WatchGuard AP

Deployment Guide

About this Guide

The *WatchGuard AP Deployment Guide* is a guide for deployment of a WatchGuard AP device with a Firebox. For the most recent product documentation, see the *Fireware XTM WatchGuard System Manager Help* or *Fireware Web UI Help* on the WatchGuard website at http://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: 1/29/2016

Copyright, Trademark, and Patent Information

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

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader of integrated, multi-function business security solutions that intelligently combine industry standard hardware, best-of-breed security features, and policy-based management tools. WatchGuard provides easy-to-use, but enterprise-powerful protection to hundreds of thousands of businesses worldwide. WatchGuard is headquartered in Seattle, Wash. with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

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

Table of Contents

Introduction

The mass adoption of smart wireless devices such as tablets, smart phones and notebooks, has greatly increased the demand for wireless access to most networks. WatchGuard AP devices enable you to add wireless access to the networks that are protected by your Firebox.

To add wireless access to your network, you can simply connect one or more WatchGuard AP devices to a trusted, optional, or custom network on your Firebox. Then you use the Gateway Wireless Controller on the Firebox to discover, configure, and manage the AP devices. The network security policies already configured on your Firebox automatically apply to wireless users.

> The AP device can be located on the custom zone network (for Fireware OS v11.9 and higher). To allow the Gateway Wireless Controller to discover an AP device on a custom zone network, you must modify the *WatchGuard Gateway Wireless Controller* policy to allow traffic from the custom zone.

You can then configure the AP device and SSIDs to meet the requirements of your wireless network.

- To increase the wireless range of your network and support wireless roaming you can use the same SSID on multiple AP devices.
- To support different groups of wireless users, you can configure your AP device to use more than one wireless SSIDs.
- You can optionally enable VLAN tagging in your SSIDs, and then use the VLANs in your policies to create more specific rules for your wireless users, based on the SSID that they connect to.

> The procedures in this document describe how to use Fireware Web UI to configure your Firebox and AP device. You could also use Policy Manager to complete these steps.

This document includes the information you must know for the initial deployment of a WatchGuard AP device on your network. For a more comprehensive reference to all AP device functionality, see the *Fireware Help*.

WatchGuard AP Device Requirements and Limitations

Before you add a WatchGuard AP device to your network, it is important to understand the requirements and limitations of the AP device.

Requirements

- The WatchGuard AP device must be managed by a WatchGuard Firebox that uses Fireware OS v11.7.2 or higher for AP100, AP102, and AP200, and v11.10.5 or higher for AP300.
- The Firebox must be configured in mixed routing mode.
- The AP device must connect to a trusted, optional, or custom network.
- The Firebox configuration must include a policy that allows NTP traffic from the AP device to the Internet. The AP device uses an NTP server to set the correct local time.
- The Firebox and AP devices on your network require access to WatchGuard servers (*.watchguard.com) on port 443. This allows the Gateway Wireless Controller on the Firebox to register and activate AP devices, and check for new firmware updates. AP devices require access to WatchGuard servers to obtain country and regional information.

Limitations

- You cannot use a WatchGuard Management Server to manage WatchGuard AP devices.
- You cannot locate WatchGuard AP devices behind a NAT firewall.
- A WatchGuard Gateway Wireless Controller is designed to manage multiple WatchGuard AP devices. If you experience management performance issues as you add more AP devices to your network, you can use another Gateway Wireless Controller instance on another Firebox to manage these AP devices.
- We recommend a maximum of 20-40 associated wireless clients per radio based on the overall airtime demand of the clients.

AP Device Deployment Steps

When you add one or more WatchGuard AP devices to your network, you can manage and configure the AP devices from the Gateway Wireless Controller on your Firebox. You do not have to connect directly to the AP device to configure it. The Gateway Wireless Controller on your Firebox manages the AP device for you.

To deploy any AP device on your Firebox network you must:

1. Enable the Gateway Wireless Controller on your Firebox.
2. Connect the AP device to your network.
3. Configure SSIDs.
4. Pair the AP device with your Firebox.
5. Configure the AP device settings.

You can optionally enable VLAN tagging in the SSIDs for your AP device. If you enable VLAN tagging, you must also configure the necessary VLANs on your Firebox.

This *AP Deployment Guide* describes the basic steps necessary to deploy an AP device on your network. For a more detailed description of the configuration settings, see the *Fireware Help*.

Benefits of VLANs for Your AP Device

To deploy an AP device on your network, you do not have to enable VLAN tagging. There are, however, several reasons you could want to enable VLAN tagging:

You want to configure different firewall policies for SSIDs that connect to the same network

If you configure more than one SSID for your AP devices, and you want to set different firewall policies for each SSID, you can enable VLAN tagging in the SSID and then use the VLAN ID associated with each SSID in policies specific to each SSID.

For example, you could add a different HTTP policy for each SSID that specifies the VLAN associated with that SSID. This enables you to specify which users can connect to each SSID.

You want to separate the traffic on the same physical network to different logical networks.

If you have several AP devices connected to the same physical network, VLAN tagging gives you the ability to separately examine traffic for wireless clients connected to each SSID.

For example, if you run a network analyzer, you can use the VLAN tags to see the traffic for the VLAN ID associated with an SSID.

Or, you might want to set up all of your AP devices with one SSID for the trusted network, and a different SSID for the optional network. You can set up a trusted VLAN and an optional VLAN to separate the traffic for the trusted and optional wireless clients.

The subsequent sections provide a more detailed overview of the steps to deploy an AP device without VLAN tagging. For more information about VLANs and for configuration examples, see the *WatchGuard System Manager Help*.

Step 1 – Enable the Gateway Wireless Controller

Before your Firebox can discover and manage your AP devices, you must enable the Gateway Wireless Controller.

1. From Fireware Web UI, select **Network > Gateway Wireless Controller**.

2. Select the **Enable the Gateway Wireless Controller** check box.
   The WatchGuard AP Passphrase dialog box appears.
3. In the **WatchGuard AP Passphrase** text box, type the passphrase that you want all your AP devices to use after they are paired.
4. Click **OK**.
5. Save the Firebox configuration.

Step 2 – Connect the AP Device

Use one of these options to connect the AP device to your trusted, optional, or custom network.

> To allow the Gateway Wireless Controller to discover an AP device on a custom zone network, you must modify the WatchGuard Gateway Wireless Controller policy to allow traffic from the custom zone.

By default, the AP device automatically requests an IP address from a DHCP server on the local network. If the network you connect your AP device to does not use DHCP, you can use the web UI on the AP device to manually assign a static IP address to the AP device before you connect it to your network.

Option 1 – Connect the AP Device to a Firebox Interface

If you have an unused interface on your Firebox, you can connect the AP device directly to a trusted, optional, or custom interface on your Firebox.
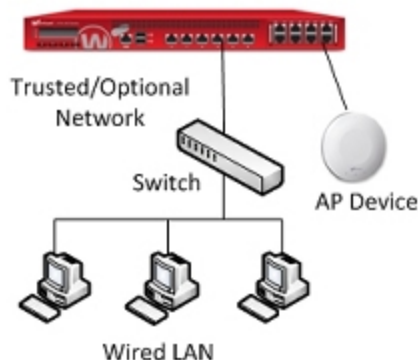
AP device connected to the Firebox

To configure the Firebox interface:

1. From Fireware Web UI, select **Network > Interfaces**.
2. Configure the Firebox interface as trusted, optional, or custom, and enable DHCP on that interface.
3. Save the configuration.
4. Connect the AP device to the interface you configured.

Option 2 – Connect the AP device to a Switch

You can connect the AP device to the switch on your trusted, optional, or a custom network. When you use this option, you do not have to change the network settings on the Firebox interface.
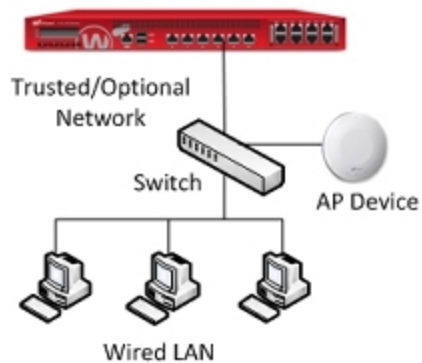
AP device connected to a switch

Step 3 – Configure SSIDs

When you configure the SSIDs that your wireless user connect to, you must select a wireless security mode for the SSID. By default, the security mode for an SSID is set to **Disabled**. In this mode, the SSID operates as an open wireless network. You can change this to one of the WPA or WPA2 security modes that use pre-shared keys (PSK) or enterprise RADIUS authentication.

- WPA only (PSK)
- WPA2 only (PSK)
- WPA/WPA2 (PSK)
- WPA Enterprise
- WPA2 Enterprise
- WPA/WPA2 Enterprise

To configure the SSIDs for your device:

1. From Fireware Web UI, select **Network > Gateway Wireless Controller**.
2. On the **SSIDs** tab, click **Add**.
   The Add SSID dialog box appears.
3. In the **Network Name (SSID)** text box, type the SSID for the wireless network.
   The SSID is the network name wireless clients see when they connect to the AP device.
4. Select the **Security** tab.
5. From the **Security Mode** drop-down list, select the wireless security mode.

6. Configure the security settings for the selected security mode.
7. Repeat these steps to create additional SSIDs.

Step 4 – Pair the AP Device

When you first connect the AP device to your network, it is an *unpaired* Access Point.

To pair the AP device to your Firebox:

1. From Fireware Web UI, select **Network > Gateway Wireless Controller**.
2. Select the **Access Points** tab.
3. To start a scan for the unpaired AP devices in your area, click **Refresh**.
   The Refresh the Unpaired Access Points list dialog box appears.
4. Specify the user name and passphrase for a user with Device Administrator privileges.
   The Firebox scans for unpaired AP devices.

5. From the **Unpaired Access Points** list, select the AP device to pair.
6. Click **Pair**.
   The Pairing Passphrase dialog box appears.

7. In the **Pairing Passphrase** text box, type the passphrase of the AP device.
   The default AP passphrase is **wgwap**.

> Do not enter a password other than **wgwap** unless you have changed the default password on your AP device.

8. Click **OK**.

When the AP device is paired, the power LED on the device changes to green.

Step 5 – Configure the AP Device Settings

The **Edit Access Point** dialog box automatically opens after you pair the AP device. Select the **Radio Settings** tab to select the radio settings to use for each radio on your AP device.

On devices that have one radio, you can configure *Radio 1* to use either the 2.4 GHz or 5 GHz band.

On devices with two single-band radios, *Radio 1* always uses the 2.4 GHz band, and *Radio 2* always uses the 5 GHz band.

1. From the **Band** drop-down list, select the band to use:
   - **2.4GHz**
   - **5GHz**
2. From the **Wireless Mode** drop-down list, select the wireless mode to use for each radio. The available modes depend on the radio band:
   - 2.4GHz band — 802.11 B, G and N wireless modes
   - 5GHz band — 802.11 A, N, and N/AC wireless modes
3. (Optional) For each radio, select the **Preferred Channel** and **Channel HT Mode**.
   For the AP 102 outdoor model, the **Use outdoor channels only** option is enabled by default.
4. (Optional) For each radio, select the **Rate** and **TX Power**.
   The rate limits the maximum data transfer rate per wireless client.
5. For each radio, select a configured SSID and click **Add**.
6. Save the configuration.

Plan your Wireless AP Device Deployment

Before you deploy WatchGuard AP devices on your network, you must research, design, and plan your wireless network deployment to make sure it meets your requirements for coverage, capacity and airtime demand, and security.

There are two primary considerations when you plan your wireless deployment:

Coverage planning

Traditional coverage planning examines your physical environment where the wireless network will be deployed and the different factors that can affect your wireless signal power, range, and attenuation.

Coverage planning provides:

- Optimal frequency usage and location of access points
- Determination of transmit power levels
- Prevents channel interference
- Examination of floor plans, physical obstructions, and building materials

Capacity planning

Previously, wireless deployment was focused primarily with coverage planning and making sure that wireless networks were available and had strong signals in all physical areas of your environment.

With so many different types of wireless devices and applications now in use, airtime utilization and demand from your clients is now the prime factor of wireless deployment planning. Simply having access to a wireless network and a strong signal does mean the wireless network has the capacity to process many connections consisting of email, web, audio, video, photos, games, and social media from multiple wireless devices.

Deployment Best Practices and Guidelines

We recommend that you review these sections for general wireless knowledge and guidelines for a successful deployment.

- **Wireless Capacity and Airtime Demand** — Determine the optimal number of clients per radio, including idle and active clients, airtime demand for wireless application traffic, and plan for capacity expansion.
- **Site Survey** — Perform a wireless site survey to analyze your current environment and wireless requirements.
- **Wireless Modes and Channels** — Determine which wireless modes and channels you support for your wireless clients.
- **Wireless Environment Factors** — Identify environmental factors that can affect the range and performance of wireless networks.
- **AP Device Placement** — Determine the best location and placement of your WatchGuard AP devices.
- **Wireless Deployment Maps** — Use the Wireless Deployment Maps feature on the Gateway Wireless Controller to help deploy your WatchGuard AP devices, check signal strength, and resolve channel conflicts.

Wireless Capacity and Airtime Demand Planning

As part of your wireless deployment planning, you must take capacity and airtime demand into consideration and not just coverage planning. The airtime demand peak amount and type of traffic must be factored in to your plan to understand traffic patterns for your wireless network and the coverage area it serves.

For example, a deployment for a hotel and its conference rooms will have very different capacity and airtime demand criteria than a general small office deployment, a retail department store, or a school. Each wireless deployment is unique and requires both coverage and capacity planning.

Capacity and airtime demand analysis provides:

- Optimal number of clients per access point radio, including idle and active
  - You must factor in slow periods and worse-case scenarios for usage
- Airtime demand and minimum data rates for different types of application traffic
  - Include email, web, video, social media, streaming, and other applications.
  - Determine bandwidth throughout per application and connection, then determine aggregate bandwidth required in the wireless network coverage area.
- Considerations for growth
  - Based on number of connected clients and application bandwidth usage

Wireless Modes and Channels

WatchGuard AP wireless devices support two different wireless bands: 2.4 GHz and 5 GHz. The band you select and the country you specify determine which wireless modes are available.

- The 2.4 GHz band supports 802.11b, 802.11g and 802.11n
- The 5 GHz band supports 802.11a, 802.11n, and 802.11ac

These wireless standards are supported:

	802.11ac (for supported APs)	802.11n	802.11g	802.11b	802.11a
Frequency Band	5GHz	2.4GHz and 5GHz	2.4GHz	2.4GHz	5GHz
Data Rate	1300Mbps	450Mbps	54Mbps	11Mbps	54Mbps
Channel Width	20, 40, and 80MHz	20 and 40MHz	20MHz	20MHz	20MHz

For most environments, you must support legacy wireless devices that do not support newer standards. Because of this, WatchGuard recommends that you configure your WatchGuard AP device to use mixed protocol modes.

> If you choose a wireless mode that supports more than one 802.11 standards, the overall performance can be impacted. This is in part because of backward compatibility requirement when devices that use slower modes are connected. The slower devices often use more of the available throughput because it can take much longer to send or receive the same amount of data to devices that use a slower mode.

Range

Although the 5GHz band is less congested and provides faster data rates than 2.4GHz, it has less range than 2.4GHz.

- 2.4 GHz — 75 to 100ft
- 5 GHz — 25 to 35ft (at full speed)

Physical obstructions and wireless interference will reduce your effective wireless range and data speeds.

Channels

A wireless channel is a specific division of frequencies within a specific wireless band.
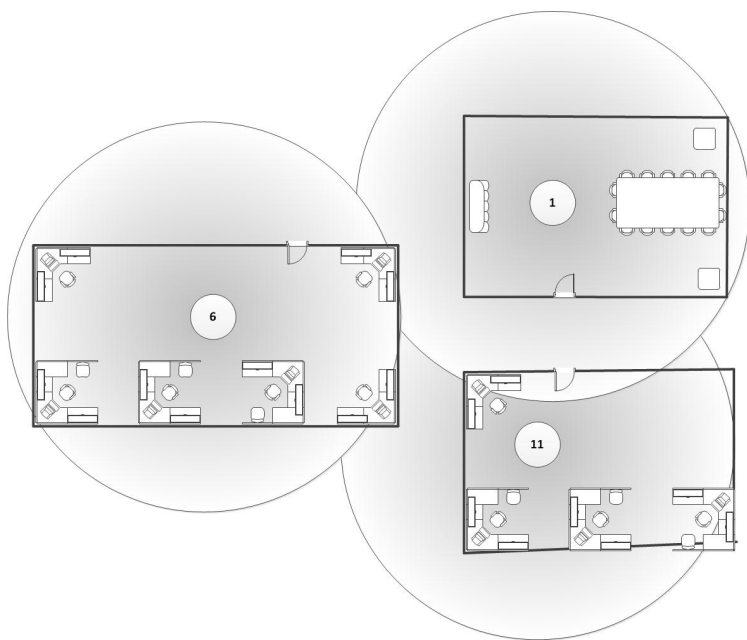
2.4GHz Band

For example, in the 2.4GHz band with a channel width of 20MHz, there are 14 defined channels spaced every 5MHz. Channels 12 and 13 are available in countries outside of North America. Channel 14 is for Japan only and is spaced at 12 MHz.

One wireless channel can overlap the frequency of another wireless channel. When you design and deploy wireless networks, you must consider which channels you use for your wireless network. For example, in the 2.4 GHz band, adjacent channels such as channel 3 and 4 have frequencies that closely overlap, which can cause interference. In the 2.4 GHz band, channels 1, 6, and 11 are the most commonly used channels. They do not overlap each other because of the space between their frequencies. The 2.4GHz band is crowded because many other devices that operate on this band (such as cordless phones, microwaves, monitors, and wireless headsets) also use the same channels, and can cause wireless congestion.
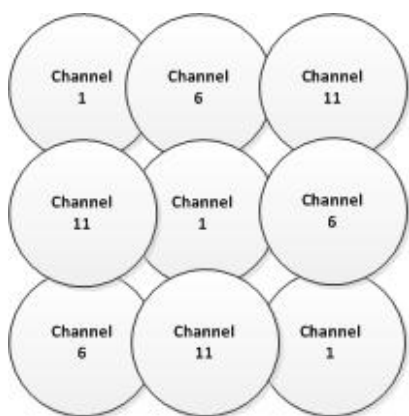
When you deploy your AP devices, consider using different channels for each AP device and position them so that different channels are used in locations that do not overlap.

5GHz Band

In the 5GHz band, there are 43 possible channels. The full channel width is reserved and there is a very large selection of channels that do not overlap.

In some regions, DFS (Dynamic Frequency Selection) channels operate in the 5GHz band. Because DFS channels are used with radar, transmissions from your AP device stop if radar signals are detected on that channel. You can disable the use of DFS channels in your AP device configuration.

> Using DFS channels can be helpful with 802.11ac and an 80MHz channel width because of the extra spectrum availability, but using these channels can result in your AP devices being slow to connect on the wireless network.

For outdoor model AP102, you can configure the device to only use outdoor channels.

Channel Selection

The WatchGuard AP device is configured by default to automatically select a wireless channel. When you power on the WatchGuard AP device, it automatically scans the network and selects the wireless channel with the least amount of interference.

Use Wireless Deployment Maps to Find Channel Conflicts

You can use the Wireless Deployment Maps feature in the Gateway Wireless Controller in Fireware Web UI to help you find wireless channel conflicts and optimize your wireless environment.

Wireless Site Survey

Before you deploy a new WatchGuard AP device, you can perform a wireless site survey to analyze your current environment and existing wireless signals. The wireless site survey helps you to identify your specific requirements for your wireless network, and any external factors that could affect your deployment.

Site survey results can help you determine this information:

- Number of wireless clients that must be supported
- Airtime utilization and demand of wireless clients and applications
- Areas of coverage and number of AP devices required
- Best physical placement of AP devices
- Range from clients to each AP device
- Wireless signal strength and potential sources of wireless noise and interference
- Environmental factors that affect wireless signals, such as building construction and materials

Typically, you begin a site survey with a physical walk-through of your environment. It is helpful to have a floor plan of your facilities that shows your existing networking environment and a list of requirements for your planned wireless networks. A visual inspection helps you to understand the areas of coverage required, the physical limitations and barriers due to building construction, and potential sources of wireless interference.

After you complete a physical inspection of your facilities, you must be able to visualize and understand where the current wireless signals are located in your environment, and how they react to your physical environment.

Many wireless site survey tools are available that enable you to map your environment and generate wireless *heat maps*, which provide a visual representation of the wireless signals in your environment. The heat map shows the strength and range of wireless access points, how their signals react to your physical environment, and identifies any existing wireless interference.
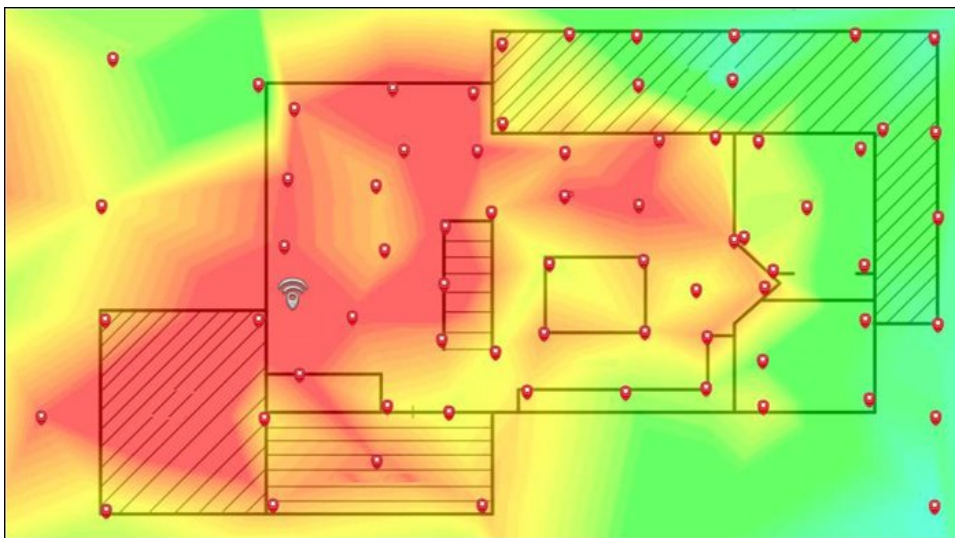
To determine what wireless signals and interference already exist in your environment, you can generate a heat map to help you plan your deployment scenario. You can use one of the many available third-party wireless site survey tools such as Ekahau HeatMapper. After you install your AP devices, you can make another heat map of your environment to see if your current placement provides adequate coverage and signal strength for your wireless network.

You can also use the Wireless Deployment Maps feature on the Gateway Wireless Controller to provide a simulated physical view of your wireless network to help you place the AP devices in optimal locations for maximum coverage, and to detect channel conflicts with other wireless devices in your area.

Wireless Environmental Factors

There are several environmental factors that can affect the range and performance of wireless networks. You must estimate the pass loss and attenuation of your wireless signals as a result of these factors.

Walls and ceilings

Walls and ceilings between the AP device and wireless clients can degrade signal strength. Wireless signals can penetrate walls and other structures, but the rate of penetration is directly related to the type of building materials, materials thickness, and the distance from the wireless antenna.

Building materials

Metal and aluminum doors, glass, concrete, metal studs, brick walls, glass, and other types of building materials can have a significantly negative effect on the signal strength of wireless signals.

EMI (Electro-magnetic interference)

EMI from other electrical devices, such as microwaves, cordless phones, and wireless headsets, can generate significant RF noise and degrade or disrupt wireless communications.

Distance

Wireless signals degrade quickly past their maximum range. You must plan your network carefully to provide adequate wireless coverage over the range you require in your environment.

Wireless Placement

For full wireless coverage and to make sure that all users in your environment receive a strong wireless signal, consider these guidelines for the location and placement of your WatchGuard AP devices:

- Place your AP devices in a central location away from any corners, walls, or other physical obstructions to provide maximum signal coverage.
- Place your AP devices in a high location to provide the overall best signal strength reception and performance for your wireless network.
- In general, one AP device can cover up to approximately 2000 ft^2 depending on the physical environment and wireless interference.
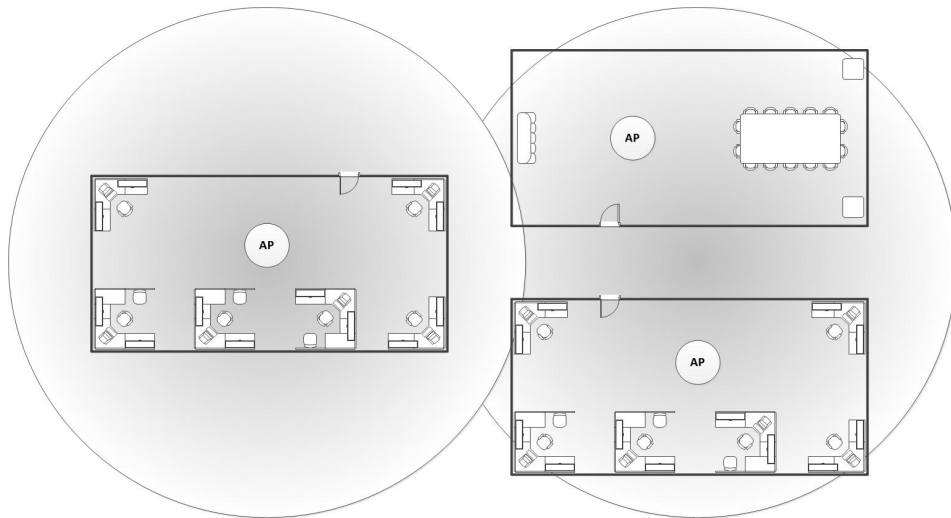
- Make sure you do not install an AP device in close proximity to any electronic devices that can interfere with the signal, such as televisions, microwave ovens, cordless phones, air conditioners, fans, or any other type of equipment that can cause signal interference.
- When you install more than one AP device, make sure to put enough space between them to provide maximum coverage for your wireless network area of availability. For wireless coverage over many floors, you can stagger the placement of devices to cover both vertical and horizontal space.
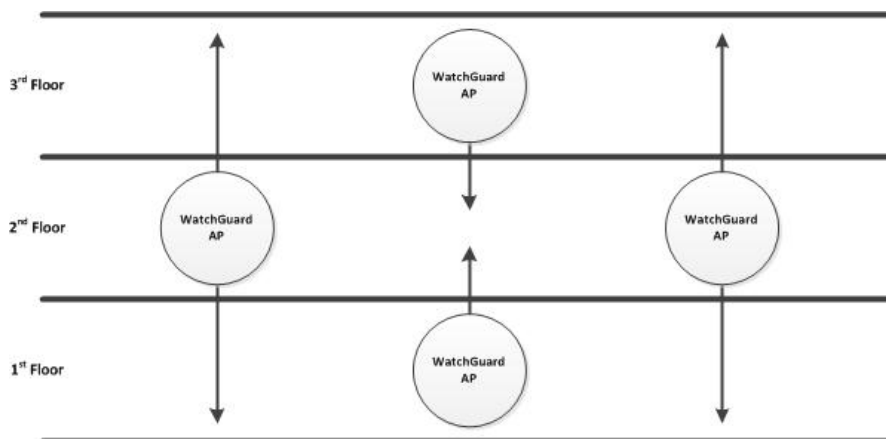
View Wireless Deployment Maps

In Fireware Web UI, you can use the **Maps** tab on the **Dashboard > Gateway Wireless Controller** page to help you visualize your wireless network, determine where to place your WatchGuard AP devices, check for wireless conflicts so that you can optimize your wireless environment, and check for rogue access points.

Wireless Deployment Maps Overview

From the **Maps** page , you can:

- View a 2D map of your wireless network.
- See the radio frequency, channel, transmit power, and SSID used by each radio.
- Check for wireless channel conflicts.
- View foreign BSSIDs (Broadcast SSID)
- Find rogue access points.

You can select two views:

- **Wireless Coverage Map** — Shows the location of your AP devices in relation to one another, and shows the connection quality and any channel conflicts between your AP devices.
- **Channel Conflict Map** — Shows the location of your AP devices and any other wireless devices in the vicinity, shows the channel and bandwidth details for each device, and shows any wireless channel conflicts between devices.

Use Maps for AP Device Placement

You can use the *Wireless Coverage Map* to provide a simulated physical view of your wireless network to help you place the AP devices in optimal locations for maximum coverage. After the initial scan, the maps display the relative location of each WatchGuard AP device. Because the Wireless Coverage Map is a two-dimensional representation of your environment, AP devices on different floors in your environment might appear to be positioned closely on the map even though they are physically distant. What is most important is the strength of the connections and links between the AP devices.

In an ideal deployment, your AP devices should be deployed at a relatively uniform distance to each other, with solid or dashed green lines between the devices on the maps. The network should resemble a mesh pattern where there are as many redundant links as possible between AP devices for uninterrupted roaming for wireless clients.

For example, in this simple wireless network:

- There are three WatchGuard AP devices managed by this Gateway Wireless Controller.
- The AP devices are well positioned for maximum coverage.
- Wireless users have no interruptions when they roam from one AP device to another.
- The solid green lines indicate a strong wireless connection with no channel conflicts between these AP devices.

> No conflicts with other wireless devices in your environment are displayed in the Wireless Coverage Map. This information is displayed in the *Channel Conflict* Map.
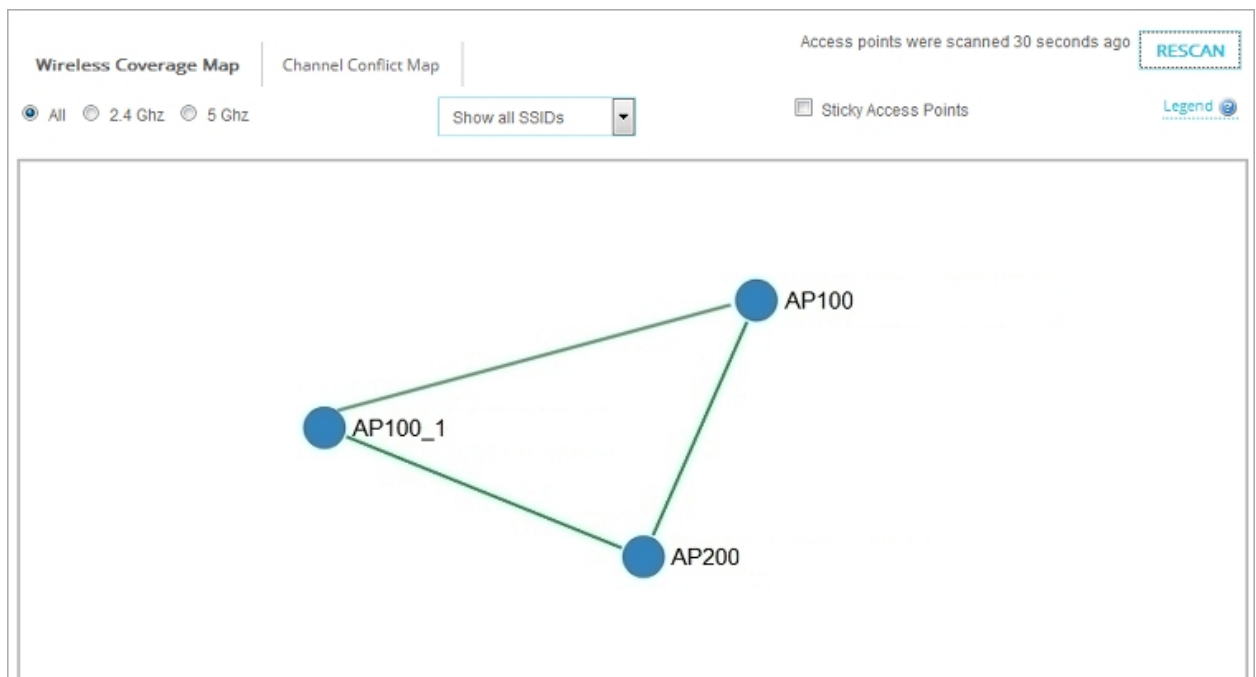
In the next example, the network is larger with more AP devices in the wireless network. There are some channel conflicts between AP devices and connection links between some AP devices are weak.
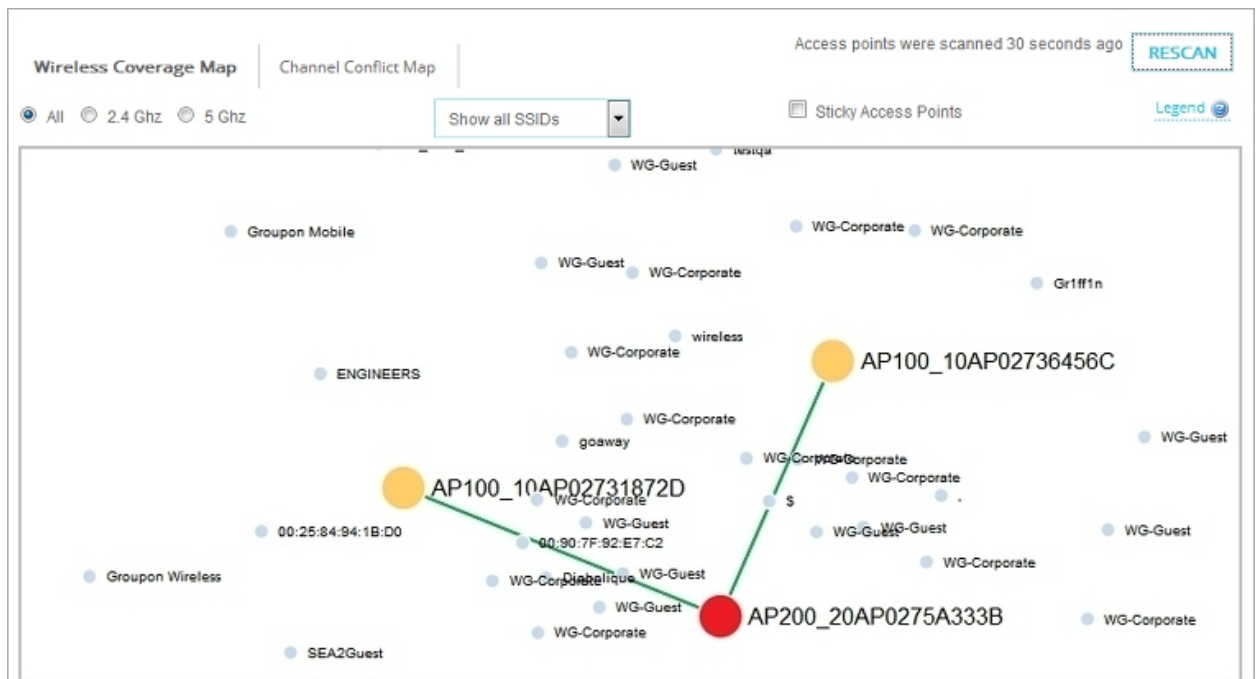
- There are seven WatchGuard AP devices managed by this Gateway Wireless Controller.
- *AP100* and *AP200* are physically close together, but have a significant level of channel conflict.
- *Remote 102* is connected with a weak signal, with no connection to the other AP devices. A wireless user could lose connectivity if they roamed from *Remote 102* to *Remote 100*.
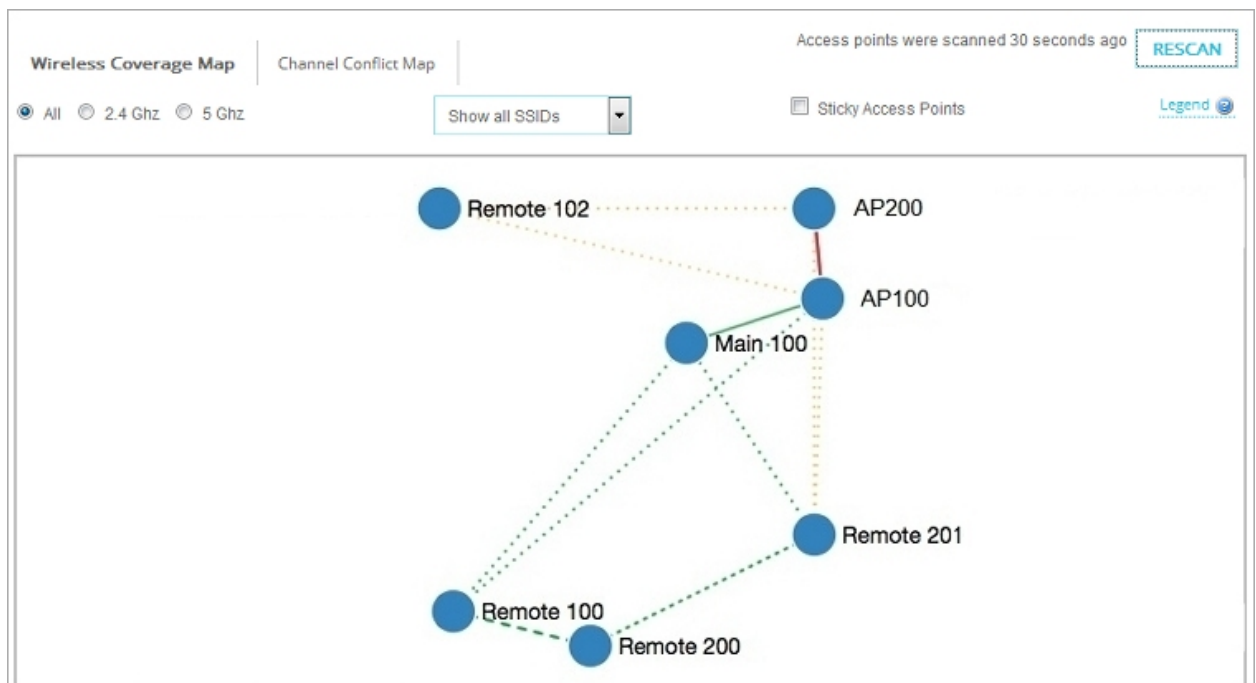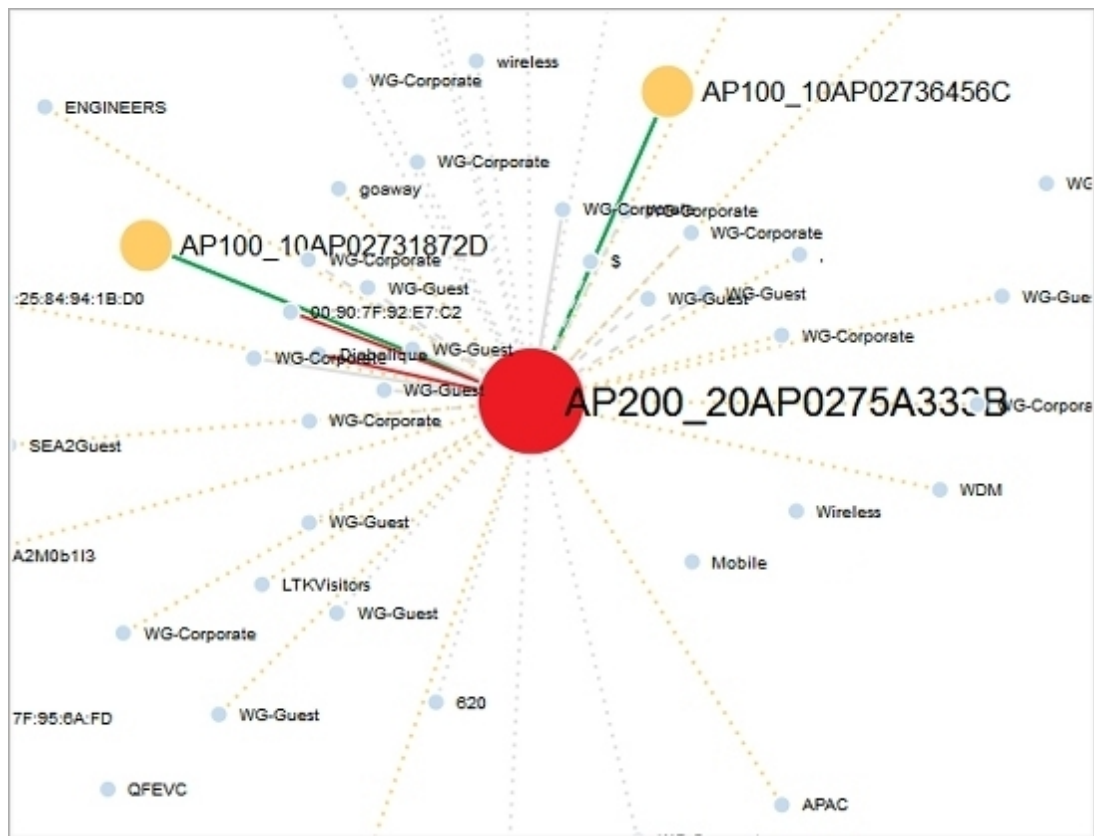
See Wireless Channel Conflicts

Use the *Channel Conflict Map* to see all wireless devices in the vicinity, and show any channel conflict between devices. This map includes all wireless devices, even those not managed by your Gateway Wireless Controller.

The color of the AP device indicates the severity of the channel conflict. In this example, the two AP100 devices have moderate channel conflict, and the AP200 device has significant channel conflict. Other non-managed devices are shown in grey. The links between the AP devices are green that indicates any wireless conflicts are with foreign devices, not with other WatchGuard AP devices in your network.

To see more detailed information on connections to other wireless devices, including foreign devices that are not other WatchGuard AP devices in your network, hover your mouse pointer over the AP200 device. The color and line detail indicate the severity of the conflict and signal loss.

To see more detailed information about the AP device and any channel conflicts, right-click an AP device and select **View Details**. The details includes a map and graph with channel conflict information on nearby devices.

To see only the devices that have channel conflicts with your AP device, select the **Show only conflicting devices** check box.

In the table, the **Conflict** column shows which devices have a channel conflict with the selected AP device. You can use this information to adjust your wireless radio configuration to find an appropriate wireless channel with the least interference.

To update the configuration of the selected AP device, click **Configure this Access Point**.

If your **Preferred Channel** selection is set to **Auto**, you can use the **Restart Wireless** option to restart the wireless interfaces and allow the device to select an appropriate channel. When you restart the wireless interfaces, the AP device does not reboot.

| Name ⬍	Signal	AP	Conflict	SSID	BSSID	Channel
00:90:7F:92:E7:C2	.ıll		🔴		00:90:7F:92:E7:C2	2
AP100_10AP02731872D	.ıll	✅				11
AP100_10AP02736456C	.ıll	✅				60 + 64
Diabolique	.ıll		🔴	Diabolique	00:90:7F:A3:2C:DD	2
WG-Guest	.ıll			WG-Guest	02:90:7F:B0:00:FD	6
WG-Corporate	.ıll			WG-Corporate	00:90:7F:B0:00:FD	6
WG-Corporate	.ıll			WG-Corporate	00:90:7F:B0:00:FE	36
WG-Guest	.ıll			WG-Guest	02:90:7F:B0:00:CA	6

Find Rogue Access Points

You can use the Wireless Deployment Maps to scan your network for all foreign wireless access points that operate within range of your managed AP devices. Some of these foreign access points could be rogue access points.

A rogue access point is any wireless access point within range of your network that is not recognized as a paired access point or configured exception in your wireless deployment.

An unauthorized access point can be installed by a malicious user, but it could also be a device installed by someone inside your organization without consent. These access points are security risks to your wireless and wired networks if they do not have proper security features enabled.

The Gateway Wireless Controller scans the wireless network on all wireless modes and channels within range for other wireless devices.

In the Wireless Deployment Maps, you can see all wireless devices and access points. This includes the AP devices managed by your Gateway Wireless Controller in the Wireless Coverage Map, and all foreign SSIDs and BSSIDs (Broadcast SSID — the MAC address is displayed if SSID broadcast is disabled) in the Channel Conflict Map.
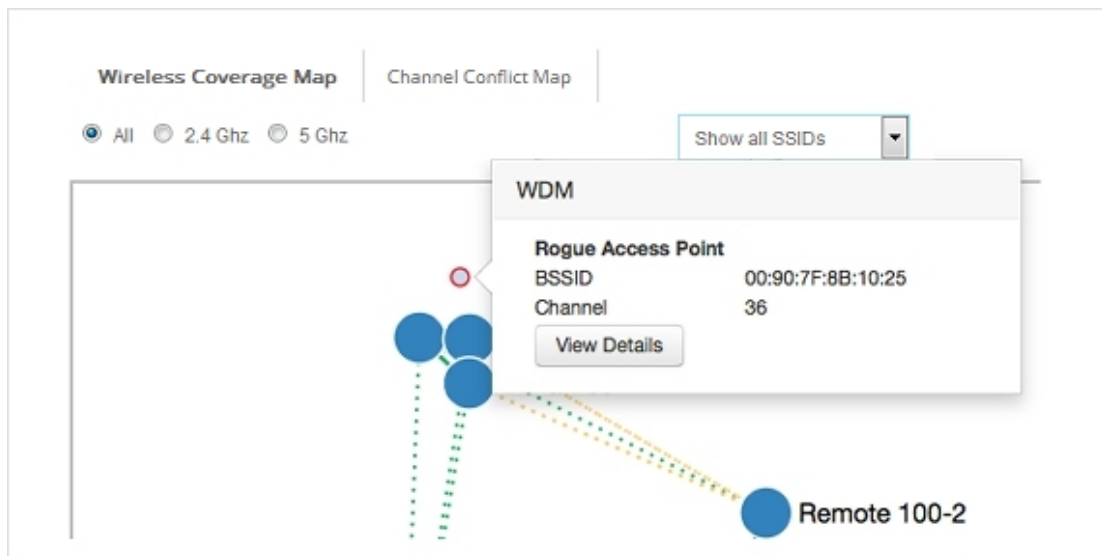
This map can help you find the relative location of any foreign device in relation to your other devices on the network. You can also click any foreign device in the map and examine wireless details for that device.

Select the **Foreign BSSIDs** tab to see all SSIDs broadcast by unknown AP devices (the MAC address is displayed if SSID broadcast is disabled). Rogue access points (identified with a red dot) are those devices that are not paired with your Gateway Wireless Controller, or do not appear in your rogue access point exception list.

MAC ADDRESS	SSID ⇕	CHANNEL	ROGUE ACCESS POINT
74:85:2A:A4:88:CA	xfinitywifi	48 + 44	🔴
00:90:7F:B0:00:22	wyi-ap200-test-5	36 + 40	
00:90:7F:B0:24:B4	mightymouse	44 + 48	
00:90:7F:B2:03:E3	goaway5	165	
00:90:7F:B3:C1:1A	WG-Guest	36 + 40	
00:90:7F:B3:C1:1D	WG-Guest	157 + 161	

The Rogue Access Point Detection feature for the Gateway Wireless Controller and managed WatchGuard AP devices is different than the Rogue Access Point Detection feature designed for Firebox and XTM wireless devices with built-in wireless capabilities.

For information on the differences between Firebox and XTM wireless devices and WatchGuard AP devices, see Wireless Access Point Types. For information on Rogue Access Point Detection for Firebox or XTM wireless devices, see Rogue Access Point Detection.
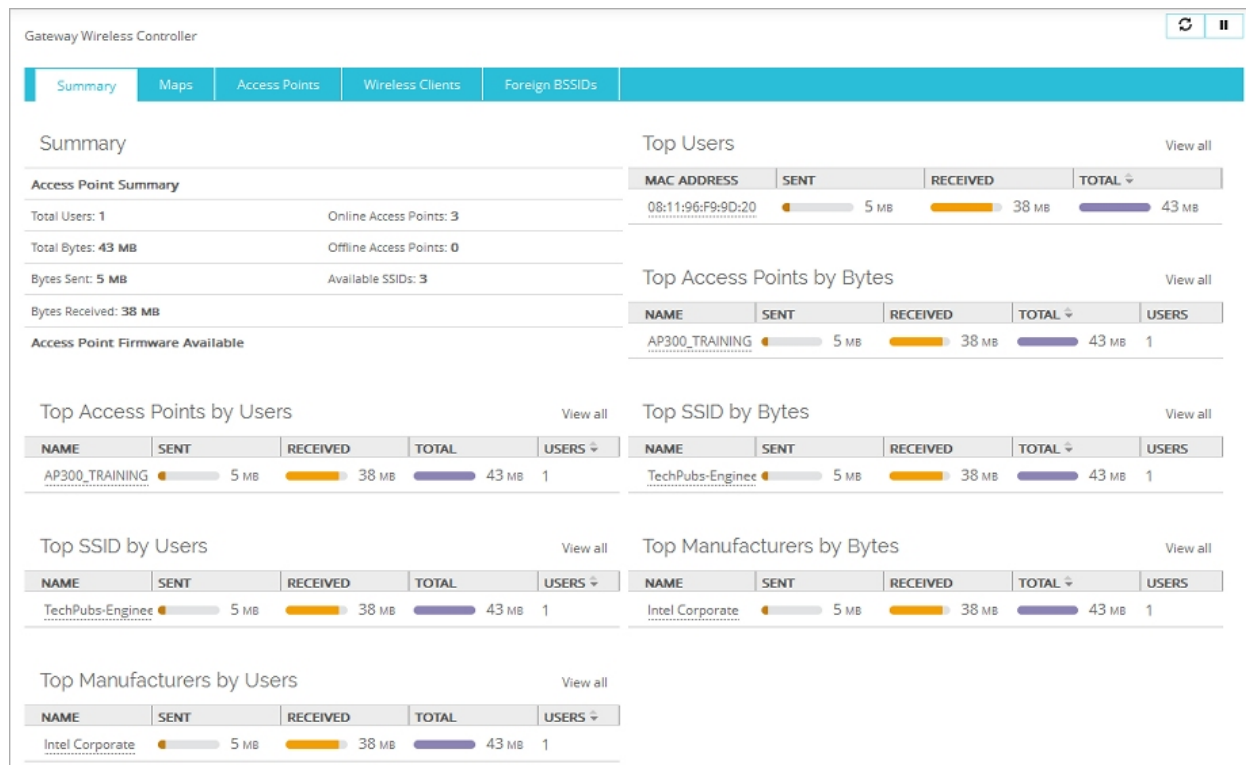
Monitor AP Device Status

You can monitor, reboot, and upgrade the WatchGuard AP devices managed by your Firebox.

To monitor AP devices, from Fireware Web UI:

1. Select **Dashboard > Gateway Wireless Controller**.
   The Gateway Wireless Controller page appears.
2. Select the **Summary** tab.

The *Summary* panel shows a status summary for the AP device, and the available firmware version. The *Top Panels* show. real-time data about the traffic through the AP device.

From the **Access Points** tab, you can:

- See the connection status and uptime of each AP device.
- See the radio frequency and channel used by each radio.
- See the transmit power and secondary channel information.
- See the AP device activation status.
- See the log messages for the selected AP device.
- See network statistics for the selected AP device.
- Flash the power LED on the AP device for identification.
- Restart wireless interfaces on AP devices.
- Reboot AP devices.
- Upgrade the firmware on AP devices.
- Perform a site survey from the selected AP device to detect other wireless access points.

Perform a Site Survey

You can use your AP device to complete a site survey to detect other wireless access points that operate in the same area. When you perform a site survey, the radios in the AP device scan the wireless channels to find other wireless access points. The site survey can detect all local wireless access points. This includes other WatchGuard AP devices and WatchGuard Firebox or XTM wireless devices. You must configure an AP device radio to use at least one SSID before that radio can perform a site survey.

When a site survey scan begins, the AP device scans the airwaves within range for other radio broadcasts in the same radio band, on all available wireless channels. The scan is not limited to the wireless mode and channel settings configured in the radio settings of your device. Dual radio devices can use both radios to scan on the 2.4GHz and 5GHz radio bands. A single radio device scans on either the 2.4GHz or 5GHz band. The band used for the scan depends on which band the radio is configured to operate in.

The site survey does not interrupt wireless connectivity for connected wireless clients.

To start a site survey from Fireware Web UI:

1. Select **Dashboard > Gateway Wireless Controller**.
2. On the **Access Points** tab, select an AP device.
3. Click **Site Survey**.
   The Site Survey page appears and the AP device begins the scan for other wireless access points. A list of detected access points appears in the Site Survey page.

For each detected wireless access point, the site survey report shows this information:

BSSID

The Basic Service Set Identifier is the MAC address of the wireless access point.

SSID

This is the SSID for the access point. If an access point has more than one SSID, each SSID appears as a separate item in the site survey.

Channel

This is the wireless channel that the wireless access point uses. If available, secondary channel information also appears.

Signal Level

This is the signal strength of the wireless access point.

Type

This is the wireless standard the wireless access point supports.

Security

This is the type of wireless security used by the wireless access point.

Mode

This is the operating mode of the wireless device.

Monitor Wireless Clients

You can view and monitor the wireless clients that are connected to your WatchGuard AP devices. You can also disconnect a wireless client from an AP device.

> The hostname and IP address of wireless clients only appear if the client uses the Firebox device as a DHCP server.

To see the connected wireless clients, from Fireware Web UI:

1. Select **Dashboard > Gateway Wireless Controller**.
   The Gateway Wireless Controller page appears.
2. Select the **Wireless Clients** tab.
   A list of connected wireless clients appears.

3. To show only wireless clients that are connected to a specific AP device, from the **Access Point** drop-down list, select an AP device .
4. To show only wireless clients that are connected to a specific SSID, from the **SSID** drop-down list, select an SSID.
5. To show only wireless clients from a specific manufacturer, from the **Manufacturer** drop-down list, select the manufacturer.
6. To view a wireless client's statistics in FireWatch or Traffic Monitor, select an IP address.
7. To disconnect a wireless client, select the client and click **Disconnect Client**.

To disconnect a wireless client from an AP device:

1. In the Wireless Clients tab, select a wireless client.
2. Click **Disconnect Client**

About AP Device Activation

You must activate your AP device with WatchGuard to enable your hardware replacement warranty, receive technical support, and get access to the latest OS updates and product news.

After you pair a WatchGuard AP device with a Firebox, the Firebox automatically connects to the WatchGuard website and sends the information necessary to activate the AP device on the same WatchGuard account where the Firebox was activated.

The Firebox and AP devices on your network require access to WatchGuard servers (*.watchguard.com) on port 443. This allows the Gateway Wireless Controller on the Firebox to register and activate AP devices, and check for new firmware updates. AP devices require access to WatchGuard servers to obtain country and regional information.

If automatic activation fails, the Firebox periodically tries to activate again. The activation status of your AP device does not affect the functionality of the AP device.

If your AP device has not been activated automatically and you want to activate it manually, you can activate the AP device in your WatchGuard account just as you would activate a Firebox or add-on feature.

Reset the WatchGuard AP Device

The reset procedure depends on the firmware version of your AP device.

For AP device firmware 1.2.9.2 or higher

1. With the AP device powered on, press and hold the reset button.
2. After 5 seconds, release the reset button.
   The AP device resets.

When the device completes initialization, it is reset to the factory-default settings.

For AP device firmware 1.2.9.1 or lower

1. With the AP device powered on, press and hold the reset button.
2. After 12 seconds, release the reset button.
   The AP device resets.

When the device completes initialization, it is reset to the factory-default settings.

> If you press the reset button briefly then release (less than 5 seconds), the AP device reboots, but it will not be reset to factory-default settings.

Additional Resources

This *AP Deployment Guide* provides information about initial setup of your WatchGuard AP devices.

For information about your AP device hardware and physical installation, see the *Quick Start Guide* and *Hardware Guide* for your specific device model.

For more detailed information about VLAN configuration, and AP device configuration examples, see the *Fireware Help*.

You can view and download the most current documentation for your WatchGuard AP device on the WatchGuard website **Documentation** page at
http://www.watchguard.com/wgrd-help/documentation/overview.