How To: ExtremeControl for ExtremeCloud IQ – Site Engine and ExtremeCloud IQ APs

Abstract: This document covers implementation of ExtremeCloud IQ APs in ExtremeControl. This guide provides guidance on configuring wireless devices to integrate with ExtremeControl. However, it does not cover implementation of ExtremeControl functionalities.

Part Number: 9037364-01 Rev AA

Published: December 2022

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

Contents

Prerequisites and Limitations

This document is intended for SEs and partners who are familiar with both ExtremeCloud IQ and ExtremeControl. Only the primary touchpoints between the two products are covered in this document; all other settings are considered out of scope.

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

- ExtremeCloud IQ – Site Engine 21.4.10.99 and later
- ExtremeControl 21.4.10.99 and later
- ExtremeCloud IQ Build Version 19.11.1.7 with AP Firmware 10.0r7a

Due to the nature of adding access points as devices that can authenticate against ExtremeControl, a few design limitations and suggestions 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 ExtremeCloud IQ - Site Engine and ExtremeControl.
- 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 ExtremeCloud IQ - Site Engine.
- An ExtremeCloud IQ - Site Engine workflow, available through GitHub, can assist with the discovery and addition of ExtremeCloud IQ APs to ExtremeCloud IQ - Site Engine. The workflow called “Import APs from XIQ” can be found at this site:

https://github.com/extremenetworks/ExtremeScripting/blob/master/XMC_XIQ-SE/oneview_workflows/README.md

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 following the steps in this guide, it is also recommended that you have IP helper addresses pointed to the Access Control Engine and SNMP Read-Only credentials configured on the router. The Access Control Engine can query these to assist with IP resolution.

Part 1: Wireless Configuration of ExtremeCloud IQ

The following must be configured on ExtremeCloud IQ in order to integrate with ExtremeControl:

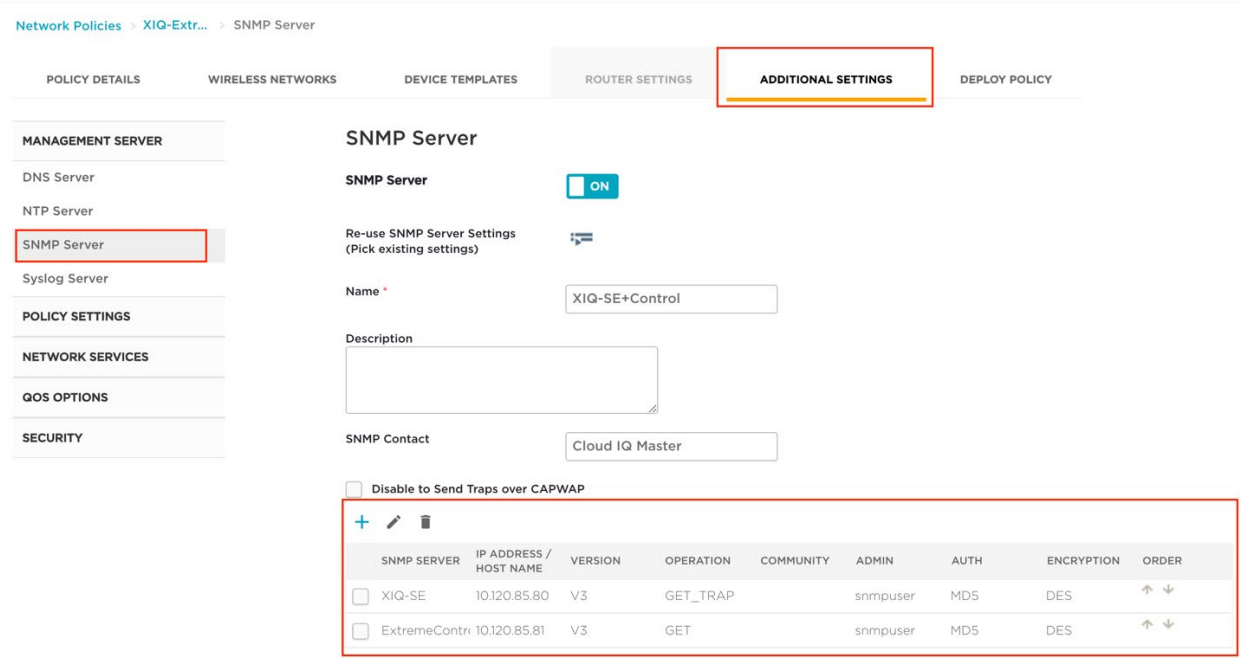
- SNMPv3 Polling
- RADIUS Authentication
- RADIUS Accounting
- RFC 3576/5176 Reauthentication
- External Captive Portal Redirection

The configuration of the access point is done through ExtremeCloud IQ. When the configuration is complete, all processing and authentication occur between the access point and ExtremeControl. The configuration consists of the following parts:

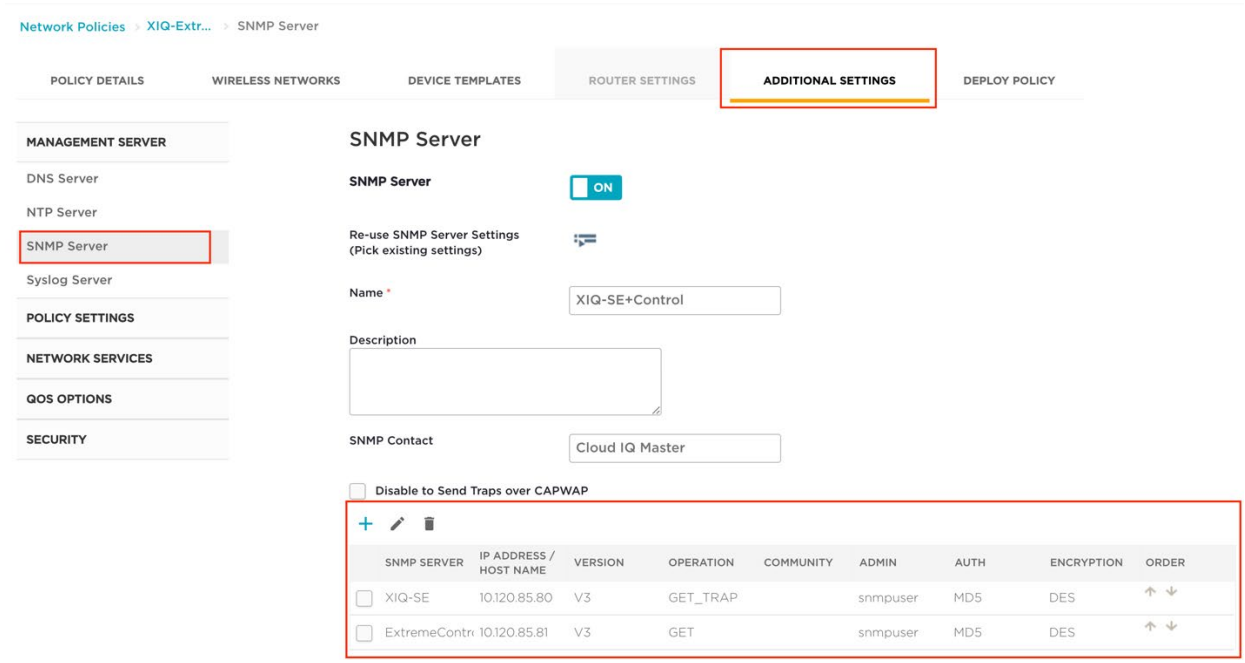
1. Configure an SNMP Server profile so that ExtremeCloud IQ - Site Engine and the Access Control Engines can poll the AP.
2. Enable SNMP on the Device Templates for all APs.
3. Configure the RADIUS settings to authenticate against the Access Control Engines.
4. Configure the User Profiles that will be 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

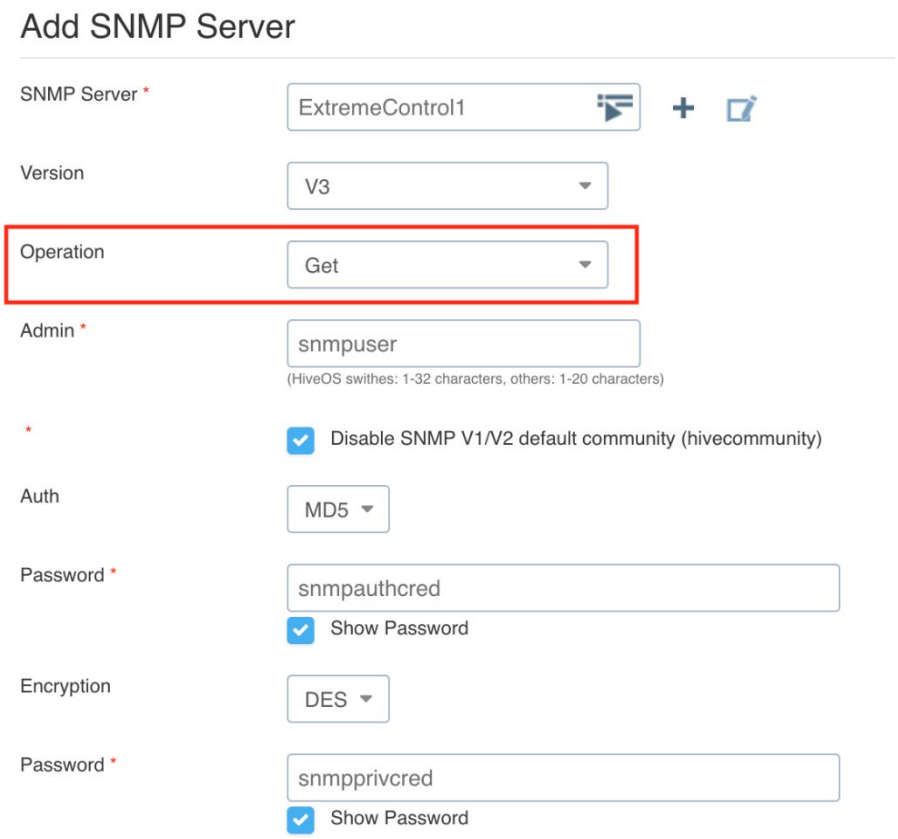
Configuration of the SNMP profile should contain ExtremeCloud IQ – Site Engine and all Access Control Engines. To configure the SNMP Profile, edit the **Network Policy** in the **Configure** menu. The settings are configured in the Additional Settings tab. In the **Management Server** section, the **SNMP Server** configuration is found.



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



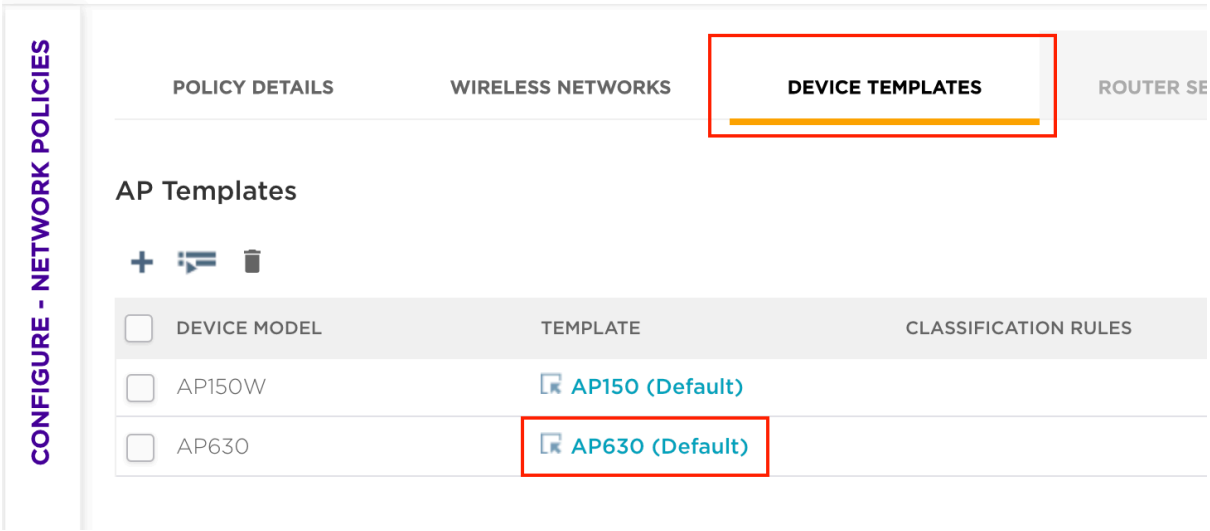
When configuring the SNMP Profile for the Access Control Engine, the same SNMP credentials that were used for ExtremeCloud IQ - Site Engine are used for the Access Control Engine. A new IP Object might need to be created for each Access Control Engine that will be used. In addition, the Operation should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



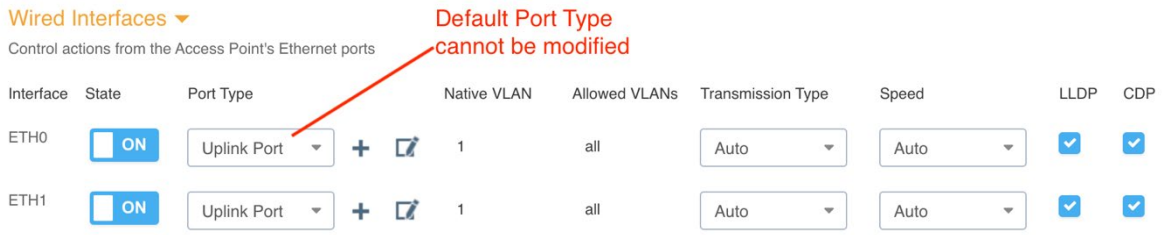
Step 2 – Enable SNMP on the Device Template.

The default setting for access points is to not allow SNMP. To enable SNMP on the access points, SNMP needs to be enabled on the wired uplink port. Because default templates cannot be edited in ExtremeCloud IQ, a new template must be created. This process is most easily performed by cloning the existing object and then adjusting it as needed.

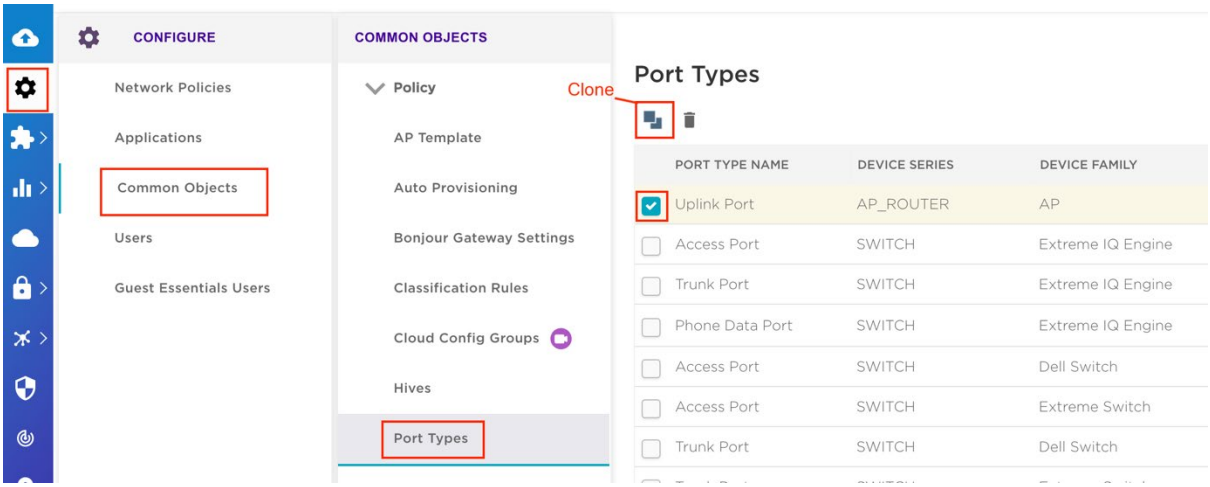
Navigate to the Device Templates by editing the Network Policy in the Configure menu. In the Device Templates, each AP Template needs to be added or modified if it already exists. Select the Template to edit:



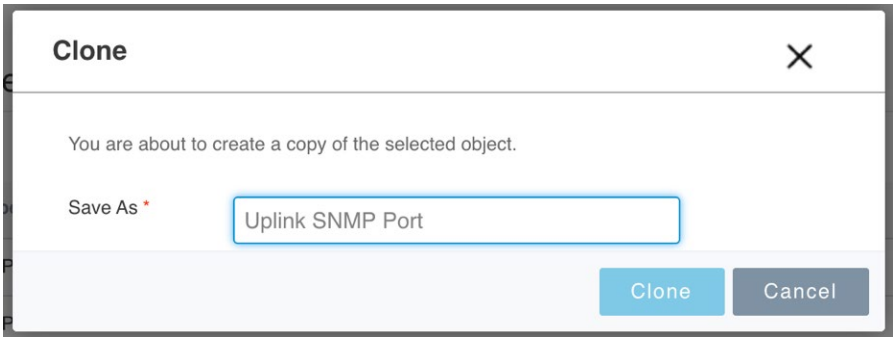
At the Wired Interfaces section, find the interface which will be used to communicate to the Access Control Engine. If the default port type of Uplink Port is in use, then the Port Type will need to be cloned. If a non-default port type is in use, skip the next steps with instructions on creating a custom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



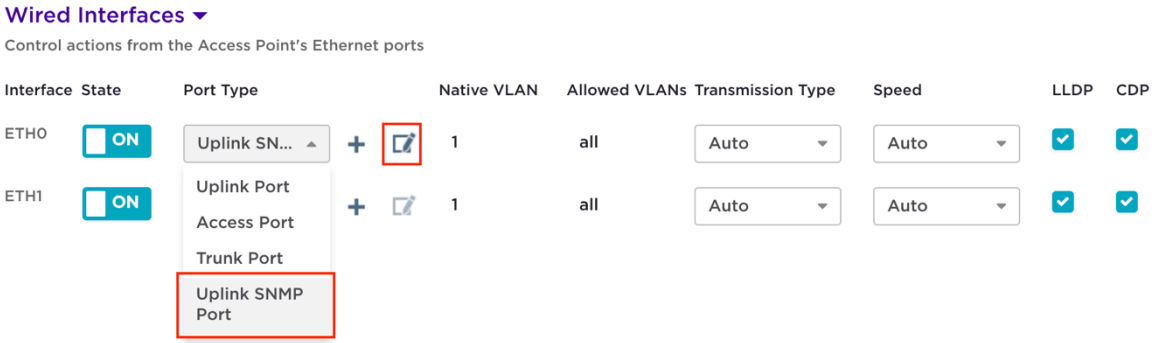
To clone the default Port Type, navigate to **Common Objects** under the Configure tab. Select **Port Types** from the **Policy** section. Select the default port type that was previously configured and then clone.



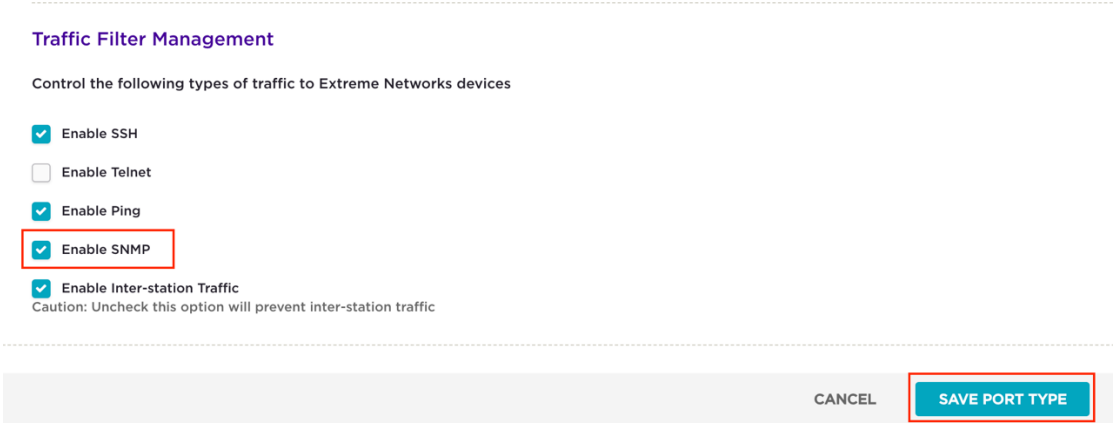
Name the new Port Type and select **Clone**.



After cloning the port, navigate back to the **Device Templates** and **Wired Interfaces** section. From the drop-down list, select the newly created Port Type and then select **Edit**.



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.

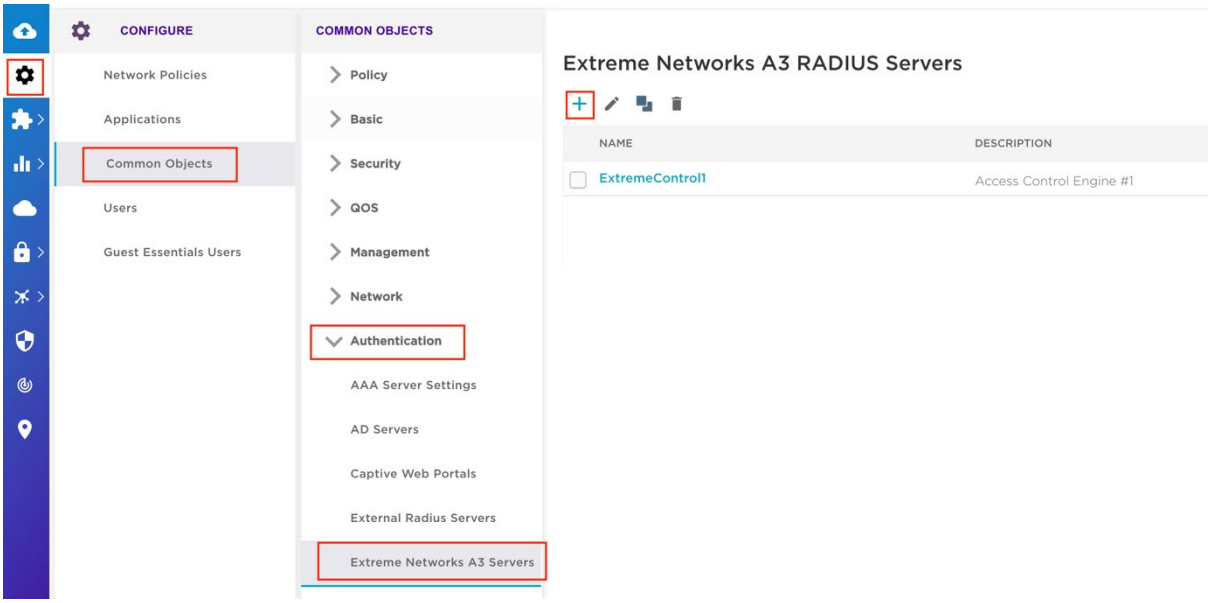


Step 3 – Configure RADIUS

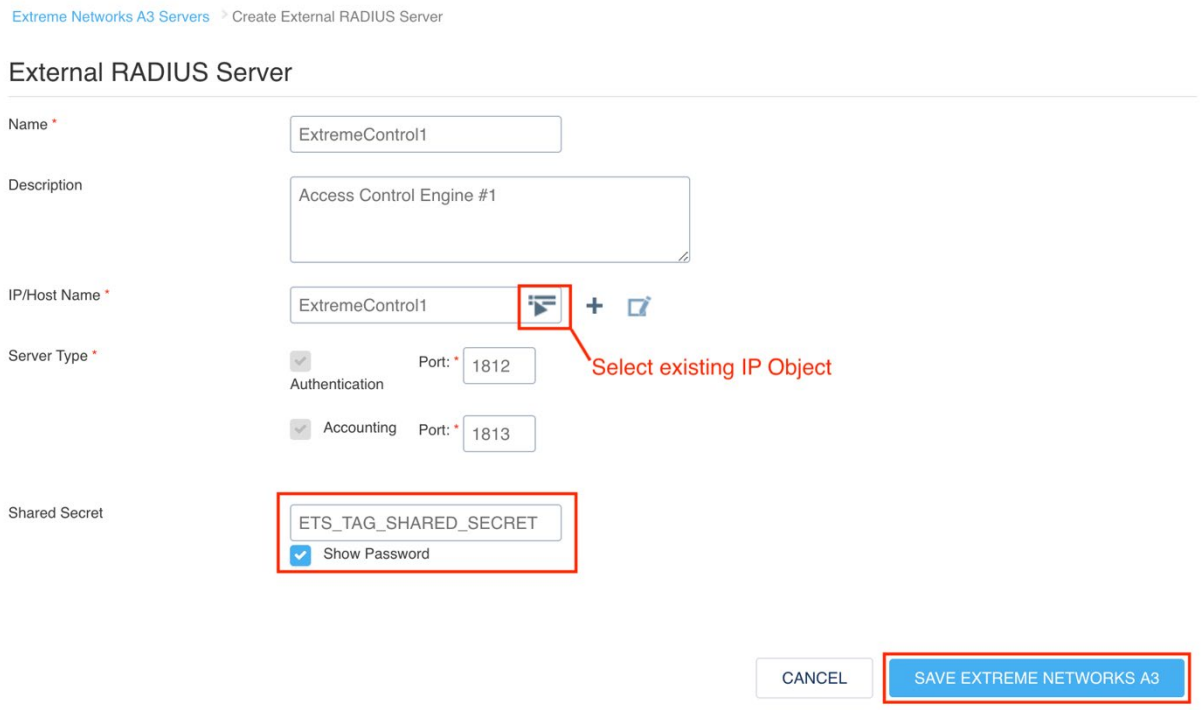
The RADIUS Server configuration can be performed in two unique ways. One method is to create it while creating the SSID. However, the method shown below is to create the Common Object before creating the SSID.

> **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 that 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 Add 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.



Step 4 – Configure User Profiles

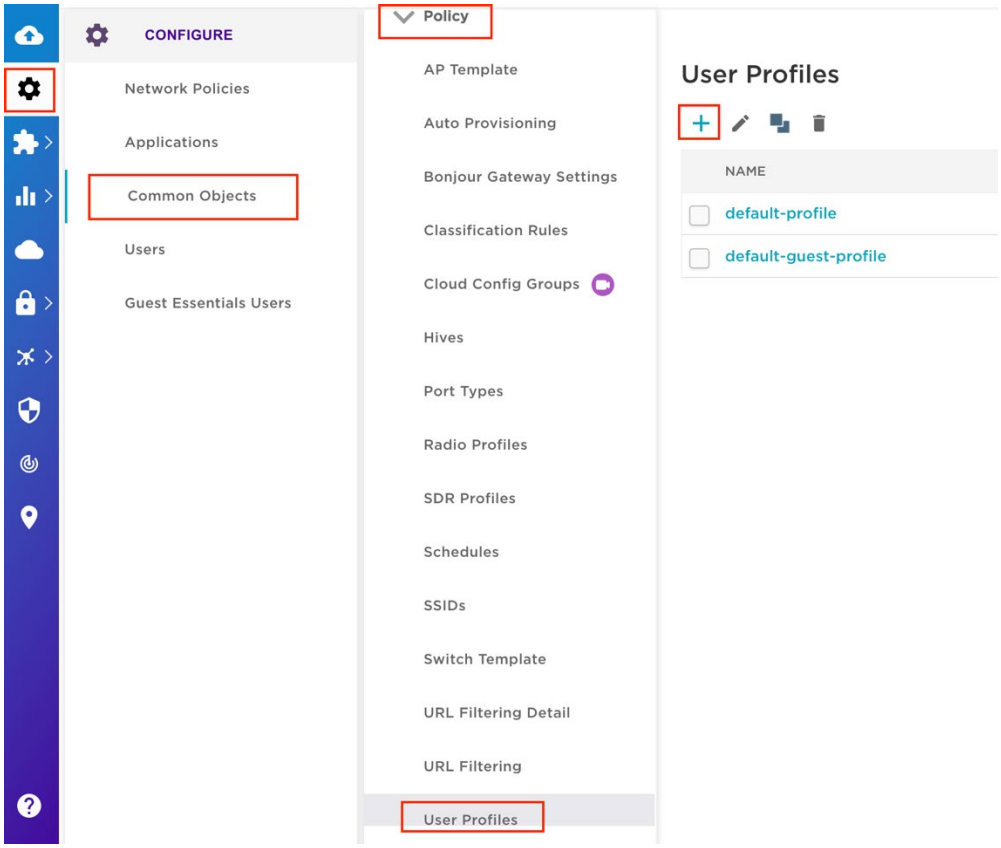
User Profiles define the access that a user or device has when connected to the network via ExtremeCloud IQ. These profiles can be dynamically assigned and contain many definitions including Firewall Rules, VLAN assignment, and QoS settings. These profiles need to be defined

before the 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:

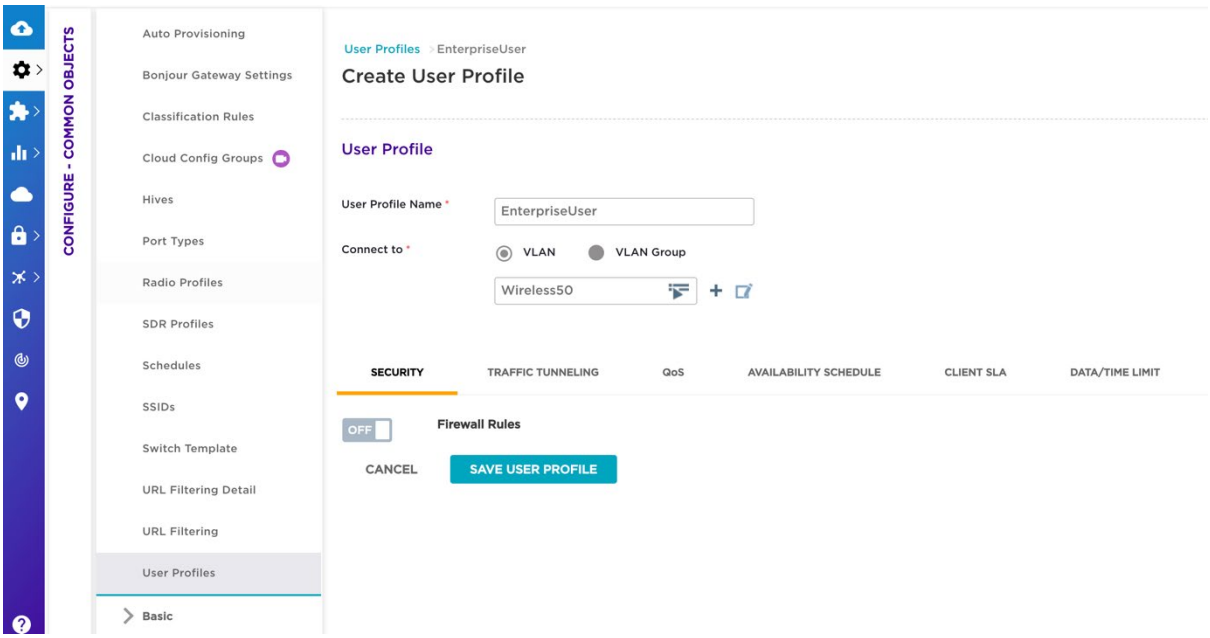
- Unregistered – This profile limits traffic and redirects web traffic to ExtremeControl
- GuestAccess – This profile limits internal traffic but allows full access to the Internet.
- EnterpriseUser – This profile allows full access to the network.

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

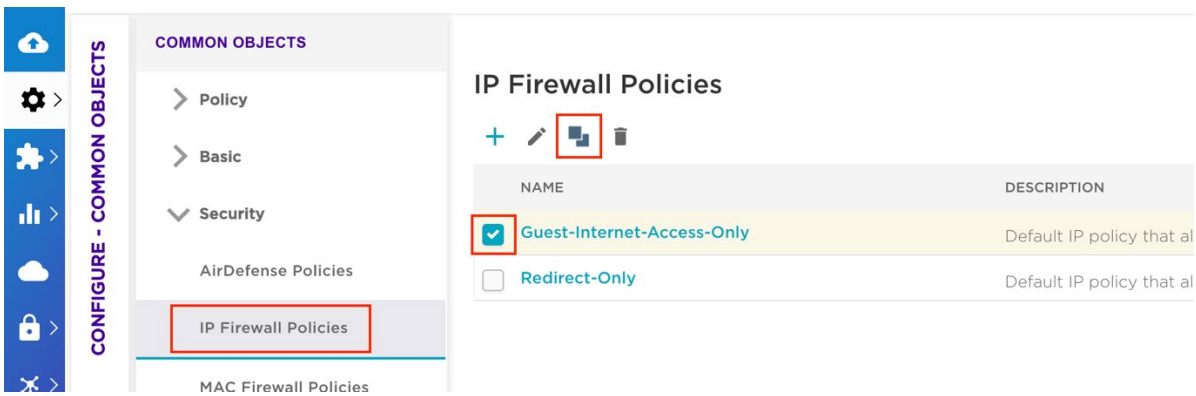
To create a new User Profile, select **Add**. Define the **User Profile Name** and **VLAN** (or VLAN Group). When selecting a VLAN, a new VLAN Object needs to be created or selected. Additional settings can be configured if desired. However, this is an example of only a VLAN being assigned to a user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



Create a GuestAccess User Profile with Firewall

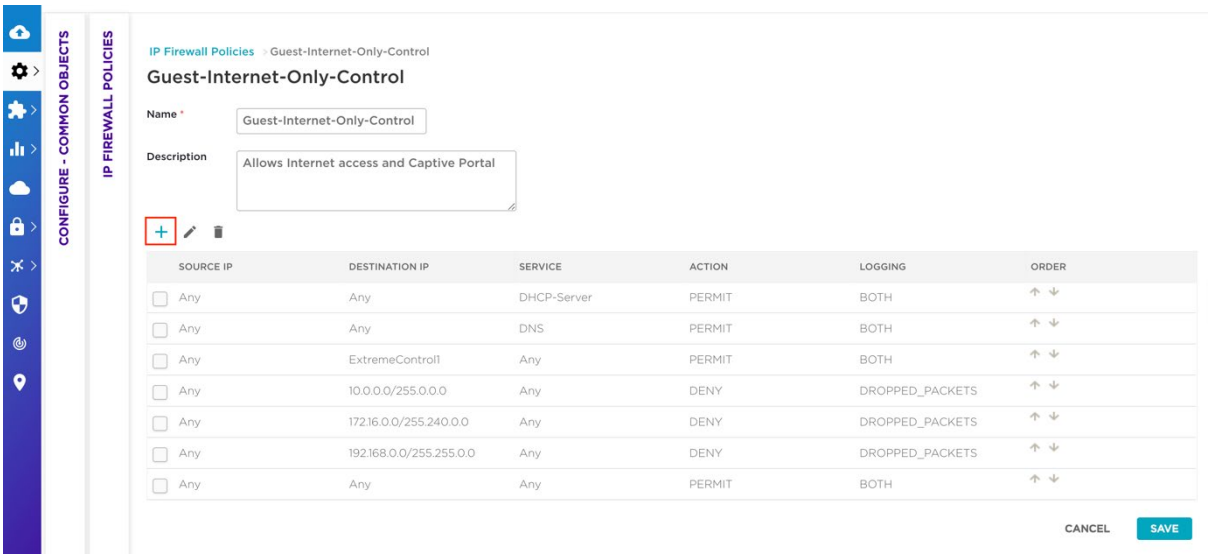
When adding a Firewall to a User Profile, it can be added in line with the profile, or a Common Object for IP Firewall can be created before the User Profile. For common configurations such as Guest Access firewalls or Redirection firewalls, it is often helpful to clone the default objects to save time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

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

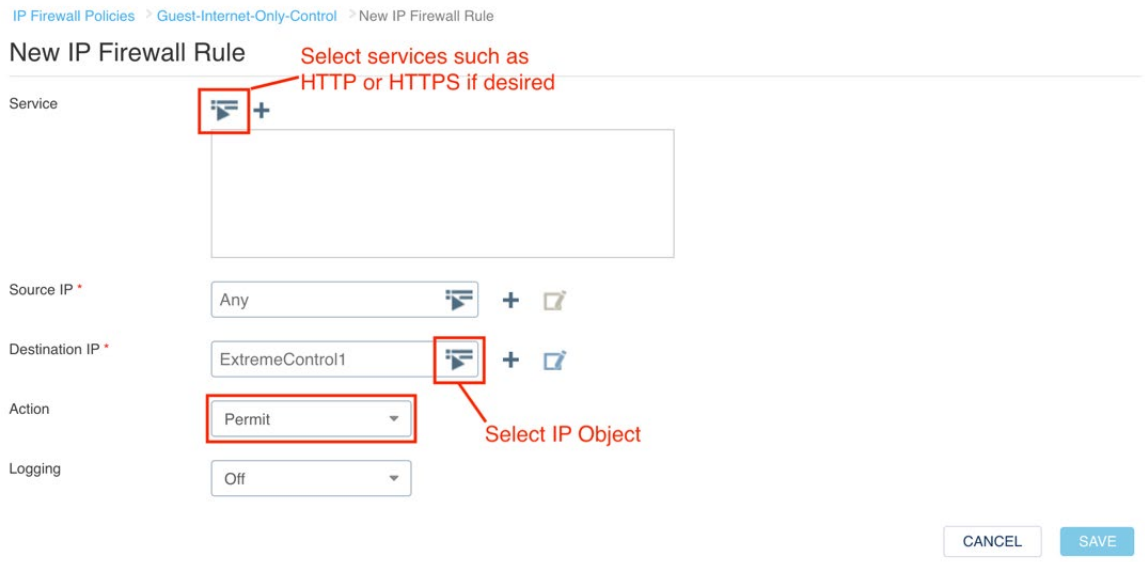


Name the new policy and select **Edit**. In the new policy, some rules need to be adjusted or added. In particular, for the GuestAccess policy, ensure that web traffic can reach

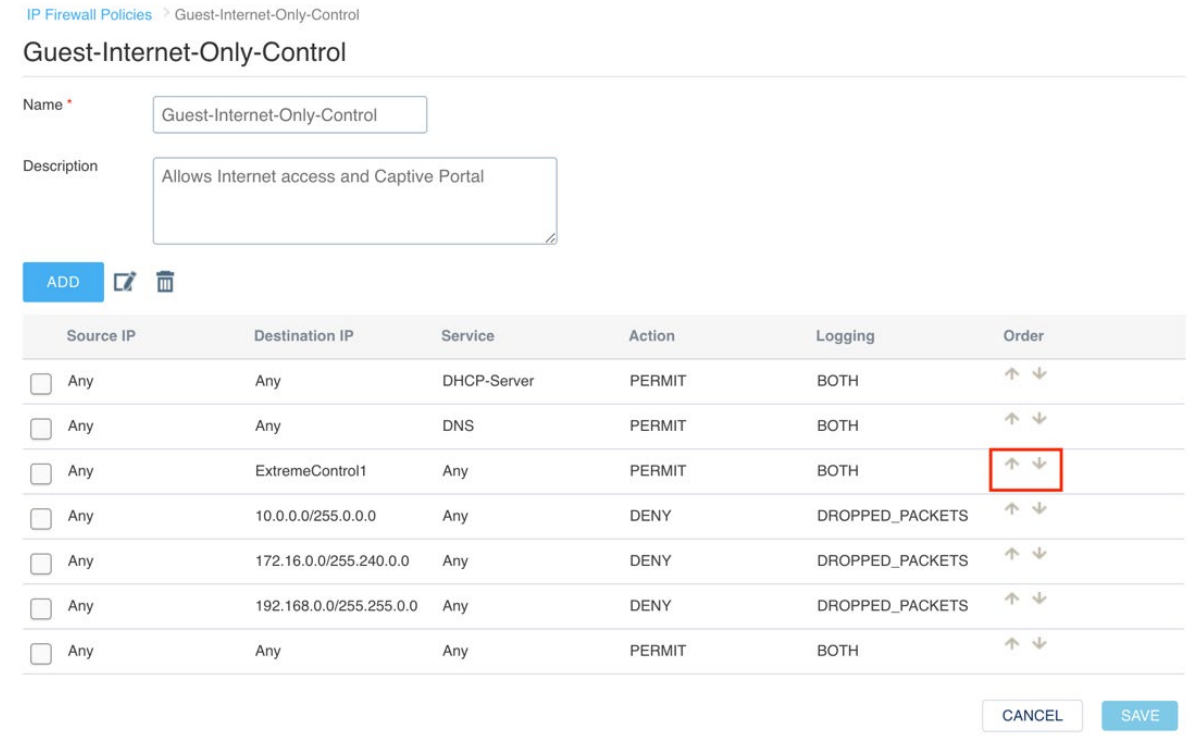
ExtremeControl so that the registration success page can be displayed. To add a new rule, select **Add**.



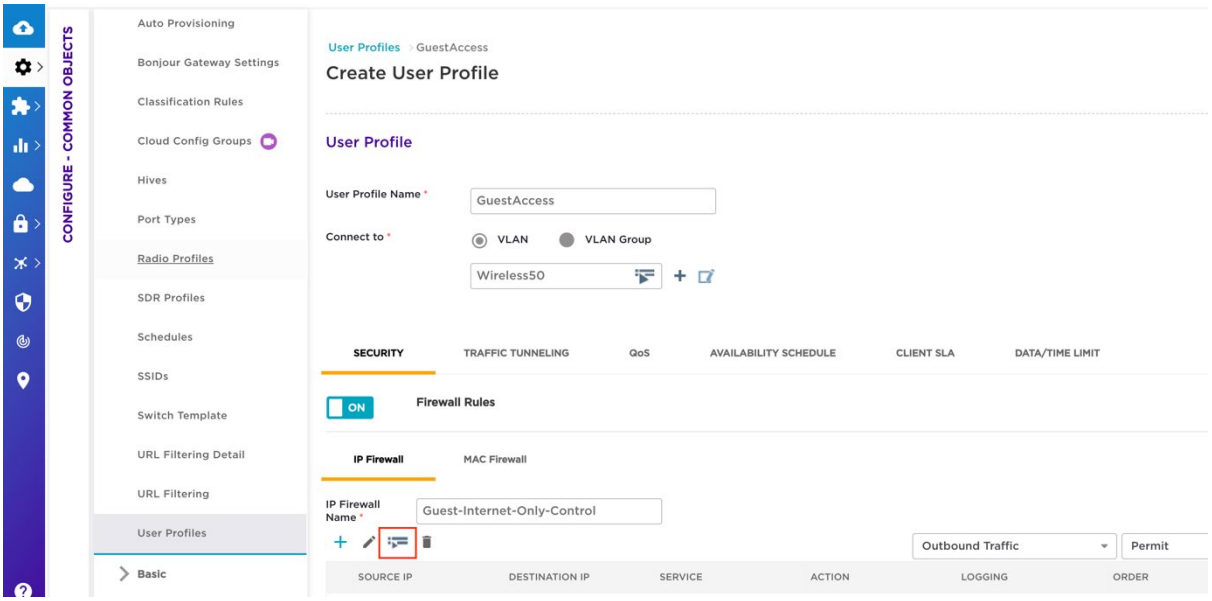
While creating a new rule to allow traffic to the Access Control Engine, set the Destination IP to the IP Object previously created for the Access Control Engines. Repeat this process for each engine that will be used.



When the rule is saved, ensure it is placed correctly in the Firewall Policy. Because the list is ordered, you can use the up and down arrows to position the rule appropriately.



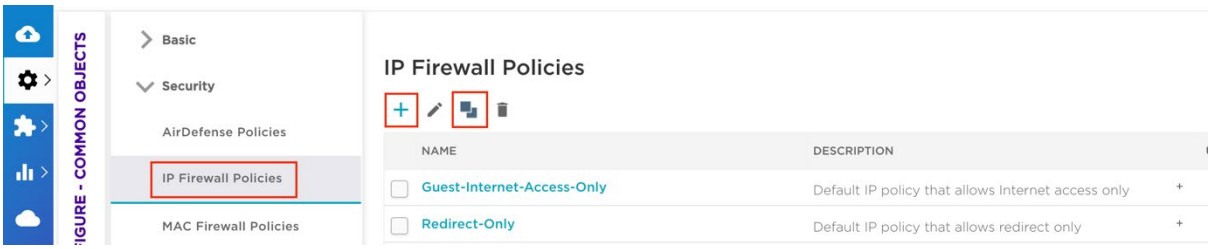
In the **User Profiles**, create a profile with the name GuestAccess. In addition to setting the VLAN, select the **IP Firewall Name** defined in the previous step.



Create an Unregistered User Profile with Firewall and Captive Portal

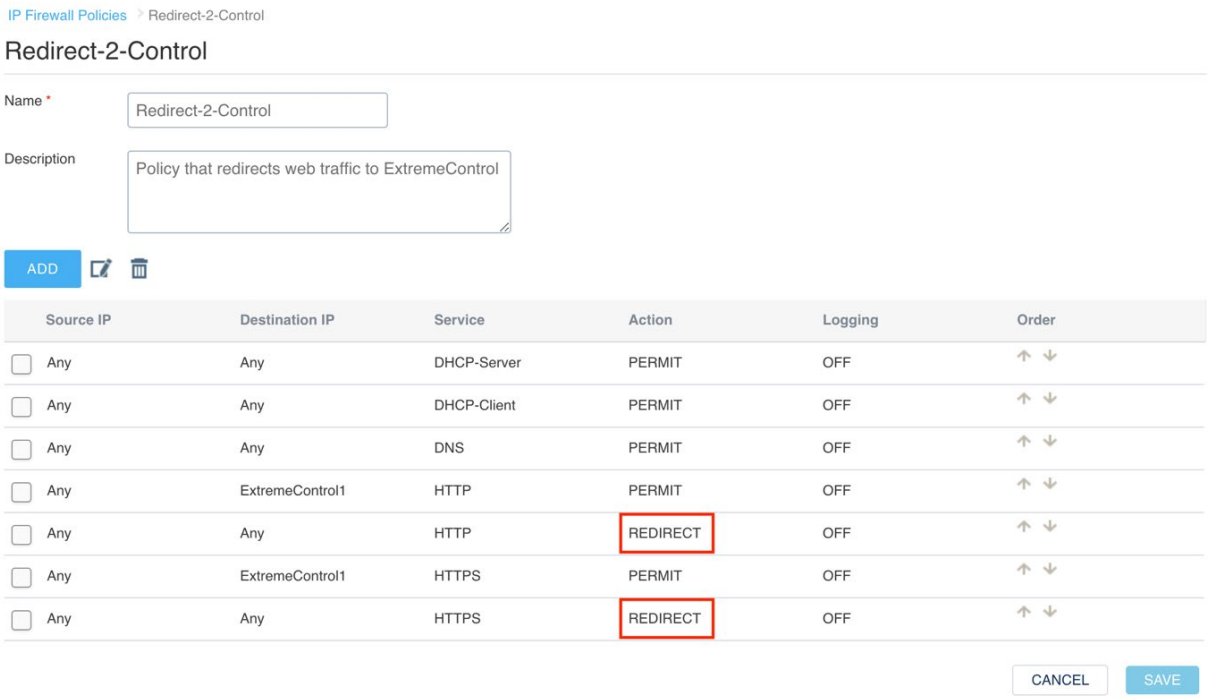
Similar to a GuestAccess User Profile, the Unregistered User Profile needs to have an IP Firewall added to limit access as well as redirect web traffic to ExtremeControl.

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



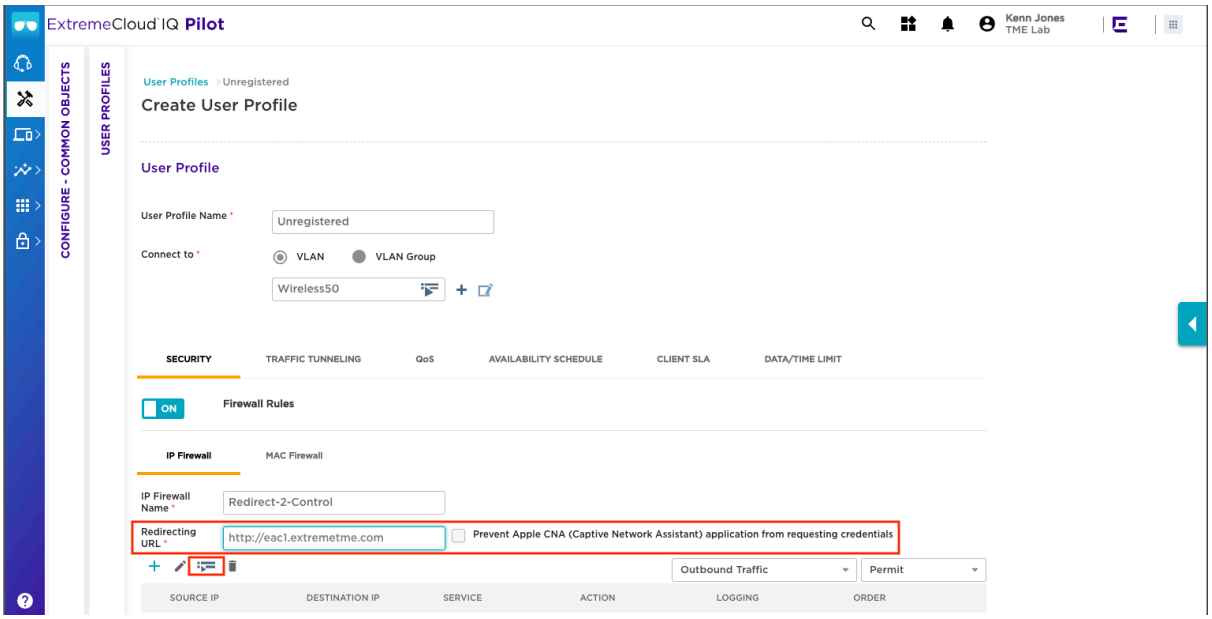
For the captive portal to work, the following rules need to be configured. This example shows one Access Control Engine. However, all Access Control Engines that provide a captive portal should be configured.

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



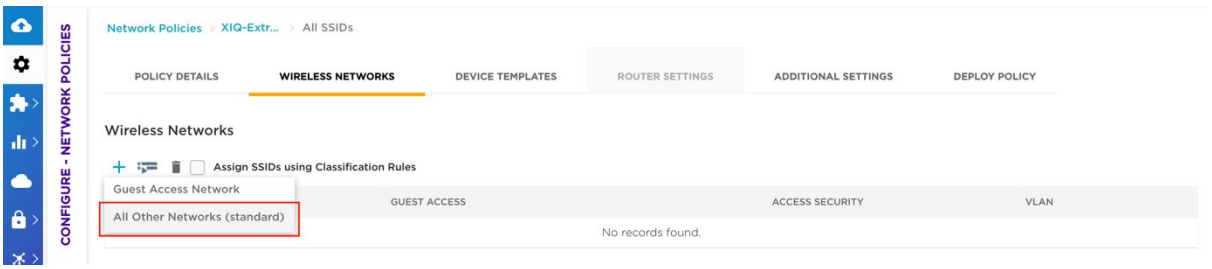
Note
The REDIRECT Action is visible only when the HTTP or HTTPS Services are configured.

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.



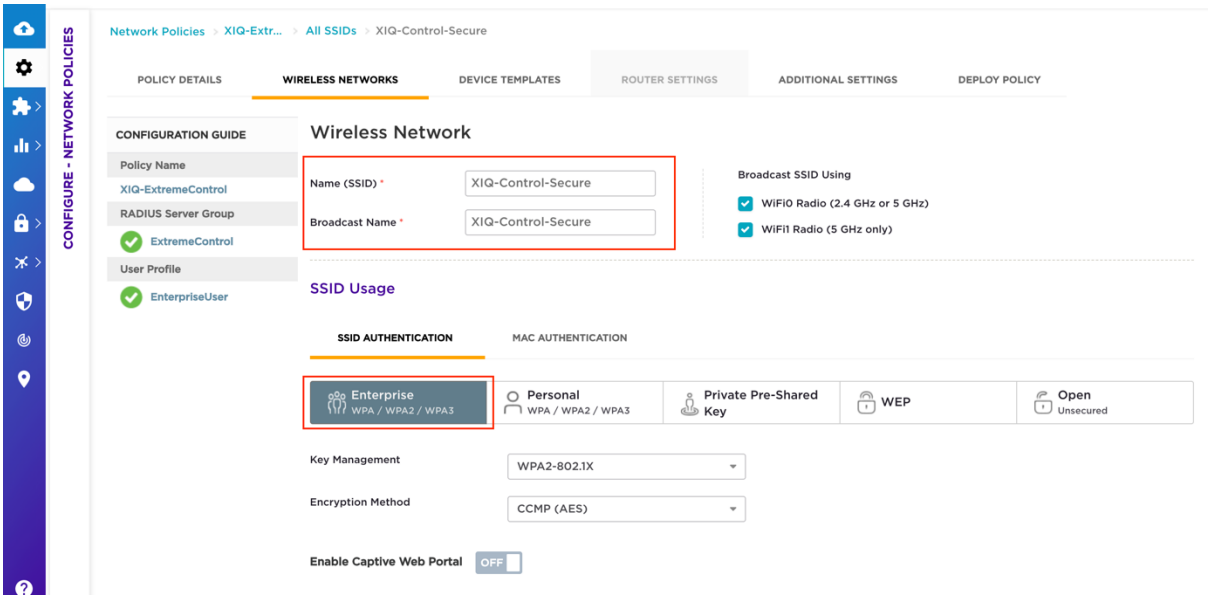
Step 5 – Configuring SSIDs for ExtremeControl

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.

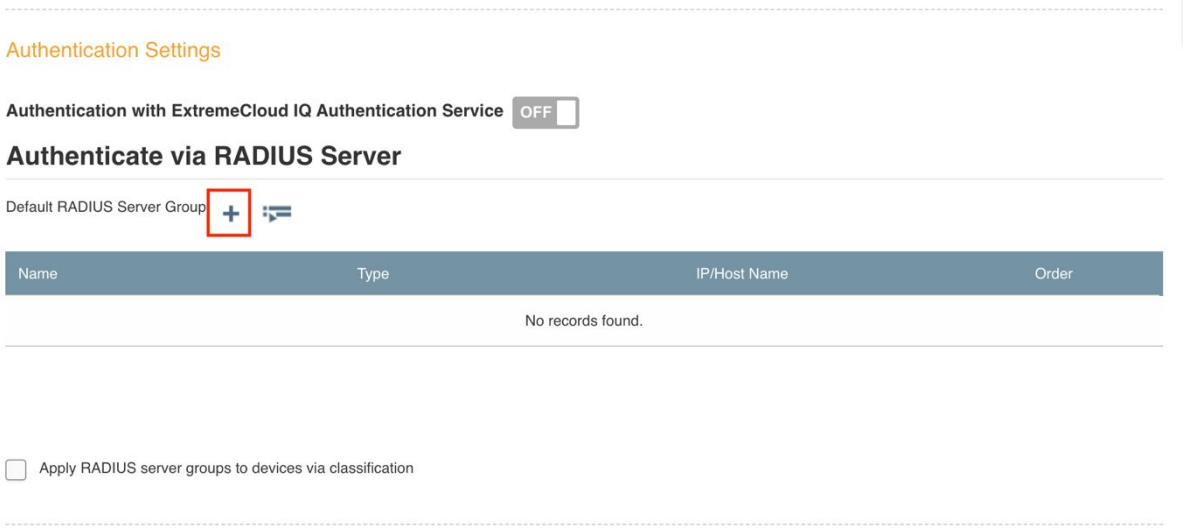


Create a Secure 802.1X SSID

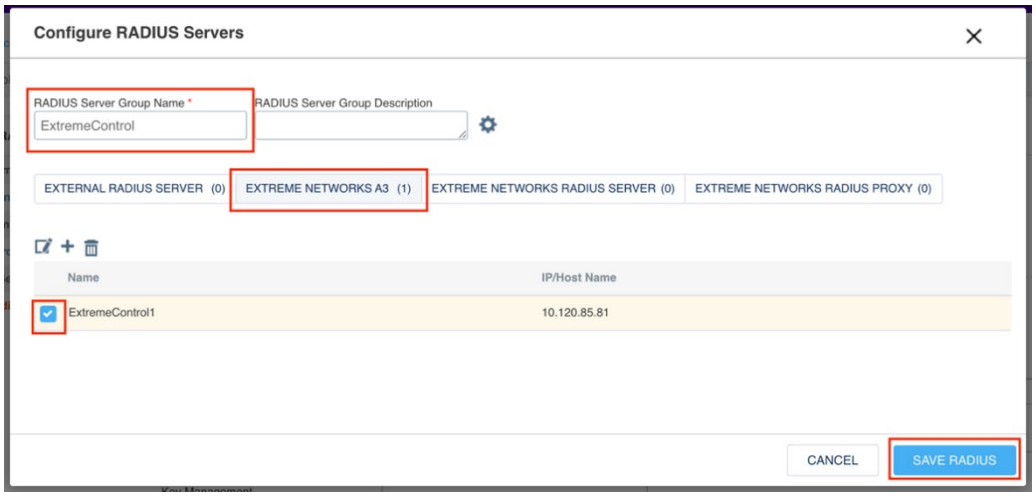
To create a secure SSID that uses 802.1X authentication, set the name of the wireless network and select **Enterprise WPA / WPA2 / WPA3** under SSID Authentication. The default settings for Key Management, Encryption Method, and Captive Web Portal can be left unchanged.



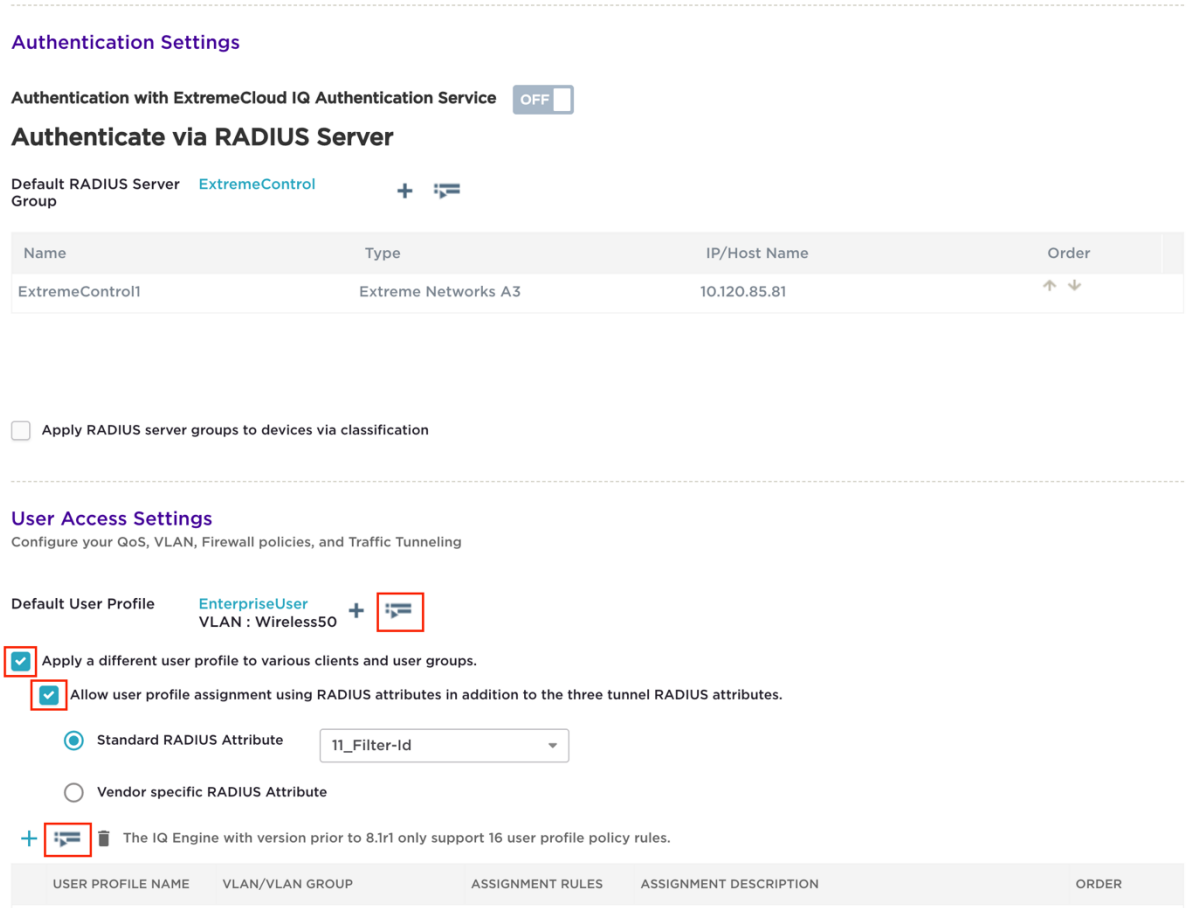
When the Enterprise SSID Authentication method is selected, you are given the option (further down the screen) to configure Authentication Settings. If a RADIUS Server Group has not yet been created, select **Add** to create a new one.



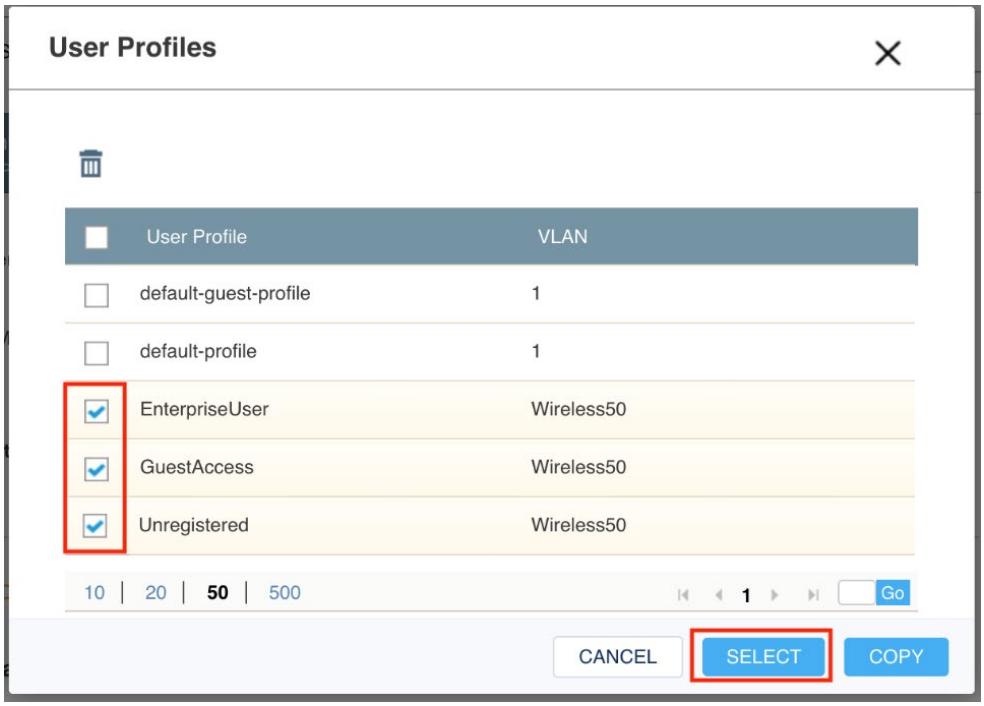
In the **Configure RADIUS Servers** window, set a name for the RADIUS Server Group and select the previously configured Access Control Engine from the Extreme Networks A3 tab.



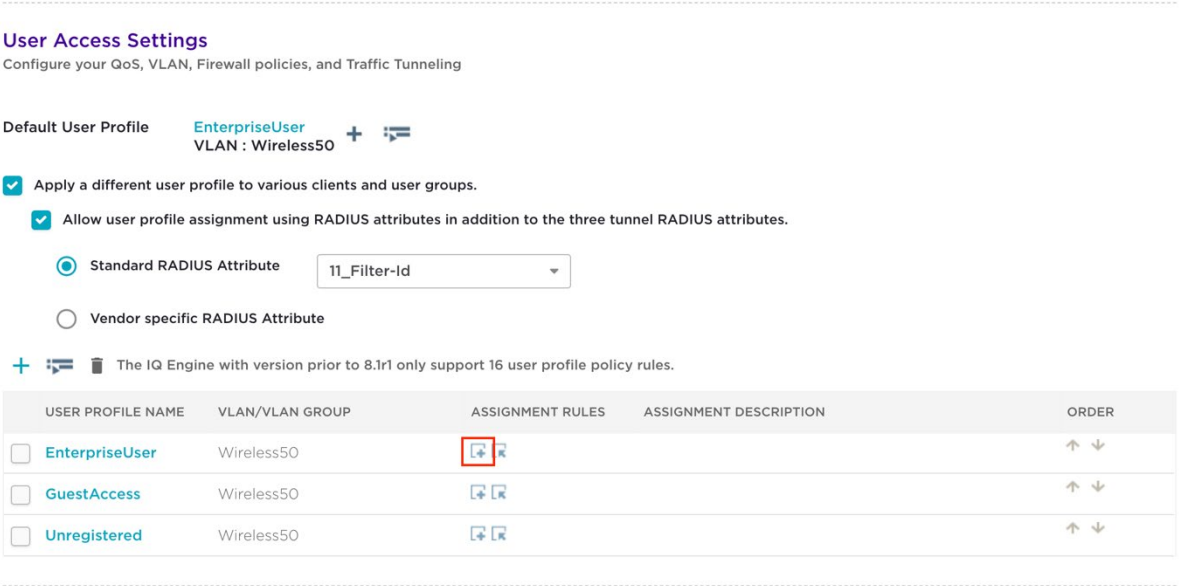
With the RADIUS Servers configured, the **User Access Settings** section needs to be configured to assign the correct User Profiles based on the authorization results from ExtremeControl. First, select the **Default User Profile** to be used if no other profiles match. Next, select the two check boxes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



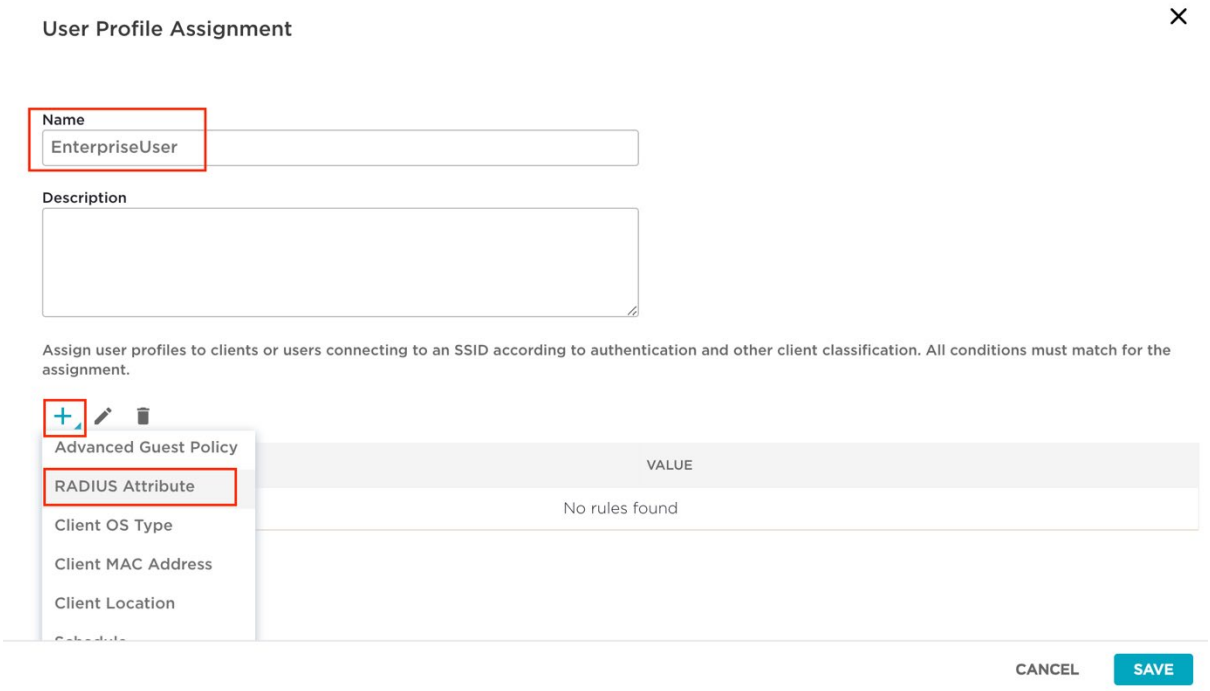
In the **User Profiles** window, enable the desired User Profiles and then click **Select**.



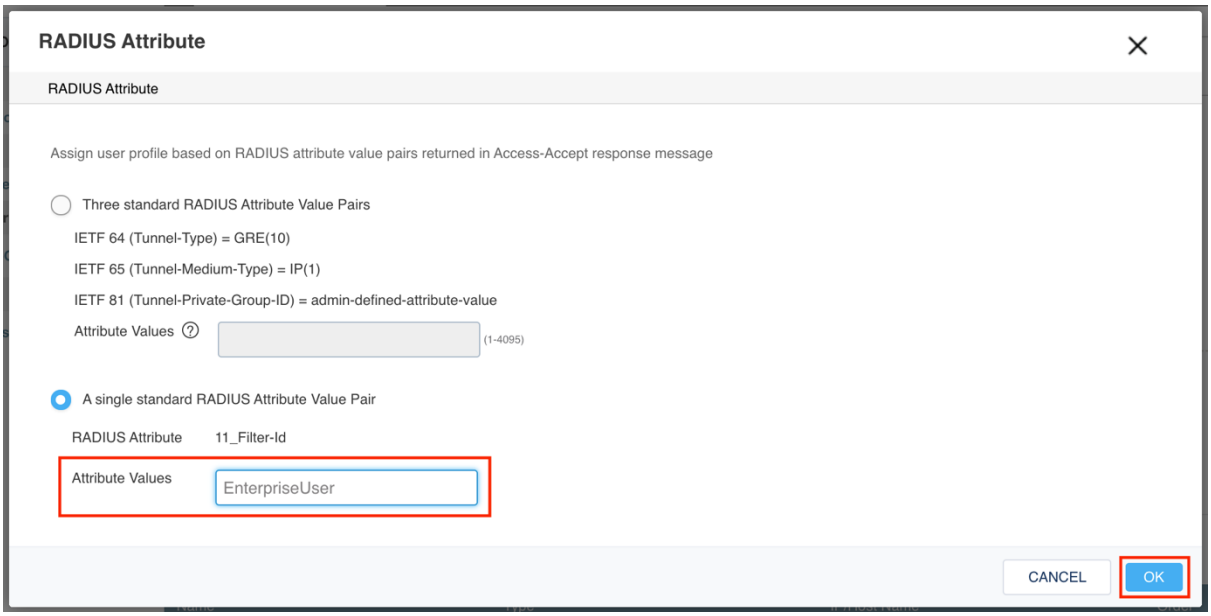
With the User Profiles added, select the **+** option to create a new User Profile Assignment Rule for each User Profile. If an assignment rule was previously created, use the arrow icon next to the plus icon to re-use the assignment rules.



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



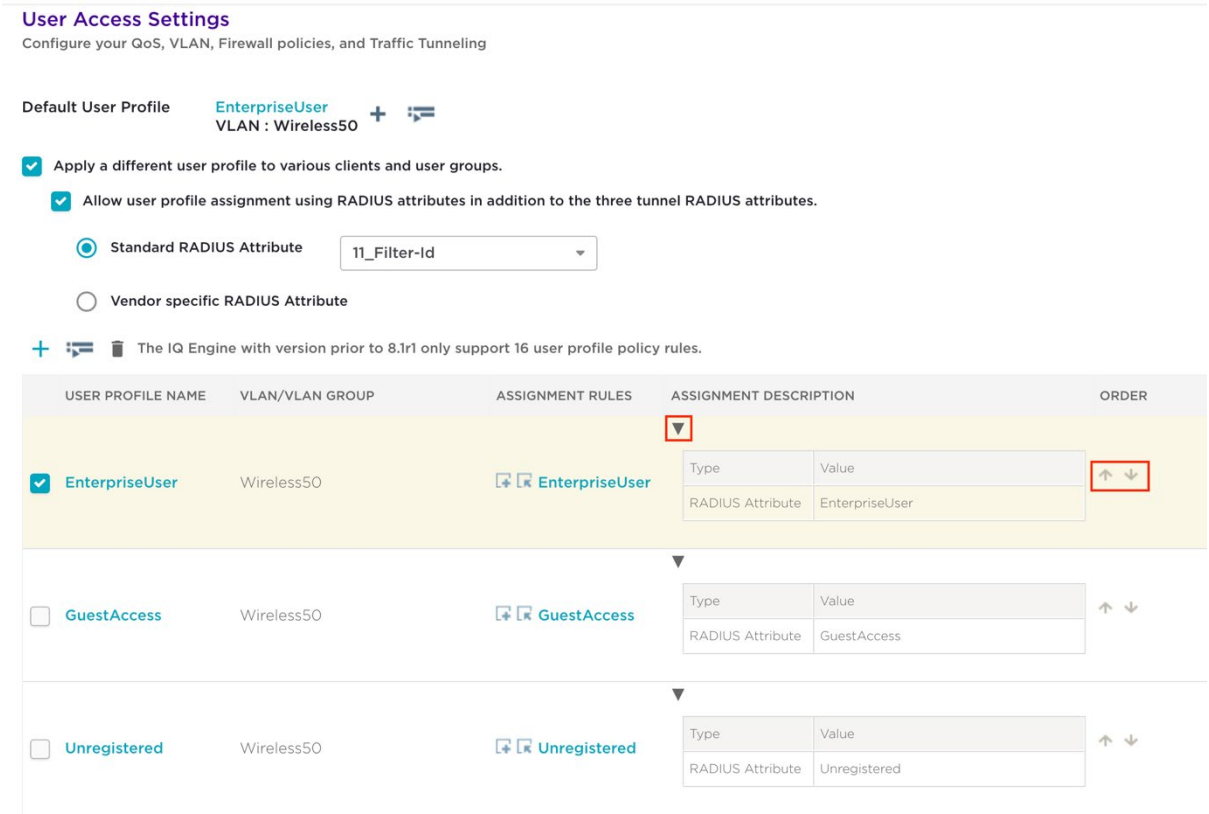
Enter the Filter-ID that will be returned from ExtremeControl as part of the Authorization rules.



Note

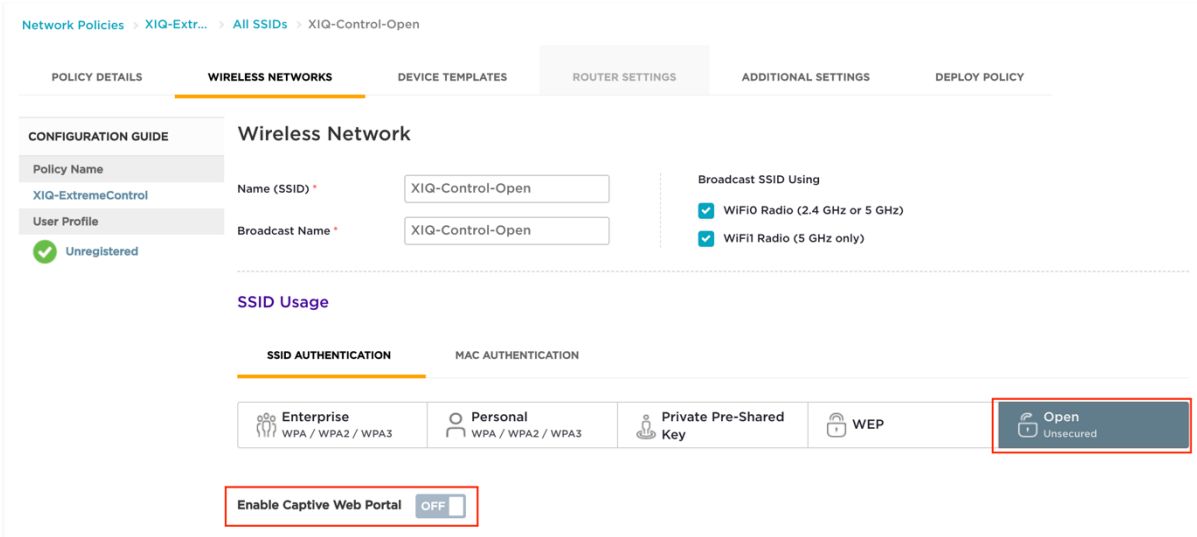
Do not use spaces in the Filter-ID name. They will not be matched correctly during authentication.

Repeat the process of creating assignment rules for each User Profile. To easily see all rule assignments, 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.

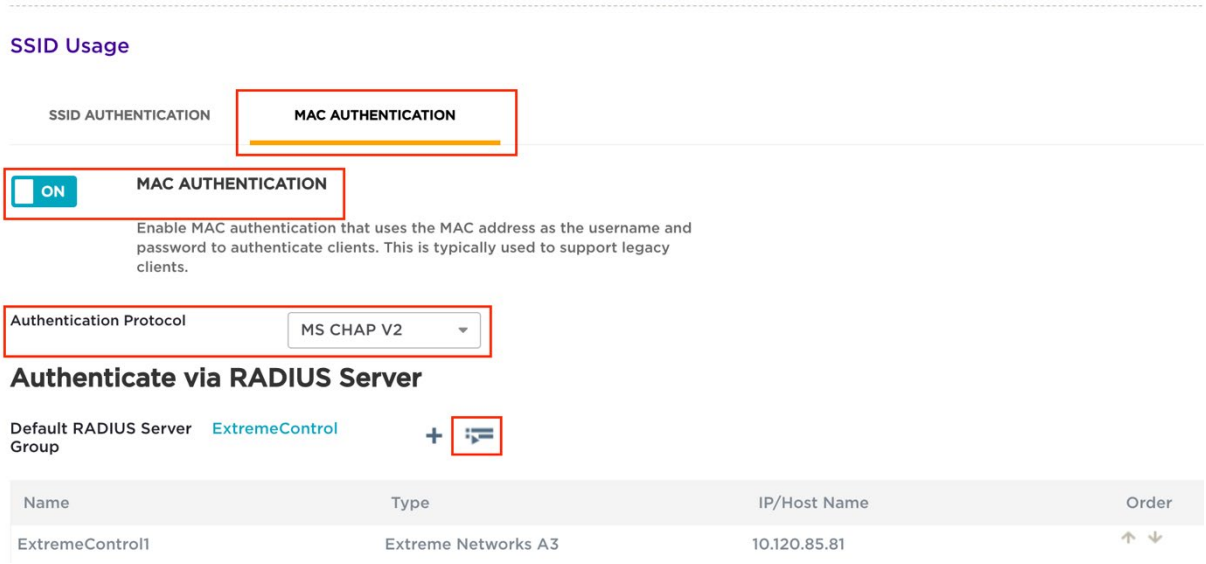


Create an Open / Guest SSID

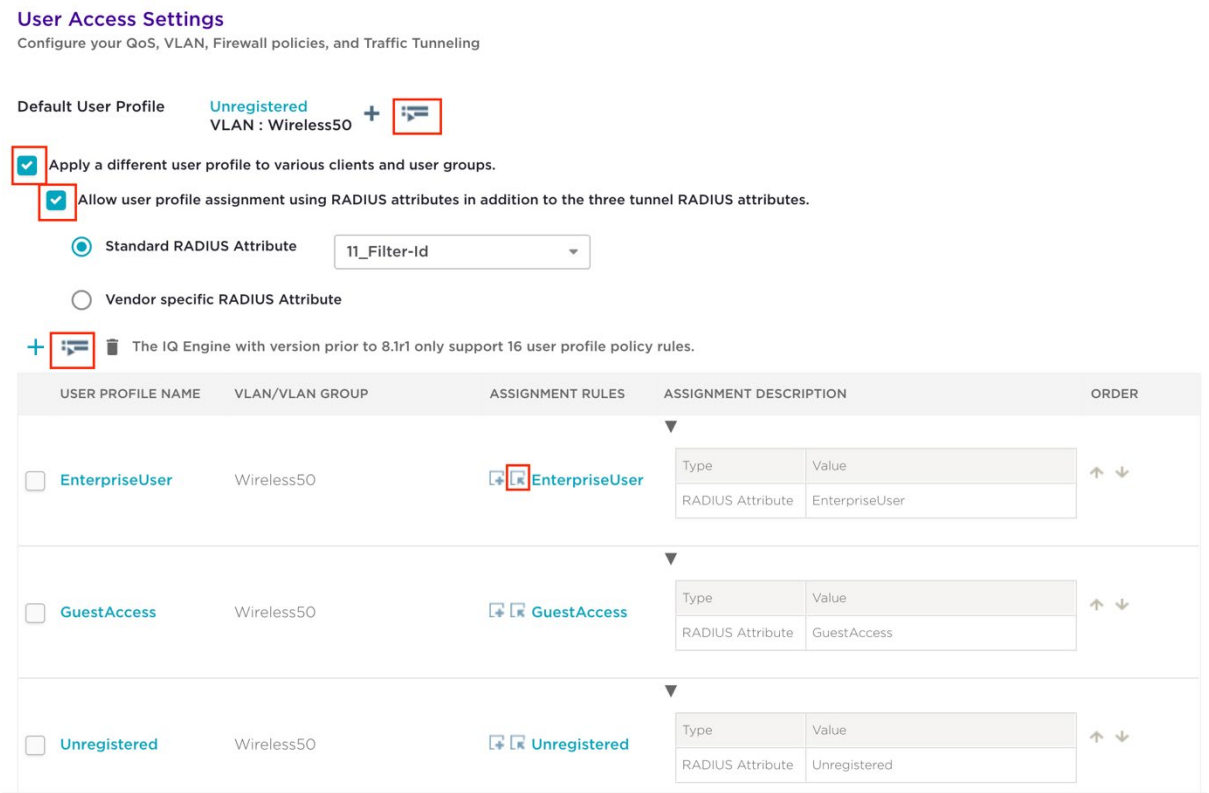
Creating an open SSID is very similar to configuring a secure SSID. The primary difference is in the SSID Usage section. In this section, select either Personal or Open for the SSID Authentication type. Ensure that Enable Captive Web Portal is disabled.



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.



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.



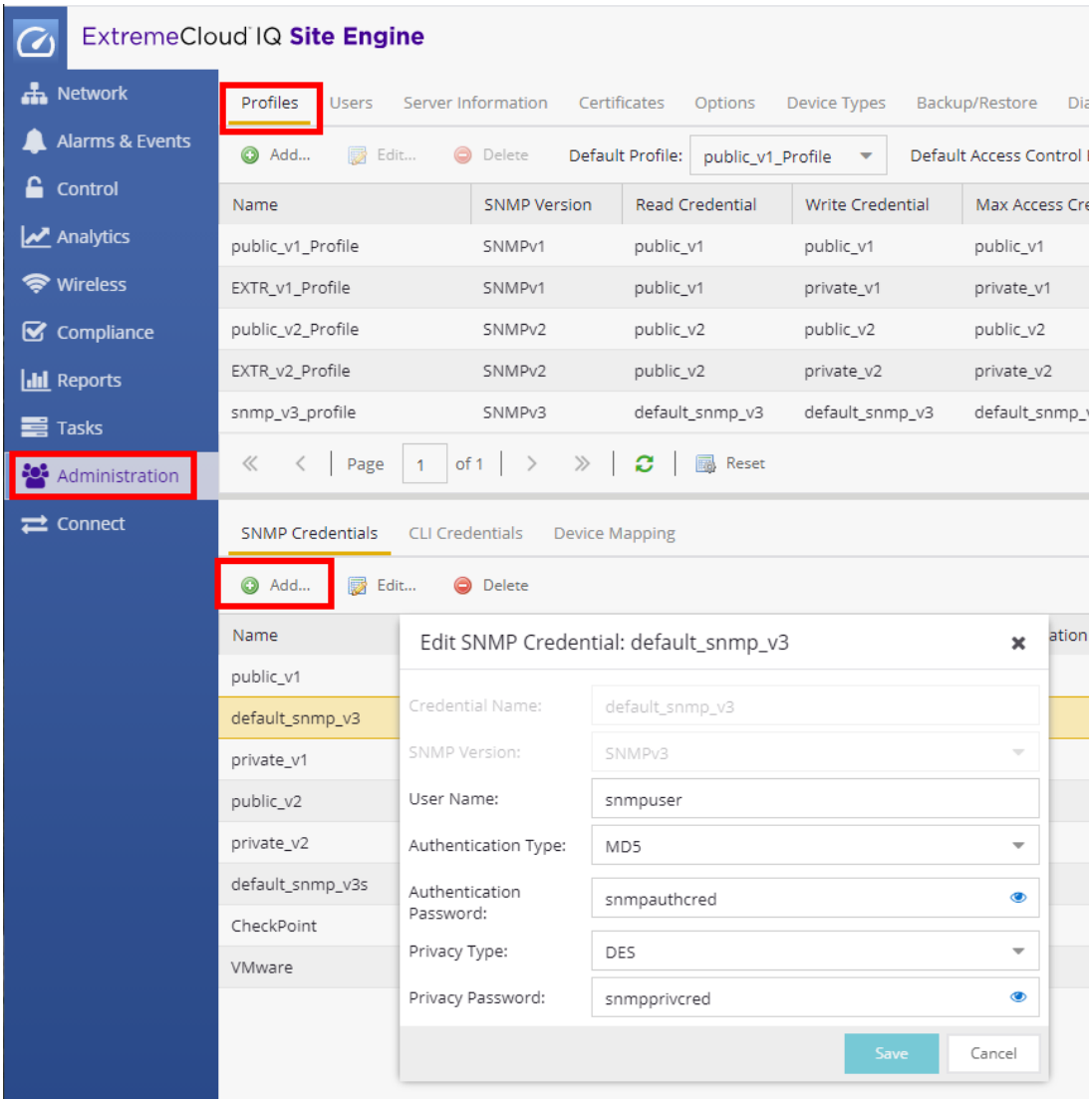
Part 2: Configuring ExtremeControl

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

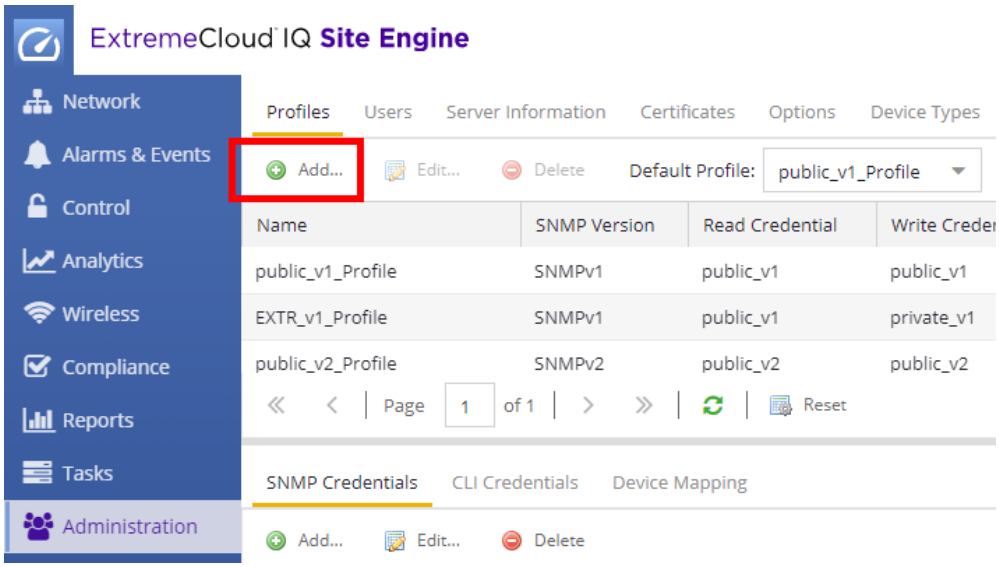
> **Note**
>
> This section assumes that the Access Control Engine is already configured and added to ExtremeControl and that Guest Registration is already enabled.

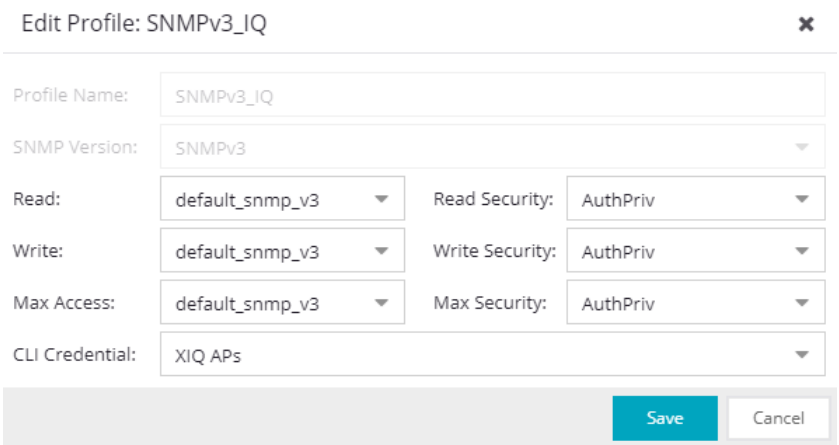
Step 1 – Create an SNMP Profile for Access Points

In ExtremeCloud IQ - Site Engine, select the Profiles tab under **Administration** and select **Add** 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.



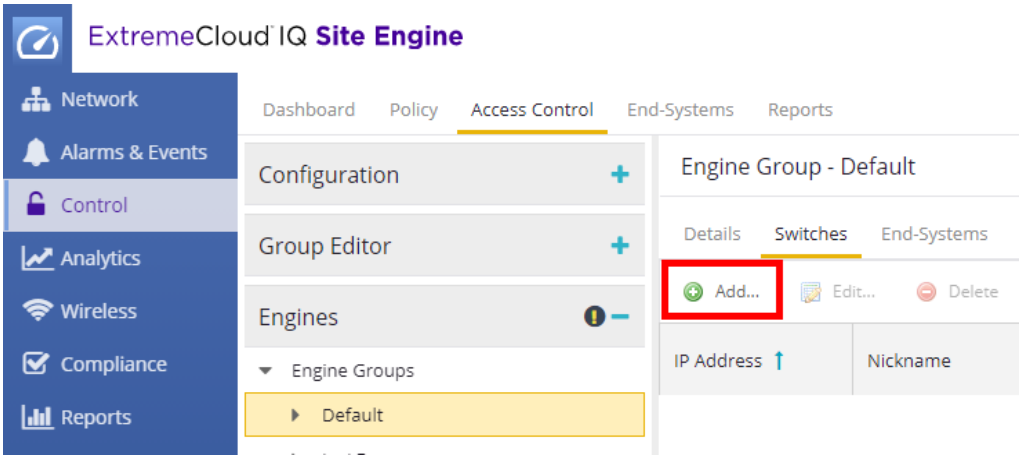
With the SNMP Credentials configured, create a **Profile** to assign to the access points. Ensure that the SNMP settings are configured for **AuthPriv** for the SNMP Read.



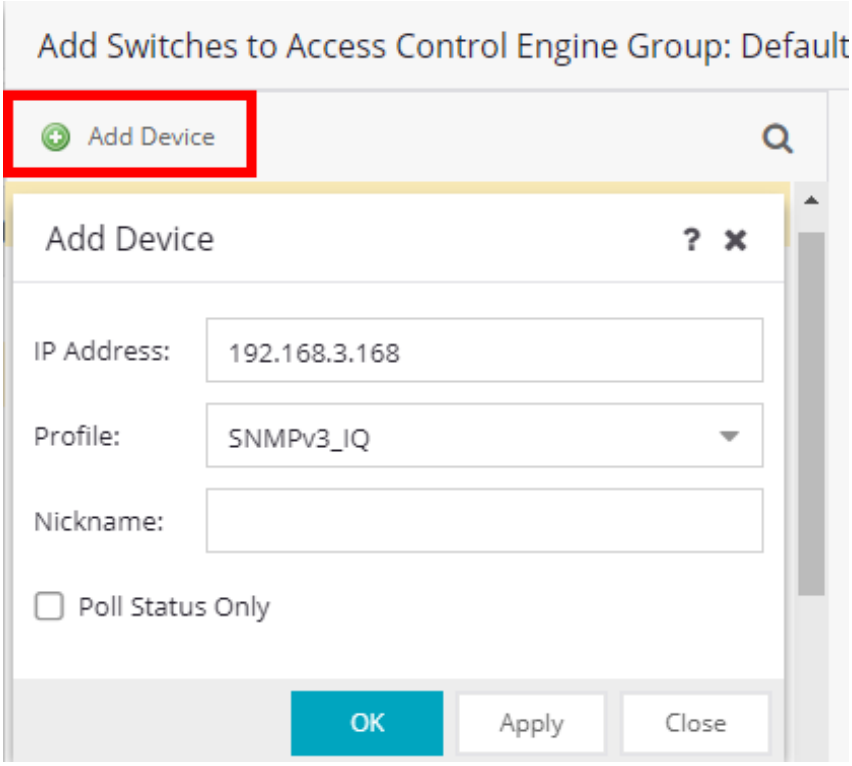


Step 2 – Add the Access Point to ExtremeControl

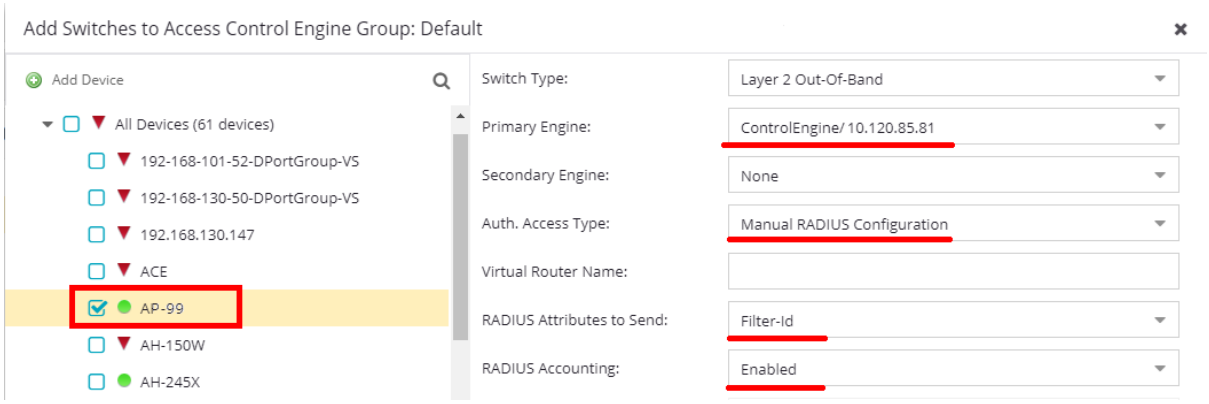
In **Control**, select the Access Control tab, followed by the **Default** Access Control Engine Group. In the group configuration, select the Switches tab and then select **Add...**.



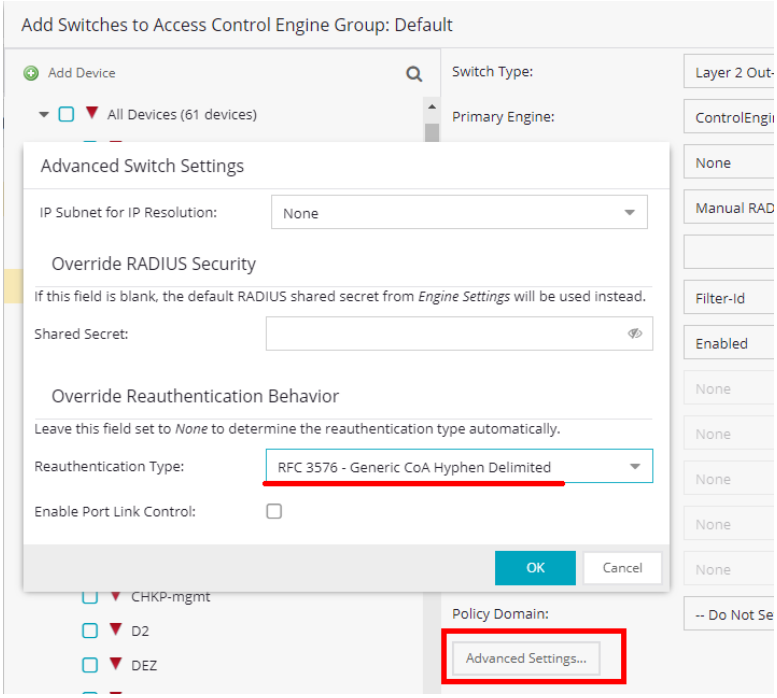
In the **Add Switches** dialog, if the access point has not been added to ExtremeCloud IQ - Site Engine, select **Add Device** to add the IP address of the access point and the SNMP Profile to use for communication.



After the access point is added to ExtremeCloud IQ - Site Engine, 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**.



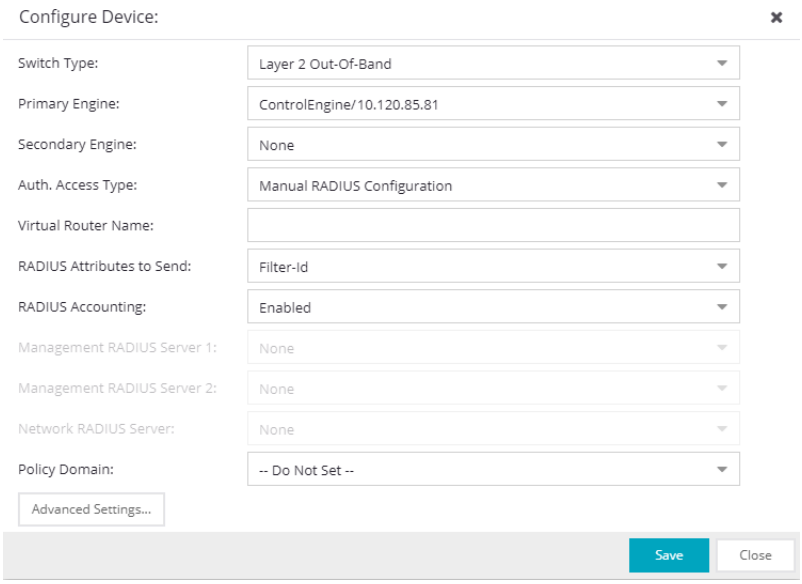
Before saving the configuration, select **Advanced Settings** and set the **Reauthentication Type** to **RFC 3576 - Generic CoA Hyphen Delimited** as shown below. (This step is not necessary in ExtremeCloud IQ - Site Engine 21.11 and later.) If the RADIUS Shared Secret was set to a value other than the default ETS_TAG_SHARED_SECRET, set the value to match what was configured in ExtremeCloud IQ.



Note

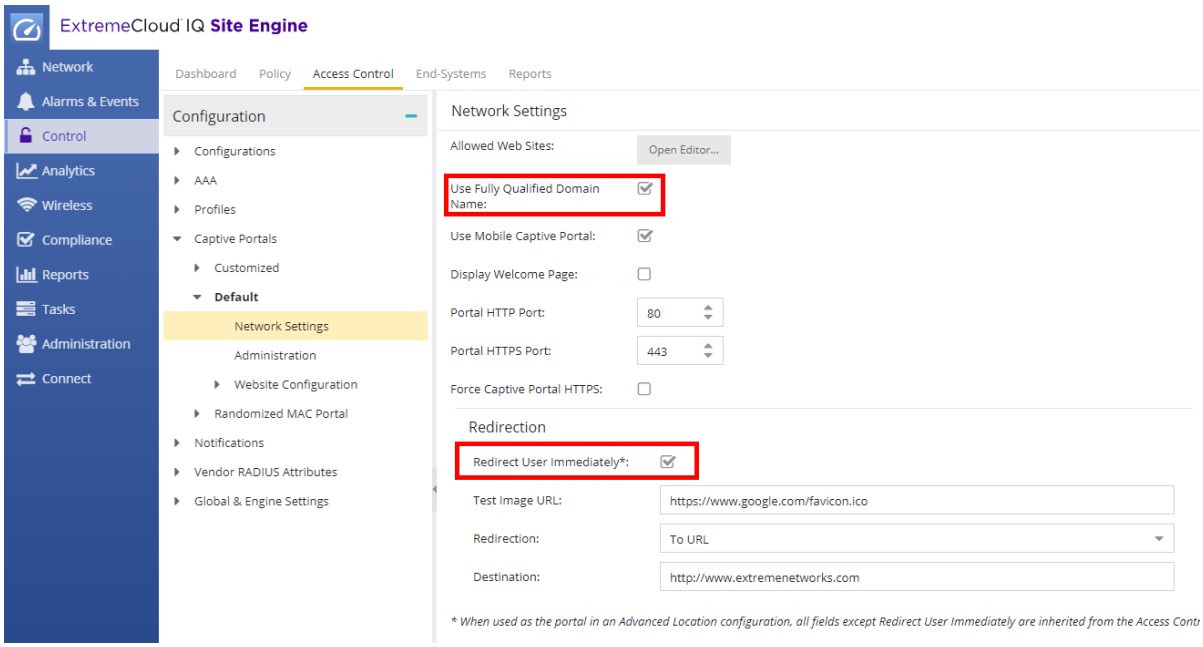
In ExtremeCloud IQ – Site Engine version 21.4 the reauthentication method needs to be set manually on a per-device basis, or a mapping to the SysObject ID can be created. See Appendix A for reference.

The final settings should look similar to the following image. When complete, select **Save**.

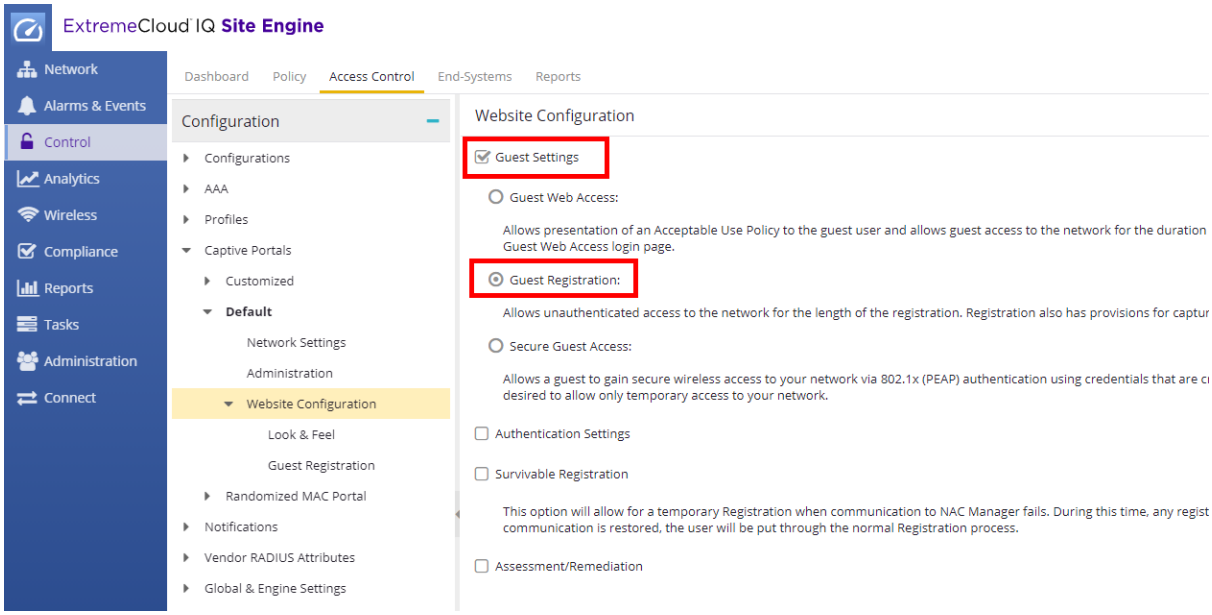


Step 3 – Configure Captive Portal Settings

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.**



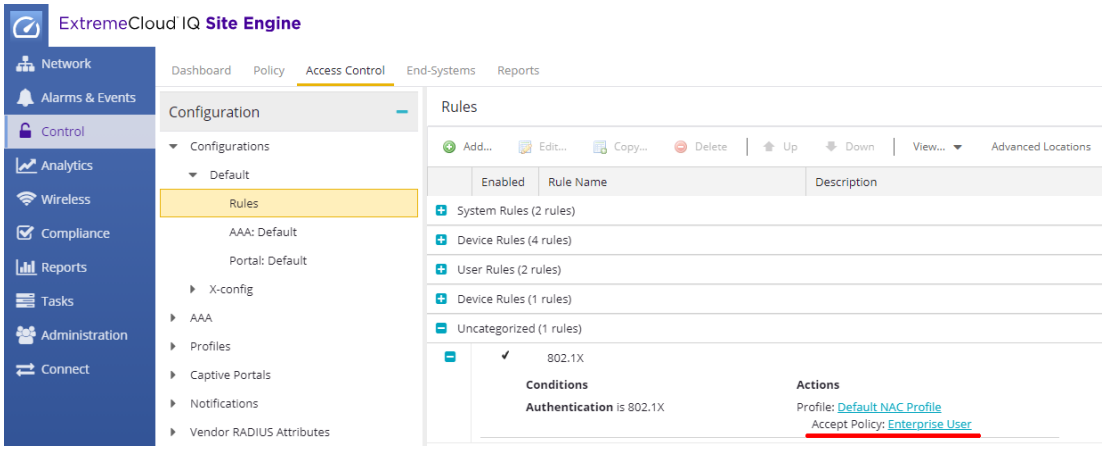
Verify that Guest Registration is also enabled by selecting **Website Configuration**.



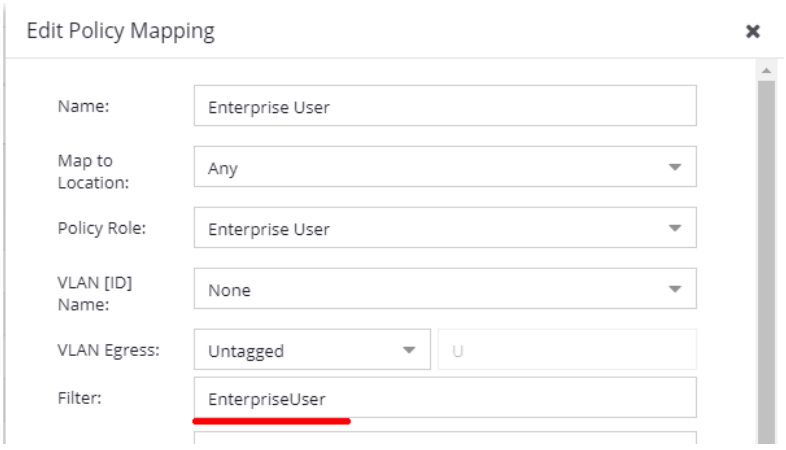
Step 4 – Configure Rules, Roles, and Policy Mappings

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 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.



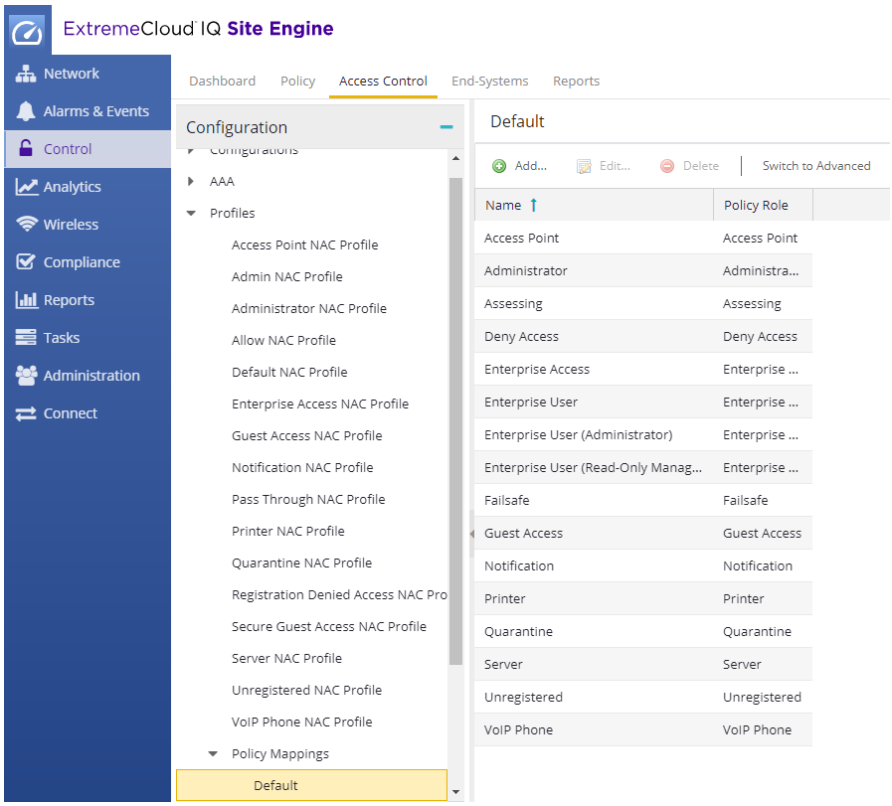
In the **Edit Policy Mapping** window, the **Filter** should be adjusted to match the Filter-ID that was configured in the Assignment Rules in ExtremeCloud IQ.



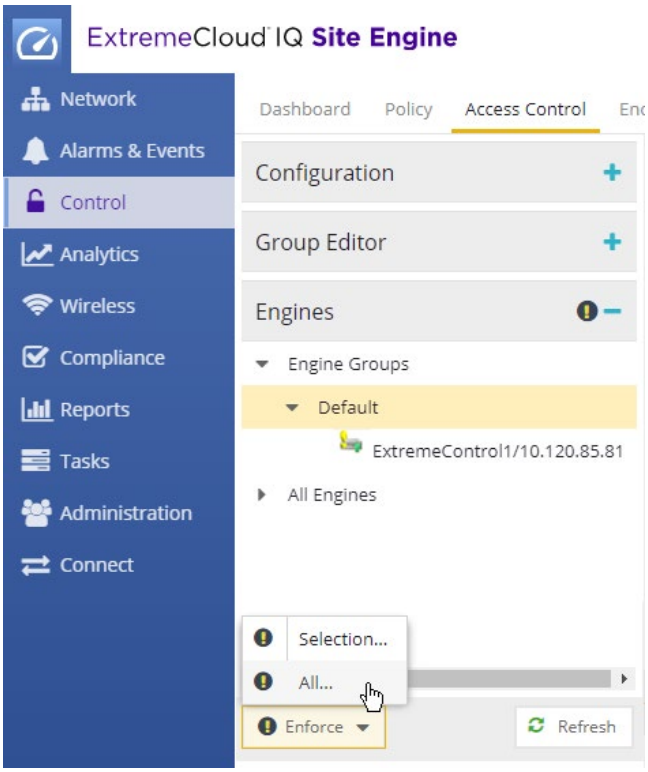
Note

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 that 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 D for steps to format the attribute values at runtime rather than individually.

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



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



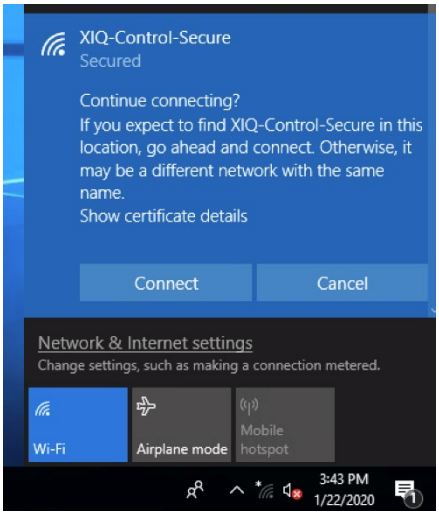
Part 3: Validation

Two validation steps 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.

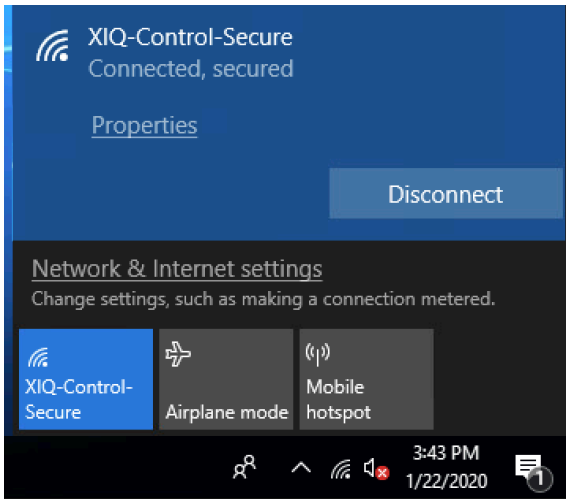
Secure SSID Validation

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.

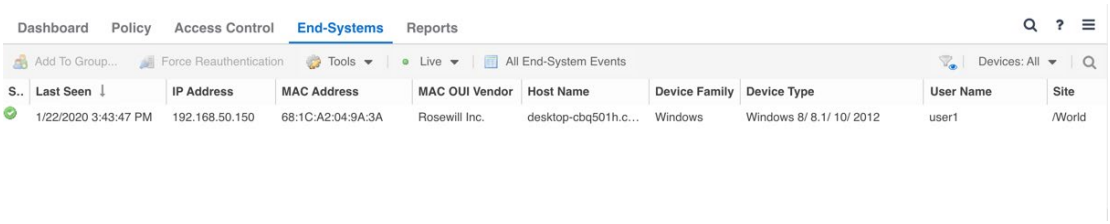
When prompted for a username and password, enter valid credentials. If prompted, also trust or ignore any certificate warnings.



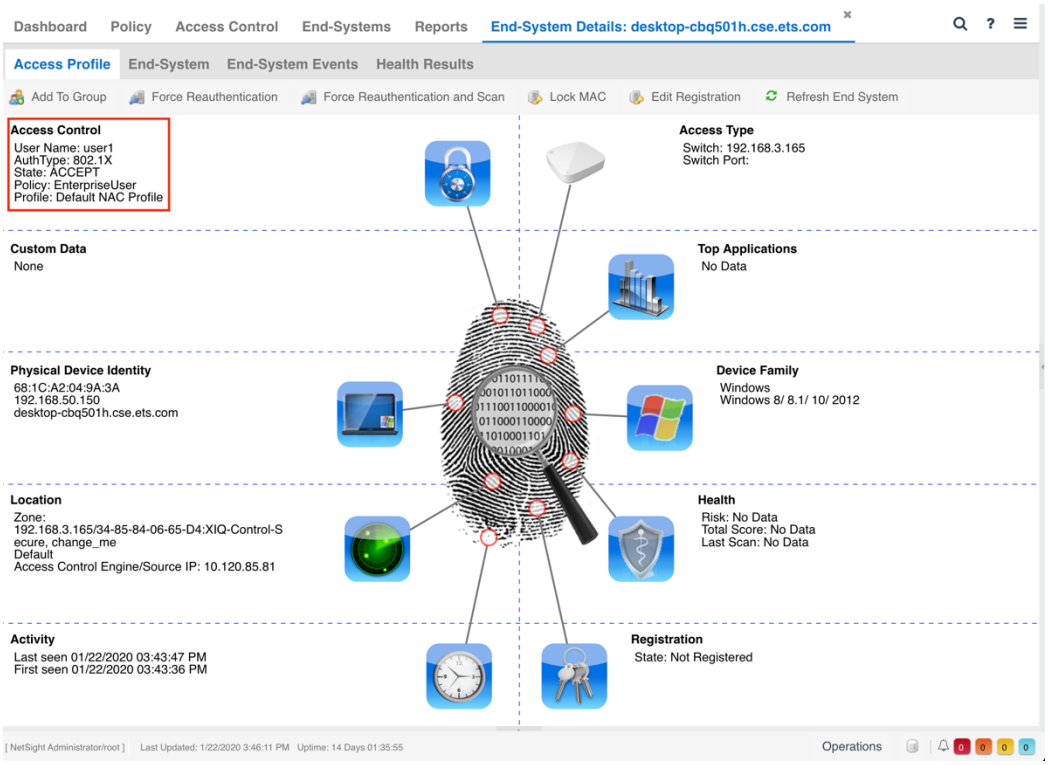
When connected, validate that traffic can be passed as expected.



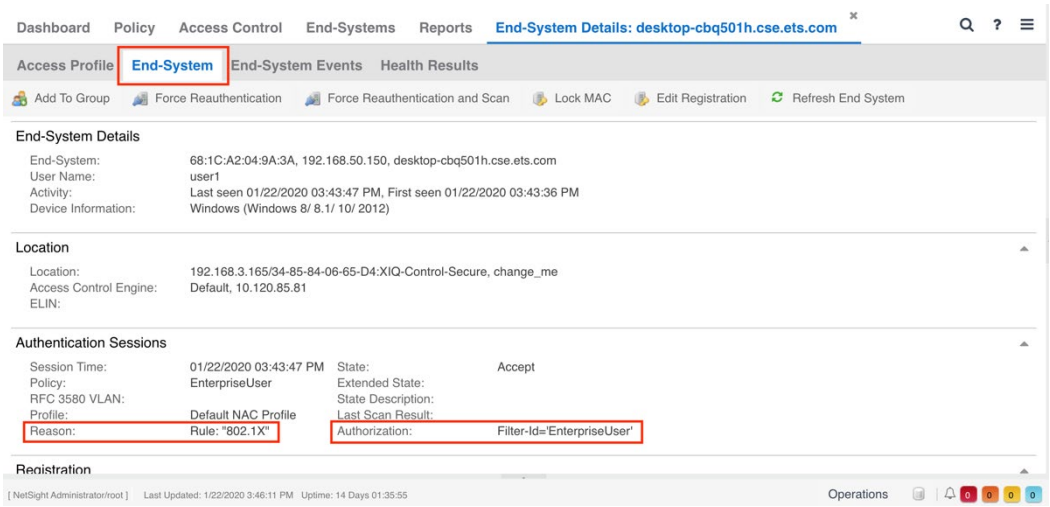
In ExtremeControl, navigate to the End-Systems tab and validate that all of the information is properly populated for the newly connected client.



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.

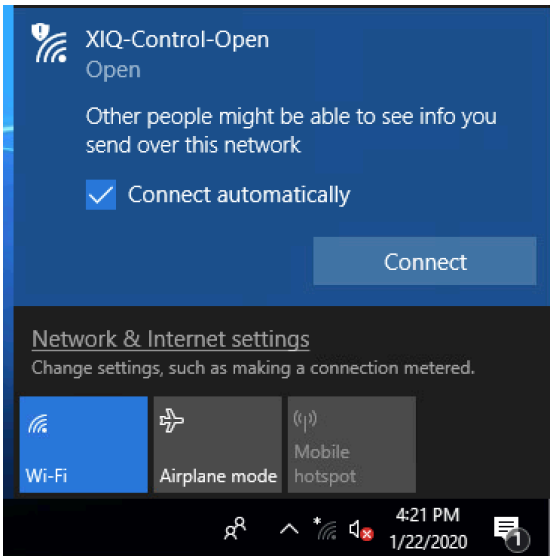


In ExtremeCloud IQ, select Clients under the Manage tab and note the username of the client, the SSID, and the assigned User Profile.

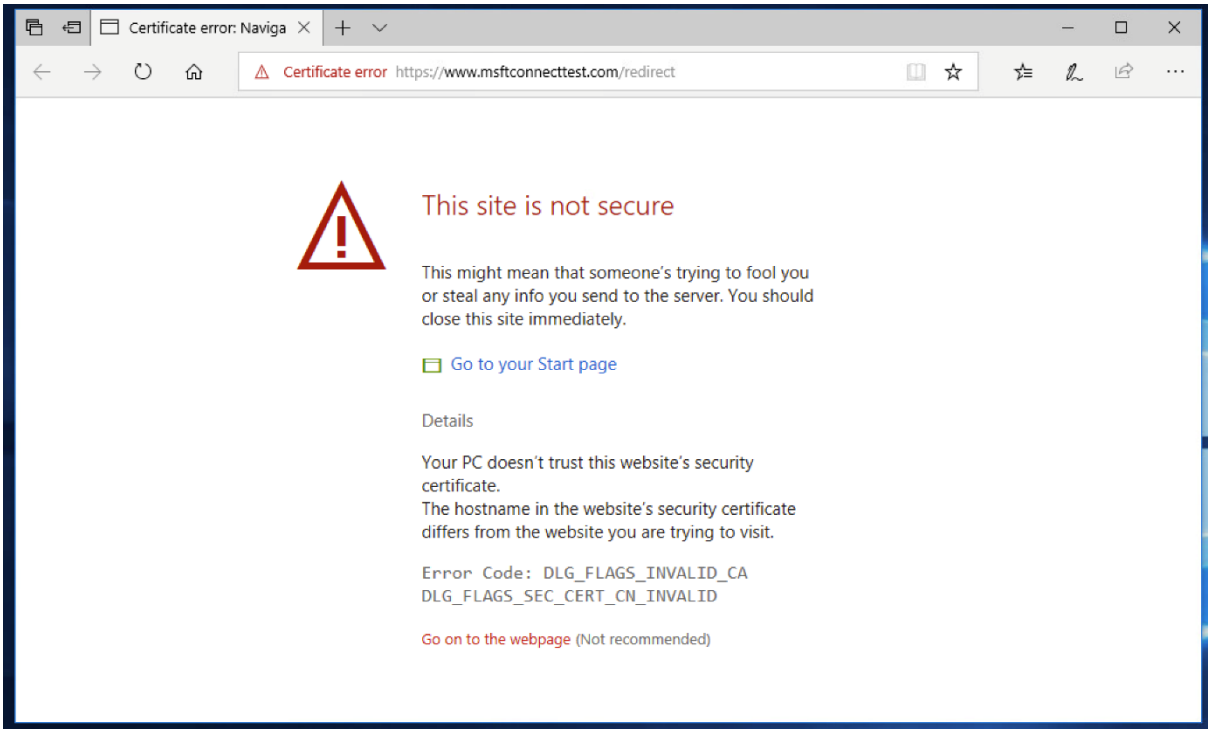
Guest SSID Validation

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

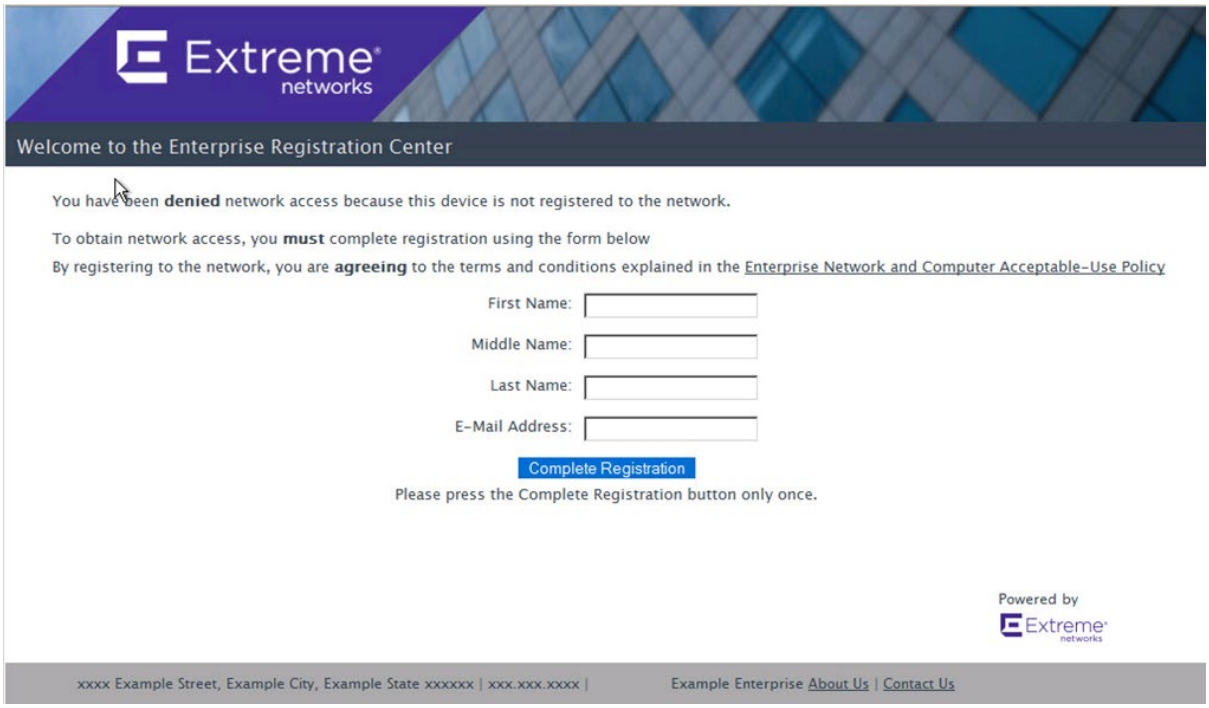
Select the open SSID from the available SSID list.



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

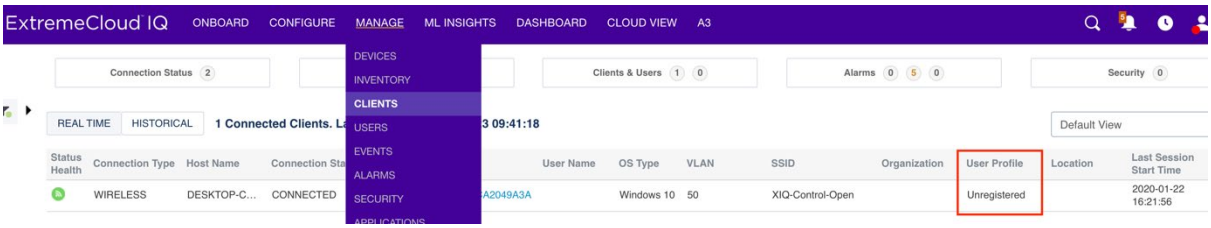


The web traffic for the client is redirected to the captive portal hosted by the Access Control Engine.

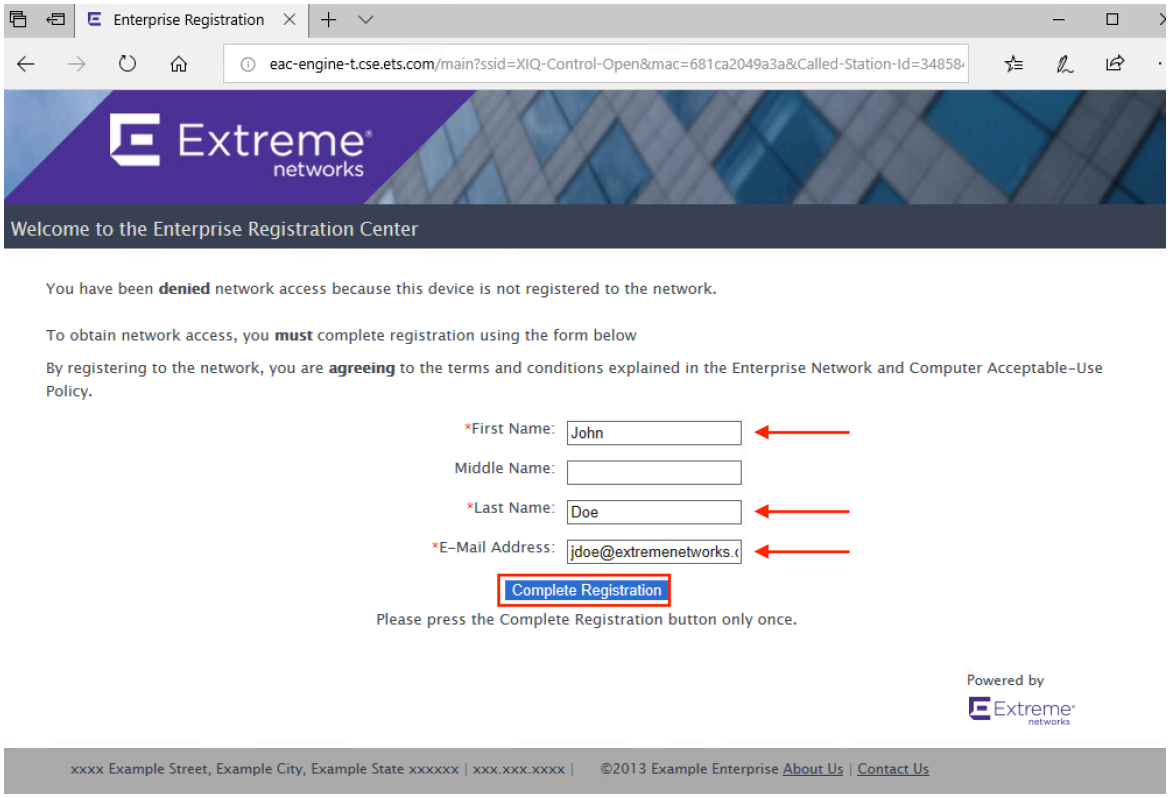


At this point, ExtremeControl assigns the **Unregistered NAC Profile** and returns the Filter-ID of **Unregistered**. This can be verified in the End-Systems tab in ExtremeControl.

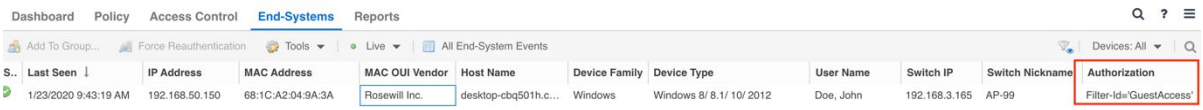
In ExtremeCloud IQ, the User Profile assigned to the client is also shown as **Unregistered**.



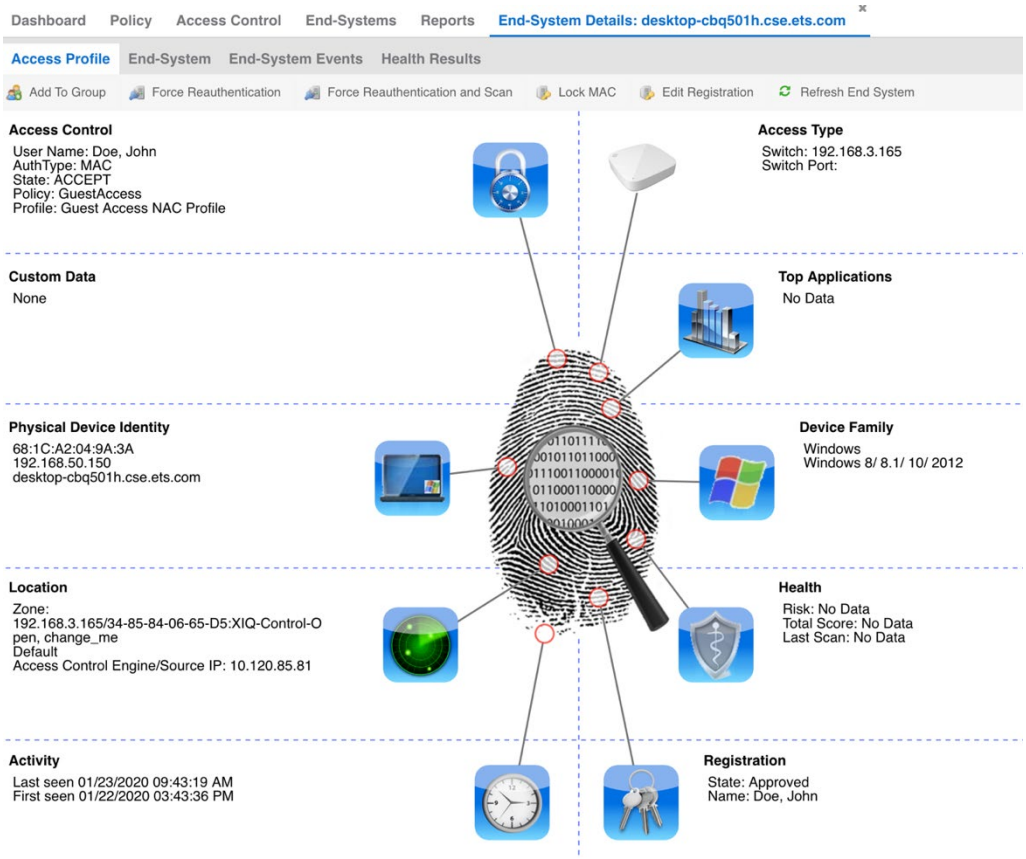
On the web page on the client, fill out the fields and select **Complete Registration** to submit the registration to ExtremeControl.



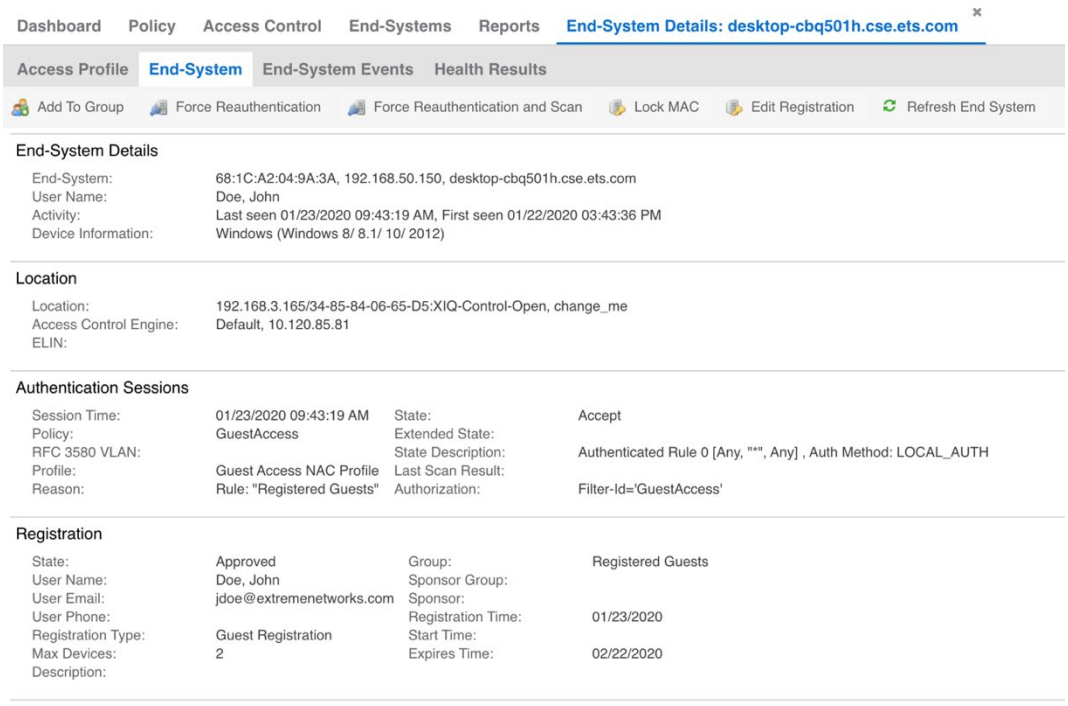
A Change of Authorization (CoA) is sent with a new Filter-ID based on the rules engine configuration. Depending on the configuration of the Captive Portal, the client's web traffic is redirected to a success page after the User Profile is changed. Looking at the **End-Systems** table in ExtremeControl,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



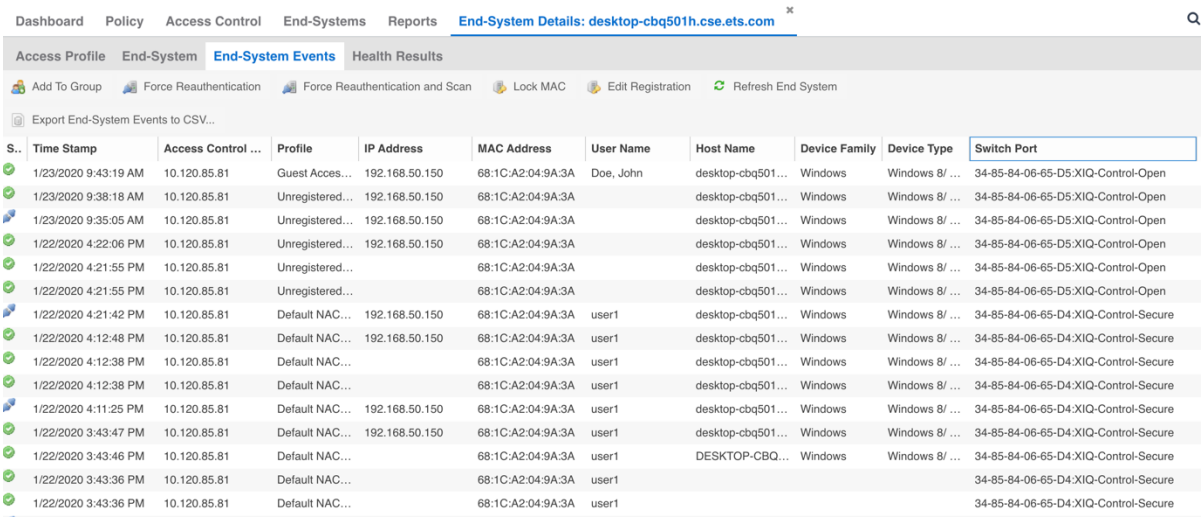
The End System Details for the client are populated with the additional information that was entered in the captive portal.



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



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

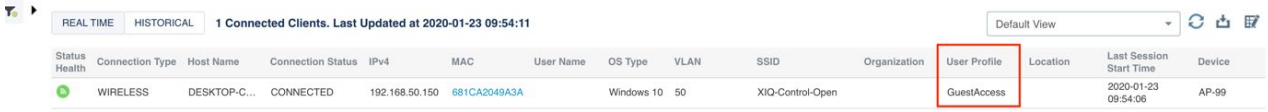


S..	Time Stamp	Access Control ...	Profile	IP Address	MAC Address	User Name	Host Name	Device Family	Device Type	Switch Port
	1/23/2020 9:43:19 AM	10.120.85.81	Guest Acces...	192.168.50.150	68:1C:A2:04:9A:3A	Doe, John	desktop-cbq501...	Windows	Windows 8/ ...	34-85-84-06-65-D5:XIQ-Control-Open
	1/23/2020 9:38:18 AM	10.120.85.81	Unregistered...	192.168.50.150	68:1C:A2:04:9A:3A		desktop-cbq501...	Windows	Windows 8/ ...	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 8/ ...	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 8/ ...	34-85-84-06-65-D5:XIQ-Control-Open
	1/22/2020 4:21:55 PM	10.120.85.81	Unregistered...		68:1C:A2:04:9A:3A		desktop-cbq501...	Windows	Windows 8/ ...	34-85-84-06-65-D5:XIQ-Control-Open
	1/22/2020 4:21:55 PM	10.120.85.81	Unregistered...		68:1C:A2:04:9A:3A		desktop-cbq501...	Windows	Windows 8/ ...	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 8/ ...	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 8/ ...	34-85-84-06-65-D4:XIQ-Control-Secure
	1/22/2020 4:12:38 PM	10.120.85.81	Default NAC...		68:1C:A2:04:9A:3A	user1	desktop-cbq501...	Windows	Windows 8/ ...	34-85-84-06-65-D4:XIQ-Control-Secure
	1/22/2020 4:12:38 PM	10.120.85.81	Default NAC...		68:1C:A2:04:9A:3A	user1	desktop-cbq501...	Windows	Windows 8/ ...	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 8/ ...	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 8/ ...	34-85-84-06-65-D4:XIQ-Control-Secure
	1/22/2020 3:43:46 PM	10.120.85.81	Default NAC...		68:1C:A2:04:9A:3A	user1	DESKTOP-CBQ...	Windows	Windows 8/ ...	34-85-84-06-65-D4:XIQ-Control-Secure
	1/22/2020 3:43:36 PM	10.120.85.81	Default NAC...		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...		68:1C:A2:04:9A:3A	user1				34-85-84-06-65-D4:XIQ-Control-Secure

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

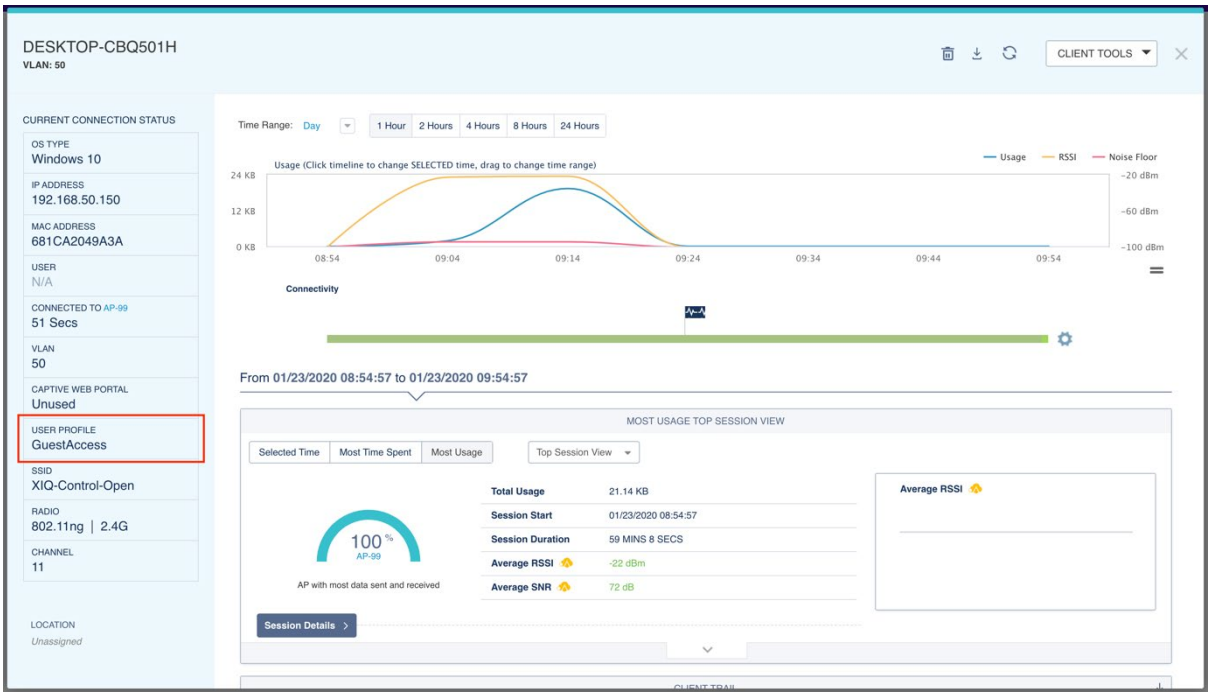
```
AP-99#show station
Chan=channel number; Pow=Power in dBm;
A-Mode=Authentication mode; Cipher=Encryption mode;
A-Time=Associated time; Auth=Authenticated;
UPID=User profile Identifier; Phymode=Physical mode;

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
AP-99#
```

Navigating to ExtremeCloud IQ, when the client is reauthenticated, 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

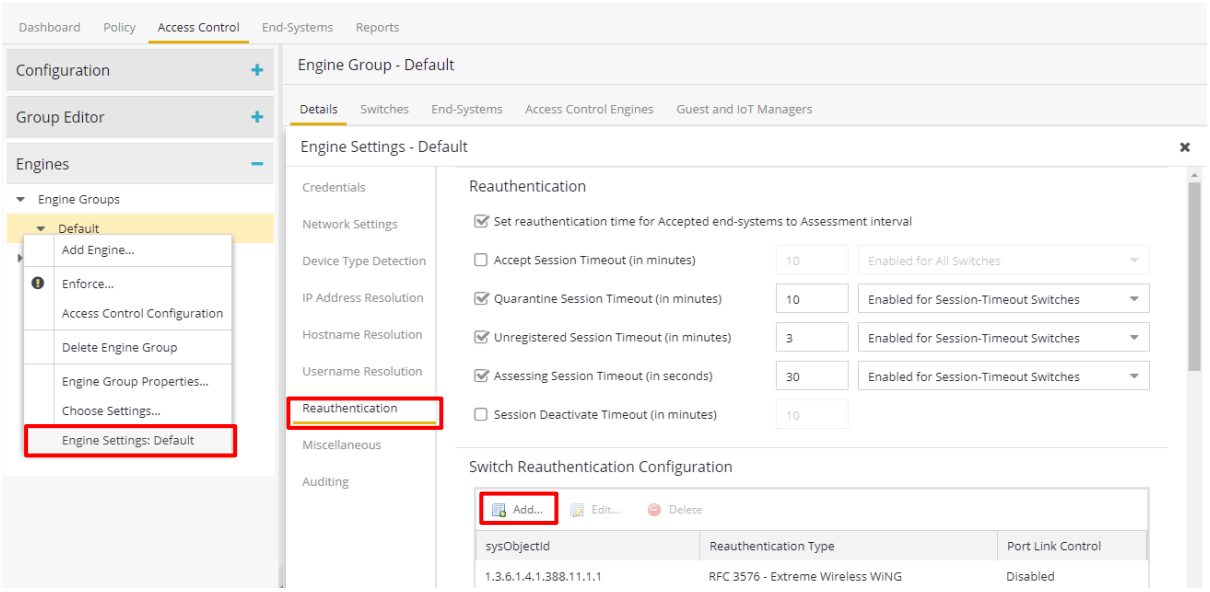
The information is also available when client details are displayed.



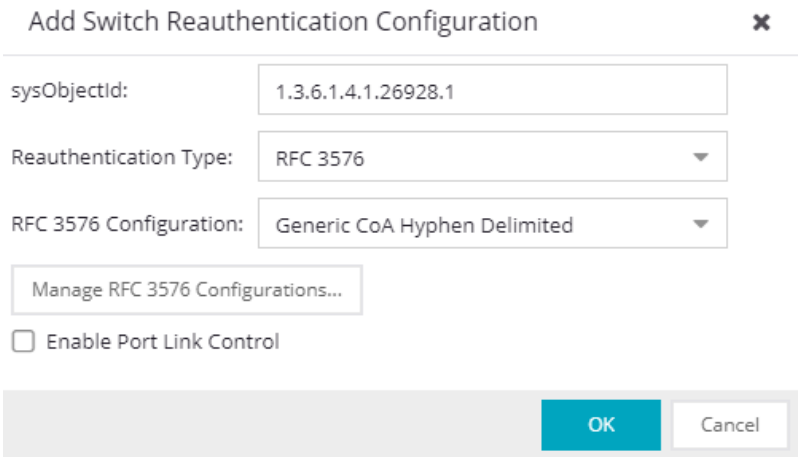
Appendix A: Creating RFC 3576 Configurations

This step is not needed in ExtremeCloud IQ - Site Engine version 21.11 and later.

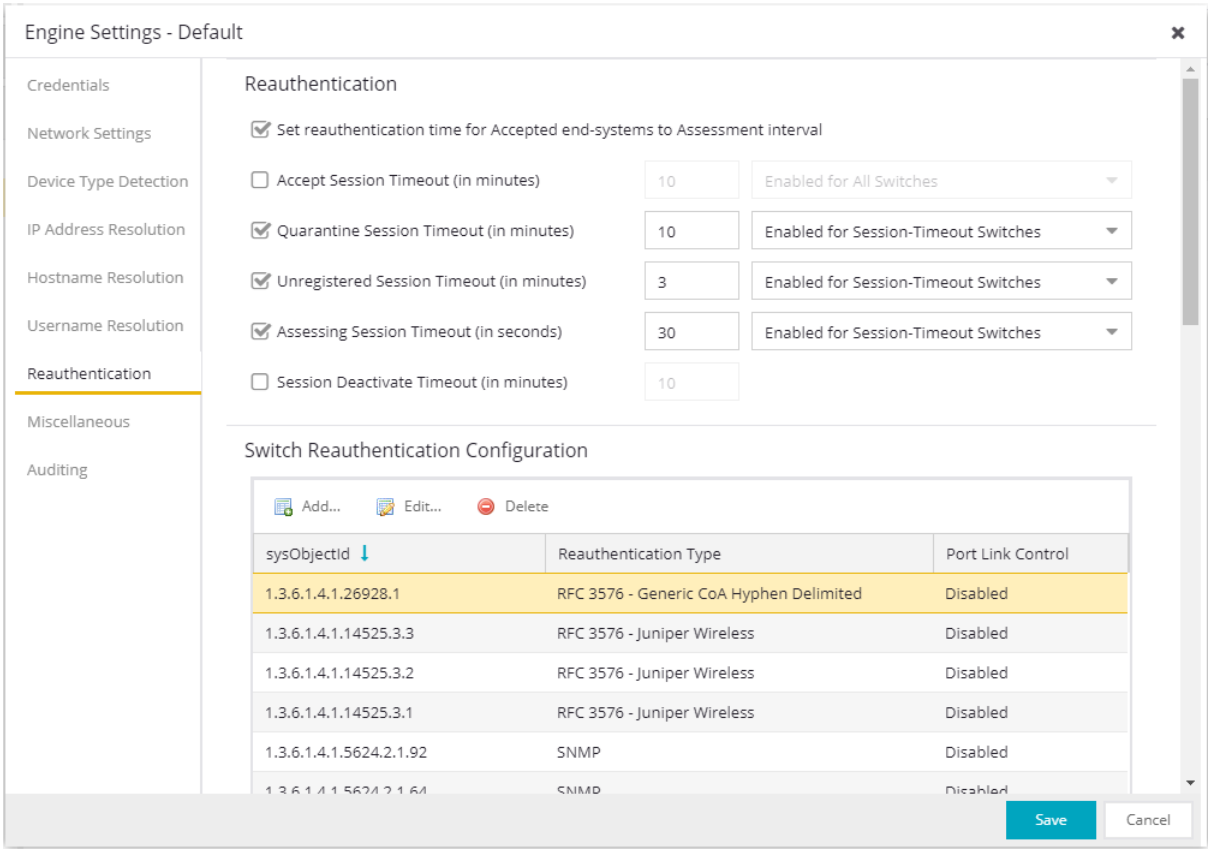
Instead of configuring the Reauthentication Type for each access point as it is added to ExtremeControl, the Reauthentication type can be set based on the SNMP SysObject ID for the AP. This is a more scalable approach when adding multiple access points. To add the entry, right click on the **Default**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



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

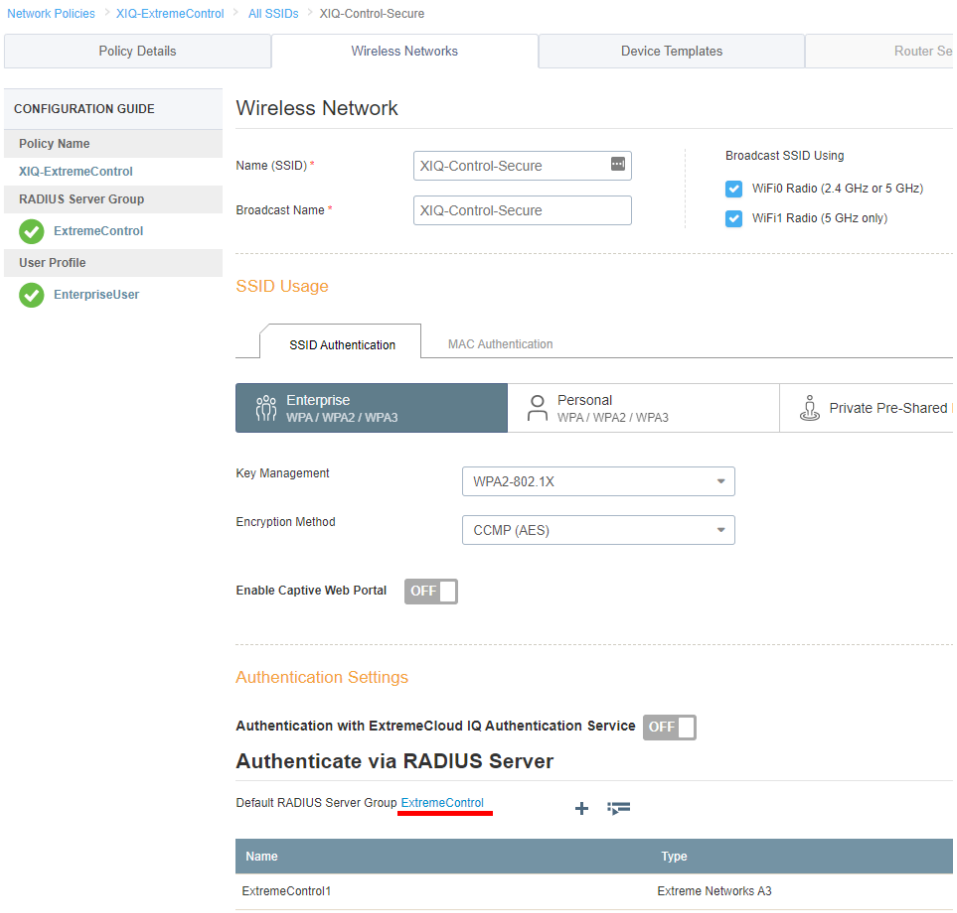


When complete, the configuration should look similar to this.

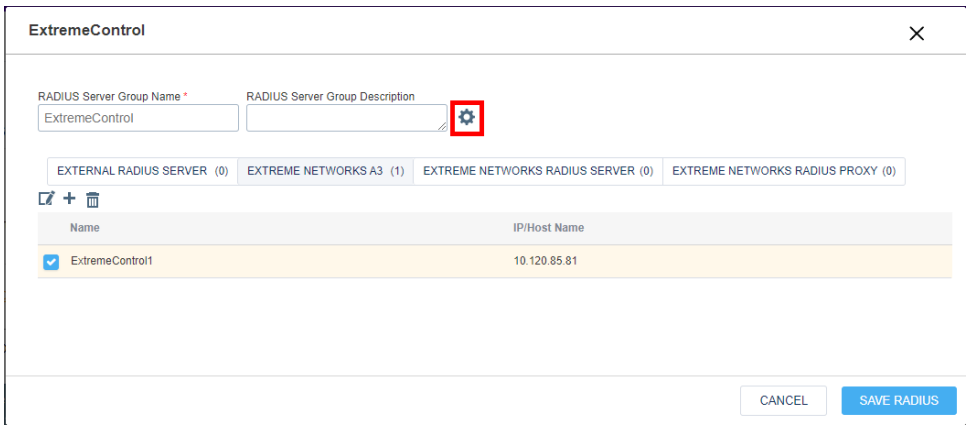


Appendix B: Enable RFC 3576 Reauthentication on ExtremeCloud IQ

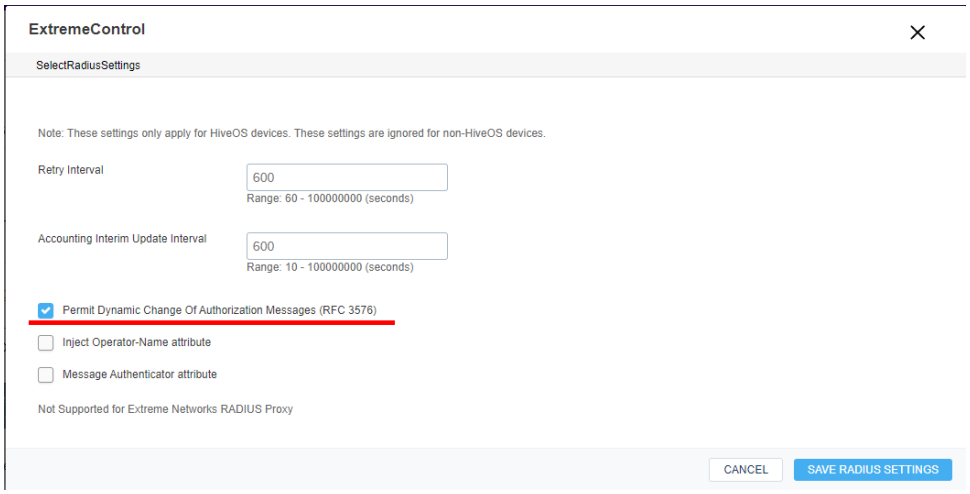
By default, if the RADIUS Server was added as an Extreme Networks A3 server, RFC 3576 is already enabled. However, if it was added as an External RADIUS Server, then it will need to be enabled manually. To do this, edit the **Network Policy** in the **Configure** menu, choose the SSID in **Wireless Networks**,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



Select the gear icon as shown below for advanced settings.

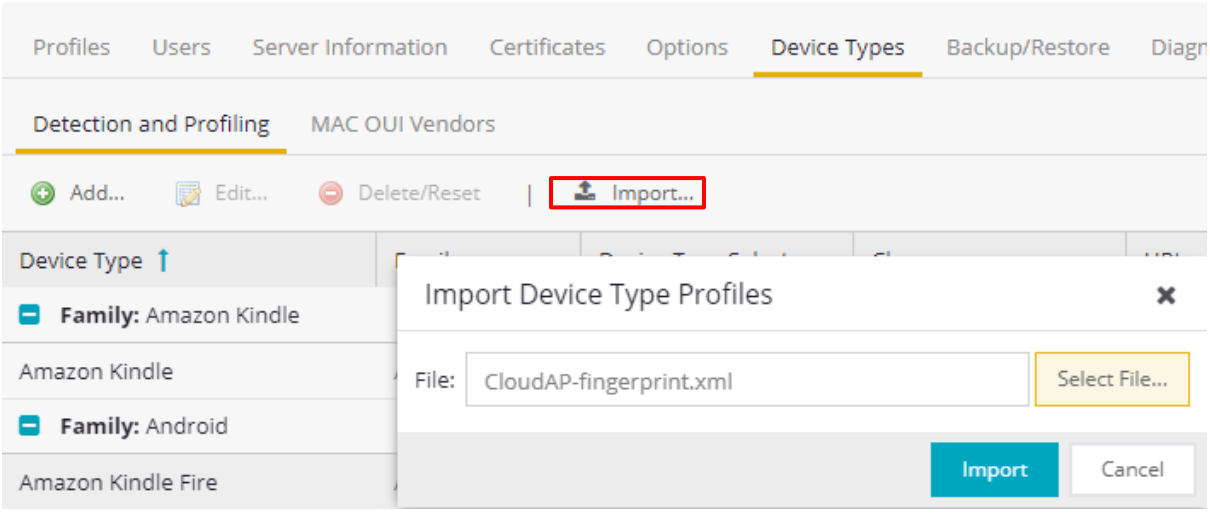


Select the check box labeled **Permit Dynamic Change Of Authorization Messages (RFC 3576)**.



Appendix C: DHCP Fingerprint for ExtremeCloud IQ Access Points

For the ExtremeCloud IQ access point to be recognized as an appropriate device type in the **End-Systems** table, a DHCP fingerprint needs to be added. Select **Administration** in the main menu and **Device Types** in the top menu. Then select **Detection and Profiling** and select **Import**.



The following content should be imported through the file with XML extension:

```
<!-- 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"
dhcpoption55="1,3,6,7,12,15,28,40,41,42,43"/>
            <test weight="5" matchtype="exact" dhcptype="Discover"
dhcpoption55="1,3,6,7,12,15,28,40,41,42,43"/>
        </tests>
    </fingerprint>
</fingerprints>
</DHCP>
```

Appendix D: RADIUS Reponse Formatting

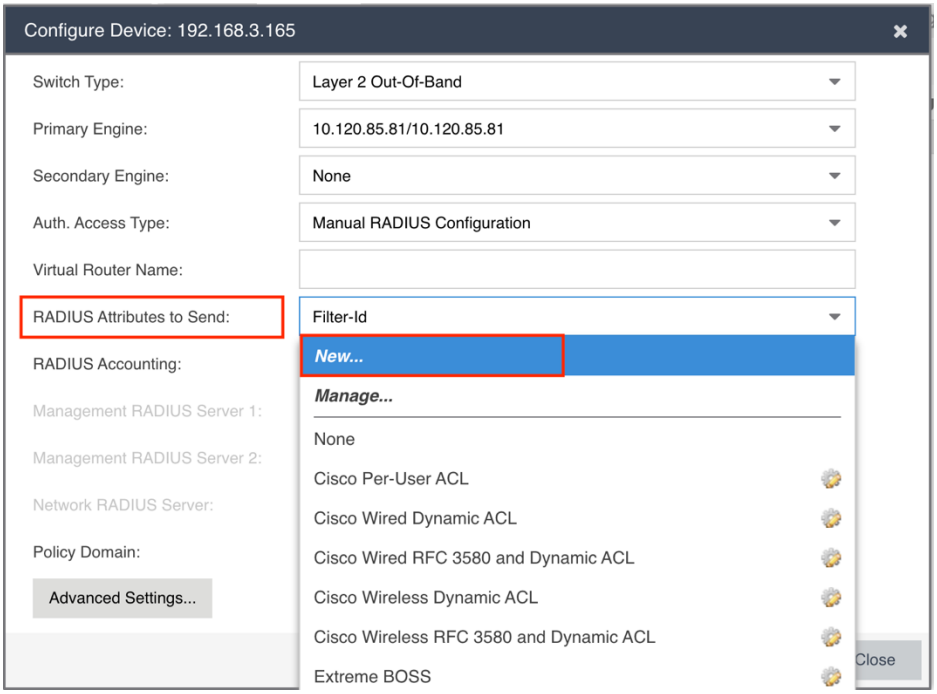
As of version 8.3, ExtremeControl can format RADIUS Attributes at runtime. This means that rather than modifying the Policy Mappings for each Accept policy to remove spaces, the RADIUS Attribute configuration can be modified to modify the response at run time.

The available modifications are:

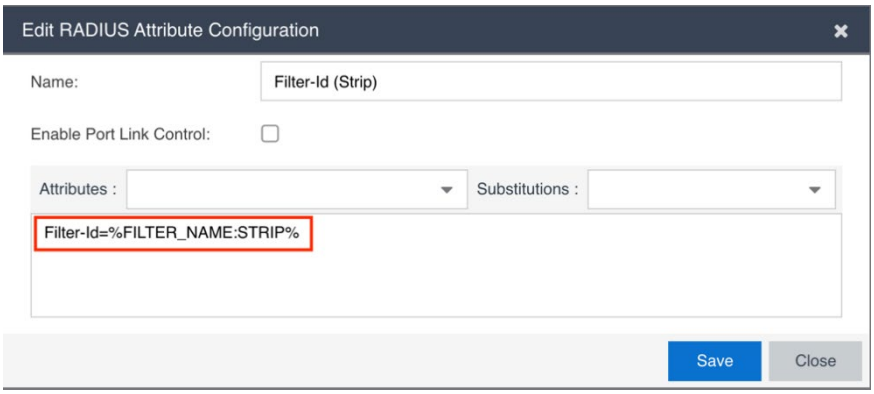
- UPPER – Changes the response variable to all uppercase.
  For example: Guest Access becomes GUEST ACCESS.
- LOWER – Changes the response variable to all lowercase.
  For example: Guest Access becomes guest access.
- STRIP – Removes all whitespace from the variable including spaces.
  For example: Guest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

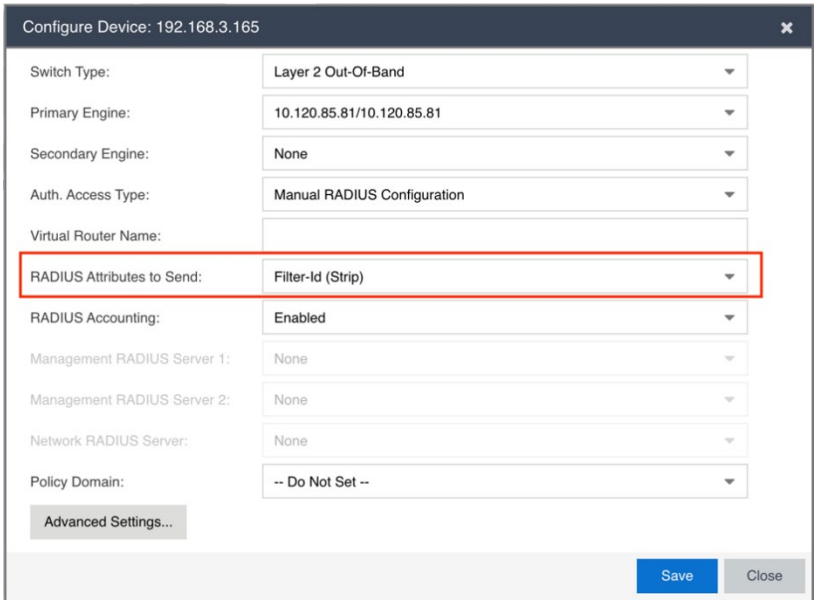
The configuration is adjusted when assigning the RADIUS Configuration in the Add Switch dialog. In the RADIUS Attributes to Send drop-down menu, select New.



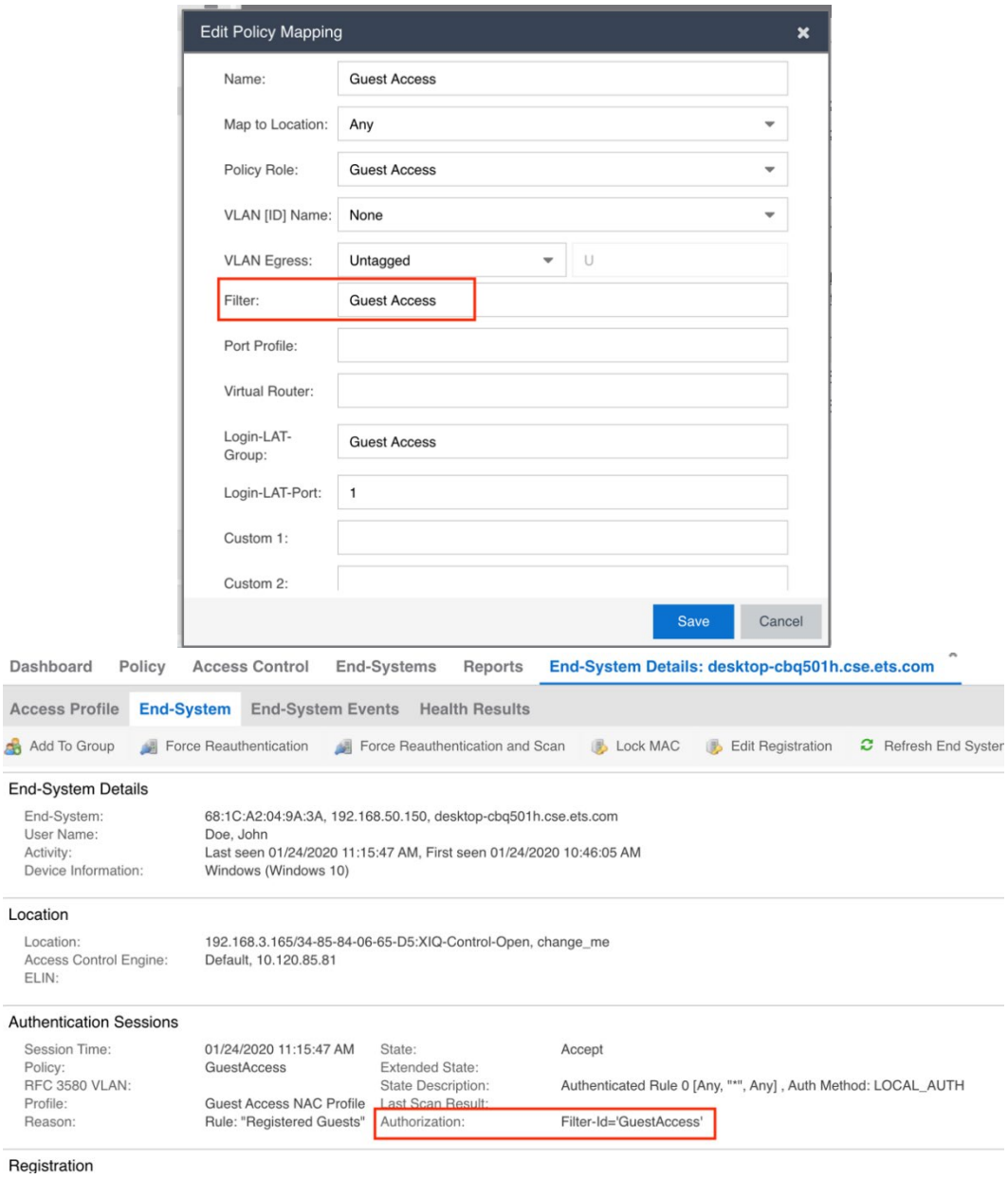
In the new window, keep the same variable, however add :STRIP to the end to remove whitespace.



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



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



Appendix E: ExtremeCloud IQ - Site Engine Licensing Note

Each RADIUS Client (the source of the RADIUS request, or the NAS) must be added to the ExtremeCloud IQ - Site Engine database. The number of added devices contributes to the total cost of ownership. Because ExtremeCloud IQ APs are expected to be managed through ExtremeCloud IQ, they will not consume any additional licenses (a license is tied to a serial number). However, any non-ExtremeCloud IQ native device will consume a Pilot or Navigator license if managed with SNMP. The exception to this is when Poll Status Only is selected. In this case, no license will be consumed by ExtremeCloud IQ - Site Engine for this device.