



ExtremeGuest™ Essentials Configuration Guide

9037976-00
January 2024



Copyright © 2024 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, see: www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses.

End-user license agreements and open source declarations can be found at: <https://www.extremenetworks.com/support/policies/open-source-declaration/>



Table of Contents

Preface.....	5
Text Conventions.....	5
Documentation and Training.....	6
Open Source Declarations.....	7
Training.....	7
Help and Support.....	7
Subscribe to Product Announcements.....	8
Send Feedback.....	8
About this Guide.....	9
Essentials Prerequisites and Limitations.....	9
Introduction to Guest Essentials Configuration	10
Splash Pages.....	11
Onboarding Policies.....	11
User Profile.....	11
Guest Essentials Onboarding with Terms and Conditions.....	12
Configure the Network Policy.....	12
Configure the Wireless Network.....	13
Configure Guest Essentials Services.....	14
Configure the Onboarding Policy.....	15
Create Onboarding Rules.....	16
Configure the Splash Template.....	17
Validating Guest Registration with Email and SMS.....	20
Configure the Wireless Network for Email and SMS.....	20
View Pre-Configured Guest Services for Email and SMS.....	21
Configure the Onboarding Policy for Email and SMS.....	22
Configure the Notification Policy for Email and SMS.....	23
Create Onboarding Rules for Email and SMS.....	24
Configure the Splash Template for Email and SMS.....	25
Social Media Onboarding.....	28
Configure the Wireless Network for Social Media.....	28
Add IP Objects to the Walled Garden List	31
Configure Guest Services for Social Media.....	33
Configure the Onboarding Policy for Social Media.....	34
Create Onboarding Rules for Social Media.....	34
Configure the Splash Template for Social Media.....	35
Validating Guest Essentials Access.....	36
Validating Guest Access with Terms and Conditions	36
Validating Guest Essentials Email and SMS.....	38

Validating Social Media Authentication.....	39
Guest Essentials Analytics.....	41
Guest Essentials Dashboard Analytics.....	41
Guest Essentials User and Device Statistics.....	42
The Clients Page.....	42
Create Custom Dashboards.....	42
Troubleshooting: Fixing Error Messages.....	44
Guest Essentials Terms & Conditions of Use.....	47



Preface

Read the following topics to learn about:

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

Text Conventions

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

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

Table 1: Notes and warnings






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

Table 2: Text

Convention	Description
screen displays	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words <i>enter</i> and <i>type</i>	When you see the word <i>enter</i> 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 <i>type</i> .
Key names	Key names are written in boldface, for example Ctrl or Esc . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

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

Documentation and Training

Find Extreme Networks product information at the following locations:

[Current Product Documentation](#)

[Release Notes](#)

[Hardware and Software Compatibility](#) for Extreme Networks products

[Extreme Optics Compatibility](#)

[Other Resources](#) such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the [Open Source Declaration](#) page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the [Extreme Networks Training](#) page.

Help and Support

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

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

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

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

Subscribe to Product Announcements

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

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

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

Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

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

To send feedback, email us at documentation@extremenetworks.com.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.



About this Guide

[Essentials Prerequisites and Limitations](#) on page 9

This guide provides the following client onboarding methods:

- Onboarding with accepted terms and conditions
- User registration with email or phone verification
- Social media onboarding with user authentication.

When onboarding and configuration is complete, the user uses their client to connect to guest service set identifiers (SSID). This document describes the steps to monitor guest statistics. Guest statistics provide valuable insights to track guest wireless usage.

Essentials Prerequisites and Limitations

This document provides the information you need to configure the ExtremeGuest Essentials services.

For more information, see the following product documentation:

- [ExtremeCloud IQ](#)
- [ExtremeGuest Essentials User Guide](#)
- [ExtremeGuest Essentials Setup Guide](#)

You must be familiar with accessing and performing basic functions in ExtremeCloud IQ.

Before you begin, you need the following:

- Network policies configured in ExtremeCloud IQ
- Access points adopted and assigned to the correct network policies.



Introduction to Guest Essentials Configuration

[Splash Pages](#) on page 11

[Onboarding Policies](#) on page 11

[User Profile](#) on page 11

This guide covers the following high-level tasks:

- ExtremeCloud IQ log in and basic network configuration
- Network policy configuration
- Guest Essentials rules and policies configuration
- Splash template creation
- Guest onboarding validation and statistics monitoring.



Note

To configure the network, you need an access point connected to ExtremeCloud IQ and a wireless client to test the guest service set identifier (SSID).

Before you begin, you must understand which configurations and processes run on ExtremeCloud IQ and which are created within ExtremeGuest Essentials. The reason for this is if you make a configuration change in ExtremeCloud IQ, you must push an update to the access point from the cloud. However, ExtremeGuest Essentials independently saves changes, so need to push changes to access points.

When a user connects to the guest network, ExtremeCloud IQ sends guest authentication requests to the ExtremeGuest Essentials process in the cloud and evaluation is performed according to the workflow defined in the onboarding policy.

When deploying the ExtremeGuest Essentials solution, configure the following in ExtremeCloud IQ:

- Create a wireless network and enable **Advanced Guest Access**. The Advanced Guest Access parameter indicates that guest onboarding is managed by ExtremeGuest Essentials
- Configure access points to treat ExtremeGuest Essentials as an external Captive Web Portal (CWP)
- Configure the wireless network on access points based on the network policy assignment.

Splash Pages

Splash pages for the captive web portal are hosted in the cloud. ExtremeGuest Essentials presents splash pages to users based on the wireless network and users location, to customize the guest experience at different locations.

Onboarding Policies

Onboarding policies define conditions that need to be met for the guest user to gain access to the network. For example, a user can only register using their corporate email. All communication related to guest users onboarding takes place between the client and ExtremeGuest Essentials based on the applicable onboarding policy. ExtremeGuest Essentials selects the onboarding policy based on the wireless network and users' location, allowing for customizing the guest experience at different locations.

User Profile

ExtremeGuest Essentials sends authentication results (success or failure) to the access point. The access point assigns a user profile to the guest user. The user profile defines further network access granted to the guest user. User profile selection is done based on the Guest Access Policy returned by ExtremeGuest Essentials after a successful onboarding.



Guest Essentials Onboarding with Terms and Conditions

[Configure the Network Policy](#) on page 12


[Configure the Wireless Network](#) on page 13

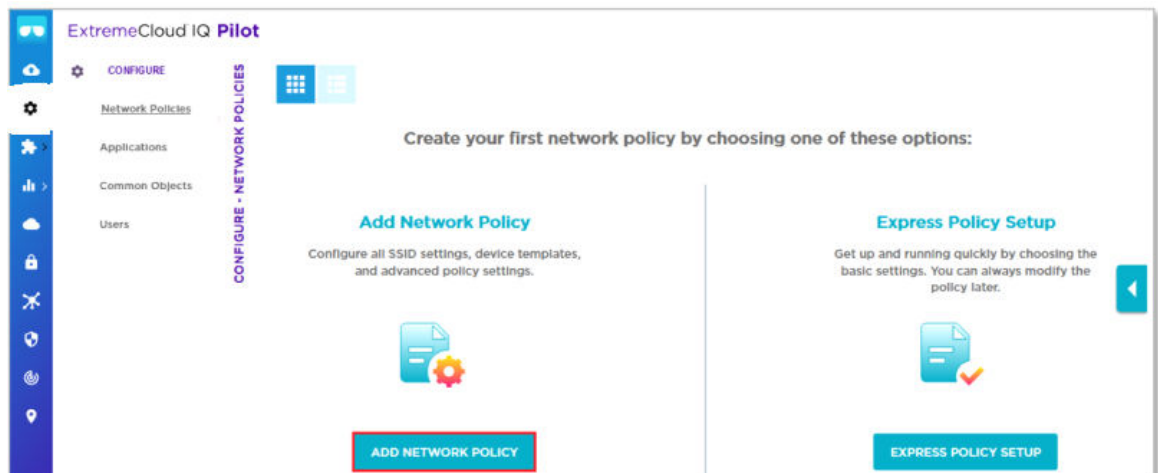
[Configure Guest Essentials Services](#) on page 14

A guest user is successfully onboarded, when they accept the Guest Essentials terms and conditions, also known as the Acceptable Use Policy (AUP).

Configure the Network Policy

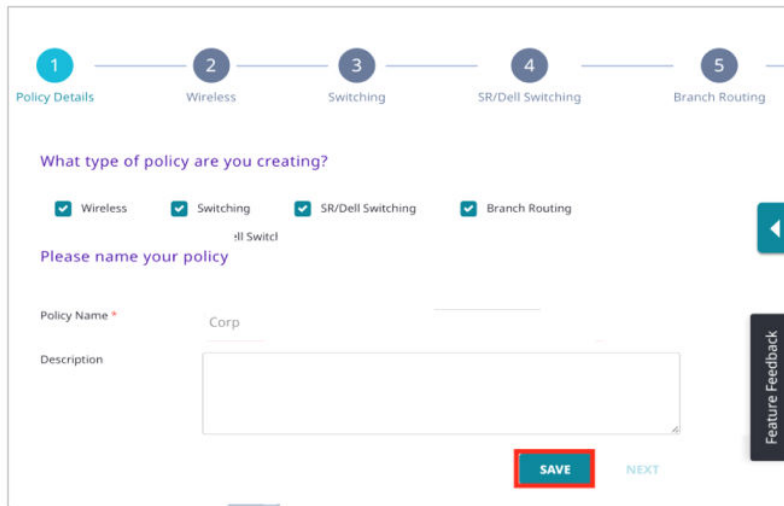
Perform these steps to login to ExtremeCloud IQ and create a network policy.

1. Log in to ExtremeCloud IQ.
2. In the main navigation bar, select .
3. Select **Network Policies**.
4. Select **Add Network Policy**.



5. In the **Policy Name** field, type a name for the policy.

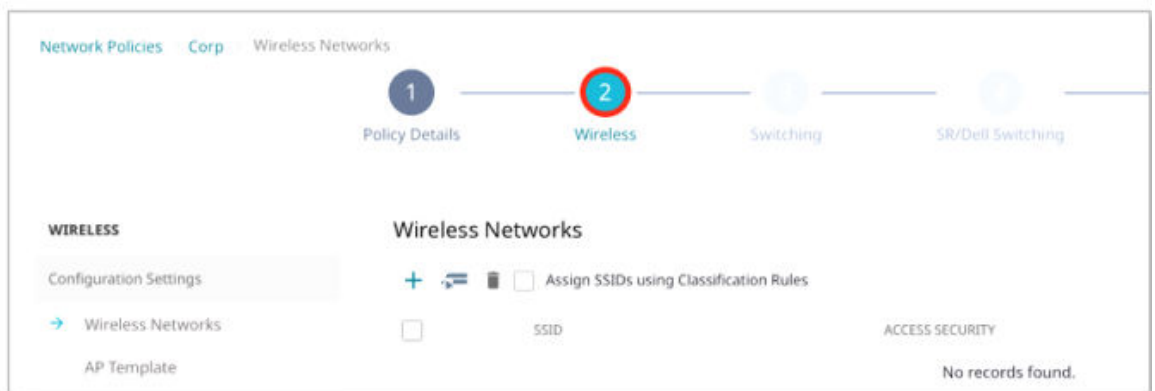
6. Select **Save**.



Configure the Wireless Network

Perform these steps to create a wireless service set identifier (SSID) with Open security.

1. Select **Wireless Networks**.
2. Select **+**.



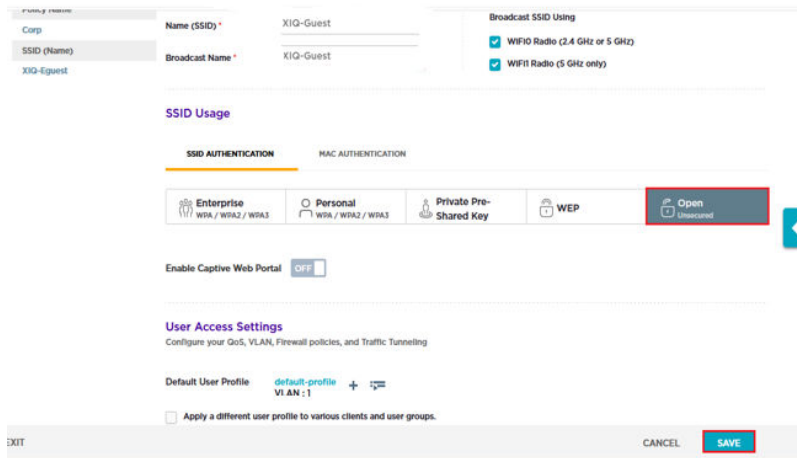
3. In the **Name (SSID)** and **Broadcast Name** fields, enter **XIQ-Guest**.
4. In the **SSID Usage** section, select **Open**.
5. In the **User Access Settings** section, **Default User Profile** field, select **Default-Profile**.

6. Select **Save**.



Note

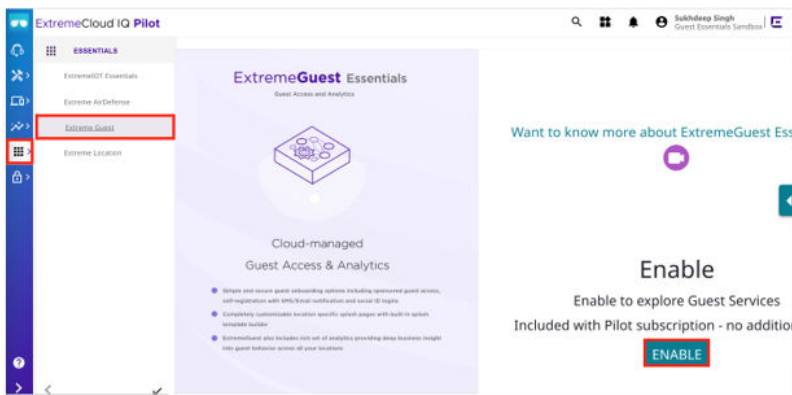
To use ExtremeGuest Essentials with the wireless network, you must enable **Advanced Guest Access**. **Advanced Guest Access** is only available after subscribing to ExtremeGuest Essentials.



Configure Guest Essentials Services

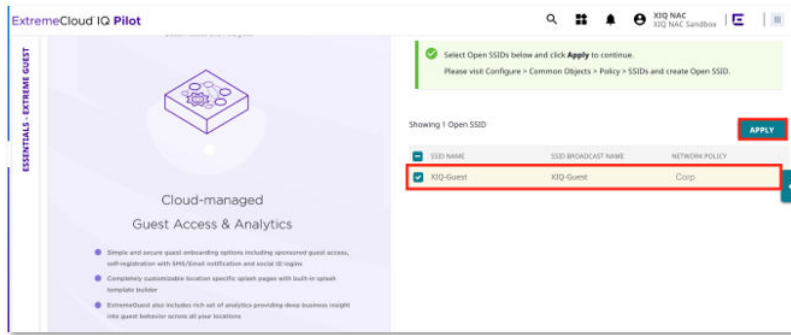
Perform these steps to configure Guest Essentials services.

1. Login to ExtremeCloud IQ.
2. In the main navigation bar, select .
3. Select **Enable**.



4. To enable Guest Services on the ExtremeCloud IQ service set identifier (SSID), select **XIQ-Guest**.

5. Select **Apply**.



Note

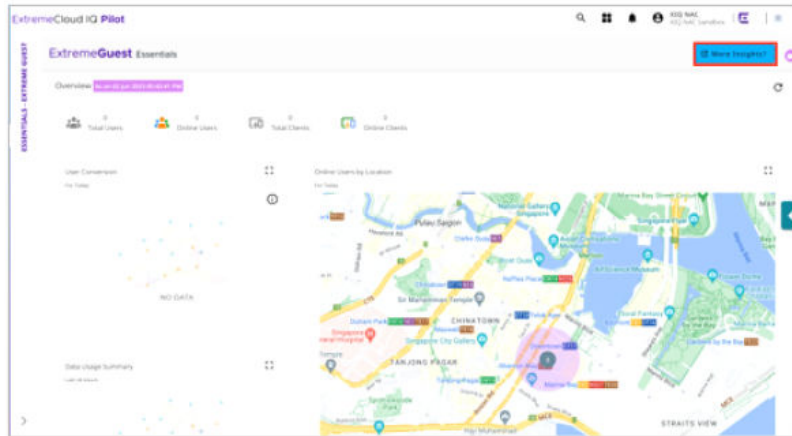
You have enabled **Advanced Guest Access** for the XIQ-Guest SSID and made a configuration change in the network policy. This configuration requires a push to the access point.

Guest Essentials Summary Page

The Guest Essentials summary page contains guest analytics, statistics and connectivity trends. As wireless devices connect to the guest SSID, Guest Essentials posts details to the summary page.

6. To access configuration options, select **More Insights**.

ExtremeGuest Essentials opens in a separate tab.



Configure the Onboarding Policy

The onboarding policy defines conditions for guest users to gain access to the network. The user must accept terms and conditions presented on the portal.

Perform these steps to configure the onboarding policy.

1. Select *
2. Select **Policy**.

3. To create a new policy, select **+**



4. Create a policy that registers clients and grants guest access to users as follows:

- Name: **Guest-AUP**
- Condition: **Any**
- Action: **Register Client**
- Time Period: **30 Minutes**

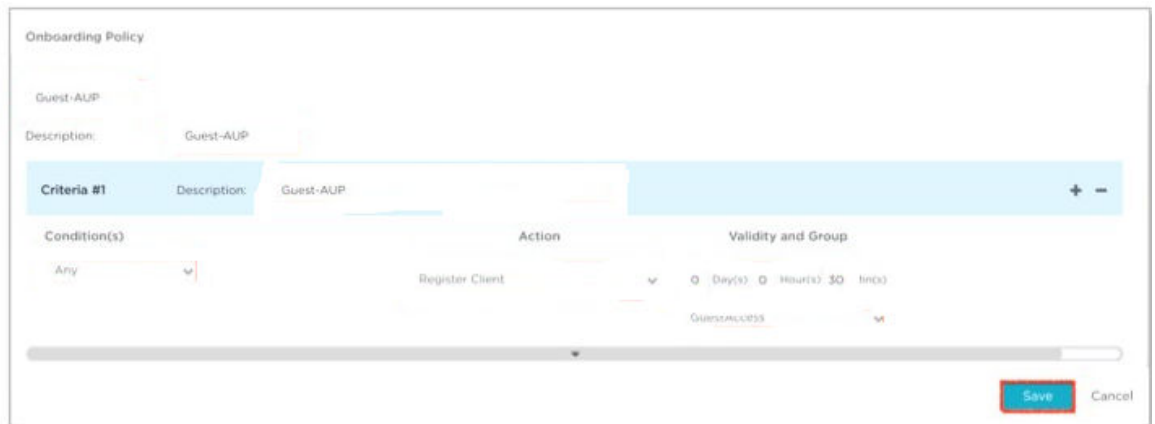


Note

The authorization policy time must be lower than the onboarding policy time.

5. Assign the user to the **GuestAccess** access group.

6. Select **Save** to complete the process.



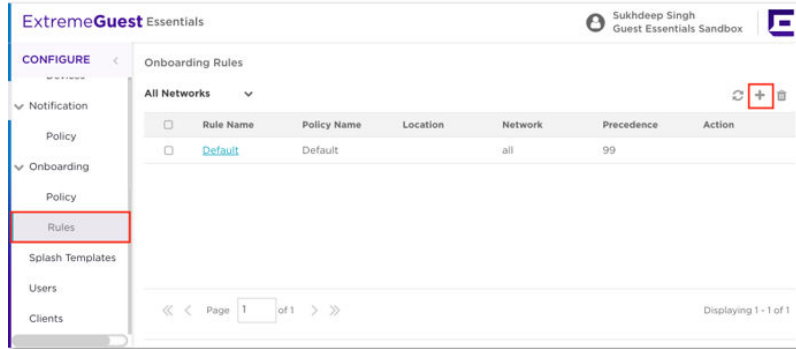
Guest Access level is assigned to a user after a successful registration.

Create Onboarding Rules

Onboarding rules tie together the SSID and the location created in ExtremeCloud IQ to trigger the Guest-AUP authorization policy.

Perform these steps to create an onboarding rule to trigger the onboarding policy.

1. From the **Configure** list, select **Onboarding > Rules**.
2. Select **+**.



3. Use this table to configure the following parameters:

Table 4: Configure Parameters


Field	Select
Rule Name	Guest-AUP
Policy	Guest-AUP
Network	XIQ-Guest
Location	San Jose

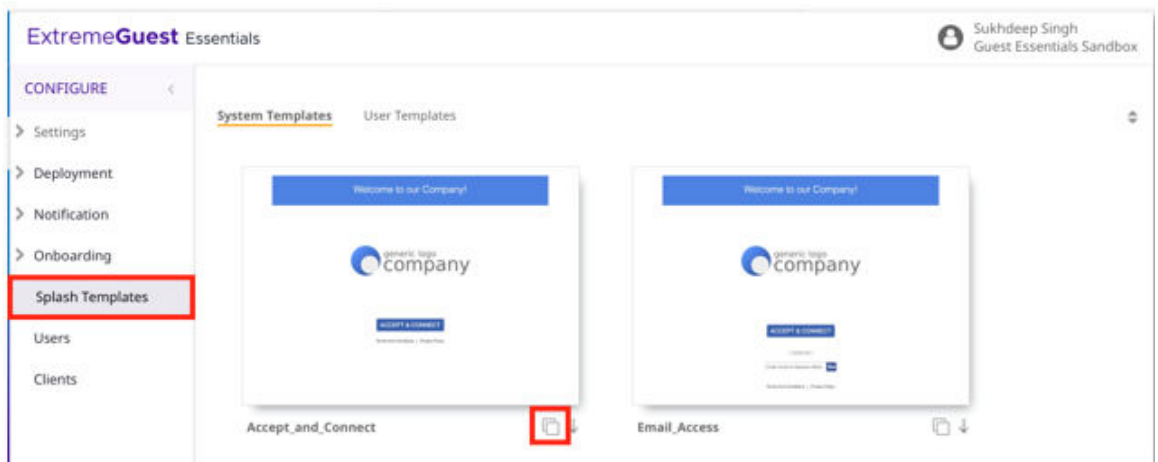
4. Select **Save** to complete the process.

Configure the Splash Template

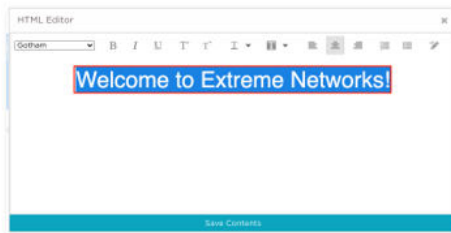
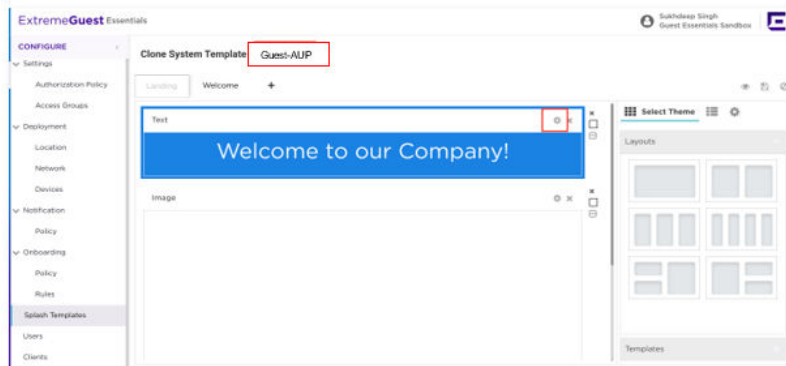
A splash template contains various captive portal web pages like the landing page, the registration page and the welcome page. You can clone multiple splash templates to customize and assign to a location or network. To create a splash page for this simple AUP guest configuration, you need to select the **Splash Template** and clone the **Accept_and_Connect** template.

Perform these steps to configure the splash template.

1. From the **Configure** list, select **Splash Templates**.
2. To clone the **Accept_and_Connect** template, select .




3. In the **Clone System Template** field, type **Guest-AUP**.
4. To edit the welcome message, select .
5. Select **Save Contents**.

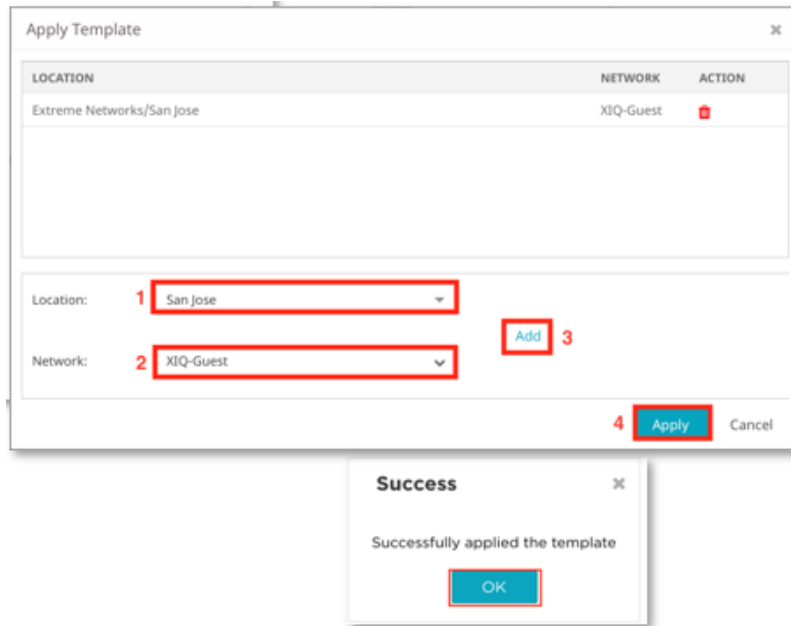


Note

You can experiment with other settings to change the color of the text, the background and the font.

6. To save the **Guest-AUP** splash template, select .
7. To assign the **Guest-AUP** splash template to the network in San Jose, in the **Location** field, select **San Jose**.
8. In the **Network** field, select **XIQ-Guest**.

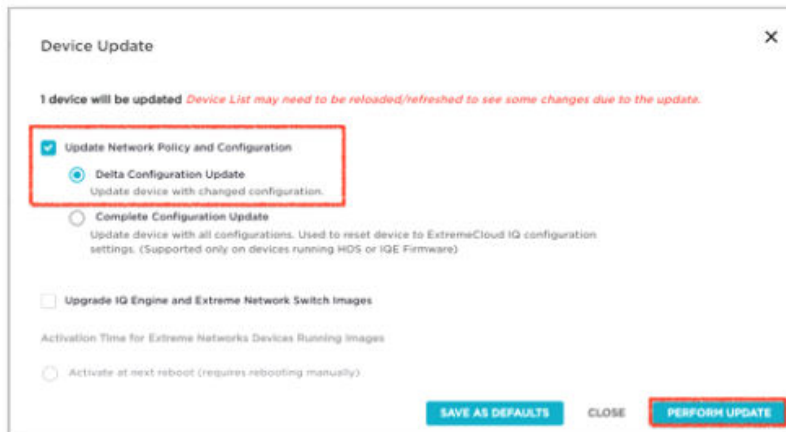
9. Select **Add > Apply > OK**.



Note

When a user connects to the **XIQ-Guest** service set identifier (SSID) in San Jose, the captive portal pages from this template is presented to the user.

10. To push the updated configuration to the access point, go to the **Configuration > Manage > Devices** view and select the access point.





Validating Guest Registration with Email and SMS

[Configure the Wireless Network for Email and SMS](#) on page 20



[View Pre-Configured Guest Services for Email and SMS](#) on page 21

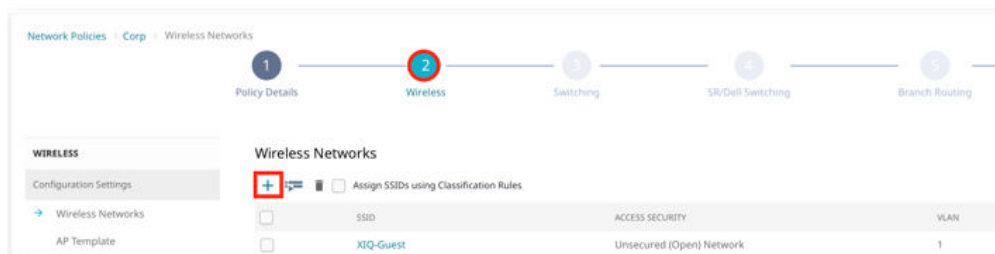
An alternative method for onboarding guest users is to have the user validate an email or a phone number. The user phone number or email address pairs the guest user to a validated identity for security reasons or marketing purposes. In this workflow, the network uses email or short messaging service (SMS) to send a one-time passcode (OTP) to the user for validation before allowing access.

Configure the Wireless Network for Email and SMS

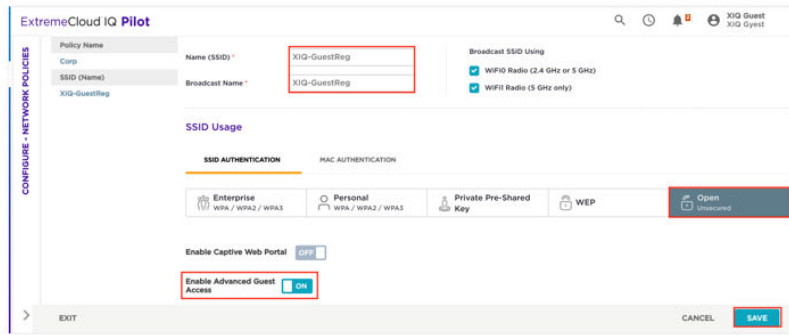
To create a second onboarding policy, you must create a second wireless network.

Perform these steps to configure the wireless network for email and SMS.

1. Login to ExtremeCloud IQ.
2. In the main navigation bar, select 
3. Select **Network Policies > Corp > Wireless Networks**.
4. Select 

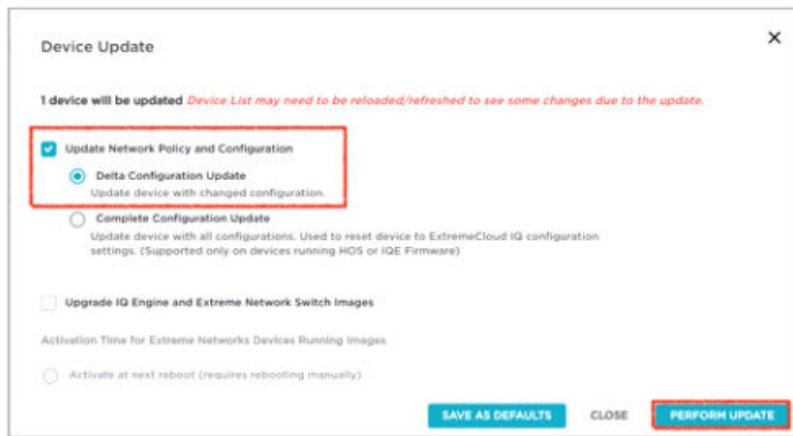


5. In the **Name (SSID)** and **Broadcast Name** fields, enter **XIQ-GuestReg**.
6. Select **Open Authentication**.
7. Select **Enable Advanced Guest Access** and toggle it **ON**.

8. Select **Save**.

9. To push the updated configuration to the access point, go to the **Configuration > Manage > Devices** view and select the access point.

10. Select **Perform Update**.

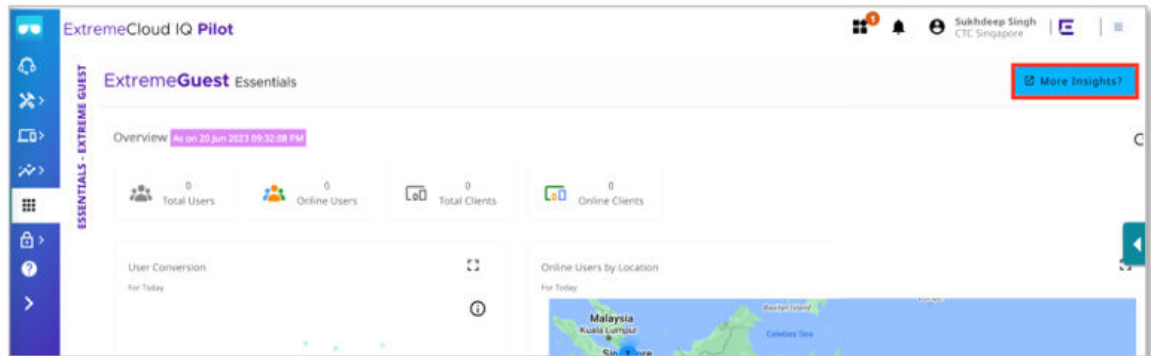


View Pre-Configured Guest Services for Email and SMS

Perform these steps to view pre-configured guest registration services for email and SMS.

1. Log into ExtremeCloud IQ.
2. In the main navigation bar, select ☰ .

3. Select **More Insights**.

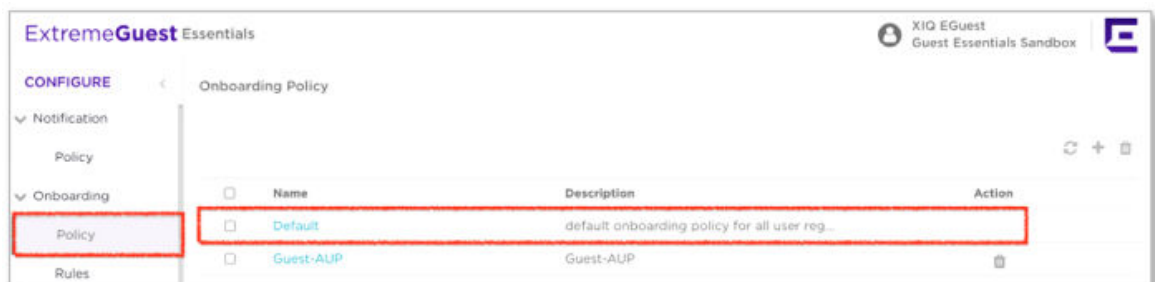


Configure the Onboarding Policy for Email and SMS

A guest user who registers using the Extreme Networks corporate email address receives a one-time passcode(OTP). The network sends the passcode to the email address and the user uses the passcode to register a device. Users can change their email domain, for example, gmail.com. If the user provided a valid phone number during the registration process, the network sends the passcode to a phone number. There are two registration criteria. If the user does not meet the first condition, the second condition automatically occurs.

Perform these steps to configure the onboarding policy for email and short messaging service (SMS).

1. From the **Configure** list, select **Onboarding > Policy**.
2. Select the default onboarding policy.



3. In the **Criteria #1 Description** field, enter **Email**.
4. In the **Action** field, select **Send a One-Time-Passcode to User**.

The network sends an OTP to the user's email address and an SMS to the phone number provided.

- Accept the default **Validity and Group** duration of **1 Day & 30 Minutes**.
After successfully validating the OTP, the network assigns the user to the **GuestAccess** group for **1 Day & 30 Minutes**. You can change the duration.

The screenshot shows the 'Onboarding Policy' configuration page. At the top, there is a 'Default' field and a 'Description' field containing 'default onboardir'. Below this is a table for 'Criteria #1' with a description of 'mail'. The table has four columns: 'Condition(s)', 'Action', 'Validity and Group', and 'Notification Policies'. Under 'Condition(s)', there is a dropdown for 'User Email Domain' and a text input 'extremenetwor' with a plus sign. Under 'Action', there is a dropdown 'Send One-Time-Passcode to User'. Under 'Validity and Group', there are input fields for '1 Day(s)', '0 Hour(s)', and '30 Min(s)', along with a 'User*' dropdown set to 'NotifPolic1'. Under 'Notification Policies', there is a dropdown set to 'GuestAccess'. There is also a checkbox for 'Provide Temporary Access' which is unchecked.

- In the **Criteria #2 Description** field, enter **Catch all**.
- Select **Save**.
If the OTP validation is unsuccessful, the user is denied access and assigned to the **DenyAccess** group.

The screenshot shows the 'Onboarding Policy' configuration page for 'Criteria #2'. The 'Description' field contains 'catch all'. The table has three columns: 'Condition(s)', 'Action', and 'Notification Policies'. Under 'Condition(s)', there is a dropdown set to 'Any'. Under 'Action', there is a dropdown 'Deny Access' and a checkbox 'Update User' which is checked. Under 'Notification Policies', there is a dropdown 'User*' set to 'NotifPolic1'. At the bottom right, there are 'Save' and 'Cancel' buttons.

Configure the Notification Policy for Email and SMS

The notification policy defines the format of the message and the one-time passcode (OTP) sent to the user. The default policy uses the pre-configured notification policy, **UserNotifPolicy**, for the message format.

Perform these steps to review the pre-configured notification policy, **UserNotifPolicy**.

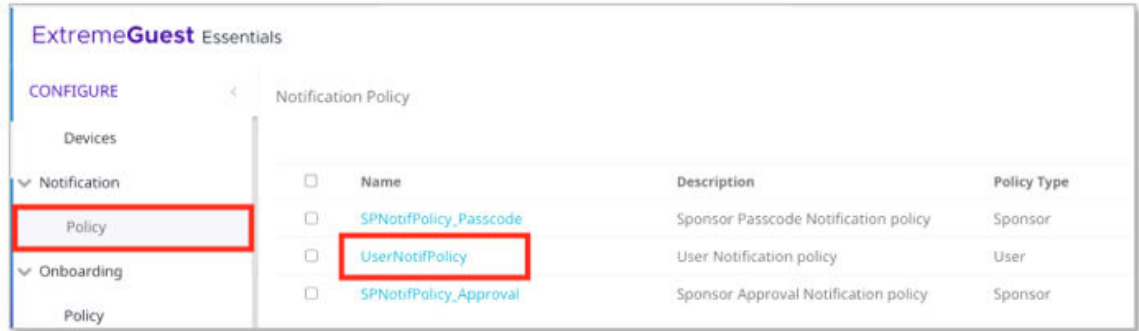
- Go to **Notification > Policy**.

2. Select **UserNotifPolicy**.



Note

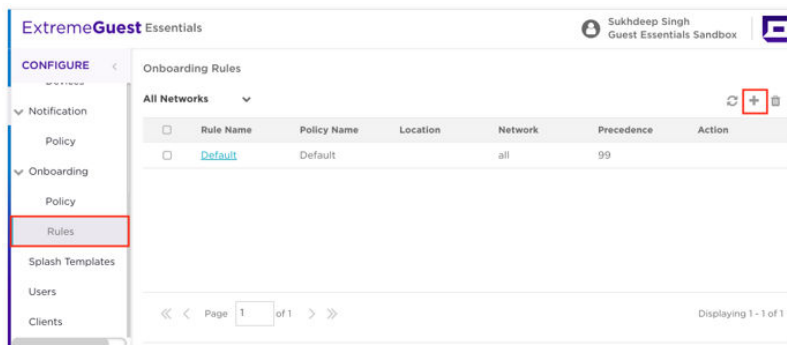
The SMS message format is designed to prevent the message from being blocked in certain countries as spam.



Create Onboarding Rules for Email and SMS

Perform these steps to create an onboarding rule using the default policy.

1. From the Configure list, select **Onboarding > Rules**.
2. To create a new rule, select **+**.



3. Use this table to configure the following parameters:

Table 5: Configure Parameters

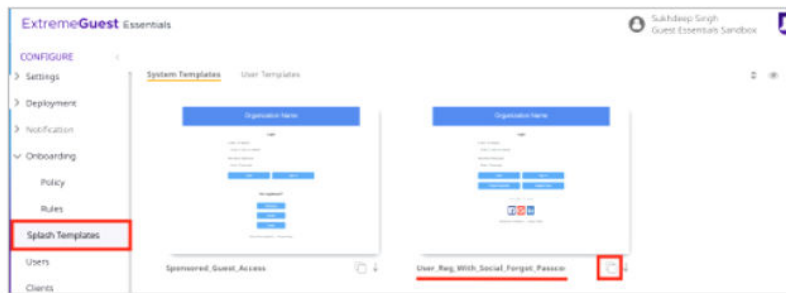
Field	Select
Rule Name	GuestReg
Policy	Default
Network	XIQ-GuestReg
Location	San Jose
Procedure	2


4. Select **Save**.

Configure the Splash Template for Email and SMS

Perform these steps to create a splash template for guest registration using email and SMS.

1. From the **Configure** list, select **Splash Template**.
2. Select the **User_Reg_with_Social_Forgot_Passcode** template.
3. To clone the **User_Reg_with_Social_Forgot_Passcode** template, select 



4. In the **Clone System Template** field, type **GuestRegistration**.
5. To edit the welcome message, select 



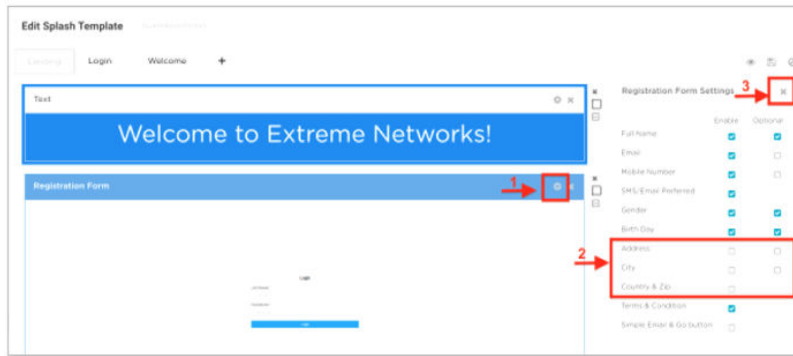
Note

When creating a splash page, do the following:

- Specify mandatory and optional fields for the user registration form
- Delete fields that are not relevant.

6. Select **Save Contents** when done.

7. In the **Registration Form** field, select  and un-check the **Address** field options.

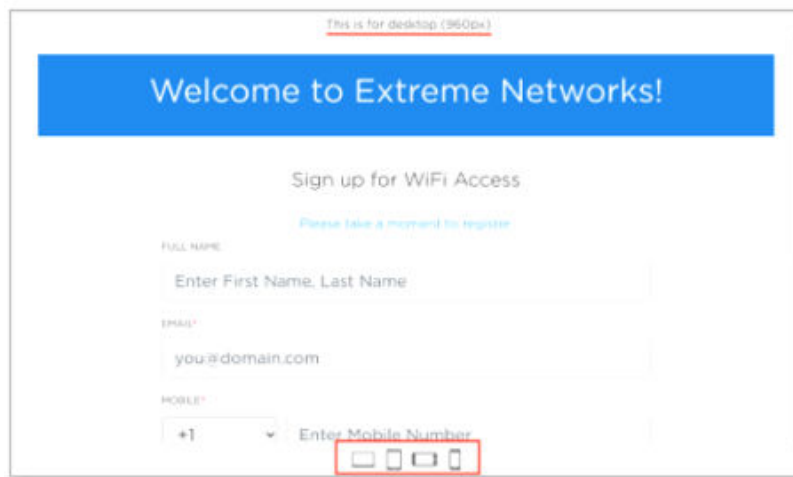


8. To view the changes, select 



Note

To confirm that the splash page displays correctly on devices with different screen sizes and orientations, select viewing options for different device types (phone, tablet, desktop). The default layout is optimized for desktops.



9. To change the title text to **Extreme Networks**, select **Login** → .



10. To complete the configuration of the splash template, select 

11. Select **User Template**.

12. In the **Location** field, select **San Jose**.

13. In the **Network** field, select **XIQ-GuestReg**.

14. Select **Apply**.

When users in San Jose connect to the **XIQ-GuestReg** service set identifier (SSID), the network presents this splash template to them.



Note

- You are not required to do a configuration update to the access point at this stage, as there are no configuration changes made to the network policy after the last configuration push to the access point.
- The ExtremeGuest Essentials configuration and workflow are stored in the ExtremeGuest Essentials application.



Social Media Onboarding

[Configure the Wireless Network for Social Media](#) on page 28

[Configure Guest Services for Social Media](#) on page 33

ExtremeGuest Essentials allows social media authentication for guest users. The access point sends open authorization (OAUTH) requests to Facebook, Google or LinkedIn to authenticate on behalf of users. On successful validation of user credentials, the user is granted access for the duration allowed by the onboarding policy.



Note

Guest Essentials do not capture or store user credentials or any other user information.

The Google OAUTH server tracks user-agent browsers used at log in and does not recognize Apple CAN and Android Mini browsers as valid user-agents. The Google OAUTH server blocks any mobile browser used as a captive portal pop-up screen. On Android devices, the Google OAUTH server redirects to Chrome. On Apple devices, the Google OAUTH server launches Safari (or other browsers) manually to complete registration using Google+. Other social media methods do not have this issue.



Note

Dependencies: You must complete all guest registration configuration before configuring social media onboarding, including the following:

- **XIQ-GuestReg** service set identifier (SSID)
- The onboarding rule, **GuestReg**
- The **GuestRegistration** splash template.

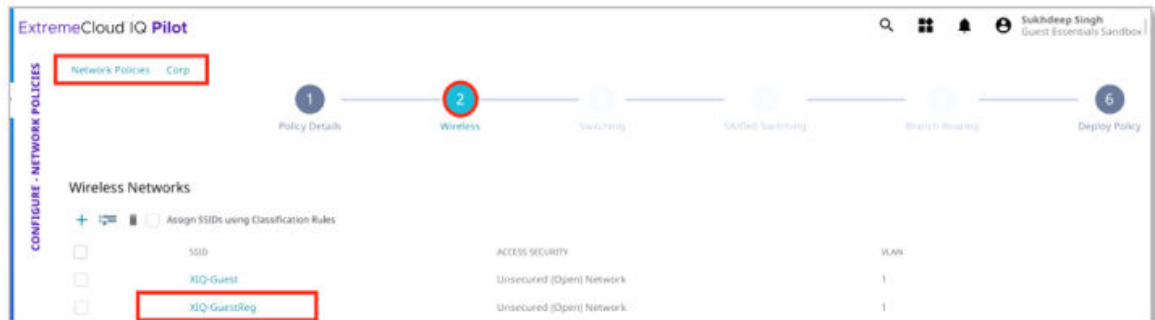
Configure the Wireless Network for Social Media

To add social media authentication to a new wireless network, after logging in to the ExtremeCloud IQ configuration menu, configure the network with open authentication and select **Enable Advanced Guest Access**.

Perform these steps to modify the **XIQ-GuestReg** service set identifier (SSID) to add social media authentication to the wireless network.

1. Log into ExtremeCloud IQ.

2. In the main navigation bar, select ✖
3. Select **Network Policy > Corp.**
4. From the **Wireless Network** list, select **XIQ-GuestReg.**



Walled Garden Entries

For every other scenario except social media authentication, when using captive portal, all internet access is blocked until the user completes the captive portal authentication and registration. For using social media authentication, internet access is required to complete the authentication. For example, when using **Facebook** authentication, the user needs access to **Facebook** servers to validate **Facebook** credentials.

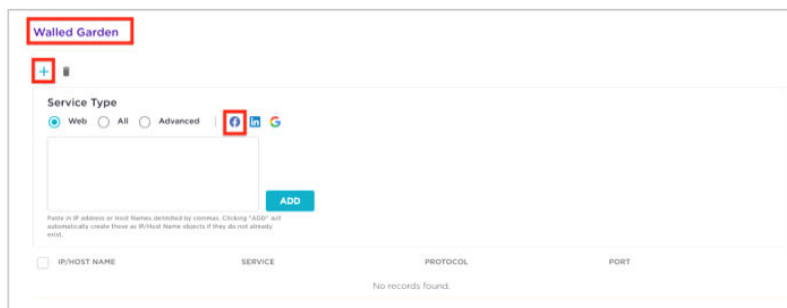
For social media authentication, you must add domain name system (DNS) and internet protocol (IP) subnets to the walled garden.



Note

Only add walled garden entries relevant to the social media authentication mechanisms being used.

5. Go to **Walled Garden**.
6. To add walled garden entries, select **+**.
7. To add Facebook entries, select **f**.



Note

Perform these steps very carefully. This is the most critical part of the process. Any mistakes can prevent successful authentication.

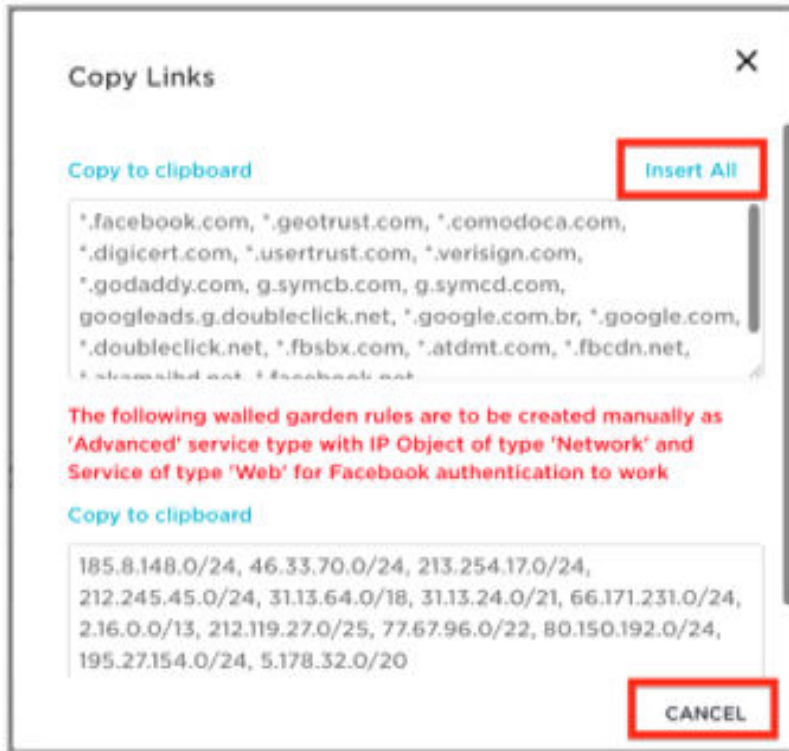
- To add fully qualified domain name entries, select **Insert All**.



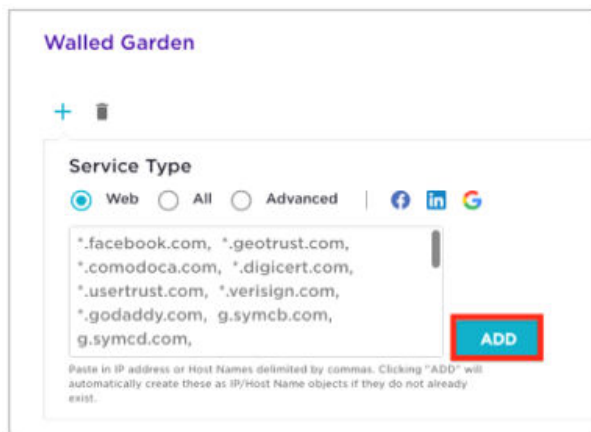
Note

Do not add the IP network at this time. You must add the IP network manually, as indicated by the warning displayed. Copy the IP list to a separate file. To be added later.

- Select **Cancel** to return to the previous screen.
- Repeat the process to add LinkedIn and Google authentication.



- Select **Add** to add all selected DNS entries to the walled garden.



Go to [Add IP Objects to the Walled Garden List](#).

Add IP Objects to the Walled Garden List

Prerequisite: Before continuing, you must complete the procedure, [Configure Wireless Network for Social Media](#)

Perform these steps to add internet protocol (IP) objects to the walled garden list.

1. In the **Walled Garden** screen, select **+**.
2. In the **Service Type** field, select **Advanced**.
3. In the **Service** field, select **Web**.
4. In the **IP Object/Host Name** field, select **+**.



5. Look at the first entry from the list of IP network entries that you saved.



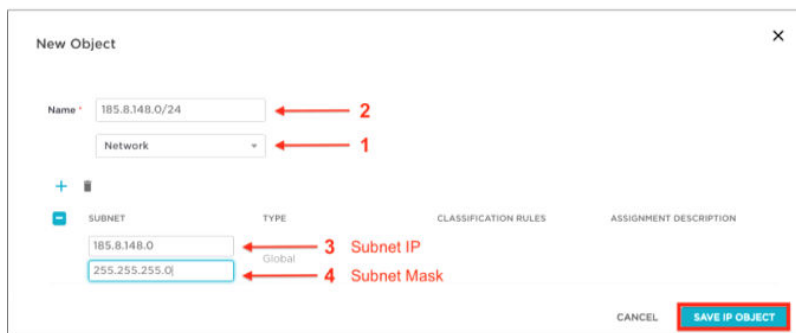
Note

The first entry is **185.8.148.0/24**.

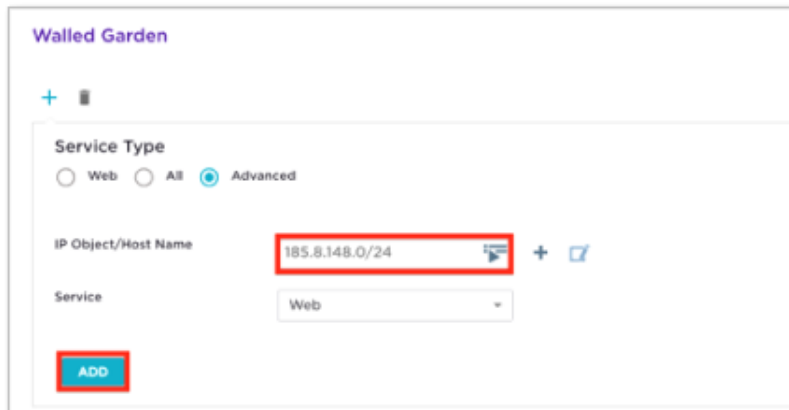
6. Use this table to configure the following parameters:

Table 6: Configure Parameters

Field	Select
Object Type	Network
Name	185.8.148.0/24
Subnet IP	185.8.148.0
Subnet Mask	255.255.255.0



- To add the IP object to the walled garden list, select **Add**.



The screenshot shows the 'Walled Garden' configuration page. At the top left, there is a plus sign and a list icon. Below that, the 'Service Type' section has three radio buttons: 'Web', 'All', and 'Advanced', with 'Advanced' selected. The 'IP Object/Host Name' field contains the text '185.8.148.0/24' and is highlighted with a red rectangular box. To the right of this field are a plus sign and a copy icon. Below the IP field is a 'Service' dropdown menu currently showing 'Web'. At the bottom left of the form, there is a blue 'ADD' button, also highlighted with a red rectangular box.

- Select **Save**.
- Repeat for the remaining entries, starting with **46.33.70.0/24**.

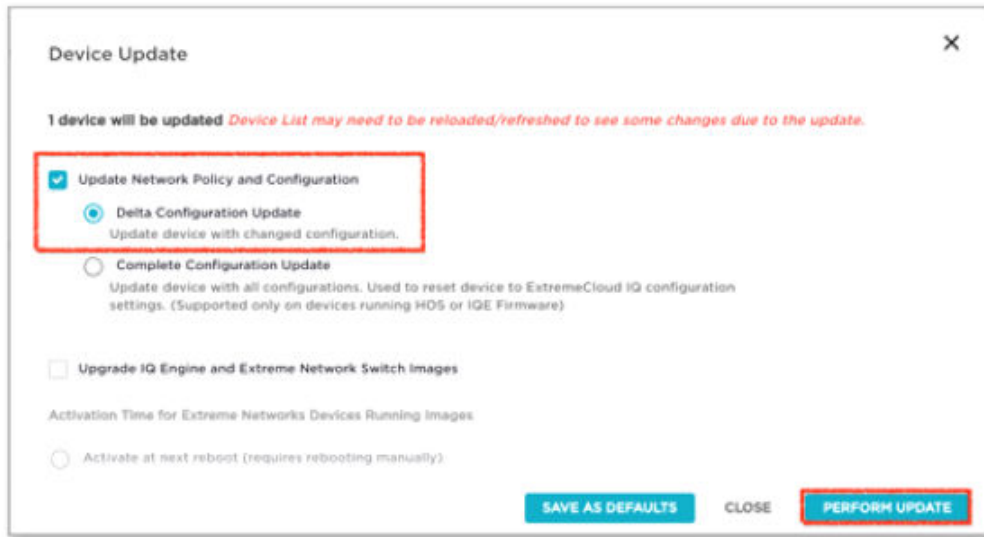


Note

- You must add all entries in one sitting. If you miss entries and add them later, that will corrupt the walled garden list. If you corrupt the walled garden list, you must restart by deleting all the entries and rebuilding the list
- These changes are made in ExtremeCloud IQ not Guest Essentials, so you must push changes to the access point.

- To push changes to the access point, go to **Configuration > Manage > Devices**.
- Select **Update Devices**.
- Select the access point and push the updated configuration to the access point.

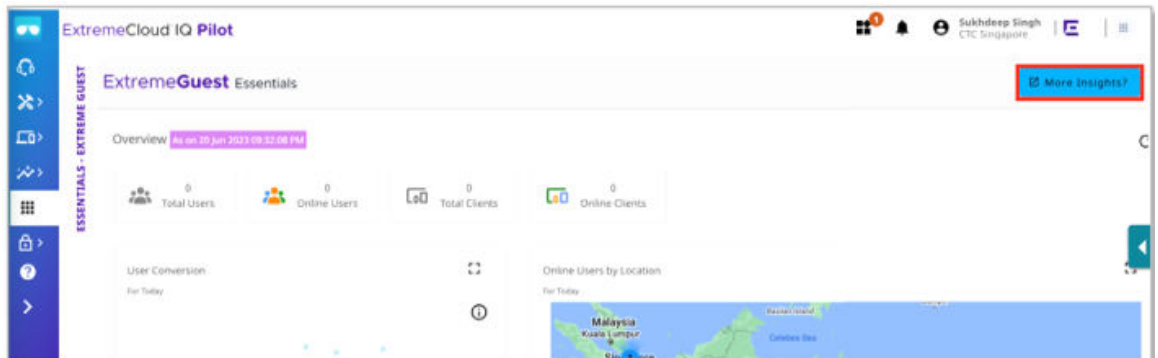
13. Select **Perform Update**.



Configure Guest Services for Social Media

Perform these steps to configure guest services for social media.

1. Go to ExtremeGuest Essentials.
2. Select **More Insights**.



Configure the Onboarding Policy for Social Media

To register clients for 30 minutes after successful onboarding through any social media authentication, edit the **Default** onboarding policy.

Perform these steps to configure the onboarding policy for social media.

1. From the **Configure** list, select **Onboarding** > **Policy**.
2. Select **Default**.

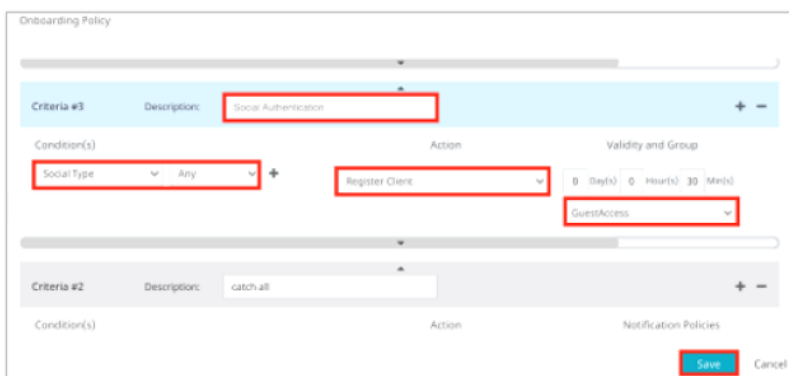


3. To add a second criteria and enable users to register using any social media authentication, select **+**.
4. Use this table to configure the following parameters:

Table 7: Configure Parameters

Field	Select
Description	Social Authentication
Condition	Social Type - Any
Action	Register Client
Time Period	30 Minutes
Access Group	GuestAccess

5. Select **Save**.



Create Onboarding Rules for Social Media

As you are using the same **XIQ-GuestReg** service set identifier (SSID) and the same onboarding policy, there is no need to create new onboarding rules for social media.

The **GuestReg** onboarding rules you created in the previous section, prompts the **Default** onboarding policy when a user connects to the **XIQ-GuestReg** SSID.

Configure the Splash Template for Social Media

The **GuestRegistration** splash template you created in the previous procedure supports social media authentication. Therefore, do not create or deploy any additional splash templates.



Validating Guest Essentials Access

[Validating Guest Access with Terms and Conditions](#) on page 36

[Validating Guest Essentials Email and SMS](#) on page 38

[Validating Social Media Authentication](#) on page 39

This section covers the following topics:

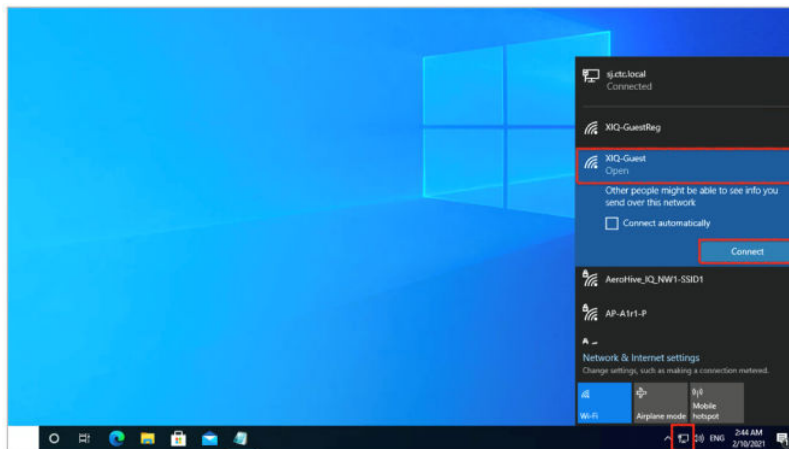
- Validating Guest Access with Terms and Conditions
- Validating Guest Essentials Email and SMS
- Validating Social Media Authentication

Validating Guest Access with Terms and Conditions

You need a wireless client to validate guest configurations. You can use a windows client or any other devices.

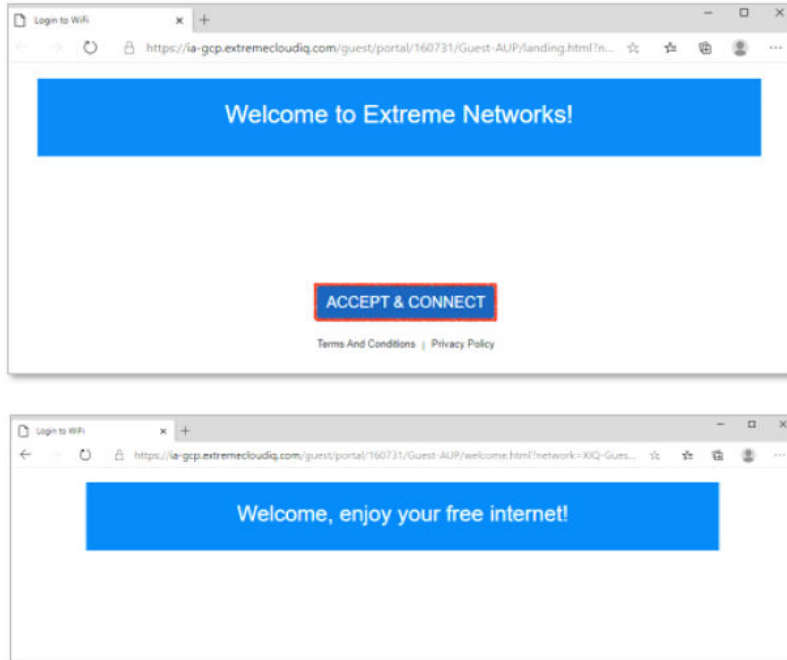
Perform these steps to validate Guest Essentials access.

1. In your task bar, select the wireless connection.
2. Select **XIQ-Guest**.
3. Select **Connect**.



The terms and conditions splash page displays.

4. To agree to the terms and gain access to the guest wireless network, select **Accept & Connect**.

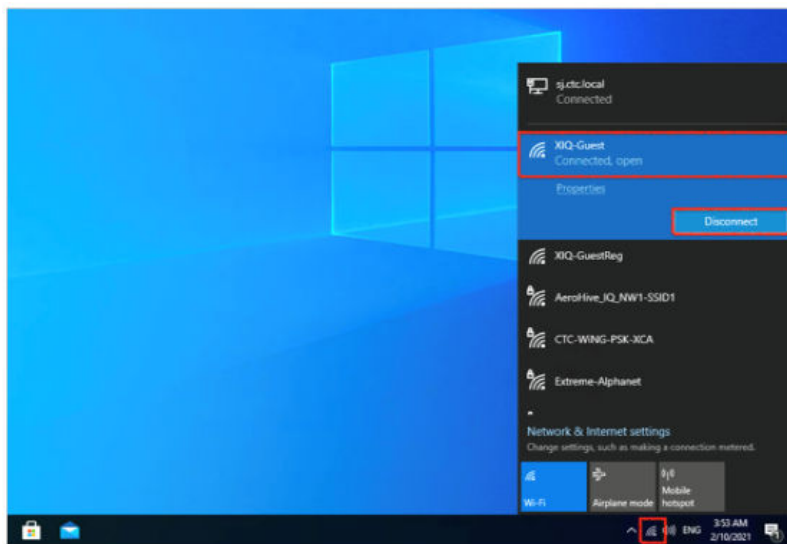



Note

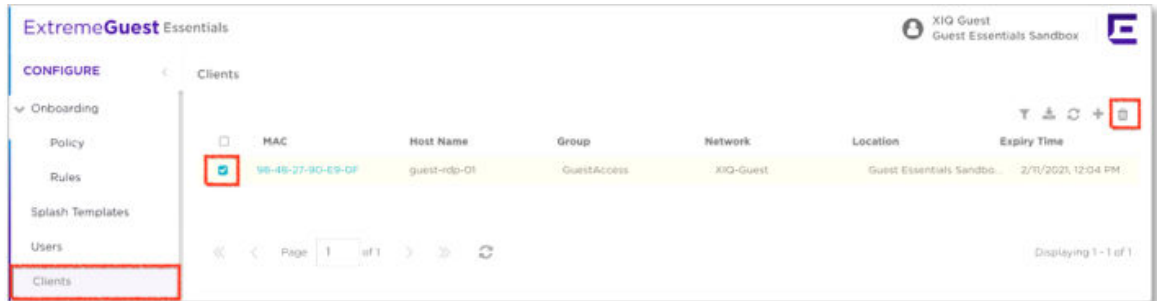
The onboarding policy allows network access for 30 minutes. To use the same client to validate guest registration on the **XIQ-GuestReg** service set identifier (SSID), you must disconnect the client from the **XIQ-Guest** SSID and delete it from the ExtremeGuest Essentials database.

If you need help, see [Troubleshooting: Fixing Error Messages - section #2](#) for more details.

5. Select **XIQ-Guest**.
6. Select **Disconnect**.



7. In the Guest Essentials **Configure** list, select **Clients**.
8. To delete the client, select 



Validating Guest Essentials Email and SMS

Perform these steps to validate Guest Essentials email and SMS.

1. In your task bar, select the wireless connection.
2. Select **XIQ-GuestReg**.
3. Select **Connect**.
The login page displays.
4. To access the registration page for the guest portal, select **Register Now**.



5. Populate all mandatory fields.



Note

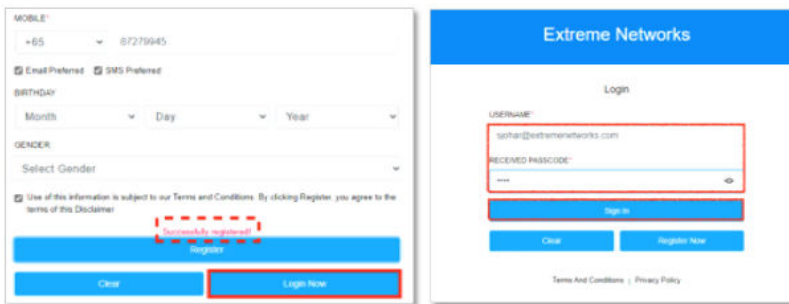
The email address must belong to the **@extremenetworks.com** domain.

- Put a check mark in the Terms and Conditions field.



Figure 1: Register Screen

- Select **Register**.
The user receives a one-time passcode by email or SMS.
- Select **Login Now**.
- In the **Username** field, type the email address you use to register.
- In the **Received Passcode** field, type the OTP.



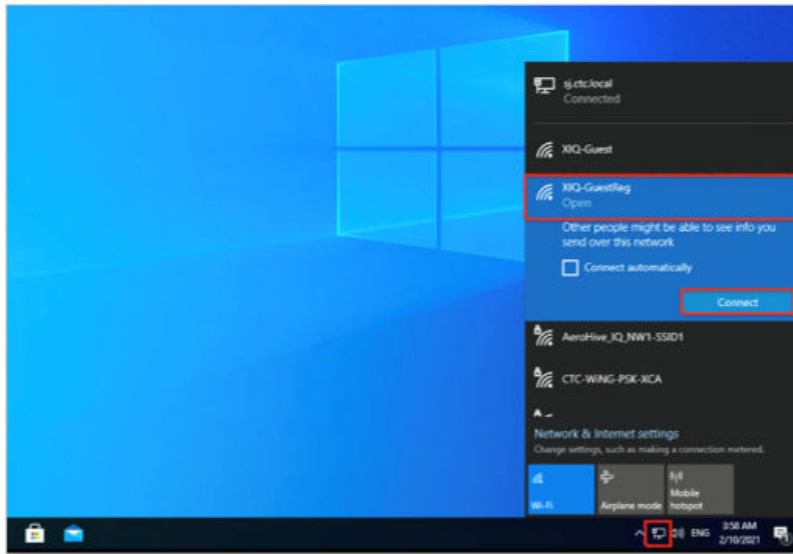
The user receives a welcome screen.

Validating Social Media Authentication

Perform these steps to connect a wireless client to the **XIQ-GuestReg** SSID.

- In your task bar, select the wireless connection.
- Select **XIQ-GuestReg**.

3. Select **Connect**.



The login page displays.

4. Select a social media platform.
5. Complete all mandatory fields.
6. Select **Register Now**.



The user receives a welcome screen.



Guest Essentials Analytics

[Guest Essentials Dashboard Analytics](#) on page 41

[Guest Essentials User and Device Statistics](#) on page 42

[Create Custom Dashboards](#) on page 42

ExtremeGuest Essentials provides guest analytics in the form of dashboard widgets that you can use for marketing and planning or to track network usage. The following are some guest analytics that Guest Essentials provides:

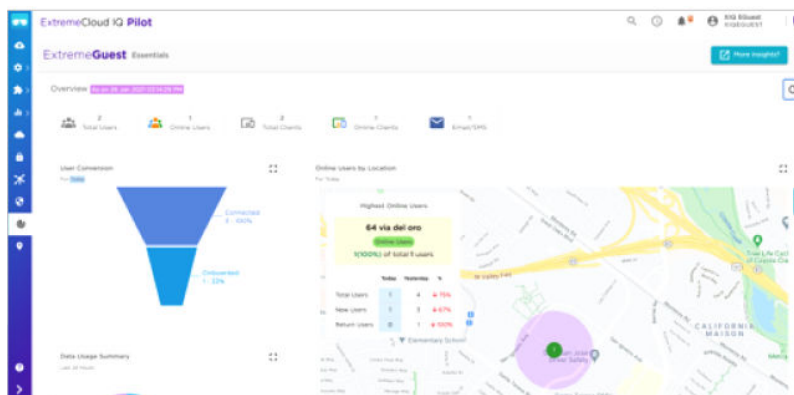
- Aggregated or site level analytics regarding user walk-in, time spent in various locations, and new users versus repeat visitors
- Tracking data on how users accessed the network, by email, vouchers, or social media. Which social media platform did users use to access the network. For example, Facebook, Google, LinkedIn
- Gathering data on the types of devices guest users use to onboard and the operating systems(OS) on these devices. For example Android, Windows, iOS
- Collecting user demographic information. For example, age and sex.

To monitor guest analytics, log into ExtremeGuest Essentials.

Guest Essentials Dashboard Analytics

Perform these steps to view and monitor Guest Essentials dashboard analytics.

1. To view a summary of old and new user walk ins and user conversion statistics for users that onboarded the guest network after connecting to the network, go to Guest Essentials.



2. To compare how the number of users varies across 24 hours today compared to 24 hours a day earlier, select **Data Usage** and **User Summary**.
3. To view a summary of the various types of client devices that have been used to connect to the guest environment, select the **Client Distribution** widget.

The **dwelt time** indicates the duration of time users have been spending on the guest network for the last 24 hours.

Guest Essentials User and Device Statistics

The **Users** page displays details about users registered on the guest wireless network. The **Users** page only displays guest information if the user used email registration or social media authentication to register on the network.

If user devices are onboarded using vouchers, or by accepting terms and conditions, the **Users** page is not available. Only the device details are available, as seen in the **Clients** page.

The Clients Page

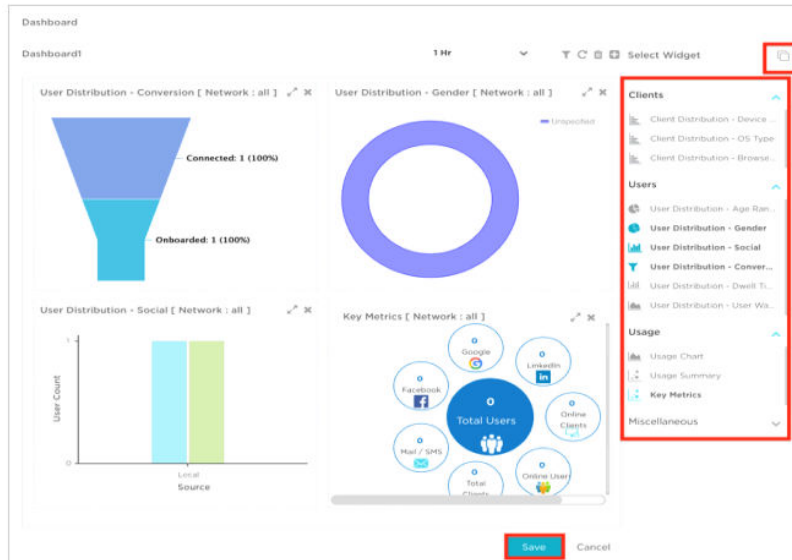
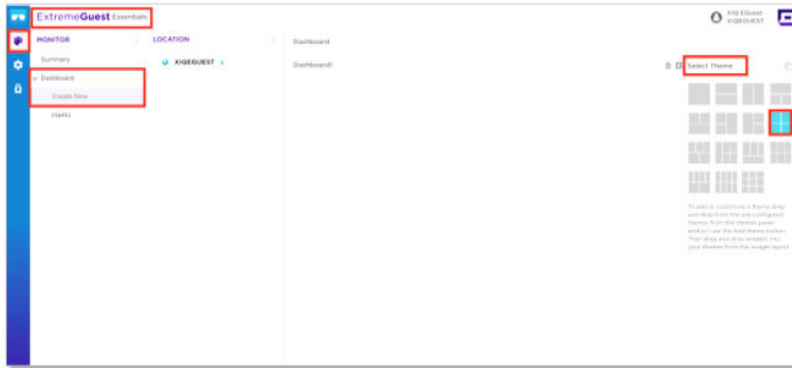
The **Clients** page displays details about client devices registered on the guest wireless network.

Create Custom Dashboards

Perform these steps to create custom dashboards.

1. Create and customize multiple dashboards by selecting a layout.
2. Add widgets from the following categories:
 - Clients
 - Users
 - Usage.

3. Select **Save**.





Troubleshooting: Fixing Error Messages

If you are having issues, carefully review whether you have followed all the steps in the guide. You can also go to the troubleshooting section for guidance, or send an email to the TME team (TME@extremenetworks.com) with as many details as you can.

This table contains troubleshooting steps for specific error messages:

Table 8: Troubleshooting Table


Error Messages	Troubleshooting Steps
<p>No login page or guest redirection failure</p>	<p>When a wireless client connects to the guest service set identifier (SSID), a browser pop up window opens and the browser is redirected to the login page. If the page displays an error:</p> <ul style="list-style-type: none"> • Review your process to ensure you followed the correct instructions to create the splash page • Ensure that the splash page is assigned to the correct location and guest SSID.
<p>Login page does not display all the time</p>	<p>If the client is connecting to a new SSID, the access point (AP) performs a new authentication sequence. But if you try to connect the client to the same guest SSID again after a previous successful session, then the AP does not prompt re-authentication until the client has completed the session timeout or the idle timeout. Perform these steps to clear the AP cache:</p> <ol style="list-style-type: none"> 1. In ExtremeCloud IQ, select  2. Select Clients. 3. Check the media access control (MAC) address of the wireless client. 4. Go to Devices. 5. Access the advanced command line interface (CLI). 6. Select the access point. 7. Select Actions AdvancedCLI Access 8. To clear the access point cache, run these commands one by one: <pre data-bbox="883 1352 1446 1535">clear auth station mac 001325b161f1 clear auth local-cache mac 001325b161f1 clear auth roaming-cache mac 001325b161f1 clear auth roaming-cache hive-neighbors</pre> <p>Note: Replace the MAC address in the command (001325b161f1) with the actual mac address of the wireless device.</p> <ol style="list-style-type: none"> 9. Reconnect the client to the wireless network.
<p>The login page displays an error after entering all the details</p>	<p>If you get the login page, but do not get a welcome page or an error displays after</p>

Table 8: Troubleshooting Table (continued)

Error Messages	Troubleshooting Steps
	<p>entering details, onboarding rules are not properly defined.</p> <ul style="list-style-type: none"> • Check the onboarding configuration rules to ensure there is a matching onboarding policy for the guest SSID and the location • Ensure that you defined onboarding policy rules in a way that reflect the desired workflow.



Guest Essentials Terms & Conditions of Use

Extreme Networks Inc. reserves all rights to its materials and the content of the materials. No material provided by Extreme Networks Inc. to a Partner (or Customer, etc.) can be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or by any information storage or retrieval system, or incorporated into any other published work, except for internal use by the Partner and except as can be expressly permitted in writing by Extreme Networks Inc.

This document and the information contained herein are intended solely for informational use. Extreme Networks Inc. makes no representations or warranties of any kind, whether expressed or implied, with respect to this information and assumes no responsibility for its accuracy or completeness.

Extreme Networks Inc. hereby disclaims all liability and warranty for any information contained herein and all the material and information herein exists to be used only on an "as is" basis. More specific information can be available on request. By your review and/or use of the information contained herein, you expressly release Extreme from any and all liability related in any way to this information. A copy of the text of this section is an uncontrolled copy, and can lack important information or contain factual errors. All information herein is Copyright ©Extreme Networks, Inc. All rights reserved. All information contain in this document is subject to change without notice.

For more information see: <https://www.extremenetworks.com/about-extreme-networks/company/legal/terms-of-use>