

ExtremeGuest™ v6.0.0 How-To Guide for ExtremeGuest™ – ExtremeCloud Appliance™ Integration

For Distributed Deployments

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

Published: September 2019

Extreme Networks, Inc.

Phone / +1 408.579.2800

Toll-free / +1 888.257.3000

www.extremenetworks.com

©2019 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

I	Pre-requisites	3
II	ExtremeGuest Overview	4
III	ExtremeCloud Appliance Overview	5
	III.A The Appliance	5
	III.B Wireless AP Overview	5
IV	ExtremeGuest – ExtremeCloud Appliance Distributed Deployment.....	7
	IV.A Deployment Scenario	7
	IV.B How it works:	7
V	Pre-configuration	9
	V.A ExtremeCloud Appliance NTP Configuration	9
	V.B ExtremeGuest NTP Configuration	9
VI	ExtremeCloud Appliance Configuration	11
	VI.A Configure the ExtremeGuest Server IP Address	11
	VI.B Configure an ExtremeGuest Enabled Network	12
	VI.C Add Walled-Garden Rules.....	13
VII	ExtremeGuest Configuration.....	15
	VII.A Configure AAA NAS Client	15
	VII.B Configure AAA Authorization Group and Policy.....	16
	VII.C Configure Onboarding Policy and Rules	17
	VII.D Configure Notification Policy and Rules	20
	VII.E Configure a Network.....	23
	VII.F Configure a Site.....	24
	VII.G Add a Device	25
	VII.H Create Splash Template.....	26
	VII.I Host and Apply Splash Template.....	27

I Pre-requisites

You will need:

- ExtremeGuest running version 6.0.0
- ExtremeCloud Appliance running version 4.56.01 or 4.56.02
- Extreme Networks Access Points:
 - AP7522, AP7532, AP7562, AP7612, AP7632, AP7662, AP8432, AP8533 running version WiNG 5.9.5 or WiNG 7.2.1
 - OR
 - AP505i and AP510i/e running version WiNG 7.x.x

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 deployed 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

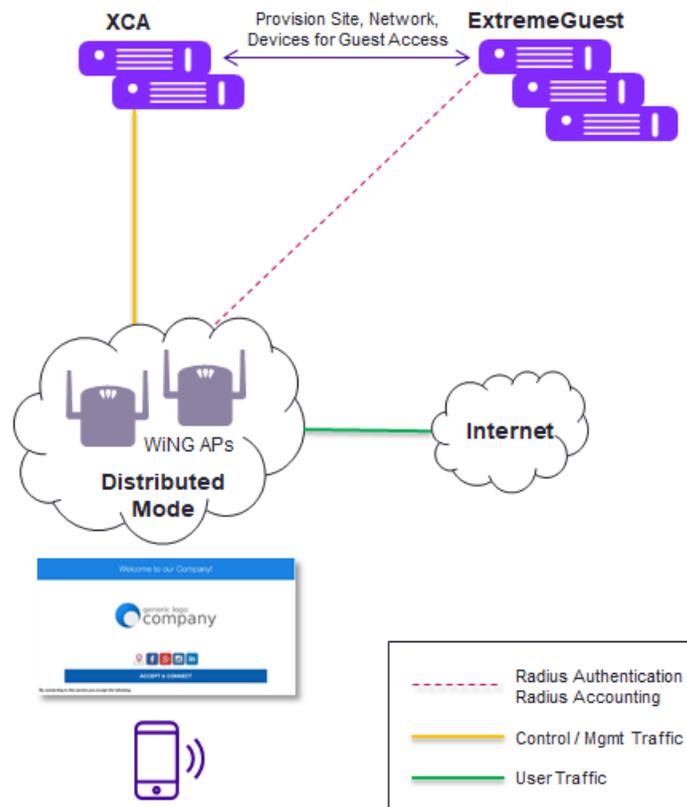
Note

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

IV ExtremeGuest – ExtremeCloud Appliance Distributed Deployment

IV.A Deployment Scenario

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



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 distributed network is captive-portal enabled, with the captive-portal type set to “**Extreme Guest**”, the **AP** forwards the request to ExtremeGuest. The “**username/password**” in the request is set to the guest’s MAC address.
- Since the request is from an unregistered wireless guest, ExtremeGuest sends back an Accept-Reject response and redirects the guest to the landing page in the splash template, where the guest registers. This is the guest onboarding process.
- During onboarding,
 - If the guest registration-type is set to “**Device**” – the **AP** uses MAC Authentication to authenticate the guest and assigns the guest to a new group. The guest is then served the *Welcome* page.
 - 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. The **AP** authenticates the *username/password* entered and provides network access. Subsequent sign-ins to the same network does not require the guest to authenticate until the registration is valid and not timed-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 guests enters the credentials. The *AP* authenticates the *username/password* entered and provides network access. Subsequent sign-ins to the same network requires the client to provide the credentials for authentication.
- On successful authentication – ExtremeGuest returns Accept-Accept with Filter-Id set to the group assigned to the client during onboarding.
- On failed authentication – ExtremeGuest returns Accept-Reject.

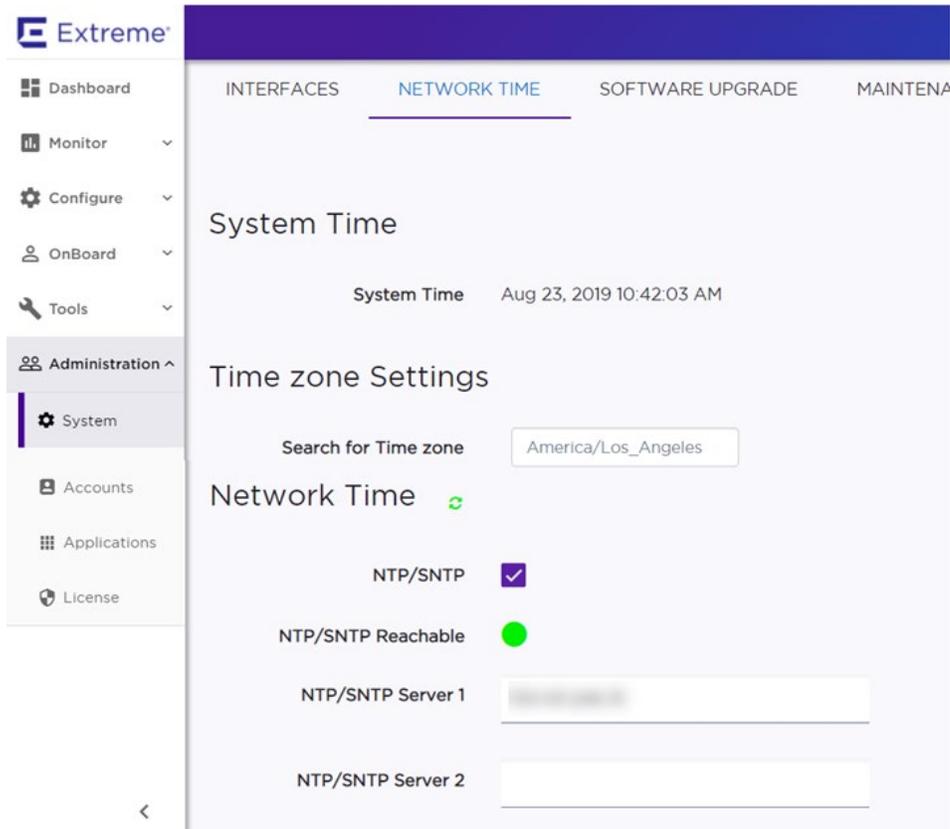
The following sets of configuration are required to enable communication between the ExtremeGuest and ExtremeCloud Appliance servers:

- **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 Pre-configuration

Enable NTP server on ExtremeCloud 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.

V.A ExtremeCloud Appliance NTP Configuration



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.

V.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
```

VI ExtremeCloud Appliance Configuration

Follow the steps below to integrate ExtremeGuest 6.0.0 with ExtremeCloud Appliance 10.56.01 or 10.56.02.

Note

It is assumed your APs are adopted to ExtremeCloud Appliance and deployed in a Distributed site. The APs have been added to the appropriate Device Group and Profile configurations with network association defined. For information on creating a Distributed site with Device Groups, see the ExtremeCloud Appliance User Guide available at <https://extremenetworks.com/documentation>.

- Configure the ExtremeGuest server IP address
- Configure an Extreme Guest Enabled Network
- Add Walled-Garden Rules

VI.A Configure the ExtremeGuest Server IP Address

ExtremeCloud Appliance Configuration

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, <i>EGuest1</i>
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](#).

VI.B Configure an ExtremeGuest Enabled Network

ExtremeCloud Appliance Configuration

The first step in the integration process is to create a captive-portal enabled wireless network and set ExtremeGuest as the captive portal type.

3. Go to **Networks > Add**.

4. Configure the following parameters:

Parameter	Description
Network Name	Provide a user-friendly name for this wireless network. For example: <i>DistributedWiFi</i>
SSID	Provide a string to uniquely identify this wireless network. For example: <i>DistributedWiFi</i>
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 that you 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. See Step 5 below, Add Walled-Garden Rules section.

Use HTTPS for connection	Uses secure HTTPS connection between ExtremeCloud Appliance and ExtremeGuest server. The client is redirected to a secure HTTPS landing page.
--------------------------	---

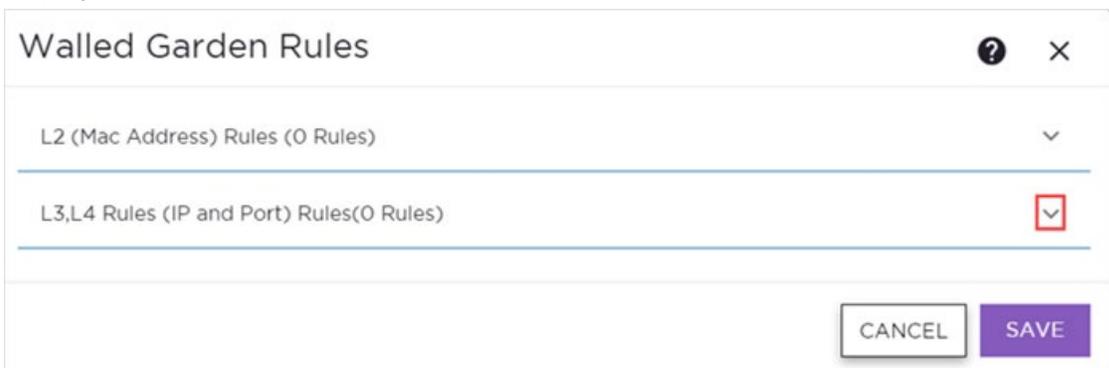
VI.C Add Walled-Garden Rules

ExtremeCloud Appliance Configuration

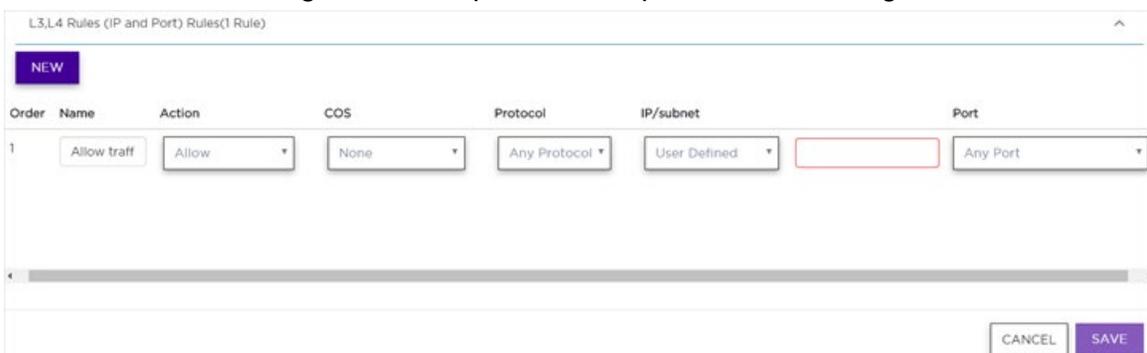
Walled Garden Rules allow guests to sign-in using third-party credentials, such as Facebook, Google, LinkedIn, etc. Follow the steps below to configure social sign-in options.

5. To add Walled Garden Rules:

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



- b. 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.



- c. Click **New** and configure the **Rule** parameters. Each application site requires specific rules to access their site domains.
 - **Name** – Provide a rule name.
 - **Action** – Set action to Allow.
 - **COS** – None
 - **Protocol** – TCP
 - **IP/subnet** – FQDN: Enter the application site FQDN in the adjacent field. Refer to the table below for details.
 - **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

VII 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 Template](#)
- [Host and Apply Splash Template](#)

Note

Auto-staging is supported on ExtremeCloud Appliance v10.56.01 and v10.56.02 for Distributed Deployments. Post ExtremeCloud Appliance and ExtremeGuest 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.

VII.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 distributed mode.

1. Log in to ExtremeGuest and go to **Configuration > AAA > NAS**.
2. To add a NAS configuration, click the + icon on the top, right-hand corner of the screen.

Specify the NAS clients that are allowed to communicate with the ExtremeGuest RADIUS server. It is possible to allow a single IP address or an IP subnet as the NAS client.

The screenshot shows a web form for configuring a NAS client. The form has a title 'NAS' and a text input field for the name, which contains 'XCADistributedD'. Below this are three required fields: 'Description*' with the value 'XCA Distributed De', 'IP Address/mask*' with the value '10.10.10.0/24', and 'Shared Secret*' which is masked with dots. To the right of the 'Shared Secret*' field is a checkbox labeled 'Show Shared Secret'. At the bottom of the form are two buttons: 'Save' and 'Cancel'.

- a. Provide a name uniquely identifying the NAS client network.
- b. Enter a brief description for this NAS configuration.

- c. Enter the IP address and mask of the NAS client.

The NAS clients here are the ExtremeCloud Appliance adopted APs in the distributed site. You can either add a NAS configuration for each AP in the site or add a single subnet NAS configuration. The best practice is to configure the IP address of the APs' subnet. The ExtremeGuest RADIUS server accepts RADIUS requests received from all APs within the specified subnet.

- d. Enter the password required 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](#).

VII.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 following screenshot:

<input type="checkbox"/>	Unregistered	default group for user before registration
<input type="checkbox"/>	DenyAccess	default group for unauthorized user after registration
<input type="checkbox"/>	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.

Group

XCARegistered

Description*: XCA Distributed Deplo

Type: Device

Authorization: GuestAccessPolicy

Save Cancel

Group

XCAUnregisterec

Description*: XCA Distributed Deplo

Type: Device

Authorization: UnregisteredPolicy

Save Cancel

- 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:

<input type="checkbox"/>	UnregisteredPolicy	user not registered
<input type="checkbox"/>	GuestAccessPolicy	for registered user without group assignment

Note

Default Authorization policies can be customized to suite your requirement. You can specify the VLAN guest users will be assigned post authentication.

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

- a. Enter a name uniquely identifying the profile.
- b. Enter a description.

VII.C Configure Onboarding Policy and Rules

ExtremeGuest Configuration

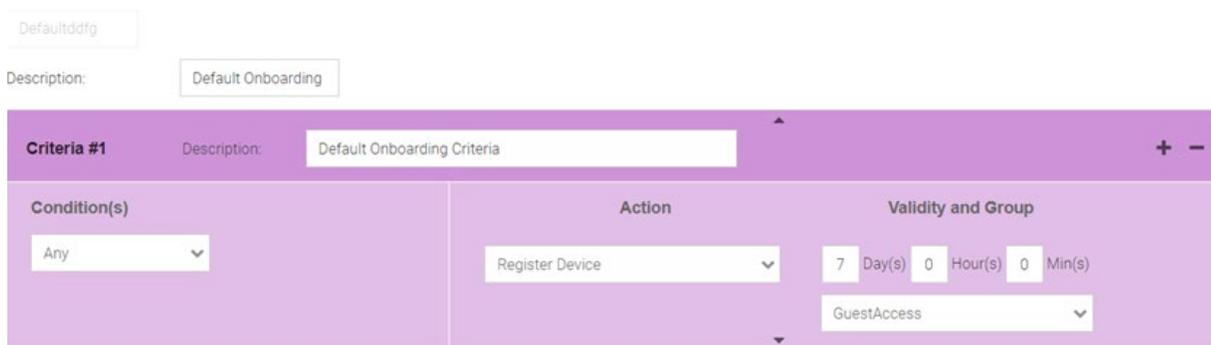
Guest onboarding is the process used to register a wired or wireless client when they join a hotspot network. Onboarding enables hotspot network providers to collect client information, send client passcodes and set up external approval for guest access using rules and policies.

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.



To create a new policy:

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



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

Access time can also be restricted by specifying the **Session Timeout** in the AAA Authorization profile. Alternately, you can use the **Schedule Policy** option to restrict access to specific day(s) and time.

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

- f. Enter a name uniquely identifying the onboarding rule.
- g. Associate the onboarding policy created above (XCADistributed).
- h. Specify network this rule applies to.

Note

Select the ExtremeGuest enabled distributed network you created on ExtremeCloud Appliance in Step 3, [Configure an ExtremeGuest Enabled Network](#). If the network name has not been auto-staged, add the network on ExtremeGuest server. For information, see Step 9, [Configure a Network](#).

- i. Select the location(s) applicable.

Note

Select the ExtremeCloud Appliance distributed site name, auto-staged on ExtremeGuest. If the site name has not been auto-staged, add the site on ExtremeGuest server. For information, see Step 12, [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.

VII.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](#).

The screenshot shows a configuration form for a notification policy. At the top, there is a text input field containing 'XCADistributed'. Below it is a 'Description*' field with the value 'XCA Distibuted Depl'. There are two radio buttons: 'User' (which is selected) and 'Sponsor'. Below these are three sections for notification modes: 'SMS', 'Email', and 'SMS over SMTP', each with a horizontal line underneath for further configuration.

- 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 HTTP API

API Key*:

Source Number:

Message:

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

Email

Enable

Host*:

Sender*:

Security*: Use SMTP with SSL encryption

Port*:

Username:

Password: Show Password

Subject:

Message:

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

SMS over SMTP

Enable

Host*:

Sender*:

Security*: Use SMTP with SSL encryption

Port*:

Username:

Password: Show Password

Email of Recipient*:

Subject *:

Message*:

```
api_id: 3650482
user: ██████████
password: ██████████
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 the <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.

- g. Enter a name uniquely identifying the notification rule.
- h. Associate the notification policy created above.
- i. Specify network this rule applies to.

Note

Select the ExtremeGuest enabled distributed network you created on ExtremeCloud Appliance in Step 3, [Configure an ExtremeGuest Enabled Network](#). If the network name has not been auto-staged, add the network on ExtremeGuest server. For information, see Step 9, [Configure a Network](#).

- j. Select the location(s) applicable.

Note

Select the ExtremeCloud Appliance distributed site name, auto-staged on ExtremeGuest. If the site name has not been auto-staged, add the site on ExtremeGuest server. For information, see Step 12, [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.

VII.E Configure a Network – Optional

ExtremeGuest Configuration

This configuration is optional. On successful integration of the ExtremeCloud Appliance and ExtremeGuest servers (see previous section), site, network, and device group configured on ExtremeCloud Appliance will be available as options in the 'Site', 'Network', 'Device' menus on ExtremeGuest. However, if the network has not been auto-staged, follow the steps below to manually add the network.

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.

The screenshot shows a 'Create Network' dialog box with the following fields and values:

- Name*: DistributedWiFi
- Description: XCADistributedDep
- SSID: DistributedWiFi
- VLAN: 1
- Status:

Buttons: Save, Cancel

- a. Enter the network name.
The name should be same as the wireless network configured on ExtremeCloud Appliance. Refer to the [Configure an ExtremeGuest 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.

VII.F Configure a Site - Optional

ExtremeGuest Configuration

This configuration is optional. On successful integration of the ExtremeCloud Appliance and ExtremeGuest servers (see previous section), site, network, and device group configured on ExtremeCloud Appliance will be available as options in the 'Site', 'Network', and 'Device' menus on ExtremeGuest. However, if the site has not been auto-staged, follow the steps below to add it manually.

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 screenshot shows a modal window titled "Add Site" with a close button (X) in the top right corner. The form contains the following fields:

- Name*: DistributedSite1
- Description: XCADistributedDeploym
- Country: United States (dropdown)
- Region: California (dropdown)
- City: SanJose (dropdown)
- Campus: Campus (dropdown)
- Time Zone: America/Los_Angeles (dropdown)
- Latitude: Latitude
- Longitude: Longitude

At the bottom right, there are two buttons: "Save" (highlighted in blue) and "Cancel" (greyed out).

- a. Enter the name of the APs' site of deployment.
This is the ExtremeCloud Appliance distributed site in which the APs are deployed.
- 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.

VII.G Add a Device - Optional

ExtremeGuest Configuration

This configuration is optional. On successful integration of the ExtremeCloud Appliance and ExtremeGuest servers (see previous section), site, network, and device group configured on ExtremeCloud Appliance will be available as options in the 'Site', 'Network', and 'Device' menus on ExtremeGuest. However, if the APs have not been auto-staged, follow the steps below to add them manually.

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 distributed 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.

- a. Enter a hostname for the AP.
- b. Set the AP model type.

Note

The ExtremeCloud Appliance distributed deployment supports the AP75xx, AP76xx, AP8432, AP8533 and AP5xx model 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.

Note

Select the ExtremeCloud Appliance distributed site name, auto-staged on ExtremeGuest. If the site name has not been auto-staged, add the site on ExtremeGuest server. For information, see Step 12, [Configure a Site](#).

- e. In the **Network** field, select the network.

Note

Select the ExtremeGuest enabled distributed network you created on ExtremeCloud Appliance in Step 3, [Configure an ExtremeGuest Enabled Network](#). If the network name has not been auto-staged, add the network on ExtremeGuest server. For information, see Step 9, [Configure a Network](#).

VII.H Create Splash Template

ExtremeGuest Configuration

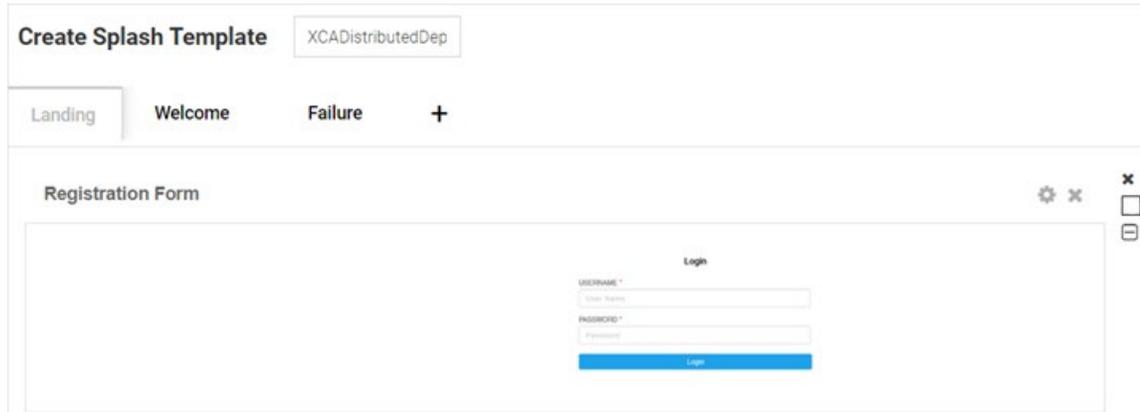
- 15. Go to **Configuration > Splash Templates**.

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.

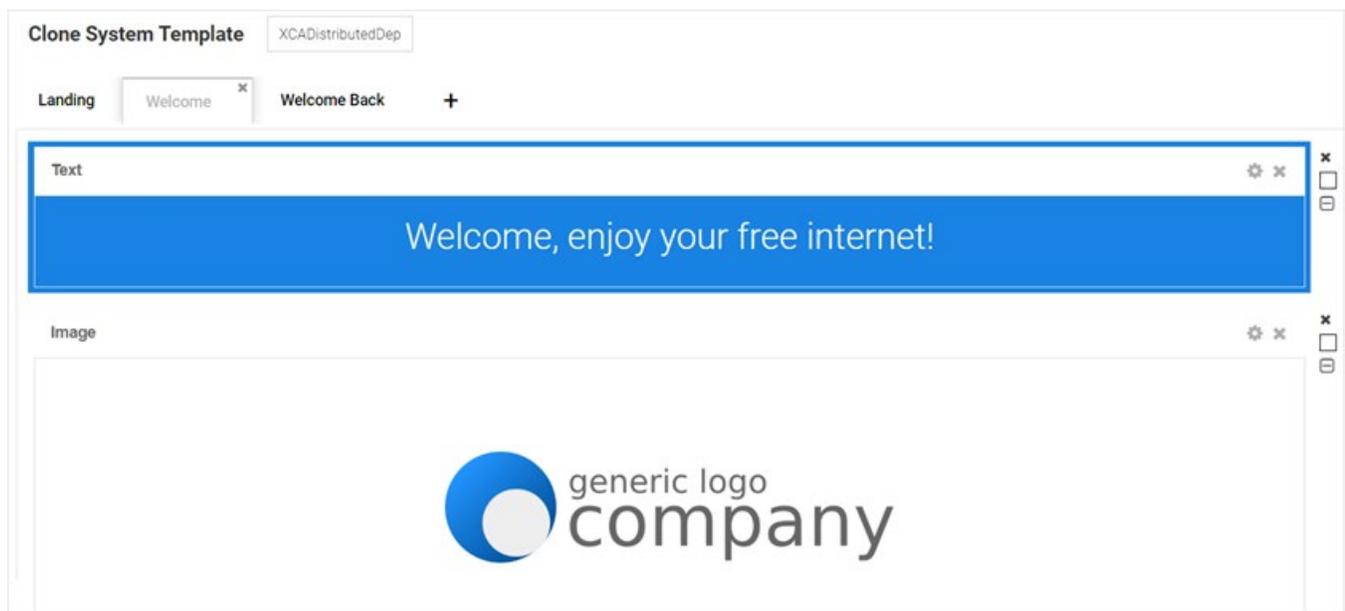
The **Splash Templates** screen has the following sub-screens: **System Templates** and **User Templates**. The *System Templates* tab displays a summary of available captive portal splash screen templates. You

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 used the User Templates option to create a landing page.



You can also clone a system template.



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.

VII.I Host and Apply Splash Template

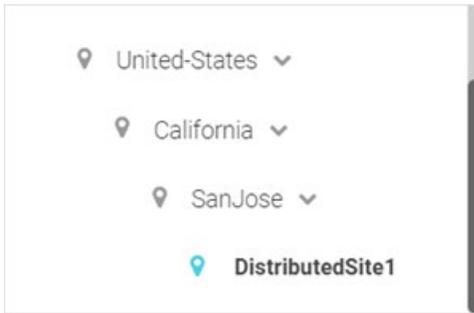
ExtremeGuest Configuration

16. To host and apply the template:

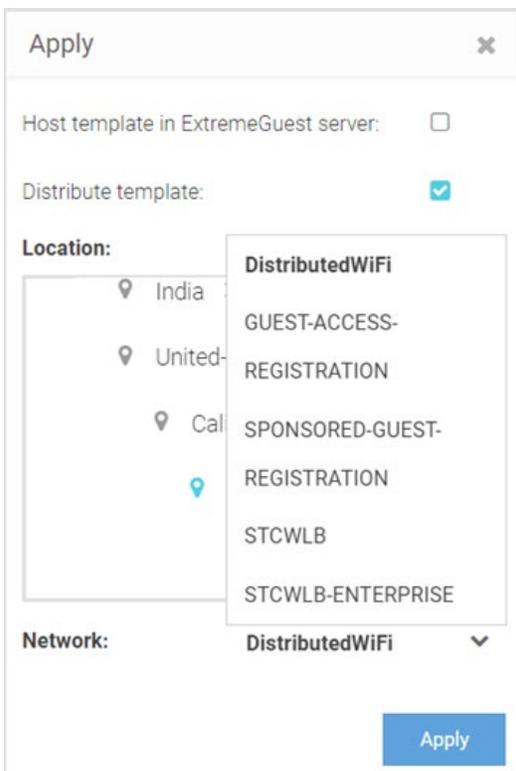
- a. Go to **User Templates**.
- b. Locate the template from the previous step and click the  icon associated with it. The **Apply** box displays.
- c. Specify splash template location. Select **Host template in ExtremeGuest server**: to host the splash template on the ExtremeGuest server. Select **Distribute Template** to host the splash templates on the APs.

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**.



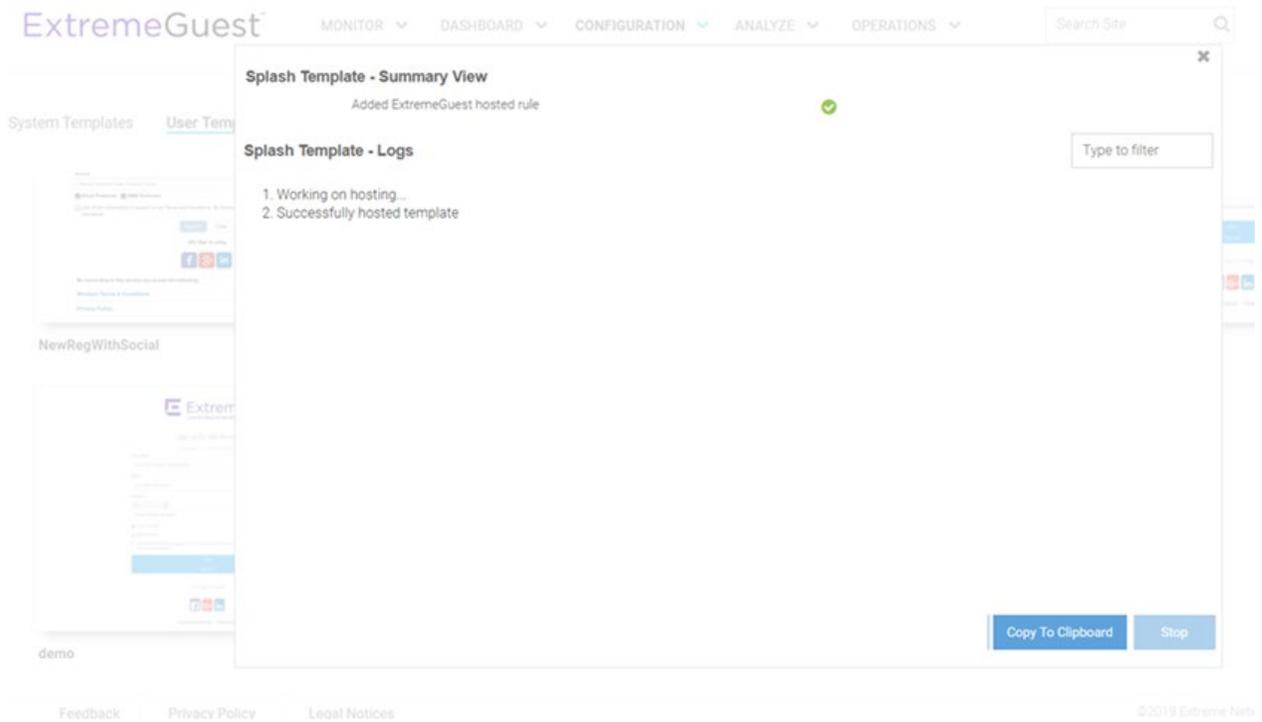
- e. Click the **Network** drop-down menu and select the network you created in Step 9 a, **Configure a Network**.



- 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.



18. To see hosted sites , go to the summary view (follow preceding steps) and select the network. The template status should display as follows:

Splash Templates Mapping Summary

ExtremeWireless WiNG Hosted ExtremeGuest Hosted

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

Location	Name	Template	Status	Action
<ul style="list-style-type: none"> System <ul style="list-style-type: none"> DistributedSite1 	XCADistributedDeployment		upload-success	

Feedback Privacy Policy Legal Notices ©2019 Extreme Networks, Inc. All rights reserved.