

# ExtremeControl<sup>™</sup> - ExtremeGuest<sup>™</sup> v6.0.0 Integration Guide

For Wired-Guest Access

Abstract: This guide describes the steps required to install and deploy ExtremeGuest<sup>™</sup> as the external guest registration and authentication server on Extreme Management Center® - ExtremeControl<sup>™</sup>. This guide covers only the configurations to be set on Extreme Management Center® - ExtremeControl<sup>™</sup> and the pre-configurations needed on ExtremeGuest.

Published: August 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.	Scope	4
III.	ExtremeGuest Overview	5
IV.	Extreme Management Center Overview	6
<b>V</b> .	ExtremeControl Overview	7
VI.	ExtremeControl – ExtremeGuest Integration Overview	8
VII.	ExtremeControl Configuration	9
	Pre-configuration	9
	Authentication and Portal Configuration	
	Switch and Policy Configuration	.19
	Role Policy Configuration and Customization	.21
VIII.	ExtremeGuest Configuration	27
	AAA NAS Configuration	
	Onboarding Policy and Rules Configuration	
	Notification Policy and Rules Configuration	
	Network Configuration	
	Site Configuration	.33
	Device Configuration	.34
	Splash Template Creation	.35
	Splash Template Hosting and Application	.36
	ExtremeControl API Settings Configuration	.38

## I. Pre-requisites

You will need:

- ExtremeGuest running version 6.0.0.
- ExtremeControl running version 8.3.0.
- EXOS Switch running versions 30.2.1.8 or 22.5.1.7.

## II. Scope

This ExtremeGuest with ExtremeControl integration uses MAC authentication for wired-clients connected to ExtremeControl.

## III. ExtremeGuest Overview

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

Starting with this release, ExtremeGuest can be deployed as the external registration and authentication server for wired-clients of ExtremeControl NAC deployments in conjunction with Extreme EXOS switches.

## IV. Extreme Management Center Overview

Extreme Networks' Extreme Management Center® provides a 360 degree view of your wired and wireless network, users, devices and applications with context and scale through integrated management, analytics and policy. It is designed to give you granular insights, visibility and automated control across your networks. It provides single pane of glass management from the wired and wireless edge all the way to the data center, with support for recently acquired switching, access control and data center products, including Ethernet Routing Switches, and Virtual Services Platform.

Extreme Management Center is a suite of applications comprised of the following products:

- ExtremeManagement
- ExtremeControl
- ExtremeAnalytics
- ExtremeCompliance

Extreme Management Center is distinguished by its web-based, unified control interface. Graphical and exceptionally easy-to-use, Extreme Management Center simplifies troubleshooting, help desk support tasks, problem-solving and reporting. ExtremeControl provides specialized visibility and control for managed and unmanaged devices connecting to the network.

## V. ExtremeControl Overview

ExtremeControl securely enables BYOD and IoT to protect your network against external threats. It let's you centrally manage and define granular policies so that you can meet compliance obligations, locate, authenticate and authorize to apply targeted policies to users and devices. ExtremeControl offers both, agent - based and agent-less assessment options. We can install either a persistent or dissolvable agent on the client-end system or the agent can be downloaded via a captive portal website. It can also be installed via a software distribution system such as Group Policy or System Center Configuration Manager. The agent-less assessment does not require an installation or running of any software on the end system.

This integration between ExtremeGuest and ExtremeControl provides you with the ability to enjoy from a highly scalable guest access and guest analytics and reporting. This integration provides unified guest and customer administrator experience for captive portal and access experience.

ExtremeControl related settings are configured on the *Access Control* tab of the *Extreme Management Center* user interface. The Access Control tab comes with a default Access Control Configuration which is automatically assigned to your Access Control engine. You can use this default configuration as is, or make changes to the default configuration, if desired. Alternately, you can add new access control configurations.

This specification guide provides access control configurations that you will need to make on ExtremeControl to deploy ExtremeGuest as the external registration and authentication server.

Going forward, for ease of documentation and readability, Extreme Management Center - ExtremeControl has been referred to as just ExtremeControl.

## VI. ExtremeControl – ExtremeGuest Integration Overview

ExtremeControl version 8.3.0 supports deployment of ExtremeGuest version 6.0.0 as the external registration, authentication and management server for wired-clients of ExtremeControl NAC deployments in conjunction with Extreme EXOS switches.

This guide documents the configurations required to integrate ExtremeControl with ExtremeGuest. This includes:

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

After integration, ExtremeControl and ExtremeGuest communicate through REST API posts.

## VII. ExtremeControl Configuration

## ExtremeControl – ExtremeGuest Integration Overview

To enable a NAC to redirect wired-guest user requests to the ExtremeGuest server, you will need to configure a series of settings on the ExtremeControl server. These configurations have been clubbed into the following groups:

- Pre-configuration
- Authentication and Portal Configuration
- Switch and Policy Configuration
- Role Policy Configuration and Customization

## **Pre-configuration**

This section consists of the following sub-sections:

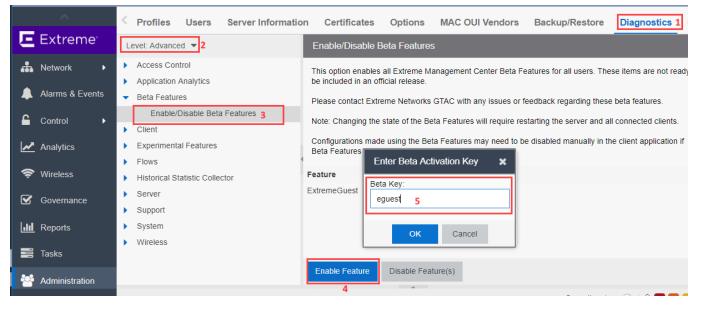
- Enabling ExtremeGuest Beta on ExtremeControl
- Configuring the EXOS Switch

### Enabling ExtremeGuest Beta on ExtremeControl

To enable ExtremeGuest Beta:

- 1. Log in to the Extreme Management Center UI as Administrator and click on the Diagnostics tab.
- 2. Click on Level: and select Advanced.
- 3. Expand the Beta Features node and select the Enable/Disable Beta Features option.

The **Enable/Disable Beta Features** screen displays in the right-hand pane.



4. Click the **Enable Feature** button at the bottom of the screen.

The Enter Beta Activation Key box displays.

5. In the Beta Key: field enter "eguest" and click OK.

ExtremeGuest features will now show up as options on ExtremeControl.

#### **Configuring the EXOS Switch**

#### **Pre-configuration**

ExtremeGuest integration with ExtremeControl only supports MAC authentication at this moment. If you have a new EXOS switch or want to reconfigure an existing one, you may have to make some configuration changes on it.

The following steps detail the basic, recommended switch configuration. However, before implementing these changes, we recommend that you save your existing switch configuration. This will make it easier for you to revert back later if required.

- 1. Log in to the EXOS switch (for example, X450G2-48t-10G4 version 22.5.1.7).
- 2. (Optional) Execute the following command to save your current configuration in case you need to restore: save configuration {name}
- 3. Reset switch to factory configuration by executing the following command:

```
unconfigure switch all
```

Where, 'all' is an optional parameter. The switch reboots and you will be promoted to log in.

- 4. Log in and click **No** at each **yes/no** prompt until you reach the CLI prompt.
- 5. Execute the following command to assign the switch a VLAN and an IP address:

configure vlan {VLAN-ID} ipaddress {ip-address} {mask}

In this example, we can assign VLAN '*Default*' and the IP address is '10.50.76.80/18' by executing the following command:

configure vlan Default ipaddress 10.50.76.80 255.255.192.0

6. Execute the following command to add a default route:

configure iproute add default {default-gateway}

For Example:

configure iproute add default 10.50.64.1

- 7. To allow ExtremeControl manage your switch, enable SNMP by executing the following commands:
  - a. Enable SNMP v1 and v2.

enable snmp access snmp-v1v2c

b. Enable SNMP v3.

enable snmp access snmpv3

c. Specify the SNMP profile ExtremeControl will use to manage the EXOS switch. configure snmp add community readwrite public

Note

The preceding step 7 c. enables ExtremeControl to manage the switch through SNMP using the **public\_v1\_Profile** profile.

- 8. Configure netlogin by executing the following commands:
  - d. Enable a netlogin policy.

enable policy

e. Enable web-based authentication of MAC addresses.

enable netlogin dot1x mac web-based

f. Specify the port on which MAC authentication is to be enabled.

enable netlogin ports {port-number} mac

g. Add a MAC list.

configure netlogin add mac-list ff:ff:ff:ff:ff 48

## Authentication and Portal Configuration

#### ExtremeControl Configuration

After enabling ExtremeGuest Beta, you will have to configure a series of settings to enable ExtremeControl to communicate with ExtremeGuest. These configurations have been grouped into the following sections:

- Configuring RADIUS Server Settings
- Configuring Authentication Settings
- Configuring Captive-portal Settings
- Configuring Authorization Settings

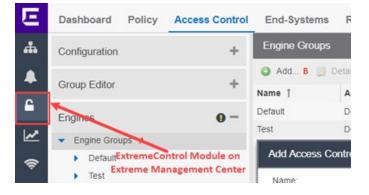
#### **Configuring RADIUS Server Settings**

#### Authentication and Portal Configuration

This section lists the steps required to configure ExtremeGuest as the external RADIUS server on the ExtremeControl server.

To configure the RADIUS server:

1. Log in to the **Extreme Management Center** UI and navigate to the **ExtremeControl** module.

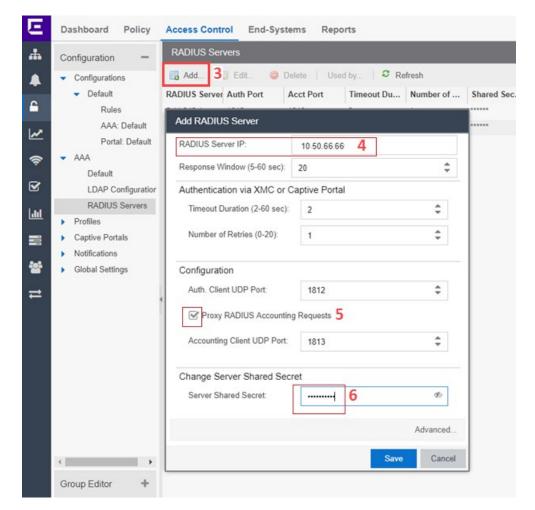


2. Go to Access Control > Configuration > AAA > RADIUS Servers.



The **RADIUS Servers** screen displays in the right-hand pane.

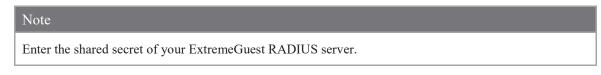
3. On the RADIUS Servers screen, click Add. The Add RADIUS Server window displays.



4. In the RADIUS Server IP: field enter the IP address of your ExtremeGuest hotspot server.

In this example, the RADIUS server IP address is configured as 10.50.66.66.

- 5. Select the **Proxy RADIUS Accounting Requests** option to have a NAC with this configuration forward accounting messages to the ExtremeGuest server.
- 6. In the Server Shared Secret field enter the shared secret.



### **Configuring Authentication Settings**

This section lists the steps required to configure the settings that will allow ExtremeControl to forward wiredguest user authentication requests to the ExtremeGuest server.

1. Go to Access Control > Configuration > AAA.

<ul> <li>Configurations</li> </ul>	Authenticate Requests Locally	tor 3 MAC (AII) IS MAC (PAP) D MAC (CHAP) IS MAC		
<ul> <li>Default</li> </ul>				
• AAA Default 2	Local Password Repository:	None	•	
LUAP Consignations	Join AD Domain:	Auto Detect	•	
RADIUS Servers Profiles	Update Trusted Authorities	No information available.		
Captive Portals	Authentication Rules			
Notifications     Global Settings	🗿 Add 👩 Edit 🌾	Delete 🔺 Up 🔻 Down		
, come comp	Authenticat User/MAC/	Location Authenticat Primary RA Secondary 3rd	RADIUS 4th RADIUS.	. Inject Au
	Any *	Any Proxy RADL 134.141.60 None Non	e None	Extreme 0
	Edit User to Authentication	on Mapping	×	
	Authentication Type:	Any	*	
	User/MAC/Host:   Patte	m O Group		
	Location:	Any	-	
	Authentication Method:	Proxy RADIUS (Failover) 5	-	
-	Primary RADIUS Server:	10.50.66.66 6	*	
	Secondary RADIUS Serv	None None	*	
	and RADIUS Server	View RADIUS Attribute Configuration ( Read-Only )	×	
	4th RADIUS Server	Name: Extreme Guest		
	5th RADIUS Server:	Enable Port Link Control:		
	6th RADIUS Server:	Extreme-Guest-NAS-IP=HNAS_IPH		
	7th RADIUS Server:		-	
	Ith RADIUS Server:		Close	
	Inject Authentication Attr	s: ExtremeGuest 7	*	
	Inject Accounting Attrs:	ExtremeGuest 8	*	
	LDAP Configuration:	None	-	
· · ·	LDAP Policy Mapping:	Default		
Group Editor +				

2. Create an **Advanced AAA Configuration**. This can be done either by right-clicking a basic configuration and choosing **Make Advanced ...** or selecting the **Advanced Configuration** checkbox when creating a new one.

In this example, we are converting the existing "Default" AAA configuration to advanced.

The Advanced AAA Configuration – Default screen displays in the right-hand pane.

- 3. Clear the Authenticate Requests Locally For: checkbox to disable local authentication.
- 4. In the Authentication Rules area, either modify the first entry or add a single rule.

In this example, we are adding a new rule. The Edit User to Authentication Mapping window displays.

- 5. Set the Authentication Method: to Proxy Radius (Failover).
- 6. In the **Primary Radius Server:** field enter the same IP address (RADIUS server IP address) that you had configured in Step 4 of the preceding section Configuring RADIUS Server Settings.

In this example, we will set the IP address as **10.50.66.66**, since that's the RADIUS server IP address we had set earlier.

- 7. Set Inject Authentication Attrs to ExtremeGuest.
- 8. Set Inject Accounting Attrs to ExtremeGuest.

#### **Configuring Captive-portal Settings**

Authentication and Portal Configuration

This section lists steps required to configure the ExtremeGuest captive-portal settings on ExtremeControl.

- 1. Log in to the Extreme Management Center UI and go to **Access Control > Configuration > Captive Portals**.
- 2. Create a new captive-portal configuration or select an existing captive portal.

In this example, we have selected the existing "Default" captive-portal configuration.

- Captive Portals
  - Default
- 3. Expand the captive-portal node and click on Website Configuration.

In this example, we expanded the 'Default' captive portal node and click on Website Configuration.

The Website Configuration screen displays in the right-hand pane.

	Website Configuration		
Configuration -	website Configuration		
Configurations			
Default			
AAA     Profiles			
Captive Portais	Redirect to ExtremeGuest		
<ul> <li>Default</li> </ul>	Traffic sent to http://\$(naclp)/redirect_with_info will b	e redirected to the base url along with the specified attributes.	
Network Settings Administration 3	Base Urt: https://10.50.66.66/landing/	5 URL or IP Address of external captive portal management.	
Administration 3 Website Configuration	Shared Secret	6 Ø Exposes the admin-specific redirect REST interface.	
Notifications	Configuration: ExtremeGuest	7	
Global Settings			
	Attributes to Send		
	Check which attributes to send, followed by the d	lesired key name.	
	Original URL: 🗹 originalUrt		
	Client IP: 😴 clientip		
	Clean Marc D2 Internation		
	Client Mac: 🔗 clientMac		
	Client Mac: 🗭 clientMac Captive Portial 🧭 cpName		
	Captive Portal 🧭 cpName		
	Captive Portal 🧭 cpName Name NAC IP 🗭 nacip		
	Captive Portal & cpName Name NAC IP & naCip NAC Group & nacGroupName		
	Captive Portal 🧭 cpName Name NAC IP 🗭 nacip		
	Captive Portal & cpName Name NAC IP & naCip NAC Group & nacGroupName		
	Captive Portal & cpName Name nacip NAC IP & nacip NAC Group & nacGroupName Switch IP & switchPort Switch Port & switchPort		
Group Editor +	Captive Portal & cpName NAC IP & naclp NAC Group & nacGroupName Switch IP & switchip		
Group Editor +	Captive Portal Capture Portal Capture Portal Capture Portal Capture Portal Port Port Port Port Port Port Port Port	*\${clientip}&clientMac=\${clientMac}&cpName=\${cpName}&nacip=\${nacip}&nacGroupNa	

4. Select the Redirect to ExtremeGuest checkbox.

 In the Base URL: field, enter the URL in the following format: "https://" + ExtremeGuest's IP address + "/landing/"

For example: https://10.50.66.66/landing/

IMPORTANT: The "*I*" at the end is mandatory. Be sure to include it.

6. In the Shared Secret: field provide the shared secret.

Note

Along with an Extreme Management Center username and password, the secret configured here must be supplied in the "Redirect" REST POST command to reauthenticate an End System on ExtremeGuest. This is documented in the ExtremeGuest User Guide under the ExtremeControl API Settings section, available at https://extremenetworks.com/documentation.

7. In the Configuration field, enter ExtremeGuest.

### **Configuring Authorization Settings**

#### Authentication and Portal Configuration

This section lists the steps required to configure the settings that will allow ExtremeControl to forward wiredguest user authentication requests to the ExtremeGuest server.

1. Go to Access Control > Configuration > Configurations.

Со	nfiguration		-
•	Configurations	←	

2. Create a new configuration or select an existing configuration.

In this example, we have selected the existing "Default" configuration.

3. Expand the **Default** configuration and select the **Portal: Default** node.

The **Portal: Default** screen displays in the right-hand pane.

Configuration	-	Portal: Default		
<ul> <li>Configurations</li> </ul>		Portal Configuration:	Default	-
<ul> <li>✓ Default</li> <li>Rules</li> <li>AAA: Default</li> </ul>		Features Registration is disabled,	remediation is disabled.	
Portal: Default	3			

- 4. On the **Portal: Default** screen use the **Portal Configuration** drop-down menu to select the **Default** captive portal from Step 2 of the preceding section Configuring Captive-portal Settings.
- 5. Go one node up and select the **AAA: Default** node.

E	Dashboard Policy Access C	ontrol End-Systems Re	ports					
#	Configuration –	Advanced AAA Configuration		Select AAA	Configuration			
	<ul> <li>Configurations</li> </ul>	Select AAA Configuration	6		Gonngaration		7 -	-
<b></b>	Default     Rules     5	Authenticate Requests Locally	for: 🗌 MAC (All)	Default				- 1
<u>~</u>	AAA: Default Portal: Default	Local Password Repository:	Default				Canc	el
Ş	- AAA	Join AD Domain:	Auto Detect				•	
Ø	Default LDAP Configurations	Update Trusted Authorities	No information av	vailable.				
<u></u>	RADIUS Servers Profiles	Authentication Rules						
	Captive Portals	Add   Edit	🕽 Delete   🔺 Uj	p 🔻 Down				
	<ul> <li>Default</li> </ul>	Authenticat User/MAC/	. Location	Authenticat	Primary RA	Secondary	3rd RADIUS	. 4th I
*	Network Settings	Any *	Any	Proxy RADI	134.141.60	None	None	None
	Administration							

The Advanced AAA Configuration – Default screen displays in the right-hand pane.

6. Click Select AAA Configuration tab.

The Select AAA Configuration box displays.

- 7. Use the drop-down menu to select the AAA configuration you created in Step 2 of the Configuring Authentication Settings section. Since, for this example, we had selected the "**Default**" AAA configuration, we will leave the AAA Configuration as "**Default**".
- 8. Go to Access Control > Configuration > Profiles.



9. Add a new profile named "ExtremeGuest".

•	Profiles				
	Access Point NAC Profile				
	Admin NAC Profile				
Administrator NAC Profile					
Allow NAC Profile					
	Assessing Profile (Auto)				
	Default NAC Profile				
	Enterprise Access NAC Profile				
	ExtremeGuest				
	ExtremeGuest Unregistered Profile (A				

The Access Control Profile - ExtremeGuest screen displays in the right-hand pane.

#### 10. Configure the following **ExtremeGuest** profile settings:

Ε	Dashboard Policy Access Control	End-Systems Reports		Q ? ≡
<b></b>	Configuration –	Access Control Profile - Extreme	Guest	
	▼ Detaun Rules	Reject Authentication Requests		
<b></b>	AAA: Default	Authorization	10 a.	
	Portal: Default	Accept Policy: No Policy		-
»	<ul> <li>AAA</li> <li>Profiles</li> </ul>	Replace RADIUS Attributes wit	th Accept Policy 10 b.	
- <del>-</del> -	Access Point NAC Profile	🗹 Use Quarantine Policy	Quarantine	~
	Admin NAC Profile	Use Failsafe Policy on Error	Failsafe	~
	Administrator NAC Profile Allow NAC Profile	Restrict to End-System Zone	None	~
	Assessing Profile (Auto) Default NAC Profile	Assessment		
**	Enterprise Access NAC Profile	Enable Assessment		
	ExtremeGuest	Assessment Configuration:	Default	~
1	ExtremeGuest Unregistered Profile (A ExtremeGuest User Profile (Auto)	Assessment Interval:	1 🚔 Weeks	~
	Failsafe Profile (Auto)	Hide assessment details and re	emediation options from end user	
	Guest Access NAC Profile	☑ Use Assessment Policy	Assessing	ents 💌
	Group Editor +			
	Engines 0+			
	O Enforce ▼ C Refresh			Save Cancel

- a. In the Accept Policy: field select -- No Policy --.
- b. Clear the **Replace RADIUS Attributes with Accept Policy** checkbox and all other associated checkboxes.
- 11. Go back to **Access Control > Configuration > Configurations** and select the configuration you had created in Steps 1 & 2 of this section Configuring Authorization Settings.

We will select the "**Default**" configuration, since we had modified the Default configuration as part of this example.

12. Expand the **Default** configuration node and click on **Rules**.

Configuration	-
<ul> <li>Configurations</li> </ul>	
<ul> <li>Default</li> </ul>	
Rules	
AAA: Default	
Portal: Default	

The **Rules** screen displays in the right-hand pane.

13. Add a new rule and configure the following settings. This rule should match all traffic type.

Dashboard Policy Access Contro	End-Syst	Add Rule	
Configuration -	Rules	Name:	EGuest 13 a.
Configurations     Default	Add  En Rule Acce	Description:	Match all traffic 13 c.
Rules AAA: Default Portal: Default	Serv	Group Label:	None
► AAA	Print	Conditions All condition	ons should be set to value "Any". 13 d.
Profiles     Access Point NAC Profile	VoIF	Authentication Method:	Any
Admin NAC Profile	Adm	User Group:	Any
Administrator NAC Profile	✓ Defa	End-System Group:	Any
Assessing Profile (Auto)		Device Type Group:	Any
Default NAC Profile Enterprise Access NAC Profile	Accept Po	Location Group:	Any
ExtremeGuest	Bala ( Bara)	Time Group:	Any
ExtremeGuest Unregistered Profile (A ExtremeGuest User Profile (Auto)	Role / Servio		
Failsafe Profile (Auto)		Actions Profile:	ExtremeGuest 13 e.
Group Editor +		Portal:	Default 13 f.
Engines 0+		Zone:	None
<pre>9 Enforce ▼ 14</pre> C Refresh			13 g. Save Cit

- a. In the **Name:** field, provide a name for this rule uniquely identifying its purpose. In this example, we have named the rule **EGuest**.
- b. Select the Rule Enabled checkbox to enable the rule.
- c. Provide a description for the rule uniquely identifying its purpose.
- d. In the Conditions section, ensure all conditions are set to "Any".
- e. In the **Actions** section, select the profile you created is Step 9 of this section Configuring Authorization Settings.

In this example, we will select "ExtremeGuest", since we created it in Step 9.

f. In the **Actions** sections, select the captive portal you created in Step 2 of the Configuring Captiveportal Settings section.

In this example, we will select the "Default" portal, since we modified it as part of this example.

- g. Click Save.
- 14. Click **Enforce**. Select your NAC, select the "**Force Reconfiguration for All Switches**" checkbox, then click "**Enforce All**" again.

	Engine	IP Address	Status	Result	Details	
	10.50.66.25	10.50.66.25	Audit Completed	Errors	Expand for details	
- Ear	- Deconfiguratio	on for All Suitches		ation for Canting	Dortal	
For	ce Reconfiguratio	on for All Switches	Force Reconfigure	ation for Captive	Portal	

## Switch and Policy Configuration

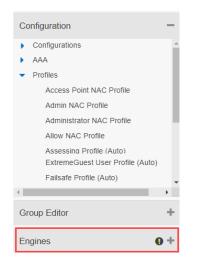
### ExtremeControl Configuration

This section describes the following set of configurations:

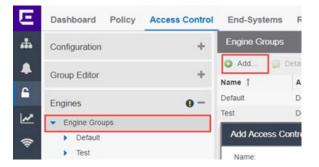
Configuring the Switch on ExtremeControl

### Configuring the Switch on ExtremeControl

1. Log in to Extreme Management center UI and go to Access Control > Engines.



2. To create a new engine group, right-click on **Engine Groups** and click "**Add..**". Alternately select an existing engine group.



The Add Access Control Engine Group box displays. Enter the details and click Add.

In this example, we have added a new engine group "Test".

3. In the engine group's details panel, ensure that the access control configuration associated matches the configuration you created in Step 2 of the Configuring Authorization Settings section.

4. If the configuration does not match, then click Choose Configuration ...

The Select NAC Configuration for Engine Group window displays in the right-hand pane.

Engines	Facility On Warrant Default	
Engine Settings	Engine Settings: Default Eng Select NAC Configuration for Engine Group	
Access Control Configuration	- Defa Choose an Access Control Configuration for this Engine Group. This configuration the rule engines for authentication and authorization, as well as the captive portal	
Edit Configuration	Defa configuration.	
Choose Configuration 4	Asse Configuration: Default 5	•
Load Balancing	Save	Canc
Load Balancing: Di	isabled	

5. Use the **Configuration** drop-down menu to associate the access control configuration.

In this example, we will select the "Default" configuration, since we modified it earlier.

- 6. Expand the **Access Control > Engines** tab and select the engine group you created/selected in Step 2 earlier in this section.
- 7. Add your NAC engine (device) to the engine group, then click on the NAC engine (device) you added.

To do this, go to the **Access Control Engines** tab and click "**Add..**" The **Add Access Control Engine** box displays. Enter the engine's IP address and name and click **Add**.

In this example, we have added device with IP address "10.50.66.25" to the engine group "Test".

Eng	jines		0-
•	Engine Gr	oups	
	Defau	It	
,	<ul> <li>Test</li> </ul>		
	S.,	10.50.66.25/10.50	0.66.25

- 8. Click on the **Switches** tab. Select an existing switch from the left. If your switch is not present, proceed to steps 10a-10d below.
- 9. Click Add...



The Add Switches to Access Control Engine Group: <NAME> screen displays.

- 10. Click Add Device. In the Add Device box, enter the appropriate information and click OK.
- 11. Refresh the left menu by collapsing and expanding the tree until your new device shows. Select it.
- 12. Configure the following settings:

Configure Device: 10.50.66.15			×
Switch Type:	Layer 2 Out-Of-Band		•
Primary Engine:	10.50.66.25/10.50.66.25	10a.	-
Secondary Engine:	None		-
Auth. Access Type:	Network Access		-
Virtual Router Name:			
RADIUS Attributes to Send:	None	10b.	•
RADIUS Accounting:	Enabled	10c.	•
Management RADIUS Server 1:	None		-
Management RADIUS Server 2:	None		~
Network RADIUS Server:	None		-
Policy Domain:	Default Policy Domain	10d.	•
Advanced Settings			
		Sa	Close

a. In the **Primary Engine:** field, use the drop-down menu to set the **NAC engine (device)** you added to your engine group in Step 7 earlier in this section.

In this example, we will select the "10.50.66.25/10.50.66.25"

- b. Set the RADIUS Attributes to Send: option to "None".
- c. Set the **RADIUS Accounting:** option to **Enabled**.
- d. In the **Policy Domain:** field, select the policy domain. This domain will be used later in the following section.

In this example, we will select the "Default Policy Domain".

13. Click **Enforce** to push these new settings to the NAC and Switch.

## **Role Policy Configuration and Customization**

### ExtremeControl Configuration

We need to configure policy roles to match the filter-ids ExtremeGuest will return upon successfully authenticating an end-system. For this exercise, we will create two roles, *ExtremeGuest User* and *ExtremeGuest Unregistered*.

This section describes the following configurations:

- Creating Policy Roles
- Redirecting ExtremeGuest Unregistered Users to NAC captive-portal Redirector

### **Creating Policy Roles**

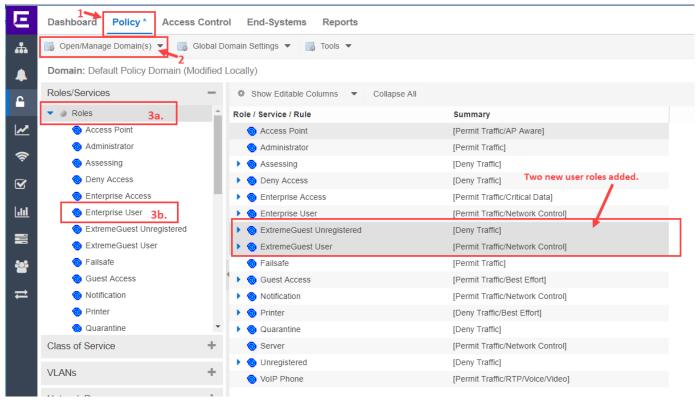
**Role Policy Configuration and Customization** 

To create policy roles:

- 1. Click on the **Policy** tab.
- 2. Expand the **Open/Manage Domain(s)** menu and select the policy domain you selected in Step 10d. in the preceding section.

In this example, we will select the "Default Policy Domain".

3. On the selected policy domain, add the following two Roles: *ExtremeGuest User* and *ExtremeGuest Unregistered*. To add the two new user roles:



- Expand the Roles/Services node, then expand Roles.
   The Role / Service / Rule screen displays in the right-hand pane.
- b. Right-click on the Enterprise User role and select *copy* from the contextual help displayed.
- c. Paste the copied role within the Role / Service / Rule table in the right-hand pane.A new user role named "Enterprise User (1)" is added.
- d. Right-click on this new role and rename it to ExtremeGuest User.
- e. In the same manner create another copy of the *Enterprise User* role and rename it to **ExtremeGuest Unregistered**.
- 4. Go to Open/Manage Domain(s) and Save the changes.

5. Click Enforce to push these changes to the switch.

#### **Redirecting ExtremeGuest Unregistered Users to NAC Captive-portal Redirector**

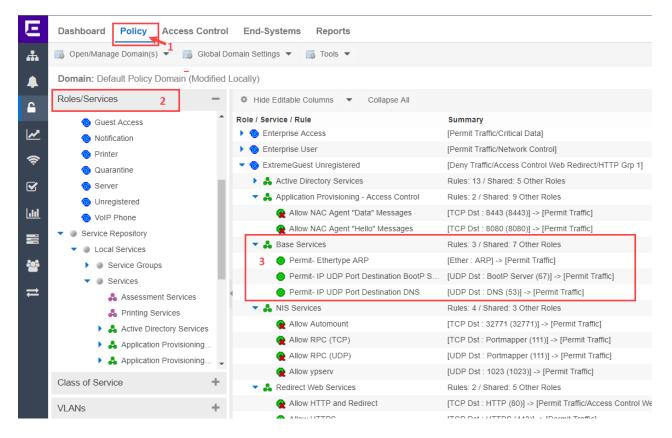
**Role Policy Configuration and Customization** 

This section describes how to redirect ExtremeGuest Unregistered users, created in Step 3e. of the preceding section, to the NAC captive portal redirector. In order to do this,

1. Click on the **Policy** tab, expand the **Roles/Services** node, then expand **Roles**.

The Role / Service / Rule screen displays in the right-hand pane.

- 2. On the Role / Service / Rule screen, expand the ExtremeGuest Unregistered role.
- 3. Enable all Base Services by right-clicking them and selecting Enable Rule(s).



4. To enable redirect http traffic on the policy, configure the following settings:

Ξ	Dashboard <b>Policy</b> Access Cor	ntrol	End-Systems	Reports			HTTP Redirect	Configuration	×		Q ·	? ∃
<b>.</b>	🐻 Open/Manage Domain(s) 🔻 📑 Glo	oal Don	nain Settings 🔻 📑	Tools 💌			controller (EWC), v	is only supported by the w which supports only a singl	le URL			
	Domain: Default Policy Domain (Modif	ied Lo	cally)				HTTP Redirect, the	ole rules in the same role s ey must use the same redi WC does not support speci	rect			
2	Roles/Services	-	Role: ExtremeGue	est Unregistered			the sockets that ap	oply to redirect directly, but ocket from the rule definition				
~	Roles 4a.     Access Point	1	General VLAN	Egress Mappi	ings Port Default L	Jsage	support only role le	s are supported). Other pla evel redirect, support 2 UR				
_	<ul> <li>Administrator</li> </ul>	11	Name:	ExtremeGuest Uni	registered			r load balancing and fault ly redirect traffic on the soc	ckets			
(î)	Assessing	н	Description: T	he Unregistered Ro	ole is used in Extreme Ma	anagen	Listen Sockets:	80, 8080 <b>4e.</b>		yste	Edit.	
2	<ul> <li>Deny Access</li> <li>Enterprise Access</li> </ul>	н	TCI Overwrite: Di	isabled			4f.			L '		
<u>.lıl</u>	Enterprise User	11	Default Actions				Group Index 1	oup Index Config 🛛 📄 Eo	dit >	-		-
	<ul> <li>ExtremeGuest Unregistered4a.</li> <li>ExtremeGuest User</li> </ul>	-	Access Control:	Deny Traffic4b.			1	1	I			
	Failsafe			VLAN:								
<b>=</b>	<ul> <li>Guest Access</li> <li>Notification</li> </ul>			Service ID:								
	Printer		Class of Service:	Access Contro	ol Web Redirect (Priority:	3) <b>4c.</b>						
	<ul> <li>Quarantine</li> <li>Server</li> </ul>		System Log:	Disabled		Cre	eate Redirect Grou	ıp				×
	<ul> <li>Unregistered</li> </ul>	-	Audit Trap:	Disabled		Gro	up Index:	1 <b>4g.</b>			<b></b>	٦
	Class of Service	+	Disable Port:	Disabled			L (Server Index 1):				•	
	VLANs	+	AP Aware:	Disabled		UR	· /	http://10.50.66.50:80/i 4h.	4i.	with_int		-
	Network Resources	+	HTTP Redirect:	View/Edit Redire	ct Group(s) 4d.			Add Secondary URL	ОК		Cance	
	Devices/Port Groups	+	Traffic Mirror:	Disabled			<ul> <li>Mirror</li> </ul>	r First 15 Packets				
	Enforce     Auto Collapse Pan	ol						Hide E	Disabled	Hic	ie All	
	Enforce      Auto Collapse Pan	CI	Services									-

- a. Expand the **Role** node and select the **ExtremeGuest Unregistered** role. The **Role: ExtremeGuest Unregistered** screen displays in the right-hand pane.
- b. Set the Access Control: option to Deny Traffic.
- c. Set the Class of Service: option to Access Control Web Redirect (Priority: 3).
- d. Set the **HTTP Redirect** option to **View/Edit Redirect Group(s)....** The **HTTP Redirect Configuration** window displays.
- e. On the HTTP Redirect Configuration window, in the Listen Sockets: field, enter "80, 8080".
- f. Click on + Add Group Index Config.
   The Create Redirect Group box displays.
- g. Set the Group Index as "1".
- h. In the **URL (Server Index 1):** field enter the URL of NAC along with port 80. Use the following format:

http://10.50.66.25:80/redirect\_with\_info

IMPORTANT: Ensure the URL has "/redirect\_with\_info" appended in the end.

- Click OK twice to close both windows.
   IMPORTANT: Ensure that the HTTP Redirect field is updated with the group (Group 1), created in the previous steps.
- 5. Go to **Open/Manage Domain(s)** and **Save** the changes made to the Policy Domain.
- 6. Click **Enforce** to push configuration to the switch.
- 7. To create a service to allow https traffic to ExtremeGuest's IP address:

Ε	Dashboard Policy * Access Control End-Systems Reports
#	7a.         Image Domain(s) ▼       Image Domain Settings ▼         Image Domain(s) ▼       Image Domain Settings ▼
	Domain: Default Policy Domain (Modified Locally)
6	Roles/Services - Vide Editable Columns - Collapse All
	Services 7a. Rule Summary
~	Assessment Services Redirect [TCP Dst : HTTP (80)] -> [Permit Traffic/Access Control Web Redirect]
_	Printing Services RAllow HTTPS [TCP Dst : HTTPS (443)] -> [Permit Traffic]
Ś	Active Directory Services Redirect EGuest
$\mathbf{\mathbf{S}}$	Application Provisioning
1	Application Provisioning         Edit Traffic Description         X
<u>.111</u>	Application Provisioning
	Base Services     Traffic Classification Layer:     All Layers
	Lenv Spoofing and Oth         Traffic Classification Type:         IP Socket Bilateral         7c.
**	A Deny Unsupported Prot
	Limit Exposure to DoS
Ħ	NIS Services
	7b. The Redirect Web Services Value: 10.50.66.66 7d.
	RIIOW HTTP and Re
	Realize Allow HTTPS Iraffic Classification Optional Value
	Redirect EGuest     Well-Known Value: HTTPS (443)     7e.
	Class of Service  Single Value: 443
	VLANs + O Range: Start Value: End Value:

- a. Click on the Policy tab, expand the Roles/Services node, then expand Services.
- b. Right-click the **Redirect Web Services** node and add a rule, enter a name for the rule, and click **OK**.

For this example, we have named the rule as **Redirect EGuest**.

- c. Set the Traffic Classification Type: option to IP Socket Bilateral.
- d. In the **Traffic Classification Value** area, for the **Value** field, enter the ExtremeGuest server's IP address.

For this example, we will enter "**10.50.66.66**", because that is the ExtremeGuest server IP address we have configured in all previous configurations.

- e. In the **Traffic Classification Optional Value** area, set the **Well-Known Value:** option as **HTTPS** (443). Save and close window.
- 8. Click the new service change the Access Control setting as shown in the screenshot below.

		100 A. C.		
Network +	(j) Open Manage Domain(s) • 🔂 Olobal Domain Settings •	🌆 Tosh 💌		
Alarms & Events	Domain: Default Policy Comain			
Control +	Roles/Services	- Rule: Redirect E	Guest	
Analytics	a Roles     a Service Repository	* Sarvice Name Description	A Redirect Web Services	
• Weekess	a Services     a Service Groups	1	Enabled	
Governance	g Services     Assessment Services	Rule Type	All Devices	 Stow all rule types.
[ Reports	A Printing Services     Active Directory Services	TCI Overwrite	Disabled	
Tinks	<ul> <li>Application Previsioning - Access Central</li> </ul>	Traffic Description	'n	
Administration	Application Provisioning - Basic     Application Provisioning - Supplemental	Type: Value	IP Socket Destination 96 96 96 250 HTTPS	
2 Connect	A Desis Services     A Deny Spectra and Other Administrative Protocol     A Deny Unsupported Protocol Access     A Lent Exposure to DoS Attacks     A Starticos     A Restruct Web Services     Altern RDP	Actions	Permit Traffic	
	Redirect EGuest     A Secure Guest Access Internet Access Univ	1000 Contract Contract		
	A Threat Management     a Global Services (A8 Domains)	System Log Audit Trap	Disabled Disabled	
	Class of Service	+ Disable Port	Disabled	
	VLANs	+ Millinger	Disting	
	Network Resources	+ Quarantine Rol	e Disabled	
		Traffic Mirror	Disabled	Mirror First 15 Packats

## VIII. ExtremeGuest Configuration

## ExtremeControl – ExtremeGuest Integration Overview

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

Follow the steps below:

## **AAA NAS Configuration**

- 1. Log in to ExtremeGuest UI 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 single IP address or an IP subnet as the NAS client. Also specify the shared secret.

This configuration is about enabling ExtremeGuest to receive and process RADIUS request from wiredguest users of ExtremeControl NAC deployments.

NAS		_			
NAC-wired	2 a.				
Description*:		NAC de	ployment	2 b.	
IP Address/mask	<b>*</b> :	10.10.1	0.1/24	2 c.	
Shared Secret*:			2 d.	Show Shared S	Secret
		Save	Cancel		

- a. In the Name field, enter a name uniquely identifying the NAS client network.
- b. In the **Description** field, enter a brief description for this NAS configuration.
- c. In the **IP Address/mask** field, enter the IP address and mask of the NAS client. You can also provide an IP subnet as the NAS client. In the latter case, RADIUS requests from the subnet are forwarded to the ExtremeGuest RADIUS server.

Note

The NAS client in this case is ExtremeControl. Enter the IP address of your ExtremeControl server.

d. In the Shared Secret field, enter the RADIUS server shared secret.

Note

This shared secret should be the same as the one configured in the ExtremeControl AAA RADIUS server configuration. For more information, refer to Step 6, Configuring RADIUS Server Settings section.

### AAA Authorization Group and Authorization Profile Configuration

3. Go to **Configuration > AAA > Group** and add wired-guest user groups for *unregistered* and *registered* wired-guest users.

These are the groups to which wired-guest users (unregistered and registered) will be added.

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

	Unregistered	default group for user before registration	
	<u>DenyAccess</u>	default group for unauthorized user after registration	
	GuestAccess	default group for user after registration	

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

Group	
Name	
Description*:	
Туре:	Туре 👻
Authorization:	Authorization
	Save Cancel

- b. In the **Name** field, enter a name uniquely identifying the group.
- c. In the Type field, set the value as Users or Devices.
- d. In the **Authorization** field, associate the authorization profile to be applied to guests assigned to this group.
- 4. Go to **Configuration > AAA > Authorization** to add two authorization profiles for *unregistered* and *registered* wired-guest users.

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

<u>UnregisteredPolicy</u>	user not registered	
<u>GuestAccessPolicy</u>	for registered user without group assignment	

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

Name			
Description*:			
VLAN:	VLAN	÷	
Network SSID:	Network SS	ID	*
Rate Limit From Air:		\$	100 to 1000000 kbp
Rate Limit To Air:		-	100 to 1000000 kbp
Inactivity Timeout:		*	60 to 86400 sec
Session Timeout:		-	5 to 144000 minute
Block Time:		÷	0 to 86400 sec
Application Policy:			

- b. In the Name field, enter a name uniquely identifying the profile.
- c. Ensure the **Role(Filter-ID)** field value matches the Policy Role names you created on ExtremeControl.

Note	
If using the default profile or creating a new authorization profile, ensure that the <b>Role(Fi</b> in the profile matches the Policy Role names you created on ExtremeControl. Refer to Ste Policy Roles section.	· · ·

## **Onboarding Policy and Rules Configuration**

5. Go to **Configuration > Onboarding** to add Onboarding Policy and Rules. Onboarding policies and rules enable wired/wireless guest registration when they join a hotspot network.

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

Onboarding Polic	у			
Description:	Default Onboard	ling		
Criteria #1	Description:	Default Onboarding	) Criteria	+ -
Condition(s)			Action	
User Type	✓ Guest	~ +	Deny Access	~
			Update User	

Onboarding policies are used by ExtremeGuest to give flexibility when determining hotspot user access. Policies are matched to the hotspot user based on onboarding rules. Then the matching policy with the highest precedence number is used to onboard the hotspot user.

To create a new policy:

- a. Click the + icon on the top, right-hand corner of the screen.
- b. In the Policy Name field, enter a name uniquely identifying the onboarding policy.
- c. In the **Description** field, enter a brief description.
- d. In the **Criteria #1** field, add the match criteria rule details.

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

- In the **Description** field, enter a description for uniquely identifying the purpose of this criteria.
- In the **Condition(s)** area, select the condition type. 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 corresponding *Action* is triggered. You can add multiple conditions. In case of multiple conditions, all conditions have to be met for the corresponding action to be triggered.

- In the **Action** area, select an action from the 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.						
Action	Validity and Group	Notification Policies				
Send Passcode to Sponsor	0 Day(s) 0 Hour(s) 30 Min(s)	Sponsor*: Email_n_SMS 🗸				
Update User	Select a group 🗸 🗸					
Provide Temporary Access	•					

- In the Validity and Group area, specify the validity for guest access in Days, Hours and Minutes.
- In the **Select a Group** field, set a group for the guest user to join.
- In the Notification Policies area, select a 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 <b>Session Timeout</b> in the AAA Authorization profile. Alternately, use the <b>Schedule Policy</b> option to restrict access to specific day 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.

Create Rule		×
Rule Name*		
Rule Name		
Policy*		
Policy	~	
Network		
All Networks	~	
Location		
System		~
Precedence Level		
Precedence Level	\$	

- f. In the **Rule Name** field, enter a name uniquely identifying the onboarding rule.
- g. In the **Policy** field, associate the onboarding policy created above.
- h. In the **Network** field, specify network this rule applies to.
   Select the appropriate network. This is the network you will add in Step 8 a. below.
- In the Location field, select the location(s) applicable.
   Select the appropriate location. This is the site you will add in Step 10 a. below.
- j. In the **Precedence Level** field, set the precedence of this rule.

## **Notification Policy and Rules Configuration**

6. Go to Configuration > Notification to add Notification Policy and Rules. 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 specifies the mode by which the passcode is communicated.

Note				
The onboarded user/device is assigned to the AAA group created in Step 3 a.				
Policy				
Name				
Description*:				
⊙ User O Sponsor				
SMS				
Email				
SMS over SMTP				

- a. Click the + icon on the top, right-hand corner of the screen.
- b. 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.
- c. 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
  - **Email** Uses an SMTP server. Requires integration with the SMTP Server.
  - SMS over SMTP Uses a third-party SMS service provider. Requires integration with an SMS gateway
- d. 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.

- e. To add a notification rule, go to **Configuration** → **Notification** → **Rules** and click on the + icon on the top, right-hand corner of the screen.
- f. In the **Rule Name** field, enter a name uniquely identifying the notification rule.
- g. In the **Policy** field, associate the notification policy created above.
- h. In the **Network** field, specify network this rule applies to. This is the network added in Step 8 a. below.
- i. In the **Location** field, select the location(s) applicable. This is the site added in Step 10 a. below.
- j. In the **Precedence Level** field, set the precedence of this rule.

## **Network Configuration**

- 7. Go to **Configuration > Networks**.
- 8. To add a network, click the + icon on the top, right-hand corner of the screen.

The Create Network box displays.

Create Netv	vork	×
Name*	ExtremeG	Guest <b>5 a.</b>
Description	Extremed	Control <b>5 b.</b>
SSID	SSID	-
VLAN	1	5 c. 韋
Status	ወ	
	Save	Cancel

- a. In the Name field, enter the network name.
   The name should be same as the captive-portal name configured on ExtremeControl. Refer to the Configuring Captive-portal Settings.
- b. In the **Description** field, enter a brief description of the network.
- c. In the VLAN field, specify the client VLAN. The client will be assigned to the VLAN specified in the AAA > Authorization profile created in Step 3.

## **Site Configuration**

9. Go to **Configuration > Sites**.

Use this option to create a site matching the location of the wired-switch to which the wired-clients are connected.

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

Add Site		×
Name*	SJC	7 a.
Description	SanJoseLocation	7 b.
Country	United States 🔹	7 c.
Region	California 💌	
City	SanJose 💌	
Campus	Extremenetworks-( 💌	
Time Zone	America/Los_Angeles	-
Latitude	Latitude	
Longitude	Longitude	
	Save	Cancel

- a. In the **Name** field, enter the name of the site in which the wired-switch is located. This is the mandatory field.
- b. In the **Description** field, 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.

## **Device Configuration**

### 11. Go to **Configuration > Devices**.

Use this option to add the wired, EXOS-switch to the ExtremeGuest device list. All the fields in this screen are mandatory.

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

Add Device				>
Name*	EXOS-switch	9 a.		
Model*:	X450-G2-24p-10GE4 <b>9 c.</b> ▼	🗹 Wired	d <mark>9 b.</mark>	
Ports*	ge.1	9 d.		
IP Address*	10.10.10.20	9 e.		
Site Name*	CA107-SJC -	9 f.		
Network*	Network	9 g.	]	
		Save	Са	ncel

- a. In the **Name** field, enter a name for the device you are adding.
- b. Select the Wired checkbox to populate the Model field with wired-switch model types.
- c. In the Model field, set the wired-switch model type.
- d. In the **Ports** field, set the ports on which the switch is reachable. You can add a single port or a range of ports. For example: 1.1 1.10.

 Note

 If the same wired-switch is used for another captive-portal based on port-range, then create a new device entry and provide the port range for that network.

 For example:

 Device Entry 1:

 Name: EXOS-switch-1

 Ports: 1.1-1.10

 Network: Network1

 Device Entry 2:

 Name: EXOS-switch-2

 Ports: 1.11-1.20

 Network: Network2

Model, IP Address will remain the same as in the previous entry.

- e. In the IP Address field, enter the IP address of the wired-switch.
- f. In the **Site Name** field, select the site that you added in Step 10 a.
- g. In the Network field, select the network you added in Step 8 a.

## **Splash Template Creation**

#### 13. Go to Configuration > Splash Templates.

Use this option to create captive portal web pages (landing, registration, welcome, etc.) that will be served to the wired-clients 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.

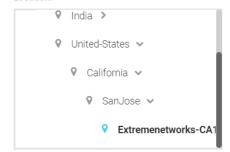
Clone System Template	WiredGuest		
Landing Welcome	Welcome Back +		@ E Ø
Text		* =	Select Theme
	Welcome to our Company!		Layouts -
Image		• × •	
Login Options		¢ × ☆	Templates +

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.

## **Splash Template Hosting and Application**

14. To host and apply the template:

- a. Go to User Templates.
- b. Locate the template from the previous step and click the <sup>©</sup> icon associated with it. The **Apply** box displays.
- c. Select the Host template in ExtremeGuest server: checkbox.
- d. Map the **Location** to the site in which the wired-switch is deployed created in Step 10 a.



e. Click the **Network** drop-down menu and select the network you created in Step 8 a.

Host templat	te in Extre	meGuest server: 🗹
Distribute ter	mplate:	
Location:		Extreme-Alphanet
0	India	GUEST-ACCESS-
9	United-	REGISTRATION
	• Cal	SPONSORED-GUEST-
	0	REGISTRATION
		STCWLB
		STCWLB-ENTERPRISE
Network:	Ì	Extreme-Alphanet

f. Click Apply.

15. Check the template hosting status in the Summary View. To do this,

- a. Click the  $\equiv$  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 <sup>①</sup>icon. The template hosting status is displayed.

ExtremeGues	ST MONITOR - DASHBOARD - CONFIGURA	TION 👻 ANALYZE 👻 OPERATIONS 👻	
item Templates User Tem	Splash Template - Summary View Added ExtremeGuest hosted rule	٥	ж
	Splash Template - Logs		Type to filter
inse inserver and an and a set of the set	Working on hosting     Successfully hosted template		
NewRegWithSocial			
Extrem			
demo		1	Copy To Clipboard Stop

16. To confirm successful hosting, again 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

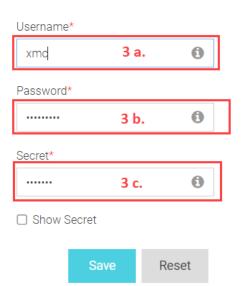
ocation	Name	Template	Status	Action
😕 System				
United-States	Test	E CONTRACTOR DE LA CONT	upload-success	Ð O î

## **ExtremeControl API Settings Configuration**

#### 17. Go to Configuration > ExtremeControl API Settings.

After completing the above configurations, use the **ExtremeControl API Settings** screen to configure the credentials and shared secret required for ExtremeGuest to authenticate with ExtremeControl.

### **Extreme Control API Settings**



- d. In the Username field, enter the username of the ExtremeControl user account.
- e. In the **Password** field, enter the password associated with specific above username.
- f. In the Shared Secret field, enter the pre-configured shared secret.

#### Note

This shared secret should be the same as the one configured in the ExtremeControl AAA RADIUS server configuration. Step 3, Configuring RADIUS Server Settings.