ExtremeGuest™ v6.0.1 How-To Guide for ExtremeGuest™ – ExtremeCloud Appliance™ Integration

For Centralized Deployments

Abstract: **This guide describes the configurations required to deploy ExtremeGuest™ as the external guest registration and authentication server for ExtremeCloud Appliance managed centralized networks. It will help you to configure ExtremeGuest as the external hotspot server for access points adopted to ExtremeCloud Appliance and deployed in a Centralized site.**

Published: **September 2019**

Extreme Networks, Inc.

Phone / +1 408.579.2800
Toll-free / +1 888.257.3000
www.extremenetworks.com

9036485-00 Rev AA

Contents

I Pre-requisites

You will need:

- ExtremeGuest running version 6.0.1
- ExtremeCloud Appliance running version 4.56.01 or 4.56.02
- Extreme Networks Access Points:
  - AP505i and AP510i/e running version WiNG 7.x.x
    OR
  - AP39xx running version 10.51

II ExtremeGuest Overview

ExtremeGuest is a robust and comprehensive guest management and engagement solution that personalizes engagement by understanding guest-user behavior and interest, and then tailor services based on those insights.

ExtremeGuest offers the following features:

- Unified Guest Access Deployment, Analytics and Management for Wireless and Wired networks
- A robust captive- portal splash template builder
- Splash template management
- Location and network-based captive-portal support
- Dashboard based report builder
- REST API support

Starting with this release, ExtremeCloud Appliance managed centralized and distributed deployments can use ExtremeGuest as the external wireless-guest registration and authentication server. ExtremeGuest collects guest analytics and information from the ExtremeCloud Appliance captive portal while providing additional access control settings, centralized splash page distribution, and new social media authentication methods.

III ExtremeCloud Appliance Overview

ExtremeCloud Appliance offers a streamlined customer experience with a common platform and operating system across multiple Extreme Networks products. It combines the power of ExtremeWireless and Extreme Management Center with the flexibility of ExtremeCloud in one easy-to-use platform. ExtremeCloud Appliance offers the following features:

- Integrated Access Control
- Integrated Maps
- Historical data charts
- Programmable REST API
- On-premise standalone deployment with integration into Cloud/XMC and on-premise services
- Clustered support for load sharing and resilience

The appliance is a network device designed to integrate with an existing wired Local Area Network (LAN). The ExtremeCloud Appliance provides both distributed and centralized management, network access, and routing to wireless devices that use Wireless APs to access the network.

III.A The Appliance

The appliance provides the following functionality:

- Controls and configures wireless APs, providing distributed or centralized management.
- Authenticates wireless devices that contact a wireless AP.
- Assigns each wireless device to a network service when it connects.
- Routes traffic from wireless devices, using a network service, to the wired network.
- Applies filtering roles to the wireless device session.
- Provides session logging and accounting capability.

III.B Wireless AP Overview

Extreme Networks APs use the 802.11 wireless standards (802.11a/b/g/n/ac) for network communications, and bridge network traffic to an Ethernet LAN. In addition to the wireless APs that run proprietary software and communicate with an appliance only, Extreme Networks offers a Cloud-enabled AP. The AP39xx series are Cloud-enabled APs that inter-operate fully with ExtremeCloud™ and other ExtremeWireless products.

ExtremeCloud Appliance supports APs that can be depolyed in the Centralized and Distributed modes.

A *Centralized* site topology allows seamless roaming within one geographic location. A Centralized configuration uses the following AP models:

- AP505i
- AP510i/e
- AP3917i/e/k
- AP3916ic
- AP3915i/e
- AP3912i
- AP3935i/e
- AP3965i/e

A *Distributed* site topology supports scaled-out deployments. A Distributed configuration uses the following AP models:

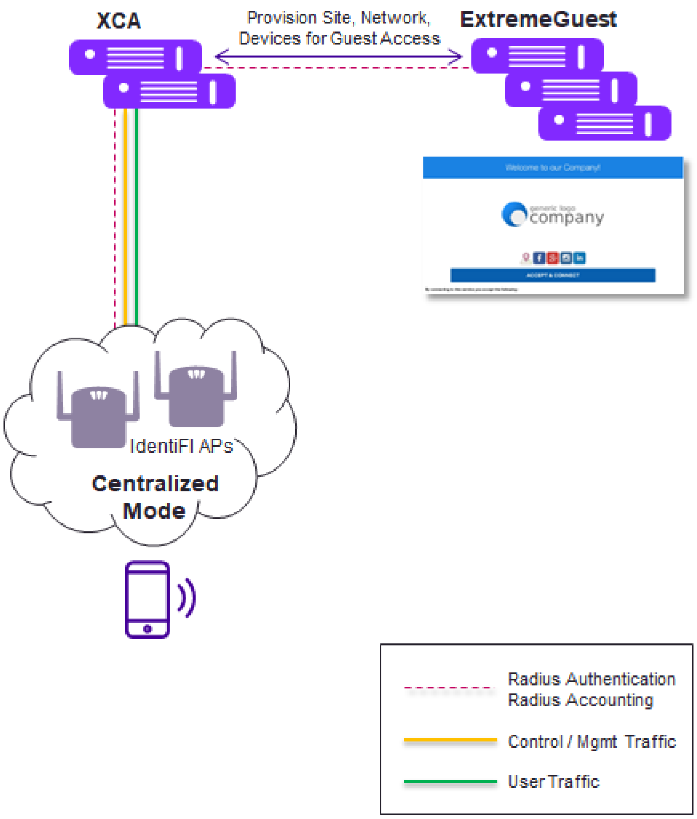
- AP505i
- AP510i/e
- AP7522
- AP7532
- AP7562
- AP7612
- AP7632
- AP7662
- AP8432
- AP8533

Note
The 802.11ax AP5XX model access points are dual-mode APs, capable of operating in Centralized and Distributed deployments.

IV ExtremeGuest – ExtremeCloud Appliance Centralized Deployment

IV.A Deployment Scenario

The following diagram outlines a typical ExtremeGuest deployment with captive-portal server and pages hosted on the ExtremeGuest server, while RADIUS communication is proxied via the ExtremeCloud Appliance server.



IV.B How it works

- When a first-time, unregistered wireless guest attempts network access, the AP tries authenticating the guest.
- If the ExtremeCloud Appliance managed centralized network is captive-portal enabled, with the captive-portal type set to "**Extreme Guest**", the access request is forwarded by ***ExtremeCloud Appliance*** to ExtremeGuest. The "**username/password**" in the request is set to the client's MAC address.
- Although the ExtremeGuest database has no records of the client (since the client is unregistered), it accepts the request.

  The protocol is designed to enable ExtremeGuest accept access requests from unregistered guests received by APs adopted to ExtremeCloud Appliance in a centralized deployment.
- ExtremeGuest initiates the **Onboarding** process:
  - adds the guest's MAC address to the database and assigns the "**Unregistered**" role to the guest.
  - then redirects the guest to the landing page, where the guest registers.
- During onboarding,
  - If the guest registration-type is set to "**Device**" – ExtremeCloud Appliance uses *MAC Authentication* to authenticate the client. Since the client's MAC address is added to ExtremeGuest database, client authentication is successful.

  - If the guest registration-type is set to "**OTP**" – ExtremeGuest sends a passcode via email/sms depending on the notification policy specification. The guest is redirected to the landing page, where the guest enters the credentials. *ExtremeCloud Appliance* authenticates the *username/password* entered and provides network access. Subsequent sign-ins to the same network does not require the client to authenticate until the registration is valid and not time-out
  - If the guest registration-type is set to "**User**" – ExtremeGuest sends a passcode via email/sms depending on the notification policy specification. The guest is redirected to the landing page, where the guest enters the credentials. *ExtremeCloud Appliance* authenticates the *username/password* entered and provides network access. Subsequent sign-ins to the same network requires the guest to provide the credentials for authentication.
- On successful authentication – ExtremeGuest returns Access-Accept with Filter-Id set to the group assigned to the client during onboarding.
- On failed authentication – ExtremeGuest returns Access-Reject.

The following sets of configuration are required to enable communication between the ExtremeGuest and ExtremeCloud Appliance servers:

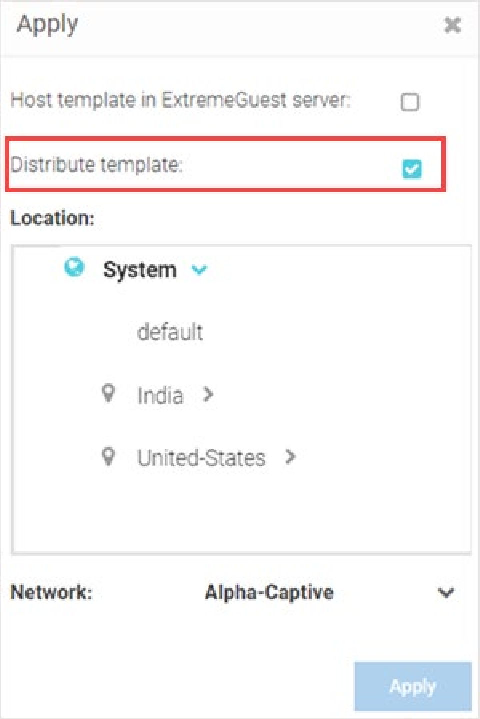
ExtremeCloud Appliance Configuration - configurations to be made on the ExtremeCloud Appliance server.

ExtremeGuest Configuration – configurations to be made on the ExtremeGuest captive-portal server.

V ExtremeGuest – Centralized Deployment Limitations

The following ExtremeGuest features are not supported:

- Splash template distribution. ExtremeGuest – ExtremeCloud Appliance centralized deployment does not support splash templates to be hosted on the APs. Splash templates have to be hosted on the ExtremeGuest server.



Apply

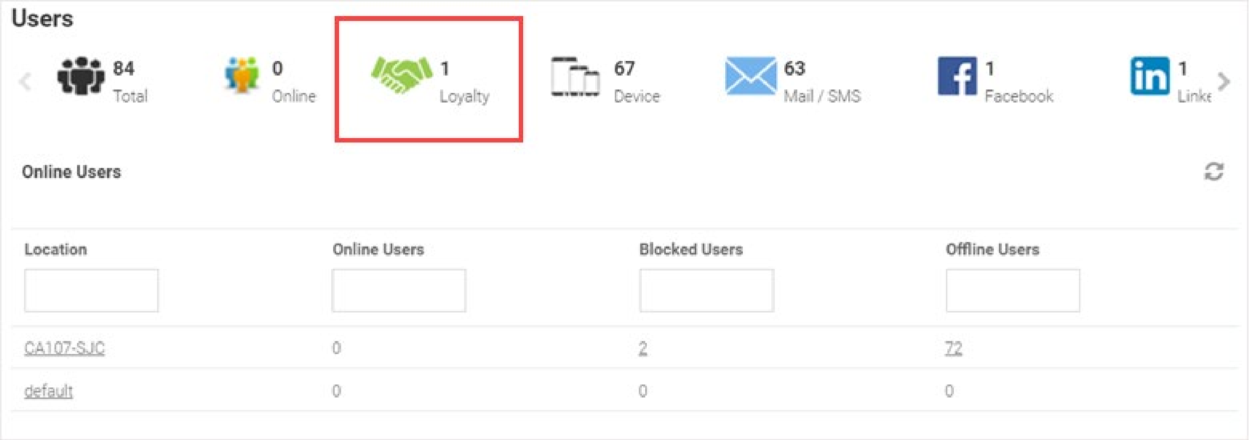
Host template in ExtremeGuest server: ☐

Distribute template: ☑

Location:

Network: Alpha-Captive

- Loyalty-client detection and reporting. Loyalty clients connected to APs adopted to ExtremeCloud Appliance in the centralized mode are not detected and reported.



Users

84	0	1	67	63	1	1
Total	Online	Loyalty	Device	Mail / SMS	Facebook	Linke

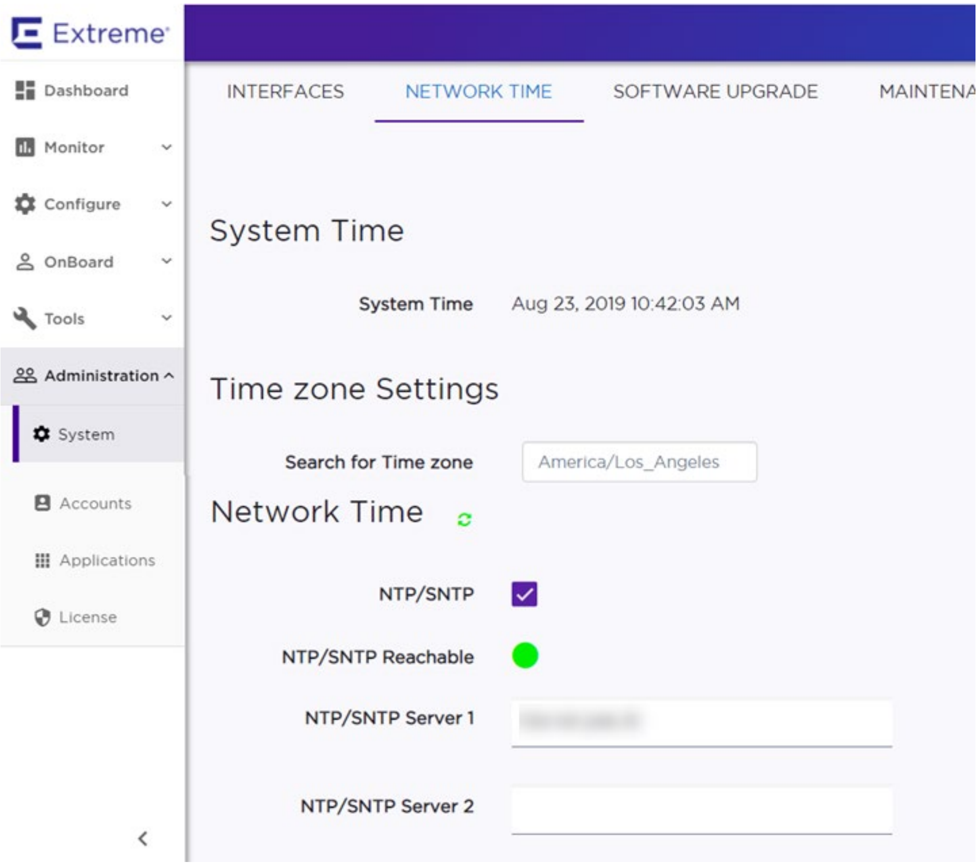
Online Users

Location	Online Users	Blocked Users	Offline Users
CA107-SJC	0	2	72
default	0	0	0

VI Pre-configuration

Enable NTP server on ExtremeCoud Appliance and ExtremeGuest. Enabling NTP ensures the Event-Timestamp (AVP code 55) in Accounting Request and Answer messages includes the actual time of the event, which represents the time, in seconds, lapsed since January 01, 1900.

VI.A ExtremeCloud Appliance NTP Configuration



System Time

System Time: Aug 23, 2019 10:42:03 AM

Time zone Settings

Search for Time zone: America/Los_Angeles

Network Time

NTP/SNTP: ☑

NTP/SNTP Reachable: ●

NTP/SNTP Server 1: [redacted]

NTP/SNTP Server 2:

To configure NTP server:

1. Login to **ExtremeCloud Appliance** and go to **System > Network Times**.
2. Set the timezone.
3. Select **NTP/SNTP** to enable the NTP/SNTP Server configuration options.
4. In the **NTP/SNTP Server 1** field, enter the primary NTP/SNTP server's IP address.
5. Optionally, in the **NTP/SNTP Server 2** field, enter the secondary NTP/SNTP server's IP address.

> **Note**
>
> The **NTP/SNTP Reachable** icon appears Green if the server is reachable. It appears Red if the server is unreachable.

VI.B ExtremeGuest NTP Configuration

To configure NTP server:

1. Login in to the **ExtremeGuest** server CLI.
2. Navigate to the server's device configuration context.

```
Test-ExtremeGuest>en

Test-ExtremeGuest#config

Test-ExtremeGuest(config)#self

Test-ExtremeGuest(config-device-00-0C-29-5D-54-64)#
```

3. Configure the NTP server's IP address.

```
Test-ExtremeGuest(config-device-00-0C-29-5D-54-64)#ntp server 1.2.3.4
```

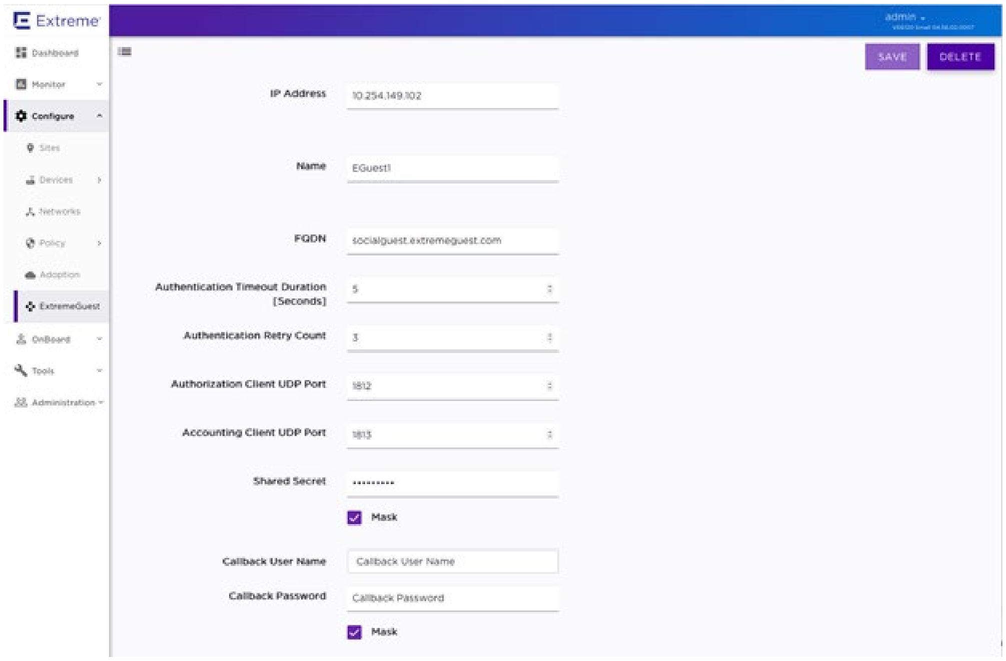
VII ExtremeCloud Appliance Configuration

Follow the steps below to integrate ExtremeGuest 6.0.1 with ExtremeCloud Appliance v10.56..01 or v10.56.02.

- Configure the ExtremeGuest Server IP Address
- Configure a Centralized Site
- Configure a Device Group
- Edit Configuration Profile of AP
- Apply Device Group to the Centralized Site
- Configure an Extreme Guest Enabled Network
- Add Walled-Garden Rules

VII.A Configure the ExtremeGuest Server IP Address

ExtremeCloud Appliance Configuration



IP Address	10.254.149.102
Name	EGuest1
FQDN	socialguest.extremeguest.com
Authentication Timeout Duration [Seconds]	5
Authentication Retry Count	3
Authorization Client UDP Port	1812
Accounting Client UDP Port	1813
Shared Secret	••••••••••
	☑ Mask
Callback User Name	Callback User Name
Callback Password	Callback Password
	☑ Mask

1. Login to **ExtremeCloud Appliance** and go to **ExtremeGuest > Add**.

2. Configure the following mandatory parameters:

Parameter	Description
IP Address	Enter the ExtremeGuest server IP address.
Name	Enter a user-friendly name for this server entry. For example, *EGuest1*
FQDN	Enter the ExtremeGuest server Fully-Qualified Domain Name (FQDN)
Shared Secret	Set the password that is used to authenticate the connection between ExtremeCloud Appliance and the ExtremeGuest server. Note: This shared secret should match the shared secret configured for the ExtremeCloud Appliance NAS settings on the ExtremeGuest server. See Configure AAA NAS Client.

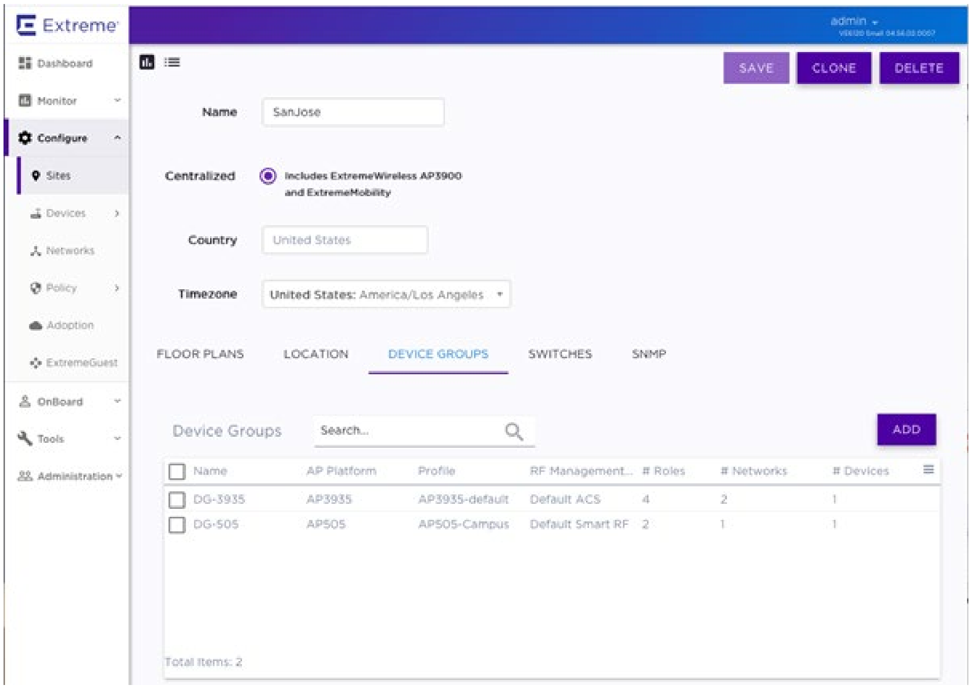
VII.B Configure a Centralized Site

ExtremeCloud Appliance Configuration

A Centralized configuration uses ExtremeWireless AP models AP39xx and AP5xx (AP505 and AP510). Each Wireless AP opens an IPSec tunnel to ExtremeCloud Appliance and the Session Manager and RF Management policy run on ExtremeCloud Appliance.

To add a centralized site:

3. Login to **ExtremeCloud Appliance** and go to **Sites > Add**.



Name: SanJose

Centralized: ● Includes ExtremeWireless AP3900 and ExtremeMobility

Country: United States

Timezone: United States: America/Los Angeles

Device Groups Search...

□ Name	AP Platform	Profile	RF Management...	# Roles	# Networks	# Devices
□ DG-3935	AP3935	AP3935-default	Default ACS	4	2	1
□ DG-505	AP505	AP505-Campus	Default Smart RF	2	1	1

Total Items: 2

4. Configure following site parameters:

Parameter	Description
Name	Provide a relevant name for the site uniquely identifying it. For example: *SanJose*
Centralized	Select the centralized site option.
Country	Select the regulatory country for the site. The country specified here should match the AP's RF Domain.
Time Zone	Select the time zone of the specified country.

5. Click the **Device Groups** tab.

   A device group is composed of APs with the same model, configuration profile, and RF Management profile. The device group is defined within a site, so device groups within a site also share the configuration type and licensing domain that is defined for the site.

6. Select a group. If the desired group is not available, click **Add** and define a new group. See following step, Configure the Device Group.

VII.C Configure a Device Group

ExtremeCloud Appliance Configuration

7. To create a device group, go to **Sites > Add**.

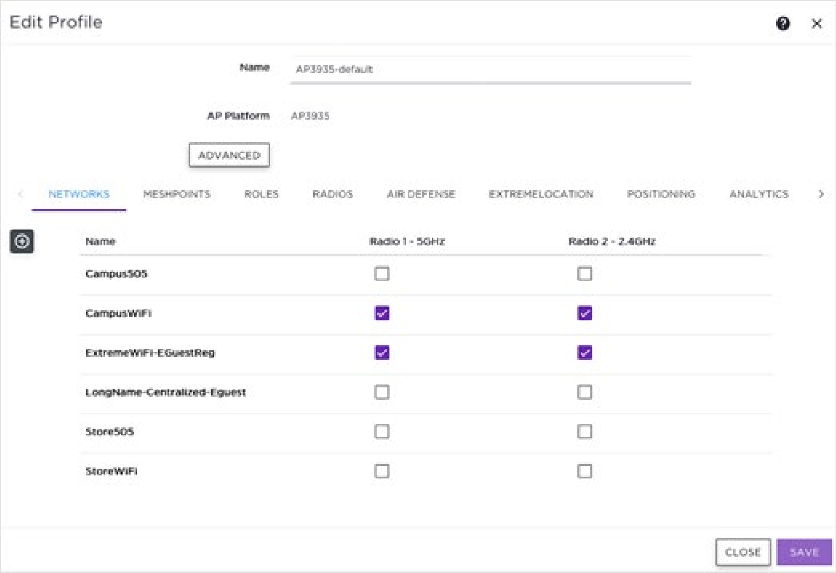
8. Go to **Device Groups > Add**.

9. Configure the following device-group parameters:

Parameter	Description
Name	Provide a relevant name for the group uniquely identifying it. For example: *DG-3935* Note: Devices within a group share the following: • AP model type • Configuration profile • Management profile
Profile	Select a configuration profile for APs in this group. Click the **Edit** icon and apply networks to the Radio -1 and Radio - 2. See Step 10 below, Edit Configuration Profile of AP. Note: Configuration profiles are specific to the AP model type. Select an appropriate profile, based on the AP model type. For example: If the AP model type is *AP3935*, set the profile as *AP3935-default*.
RF Management	Select **Default ACS**. This is applicable to the AP39xx model access points.
Access Points	Search and add APs to the group. The **Access Points** field lists auto-discovered APs matching the configuration profile selected.

VII.D Edit Configuration Profile of AP

ExtremeCloud Appliance Configuration



Name AP3935-default

AP Platform AP3935

Name	Radio 1 - 5GHz	Radio 2 - 2.4GHz
CampusSOS	□	□
CampusWiFi	☑	☑
ExtremeWiFi-EGuestReg	☑	☑
LongName-Centralized-Eguest	□	□
StoreSOS	□	□
StoreWiFi	□	□

10. Select and apply the networks that have **Extreme Guest** as the captive-portal type. For information on configuring Extreme Guest enabled captive-portal, see Configure an Extreme Guest Enabled Network.

VII.E Apply Device Group to the Centralized Site

ExtremeCloud Appliance Configuration

11. Go to **Sites** and select the site created in Step 4, Configure a Centralized Site.

12. Click **Configure Sites > Device Groups**.

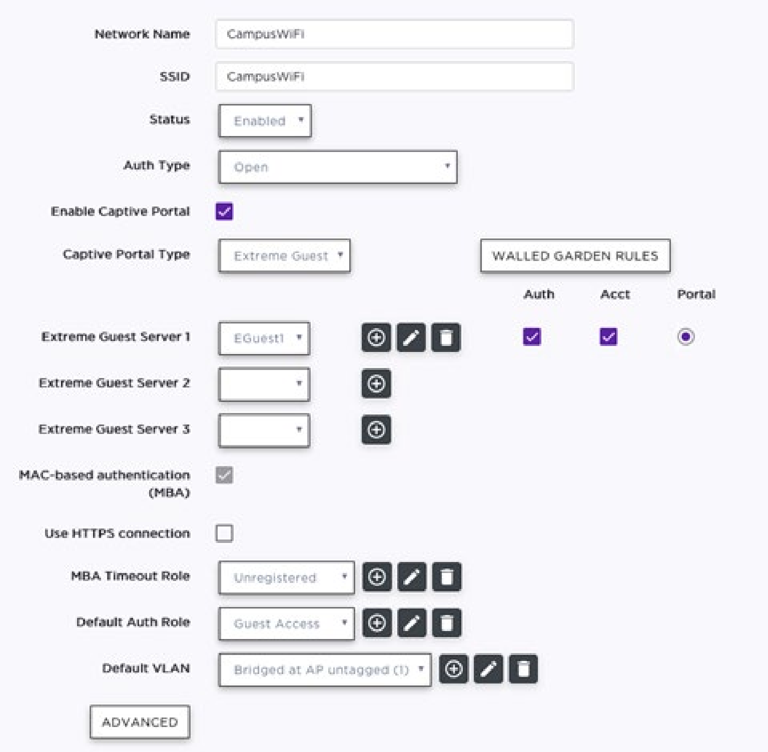
13. Select the group configured in Step 9, Configure the Device Group.

VII.F Configure an Extreme Guest Enabled Network

ExtremeCloud Appliance Configuration

This section describes how to create a wireless network and enable ExtremeGuest as the external captive portal on the network.

14. Go to **Networks > Add**.



Network Name: CampusWiFi
SSID: CampusWiFi
Status: Enabled
Auth Type: Open
Enable Captive Portal: ☑
Captive Portal Type: Extreme Guest
Extreme Guest Server 1: EGuest1 — Auth ☑ Acct ☑ Portal ●
Extreme Guest Server 2:
Extreme Guest Server 3:
MAC-based authentication (MBA): ☑
Use HTTPS connection: □
MBA Timeout Role: Unregistered
Default Auth Role: Guest Access
Default VLAN: Bridged at AP untagged (1)

15. Configure following parameters:

Parameter	Description
Network Name	Provide a user-friendly name for this wireless network. For example: *CampusWiFi*
SSID	Provide a string to uniquely identify this wireless network. For example: *CampusWiFi*
Status	Enable the network. When enabled, the network is up and running and wireless clients can access the network service.

Enable Captive Portal	Select this option to enable captive-portal support on the network.
Captive Portal Type	Set this option as **Extreme Guest**.
Extreme Guest Server 1	Select the ExtremeGuest server added in Step1, Configure the ExtremeGuest Server IP Address.
Walled Garden Rules	If using social sign-in, click this option to configure policy rule parameters associated with each supported application site. Walled Garden Rules allow clients to sign using third-party credentials, such Facebook, Google, Linkedin, etc. See Step 16 below for information on configuring **Walled Garden Rules**.
Use HTTPS for connection	Uses secure HTTPS connection between the ExtremeCloud Appliance and ExtremeGuest servers.

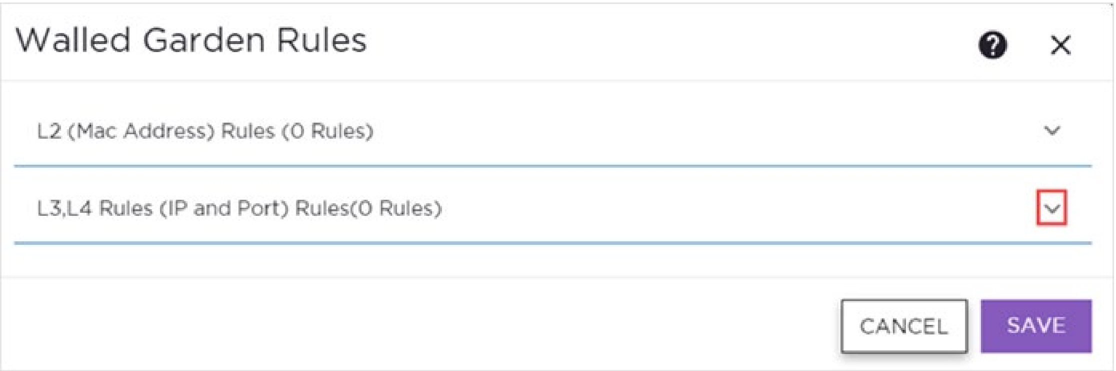
VII.G Add Walled-Garden Rules

ExtremeCloud Appliance Configuration

Walled Garden Rules allow guests to sign-in using third-party credentials, such as Facebook, Google, Linkedin, etc. Follow the steps below to configure social sign-in options.

To add Walled Garden Rules:

16. Click the **WALLED GARDEN RULES** button. The **Walled Garden Rules** configuration screen displays.

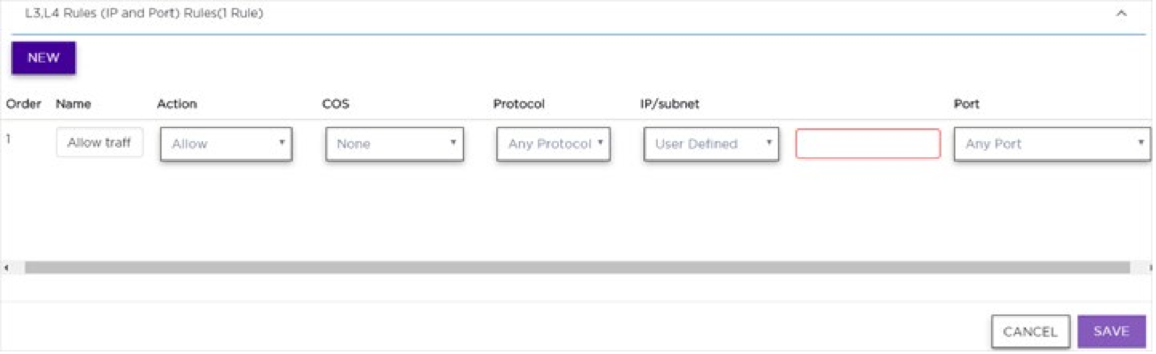


Walled Garden Rules

L2 (Mac Address) Rules (0 Rules)

L3,L4 Rules (IP and Port) Rules(0 Rules)

17. Click the **L3,L4 Rules** (IP **and Port) Rules (0 Rules)** drop-down arrow. This option is selected, since we will be defining the FQDN, protocol and port for the walled garden rules.



L3,L4 Rules (IP and Port) Rules(1 Rule)

Order	Name	Action	COS	Protocol	IP/subnet		Port
1	Allow traff	Allow	None	Any Protocol	User Defined		Any Port

a. Click **New** and configure the **Rule** parameters. Each application site requires specific rules to access their site domains.

b. **Name** – Provide a rule name.

c. **Action** – Set action to Allow.

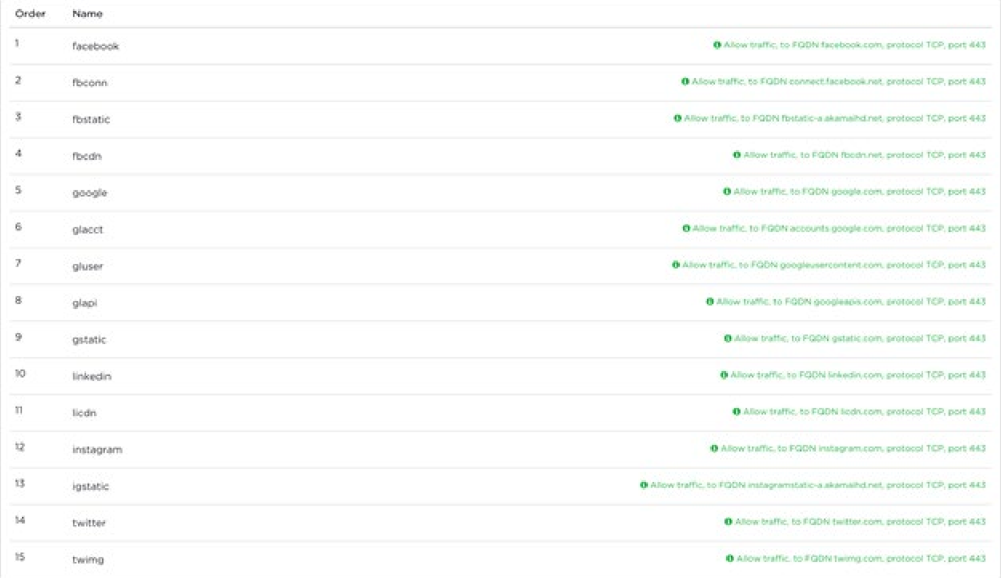
d. **COS** – None

e. **Protocol** – TCP

f. **IP/subnet** – FQDN: Enter the application site FQDN in the adjacent field. Refer to the table below for details.

g. **Port** – Provide the TCP port number.

Refer to Table 1 below for rule parameters.



Order	Name	
1	facebook	● Allow traffic, to FQDN facebook.com, protocol TCP, port 443
2	fbconn	● Allow traffic, to FQDN connect.facebook.net, protocol TCP, port 443
3	fbstatic	● Allow traffic, to FQDN fbstatic-a.akamaihd.net, protocol TCP, port 443
4	fbcdn	● Allow traffic, to FQDN fbcdn.net, protocol TCP, port 443
5	google	● Allow traffic, to FQDN google.com, protocol TCP, port 443
6	glacct	● Allow traffic, to FQDN accounts.google.com, protocol TCP, port 443
7	gluser	● Allow traffic, to FQDN googleusercontent.com, protocol TCP, port 443
8	glapi	● Allow traffic, to FQDN googleapis.com, protocol TCP, port 443
9	gstatic	● Allow traffic, to FQDN gstatic.com, protocol TCP, port 443
10	linkedin	● Allow traffic, to FQDN linkedin.com, protocol TCP, port 443
11	licdn	● Allow traffic, to FQDN licdn.com, protocol TCP, port 443
12	instagram	● Allow traffic, to FQDN instagram.com, protocol TCP, port 443
13	igstatic	● Allow traffic, to FQDN instagramstatic-a.akamaihd.net, protocol TCP, port 443
14	twitter	● Allow traffic, to FQDN twitter.com, protocol TCP, port 443
15	twimg	● Allow traffic, to FQDN twimg.com, protocol TCP, port 443

Table 1. Application Site FQDN, Protocol and Port Information

Application	Rule Parameters
Facebook	Allow FQDN facebook.com protocol TCP port 443 Allow FQDN fbstatic-a.akamaihd.net protocol TCP port 443 Allow FQDN fbcdn.net protocol TCP port 443 Allow FQDN connect.facebook.net protocol TCP port 443
Google	Allow FQDN google.com protocol TCP port 443 Allow FQDN ssl.gstatic.com protocol TCP port 443 Allow FQDN accounts.google.com protocol TCP port 443 Allow FQDN gstatic.com protocol TCP port 443 Allow FQDN apis.google.com protocol TCP port 443 Allow FQDN googleusercontent.com protocol TCP port 443 Allow FQDN googleapis.com protocol TCP port 443
Instagram	Allow FQDN instagram.com protocol TCP port 443 Allow FQDN instagramstatic-a.akamaihd.net protocol TCP port 443
Linkedin	Allow FQDN linkedin.com protocol TCP port 443 Allow FQDN static.licdn.com protocol TCP port 443

VIII ExtremeGuest Configuration

This section describes the configurations you will have to make on the ExtremeGuest server to enable it to communicate with ExtremeCloud Appliance.

- Configure AAA NAS Client
- Configure AAA Authorization Policy and Group
- Configure Onboarding Policy and Rules
- Configure Notification Policy and Rules
- Configure a Network – Optional
- Configure a Site - Optional
- Add a Device - Optional
- Create Splash Templates
- Host and Apply Splash Template to Network

> Note
>
> ExtremeCloud Appliance supports auto-staging of configuration to the ExtremeGuest server. However, for Centralized Deployments, this support is *only* available on ExtremeCloud Appliance v10.56.02. Post integration (see ExtremeCloud Appliance Configuration), site, network, device group configurations are auto-staged to the ExtremeGuest server and are available as options in the 'Site', 'Network', 'Device' menus on ExtremeGuest.
>
> ExtremeCloud Appliance v10.56.01 *does not* support auto-staging for Centralized Deployments. For ExtremeCloud Appliance v10.56.01 managed Centralized sites, you will have to manually add the network, site and APs on the ExtremeGuest server.

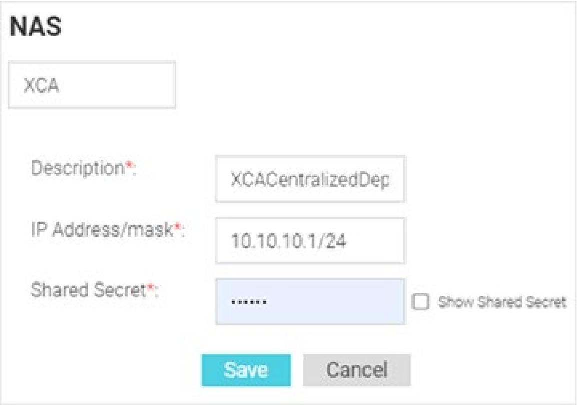
VIII.A Configure AAA NAS Client

ExtremeGuest Configuration

This configuration enables ExtremeGuest to receive and process RADIUS request from APs adopted to ExtremeCloud Appliance in the centralized mode. Specify the NAS clients that are allowed to communicate with the ExtremeGuest RADIUS server. It is possible to allow single IP address or an IP subnet as the NAS client. Also specify the shared secret.

1. Log in to ExtremeGuest UI and go to **Configuration > AAA > NAS**.

2. To add a NAS client, click the **+** icon on the top, right-hand corner of the screen.



NAS

XCA

Description*: XCACentralizedDep

IP Address/mask*: 10.10.10.1/24

Shared Secret*: ······ □ Show Shared Secret

   a. Provide a name uniquely identifying the NAS client network. The NAS client here is the ExtremeCloud Appliance.

b. Enter a brief description for this NAS configuration.

c. Enter the IP address and mask of the ExtremeCloud Appliance. This allows ExtremeGuest to recognize ExtremeCloud Appliance as the NAS client.

d. Enter the password used to validate the connection between ExtremeCloud Appliance and ExtremeGuest server.

> **Note**
>
> Ensure the shared secret is the same as the one configured in the *ExtremeCloud Appliance > Extreme Guest* context. See, Configure the ExtremeGuest Server IP Address.

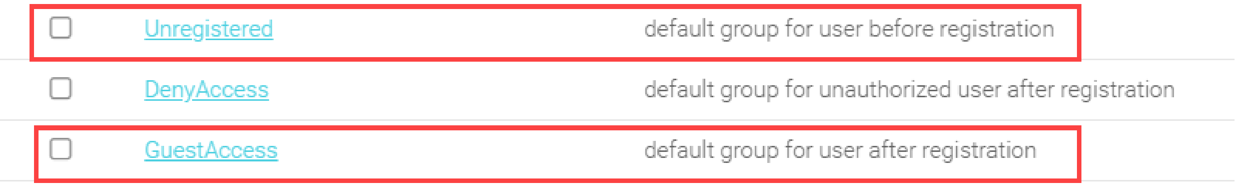
VIII.B Configure AAA Authorization Group and Policy

ExtremeGuest Configuration

3. Go to **Configuration > AAA > Group** and add user groups for *unregistered* and *registered* wireless clients.

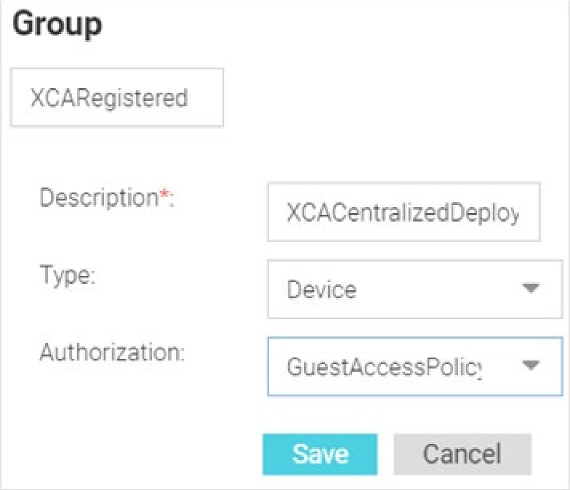
These are the groups to which wireless clients (unregistered and registered) will be added.

This step is optional. By default, registered wireless-guests are assigned to the default "**GuestAccess**" group and enforced "**GuestAccessPolicy**" associated with it. And, unregistered clients are assigned to the "**Unregistered**" group and enforced "**UnregisteredPolicy**" associated with it. See screenshot below:



☐	Unregistered	default group for user before registration
☐	DenyAccess	default group for unauthorized user after registration
☐	GuestAccess	default group for user after registration

4. If adding a new group, click the **+** icon on the top, right-hand corner of the screen.

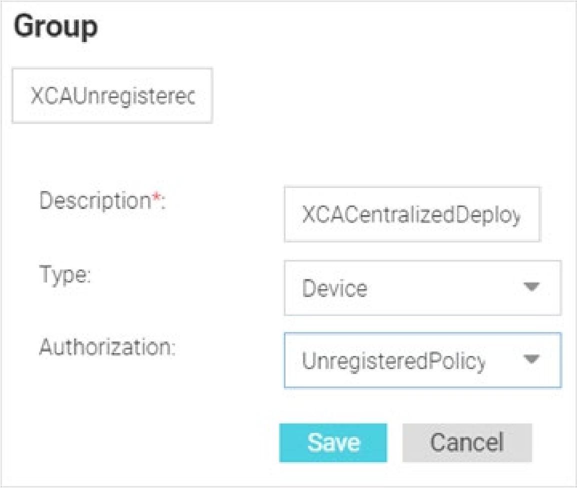


XCARegistered

Description*: XCACentralizedDeploy

Type: Device

Authorization: GuestAccessPolic



XCAUnregisterec

Description*: XCACentralizedDeploy

Type: Device

Authorization: UnregisteredPolicy

a. Enter a name uniquely identifying the group.

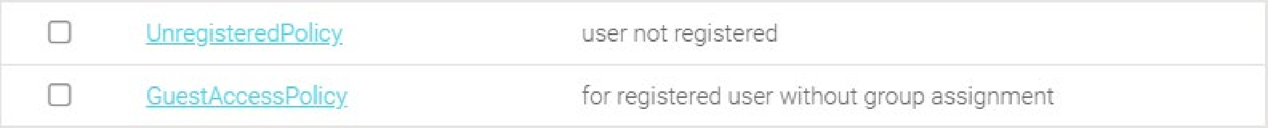
b. Specify the client as **Devices**.

c. Associate the authorization profile to be applied to guests assigned to this group.

> **Note**
>
> The default 'GuestAccess' and 'Unregistered' are associated with the 'GuestAccessPolicy' and 'UnregisteredPolicy' respectively. If you are creating a customized group, ensure that you apply the appropriate default authorization policy to the groups.

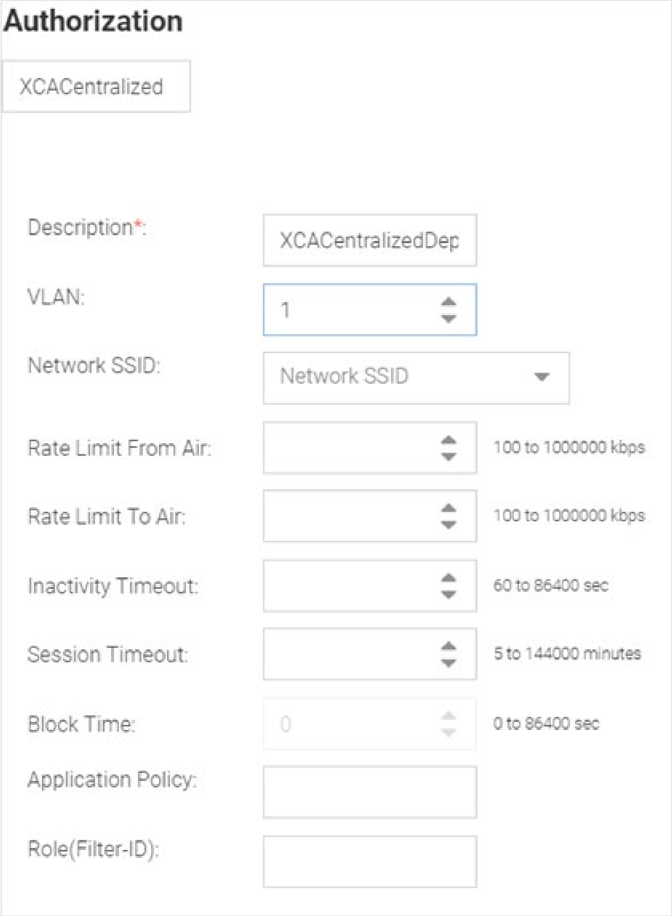
5. Go to **Configuration > AAA > Authorization** to add two authorization profiles for *unregistered* and *registered* wireless-guest users.

   This step is optional. By default, registered wireless guests are assigned to the default "**GuestAccess**" group and enforced "**GuestAccessPolicy**" associated with it. And non-registered wireless-guests are assigned to the "**Unregistered**" group and enforced "**UnregisteredPolicy**". See screenshot below:



☐	UnregisteredPolicy	user not registered
☐	GuestAccessPolicy	for registered user without group assignment

6. If adding a new authorization profile, click the **+** icon on the top, right-hand corner of the screen.



Authorization

XCACentralized

Description*:	XCACentralizedDep	
VLAN:	1	
Network SSID:	Network SSID	
Rate Limit From Air:		100 to 1000000 kbps
Rate Limit To Air:		100 to 1000000 kbps
Inactivity Timeout:		60 to 86400 sec
Session Timeout:		5 to 144000 minutes
Block Time:	0	0 to 86400 sec
Application Policy:		
Role(Filter-ID):		

   a. Enter a name uniquely identifying the profile.
   b. Enter a description.
   c. Leave the **Network SSID:** and **Role(Filter-ID):** fields blank.

VIII.C Configure Onboarding Policy and Rules

ExtremeGuest Configuration

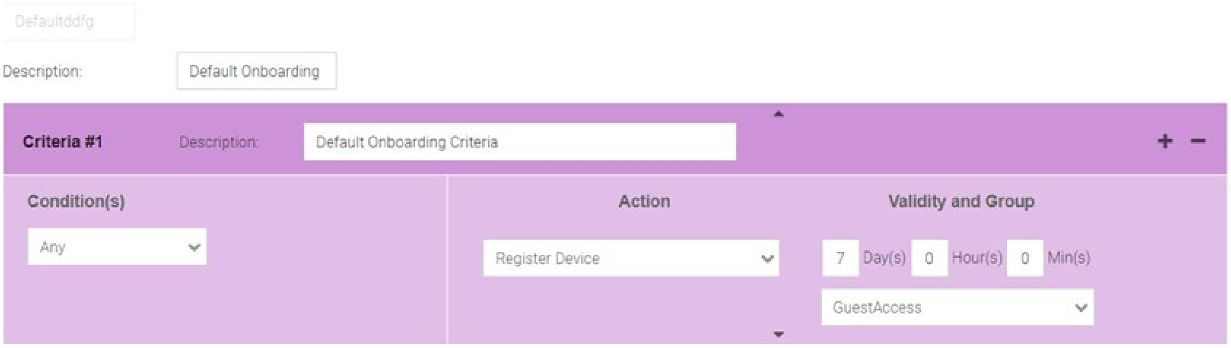
Guest onboarding is the process used to register a wired or wireless client when they join a hotspot network. Onboarding enables hotspot network providers to collect client information, send client passcodes and set up external approval for guest access using rules and policies.

A captive-portal guest user requesting access is matched against onboarding rules. When a matching rule is found, the associated policy with the “lowest” precedence number (represented by **Criteria #x**) is used to onboard the hotspot user.

To add an onboarding policy:

7. Go to **Configuration > Onboarding**.

   This step is optional. By default, onboarded wireless guests are applied the default Onboarding Policy and Rules associated with the policy. You can edit the default policy by selecting it and updating the parameters. Alternately, you can add a new Onboarding Policy.



Defaultddfg

Description: Default Onboarding

Criteria #1 Description: Default Onboarding Criteria

Condition(s): Any

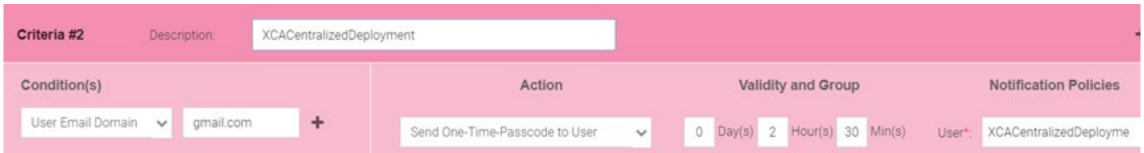
Action: Register Device

Validity and Group: 7 Day(s) 0 Hour(s) 0 Min(s)

GuestAccess

To create a new policy:

a. Click the **+** icon on the top, right-hand corner of the screen.



Criteria #2 Description: XCACentralizedDeployment

Condition(s): User Email Domain gmail.com +

Action: Send One-Time-Passcode to User

Validity and Group: 0 Day(s) 2 Hour(s) 30 Min(s)

Notification Policies: User*: XCACentralizedDeployme

b. Enter a name uniquely identifying the onboarding policy. For example, **XCACentralized**.

c. Enter a brief description for this onboarding policy.

d. In the **Criteria #x** field, add the match criteria details.

   An onboarding policy consists of one or more match criteria that are used to filter guests and apply an action.

   - Enter a *Description* uniquely identifying the purpose of this criteria.
   - Select the *Condition(s)*. The options are: *User Email Domain*, *Sponsor Email Domain*, *Social Type*, *User Type*, *Loyalty User*, *LDAP/Directory Group*, *User’s Device Count*, and *Any*.
   - For each condition selected, set the corresponding value.

     These conditions determine when the *action* associated with the criteria is triggered. You can add multiple conditions. In case of multiple conditions, all conditions have to be met for the associated action to be triggered.
   - Select the *Action* from the available menu. The selected *Action* is triggered when all of the Condition(s) are met. The options are: *Deny Access*, *Register Device*, *Send One-Time Passcode to User*, *Send Passcode to User*, *Send One-Time Pass. On Sponsor Approval*, *Send Passcode on Sponsor Approval*, *Send One-Time Passcode to Sponsor*, and *Send Passcode to Sponsor*.

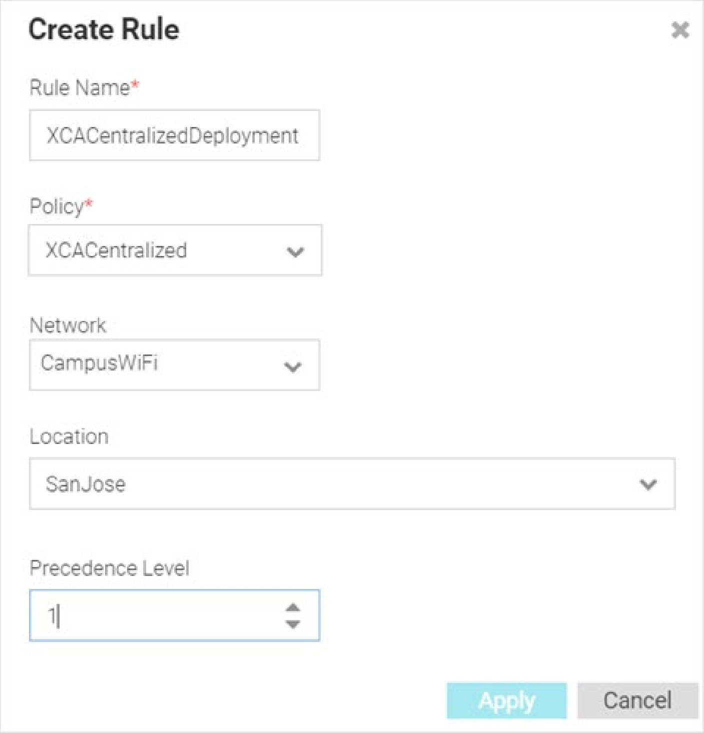
     > **Note**
     >
     > Selecting any of the “**Send Passcode ……………..**” action types enables the **Notification Policies** field.

   - Specify the validity of access in **Days**, **Hours** and **Minutes**.

- In the **Select a Group** field, set a group for the guest user to join.
- Set a *Notification Policy* for sending the One-Time-Passcode to the guest, sponsor, or both depending on the action type selected. If the action requires sponsor approval, then the approval request is sent to the sponsor.
- Select the **Update User** checkbox to send status to a user's email or mobile when registration is pending approval or is rejected.
- Select the **Provide Temporary Access** checkbox to give the user temporary access to check email for a passcode.

> Note
>
> The guest user's access time can be restricted by specifying the **Session Timeout** in the AAA Authorization profile. Alternately, use the **Schedule Policy** option to restrict access to specific day and time.

e. To add an onboarding rule, go to **Configuration > Onboarding > Rules** and click the **+** icon on the top, right-hand corner of the screen.



Create Rule

Rule Name*: XCACentralizedDeployment

Policy*: XCACentralized

Network: CampusWiFi

Location: SanJose

Precedence Level: 1

f. Enter a name uniquely identifying the onboarding rule.

g. Associate the onboarding policy created above (for example, XCACentralized).

h. Specify network this rule applies to.

Select the appropriate network. This is the network you will add in Step 10 a, Configure a Network.

i. Select the location(s) applicable.

Select the appropriate location. This is the site you will add in Step 12 a, Configure a Site.

j. Set the precedence of this rule.

Note, lower the precedence higher is the priority. Rules with lower precedence are applied first.

VIII.D Configure Notification Policy and Rules

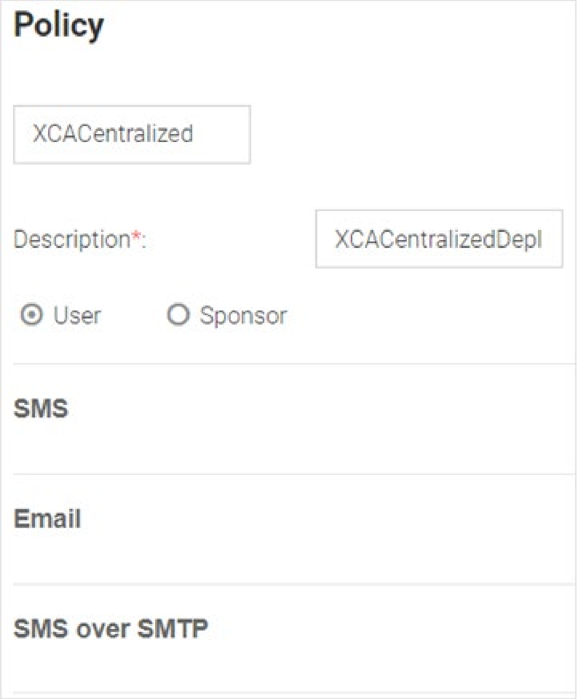
ExtremeGuest Configuration

The guest-user onboarding workflow includes the generation and sending of passcode to the guest user directly or sponsoring access for a guest user. The notification policy defines the mode of communication used to communicate the passcode.

To add a notification policy:

8. Go to **Configuration > Notification**.

> **Note**
>
> The onboarded user/device is assigned to the AAA group created in Step 4 a. See Configure AAA Authorization Group and Policy.



Policy

XCACentralized

Description*: XCACentralizedDepl

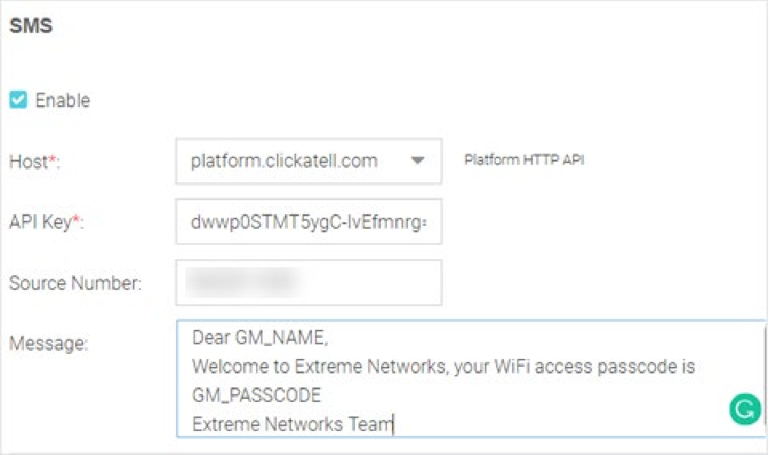
◉ User ○ Sponsor

SMS

Email

SMS over SMTP

a. Click the **+** icon on the top, right-hand corner of the screen.
b. Provide a brief description.
c. Select either the **User** or **Sponsor** radio button. The *User* option creates a guest user notification policy. The *Sponsor* option creates a sponsor notification policy.
d. Select one of the following modes by which the guest-user will be notified the passcode:
   - **SMS** - Uses a third-party SMS service provider. Requires integration with an SMS gateway.



SMS

☑ Enable

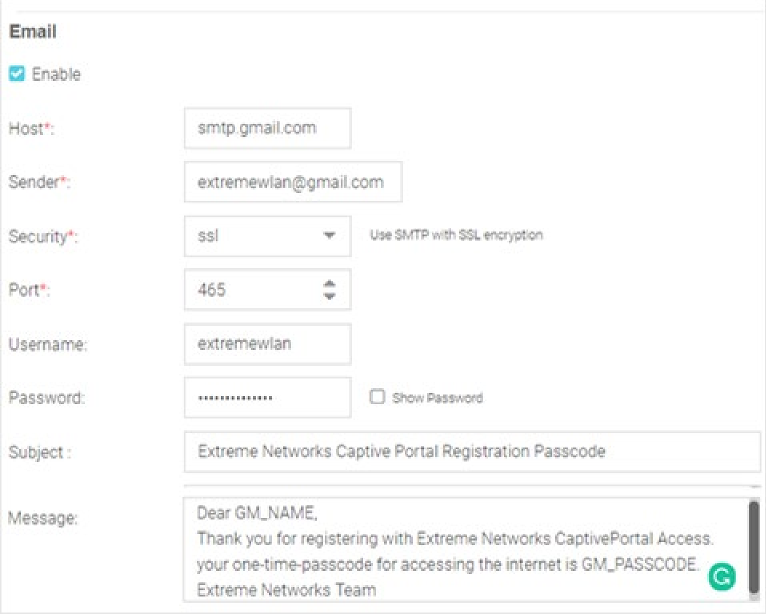
Host*: platform.clickatell.com — Platform HTTP API

API Key*: dwwp0STMT5ygC-lvEfmnrg

Source Number: [redacted]

Message:
Dear GM_NAME,
Welcome to Extreme Networks, your WiFi access passcode is GM_PASSCODE
Extreme Networks Team

- **Email** - Uses an SMTP server. Requires integration with the SMTP Server.



Email

☑ Enable

Host*: smtp.gmail.com

Sender*: extremewlan@gmail.com

Security*: ssl — Use SMTP with SSL encryption

Port*: 465

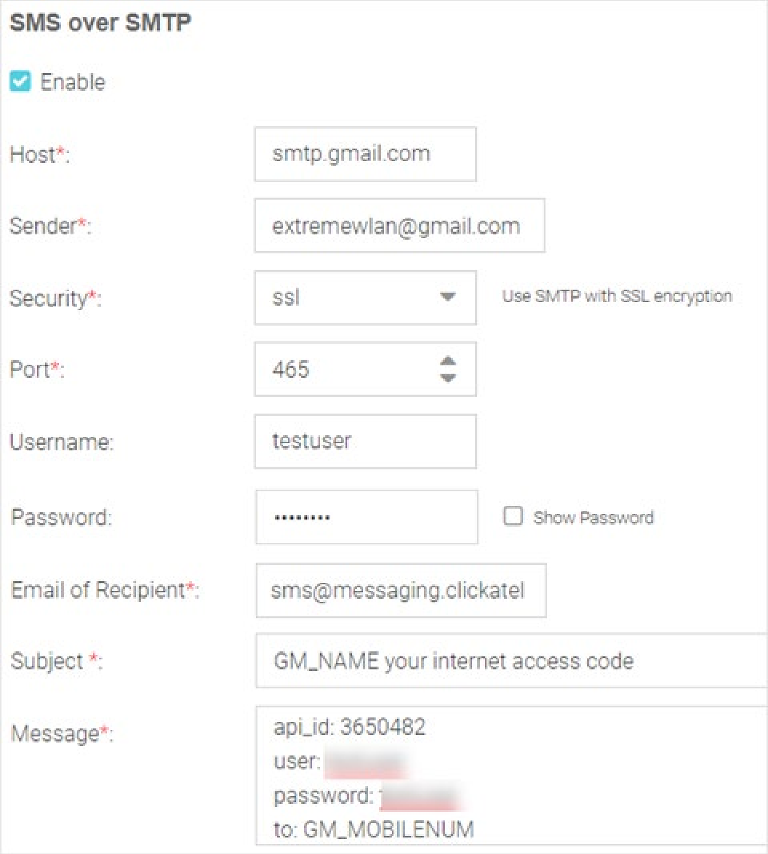
Username: extremewlan

Password: ••••••••••••••• ☐ Show Password

Subject : Extreme Networks Captive Portal Registration Passcode

Message:
Dear GM_NAME,
Thank you for registering with Extreme Networks CaptivePortal Access.
your one-time-passcode for accessing the internet is GM_PASSCODE.
Extreme Networks Team

- **SMS over SMTP** - Uses a third-party SMS service provider. Requires integration with an SMS gateway



SMS over SMTP

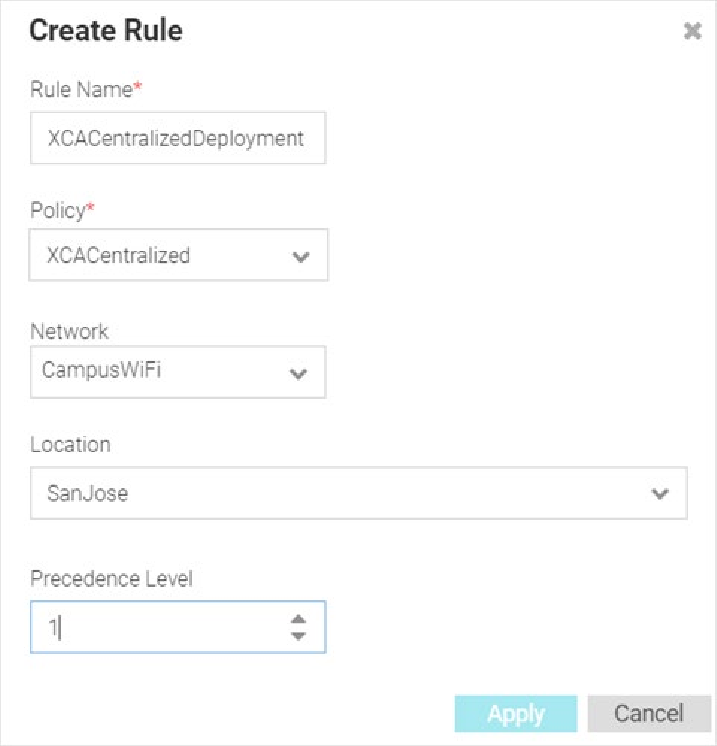
☑ Enable

Host*:	smtp.gmail.com	
Sender*:	extremewlan@gmail.com	
Security*:	ssl	Use SMTP with SSL encryption
Port*:	465	
Username:	testuser	
Password:	•••••••••	□ Show Password
Email of Recipient*:	sms@messaging.clickatel	
Subject *:	GM_NAME your internet access code	
Message*:	api_id: 3650482 user: [redacted] password: [redacted] to: GM_MOBILENUM	

e. Configure the settings for the selected notification mode.

> **Note**
>
> For detailed information on these settings, refer to the ExtremeGuest User Guide v 6.0.0 available at https://extremenetworks.com/documentation.

f. To add a notification rule, go to **Configuration** → **Notification** → **Rules** and click on the **+** icon on the top, right-hand corner of the screen.



Create Rule

Rule Name*

XCACentralizedDeployment

Policy*

XCACentralized

Network

CampusWiFi

Location

SanJose

Precedence Level

1

g. Enter a name uniquely identifying the notification rule.
h. Associate the notification policy created above.
i. Specify network this rule applies to. This is the network added in Step 10 a below, Configure a Network.
j. Select the location(s) applicable. This is the site added in Step 12 a below, Configure a Site.
k. Set the precedence of this rule.

   Note, lower the precedence higher is the priority. Rules with lower precedence are applied first.

VIII.E Configure a Network – Optional

ExtremeGuest Configuration

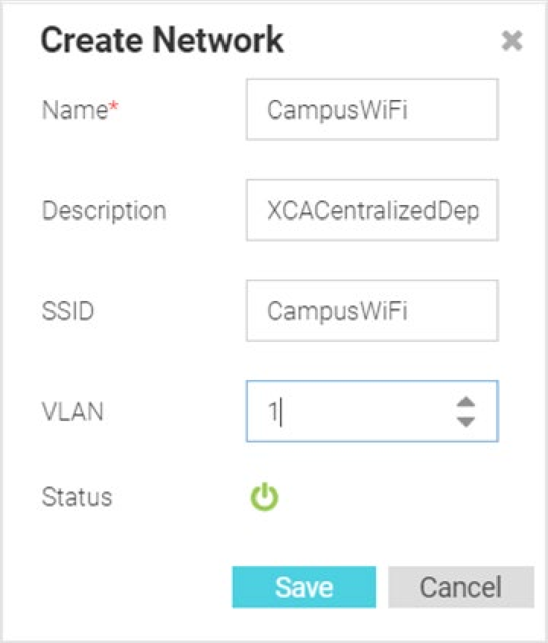
Follow the steps below to manually add the network. This configuration is required ONLY for ExtremeCloud Appliance v10.56.01 managed centralized deployments.

For ExtremeCloud Appliance v10.56.02 managed centralized deployments, network configurations are auto-staged to the ExtremeGuest server.

9. Go to **Configuration > Networks**.

10. To add a network, click the **+** icon on the top, right-hand corner of the screen.

    The **Create Network** box displays.


Create Network

Name* CampusWiFi

Description XCACentralizedDep

SSID CampusWiFi

VLAN 1

Status

a. Enter the network name.

   The name should be same as the wireless network configured on ExtremeCloud Appliance. Refer to the Configure an Extreme Guest Enabled Network section.

b. Enter a brief description of the network.

c. Enter the network **SSID**.

d. Specify the client VLAN. This is VLAN the client will be assigned post authentication. It should be the same as the VLAN specified in the **AAA > Authorization** profile created in Step 6 above.

VIII.F Configure a Site - Optional

ExtremeGuest Configuration

Follow the steps below to manually add the site. This configuration is required ONLY for ExtremeCloud Appliance v10.56.01 managed centralized deployments.

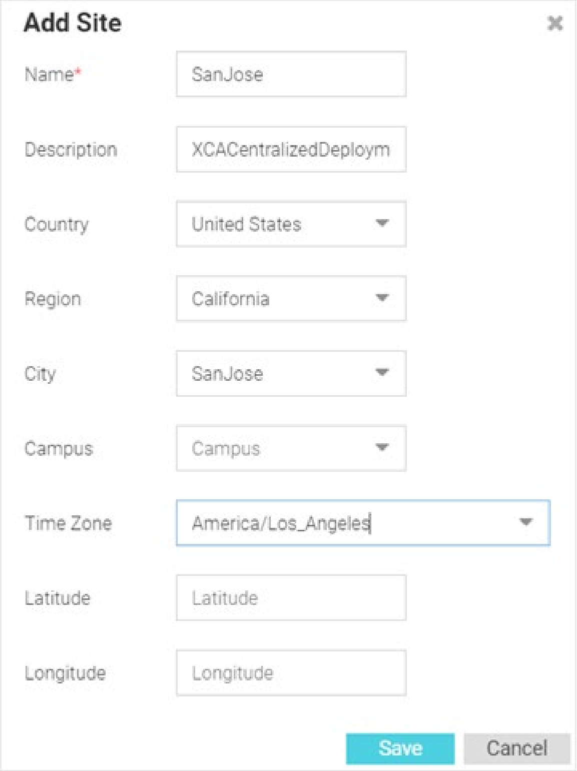
For ExtremeCloud Appliance v10.56.02 managed centralized deployments, site configurations are auto-staged to the ExtremeGuest server.

11. Go to **Configuration > Sites**

    Use this option to create a site matching the location of the APs adopted to ExtremeCloud Appliance in the centralized site.

12. To add a site, click on the **+** icon on the top, right-hand corner of the screen.

    The **Add Site** box displays.



Add Site

Name*	SanJose
Description	XCACentralizedDeploym
Country	United States
Region	California
City	SanJose
Campus	Campus
Time Zone	America/Los_Angeles
Latitude	Latitude
Longitude	Longitude

a. Enter the name of the APs' site of deployment.

This is the centralized-site configured on ExtremeCloud Appliance in which the APs are deployed. Refer to the Configure a Centralized Site section.

b. Enter a brief description of the site.

c. Use the other fields (Country, Region, City, etc.) to define the exact geographical location of the site. These parameters should be same as that of the site created on ExtremeCloud Appliance.

VIII.G Add a Device – Optional

ExtremeGuest Configuration

Follow the steps below to manually add the APs. This configuration is required ONLY for ExtremeCloud Appliance v10.56.01 managed centralized deployments.

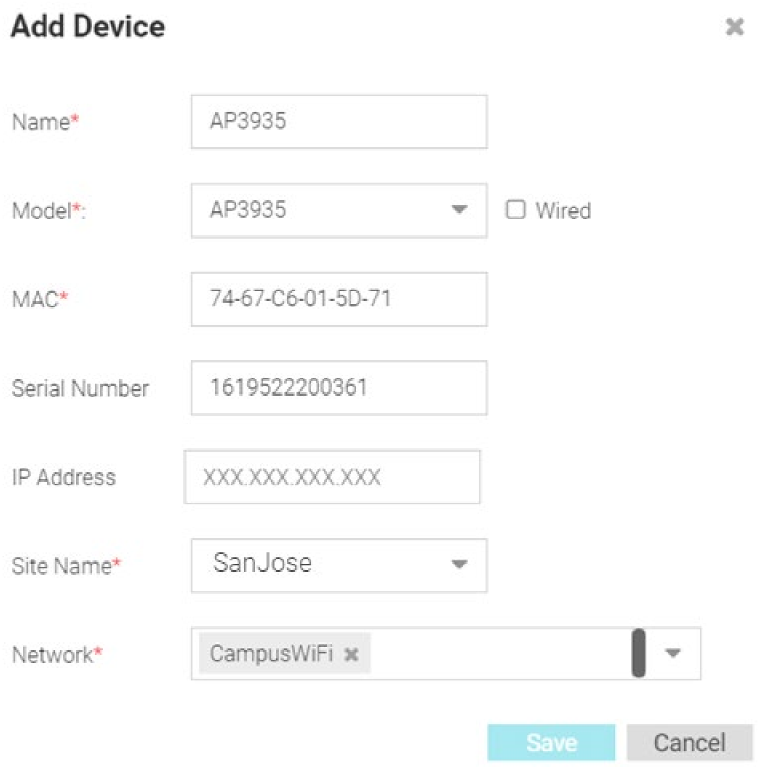
For ExtremeCloud Appliance v10.56.02 managed centralized deployments, devices are auto-staged to the ExtremeGuest server.

13. Go to **Configuration > Devices**.

Use this option to add the APs to the ExtremeGuest device list. These are the APs adopted to ExtremeCloud Appliance and deployed in the Centralized site. All the fields in this screen are mandatory.

14. To add a device, click the **+** icon on the top, right-hand corner of the screen.

The **Add Device** box displays.



Add Device

Name*	AP3935
Model*:	AP3935 □ Wired
MAC*	74-67-C6-01-5D-71
Serial Number	1619522200361
IP Address	XXX.XXX.XXX.XXX
Site Name*	SanJose
Network*	CampusWiFi

a. Enter a hostname for the AP.

b. Set the AP model type.

> **Note**
>
> The ExtremeCloud Appliance Centralized deployment only supports AP505i, AP510i/e and AP39xx series access points. Refer to the Pre-requisites section for information on the software versions these devices need to be running.

c. Enter the AP's MAC address.

d. Select the site to which the AP belongs. This is the site you added in Step 12 a, Configure a Site.

e. In the **Network** field, select the network you added in Step 10 a, Configure a Network.

VIII.H Create Splash Template

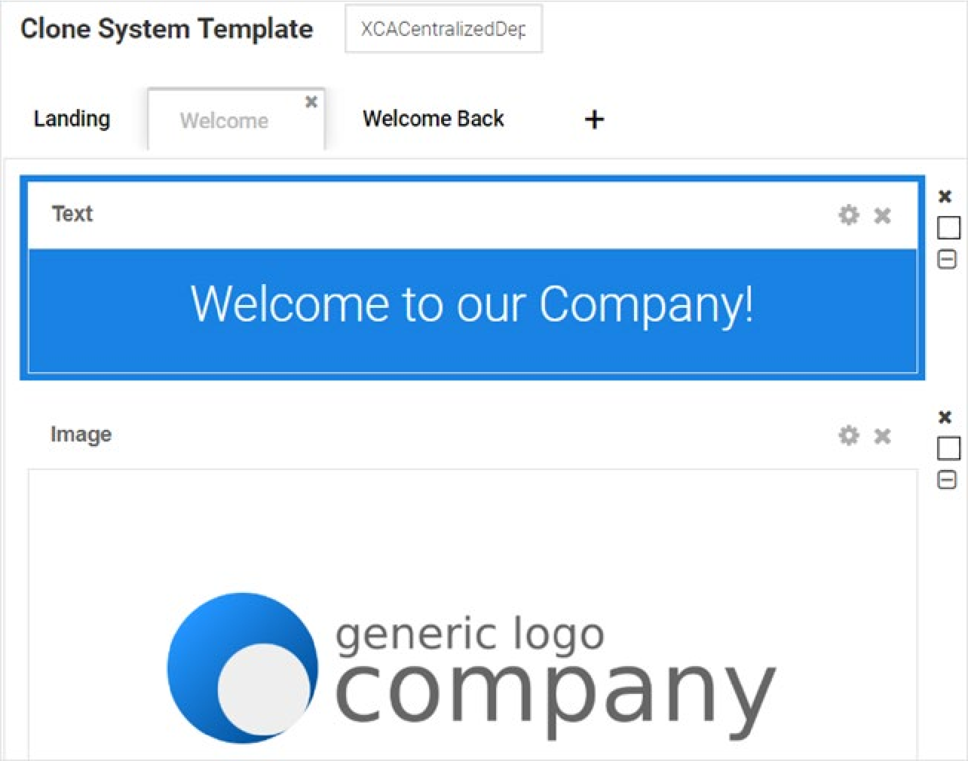
ExtremeGuest Configuration

15. Go to **Configuration > Splash Templates**.

Use this option to create captive portal web pages (landing, registration, welcome, etc.) that will be served to the wireless guests attempting to access the captive-portal network.

The **Splash Templates** screen has the following sub-screens: **System Templates** and **User Templates**. The *System Templates* tab displays a summary of available captive portal splash screen templates. You can clone one of these templates and customize it to suit your purpose. Or, you can go to the *User Templates* tab and use the splash template builder to create customized captive-portal Web pages.

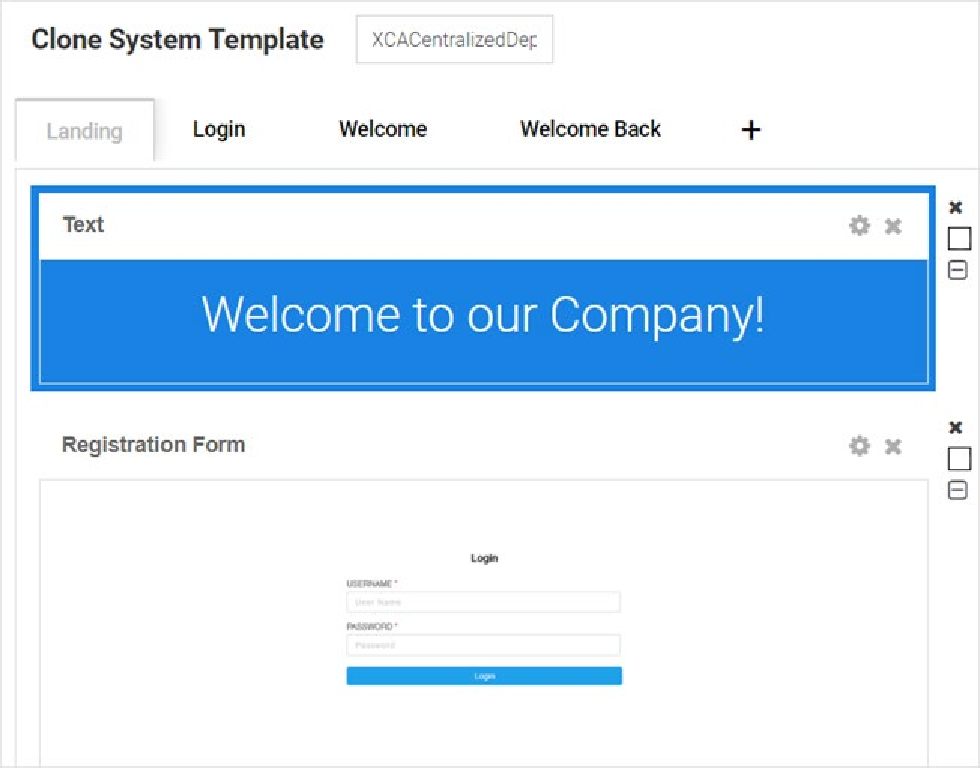
In this example, we have cloned a system-template.



Clone System Template XCACentralizedDep

The cloned and customized template is automatically available in the **User Templates** tab. Once the splash template is in place specify where the template is to be hosted and to which network is it to be applied.

You can use the User Templates option to create customized Web pages.



Clone System Template XCACentralizedDep

VIII.I Host and Apply Splash Template

ExtremeGuest Configuration

16. To host and apply the template:

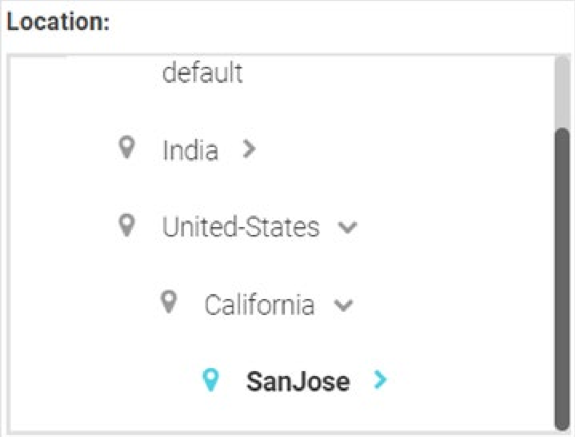
   a. Go to **User Templates**.

   b. Locate the template from the previous step and click the ✓ icon associated with it. The **Apply** box displays.

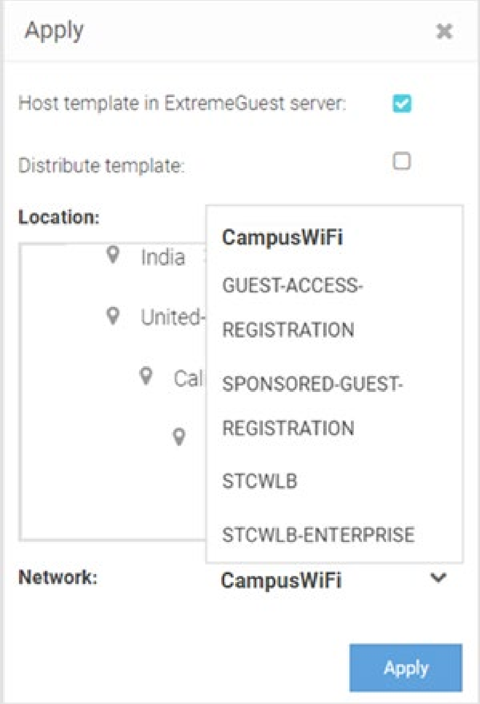
   c. Select the **Host template in ExtremeGuest server:** checkbox.

Note
The ExtremeCloud Appliance Centralized deployment does not support distribution of splash template to APs.

   d. Map the **Location** to the centralized site in which the APs are deployed. Refer to Step 12 a, Configure a Site.



   e. Click the **Network** drop-down menu and select the network you created in Step 10 a, Configure a Network.



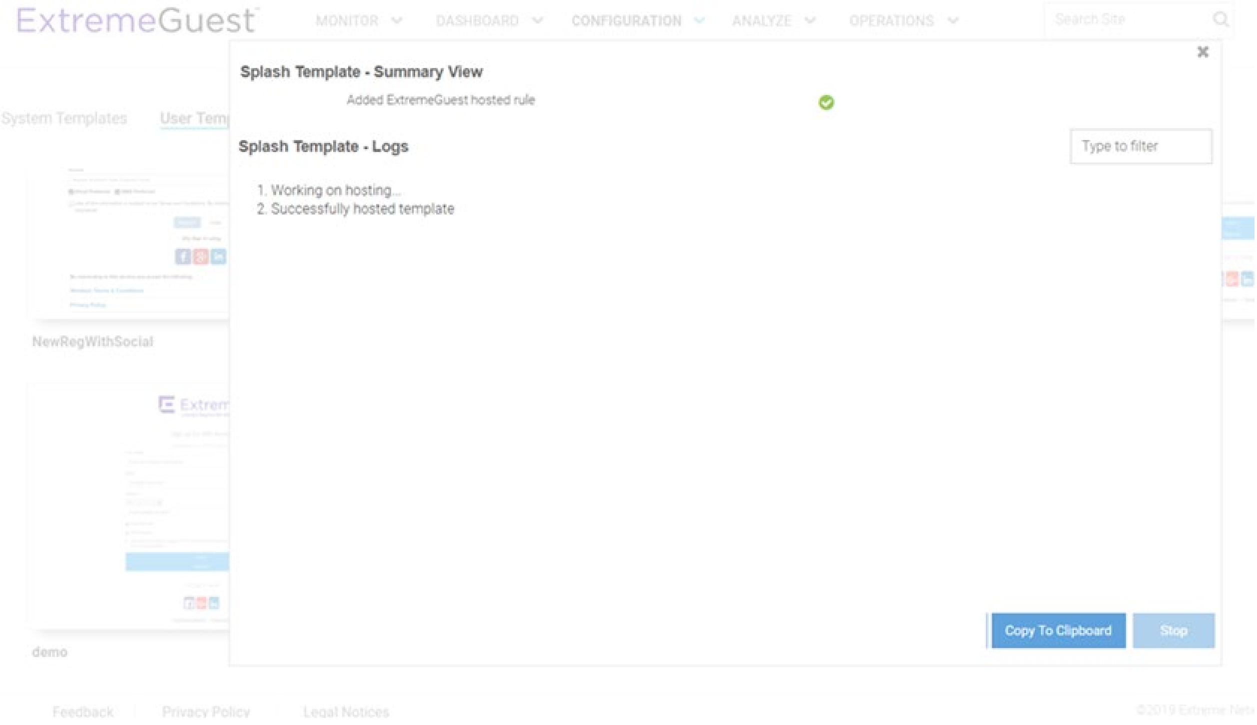
Host template in ExtremeGuest server: ☑

Distribute template: □

Network: CampusWiFi

   f. Click **Apply**.

17. Check the template hosting status in the **Summary View**. To do this,
    a. Click the ≡ icon on the top, right-hand corner of the screen.
    b. Go to **ExtremeGuest Hosted**.
    c. Select the network from the previous step and click on the ℹ icon. The template hosting status is displayed.



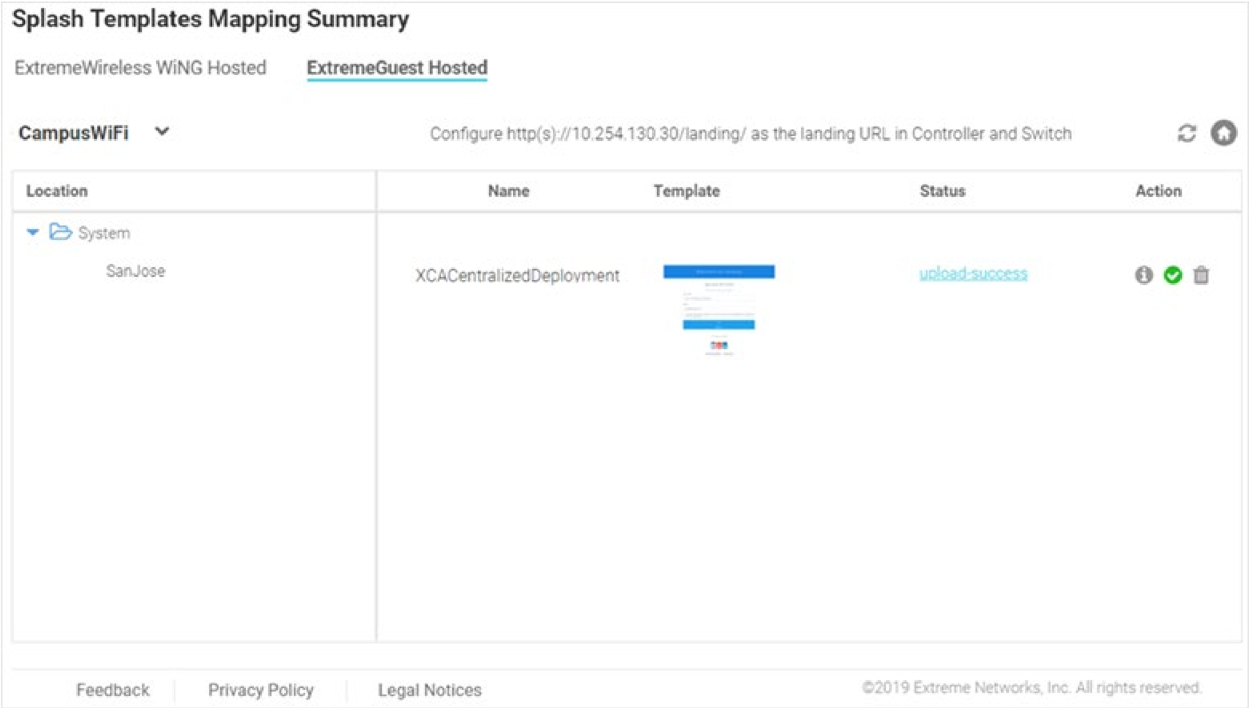
Splash Template - Summary View

Added ExtremeGuest hosted rule ✓

Splash Template - Logs

1. Working on hosting...
2. Successfully hosted template

18. To confirm successful hosting, again go to the summary view (follow preceding steps) and select the network. The template status should display as follows:


ExtremeWireless WiNG Hosted
ExtremeGuest Hosted
Feedback
Privacy Policy
Legal Notices
©2019 Extreme Networks, Inc. All rights reserved.

Splash Templates Mapping Summary

CampusWiFi

Configure http(s)://10.254.130.30/landing/ as the landing URL in Controller and Switch

Location	Name	Template	Status	Action
System SanJose	XCACentralizedDeployment		upload-success	ℹ ✓ 🗑