ExtremeControl™ - ExtremeGuest™ v6.0.0

Integration Guide

For Wired-Guest Access

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

P/N 9036413-00 Rev AB

Contents

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-section:

Configuring the EXOS Switch

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: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

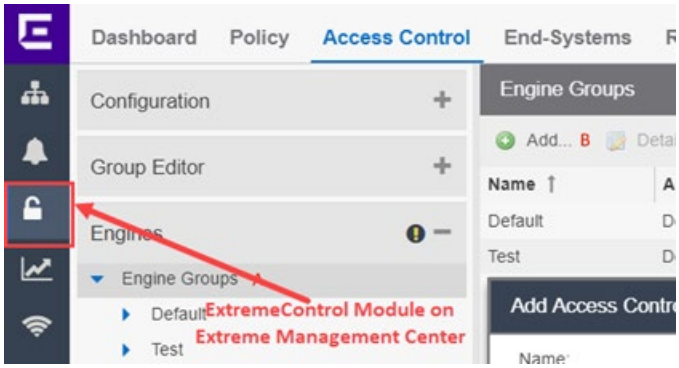
Configuring RADIUS Server Settings

Authentication and Portal Configuration

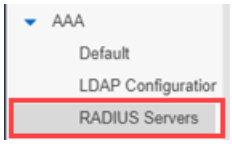
This section lists the steps required to configure ExtremeGuest as the external RADIUS server on the ExtremeControl server.

To configure the RADIUS server:

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

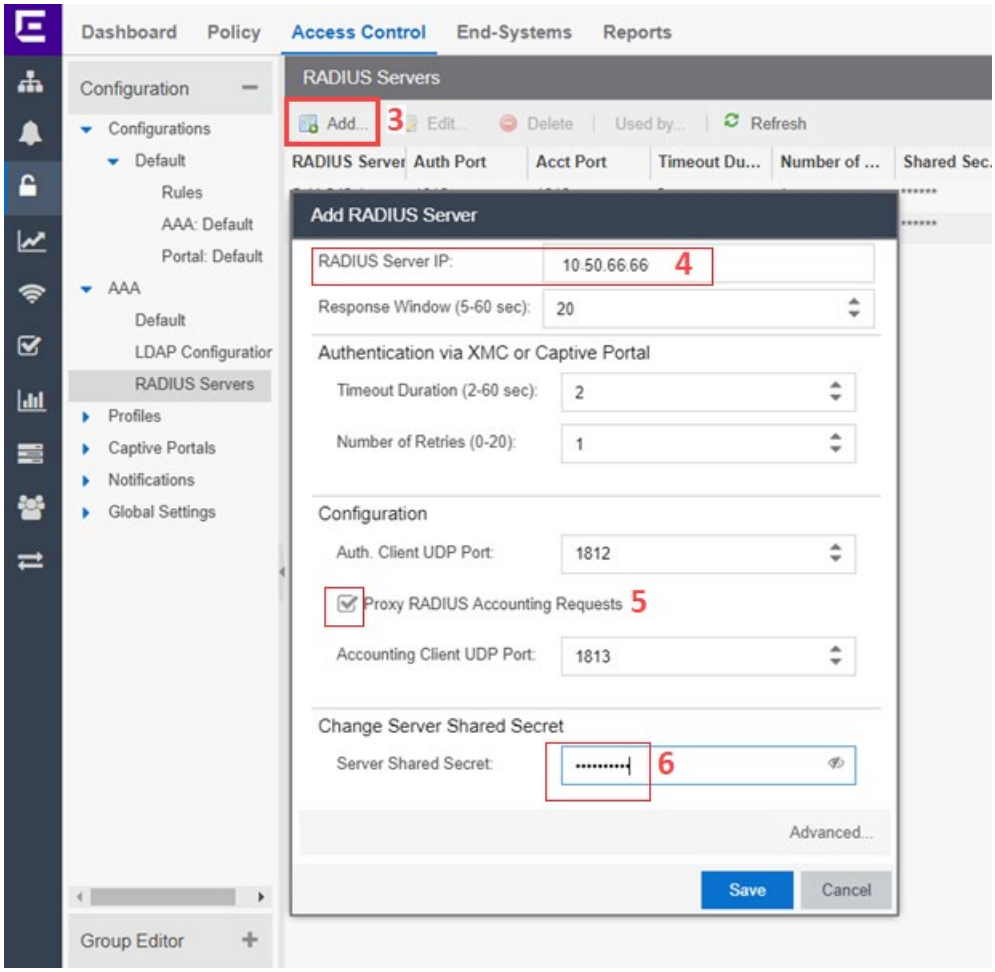


2. Go to **Access Control > Configuration > AAA > RADIUS Servers**.



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.

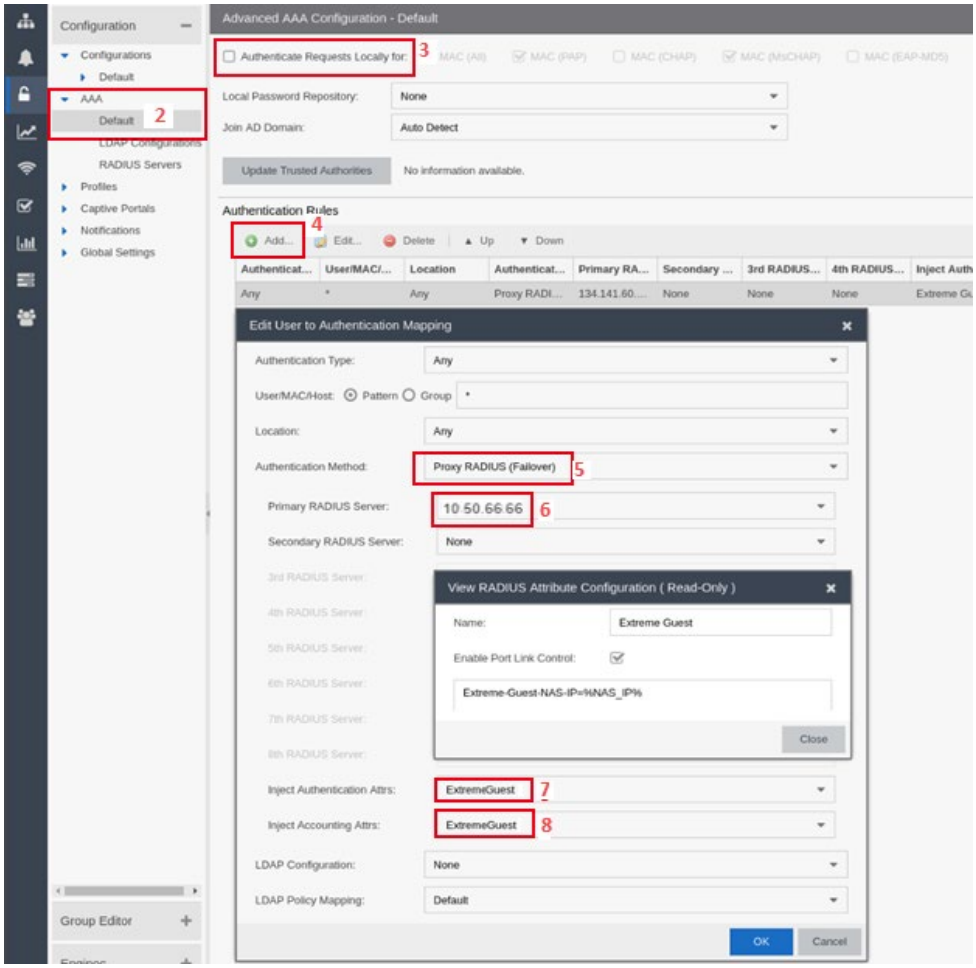
Note
Enter the shared secret of your ExtremeGuest RADIUS server.

Configuring Authentication Settings

Authentication and Portal Configuration

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

1. Go to **Access Control > Configuration > AAA**.



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**.

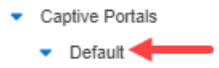
Configuring Captive-portal Settings

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.

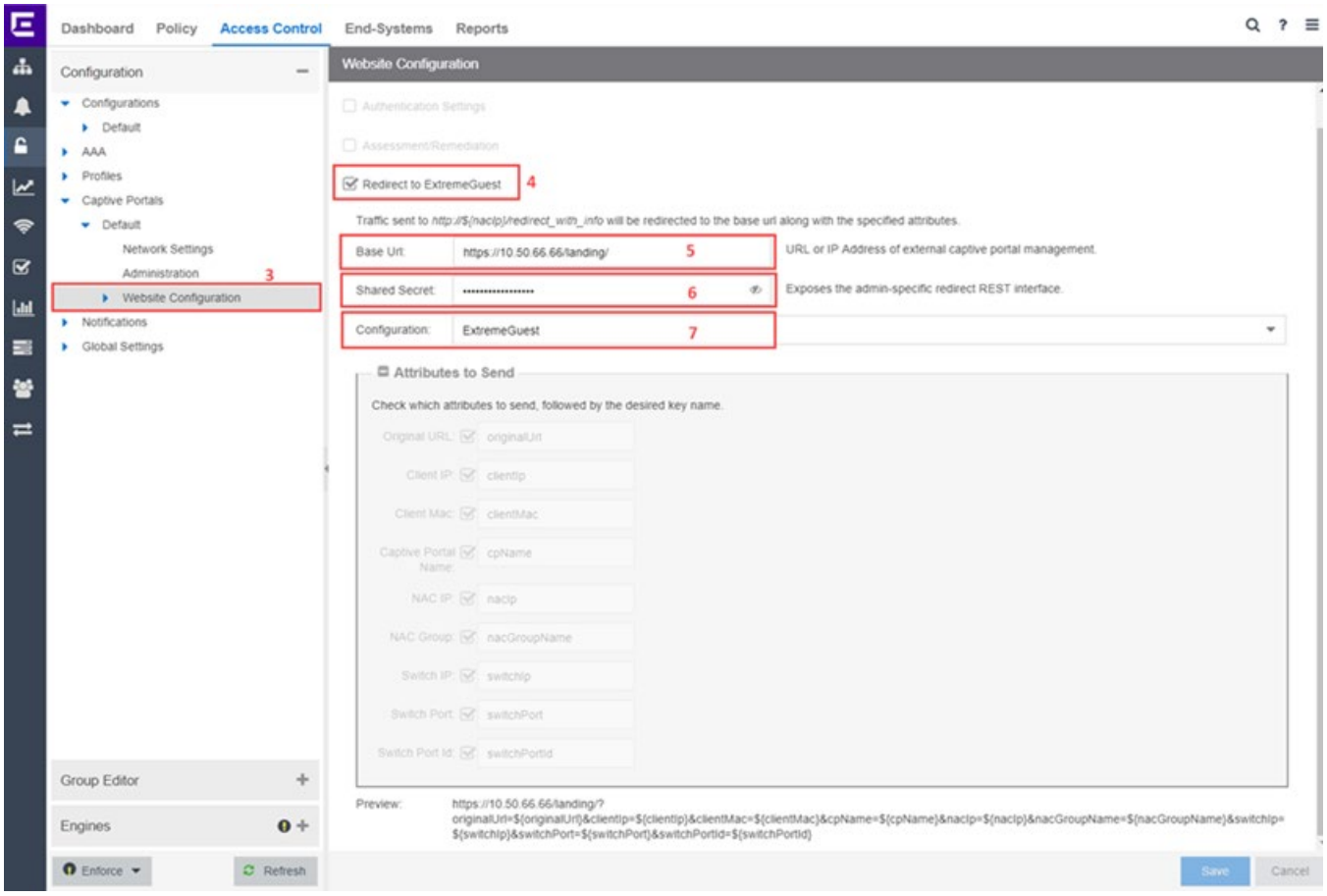
   In this example, we have selected the existing "**Default**" captive-portal configuration.



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.



4. Select the **Redirect to ExtremeGuest** checkbox.
5. 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 “**/**” 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.

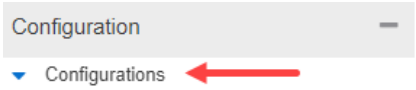
7. In the **Configuration** field, enter **ExtremeGuest**.

Configuring Authorization Settings

Authentication and Portal Configuration

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

1. Go to **Access Control > Configuration > Configurations**.

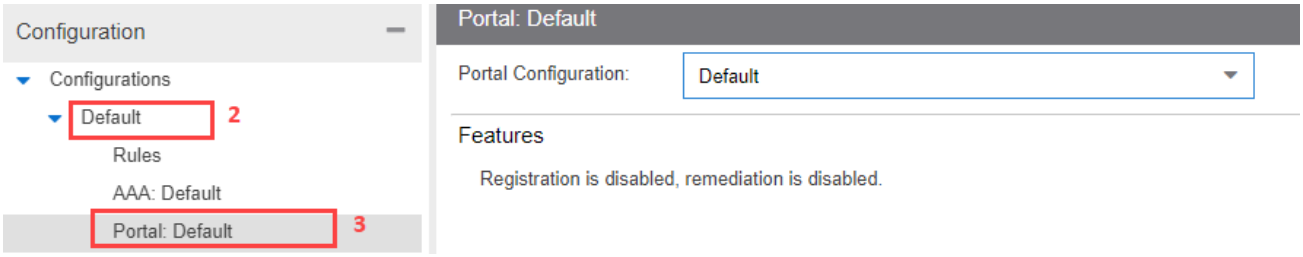


2. Create a new configuration or select an existing configuration.

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

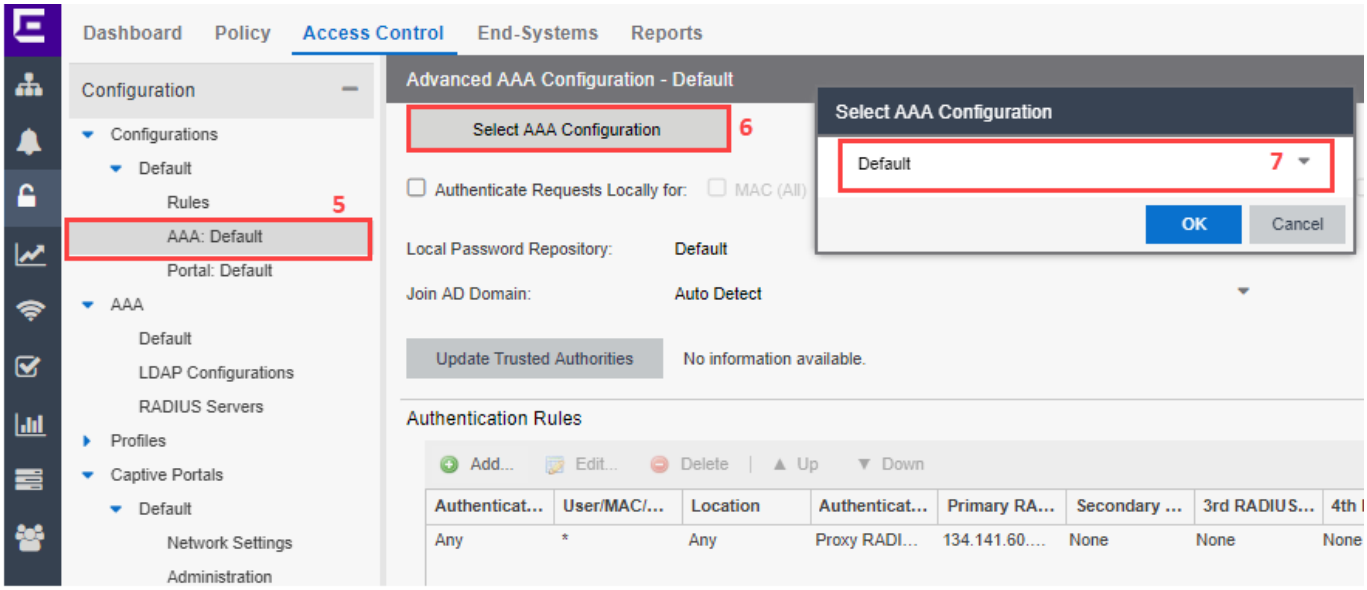
3. Expand the **Default** configuration and select the **Portal: Default** node.

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



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.



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

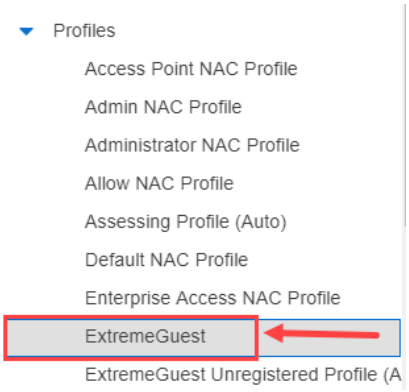
6. Click **Select AAA Configuration** tab.

   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**".

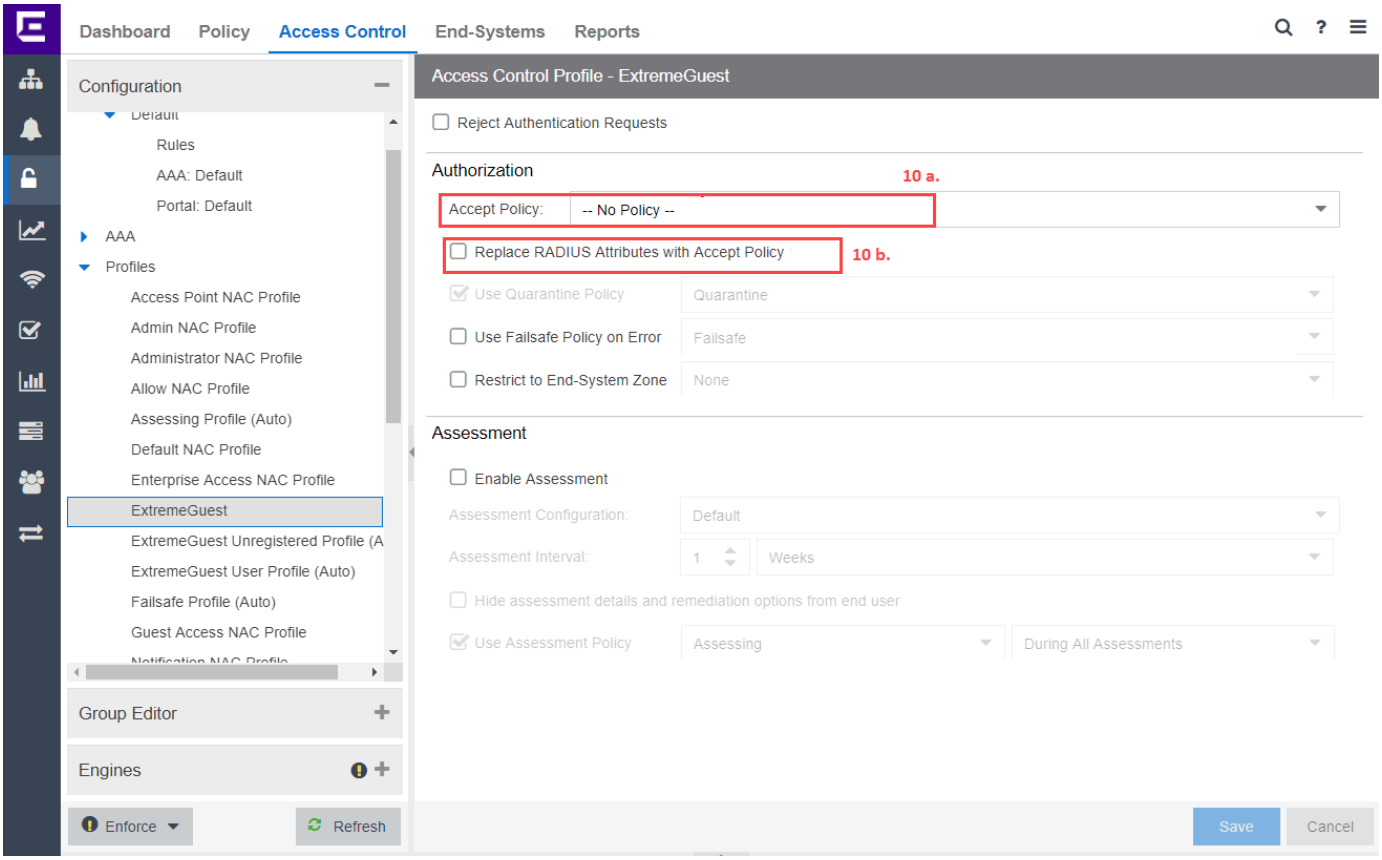
8. Go to **Access Control > Configuration > Profiles**.

9. Add a new profile named "**ExtremeGuest**".



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

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



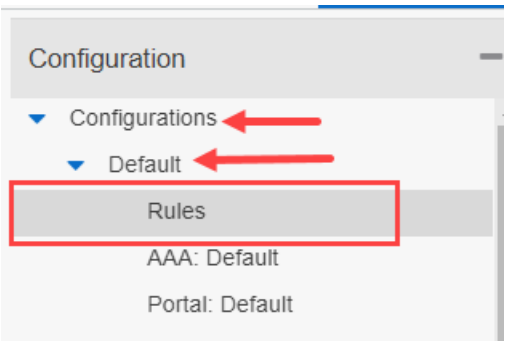
a. In the **Accept Policy:** field select **-- No Policy --.**

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.

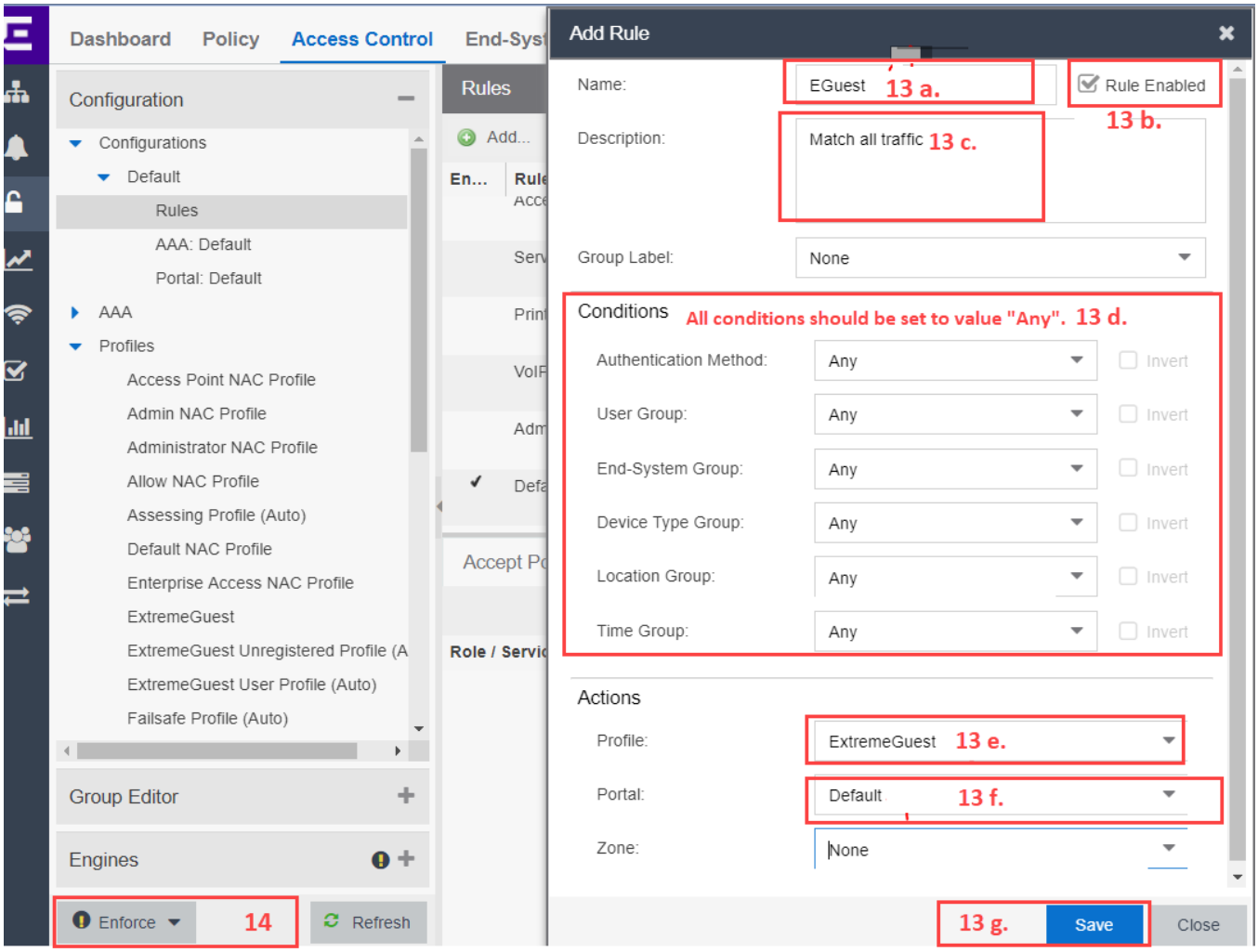
    We will select the "**Default**" configuration, since we had modified the Default configuration as part of this example.

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



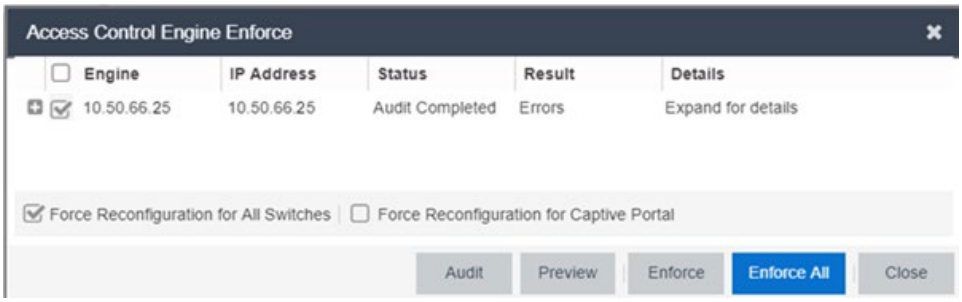
    The **Rules** screen displays in the right-hand pane.

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



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 Captive-portal 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.



Switch and Policy Configuration

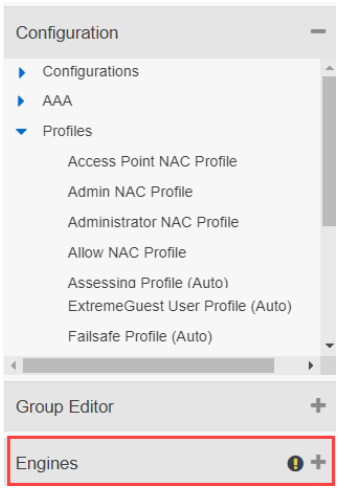
ExtremeControl Configuration

This section describes the following set of configurations:

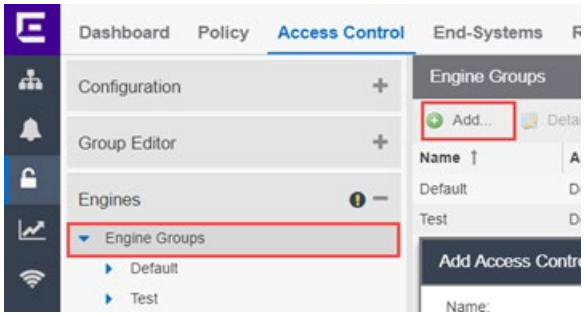
- Configuring the Switch on ExtremeControl

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.



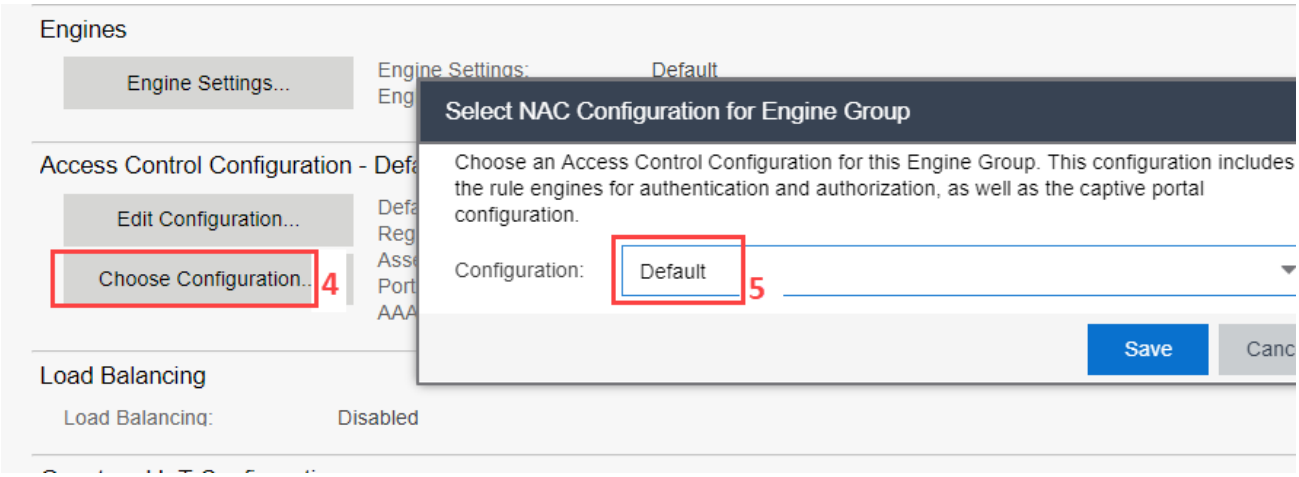
   The **Add Access Control Engine Group** box displays. Enter the details and click **Add**.

   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.



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.

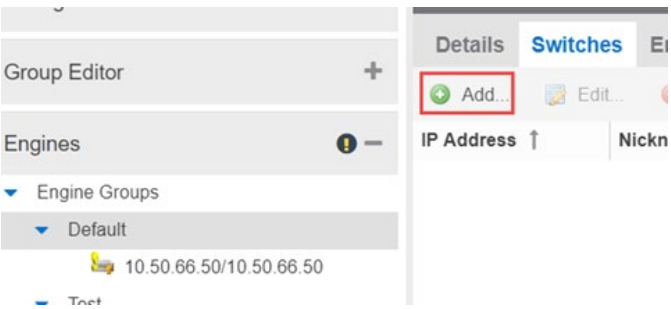
7. Add your **NAC engine (device)** to the engine group, then click on the **NAC engine (device)** you added.

   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".

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…**

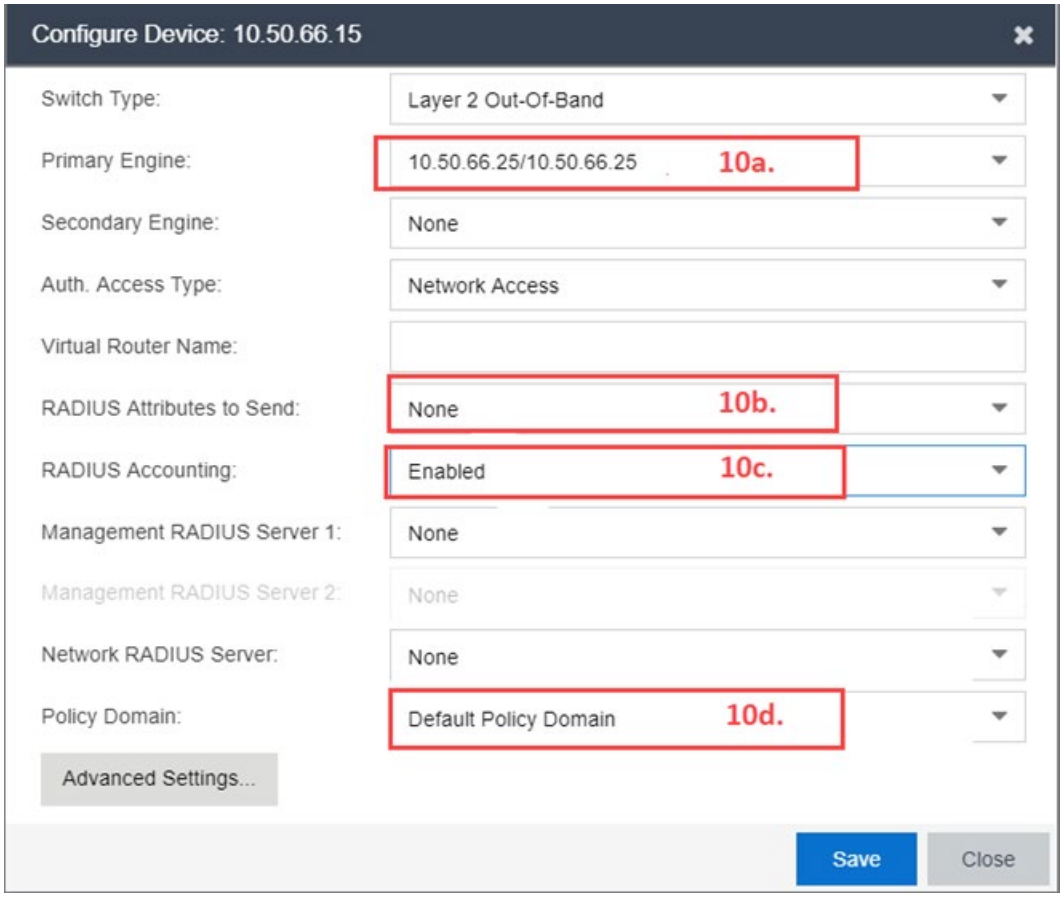


The **Add Switches to Access Control Engine Group: <NAME>** screen displays.

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:



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

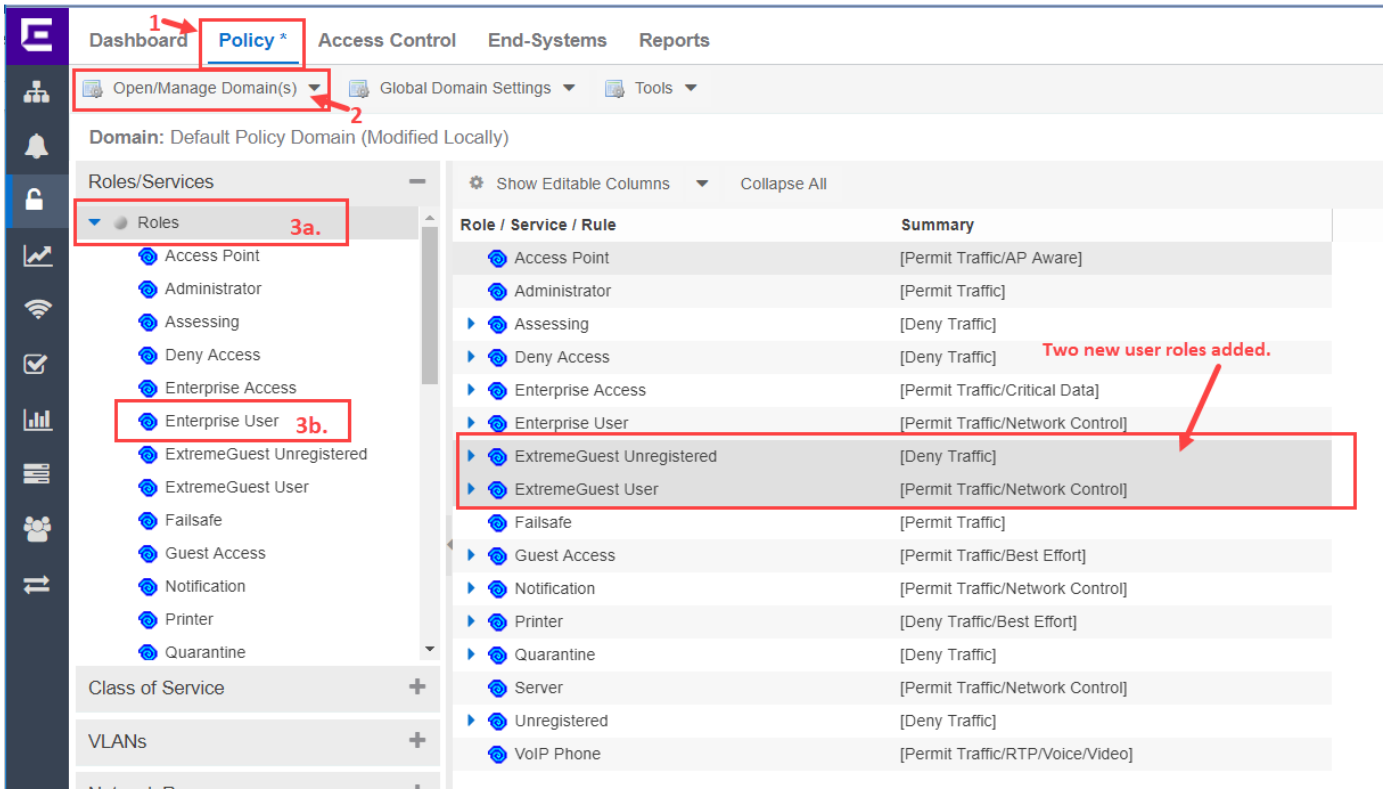
Creating Policy Roles

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:



   a. 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

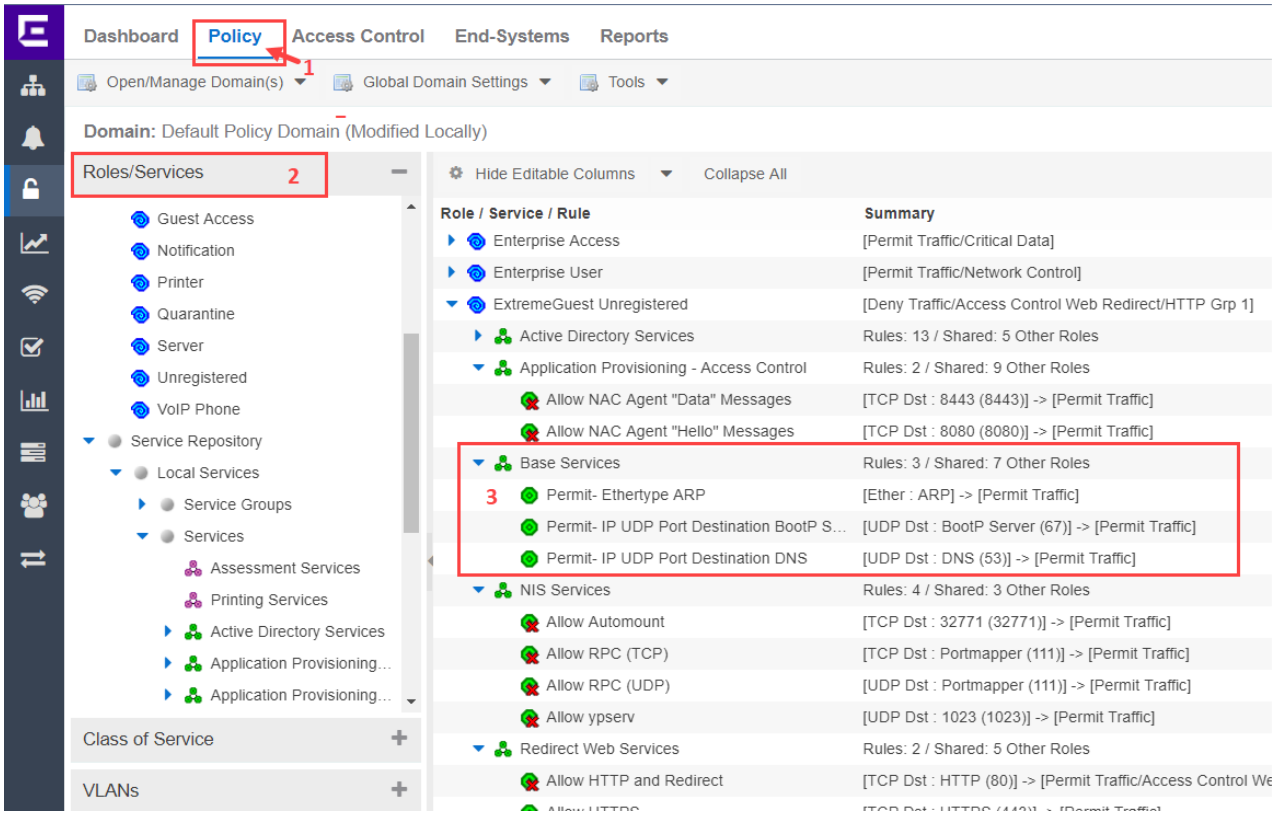
This section describes how to redirect ExtremeGuest Unregistered users, created in Step 3e. of the preceding section, to the NAC captive portal redirector. In order to do this,

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

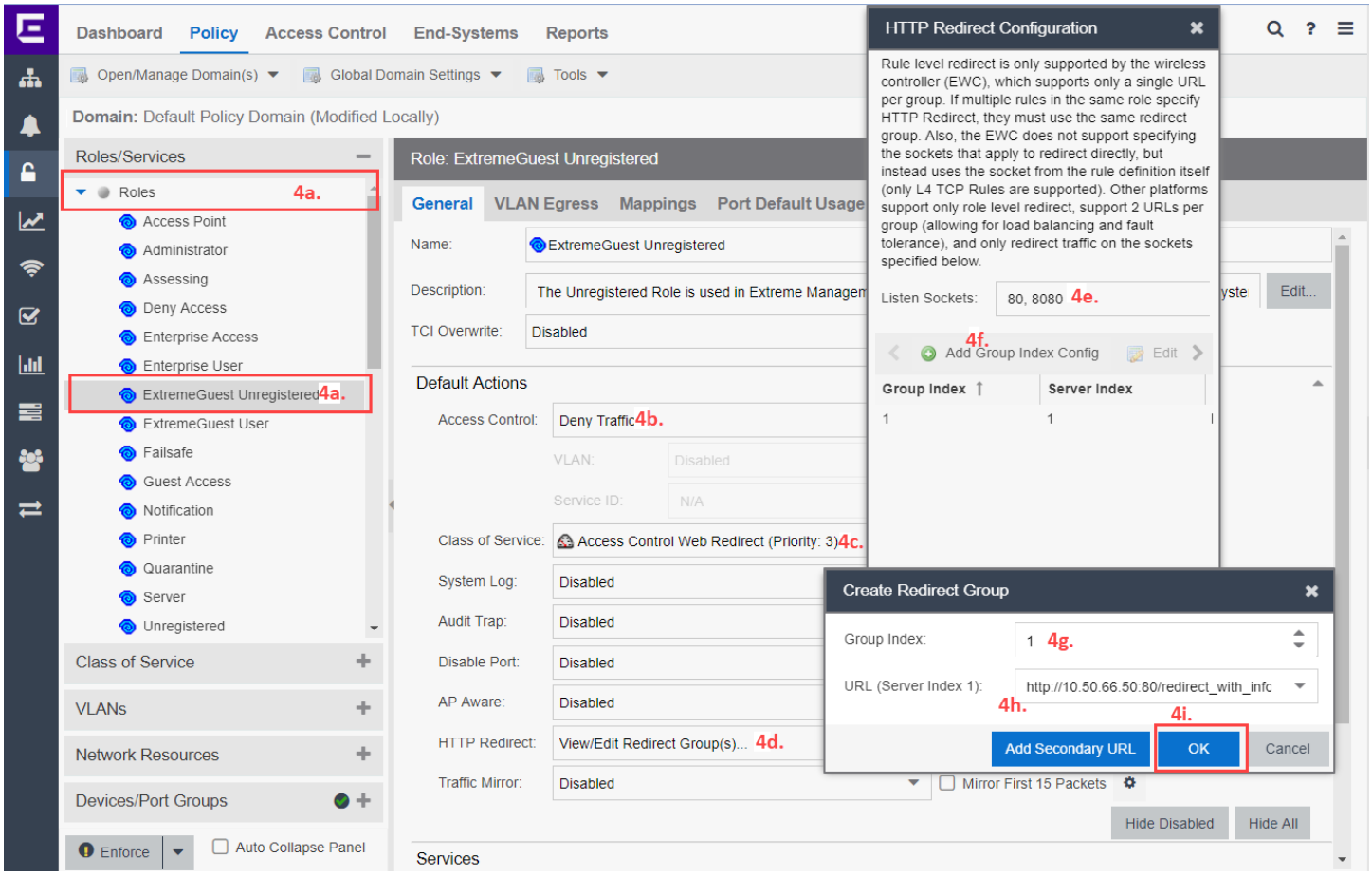
   The **Role / Service / Rule** screen displays in the right-hand pane.

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:

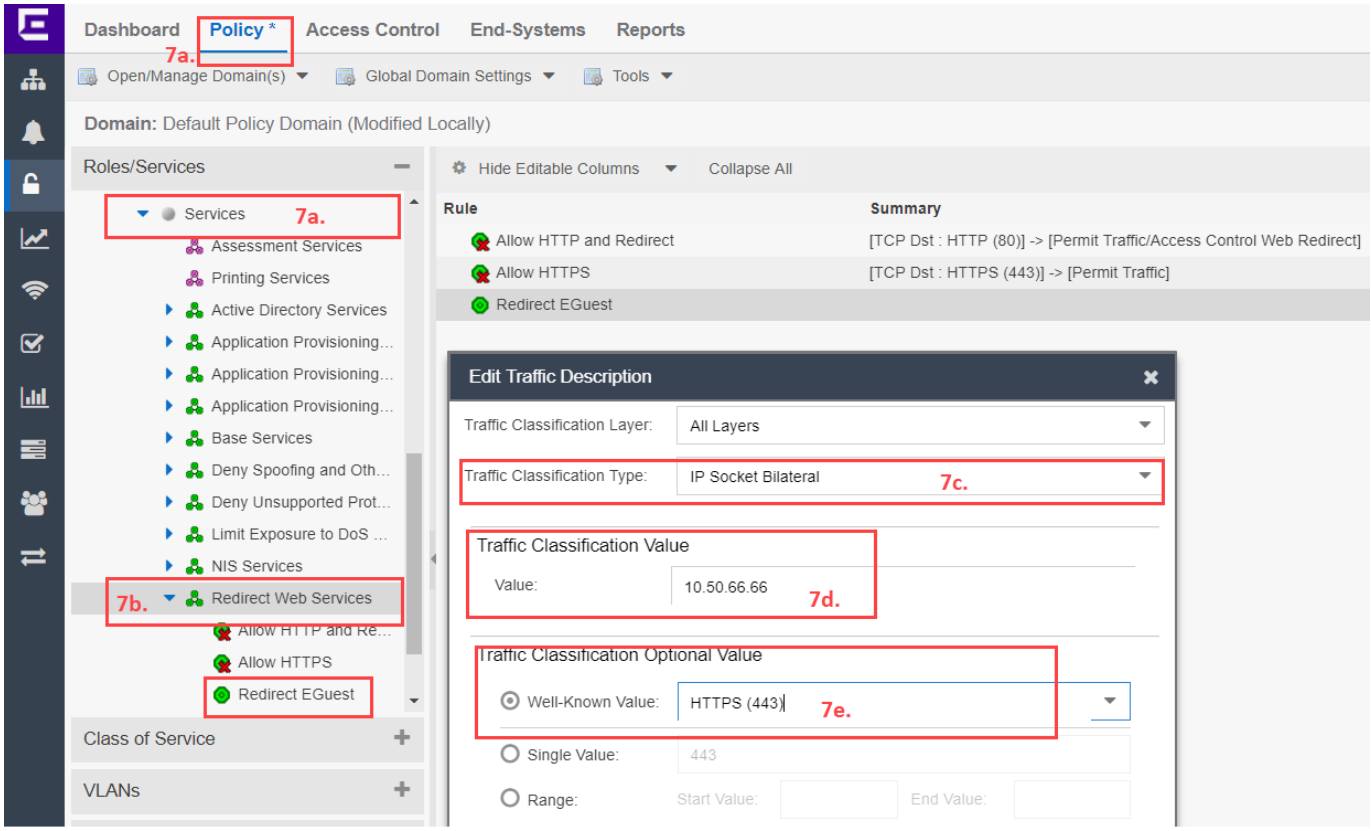


a. Expand the **Role** node and select the **ExtremeGuest Unregistered** role.
   The **Role: ExtremeGuest Unregistered** screen displays in the right-hand pane.
b. Set the **Access Control:** option to **Deny Traffic**.
c. Set the **Class of Service:** option to **Access Control Web Redirect (Priority: 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.
i. 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:



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**.

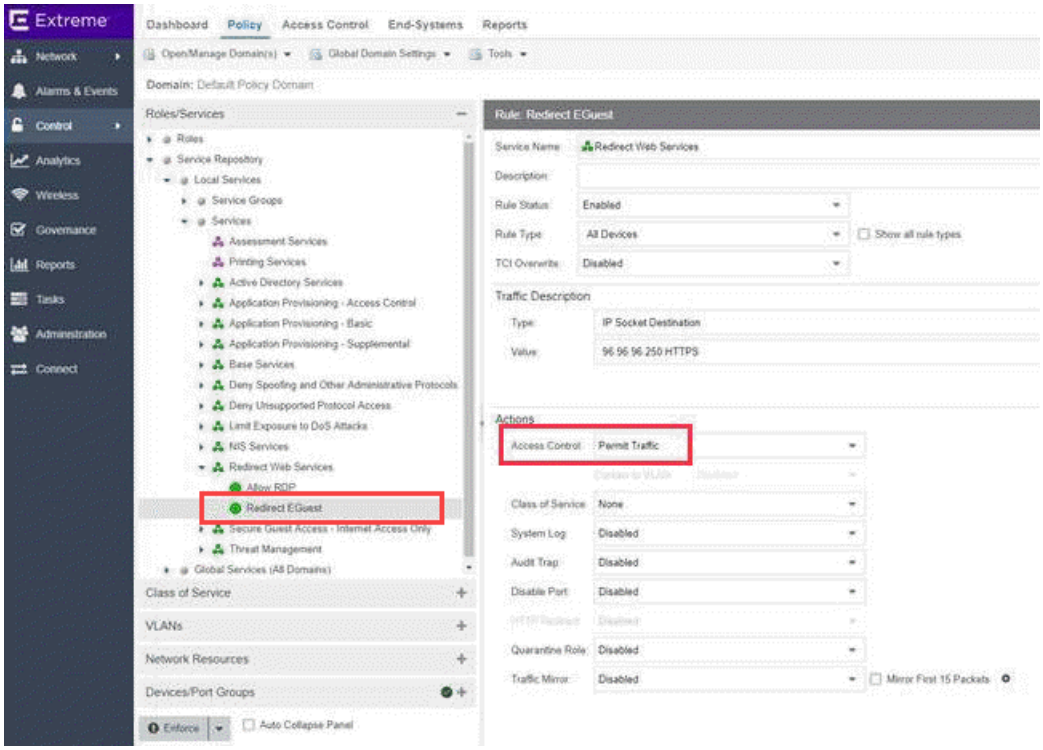
c. Set the **Traffic Classification Type:** option to **IP Socket Bilateral**.

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.



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 wired-guest users of ExtremeControl NAC deployments.

   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.

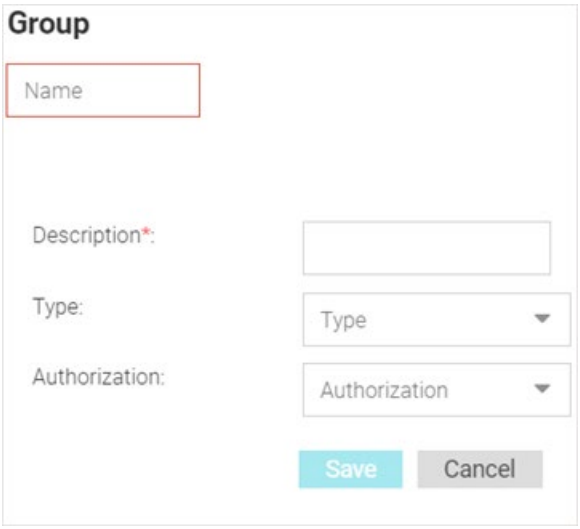
AAA Authorization Group and Authorization Profile Configuration

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:

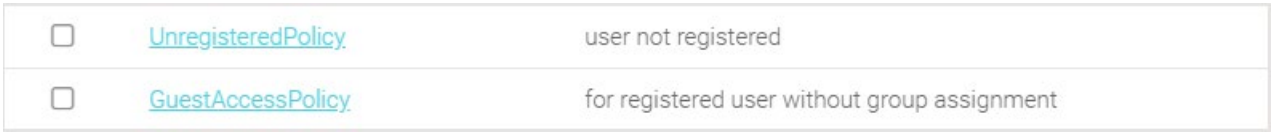
   a. If adding a new group, click the **+** icon on the top, right-hand corner of the screen.



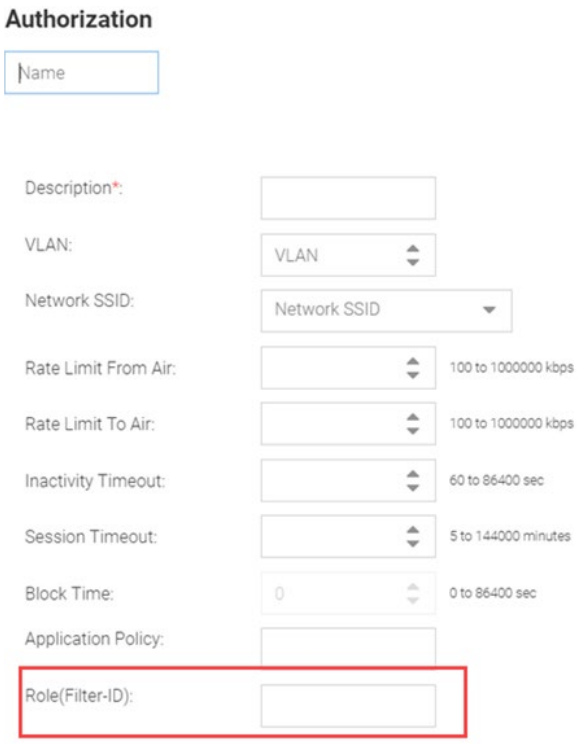
   b. In the **Name** field, enter a name uniquely identifying the group.
   c. In the **Type** field, set the value as **Users** or **Devices**.
   d. In the **Authorization** field, associate the authorization profile to be applied to guests assigned to this group.

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:



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



b. In the **Name** field, enter a name uniquely identifying the profile.

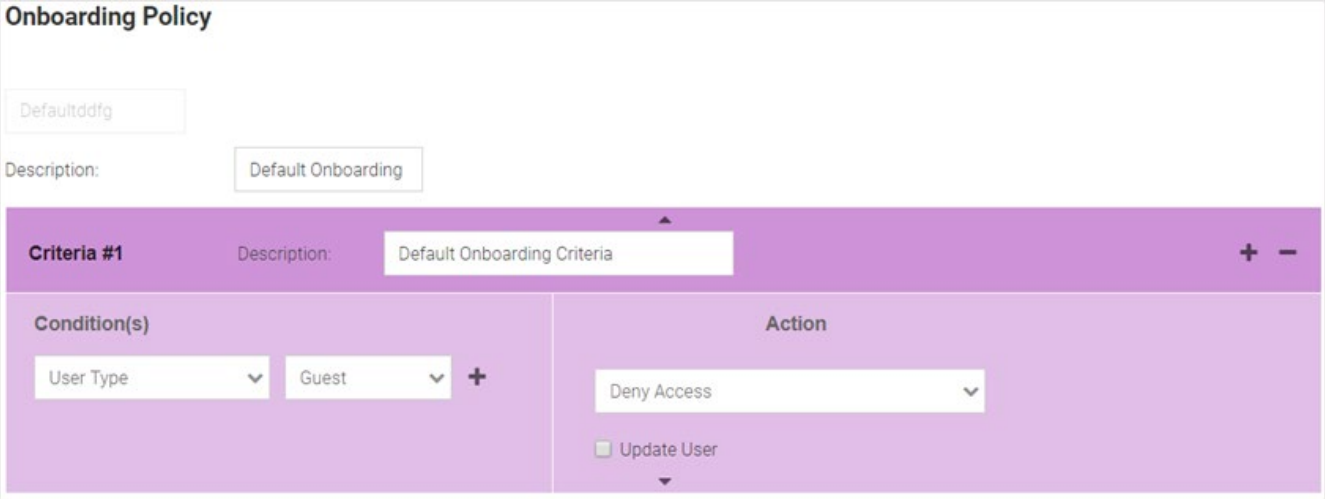
c. Ensure the **Role(Filter-ID)** field value matches the Policy Role names you created on ExtremeControl.

Note
If using the default profile or creating a new authorization profile, ensure that the **Role(Filter-ID)** value in the profile matches the Policy Role names you created on ExtremeControl. Refer to Step 3, Creating 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 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.

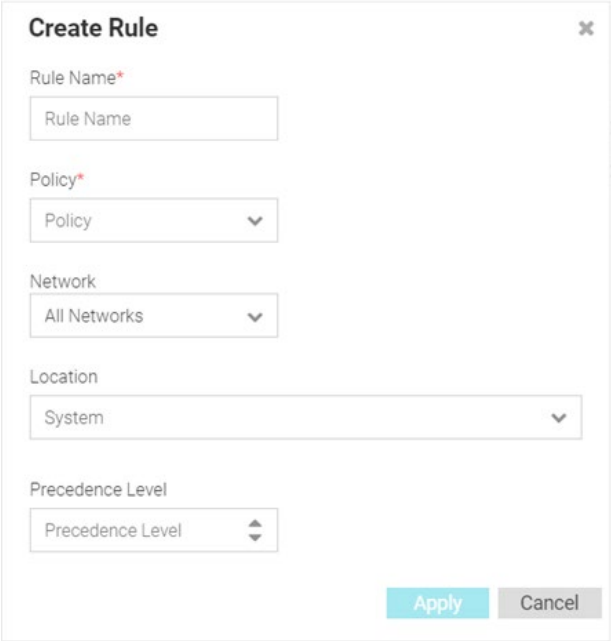
     These conditions determine when the corresponding *Action* is triggered. You can add multiple conditions. In case of multiple conditions, all conditions have to be met for the corresponding action to be triggered.
   - In the **Action** area, select an action from the menu. The selected *Action* is triggered 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.

- 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 **Session Timeout** in the AAA Authorization profile. Alternately, use the **Schedule Policy** 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.



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.

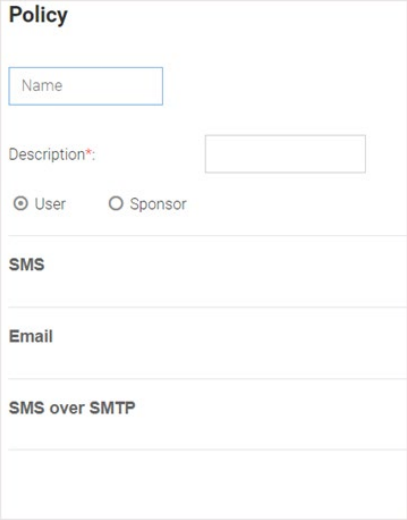
i. In the **Location** field, select the location(s) applicable.
Select the appropriate location. This is the site you will add in Step 10 a. below.

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.



   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.

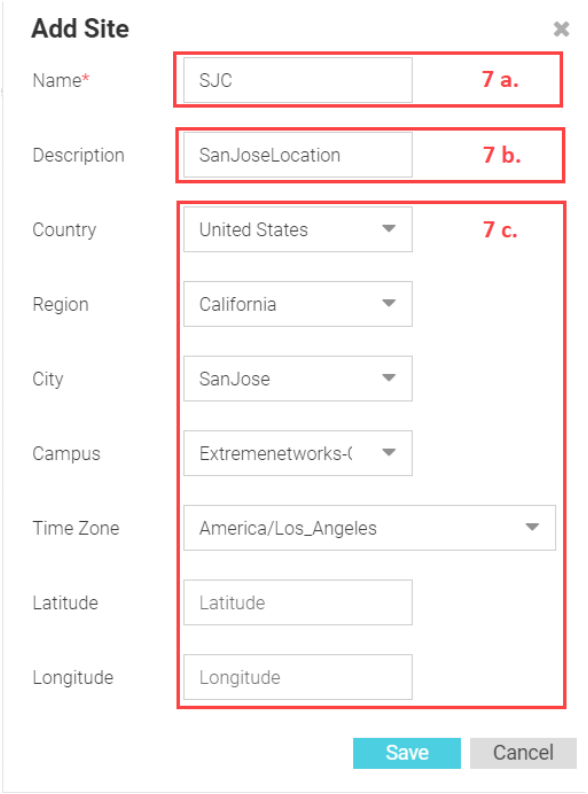
   a. In the **Name** field, enter the network name.
      The name should be same as the captive-portal name configured on ExtremeControl. Refer to the Configuring Captive-portal Settings.
   b. In the **Description** field, enter a brief description of the network.
   c. In the **VLAN** field, specify 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.



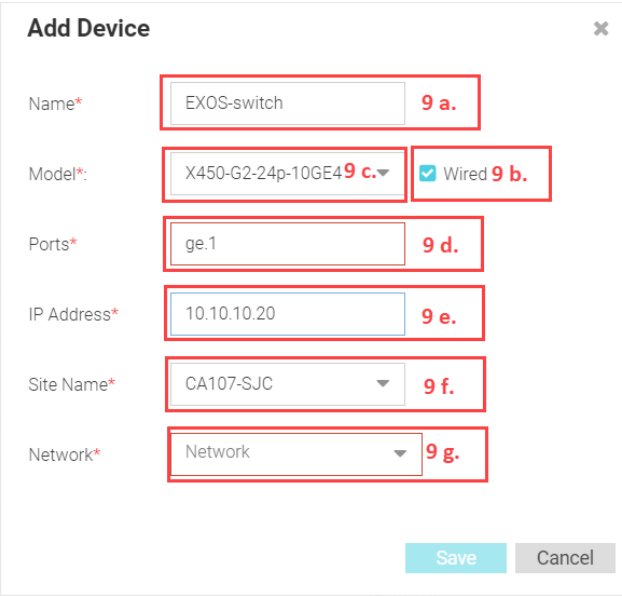
a. In the **Name** field, enter the name of the site in which the wired-switch is located. This is the mandatory field.
b. In the **Description** field, enter a brief description of the site.
c. Use the other fields (Country, Region, City, etc.) to define the exact geographical location of the site.

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.



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 b**ased 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

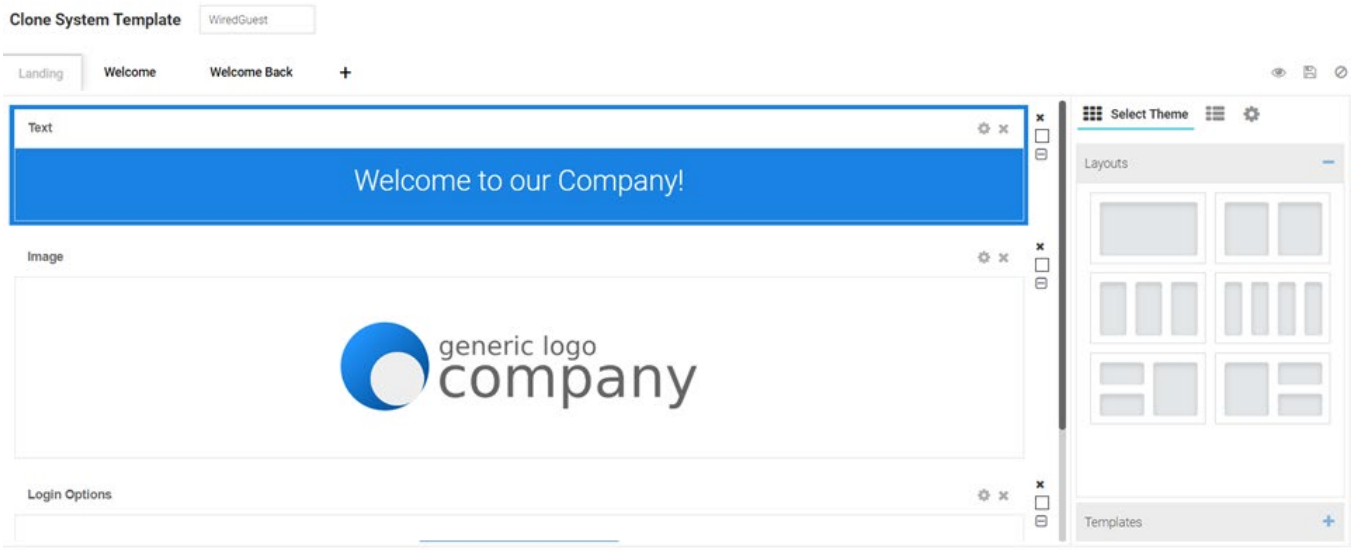
13. Go to **Configuration > Splash Templates**.

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.

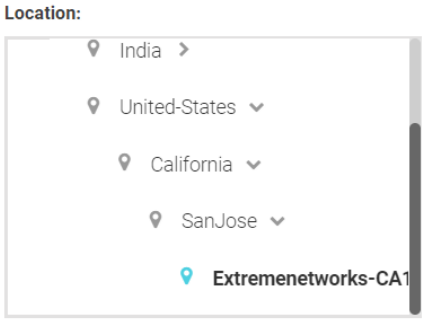
In this example, we have cloned a system-template.



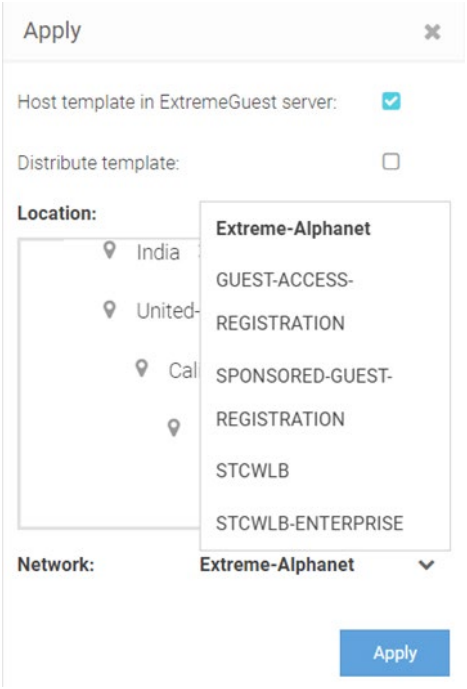
The cloned and customized template is automatically available in the **User Templates** tab. Once the splash template is in place specify where the template is to be hosted and to which network is it to be applied.

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 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.

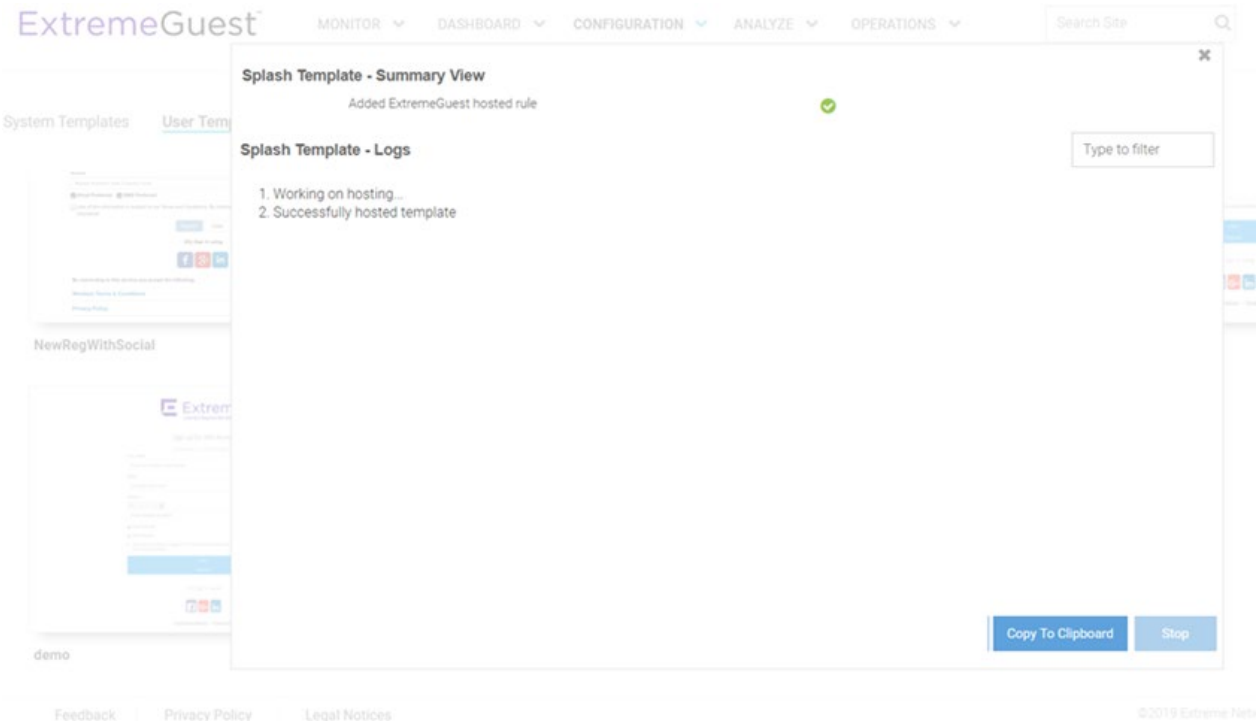


    e. Click the **Network** drop-down menu and select the network you created in Step 8 a.

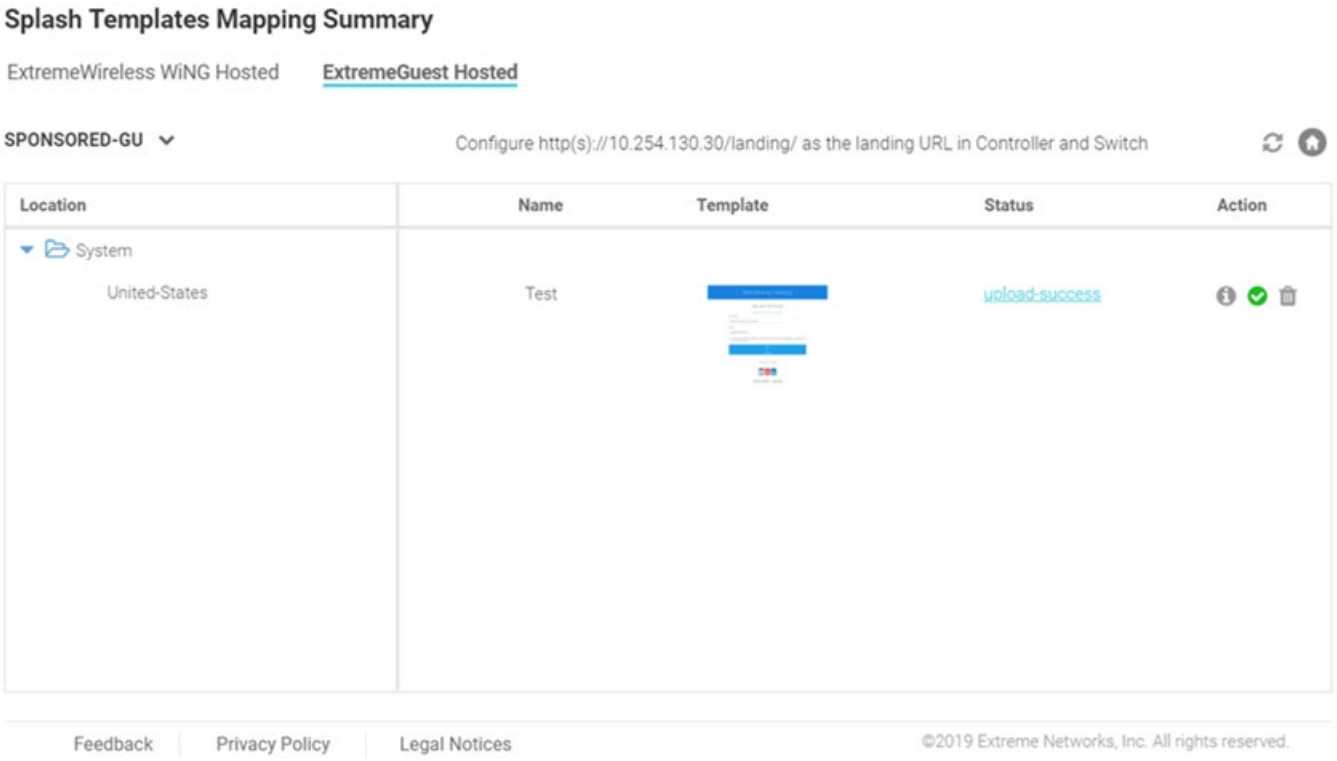


f. Click **Apply**.

15. 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 ⓘ icon. The template hosting status is displayed.



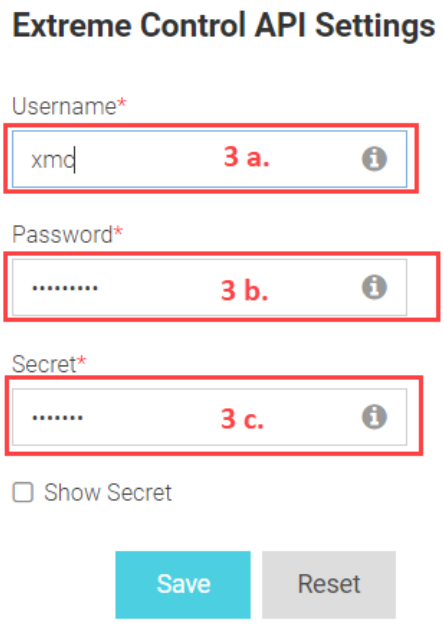
16. To confirm successful hosting, again go to the summary view (follow preceding steps) and select the network. The template status should display as follows:



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.



    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.