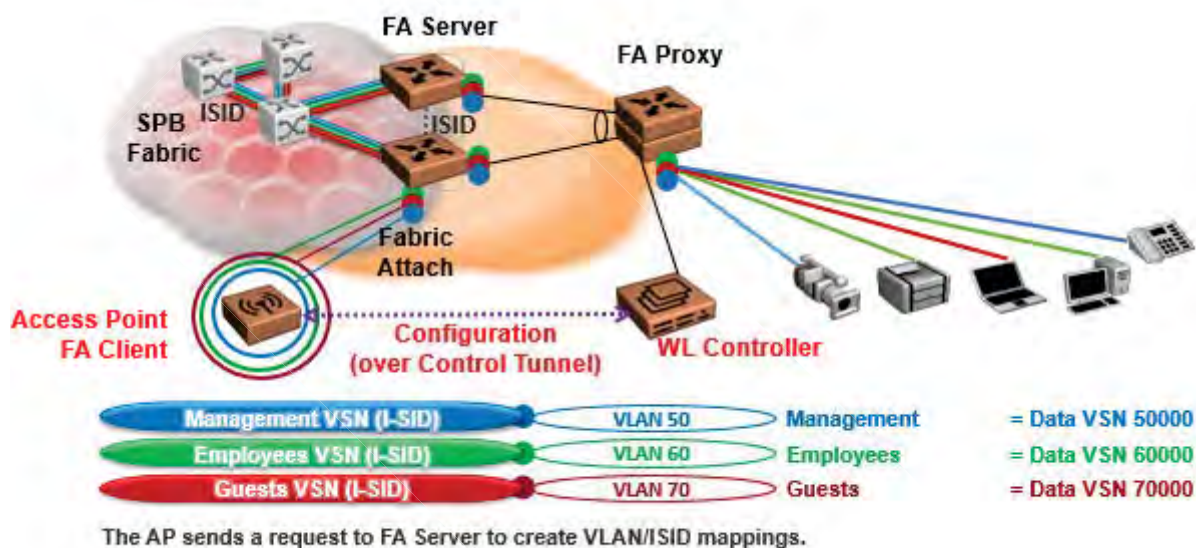


Figure 76: Fabric Attach for FA Clients — Automated Network Services

Important



In rare cases, an unstable AP image can cause the AP to revert to an image that does not support Fabric Attach topologies. Connectivity between the AP and controller is preserved because the configuration is preserved, but the Fabric Attach feature will not work until the AP v10.41 image is restored. Therefore, we recommend that you upgrade an AP running v10.31 twice, ensuring that both the current and previous images are v10.41.

Creating a Topology Group

A topology group is a list of topologies with a unique name and a VLAN ID of its own. A topology group's name must be unique across topology groups and topologies since it will be used anywhere the topology name can be used. All the topologies in a defined group have the same type. For example, if the topology group mode is Routed, it only contains Routed topologies. The maximum number of topology groups for all platforms is 32.

- 271

Figure 77: Topology Group

- ## Edit or Delete a Topology Group

- 6 Click **Save**.
- 7 You can also delete the topology group from the **Topologies** tab.
 - a From the top menu, click **VNS**.
 - b From the left pane, click **Topologies**.
 - c Select the check box for the topology group to delete and click **Delete Selected**.
 - d Click **Save**.

Enabling Management Traffic

If management traffic is enabled for a VNS, it overrides the built-in exception filters that prohibit traffic on the controller data interfaces. For more information, see [Policy Rules](#) on page 288.

To enable management traffic for a topology:

- 1 From the top menu, click either **Controller** or **VNS**. Then, in the left pane, select **Topologies**.
- 2 Select the desired physical or Routed topology. If the Layer 3 parameters are not displayed, check the **Layer 3** check box.
- 3 Select the **Management Traffic** check box.
- 4 Click **Save**.

Layer 3 Configuration

This section describes configuring Layer 3 of the network topology. Layer 3 configuration includes defining IP addresses, [DHCP](#) options, Next Hop and [OSPF \(Open Shortest Path First\)](#) parameters, for Physical port, Routed, and Bridge Traffic Locally at EWC topologies. Not all topologies support Layer 3.



Note

IPv6 is not supported in Layer 3 configuration.

Related Links

[IP Address Configuration](#) on page 272

[DHCP Configuration](#) on page 274

[Defining a Next Hop Route and OSPF Advertisement](#) on page 277

IP Address Configuration

The L3 (IP) address definition is only required for Physical port and Routed topologies. For Bridge Traffic Locally at EWC topologies, L3 configuration is optional. L3 configuration would be necessary if services such as [DHCP](#), captive portal, AP registration (with up to 4 topologies) are required over the configured network segment or if controller management operations are intended to be done through the configured interface.

Bridge Traffic Locally at AP topologies can define a Mask and do not require the definition of a corresponding IP address since all traffic for users in that VNS will be directly bridged by the AP at the local network point of attachment ([VLAN](#) at AP port).

To define the IP address for the topology:

- 1 From the top menu, click **Controller > Topologies**, or **VNS > Topologies**.
- 2 Click **New** to create a new topology or select the topology you want to define the IP address for. The **Topologies** window is displayed. Depending on the preselected options, two or three tabs are displayed.

The screenshot shows the 'Topology: BAC' configuration interface. The top navigation bar includes 'Logs', 'Reports', 'Controller', 'AP', 'VNS' (selected), 'WIPS', and 'Help'. A 'Logout' link is in the top right. The main content area has three tabs: 'General' (selected), 'Multicast Filters', and 'Exception Filters'. Under the 'General' tab, there are three sections: 'Core' with 'Name: BAC' and 'Mode: Routed'; 'Layer 2' with 'VLAN Setting: VLAN ID: 446 (1 - 4094)' and radio buttons for 'Untagged' (selected) and 'Tagged'; and 'Status' with a 'Synchronize' checkbox and a red note 'Replicated when Synchronize Configuration is enabled'. The 'Layer 3' section is expanded, showing 'Layer 3: [checked]', 'Layer 3 - IPv4' with 'Gateway: 46.1.1.1', 'Mask: 255.255.255.0', 'DHCP: Local Server' (with a 'Configure' button), 'MTU: 1436', and 'Management Traffic: [checked]'.

Figure 78: Configuring IP Address for Routed Topology

- 3 For IP interface configuration for **Routed** topologies, configure the following Layer 3 parameters.
 - a In the **Gateway** field, type the controller's own IP address in that VNS. This IP address is the default gateway for the VNS. The controller advertises this address to the wireless devices when they sign on. For routed VNSs, it corresponds to the IP address that is communicated to MUs (in the VNS) as the default gateway for the VNS subnet. (MUs target the controller's interface in their effort to route packets to an external host.)
-
- Note**
The Gateway field only supports IPv4 addresses.
-
- b In the **Mask** field, type the appropriate subnet mask for the IP address. This separates the network portion from the host portion of the address (typically, 255.255.255.0).
 - c If desired, enable Management traffic.
 - 4 For IP interface configuration for **Bridge Traffic Locally at EWC Topologies**, configure the following Layer 3 parameters.

The screenshot shows the VNS configuration interface for a topology named 'BAC'. The 'General' tab is active, displaying settings for Layer 2 and Layer 3. In the Layer 2 section, the 'Name' is 'BAC', the 'Mode' is 'Bridge Traffic Locally at EWC', the 'VLAN ID' is 446, and the 'Port' is 'esa1'. In the Layer 3 section, 'Strict Subnet Adherence' is checked, the 'Interface IP' is 46.1.1.1, the 'Mask' is 255.255.255.0, and 'DHCP' is set to 'Local Server'. The 'AP Registration' checkbox is unchecked, and 'Management Traffic' is checked. A 'Synchronize' checkbox is also present with a note: 'Replicated when Synchronize Configuration is enabled'.

Figure 79: IP Address for Bridged Traffic Locally

- 1 In the **Interface IP** field, type the IP address that corresponds to the controller's own point of presence on the VLAN. In this case, the controller's interface is typically not the gateway for the subnet. The gateway for the subnet is the infrastructure router defined to handle the VLAN.
- 2 In the **Mask** field, type the appropriate subnet mask for the IP address. This separates the network portion from the host portion of the address (typically, 255.255.255.0).
- 3 Configure Strict Subnet Adherence.
- 4 If desired, configure AP Registration. If selected, wireless APs can use this port for discovery and registration.
- 5 If desired, enable Management traffic.

Related Links

[Enabling Management Traffic](#) on page 272

DHCP Configuration

You can configure *DHCP* settings for all modes except **Bridge Traffic Locally at AP** mode since all traffic for users in that VNS will be directly bridged by the AP at the local network point of attachment (*VLAN* at AP port). DHCP assignment is disabled by default for Bridged to VLAN mode. However, you can enable DHCP server/relay functionality to have the controller service the IP addresses for the VLAN (and wireless users).

To configure DHCP options:

- 1 Click **VNS > Topologies > General** and enable Layer 3.
- 2 From the **DHCP** drop-down list, select one of the following options and click **Configure**.
 - **Local Server** if the controller's local DHCP server is used for managing IP address allocation.
 - **Use Relay** if the controller forwards DHCP requests to an external DHCP server on the enterprise network. DHCP relay bypasses the local DHCP server for the controller and allows the enterprise to manage IP address allocation to a VNS from its existing infrastructure.
- 3 If you selected **Local Server**, the following window displays. Configure the following parameters:

- 1 In the **Domain Name** box, type the external enterprise domain name server to be used.
- 2 In the **Lease default** box, type the default time limit. The default time limit dictates how long a wireless device can keep the DHCP server assigned IP address. The default value is 36000 seconds (10 hours).
- 3 In the **DNS Servers** box, type the IP Address of the Domain Name Servers to be used.
- 4 In the **WINS** box, type the IP address if the DHCP server uses Windows Internet Naming Service (WINS).
- 5 Check the **Enable DLS DHCP Option** check box if you expect optiPoint WL2 wireless phone traffic on the VNS. DLS is a Siemens application that provides configuration management and software deployment and licensing for optiPoint WL2 phones.
- 6 In the **Gateway** field, type the controller's own IP address in that topology. This IP address is the default gateway for the topology. The controller advertises this address to the wireless devices when they sign on. For routed topologies, it corresponds to the IP address that is communicated to wireless clients as the default gateway for the subnet. (wireless clients target the controller's interface in their effort to route packets to an external host).

For a Bridge traffic locally at the EWC topology, the IP address corresponds to the controller's own point of presence on the VLAN. In this case, the controller's interface is typically not the gateway for the subnet. The gateway for the subnet is the infrastructure router defined to handle the VLAN.

- 7 The **Address Range** boxes (from and to) populate automatically with the range of IP addresses to be assigned to wireless devices using this VNS, based on the IP address you provided.
 - To modify the address in the **Address Range from** box, type the first available address.

- To modify the address in the **Address Range to** box, type the last available address.
- If there are specific IP addresses to be excluded from this range, click Exclusion(s). The **DHCP Address Exclusion** dialog is displayed.

Figure 81: DHCP Address Exclusion

- In the **DHCP Address Exclusion** dialog, do one of the following:
 - To specify an IP range, type the first available address in the **From** box and type the last available address in the **to** box. Click **Add** for each IP range you provide.
 - To specify an IP address, select the **Single Address** option and type the IP address in the box. Click **Add** for each IP address you provide.
 - To save your changes, click **OK**.
- 1 The **Broadcast Address** box populates automatically based on the Gateway IP address and subnet mask of the VNS.
 - 2 Click **Close**.

Figure 80: DHCP Configuration

- 4 If you selected **Use Relay**, a **DHCP** window displays.
 - a in the **DHCP Servers** box, type the IP address of the DHCP server to which DHCP discover and request messages will be forwarded for clients on this VNS. The controller does not handle DHCP requests from users, but instead forwards the requests to the indicated DHCP server.

Note



The DHCP Server must be configured to match the topology settings. In particular for Routed topologies, the DHCP server must identify the controller's interface IP as the default Gateway (router) for the subnet. Users intending to reach devices outside of the subnet will forward the packets to the default gateway (controller) for delivery upstream.

- 5 To save your changes, click **Save**.

Defining a Next Hop Route and OSPF Advertisement

The next hop definition allows the administrator to define a specific host as the target for all non-VNS targeted traffic for users in a VNS. The next hop IP identifies the target device to which all VNS (user traffic) will be forwarded to. Next-hop definition supersedes any other possible definition in the routing table.

If the traffic destination from a wireless device on a VNS is outside of the VNS, it is forwarded to the next hop IP address, where this router applies role and forwards the traffic. This feature applies to unicast traffic only. In addition, you can also modify the *OSPF* route cost.

OSPF is an interior gateway routing protocol developed for IP networks based on the shortest path first or link-state algorithm. Using OSPF, a host that obtains a change to a routing table or detects a change in the network immediately distributes the information to all other hosts in the network so that all will have the same routing table information. The host using OSPF sends only the part that has changed, and only when a change has taken place.

To define a Next Hop Route and OSPF Advertisement:

- 1 From the top menu, click **VNS**.
- 2 In the left pane, expand the **Topologies** pane, then click the Routed topology for which you want to define a next-hop route.
- 3 In the Layer 3 area, click the **Configure** button. The *DHCP* configuration dialog displays.



Figure 82: DHCP configuration

- 4 In the **Next Hop Address** box, type the IP address of the next hop router on the network through which you wish all traffic on the VNS using this Topology to be directed.

- 5 In the **OSPF Route Cost** box, type the OSPF cost of reaching the VNS subnet.
The OSPF cost value provides a relative cost indication to allow upstream routers to calculate whether or not to use the controller as a better fit or lowest cost path to reach devices in a particular network. The higher the cost, the less likely of the possibility that the controller will be chosen as a route for traffic, unless that controller is the only possible route for that traffic.
- 6 To disable **OSPF advertisement** on this VNS, select the **Disable OSPF Advertisement** check box.
- 7 Click **Close**.
- 8 Click **Save**.

Exception Filtering

The exception filter provides a set of rules aimed at restricting the type of traffic that is delivered to the controller. By default, your system is shipped with a set of restrictive filter rules that help control access through the interfaces to only those services that are absolutely necessary.

By configuring to allow management on an interface, an additional set of rules is added to the shipped filter rules that provide access to the system's management configuration framework (SSH, HTTPS, *SNMP* Agent). Most of this functionality is handled directly behind the scenes by the system, rolling and unrolling canned filters as the system's topology and defined access privileges for an interface change.



Note

An interface for which Allow Management is enabled can be reached by any other interface. By default, Allow Management is disabled and shipped interface filters will only permit the interface to be visible directly from its own subnet.

The visible exception filter definitions, both in physical ports and topology definitions, allow administrators to define a set of rules to be added to the system's dynamically updated exception filter protection rules. Rule evaluation is performed top to bottom, until an exact match is determined. Therefore, these user-defined rules are evaluated before the system's own generated rules. As such, these user-defined rules may inadvertently create security lapses in the system's protection mechanism or create a scenario that filters out packets that are required by the system.



Note

Use exception filters only if absolutely necessary. It is recommended that you avoid defining general allow all or deny all rule definitions since those definitions can easily be too liberal or too restrictive to all types of traffic.

The exception rules are evaluated in the context of referring to the specific controller's interface. The destination address for the role rule definition is typically defined as the interface's own IP address. The port number for the filter definition corresponds to the target (destination) port number for the applicable service running on the controller's management plane.

The exception filter on an topology applies only to the packets directed to the controller and can be applied to the destination portion of the packet, or to the source portion of the packet when filtering is enabled. Traffic to a specified IP address and IP port is either allowed or denied. Adding exception filter rules allows network administrators to either tighten or relax the built-in filtering that automatically drops packets not specifically allowed by role rule definitions. The exception filter rules can deny access in the event of a DoS attack, or can allow certain types of management traffic that would otherwise be denied. Typically, Allow Management is enabled.

To define exception filters:

- 1 From the top menu, click **VNS**.
- 2 In the left pane, select **Topologies**.
- 3 On the **Topologies** page, click the **Exception Filters** tab.

The **Exceptions Filter** page displays.

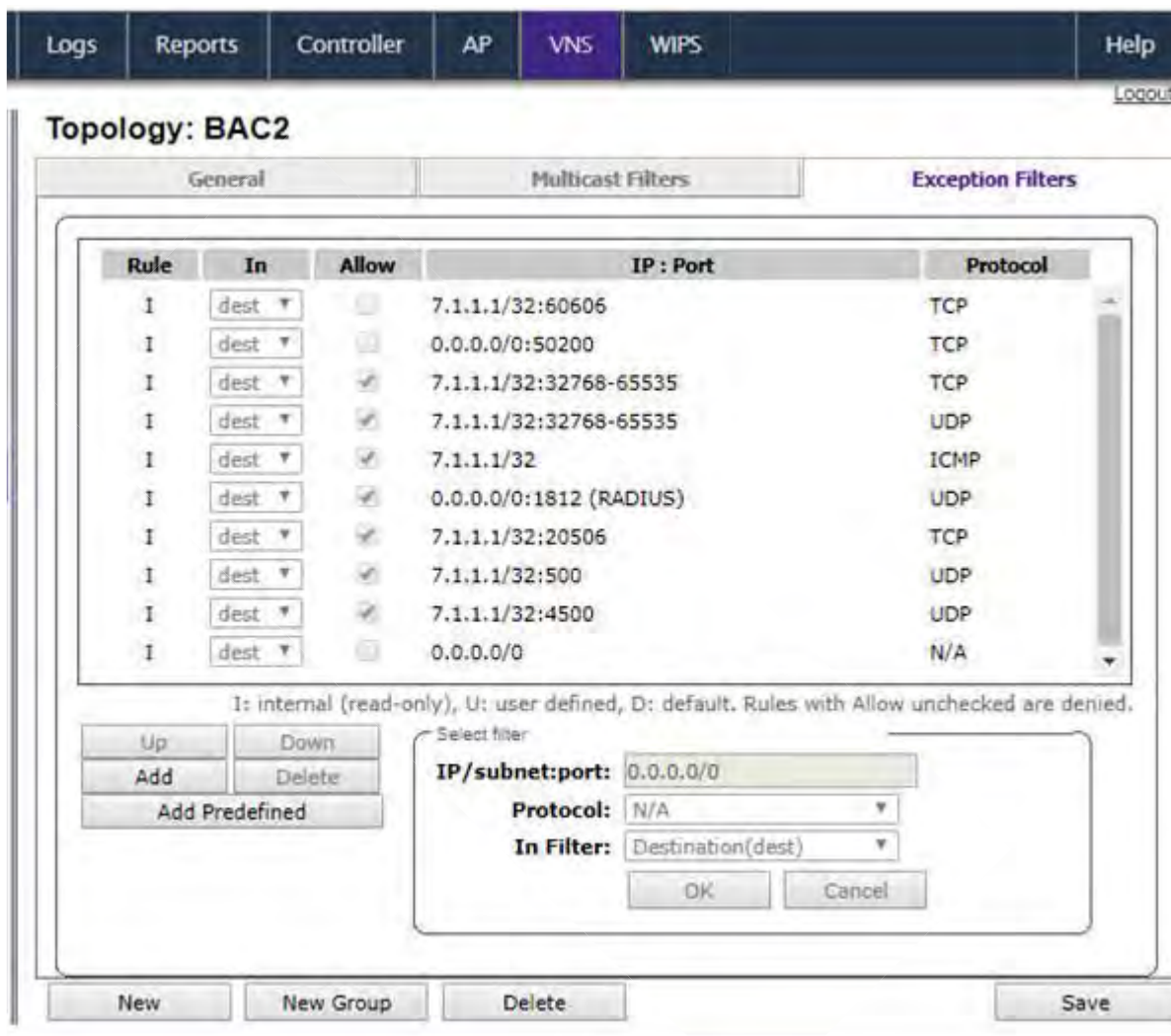


Figure 83: Topology Exception Filters

- 4 Select an existing topology from the right-hand pane to edit an existing topology, or click **New** to create a new topology.

The **Topologies** configuration page displays. The **Exception Filters** tab is available only if Layer 3 (L3) configuration is enabled.

- 5 Click the **Exception Filters** tab to display the **Exception Filters** page.

Table 42: Exception Filters page - Fields and Buttons

Field/Button	Description
Rule	Identifies the type of role rule. Options are: • D - Default rule • I - Internal (read-only) • T - Local interface rule • U - user-defined rule
In	Identifies the rule that applies to traffic from the network host or wireless device that is trying to get to a controller. You can change this setting using the drop-down menu. Options include: • Destination (dest) • Source (src) - available in Advanced Filtering Mode only • None • Both - available in Advanced Filtering Mode only
Allow	Select the Allow check box to allow this rule. Otherwise the rule is denied.
IP:Port	Identifies the IP address and port to which this role rule applies.
Protocol	In the Protocol drop-down list, click the applicable protocol. The default is N/A.
Up, Down	Select a role rule and click to either move the rule up or down in the list. The filter rules are executed in the order in which you define them here
Add	Click to add a role rule. The fields in the Add Filter area are enabled.
Delete	Click to remove this role rule.
Add Predefined	Select a predefined role rule. Click Add to add the rule to the rule table, otherwise click Cancel
Save	Click to save the configuration.
Advanced Mode	Advanced filtering mode provides the ability to create bidirectional filters. If this controller participates in a mobility zone, before enabling advanced mode be sure that all controllers in the mobility zone are running V7.41 or greater. Note: After enabling advanced filtering mode, you can no longer use NMS Wireless Manager V4.0 to manage the controller's roles and you cannot switch back to basic filter mode unless you return the controller to its default state.
Add Filter section	
IP/subnet:port	Type the destination IP address. You can also specify an IP range, a port designation, or a port range on that IP address
Protocol	In the Protocol drop-down list, click the applicable protocol. The default is N/A.

Table 42: Exception Filters page - Fields and Buttons (continued)

Field/Button	Description
In Filter	In the drop-down menu, select an option that refers to traffic from the network host that is trying to get to a wireless device. Options include: • Destination (dest) • Source (src) - available in Advanced Filtering Mode only • None • Both - available in Advanced Filtering Mode only By default, user-defined rules are enabled on ingress (In), and are assumed to be Allow rules. To disable the rule in either direction, or to make it a Deny rule, click the new filter, then de-select the relevant check box.
OK	Click to add the role rule to the filter group. The information displays in the role rule table.
Cancel	Click Cancel to discard your changes.

**Note**

For External Captive Portal, you need to add an external server to a non-authentication filter.

Multicast Filtering

A mechanism that supports multicast traffic can be enabled as part of a topology definition. This mechanism is provided to support the demands of VoIP and IPTV network traffic, while still providing the network access control.

**Note**

To use the mobility feature with this topology, you must select the **Enable Multicast Support** check box for the data port.

Define a list of multicast groups whose traffic is allowed to be forwarded to and from the VNS using this topology. The default behavior is to drop the packets. For each group defined, you can enable Multicast Replication by group.

**Note**

Before enabling multicast filters and depending on the topology, you may need to define which physical interface to use for multicast relay. Define the multicast port on the **IP Addresses** tab. For more information, see [Setting Up the Data Ports](#) on page 51.

To enable Multicast for a topology:

- 1 On the **Topologies** page, click the **Multicast Filters** tab.

Topology: AH-BAC-2005

General

Multicast Filters

☒ **Multicast bridging** (only the multicasts matching the rules defined will be allowed)

IP	Group	Wireless Replication 
ff00::/8	All V6 Multicast	☒
ff02::fb/128	mDNSV6/Bonjour	☒
ff05:2005::16/32		☒

☐ **IP Group:**

☒ **Defined groups:**

Figure 84: Topology Multicast Filters

- To enable the multicast function, select **Multicast bridging**.
- Define the multicast groups by selecting one of the radio buttons:
 - IP Group** — Type the IP address range.
 - Defined groups** — Click from the drop-down list.



Note

IPv6 traffic is supported for B@AC and B@AP topologies.

- To enable the wireless multicast replication for this group, select the corresponding **Wireless Replication** check box. Wireless Replication filters multicast traffic being sent back to the wireless AP channel or wired network.



Note

Wireless replication takes effect only when Multicast Address is allowed.

- Click **Add**. The group is added to the list above.

- 6 To modify the priority of the multicast groups, click the group row, and then click the **Up** or **Down** buttons.

A Deny All rule is automatically added as the last rule, IP = *.*.* and the **Wireless Replication** check box is not selected. This rule ensures that all other traffic is dropped.

- 7 To save your changes, click **Save**.

**Note**

The multicast packet size should not exceed 1450 bytes.

Draft

6 Configuring Roles

Roles Overview

Configuring Default VLAN and Class of Service for a Role Policy Rules

Roles Overview

A role is a set of network access services that can be applied at various points in a policy-enabled network. A port takes on a user's role when the user authenticates. Roles are usually named for a type of user such as Student or Engineering. Often, role names will match the naming conventions that already exist in the organization. The role name should match filter ID values set up on the RADIUS servers.

A role can contain any number of services in Policy Manager.

A VNS can have up to two roles assigned to it. The default non-authenticated role will be used while the station is not authenticated but able to access the network. The default authenticated role will be assigned to a station if it completes authentication successfully but the authentication process did not explicitly assign a role to the station.

A role may also contain default access control (VLAN (Virtual LAN)) and/or Class of Service (priority) characteristics that will be applied to traffic not identified specifically by the set of access services contained in the role. The set of services included in a role, along with any access control or class of service defaults, determine how all network traffic will be handled at any network point configured to use that role.

Roles don't need to be fully specified; unspecified attributes are retained by the user or inherited from Global Role definitions (see [Configuring the Global Default Policy](#) on page 408 for more information).

Default Global Role definitions provide a placeholder for completion of incomplete roles for initial default assignment. If a role is defined as Default for a particular VNS, the role inherits incomplete attributes from Default Global Role definitions.

Configuring Default VLAN and Class of Service for a Role

From the **VLAN & Class of Service** tab you can assign a previously configured topology to a role. You can also launch the Topology Configuration page to edit an existing topology or create a new one. For

information about how to configure a topology, refer to [Configuring a Basic Data Port Topology](#) on page 266.

Note

The Configuration Manager (CM) checks overall configuration as configuration is entered. If CM detects mixed B@AC and B@AP rules in the same role, and the role has L7 filter rules, then the configuration is rejected. For more information, see [Configuration Rules with L7 Filters](#) on page 307.

In general, *CoS (Class of Service)* refers to a set of attributes that define the importance of a frame while it is forwarded through the network relative to other packets, and to the maximum throughput per time unit that a station or port assigned to the role is permitted. The CoS defines actions to be taken when rate limits are exceeded.

To configure VLAN and Class of Service for a role:

- 1 From the top menu, click **VNS**.

- 2 In the left pane expand the **Roles** pane and click the role you want to edit, or click **New** to create a new role.

Logs

Reports

Controller

AP

VNS

WIPS

Role: CNL-412-0-0-default

VLAN & Class of Service

Policy Rules

Core

Role Name:

CNL-412-0-0-default

Default Action

Access Control:

Containment VLAN

VLAN:

CNL-412-0-0(4094)

Edit

New

Default Class of Service:

No change

Edit

New

Traffic Mirror:

None

Advanced...

New

Delete

Save

Figure 85: VLAN & Class of Service Tab

- 3 Select **Policy Rules** to configure the policy rules for the Role. For more information, see [Configuring Policy Rules](#) on page 298.

Table 43: VLAN & Class of Service Tab - Fields and Buttons

Field/Button	Description
Core	
Role Name	Enter a name to assign to this role.
Default Action	

Table 43: VLAN & Class of Service Tab - Fields and Buttons (continued)

Field/Button	Description
Access Control	Select from one of the following: • None - No role defined • No change - Default setting • Allow - Packets contained to role's default action's VLAN/topology. • Deny - Any packet not matching a rule in the Role is dropped. • Containment VLAN - Any packet not matching a rule is sent to defined VLAN.
VLAN	Note: VLAN is only visible when the user selects "Contain to VLAN" as the default access control action. Select an existing Topology, Topology Group, or click New to create a new Topology. To edit an existing Topology, select the VLAN and then click Edit. The Edit Topology page displays. For more information, see Configuring a Basic Topology on page 267.
Default Class of Service	Select an existing class of service from the Default Class of Service drop-down list, or click New to create a new topology. To edit an existing class of service, select the class of service and then click Edit. The Edit Class of Service page displays. For more information, see Configuring Classes of Service on page 487.
Traffic Mirror	When enabled, this option sends a copy of the network packets to a mirroring L2 port for analysis, in an effort to monitor network traffic. The Purview Engine analyses the traffic. The assigned port can only be used for traffic analysis. You can enable traffic mirroring from the WLAN Service, from the Role, or from the Filter Rule. Setting traffic mirroring at the Filter Rule takes precedence over settings for the Role and WLAN Service. The order of precedence for the traffic mirror setting is: Filter Rule, Role, WLAN Service. To set the L2 port, go to VNS > Global > Netflow/MirrorN Configuration. Valid values for Filter Rule and Role are: • None - No traffic mirroring • Enable - Traffic mirroring enabled. Traffic is copied if the filter rule matches or the role is applied. • Prohibited - Traffic mirroring is prohibited for this role. Traffic is not copied when the filter rule matches or the role is applied.
HTTP Redirection	HTTP Redirection appears when the following conditions are present: • Rule-based Redirection is enabled on the VNS > Global > Filtering Mode screen. • A filter exits with Access Control = HTTP Redirect. (See Understanding the Filter Rule Definition Dialog on page 302.)

Table 43: VLAN & Class of Service Tab - Fields and Buttons (continued)

Field/Button	Description
Redirection URL:	Select from one of the previously configured redirection URLs or click New to create a new redirection URL. For more information about setting up a redirection URL, see Managing Redirection URLs on page 421. <i>WLAN (Wireless Local Area Network)</i> Services with Captive Portals are included in this list. The default value for the redirection URL is Own WLAN , which indicates the current WLAN. This is identical to the current redirection behaviour.
Status	
Synchronize	Enable automatic synchronization with its availability peer. For more information about viewing synchronization status, see Using the Sync Summary on page 414. If this VNS is part of an availability pair, Extreme Networks recommends that you enable Synchronize. By default the WLAN Service is enabled. Clear this check box to disable the WLAN Service.
Advanced Button	
Static Egress Untagged VLANs	Lists those VLANs (for multicast, broadcast, unicast) that a station assigned to a role receives from, even if it hasn't sent on it. Choose a VLAN as follows: - Click a VLAN from the list of available VLANs to use - Click >> to move the VLAN to the active list of VLANs used - Click OK to permit static configuration of egress untagged VLANs.

For more information about rate control profiles, see [Working with Bandwidth Control Profiles](#) on page 407.

Policy Rules

You can define policy rules for a role to specify network access settings for a specific user role. Network policies are a set of rules, defined in a specific order, that determine how connections are authorized or denied. If you do not define policy rules for a role, the role's default action is applied to all traffic subject to that role. However, if you require user-specific filter definitions, then the filter ID configuration identifies the specific role that is applied to the user.

ExtremeWireless supports IPv6 prefixes specified in policy filter rules. With a few considerations:

- You cannot configure Captive Portal Redirection using IPv6 classifiers. While you can http to IPv6 websites, you cannot apply Captive Portal redirection to http [s] over IPv6 .
- Application visibility rules are ignored for http[s] flows over IPv6.

Related Links

[Understanding the Filter Rule Definition Dialog](#) on page 302

[L7 Configuration](#) on page 307

Matching Policy Rules Criteria

The following criteria apply when trying to match rules. Many of these criteria accept a range of addresses or codes not just a single address or code.

A policy rule consists of:

- Match criteria
- An optional access control action (allow, deny)
- An optional class of service assignment

Policy rules can match on:

- Source MAC address
- Destination MAC address
- IPv4 or IPv6 Source IP address
- IPv4 or IPv6 Destination IP address
- Source layer 4 port
- Destination layer 4 port
- IPv4 or IPv6 Source socket (IP address + port)
- IPv4 or IPv6 Destination socket (IP address + port)
- IP type
- *ICMP (Internet Control Message Protocol)* packet type and code
- ToS/DSCP marking
- 802.1p priority
- Ethertype

Policy rule access control actions can be:

- Allow — Forward matching frames on the WLAN Service's default topology.
- Deny — Drop matching frames.
- Contain to VLAN — Forward matching frames on the indicated VLAN.
- None — The rule does not have an access control action. The matching engines ignore a rule with an access control action of 'None'.
- HTTP Redirect — Redirect traffic to default URL 'Own WLAN' or to a URL that is defined on the **Redirection URL** screen. For more information, see [Managing Redirection URLs](#) on page 421. You can also specify a Redirection URL when you configure an External Captive Portal. For more information, see [Configuring Firewall Friendly External Captive Portal](#) on page 353.

Rule-Based Redirection

You can now configure policy rules to explicitly redirect traffic to the captive portal definition assigned to the role, regardless of authentication status. Rule-based Redirection applies to HTTP and HTTPS traffic, and explicitly defines when traffic will be redirected. In previous releases, redirection automatically redirected an un-authenticated client to an ECP when a deny action, on HTTP(S) traffic, occurred.

Rule-based redirection requires explicit enablement. For new installations, Rule-based Redirection is enabled by default. For upgrades from releases prior to v10.11, ExtremeWireless preserves the previous

captive portal redirection method of triggering redirect off denied HTTP/HTTPS for non-authenticated roles.

To enable Rule-based Redirection upon an upgrade, go to **VNS > Global > Filtering Mode**.

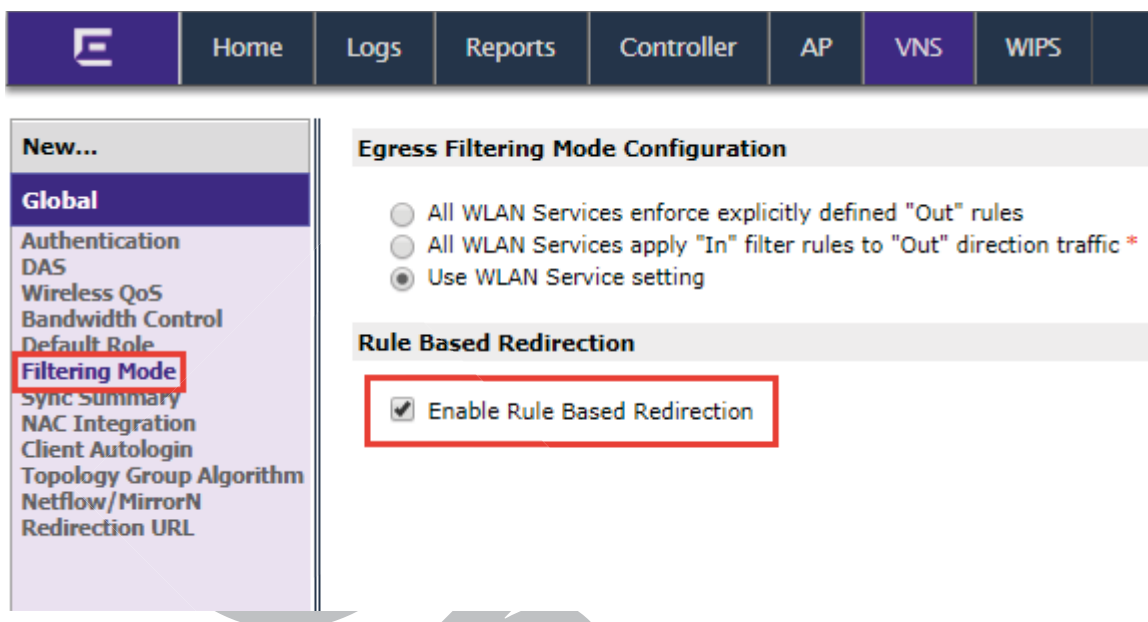


Figure 86: Enabling Rule-based Redirection

To use Rule-based Redirection:

- Verify that the feature is enabled.
- Configure roles with policy rules for redirection. Add the Redirect rules to the (non-auth) role definition; otherwise, the Deny All default action is interpreted explicitly, and traffic will be denied not redirected.
- Configure a list of redirection URLs.
- Specify the redirection URL on the Role **VLAN & Class of Service** tab. This value can be an IP address, URL, or host name if using L7 host name rules.
- (Optional) And if redirecting to an ECP, configure the captive portal for redirected traffic.

Rule-based Redirection is explicit when the redirection flag is enabled and a rule is defined for redirection. The redirection destination can be defined on the role or as part of a WLAN Service configuration. If a redirection destination is not configured, the default destination is 'Own WLAN', which indicates the WLAN of the device. Redirection is allowed on any port.

Figure 87: Example Role with Redirection specified.

Related Links

- [Understanding the Filter Rule Definition Dialog](#) on page 302
- [Host Name DNS Support](#) on page 312
- [Managing Redirection URLs](#) on page 421
- [Configuring Firewall Friendly External Captive Portal](#) on page 353
- [Configuring External and Mode 802.1 Captive Portal](#) on page 351
- [Configuring Default VLAN and Class of Service for a Role](#) on page 284

Configuring Rule-Based Redirection

Deciding how to configure HTTP Redirection depends on the type of traffic you are allowing and the default Access Control value you configure on the role. You must configure the policy rules in the following order:

- Allow policies
- Redirect policies (if using Rule-based Redirection)
- Deny policies.

Allow Policies

You can configure five Allow policies or any combination of Allow and Deny policies on a single role. The following are ways to implement policy rules:

- Allow All Policy.

If you opt to allow all traffic. You only need one policy rule indicating that all traffic is allowed.

Layer 2,3,4 Classification

Layer 2

Ethertype: Internet Protocol, Version 4 (IPv4) ▼ 0x0800

Mac Address: Any Mac ▼ 00:00:00:00:00:00/0

Priority: Any Priority ▼

Layer 3,4

IP/subnet: Any IP Address ▼ 0.0.0.0/0

Port: Any Port ▼ 0

Protocol: Any Protocol ▼ 0

ToS/DSCP: 0x (DSCP:) Select Mask: 0xFF ▼

Application

Application: none ▼

Action

Access Control: Allow ▼

Class of Service: None ▼

Traffic Mirror: None ▼

Figure 88: Allow All Policy Configuration

- Combination of Allow and Deny policies, allowing specific traffic.

Role: bapUnauth

VLAN & Class of Service

Policy Rules

☐ Inherit filter rules from currently applied role ⓘ

Rules ☒ AP Filtering ☐ Custom AP Rules

Action	Name	Protocol	QoS	In	Out
Allow	0.0.0.0/0:68 (DHCP Client)	UDP	None	both	both
Allow	0.0.0.0/0:67 (DHCP Server)	UDP	None	both	both
Allow	192.0.1.203/32	Any	None	both	both
Deny	0.0.0.0/0	Any	None	both	both

Figure 89: Policy Rules Configuration

- Deny All Policy.

When opting to deny all traffic, you must first configure the 5 Allow policies to gather the parameters that direct the client to the FFECP. First configure the specific Allow policies, then configure the Deny All policy.

The image shows a configuration window for a network policy. It is divided into two main sections: 'Layer 2,3,4 Classification' and 'Action'.

Layer 2,3,4 Classification:

- Layer 2:**
 - Ethertype: Internet Protocol, Version 4 (IPv4) (dropdown), 0x0800 (text)
 - Mac Address: Any Mac (dropdown), 00:00:00:00:00:00/0 (text)
 - Priority: Any Priority (dropdown)
- Layer 3,4:**
 - IP/subnet: Any IP Address (dropdown), 0.0.0.0/0 (text)
 - Port: Any Port (dropdown), 0 (text)
 - Protocol: Any Protocol (dropdown), 0 (text)
 - ToS/DSCP: 0x (text), (DSCP:) (text), Select (button), Mask: 0xFF (dropdown)
- Application:**
 - Application: none (dropdown)

Action:

- Access Control: Deny (dropdown)
- Class of Service: None (dropdown)
- Traffic Mirror: None (dropdown)

Figure 90: Deny All Policy Configuration

- Redirect Policy
 - If Rule-based Redirection is enabled, configure at least one policy rule where the Access Control is set to **HTTP Redirect**.
 - If Rule-based Redirection is disabled, configure at least one policy rule where the Access Control is set to **Deny**.

For more information on configuring policy rules, including host name rules, see [Understanding the Filter Rule Definition Dialog](#) on page 302 and [Configuring a Host Name Rule](#) on page 312.

Related Links

[Configuring Rule-Based Redirection](#) on page 291
[Understanding the Filter Rule Definition Dialog](#) on page 302
[Rule-Based Redirection](#) on page 289
[Host Name DNS Support](#) on page 312
[Configuring a Captive Portal on an AP](#) on page 222

Rule Based Redirection to a Captive Portal

Redirecting to a captive portal is a common rule-based redirection use case. The following is an example Allow configuration for rule-based redirection to a captive portal.

- The role allows the station to use [DHCP \(Dynamic Host Configuration Protocol\)](#) and DNS:
 - Access Control = **Allow**, Port = **DNS**
 - Access Control = **Allow**, Port = **DHCP Client**.

- Access Control = **Allow**, Port = **DHCP Server**.
- The role allows the station to communicate with the external captive portal server using HTTP or HTTPS.
 - Access Control = **Allow**, IP/subnet = IP of Captive Portal Server

Then specify the Captive Portal Server on the **VLAN Class of Service** tab in the **Redirection URL** field. The Redirection URL can be provided as a URL, IP address, or host name if using L7 Host Name DNS support.

- The role must allow the station to send traffic to the controller's IP address on the VLAN containing the station's traffic; therefore, one Allow policy must include the IP/subnet that corresponds to the VLAN ID. Depending on the Default Access Control value on the role, this can be the VLAN ID specified on the role or the VLAN ID specified during WLAN Service configuration.
 - When default Access Control = Allow, VLAN ID on the WLAN Service configuration is used.
 - When default Access Control = Contain to VLAN, the VLAN ID on the Role configuration is used.
- Access Control = **Allow**, IP/subnet = Configured VLAN subnet.



Note

You cannot configure Captive Portal Redirection using IPv6 classifiers. While you can http to IPv6 websites, you cannot apply Captive Portal redirection to http [s] over IPv6 .

Policy Rules for a Non-authenticated Role

A VNS' non-authenticated role controls the access of stations until the station completes authentication. The role can be as restrictive or open as necessary. If the station is expected to authenticate, then the role may need to grant it access to resources required to complete the authentication. For example, if the station is expected to perform captive portal authentication then the non-authenticated role must allow the station to:

- Perform DHCP address acquisition
- DNS name lookups
- Forward to the Captive Portal web server

The administrator may grant unauthenticated stations access to other resources, but the recommended default action of a non-authenticated role is to drop all traffic that does not match a rule.

Defining non-authenticated roles allows administrators to identify destinations that a mobile user is allowed to access without incurring an authentication redirection. Typically, the recommended default rule is Deny All. However, administrators should define a rule set that permits users to access essential services:

- DNS (IP of DNS server)
- Default Gateway (VNS Interface IP)

Any HTTP streams requested by the client for denied targets is redirected to the specified location.

The non-authenticated role should allow access to the Captive Portal page IP address, as well as to any URLs for the header and footer of the Captive Portal page. This filter should also allow network access to the IP address of the DNS server and to the network address—the gateway of the Topology. The

gateway is used as the IP for an internal Captive Portal page. An external Captive Portal provides a specific IP definition of a server outside the wireless network.

Redirection and Captive Portal credentials apply to HTTP traffic only. A wireless device user attempting to reach websites other than those specifically allowed in the non-authenticated filter is redirected to the allowed destinations. Most HTTP traffic outside of that defined in the non-authenticated filter is redirected.

Note



Although non-authenticated role definitions are used to assist in the redirection of HTTP traffic for restricted or denied destinations, the non-authenticated filter is not restricted to HTTP operations. The filter definition is general. Any traffic, other than HTTP, that the filter does not explicitly allow is discarded by the controller.

The non-authenticated filter is applied to sessions until they successfully complete authentication. The authentication procedure results in an adjustment to the user's applicable Policy Rule for the access role.

Typically, default filter ID access is less restrictive than a non-authenticated profile. It is the administrator's responsibility to define the correct set of access privileges.

Note



Administrators must ensure that the non-authenticated filter allows access to the corresponding authentication server:

- **Internal Captive Portal** — IP address of the VNS interface
- **External Captive Portal** — IP address of external Captive Portal server

Non-authenticated Role Examples

Table 44 lists the rules that a basic non-authenticated role for internal Captive Portal should have, in the specified order:

Table 44: Non-authenticated Role Example A

In	Out	Allow	IP / Port	Description
x	x	x	IP address of the captive portal	Allow all incoming wireless devices access to the default gateway of the VNS.
x	x	x	IP address of the DNS Server	Allow all incoming wireless devices access to the DNS server of the VNS.
x	x		***.	Default access control action is to deny all.

Note



For external Captive Portal, an additional rule to Allow (in/out) access to the external Captive Portal authentication/web server is required.

If you place URLs in the header and footer of the Captive Portal page, you must explicitly allow access to any URLs mentioned in the authentication server's page, such as:

- **Internal Captive Portal** — URLs referenced in a header or footer
- **External Captive Portal** — URLs mentioned in the page definition

Table 45 is another example of a non-authenticated filter that adds additional policy rules. The additional rules do the following:

- Deny access to a specific IP address.
- Allow only HTTP traffic.

Table 45: Non-authenticated Role Example B

In	Out	Allow	IP / Port	Description
x	x	x	IP address of the default gateway	Allow all incoming wireless devices access to the default gateway of the VNS.
x	x	x	IP address of the DNS Server	Allow all incoming wireless devices access to the DNS server of the VNS.
x	x		[a specific IP address, or address plus range]	Deny all traffic to a specific IP address, or to a specific IP address range (such as:0/24).
x	x	x	*.*.*.*:80	Allow all port 80 (HTTP) traffic.
x	x		*.*.*.*	Default access control action is to deny all.

Once a wireless device user has logged in on the Captive Portal page and has been authenticated by the RADIUS server, then the following rules apply:

- **Role filters** — If a filter ID associated with this user is returned by the authentication server, then the Role with the same name as the filter ID will be applied.
- **Default filter** — If no matching filter ID is returned from the authentication server.

Authenticated Rules Examples

Here are examples of possible policy rules for authenticated users. Table 46 disallows some specific access before allowing everything else.

Table 46: Policy Rules Example A

In	Out	Allow	IP / Port	Description
x	x		*.*.*.*:22-23	SSH sessions
x	x		192.168.18.0/24	Deny all traffic to a specific IP address or address range
x	x	x	*.*.*.*	Default action is to allow everything else

Table 47 allows some specific access and denies everything else.

Table 47: Policy Rules Example B

In	Out	Allow	IP / Port	Description
x	x	x	192.168.18.0/24	Allow traffic to a specific IP address or address range.
x	x		****.	Default action is to deny all.

Policy Rules for a Default Role

After authentication of the wireless device user, the default filter applies only after the following conditions are met:

- No filter ID attribute value is returned by the authentication server for this user.
- No Role match is found on the controller for the filter ID value.

The final rule in the default filter should be a catch-all rule for any traffic that did not match a filter. A final 'Allow All' rule in a default filter ensures that a packet is not dropped entirely if no match is found. VNS Role is also applicable for Captive Portal and MAC-based authorization.

Default Role Examples

The following are examples of policy rules for a default filter:

Table 48: Default Role Examples

In	Out	Allow	IP / Port	Description
x	x		192.168.18.0/24	Deny all access to an IP range
x	x		Port 80 (HTTP)	Deny all access to Web browsing
x	x		192.168.18.10	Deny all access to a specific IP
x	x	x	****.	Default access control action is to allow or contain to <u>VLAN</u> .
	x		Port 80 (HTTP) on host IP	Deny all incoming wireless devices access to Web browsing the host
x			10.3.0.20, ports 10-30	Deny all traffic from the network to the wireless devices on the port range, such as FTP (port 21)
	x	x	10.3.0.20	Allow all other traffic from the wireless devices to the Intranet network
x		x	10.3.0.20	Allow all other traffic from Intranet network to wireless devices
x	x		****.	Default action is to deny/drop

Policy Rules Between Two Wireless Devices

Traffic from two wireless devices that are on the same VNS and that are connected to the same AP will pass through the controller and therefore be subject to a filtering role. You can set up policy rules that

allow each wireless device access to the default gateway, but also prevent each device from communicating with each other.

Add the following two rules to a filter, before allowing everything else:

Table 49: Rules Between Two Wireless Devices

In	Out	Allow	IP / Port	Description
x	x	x	10.3.2.25	Allow access to the Gateway IP address of the VNS only
x	x		10.3.5.28.0/24	Deny all access to the VNS subnet range (such as 0/24)
x	x	x	****	Default access control action is contain to <u>VLAN</u> .



Note

You can also prevent the two wireless devices from communicating with each other by setting Block Mu to MU traffic. See [Configuring a Basic WLAN Service](#) on page 319.

Defining Policy Rules for Wireless APs

You can also apply policy rules on the wireless AP. Applying policy rules at the AP helps restrict unwanted traffic at the edge of your network. All APs support 64 rules. Filtering at the AP can be configured with the following Topology types:

- **Bridge Traffic Locally at the AP** — If filtering at the AP is enabled on a Bridge Traffic Locally at the AP topology, the filtering is applied to traffic in both the inbound and outbound direction, the inbound direction is from the wireless device to the network, and the outbound direction is from the network to the wireless device.
- **Routed and Bridge Traffic Locally at the EWC** — If filtering at the AP is enabled on a Routed or Bridge Traffic Locally at the EWC topology, the filtering is applied only to traffic in the inbound direction. The filters applied in the outbound direction at the AP can be the same as or different from filters applied at the controller.

A role can use more than one topology and more than one type of topology. If a role uses at least one Bridged at AP topology, the AP filters all inbound traffic assigned to the rule. The controller performs all outbound filtering.

Configuring Policy Rules

From the **Policy Rules** tab, create and work with the policy rules for a role. If you do not define policy rules for a role, then the role's default action is applied to all traffic subject to the role.

To configure policy rules:

- 1 Navigate to the **Policy Rules** tab. (Click **VNS > Roles > Policy Rules**.)
By default, the **Rules** tab appears, displaying a list of Policy Rules for the Role.

2 You can take the following actions:

- **Add**
- **Edit**
- **Delete**
- **Up**
- **Down**
- **Top**
- **Bottom**

For information about adding or editing a rule, see [Understanding the Filter Rule Definition Dialog](#) on page 302.

Related Links

[Configuring a Captive Portal on an AP](#) on page 222

[Rule-Based Redirection](#) on page 289

Understanding the Policy Rules Tab

The **Policy Rules** tab displays the authentication policy rules for a user role. If you do not define policy rules for a role, then the role's default action is applied to all traffic subject to the role.

VLAN & Class of Service
Policy Rules

☐ **Inherit filter rules from currently applied role** i

Rules

☒ **AP Filtering**
☐ Custom AP Rules

Action	Name	Protocol	QoS	In	Out
Deny	0.0.0.0/0	Any	None	dest	none
Deny	0.0.0.0/0	Any	None	none	src

Add
Edit
Delete
Up
Down
Top
Bottom

Multicast/Broadcast policy rules cannot be applied in the Out direction. Please use Topology Multicast Filters instead.

Figure 91: Policy Rules Tab

Table 50: Policy Rules Tab - Fields and Buttons

Field/Button	Description
Inherit policy rules from currently applied role	Select if you do not want to apply new filter settings. If you do not apply new filter settings, the wireless client uses filter settings from a previously applied role. If rules were never defined, then the system enforces the rules from the Global Default Policy. If you choose to apply new filter settings by not selecting this option, the new filter settings will overwrite any pre-existing filter settings.
"Allow" action in policy rules contains to the <u>VLAN</u> assigned by the role	Note: This option only appears on roles that have been upgraded to 8.31 or later from a previous release and on new roles that have custom AP filtering enabled. The flag is provided for backward compatibility. The administrator can achieve the same effect by modifying each rule with an "Allow" action to "Contain to VLAN" where the containment VLAN is the one referenced by the role's default access control action. When enabled, the "Allow" action forwards the packet on the VLAN of the assigned topology of the containing policy. If the policy does not have a default topology, a series of decision rules are applied to decide which topology the packet was forwarded on. When disabled, the "Allow" action in policy rules is interpreted as "contain to PVID".
AP Filtering	Select to apply the configured rules to the AP.
Custom AP Rules	Select to create a new filter definition to apply to the AP.
Rules/Custom AP rules Tab	
Action	Identifies the access control.
Name	Displays the IP address and port to which this policy rule applies.
Protocol	Displays the applicable protocol.
QoS	Indicates if the rule has QoS enabled. Policy-enabled QoS is a network service that provides the ability to prioritize different types of traffic and to manage bandwidth over a network.
In	Identifies the rule that applies to traffic from the wireless device that is trying to get on the network. You can change this setting using the drop-down menu. Options include: • Source (src) • None • Both - available in Advanced Filtering Mode only
Out	Identifies which IPv4 address field is matched by the rule when applied in the outbound direction (toward the wireless device.) You can change this setting using the drop-down menu. Options include: • Destination (dest) • Source (src) - available in Advanced Filtering Mode only • None • Both - available in Advanced Filtering Mode only The role for outbound traffic may be impacted by the selection (mode) for Egress Filtering. For more information, see Configuring Egress Filtering Mode on page 410.

Table 50: Policy Rules Tab - Fields and Buttons (continued)

Field/Button	Description
Add	Click to add a new rule. The Filter Rule Definition dialog displays. See Understanding the Filter Rule Definition Dialog on page 302.
Edit	Click to edit the selected definition. See Understanding the Filter Rule Definition Dialog on page 302.
Delete	Click to delete the rule.
Up, Down, Top, Bottom	Select a rule and click to either move the rule up or down in the list, or move the rule to the top of the list. The policy rules are executed in the order in which you define them.
Save	Click to save the configuration.

Custom AP Rules

In general, an AP that performs filtering should apply the same set of policy rules for a role as the controller. However, this is not mandatory. An AP can enforce a different set of rules than the controller. In general, avoid using Custom AP filters. Custom AP filters are provided primarily for backward compatibility. For example, they are useful when using policies that have more than 32 rules.

There are restrictions on a role that uses custom AP filtering, including the following:

- Custom Rules option is not visible when L7 filter rules are present.
- The role cannot use Layer 2 filter rules.
- The role cannot use 'Contain to VLAN' actions in rules.
- The role's default action must be 'Contain to VLAN' or 'No Change'.
- The role's static untagged egress VLAN list must be empty.

Related Links

[Creating a Custom AP Filter](#) on page 301

[Understanding the Filter Rule Definition Dialog](#) on page 302

Creating a Custom AP Filter

To create a custom AP filter:

- 1 Click **VNS > Roles > Policy Rules** and select the **AP Filtering** check box.



Note

The AP Filtering option is not available when L7 filters are present. For more information, see [Configuration Rules with L7 Filters](#) on page 307.

The Custom AP Rules check box appears.

- 2 Select the **Custom AP Rules** check box.

The **Custom AP Rules** tab appears.

- 3 Click the **Custom AP Rules** tab.

4 You can take the following actions:

- **Add**
- **Edit**
- **Delete**
- **Up**
- **Down**
- **Top**
- **Bottom**

For information about adding or editing a rule, see [Understanding the Filter Rule Definition Dialog](#) on page 302.

Related Links

[Custom AP Rules](#) on page 301

Understanding the Filter Rule Definition Dialog

Define filter rules from the [Figure 92](#). This dialog displays when you click **Add** or **Edit** from the **Rules** tab or from the **Custom AP Rules** tab.

Filter Rule Definition

Classification

☒ L2 / L3 / L4

☐ L7

Direction

In Filter: Destination(dest)

Out Filter: Source(src)

Layer 2,3,4 Classification

Layer 2

Ethertype: Internet Protocol, Version 4 (IPv4)

Mac Address: Any Mac

Priority: Any Priority

Layer 3,4

IP/subnet: User Defined

Port: Any Port

Protocol: Any Protocol

ToS/DSCP: 0x (DSCP:)

Mask: 0xFF

Application

Application: none

Action

Access Control: None

Class of Service: None

Traffic Mirror: None

OK

Cancel

Figure 92: Filter Rule Definition Dialog

Table 51: Filter Rule Definition Dialog - Fields and Buttons

Field/Button	Description
Classification	Select Layers 2-4 to display configuration options for the data link, routing, and transport layers. Select Layer 7 to configure options related to the application layer. For more information, see Layer 7 configuration .
Direction	

ExtremeWireless™ V10.41.06 User Guide

303

Table 51: Filter Rule Definition Dialog - Fields and Buttons (continued)

Field/Button	Description
In Filter	In the drop-down menu, select which IPv4 addresses in the IP header to match for traffic flowing from the station to the network. Options include: • Destination (dest) • Source (src) - available in Advanced Filtering Mode only • None • Both - available in Advanced Filtering Mode only
Out Filter	In the drop-down menu, select which IPv4 addresses in the IP header to match for traffic flowing from the network to the station. Options include: • Destination (dest) • Source (src) - available in Advanced Filtering Mode only • None • Both - available in Advanced Filtering Mode only The role for outbound traffic rules may be impacted by the selection (mode) for Egress Filtering. For more information, see Configuring Egress Filtering Mode on page 410.
Classification - Layer 2, 3, 4	
Ethertype	Select a matching Ethertype filter for the selected policy rule. Note: You cannot configure Captive Portal Redirection using IPv6 classifiers. While you can http to IPv6 websites, you cannot apply Captive Portal redirection to http [s] over IPv6 .
Mac Address	Select Any MAC or User Defined and provide the Mac Address.
Priority	Select a Priority from the drop-down list.
IP/subnet	Select one of the following: • User Defined, then type the destination IP address and mask. Use this option to explicitly define the IP/subnet aspect of the rule. • IP - select to map the rule to the associated Topology IP address. • Subnet - select to map the rule to the associated Topology segment definition (IP address/mask).
Port	From the Port drop-down list, select one of the following: User Defined, then type the port number. Use this option to explicitly specify the port number. A specific port type. The appropriate port number or numbers are added to the Port text field.
Protocol	In the Protocol drop-down list, click the applicable protocol. The default is N/A.
ToS/DSCP	Select the ToS/DSCP value to match, if any, to define the Layer 3, 4 ToS/DSCP bits. Enter a hexadecimal value in the 0x (DSCP:) field.
Select	Click the Select button to open the ToS/DSCP Configuration dialog. For more information, see Priority and ToS/DSCP Marking on page 491.

Table 51: Filter Rule Definition Dialog - Fields and Buttons (continued)

Field/Button	Description
Mask	This is a mask for the ToS/DSCP field match. The mask allows the match to be based on specific bits in the ToS/DSCP match value. Enter a hexadecimal value.
Application	
Application	Select from one of the following pre-defined IDs to support L5+ filtering: • None • Link Local Multicast Name Resolution Query • Link Local Multicast Name Resolution Response • Simple Service Discovery Protocol Query • Simple Service Discovery Protocol Unsolicited Announcement • mDNS-SD Query • mDNS-SD Response
Action	
Access Control	Select from one of the following: • None - No role defined. • Allow - Packets contained to role's default action's VLAN topology. • Deny - Any packet not matching a rule in the policy is dropped. • Containment VLAN - A topology to use when a VNS is created using a role that does not specify a topology. • HTTP Redirect - Indicates redirect action. Rule-based Redirection is explicit when the redirection flag is enabled and a rule is defined for redirection. The redirection destination can be defined on the role or as part of a WLAN Service configuration. If a redirection destination is not configured, the default destination is 'Own WLAN', which indicates the WLAN of the device. Redirection is allowed on any port. For more information about Rule-based Redirection, see Rule-Based Redirection on page 289. Note: Access control option "Contain to VLAN" and "Redirect" are not supported for L7 rules.
Class of Service	Select an existing class of service from the drop-down list. For information about how to configure a Class of Service, go to Configuring Roles on page 284.

Table 51: Filter Rule Definition Dialog - Fields and Buttons (continued)

Field/Button	Description
Traffic Mirror	When enabled, this option sends a copy of the network packets to a mirroring L2 port for analysis, in an effort to monitor network traffic. The Purview Engine analyses the traffic. The assigned port can only be used for traffic analysis. You can enable traffic mirroring from the WLAN Service, from the Role, or from the Filter Rule. Setting traffic mirroring at the Filter Rule takes precedence over settings for the Role and WLAN Service. The order of precedence for the traffic mirror setting is: Filter Rule, Role, WLAN Service. To set the L2 port, go to VNS > Global > Netflow/MirrorN Configuration. Valid values for Filter Rule and Role are: • None - No traffic mirroring • Enable - Traffic mirroring enabled. Traffic is copied if the filter rule matches or the role is applied. • Prohibited - Traffic mirroring is prohibited for this role. Traffic is not copied when the filter rule matches or the role is applied.
OK	Click to add the rule to the filter group. The information is displayed in the role rule table.
Cancel	Click Cancel to discard your changes.

Related Links

[L7 Configuration](#) on page 307

[Rule-Based Redirection](#) on page 289

[Configuring Policy Rules](#) on page 298

[Configuring a Captive Portal on an AP](#) on page 222

DPI L7 Configuration Restrictions

The Deep Packet Inspection (DPI) engine runs independently on the controller and on selected AP models (AP38xx and AP39xx). The DPI engine that is used depends on the underlying topology of the role. The controller DPI handles traffic for centralized topologies (Bridged@Controller and Routed) for traffic in both directions. The AP's DPI handles distributed topologies (Bridged@AP).

Enabling “App Visibility” in the WLAN causes end-user traffic of the particular WLAN to be sent to and processed by the respective DPI engine. For DPI and L7 filters to work, each instance of the DPI engine running on the AP or on the controller must inspect traffic that is moving in both directions of the connection.

The mixed topologies (B@AP & tunneled in same role) are not supported, and are disabled in the user interface, when L7 application rules are defined in a role. As a result, the “Contain to VLAN” Action option is unavailable for configuration of an L7 Application Rule.

For more information, see [Configuration Rules with L7 Filters](#) on page 307.

Related Links

[Configuration Rules with L7 Filters](#) on page 307

[L7 Configuration](#) on page 307

Configuration Rules with L7 Filters

The controller imposes the following L7 filter configuration rules:

- Rule #1 – If L7 filter rules are configured, “AP filter” and “custom AP filter” in Roles is disabled and the corresponding check box options are hidden.

This allows the Configuration Manager to configure the system for upstream filtering at the controller, if possible, with no mixed B@AC and B@AP configuration within a role - enforced by [Rule # 3](#).

- Rule # 2 – Access control options “Contain to VLAN” and “Redirect” are not supported for L7 rules.

For DPI to identify a flow, TCP packets (three-way handshake exchanges and initial payload packets) must be allowed to pass through the system. If after the traffic flow is classified and the system diverts the rest of the traffic flow to a different VLAN (and most likely to a different server), then the new server treats the packets as stray traffic. This is because the new server did not exchange a three-way handshake with the client for the connection.

- Rule # 3 – Configuration Manager (CM) checks overall configuration as configuration is entered.

If CM detects mixed B@AC and B@AP rules in the same role, and the role has L7 filter rules, then the configuration is rejected.

- Rule # 4 – For L2/L3/L4 rule configuration, if COS is configured, the GUI prompts users to set “AP filter”. But, if L7 rules are present, then the GUI will always disable the AP filter option. (See [Rule # 1](#).)

L7 Configuration

Define Layer 7 filter rules. This dialog displays when you select **L7** on the **Filter Rule Definition** dialog.

Use this dialog to configure filters that allow or deny specific applications or application groups from running on the network, and specify class of service and traffic mirroring.

Filter Rule Definition

Classification

☐ L2 / L3 / L4

☒ L7

Direction

In Filter:

Apply

Out Filter:

Apply

Application

Search for Application

Group:

--

Name:

All

[Custom Web Applications](#)

Action

Access Control:

Deny

Class of Service:

None

Traffic Mirror:

None

OK

Cancel

Figure 93: L7 Properties - Filter Rule Definition Dialog

Table 52: Filter Rule Definition Dialog - Fields and Buttons

Field/Button	Description
Classification	Select Layer 7 to configure options related to the application layer. For more information about layers 2-4, see Understanding the Filter Rule Definition Dialog on page 302.
Direction	
In Filter	Select which IPv4 addresses in the IP header to match for traffic flowing from the station to the network. Options include: • Destination (dest) • Source (src) - available in Advanced Filtering Mode only • None • Both - available in Advanced Filtering Mode only

ExtremeWireless™ V10.41.06 User Guide

308

Table 52: Filter Rule Definition Dialog - Fields and Buttons (continued)

Field/Button	Description
Out Filter	Select which IPv4 addresses in the IP header to match for traffic flowing from the network to the station. Options include: • Destination (dest) • Source (src) - available in Advanced Filtering Mode only • None • Both - available in Advanced Filtering Mode only The role for outbound traffic rules may be impacted by the selection (mode) for Egress Filtering. For more information, see Configuring Egress Filtering Mode on page 410.
Application	
Application Search	Type the application to search for. The Group and Name fields are automatically populated when you select an application from the Search field.
Group	Internet applications are organized in groups based on the type or purpose of the application. Once you select an Application Group, the Name drop-down is populated with application names that are part of the specified group. See Application Groups on page 311.
Name	Names of applications that are a member of the specified group.
Custom Web Applications	You can include custom applications in the Filter Rule Definition dialog. For more information, see Including Custom Apps on page 313.
Note: A role can be configured with application visibility rules and rules referencing IPv6 classifiers, but the application visibility rules are ignored for http[s] flows over IPv6. They will continue to apply to flows over IPv4.	
Action	

Table 52: Filter Rule Definition Dialog - Fields and Buttons (continued)

Field/Button	Description
Access Control	Select from one of the following: • None - No role defined. • No change - Default setting. • Allow - Packets contained to role's default action's <u>VLAN</u>/topology. • Deny - Any packet not matching a rule in the policy is dropped. • Containment VLAN - A topology to use when a VNS is created using a role that does not specify a topology. Note: Do not specify a VLAN with a Routed topology if the IPv6 classifier is used. IPv6 classifiers are not supported on a Routed topology. • HTTP Redirect - Indicates redirect action. Rule-based Redirection is explicit when the redirection flag is enabled and a rule is defined for redirection. The redirection destination can be defined on the role or as part of a WLAN Service configuration. If a redirection destination is not configured, the default destination is 'Own WLAN', which indicates the WLAN of the device. Redirection is allowed on any port. For more information about Rule-based Redirection, see Rule-Based Redirection on page 289.
Class of Service	Select an existing class of service from the drop-down list. For information about how to configure a Class of Service, go to Configuring Roles on page 284.
Traffic Mirror	Select from one of the following: • None - No rule defined • Enable - Default setting • Prohibited - Traffic Mirroring prohibited for this Filter Rule.
OK	Click to add the rule to the filter group. The information is displayed in the role rule table.
Cancel	Click Cancel to discard your changes.

Related Links

[DPI L7 Configuration Restrictions](#) on page 306

[Configuration Rules with L7 Filters](#) on page 307

[Application Groups](#) on page 311

[Allowing for Restricted Sets of Applications and Resources](#) on page 311

[Host Name DNS Support](#) on page 312

[Including Custom Apps](#) on page 313

Application Groups

Advertising
Business Applications
Certificate Validation
Cloud Computing
Cloud Storage
Corporate Website
Databases
E-commerce
Education
Finance
Games
Health Care
Location Services
Mail
News and Information
Peer to Peer
Protocols
Real Time and Cloud Communications
Restricted Content
Search Engines
Social Networking
Software Updates
Sports
Storage
Streaming
Travel
VPN and Security
Web Applications
Web Collaboration
Web Content Services
Web File Sharing
All

ExtremeWireless Special Purpose Groups

Unknown Apps
Wild Card

Allowing for Restricted Sets of Applications and Resources

With the use of two new groups: the Unknown Apps group and the Wild Card group, you can configure policy filters that improve application control. Defined signature rules allow fine-tuning of how to handle traffic for specific applications or traffic categories.

The Unknown Apps group allows you to take action on applications that the Deep Packet Inspection (DPI) sensor does not recognize. When the DPI sensor fails to classify a flow, the flow is automatically

considered unknown and it is classified as part of the Unknown Apps group. You can assign standard actions (allow, deny, rate limit, etc) to flows belonging to the Unknown Apps group.

The Wild Card group makes it simple to allow access to restricted sets of applications and resources. When configuring filters for restrictive sets:

- 1 Configure the Allowed application filters first.
- 2 Configure a Deny filter specifying the Group = **Wild Card** and Name = **All**.
- 3 Configure a Deny filter specifying Group = **Unknown Apps** and Name = **All**.

Host Name DNS Support

When redirecting to an external captive portal (ECP), you can permit end users to log in with their credentials from a third-party site. ExtremeWireless builds a dynamic list of server addresses for sites by monitoring the DNS replies between DNS servers and the mobile user.

Configure an Allow filter rule that applies to all learned server addresses for a specific site.

Related Links

[DNS Resolution](#) on page 312

[Configuring a Host Name Rule](#) on page 312

DNS Resolution

The controller and AP handle DNS resolution (mapping of the host name to an IP address) at runtime for third-party login support. DNS resolution is handled by the AP for B@AP topologies and handled by the controller for B@AC and Routed topologies.

First, configure a host name pattern in the Custom Application dialog as part of the Layer 7 filter configuration. The ExtremeWireless data plane inspects DNS replies for host name patterns that match the user-configured patterns. When a match is found, the host name IP pair is stored in the database. The data plane only considers the user-configured patterns when inspecting the DNS reply.

For example, the pattern facebook.com matches any string that ends with "facebook.com". Valid matches include **any.facebook.com** and **1.any.2.facebook.com**. Patterns that do *not* match include: **facebook.org.com**.

A single host name supports multiple IP addresses. The data plane reserves space for up to 128 IP addresses per host name.

Configuring a Host Name Rule

DNS-based rules are defined as custom L7 signatures. ExtremeWireless matches the defined pattern to the corresponding IP address. Take the following steps to configure a rule that allows mobile clients to authenticate using credentials from a specific host.

- 1 Go to **VNS > Roles > Policy Rules** and click **Add**.
- 2 Create a new filter definition. For more information, see [Understanding the Filter Rule Definition Dialog](#) on page 302.
- 3 On the **Filter Rule Definition** dialog, select the **L7** radio button.
- 4 Select the link **Custom Web Applications**.

- Click the plus button and configure the parameters on the **Custom Web Application** dialog.

Specify Type = **Host name**. The Host Name type differentiates the definition from other extended signatures.

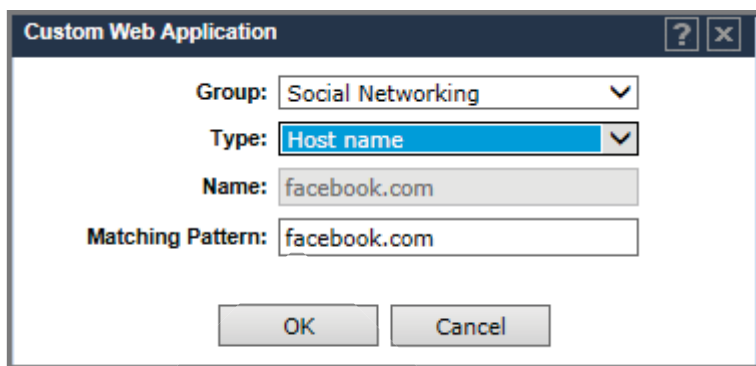


Figure 94: Host Name Rule Configuration

Custom Apps List

Use the custom web application definition editor to define the characteristics of traffic fingerprints used for Deep Packet Inspection and Layer 7 policy enforcement. To add or remove custom Apps from the **Filter Rule Definition** dialog:

- Select **Custom Web Applications**.
- To add an App, click the plus sign. See [Including Custom Apps](#) on page 313.
- To remove an App, select the App and click the minus sign.
- Click **OK**.

Related Links

[Understanding the Filter Rule Definition Dialog](#) on page 302

[L7 Configuration](#) on page 307

[Including Custom Apps](#) on page 313

Including Custom Apps

To add custom apps to the **L7 Filter Rule Definition** dialog:

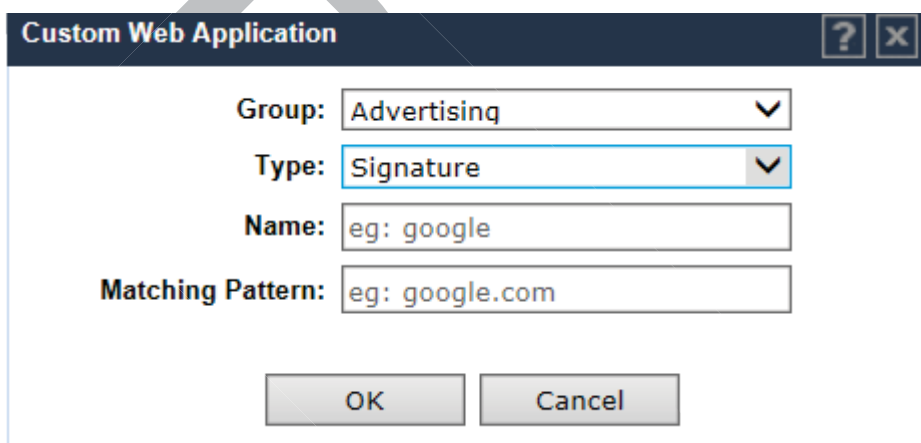
- From the **Filter Rule Definition** dialog, select **L7**.
- Click **Custom Web Application**.

3 Click the plus sign and enter the following:

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

The group names are pre-defined standard Extreme Application Analytics™ signature groups. The group names are case-sensitive.

- Type. Type of authentication. Valid values are:
 - Signature. Standard IP address sent in Signature.
 - Layer 3 host name. Authentication based on User Defined IP/subnet parameter in Layer 3 configuration. You can define up to 64 host name patterns per controller or site.
- The Matching Pattern is the URL pattern that is associated with the application (case-sensitive, up to 64 characters).



Custom Web Application

Group: Advertising

Type: Signature

Name: eg: google

Matching Pattern: eg: google.com

OK Cancel

Figure 95: Adding Custom Web Applications

- 4 Click **OK**.

The Custom Web Application list displays.

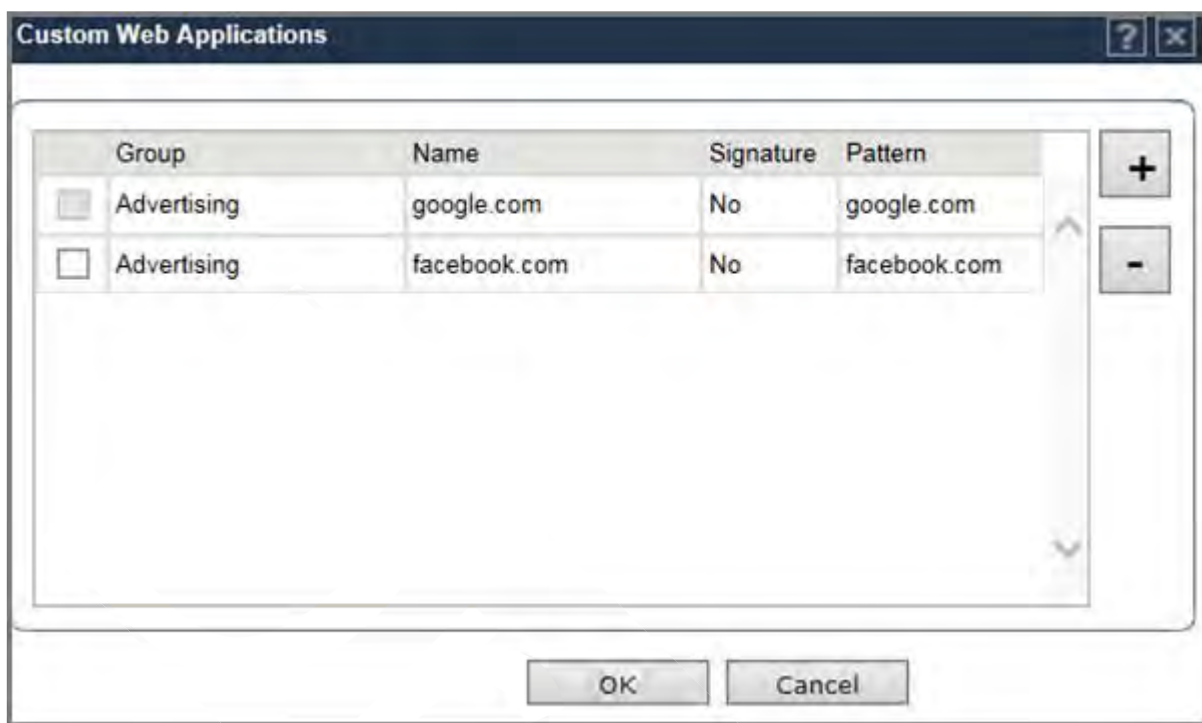


Figure 96: Custom Web Applications List

- 5 Select the check box and click **OK** to add the custom app to the Name drop-down field on the **L7 Configuration** dialog.

Application

Search for Application

Group: Advertising

Name:

- Videology
- VigLink
- Vindico Group
- Visual Revenue
- VitruvianLeads
- VoiceFive
- Vungle
- Wakoopa
- Webtrends
- Whos Amung Us
- Woopra
- Xiti
- Xplusone
- xtify
- Yahoo Ads
- Yahoo Genome
- Ybrant Digital
- youknowbest
- zedo
- ZeusClicks
- Zope
- BidSwitch
- Yashi
- Travel Spike
- OnClick
- Metrigo
- LKQD
- Turn Inc
- google.com (hostname)
- facebook.com (hostname)

Action

Access Control: None

Class of Service: None

Traffic Mirror: None

Successfully

10 Medium | 00 days, 00:31 | User: admin

Figure 97: L7 Configuration: Custom Apps with hostname rule

Related Links

[Application Groups](#) on page 311

[Host Name DNS Support](#) on page 312

Partially Specified Policy

A partially specified policy is one that has “No change” selected for filters, default topology, or default qos. When two policies are applied to a station and one of them is “partially specified”, the “No change” settings are overwritten by the settings of the other policy. When a station successfully authenticates

and is assigned a partially specified policy, the “No change” elements of the policy are replaced with the corresponding elements of the WLAN Service’s default authenticated policy.

Consider the following example. Suppose a VNS is defined that uses policy P1 for its default non-authenticated policy and policy P2 for its default authenticated policy. Policy P1 assigns the station to topology T1 and policy P2 assigns the station to topology T2. Suppose there is a policy P3, which has “No change” set for its topology.

A client on the VNS will be assigned to P1 with topology T1 when he first associates to the VNS. Now suppose the station is assigned P3 by the RADIUS server when the station authenticates. Even though the station is on T1 and P3 has no change set for the topology, the station will be assigned to T2. When the client is authenticated, internally on the controller, the client is first assigned to P2 then P3 is applied.

A similar scenario exists when the hybrid mode policy feature is set to use tunnel-private-group-id to assign both policy and topology but for some reason the VLAN-id-to-Policy mapping table does not contain a mapping for the returned tunnel private group id. In this case a station that successfully authenticates would be assigned the filters and default QoS of the WLAN Service’s default authenticated policy and the topology with the VLANID contained in the Tunnel-Private-Group-ID of the ACCESS-ACCEPT response.

If this is not the desired behavior, then consider the following:

- Avoid using partially specified policies.
- When the controller is configured to map the VLAN ID in the Tunnel-Private-Group-ID response to a policy using the mapping table, ensure that there is a policy mapping for each VLAN ID that can be returned to the controller by the RADIUS server.

7 Configuring WLAN Services

WLAN Services Overview

Third-party AP WLAN Service Type

Configuring a Basic WLAN Service

Configuring Privacy

Configuring Accounting and Authentication

Configuring QoS Modes

Configuring Hotspots

WLAN Services Overview

A *WLAN (Wireless Local Area Network)* Service represents all the RF, authentication and QoS attributes of a wireless access service. The WLAN Service can be one of the following types:

- **Standard** — A conventional service. Only APs running Extreme Networks ExtremeWireless software can be part of this WLAN Service. This type of service may be used as a Bridged @ Controller, Bridged @ AP, or Routed VNS. This type of service provides access for mobile stations. Therefore, roles can be assigned to this type of WLAN service to create a VNS.
- **Third Party AP** — A wireless service offered by third party APs. This type of service provides access for mobile stations. Therefore, roles can be assigned to this type of WLAN service to create a VNS.
- **Dynamic Mesh and WDS (Static Mesh)**— A group of APs organized into a hierarchy for the purposes of providing a Wireless Distribution Service. This type of service is in essence a wireless trunking service rather than a service that provides access for stations. As such, this service cannot have roles attached to it.
- **Remote** — A service that resides on the edge (foreign) controller. Pairing a remote service with a remoteable service on the designated home controller allows you to provision centralized WLAN Services in the mobility domain. This is known as centralized mobility.

The remote service should have the same SSID name and privacy as the home remoteable service. Any WLAN Service/VNS can be a remoteable service, though deployment preference is given to tunneled topologies (Bridged@Controller and Routed).

To reduce the amount of information distributed across the mobility domain, you will explicitly select which WLAN Services are available from one controller to any other controller in the mobility domain.

The WLAN Service remoteable property is synchronized with the availability peer, making the WLAN service published by both the home and foreign controllers.

The following types of authentication are supported for remote WLAN services:

- None
- Internal/External Captive Portal
- Guest Portal

- Guest Splash
- AAA/802.1x

Third-party AP WLAN Service Type

For more information, see [Working with Third-party APs](#) on page 561.

A third-party AP WLAN Service allows for the specification of a segregated subnet by which non-Extreme Networks ExtremeWireless APs are used to provide RF services to users while still utilizing the controller for user authentication and user role enforcement.



Note

Third-party AP devices are not fully integrated with the system and therefore must be managed individually to provide the correct user access characteristics.

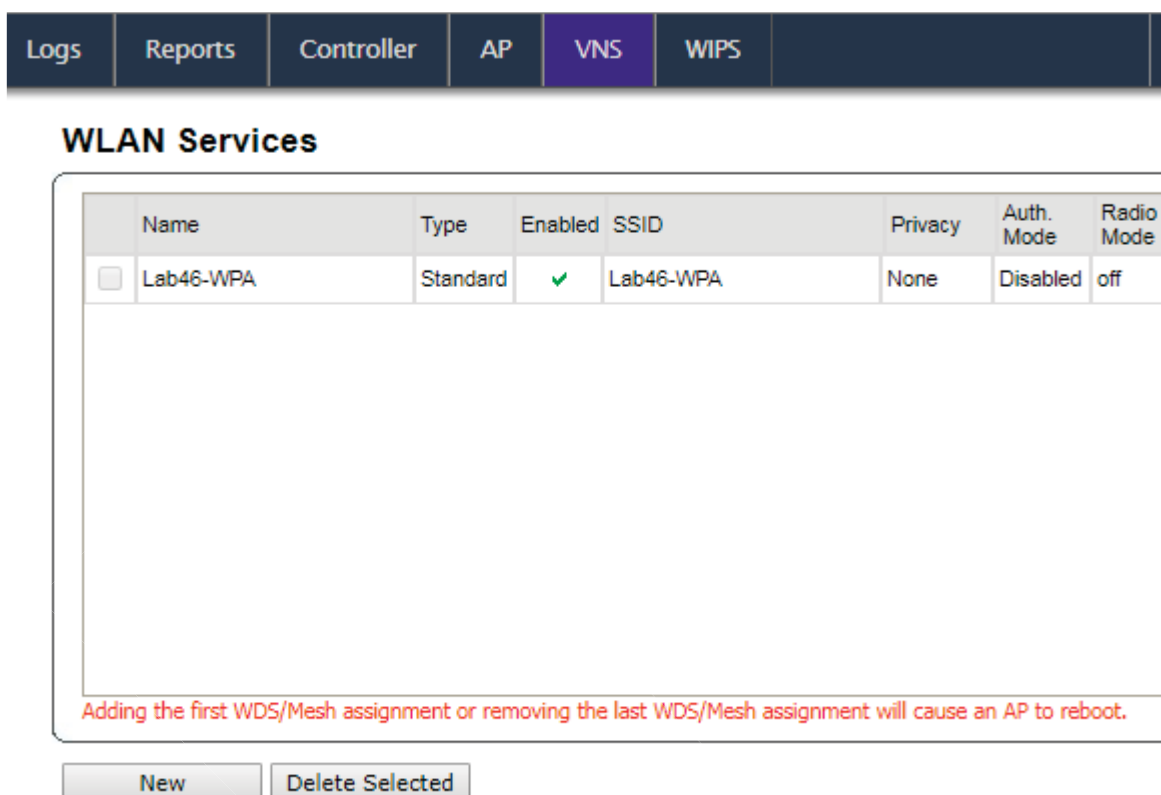
The definition of third-party AP identification parameters allows the system to be able to differentiate the third-party AP device (and corresponding traffic) from user devices on that segment. Devices identified as third-party APs are considered pre-authenticated, and are not required to complete the corresponding authentication verification stages defined for users in that segment (typically Captive Portal enforcement).

In addition, third-party APs have a specific set of filters (third-party) applied to them by default, which allows the administrator to provide different traffic access restrictions to the third-party AP devices for the users that use those resources. The third-party filters could be used to allow access to third-party APs management operations (for example, HTTP, SNMP (Simple Network Management Protocol)).

Configuring a Basic WLAN Service

To configure a WLAN service:

- 1 Go to **VNS > WLAN Services**.



The screenshot shows the 'WLAN Services' configuration page. At the top is a navigation bar with tabs: Logs, Reports, Controller, AP, VNS (selected), WIPS, and an empty tab. Below the navigation bar is the 'WLAN Services' title. Underneath is a table with columns: Name, Type, Enabled, SSID, Privacy, Auth. Mode, and Radio Mode. The table contains one entry: 'Lab46-WPA' with Type 'Standard', Enabled '✓', SSID 'Lab46-WPA', Privacy 'None', Auth. Mode 'Disabled', and Radio Mode 'off'. Below the table is a red warning message: 'Adding the first WDS/Mesh assignment or removing the last WDS/Mesh assignment will cause an AP to reboot.' At the bottom are two buttons: 'New' and 'Delete Selected'.

Name	Type	Enabled	SSID	Privacy	Auth. Mode	Radio Mode
☐ Lab46-WPA	Standard	✓	Lab46-WPA	None	Disabled	off

Adding the first WDS/Mesh assignment or removing the last WDS/Mesh assignment will cause an AP to reboot.

[New](#) [Delete Selected](#)

Figure 98: Configuring a WLAN Service

- 2 Click **New** to create a new service.

Figure 99: New WLAN Service

- Enter a name for the WLAN service.
- Select the service type.
- Change the SSID (optional).
- Enable Hotspot functionality (optional). For more information, see [Configuring Hotspots](#) on page 376.
- The default status of the WLAN service is Synchronized and Enabled.

Synchronize — Enable automatic synchronization with its availability peer. Refer to [Using the Sync Summary](#) on page 414 for information about viewing synchronization status. If this VNS is part of an availability pair, Extreme Networks recommends that you enable **Synchronize**.

By default the WLAN Service is enabled. Clear this check box to disable the WLAN Service.

- Click **Save**.

- 3 For information about fields and buttons on this page, see [Table 53](#).

The screenshot shows the 'WLAN: mba1' configuration page. On the left is a sidebar with navigation links: New..., Global, Sites, Virtual Networks, WLAN Services (selected), anGP1, jint, m1, mba1, r1, t1, test111, tp1, vl7-open1, vl7-psk1, vl7-wpa1, w1, wds1, wds12, wds2, Roles, Classes of Service, and Topologies. The main area is titled 'WLAN Services' and has tabs for Privacy, Auth & Acct, and QoS. The 'Core' tab is active, showing fields for Name (mba1), Service Type (Standard), SSID (mba1), Default Topology (a dropdown menu), Default CoS (No CoS), Default Traffic Mirror (Prohibited), and Application Visibility. There are buttons for 'New Topology...', 'New CoS...', and 'Status' (with an 'Enable' checkbox). Below these is a note: '* Traffic Mirror configure in Wds service applied to tcp/udp only'. On the right, the 'Wireless APs' section shows a 'Select APs:' dropdown and a table with columns: 1, Radio 2, Ports, Airtime %, and a final column. The table lists various AP configurations with radio types like g/n, b/g, and b/g/n, and airtime percentages. At the bottom are 'New', 'Delete', and 'Save' buttons.

Figure 100: WLAN Service Configuration

Table 53: WLAN Services Configuration Page

Field/Button	Description
Core	
Name	Enter a name for this WLAN service
Service Type	Select the type of service to apply to this WLAN service. Options include: - Standard - WDS - Mesh - Third Party AP - Remote If you selected Remote as the Service Type, select the Privacy type. If you set Service Type as either Standard or Remote, select Synchronize, in the Status area, if desired. Enabling this feature allows availability pairs to be synchronized automatically
SSID	The software automatically populates this field with the WLAN service name that you supply. Optionally, you can change this. If you are creating a remote WLAN service, select the SSID of the remoteable service that this remote service will be paired with.

Table 53: WLAN Services Configuration Page (continued)

Field/Button	Description
Default Topology	From the drop-down list, select a preconfigured topology, topology group, or click New Topology to create a new one. Refer to Configuring a Basic Data Port Topology on page 266 for information about how to create a new topology. A WLAN service uses the topology of the role assigned to the VNS, if such a topology is defined. If the role doesn't define a topology, you can assign an existing topology as the default topology to the WLAN service. If you choose not to assign a default topology to the WLAN service, the WLAN service will use the topology of the global default policy (by default, Bridged at AP Untagged). Note: You cannot assign a default topology to a WDS, 3rd party, or remote WLAN service.
Default <u>CoS (Class of Service)</u>	From the drop-down list, select a preconfigured CoS or click New CoS to create a new one. Refer to Configuring Classes of Service on page 487 for information on how to create a new CoS. A WLAN service uses the CoS of the role assigned to the VNS, if such a CoS is defined. If the role doesn't define a CoS, you can assign an existing CoS as the default CoS to the WLAN service. If you choose not to assign a default CoS to the WLAN service, the WLAN service will use the CoS of the global default policy (by default, Bridged at AP Untagged). Note: You cannot assign a default CoS to a WDS, 3rd party, or remote WLAN service.
Default Traffic Mirror	When enabled, this option sends a copy of the network packets to a mirroring L2 port for analysis, in an effort to monitor network traffic. The Purview Engine analyses the traffic. The assigned port can only be used for traffic analysis. You can enable traffic mirroring from the WLAN Service, from the Role, or from the Filter Rule. Setting traffic mirroring at the Filter Rule takes precedence over settings for the Role and WLAN Service. The order of precedence for the traffic mirror setting is: Filter Rule, Role, WLAN Service. To set the L2 port, go to VNS > Global > Netflow/MirrorN Configuration. Valid values for the WLAN Service are: - Prohibited - Traffic is not copied for this WLAN Service. - Enable in both directions - Traffic coming from wireless clients and traffic targeted at specific clients is copied. - Enable in direction only - Traffic generated by wireless clients only is copied. Note: Traffic Mirror configured in WLAN service applies to TCP/UDP only.
App Visibility	Check this option to enable Application Visibility and Application Enforcement on the specific WLAN. Application Visibility allows the controller to capture throughput and byte statistics for 31 pre-selected application groups per client. The data is refreshed every 2 minutes. Enabling this option increases CPU load. Clear this option when Application Visibility and Application Enforcement is not required.
Status	

Table 53: WLAN Services Configuration Page (continued)

Field/Button	Description
Synchronize	Synchronize — Enable automatic synchronization with its availability peer. Refer to Using the Sync Summary on page 414 for information about viewing synchronization status. If this VNS is part of an availability pair, Extreme Networks recommends that you enable this feature.
Enable	The WLAN service is enabled by default, unless the number of supported enabled WLAN services has been reached. To disable the WLAN service, clear the check box.
Wireless APs	
Select APs	Select APs and their radios by grouping. Options include: • all radios — Click to assign all of the APs' radios. • all ports — Click to assign all of the AP ports for an AP3912. • radio 1 — Click to assign only the APs' Radio 1. • radio 2 — Click to assign only the APs' Radio 2. • local APs - all radios — Click to assign only the local APs. • local APs - radio 1 — Click to assign only the local APs' Radio 1. • local APs - radio 2 — Click to assign only the local APs' Radio 2. • foreign APs - all radios — Click to assign only the foreign APs. • foreign APs - radio 1 — Click to assign only the foreign APs' Radio 1. • foreign APs - radio 2 — Click to assign only the foreign APs' Radio 2. • clear all ports — Click to clear all of the AP port assignments. • clear all selections — Click to clear all of the AP radio assignments. • original selections — Click to return to the AP radio selections prior to the most recent save. Note: If two controllers have been paired for availability (for more information, see Availability on page 537), each controller's registered APs are displayed as foreign in the list of available APs on the other controller
Radio 1	Assign the APs' Radios to the service by selecting the individual radios' check boxes. Alternatively, you can use the Select APs list.
Radio 2	Assign the APs' Radios to the service by selecting the individual radios' check boxes. Alternatively, you can use the Select APs list.
Ports	Supported on the AP3912 and AP3917. Select one or more client ports for each WLAN Service. • One WLAN can be assigned per port. The assignment enables the port. • Wireless and wired users associated to the same WLAN service receive identical service. They are affected by the same policies and filters. Alternatively, you can use the Select APs list.
CAM	Camera port for the AP3916ic. For more information, see Assigning WLAN Services to Client Ports on page 170.
IoT	Client port for the IoT Network Thread, supported on all AP391x models. For more information, see IoT Thread Gateway on page 196.

Table 53: WLAN Services Configuration Page (continued)

Field/Button	Description
Airtime %	Percentage of airtime. Airtime % is available for AP38xx and AP39xx access point models that are assigned WLANs configured with Reserved Airtime. For more information, see Configuring Airtime Fairness: Reservation Mode on page 406.
AP Name	Displays the AP name that you assigned on the AP Properties screen.
Advanced	Click to access the WLAN service advanced configuration options. The Advanced configuration page options are described in Advanced WLAN Service Configuration on page 326.
New	Click to create a new WLAN service.
Delete	Click to delete this WLAN service.
Save	Click to save the changes to this WLAN service. If you are creating a new service, the WLAN Services configuration window is displayed, allowing you to assign APs to the service.

**Note**

If two controllers have been paired for availability each controller's registered wireless APs are displayed as foreign in the list of available APs on the other controller. For more information, see [Availability](#) on page 537.

After you have assigned an AP Radio to eight WLAN Services, it will not appear in the list for another WLAN Service setup. Each Radio can support up to eight SSIDs (16 per AP). Each AP can be assigned to any of the VNSs defined within the system.

The controller can support the following active VNSs:

- C5110 — Up to 128 VNSs
- C5210 — Up to 128 VNSs
- C5215 — Up to 128 VNSs
- C4110 — Up to 64 VNSs
- C25 — Up to 16 VNs
- C35 — Up to 16 VNs
- V2110 — Up to 128 VNSs

**Note**

You can assign the Radios of all three AP variants — ExtremeWireless Appliance, Outdoor AP, and Wireless 802.11n AP — to any VNS.

Advanced WLAN Service Configuration

Table 54: Advanced WLAN Service Configuration Page

Field/Button	Description
Timeout	
Idle (pre)	Specify the amount of time in minutes that a Mobile user can have a session on the controller in pre-authenticated state during which no active traffic is passed. The session will be terminated if no active traffic is passed within this time. The default value is 5 minutes.
Idle (post)	Specify the amount of time in minutes that a Mobile user can have a session on the controller in authenticated state during which no active traffic is passed. The session will be terminated if no active traffic is passed within this time. The default value is 30 minutes.
Session	Specify the maximum number of minutes of service to be provided to the user before the termination of the session.
RF - select one or more of the following options:	
Suppress SSID	Select to prevent this SSID from appearing in the beacon message sent by the AP. The wireless device user seeking network access will not see this SSID as an available choice, and will need to specify it.
Enable 11h support	Select to enable 11h support. By default this option is disabled. It is recommended that you enable this option.
Apply power reduction to 11h clients	Select to enable the AP to use reduced power (as does the 11h client). By default this option is disabled. It is recommended that you enable this option. This option is available only if you enable 11h support.
Process client IE requests	Select to enable the AP to accept IE requests sent by clients via Probe Request frames and responds by including the requested IE's in the corresponding Probe Response frames. By default this option is disabled. It is recommended that you enable this option.
Energy Save Mode	Select to reduce the number of beacons the AP transmits on a BSSID when no client is associated with the BSSID. This reduces both the power consumption of the AP and the interference created by the AP when no client is associated.
Radio Management (11k) support	Select to enable background scan. Optionally, enable Beacon Report and/or Quiet IE.
Egress Filtering Mode	
Enforce explicitly defined "Out" rules	Traffic is filtered as configured. For more information, see Configuring Egress Filtering Mode on page 410.
Apply "In" rules to "out" direction traffic	The role of the source and destination addresses are reversed. For more information, see Configuring Egress Filtering Mode on page 410.
Client Behavior	
Block MU to MU traffic	Select the Block Mu to MU traffic check box if you want to prevent two devices associated with this SSID and registered as users of the controller, to be able to talk to each other. The blocking is enforced at the L2 (device) classification level.
802.1D	

Table 54: Advanced WLAN Service Configuration Page (continued)

Field/Button	Description
8021D Base Port: xxx	The 802.1D Base Port number in the 802.1D area is the port number by which Extreme Management Center recognizes the SSID. It is read-only.
Remote Service	
Remoteable	Select the check box if you want to pair this service with a remote service.
Inter-WLAN Service Roaming	
Permit Inter-WLAN Service Roaming	Select to enable a client on a controller to maintain the session, including the IP address and role assignment, while roaming between VNSs having the same SSID and privacy settings. If not selected, when the client roams among VNSs, the existing session terminates and a new session starts with the client having to associated and authenticate again. The list of VNSs that share the same SSID and privacy settings displays below.
Unauthenticated Behavior	
Discard Unauthenticated Traffic	Select the check box to drop all traffic flowing to and from an unauthenticated station.
Default Non-Authenticated Policy	Select the check box to apply the default non-authenticated policy to all traffic flowing to and from an unauthenticated station.
Netflow	Click to Enable/Disable Netflow flag. For more information, see Using Netflow/MirrorN on page 419.
Apply	Click to apply changes.
Cancel	Click to close the Advanced dialog without saving changes.

Configuring Privacy

Privacy is a mechanism that protects data over wireless and wired networks, usually by encryption techniques. The controller provides several privacy mechanism to protect data over the WLAN.

The following are privacy options:

- **None**
- **Static Wired Equivalent Privacy (WEP)** — Keys for a selected VNS, so that it matches the WEP mechanism used on the rest of the network. Each AP can participate in up to 50 VNSs. For each VNS, only one WEP key can be specified. It is treated as the first key in a list of WEP keys.
- **Dynamic Keys** — The dynamic key WEP mechanism changes the key for each user and each session.
- **Wi-Fi Protected Access (WPA)**
 - version 1 with encryption by temporal key integrity protocol (TKIP)
 - version 2 with encryption by advanced encryption standard with counter-mode/CBC-MAC protocol (AES-CCMP)
- **Wi-Fi Protected Access (WPA) Pre-Shared key (PSK)** — Privacy in PSK mode, using a Pre-Shared Key (PSK), or shared secret for authentication. WPA-PSK is a security solution that adds

authentication to enhanced WEP encryption and key management. WPA-PSK mode does not require an authentication server. It is suitable for home or small office.



Note

Regardless of the AP model or WLAN Service type, a maximum of 112 simultaneous clients, per radio, are supported by all of the data protection encryption techniques.

About Wi-Fi Protected Access (WPA V1 and WPA V2)



Note

To achieve the strongest encryption protection for your VNS, it is recommended that you use WPA v.1 or WPA v.2.

WPA v1 and WPA v2 add authentication to WEP encryption and key management. Key features of WPA privacy include:

- Specifies 802.1x with Extensible Authentication Protocol (EAP)
- Requires a RADIUS or other authentication server
- Uses RADIUS protocols for authentication and key distribution
- Centralizes management of user credentials

The encryption portion of WPA v1 is Temporal Key Integrity Protocol (TKIP). TKIP includes:

- A per-packet key mixing function that shares a starting key between devices, and then changes their encryption key for every packet (unicast key) or after the specified re-key time interval (broadcast key) expires
- An enhanced Initialization Vector (IV) of 48 bits, instead of 24 bits, making it more difficult to compromise
- A Message Integrity Check or Code (MIC), an additional 8-byte code that is inserted before the standard WEP 4-byte Integrity Check Value (ICV). These integrity codes are used to calculate and compare, between sender and receiver, the value of all bits in a message, which ensures that the message has not been tampered with.

The encryption portion of WPA v2 is Advanced Encryption Standard (AES). AES includes:

- A 128-bit key length, for the WPA2/802.11i implementation of AES
- Four stages that make up one round. Each round is iterated 10 times.
- A per-packet key mixing function that shares a starting key between devices, and then changes their encryption key for every packet or after the specified re-key time interval expires.
- The Counter-Mode/CBC-MAC Protocol (CCMP), a new mode of operation for a block cipher that enables a single key to be used for both encryption and authentication. The two underlying modes employed in CCM include:
 - Counter mode (CTR) that achieves data encryption
 - Cipher Block Chaining Message Authentication Code (CBC-MAC) to provide data integrity

The following is an overview of the WPA authentication and encryption process:

- 1 The wireless device client associates with Wireless APs.
- 2 Wireless AP blocks the client's network access while the authentication process is carried out (the controller sends the authentication request to the RADIUS authentication server).

- 3 The wireless client provides credentials that are forwarded by the controller to the authentication server.
- 4 If the wireless device client is not authenticated, the wireless client stays blocked from network access.
- 5 If the wireless device client is authenticated, the controller distributes encryption keys to the AP and the wireless client.
- 6 The wireless device client gains network access via the AP, sending and receiving encrypted data. The traffic is controlled with permissions and role applied by the controller.

Wireless 802.11n APs and WPA Authentication



Note

If you configure a WLAN Service to use either WEP or TKIP authentication, any wireless 802.11n AP associated to a VNS using that service will be limited to legacy AP performance rates.

If a VNS is configured to use WPA authentication, any wireless 802.11n AP within that VNS will do the following:

- WPA v.1 — If WPA v.1 is enabled, the wireless AP will advertise only TKIP as an available encryption protocol.
- WPA v.2 — If WPA v.2 is enabled, the wireless AP will do the following:
 - If WPA v.1 is enabled, the wireless AP will advertise TKIP as an available encryption protocol.



Note

If WPA v.2 is enabled, the wireless AP does not support the Auto option.

- If WPA v.1 is disabled, the wireless AP will advertise the encryption cipher AES (Advanced Encryption Standard).



Note

The security encryption for some network cards must not to be set to WEP or TKIP to achieve a data rate beyond 54 Mbps.

WPA Key Management Options

Wi-Fi Protected Access (WPA v1 and WPA v2) privacy offers you the following key management options:

- None — The wireless client device performs a complete 802.1x authentication each time it associates or tries to connect to an AP.
- Opportunistic Keying — Opportunistic Keying or opportunistic key caching (OKC) enables the client devices to roam fast and securely from one wireless AP to another in 802.1x authentication setup.

The client devices that run applications such as video streaming and VoIP require rapid reassociation during roaming. OKC helps such client devices by enabling them to rapidly reassociate with the APs. This avoids delays and gaps in transmission and thus helps in secure fast roaming (SFR).

**Note**

The client devices should support OKC to use the OKC feature in the WLAN.

- Pre-authentication — Pre-authentication enables a client device to authenticate simultaneously with multiple APs in 802.1x authentication setup. When the client device roams from one AP to another, it does not have to perform the complete 802.1x authentication to reassociate with the new AP as it is already pre-authenticated with it. This reduces the reassociation time and thus helps in seamless roaming.

**Note**

The client devices should support pre-authentication to use the pre-authentication feature in the WLAN.

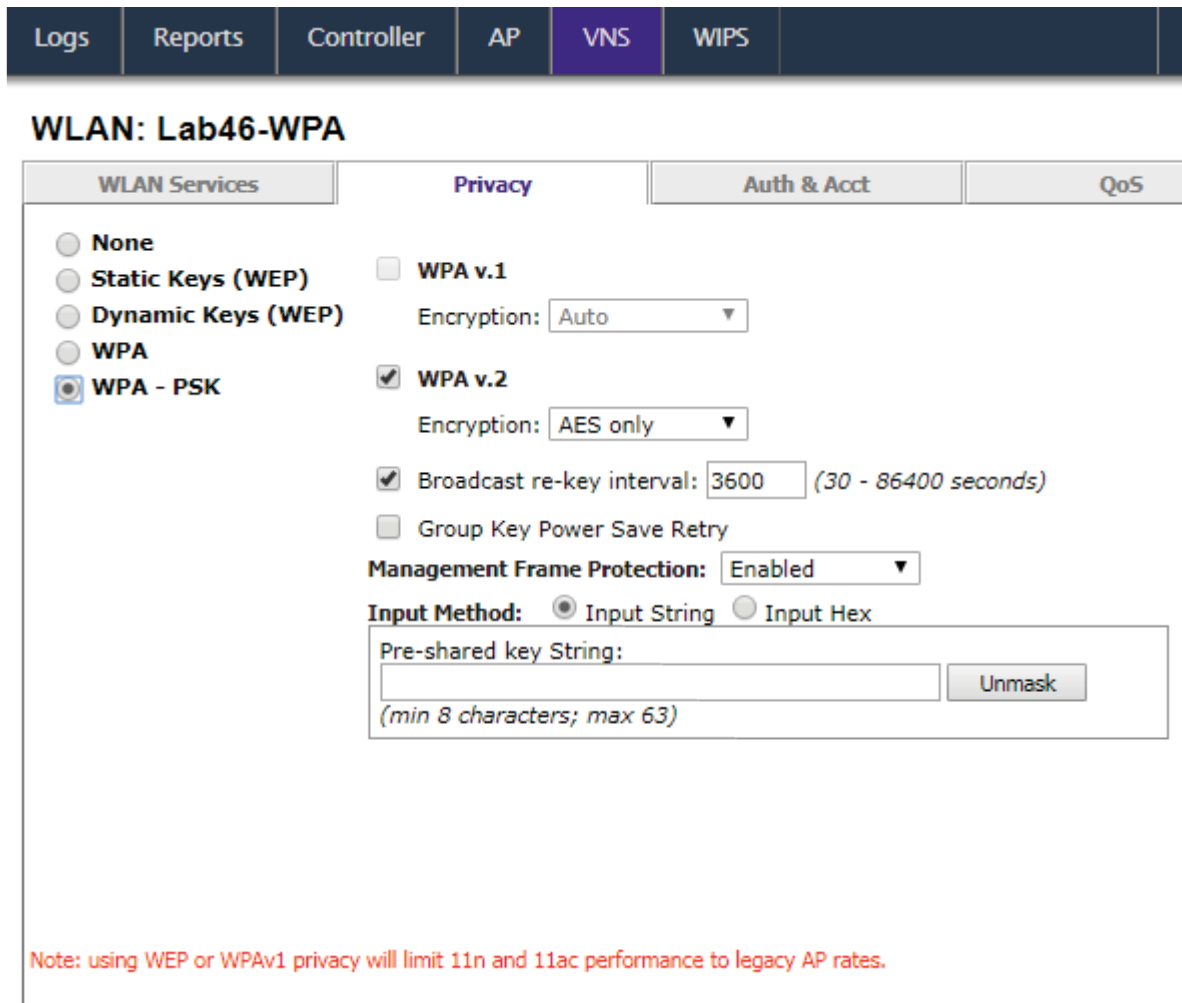
- Opportunistic Keying & Pre-auth — Opportunistic Keying and Pre-auth options is meant for environments where device clients supporting either authentication method (OKC or Pre-Auth) may be expected. The method that is used in each case is up to the individual client device.

Configuring WLAN Service Privacy

To configure privacy:

- 1 From the top menu, click **VNS**. Then, in the left pane, select **WLAN Services**. The **WLAN Services** window displays.
- 2 Select the desired service to edit from the left pane. The **WLAN Service** configuration page is displayed.

- 3 Click the **Privacy** tab, then select the desired privacy method. The WLAN Services Privacy tab displays. [Table 55](#) describes the WLAN services privacy tab fields and buttons.



WLAN: Lab46-WPA

WLAN Services | **Privacy** | Auth & Acct | QoS

☐ None
☐ Static Keys (WEP)
☐ Dynamic Keys (WEP)
☐ WPA
☒ **WPA - PSK**

☐ WPA v.1
 Encryption: Auto

☒ **WPA v.2**
 Encryption: AES only

☒ Broadcast re-key interval: 3600 (30 - 86400 seconds)
☐ Group Key Power Save Retry

Management Frame Protection: Enabled

Input Method: ☒ Input String ☐ Input Hex

Pre-shared key String:
 (min 8 characters; max 63)

Note: using WEP or WPAv1 privacy will limit 11n and 11ac performance to legacy AP rates.

Figure 101: Configuring WLAN Service Privacy

Table 55: WLAN Services Privacy Tab - Fields and Buttons

Field/Button	Description
None	Select to configure a WLAN service with no privacy settings.
Static Keys (WEP)	Select to configure static key (WEP) privacy settings.
WEP Key Index	From the WEP Key Index drop-down list, select the WEP encryption key index. Options are 1 to 4. This field is available only when configuring static keys.
WEP Key Length	From the WEP Key Length drop-down list, click the WEP encryption key length . Options are: 64-bit, 128-bit, and 152-bit. This field is available only when configuring static keys.

Table 55: WLAN Services Privacy Tab - Fields and Buttons (continued)

Field/Button	Description
Input Method	Select one of the following input methods: • Input Hex — If you select Input Hex, type the WEP key input in the WEP Key box. The key is generated automatically, based on the input. • Input String — If you select Input String, type the secret WEP key string used for encrypting and decrypting in the Strings box. The WEP Key box is automatically filled by the corresponding Hex code. This field is available only when configuring static keys.
WEP Key	Type the WEP key using the input method chosen above.
Dynamic Keys (WEP)	Select to configure dynamic keys (WEP) privacy settings.
WPA	Select to configure WPA privacy settings.
WPA - PSK	Select to configure dynamic keys (WEP) privacy settings.
WPA v.1	Select the check box to enable WPA v.1 encryption, and then select an encryption method: Auto — If you click Auto, the AP advertises both TKIP and CCMP (counter mode with cipher block chaining message authentication code protocol). CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). Auto is the default. TKIP only — If you click TKIP, the AP advertises TKIP as an available encryption protocol. It will not advertise CCMP. This field is available only when configuring WPA and WPA - PSK privacy settings. Note: TKIP is no longer a supported configuration. Instead you will be directed to configure WPA/WPA2 mixed mode security.

Table 55: WLAN Services Privacy Tab - Fields and Buttons (continued)

Field/Button	Description
WPA v.2	Select the check box to enable WPA v.2 encryption, and then select an encryption method: Auto — If you click Auto, the AP advertises both TKIP and CCMP (counter mode with cipher block chaining message authentication code protocol). CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). Auto is the default. AES only — If you click AES, the AP advertises CCMP as an available encryption protocol. It will not advertise TKIP. This field is available only when configuring WPA and WPA - PSK privacy settings. TKIP — If you click AES, the wireless AP advertises CCMP as an available encryption protocol.
Key Management Options	Click one of the following key management options: • None — The mobile units (client devices) perform a complete 802.1x authentication each time they associate or connect to an AP. • Opportunistic Keying — Enables secure fast roaming (SFR) of mobile units. For more information, see Configuring WLAN Service Privacy on page 330. • Pre-authentication — Enables seamless roaming. For more information, see Configuring WLAN Service Privacy on page 330. • Opportunistic Keying & Pre-auth — For more information, see Configuring WLAN Service Privacy on page 330.
Broadcast re-key interval	To enable re-keying after a time interval, select the Broadcast re-key interval box, then type the time interval after which the broadcast encryption key is changed automatically. The default is 3600 seconds. If this check box is not selected, the Broadcast encryption key is never changed and the AP will always use the same broadcast key for Broadcast/Multicast transmissions which will reduce the level of security for wireless communications.
Management Frame Protection	Select to enable or disable frame protection for WPA v.2 privacy.
Fast Transition	Click to Enable for 11r enabled APs. This feature only applies to 37xx and 38xx APs.
Input Method	Select one of the following input methods: • Input Hex — If you select Input Hex, type the pre-shared key as hex characters. • Input String — If you select Input String, type the pre-shared key as a string of characters.

Table 55: WLAN Services Privacy Tab - Fields and Buttons (continued)

Field/Button	Description
Pre-shared key String	In the Pre-Shared Key box, type the shared secret key to be used between the wireless device and AP. The shared secret key is used to generate the 256-bit key. To proofread your entry before saving the configuration, click Unmask to display the Pre-Shared Key. To mask the key, click Mask
Save	Click to save the configuration.

Configuring Accounting and Authentication

The next step in configuring a [WLAN Service](#) is to set up the authentication mechanism. There are various authentication modes available:

- None
- Internal Captive Portal
- External Captive Portal
- GuestPortal
- GuestSplash
- Firewall-Friendly External Captive Portal
- 802.1x authentication (The wireless device user must be authenticated before gaining network access.)



Note

You cannot configure accounting and authentication for a remote WLAN service. The authentication that you configure for the corresponding remoteable WLAN service applies to the remote WLAN service as well.

The first step for any type of authentication is to select RADIUS servers for the following:

- Authentication
- Accounting
- MAC-based authentication

The selected RADIUS servers are displayed in a tri-pane under RADIUS Servers. The RADIUS Server pane changes depending on the Authentication and Accounting methods you enable:

- If the Authentication Mode is enabled, the **Auth** pane displays.
- If MAC-based Authentication is enabled, a **MAC** pane displays.
- If RADIUS Accounting is enabled an **Accounting** pane displays.

For more information, see [Selecting RADIUS Servers](#) on page 335.

For more information about captive portal, see [Configuring Basic Captive Portal Settings](#) on page 349

Related Links

[Selecting RADIUS Servers](#) on page 335

[MAC-Based Authentication for a WLAN Service](#) on page 338

Defining Accounting Methods for a WLAN Service on page 336

Selecting RADIUS Servers

You have the option to specify up to three RADIUS servers for authentication and accounting. The first server in the list is the first active server for both Primary-Backup and Round-Robin. For Primary-Backup, the first server is also the primary server. In the event of the first server fails, the next server in the list (backup server) becomes active. In the case of Round-Robin configuration, each server in the list is contacted in a round-robin fashion starting with the first server. See [Configuring Advanced RADIUS Servers Settings](#) on page 397.

To select RADIUS servers for authentication and accounting:

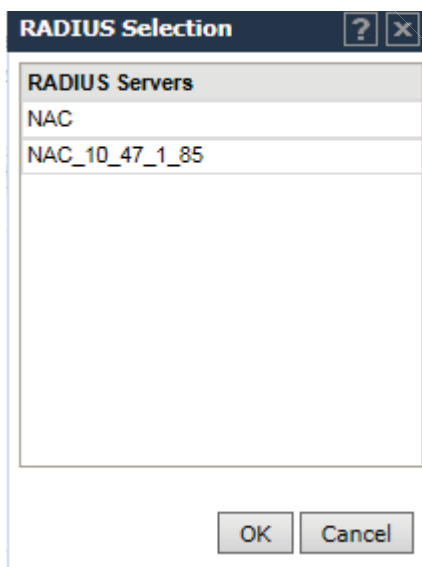
- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **WLAN Services** pane, then click the WLAN Service.
The **WLAN Services** configuration page is displayed.
- 3 Click the **Auth & Acct** tab.
- 4 Select one or more servers. To select a server:
 - Click the **+** sign in the appropriate column heading to select a server for that specific function, or
 - Click **Select RADIUS** to apply your selection to all three functions.

The **RADIUS Selection** dialog displays.



Note

Once selected, the server is no longer available in the RADIUS servers selection list.
Maximum number of selected servers is three.



- 5 Once you have more than one server listed, select a server and click **Move Up** or **Move Down** to arrange the order.

The screenshot shows the 'RADIUS Servers' configuration window. At the top, there are two checked options: 'Enable MAC-based authentication' and 'Enable RADIUS Accounting'. Below these are three columns: 'Auth', 'MAC', and 'Accounting'. Each column has a '+' button in the top right corner. The 'Auth' column contains 'NPS_2012_R2' and 'NAC_10_47_1_85'. The 'MAC' column contains 'NAC_10_47_1_85'. The 'Accounting' column contains 'NPS_2012_R2' and 'NAC_10_47_1_85'. To the right of the columns is a vertical menu with buttons: 'Select Radius', 'New', 'Move Up', 'Move Down', 'Configure', 'Test', 'Summary', 'Remove', and 'Radius TLVs'. A red arrow points to the 'Move Up' button.

- 6 To save your changes, click **Save**.

Defining Accounting Methods for a WLAN Service

Accounting tracks the activity of wireless device users. There are two types of accounting available:

- **Controller accounting** — Enables the controller to generate Call Data Records (CDRs), containing usage information about each wireless session. CDR generation is enabled on a per VNS basis. For more information on CDRs, refer to section [Call Detail Records \(CDRs\)](#) on page 663.
- **RADIUS accounting** — Enables the controller to generate an accounting request packet with an accounting start record after successful login by the wireless device user, and an accounting stop record based on session termination. The controller sends the accounting requests to a remote RADIUS server.

Controller accounting creates Call Data Records (CDRs). If RADIUS accounting is enabled, a RADIUS accounting server needs to be specified.

To define accounting methods:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **WLAN Services** pane, then click the WLAN Service you want to define accounting methods for.

The **WLAN Services** configuration page is displayed.

- 3 Click the **Auth & Acct** tab.
- 4 Select an authentication method under **Mode** or click **Enable MAC-based authentication**.

The **Enable RADIUS Accounting** check box displays.

- 5 In the **Accounting** column, select the RADIUS server. For more information, see [Selecting RADIUS Servers](#) on page 335.

**Note**

The RADIUS servers are defined on the **Global Settings** screen. For more information, see [Defining RADIUS Servers and MAC Address Format](#) on page 394.

**Note**

When multiple RADIUS servers are configured for a WLAN Service, Accounting packets are sent to the primary RADIUS server only. The secondary servers are used as fail over when necessary. When upgrading to v10.31.02, the previous behavior of sending Accounting packets to all servers is maintained.

- 6 One a server is selected, click **Configure**.
- 7 The **RADIUS Parameters** dialog is displayed.
The configured values for the selected server are displayed in the table at the top.

	Port	Timeout	NAS IP	NAS Identifier	Auth Type
Auth	1812	15	VNS IP	VNS NAME	EAP
Acct	1813	10	VNS IP	VNS NAME	-

NAS IP Address: ☐ Use VNS IP address or use:

NAS identifier: ☐ Use VNS name or use:

OK Cancel

Figure 102: RADIUS Parameters dialog

- 8 For **NAS IP Address**, accept the default of “Use VNS IP address” or de-select the check box and type the IP address of a Network Access Server (NAS).
- 9 For **NAS Identifier**, accept the default of “Use VNS name” or type the Network Access Server (NAS) identifier. The NAS identifier is a RADIUS attribute that identifies the server responsible for passing information to designated RADIUS servers and then acting on the response returned.
- 10 For **Auth. type**, select the Protocol using the drop down list. Choices are PAP, CHAP, MS-CHAP, or MS-CHAP2.
- 11 In the **Password** box, type the password that will be passed to RADIUS for wireless MAC authentication.
To proofread your shared secret key, click **Unmask**. The password is displayed.
- 12 Click **OK**.

- 13 To enable controller accounting, select **Collect Accounting Information of Wireless Controller**.
- 14 To save your changes, click **Save**.

Configuring Authentication for a WLAN Service

- **802.1x Authentication** — If 802.1x authentication mode is configured, the wireless device must successfully complete the user authentication verification prior to being granted network access. This enforcement is performed by both the user's client and the AP. The wireless device's client utility must support 802.1x. The user's EAP packets request for network access along with login identification or a user profile is forwarded by the controller to a RADIUS server.
- **Captive Portal Authentication** — For Captive Portal authentication, the wireless device connects to the network, but can only access the specific network destinations defined in the non-authenticated filter. For more information, see [Policy Rules](#) on page 288. One of these destinations should be a server, either internal or external, which presents a Web login page — the Captive Portal. The wireless device user must input an ID and a password. This request for authentication is sent by the controller to a RADIUS server or other authentication server. Based on the permissions returned from the authentication server, the controller implements role and allows the appropriate network access.

Captive Portal authentication relies on a RADIUS server on the enterprise network. There are three mechanisms by which Captive Portal authentication can be carried out:

- **Internal Captive Portal** — The controller displays the Captive Portal Web page, carries out the authentication, and implements role.
- **External Captive Portal** — After an external server displays the Captive Portal Web page and carries out the authentication, the controller implements role.
- **External Captive Portal with internal authentication** — After an external server displays the Captive Portal Web page, the controller carries out the authentication and implements role.
- **RADIUS servers** — RADIUS servers can perform the following for a WLAN Service:
 - **Authentication** — RADIUS servers are configured to provide authentication.
 - **MAC authentication** — RADIUS servers are configured to provide MAC-based authentication.
 - **Accounting** — RADIUS servers are configured to provide accounting services.

MAC-Based Authentication for a WLAN Service

- **MAC-based authentication** — MAC-based authentication enables network access to be restricted to specific devices by MAC address. The controller queries a RADIUS server for a MAC address when a wireless client attempts to connect to the network.
- MAC-based authentication can be set up on any type of WLAN Service. To set up a RADIUS server for MAC-based authentication, you must set up a user account with UserID=MAC and Password=MAC (or a password defined by the administrator) for each user. Specifying a MAC address format and role depends on which RADIUS server is being used.
- If MAC-based authentication is to be used in conjunction with the 802.1x or Captive Portal authentication, an additional account with a real User ID and Password must also be set up on the RADIUS server.

MAC-based authentication responses may indicate to the controller what VNS a user should be assigned to. Authentication (if enabled) can apply on every roam.

Related Links

[Configuring MAC-Based Authentication](#) on page 339

Configuring MAC-Based Authentication

This topic outlines the MAC-Based Authentication settings.

Click the **Configure** button to open the **MAC-Based Authorization** dialog.

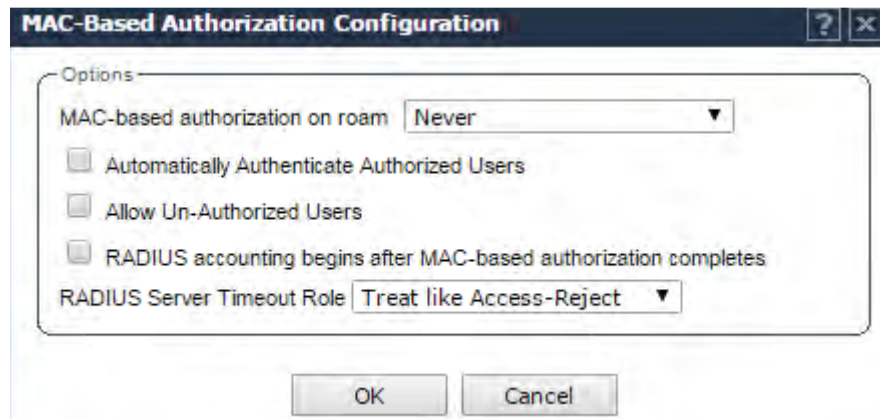


Figure 103: MAC-Based Authorization Configuration

Table 56: MAC-Based Authorization Configuration - Fields and Buttons

Field/Button	Description
MAC-based authorization on roam	Select method for MAC-based authorization: Never: disables the feature On inter-AP roam: enables MAC-based authorization on roam. On inter-Area roam: enables MAC-based authorization sent to the RADIUS server on area roams. Note: Enable this option if you want your clients to be authorized every time they roam to another AP or area. If this option is not enabled, and MAC-based authentication is in use, the client is authenticated only at the start of a session.
Automatically Authenticate Authorized Users	Select to automatically authenticate authorized users. When set, a station that passes MAC-based authentication is treated as fully authorized. For example, its authentication state is set to fully authenticated. This can trigger a change to the role applied to the station. If Captive Portal authentication is also configured on the WLAN Service, a station that passes MAC-based authentication will not have to pass Captive Portal authentication as well.
Allow Un-Authorized Users	Select to allow un-authorized users which permits stations that do not pass MAC-based authentication to stay on the network in an un-authorized state. The station can be confined to a “Walled Garden” by its assigned role. If Captive Portal authentication is also configured on the WLAN Service, a station that fails MAC-based authentication can still become authorized by passing Captive Portal authentication.

Table 56: MAC-Based Authorization Configuration - Fields and Buttons (continued)

Field/Button	Description
RADIUS accounting begins after MAC-based authorization completes	Select to delay RADIUS accounting until after MAC-based authorization is complete.
RADIUS Server Timeout Role	Select a Radius Server Timeout Role from the drop-down list.

Assigning RADIUS Servers for Authentication

To assign RADIUS servers for authentication:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **WLAN Services** pane, then click the WLAN Service.
- 3 Click the **Auth & Acct** tab.

WLAN: h1

WLAN Services Privacy **Auth & Acct** QoS

Authentication

Mode: 802.1x no HTTP Redirection Configure...

☒ Enable MAC-based authentication Configure...

☒ Enable RADIUS Accounting

RADIUS Servers

Auth	MAC	Accounting
+	+	+
nac-1		nac-1

Select Radius
New
Move Up
Move Down
Configure
Test
Summary
Remove
Radius TLVs

☐ Collect Accounting Information of Wireless Controller

Figure 104: Auth & Acct Tab

Table 57: WLAN Services Auth & Acct Tab - Fields and Buttons

Field/Button	Description
Authentication	
Mode	Select an authentication mode from the drop-down list: • Disabled • 802.1x • Internal • External • Firewall Friendly External • Guest Portal • Guest Splash
Configure	Click to configure the selected mode. For more information, see Configuring Accounting and Authentication on page 334.
Enable MAC-based authentication	Select to enable the RADIUS server to perform MAC-based authentication for the VNS with Captive Portal.
RADIUS Servers	To select a server, see Selecting RADIUS Servers on page 335. The RADIUS servers are defined on the Global Settings screen. For more information, see Defining RADIUS Servers and MAC Address Format on page 394.
Collect Accounting Information of Wireless Controller	Select this check box to enable Controller accounting.

Note

Both MAC-based Authorization settings work together so that a station can be allowed onto a WLAN Service if it passes MAC-based authentication or Captive Portal authentication. Owners of known stations do not have to enter credentials and owners of unknown stations can get onto the network, if authorized, via Captive Portal.

- 4 Click the **Radius TLVs** button to open the RADIUS Access-Request Message Options dialog.

RADIUS Access-Request Message Options

VSAs

Include the following Vendor-Specific-Attributes in RADIUS Requests:

☐ Ingress Rate Control ☒ VNS Name

☐ Egress Rate Control ☒ AP Name

☐ Topology Name ☒ SSID

☐ Role Name

Optional TLVs

Include the following Standard-Attributes in RADIUS Requests:

☒ Chargeable-User-Identity

☐ Treat Access-Accept without Chargeable-User-Identity attribute as Access-Reject

Zone Support

☒ RADIUS Request Called Station ID Options

☒ Replace BSSID with Zone name

☐ Replace BSSID with AP Ethernet MAC

Operator Name Disabled ▼

OK Cancel

Figure 105: RADIUS Access Request Message Options

Table 58: RADIUS TLVs Dialog - Fields and Buttons

Field/Button	Description
VSAs	
Vendor-Specific-Attributes in RADIUS Requests	Select the appropriate check boxes to include the Vendor Specific Attributes (VSAs) in the message to the RADIUS server: • Ingress Rate Control • Egress Rate Control • Topology Name • Role Name • VNS Name • AP Name • SSID For more information, see Defining Common RADIUS Settings on page 344.
Optional TLVs	
Chargeable-User-Identity	Select to NOT return a Chargeable-User-Identity attribute for the RADIUS Server.

Table 58: RADIUS TLVs Dialog - Fields and Buttons (continued)

Field/Button	Description
Treat Access-Accept without Chargeable-User-Identity attribute as Access-Reject	Select to enable feature.
Zone Support	
RADIUS Request Call Station ID Options:	
Replace BSSID with Zone name	Selecting this check box to allows the RADIUS client to send the AP Zone name as the BSSID instead of the radio MAC address. This feature can be enabled regardless of whether the Site is using centrally located or local RADIUS servers. Zone name is limited to 32 bytes. Each AP can have its own Zone label although it is often useful to assign the same Zone to multiple APs.
Replace BSSID with AP Ethernet MAC	Selecting this check box allows the RADIUS client to send the AP Ethernet MAC as the BSSID instead of the radio MAC address. This feature can be enabled regardless of whether the Site is using centrally located or local RADIUS servers. The AP MAC address value is always the AP LAN1 MAC address.
Operator Name	Select the name of the user assigned to this RADIUS server from the drop-down list. Once a name is selected, a text box displays to allow text to be entered.

- 5 To save your changes, click **Save**.

Defining the RADIUS Server Priority for RADIUS Redundancy

If more than one server has been defined for any type of authentication or accounting, you can define the priority of the servers.

You have the option to specify up to three RADIUS servers for authentication and accounting. The first server in the list is the first active server for both Primary-Backup and Round-Robin. For Primary-Backup, the first server is also the primary server. In the event of the first server fails, the next server in the list (backup server) becomes active. In the case of Round-Robin configuration, each server in the list is contacted in a round-robin fashion starting with the first server. See [Configuring Advanced RADIUS Servers Settings](#) on page 397.

If all defined RADIUS servers fail to respond, a critical message is generated in the logs.

To define the RADIUS server priority for RADIUS redundancy:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **WLAN Services** pane, then click the WLAN Service.
The **WLAN Services** configuration page is displayed.
- 3 Click the **Auth & Acct** tab.
- 4 Select one or more servers. See [Selecting RADIUS Servers](#) on page 335.

- Once you have more than one server listed, select a server and click **Move Up** or **Move Down** to arrange the order.

The screenshot shows the 'RADIUS Servers' configuration window. At the top, there are checkboxes for 'Enable MAC-based authentication' and 'Enable RADIUS Accounting', both of which are checked. A 'Configure...' button is next to the first checkbox. Below these are three columns: 'Auth', 'MAC', and 'Accounting'. Each column has a '+' button in the top right corner. The 'Auth' column contains 'NPS_2012_R2' and 'NAC_10_47_1_85'. The 'MAC' column contains 'NAC_10_47_1_85'. The 'Accounting' column contains 'NPS_2012_R2' and 'NAC_10_47_1_85'. To the right of the columns is a vertical stack of buttons: 'Select Radius', 'New', 'Move Up', 'Move Down', 'Configure', 'Test', 'Summary', 'Remove', and 'Radius TLVs'. A red arrow points to the 'Move Up' button.

- To save your changes, click **Save**.

Configuring Assigned RADIUS Servers

Configuring assigned RADIUS servers for a VNS can include the following:

- [Defining Common RADIUS Settings](#) on page 344
- [Defining RADIUS Settings for Individual RADIUS Servers](#) on page 345
- [Testing RADIUS Server Connections](#) on page 346
- [Viewing the RADIUS Server Configuration Summary](#) on page 347
- [Removing an Assigned RADIUS Server from a WLAN Service](#) on page 348

Defining Common RADIUS Settings

To Define Common RADIUS Settings:

- From the top menu, click **VNS**.
- In the left pane expand the **WLAN Services** pane, then click the WLAN Service. The **WLAN Services** configuration page is displayed.
- Click the **Auth & Acct** tab.
- In the **RADIUS Servers** section, click the **Radius TLVs** button and select the appropriate check boxes to include the Vendor Specific Attributes in the message to the RADIUS server. For more information, see [Vendor Specific Attributes](#) on page 344.
- To save your changes, click **Save**.

Vendor Specific Attributes

In addition to the standard RADIUS message, you can include Vendor Specific Attributes (VSAs). The ExtremeWireless authentication mechanism provides VSAs for RADIUS and other authentication mechanisms (see [Table 59](#).)

Table 59: Vendor Specific Attributes

Attribute Name	ID	Type	Messages	Description
AP-Name	2	string	Sent to RADIUS server	The name of the AP the client is associating to. It can be used to assign role based on AP name or location.
AP-Serial	3	string	Sent to RADIUS server	The AP serial number. It can be used instead of (or in addition to) the AP name.
AP Ethernet MAC		string	Sent to RADIUS server	The MAC address of the AP used by the ECP to determine client location.
AP Location		string	Sent to RADIUS server	The physical location of the AP. Provided by the network administrator.
VNS-Name	4	string	Sent to RADIUS server	The name of the Virtual Network the client has been assigned to. It is used in assigning role and billing options, based on service selection.
SSID	5	string	Sent to RADIUS server	The name of the SSID the client is associating to. It is used in assigning role and billing options, based on service selection.
BSS-MAC	6	string	Sent to RADIUS server	The name of the BSS-ID the client is associating to. It is used in assigning role and billing options, based on service selection and location.
Role-Name	7	string	Sent to RADIUS server	The name of the role applied to the station's session.
Topology-Name	8	string	Sent to RADIUS server	The name of the topology applied to the station's session.
Ingress-RC-Name	9	string	Sent to RADIUS server	The name of the rate limit applied to the station's session's outbound traffic.
Egress-RC-Name	10	string	Sent to RADIUS server	The name of the rate limit applied to the station's session's inbound traffic.

The RADIUS message also includes RADIUS attributes Called-Station-Id and Calling-Station-Id to include the MAC address of the wireless device.

**Note**

Siemens-URL-Redirection is supported by MAC-based authentication.

Defining RADIUS Settings for Individual RADIUS Servers

To define RADIUS settings for individual RADIUS servers:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **WLAN Services** pane, then click the WLAN Service. The **WLAN Services** configuration page is displayed.
- 3 Click the **Auth & Acct** tab.

- 4 In the **Server** table, click the RADIUS server you want to define, and then click **Configure**.
The **RADIUS Parameters** dialog is displayed.

RADIUS Parameters

Server: nac-1

	Port	Timeout	NAS IP	NAS Identifier	Auth Type
Auth	1812	15	VNS IP	VNS NAME	EAP
Acct	1813	10	VNS IP	VNS NAME	-

NAS IP Address: ☐ Use VNS IP address or use:

NAS Identifier: ☐ Use VNS name or use:

OK Cancel

- 5 For **NAS IP Address**, accept the default of “Use VNS IP address” or de-select the check box and type the IP address of a Network Access Server (NAS).
- 6 For **NAS Identifier**, accept the default of “Use VNS name” or type the Network Access Server (NAS) identifier. The NAS identifier is a RADIUS attribute that identifies the server responsible for passing information to designated RADIUS servers and then acting on the response returned.
- 7 For **Auth. type**, select the Protocol using the drop down list. Choices are PAP, CHAP, MS-CHAP, or MS-CHAP2.
- 8 In the **Password** box, type the password that will be used to validate the connection between the controller and the RADIUS server.
To proofread your shared secret key, click **Unmask**. The password is displayed.
- 9 Click **OK**.
- 10 To save your changes, click **Save**.

Testing RADIUS Server Connections

To test RADIUS server connections:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **WLAN Services** pane, then click the WLAN Service. The **WLAN Services** configuration page is displayed.
- 3 Click the **Auth & Acct** tab.

- 4 In the **Server** table, click the RADIUS server whose connection you want to test, and then click **Test**.

The RADIUS test is a test of connectivity to the RADIUS server, not of full RADIUS functionality. The controller's RADIUS connectivity test initiates an access-request, to which the RADIUS server will respond. If a response is received (either access-reject or access-accept), then the test is deemed to have succeeded. If a response is not received, then the test is deemed to have failed. In either case, the test ends at this point.

If the WLAN Service Authentication mode is Internal or External Captive Portal, or if MAC-Based Authorization is selected, then this test can also test a user account configured on the RADIUS server. In these cases, if proper credentials are filled in for User ID and Password, an access-accept could be returned.

If the WLAN Service Authentication mode is 802.1x, however, an Access-Reject is expected if the RADIUS server is accessible, and the test is considered a success.

Figure 106: Test RADIUS Server

- 5 In the **User ID** box, type the user ID that you know can be authenticated.
- 6 In the **Password** box, type the corresponding password. A password is not required for a AAA VNS.
- 7 Click **Test**. The **Test Result** screen displays.
- 8 Click **Close** after reviewing the test results.
- 9 To save your changes, click **Save**.

Viewing the RADIUS Server Configuration Summary

To view the RADIUS server configuration summary:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **WLAN Services** pane, then click the WLAN Service. The **WLAN Services** configuration page is displayed.
- 3 Click the **Auth & Acct** tab.

- 4 In the **Server** table, click a RADIUS server whose configuration summary you want to view, and then click **Summary**. The **RADIUS Summary** screen displays.

Server	Use For	Priority	Port	# of Retries	Timeout	NAS Identifier	Auth. Type
Smoke Test Radius Server							
	Auth	1	1812	3	5	CNL-422-0-0	PAP
	MAC	1	1812	3	5	CNL-422-0-0	CHAP
	Acct	1	1813	3	5	CNL-422-0-0	N/A

Figure 107: RADIUS Summary

- 5 Click **Close**.
- 6 To save your changes, click **Save**.

Removing an Assigned RADIUS Server from a WLAN Service

To remove an assigned RADIUS Server from a WLAN Service:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **WLAN Services** pane and click the WLAN Service you want to define accounting methods for.
- 3 Click the **Auth & Acct** tab.
- 4 In the **Server** table, click the assigned RADIUS server that you want to remove from the VNS, and then click **Remove**. The RADIUS server is removed from the VNS.
- 5 Click **Save**.

Defining a WLAN Service with No Authentication

You can set up a WLAN Service that will bypass all authentication mechanisms and run the ExtremeWireless Appliance with no authentication of a wireless device user.

A WLAN Service with no authentication can still control network access using policy rules. For more information on how to set up policy rules that allow access only to specified IP addresses and ports, see [Policy Rules](#) on page 288.

To define a WLAN Service with No Authentication:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **WLAN Services** pane, then click the WLAN Service you want to configure or click **New**.
- 3 Configure the service as described in [WLAN Services Overview](#) on page 318.
- 4 Click the **Auth & Acct** tab.
- 5 From the **Authentication Mode** drop-down list, select **Disabled**.
- 6 Click **Save**.

Configuring Captive Portal for Internal or External Authentication

Captive Portal allows you to require network users to complete a defined process, such as logging in or accepting a network usage role, before accessing the Internet.

The Captive Portal options are:

- **802.1x** - Define the parameters of the external Captive Portal page displayed by an external server. The authentication can be carried out by an external authentication server or by the controller request to a RADIUS server.
- **Internal Captive Portal** — Define the parameters of the internal Captive Portal page displayed by the controller, and the authentication request from the controller to the RADIUS server.
- **External Captive Portal** — Define the parameters of the external Captive Portal page displayed by an external server. The authentication can be carried out by an external authentication server or by the appliance request to a RADIUS server.
- **Firewall Friendly External** — Define the parameters of the Firewall Friendly Captive Portal page displayed by an external server. This parameter minimizes the need to open firewall ports and any device on the secure side is allowed to connect to the Internet on port 80, 443.
- **GuestPortal** — Define the parameters for a GuestPortal Captive Portal page. A GuestPortal provides wireless device users with temporary guest network services.
- **Guest Splash** — Define the parameters of the Guest Splash page displayed by the controller. These parameters are similar to those for an internal Captive Portal page, except that the options to configure the labels for user id and password fields are not present since login information is not required when the user is re-directed to the authorization web page. This type of Captive Portal could be used where the user is expected to read and accept some terms and conditions before being granted network access.

Configuring Basic Captive Portal Settings

When configuring captive portal, different settings become available depending on the captive portal option you choose.

To configure the captive portal settings:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **WLAN Services** pane, then click the WLAN Service. The **WLAN Services** configuration page is displayed.

- 3 Click the **Auth & Acct** tab.

WLAN: h1

WLAN Services Privacy **Auth & Acct** QoS

Authentication

Mode: 802.1x no HTTP Redirection Configure...

☒ Enable MAC-based authentication Configure...

☒ Enable RADIUS Accounting

RADIUS Servers

Auth	MAC	Accounting	
+	+	+	
nac-1		nac-1	Select Radius New Move Up Move Down Configure Test Summary Remove Radius TLVs

☐ Collect Accounting Information of Wireless Controller

Figure 108: Configuring Basic Captive Portal

- 4 In the **Authentication Mode** drop-down list, select a Captive Portal option.

- Disabled
- 802.1x
- Internal
- External
- Firewall Friendly External
- Guest Portal



Note

You must configure a Guest Portal before **Guest Portal** appears as a Captive Portal option. Only one WLAN Service can be configured for Guest Portal on a VNS.

- Guest Splash

5 Click **Configure**.

The Captive Portal configuration page displays. The page display differs depending on the mode that you have selected:

- Internal and Splash modes, see [Configuring Internal Captive Portal and Guest Splash](#) on page 359
- External and 802.1x modes, see [Configuring External and Mode 802.1 Captive Portal](#) on page 351
- Guest Portal mode, see [Configuring Guest Portal](#) on page 360
- Firewall Friendly External Captive Portal mode, see [Configuring Firewall Friendly External Captive Portal](#) on page 353.

Configuring External and Mode 802.1 Captive Portal

The screenshot shows a window titled "HTTP Redirect". Inside, there's a "Session Control Interface" section. It contains an "EWC Connection" field with a dropdown menu showing "192.168.3.225" and a port field showing "0". Below this is the text "External authentication server access. Port range: 32768 - 65535". There's a checkbox for "Enable https support" which is currently unchecked. Below that is an "Encryption" dropdown menu showing "None". Then there's a "Shared Secret" text field with a note below it: "Shared secret should be between 16 - 64 characters". Below that is a "Redirection URL" text field with a note: "Note: token=<integer_val>&dest=<original_target_url> will be APPENDED to the redirection URL". At the bottom of the form is a checkbox for "Add EWC IP & Port to redirection URL" which is unchecked. At the bottom right of the window are "Close" and "Cancel" buttons.

Figure 109: Captive Portal Page for External and 802.1x Modes

Table 60: External Captive Portal Page - Fields and Buttons

Field/Button	Description
Session Control Interface	
EWC Connection	In the drop-down list, click the IP address of the external Web server. and then enter the port of the controller. If there is an authentication server configured for this VNS, the external Captive Portal page on the external authentication server will send the request back to the controller to allow the controller to continue with the RADIUS authentication and filtering.
Enable HTTPS support	Select Enable https support if you want to enable HTTPS support (TLS/SSL) for this external captive portal. This has no impact on the traffic exchanged between users' browsers and the External Captive Portal. When enabled, this option protects the session control traffic between the external captive portal and the controller from being read by a third party. This is particularly useful when a dedicated network management <i>VLAN (Virtual LAN)</i> is unavailable to carry the session control traffic. For more information, see the <i>Integration Guide</i> .

Table 60: External Captive Portal Page - Fields and Buttons (continued)

Field/Button	Description
Encryption	Select the data encryption to use. Options are: • None—no encryption is performed. If the HTTPS option is not enabled, session control messages are sent in plain text over the network. • Legacy—both the ECP and the controller are expected to use simple message encryption based on <i>MD5 (Message-Digest algorithm 5)</i>. Frames are encrypted by Xoring session control message payload with a keystream generated from an MD5 hash of a shared key. This is a weak encryption algorithm and is only supported for backward compatibility. If encryption is needed, consider using the option below. • AES—session control messages sent by the controller and ECP are encrypted with the “Advanced Encryption Standard” based on the Rijndael cipher. AES encryption is considerably more secure than legacy encryption. If encryption is enabled then a shared key must be entered. Note: Using the encryption option has one advantage over using the HTTPS option alone. When HTTPS is enabled, the ECP can authenticate the controller’s certificate, but the controller does not ask the client to provide one. Consequently, HTTPS does not prevent unauthorized users from sending messages to the session control interface. Because the encryption option is based on a shared key, the encryption provides a form of authentication. If the controller can decrypt the payload of a session control message, then it has reason to believe the message came from the external captive portal.
Shared Secret	Type the password common to both the controller and the external web server if you want to encrypt the information passed between the controller and the external web server. If encryption is enabled then a shared key must be entered. A shared key is a string that both the controller and the ECP use to encrypt and decrypt session control messages. The shared key must be between 16 and 64 characters long. For better security, use a long key composed of randomly selected characters.
Redirection URL	The Redirection URL field contains the URL to which the controller will redirect all blocked, unauthenticated HTTP traffic on this WLAN Service, or traffic that has been explicitly configured for redirection, depending on your configuration. This should be the URL of the page that will prompt the user to authenticate. If using host name rules, the redirection url can be the configured host name. The redirected browser will issue a “get” to the ECP for this URL. The “Redirection URL”: • Can begin with “http://” or “https://”. • Must end with a “?” or “&”. Use “&” if the base URL contains some query strings. Note: The Redirection URL does not support IPv6.

Table 60: External Captive Portal Page - Fields and Buttons (continued)

Field/Button	Description
Add EWC IP & Port to redirection URL	The Add HWC IP & Port to redirection URL option is useful if the external captive portal serves more than one controller. An ECP must send its session control messages to the controller hosting the controlled session. If an ECP serves more than one controller, then the Add HWC IP & Port to redirection URL option must be used to identify the source of the redirection. The ECP should store the controller address and port with the token and other session details so that it is available throughout the authentication process.
Special	
ToS override for NAC	Allows for ToS marking results in redirection to a captive portal via a NAC server.
Close	Click to save your changes and close this page.
Cancel	Click to discard the configuration

**Note**

You must add a role rule to the non-authenticated filter that allows access to the external Captive Portal site. For more information, see [Policy Rules](#) on page 288.

Related Links

[Configuring Basic Captive Portal Settings](#) on page 349

[Policy Rules](#) on page 288

Configuring Firewall Friendly External Captive Portal

This task describes how to configure a Firewall Friendly External Captive Portal.

- 1 From the **Auth & Account** tab, in the Mode field, select **Firewall Friendly External**.
- 2 Click **Save**.
The **Configure** button is enabled.
- 3 Configure RADIUS servers for authentication. For more information, see [Assigning RADIUS Servers for Authentication](#) on page 340.

- 4 Click **Configure**.

Configure

Redirect to External Captive Portal

Identity:

Shared Secret:
 Shared secret should be between 16 - 255 characters

Redirection URL:
Note: token=<integer_val>&dest=<original_target_url> will be APPENDED to the redirection URL

☐ EWC/AP IP & port
 Replace EWC IP with EWC FQDN:

☐ AP name & serial number

☐ AP Ethernet MAC

☐ AP Location

☐ Associated BSSID

☐ VNS Name

☐ SSID

☐ Station's MAC address

☐ Currently assigned role

☐ Containment VLAN (if any) of assigned role

☐ Timestamp

☐ Signature

Note: When configuring Redirect to External Captive Portal on the AP:

- The IP/Port field is enabled by default and Replace with EWC FQDN is not supported.

Redirect From External Captive Portal

Use HTTPS for User Connections: ☒

Send Successful Login To: ▼

*

Figure 110: Configuring Firewall Friendly External Captive Portal

ExtremeWireless offers a scalable external captive portal (ECP) solution on the AP that can be managed locally or through a Cloud solution, in addition to the controller based ECP. The following table illustrates the WLAN redirection configuration options for the AP and the controller. Each setting is identified as mandatory or optional for redirection on the AP or on the controller. For more information about configuring ECP on an AP, see [Configuring a Captive Portal on an AP](#) on page 222.

Table 61: Firewall Friendly External Captive Portal

Field/Button	Description	Redirection at the AP	Redirection at the Controller
Redirect to External Captive Portal			
Identity	Type the name common to both the controller and the external Web server if you want to encrypt the information passed between the controller and the external Web server.	Mandatory Required for signing the redirected URL. If you do not configure the Identity, the redirector on the AP drops the traffic.	Optional
Shared Secret	Type the password common to both the controller and the external Web server if you want to encrypt the information passed between the controller and the external Web server.	Mandatory Required for signing the redirected URL. If you do not configure the Shared Secret, the redirector on the AP drops the traffic.	Optional
Redirection URL	Type the URL to which the wireless device user will be directed to after authentication. Note: Ensure the request does not exceed the browser character limit. Older browsers limit requests to 255 characters. Newer browsers allow up to 2048 characters. The Redirection URL does not support IPv6.	Mandatory	Mandatory
EWC IP and Port	IP address and Port number	Mandatory By default, this option is enabled. The IP address and port of the AP are always URL parameters. A deployment will have multiple APs. The IP address and port communicate to the External Captive Portal through the client, identifying which AP is redirecting the client.	Optional This option is not required when the deployment includes only one controller. However, we recommend enabling this option when the deployment includes multiple controllers.

Table 61: Firewall Friendly External Captive Portal (continued)

Field/Button	Description	Redirection at the AP	Redirection at the Controller
Replace EWC IP with EWC FQDN	Use controller's Fully-Qualified Domain Name instead of IP address.	Not supported	Optional You can enable this setting if the deployment uses a single controller.
AP Name and Serial Number	Name and Serial Number of AP	N/A AP has this information locally.	Optional
AP Ethernet MAC	MAC address of the AP	N/A AP has this information locally.	Optional
AP Location	Text string used to describe physical AP location.	Optional	Optional
Associated BSSID	Associated BSSID of AP	N/A AP has this information locally.	Optional
VNS Name	Virtualized Network Service Name	Optional For non-site deployments, the VNS Name is not available on the AP. Therefore, it must be included in the mobile user associated response or as part of the mobile user update requirement from the controller.	Optional
SSID	Service Set Identifier	N/A AP has this information locally.	Optional
Station MAC Address	Media Access Control Address	N/A AP has this information locally.	Optional
Currently Assigned Role		Optional For non-site deployments, the Assigned Role is not available on the AP. Therefore, it must be included in the mobile user associated response or as part of the mobile user update requirement from the controller.	Optional

Table 61: Firewall Friendly External Captive Portal (continued)

Field/Button	Description	Redirection at the AP	Redirection at the Controller
Containment <i>VLAN</i> of Assigned Role		Optional For non-site deployments, the Assigned Role is not available on the AP. Therefore, it must be included in the mobile user associated response or as part of the mobile user update requirement from the controller.	Optional
Timestamp	Timestamp (in UTC)	Mandatory The timestamp (in UTC) is always included, because it prevents replay attacks of a recorded redirected URL. The AP must have access to UTC time, which is provided by the controller.	Optional
Signature		Optional Signature is included when full authentication is employed. If configuring a RADIUS authentication server, clear the Signature check box. The Signature option is the flag that indicates how authentication is achieved.	Optional
Redirect From External Captive Portal			
Use HTTPS for Users Connections	Select this option to use HTTPS instead of HTTP. The default state will be set for HTTPS. This applies to both new WLAN Services and WLAN Services that existed prior to upgrading to V9.15 and later.	Optional The AP presents a self-signed certificate that triggers a warning page in most browsers. The AP does <i>not</i> support installing signed certificates from a trusted certificate authority.	Optional

Table 61: Firewall Friendly External Captive Portal (continued)

Field/Button	Description	Redirection at the AP	Redirection at the Controller
Send Successful Login to:	Select the IP address of the external Web server, and then enter the port of the controller.	Mandatory The session management page can contain a link to the original URL that was served when it was redirected. The session management page includes a button to terminate the user's session. The only way the client can come directly to this page is by replaying the redirection URL from the External Captive Portal within the grace period measured by the timestamp.	Optional The session management page <i>does</i> include a button to terminate the user's session.
View Sample	Displays an example format of the redirection URL that the controller/AP expects to receive (indirectly) from the ECP. If the WLAN Service is part of a VNS or has a default topology, then the server portion of the URL contains the IP address of the controller/AP. The query string is populated with realistic but fictional data. This information is provided to assist in developing the ECP program.		

Configuring Internal Captive Portal and Guest Splash

Configure

Message Configuration [Configure](#)

Communication Options

Use HTTPS for User Connections: ☒

Replace Gateway IP with FQDN:

Send Successful Login To: original destination ▼
 *

☒ Manual Settings ☐ Use Zip File

The page width is 790 pixels. Extra content will be cropped out. Please make sure that the height is also reasonable.

[Launch Captive Portal Editor](#)

*Note: Only supported for VNSs where the topology doesn't change.
 Certificates can be added on the Topologies page under the Certificates tab.

Figure 111: Captive Portal Page Configuration Page for Internal and Guest Splash Modes

Table 62: Captive Portal Page Configuration Page for Internal and Guest Splash Modes - Fields and Buttons

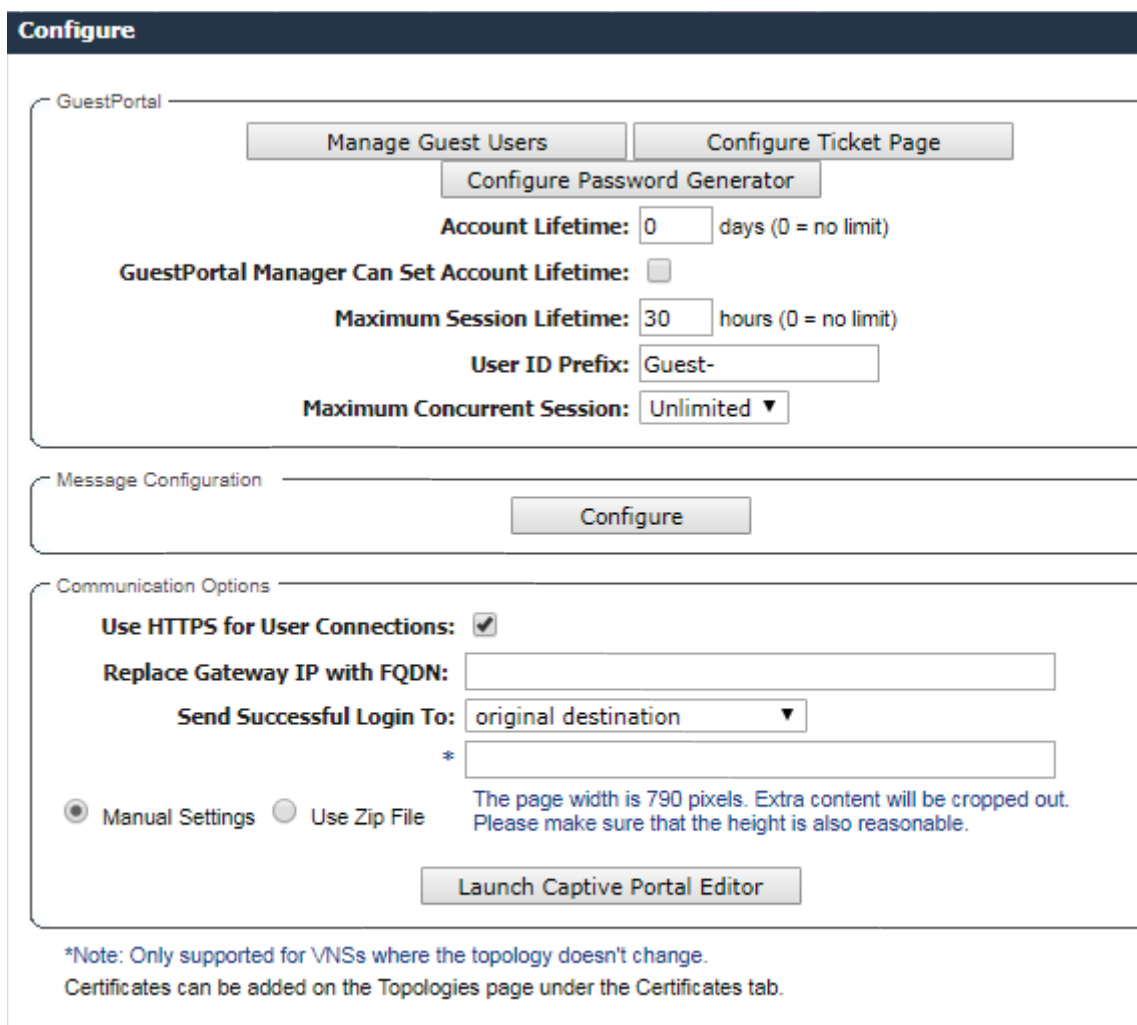
Field/Button	Description
Message Configuration	
Configure	Click to configure error messages that may display on the internal captive portal page. The Message Configuration page displays. See Configuring Error Messages on page 363.
Communication Options	
Use HTTPS for Users Connections	Select this option to use HTTPS instead of HTTP. The default state will be set for HTTPS. This applies to both new WLAN Services and WLAN Services that existed prior to upgrading to V9.01 and later.
Replace Gateway IP with FDQN	Type the appropriate name if a Fully Qualified Domain Name (FQDN) is used as the gateway address.
Send Successful Login To:	
Manual Settings	Select this option if you want to manually define the elements on the Captive Portal page. When you select this option, you enable the Launch Captive Portal Editor button.

Table 62: Captive Portal Page Configuration Page for Internal and Guest Splash Modes - Fields and Buttons (continued)

Field/Button	Description
Use Zip File	Select this option to upload a zip file that contains custom Captive Portal content. The zip file you upload must have a flat structure — it cannot contain any sub-directories. The contents of the zip must adhere to the following file formats: - Content to be used in the captive portal login page must be in a file named login.htm - Content to be used in the captive portal index page must be in a file named index.htm. - The number of graphics and the size of the graphics is unlimited, and can be either .gif, .jpg, or .png.
Upload Zip File	Click the Browse button and navigate to the zip file to use for setting up the captive portal.
View Sample Login Page	Click to view the sample login page for this captive portal.
View Sample Index Page	Click to view the sample index page for this captive portal.
Download	Click to download the specified zip file. The File Download page displays.
Launch Captive Portal Editor	Click to launch the Captive Portal Editor. Using the Captive Portal Editor, you can configure the elements on the captive portal page. This button becomes available when you select the Manual Setting radio button.
Close	Click to save your changes and close this page.
Cancel	Click to discard your configuration changes and close this page.

Configuring Guest Portal**Note**

You must configure a Guest Portal before **Guest Portal** appears as a Captive Portal option. Only one WLAN Service can be configured for Guest Portal on a VNS.



Configure

GuestPortal

Manage Guest Users Configure Ticket Page

Configure Password Generator

Account Lifetime: 0 days (0 = no limit)

GuestPortal Manager Can Set Account Lifetime: ☐

Maximum Session Lifetime: 30 hours (0 = no limit)

User ID Prefix: Guest-

Maximum Concurrent Session: Unlimited ▼

Message Configuration

Configure

Communication Options

Use HTTPS for User Connections: ☒

Replace Gateway IP with FQDN:

Send Successful Login To: original destination ▼

*

☒ Manual Settings ☐ Use Zip File

The page width is 790 pixels. Extra content will be cropped out. Please make sure that the height is also reasonable.

Launch Captive Portal Editor

*Note: Only supported for VNSs where the topology doesn't change.
Certificates can be added on the Topologies page under the Certificates tab.

Figure 112: Captive Portal Page for Guest Portal Mode

Table 63: Configure Internal Captive Portal Page - Fields and Buttons

Field/Button	Description
Guest Portal	this section becomes available only when configuring a Guest Portal.
Manage Guest Users	Click to add and configure guest user accounts. The Manage Guest Users page displays. For information about adding and managing guest users, see Working with GuestPortal Administration on page 690.
Configure Ticket Page	Click to configure the guest portal ticket. The Configure ticket page displays. For information about how to configure and activate guest portal ticket pages, see Working with GuestPortal Administration on page 690.
Configure Password Generator	Click to configure the guest password. The Configure Password Generator page displays. For information about how to configure and activate guest passwords, see Configuring Guest Password Patterns on page 701.

Table 63: Configure Internal Captive Portal Page - Fields and Buttons (continued)

Field/Button	Description
Account Lifetime	Type the account lifetime, in days, for the guest account. A value of 0 specifies no limit to the account lifetime.
Guest Admin Can Set Account Lifetime	Select to enable the guest administrator to set the amount of time for which this account will be active.
Maximum Session Lifetime	Type the maximum session lifetime, in hours, for the guest account. The default 0 value does not limit a session lifetime. The session lifetime is the allowed cumulative total in hours spent on the network during the account lifetime.
User ID Prefix	Type a prefix that will be added to all guest account user IDs. The default is Guest.
Minimum Password Length	Type a minimum password length that will be applied to all guest accounts.
Message Configuration	
Configure	Click to configure error messages that may display on the internal captive portal page. The Message Configuration page displays. See Configuring Error Messages on page 363.
Communication Options	
Use HTTPS for Users Connections	Select this option to use HTTPS instead of HTTP. The default state will be set for HTTPS. This applies to both new WLAN Services and WLAN Services that existed prior to upgrading to V9.01 and later.
Replace Gateway IP with FQDN	Type the appropriate name if a Fully Qualified Domain Name (FQDN) is used as the gateway address.
Send Successful Login To:	
Manual Settings	Select this option if you want to manually define the elements on the Captive Portal page. When you select this option, you enable the Launch Captive Portal Editor button.
Use Zip File	Select this option to upload a zip file that contains custom Captive Portal content. The zip file you upload must have a flat structure — it cannot contain any sub-directories. The contents of the zip must adhere to the following file formats: - Content to be used in the captive portal login page must be in a file named login.htm - Content to be used in the captive portal index page must be in a file named index.htm. - The number of graphics and the size of the graphics is unlimited, and can be either .gif, .jpg, or .png.
Upload Zip File	Click the Browse button and navigate to the zip file to use for setting up the captive portal.
View Sample Login Page	Click to view the sample login page for this captive portal.
View Sample Index Page	Click to view the sample index page for this captive portal.
Download	Click to download the specified zip file. The File Download page displays.

Table 63: Configure Internal Captive Portal Page - Fields and Buttons (continued)

Field/Button	Description
Launch Captive Portal Editor	Click to launch the Captive Portal Editor. Using the Captive Portal Editor, you can configure the elements on the captive portal page. This button becomes available when you select the Manual Setting radio button.
Close	Click to save your changes and close this page.
Cancel	Click to discard your configuration changes and close this page.

Configuring Error Messages

You can configure informational and error messages that a user may encounter when trying to access a captive portal.

To configure error and informational messages:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **WLAN Services** pane, then click the WLAN Service. The **WLAN Services** configuration page is displayed.
- 3 Click the **Auth & Acct** tab.
- 4 In the **Authentication Mode** drop-down list, select a Captive Portal option.
- 5 Click **Configure**.

The **Captive Portal Configuration** page displays.

- 6 In the Message Configuration section, click the **Configure** button.

The Message Configuration page displays.

Configure

Message Configuration

Invalid:	Empty id / password not
Success:	Success
Access Fail:	Userid or password incorrect. Please try again.
Fail:	A problem has occurred while trying to validate your userid & password.
Timeout:	A problem has occurred while trying to validate your userid & password.
RADIUS shared security key fail:	A problem has occurred while trying to validate your userid & password.
RADIUS internal error:	A problem has occurred while trying to validate your userid & password.
Max RADIUS login fail:	Too many users trying to
Max concurrent session fail:	Login rejected because
Invalid Login parameters:	Userid or password
General failure:	A problem has occurred while trying to validate your userid & password.
Invalid third party parameters:	Invalid third party
Authentication in progress fail:	Authentication is in

For information about the Message Configuration fields, see [Understanding the Message Configuration Page](#) on page 364.

Understanding the Message Configuration Page

Table 64: Message Configuration Page - Fields and Buttons

Field/Button	Description
Invalid	Enter a message indicating that the user entered an invalid username or password combination.
Success	Enter a message to indicate when a user successfully logs in.
Access Fail	Enter an error message that indicates the a user login was unsuccessful.
Fail	Enter a message indicating an internal error.
Timeout	Enter an error message indicating that the user authentication timed out.
RADIUS shared secret security key fail	Enter an error message indicating that RADIUS shared secret failed.
RADIUS internal error	Enter an error message indicating an internal RADIUS client error
Max RADIUS login fail	Enter a message that indicates that the maximum number of simultaneous captive portal logins have been reached.

Table 64: Message Configuration Page - Fields and Buttons (continued)

Field/Button	Description
Invalid Login parameters	Enter a message indicating that the user entered an invalid username or password combination.
General failure	Enter a message indicating that a general failure has occurred.
Invalid third party parameters	Enter an error message indicating that one or more parameters passed from the external captive portal server to the controller is either invalid or missing.
Authentication in progress fail	Enter a message indicating that the user credentials were not authenticated.
Topology Change	Enter an error message indicating that the topology failed.
Close	Click to save your changes and close this page.
Cancel	Click to discard your configuration changes and close this page.

Using the Captive Portal Editor

The Captive Portal Editor enables you to configure the look and feel of a captive portal page.

To configure the editor:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand **WLAN Services**, then select the WLAN Service. The **WLAN Services** configuration page displays.
- 3 Click the **Auth & Acct** tab. The **Auth & Accounting** page displays.
- 4 In the **Authentication Mode** drop-down list, select a Captive Portal option.
- 5 Click **Configure**. The **Captive Portal Configuration** page displays.
- 6 In the Communications Options section, select **Manual Settings** and then click **Launch Captive Portal Editor**. For more information see [Table 65](#) on page 367.



Note

The Captive Portal Editor page supports only one administrator editing a captive portal page at one time.



Caution

In order for Captive Portal authentication to be successful, all the URLs referenced in the Captive Portal setup must also be specifically identified and allowed in the non-authenticated filter. For more information, see [Policy Rules](#) on page 288.



Caution

If you use logos or graphics, ensure that the graphics or logos are appropriately sized. Large graphics or logos may force the login section out of view.

Understanding the Captive Portal Editor

Table 65: Captive Portal Editor - Fields and Buttons

Field/Button	Description
Login Page tab	Click to view and configure the elements that will display on the Captive Portal login page. By default, widgets for a Login username and Password, as well as an Accept button are configured by default. You can accept or change these widgets using the Captive Portal Editor widget management tools in the right-hand panel. Using the Captive Portal Editor widget management tools in the right-hand pane on this page you can: • configure the background colors and forms • add graphics • add an external cascading style sheet (.css) • VSA attributes
Index Page Tab	Click to view and configure the elements that will display on the Captive Portal Index page. Using the Captive Portal Editor widget management tools in the right-hand pane on this page you can: • configure the background colors and forms • add graphics • add a Logoff button. The Logoff button launches a pop-up logoff page, allowing users to control their logoff. • add a Status Check button The Status check button launches a pop-up window, which allows users to monitor session statistics such as system usage and time left in a session. • add an external cascading style sheet (.css)
Topology Change Tab	Click to view and configure the elements that will display on the Captive Portal Topology change page. By default, a login confirmation and informational message, as well as a Close button, are preconfigured. You can accept or change these elements using the Captive Portal Editor widget management tools in the right-hand panel. Using the Captive Portal Editor widget management tools in the right-hand pane on this page you can: • configure the background colors and forms • add graphics • add an external cascading style sheet (.css)
Design Management	
Cached	Select to cache most of the widgets from the design to rescue the amount of time it takes a captive portal page to load.
Preview	Select to view the way the configured widgets will display to a user.
Close	Select to close this page without saving the configuration.
Save	Select to save the configuration changes.
Save&Close	Select to save the configuration changes and close this window.
Data Management	
Import	Select and click Browse to navigate to the directory and filename of the a configuration that you want to import. Click OK to import the configuration.

Table 65: Captive Portal Editor - Fields and Buttons (continued)

Field/Button	Description
Export	Select to save this configuration and enter the name of the file you want to save it in. Click the Browse button to navigate to a directory where you want to store the configuration file. Click OK to save the configuration.
Widget Management	Use the fields in this section to configure the widgets.
Graphics	Click to locate and upload a graphic. The graphic becomes available in the Show Images section of the Property Editor.
Background	Click to configure the background color of the page
External CSS	Click to identify a cascading style sheet (.css) that will determine the page format.
Session Variables	Click to configure the following VSA attributes: • AP Serial • AP Name • VNS Name • SSID • MAC Address The selections influence what URL is returned in either section. For example, wireless users can be identified by which AP or which VNS they are associated with, and can be presented with a Captive Portal Web page that is customized for those identifiers.
Add Widget to Panel	Use the fields in this section to add the configured widgets to the page.
Graphic	Select to add a graphic to the page. Use the Property Editor select a preconfigured graphic, and to determine the size and location of the graphic.
Text	Select to add text to the page. Use the Property Editor to type and format the text, and to determine the location of the text and the conditions under which it displays.
Header	Select to add a Header attribute to the panel. Use the Property Editor to determine the size and position of the Header attribute, the conditions under which it displays, and identify the link and type of Header attribute to include.
Session Variables	Use the Property Editor to determine the size and position of the Header attribute and the conditions under which it displays, select a Display Option, and select a type of VSA.
External HTML	Select to add an external HTML link to the page. Use the Property Editor select a preconfigured graphic, and to determine the size and location of the graphic
Text (Scrollable)	Select to add scrollable text to the page. Use the Property Editor to type and format the text, and to determine the location of the text and the conditions under which it displays.
Footer	Select to add a Footer attribute to the panel. Use the Property Editor to determine the size and position of the Footer attribute, the conditions under which it displays, and identify the link and type of Footer attribute to include.

Defining Priority Level and Service Class

Voice over Internet Protocol (VoIP) using 802.11 wireless local area networks are enabling the integration of internet telephony technology on wireless networks. Various issues including Quality-of-Service (QoS), call control, network capacity, and network architecture are factors in VoIP over 802.11 WLANs.

Wireless voice data requires a constant transmission rate and must be delivered within a time limit. This type of data is called isochronous data. This requirement for isochronous data is in contradiction to the concepts in the 802.11 standard that allow for data packets to wait their turn to avoid data collisions. Regular traffic on a wireless network is an asynchronous process in which data streams are broken up by random intervals.

To reconcile the needs of isochronous data, mechanisms are added to the network that give voice data traffic or another traffic type priority over all other traffic, and allow for continuous transmission of data.

To provide better network traffic flow, the controller provides advanced Quality of Service (QoS) management. These management techniques include:

- WMM (Wi-Fi Multimedia) — Enabled on individual WLAN Services, is a standard that provides multimedia enhancements that improve the user experience for audio, video, and voice applications. WMM is part of the 802.11e standard for QoS.
- IP ToS (Type of Service) or DSCP (Diffserv Codepoint) — The ToS/DSCP field in the IP header of a frame is used to indicate the priority and Quality of Service for each frame. Adaptive QoS ensures correct priority handling of client payload packets tunneled between the controller and AP by copying the IP ToS/DSCP setting from client packet to the header of the encapsulating tunnel packet.

Defining the Service Class

Service class is determined by the combination of the following operations:

- The class of treatment given to a packet. For example, queuing or per hop behavior (PHB).
- The packet marking of the output packets (user traffic and/or transport).

Table 66: Service Classes

Service class name (number)	Priority level
Network Control (7)	7 (highest priority)
Premium (Voice) (6)	6
Platinum (video) (5)	5
Gold (4)	4
Silver (3)	3
Bronze (2)	2
Best Effort (1)	1
Background (0)	0 (lowest priority)

The service class is equivalent to the 802.1D UP (user priority).

Table 67: Relationship Between Service Class and 802.1D UP

SC name	SC Value	802.1d UP	AC	Queue
Network Control	7	7	VO	VO or TVO
Premium (voice)	6	6	VO	VO or TVO
Platinum (video)	5	5	VI	VI
Gold	4	4	VI	VI
Silver	3	3	BE	BE
Bronze	2	0	BE	BE
Best Effort	1	2	BK	BK
Background	0	1	BK	BK

Configuring the Priority Override

Priority override allows you to define and force the traffic to a desired priority level. Priority override can be used with any combination, as displayed in [Table 67](#) on page 370. You can configure the service class and the DSCP values.

When **Priority Override** is enabled, the configured service class overrides the queue selection in the inbound and outbound directions, the 802.1P UP for the WLAN tagged Ethernet packets, and the UP for the wireless QoS packets (WMM or 802.11e) according to the mapping in [Table 66](#) on page 369. If **Priority Override** is enabled and the VNS is not locally bridged, the configured DSCP value is used to tag the IP header of the encapsulated packets. The AP does not override the DSCP in the IP header of the user packet.

Configuring QoS Modes

You can enable the following QoS modes for a WLAN Service:

- **WMM** — If enabled, the AP will accept WMM client associations, and will classify and prioritize the outbound traffic for all WMM clients. WMM clients will also classify and prioritize the inbound traffic.
- **802.11e** — If enabled, the AP will accept WMM client associations, and will classify and prioritize the outbound traffic for all 802.11e clients. The 802.11e clients will also classify and prioritize the inbound traffic.
- **Turbo Voice** — If any of the above QoS modes are enabled, the Turbo Voice mode is available. If enabled, all the out traffic that is classified to the Voice (VO) AC and belongs to that VNS is transmitted by the AP via a queue called Turbo Voice (TVO) instead of the normal Voice (VO) queue. The TVO queue is tailored in terms of contention parameters and number of retries to maximize voice quality and voice capacity.
- **U-APSD**— Unscheduled Automatic Power Save Delivery feature works in conjunction with WMM and/or 802.11e, and it is automatically disabled if both WMM and 802.11e are disabled.

The APs are capable of supporting five queues. The queues are implemented per radio; for example, five queues per radio. The queues are:

Table 68: Queues

Queue Name	Purpose
AC_VO	Voice
AC_VI	Video
AC_BK	Background
AC_BE	Best Effort
AC_TVO	Turbo Voice

The controller supports the definition of 8 levels of user priority (UP). These priority levels are mapped at the AP to the best appropriate access class. Of the 8 levels of user priority, 6 are considered low priority levels and 2 are considered high priority levels.

WMM clients have the same 4 AC queues. WMM clients will classify the traffic and use these queues when they are associated with a WMM-enabled AP. WMM clients will behave like non-WMM clients—map all traffic to the Best Effort (BE) queue—when not associated with WMM-enabled AP.

The prioritization of the traffic on the downstream (for example, from wired to wireless) and on the upstream (for example, from wireless to wired) is dictated by the configuration of the WLAN Service and the QoS tagging within the packets, as set by the wireless devices and the host devices on the wired network.

Both Layer 3 tagging (DSCP) and Layer 2 (802.1d) tagging are supported, and the mapping conforms with the WMM specification. If both L2 and L3 priority tags are available, then both are taken into account and the chosen AC is the highest resulting from L2. If only one of the priority tags is present, it is used to select the queue. If none is present, the default queue AC_BE is chosen.

Note



If the wireless packets to be transmitted must include the L2 priority (send to a WMM client from a WMM-enabled AP), the outbound L2 priority is copied from the inbound L2 priority if available, or it is inferred from the L3 priority using the above table if the L2 inbound priority is missing.

Table 69: Traffic Prioritization

VNS type	Packet Source	Packet type	L2	L3
Tunneled	Wired	Untagged	No	Yes
Branch	Wired	VLAN tagged	Yes	Yes
Branch	Wired	Untagged	No	Yes
Branch or Tunneled	Wireless	WMM	Yes	Yes
Branch or Tunneled	Wireless	non-WMM	No	Yes

To configure QoS Role:

- 1 From the top menu, click **VNS**.
- 2 In the left pane expand the **WLAN Services** pane, then click the WLAN Service.

- 3 Click the QoS tab.

The screenshot shows the configuration page for the WLAN service named 'guest_portal'. At the top, there is a navigation bar with tabs: Logs, Reports, Controller, AP, VNS, WIPS, and Help. The 'VNS' tab is currently selected. Below the navigation bar, the page title is 'WLAN: guest_portal' with a 'Logout' link to the right. The main content area has four sub-tabs: WLAN Services, Privacy, Auth & Acct, and QoS. The 'QoS' tab is selected. Under the 'Wireless QoS' section, the following options are listed:

- ☒ WMM
- ☐ 802.11e
- ☐ Turbo Voice
- ☐ U-APSD

 Under the 'Admission Control' section, the following options are listed:

- ☐ Use Global Admission Control for Voice (VO)
- ☐ Use Global Admission Control for Video (VI)
- ☐ Use Global Admission Control for Best Effort (BE)
- ☐ Use Global Admission Control for Background (BK)

 A note below these options states: '* Global admission controls are configured through Global Settings'. On the right side of the QoS tab, there is a section for 'Flexible Client Access' with a checkbox that is currently unchecked. Below this checkbox, there are three lines of explanatory text:

- * Flexible Client Access may not work if Global Admission Controls for Voice and Video (Advanced QoS settings) are enabled.
- * Enabling Flexible Client Access will cause the AP to reboot.
- * applicable for AP37xx

Figure 113: Configuring QoS

Table 70: WLAN Services QoS Tab - Fields and Buttons

Field/Button	Description
Wireless QoS	From the Wireless QoS list, do the following: WMM — Select to enable the AP to accept WMM client associations, and classify and prioritize the outbound traffic for all WMM clients. Note that WMM clients will also classify and prioritize the inbound traffic. WMM is part of the 802.11e standard for QoS. If selected, the Turbo Voice and Enable U-APSD options are displayed. 802.11e — Select to enable the AP to accept WMM client associations, and classify and prioritize the outbound traffic for all 802.11e clients. The 802.11e clients will also classify and prioritize the inbound traffic. If selected, the Turbo Voice and the Enable U-APSD options are displayed: Turbo Voice — Select to enable all out traffic that is classified to the Voice (VO) AC and belongs to that VNS to be transmitted by the AP via a queue called Turbo Voice (TVQ) instead of the normal Voice (VO) queue. When Turbo Voice is enabled together with WMM or 802.11e, the WMM and/or 802.11e clients in that VNS are instructed by the AP to transmit all traffic classified to VO AC with special contention parameters tailored to maximize voice performance and capacity. Enable U-APSD — Select to enable the Unscheduled Automatic Power Save Delivery (U-APSD) feature. This feature can be used by mobile devices to efficiently sustain one or more real-time streams while being in power-save mode. This feature works in conjunction with WMM and/or 802.11e, and it is automatically disabled if both WMM and 802.11e are disabled.
Admission Control	From the Admission Control list, do the following: Use Global Admission Control for Voice (VO) - Select to enable admission control for Voice. With admission control, clients are forced to request admission to use the high priority access categories in both inbound and outbound directions. Admission control protects admitted traffic against new bandwidth demands. For more information, see VNS Global Settings on page 392. Use Global Admission Control for Video (VI) - This feature is only available if admission control is enabled for Voice. With admission control, clients are forced to request admission to use the high priority access categories in both inbound and outbound directions. Admission control protects admitted traffic against new bandwidth demands. Select to provide distinct thresholds for VI (video). For more information, see VNS Global Settings on page 392. Use Global Admission Control for Best Effort (BE) - If the client does not support admission control for the access category that requires admission control, the traffic category will be downgraded to lower access category that does not have Mandatory Admission control. For example, if admission control is required for video, and client does not support admission control for video, traffic will be downgraded to Best Effort (BE).

Table 70: WLAN Services QoS Tab - Fields and Buttons (continued)

Field/Button	Description
	For more information, see VNS Global Settings on page 392. Use Global Admission Control for Background (BK)- This feature is only available if admission control is enabled for Background. With admission control, clients are forced to request admission to use the high priority access categories in both inbound and outbound directions. Admission control protects admitted traffic against new bandwidth demands. For more information, see VNS Global Settings on page 392.
Flexible Client Access	Select the check box to enable flexible client access. Flexible client access levels are set as part of the VNS global settings. Note: TSPEC must be disabled when using Flexible Client Access.
Advanced button	
Priority Processing	
Priority Override	Select this check box to force DSCP and a service class. Note: When Priority Override is enabled, the configured service class forces queue selection in the outbound direction, the 802.1P user priority for the VLAN tagged Ethernet packets and the user priority for the wireless QoS packets (WMM or 802.11e), according to the mapping between service class and user priority. If Priority Override is enabled and the VNS is not locally bridged, the configured DSCP value is used to tag the IP header of the encapsulated packets. The AP does not override the DSCP in the IP header of the user packet.
DSCP	From the drop-down list, click the DSCP value used to tag the IP header of the encapsulated packets. For more information, see Defining the DSCP and Service Classifications on page 375.
Service Class	Select one of the following service classes: • Network control (7) — The highest priority level. • Premium (Voice) (6) • Platinum (5) • Gold (4) • Silver (3) • Bronze (2) • Best Effort (1) • Background (0) — The lowest priority level Note: If you want to assign a service class to each DSCP marking, clear the Priority Override check box and define the DSCP service class priorities in the DSCP classification table.

Table 70: WLAN Services QoS Tab - Fields and Buttons (continued)

Field/Button	Description
Advanced Wireless QoS options (Options are only displayed if the WMM or 802.11e check boxes are selected)	
UL Policer Action	If Use Global Admission Control for Voice (VO) or Use Global Admission Control for Video (VI) is enabled, click the action you want the AP to take when TSPEC violations occurring on the inbound direction are discovered: Do nothing — Click to allow TSPEC violations to continue when they are discovered. Data transmissions will continue and no action is taken against the violating transmissions. Send DELTS to Client — Click to end TSPEC violations when it they are discovered. This action deletes the TSPEC.
DL Policer Action	If Use Global Admission Control for Voice (VO) or Use Global Admission Control for Video (VI) is enabled, click the action you want the AP to take when TSPEC violations occurring on the outbound direction are discovered: Do nothing — Click to allow TSPEC violations to continue when they are discovered. Data transmissions will continue and no action is taken against the violating transmissions. Downgrade — Click to force the transmission's data packets to be downgraded to the next priority when a TSPEC violation is discovered. Drop — Click to force the transmission's data packets to be dropped when a TSPEC violation is discovered.

Defining the DSCP and Service Classifications

To define the DSCP and Service Class classifications:

All 64 DSCP code-points are supported. The IETF defined codes are listed by name and code. Undefined codes are listed by code. The following is the default DSCP service class classification (where SC is Service Class and UP is User Priority):

Table 71: DSCP Code-Points

DSCP	SC/UP	DSCP	SC/UP	DSCP	SC/UP
CS0/DE	2/0	AF11	2/0	AF33	4/4
CS1	0/1	AF12	2/0	AF41	5/5
CS2	1/2	AF13	2/0	AF42	5/5
CS3	3/3	AF21	3/3	AF43	5/5
CS4	4/4	AF22	3/3	EF	6/6
CS5	5/5	AF23	3/3	Others	0/1

Table 71: DSCP Code-Points (continued)

DSCP	SC/UP	DSCP	SC/UP	DSCP	SC/UP
CS6	6/6	AF31	4/4		
CS7	7/7	AF32	4/4		

Configuring Hotspots

Traditionally, using a hotspot presents end users with several challenges, including initial connection issues, security concerns, and connectivity while roaming. The ExtremeWireless solution offers the following features to improve the hotspot end-user experience:

- Pre-association network discovery and selection using the dot11u ANQP protocol, resulting in a seamless initial connection.
- Simplified account registration. Network administrators create accounts easily, and provisioning is achieved without user input.
- Enhanced security, using over the air transmission secured by WPAv2.

Each hotspot WLAN has its own Access Network Query Protocol (ANQP) configuration. The HESSID and ANQP Domain ID are specific to the hotspot WLAN.

With pre-association, a mobile device uses ANQP to perform network discovery. The mobile device's connection manager uses hotspot information, such as the service provider policy and user preferences, to automatically select a hotspot network. A mobile device queries the hotspot for key service provider identification and authentication information and selects a network. The ANQP response is generated using parameters configured by the hotspot operator.

Only one hotspot WLAN can be assigned to an AP and to a specific site configuration. The hotspot WLAN can refer to a single Online Signup (OSU) WLAN, which can be open or encrypted. Network operators define the filter policy during hotspot configuration.

Configuring a New Hotspot

Configure hotspots under the WLAN Services workbench.

To configure a hotspot:

- 1 From the top menu, click **VNS**. Then, in the left pane, select **WLAN Services**. The **WLAN Services** window displays.
- 2 Click **New** to configure a new WLAN service.
- 3 Provide the service Name, Service Type, and SSID.

4 Select the **Hotspot** option. Valid values are:

- **Disabled.** Hotspot functionality is not enabled.
- **Enabled.** Hotspots are enabled for this WLAN and the **Hotspot** tab appears on the WLAN page.

Privacy is set by default to WPA and Mandatory Frame Protection (MFP) is enable.

The authentication method is set to AAA with External Radius Server,. You can configure MBA, if required .

- **OSU.** Allows the definition of Online Sign Up or OSEN WLAN.



Note

Configure the policy and topology assigned to the OSU WLAN to allow access *only* to the OSU server. No access to the internet.



Note

Once you have defined a WLAN service with a hotspot, you cannot disable the hotspot. You can only delete the WLAN service and recreate it.

5 Select the **Hotspot** tab.

The screenshot shows the 'WLAN: hotspot' configuration page. The top navigation bar includes 'Logs', 'Reports', 'Controller', 'AP', 'VNS' (selected), 'WIPS', and 'Help'. Below the navigation bar, the 'WLAN: hotspot' title is followed by tabs: 'WLAN Services', 'Privacy', 'Auth & Acct', 'QoS', and 'Hotspot' (selected). The main configuration area contains the following fields:

- HESSID:** 00:0C:29:AE:74:77
- Access Network:** Chargeable public network (dropdown menu)
- DGAF Disabled:** ☒

Below these fields are four sub-tabs: 'Hotspot Identification' (selected), 'SP Identification', 'Network Characteristics', and 'Online Signup'. Under 'Hotspot Identification', there are fields for 'Domain:', 'Venue info:' (with two dropdown menus, both set to 'Unspecified'), and a table for venue details:

Language	Operator Name	Venue Name

On the right side of the table, there are '+' and '-' buttons for adding or removing rows.

Figure 114: Hotspot Configuration

Table 72: WLAN Services Hotspot Tab - Fields and Buttons

Field/Button	Description
HESSID	One SSID can be used across multiple WLANs (BSS), so the HESSID helps a client identify when the BSSID belongs to a homogenous BSS with identical configuration. Beacon with same {HESSID, SSID} pair belong to same WLAN. The {HESSID, SSID} pair must be unique for each WLAN. By default, the HESSID is set to the MAC address of the controller Ethernet port. Hotspots can have the same HESSID as long as the SSID is unique. If opting to configure the HESSID manually, we recommend using an AP BSSID as the HESSID. Note: In a mobility domain, manually configure the HESSID to a unique value, differentiating it from the value used in the controller's WLAN.
Access Network	Identifies the type of network. Valid values are: • Private network. An enterprise network with user accounts. • Private network with guest access. An enterprise network providing guest access. • Chargeable public network. (Default) Open to anyone but access requires payment. • Free public network. Open network, free of charge but may still require acceptance of terms of use (and may involve OSU servers with captive portal).
DGAF Disabled	Downstream Group-Address Forwarding Disabled. By default this option is checked. When checked, the AP is not forwarding downstream group-addressed frames.

- 6 From the **Hotspot Identification** tab, configure the following parameters:

Domain. FQDN specified by the user. Default value is empty string.

This is a list of one or more domain names of the entity operating the hotspot network. Domain names in the domain name list may contain sub-domains. If the service provider's FQDN is not in the domain name list but is in the realm list, then a mobile device that chooses that service provider is considered to be roaming.

Venue Info. Describes the venue. Select from a list of predefined values:

- 1 Select a description of the venue group in the first field.
- 2 Select a value from the second field.



Note

The second field is not populated with values until after you select a value from the first field.

Default value is **Unspecified**.

- 7 You can configure up to four languages for each venue. Click the plus sign.

The screenshot shows a configuration window with four tabs: **Hotspot Identification**, **SP Identification**, **Network Characteristics**, and **Online Signup**. The **Hotspot Identification** tab is active. It contains a **Domain:** text field, a **Venue info:** section with two dropdown menus (currently showing 'Assembly' and 'Stadium'), and a table with three columns: **Language**, **Operator Name**, and **Venue Name**. The table has one row with a checked checkbox, 'English', 'John Doe', and 'Capital City Civic Center'. To the right of the table are a plus sign (+) button and a minus sign (-) button.

Figure 115: Hotspot Identification Tab

A configuration dialog displays.

The screenshot shows a dialog box titled **Operator Name and Venue Name Configuration**. It contains three fields: **Language:** with a dropdown menu showing '-', **Operator Name:** with a text input field, and **Venue Name:** with a text input field. At the bottom are **OK** and **Cancel** buttons.

Figure 116: Configuring Operator and Venue

Select a language preference, specifying the venue name and operator name, and click **OK**.

Describe the venue where the hotspot is located. If there are multiple hotspot APs in one venue, use the same venue name. However, when one hotspot covers multiple venues, you can list multiple venues here even though they may share a single service set identifier (SSID).

List venue names in multiple languages. The mobile device selects the language that is used to display information to the user. The mobile device can obtain venue name information through an ANQP query, which can help the user when they are manually selecting a hotspot. The mobile device implementation determines if the venue name information is displayed.

- 8 To remove a language row from the Venue list, select the check box in the list row and click the minus sign.

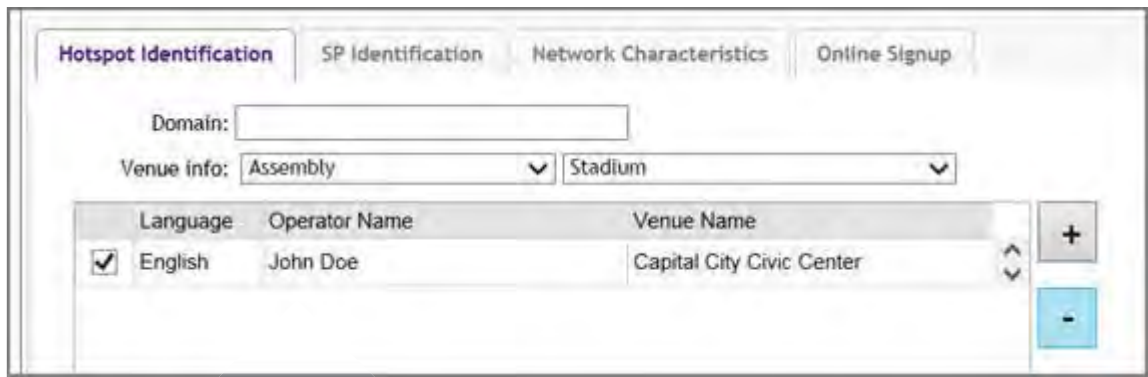


Figure 117: Removing a Venue

- 9 To edit a list row, click the list row. In the resulting dialog, modify the values and click **OK**.
- 10 Click **Save** to save the configuration.

SP Identification Tab

The hotspot SP identification tab displays hotspot properties for service provider identification and authentication.

To configure SP Identification for the hotspot:

- 1 Configure a WLAN Services Hotspot. For more information, see [Configuring a New Hotspot](#) on page 376.
- 2 Select the **SP Identification** tab.

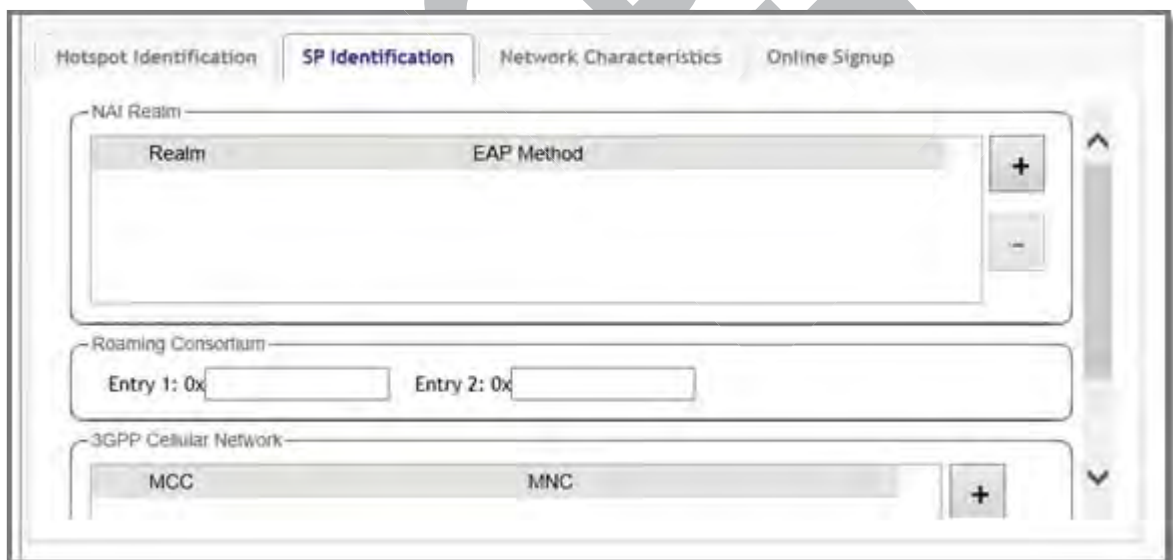


Figure 118: Service Provider Identification

3 Configure the following parameters:

NAI Realm. The the NAI (Network Access Identification) Realms list is a FQDN of the service provider. This is a list of realms that can be successfully authenticated. Each realm may have up to 8 supported EAP methods. Click the plus sign to add realms and select the EAP Method. Then, click **OK**.

Configure an NAI Realm list for each hotspot as follows:

- Add all realms that can authenticate a mobile device's logon credentials or certificate credentials, including the realms of all roaming partners that are accessible from the hotspot AP. Include the realm of the home SP.
- Add a realm for the PLMN ID. This is the cellular network identity based on public land mobile network (PLMN) information. See [Figure 120](#) on page 382.
- You can configure the EAP method list to support devices that do not know the EAP methods that are being used by a given service provider.

If the device has been provisioned with the home service provider, the device does not need to use the EAP methods in the NAI Realm List. The mobile device knows the EAP method required to authenticate against its home service provider and automatically uses it.



Note

Keep your DNS server records up to date so that mobile devices can resolve the server domain names (FQDN).

Realm Configuration

Realm:

EAP Methods:

☐ EAP-TTLS PAP	☐ EAP-TTLS CHAP
☐ EAP-TTLS MSCHAP	☐ EAP-TTLS MSCHAPv2
☐ EAP-TLS SIM	☐ EAP-SIM SIM
☐ EAP-AKA USIM	☐ EAP-AKA' USIM

OK **Cancel**

Figure 119: Realm Configuration

Mobile devices with a SIM or USIM credential, can obtain a realm from the hotspot NAI Realm list. While 3GPP credentials are usually used to access a hotspot, a targeted NAI home query is an efficient alternative approach. The device's connection manager compares the realm information in the list to the information that is stored on the device. The connection manager uses the mobile

device's preconfigured user preferences and policy to make a decision between a hotspot AP or a non-hotspot AP, if both are available.

Roaming Consortium. To configure authentication of mobile devices to the members of a roaming consortium, or to a particular SP that has a roaming consortium, add the appropriate IEEE-assigned Organizational Identifier (OI) here. Specify two identifiers unique to the organization that are part of the MAC address.

Use roaming consortium authentication when you do not know all the authenticated realms. Using identifiers unique to the organization in the beacon is a battery efficient roaming method because there are no ANQP queries needed.

3GPP Cellular Network. This is a list of cellular network IDs in the form of mobile country code, mobile network code (MCC, MNC). This list establishes whether an AP has a roaming arrangement with the 3GPP service providers. Click the plus sign to add mobile country code, mobile network code (MCC, MNC) values. Then, click **OK**.

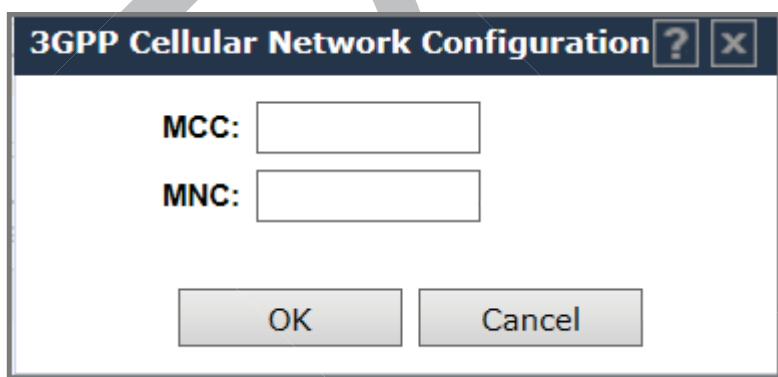


Figure 120: 3GPP Cellular Network Configuration

- 4 Click **Save** to save the configuration.

Network Characteristics Tab

The hotspot Network Characteristics tab displays network parameters for the hotspot.

To configure Network Characteristics for the hotspot:

- 1 Configure a WLAN Services Hotspot. For more information, see [Configuring a New Hotspot](#) on page 376.

- 2 Select the **Network Characteristics** tab.

Figure 121: Configuring Network Characteristics

- 3 Configure the following parameters:

IP Address Type Availability. The mobile device uses the IP Address Type Availability information to make network selection decisions. Select the level of restriction for each network type. Levels of restriction range from **Public Address Available** to **Port Restricted and Double NATed Private Address Available**.

WLAN Metrics. Enter the values for maximum Uplink and Downlink speed and load parameters for the WLAN service.

The mobile device uses information from the WAN Metrics configured here to make network selection decisions. The mobile device can determine if necessary throughput is available from the hotspot before connecting. If the mobile device receives indication that the basic service set (BSS) is at capacity, the device will not associate with that AP.

Connection Capability. The mobile device uses connection capability information to make network selection decisions by determining which services are blocked or supported at the hotspot. Configure up to 16 ports.

- To add a protocol, click the plus sign. Specify the protocol, the port number, and the status associated with the protocol. Valid Status values include: Closed, Open, or Unknown.



Note

Make an effort to configure all ports and do not rely on the Unknown value.

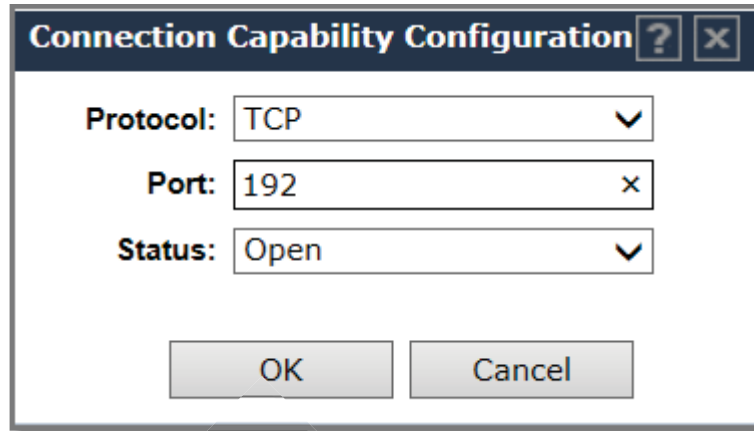


Figure 122: Configuring Connection Capability

- To remove a port from the Connection Capability list, select the check box in the list row and click the minus sign.

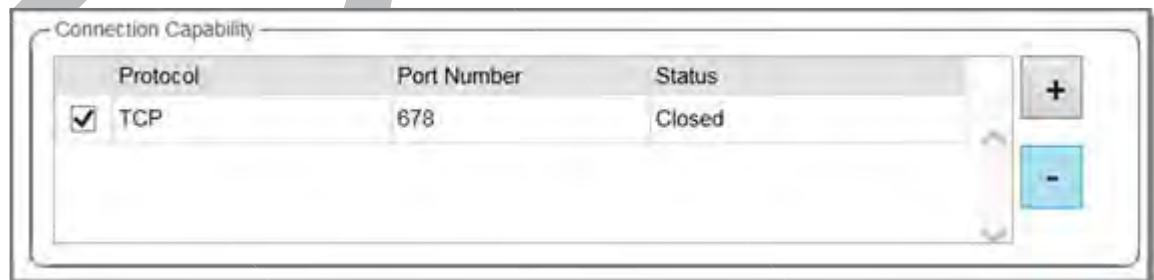


Figure 123: Removing a Connection Port

- To edit a port, click the list row. In the resulting dialog, modify the values and click **OK**.
- 4 Click **Save**.

Online Signup Tab

The hotspot **Online Signup** tab displays hotspot properties for Online Signup users. Online Signup allows users who are not part of the provider network to manually connect to the hotspot. It also allows for added security for users who want to connect anonymously.

To configure Online Signup for the hotspot:

- 1 Configure a WLAN Services Hotspot. For more information, see [Configuring a New Hotspot](#) on page 376.

- 2 Select the **Online Signup** tab.

Figure 124: Configuring Online Signup

- 3 Configure the following parameters:

Network Authentication Type. Possible values for network authentication are:

- Acceptance of terms and conditions. Redirection is accomplished after user accepts Terms and Conditions.
- Http/Https redirection. Redirect Http or Https automatically.
- Online enrollment supported. Authentication supports online enrollment.
- DNS redirection. DNS redirection serves a web page other than what the end user had requested.

OSU WLAN. This is the address of the Online Signup WLAN. When you created the hotspot, you specified OSU in step 1 above. The OSU WLAN can be either Open or Encrypted (OSEN).

Server Provider Setting. This is service provider configuration settings.

- To add a provider to the list, click the plus sign and configure the provider settings. For more information, see [Configuring the OSU Service Provider](#) on page 385.
- To remove a provider from the list, select the check box in the list row and click the minus sign.
- To edit provider information, click the list row. In the resulting dialog, modify the values and click **OK**. For more information, see [Configuring the OSU Service Provider](#) on page 385.

- 4 Click **Save** to save the configuration.

Configuring the OSU Service Provider

Hotspot configuration supports Online Signup. This task outlines how to create a list of service providers that support Online Signup.

Take the following steps to configure an Online Signup service provider:

- 1 Configure a WLAN Services Hotspot. For more information, see [Configuring a New Hotspot](#) on page 376.

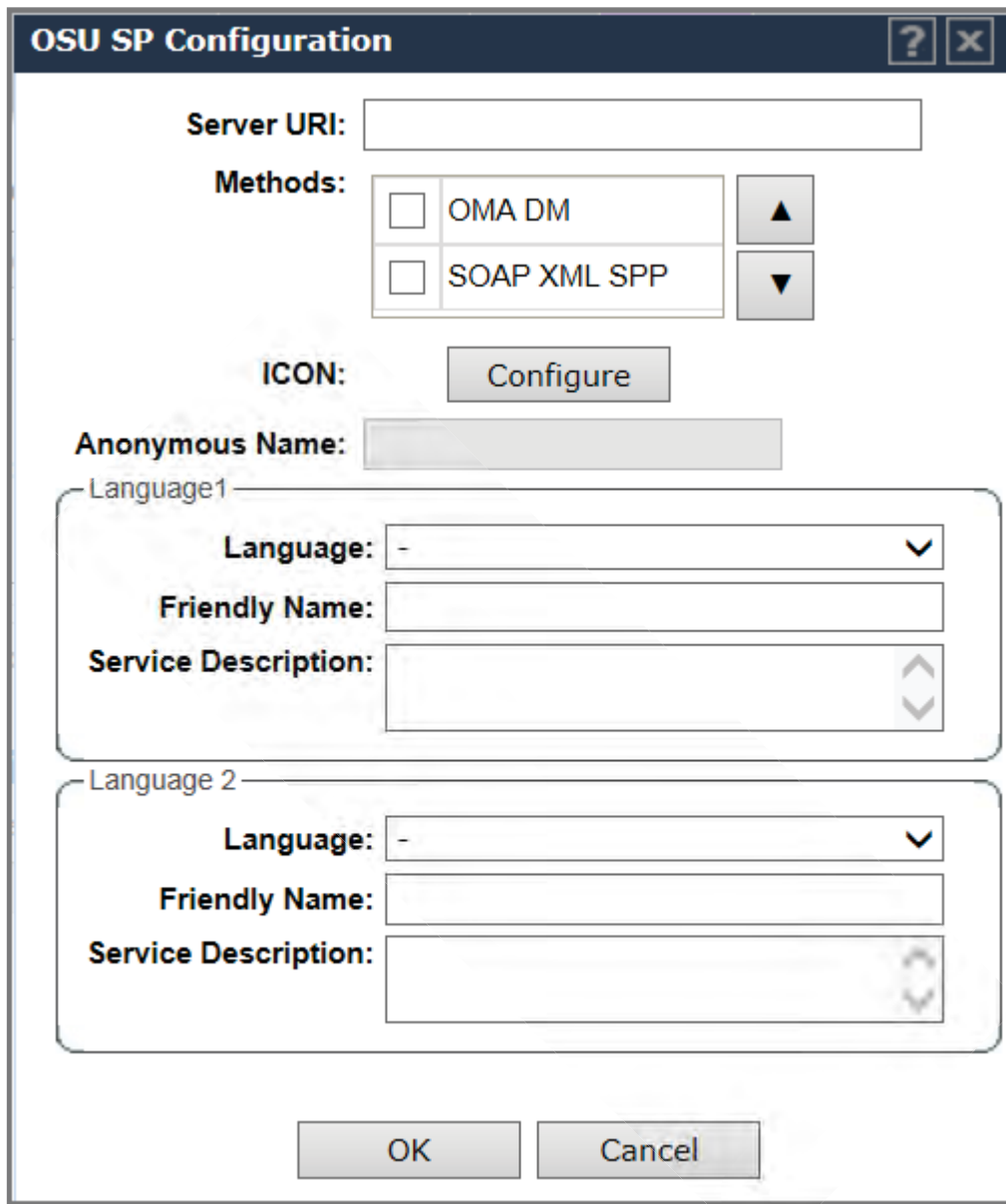
- 2 From the WLAN Services Hotspot tab, select the **Online Signup** tab.

The screenshot shows the 'Online Signup' tab of a configuration window. At the top, there are four tabs: 'Hotspot Identification', 'SP Identification', 'Network Characteristics', and 'Online Signup' (which is selected). Below the tabs, there are two dropdown menus: 'Network Authentication Type' set to 'Online enrollment supported' and 'OSU WLAN' set to 'osu'. A section titled 'Service Provider Setting' contains a table with the following columns: 'Server URI', 'Methods', 'Icon', 'Language', 'Friendly Name', and 'Description'. The table is currently empty. To the right of the table are two buttons, '+' and '-'. At the bottom of the window, there are three buttons: 'New', 'Delete', and 'Save'.

Server URI	Methods	Icon	Language	Friendly Name	Description
------------	---------	------	----------	---------------	-------------

Figure 125: Online Signup Tab

- 3 In the Service Provider Setting pane, select the plus sign.
The OSU SP Configuration dialog appears.



The image shows the 'OSU SP Configuration' dialog box. It has a title bar with a question mark and a close button. The main area contains several fields and controls:

- Server URI:** A text input field.
- Methods:** A section with two checkboxes: 'OMA DM' and 'SOAP XML SPP'. To the right of these checkboxes are two arrow buttons (up and down).
- ICON:** A button labeled 'Configure'.
- Anonymous Name:** A text input field.
- Language1:** A section containing:
 - Language:** A dropdown menu with a '-' symbol and a downward arrow.
 - Friendly Name:** A text input field.
 - Service Description:** A text area with up and down arrow buttons on the right.
- Language 2:** A section containing:
 - Language:** A dropdown menu with a '-' symbol and a downward arrow.
 - Friendly Name:** A text input field.
 - Service Description:** A text area with up and down arrow buttons on the right.
- Buttons:** At the bottom, there are 'OK' and 'Cancel' buttons.

Figure 126: Configuring the OSU Service Provider

- 4 Configure the following parameters:

Server URI. The OSU server URI.

Methods. OSU Method is the preferred list of encoding methods that the OSU server supports in order of priority. Select the connection method used by the provider.

Icon. Click **Configure** to add or remove an icon associated with Online Signup. For more information, see [Configuring an OSU Icon](#) on page 388.

Anonymous Name. Configure a name that anonymous users can use to access the network.

Language. Configure the Language, Friendly Name, and Service Description for the Online Signup user interface.

- 5 Click **OK** to save the OSU SP configuration.

Configuring an OSU Icon

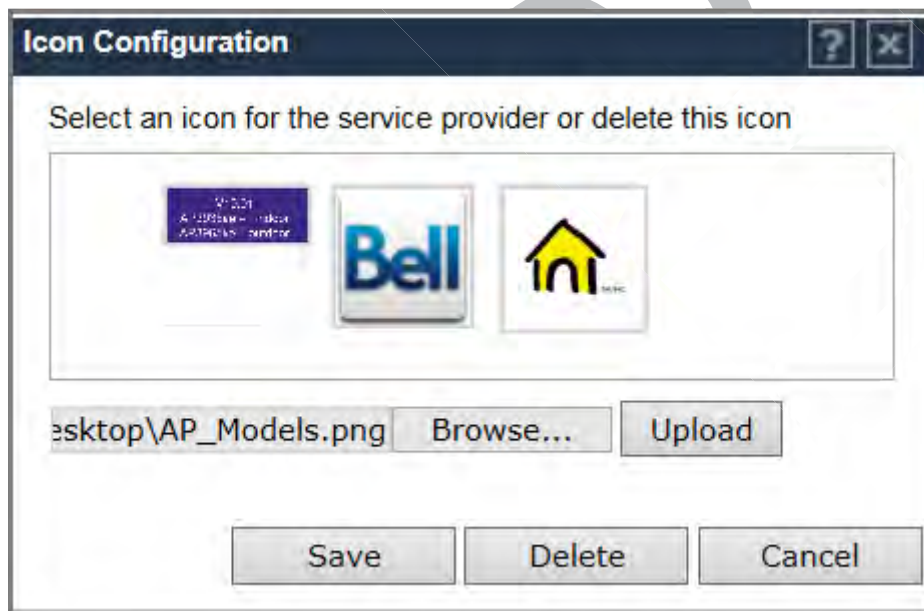
This task outlines how to add, change, or remove icons to a list of icons that are associated with Online Signup. The icon list contains the metadata for the available icon files. The metadata defines the image size, language, type, and file name. The mobile device determines which icon in the list best fits the display and downloads the appropriate file. The list can be blank.

The NAI realm is used in cases where the OSU ESS (OSEN) SSID is configured. This allows the device to authenticate to the OSU OSEN SSID for access to the OSU server.

To add an icon:

- 1 From the **OSU SP Configuration** dialog, click **Configure**.

The **Icon Configuration** dialog appears.



- 2 Click **Browse** to navigate to the icon file. Then, click **Open** and **Upload**.

The icon file is added to the **Icon Configuration** dialog.

- 3 Select the icon and click **Save**.

To delete an icon:

- 1 Open the **Icon Configuration** dialog.
- 2 Select the icon and click **Delete**.
- 3 Click **Save**.

Draft

8 Configuring a VNS

Configuring a VNS

VNS Global Settings

Methods for Configuring a VNS

Manually Creating a VNS

Creating a VNS Using the Wizard

Enabling and Disabling a VNS

Renaming a VNS

Deleting a VNS

Configuring a VNS

Setting up a VNS defines a binding between a default role specified for wireless users and an associated *WLAN (Wireless Local Area Network)* Service set, as shown in [Figure 127](#).

There are conceptually hierarchical dependencies on the configuration elements of a VNS. However, the provisioning framework is flexible enough that you may select an existing dependent element or create one on the fly. Therefore, each element can be provisioned independently (WLAN services, Topologies, and Roles). For service activation, all the pieces will need to be in place, or defined during VNS configuration.

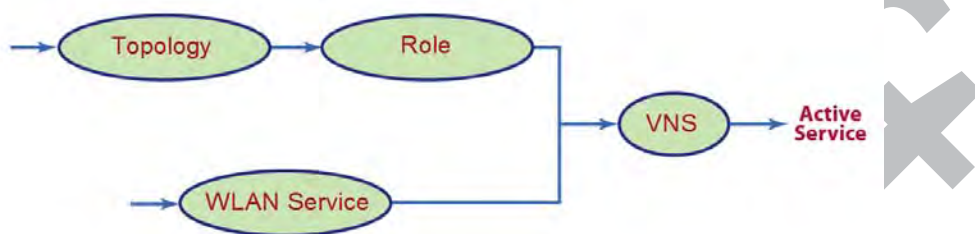


Figure 127: VNS Configuration Flow

You can use the VNS Creation Wizard to guide you through the necessary steps to create a virtual network service (and the necessary subcomponents during the process). The end result is a fully resolved set of elements and an active service.

The recommended order of configuration events is:

- 1 Before you begin, draft out the type of services the system is expected to provide — wireless services, encryption types, infrastructure mapping (*VLAN (Virtual LAN)s*), and connectivity points (switch ports). Switch port VLAN configuration/trunks must match the controller's.
- 2 Set up basic controller services such as NTP, Routing, DNS, and RADIUS Servers, using one of the following methods:

- Run the **Basic Configuration Wizard**, or
 - Manually define the necessary infrastructure components such as RADIUS Servers. RADIUS Servers are defined via the **VNS > Global > Authentication**.
- 3 Define Topologies. Topologies represent the controller's points of network attachment. Therefore, VLANs and port assignments need to be coordinated with the corresponding switch ports.
 - 4 Define Roles. Roles are typically bound to Topologies. Role application assigns user traffic to the corresponding network point of attachment.
 - Roles define mobile user access rights by filtering.
 - Policies reference the mobile user's traffic rate control profiles.
 - 5 Define the WLAN Service.
 - Define SSID and privacy settings for the wireless link.
 - Select the set of APs and radios on which the service is present.
 - Configure the method of credential authentication for wireless users (None, Internal CP, External CP, Guest Portal, 802.1x[EAP]).
 - 6 Create a **VNS** that binds the **WLAN Service** to the **Role** that will be used for default assignment upon user network attachment.

The VNS configuration page in turn allows for in-place creation of any dependencies it may require. For example:

- Create a new WLAN Service.
- Create a new Role.
 - Create a new Topology.
 - Create a new Class of Service.

Controller Defaults

The default shipping controller configuration does not include any pre-configured [WLAN Services](#), VNSs, or Roles.

The ExtremeWireless system does ship with Topology entities representing each of its physical interfaces, plus an admin interface.

The controller system ships with a Topology entity for an admin interface. Topology entities representing the controller physical interfaces must be set manually or using the basic installation wizard.

There are, however, global default settings corresponding to:

- A Default Topology named "Bridged @ AP Untagged"
- An "Unlimited" Rate Control Profile
- A Filter Definition of "Deny all"

These entities are simply placeholders for Role completion, in case roles are incompletely defined. For example, a Role may be defined as "no-change" for Topology assignment.

If an incomplete Role is assigned as the default for a VNS / WLAN Service (wireless port), the incomplete Role needs to be fully qualified, at which point the missing values are picked from the Default Global Role definitions, and the resulting role is applied as default.



Note

You can edit the attributes of the Default Global Role (under **VNS > Global** tab). For example, change the topology, apply more permissive filter sets, or use a more restrictive Rate Control profile).

It is possible to define a Default Global Role to refer to a specific Topology (for example, Topology_VLAN). Then configure every other Role's topology as "No-change." This configuration defines Topology_VLAN as the default assignment. All user traffic, regardless of the role assignment (applying different access rights, different rate controls) will be carried through the same VLAN.

VNS Global Settings

Before defining a specific VNS, define the global settings that apply to all VNS definitions. These global settings include:

- Authentication
 - Configuring RADIUS servers on the enterprise network. The defined servers are displayed as available choices when you set up the authentication mechanism for each WLAN Service.
 - Configuring the MAC format.
 - Configuring RFC 3580 (ACCESS -ACCEPT) RADIUS attributes for the selected server. A Role Map Table maps each VLAN ID to a Role ID.
- DAS (Dynamic Authorization Service)
 - Configuring Dynamic Authorization Service (DAS) support. DAS helps secure your network by providing the ability to disconnect a mobile device from your network.
- Wireless QoS, comprising Admission Control Thresholds and Flexible Client Access Fairness Role.
 - Admission control thresholds protect admitted traffic against overloads, provide distinct thresholds for VO (voice) and VI (video), and distinct thresholds for roaming and new streams.
 - (AP37xx Only) Flexible Client Access provides the ability to adjust media access fairness in five levels between Packet Fairness and Airtime Fairness.
 - **Airtime %** is available for AP38xx and AP39xx access point models that are assigned WLANS configured with Reserved Airtime.
- Bandwidth Control
 - The Bandwidth Control Profiles you define are displayed as available choices in the Rate Profiles menu when you set up CoS (Class of Service) role.
- Default Role

The Global Default Policy specifies:

- A topology to use when a VNS is created using a role that does not specify a topology
- A set of filters

The controller ships from the factory with a default "Global Default Policy" that has the following settings:

- Topology is set to an Bridged at AP untagged topology. This topology will itself be defined in controllers by default.
- Filters - A single “Allow All” filter.

The Global Default Policy is user-configurable. Changes to the Global Default Policy immediately effect all shadow roles created from it, just as if the administrator had made a comparable change directly to the incomplete role.

- Egress Filtering Mode

The global Egress Filtering Mode setting overrides the individual WLAN service Egress Filtering Mode setting.

- Sync Summary

The **Sync Summary** screen provides an overview of the synchronization status of paired controllers. The screen is divided into sections: Virtual Networks, WLAN services, Roles, and Topologies. Each section lists the name of the corresponding configuration object, its synchronization mode, and the status of last synchronization attempt. For more information, see [Using the Sync Summary](#) on page 414.

- NAC Integration

NAC Integration provides a list of NAC servers for use by the controller for passing *DHCP (Dynamic Host Configuration Protocol)* traffic. The NAC server can accept DHCP messages from the controller’s DHCP server and use them to fingerprint devices. For more information, see [Using NAC Integration](#) on page 416.

- Client Auto Login

This features configures how auto login behavior is handled for users with devices that need to authenticate to a captive portal to gain network access. For more information, see [Using Client Login](#) on page 417.

- Topology Group Algorithm

Topology Group Algorithms are used for selecting a member Topology from a Topology Group. The wireless controller will run one of the following algorithms: MAC based, Round Robin, Random Selected, and Lease used. For more information, see [Using Topology Group Algorithm](#) on page 418.

- Netflow/MirrorN

Use Netflow to forward packet information. Integration with ExtremeAnalytics no longer requires Netflow/MirrorN. See [ExtremeAnalytics Support with Enhanced IPFIX Records](#) on page 419 for more information.

- Redirection URL

Configure a list of redirection URLs from the Redirection URL dialog. You can add and delete a URL.



Note

To display the **Redirection URL** option, enable **Rule-based Redirection** under **Filtering Mode**.

Related Links

[Configuring Airtime Fairness: Reservation Mode](#) on page 406

Defining RADIUS Servers and MAC Address Format

The Authentication global settings include configuring RADIUS servers, the MAC format to be used, the SERVICE-TYPE attribute in the client ACCESS-REQUEST messages, and how long a notice web page displays if a topology change occurs during authentication. The notice Web page indicates that authentication was successful and that the user must restart the browser to gain access to the network.

Defining RADIUS Servers for VNS Global Settings

To define RADIUS servers for VNS global settings:

- 1 From the top menu, click **VNS**.
- 2 In the left pane, click **Global** > **Authentication**.
- 3 Select **Strict Mode** to force the top three Radius servers in priority order for each WLAN where applicable. Clearing this check box, allows individual Radius change per WLAN.

RADIUS Servers RFC 3580 (ACCESS-ACCEPT) Options

☐ Strict Mode

	Server	Default	Retries	Timeouts	Ports	Priority					
	Alias	Hostname/IP	Protocol	Auth	Acct	Auth	Acct	Auth	Acct	Auth	Acct
☐	kubuntu-1	192.168.0.92	PAP	3	3	5	5	1812	1813	8	8
☐	nac-1	192.168.0.115	PAP	3	3	15	10	1812	1813	9	9
☐	opensuse-	192.168.0.90	PAP	3	3	5	5	1812	1813	14	14
☐	RADIUS_	192.168.0.115	PAP	3	3	15	5	1812	1813	11	11
☐	radius_tes	192.168.10.10	PAP	3	3	5	5	1812	1813	15	21
☐	win-2008	192.168.0.121	PAP	3	3	5	5	1812	1813	12	12
☐	win2003/6	192.168.0.113	PAP	3	3	15	5	1812	1813	13	13

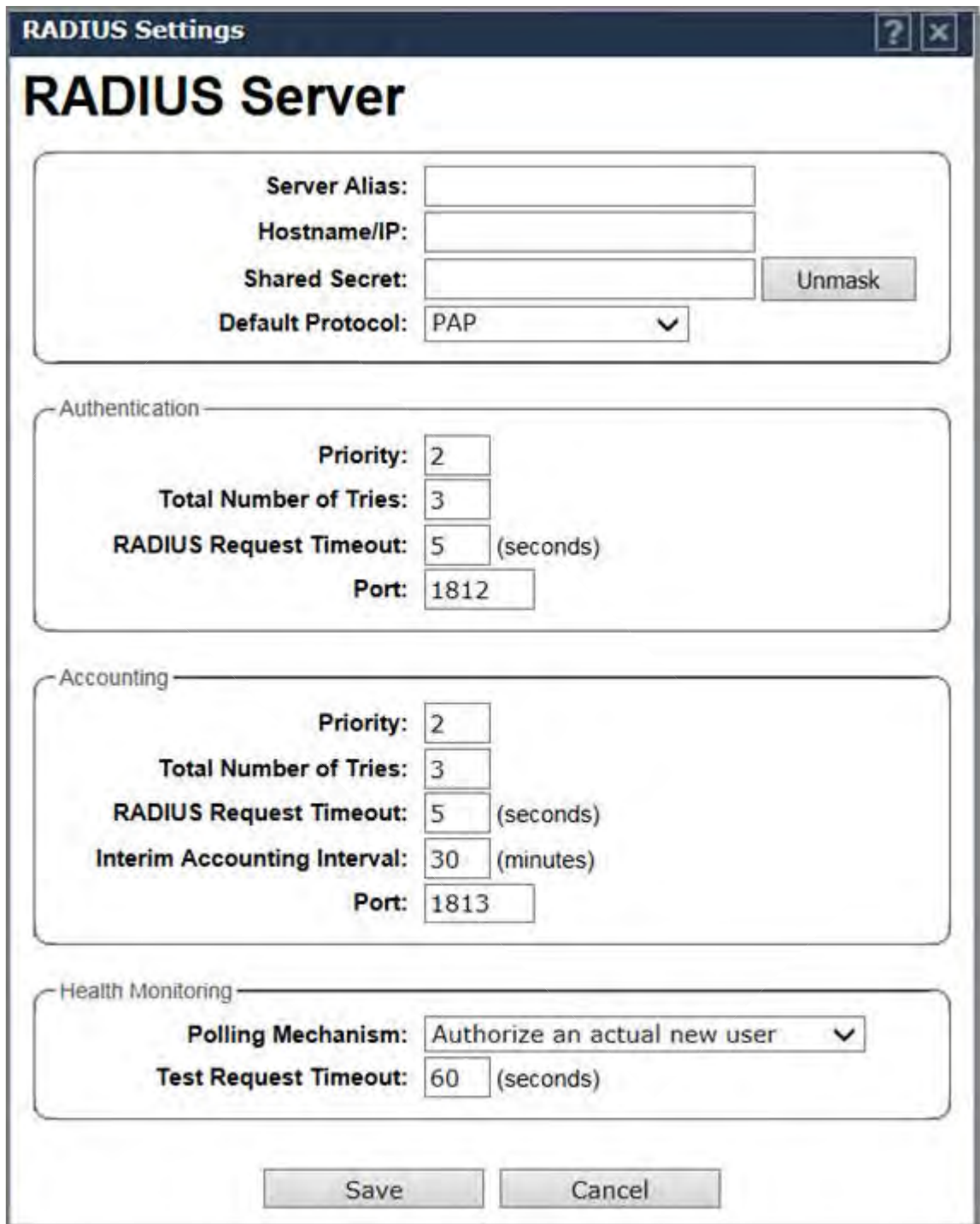
* RADIUS servers which are currently associated with WLAN Service(s) cannot be removed

MAC Address

MAC Address Format: XX-XX-XX-XX-XX-XX ▼ (for MAC-Based authentication only)

Figure 128: Global Authentication Settings

- 4 To define a new RADIUS server available on the network, click **New**. The **RADIUS Settings** dialog displays.



The image shows a screenshot of the 'RADIUS Settings' dialog box. The title bar reads 'RADIUS Settings' with a question mark and a close button. The main title is 'RADIUS Server'. The dialog is divided into several sections: 1. General settings: 'Server Alias' (text field), 'Hostname/IP' (text field), 'Shared Secret' (text field with an 'Unmask' button), and 'Default Protocol' (dropdown menu showing 'PAP'). 2. Authentication section: 'Priority' (2), 'Total Number of Tries' (3), 'RADIUS Request Timeout' (5 seconds), and 'Port' (1812). 3. Accounting section: 'Priority' (2), 'Total Number of Tries' (3), 'RADIUS Request Timeout' (5 seconds), 'Interim Accounting Interval' (30 minutes), and 'Port' (1813). 4. Health Monitoring section: 'Polling Mechanism' (dropdown menu showing 'Authorize an actual new user') and 'Test Request Timeout' (60 seconds). At the bottom are 'Save' and 'Cancel' buttons.

RADIUS Settings

RADIUS Server

Server Alias:

Hostname/IP:

Shared Secret: Unmask

Default Protocol: PAP ▼

Authentication

Priority:

Total Number of Tries:

RADIUS Request Timeout: (seconds)

Port:

Accounting

Priority:

Total Number of Tries:

RADIUS Request Timeout: (seconds)

Interim Accounting Interval: (minutes)

Port:

Health Monitoring

Polling Mechanism: ▼

Test Request Timeout: (seconds)

Save Cancel

Figure 129: RADIUS Server Settings

- 5 In the **Server Alias** field, type a name that you want to assign to the RADIUS server.

Note



You can also type the RADIUS server's IP address in the **Server Alias** box in place of a nickname. The RADIUS server will identify itself by the value typed in the **Server Alias** box in the RADIUS Servers drop down list on the **RADIUS Authentication** tab of the **Login Management** screen (**top menu > Wireless Controller > Login Management**). For more information, see [Configuring the Login Authentication Mode](#) on page 75.

- 6 In the **Hostname/IP** field, type either the RADIUS server's FQDN (fully qualified domain name) or IP address.

Note



If you type the host name in the **Hostname/IP address** box, the controller will send a host name query to the DNS server for host name resolution. The DNS servers must be appropriately configured for resolving the RADIUS servers' host names. For more information, see [Configuring DNS Servers for Resolving Host Names of NTP and RADIUS Servers](#) on page 94.

- 7 In the **Shared Secret** field, type the password that will be used to validate the connection between the controller and the RADIUS server.

To proofread your shared secret key, click Unmask. The password is displayed.

Note



You should always proofread your Shared Secret key to avoid any problems later when the controller attempts to communicate with the RADIUS server.

- 8 If desired, change the **Default Protocol** using the drop down list. Choices are PAP, CHAP, MS-CHAP, or MS-CHAP2.
- 9 If desired, change the pre-defined default values for **Authentication** and **Accounting** operations:
- a Priority — default is 4.
 - b Total number of tries — default is 3.
 - c RADIUS Request timeout — default is 5 seconds.
 - d For Accounting operations, the Interim Accounting Interval — default is 30 minutes. Setting the Interim Accounting Interval value to 0 results in no interims being sent.
 - e Port — default Authentication port is 1812. Default Accounting port is 1813.
- 10 If desired, setup Health Monitoring by selecting a **Polling Mechanism** from the drop-down menu, and enter a **Test Request Timeout** (shown in seconds).
- 11 To save your changes, click **Save**. The new server is displayed in the **RADIUS Servers** list.

Note



The RADIUS server is identified by its Server Alias.

- 12 To edit an existing server, click the row containing the server. The **RADIUS Settings** window displays, containing the server's configuration values.
- 13 To remove a server from the list, select the check box next to the server, and then click **Delete Selected**. You cannot remove a server that is used by any VNS.

Configuring the Global MAC Address Format for Use with the RADIUS Servers

To configure the Global MAC Address Format for use with the RADIUS servers:

- 1 From the top menu, click **VNS**.
- 2 In the left pane, click **Global**, then **Authentication**.
- 3 In the **MAC Address** area, select the **MAC Address Format** from the drop down list.
- 4 Click **Save** to save your changes.

Configuring Advanced RADIUS Servers Settings

- 1 From the top menu, click **VNS**.
- 2 In the left pane, click **Global > Authentication**.
- 3 In the **MAC Address** area, click **Advanced**.

Advanced [?] [X]

☐ Include the Service-Type attribute in Client Access Request messages

☐ Set Service-Type to Login *

* This is incompatible with using RADIUS for administrative access to the controller.

Delay for Client Message for Topology Change seconds

How should multiple RADIUS servers be used?

For authentication: ▼

For accounting: ▼

☒ Use MAC-Based Authentication MAC address format for user authentication and accounting via RADIUS

☒ Override 802.1x authentication Called-Station-Id format with 'XX-XX-XX-XX-XX-XX:SSID'

☒ RADIUS Accounting *

☐ Defer sending the accounting start request until the client's IP address is known.

* Disabling RADIUS accounting overrides the RADIUS accounting settings of individual WLAN Services. Enabling RADIUS accounting activates RADIUS accounting only in WLAN Services specifically configured to perform it.

Close

Figure 130: Advanced RADIUS Server Settings

4 Configure the following parameters:

Table 73: Advanced Radius Settings

Field	Description
Include Service-Type attribute in Client Access Request messages	Select if the client RADIUS Access Request message includes the "Service-Type" attribute. If included, the attribute is set to "Framed" by default.
Set Service Type to Login	If selected, the RADIUS "Service-Type" attribute of the client Access Request is set to "Login" (instead of "Framed"). Note: RADIUS-based controller administrative access also sets the Service-Type attribute to "Login". Therefore, if you enable Service Type Login here, RADIUS-based administrative access is not allowed (and vice versa).
Delay for Client Message for Topology Change	Defines a delay during client authentication when switching from one topology to another. This is relevant for Captive Portal authentication. The delay gives time for the client to be assigned an IP address for the new topology before browser redirection. Set the delay in seconds.
How should multiple RADIUS servers be used?	Select an authentication or accounting option. The selection applies to all <u>WLAN</u> Services and to all sites on the EWC. • Round-Robin. The server is selected on a round-robin basis starting at the top of the list of approved servers. The first server is used until it fails, and that pattern continues down the list. When the last server fails, then the first server is used again. • Primary-Backup. Select a primary failover server to have control over which server provides redundancy. When you select Primary-Backup, the RADIUS server assigned to the site or WLAN Service is the primary for the WLAN Service. All other RADIUS servers assigned to WLAN Service are backups for the primary and continue to be selected in a round-robin approach. For controllers in an availability pair, the Primary and Backup servers must be synchronized (enable "Synchronize System Configuration" in Availability setup) if the WLAN Services are synchronized. If the primary server has failed resulting in a backup server being used for authentication, the controller will periodically send a "Health Check" to the primary server to see if it has recovered. If the primary server has recovered, the controller starts using the primary server for all new authentications. All authentications in progress continue to use the backup server.
Use MAC-Based Authentication MAC address format for user authentication and accounting via RADIUS	Allows the administrator to override the default MAC address colon-separated format (for example 00:11:22:33:44:55) with the Global Authentication MAC Address format for the following attributes: • Calling-Station-Id attribute of the RADIUS packet • Called-Station-Id attribute (if Called-Station-Id is not overridden by Zone name) • AP BSSID Mac in one of the vendor attributes • User-Name attribute. Note: This setting is enabled for new deployments. You must manually enable this setting for upgraded deployments.

Table 73: Advanced Radius Settings (continued)

Field	Description
Override 802.1x Authentication Call-Station-Id format with XX-XX-XX-XX-XX-XX:SSID	Allows the administrator to override the Called-Station-Id attribute format for 802.1x authentication with the format XX-XX-XX-XX-XX-XX:SSID. This setting is disabled by default. When you select this option, the Called-Station-Id conforms to the format specified in RFC 3580 (IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines). If the RADIUS server is processing this attribute, the RADIUS server has to support this format. Note: This setting overrides the setting Use MAC-Based Authentication MAC address format for user authentication and accounting via RADIUS.
Radius Accounting	Enabling RADIUS accounting activates RADIUS accounting only in WLAN Services specifically configured to perform it. Disabling RADIUS accounting overrides the RADIUS accounting settings of individual WLAN Services.
Defer sending the accounting start request until the client's IP address is known	Specify Authentication Behavior of RADIUS servers on Server Failure. If selected, the client RADIUS Accounting Request "start" command is not sent to the RADIUS server until the client IP address is known. By default, this option is not selected and the "start" command is sent once the client is authenticated.

- 5 Click **Close** to close the **Advanced Settings** dialog.
- 6 Click **Save** to save your changes.

Changing the Display Time of the Notice Web Page

You can modify the amount of time that the **Notice** web page displays if a topology change occurs during authentication. Take the following steps:

- 1 From the top menu, click **VNS**.
- 2 In the left pane, click **Global**, then **Authentication**.
- 3 In the **MAC Address** area, click **Advanced**.
- 4 In the **Delay for Client Message for Topology Change** field, specify the number of seconds the web page is displayed to the client when the topology changes as a result of a role change.

The Web page indicates that authentication was successful and that the user must close all browser windows and then restart the browser for access to the network.

Currently this is supported for Internal Captive Portal, Guest Portal, and Guest Splash.

- 5 Click **Close**.
- 6 Click **Save** to save your changes.

Configuring RADIUS Attribute for Hybrid Role Mode

Hybrid Role mode (RFC 3580 Mapping mode) enables the wireless controller to separately assign different roles or topologies depending on a mobile station location. The following are available modes of operation:

- **RADIUS Filter-ID attribute** — Controller uses the topology assigned by the role and ignores the VLAN tunnel ID.
- **RADIUS Tunnel-Private-Group-ID attribute** — Controller selects a role for the station based on the VLAN tunnel ID and ignores the filter ID. When selected, a mapping table maps each VLAN ID to a role.
- **Both RADIUS Filter-ID and Tunnel-Private-Group-ID attribute** — Controller uses both the role identified in the filter ID and the topology associated with the VLAN tunnel ID.

**Note**

The selected mode of operation applies to all WLAN Services on the controller.

Defining RFC 3580 Mapping Mode for VNS Global Settings

To define RFC 3580 for VNS global settings:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 2 In the left pane, click **Global** > **Authentication**.
- 3 Click the **RFC 3580 (ACCESS-ACCEPT) Options** tab.

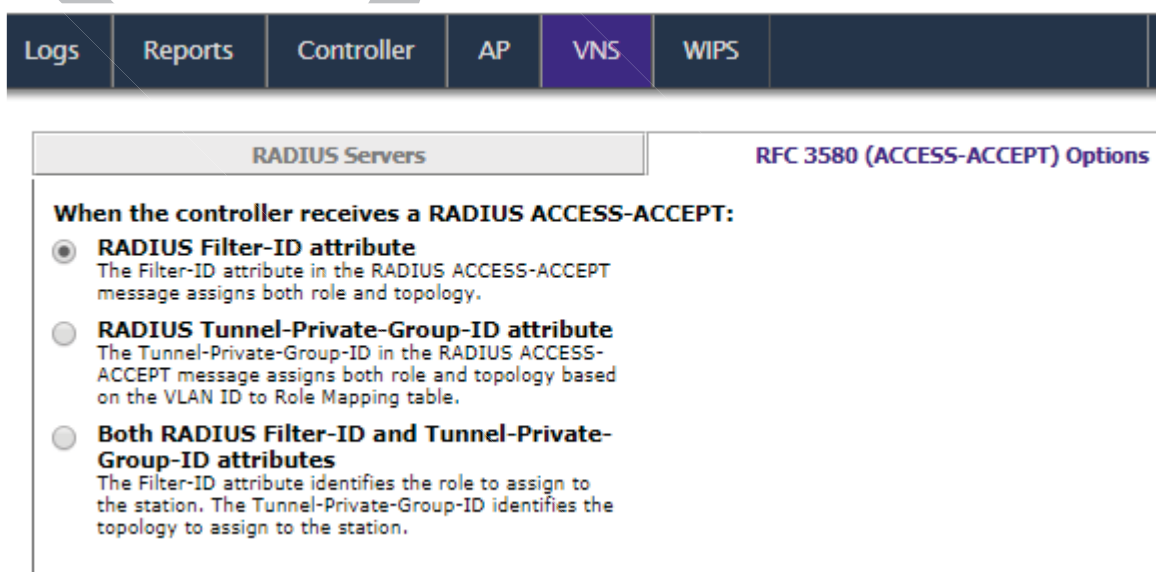
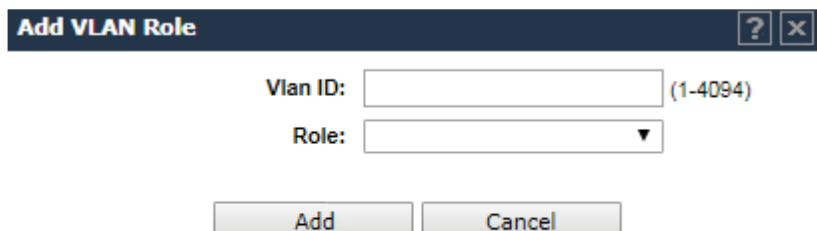


Figure 131: Authentication Settings

- 4 Select **RADIUS Filter - ID attribute** to assign both role and topology when the controller receives a RADIUS ACCESS-ACCEPT message. To save your changes, click **Save**.

- 5 Select **RADIUS Tunnel-Private-Group-ID attribute** to assign both role and topology (based on the VLAN ID to Role Mapping table selection) when the controller receives a RADIUS ACCESS-ACCEPT message.
 - In the VLAN ID Role Mapping table, select an existing VLAN ID and Role.
 - Click **New** to create a new mapping entry. In the **Add VLAN Role** dialog, enter a VLAN ID, and select a Role from the drop-down list.



The image shows a dialog box titled "Add VLAN Role". It has a dark blue header bar with a question mark icon and a close button (X). Below the header, there are two input fields: "Vlan ID:" followed by a text box with a range "(1-4094)" to its right, and "Role:" followed by a dropdown menu with a downward arrow. At the bottom of the dialog, there are two buttons: "Add" and "Cancel".

- Click **Add**.
 - To save your changes, click **Save**.
- 6 Select **Both RADIUS Filter-ID and Tunnel-Private-Group-ID attributes** to identify the role to assign to the station and the topology to assign to the station (based on the VLAN ID to Role Mapping table selection), when the controller receives a RADIUS ACCESS-ACCEPT message.
 - In the VLAN ID Role Mapping table, select an existing VLAN ID and Role.
 - Click **New** to create a new mapping entry. In the **Add VLAN Role** dialog, enter a VLAN ID, and select a Role from the drop-down list.
 - Click **Add**.
 - To save your changes, click **Save**.

Configuring Dynamic Authorization Server Support

DAS helps secure your network by forcing the disconnection of any mobile device from your network. Typically, you would want to disconnect any unwelcome or unauthorized mobile device from your network. The “disconnect message” that is defined in RFC 3576 is enforced by the DAS support. If an unauthorized mobile device is detected on the network, the DAS client sends a disconnect packet, forcing the mobile device off the network. Your DAS client can be an integration with ExtremeControl or another third-party application, including RADIUS applications. For more information, see [NAC Integration with the Wireless WLAN](#) on page 24.

DAS support is available to all physical interfaces of the controller, and by default DAS listens to the standard-specified UDP port 3799.

To Configure Dynamic Authorization Server Support:

- 1 From the top menu, click **VNS**.

- 2 In the left pane, click **Global** > **DAS**.

The screenshot shows the VNS web interface. At the top is a navigation bar with tabs: Home, Logs, Reports, Controller, AP, VNS (selected), and WIPS. On the left is a sidebar menu with categories: New..., Global (selected), Authentication, DAS (selected), Wireless QoS, Bandwidth Control, Default Role, Filtering Mode, NAC Integration, Client Autologin, Topology Group Algorithm, and Netflow/MirrorN. Below these are sections for Sites, Virtual Networks, WLAN Services, Roles, Classes of Service, and Topologies. The main content area is titled 'Dynamic Authorization Server Configuration'. It contains two input fields: 'Port' with the value '3799' and 'Replay Interval' with the value '300' followed by the text 'seconds'.

Figure 132: Global DAS Settings

- 3 In the **Port** box, type the UDP port you want DAS to monitor. By default, DAS is configured for the standard-specified UDP port 3799. It is unlikely this port value needs to be revised.
- 4 In the **Replay Interval** box, type how long you want DAS to ignore repeated identical messages. By default, DAS is configured for 300 seconds.
- This time buffer helps defend against replay network attacks.
- 5 To save your changes, click **Save**.

Defining Wireless QoS Global Settings

Defining the wireless QoS global settings include the following:

- [Configuring QoS Admission Control Thresholds](#) on page 403
- [Configuring QoS Flexible Client Access](#) on page 404

Configuring QoS Admission Control Thresholds

To define Admission Control Thresholds for VNS Global Settings:

- 1 From the top menu, click **VNS**.
- 2 In the left pane, click **Global** > **Wireless QoS**.

The screenshot shows the VNS configuration interface. The top navigation bar includes Home, Logs, Reports, Controller, AP, VNS, WIPS, and Help. The left sidebar shows a tree view with 'Global' selected, containing sub-items like Authentication, DAS, Wireless QoS, Bandwidth Control, Default Role, Filtering Mode, Sync Summary, NAC Integration, Client Autologin, Topology Group Algorithm, Netflow/Mirror, and Redirection URL. The main content area is titled 'Admission Control Thresholds' and contains several settings with dropdown menus:

- Max Voice (VO) BW for roaming streams: 80%
- Max Voice (VO) BW for new streams: 60%
- Max Video (VI) BW for roaming streams: 60%
- Max Video (VI) BW for new streams: 50%
- Max Best Effort (BE) BW for roaming streams: 40%
- Max Best Effort (BE) BW for new streams: 30%
- Max Background (BK) BW for roaming streams: 30%
- Max Background (BK) BW for new streams: 20%

Below these settings is a note: 'Notes: Settings only apply on APs serving QoS-enabled WLAN Service with Admission Control enabled'. The section 'Flexible Client Access' includes a 'WLAN Airtime Reservation Configuration' box with a 'Configure' button and a 'Fairness Policy' dropdown set to '100% Airtime' (applicable for AP37xx). A note below states 'This feature is applicable for AP38xx/AP39xx'. A 'Save' button is located at the bottom right.

Figure 133: Wireless QoS Settings

- 3 In the **Admission Control Thresholds** area, define the thresholds for the following:
 - **Max Voice (VO) BW for roaming streams** — The maximum allowed overall bandwidth on the new AP when a client with an active voice stream roams to a new AP and requests admission for the voice stream.
 - **Max Voice (VO) BW for new streams** — The maximum allowed overall bandwidth on an AP when an already associated client requests admission for a new voice stream.
 - **Max Video (VI) BW for roaming streams** — The maximum allowed overall bandwidth on the new AP when a client with an active video stream roams to a new AP and requests admission for the video stream.
 - **Max Video (VI) BW for new streams** — The maximum allowed overall bandwidth on an AP when an already associated client requests admission for a new video stream.
 - **Max Best Effort (BE) BW for roaming streams** —
 - **Max Best Effort (BE) BW for new streams** —
 - **Max Background (BK) BW for roaming streams** — The maximum allowed background bandwidth on an AP for roaming streams.
 - **Max Background (BK) BW for new streams** — The maximum allowed background bandwidth on an AP for new streams.

These global QoS settings apply to all APs that serve QoS enabled VNSs with admission control.

- 4 To save your changes, click **Save**.

Related Links

[Configuring Airtime Fairness: Reservation Mode](#) on page 406

[Legacy Airtime Fairness: AP37xx](#) on page 407

Configuring QoS Flexible Client Access

This feature allows you to adjust client access role in multiple steps between “packet fairness” and “airtime fairness.”

To define flexible client access for VNS global settings:

- 1 Go to **VNS**.

- 2 In the left pane, click **Global** > **Wireless QoS**.

Global

- Authentication
- DAS
- Wireless QoS**
- Bandwidth Control
- Default Role
- Filtering Mode
- NAC Integration
- Client Autologin
- Topology Group Algorithm
- Netflow/MirrorN

Sites

Virtual Networks

WLAN Services

Roles

Classes of Service

Topologies

Admission Control Thresholds

Max Voice (VO) BW for roaming streams: 80%

Max Voice (VO) BW for new streams: 60%

Max Video (VI) BW for roaming streams: 60%

Max Video (VI) BW for new streams: 40%

Max Best Effort (BE) BW for roaming streams: 40%

Max Best Effort (BE) BW for new streams: 30%

Max Background (BK) BW for roaming streams: 30%

Max Background (BK) BW for new streams: 20%

Note: Settings only apply on APs serving QoS-enabled WLAN Service with Admission Control enabled.

Flexible Client Access

WLAN Airtime Reservation Configuration

Fairness Policy: 100% Airtime

applicable for AP37xx

This feature is applicable for AP38xx/AP39xx.

Configure

Save

Figure 134: Wireless QoS Settings

- 3 Depending on your AP model, do one of the following:
- If configuring an AP37xx, select a role from the **Fairness Policy** drop-down list.

Fairness Policy:

applicable for AP37xx

100% Packet

100% Packet

Mostly Packet

Mixed

Mostly Airtime

100% Airtime



Note

TSPEC must be disabled when using Flexible Client Access.

- If configuring an AP38xx or AP39xx using Reservation Mode, click **Configure**.

The **Airtime Reservation Configuration** dialog displays.

Related Links

[Configuring Airtime Fairness: Reservation Mode](#) on page 406

[Legacy Airtime Fairness: AP37xx](#) on page 407

Configuring Airtime Fairness: Reservation Mode

With Airtime Reservation, reserve a percentage of air time for clients associated to a WLAN. The Airtime Reservation algorithm monitors the down link traffic from all clients. When congestion starts, the reservation algorithm guarantees that these clients have access to the air for the configured amount of time. If clients do not request to transmit, the reserved airtime is consumed by other clients.



Note

Airtime Reservation Mode is supported by AP38xx and AP39xx models. The legacy Flexible Client Access feature continues to support AP37xx models. Configuring Airtime Reservation Mode may cause the AP to reboot.

- 1 Go to **VNS > Global > Wireless QoS**.
- 2 Click **Configure**

The Airtime Reservation Configuration dialog displays.

WLAN Name	Airtime (%)
CNL-422-0-0	- ▼
CNL-422-0-1	- ▼
CNL-422-0-2	- ▼
CNL-422-0-3	- ▼
CNL-422-1-2-wds	- ▼
CNL-422-1-4-wds	- ▼
CNL-422-1-5	- ▼
CNL-422-1-6	- ▼
CNL-422-1-7	- ▼
CNL-422-2-10	- ▼

OK Cancel

Figure 135: Airtime Reservation Configuration Dialog

3 Select the percentage of airtime for each WLAN.

Airtime Reservation configuration rules:

- Four WLAN services associated with a controller can be configured with Airtime Reservation. The total Airtime Reservation of four WLAN services is limited to 80 percent of the total. The remaining 20 percent of the total time is reserved for the other WLAN services.
- If a WLAN service with Airtime Reservation is associated to a radio, the QCA ATF module is turned on, and the AP will restart in order to load the ATF module. The number of clients supported by QCA ATF is 50.
- If the radio does not have a WLAN service with Airtime Reservation associated, the QCA ATF module is turned off.
- When Mesh and WDS is configured, the first WLAN gets 20 percent of the available channel airtime. The other clients on the radio channel get the remaining airtime. This takes co-channel interference into account. If there is 50 percent interference, WLAN1 gets 20 percent of the available 50 percent.

When configured, Airtime Fairness percentage displays on the **WLAN Assignment** page for the AP.

Related Links

[Configuring QoS Flexible Client Access](#) on page 404

[Legacy Airtime Fairness: AP37xx](#) on page 407

Legacy Airtime Fairness: AP37xx

This topic outlines the legacy Airtime Fairness behaviour that is supported by AP37xx. Airtime Fairness Reservation Mode, is supported by AP38xx and AP39xx models.

Legacy Airtime Fairness is described as:

- Packet fairness is the default 802.11 access role. Each WLAN participant gets the same (equal) opportunity to send packets. All WLAN clients will show the same throughput, regardless of their PHY rate.
- Airtime fairness gives each WLAN participant the same (equal) time access. WLAN clients' throughput will be proportional to their PHY rate.



Note

Flexible Client Access may not work if Global Admission Controls for Voice and Video (Advanced QoS settings) are enabled.

Related Links

[Configuring Airtime Fairness: Reservation Mode](#) on page 406

[Configuring QoS Flexible Client Access](#) on page 404

Working with Bandwidth Control Profiles

Bandwidth control limits the amount of bidirectional traffic from a mobile device. A bandwidth control profile provides a generic definition for the limit applied to certain wireless clients' traffic. A bandwidth control profile is assigned on a per role basis. A bandwidth control profile is not applied to multicast traffic.

A bandwidth control profile consists of the following parameters:

- **Profile Name** — Name assigned to a profile
- **Committed Information Rate (CIR)** — Rate at which the network supports data transfer under normal operations. It is measured in kilo bits per second (Kbps).

The bandwidth control profiles you define on the **Global Settings** screen are displayed as available choices in the **Bandwidth Control Profiles** list on the **Classes of Service** screen.

To create a bandwidth control profile:

- 1 From the top menu, click **VNS**.
- 2 In the left pane, click **Global** > **Bandwidth Control**.

Figure 136: Global Bandwidth Control Profiles

- 3 Provide a **Profile Name** for the bandwidth control profile.
- 4 Provide the **Average Rate (CIR)** value for the bandwidth control profile.
- 5 Click **Add Profile**.

The profile is created and displayed in the **Bandwidth Control Profiles** list.

- 6 Create additional bandwidth control profiles, if applicable.
- 7 Click **Save**.

Configuring the Global Default Policy

The controller ships with a Global Default Policy that can be configured. The Global Default Policy specifies:

- A topology to use when a VNS is created using a role that does not specify a topology. The default assigned topology is named Bridged at AP untagged.

- A set of filters.

Configuring the Topology and Rate Profiles

To configure the topology and rate profiles:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 2 In the left pane, click **Global > Default Role**.
- 3 Select the **VLAN & Class of Service** tab.

Figure 137: Default Role Settings

- 4 In the **Default Action** area, select a VLAN using one of the following methods:
 - Select an existing VLAN from the drop-down list.
 - Select an existing VLAN from the drop-down list, then click **Edit**. The **Edit Topology** window displays, showing the current values for the selected topology.
 - Click **New**. The **New Topology** window displays.

Edit or create the selected topology as described in [Configuring a Basic Data Port Topology](#) on page 266.

- 5 Select an Invalid Role Action from the one of the following:
 - Select **Apply VNS Default Role**.
 - Select **Allow All traffic**.
 - Select **Deny All traffic**.
- 6 Click **Save**.

Configuring the Filters

To configure the filters:

- 1 Click the **Policy Rules** tab. The **Rules** tab displays, allowing you to create policy rules that will be applied by the controller when default non-authentication role does not specify filters.

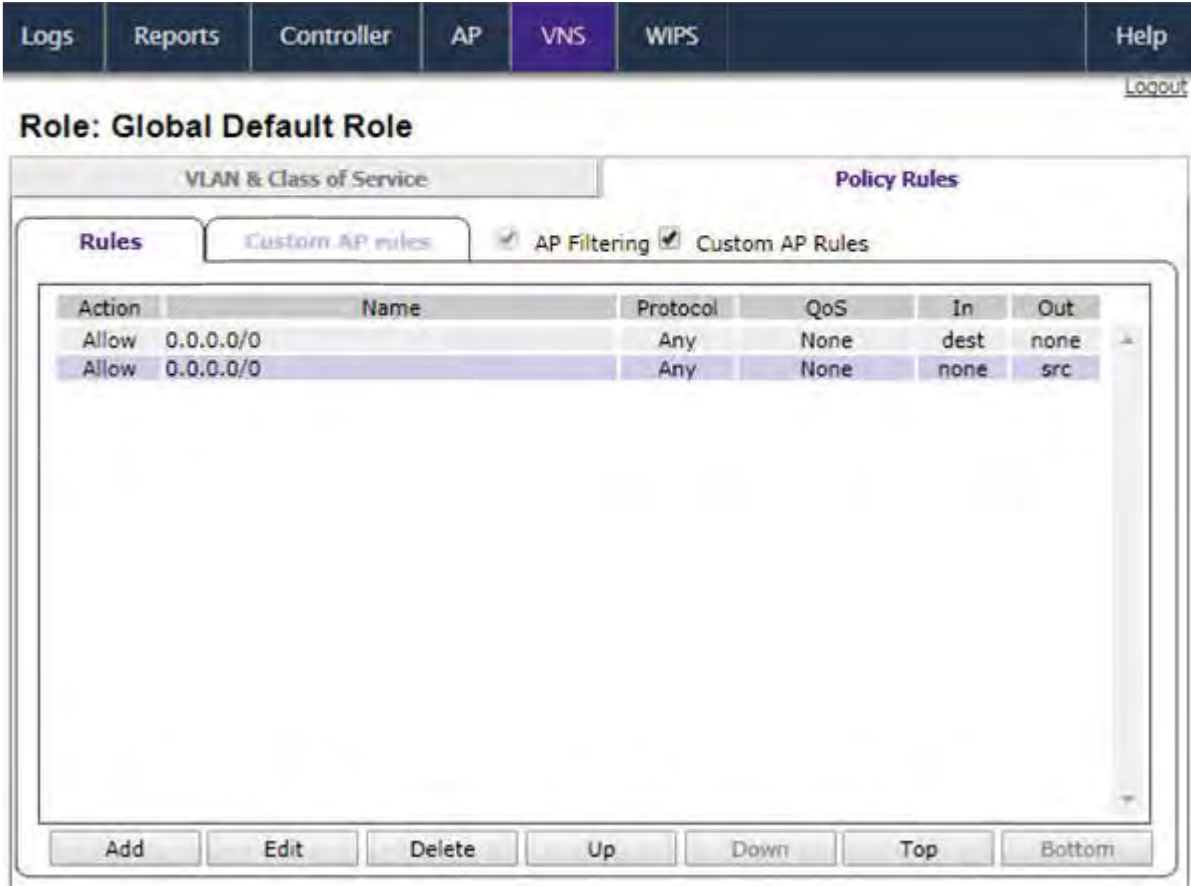


Figure 138: Default Role Settings

- 2 To add a rule, click **Add**.
For more information, see [Policy Rules](#) on page 288.
- 3 To configure custom AP filters, select **AP Filtering** and **Custom AP Rules** then click the **Custom AP rules** tab.
For more information, see [Defining Policy Rules for Wireless APs](#) on page 298.

Related Links

- [Understanding the Filter Rule Definition Dialog](#) on page 302
- [L7 Configuration](#) on page 307

Configuring Egress Filtering Mode

The controller can be configured to support Policy Manager’s Egress Role mode. Egress Role refers to taking the ingress filters assigned to a port, exchanging the source and destination addresses with each other in each role rule and applying the result to the traffic egressing the port.

The ExtremeWireless solution applies egress filtering mode to WLAN services. When egress filtering is enabled, any role that is applied to a station on the WLAN service will have its outbound filters replaced with rules in which the source and destination addresses of the inbound filters are swapped.

The same role can be assigned to stations on WLAN services that have egress filtering mode enabled and on WLAN services that have it disabled.

- For stations that are on WLAN services with egress filtering mode enabled, the roles outbound filters will be replaced by ones derived from the inbound policy rules.
- For stations that are on WLAN services with egress filtering disabled, the outbound filters of the role will be applied as defined. In other words the same role can be applied in two different ways at the same time, based on the egress filter mode settings of the WLAN services it is used with.

The global Egress Filtering Mode setting overrides the individual WLAN service Egress Filtering Mode setting. By default, the global setting is set to **Use WLAN**. In this mode, egress filtering can be enabled for some WLAN services and not others. Set the Egress Filtering Mode setting from the Advanced configuration dialog of each WLAN service.

Changing the global setting does not alter each individual WLAN egress filtering mode setting, although the global setting can override the individual setting. Changing the global setting does not alter the outbound policy rules of each role. Each role's policy rules are stored on the controller as they were entered. Changing the global egress filtering mode flag does, however, affect how a role's rules are interpreted when they are applied.

Rule-Based Redirection

Rule-based redirection requires explicit enablement. For new installations, Rule-based Redirection is enabled by default. For upgrades from releases prior to v10.11, ExtremeWireless preserves the previous captive portal redirection method of triggering redirect off denied HTTP/HTTPS for non-authenticated roles. For more information, see [Rule-Based Redirection](#) on page 289.



Note

The option to disable Rule-based Redirection is available for backward capability only.

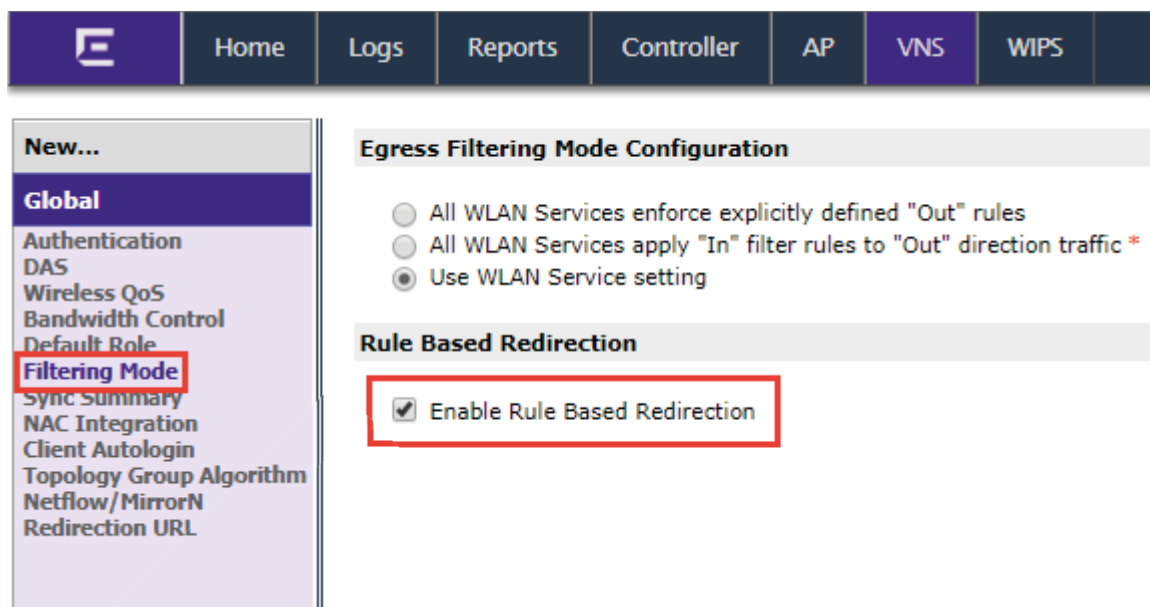


Figure 139: Enabling Rule-based Redirection

Related Links

[Configuring the In/Out Rules for WLAN Services Settings](#) on page 412

[Rule-Based Redirection](#) on page 289

Configuring the In/Out Rules for WLAN Services Settings

To configure the Egress Filtering Mode:

- 1 From the top menu, click **VNS**.
The **Virtual Network Configuration** screen displays.

- 2 In the left pane, click **Global > Filtering Mode**.

The **Egress Filtering Mode Configuration** screen displays.

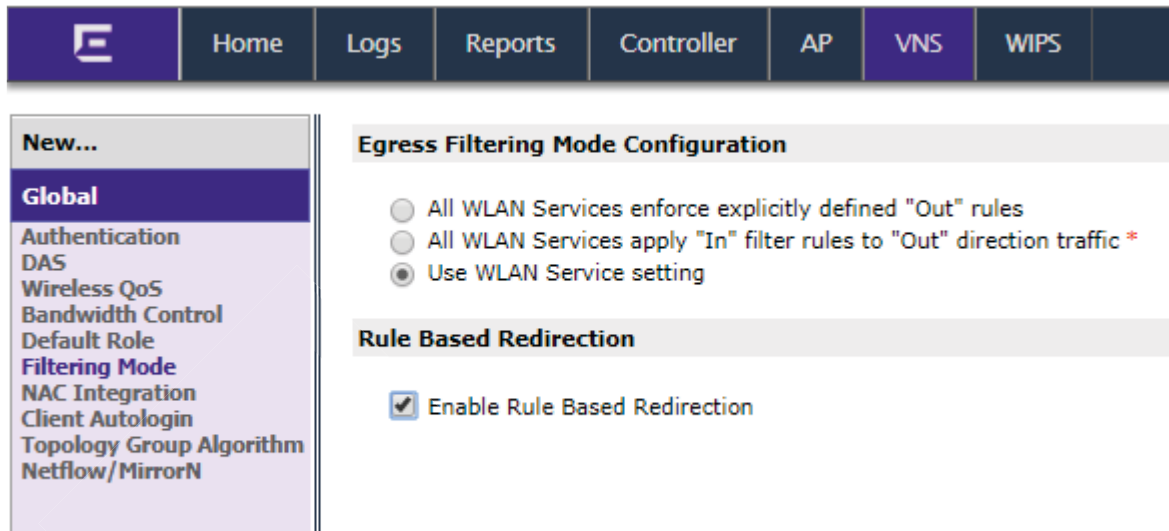


Figure 140: Egress Filtering Mode

- 3 Select an egress filtering mode:
- **All WLAN Services enforce explicitly defined “Out” rules** – All *WLAN* services enforce outbound filters on egress traffic exactly as they are defined in the role.
 - **All WLAN Services apply “In” policy rules to “Out” direction traffic** – All WLAN services enforce that outbound policy rules that are explicitly defined in the role are overridden by a set of rules created by copying each inbound role rule and swapping the source and destination address roles in the rule.
 - **Use WLAN Service setting** – Each role’s rules are interpreted in accordance with the **Egress Filtering Mode** setting of each WLAN Service on which the role is applied. In this mode, it is possible that a role’s rules can be interpreted in two different ways at the same time, if it is used simultaneously on a WLAN service that has **Enforce explicitly defined “Out” rules** enabled and on a WLAN service that has **Apply “In” rules to “Out” direction traffic** at the same time.

Note



The **Use WLAN Service setting** is recommended. If you are using Policy Manager, configure each WLAN Service’s Egress filtering option directly from Policy Manager. Enabling Egress Filtering on a WLAN Service port in Policy Manager is equivalent to setting **Apply “In” rules to “Out” direction traffic** in the WLAN Service’s Advanced dialog.

- 4 Select **Rule-based Redirection** to enable redirection based on configured policy rules after a packet is denied. For more information, see [Rule-Based Redirection](#) on page 289.

Upgrade considerations for default Rule-based Redirection setting:

- This setting is enabled for the following installation scenarios:
 - For new installations of ExtremeWireless v10.11 or later
 - When upgrading from ExtremeWireless v10.11 or later
 - For factory resets of ExtremeWireless v10.11 or later
- When upgrading from a previous version of ExtremeWireless, this check box is cleared, and Rule-based Redirection is disabled.

Related Links

[Configuring Egress Filtering Mode](#) on page 410

[Rule-Based Redirection](#) on page 289

[Managing Redirection URLs](#) on page 421

Using the Sync Summary

The **Sync Summary** screen provides an overview of the synchronization status of paired controllers.

Global

☒ **Synchronize System Configuration**

Global Settings [Hide]

Global Settings

Sites [Hide]

Name	Sync	Status
s1	☒	Unknown

Virtual Networks [Hide]

Name	Sync	Status
Lab42-WPA	☐	Synchronize Now

The screen is divided into five sections: Virtual Networks, *WLAN* services, Roles, Classes of Service, and Topologies. Each section lists the name of the corresponding configuration object, its synchronization mode, and the status of last synchronization attempt.

If Synchronization of an object is not enabled, then there is a button in the Status field which says “Synchronize Now”, which performs a single synchronization of the object, pushing the object from local controller to the peer.

If Synchronization of an object is enabled, then the “Status” field can have the following values:

- Synchronized
- Not Synchronized
- Failed
- Conflict (with a button called “Resolve”)

The **Synchronize System Configuration** check box acts as a global synchronization flag. When it's disabled, synchronization is not performed in the background. When it is enabled, only the objects that have “Sync” enabled are synchronized.

An object may have a synchronization state of “Conflict” if it was updated on both controllers in the availability pair while the availability link was down. In such a case, the **Resolve** button lets you choose which version of the object should be taken, local or remote. Please note that controllers don't compare the actual configuration when they declare a conflict — only the fact that the object was updated on both controllers in the availability pair triggers the “Conflict” state.

Using NAC Integration

NAC Integration provides the ability to forward *DHCP* traffic from a controller to a configured NAC server. When a controller is configured to be a topology's DHCP server, or a relay for a topology, and this feature is enabled, traffic is forwarded to the NAC server. The NAC Integration Options screen provides a list of NAC servers that will accept DHCP messages from the controller. A maximum of three address can be entered and only one address can be entered for each NAC Server. To stop DHCP forwarding, all configured NAC servers need to be deleted from the list. The screen lists the NAC Server, NAC Name and IP Address. The screen provides the ability to add a new server or delete an existing entry.

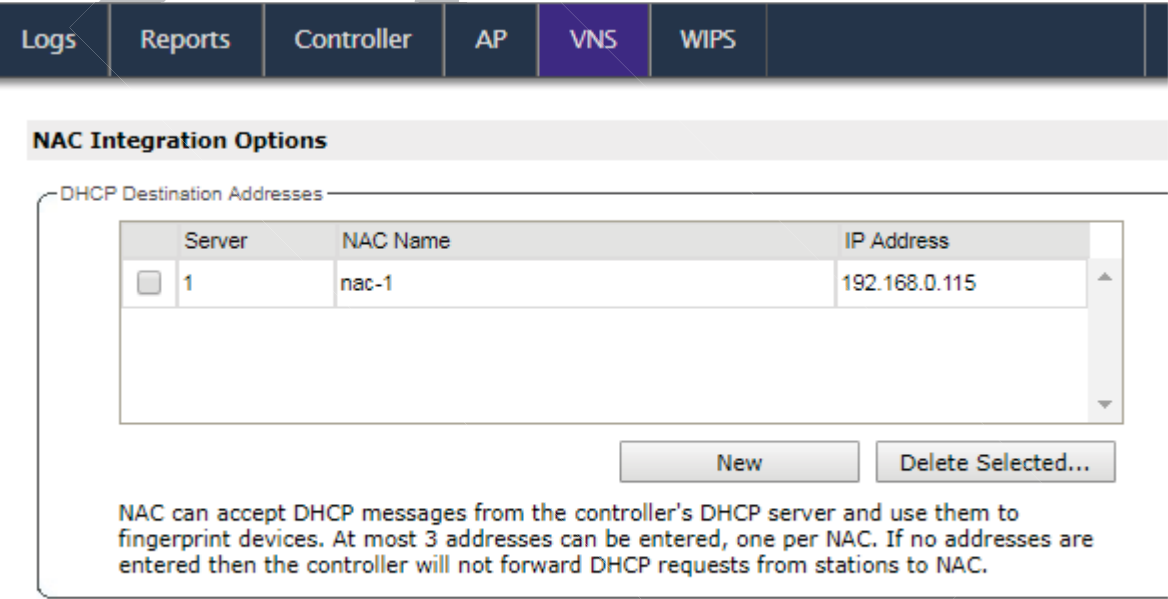


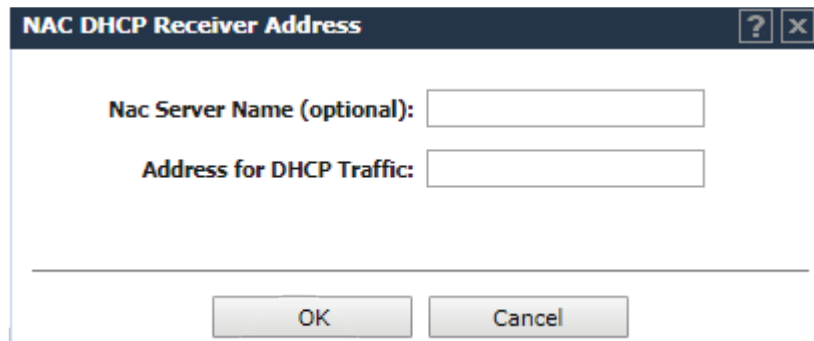
Figure 141: NAC Integration Settings

Adding a New NAC Server Destination

- 1 From the top menu, click **VNS**.
- 2 In the left pane, click **Global > NAC Integration**.

- 3 Click **New**.

The NAC DHCP Receiver Address dialog appears.



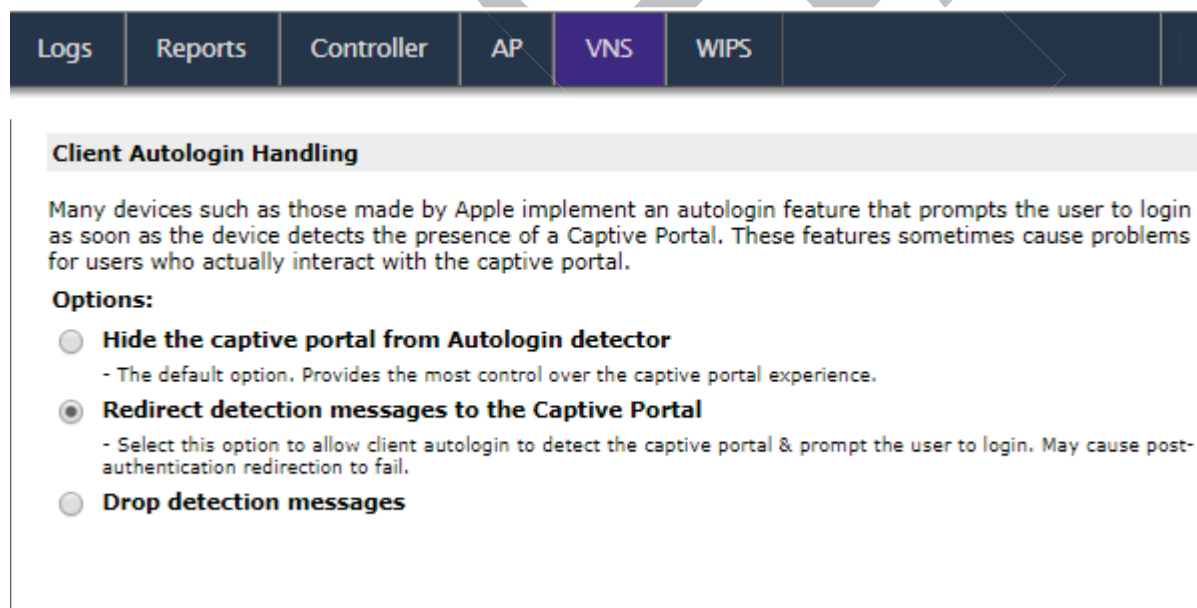
The dialog box is titled "NAC DHCP Receiver Address" and has a question mark icon and a close button in the top right corner. It contains two input fields: "Nac Server Name (optional):" and "Address for DHCP Traffic:". Below the input fields are "OK" and "Cancel" buttons.

- 4 For **Nac Server Name**, enter a name for the NAC Server. This is an optional step, but it helps to identify a specific server.
- 5 For **Address for DHCP Traffic**, enter the IPv4 address for *DHCP* Traffic.
- 6 Click **OK**.

Using Client Login

When a client uses a device that provides autologin capabilities, an attempt is made to detect whether the device needs to authenticate to a captive portal to gain network access via the controller. If the device determines that captive portal authentication is required, a login dialog is displayed. After logging in, access is granted and the browser window closes.

This autologin behavior is incompatible with deployments that need to direct all wireless users to a specific web page after the login completes. Using the Client Autologin feature provides configuration options to control autologin behavior.



The screenshot shows the VNS configuration page with a navigation bar at the top containing "Logs", "Reports", "Controller", "AP", "VNS" (highlighted), and "WIPS". Below the navigation bar is a section titled "Client Autologin Handling". The text in this section reads: "Many devices such as those made by Apple implement an autologin feature that prompts the user to login as soon as the device detects the presence of a Captive Portal. These features sometimes cause problems for users who actually interact with the captive portal." Below this text are three options, each with a radio button:

- ☐ **Hide the captive portal from Autologin detector**
- The default option. Provides the most control over the captive portal experience.
- ☒ **Redirect detection messages to the Captive Portal**
- Select this option to allow client autologin to detect the captive portal & prompt the user to login. May cause post-authentication redirection to fail.
- ☐ **Drop detection messages**

Figure 142: Global Client Autologin

Selecting a Client Autologin Option

- 1 From the top menu, click **VNS**.
- 2 In the left pane, click **Global > Client Autologin**.
The **Client Autologin Handling** screen displays.
- 3 Select from one of the following options:
 - When Autologin is set to **Hide the captive portal from Autologin detector**, the server is spoofed and creates the impression that there is no captive portal. This is the default option.
 - When Autologin is set to **Redirect detection messages to the Captive Portal**, the client detects the captive portal and prompts the user to login.
 - When Autologin is set to **Drop detection messages**, the controller ignores the connection request and drops the client.
- 4 Click **Save** to save the desired option.

Using Topology Group Algorithm

Tunneled station traffic is forwarded from the AP to the controller as if the groups were plain topologies. The controller provides minimum support to use only tunneled topology groups (B@AC, routed). The controller will run the Topology Group Algorithm and will not forward the mapping table to the AP.

Go to **VNS > Global > Topology Group Algorithm**.

Topology Group Selection Algorithm

Algorithm for Selecting a Member Topology from a Topology Group

Options:

- ☒ **MAC-Based**
 - Hash on selected bits of the MAC address mod the number of topologies in the topology group. This algorithm always assigns a client to the same topology within the topology group.
- ☐ **Round Robin**
 - The list is considered ordered; start at the top of the list. The next assignment is the next topology on the list; wrap around at the bottom.
- ☐ **Random Selected**
 - Random number selected from a uniform distribution mod the number of topologies in the topology group.
- ☐ **Least Used**
 - Assign a topology in the topology group with the least number of stations assigned to it at the moment of assignment.

Figure 143: Topology Group Algorithm

The following algorithms are available for selecting a member topology from a Topology Group:

- **MAC-Based:** This algorithm always assigns a client to the same topology within the topology group.
- **Round Robin:** The list is considered ordered; start at the top of the list. The next assignment is the next topology on the list; wrap around at the bottom.
- **Random Selected:** Random number selected from a uniform distribution mod the number of topologies in the topology group.
- **Least Used:** Assign a topology in the topology group with the least number of stations assigned to it at the moment of assignment.

Using Netflow/MirrorN

Use Netflow to forward packet information. Integration with ExtremeAnalytics no longer requires Netflow/MirrorN. See [ExtremeAnalytics Support with Enhanced IPFIX Records](#) on page 419 for more information.

Netflow/MirrorN Configuration

Netflow Export-Destination IP Address:

Netflow Export Interval: (30-360 seconds)

Mirror first N: (1-31 packets/flow)

Traffic Mirror L2 Port:

Figure 144: Netflow/MirrorN

The following configuration items are supported:

- **Netflow Export-Destination IP Address:** Configure the ExtremeAnalytics engine IP to receive Netflow records.
- **Netflow Export Interval:** Configure the Netflow sending interval for same flow. The default value is 60. It will support from 30 to 360 seconds.
 - **Mirror first N:** Configure the MirrorN first N packets. It is a global setting per controller and all APs (per link). Default setting is 15.
 - **Traffic Mirror L2 Port:**

Configure the mirror port on the controller. The default value is **None**. The other I2 ports can only be selected when it is not referred elsewhere (lag, topologies).

ExtremeAnalytics Support with Enhanced IPFIX Records

ExtremeWireless leverages and integrates with ExtremeAnalytics for decoding, detection, collection of Metadata, and scrutinization of Layer 7 data. The solution functions by first enabling WLAN Services on the wireless controller to forward packets to the ExtremeAnalytics engine. This feature requires ExtremeAnalytics 7.0.8 or later.

Depending on your topology, the controller and the AP can inspect the flow, generate the application ID and round trip time (RTT), and format the IPFIX record. With B@AP, the AP sends the IPFIX record to the controller via a WASSP tunnel and then the controller exports the record to ExtremeAnalytics. With B@AC, the controller exports the IPFIX record to ExtremeAnalytics directly.

The IPFIX packets provide all the standard information found in a Netflow v9 packet with enhanced IPFIX parameters. The standard packet includes source and destination IP addresses, ports, protocol, and packet counter information. The enhanced IPFIX records include the application group ID, display ID, the DNS and TCP round trip times (RTT), and flow metadata (which is part of the URL to help classify the flow). The enhanced IPFIX records that the controller sends, releases the dedicated MirrorN port and reduces ExtremeAnalytics CPU resources previously used to identify the application.

IPFIX record templates are supported for IPv4 and IPv6.

Upgrades retain NETFLOW configuration, delivering enhanced records. Netflow with IPFIX reporting is disabled by default.

Live Signature Update

ExtremeWireless supports Live Signature Update to synchronize standard application signatures with ExtremeAnalytics. Through the use of Live Signature Update, the ExtremeWireless controller and its connected APs receive standard signature updates and custom signatures from ExtremeAnalytics.

Both standard and custom signatures are updated. When configuring applications from ExtremeAnalytics, you can define a custom application and custom group. When configuring applications from ExtremeWireless, you can define a custom application specifying a pre-configured ExtremeAnalytics group. The following is the maximum number of custom signatures that can be supported simultaneously:

- ExtremeAnalytics — 512 signatures
- ExtremeWireless — 64 signatures

ExtremeAnalytics users download the updated signature list to ExtremeWireless through the CLI. Once downloaded, the signatures are available for configuration in role filters using L7 Application Rules, and the new signatures are automatically propagated to all attached APs.

CLI Command: `copy signature (<server> <user> <dir> <file> [ftp <ftp_password> | scp <scp_password>]) | show`

For more information about the ExtremeWireless CLI, see the *CLI Guide*.

The latest downloaded signature files are saved in permanent storage on both the controller and the AP and will remain intact after software upgrades and system restarts.

During a configuration import, if ExtremeWireless encounters a filter with a group or application name that is not recognized, ExtremeWireless converts the group to the predefined *Unknown Apps* group and the application name to *Undefined*. A log file is generated to alert the administrator. The original group and application name are lost. A new signature set is applied to the group and the application is re-defined.

Note

Live Signature Update is supported when using the following software and AP models:



- ExtremeWireless v10.41 on-premise with the following AP models: AP3805, AP3825, and AP39xx models. This feature does not support APs connected to ExtremeCloud.
- ExtremeAnalytics v8.1 or later. It can be ported to v8.0.x branch earlier) with ExtremeAnalytics and the appropriate licenses.

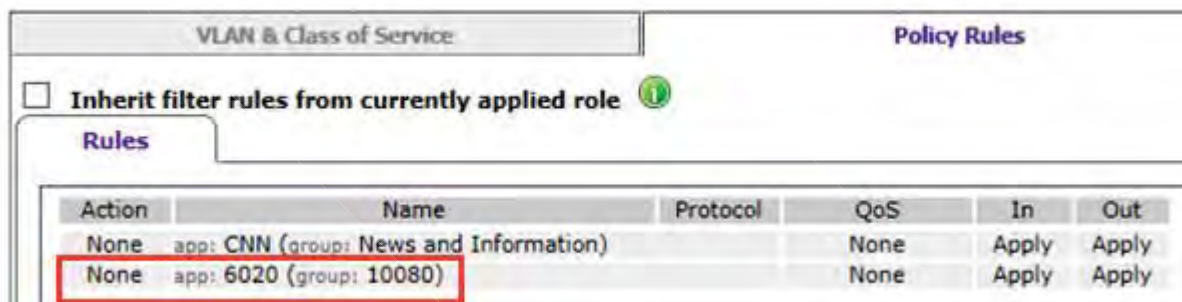
Related Links

- [Deleted Signature Support](#) on page 421
- [L7 Configuration](#) on page 307
- [Including Custom Apps](#) on page 313
- [Configuring Policy Rules](#) on page 298
- [Allowing for Restricted Sets of Applications and Resources](#) on page 311

Deleted Signature Support

Deleted signature support — If a signature that is used in an L7 Application Rule is deleted by Live Signature Update, ExtremeWireless does not delete the filter, but displays the ID of the application and the group instead of the text names, see [Figure 145](#). The display of the ID number indicates that the signature has been deleted. You can delete the filter rule or reconfigure the rule with a different signature. Application filters that employ deleted signatures will not match any network traffic and the filter is treated as NULL.

If the deleted signature is included again through a signature update, the ExtremeWireless user interface automatically replaces the ID numbers with text names.



Action	Name	Protocol	QoS	In	Out
None	app: CNN (group: News and Information)		None	Apply	Apply
None	app: 6020 (group: 10080)		None	Apply	Apply

Figure 145: L7 Application Filter Rule with Deleted Signature

Related Links

- [Live Signature Update](#) on page 420

Managing Redirection URLs

Configure a list of redirection URLs from the Redirection URL dialog. You can add and delete a URL.



Note

To display the **Redirection URL** option, enable **Rule-based Redirection** under **Filtering Mode**.

For more information, see [Configuring the In/Out Rules for WLAN Services Settings](#) on page 412.

The URL list can contain up to 255 proper URLs, consisting of Fully-Qualified Domain Name (FQDN) addresses and IPV4 addresses. Duplicate entries are not permitted, and you must ensure that network traffic is accessible to the required IP addresses. The name of the WLAN Service that these entries are created for is displayed on the user interface and on the command line interface. SNMP also displays the URLs when queried through the Policy Profile MIB.

External Captive Portal URLs are not required, but when they exist, they are automatically added to the list.



Note

You cannot configure Captive Portal Redirection using IPv6 classifiers. While you can http to IPv6 websites, you cannot apply Captive Portal redirection to http [s] over IPv6 .

For URL specifications, see [Adding a Redirection URL](#) on page 422.

Related Links

[Configuring the In/Out Rules for WLAN Services Settings](#) on page 412

[Adding a Redirection URL](#) on page 422

[Deleting a Redirection URL](#) on page 423

Adding a Redirection URL

- 1 There are two ways to add a redirection URL:
 - Adding from the **Redirection URL** list, go to **VNS > Global > Redirection URL** and click **Add**.
 - Adding from the **VLAN & Class of Service** tab, go to **VNS > Roles > VLAN & Class of Service**. Beside the **Redirection URL** field, click **New**.

The **Redirection URL** dialog displays.

- 2 Enter the URL for redirection.

Redirection destinations have the following specifications:

- Only one redirection destination per role.
- The redirection destination is configurable and is comprised of one of the following items:
 - The IP address and port of the destination server. In this case, the redirection is driven by the HTTP Get query from the redirected request.
 - A complete URL. In this case, the redirection is driven by the HTTP Get query that the administrator specifies. Using the controller interface, you can augment the Get query with the following parameters:
 - Session identifier or token for the station of the redirected traffic
 - Address & port of the controller that is performing the redirection
 - Destination URL of the redirection. The default redirection destination is 'Own WLAN'.



Note

The default Redirection destination is 'Own WLAN'.

Related Links

[Managing Redirection URLs](#) on page 421

Modifying a Redirection URL

To modify a redirection URL:

Navigate to **VNS > Global > Redirection URL**, and click **Edit**.



Note

Changes made to an existing redirection URL affect all roles using that redirection URL.

Deleting a Redirection URL

To delete a redirection URL:

- 1 Navigate to **VNS > Global > Redirection URL**.



Note

To display the **Redirection URL** option, enable **Rule-based Redirection** under **Filtering Mode**. For more information, see [Configuring the In/Out Rules for WLAN Services Settings](#) on page 412.

- 2 Select the URL in the list to delete, and click **Delete Selected**.



Note

URLs that are in use, cannot be deleted from the list.

Methods for Configuring a VNS

To configure a VNS, you can use one of the following methods:

- **Manual configuration** — Allows you to create a new VNS by first configuring the topology, role, and WLAN services and then configuring any remaining individual VNS tabs that are necessary to complete the process.

When configuring a VNS, you can navigate between the various VNS tabs and define your configuration without having to save your changes on each individual tab. After your VNS configuration is complete, click Save on any VNS tab to save your completed VNS configuration.



Note

If you navigate away from the VNS configuration tabs without saving your VNS changes, your VNS configuration changes will be lost.

- **Wizard configuration** — The VNS wizard helps create and configure a new VNS by prompting you for a minimum amount of configuration information. The VNS is created using minimum parameters. The remaining parameters are automatically assigned in accordance with best practice standards.

After the VNS wizard completes the VNS creation process, you can then edit or revise any of the VNS configuration to suit your network needs.

Manually Creating a VNS

Advanced configuration allows administrators to create a new VNS once the topology, role, and WLAN services required by the VNS parameters are available. The topology, role and WLAN services could be created in advance or could be created at the time of VNS configuration.

When you create a new VNS, additional tabs are displayed depending on the selections made in the Core box of the main VNS configuration tab.

When configuring a VNS, you can navigate between the various VNS tabs and define your configuration without having to save your changes on each individual tab. After your VNS configuration is complete, click Save on any VNS tab to save your complete VNS configuration.

**Note**

If you navigate away from the VNS Configuration tabs without saving your VNS changes, your VNS configuration changes will be lost.

The following procedure lists the steps necessary to create a VNS in advanced mode. Each step references a section in this document that describes the full details. Follow the links provided to go directly to the appropriate sections.

Creating a VNS Manually

To create a VNS manually:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.

- 2 In the left pane, expand the **Virtual Networks** pane and select an existing VNS to edit, or click **New**.

The screenshot shows the VNS configuration interface with the following sections:

- General** (Tab):
 - Core**: VNS Name: Lab46-WPA
 - WLAN Service**: WLAN Service: Lab46-WPA (dropdown), Edit, New
 - Default Roles**:
 - Non-Authenticated**: Default (dropdown), Edit, New
Action: Class of Service:
 - Authenticated**: <Same as non-authenticated> (dropdown), Edit, New
Action: Class of Service:
 - Status**:
 - Synchronize**: ☒ Replicated when Synchronize Configuration is enabled
 - Enable**: ☒

Figure 146: VNS Settings

- 3 Enter a name for the VNS.
- 4 Select an existing WLAN Service for the VNS, or create a new WLAN Service, or edit an existing one. For more information, see [Configuring a Basic WLAN Service](#) on page 319.
- 5 Configure the Default Roles for the VNS. Select existing roles, or create new roles, or edit existing ones. For more information, see [Configuring a VNS](#) on page 390.
- 6 Configure the Status parameters for the VNS:
 - **Synchronize** — Enable automatic synchronization with its availability peer. Refer to [Using the Sync Summary](#) on page 414 for information about viewing synchronization status. If this VNS is part of an availability pair, Extreme Networks recommends that you enable this feature.
 - **Enabled** — Check to enable the VNS.
- 7 Click **Save** to save your changes.

Also, as with creating a new VNS, you can:

- Configure a topology for the VNS
- Configure a role for the VNS
- Configure WLAN services for the VNS
- Configure additional roles for the VNS

Creating a VNS Using the Wizard

The VNS wizard helps create and configure a new VNS by prompting you for a minimum amount of configuration information during the sequential configuration process. After the VNS wizard completes the VNS creation process, you can then continue to configure or revise any of the VNS configuration to suit your network needs.

When using the VNS wizard to create a new VNS, you can create the following types of VNSs:

- **NAC SSID-based VNS** — NAC gateway-compatible VNS. The controller integrates with an Extreme Networks NAC Controller to provide authentication, assessment, remediation and access control for mobile users. For more information, see [Creating a NAC VNS Using the VNS Wizard](#) on page 426.
- **Voice** — Voice-specific VNS that can support various wireless telephones, including optiPoint, Spectralink, Vocera, and Mobile Connect - Nokia. For more information, see [Creating a Voice VNS Using the VNS Wizard](#) on page 428.
- **Data** — Data-specific VNS, that can be configured to use either SSID or AAA authentication. For more information, see [Creating a Data VNS Using the VNS Wizard](#) on page 436.
- **Captive Portal** — A VNS that employs a Captive Portal page, which requires mobile users to provide login credentials when prompted to access network services. In addition, use the VNS wizard to configure a GuestPortal VNS using the Captive Portal option. For more information, see [Creating a Captive Portal VNS Using the VNS Wizard](#) on page 446.

The VNS type dictates the configuration information that is required during the VNS creation process.

Creating a NAC VNS Using the VNS Wizard

The ExtremeWireless controller integrates with an Extreme Networks NAC controller to provide authentication, assessment, remediation and access control for mobile users. For more information, see [NAC Integration with the Wireless WLAN](#) on page 24.

Use the VNS wizard to configure a NAC gateway-compatible VNS by defining the following essential parameters:

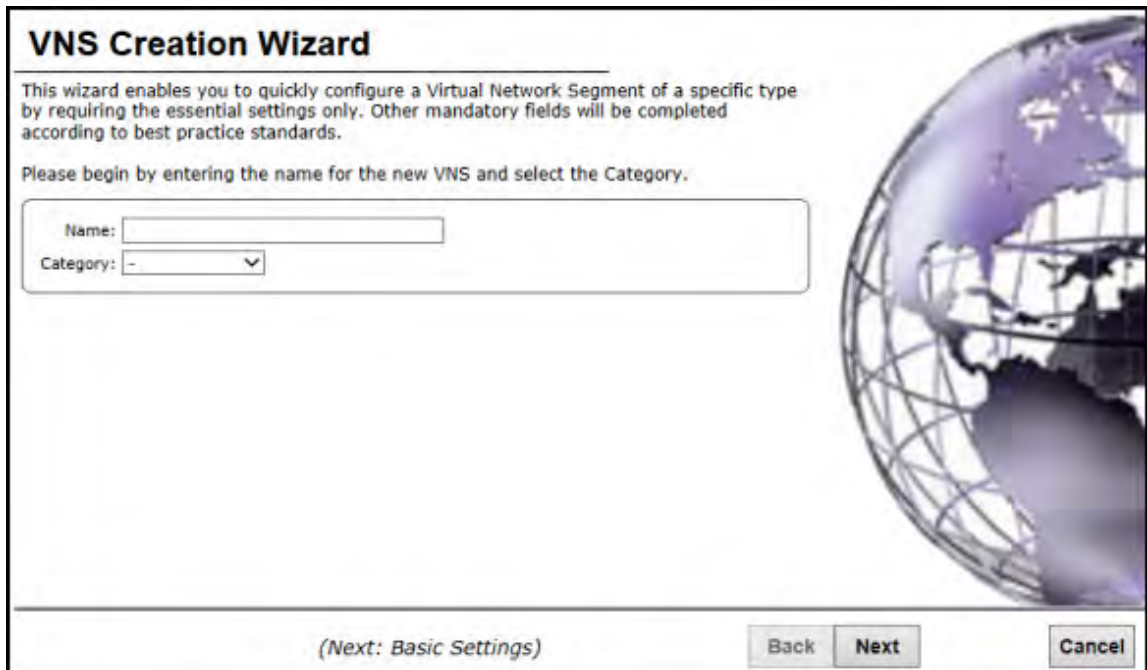
- **VNS Name** — The name that will be assigned to the VNS and SSID.
- **IP Address** — The IP address of the ExtremeWireless controller's interface on the VLAN.
- **Mask** — The subnet mask for the IP address to separate the network portion from the host portion of the address.
- **VLAN ID** — ID number of the VLAN to which the ExtremeWireless controller is bridged for the VNS.
- **Port** — Physical L2 port to which the configured VLAN is attached.
- **RADIUS server** — IP address of the NAC controller.
- **Redirection URL** — The URL that points to the NAC controller's web server.

The VNS wizard creates a Bridge Traffic Locally at EWC VNS. This VNS has the crucial attributes — SSID Network Assignment Type, MAC-based external captive portal authentication and WPA-PSK encryption

— that makes it compatible with the NAC controller. The remaining VNS parameters are defined automatically according to best practice standards.

To configure a NAC VNS using the VNS wizard:

- 1 From the top menu, click **VNS**.
- 2 In the left pane, click **New > START VNS WIZARD**.



VNS Creation Wizard

This wizard enables you to quickly configure a Virtual Network Segment of a specific type by requiring the essential settings only. Other mandatory fields will be completed according to best practice standards.

Please begin by entering the name for the new VNS and select the Category.

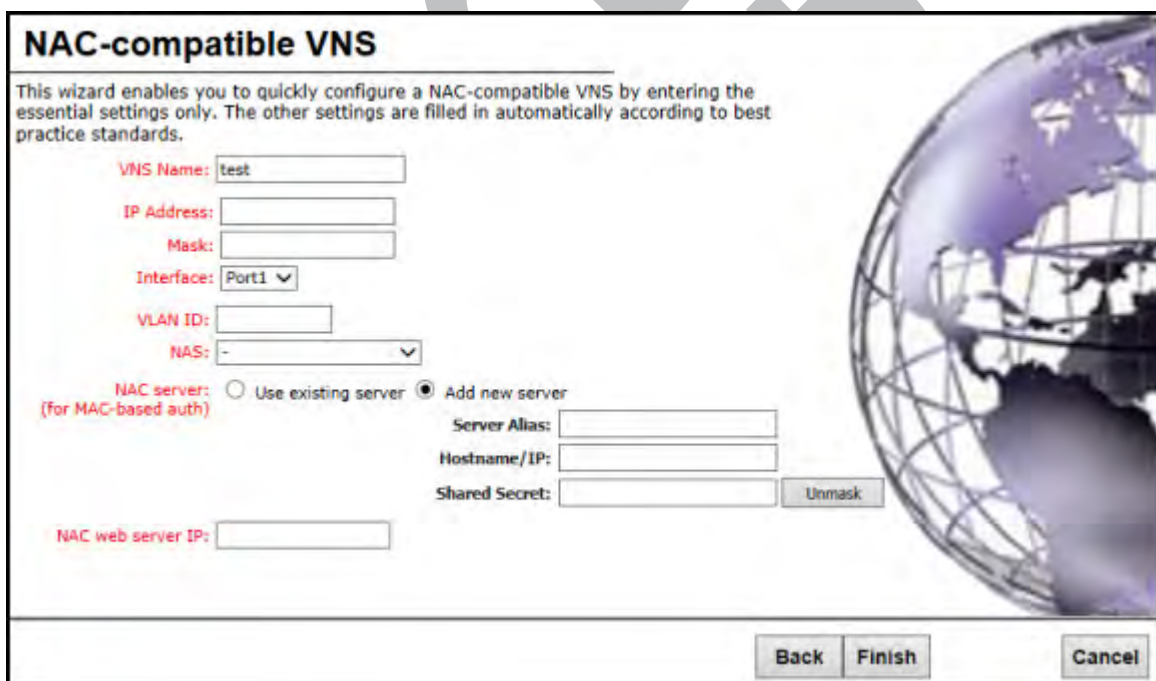
Name:

Category:

(Next: Basic Settings)

Back Next Cancel

- 3 In the **Name** box, type a name for the NAC SSID-based VNS.
- 4 In the **Category** drop-down list, click **NAC VNS**, and then click **Next**.



NAC-compatible VNS

This wizard enables you to quickly configure a NAC-compatible VNS by entering the essential settings only. The other settings are filled in automatically according to best practice standards.

VNS Name:

IP Address:

Mask:

Interface:

VLAN ID:

NAS:

NAC server: ☐ Use existing server ☒ Add new server

(for MAC-based auth)

Server Alias:

Hostname/IP:

Shared Secret: Unmask

NAC web server IP:

Back Finish Cancel

Table 74: NAC-compatible VNS Page - Fields and Buttons

Field/Button	Description
IP Address	Type the IP address of the ExtremeWireless Appliance's interface on the VLAN.
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
Interface	From the drop-down list, select the physical port that provides the access to the VLAN.
VLAN ID	Type the VLAN tag to which the ExtremeWireless Appliance will be bridged for the VNS.
NAS	From the drop-down list, click the interface/port through which the NAC gateway will communicate with the ExtremeWireless Appliance. The IP address in this field will be used as the NAS IP RADIUS attribute when communicating with the NAC gateway.
NAC Server	
Server Alias	Type the name or IP address of the NAC server.
Hostname/IP	Type the NAC server's FQDN (fully qualified domain name) or IP address.
Shared Secret	Type the password that will be used to validate the connection between the ExtremeWireless Appliance and the NAC server. To proofread your shared secret key, click Unmask . The password is displayed. Note: You should always proofread your Shared Secret key to avoid any problems later when the wireless appliance attempts to communicate with the NAC controller.
NAC web server IP	Type the NAC web server IP address.

- 5 To save your changes, click **Finish**.

The VNS wizard creates a SSID-based NAC controller-compatible VNS, and displays the configuration summary.

- 6 To close the VNS wizard, click **Close**.

If applicable, you can continue to configure or edit the new VNS by clicking the individual VNS configuration tabs.

Creating a Voice VNS Using the VNS Wizard

Use the VNS wizard to create a voice-specific VNS that can support various wireless telephones, including optiPoint, Spectralink, Vocera, and Mobile Connect - Nokia.

When you use the VNS wizard to create a voice-specific VNS, you optimize the voice VNS to support one wireless telephone vendor. If the voice VNS needs to be optimized for more than one wireless phone vendor, use the advanced method to create the voice-specific VNS. For more information, see [Enabling and Disabling a VNS](#) on page 485.

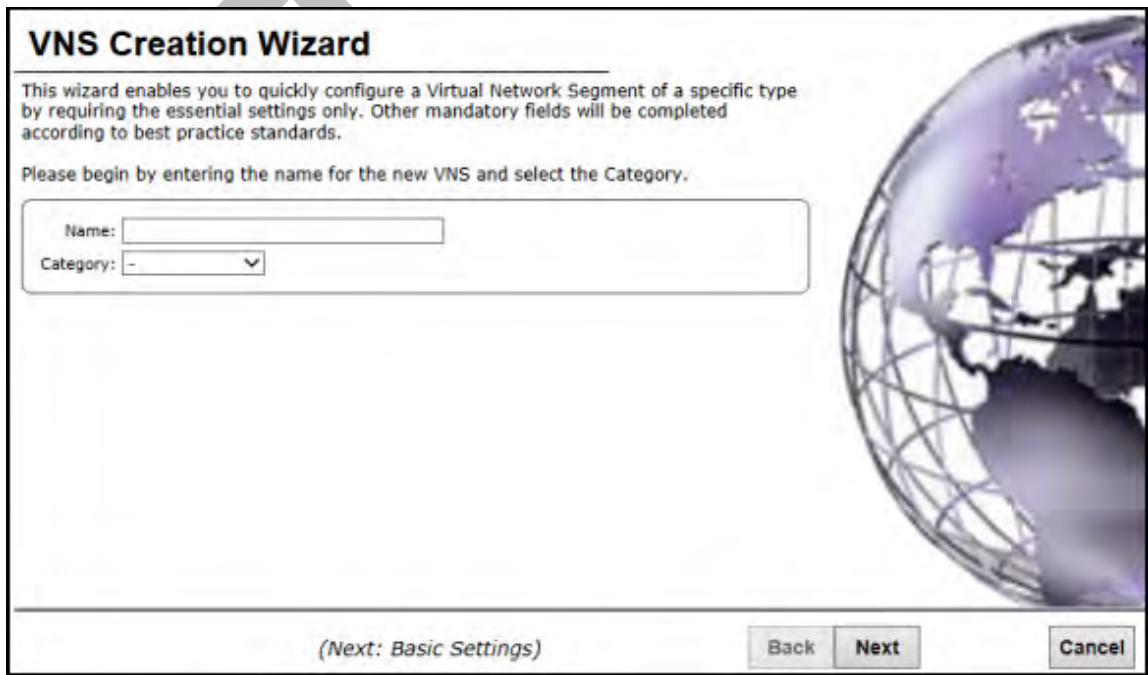
When you create a new voice VNS using the VNS wizard, you configure the VNS in the following stages:

- [Basic settings](#)
- [Authentication settings](#), if applicable
- [DHCP settings](#)
- [Privacy settings](#)
- [Radio assignment settings](#)
- [Summary](#)

To configure a Voice VNS using the VNS Wizard:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 2 In the left pane, expand the **New** pane, then click **START VNS WIZARD**.

The **VNS Creation Wizard** screen displays.



- 3 In the **Name** box, type a name for the voice VNS.
- 4 In the **Category** drop-down list, click **Voice**.
- 5 Click **Next**. The [Basic Settings](#) screen displays.

Creating a Voice VNS Using the VNS Wizard - Basic Settings Screen

The **Basic Settings** screen displays:

Basic Settings
Test, Voice

Enabled: ☒

Name: Test

Category: Voice

SSID: Test

Type:

Mode:

(Next: Privacy)

Back Next Cancel

Table 75: Voice VNS Basic Settings Page - Fields and Buttons

Field/Button	Description
Enabled	By default, the Enabled check box for the new VNS is enabled. A VNS must be enabled for it to be able to provide service for mobile user traffic.
Synchronize	By default, the Synchronize check box for the new VNS is disabled.
Name	Identifies the name of the VNS.
Category	Identifies the VNS category.
SSID	Identifies the SSID assigned to the VNS.
Type	Click the wireless phone you want to support for the new voice VNS you are creating.
Mode	Click the VNS Mode you want to assign: • Routed is a VNS type where user traffic is tunneled to the controller. • Bridge Traffic Locally at EWC is a VNS type that has associated with it a Topology with a mode of Bridge Traffic Locally at EWC. User traffic is tunneled to the controller and is directly bridged at the controller to a specific <u>VLAN</u>. With this VNS type, mobile users become a natural extension of a VLAN subnet. For each Bridge Traffic Locally at EWC VNS that is created, a VLAN needs to be specified. In addition, the network port on which the VLAN is assigned must be configured on the switch, and the corresponding controller interface must match the correct VLAN.
Routed Voice VNS	

Table 75: Voice VNS Basic Settings Page - Fields and Buttons (continued)

Field/Button	Description
Gateway	Type the controller's own IP address of the topology associated with that VNS. This IP address is also the default gateway for the VNS. The controller advertises this address to the wireless devices when they sign on. For routed VNSs, it corresponds to the IP address that is communicated to mobile users (in the VNS) as the default gateway for the VNS subnet. (Mobile users target the controller's interface in their effort to route packets to an external host).
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
Gateway/SVP	If the voice VNS is to support Spectralink wireless phones, type the IP address of the SpectraLink Voice Protocol (SVP) gateway.
Vocera Server	If the voice VNS is to support Vocera wireless phones, type the IP address of the Vocera server.
PBX Server	If the voice VNS is to support either WL2 or Mobile Connect - Nokia wireless phones, type the PBX IP address.
Enable Authentication	If applicable, select this check box to enable authentication for the new voice VNS.
Enable <i>DHCP</i>	By default, this option is selected.
Bridge Traffic Locally- Voice VNS	
Interface	Click the physical interface that provides the access to the VLAN.
Interface IP	Type the IP address of the controller's interface on the VLAN.
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
VLAN ID	Type the VLAN tag to which the controller will be bridged for the VNS.
Gateway/SVP	If the voice VNS is to support Spectralink wireless phones, type the IP address of the SpectraLink Voice Protocol (SVP) gateway.
Vocera Server	If the voice VNS is to support Vocera wireless phones, type the IP address of the Vocera server.
PBX Server	If the voice VNS is to support either WL2 or Mobile Connect - Nokia wireless phones, type the PBX IP address.
Enable Authentication	If applicable, select this check box to enable authentication for the new voice VNS.
Enable DHCP	If applicable, select this check box to enable DHCP authentication for the new voice VNS.

Click **Next**. The **Authentication** screen displays.

Creating a Voice VNS Using the VNS Wizard - Authentication Settings Screen

The **Authentication** screen displays:

Authentication

Test, Voice, SpectraLink

Radius Server: Add New Server ▾

Server Alias:

Hostname/IP:

Shared Secret:

Roles: ☒ MAC-based Authentication



(Next: DHCP)

Table 76: Voice VNS Authorization Page - Fields and Buttons

Field/Button	Description
Radius Server	Click the RADIUS server you want to assign to the new voice VNS, or click Add New Server and then do the following
Server Alias	Type a name you want to assign to the new RADIUS server.
Hostname/IP	Type either the RADIUS server's FQDN (fully qualified domain name) or IP address.
Shared Secret	Type the password that will be used to validate the connection between the controller and the RADIUS server.
Mask/Unmask	Click to display or hide your shared secret key.
Roles	Select the authentication role options for the RADIUS server: • MAC-based Authentication — Select to enable the RADIUS server to perform MAC-based authentication on the voice VNS. • If applicable, and the MAC-based authentication option is enabled, select to enable MAC-based authorization on roam.
Radius Server	Click the RADIUS server you want to assign to the new data VNS, or click Add New Server and then do the following
Server Alias	Type a name you want to assign to the new RADIUS server.

Click **Next**. The **DHCP** screen displays.

Creating a Voice VNS Using the VNS Wizard - DHCP Screen

The **DHCP** screen displays:

433

Field/Button	Description
DHCP Option	From the drop-down list, click one of the following: • Use DHCP Relay — Using <u>DHCP</u> relay forces the controller to forward DHCP requests to an external DHCP server on the enterprise network. DHCP relay bypasses the local DHCP server for the controller and allows the enterprise to manage IP address allocation to a VNS from its existing infrastructure. • DHCP Servers — Type the IP address of the DHCP server to which DHCP discover and request messages will be forwarded for clients on this VNS. The controller does not handle DHCP requests from users, but instead forwards the requests to the indicated DHCP server. The DHCP server must be configured to match the VNS settings. In particular for a Routed VNS, the DHCP server must identify the controller's interface IP as the default Gateway (router) for the subnet. (Users intending to reach devices outside of the subnet will forward the packets to the default gateway (controller) for delivery upstream.) • Local DHCP Server — If applicable, edit the local DHCP server settings.
DNS Servers	Type the IP Address of the Domain Name Servers to be used.
WINS	Type the IP address if the DHCP server uses Windows Internet Naming Service (WINS).

Click **Next**. The **Privacy** screen displays.

Creating a Voice VNS Using the VNS Wizard - Privacy Screen

The **Privacy** screen displays:

Privacy
Test Voice, SpectraLink

WARNING: To use 11n, Privacy can only be "None" or WPA v.2 with AES only Encryption

☐ None
☐ Static Keys (WEP)
☒ WPA - PSK

☐ WPA v.1
 Encryption: Auto

☒ WPA v.2
 Encryption: AES only

☐ Broadcast re-key interval: seconds (30 - 86400 seconds)

Input Method: ☒ Input String ☐ Input Hex

Pre-shared key String: Unmask
 (min 8 characters; max 63)

(Next: RF) Back Next Cancel

- 1 Most options on this screen are view-only, but you can do the following:
 - **Pre-shared key** — Type the shared secret key to be used between the wireless device and AP. The shared secret key is used to generate the 256-bit key.
 - **Mask/Unmask** — Click to display or hide your shared secret key.
- 2 Click **Next**. The **Radio Assignment** screen displays.

Creating a Voice VNS Using the VNS Wizard - Radio Assignment Screen

The **Radio Assignment** screen displays:

Radio Assignment
Test, Voice, SpectraLink

AP Default Settings
To add this VNS to the AP Default Settings Profile, please select which radio(s) you would like to broadcast this VNS.

☒ Radio 1
☒ Radio 2

AP Selection
Use the drop down list on the left to select the groups of APs and sites that will serve the VNS (such as "All APs" or "radio 1". The list to the right will show the resulting assignment. Note that if your VNS is set to Enabled, and an AP radio or site has the maximum 8 VNSs assigned, the VNS will not be assigned to the AP or site.

Select APs:
WMM: ☐

WARNING: To use 11n, WMM is required.

Radio 1	Radio 2	AP/Site Name
a	b/g	LAB43-2610-0166
a/n	b/g/n	LAB43-3705i-0000
a/n	b/g	LAB43-3725e-3333
a/n	b/g	LAB43-3725i-3456
a	b/g	LAB47-3620-7024[F]
a/n	b/g/n	LAB47-3705i-0047[F]
a	g	LAB47-W788-1503[F]
a/n	b/g	test
a/n	b/g	test2

(Next: Summary) Back Next Cancel

Table 78: Voice VNS Radio Assignment Page - Fields and Buttons

Field/Button	Description
AP Default Settings	
Radio 1 / Radio 2	Select the radios of the AP default settings profile that you want to broadcast the voice VNS.
AP Selection	
Select APs	Select the group of APs that will broadcast the voice VNS: • all radios — Click to assign all of the APs' radios. • radio 1 — Click to assign only the APs' Radio 1. • radio 2 — Click to assign only the APs' Radio 2. • local APs - all radios — Click to assign only the local APs. • local APs - radio 1 — Click to assign only the local APs' Radio 1. • local APs - radio 2 — Click to assign only the local APs' Radio 2. • foreign APs - all radios — Click to assign only the foreign APs. • foreign APs - radio 1 — Click to assign only the foreign APs' Radio 1. • foreign APs - radio 2 — Click to assign only the foreign APs' Radio 2.
WMM	(Wi-Fi Multimedia) If enabled on an individual VNS, provides multimedia enhancements that improve the user experience for audio, video, and voice applications. WMM is part of the 802.11e standard for QoS. If enabled, the AP will accept WMM client associations, and will classify and prioritize the out traffic for all WMM clients. WMM clients will also classify and prioritize the inbound traffic.

Click **Next**. The **Summary** screen displays.

Creating a Voice VNS Using the VNS Wizard - Summary Screen

The **Summary** screen displays:

- 1 Confirm your voice VNS configuration. To revise your configuration, click **Back**.
- 2 To create your VNS, click **Finish**, and then click **Close**.
- 3 If applicable, you can continue to configure or edit the new VNS by clicking the individual VNS configuration tabs.

Creating a Data VNS Using the VNS Wizard

Use the VNS wizard to create a data-specific VNS that can be configured to use either SSID or AAA authentication.

When you create a new data VNS using the VNS wizard, you configure the VNS in the following stages:

- [Basic settings](#)
- [Authentication settings](#)
- [DHCP settings](#)
- [Filter settings](#)
- [Privacy settings](#)
- [Radio assignment settings](#)
- [Summary](#)

To configure a data VNS using the VNS wizard:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.

- 2 In the left pane, expand the New pane, then click **START VNS WIZARD**. The VNS Creation Wizard screen displays.



VNS Creation Wizard

This wizard enables you to quickly configure a Virtual Network Segment of a specific type by requiring the essential settings only. Other mandatory fields will be completed according to best practice standards.

Please begin by entering the name for the new VNS and select the Category.

Name:

Category:

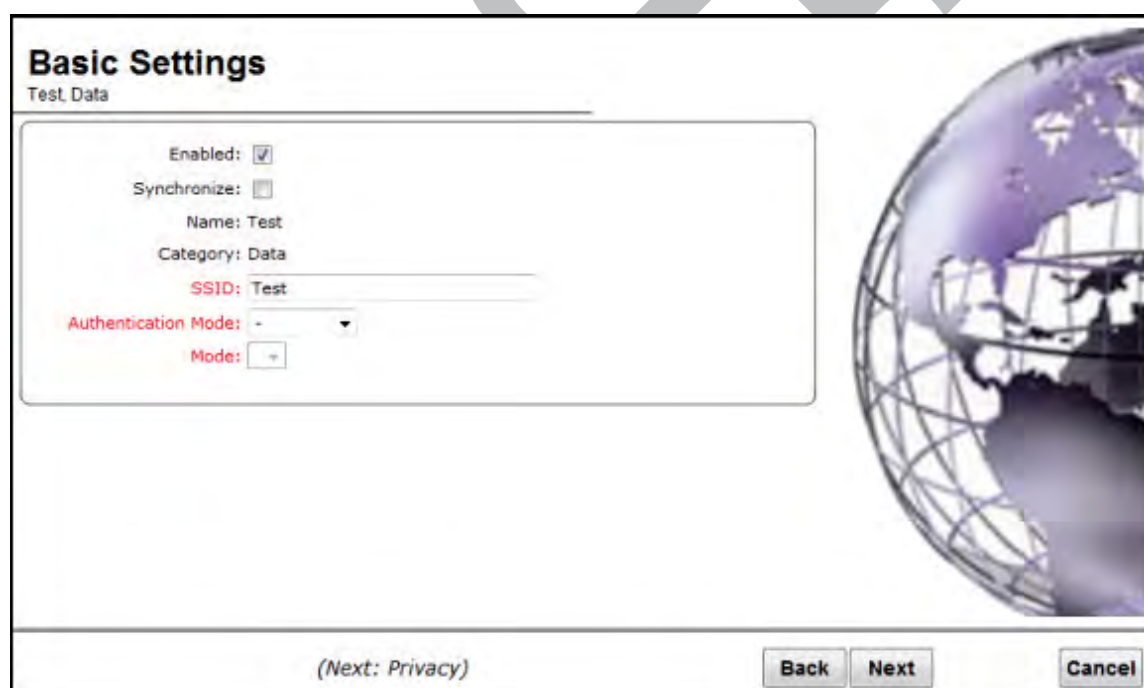
(Next: Basic Settings)

Back Next Cancel

- 3 In the **Name** box, type a name for the data VNS.
- 4 In the **Category** drop-down list, click **Data**.
- 5 Click **Next**. The **Basic Settings** screen displays.

Creating a Data VNS Using the VNS Wizard - Basic Settings Screen

The **Basic Settings** screen displays:



Basic Settings

Test Data

Enabled: ☒

Synchronize: ☐

Name: Test

Category: Data

SSID: Test

Authentication Mode:

Mode:

(Next: Privacy)

Back Next Cancel

Table 79: Data VNS Basic Settings Page - Fields and Buttons

Field/Button	Description
Enabled	By default, the Enabled check box for the new VNS is enabled. A VNS must be enabled for it to be able to provide service for mobile user traffic.
Synchronize	By default, the Synchronize check box for the new VNS is disabled.
Name	Identifies the name of the VNS.
Category	Identifies the VNS category.
SSID	Identifies the SSID assigned to the VNS.
Authentication Mode	Click the type of network assignment for the VNS. There are two options for network assignment, Disabled or 802.1x.
Mode	Click the VNS mode you want to assign: • Routed is a VNS type where user traffic is tunneled to the controller. • Bridge Traffic Locally at EWC is a VNS type where user traffic is tunneled to the controller and is directly bridged at the controller to a specific <i>VLAN</i>. With this VNS type, mobile users become a natural extension of a VLAN subnet. For each Bridge Traffic Locally at EWC VNS that is created, a VLAN needs to be specified. In addition, the network port on which the VLAN is assigned must be configured on the switch, and the corresponding controller interface must match the correct VLAN. • Bridge Traffic Locally at AP is a VNS type where user traffic is directly bridged to a VLAN at the AP network point of access (switch port).
Routed Data VNS	
Gateway	Type the controller's own IP address of the topology associated with that VNS. This IP address is the default gateway for the VNS. The controller advertises this address to the wireless devices when they sign on. For routed VNSs, it corresponds to the IP address that is communicated to mobile users (in the VNS) as the default gateway for the VNS subnet. (Mobile users target the controller's interface in their effort to route packets to an external host).
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
Enable Authentication	This option is enabled by default if the Type is 802.1x.
Enable <i>DHCP</i>	By default, this option is enabled for a routed data VNS.
Bridged Traffic Locally @ AP Data VNS	
Tagged	Select if you want to assign this VNS to a specific VLAN.
VLAN ID	Type the VLAN tag to which the controller will be bridged for the data VNS.
Untagged	Select if you want this VNS to be untagged. This option is selected by default.
Enable Authentication	If applicable, select this check box to enable authentication for the new data VNS. This option is enabled by default if the Type is 802.1x.

Table 79: Data VNS Basic Settings Page - Fields and Buttons (continued)

Field/Button	Description
Bridge Traffic Locally at EWC Data VNS	
Interface	Click the physical port that provides the access to the VLAN.
Interface IP address	Type the IP address of the controller's interface on the VLAN.
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
VLAN ID	Type the VLAN tag to which the controller will be bridged for the VNS.
Enable Authentication	If applicable, select this check box to enable authentication for the new data VNS. This option is enabled by default if the Type is 802.1x.
Enable DHCP	If applicable, select this check box to enable DHCP authentication for the new data VNS.

Click **Next**. The **Authentication** screen displays.

Creating a Data VNS Using the VNS Wizard - Authentication Screen

The **Authentication** screen displays:

Authentication
Test Data, 802.1x

Radius Server: Add New Server ▼

Server Alias:

Hostname/IP:

Shared Secret: Unmask

Roles: ☒ Authentication
☐ MAC-based Authentication
☐ Accounting

(Next: DHCP)

Back Next Cancel

Table 80: Data VNS Authentication Page - Fields and Buttons

Field/Button	Description
Radius Server	Click the RADIUS server you want to assign to the new data VNS, or click Add New Server and then do the following
Server Alias	Type a name you want to assign to the new RADIUS server.
Hostname/IP	Type either the RADIUS server's FQDN (fully qualified domain name) or IP address.
Shared Secret	Type the password that will be used to validate the connection between the controller and the RADIUS server.
Mask/Unmask	Click to display or hide your shared secret key.
Roles	Select the authentication role options for the RADIUS server: • MAC-based Authentication — Select to enable the RADIUS server to perform MAC-based authentication on the data VNS. • If applicable, and the MAC-based authentication option is enabled, select to enable MAC-based authorization on roam.

Click **Next**. The **DHCP** screen displays.

Creating a Data VNS Using the VNS Wizard - DHCP Screen

If **DHCP** was enabled previously, the **DHCP** screen displays:

DHCP
Test, Data, 802.1x

DHCP Option: Local DHCP Server ▼

Address Range: From: 127.0.1.2 To: 127.0.1.254

B'cast Address: 127.0.1.255

Lease (seconds): default: 36000 max: 2592000

DNS Servers:

WINS:

(Next: Filtering)

Back Next Cancel

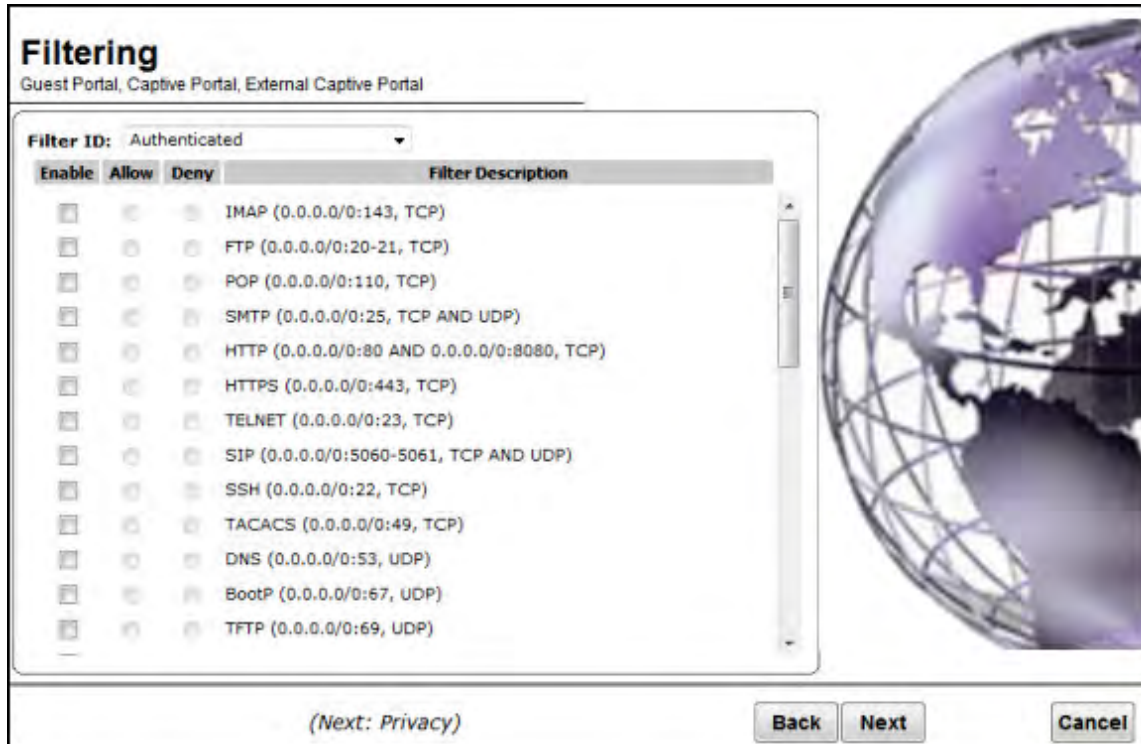
Table 81: Data VNS DHCP Page - Fields and Buttons

Field/Button	Description
DHCP Option	In the DHCP Option drop-down list, click one of the following: • Use DHCP Relay — Using DHCP relay forces the controller to forward DHCP requests to an external DHCP server on the enterprise network. DHCP relay bypasses the local DHCP server for the controller and allows the enterprise to manage IP address allocation to a VNS from its existing infrastructure. • DHCP Servers — If Use DHCP Relay was selected, type the IP address of the DHCP server to which DHCP discover and request messages will be forwarded for clients on this VNS. The controller does not handle DHCP requests from users, but instead forwards the requests to the indicated DHCP server. The DHCP server must be configured to match the VNS settings. In particular for a Routed VNS, the DHCP server must identify the controller's interface IP as the default Gateway (router) for the subnet. (Users intending to reach devices outside of the subnet will forward the packets to the default gateway (controller) for delivery upstream.) • Local DHCP Server — If applicable, edit the local DHCP server settings.
DNS Server	Type the IP Address of the Domain Name Servers to be used.
WINS	Type the IP address if the DHCP server uses Windows Internet Naming Service (WINS).

Click **Next**. The **Filtering** screen displays.

Creating a Data VNS Using the VNS Wizard - Filtering Screen

The **Filtering** screen displays:



- 1 In the **Filter ID** drop-down list, click one of the following:
 - **Default** — Controls access if there is no matching filter ID for a user.
 - **Exception** — Protects access to the controller's own interfaces, including the VNSs own interface. VNS exception filters are applied to user traffic intended for the controller's own interface point on the VNS. These filters are applied after the user's specific VNS state assigned filters
- 2 In the **Filter** table, select the **Allow** or **Deny** option buttons for each filter if applicable, and then select the **Enable** check box accordingly.
- 3 Click **Next**. The **Privacy** screen displays.

Creating a Data VNS Using the VNS Wizard - Privacy Screen

The **Privacy** screen displays:

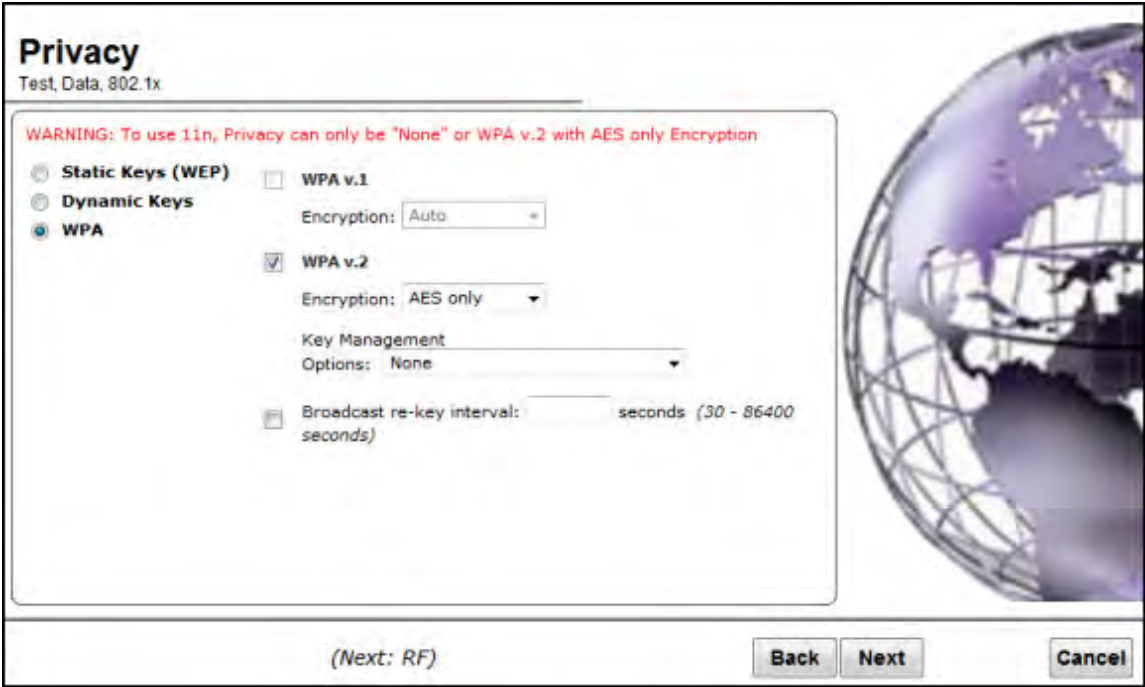


Table 82: Data VNS Privacy Page - Fields and Buttons

Field/Button	Description
Static Keys (WEP)	Select to configure static keys. Then enter: • WEP Key Index — Click the WEP encryption key index: 1, 2, 3, or 4. Specifying the WEP key index is supported only for AP37XX wireless APs. • WEP Key Length — Click the WEP encryption key length: 64 bit, 128 bit, or 152 bit. Select an Input Method: • Input Hex — type the WEP key input in the WEP Key box. The key is generated automatically based on the input. • Input String — type the secret WEP key string used for encrypting and decrypting in the WEP Key String box. The WEP Key box is automatically filled by the corresponding Hex code.
Dynamic Keys	Select to allow the dynamic key WEP mechanism to change the key for each user and each session.

Table 82: Data VNS Privacy Page - Fields and Buttons (continued)

Field/Button	Description
WPA	Select to configure Wi-Fi Protected Access (WPA v1 and WPA v2), a security solution that adds authentication to enhanced WEP encryption and key management. To enable WPA v1 encryption, select WPA v.1. In the Encryption drop-down list, select one of the following encryption types: • Auto — The AP will advertise both TKIP and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for WPAv1. CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). • TKIP only — The AP will advertise TKIP as an available encryption protocol for WPAv1. It will not advertise CCMP. To enable WPA v2 encryption, select WPA v.2. In the Encryption drop-down list, click one of the following encryption types: • Auto — The AP advertises both TKIP and CCMP (counter mode with cipher block chaining message authentication code protocol). CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard).
WPA-PSK	AES only — The AP advertises CCMP as an available encryption protocol. It will not advertise TKIP. To enable re-keying after a time interval, select Broadcast re-key interval, then type the time interval after which the broadcast encryption key is changed automatically. The default is 3600. If this check box is not selected, the Broadcast encryption key is never changed and the AP will always use the same broadcast key for Broadcast/Multicast transmissions. This will reduce the level of security for wireless communications. To enable the group key power save retry, select Group Key Power Save Retry. The group key power save retry is supported only for AP37XX wireless APs. In the Pre-shared key box, type the shared secret key to be used between the wireless device and AP. The shared secret key is used to generate the 256-bit key. Mask/Unmask — Click to display or hide your shared secret key.

Click **Next**. The **Radio Assignment** screen displays.

Creating a Data VNS Using the VNS Wizard - Radio Assignment Screen

The **Radio Assignment** screen displays:

Radio Assignment

Test, Data, 802.1x

AP Default Settings

To add this VNS to the AP Default Settings Profile, please select which radio(s) you would like to broadcast this VNS.

☒ Radio 1

☒ Radio 2

AP Selection

Use the drop down list on the left to select the groups of APs and sites that will serve the VNS (such as "All APs" or "radio 1". The list to the right will show the resulting assignment. Note that if your VNS is set to Enabled, and an AP radio or site has the maximum 8 VNSs assigned, the VNS will not be assigned to the AP or site.

Select APs:

WMM: ☐

WARNING: To use 11n, WMM is required.

Radio 1	Radio 2	AP/Site Name
a	b/g	LAB43-2610-0166
a/n	b/g/n	LAB43-3705i-0000
a/n	b/g	LAB43-3725e-3333
a/n	b/g	LAB43-3725i-3456
a	b/g	LAB47-3620-7024[F]
a/n	b/g/n	LAB47-3705i-0047[F]
a	g	LAB47-W788-1503[F]
a/n	b/g	test
a/n	b/g	test2

(Next: Summary)

Back

Next

Cancel



Table 83: Data VNS Radio Assignment Page - Fields and Buttons

Field/Button	Description
AP Default Settings	
Radio 1 / Radio 2	Select the radios of the AP default settings profile that you want to broadcast the data VNS.
AP Selection	
Select APs	Select the group of APs that will broadcast the data VNS: • all radios — Click to assign all of the APs' radios. • radio 1 — Click to assign only the APs' Radio 1. • radio 2 — Click to assign only the APs' Radio 2. • local APs - all radios — Click to assign only the local APs. • local APs - radio 1 — Click to assign only the local APs' Radio 1. • local APs - radio 2 — Click to assign only the local APs' Radio 2. • foreign APs - all radios — Click to assign only the foreign APs. • foreign APs - radio 1 — Click to assign only the foreign APs' Radio 1. • foreign APs - radio 2 — Click to assign only the foreign APs' Radio 2.
WMM	(Wi-Fi Multimedia), if enabled on an individual VNS, provides multimedia enhancements that improve the user experience for audio, video, and voice applications. WMM is part of the 802.11e standard for QoS. If enabled, the AP will accept WMM client associations, and will classify and prioritize the outbound traffic for all WMM clients. WMM clients will also classify and prioritize the inbound traffic.

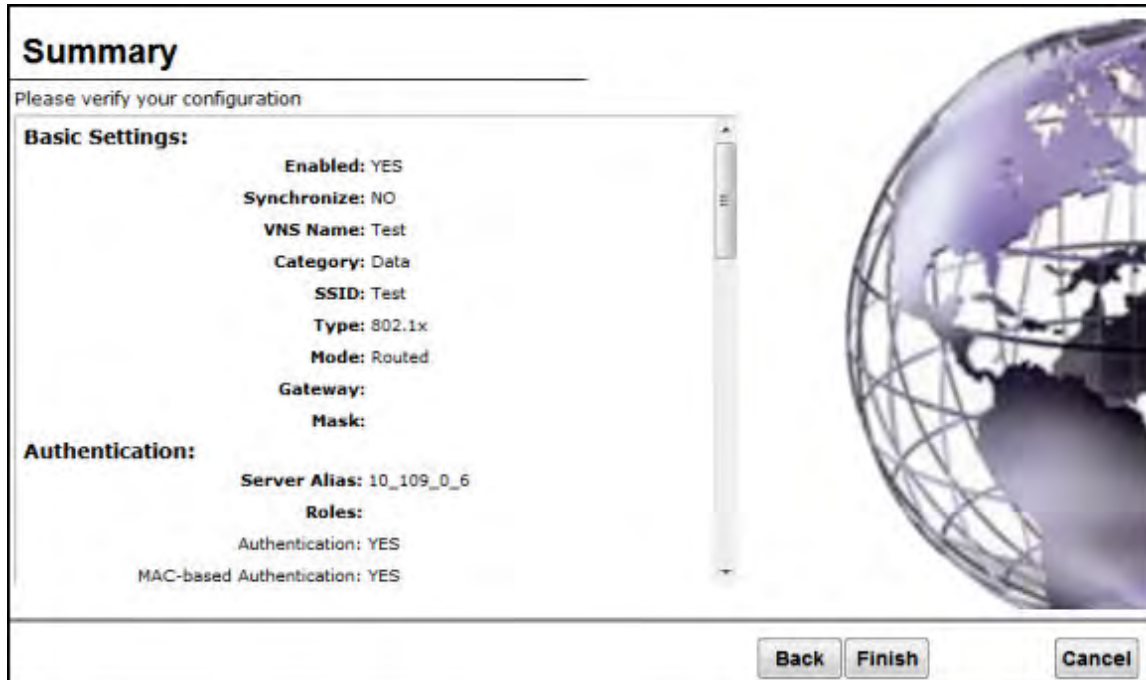
Click **Next**. The **Summary** screen displays.

Creating a Data VNS Using the VNS Wizard - Summary Screen

The **Summary** screen displays:

ExtremeWireless™ V10.41.06 User Guide

445



Summary

Please verify your configuration

Basic Settings:

- Enabled: YES
- Synchronize: NO
- VNS Name: Test
- Category: Data
- SSID: Test
- Type: 802.1x
- Mode: Routed
- Gateway:
- Mask:

Authentication:

- Server Alias: 10_109_0_6
- Roles:
- Authentication: YES
- MAC-based Authentication: YES

Buttons: Back, Finish, Cancel

- 1 Confirm your data VNS configuration. To revise your configuration, click **Back**.
- 2 To create your VNS, click **Finish**, and then click **Close**.
The data VNS is created and saved.
- 3 If applicable, you can continue to configure or edit the new VNS by clicking the individual VNS configuration tabs.
If the controller is configured to be part of an availability pair, you can chose to synchronize the VNS on the secondary controller. See [Availability and Session Availability](#) on page 537 for more information.

Creating a Captive Portal VNS Using the VNS Wizard

Use the VNS wizard to create a Captive Portal VNS. A Captive Portal VNS employs an authentication method that uses a Web redirection which directs a mobile user's Web session to an authentication server. Typically, the mobile user must provide their credentials (user ID, password) to be authenticated. You can create the following types of Captive Portal VNSs:

- **Internal Captive Portal** — The controller's own Captive Portal authentication page — configured as an editable form — is used to request user credentials. The redirection triggers the locally stored authentication page where the mobile user must provide the appropriate credentials, which then is checked against what is listed in the configured RADIUS server.
- **External Captive Portal** — An entity outside of the controller is responsible for handling the mobile user authentication process, presenting the credentials request forms and performing user authentication procedures. The external Web server location must be explicitly listed as an allowed destination in the non-authenticated filter.
- **Firewall Friendly External Captive Portal** — A Firewall Friendly External Captive Portal VNS provides wireless connections to any device on the secure side (behind the Firewall). When you create a new captive portal VNS using the VNS wizard, you configure the VNS in the following stages:

- **GuestPortal** — A GuestPortal VNS provides wireless device users with temporary guest network services.
- Basic settings
- Authentication settings
- DHCP settings
- Filter settings
- Privacy settings
- Radio assignment settings
- Summary review

Related Links

[Creating an Internal Captive Portal VNS](#) on page 447

[Creating an External Captive Portal VNS](#) on page 456

[Creating a Firewall Friendly External Captive Portal VNS](#) on page 467

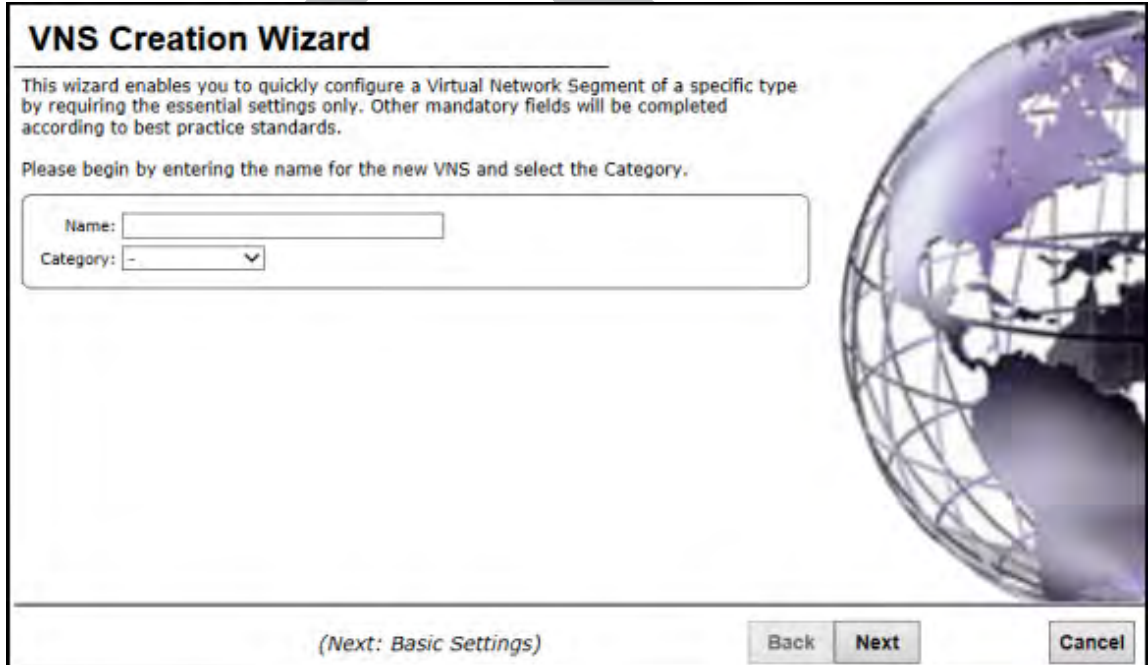
[Creating a GuestPortal VNS](#) on page 477

Creating an Internal Captive Portal VNS

To configure an Internal Captive Portal VNS using the VNS Wizard:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 2 In the left pane, expand the **New** pane, then click **START VNS WIZARD**.

The **VNS Creation Wizard** screen displays.



VNS Creation Wizard

This wizard enables you to quickly configure a Virtual Network Segment of a specific type by requiring the essential settings only. Other mandatory fields will be completed according to best practice standards.

Please begin by entering the name for the new VNS and select the Category.

Name:

Category:

(Next: Basic Settings)

Back Next Cancel

- 3 In the **Name** box, type a name for the Captive Portal VNS.
- 4 In the **Category** drop-down list, click **Captive Portal**.
- 5 Click **Next**. The **Basic Settings** screen displays.

Creating an Internal Captive Portal VNS - Basic Settings Screen

The Basic Settings screen displays:

Basic Settings

Captive Portal 000, Captive Portal

Enabled: ☒

Synchronize: ☐

Name: Captive Portal 000

Category: Captive Portal

SSID: Captive Portal 000

Authentication Mode:

-

Mode:



(Next: Privacy)

BackNextCancel

Table 84: Captive Portal Basic Settings Page - Fields and Buttons

Field/Button	Description
Enabled	By default, the Enabled check box for the new VNS is enabled. A VNS must be enabled for it to be able to provide service for mobile user traffic.
Name	Identifies the name of the VNS.
Category	Identifies the VNS category.
SSID	Identifies the SSID assigned to the VNS.
Authentication Mode	Click Internal Captive Portal
Mode	Click the VNS Mode you want to assign: Routed is a VNS type where user traffic is tunneled to the controller. Bridge Traffic Locally at EWC is a VNS type where user traffic is tunneled to the controller and is directly bridged at the controller to a specific <i>VLAN</i> . With this VNS type, mobile users become a natural extension of a VLAN subnet. For each Bridge Traffic Locally at EWC VNS that is created, a VLAN needs to be specified. In addition, the network port on which the VLAN is assigned must be configured on the switch, and the corresponding controller interface must match the correct VLAN.
Routed Internal Captive Portal	

Table 84: Captive Portal Basic Settings Page - Fields and Buttons (continued)

Field/Button	Description
Gateway	Gateway — Type the controller's own IP address in that VNS. This IP address is the default gateway for the VNS. The controller advertises this address to the wireless devices when they sign on. For routed VNSs, it corresponds to the IP address that is communicated to mobile users (in the VNS) as the default gateway for the VNS subnet. (Mobile users target the controller's interface in their effort to route packets to an external host).
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
Message	Type a brief message that will be displayed above the Login button that greets the mobile device user.
Enable Authentication	By default, this option is selected if the VNS Type is Internal Captive Portal , which enables authentication for the new Captive Portal VNS.
Enable DHCP	By default, this option is selected if the VNS Type is Internal Captive Portal , which enables <u>DHCP</u> authentication for the new Captive Portal VNS.
Bridge Traffic Locally- Voice VNS	
Interface	Click the physical interface that provides the access to the VLAN.
Interface IP address	Type the IP address of the controller's interface on the VLAN.
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
VLAN ID	Type the VLAN tag to which the controller will be bridged for the VNS.
Message	Type a brief message that will be displayed above the Login button that greets the mobile device user.
Enable Authentication	By default, this option is selected if the VNS Type is Internal Captive Portal , which enables authentication for the new Captive Portal VNS.
Enable DHCP	If applicable, select this check box to enable DHCP authentication for the new Captive Portal VNS.

Click **Next**. The **Authentication** screen displays.

Creating an Internal Captive Portal VNS - Authentication Screen

The **Authentication** screen displays:

Authentication

Captive Portal 000, Captive Portal, Internal Captive Portal

Radius Server: Add New Server ▾

Server Alias:

Hostname/IP:

Shared Secret:

Roles: ☒ Authentication
☐ MAC-based Authentication
☐ Accounting



(Next: DHCP)

Table 85: Captive Portal Authentication Page - Fields and Buttons

Field/Button	Description
Radius Server	Click the RADIUS server you want to assign to the new Captive Portal VNS, or click Add New Server and then do the following
Server Alias	Type a name you want to assign to the new RADIUS server.
Hostname/IP	Type either the RADIUS server's FQDN (fully qualified domain name) or IP address.
Shared Secret	Type the password that will be used to validate the connection between the controller and the RADIUS server.
Mask/Unmask	Click to display or hide your shared secret key.
Roles	Select the authentication role options for the RADIUS server: • Authentication — By default, this option is selected if the VNS Type is Internal Captive Portal, which enables the RADIUS server to perform authentication on the Captive Portal VNS. • MAC-based Authentication — Select to enable the RADIUS server to perform MAC-based authentication on the Captive Portal VNS. If the MAC-based authentication option is enabled, select to enable MAC-based authorization on roam, if applicable. • Accounting — Select to enable the RADIUS server to perform accounting on the Captive Portal VNS.

Click **Next**. The **DHCP** screen displays.

Creating an Internal Captive Portal VNS - DHCP Screen

The DHCP screen displays:

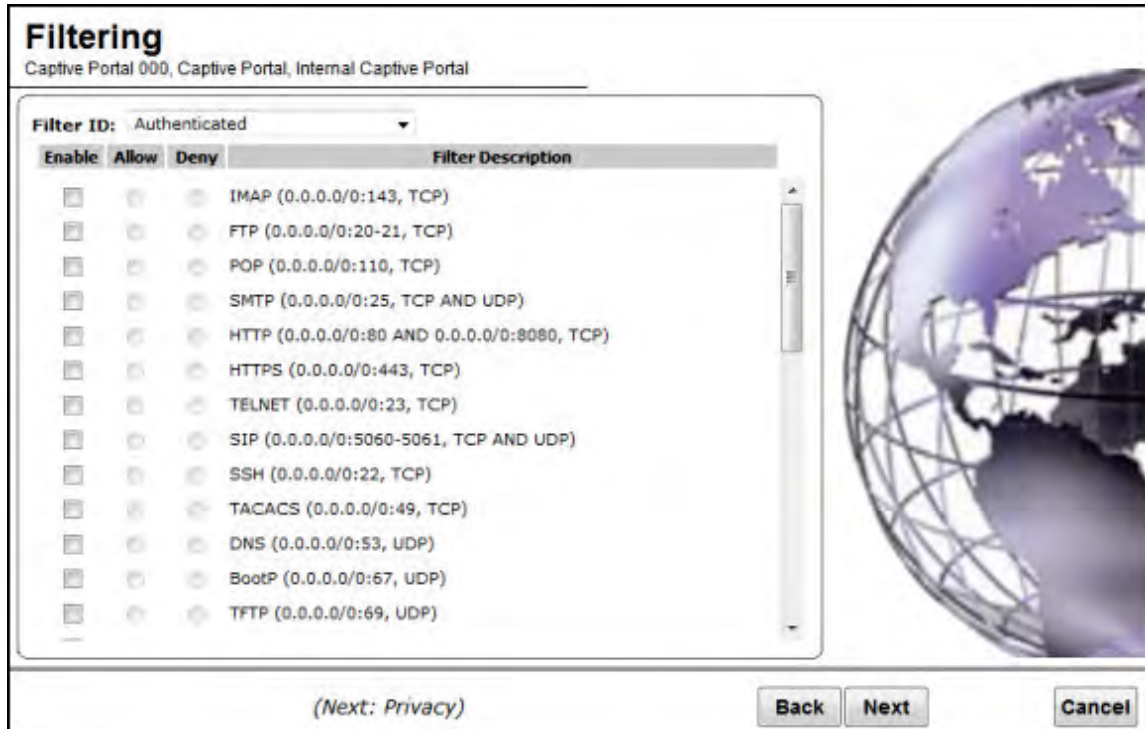
Creating an Internal Captive Portal VNS - Filtering Screen

ExtremeWireless™ V10.41.06 User Guide

ExtremeWireless™ V10.41.06 User Guide

ExtremeWireless™ V10.41.06 User Guide

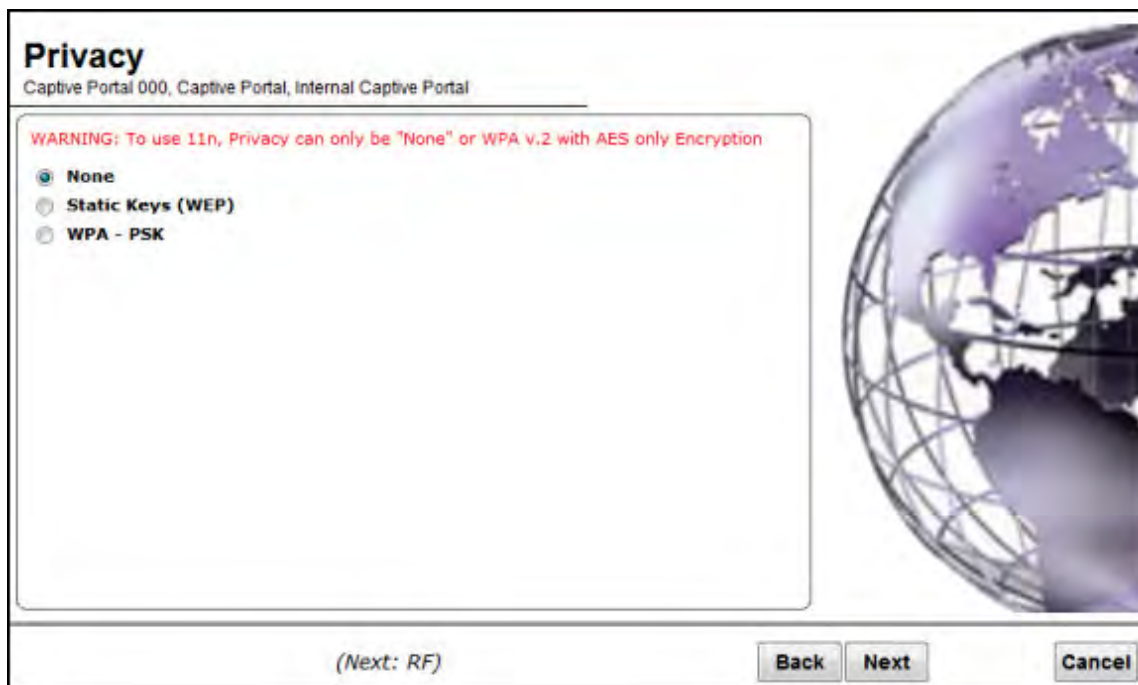
ExtremeWireless™ V10.41.06 User Guide



- 1 In the **Filter ID** drop-down list, click one of the following::
 - **Default** — Controls access if there is no matching filter ID for a user.
 - **Exception** — Protects access to the controller's own interfaces, including the VNSs own interface. VNS exception filters are applied to user traffic intended for the ExtremeWireless Controller's own interface point on the VNS. These filters are applied after the user's specific VNS state assigned filters.
 - **Non-Authenticated** — Controls network access and also used to direct mobile users to a Captive Portal web page for login.
- 2 In the **Filter** table, select the **Allow** or **Deny** option buttons for each filter if applicable, and then select the **Enable** check box accordingly.
- 3 Click **Next**.
The **Privacy** screen displays.

Creating an Internal Captive Portal VNS - Privacy Screen

The **Privacy** screen displays:



Privacy
Captive Portal 000, Captive Portal, Internal Captive Portal

WARNING: To use 11n, Privacy can only be "None" or WPA v.2 with AES only Encryption

☒ None
☐ Static Keys (WEP)
☐ WPA - PSK

(Next: RF) Back Next Cancel

Table 87: Captive Portal Privacy Page - Fields and Buttons

Field/Button	Description
None	Select if you do not want to assign any privacy mechanism.
Static Keys (WEP)	Select to configure static keys. Then enter: WEP Key Index — Click the WEP encryption key index: 1, 2, 3, or 4. Specifying the WEP key index is supported only for AP37XX wireless APs. WEP Key Length — Click the WEP encryption key length: 64 bit, 128 bit, or 152 bit. Select an Input Method: Input Hex — type the WEP key input in the WEP Key box. The key is generated automatically based on the input. Input String — type the secret WEP key string used for encrypting and decrypting in the WEP Key String box. The WEP Key box is automatically filled by the corresponding Hex code.
WPA-PSK	Select to use a Pre-Shared Key (PSK), or shared secret for authentication. WPA-PSK (Wi-Fi Protected Access Pre-Shared key) is a security solution that adds authentication to enhanced WEP encryption and key management. WPA-PSK mode does not require an authentication server. It is suitable for home or small office. To enable WPA v1 encryption, select WPA v.1. In the Encryption drop-down list, select one of the following encryption types: • Auto — The AP will advertise both TKIP and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for WPAv1. CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). • TKIP only — The AP will advertise TKIP as an available encryption protocol for WPAv1. It will not advertise CCMP. To enable WPA v2 encryption, select WPA v.2. In the Encryption drop-down list, click one of the following encryption types: • Auto — The AP advertises both TKIP and CCMP (counter mode with cipher block chaining message authentication code protocol). CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). • AES only — The AP advertises CCMP as an available encryption protocol. It will not advertise TKIP. To enable re-keying after a time interval, select Broadcast re-key interval. If this check box is not selected, the Broadcast encryption key is never changed and the AP will always use the same broadcast key for Broadcast/Multicast transmissions. This will reduce the level of security for wireless communications. In the Broadcast re-key interval box, type the time interval after which the broadcast encryption key is changed automatically. To enable the group key power save retry, select Group Key Power Save Retry. The group key power save retry is supported only for AP37XX wireless APs. In the Pre-shared key box, type the shared secret key to be used between the wireless device and AP. The shared secret key is used to generate the 256-bit key. Mask/Unmask — Click to display or hide your shared secret key.

Click **Next**. The **Radio Assignment** screen displays.

Creating an Internal Captive Portal VNS - Radio Assignment Screen

The Radio Assignment screen displays:

Radio Assignment
Captive Portal 000, Captive Portal, Internal Captive Portal

AP Default Settings
To add this VNS to the AP Default Settings Profile, please select which radio(s) you would like to broadcast this VNS.

☒ Radio 1
☒ Radio 2

AP Selection
Use the drop down list on the left to select the groups of APs and sites that will serve the VNS (such as "All APs" or "radio 1". The list to the right will show the resulting assignment. Note that if your VNS is set to Enabled, and an AP radio or site has the maximum 8 VNSs assigned, the VNS will not be assigned to the AP or site.

Select APs:
WMM: ☐

WARNING: To use 11n, WMM is required.

Radio 1	Radio 2	AP/Site Name
a	b/g	0409920201201314
a	b/g	LAB43-2610-0166
a/n	b/g/n	LAB43-3705i-0000
a/n	b/g	LAB43-3725e-3333
a/n	b/g	LAB43-3725i-3456
a	b/g	LAB47-3620-7024[F]
a/n	b/g/n	LAB47-3705i-0047[F]
a	g	LAB47-W788-1503[F]
a/n	b/g	test
a/n	b/g	test2

(Next: Summary) Back Next Cancel

Table 88: Captive Portal Radio Assignment Page - Fields and Buttons

Field/Button	Description
AP Default Settings	
Radio 1 / Radio 2	Select the radios of the AP default settings profile that you want to broadcast the Captive Portal VNS.
AP Selection	
Select APs	Select the group of APs that will broadcast the Captive Portal VNS: • all radios — Click to assign all of the APs' radios. • radio 1 — Click to assign only the APs' Radio 1. • radio 2 — Click to assign only the APs' Radio 2. • local APs - all radios — Click to assign only the local APs. • local APs - radio 1 — Click to assign only the local APs' Radio 1. • local APs - radio 2 — Click to assign only the local APs' Radio 2. • foreign APs - all radios — Click to assign only the foreign APs. • foreign APs - radio 1 — Click to assign only the foreign APs' Radio 1. • foreign APs - radio 2 — Click to assign only the foreign APs' Radio 2.
WMM	(Wi-Fi Multimedia) If enabled on an individual VNS, provides multimedia enhancements that improve the user experience for audio, video, and voice applications. WMM is part of the 802.11e standard for QoS. If enabled, the AP will accept WMM client associations, and will classify and prioritize the outbound traffic for all WMM clients. WMM clients will also classify and prioritize the inbound traffic.

Click **Next**. The **Summary** screen displays.

Creating an Internal Captive Portal VNS - Summary Screen

The **Summary** screen displays:

Summary

Please verify your configuration

Basic Settings:

Enabled: YES

Synchronize: NO

VNS Name: Captive Portal 000

Category: Captive Portal

SSID: Captive Portal 000

Type: Internal Captive Portal

Mode: Routed

Gateway:

Mask:

Authentication:

Server Alias: 10_109_0_6

Roles:

Authentication: YES

MAC-based Authentication: NO

Back Finish Cancel

- 1 Confirm your data VNS configuration. To revise your configuration, click **Back**.
- 2 To create your VNS, click **Finish**, and then click **Close**.
- 3 If applicable, you can continue to configure or edit the new VNS by clicking the individual VNS configuration tabs.

Creating an External Captive Portal VNS

To configure an external Captive Portal VNS using the VNS wizard:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.

- 2 In the left pane, expand the New pane, then click **START VNS WIZARD**. The VNS Creation Wizard screen displays.

The image shows the 'VNS Creation Wizard' window. At the top, the title is 'VNS Creation Wizard'. Below the title, a paragraph states: 'This wizard enables you to quickly configure a Virtual Network Segment of a specific type by requiring the essential settings only. Other mandatory fields will be completed according to best practice standards.' Below this, a prompt says: 'Please begin by entering the name for the new VNS and select the Category.' There are two input fields: 'Name:' followed by a text box, and 'Category:' followed by a drop-down menu. To the right of the input fields is a large, stylized globe graphic. At the bottom of the window, there is a status bar that says '(Next: Basic Settings)' and three buttons: 'Back', 'Next', and 'Cancel'.

- 3 In the **Name** box, type a name for the Captive Portal VNS.
- 4 In the **Category** drop-down list, click **Captive Portal**.
- 5 Click **Next**. The **Basic Settings** screen displays.

Creating an External Captive Portal VNS - Basic Settings Screen

The **Basic Settings** screen displays:

Basic Settings
EXT Captive Portal, Captive Portal

Enabled: ☒
 Synchronize: ☐
 Name: EXT Captive Portal
 Category: Captive Portal
 SSID: EXT Captive Portal
 Authentication Mode: External Captive Portal
 Mode: Routed
 Gateway:
 Mask:
 HWC Connection: 192.168.3.43 :
 Redirection URL:
 Shared Secret:
 Enable Authentication: ☐
 Enable DHCP: ☒

(Next: DHCP) Back Next Cancel

Table 89: External Captive Portal Basic Settings Page - Fields and Buttons

Field/Button	Description
Enabled	By default, the Enabled check box for the new VNS is enabled. A VNS must be enabled for it to be able to provide service for mobile user traffic.
Synchronize	Synchronize — Enable automatic synchronization with its availability peer. Refer to Using the Sync Summary on page 414 for information about viewing synchronization status. If this VNS is part of an availability pair, Extreme Networks recommends that you enable this feature.
Name	Identifies the name of the VNS.
Category	Identifies the VNS category.
SSID	Identifies the SSID assigned to the VNS.
Authentication Mode	Click External Captive Portal
Mode	Click the VNS Mode you want to assign: • Routed is a VNS type where user traffic is tunneled to the controller. • Bridge Traffic Locally at EWC is a VNS type where user traffic is tunneled to the controller and is directly bridged at the controller to a specific <u>VLAN</u>. With this VNS type, mobile users become a natural extension of a VLAN subnet. For each Bridge Traffic Locally at EWC VNS that is created, a VLAN needs to be specified. In addition, the network port on which the VLAN is assigned must be configured on the switch, and the corresponding controller interface must match the correct VLAN.

Table 89: External Captive Portal Basic Settings Page - Fields and Buttons
(continued)

Field/Button	Description
Routed External Captive Portal	
Gateway	Gateway — Type the controller's own IP address in that VNS. This IP address is the default gateway for the VNS. The controller advertises this address to the wireless devices when they sign on. For routed VNSs, it corresponds to the IP address that is communicated to mobile users (in the VNS) as the default gateway for the VNS subnet. (Mobile users target the controller's interface in their effort to route packets to an external host).
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
EWC Connection	Click the controller IP address. Also type the port of the controller in the accompanying box. If there is an authentication server configured for this VNS, the external Captive Portal page on the external authentication server will send the request back to the controller to allow the controller to continue with the RADIUS authentication and filtering.
Redirection URL	Type the URL to which the wireless device user will be directed to after authentication.
Shared Secret	Type the password that is common to both the controller and the external Web server if you want to encrypt the information passed between the controller and the external Web server.
Enable Authentication	By default, this option is selected if the VNS Type is External Captive Portal , which enables authentication for the new Captive Portal VNS.
Enable DHCP	By default, this option is selected if the VNS Type is External Captive Portal , which enables <i>DHCP</i> services for the new Captive Portal VNS.
EWC External Captive Portal VNS	
Interface	Click the physical interface that provides the access to the VLAN.
Interface IP address	Type the IP address of the controller's interface on the VLAN.
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
VLAN ID	Type the VLAN tag to which the controller will be bridged for the VNS.
EWC Connection	Click the controller IP address. Also type the port of the controller in the accompanying box. If there is an authentication server configured for this VNS, the external Captive Portal page on the external authentication server will send the request back to the controller to allow the controller to continue with the RADIUS authentication and filtering.
Redirection URL	Type the URL to which the wireless device user will be directed to after authentication.
Shared Secret	Type the password that is common to both the controller and the external Web server if you want to encrypt the information passed between the controller and the external Web server.

Table 89: External Captive Portal Basic Settings Page - Fields and Buttons (continued)

Field/Button	Description
Enable Authentication	By default, this option is selected if the VNS Type is External Captive Portal , which enables authentication for the new Captive Portal VNS.
Enable DHCP	If applicable, select this check box to enable DHCP authentication for the new Captive Portal VNS.

Click **Next**. The **Authentication** screen displays.

Creating an External Captive Portal VNS - Authentication Screen

The VNS wizard displays the appropriate configuration screens, depending on your selection of the **Enable Authentication** and **Enable DHCP** check boxes.

Table 90: External Captive Portal Authentication Page - Fields and Buttons

Field/Button	Description
Radius Server	Click the RADIUS server you want to assign to the new Captive Portal VNS, or click Add New Server and then do the following
Server Alias	Type a name you want to assign to the new RADIUS server.
Hostname/IP	Type either the RADIUS server's FQDN (fully qualified domain name) or IP address.
Shared Secret	Type the password that will be used to validate the connection between the controller and the RADIUS server.

**Table 90: External Captive Portal Authentication Page - Fields and Buttons
(continued)**

Field/Button	Description
Mask/Unmask	Click to display or hide your shared secret key.
Roles	Select the authentication role options for the RADIUS server: • Authentication — By default, this option is selected if the VNS Type is External Captive Portal, which enables the RADIUS server to perform authentication on the Captive Portal VNS. • MAC-based Authentication — Select to enable the RADIUS server to perform MAC-based authentication on the Captive Portal VNS. If the MAC-based authentication option is enabled, select to enable MAC-based authorization on roam, if applicable. • Accounting — Select to enable the RADIUS server to perform accounting on the Captive Portal VNS.

Click **Next**. The **DHCP** screen displays.

Creating an External Captive Portal VNS - DHCP Screen

The DHCP screen displays:

DHCP
EXT Captive Portal, Captive Portal, External Captive Portal

DHCP Option: Local DHCP Server ▼

Address Range: From: 127.0.1.2 To: 127.0.1.254

B'cast Address: 127.0.1.255

Lease (seconds): default: 36000 max: 2592000

DNS Servers:

WINS:

(Next: Filtering)

Back Next Cancel

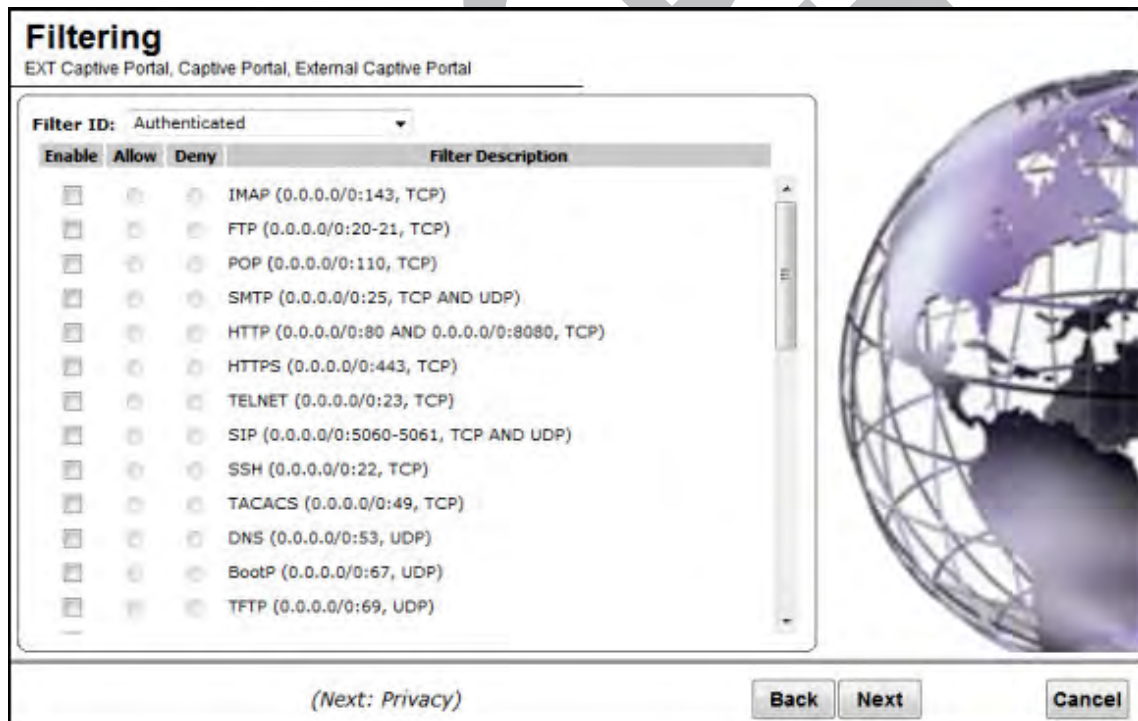
Table 91: External Captive Portal DHCP Page - Fields and Buttons

Field/Button	Description
DHCP Option	In the DHCP Option drop-down list, click one of the following: Use DHCP Relay — Using <i>DHCP</i> relay forces the controller to forward DHCP requests to an external DHCP server on the enterprise network. DHCP relay bypasses the local DHCP server for the controller and allows the enterprise to manage IP address allocation to a VNS from its existing infrastructure. DHCP Servers — If Use DHCP Relay was selected, type the IP address of the DHCP server to which DHCP discover and request messages will be forwarded for clients on this VNS. The controller does not handle DHCP requests from users, but instead forwards the requests to the indicated DHCP server. The DHCP server must be configured to match the VNS settings. In particular for a Routed VNS, the DHCP server must identify the controller's interface IP as the default Gateway (router) for the subnet. (Users intending to reach devices outside of the subnet will forward the packets to the default gateway (controller) for delivery upstream.) Local DHCP Server — If applicable, edit the local DHCP server settings.
DNS Server	Type the IP Address of the Domain Name Servers to be used.
WINS	Type the IP address if the DHCP server uses Windows Internet Naming Service (WINS).

Click **Next**. The **Filtering** screen displays.

Creating an External Captive Portal VNS - Filtering Screen

The **Filtering** screen displays:



Filtering
EXT Captive Portal, Captive Portal, External Captive Portal

Filter ID: Authenticated

Enable	Allow	Deny	Filter Description
☐	☐	☐	IMAP (0.0.0.0/0:143, TCP)
☐	☐	☐	FTP (0.0.0.0/0:20-21, TCP)
☐	☐	☐	POP (0.0.0.0/0:110, TCP)
☐	☐	☐	SMTP (0.0.0.0/0:25, TCP AND UDP)
☐	☐	☐	HTTP (0.0.0.0/0:80 AND 0.0.0.0/0:8080, TCP)
☐	☐	☐	HTTPS (0.0.0.0/0:443, TCP)
☐	☐	☐	TELNET (0.0.0.0/0:23, TCP)
☐	☐	☐	SIP (0.0.0.0/0:5060-5061, TCP AND UDP)
☐	☐	☐	SSH (0.0.0.0/0:22, TCP)
☐	☐	☐	TACACS (0.0.0.0/0:49, TCP)
☐	☐	☐	DNS (0.0.0.0/0:53, UDP)
☐	☐	☐	BootP (0.0.0.0/0:67, UDP)
☐	☐	☐	TFTP (0.0.0.0/0:69, UDP)

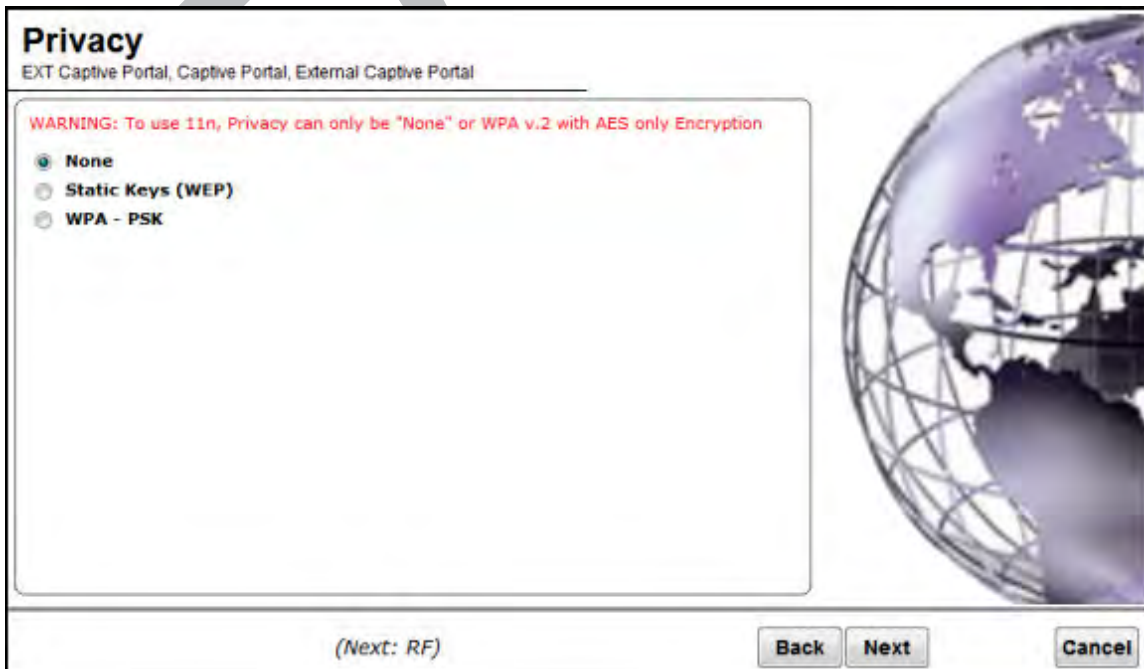
(Next: Privacy)

Back Next Cancel

- 1 In the **Filter ID** drop-down list, click one of the following:
 - **Default** — Controls access if there is no matching filter ID for a user.
 - **Exception** — Protects access to the controller's own interfaces, including the VNSs own interface. VNS exception filters are applied to user traffic intended for the controller's own interface point on the VNS. These filters are applied after the user's specific VNS state assigned filters.
 - **Non-Authenticated** — Controls network access and also used to direct mobile users to a Captive Portal Web page for login.
- 2 In the **Filter** table, select the **Allow** or **Deny** option buttons for each filter if applicable, and then select the **Enable** check box accordingly.
- 3 Click **Next**. The **Privacy** screen displays.

Creating an External Captive Portal VNS - Privacy Screen

The Privacy screen displays:



The screenshot shows the 'Privacy' configuration screen. At the top, the title 'Privacy' is displayed in bold, followed by the subtitle 'EXT Captive Portal, Captive Portal, External Captive Portal'. Below this, a red warning message states: 'WARNING: To use 11n, Privacy can only be "None" or WPA v.2 with AES only Encryption'. There are three radio button options: 'None' (which is selected), 'Static Keys (WEP)', and 'WPA - PSK'. On the right side of the screen, there is a graphic of a globe. At the bottom of the screen, there is a status indicator '(Next: RF)' and three buttons: 'Back', 'Next', and 'Cancel'.

Table 92: External Captive Portal Privacy Page - Fields and Buttons

Field/Button	Description
None	Select if you do not want to assign any privacy mechanism.
Static Keys (WEP)	Select to configure static keys. Then enter: • WEP Key Index — Click the WEP encryption key index: 1, 2, 3, or 4. Specifying the WEP key index is supported only for AP37XX wireless APs. • WEP Key Length — Click the WEP encryption key length: 64 bit, 128 bit, or 152 bit. Select an Input Method: • Input Hex — type the WEP key input in the WEP Key box. The key is generated automatically based on the input. • Input String — type the secret WEP key string used for encrypting and decrypting in the WEP Key String box. The WEP Key box is automatically filled by the corresponding Hex code.
WPA-PSK	Select to use a Pre-Shared Key (PSK), or shared secret for authentication. WPA-PSK (Wi-Fi Protected Access Pre-Shared key) is a security solution that adds authentication to enhanced WEP encryption and key management. WPA-PSK mode does not require an authentication server. It is suitable for home or small office. To enable WPA v1 encryption, select WPA v.1. In the Encryption drop-down list, select one of the following encryption types: • Auto — The AP will advertise both TKIP and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for WPAv1. CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). • TKIP only — The AP will advertise TKIP as an available encryption protocol for WPAv1. It will not advertise CCMP. To enable WPA v2 encryption, select WPA v.2. In the Encryption drop-down list, click one of the following encryption types: • Auto — The AP advertises both TKIP and CCMP (counter mode with cipher block chaining message authentication code protocol). CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). • AES only — The AP advertises CCMP as an available encryption protocol. It will not advertise TKIP. To enable re-keying after a time interval, select Broadcast re-key interval. If this check box is not selected, the Broadcast encryption key is never changed and the AP will always use the same broadcast key for Broadcast/Multicast transmissions. This will reduce the level of security for wireless communications. In the Broadcast re-key interval box, type the time interval after which the broadcast encryption key is changed automatically. To enable the group key power save retry, select Group Key Power Save Retry. The group key power save retry is supported only for AP37XX Wireless APs.

Table 92: External Captive Portal Privacy Page - Fields and Buttons (continued)

Field/Button	Description
	In the Pre-shared key box, type the shared secret key to be used between the wireless device and AP. The shared secret key is used to generate the 256-bit key. Mask/Unmask — Click to display or hide your shared secret key.

Click **Next**. The **Radio Assignment** screen displays.

Creating an External Captive Portal VNS - Radio Assignment Screen

The Radio Assignment screen displays:

Radio Assignment
EXT Captive Portal, Captive Portal, External Captive Portal

AP Default Settings
To add this VNS to the AP Default Settings Profile, please select which radio(s) you would like to broadcast this VNS.
☒ Radio 1
☒ Radio 2

AP Selection
Use the drop down list on the left to select the groups of APs and sites that will serve the VNS (such as "All APs" or "radio 1"). The list to the right will show the resulting assignment. Note that if your VNS is set to Enabled, and an AP radio or site has the maximum 8 VNSs assigned, the VNS will not be assigned to the AP or site.

Select APs:
WMM: ☐
WARNING: To use 11n, WMM is required.

Radio 1	Radio 2	AP/Site Name
a	b/g	0409920201201314
a	b/g	LAB43-2610-0166
a/n	b/g/n	LAB43-3705i-0000
a/n	b/g	LAB43-3725e-3333
a/n	b/g	LAB43-3725i-3456
a	b/g	LAB47-3620-7024[F]
a/n	b/g/n	LAB47-3705i-0047[F]
a	g	LAB47-W788-1503[F]
a/n	b/g	test
a/n	b/g	test2

(Next: Summary) Back Next Cancel

Table 93: External Captive Portal Radio Assignment Page - Fields and Buttons

Field/Button	Description
AP Default Settings	
Radio 1 / Radio 2	Select the radios of the AP default settings profile that you want to broadcast the Captive Portal VNS.
AP Selection	

Table 93: External Captive Portal Radio Assignment Page - Fields and Buttons (continued)

Field/Button	Description
Select APs	Select the group of APs that will broadcast the Captive Portal VNS: • all radios — Click to assign all of the APs' radios. • radio 1 — Click to assign only the APs' Radio 1. • radio 2 — Click to assign only the APs' Radio 2. • local APs - all radios — Click to assign only the local APs. • local APs - radio 1 — Click to assign only the local APs' Radio 1. • local APs - radio 2 — Click to assign only the local APs' Radio 2. • foreign APs - all radios — Click to assign only the foreign APs. • foreign APs - radio 1 — Click to assign only the foreign APs' Radio 1. • foreign APs - radio 2 — Click to assign only the foreign APs' Radio 2.
WMM	(Wi-Fi Multimedia), if enabled on an individual VNS, provides multimedia enhancements that improve the user experience for audio, video, and voice applications. WMM is part of the 802.11e standard for QoS. If enabled, the AP will accept WMM client associations, and will classify and prioritize the outbound traffic for all WMM clients. WMM clients will also classify and prioritize the inbound traffic.

Click **Next**. The **Summary** screen displays.

Creating an External Captive Portal VNS - Summary Screen

The **Summary** screen displays:

Summary

Please verify your configuration

Basic Settings:

Enabled: YES

Synchronize: NO

VNS Name: EXT Captive Portal

Category: Captive Portal

SSID: EXT Captive Portal

Type: External Captive Portal

Mode: Routed

Gateway:

Mask:

HWC Connection: 192.168.3.43:

Redirection URL:

Shared Secret:

Authentication:

Server Alias: 10_109_0_6

Back Finish Cancel

- 1 Confirm your data VNS configuration. To revise your configuration, click **Back**.
- 2 To create your VNS, click **Finish**, and then click **Close**.

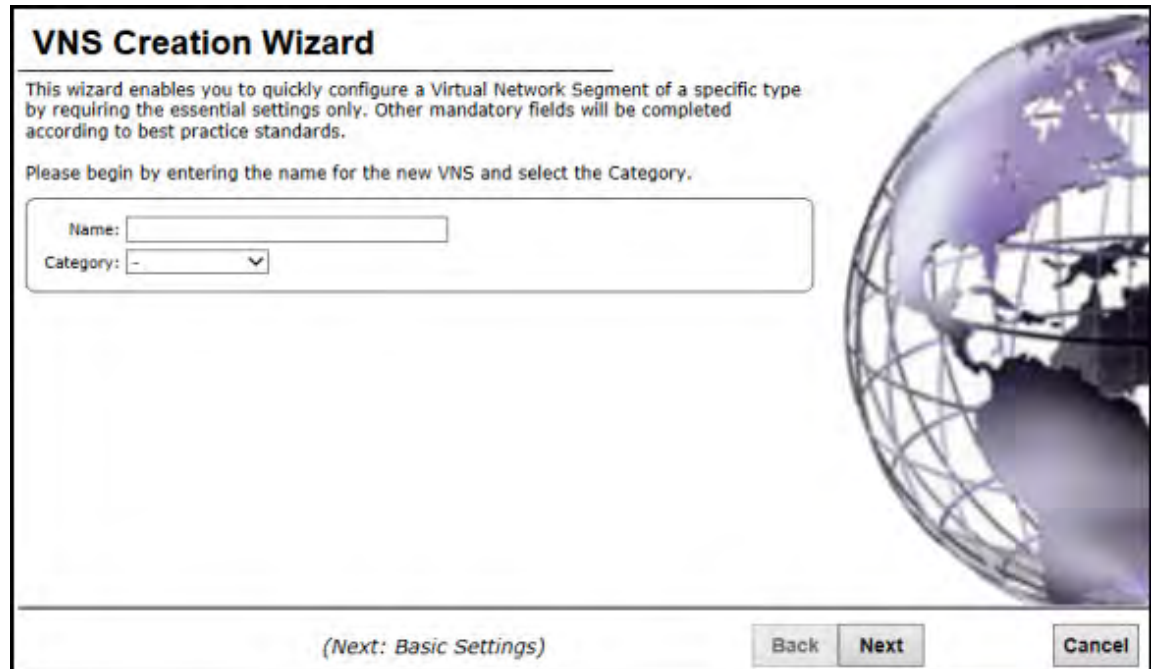
- 3 If applicable, you can continue to configure or edit the new VNS by clicking the individual VNS configuration tabs.

Creating a Firewall Friendly External Captive Portal VNS

To configure a Firewall Friendly External Captive Portal VNS using the VNS wizard:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 2 In the left pane, click **New**, then click **START VNS WIZARD**.

The VNS Creation Wizard displays.



- 3 In the **Name** box, type a name for the Firewall Friendly Captive Portal VNS.
- 4 In the **Category** drop-down list, click **Captive Portal**.
- 5 Click **Next**. The **Basic Settings** screen displays.

If applicable, you can continue to configure or edit the new VNS by clicking the individual VNS configuration tabs.

Creating a Firewall Friendly External Captive Portal VNS - Basic Settings Screen

The **Basic Settings** screen displays:

[Logout](#)

Basic Settings

FF EXT Captive Portal, Captive Portal

Enabled: ☒

Synchronize: ☐

Name: FF EXT Captive Portal

Category: Captive Portal

SSID:

Authentication Mode:

Mode:

Gateway:

Mask:

VLAN ID: (1 - 4094) ☐ Untagged ☐ Tagged

Redirection URL:

Identity:

Shared Secret:

Enable Authentication: ☐

Enable DHCP: ☒

(Next: DHCP)



Table 94: Firewall Friendly External Captive Portal Basic Settings Page - Fields and Buttons

Field/Button	Description
Enabled	By default, the Enabled check box for the new VNS is enabled. A VNS must be enabled for it to be able to provide service for mobile user traffic.
Name	Identifies the name of the VNS.
Category	Identifies the VNS category.
SSID	Identifies the SSID assigned to the VNS.
Authentication Mode	Click External Captive Portal
Mode	Click the VNS Mode you want to assign: Routed is a VNS type where user traffic is tunneled to the controller. Bridge Traffic Locally at EWC is a VNS type where user traffic is tunneled to the controller and is directly bridged at the controller to a specific <u>VLAN</u>. With this VNS type, mobile users become a natural extension of a VLAN subnet. For each Bridge Traffic Locally at EWC VNS that is created, a VLAN needs to be specified. In addition, the network port on which the VLAN is assigned must be configured on the switch, and the corresponding controller interface must match the correct VLAN.

Table 94: Firewall Friendly External Captive Portal Basic Settings Page - Fields and Buttons (continued)

Field/Button	Description
Gateway	Gateway — Type the controller's own IP address in that VNS. This IP address is the default gateway for the VNS. The controller advertises this address to the wireless devices when they sign on. For routed VNSs, it corresponds to the IP address that is communicated to mobile users (in the VNS) as the default gateway for the VNS subnet. (Mobile users target the controller's interface in their effort to route packets to an external host).
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
Redirection URL	Type the URL to which the wireless device user will be directed to after authentication.
Shared Secret	Type the password that is common to both the controller and the external Web server if you want to encrypt the information passed between the controller and the external Web server.
Enable Authentication	By default, this option is selected if the VNS Type is External Captive Portal , which enables authentication for the new Captive Portal VNS.
Enable DHCP	By default, this option is selected if the VNS Type is External Captive Portal , which enables <i>DHCP</i> services for the new Captive Portal VNS.
Interface	Click the physical interface that provides the access to the VLAN.
Interface IP address	Type the IP address of the controller's interface on the VLAN.
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
VLAN ID	Type the VLAN tag to which the controller will be bridged for the VNS.
EWC Connection	Click the controller IP address. Also type the port of the controller in the accompanying box. If there is an authentication server configured for this VNS, the external Captive Portal page on the external authentication server will send the request back to the controller to allow the controller to continue with the RADIUS authentication and filtering.
Redirection URL	Type the URL to which the wireless device user will be directed to after authentication.
Shared Secret	Type the password that is common to both the controller and the external Web server if you want to encrypt the information passed between the controller and the external Web server.
Enable Authentication	By default, this option is selected if the VNS Type is External Captive Portal , which enables authentication for the new Captive Portal VNS.
Enable DHCP	If applicable, select this check box to enable DHCP authentication for the new Captive Portal VNS.

Click **Next**. The **Authentication** screen displays.

Creating a Firewall Friendly External Captive Portal VNS - Authentication Screen

The VNS wizard displays the appropriate configuration screens, depending on your selection of the **Enable Authentication** and **Enable DHCP** check boxes.

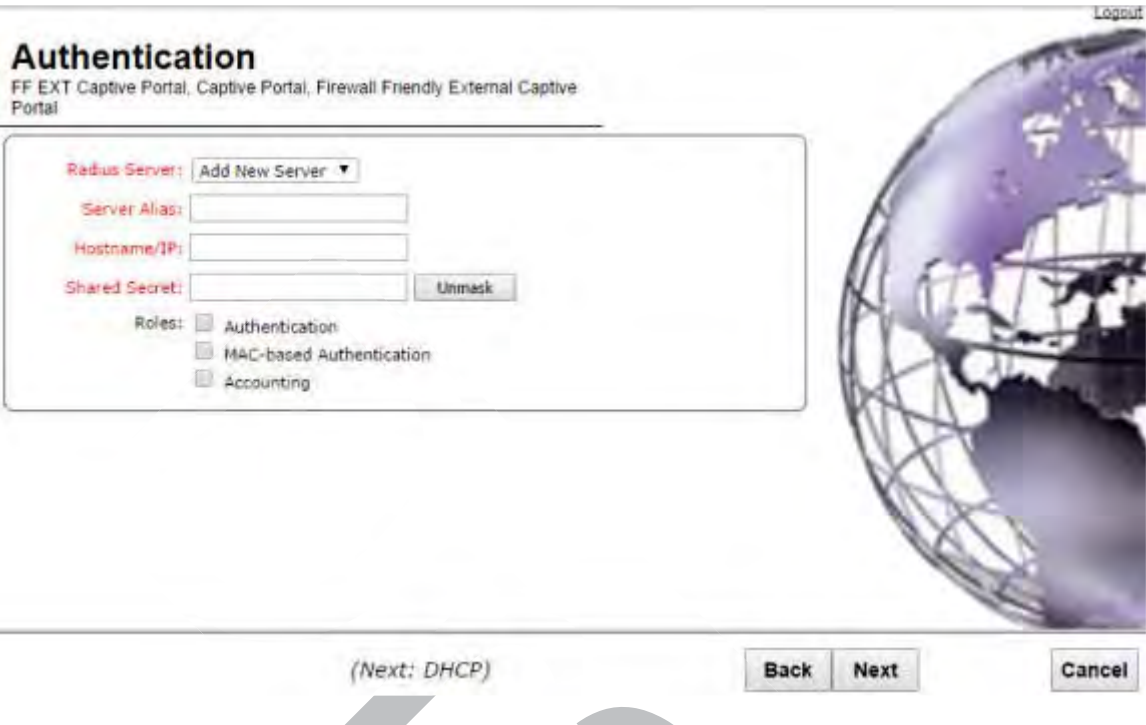


Table 95: Firewall Friendly External Captive Portal Authentication Page - Fields and Buttons

Field/Button	Description
Radius Server	Click the RADIUS server you want to assign to the new Captive Portal VNS, or click Add New Server and then do the following
Server Alias	Type a name you want to assign to the new RADIUS server.
Hostname/IP	Type either the RADIUS server's FQDN (fully qualified domain name) or IP address.
Shared Secret	Type the password that will be used to validate the connection between the controller and the RADIUS server.
Mask/Unmask	Click to display or hide your shared secret key.
Roles	Select the authentication role options for the RADIUS server: • Authentication — By default, this option is selected if the VNS Type is External Captive Portal, which enables the RADIUS server to perform authentication on the Captive Portal VNS. • MAC-based Authentication — Select to enable the RADIUS server to perform MAC-based authentication on the Captive Portal VNS. If the MAC-based authentication option is enabled, select to enable MAC-based authorization on roam, if applicable. • Accounting — Select to enable the RADIUS server to perform accounting on the Captive Portal VNS.

Click **Next**. The **DHCP** screen displays.

Creating a Firewall Friendly External Captive Portal VNS - DHCP Screen

The DHCP screen displays:

Logout

DHCP
FF EXT Captive Portal, Captive Portal, Firewall Friendly External Captive Portal

DHCP Option: Local DHCP Server ▼

Address Range: From: 192.168.101.1 To: 192.168.101.254

B'cast Address: 192.168.101.255

Lease (seconds): default: 36000 max: 2592000

DNS Servers:

WINS:

(Next: Filtering)

Back Next Cancel

Table 96: External Captive Portal DHCP Page - Fields and Buttons

Field/Button	Description
DHCP Option	In the DHCP Option drop-down list, click one of the following: • Use DHCP Relay — Using <i>DHCP</i> relay forces the controller to forward DHCP requests to an external DHCP server on the enterprise network. DHCP relay bypasses the local DHCP server for the controller and allows the enterprise to manage IP address allocation to a VNS from its existing infrastructure. • DHCP Servers — If Use DHCP Relay was selected, type the IP address of the DHCP server to which DHCP discover and request messages will be forwarded for clients on this VNS. The controller does not handle DHCP requests from users, but instead forwards the requests to the indicated DHCP server. The DHCP server must be configured to match the VNS settings. In particular for a Routed VNS, the DHCP server must identify the controller's interface IP as the default Gateway (router) for the subnet. (Users intending to reach devices outside of the subnet will forward the packets to the default gateway (controller) for delivery upstream.) • Local DHCP Server — If applicable, edit the local DHCP server settings.
DNS Server	Type the IP Address of the Domain Name Servers to be used.
WINS	Type the IP address if the DHCP server uses Windows Internet Naming Service (WINS).

Click **Next**. The **Filtering** screen displays.

Creating a Firewall Friendly External Captive Portal VNS - Filtering Screen

The **Filtering** screen displays:

Filtering
FF EXT Captive Portal, Captive Portal, Firewall Friendly External Captive Portal

Filter ID: Authenticated

Enable	Allow	Deny	Filter Description
☐	☐	☐	IMAP (0.0.0.0/0:143, TCP)
☐	☐	☐	FTP (0.0.0.0/0:20-21, TCP)
☐	☐	☐	POP (0.0.0.0/0:110, TCP)
☐	☐	☐	SMTP (0.0.0.0/0:25, TCP AND UDP)
☐	☐	☐	HTTP (0.0.0.0/0:80 AND 0.0.0.0/0:8080, TCP)
☐	☐	☐	HTTPS (0.0.0.0/0:443, TCP)
☐	☐	☐	TELNET (0.0.0.0/0:23, TCP)
☐	☐	☐	SIP (0.0.0.0/0:5060-5061, TCP AND UDP)
☐	☐	☐	SSH (0.0.0.0/0:22, TCP)
☐	☐	☐	TACACS (0.0.0.0/0:49, TCP)
☐	☐	☐	DNS (0.0.0.0/0:53, UDP)
☐	☐	☐	TFTP (0.0.0.0/0:69, UDP)
☐	☐	☐	Finger (0.0.0.0/0:79, TCP)
☐	☐	☐	Portmapper (0.0.0.0/0:111, UDP)

(Next: Privacy) Back Next Cancel

- In the **Filter ID** drop-down list, click one of the following:
 - Default** — Controls access if there is no matching filter ID for a user.
 - Exception** — Protects access to the controller's own interfaces, including the VNSs own interface. VNS exception filters are applied to user traffic intended for the controller's own interface point on the VNS. These filters are applied after the user's specific VNS state assigned filters.
 - Non-Authenticated** — Controls network access and also used to direct mobile users to a Captive Portal Web page for login.
- In the **Filter** table, select the **Allow** or **Deny** option buttons for each filter if applicable, and then select the **Enable** check box accordingly.
- Click **Next**. The **Privacy** screen displays.

Creating a Firewall Friendly External Captive Portal VNS - Privacy Screen

The **Privacy** screen displays:

Logout

Privacy

FF EXT Captive Portal, Captive Portal, Firewall Friendly External Captive Portal

WARNING: To use 11n, Privacy can only be "None" or WPA v.2 with AES only Encryption

☒ None
☐ Static Keys (WEP)
☐ WPA - PSK



(Next: RF)

Back Next Cancel

Table 97: External Captive Portal Privacy Page - Fields and Buttons

Field/Button	Description
None	Select if you do not want to assign any privacy mechanism.
Static Keys (WEP)	Select to configure static keys. Then enter: • WEP Key Index — Click the WEP encryption key index: 1, 2, 3, or 4. Specifying the WEP key index is supported only for AP37XX wireless APs. • WEP Key Length — Click the WEP encryption key length: 64 bit, 128 bit, or 152 bit. Select an Input Method: • Input Hex — type the WEP key input in the WEP Key box. The key is generated automatically based on the input. • Input String — type the secret WEP key string used for encrypting and decrypting in the WEP Key String box. The WEP Key box is automatically filled by the corresponding Hex code.
WPA-PSK	Select to use a Pre-Shared Key (PSK), or shared secret for authentication. WPA-PSK (Wi-Fi Protected Access Pre-Shared key) is a security solution that adds authentication to enhanced WEP encryption and key management. WPA-PSK mode does not require an authentication server. It is suitable for home or small office. To enable WPA v1 encryption, select WPA v.1. In the Encryption drop-down list, select one of the following encryption types: • Auto — The AP will advertise both TKIP and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for WPAv1. CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). • TKIP only — The AP will advertise TKIP as an available encryption protocol for WPAv1. It will not advertise CCMP. To enable WPA v2 encryption, select WPA v.2. In the Encryption drop-down list, click one of the following encryption types: • Auto — The AP advertises both TKIP and CCMP (counter mode with cipher block chaining message authentication code protocol). CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). • AES only — The AP advertises CCMP as an available encryption protocol. It will not advertise TKIP. To enable re-keying after a time interval, select Broadcast re-key interval. If this check box is not selected, the Broadcast encryption key is never changed and the AP will always use the same broadcast key for Broadcast/Multicast transmissions. This will reduce the level of security for wireless communications. In the Broadcast re-key interval box, type the time interval after which the broadcast encryption key is changed automatically. To enable the group key power save retry, select Group Key Power Save Retry. The group key power save retry is supported only for AP37XX wireless APs. In the Pre-shared key box, type the shared secret key to be used between the wireless device and AP. The shared secret key is used to generate the 256-bit key.

Table 97: External Captive Portal Privacy Page - Fields and Buttons (continued)

Field/Button	Description
	Mask/Unmask — Click to display or hide your shared secret key.

Click **Next**. The **Radio Assignment** screen displays.

Creating a Firewall Friendly External Captive Portal VNS - Radio Assignment Screen

The Radio Assignment screen displays:

Radio Assignment
FF EXT Captive Portal, Captive Portal, Firewall Friendly External Captive Portal

Logout

AP Default Settings
To add this VNS to the AP Default Settings Profile, please select which radio(s) you would like to broadcast this VNS.

☒ Radio 1
☒ Radio 2

AP Selection
Use the drop down list on the left to select the groups of APs and sites that will serve the VNS (such as "All APs" or "radio 1"). The list to the right will show the resulting assignment. Note that if your VNS is set to Enabled, and an AP radio or site has the maximum 8 VNSs assigned, the VNS will not be assigned to the AP or site.

Select APs: [v]
WMM: ☒
WARNING: To use 11n, WMM is required.

Radio 1	Radio 2	AP/Site Name
a	b/g	AP2660 Dummy
a/n	b/g	AP3660 Dummy
a/n	b/g	AP3705i Dummy
a/n	b/g	AP3715e Dummy
a/n	b/g	AP3715i Dummy
a/n	b/g	AP3765e[F]
a/n	b/g	AP3765i Dummy
a/n/ac	b/g/n	ap3805_t
a/n/ac	b/g/n	AP3825i Dummy

(Next: Summary) [Back] [Next] [Cancel]

Table 98: External Captive Portal Radio Assignment Page - Fields and Buttons

Field/Button	Description
AP Default Settings	
Radio 1 / Radio 2	Select the radios of the AP default settings profile that you want to broadcast the Captive Portal VNS.
AP Selection	

Table 98: External Captive Portal Radio Assignment Page - Fields and Buttons (continued)

Field/Button	Description
Select APs	Select the group of APs that will broadcast the Captive Portal VNS: • all radios — Click to assign all of the APs' radios. • radio 1 — Click to assign only the APs' Radio 1. • radio 2 — Click to assign only the APs' Radio 2. • local APs - all radios — Click to assign only the local APs. • local APs - radio 1 — Click to assign only the local APs' Radio 1. • local APs - radio 2 — Click to assign only the local APs' Radio 2. • foreign APs - all radios — Click to assign only the foreign APs. • foreign APs - radio 1 — Click to assign only the foreign APs' Radio 1. • foreign APs - radio 2 — Click to assign only the foreign APs' Radio 2.
WMM	(Wi-Fi Multimedia), if enabled on an individual VNS, provides multimedia enhancements that improve the user experience for audio, video, and voice applications. WMM is part of the 802.11e standard for QoS. If enabled, the AP will accept WMM client associations, and will classify and prioritize the outbound traffic for all WMM clients. WMM clients will also classify and prioritize the inbound traffic.

Click **Next**. The **Summary** screen displays.

Creating a Firewall Friendly External Captive Portal VNS - Summary Screen

The **Summary** screen displays:

Summary

Please verify your configuration

Basic Settings:

- Enabled: YES
- Synchronize: NO
- VNS Name: FF EXT Captive Portal
- Category: Captive Portal
- SSID: FF EXT Captive Portal
- Type: Firewall Friendly External Captive Portal
- Mode: Routed
- Gateway: 192.168.101.2
- Mask: 255.255.255.0
- VLAN TAG: Untagged
- VLAN ID: 4094

Authentication:

- Radius Server: Add New Server
- Server Alias: test

Logout

Back Finish Cancel

- 1 Confirm your data VNS configuration. To revise your configuration, click **Back**.
- 2 To create your VNS, click **Finish**, and then click **Close**.

Creating a GuestPortal VNS

A GuestPortal provides wireless device users with temporary guest network services. A GuestPortal is serviced by a GuestPortal-dedicated VNS. A controller is allowed only one GuestPortal-dedicated VNS at a time. GuestPortal user accounts are administered by a GuestPortal manager. A GuestPortal manager is a login group — GuestPortal managers must have their accounts created for them on the controller. For more information, see [Working with GuestPortal Administration](#) on page 690

The GuestPortal VNS is a Captive Portal authentication-based VNS that uses a database on the controller for managing user accounts. The database is administered through a simple, user-friendly graphic user interface that can be used by non-technical staff.

The GuestPortal VNS can be a Routed or a Bridge Traffic Locally at the EWC VNS, with SSID-based network assignment. The GuestPortal VNS is a simplified VNS. It does not support the following:

- RADIUS authentication or accounting
- MAC-based authorization
- Child VNS support

The GuestPortal VNS can be created as a new VNS or can be configured from an already existing VNS. When you create a new VNS using the VNS wizard, you configure the VNS in the following stages:

- Basic settings
- *DHCP* settings
- Filter settings
- Privacy settings
- Radio assignment settings
- Summary

Use the following high-level description to set up a GuestPortal on your system:

- 1 Create a GuestPortal VNS.
The GuestPortal VNS can be created as a new VNS or can be configured from an already existing VNS.
- 2 Configure the GuestPortal ticket.
A GuestPortal account ticket is a print-ready form that displays the guest account information, system requirements, and instructions on how to log on to the guest account. For more information, see [Working with the Guest Portal Ticket Page](#) on page 700.
- 3 Configure availability, if applicable.
Availability maintains service availability in the event of a controller outage. For more information, see [Availability and Session Availability](#) on page 537.
- 4 Create GuestPortal manager and user accounts.
For more information, see [Working with GuestPortal Administration](#) on page 690.
- 5 Manage your guest accounts and GuestPortal logs.
For more information, see the Extreme Networks *ExtremeWireless Maintenance Guide*.

Creating a GuestPortal VNS from an Existing VNS

The GuestPortal VNS can be created as a new VNS or can be configured from an already existing VNS. A controller is allowed only one GuestPortal-dedicated VNS at a time.

To create a GuestPortal VNS from an already existing VNS:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 2 In the left pane, select and expand the **Virtual Networks** pane.
- 3 Click on the VNS you want to configure as a GuestPortal VNS. The VNS configuration window **Core** tab is displayed.
- 4 Select a preconfigured **WLAN** Service and click **Edit**, or press **New** to create a new WLAN Service.
- 5 In the Edit WLAN Service window, click the **Auth & Acct** tab
- 6 In the **Authentication Mode** drop-down list, click **GuestPortal**.
- 7 To save your changes, click **Save**.

Creating a New GuestPortal VNS Using the VNS Wizard

To create a new GuestPortal VNS using the VNS Wizard:

- 1 From the top menu, click **VNS**. The **Virtual Network Configuration** screen displays.
- 2 In the left pane, expand the **New** pane, and then click **START VNS WIZARD**.

The VNS Creation Wizard displays.



- 3 In the **Name** box, type a name for the GuestPortal VNS.
- 4 In the **Category** drop-down list, click **Captive Portal**.
- 5 Click **Next**. The **Basic Settings** screen displays.

Creating a New GuestPortal VNS Using the VNS Wizard - Basic Settings Screen

The **Basic Settings** screen displays:

Basic Settings
Guest-Portal, Captive Portal

Enabled: ☒
 Synchronize: ☐
 Name: Guest-Portal
 Category: Captive Portal
 SSID: Guest-Portal
 Authentication Mode: GuestPortal
 Mode: Routed
 Gateway:
 Mask:
 Enable DHCP: ☒

(Next: DHCP)

Back Next Cancel

Table 99: Guest Portal Basic Settings Page - Fields and Buttons

Field/Button	Description
Enabled	By default, the Enabled check box for the new VNS is enabled. A VNS must be enabled for it to be able to provide service for mobile user traffic.
Synchronize	By default, the Synchronize check box for the new VNS is disabled.
Name	Identifies the name of the VNS.
Category	Identifies the VNS category.
SSID	Identifies the SSID assigned to the VNS.
Authentication Mode	Click Guest Portal
Mode	Click the VNS Mode you want to assign: • Routed is a VNS type where user traffic is tunneled to the controller. • Bridge Traffic Locally at EWC is a VNS type where user traffic is tunneled to the controller and is directly bridged at the controller to a specific <u>VLAN</u>. With this VNS type, mobile users become a natural extension of a VLAN subnet. For each Bridge Traffic Locally at EWC VNS that is created, a VLAN needs to be specified. In addition, the network port on which the VLAN is assigned must be configured on the switch, and the corresponding controller interface must match the correct VLAN.
Routed	

Table 99: Guest Portal Basic Settings Page - Fields and Buttons (continued)

Field/Button	Description
Gateway	Gateway — Type the controller's own IP address in that VNS. This IP address is the default gateway for the VNS. The controller advertises this address to the wireless devices when they sign on. For routed VNSs, it corresponds to the IP address that is communicated to mobile users (in the VNS) as the default gateway for the VNS subnet. (Mobile users target the controller's interface in their effort to route packets to an external host).
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
Bridge Traffic Locally at EWC	
Interface	Click the physical interface that provides the access to the VLAN.
Interface IP address	Type the IP address of the controller's interface on the VLAN.
Mask	Type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).
VLAN ID	Type the VLAN to which the controller will be bridged for the VNS. Then, select either Untagged or Tagged .
Enable DHCP	If applicable, select this check box to enable <i>DHCP</i> .

Click **Next**. The **DHCP** screen displays.

Creating a New GuestPortal VNS Using the VNS Wizard - DHCP Screen

The **DHCP** screen displays:

DHCP
Guest Portal, Captive Portal, External Captive Portal

DHCP Option: Local DHCP Server ▼

Address Range: From: 127.0.1.2
To: 127.0.1.254

B'cast Address: 127.0.1.255

Lease (seconds): default: 36000 max: 2592000

DNS Servers:

WINS:

(Next: Filtering)

Back Next Cancel

Table 100: Guest Portal DHCP Page - Fields and Buttons

Field/Button	Description
DHCP Option	In the DHCP Option drop-down list, click one of the following: Use DHCP Relay — Using <i>DHCP</i> relay forces the controller to forward DHCP requests to an external DHCP server on the enterprise network. DHCP relay bypasses the local DHCP server for the controller and allows the enterprise to manage IP address allocation to a VNS from its existing infrastructure. DHCP Servers — If Use DHCP Relay was selected, type the IP address of the DHCP server to which DHCP discover and request messages will be forwarded for clients on this VNS. The controller does not handle DHCP requests from users, but instead forwards the requests to the indicated DHCP server. The DHCP server must be configured to match the VNS settings. In particular for a Routed VNS, the DHCP server must identify the controller's interface IP as the default Gateway (router) for the subnet. (Users intending to reach devices outside of the subnet will forward the packets to the default gateway (controller) for delivery upstream.) Local DHCP Server — If applicable, edit the local DHCP server settings.
DNS Server	Type the IP Address of the Domain Name Servers to be used.
WINS	Type the IP address if the DHCP server uses Windows Internet Naming Service (WINS).

Click **Next**. The **Filtering** screen displays.

Creating a New GuestPortal VNS Using the VNS Wizard - Filtering Screen

The **Filtering** screen displays:

Filtering
Guest Portal, Captive Portal, External Captive Portal

Filter ID: Authenticated

Enable	Allow	Deny	Filter Description
☐	☐	☐	IMAP (0.0.0.0/0:143, TCP)
☐	☐	☐	FTP (0.0.0.0/0:20-21, TCP)
☐	☐	☐	POP (0.0.0.0/0:110, TCP)
☐	☐	☐	SMTP (0.0.0.0/0:25, TCP AND UDP)
☐	☐	☐	HTTP (0.0.0.0/0:80 AND 0.0.0.0/0:8080, TCP)
☐	☐	☐	HTTPS (0.0.0.0/0:443, TCP)
☐	☐	☐	TELNET (0.0.0.0/0:23, TCP)
☐	☐	☐	SIP (0.0.0.0/0:5060-5061, TCP AND UDP)
☐	☐	☐	SSH (0.0.0.0/0:22, TCP)
☐	☐	☐	TACACS (0.0.0.0/0:49, TCP)
☐	☐	☐	DNS (0.0.0.0/0:53, UDP)
☐	☐	☐	BootP (0.0.0.0/0:67, UDP)
☐	☐	☐	TFTP (0.0.0.0/0:69, UDP)

(Next: Privacy)

Back Next Cancel