ExtremeGuest Essentials User Guide

Version 23R3

9037815-00 Rev AA
May 2023

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

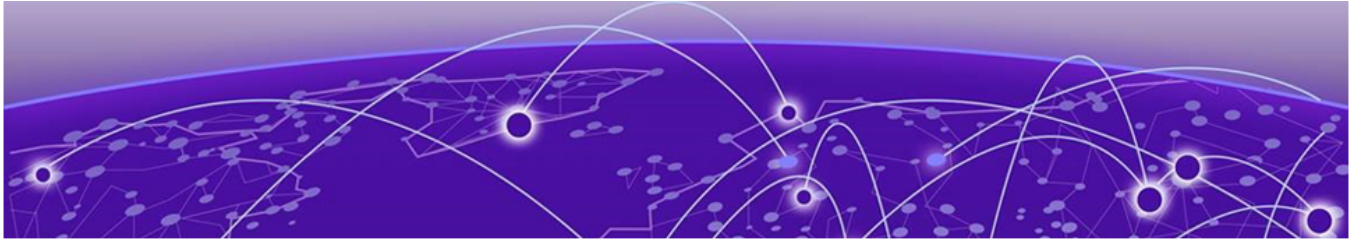


Table of Contents

Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as ExtremeSwitching switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed 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 in boldface, for example **Ctrl** 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.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[ ]`	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
`{ x | y | z }`	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
`x | y`	A vertical bar separates mutually exclusive elements.
`< >`	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*`[`*member*`...]`.
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Send Feedback

The Information Development team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve

our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, do either of the following:

- Access the feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

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.

Help and Support

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: (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, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions 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

Subscribe to Product Announcements

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

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

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

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes
Hardware and software compatibility for Extreme Networks products
Extreme Optics Compatibility
Other resources such as white papers, data sheets, and case studies

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

Introduction to ExtremeGuest Essentials

ExtremeGuest Essentials is a robust and comprehensive guest management and engagement solution that personalizes engagement by understanding customer behavior and interest, and then tailoring services based on those insights. For example, the number of customers that enter a store, how often they visit, and how much time they spend are all metrics that can be measured through ExtremeGuest Essentials.

ExtremeGuest Essentials 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 Essentials supports all access point models that are supported with ExtremeCloud IQ.

For documentation on each access point, refer to the AP model number under Extreme Documentation at extremenetworks.com/documentation.

To get started, go to the ExtremeCloud IQ Dashboard and select the Essentials icon from the list. Then select ExtremeGuest Essentials. The ExtremeGuest Essentials Connection Status launches in ExtremeCloud IQ.

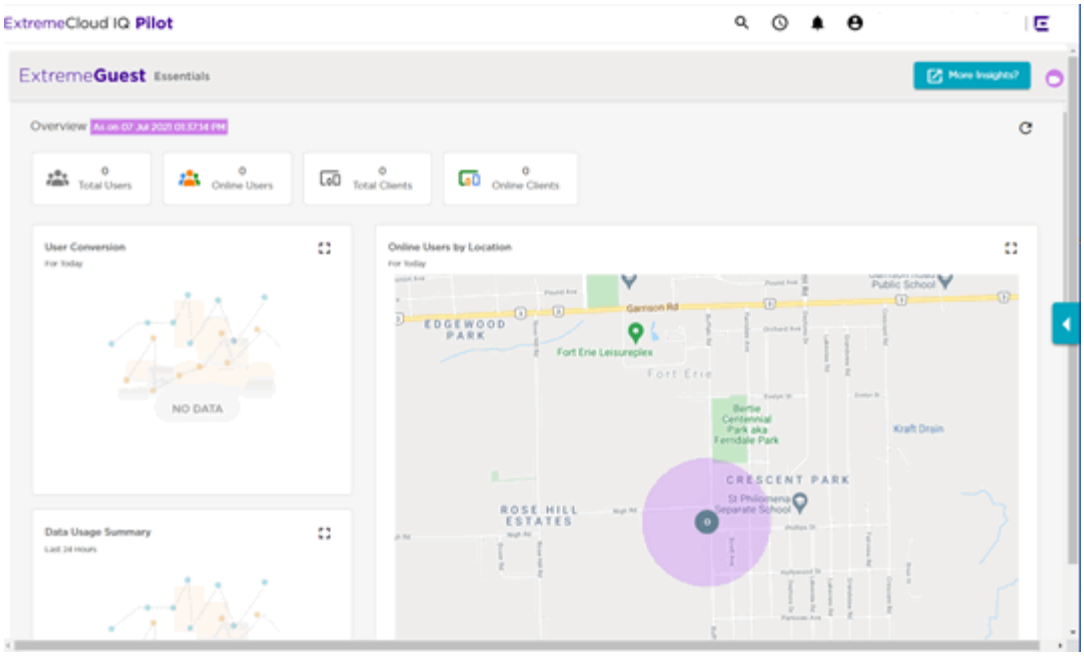
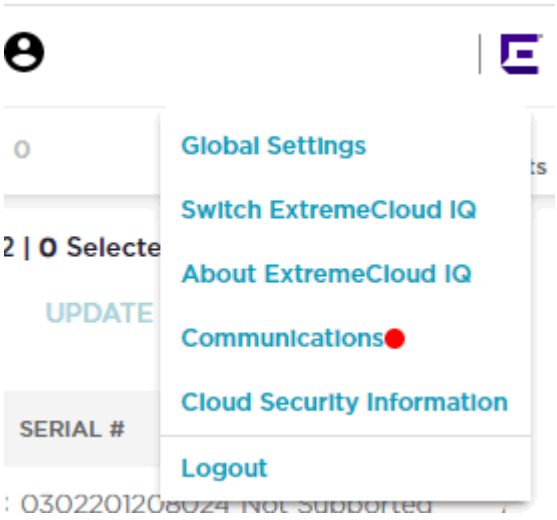


Figure 1: ExtremeGuest Essentials Overview View in ExtremeCloud IQ

Select the  to access the ExtremeCloud IQ HelpDesk feature, which provides you with access to several additional functions in the drop-down list:



The following options are included in the HelpDesk feature:

Global Settings	Provides settings details related to ExtremeCloud IQ Accounts, Administration, API, Logs, and SSH Availability. Use the Accounts > Account Management tab to add, edit, or delete Admin Accounts. Select the icon to edit the information displayed.
Switch ExtremeCloud IQ	Select to switch ExtremeCloud IQ accounts. This link is only available if you have more than one ExtremeCloud IQ account.
About ExtremeCloud IQ	Displays details about your ExtremeCloud IQ account.
Communications	Displays what's new in Extreme Networks, important notices from Extreme Networks, and previews (if available) of new features.
Cloud Security Information	Select to access Extreme Networks' Cloud Security web page.
Logout	Select to log out of the ExtremeCloud IQ account.

Note
You can configure ExtremeGuest Essentials bulk vouchers using the HelpDesk feature in ExtremeCloud IQ. Or refer to ExtremeGuest Essentials instructions under Create Bulk Vouchers on page 86.

Select the **More Insights** button at the top right corner of the Overview to launch ExtremeGuest Essentials and open the ExtremeGuest Essentials Dashboard.

Related Topics

User Management on page 11
Create Bulk Vouchers on page 86

User Management

Select **Global Settings** > **Account Management** to review and edit ExtremeCloud IQ Admin Account information. To add a new Admin account, select the Add icon in the top left corner of the **Admin Accounts** page to open the **Add New Admin** page:

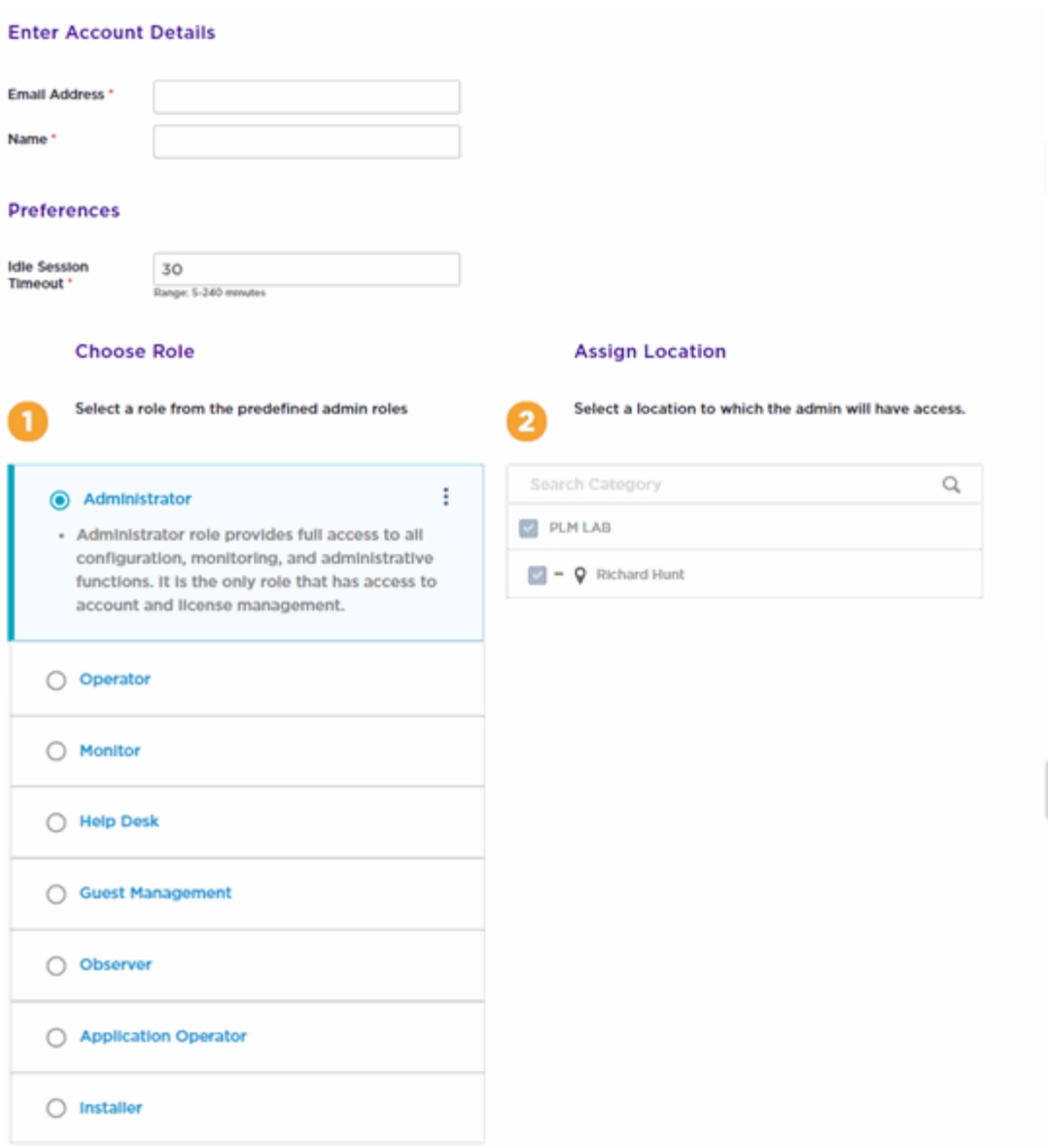


Figure 2: Add New ExtremeCloud IQ Admin Account

The ExtremeGuest Essentials user interface supports the following user roles:

Administrator

The admin user has full control of the ExtremeGuest Essentials system and access to all configuration items. This guide is written for admin users.

Operator

Operator role provides full access to most functions including network and device configuration. However, it does not allow access to user account and license management.

Monitor

Monitor role provides full access to troubleshooting and read-only access to monitoring and configuration functions.

Monitor role has the ability to view dashboards, view active users (with block access) including devices. Monitor role can create and execute reports based on assigned location and create vouchers. Monitor role does not have access to configuration dialogs including templates.

UI Overview

ExtremeGuest Essentials is a comprehensive solution that customizes engagement by analyzing customer behavior and interest, and then tailoring services based on those insights. For example, using ExtremeGuest Essentials, you can track how many customers use the guest network, how often they visit, and how much time they spend on the guest network.

ExtremeGuest Essentials offers the following main options. Select each option to display the ExtremeGuest Essentials tools and configuration settings:

	Monitor on page 15
	Configure on page 32
	Analyze on page 92

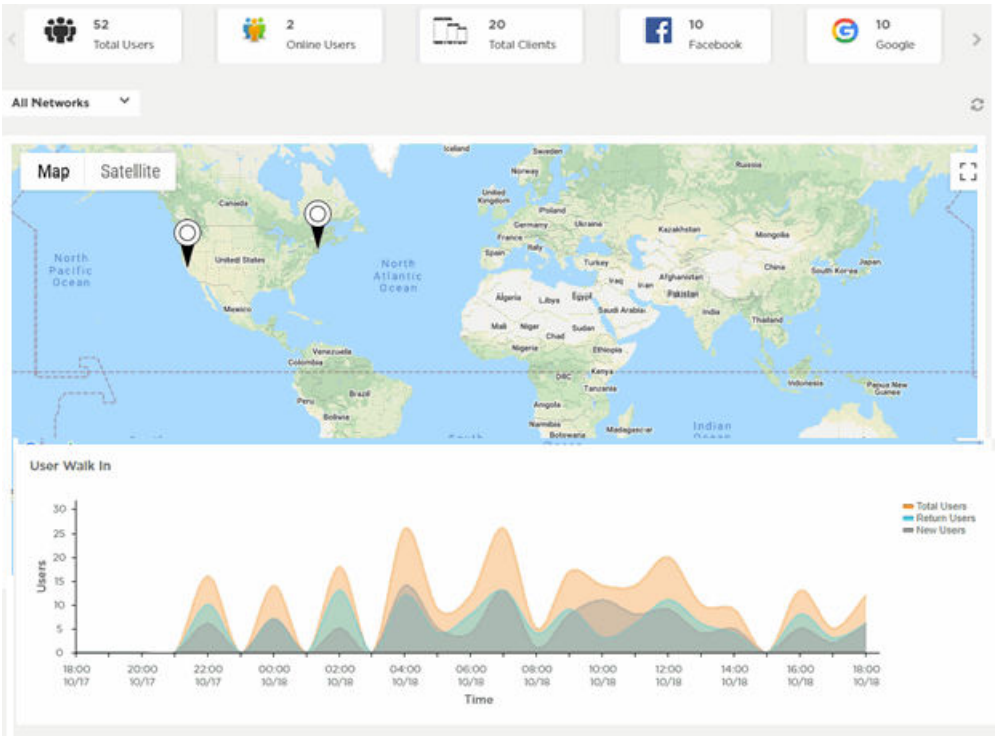


Figure 3: User Interface in Standard View – Top Widgets

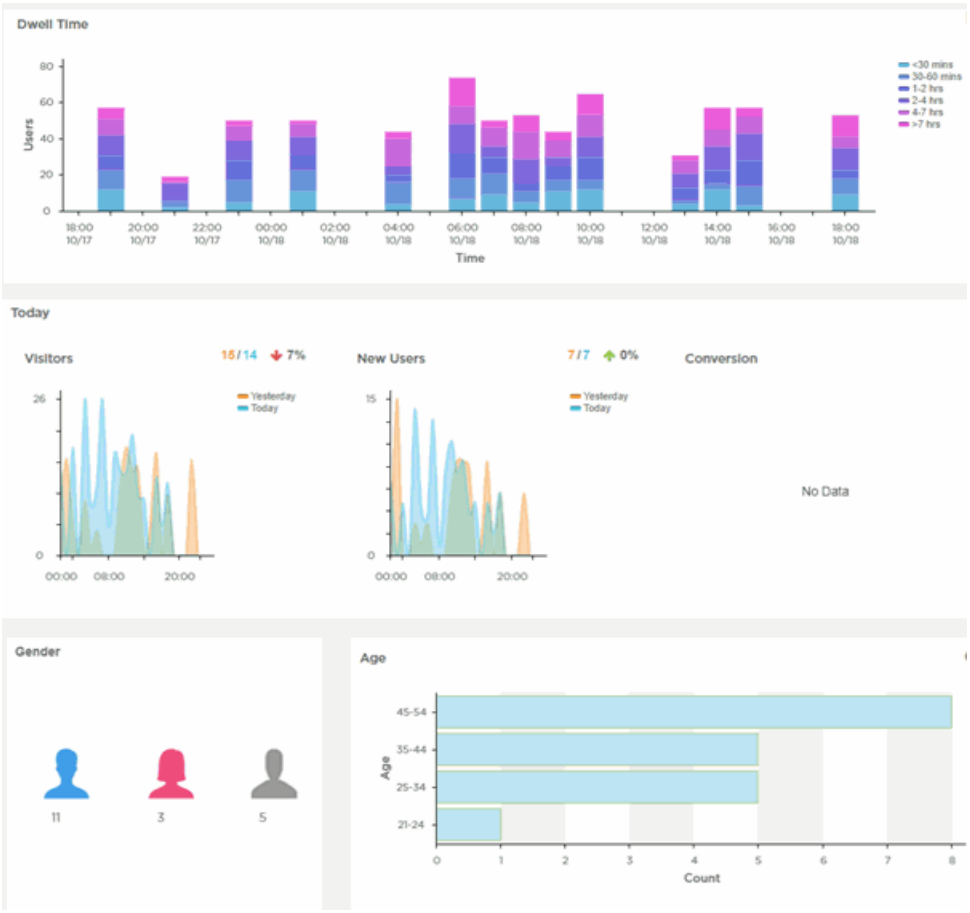


Figure 4: User Interface in Standard View – Bottom Widgets

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.

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 15
- Dashboard on page 21
- Configure on page 32
- Analyze on page 92

Monitor

The **Monitor** workbench includes ExtremeGuest Essentials Summary information and Dashboard information.

The **Summary** screen displays map-based views and active user summaries.

The **Dashboard** screen displays reports to help you manage ExtremeGuest Essentials.

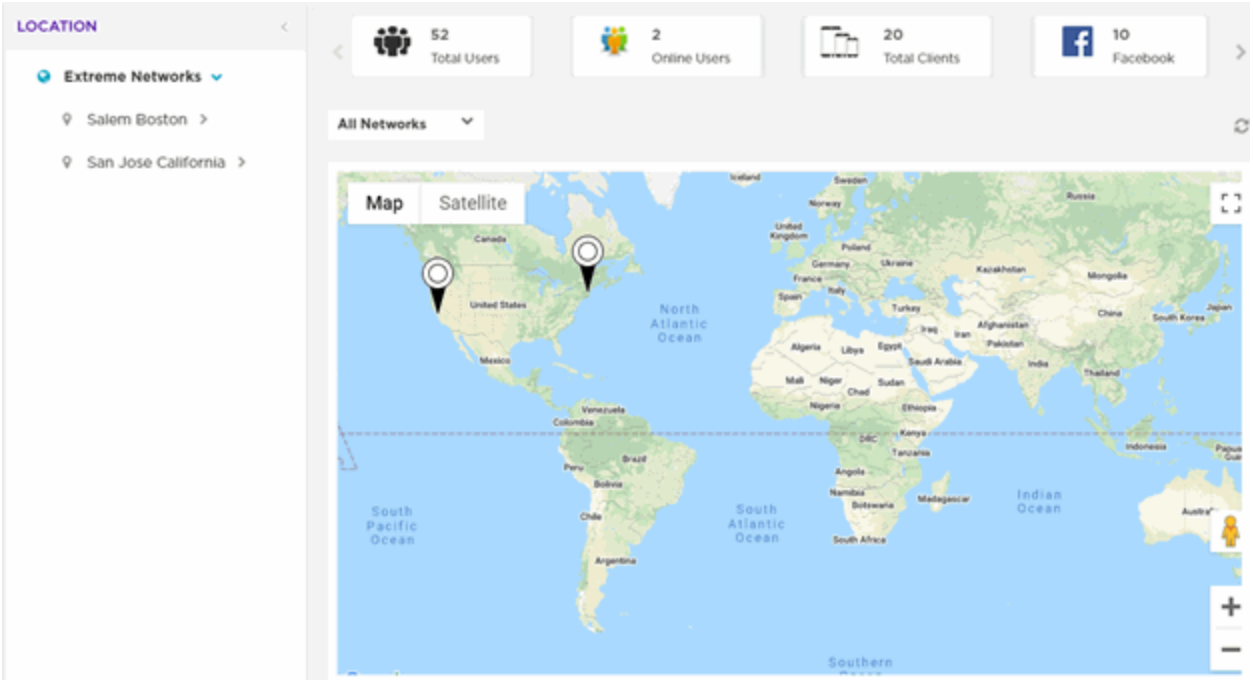
Summary

The **Summary** screen displays map-based views and active user summaries.

The Summary is divided into to two sections: The left-panel tree and the right-panel Summary Details on page 20 panel. Use the left-panel tree to navigate to sites within your networks. Expand the tree and select a site to display user information specific to that site location.

The Map View is divided into to two sections: The left-panel tree and the right-panel map.

Use the left-panel tree to navigate to sites within your networks. Expand the tree and select a site to refocus the map to that site location.



The 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, or LinkedIn.

A map view is generated using Google Maps based on site locations. Place your cursor over a site to display key user metrics for that location.

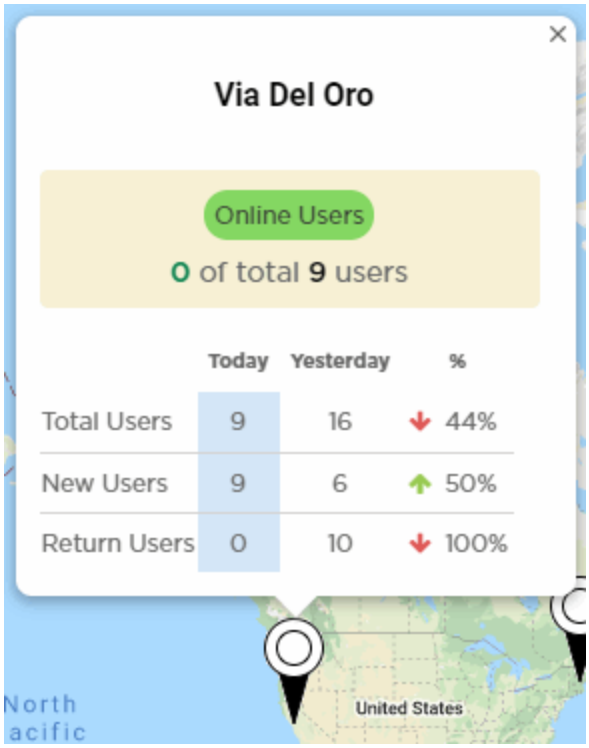


Figure 5: Map View

Map View Controls

Use the following controls to manipulate the map view and to review details of places on the map:

Table 4: Map View Controls

Map View Control	Location	Description
	Bottom-right corner of the map	Drag and drop the icon on a specific area on the map to display a street view of the area.
	Bottom-right corner of the map	Use to zoom in and out on the map.
	Top-right corner of the map	Use to open the map in full-screen mode. Select the [Esc] button to exit full-screen mode.
	Top-left corner of the map	Use to toggle between map view and satellite view. You can also add Terrain details to the map view and labels to the satellite view.

Figure 6: Summary Screen

The **Summary** screen provides a high-level overview of user activity over the past 24 hours, which updates automatically.

The bar at the top of the window displays information about the total number of users and the total number of users online.

If social media authentication is enabled, the number of users authenticated using Facebook, Google Plus or LinkedIn also displays. The Summary Details on page 20 panel displays additional summary information.

Summary Details

Figure 7: Summary Details

The **Summary** screen displays the 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 durations:

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

Note

Use the Show Grouped /Show Stacked icons to display user data grouped into categories or stacked into separate categories for each of the time durations.

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** customers. The information displayed in all three graphs starts at midnight of the previous day and goes through the current time. The data resets each day at midnight.

Gender

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

Age

Use the Show Bar Chart /Show Pie Chart icons to display user data as a bar chart or pie chart respectively. The **Age** chart displays the total number of users, separated into the following age ranges:

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

Dashboard

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 22
- Available Dashboard Widgets on page 30

Creating a New Dashboard

Dashboard → Create New

This section describes how to create customized ExtremeGuest Essentials dashboards.

Note
Dashboards can be created based on the selected location.

You can create customized ExtremeGuest Essentials 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 Essentials 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.

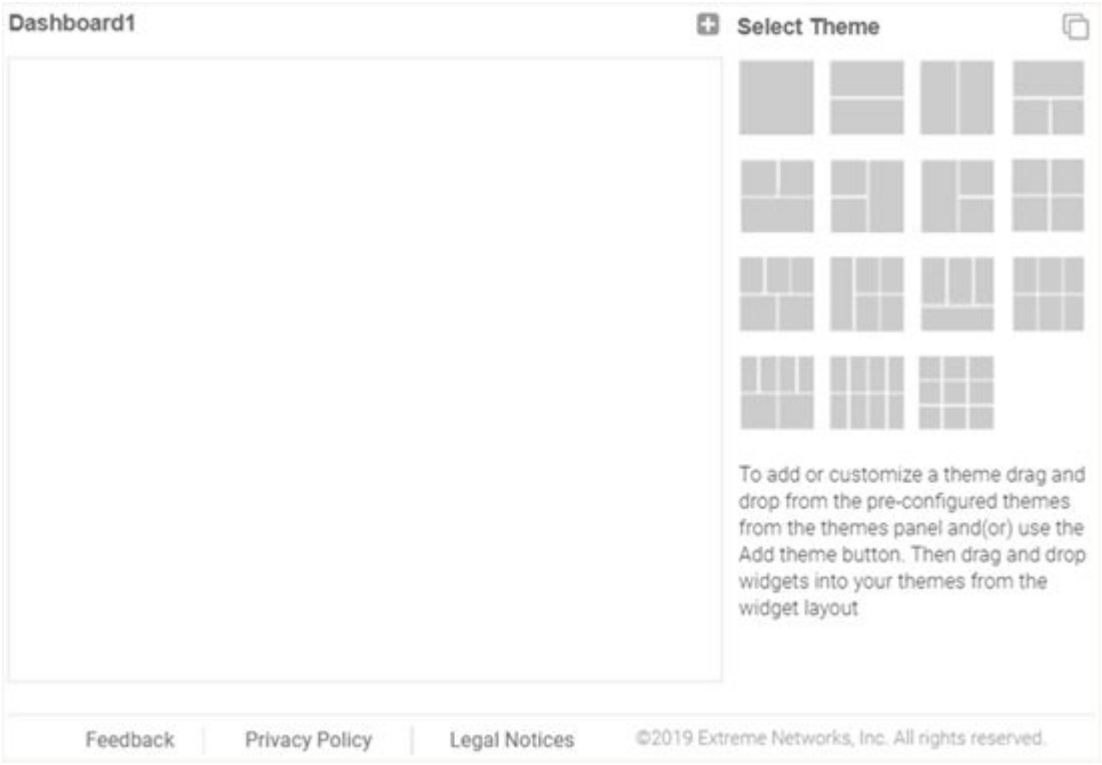


Figure 8: ExtremeGuest Essentials New Dashboard Screen

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

2. Drag and drop a theme from the **Select Theme** menu onto the main window.
   To change the layout, drag another theme in place of the current one.
   The dashboard layout displays the theme outline.

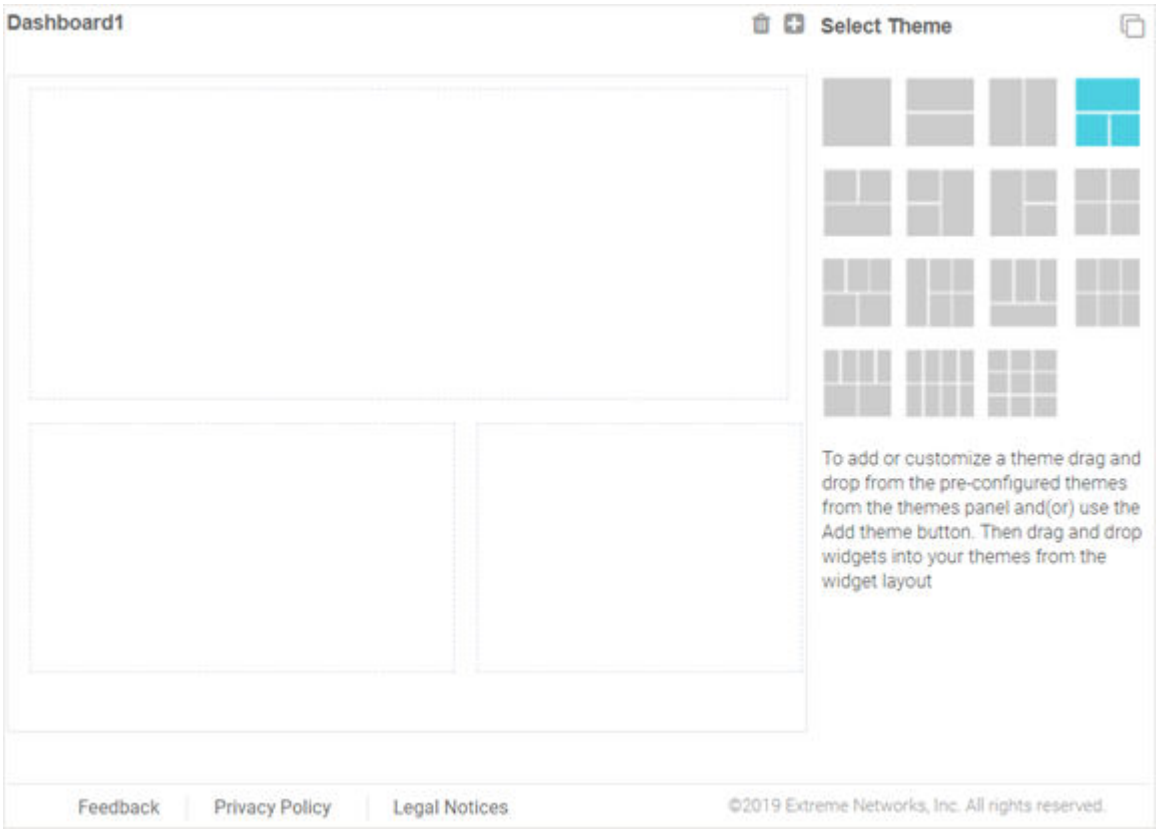


Figure 9: Selecting a Dashboard Theme

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

4. Drag widgets into the layouts to populate the dashboard.

Figure 10: 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 Available Dashboard Widgets on page 30.

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.

Dwell Charts

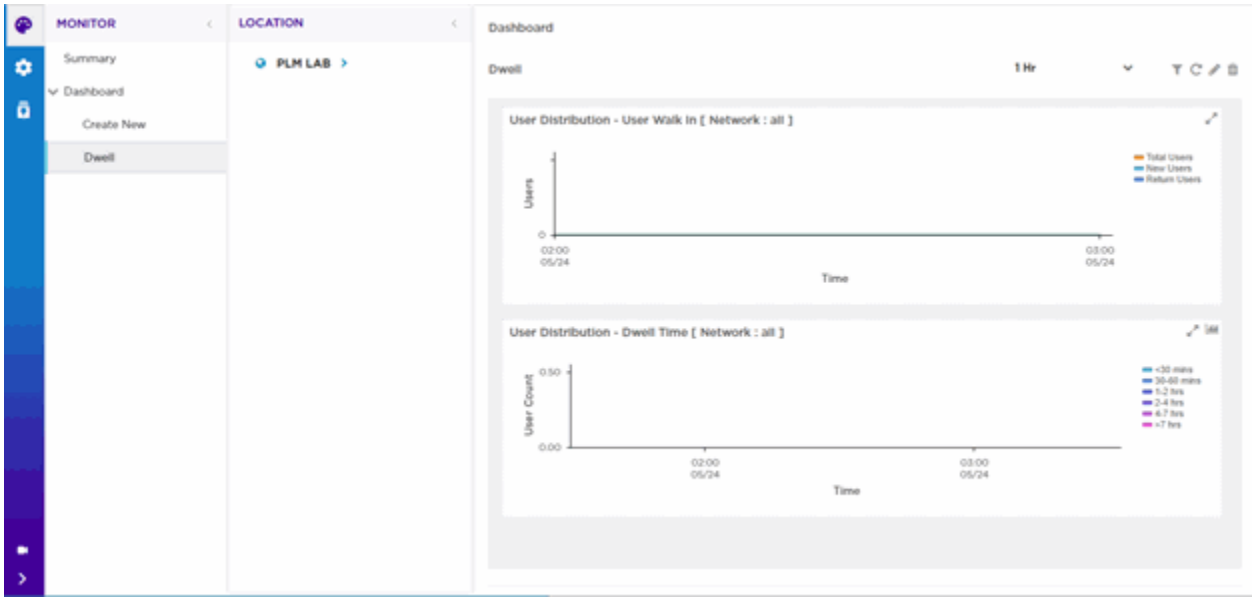


Figure 11: Dashboard Dwell Charts

Dwell Charts

The **Dwell** tab displays two User Distribution Dwell charts that provide detailed dwell time information:

- User Distribution - User Walk-In
- User Distribution - Dwell Time

User Distribution - User Walk In

This chart shows the dwell time of Walk-In users for the duration you select. The chart displays the dwell time for:

- Total Users
- New Users
- Return Users

User Distribution - Dwell Time

This chart shows the dwell time for all users in your network for the duration you select. User dwell time is displayed for the following dwell times:

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

- 4-7 Hours
- > 7 Hours

Dashboard Controls

Filter data in the charts using the following Dashboard controls:

Table 5: Dashboard Controls

Dashboard Control	Location	Description
	Top-right corner of the dashboard	Select to enable the network filter option within each chart. 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 Dwell chart data.
	Top-right corner of the dashboard	Select to add, edit or remove data from the chart.
	Top-right corner of the dashboard	Select to remove data from the chart.
and	Top-right corner of the widget	Select to maximize and minimize a chart respectively.

Report Duration Filter

The Dwell charts include a filter data based on time duration. Select the report duration from the drop-down menu on the top-right, corner of the **Dwell** tab.

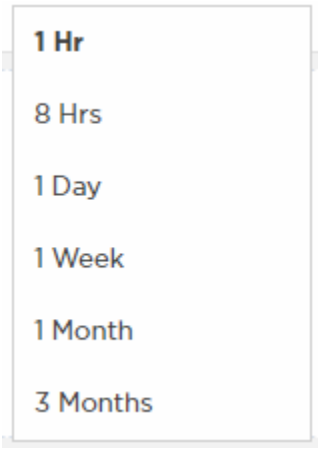


Figure 12: Report Duration Filter

The filter options are:

- 1 Hr
- 8 Hrs
- 1 Day
- 1 Week

- 1 Month
- 3 Months

Dashboard Basics

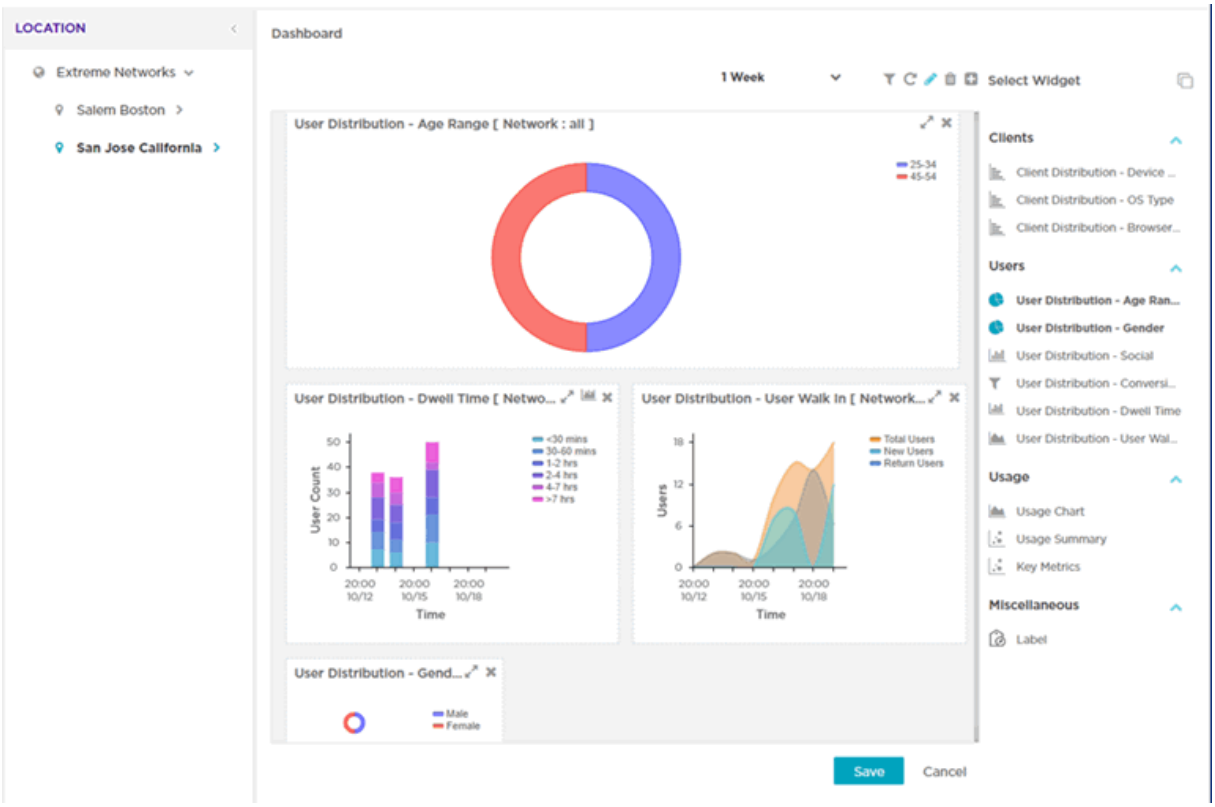


Figure 13: Example Dashboard Screen

Dashboard Components

The Dashboard includes several components:

- Location
- Main
- Controls
- Report Duration Filter

Location

The left-panel includes your networks. Expand your networks to display the locations within each network. Select a locationa and the widgets you select in the Main panel displays client and usage data from those locations.

Main

The Main Dashboards area displays the following:

- **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 30.

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 6: 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.

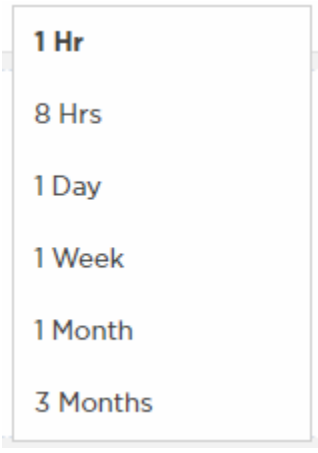


Figure 14: Report Duration Filter

The filter options are:

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

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	Distribution - Conversion	Graph displaying the number and percentage of users who converted from **Connected** to **Onboarded** 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

Category	Widget	Description
		• 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 • 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, and social media sign in status.
Miscellaneous	Label	Custom label for creating Dashboard titles.

Configure

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

- Settings on page 32
- Network on page 41
- Location on page 40
- Devices on page 43
- Notification on page 44
- Onboarding on page 47
- Splash Templates on page 54

Settings

Configure → Settings

Settings includes detailed information about your network's Authorization Policy on page 32 and Access Groups on page 36. Use these tabs to add, modify, or review access profile and group information.

Authorization Policy

Configure → Settings → Authorization Policy

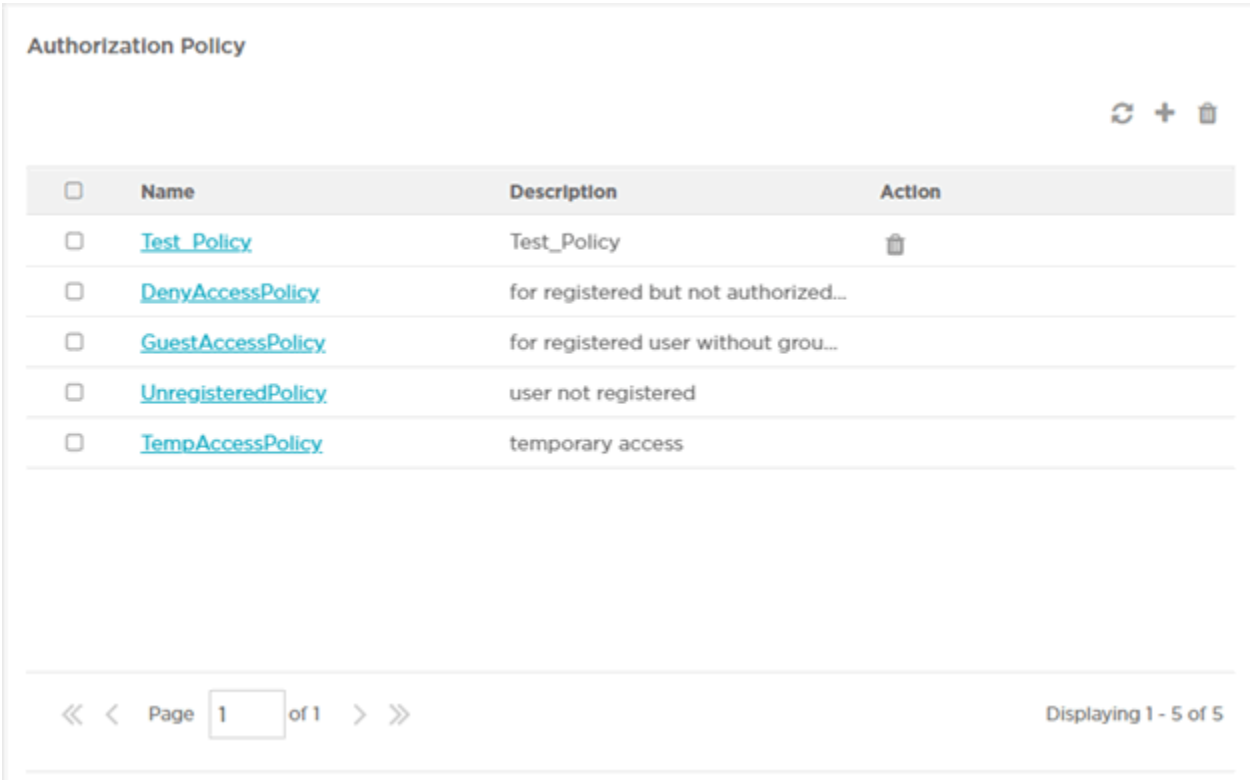


Figure 15: Authorization Policy Screen

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

Name
: Displays the unique name assigned to the Authorization Policy when it was created.

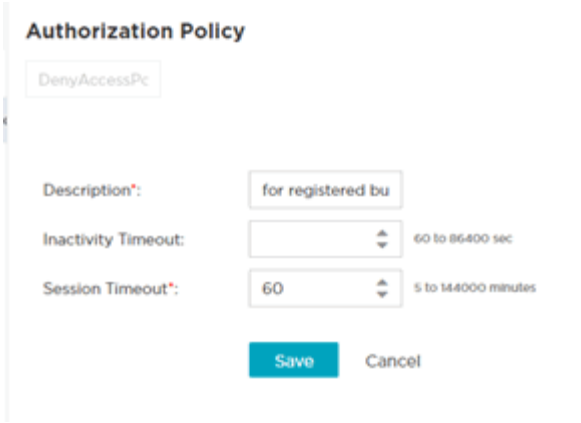
Description
: Displays the description entered when the Authorization Policy was created.

Action
: Select the icon to delete an existing Authorization Policy.

Default, System-provided Authorization Policies

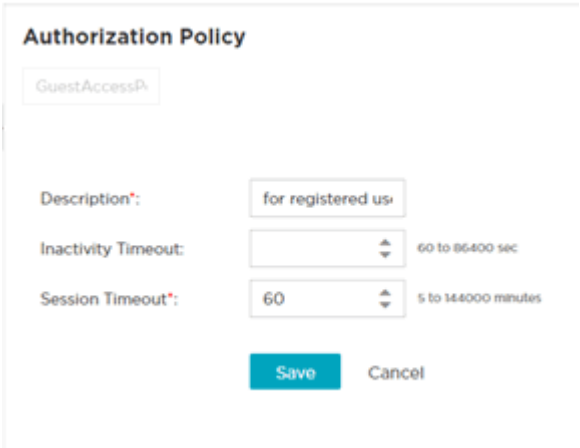
ExtremeGuest Essentials portal provides the following default Authorization Policies:

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



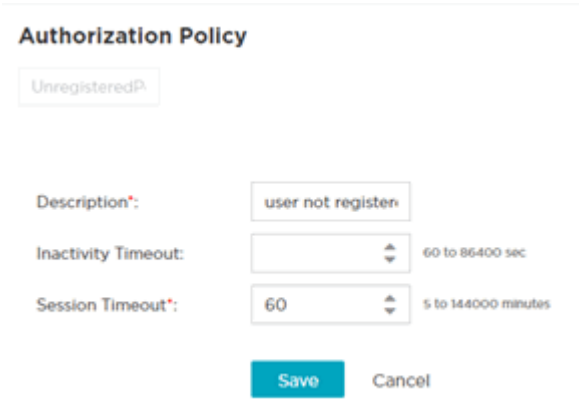
GuestAccessPolicy

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



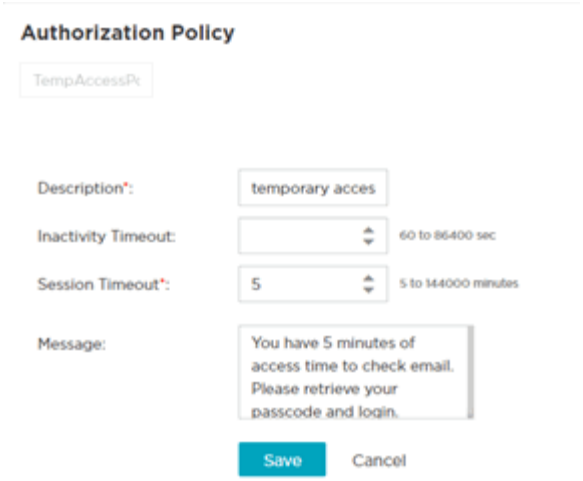
UnregisteredPolicy

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



TempAccessPolicy

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



Adding Authorization Policies

Configure → Settings → Authorization Policies → Add

To add an Authorization Policy:

1. Go to **Configure → Settings** .
   The **Authorization Policy** screen displays by default.
2. Select the + icon to add a new authorization profile.
   The add **Authorization Policy Add** screen displays.

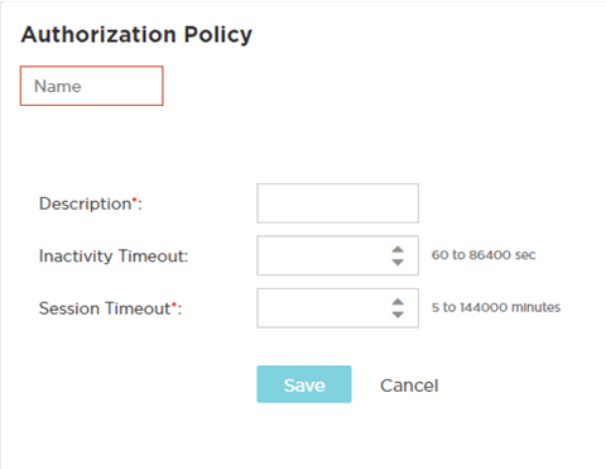


Figure 16: Authorization Policy Add Screen

3. Configure the following settings:

Name

Specify a unique designation for the new authorization policy.

Note
This setting is mandatory.

Description

Enter a description for the new authorization policy.

Note
This setting is mandatory.

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.

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

Access Groups

Configure → Settings → Access Groups

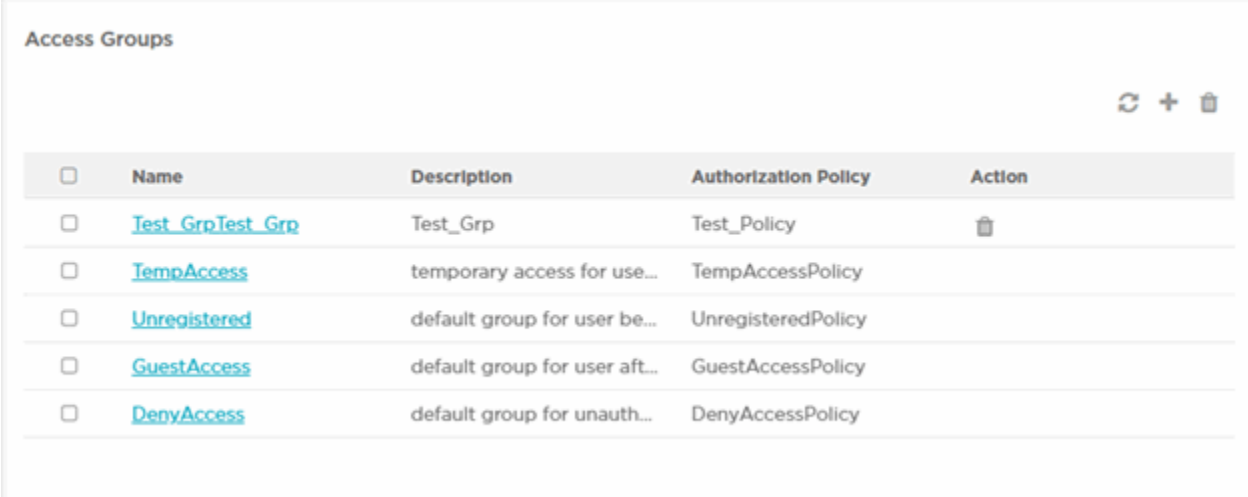


Figure 17: Access Groups Screen

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

Name

Displays the unique name assigned to the Access Group when it was created.

Description

Displays the description entered when the Access Group was created.

Action

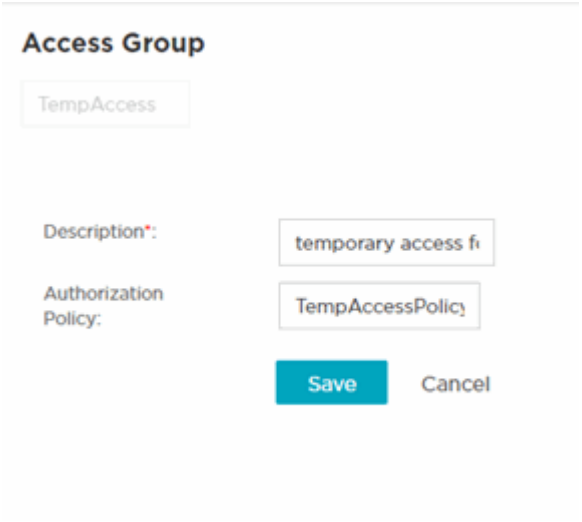
Select the icon to delete an existing Access Group.

Default, System-provided Access Groups

The ExtremeGuest Essentials portal provides the following default Access Groups that you can edit and use or use as is:

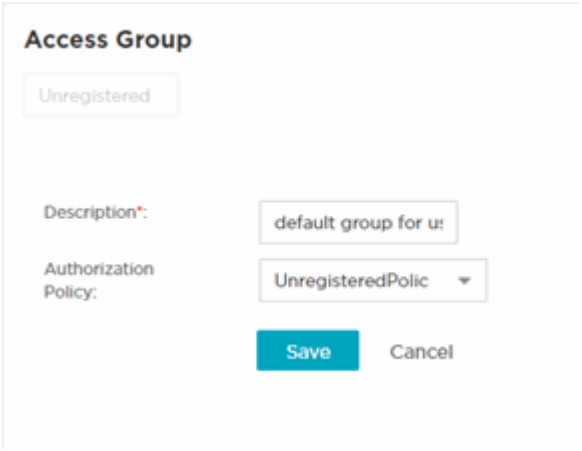
TempAccess

This is the default group applied for guests who have temporary access to your network. The Authorization Policy associated with this group is *TempAccess Policy*.



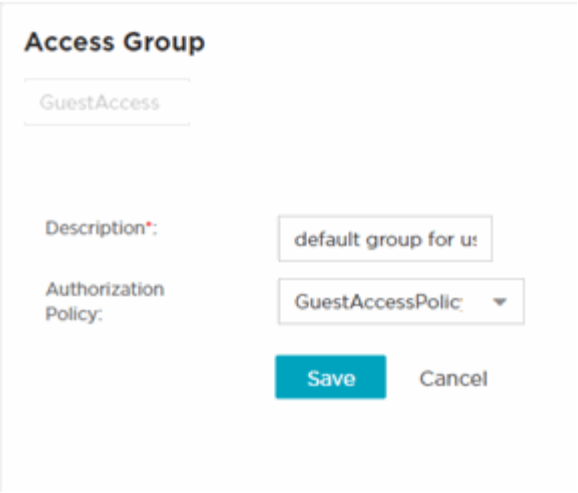
Unregistered

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



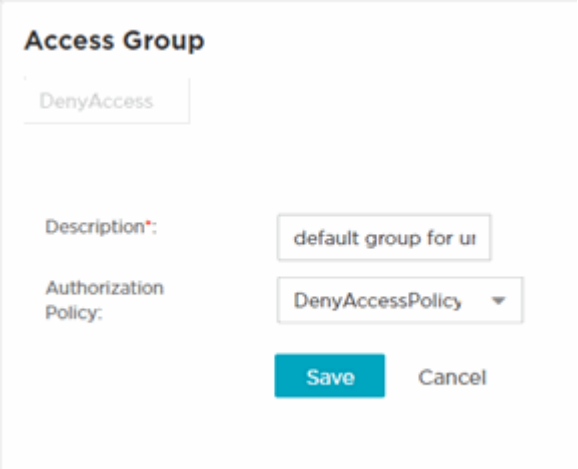
GuestAccess

This is the default group applied to users after they have registered. The Authorization Policy associated with this group is *GuestAccessPolicy*



DenyAccess

This is the default group applied to users who are already registered but are unauthorized to use the network. The Authorization Policy associated with this group is *DenyAccessPolicy*



Adding Access Groups

Configure → Access Settings → Access Groups → Add

To add Access Groups:

1. Go to **Configure → Access Settings → Access Groups** from the navigation menu.
   The **Access Groups** screen displays by default.
2. Select the + icon to create a new group.
   The Add Access Group screen displays.

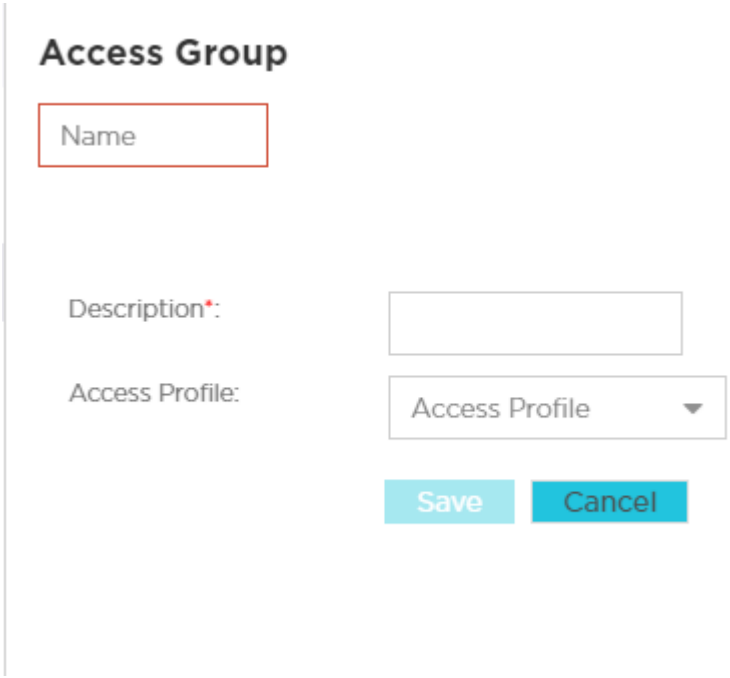


Figure 18: Access Groups Add Screen

3. Configure the following settings:

Name

Enter a unique name for the new Access Group.

Note
This setting is mandatory.

Description

Enter a description for the new Access Group.

Note
This setting is mandatory.

Access Profile

Select the Access Profile policy from the pull down menu. Available policy types are **`DenyAccessPolicy`**, **`GuestAccessPolicy`**, **`TempAccessPolicy`**, and **`UnregisteredPolicy`**.

4. Select **Save** to save your changes, or select **Cancel** to discard the new Access Group.

Deployment

Configure → Deployment

Deployment includes detailed user access information related to your locations, network, and devices..

Location

Configure > **Deployment** > **Location**

The **Location** screen lists sites attached to ExtremeGuest Essentials. It provides description and location information for sites.

1. From the main menu, go to **Configure** > **Deployment** > **Location**.

   A list of existing sites displays. Sites that are enabled display a green icon. Disabled sites display a gray icon. APs connected to disabled sites do not count against the licenses in use.

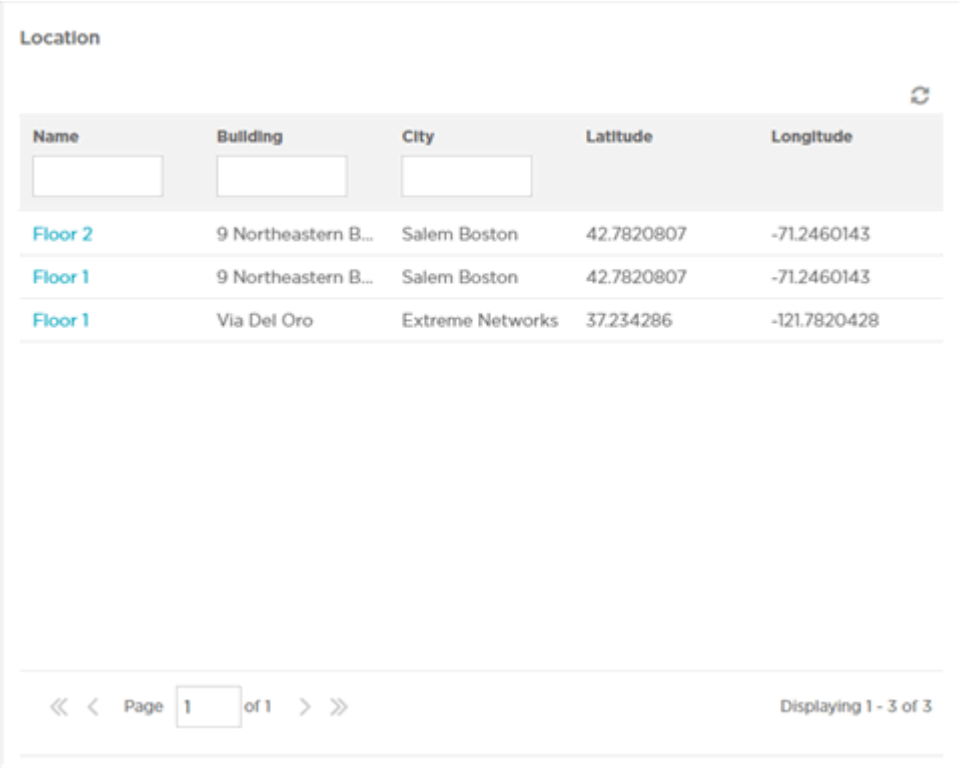


Figure 19: Location Screen

2. The **Location** screen displays the following:

   Name

Displays the name associated with each location. Double-click the required location name from the displayed list. The location details open as a dialogue box, where you can edit the location's **Name**, **Building**, **City**, **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.

Building

Displays the name of the building associated with the site.

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.

Latitude

Displays the latitude of the location.

Longitude

Displays the longitude of the location.

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

Network

Configure > **Deployment** > **Network**

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

1. From the main menu, go to **Configure** > **Deployment** > **Network**.

   A list of existing networks displays.

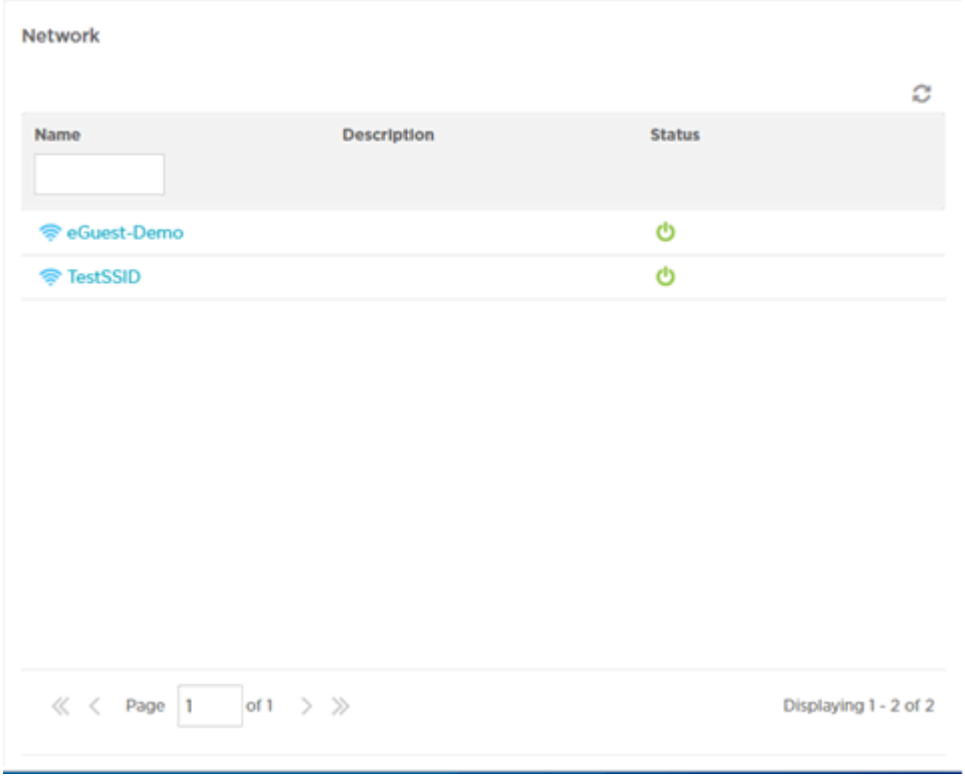


Figure 20: Network Screen

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**, and **Status**. To filter by name or portion of a name, enter the string in the box at the top of the **Name** column.

   Description

   Displays the optional description associated with each network.

   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.

3. Select the icon periodically to refresh the data.

Devices

Configure > **Deployment** > **Devices**

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

1. From the main menu, go to **Configure** > **Deployment** > **Devices** .

   The devices screen displays. It provides a list of known devices.

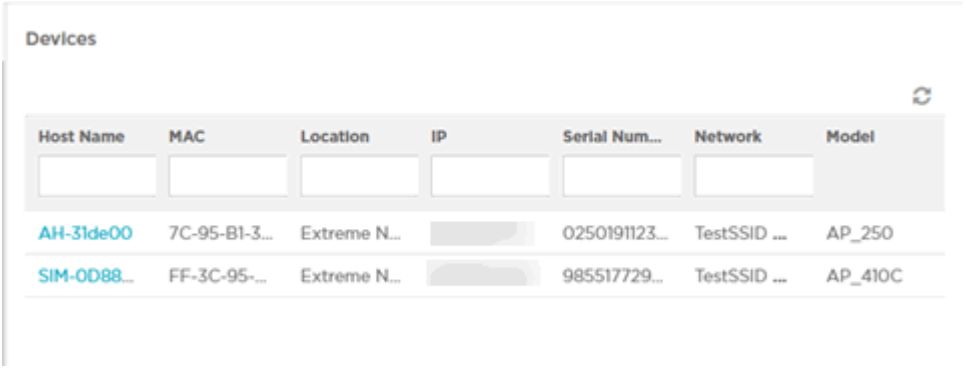


Figure 21: Devices Screen

2. Review the following information for existing devices:

   Name

   Displays the name associated with each device. Select the required device name from the displayed list. The **Edit Device** dialog box opens. Edit the device's **Name**, **MAC**, **Location**, **IP Address**, **Serial Number**, **Network**, and **Model** 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.

   Location

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.

3. Select the icon to update the data in the devices table.

Notification

Configure > **Notification**

The **Notification** screens allows you to configure and implement notification policies and rules. Notification policies specify the method used for all types of communication with guest user, such as communicating the pass code to newly registered guest users or sending a report to specified guest users. Refer to the following for more information:

- Policy on page 44

Policy

Configure > **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.

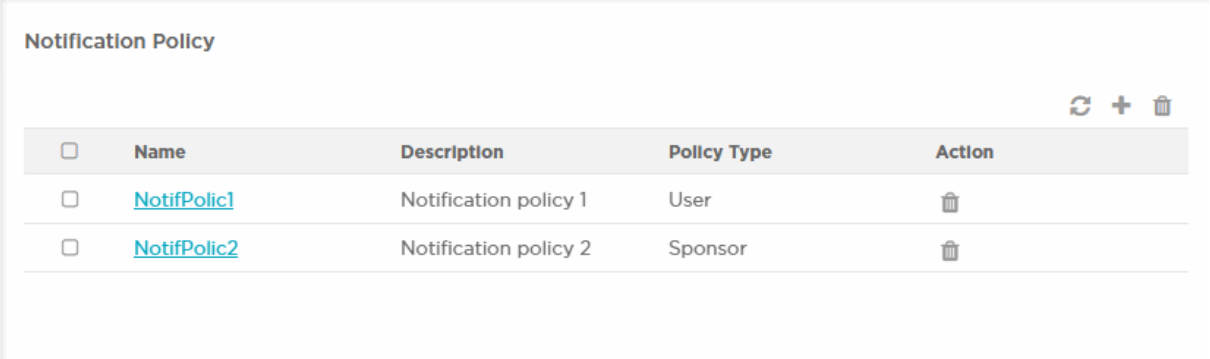


Figure 22: Notification Policy Screen

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.

Policy Type
: Displays the policy type entered when the notification policy was created.

Action
: Deletes a notification policy. To delete a policy, select the check box next to it and then select the icon associated with the policy.

Adding a Notification Policy

Configure → 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.
- Email - Uses an SMTP server.

To add a notification policy:

1. Navigate to **Configure → Notification → Policy** .
   The **Notification Policy** screen displays.
2. Select the icon to create a new policy.
   The add **Policy** screen displays.

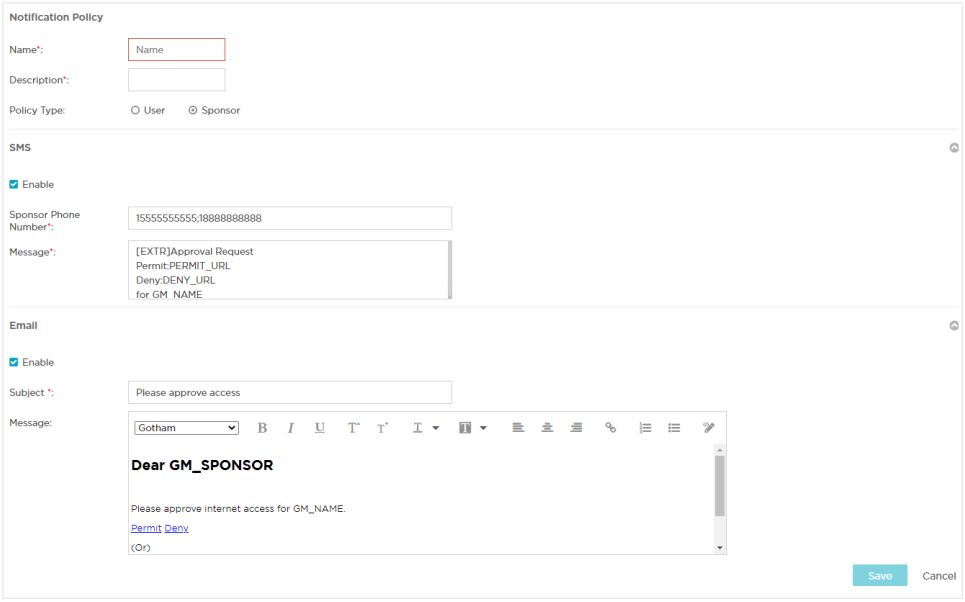


Figure 23: Notification Policy Add screen

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** Policy Type 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 **Sponsor Phone Number** field, enter the country code and phone number or multiple phone numbers with country codes separated by a semicolon. These are the phone numbers of the approvers for guest access. Providing more than one phone number ensures there are backup approvers available.
   c. In the **Message** field, specify the content of the SMS sent to the guest user notifying the passcode. The content should not exceed 1024 characters. For User Policy Type, use the following tags in the message: **GM_NAME** for the guest user's name, **GM_USERNAME** for the guest user's log-in name, and **GM_PASSCODE** for the pass code. For Sponsor Policy Type, use the following tags in the message: **GM_SPONSOR** for the name of the sponsor, **GM_NAME** for the guest user's name, **GM_USERNAME** for the guest user's log-in name, **PERMIT_URL** to permit access, **DENY_URL** to deny access, and **GM_PASSCODE** for the passcode.

      For example (User Policy Type):

```
[EXTR]Dear GM_NAME, Your username is GM_USERNAME &
passcode is GM_PASSCODE for internet access.
Powered by Extreme Networks.
```

(In the actual message, the tags are replaced with the user's name, username, and passcode.)

For example (Sponsor Policy Type):

```
[EXTR]Internet Access details for GM_USERNAME
Username: GM_USERNAME
Passcode: GM_PASSCODE
Powered by Extreme Networks.
```

(In the actual message, the tags are replaced with the user's name, username, and passcode.)

Note
The prefix **[EXTR]** (optional) in the message field is a filter to prevent notifications from being interpreted as spam, causing them to be blocked .

Enabling Email notifications

7. To enable email notifications, click the icon to open the email configuration fields.
   a. Select **Enable** the policy. When enabled, notifications are sent to newly registered guest users via email.
   b. In the **Subject** field, configure the subject line of the email sent to the guest user notifying the pass code (should not exceed 100 characters).
   c. In the **Message** field, configure the content of the email sent to the guest user notifying them of a pass code (should not exceed 1024 characters).
8. Select **Save** to save your changes or select **Cancel** to discard the notification policy.

Onboarding

Configure > **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 48
- Onboarding Rules on page 51

Onboarding Policy

Configure > **Onboarding** > **Policy**

Onboarding policies are used by ExtremeGuest Essentials 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. From the main menu, go to **Configure** > **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.

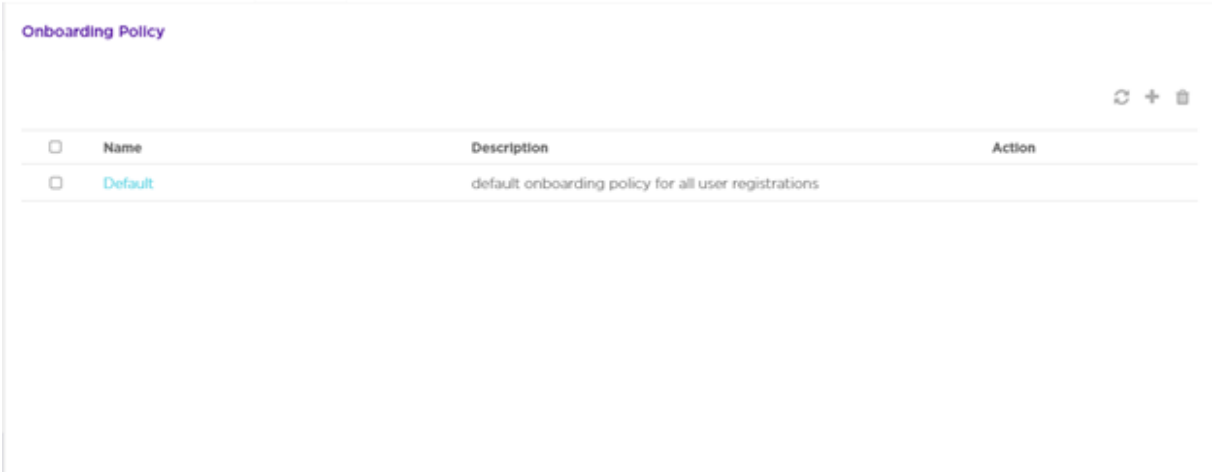


Figure 24: Onboarding Policy Screen

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 Essentials.

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

Adding an Onboarding Policy

4. To add a new onboarding policy, select the + icon.
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** If you select this condition, an additional Value condition field displays. Enter the domain in the Value field.

     Note
     Enter "Any" (case sensitive) in the Value field to indicate any email address, regardless of domain. Use "Any" when you want to allow or deny all users to access the network.

   - **Sponsor Email Domain** If you select this condition, an additional Value condition field displays. Enter the domain in the Value field.
   - **Social Type** If you select this condition, an additional condition field displays. Select the type of social media (Facebook, Google, LinkedIn) from the drop-down list.
   - **User Type** If you select this condition, an additional condition field displays. Select the user type (Employee, Vendor, Guest) from the drop-down list.
   - **User's Device Count** an additional condition field displays. Select the number of devices being used from the drop-down list.
   - **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. To remove multiple onboarding policies from ExtremeGuest Essentials, select the boxes for each policy then select the icon.

Onboarding Rules

Configure > **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. From the main menu, go to **Configure** > **Onboarding** > **Rules**
   The **Onboarding Rules** screen displays 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

Displays the you can use to remove the associated onboarding rule from ExtremeGuest Essentials.

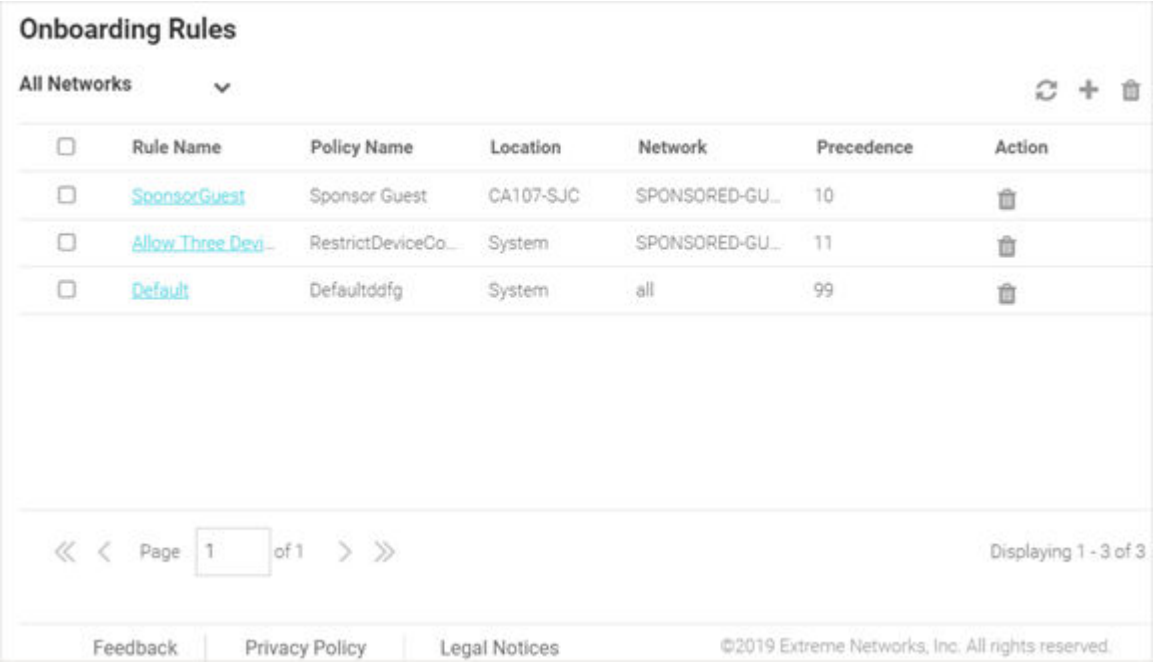
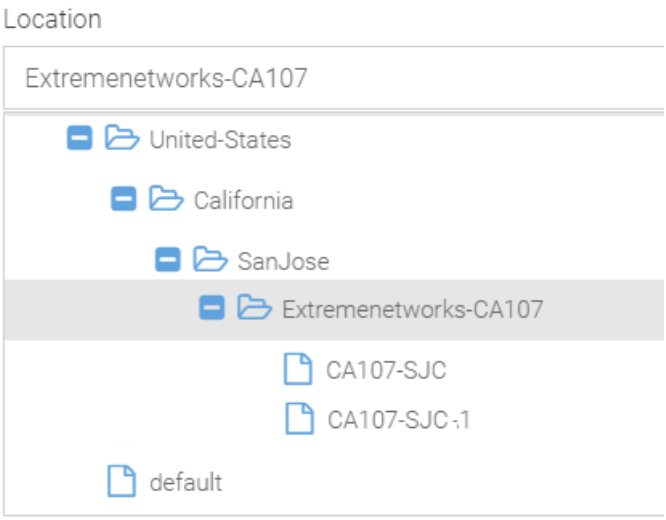
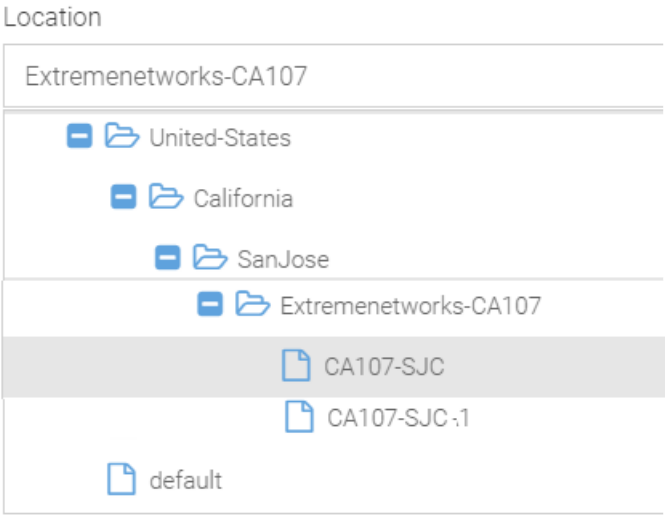


Figure 25: Onboarding Rules Screen

2. Select the icon to update the data in the onboarding rules list.
3. Select the icon to add a new onboarding rule.
4. Select the icon to remove onboarding rules.
5. 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.
6. Use the **Location** pull-down menu to navigate the system tree and select the location(s) to which the onboarding rule will apply.
   Starting with this release onboarding rule can be applied at any point on the location tree. You can either select the endpoint of the location tree (representing an RF Domain) or a node higher up in the tree. In the following screen shot, selecting '**Extremenetworks-CA107**' applies the rule to both RF Domains '**CA107-SJC**' and '**CA107-SJC-1**'.



In the following screen shot the rule has been applied only to the '**CA107-SJC**' RF Domain.



When a client registration request is received from the network specified in Step 4 above, the onboarding rule is applied only if the client's RF Domain matches the locations specified here. In the above scenario the match criteria is only 'CA107-SJC', whereas in the previous scenario it is 'CA107-SJC' and 'CA107-SJC-1'. Once the 'Network' and 'Location' criteria match, the onboarding policy associated with the rule is applied.

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

   Note
   The lower the precedence value, the higher the priority. Rules with lower precedence will be applied first.

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

9. To remove multiple onboarding rules from ExtremeGuest Essentials, select the boxes for each policy then select the trashcan icon.

Splash Templates

Configure > **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 Essentials system templates:

1. From the main menu, go to **Configure** > **Splash Templates**.
   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.

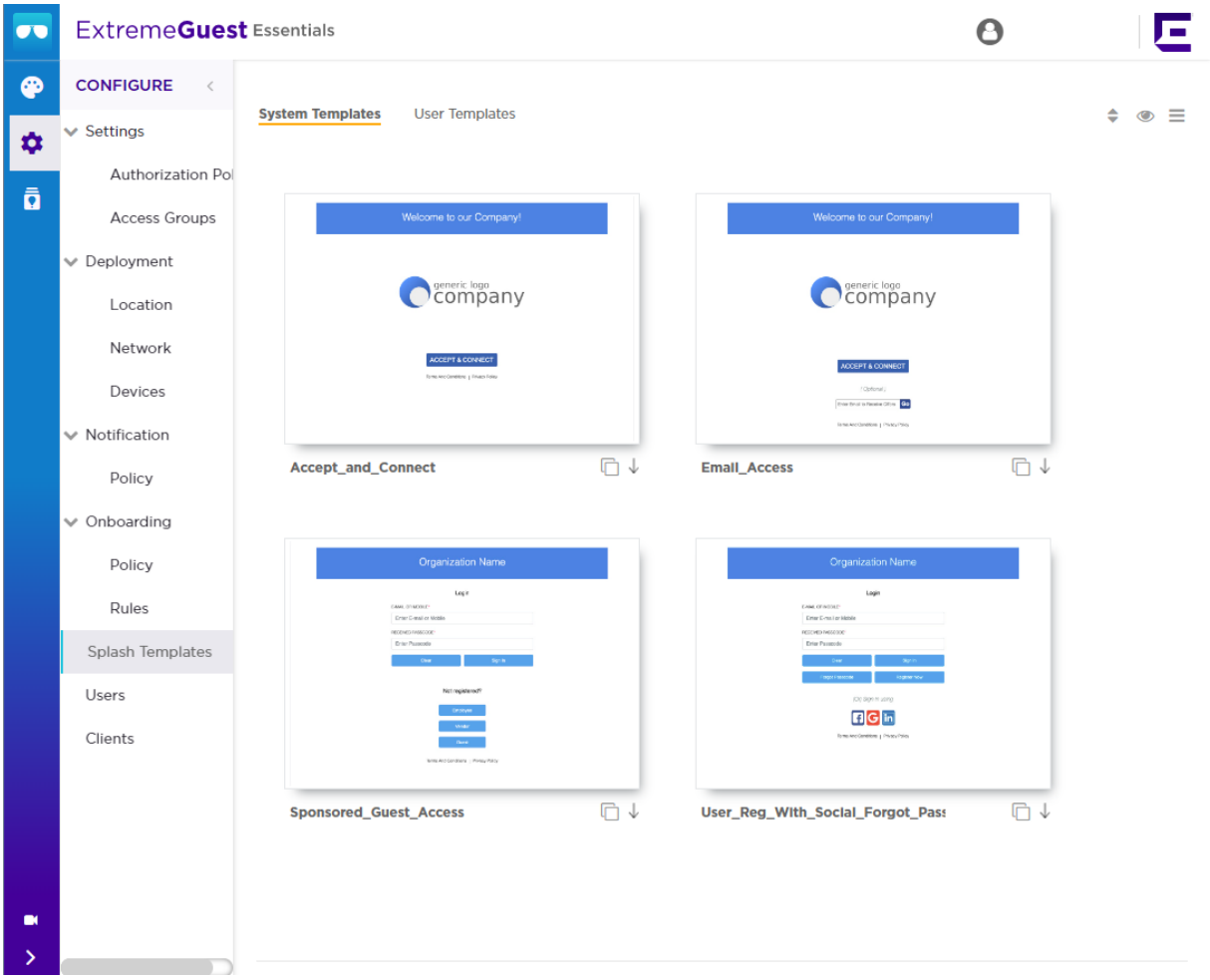


Figure 26: System Templates Screen

Note

Four common System Templates are shown. You can select the **eye** icon in the upper right to show all available System Templates.

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 Wi-Fi access with a simple Accept & Connect button. Selecting this button provides internet access and also registers the device with ExtremeGuest Essentials.

Accept_and_Connect_with_terms_and_agreement

Splash template to use for free Wi-Fi access with a simple Accept & Connect button and a hyperlink to view terms and conditions. Selecting this button

provides internet access and also registers the device with ExtremeGuest Essentials.

Device_Registration_with_Social_WiFi

Splash template to use for free Wi-Fi access with a customizable registration form and social sign-in options. Guest users' devices are registered along with their registration or social profile details with ExtremeGuest Essentials.

Email_Access

Splash template to use for free Wi-Fi access with an option to capture guest users' **Email Addresses** or **Mobile Numbers**. Guest users' devices are registered along with their email addresses or mobile numbers with ExtremeGuest Essentials.

Social_WIFI_with_Facebook_and_GooglePlus

Splash template to use for free Wi-Fi access with Facebook or GooglePlus social sign-in options. Guest users' devices are registered along with their social profile details with ExtremeGuest Essentials.

Social_WIFI_with_all

Splash template to use for free Wi-Fi access with customizable Facebook/ GooglePlus/LinkedIn social sign-in options. Guest users' devices are registered along with their social profile details with ExtremeGuest Essentials.

Sponsored_Guest_Access

Splash template to use for sponsored Wi-Fi access for different category of users. For example, employees can self-register their devices, and guests and vendors can request the sponsor to approve the Wi-Fi access.

User_Reg_with_Social_Forgot_Passcode

Splash template to use for free Wi-Fi 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 Essentials. Each 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.

User_Registration_with_Social_WIFI

Splash template to use for free Wi-Fi 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 Essentials. Each guest user receives a One-Time-Passcode/Passcode to sign-in to the network.

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 59.

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.

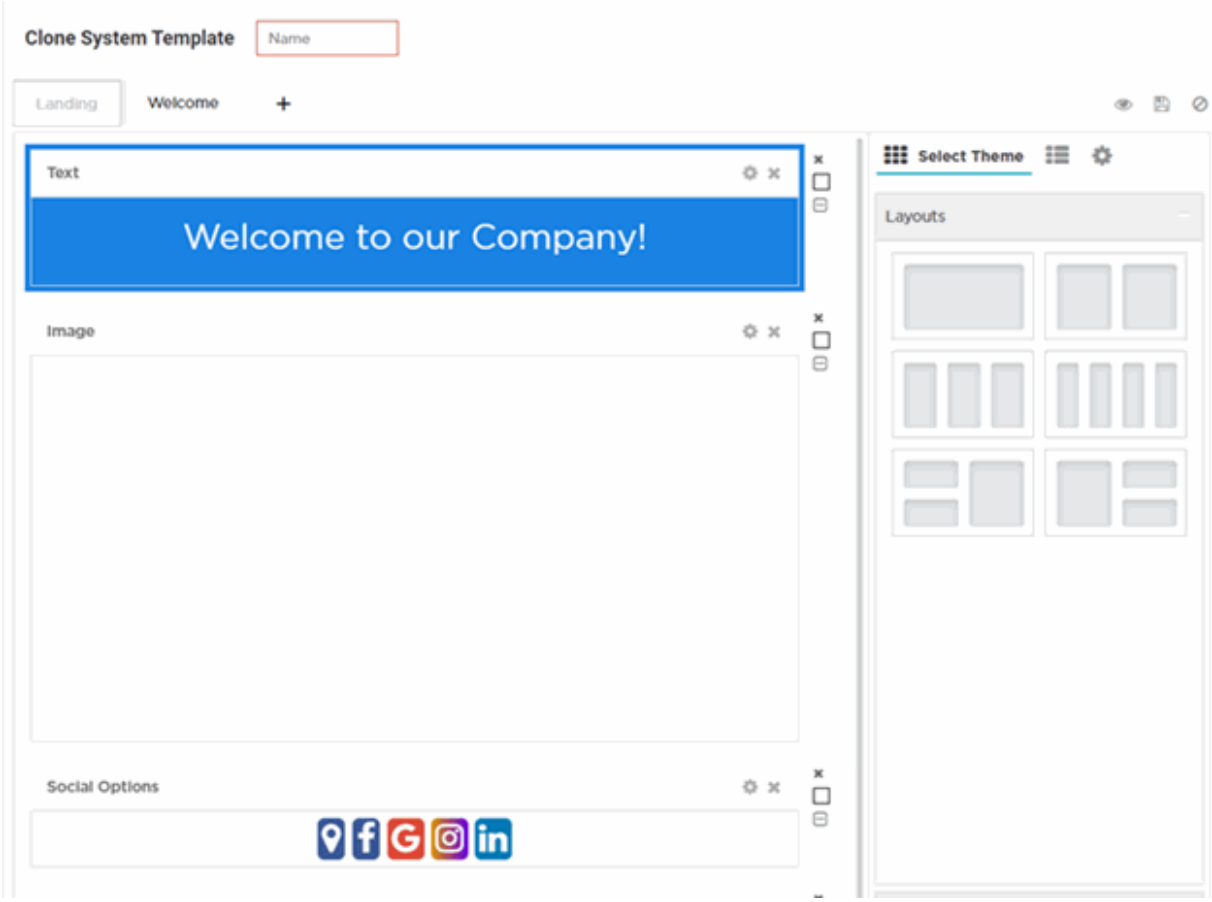


Figure 27: Clone System Template Screen

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 59 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.

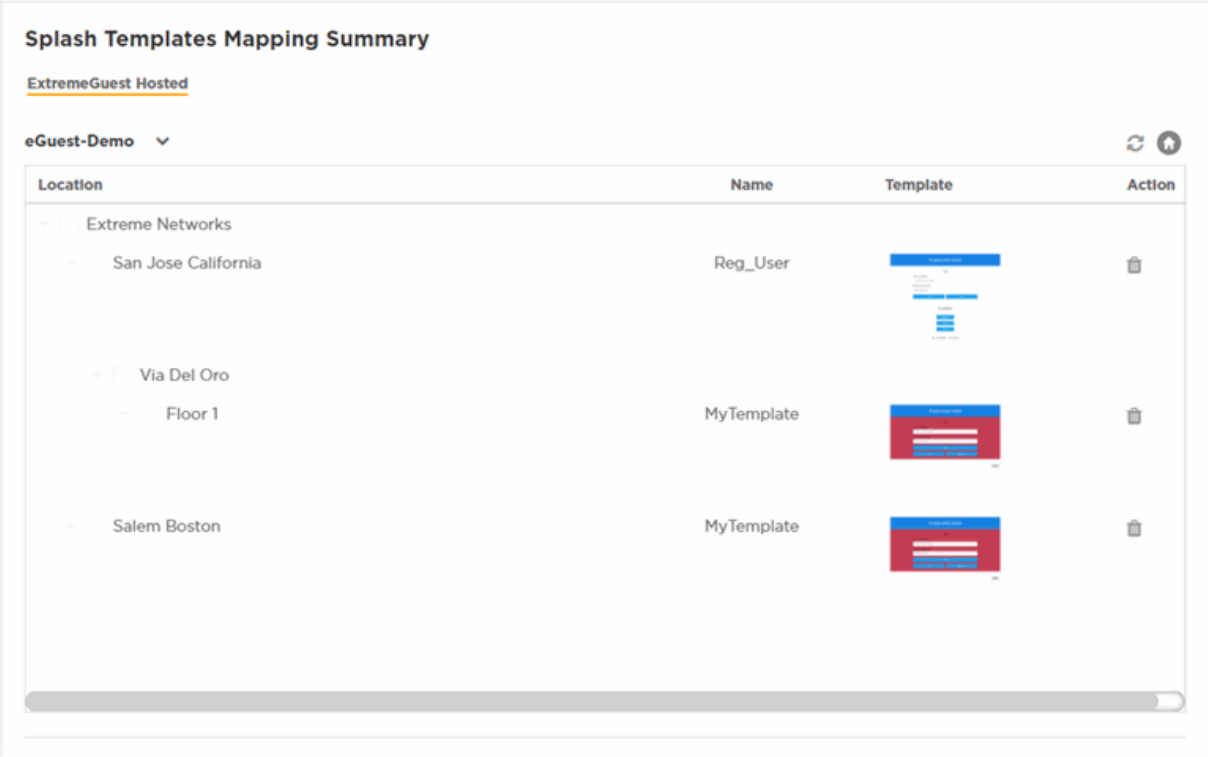


Figure 28: Summary View Screen

In the **Summary View**, the **ExtremeGuest Hosted** templates are listed. These templates are hosted directly on ExtremeGuest Essentials.

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 Essentials.

User Templates

Configure > **Splash Template** > **User Templates**.

The **User Templates** screen displays a summary of captive portal splash templates hosted by ExtremeGuest Essentials.

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.

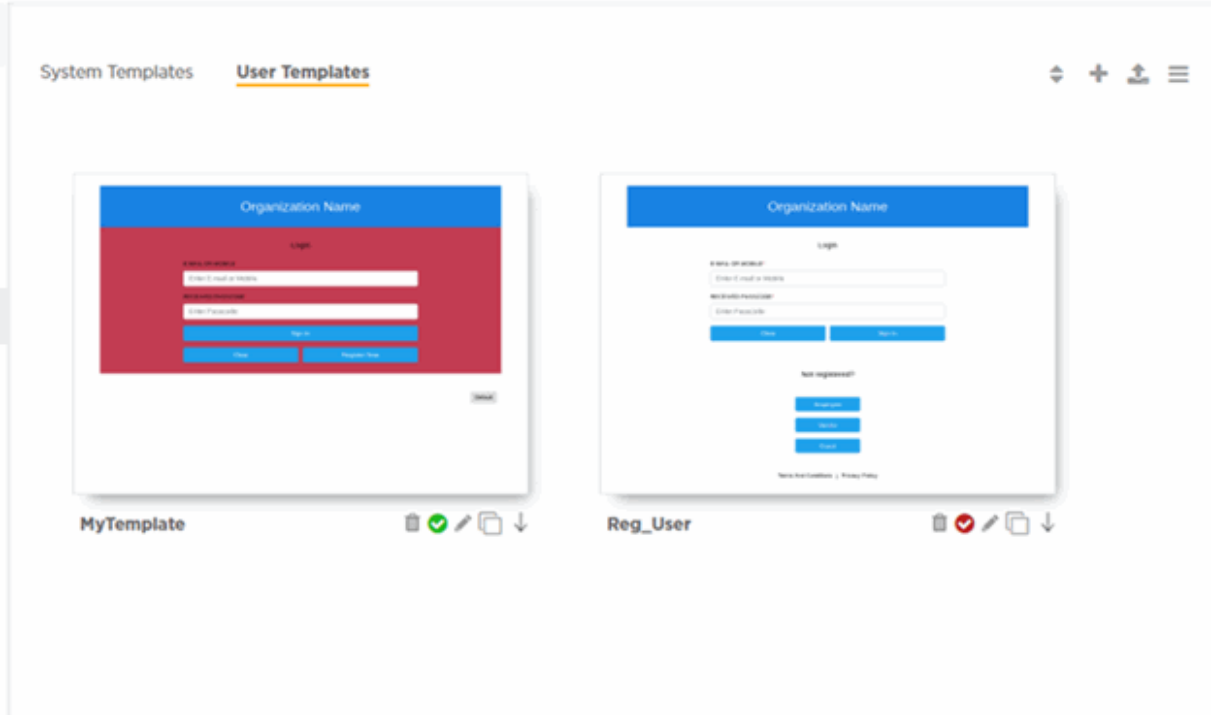


Figure 29: Splash Template - User Templates Screen

2. Select the icon at the top right corner of the screen.

   The **Upload Template** window opens.

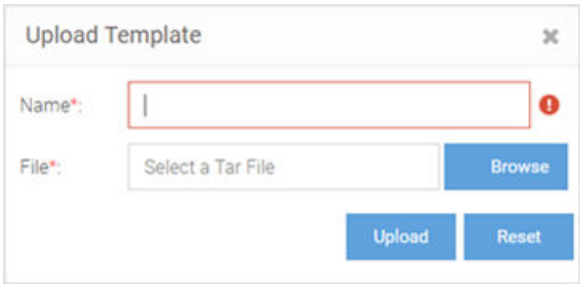


Figure 30: User Templates - Upload Template Screen

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 Essentials 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.

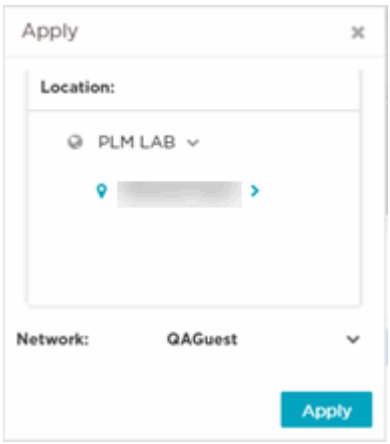


Figure 31: Apply Template to Network Screen

Refer the table below for details:

Location	Map the captive portal page with one or more locations. When mapped, the APs within one or more locations serve the captive portal pages to guest users, either directly or through the ExtremeGuest Essentials web server. 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 any one of the upper nodes (country, state, region, or campus) to apply the captive portal pages to multiple sites.
Network	Select 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.

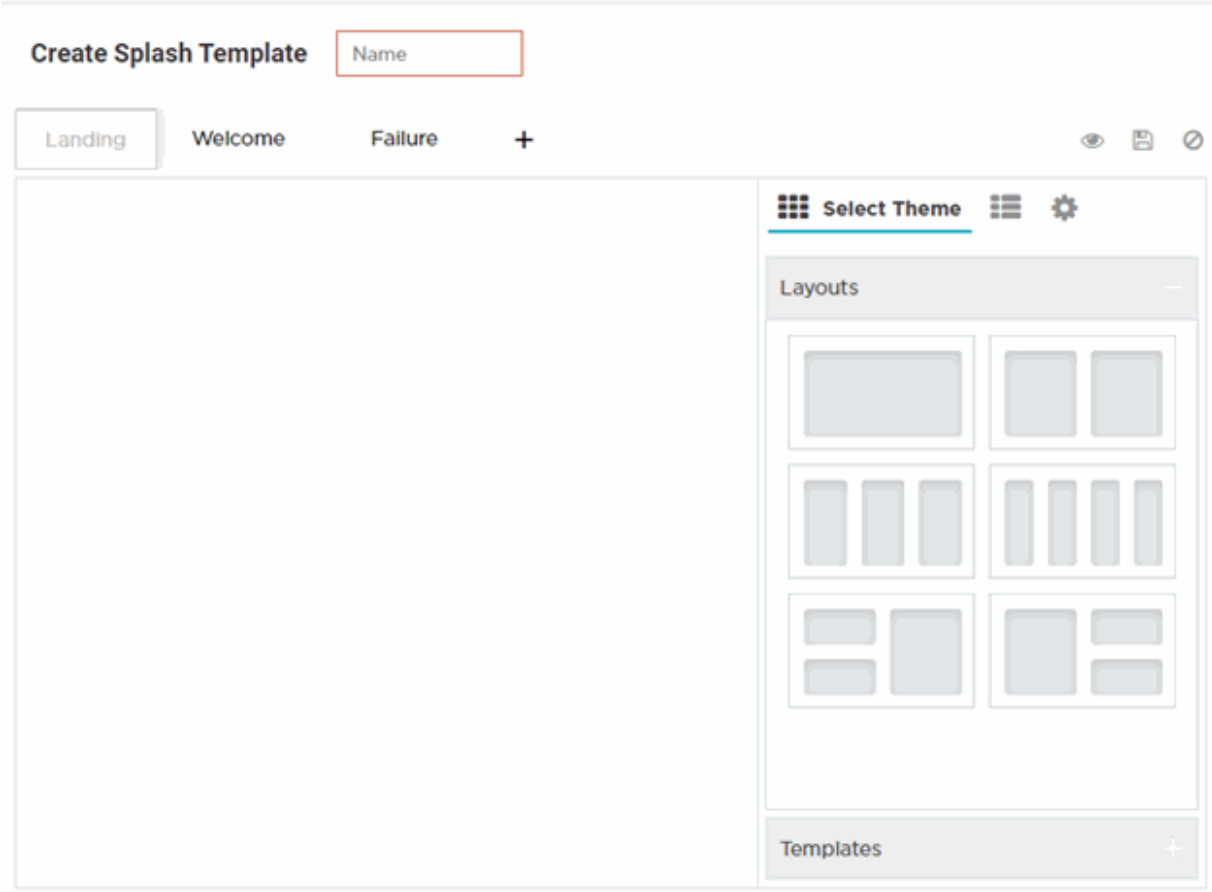


Figure 32: Create Splash Template Screen

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`** page.

> **Note**
> You can remove all other splash template pages except the **`Landing`** page. To remove a page, place 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 onto 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 onto 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.

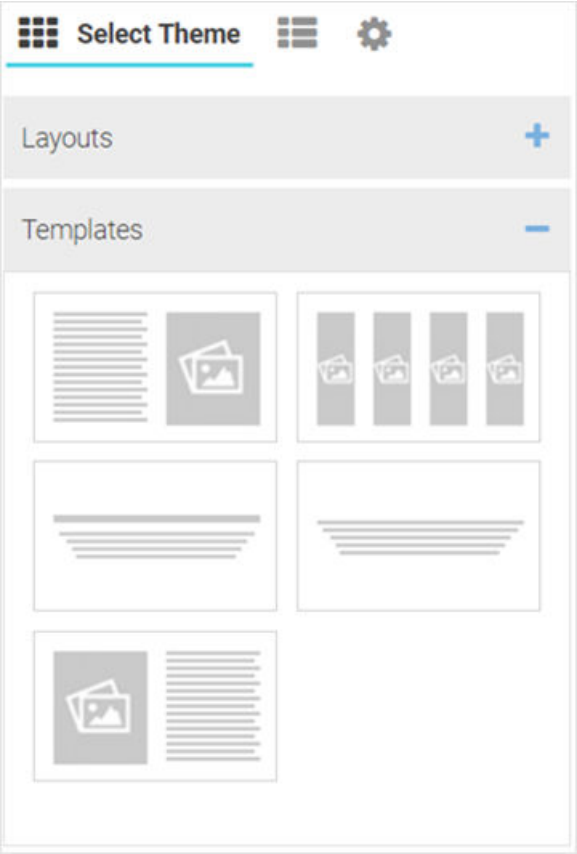


Figure 33: Create Splash Template - Select Theme Options

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.

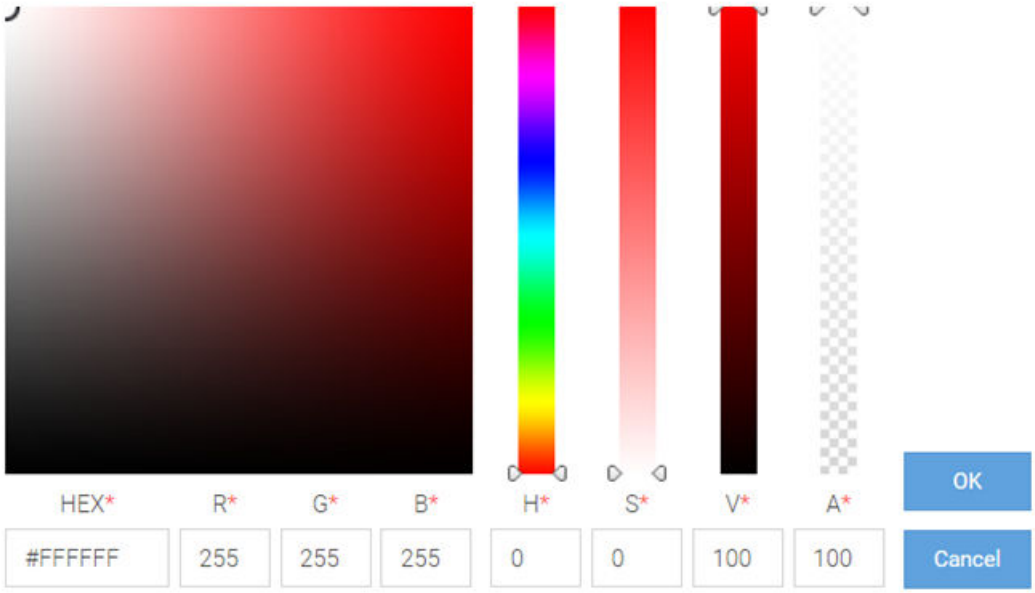


Figure 34: Create Splash Template - Built-in Color Palette

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.

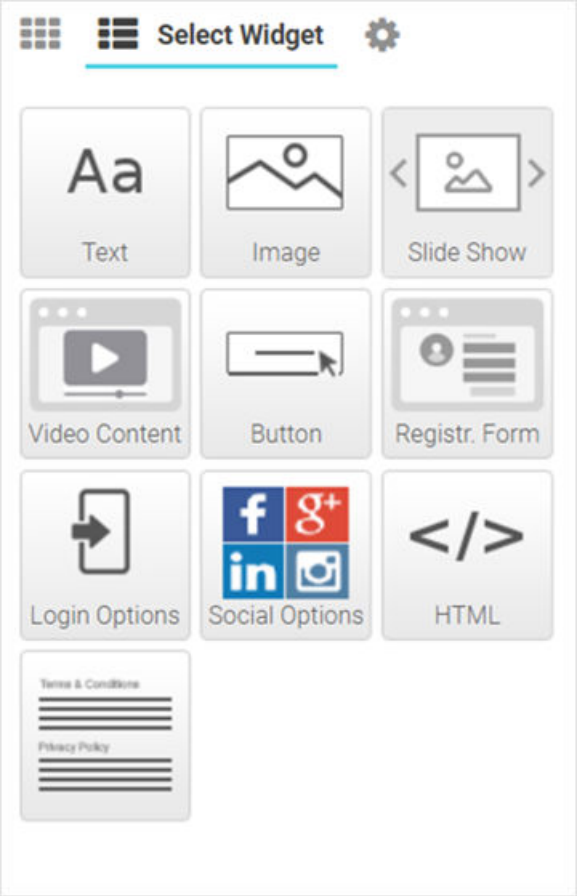


Figure 35: Create Splash Template - Select Widget Options

19. Drag and drop a widget into the layouts/templates on the splash page. The 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 Essentials 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.

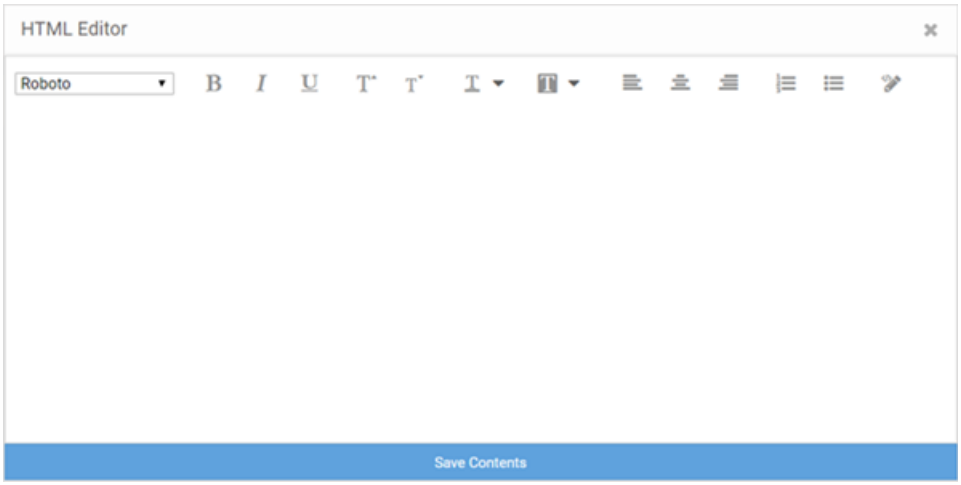


Figure 36: Create Splash Template - Text Widget - HTML Editor

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.

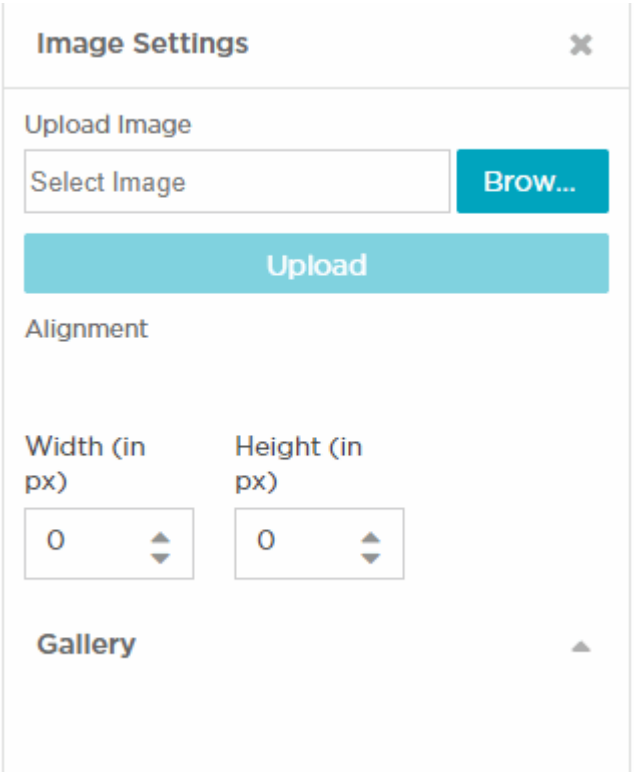


Figure 37: Image Widget Settings

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.

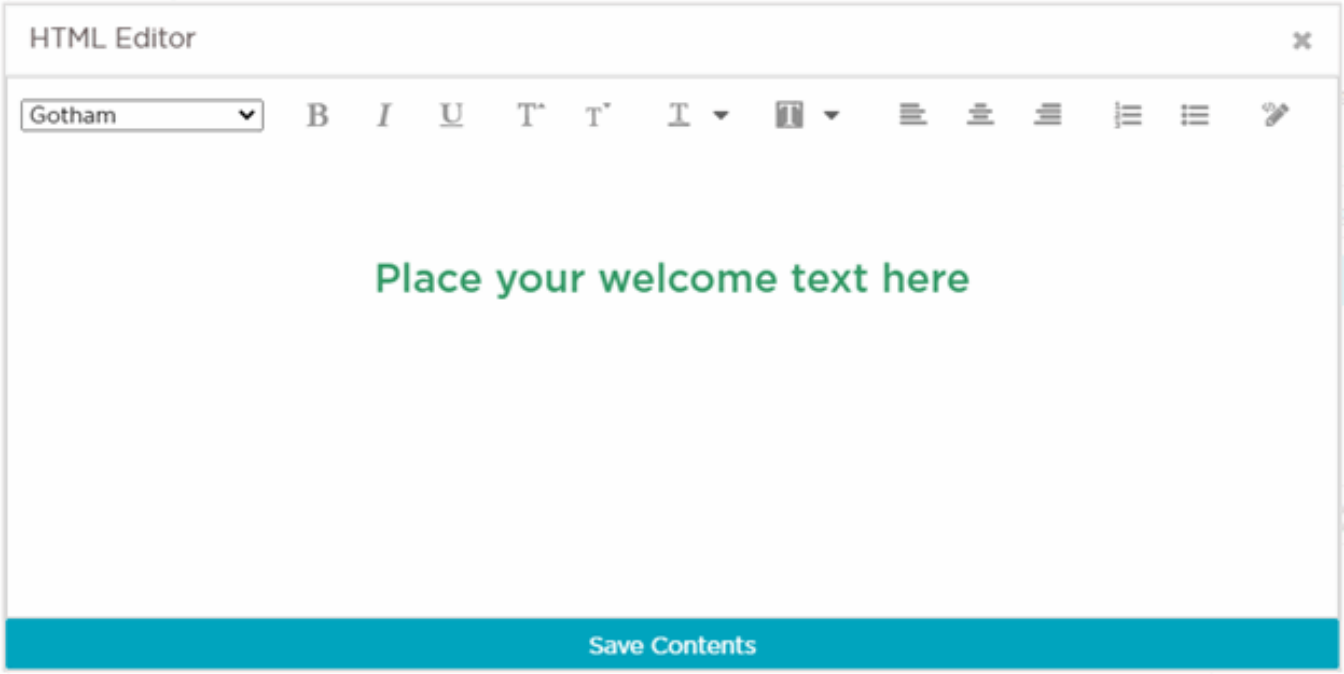


Figure 38: Create Splash Template - HTML Widget - HTML Editor

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.

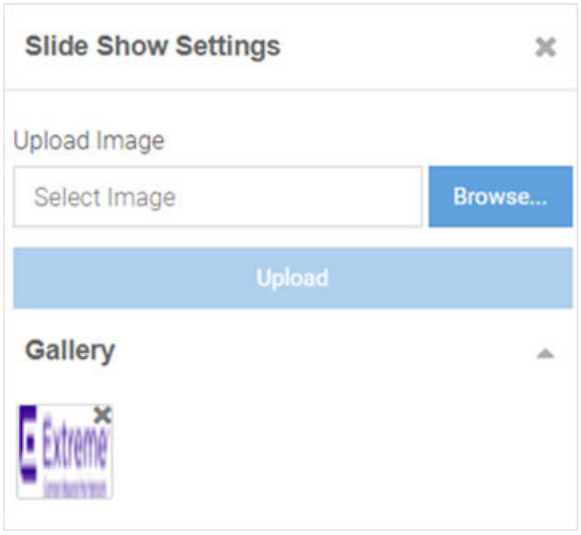


Figure 39: Create Splash Template - Slide Show Settings Panel

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.

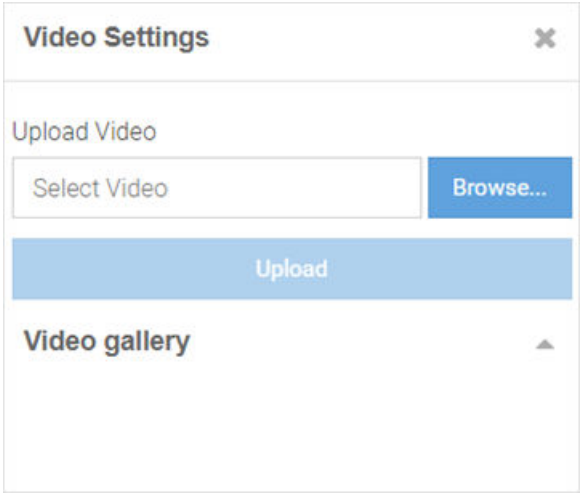


Figure 40: Create Splash Template - Video Settings Panel

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 predefined URL.

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

    The **Button Settings** panel displays.

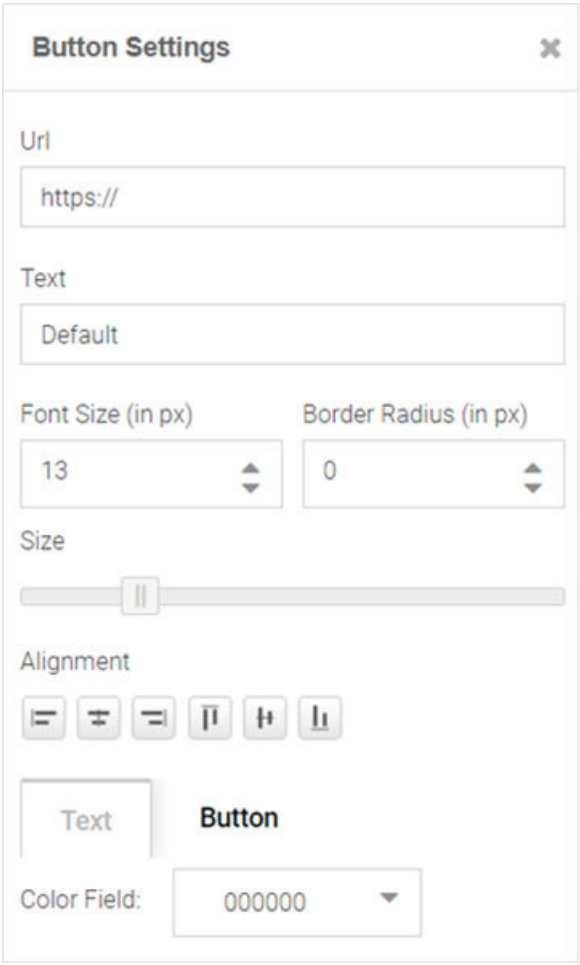


Figure 41: Create Splash Template - Button Settings Panel

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

Back to Widget Options Table

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.

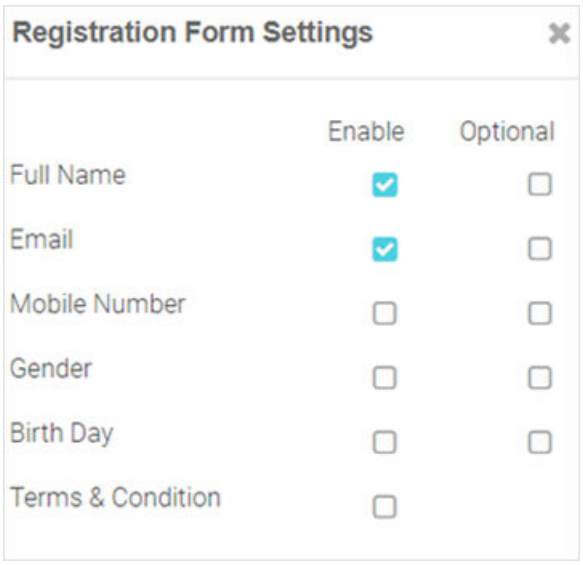


Figure 42: Create Splash Template - Registration Form Settings Panel

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 **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.

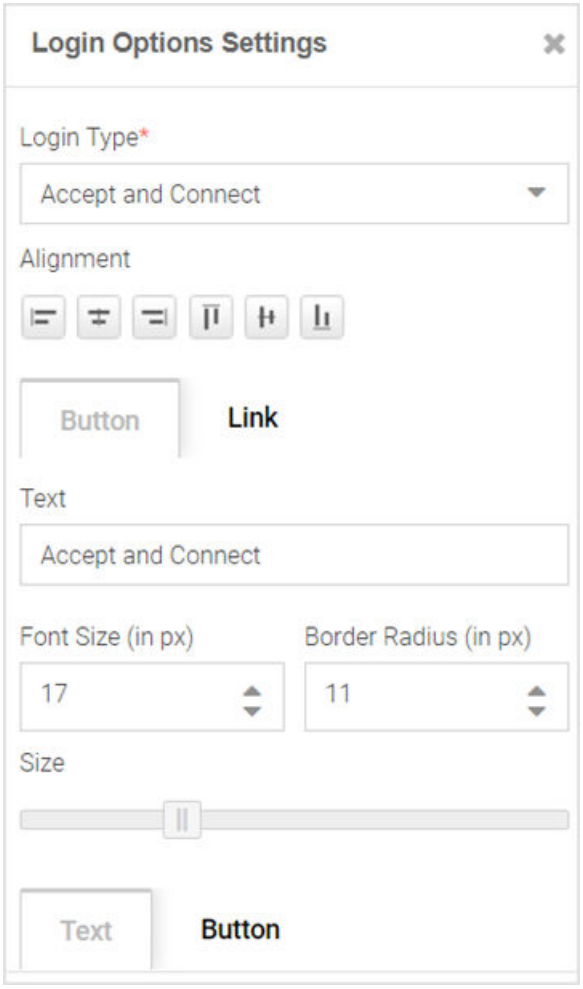


Figure 43: Create Splash Template - Login Options Settings Panel

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`**, **`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.

The **Social Options Settings** panel.

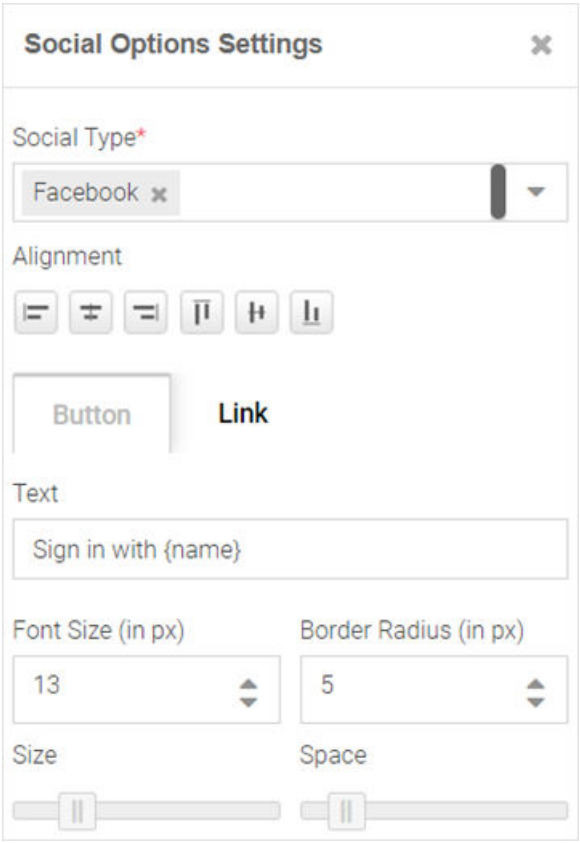


Figure 44: Create Splash Template - Social Options Settings Panel

Social Type	Use this drop-down menu to select the social media sign-in options. **Note:** Available options are: **`Facebook`**, **`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.

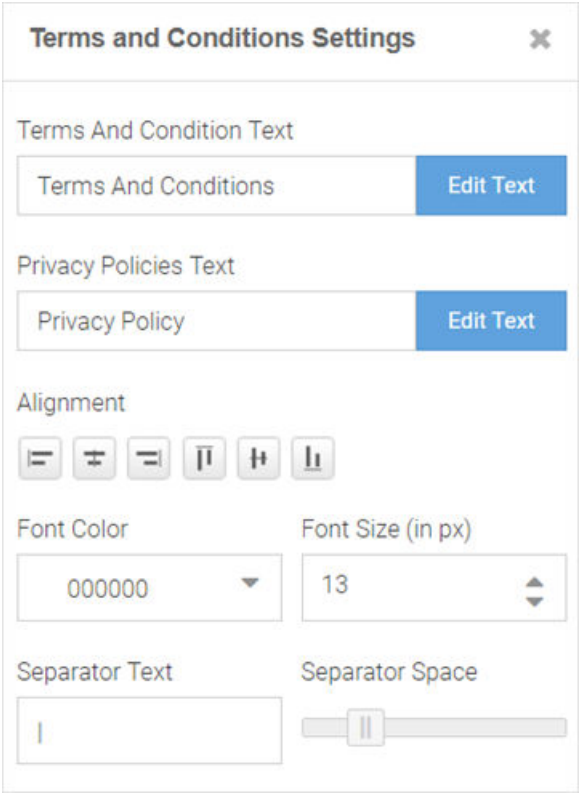


Figure 45: Create Splash Template - Terms And Conditions Settings Panel

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.

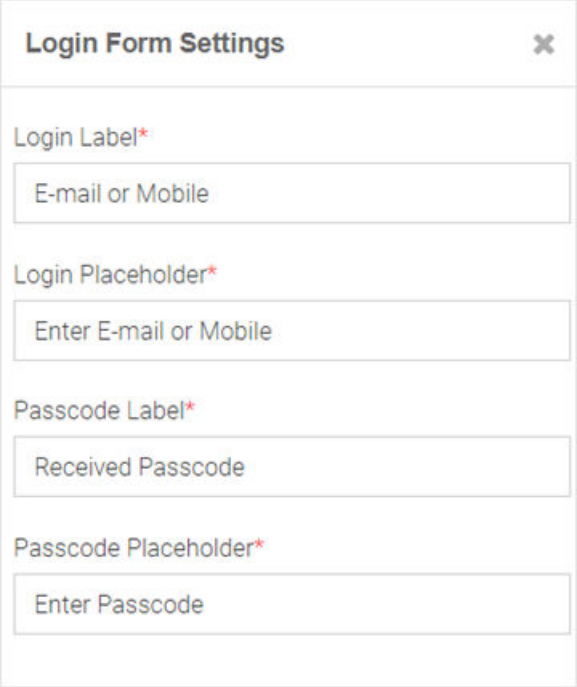


Figure 46: Create Splash Template - Login Form Settings Panel

The login form allows guest users to enter their username and passcode registered with the ExtremeGuest Essentials 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.

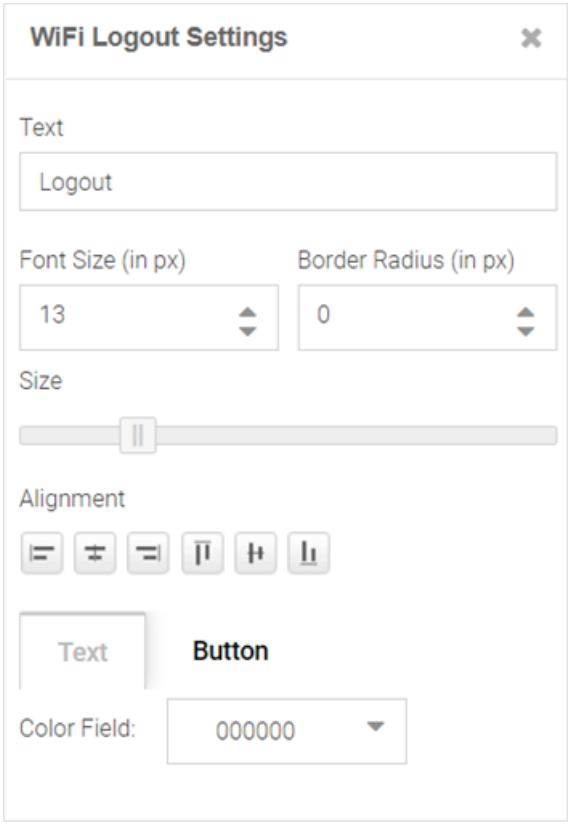


Figure 47: Create Splash Template - Logout Button Settings Panel

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.

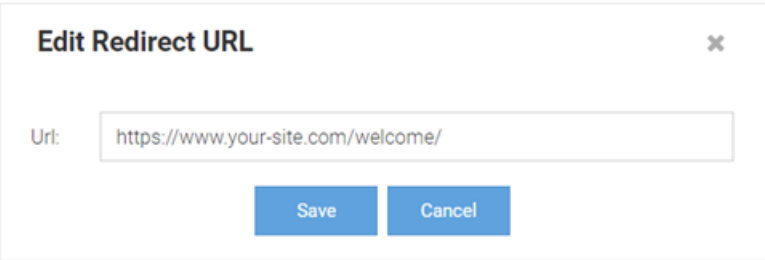


Figure 48: Create Splash Template - Edit Redirect URL Box

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.

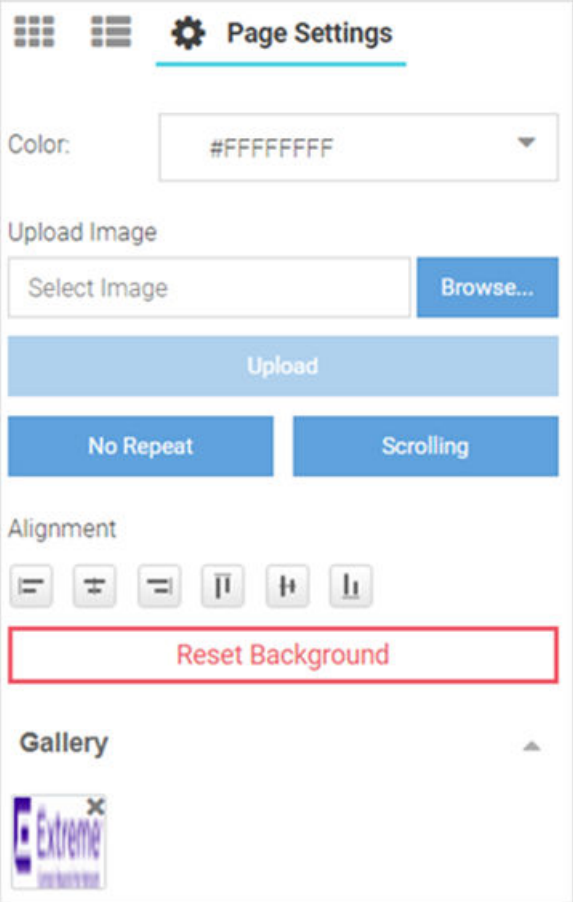


Figure 49: Create Splash Template - Select Page Settings Options

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.

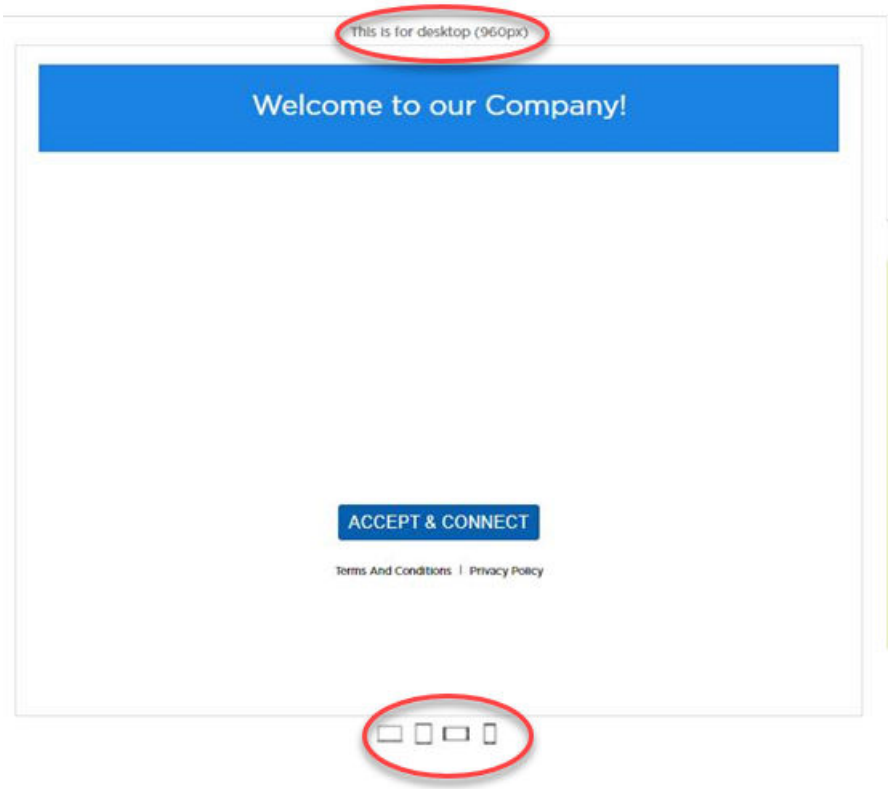


Figure 50: Create Splash Template - Device Type and Orientation Settings

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.

Configure Users

Configure > **Users**

The **Users** table displays detailed information about the users in your network.

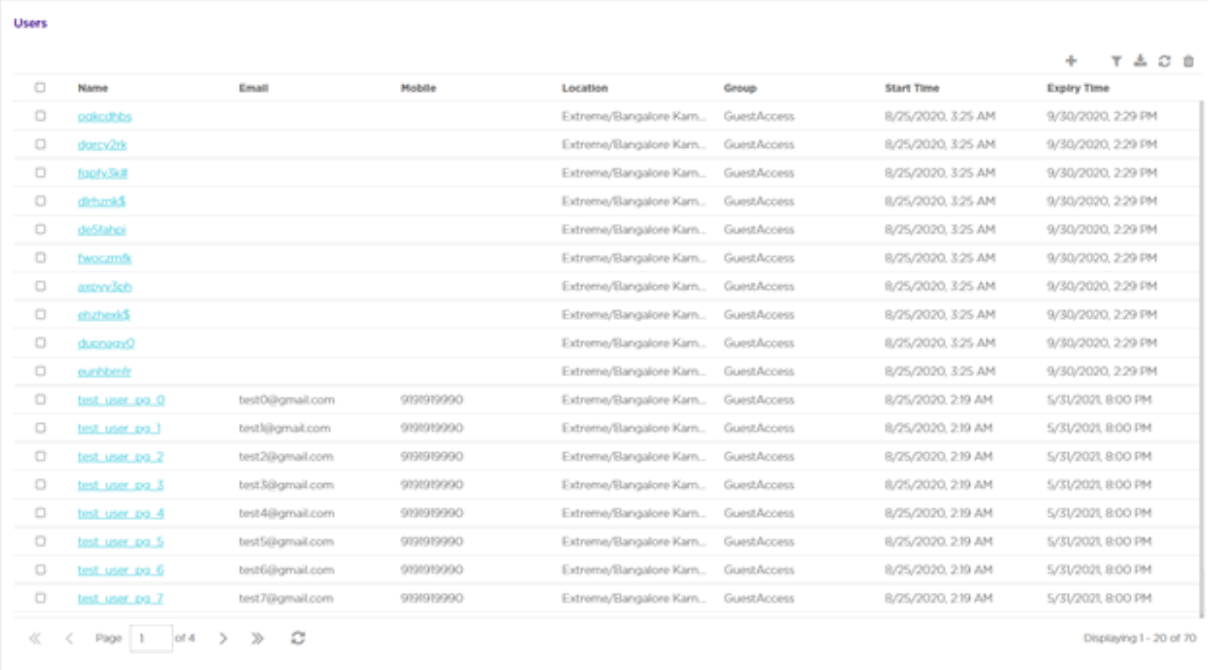


Figure 51: Configure Users Screen

Use the tools at the top right corner of the table to perform the following functions:

- Add - Create a new user.
- Filer - Filter the data in the table
- Download - Download user data
- Refresh - Update the data in the table
- Delete - Remove user data from the table

The **Users** table includes the following columns:

Name

The first and last name of the user.

Email

The email address for the user.

Mobile

The user's cellphone number.

Location

The location to which the user is associated.

Group

The access group to which the user is associated.

Start Time

The starting date and time that the user was first active.

Expiry Time

The date and time that the user was no longer active.

Create Users

Configuration → Users → Create Users

You can create new users and add them to your network from the Configuration → Users → Create Users tab.

Note
You can also configure ExtremeGuest Essentials Users using the HelpDesk Feature in ExtremeCloud IQ.

To create a user:

1. Navigate to **Configuration → Users** from the main menu.
2. Select the Add icon at the top right corner of the page.
3. Select **Create Users**.
   The **Create Users** tab displays.

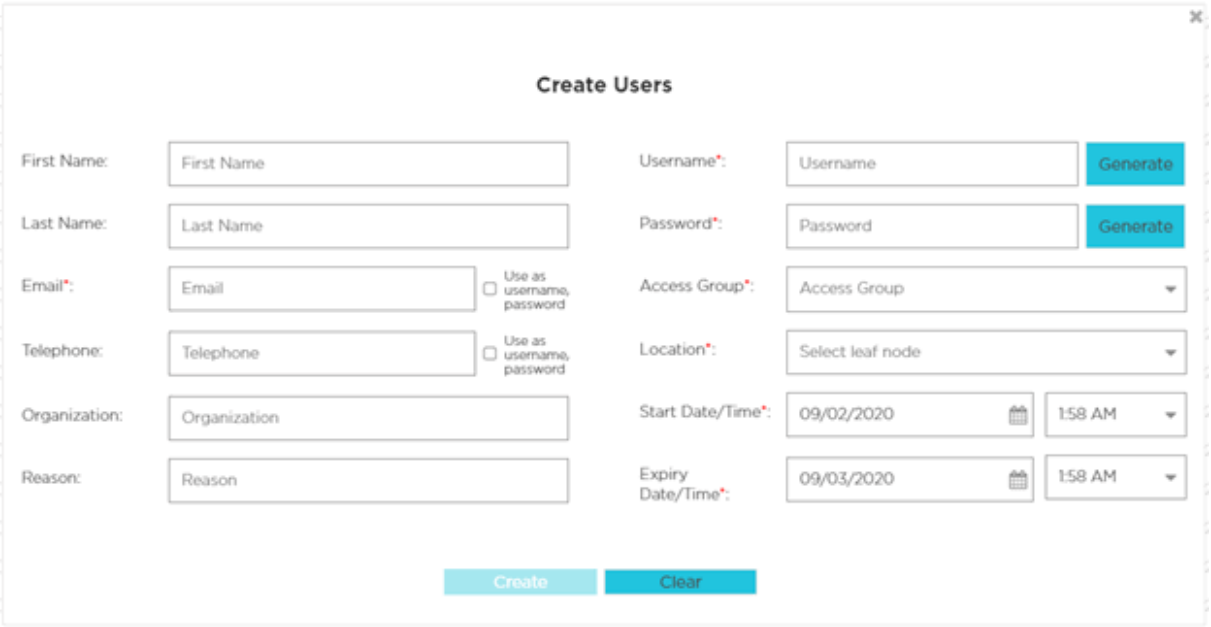


Figure 52: Create Users Window

4. Configure the following details for each user:

   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.

Access Group

Optionally, select an access 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.

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

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

Related Topics

Create Bulk Vouchers on page 86
Create Users and Bulk Vouchers from ExtremeCloud IQ on page 87

Create Bulk Vouchers

Configure > **Users** > **Bulk Vouchers**

Note
You can also configure ExtremeGuest Essentials bulk vouchers using the HelpDesk feature in ExtremeCloud IQ.

1. From the main menu, go to **Configure** > **Users**.
2. Select the Add icon at the top right corner of the page.
3. Select **Create Bulk Vouchers**.
   The **Create Bulk Vouchers** window displays.

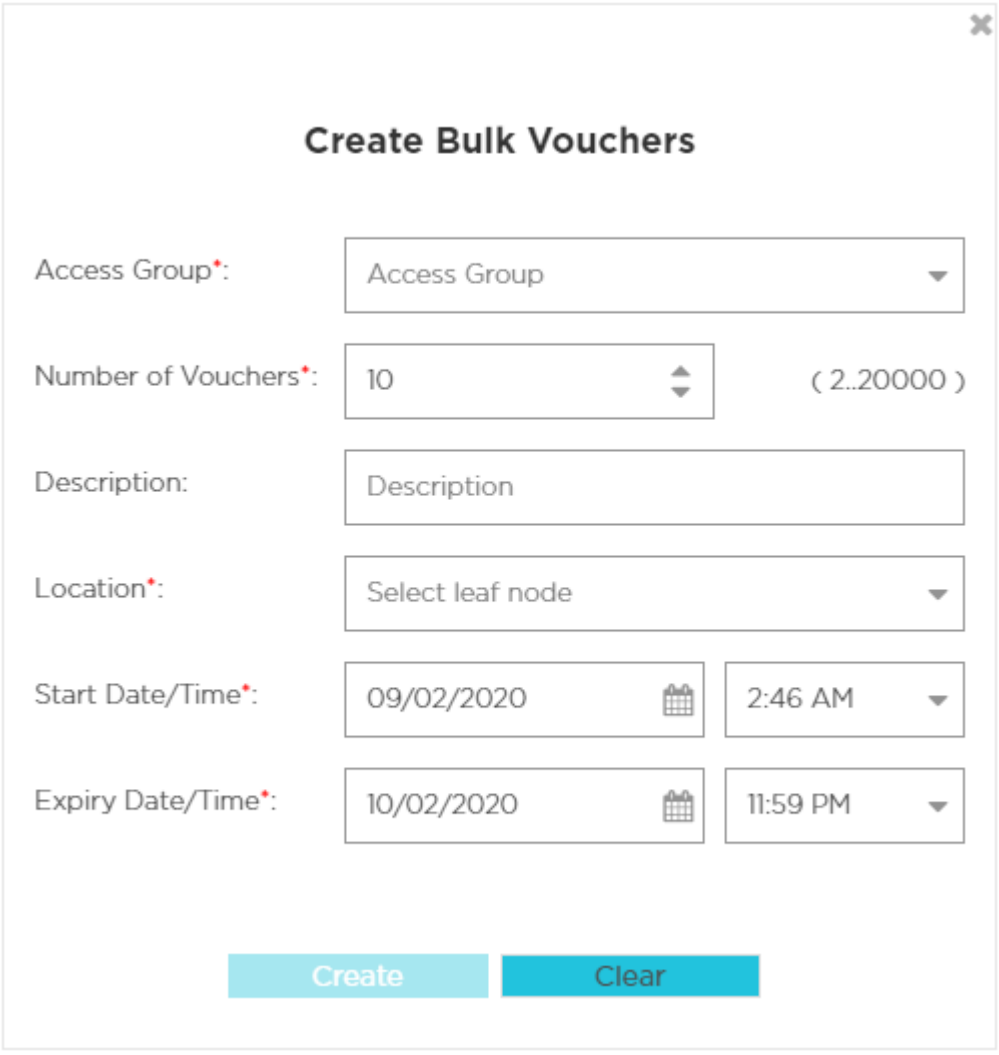


Figure 53: Create Bulk Vouchers Screen

4. Configure the following details for bulk voucher creation:
   Access Group
   Select an access 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.

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

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

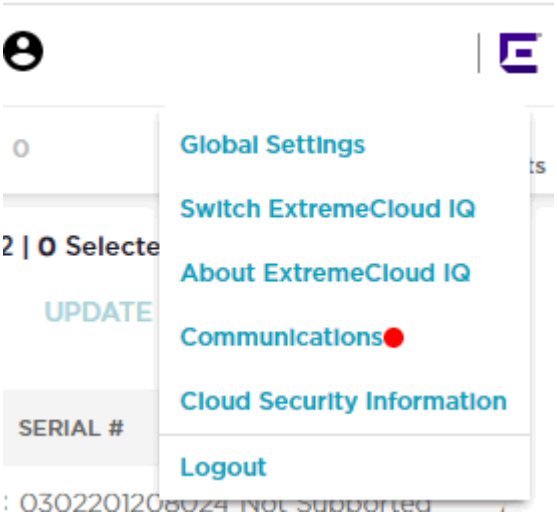
Related Topics

Create Users on page 84
Create Users and Bulk Vouchers from ExtremeCloud IQ on page 87

Create Users and Bulk Vouchers from ExtremeCloud IQ

You can create new users and Bulk Vouchers via the HelpDesk feature in ExtremeCloud IQ.

1. From the ExtremeCloud IQ page, select the icon in the top right corner to access the ExtremeCloud IQ HelpDesk feature, which provides you with access to several additional functions in the drop-down list:



2. Select **Global Settings**
3. From the left-panel tree, select **Account Management**.

   The **Admin Accounts** window opens.
4. To create the Guest Management role, select the Add icon at the top left corner of the **Admin Accounts** window.
5. You can select an existing admin role or grant access to an external admin from this window.

   The **Add New Admin** window opens.
6. Select **Guest Management** from the list of roles.

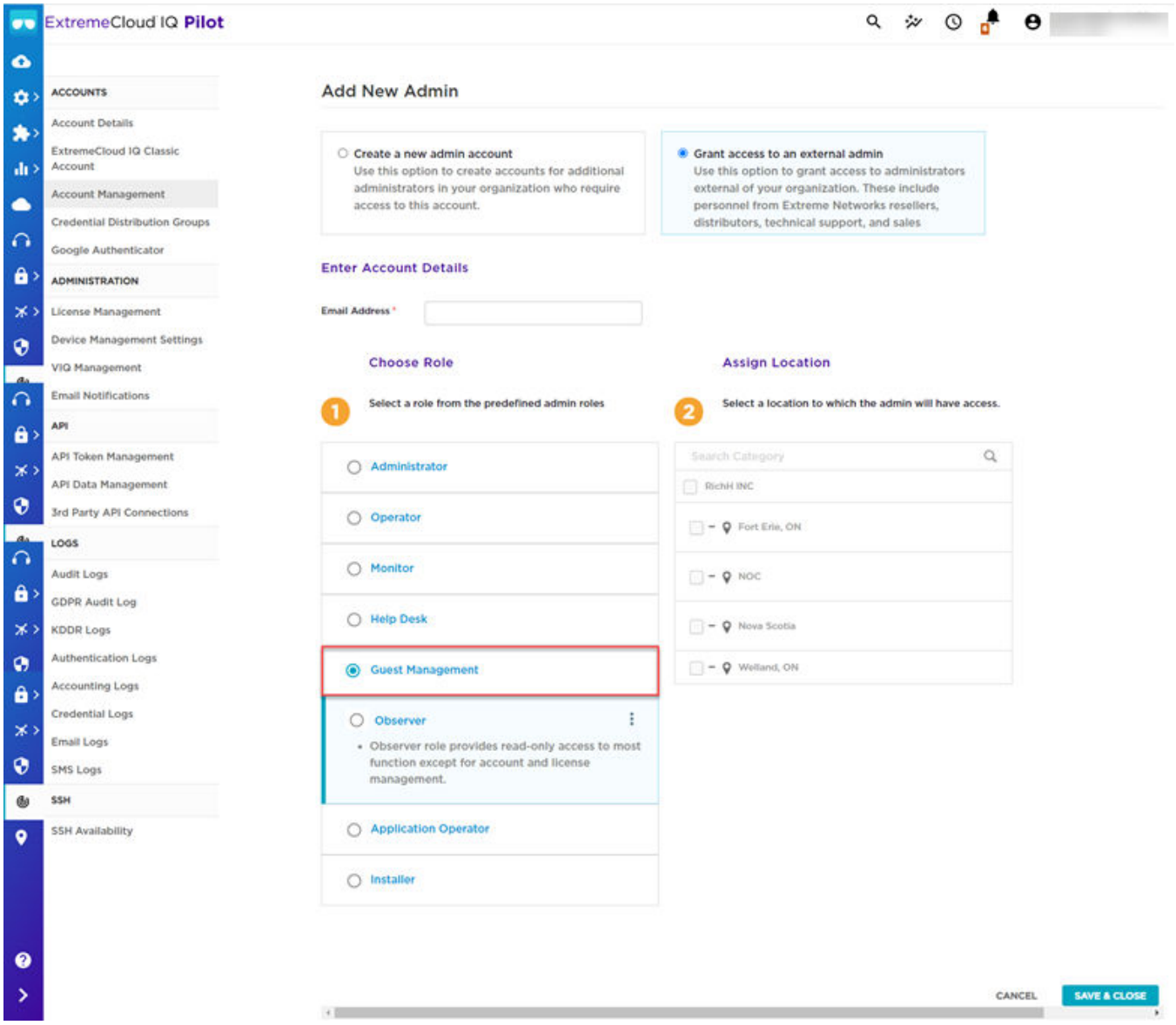


Figure 54: Adding Guest Management Role

7. Select **Save & Close**.

   The Guest Management admin you just created is included on the Admin Accounts table.

8. Log in to ExtremeCloud IQ again.

   The ExtremeCloud IQ Users page opens by default.
9. Expand the **Configure** left-panel tree and select **Guest Essentials Users**.

   The ExtremeGuest Essentials window opens.
10. Select the Add icon from the top right corner to Create Users or Create Bulk Vouchers on page 86.

Configure Clients

Configure > **Clients**

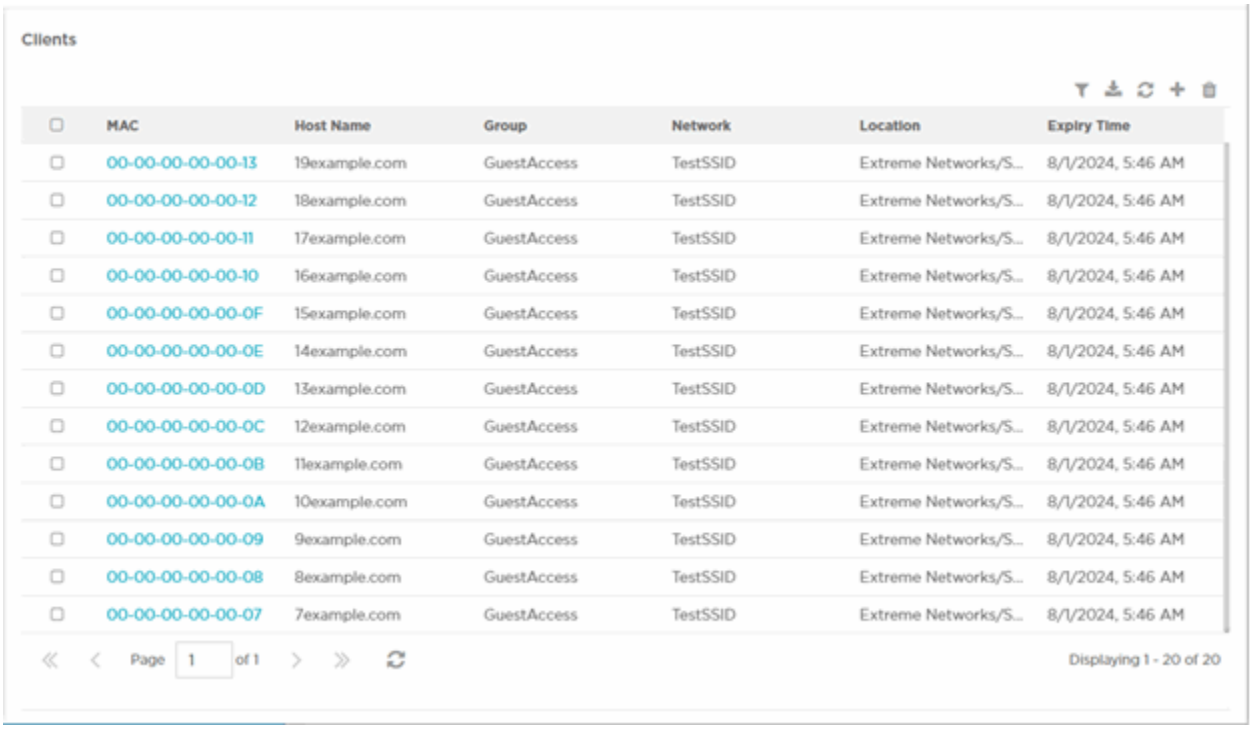


Figure 55: Clients Screen

Use the tools at the top right corner of the table to perform the following functions:

- Add - Create a new client.
- Filer - Filter the data in the table
- Download - Download client data
- Refresh - Update the data in the table
- Delete - Remove client data from the table

The **Clients** table includes the following columns:

MAC

The MAC address of the client end point.

Host Name

The host name assigned to the client end point.

Group

The access group to which the client end point is associated.

Network

The network to which the client end point is included.

Location

The location to which the client end point is associated.

Expiry Time

The date and time that the client end point was no longer active.

Create Clients

Configuration → End Points → Create End Points

Use the Configuration → Clients tab to create client end points.

To create a client end point:

1. Go to **Configuration → Clients** from the main menu.
2. Select the Add icon (+) in the top right corner of the page.
   The **Create Clients** tab displays by default.

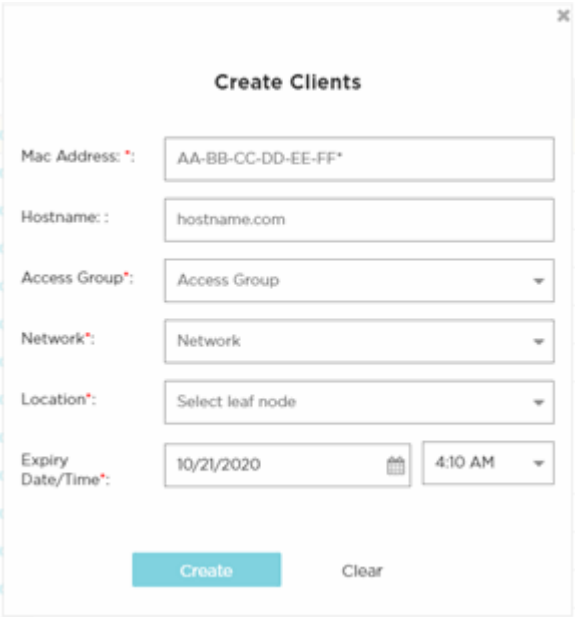


Figure 56: Create Clients Screen

3. Configure the following details for each end point voucher:

   MAC Address

   Enter the MAC address for the client 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 client end point.

Access Group

Select an access group from the list to associate it to the client end point.

Network

Select a network from the list to associate it to the client end point.

Location

Select a location from the list to associate it to the client end point.

Expiry Date/Time

Use the calendar to specify the ending date and time that the client end point will be deactivated.

4. When all mandatory fields have been completed, select **Create**.

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

Analyze

The **Analyze** workbench provides reports and key-metrics about users and clients.

The following options are available:

- Analyze Clients on page 92
- Reports on page 95
- Analyze Users on page 99

Analyze Clients

Analyze → Clients

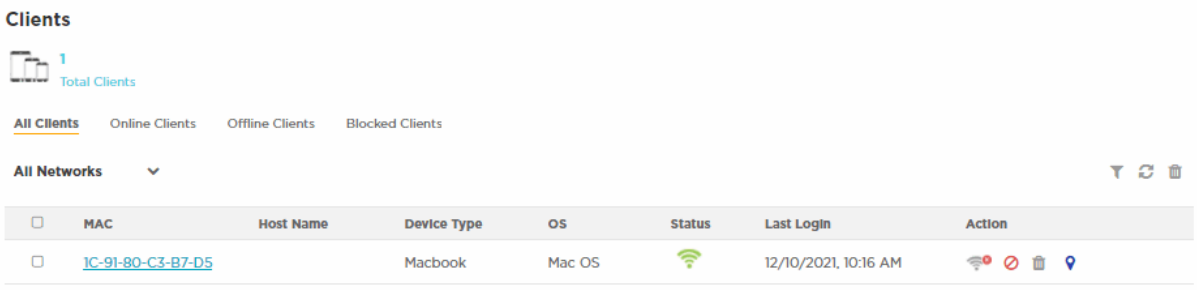


Figure 57: Clients Screen

The **Clients** screen provides a system-wide summary of all client status, as well as detailed information for each clients. Clients are guest users, including users logged in via email or SMS, social-media login, and devices registered with and authenticated by the ExtremeGuest Essentials captive portal server.

The **Clients Summary** table includes the following tabs.

Total Clients

Select to display the total number of clients per location.

Online Clients

Select to display the total number of clients per location that are currently online.

Offline Clients

Select to display the total number of clients per location that are currently offline.

Blocked Clients

Select to display the total number of blocked clients per location.

Clients Details Table

The **Clients Details** table displays the following information:

MAC

Displays the end point MAC address.

Host Name

Displays the client end point host name.

Device Type

Displays the client end point device model.

OS

Displays the operating system used by the client end point.

Status

Displays the client end point authentication status.

Last Login

Displays the full date and time when the client end point last authenticated on the network.

Action

There are four functions in the **Action** column that you can use on client devices:

- **Disconnect** - Terminates the client end point's session on the network.
- **Block** - Prevents the client end point from passing traffic on the network.
- **Delete** - Removes the client end point from the database. If the end point connects again, it is treated as new end point.
- **Location** - Locates the client device on a floor plan in ExtremeLocation Essentials. Click the location icon to launch ExtremeLocation Essentials, and see the location of the client device on the floor plan.

> **Note**
> Before locating a client device, you must enable ExtremeLocation Essentials and configure a floor map for each location.

Clients Detail

Select an entry in the **Clients Summary** table to open the **Clients Details** table.

Filter Client Results

Analyze → Clients → Filter Clients

Use the filter functionality to distill client data based on specific criteria.

To filter clients results:

1. Access the **Analyze → Clients** tab.
2. Select the Filter icon in the top right corner of the table. The **Filter Clients** window displays.
   The **Filter Clients** window.

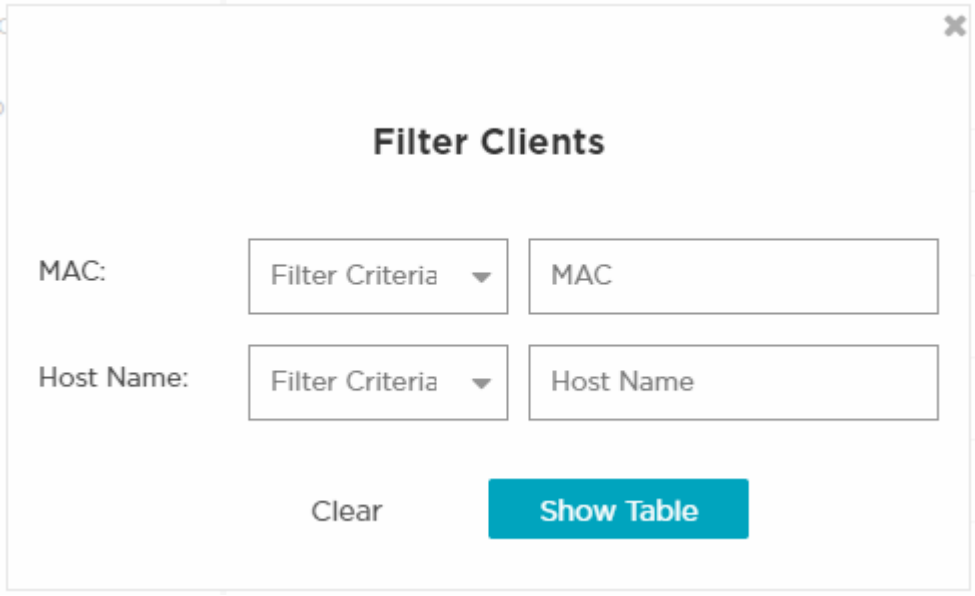


Figure 58: Filter Clients

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

MAC Address

Select the Filter Criteria drop-down list to select either **equals**, **starts with**, or **contains** as filtering criteria.

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

Host Name

Select the Filter Criteria drop-down list to select either **equals**, **starts with**, or **contains** as filtering criteria.

Enter a Host Name or portion of a Host Name address to filter users with host names 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**

Generate and work with reports in ExtremeGuest Essentials.

The following reports are available:

- **Dashboard Report** — A summary of widget data for a selected dashboard. Select from a list of configured dashboards.

  Note
  The time period selected for the dashboard is used when generating the report.

- **Guest Summary Report** — A summary of total and average unique guests and client visits. This information can be reported in daily or one month time intervals. The report consists of user and client distribution summaries for each SSID location.
- **Guest Visit** — A summary and history of guest visits. This information is stored for up to three months. The report consists of email, location, user name, and MAC address information.

To create a report or manage a list of available reports, go to **Analyze** > **Reports** > **Manage**.

To view a list of generated reports, go to **Analyze** > **Reports** > **Generated**.

From the **Reports** workbench, you can do the following:

- Create a new report
- Modify report settings
- Schedule a report
- Search for available reports
- Review a list of generated reports
- Export a report in PDF or CSV format
- Delete a report

Create and Delete reports functionality is made available to users at the Admin, Monitor, and Operator roles. Users at the Monitor and Operator role can view reports that are generated for the root location when they have access to all the locations under the root location. Otherwise, the generated report is not displayed.

Note
Root location is at the top of the location tree. If a user is granted access to the root location, they inherit all locations below the root.

Related Topics

Create and Schedule a Report on page 96

Work with Existing Reports on page 96
Report Settings on page 98

Create and Schedule a Report

Take the following steps to create a report in ExtremeGuest Essentials:

1. Go to **Analyze** > **Reports** > **Manage**.
2. Select the plus sign in the top right corner.

   The **Add Report** dialog displays.
3. Configure the report settings.

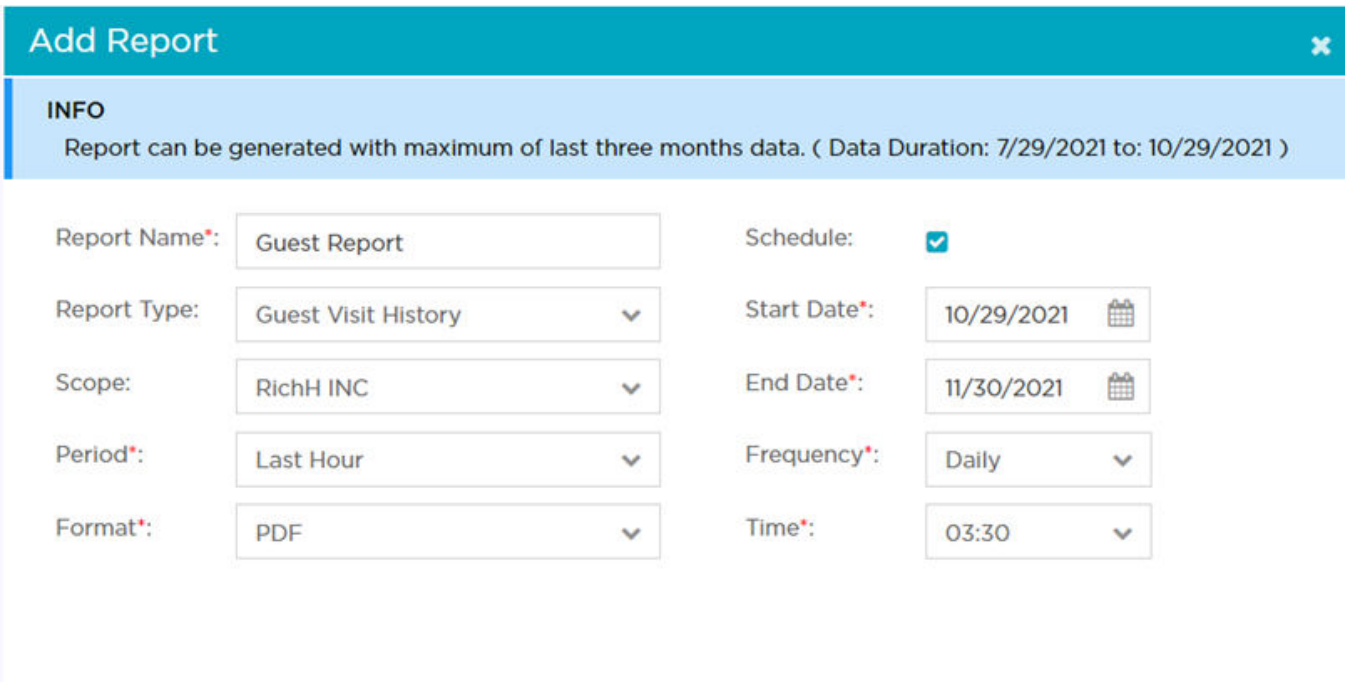


Figure 59: Report Settings

4. Save and run the report:
   - To save the report settings without running the report, select **Save**.
   - To save the report settings and run the report, select **Save & Run**.

Related Topics

Report Settings on page 98

Work with Existing Reports

After you have configured report settings, you can work with the report. The following tasks are described in this topic:

- Modify Report Settings on page 97
- Download a Report on page 97

- View a Report Online on page 97
- Delete a Report on page 97

Modify Report Settings

To modify an existing report:

1. Go to **Analyze** > **Reports** > **Manage**.
2. Select a report from the list.

   The **Edit Report** dialog displays.
3. Modify the report settings.
4. Save and run the report:
   - To save the report settings without running the report, select **Save**.
   - To save the report settings and run the report, select **Save & Run**.

Related Topics

Report Settings on page 98

Download a Report

When configuring the report settings, select the generated report format. Once the report is generated, it is added to the Generated Report List.

To download a generated report:

1. Go to **Analyze** > **Reports** > **Generated**.
2. Select the report icon in the Action column next to the report that you want to download.

   The report is downloaded in the format that you have configured under Report Settings. Valid formats are PDF or CSV.

View a Report Online

To open and view a report online in a browser window, select the report link.

Delete a Report

You can delete generated reports and report templates. To delete an existing report:

1. Navigate to the **Reports** workbench:
   - To delete a report template with saved report settings, go to **Analyze** > **Reports** > **Manage**.
   - To delete generated reports, go to **Analyze** > **Reports** > **Generated**.

   A list of reports is displayed.
2. Select a report to delete:
   - Select the check box next to one or more reports that you want to delete. Then, select at the top of the screen.
   - Select next to the report row that you want to delete.

Related Topics

Reports on page 95
Create and Schedule a Report on page 96
Report Settings on page 98

Report Settings

Configure or modify the following settings before generating a report:

Report Name

The name of the report.

Report Type

The type of report. Some report settings are specific to the report type. Valid values are:

- **Guest Visit History**

  Scope

  The selected site.

  Period

  Time period for which the report data is collected. Valid values are:

  - Last Hour
  - Last Day
  - Last Week
  - Last Month
  - Last 3 Months (Maximum time period)
  - Custom

    After selecting **Custom**, provide a Start Date and Time and an End Date and Time to create a custom time period.

- **Dashboard Report**

  Dashboard Name

  Select from a list of configured dashboards. Configure the dashboard before you run the report.

- **Guest Summary Report**

  Scope

  The selected site.

  Period

  Time period for which the report data is collected. Valid values are:

  - Last Day
  - Last Month

Format

The output format for the generated report. Valid values are:

- PDF

- CSV

Note
CSV format is only available for **Guest Visit History** reports.

Schedule

Select **Schedule** to schedule a report generation. Configure the following scheduling parameters:

- Start Date and Time
- End Date and Time
- Frequency — The report is generated once over a particular period of time. Valid values are:
  - Daily
  - Weekly
  - Monthly
- Time — Specific time the report is generated. This value corresponds to the selected Frequency value.
  - Daily:
    - Single time of day
  - Weekly:
    - Single day of the week
    - Single time of day
  - Monthly:
    - Single day of the month
    - Single time of day

Related Topics

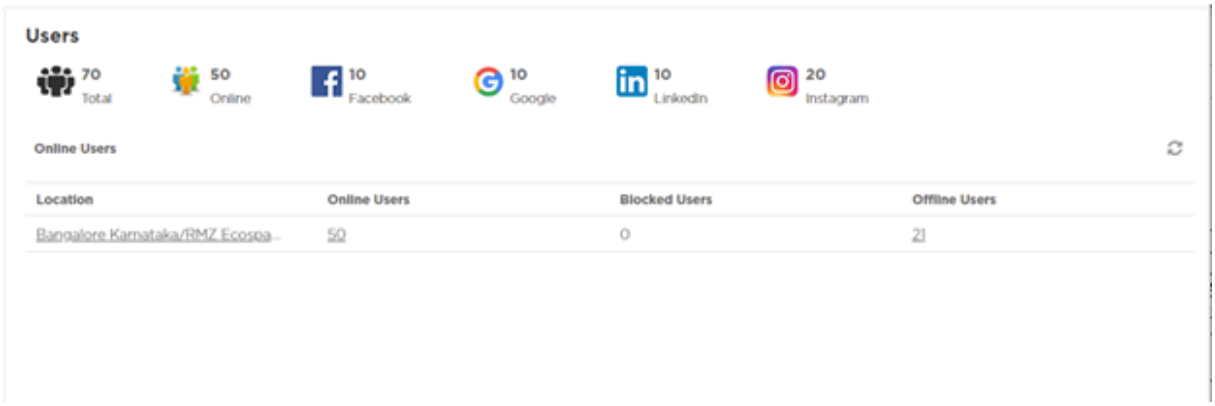
Dashboard on page 21

Analyze Users

Analyze → 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

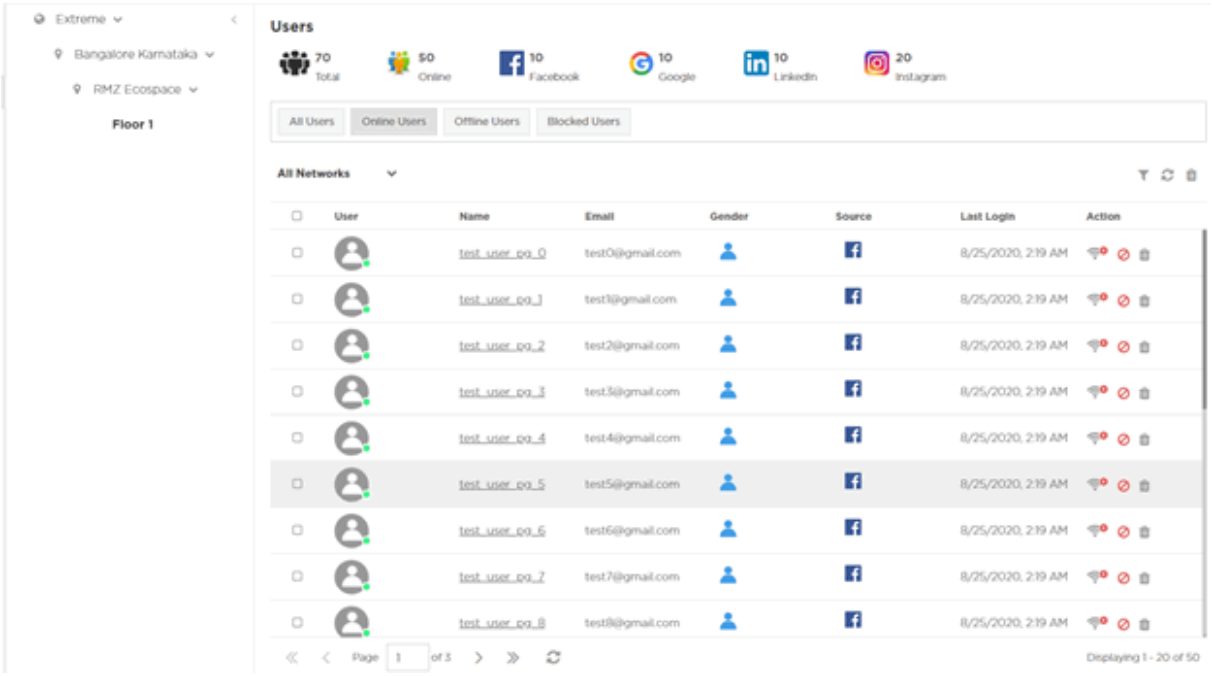
Displays the number of users that are not currently connected to the network for each Location.

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 user name 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 email address associated with each online user. If using social media authentication, the email 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, and LinkedIn.

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 **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.

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 filter icon in the upper right of the table.

   The **Filter Users** window displays.

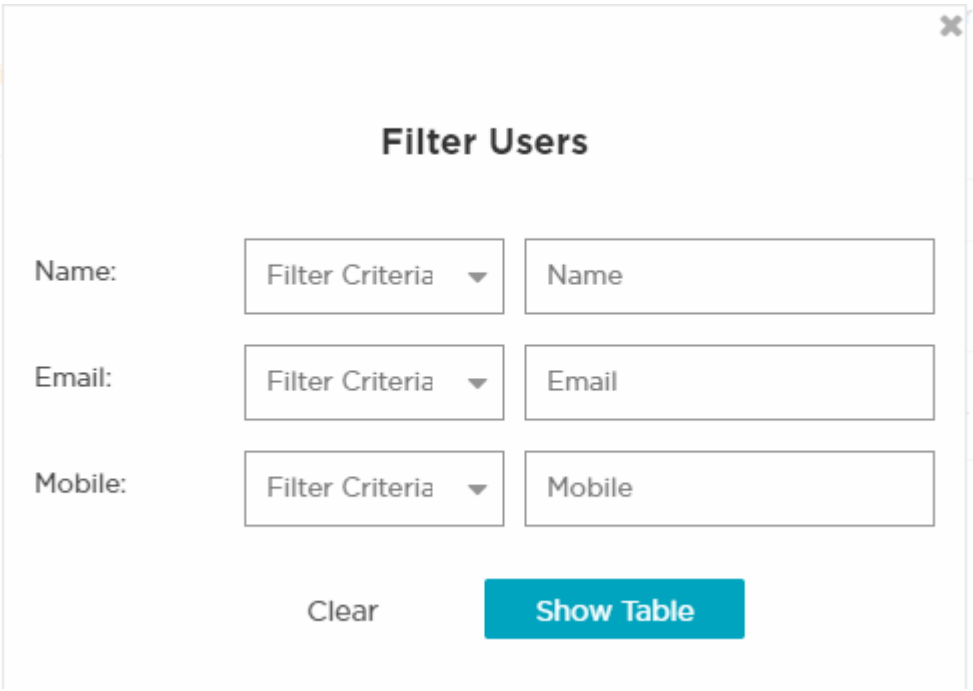


Figure 60: Filtering Users Screen

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.

   Email

   Enter an email address or portion of an address such as a domain to filter users with email address 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.

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

   To remove any text entered into the search fields, select **Clear**.