



ExtremeGuest User Guide

Copyright © 2017 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 Publications.....	5
Chapter 1: Introduction to ExtremeGuest.....	6
Supported Platforms.....	6
UI Overview.....	6
Chapter 2: Monitor.....	13
Summary.....	13
Map View.....	15
Active Users.....	17
Chapter 3: Dashboard.....	20
Dashboard Basics.....	21
Creating a New Dashboard.....	21
Available Dashboard Widgets.....	24
Chapter 4: Configuration.....	26
AAA Configuration.....	26
Splash Templates.....	33
Notification.....	33
Social.....	38
Chapter 5: Analyze.....	41
Reports.....	41
Analyze Users.....	47
Analyze End Points.....	49
Chapter 6: Operations.....	51
Database Operations.....	51
Troubleshooting.....	54



Preface

Text Conventions

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

Table 1: Notice Icons






Icon	Notice Type	Alerts you to...
	General Notice	Helpful tips and notices for using the product.
	Note	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.
	New	This command or section is new for this release.

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 internalinfodev@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.
- **GTAC Knowledge** — Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- **The Hub** — A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- **Support Portal** — Manage cases, downloads, service contracts, product licensing, and training and certifications.

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 Publications

General

Product documentation is available at: <http://documentation.extremenetworks.com>. Release notes are available at: 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

Supported Platforms UI Overview

ExtremeGuest is available on supported WiNG platforms and provides centralized guest management including multiple guest onboarding methods and guest analytics. Licenses for ExtremeGuest are acquired the same method as WiNG AP licenses.

Supported Platforms

The ExtremeGuest service is supported on standalone and replica-set configurations. It also can be hosted on a 2 WiNG VX controllers with an arbiter.

The following are supported ExtremeGuest hosting configurations:

- 3 x VX 9000
- 2 x VX 9000 with 1 x NX 5500 or NX 7500 as an arbiter

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
- Dashboard
- Configuration
- Analyze
- Operations

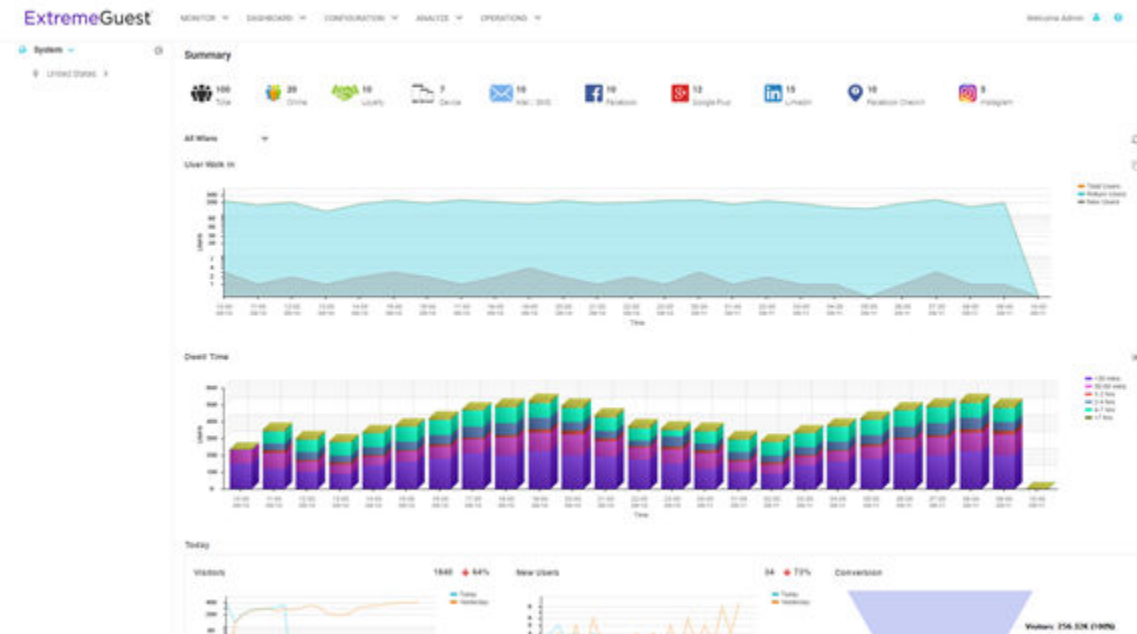


Figure 1: User Interface in Standard View

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.

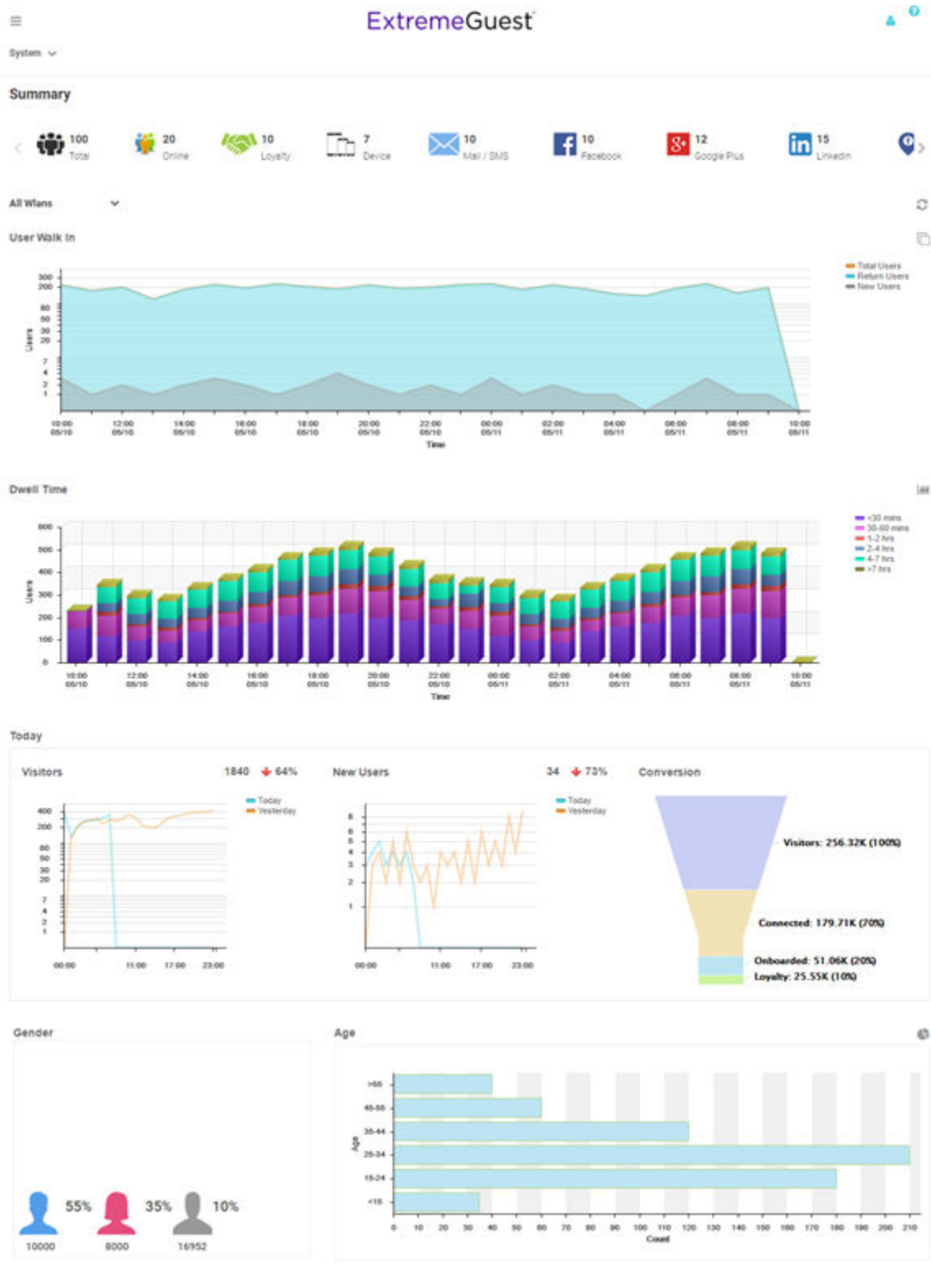


Figure 2: User Interface in Tablet View

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
- Dashboard
- Configuration
- Analyze
- Operations

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 under the 'NEW USER' navigation option. The form 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**.

The screenshot shows the 'Bulk Voucher' configuration screen in the ExtremeGuest web interface. The page header includes the 'ExtremeGuest' logo, navigation tabs for 'NEW USER' and 'BULK VOUCHER', and a user greeting 'Welcome Webserver1'. The main form area is titled 'Bulk Voucher' and contains the following fields:

- User Group*:** A dropdown menu with 'split-group' selected.
- Number of Vouchers*:** A numeric input field with '10' and a range indicator '(2..20000)'.
- Description:** A text input field containing 'Description'.
- Location*:** A dropdown menu with 'Location' selected.
- Start Date/Time*:** A date and time picker showing '05/26/2017' and '12:12 PM'.
- Expiry Date/Time*:** A date and time picker showing '06/25/2017' and '11:59 PM'.

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

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 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/Time picker]

At the bottom of the form 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.
WLAN	Use the pull-down menu to select a wireless LAN 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.

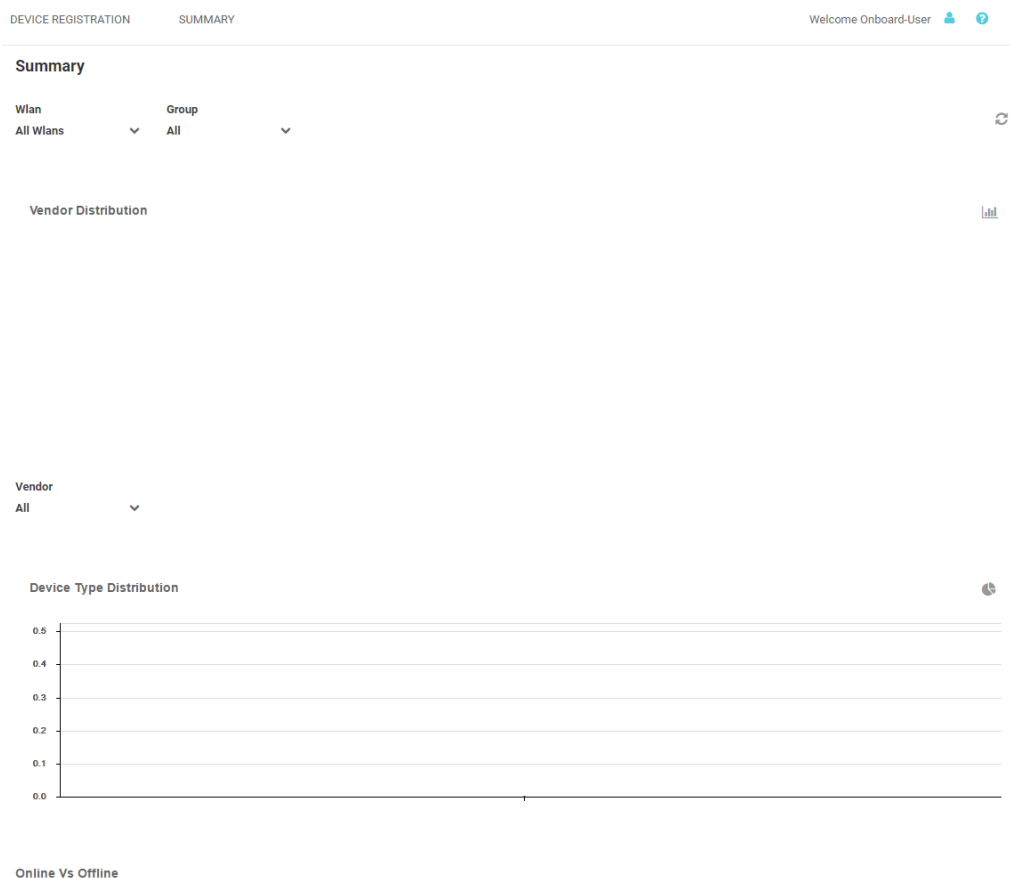


Figure 6: Onboard User Interface - Summary Screen

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

Summary
Map View
Active Users

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

- Summary
- Map View
- Active Users

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

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 15

Summary Screen

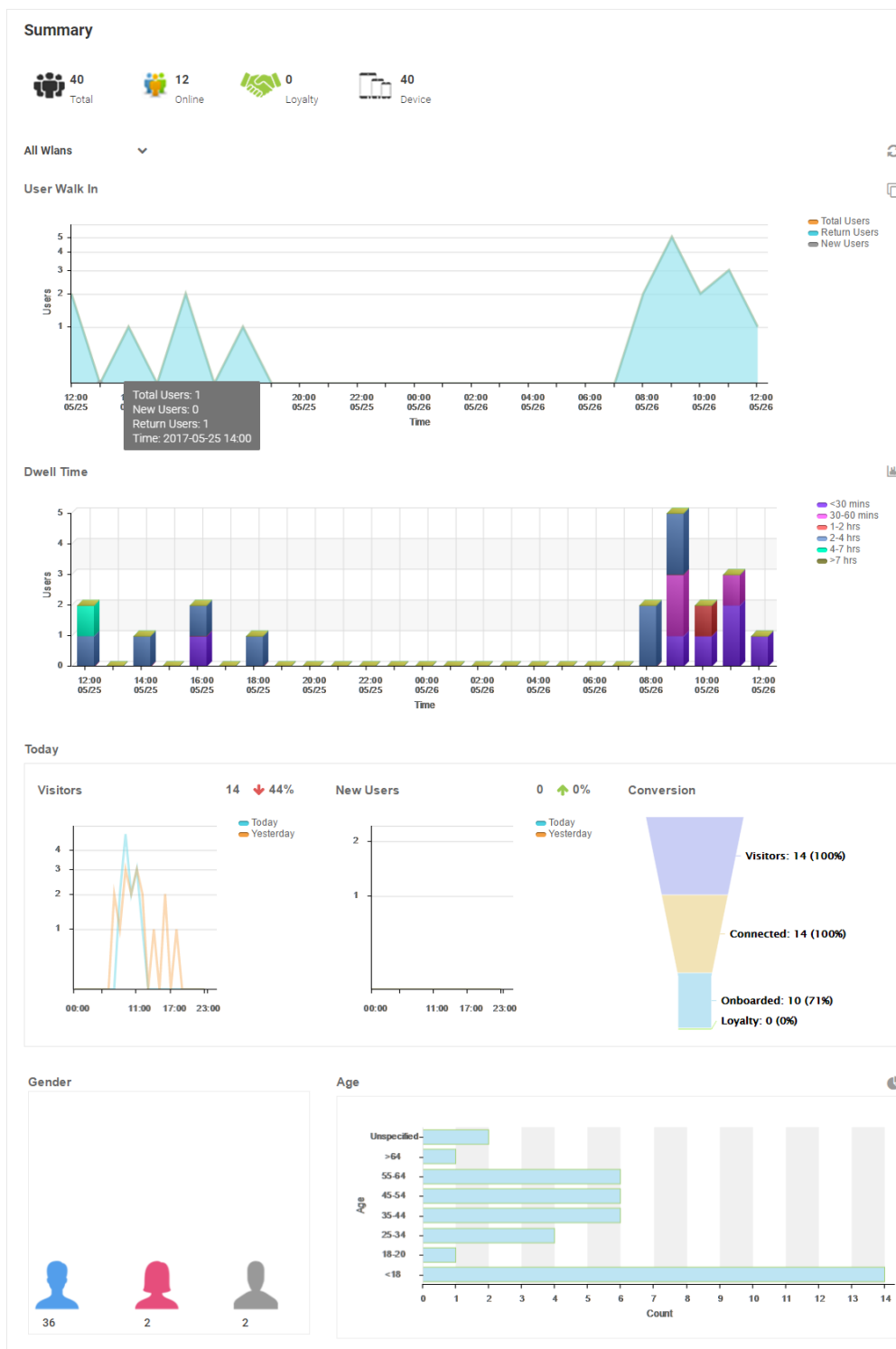


Figure 7: Monitor > Summary Screen

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

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.

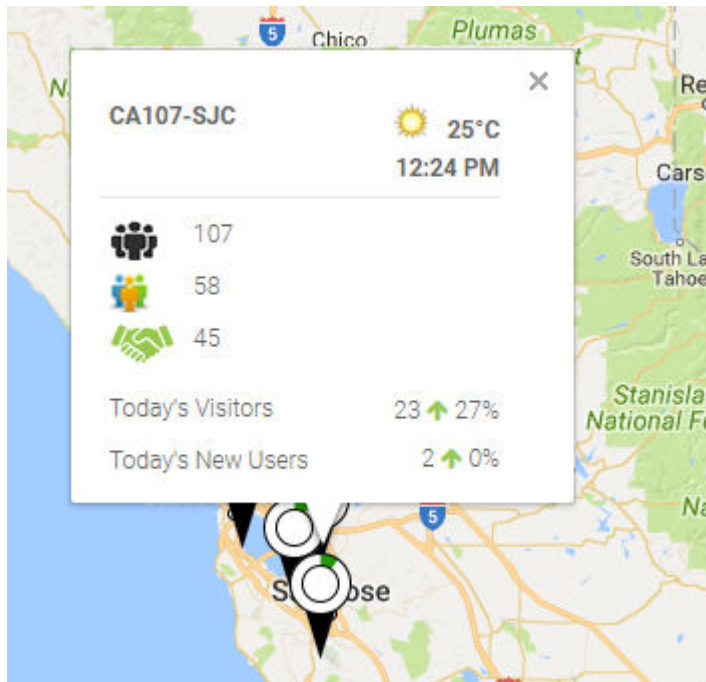


Figure 8: Monitor > Map View Mouse Over

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

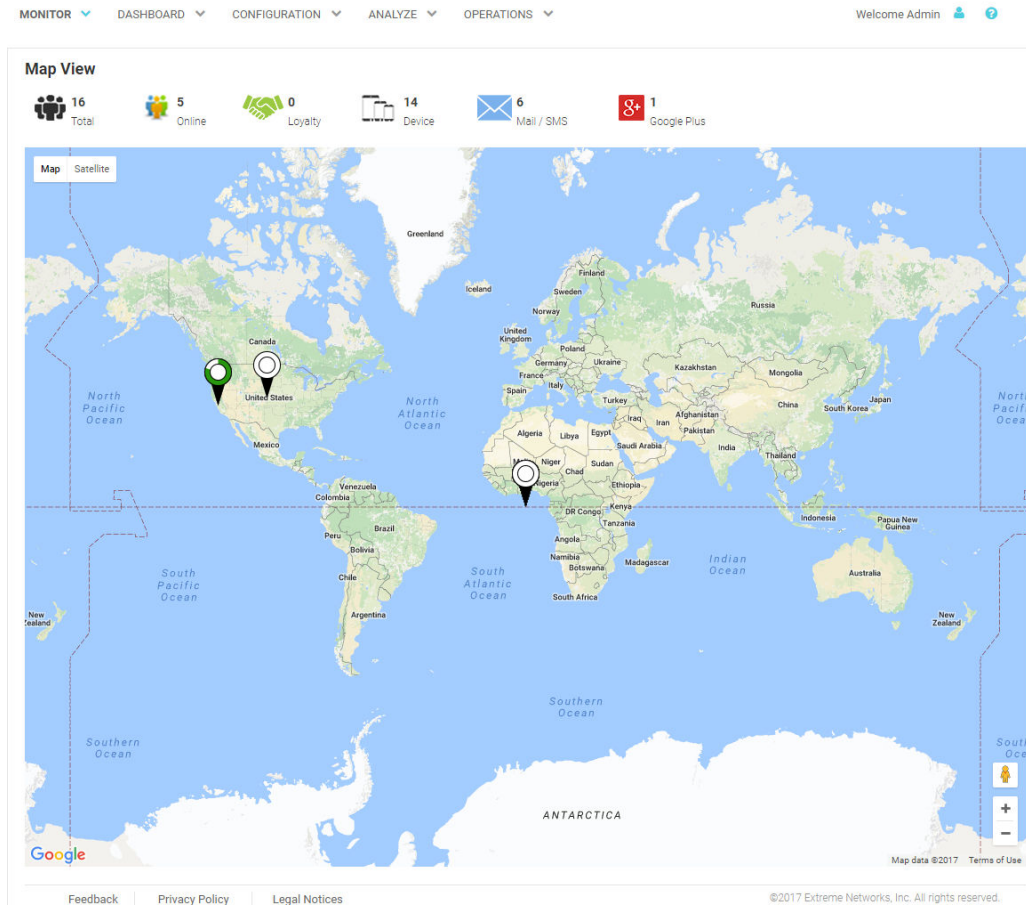




Figure 9: Monitor > Map ViewScreen

Active Users







Monitor > Active Users

The **Active 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 users. [Active User Details](#) on page 18

Active Users Screen

MONITOR ▾ DASHBOARD ▾ CONFIGURATION ▾ ANALYZE ▾ OPERATIONS ▾ Welcome Admin  

Active Users

 **16** Total
  **5** Online
  **0** Loyalty
  **14** Device
  **6** Mail / SMS
  **1** Google Plus

Active Users Details

Location	Online Users	Offline Users	Total Users
default	0	1	1
domain-www	0	0	0
server-domain	0	0	0
rfd-third	0	0	0
6K-site	4	6	10
domain-noc	0	0	0
SITE4	0	2	2
SITE2	0	0	0
SITE3	1	1	2
SITE1	0	1	1
Test-Def	0	0	0
rfd-four	0	0	0
rfd1	0	0	0

[Feedback](#) | [Privacy Policy](#) | [Legal Notices](#)
©2017 Extreme Networks, Inc. All rights reserved.

Active 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.

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.
- WLAN** The **WLAN** 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.

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:

- Create New
- *User Created Dashboards*

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 21

[Available Dashboard Widgets](#) on page 24

Dashboard Basics

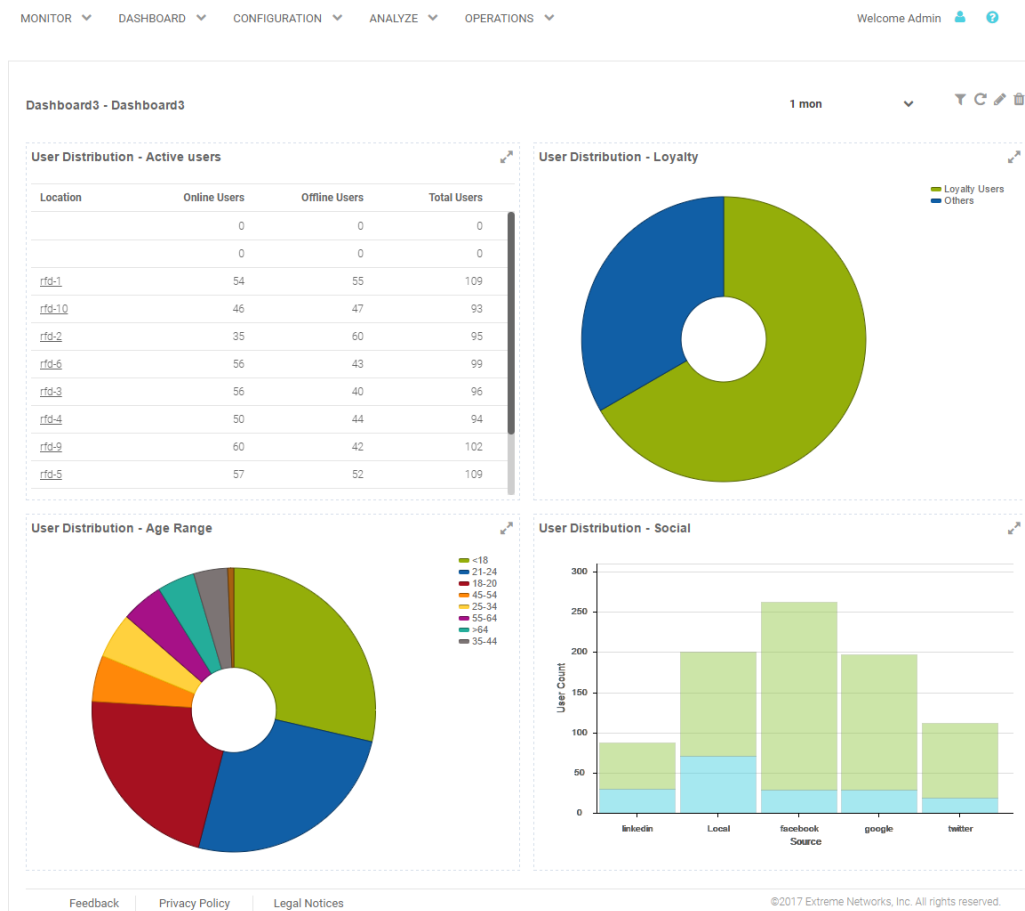


Figure 10: Example Dashboard Screen

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 24. 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 **WLAN** or by **Time**. To change the **WLAN** 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**, or **3 months**. Changes to the **WLAN** 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.

To create a new dashboard:

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

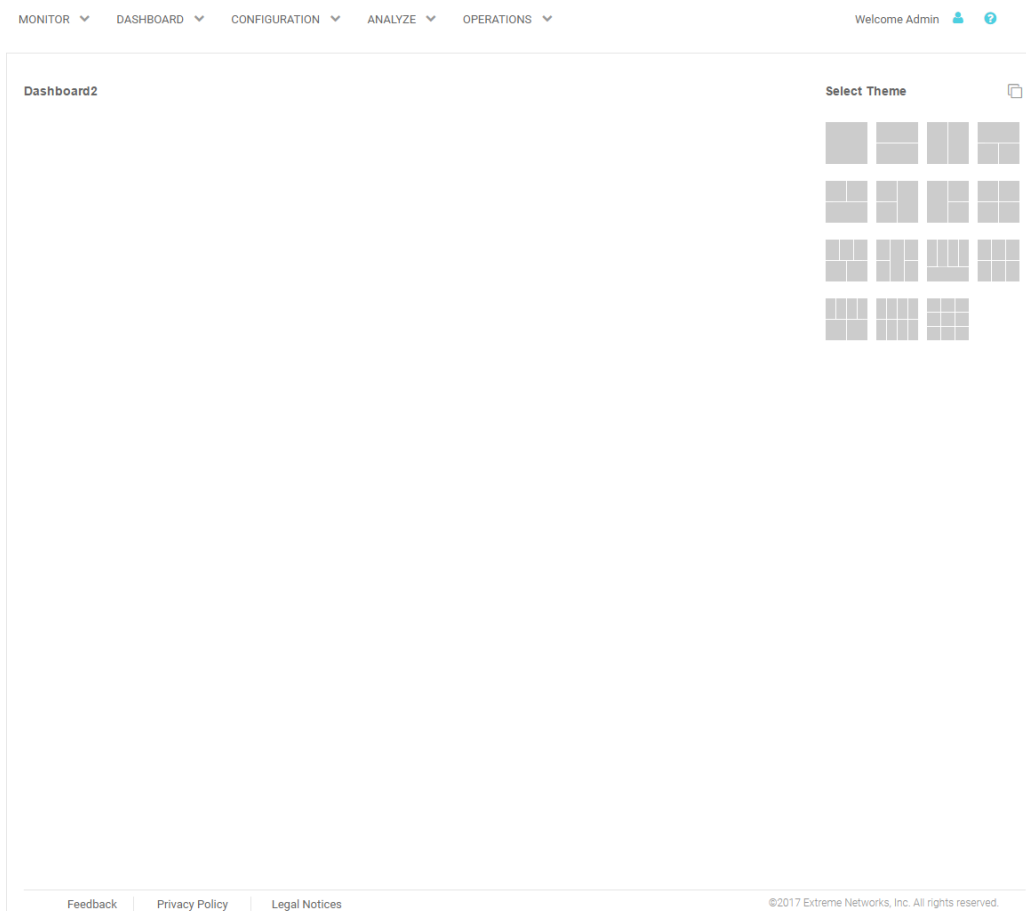


Figure 11: Blank New Dashboard Screen

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.

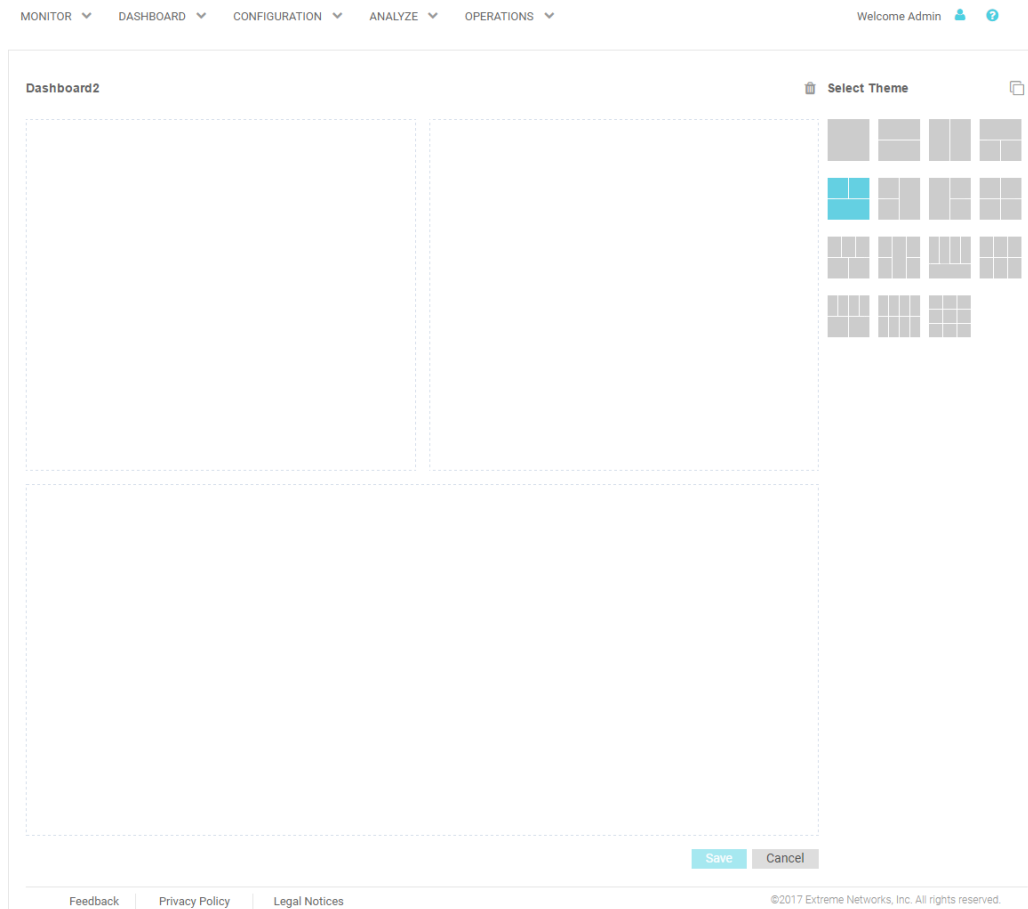


Figure 12: Selecting a Dashboard Theme

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.

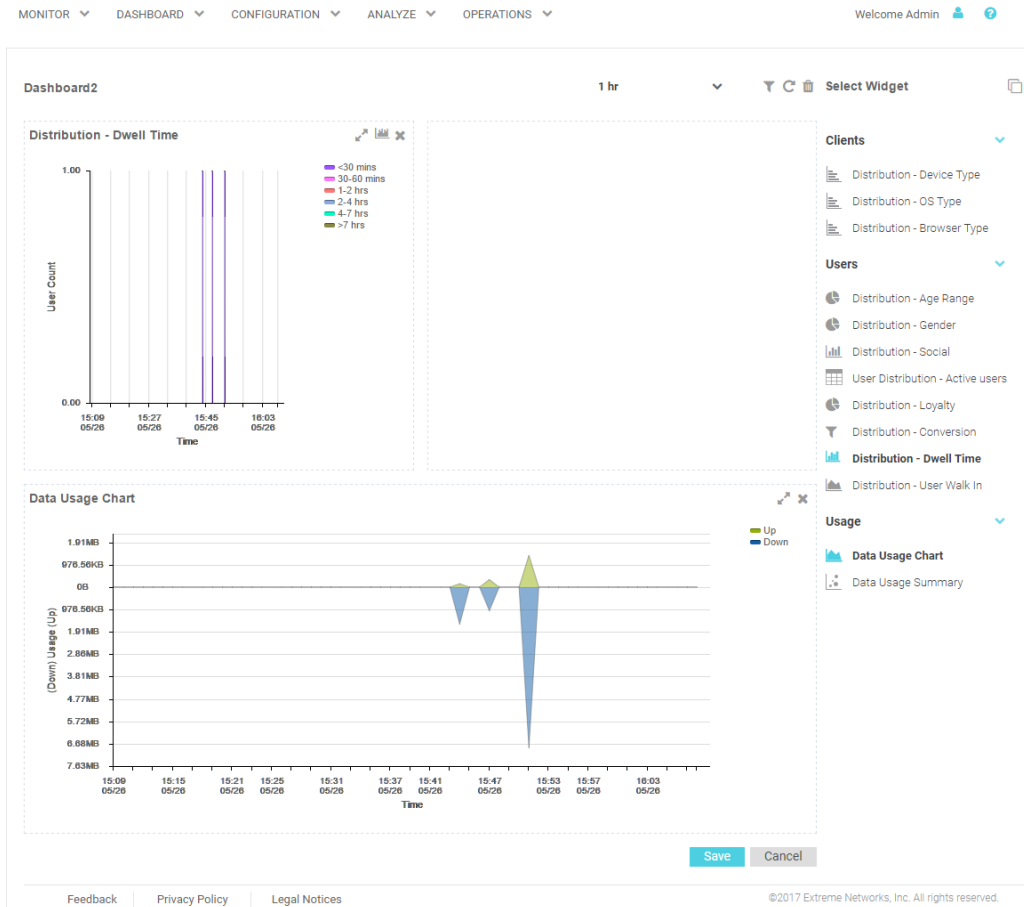


Figure 13: Selecting and Placing Widgets

Available [Dashboard Widgets](#) on page 24

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
Client Distribution	Device Type	Bar graph displaying client count sorted by mobile device model.

Category	Widget	Description
Client Distribution	OS Type	Bar graph displaying client count sorted by the operating system used on the user's mobile device.
Client Distribution	Browser Type	Bar graph displaying client count sorted by the web browser used to authenticate on the user's mobile device.
User 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
User Distribution	Gender	Pie chart displaying user distribution by gender.
User 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.
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.
User Distribution	Loyalty	Graph displaying number of users with the customer app installed on their device.
User Distribution	Conversion	Graph displaying the number and percentage of users who converted from Connected to Onboarded to Loyalty customers.
User 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
User 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 <p>Data is further separated between Total Users, Return Users, and New Users.</p>
Usage	Usage Chart	Graph displaying upstream and downstream bandwidth usage over time.
Usage	Usage Summary	Graph displaying upstream, downstream, and total bandwidth usage.

4 Configuration

AAA Configuration
Splash Templates
Notification
Social

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

- AAA Configuration
- Splash Templates
- Notifications
- Social

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 27

[AAA Group](#) on page 29

[AAA Networks](#) on page 30

AAA Authorization

MONITOR ▾ DASHBOARD ▾ CONFIGURATION ▾ ANALYZE ▾ OPERATIONS ▾ Welcome Admin

AAA

Authorization Group Networks

<input type="checkbox"/>	Name	Description	Action
<input type="checkbox"/>	Network-remote	authorization	
<input type="checkbox"/>	Network-Branch	authorization	

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

[Feedback](#) [Privacy Policy](#) [Legal Notices](#) ©2017 Extreme Networks, Inc. All rights reserved.

Figure 14: 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 15: 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 WLAN 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, 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

AAA

Authorization Group Networks

↻ + 🗑️

<input type="checkbox"/>	Name	Description	Action
<input type="checkbox"/>	Alphanet-Guest	Alphanet-Guest	🗑️

⏪ < Page 1 of 1 > ⏩

Displaying 1 - 1 of 1

Figure 16: 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

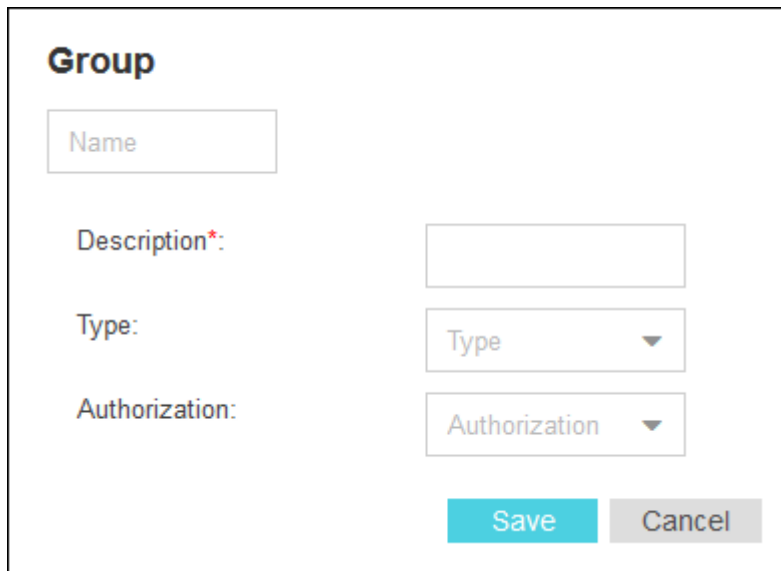


Figure 17: AAA Groups Add Screen

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 Networks


Configuration > AAA > Networks

MONITOR ▾ DASHBOARD ▾ CONFIGURATION ▾ ANALYZE ▾ OPERATIONS ▾ Welcome Admin  

AAA

Authorization Group Networks

<input type="checkbox"/>	Name	Description	IP Address/mask	Action
<input type="checkbox"/>	Branch	test post	10.10.10.10/24	

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

[Feedback](#) | [Privacy Policy](#) | [Legal Notices](#) ©2017 Extreme Networks, Inc. All rights reserved.

Figure 18: AAA Networks Screen

The AAA Networks 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 Networks

The screenshot shows the 'Networks' configuration page. At the top, there is a navigation menu with 'MONITOR', 'DASHBOARD', 'CONFIGURATION', 'ANALYZE', and 'OPERATIONS'. The 'CONFIGURATION' menu is expanded. In the top right corner, it says 'Welcome Admin' with a user icon and a help icon. The main content area is titled 'Networks' and contains a form with the following fields:

- Name:** A text input field.
- Description*:** A text input field.
- IP Address/mask*:** A text input field.
- Shared Secret*:** A text input field with a checkbox labeled 'Show Shared Secret' to its right.

At the bottom right of the form, there are two buttons: 'Save' (in blue) and 'Cancel' (in grey). At the bottom of the page, there are links for 'Feedback', 'Privacy Policy', and 'Legal Notices', and a copyright notice: '©2017 Extreme Networks, Inc. All rights reserved.'

Figure 19: AAA Networks Add Screen

To add AAA Networks:

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

The **Authorization** screen displays by default.

- 2 Select the **Networks** 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.

Splash Templates

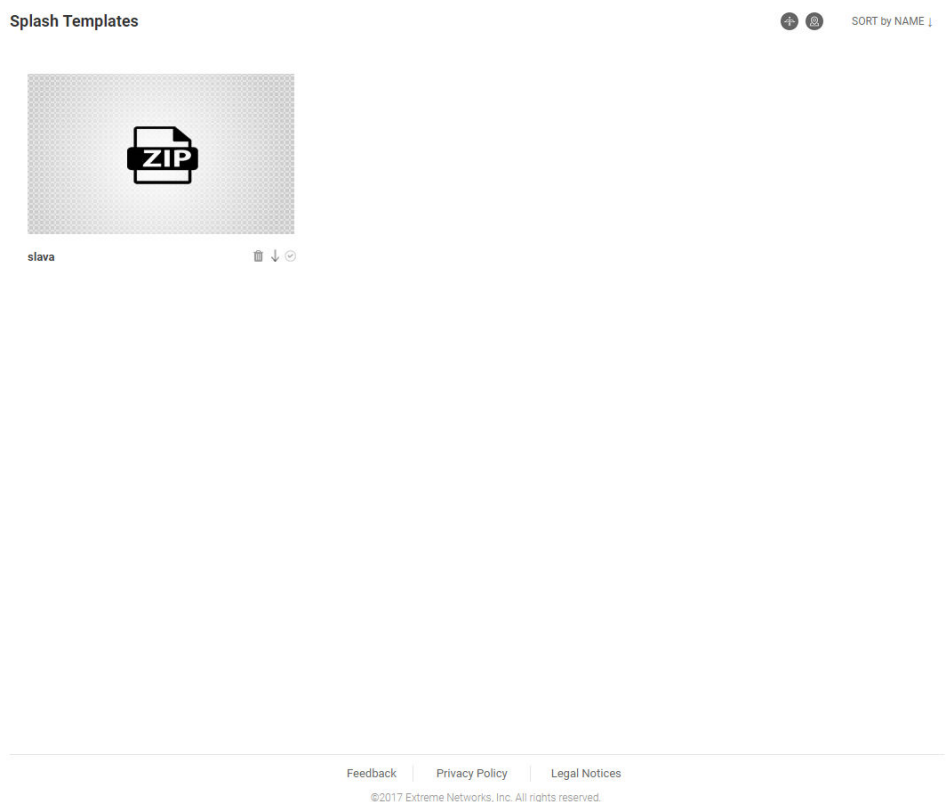


Figure 20: Splash Templates Screen

The **Splash Templates** screen displays a summary of available captive portal splash screen templates. Existing templates may be deleted, downloaded, or applied to a WLAN. New templates may be added by selecting the **Upload New Template** button. Select **Summary View** to view a summary of templates in use by location and those that are hosted by ExtremeGuest.

Notification

Configuration > Notification

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

[Policy](#) on page 34

[Rules](#) on page 37

Policy

MONITOR ▾ DASHBOARD ▾ CONFIGURATION ▾ ANALYZE ▾ OPERATIONS ▾ Welcome Admin

Policy

<input type="checkbox"/>	Name	Description	Action
<input type="checkbox"/>	test1	testing policy	
<input type="checkbox"/>	test3	testing policy	

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

[Feedback](#) | [Privacy Policy](#) | [Legal Notices](#) ©2017 Extreme Networks, Inc. All rights reserved.

Figure 21: 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.

Figure 22: Add 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:

- 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.

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	Wlan	Precedence	Action
<input type="checkbox"/>	NewRule	test1	rfd-9	test	10	
<input type="checkbox"/>	Rule	test3	System	test	10	

Figure 23: 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.
- 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.

The screenshot shows a 'Create Rule' dialog box with the following fields and controls:

- Rule Name***: A text input field containing 'Rule Name'.
- Policy***: A dropdown menu showing 'Policy'.
- Wlan**: A dropdown menu showing 'All Wlans'.
- Location**: A dropdown menu showing 'System'.
- Precedence Level**: A spinner control showing 'Precedence Level'.
- Buttons: 'Apply' (highlighted in blue) and 'Cancel' (greyed out).

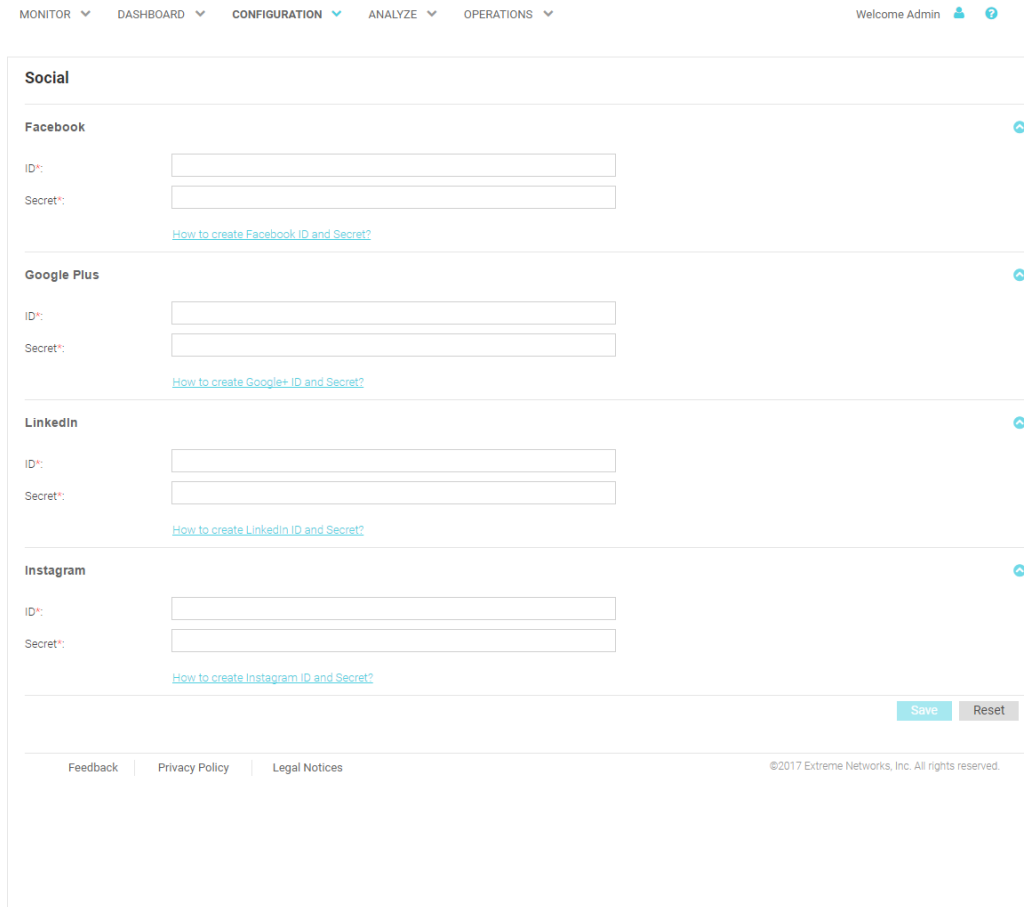
Figure 24: Create Rules



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. |
| WLAN | Use the pull-down menu to select the WLANs that the notification rule applies to. To apply the rule to all WLANs select All WLANS . |
| 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



MONITOR ▾ DASHBOARD ▾ CONFIGURATION ▾ ANALYZE ▾ OPERATIONS ▾ Welcome Admin  


Social

Facebook 

ID*:

Secret*:


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

Google Plus 

ID*:

Secret*:


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

LinkedIn 

ID*:

Secret*:

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

Instagram 

ID*:

Secret*:

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

[Feedback](#) | [Privacy Policy](#) | [Legal Notices](#) ©2017 Extreme Networks, Inc. All rights reserved.

Figure 25: 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**.

5 Analyze

Reports

Analyze Users

Analyze End Points

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

- Reports
- Users
- End Points

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



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: <ul style="list-style-type: none">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: <ul style="list-style-type: none">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

MONITOR ▾ DASHBOARD ▾ CONFIGURATION ▾ **ANALYZE** ▾ OPERATIONS ▾ Welcome Admin  

Generated Reports  

<input type="checkbox"/> Report	Type	User	Generated At	Action
Device Distribution	NA	admin	2/7/2011, 2:00:04 PM	 
User Demographics	NA	admin	2/7/2011, 2:00:04 PM	 

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



[Feedback](#) | [Privacy Policy](#) | [Legal Notices](#)
©2017 Extreme Networks, Inc. All rights reserved.

Figure 26: 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 Trashcan icon to delete a generated report.

Manage Reports

MONITOR ▾ DASHBOARD ▾ CONFIGURATION ▾ **ANALYZE ▾** OPERATIONS ▾ Welcome Admin  

Manage Reports + ↻ 🗑

<input type="checkbox"/>	Report	Type	User	Start Date	End Date	Frequency	Action
<input type="checkbox"/>	Test 1	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Daily	
<input type="checkbox"/>	Test 2	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Weekly	
<input type="checkbox"/>	Test 4	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Monthly	
<input type="checkbox"/>	Test 5	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Daily	
<input type="checkbox"/>	Test 6	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Weekly	
<input type="checkbox"/>	Test 7	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Monthly	
<input type="checkbox"/>	Test 8	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Daily	
<input type="checkbox"/>	Test 9	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Daily	
<input type="checkbox"/>	Test 10	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Daily	
<input type="checkbox"/>	Test 11	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Monthly	
<input type="checkbox"/>	Test 12	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Daily	
<input type="checkbox"/>	Test 13	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Monthly	
<input type="checkbox"/>	Test 14	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Weekly	
<input type="checkbox"/>	Test 15	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Weekly	
<input type="checkbox"/>	Test 16	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Daily	
<input type="checkbox"/>	Test 16	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Monthly	

« < Page 1 of 1 > » Displaying 1 - 16 of 16

[Feedback](#) | [Privacy Policy](#) | [Legal Notices](#) ©2017 Extreme Networks, Inc. All rights reserved.

Figure 27: 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.

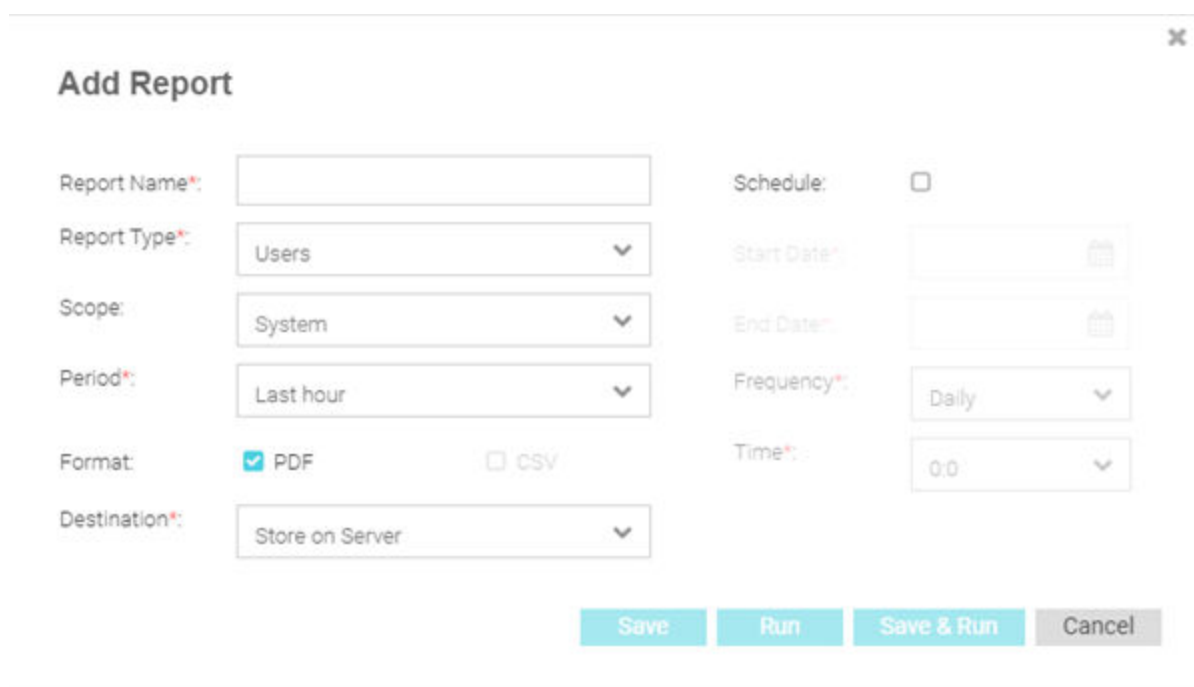


Figure 28: Add Reports Screen

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

MONITOR ▾ DASHBOARD ▾ CONFIGURATION ▾ **ANALYZE** ▾ OPERATIONS ▾ Welcome Admin  

Scheduled Reports

<input type="checkbox"/>	Report	Type	User	Start Date	End Date	Frequency	Action
<input type="checkbox"/>	Test 1	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Daily	
<input type="checkbox"/>	Test 2	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Weekly	
<input type="checkbox"/>	Test 4	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Monthly	
<input type="checkbox"/>	Test 5	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Daily	
<input type="checkbox"/>	Test 6	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Weekly	
<input type="checkbox"/>	Test 7	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Monthly	
<input type="checkbox"/>	Test 8	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Daily	
<input type="checkbox"/>	Test 9	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Daily	
<input type="checkbox"/>	Test 10	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Daily	
<input type="checkbox"/>	Test 11	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Monthly	
<input type="checkbox"/>	Test 12	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Daily	
<input type="checkbox"/>	Test 13	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Monthly	
<input type="checkbox"/>	Test 14	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Weekly	
<input type="checkbox"/>	Test 15	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Weekly	
<input type="checkbox"/>	Test 16	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Daily	
<input type="checkbox"/>	Test 16	NA	admin	Tue Feb 16 2016 00:00:...	Sat Feb 20 2016 00:00:0...	Monthly	

« < Page 1 of 1 > » Displaying 1 - 16 of 16



[Feedback](#) | [Privacy Policy](#) | [Legal Notices](#) ©2017 Extreme Networks, Inc. All rights reserved.

Figure 29: 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

MONITOR ▾ DASHBOARD ▾ CONFIGURATION ▾ ANALYZE ▾ OPERATIONS ▾ Welcome Admin  

Users

 100 Total
  20 Online
  10 Loyalty
  7 Device
  10 Mail / SMS
  10 Facebook
  12 Google Plus
  15 LinkedIn

Users Details

<input type="checkbox"/>	User	Name	Email	Gender	Source	Last Login	Action
<input type="checkbox"/>		undefined	ankit.deshmukh15@gm...			4/3/2017, 3:48:44 PM	  
<input type="checkbox"/>		undefined	ait.caiey1990@gmail.co...			4/3/2017, 2:29:22 PM	  
<input type="checkbox"/>		Test-100000-100037	100000100037@abc.co...			2/21/2017, 6:41:38 AM	 
<input type="checkbox"/>		Test-100000-100084	100000100084@abc.co...			2/11/2017, 10:00:36 AM	 
<input type="checkbox"/>		Test-100000-100090	100000100090@abc.co...			2/21/2017, 6:41:38 AM	 
<input type="checkbox"/>		Test-100000-100105	100000100105@abc.co...			2/21/2017, 6:41:38 AM	 
<input type="checkbox"/>		Test-100000-100113	100000100113@abc.co...			2/21/2017, 6:41:38 AM	 
<input type="checkbox"/>		Test-100000-100115	100000100115@abc.co...			2/11/2017, 8:09:36 PM	  
<input type="checkbox"/>		Test-100000-100216	100000100216@abc.co...			2/7/2017, 2:58:36 PM	 
<input type="checkbox"/>		Test-100000-100245	100000100245@abc.co...			2/5/2017, 7:23:36 AM	 
<input type="checkbox"/>		Test-100000-100251	100000100251@abc.co...			2/20/2017, 5:51:36 AM	 

<< < Page 1 of 1 > >> Displaying 1 - 13 of 13

[Feedback](#) [Privacy Policy](#) [Legal Notices](#) ©2017 Extreme Networks, Inc. All rights reserved.

Figure 30: Analyze Users Screen

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

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

[Filtering User Results](#) on page 48

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:

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.

Analyze End Points

MONITOR ▾ DASHBOARD ▾ CONFIGURATION ▾ ANALYZE ▾ OPERATIONS ▾ Welcome Admin

End Points

100 Total
 20 Online
 10 Loyalty
 7 Device
 10 Mail / SMS
 10 Facebook
 12 Google Plus
 15 LinkedIn

End Points Details

<input type="checkbox"/>	MAC	Host Name	Device Type	OS	Status	Last Login	Action
<input type="checkbox"/>	aabbccdde44			Android			
<input type="checkbox"/>	aabbcc33ee44			iOS			
<input type="checkbox"/>	aabb22ddee44			Android			
<input type="checkbox"/>	aabbccddeeff			Android			
<input type="checkbox"/>	aa22cc14ee44			iOS			
<input type="checkbox"/>	aa22ccdde44			iOS			
<input type="checkbox"/>	aabbccdde44			Android			
<input type="checkbox"/>	aabbcc33ee44			iOS			
<input type="checkbox"/>	aabb22ddee44			Android			
<input type="checkbox"/>	aabbccddeeff			Android			
<input type="checkbox"/>	aa22cc14ee44			iOS			
<input type="checkbox"/>	aa22ccdde44			iOS			
<input type="checkbox"/>	aabbccdde44			Android			
<input type="checkbox"/>	aabbcc33ee44			iOS			

<< < Page 1 of 2 > >> Displaying 1 - 30 of 57

[Feedback](#) | [Privacy Policy](#) | [Legal Notices](#) ©2017 Extreme Networks, Inc. All rights reserved.

Figure 31: Analyze End Points Screen

The **Analyze End Points** screen displays 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 50

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:

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.

6 Operations

Database Operations Troubleshooting

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

- Database
- Troubleshoot

The **Operations** screens provide database import and export options and captive portal debugging.

Database Operations

Operations > Database

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

- Export
- Import

[Database Export](#) on page 52

[Database Import](#) on page 53

Database Export

The screenshot shows the 'Export' screen in the Operations menu. The navigation bar at the top includes MONITOR, DASHBOARD, CONFIGURATION, ANALYZE, and OPERATIONS. The user is logged in as 'Welcome Admin'. The main form is titled 'Export' and contains the following fields and options:

- Protocol*:** A dropdown menu with 'Protocol' selected.
- IP Address/ Hostname*:** A text input field with 'XXX.XXX.XXX.XXX' entered.
- Username*:** A text input field with 'Username' entered.
- Password*:** A text input field with 'Password' entered.
- Path:** A text input field with 'Path' entered.
- Filters:** Three checkboxes: Wlan, Time, and Location.
- File Type:** Two radio buttons: JSON and CSV.

At the bottom right of the form are two buttons: 'Export' (highlighted in teal) and 'Reset' (grey). The footer contains links for 'Feedback', 'Privacy Policy', and 'Legal Notices', along with the copyright notice '©2017 Extreme Networks, Inc. All rights reserved.'

Figure 32: 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:

- 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 **WLAN**, **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

The screenshot shows the 'Import' screen within the 'OPERATIONS' menu. The navigation bar at the top includes 'MONITOR', 'DASHBOARD', 'CONFIGURATION', 'ANALYZE', and 'OPERATIONS'. The user is logged in as 'Admin'. The 'Import' form contains the following fields:

- Protocol:** A dropdown menu currently showing 'Protocol'.
- IP Address/Hostname:** A text input field containing 'XXX.XXX.XXX.XXX'.
- Username:** A text input field containing 'Username'.
- Password:** A text input field containing 'Password'.
- Path:** A text input field containing 'Path'.
- File Type:** A radio button selection with 'JSON' selected.

At the bottom right of the form, there are two buttons: 'Import' (highlighted in blue) and 'Reset' (grey). The footer of the page includes links for 'Feedback', 'Privacy Policy', and 'Legal Notices', and a copyright notice: '©2017 Extreme Networks, Inc. All rights reserved.'

Figure 33: 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**
- 3 When all server parameters have been configured, select **Import** to execute the database export. Select **Reset** to remove server information from the screen.

Troubleshooting

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

- Captive Portal Debug

[Captive Portal Debug Log](#) on page 54

Captive Portal Debug Log

Captive Portal Debug Log

RF Domain: Include all devices

Select Debug Messages

All Debug Messages

Authentication debug messages

Captive-portal client debug messages

Wireless Clients

All Wireless Clients

Selected Wireless Clients (up to 9)

Filter Criteria

Duration Of Message Capture*: Minute(s)

Maximum Events Per Wireless Client*:

Figure 34: 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:

- 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:

- 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.

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

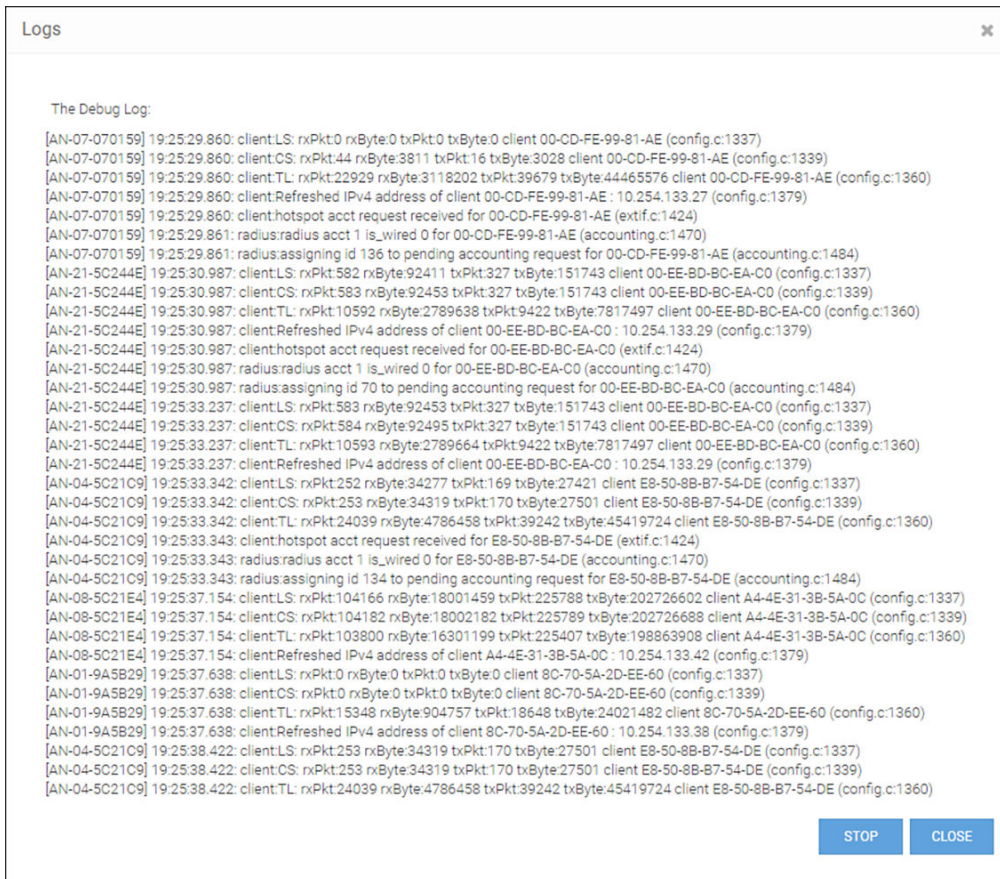


Figure 35: Captive Portal Debug Log Output