



ExtremeControl with ExtremeWireless WiNG

Abstract: This document covers implementation of ExtremeWireless WiNG in ExtremeControl. The enforcement to the wireless controller is done via Wireless Client Roles that are dynamically applied on the wireless controller after a Filter-ID is returned from Access Control. The Wireless Client Role can enforce Application Rules, IPv6 Rules, IPv4 Rules, and MAC Rules. Web redirection is done via a custom RADIUS attribute that sends the redirection URL. Note that this guide only provides guidance on the configuration of the wireless controller to integrate with Access Control and does not cover implementation of Access Control functionalities.

Published: November 2017

Extreme Networks, Inc.
6480 Via Del Oro
San Jose, California 95119
Phone / +1 408.579.2800
Toll-free / +1 888.257.3000

www.extremenetworks.com

©2017 Extreme Networks, Inc. All rights reserved.

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries. All other names are the property of their respective owners. All other registered trademarks, trademarks, and service marks are property of their respective owners. For additional information on Extreme Networks trademarks, see www.extremenetworks.com/company/legal/trademarks.

Contents

Pre-Requisites and Limitations	3
Overview	3
Part 1 – Configuring the Wireless Controller to Authenticate to Access Control.....	5
Step 1 – Configure SNMP	5
Step 2 – Configure RADIUS	7
Step 3 – Configure Roles and Firewall Rules	12
Application Policies	12
IPv4 Firewall Policies	14
Wireless Client Role	15
Assign the Roles Profiles	18
Step 4 – Captive Portal Configuration	20
Step 5 – Create the Wireless Networks	24
Part 2 – Configuring ExtremeControl	28
Step 1 – Create an SNMP Profile for WiNG.....	28
Step 2 – Add the Wireless Controller to ExtremeControl	30
Step 3 – Configure Rules, Roles and Policy Mappings	32
Part 3 – Validation	34
Appendix A: Creating RFC 3576 Configurations	37
Revision History	41

Pre-Requisites and Limitations

- Extreme ExtremeManagement 8.0.4.54 or later.
- Extreme Access Control 8.0.4.54 or later.
- WiNG Firmware version 5.9.1 or later. A controller with an Advanced Security license should be used.
- There is currently no common wired and wireless policy management with ExtremeWireless WiNG. User access is manually created on the wireless controller.
- ExtremeAnalytics can be configured in an Overlay mode on a network that runs ExtremeWireless WiNG. There is currently no integrated mode available on WiNG.
- ExtremeManagement does not currently provide heat maps, location, or area based access control when using ExtremeWireless WiNG.
- ExtremeManagement does not currently report wireless RF stats, or MU History reporting when using ExtremeWireless WiNG

Overview

This section provides a brief overview of the traffic flow and RADIUS authentication. The figure below shows the components in use and how authentication flows through the solution.

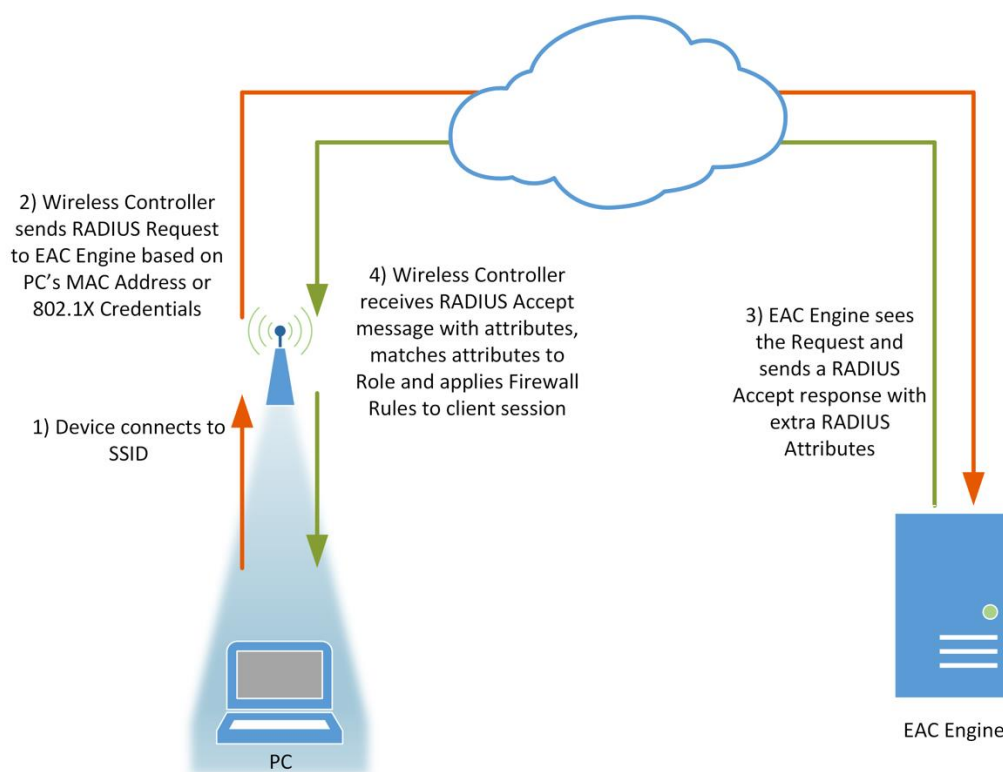


Figure 1. Authentication Packet Flow

1. As the device connects to the wireless SSID, either MAC-based authentication or 802.1X authentication will occur.
2. The wireless controller will send a RADIUS request destined to the Access Control Engine for authentication.
3. The Access Control Engine will authenticate the RADIUS request per its configuration. It will pass back RADIUS attributes that the wireless controller can interpret.
4. The wireless controller will match the attributes to a Wireless Client Role and enforce the corresponding Firewall rules or application policies.

Note

In addition to the steps created in this guide, it is also recommended to have IP helper addresses pointed to the Access Control Engine and SNMP Read-Only credentials configured on the router which Access Control can query to assist with IP resolution.

Part 1 – Configuring the Wireless Controller to Authenticate to Access Control

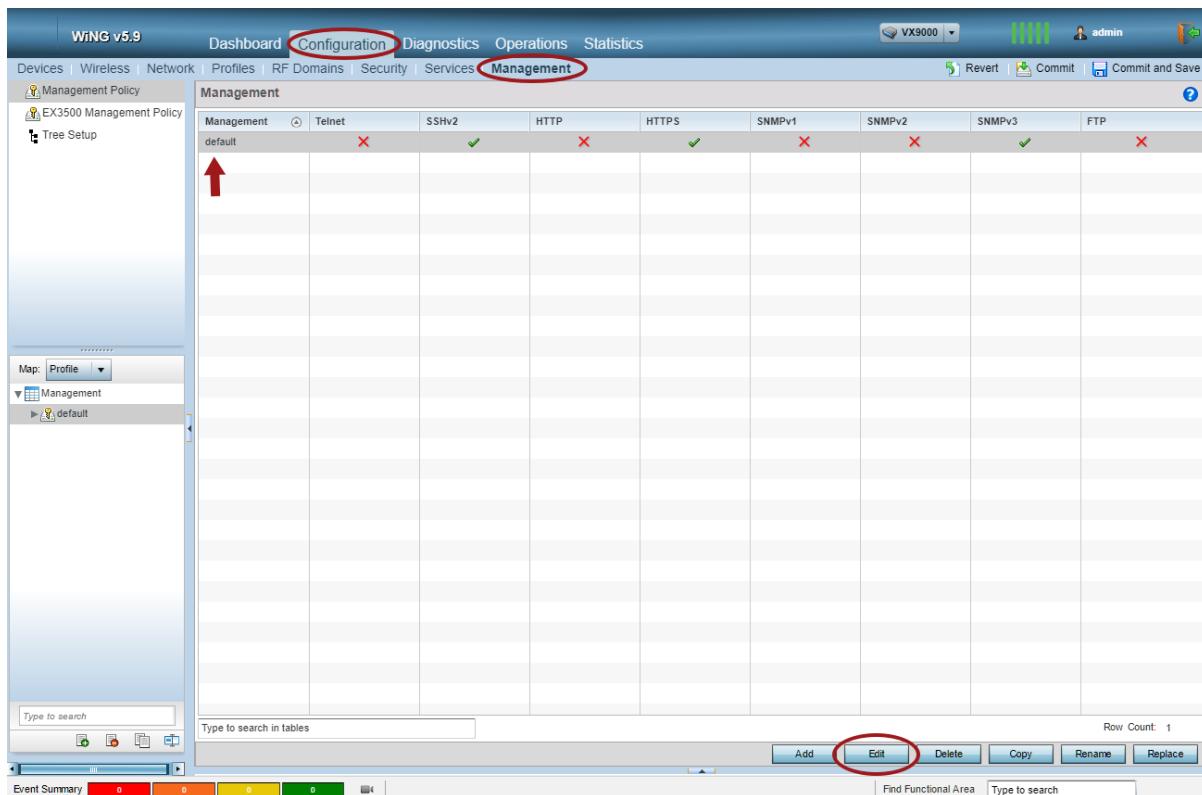
The configuration of the ExtremeWireless WiNG controller to authenticate to Access Control consists of five parts.

1. Configure SNMP to manage the wireless controller.
2. Configure the RADIUS settings to authenticate against the Access Control Engine.
3. Configure the Wireless Client Roles that will be assigned from Access Control.
4. Configure the Captive Portal on the wireless controller.
5. Configure the SSID for authentication against Access Control.

Step 1 – Configure SNMP

In order for ExtremeManagement to manage a wireless controller, SNMP needs to be configured. Ideally SNMPv3 is used due to its security and efficiency compared to SNMPv1 or SNMPv2.

SNMP configuration is accomplished by logging into the wireless controller and navigating to **Management** tab under **Configuration**. In the **Management Policy** section select the the management policy in use and select **Edit**:



In the management policy, select the **SNMP** tab. Ensure that **SNMPv3** is enabled. Then select the SNMPv3 Users and verify the settings so that they can be used when configuring Access Control. If desired, change the password from the default, Once complete, if any changes were made, select **OK** followed by a Commit.


Management Policy default

Administrators Allowed Locations Access Control Authentication **SNMP** SNMP Traps T5 PowerBroadband SNMP



SNMP


Enable SNMPv1 ☐

Enable SNMPv2 ☐



Enable SNMPv3 ☒ 

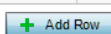
SNMPv1/v2c Community String

Community	Access Control	IP SNMP ACL	
private	Read-Write	default	
public	Read Only	default	



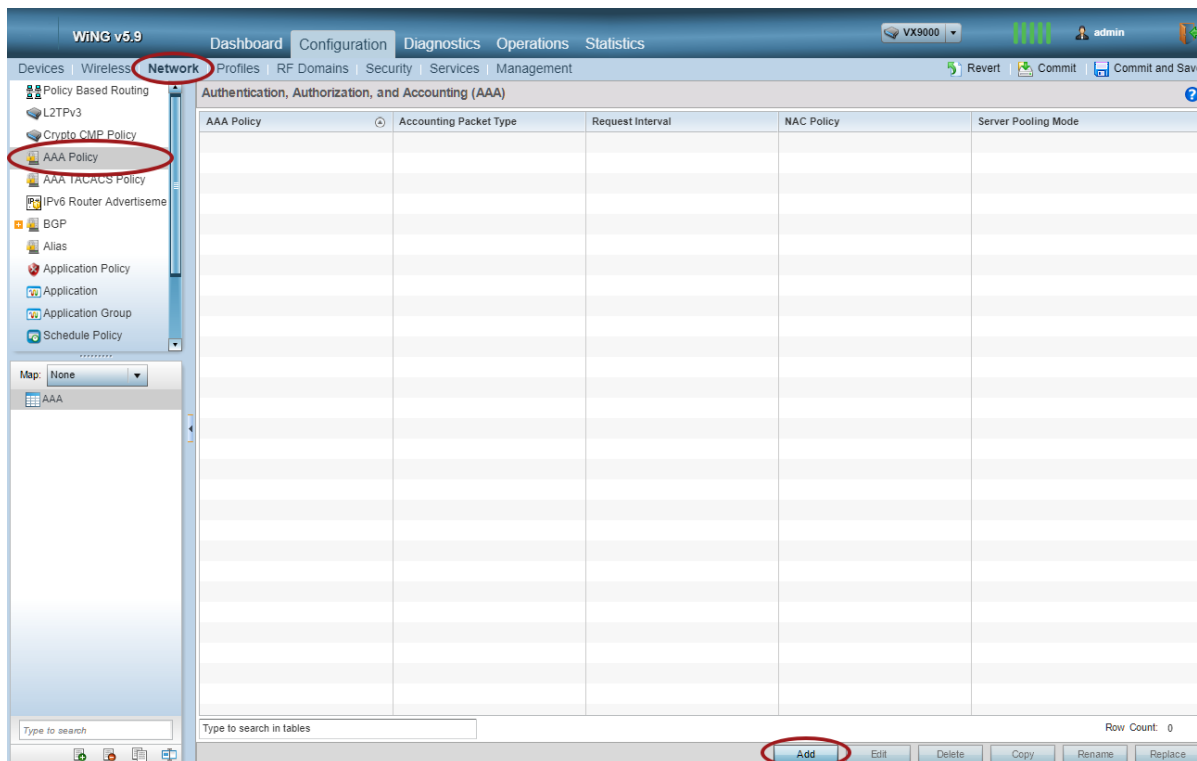
SNMPv3 Users

User Name	Authentication	Encryption	Password	
* snmpmanager	* MD5	* DES	* admin123 <input checked="" type="checkbox"/> Show	
snmptrap	MD5	DES	*****	



Step 2 – Configure RADIUS

In order for the wireless controller to authenticate against Access Control, the Access Control Engine needs to be configured as a RADIUS server in the wireless controller with some specific settings enabled. To accomplish this, navigate to the **Network** tab under **Configuration**. Then select the **AAA Policy** section. Select the **Add** button to create a new AAA policy. Name the new policy and select **Continue**.



In the RADIUS Authentication tab, select the **Add** button to create a new RADIUS Server.



[illegible]

In the Authentication Server window, use the following settings in addition to the defaults that are populated. Select **OK** and then **Exit** when the settings are complete.

- Host: <Access Control Engine IP Address>
- Secret: ETS_TAG_SHARED_SECRET
- Request Proxy Mode: Through Wireless Controller

Authentication Server

Server Id 1 (1 to 6)

Settings

Server Type

Host

Host

192.168.7.135

IP Address

Alias

Port

1812

(1 to 65,535)

Secret

ETS_TAG_SHARED_SECRET

Show

Request Proxy Mode

Through Wireless Controller

Proxy Mint Host

Request Attempts

3

(1 to 10)

Request Timeout

3

Seconds

(1 to 60)

Retry Timeout Factor

100

(50 to 200)

DSCP

0

(0 to 63)

Network Access Identifier Routing

NAI Routing Enable

Realm

Realm Type

Prefix

Suffix

Strip Realm

OK

Reset

Exit

Select the **RADIUS Accounting** tab and add a RADIUS Accounting Server. Use the default settings with the exception for the Host IP, Secret, and Request Proxy Mode as with the Authentication Server. Select **OK** and **Exit** when the settings are complete.

Accounting Server [X]

Server Id 1 (1 to 6) [?]

Settings

Server Type [Host]

Host [192.168.7.135] [IP Address]

Alias []

Port [1813] (1 to 65,535)

Secret [ETS_TAG_SHARED_SECRET] [Show]

Request Proxy Mode [Through Wireless Controller]

Proxy Mint Host []

Request Attempts [3] (1 to 10)

Request Timeout [5] [Seconds] (1 to 60)

Retry Timeout Factor [100] (50 to 200)

DSCP [34] (0 to 63)

Network Access Identifier Routing

NAI Routing Enable []

Realm []

Realm Type [Prefix] [Suffix]

Strip Realm []

[OK] [Reset] [Exit]

Finally, select the **Settings** tab of the AAA policy. In this screen, a few items need to be adjusted. Once completed, select the **OK** button followed by **Exit** and then **Commit**.

- In the RADIUS Accounting section, change the **Accounting Packet Type** to **Start/Interim/Stop**.
- In the RADIUS Address Format section, change **Attributes** to **All**.
- In the Access Request Attributes section, enable the **Cisco VSA Audit Session Id** option and the **Add Framed IP Address** option.

Once completed, select the **OK** button followed by **Exit** and then **Commit and Save**.

The screenshot displays the 'AAA Policy EAC' configuration window, specifically the 'Settings' tab. The interface is organized into several sections:

- RADIUS Authentication:** Includes a protocol selection area with radio buttons for PAP, CHAP, MS-CHAP, and MS-CHAPv2.
- RADIUS Accounting:** Contains settings for 'Accounting Packet Type' (set to 'Start/Interim/Stop'), 'Request Interval' (1 minute), and 'Accounting Server Preference' (Prefer Same Authentication Server Host).
- RADIUS Address Format:** Includes 'Format' (Dash Delimiter), 'Case' (Uppercase), and 'Attributes' (set to 'All').
- Server Pooling:** Features a 'Server Pooling Mode' section with radio buttons for 'Failover' and 'Load Balanced'.
- EAP Wireless Client Settings:** Includes 'Client Attempts' (3), 'Request Timeout' (3 seconds), and 'ID Request Timeout' (30 seconds).
- Access Request Attributes:** This section on the right contains several options, with 'Cisco VSA Audit Session Id' and 'Add Framed IP Address' highlighted with red boxes. Other options include 'Accounting Delay Time', 'Accounting Multi Session Id', 'Chargeable User Id', 'Framed MTU', 'RFC5580 Location Information', 'RFC5580 Operator Name', 'Service-Type', 'NAS IPv6 Address', 'Proxy NAS Identifier', and 'Proxy NAS IPv4/IPv6 Address'.

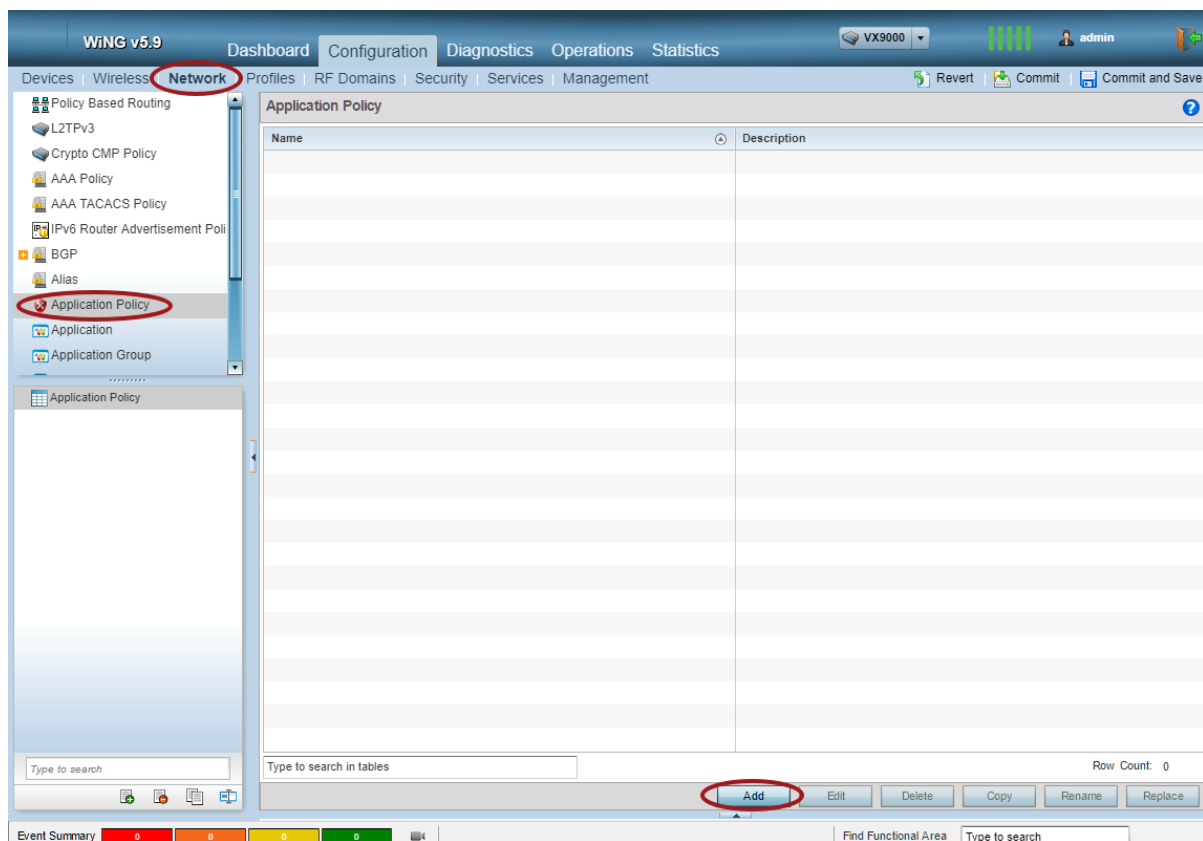
At the bottom right of the window, there are three buttons: 'OK', 'Reset', and 'Exit', with 'OK' and 'Exit' highlighted by red boxes.

Step 3 – Configure Roles and Firewall Rules

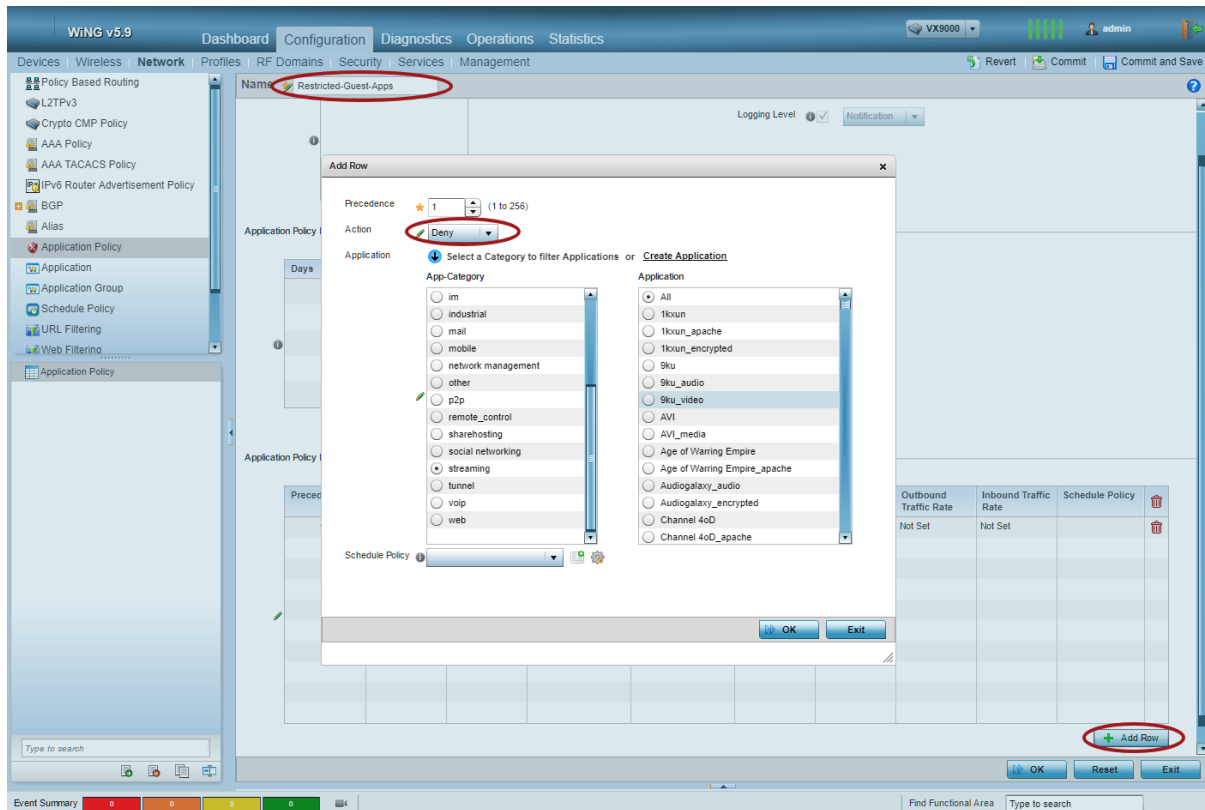
Differing levels of access to users and devices can be assigned based on a rules engine running on Access Control. These levels of access are defined by Wireless Client Roles in the wireless controller. The Roles allow for a mapping of a VLAN ID, Application Policies, IPv6 Firewall Rules, IPv4 Firewall Rules, and MAC-Based Firewall Rules. For the purposes of this document, Application Policies and IPv4 Firewall rules will be shown.

Application Policies

An application policy can be created to control layer 7 applications such as streaming video applications, social media, and peer to peer applications. To create such policies, navigate to the **Network** tab under Configuration. Then select the **Application Policy** section. Select the **Add** button to create a new Application Policy.

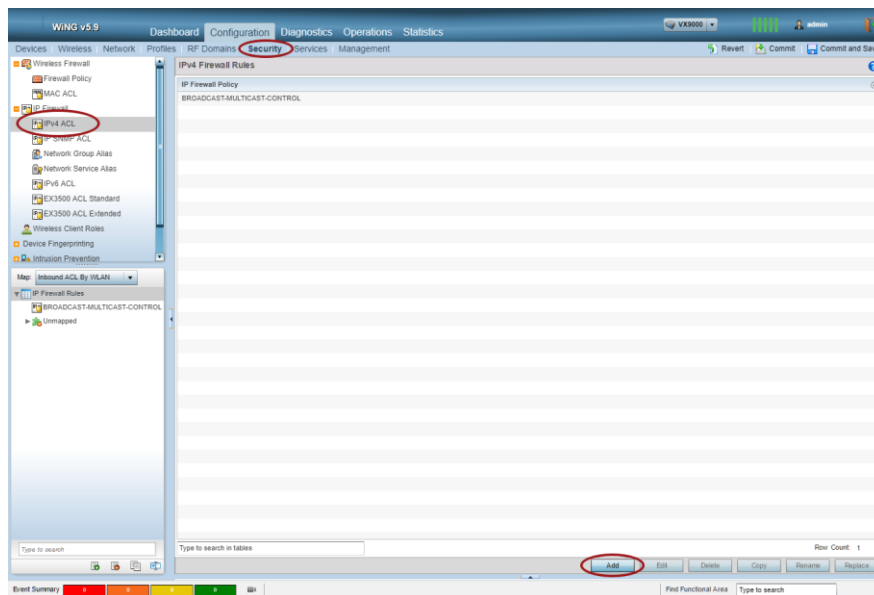


Name the new application policy and create the types of Application Policy Rules that are desired. Each Application Policy Rule can be added by creating new rows. Once the rules are created, select **OK** and **Exit**. **Commit and Save** the changes when complete.

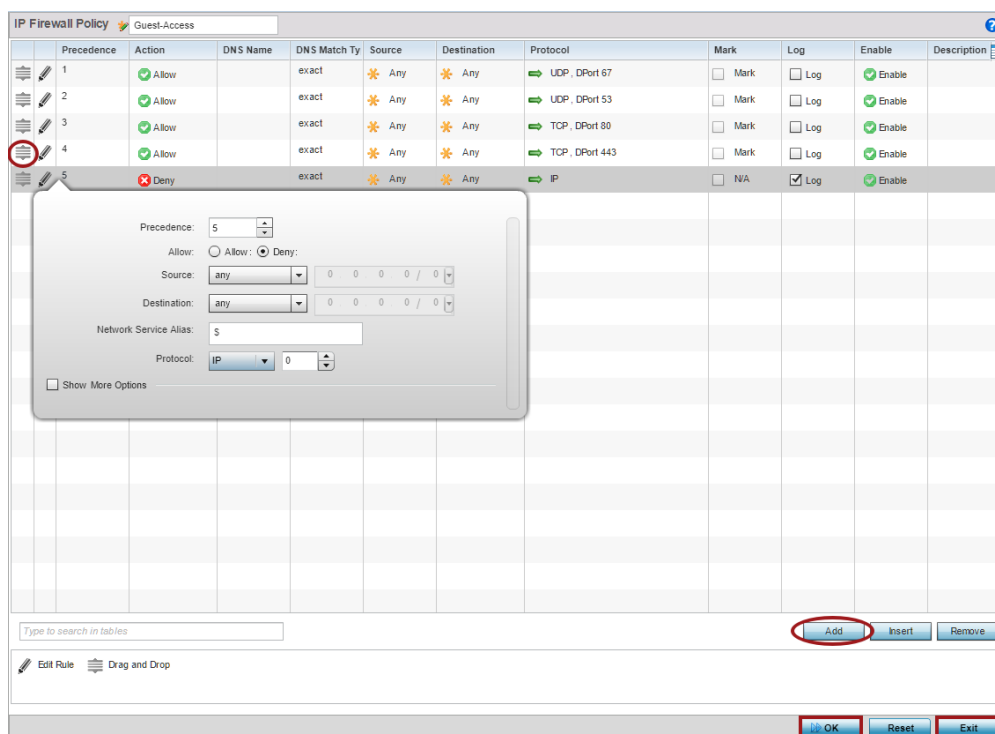


IPv4 Firewall Policies

To create the desired IPv4 Firewall rules, navigate to the **Security** tab under **Configuration**. Then select expand the IP Firewall tree and select the **IPv4 ACL** section. In this section, IP Firewall Policies can be created for use in the Wireless Client Roles. To create a new policy, select the **Add** button.

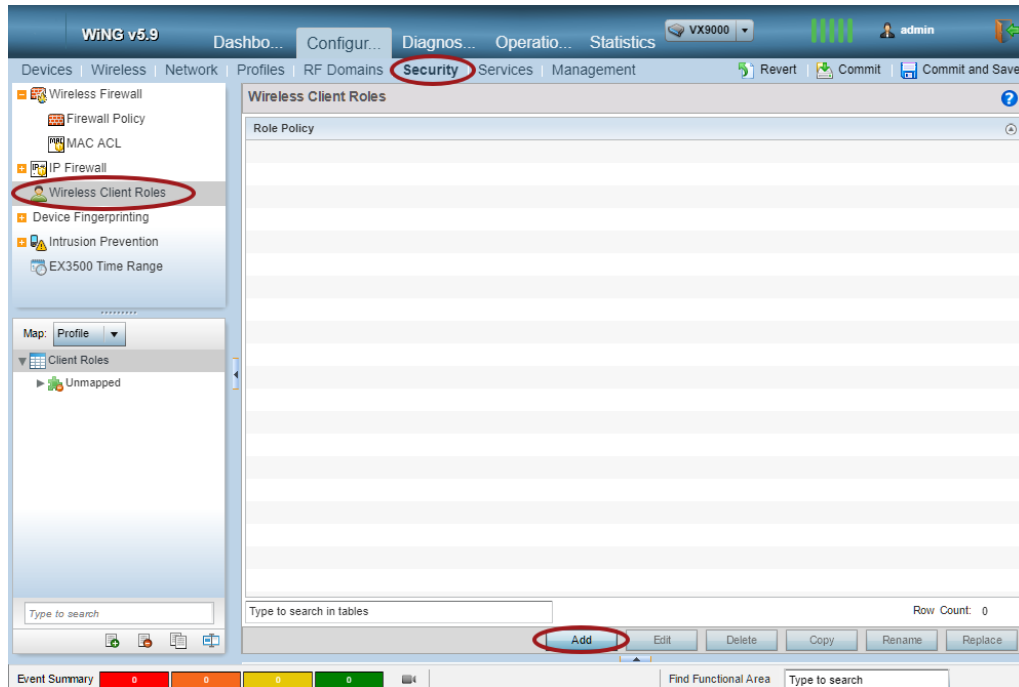


In the new IP Firewall Policy, assign a name that can be used for the Wireless Client Role. Create individual ACL rules that will be assigned to match the desired level of access. The rules can be re-ordered with drag-and-drop if desired. Once complete, select the **OK** button followed by **Exit**. Then select the **Commit and Save** button.

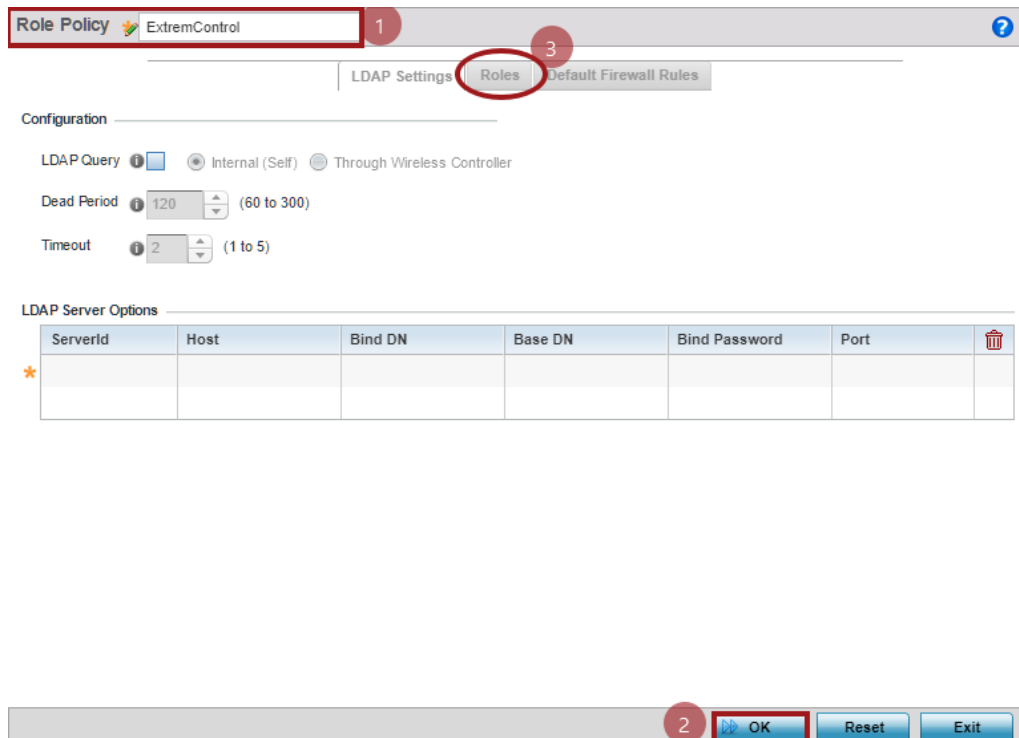


Wireless Client Role

To create the role that will be assigned by Access Control, navigate to the **Security** tab under Configuration. Then select the **Wireless Client Roles** section. In this section, role policies can be created. In most networks, only one policy will be created with multiple roles within the policy. To create a new policy, select the **Add** button.



Name the role policy, then press **OK**. Next, select the **Roles** tab to start creating the roles.



In the new Role, enter a name and select **OK**. In the Match Expressions field, change the **Group Configuration** to create an Exact match of the name of the Filter-Id that will be received from Access Control. For instance, if the Guest Access role is being sent back, the matching configuration should match the screenshot below. Also note that for different roles, the Role Precedence needs to be different. Once that is set, select the **Firewall Rules** tab to assign the access.

Role Policy Roles

Role Name 1

Settings **Firewall Rules** 4

Information

To configure LDAP attributes in the Role, the LDAP Settings should be configured first.

Role Precedence

Precedence (1 to 10,000)

Bonjour Gateway

Discovery Policy

Client Identity

Client Identity Name

Match Expressions

AP Location

2 SSID Configuration

Group Configuration

Radius User

Wireless Client Filter

Wireless Client MAC/MAC Mask or ☒ Any

Captive Portal Connection

Authentication State ☒ Pre-Login ☐ Post-Login ☐ Any

Authentication / Encryption

Authentication Type ☐ EAP ☐ Kerberos ☐ MAC Authentication ☐ None

Encryption Type ☐ CCMP ☐ KeyGuard ☐ TKIP ☐ WEP128 ☐ WEP64 ☐ None

☒ LDAP Attributes

3

In the **Firewall Rules** tab, the previously created Application Policy and IP ACL rules can be assigned as well as a VLAN override if desired. Once the firewall rules are complete, select the **OK** button followed by **Exit**.

Role Policy Roles

Role Name: Guest Access

Settings | **Firewall Rules**

Vlan ID: VLAN 1 (1 to 4,094)

Application Policy: **Restricted-Guest-Apps**

IPv6 Inbound

IPv6 Firewall Rules Name	Precedence	

+ Add Row

IPv6 Outbound

IPv6 Firewall Rules Name	Precedence	

+ Add Row

IP Inbound

IP Firewall Rules Name	Precedence	
Guest-Access	1	

+ Add Row

IP Outbound

IP Firewall Rules Name	Precedence	

+ Add Row

MAC Inbound

MAC Firewall Rules Name	Precedence	

+ Add Row

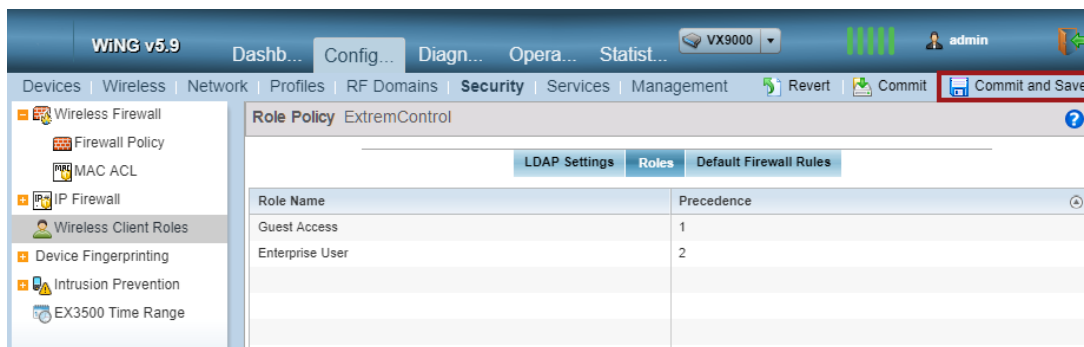
MAC Outbound

MAC Firewall Rules Name	Precedence	

+ Add Row

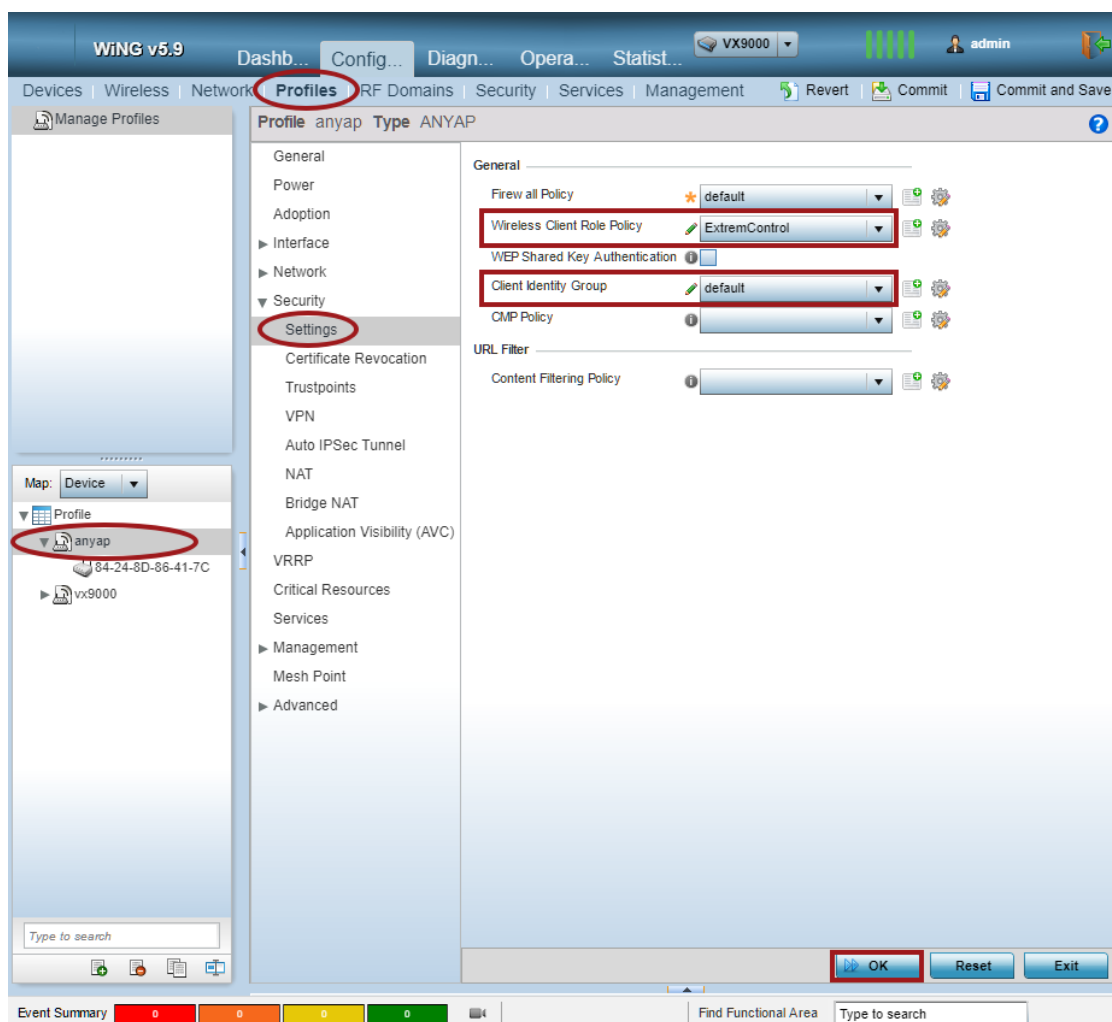
OK | Reset | Exit

Repeat this process for any additional roles that need to be created. **Commit** and **Save** the changes once complete.

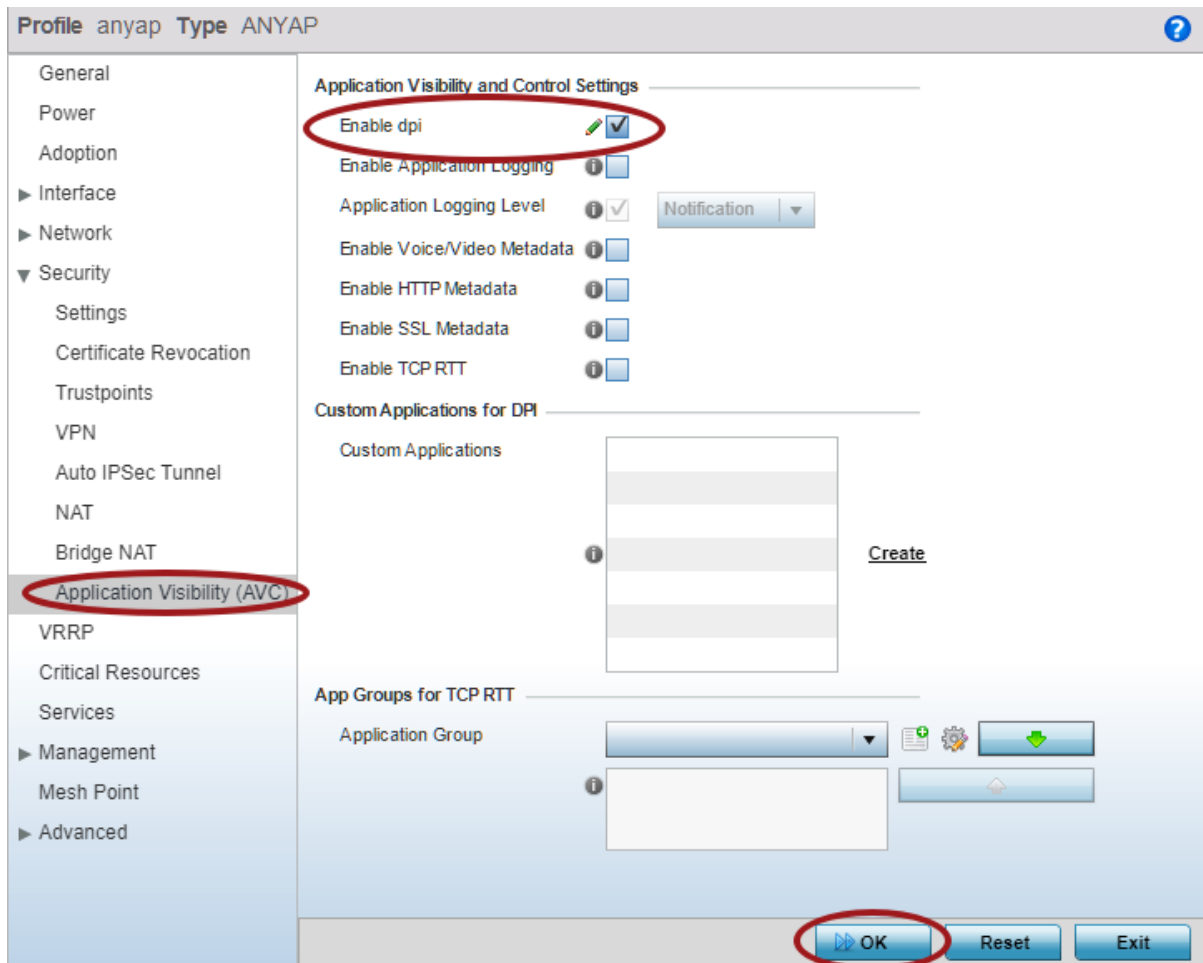


Assign the Roles Profiles

The last step to enable the Roles is to assign it to a Device or Profile. If Application Policies are also being used the DPI engine needs to be enabled. Accomplish this by navigating to the **Profiles** tab under Configuration. Select the Profile that needs to be modified and expand the **Security** section of the profile. In the **Settings** section, select the **Wireless Client Role** that was created from the dropdown list. Select **OK** to save the setting then select the **Application Visibility (AVC)** section.



In the Application Visibility (AVC) section, enable the checkbox for **Enable dpi** and select **OK** followed by **Exit** and then **Commit and Save** changes.



Step 4 – Captive Portal Configuration

ExtremeWireless WiNG can use a centralized external captive portal for authentication and registration. The captive portal configuration also needs to include a DNS whitelist of websites that a client is allowed to go to while still in the captive state. The captive portal URL is dynamically assigned from Access Control via a RADIUS attribute when a client needs to be redirected.

To create the captive portal configuration, select the **Services** section of **Configuration**. Then select the **Captive Portals** section. Select **Add** to create a new configuration.

The screenshot shows the ExtremeControl WiNG v5.9.1 interface. The top navigation bar includes tabs for Dashb..., Config..., Diagn..., Opera..., and Statist..., with 'Services' highlighted. Below this, a secondary navigation bar shows 'Devices | Wireless | Network | Profiles | RF Domains | Security | Services | Management', with 'Services' selected. The left sidebar contains a tree view with 'Captive Portals' selected. The main content area is titled 'Captive Portal' and contains a table with the following columns: Captive Portal Policy, Captive Portal Server Host, Captive Portal IPv6 Server, Captive Portal Server Mode, Hosting VLAN Interface, Connection Mode, Simultaneous Access, Web Page Source, and AAA Policy. The table is empty. At the bottom of the table, there is a search bar and a row count of 0. Below the search bar, there are buttons for 'Add', 'Edit', 'Delete', 'Copy', 'Rename', and 'Replace'. The 'Add' button is circled in red. The bottom status bar shows 'Event Summary' with four colored boxes (red, orange, yellow, green) each containing a '0'.

In the new Captive Portal policy, select **Internal(Self)** for the Captive Portal Server Mode. In the **Captive Portal Server Host** field, specify a *non-existent* server host where the web request would typically be sent. In the Access field, select **No authentication required** for the Access Type. Press **OK** to save the new Policy.

Captive Portal Policy ExtremeControl-Portal

Basic Configuration Web Page

Settings

Captive Portal Server Mode: ☒ Internal (Self) ☐ Centralized ☐ Centralized Controller

Hosting VLAN Interface: 0 (0 to 4,096)

Captive Portal Server Host: virtual.extremewireless.ca

Captive Portal IPv6 Server: ☐ IPv6

Connection Mode: ☒ HTTP ☐ HTTPS

Simultaneous Access: 1 (1 to 8,192)

Security

AAA Policy: EAC

Access

Access Type: ☒ No authentication required ☐ RADIUS Authentication ☐ Registration ☐ E-mail Access ☐ Mobile Access ☐ Other Access

Terms and Conditions page: ☐

OK Reset Exit

While still in the newly created Captive Portal Policy, scroll down to DNS Whitelist and select the **Add** button.

Captive Portal Policy ExtremeControl-Portal

Basic Configuration Web Page

Client Access Time: 1440 (10 to 10,080 minutes)

Inactivity Timeout: 10 Minutes (1 to 1,440)

Loyalty App

Enable: ☐

App Name:

DNS Whitelist

DNS Whitelist: <none> Add

Accounting

Enable RADIUS Accounting: ☐

Enable Syslog Accounting: ☐

Syslog Host: Hostname

Syslog Port: 514

Data Limit

Limit: 1 (1 to 102,400 MegaBytes)

Action: Log Only

Logout FQDN

Logout FQDN: (e.g., logout.guestaccess.com)

Localization

FQDN: (e.g., local.guestaccess.com)

OK Reset Exit

Create entries in the DNS whitelist for both the IP address and hostname of the Access Control Engines used on the network. Once added, select the **OK** and **Exit** buttons.

DNS Entry	Match Suffix
nac-1.wingsecure.com	No

+ Add Row

OK Reset Exit

In the Captive Portal Policy, select the newly created DNS Whitelist from the dropdown menu and then select **OK** followed by **Commit and Save**.

WiNG v5.9 Dashb... Config... Diagn... Opera... Statist... VX9000 admin

Devices | Wireless | Network | Profiles | RF Domains | Security | **Services** | Management | Revert | Commit | **Commit and Save**

Captive Portals

Captive Portals

DNS Whitelist

Guest Management

DHCP Server Policy

Bonjour Gateway

DHCPv6 Server Policy

RADIUS

URL Lists

Map: None

Captive Portal

ExtremeControl-Portal

Captive Portal Policy ExtremeControl-Portal

Basic Configuration Web Page

Client Access Time 1440 (10 to 10,080 minutes)

Inactivity Timeout 10 Minutes (1 to 1,440)

Loyalty App

Enable

App Name

DNS Whitelist

ExtremeControl-DNS-Whit

Accounting

Enable RADIUS Accounting

Enable Syslog Accounting

Syslog Host

Syslog Port 514

Data Limit

Limit 1 (1 to 102,400 MegaBytes)

Action Log Only

Logout FQDN

Logout FQDN

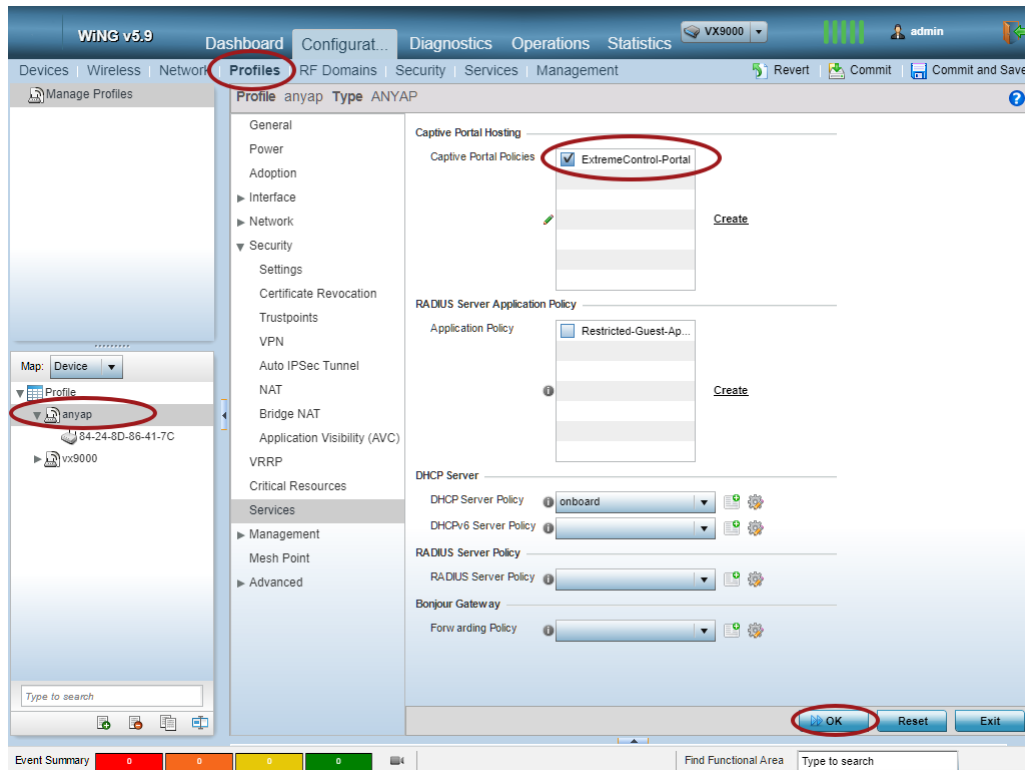
Localization

FQDN

OK Reset Exit

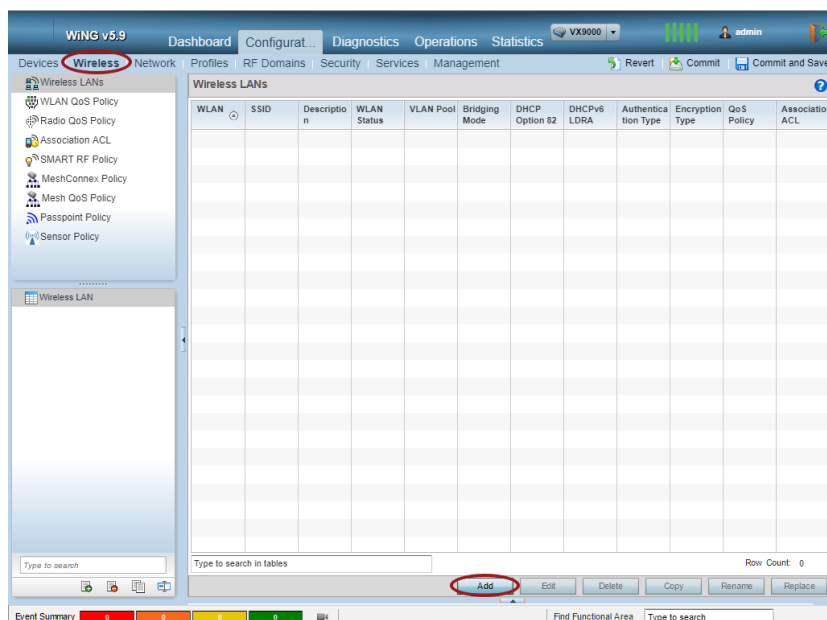
Event Summary 0 0 0 0 0 0 Find Functional Area Type to search

The final step is to assign the new Captive Portal policy to the Device Profiles in use. To do this, select the **Profiles** tab under **Configuration** and then navigate to the profile to be modified. Select the **Services** tab of the profile and then select the checkbox next to the new Captive Portal Policy. Once complete, select the **OK** button followed by **Commit**.

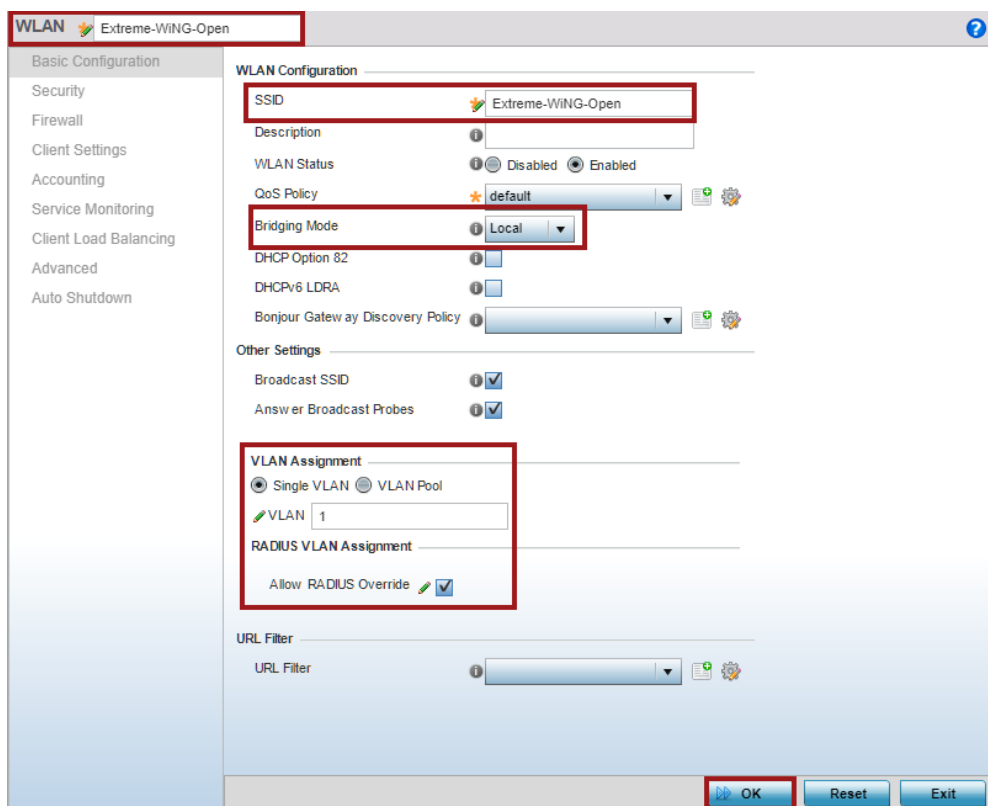


Step 5 – Create the Wireless Networks

The last part of the configuration of the wireless controller is the mapping of all of the settings to a wireless network. Navigate to the **Wireless** tab of **Configuration** and select the **Wireless LANs** section. Select the **Add** button to create a new wireless network.



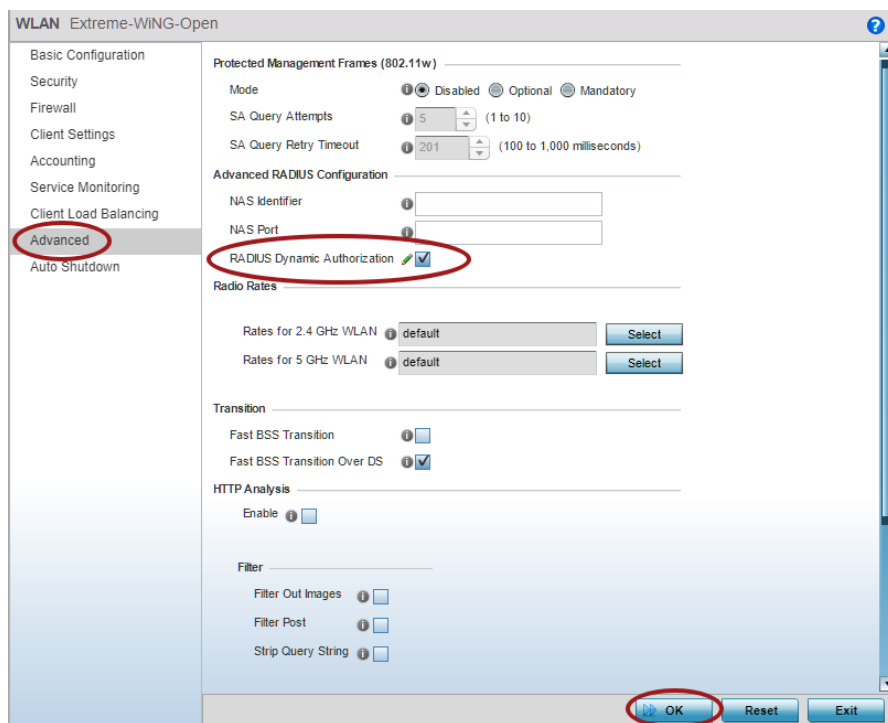
In the new WLAN screen, create the basic configurations required such as the SSID name, Bridging Mode and VLAN Assignment. Then enable the **Allow RADIUS Override** checkbox and select the OK button.



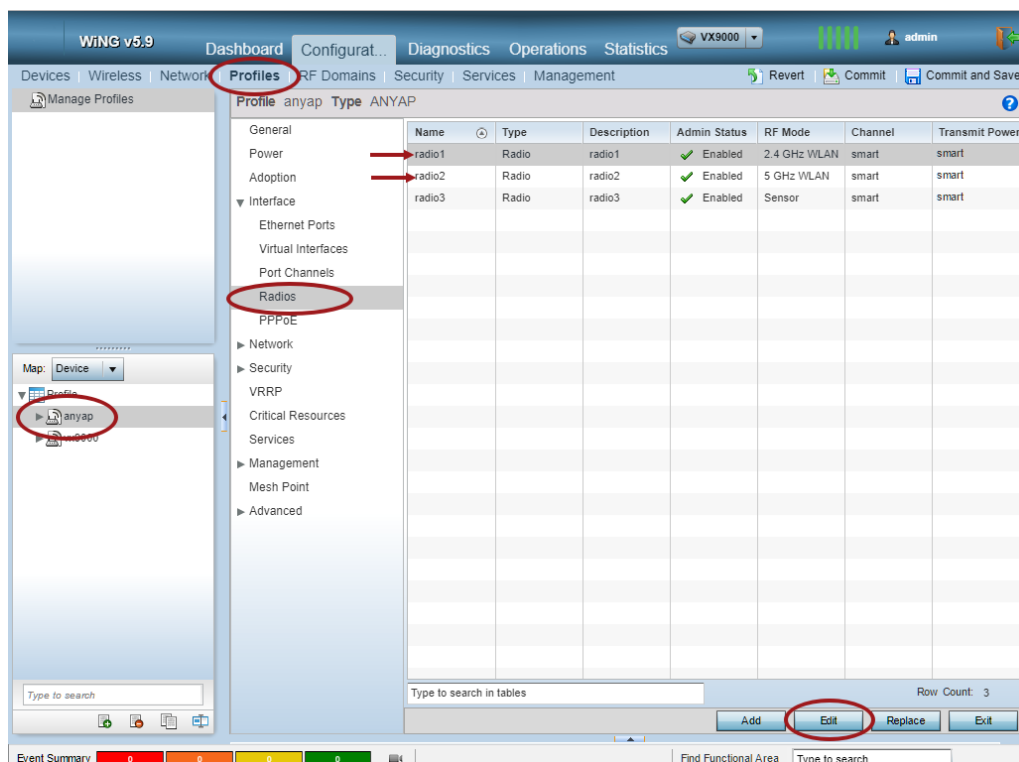
Next, navigate to the **Security** section of the WLAN. Select **MAC** for the authentication type. Once the authentication type is set, select the AAA Policy that was created from the drop down list. Next, select the checkboxes next to **Captive Portal Enable** and **Captive Portal if Primary Authentication Fails**. From the **Captive Portal Policy** drop down list select the previously created Captive Portal Policy. If the encryption methods need to be set for the SSID type, scroll further down the page and select the appropriate settings for the type of SSID. Select the **OK** button to continue.

Next, select the **Accounting** section of the WLAN. Select the checkbox for **Enable RADIUS Accounting** and ensure that the AAA Policy previously created is selected. Select the **OK** button to continue.

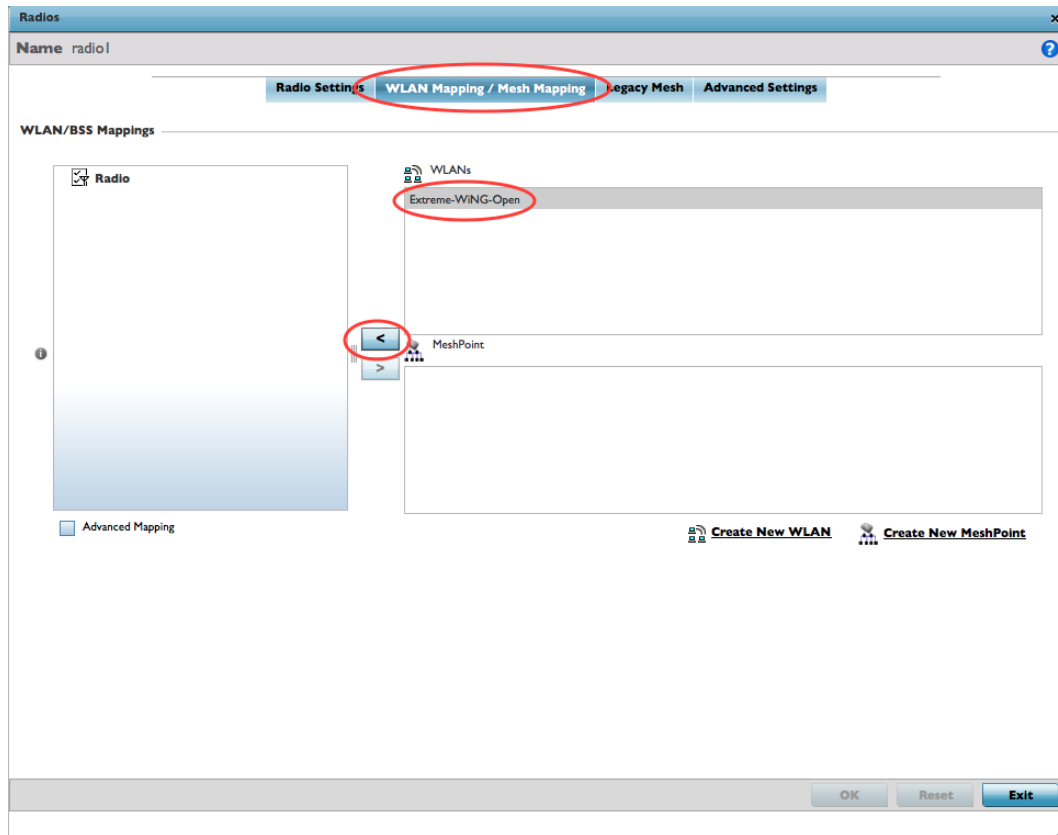
The last configuration step for the WLAN is in the **Advanced** section. Select the checkbox next to **RADIUS Dynamic Authorization** and then select **OK** followed by **Exit**. Then Commit the configuration.



The last configuration step for the Wireless Network is to assign it to the AP Radios. Navigate to the appropriate **Profile** and expand the **Interface** section to select the **Radio**. Select a radio and then the **Edit** button.



In the **Radios** window, select the **WLAN Mapping / Mesh Mapping** tab. Select the newly created WLAN and then the arrow to map it to the radio. Select the **OK** button followed by **Exit** and repeat the process for any additional radios.



Part 2 – Configuring ExtremeControl

In this section, the WiNG wireless controller will be added to Extreme Access Control as a switch so that clients can be authenticated and controlled.

Note

This section assumes that the Access Control Engine is already configured and added to Access Control. It also assumes that Guest Registration is already enabled.

Step 1 – Create an SNMP Profile for WiNG

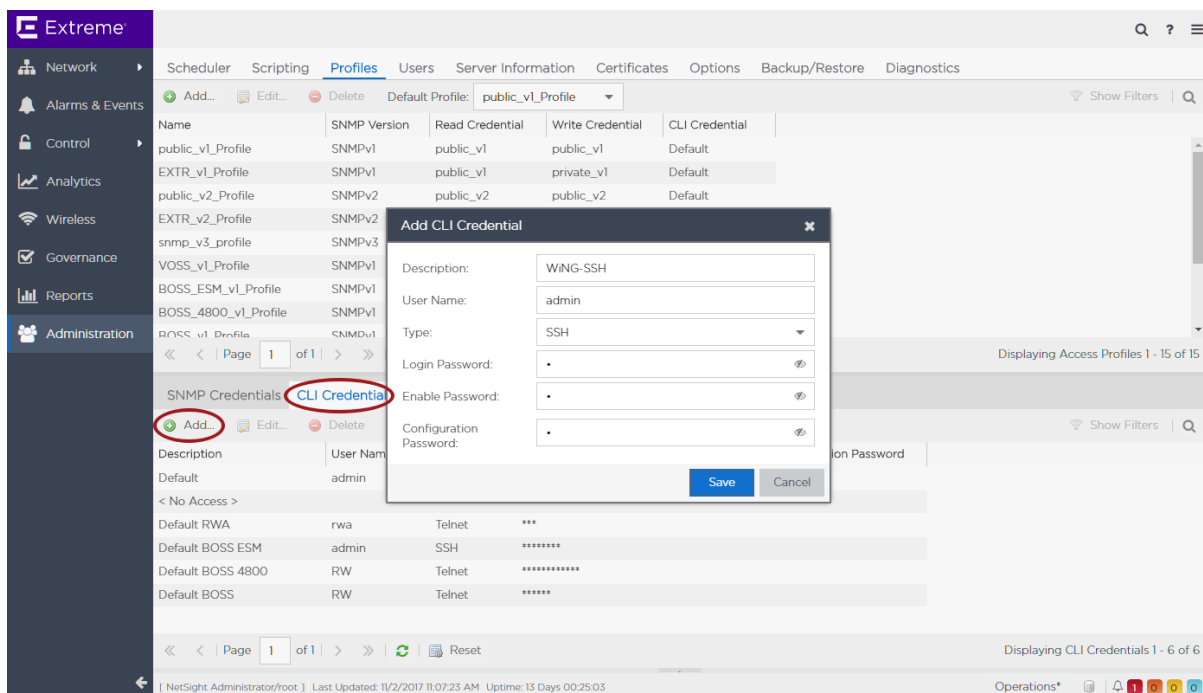
In ExtremeManagement, select the Profiles tab under Administration. Select the Add button for SNMP Credentials. Create new SNMP credentials that correlate with the credentials configured in the wireless controller.

The screenshot shows the ExtremeManagement web interface. In the left sidebar, the 'Administration' tab is selected. Under 'Administration', the 'Profiles' sub-tab is active. A table displays a list of profiles with columns: Name, SNMP Version, Read Credential, Write Credential, and CLI Credential. The table lists several profiles, including 'public_v1_Profile', 'EXTR_v1_Profile', 'public_v2_Profile', 'EXTR_v2_Profile', 'snmp_v3_profile', 'VOSS_v1_Profile', 'BOSS_ESM_v1_Profile', 'BOSS_4800_v1_Profile', and 'BOSS_v1_Profile'. Below the table, the 'Add...' button is circled in red. A modal window titled 'Add SNMP Credential' is open, showing the following fields:

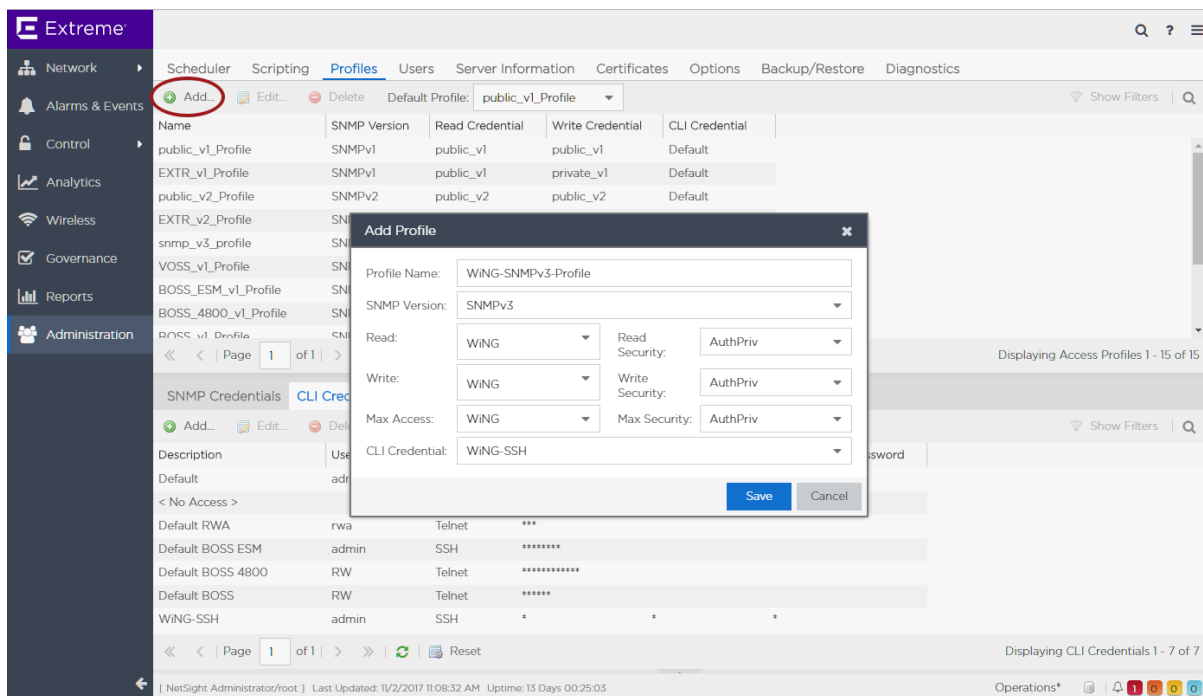
- Credential Name: WING
- SNMP Version: SNMPv3
- User Name: snmpmanager
- Authentication Type: MD5
- Authentication Password: admin123
- Privacy Type: DES
- Privacy Password: admin123

The 'Save' button is highlighted in blue. The bottom status bar shows the user is 'NetSight Administrator/root' and the system was last updated on 11/2/2017 at 11:04:37 AM.

Next, select CLI Credentials in the Profiles tab and create a new CLI configuration to access the WiNG Controller in the event that scripts are used in ExtremeManagement. If no scripts are going to be used, this step can be skipped.

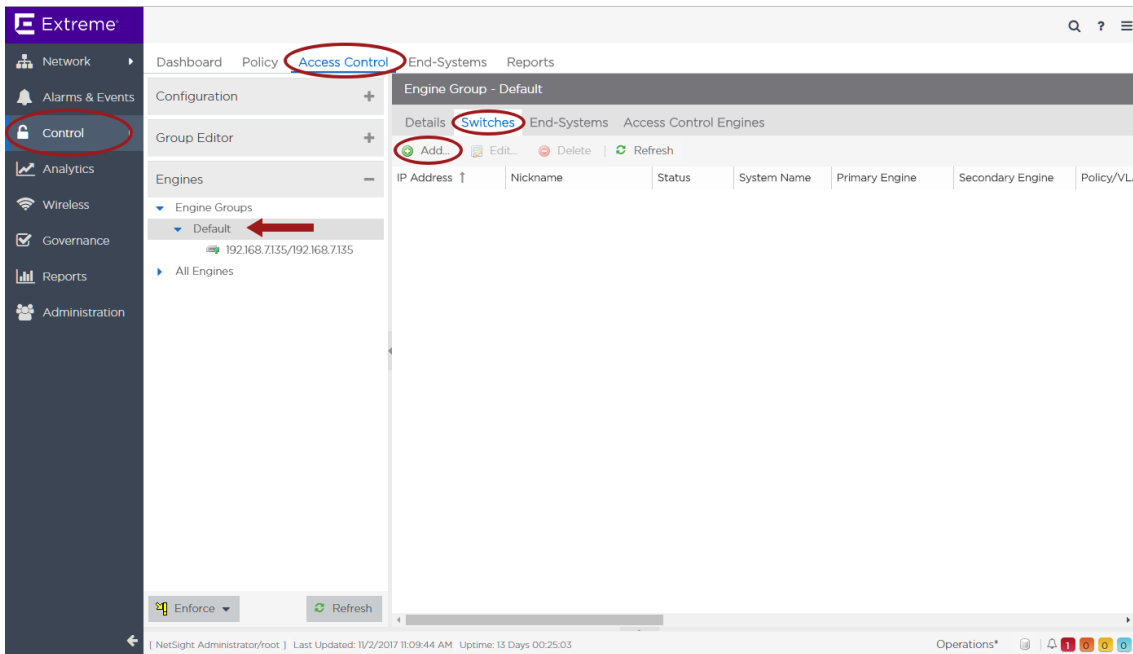


With the SNMP Credentials and CLI Credentials configured, create a **Profile** to map them together. Ensure that the SNMP settings are configured for **AuthPriv** for the SNMP Read, Write, and Max Access.

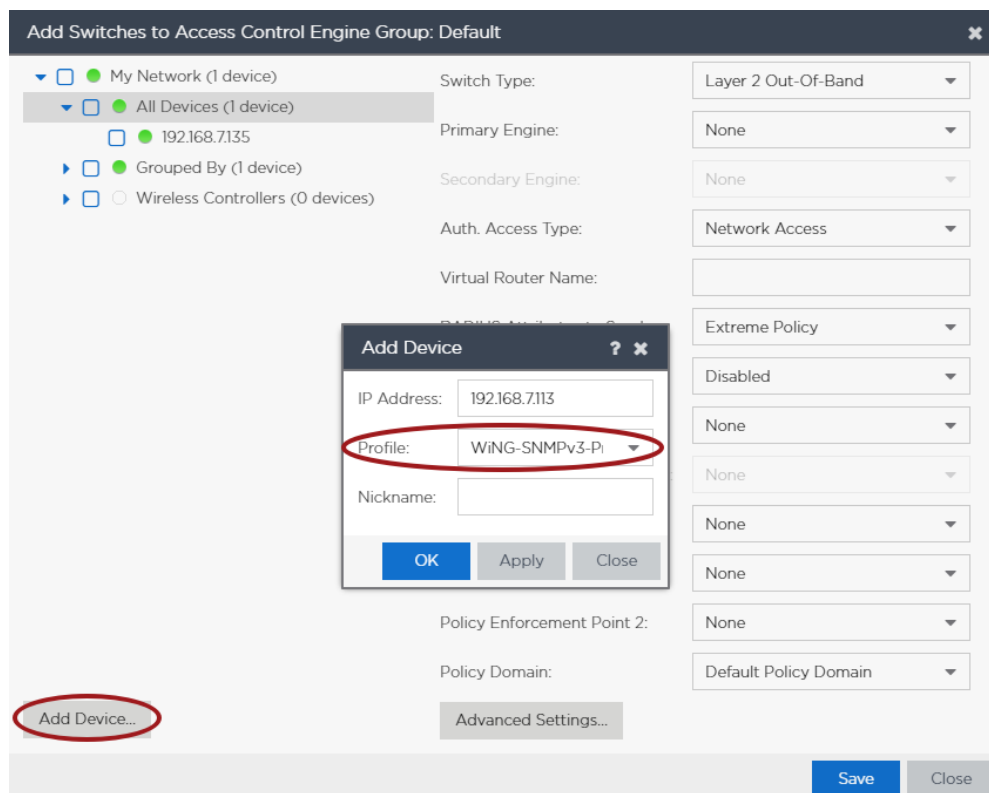


Step 2 – Add the Wireless Controller to ExtremeControl

Select the **Access Control** tab of **Control** followed by the **Default** Access Control Engine Group. In the group configuration, select the **Switches** tab and then select the **Add Switches** button.



In the Add Switches dialog, if the wireless controller hasn't been added to ExtremeManagement yet, select the **Add Device** button to add the IP address of the wireless controller and the SNMP Profile to use for communication.



Once the wireless controller is added to ExtremeManagement, select the wireless controller from the device list. Some configurations of the dialog are automatically populated. Select the Access Control Engine from the **Primary Engine** drop down list. If there is more than one Access Control Engine, do the same for the **Secondary Engine**. Set the **RADIUS Attributes** to **Send to Filter-Id & Custom Attribute** and then set the Policy Domain to **Do Not Set**.

Add Switches to Access Control Engine Group: Default

☐ My Network (2 devices)
☐ All Devices (2 devices)
☐ 192.168.7.135
☒ 192.168.7.113
☐ Grouped By (2 devices)
☐ Wireless Controllers (0 devices)

Switch Type: Layer 2 Out-Of-Band

Primary Engine: 192.168.7.135/192.168.7.135

Secondary Engine: None

Auth. Access Type: Manual RADIUS Configuratio

Virtual Router Name:

RADIUS Attributes to Send: Filter-Id & Custom Attribute

RADIUS Accounting: Enabled

Management RADIUS Server 1: None

Management RADIUS Server 2: None

Network RADIUS Server: None

Policy Enforcement Point 1: None

Policy Enforcement Point 2: None

Policy Domain: -- Do Not Set --

Add Device...

Advanced Settings...

Save Close

In the Advanced Switch Settings dialog, the **Reauthentication Type** must be modified. From the drop down list select **RFC3576 - ExtremeWireless WiNG**. If the setting is not currently available, see Appendix A to create the Reauthentication Configuration.

Advanced Switch Settings

IP Subnet for IP Resolution: None

RADIUS Security

Shared Secret:

Reauthentication Behavior

Reauthentication Type: RFC 3576 - Extreme

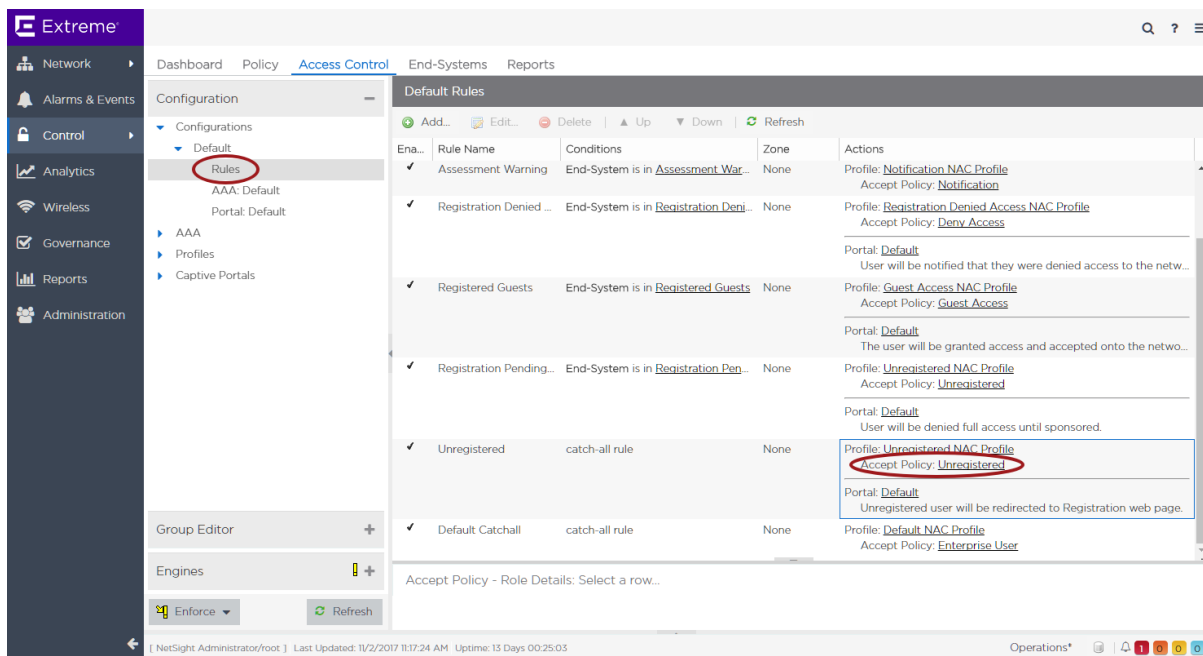
Enable Port Link Control: ☐

OK Cancel

Step 3 – Configure Rules, Roles and Policy Mappings

The last step to configuring ExtremeControl is to create and modify the Accept Policies for various Rules. Since ExtremeWireless WiNG controllers use a Filter-ID to pass back Wireless Client roles, most of the configuration is already done. However, for roles that require redirection to the captive portal, an additional VSA must be added. This will typically be used in the Unregistered Role, Quarantine Role and Assessing Role. This example shown will be for the Unregistered Role, however it can be re-used for any role that needs redirection.

Select the **Rules** section in the Access Control Configuration. Find the Unregistered rule and then select the **Unregistered** Accept policy.



In the Edit Policy Mapping dialog, there is a field available for Custom 1. The following attribute format should be used to instruct the controller to redirect to the Access Control Engine:

Custom 1: cisco-avpair=url-redirect=http://<AccessControlEngineIP>/?client_ip=WING_TAG_CLIENT_IP&client_mac=WING_TAG_CLIENT_MAC

For example, if the Access Control Engine IP address is 10.120.85.81, the attribute is:

Custom 1: cisco-avpair=url-redirect=http://10.120.85.81/?client_ip=WING_TAG_CLIENT_IP&client_mac=WING_TAG_CLIENT_MAC

If HTTPS and a fully qualified domain name are used on the Access Control Engine, the attribute is:

Custom 1: cisco-avpair=url-redirect=https://eac-engine-poc.cse.ets.com/?client_ip=WING_TAG_CLIENT_IP&client_mac=WING_TAG_CLIENT_MAC

Edit Policy Mapping

Name:

Filter:

Custom 1:

Save **Cancel**

Once the configuration for each Accept Policy is complete, Enforce to the Access Control Engines.

Extreme

Dashboard Policy **Access Control** End-Systems Reports

Configuration Group Editor Engines

Engine - 192.168.7135/192.168.7135

Details End-Systems Switches

Add... Edit... Delete Refresh

IP Address	Nickname	Status	System Name	Primary Engine	Secondary Engine	Policy/VLAN	Filter-Id & Cu...
192.168.7135	controller-1	Contact Est...	controller-1	192.168.7135			

Selection... All... Enforce Refresh

https://emc-1.wingsecure.com:8443/OneView/view/control# 12:10 AM Uptime: 13 Days 00:25:03 Operations*

Access Control Engine Enforce

Engine	IP Address	Status	Result	Details
<input checked="" type="checkbox"/>	192.168.7135	192.168.7135	Audit Comple...	Pass

☐ Force Reconfiguration for All Switches ☐ Force Reconfiguration for Captive Portal

Audit **Enforce** **Enforce All** **Close**

Part 3 – Validation

Validation of the configuration is completed by connecting a device to the SSID that was created and verifying that network connectivity is established. Opening a web page on the client should redirect to the captive portal provided by the Access Control Engine. Once the registration is complete and the user selects the **Complete Registration** button, the user will be seamlessly moved to a new role.

The screenshot shows a web browser window titled "Enterprise Registration" with the address bar displaying "10.120.85.81/main". The page features the Extreme Networks logo and a header that reads "Welcome to the Enterprise Registration Center". The main content area contains a message: "You have been **denied** network access because this device is not registered to the network. To obtain network access, you **must** complete registration using the form below. By registering to the network, you are **agreeing** to the terms and conditions explained in the [Enterprise Network and Computer Acceptable-Use Policy](#)". Below this message is a registration form with four input fields: "First Name:", "Middle Name:", "Last Name:", and "E-Mail Address:". A blue button labeled "Complete Registration" is positioned below the form. A note states: "Please press the Complete Registration button only once." The footer of the page includes the text "xxxx Example Street, Example City, Example State xxxxxx | xxx.xxx.xxxx | ©2013 Example Enterprise [About Us](#) | [Contact Us](#)" and a "Powered by Extreme Networks" logo.

Enterprise Registration

10.120.85.81/main

Extreme networks

Welcome to the Enterprise Registration Center

You have been **denied** network access because this device is not registered to the network.

To obtain network access, you **must** complete registration using the form below

By registering to the network, you are **agreeing** to the terms and conditions explained in the [Enterprise Network and Computer Acceptable-Use Policy](#)

First Name:

Middle Name:

Last Name:

E-Mail Address:

[Complete Registration](#)

Please press the Complete Registration button only once.

Powered by
Extreme networks

xxxx Example Street, Example City, Example State xxxxxx | xxx.xxx.xxxx | ©2013 Example Enterprise [About Us](#) | [Contact Us](#)

When looking at ExtremeControl, the end system information should also be populated with detailed end system information.

When looking at the End-System Details for a device that has not yet gone through registration, the RADIUS attributes that were configured should be shown.

In the End System Events for the device, the audit trail of the states and access assigned will be shown.

St.	Time Stamp	Access Con...	Profile	IP Address	MAC Address	User Name	Host Name	Device Fam...	Device Type	State Descri...	Extended State	Reason	Authorizati...	Auth Type	Switch IP
11/2/2017 12...	192.168.7135	Unregistr...	172.16.57.51	CO:EE:FB:F...			android-414...	Android	Android	Resolving IP A...	Rule: "Unre...	Filter-Id="U...	MAC (PAP)	192.168.7113	
11/2/2017 12...	192.168.7135	Unregistr...	172.16.57.51	CO:EE:FB:F...			android-414...	Android	Android	No Error	Operating S...	Filter-Id="U...	MAC (PAP)	192.168.7113	
11/2/2017 12...	192.168.7135	Guest Acce...	172.16.57.51	CO:EE:FB:F...		Dementyev...	android-414...	Android	Android	No Error	Rule: "Regis...	Filter-Id="G...	MAC (PAP)	192.168.7113	

In the wireless controller, the role application can be verified by locating the wireless client and selecting the Details. The role will be displayed in the window.

Statistics
Wireless Client C0-EE-FB-F8-4C-52

Health
Details
Traffic
WMM TSPEC
Association History
Graph

Wireless Client

SSID	Extreme-WING-Open
Hostname	android-414dad10...
Device Type	Non Voice
RF Domain	remote
OS	Android
Browser	Chrome
Type	Android Tablet
Role	Guest Access
Role Policy	ExtremeControl
Client Identity	Unknown
Client Identity Precedence	0

User Details

UserName	C0-EE-FB-F8-4C-52
Authentication	mac
Encryption	none
Captive Portal Auth.	✗ No

Connection

Idle Time	30m 0s
Last Active	1
Last Association	1m 38s
Session Times	1d 0h 0m 0s
SM PowerSave Mode	off
Power Save Mode	✓ Yes
WMM Support	✓ Yes
40 MHz Capable	✓ Yes
Max Physical Rate	433,300
Max User Rate	324,900

Association

AP	84-24-8D-86-41-7C
BSS	84-24-8D-B3-7F-E0
Radio Number	2
Radio Type	11ac
Rates	6 9 12 18 24 36 48 54 mcs-1s

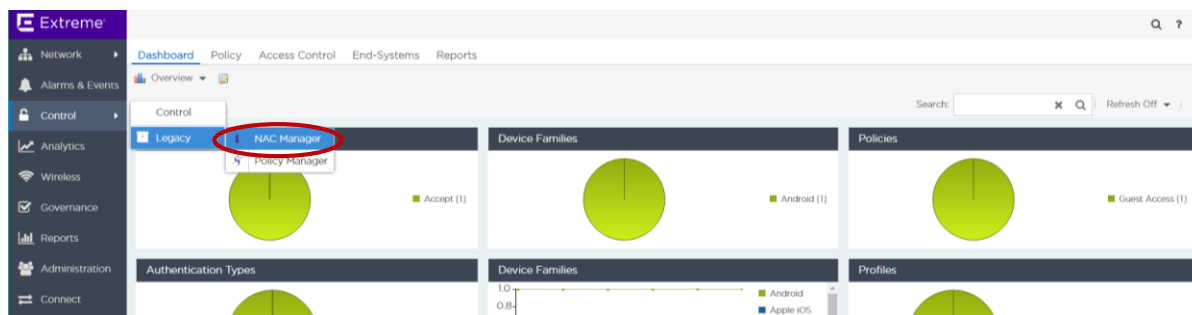
802.11 Protocol

High-Throughput	✓ Supported
RIFS	✗ Unsupported
Unscheduled PASD	Disabled
AID	1
Max AMSDU Size	3,839
Max AMPDU Size	1,048,575
Interframe Spacing	16
Short Guard Interval	✓ Supported

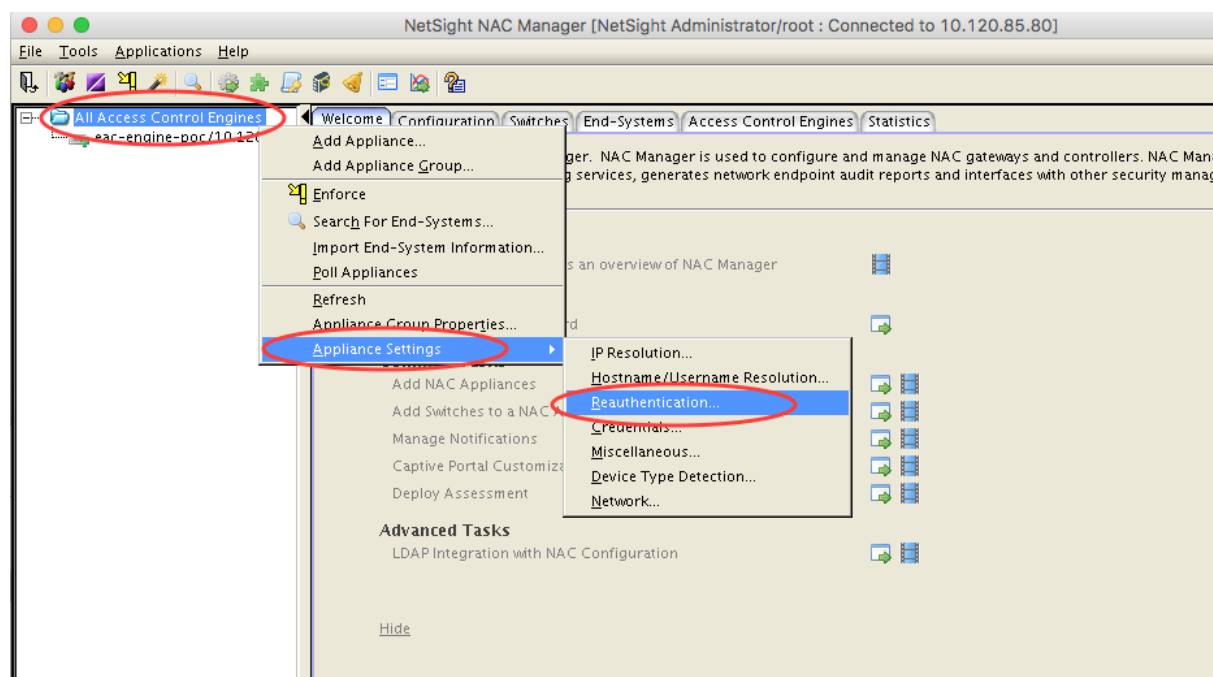
Refresh **Exit**

Appendix A: Creating RFC 3576 Configurations

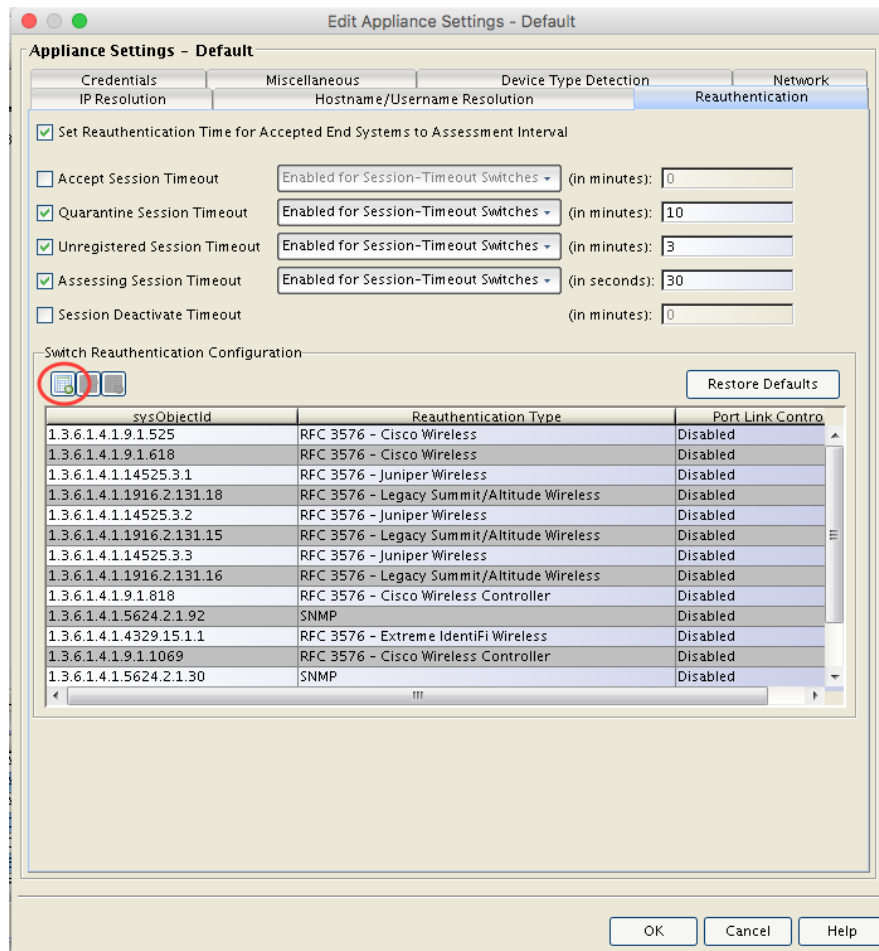
In the case where the RFC 3576 reauthentication configuration is not available, it will need to be manually created via the NAC Manager java client. To open the client, navigate to the **Legacy** section of the **Control** tab and select **NAC Manager**.



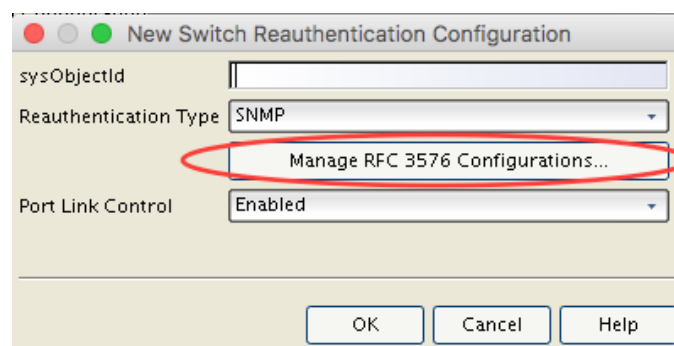
Once in NAC Manager, right-click on the **All Access Control Engines** group and select **Appliance Settings** → **Reauthentication**.



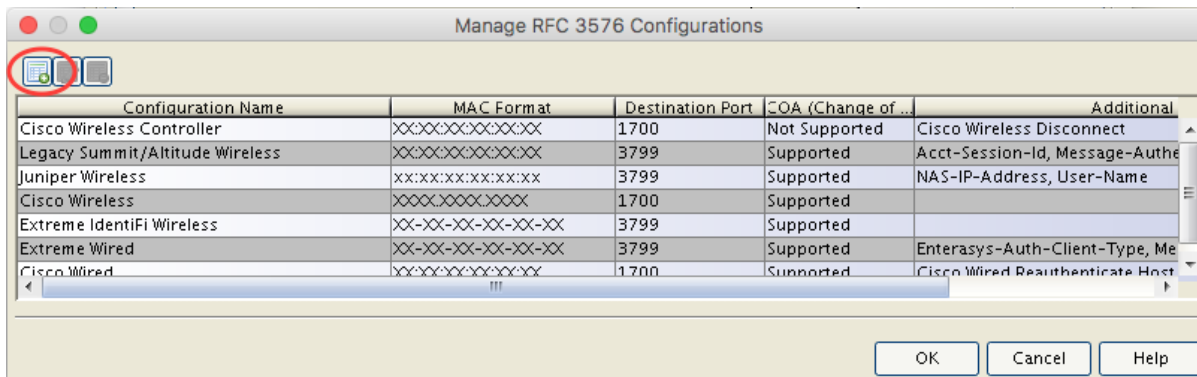
Select the **Add** button to create a new **Switch Reauthentication Configuration**.



In the new Switch Reauthentication Configuration window, select **Manage RFC 3576 Configurations**.



Select the **Add** button to create a new RFC 3576 Configuration.

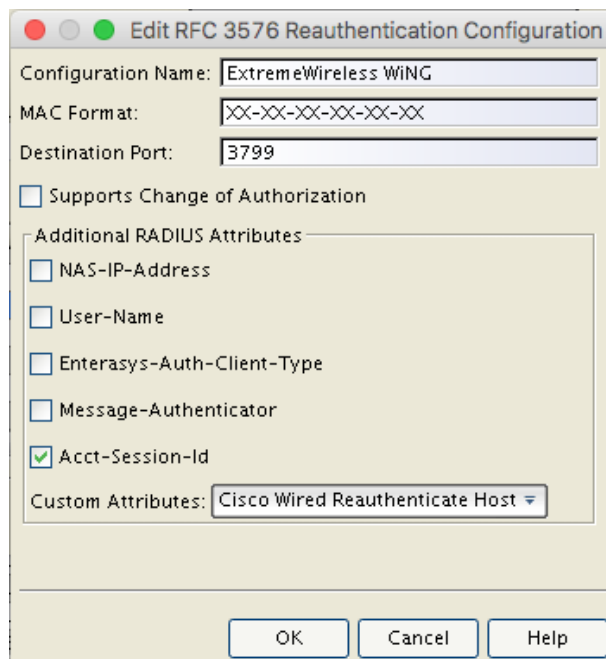


Use the following settings in the new RFC 3576 Configuration and then press OK to save the configuration.

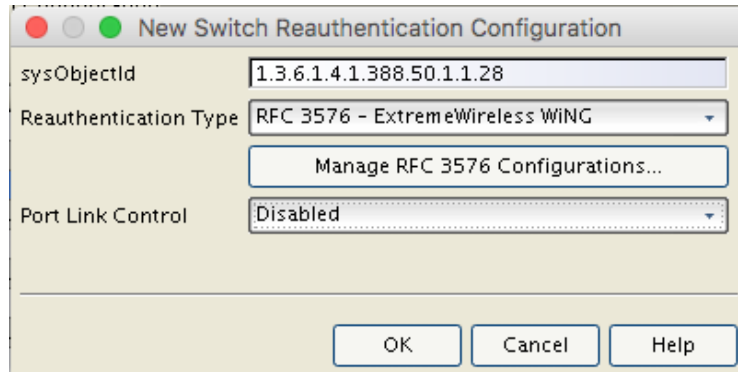
Configuration Name: ExtremeWireless WiNG
 MAC Format: XX-XX-XX-XX-XX-XX
 Destination Port: 3799
 Supports CoA: Enabled

Additional Attributes

Acct-Session-Id: Enabled
 Custom Attributes: Cisco Wired Reauthenticate Host



Press **OK** to save the RFC 3576 Configurations. If the sysObjectId of the wireless controller is known, it can be mapped to the reauthentication configuration in the window below. Otherwise select Cancel and the configuration can be statically mapped in the Advanced Settings of the Add Switch dialog when adding the wireless controller to Access Control. Enforce the configuration once complete.



Revision History

Date	Revision	Changes Made	Author
11/1/16	1.0	Initial Release	T. Marcotte
11/18/16	1.1	Minor edit regarding CoA.	T. Marcotte
11/02/17	2.0	Supporting clients behind NAT addition	V.Dementyev/Y.Ostrovsky