



How To: ExtremeCloud IQ - Controller Integration with ExtremeCloud IQ – Site Engine and External Guest Captive Portal with ExtremeControl

Abstract: This document covers integration of ExtremeCloud IQ - Controller with ExtremeControl for guest captive portal. 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: November 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

©2022 Extreme Networks, Inc. All rights reserved.

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

Contents

Pre-requisites and Limitations	4
Overview	5
Part 1: XIQ-C Initial Configuration	6
SNMP and NTP Configuration	6
Part 2: Site Engine Configuration	8
SNMP Profile Configuration	8
Add XIQ-C to Site Engine	10
Enable XIQ-C Statistics Collection	11
Part 3: Policy Manager Configuration	13
Adding XIQ-C to Policy Manager	13
VLAN Creation	15
VLANs for Guest Traffic	15
Role Creation	17
Part 4: XIQ-C Configuration	21
AAA Policy Configuration	21
Guest SSID Configuration	23
XIQ-C Internal Unregistered role for Guest Networks	24
Verifying VLANs and Roles on XIQ-C	25
AP Profile: SSID, VLANs and Roles Mapping	27
Part 5 – ExtremeControl Configuration	30
Adding XIQ-C to ExtremeControl	30
Captive Portal Authentication Configuration	32
MAC Authentication	32
Location Group Configuration	33
Policy Mapping Configuration	34
Captive Portal Configuration	35
Guest Registration Settings	37
Authenticated Registration (BYOD) Settings	39
Guest Access Authentication Rules	39
LDAP Configuration	41
Active Directory Integration	41
AAA Rules	43
Part 6: Configuration Validation	44
Authenticated Registration (BYOD)	44
Guest Registration	45

Wireless Management Statistics	47
Revision History	51

Pre-requisites and Limitations

The scope of this document is intended for SEs and partners that are familiar with ExtremeCloud IQ – Controller, ExtremeCloud IQ - Site Engine and ExtremeControl. Only the primary touchpoints between these products are covered in this document. All other settings are considered out of scope. It is also assumed that the ExtremeCloud IQ - Controller already has Sites and Device Groups configured and that APs are adopted and assigned to the correct Device Groups.

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

- ExtremeCloud IQ – Site Engine (Site Engine) 22.6.12.13
- ExtremeControl 22.6.12.13
- ExtremeCloud IQ - Controller Build Version 10.02.01.0029 with AP Firmware 10.1.0.0-036R

For the sake of brevity, the product names are described with the following terms throughout this document.

- ExtremeCloud IQ - Controller = XIQ-C
- ExtremeCloud IQ - Site Engine = Site Engine
- ExtremeControl = ExtremeControl

Overview

This document is divided into six major parts, the summary of each section is as follows:

- Part 1 - This section deals with configuring the basic settings on XIQ-C to allow it to communicate with the Site Engine.
- Part 2 - The second section describes the configuration process of integrating XIQ-C with the Site Engine.
- Part 3 - This section covers the XIQ-C and Policy Manager integration configuration.
- Part 4 - This section goes over the configuration required on the XIQ-C to authenticate WLAN users against ExtremeControl.
- Part 5 - This section outlines the configuration of ExtremeControl to recognize requests from the wireless network and respond in a format that can be properly interpreted by the controller.
- Part 6 - Lastly, this section validates the configuration of the entire solution.

A brief summary of the interactions between the XIQ-C and ExtremeControl can be broken down into the following steps:

1. As the device connects to the wireless SSID, MAC-based authentication occurs.
2. The XIQ-C sends a RADIUS request destined to ExtremeControl for authentication.
3. The ExtremeControl authenticates and authorizes the RADIUS request per its configuration. It passes back a RADIUS Accept message with attributes that the XIQ-C can interpret such as Filter-ID.
4. The XIQ-C matches the attributes to a policy role.
5. If the policy role 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 XIQ-C to change the policy role assigned to the device.

Note

In addition to the steps created in this guide, it is also recommended to configure 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: XIQ-C Initial Configuration

The first step is to configure the XIQ-C with the following settings:

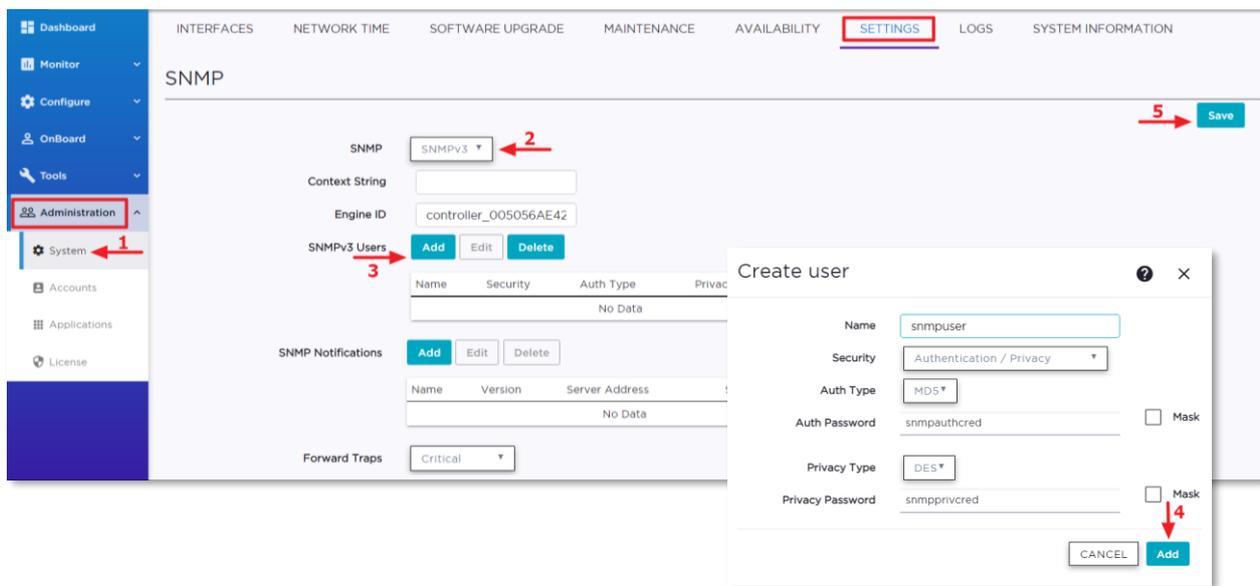
- SNMP
- NTP

Upon completion of these configurations steps, XIQ-C will be ready to communicate with Site Engine.

SNMP and NTP Configuration

For the XIQ-C to communicate with Site Engine and ExtremeControl, SNMP must be configured. Ideally, SNMPv3 is used due to its security and efficiency compared to SNMPv1 or SNMPv2.

To enable SNMP on XIQ-C, navigate to **Administration** tab, select **System** and then under the **Settings** tab, choose **SNMPv3**. Add an SNMPv3 user and Save the configuration.



Note

For the purpose of this guide, the default pre-defined SNMPv3 credentials are used, make sure the SNMPv3 user settings in XIQ-C match with **default_snmp_v3** credentials in the Site Engine. In a real deployment scenario, SNMP setting must be configured according to the customer's network settings.

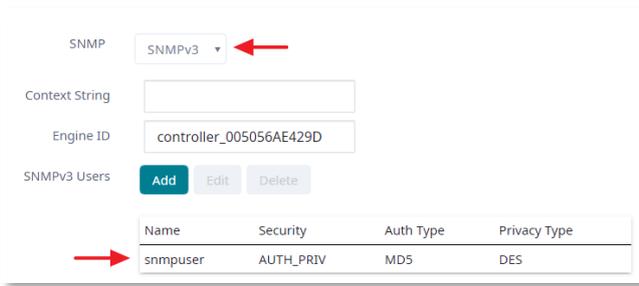


Figure-1: XIQ-C SNMP settings

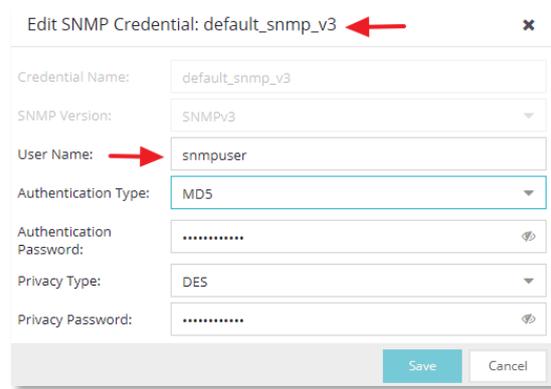
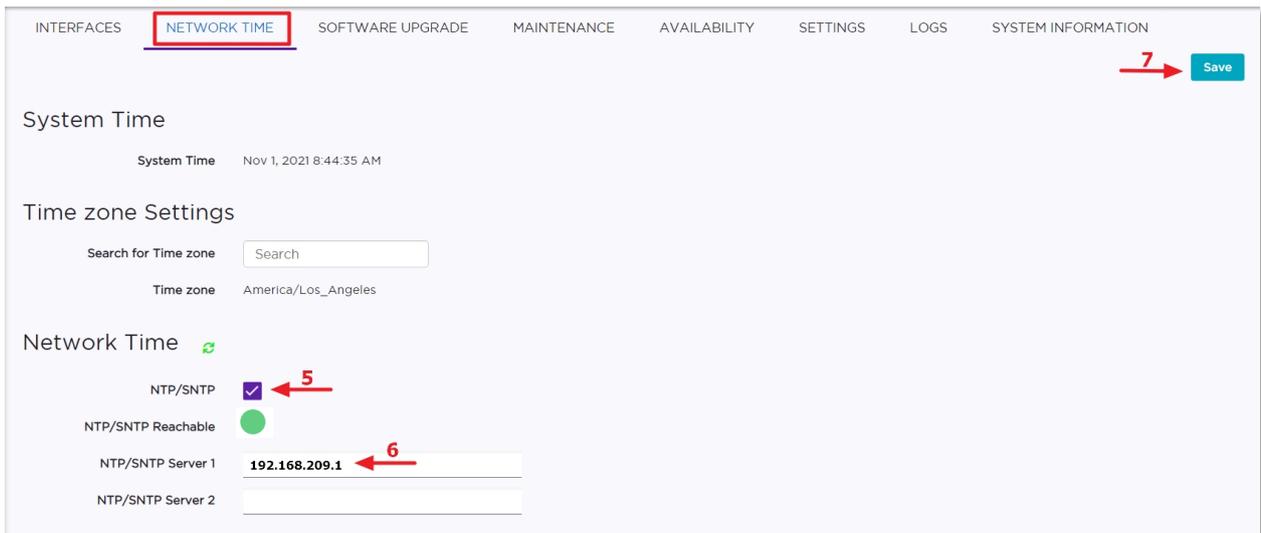


Figure-2: Site Engine SNMP settings

Next, select the **Network Time** tab to setup the NTP server. **Enable** the NTP/SNTP server setting, use an appropriate public or private NTP server as NTP Server IP address and save the configuration. The **NTP/SNTP Reachable** icon may not turn green immediately, a refresh may be required to sync with the NTP server.



Part 2: Site Engine Configuration

This section covers the configuration steps specific to the integration of the XIQ-C with Site Engine. At this point, the XIQ-C has already been configured with the required settings to provision the network connectivity to communicate with the Site Engine. Next step is to integrate the XIQ-C with Site Engine for ongoing monitoring, maintenance, and management. The following steps are required to successfully integrate the XIQ-C into Site Engine.

- Modifying SNMPv3 Profile with CLI credentials
- Adding XIQ-C to Site Engine
- Enabling statistics collection

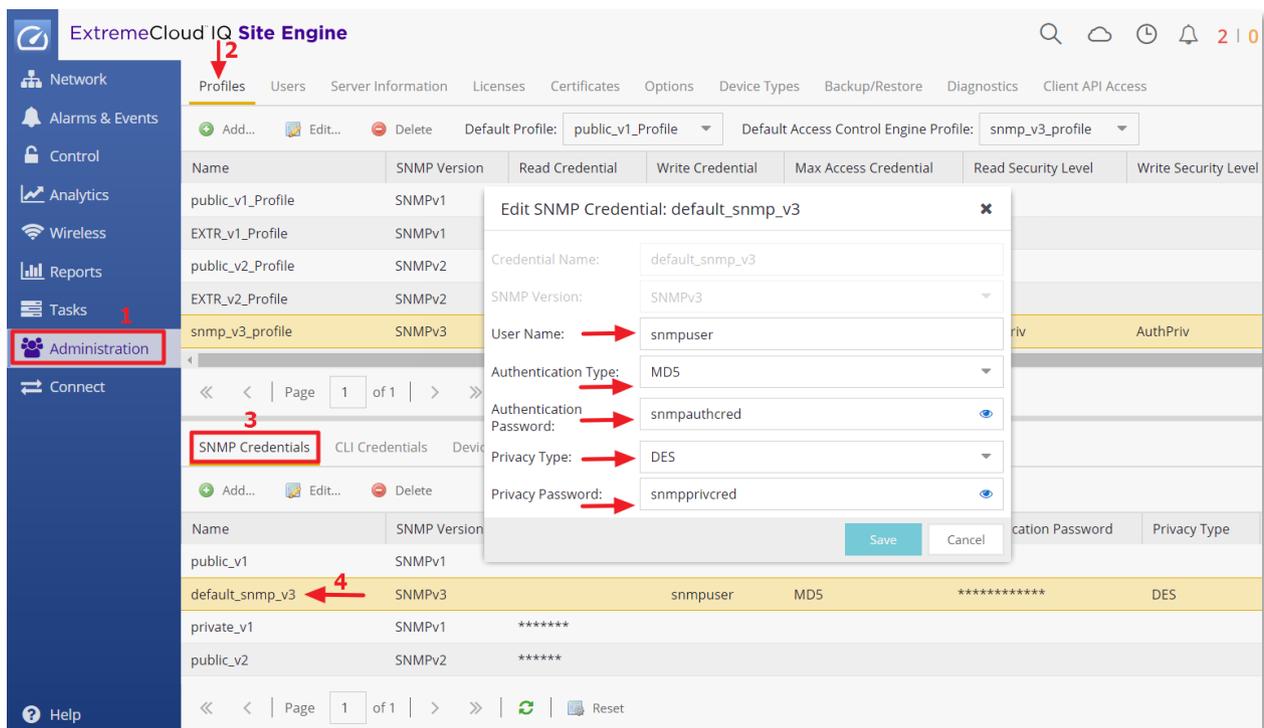
SNMP Profile Configuration

In order to establish SNMP communication between XIQ-C and Site Engine, an SNMP Profile must be created. Ideally, SNMPv3 is used due to its security and efficiency compared to SNMPv1 or SNMPv2. For a Proof of Concept or Demo exercise, it is generally easiest to use one of the default profiles available on Site Engine. If desired, a custom SNMP profile can be created to match the customer environment, however the profile will need to be created in Site Engine.

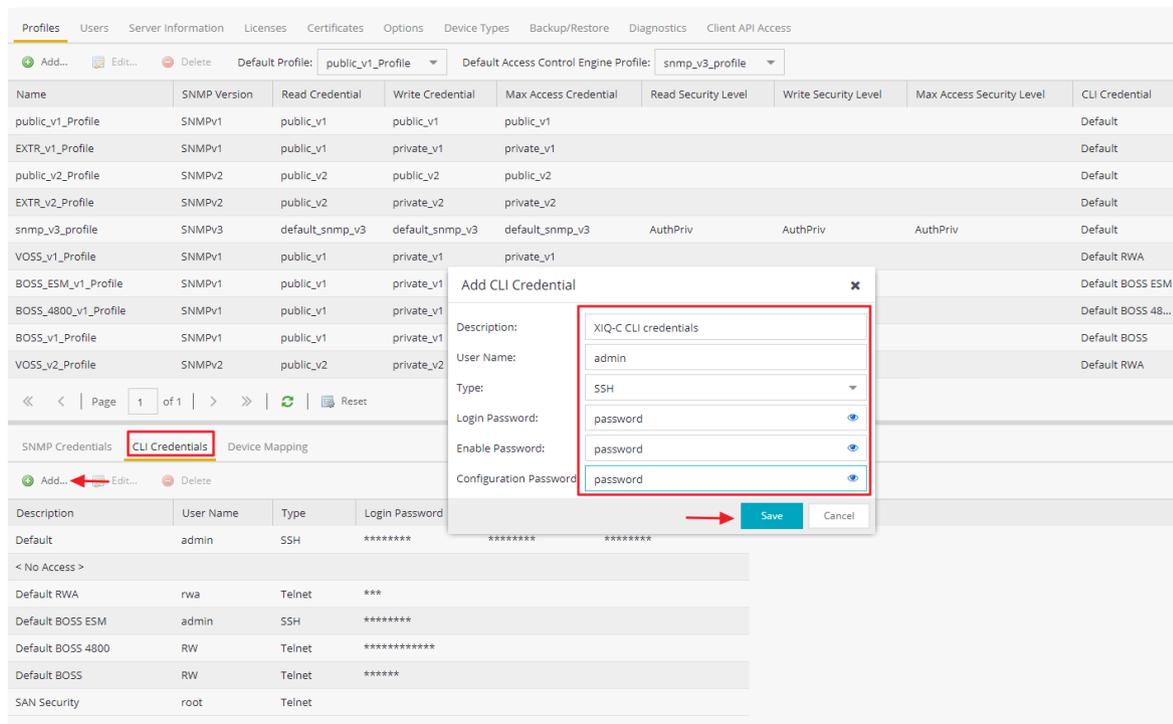
In this guide, the default SNMPv3 Site Engine profile is used which correlates to the SNMPv3 settings previously created in XIQ-C.

Review the SNMPv3 profile settings by navigating to the **Administration** tab. The first step is to check the SNMP credentials. All the SNMP profile settings are available under the **Profiles** tab. Select the sub-tab **SNMP Credentials** to view the list of the default SNMP credentials. Next, select the **default_snmp_v3** credentials to reveal the SNMPv3 credentials.

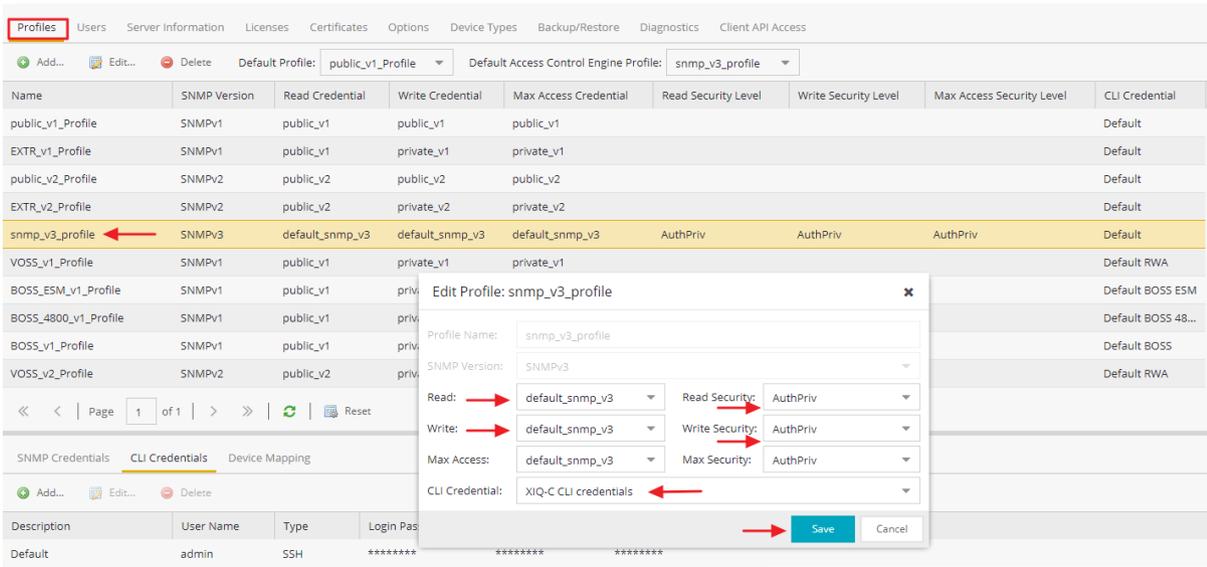
Make sure that the SNMPv3 profile configuration in the Site Engine matches the credentials previously configured in XIQ-C SNMPv3 settings.



Next, select **CLI Credentials** and then the **Add** button. When the **Create CLI Credential** pop-up window is displayed, apply a Description, User Name, and Password to the new credential and ensure that the **Type** field is set to **SSH**. The **User Name** field is set to **admin** and the **Login, Enable and Config** passwords are set to the credentials configured for the admin account on the XIQ-C. In this example, the admin account credentials for the XIQ-C are **admin/password**. Select the **Save** button to add the new CLI Credential to Site Engine.



Remaining within the **Profiles** tab, select **snmp_v3_profile**. The **default_snmp_v3** credentials must be selected for the Read and Write operation. In addition, the Read Security and Write Security must have AuthPriv selected as the security type. Finally, select the CLI credentials created in the previous step (e.g. XIQ-C CLI credentials) and Save.

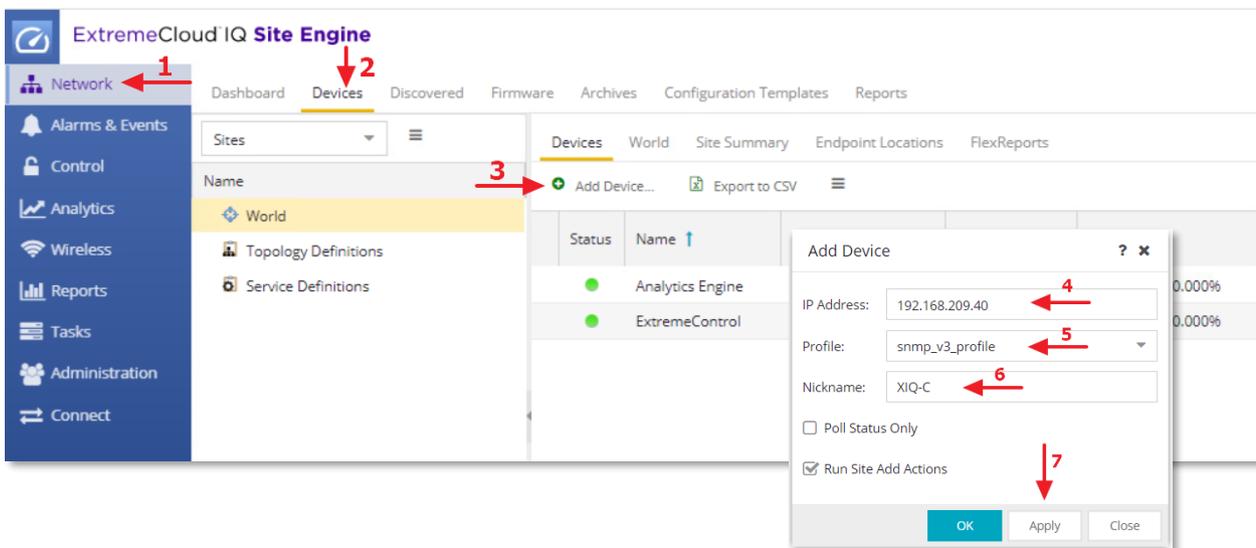


Note:

The CLI credentials are mandatory for the Site Engine Wireless Management function to sync XIQ-C logs, device status, AP and Client stats. The CLI Credentials are also required if scripts are used or the SSH access to a device via Site Engine is needed.

Adding XIQ-C to Site Engine

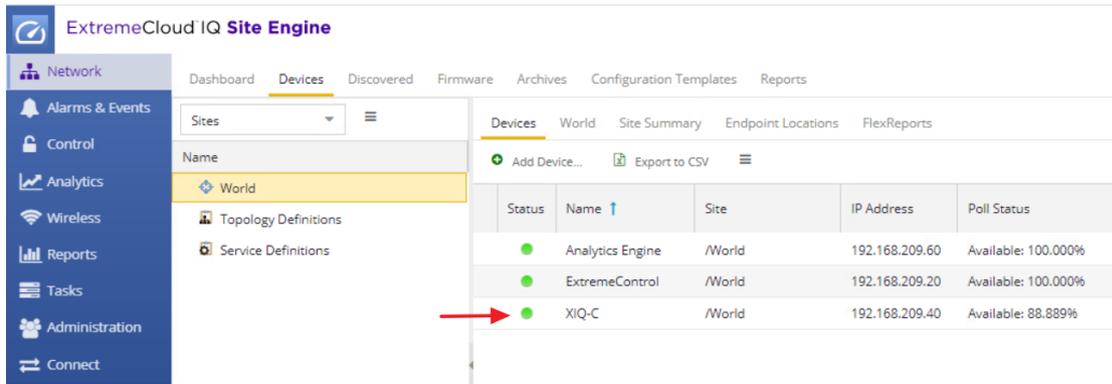
To add XIQ-C to the Site Engine, select the **Devices** button under the **Networks** tab. Add the XIQ-C by using its IP address, select correct SNMPv3 profile and give the newly added device a Nickname.



Before continuing, allow the XIQ-C device to report to Site Engine and display the status icon in the connected state (colored **green**). It may take a few seconds for the device to establish the SNMP communication with Site Engine and report its status.

Note:

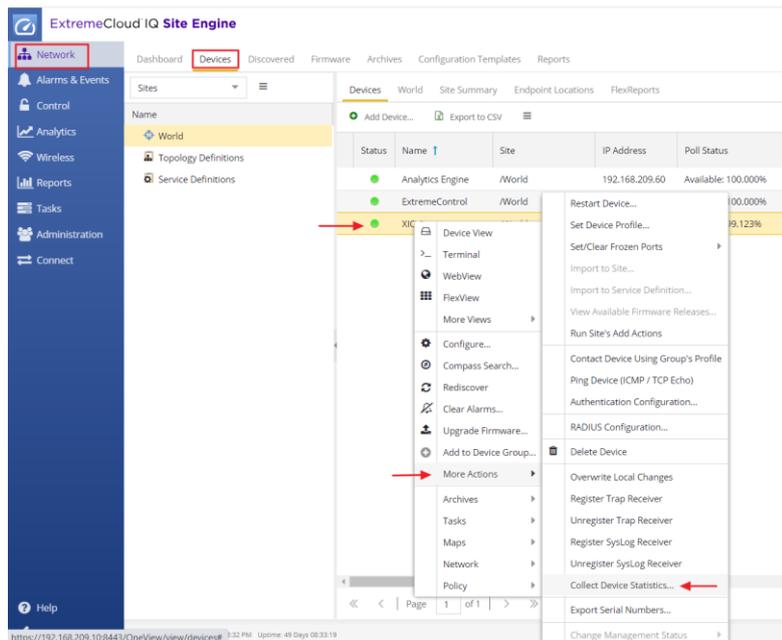
If the device fails to appear online, select the device, right click, and then choose **Rediscover** from the list of options. Otherwise, double check the **snmp_v3_profile** credentials and SNMPv3 settings previously configured in XIQ-C.



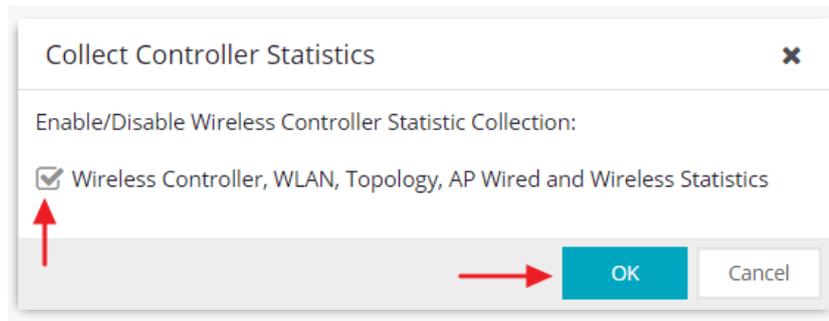
Enable XIQ-C Statistics Collection

Once the SNMP communication channel is functioning between the XIQ-C and Site Engine, the next step is to enable statistics collection for the Wireless LAN, Topologies, Access Points, and wireless clients.

Navigate to the **Network** screen in Site Engine, select the **Devices** tab, and select XIQ-C from the listed device. Right-click on the device, select the menu option for **More Actions** and then select **Collect Device Statistics**.



When the **Collect Controller Statistics** pop-up window is displayed, enable the statistics collection option followed by the **OK** button to preserve the changes.



Part 3: Policy Manager Configuration

One of the strongest features of ExtremeControl is the Policy architecture that allows for user and device control. Policy should always be configured and maintained through Site Engine for all policy-capable devices. To assist with Policy management, the Site Engine ships with two embedded policy domains which can be further modified to meet a particular customer's requirements.

The Default Policy Domain can be used for a vast array of policy examples. The policy domain that should be used for POCs is called ExtremeControl. This policy domain is optimized to simultaneously work with both Extreme Wired and Wireless policy capable devices.

In this section, the following tasks are completed:

- Adding XIQ-C to Policy Manager
- Configuring VLANs and Policy roles
- Deploying Policy configuration on XIQ-C via Policy Manager

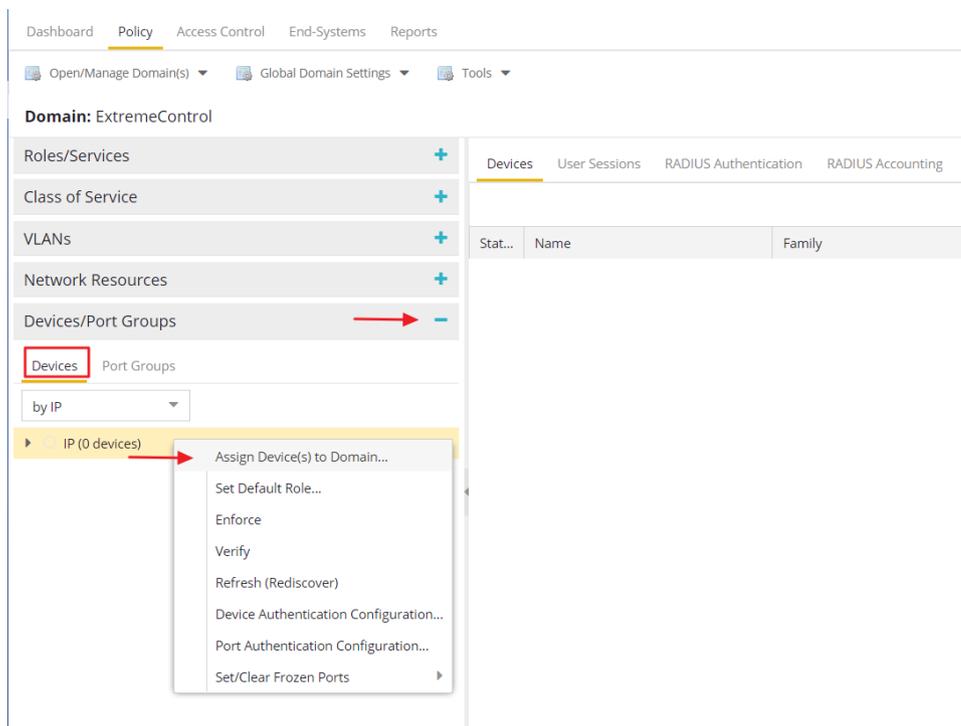
Adding XIQ-C to Policy Manager

Since Site Engine ships with the default domains, ensure that the **ExtremeControl** Policy domain is selected in the Policy tab as shown below.

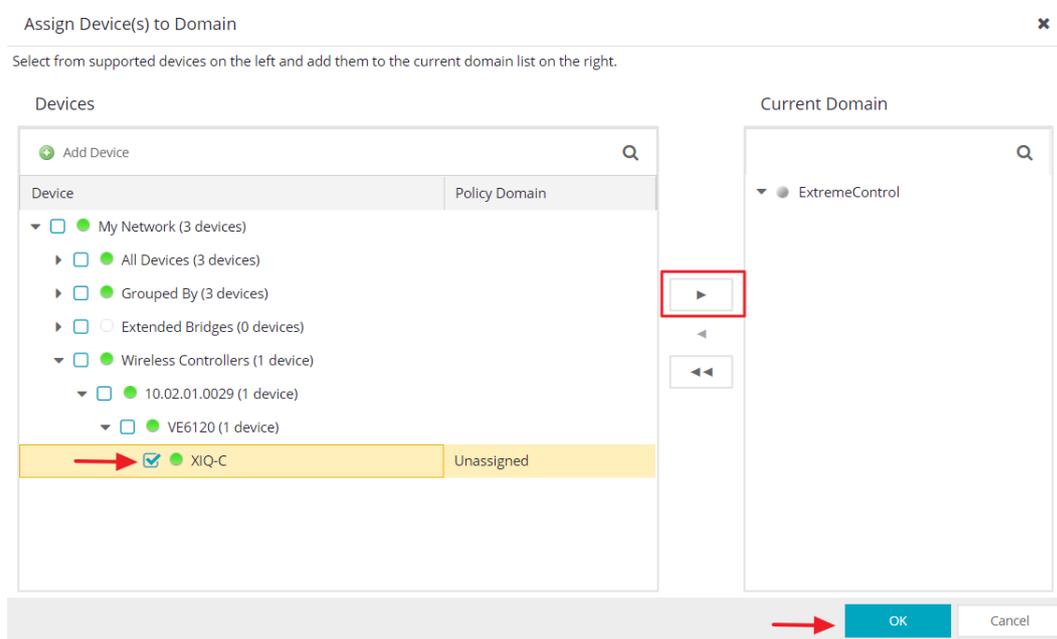
The screenshot shows the ExtremeCloud IQ Site Engine interface. The 'Policy' tab is selected in the top navigation bar. The 'Domain' dropdown is set to 'ExtremeControl', indicated by a red arrow. The 'Roles/Services' section is expanded to show a list of roles. The 'Roles' list includes: Access Point, Administrator, Assessing, Deny Access, Enterprise Access, Enterprise User, Fallsafe, Guest Access, Notification, Printer, Quarantine, Server, Unregistered, and VoIP Phone. The 'Class of Service' section is also visible at the bottom.

Role / Service / Rule	Summary
Access Point	[Permit Traffic/AP Aware]
Administrator	[Permit Traffic]
Assessing	[Deny Traffic]
Deny Access	[Deny Traffic]
Enterprise Access	[Permit Traffic/Critical Data]
Enterprise User	[1205 [BYOD]/High Priority]
Fallsafe	[Permit Traffic]
Guest Access	[1204 [Guest]/Best Effort]
Notification	[Permit Traffic/Network Control]
Printer	[Deny Traffic/Best Effort]
Quarantine	[Deny Traffic]
Server	[Permit Traffic/Network Control]
Unregistered	[1203 [Unregistered]]
VoIP Phone	[Permit Traffic/RTP/Voice/Video]

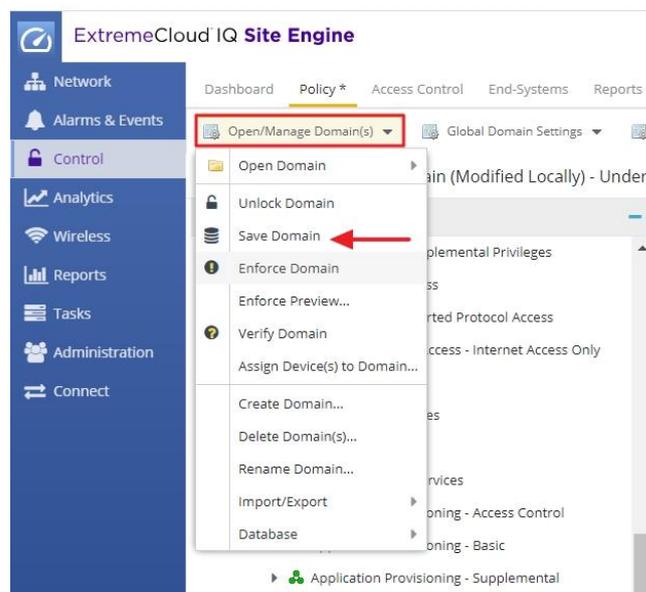
Select the **Devices** section to add Policy capable devices that should have Policy enforced to them. To add XIQ-C to the Policy domain, right-click the **Devices** tree and select **Assign Devices to Domain**.



In the resulting dialog, select XIQ-C from the left panel and then the arrow in the middle to move it to the right panel. When the device has been added, select the **OK** button to save the configuration.



Next, save the Policy domain settings by clicking on the **Open/Manage Domains** drop-down menu and selecting the **Save Domain** option.



VLAN Creation

A VLAN defines how the user traffic is presented through the network interface. Depending on the network connectivity requirements, multiple VLANs can be created with each mapped to a Policy role. When XIQ-C is integrated with Policy Manager, VLANs can be created in a Policy domain and assigned to XIQ-C as part of Policy role configuration.

Following are the three VLAN modes available in XIQ-C:

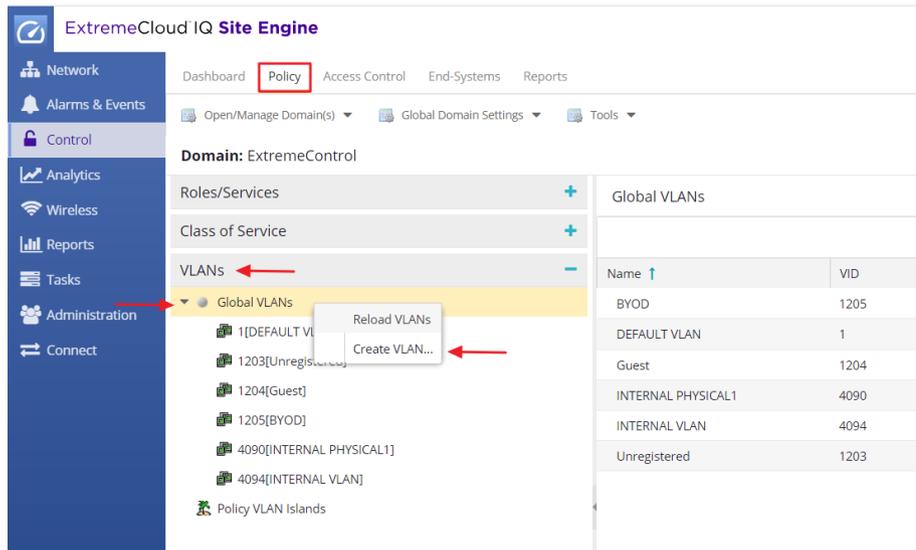
- **Bridged@AC:** The XIQ-C bridges traffic for the station through its interfaces, rather than routing the traffic. For the B@AC topology the station's "point of presence" on the wired network is the data plane port assigned to the topology.
- **Bridged@AP:** Assigned to APs, the AP bridges traffic between its wired and wireless interfaces without involving the XIQ-C. The station's "point of presence" on the wired network for a B@AP topology is the AP's wired port.
- **Fabric Attach:** The Fabric Attach topology type allows an AP to attach to a Fabric Connect Network. The client component on the AP communicates directly with the server on an edge switch (or it can communicate with the server through a proxy) to allow the AP to request VLAN to I-SID (backbone Service Identifier [IEEE 802.1 ah] mapping). The Fabric Attach topology type is similar to B@AP with the added I-SID parameter. Fabric Attach can be configured on the XIQ-C anywhere a B@AP topology can be configured.

VLANs for Guest Traffic

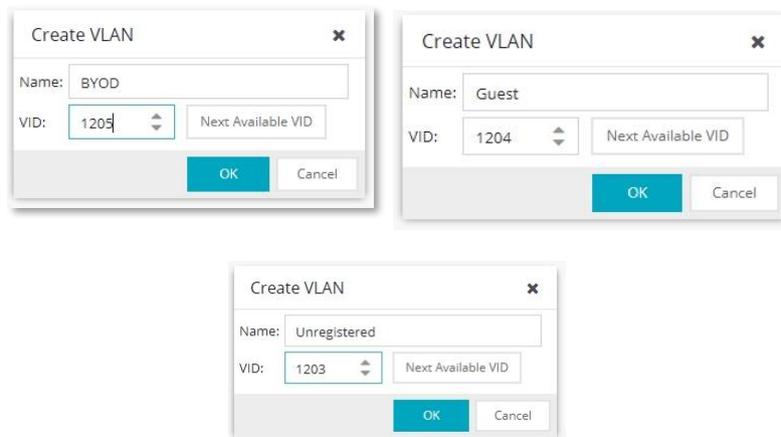
To implement a Guest Captive Portal that provides Guest Registration and Authenticated Registration (BYOD) access, as a best practice, a minimum of three VLANs are recommended to isolate the guest traffic. These VLANs are used for **Registered**, **Authenticated Registration**, and **Unregistered** guest traffic respectively. However, if separate VLANs are not possible, administrators can have all the guest traffic in the same VLAN and use policy to contain the traffic. The VLAN for Unregistered users is used to isolate the client traffic on the network prior to successful registration. Usually, this VLAN

only provides connectivity to network services such as DNS, DHCP and the Captive Portal server (ExtremeControl in this case) that are necessary for the web redirect to happen. In addition to the VLAN for Unregistered guest traffic, two more VLANs are configured to isolate Registered Guest and Authenticated Registration users i.e. BYOD traffic.

To create new VLANs, under the **Policy** tab, select the **VLANS** tree menu and then right-click the **Global VLANS** option. Select the **Create VLAN** option to begin creating VLANs.



Create VLANs for **BYOD**, **Guest** and **Unregistered** users. The VLAN ID and tag information must be configured based on the network configuration to ensure proper operation and isolation of the guest traffic.



Note:

On wireless devices (for example, XIQ-C), the VLAN is written to the device as part of Policy domain configuration push if it is being used in either a rule or Policy role.

Role Creation

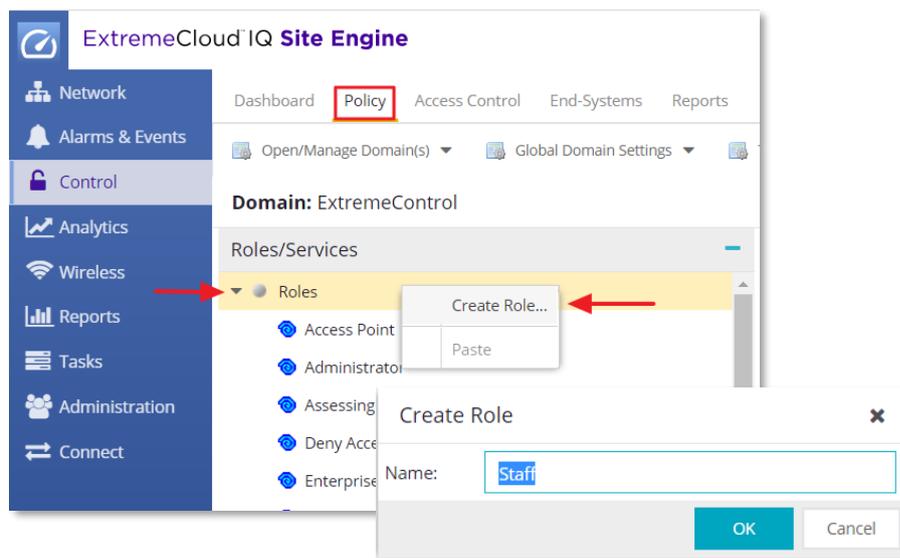
Policy roles define the access that a user or device has when connected to the network via XIQ-C. The roles can be dynamically assigned and contain many definitions including Firewall Rules, VLAN assignment, and QoS settings. The roles need to be defined before the assignment and should represent the Accept Policies that are assigned from ExtremeControl via the rules engine.

The minimum required Policy roles to be configured for this guide are:

- Unregistered – This profile limits traffic and redirects web traffic to ExtremeControl.
- Guest Access – This profile limits internal traffic but allows full access to the Internet and is used for Guest Users.
- Enterprise User – This profile when used for Authenticated Registration (BYOD). Corporate users may allow limited access internal corporate resources while allowing full access to the Internet.

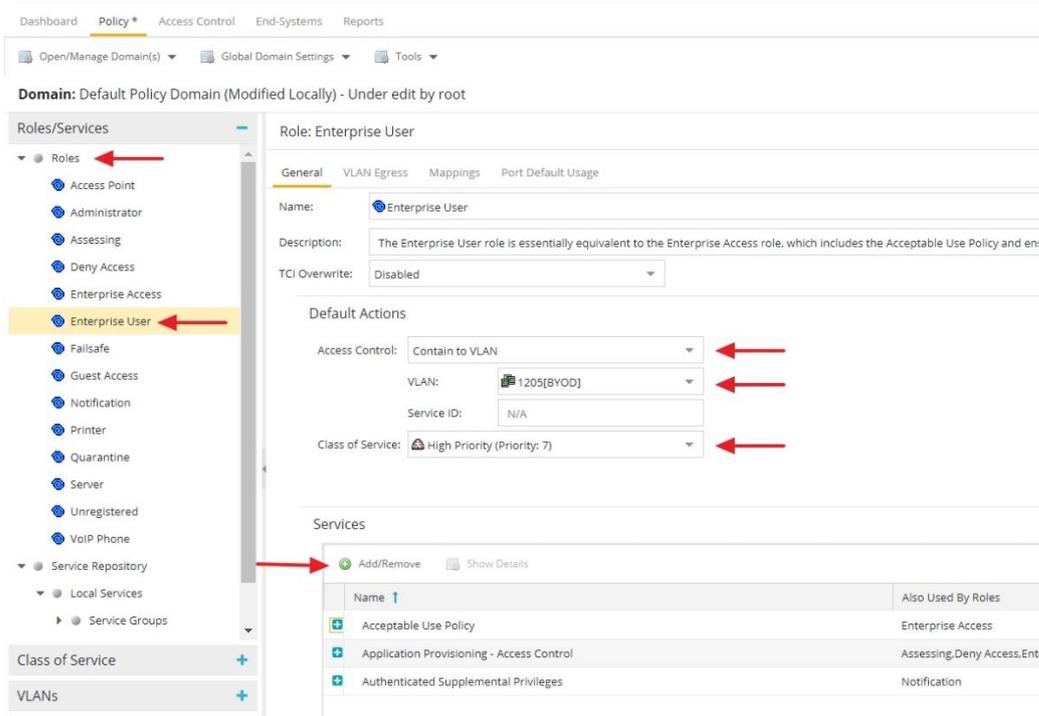
For test setups and POCs, it is sufficient to use the default Guest Access and Enterprise User roles to assign Firewall rules and VLANs to the users. For a real deployment, if needed, additional roles with appropriate policy names must be created and configured with relevant VLANs, QoS policies, and firewall rules.

For example, to create a new Policy role, right-click the **Roles** node in the **Roles/Services** section as shown below. Name the role in a way that describes the type of access being assigned, the type of user, or the type of device.

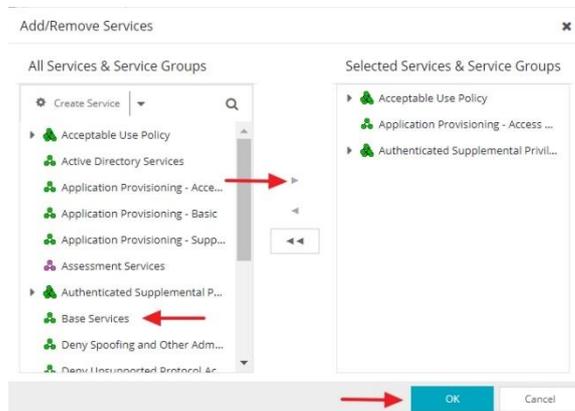


This guide uses the default **Guest Access**, **Enterprise User** and **Unregistered** roles. Select these roles from the list of default roles and specify the Default Actions to be performed. In general, all policy-capable devices support **Access Control** and **Class of Service** configuration. The available options for Access Control are: **Permit Traffic**, **Deny Traffic**, or **Contain to VLAN** where the VLAN ID can be selected from a dropdown list.

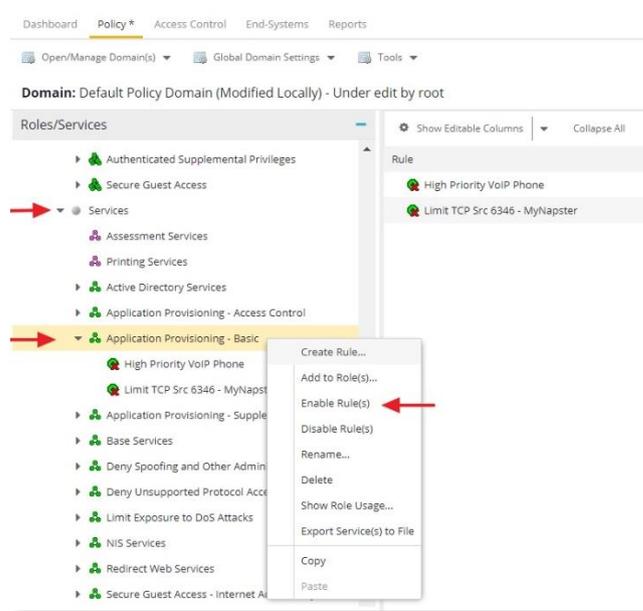
If necessary, **Class of Service** can also be defined for each role. Site Engine includes multiple default Class of Service objects. These objects can be used to assist with prioritization of the traffic within the network. In addition, If more specific services are required for the role to permit or deny access, services can be assigned to the role via the **Add/Remove** button in the **Services** tab.



In the resulting **Add/Remove** Services dialog, select the services that should be included for the role and move them to the window panel on the right. Once the appropriate services have been selected, select **OK** to save them to the role.



To ensure that all the rules defined within the selected services are enabled, select the **Services** option, right-click on the service and select **Enable Rules**.



Repeat this process for all the remaining roles (for example: Guest Access and Unregistered) and configure **VLAN**, **Class of Service** and **Services** according to the any pre-defined POC requirements.

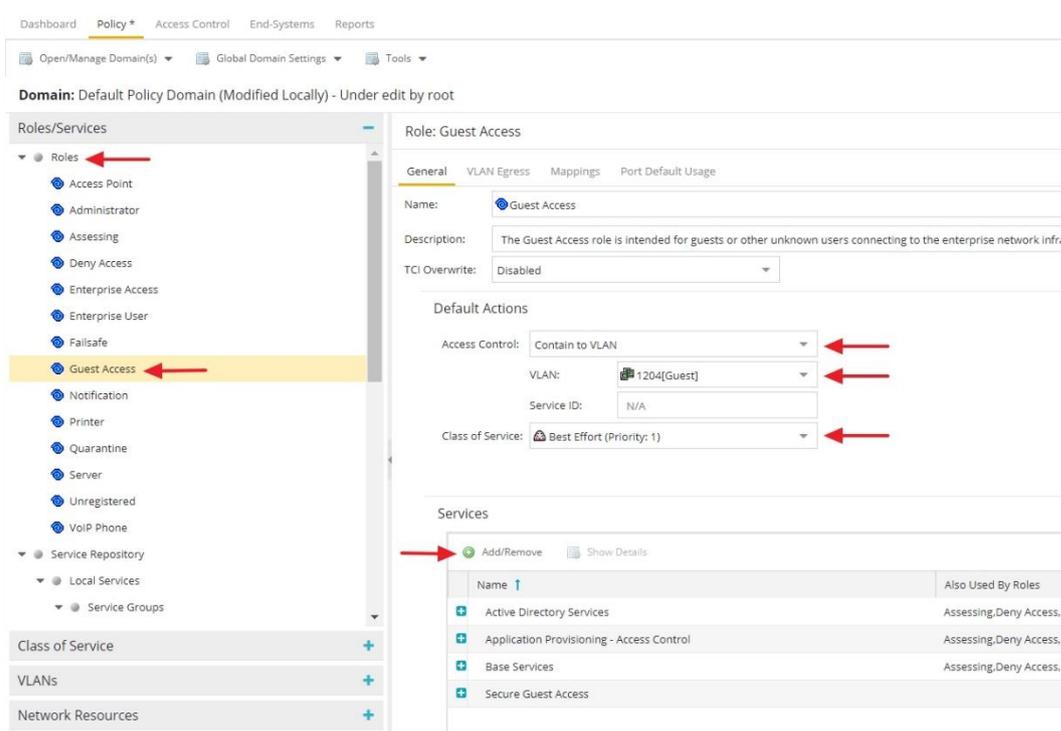


Figure 1 Guest Access Role Configuration

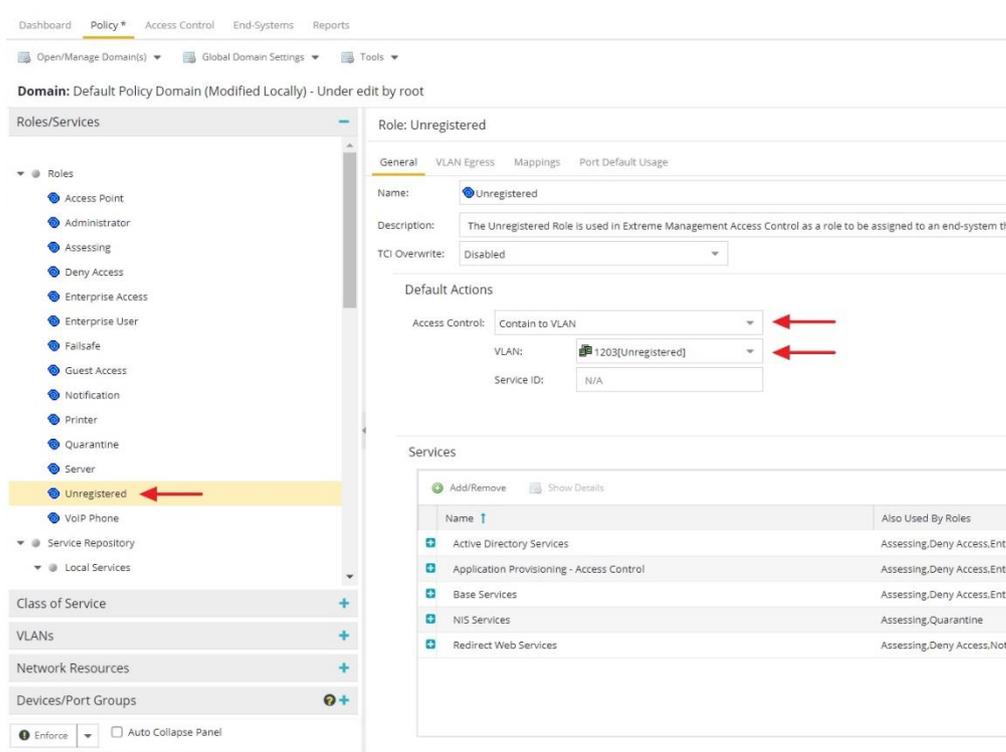


Figure 2 Unregistered Role Configuration

Note:

The Unregistered role configured in this section is only used to push the **Unregistered VLAN** to XIQ-C. Keep in mind that when XIQ-C integrates with ExtremeControl, the default Unregistered role will not be a part of the RADIUS Accept attribute and none of the CoS and Services settings defined in this role are used. More details on this are available in the [XIQ-C internal Unregistered role for Guest networks](#) section of this guide.

Part 4: XIQ-C Configuration

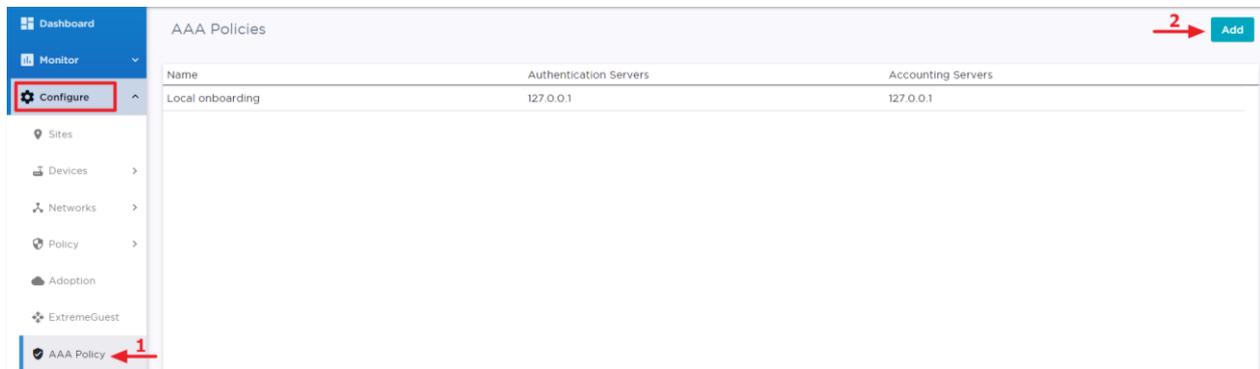
The first step to configuring XIQ-C is to complete the following activities:

- Configuring AAA policy
- Creating the Captive Portal SSID for guest
- Verifying VLANs and Roles on XIQ-C
- Mapping SSIDs, VLANs and Roles to AP Profile

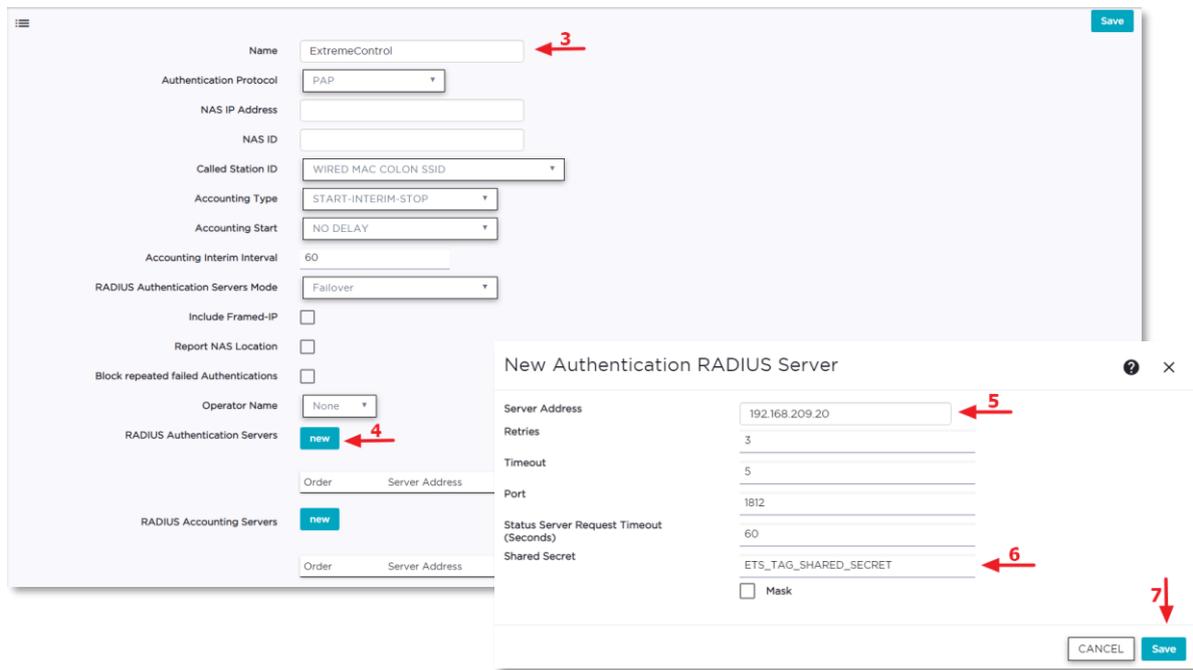
Once this configuration is complete, all processing and authentication occurs between the XIQ-C and ExtremeControl.

AAA Policy Configuration

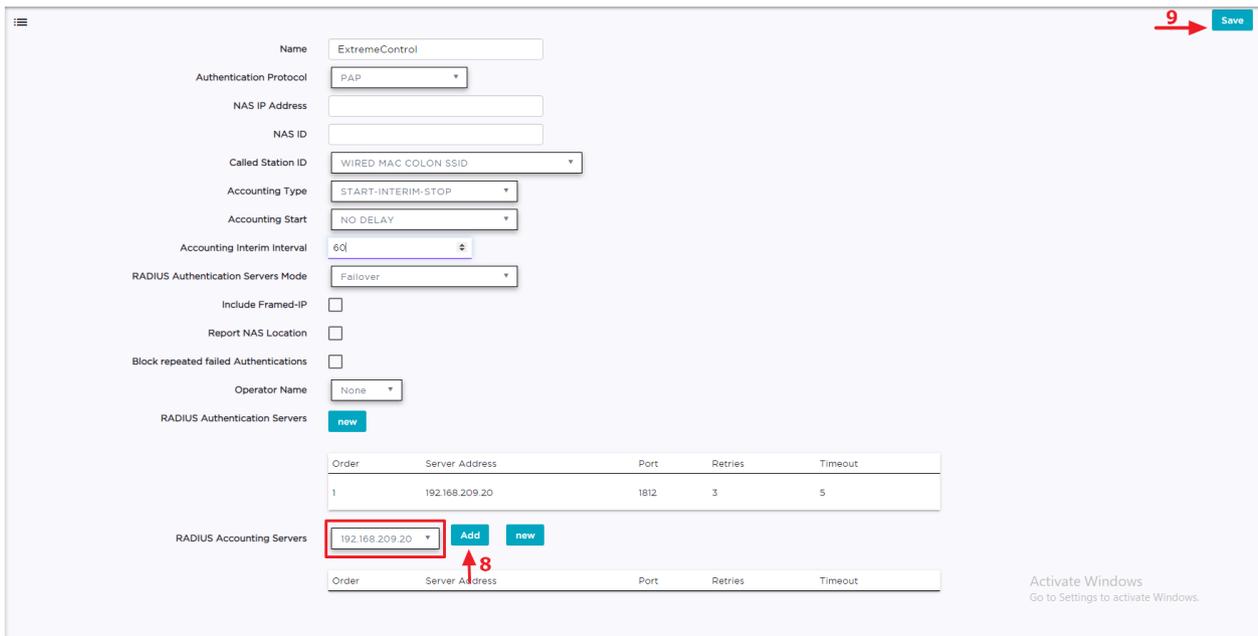
One of the key configuration steps is to configure a AAA policy in XIQ-C. XIQ-C to authenticate users against ExtremeControl, the ExtremeControl engine needs to be configured as a designated RADIUS server. To accomplish this, navigate to the **Configure** tab and select **AAA Policy**. Add a new AAA policy and give it a name, for example ExtremeControl.



Select **New** to add a RADIUS Authentication Server with Server Address that points to ExtremeControl, 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 proofs of concept. For a real deployment, it is expected that the shared secret will be changed from the defaults. Save the settings and move on to the **RADIUS Accounting Server** configuration.



Add a **RADIUS Accounting Server** by selecting the newly created RADIUS server from the drop-down menu and Save the settings.



Guest SSID Configuration

At this point, all the configuration elements that are required to create an SSID are configured, and an SSID can be created for guest access. A guest SSID is similar to an open SSID but with MAC authentication and Captive Portal enabled.

Use the following configuration template to create a guest SSID and change the ECP URL, AAA Policy and the Default VLAN settings as needed.

Network Name: XIQ-C-EAC-Guest

SSID: XIQ-C-EAC-Guest

Status: Enabled

Auth Type: Open

Enable Captive Portal: Yes

Captive Portal Type: External

ECP URL: <https://extremcontrol-ip-address>

Use HTTPS Connection: Enabled

Send Successful Login To: Original Destination

MAC Based Authentication (MBA): Enabled

MBA Timeout Role: Unregistered

AAA Policy: ExtremeControl

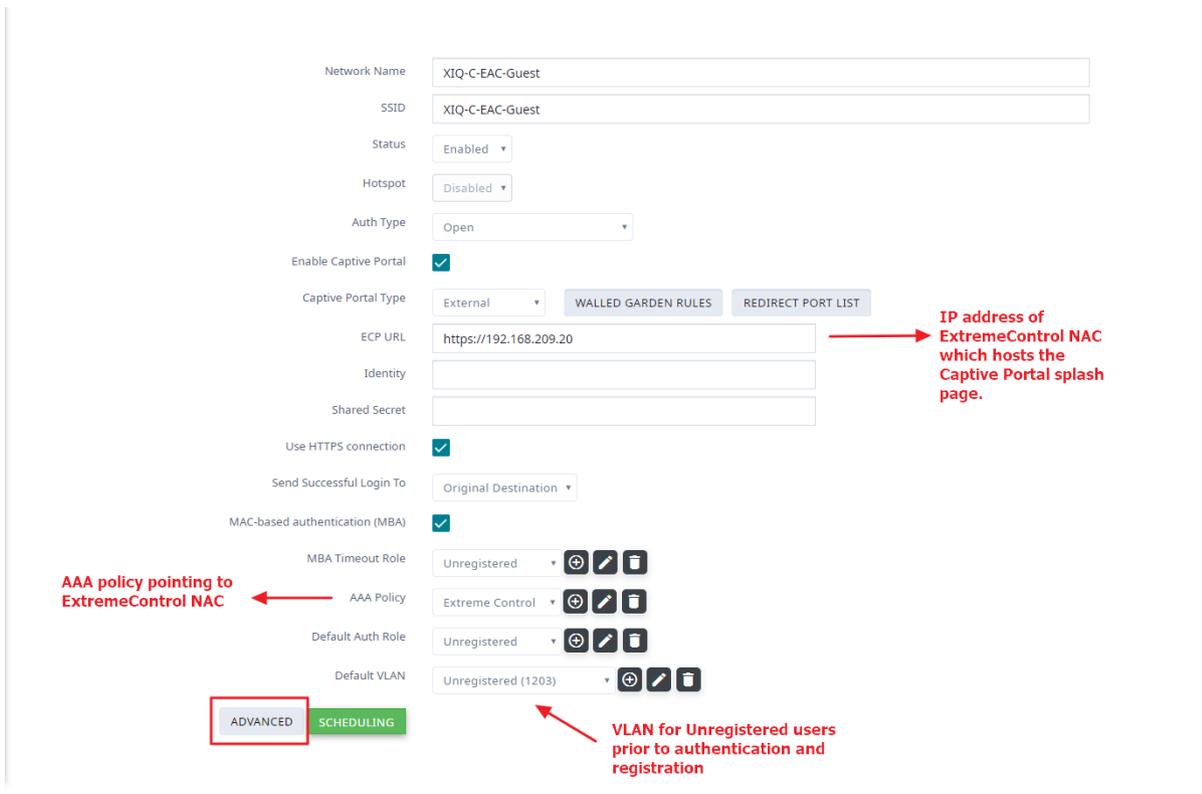
Default Auth Role: Unregistered

Default VLAN: Unregistered (1203)

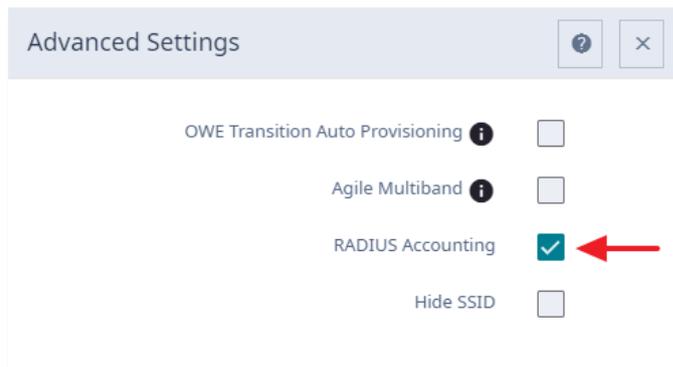
Often times it is observed that customers utilize the same VLAN for both Unregistered and Registered guest traffic, although this works, it is not the most secure way to implement a guest WiFi solution. Ideally, the Default VLAN value should be set to a VLAN that is configured for Unregistered guest traffic.

Note:

The “Default Auth Role” setting is for failsafe only and will not be utilized if the proper Filter-Id is sent from the ExtremeControl. So, the value selected here is mainly arbitrary.



To enable Radius accounting for the guest SSID, select **Advanced** and enable the RADIUS Accounting option. Finally, save the settings and **do not** map the SSID to the Profile when prompted by selecting SKIP button.



XIQ-C Internal Unregistered role for Guest Networks

Everytime a guest SSID is created in XIQ-C, the configuration workflow automatically creates an internal Unregistered policy role for the guest network. This internal Unregistered role is unique to each guest network and contains the name of the guest network it is created for, for example, “Unregistered role for XIQ-C-EAC-Guest” in this instance.

These internal Unregistered roles can be viewed under the **Onboard > Rules** screen. Make sure to take a note of this Unregistered role name (it is case sensitive), as it will be utilized later during the ExtremeControl policy mapping configuration.

Rules

Enabled	Name	Conditions	Accept Policy	Portal
✓	Blacklist	End-System is in Blacklist	Quarantine	Default
✓	Unregistered Loc: Network: XIQ-C-EAC-Guest	Location is in Network: XIQ-C-EAC-Guest	Unregistered role for XIQ-C-EAC-Guest	Default
✓	Default Catchall		Use Default Auth Role	Default

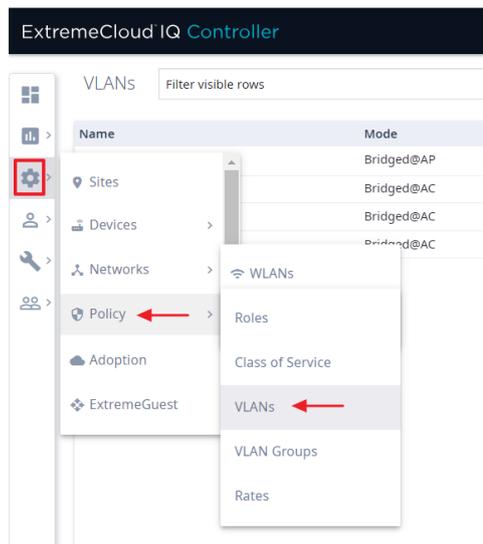
The internal Unregistered role contains all the necessary rules to allow access to network services such as ARP, DNS, DHCP, the captive portal server, and HTTP/HTTPS to enable Captive Portal redirect.

Since this is an internal system generated role, the rule entries within the role can't be deleted. However, if additional rule entries are needed to allow/deny traffic to specific network services and resources for Unregistered users, for example, third-party Captive Portal server communication ports or OAUTH URLs, the **Walled Garden Rules** under the guest SSID settings can be utilized.

Verifying VLANs and Roles on XIQ-C

Before the VLANs and Roles can be mapped to an AP profile in XIQ-C, a good practice is to first verify the VLANs and Roles configuration which is deployed from the Policy Domain. On XIQ-C, both the VLAN and Role configurations are available under **Configure > Policy** tab.

First, check the VLANs and confirm that the VLAN settings deployed by the Policy Domain configuration are in-line with the network setup.



Here, an important thing to remember is, that the default **VLAN Mode** supported by the Policy Domain is either **B@AC** or **Fabric Attach** (if the ISID was specified when VLANs were created in the Policy Domain), **B@AP** is not the default VLAN Mode and must be selected manually in XIQ-C.

Name	Mode	Tagged	VLAN ID
Bridged at AP untagged	Bridged@AP		1
Guest	Bridged@AC	✓	1204
BYOD	Bridged@AC	✓	1205
Unregistered	Bridged@AC	✓	1203

Select the VLAN and change the **Mode** for each VLAN as per customer’s network configuration or the POC requirement. For example, if the network configuration requires the traffic to be tunneled back to the XIQ-C appliance, use B@AC. Otherwise, in case of local traffic bridging, select B@AP or Fabric Attach if the network is Fabric capable and the VLANs were configured with ISIDs in the Policy Domain.

Name: Guest

Mode: Bridged@AC (dropdown menu open showing options: Bridged@AC, Bridged@AP, Fabric Attach, VXlan)

VLAN ID: [] Tagged:

Port: Port1

ADVANCED

Associated Profiles: Vlan is not associated with any Profiles

Note:

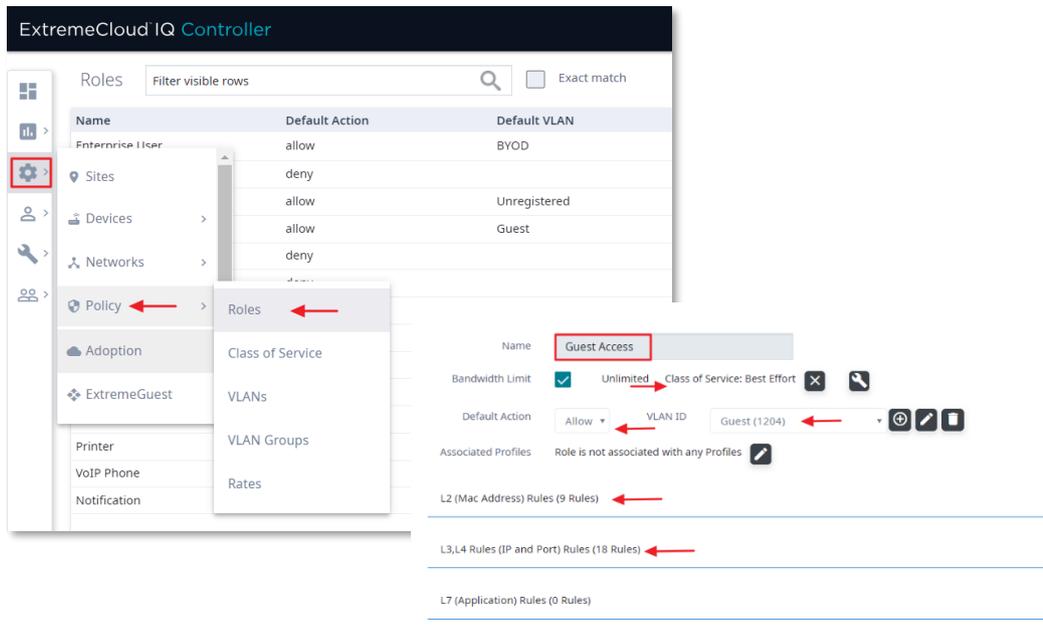
As part of Policy Domain configuration, VLANs are tied to Roles and then deployed on XIQ-C. Due to a configuration workflow limitation on XIQ-C, to change the VLAN Mode, one must first un-map the VLAN from its associated Role, change the VLAN mode and then tie the VLAN back to its Role again.

In this guide, **B@AP** Mode is used for **Guest**, **BYOD** and **Unregistered** VLANs.

ExtremeCloud IQ Controller

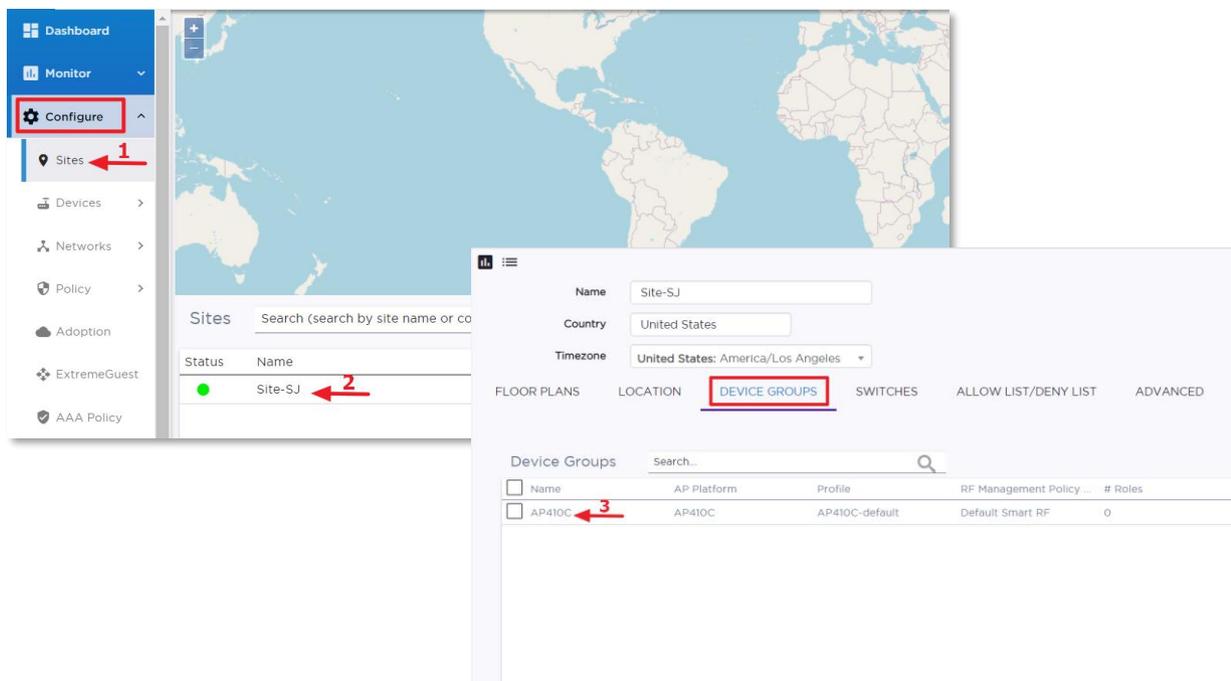
Name	Mode	Tagged	VLAN ID
Bridged at AP untagged	Bridged@AP		1
Guest	Bridged@AP	✓	1204
BYOD	Bridged@AP	✓	1205
Unregistered	Bridged@AP	✓	1203

Secondly, select **Roles** under **Configure > Policy** tab and review the configuration such as the Default Action, VLAN, Class of Service and Rules for the **Enterprise User** and **Guest Access** roles. The configuration review is not needed for **Unregistered** role since it is only used to push the Unregistered VLAN configuration to the XIQ-C via Policy Domain.

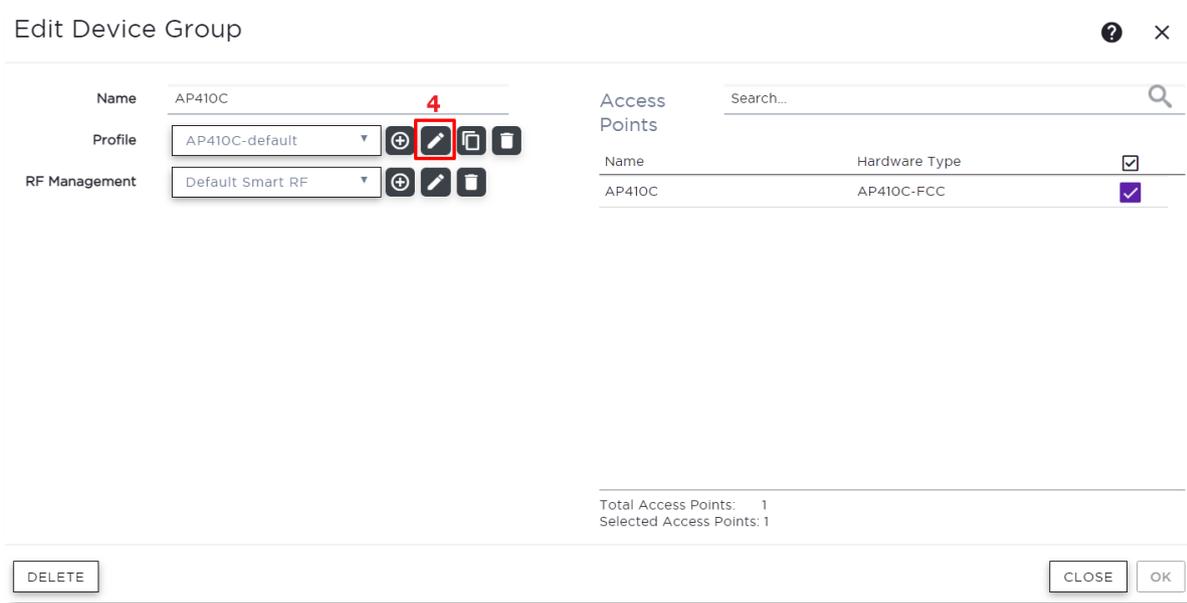


AP Profile: SSID, VLANs and Roles Mapping

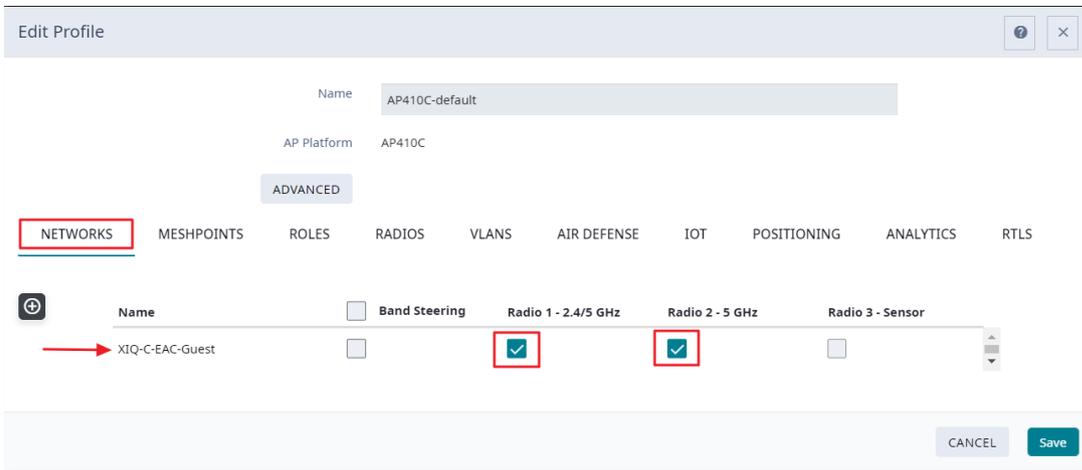
The next step is to map the SSID, Policy Roles, and VLANs to the AP Profile. Navigate to **Configure** tab and select **Sites**. From the list of Sites, select the site that is going to provide Guest WiFi service and select the **Device Group**.



Next, on the **Edit Device Group** screen, edit the **AP Profile** settings.



The **Network** tab on the Edit Profile screen is where wireless SSIDs are applied to the radios. Map the guest SSID e.g. **XIQ-C-EAC-Guest** to the radio interface. There is no need to save the settings yet as more changes need to be made.



Assign the necessary Roles and VLANs to the AP Profile . Keep in mind that when XIQ-C integrates with ExtremeControl, the default **Unregistered** role will not be a part of the RADIUS Accept attribute. Instead, for Unregistered role, XIQ-C will send “**Unregistered role for <network_name>**” (note the spelling and spaces between the words; the network name should match exactly as it is spelled in the configuration). Configuration of this attribute is covered later in the ExtremeControl configuration section. After the Roles and VLANs have been selected, the configuration can be saved.

The image displays two overlapping screenshots of the 'Edit Profile' configuration window for an AP410C device. The top screenshot shows the 'ROLES' tab, and the bottom screenshot shows the 'VLANS' tab.

Top Screenshot: ROLES Tab

Name: AP410C-default
AP Platform: AP410C

Navigation: NETWORKS, MESHPOINTS, **ROLES**, RADIOS, VLANS, AIR DEFENSE, IOT, POSITIONING, ANALYTICS, RTLS

Name	Selected
Enterprise User	<input checked="" type="checkbox"/>
Access Point	<input type="checkbox"/>
Assessing	<input type="checkbox"/>
Deny Access	<input type="checkbox"/>
Failsafe	<input type="checkbox"/>
Guest Access	<input checked="" type="checkbox"/>
Quarantine	<input type="checkbox"/>
Unregistered	<input type="checkbox"/>

Bottom Screenshot: VLANS Tab

Name: AP410C-default
AP Platform: AP410C

Navigation: NETWORKS, MESHPOINTS, ROLES, RADIOS, **VLANS**, AIR DEFENSE, IOT, POSITIONING, ANALYTICS, RTLS

Name	Referenced	Additional
Bridged at AP untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
BYOD	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Guest	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Unregistered	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Buttons: CLOSE, Save

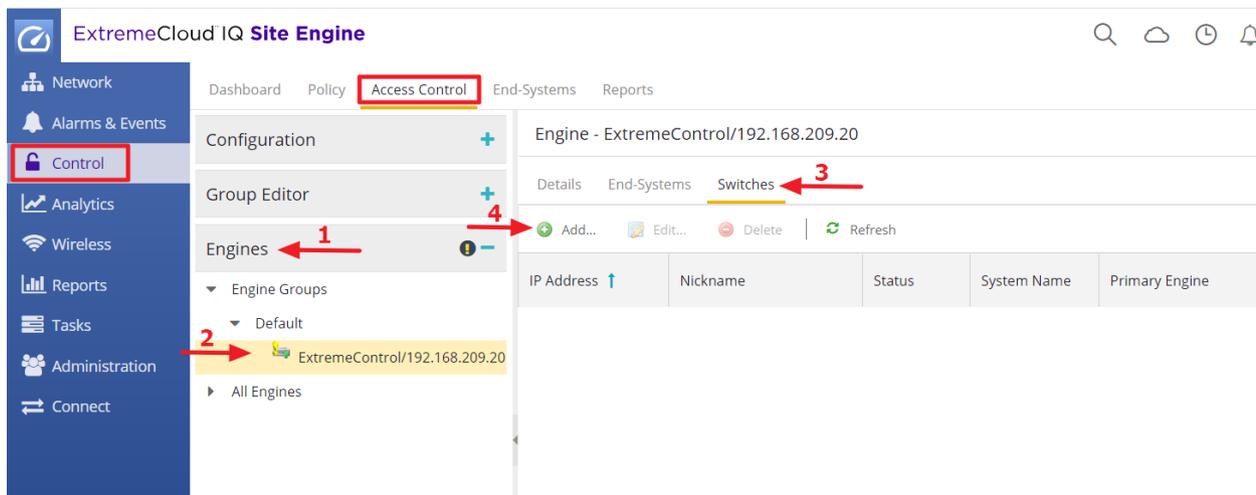
Part 5 – ExtremeControl Configuration

This section covers the configuration steps specific to the integration of the XIQ-C and ExtremeControl. At the end of this section, XIQ-C should be able to communicate with ExtremeControl and authenticate wireless users.

The configuration of authentication and authorization to ExtremeControl is broken up into two parts. The first part adds the XIQ-C to ExtremeControl for authentication. Additionally, the XIQ-C needs to be configured for authentication which is performed through ExtremeControl. The second part is configuring the ExtremeControl to properly authenticate the clients.

Adding XIQ-C to ExtremeControl

To add XIQ-C into ExtremeControl, select **Access Control** under the **Control** main menu tab. In the Access Control tree menu, select Engines, use the drop-down button to expand the tree and click the ExtremeControl engine. In the right-hand side panel, select the Switches tab. From there select the **Add** button as shown below.



On the next screen, add XIQ-C using the following configuration parameters.

Primary Engine: ExtremeControl/<ip-address>

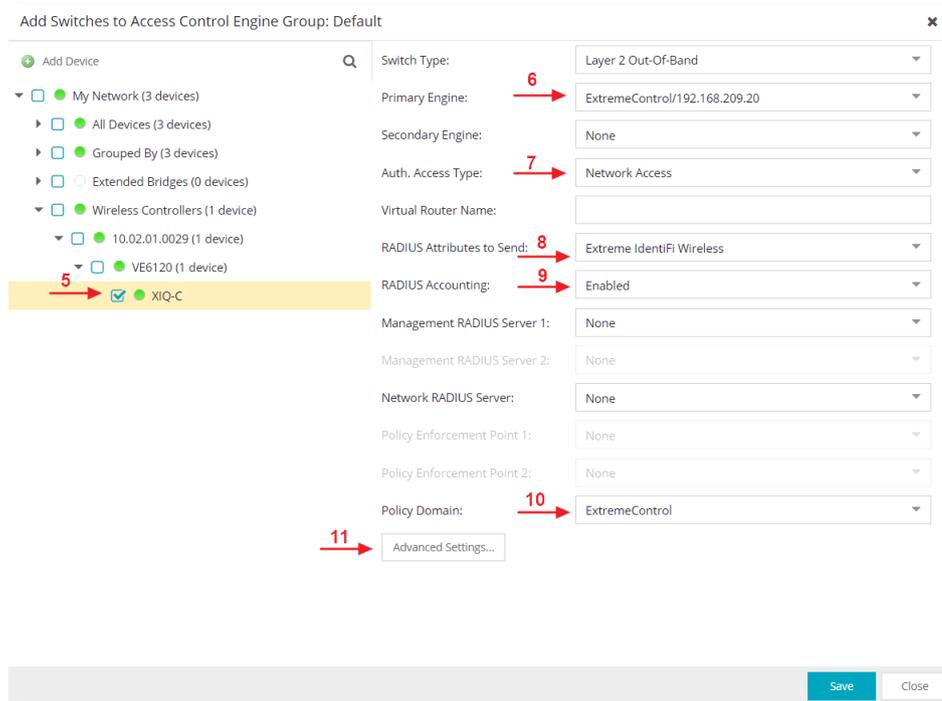
Auth. Access type: Network Access

RADIUS Attributes to Send: Extreme Identifi Wireless

RADIUS Accounting: Enabled

Policy Domain: ExtremeControl

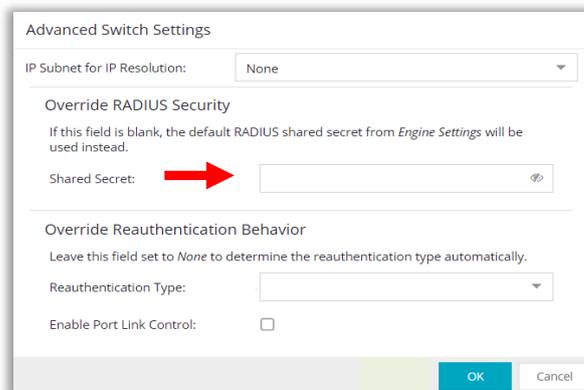
By default, the ExtremeControl engine uses SNMP to trigger reauthentication using the SysObjectID in different MIBs, therefore, it is not necessary to set the **Reauthentication Type** manually. If for some reason the Reauthentication Type needs to be changed, it can be done under the **Advanced Settings**.



In most POCs and test setups, using the default **Shared Secret** on ExtremeControl suffices. However, in real deployment, for increased security the Shared Secret should be modified according to the customer’s security guidelines.

ExtremeControl allows for the Shared Secret value to be either uniquely defined for each device or configured globally for all the devices. In this guide, the default shared secret (**ETS_TAG_SHARED_SECRET**) is used which is globally applicable to all devices that are added to ExtremeControl.

If the Shared Secret must be modified as per customer’s specifications, it is recommended that it is changed under the **Advanced Settings** while adding the device (example XIQ-C), the Shared Secret value defined here remains device specific and does not affect other devices.

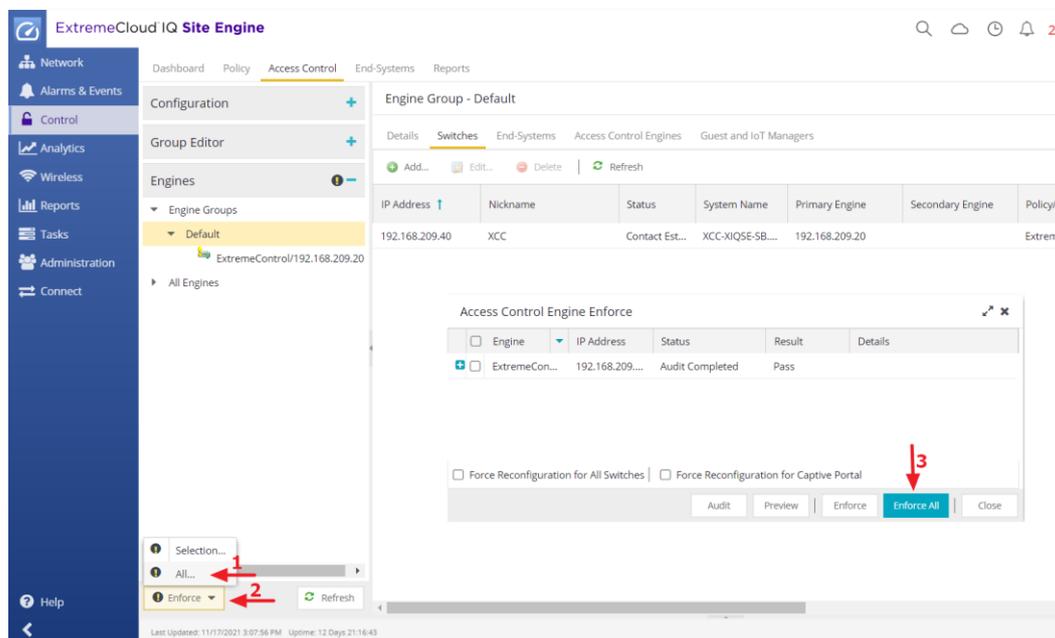


Note:

To change the shared secret globally, navigate to **Engines** tab, select the ExtremeControl engine listed under the **Engine Groups > Default**. On the resulting screen, under the **Details** tab, select **Engine Settings** and then the **Credentials** tab to change the Shared Secret.

After the device is added to Access Control, select the **Enforce** button followed by **All** to push the configuration to the Access Control Engine and the RADIUS configuration to the XIQ-C device.

A configuration audit will occur to ensure there are no unexpected issues with the current configuration. If an audit warning appears, select the checkbox to acknowledge the warning and then select the **Enforce All** button.

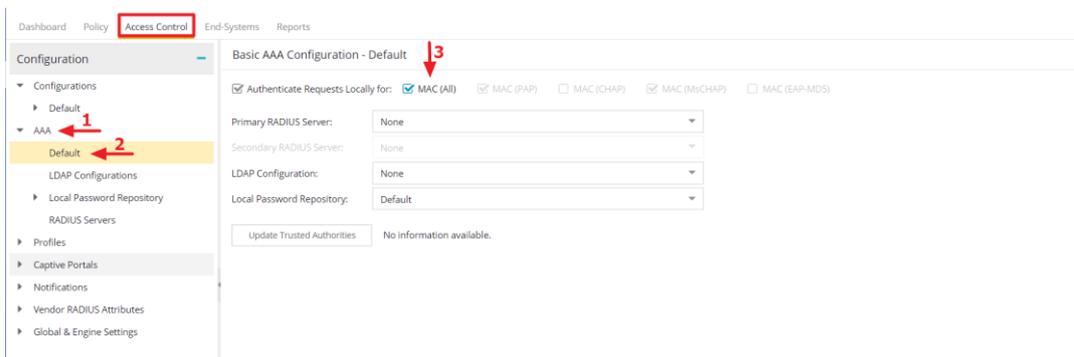


Captive Portal Authentication Configuration

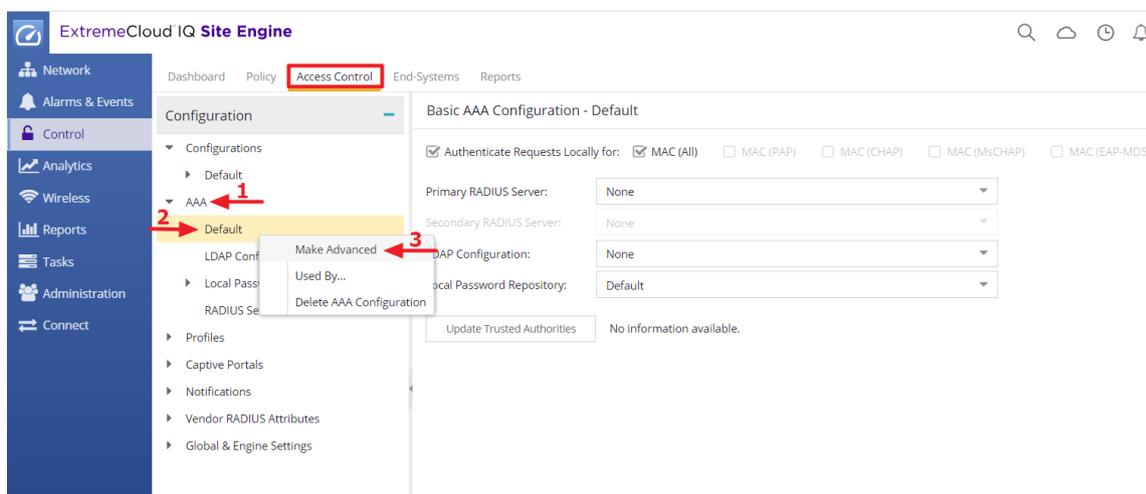
One of the most frequently used features within ExtremeControl is the Captive Portal for guest access. ExtremeControl provides a streamlined workflow for connecting a guest to the network while gathering as much information as possible for administrators.

MAC Authentication

When ExtremeControl is used as a Captive Portal server for guest registration, it authenticates guest users locally by the means of MAC authentication. To enable MAC authentication, in the **Access Control** configuration tree, navigate to the AAA menu option and select **Default**. For **Authenticate Request Locally** option, enable MAC (All) and Save.



While some configurations can be deployed using a basic AAA configuration, most deployments make use of an Advanced AAA configuration. This is accomplished by right-clicking Default under the AAA configuration and then selecting **Make Advanced** as shown below.

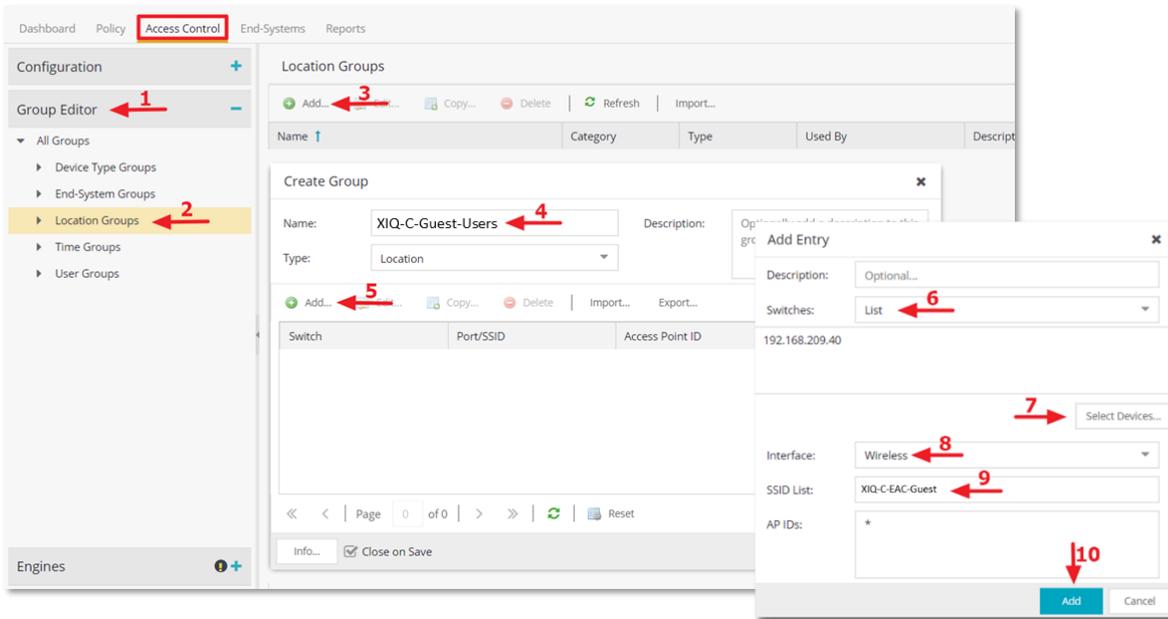


Location Group Configuration

A Location Group is a rule component that allows administrators to specify network access requirements or apply restrictions based on the network location that the end-user is connecting from. A new Location Group is created by selecting **Group Editor** and then the **Location Group** option.

On the **Create Group** pop-up screen, create a Location Group by specifying the XIQ-C controller IP address and SSID name. This Location Group is utilized to assign a Captive Portal policy to all the guest users that connect using the guest SSID on the XIQ-C.

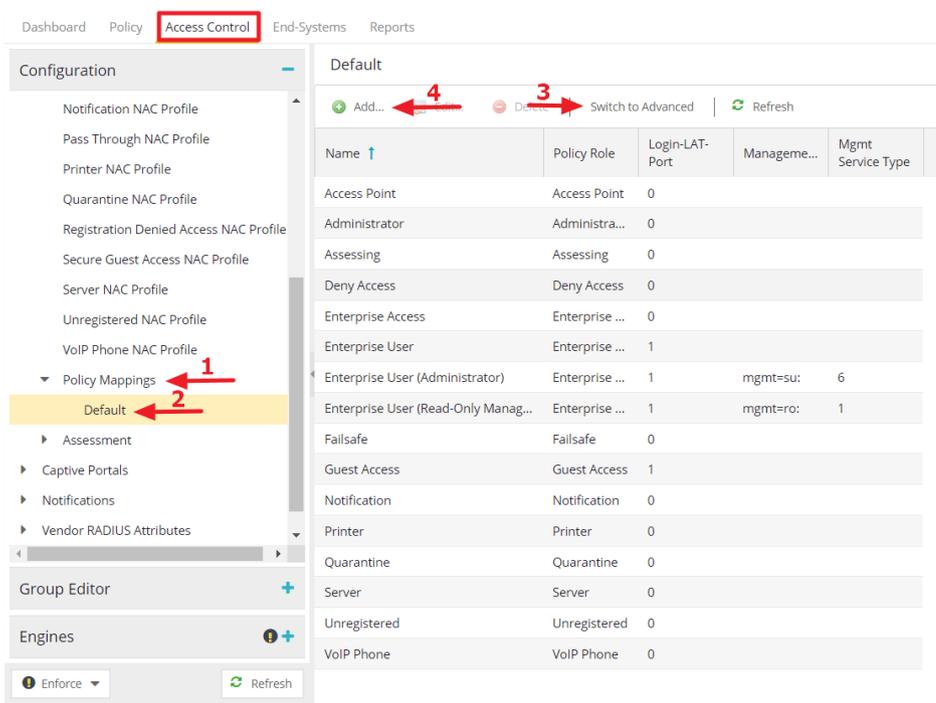
Note: Location Groups can be very granular and may contain AP ID/names, Site names, and Device Groups. For example, an administrator can create two Location Groups for the same guest SSID based on two different Sites or Device Groups, with each Site or Device Group utilizing different Roles or VLANs. Therefore, effectively allowing the guest users to connect to the same SSID but receive different Roles, VLANs or FW rules based on their location.



Policy Mapping Configuration

In ExtremeControl profiles, each access Policy (Accept, Quarantine, Failsafe, and Assessment) is associated to a policy mapping that defines exactly how end-system traffic is handled on the network. Each mapping specifies a Policy Role and/or any additional RADIUS attributes included as part of a RADIUS response to a switch/controller.

It is not recommended to change the default **Unregistered** Policy Mapping, as it may be used by other network devices. Create a new policy mapping for the **Unregistered** role by navigating to the **Profiles** under the main **Configuration** tree menu. Select **Policy Mappings** and then select **Default, Switch to Advanced** to show policy details.



Add a new Policy mapping. Make sure that the name of this mapping is **Unregistered** and the **Map to Location** is set to the previously created Location Group. For the Policy Role, type **Unregistered role for <Network Name>**. MNote that the Policy Role name is case sensitive. Select **Apply** and then **Save** the settings.

Defining the Policy Role “Unregistered role for <Network Name>” is enough for ExtremeControl to send the correct role (Filter-ID Attribute) to XIQ-C. Upon receiving the Filter-ID, the XIQ-C matches it with the internally generated Unregistered role for the guest network i.e. “Unregistered role for <Network Name>” and the user is assigned this role until the guest registration is successful and a new Filter-ID is sent by the ExtremeControl.

As mentioned in the previous section, this “Unregistered role for <Network Name>” is automatically created on XIQ-C when a guest SSID is configured. This internal Unregistered role is unique to each guest network and contains the name of the guest network for which it was created, for example, “Unregistered role for XIQ-C-EAC-Guest” in this instance.

If a “Duplicate Policy Role” warning appears, select **Cancel** and then **Enforce** settings on the Access Control engine.

Captive Portal Configuration

Most POC installations include some level of Captive Portal integration. This can be a Guest Registration screen or an Authenticated Registration screen that is used for BYOD devices. ExtremeControl offers different types of workflows for guest access such as Captive Portal with AUP, SMS/Email verification and Sponsored Guest. In this guide, Guest Registration and Authenticated Registration Captive Portal workflows are used.

Guest Registration allows unauthenticated access to the network for the length of the registration. Registration also has provisions for capturing end-user specific information during the registration process. **Authenticated Registration** provides a way for existing corporate end users to access the network on end-systems that don't run 802.1X, by requiring them to authenticate to the network using the registration web page. After

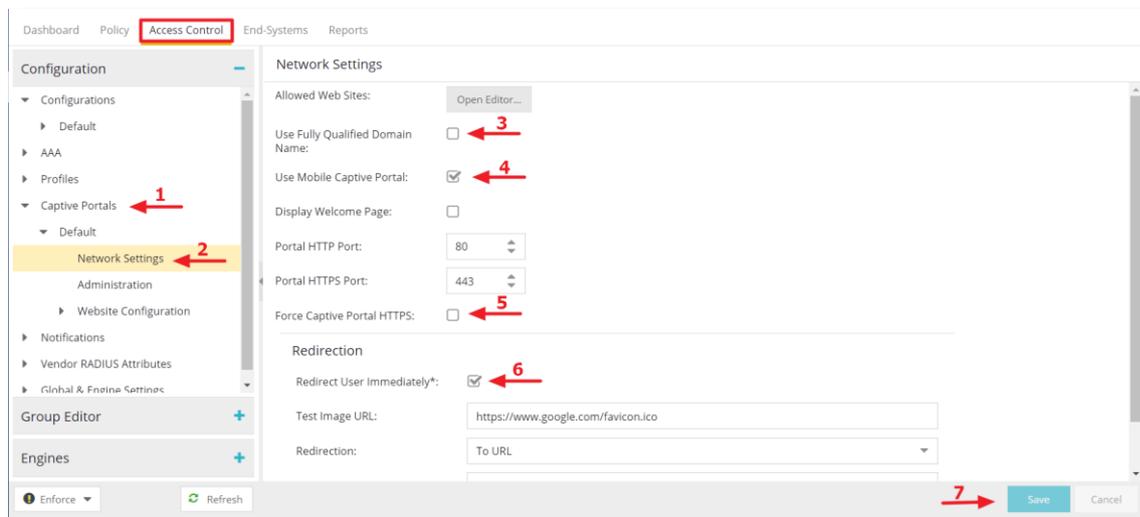
successful registration, the end-system is permitted access until the registration expires or is administratively revoked. Under the Access Control menu, go to Captive Portals then Network Settings and enable the following settings and save the configuration.

Use Fully Qualified Domain Name: When this is enabled, the user's browser does a DNS lookup to find the IP address for the fully qualified hostname of the ExtremeControl engine. Enable this option only if all ExtremeControl engines have their hostnames defined in DNS. Moreover, if SSL certificates are used for the captive portal splash pages, this option must be enabled to avoid certificate warnings.

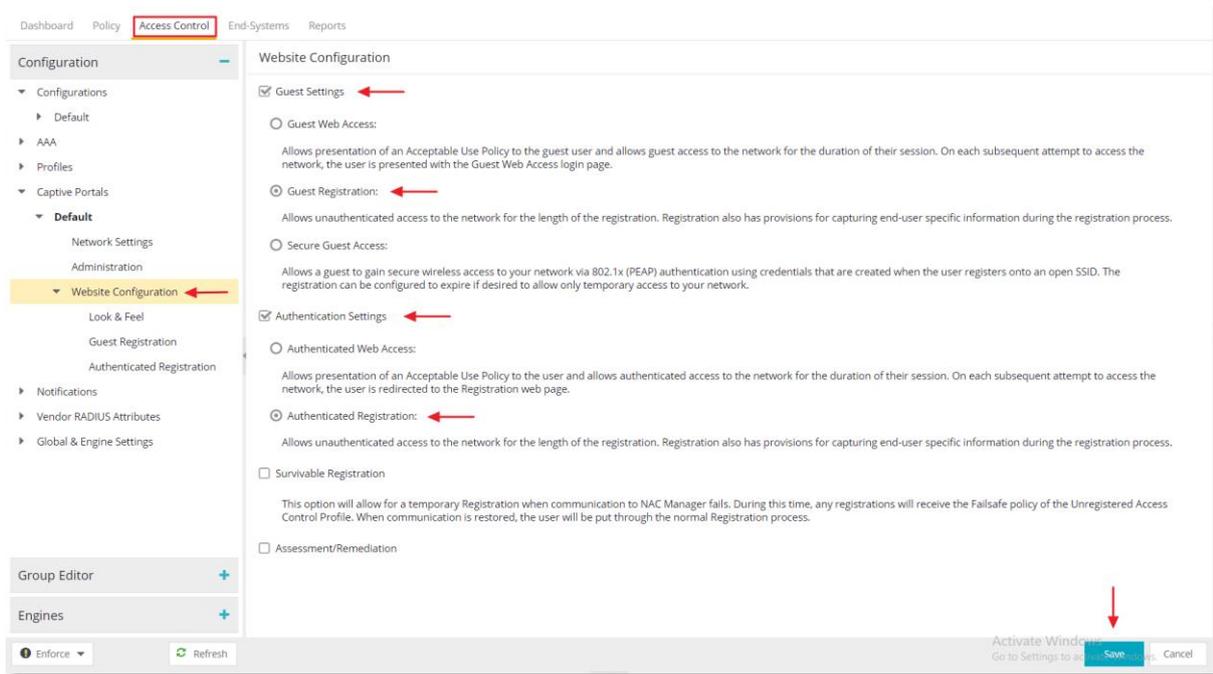
Use Mobile Captive Portal: Enabled

Force Captive Portal HTTPS: Select this checkbox to force captive portal web pages to be served securely over HTTPS (instead of HTTP) to end users on the network. Make sure the “Use HTTPS Connection” setting in the SSID configuration is also enabled to avoid Captive Portal redirection issues.

Redirect User Immediately: Enabled



In the **Website Configuration** screen, enable the Guest Settings and Authentication Settings and select **Guest Registration** and **Authenticated Registration** from the list of available options. These are the most typical settings for any installation as well as the best practice settings for a Proof of Concept. Save the settings.



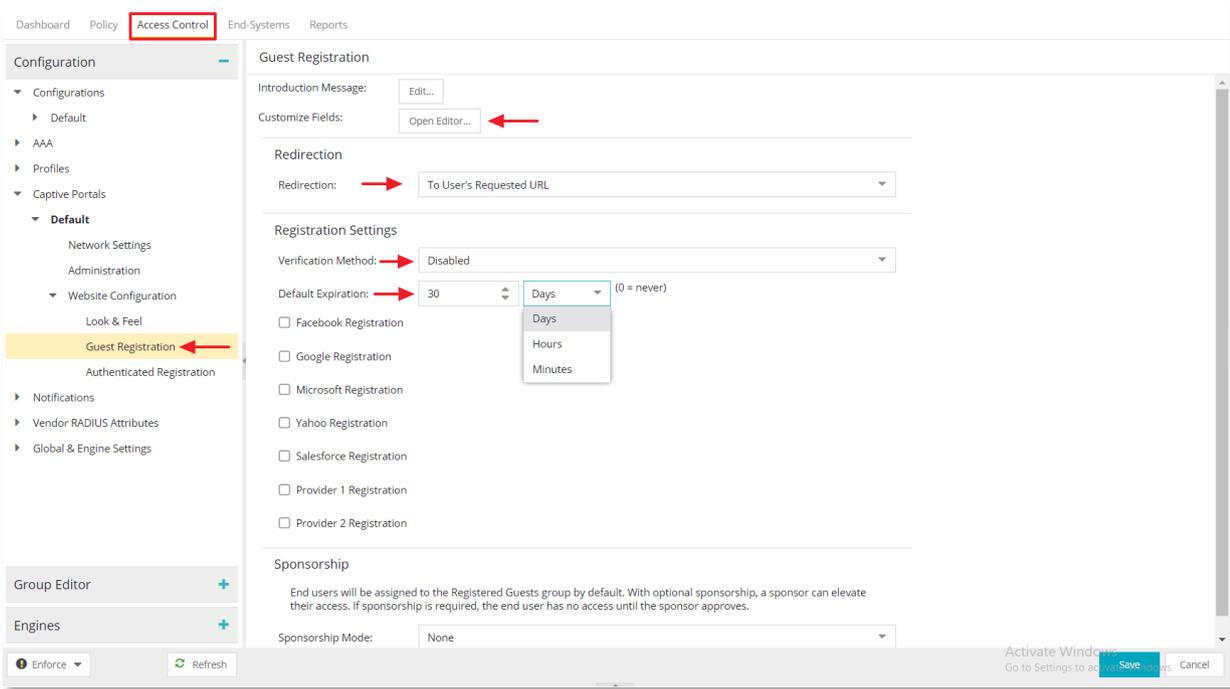
At this point if desired, the **Look & Feel** option under Website Configuration can be accessed to modify the appearance of the Captive Portal Splash page to be customer specific.

Guest Registration Settings

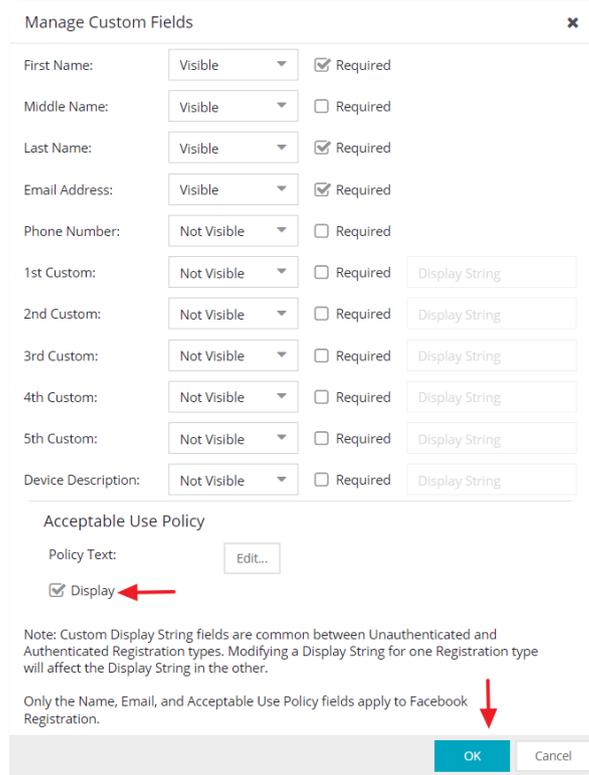
In the Guest Registration section, there are a few settings that are typically modified for each customer. The Redirection setting by default redirects the user to their originally requested URL after registration is completed. Alternatively, many customers prefer to have this setting redirect the user to the organization's homepage.

In the Registration Settings section, a verification method can be defined. A popular choice with many customers is to use SMS Text verification for guest users. However, for this guide the verification method is kept disabled.

Lastly, in the Registration Settings section, the **Default Expiration** should be configured for an amount of time (e.g. 30 days) to be specified by the customer. For the Guest Registration function in general, the fields that are required to be filled out should be reviewed and customized by selecting the **Open Editor** button.



In the Manage Custom Fields window, the fields presented to the user can be configured and it is common to have one or more custom fields specified. If the custom fields are made visible, be sure to enter the Display String that is displayed to the user. Additionally, it is common for an **Acceptable Use Policy** to be displayed to guests. If this is the case, select the checkbox for **Display** in that section. When complete, press the **OK** button to save the settings.

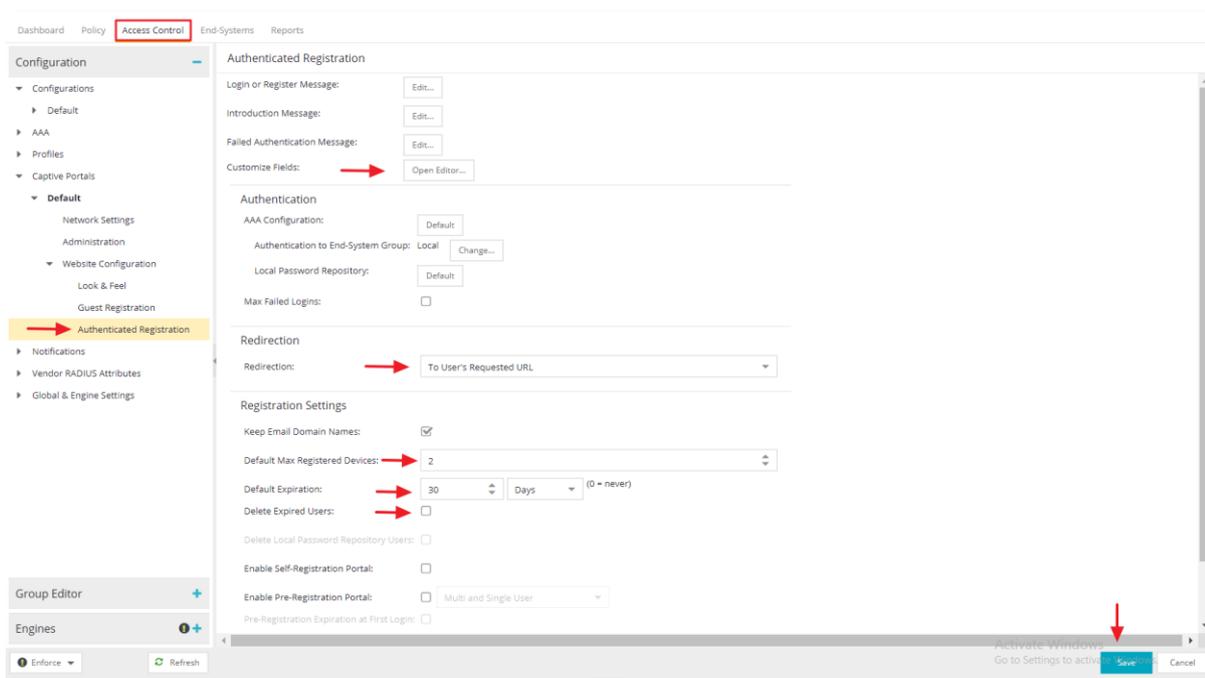


Authenticated Registration (BYOD) Settings

In the Authenticated Registration screen there are some settings that are similar to Guest Registration. One thing to note is that the Customize Fields section can have individual fields enabled or disabled, however, any phrasing for the Display Strings or Acceptable Use Policy is shared with Guest Registration. Two other common altered settings are the Redirection and the Default Expiration fields.

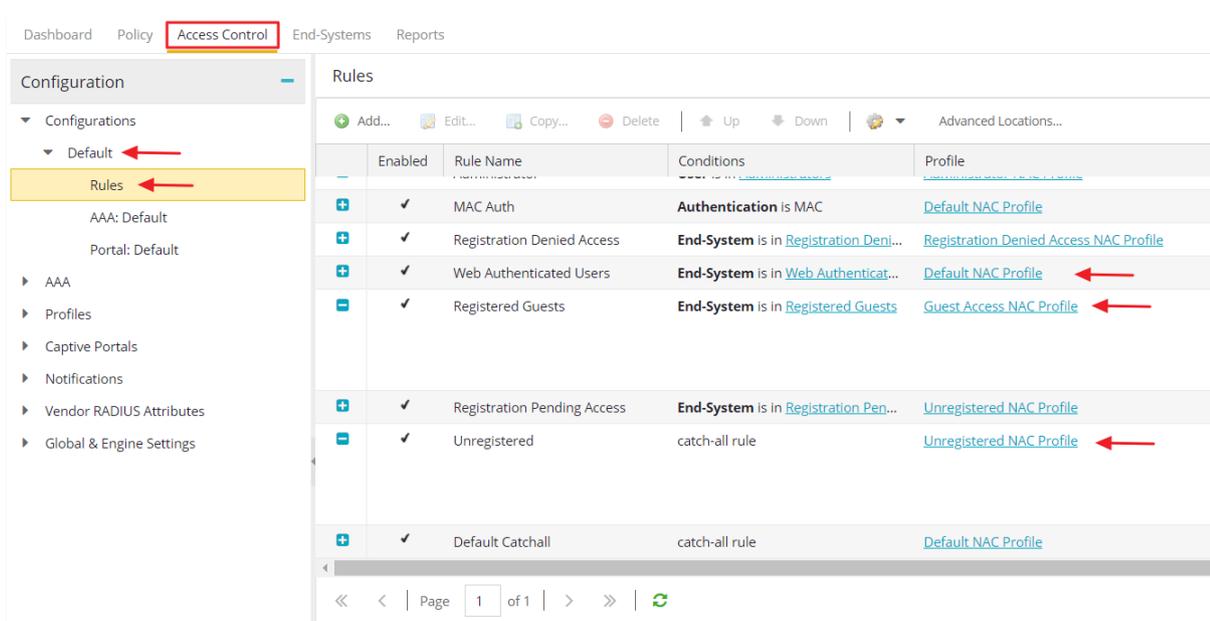
The first unique setting that should be modified is the **Default Max Registered Devices**. The default is two. The number of BYOD devices allowed to each user is typically dictated by the organization.

The next setting, **Delete Expired Users**, is typically left disabled. This will allow ExtremeControl to keep the user information from expired devices in order to expedite future registrations.

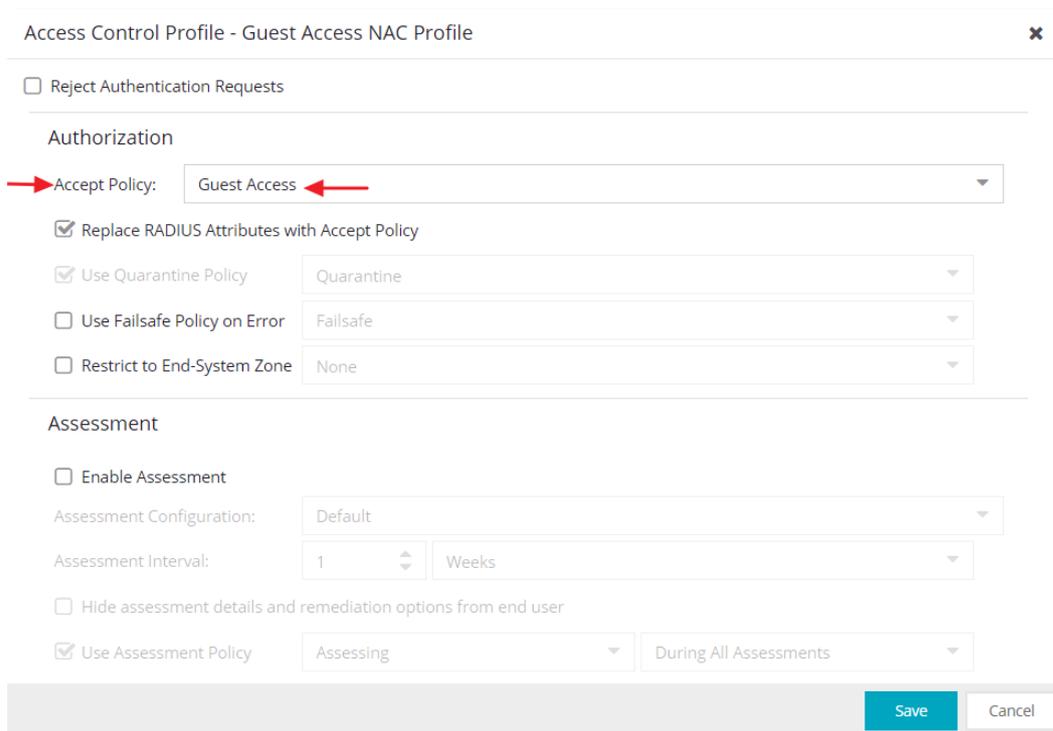


Guest Access Authentication Rules

When the Captive Portal settings are enabled, the Unregistered, Registered Guests, and Web Authenticated Users rules are added to the Default Rules. Navigate to **Configuration**, **Default** and then **Rules** to view the list of rules in the Rules Engine. Take note of these newly created rules and their resulting actions for particular end systems. Successfully registered guests will have their end systems added to the Registered Guests end system group. Likewise, authenticated users will have their devices added to the Web Authenticated Users end system group.



To verify and confirm that the Policy Roles for each of these rules will be returning a match with the Policy Roles configured on the XIQ-C, select the **Default NAC Profile**, **Guest Access NAC Profile**, and the **Unregistered NAC Profile** and check the **Accept Policy** field. This is the Filter-ID that ExtremeControl will return to the XIQ-C when a rule is successfully matched. As a result, the XIQ-C will match this Filter-ID with the Policy Roles mapped onto the AP profile. If a match is found, the user is assigned that role. Otherwise, the packet is dropped.



LDAP Configuration

ExtremeControl can perform 802.1X authentication and domain user lookup in a variety of ways. For environments that have RADIUS servers available, ExtremeControl can proxy the RADIUS request attributes to the RADIUS server. In deployment cases where a RADIUS server is not available, the ExtremeControl can act as a full RADIUS server and utilize the LDAP configuration to authenticate users against the Directory Service such as Microsoft Active Directory.

In this guide, ExtremeControl is integrated with Microsoft Active Directory via LDAP to perform username lookups for Autheticated Registration of BYOD users.

Active Directory Integration

Expand the **AAA** Configurations section of the **Access Control** Configuration tree and select **LDAP Configurations**. Create a new LDAP configuration.

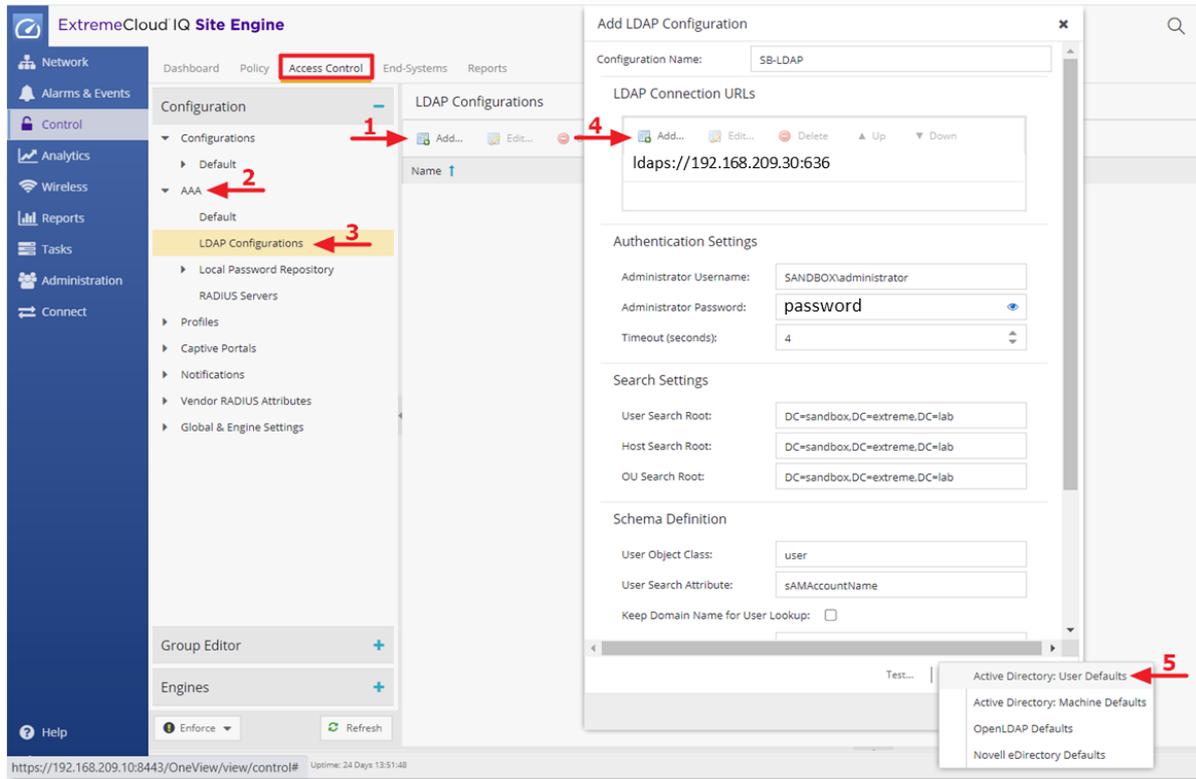
Use this table to add, edit, or delete connection URLs for the LDAP server and any backup servers to be configured (The backup servers are redundant servers containing the same directory information.)

The format for the connection URL is `ldap://host:port` where host equals hostname or IP address, and the default port is 389. For example, `ldap://10.20.30.40:389`. If a secure connection is used, the format is `ldaps://host:port` and the default port is 636.

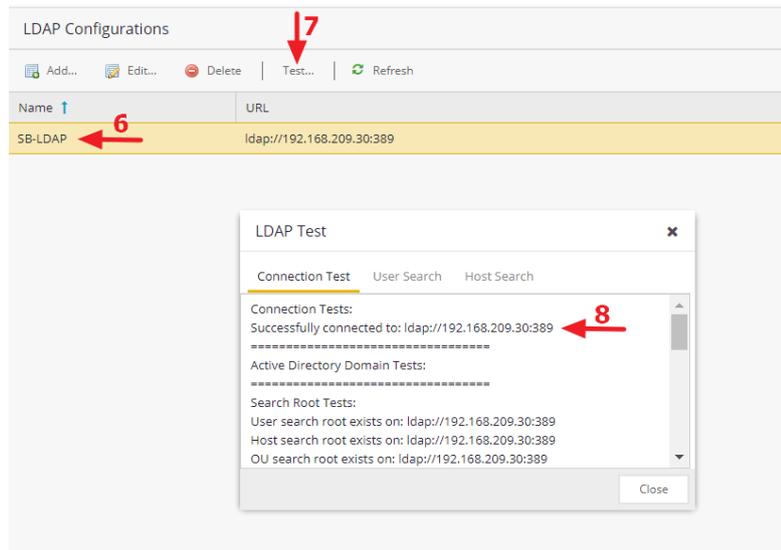
Enter the administrator username and password that will be used to connect to the LDAP server to make queries. The credentials only need to provide read access to the LDAP server.

Under the Search Settings, for the three fields, enter the root node of the LDAP server. To improve search performance, you can specify a sub tree node to confine the search to a specific section of the directory. The search root format should be a DN (Distinguished Name).

There are default values that can be selected to pre-fill the schema definition. For an Active Directory domain in a POC, select the **Populate Default Values** option in the bottom right of the screen and select the **Active Directory: User Defaults** option.



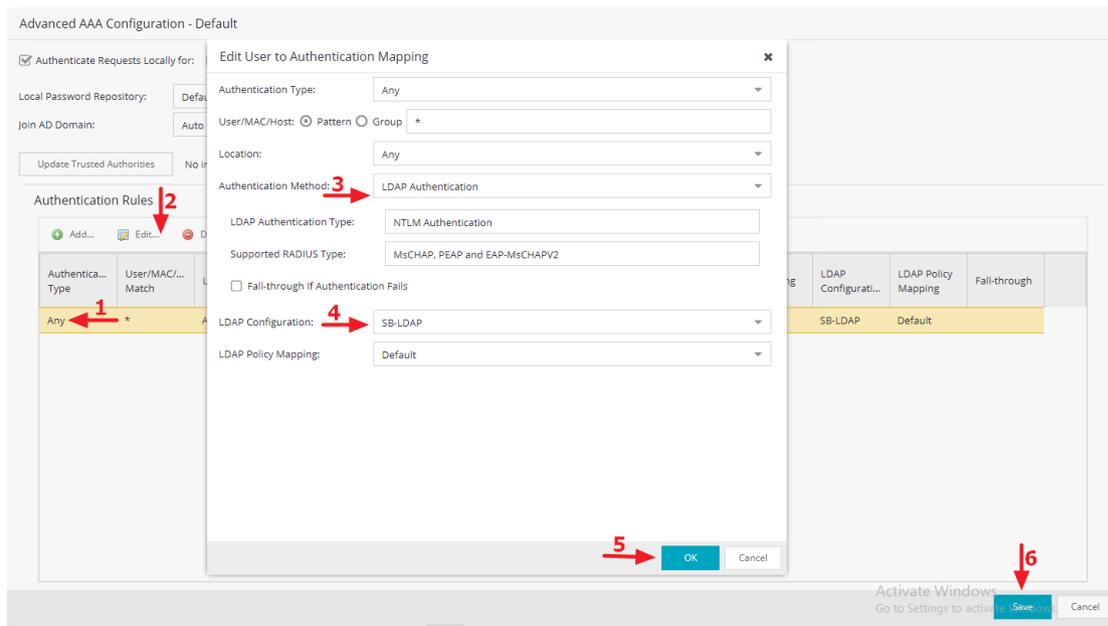
Test the LDAP integration by selecting the **LDAP** configuration profile and then **Test**. Note that Access Control has successfully established the connection with Active Directory server.



Once the connection test is successful, a **User Search** can be performed to verify users can be found.

AAA Rules

On the Advanced AAA Configuration screen, go to **Authentication Rules** and edit the Default rule. For ExtremeControl to authenticate users against the Active Directory, modify the rule by changing the **Authentication Method** to **LDAP Authentication**. Once that setting is selected, the LDAP Authentication Type should show as NTLM Authentication with the supported RADIUS types listed below. It is recommended to enable **Fall-through if Authentication Fails** option to authenticate against the next AAA authentication rule in case the first AAA authentication rule results in an authentication failure or the directory service is unreachable. Select the LDAP policy from the LDAP Configuration drop-down menu, make sure to save all the changes made to the AAA Authentication Rule by selecting the **Save** button.

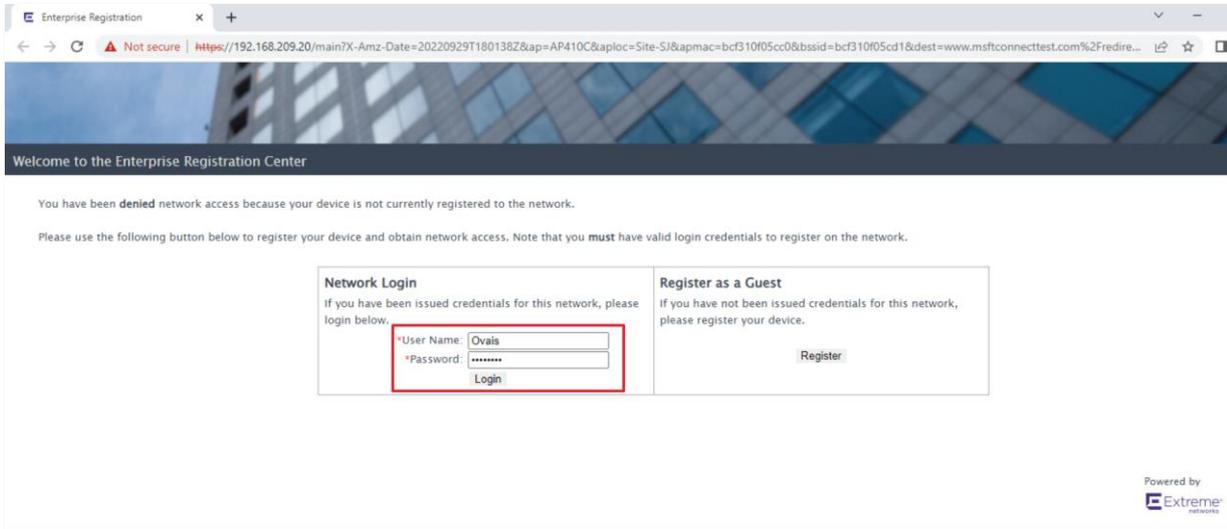


Part 6: Configuration Validation

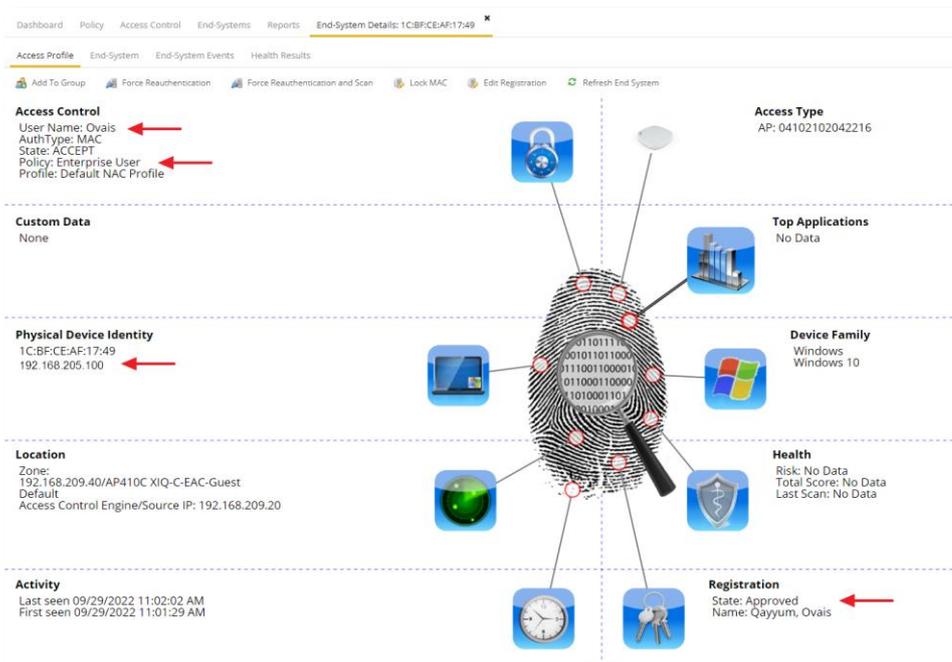
Validate the Captive Portal configuration by connecting an end-system to the guest SSID. The end system’s web traffic should be redirected to ExtremeControl and the Captive Portal should display both Guest Registration and Authenticated Registration options.

Authenticated Registration (BYOD)

Log into the Authenticated Registration side with a valid username and password to ensure LDAP authentication is working properly.



The Acceptable Use Policy is presented. After the registration is completed, the end-system should be added to the network with the associated username. Additionally, the registration information for the user is now displayed in the End-System Details.



One of the most important aspects of this integration that must be checked is to ensure that both the XIQ-C and ExtremeControl are aware of the end-system session. The end-system session details such as Role assignment, IP address, and First and Last seen time must be in sync between XIQ-C and ExtremeControl.

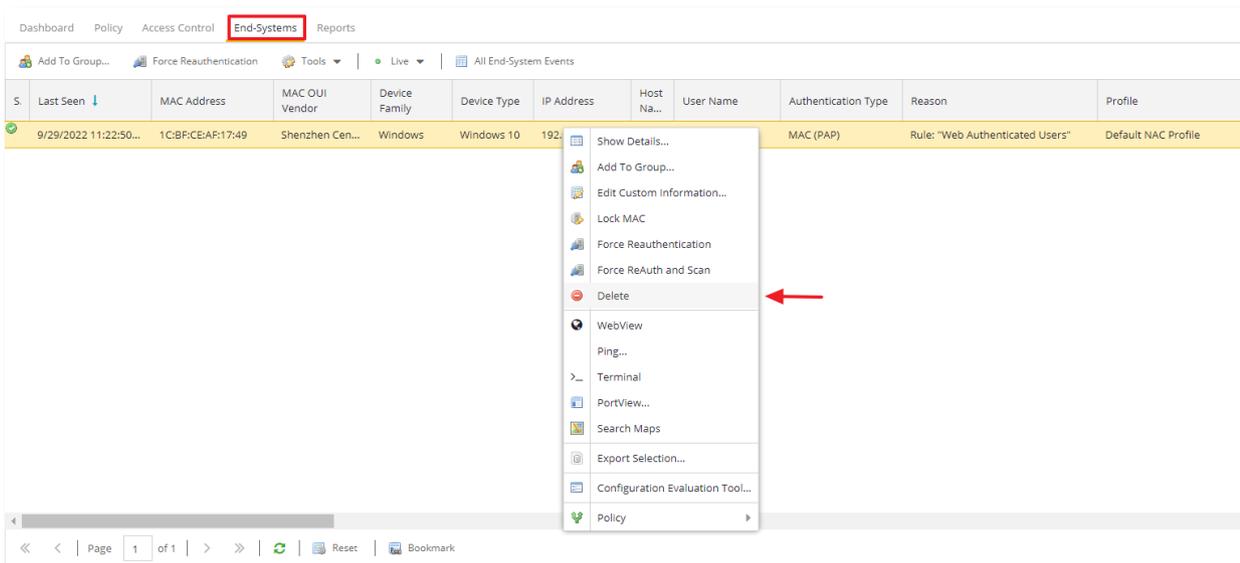
Log into the XIQ-C and navigate to **Monitor** in the main configuration menu. Select the **Clients** tab and review end-system details.



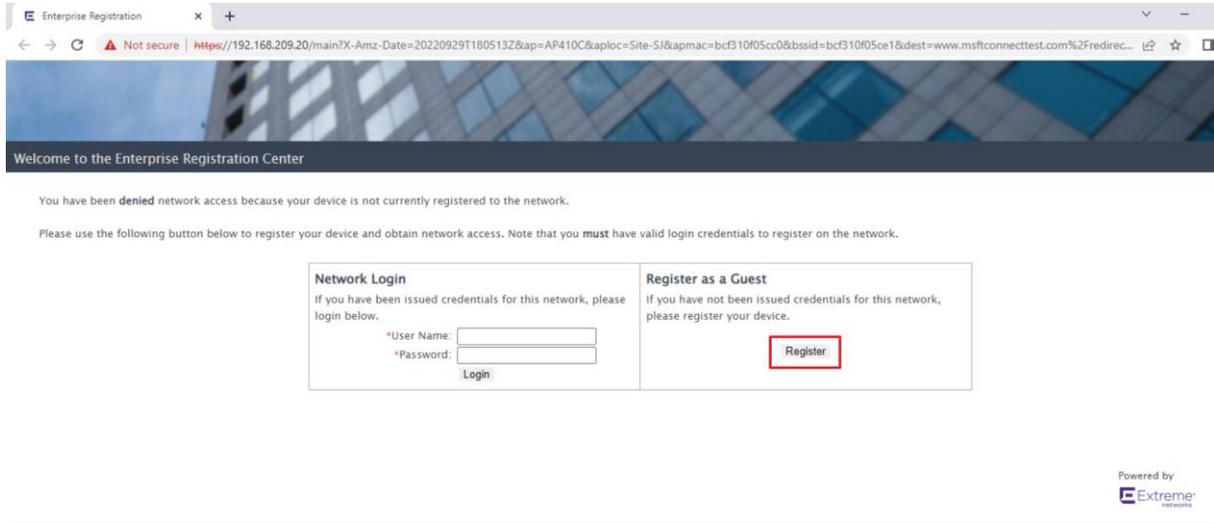
Ensure that the test client has acquired an IP address from the designated BYOD user VLAN and the XIQ-C has assigned the Enterprise User role to the test client proving that ExtremeControl has returned the correct role “Enterprise User” via the Filter-ID.

Guest Registration

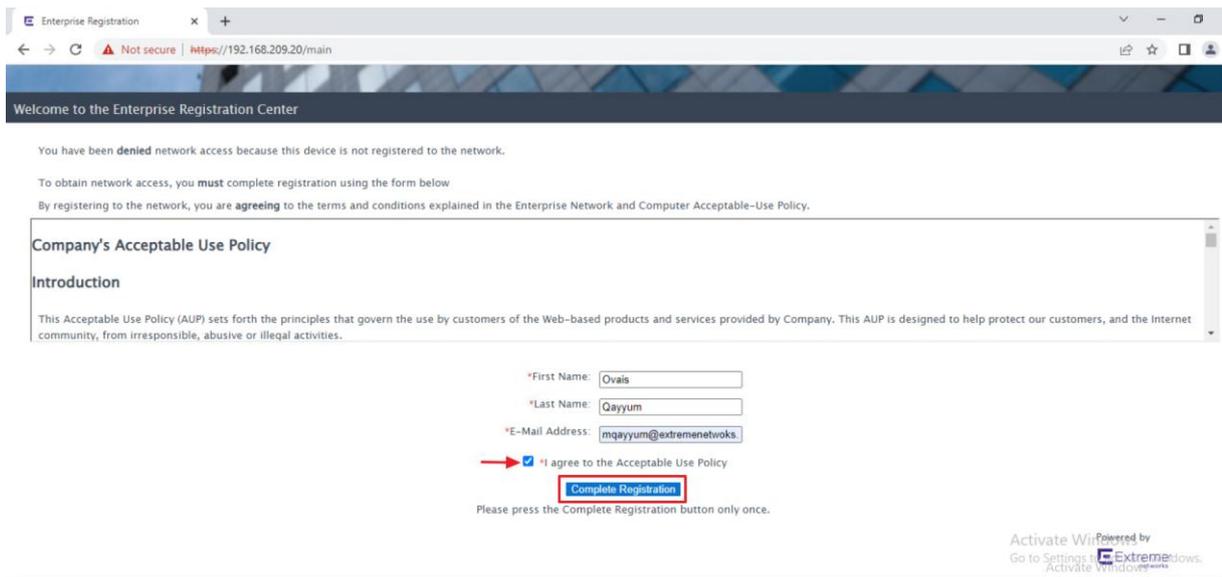
To test Guest Registration, the same device can be used, but it will need to be deleted from the end-system table by right-clicking it and selecting Delete.



Returning to the client device, the registration page is presented again when another attempt is made to open a new web page. Select the **Register** button to log in using guest registration.



In the registration screen, fill out all identity fields, select the checkbox to agree to the Acceptable Use Policy, and then select the **Complete Registration** button.



Once registration is complete, the device is assigned Guest Access role and the registration information for the device is populated in the End System table.

Access Control
 User Name: Qayyum, Ovais
 AuthType: MAC
 State: ACCEPT
 Policy: Guest Access
 Profile: Guest Access NAC Profile

Custom Data
 None

Physical Device Identity
 1C:BF:CE:AF:17:49
 192.168.204.100

Location
 Zone:
 192.168.209.40/AP410C XIQ-C-EAC-Guest
 Default
 Access Control Engine/Source IP: 192.168.209.20

Activity
 Last seen 09/29/2022 11:07:10 AM
 First seen 09/29/2022 11:06:49 AM

Access Type
 AP: 04102102042216

Top Applications
 No Data

Device Family
 Windows
 Windows 10

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

Registration
 State: Approved
 Name: Qayyum, Ovais

Ensure that the test client has acquired an IP address from the Guest VLAN and that XIQ-C has assigned the Guest Access role to the test client. This confirms that ExtremeControl has returned the correct role, Guest Access, via the Filter-ID.

ExtremeCloud IQ Controller

Clients Auto Refresh OFF

Filter visible rows

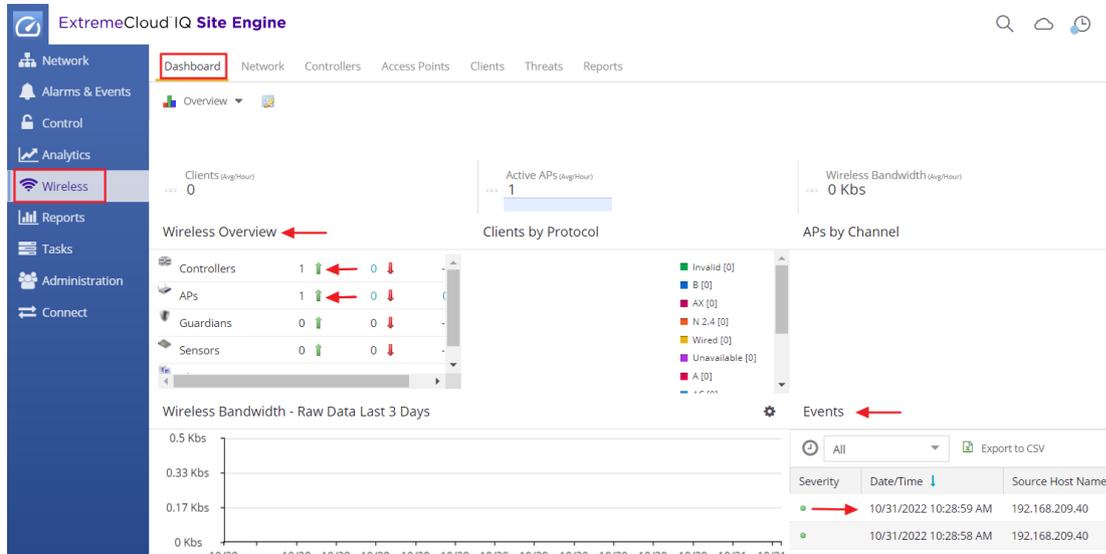
Status	IP Address	Hostname	Site name	Last seen	Device Type	AP	Username	Role	Network
●	192.168.204.100 IPv6	PC	Site-Sj	Sep 29, 2022 11:07:33 AM	Windows 8/ 8.1/ 10/ 11/ ...	AP410C		Guest Access	XIQ-C-EAC-Guest

Wireless Management Statistics

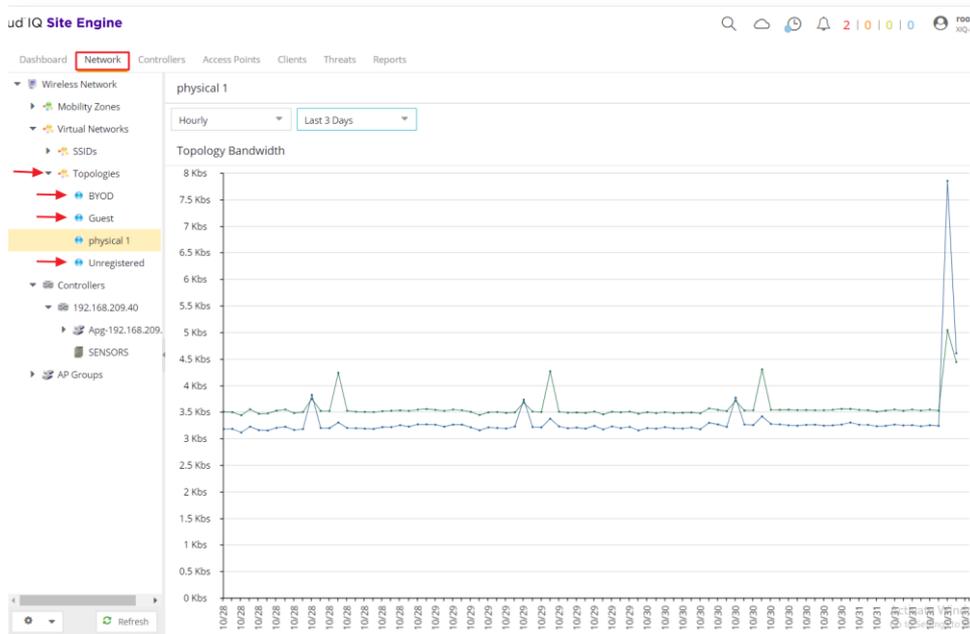
The **Wireless** tab in Site Engine provides dashboards and detailed charts to help monitor the overall status of the wireless network.

To view wireless reporting data, the **Wireless Controller Statistics Collection** option must be enabled for the XIQ-C (this was previously accomplished in the [Enable XIQ-C Statistics Collection](#) section of this guide). When the Wireless Controller statistics collection is enabled, Wireless Controller, WLAN, Topology, and AP wired and wireless statistics is populated within Site Engine.

Select the **Wireless** tab from the Site Engine main-menu and select **Dashboard**. Review the wireless network information presented in the form of different widgets such as **Wireless Overview** and **Events**. Notice the **Controllers** and **APs** icons appear **UP/Online** which indicate that XIQ-C has successfully established a connection with the Site Engine Wireless Management module and data is being collected.



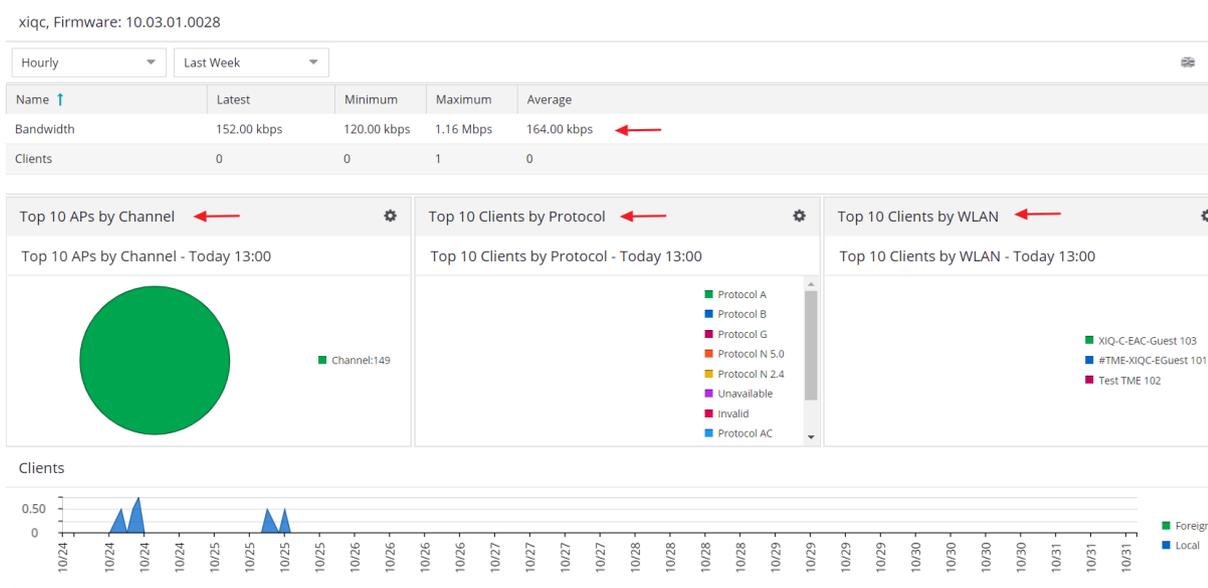
Use the **Network** tab to view wireless network related statistics such as SSIDs and Topologies. Select the **Topologies** menu to check the utilization of each VLAN and confirm that the VLANs configured on XIQ-C are reported correctly.



The **Controllers** tab displays summary information for each controller.

Controller ↑	Clients	Bandwidth	Active APs	Role	Mobility Zone	Version	Client History	Availability
192.168.209.40	0	7.12 Kbs	1	None		10.02.01.0...		

Select the controller IP address link to open a report that shows APs by channel, clients by protocol, clients by WLAN, clients, and bandwidth usage information for just that controller.



The **Access Points** tab displays summary information for all the Access Points in the wireless network. Select an AP to open an in-depth AP Summary view for the selected AP.

St...	Name	IP Address	MAC Address	Controller	Controller Version	AP Version	Family	AP HW Type
●	AP410C	192.168.209...	BC:F3:10:F0:5C:C0	192.168.209...	10.02.01.0029	10.1.0.0-036R	AP410	Wireless AP410C-FCC In...

Select the **Network Information** to review **Wireless Details**.

Dashboard Network Controllers Access Points Clients Threats Reports AP PortView: AP410C ✕

192.168.209.100 04102102042216

Overview Network Information ←

Wireless Details ← AP History

Controller - XIQ-C-XIQSE-SB 192.168.209.40

Availability Status: Standalone	Pair IP: Standalone	VNS Count: 0
Physical Ports: 3	Total APs: 1	VN Local Clients: 0
Clients: 0	Active APs: 1	VN Foreign Clients: 0
Tunnels: 0	AP Registration Requests: 1	VN Total Clients: 0
Tunnels TX/RX Bandwidth: 0 bps	Uptime: 72 Days 23:03:13	

AP - AP410C Role: Access Point Location: Site-SJ

IP Address: 192.168.209.100	Status: Approved	State: Active
MAC Address: BC:F3:10:F0:5C:C0	Clients: 0	Uptime: 1 Day 02:39:10
Serial Number: 04102102042216		Protocols in Use: None
Home: Local		

Radio 1 2.4 GHz Protocol: b/g

Channel: None	Discards (in/out): 0 pps/0 pps	Current Power Level: 0 dBm
	Errors (in/out): 0 pps/0 pps	Minimum Basic Rate: 1
	Bandwidth (in/out): 0 bps/0 bps	Average Busy Channel %: 0
	Unicasts (in/out): 0 pps/0 pps	Maximum Busy Channel %: 0
	Multicasts (in/out): 0 pps/0 pps	Average RX Channel Utilization: 0
	Broadcasts (in/out): 0 pps/0 pps	Maximum RX Channel Utilization: 0

At this point, the XIQ-C integration with the Site Engine, Policy Manager and ExtremeControl is complete and the Site Engine user interface can be used as a “Single Pane of Glass” for monitoring and managing wireless clients.

Since the RFC-3576 (CoA) has been enabled as part of the ExtremeControl configuration, it allows an administrator to delete, re-authenticate and assign new Policy roles to a wireless client directly from the Access Control engine’s End-Systems tab without having to log into the XIQ-C user interface.

Revision History

Date	Revision	Changes Made	Author
13/09/2022	1.0	First draft	Ovais Qayyum
03/10/2022	1.1	Added BYOD Captive Portal configuration	Ovais Qayyum
14/10/2022	1.1	Review	Tyler Marcotte, Zdenek Pala
17/10/2022	1.2	Added CLI and Policy Manager configuration.	Ovais Qayyum
07/11/2022	1.3	Added XIQ-SE Wireless Management validation section.	Ovais Qayyum