



# ExtremeControl HOW-TO Guide Deploy with ExtremeCloud IQ

**Abstract:** This document covers implementation of ExtremeCloud IQ APs in ExtremeControl. Note that this guide only provides guidance on the configuration of the wireless to integrate with ExtremeControl and does not cover implementation of ExtremeControl functionalities.

**Published:** April 2020

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](http://www.extremenetworks.com)

©2020 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](http://www.extremenetworks.com/company/legal/trademarks).

# Contents

---

<b>Prerequisites and Limitations .....</b>	<b>3</b>
<b>Overview .....</b>	<b>4</b>
<b>Part 1: Wireless Configuration of ExtremeCloud IQ (XIQ) .....</b>	<b>5</b>
Step 1 – Configure SNMP .....	6
Step 2 – Enable SNMP on the Device Template. ....	8
Step 3 – Configure RADIUS .....	10
Step 4 – Configure User Profiles .....	11
Create an EnterpriseUser User Profile .....	12
Create a GuestAccess User Profile with Firewall .....	13
Create an Unregistered User Profile with Firewall and Captive Portal .....	15
Step 5 – Configuring SSIDs for ExtremeControl .....	17
Create a Secure 802.1X SSID .....	18
Create an Open / Guest SSID .....	23
<b>Part 2: Configuring ExtremeControl .....</b>	<b>25</b>
Step 1 – Create an SNMP Profile for Access Points .....	25
Step 2 – Add the Access Point to ExtremeControl .....	26
Step 3 – Configure Captive Portal Settings .....	29
Step 4 – Configure Rules, Roles, and Policy Mappings .....	30
<b>Part 3: Validation .....</b>	<b>33</b>
Secure SSID Validation .....	33
Guest SSID Validation .....	35
<b>Appendix A: Creating RFC 3576 Configurations .....</b>	<b>41</b>
<b>Appendix B: Enable RFC 3576 Reauthentication on XIQ .....</b>	<b>43</b>
<b>Appendix C: DHCP Fingerprint for XIQ Access Points .....</b>	<b>45</b>
<b>Appendix D: Vendor Profile for XIQ Access Points .....</b>	<b>47</b>
<b>Appendix E: RADIUS Reponse Formatting .....</b>	<b>48</b>
<b>Appendix F: XMC licensing .....</b>	<b>51</b>
<b>Revision History .....</b>	<b>53</b>

## Prerequisites and Limitations

---

The scope of this document is intended for SE's and partners that are familiar with both ExtremeCloud IQ and ExtremeControl. Only the primary touch points between the two products are covered in this document and all other settings are considered out of scope.

This document was originally written using the following firmware and software versions.

- Extreme Management Center (XMC) 8.4.0.116
- ExtremeControl 8.4.0.116
- ExtremeCloud IQ Build Version 19.11.1.7 with AP Firmware 10.0.r7a

Due to the nature of adding Access Points as devices that can authenticate against ExtremeControl, there are a couple of design limitations and suggestions that should be followed.

- It is highly recommended that DHCP Reservations are created for Access Points that connect to the network. If an Access Point changes its IP Address, it needs to be re-added to XMC and Control.
- While this guide shows how to add individual Access Points to ExtremeControl, when adding multiple Access Points, it is recommended to use one of the Device Discovery methods in XMC.

## Overview

---

This document is broken up into three major sections. The first is configuring the Wireless Network to authenticate against ExtremeControl. The second handles configuration of ExtremeControl to recognize requests from the wireless network and respond in a format that can be properly interpreted by the Access Point. Lastly, the third section validates the configuration of the entire solution.

A brief summary of the interactions between the Access Point and ExtremeControl can be broken down into the following steps:

1. As the device connects to the wireless SSID, either MAC-based authentication or 802.1X authentication occurs.
2. The Access Point sends a RADIUS request destined to the Access Control Engine for authentication.
3. The Access Control Engine authenticates and authorizes the RADIUS request per its configuration. It passes back a RADIUS Accept message with attributes that the Access Point can interpret such as Filter-ID.
4. The Access Point matches the attributes to a User Profile.
5. If the User Profile is set to redirect the client's web traffic, the Access Point intercepts the web requests and redirects based on IP Filter rules.
6. Upon change of access, such as successful Web Registration, the Access Control Engine sends a Change of Authorization (CoA) message to the Access Point to change the User Profile assigned to the device.

### 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 the Access Control Engine can query to assist with IP resolution.

## Part 1: Wireless Configuration of ExtremeCloud IQ (XIQ)

---

The following configurations on ExtremeCloud IQ (XIQ) are required in order to integrate with ExtremeControl:

- SNMPv3 Polling
- RADIUS Authentication
- RADIUS Accounting
- RFC 3576/5176 Reauthentication
- External Captive Portal Redirection

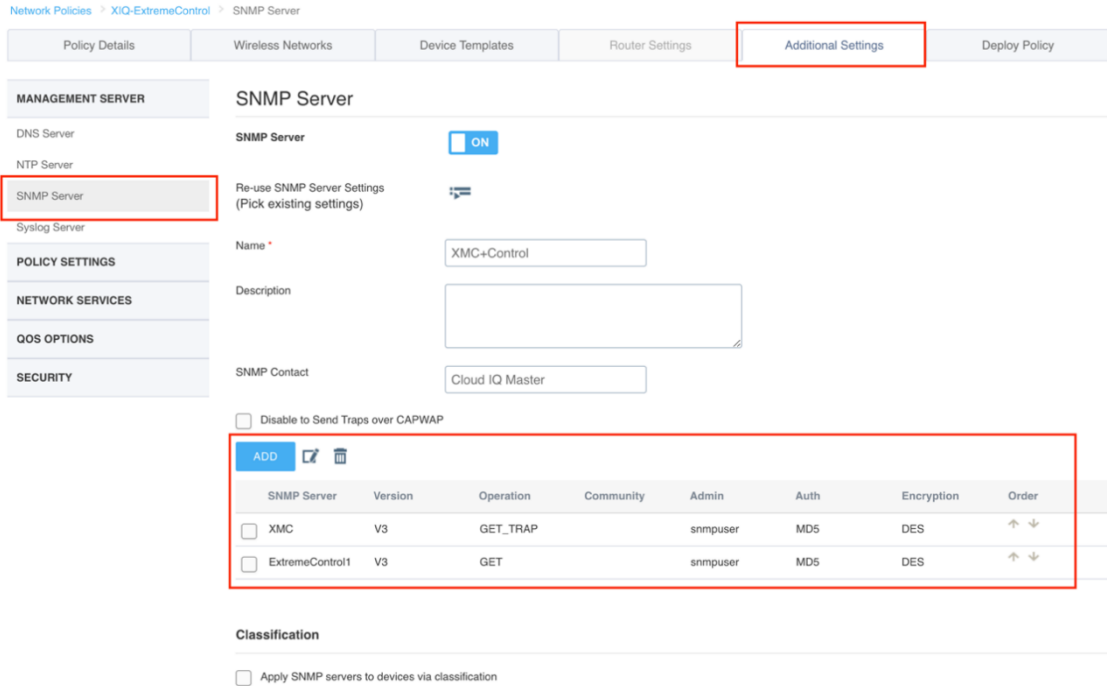
The configuration of the Access Point is done through XIQ. Once configuration is complete, all processing and authentication occurs between the Access Point and ExtremeControl.

The configuration consists of following parts:

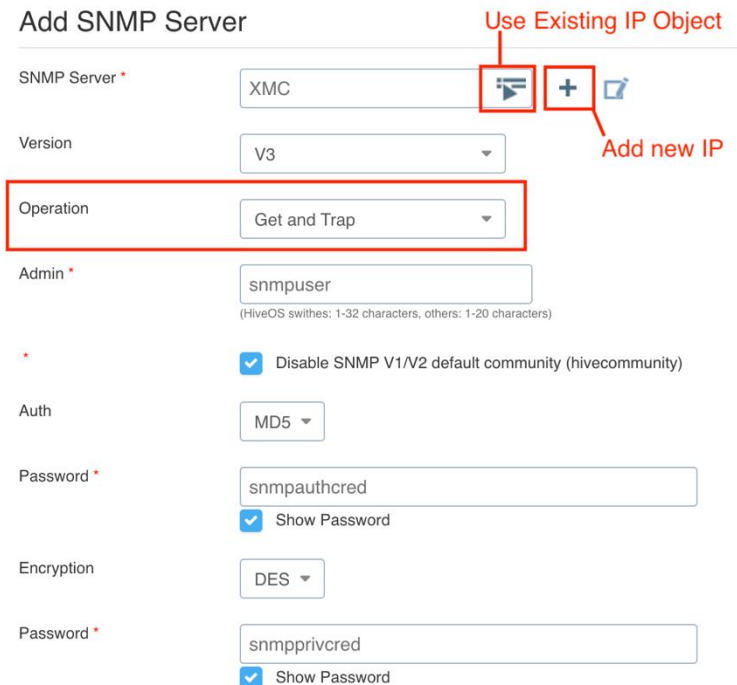
1. Configure an SNMP Server profile so that Extreme Management Center (XMC) and the Access Control Engines can poll the AP.
2. Enable SNMP on the Device Templates for all APs.
3. Configure the RADIUS settings to authenticate against the Access Control Engines.
4. Configure the User Profiles that will be assigned from Access Control. This also includes the IP Filters that are used within the profiles.
5. Configure the SSID for authentication against ExtremeControl.

# Step 1 – Configure SNMP

Configuration of the SNMP profile should contain Extreme Management Center and all Access Control Engines. To configure the SNMP Profile, edit the **Network Policy** in the **Configure** menu. The settings are configured in the **Additional Settings** tab. In the **Management Server** section the **SNMP Server** configuration can be found.





When adding a new SNMP Server entry, if the IP of the server does not exist in XIQ, a new IP Object needs to be created. Otherwise an existing IP can be selected. Note that when configuring the SNMP Server for XMC, both the **Get and Trap** operations are configured.



When configuring the SNMP Profile for the Access Control Engine, the same SNMP credentials that were used for XMC are used for the Access Control Engine. A new IP Object may need to be created for each Access Control Engine that will be used. In addition, the Operation should be set to **Get** as Access Control Engines do not process SNMP Traps from the APs.

### Add SNMP Server

SNMP Server *	ExtremeControl1  
Version	V3
Operation	Get
Admin *	snmpuser <small>(HiveOS switches: 1-32 characters, others: 1-20 characters)</small>
*	<input checked="" type="checkbox"/> Disable SNMP V1/V2 default community (hivecommunity)
Auth	MD5
Password *	snmpauthcred <input checked="" type="checkbox"/> Show Password
Encryption	DES
Password *	snmpprivcred <input checked="" type="checkbox"/> Show Password

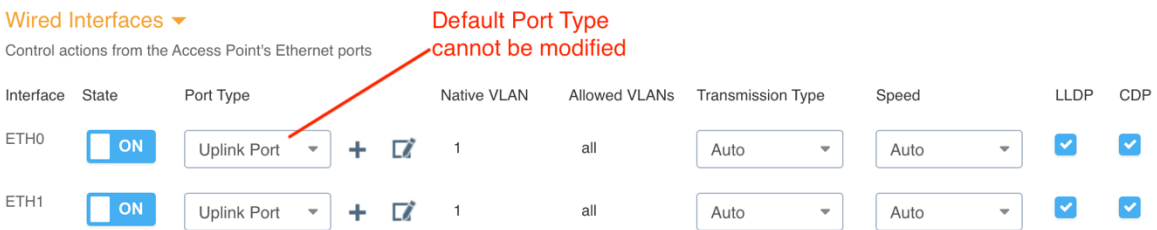
## Step 2 – Enable SNMP on the Device Template.

The default setting for an Access Points is to not allow SNMP. In order to enable SNMP on the Access Points it needs to be enabled on the wired uplink port. Since default templates cannot be edited in XIQ, a new template must be created. This process is most easily performed by cloning the existing object, and then adjusting it as needed.

Navigate to the Device Templates by editing the **Network Policy** in the **Configure** menu. In the **Device Templates** each AP Template needs to be added or modified if it already exists. Select the Template to edit:

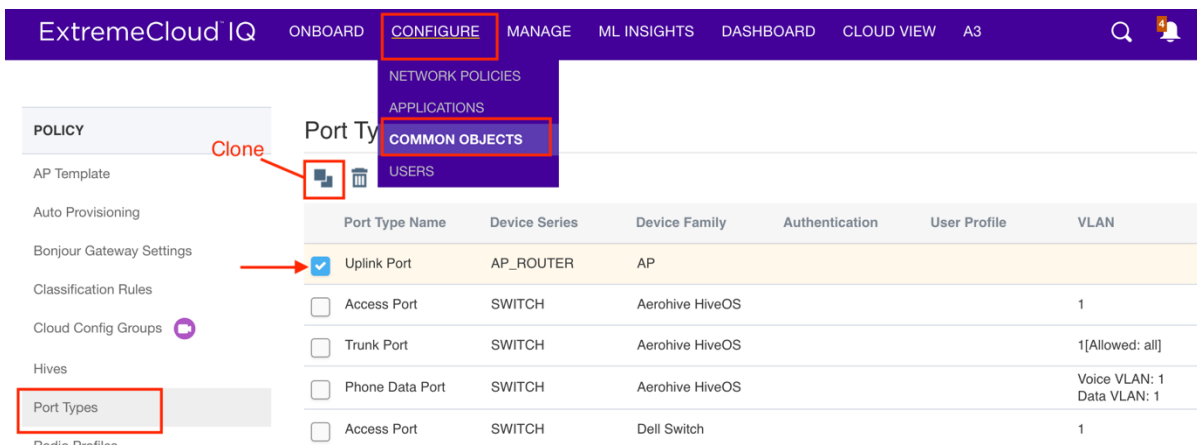


At the **Wired Interfaces** section, find the interface which will be used to communicate to the Access Control Engine. If the default port type of **Uplink Port** is in use, then the Port Type will need to be cloned. If it is a non-default port type, skip the next steps with instructions on creating a custom Port Type.

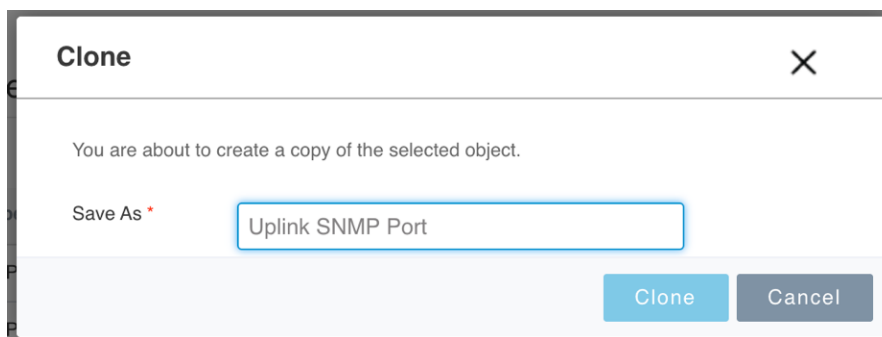




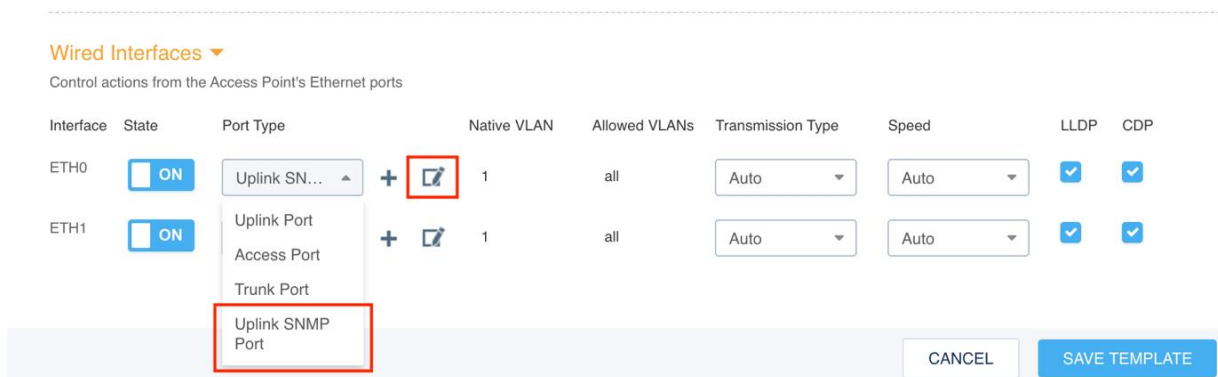
To clone the default Port Type, navigate to **Common Objects** under the **Configure** tab. Select **Port Types** from the **Policy** section. Select the default port type that was previously configured and then clone.



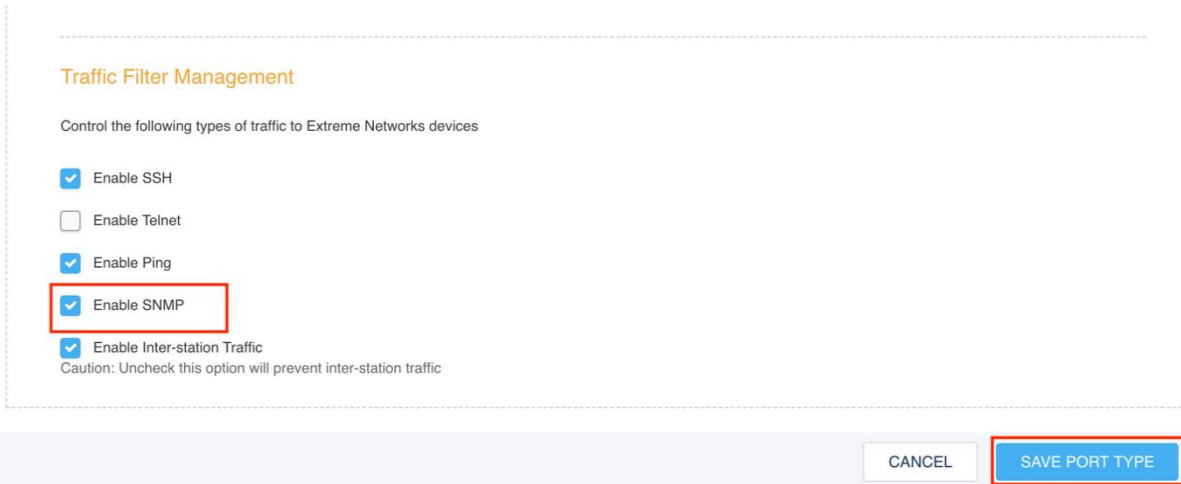
Name the new Port Type and select **Clone**.



Once cloned, navigate back to the **Device Templates** and **Wired Interfaces** section. From the dropdown list, select the newly created Port Type followed by the Edit button.



Check the **Enable SNMP** option under **Traffic Filter Management**. Finish by selecting the **Save Port Type** box. Repeat the Port Type selection for any other Device Templates that are used.



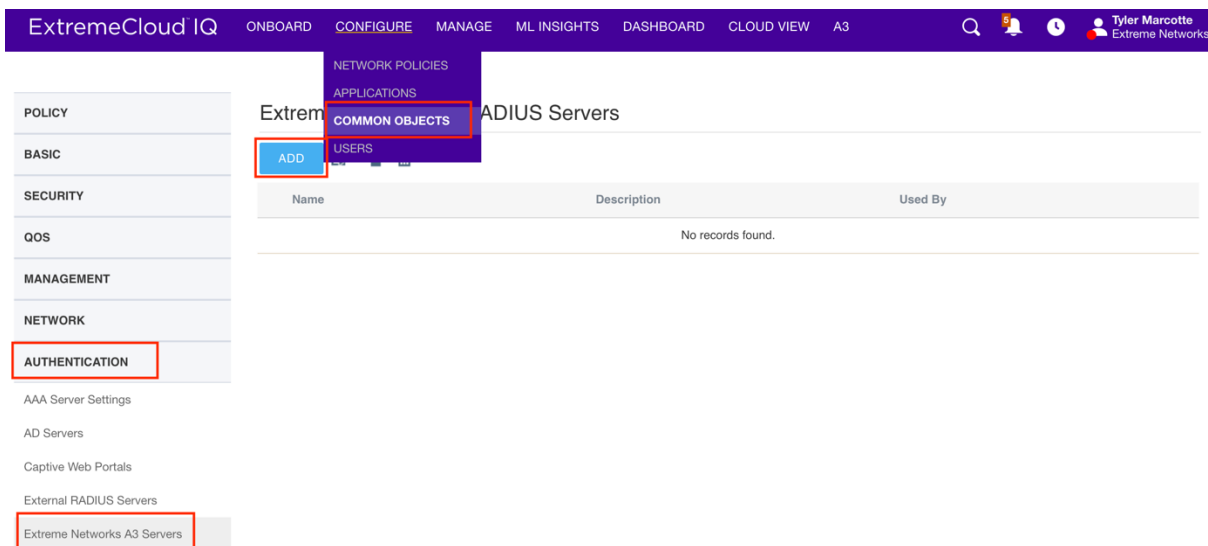
### Step 3 – Configure RADIUS

The RADIUS Server configuration can be performed in two unique ways. One method is to create it while creating the SSID. However, the method shown below is to create the Common Object prior to creating the SSID.

**Note**

The Access Control Engines are added to ExtremeCloud IQ as A3 servers rather than External RADIUS Servers. The reason they are added this way is because the RFC 3576 Change of Authorization settings are automatically configured using this method. If added as an External RADIUS Server, RFC 3576 needs to be manually configured as referenced in Appendix B.

Under the **Configure** menu, select **Common Objects**. On the left panel, expand **Authentication** and select **Extreme Networks A3 Servers**. With this section selected, select the **Add** button to create a new entry for the Access Control Engines.





In the new entry, select the **IP Object** that was previously created when enabling SNMP. Leave the default port settings. Specify a **Shared Secret** to be used with ExtremeControl. **ETS\_TAG\_SHARED\_SECRET** is the default Shared Secret used by ExtremeControl and can be used for testing and proof of concepts. For a real deployment, it is expected that the Shared Secret will be changed from the defaults. Save the new server and repeat the process for all Access Control Engines.

Extreme Networks A3 Servers > Create External RADIUS Server

### External RADIUS Server

Name \*

Description

IP/Host Name \*   + 

Server Type \*

Authentication Port:  Select existing IP Object

Accounting Port:

Shared Secret   Show Password

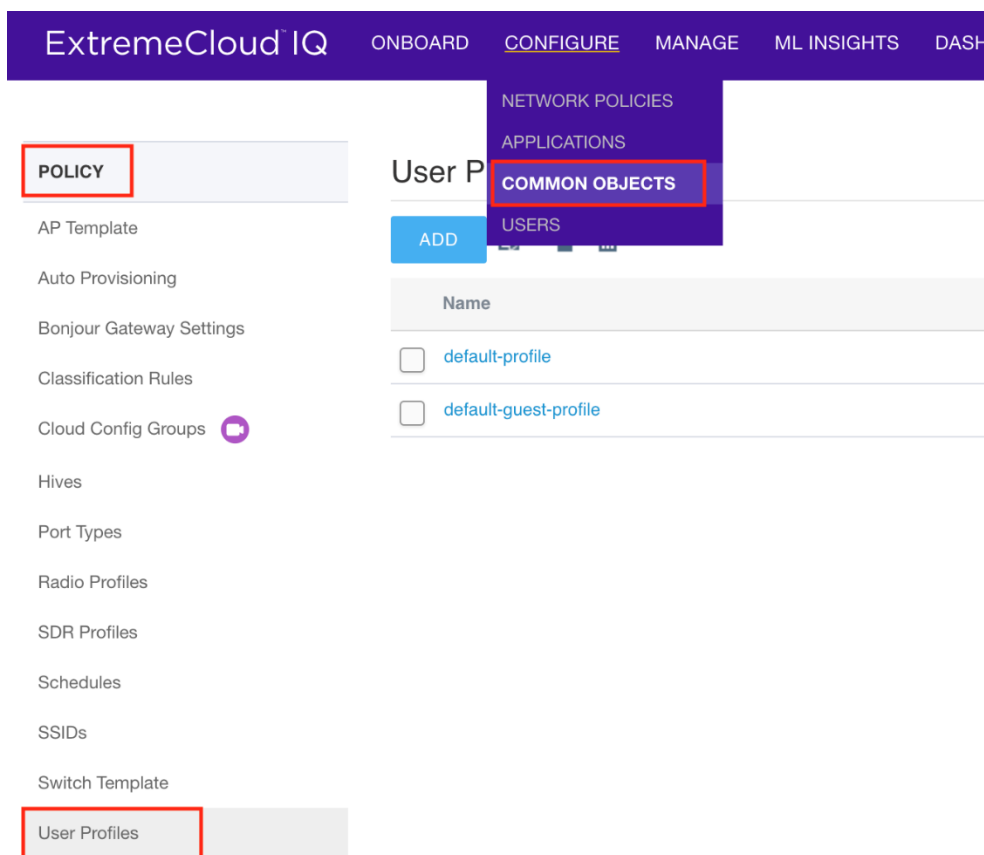
## Step 4 – Configure User Profiles

User Profiles define the access that a user or device has when connected to the network via ExtremeCloud IQ. These profiles can be dynamically assigned and contain many definitions including Firewall Rules, VLAN assignment, and QoS settings. These profiles need to be defined prior to assignment and should represent the Accept Policies that are assigned from ExtremeControl via the rules engine.

The minimum recommended User Profiles to be created are:

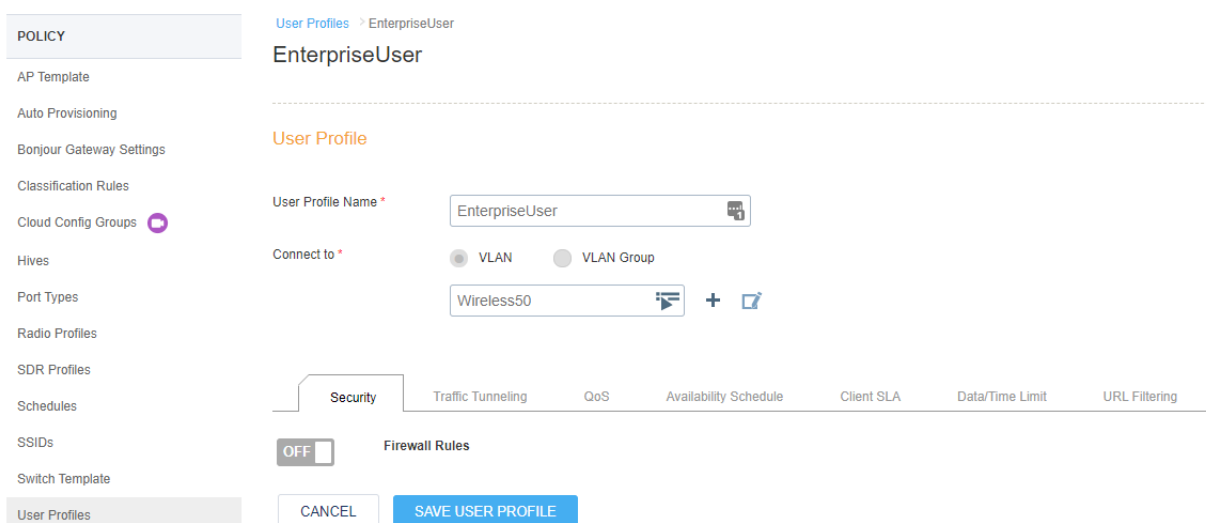
- Unregistered – This profile limits traffic and redirects web traffic to ExtremeControl
- GuestAccess – This profile limits internal traffic but allows full access to the Internet.
- EnterpriseUser – This profile allows full access onto the network.

The User Profiles can be found under the **Common Objects** in the **Configure** menu. Select **User Profiles** in the **Policy** section.



### Create an EnterpriseUser User Profile

To create a new User Profile, select the **Add** button. Define the **User Profile Name** and **VLAN** (or VLAN Group). When selecting a VLAN, a new VLAN Object needs to be created or selected. Additional settings can be configured if desired. However, this is an example of only a VLAN being assigned to a user or device.



## Create a GuestAccess User Profile with Firewall

When adding a Firewall to a User Profile, it can be added inline with the profile, or a Common Object for IP Firewall can be created prior to the User Profile. For common configuration such as Guest Access firewalls or Redirection firewalls, it is often helpful to clone the default objects to save time and configuration.

To create or clone an IP Firewall Policy, choose **IP Firewall Policies** from the **Security** section of the **Common Objects**.

IP Firewall Policies

Name	Description	Used By
<input checked="" type="checkbox"/> Guest-Internet-Access-Only	Default IP policy that allows Internet access only	+
<input type="checkbox"/> Redirect-Only	Default IP policy that allows redirect only	+

Name the new policy and select edit. In the new policy, some rules need to be adjusted or added. In particular for the GuestAccess policy, ensure that web traffic can reach ExtremeControl so the registration success page can be displayed. To add a new rule, select the **Add** button.

IP Firewall Policies > Guest-Internet-Only-Control

Guest-Internet-Only-Control

Name: Guest-Internet-Only-Control

Description: Allows Internet access and Captive Portal

Source IP	Destination IP	Service	Action	Logging	Order
<input type="checkbox"/> Any	Any	DHCP-Server	PERMIT	BOTH	↑ ↓
<input type="checkbox"/> Any	Any	DNS	PERMIT	BOTH	↑ ↓
<input type="checkbox"/> Any	10.0.0.0/255.0.0.0	Any	DENY	DROPPED_PACKETS	↑ ↓
<input type="checkbox"/> Any	172.16.0.0/255.240.0.0	Any	DENY	DROPPED_PACKETS	↑ ↓
<input type="checkbox"/> Any	192.168.0.0/255.255.0.0	Any	DENY	DROPPED_PACKETS	↑ ↓
<input type="checkbox"/> Any	Any	Any	PERMIT	BOTH	↑ ↓

CANCEL SAVE

While creating a new rule to allow traffic to the Access Control Engine, set the Destination IP to the IP Object previously created for the Access Control Engines. Repeat this process for each engine that will be used.

IP Firewall Policies > Guest-Internet-Only-Control > New IP Firewall Rule

### New IP Firewall Rule

Select services such as HTTP or HTTPS if desired

Service:

Source IP:

Destination IP:

Action:

Logging:

When the rule is saved, ensure it is placed correctly in the Firewall Policy. Since the list is ordered, use the **Up** and **Down** arrows to position the rule appropriately.

IP Firewall Policies > Guest-Internet-Only-Control

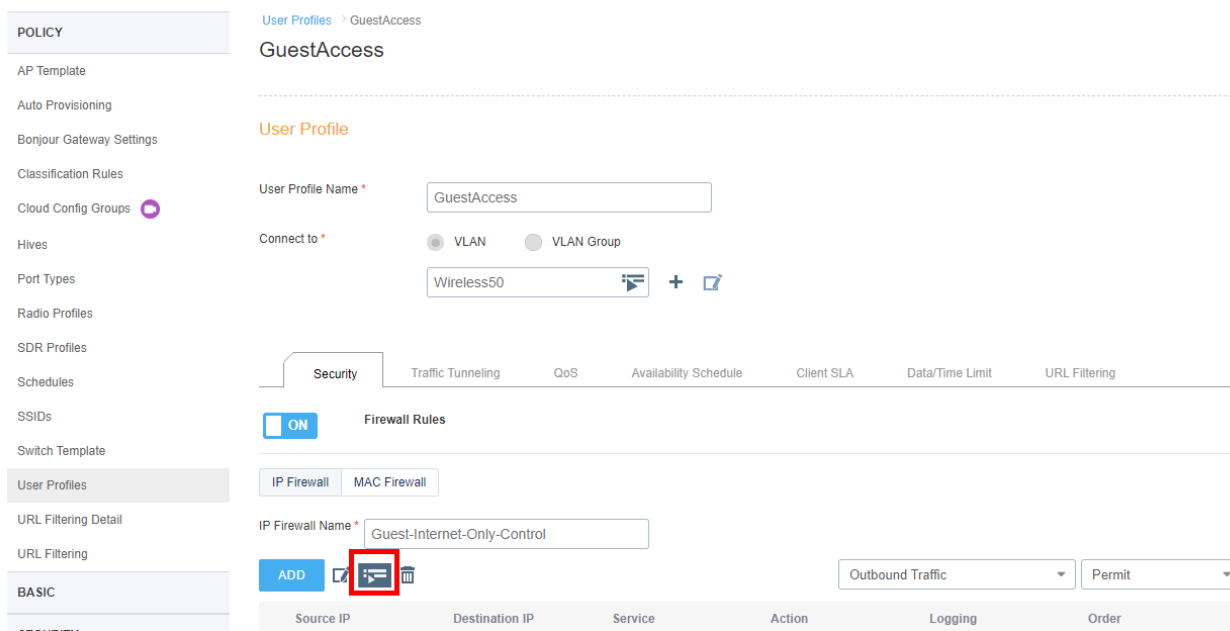
### Guest-Internet-Only-Control

Name:

Description:

	Source IP	Destination IP	Service	Action	Logging	Order
<input type="checkbox"/>	Any	Any	DHCP-Server	PERMIT	BOTH	↑ ↓
<input type="checkbox"/>	Any	Any	DNS	PERMIT	BOTH	↑ ↓
<input type="checkbox"/>	Any	ExtremeControl1	Any	PERMIT	BOTH	↑ ↓
<input type="checkbox"/>	Any	10.0.0.0/255.0.0.0	Any	DENY	DROPPED_PACKETS	↑ ↓
<input type="checkbox"/>	Any	172.16.0.0/255.240.0.0	Any	DENY	DROPPED_PACKETS	↑ ↓
<input type="checkbox"/>	Any	192.168.0.0/255.255.0.0	Any	DENY	DROPPED_PACKETS	↑ ↓
<input type="checkbox"/>	Any	Any	Any	PERMIT	BOTH	↑ ↓

In the **User Profiles** create a profile with the name GuestAccess. In addition to setting the VLAN, select the **IP Firewall Name** defined in the previous step.



### Create an Unregistered User Profile with Firewall and Captive Portal

Similar to a GuestAccess User Profile, the Unregistered User Profile needs to have an IP Firewall added to limit access as well as redirect web traffic to ExtremeControl.

In the **Security** menu choose **IP Firewall Policies** and create IP Firewall Policy or clone the default Redirect-Only policy. Set the name and add rules by selecting the **Add** button.



For the captive portal to work, the following rules need to be configured. This example shows one Access Control Engine. However, all Access Control Engines that provide a captive portal should be configured.

Order	Source IP	Destination IP	Service	Action
1	ANY	ANY	DHCP-Server	PERMIT
2	ANY	ANY	DHCP-Client	PERMIT
3	ANY	ANY	DNS	PERMIT
4	ANY	ExtremeControl1	HTTP	PERMIT
5	ANY	ANY	HTTP	REDIRECT
6	ANY	ExtremeControl1	HTTPS	PERMIT
7	ANY	ANY	HTTPS	REDIRECT

IP Firewall Policies > Redirect-2-Control

### Redirect-2-Control

Name \*

Description

ADD  

	Source IP	Destination IP	Service	Action	Logging	Order
<input type="checkbox"/>	Any	Any	DHCP-Server	PERMIT	OFF	↑ ↓
<input type="checkbox"/>	Any	Any	DHCP-Client	PERMIT	OFF	↑ ↓
<input type="checkbox"/>	Any	Any	DNS	PERMIT	OFF	↑ ↓
<input type="checkbox"/>	Any	ExtremeControl1	HTTP	PERMIT	OFF	↑ ↓
<input type="checkbox"/>	Any	Any	HTTP	REDIRECT	OFF	↑ ↓
<input type="checkbox"/>	Any	ExtremeControl1	HTTPS	PERMIT	OFF	↑ ↓
<input type="checkbox"/>	Any	Any	HTTPS	REDIRECT	OFF	↑ ↓

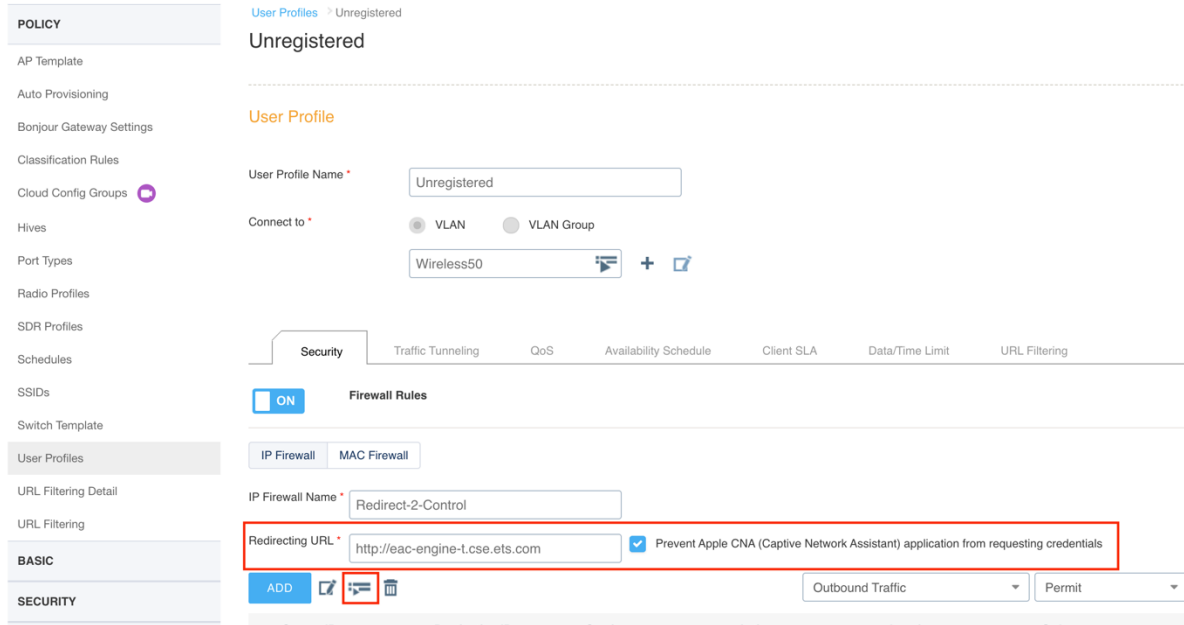
CANCEL SAVE

#### Note

The REDIRECT Action is only visible when the HTTP or HTTPS Services are configured.

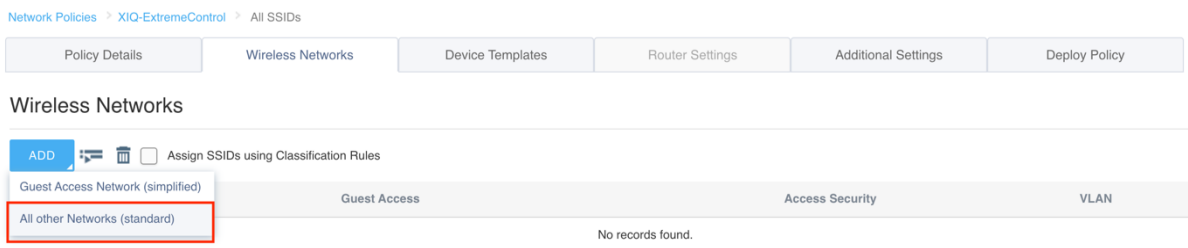


In the **User Profiles**, create a new profile with the name Unregistered, set the VLAN, and select the **IP Firewall Name** defined in the previous step. The **Redirection URL** should contain the FQDN of the Access Control Engine. Additionally, the checkbox for **Prevent Apple CNA** should be selected as ExtremeControl manages the popup windows for devices.



## Step 5 – Configuring SSIDs for ExtremeControl

The creation of the SSID is configured as part of the Network Policy under Wireless Networks. To create a new Wireless Network, it's recommended to select **All other Networks (standard)** from the drop down options.



## Create a Secure 802.1X SSID

To create a secure SSID that uses 802.1X authentication, set the name of the wireless network and select **Enterprise WPA / WPA2 / WPA3** under SSID Authentication. The default settings for Key Management, Encryption Method, and Captive Web Portal can be left unchanged.

Network Policies > XIQ-ExtremeControl > All SSIDs > New SSID

Policy Details | Wireless Networks | Device Templates | Router Settings | Additional Settings | Deploy Policy

**CONFIGURATION GUIDE**

Policy Name: XIQ-ExtremeControl

SSID (Name): XIQ-Control-Secure

RADIUS Server Group: + Add RADIUS Server Group

**Wireless Network**

Name (SSID) \* XIQ-Control-Secure

Broadcast Name \* XIQ-Control-Secure

Broadcast SSID Using

- WiFi0 Radio (2.4 GHz or 5 GHz)
- WiFi1 Radio (5 GHz only)

**SSID Usage**

SSID Authentication | MAC Authentication

Enterprise WPA / WPA2 / WPA3 | Personal WPA / WPA2 / WPA3 | Private Pre-Shared Key | WEP | Open Unsecured

Key Management: WPA2-802.1X

Encryption Method: CCMP (AES)

Enable Captive Web Portal: OFF

Once the Enterprise SSID Authentication method is selected, an option appears further down the screen to configure Authentication Settings. If a RADIUS Server Group has not been created yet, select the **Add** button to create a new one.

### Authentication Settings

Authentication with ExtremeCloud IQ Authentication Service  OFF

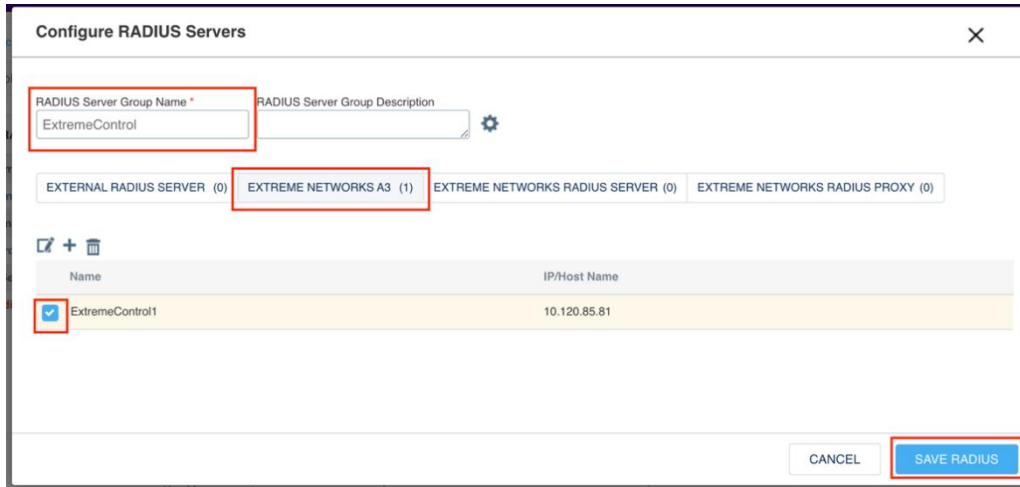
### Authenticate via RADIUS Server

Default RADIUS Server Group

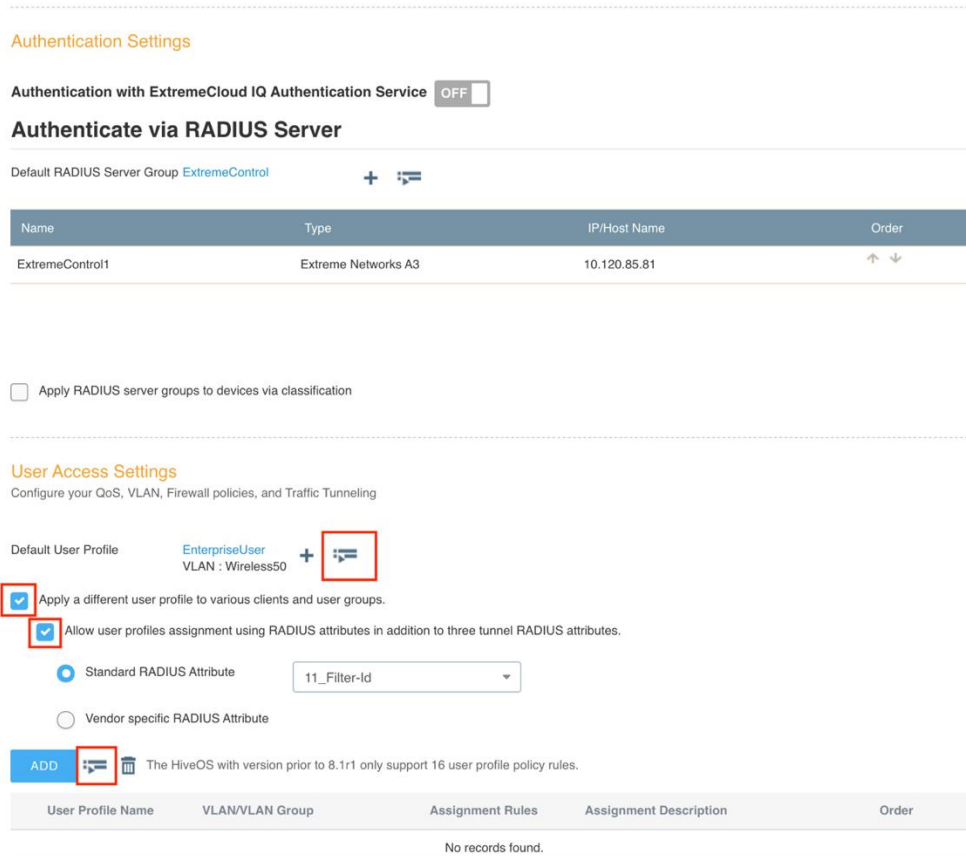
Name	Type	IP/Host Name	Order
No records found.			

Apply RADIUS server groups to devices via classification

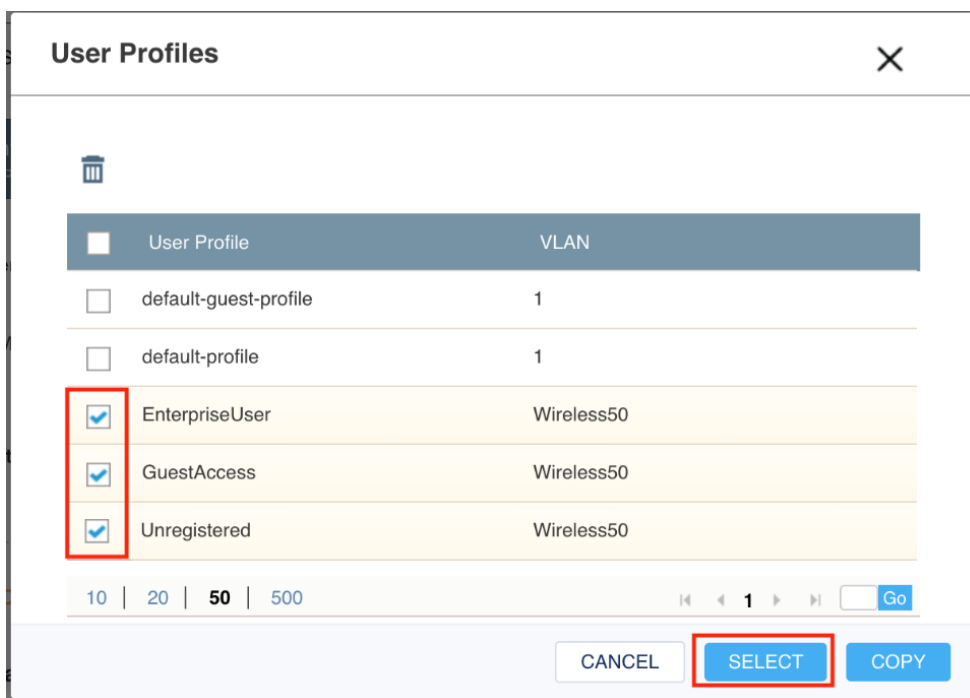
In the Configure RADIUS Servers window, set a name for the RADIUS Server Group and select the previously configured Access Control Engine from the **Extreme Networks A3** tab.



With the RADIUS Servers configured, the **User Access Settings** section needs to be configured to assign the correct User Profiles based on the authorization results from ExtremeControl. First select the **Default User Profile** to be used if no other profiles match. Next, select the two checkboxes shown below to apply different user profiles based on a Filter-ID. With the checkboxes enabled, the User Profiles that were previously created need to be selected so they can be utilized.



In the **User Profiles** window, enable the desired User Profiles and then click the **Select** button.



With the User Profiles added, select the **+** option to create a new User Profile Assignment Rule for each User Profile. If an assignment rule was previously created, utilize the arrow icon next to the plus icon to re-use the assignment rules.

### User Access Settings

Configure your QoS, VLAN, Firewall policies, and Traffic Tunneling

Default User Profile EnterpriseUser **+**

VLAN : Wireless50

- Apply a different user profile to various clients and user groups.
  - Allow user profiles assignment using RADIUS attributes in addition to three tunnel RADIUS attributes.
    - Standard RADIUS Attribute 11\_Filter-Id
    - Vendor specific RADIUS Attribute

**ADD** The HiveOS with version prior to 8.1r1 only support 16 user profile policy rules.

User Profile Name	VLAN/VLAN Group	Assignment Rules	Assignment Description	Order
<input checked="" type="checkbox"/> EnterpriseUser	Wireless50			↑ ↓
<input type="checkbox"/> GuestAccess	Wireless50		Add a user profile assignment rule	↑ ↓
<input type="checkbox"/> Unregistered	Wireless50			↑ ↓

Additional Settings

Name the User Profile Assignment, select the **+** button, and then select the **RADIUS Attribute**.

**User Profile Assignment**

Name: EnterpriseUser

Description:

Assign user profiles to clients or users connecting to an SSID according to authentication and other client classification. All conditions must match for the assignment.

+ [edit] [delete]

RADIUS Attribute	Value
No rules found	

CANCEL SAVE

Enter the Filter-ID that will be returned from ExtremeControl as part of the Authorization rules.

**RADIUS Attribute**

RADIUS Attribute

Assign user profile based on RADIUS attribute value pairs returned in Access-Accept response message

Three standard RADIUS Attribute Value Pairs

- IETF 64 (Tunnel-Type) = GRE(10)
- IETF 65 (Tunnel-Medium-Type) = IP(1)
- IETF 81 (Tunnel-Private-Group-ID) = admin-defined-attribute-value

Attribute Values ?  (1-4095)

A single standard RADIUS Attribute Value Pair

RADIUS Attribute 11\_Filter-Id

Attribute Values

CANCEL OK

**Note**

Spaces in the Filter-ID name should not be used as they will not be matched correctly during authentication.

Repeat the process of creating assignment rules for each User Profile. To easily see all rule assignment, the arrow in each rule can be selected to expand the rule. The rules are ordered for assignment as well. If the order needs to be changed, select the up or down arrows to the right of the rule.

### User Access Settings

Configure your QoS, VLAN, Firewall policies, and Traffic Tunneling

Default User Profile EnterpriseUser +

VLAN : Wireless50

- Apply a different user profile to various clients and user groups.
- Allow user profiles assignment using RADIUS attributes in addition to three tunnel RADIUS attributes.

Standard RADIUS Attribute 11\_Filter-Id

Vendor specific RADIUS Attribute

ADD The HiveOS with version prior to 8.1r1 only support 16 user profile policy rules.

User Profile Name	VLAN/VLAN Group	Assignment Rules	Assignment Description	Order				
<input type="checkbox"/> EnterpriseUser	Wireless50	EnterpriseUser	<div style="border: 1px solid #ccc; padding: 2px;"> <table border="1"> <thead> <tr> <th>Type</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>RADIUS Attribute</td> <td>EnterpriseUser</td> </tr> </tbody> </table> </div>	Type	Value	RADIUS Attribute	EnterpriseUser	
Type	Value							
RADIUS Attribute	EnterpriseUser							
<input type="checkbox"/> GuestAccess	Wireless50	GuestAccess	<div style="border: 1px solid #ccc; padding: 2px;"> <table border="1"> <thead> <tr> <th>Type</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>RADIUS Attribute</td> <td>GuestAccess</td> </tr> </tbody> </table> </div>	Type	Value	RADIUS Attribute	GuestAccess	
Type	Value							
RADIUS Attribute	GuestAccess							
<input type="checkbox"/> Unregistered	Wireless50	Unregistered	<div style="border: 1px solid #ccc; padding: 2px;"> <table border="1"> <thead> <tr> <th>Type</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>RADIUS Attribute</td> <td>Unregistered</td> </tr> </tbody> </table> </div>	Type	Value	RADIUS Attribute	Unregistered	
Type	Value							
RADIUS Attribute	Unregistered							

## Create an Open / Guest SSID

Creating an open SSID is very similar to configuring a secure SSID. The primary difference is in the **SSID Usage** section. In this section, select either **Personal** or **Open** for the SSID Authentication type. Ensure that **Enable Captive Web Portal** is disabled.

Network Policies > XIQ-ExtremeControl > All SSIDs > XIQ-Control-Open

Policy Details | Wireless Networks | Device Templates | Router Settings | Additional Settings | Deploy Policy

**CONFIGURATION GUIDE**

Policy Name: XIQ-ExtremeControl  
 User Profile: Unregistered

**Wireless Network**

Name (SSID): XIQ-Control-Open  
 Broadcast Name: XIQ-Control-Open

Broadcast SSID Using:  
 WiFi0 Radio (2.4 GHz or 5 GHz)  
 WiFi1 Radio (5 GHz only)

**SSID Usage**

SSID Authentication | MAC Authentication

Enterprise WPA / WPA2 / WPA3 | Personal WPA / WPA2 / WPA3 | Private Pre-Shared Key | WEP | **Open Unsecured**

Enable Captive Web Portal: OFF

Select the **MAC Authentication** tab to the right of the **SSID Authentication** tab and enable **MAC Authentication**. Select **MS CHAPV2** as the Authentication protocol and select the **RADIUS Server Group** (e.g. ExtremeControl) previously created for the Secure SSID.

**SSID Usage**

SSID Authentication | **MAC Authentication**

**MAC Authentication**

Enable MAC authentication that uses the MAC address as the username and password to authenticate clients. This is typically used to support legacy clients.

Authentication Protocol: MS CHAP V2

**Authenticate via RADIUS Server**

Default RADIUS Server Group: ExtremeControl

Name	Type	IP/Host Name	Order
ExtremeControl1	Extreme Networks A3	10.120.85.81	↑ ↓

Adjust the User Access Settings so the authorization rules match the Filter-ID that is returned from ExtremeControl. The Assignment Rules can be reused by selecting the arrow icon next in the Assignment Rule as shown below.

### User Access Settings

Configure your QoS, VLAN, Firewall policies, and Traffic Tunneling







Default User Profile Unregistered +   
 VLAN : Wireless50

- Apply a different user profile to various clients and user groups.
- Allow user profiles assignment using RADIUS attributes in addition to three tunnel RADIUS attributes.

Standard RADIUS Attribute 11\_Filter-Id

Vendor specific RADIUS Attribute

ADD   The HiveOS with version prior to 8.1r1 only support 16 user profile policy rules.

User Profile Name	VLAN/VLAN Group	Assignment Rules	Assignment Description	Order				
<input type="checkbox"/> EnterpriseUser	Wireless50	  EnterpriseUser	<table border="1"> <tr> <th>Type</th> <th>Value</th> </tr> <tr> <td>RADIUS Attribute</td> <td>EnterpriseUser</td> </tr> </table>	Type	Value	RADIUS Attribute	EnterpriseUser	↑ ↓
Type	Value							
RADIUS Attribute	EnterpriseUser							
<input type="checkbox"/> GuestAccess	Wireless50	  GuestAccess	<table border="1"> <tr> <th>Type</th> <th>Value</th> </tr> <tr> <td>RADIUS Attribute</td> <td>GuestAccess</td> </tr> </table>	Type	Value	RADIUS Attribute	GuestAccess	↑ ↓
Type	Value							
RADIUS Attribute	GuestAccess							
<input type="checkbox"/> Unregistered	Wireless50	  Unregistered	<table border="1"> <tr> <th>Type</th> <th>Value</th> </tr> <tr> <td>RADIUS Attribute</td> <td>Unregistered</td> </tr> </table>	Type	Value	RADIUS Attribute	Unregistered	↑ ↓
Type	Value							
RADIUS Attribute	Unregistered							



## Part 2: Configuring ExtremeControl

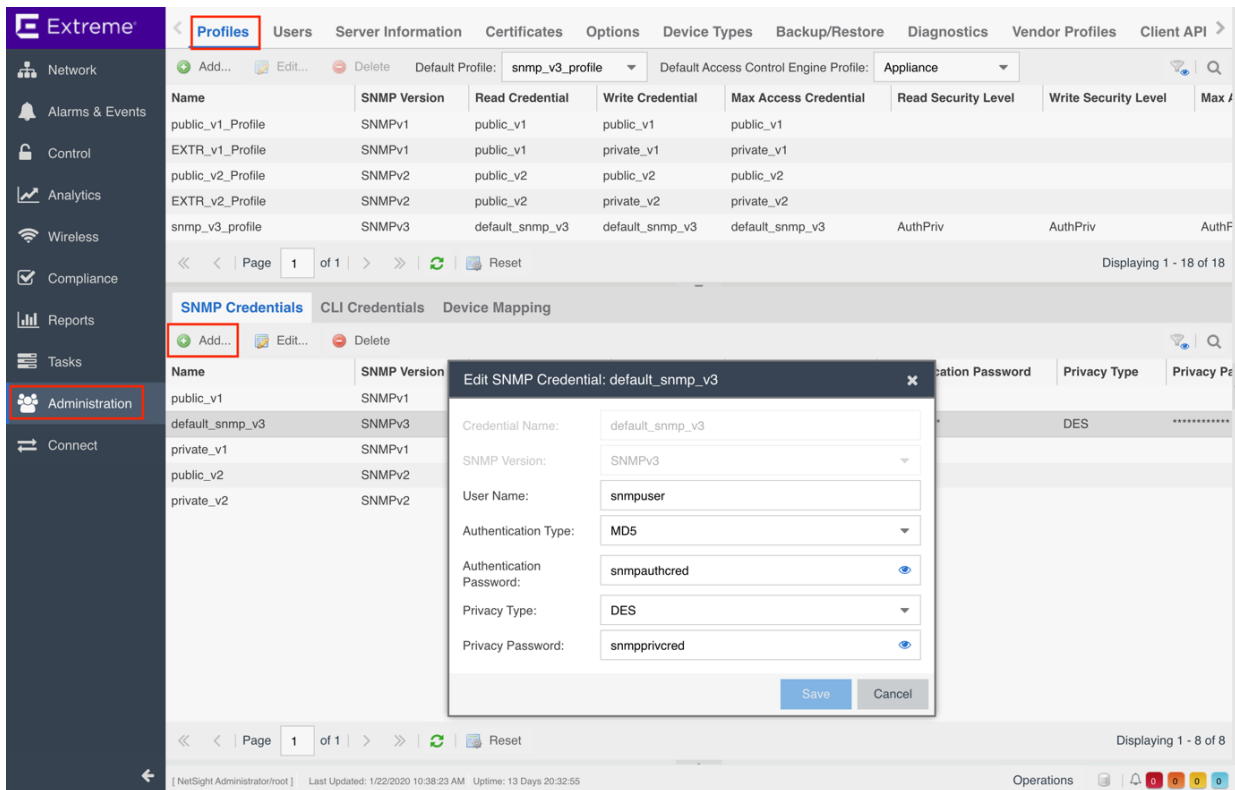
In this section, the Access Point will be added to ExtremeControl as a switch so that clients can be authenticated and controlled.

**Note**

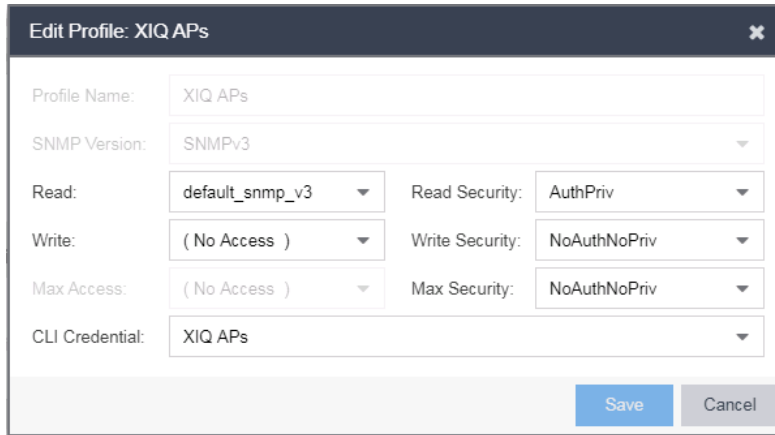
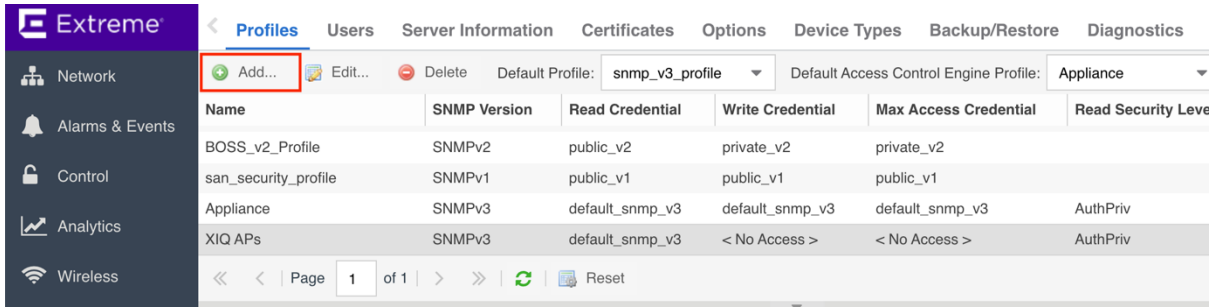
This section assumes that the Access Control Engine is already configured and added to ExtremeControl and that Guest Registration is already enabled.

### Step 1 – Create an SNMP Profile for Access Points

In ExtremeManagement, select the **Profiles** tab under **Administration** and select the **Add** button for **SNMP Credentials**. Create new SNMP credentials that correlate with the credentials configured in ExtremeCloud IQ. The default SNMP credentials can be used if desired.

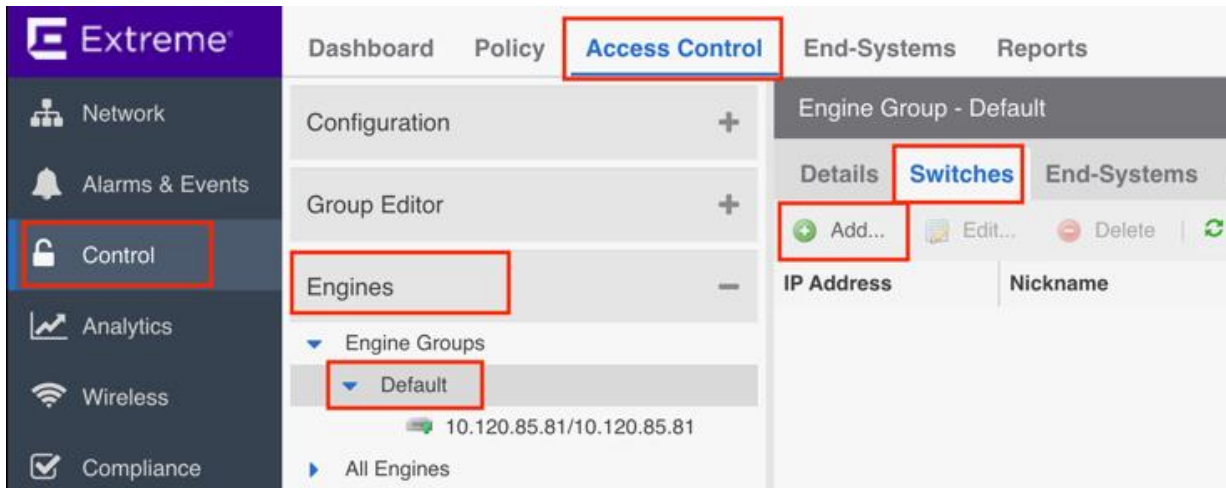


With the SNMP Credentials configured, create a **Profile** to assign to the Access Points. Ensure that the SNMP settings are configured for **AuthPriv** for the SNMP Read.

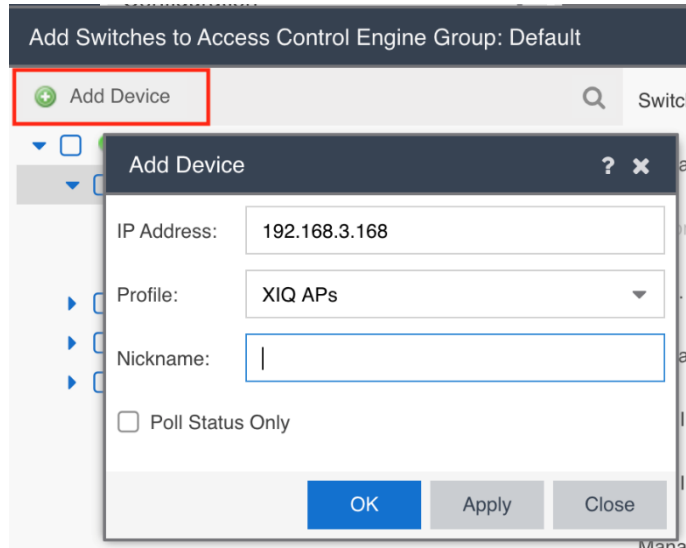


## Step 2 – Add the Access Point to ExtremeControl

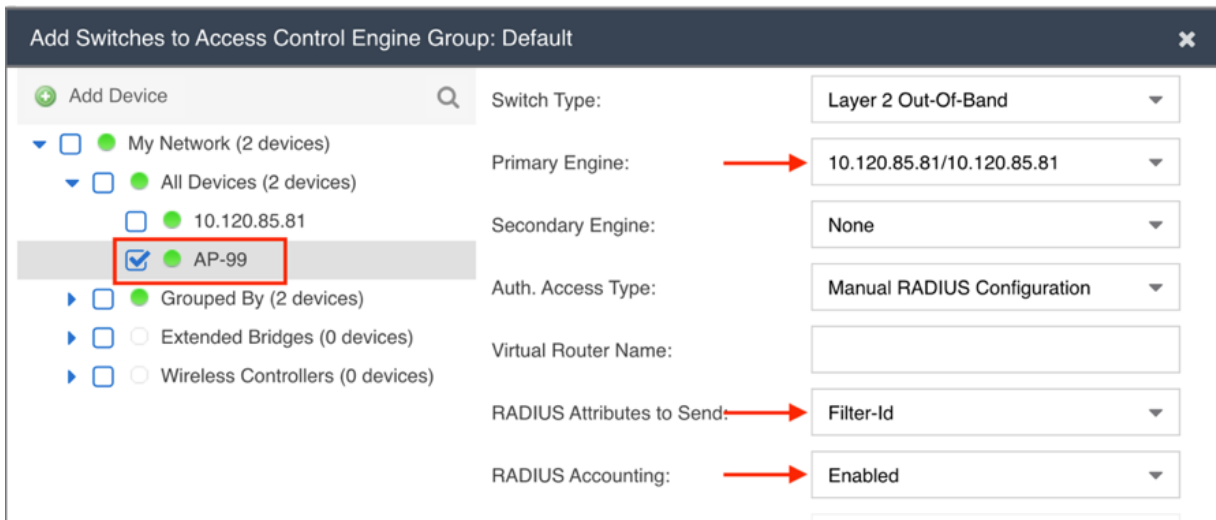
Select the **Access Control** tab of **Control** followed by the **Default** Access Control Engine Group. In the group configuration, select the **Switches** tab and then select the **Add...** button.



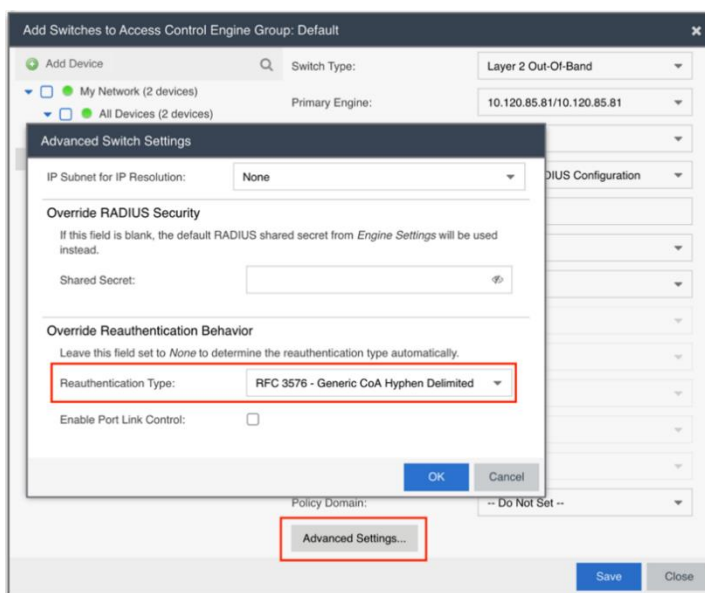
In the Add Switches dialog, if the Access Point has not been added to ExtremeManagement, select the **Add Device** button to add the IP address of the Access Point and the SNMP Profile to use for communication.



Once the Access Point is added to ExtremeManagement, select the Access Point from the device list and 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** field to a value of **Filter-ID** and enable **RADIUS Accounting**.



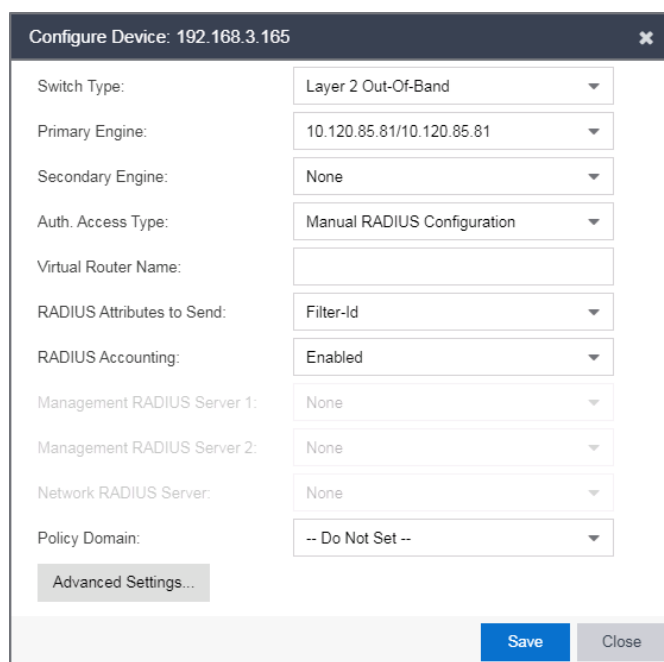
Prior to hitting Save, select the **Advanced Settings** button and set the **Reauthentication Type** to **RFC 3576 - Generic CoA Hyphen Delimited** as shown below. If the RADIUS Shared Secret was set to a value other than the default ETS\_TAG\_SHARED\_SECRET, set the value to match what was configured in XIQ.



**Note**

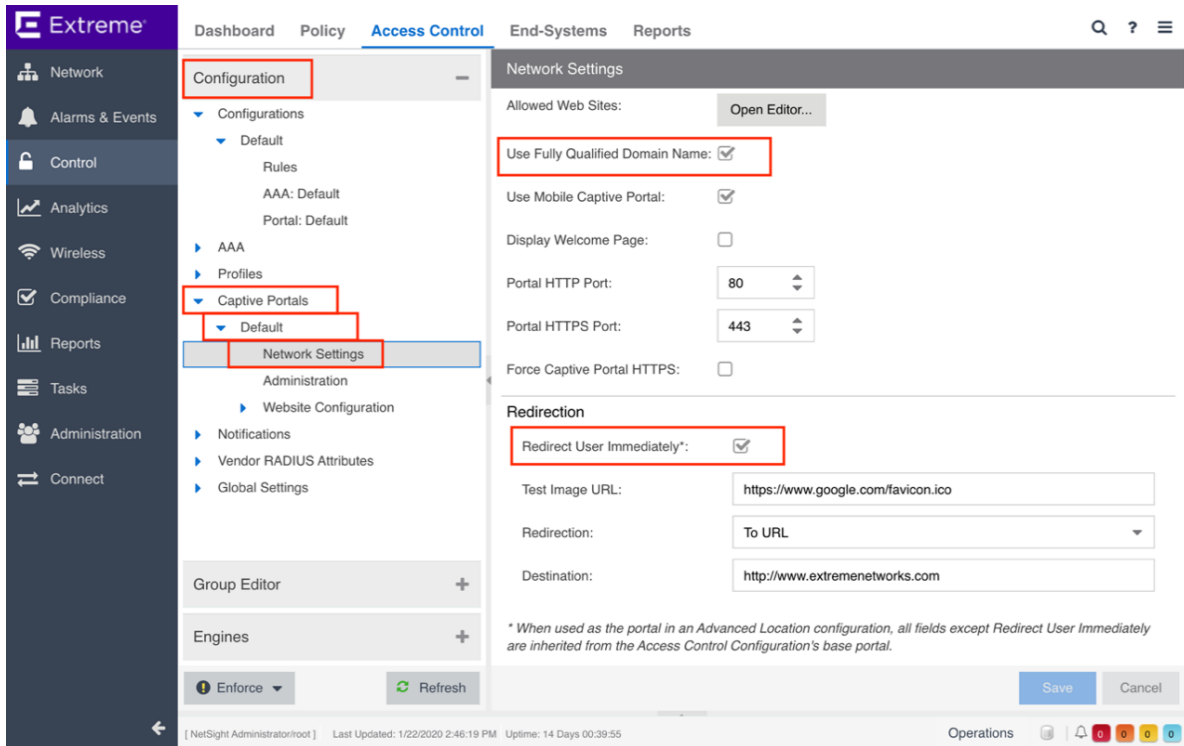
In ExtremeManagement version 8.4 the reauthentication method needs to either be manually set on a per-device basis, or a mapping to the SysObject ID can be created. See Appendix A for reference.

The final settings should look similar to the below image. Once complete, press the **Save** button.

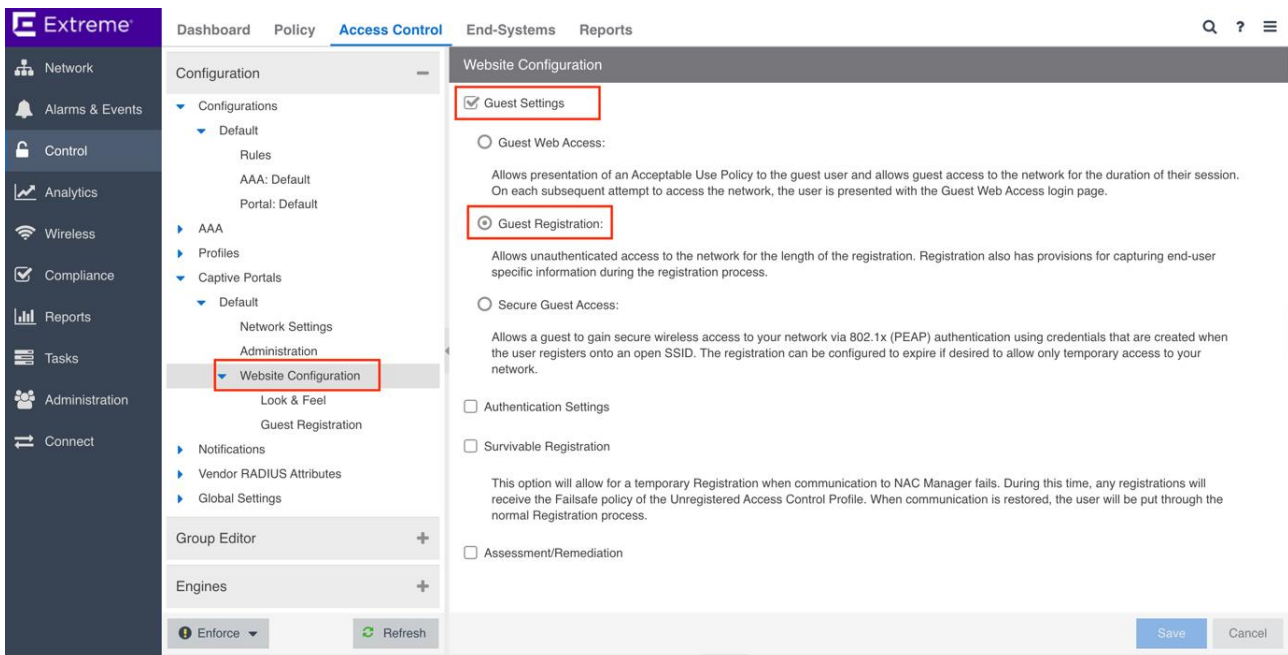


## Step 3 – Configure Captive Portal Settings

Assuming that Guest Registration is already configured, the Network Settings for the Captive Portal need to be verified. Under the **Configuration** section, expand the **Captive Portal** that is in use, typically this is the **Default** captive portal. Select **Network Settings** and verify that **Use Fully Qualified Domain Name** is selected as well as **Redirect User Immediately**.



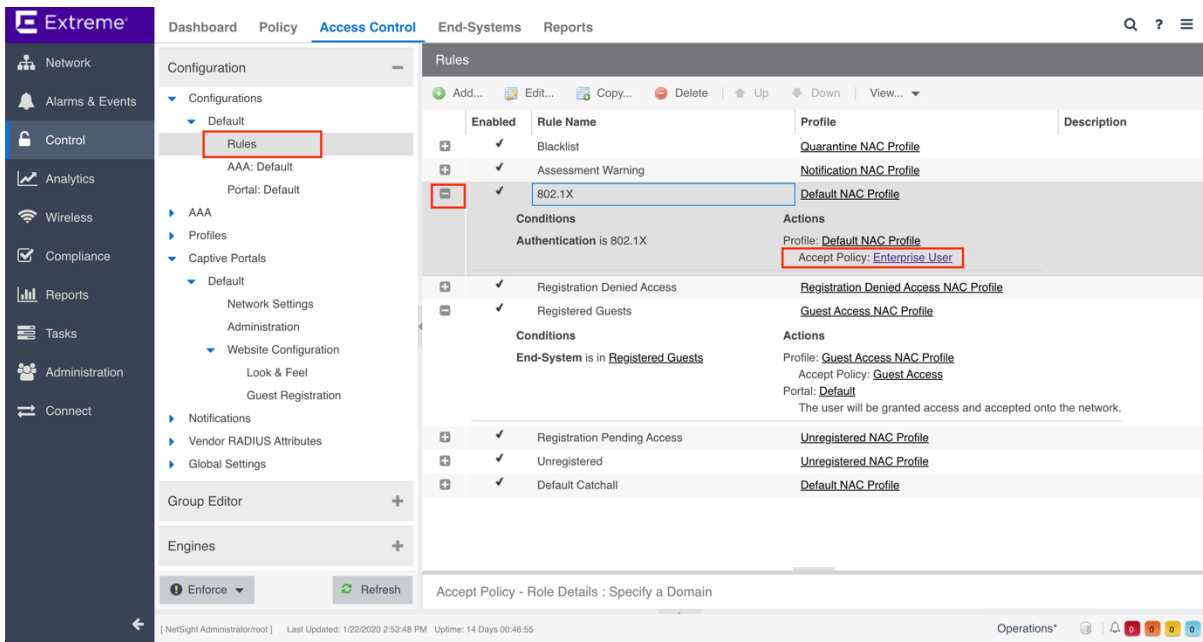
Verify that Guest Registration is also enabled by selecting **Website Configuration**.



## Step 4 – Configure Rules, Roles, and Policy Mappings

With the captive portal settings verified, the authorization rules need to be adjusted to match the Filter-ID settings that the Access Points are expecting. Following the examples that were used in this guide, Enterprise User, Guest Access, and Unregistered should be verified.

Select the **Rules** section under **Configurations**. Enabling Guest Registration auto-generates multiple rules in the rules engine. Additional rules can be added in order to match the authorization criteria desired. In the example below, a rule matching **802.1X** authentication is added and the **Default NAC Profile** assigned, which applies the **Enterprise User** Accept Policy. To verify which Filter-ID is being passed back to the Access Point, select the Accept Policy name to show the Policy Mapping window.



In the Edit Policy Mapping window, the **Filter** should be adjusted to match the Filter-ID that was configured in the Assignment Rules in XIQ.

The screenshot shows the 'Edit Policy Mapping' dialog box. The 'Filter' field is highlighted with a red rectangle and contains the text 'EnterpriseUser'. Other fields include Name: Enterprise User, Map to Location: Any, Policy Role: Enterprise User, VLAN [ID] Name: None, VLAN Egress: Untagged, Port Profile, Virtual Router, Login-LAT-Group: Enterprise User, Login-LAT-Port: 1, and Custom 1.

**Note**

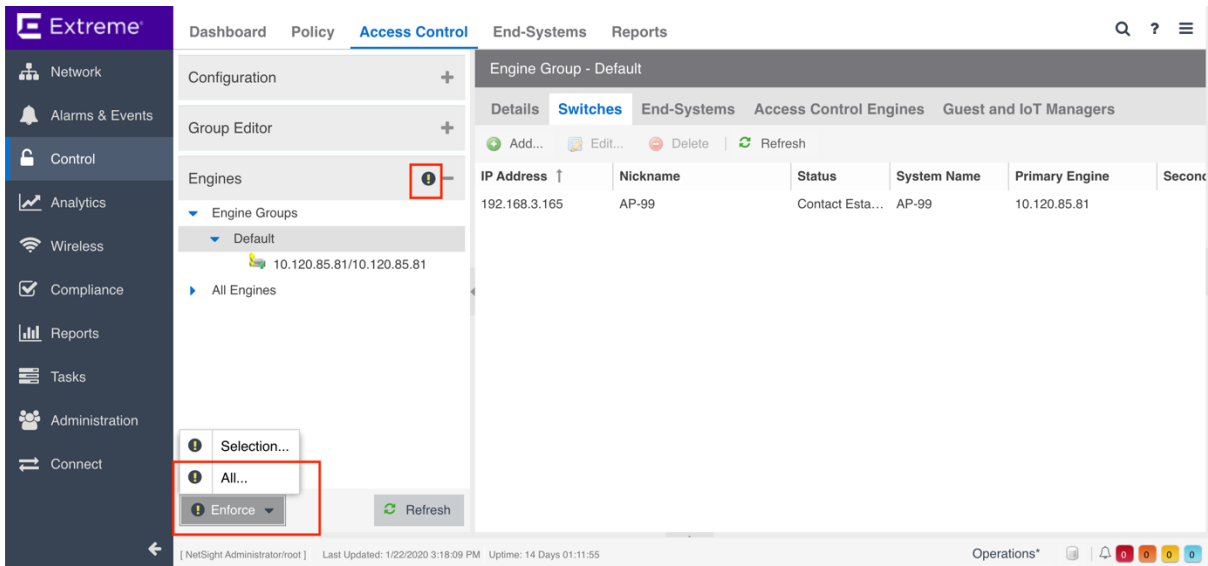
Many of the Accept policies will match correctly without adjustment. However, any multi-word Accept policies such as “Enterprise User” or “Guest Access” need to be adjusted so no spaces are included in the Filter-ID (The radius attribute sent by the Access Control Engine must exactly match the mapping configured on the Access Point). Alternatively, see Appendix E for steps to format the attribute values at runtime rather than individually.

If additional roles are required, they can be added via the Policy Mappings section under Profiles. This screen is also useful to easily verify all policy mappings.

The screenshot shows the Extreme Networks web interface. The 'Access Control' section is active. The 'Profiles' and 'Policy Mappings' sections are highlighted with red boxes. A table of policy mappings is visible on the right.

Name	Filter
Access Point	Access Point
Administrator	Administrator
Assessing	Assessing
Deny Access	Deny Access
Enterprise Access	Enterprise Access
Enterprise User	EnterpriseUser
Enterprise User (Administrator)	Enterprise User
Enterprise User (Read-Only Manage...)	Enterprise User
Failsafe	Failsafe
Guest Access	GuestAccess
Notification	Notification
Printer	Printer
Quarantine	Quarantine
Server	Server
Unregistered	Unregistered
VoIP Phone	VoIP Phone

After enforcing the changes to ExtremeControl, validation of the configuration can be performed.



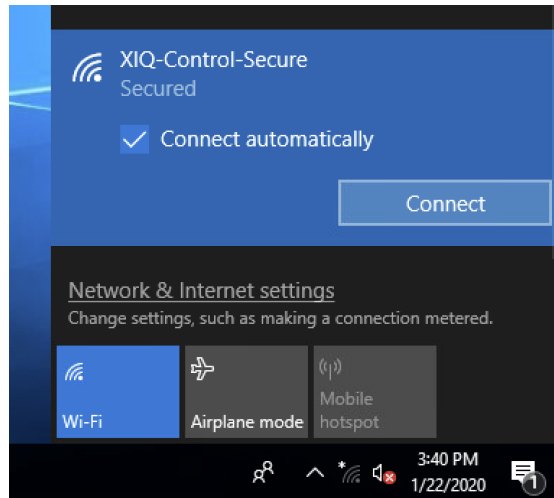


## Part 3: Validation

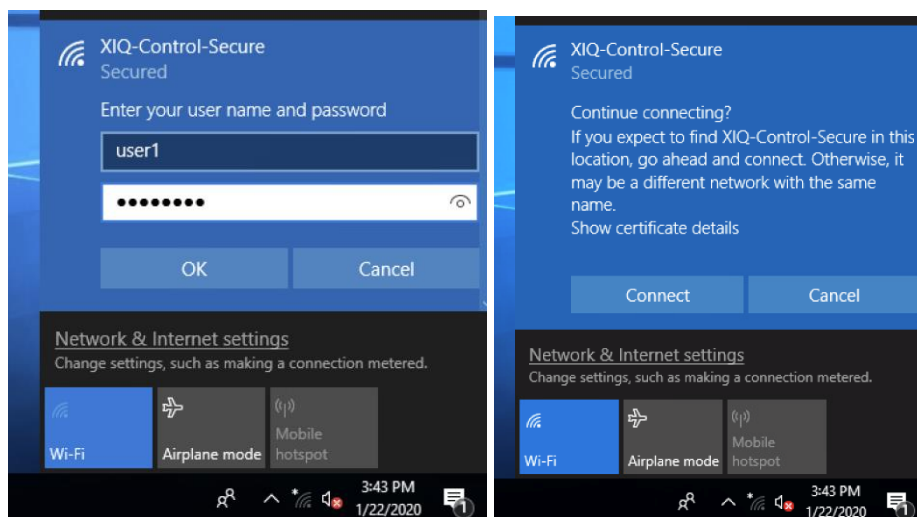
There are two parts of the validation that should be performed. The first is for the secure SSID, ensuring that 802.1X is working as expected. The second point of validation is for the Guest Network. This validation includes Captive Portal Redirection, Change of Authorization based on registration, and User Profile assignment based on the state of the end system.

### Secure SSID Validation

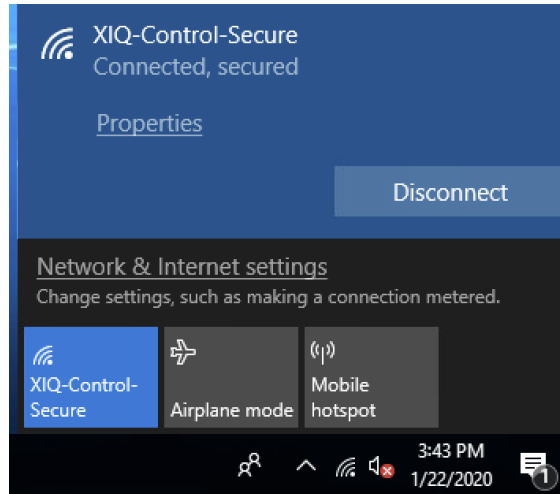
Assuming that ExtremeControl is properly configured to authenticate 802.1X requests, the secure SSID can be tested. Select the SSID from the available SSID list.



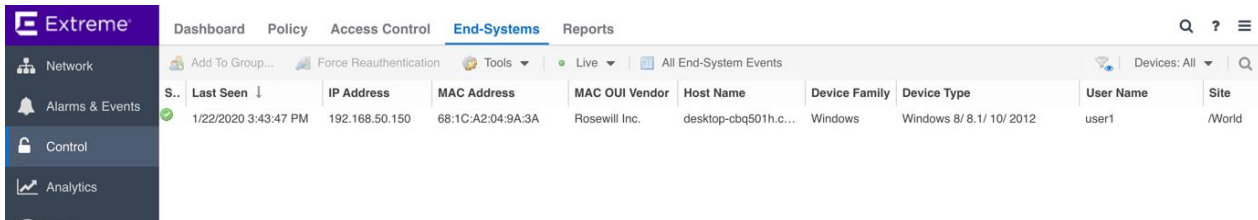
When prompted for a username and password, enter valid credentials. If prompted, also trust or ignore any certificate warnings.



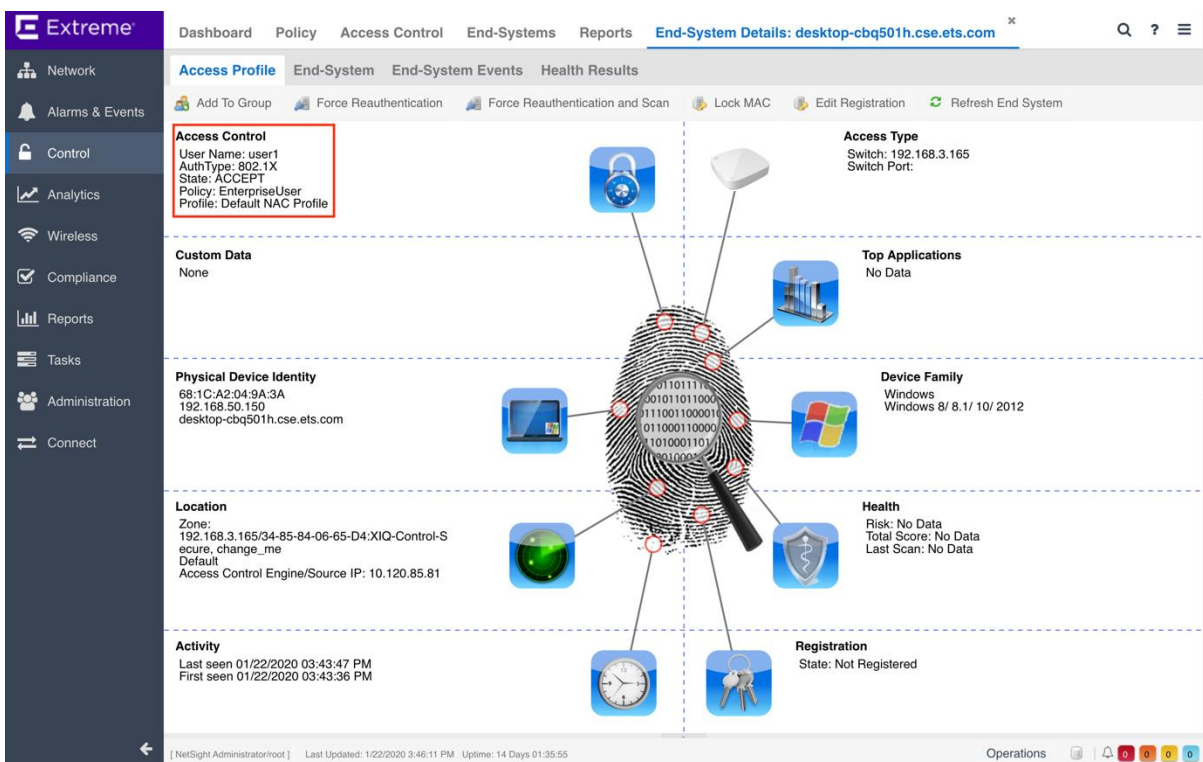
Once connected, validate that traffic can be passed as expected.



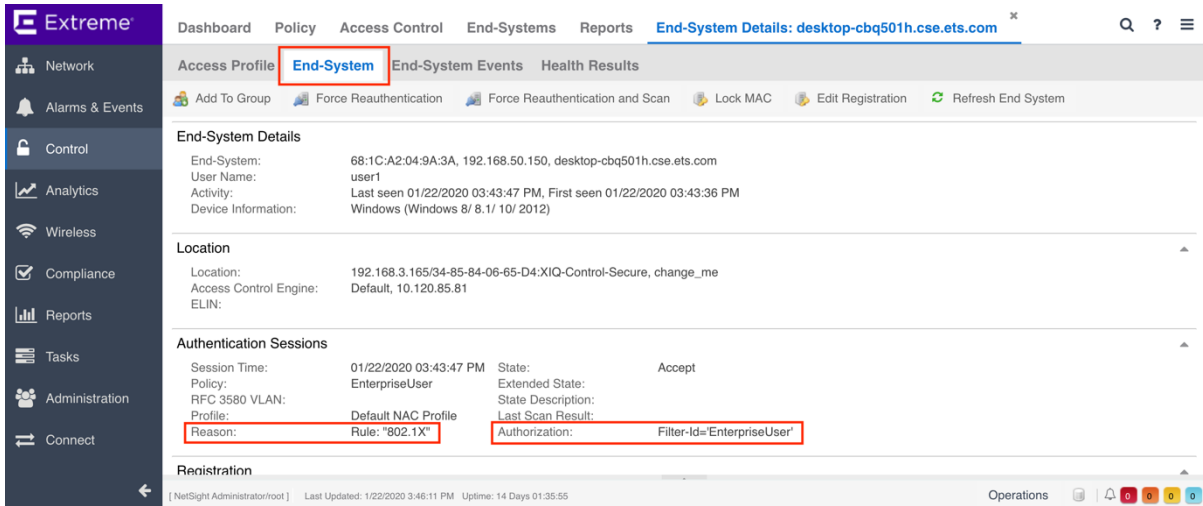
In ExtremeControl, navigate to the End-Systems tab and validate that all of the information is properly populated for the newly connected client.



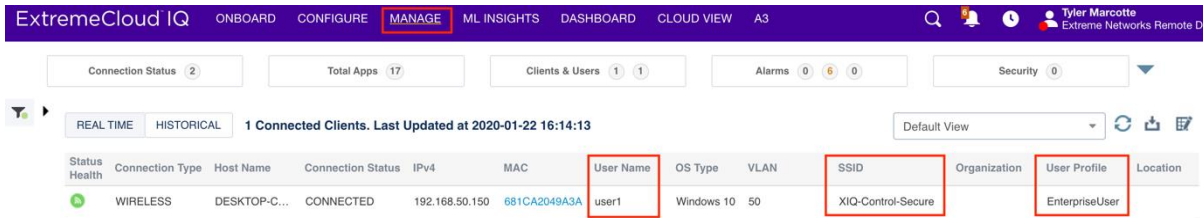
Open the End-System Details screen by double-clicking the client. This screen shows information regarding the connected client. In particular, the policy and profile assigned to the client as well as the username that authenticated to the network.



Selecting the End-System tab shows additional information including the Reason (rule) that the end system hit as well as the raw Filter-ID that was returned in the RADIUS Accept message.



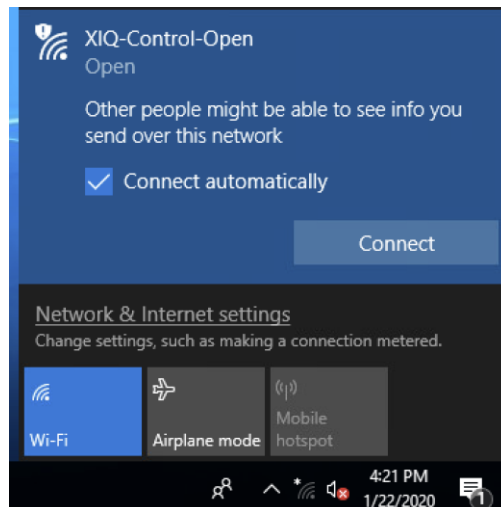
In XIQ, select **Clients** under the **Manage** tab and note the username of the client, the SSID, and the assigned User Profile.



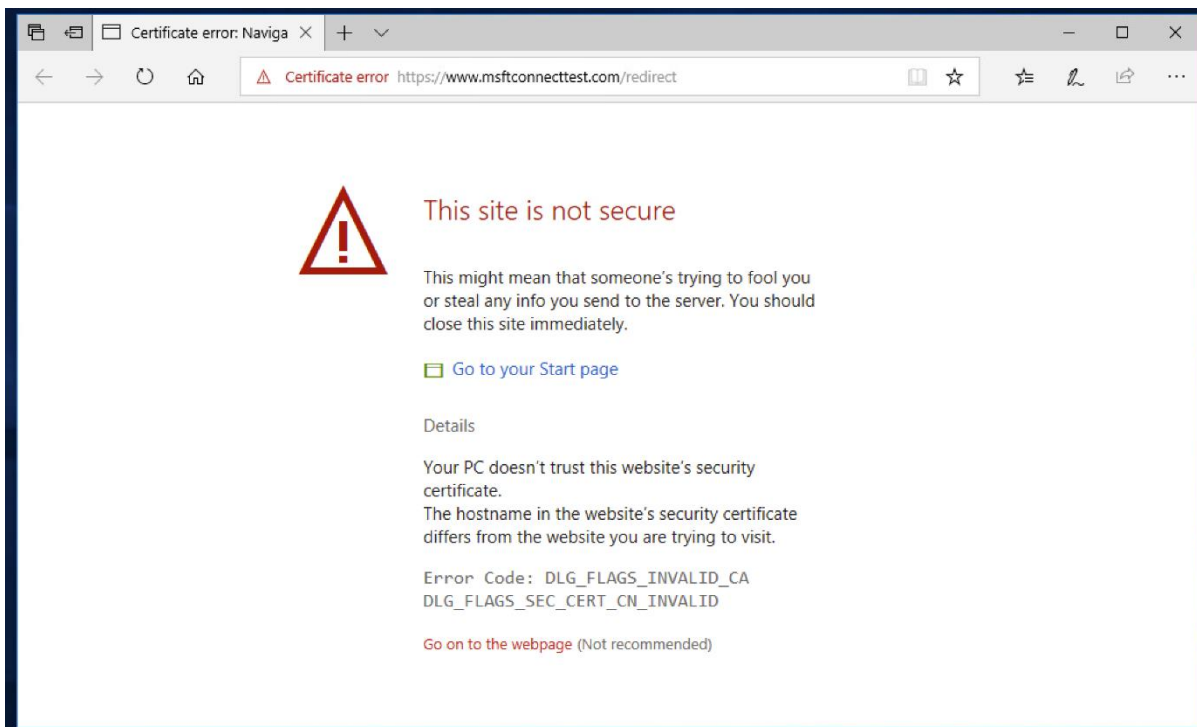
## Guest SSID Validation

Prior to starting the Guest SSID validation, ensure that any previously known SSID is forgotten.

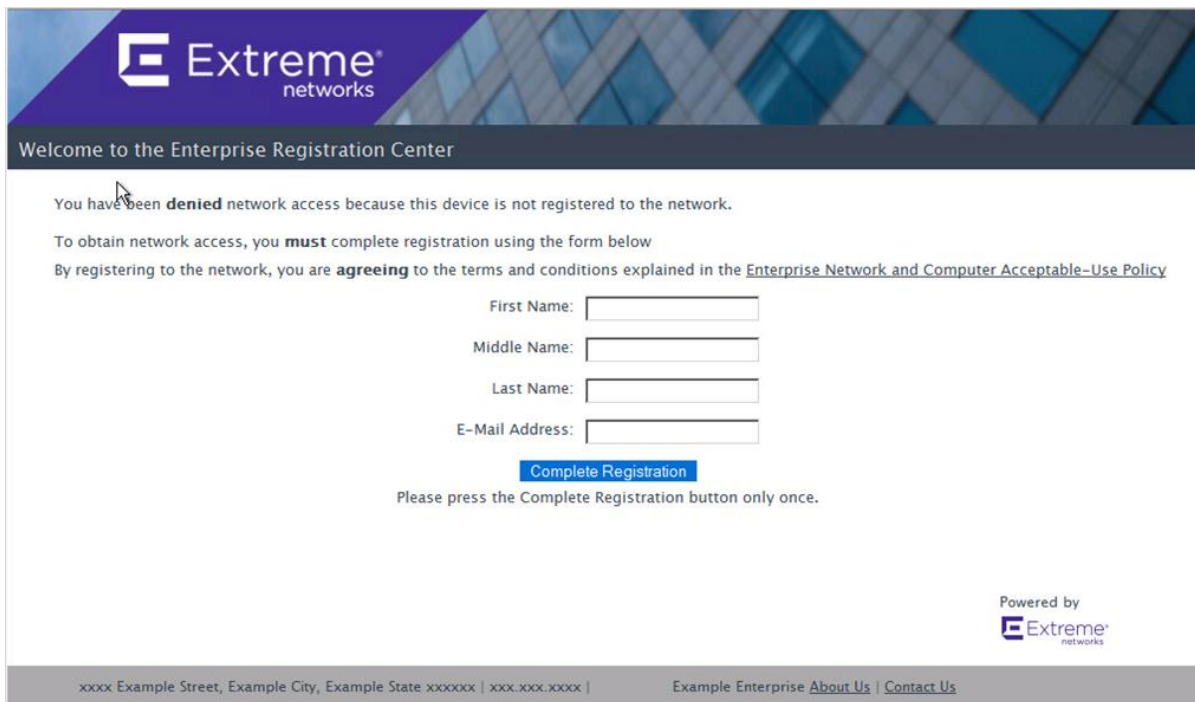
Select the open SSID from the the available SSID list.



Once connected, an automatic redirection may occur based on the operating system. Ignore any certificate warnings and continue.



The web traffic for the client is redirected to the captive portal hosted by the Access Control Engine.



At this phase, ExtremeControl assigns the **Unregistered NAC Profile** and returns the Filter-ID of **Unregistered**. This can be verified in the End-Systems tab in ExtremeControl.

S..	Last Seen ↓	IP Address	MAC Address	MAC OUI Vendor	Host Name	Device Family	Device Type	User Name	Switch IP	Switch Nickname	Authorization
1/23/2020	9:38:18 AM	192.168.50.150	68:1C:A2:04:9A:3A	Rosewill Inc.	desktop-cbq501h.c...	Windows	Windows 8/ 8.1/ 10/ 2012		192.168.3.165	AP-99	Filter-ID='Unregistered'

In XIQ, the User Profile assigned to the client is also shown as **Unregistered**.

User Name	OS Type	VLAN	SSID	Organization	User Profile	Location	Last Session Start Time
A2049A3A	Windows 10	50	XIQ-Control-Open		Unregistered		2020-01-22 16:21:56

In the web page on the client, fill out the fields and select **Complete Registration** to submit the registration to ExtremeControl.

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

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

A CoA is sent with a new Filter-ID based on the rules engine configuration. Depending on the configuration of the Captive Portal, the client’s web traffic is redirected to a success page once the User Profile is changed. Looking at the **End-Systems** table in ExtremeControl, the Authorization column shows that the GuestAccess Filter-ID is assigned to the client.

S..	Last Seen ↓	IP Address	MAC Address	MAC OUI Vendor	Host Name	Device Family	Device Type	User Name	Switch IP	Switch Nickname	Authorization
1/23/2020	9:43:19 AM	192.168.50.150	68:1C:A2:04:9A:3A	Rosewill Inc.	desktop-cbq501h.c...	Windows	Windows 8/ 8.1/ 10/ 2012	Doe, John	192.168.3.165	AP-99	Filter-ID='GuestAccess'

The end system details for the client are populated with the additional information that was entered in the captive portal.

**Access Control**  
 User Name: Doe, John  
 AuthType: MAC  
 State: ACCEPT  
 Policy: GuestAccess  
 Profile: Guest Access NAC Profile

**Access Type**  
 Switch: 192.168.3.165  
 Switch Port:

**Custom Data**  
 None

**Physical Device Identity**  
 68:1C:A2:04:9A:3A  
 192.168.50.150  
 desktop-cbq501h.cse.ets.com

**Location**  
 Zone:  
 192.168.3.165/34-85-84-06-65-D5:XIQ-Control-O  
 pen, change\_me  
 Default  
 Access Control Engine/Source IP: 10.120.85.81

**Activity**  
 Last seen 01/23/2020 09:43:19 AM  
 First seen 01/22/2020 03:43:36 PM

**Access Type**  
 Switch: 192.168.3.165  
 Switch Port:

**Top Applications**  
 No Data

**Device Family**  
 Windows  
 Windows 8/ 8.1/ 10/ 2012

**Health**  
 Risk: No Data  
 Total Score: No Data  
 Last Scan: No Data

**Registration**  
 State: Approved  
 Name: Doe, John

When looking at the End-System Details, additional information can be verified in regards to the Registration and Authentication information.

**End-System Details**

End-System:	68:1C:A2:04:9A:3A, 192.168.50.150, desktop-cbq501h.cse.ets.com		
User Name:	Doe, John		
Activity:	Last seen 01/23/2020 09:43:19 AM, First seen 01/22/2020 03:43:36 PM		
Device Information:	Windows (Windows 8/ 8.1/ 10/ 2012)		

**Location**

Location:	192.168.3.165/34-85-84-06-65-D5:XIQ-Control-Open, change_me		
Access Control Engine:	Default, 10.120.85.81		
ELIN:			

**Authentication Sessions**

Session Time:	01/23/2020 09:43:19 AM	State:	Accept
Policy:	GuestAccess	Extended State:	
RFC 3580 VLAN:		State Description:	Authenticated Rule 0 [Any, "", Any] , Auth Method: LOCAL_AUTH
Profile:	Guest Access NAC Profile	Last Scan Result:	
Reason:	Rule: "Registered Guests"	Authorization:	Filter-Id='GuestAccess'

**Registration**

State:	Approved	Group:	Registered Guests
User Name:	Doe, John	Sponsor Group:	
User Email:	jdoe@extremenetworks.com	Sponsor:	
User Phone:		Registration Time:	01/23/2020
Registration Type:	Guest Registration	Start Time:	
Max Devices:	2	Expires Time:	02/22/2020
Description:			

In the **End-System Events** for the device, the historical audit trail is available.

S.	Time Stamp	Access Control ...	Profile	IP Address	MAC Address	User Name	Host Name	Device Family	Device Type	Switch Port
✓	1/23/2020 9:43:19 AM	10.120.85.81	Guest Acces...	192.168.50.150	68:1C:A2:04:9A:3A	Doe, John	desktop-cbq501...	Windows	Windows B/ ...	34-85-84-06-65-D5:XIQ-Control-Open
✓	1/23/2020 9:38:18 AM	10.120.85.81	Unregistered...	192.168.50.150	68:1C:A2:04:9A:3A		desktop-cbq501...	Windows	Windows B/ ...	34-85-84-06-65-D5:XIQ-Control-Open
✓	1/23/2020 9:35:05 AM	10.120.85.81	Unregistered...	192.168.50.150	68:1C:A2:04:9A:3A		desktop-cbq501...	Windows	Windows B/ ...	34-85-84-06-65-D5:XIQ-Control-Open
✓	1/22/2020 4:22:06 PM	10.120.85.81	Unregistered...	192.168.50.150	68:1C:A2:04:9A:3A		desktop-cbq501...	Windows	Windows B/ ...	34-85-84-06-65-D5:XIQ-Control-Open
✓	1/22/2020 4:21:55 PM	10.120.85.81	Unregistered...	192.168.50.150	68:1C:A2:04:9A:3A		desktop-cbq501...	Windows	Windows B/ ...	34-85-84-06-65-D5:XIQ-Control-Open
✓	1/22/2020 4:21:55 PM	10.120.85.81	Unregistered...	192.168.50.150	68:1C:A2:04:9A:3A		desktop-cbq501...	Windows	Windows B/ ...	34-85-84-06-65-D5:XIQ-Control-Open
✓	1/22/2020 4:21:42 PM	10.120.85.81	Default NAC...	192.168.50.150	68:1C:A2:04:9A:3A	user1	desktop-cbq501...	Windows	Windows B/ ...	34-85-84-06-65-D4:XIQ-Control-Secure
✓	1/22/2020 4:12:48 PM	10.120.85.81	Default NAC...	192.168.50.150	68:1C:A2:04:9A:3A	user1	desktop-cbq501...	Windows	Windows B/ ...	34-85-84-06-65-D4:XIQ-Control-Secure
✓	1/22/2020 4:12:38 PM	10.120.85.81	Default NAC...	192.168.50.150	68:1C:A2:04:9A:3A	user1	desktop-cbq501...	Windows	Windows B/ ...	34-85-84-06-65-D4:XIQ-Control-Secure
✓	1/22/2020 4:12:38 PM	10.120.85.81	Default NAC...	192.168.50.150	68:1C:A2:04:9A:3A	user1	desktop-cbq501...	Windows	Windows B/ ...	34-85-84-06-65-D4:XIQ-Control-Secure
✓	1/22/2020 4:11:25 PM	10.120.85.81	Default NAC...	192.168.50.150	68:1C:A2:04:9A:3A	user1	desktop-cbq501...	Windows	Windows B/ ...	34-85-84-06-65-D4:XIQ-Control-Secure
✓	1/22/2020 3:43:47 PM	10.120.85.81	Default NAC...	192.168.50.150	68:1C:A2:04:9A:3A	user1	desktop-cbq501...	Windows	Windows B/ ...	34-85-84-06-65-D4:XIQ-Control-Secure
✓	1/22/2020 3:43:46 PM	10.120.85.81	Default NAC...	192.168.50.150	68:1C:A2:04:9A:3A	user1	DESKTOP-CBQ...	Windows	Windows B/ ...	34-85-84-06-65-D4:XIQ-Control-Secure
✓	1/22/2020 3:43:36 PM	10.120.85.81	Default NAC...	192.168.50.150	68:1C:A2:04:9A:3A	user1				34-85-84-06-65-D4:XIQ-Control-Secure
✓	1/22/2020 3:43:36 PM	10.120.85.81	Default NAC...	192.168.50.150	68:1C:A2:04:9A:3A	user1				34-85-84-06-65-D4:XIQ-Control-Secure

Even though the User Profile is correctly assigned, XIQ does not show the updated information until the client fully re-authenticates either by disconnecting from the network or by an administrator selecting Force Reauthentication. Furthermore, XIQ periodically updates the information. Lastly, the profile can be verified via CLI using the commands **show station** and **show user-profile**.

```

AP-99#show station
Chan=channel number; Pow=Power in dBm;
A-Mode=Authentication mode; Cipher=Encryption mode;
A-Time=Associated time; Auth=Authenticated;
UPID=User profile Identifier; Phymode=Physical mode;

Ifname=wifi0.1, Ifindex=19, SSID=XIQ-Control-Secure:
Mac Addr      IP Addr      Chan Tx Rate Rx Rate Pow(SNR)      A-Mode  Cipher  A-Time  VLAN Auth UPID Phymode LDPC Tx-STBC Rx-STBC  SM-PS Chan-width  MU-MIMO Release Station-State
-----
Ifname=wifi1.1, Ifindex=21, SSID=XIQ-Control-Secure:
Mac Addr      IP Addr      Chan Tx Rate Rx Rate Pow(SNR)      A-Mode  Cipher  A-Time  VLAN Auth UPID Phymode LDPC Tx-STBC Rx-STBC  SM-PS Chan-width  MU-MIMO Release Station-State
-----
Ifname=wifi0.2, Ifindex=22, SSID=XIQ-Control-Open:
Mac Addr      IP Addr      Chan Tx Rate Rx Rate Pow(SNR)      A-Mode  Cipher  A-Time  VLAN Auth UPID Phymode LDPC Tx-STBC Rx-STBC  SM-PS Chan-width  MU-MIMO Release Station-State
681c:a204:9a3a 192.168.50.150  11    65M   72.2M  -28(66)      open    none   00:02:53  50  Yes  1    11ng  No   No   No   static  20MHz  No   No   Good
-----
Ifname=wifi1.2, Ifindex=23, SSID=XIQ-Control-Open:
Mac Addr      IP Addr      Chan Tx Rate Rx Rate Pow(SNR)      A-Mode  Cipher  A-Time  VLAN Auth UPID Phymode LDPC Tx-STBC Rx-STBC  SM-PS Chan-width  MU-MIMO Release Station-State
-----

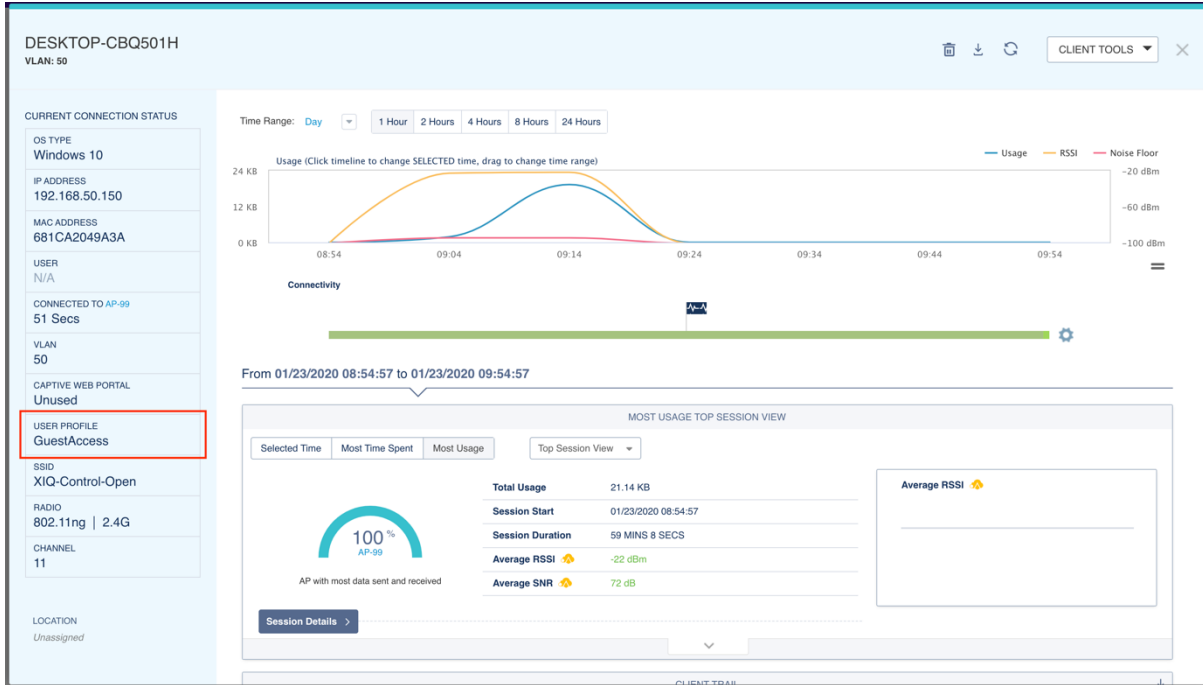
AP-99#show user-profile
User Profile Table
VLAN(*) means User Profile use a VLAN GROUP.
Total Entries = 4

No. User Profile Name      VLAN  Attribute
-----
1  default-profile          1     0
2  GuestAccess              50    1
3  EnterpriseUser           50    2
4  Unregistered             50    3
    
```

Navigating to XIQ, once the client is re-authenticated, the User Profile can be verified in the Clients view.

Status Health	Connection Type	Host Name	Connection Status	IPv4	MAC	User Name	OS Type	VLAN	SSID	Organization	User Profile	Location	Last Session Start Time	Device
✓	WIRELESS	DESKTOP-C...	CONNECTED	192.168.50.150	681CA2049A3A		Windows 10	50	XIQ-Control-Open		GuestAccess		2020-01-23 09:54:06	AP-99

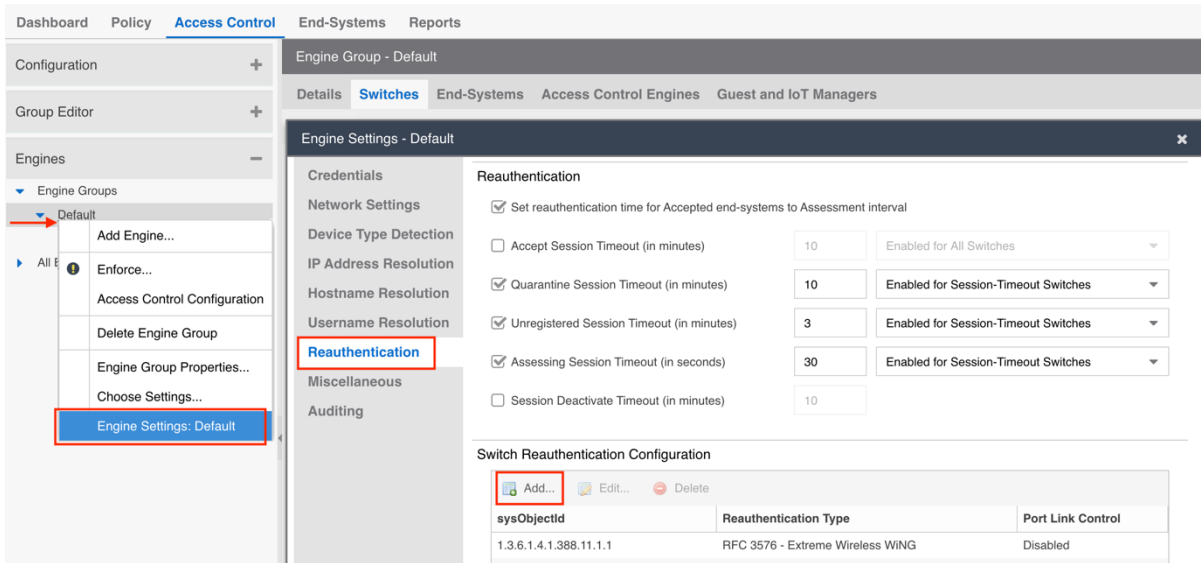
The information is also available when client details are displayed.





## Appendix A: Creating RFC 3576 Configurations

Instead of configuring the Reauthentication Type for each Access Point as its added to ExtremeControl, the Reauthentication type can be set based on the SNMP SysObject ID for the AP. This is a more scalable approach when adding multiple Access Points. To add the entry, right click on the **Default** Engine Group and select **Engine Settings**. Choose the **Reauthentication** menu item and **Add** a new Reauthentication Configuration.



Set the sysObjectID as **1.3.6.1.4.1.26928.1** as it is the same for all ExtremeCloud IQ APs. Set the Reauthentication Type to **RFC 3576** and the Configuration to **Generic CoA Hyphen Delimited**.

Add Switch Reauthentication Configuration
✕

sysObjectId:

Reauthentication Type:

RFC 3576 Configuration:

Manage RFC 3576 Configurations...

Enable Port Link Control

If the Reauthentication Type **Generic CoA Hyphen Delimited** is missing, it can be created based on the settings below.

**Edit RFC 3576 Reauthentication Configuration**

Configuration Name:

MAC Format:

Destination Port:

Supports Change of Authorization

Custom Attributes:

Additional RADIUS Attributes:

- NAS-IP-Address
- User-Name
- Enterasys-Auth-Client-Type
- Message-Authenticator
- Acct-Session-Id

Once complete, the configuration should look similar to below.

**Engine Settings - Default**

**Reauthentication**

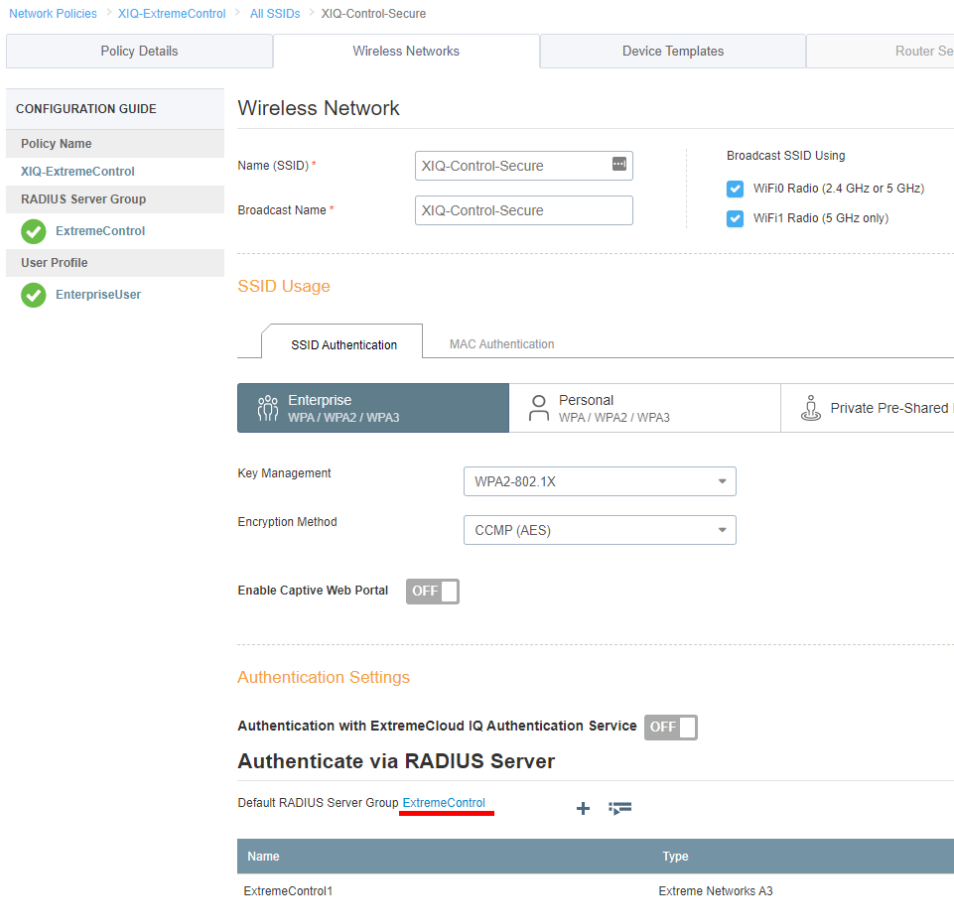
- Set reauthentication time for Accepted end-systems to Assessment interval
- Accept Session Timeout (in minutes)
- Quarantine Session Timeout (in minutes)
- Unregistered Session Timeout (in minutes)
- Assessing Session Timeout (in seconds)
- Session Deactivate Timeout (in minutes)

**Switch Reauthentication Configuration**

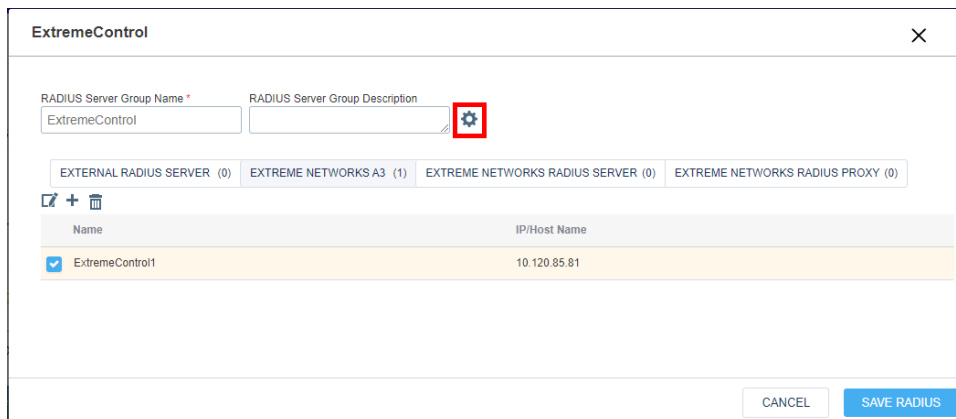
sysObjectId	Reauthentication Type	Port Link Control
1.3.6.1.4.1.388.11.1.1	RFC 3576 - Extreme Wireless WING	Disabled
1.3.6.1.4.1.9.1.618	RFC 3576 - Cisco Wireless	Disabled
1.3.6.1.4.1.1916.2.131.18	RFC 3576 - Legacy Summit/Altitude Wireless	Disabled
1.3.6.1.4.1.1916.2.131.15	RFC 3576 - Legacy Summit/Altitude Wireless	Disabled
1.3.6.1.4.1.1916.2.131.16	RFC 3576 - Legacy Summit/Altitude Wireless	Disabled
1.3.6.1.4.1.9.1.818	RFC 3576 - Cisco Wireless Controller	Disabled
1.3.6.1.4.1.388.50.1.1	RFC 3576 - Extreme Wireless WING	Disabled
1.3.6.1.4.1.26928.1	RFC 3576 - Generic CoA Hyphen Delimited	Disabled

## Appendix B: Enable RFC 3576 Reauthentication on XIQ

By default, if the RADIUS Server was added as an Extreme Networks A3 server, RFC 3576 is already enabled. However, if it's added as an External RADIUS Server, then it will need to be manually enabled. To do this, edit the **Network Policy** in the **Configure** menu, choose the SSID in the **Wireless Networks** and find the **Authentication Settings** section. Edit the Radius Server Group. For Enterprise WPA / WPA2 / WPA3 the screen will look similar to below:



Select the gear icon as shown below for advanced settings.



## Select the checkbox **Permit Dynamic Change Of Authorization Messages (RFC 3576)**.

ExtremeControl ×

SelectRadiusSettings

Note: These settings only apply for HiveOS devices. These settings are ignored for non-HiveOS devices.

Retry Interval   
Range: 60 - 100000000 (seconds)

Accounting Interim Update Interval   
Range: 10 - 100000000 (seconds)

**Permit Dynamic Change Of Authorization Messages (RFC 3576)**

Inject Operator-Name attribute

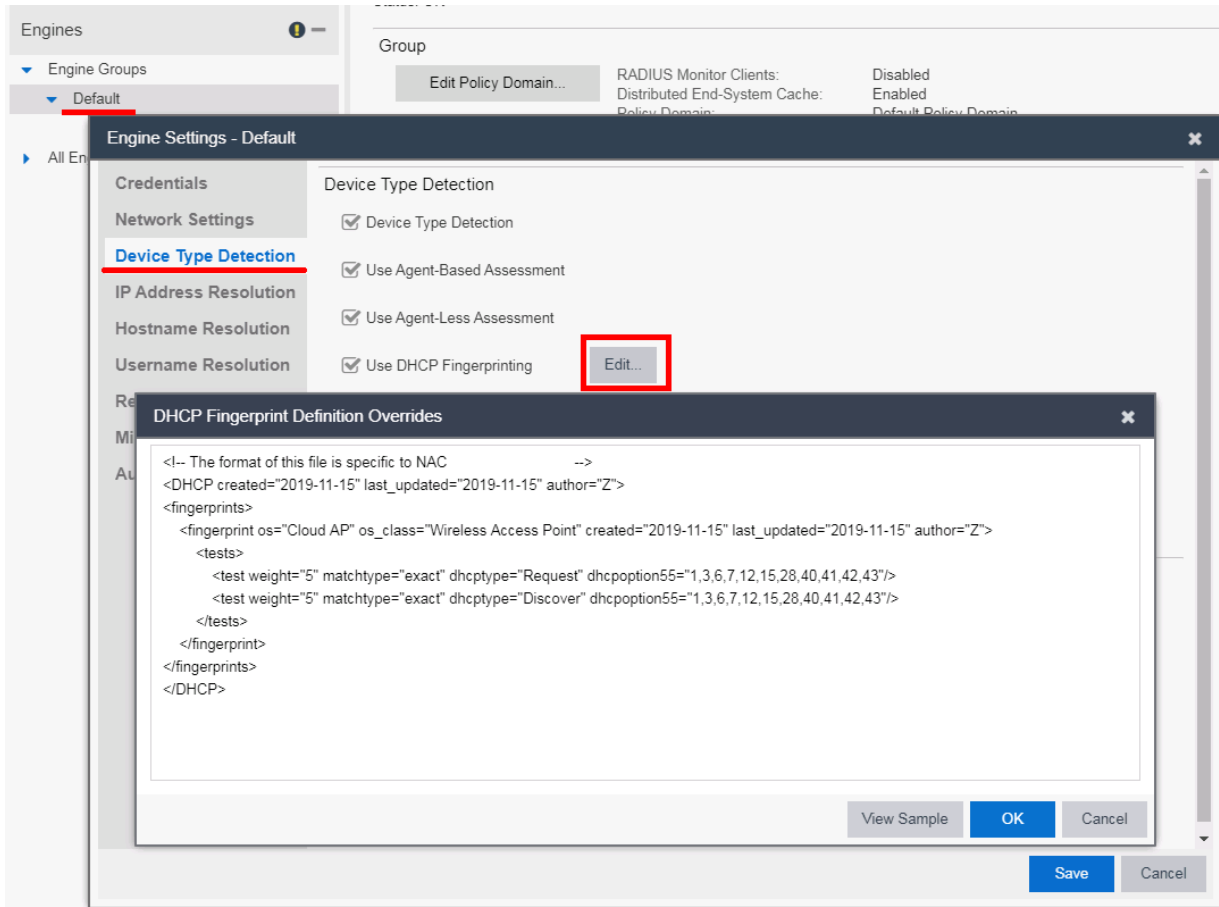
Message Authenticator attribute

Not Supported for Extreme Networks RADIUS Proxy

CANCEL SAVE RADIUS SETTINGS

## Appendix C: DHCP Fingerprint for XIQ Access Points

In order for the ExtremeCloud IQ Access Point to be recognized as an appropriate device type in the End-System table, a DHCP fingerprint needs to be added. Right-click the **Default** Engine Group and select **Engine Settings**. In the settings, select the **Device Type Detection** menu and the **Edit** button next to **Use DHCP Fingerprinting**.



If a fingerprint is being added to existing custom fingerprints, use the following values:

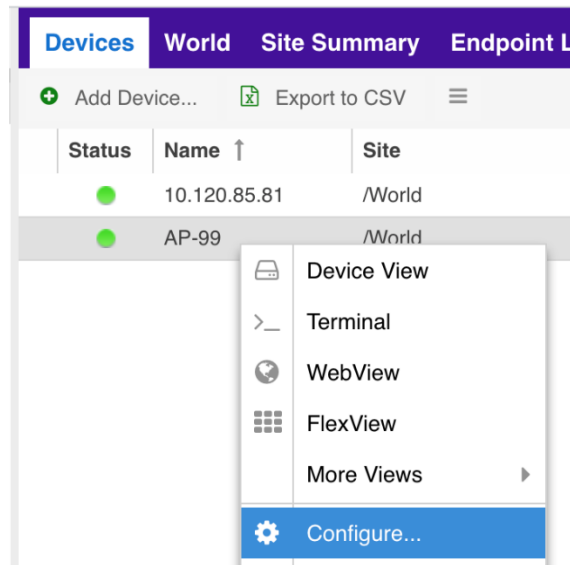
```
<fingerprint os="Cloud AP" os_class="Wireless Access Point"
created="2019-11-15" last_updated="2019-11-15" author="Z">
  <tests>
    <test weight="5" matchtype="exact" dhcptype="Request"
dhcption55="1,3,6,7,12,15,28,40,41,42,43"/>
    <test weight="5" matchtype="exact" dhcptype="Discover"
dhcption55="1,3,6,7,12,15,28,40,41,42,43"/>
  </tests>
</fingerprint>
```

If there are no existing custom fingerprints, use this value:

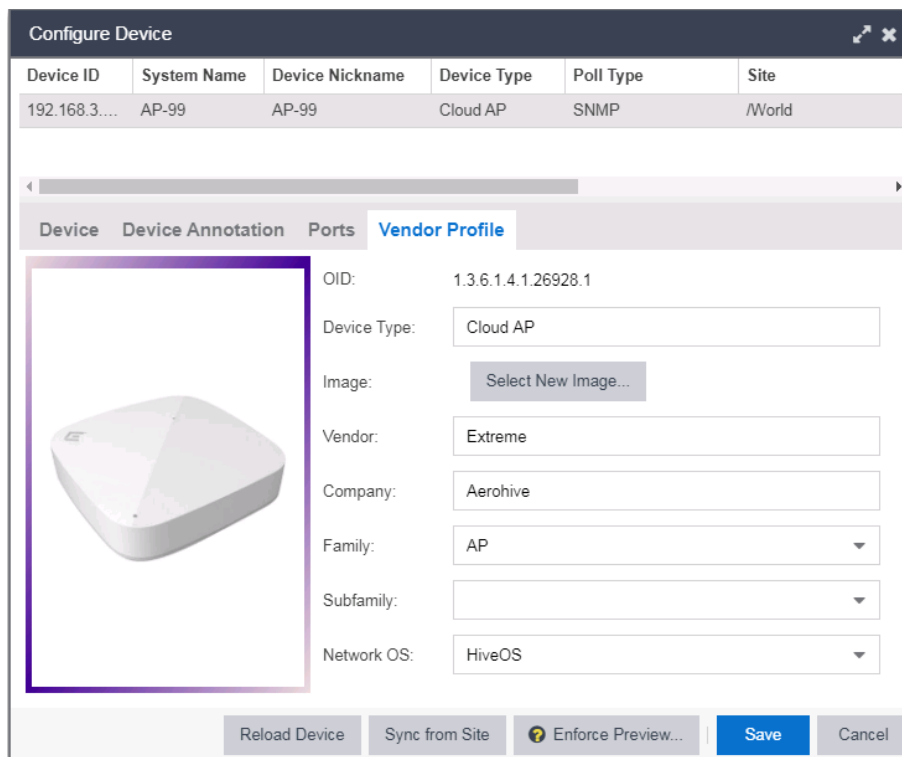
```
<!-- The format of this file is specific to NAC
-->
<DHCP created="2019-11-15" last_updated="2019-11-15" author="Z">
<fingerprints>
  <fingerprint os="Cloud AP" os_class="Wireless Access Point"
created="2019-11-15" last_updated="2019-11-15" author="Z">
    <tests>
      <test weight="5" matchtype="exact" dhcptype="Request"
dhcption55="1,3,6,7,12,15,28,40,41,42,43"/>
      <test weight="5" matchtype="exact" dhcptype="Discover"
dhcption55="1,3,6,7,12,15,28,40,41,42,43"/>
    </tests>
  </fingerprint>
</fingerprints>
</DHCP>
```

## Appendix D: Vendor Profile for XIQ Access Points

In XMC version 8.4, an ExtremeCloud IQ Access Point shows up as an unknown third party device. To configure some default settings for the AP, a Vendor Profile can be adjusted to show more friendly information for the APs. To configure this, right-click the AP in the Devices tab and select **Configure**.



In the Configure Device screen, a tab called **Vendor Profile** can be selected. In this screen, the values can be configured as desired.



With the configured Vendor Profile many visuals are more user friendly. The AP picture is displayed in the End-System Details (thumb print screen) and on topology maps.

## Appendix E: RADIUS Reponse Formatting

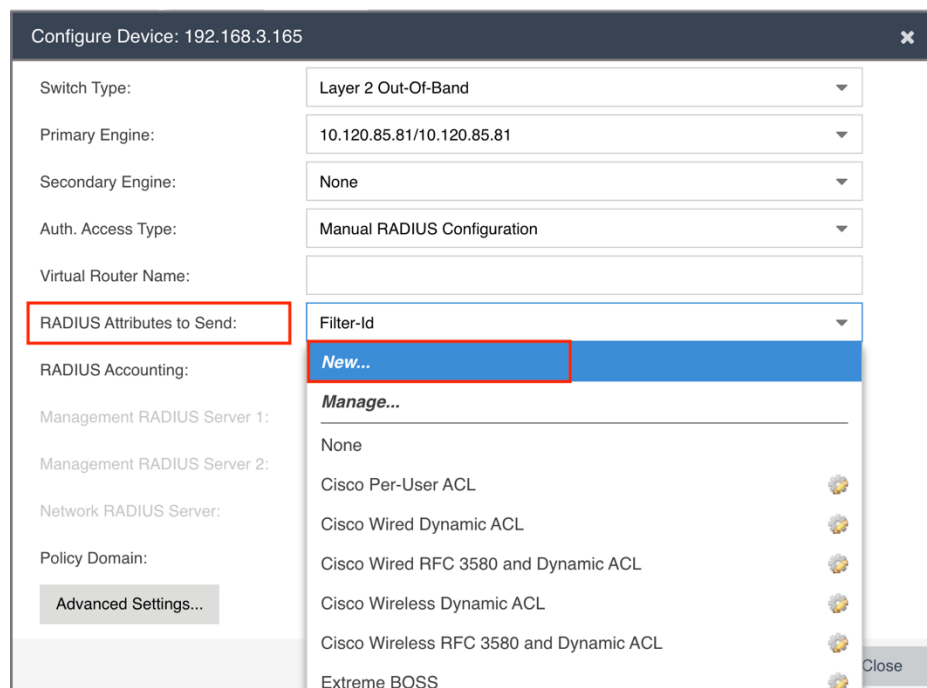
As of version 8.3, ExtremeControl has the ability to format RADIUS Attributes at runtime. This means that rather than modifying the Policy Mappings for each Accept policy to remove spaces, the RADIUS Attribute configuration can be modified to modify the response at run time.

The available modifications are:

- UPPER – Changes the response variable to be all uppercase. For example: **Guest Access** becomes **GUEST ACCESS**.
- LOWER – Changes the response variable to be all lowercase. For example: **Guest Access** becomes **guest access**.
- STRIP – Removes all whitespace from the variable including spaces. For example: **Guest Access** becomes **GuestAccess**.
- UPPER-STRIP – Removes all whitespace and changes the response to be uppercase. For example: **Guest Access** becomes **GUESTACCESS**.
- LOWER-STRIP – Removes all whitespace and changes the response to be lowercase. For example: **Guest Access** becomes **guestaccess**.

The modifications are applied to the variable portion of the RADIUS Attribute Configuration. Using a simple Filter-ID configuration as an example, The value of **Filter-Id=%FILTER\_NAME%** would be changed to **Filter-Id=%FILTER\_NAME:STRIP%** to remove the whitespace from the variable.

The configuration is adjusted when assigning the RADIUS Configuration in the Add Switch dialog. In the **RADIUS Attributes to Send** drop-down menu, select **New**.





In the new window, keep the same variable, however add **:STRIP** to the end in order to remove whitespace.

Dialog box titled "Edit RADIUS Attribute Configuration".

Name: Filter-Id (Strip)

Enable Port Link Control:

Attributes : [dropdown] Substitutions : [dropdown]

Filter-Id=%FILTER\_NAME:STRIP%

Save Close

Ensure the new configuration is selected when saving the Switch configuration.

Dialog box titled "Configure Device: 192.168.3.165".

Switch Type: Layer 2 Out-Of-Band

Primary Engine: 10.120.85.81/10.120.85.81

Secondary Engine: None

Auth. Access Type: Manual RADIUS Configuration

Virtual Router Name:

RADIUS Attributes to Send: Filter-Id (Strip)

RADIUS Accounting: Enabled

Management RADIUS Server 1: None

Management RADIUS Server 2: None

Network RADIUS Server: None

Policy Domain: -- Do Not Set --

Advanced Settings...

Save Close

After enforcing, the next time the Policy is assigned, the modification to the RADIUS Attribute is applied automatically.

**Edit Policy Mapping** ✕

Name:

Map to Location:

Policy Role:

VLAN [ID] Name:

VLAN Egress:

**Filter:**

Port Profile:

Virtual Router:

Login-LAT-Group:

Login-LAT-Port:

Custom 1:

Custom 2:

Dashboard Policy Access Control End-Systems Reports [End-System Details: desktop-cbq501h.cse.ets.com](#)

Access Profile **End-System** End-System Events Health Results

---

**End-System Details**

End-System: 68:1C:A2:04:9A:3A, 192.168.50.150, desktop-cbq501h.cse.ets.com  
 User Name: Doe, John  
 Activity: Last seen 01/24/2020 11:15:47 AM, First seen 01/24/2020 10:46:05 AM  
 Device Information: Windows (Windows 10)

---

**Location**

Location: 192.168.3.165/34-85-84-06-65-D5:XIQ-Control-Open, change\_me  
 Access Control Engine: Default, 10.120.85.81  
 ELIN:

---

**Authentication Sessions**

Session Time:	01/24/2020 11:15:47 AM	State:	Accept
Policy:	GuestAccess	Extended State:	
RFC 3580 VLAN:		State Description:	Authenticated Rule 0 [Any, "", Any] , Auth Method: LOCAL_AUTH
Profile:	Guest Access NAC Profile	Last Scan Result:	
Reason:	Rule: "Registered Guests"	Authorization:	Filter-Id='GuestAccess'

---

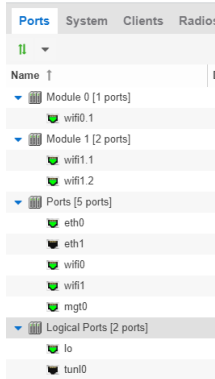
**Registration**

## Appendix F: XMC licensing note

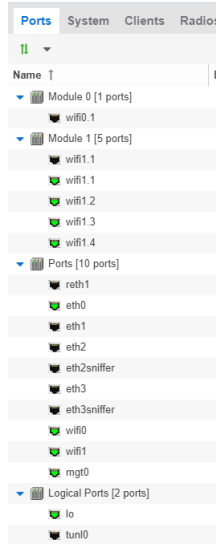
Each Radius Client (the source of the radius request, aka NAS) must be added to the XMC database. With the perpetual licensing (NMS-xxx, NMS-ADV-xxx) and per switch subscription licensing (97203-27001, 97202-2700, 97201-27001) the number of added nodes contribute to the total cost of ownership.

The licensing in XMC version 8.4 handles XIQ Access Point as Non Extreme device. If the XIQ Access Point reports less than 10 ports then it consumes 1:10 of node license. If the XIQ Access Point reports 10 or more physical ports then it consumes a full node license.

Port tree example of AP245X



Port tree example of AP150W



The actual license impact can be checked by selecting the **Diagnostics** tab in the **Administration** menu, then chose **Level: Diagnostics**, expand the tree, click on **System** and chose **License Diagnostics**.

License Diagnostics

[License Device Limits]  
 License Count: 37  
 Soft Limit: 10,000  
 Hard Limit: 10,005

Status Only Count: 0  
 Status Only Limit: 10,000

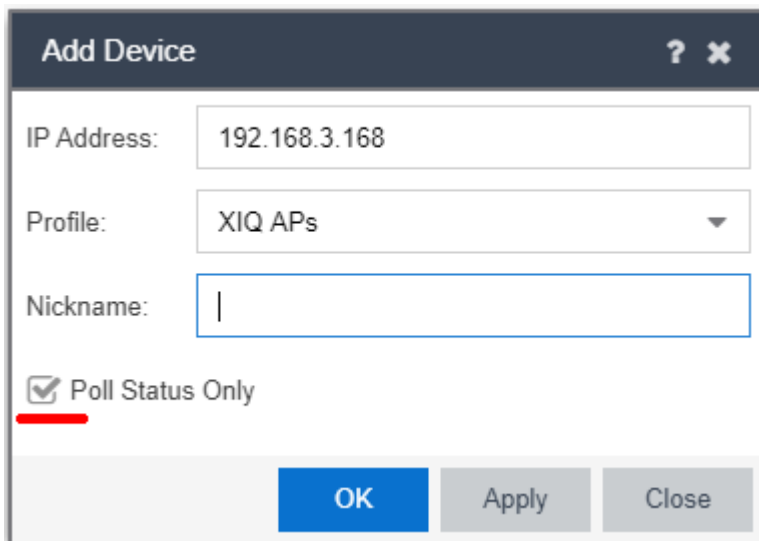
[License Impact Details by Device Type]

Device Type	Count	Ratio	Impact
APs	0	1:10	0
BPEs	0	1:10	0
Extreme (Not including APs)	28	1:1	28
Non Extreme < 10 ports	16	1:10	2
Non Extreme >= 10 ports	5	1:1	5
Ping Only	2	1:10	1
vSensors	2	1:10	1

[License Details]  
 Licenses: 1

Valid Eval Subscription Updatable Expiring Days Size Type Clients License  
 0001:NETSIGHTFEVAL:

The XIQ Access Point can be added to the XMC database as **“Poll Status Only”**.



The screenshot shows a dialog box titled "Add Device" with a dark header bar containing a question mark and a close button. The dialog contains the following fields and controls:

- IP Address:** A text input field containing the value "192.168.3.168".
- Profile:** A dropdown menu with "XIQ APs" selected.
- Nickname:** An empty text input field.
- Options:** A checkbox labeled "Poll Status Only" is checked. A red underline is visible under the text "Poll Status Only".
- Buttons:** Three buttons are located at the bottom: "OK" (highlighted in blue), "Apply", and "Close".

Poll Status Only devices do not support collection of statistics, FlexViews, Network Status Monitor, map links, or enforcement via Extreme Management Center. You can add a maximum of 10,000 Status Only devices in Extreme Management Center, which do not count against your licensed device limit.

## Revision History

---

Date	Revision	Changes Made	Author
2020-01-24	1.0	Initial Release	T. Marcotte Z. Pala
2020-01-29	1.1	Small typo fix in Appendix E	T. Marcotte
2020-04-12	1.2	Added Appendix F	Z. Pala