



Wi-Fi Cloud

Create a Trusted Wireless Environment with WIPS

About This Guide

This guide helps you create a Trusted Wireless Environment with Wi-Fi Cloud WIPS. 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: 2/21/2024

Copyright, Trademark, and Patent Information

Copyright © 2024 WatchGuard Technologies, Inc. All rights reserved. All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

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

255 S. King St.
Suite 1100
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

Create a Trusted Wireless Environment with WIPS	1
About the Trusted Wireless Environment	2
Wi-Fi Security Report.....	3
Create a Trusted Wireless Environment with WatchGuard.....	4
WatchGuard Access Point Models.....	5
About WatchGuard Wi-Fi Cloud WIPS	6
WIPS Classifications.....	6
Access Points.....	6
Clients.....	7
WatchGuard AP Operation Modes.....	8
Protect WatchGuard Networks and Third-Party Networks with WIPS	9
WatchGuard Wi-Fi Network Protection.....	9
Third-Party Wi-Fi Network Protection (WIPS Overlay).....	10
About the Navigator and Location Folders	12
Add a New Folder.....	13
Move an AP to a New Folder.....	14
About AP Groups	15
Configure Wi-Fi Cloud WIPS	18
Before You Begin.....	18
Configure SSID Profiles.....	19
Configure Radio and Device Settings.....	22
Configure the Authorized WiFi Policy.....	25
Customize an Authorized WiFi Policy.....	26
Configure Access Point Auto-Classification.....	28
Configure Client Auto-Classification.....	29
Configure Automatic Intrusion Prevention.....	31

How Intrusion Prevention Stops the Six Known Wi-Fi Threat Categories.....	32
Rogue Access Point Protection.....	32
Rogue Client Protection.....	33
Neighbor AP Protection.....	34
Ad-Hoc Connection Protection.....	35
Evil Twin AP Protection.....	36
Misconfigured AP Protection.....	37
Monitor WIPS Activity.....	38
Monitor AP Classifications.....	38
Change AP Classification.....	39
Monitor Client Classifications.....	40
Change Client Classification.....	41
Configure and Monitor WIPS Security Alerts.....	42
Configure WIPS Alerts.....	43
Monitor WIPS Alerts.....	44
Activate Automatic Intrusion Prevention.....	45
Test Intrusion Prevention.....	47
Monitor WIPS Alerts.....	48

Create a Trusted Wireless Environment with WIPS

This guide provides best practices and a step-by-step guide to create a Trusted Wireless Environment with WatchGuard Wi-Fi Cloud and WIPS.

This guide includes these topics:

- [About the Trusted Wireless Environment](#)
- [About WatchGuard Wi-Fi Cloud WIPS](#)
- [Protect WatchGuard Networks and Third-Party Networks with WIPS](#)
- [About the Navigator and Location Folders](#)
- [About AP Groups](#)
- [Configure Wi-Fi Cloud WIPS](#)
 - [Configure SSID Profiles](#)
 - [Configure Radio and Device Settings](#)
 - [Configure the Authorized WiFi Policy](#)
 - [Configure Access Point Auto-Classification](#)
 - [Configure Client Auto-Classification](#)
 - [Configure Automatic Intrusion Prevention](#)
 - [Monitor WIPS Activity](#)
 - [Activate Automatic Intrusion Prevention](#)

About the Trusted Wireless Environment

A Trusted Wireless Environment is a framework used to build a complete Wi-Fi network that is fast, easy to manage, and most importantly, secure.



A Trusted Wireless Environment is based on these three core concepts:

1. **Market-Leading Performance:** You should never be forced to compromise security to achieve adequate performance to support your environment with the speed, connections and density that it requires.
2. **Scalable Management:** With easy set-up and management, you should be able control your entire wireless network, big or small, from a single interface and execute key processes to safeguard the environment and its users.
3. **Verified Comprehensive Security:** You should be able to prove that your security solution defends your business against Wi-Fi attacks and can deliver on these benefits:
 - Provide automatic protection from the six known Wi-Fi threat categories:
 - Rogue access point
 - Rogue client
 - Neighbor access point
 - Ad-hoc connection
 - Evil Twin access point
 - Misconfigured access point
 - Allow legitimate external access points to operate in the same airspace
 - Prevent user connections to unsanctioned Wi-Fi access points

For more information, see [Trusted Wireless Environment](#) on the WatchGuard web site.

You can test your own wireless network security measures to see if they are able to detect and prevent the six known threats identified by the Trusted Wireless Environment. For more information, see the [Trusted Wireless Environment Test Guide](#).

Wi-Fi Security Report

The industry's first Wi-Fi security report has been published by Miercom. This report compares product efficacy against the six known Wi-Fi threat categories, and illustrates the hidden, security deficits with many competing Wi-Fi solutions.

Test	WatchGuard AP420		Aruba IAP335		Cisco Meraki MR53		Ruckus R710	
	Detect	Prevent	Detect	Prevent	Detect	Prevent	Detect	Prevent
Rogue AP	P	P	F	N/A	F	MP	F	N/A
Rogue Client	P	P	F	N/A	F	MP	N/A	MP
Neighbor AP	P	P	P	P	F	N/A	F	N/A
Ad-Hoc Network	P	P	F	N/A	F	N/A	P	N/A
"Evil Twin" AP	P	P	P	F	P	MP	P	F
Misconfigured AP	P	P	P	N/A	N/A	N/A	N/A	N/A
Concurrent Threats	P	P	F	F	F	F	F	F

P – Pass
MP Marginal Pass; require manual prevention
F – Failure to detect or protect from the referenced test
N/A – Feature not supported

The Wi-Fi Security report found that WatchGuard access points with a Secure Wi-Fi or Total Wi-Fi management subscription is the only solution to:

- Automatically detect and prevent the six known Wi-Fi threat categories simultaneously and still maintain performance
- Support automatic detection and prevention of rogue APs and rogue clients
- Automatically block endpoints from communicating over ad-hoc Wi-Fi connections
- Automatically prevent connections to "evil twin" APs and dangerous connections to misconfigured APs, such as private SSIDs without encryption

Create a Trusted Wireless Environment with WatchGuard

With WatchGuard Wi-Fi Cloud and WIPS (Wireless Intrusion Prevention System), it is easy to quickly create a Trusted Wireless Environment with WIPS and automatically protect your Wi-Fi network against the six known Wi-Fi threat categories.

WIPS is a collection of features that run on WatchGuard APs and Wi-Fi Cloud. You can use WatchGuard APs for both Wi-Fi access and WIPS security protection, or you can use APs as dedicated WIPS security sensors that you can deploy together with other WatchGuard APs or third-party APs and Wi-Fi controllers.






To create a Trusted Wireless Environment, WatchGuard APs must have either a **Total Wi-Fi** or **Secure Wi-Fi** AP management subscription.

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.

WatchGuard Access Point Models

WatchGuard currently offers these access point models:

					
Recommended Use Case	AP125 Lower-density high performance ideal for small schools, distributed remote offices, and small meeting rooms	AP225W Medium-density high performance ideal for multi-dwelling units (MDU) structures such as dorm rooms, hotels, assisted living, and military housing units.	AP325 Medium-density high performance including K-12 schools, SMBs, restaurants	AP327X Medium-density high performance IP-67 rated rugged outdoor including school campuses, RV parks, manufacturing yards, warehouses	AP420 High-density, high performance including large schools, meeting rooms, shopping malls
Radios & Streams	2x2:2 MU-MIMO Wave 2	2x2:2 MU-MIMO Wave 2 3rd WIPS Radio	2x2:2 MU-MIMO Wave 2 3rd WIPS Radio	2x2:2 MU-MIMO Wave 2	4x4:4 MU-MIMO Wave 2 3rd WIPS radio
Deployment	Indoor	Indoor	Indoor	Outdoor	Indoor
Number of Antennas	4 Internal	4 Internal	6 Internal	4 N-Type External Connectors	10 Internal
Maximum Data Rate	867 Mbps/300 Mbps	867 Mbps / 400 Mbps	867 Mbps/300 Mbps	867 Mbps/400 Mbps	1.7 Gbps/800 Mbps
Ports	2x Gbe	3x Gbe	2x Gbe	2x Gbe	2x Gbe
Power over Ethernet (PoE)	802.3af (PoE)	802.3at (PoE+)	802.3at (PoE+)	802.3at (PoE+)	802.3at (PoE+)
Product Dimensions	5.83" x 5.83" x 1.29" (148 x 148 x 33 mm)	7.3" x 4.9" x 1" (186.4 x 123.9 x 25.5mm)	7.72" x 7.72" x 1.69" (196 x 196 x 43 mm)	8.42" x 8.42" x 2.66" (213.9 x 213.9 x 67.5 mm)	8.66" x 8.66" x 2.24" (220 x 220 x 57 mm)

About WatchGuard Wi-Fi Cloud WIPS

WIPS (Wireless Intrusion Prevention System) is a powerful, cloud-based, enterprise-level wireless security solution that helps detect and prevent threats to your wireless network.

WIPS includes these security technologies that work together to secure your wireless network:

- Auto-classification of APs and clients using marker packet techniques that classify APs, clients, and networks, including vulnerable and guest SSIDs, based on the sources and types of wireless traffic
- Authorized Wi-Fi policies to enforce a minimum set of security parameters for wireless access
- Intrusion Prevention capabilities to detect wireless security threats and actively mitigate certain types of attacks

WIPS Classifications

WIPS uses device classifications together with your security policies to monitor your network for threats.

Access Points

APs are classified by WIPS in these categories:

DASHBOARD	WIPS	Managed WiFi Devices	Access Points	Clients	Networks
MONITOR	A Authorized	R Rogue	E External	U Uncategorized	
CONFIGURE	172 Access Points				
TROUBLESHOOT	Classification	Status	Name	MAC Address	Prevention Status
FLOOR PLANS	A		WatchGuard_13:05:...	00:90:7F:13:05:FF	--
REPORTS	A		WatchGuard_ED:00:...	00:90:7F:ED:00:70	--
SYSTEM	A		WatchGuard_13:03:...	00:90:7F:13:03:5F	--
	E		WatchGuard_F4:13:...	00:90:7F:F4:13:61	--
	R		Ag Acquisition_01:D...	40:47:6A:01:DA:DD	--
	E		WatchGuard_E8:3E:...	00:90:7F:E8:3E:E0	--

- **Authorized** – Managed APs that match your defined Authorized WiFi Policy.
- **Guest** – Authorized APs that are configured for guest Wi-Fi access.
- **Misconfigured** – Authorized APs with a configuration that does not match your defined Authorized WiFi Policy.
- **Rogue** – Unauthorized APs connected to your wired network.
- **External** – Neighborhood APs that are not part of your Wi-Fi network but operate in the vicinity.
- **Uncategorized** – New APs discovered by Wi-Fi Cloud that have not yet been classified.

Clients

Clients are classified at initial discovery and subsequent associations with your APs:

Classification	Status	Name	User Name
A	<input type="checkbox"/>	Intelorate_E2:AC:3E	--
A	<input type="checkbox"/>	Intel_45:1B:8B	--
A	<input type="checkbox"/>	Intel_28:F7:88	--
U	<input type="checkbox"/>	Apple_D4:6D:D3	--
E	<input type="checkbox"/>	E2:55:7D:40:FB:8F	--
R	<input type="checkbox"/>	Google_51:60:F8	--

- **Authorized** – Managed clients that connect through an Authorized AP.
- **Guest** – Clients that connect to an Authorized AP for guest Wi-Fi access.
- **Rogue** – Unauthorized clients on your network that connect through a Rogue AP.
- **External** – Neighborhood clients that are not part of your Wi-Fi network but operate in the vicinity. External clients can be reclassified if they connect to an Authorized, Authorized Guest, or Rogue access point.
- **Uncategorized** – New clients discovered by Wi-Fi Cloud that have not yet been classified.
- **Misbehaving** – Authorized clients that connected to an external, guest, or rogue AP, ad hoc network, or performed bridging between the wired and wireless network.

WatchGuard AP Operation Modes

You can configure WatchGuard APs in these modes of operation:

Access Point

- Performs normal AP functions for Wi-Fi access to the network.
- Does not perform security scanning.

Access Point with Background Scanning

- Performs normal AP functions for Wi-Fi access to the network.
- Scans the RF environment for radio and channel optimization.
- Scans the wireless network for security threats on available channels.
- VoIP-aware scanning option is available to optimize high priority traffic while background scanning.
- Limited ability to detect over-the-air threats.
- Cannot perform active prevention of over-the-air threats.
- Not as effective as a dedicated WIPS sensor.

WIPS Sensor

- Dedicated to WIPS security and intrusion prevention.
- Does not perform normal AP functions for wireless access to the network.
- Can be used to protect a WatchGuard AP network or any third-party AP network. WIPS can protect APs from any vendor. For more information, see [Protect WatchGuard Networks and Third-Party Networks with WIPS](#).
- Dual-radio AP models configured as dedicated WIPS sensors use both 2.4 and 5 GHz radios for security scanning, and do not perform normal AP functions for Wi-Fi access to the network.
- Tri-radio models (AP225W, AP325, and AP420) have a third radio as a dedicated WIPS sensor and offer dedicated 2.4 and 5 GHz Wi-Fi access on the other two radios.



If you configure a tri-radio AP into a dedicated WIPS sensor, the 2.4 GHz and 5 GHz radios are dedicated to WIPS security scanning, while the third scanning radio is disabled.

Some AP models must use full PoE+ power or be connected to a power adapter for the third WIPS scanning radio to be fully effective. Lower PoE power results in reduced performance and effectiveness of WIPS scanning and intrusion prevention functions. For more information, see [AP Power Requirements](#).

Protect WatchGuard Networks and Third-Party Networks with WIPS

With WIPS, you can protect both WatchGuard AP networks and also third-party AP networks.

WatchGuard Wi-Fi Network Protection

The patented WIPS security protection in WatchGuard APs and Wi-Fi Cloud can protect Wi-Fi networks in which all APs deployed on the network are WatchGuard APs. WatchGuard APs are categorized in Wi-Fi Cloud as Authorized APs and automatically protected, while other APs in the airspace are detected as rogue or external neighbor access points and blocked.

We recommend you deploy at least one dedicated WIPS sensor for every 3-5 Wi-Fi access points, depending on the physical environment and signal attenuation.

- Place your WIPS sensors to provide full coverage over your Wi-Fi airspace, but do not install them too close to your existing APs to avoid interference.
- Make sure there is some overlap in the coverage area so that at least two sensors are active in the same area in the event of multiple threats.



- Tri-radio models (AP225W, AP325, and AP420) have a third radio as a dedicated WIPS sensor and offer dedicated 2.4 and 5 GHz Wi-Fi access on the other two radios.
- Dual-radio models offer 2.4 and 5 GHz Wi-Fi access. You can also configure a dual-radio AP as a dedicated WIPS sensor where both radios are dedicated to security scanning and do not broadcast Wi-Fi.

Third-Party Wi-Fi Network Protection (WIPS Overlay)

Secure Wi-Fi and Total Wi-Fi management subscriptions also enable you to use WatchGuard APs as dedicated WIPS sensors in a third-party AP and Wi-Fi controller environment.

WatchGuard WIPS sensors are dedicated to WIPS security protection and monitor, detect, and prevent security threats in all third-party AP networks. WIPS can protect APs from any vendor.



- We recommend you deploy one WatchGuard WIPS sensor for every 3-5 third-party APs, depending on the physical environment and signal attenuation.
- Use dual-radio APs, such as the AP125, configured as dedicated WIPS sensors for WIPS overlay deployments. Dedicated WIPS sensors do not provide Wi-Fi access which is not required when protecting third-party AP networks.

- Third-party APs must be classified in Wi-Fi Cloud as Authorized APs before they can be protected by WIPS. You can upload lists of authorized third-party AP MAC addresses to Wi-Fi Cloud. For more information, see [Import Device List](#).
- In addition, Wi-Fi Cloud offers direct integration with Aruba and Cisco wireless controllers to import AP information with an AP420 in Cloud Integration Point (CIP) mode. For more information, see [Wi-Fi Cloud Integration with Third-Party Controllers using CIP](#).

About the Navigator and Location Folders

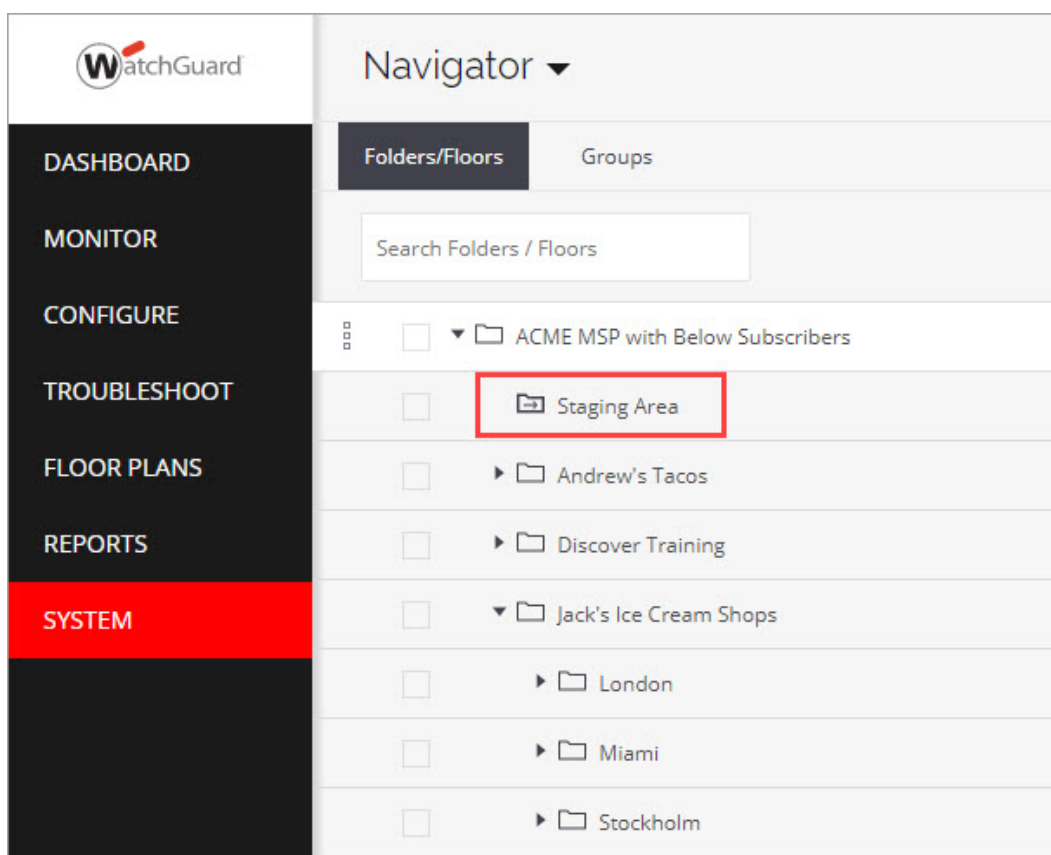
In Discover, the **Navigator** enables you to organize your wireless deployment into a hierarchical structure and simplifies management of geographically distributed networks. For example, you can organize your locations by country, cities, buildings, functional departments, and floors.

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.

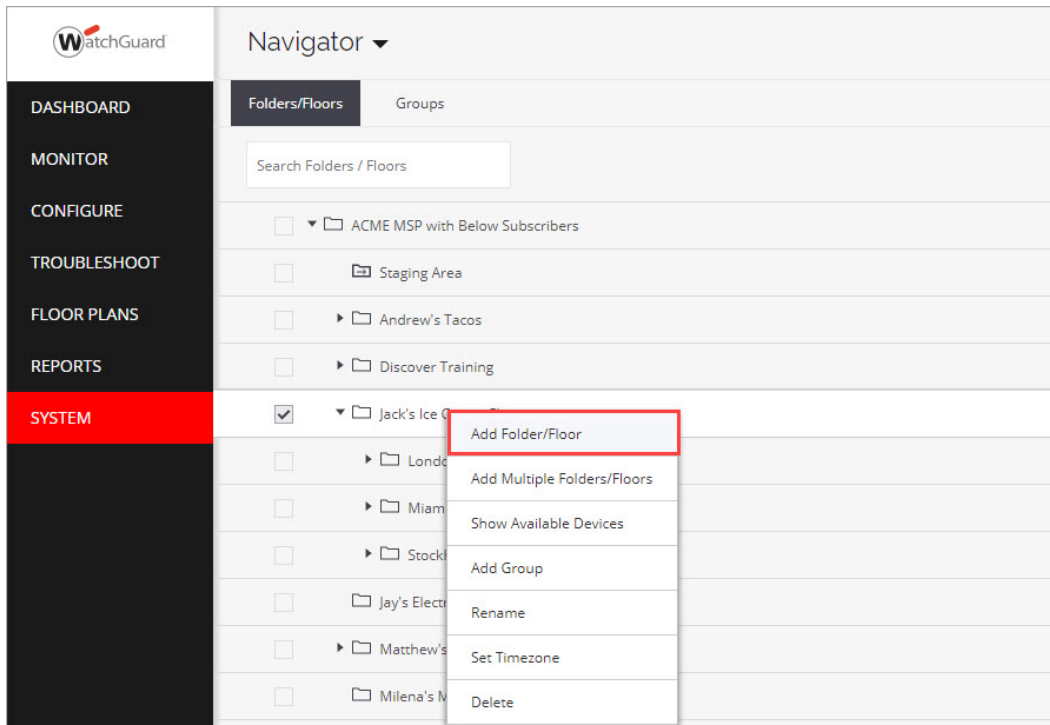


Add a New Folder

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**.

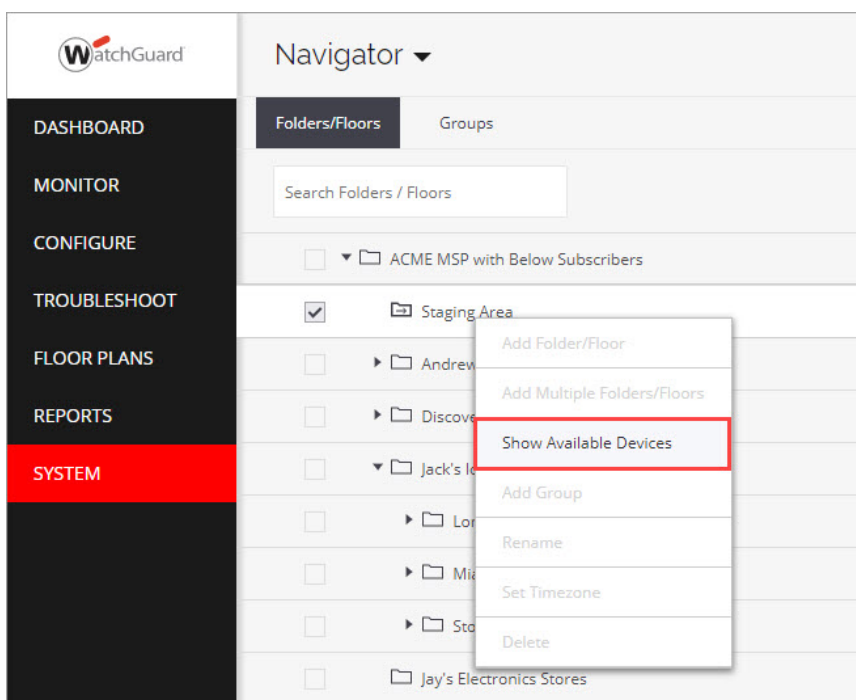


Move an AP to a New Folder

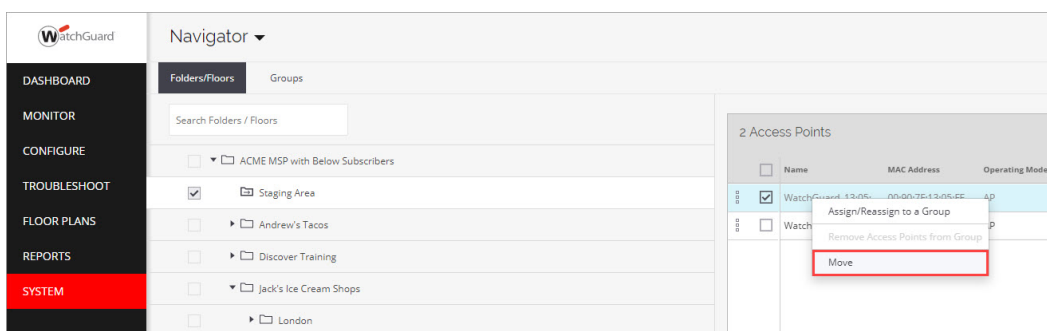
You can add new location folders and move your new APs from the **Staging Area** folder or existing APs in any folder to a new folder.

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**.




About AP Groups

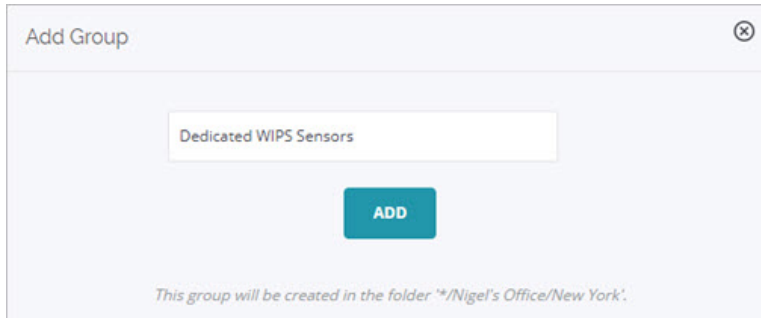
AP groups enable you to organize and manage your APs across your location tree. For example, you can apply the same configuration to APs even though they are placed in different locations and floors. This enables you to create custom configurations (SSIDs, radio, device settings, WIPS mode) for a group of APs regardless of location.

This is useful if you need to group APs based on specific device or radio settings that should not apply to other APs in a location folder.

For example, you may need to create a configuration for dual-radio APs configured as dedicated WIPS sensors, and a different configuration for dual-radio APs configured as dedicated Wi-Fi access points in your deployment.

To add a group:

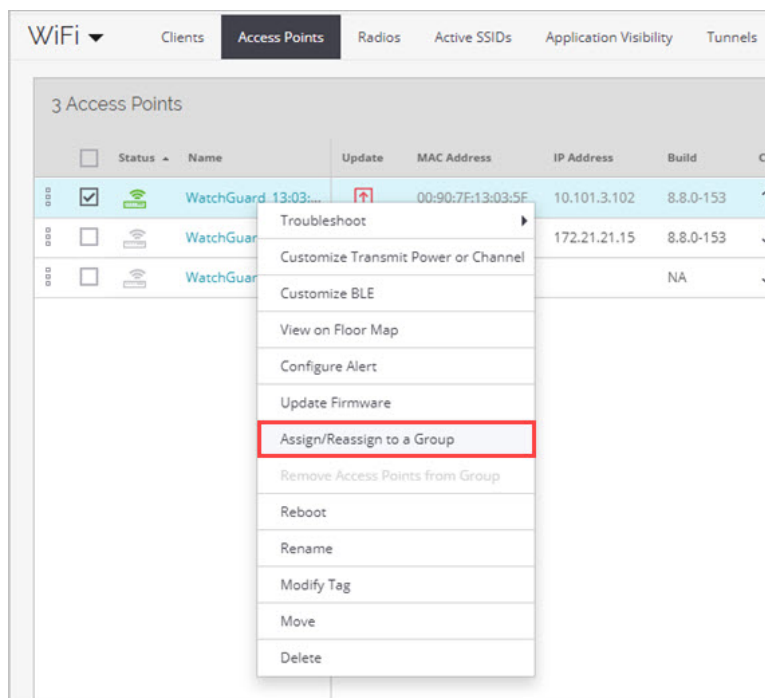
1. Select **System > Navigator > Groups**.
2. From the Navigator, select a location where you want to add the group.
3. Click the  icon to add a group.
The Add Group dialog box appears in the selected location.
4. Type a name for the group and click **Add**.



The image shows a screenshot of the 'Add Group' dialog box. The dialog has a title bar with 'Add Group' and a close button. Inside, there is a text input field containing 'Dedicated WIPS Sensors'. Below the input field is a blue button labeled 'ADD'. At the bottom of the dialog, there is a small line of text: 'This group will be created in the folder "/>

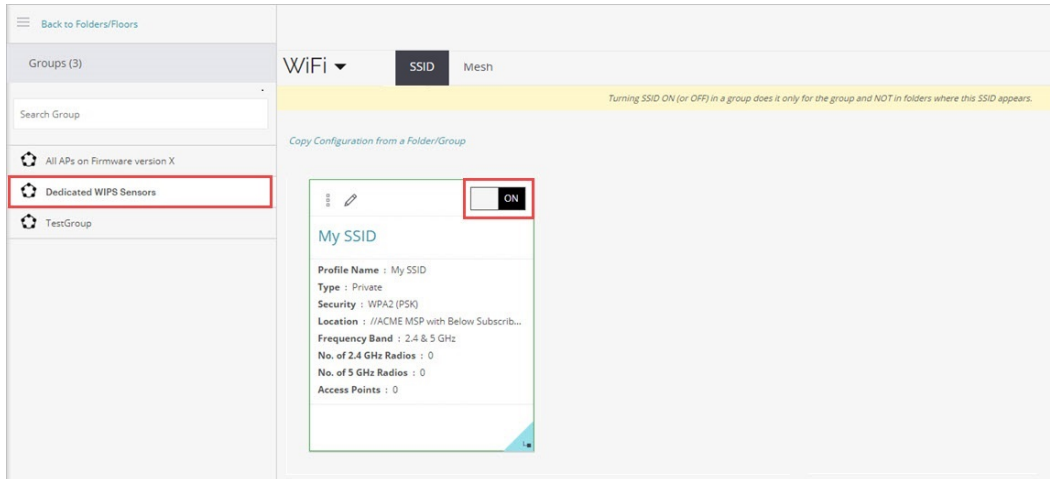
To assign an AP to a group:

1. Select **Monitor > WiFi > Access Points**.
2. From the Navigator, select a location where the AP is located.
3. Right-click an AP.
4. Select **Assign/Reassign to a Group**.
5. Select the group, then click **Assign**.



To configure a group with SSID, radio, and device settings:

1. Select **Configure > WiFi**.
2. Open the Navigator and select a location. Expand the list of groups available for that location at the bottom of the Navigator window.
3. Select the group to which you will apply the configuration.
When you select the group, the list of SSIDs on the right hand side panel is refreshed.
4. From the list of SSIDs, set the SSID you want to enable **ON**.
The configuration of the SSID will be applied to the selected AP Group.



Configure Wi-Fi Cloud WIPS

Follow these steps to configure Wi-Fi Cloud WIPS to meet the security standards for a Trusted Wireless Environment:

1. [Configure SSID Profiles](#)
2. [Configure Radio and Device Settings](#)
3. [Configure the Authorized WiFi Policy](#)
4. [Configure Access Point Auto-Classification](#)
5. [Configure Client Auto-Classification](#)
6. [Configure Automatic Intrusion Prevention](#)
7. [Monitor WIPS Activity](#)
8. [Activate Automatic Intrusion Prevention](#)

Before You Begin

These instructions assume you have already activated and connected your WatchGuard APs and have subscribed to Wi-Fi Cloud with a Total Wi-Fi or Secure Wi-Fi subscription.

For detailed information on getting started with Wi-Fi Cloud and WatchGuard cloud-ready APs, see [Getting Started with WatchGuard Wi-Fi Cloud](#).

About AP Power Requirements for WIPS

AP225W, AP325, and AP420 models must use full PoE+ power or be connected to a power adapter for the third WIPS scanning radio to be fully effective. Lower PoE power results in reduced performance and effectiveness of WIPS scanning and intrusion prevention functions. For more information, see [AP Power Requirements](#).

To make sure that LLDP-capable switches provide appropriate PoE+ power to APs:

- You must enable LLDP on the switch
- Disable static allocation of maximum power of 30W (if previously configured)

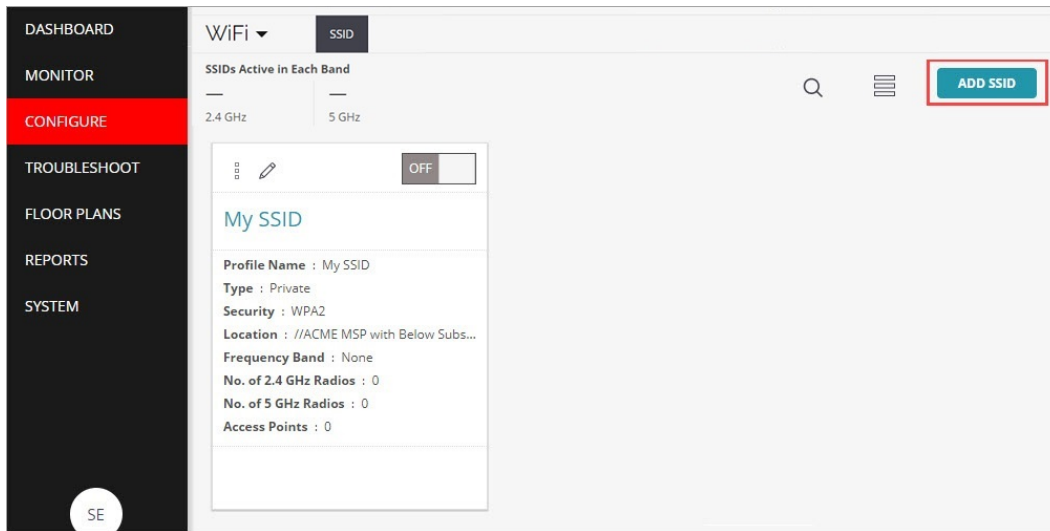
For more information, see [WatchGuard APs and PoE+ power with switches and LLDP](#).

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**.



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

Basic Settings

The screenshot shows the 'Basic Settings' page for configuring a Wi-Fi network. At the top, there is a navigation bar with tabs: 'Basic' (highlighted with a red box), 'Security', 'Network', and a menu icon. Below the navigation bar, the page is titled 'My SSID'. The main content area is divided into sections. The first section is 'Name', which contains two text input fields: 'SSID Name *' and 'Profile Name *'. Both fields are currently filled with the text 'My SSID'. Below these fields is a section titled 'Select SSID Type', which contains two radio button options: 'Private' (selected) and 'Guest'. At the bottom of the page, there is a footer bar with three buttons: 'Cancel', 'SAVE', and 'SAVE & TURN SSID ON'.

- Type a descriptive **SSID Name** and **Profile Name**.
- In the **Select SSID Type** section, select **Private** for a private Wi-Fi network SSID, or select **Guest** for a guest Wi-Fi network SSID.
- (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

← My SSID

Basic **Security** Network

Select Security Level for Associations

WPA2 PSK 802.1x

Enter a Passphrase *

☐ Mitigate WPA/WPA2 key reinstallation vulnerabilities in clients

Cancel SAVE SAVE & TURN SSID ON

- 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 are applied per location, and are automatically inherited by subfolder locations. This enables you to create a custom configuration for a specific location folder.

You can also utilize [AP Groups](#) to configure common device settings to APs located in different location folders, such as dual-radio APs configured as dedicated WIPS sensors or dedicated Wi-Fi access points in the same deployment.

To configure radio 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 > Device > Access Points**, then select the **WiFi Radios** tab.

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.

To configure device settings for your APs:

1. Select **Configure > Device > Access Points**.
2. Select the **General** tab.

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** for the 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.
 - We recommend you create a separate location folder or use [AP Groups](#) to apply these settings to dual-radio APs that are dedicated to WIPS scanning.
- **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**.
 - We recommend you create a separate location folder or use [AP Groups](#) to apply these settings to dual-radio APs that are dedicated to Wi-Fi access with no scanning.

3. In the **Device Password** section, type and confirm a **Password** for the AP.

You cannot save the device settings if the password is not defined.


Device Password

Username

config


Password *

.....



Confirm Password *

.....



4. Click **Save**.

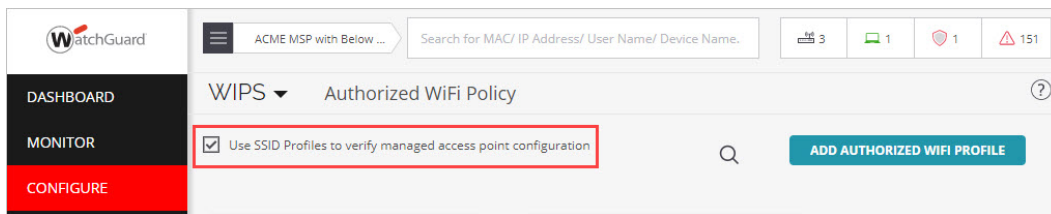
Configure the Authorized WiFi Policy

The Authorized WiFi Policy is how WIPS determines what is considered an Authorized AP on your network. The Authorized WiFi Policy specifies the SSIDs allowed to be broadcast, allowed AP vendor types, required security and encryption settings, and other settings that allow an AP to be considered “Authorized”.

WIPS identifies and continually monitors Authorized APs to make sure they conform to the access parameters you specify in your security policy.

There are two ways you can define your policy for authorized Wi-Fi access points:

- **Use SSID Profiles** – In the default configuration, the **Use SSID Profiles to verify managed access point configuration** option is selected. This option uses the settings of your SSID Profiles to validate the configuration of your APs. We recommend you use this option to simplify the security settings of your Wi-Fi deployment if you are protecting a WatchGuard AP network.

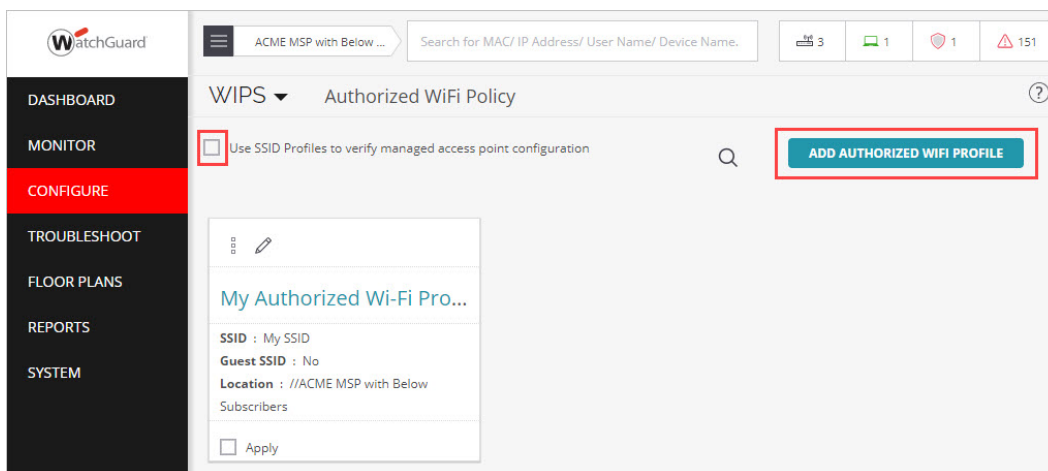


- **Use Authorized WiFi Policy** – If you want to provide specific policy settings such as allowed AP vendors or allowed networks, you can also create an **Authorized WiFi Policy** for each SSID you use. You must disable the **Use SSID Profiles to verify managed access point configuration** option to apply a new policy. We recommend you use Authorized WiFi Policies when you deploy WatchGuard APs as dedicated WIPS sensors in a third-party AP network.

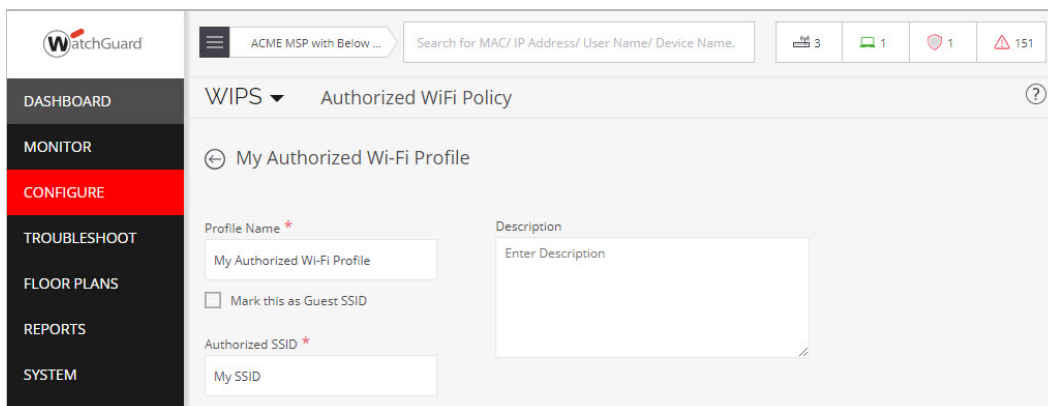
Customize an Authorized WiFi Policy

To create a custom Authorized WiFi Policy for an SSID:

1. Open Discover.
2. From the **Navigator**, select the location where the Authorized WiFi Policy will be applied. Make sure that you select the correct top-level location. Settings are inherited by subfolders automatically. If you select a subfolder that has inherited a policy, you can enable editing to customize the policy for the specific subfolder location.
3. Select **Configure > WIPS > Authorized WiFi Policy**.

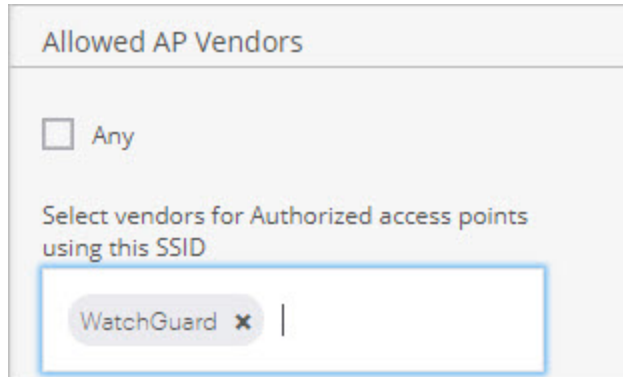


4. Clear the **Use SSID Profile to verify managed access point configuration** option if you want to create custom Authorized WiFi policies for your deployment.
5. Click **Add Authorized WiFi Profile**, or select an existing profile to edit.
6. Configure these settings in the Authorized WiFi Policy:



- Type a descriptive **Profile Name**.
- (Optional) Type a description to describe the policy.
- (Optional) Select the **Mark this as Guest SSID** check box if you intend this SSID to be used by guest users. Clear this check box for private SSIDs.

- Select the **Authorized SSID** for this policy. The list displays any SSIDs you have already deployed. You can also type the SSID name (case-sensitive). This SSID can be an SSID Profile you created in Wi-Fi Cloud to be broadcast by WatchGuard APs, or it can be an SSID broadcast by third-party APs.
- In the **Allowed AP Vendors** section, clear the **Any** check box, then select “WatchGuard” from the drop-down list if you plan to use only WatchGuard APs to broadcast this SSID. If you want to protect third-party APs, select the AP vendor that you use in your deployment.



Allowed AP Vendors

☐ Any

Select vendors for Authorized access points using this SSID

WatchGuard X |

- You can leave the other policy settings at their default values unless you have specific security policies to customize for your deployment.
7. Click **Save** to save the policy or click **Save & Apply** to save the policy and apply it to the current location.

Repeat these steps for each SSID that you want to protect.

Configure Access Point Auto-Classification

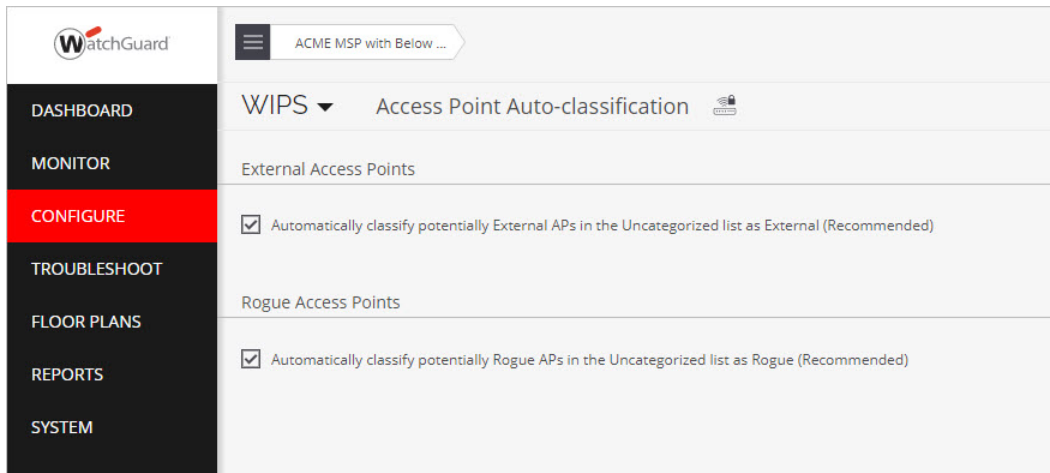
New APs are automatically assigned a classification based on their network connectivity to the monitored network and their compliance with the SSID configuration or Authorized WiFi Policy.

APs that comply with your policy are classified as “Authorized”. By default, AP auto-classification is also configured to automatically classify External APs and Rogue APs.

To review the default AP Auto-classification settings:

1. Open Discover.
2. From the **Navigator**, select the top-level folder. We recommend you set the AP auto-classification settings at the top-level folder so that the settings are inherited by all subfolders.
3. Select **Configure > WIPS > Access Point Auto-classification**.
4. By default, the **External Access Points** and **Rogue Access Points** classification options are enabled.

If required, click **Restore Defaults** to restore the default settings, then click **Save**.

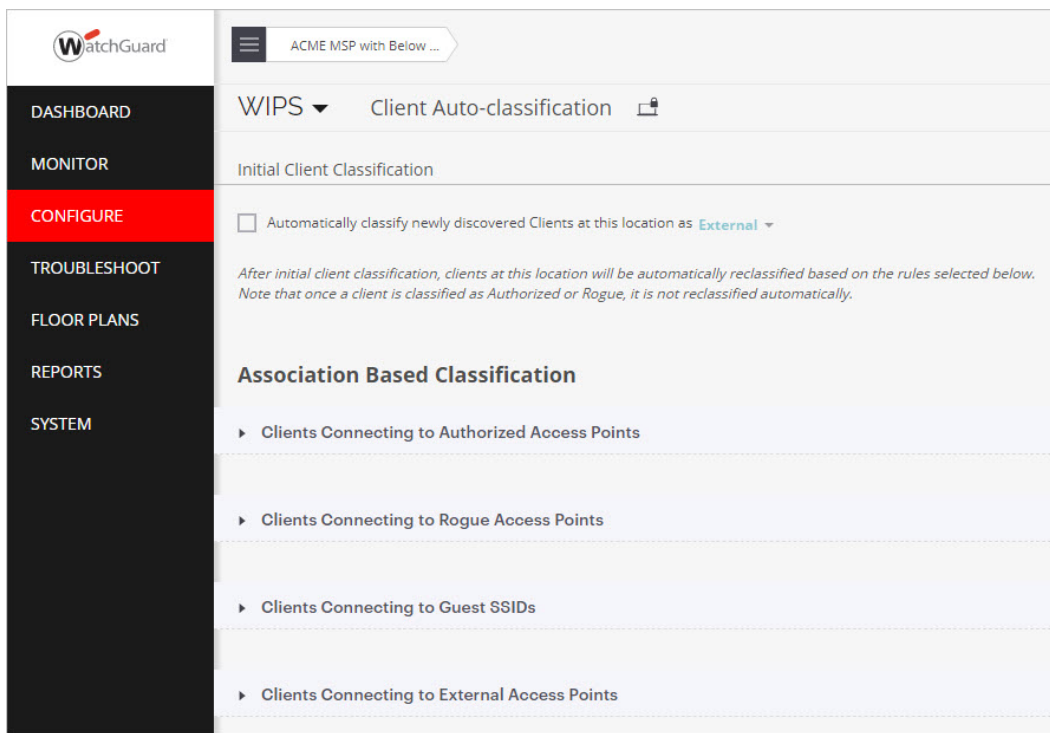


Configure Client Auto-Classification

Similar to AP auto-classification, detected wireless clients are also automatically classified based on their initial detection and subsequent behavior and AP associations.

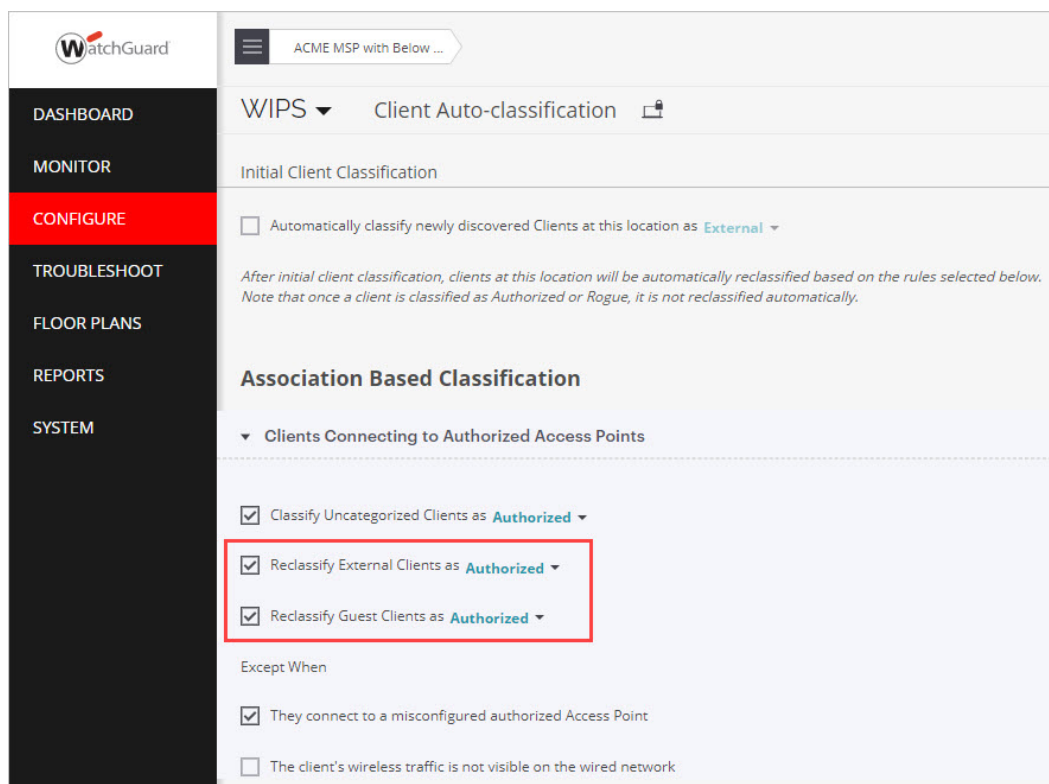
To review the client auto-classification settings:

1. Open Discover.
2. From the **Navigator**, select the top-level location folder. We recommend you set the client auto-classification settings at the top-level location so that the settings are inherited by all subfolders.
3. Select **Configure > WIPS > Client Auto-classification**.
4. Review the default settings for your deployment.
If required, click **Restore Defaults** to restore the default settings.



5. Modify these options in the **Clients Connecting to Authorized Access Points** section from the default settings:
 - Select **Reclassify External Clients as** and set the value to “Authorized”.
 - Select **Reclassify Guest Clients as** and set the value to “Authorized”.

When you first deploy WIPS, you may encounter cases where new corporate devices mistakenly connect to your Guest network or an External AP instead of an Authorized AP, and are permanently classified as Guest or External clients. To prevent this, you can reclassify the client as Authorized when it successfully connects to an Authorized AP.



WatchGuard

ACME MSP with Below ...

WIPS Client Auto-classification

Initial Client Classification

☐ Automatically classify newly discovered Clients at this location as **External** ▼

After initial client classification, clients at this location will be automatically reclassified based on the rules selected below. Note that once a client is classified as Authorized or Rogue, it is not reclassified automatically.

Association Based Classification

▼ Clients Connecting to Authorized Access Points

☒ Classify Uncategorized Clients as **Authorized** ▼

☒ Reclassify External Clients as **Authorized** ▼

☒ Reclassify Guest Clients as **Authorized** ▼

Except When

☒ They connect to a misconfigured authorized Access Point

☐ The client's wireless traffic is not visible on the wired network

You can manually change the classification of a misclassified client from the **Monitor > WIPS > Clients** page. For more information, see [Monitor WIPS Activity](#).

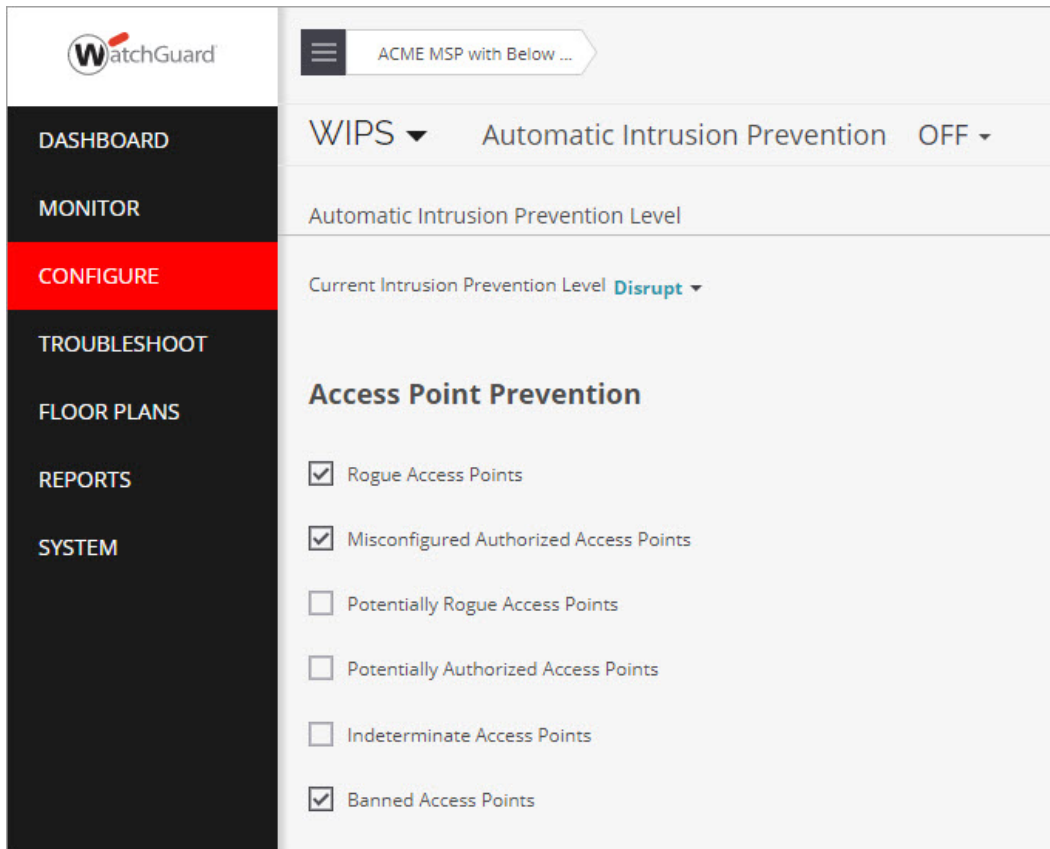
6. Click **Save**.

Configure Automatic Intrusion Prevention

The Intrusion Prevention policy settings define the types of wireless threats your Wi-Fi network is protected from. By default, Wi-Fi Cloud WIPS automatically prevents connections to APs and clients that potentially threaten your network. You can customize the Intrusion Prevention policy based on the specific requirements of your deployment.

To review Automatic Intrusion Prevention settings:

1. Open Discover.
2. From the **Navigators**, select the top-level location folder. WatchGuard recommends you set the Intrusion Prevention policy settings at the top-level folder so that the settings are inherited by all subfolder locations.
3. Select **Configure > WIPS > Automatic Intrusion Prevention**.



4. The default **Current Intrusion Prevention Level** is set to **Disrupt**.
WatchGuard recommends you use the default value to disrupt unwanted communications on any two channels on the 2.4 GHz radio and any two channels on the 5 GHz radio. You can customize the level based on your deployment, but there are trade-offs between the number of channels that you can scan and the blocking effectiveness. The more channels across which simultaneous prevention is applied, the less effective prevention will be.

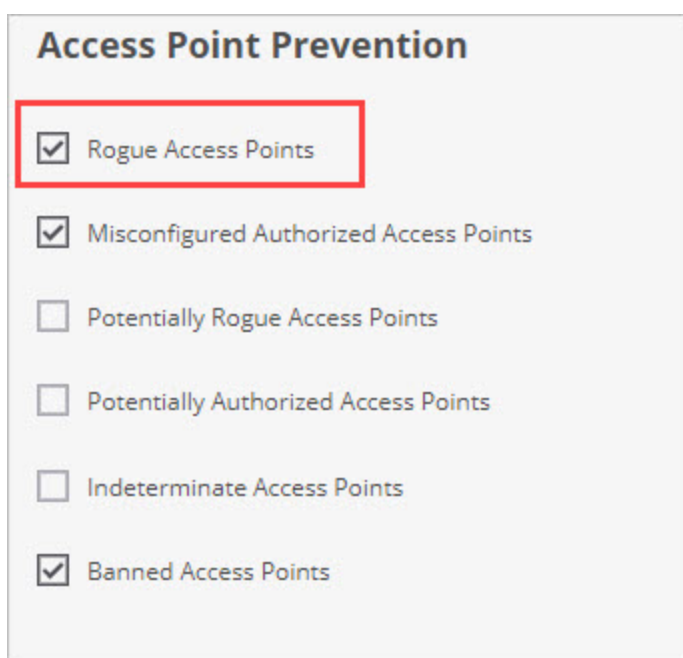
How Intrusion Prevention Stops the Six Known Wi-Fi Threat Categories

As part of your Trusted Wireless Environment, the Intrusion Prevention default settings automatically protect you from these known wireless threats, prevent your users from connecting to unauthorized Wi-Fi access points, and allow legitimate external access points to operate in the same airspace.

Rogue Access Point Protection

Rogue access points are unauthorized APs that are physically connected to the authorized network, usually with an open SSID that enables attackers to bypass perimeter security. Rogue access points can be a physical access point (AP), or a hotspot created in software on a computer and bridged to the authorized network.

By default, the Intrusion Prevention policy is already configured to prevent connections to Rogue APs.



Access Point Prevention

- ☒ Rogue Access Points
- ☒ Misconfigured Authorized Access Points
- ☐ Potentially Rogue Access Points
- ☐ Potentially Authorized Access Points
- ☐ Indeterminate Access Points
- ☒ Banned Access Points

Rogue Client Protection

Rogue clients are clients that connected to a rogue AP or other malicious AP within the range of the private wireless network. This client could have been victimized by man-in-the-middle attacks, ransomware, viruses and malware, or backdoor software installation.

By default, Rogue Clients are not permitted to connect to Authorized APs. You can also enable these Intrusion Prevention settings for Rogue Clients:

- Prevent Rogue Client connection to Guest APs
- Prevent Rogue Client in Bridging/ICS configuration or part of an Ad Hoc network

Client Prevention	
<p>▶ Authorized Client Misassociation</p> <hr/> <p>▶ Guest Client Misassociation</p> <hr/> <p>▶ Unauthorized Associations to Authorized Access Points</p> <hr/> <p>▼ Unauthorized Associations to Guest SSIDs</p> <hr/> <p><input checked="" type="checkbox"/> Rogue Client Connection to a Guest Access Point</p> <p><input type="checkbox"/> Uncategorized Client Connection to a Guest Access Point</p> <p><input type="checkbox"/> External Client Connection to a Guest Access Point</p>	<p>▼ Client Bridging/ICS (for all connections of the Client)</p> <hr/> <p><input checked="" type="checkbox"/> Authorized Client in Bridging/ICS Configuration</p> <p><input checked="" type="checkbox"/> Guest Client in Bridging/ICS Configuration</p> <p><input checked="" type="checkbox"/> Rogue Client in Bridging/ICS Configuration</p> <p><input type="checkbox"/> External/Uncategorized Client in Bridging/ICS Configuration</p> <p><input checked="" type="checkbox"/> Bridging/ICS Client Connected to Enterprise Monitored Subnet</p> <hr/> <p>▼ Ad Hoc Connections</p> <hr/> <p><input checked="" type="checkbox"/> Authorized Client Participating in an Ad Hoc Network</p> <p><input type="checkbox"/> Guest Client Participating in an Ad Hoc Network</p> <p><input checked="" type="checkbox"/> Rogue Client Participating in an Ad Hoc Network</p>

Neighbor AP Protection

A Neighbor access point is an External AP that is not managed or under the control of your network. These neighbor APs are located in close proximity to your authorized wireless network but are not connected to your network.

Company-managed Wi-Fi clients must never be allowed to connect to nearby third-party or neighbor SSIDs. This enables clients to bypass important network security controls.

By default, authorized client connections to External (Neighbor) APs are not permitted.

Client Prevention

▼ Authorized Client Misassociation

Prevent a client from connecting to:

☐ Guest SSID

☒ External or Potentially External Access Point

☒ Indeterminate Access Point

☒ Disallowed SSID

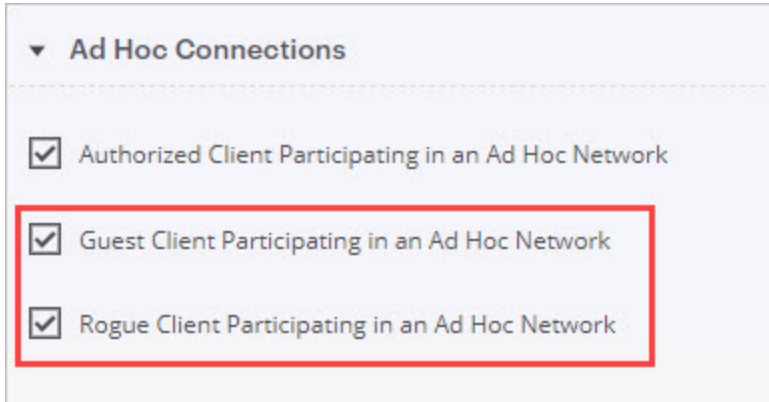
Ad-Hoc Connection Protection

An Ad-hoc Connection is a peer-to-peer Wi-Fi connection between clients that can circumvent perimeter security and allow clients to evade firewalls, content controls, and security policies.

By default, Authorized Clients cannot participate in an ad-hoc network.

In addition, you can optionally enable these settings for greater security:

- Guest Clients participating in any ad-hoc network
- Rogue Clients participating in any ad-hoc network



Evil Twin AP Protection

An Evil Twin access point mimics a legitimate AP by spoofing its SSID and unique MAC address. This can be a physical access point, or attackers can use software that uses Wi-Fi network adapters in laptops and mobile devices to create a hotspot.

By default, Threat Prevention blocks Authorized Client connections to Honeypot/Evil Twin APs.

In addition, you can optionally enable **MAC Spoofing** protection to prevent spoofing of any Authorized AP's MAC address.

Prevent the following threats:

MAC Spoofing

☒ Spoofing of an Authorized Access Point MAC address

Honeypot/Evil Twin Access Points

☒ Authorized client connecting to Honeypot/Evil Twin Access Points

Misconfigured AP Protection

Misconfigured access points are APs connected to your private network with a configuration that does not conform to your Authorized WiFi Policy and allows insecure connections. For example, if your security policy is configured to only allow SSIDs to broadcast on your authorized APs with WPA2 encryption, and an administrator accidentally misconfigures an authorized AP to broadcast an open, unencrypted SSID, that AP would be considered misconfigured.

By default, connections to Misconfigured Authorized APs are blocked.

Access Point Prevention

- ☒ Rogue Access Points
- ☒ Misconfigured Authorized Access Points
- ☐ Potentially Rogue Access Points
- ☐ Potentially Authorized Access Points
- ☐ Indeterminate Access Points
- ☒ Banned Access Points

Monitor WIPS Activity

Before you activate Automatic Intrusion Prevention, it is critical that you monitor WIPS classifications and security events and adjust your WIPS policy as required. We recommend you monitor your network for a period of several days to make sure APs and clients are properly classified and the wireless network is stable before you enable prevention.

Monitor AP Classifications

To monitor WIPS classifications for your APs, in Discover, select **Monitor > WIPS > Access Points**.

Classification	Status	Name	MAC Address	Prevention Status	Is Networked	Network	Active/Inactive Since	First Detected At	Location	RSSI (dBm)	Channel
Authorized	Active	WatchGuard_13.05...	00:90:7F:13:05:FF	--	--	--	↑ Jul 2	May 22	//ACME MSP with Belo...	-90	6
Authorized	Active	WatchGuard_13.03...	00:90:7F:13:03:5F	--	--	--	↑ Jun 17	May 21	*//Matthew's Software ...	0	40,6
Rogue	Inactive	WatchGuard_ED00...	00:90:7F:ED:00:70	--	No	--	↓ Jul 2	Jun 25	//ACME MSP with Belo...	--	--
External	Active	Netgear_71:71:38	A0:04:60:71:71:38	--	No	--	↑ Jun 27	Jun 27	*//Matthew's Software ...	-66	44

The color coding makes it easy to view AP classifications:

- Authorized APs (Green)
- Guest APs (Light Green)
- Misconfigured APs (Orange)
- Rogue APs (Red)
- External Neighbor APs (Blue)
- Uncategorized (White)

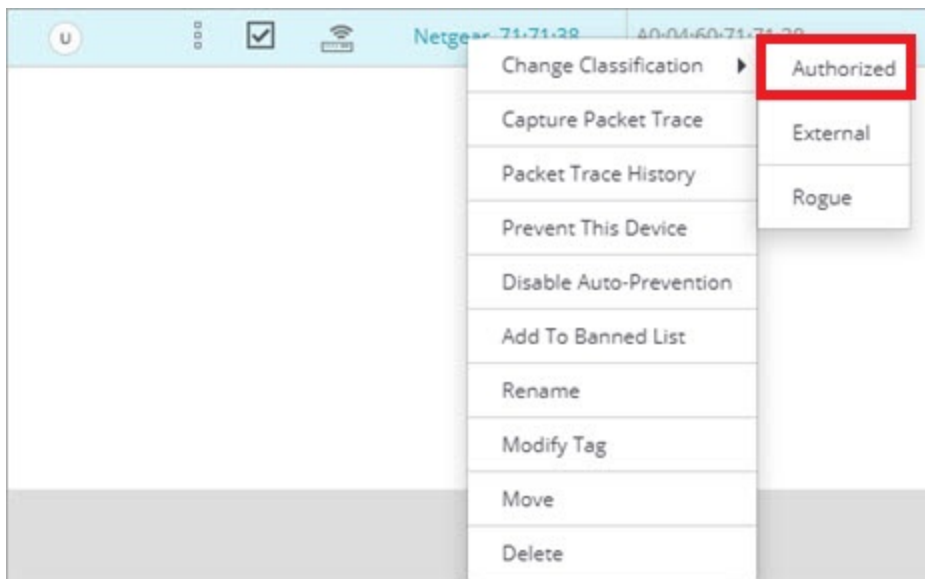
This enables you to correct misconfigured APs, make sure your known APs are classified as authorized, and confirms that external and rogue APs are correctly identified.

Change AP Classification

If a known AP in your environment is classified as **Misconfigured**, this means the AP has a configuration that does not conform to your SSID Profiles or Authorized WiFi Policy. This can occur if the AP has been reset or tampered with, or if there is a configuration error or change in your SSID settings or Authorized WiFi Policy. Verify the configuration of the AP to make sure it conforms to your policies.

If you have known APs that are listed as **Uncategorized**, you can manually set the classification category of the AP to set it as **Authorized**. Make sure you verify the location and configuration of the device before you change an AP classification category.

1. Open Discover.
2. Select **Monitor > WIPS > Access Points**.
3. Right-click the AP that is classified as **Uncategorized**.
4. Select **Change Classification**.
5. Select **Authorized**.



You can perform this procedure for other misclassified APs, but to prevent security vulnerabilities on your wireless network, you must make sure that the AP is a known AP connected to your network and the configuration conforms to your security policies.

Monitor Client Classifications

To monitor WIPS classifications for your clients, in Discover, select **Monitor > WIPS > Clients**.

The screenshot shows the WatchGuard WIPS interface. The left sidebar contains navigation links: DASHBOARD, MONITOR (highlighted), CONFIGURE, TROUBLESHOOT, FLOOR PLANS, REPORTS, and SYSTEM. The main content area is titled 'WIPS' and shows 'Managed WiFi Devices', 'Access Points', 'Clients' (selected), and 'Networks'. A search bar is at the top right. Below the search bar, there are filters for 'Authorized' (green), 'Guest' (light green), 'Rogue' (red), 'External' (blue), and 'Uncategorized' (grey). The table below lists 19 clients with columns for Classification, Status, Name, User Name, MAC Address, IP Address, OS, Associated Access Point, Associated SSID, Protocol, and Channel.

Classification	Status	Name	User Name	MAC Address	IP Address	OS	Associated Access Point	Associated SSID	Protocol	Channel
Authorized	On	Intelorante_E2AC3E	--	1C1B85E2AC3E	--	--	--	--	ac	--
Guest	On	DESKTOP-83CPRAN	--	5C35D4A65D3D	172.20.20.52	--	--	--	b g n	--
External	On	Intel Corporate_9B850F	--	8B811198850F	--	--	--	--	ac	--
Rogue	On	Intel Corporate_905ED4	--	60F677905ED4	--	--	--	--	b g n	--
External	On	Intelorante_8DFB3C	--	645D868DFB3C	--	--	--	--	ac	--
Uncategorized	On	Apple_14E9E0	--	D0034B14E9E0	--	--	--	--	ac	--
Guest	On	Rivet-Networks_EE96C7	--	9C86D0EE96C7	--	--	--	--	b g	--
Rogue	On	Vizio_BF9FB3	--	C41CFFBF9FB3	--	--	--	--	b g n	--

The color coding makes it easy to view client classifications:

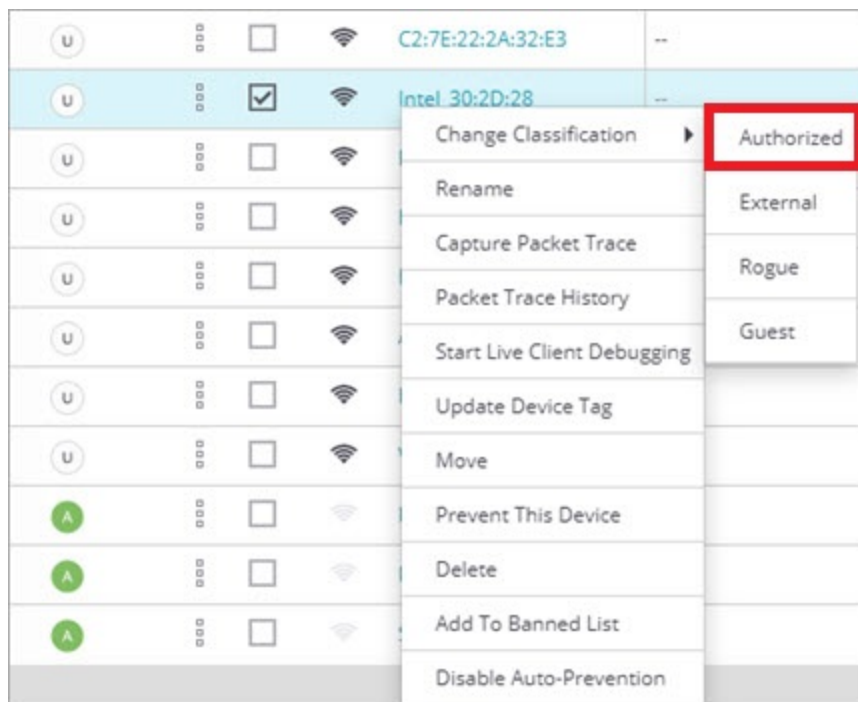
- Authorized Clients (Green)
- Guest Clients (Light Green, connected to an authorized guest network)
- Rogue Client (Red)
- Misbehaving Clients (Orange)
- External Neighbor Clients (Blue)

This enables you to make sure clients are properly classified and helps you detect any rogue or external clients connected to your Wi-Fi network.

Change Client Classification

You can manually change the classification of a client if it is **Uncategorized** or incorrectly classified. Before you perform this action, make sure that the client is a known client to prevent security vulnerabilities on your wireless network.

1. Open Discover.
2. Select **Monitor > WIPS > Clients**.
3. Right-click the client, then select **Change Classification**.
4. Select **Authorized**.



Configure and Monitor WIPS Security Alerts

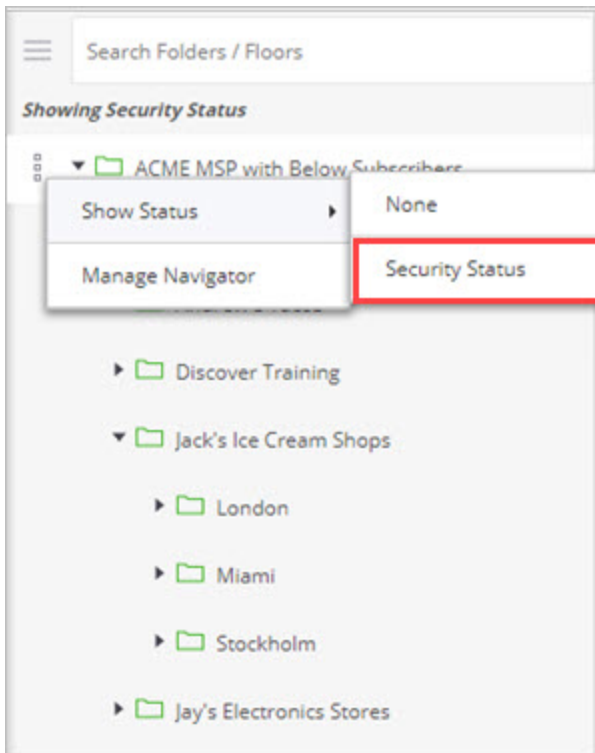
In Discover, you can configure and monitor WIPS alerts to see detailed information about rogue APs, rogue clients, and other security-related events for your Wi-Fi network.

There are three methods for alert notification in Discover:

- **Email** – An email about the alert is sent to the recipients configured in the **Email Recipients** tab of the **Alerts** configuration page.
- **Display** – The alert is displayed on the **Monitor > Alerts** page and on the respective widgets in Discover.
- **Syslog** – Discover sends alert events to the syslog servers configured in **System > Third-party Servers > Syslog**.

You can also set the **Security Status** for alerts. For *WIPS* and *System* events, select the **Affects Security Status** option to enable an alert to change the security status of a device's location.

In the location tree, you can view the security status of a location by the color code. **Red** indicates a location with a live security alert to indicate a vulnerable device. **Green** indicates no live security alerts for that location. To view the security status in the location tree, select **Show Status > Security Status** for the top-level location folder.



Configure WIPS Alerts

To configure WIPS alerts:

1. Open Discover.
2. Select **Configure > Alerts**.
3. In the *Alert Category* pane, expand the **WIPS** section.
4. For each type of WIPS event, review your alert notification settings, then click **Save**.

The screenshot shows the WatchGuard web interface for configuring alerts. The left sidebar contains navigation links: DASHBOARD, MONITOR, CONFIGURE (highlighted), TROUBLESHOOT, FLOOR PLANS, REPORTS, and SYSTEM. The main content area is titled 'Alerts' and includes a search bar and tabs for 'Configure Alerts' and 'Email Recipients'. Under the 'WIPS' section, several alert categories are listed: Rogue AP, Misconfigured AP, Misbehaving Clients, Man-in-the-middle, MAC Spoofing, Ad Hoc Network, Prevention, DoS, and Reconnaissance. The 'Rogue AP' category is expanded, showing five sub-alerts with their respective notification settings and severity levels.

Alert Category	Display	Email	Notify	Affects Security Status	Severity
Unauthorized AP operating on non-allowed channel	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low
Banned AP active	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High
Rogue AP active	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High
Offline mode: Rogue AP detected	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low
Indeterminate AP active	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Medium

Monitor WIPS Alerts

To monitor WIPS alerts:

1. Open Discover.
2. Select **Monitor > Alerts**, then select the **WIPS** tab.

ID	Severity	Status	Summary	Affects Security Status	Category	Location	Start Time	Stop Time
644	Medium	●	Indeterminate AP [WatchGuard_34-4E:F0] is active.	No	Rogue AP	*Matthew's Softwar...	Jul 3, 2019 9:29 PM	Jul
643	Medium	●	Indeterminate AP [WatchGuard_F4:13:50] is active.	No	Rogue AP	*Matthew's Softwar...	Jul 3, 2019 6:24 PM	Jul
642	Medium	●	Indeterminate AP [WatchGuard_F5:00:D0] is active.	No	Rogue AP	*Matthew's Softwar...	Jul 3, 2019 5:16 PM	Jul
641	Low	●	An Ad hoc network [] involving two or more non-authorized Clients is active.	No	Ad Hoc Network	*Matthew's Softwar...	Jul 3, 2019 2:36 PM	Jul
640	Low	●	An Ad hoc network [] involving two or more non-authorized Clients is active.	No	Ad Hoc Network	*Matthew's Softwar...	Jul 3, 2019 12:46 PM	Jul
639	Medium	⊙	Indeterminate AP [Netgear_71:71:38] is active.	No	Rogue AP	*Matthew's Softwar...	Jul 3, 2019 11:04 AM	Jul
638	Medium	●	Indeterminate AP [92:F0:6B:B6-AB-D6] is active.	No	Rogue AP	*Matthew's Softwar...	Jul 3, 2019 10:48 AM	Jul

You can filter the events based on the security category type.

Affects Security Status	Category	Location	Start Time	Stop Time
No	All	*Matthew's Softwar...	Jul 3, 2019 9:29 PM	Jul
No	All	*Matthew's Softwar...	Jul 3, 2019 6:24 PM	Jul
No	All	*Matthew's Softwar...	Jul 3, 2019 5:16 PM	Jul
No	All	*Matthew's Softwar...	Jul 3, 2019 2:36 PM	Jul
No	All	*Matthew's Softwar...	Jul 3, 2019 12:46 PM	Jul
No	All	*Matthew's Softwar...	Jul 3, 2019 11:04 AM	Jul
No	All	*Matthew's Softwar...	Jul 3, 2019 10:48 AM	Jul

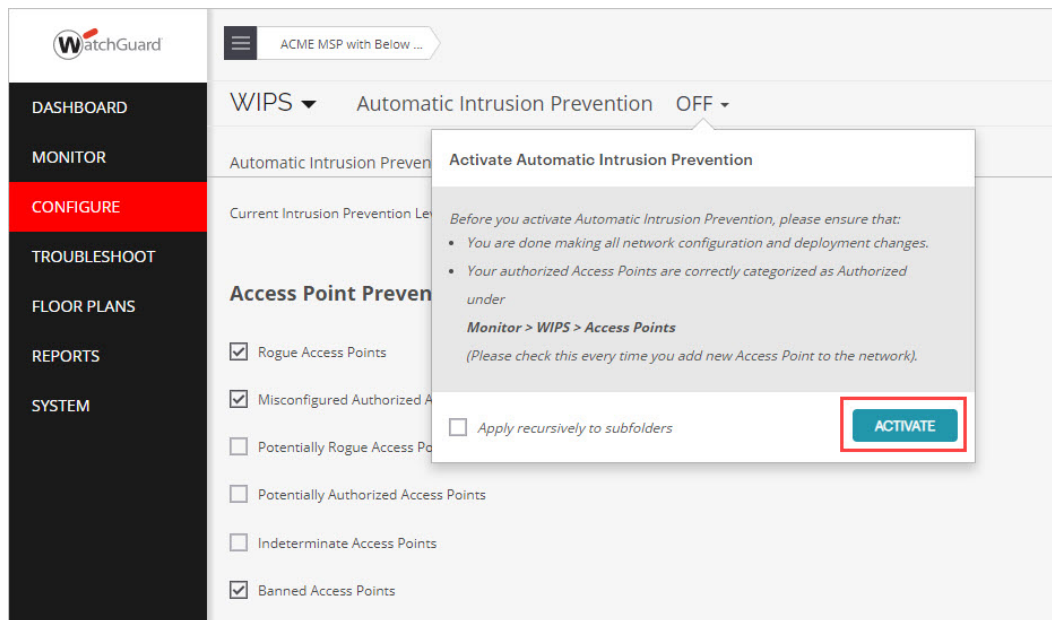
Activate Automatic Intrusion Prevention

When your Wi-Fi network devices are correctly classified, and you have determined over a period of several days that your network is stable, you can then activate Automatic Intrusion Prevention to allow WIPS to take active prevention against wireless threats.

Intrusion Prevention is disabled by default, and you must activate the feature for a location before your Intrusion Prevention policy settings take effect.

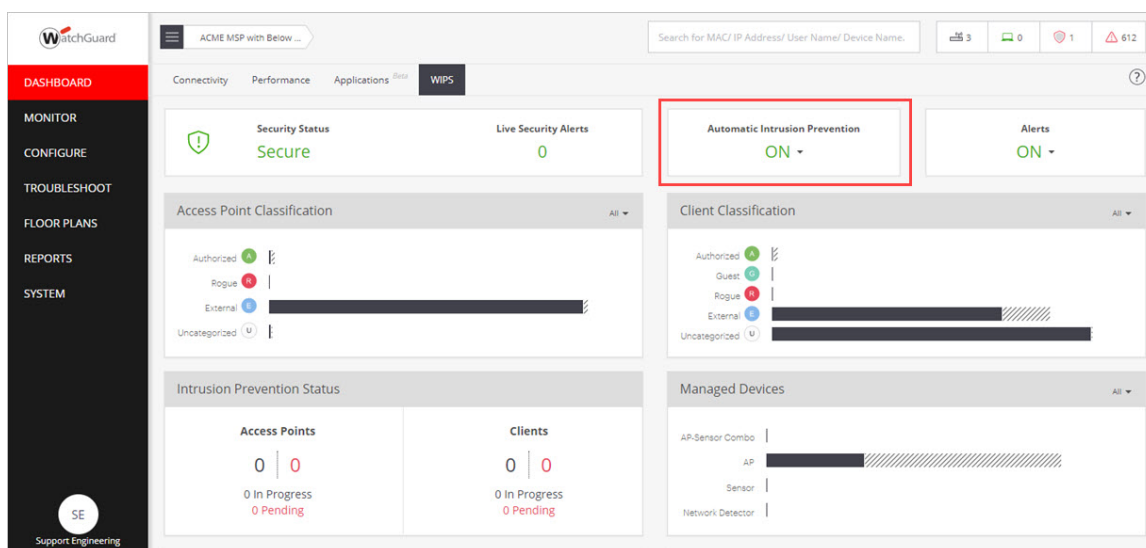
To activate Intrusion Prevention for a location:

1. Open Discover.
2. From the **Navigator**, select the location where you want to enable Intrusion Prevention. Make sure this location folder contains the APs that you want to protect with WIPS. Intrusion Prevention activation settings are location-specific and cannot be inherited from a parent location, but you can apply Intrusion Prevention activation recursively to subfolders of the current location when you save the settings.
3. Select **Configure > WIPS > Automatic Intrusion Prevention**.



4. Select the **Automatic Intrusion Prevention** drop-down.
5. (Optional) Select the **Apply recursively to subfolders** check box if you want this action to apply to all subfolders of your current location folder.
6. Click **Activate**.

You can also enable Automatic Intrusion Prevention directly from the **Dashboard** page on the **WIPS** tab.



Test Intrusion Prevention

When you have activated Intrusion Prevention for a location, you can perform a simple test to make sure that WIPS is functioning correctly.

In this example, to test the Neighborhood APs threat, you will attempt to connect to a mobile hotspot classified as an External AP with an Authorized client. Authorized clients must not be able to connect to external neighbor APs in the vicinity of your Wi-Fi network.

1. Create a mobile hotspot on a personal device that will act as the External access point.

When the hotspot is enabled, the hotspot device should be classified as an External device and appear in blue on the **Monitor > WIPS > Access Points** page in Discover.

Classification	Status	Name	MAC Address	Prevention Status
E	---	Apple_EC:53:08	0C:51:01:EC:53:08	---
A	---	WatchGuard_F4:1B:...	00:90:7F:F4:1B:10	---
A	---	WatchGuard_F5:0D:...	00:90:7F:F5:0D:E2	---
A	---	WatchGuard_38:EC:...	00:90:7F:38:EC:C2	---

2. Make sure the wireless client that you want to test with is classified as an Authorized client.

To become an Authorized client, you must have previously connected to an Authorized AP on your network. The client should appear in green in the **Monitor > WIPS > Clients** page in Discover.

To find the specific client, search for the device name or MAC address using the page filters.

Classification	Status	Name	User Name	MAC Address	IP Address	OS	Associated Access Point	Associated SSID	Protocol	Client
A	---	SAMSUNG-SM-G950U	---	B0:72:BF:EC:F3:C7	172.20.20.40	Android	---	8C	---	---

3. From your Authorized client, attempt to connect to the SSID broadcast by the mobile hotspot classified as External. The connection should be prevented.

In the **Monitor > WIPS > Clients** page in Discover, you should see that the client has been classified as a misbehaving client and is displayed in orange. After a short time, the client will be released from quarantine and reconnected to an Authorized AP.

To see the related security event in Discover, select **Monitor > Alerts > WIPS**. The event logs should indicate a misbehaving client event.



ID	Severity	Status	Summary	Affects Security Status	Category	Location	Start Time	Stop Time
577	High	🔴	Client [Galaxy-Tab-S2] needs to be quarantined.	No	Prevention	*/Matthew's Softwar...	Jun 24, 2019 7:22 AM	
578	Low	🟡	Authorized Client [Galaxy-Tab-S2] is connected to a non-authorized AP.	No	Misbehaving Clients	*/Matthew's Softwar...	Jun 24, 2019 6:55 AM	

If the client was not correctly prevented from connecting to the External AP, check the following:

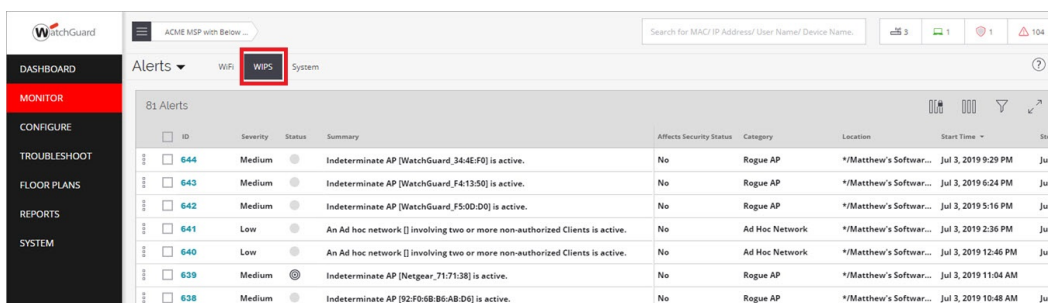
- Make sure you are in the vicinity of a dedicated WIPS sensor and that it is correctly powered. AP325 and AP420 devices require PoE+ power or a power adapter for best effectiveness when they operate as a WIPS sensor.
- Make sure Intrusion Prevention is enabled in the correct location.
- Make sure the option to prevent Authorized Client connection to **External or Potentially External Access Point** is enabled in your Intrusion Prevention settings. This option is enabled by default.
- Make sure the hotspot AP is correctly classified as External and the client is correctly classified as Authorized before you attempt a connection.
- Check the WIPS alerts for any related security events.

Monitor WIPS Alerts

After you have enabled Automatic Intrusion Prevention, continue to monitor WIPS alerts as described in the [Monitor WIPS Activity](#) section for potential security or configuration issues.

To monitor WIPS alerts:

1. Open Discover.
2. Select **Monitor > Alerts**, then select the **WIPS** tab.



ID	Severity	Status	Summary	Affects Security Status	Category	Location	Start Time	Stop Time
644	Medium	🟡	Indeterminate AP [WatchGuard_3A4E:F0] is active.	No	Rogue AP	*/Matthew's Softwar...	Jul 3, 2019 9:29 PM	Jul
643	Medium	🟡	Indeterminate AP [WatchGuard_F413:50] is active.	No	Rogue AP	*/Matthew's Softwar...	Jul 3, 2019 6:24 PM	Jul
642	Medium	🟡	Indeterminate AP [WatchGuard_F50D:D0] is active.	No	Rogue AP	*/Matthew's Softwar...	Jul 3, 2019 5:16 PM	Jul
641	Low	🟢	An Ad hoc network [] involving two or more non-authorized Clients is active.	No	Ad Hoc Network	*/Matthew's Softwar...	Jul 3, 2019 2:36 PM	Jul
640	Low	🟢	An Ad hoc network [] involving two or more non-authorized Clients is active.	No	Ad Hoc Network	*/Matthew's Softwar...	Jul 3, 2019 12:46 PM	Jul
639	Medium	🟡	Indeterminate AP [Netgear_7171:38] is active.	No	Rogue AP	*/Matthew's Softwar...	Jul 3, 2019 11:04 AM	Jul
638	Medium	🟡	Indeterminate AP [92:F0:6B:B6:AB:D6] is active.	No	Rogue AP	*/Matthew's Softwar...	Jul 3, 2019 10:48 AM	Jul