



ExtremeGuest User Guide

Copyright © 2018 Extreme Networks, Inc. All rights reserved.

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, please see:

www.extremenetworks.com/company/legal/trademarks

Software Licensing

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:

www.extremenetworks.com/support/policies/software-licensing

Support

For product support, phone the Global Technical Assistance Center (GTAC) at 1-800-998-2408 (toll-free in U.S. and Canada) or +1-408-579-2826. For the support phone number in other countries, visit: <http://www.extremenetworks.com/support/contact/>

For product documentation online, visit: <https://www.extremenetworks.com/documentation/>

Table of Contents

Preface.....	4
Text Conventions.....	4
Providing Feedback to Us.....	4
Getting Help.....	5
Extreme Networks Documentation.....	5
Chapter 1: Introduction to ExtremeGuest.....	6
Installing ExtremeGuest on a Hypervisor.....	6
UI Overview.....	7
Chapter 2: Monitor.....	13
Map View.....	13
Summary.....	15
Users.....	17
Chapter 3: Dashboard.....	22
Dashboard Basics.....	22
Creating a New Dashboard.....	23
Available Dashboard Widgets.....	25
Chapter 4: Configuration.....	28
AAA Configuration.....	28
Networks.....	35
Sites.....	36
Devices.....	38
Onboarding.....	39
Splash Templates.....	41
Notification.....	44
Social.....	49
Vouchers.....	51
Chapter 5: Analyze.....	55
Analyze End Points.....	56
Reports.....	57
Analyze Users.....	63
Chapter 6: Operations.....	65
Database.....	65
License.....	68
Maintenance.....	69
REST API.....	71
Troubleshooting.....	71
Chapter 7: REST API.....	74
About the ExtremeGuest REST API.....	74
Accessing the ExtremeGuest REST API.....	76
Guest Users Examples.....	77
Guest Devices Examples.....	82

Preface

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

Text Conventions

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

Table 1: Notice Icons





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

Table 2: Text Conventions

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

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

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

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short [online feedback form](#). You can also email us directly at documentation@extremenetworks.com.

Getting Help

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

- **GTAC (Global Technical Assistance Center) for Immediate Support**
 - **Phone:** 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
 - **Email:** support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- **Extreme Portal** — Search the GTAC knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
- **The Hub** — A forum for Extreme 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.

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

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

Extreme Networks Documentation

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

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for earlier versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/software-licensing.

1 Introduction to ExtremeGuest

Installing ExtremeGuest on a Hypervisor UI Overview

ExtremeGuest is a robust and comprehensive guest management and engagement solution which gives unique opportunity to personalize engagement by understanding the customer behavior and interest, and then tailor services based on those insights. For example, knowing how many customers enter a store, how often they visit, and how much time they spend are all metrics that can be measured through ExtremeGuest. ExtremeGuest can take advantage of social networking behavior to increase patronage, expand brand exposure, and understand client demographics and preferences in a more comprehensive and personal way. Guest onboarding with sponsor approval is supported allowing a sponsor to approve or deny guest access with a single click.

ExtremeGuest is available as a virtual machine and provides centralized guest management including multiple guest onboarding methods and guest analytics. ExtremeGuest is supported as a standalone application, or in replica set mode. Replica set mode is supported with three instances of the ExtremeGuest platform or two instances of ExtremeGuest and an NX5500 or NX7500 as an arbiter.

For information on scale and hardware requirements for ExtremeGuest view the [ExtremeGuest Datasheet](#).

Installing ExtremeGuest on a Hypervisor

- 1 Use the following link to go to the Extreme Networks extranet downloads page: [Extreme Networks Extranet Download Page](#)
- 2 If you do not have an extranet account, register here: <https://secure.extremenetworks.com/register.aspx>
- 3 Select the ExtremeWireless product family.
- 4 Select the Firmware tab.
- 5 The Firmware page displays the resources that you are entitled to. If you do not see the items that you need or think that you are entitled to, please contact GTAC [http:// www.extremenetworks.com/support/contact/](http://www.extremenetworks.com/support/contact/) or e-mail portal@extremenetworks.com
- 6 Download the ExtremeGuest application. The application is downloaded as an .iso image.



Note

Ensure a hypervisor (ESXi, Xen, Hyper V) is installed in your server environment or the downloaded .iso image will not run.

- 7 Install the .iso following the the hypervisors instructions for installing a virtual machine.
- 8 Boot the ExtremeGuest application for the first time.
The system prompts the user to change the password.
- 9 Install the license obtained from the licensing portal on the **Operations > Licenses** screen. For more detailed licensing instructions see: [License](#) on page 68.

UI Overview

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

When viewed in a browser window with enough width the ExtremeGuest navigation menus are displayed as the following pull-down menus at the top of user interface:

- [Monitor](#) on page 13
- [Dashboard](#) on page 22
- [Configuration](#) on page 28
- [Analyze](#) on page 55
- [Operations](#) on page 65

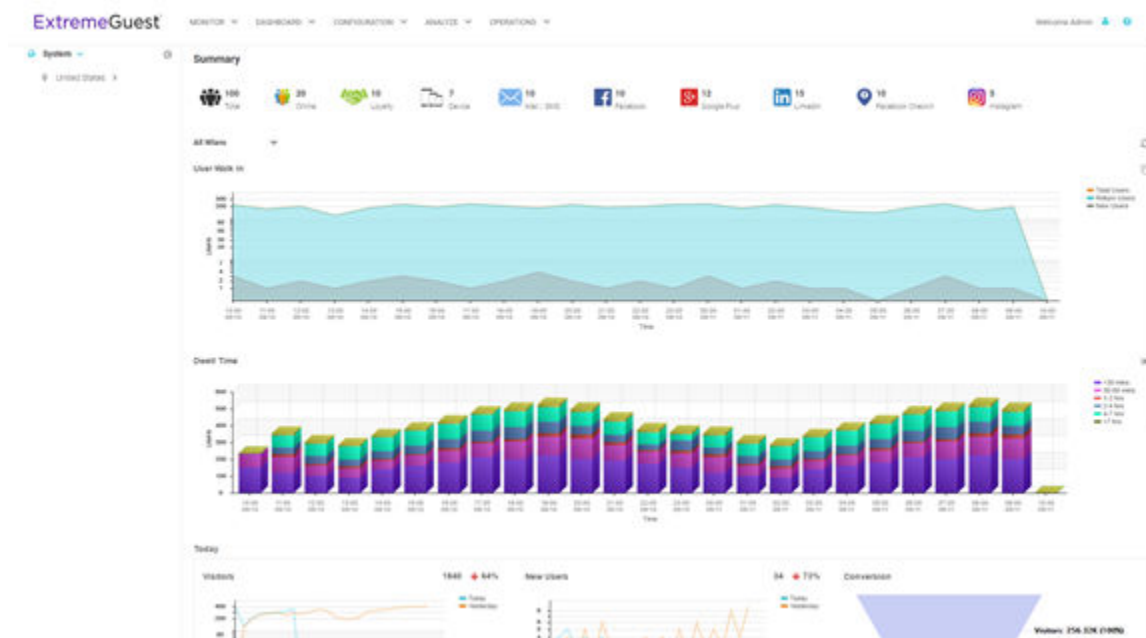


Figure 1: User Interface in Standard View

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

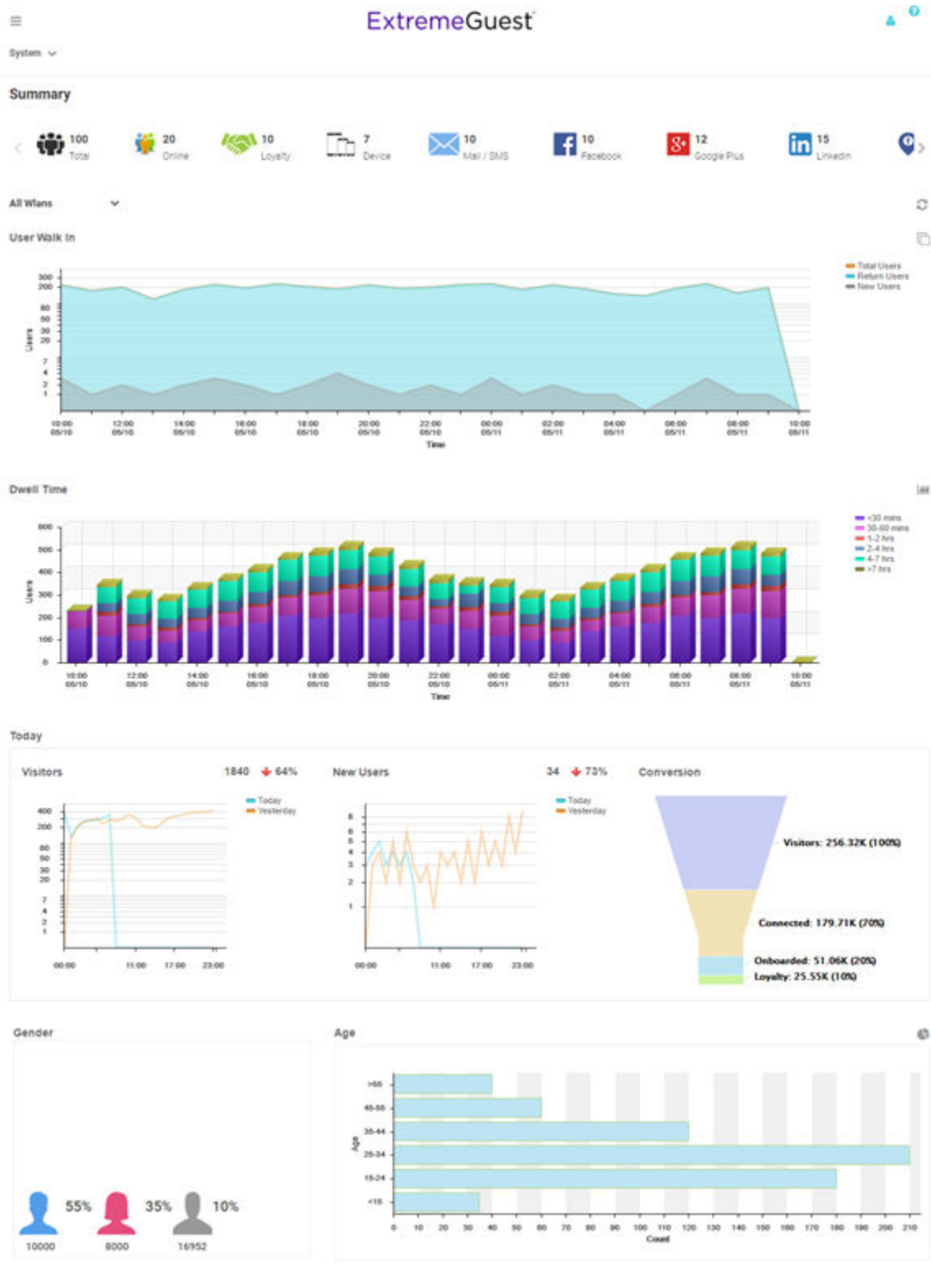


Figure 2: User Interface in Tablet View

When using a browser with a narrow width, 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 13
- [Dashboard](#) on page 22
- [Configuration](#) on page 28
- [Analyze](#) on page 55
- [Operations](#) on page 65

The ExtremeGuest user interface supports the following user roles:

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

Web User Interface

The web user interface is used to manually add individual users or bulk add users through vouchers. To access the web user interface a web user must be created by the administrator. Once created, login with the webuser's username and password to access the web user interface.

The screenshot shows the 'New User' form in the ExtremeGuest web interface. The form is titled 'New User' and is located in the center of the page. It contains the following fields and controls:

- First Name:** Text input field.
- Last Name:** Text input field.
- Email*:** Text input field with a checkbox labeled 'Use as username/password'.
- Telephone:** Text input field with a checkbox labeled 'Use as username/password'.
- Organization:** Text input field.
- Reason:** Text input field.
- Username*:** Text input field with a blue 'Generate' button.
- Password*:** Text input field with a blue 'Generate' button.
- User Group:** Dropdown menu with 'split-group' selected.
- Location*:** Dropdown menu.
- Start Date/Time*:** Date and time selection fields (05/26/2017, 12:10 PM).
- Expiry Date/Time*:** Date and time selection fields (05/27/2017, 12:10 PM).

At the bottom of the form are two blue buttons: 'Create User' and 'Clear Fields'.

Figure 3: Web User Interface - New User Screen

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

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

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

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

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

Figure 4: Web User Interface - Bulk Voucher Screen

User Group	User the pull-down menu to select a user group for all new users in the bulk voucher. New user groups are created by the admin user. This is a required field.
Number of Vouchers	Use the spinner controls to specify the number of vouchers to create. The number of vouchers may be between 2 and 20,000. This is a required field.
Description	Optionally, enter a description for the users being added to the voucher.
Location	User the pull-down menu to select a location for the new users to be added to. New locations are added by the admin user. This is a required field.
Start Date / Time	Specify the starting date and time for the new users to be activated. This is a required field.
Expiry Date / Time	Specify an ending date and time for the users to be deactivated. This is a required field.

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

Onboard User Interface

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

The screenshot shows a web interface for device registration. At the top, there are tabs for 'DEVICE REGISTRATION' and 'SUMMARY', and a user greeting 'Welcome Onboard-User'. The main heading is 'HELLO TEST ONBOARD'. Below this, there is a form with the following fields:

- MAC Address: AA-BB-CC-DD-EE-FF*
- Group: [Dropdown menu]
- Wlan: [Dropdown menu]
- Location: [Dropdown menu]
- Vendor: [Dropdown menu]
- Device: [Dropdown menu]
- Device Os: [Dropdown menu]
- Device Browser: [Dropdown menu]
- Expiry Time: [Date and time picker]

At the bottom of the form, there are two buttons: 'Register' and 'Cancel'.

Figure 5: Onboard User Interface - Device Registration

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

MAC Address	Enter the MAC address for the device being added.
Group	Use the pull-down menu to select a group to add the new device to. New groups are added by the admin user.
Network	Use the pull-down menu to select a network to associate the new device with. New WLANs are added by the admin user.

- Location** Use the pull-down menu to select a site to associate the new device with.
- Vendor** Use the pull-down menu to select the **Vendor** who manufactured the device being added.
- Device** Use the pull-down menu to specify the type of device being added to the network.
- Device OS** Use the pull-down menu to specify the operating system running on the device being added.
- Device Browser** Use the pull-down menu to specify the browser type in use on the new device.
- Expiry Time** Specify a date when the device will be automatically removed from the network.

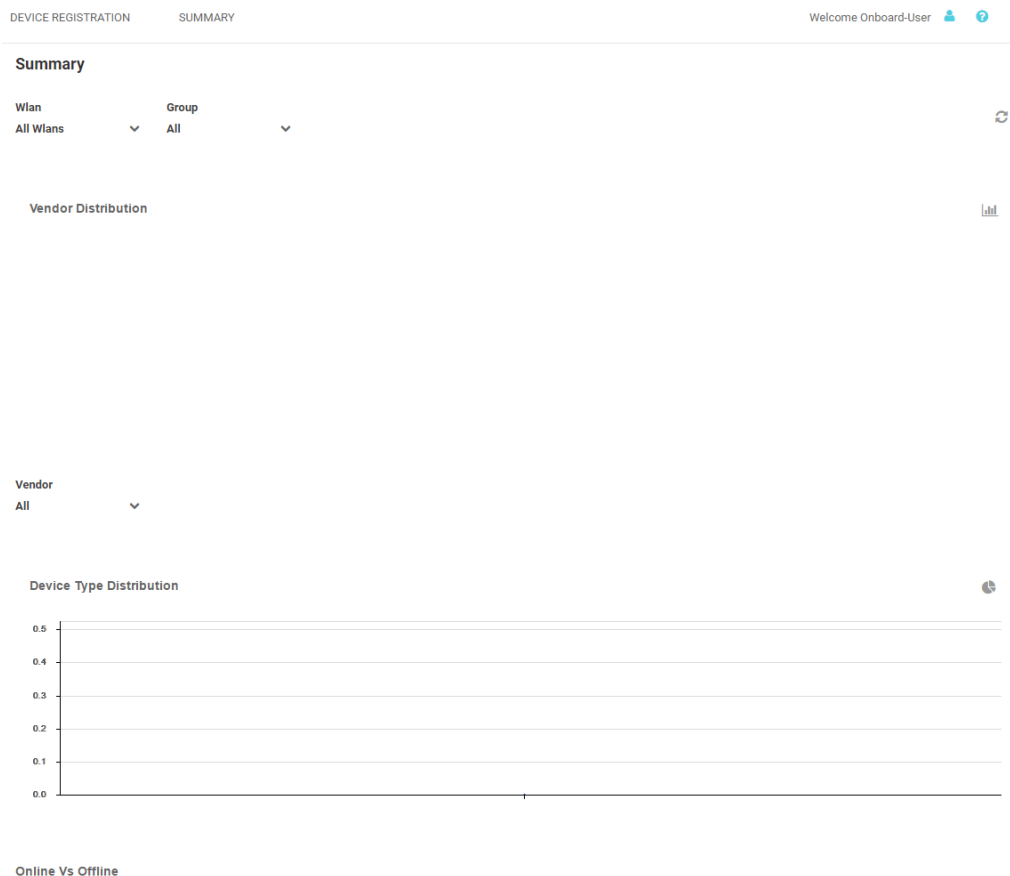


Figure 6: Onboard User Interface - Summary Screen

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

2 Monitor

Map View Summary Users

Access the **Monitor** screens by selecting **Monitor** from the menu and selecting one of the following options:

- Summary
- Map View
- Users

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

Map View

Monitor > Map View

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

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

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

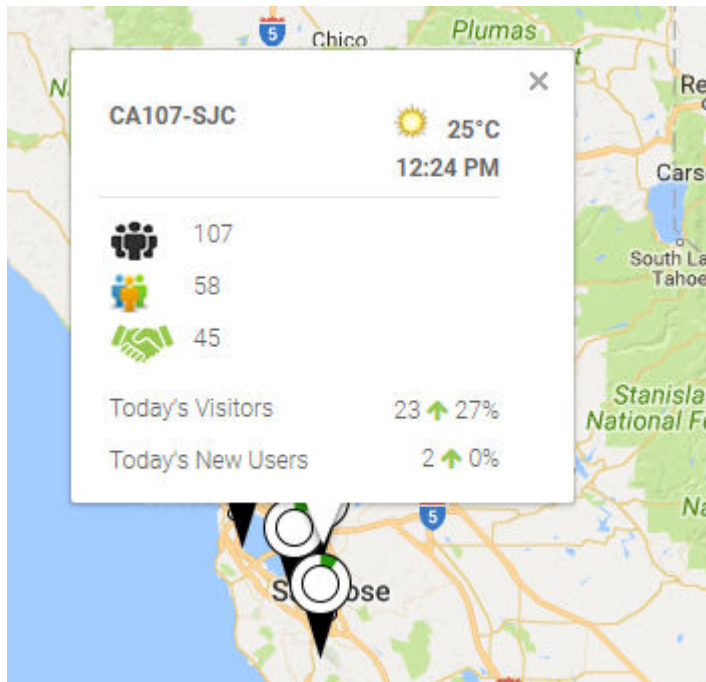


Figure 7: Monitor > Map View Mouse Over

To zoom in or out on the map use the + and - buttons.

To toggle between map view and satellite view, select **Map** or **Satellite** from the upper-left corner of the map.

Map View Screen

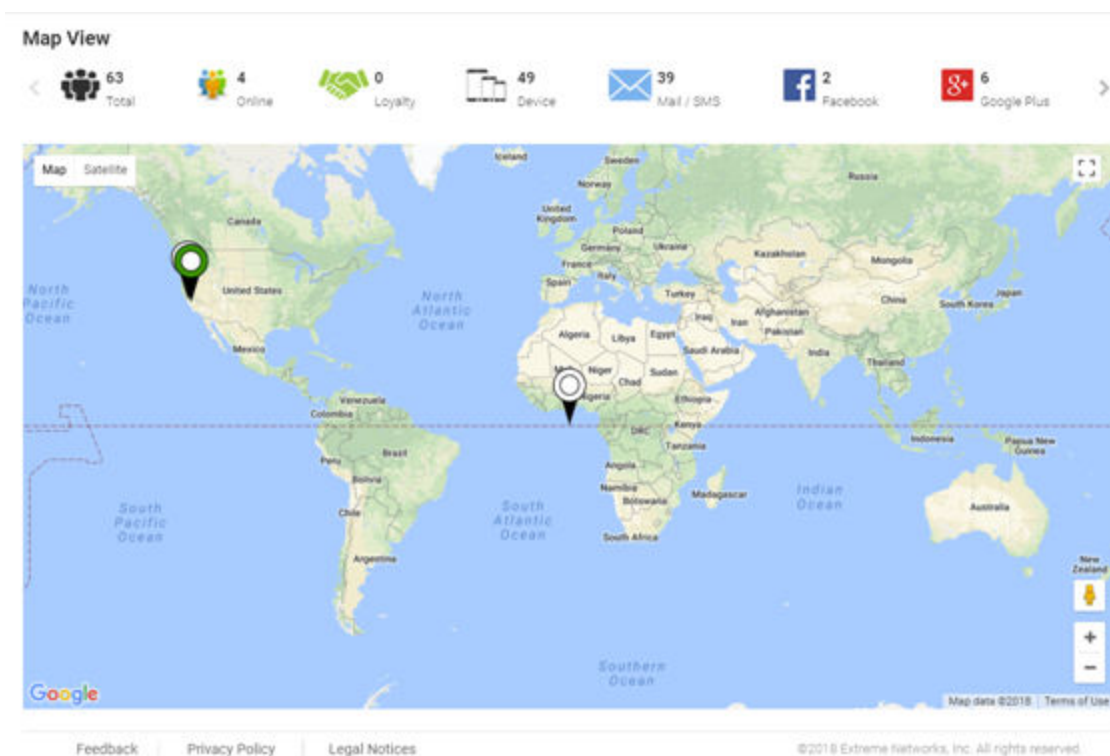


Figure 8: Monitor > Map ViewScreen

Summary

Monitor > Summary

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

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

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

[Summary Details](#) on page 17

Summary Screen

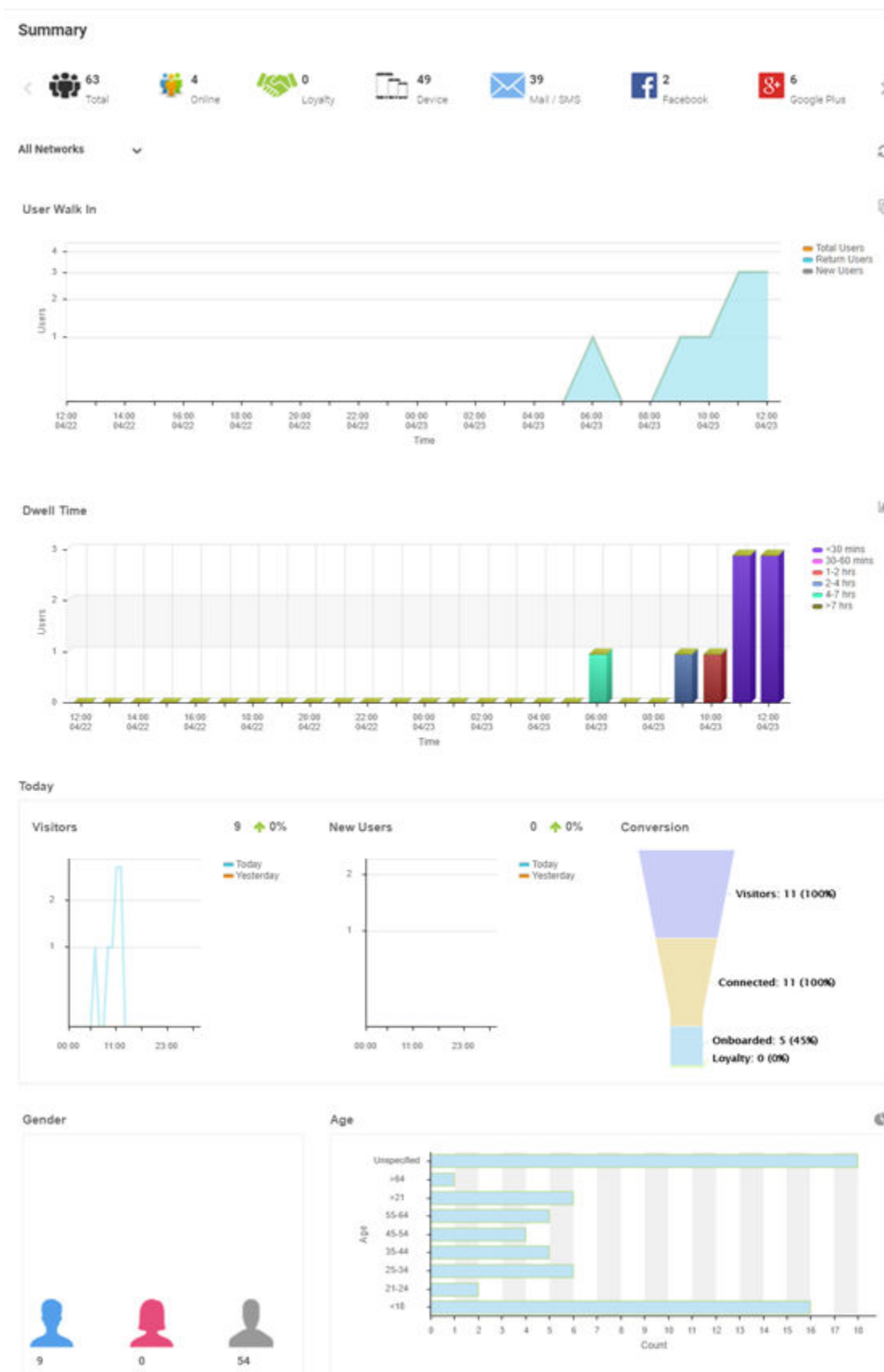


Figure 9: Monitor > Summary Screen

Summary Details

User Walk In	The User Walk In graph displays the number of users entering a location over a 24 hour time period with data points at each hour. Data is further separated between Total Users , Return Users , and New Users .
Dwell Time	The Dwell time graph displays the amount of time users stayed at a location over a 24 hour time period with data points at each hour. Data is further separated into the following time windows: <ul style="list-style-type: none"> • < 30 Minutes • 30-60 Minutes • 1-2 Hours • 2-4 Hours • 4-7 Hours • > 7 Hours
Today	The Today chart displays data from the last two days and a comparison of Visitors and New Users data in percentages. The Visitors graph displays the total number of users over time. The New Users graph displays the number of first time users over time. The Conversion graph displays the number and percentage of users who converted from Connected to Onboarded to Loyalty customers. The information displayed in all three graphs starts at midnight of the previous day and goes through the current time. This information resets each day at midnight.
Gender	The Gender chart displays the percentage of users by gender.
Age	The Age bar graph displays the total number of users separated into the following age ranges: <ul style="list-style-type: none"> • > 55 • 45-55 • 35-44 • 25-34 • 15-24 • < 15

Users

Monitor > Users

The **Users** screen displays a summary of the total number of users and their status. The content of this screen changes based on what is selected in the navigation tree. When a single site is selected, this screen will display user details for currently connected and users.

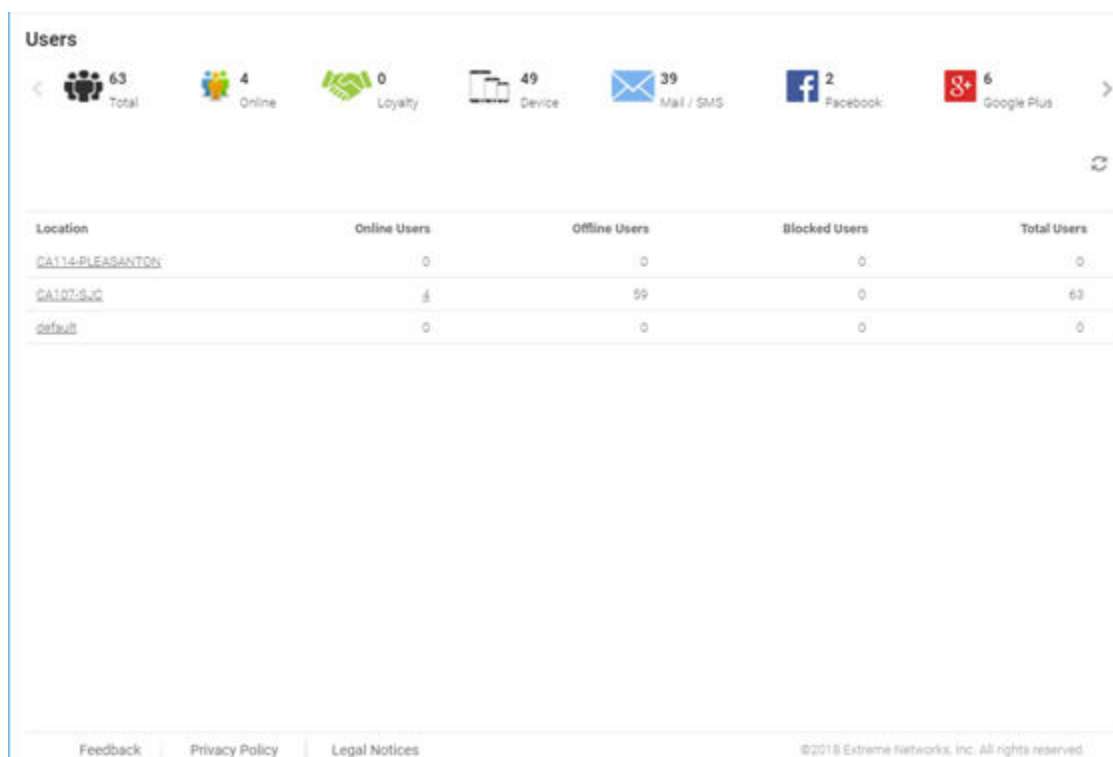


Figure 10: Monitor > Users Screen

- [Active Users Details](#) on page 19
- [Blocked User Details](#) on page 20

Active Users Details

The screenshot displays the 'Users' section of the Monitor interface. At the top, there are several statistics: Total (64), Online (6), Loyalty (0), Device (50), Mail / SMS (40), Facebook (2), and Google Plus (6). Below these are tabs for 'Active Users' and 'Blocked Users', and a dropdown for 'All Networks'. The main part of the screen is a table with the following columns: User, Name, Email, Gender, Source, Last Login, MAC, and Action. The table lists several active users with their respective details. At the bottom, there are links for 'Feedback', 'Privacy Policy', and 'Legal Notices', and a copyright notice for ©2018 Extreme Networks, Inc.

User	Name	Email	Gender	Source	Last Login	MAC	Action
<input type="checkbox"/>							
<input type="checkbox"/>		@extreme...	Male	Device	4/23/2018, 100...		📶 🔴 🗑️
<input type="checkbox"/>		@gmail...	Male	Device	4/23/2018, 121...		📶 🔴 🗑️
<input type="checkbox"/>		@acron...	Male	Device	4/23/2018, 102...		📶 🔴 🗑️
<input type="checkbox"/>		@ex...	Male	Device	4/23/2018, 122...		📶 🔴 🗑️
<input type="checkbox"/>		@gm...	Male	Device	4/23/2018, 120...		📶 🔴 🗑️
<input type="checkbox"/>		@co...	Male	Device	4/23/2018, 105...		📶 🔴 🗑️

Figure 11: Monitor > Users Screen




System / RF Domain Level

- Location** Displays the location name or RF Domain for each configured site.
- Online Users** Displays the number of users currently connected to the network 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

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

- User** The **User** column displays the user icon associated with each online user.
- Name** The **Name** column displays the username associated with each online user. If using social media authentication, the name is provided by the social media source.
- Email** The **Email** column displays the e-mail address associated with each online user. If using social media authentication, the e-mail address is provided by the social media source.
- Gender** The **Gender** column displays an icon representing the gender of each online user.
- Source** The **Source** column displays the method that each online user used to authenticate. When social media authentication is enabled this will include Facebook, Google Plus, LinkedIn and Instagram.
- Last Login** The **Last Login** column displays the full date and time when the user last authenticated on the network.

Action	From the Action column perform one of the following actions on a user.    Select Disconnect to end a user's session on the network. Select Block to stop a user from passing traffic on the network. The user may reconnect if they re-authenticate. Select Delete to remove a user from the database. If the user connects again they will be treated as new user.
MAC	The MAC column displays the MAC address for each listed user. This column is not displayed by default, but may be enabled from the Columns menu.
Mobile	The Mobile column displays the mobile phone number for each listed user. This column is not displayed by default, but may be enabled from the Columns menu.
City	The City column displays the city associated with each listed user. This column is not displayed by default, but may be enabled from the Columns menu.
SSID	The SSID column displays the wireless network SSID that each listed user is connected through. This column is not displayed by default, but may be enabled from the Columns menu.
Network	The Network column displays the wireless network that each listed user is connected through. This column is not displayed by default, but may be enabled from the Columns menu.




Blocked User Details

System / RF Domain Level

Location	Displays the location name or RF Domain for each configured site.
Online Users	Displays the number of users currently connected to the network 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.
Unblock	Select to unblock the selected blocked user.

Site Level

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

User	The User column displays the user icon associated with each online user.
Name	The Name column displays the username associated with each online user. If using social media authentication, the name is provided by the social media source.
Email	The Email column displays the e-mail address associated with each online user. If using social media authentication, the e-mail address is provided by the social media source.
Gender	The Gender column displays an icon representing the gender of each online user.
Source	The Source column displays the method that each online user used to authenticate. When social media authentication is enabled this will include Facebook, Google Plus, LinkedIn and Instagram.
Last Login	The Last Login column displays the full date and time when the user last authenticated on the network.
Action	From the Action column perform one of the following actions on a user.    Select Disconnect to end a user's session on the network. Select Block to stop a user passing traffic on the network. Select Unblock to restore the users ability to pass traffic on the network. The user may reconnect if they re-authenticate. Select Delete to remove a user from the database. If the user connects again they will be treated as new user.

- MAC** The **MAC** column displays the MAC address for each listed user. This column is not displayed by default, but may be enabled from the **Columns** menu.
- Mobile** The **Moblie** column displays the mobile phone number for each listed user. This column is not displayed by default, but may be enabled from the **Columns** menu.
- City** The **City** column displays the city associated with each listed user. This column is not displayed by default, but may be enabled from the **Columns** menu.
- SSID** The **SSID** column displays the wireless network SSID that each listed user is connected through. This column is not displayed by default, but may be enabled from the **Columns** menu.
- Network** The **Network** column displays the network that each listed user is connected through. This column is not displayed by default, but may be enabled from the **Columns** menu.

3 Dashboard

Dashboard Basics

Creating a New Dashboard

Available Dashboard Widgets

Access the **Dashboard** screens by selecting **Dashboard** from the menu and selecting one of the following options:

Use Dashboards to simplify the presentation of user data within a system or individual sites. The dashboard utilizes customizable widgets and layout themes and supports multiple dashboards.

[Creating a New Dashboard](#) on page 23

[Available Dashboard Widgets](#) on page 25

Dashboard Basics

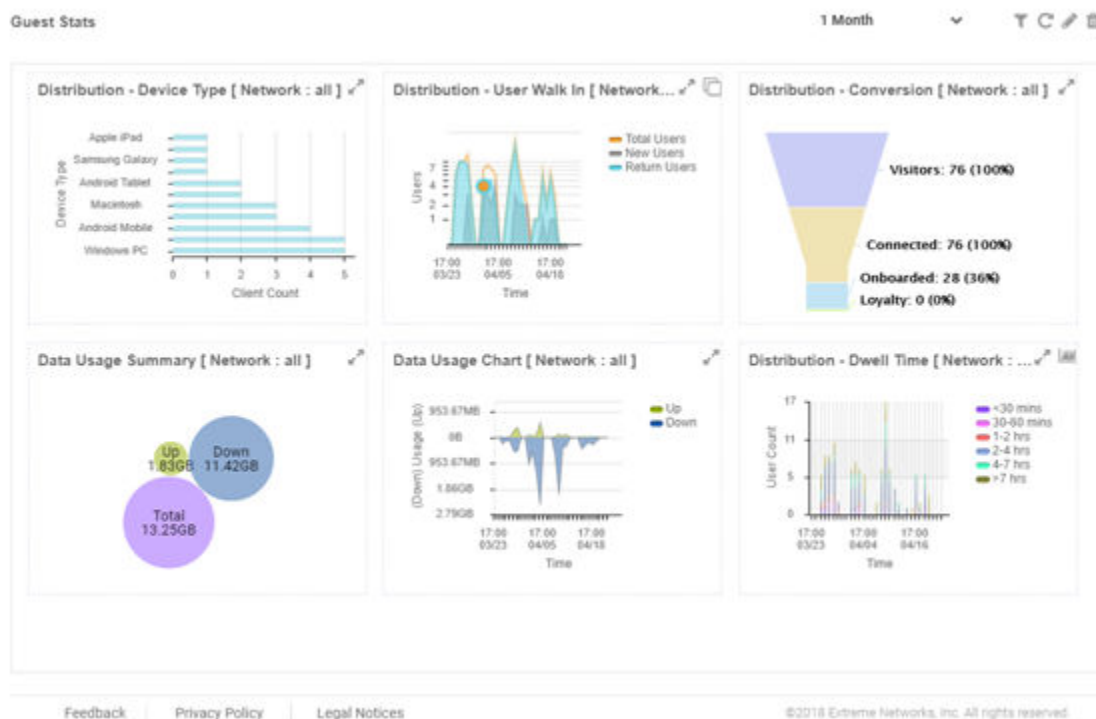


Figure 12: Example Dashboard Screen

Dashboards contain three main components: **Theme**, **Widgets**, and **Time**. The **Theme** controls the layout of a dashboard page and the number of widgets that can be displayed. The **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 25. The **Time** setting controls the period of time that data is displayed for in the widgets.

When accessing a user created dashboard the results can be further filtered by **Network** or by **Time**. To change the **Network** filter select a WLAN from the pull-down menu and the dashboard updates to show only data from that WLAN. To change the **Time** setting, use the pull-down menu to specify a time period of **1 Hour**, **8 Hours**, **1 Day**, **1 Week**, **1 Month**, **3 Months**, **6 Months** or **1 Year**. Changes to the **Network** or **Time** are retained when accessing this dashboard.

Creating a New Dashboard

Describes the steps to create a customized ExtremeGuest dashboard.

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

To create a new dashboard:

- 1 Select **Dashboard** from the menu. Then select **Create New**.

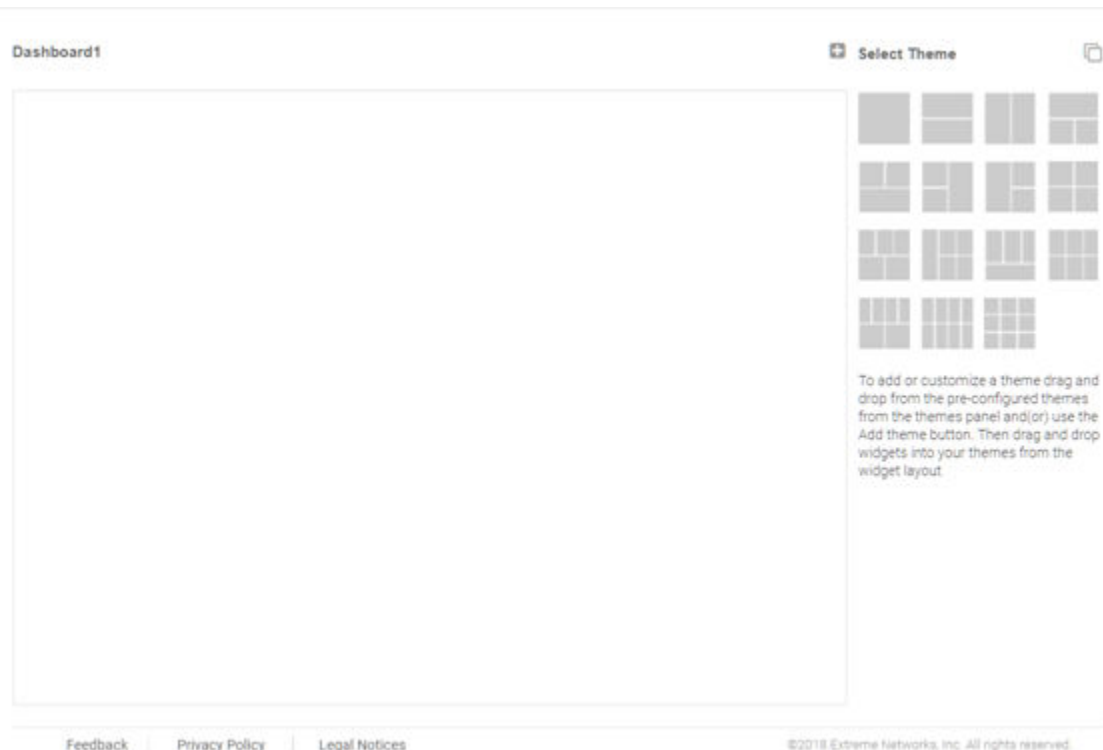


Figure 13: Blank New Dashboard Screen

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

- 2 Select a theme from the **Select Theme** menu by dragging the layout to the main window. To change the layout, drag another theme in place of the current one.

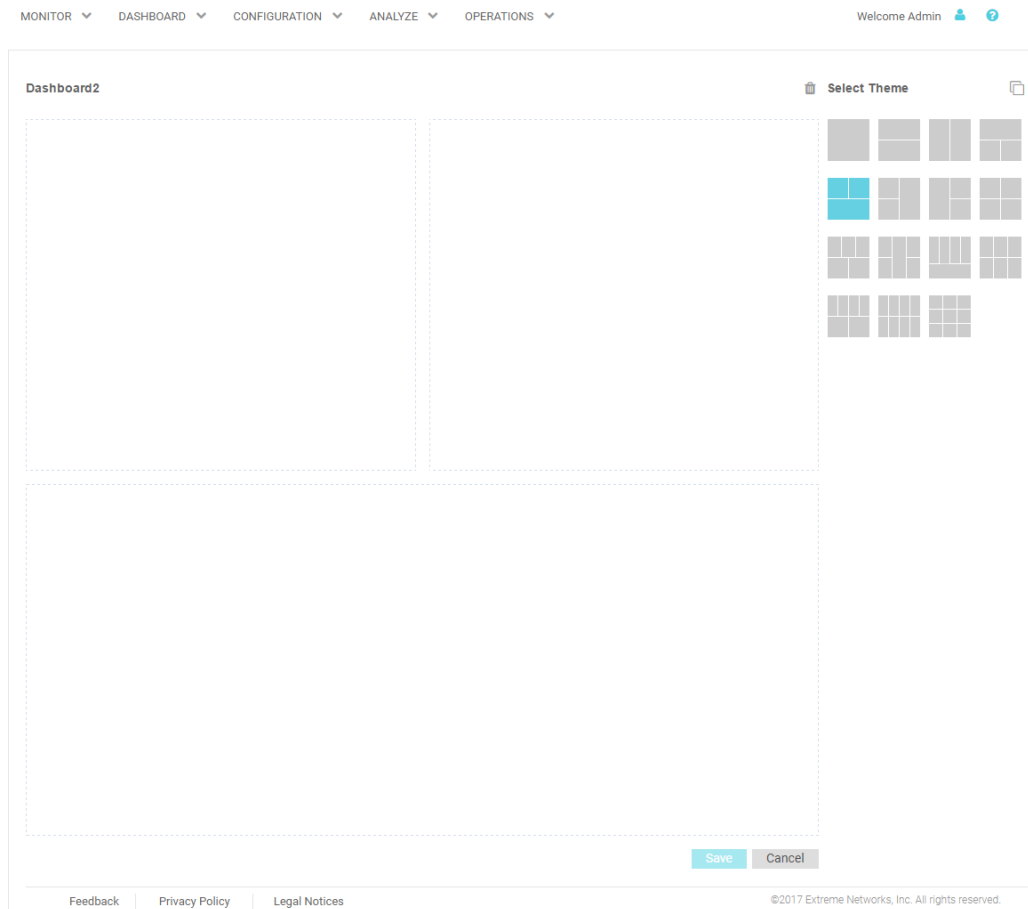


Figure 14: Selecting a Dashboard Theme

When a theme has been selected, an outline of the dashboard layout displays.

- 3 Change to the **Select Widget** view, by clicking on the icon next to **Select Themes**.
- 4 Drag widgets into empty windows to populate the dashboard.

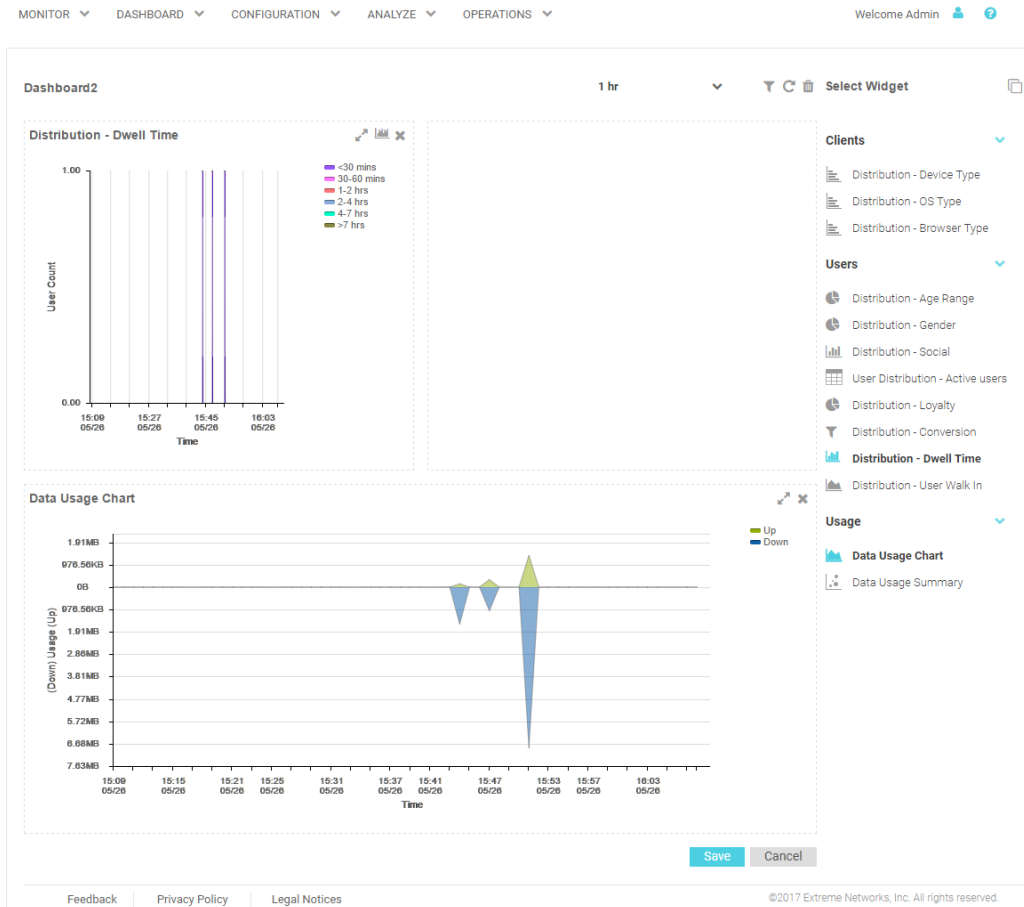


Figure 15: Selecting and Placing Widgets

Available [Dashboard Widgets](#) on page 25

Once a widget is placed it displays the data associated with that widget.

5 Select **Save** to commit the dashboard layout or select **Cancel** to cancel dashboard creation.

When saving a new dashboard provide the following information:

Name The dashboard **Name** is used to identify the customized dashboard. This name displays in the menu when selecting **Dashboard > Dashboard Name**. This value is mandatory.

Description Provide a brief description of the newly created dashboard. This value is optional.

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

6 Select **OK** to finish saving the dashboard.

Available Dashboard Widgets

Category	Widget	Description
Clients	Distribution - Device Type	Bar graph displaying client count sorted by mobile device model.

Category	Widget	Description
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: <ul style="list-style-type: none"> • < 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 the user authenticated using.
Users	User Distribution - Active users	Chart displaying user details for active users. Details include Usericon , Name , Email , Gender , Authentication Source , and Last Login date and time.
Users	Distribution - Loyalty	Graph displaying number of users with the customer app installed on their device.
Users	Distribution - Conversion	Graph displaying the number and percentage of users who converted from Connected to Onboarded to Loyalty customers.
Users	Distribution - Dwell Time	Bar graph displaying the amount of time users stayed at a location over a filtered time period. Filter the Dwell Time information into the following time periods: <ul style="list-style-type: none"> • 1 hour: with data points each minute • 8 hours: with data points each hour • 1 day: with data points each hour • 1 week: with data points each day • 1 month: with data points each day • 3 months: with data points each day
Users	Distribution - User Walk In	Graph displaying the number of users entering a location over a filtered time period. Filter the User Walk In information into the following time periods: <ul style="list-style-type: none"> • 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 <p>Data is further separated between Total Users, Return Users, and New Users.</p>

Category	Widget	Description
Usage	Data Usage Chart	Graph displaying upstream and downstream bandwidth usage over time.
Usage	Data Usage Summary	Graph displaying upstream, downstream, and total bandwidth usage.
Usage	Key Metrics	Infographic displaying user information about online status, device, loyalty and social media sign in status.
Miscellaneous	Label	Custom label for creating Dashboard titles.

4 Configuration

AAA Configuration
Networks
Sites
Devices
Onboarding
Splash Templates
Notification
Social
Vouchers

Access the **Configuration** screens by selecting **Configuration** from the menu and selecting one of the following options:

- [AAA Configuration](#) on page 28
- [Networks](#) on page 35
- [Sites](#) on page 36
- [Devices](#) on page 38
- [Notification](#) on page 44
- [Onboarding](#) on page 39
- [Social](#) on page 49
- [Splash Templates](#) on page 41
- [Vouchers](#) on page 51

AAA Configuration

Configuration > AAA

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

AAA provides a modular way of performing the following services:

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

Authorization Authorization occurs immediately after authentication. Authorization is a method for remote access control, including authorization for services and individual user accounts and profiles. Authorization functions through the assembly of attribute sets describing what the user is authorized to perform. These attributes are compared to information contained in a database for

a given user and the result is returned to AAA to determine the user's actual capabilities and restrictions. The database could be located locally or be hosted remotely on a RADIUS server. Remote RADIUS servers authorize users by associating attribute-value (AV) pairs with the appropriate user. Each authorization method must be defined through AAA. When AAA authorization is enabled it's applied equally to all interfaces.

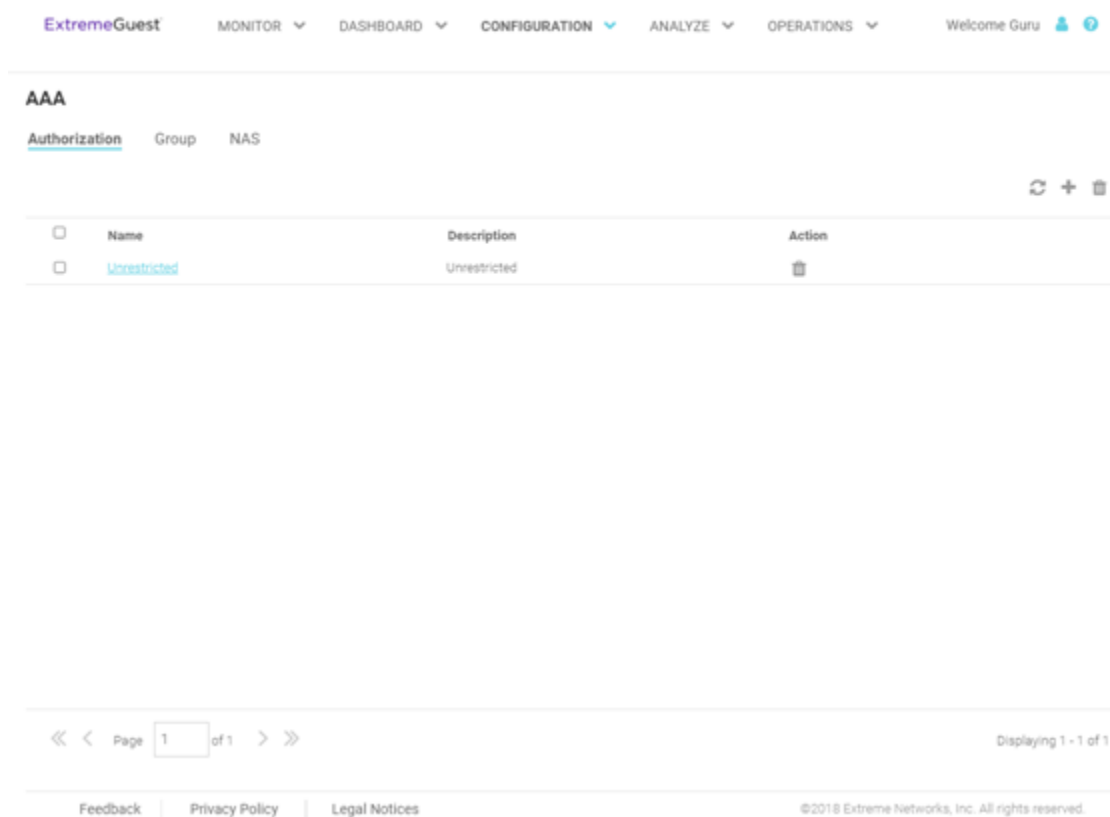
Accounting Accounting is the method for collecting and sending security server information for billing, auditing, and reporting user data; such as start and stop times, executed commands (such as PPP), number of packets, and number of bytes. Accounting enables wireless network administrators to track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

[AAA Authorization](#) on page 29

[AAA Group](#) on page 31

[AAA NAS](#) on page 33

AAA Authorization



ExtremeGuest MONITOR ▾ DASHBOARD ▾ CONFIGURATION ▾ ANALYZE ▾ OPERATIONS ▾ Welcome Guru 👤 ⓘ

AAA

Authorization Group NAS

<input type="checkbox"/>	Name	Description	Action
<input type="checkbox"/>	Unrestricted	Unrestricted	🗑️

⏪ < Page 1 of 1 > ⏩ Displaying 1 - 1 of 1

Feedback | Privacy Policy | Legal Notices ©2018 Extreme Networks, Inc. All rights reserved.

Figure 16: AAA Authorization Screen

The AAA Authorization screen displays the following information about existing AAA Authorization policies:

Name	Displays the unique name assigned to the AAA Authorization policy when it was created.
Description	Displays the description entered when the AAA Authorization policy was created.
Action	Select the Trashcan icon to delete an existing AAA Authentication policy.

Adding AAA Authorization

Configuration > AAA > Authorization > Add



Figure 17: Add AAA Authorization Screen

To add AAA Authorization:

- 1 Select **Configuration > AAA** from the navigation menu.

The **Authorization** screen displays by default.

- 2 Select the **+** icon to create a new authorization profile.

The **Add AAA Authorization** screen displays.

- 3 Configure the following **Authorization** settings:

Name	Specify a unique designation for the new authorization profile. This setting is mandatory.
Description	Enter a description for the new authorization profile. This setting is mandatory.
VLAN	Use the spinner controls assign a specific VLAN to this RADIUS user group. Ensure Dynamic VLAN assignment (single VLAN) is enabled for the network and RADIUS VLAN assignment is configured in the captive portal policy in order for the VLAN assignment to work properly.

- WLAN SSID** Assign a list of SSIDs users within this RADIUS group are allowed to associate with. Assign WLAN SSIDs representative of the configurations a guest user will need to access.
- Rate Limit From Air** Set the rate limit for clients within the RADIUS group. Use the spinner to set value from 100-1,000,000 kbps. Leave this field blank to disable rate limiting.
- Rate Limit To Air** Set the rate limit from clients within the RADIUS group. Use the spinner to set value from 100-1,000,000 kbps. Leave this field blank to disable rate limiting.
- Inactivity Timeout** Set an inactivity timeout from 60 - 86,400 seconds. If a frame is not received from a client within the set time, the current session is terminated.
- Session Timeout** Enable this option to set a client session timeout from 5 - 144,000 minutes. This is the session time a client is granted upon successful authentication. Upon expiration, the RADIUS session is terminated.
- Block Time** Specify a **Block Time** to control the amount of time before a user can reconnect after their session ends.
- Application Policy** Specify an **Application Policy** to associate with this authorization profile.
- Role Policy** Specify a **Role Policy** to associate with this authorization profile.
- 4 To limit access to the network at certain days or times, under **Schedule** select **Restrict Access** and configure the schedule including **Start** time and **End** time. Optionally select **By Day of Week** to limit access on certain days of the week.
 - 5 Select **Save** to save the new authorization profile. Select **Cancel** to discard the new authorization policy.

AAA Group

The screenshot displays the AAA Group configuration interface. At the top, there are tabs for 'Authorization', 'Group' (which is selected), and 'NAS'. Below the tabs, there are icons for refresh, add, and delete. A table lists the configured groups:

Name	Description	Action
<input type="checkbox"/> Alphanet-Guest	Alphanet-Guest	<input type="checkbox"/> [trash icon]

At the bottom of the screen, there is a pagination control showing 'Page 1 of 1' and a 'Displaying 1 - 1 of 1' indicator. Footer links for 'Feedback', 'Privacy Policy', and 'Legal Notices' are also present, along with the copyright notice '©2018 Extreme Networks, Inc. All rights reserved.'

Figure 18: AAA Group Screen

The AAA Group screen displays the following information about existing AAA Groups:

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

Adding AAA Groups

Configuration > AAA > Group > Add

The screenshot shows the 'Add AAA Group' configuration screen. The 'Group' field contains 'Alphanet-Guest'. The 'Description*' field also contains 'Alphanet-Guest'. The 'Type' dropdown menu is set to 'Device', and the 'Authorization' dropdown menu is set to 'Unrestricted'. At the bottom of the form, there are two buttons: 'Save' and 'Cancel'.

Figure 19: AAA Groups Add Screen

To add AAA Groups:

- 1 Select **Configuration > AAA** from the navigation menu.

The **Authorization** screen displays by default.

- 2 Select the **Group** tab.
- 3 Select the **+** icon to create a new group.

The **Add AAA Group** screen displays.

- 4 Configure the following **Group** settings:

Name	Enter a unique name for the new AAA group. This setting is mandatory.
Description	Enter a description for the new AAA group. This setting is mandatory.
Type	Specify the type of group using the pull down menu. Available group types are User and Device .
Authorization	Select an Authorization policy from the pull-down menu.

- 5 Select **Save** to save the new AAA group. Select **Cancel** to discard the new AAA group.

AAA NAS

Configuration > AAA > NAS

The screenshot shows the AAA NAS configuration page. At the top, there is a navigation bar with 'ExtremeGuest' and several menu items: MONITOR, DASHBOARD, CONFIGURATION (selected), ANALYZE, and OPERATIONS. A user profile 'Welcome Guru' is visible on the right. Below the navigation bar, the 'AAA' section is active, with sub-tabs for 'Authorization', 'Group', and 'NAS'. A table lists the configured AAA networks. The table has columns for Name, Description, IP Address/mask, and Action. One entry is shown: 'Alphanet-contr' with description 'Alphanet-controller-ip' and IP address '10.254.130.0/24'. There are icons for refresh, add, and delete at the top right of the table. At the bottom, there is a pagination control showing 'Page 1 of 1' and a footer with '©2018 Extreme Networks, Inc. All rights reserved.'

Name	Description	IP Address/mask	Action
Alphanet-contr	Alphanet-controller-ip	10.254.130.0/24	

Figure 20: AAA NAS Screen

The AAA NAS screen is used to identify and authenticate RADIUS requests from the specified network and displays the following information for each network:

Name	Displays the unique name assigned to the AAA network when it was created.
Description	Displays the description entered when the AAA network was created.
IP Address / mask	Displays the IP address and network mask associated with each network.
Action	Select the Trashcan icon to delete an existing AAA Group.

Adding AAA NAS

NAS

Alphanet-contr

Description*: Test

IP Address/mask*: 10.254.130.0/24

Shared Secret*: ***** Show Shared Secret

Save Cancel

[Feedback](#) | [Privacy Policy](#) | [Legal Notices](#)

©2018 Extreme Networks, Inc. All rights reserved.

Figure 21: AAA NAS Add Screen

To add AAA Networks:

- 1 Select **Configuration** > **AAA** from the navigation menu.

The **Authorization** screen displays by default.

- 2 Select the **NAS** tab.
- 3 Select the **+** icon to create a new group.

The **Add AAA Networks** screen displays.

- 4 Configure the following **Network** settings:

Name	Specify a unique name for the new AAA network. This setting is mandatory.
Description	Specify a description for the new AAA network. This setting is mandatory.
IP Address / mask	Displays the IP address and network mask associated with each network. This setting is mandatory.
Shared Secret	Enter the RADIUS client shared secret password in the Shared Secret field. This password is for authenticating the RADIUS NAS clients. Select the Show check box to expose the shared secret's actual character string, leaving the option unselected displays the shared secret as a string of asterisks (*).

- 5 Select **Save** to save the new AAA network. Select **Cancel** to discard the new AAA network.

Networks

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



Note




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




























- 1 Select **Configuration > Networks** from the main menu.

The **Network** screen displays a list of known networks. If you are using an ExtremeWireless WiNG deployment and have entered the IP address of the ExtremeGuest application, the known networks will auto populate.

- 2 The **Network** screen displays the following:

Networks

For ExtremeWireless WiNG deployments, it is recommended to configure ExtremeGuest IP Address on the WiNG Controller/AP for automatic sync of networks.   

<input type="checkbox"/>	Name	Description	SSID	VLAN	Status	Action
<input type="checkbox"/>	<input type="text"/>		<input type="text"/>	<input type="text"/>		
<input type="checkbox"/>	 GUEST-ACCESS-RE-		EGuest	666		
<input type="checkbox"/>	 STCWLB		stcwlb	100		
<input type="checkbox"/>	 STCWLB-ENTERP-		stcwlb-ent	68,100		
<input type="checkbox"/>	 STCWLB-PL		stcwlb	1		
<input type="checkbox"/>	 CA107-SecondFloor-			68		
<input type="checkbox"/>	 CA107-SecondFloor-			666		
<input type="checkbox"/>	 CA107-SecondFloor-			100		
<input type="checkbox"/>	 CA107-SecondFloor-			400		
<input type="checkbox"/>	 end		end	1		

« < Page of 1 > » Displaying 1 - 9 of 9

[Feedback](#) | [Privacy Policy](#) | [Legal Notices](#) ©2018 Extreme Networks, Inc. All rights reserved.

Figure 22: Networks Screen

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



Note

SSID is only applicable to wireless networks.

Description Displays the optional description associated with each wired or wireless network.

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

- VLAN** Displays the VLAN ID associated with each network. To filter by VLAN, enter the VLAN number in the box at the top of the **VLAN** column.
- Status** The status icon displays green for networks that are online and grey for networks that are disabled. Selecting that icon will toggle the status between online and disabled.
- Action** Select the trashcan icon to remove the associated wired or wireless network from ExtremeGuest.
- 3 Select the **Refresh** icon to update the data in the network table.
 - 4 Select the **+** icon to add a new network. Provide a **Name, Description, VLAN** and **Status**. If the network is a wireless network, additionally enter a **SSID**.
 - 5 To remove multiple networks from ExtremeGuest, select the boxes for each network then select the trashcan icon.

Sites

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



Note

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

- 1 Select **Configuration > Sites** from the main menu.

The **Sites** screen displays a list of known sites. Sites that are enabled display a green icon. Disabled sites display a grey icon. APs connected to disabled sites do not count against the licenses in use. If you are using an ExtremeWireless WiNG deployment and have entered the IP address of the ExtremeGuest application, the known sites will auto populate.

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

Sites

For ExtremeWireless WING deployments, it is recommended to configure ExtremeGuest IP Address on the WING Controller/AP for automatic sync of sites.   

	Name	Description	Country	Region	City	Campus	Time Zone	Action
<input type="checkbox"/>	<input type="text"/>		<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	
<input type="checkbox"/>	CA114.PLEASA		United-States	California	Pleasanton	MSI-CA114	PST8PDT	
<input type="checkbox"/>	CA127.SJC		United-States	California	SanJose	Extremenetwork...	PST8PDT	
<input type="checkbox"/>	Default						Etc/UTC	

  Page of 1  

Displaying 1 - 3 of 3

[Feedback](#) | [Privacy Policy](#) | [Legal Notices](#)

©2018 Extreme Networks, Inc. All rights reserved.

Figure 23: Sites Screen

Name Displays the name associated with each site. To filter by name or portion of a name, enter the string in the box at the top of the **Name** column. Selecting a site name displays a dialogue for editing the site's **Name, Description, Country, Region, City, Campus, Time Zone, Latitude** or **Longitude**. To filter by site name or portion of a site name, enter the string in the box at the top of the **Name** column. To clear the filter select the X icon.

Description Displays the optional description associated with each site.

Country Displays the optional name of the country for each site. To filter by country name or portion of a country name, enter the string in the box at the top of the **Country** column. To clear the filter select the X icon.

Region Displays the optional region associated with each site such as the state, province, or county. To filter by region name or portion of a region name, enter the string in the box at the top of the **Region** column. To clear the filter select the X icon.

City Displays the optional city associated with each site. To filter by city name or portion of a city name, enter the string in the box at the top of the **City** column. To clear the filter select the X icon.

Campus Displays the optional campus name configured for each site. To filter by campus name or portion of a campus name, enter the string in the box at the top of the **Campus** column. To clear the filter select the X icon.

Time Zone Displays an abbreviated version of the optional time zone configured for each site. To filter by time zone, enter the abbreviated time zone name in the box at the top of the **Time Zone** column. To clear the filter select the X icon.

Action Select the trashcan icon to remove the associated site from ExtremeGuest.

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

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

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

Devices

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



Note




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




- Select **Configuration > Devices** from the main menu.

The **Devices** screen displays a list of known devices. If you are using an ExtremeWireless WiNG deployment and have entered the IP address of the ExtremeGuest application, the known devices will auto populate.

- The **Devices** screen displays the following:

Sites

For ExtremeWireless WiNG deployments, it is recommended to configure ExtremeGuest IP Address on the WiNG Controller/AP for automatic sync of sites.   

<input type="checkbox"/>	Name	Description	Country	Region	City	Campus	Time Zone	Action
<input type="checkbox"/>	<input type="text"/>		<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	
<input type="checkbox"/>	CA114-PLEASE		United-States	California	Pleasanton	MSI-CA114	PST8PDT	
<input type="checkbox"/>	CA127-SJC		United-States	California	SanJose	Extremenetwork	PST8PDT	
<input type="checkbox"/>	default						Etc/UTC	

« < Page 1 of 1 > » Displaying 1 - 3 of 3

[Feedback](#) | [Privacy Policy](#) | [Legal Notices](#) ©2018 Extreme Networks, Inc. All rights reserved.

Figure 24: Devices Screen

Name Displays the name associated with each device. To filter by device name or portion of a device name, enter the string in the box at the top of the **Name** column. Selecting a device name displays a dialogue for editing the device's **Name**, **Site Name**, **MAC** address, **Model**, **IP** address, **Network**, and **Managed By** description. To filter by device name or portion of a device name, enter the string in the box at the top of the **Name** column. To clear the filter select the X icon.

- MAC** Displays the MAC address for each known device. To filter by MAC address or portion of a MAC address, enter the string in the box at the top of the **MAC** column. To clear the filter select the X icon.
- Site Name** Displays the site name associated with each device. 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. To clear the filter select the X icon.
- Network** Displays the optional network that each device is associated with. To filter by network name or portion of a network name, enter the string in the box at the top of the **Network** column. To clear the filter select the X icon.
- Reported By** Displays the name of the controller that reported each device to ExtremeGuest.
- Managed By** Displays the name of the controller that is optionally associated with each device.
- Action** Select the trashcan icon to remove the associated device from ExtremeGuest.
- 3 To associate a controller with a device or multiple devices, select the devices from the table and select the checkmark icon. Then select a controller to associate with all selected devices.
 - 4 To remove a controller from a device or multiple devices, select the devices from the table and select the X icon. This will remove the associated controller from all selected devices.
 - 5 Select the **Refresh** icon to update the data in the devices table.
 - 6 Select the **+** icon to add a new device. Provide a **Name**, **Site Name**, **MAC** address, device **Model**, **IP** address, and **Network** and select **Save**.
 - 7 To remove multiple devices from ExtremeGuest, select the boxes for each device then select the trashcan icon.

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:

- [Onboarding Policy](#) on page 39
- [Onboarding Rules](#) on page 41

Onboarding Policy

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

To create an **Onboarding Policy**:

- 1 Select **Configuration > Onboarding > Policy** from the main menu.

Configured onboarding policies display with 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 user created description for each onboarding policy. This field is optional.
- Action** Select the trashcan icon to remove the associated onboarding policy from ExtremeGuest.
- 2 Select the **Refresh** icon to update the data in the onboarding policy table.

3 Select the **+** icon to add a new onboarding policy.

4 Provide the following information:

Policy Name	Enter a name for the onboarding policy.
Policy Description	Enter a description for the onboarding policy.
Criteria Description	Enter a description for each of the matching criteria in the onboarding policy.
Condition(s)	<p>Select one or more of the following matching conditions.</p> <ul style="list-style-type: none"> • User Email Domain • Sponsor Email Domain • Social Type • User Type • LDAP/Directory Group • User's Device Count • Any • <p>These conditions determine when the corresponding Action is triggered. Adding multiple conditions requires all conditions be met before triggerign the Action.</p>
Action	<p>Select an Action from the menu. The Action is the triggered when all of the Condition(s) are met. Select from the following:</p> <p>Deny Access Select this Action to deny network access to any guests matching the configured Condition(s).</p> <p>Register Device Select this Action to register any guests matching the configured Condition(s). Specify the Validity for guest access in Days, Hours, and Minutes. Select a Group for the guest user to join.</p> <p>Send One-Time-Passcode to User Select this Action to deliver a single-use passcode to guests matching the configured Condition(s). 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.</p> <p>Send Passcode to User Select this Action to deliver a multiple use passcode to guests matching the configured Condition(s). 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.</p> <p>Send One-Time-Pass. on Sponsor Approval Select this Action to deliver a single-use passcode to guests matching the configured Condition(s) once the guest has been approved by a sponsor. 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.</p> <p>Send Passcode on Sponsor Approval Select this Action to deliver a multiple use passcode to guests matching the configured Condition(s) once the guest has been approved by a sponsor. 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.</p> <p>Send One-Time-Passcode to Sponsor Select this Action to deliver a single-use passcode to the sponsor when the configured Condition(s) are met. 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.</p>

Send Passcode to Sponsor Select this **Action** to deliver a multiple use passcode to the sponsor when the configured **Condition(s)** are met. 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.

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

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**:

- Select **Configuration > Onboarding > Rules** from the main menu.

Configured onboarding rules display with the following information:

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

- Select the **Refresh** icon to update the data in the onboarding rules list.
- Select the **+** icon to add a new onboarding rule. Provide a **Rule Name**, associated onboarding **Policy, Network, Location**, and **Precedence Level**. Select **Save** when complete to add the onboarding rule.
- To remove multiple onboarding rule from ExtremeGuest, select the boxes for each policy then select the trashcan icon.

Splash Templates

The **Splash Templates** screen is divided between **System Templates** and **User Templates**. The **System Templates** tab displays a summary of available captive portal splash screen templates. System templates may be downloaded and edited then uploaded on the **User Templates** tab. New templates may be added by selecting the upload icon. Select the summary view icon to view a tree view of templates that are hosted by ExtremeGuest.

To view and download **System Templates**:

- Select **Configuration > Splash Templates** from the navigation menu.

The **System Templates** tab displays.

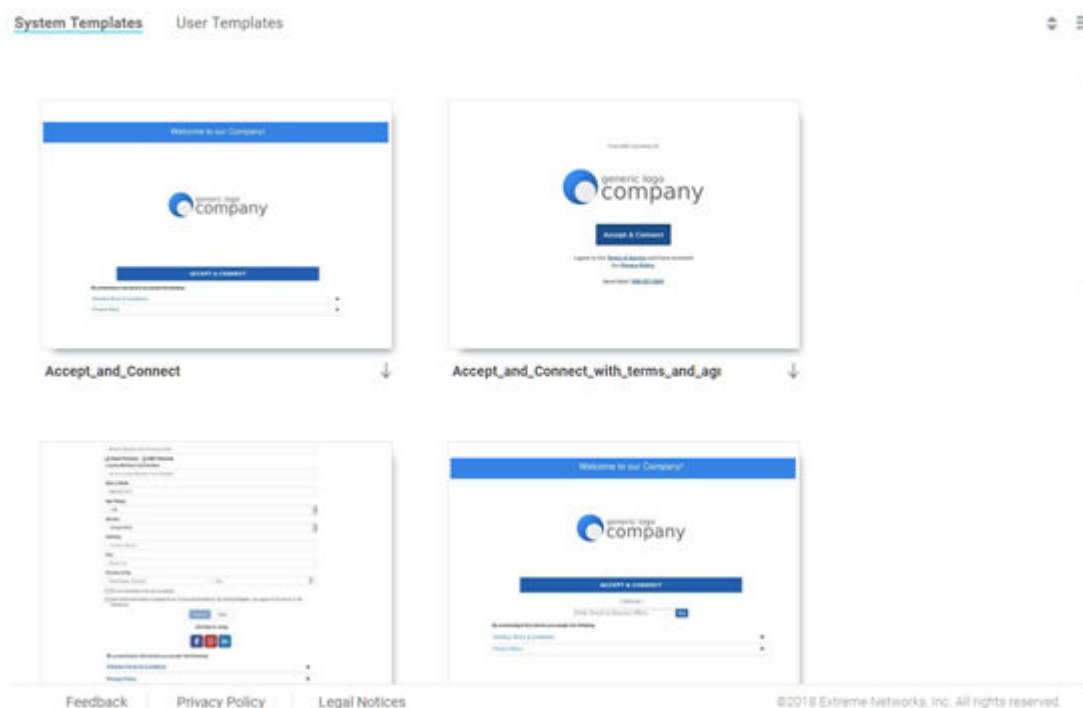


Figure 25: Splash Templates - System Templates Screen

- 2 Select a premade **System Template** from the following options:

Accept_and_Connect Splash template to use for Free WiFi access with a simple Accept & Connect button. Clicking on this button provides internet access and also registers the device with ExtremeGuest.

Accept_and_Connect_with_terms_and_agreement Splash template to use for Free WiFi access with a simple Accept & Connect button and a hyperlink to view terms and conditions. Clicking on this button provides internet access and also registers the device with ExtremeGuest.

Device_Registration_with_Social_WiFi Splash template to use for Free WiFi access with a customizable registration form and social sign-in options. Guest user's device is registered along with their registration or social profile details with ExtremeGuest.

Email_Access Splash template to use for Free WiFi access with an option to capture guest user's **Email Address** or **Mobile Number**. User's device is registered along with their email address or mobile number with ExtremeGuest.

Social_WiFi_with_Facebook_and_GooglePlus Splash template to use for free WiFi access with Facebook or GooglePlus social sign-in options. Guest user's device is registered along with their social profile details with ExtremeGuest.

Social_WiFi_with_all Splash template to use for free WiFi access with customizable Facebook/GooglePlus/LinkedIn/Instagram social sign-in options. Guest user's device is registered along with their social profile details with ExtremeGuest.

Sponsored_Guest_Access Splash template to use for sponsored WiFi access for different category of users, i.e Employees can self-register their devices, Guests and Vendor's can request the sponsor to approve the WiFi access.

User_Registration_with_Social_WiFi Splash template to use for free WiFi access with a customizable user registration form and social sign-in options. Guest user registration details or social media profile details are registered with ExtremeGuest. Guest user receives a One-Time-Passcode/Passcode to sign-in to the network.

User_Registration_with_Social_WiFi_and_Forgot_Passcode

- 3 Click the arrow 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.

To view and upload **User Templates**:

- 1 Select **Configuration > Splash Templates** from the navigation menu.

Select the **User Templates** tab.

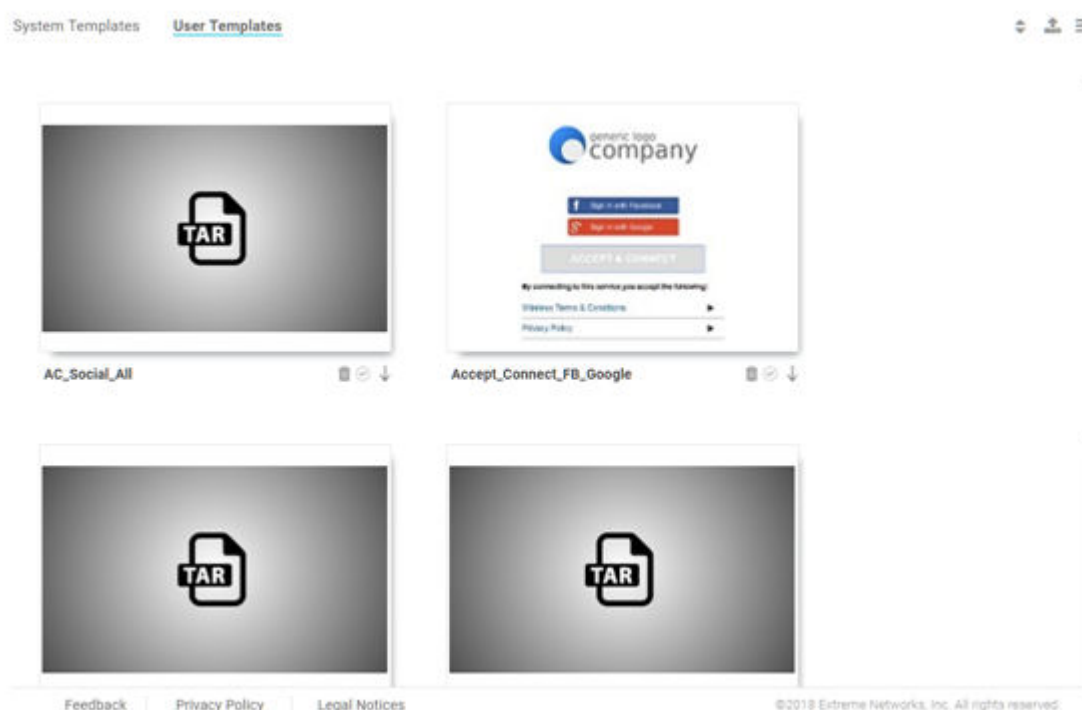


Figure 26: Splash Templates - User Templates Screen

- 2 To upload a template, select the upload icon and select a template to upload from your local filesystem.
- 3 Once the template has uploaded, select the checkbox to activate the template, select the arrow to download the user template locally, and select the trashcan icon to delete it from the list of **User Templates**.

Notification

Configuration > Notification

The **Notifications** screens provide configuration of notification policies and rules to implement them.

[Policy](#) on page 44

[Rules](#) on page 47

Policy

<input type="checkbox"/>	Name	Description	Action
<input type="checkbox"/>	Email_SMS	Email_N_SMS	

Figure 27: Configuration > Notification > Policy Screen

The **Policy** screen displays the following information about existing notification policies:

- Name** Displays the unique name assigned to the notification policy when it was created.
- Description** Displays the description entered when the notification policy was created.
- Action** Select the **Check mark** to apply a notification policy's location filter. Select the **Trashcan** icon to delete an existing notification policy.

Adding a Notification Policy

Configuration > Notification > Policy > Add

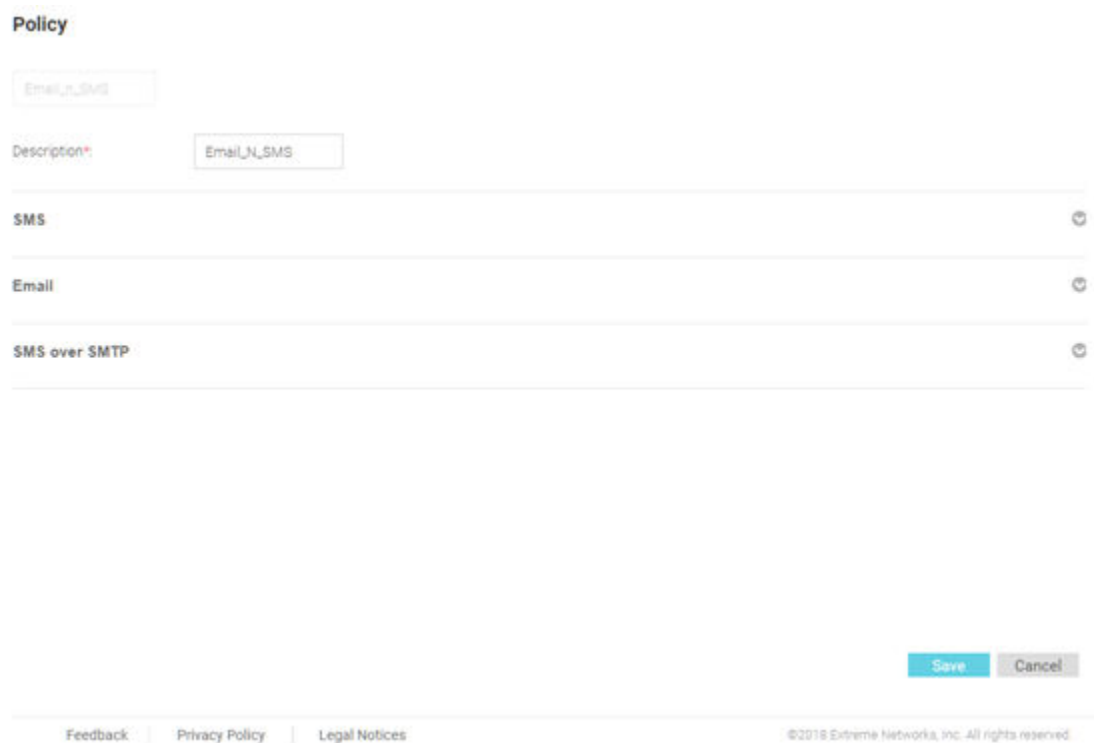
To add a notification policy:

- 1 Select **Configuration > Notification > Policy** from the navigation menu.

The **Policy** screen displays.

- 2 Select the **+** icon to create a new group.

The **Add Policy** screen displays.



Policy

Name: Email_N_SMS

Description*: Email_N_SMS

SMS Email SMS over SMTP

Save Cancel

Feedback | Privacy Policy | Legal Notices | ©2018 Extreme Networks, Inc. All rights reserved.

Figure 28: Add Notification Policy Screen

- 3 Configure the following **Policy** settings:

- | | |
|--------------------|---|
| Name | Provide a unique name for the notification policy. This setting is mandatory. |
| Description | Provide a description for the notification policy. This setting is mandatory. |
- 4 To enable notifications using **SMS** select **Enable** and configure the following SMS settings:
- | | |
|-----------------------|---|
| Host | Select the host for the SMS server. Available host options are: <ul style="list-style-type: none"> • api.clickatell.com • platform.clickatell.com |
| Username | Configure a username unique to this SMS guest management configuration. After configuring the username, specify the associated password. |
| Password | Configures the password associated with the specified username. Selecting Show Password displays the password in plain text on the screen. |
| User / Sponsor | Select User to create a guest user notification policy. Select Sponsor to create a sponsor notification policy. |
| API ID | Set a 32 character maximum API ID. |
| User Agent | The SMS service provider by default is Clickatell, set the User Agent name to pyclickatell. The user-agent value ensures the Clickatell SMS gateway server and its related credentials, needed for sending the pass code to guest users, are configured. |
| Source Number | Configures the long-address or the from-number associated with this Clickatell user account. This setting is mandatory for users in the United States. |

Message Configures the content of the SMS sent to the guest user notifying the pass code (should not exceed 1024 characters). Specify the message content. When entering the message, use the following tags: **GM_NAME** for the guest user's name **GM_PASSCODE** for the pass code. For example: Dear GM_NAME, your internet access pass code is GM_PASSCODE.

5 To enable notifications using **Email** select **Enable** and configure the following Email settings:

Host Configure the SMTP server resource's IPv4 address or host name used for guest management email traffic, guest user credential validation, and pass code reception. Optionally you can use an existing host alias to identify the SMTP server resource.

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

Security Configure the encryption protocol used by the SMTP server when communicating the pass code.

none No encryption used. Use if no additional user authentication is needed beyond the required username and password combination.

SSL Uses SSL encryption. This is the default setting.

STARTTLS Uses STARTTLS encryption.

Username Specify a username unique to this Email guest management configuration. After configuring the username, specify the associated password.

Password Configure the password associated with the specified SMTP user name.

Subject Configure the subject line of the e-mail sent to the guest user notifying the pass code (should not exceed 100 characters).

Message Configure the content of the e-mail sent to the guest user notifying them of a pass code (should not exceed 1024 characters).

6 To enable notifications using **SMS over SMTP** select **Enable** and configure the following Email settings:

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

Sender Configure the sender's e-mail address. The sender here is the guest user receiving the pass code. Guest users require this pass code for registering their guest e-mail credentials using SMTP.

Security Configure the encryption protocol used by the SMTP server when communicating the pass code.

none No encryption used. Use if no additional user authentication is needed beyond the required username and password combination.

SSL Uses SSL encryption. This is the default setting.

STARTTLS Uses STARTTLS encryption.

Username Configure a username unique to this SMTP guest management configuration. After configuring the username, specify the associated password. Ensure that the correct password is provided to receive the pass code required for registering guest user credentials with SMTP.

Password Configure the password associated with the specified SMTP user name.

Email of Recipient Configures the e-mail recipient's e-mail address (should not exceed 64 characters in length).

Subject Configure the subject line of the SMS over SMTP sent to the guest user notifying the pass code (should not exceed 100 characters).

Message Configure the content of the SMS over SMTP sent to the guest user notifying the pass code (should not exceed 1024 characters).

- 7 Select **Save** to save the notification policy. Select **Cancel** to discard the notification policy.

Rules

<input type="checkbox"/>	Rule Name	Policy Name	Location	Network	Precedence	Action
<input type="checkbox"/>	Alphabet_Guest	Email_SMS	CA107-SJC	GUEST-ACCESS-REGIS...	10	

Figure 29: Configuration > Notification > Rules Screen

The **Rules** screen displays the following information about existing notification policies:

- Rule Name** Displays the unique rule name assigned to the rule when it was created.
- Policy Name** Displays the name of the notification policy that was associated with the rule when it was created.
- Location** Displays the site that the notification rule applies to.
- Network** Displays the Network that the notification rule applies to.
- Precedence** Displays the precedence (sequence) that the rules are applied. Rules with higher precedence receive the higher priority. This value is set (from 1 - 1000) for new notification rule configurations.
- Action** Select the **Check mark** to apply a notification policy's location filter. Select the **Trashcan** icon to delete an existing notification policy.

Adding a Notification Rule

Configuration > Notification > Rules > Add

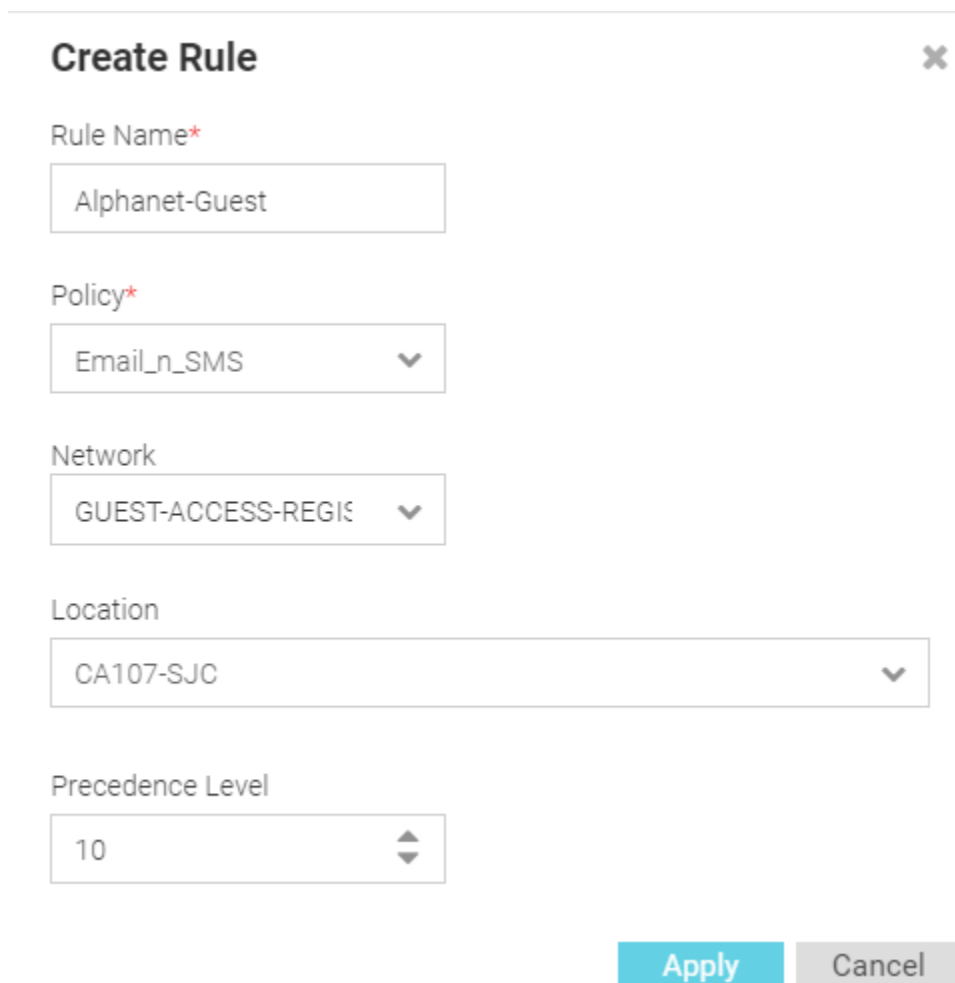
To add a notification rule:

- 1 Select **Configuration > Notification > Rules** from the navigation menu.

The **Rules** screen displays.

- 2 Select the **+** icon to create a new group.

The **Add Rules** screen displays.



Create Rule ✕

Rule Name*
Alphanet-Guest

Policy*
Email_n_SMS ▼

Network
GUEST-ACCESS-REGIE ▼

Location
CA107-SJC ▼

Precedence Level
10 ▲▼

Apply **Cancel**

Figure 30: Create Rules

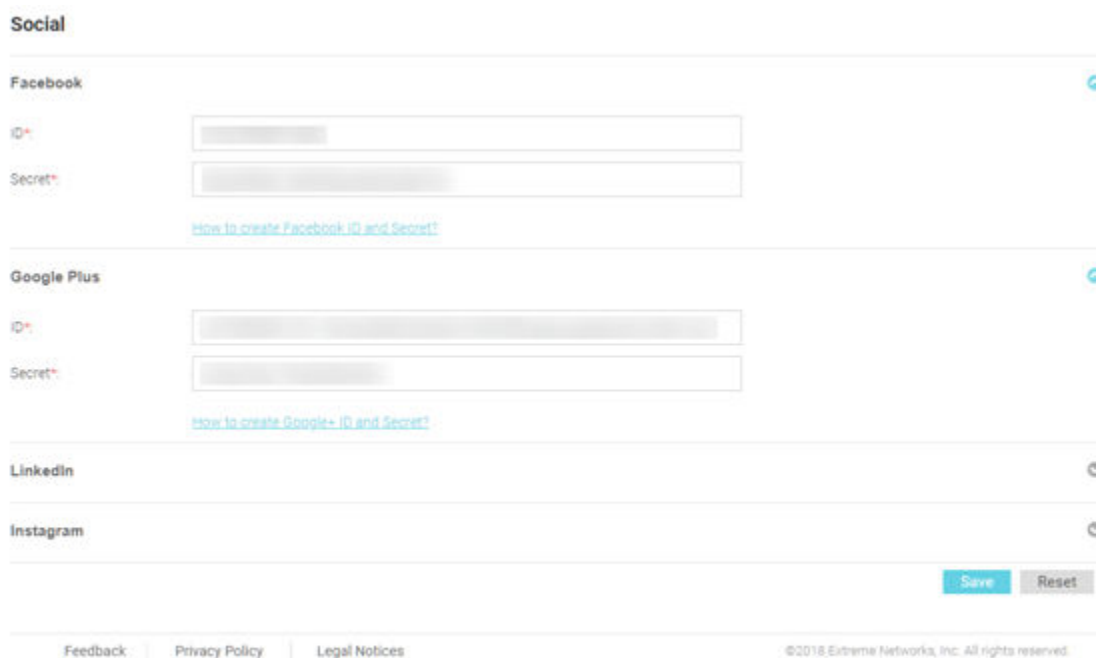
- 3 Configure the following **Policy** settings:

Rule Name	Specify an unique name for the new rule. This setting is mandatory.
Policy	Use the pull-down menu to specify the notification policy to use with the new rule. This setting is mandatory.
Network	Use the pull-down menu to select the networks that the notification rule applies to. To apply the rule to all networks select All Networks .
Location	Use the pull-down menu to navigate the system tree and select the site that the notification rule applies to. To apply the rule to all locations, select System
Precedence Level	Select the precedence (sequence) that the rules are applied. Rules with higher precedence receive the higher priority. This value is set (from 1 - 1000) for new notification rule configurations.

- 4 Select **Apply** to save the new notification rule. Select **Cancel** to discard the new rule and return to the **Rules** screen.

Social

Configuration > Social



Social

Facebook

ID*

Secret*

[How to create Facebook ID and Secret?](#)

Google Plus

ID*

Secret*

[How to create Google+ ID and Secret?](#)

LinkedIn

Instagram

Save Reset

Feedback | Privacy Policy | Legal Notices

©2018 Extreme Networks, Inc. All rights reserved.

Figure 31: Configuration > Social Screen

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

- Facebook
- Google Plus
- LinkedIn
- Instagram

Facebook Configuration

Configuration > Social > Facebook

To add Facebook as an authenticator:

- 1 Select **Configuration > Social** from the navigation menu.
- The **Social** screen displays by default.
- 2 Click the arrow to expand the **Facebook** configuration.
 - 3 Enter the Facebook **ID**.
 - 4 Enter the Facebook **Secret**.
 - 5 For more information about creating a Facebook **ID** and **Secret** click the **How to create Facebook id and secret** link in the user interface.

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

Google Plus Configuration

Configuration > Social > Google Plus

To add Google Plus as an authenticator:

- 1 Select **Configuration > Social** from the navigation menu.
The **Social** screen displays by default.
- 2 Click the arrow to expand the **Google Plus** configuration.
- 3 Enter the Google Plus **ID**.
- 4 Enter the Google Plus **Secret**.
- 5 For more information about creating a Google Plus **ID** and **Secret** click the **How to create Google+ id and secret** link in the user interface.
- 6 Select **Save** to save changes to the Google Plus **ID** and **Secret**.

LinkedIn Configuration

Configuration > Social > LinkedIn

To add LinkedIn as an authenticator:

- 1 Select **Configuration > Social** from the navigation menu.
The **Social** screen displays by default.
- 2 Click the arrow to expand the **LinkedIn** configuration.
- 3 Enter the LinkedIn **ID**.
- 4 Enter the LinkedIn **Secret**.
- 5 For more information about creating a LinkedIn **ID** and **Secret** click the **How to create LinkedIn id and secret** link in the user interface.
- 6 Select **Save** to save changes to the LinkedIn **ID** and **Secret**.

Instagram Configuration

Configuration > Social > Instagram

To add Instagram as an authenticator:

- 1 Select **Configuration > Social** from the navigation menu.
The **Social** screen displays by default.
- 2 Click the arrow to expand the **Instagram** configuration.
- 3 Enter the Instagram **ID**.
- 4 Enter the Instagram **Secret**.
- 5 For more information about creating a Instagram **ID** and **Secret** click the **How to create Instagram id and secret** link in the user interface.
- 6 Select **Save** to save changes to the Instagram **ID** and **Secret**.

Vouchers

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

For detailed voucher configuration see:

- [Create Users](#) on page 51
- [Create End Points](#) on page 52
- [Create Bulk Vouchers](#) on page 53

Create Users

User vouchers can be created individually or in bulk.

To create an individual user voucher:

- 1 Select **Configuration > Vouchers** from the main menu.

The **Users** tab displays by default.

Create Users

[Users](#) [End Points](#) [Bulk Vouchers](#)

First Name:

Last Name:

Email*: Use as username/password

Telephone: Use as username/password

Organization:

Reason:

Username*:

Password*:

User Group:

Location*:

Start Date/Time*:

Expiry Date/Time*:

[Feedback](#) | [Privacy Policy](#) | [Legal Notices](#) ©2018 Extreme Networks, Inc. All rights reserved.

Figure 32: Configuration > Vouchers Create Users Screen

2 Configure the following details for each user voucher:

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



Note

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

Password	Enter a login password for the voucher user.
-----------------	--



Note

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

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

3 When all mandatory fields have been completed, select **Create** to complete voucher creation. To discard any changes made to the form select **Clear**.

Create End Points

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

To create an end point voucher:

- 1 Select **Configuration > Vouchers** from the main menu.
The **Users** tab displays by default.

Create End Points

Users **End Points** Bulk Vouchers

Mac Address*: AA-BB-CC-DD-EE-FF*

Host Name: hostname.com

User Group*: User Group ▼

Network*: Network ▼

Location*: Location ▼

Expiry Time*: Expiry Time 📅

Create Clear

Feedback | Privacy Policy | Legal Notices

©2018 Extreme Networks, Inc. All rights reserved.

Figure 33: Configuration > Vouchers Create End Points Screen

- 2 Select the **End Points** tab.
- 3 Configure the following details for each end point voucher:
 - MAC Address** Enter the MAC address for the end point. The MAC address should be added in the following format: *AA-BB-CC-DD-EE-FF*
 - Host Name** Optionally, enter a hostname to associate with the network end point.
 - User Group** Select a user group from the list to associate it to the network end point.
 - Network** Select a network from the list to associate it to the network end point.
 - Location** Select a location from the list to associate it to the network end point.
 - Expiry Time** Use the calendar to specify the ending date and time that the end point will be deactivated.
- 4 When all mandatory fields have been completed, select **Create** to complete voucher creation. To discard any changes made to the form select **Clear**.

Create Bulk Vouchers

- 1 Select **Configuration > Vouchers** from the main menu. The **Users** tab displays by default.

Create Bulk Vouchers

Users End Points Bulk Vouchers

User Group*:

Number of Vouchers*: (2 - 20000)

Description:

Location*:

Start Date/Time*:

Expiry Date/Time*:

Figure 34: Configuration > Vouchers Create Bulk Vouchers Screen

- 2 Select the **Bulk Vouchers** tab.
- 3 Configure the following details for bulk voucher creation:

User Group	Select a user group from the list to associate it to the group of bulk created vouchers.
Number of Vouchers	Enter a value or use 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 pulldown menu to specify the starting date and time to activate the group of bulk created vouchers.
Expiry Date / Time	Use the calendar and pulldown menu to specify the ending date and time that the bulk created vouchers will be deactivated.
- 4 When all mandatory fields have been completed, select **Create** to complete bulk voucher creation. To discard any changes made to the form select **Clear**.

5 Analyze

Analyze End Points Reports Analyze Users

Access the **Analyze** screens by selecting **Analyze** from the menu and selecting one of the following options:

- [Analyze End Points](#) on page 56
- [Reports](#) on page 57
 - [Generated Reports](#) on page 58
 - [Manage Reports](#) on page 59
 - [Scheduled Reports](#) on page 62
- [Analyze Users](#) on page 63

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

Analyze End Points

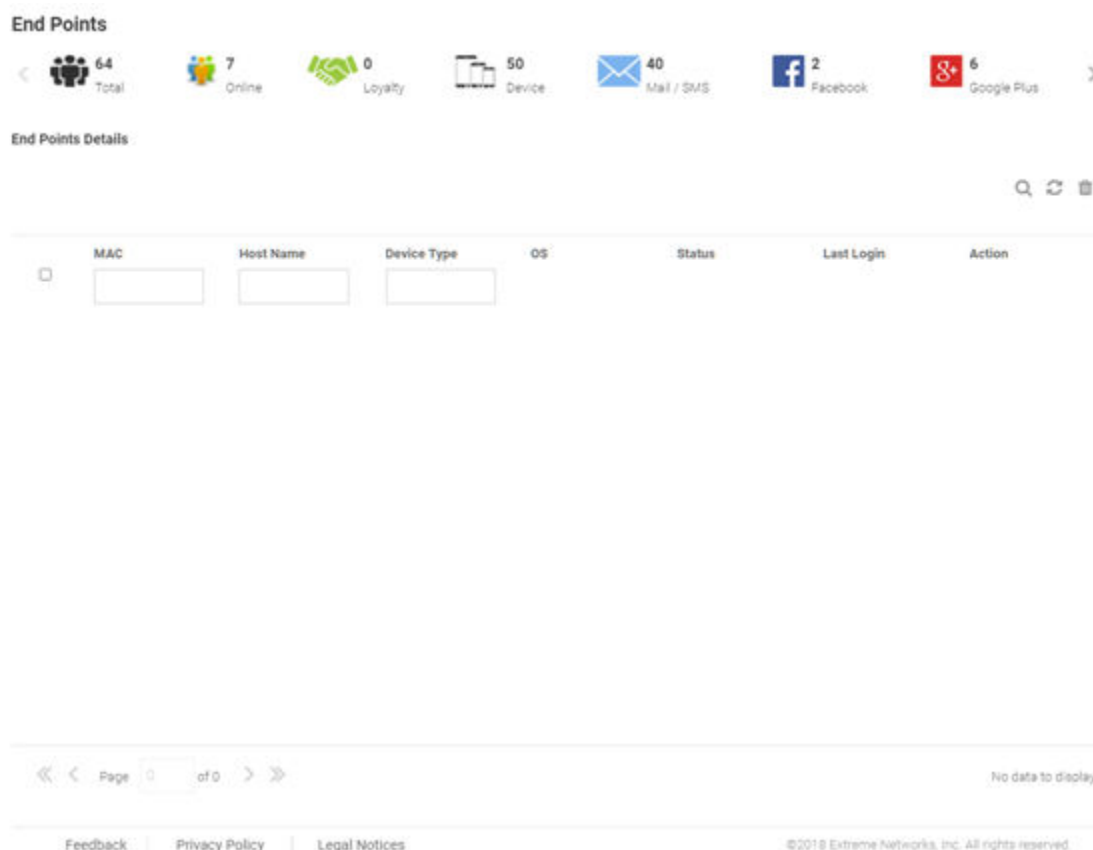


Figure 35: Analyze End Points Screen

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

- MAC** The **MAC** column displays the MAC (Media Access Control) Address associated with each end point.
- Host Name** The **Host Name** column displays the Host Name associated with each end point.
- Device Type** The **Device Type** column displays the device model associated with each end point.
- OS** The **OS** column displays the operating system used by each end point.
- Status** The **Status** column displays the authentication status of each end point.
- Last Login** The **Last Login** column displays the full date and time when the end point last authenticated on the network.
- Action** From the **Action** column perform one of the following actions on an end point. Select **Block** to stop an end point from passing traffic on the network. Select **Disconnect** to terminate an end point's session on the network. Select **Delete** to remove an end point from the database. If the end point connects again they will be treated as new end point.

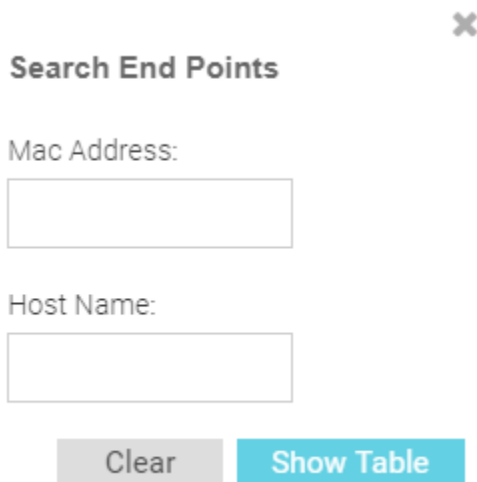
[Filtering End Points Results](#) on page 56

Filtering End Points Results

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

To filter end point results:

- 1 Select **Analyze > End Points** from the navigation menu.
- 2 Select the search icon in the upper right of the table.
- 3 Configure any one or more of the following filter options:



✕

Search End Points

Mac Address:

Host Name:

Clear Show Table

Figure 36: Filtering End Points

MAC Address Enter a MAC Address or portion of a MAC address to display only users that match this filter.

Host Name Enter a Host Name or portion of a Host Name address to display only users that match this filter.

- 4 When all filters have been configured select **Show Table** to display the filtered results. Select **Clear** to remove any text entered into the search fields.

Reports

Analyze > Reports

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

Users	The Users report is a consolidated report of the following:
Social	Bar chart displaying users online and total users categorized by social networking site.
Age	A pie chart displaying users classified by age group and percentage.
Gender	Pie chart displaying the percentage of users based on gender.
User Trend	Graph displaying total users, returning users and new users plotted against each week and number users visited.
Visitors	Pie chart displaying new visitors vs returning users.
Devices	The Devices report is a consolidated report of the following:
Device	Pie chart displaying the percentage of devices by type for connected clients.

Operating System Pie chart displaying the percentage of operating system by type for connected clients.

Device Browser Pie chart to displaying the percentage for each browser type used by registered clients.

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

Generated Reports

Generated Reports

Report	Type	User	Generated At	Action
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>		
<input type="checkbox"/> GuestVisitHistoryLastMonth	Guest Visit History	guru	4/22/2018, 3:00:00 PM	
<input type="checkbox"/> GuestVisitHistoryLastMonth	Guest Visit History	guru	4/21/2018, 3:00:00 PM	
<input type="checkbox"/> GuestVisitHistoryLastMonth	Guest Visit History	guru	4/20/2018, 3:00:00 PM	
<input type="checkbox"/> GuestVisitHistoryLastMonth	Guest Visit History	guru	4/19/2018, 3:00:01 PM	
<input type="checkbox"/> GuestVisitHistoryLastMonth	Guest Visit History	guru	4/18/2018, 3:00:01 PM	
<input type="checkbox"/> GuestVisitHistoryLastMonth	Guest Visit History	guru	4/17/2018, 3:00:01 PM	
<input type="checkbox"/> GuestVisitHistoryLastMonth	Guest Visit History	guru	4/16/2018, 3:00:00 PM	
<input type="checkbox"/> GuestVisitHistoryLastMonth	Guest Visit History	guru	4/15/2018, 3:00:00 PM	
<input type="checkbox"/> GuestVisitHistoryLastMonth	Guest Visit History	guru	4/14/2018, 3:00:01 PM	
<input type="checkbox"/> GuestVisitHistoryLastMonth	Guest Visit History	guru	4/13/2018, 3:00:01 PM	
<input type="checkbox"/> GuestVisitHistoryLastMonth	Guest Visit History	guru	4/12/2018, 3:00:01 PM	
<input type="checkbox"/> GuestVisitHistoryLastMonth	Guest Visit History	guru	4/11/2018, 3:00:01 PM	
<input type="checkbox"/> GuestVisitHistoryLastMonth	Guest Visit History	guru	4/10/2018, 3:00:01 PM	

Page 1 of 4 Displaying 1 - 30 of 114

Feedback | Privacy Policy | Legal Notices ©2018 Extreme Networks, Inc. All rights reserved.

Figure 37: Generated Reports Screen

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

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

Manage Reports

Manage Reports + ↻ 🗑

<input type="checkbox"/>	Report	Type	User	Start Date	End Date	Frequency	Action
<input type="checkbox"/>	LastWeekGuestVis...	Guest Visit History	guru	Tue Jan 23 2018 00:...	Sat Mar 31 2018 00:...	Weekly	🗑
<input type="checkbox"/>	UsersLastDay	Users	guru	Tue Jan 23 2018 00:...	Sat Mar 31 2018 00:...	Daily	🗑
<input type="checkbox"/>	Devices	Devices	guru	Tue Jan 23 2018 00:...	Sat Mar 31 2018 00:...	Monthly	🗑
<input type="checkbox"/>	GuestVisitHistory...	Guest Visit History	guru	Tue Mar 13 2018 0...	Mon Apr 30 2018 0...	Daily	🗑

<< < Page of 1 > >> Displaying 1 - 4 of 4

[Feedback](#) | [Privacy Policy](#) | [Legal Notices](#) ©2018 Extreme Networks, Inc. All rights reserved.

Figure 38: Manage Reports Screen

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

- Report** Displays the report name for each existing generated report.
- Type** Displays the report type for each generated report. The field at the top of this column allows filtering the **Type** by keyword.
- User** Displays the user that generated each report. The field at the top of this column allows filtering the **User** by keyword.
- Start Date** Displays the starting date and time that each report was initiated.
- End Date** Displays the ending date and time that each report was completed.
- Frequency** Displays the interval that each report is scheduled to run.
- Action** Select the **Trashcan** icon to delete a generated report.

Adding a Report

To create a new report:

- 1 Select **Analyze > Reports > Manage Reports** from the navigation menu

The **Add Reports** screen displays.

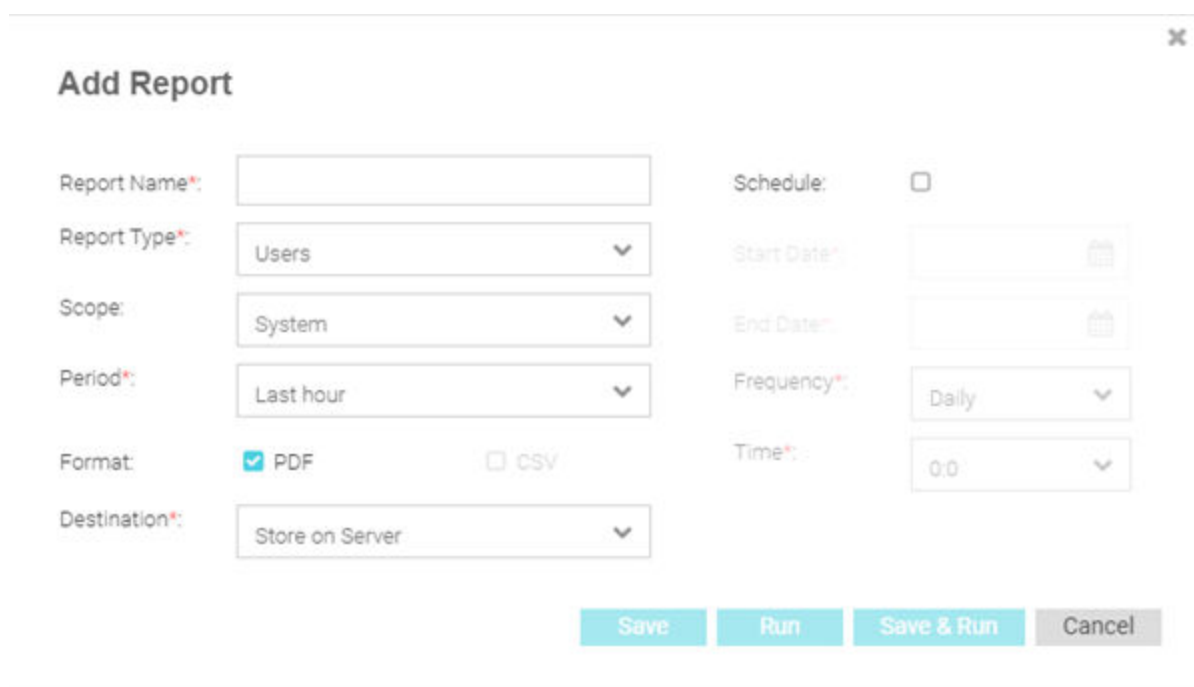


Figure 39: Add Reports Screen

2 Configure the following information to create a new report:

Report Name Specify a unique name for the new report. This setting is mandatory.

Report Type There are three different types of reports can be created:

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

Social Bar chart displaying users online and total users categorized by social networking site.

Age A pie chart displaying users classified by age group and percentage.

Gender Pie chart displaying the percentage of users based on gender.

User Trend Graph displaying total users, returning users and new users plotted against each week and number users visited.

Visitors Pie chart displaying new visitors vs returning users.

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

Device Pie chart displaying the percentage of traffic generated by the device's name.

Operating System Pie chart displaying the percentage of traffic generated by the user's operating system.

Device Browser Pie chart to displaying the percentage of traffic generated sorted by the user's browser.

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

- Scope** Use the **Scope** menu to navigate the system tree and select which sites to include in the report. To include all site, select **System**.
- Period** Select the time period for the report to include. Available options are:
- Last Hour
 - Last Day
 - Last Week
 - Last Month
 - Custom
- Format** Select an output format to generate the report in. Available options are:
- PDF
 - CSV
- Destination** Select a destination to save the reports to. Available options are:
- Store on Server
 - Store & Mail
- Recipient Email** When **Store & Mail** is selected in **Destination**, specify the Email address to send the report to.
- Email Policy** When **Store & Mail** is selected in **Destination**, use the pull-down menu to select an Email policy to use when sending the report. To create a new policy select **Configuration > Notification > Policy** and select **+**.
- 3 To run the new report on a schedule, select **Schedule** and configure the **Start Date, End Date, Frequency,** and **Time**.
 - 4 When all configuration is complete, select **Save** to save the new report. Select **Run** to execute the report without saving it. Select **Save & Run** to save the new report and run it. Select **Cancel** to discard the new report without saving.

Scheduled Reports

Scheduled Reports ↻ 🗑

<input type="checkbox"/>	Report	Type	User	Start Date	End Date	Frequency	Action
<input type="checkbox"/>		<input type="text"/>	<input type="text"/>				
<input type="checkbox"/>	Devices	Devices	guru	Tue Jan 23 2018 00:00:00	Sat Mar 31 2018 00:00:00	Monthly	🗑
<input type="checkbox"/>	GuestVis/HHistoryLa...	Guest Visit History	guru	Tue Mar 13 2018 00:00:00	Mon Apr 30 2018 00:00:00	Daily	🗑

<< < Page of 1 > >> Displaying 1 - 2 of 2

[Feedback](#) | [Privacy Policy](#) | [Legal Notices](#) ©2018 Extreme Networks, Inc. All rights reserved.

Figure 40: Scheduled Reports Screen

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

- Report** Displays the report name for each existing generated report.
- Type** Displays the report type for each generated report. The field at the top of this column allows filtering the **Type** by keyword.
- User** Displays the user that generated each report. The field at the top of this column allows filtering the **User** by keyword.
- Start Date** Displays the starting date and time that each report was last initiated.
- End Date** Displays the ending date and time that each report was last completed.
- Frequency** Displays the interval that each report is scheduled to run.
- Action** Select the **Trashcan** icon to delete a scheduled report.

Analyze Users

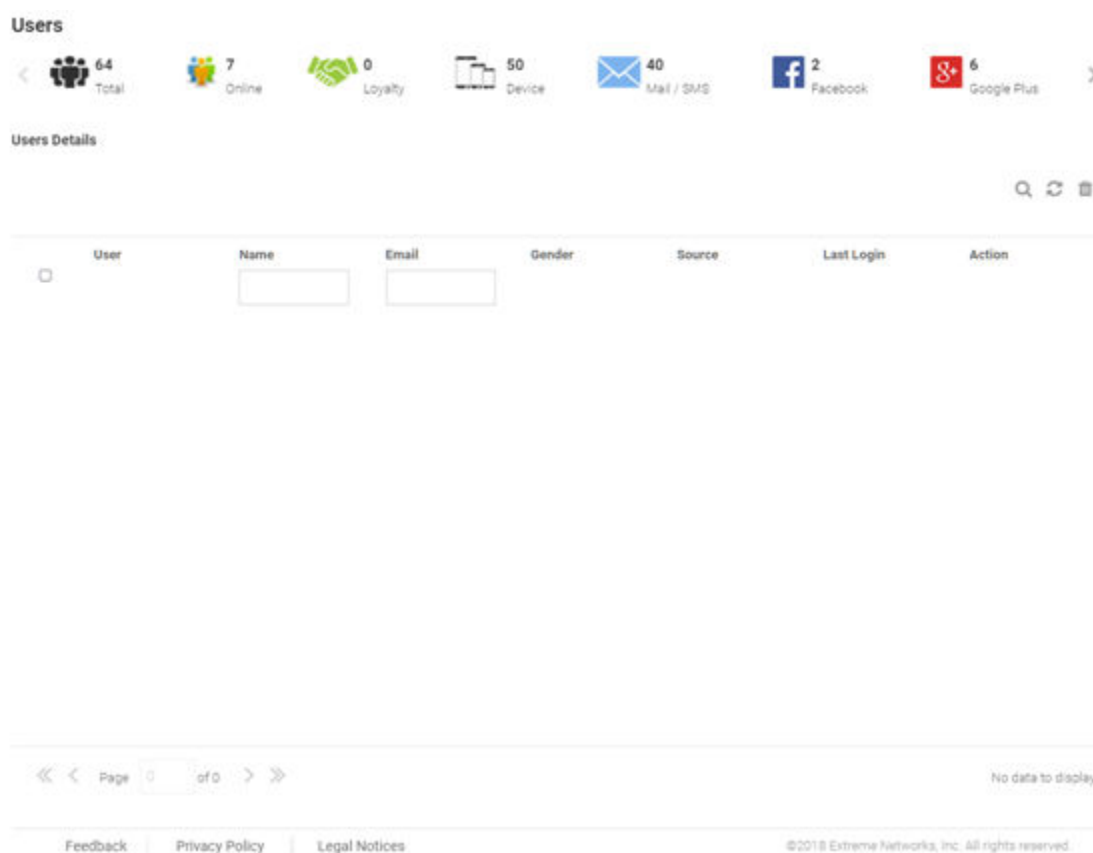


Figure 41: Analyze Users Screen

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

- User** The **User** column displays the user icon associated with each online user.
- Name** The **Name** column displays the username associated with each online user.
- Email** The **Email** column displays the e-mail address associated with each online user.
- Gender** The **Gender** column displays an icon representing the gender of each online user.
- Source** The **Source** column displays the method that each online user used to authenticate. When social media authentication is enabled this will include Facebook, Google Plus, LinkedIn and Instagram.
- Last Login** The **Last Login** column displays the full date and time when the user last authenticated on the network.
- Action** From the **Action** column perform one of the following actions on a user. Select **Block** to stop a user from passing traffic on the network. Select **Disconnect** to end a user's session on the network. The user may reconnect if they re-authenticate. Select **Delete** to remove a user from the database. If the user connects again they will be treated as new user.

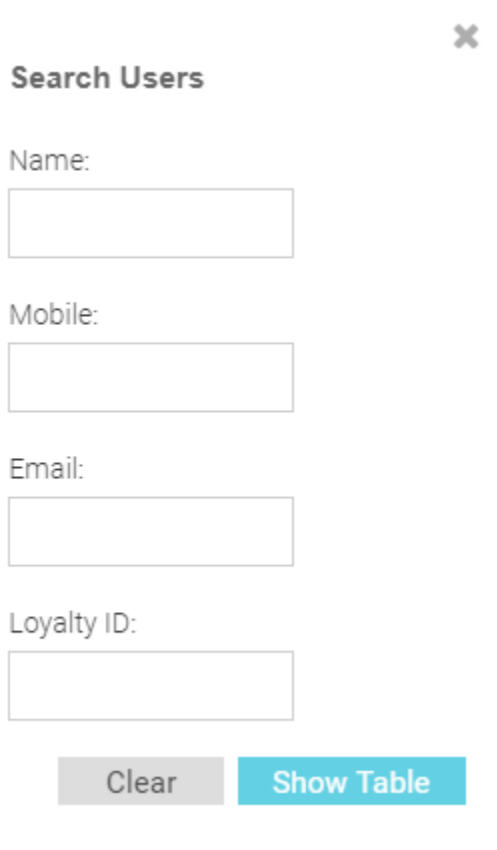
[Filtering User Results](#) on page 64

Filtering User Results

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

To filter user results:

- 1 Select **Analyze > Users** from the navigation menu.
- 2 Select the search icon in the upper right of the table.
- 3 Configure any one or more of the following search options:



Search Users ✕

Name:

Mobile:

Email:

Loyalty ID:

Figure 42: Filtering the Analyze Users Screen

- Name** Enter a user name or portion of a name to display only users that match this filter.
- Mobile** Enter a user's mobile number or a portion of a user's mobile number to display only users that match this filter.
- Email** Enter an Email address or portion of an address such as a domain to display only users that match this filter.
- Loyalty ID** Enter a user's loyalty ID number to display only users that match this filter. Loyalty ID should be enabled as a separate field during guest registration.
- 4 When all filters have been configured select **Show Table** to display the filtered results. Select **Clear** to remove any text entered into the search fields.

6 Operations

Database
License
Maintenance
REST API
Troubleshooting

Access the **Operations** screens by selecting **Operations** from the menu and selecting one of the following options:

- [Database](#) on page 65
- [License](#) on page 68
- [Maintenance](#) on page 69
- [REST API](#) on page 71
- [Troubleshooting](#) on page 71

Database

Operations > Database

The **Operations > Database** screens contain the following screens:

- [Database Export](#) on page 66Export
- [Database Import](#) on page 67Import

Database Export

Export

Protocol*: Protocol

IP Address/Hostname*: XXX.XXX.XXX.XXX

Username*: Username

Password*: Password

Path: Path

Filters:

- Network
- Time
- Location

File Type:

- JSON
- CSV

Export Reset

[Feedback](#) | [Privacy Policy](#) | [Legal Notices](#)

©2018 Extreme Networks, Inc. All rights reserved.

Figure 43: Operations > Database > Export Screen

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

To export a database:

- 1 Select **Operations > Database > Export** from the navigation menu.
- 2 Configure the following server options to export the database:

Protocol	Select the protocol used for exporting the guest user database. Available options are: <ul style="list-style-type: none"> • SFTP • TFTP • FTP
IP Address / Hostname	Provide a hostname string or numeric IP address of the server to export the guest user database to. Hostname cannot include an underscore character.
Username	Specify the username for the user authenticating to the remote server.
Password	Specify the password for the user authenticating to the remote server.
Path	Specify the path on the remote server where the guest user database file is copied to. Enter the complete relative path to the file on the remote server.
Filters	Optionally, specify which filters to apply to the database export. Available options are Network , Time , and Location . If selecting one or more of these options, use the associated pull-down menu to filter the database export.

- File Type** Specify the file format for the exported database. Available options are: **JSON** and **CSV**.
- When all server parameters have been configured, select **Export** to execute the database export. Select **Reset** to remove server information from the screen.

Database Import

Import

Protocol*

IP Address/
Hostname*

Username*

Password*

Path*

File Type: JSON

Figure 44: Operations > Database > Import Screen

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

To import a database:

- Select **Operations > Database > Import** from the navigation menu.
- Configure the following server options to import the database from:

- Protocol** Select the protocol used for importing the guest user database. Available options are:
- SFTP
 - TFTP
 - FTP
- IP Address/
Hostname** Provide a hostname string or numeric IP address of the server to import the guest user database from. Hostname cannot include an underscore character.
- Username** Specify the username for the user authenticating to the remote server.

- Password** Specify the password for the user authenticating to the remote server.
- Path** Specify the path on the remote server where the guest user database file are copied from. Enter the complete relative path to the file on the remote server.
- File Type** Specify the file format for the exported database. Available options are: **JSON**
- When all server parameters have been configured, select **Import** to execute the database export. Select **Reset** to remove server information from the screen.

License

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

To access the **License** page:

- Select **Operations** > **Licenses** from the main menu.

The license screen displays the following ExtremeGuest license information:

License

Product ID: 48781D86932C1F38

License Key*:

License installed: 100 End Point(s) [Never Expires](#)

License Used: 64

License Available: 36

[Update License](#) [Cancel](#)

Figure 45: Operations > License Screen

- Product ID** Displays the unique product ID for this ExtremeGuest installation. This product ID is needed to generate the ExtremeGuest license key.
- License Key** Enter a key into this field to activate a new license.

- License Installed** Displays the number of end point licenses are configured for this ExtremeGuest installation. The system includes a license for 100 end points.
- License Used** Displays the number of end point licenses currently in use.
- License Available** Displays the number of end point licenses available for use. This number is the number of installed licenses minus the current number of licenses in use.

**Note**

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

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

Maintenance

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

To view the maintenance screen:

- 1 Select **Operations** > **Maintenance** from the main menu.

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

Maintenance

Deleted Devices There are 6 Deleted Devices. [Delete All](#)

<input type="checkbox"/>	Name	Mac address	location	Reported by	Offline	Offline since	Action
<input type="checkbox"/>							
<input type="checkbox"/>			/United-States/Calif..	84-24-8D-7F-34-17	0 days 2 hours	04/23/2018 12:01 ..	
<input type="checkbox"/>			/United-States/Calif..	84-24-8D-7F-34-17	0 days 2 hours	04/23/2018 12:01 ..	
<input type="checkbox"/>			/United-States/Calif..	84-24-8D-7F-34-17	0 days 2 hours	04/23/2018 12:01 ..	
<input type="checkbox"/>			/United-States/Calif..	84-24-8D-7F-34-17	0 days 2 hours	04/23/2018 12:01 ..	
<input type="checkbox"/>			Triv-LAB-Sensor	84-24-8D-7F-34-17	0 days 2 hours	04/23/2018 12:01 ..	
<input type="checkbox"/>			/United-States/Calif..	84-24-8D-7F-34-17	0 days 2 hours	04/23/2018 12:01 ..	

Offline Devices for days hours There are 2 Offline Devices. [Delete All](#)

<input type="checkbox"/>	Name	Mac address	location	Reported by	Offline	Offline since	Action
<input type="checkbox"/>							
<input type="checkbox"/>			/United-States/Calif..	84-24-8D-7F-34-17	.26 days 4 hours	03/28/2018 10:23 ..	
<input type="checkbox"/>			/United-States/Calif..	84-24-8D-7F-34-17	.26 days 4 hours	03/28/2018 10:23 ..	

Reset ExtremeGuest to Defaults [Reset](#)

[Feedback](#) | [Privacy Policy](#) | [Legal Notices](#) ©2018 Extreme Networks, Inc. All rights reserved.

Figure 46: Operations > Maintenance Screen

- 2 To view details of **Deleted Devices** select the arrow to expand the panel. The **Deleted Devices** section displays the **Name**, **MAC Address**, **Location**, controller **Reported by**, **Offline** duration, and **Offline since** date. The **Action** column allows individual devices to be removed.
- 3 Select **Delete All** to remove all **Deleted Devices** from ExtremeGuest.
- 4 To view details of **Offline Devices** select the arrow to expand the panel. Select the number of **Days** and **Hours** to filter the devices included. The **Offline Devices** section displays the **Name**, **MAC Address**, **Location**, controller **Reported by**, **Offline** duration, and **Offline since** date. The **Action** column allows individual devices to be removed.
- 5 Select **Delete All** to remove all **Offline Devices** from ExtremeGuest.
- 6 To reset the ExtremeGuest system to default settings, select **Reset** next to **Reset ExtremeGuest to Defaults**. This will erase all data and settings from the ExtremeGuest application.

REST API

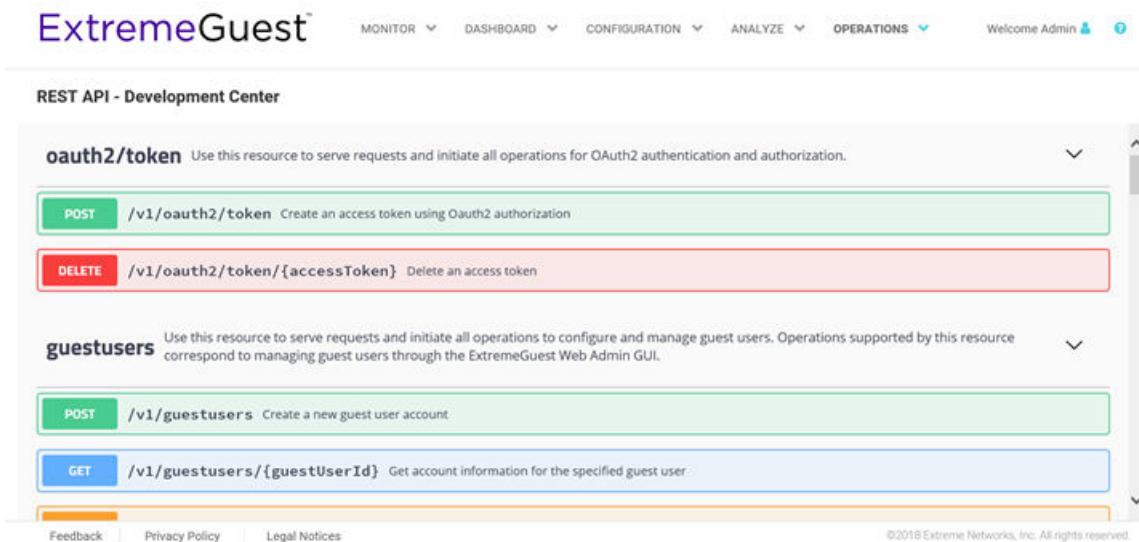


Figure 47: Operations > REST API Screen

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

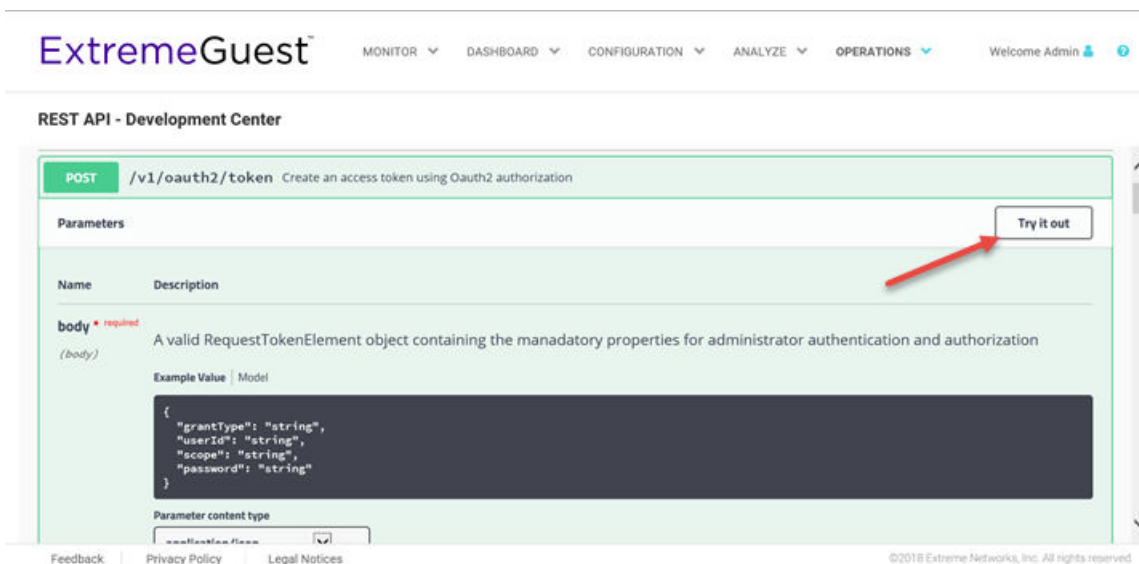


Figure 48: Try Out Feature to Test API Calls

For detailed information about ExtremeGuest's REST API functionality see [About the ExtremeGuest REST API](#) on page 74.

Troubleshooting

The **Operations > Troubleshooting** screens contain the following screen:

- [Captive Portal Debug Log](#) on page 72

Captive Portal Debug Log

Figure 49: Operations > Troubleshoot > Captive Portal Debug Screen

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

To create a captive portal debug log:

- 1 Select **Operations > Troubleshoot > Captive Portal Debug** from the navigation menu.
- 2 Configure the following debug log options:

RF Domain	Specify a RF Domain to include logging information about. Select Include all devices to include devices in the generated debug log. If Include all devices is not selected, specify an individual device name in the field.
Select Debug Messages	Specify what level of debug messages to include. Available options are: <ul style="list-style-type: none"> • All Debug Messages • Authentication Debug Messages • Captive-portal client debug messages
Wireless Clients	Select which wireless clients to include in the log. Available options are: <ul style="list-style-type: none"> • All Wireless Clients • Selected Wireless Clients (up to 3)
Filter Criteria	Configure the following filter criteria:

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

Maximum Events Per Wireless Client Specify the maximum number of events to log for each wireless client. Once this threshold is reached, older log entries for that client will be removed.

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

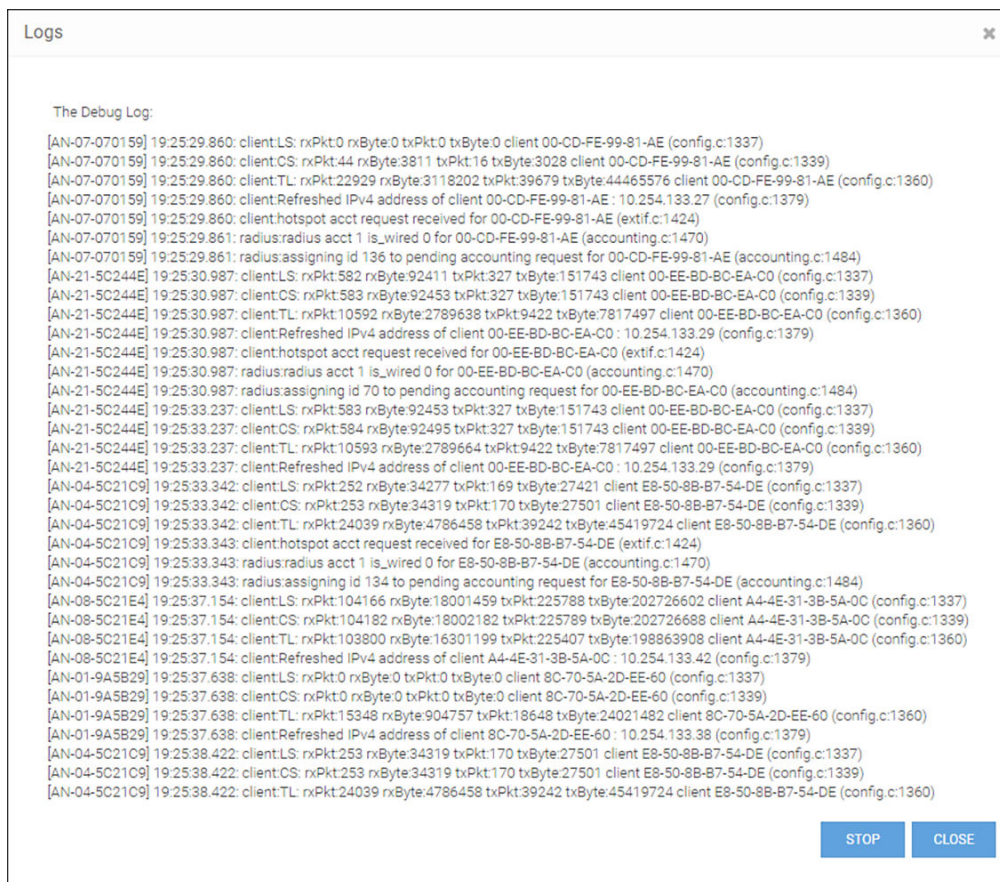


Figure 50: Captive Portal Debug Log Output

7 REST API

About the ExtremeGuest REST API
Accessing the ExtremeGuest REST API
Guest Users Examples
Guest Devices Examples

About the ExtremeGuest REST API

The ExtremeGuest API provides a programmatic interface to access guest user and device information and issue additional configuration parameters. It is based on RESTful principles and uses standard HTTP methods for requests and responses. API request and response bodies are formatted in JavaScript Object Notation (JSON). To submit API calls, your RESTful API consuming program needs to have logged in using credentials granting at least read permissions. Any administrator account can be used with the REST API, but only fully privileged accounts can be used to make configuration changes through the REST API.

There are two parts to the REST API documentation:

- The examples in this chapter are a representative sample of what is available. For a complete list of endpoints, parameters, requests, and responses, see the [ExtremeGuest API Reference](#).



Note

You can access the REST API Development Center via the ExtremeGuest graphical user interface. Go to **Operations > REST API** in the GUI to test out API calls.

- This guide, which provides information about accessing the API, structure of the API request and response bodies, error codes, and examples.



Note

You cannot run the sample requests in this guide as-is. Replace call-specific parameters such as tokens and IDs with your own values.

More Information

- [API Request](#) on page 74
- [API Response](#) on page 75
- [Accessing the ExtremeGuest REST API](#) on page 76

API Request

To construct a REST API request, combine the following components:

Component	Description
The HTTP method	<ul style="list-style-type: none"> • GET: Return data from the server • DELETE: Delete a resource from the server • POST: Create a new resource on the server • PUT: Update a resource on the server
The base URL of the API	<code>https://EGuest_host_name_or_IP_address/eguest-api</code>
The URI to the resource	The resource to create, update, query, or delete. For example, <code>/v1/guestdevices</code> .
Path parameters	These variables are part of the full URL path and are used to point to a specific resource within a collection. For example, <code>/v1/guestusers/{guestUserId}</code> , where <code>{guestUserId}</code> is the path parameter and is substituted with an actual value when making the API call.
HTTP request headers	The following HTTP headers are supported: <ul style="list-style-type: none"> • Accept: Required for operations with a response body, syntax is <code>Accept: application/json</code>. • Content-Type: Required for operations with a request body, syntax is <code>Content-Type: application/json</code>. • Authorization: Required to get an access token or make API calls.
JSON request body	Required for most POST and PUT requests.

API Response

ExtremeGuest API calls return standard HTTP success or error status codes. Some API calls also return JSON response bodies that include information about the resource.

Table 3: HTTP Response Status Codes

Code	Description
200 OK	The request was successful
201 Created	The resource was created successfully
204 No Content	Success with no response body
400 Bad Request	The operation failed because the request is syntactically incorrect or violated schema.
401 Unauthorized	The authentication credentials are invalid or the user is not authorized to use the API

Table 3: HTTP Response Status Codes (continued)

Code	Description
404 Not Found	The server did not find the specified resource that matches the request URI
405 Method Not Allowed	The API does not support the requested HTTP method, for example, PATCH.

Accessing the ExtremeGuest REST API

To access the ExtremeGuest REST API server and make API calls, you need to:

- 1 Get an access token.
- 2 Forward the access token as part of the authorization header when you make REST API calls.

You can use any language or library that can submit REST API requests and process JSON. Examples of languages and libraries that have been used to build REST API clients include:

- For Java, the Jersey library provides the reference implementation of JAX-RS, a Java standard for RESTful web services. The implementation includes a client library that can run directly on the JVM.
- For Python, the Requests and JSON libraries facilitate REST API applications.
- For .Net, the core language provides facilities for submitting HTTP requests and .Net libraries include a serializer for JSON.
- For Linux shell, **Wget** and **cURL** can execute REST API calls. Linux shell utilities, like **awk** and **grep**, can parse and process JSON.

You can also explore the REST API interactively using tools like [Postman](#).



Note

The examples in this chapter use the command line utility **cURL**.

More Information

- [Authentication and Authorization](#) on page 76
- [Guest Devices Examples](#) on page 82
- [Guest Users Examples](#) on page 77

Authentication and Authorization

The ExtremeGuest REST API uses the OAuth 2.0 protocol to authorize calls. OAuth is an open standard that is used to provide secure access to protected resources. You pass your login credentials in the Authorization header in a get access token request. In exchange for these credentials, the ExtremeGuest authorization server issues access tokens called *bearer tokens* that you use for authorization when you make REST API requests.

Example: Token Request

```
curl -X POST "https://10.254.168.25/eguest-api/v1/oauth2/token"
-H "Content-Type: application/json"
-d '{
```

```

    "grantType": "password",
    "userId": "exampleid",
    "scope": "myScope",
    "password": "examplepwd"
  },

```

Example: Successful Response

```

{
  "access_token": "OWtsSajgOvHo7TOQV4nrQdMWplbW8TZG",
  "token_type": "Bearer",
  "idle_timeout": 0,
  "twoFactorAuthenticationRequired": false,
  "resetPassword": false,
  "aclTemplate": {},
  "expires_in": 86400
}

```

Note



The `access_token` field in the response contains a bearer token, indicated by the `token_type` of `Bearer`.

Include this bearer token in subsequent API requests in the `Authorization` header with the `Bearer` authentication scheme.

Access tokens have a finite lifetime. The `expires_in` field in the response indicates the lifetime, in seconds, of the access token. For example, an expiry value of 3600 indicates that the access token expires in one hour from the time the response was generated. The API endpoint issues a HTTP 401 Unauthorized status code when it detects an expired token.

More Information

- [Guest Users Examples](#) on page 77
- [Guest Devices Examples](#) on page 82

Guest Users Examples

This section contains examples of tasks to configure and manage guest users with the REST API. To perform REST API operations in the Guest User space, such as creating a new , you must log in to the API using an account that grants Super User Admin privileges.

Note



The examples in this chapter are a representative sample of what is available. For a complete list of endpoints, parameters, requests, and responses, see the [ExtremeGuest API Reference](#). You can use these examples to help familiarize yourself with the REST functionality, or use them as a starting point to create your own REST client applications.

Create a New Guest User Account

- 1 [Log in to the API server and get an access token using your Super User admin credentials](#). After you log in, you must also forward this token in the Authorization header with each API call.
- 2 Create a new user using the POST method:

```
POST https://EGuest_host_name_or_IP_address/eguest-api/v1/guestusers
```

Example: POST Request

```
curl -X POST "https://10.254.168.25/eguest-api/v1/guestusers"
-H "accept: application/json"
-H "Authorization: Bearer OWtsSajgOvHo7TOQV4nrQdMWp1bW8TZG"
-H "Content-Type: application/json"
-d '{
  "firstName": "John",
  "lastName": "Doe",
  "email": "jdoe@extremenetworks.com",
  "mobileNumber": "12345678990",
  "userId": "jdoe",
  "password": "abc",
  "organization": "Extreme Networks",
  "reason": "Executive Administrator",
  "siteName": "rfd1",
  "groupName": "group1",
  "startTime": "2018-03-28T23:36:39.081Z",
  "expiryTime": "2019-03-28T23:36:39.081Z"
}'
```

where:

Request Body Element	Data Type	Required/Optional	Description
firstName	String	Required	First name of the guest user
lastName	String	Required	Last name of the guest user
email	String	Optional	Email address of the guest user. Email addresses cannot be duplicated. At least one field must be provided among userId, email, and mobileNumber. This property cannot be modified after creation.
mobileNumber	String	Optional	Mobile number of the guest user. The string must contain numbers only including country code. The mobile number can not be reused for another guest user. At least one field must be provided among userId, email, and mobileNumber. This property can not be modified after creation.

Request Body Element	Data Type	Required/Optional	Description
userId	String	Optional	User name for the guest user account. It is recommended to use only lower case letters and digits in the user name. White space characters and the characters @, -, ;, . are not permitted in user name. The user name cannot be all digits and cannot be reused for another guest user. At least one field must be provided among userId, email, and mobileNumber. This property can not be modified after creation.
password	String	Required	Password for the guest user account
organization	String	Optional	Name of the guest user's organization
reason	String	Optional	Field to add any additional notes
groupName	String	Required	The user group of the guest device. The group must be already present. You can locate it in the ExtremeGuest GUI at Configuration > AAA > Group
siteName	String	Required	The name of the site. The site must be already present. You can locate it in the ExtremeGuest GUI at Configuration > Sites
startTime	Date	Required	Time when the guest user account will be activated
expiryTime	Date	Required	Time when the guest device will be automatically deleted
Id	String	Optional	A unique identifier generated by ExtremeGuest for each resource

Example: Successful Response

```
{
  "id": "5abc2bdc4ad77b0a8c40c719",
  "firstName": "John",
  "lastName": "Doe",
  "email": "jdoe@extremenetworks.com",
```

```

    "mobileNumber": "12345678990",
    "userId": "jdoe",
    "password": "abc",
    "organization": "Extreme Networks",
    "reason": "Executive Administrator",
    "siteName": "rfdl",
    "groupName": "group1",
    "startTime": "2018-03-28T23:36:39.081Z",
    "expiryTime": "2019-03-28T23:36:39.081Z"
  }

```

Get Account Information for the Specified Guest User

- 1 Log in to the API server and get an access token using your Super User admin credentials. After you log in, you must also forward this token in the Authorization header with each API call.
- 2 Use the GET method to get account information for a specified guest user:

```
GET https://EGuest_host_name_or_IP_address/eguest-api/v1/guestusers/
{guestUserId}
```

Example: GET Request

```
curl -X GET "https://10.254.168.25/eguest-api/v1/guestusers/5abc2bdc4ad77b0a8c40c719"
-H "accept: application/json"
-H "Authorization: Bearer OWtsSajgOvHo7TQQV4nrQdMWp1bW8TZG"
```

where:

{guestUserId} is a valid guest user account Id and is passed as a path parameter.

Example: Successful Response

```

{
  "id": "5abc2bdc4ad77b0a8c40c719",
  "firstName": "John",
  "lastName": "Doe",
  "email": "jdoe@extremenetworks.com",
  "mobileNumber": "12345678990",
  "userId": "jdoe",
  "password": "abc",
  "organization": "Extreme Networks",
  "reason": "Executive Administrator",
  "siteName": "rfdl",
  "groupName": "group1",
  "startTime": "2018-03-28T23:36:39.081Z",
  "expiryTime": "2019-03-28T23:36:39.081Z"
}

```

Update a Guest User Account

- 1 Log in to the API server and get an access token using your Super User admin credentials. After you log in, you must also forward this token in the Authorization header with each API call.
- 2 Update the guest user account using the PUT method:

```
PUT https://EGuest_host_name_or_IP_address/eguest-api/v1/guestusers/
{guestUserId}
```


Example: PUT Request

```
curl -X PUT "https://10.254.168.25/eguest-api/v1/guestusers/5abc2bdc4ad77b0a8c40c719"
-H "accept: application/json"
-H "Authorization: Bearer OWtsSajgOvHo7TOQV4nrQdMWp1bW8TZG"
-H "Content-Type: application/json"
-d '{
  "firstName": "John",
  "lastName": "Doe",
  "email": "jdoe@extremenetworks.com",
  "mobileNumber": "12345678990",
  "userId": "jdoe",
  "password": "abcdef",
  "organization": "Extreme Networks",
  "reason": "Executive Administrator",
  "siteName": "rfd1",
  "groupName": "group1",
  "startTime": "2018-03-28T23:36:39.081Z",
  "expiryTime": "2019-03-28T23:36:39.081Z"
}'
```

where:

{guestUserId} is a valid guest user account Id and is passed as a path parameter.



Note

The PUT request changes the password property for this account.

Example: Successful Response

```
{
  "id": "5abc2bdc4ad77b0a8c40c719",
  "firstName": "John",
  "lastName": "Doe",
  "email": "jdoe@extremenetworks.com",
  "mobileNumber": "12345678990",
  "userId": "jdoe",
  "password": "abcdef",
  "organization": "Extreme Networks",
  "reason": "Executive Administrator",
  "siteName": "rfd1",
  "groupName": "group1",
  "startTime": "2018-03-28T23:36:39.081Z",
  "expiryTime": "2019-03-28T23:36:39.081Z"
}
```

Delete a Guest User Account

- 1 [Log in to the API server and get an access token using your Super User admin credentials](#). After you log in, you must also forward this token in the Authorization header with each API call.
- 2 Use the DELETE method to delete the specified guest user account:

```
DELETE https://EGuest_host_name_or_IP_address/eguest-api/v1/guestusers/
{guestUserId}
```

Example: DELETE Request

```
curl -X DELETE "https://10.254.168.25/eguest-api/v1/guestusers/5abc2bdc4ad77b0a8c40c719"
-H "accept: application/json"
-H "Authorization: Bearer OWtsSajgOvHo7TOQV4nrQdMWp1bW8TZG"
```

where:

{guestUserId} is a valid guest user account Id and is passed as a path parameter.

Example: Successful Response

```
{
  "success": true
}
```

Guest Devices Examples

This section contains examples of tasks to configure and manage guest devices with the REST API.

Note



The examples in this chapter are a representative sample of what is available. For a complete list of endpoints, parameters, requests, and responses, see the [ExtremeGuest API Reference](#). You can use these examples to help familiarize yourself with the REST functionality, or use them as a starting point to create your own REST client applications.

Create a New Guest Device

- 1 [Log in to the API server and get an access token using your Super User admin credentials](#). After you log in, you must also forward this token in the Authorization header with each API call.
- 2 Create the new device using the POST method.

POST https://EGuest_host_name_or_IP_address/eguest-api/v1/guestdevices

Example: POST Request

```
curl -X POST "https://10.254.168.25/eguest-api/v1/guestdevices"
-H "accept: application/json"
-H "Authorization: Bearer OWtsSajgOvHo7TOQV4nrQdMWp1bW8TZG"
-H "Content-Type:application/json"
-d '{
  "macAddress": "8C-DC-D4-34-0B-68",
  "siteName": "rfd1",
  "networkName": "wlan1",
  "groupName": "group1",
  "vendorName": "Apple",
  "deviceType": "Apple iPad",
  "deviceOs": "Apple iOS",
  "deviceBrowser": "Safari",
  "expiryTime": "2019-03-29T00:50:00.454Z"
}'
```

where:

Request Body Element	Data Type	Required/Optional	Description
macAddress	String	Required	The MAC address of the guest device in "AA-BB-CC-DD-EE-FF" format. This property can not be modified after creation.
groupName	String	Required	The user group of the guest device. The group must be already present. You can locate it in the ExtremeGuest GUI at Configuration > AAA > Group
networkName	String	Required	The name of the network that serves this guest device. The network must be already present. You can locate it in the ExtremeGuest GUI at Configuration > Networks
siteName	String	Required	The name of the site. The site must be already present. You can locate it in the ExtremeGuest GUI at Configuration > Sites
vendorName	String	Required	Name of the vendor to classify the guest device
deviceType	String	Required	Type of the guest device
deviceOs	String	Required	Name of the operating system in the guest device
deviceBrowser	String	Required	Name of the web browser in the guest device
expiryTime	Date	Required	Time when the guest device will be automatically deleted
id	String	Optional	A unique identifier generated by ExtremeGuest for each resource

Example: Successful Response

```
{
  "id": "5abc3a584ad77b0a8c40c71b",
  "macAddress": "8C-DC-D4-34-0B-68",
  "siteName": "rfd1",
  "networkName": "wlan1",
  "groupName": "group1",
  "deviceType": "Apple iPad",
  "deviceOs": "Apple iOS",
  "deviceBrowser": "Safari",
  "vendorName": "Apple",
```

```
    "expiryTime": "2019-03-29T00:50:00.454Z"
  }
}
```

Get Information for a Specified Guest Device

- 1 Log in to the API server and get an access token using your Super User admin credentials. After you log in, you must also forward this token in the Authorization header with each API call.
- 2 Use the GET method to get account information for a specified guest user:

```
GET https://EGuest_host_name_or_IP_address/eguest-api/v1/guestdevices/
{guestDeviceId}
```

Example: GET Request

```
curl -X GET "https://10.254.168.25/eguest-api/v1/guestdevices/5abc3a584ad77b0a8c40c71b"
-H "accept: application/json"
-H "Authorization: Bearer OWtsSajgOvHo7TQqV4nrQdMWplbW8TZG"
```

where:

{guestDeviceId} is a valid Id of the specified guest device and is passed as a path parameter.

Example: Successful Response

```
{
  "id": "5abc3a584ad77b0a8c40c71b",
  "macAddress": "8C-DC-D4-34-0B-68",
  "siteName": "rfdl",
  "networkName": "wlan1",
  "groupName": "group1",
  "deviceType": "Apple iPad",
  "deviceOs": "Apple iOS",
  "deviceBrowser": "Safari",
  "vendorName": "Apple",
  "expiryTime": "2019-03-29T00:50:00.454Z"
}
```

Update a Guest Device

- 1 Log in to the API server and get an access token using your Super User admin credentials. After you log in, you must also forward this token in the Authorization header with each API call.
- 2 Update the guest device information using the PUT method:

```
PUT https://EGuest_host_name_or_IP_address/eguest-api/v1/guestdevices/
{guestDeviceId}
```

Example: PUT Request

```
curl -X PUT "https://10.254.168.25/eguest-api/v1/guestdevices/5abc3a584ad77b0a8c40c71b"
-H "accept: application/json"
-H "Authorization: Bearer OWtsSajgOvHo7TQqV4nrQdMWplbW8TZG"
-H "Content-Type: application/json"
-d '{
  "macAddress": "8C-DC-D4-34-0B-68",
  "siteName": "rfdl",
  "networkName": "wlan1",
  "groupName": "group1",
}
```

```

    "vendorName": "Amazon",
    "deviceType": "Apple iPad",
    "deviceOs": "Apple iOS",
    "deviceBrowser": "Safari",
    "expiryTime": "2019-03-29T00:50:00.454Z"
  },

```

where:

{guestDeviceId} is a valid Id of the specified guest device and is passed as a path parameter.



Note

The PUT request changes the vendorName property for this device.

Example: Successful Response

```

{
  "id": "5abc3a584ad77b0a8c40c71b",
  "macAddress": "8C-DC-D4-34-0B-68",
  "siteName": "rfd1",
  "networkName": "wlan1",
  "groupName": "group1",
  "deviceType": "Apple iPad",
  "deviceOs": "Apple iOS",
  "deviceBrowser": "Safari",
  "vendorName": "Amazon",
  "expiryTime": "2019-03-29T00:50:00.454Z"
}

```

Delete a Guest Device

- 1 [Log in to the API server and get an access token using your Super User admin credentials](#). After you log in, you must also forward this token in the Authorization header with each API call.
- 2 Use the DELETE method to delete a specified guest device:

```
DELETE https://EGuest_host_name_or_IP_address/eguest-api/v1/guestdevices/{guestDeviceId}
```

Example: DELETE Request

```
curl -X DELETE "https://10.254.168.25/eguest-api/v1/guestdevices/5abc3a584ad77b0a8c40c71b"
-H "accept: application/json"
-H "Authorization: Bearer OWtsSajgOvHo7TOQV4nrQdMWp1bW8TZG"
```

where:

{guestDeviceId} is a valid Id of the specified guest device and is passed as a path parameter.

Example: Successful Response

```

{
  "success": true
}

```