ExtremeGuest Essentials Setup Guide

ExtremeCloud IQ Essentials Documentation

Published: March 2022

Part number: 9037476-00

Extreme Networks, Inc.

Phone / +1 408.579.2800

Toll-free / +1 888.257.3000

www.extremenetworks.com

Contents

Table of Figures

Introduction to ExtremeGuest Essentials

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

It includes a customizable Dashboard that provides a holistic view of user data at the entity level or for individual sites. You can use the dashboard graphs and themes to create customized dashboards providing a comprehensive overview of user trends and engagement.

ExtremeGuest Essentials utilizes social networking behavior to increase patronage, expand brand exposure, and understand client demographics and preferences in a more comprehensive and personal way. Guest onboarding with sponsor approval is supported, allowing a sponsor to approve or deny guest access with a single click.

Use ExtremeGuest Essentials to configure and implement user notification policies and rules to specify the method used for all types of communication with guest user, such as communicating the passcode to newly registered guest users or sending a report to specified guest users.

Onboarding policies are used by ExtremeGuest Essentials to give flexibility when determining hotspot user access. Policies are matched to the hotspot user based on onboarding rules. Then the matching policy with the highest precedence number is used to onboard the hotspot user. An onboarding policy consists of one or more match criteria that are used to filter guests and apply an action..

ExtremeGuest Essentials includes a summary of captive portal splash templates. These splash templates are either customized-system templates or user-defined templates. The System Templates tab displays a summary of available captive portal splash screen templates, which you can use to download a system template and customize it to suit your requirements, clone a system template, or view a summary of networks to splash templates mapping.

The User Templates provide a robust, easy-to-use splash template builder wizard. Use the wizard's 'drag & drop' elements, color, text, and language customization tools and logo upload options to create your branded captive portal web pages, as well as the addition of photos and video.

You can analyze client and online user details at the site level. You can access a summary of all client status, as well as detailed information for each client. Drill down to the site level to view online and blocked user details for a specific site.

Initial Setup for ExtremeGuest Essentials

To set up ExtremeGuest Essentials, you will create a network policy, onboard a device, and launch the ExtremeGuest Essentials app. Follow these steps:

1. Log into ExtremeCloud IQ.

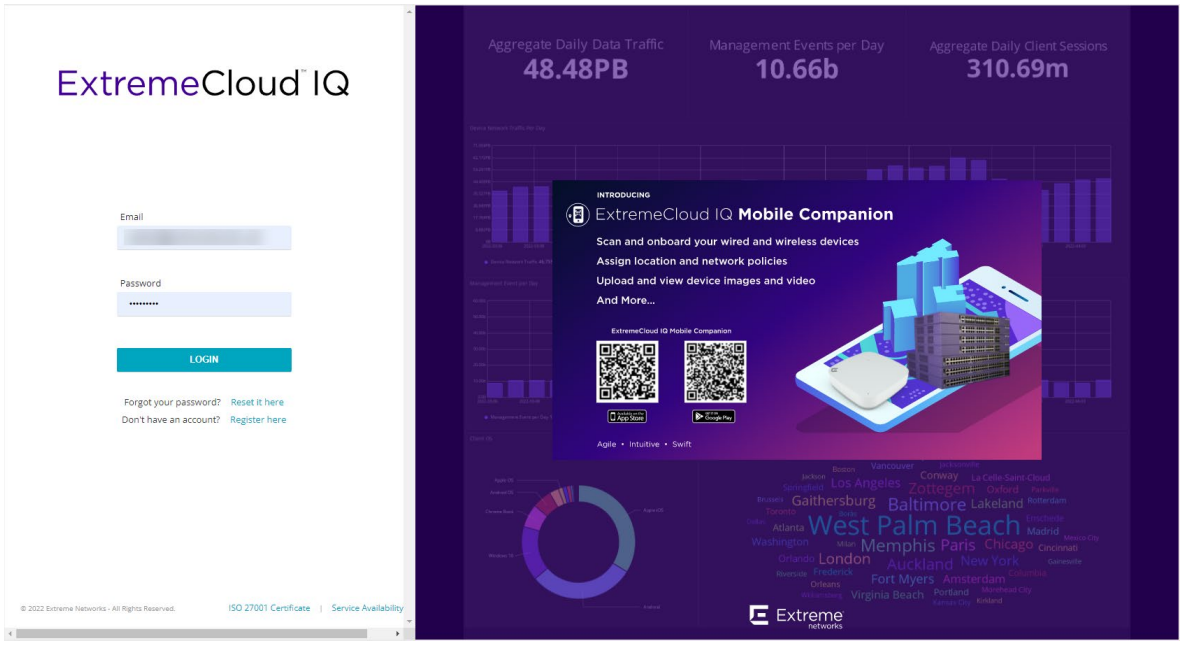


Figure 1: Login Screen

2. Set up the Network Policies:

   a. Select **Configure** > **Network Policies** > **ADD NETWORK POLICY**

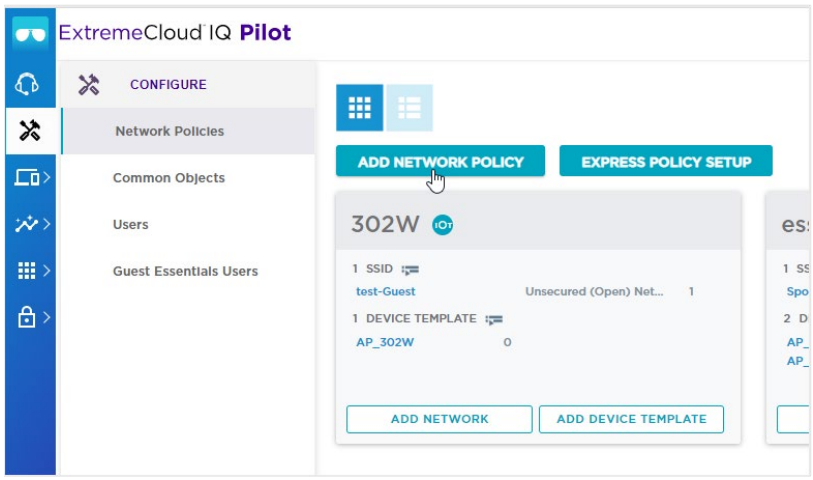


Figure 2: Add Network Policy

   b. Enter a **Policy Name**

   c. Select **Save**

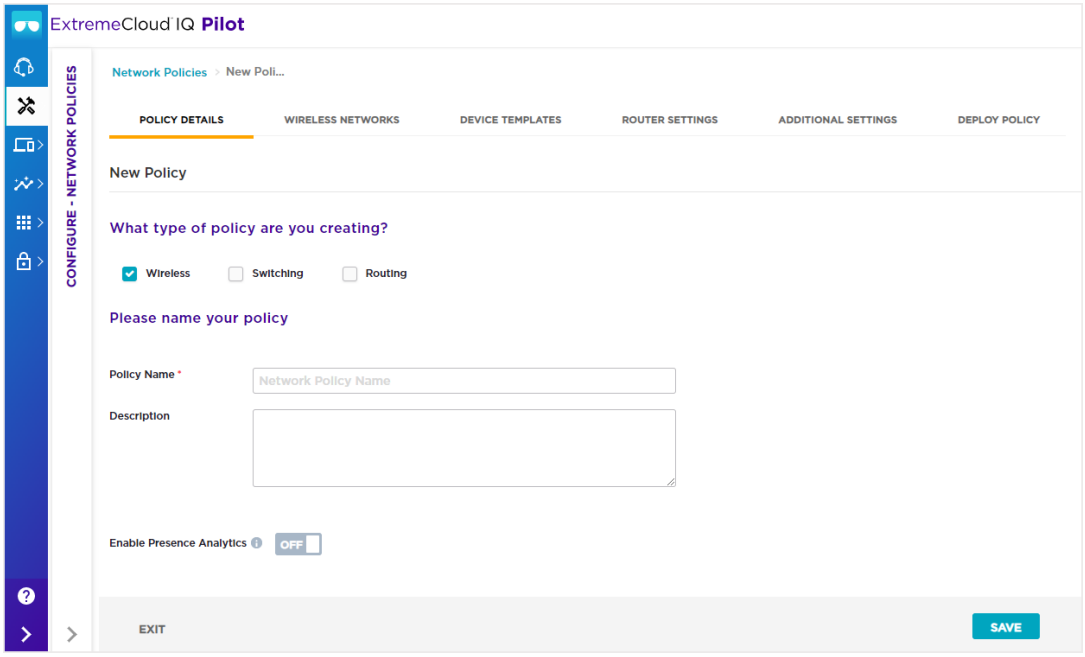


Figure 3: Policy Details

3. Set up the Wireless Networks:

   a. Select the **WIRELESS NETWORKS** tab

   b. Select the **+** icon

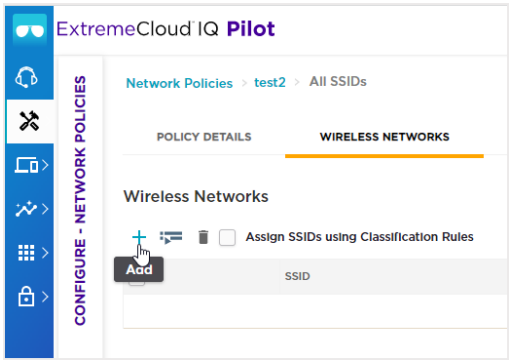


Figure 4: Add Wireless Networks

   c. Enter a **Name (SSID)**

   d. Enter a **Broadcast Name**

   e. Under **SSID Authentication**, select **Open**

   f. (*Optional*) Assign a **VLAN**

   g. Select **SAVE**

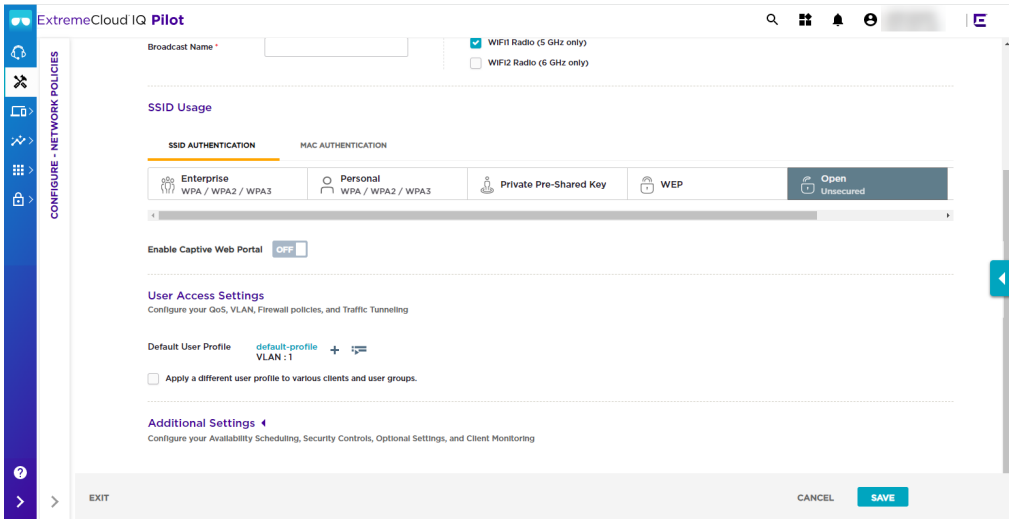


Figure 5: Wireless configuration

4. Add the corresponding device templates:

   a. Select the **DEVICES TEMPLATES** tab (See Figure 3: Policy Details for the location of the Device Templates tab)

   b. Select the ➕ icon and a device from the list

   c. Give the template a name

   d. Under the **Wifi0** and **Wifi1** tabs, select as **Client Access** mode.

   e. Select **SAVE TEMPLATE**

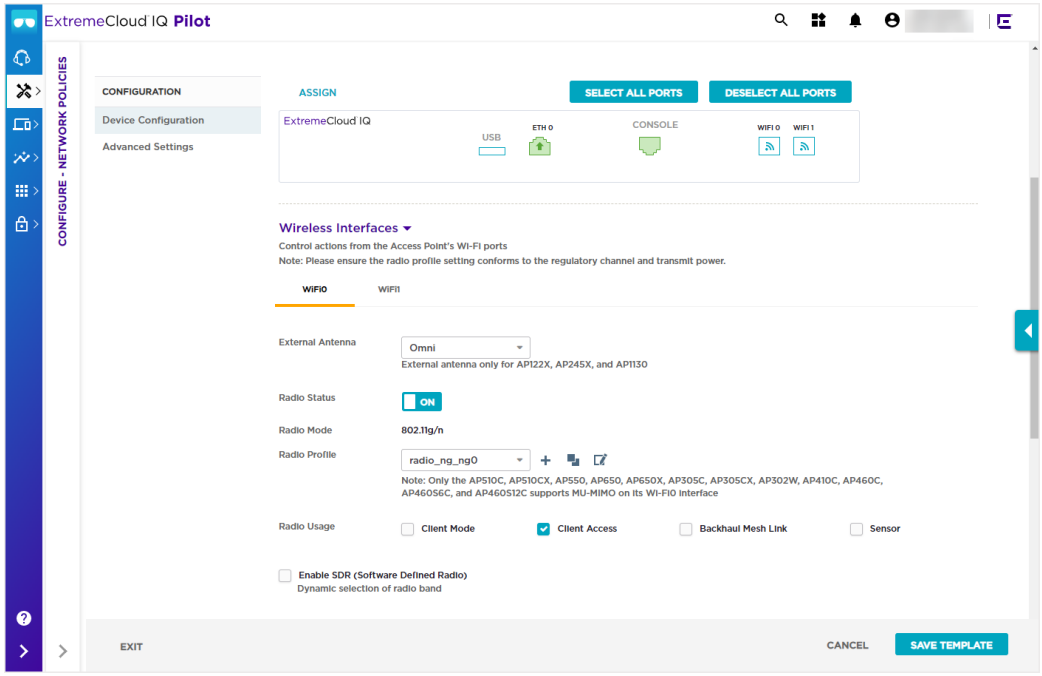


Figure 6: Device Templates configuration

5. Onboard a device:
    a. Select **Manage > Devices**
    b. Select **+ > Advanced Onboarding**
    c. Select either **Deploy your devices to the cloud** or **Deploy your devices locally**
    d. Select **Let's Get Started!**
    e. Refer to the online Onbording Getting Started Guide for the complete onboarding procedure.

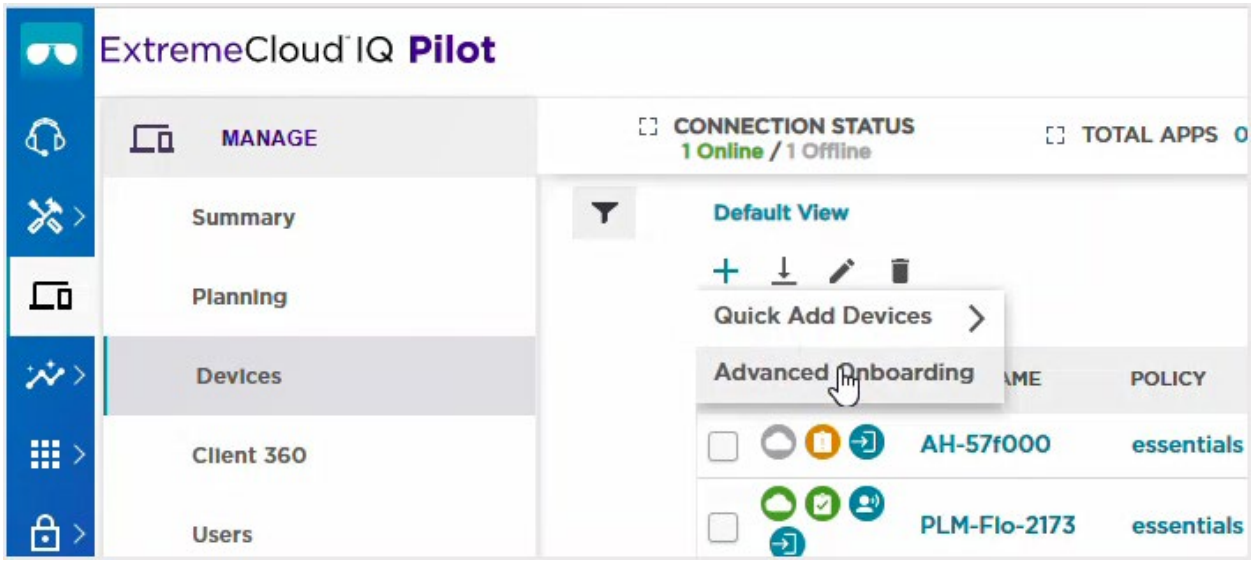


Figure 7: Device onboarding

6. When the device is reported online in ExtremeCloud IQ, assign the location and the network policy you created in step 2 on page 4.

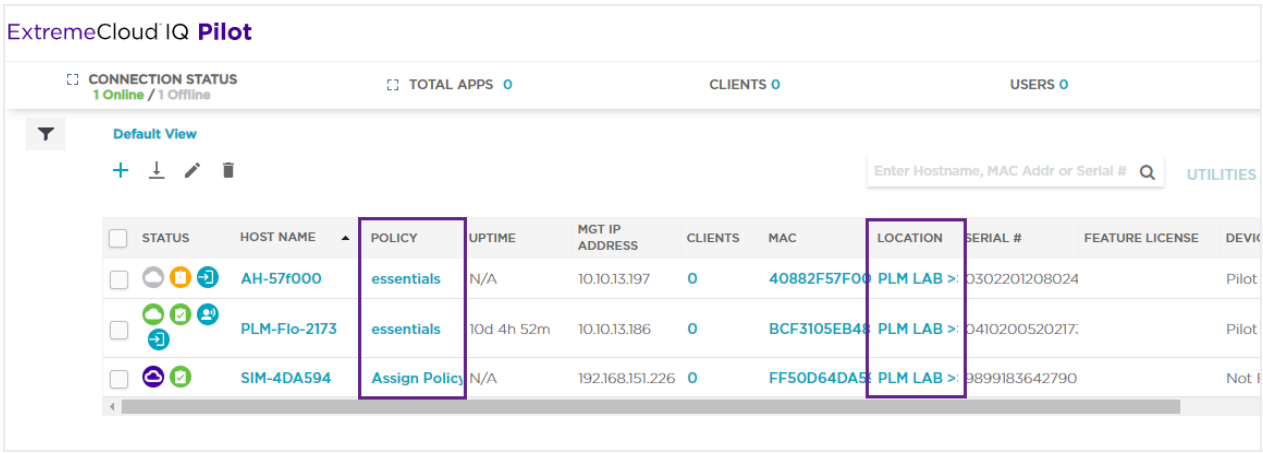


Figure 8: Policy name and location

7. After the *very first* onboarding and assignment of the network policy, perform a complete CONFIG PUSH on the onboarded AP.

    a. Select a device or devices.

    b. Select **UPDATE DEVICES**

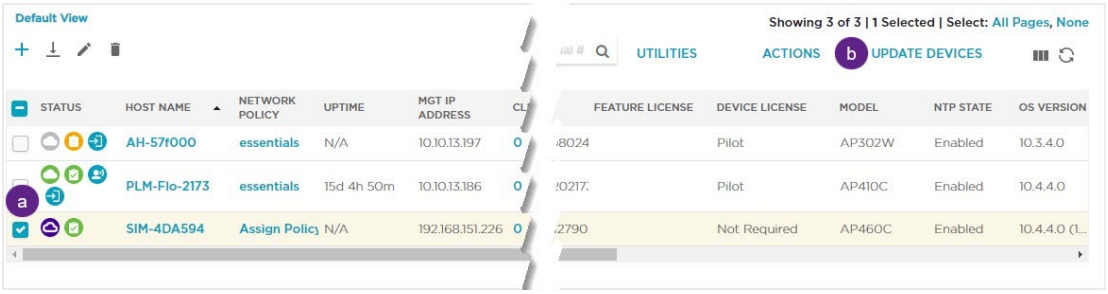


Figure 9: Update Devices

    c. Select **Update Network Policy and Configuration** and then **Complete Configuration Update**

    d. Select **PERFORM UPDATE**

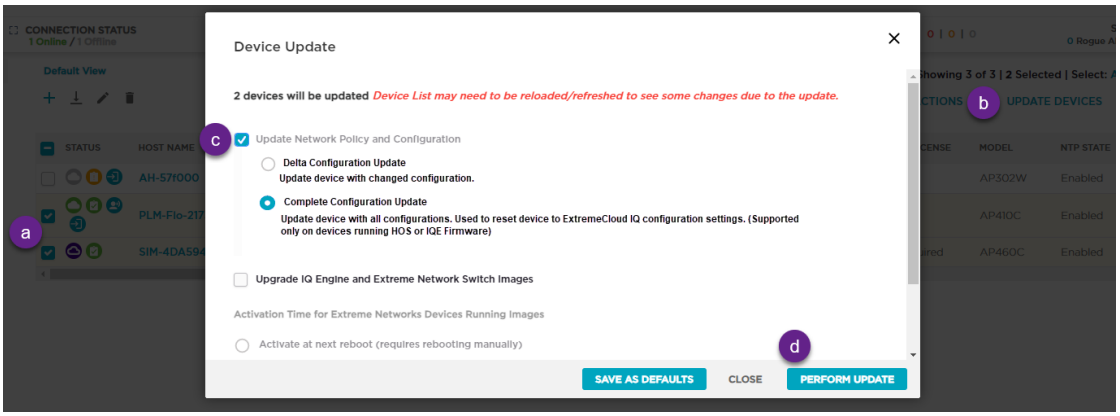


Figure 10: Update Network Policy and Configuration

8. Launch ExtremeGuest Essentials:

    a. Select **Essentials > Extreme Guest**

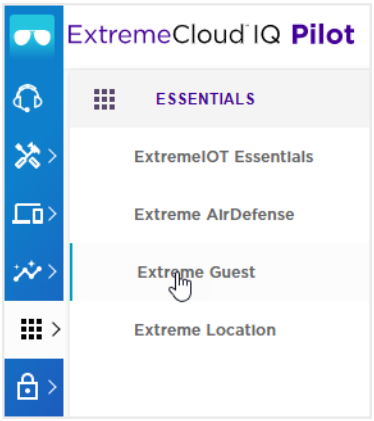


Figure 11: Select Extreme Guest

    b. Select **Enable**

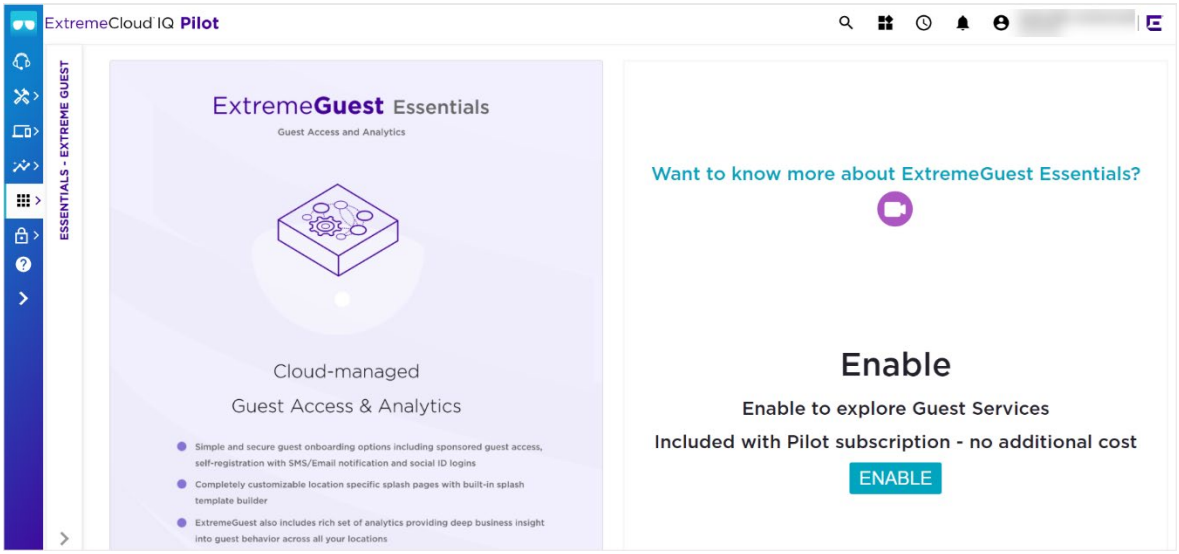


Figure 12: Enable ExtremeGuest Essentials

9. Select the open wireless network you created and select apply (see step 3 on page 5).

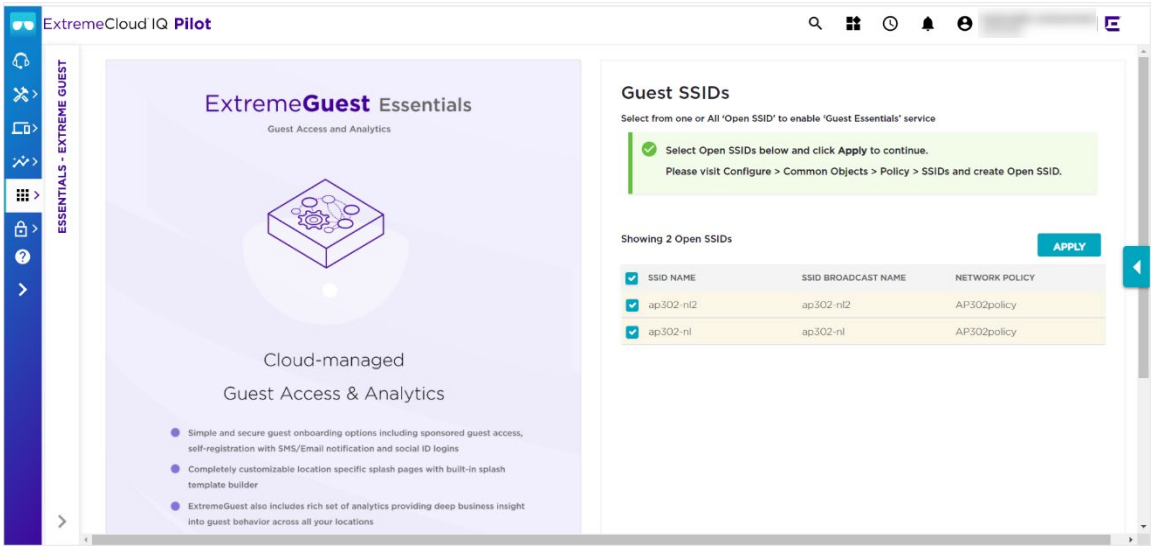


Figure 13: Select wireless network

As devices start to use the WLAN, the ExtremeGuest Essentials Summary screen begins to load data and display analytics.

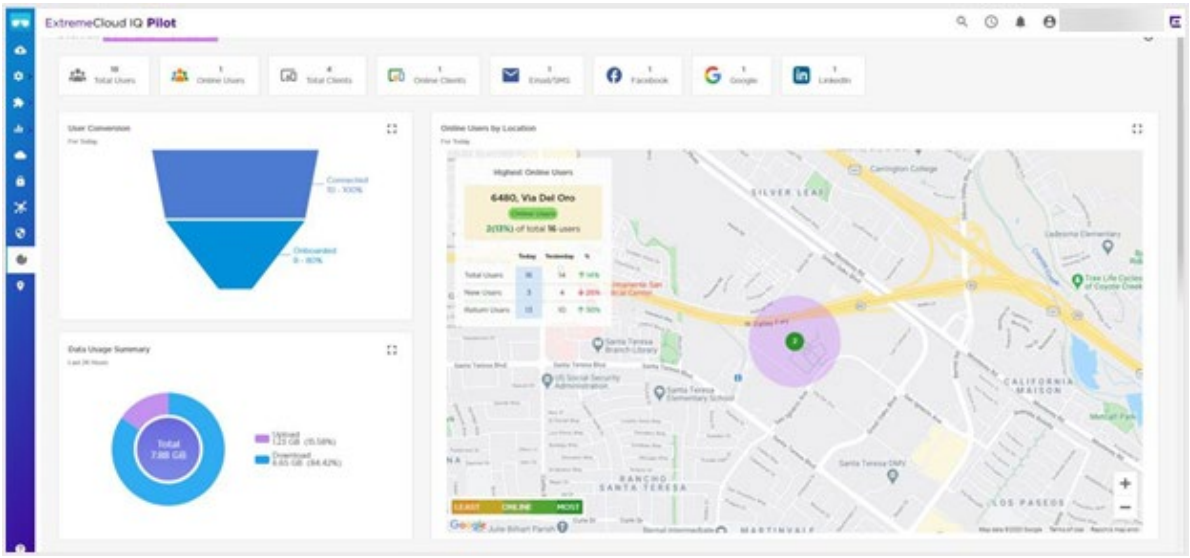


Figure 14: Guest Essentials Summary

You can view additional details by selecting More Insights.

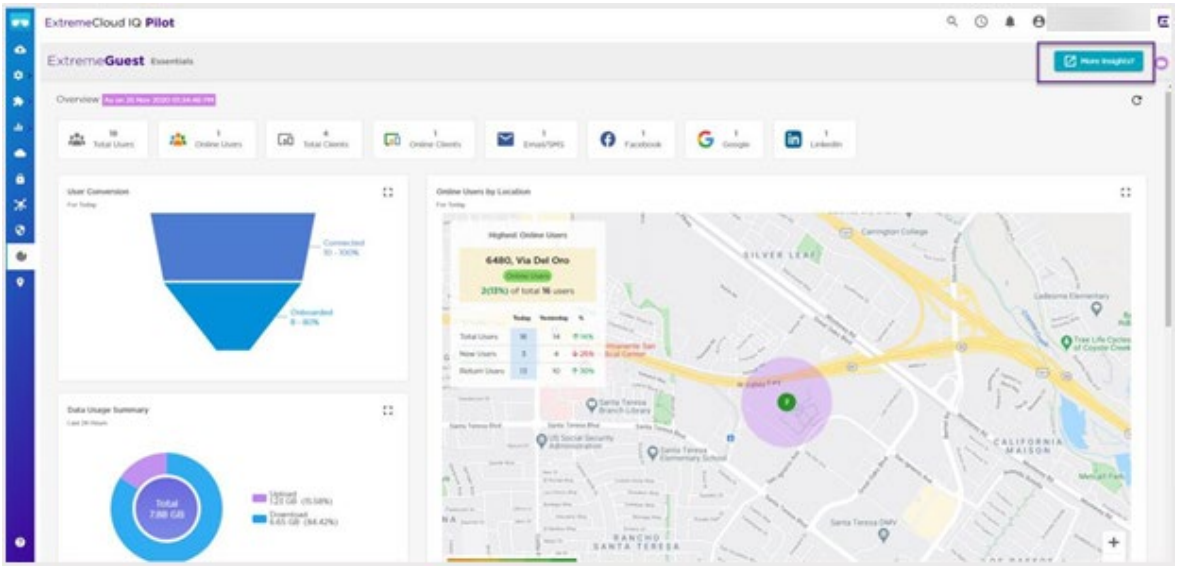


Figure 15: More Insights

On the More Insights page, you can configure additional dashboards and advanced configurations as shown is Figure 16: Additional dashboards and advanced configurations.

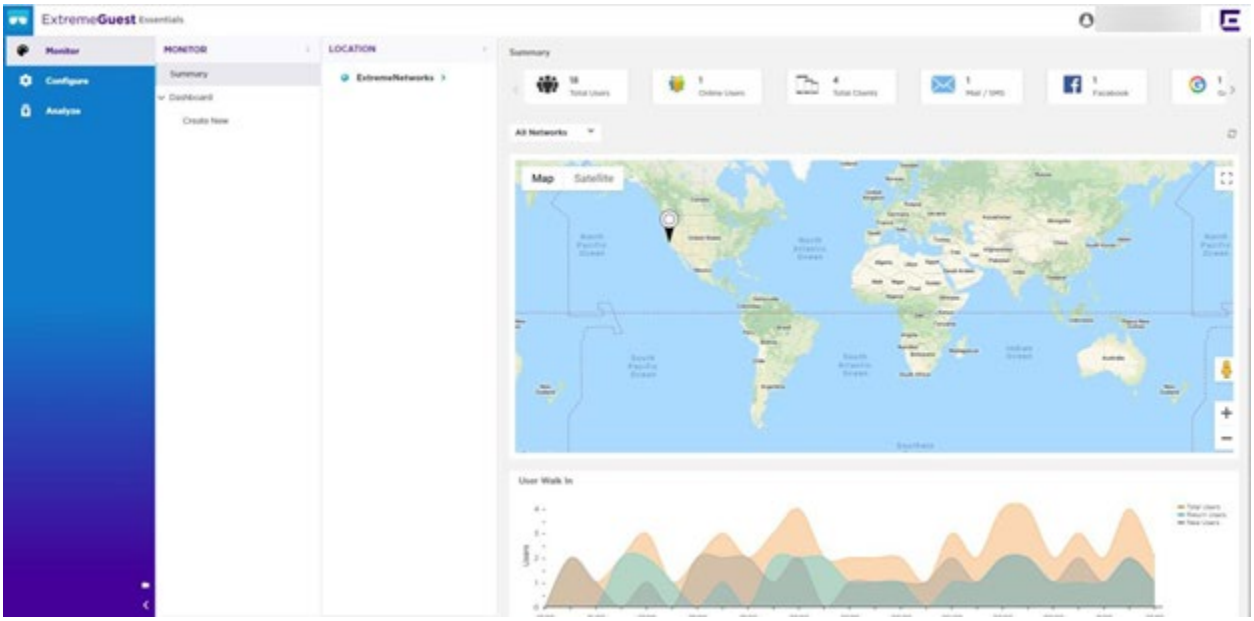
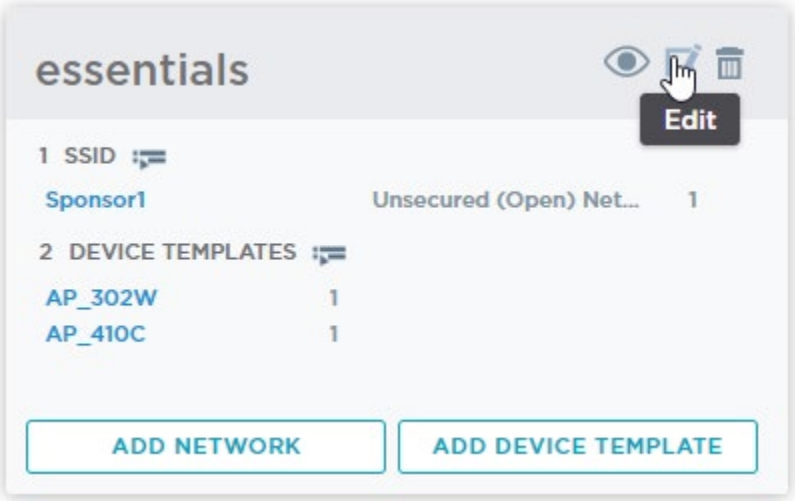


Figure 16: Additional dashboards and advanced configurations

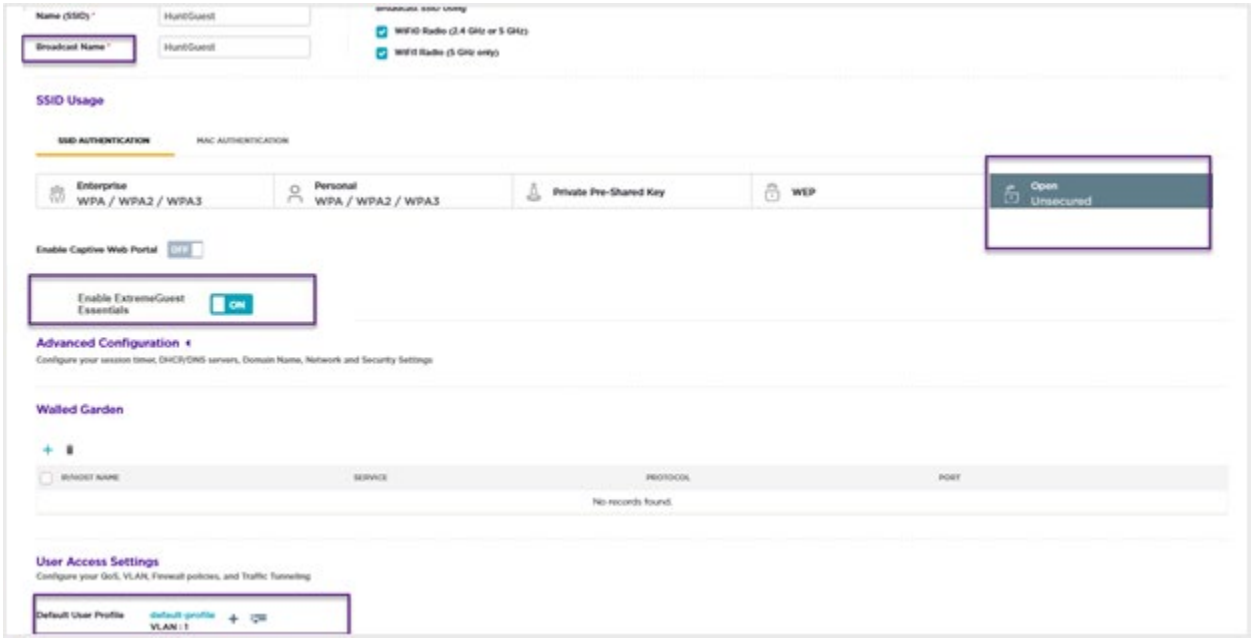
Test a Simple Accept and Connect

The following steps take you through the process of testing a simple accept and connect operation.

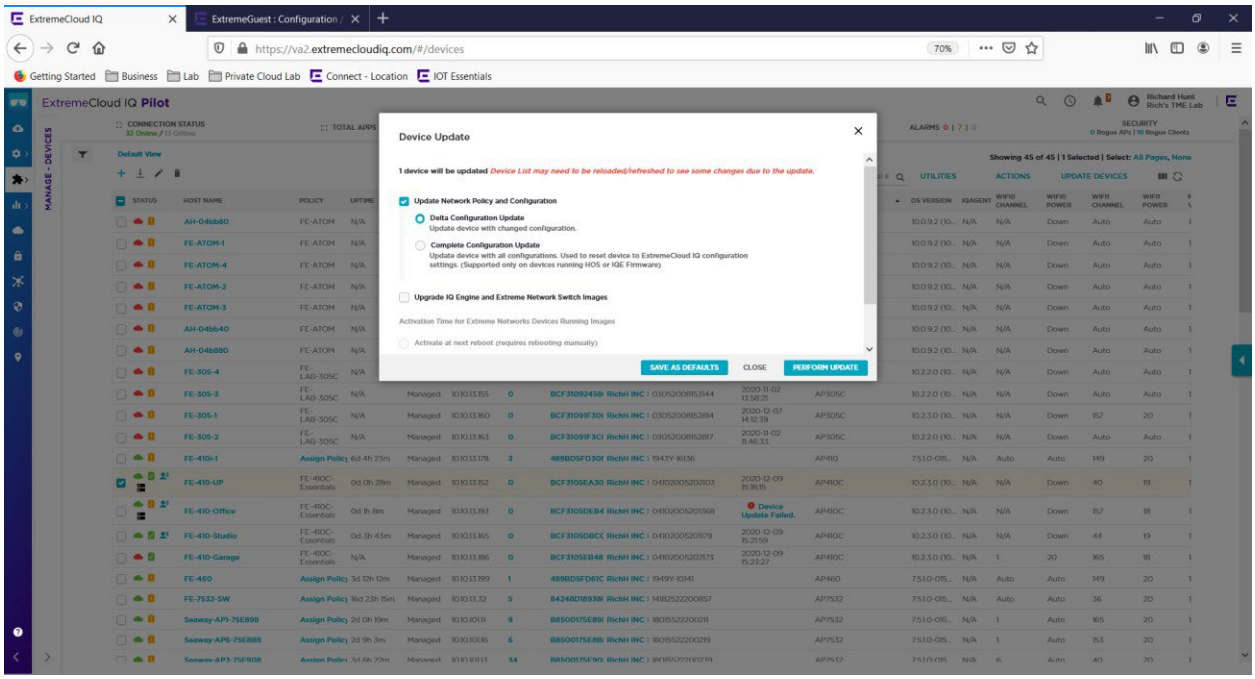
1. Configure the Network Policy.
    a. Open **Network Policies**
    b. Edit the existing policy (see step 2 on page 4 to locate your policy)
    a. Select its edit icon.



    b. Follow steps 3a - 3d on page 5 and create an open WLAN
    c. Select **Enable ExtremeGuest Essentials**
    d. (*Optional*) Select a **VLAN**
    e. Select **Save**



2. Push the configuration to the AP. To do this, follow the procedures in step 7 on page 8 but replace step c with **Delta Configuration Update**



3. To onboard guest devices:

   a. Select **More Insights > Configure > Onboarding > Policy**

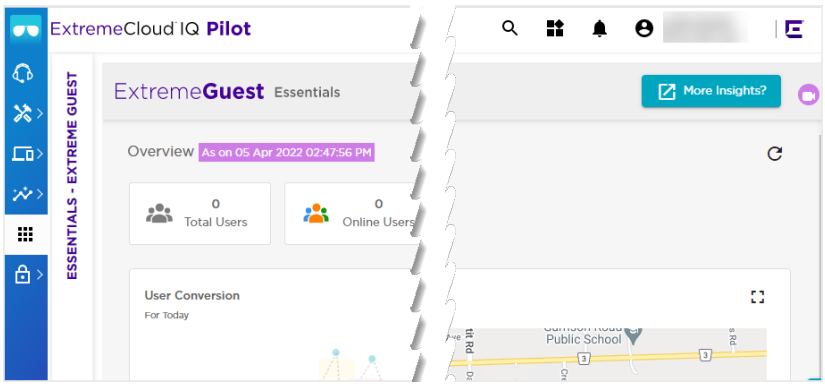


Figure 17: More Insights

b. Select + icon to onboard guest devices

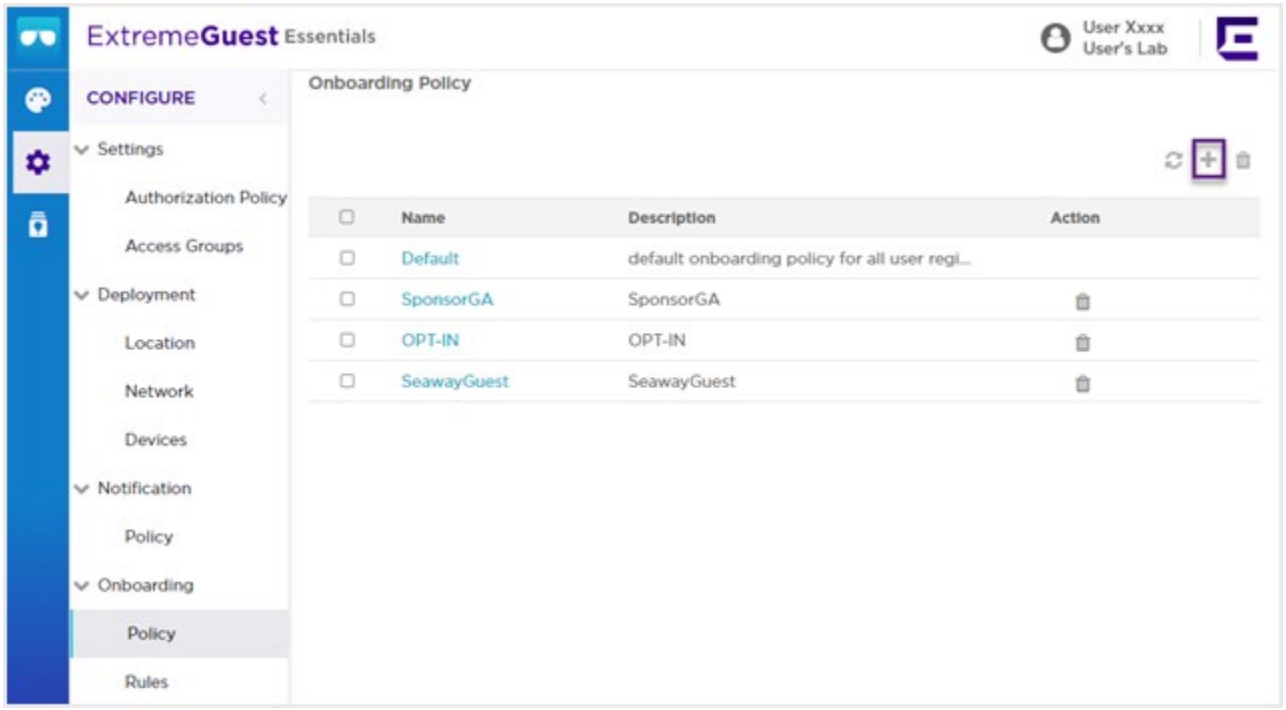


Figure 18: Policy Onboarding

4. Add an **Onboarding Policy** (see Figure 18: Policy Onboarding to find the Policy screen):
    a. Select ➕ icon
    b. Enter a **Policy Name**
    c. Enter the **Criteria #1** parameters:
        i. For **Conditions**, select **Any**
        ii. For **Action**, select **Register Client**
        iii. For **Validity and Group**, enter **days, hours, or mins for which the registered client is valid**
        iv. For **Select a group**, select **GuestAccess**
    b. Select **Save**

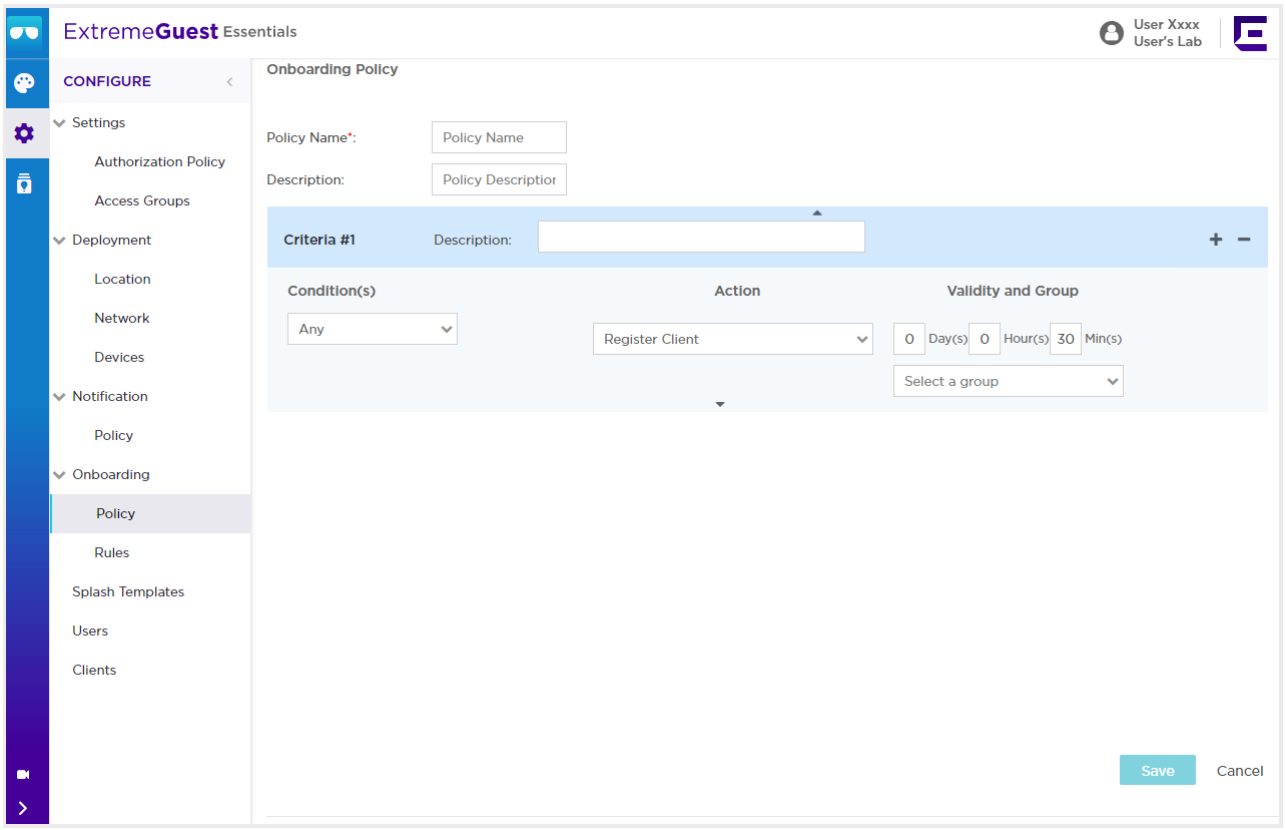


Figure 19: Create Onboarding Policy

5. Add a rule (see Figure 18: Policy Onboarding to find the Rules screen):

    d. Select ➕ icon

    e. Enter a **Rule Name**

    f. Select a **Policy**

    g. Select a WLAN **Network**

    h. Select a **Location**

    i. Select a **Precedence Level**

    The Precedence Level determines the priority of a rule. The lower the value, the higher the priority. Rules with lower precendence will be applied first. The level ranges from 1 to 100.

    j. Select **Save**

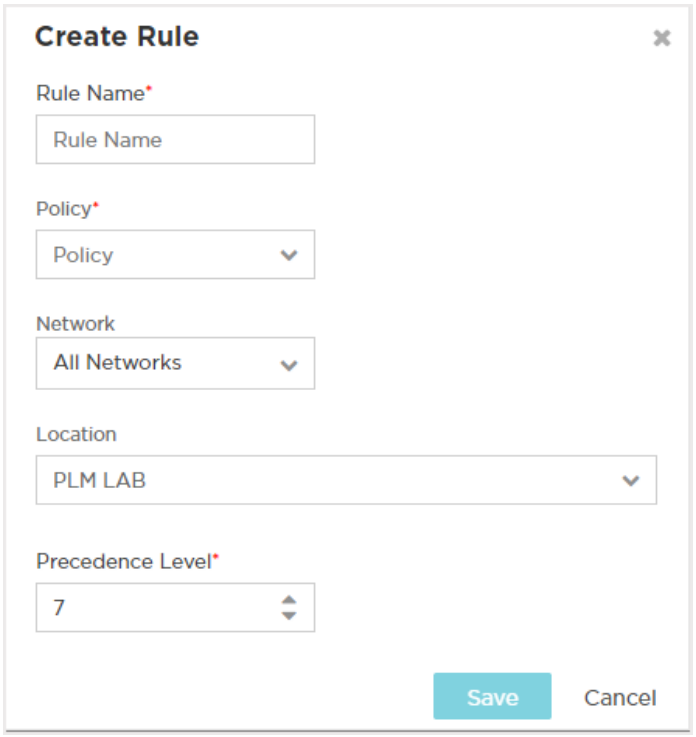


Figure 20:Create Rule

6. Configure the **Splash Template**:
    a. Select **Accept_and_Connect** under the **System Templates** tab
    b. Select the clone icon

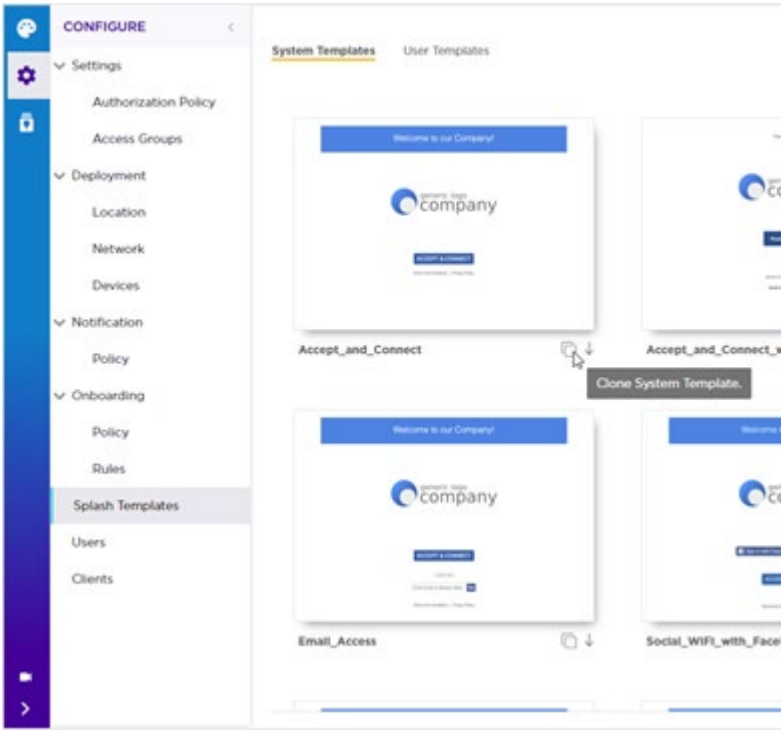


Figure 21: Splash Template

    c. Customize the Splash Template
        i. Drag and drop the layouts into the template
        ii. Complete each layout

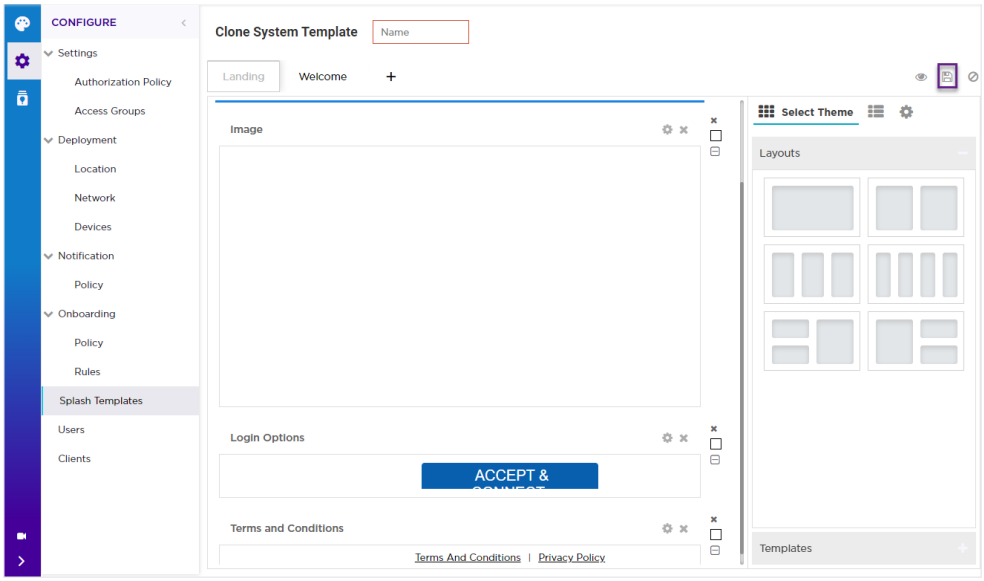


Figure 22: Template configuration

d. Select the save icon

10. Configure **User Templates**:

a. Select the **User Templates** tab

b. Select the add + icon

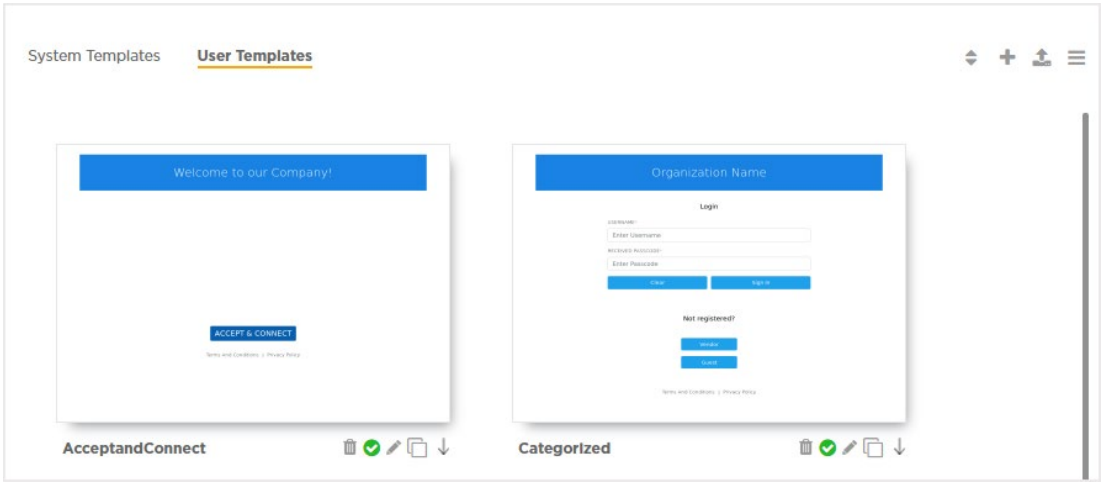


Figure 23: User Templates

c. Customize the template

   i. Drag and drop the layouts into the template

   ii. Complete each layout

d. Select the check mark your new template to distribute the splash page to the network

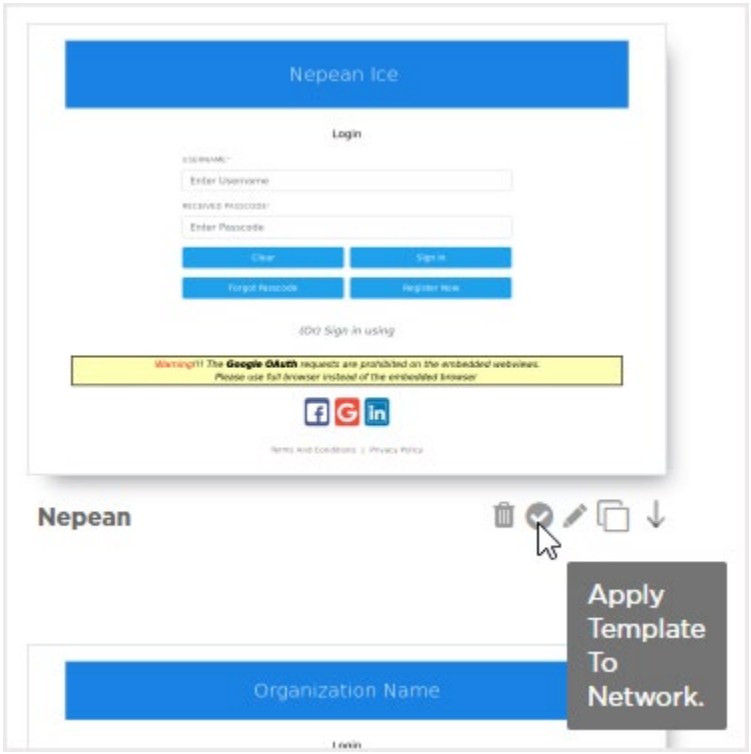


Figure 24:Customize User Templates

e. Select a Location

f. Select a Network

g. Select Add

h. Select Apply

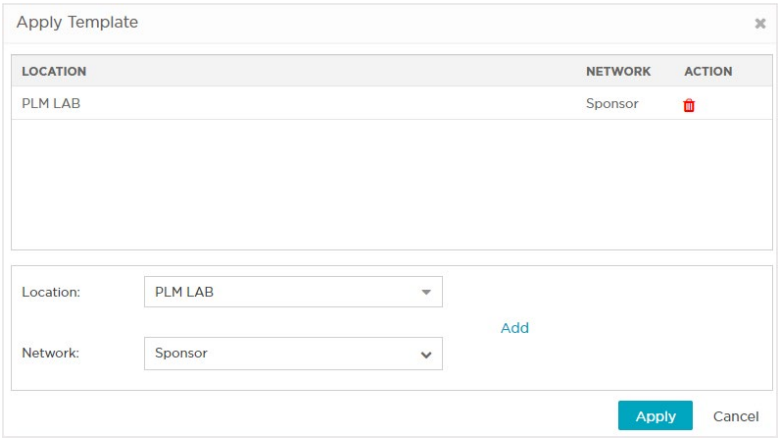


Figure 25: Apply Template

The operation is complete. You can test the splash page setup with a device.

Using HTTPS with ExtremeGuest Essentials

Browser updates are causing security exceptions when the user submits their login credentials. This occurs because they are using HTTP in an HTTPS connection. The following procedure is an option if you want to prevent security exceptions. The procedure requires a domain certificate that is pushed to the Access Points (AP) through ExtremeCloud IQ, adding a dummy record in your Domain Name Server (DNS) file for the webserver Fully Qualified Doman Name (FQDN).

How to use HTTPS

1. Obtain a certificate. You can use your company's wildcard domain certificate. If you do not have one, you will have to purchase one from a well-known Certificate Authority (CA) provider.

   There are two different certificate formats that can be used:

   e. A wildcard certificate where the Common Name (CN) is a wildcard domain.

      *.*domain*.com à CN=`*.iqe-ext.com`

   f. A certificate with CN as a dummy hostname, for example *guest* or *eguest*.

      hostname.domain.com à CN=`guest.iqe-ext.com` or CN=`eguest.iqe-ext.com`

2. Map the hostname to an IP address
   a. On the DNS server serving the wireless guest clients, create an "A" record
   b. Map the hostname to a private unused IP address. For example:

      ```
      guest.iqe-ext.com  300 IN A 192.168.14.1
      ```

      NOTE: IP mapping can be to any private unassigned address. The IP address is a placeholder.

   c. Verify the FQDN resolves using `nslookup`.
   d. Verify that the wireless clients connecting to the guest SSIDs are pointed to the DNS.

      NOTE: The same FQDN *hostname.domain*.com used as the CN needs to be specified as a webserver name in the Wireless Local Area Network (WLAN).

3. Import the certificate and corresponding private key into ExtremeCloud IQ.
   a. Log into ExtremeCloud IQ.
   b. Select Configure > Common Objects > Certificate > Certificate Management
   c. Select the import icon

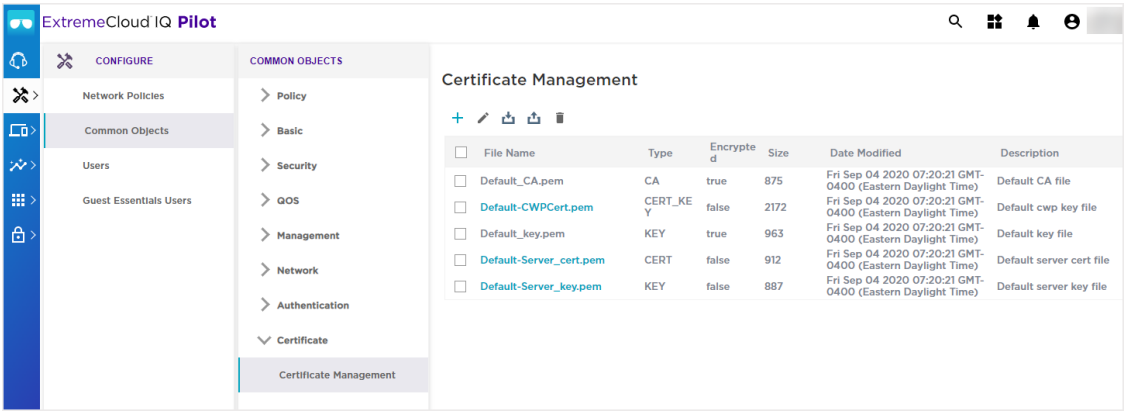


Figure 26: Certificate Management

4. Import the Certificate and Certificate Key files
    a. Choose **SELECT**
    b. Select the certificate file or certificate key file
    c. For **File Type**, select **CERT** or **CERT_KEY**
    d. (*Optional*) Select one or both options for **Certificate Conversion Options**
    e. Select **SAVE**
    f. Repeat these steps for **CERT_KEY**

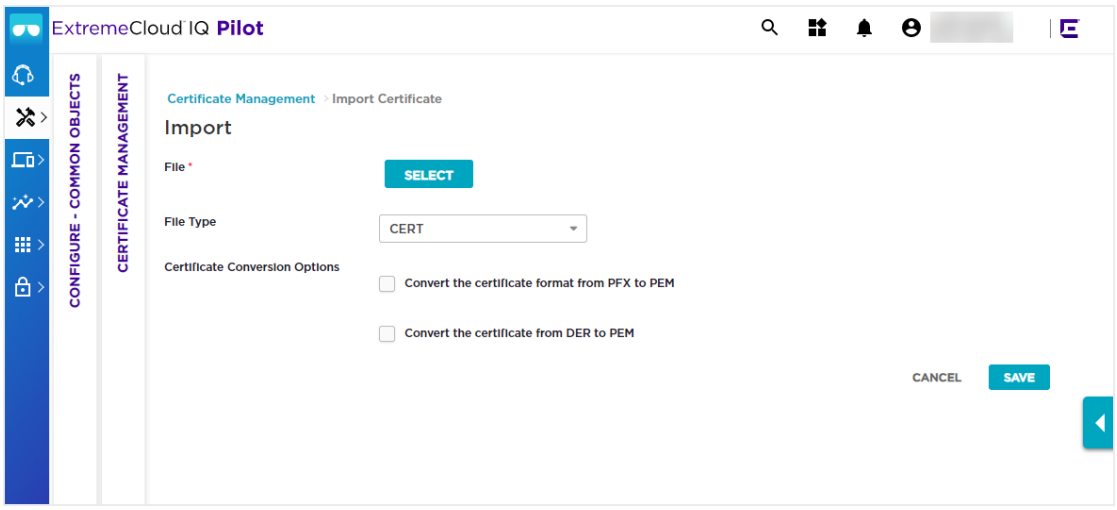
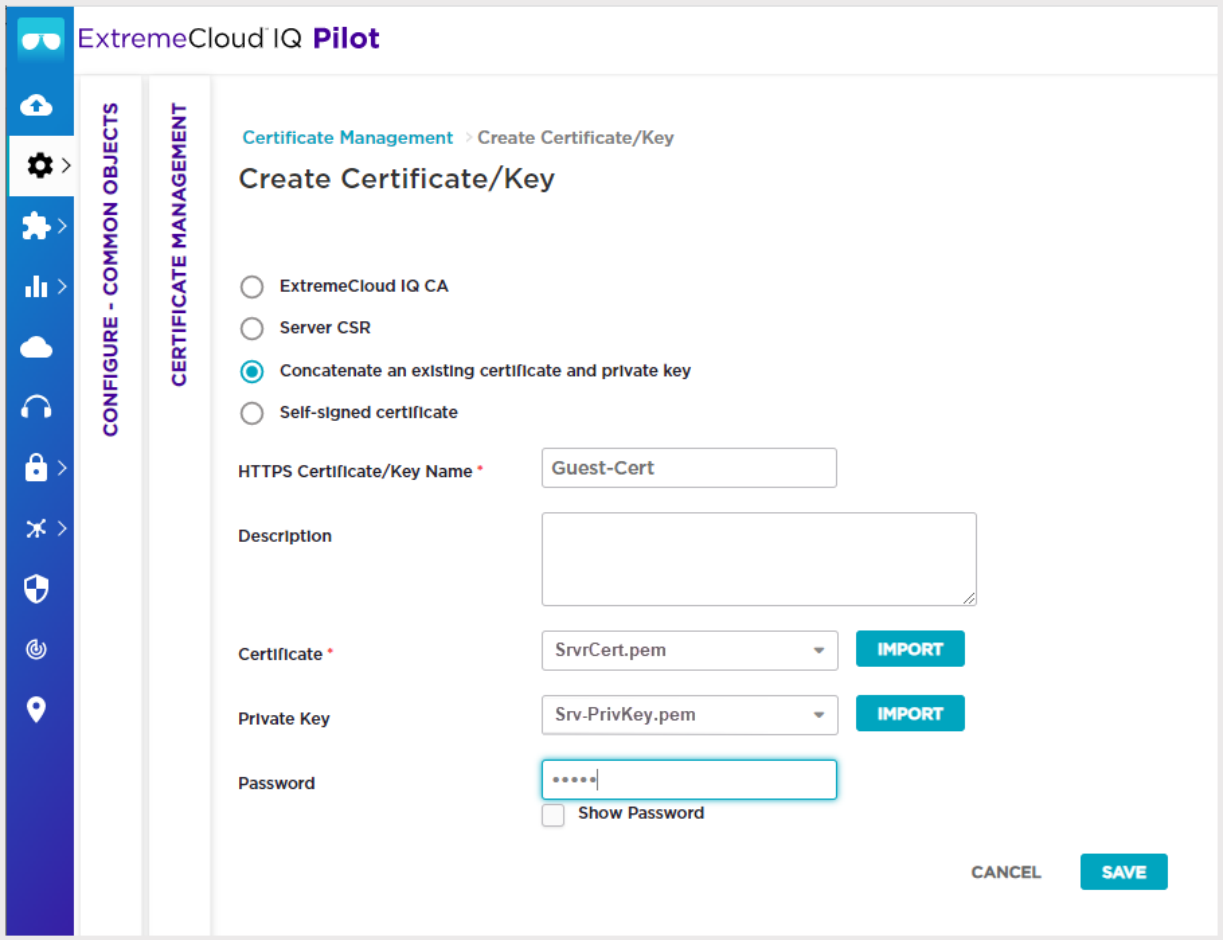


Figure 27: Certificate Management import

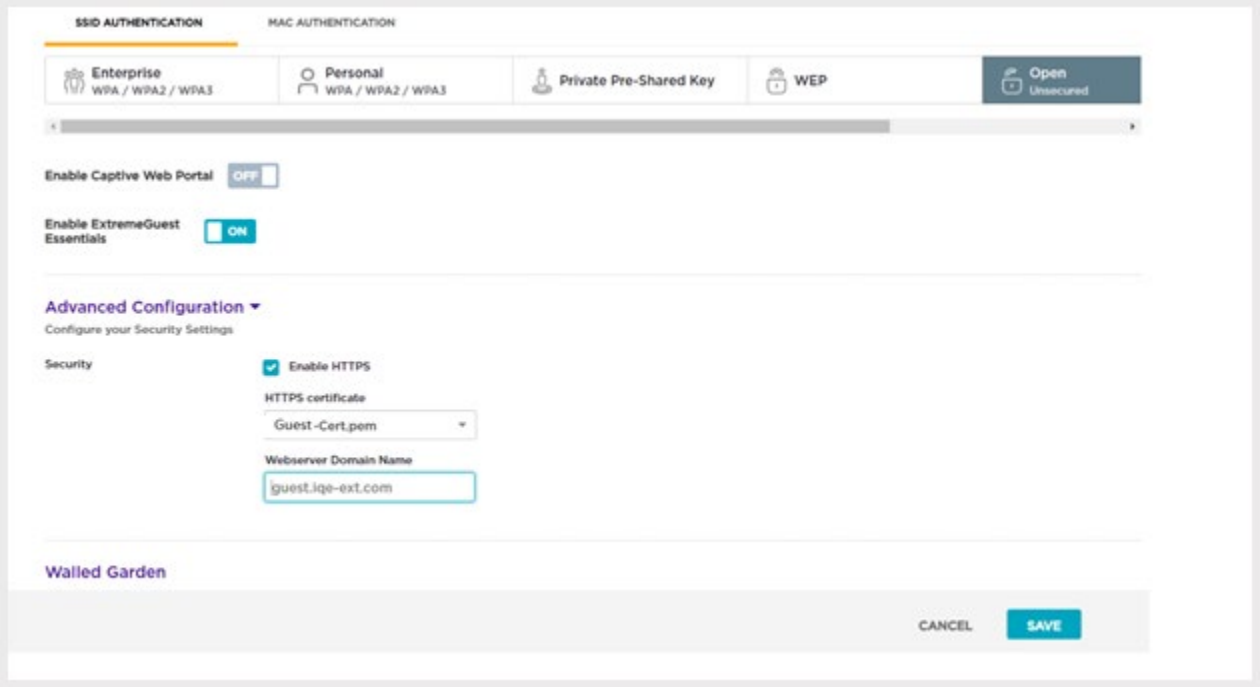
5. Concatenate the certificate and private key
    a. Select **Configure > Common Objects > Certificate > Certificate Management**
    b. Select the add icon (see + in Figure 26: Certificate Management for the location of the icon)
    c. Select **Concatenate an existing certificate and private key**
    d. Enter an **HTTPS Certificate/Key Name**. This is the name that is displayed when selecting the HTTPS certificate in the WLAN.
    e. For **Certificate**, select the one you supplied.
    f. For **Private Key**, select the private key obtained from the CA.

NOTE: The Private Key file is generated when creating a Certificate Signing Request (CSR). Save the file and upload it here.

g. For **Password**, enter the Private Key password used when the CSR was generated. If a password was not used for the CSR generation, then leave **Password** blank.



6. Create the WLAN
   a. Select **Configure>Network Policies**
   b. Select the **WIRELESS NETWORKS** tab
   c. Right-click the add icon + and select **All Other Networks (standard)**
   d. Enter a **Name (SSID)**
   e. Enter a **Broadcast Name**
   f. Under SSID Usage, select **Open (Unsecured)**
   g. Select **Enable ExtremeGuest Essentials**
   h. Select **Advanced Configuration**
   i. Select **Enable HTTPS** and select the **HTTPS certificate** file you created in step 5 on page 22
   j. Enter the **Webserver Domain Name**. This is the FQDN that was mapped to the customer DNS in step 2 on page 21.
   k. Select **Save**



Continue with the common setup based on the guest use case.