Wi-Fi Cloud

Getting Started Guide

WatchGuard Wi-Fi Cloud

About This Guide

The *WatchGuard Wi-Fi Cloud Getting Started Guide* is a guide to help you with your deployment of a WatchGuard Wi-Fi Cloud appliance. For the most recent product documentation, see the *WatchGuard Wi-Fi Cloud Help* on the WatchGuard website at https://www.watchguard.com/wgrd-help/documentation/overview.

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Guide revised: 8/5/2020

Copyright, Trademark, and Patent Information

Complete copyright, trademark, patent, and licensing information can be found in the Copyright and Licensing Guide, available online at https://www.watchguard.com/wgrd-help/documentation/overview.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, providing best-in-class Unified Threat Management, Next Generation Firewall, secure Wi-Fi, and network intelligence products and services to more than 75,000 customers worldwide. The company's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for Distributed Enterprises and SMBs. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

For additional information, promotions and updates, follow WatchGuard on Twitter, @WatchGuard on Facebook, or on the LinkedIn Company page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at www.secplicity.org.

Address

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

Support

www.watchguard.com/support
U.S. and Canada +877.232.3531
All Other Countries
+1.206.521.3575

Sales

U.S. and Canada +1.800.734.9905
All Other Countries
+1.206.613.0895

Contents

Getting Started with WatchGuard Wi-Fi Cloud

WatchGuard Wi-Fi Cloud is a powerful, cloud-based, enterprise-level wireless management solution that enables you to configure and monitor your WatchGuard APs from anywhere.

To activate and configure your APs with WatchGuard Wi-Fi Cloud, see:

- *Activate Your AP*
- *Connect and Power On the AP*
- *Connect to WatchGuard Wi-Fi Cloud*
- *Set up a Wireless Network with Discover*
- *Enable a Captive Portal for Guest Users*

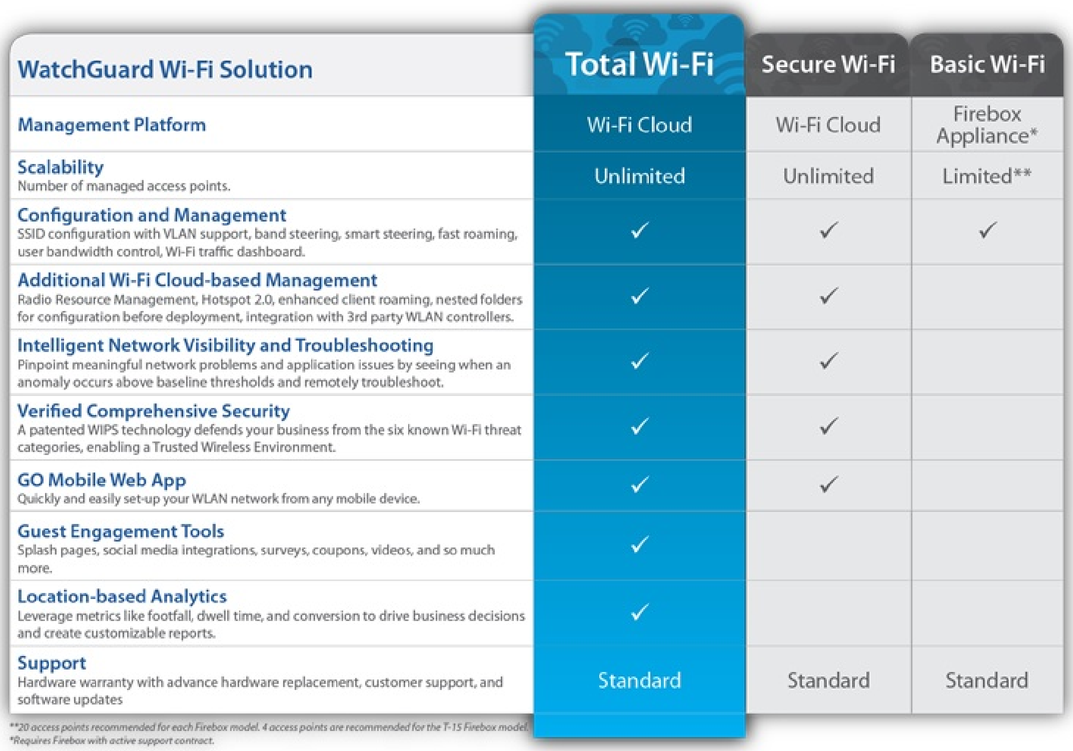
For additional resources, see the Wi-Fi Cloud documentation page on the WatchGuard web site.

For more information about how to use Wi-Fi Cloud WIPS to create a Trusted Wireless Environment, see Create a Trusted Wireless Environment with WIPS.

WatchGuard Wi-Fi Solutions

WatchGuard offers these types of wireless security subscriptions for WatchGuard APs:

- **Basic Wi-Fi** – Use the Gateway Wireless Controller on a WatchGuard Firebox to configure, manage, and monitor WatchGuard APs directly from the Firebox.
- **Secure Wi-Fi** – Use WatchGuard Wi-Fi Cloud for WatchGuard AP management, security, and monitoring.
- **Total Wi-Fi** – Use WatchGuard Wi-Fi Cloud for WatchGuard AP management, security, and monitoring. Provides additional tools for guest user engagement, analytics, social media integration, captive portals, and splash page design.



WatchGuard Wi-Fi Solution	Total Wi-Fi	Secure Wi-Fi	Basic Wi-Fi
Management Platform	Wi-Fi Cloud	Wi-Fi Cloud	Firebox Appliance*
Scalability Number of managed access points.	Unlimited	Unlimited	Limited**
Configuration and Management SSID configuration with VLAN support, band steering, smart steering, fast roaming, user bandwidth control, Wi-Fi traffic dashboard.	✓	✓	✓
Additional Wi-Fi Cloud-based Management Radio Resource Management, Hotspot 2.0, enhanced client roaming, nested folders for configuration before deployment, integration with 3rd party WLAN controllers.	✓	✓	
Intelligent Network Visibility and Troubleshooting Pinpoint meaningful network problems and application issues by seeing when an anomaly occurs above baseline thresholds and remotely troubleshoot.	✓	✓	
Verified Comprehensive Security A patented WIPS technology defends your business from the six known Wi-Fi threat categories, enabling a Trusted Wireless Environment.	✓	✓	
GO Mobile Web App Quickly and easily set-up your WLAN network from any mobile device.	✓	✓	
Guest Engagement Tools Splash pages, social media integrations, surveys, coupons, videos, and so much more.	✓		
Location-based Analytics Leverage metrics like footfall, dwell time, and conversion to drive business decisions and create customizable reports.	✓		
Support Hardware warranty with advance hardware replacement, customer support, and software updates	Standard	Standard	Standard

***20 access points recommended for each Firebox model. 4 access points are recommended for the T-15 Firebox model.*
**Requires Firebox with active support contract.*

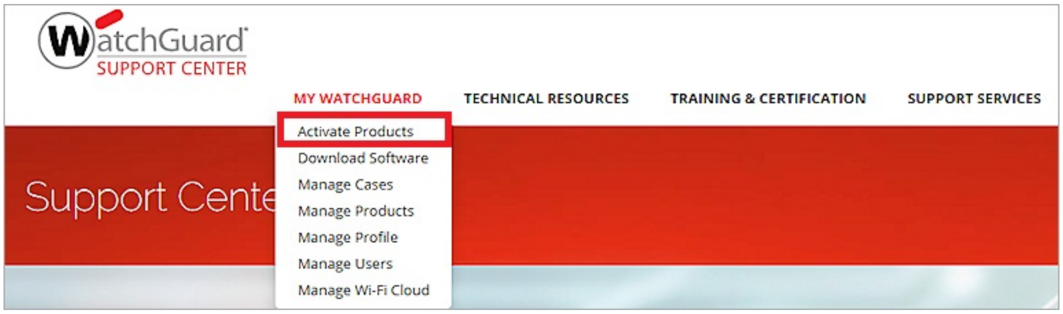
Activate Your AP

Before you can manage and monitor your AP with WatchGuard Wi-Fi Cloud, you must activate the AP. When you activate your AP, you also enable your hardware replacement warranty, receive technical support, and get access to the latest AP firmware updates.

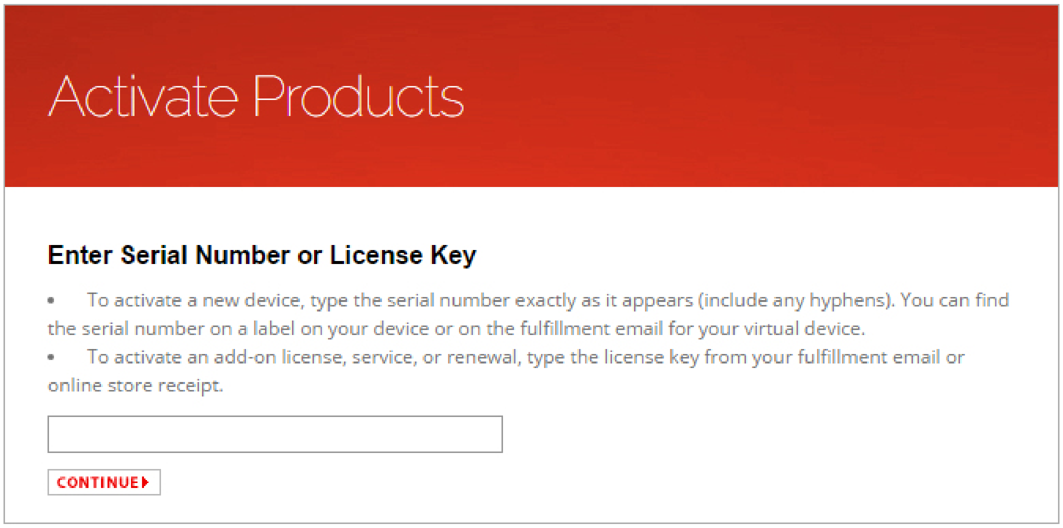
To activate your AP for WatchGuard Wi-Fi Cloud:

1. Go to www.watchguard.com/activate.
2. Log in to your WatchGuard account, or create a new account if you do not have a WatchGuard account.

   If you create a new WatchGuard account, after you finish the account creation process, go to www.watchguard.com/activate, or select **My WatchGuard > Activate Products** from your account menu.



3. Type the serial number for your AP. Click **Continue**.
   Make sure the AP you want to activate has a *Total Wi-Fi* or *Secure Wi-Fi* subscription for Wi-Fi Cloud.



Activate Products

Enter Serial Number or License Key

- To activate a new device, type the serial number exactly as it appears (include any hyphens). You can find the serial number on a label on your device or on the fulfillment email for your virtual device.
- To activate an add-on license, service, or renewal, type the license key from your fulfillment email or online store receipt.

4. Specify a friendly name for the AP in your WatchGuard account.
5. Accept the End-User License Agreement.

6. When the activation is complete, click **Finish**.
   From this page you have three options:
   - You can activate another WatchGuard device
   - You can go to the *WatchGuard Wi-Fi Cloud Help* to learn how to set up your new AP
   - You can go directly to the WatchGuard Wi-Fi Cloud management interface. To connect to WatchGuard Wi-Fi Cloud for future management sessions, go to: https://dashboard.watchguard.cloudwifi.com/

ⓘ You do not have to download or import the generated feature key that appears in your WatchGuard account for your Total or Secure Wi-Fi AP into Wi-Fi Cloud. The expiry date information is automatically communicated from WatchGuard servers to Wi-Fi Cloud.

About Wi-Fi Cloud AP License Expiry

If your Total Wi-Fi or Secure Wi-Fi subscription expires for an AP:

- The expired AP will continue to broadcast SSIDs and allow wireless access to the network based on the most recent configuration applied to the AP.
- Captive portal splash pages will still be available for guest access based on the most recent configuration applied to the AP, but you cannot change the URL or other configuration options.
- You cannot perform further configuration or software updates to an expired AP.
- Reduced monitoring, analytics, and reporting data will be available for expired APs.
- WIPS security detection and prevention capabilities will be available based on the offline WIPS configuration in Wi-Fi Cloud that you configured before the subscription expired.
  - In the default WIPS Offline Configuration, only classification features are available, and all prevention measures are disabled.
  - You can configure the WIPS Offline Configuration in a device template in Manage. For more information, see WIPS Offline Configuration.
- You will not receive technical support for an expired or end of life AP.

For more information, see Wi-Fi Cloud AP License Subscriptions.

Connect and Power On the AP

After you have activated your AP, you can connect it to your network and power on the AP.

To connect and power on your AP:

1. Connect an Ethernet cable to the Ethernet interface on the WatchGuard AP.
    - AP120 – LAN interface
    - AP125 – LAN2 interface (PoE)
    - AP225W – POE In LAN/Uplink interface
    - AP320 / AP322 – LAN1 interface (PoE)
    - AP325 / AP327X / AP420 – LAN1 interface (PoE+)
2. Connect the other end of the Ethernet cable to your network.
3. Make sure DHCP is enabled on the network where you connect the AP.
4. Make sure that the AP has Internet connectivity and can communicate on these ports to the specified domains:
    - HTTP port 80
    - HTTPS port 443
    - UDP port 3851
    - UDP port 3852 is also required if you have AP420 devices that run in Cloud Integration Point (CIP) mode

    To these domains:

    - `*.cloudwifi.com`
    - `redirector.online.spectraguard.net`

    If you use a WatchGuard Firebox that runs Fireware OS v11.11.4 or higher, the Firebox configuration file includes the predefined *WG-Cloud-Managed-WiFi* packet filter policy that you can add to the configuration to enable traffic over the ports required for WatchGuard Wi-Fi Cloud domains.
5. If your network does not support Power over Ethernet (PoE), connect the optional power adapter or PoE injector (sold separately).

After you power on the AP, wait a few minutes for the AP to initialize, then verify that the AP LED indicators are lit, and make sure the AP is online and can communicate with WatchGuard Wi-Fi Cloud.

For more information, see Troubleshoot WatchGuard AP LED Status or the Hardware Guide for your AP.

Troubleshoot Connection Issues

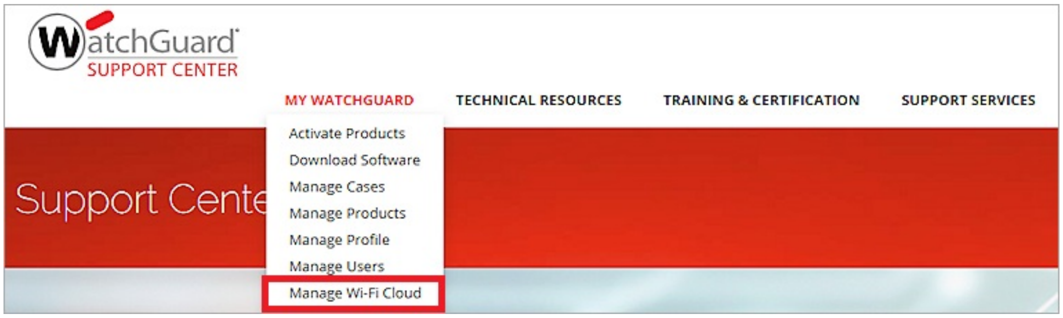
If you have problems with your AP connection:

- Make sure that the Ethernet cable is correctly connected to the Ethernet port on the AP and the other end of the cable is connected to an Ethernet jack or a port on a switch that is enabled.
- If the AP did not receive a valid IP address from the DHCP server, make sure that a DHCP server is enabled and available on the network to which the AP is connected. If the AP still fails to get a valid IP address, you can reboot it once to try to resolve the problem.
- Make sure that Internet connectivity is available from the network to which the AP is connected. Verify that the required ports for communications to WatchGuard Wi-Fi Cloud (HTTP TCP ports 80/443, and UDP port 3851 to redirector.online.spectraguard.net) are open on the firewall. If you use a web proxy server, make sure the settings allow communication between the AP and WatchGuard Wi-Fi Cloud.

Connect to WatchGuard Wi-Fi Cloud

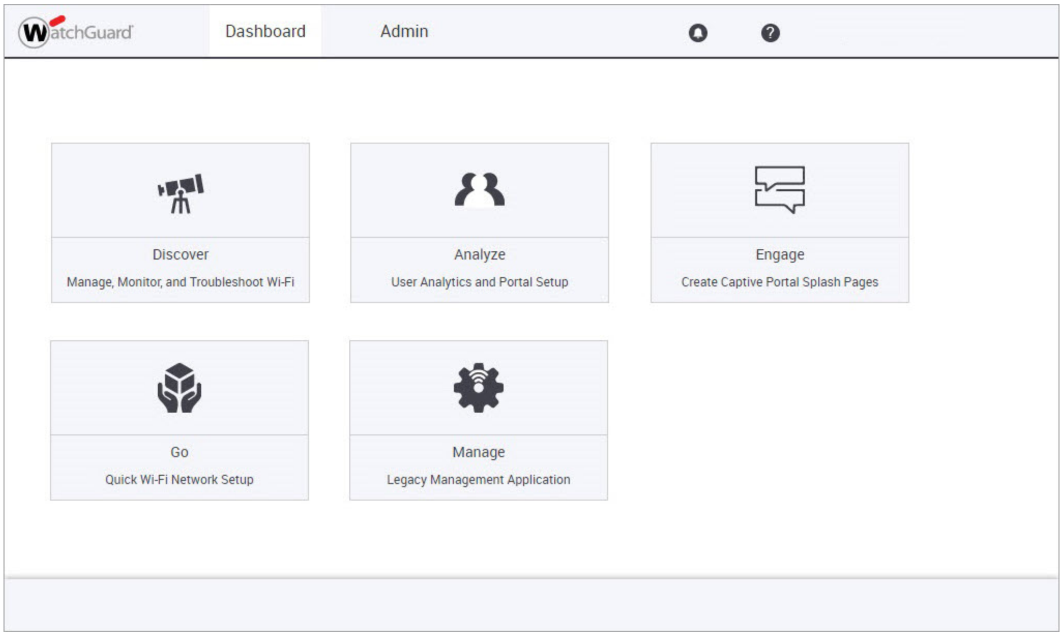
The WatchGuard Wi-Fi Cloud Launchpad includes services and apps that you can use to manage WatchGuard Wi-Fi Cloud. To connect to Wi-Fi Cloud and access the Launchpad Dashboard:

From your WatchGuard account in the Support Center, select **My WatchGuard > Manage Wi-Fi Cloud**.



If you have already logged in to your WatchGuard account, you can also go directly to: https://dashboard.watchguard.cloudwifi.com/

Launchpad Dashboard


WatchGuard
Dashboard
Admin
Discover
Manage, Monitor, and Troubleshoot Wi-Fi
Analyze
User Analytics and Portal Setup
Engage
Create Captive Portal Splash Pages
Go
Quick Wi-Fi Network Setup
Manage
Legacy Management Application

The **Dashboard** page includes the WatchGuard Wi-Fi Cloud services and applications that you use to manage and monitor your APs.

- **Discover** – Configure Wi-Fi networks and WIPS security, monitor the health of your Wi-Fi networks, and troubleshoot Wi-Fi connectivity issues.

- **Analyze** – Provide guest users with access to the Internet through your wireless network from a customized captive portal, and see analytics and reports about guest user access.
- **Engage** – Create and customize splash pages and campaigns for your guest wireless portal.
- **Go** – Quickly set up a wireless network with this mobile-optimized application.
- **Manage** – Legacy application for advanced management of your APs, SSIDs, and security policies.

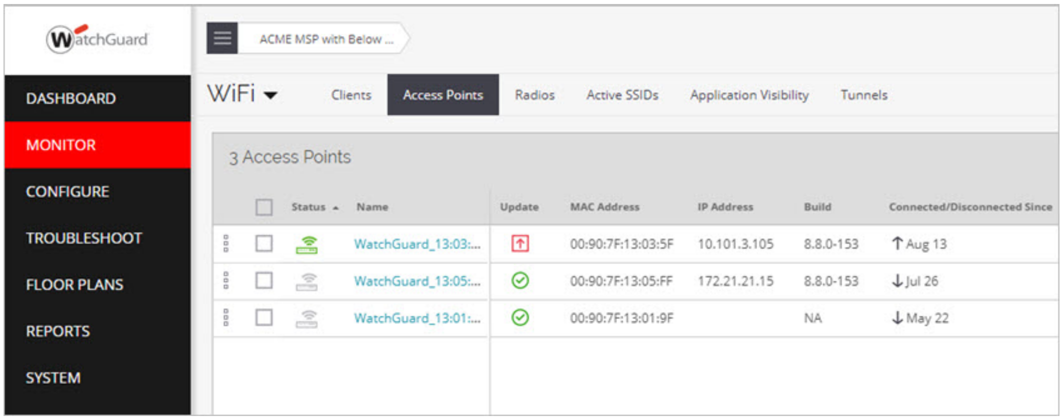
Set up a Wireless Network with Discover

Discover is Wi-Fi Cloud's newest application to configure, monitor, and troubleshoot your Wi-Fi networks.

You can open Discover from the WatchGuard Wi-Fi Cloud Launchpad Dashboard, or go to https://discover.watchguard.cloudwifi.com/.

To configure your wireless networks with Discover:

1. Open Discover.
2. To see your activated APs, select **Monitor > WiFi**, then select **Access Points**.



3 Access Points

☐	Status ▲	Name	Update	MAC Address	IP Address	Build	Connected/Disconnected Since
☐		WatchGuard_13:03:...	↑	00:90:7F:13:03:5F	10.101.3.105	8.8.0-153	↑ Aug 13
☐		WatchGuard_13:05:...	✓	00:90:7F:13:05:FF	172.21.21.15	8.8.0-153	↓ Jul 26
☐		WatchGuard_13:01:...	✓	00:90:7F:13:01:9F		NA	↓ May 22

To continue with your wireless network configuration, see:

- *Upgrade AP Firmware*
- *About the Navigator and Location Folders*
- *Configure SSID Profiles*
- *Configure Radio and Device Settings*

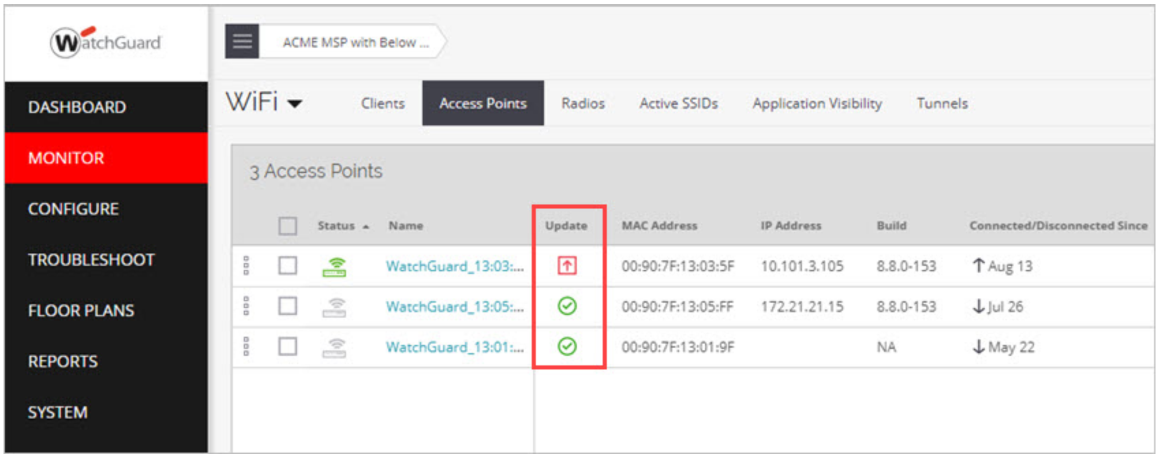
Upgrade AP Firmware

We recommend you make sure that your APs have the latest software version installed, and that it is the same version as the WatchGuard Wi-Fi Cloud server software.

To check your AP firmware update status:

1. Open Discover
2. Select **Monitor > WiFi** then click the **Access Points** tab.

   If the AP needs to be upgraded, ⇧ appears in the **Update** column.



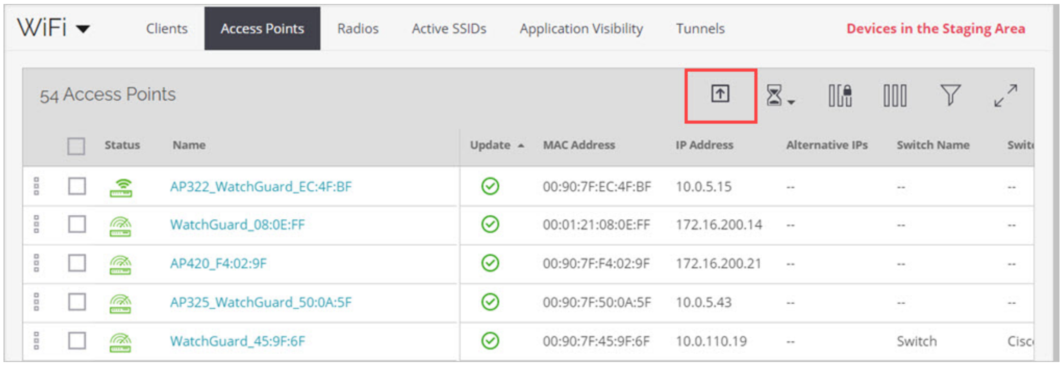
3 Access Points

□	Status	Name	Update	MAC Address	IP Address	Build	Connected/Disconnected Since
□		WatchGuard_13:03:...	⇧	00:90:7F:13:03:5F	10.101.3.105	8.8.0-153	↑ Aug 13
□		WatchGuard_13:05:...	✓	00:90:7F:13:05:FF	172.21.21.15	8.8.0-153	↓ Jul 26
□		WatchGuard_13:01:...	✓	00:90:7F:13:01:9F		NA	↓ May 22

3. To upgrade the firmware on your AP, right-click the AP and select **Update Firmware**.

You can configure Wi-Fi Cloud to automatically update new devices and schedule updates for existing deployed devices.

To configure these options, in Discover, go to **Monitor > WiFi > Access Points**, then click ⇧ in the tool bar.



54 Access Points

□	Status	Name	Update	MAC Address	IP Address	Alternative IPs	Switch Name	Swit
□		AP322_WatchGuard_EC:4F:BF	✓	00:90:7F:EC:4F:BF	10.0.5.15	--	--	--
□		WatchGuard_08:0E:FF	✓	00:01:21:08:0E:FF	172.16.200.14	--	--	--
□		AP420_F4:02:9F	✓	00:90:7F:F4:02:9F	172.16.200.21	--	--	--
□		AP325_WatchGuard_50:0A:5F	✓	00:90:7F:50:0A:5F	10.0.5.43	--	--	--
□		WatchGuard_45:9F:6F	✓	00:90:7F:45:9F:6F	10.0.110.19	--	Switch	Cisc

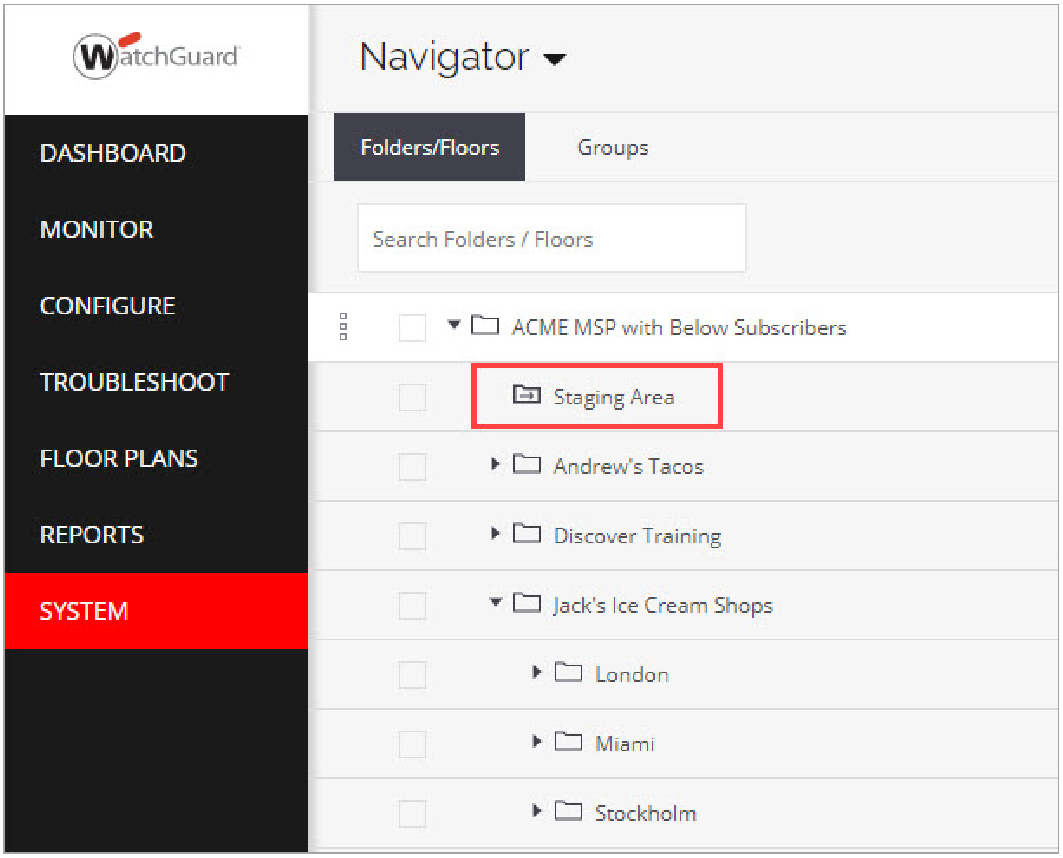
About the Navigator and Location Folders

In Discover, the **Navigator** enables you to organize your wireless deployment into a hierarchical structure and simplifies management of geographically distributed networks. For example, you can organize your locations by country, cities, buildings, functional departments, and floors.

To simplify management of your Wi-Fi networks, location subfolders inherit the SSID profiles, device settings, and security policies from the parent location folder. This also enables you to create a custom configuration for a specific location folder.

In Discover, click **System > Navigator** to view and manage your location folders.

When new APs are deployed, they appear by default in the **Staging Area** folder.

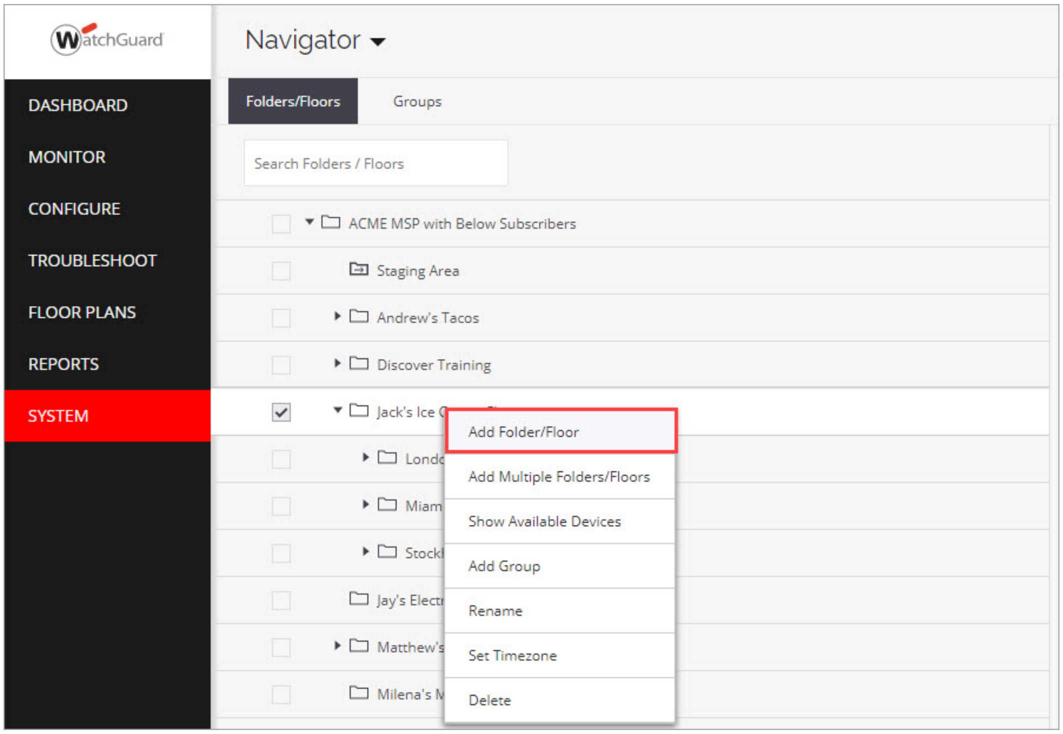


Add a New Folder

You can add new location folders to create an organizational structure for your Wi-Fi network.

To add a new location folder:

1. In Discover, select **System > Navigator**.
2. Right-click an existing folder, then select **Add Folder/Floor**.
   To add multiple folders and floors at the same time, click **Add Multiple Folders/Floors**.
3. Type the name of the new location folder or floor, then click **Add**.

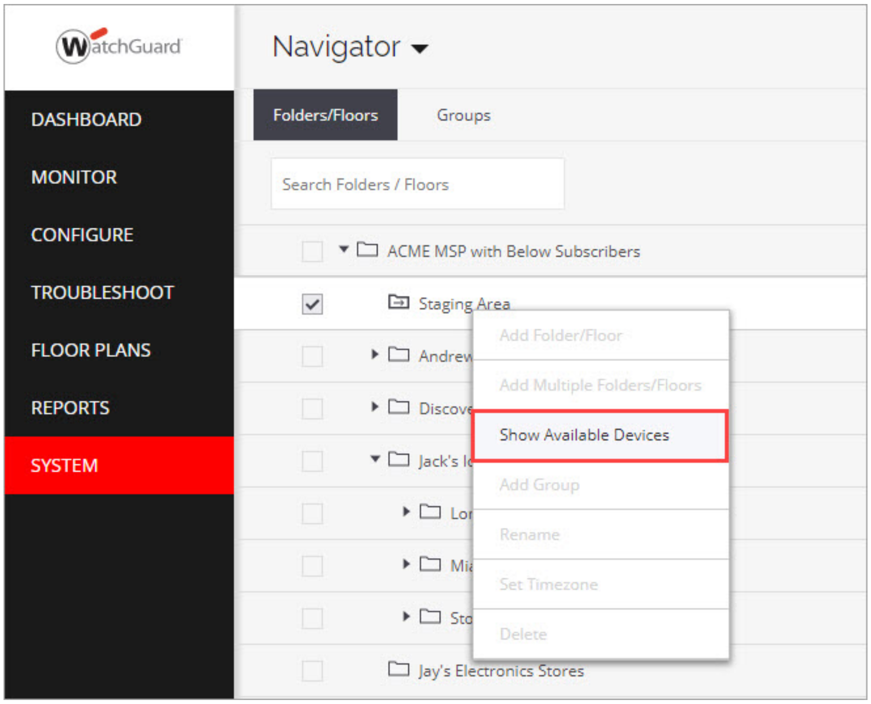


Move an AP to a New Folder

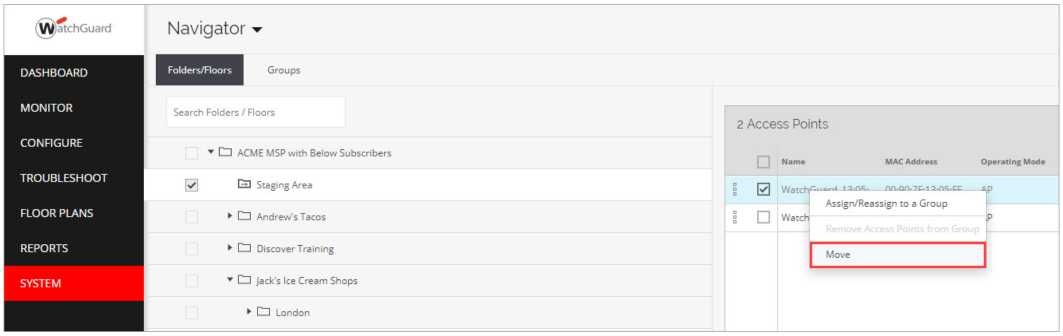
You can add new location folders and move your new APs from the **Staging Area** folder or existing APs in any folder to a new folder.

To move an AP to a new location folder:

1. Open Discover.
2. Select **System > Navigator**.
3. Right-click the location folder, then select **Show Available Devices**.



4. From the Access Points list, right-click the AP to move, then select **Move**. Select the new location folder, then click **Move**.

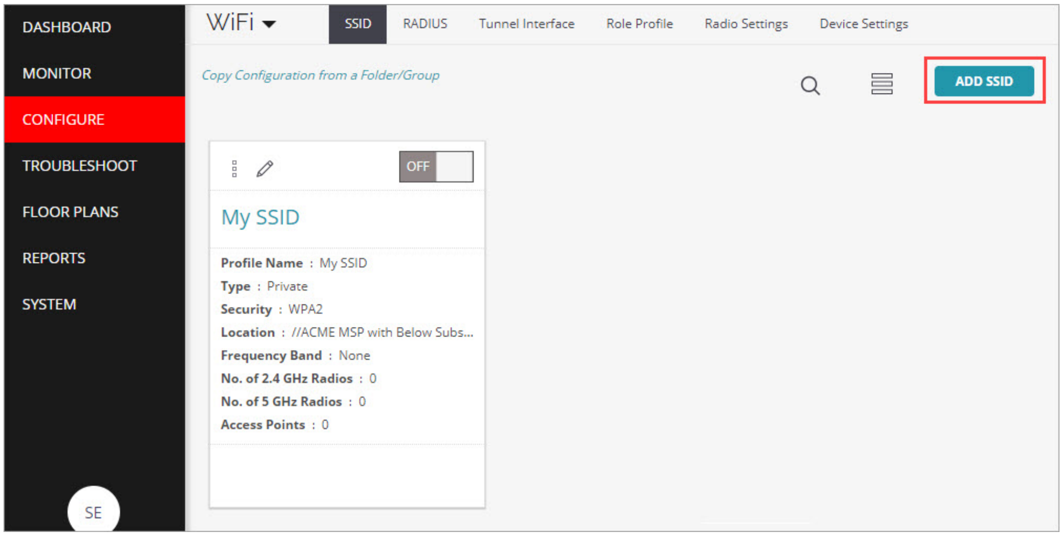


Configure SSID Profiles

SSID profiles define the parameters for wireless access, including the SSID name, security mode, and encryption settings for the Wi-Fi network.

To configure an SSID:

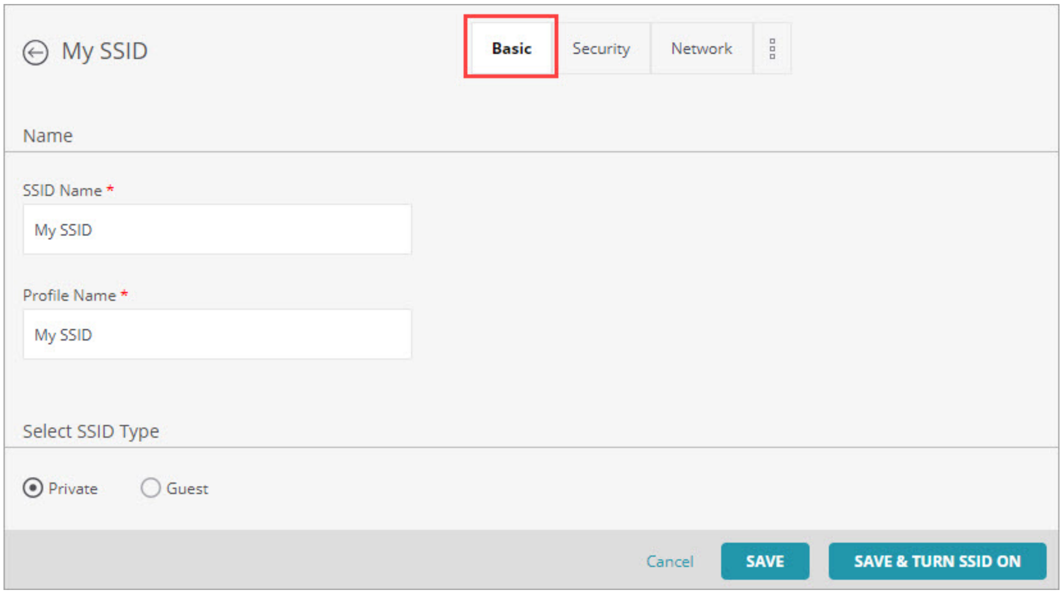
1. Open Discover.
2. From the **Navigator**, select a location for the SSID. SSIDs are automatically inherited by subfolder locations. Make sure to select the correct top-level location when you create an SSID.
3. Select **Configure > WiFi**.



Profile Name : My SSID
Type : Private
Security : WPA2
Location : //ACME MSP with Below Subs...
Frequency Band : None
No. of 2.4 GHz Radios : 0
No. of 5 GHz Radios : 0
Access Points : 0

4. Click **Add SSID** or select an existing SSID to configure.
5. Configure these SSID settings:

Basic Settings



My SSID

Name

SSID Name *
My SSID

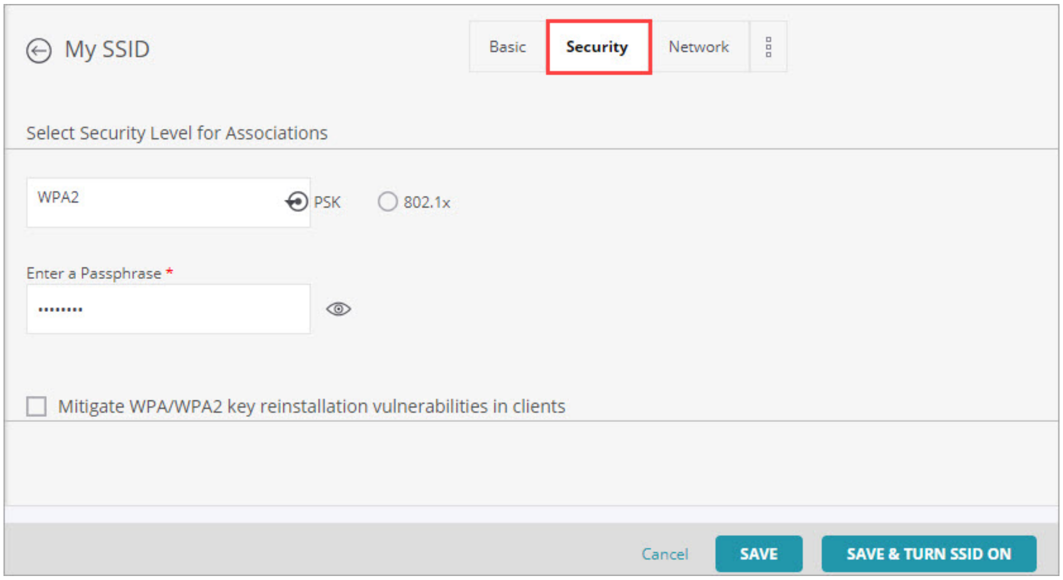
Profile Name *
My SSID

Select SSID Type

● Private ○ Guest

- Type the **SSID Name** and **Profile Name**. Use a descriptive name for the SSID and Profile name for your specific deployment.
- In the **Select SSID Type** section, select **Private** for a private Wi-Fi network SSID, or select **Guest** for a guest SSID Wi-Fi network.
- (Optional) Select the **Hide SSID** check box to not broadcast the SSID name on the Wi-Fi network.
- Click **Next** or click the **Security** tab to go to the next configuration section.

Security Settings



Select Security Level for Associations

WPA2 ● PSK ○ 802.1x

Enter a Passphrase *

••••••••

□ Mitigate WPA/WPA2 key reinstallation vulnerabilities in clients

- From the **Select Security Level for Associations** drop-down list, we recommend at minimum you select WPA2 with PSK security. If required, you can customize the security settings specific to your deployment.
- Type a **Passphrase** for the security mode you selected.
- Keep other settings at their default value or customize the settings for your deployment as required.

Network and Other SSID Settings

- Leave the default settings in this section unless you have specific configuration requirements for your deployment.

6. Click **Save** to save the SSID settings, or click **Save & Turn SSID On** to save your settings and enable the SSID on your Wi-Fi network.

Repeat these steps to add additional SSIDs to your network.

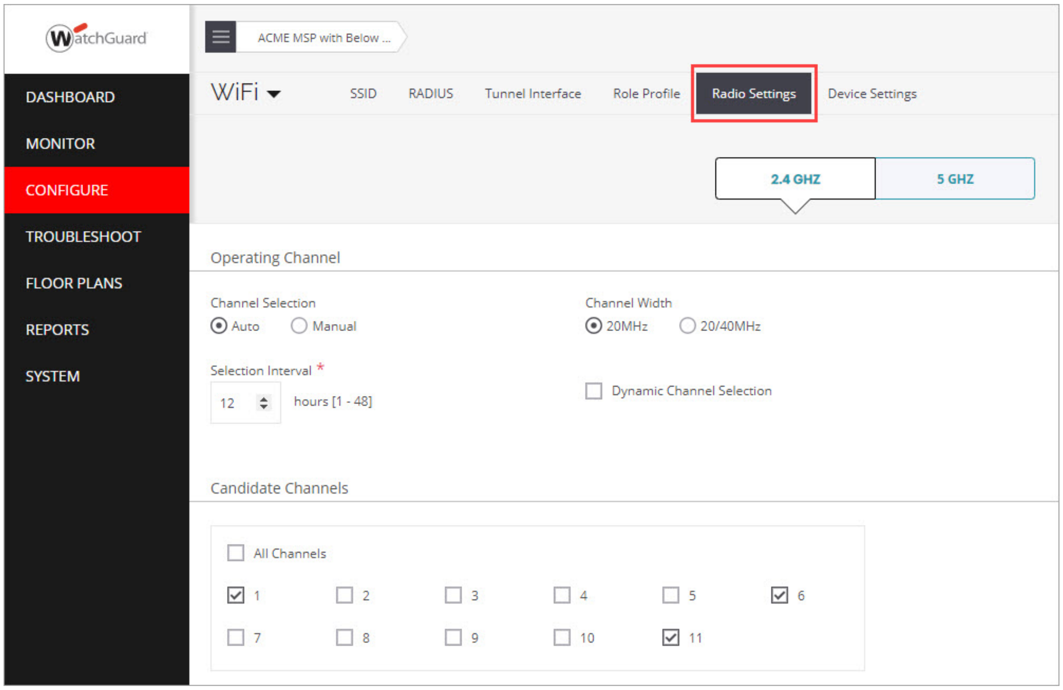
Configure Radio and Device Settings

You can specify radio and device settings for your APs, including the operation mode, frequency bands, wireless channels, and the AP password.

Radio and device settings (device templates) are applied per location, and are automatically inherited by subfolder locations. This enables you to create a custom configuration for a specific location folder.

To configure radio and device settings for your APs:

1. Open Discover.
2. From the **Navigator**, select the location where you want to apply the radio and device settings. These settings are inherited by all subfolders of the selected location.
3. Select **Configure > WiFi**, then select the **Radio Settings** tab.



Operating Channel

Channel Selection ● Auto ○ Manual

Channel Width ● 20MHz ○ 20/40MHz

Selection Interval * 12 hours [1 - 48]

□ Dynamic Channel Selection

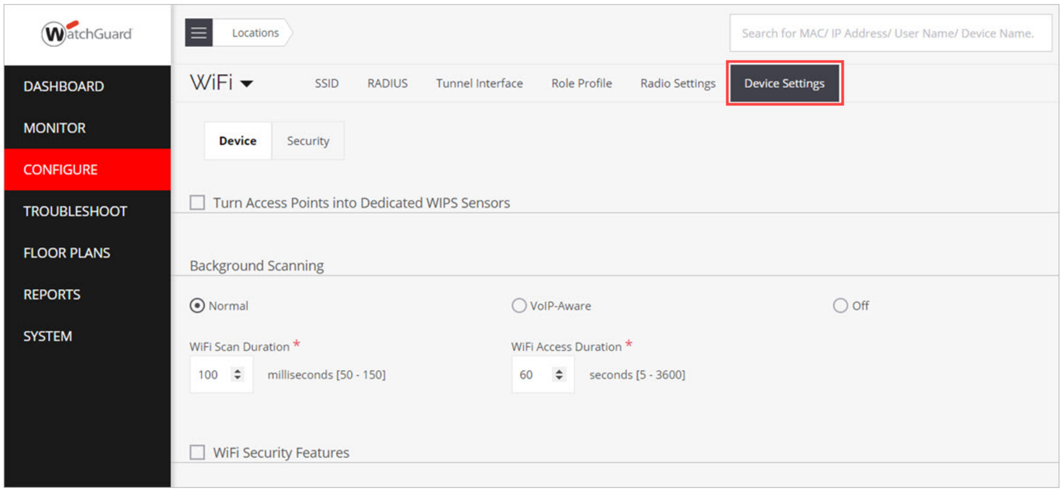
Candidate Channels

□ All Channels

☑ 1 □ 2 □ 3 □ 4 □ 5 ☑ 6

□ 7 □ 8 □ 9 □ 10 ☑ 11

4. Configure the radio settings for your deployment for both 2.4 GHz and 5 GHz radios.
   - We recommend you use the default settings for most deployments.
   - You can optionally enable **Dynamic Channel Selection** so that AP radios automatically switch to a better channel if the current channel experiences high interference.
5. Select the **Device Settings** tab.



□ Turn Access Points into Dedicated WIPS Sensors

Background Scanning

● Normal ○ VoIP-Aware ○ Off

WiFi Scan Duration * 100 milliseconds [50 - 150]

WiFi Access Duration * 60 seconds [5 - 3600]

□ WiFi Security Features

Configure your device settings based on your AP models and deployment:

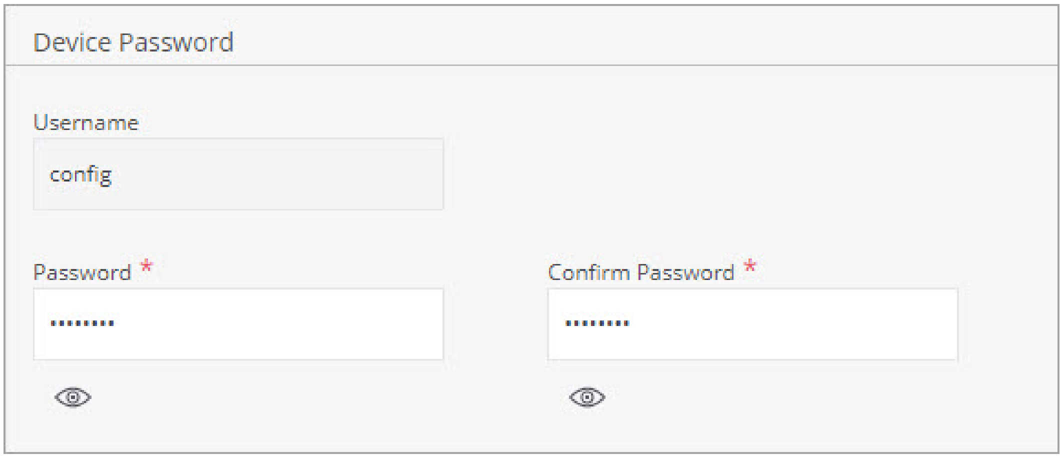
Tri-Radio Access Points (AP225W, AP325, and AP420)

- Use the default radio and device settings to broadcast Wi-Fi on the 2.4 GHz and 5 GHz radios.
- The third radio is configured by default as a WIPS Sensor.

Dual-Radio Access Points (AP120, AP125, AP320, AP322, and AP327X)

- **Wi-Fi Access Points with Background Scanning**
  - Use the default radio and device settings to broadcast Wi-Fi on the 2.4 GHz and 5 GHz radios.
  - Set the **Background Scanning** mode to **VoIP-Aware** scanning for AP125. Set the **Background Scanning** mode to **Normal** for AP120, AP320, and AP322 because they do not support VoIP-aware scanning.
  - Configure one dedicated WIPS sensor for every 3-5 Wi-Fi access points.
- **Dedicated WIPS Sensor for WIPS Overlay**
  - Select the **Turn Access Points into Dedicated WIPS Sensors** check box.
  - No Wi-Fi is broadcast from APs configured as dedicated WIPS sensors.
  - Configure one dedicated WIPS sensor for every 3-5 Wi-Fi access points.
- **Dedicated Wi-Fi Access Points**
  - Use the default radio and device settings to broadcast Wi-Fi on the 2.4 GHz and 5 GHz radios.
  - Set the **Background Scanning** mode to **Off**.

6. In the **Device Password** section, type a **Password** for the AP.
   You cannot save the device settings if the password is not defined.



Device Password

Username

config

Password *

••••••••

Confirm Password *

••••••••

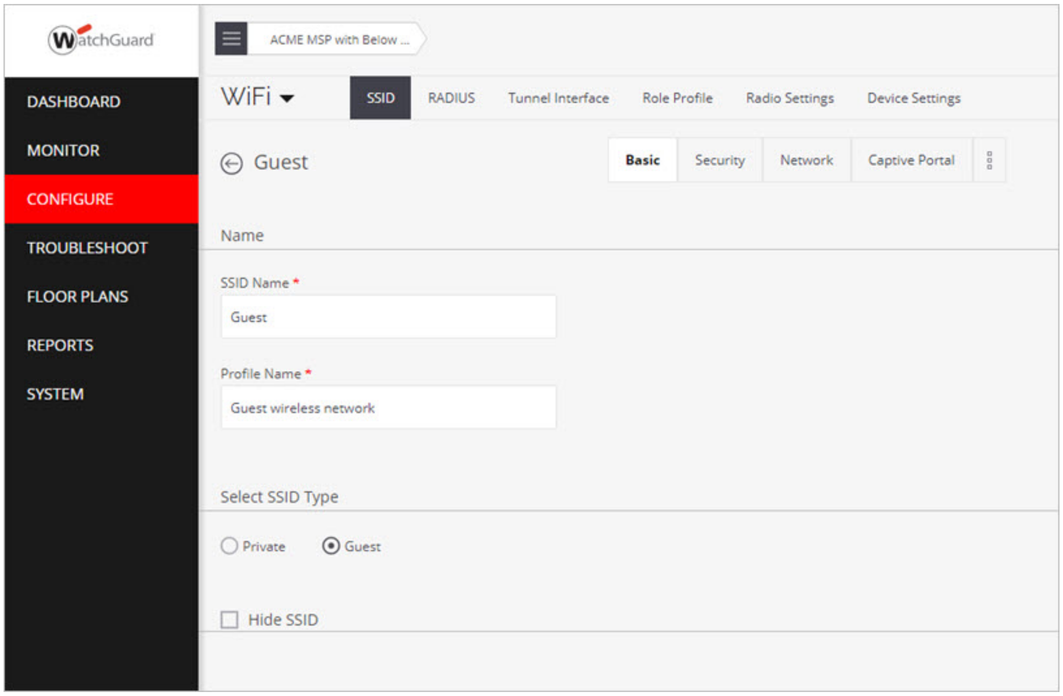
7. Click **Save**.

Enable a Captive Portal for Guest Users

For guest wireless access, you can use Discover to quickly create a captive portal with a basic layout for click-through or authenticated guest wireless access.

To create a guest SSID with a Captive Portal:

1. Open Discover.
2. From the **Navigator**, select a location for the guest SSID. SSIDs are automatically inherited by subfolder locations. Make sure to select the correct top-level location when you create an SSID.
3. Select **Configure > WiFi**.
4. Click **Add SSID**.



Name

SSID Name *
Guest

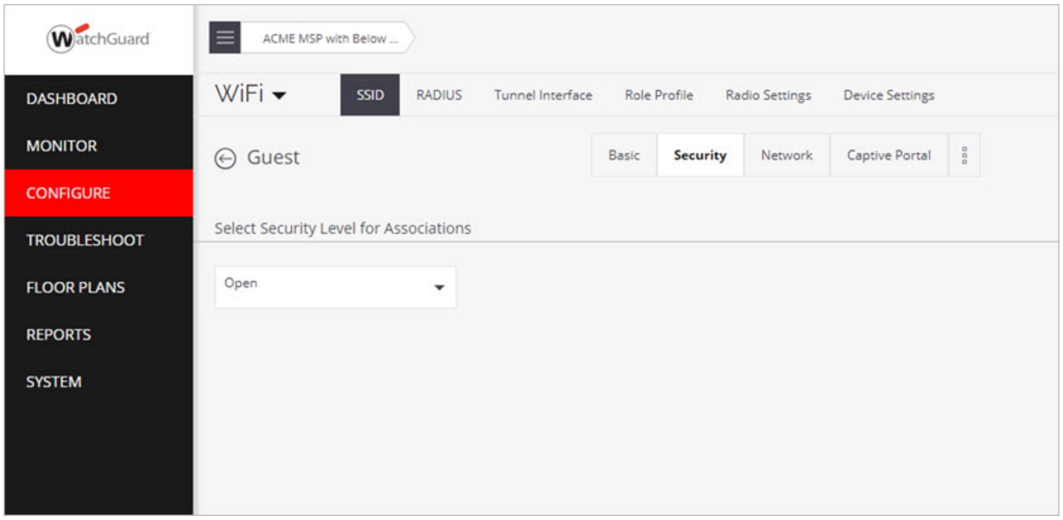
Profile Name *
Guest wireless network

Select SSID Type

○ Private ● Guest

□ Hide SSID

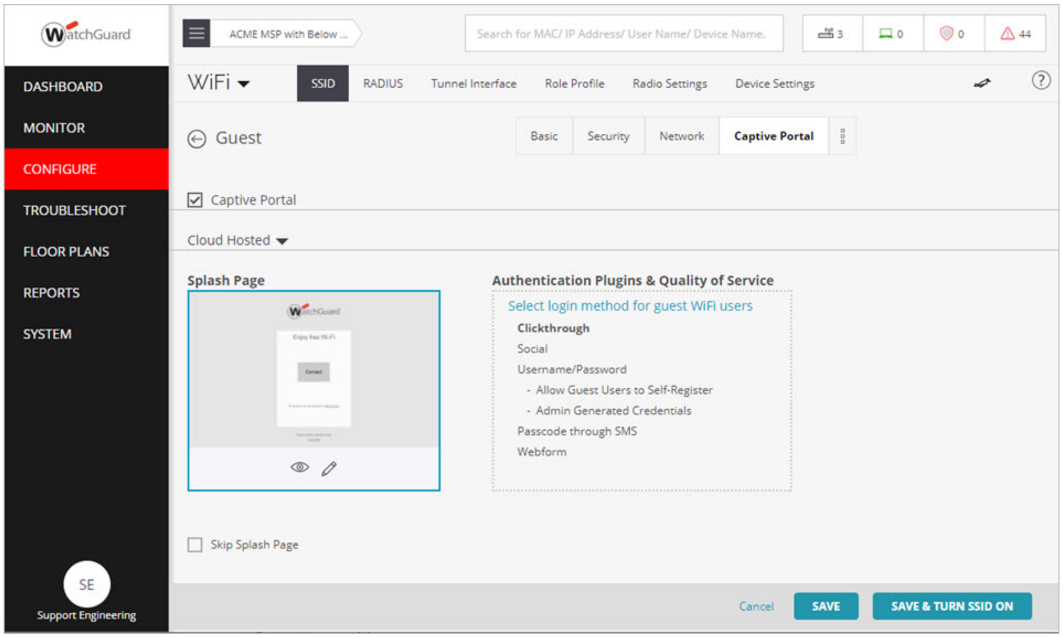
5. Type the **SSID Name** and **Profile Name**.
6. In the **Select SSID Type** section, select **Guest**.
7. Click **Next** or click the **Security** tab to go to the next configuration section.



Select Security Level for Associations

Open

8. From the **Select Security Level for Associations** drop-down list, select **Open** for an open network with no security, or select **WPA2** with **PSK** security to use a passphrase for your guest network.
9. Select the **Captive Portal** tab.



☑ Captive Portal

Cloud Hosted

Splash Page

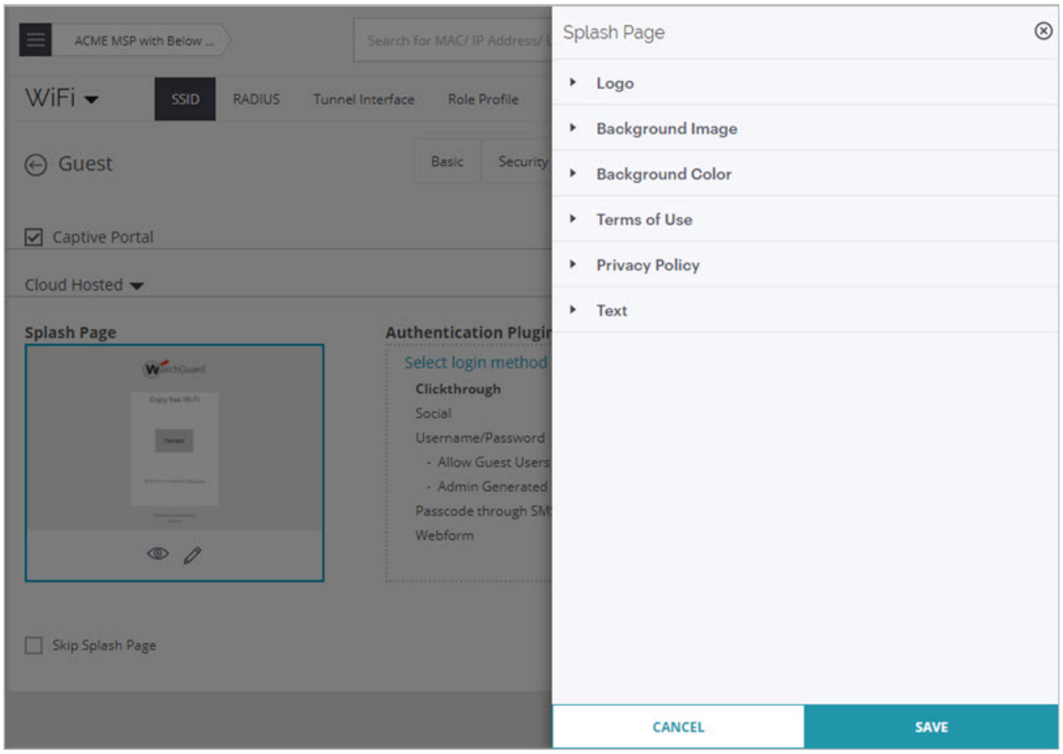
Authentication Plugins & Quality of Service

Select login method for guest WiFi users

Clickthrough
Social
Username/Password
- Allow Guest Users to Self-Register
- Admin Generated Credentials
Passcode through SMS
Webform

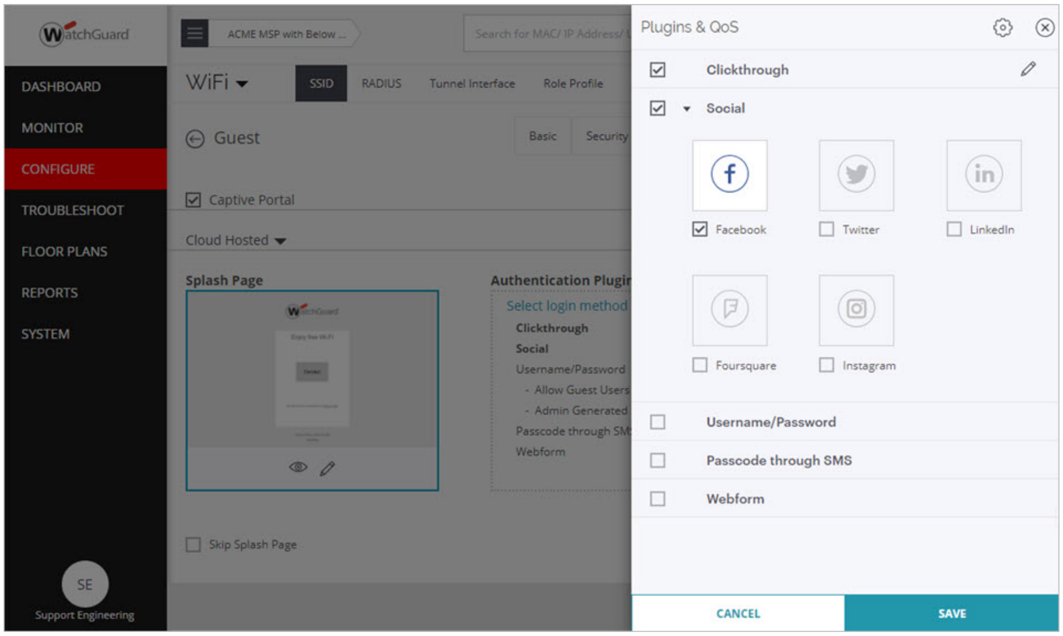
□ Skip Splash Page

10. Select the **Captive Portal** check box.
11. From the drop-down list, select **Cloud Hosted** as the portal type.
12. In the **Splash Page** section, edit the splash page to customize the text and images for your portal. You can preview your splash page to see how it will appear to guest users.



13. Click **Save** to save your splash page settings.

14. In the **Authentication Plugins & Quality of Service** section, click **Select login method for guest WiFi users**, then customize your authentication settings.



15. Click **Save** to save your authentication plugin settings.

16. Click **Save & Turn SSID ON**.