ExtremeGuest User Guide

For Version 6.0.0

Table of Contents

Preface

This section discusses the conventions used in this guide, ways to provide feedback, additional help, and other Extreme Networks® publications.

Text Conventions

The following tables list text conventions that are used throughout this guide.

Table 1: Notice Icons

Icon	Notice Type	Alerts you to...
	General Notice	Helpful tips and notices for using the product.
	Note	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.
New!	New Content	Displayed next to new content. This is searchable text within the PDF.

Table 2: Text Conventions

Convention	Description
`Screen displays`	This typeface indicates command syntax, or represents information as it appears on the screen.
The words **enter** and **type**	When you see the word "enter" in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says "type."
[Key] names	Key names are written with brackets, such as **[Return]** or **[Esc]**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **[Ctrl]**+**[Alt]**+**[Del]**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.

Providing Feedback to Us

Quality is our first concern at Extreme Networks, and we have made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

• Content errors or confusing or conflicting information.

- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team, you can do so in two ways:

- Use our short online feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Please provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal	Search the GTAC (Global Technical Assistance Center) knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
The Hub	A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
Call GTAC	For immediate support: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribing to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1 Go to www.extremenetworks.com/support/service-notification-form.
2 Complete the form with your information (all fields are required).

3   Select the products for which you would like to receive notifications.

> **Note**
> You can modify your product selections or unsubscribe at any time.

4   Click **Submit**.

Documentation and Training

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for earlier versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes
Hardware/Software Compatibility Matrices	https://www.extremenetworks.com/support/compatibility-matrices/
White papers, data sheets, case studies, and other product resources	https://www.extremenetworks.com/resources/

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For more information, visit www.extremenetworks.com/education/.

1 Introduction

Introduction to ExtremeGuest

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. For example, knowing how many customers enter a store, how often they visit, and how much time they spend are all metrics that can be measured through ExtremeGuest. ExtremeGuest can take advantage of social networking behavior to increase patronage, expand brand exposure, and understand client demographics and preferences in a more comprehensive and personal way. Guest onboarding with sponsor approval is supported allowing a sponsor to approve or deny guest access with a single click.

ExtremeGuest is available as a virtual machine and provides centralized guest management, including multiple guest onboarding methods, and guest analytics. ExtremeGuest is supported both as a standalone application and in replica set mode. A typical ExtremeGuest replica set deployment consists of the ExtremeGuest platform running on three standalone virtual machine instances. Of these, two instances are full-nodes and the third instance is the arbiter.

> **Note**
> For information on various ExtremeWireless WiNG deployment scenarios, refer to the ExtremeGuest Server Deployment guide, available at https://extremenetworks.com/documentation.

For information on scale and hardware requirements for ExtremeGuest view the ExtremeGuest Datasheet.

For information on various ExtremeWireless WiNG deployment scenarios, refer to the ExtremeGuest Server Deployment guide.

ExtremeGuest was designed to be deployed into *ExtremeWireless WiNG* installations to collect guest analytics information from WiNG captive portal and enforce access control. Starting with this release, this support has been extended to *ExtremeCloud Appliance* managed networks and *ExtremeControl* managed wired networks.

Downloading and Installing ExtremeGuest

1. Go to the Extreme Networks Portal download page at: Extreme Networks Portal Download Page.
2. If you are not a registered user, register here: https://extremeportal.force.com/ExtrAccountRegistration.
3. Select the *ExtremeWireless* product family.
4. Select the **WiNG (Formerly Zebra WLAN) → ExtremeGuest** option.

5 Select the **SOFTWARE / RELEASE NOTES** tab.

This page displays the resources that you are entitled to. If you do not see the items that you need or think that you are entitled to, please contact GTAC http:// www.extremenetworks.com/support/ contact/.

6 Download the **ExtremeGuest** application. The application downloads as an *.iso* image.

7 Install the .iso image. Follow the hypervisors instructions for installing a virtual machine.

> **Note**
> Ensure a virtual machine hypervisor is installed in your server environment or the downloaded *.iso* image will not run.

8 Boot the ExtremeGuest application.

On the first boot, the system will prompt you to change the password.

9 Install the license obtained from the licensing portal on the **Operations → Licenses** screen.

For more detailed licensing instructions see: License on page 120.

UI Overview

ExtremeGuest uses an adaptive user interface that changes the navigation interface based on the layout of the browser window it is viewed on.

On a wide browser window, the ExtremeGuest navigation menus are displayed at the top of the user interface. These options are:

- Monitor on page 18
- Dashboard on page 26
- Configuration on page 34
- Analyze on page 105
- Operations on page 117

To search for a specific **Site** enter the site name, or a portion of the site name, in the **Search Site** box. Selecting a site from the results opens the left navigation menu to that site.
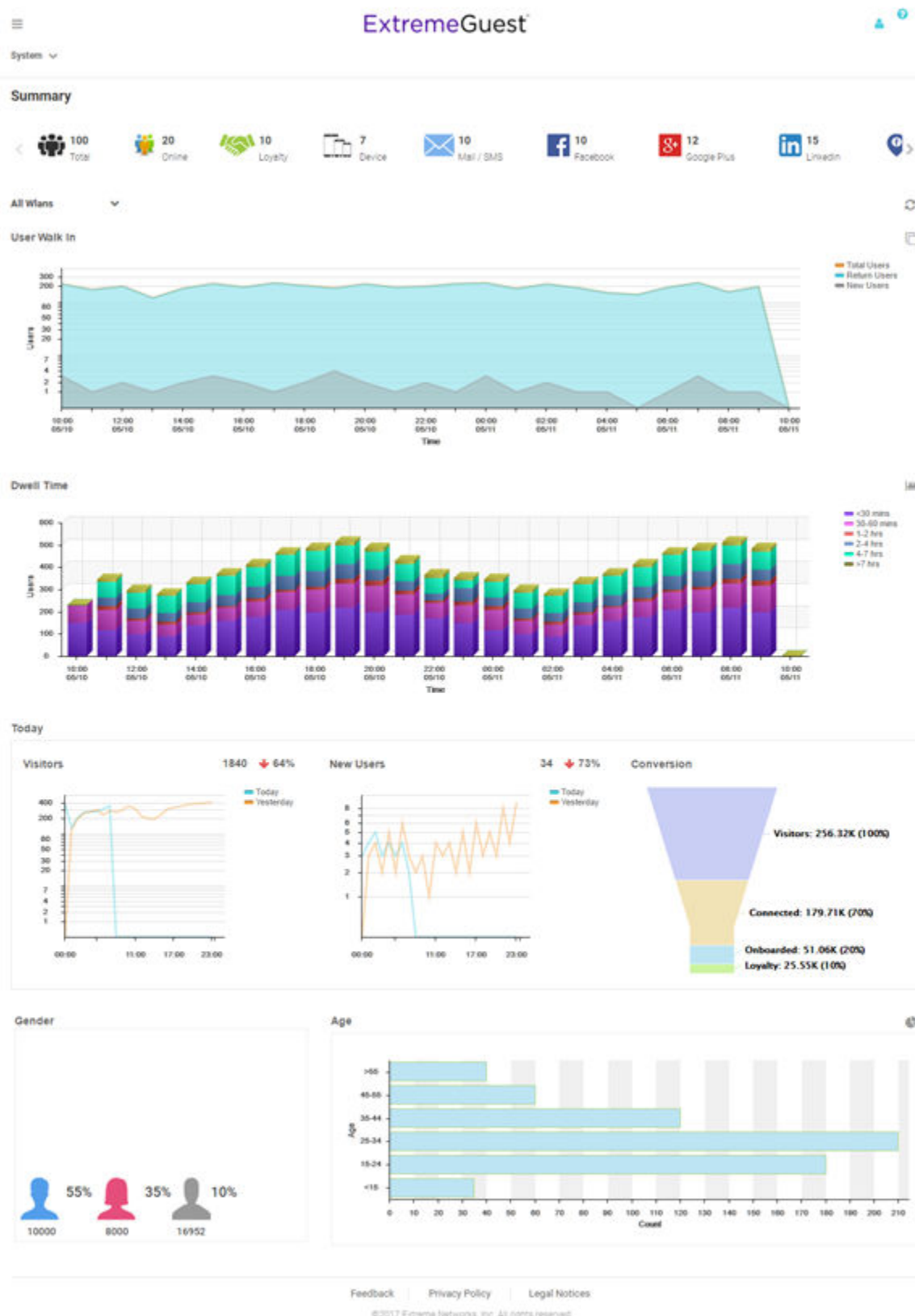
Figure 1: User Interface in Standard View

When the browser window is wide enough a system navigation tree displays on the left of the user interface. Filter the information displayed by selecting regions or individual sites from the navigation tree. The information in the main window updates when a new region or site is selected.

Figure 2: User Interface in Tablet View

On a narrow browser, such as a phone or tablet, the menu displays as three horizontal lines. Selecting the lines produces a pull down navigation menu with the following items:

- Monitor on page 18
- Dashboard on page 26
- Configuration on page 34
- Analyze on page 105
- Operations on page 117

The ExtremeGuest user interface supports the following user roles:

Admin	The admin user has full control of the ExtremeGuest system and access to all configuration items. This guide is written for admin users.
Web User	The web user can manually add users individually or through bulk vouchers.
Onboard User	The onboard user is used to manually add headless devices to the network. The onboard user can also view a basic summary of the system.

Web User Interface

The web user interface is used to manually add individual users or bulk users through vouchers. The web user interface can be accessed only by a web user. A web user account must be created by the administrator. Use the web user credentials (username/password) to access the web user interface.

Figure 3: Web User Interface - New User Screen

Configure the following user details to add a new user to the network:

First Name	Enter the first name of the user you wish to add to the network.
Last Name	Enter the surname of the user you wish to add to the network.
Email	Enter the e-mail address for the user you wish to add to the network. This field is required. Select **Use as username/password** to use the e-mail address as the username and password for the user. Selecting this will remove the **Username** and **Password** fields from this screen.
Telephone	Enter the telephone number for the user you wish to add to the network. Select **Use as username/password** to use the telephone number as the username and password for the user. Selecting this will remove the **Username** and **Password** fields from this screen.
Organization	Optionally, enter an organization name for the user.
Reason	Optionally, enter a reason that the user is being created.
Username	If **Use as username/password** is not selected in the **Email** or **Telephone** fields, specify a unique username for the new user.
Password	If **Use as username/password** is not selected in the **Email** or **Telephone** fields, specify a unique password for the new user.
User Group	Optionally, select a user group to associate the new user with. New user groups are added by the admin user.
Location	Use the pull-down menu to select a site for the user to be added to. New locations are created by the admin user. This is a required field.
Start Date / Time	Specify the starting date and time for the new user to be activated. This is a required field.
Expiry Date / Time	Specify an ending date and time for the user to be deactivated. This is a required field.

Select **Create**, once all required fields are populated, to add the user to the network. To erase any information entered in the fields, select **Clear**.

The **Bulk Voucher** screen is used to create between 2 and 20,000 users at a time.

Configure the following fields to add a **Bulk Voucher**.

Figure 4: Web User Interface - Bulk Voucher Screen

User Group	User the pull-down menu to select a user group for all new users in the bulk voucher. New user groups are created by the admin user. This is a required field.

Number of Vouchers Use the spinner controls to specify the number of vouchers to create. The number of vouchers may be between 2 and 20,000. This is a required field.

Description Optionally, enter a description for the users being added to the voucher.

Location User the pull-down menu to select a location for the new users to be added to. New locations are added by the admin user. This is a required field.

Start Date / Time Specify the starting date and time for the new users to be activated. This is a required field.

Expiry Date / Time Specify an ending date and time for the users to be deactivated. This is a required field.

Select **Create**, once all required fields are populated, to add the user vouchers to the network. To erase any information entered in the fields, select **Clear**.

Onboard User Interface

The web user interface is used to manually add headless devices that do not have a browser available for authentication. To access the onboard user interface an onboarding user must be created by the administrator. Once created, login with the onboard user's username and password to access the onboard user interface.

Figure 5: Onboard User Interface - Device Registration

Configure the following device details to add a headless device to the network:

MAC Address Enter the MAC address for the device being added.

Group Use the pull-down menu to select a group to add the new device to. New groups are added by the admin user.

Network Use the pull-down menu to select a network to associate the new device with. New WLANs are added by the admin user.

Location Use the pull-down menu to select a site to associate the new device with.

Vendor Use the pull-down menu to select the **Vendor** who manufactured the device being added.

Device Use the pull-down menu to specify the type of device being added to the network.

Device OS   Use the pull-down menu to specify the operating system running on the device being added.

Device Browser Use the pull-down menu to specify the browser type in use on the new device.

Expiry Time   Specify a date when the device will be automatically removed from the network.
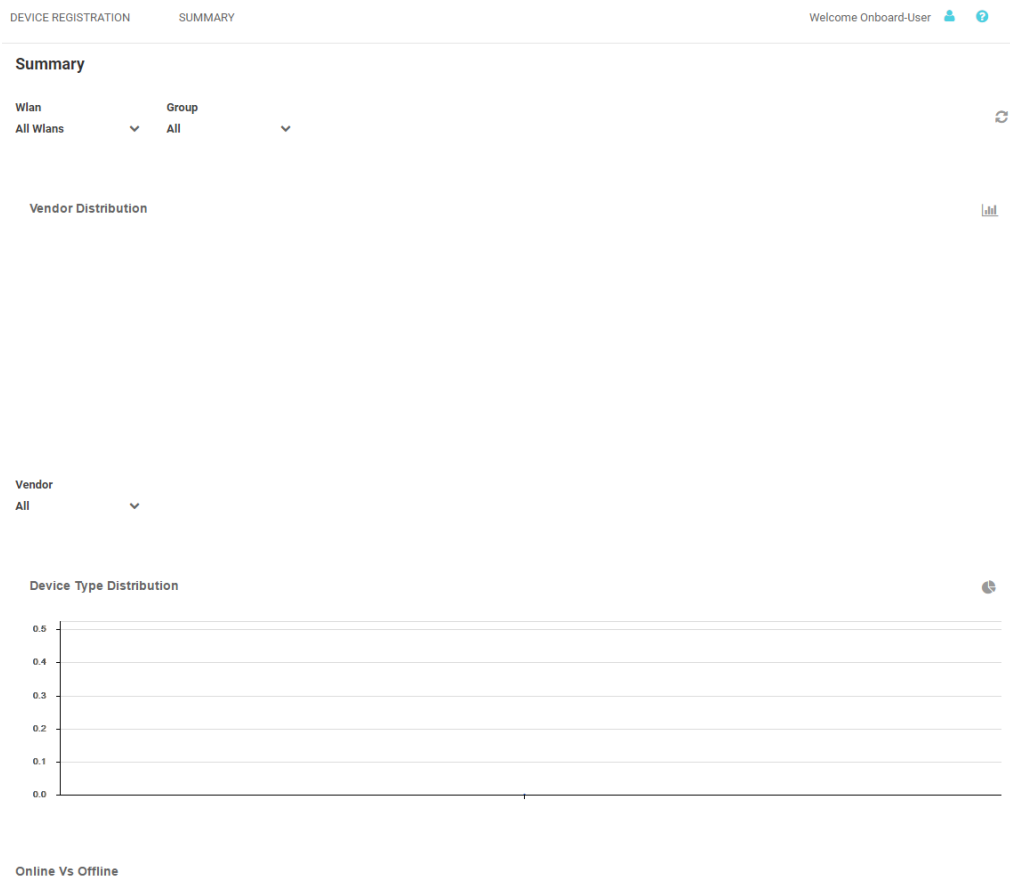

Figure 6: Onboard User Interface - Summary Screen

The **Summary** tab displays **Vendor Distribution**, **Device Type Distribution**, and **Online Vs Offline** status for devices. These results can be filtered by **WLAN** or **Group**.

2 New in this Guide

> **ExtremeControl API Settings**
> **ExtremeCloud Appliance Integration**
> **ExtremeGuest Evaluation License**
> **Dashboard Report Generation**
> **Splash Template Builder**
> **ExtremeGuest REST API Commands**

ExtremeControl API Settings

Starting with this release, you can configure ExtremeGuest as the external registration and authentication server for wired-clients of *ExtremeControl* NAC deployments in conjunction with Extreme EXOS switches. On the ExtremeGuest UI, configure the **ExtremeControl API Settings** to enable this functionality.

For more information, see ExtremeControl on page 47.

ExtremeCloud Appliance Integration

Starting with this release, you can deploy ExtremeGuest as the external captive portal server authenticating clients connected to *ExtremeCloud Appliance* managed access points (centralized and distributed). To enable this functionality, the AAA NAS configuration should point to the IP address/IP subnet and shared secret of the ExtremeCloud Appliance host.

For more information, see Adding AAA NAS on page 45.

ExtremeGuest Evaluation License

Starting with this release, an ExtremeGuest Evaluation License is available for fresh installations of the application software.

For more information on licenses, see License on page 120.

Dashboard Report Generation

ExtremeGuest UI provides a new *Dashboard* report generation feature. This report is generated in the PDF format. It displays the widgets used in a dashboard, along with the current data displayed within each widget .

For more information, see Manage Reports on page 109.

Splash Template Builder

ExtremeGuest UI now provides a robust, easy-to-use splash template builder that allows you to create customized captive portal web pages.

For more information on splash template builder, see User Templates on page 75.

ExtremeGuest REST API Commands

Starting with this release, the ExtremeGuest REST API guide is being released as a separate guide.

To download this guide, please visit http://developer.extremenetworks.com.

3 Monitor

The **Monitor** screens provide key-metrics about users, map-based views and active user summaries.

Select **Monitor** from the main menu, to access the following sub-menus:

Map View
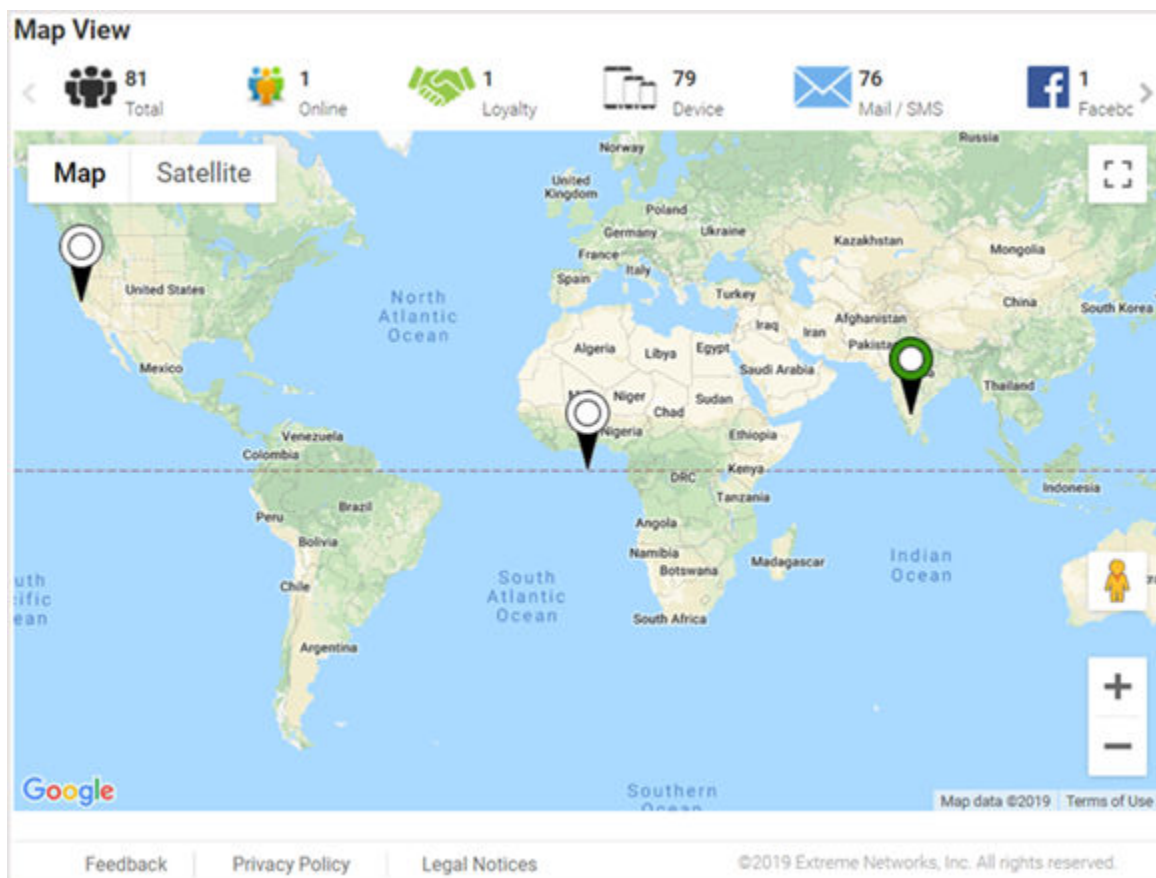
Monitor → Map View

Figure 7: Map View Screen

A bar at the top of the screen provides information about the total number of users and the total number of users online.

If social media authentication is enabled the bar will also display the number of users authenticated using Facebook, Facebook Checkin, Google Plus, LinkedIn or Instagram.

A map view is generated using Google Maps based on site locations. Hover the mouse over a site to view key user metrics for that location.
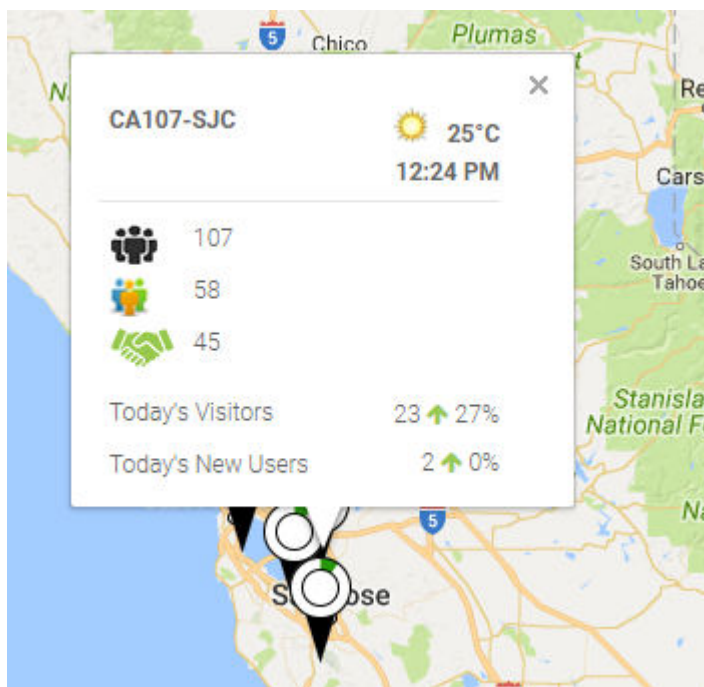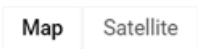

Figure 8: Map View Mouse Over

Map-View Controls

Use the following controls available on the screen to get a granular view of places and information:

Table 3: Map-View Controls

| Map-View Control	Location	Description
	Bottom-right corner of the map	Drag and drop this icon on to a specific area on the map to open a street view of the area.
+ −	Bottom-right corner of the map	Use these buttons to zoom in and out on the map.
	Top-right corner of the map	Use this icon to open the map in the full-screen mode. Press the [Esc] button to exit the full-screen mode.
Map Satellite	Top-left corner of the map	Use these buttons to toggle between map view and satellite view.

Summary

Monitor → Summary
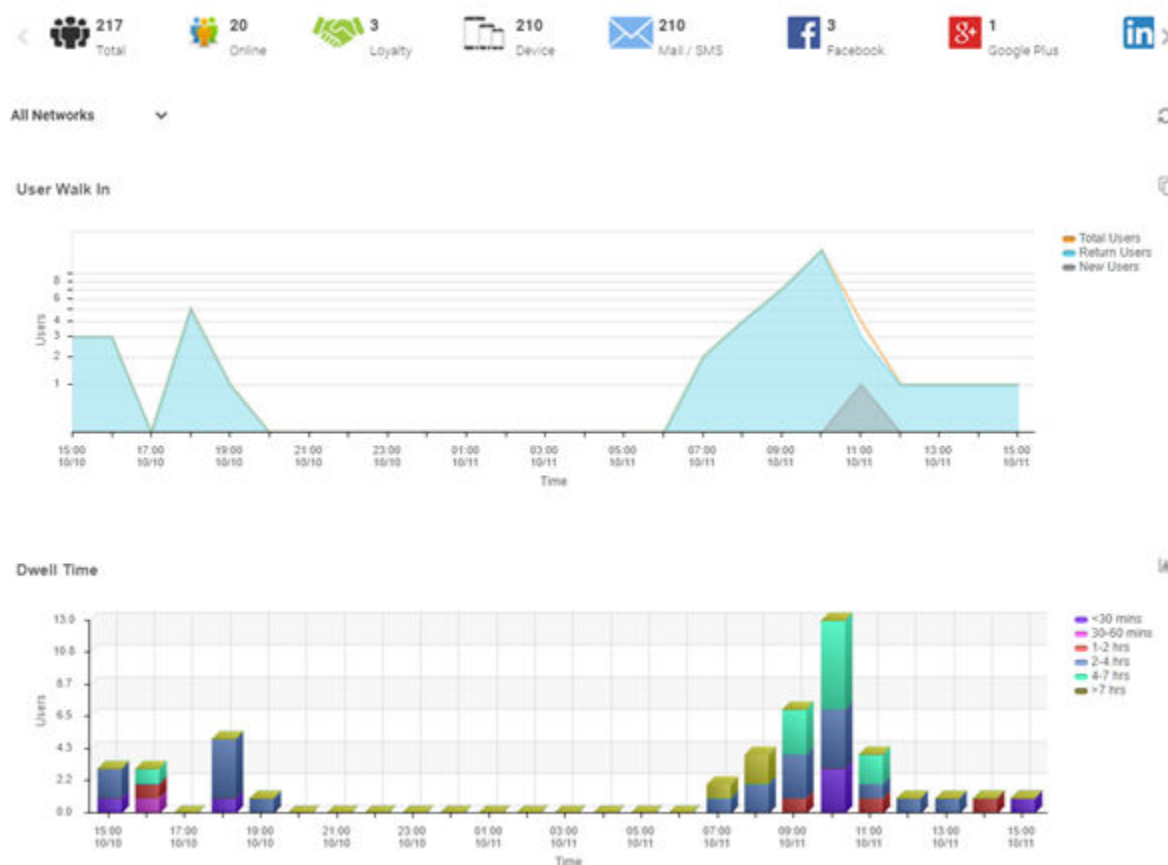
Figure 9: Summary Screen

The **Summary** screen provides a high-level overview of user activity over the past 24 hours. This information is updated automatically.

A bar at the top of the screen provides information about the total number of users and the total number of users online.

If social media authentication is enabled the bar will also display the number of users authenticated using Facebook, Facebook Checkin,Google Plus, LinkedIn or Instagram. For more information, see

Summary Details

Monitor → Summary

The **Summary** screen displays following user activity details:

| User Walk In | The **User Walk In** graph displays the number of users entering a location over a 24 hour time period with data points at each hour. Data is further separated between **Total Users**, **Return Users**, and **New Users**. |

| Dwell Time | The **Dwell time** graph displays the amount of time users stayed at a location over a 24 hour time period with data points at each hour. Data is further separated into the following time windows: |

- < 30 Minutes
- 30-60 Minutes
- 1-2 Hours
- 2-4 Hours
- 4-7 Hours
- > 7 Hours

Note

Use the Show Grouped /Show Stacked icons on the top-right hand corner of this section to display user data grouped into categories or stacked into separate categories for each of the above time windows.

| Today | The **Today** chart displays data from the last two days and a comparison of **Visitors** and **New Users** data in percentages. The **Visitors** graph displays the total number of users over time. The **New Users** graph displays the number of first time users over time. The **Conversion** graph displays the number and percentage of users who converted from **Connected** to **Onboarded** to **Loyalty** customers. The information displayed in all three graphs starts at midnight of the previous day and goes through the current time. This information resets each day at midnight. |

| Gender | The **Gender** chart displays the percentage of users by gender. |

| Age | The **Age** bar/pie graph displays the total number of users separated into the following age ranges: |

- > 55
- 45-55
- 35-44
- 25-34
- 15-24
- < 15

Note

Use the Show Bar Chart /Show Pie Chart icons on the top-right hand corner of this section to display user data as a bar chart or pie chart respectively.

Users

Monitor → Users

The **Users** screen lists all of the clients in the networks, their status, MAC address, IP address, and other information. The content of this screen changes based on the node selected in the left-hand, navigation tree. The **System** node displays users and their details for the entire network. If a site is selected in the navigation tree, the screen updates with user details, blocked and currently connected, pertaining to the selected site.
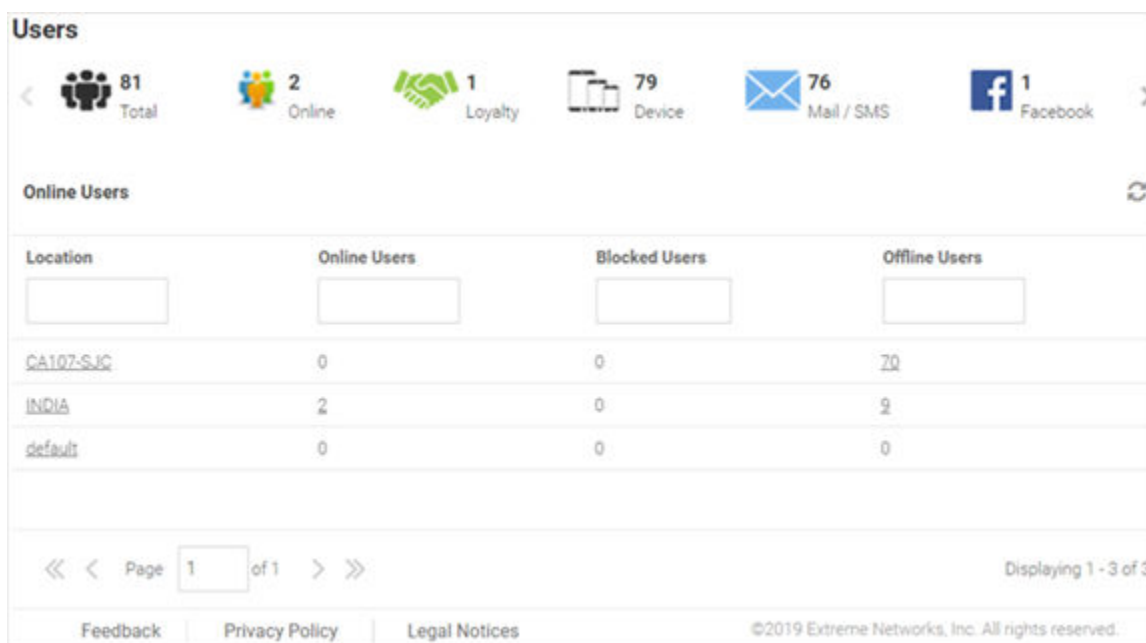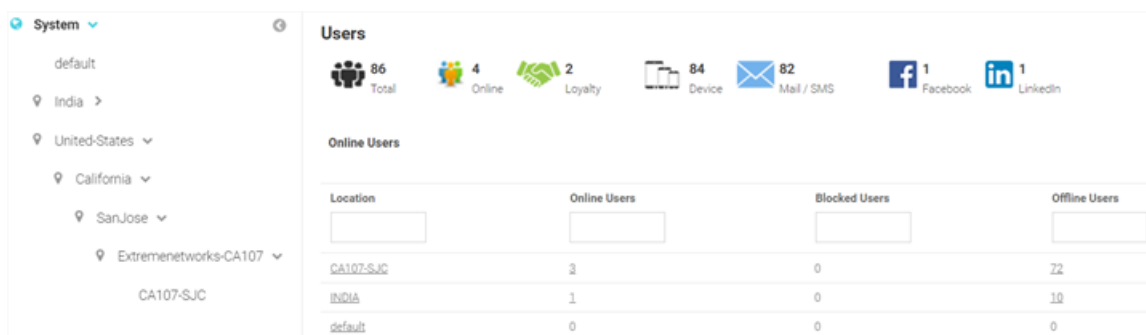
Figure 10: System Users Screen

-
-

Online Users Details

Monitor → Users → Online Users

System Level

You can view user details for the entire network or drill down to the site level to view user details for a specific site. The system-level user details displayed are:

Location — Displays the location or RF Domain name for each configured site.

Online Users — Displays the number of users currently connected to the network for each Location.

Blocked Users — Displays the number of users that are currently blocked from accessing the networks for each Location.

Offline Users — Displays the number of users that are not currently connected to the network for each Location.

Total Users   Displays the number of users, both online and offline, known to the system.

Site Level

Drill down to the site level to view online and blocked user details for a specific site.

Site Level information is displayed when a site is selected from the navigation pane.

User   The **User** column displays the user icon associated with each online user.

Name   The **Name** column displays the username associated with each online user. If using social media authentication, the name is provided by the social media source.

Email   The **Email** column displays the e-mail address associated with each online user. If using social media authentication, the e-mail address is provided by the social media source.

Loyalty ID   The **Loyalty ID** column displays the loyalty id number associated with each online loyalty customer.

Gender   The **Gender** column displays an icon representing the gender of each online user.

Source   The **Source** column displays the method that each online user used to authenticate. When social media authentication is enabled this will include Facebook, Google Plus, LinkedIn and Instagram.

Last Login   The **Last Login** column displays the full date and time when the user last authenticated on the network.

MAC   The **MAC** column displays the MAC address for each listed user. This column is not displayed by default, but may be enabled from the **Columns** menu.

Mobile   The **Mobile** column displays the mobile phone number for each listed user. This column is not displayed by default, but may be enabled from the **Columns** menu.

City   The **City** column displays the city associated with each listed user. This column is not displayed by default, but may be enabled from the **Columns** menu.

SSID   The **SSID** column displays the wireless network SSID that each listed user is connected through. This column is not displayed by default, but may be enabled from the **Columns** menu.

Network   The **Network** column displays the wireless network that each listed user is connected through. This column is not displayed by default, but may be enabled from the **Columns** menu.

Action
               From the **Action** column perform one of the following actions on a user. Select **Disconnect** to end a user's session on the network. Select **Block** to stop a user from using the network

for 24 hours. The user may reconnect if they re-authenticate. Select **Delete** to remove a user from the database. If the user connects again they will be treated as new user.

Blocked User Details

Monitor → Users → Blocked Users

The data displayed on the user screen changes with the tree-node selected in the left-hand pane. To view user details for a specific site (RF Domain), drill-down to the site level, which is the last node in each branch.

System Level

The system node displays user details for all sites configured within the system. The following information is displayed on a per-site basis:

Location	This column displays the location name or RF Domain for each configured site.
Online Users	This column displays the number of users currently connected to the network.
Blocked Users	This column displays the number of users currently blocked from accessing the network.
Offline Users	This column displays the number of users that are not currently connected to the network for each **Location**.
Total Users	Displays the number of users, both online and offline, known to the system.
Unblock	Select to unblock the selected blocked user.

Site Level

The site level information is displayed when a site is selected from the navigation pane.

User	Displays the user icon associated with each online user.
Name	The **Name** column displays the username associated with each online user. If using social media authentication, the name is provided by the social media source.
Email	The **Email** column displays the e-mail address associated with each online user. If using social media authentication, the e-mail address is provided by the social media source.
Gender	The **Gender** column displays an icon representing the gender of each online user.
Source	The **Source** column displays the method that each online user used to authenticate. When social media authentication is enabled this will include Facebook, Google Plus, LinkedIn and Instagram.
Last Login	The **Last Login** column displays the full date and time when the user last authenticated on the network.
MAC	The **MAC** column displays the MAC address for each listed user. This column is not displayed by default, but may be enabled from the **Columns** menu.
Mobile	The **Mobile** column displays the mobile phone number for each listed user. This column is not displayed by default, but may be enabled from the **Columns** menu.
City	The **City** column displays the city associated with each listed user. This column is not displayed by default, but may be enabled from the **Columns** menu.
SSID	The **SSID** column displays the wireless network SSID that each listed user is connected through. This column is not displayed by default, but may be enabled from the **Columns** menu.
Network	The **Network** column displays the wireless network that each listed user is connected through. This column is not displayed by default, but may be enabled from the **Columns** menu.

Action

From the **Action** column perform one of the following actions on a user. Select **Disconnect** to end a user's session on the network. Select **Block** to stop a user passing traffic on the network for 24 hours. Select **Unblock** to restore the users ability to pass traffic on the network. The user may reconnect if they re-authenticate. Select **Delete** to remove a user from the database. If the user connects again they will be treated as new user.

4 Dashboard

Dashboard Basics
Creating a New Dashboard
Available Dashboard Widgets

Dashboard provides a holistic view of user data at the entity level or for individual sites. The Dashboard menu offers customizable widgets and layout themes. Use these widgets and themes to create customized dashboards providing a comprehensive overview of user trends and engagement.

Select **Dashboard** from the main menu, to view existing dashboards and to access the create dashboard option. For more information, refer to the following sections:

- Creating a New Dashboard on page 29
- Available Dashboard Widgets on page 32

Dashboard Basics
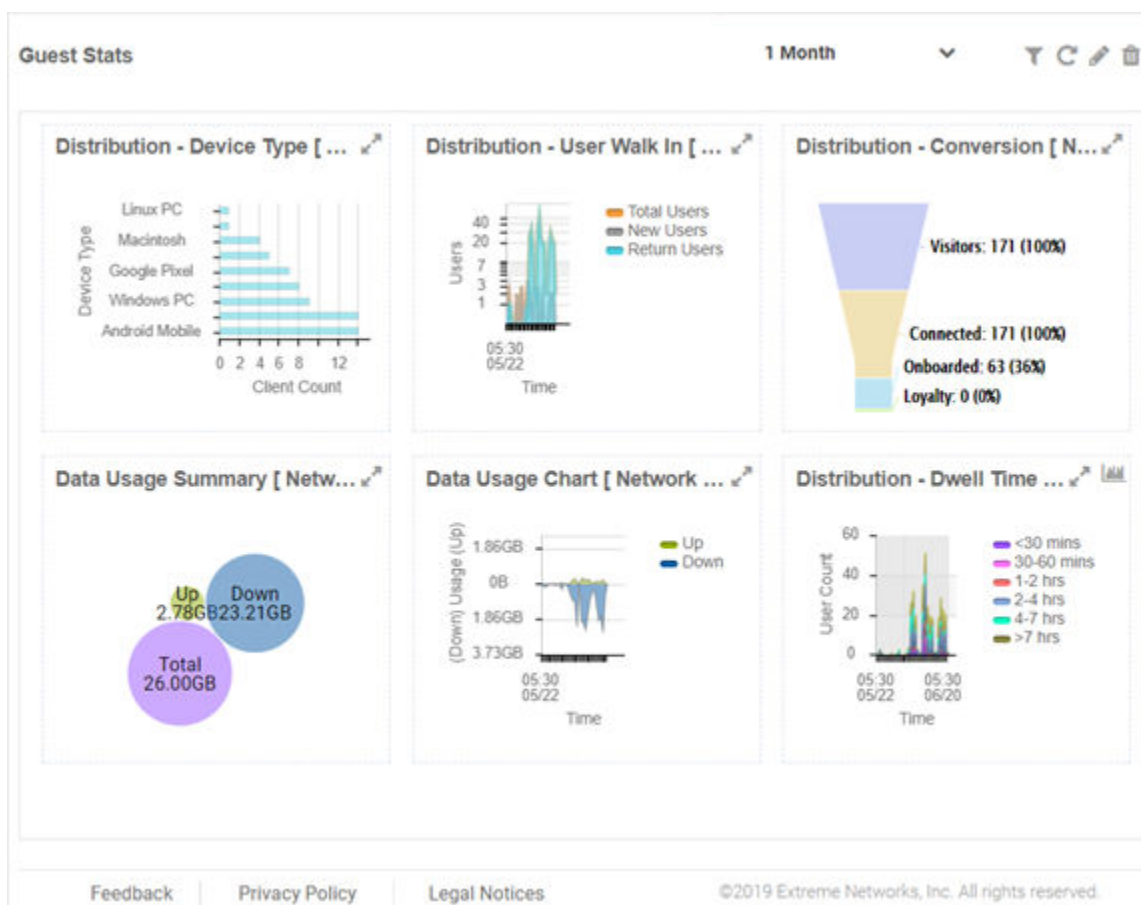
Figure 11: Example Dashboard Screen

Dashboard Components

Dashboards contain the following two main components:

- **Themes** - define the layout of the dashboard page and control the number of widgets that can be displayed.
- **Widgets** - control the type of information that is displayed in the dashboard. For more information on what dashboard widgets are available see: Available Dashboard Widgets on page 32.

Dashboard Controls

Filter data or change the view of a widget using the controls available on the dashboard. Not all controls are available for each widget. The following table describes the widget controls:

Table 4: Dashboard Controls

Dashboard Control	Location	Description
▼	Top-right corner of the dashboard	Select to enable the ⌄ network filter option within each widget. Select a network from the pull-down menu, and the dashboard updates to show data only for the selected network.
↻	Top-right corner of the dashboard	Select to refresh the dashboard data.
✏	Top-right corner of the dashboard	Select to add, edit or remove widgets from the dashboard.
🗑	Top-right corner of the dashboard	Select to remove widgets from the dashboard.
↗ and ↙	Top-right corner of the widget	Select to maximize and minimize a widget respectively.

Report Duration Filter

The dashboard widgets let you filter data based on time duration. Select the report duration from the drop-down menu on the top-right, corner of the dashboard.

Figure 12: Report Duration Filter

The filter options are:

- **1 Hr**
- **8 Hrs**
- **1 Day**
- **1 Week**
- **1 Month**
- **3 Months**

- **6 Months**
- **1 Year**

Creating a New Dashboard

Dashboard → Create New

This section describes how to create customized ExtremeGuest dashboards.

You can create customized ExtremeGuest dashboards with specific theme and widget layouts. Themes define the number of data fields displayed in respect to the number of data items (widgets) trended. ExtremeGuest features a flexible dashboard design where the dashboard widgets can be added individually and freely resized once added to the dashboard.

To create a new dashboard:

1   Go to **Dashboard → Create New**.
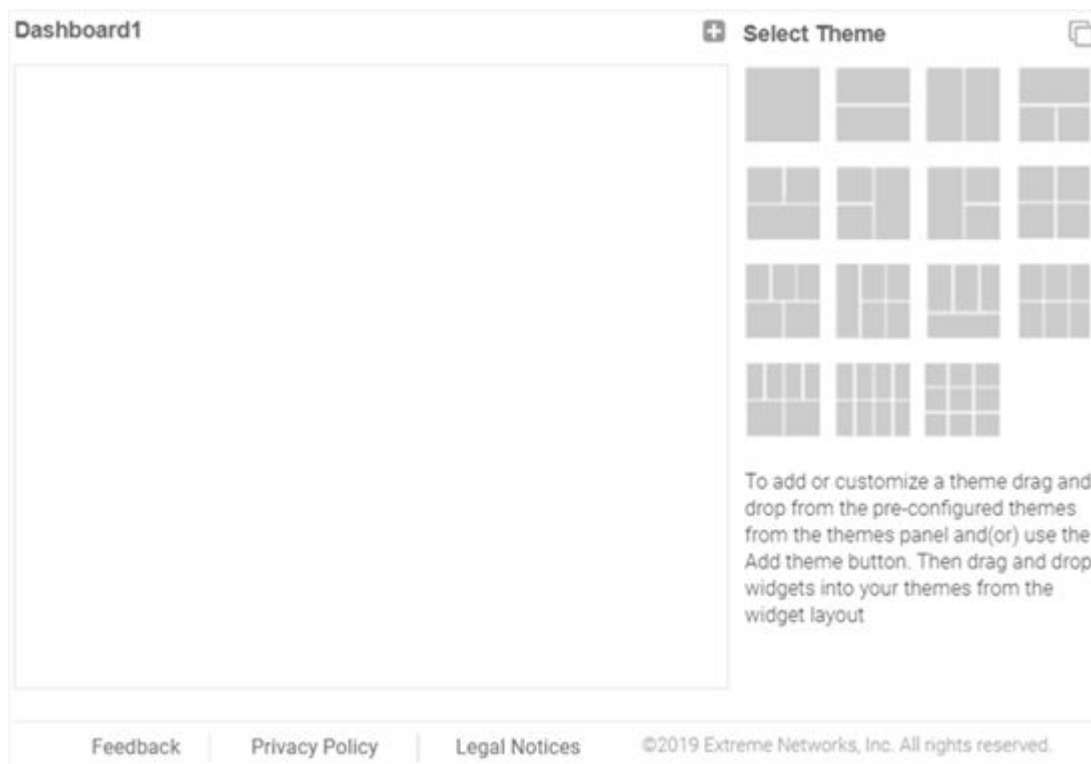
The create new dashboard screen displays.

Figure 13: ExtremeGuest New Dashboard Screen

> **Note**
> The new dashboard screen displays with no themes or widgets selected.

2   Drag and drop a theme from the **Select Theme** menu on to the main window.

To change the layout, drag another theme in place of the current one.

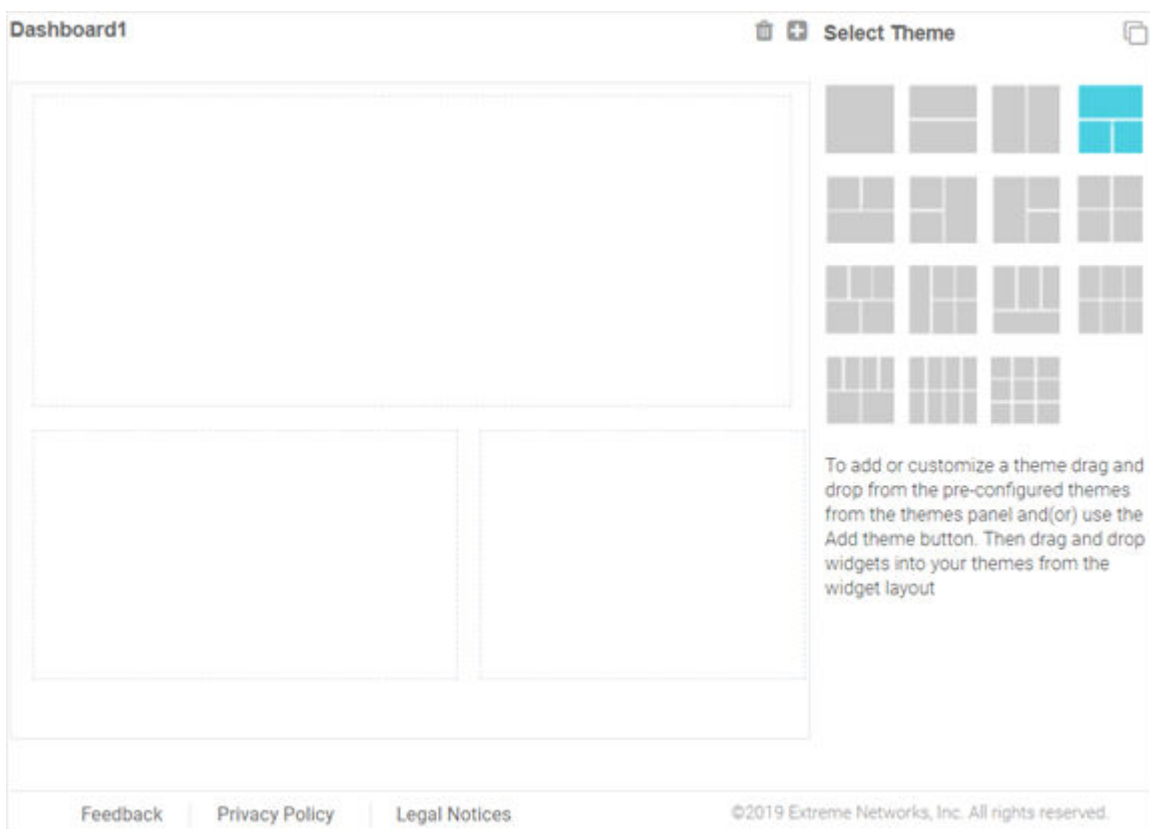The dashboard layout displays the theme outline.

Figure 14: Selecting a Dashboard Theme

3   Change to the **Select Widget** view, by clicking the ⬜ icon.

4   Drag widgets into the layouts to populate the dashboard.

Figure 15: Selecting Dashboard Widgets

> **Note**
>
> Once a widget is placed it displays the data associated with that widget. For information on the widget types available, see

---

5   Select **Save** to commit your changes or select **Cancel** to cancel dashboard creation.

When saving a new dashboard provide the following information:

Name   Enter a `name` that uniquely identifies the dashboard and defines its purpose. Once added, this dashboard name displays in the **Dashboard** menu.

> **Note**
>
> This value is mandatory.

Description   Enter a brief description of the newly created dashboard.

> **Note**
>
> This value is optional.

Public   Select this option to make the dashboard available to all ExtremeGuest management interface users.

6   Select **Save** to save and exit.

Available Dashboard Widgets

Category	Widget	Description
Clients	Distribution - Device Type	Bar graph displaying client count sorted by mobile device model.
Clients	Distribution - OS Type	Bar graph displaying client count sorted by the operating system used on the user's mobile device.
Clients	Distribution - Browser Type	Bar graph displaying client count sorted by the web browser used to authenticate on the user's mobile device.
Users	Distribution - Age Range	Pie chart displaying client age ranges in the following distribution: • **< 18** • **18-20** • **21-24** • **25-34** • **35-44** • **45-54** • **55-64** • **> 64**
Users	Distribution - Gender	Pie chart displaying user distribution by gender.
Users	Distribution - Social	Bar graph displaying user distribution by authentication source. When social media authentication is enabled this includes the social media platform users used as mode of authentication.
Users	User Distribution - Active users at current location	Chart displaying active user details. Details include **User** icon, **Name**, **Email**, **Gender**, **Source** (the authentication mode used), and **Last Login** (date and time of last login).
Users	Distribution - Loyalty	Graph displaying number of users with the customer app installed on their device.
Users	Distribution - Conversion	Graph displaying the number and percentage of users who converted from **Connected** to **Onboarded** to **Loyalty** customers.
Users	Distribution - Dwell Time	Bar graph displaying the amount of time users stayed at a location over a filtered time period. Filter the **Dwell Time** information into the following time periods: • 1 hour: with data points each minute • 8 hours: with data points each hour • 1 day: with data points each hour • 1 week: with data points each day • 1 month: with data points each day • 3 months: with data points each day
Users	Distribution - User Walk In	Graph displaying the number of users entering a location over a filtered time period. Filter the **User Walk In** information into the following time periods: • 1 hour: with data points each minute • 8 hours: with data points each hour • 1 day: with data points each hour • 1 week: with data points each day • 1 month: with data points each day

Category	Widget	Description
		• 3 months: with data points each day • 6 months: with data points each day • 1 year: with data points each day Data is further separated between **Total Users**, **Return Users**, and **New Users**.
Usage	Data Usage Chart	Graph displaying upstream and downstream bandwidth usage over time.
Usage	Data Usage Summary	Graph displaying upstream, downstream, and total bandwidth usage.
Usage	Key Metrics	Infographic displaying user information about online status, device, loyalty and social media sign in status.
Miscellaneous	Label	Custom label for creating Dashboard titles.

5 Configuration

The **Configuration** menu provides sub-menus that define the various aspects of your ExtremeGuest captive portal. For more information, refer to the following sections:

AAA Configuration

Configuration → AAA

AAA (Authentication, Authorization, and Accounting) provides the mechanism network administrators use to define access control within their networks.

AAA provides a modular way of performing the following services:

Authentication Authentication provides a means for identifying users, including login and password dialog, challenge and response, messaging support and (depending on the security protocol), encryption. Authentication is the technique by which a user is identified before allowed access to the network. Configure AAA authentication by defining a list of authentication methods, and then applying the list to various interfaces. The list defines the authentication schemes performed and their sequence. The list must be applied to an interface before the defined authentication technique is conducted.

Authorization   Authorization occurs immediately after authentication. Authorization is a method for remote access control, including authorization for services and individual user accounts and profiles. Authorization functions through the assembly of attribute sets describing what the user is authorized to perform. These attributes are compared to information contained in a database for a given user and the result is returned to AAA to determine the user's actual capabilities and restrictions. The database could be located locally or be hosted remotely on a RADIUS server. Remote RADIUS servers authorize users by associating attribute-value (AV) pairs with the appropriate user. Each authorization method must be defined through AAA. When AAA authorization is enabled it's applied equally to all interfaces.

Accounting   Accounting is the method for collecting and sending security server information for billing, auditing, and reporting user data; such as start and stop times, executed commands (such as PPP), number of packets, and number of bytes. Accounting enables wireless network administrators to track the services users are accessing and the network resources they are consuming. When accounting is enabled, the network access server reports user activity to a RADIUS security server in the form of accounting records. Each accounting record is comprised of AV pairs and is stored on the access control server. The data can be analyzed for network management, client billing, and/or auditing. Accounting methods must be defined through AAA. When AAA accounting is activated, it's applied equally to all interfaces on the access servers.

For more information on configuring AAA parameters, refer to the following sections:

- AAA Authorization on page 35
- AAA Group on page 40
- AAA NAS on page 44

AAA Authorization

Configuration → AAA → Authorization

Figure 16: AAA Authorization Screen

The AAA Authorization screen lists existing AAA Authorization policy details. This list contains both user-defined and system-provided policies.

Name Displays the unique name assigned to the AAA Authorization policy when it was created.

Description Displays the description entered when the AAA Authorization policy was created.

Action Select the 🗑 icon to delete an existing AAA Authorization policy.

Default, System-provided Authorization Policies

The ExtremeGuest portal provides the following default authorization policies that you can edit and use or use as is:

TempAccessPolicy Provides temporary guest access to your network. Note, temporary guest users are not applied any role/group.

UnregisteredPolicy Registers a first-time guest user and applies the *Unregistered* role to the user.

GuestAccessPolicy This policy is applicable for already registered guest users. It authenticates the user, applies the *Guest Access* role/group and provides network access.

DenyAccessPolicy Denies access to registered users who are not authorized to access the network.

Adding AAA Authorization

Configuration → AAA → Authorization → Add

To add AAA Authorization policy:

1   Go to **Configuration → AAA** .

The **Authorization** screen displays by default.

2   Select the ✚ icon to add a new authorization profile.

The add **Authorization** screen displays.

Figure 17: AAA Authorization Add Screen

3   Configure the following settings:

Name   Specify a unique designation for the new authorization profile.

> **Note**
> This setting is mandatory.

Description   Enter a description for the new authorization profile.

> **Note**
> This setting is mandatory.

VLAN	Use the spinner controls to assign a specific VLAN to this RADIUS user group. Ensure Dynamic VLAN assignment (single VLAN) is enabled for the network and RADIUS VLAN assignment is configured in the captive portal policy in order for the VLAN assignment to work properly.
Network SSID	Assign a list of SSIDs users within this RADIUS group are allowed to associate with. Assign WLAN SSIDs representative of the configurations a guest user will need to access.
Rate Limit From Air	Set the rate limit for clients within the RADIUS group. Use the spinner to set value from 100-1,000,000 Kbps.

> **Note**
> Leave this field blank to disable rate limiting.

Rate Limit To Air	Set the rate limit from clients within the RADIUS group. Use the spinner to set value from 100-1,000,000 Kbps.

> **Note**
> Leave this field blank to disable rate limiting.

Inactivity Timeout	Set an inactivity timeout from 60 - 86,400 seconds. If a frame is not received from a client within the set time, the current session is terminated.
Session Timeout	Enable this option to set a client session timeout from 5 - 144,000 minutes. This is the session time a client is granted upon successful authentication. Upon expiration, the RADIUS session is terminated.
Block Time	Specify a **Block Time** to control the amount of time before a user can reconnect after their session ends.
Application Policy	Specify an **Application Policy** to associate with this authorization profile.
Role (Filter-ID)	Specify a **Role** to associate with this authorization profile.

> **Note**
> If you are deploying ExtremeGuest as the external authentication server for *ExtremeCloud Appliance* or *ExtremeControl* managed networks, ensure the *Role (Filter-ID)* value is the same as the roles configured in the ExtremeGuest captive-portal configurations set on ExtremeCloud Appliance and ExtremeControl servers.

4 In the **Schedule** section, select **Restrict Access** to restrict network access to certain days or time.

By Time	Select this option to set an access time period. When selected, the **Start** and **End** options are enabled. Schedule the network access time period. Guest users will have daily access only during the time specified here.
By Day of Week	Select this option to limit access on certain days of the week. Guest users will have access only on the days specified here.

> **Note**
> Use both options to restrict access to a specific time on specific days.

5 Select **Save** to save your changes or select **Cancel** to discard the new authorization policy.

AAA Group

Configuration → AAA → Group

Figure 18: AAA Group Screen

The AAA Group screen displays existing AAA Groups and their basic configuration.

Name	Displays the unique name assigned to the AAA Group when it was created.
Description	Displays the description entered when the AAA Group was created.
Action	Select the 🗑 icon to delete an existing AAA Group.

Default, System-provided AAA Groups

The ExtremeGuest portal provides the following default AAA groups that you can edit and use or use as is:

Unregistered	This is the default group applied to users before registration. The AAA Authorization policy associated with this group is *UnregisteredPolicy*.

DenyAccess   This is the default group applied to users who are already registered but are unathorized to use the network. The AAA Authorization policy associated with this group is *DenyAccessPolicy*
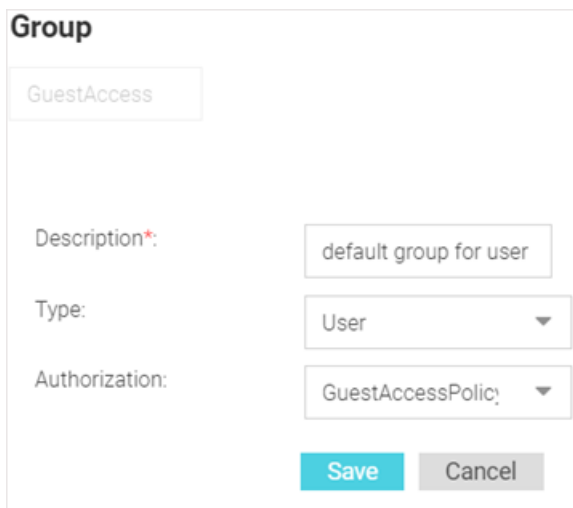

GuestAccess   his is the default group applied to users have they have registered. The AAA Authorization policy associated with this group is *GuestAccessPolicy*

Adding AAA Groups

Configuration → AAA → Group → Add

To add AAA Groups:

1   Go to **Configuration → AAA** from the navigation menu.

    The **Authorization** screen displays by default.

2   Select the **Group** tab.

3   Select the ➕ icon to create a new group.

    The add AAA Group screen displays.
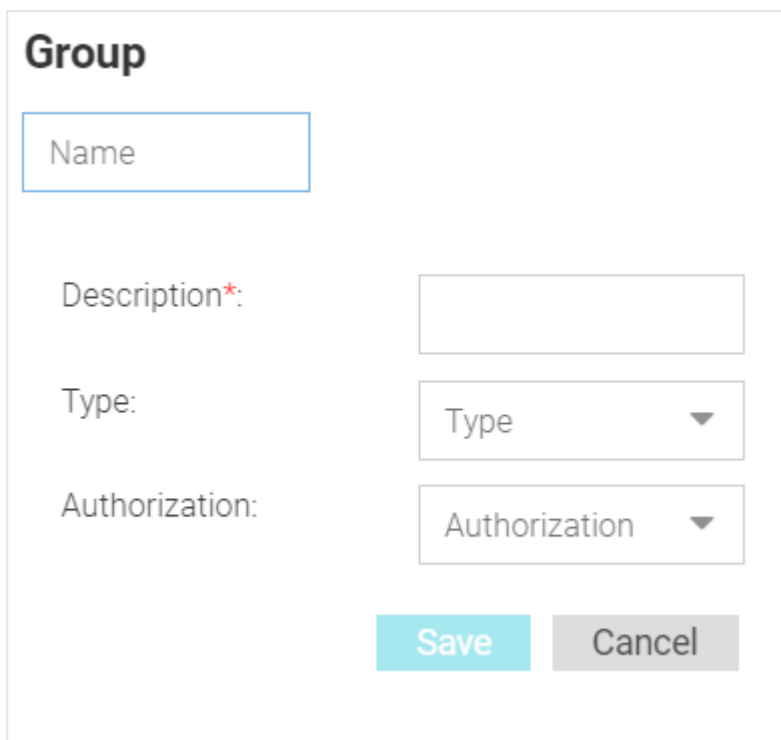
Figure 19: AAA Groups Add Screen

4   Configure the following settings:

Name   Enter a unique name for the new AAA group.

> **Note**
> This setting is mandatory.

Description   Enter a description for the new AAA group.

> **Note**
> This setting is mandatory.

Type   Specify the type of group using the pull down menu. Available group types are **User** and **Device**.

Authorization Select an **Authorization** policy from the pull-down menu.

5   Select **Save** to save your changes, or select **Cancel** to discard the new AAA group.

AAA NAS

Configuration → AAA → NAS

Figure 20: AAA NAS Screen

The AAA NAS screen lists existing RADIUS clients and their IP address/IP subnet. These are individual clients or a group of clients within a specified subnet that can communicate with the ExtremeGuest RADIUS server.

This screen displays following information:

Name	The unique name assigned to the AAA network when it was created.
Description	The description entered when the AAA network was created.
IP Address / mask	The IP address and network mask associated with the network.

Select the 🗑 icon to delete an existing AAA network configuration.

Adding AAA NAS

Configuration → AAA → NAS → Add

Use the add *NAS (Network Access Server)* screen to configure RADIUS clients and their shared secret. Authentication requests received from RADIUS clients specified here are accepted by the ExtremeGuest RADIUS server. You can configure a single IP address or an IP subnet.

Starting with this release, ExtremeGuest can be deployed as the external authenticating server for the *ExtremeCloud Appliance* and *ExtremeControl* managed networks.

The ExtremeGuest *AAA NAS* configuration (IP address/IP subnet and shared secret) should always point to the RADIUS client, the host sending the RADIUS request to the ExtremeGuest RADIUS server.

• In WiNG deployments - the RADIUS client could be the controller, RF Domain manager or individual APs. If the RADIUS request is being proxied through the controller or RF Domain manager, configure the IP address and shared secret of the controller or RF Domain manager respectively. If the APs are

directly communicating with the ExtremeGuest RADIUS server, configure the IP address and shared secret of each AP.

> **Note**
> The shared secret configured here should match with the RADIUS server shared secret configured in the AAA policy on the WING device (controller/RF Domain manager/APs).

• In ExtremeCloud Appliance deployments - the RADIUS client is the ExtremeCloud Appliance host. Configure the IP address/IP subnet and shared secret of the ExtremeCloud Appliance host.

> **Note**
> The shared secret configured here should match with the RADIUS server shared secret configured in the AAA policy on the ExtremeCloud Appliance server.

• In ExtremeControl deployments - the RADIUS client is the ExtremeControl host. Configure the IP address/IP subnet and shared secret of the ExtremeControl host.

> **Note**
> The shared secret configured here should match with the RADIUS server shared secret configured under **Access Control** → **Configurations** → **AAA** → **RADIUS Servers** on the ExtremeControl server.

To add AAA Networks:

1 Go to **Configuration** → **AAA** from the navigation menu.

   The **Authorization** screen displays by default.

2 Select the **NAS** tab.

   A list of existing AAA NAS configurations is displayed.

3 Select the ➕ icon to create a new NAS configuration.

   The add AAA NAS screen displays.

Figure 21: AAA NAS Add Screen

4 Configure the following settings:

Name Specify a unique name for the new AAA network.

> **Note**
> This setting is mandatory.

Description Specify a description for the new AAA network.

> **Note**
> This setting is mandatory.

IP Address / mask Displays the IP address and network mask associated with each network.

> **Note**
> This setting is mandatory.

Shared Secret Enter the RADIUS client shared secret password in the **Shared Secret** field. This password is for authenticating the RADIUS NAS clients. Select the **Show** check box to expose the shared secret's actual character string, leaving the option unselected displays the shared secret as a string of asterisks (*).

> **Note**
> The shared secret configured here should be the same as the one configured in the AAA RADIUS server context on the WiNG device, ExtremeCloud Appliance, or ExtremeControl depending on where the network is configured.

5   Select **Save** to save your changes.

Select **Cancel** to discard the new AAA network.

ExtremeControl

Configuration → ExtremeControl

Starting with this release, ExtremeGuest can be deployed as the external captive portal server handling guest registration and authentication for wired users of *ExtremeControl* NAC deployments in conjunction with Extreme EXOS switches.

ExtremeGuest can now handle RADIUS authentication requests from wired-guest users connected to ExtremeControl managed switches. Where, ExtremeControl acts as the proxy between the switch and ExtremeGuest. It receives the clients' RADIUS request, includes a *VSA (Vendor Specific Attribute)* attribute in the RADIUS request and forwards it to ExtremeGuest. The VSA attribute indicates that the RADIUS request is proxied through ExtremeControl. Communication between ExtremeGuest and ExtremeControl is through REST APIs.
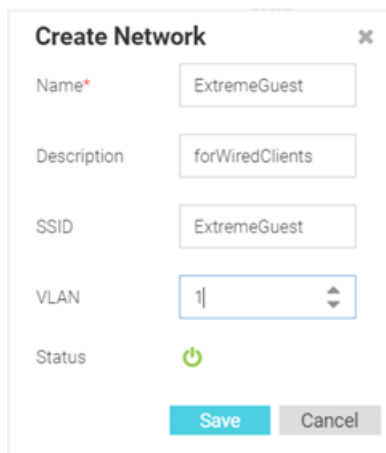
Use the **ExtremeControl API Settings** screen to configure the credentials and shared secret required for ExtremeGuest to authenticate with ExtremeControl.

> **Note**
> ExtremeControl - ExtremeGuest integration is mandatory to enable this functionality. You will also need to make pre-configurations on the ExtremeGuest server. For detailed information on both, please refer to the "ExtremeGuest_6.0.0_HOW-TO_Deploy_with_ExtremeControl" guide available at https://extremenetworks.com/documentation.

Pre-configurations:

Following configurations are prerequisites for this feature to work:

1 *ExtremeControl* with *ExtremeGuest* integration completed.
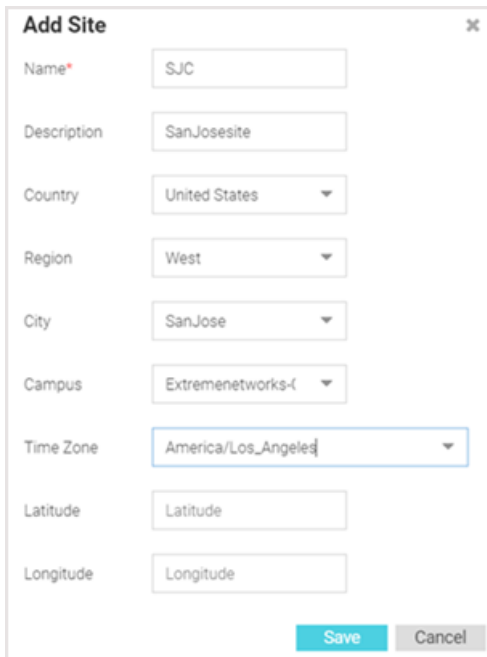2 On the *ExtremeGuest* UI configure the following settings:

    a Add Network.

> **Note**
> The *network* name should be the same as the *captive portal* name configured on ExtremeControl.

> **Note**
> For information on adding a network, see Networks on page 53.

    b Add a Site.

> **Note**
>
> Add the site in which the wired-switch is deployed. The Site Name should match the name of the site to which the EXOS, wired-switch is mapped.

> **Note**
>
> For information on adding a site, see Sites on page 55.

c   Add ExtremeControl managed switch to the device list:

Note

Select the **Wired** checkbox to populate the **Model** drop-down menu with the supported wired switches. For information on adding a device, see Devices on page 58.

d   Create a AAA authorization policy. This is optional, as you can use the default AAA Authorization policy. See screenshot below:

	UnregisteredPolicy	user not registered
	GuestAccessPolicy	for registered user without group assignment

Note

Create authorization profiles for the wired-guest users (unregistered and registered) connected to ExtremeControl managed switches. Alternately, you can use following two default, system-provided authorization policies: *UnregisteredPolicy* and *GuestAccessPolicy*.

Ensure that the **Role (filter-id)** value configured in the authorization policy (customized or default) matches the Policy Role names configured on ExtremeControl.

Authorization profiles define access rules, such as rate-limiting, session timeout, block time, application policies, etc. After configuring the authorization profile, apply it to a user group. For information on creating AAA Authorization policy, see Adding AAA Authorization on page 39.

e   Create a AAA user group. This is optional, as you can use the default AAA Group. See screenshot below:

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

Ensure the authorization policy, created in the previous step is applied to the group (customized or default).

> **Note**
>
> This is the group to which the authenticated wired guest user will be added. Ensure that the group name is same as the group name specified in the ExtremeControl AAA group configuration context. For information on creating a AAA group, see Adding AAA Groups on page 43.

f   Create a AAA NAS configuration pointing to the ExtremeControl host's network/IP address. Ensure that the AAA NAS is configured to handle RADIUS authentication and accounting requests from the ExtremeControl managed switch.

> **Note**
>
> For information on configuring AAA NAS parameters, see Adding AAA NAS on page 45.

3   Add On-boarding Policy and Rules to enable wired/wireless guest registration when they join a hotspot network.

> **Note**
>
> On-boarding enables hotspot network providers to collect client information, send client passcodes and set up external approval for guest access using rules and policies. For information on creating a On-boarding Policy and Rules, see Onboarding Policy on page 67 and Onboarding Rules on page 69.

4   Add splash templates. These are the captive portal web pages (landing, registration, welcome, etc.) served to the wired-client.
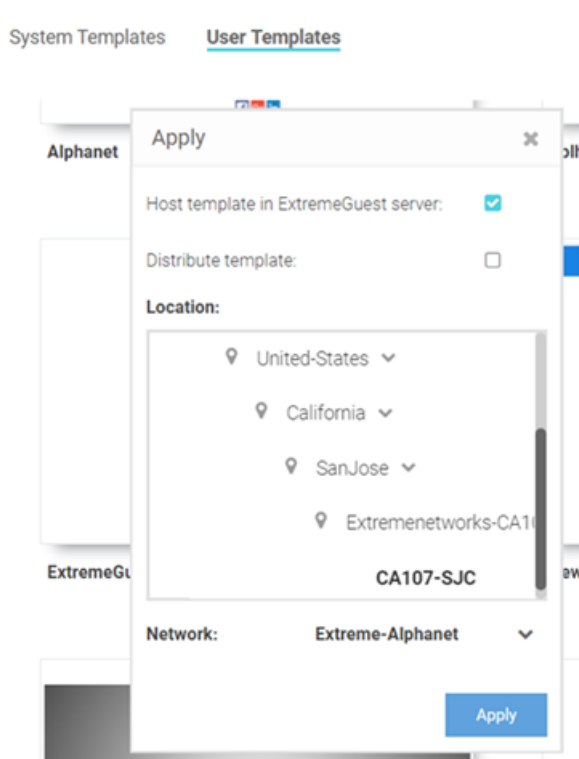
Once the above configurations are in place, configure the **ExtremeControl API Settings**. This consists of the ExtremeControl *management user account credentials* and *shared secret*. This enables ExtremeGuest server to post REST requests to ExtremeControl on successful registration of the wired-guest client.

1 Go to **Configuration** → **ExtremeControl**.

   The **ExtremeControl API Settings** window displays.

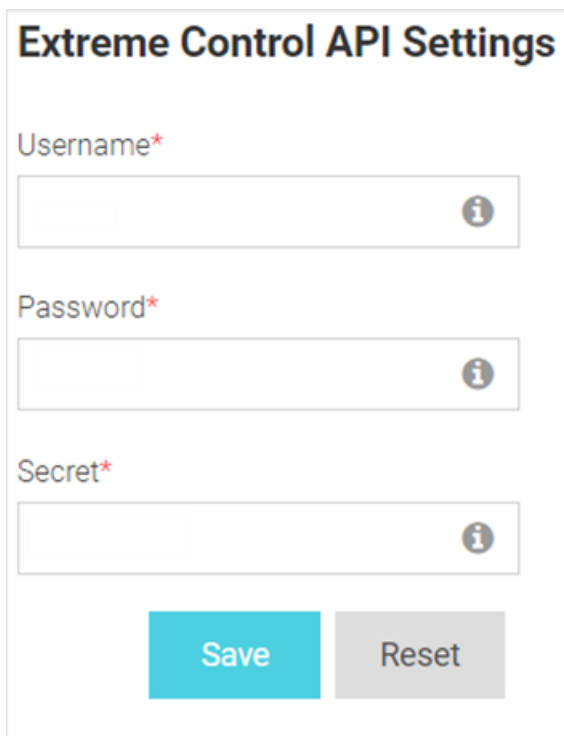**Figure 22: ExtremeControl API Settings Window**

2 In the **Username** field enter user name of the ExtremeControl user.

3 In the **Password** field, configure the password associated with the above specified username.

4 In the **Secret** field, enter the pre-configured shared secret.

> **Note**
> This value should be the same as the RADIUS server shared secret configured in the AAA policy context on ExtremeControl.

5 Click **Save** to save your changes.

   Click **Reset** to revert to original settings.

Networks

Configuration → **Networks**

The **Networks** screen provides status and management for networks attached to the ExtremeGuest application.

> **Note**
> For *ExtremeWireless WiNG* deployments, enter the ExtremeGuest IP address on the WiNG Controller or AP for automatic synchronization of networks. In these deployments there is no need to add or edit networks.

Note

For *ExtremeCloud Appliance* deployments, enter the ExtremeGuest IP on the ExtremeCloud Appliance host for automatic synchronization of networks. In these deployments there is no need to add or edit networks.

1 Go to **Configuration** → **Networks** from the main menu.

A list of existing networks displays. If you are using an *ExtremeWireless WiNG* or *ExtremeCloud Appliance* deployment and have entered the IP address of the ExtremeGuest server, the known networks added on these deployments will auto populate.

Figure 23: Networks Screen

2 Review existing network details:

Name	Displays the name associated with each known wired or wireless network. Selecting a network name displays a dialogue for editing the network's **Name**, **Description**, **SSID**, or **VLAN**. To filter by name or portion of a name, enter the string in the box at the top of the **Name** column.

Note

SSID is only applicable to wireless networks.

Description	Displays the optional description associated with each wired or wireless network.
SSID	Displays the SSID associated with each wireless network. Wired networks do not have SSIDs and are blank. To filter by SSID or partial SSID, enter the string in the box at the top of the **SSID** column.

VLAN   Displays the VLAN ID associated with each network. To filter by VLAN, enter the VLAN number in the box at the top of the **VLAN** column.

Status   The status icon displays green for networks that are online and grey for networks that are disabled. Selecting that icon will toggle the status between online and disabled.

Action   Select the 🗑 icon to remove the associated wired or wireless network from ExtremeGuest.

3   Select the ↻ icon periodically to refresh the data.

4   Select the ➕ icon to add a new network.

Name	Provide a name for the network.
	Note: This field is mandatory.
Description	Optionally, provide a brief description for the network.
SSID	Optionally, specify the network's SSID.
VLAN	Optionally, specify the VLAN associated with this network.
Status	Use the ⏻ icon to disable/enable the network.
	Note: Green/Grey colors indicate the network is enabled/disabled respectively. By default the network is enabled.
Save/Cancel	Select **Save** to save your changes. Select **Cancel** to exit without saving your changes.

5   To remove multiple networks from ExtremeGuest, select the boxes for each network then select the 🗑 icon.

Sites

Configuration → Sites

The **Sites** screen lists sites attached to the ExtremeGuest application. It provides description and location information for sites.

> **Note**
> For *ExtremeWireless WiNG* deployments, enter the ExtremeGuest IP address on the WiNG Controller or AP for automatic synchronization of sites. In these deployments there is no need to add or edit sites.

> **Note**
> For *ExtremeCloud Appliance* deployments, enter the ExtremeGuest IP on the ExtremeCloud Appliance host for automatic synchronization of sites. In these deployments there is no need to add or edit sites.

1   Go to **Configuration** → **Sites** from the main menu.

A list of existing sites displays. If you are using an *ExtremeWireless WiNG* or *ExtremeCloud Appliance* deployment and have entered the IP address of the ExtremeGuest server, the known sites added on these deployments will auto populate. Sites that are enabled display a green icon. Disabled sites display a grey icon. APs connected to disabled sites do not count against the licenses in use.

Figure 24: Sites Screen

2   The **Sites** screen displays the following:

Name   Displays the name associated with each site. Double-click the required site name from the displayed list. The site details open as a dialogue box, where you can edit the site's **Name**, **Description**, **Country**, **Region**, **City**, **Campus**, **Time Zone**, **Latitude** or **Longitude**.

> **Note**
> To filter by name or portion of a name, enter the string in the box at the top of the **Name** column. The screen updates with sites having names matching the specified string. To clear the filter select the ✖ icon.

Description   Displays the description associated with each site.

Country   Displays the name of the country for each site.

> **Note**
> To filter by country name or portion of a country name, enter the string in the box at the top of the **Country** column. The screen updates with sites having *country* configuration matching the specified string. To clear the filter select the ✖ icon.

Region   Displays the optional region associated with each site such as the state, province, or county.

> **Note**
> To filter by region name or portion of a region name, enter the string in the box at the top of the **Region** column. The screen updates with sites having *region* configuration matching the specified string. To clear the filter select the ✖ icon.

City   Displays the optional city associated with each site.

> **Note**
> To filter by city name or portion of a city name, enter the string in the box at the top of the **City** column. The screen updates with sites having *city* configuration matching the specified string. To clear the filter select the ✖ icon.

Campus   Displays the optional campus name configured for each site.

> **Note**
> To filter by campus name or portion of a campus name, enter the string in the box at the top of the **Campus** column. The screen updates with sites having *campus* configuration matching the specified string. To clear the filter select the ✖ icon.

Time Zone   Displays an abbreviated version of the optional time zone configured for each site.

> **Note**
> To filter by time zone, enter the abbreviated time zone name in the box at the top of the **Time Zone** column. The screen updates with sites falling within the specified *timezone*. To clear the filter select the ✖ icon.

Action   Select the 🗑 icon to remove the site from ExtremeGuest.

3 Select the ⟳ icon to update the data in the sites table.

4 Select the ➕ icon to add a new site.

Provide a **Name** for the new site. Optionally configure a **Description**, **Country**, **Region**, **City**, **Campus**, **Time Zone**, **Latitude** and **Longitude** and select **Save**.

Name	Provide a name for the site. **Note:** This field is mandatory
Description	Optionally, provide a description for the site.
Country	Optionally, specify the code of the country where this site will fall.
Region	Optionally, specify the region within the specified country where this site will fall.
City	Optionally, specify the city within the specified region where this site will fall.
Campus	Optionally, specify the campus within the specified city where this site will fall.
Timezone	Optionally, specify the timezone applicable to this site.

Latitude/Longitude	Optionally, specify the latitude and longitude to identify the exact geographical location of the site.
Save/Cancel	Select **Save** to save your changes. Select **Cancel** to exit without saving your changes.

5　To remove multiple sites from ExtremeGuest, select the boxes for each site then select the 🗑 icon.

Devices

Configuration → Devices

The **Devices** screen provides name, MAC address, location and network information for devices on networks attached to the ExtremeGuest application.

> **Note**
>
> For *ExtremeWireless WiNG* deployments, enter the ExtremeGuest IP address on the WiNG Controller or AP for automatic synchronization of devices. In these deployments there is no need to add or edit devices.

> **Note**
>
> For *ExtremeCloud Appliance* deployments, enter the ExtremeGuest IP on the ExtremeCloud Appliance host for automatic synchronization of devices. In these deployments there is no need to add or edit devices.

1　Select **Configuration → Devices** from the main menu.

The devices screen displays. It provides a list of known devices. If you are using an *ExtremeWireless WiNG* or *ExtremeCloud Appliance* deployment and have entered the IP address of the ExtremeGuest server, the known devices added to these deployments will auto populate.

Figure 25: Devices Screen

2   Review the following information for existing devices:

Name	Displays the name associated with each device. Double-click the required device name from the displayed list. The **Edit Device** dialogue box opens. Edit the device's **Name**, **Site Name**, **MAC** address, **Model**, **IP Address**, **Network** and **Managed By** settings.

> **Note**
> To filter by device name or portion of a device name, enter the string in the box at the top of the **Name** column. The screen updates with devices having *name* matching the specified string. To clear the filter select the ✖ icon.

MAC	Displays the MAC address for each known device.

> **Note**
> To filter by MAC address or portion of a MAC address, enter the string in the box at the top of the **MAC** column. The screen updates with devices having *MAC address* matching the specified string. To clear the filter select the ✖ icon.

Site Name	Displays the site name associated with each device.

> **Note**
> To filter by site name or portion of a site name, enter the string in the box at the top of the **Site Name** column. The screen updates with devices having *site* configuration matching the specified string. To clear the filter select the ✖ icon.

Network	Displays the optional network that each device is associated with.

> **Note**
> To filter by network name or portion of a network name, enter the string in the box at the top of the **Network** column. The screen updates with sites having *network* configuration matching the specified string. To clear the filter select the ✖ icon.

Reported By	Displays the name of the controller that reported each device to ExtremeGuest.
Managed By	Displays the name of the controller that is optionally associated with each device.
Action	Select the 🗑 icon to remove an associated device from ExtremeGuest.

3   To associate a controller with a device or multiple devices, select the devices from the table and select the ⊘ icon. Then select a controller to associate with all selected devices.

4   To disassociate a controller from a device or multiple devices, select the devices from the table and select the ⊗ icon. This will remove the associated controller from all selected devices.

5   Select the ⟳ icon to update the data in the devices table.

6   Select the ➕ icon to add a new device.

Name	Provide a name for the device.
Model	Use this drop-down menu to select access point model type. **Note:** To add wired switches, select the **Wired** checkbox. The drop-down menu will now display supported wired switches. Select the required model type from the displayed list.
MAC	Specify the MAC address of the device.

IP Address	Specify the IP address of the device.
Site Name	Use this drop-down menu to specify the site (location/RF Domain) to which this device will be added.
Network	Use this drop-down menu to specify the networks associated with this device.
Save/Cancel	Select **Save** to save your changes. Select **Cancel** to exit without saving your changes.

> **Note**
> All of these fields are mandatory.

7   To remove multiple devices from ExtremeGuest, select the boxes for each device then select the 🗑 icon.

Notification

Configuration → Notification

The **Notification** screens allows you to configure and implement notification policies and rules. Refer to the following for more information:

- Policy on page 60
- Rules on page 64

Policy

Configuration → Notification → Policy

The **Policy** screen displays existing notification policies and their basic configuration. Double-click each policy to view the detailed configuration. Review the configuration details to determine if the policy warrants modification or removal.

Figure 26: Notification Policy Screen

Name   Displays the unique name assigned to the notification policy when it was created.

Description Displays the description entered when the notification policy was created.

Action   Deletes a notification policy. To delete a policy, select the checkbox next to it and then select the 🗑
             icon associated with the policy.

Adding a Notification Policy

Configuration → Notification → Policy → Add

Notification policies specify the method used to communicate the passcode to newly registered guest users.

This screen allows you to specify the mode by which the passcode is communicated. The options are:

- SMS - Uses a third-party SMS service provider. Requires integration with an SMS gateway.
- E-mail - 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.

To add a notification policy:

1 Go to **Configuration → Notification → Policy** .

   The **Policy** screen displays.

2 Select the ➕ icon to create a new policy.

   The add **Policy** screen displays.

Figure 27: Notification Policy Add Screen

3 Provide a name for the policy uniquely identifying its mode and purpose.

> **Note**
> This setting is mandatory.

4 Provide a description for the policy.

This setting is mandatory.

5 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.

Enabling SMS notifications

6   To enable SMS notifications, click the 🔽 icon to open the SMS configuration fields.

   a   Select **Enable** the policy. When enabled, notifications are sent to newly registered guest users via SMS.

   b   In the **Host** field, select one of the following third-party, SMS service providers:

      • api.clickatell.com
      • platform.clickatell.com

   c   In the **API Key** field, enter the API Key (should not exceed 32 characters in length). This is the authentication token provided at the time of registration with the SMS service provider.

   d   In the **Source Number** field, configure the long-address or the from-number associated with this Clickatell user account.

   > **Note**
   > This setting is mandatory for users in the United States.

   e   In the **Message** field, specify the content of the SMS sent to the guest user notifying the pass code. The content should not exceed 1024 characters. Use the following tags in the message: **GM_NAME** for the guest user's name **GM_PASSCODE** for the pass code.

   For example: Dear GM_NAME, your internet access pass code is GM_PASSCODE. In the actual message, the tags are replaced with the username and passcode.

Enabling E-Mail notifications

7   To enable e-mail notifications, click the 🔽 icon to open the e-mail configuration fields.

   a   Select **Enable** the policy. When enabled, notifications are sent to newly registered guest users via e-mail.

   b   In the **Host** field, configure the SMTP server resource's IPv4 address or host name.

   This is the server used for guest management email traffic, guest user credential validation, and pass code reception. Optionally, you can use an existing host alias to identify the SMTP server resource.

   c   In the **Sender** field, configure the sender's e-mail address.

   The sender here is the e-mail address that the pass code is sent from. Guest users require this pass code for registering their guest e-mail credentials using SMTP.

   d   Use the **Security** field to configure the encryption protocol used by the SMTP server when communicating the pass code. The available options are:

none	No encryption used. Use if no additional user authentication is needed beyond the required username and password combination.
SSL	Uses SSL as the encryption protocol. This is the default setting.
STARTTLS	Uses STARTTLS encryption as the encryption protocol.

   e   In the **Port** field, enter the outgoing SMTP port number used by the mail server to send messages.

   > **Note**
   > The default port for the **Security** type selected above displays by default.

   f   In the **Username** field, specify a username unique to this e-mail guest management configuration. After configuring the username, specify the associated password.

   g   In the **Password** field, configure the password associated with the specified SMTP user name.

    h In the **Subject** field, configure the subject line of the e-mail sent to the guest user notifying the pass code (should not exceed 100 characters).

    i In the **Message** field, configure the content of the e-mail sent to the guest user notifying them of a pass code (should not exceed 1024 characters).

Enabling SMS over SMTP notifications

8 To enable SMS over SMTP notifications, click the ⌄ icon to open the associated configuration fields.

    a Select **Enable** the policy. Some SMS gateways send the passcode in an email to the SMS gateway, which in turn forwards the passcode to the user via SMS.

    b In the **Host** field, configure the SMS gateway server's IPv4 address or hostname. This is server used for guest management SMS over SMTP traffic, guest user credential validation and pass code reception. Optionally, you can use an existing host alias to identify the SMS gateway server resource.

    c In the **Sender** field, configure the sender's e-mail address. The sender here is the guest user receiving the pass code. The sender here is the e-mail address that the pass code is sent from. Guest users require this pass code for registering their guest e-mail credentials using SMTP.

    d Use the **Security** field to configure the encryption protocol used by the SMTP server when communicating the pass code. The available options are:

none	No encryption used. Use if no additional user authentication is needed beyond the required username and password combination.
SSL	Uses SSL as the encryption protocol. This is the default setting.
STARTTLS	Uses STARTTLS encryption as the encryption protocol.

    e In the **Port** field, enter the SMTP port number used by the SMTP server to relay SMS messages.

> **Note**
> Selecting the encryption mode in the *Security* field, updates the *Port* field with the default port number associated with the selected encryption mode. For example, if you select SSL encryption, the port number will display as 465 (the default port used by SSL).

    f In the **Username** field, configure a username unique to this SMTP guest management configuration. After configuring the username, specify the associated password. Ensure that the correct password is provided to receive the passcode required for registering guest user credentials with SMTP.

    g In the **Password** field, configure the password associated with the specified SMTP user name.

    h In the **Email of Recipient** field, configures the e-mail recipient's e-mail address (should not exceed 64 characters in length).

    i In the **Subject** field, configure the subject line of the SMS over SMTP sent to the guest user notifying the pass code (should not exceed 100 characters).

    j In the **Message** field, configure the content of the SMS over SMTP sent to the guest user notifying the pass code (should not exceed 1024 characters).

9 Select **Save** to save your changes or select **Cancel** to discard the notification policy.

Rules

Configuration → Notification → Rules

The **Rules** screen displays existing notification rules and their basic configuration. Double-click each rule to view the detailed configuration. Review the configuration details to determine if the rule warrants modification or removal.

Figure 28: Notification Rules Screen

The **Rules** screen displays following information:

Rule Name	Displays the unique name assigned to the rule when it was created.
Policy Name	Displays the name of the notification policy associated with the rule when it was created.
Location	Displays the site that the notification rule applies to.
Network	Displays the Network that the notification rule applies to.
Precedence	Displays the precedence (sequence) of the rule. The precedence value of a rule determines its priority. Rules with higher precedence receive higher priority and are applied first. This value is set (from 1 - 1000) for new notification rule configurations.
Action	Deletes a notification rule. To delete a rule, select the checkbox next to it and then select the 🗑 icon associated with the rule.

Adding a Notification Rule

Configuration → Notification → Rules → Add

To add a notification rule:

1   Go to **Configuration → Notification → Rules** .

    The **Rules** screen displays.

2   Select the ➕ icon to create a new rule.

    The **Create Rule** screen displays.

Figure 29: Notification Create Rules Screen

3 Provide a unique name for the rule.

This is a mandatory field.

4 Use the **Policy** pull-down menu to specify the notification policy to use with the new rule.

> **Note**
> This setting is mandatory.

5 Use the **Network** pull-down menu to select the networks that the notification rule applies to. The default value is **All Networks**, which applies the rule to all networks.

6 Use the **Location** pull-down menu to navigate the system tree and select the site that the notification rule applies to. The default value is **System**, which applies the rule to all locations.

7 Use the **Precedence Level** spinner control to assign a precedence to the rule. The precedence value of a rule determines its priority.

> **Note**
> Lower the precedence value, higher is the priority. Rules with lower precedence will be applied first.

8 Select **Apply** to save the new notification rule. Select **Cancel** to discard the new rule.

Onboarding

Configuration → Onboarding

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

To create an onboarding policy or rule, refer to the following sections:
- Onboarding Policy on page 67
- Onboarding Rules on page 69

Onboarding Policy

Configuration → 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 an onboarding policy:

1 Go to **Configuration → Onboarding → Policy**.

The **Onboarding Policy** screen displays. This screen displays existing onboarding policies and their basic configuration. Double-click each policy to view the detailed configuration. Review the configuration details to determine if the policy warrants modification or removal.

Figure 30: Onboarding Policy Screen

2 Review the following information:

Name	Displays the name assigned to each onboarding policy. Selecting a policy displays the policy criteria details and allows editing of the policy.
Description	Displays the description for each onboarding policy.
Action	Select the 🗑 icon to remove the associated onboarding policy from ExtremeGuest.

3 Select the ↻ icon to update the data in the onboarding policy table.

Adding an Onboarding Policy

4 Select the ➕ icon to add a new onboarding policy.

5 Provide the following information:

Policy Name	Enter a name for the onboarding policy.

Policy Description   Enter a description for the onboarding policy.

Adding Match Criteria to the Onboarding Policy

6   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.

Description   Enter a description for this criteria uniquely identifying its purpose.

Condition(s)   Select one or more of the following conditions to match.

- **User Email Domain**
- **Sponsor Email Domain**
- **Social Type**
- **User Type**
- **Loyalty User**
- **LDAP/Directory Group**
- **User's Device Count**
- **Any**

These conditions determine when the corresponding **Action** is triggered. Adding multiple conditions requires all conditions be met before the action is triggered. Multiple conditions can be specified to enact different policies based on matching conditions.

Action   Select an **Action** from the menu. The **Action** is triggered when all of the **Condition(s)** are met. Select from the following:

Deny Access   Denies network access to any guests matching the configured **Condition(s)**.

Register Device   Registers guests matching the configured **Condition(s)**.

> **Note**
> Specify the **Validity** for guest access in **Days**, **Hours**, and **Minutes**. Select a **Group** for the guest user to join.

Send One-Time-Passcode to User   Delivers a single-use passcode to guests matching the configured **Condition(s)**.

> **Note**
> Specify the **Validity** for guest access in **Days**, **Hours**, and **Minutes**. Select a **Group** for the guest user to join. Select a user **Notification Policy** for sending the One-Time-Passcode to the guest.

Send Passcode to User   Delivers a multiple use passcode to guests matching the configured **Condition(s)**.

> **Note**
> Specify the **Validity** for guest access in **Days**, **Hours**, and **Minutes**. Select a **Group** for the guest user to join. Select a configured user **Notification Policy** for sending the One-Time-Passcode to the guest.

Send One-Time-Pass. on Sponsor Approval	Delivers a single-use passcode to guests matching the configured **Condition(s)** once the guest has been approved by a sponsor.
	Note Specify the **Validity** for guest access in **Days**, **Hours**, and **Minutes**. Select a **Group** for the guest user to join. Select a sponsor **Notification Policy** for sending the approval request to the sponsor.
Send Passcode on Sponsor Approval	Delivers a multiple use passcode to guests matching the configured **Condition(s)** once the guest has been approved by a sponsor.
	Note Specify the **Validity** for guest access in **Days**, **Hours**, and **Minutes**. Select a **Group** for the guest user to join. Select a configured sponsor **Notification Policy** for sending the One-Time-Passcode to the guest.
Send One-Time-Passcode to Sponsor	Delivers a single-use passcode to the sponsor when the configured **Condition(s)** are met.
	Note The sponsor can then provide the single-use passcode to the guest. Specify the **Validity** for guest access in **Days**, **Hours**, and **Minutes**. Select a **Group** for the guest user to join. Select a sponsor **Notification Policy** for sending the approval request to the sponsor.
Send Passcode to Sponsor	Delivers a multiple use passcode to the sponsor when the configured **Condition(s)** are met.
	Note The sponsor can then provide the passcode to the guest. Specify the **Validity** for guest access in **Days**, **Hours**, and **Minutes**. Select a **Group** for the guest user to join. Select a sponsor **Notification Policy** for sending the approval request to the sponsor.

7   Select **Update User** to send status to a user's email or mobile when registration is pending approval or is rejected.

Selecting the **Update User** option enables the **Notification Policies** field. Select a notification policy to specify how the user is notified.

8   Select **Provide Temporary Access** to give the user temporary access to check email for a passcode. Refer to Adding AAA Groups on page 43 for information on adding temporary access policies and authorization.

9   To remove multiple onboarding policies from ExtremeGuest, select the boxes for each policy then select the 🗑 icon.

Onboarding Rules

Configuration → Onboarding → Rules

Onboarding rules are used in conjunction with onboarding policies 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. Create onboarding policies before creating onboarding rules.

To create an Onboarding Rule:

1   Go to **Configuration** → **Onboarding** → **Rules** from the main menu.

    The **Onboarding Rules** screen displays.

Figure 31: Onboarding Rules Screen

Configured onboarding rules display with the following information:

Rule Name	Displays the user configured rule name for each onboarding rule.
Policy Name	Displays the **Policy Name** associated with each rule.
Location	Displays the location associated with each rule. Locations are based on the network associated with the rule.
Network	Displays the network associated with each onboarding rule. A rule can also apply to **All Networks**.
Precedence	Displays the precedence number for each onboarding rule. Precedence determines which order rules are applied in with the higher precedence rules matched first.
Action	Select the 🗑 icon to remove the associated onboarding rule from ExtremeGuest.

2   Select the ↻ icon to update the data in the onboarding rules list.

3   Select the ✚ icon to add a new onboarding rule.

4   Use the **Network** pull-down menu to select the networks that the onboarding rule applies to. The default value is **All Networks**, which applies the rule to all networks.

5   Use the **Location** pull-down menu to navigate the system tree and select the site that the onboarding rule applies to. The default value is **System**, which applies the rule to all locations.

6   Use the **Precedence Level** spinner control to assign a precedence to the rule. The precedence value of a rule determines its priority.

> **Note**
>
> Lower the precedence value, higher is the priority. Rules with lower precedence will be applied first.

7   Select **Apply** when complete to add the onboarding rule.

8   To remove multiple onboarding rule from ExtremeGuest, select the boxes for each policy then select the trashcan icon.

Splash Templates

Configuration → Splash Template → System Templates

The **Splash Template** 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 perform the following actions:

*   Download a system template and customize it to suit your requirements.
*   Clone a system template.
*   View a summary of networks to splash templates mapping.

To access the ExtremeGuest system templates:

1   Go to **Configuration** → **Splash Templates** from the navigation menu.

The **System Templates** tab displays. To sort the templates alphabetically, select the arrows in the upper right. Select the arrows again to reverse the alphabetic sort.
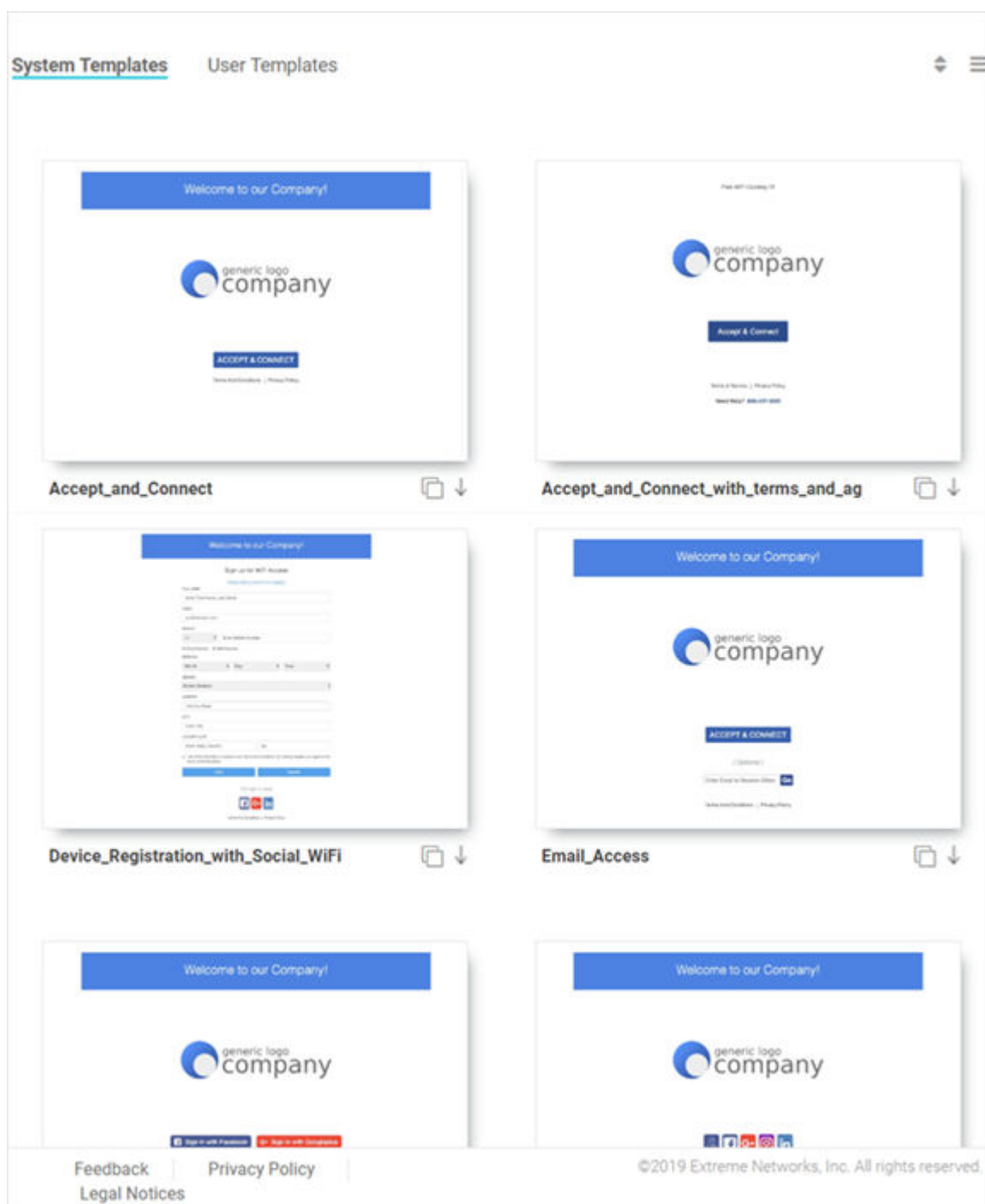

Figure 32: System Templates Screen

Downloading and Customizing Splash Templates

2   Select a pre-made **System Template** from the screen. The available options are:

Accept_and_Connect	Splash template to use for Free WiFi access with a simple Accept & Connect button. Clicking on this button provides internet access and also registers the device with ExtremeGuest.
Accept_and_Connect_with_terms_and_agreement	Splash template to use for Free WiFi access with a simple Accept & Connect button and a hyperlink to view terms and conditions. Clicking on this button provides internet access and also registers the device with ExtremeGuest.
Device_Registration_with_Social_WiFi	Splash template to use for Free WiFi access with a customizable registration form and social sign-in options. Guest user's device is registered along with their registration or social profile details with ExtremeGuest.
Email_Access	Splash template to use for Free WiFi access with an option to capture guest user's **Email Address** or **Mobile Number**. Guest user's device is registered along with their e-mail address or mobile number with ExtremeGuest.
Social_WiFi_with_Facebook_and_GooglePlus	Splash template to use for free WiFi access with Facebook or GooglePlus social sign-in options. Guest user's device is registered along with their social profile details with ExtremeGuest.
Social_WiFi_with_all	Splash template to use for free WiFi access with customizable Facebook/GooglePlus/LinkedIn/Instagram social sign-in options. Guest user's device is registered along with their social profile details with ExtremeGuest.
Sponsored_Guest_Access	Splash template to use for sponsored WiFi access for different category of users, i.e., Employees can self-register their devices, Guests and Vendor's can request the sponsor to approve the WiFi access.
User_Registration_with_Social_WiFi	Splash template to use for free WiFi access with a customizable user registration form and social sign-in options. Guest user registration details or social media profile details are registered with ExtremeGuest. Guest user receives a One-Time-Passcode/Passcode to sign-in to the network.
User_Registration_with_Social_WiFi_and_Forgot_Passcode	Splash template to use for free WiFi access with a customizable user registration form and social sign-in options. Guest user registration details or social media profile details are registered with ExtremeGuest. Guest user receives a One-Time-Passcode/Passcode to sign-in to the network. The template includes a Forgot Passcode button for users to recover forgotten passcodes.

3   Select the ⬇ icon to download the template locally.

4   Edit the company name and logo, where applicable, and use the **User Templates** tab to upload the edited template.

For information on uploading the template, see User Templates on page 75.

Cloning System Templates

5   Select the ⬜ icon, at the bottom, right corner of a template, to clone it.
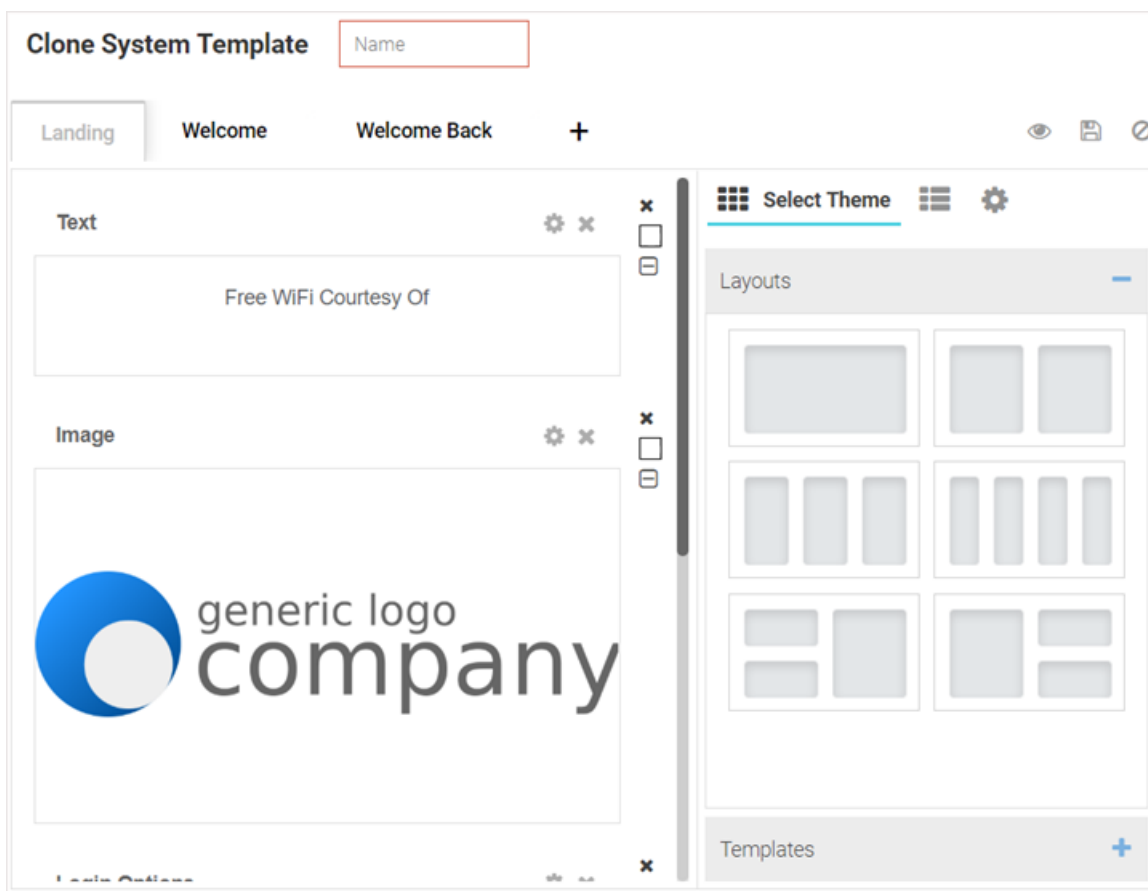
The selected template opens in the edit mode.

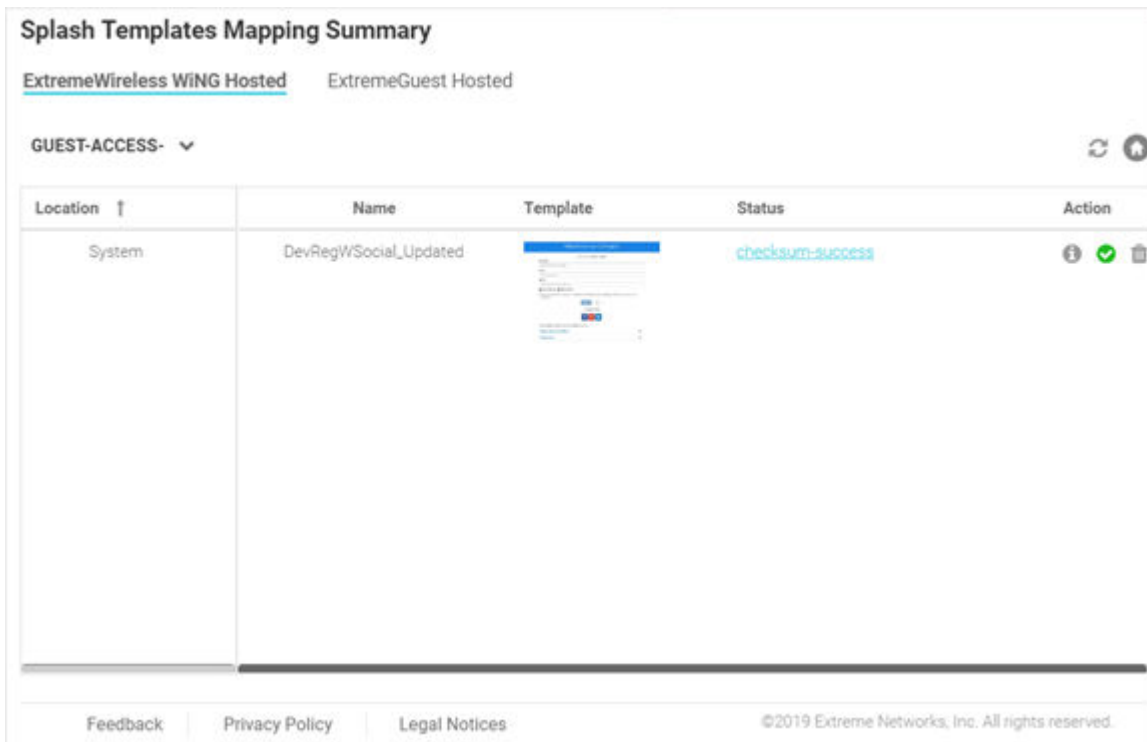**Figure 33: Clone System Template Screen**

6   Provide a `Name` for the cloned template.

7   Customize the template as per your requirement. You can change the page layout, content, logo and the widgets applied to the themes on the screen. Refer to the User Templates on page 75 section for information on editing a splash page.

Viewing Splash Templates to Network Mapping Summary

8   To view a summary of splash template to network mapping, select the ≡ icon.

Select the 🏠 icon to return to the **System Templates** screen.

The **Splash Templates Mapping Summary** screen displays.

Figure 34: Summary View Screen

In the **Summary View**, templates are organized into following two categories:

* **ExtremeWireless WiNG Hosted** - These are templates hosted on the ExtremeWireless WiNG controller.
* **ExtremeGuest Hosted** - These are templates hosted directly on ExtremeGuest.

9   Select the ⌄ icon and select a Network from the drop-down menu displayed. The screen updates to display templates associated with the selected network.

For each template, the **Name** and **Status** is displayed.

10   You can perform the following actions on the **Splash Template Mapping Summary** screen:

Check Template Status	Select the ⓘ icon to display troubleshooting and log information for a template. This information includes network reachability, configuration validity and splash template verification. It also displays log entries for this template. Use the filter field to filter log entries. Download or copy the log using the **Save to Disk** and **Copy to Clipboard** buttons respectively.
Re-Apply	Select the ✔ or ✖ icons to clear and re-apply the splash template to its associated site.
Delete	Select the 🗑 icon to remove the splash template from ExtremeGuest.

User Templates

Configuration → **Splash Template** → **User Templates**.

The **User Templates** screen displays a summary of captive portal splash templates hosted by ExtremeGuest and templates that can be pushed to ExtremeWireless WiNG devices.

These splash templates are of two types: *customized-system templates* and *user-defined templates*. The **User Templates** screen allows you to:

- upload a splash template from your local file system.
- apply splash template to a network.
- edit an existing splash template.
- create a new splash template.
- view splash template to network mapping summary.

Follow the steps below to *upload*, *edit*, *create a splash template* or *get a summary view of existing templates*.

Uploading Splash Templates

1 Select the **User Templates** tab.
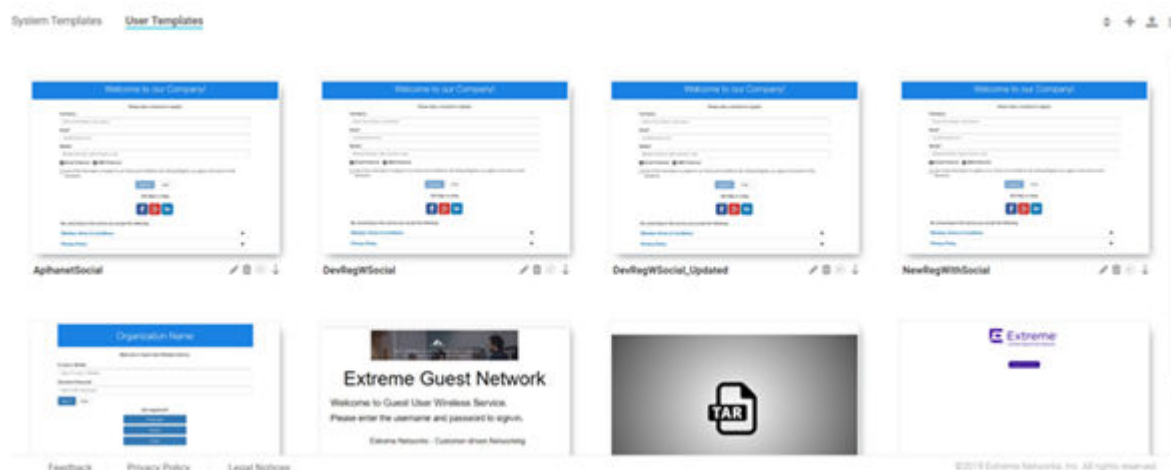
The **User Templates** screen displays.

Figure 35: Splash Template - User Templates Screen

2 Select the ⬆ icon, on the top, right corner of the screen.

The **Upload Template** window opens.

Figure 36: User Templates - Upload Template Screen

3 Enter a name for the template, select **Browse** and navigate your local file system to locate and select the splash template file.

4   Select **Upload**.

The selected splash template is uploaded to ExtremeGuest from your local system.

Applying Splash Templates to Networks

Splash templates displayed on the **User Templates** screen can be applied to networks.

5   Select ⊘ to apply the captive portal template to a network.

> **Note**
>
> The ✅ icon indicates that the template is already applied to a network. The ❎ icon indicates that the template has been changed after it has been applied to a network.

The **Apply** template window opens.

Figure 37: Apply Template to Network Screen

Refer the table below for details:

Host Template in ExtremeGuest Server	Select this option to use ExtremeGuest web-server hosted captive portal pages. When selected, APs within the specified location(s) point to the ExtremeGuest server. The ExtremeGuest server serves captive portal pages to guest users.
Distribute Template	Select this option to distribute the ExtremeGuest web server hosted captive portal pages to APs within the specified location(s). The APs directly serve captive portal pages to guest users.
Location	Map the captive portal page with a location(s). When mapped, the APs within location(s) (either directly or through the ExtremeGuest web server) serve the captive portal pages to guest users. Expand the **Location** tree to view the locations (RF Domains) defined within your network. Drill-down to the last node and select a site. Or, select anyone of the upper node (country, state, region or campus) to apply the captive portal pages to multiple sites.
Network	Click the ⌄ icon to view available networks. Select the **Network** to which this captive portal provides access. When selected, guest users attempting access to the specified network are required to authenticate with the captive portal and are allowed access only if successfully authenticated.
Apply	Select to activate the captive portal template. **Note:** The **Apply** button is enabled only if the mode of distribution, location and network settings are specified.

6 Select ↓ to download a template locally.

7 Select 🗑 to delete a template.

8 Select ✎ to edit a template.

> **Note**
> If editing a template, go to Creating/Editing Splash Templates for more information.

Viewing Splash Templates to Network Mapping Summary

9 To view a summary of splash template to network mappings, select the ☰ icon.

> **Note**
> For information about this screen and its content, see Viewing a Summary of Available Splash Templates.

10 To return to the default view, select the 🏠 icon.

Creating/Editing Splash Templates

The **User Templates** screen provides a robust, easy-to-use splash template builder wizard. Use the wizard's 'drag & drop' elements, color, text and language customization tools and logo upload options to create your branded captive portal web pages.

11 To create a new splash template, select the ➕ icon.

To edit an existing template, select the ✎ icon below the template. The template opens in the edit mode.

The **Create Splash Template** screen opens.

Figure 38: Create Splash Template Screen

12 Enter a name for the splash template. Provide a name that uniquely identifies its purpose.

13 Select the type of web pages your users will be served.

> **Note**
> Below the **Name** field is the splash template page tabs. By default the following three tabs are displayed: **Landing**, **Welcome** and **Failure**.

14 To add pages, select ✚ and select the **Login**, **No Service** or **Welcome Back** page.

> **Note**
> Barring the **Landing** page, you can remove all other splash template pages. To remove a page, hover the cursor on the tab and select the ✖ icon.

15 Select a splash template tab to add or edit the page contents.

> **Note**
> The add/edit page screen is divided into a bigger, main pane and a right-hand panel. Each splash page type has its own collection of *themes*, *widgets* and *page settings* options that are displayed in the right-hand panel. These options are the building components that you will use to build your page content.

16 Select **Select Theme**.

Themes divide the page into sections/cells, which are place holders for widgets. To add widgets, you need to first place themes on the splash page. Themes are grouped into `Layouts` and `Templates`. Perform one or both of the following tasks:

- Expand the **Layouts** section. You have *six* layout themes to select. Each layout theme has one or more cells. Each cell can contain only one widget. Drag and drop one or more layout on to the main splash template pane.
- Expand the **Templates** section. Templates are layouts with pre-filled text and/or image widgets. You have *five* template themes to select. Drag and drop one or more template on to the main splash template pane.

> **Note**
> When creating the page layout, take into consideration the various elements (text, image, buttons, login options, etc.) that you plan at add to the page.

The **Select Theme** menu displays.
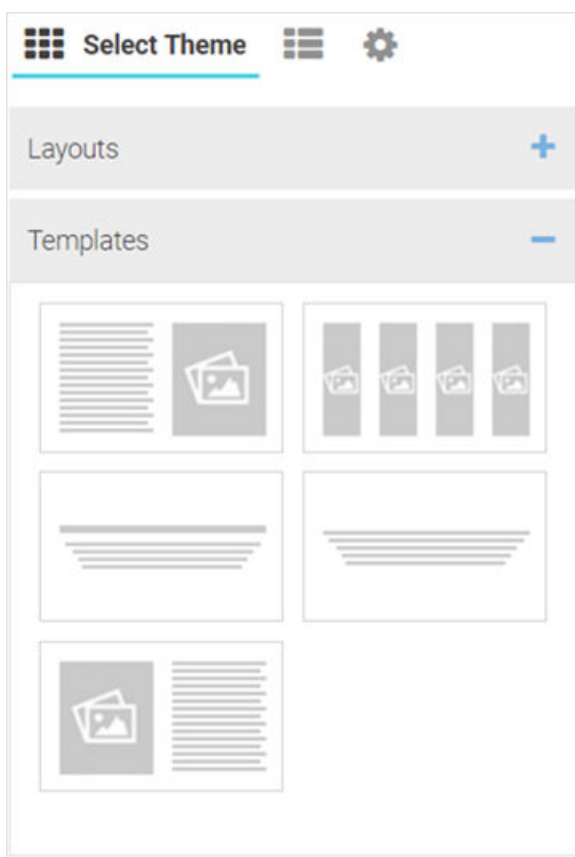
Figure 39: Create Splash Template - Select Theme Options

> **Note**
> You can use multiple layouts or templates or a combination of layouts and templates to divide the page into sections. The height of these sections can be adjusted by dragging the bottom margins.

17 Once the themes are added, you can perform following actions:

a Change background color of a layout or template. Select the ☐ icon to open the built-in color palette. Select the background color and select **OK** .
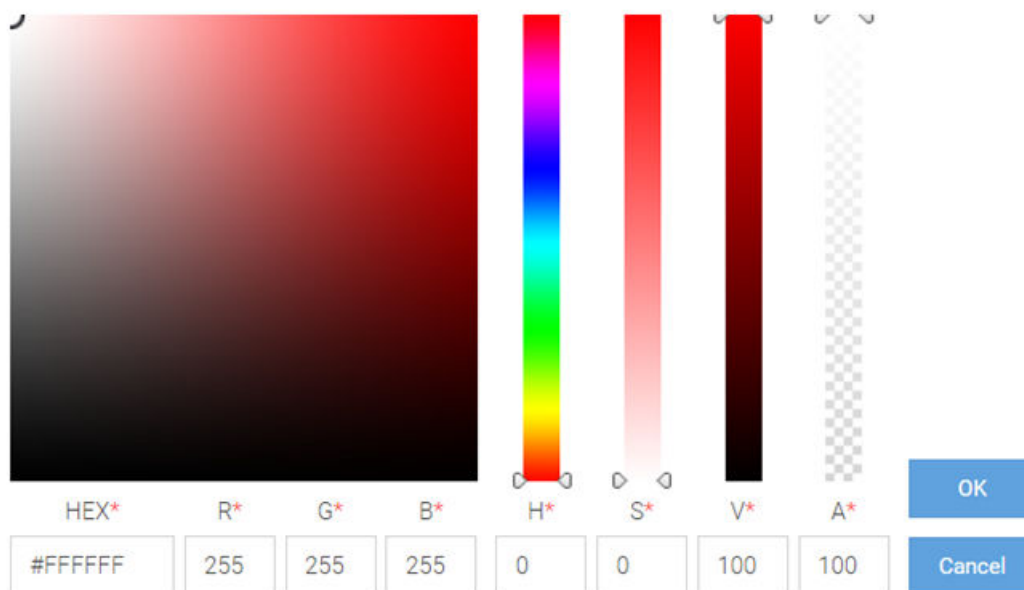
The **Color Palette** displays.

Figure 40: Create Splash Template - Built-in Color Palette

b Reset background color. Select the ⊟ icon to reset background color to transparent.

c Remove a layout or template. Select the ✖ icon to remove the layout or template.

18 Select **Select Widget**.

The **Select Widget** menu displays.
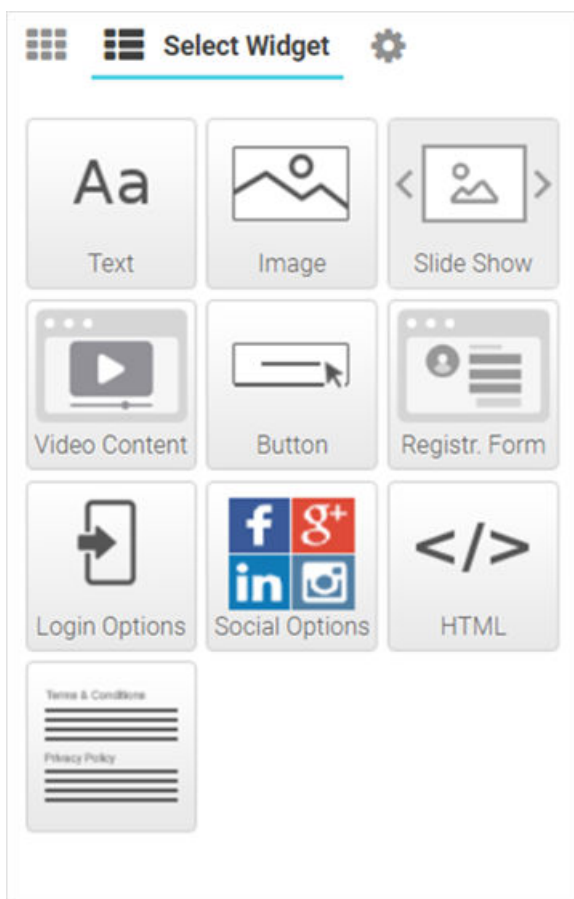
Figure 41: Create Splash Template - Select Widget Options

19 Drag and drop a widget into the layouts/templates on the splash page. Following are the available widget types:

Text Widget	Adds text to the page.
Image Widget	Adds image to the page.
HTML Widget	Adds HTML content to the page. Use this widget to design your web page from scratch, without using any of the system-provided themes or widgets.
Slide Show Widget	Adds a slide-show component to the page, using the images available in the gallery.
Video Content Widget	Adds video to the page.
Button Widget	Adds any button with a per-defined hyperlink to a page.
Registration Form Widget	Adds a registration form to the page. Users are served an internal (or) externally hosted registration page where they have to complete the registration process if not previously registered.
Login Options Widget	Adds buttons that enable "Accept and Connect" action or go to "Login" page action

Social Options Widget	Adds social media sign-in options.
Terms and Conditions Widget	Adds "Terms and Conditions" and "Privacy Policy" hyperlinks with pop-up texts.
Login Form Widget	Adds a simple login form with "Email or Mobile" and "Received Passcode" fields.
WiFi Logout Widget	Adds button that enables the user to logout from connected WiFi.
Redirect Widget	Adds a redirection URL to the web page.

Note

Each of the above widgets has two icon tools on the top, right corner of the widget bar.

Use the ⚙ icon to edit the widget settings, use the ✖ icon to remove the widget.

Editing Text Widget

Back to Widget Options Table

Use this widget to insert content/text in the web page. The ExtremeGuest text widget provides a pop-up, HTML editor to add text.

20 Select the ⚙ icon to open the HTML text editor.

The **Text widget - HTML Editor** window displays.
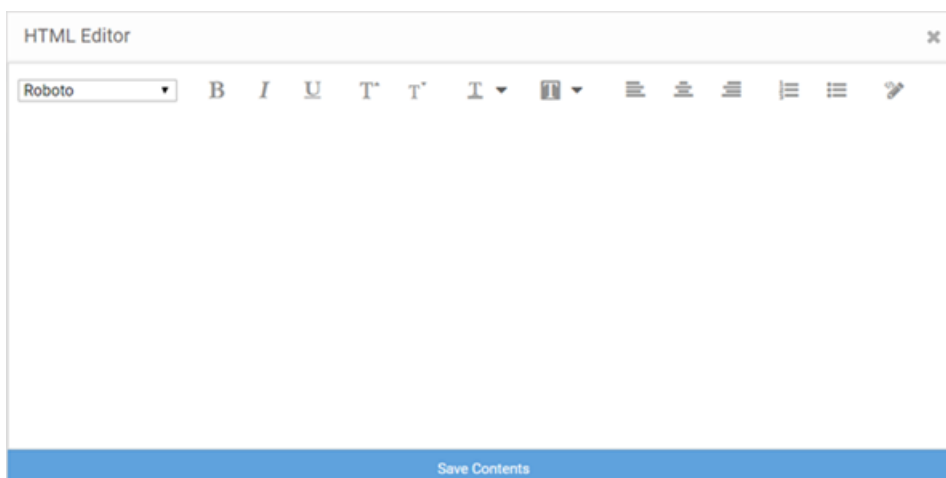
Figure 42: Create Splash Template - Text Widget - HTML Editor

21 Enter your text and use the HTML editor tools to set the font style, size, color and text alignment.

22 Use the ✎ tool to preview the content. Make changes if necessary.

23 Select **Save Contents** to save and exit the editor.

Editing Image Widget

Back to Widget Options Table

Use this widget to insert images in the splash page.

Note
The **Image** widget not available for the 'Failure' web page.

24 Select the ⚙ icon to open the Image Settings panel.

The **Image Widget Settings** panel displays.

Upload Image	Select **Browse** and navigate your local file system to locate and select the image file. Select **Upload**. The image is uploaded to the **Gallery** .
	Note: The following image file types are supported: `.jpg`, `.jpeg` and `.png`.
Alignment	Use the alignment buttons to set the alignment of the image within the layout cell.
Width and Height	Use these options to change the image size. By default, an image auto-resizes to fit in the layout cell.
Gallery	The gallery displays user-uploaded images. Drag and drop an image into the image widget. Select ✖ icon to remove an image.

Editing HTML Widget

Back to Widget Options Table

The HTML widget allows you to design the content of the selected section of the web page using HTML or JavaScript. Use this widget, to create the content of a specific section of the web page from scratch instead of using the system-provided widget content.

> **Note**
> Both HTML and JavaScript is supported.

25 Select the ⚙ icon to open the HTML editor.

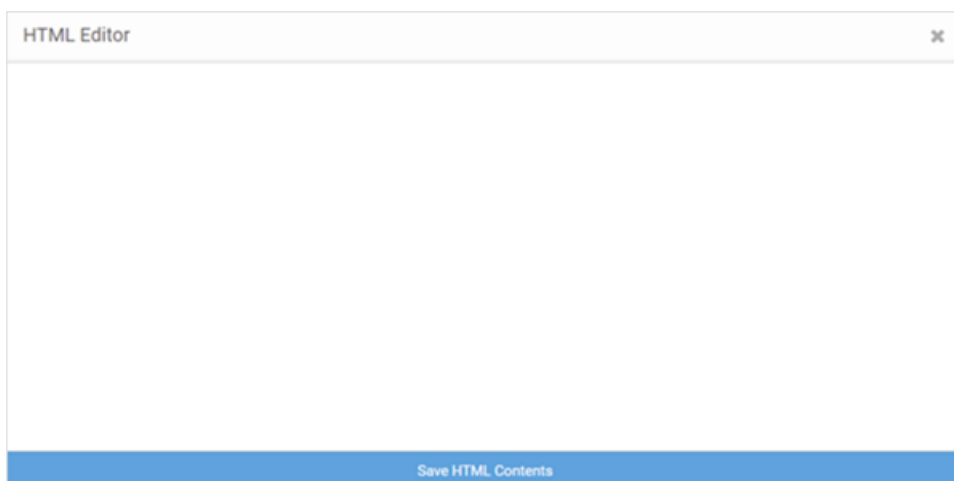The **HTML Widget - HTML Editor** panel displays.

Figure 43: Create Splash Template - HTML Widget - HTML Editor

26 Enter your HTML code or JavaScript and select **Save HTML Contents** to save and exit the editor.

Editing Slide Show Widget

Back to Widget Options Table

Image slide-shows are an excellent means of enhancing user engagement and experience. Use this widget to add slide shows of images to the splash pages.

27 Select the ⚙ icon to open the Slide Show Settings panel.

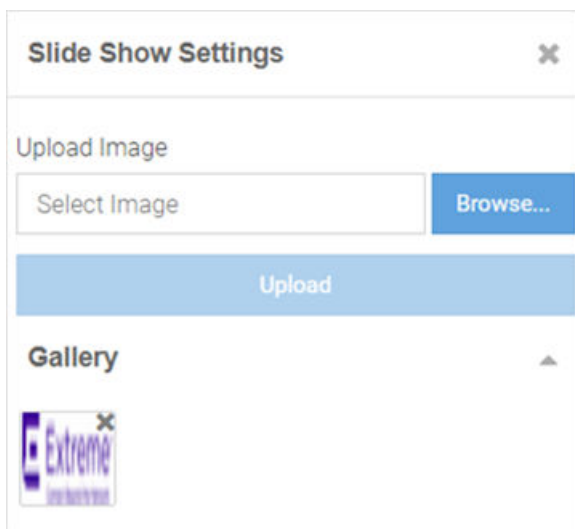The **Slide Show Settings** panel displays.

Figure 44: Create Splash Template - Slide Show Settings Panel

Drag and drop images from the **Gallery** to create a slide show. You can upload and delete images from the gallery as described in Step 20: Editing Image Widget.

Editing Video Content Widget

Back to Widget Options Table

Videos enhance user engagement and experience. Make your web pages informative and attractive by adding didoes to your web pages.

28 Select the ⚙ icon to open the Video Settings panel.

The **Video Settings** panel displays.
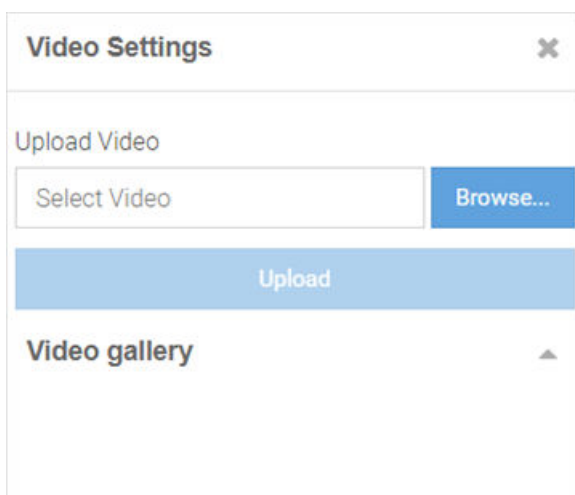
Figure 45: Create Splash Template - Video Settings Panel

The **Video Settings** panel has the **`Upload Video`** and **`Video gallery`** options, similar to the **Image Settings** panel. Upload your video to the gallery, then drag and drop the video file into the widget.

Note

This widget uses HTML5 Video tag. The following image file types are supported: **`.mp4`**, **`.ogv`** and **`.webm`**. To ensure cross-browser compatibility, upload your video file in all three formats. For example, save the video 'test' as 'test.mp4', test.ogv' and 'test.webm'. Upload all three files to the video gallery at the same time.

Editing Button Widget

Back to Widget Options Table

Button Widget is a simple and effective tool for inserting a button with hyper link to a web page. Use this widget to create a button that directs users to a pre-defined URL.

29 Select the ⚙ icon to open the Button Settings panel.

The **Button Settings** panel displays.

Figure 46: Create Splash Template - Button Settings Panel

The **Button Settings** panel has the following fields:

Url field	Use this widget to insert a button that is hyperlinked to a pre-defined page. In the URL field, enter the URL of the page the user is directed to on clicking the button.
Text field	Enter the text displayed on the button.
Font Size (in px)	Set the font size in pixels.
Border Radius (in px)	Set the button's border radius in pixels.
Size	Use the slider to set the button size.
Alignment	Set the button's alignment within the layout cell.
Text	Use this tab to set the color of the text appearing on the button.
Button	Use this tab to set the color of the button itself.

Editing Registration Form Widget

Use the Registration Form widget to insert a form where guest users enter specific information in order to register with your captive portal.
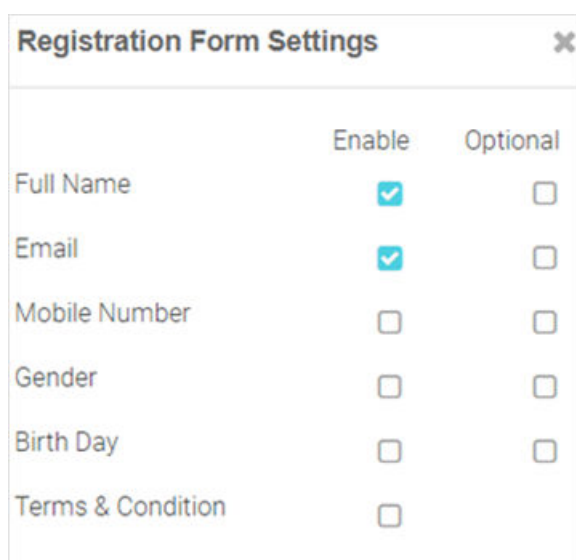
> **Note**
>
> The **Registration Form** widget is available only for the '*Landing*' web page.

30 Select the ⚙ icon to open the Registration Form Settings panel.

The **Registration Form Settings** panel displays.

Figure 47: Create Splash Template - Registration Form Settings Panel

Insert a registration form for first-time users. First-time users are required to enter information in the fields displayed on the page. The available field options are: **Full Name**, **Email**, **Mobile Number**, **Gender**, **Birth Day**, **Terms & Conditions**. Each field has an associated **Enable** and

Configuration

Optional checkbox. Select **Enable** to add the field to the form. Select **Optional** to make the field optional.

> **Note**
> The **Terms & Conditions** option adds the Terms & Conditions Widget at the end of the page.

Editing Login Options Widget

Back to Widget Options Table

Use the Login Options Widget if you wish to enforce a 'Accept and Connect' or go to 'Login' page action.

31 Select the ⚙ icon to open the Login Options Settings panel.

The **Login Options Settings** panel displays.

Figure 48: Create Splash Template - Login Options Settings Panel

The **Login Options Settings** panel has the following fields:

Login Type	Select one of the following login type action: • Accept and Connect - redirects user to the accept and connect page. • Login - redirects user to the login page.
Alignment	Set the alignment of the button/link within the layout cell.
Button	Select to insert a button.
Link	Select to insert a hyperlink.
Text	If selecting the 'Button' option, specify the text on the button. If selecting the 'Link' option, specify the hyperlink text.
Font Size (in px)	Set the font size in pixels.
Border Radius (in px)	Set the button's border radius in pixels.
Text/Button	Selecting the 'Button' option, enables these tabs. Use these tabs to set the color of the text on the button and the color of the button itself.
Font Size/Font Color	Selecting the 'Link' option, enables these tabs. Use these tabs to set the font size and color of the hyperlink text.

Editing Social Options Widget

Back to Widget Options Table

Use this widget to add user authentication through social media applications. Guest users can use their **Facebook**, **Instagram**, **Google** or **LinkedIn** account credentials to authenticate and access the internet.

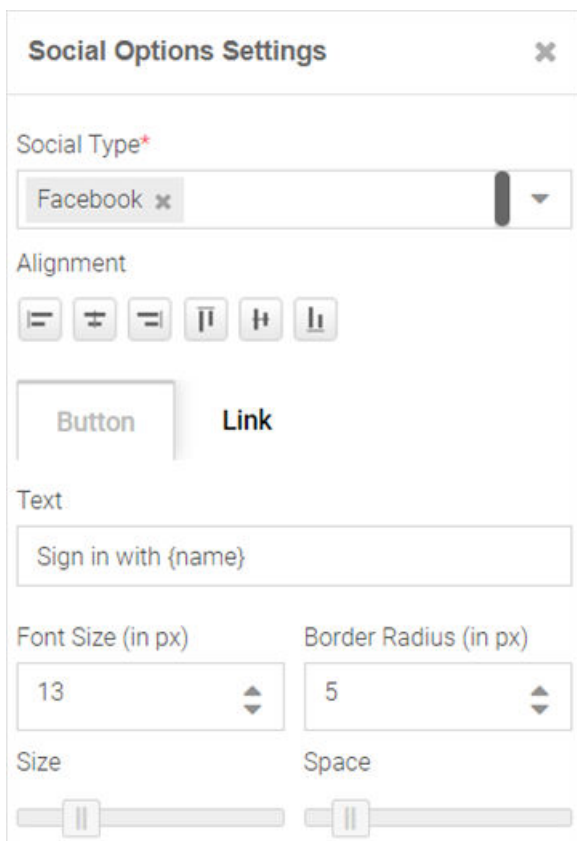32 Select the ⚙ icon to open the Social Options Settings panel.

> **Note**
> The **Social Options Settings** widget is available only for the '*Landing*' and '*Login*' web pages.

> **Note**
> Ensure that the social media is added as an authenticator on the portal. For information on adding social media API keys, see Social on page 97.

The **Social Options Settings** panel.

Figure 49: Create Splash Template - Social Options Settings Panel

Social Type	Use this drop-down menu to select the social media sign-in options. **Note:** Available options are: **Facebook**, **Instagram**, **Google** or **LinkedIn**. You can add more than one social-media login option.
Button	Select to insert a button.
Link	Select to insert a link.
Alignment	Set the alignment of the button/link within the layout cell.
Text	Enter the social media name in the 'Sign in with {name}' field. For example: Sign in with Facebook
Font Size (in px)	Set the text font size.
Border Radius (in px)	Set the button's border radius in pixels.
Size	Use the slider to set the button size.
Space	Use the slider to set the space between buttons.

Editing Terms and Conditions Widget

Back to Widget Options Table

Use this widget to insert 'Terms and Conditions' and 'Privacy Policy' hyperlinks with pop-up texts.

> **Note**
> The **Terms and Conditions** widget is available only for the 'Landing' web page.

33 Select the ⚙ icon to open the Terms and Conditions Settings panel.

The **Terms and Conditions Settings** panel displays.

Figure 50: Create Splash Template - Terms And Conditions Settings Panel

Terms And Conditions Text	Select the **Edit Text** button to open the HTML editor. Enter the terms and conditions that the captive portal user views on clicking the Terms And Conditions link.
Privacy Policy	Select the **Edit Text** button to open the HTML editor. Enter your company's privacy policies that the captive portal user views on clicking the Privacy Policy link.
Alignment	Set the alignment of the links within the layout cell.
Font Color	Set the link text font color.
Font Size (in px)	Set the link text font size in pixels.
Separator Text	Set the separator between the two links.
Separator Space	Use the slider to set the space between the separator and the links on either side.

Editing Login Form Widget

Back to Widget Options Table

Use this option to insert a simple login form. A login form is an easy and simple mode of authenticating already registered guest users.

34 Select the ⚙ icon to open the Login Form Settings panel.
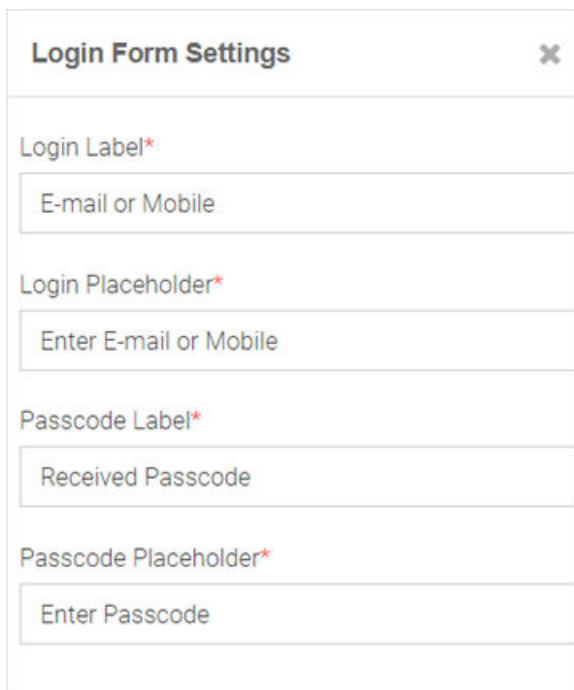
The **Login Form Settings** panel displays.

Figure 51: Create Splash Template - Login Form Settings Panel

The login form allows guest users to enter their username and passcode registered with the ExtremeGuest database. The form has two fields. Each of these fields has two parameters: The *field label* and the *text* displayed within the field placeholder. Customize the field labels and the prompt-text displayed within the placeholder.
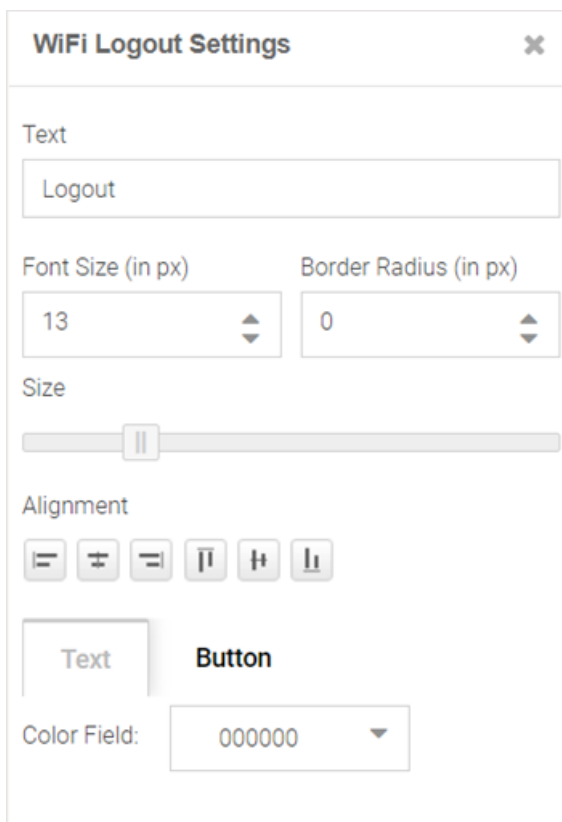
Editing WiFi Logout Widget

Back to Widget Options Table

Use this option to insert a WiFi-Logout button. This option allows successfully authenticated guest users to logout from the connected WiFi.

35 Select the ⚙ icon to open the WiFi Logout Settings panel.

The **WiFi Logout Settings** panel displays.

Figure 52: Create Splash Template - Logout Button Settings Panel

Use the WiFi Logout Settings panel to customize the logout button as per your requirement. This panel provides settings similar to the *Button Settings* panel with one exception, there is no URL field in the WiFi Logout Settings panel. For more information, click here.

Editing Redirect Widget

Back to Widget Options Table

Use this option to redirect the guest user to another web page. Since the redirect widget takes the user to another page, you cannot use it in combination with other widgets. If your page layout has space for more than one widget, you will be prompted to provide permission to delete other widgets on the web page.

> **Note**
> The **Redirect** widget is available only for the '*Welcome*', '*Failure*' and '*No Service*' web pages.

36 In the **Edit Redirect URL** box, specify the URL of the web page to which your users are to be redirected.

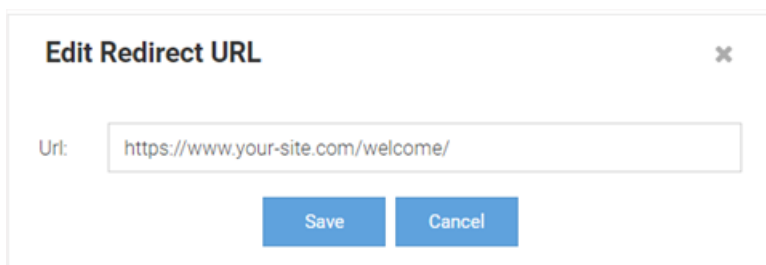The **Edit Redirect URL** window displays.

Figure 53: Create Splash Template - Edit Redirect URL Box

37 Select **Page Settings**. Use the page settings fields to either upload a background image or select a background color for the remainder of the web page that lies outside of the Theme or Widget pane.
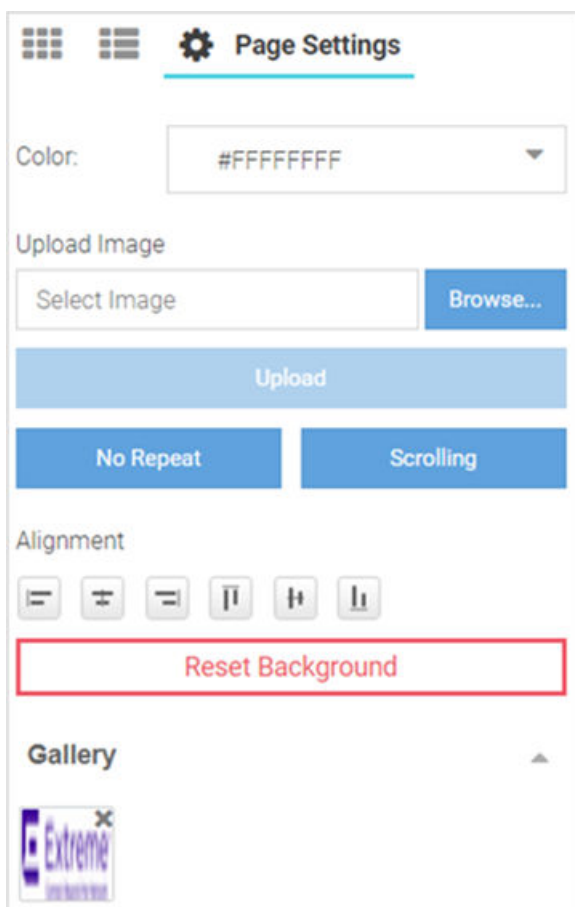
The **Page Settings** window displays.

Figure 54: Create Splash Template - Select Page Settings Options

Color   Use the built-in color palette to select the background color of the splash template. This background color can be viewed in the Preview mode.

Upload Image	Use this option to upload and insert a background image. Select **Browse** and navigate your local file system to locate and select the image. Select **Upload**. A thumbnail of the uploaded image is added to the Gallery section. You can upload multiple images, however, only one image can be used as the background image at a time.
No Repeat/ Repeat/Horizontal Repeat/Vertical Repeat	This button changes the background image repeat status. If the image is small and does not cover the entire page, you can repeat the image as multiple tiles in the background. `No Repeat` prevents the image from displaying as tiles. `Repeat` makes the image repeat horizontally and vertically. `Horizontal Repeat` makes the image repeat horizontally. `Vertical Repeat` makes the image repeat vertically.
Scrolling/Fixed	This button changes the background image scrolling state. If the page is long and scrolls, you can set the image to scroll along with the page content by setting the image state to `Scrolling`. In the `Fixed` state, the background image remains still while the content scrolls.
Alignment	These buttons align the image horizontally (left, center and right) and vertically (top, middle and bottom).
Reset Background	This button removes background image and color.

38 Select the preview 👁 icon to review your page design.
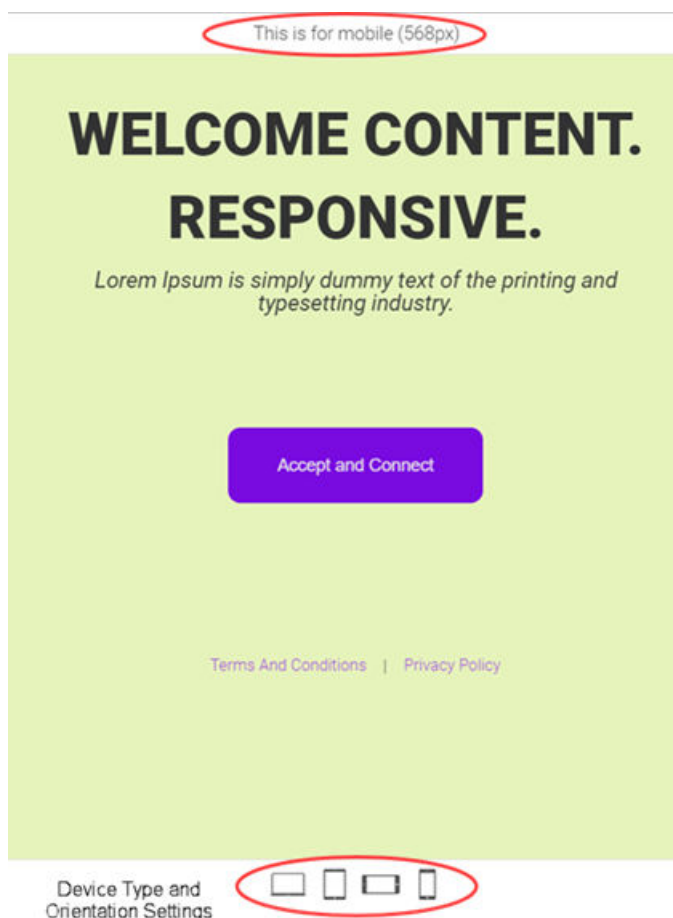
The splash page displays in the preview mode.

Figure 55: Create Splash Template - Device Type and Orientation Settings

Use the device orientation icons at the bottom of the screen to preview the splash page as seen on different devices and orientation. The following viewing options are available for:

- Large screen devices like laptops (960 px wide)
- Tablets and other wide screen devices (768 px wide)
- Mobile devices with landscape orientation (568 px wide)
- Mobile devices with portrait orientation (320 px wide)

39 Exit the preview mode. Make changes to the page design if needed.

40 Select **Save** to save and exit.

41 Select **Cancel** to exit without saving.

Social

Configuration → Social

Figure 56: Configuration Social Media Login Configuration Screen

The **Social** screens provides configuration for social media authentication on the following platforms:

- Facebook
- Google Plus
- LinkedIn
- Instagram

Facebook Configuration

Configuration → Social → Facebook

To add Facebook as an authenticator:

1   Go to **Configuration → Social** from the navigation menu.

The **Social** screen displays by default.

2   Click the arrow to expand the **Facebook** configuration.

3   Enter the Facebook **ID**.

4   Enter the Facebook **Secret**.

5   For more information about creating a Facebook **ID** and **Secret** click the **How to create Facebook id and secret** link in the user interface.

6   Select **Save** to save changes to the Facebook **ID** and **Secret**.

Google Plus Configuration

Configuration → Social → Google Plus

To add Google Plus as an authenticator:

1   Go to **Configuration → Social** from the navigation menu.

The **Social** screen displays by default.

2   Click the arrow to expand the **Google Plus** configuration.

3   Enter the Google Plus **ID**.

4   Enter the Google Plus **Secret**.

5   For more information about creating a Google Plus **ID** and **Secret** click the **How to create Google+ id and secret** link in the user interface.

6   Select **Save** to save changes to the Google Plus **ID** and **Secret**.

LinkedIn Configuration

Configuration → Social → LinkedIn

To add LinkedIn as an authenticator:

1   Go to **Configuration → Social** from the navigation menu.

The **Social** screen displays by default.

2   Click the arrow to expand the **LinkedIn** configuration.

3   Enter the LinkedIn **ID**.

4   Enter the LinkedIn **Secret**.

5 For more information about creating a LinkedIn **ID** and **Secret** click the **How to create Linkedin id and secret** link in the user interface.

6 Select **Save** to save changes to the LinkedIn **ID** and **Secret**.

Instagram Configuration

Configuration → Social → Instagram

To add Instagram as an authenticator:

1 Go to **Configuration → Social** from the navigation menu.

The **Social** screen displays by default.

2 Click the arrow to expand the **Instagram** configuration.

3 Enter the Instagram **ID**.

4 Enter the Instagram **Secret**.

5 For more information about creating a Instagram **ID** and **Secret** click the **How to create Instagram id and secret** link in the user interface.

6 Select **Save** to save changes to the Instagram **ID** and **Secret**.

Vouchers

Configuration → Vouchers

Vouchers are used to authenticate users on a hotspot network. ExtremeGuest can generate individual user and end-point vouchers or bulk generate up to 20,000 vouchers at a time.

For detailed voucher configuration see:

Create Users

Configuration → Vouchers → Create Users

User vouchers can be created individually or in bulk.

To create an individual user voucher:

1 Go to **Configuration** → **Vouchers** from the main menu.

The **Users** tab displays by default.

Figure 57: Create Users Screen

2 Configure the following details for each user voucher:

First Name	Optionally, enter the first name for the voucher user.
Last Name	Optionally enter the surname for the voucher user.
Email	Enter an email address for the voucher user. To set the email address as the username and password select **Use as username/password**. This will remove the **Username** and **Password** fields from the form.
Telephone	Enter a telephone number for the voucher user. To set the telephone number as the username and password select **Use as username/password**. This will remove the **Username** and **Password** fields from the form.
Organization	Optionally, enter an organization to associate the voucher user with. This can used to specify a company or organizational group for the voucher user.
Reason	Optionally, enter a reason why the voucher user was created. This can be helpful when there are multiple administrators adding users.

Username	Enter a login username for the voucher user.

> **Note**
> If **Use as username/password** is selected in the **Email** or **Telephone** fields, the **Username** field is not present.

Password	Enter a login password for the voucher user.

> **Note**
> If **Use as username/password** is selected in the **Email** or **Telephone** fields, the **Password** field is not present.

User Group	Optionally, select a user group from the list to associate the voucher user to that group.
Location	Select a location from the list to associate the voucher user with that location.
Start Date / Time	Use the calendar and pull-down menu to specify the starting date and time to activate the voucher user.
Expiry Date / Time	Use the calendar and pull-down menu to specify the ending date and time that the voucher user will be deactivated.

3   When all mandatory fields have been completed, select **Create** to complete voucher creation.

To discard any changes made to the form select **Clear**.

Create End Points

Configuration → Vouchers → Create End Points

ExtremeGuest allows network end points to be added to the network using vouchers.

To create an end point voucher:

1   Go to **Configuration → Vouchers** from the main menu.

The **Users** tab displays by default.

2 Select the **End Points** tab.

The **Create End Points** window displays.

Figure 58: Create End Points Screen

3 Configure the following details for each end point voucher:

MAC Address	Enter the MAC address for the end point. The MAC address should be added in the following format: *AA-BB-CC-DD-EE-FF*
Host Name	Optionally, enter a hostname to associate with the network end point.
User Group	Select a user group from the list to associate it to the network end point.
Network	Select a network from the list to associate it to the network end point.
Location	Select a location from the list to associate it to the network end point.
Expiry Time	Use the calendar to specify the ending date and time that the end point will be deactivated.

4 When all mandatory fields have been completed, select **Create** to complete voucher creation.

To discard any changes made to the form select **Clear**.

Create Bulk Vouchers

Configuration → Vouchers → Bulk Vouchers

To create a bulk voucher:

1   Go to **Configuration** → **Vouchers** from the main menu.

The **Users** tab displays by default.

2   Select the **Bulk Vouchers** tab.

The **Create Bulk Vouchers** window displays.

Figure 59: Create Bulk Vouchers Screen

3   Configure the following details for bulk voucher creation:

User Group	Select a user group from the list to associate it to the group of bulk created vouchers.
Number of Vouchers	Enter a value or user the spinner control to specify the number of vouchers to create. ExtremeGuest supports creating between 2 and 20,000 vouchers at a time.
Description	Optionally, enter a description that will apply to the group of bulk vouchers.
Location	Select a location from the list to associate it to the group of bulk vouchers.
Start Date / Time	Use the calendar and pull-down menu to specify the starting date and time to activate the group of bulk created vouchers.
Expiry Date / Time	Use the calendar and pull-down menu to specify the ending date and time that the bulk created vouchers will be deactivated.

4   When all mandatory fields have been completed, select **Create** to complete bulk voucher creation.

To discard any changes made to the form select **Clear**.

6 Analyze

The **Analyze** screen provides the following sub-menus:

The Analyze screens provide key-metrics about users and end points. It also provides access to reports.

Analyze End Points

Analyze → End Points
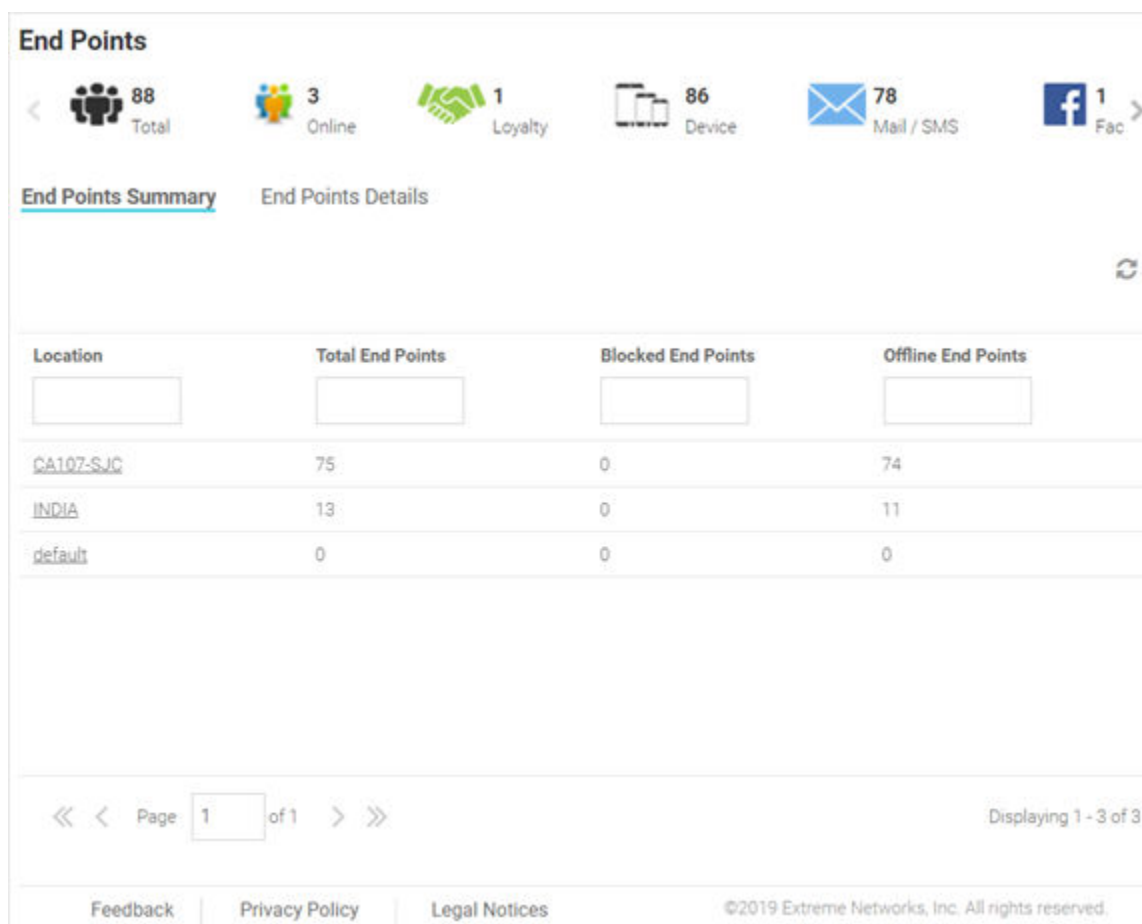
Figure 60: End Points Summary Screen

The **End Points** screen provides a system-wide summary of all end-points as well as detailed information for each end-point. End points are the guest users/devices registered with and authenticated by ExtremeGuest captive portal server. This includes users logged in via e-mail/sms, social-media login, loyalty card holders, devices, etc.

End Point Summary

The **End Point Summary** screen displays the following information:

Location	The name of the location/site (RF Domain).
Total End Points	The total number of end points per location.
Blocked End Points	The total number of blocked end points per location.
Offline End Points	The total number of end points per location that are currently offline.

End Point Details

The **End Point Details** screen displays the following online users information:

MAC	The **MAC** column displays the MAC (Media Access Control) Address associated with each end point.

Host Name   The **Host Name** column displays the Host Name associated with each end point.

Device Type   The **Device Type** column displays the device model associated with each end point.

OS   The **OS** column displays the operating system used by each end point.

Status   The **Status** column displays the authentication status of each end point.

Last Login   The **Last Login** column displays the full date and time when the end point last authenticated on the network.

Action   From the **Action** column perform one of the following actions on an end point. Select **Block** to stop an end point from passing traffic on the network. Select **Disconnect** to terminate an end point's session on the network. Select **Delete** to remove an end point from the database. If the end point connects again they will be treated as new end point.

For information on how to filter end-points, see Filtering End Points Results on page 107.

Filtering End Points Results
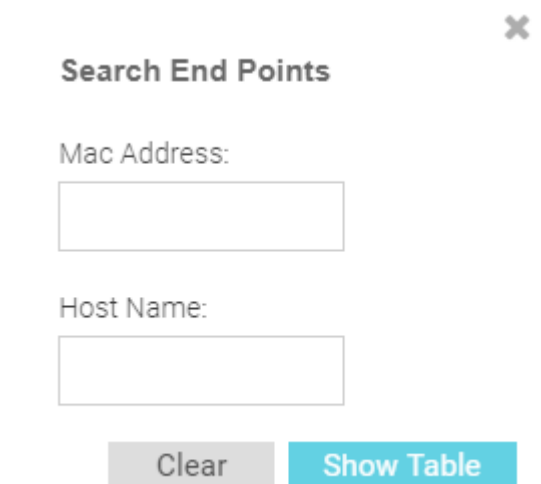
Analyze → End Points → Search End Point

Filters provide the ability to distill user data based on specific criteria.

To filter end point results:

1   Go to **Analyze → End Points** from the navigation menu.
2   Select the search icon in the upper right of the table.

The **Search End Points** window.

Figure 61: Search End Points

3   Configure any one or more of the following filter options:

MAC Address   Enter a MAC Address or portion of a MAC address to filter users with MAC address matching the specified string.

Host Name   Enter a Host Name or portion of a Host Name address to filter users with host name matching the specified string.

4   After specifying the filter options, select **Show Table**to display the filtered results.

Select **Clear** to remove any text entered into the search fields.

Reports

Analyze → Reports

In the report section, users can select schedule reports, view generated reports and manage reports. Create reports in the Manage Reports section. There are three different types of reports that can be created:

Users	The Users report is a consolidated report of the following:

	Social	Bar chart displaying users online and total users categorized by social networking site.
	Age	A pie chart displaying users classified by age group and percentage.
	Gender	Pie chart displaying the percentage of users based on gender.
	User Trend	Graph displaying total users, returning users and new users plotted against each week and number users visited.
	Visitors	Pie chart displaying new visitors vs returning users.

Devices	The Devices report is a consolidated report of the following:

	Device	Pie chart displaying the percentage of devices by type for connected clients.
	Operating System	Pie chart displaying the percentage of operating system by type for connected clients.
	Device Browser	Pie chart to displaying the percentage for each browser type used by registered clients.

Guest Visit History	This reports displays all users' information based on time frame parameter and displays them in a list.

Generated Reports

Analyze → Reports → Generated Reports

Figure 62: Generated Reports Screen

The **Generated Reports** screen provides the following information about existing reports that have been run:

Report	Displays the report name for each existing generated report.
Type	Displays the report type for each generated report. The field at the top of this column allows filtering the **Type** by keyword.
User	Displays the user that generated each report. The field at the top of this column allows filtering the **User** by keyword.
Generated At	Displays the ending date and time that each report was completed.
Action	Select the **PDF** icon to download a PDF copy of the generated report. Select the 🗑 icon to delete a generated report.

Manage Reports

Analyze → Reports → Manage Reports

Figure 63: Manage Reports Screen

The **Manage Reports** screen enables adding and removing of reports and provides the following information about existing reports that have been run:

Report   Displays the report name for each existing generated report.

Type   Displays the report type for each generated report. The field at the top of this column allows filtering the **Type** by keyword.

User   Displays the user that generated each report. The field at the top of this column allows filtering the **User** by keyword.

Start Date Displays the starting date and time that each report was initiated.

End Date   Displays the ending date and time that each report was completed.

Frequency   Displays the interval that each report is scheduled to run.

Action   Select the **Trashcan** icon to delete a generated report.

Adding a Report

Analyze → Reports → Manage Reports → Add Report

To create a new report:

1 Go to **Analyze → Reports → Manage Reports** from the navigation menu.

2 Click the ➕ icon.

The **Add Report** window displays.

Figure 64: Add Report Screen

3 Configure the following information to create a new report:

Report Name	Specify a unique name for the new report. This setting is mandatory.
Report Type	Select the report type. There are five different types of reports that can be created:

Users   The Users report is a consolidated report of the following:

Social	Bar chart displaying users online and total users categorized by social networking site.
Age	A pie chart displaying users classified by age group and percentage.
Gender	Pie chart displaying the percentage of users based on gender.
User Trend	Graph displaying total users, returning users and new users plotted against each week and number users visited.
Visitors	Pie chart displaying new visitors vs returning users.

Devices   The Users report is a consolidated report of the following:

Device	Pie chart displaying the percentage of traffic generated by the device's name.
Operating System	Pie chart displaying the percentage of traffic generated by the user's operating system.
Device Browser	Pie chart to displaying the percentage of traffic generated sorted by the user's browser.

Guest Visit History   This reports displays all users' information based on time frame parameter and displays them in a list.

Guest Visit History Summary	This reports displays a summary of guest users' information based on time frame parameter and displays them in a list.
Dashboard Report	This report provides an overview of widgets used in the specified user-created dashboard. If you have customized dashboards saved on ExtremeGuest, generate a dashboard report displaying the widgets and the data in them for a dashboard. This report is generated in the PDF format.

```
Dashboard Report          ∨

Users

Devices

Guest Visit History

Guest Visit History Summary

Dashboard Report
```
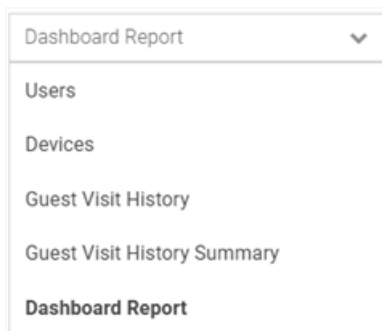
4 After selecting the **Report Type**, specify the following parameters determining the other aspects of the report:

Scope	Use the **Scope** menu to navigate the system tree and select which sites to include in the report. To include all site, select **System**.
Period	Select the time period for the report to include. Available options are: • `Last Hour` • `Last Day` • `Last Week` • `Last Month` • `Custom`
Format	Select an output format to generate the report in. Available options are: • `PDF` • `CSV`

> **Note**
> The **CSV** format is applicable only for the `Guest Visit History` and `Guest Visit History Summary` reports.

Destination	Select a destination to save the reports to. Available options are: • `Store on Server` • `Store & Mail`
Recipient Email	When **Store & Mail** is selected in **Destination**, specify the e-mail address to send the report to.
Email Policy	When **Store & Mail** is selected in **Destination**, use the pull-down menu to select an e-mail policy to use when sending the report. To create a new policy go to **Configuration →** **Notification → Policy** and select the ➕ icon.

5 To schedule a report generation process, select **Schedule** and configure the **Start Date**, **End Date**, **Frequency**, and **Time**.

6   When all configuration is complete, select **Save** to save the new report.

Select **Run** to execute the report without saving it. Select **Save & Run** to save the new report and run it. Select **Cancel** to discard the new report without saving.

7   To view the generated report go to **Analyze → Reports → Generated Reports**. For more information, see Generated Reports on page 108.

Scheduled Reports

Analyze → Reports → Scheduled Reports

Figure 65: Scheduled Reports Screen

The **Scheduled Reports** screen provides the following information about existing reports that are scheduled to run:

Report   Displays the report name for each existing generated report.

Type   Displays the report type for each generated report. The field at the top of this column allows filtering the **Type** by keyword.

User   Displays the user that generated each report. The field at the top of this column allows filtering the **User** by keyword.

Start Date   Displays the starting date and time that each report was last initiated.

End Date   Displays the ending date and time that each report was last completed.

Frequency Displays the interval that each report is scheduled to run.

Action   Select the **Trashcan** icon to delete a scheduled report.

Analyze Users

Analyze → Users

Figure 66: Analyze Users Screen

The **Analyze Users** screen display the following information about online users:

User   The **User** column displays the user icon associated with each online user.

Name   The **Name** column displays the username associated with each online user.

Email   The **Email** column displays the e-mail address associated with each online user.

Gender   The **Gender** column displays an icon representing the gender of each online user.

Source   The **Source** column displays the method that each online user used to authenticate. When social media authentication is enabled this will include Facebook, Google Plus, LinkedIn and Instagram.

Last Login The **Last Login** column displays the full date and time when the user last authenticated on the network.

Action From the **Action** column perform one of the following actions on a user. Select **Block** to stop a user from passing traffic on the network. Select **Disconnect** to end a user's session on the network. The user may reconnect if they re-authenticate. Select **Delete** to remove a user from the database. If the user connects again they will be treated as new user.

For information on how to filter user-results, see Filtering User Results on page 115.

Filtering User Results

Analyze → Users

Filters provide the ability to distill user data based on specific criteria.

To filter user results:

1 Go to **Analyze → Users** from the navigation menu.
2 Select the search icon in the upper right of the table.
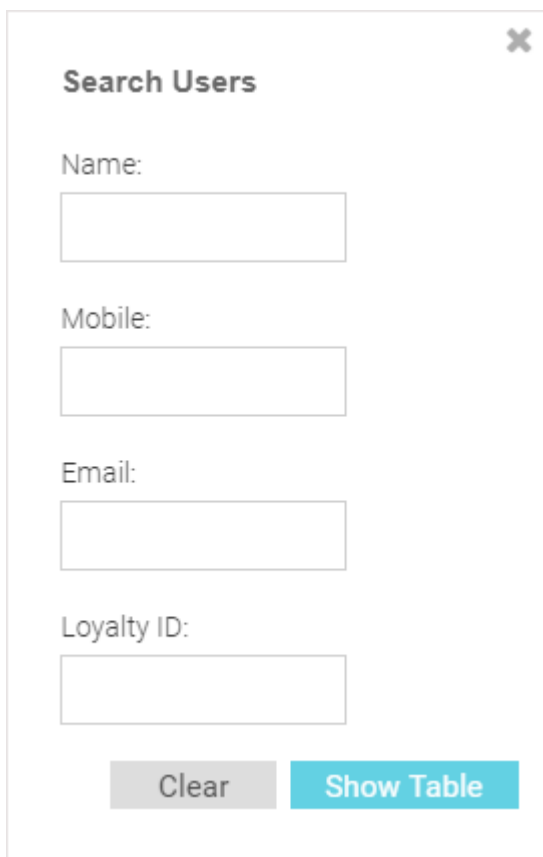
The **Search Users** window displays.

Figure 67: Filtering the Analyze Users Screen

3 Configure any one or more of the following search options:

Name Enter a user name or portion of a name to filter users with name matching the specified string.

Mobile   Enter a user's mobile number or a portion of a user's mobile number to filter users with mobile numbers matching the specified string.

Email   Enter an Email address or portion of an address such as a domain to filter users with e-mail address matching the specified string.

Loyalty ID   Enter a user's loyalty ID number to filter users with loyalty id matching the specified string.

> **Note**
> Loyalty ID should be enabled as a separate field during guest registration.

4   When all filters have been configured select **Show Table** to display the filtered results.

Select **Clear** to remove any text entered into the search fields.

7 Operations

The **Operations** menu provides the following sub-menus:

- Database on page 117
- License on page 120
- Maintenance on page 121
- REST API on page 122
- Troubleshooting on page 123

Database

Operations → Database

The **Database** screen contains the following sub-screens:

- Database Export on page 117
- Database Import on page 119

Database Export

Operations → Database → Export

The **Database Export** screen provides a method to back up guest user databases to an external server.

To export a database:

1 Go to **Operations** → **Database** → **Export** from the navigation menu.

The database **Export** screen displays.

Figure 68: Database Export Screen

2 Configure the following server options to export the database:

Protocol	Select the protocol used for exporting the guest user database. Available options are:
	• **SFTP**
	• **TFTP**
	• **FTP**
IP Address / Hostname	Provide a hostname string or numeric IP address of the server to export the guest user database to. Hostname cannot include an underscore character.
Username	Specify the username for the user authenticating to the remote server.
Password	Specify the password for the user authenticating to the remote server.
Path	Specify the path on the remote server where the guest user database file is copied to. Enter the complete relative path to the file on the remote server.
Filters	Optionally, specify which filters to apply to the database export. Available options are **Network**, **Time**, and **Location**. If selecting one or more of these options, use the associated pull-down menu to filter the database export.
File Type	Specify the file format for the exported database. Available options are: **JSON** and **CSV**.

3 After configuring server parameters, select **Export** to execute the database export.

Select **Reset** to remove server information from the screen.

Database Import

Operations → Database → Import

The **Database Import** screen provides a method to restore guest user databases from an external server.

To import a database:

1   Go to **Operations → Database → Import** from the navigation menu.

The database **Import** screen displays.

Figure 69: Database Import Screen

2   Configure the following server options to import the database from:

Protocol
: Select the protocol used for importing the guest user database. Available options are:
  - **SFTP**
  - **TFTP**
  - **FTP**

IP Address / Hostname
: Provide a hostname string or numeric IP address of the server to import the guest user database from. Hostname cannot include an underscore character.

Username
: Specify the username for the user authenticating to the remote server.

Password
: Specify the password for the user authenticating to the remote server.

Path
: Specify the path on the remote server where the guest user database file are copied from. Enter the complete relative path to the file on the remote server.

File Type
: Specify the file format for the exported database. Available options are: **JSON**

3   After configuring the server parameters, select **Import** to import the database.

Select **Reset** to remove server information from the screen.

License

Operations → License

The **License** screen displays product ID and license information for ExtremeGuest and provides a method to enter license keys.

Starting with this release, ExtremeGuest comes with the following two licenses:

- **Evaluation License**: This license is for fresh installations of the application software. First-time, ExtremeGuest administrators will use the evaluation license. It is a trial license with a validity period of 120 days and supports up to 100 endpoints (guest users/devices).
- **Production License**: This is the product perpetual license installed upon purchase of the product. It is applied on top of the evaluation license. Production license is based on the number of APs deployed. Please consult with your Extreme Networks representative for the tiers available for the ExtremeGuest production license.

> **Note**
> The production license is based on the number of *access points* deployed across your sites and not the number of *endpoints* associated with these access points.

To access the **License** page:

1 Go to **Operations → License** from the main menu.

The **License** screen displays.

Figure 70: License Screen

2 Review the following ExtremeGuest license information:

Product ID	Displays the unique product ID for this ExtremeGuest installation. This product ID is needed to generate the ExtremeGuest license key.
License Key	Enter a key into this field to activate a new license.
License Installed	Displays the number of end-point/access point licenses are configured for this ExtremeGuest installation. The system includes a license for 100 end points.
License Used	Displays the number of end-point/access point licenses currently in use.
License Available	Displays the number of end-point/access point licenses available for use. This number is the number of installed licenses minus the current number of licenses in use.

> **Note**
> If no valid license exists after the grace period expires, login will be restricted until a valid license is installed. For invalid licenses the user interface will display only a username, password and license field.

3 To activate a new license, enter the key into the **License Key** field and select **Update License**.

Maintenance

Operations → Maintenance

The **Maintenance** screen provides the ability to view and remove deleted and offline devices. It also provides the ability to reset the ExtremeGuest user interface to its factory default settings.

To view the maintenance screen:

1   Go to **Operations** → **Maintenance** from the main menu.

The **Maintenance** screen displays a summary view of deleted and offline devices with the option to **Delete All** for each section. There is also the option to **Reset ExtremeGuest to Defaults**.

The **Maintenance** screen displays.

Figure 71: Maintenance Screen

2   To view details of **Deleted Devices** select the arrow to expand the panel.

The **Deleted Devices** section displays the **Name**, **MAC Address**, **Location**, controller **Reported by**, **Offline** duration, and **Offline since** date. The **Action** column allows individual devices to be removed.

3   Select **Delete All** to remove all **Deleted Devices** from ExtremeGuest.

4   To view details of **Offline Devices** select the arrow to expand the panel. Select the number of **Days** and **Hours** to filter the devices included.

The **Offline Devices** section displays the **Name**, **MAC Address**, **Location**, controller **Reported by**, **Offline** duration, and**Offline since** date. The **Action** column allows individual devices to be removed.

5   Select **Delete All** to remove all **Offline Devices** from ExtremeGuest.

6   To reset the ExtremeGuest system to default settings, select **Reset** next to **Reset ExtremeGuest to Defaults**. This will erase all data and settings from the ExtremeGuest application.

REST API

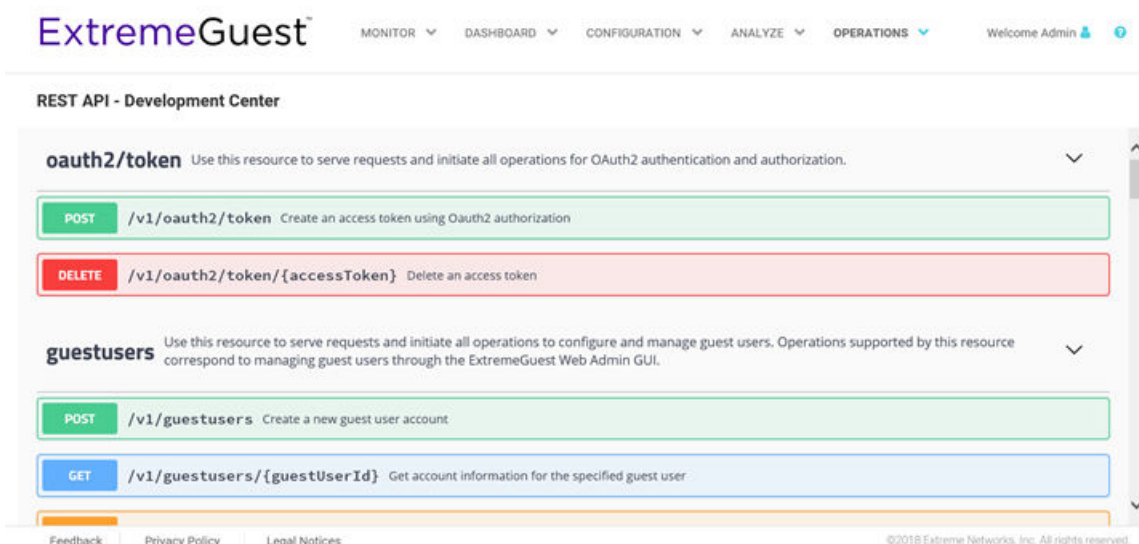**Operations** → **REST API**

Figure 72: REST API Screen

The REST API screen provides an interactive interface to try out all available API resources, methods, endpoints, and operations.
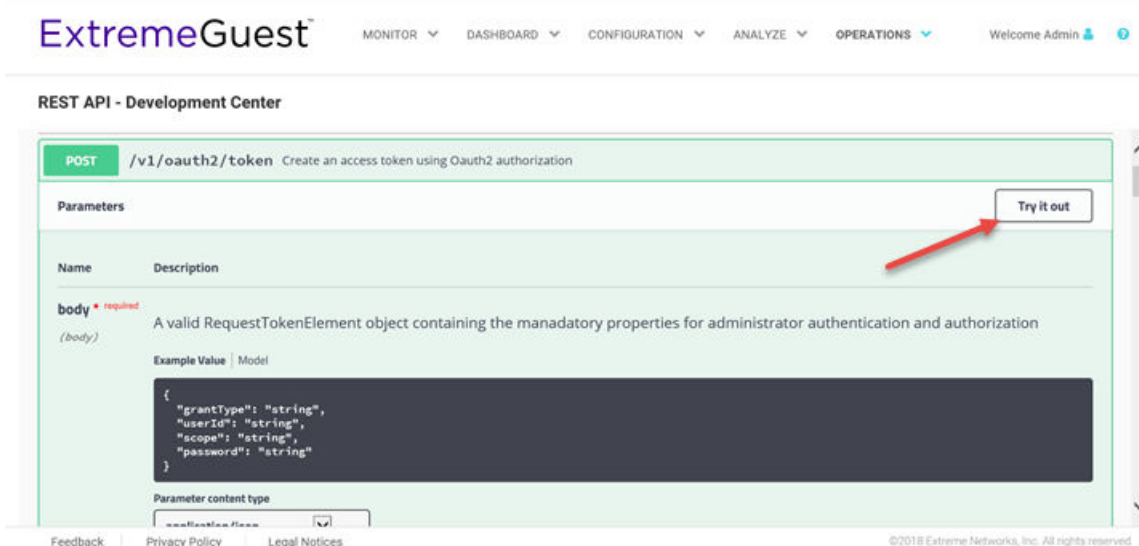

Figure 73: Try Out Feature to Test API Calls

For detailed information about the REST API functionality, refer the ExtremeGuest REST API guide available at http://developer.extremenetworks.com.

Troubleshooting

Operations → Troubleshoot

The ExtremeGuest UI allows you to generate customized debug logs that facilitate troubleshooting captive portal issues. Refer to the following topic for more information:

-

ExtremeWireless WiNG Captive Portal Debug

Operations → Troubleshoot → Extreme Wireless Wing Captive Portal Debug

The **Captive Portal Debug Log** screen provides a method to troubleshoot ExtremeWireless WiNG deployed ExtremeGuest captive portal issues using customized debug logs.

To create a captive portal debug log:

1   Go to **Operations → Troubleshoot → Extreme Wireless Captive Portal Debug** from the navigation menu.

   The **Extreme Wireless WiNG Captive Portal Debug** screen displays.

Figure 74: Extreme Wireless WiNG Captive Portal Debug Screen

2 Configure the following debug log options:

| Site | Specify a site (RF Domain) to include logging information about. Select **Include all devices** to include devices in the generated debug log. If **Include all devices** is not selected, specify an individual device name in the field. |

Select Debug Messages — Specify what level of debug messages to include. Available options are:

- **All Debug Messages**
- **Authentication Debug Messages**
- **Captive-portal client debug messages**

Clients — Select which clients to include in the log. Available options are:

- **All Clients**
- **Selected Clients (up to 3)**

Filter Criteria — Configure the following filter criteria:

| Duration of Message Capture | Specify an amount of time to capture messages for the debug log. Time can be set in **Hour(s)**, **Minute(s)**, and **Second(s)**. |

Maximum Events Per Remote System — Specify the maximum number of events to log for each remote system (client or device). Once this threshold is reached, older log entries for that system will be removed.

3 When all log parameters have been configured, select **Start** to start capturing log events. Select **Stop** to halt capturing log events.

4 While the **Logs** screen is active, select **Save to Disk** to save the current log output to a text file. Select **Copy to Clipboard** to copy the current log output to your system's clipboard.

The Logs are displayed

Figure 75: Captive Portal Debug Log Output

Glossary

AAA

Authentication, Authorization, and Accounting is a system in IP-based networking to control which computer resources specific users can access and to keep track of the activity of specific users over the network.

ad hoc mode

An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an AP.

ARP

Address Resolution Protocol is part of the TCP/IP suite used to dynamically associate a device's physical address (MAC address) with its logical address (IP address). The system broadcasts an ARP request, containing the IP address, and the device with that IP address sends back its MAC address so that traffic can be transmitted.

ATM

Asynchronous Transmission Mode is a start/stop transmission in which each character is preceded by a start signal and followed by one or more stop signals. A variable time interval can exist between characters. ATM is the preferred technology for the transfer of images.

BSS

Basic Service Set is a wireless topology consisting of one access point connected to a wired network and a set of wireless devices. Also called an infrastructure network. See also *IBSS (Independent Basic Service Set)*.

Chalet

Chalet is a web-based user interface for setting up and viewing information about a switch, removing the need to enter common commands individually in the CLI.

CHAP

Challenge-Handshake Authentication Protocol is one of the two main authentication protocols used to verify a user's name and password for PPP Internet connections. CHAP is more secure because it performs a three-way handshake during the initial link establishment between the home and remote machines. It can also repeat the authentication anytime after the link has been established.

CLI

Command Line Interface. The CLI provides an environment to issue commands to monitor and manage switches and wireless appliances.

Data Center Connect

DCC, formerly known as DCM (Data Center Manager), is a data center fabric management and automation tool that improves the efficiency of managing a large virtual and physical network. DCC provides an integrated view of the server, storage, and networking operations, removing the need to use multiple tools and management systems. DCC automates VM assignment, allocates appropriate network resources, and applies individual policies to various data objects in the switching fabric (reducing VM sprawl). Learn more about DCC at http://www.extremenetworks.com/product/data-center-connect/.

DoS attack

Denial of Service attacks occur when a critical network or computing resource is overwhelmed so that legitimate requests for service cannot succeed. In its simplest form, a DoS attack is indistinguishable from normal heavy traffic. ExtremeXOS software has configurable parameters that allow you to defeat DoS attacks.

DSSS

Direct-Sequence Spread Spectrum is a transmission technology used in Local Area Wireless Network (LAWN) transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission. (Compare with *FHSS (Frequency-Hopping Spread Spectrum)*.)

EAP-TLS/EAP-TTLS

EAP-TLS Extensible Authentication Protocol - Transport Layer Security. A general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards.

IEEE 802.1x specifies how EAP should be encapsulated in LAN frames.
In wireless communications using EAP, a user requests connection to a WLAN through an access point, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS The server asks the access point for proof of identity, which the access point gets from the user and then sends back to the server to complete the authentication.

EAP-TLS provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys.

EAP-TTLS (Tunneled Transport Layer Security) is an extension of EAP-TLS to provide certificate-based, mutual authentication of the client and network through an encrypted tunnel, as well as to generate dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
(See also *PEAP (Protected Extensible Authentication Protocol)*.)

ESRP

Extreme Standby Router Protocol is an Extreme Networks-proprietary protocol that provides redundant Layer 2 and routing services to users.

Extreme Application Analytics

EAA, formerly Purview™, is a network powered application analytics and optimization solution that captures and analyzes context-based application traffic to deliver meaningful intelligence about applications, users, locations, and devices. EAA provides data to show how applications are being used. This can be used to better understand customer behavior on the network, identify the level of user engagement, and assure business application delivery to optimize the user experience. The software also provides visibility into network and application performance allowing IT to pinpoint and resolve performance issues in the infrastructure whether they are caused by the network, application, or server. Learn more about EAA at http://www.extremenetworks.com/product/extremeanalytics/.

Extreme Management Center

Extreme Management Center (Management Center), formerly Netsight™, is a web-based control interface that provides centralized visibility into your network. Management Center reaches beyond ports, VLANs, and SSIDs and provides detailed control of individual users, applications, and protocols. When coupled with wireless and Identity & Access Management products, Management Center becomes the central location for monitoring and managing all the components in the infrastructure. Learn more about Management Center at http://www.extremenetworks.com/product/management-center/.

ExtremeCloud Appliance

The ExtremeCloud Appliance, the newest addition to the Smart OmniEdge portfolio, is a next generation orchestration application offering all the mobility services required for modern unified access deployments. The ExtremeCloud Appliance extends the simplified workflows of the ExtremeCloud public cloud application to on-prem/private cloud deployments.

The ExtremeCloud Appliance includes comprehensive critical network services for wireless and wired connectivity, wireless device secure onboarding, distributed and centralized data paths, role-based access control through the Application Layer, integrated location services, and IoT device onboarding through a single platform.

Built on architecture with the latest technology, the embedded operating system supports application containers that enable future expansion of value added applications for the unified access edge. Learn more about ExtremeCloud Appliance at https://www.extremenetworks.com/product/extremecloud-appliance/.

ExtremeCloud

ExtremeCloud is a cloud-based network management Software as a Service (SaaS) tool. ExtremeCloud allows you to manage users, wired and wireless devices, and applications on corporate and guest networks. You can control the user experience with smarter edges – including managing QoS, call admission control, secure access policies, rate limiting, multicast, filtering, and traffic forwarding, all from an intuitive web interface. Learn more about ExtremeCloud at http://www.extremenetworks.com/product/extremecloud/.

ExtremeControl

ExtremeControl, formerly Extreme Access Control™ (EAC), is a set of management software tools that use information gathered by a hardware engine to control policy to all devices on the network. The software allows you to automate and secure access for all devices on the network from a central dashboard, making it easier to roll out security and identity policies across the wired and wireless network. Learn more about ExtremeControl at https://www.extremenetworks.com/product/extremecontrol/.

ExtremeSwitching

ExtremeSwitching is the family of products comprising different switch types: **Modular** (X8 and 8000 series [formerly BlackDiamond] and S and K series switches); **Stackable** (X-series and A, B, C, and 7100 series switches); **Standalone** (SSA, X430, and D, 200, 800, and ISW series); and **Mobile Backhaul** (E4G). Learn more about ExtremeSwitching at http://www.extremenetworks.com/products/switching-routing/.

ExtremeWireless

ExtremeWireless products and solutions offer high-density WiFi access, connecting your organization with employees, partners, and customers everywhere they go. The family of wireless products and solutions includes APs, wireless appliances, and software. Learn more about ExtremeWireless at http://www.extremenetworks.com/products/wireless/.

ExtremeWireless WiNG

The WiNG architecture is a solution designed for 802.11n and 802.11ac networking. It is designed for standalone or distributed hierarchical networks. The ExtremeWireless WiNG software distributes intelligence right to the network edge, empowering every controller and access point with the intelligence needed to be network-aware, able to identify and dynamically route traffic over the most efficient path available at that time. It is highly scalable and well suited to meet the needs of large, geographically distributed enterprises. It is an ideal wireless networking solution for the retail, manufacturing, transportation & logistics, and hospitality verticals.

ExtremeWireless

ExtremeWireless products and solutions offer high-density WiFi access, connecting your organization with employees, partners, and customers everywhere they go. The family of wireless products and solutions includes APs, wireless appliances, and software. Learn more about ExtremeWireless at http://www.extremenetworks.com/products/wireless/.

ExtremeXOS

ExtremeXOS, a modular switch operating system, is designed from the ground up to meet the needs of large cloud and private data centers, service providers, converged enterprise edge networks, and everything in between. Based on a resilient architecture and protocols, ExtremeXOS supports network virtualization and standards-based SDN capabilities like VXLAN gateway, OpenFlow, and OpenStack Cloud orchestration. ExtremeXOS also supports comprehensive role-based policy. Learn more about ExtremeXOS at http://www.extremenetworks.com/product/extremexos-network-operating-system/.

FHSS

Frequency-Hopping Spread Spectrum is a transmission technology used in Local Area Wireless Network (LAWN) transmissions where the data signal is modulated with a narrowband carrier signal that 'hops' in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. This technique reduces interference. If synchronized properly, a single logical channel is maintained. (Compare with *DSSS (Direct-Sequence Spread Spectrum)*.)

IBSS

An IBSS is the 802.11 term for an ad hoc network. See *ad hoc mode*.

MIC

Message Integrity Check (or Code), also called 'Michael', is part of WPA and TKIP. The MIC is an additional 8-byte code inserted before the standard 4-byte ICV appended in by standard WEP to the 802.11 message. This greatly increases the difficulty in carrying out forgery attacks.
Both integrity check mechanisms are calculated by the receiver and compared against the values sent by the sender in the frame. If the values match, there is assurance that the message has not been tampered with.

NAS

The Network Access Serve is responsible for passing information to designated RADIUS servers and then acting on the response returned. A NAS-Identifier is a RADIUS attribute identifying the NAS server. (RFC 2138)

netmask

A netmask is a string of 0s and 1s that mask, or screen out, the network part of an IP address, so that only the host computer part of the address remains. A frequently-used netmask is 255.255.255.0, used for a Class C subnet (one with up to 255 host computers). The ".0" in the netmask allows the specific host computer address to be visible.

PEAP

Protected Extensible Authentication Protocol is an IETF draft standard to authenticate wireless LAN clients without requiring them to have certificates. In PEAP authentication, first the user authenticates the authentication server, then the authentication server authenticates the user. If the first phase is successful, the user is then authenticated over the SSL tunnel created in phase one using EAP-Generic Token Card (EAP-GTC) or Microsoft Challenged Handshake Protocol Version 2 (MSCHAP V2). (See also *EAP-TLS/EAP-TTLS*.)

SSL

Secure Socket Layer is a protocol for transmitting private documents using the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. SSL uses the public-and-private key encryption system, which includes the use of a digital certificate. SSL is used for other applications than SSH, for example, OpenFlow.

syslog

A protocol used for the transmission of event notification messages across networks, originally developed on the University of California Berkeley Software Distribution (BSD) TCP/IP system implementations, and now embedded in many other operating systems and networked devices. A device generates a messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.
syslog uses the UDP as its underlying transport layer mechanism. The UDP port that has been assigned to syslog is 514. (RFC 3164)

VSA

Vendor Specific Attribute is a RADIUS server attribute defined by the manufacturer. (Compared to the RADIUS attributes defined in the original RADIUS protocol RFC 2865). A VSA attribute is defined in order that it can be returned from the RADIUS server in the Access Granted packet to the Radius Client.

Index

C

conventions
    notice icons 5
    text 5

D

documentation
    feedback 5
    location 7

O

Open Source Declaration 7

S

support, *see* technical support

T

technical support
    contacting 6