Fireware

AP Deployment Guide

WatchGuard APs
Gateway Wireless Controller
Fireware OS v12.5.3

About This Guide

The *WatchGuard Fireware AP Deployment Guide* is a guide for deployment of a WatchGuard AP with a Firebox. For the most recent product documentation, see the *Fireware 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: 3/25/2020

Copyright, Trademark, and Patent Information

Copyright © 1998-2020 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

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

Support

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

Sales

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

Contents

Introduction 1

WatchGuard AP Management 2

WatchGuard APs Managed by a Gateway Wireless Controller 2

AP Deployment Steps 3

AP Deployment 3

About Automatic Deployment 3

Benefits of VLANs for Your AP 3

Step 1 – Activate your AP 5

Step 2 – Enable the Gateway Wireless Controller on your Firebox 6

Step 3 – Connect the AP to your Network 7

Step 4 – Configure SSIDs 8

Step 5 – Pair the AP with your Firebox 9

Step 6 – Configure the AP Settings 10

Step 7 – Check the AP Status 11

Monitor AP Status 13

Monitor Wireless Clients 15

Reset a WatchGuard AP 17

Reset a WatchGuard AP from the Gateway Wireless Controller 17

Reset a WatchGuard AP with the Reset Button 18

Plan your Wireless AP Deployment 19

Deployment Best Practices and Guidelines 20

Wireless Capacity and Airtime Demand Planning 21

Wireless Modes and Channels 22

Range 22

Channels 22

2.4GHz Band 22

5GHz Band 23
About DFS Channels 23
AP Channel Selection 23
Use Wireless Deployment Maps to Find Channel Conflicts 23
Wireless Site Survey 24
Wireless Environmental Factors 26
Wireless Placement 27
View Wireless Deployment Maps 29
Wireless Deployment Maps Overview 29
Use Maps for AP Placement 30
See Wireless Channel Conflicts 31
Find Rogue Access Points 35
Additional Resources 37

Introduction

You can use WatchGuard APs to add wireless access to your network. WatchGuard offers these wireless security solutions for WatchGuard APs:

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

WatchGuard Wi-Fi Solution	Total Wi-Fi	Secure Wi-Fi	Basic Wi-Fi
Wi-Fi Cloud License	✓	✓	
Wireless Intrusion Prevention System (WIPS) Cloud-managed APs have built-in WIPS to help ensure you have the protection you need from malicious attacks and rogue APs	✓	✓	
GO Mobile Web App Easily set-up your network and configuration from any mobile device	✓	✓	
Customer Engagement Tools Splash pages, social media integration, surveys, coupons, videos, and so much more	✓		
Location-based Analytics Know how and when visitors are using your Wi-Fi, customizable reports and alerts for real-time and historical usage data	✓		
Fireware Gateway Wireless Controller License			✓
Standard 24x7 Support Hardware warranty with advance hardware replacement, customer support, and software updates	✓	✓	✓

WatchGuard AP Management

There are two ways you can manage a WatchGuard AP:

WatchGuard Firebox Gateway Wireless Controller

You can use Gateway Wireless Controller on your Firebox to configure, manage, and monitor WatchGuard APs directly from the Firebox. You can connect multiple WatchGuard APs to the trusted, optional, or custom networks of a Firebox, and manage them from the Gateway Wireless Controller on the Firebox.

To configure WatchGuard APs from Gateway Wireless Controller, select **Network > Gateway Wireless Controller** in Fireware Web UI or Policy Manager.

WatchGuard Wi-Fi Cloud

WatchGuard Wi-Fi Cloud is a powerful cloud-based enterprise wireless management solution for WatchGuard AP configuration, security, and monitoring. For more information on WatchGuard Wi-Fi Cloud, see Wi-Fi Cloud Management.

WatchGuard APs Managed by a Gateway Wireless Controller

WatchGuard APs 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 APs 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 APs. The network security policies already configured on your Firebox automatically apply to wireless users.

You can then configure the APs 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 APs.
- To support different groups of wireless users, you can configure your APs 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 APs. 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 on your network. For a more comprehensive reference to all AP functionality, see *Fireware Help*.

AP Deployment Steps

Before you deploy WatchGuard APs 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. For more information, see the *Plan your Wireless AP Deployment* section of this guide.

AP Deployment

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

To deploy any AP on your Firebox network you must:

- *Step 1 – Activate your AP*
- *Step 2 – Enable the Gateway Wireless Controller on your Firebox*
- *Step 3 – Connect the AP to your Network*
- *Step 4 – Configure SSIDs*
- *Step 5 – Pair the AP with your Firebox*
- *Step 6 – Configure the AP Settings*
- *Step 7 – Check the AP Status*

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

About Automatic Deployment

For wireless networks with a large number of WatchGuard APs to deploy that will be assigned the same SSIDs and do not require unique configurations, you can enable automatic deployment on specific SSIDs. Unpaired APs will be automatically deployed by the Gateway Wireless Controller and configured with the specified SSID.

For more information on Automatic Deployment, see the *Fireware Help*.

Benefits of VLANs for Your AP

To deploy an AP on your network, you do not have to enable VLAN tagging. There are, however, several reasons you might 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 APs, 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 APs 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 APs 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.

This topic provides a more detailed overview of the steps to deploy an AP without VLAN tagging. For more information about VLANs and for configuration examples, see the *Fireware Help*.

Step 1 – Activate your AP

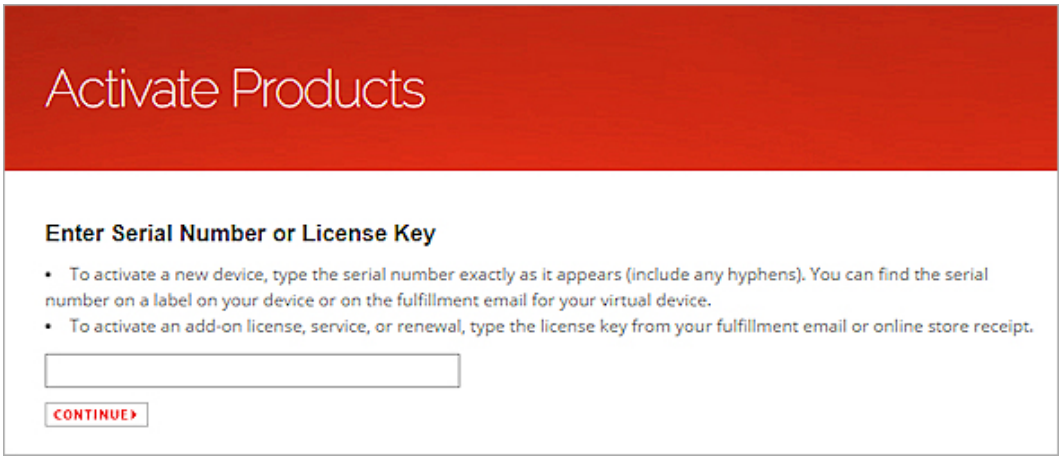
You must activate your AP with WatchGuard to enable your hardware replacement warranty, receive technical support, and get access to the latest OS updates and product news. You cannot manage the AP with the Gateway Wireless Controller until the AP is activated with a valid Basic Wi-Fi AP subscription, and an AP feature key downloaded to the Firebox.

You can activate the AP in your WatchGuard account just as you would activate a Firebox or add-on feature.

To activate your WatchGuard AP:

1. Open a web browser and go to https://www.watchguard.com/activate.
2. Log in with your WatchGuard account user name and password.
   If you are already logged in to your WatchGuard account, select **My WatchGuard > Activate Products** from the WatchGuard Support Center.
3. Type the serial number of the WatchGuard AP. Make sure to include any hyphens.

> Make sure the AP you want to activate has a Basic Wi-Fi subscription.



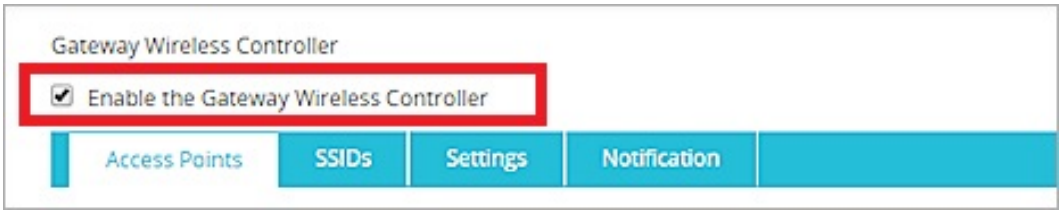
4. Click **Continue**.
5. Type a friendly name to identify your AP in your account.
6. (Optional) Select free trials for your AP, if available.

After activation is complete, the AP appears in the **Manage Products** list in your WatchGuard account.

Step 2 – Enable the Gateway Wireless Controller on your Firebox

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

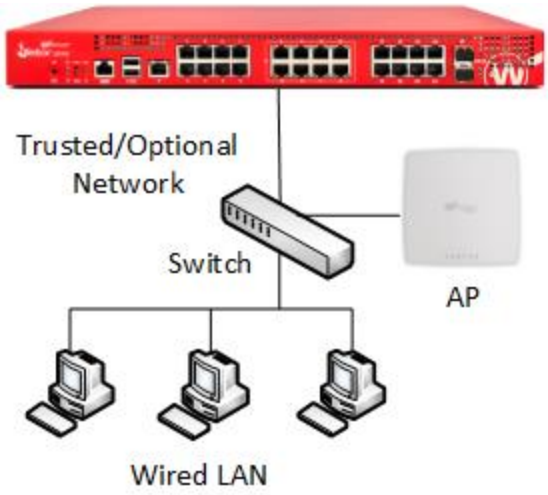
1. From Fireware Web UI, select **Network > Gateway Wireless Controller**.



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 APs to use after they are paired.
4. Click **OK**.
5. Save the Firebox configuration.

Step 3 – Connect the AP to your Network

You can connect the AP to a trusted, optional, or custom Firebox network. To allow the Gateway Wireless Controller to discover an AP 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 automatically requests an IP address from a DHCP server on the local network.

To configure a Firebox interface:

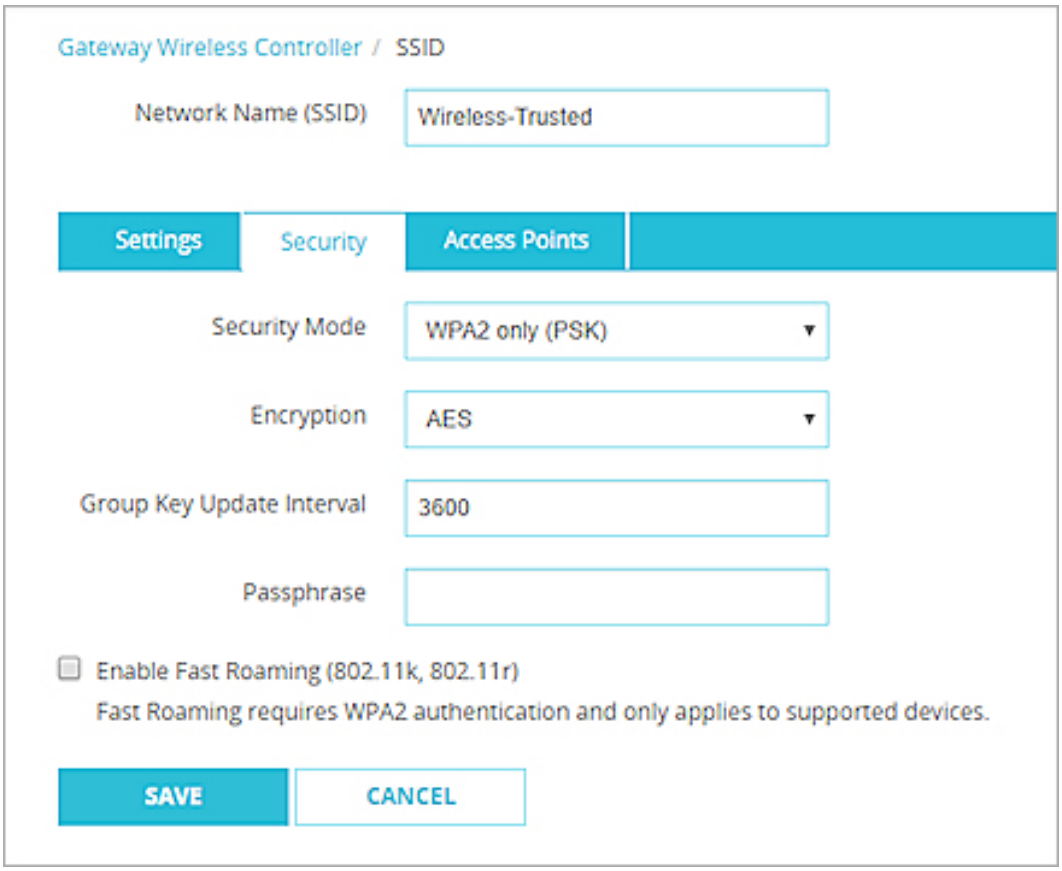
1. From Fireware Web UI, select **Network > Interfaces**.
2. Configure the Firebox interface as trusted, optional, or custom, and enable DHCP on that interface.
3. Save the configuration.

Step 4 – Configure SSIDs

When you configure the SSID that your wireless users connect to, you must select a wireless security mode for the SSID. By default, the security mode for an SSID is set to **WPA2 only**.

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.
4. Select the **Security** tab.
5. From the **Security Mode** drop-down list, select the wireless security mode. The default is **WPA2 only (PSK)**.



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

Step 5 – Pair the AP with your Firebox

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

To pair the AP 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 APs in your area, click **Refresh**.

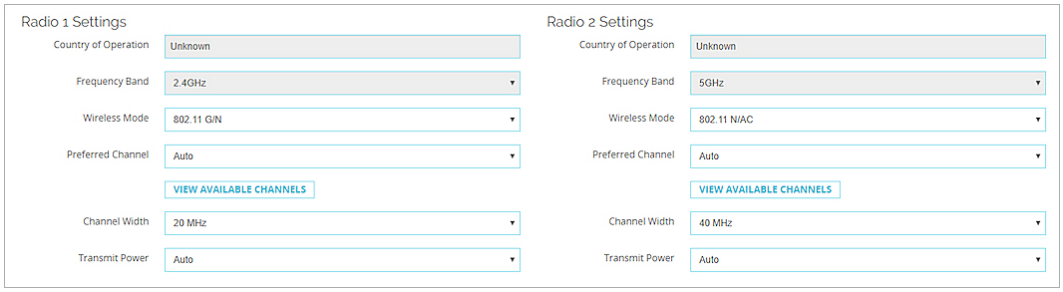
4. From the **Unpaired Access Points** list, select the AP to pair.
5. Click **Pair**.
6. Click **OK**.

Step 6 – Configure the AP Settings

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

To configure radio settings:

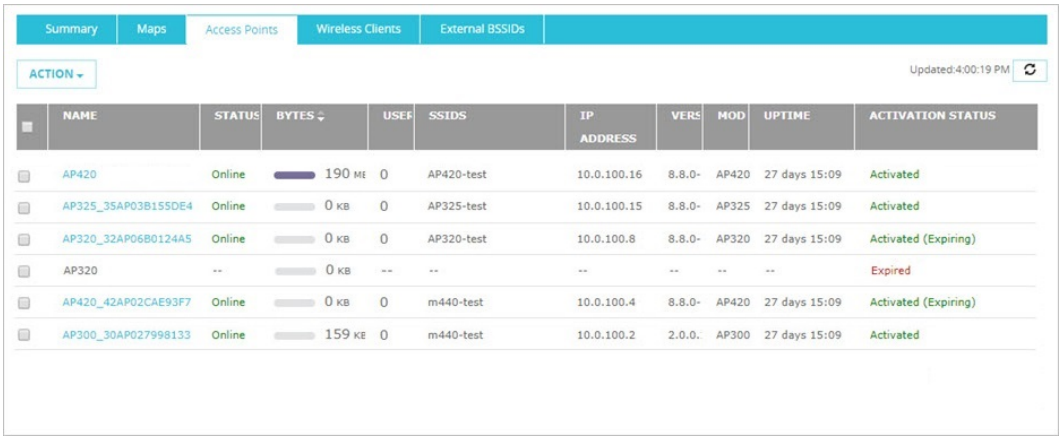
1. From the **Frequency Band**drop-down list, select a band: **2.4 GHz** or **5 GHz**.
2. From the **Wireless Mode** drop-down list, select the wireless mode to use for each radio. The available modes depend on the radio band:
   - 2.4 GHz band – 802.11 B, G, and N wireless modes
   - 5 GHz band – 802.11 A, N, and N/AC wireless modes
5. (Optional) For each radio, select the **Preferred Channel** and **Channel Width**.
6. (Optional) For each radio, select the **Rate** and **Transmit Power**.
   The rate limits the maximum data transfer rate per wireless client.
7. Save the configuration.



Step 7 – Check the AP Status

To see the status of your paired APs:

1. From Fireware Web UI, select **Dashboard > Gateway Wireless Controller > Access Points**.
2. Verify that the AP status is **Online**.



If your AP status is **Not Trusted**, you must make sure this AP is a known AP in your deployment before you trust the device. For more information on the AP Trust Store, see the *Fireware Help*.

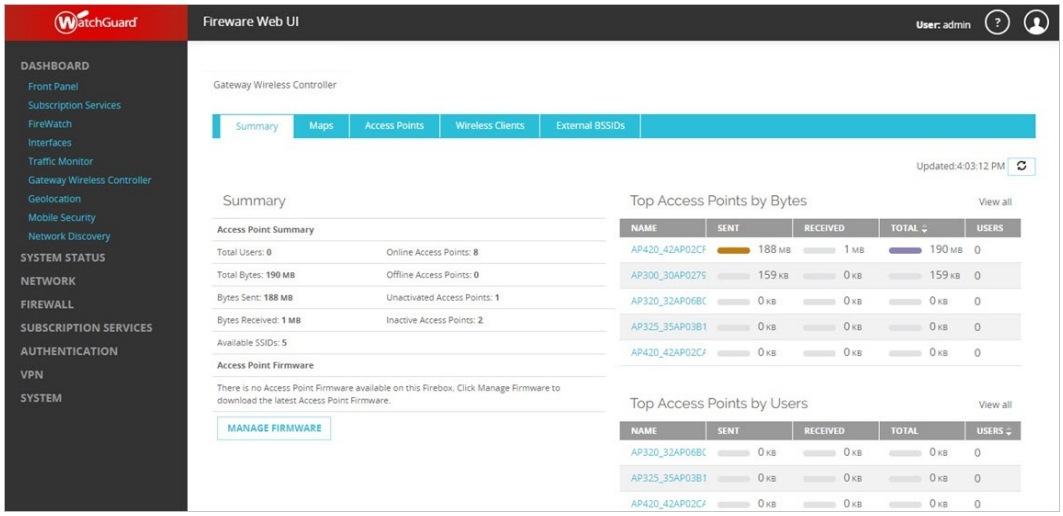
To trust an AP:

1. Select the AP.
2. Click **Action**.
3. Select **Mark Trusted**.

Monitor AP Status

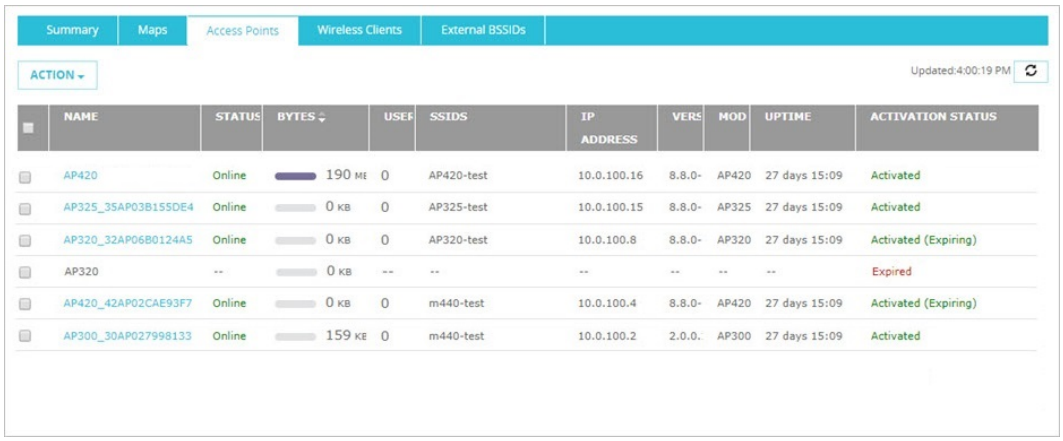
You can monitor, reboot, upgrade, view and update the status of AP licenses, and complete many other actions on WatchGuard APs managed by your Firebox.

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

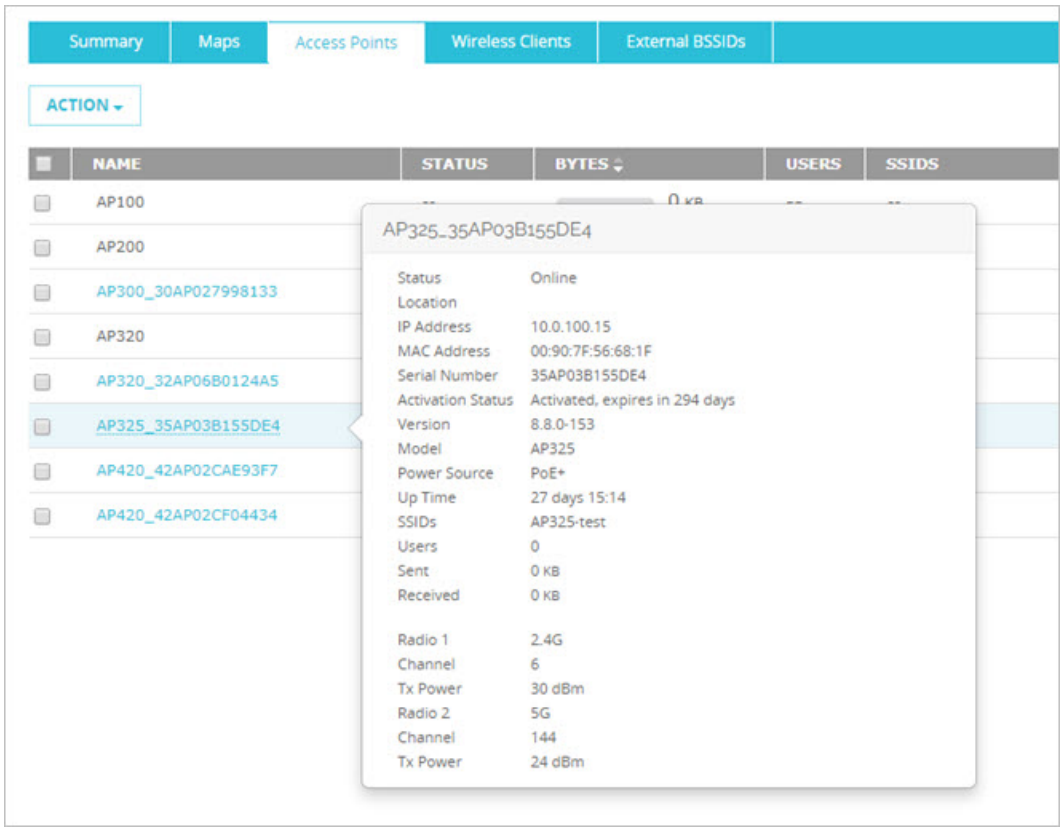


   The *Summary* section shows a status summary for the AP and the available firmware version. The *Top Panel* sections show real-time data about the traffic through the AP.

3. Select the **Access Points** tab.



Click on an AP to see a pop-up window that shows detailed information about the AP.



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

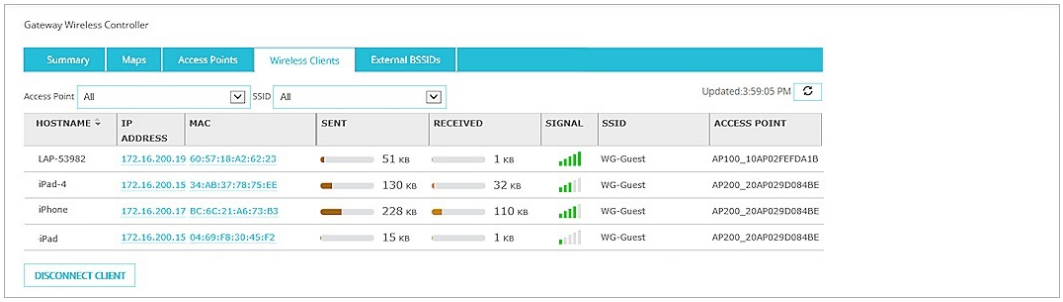
- See the connection status and uptime of each AP.
- See the radio frequency and channel used by each radio.
- See the power source used by an AP.
- See the transmit power and secondary channel information.
- See the AP activation and feature key status.
- See the log messages for the selected AP.
- See network statistics for the selected AP.
- Flash the power LED on the AP for identification.
- Reboot APs.
- Upgrade the firmware on APs.
- Trust an AP.
- Reset APs to factory default settings.
- Perform a site survey from a selected AP to detect other wireless access points.

Monitor Wireless Clients

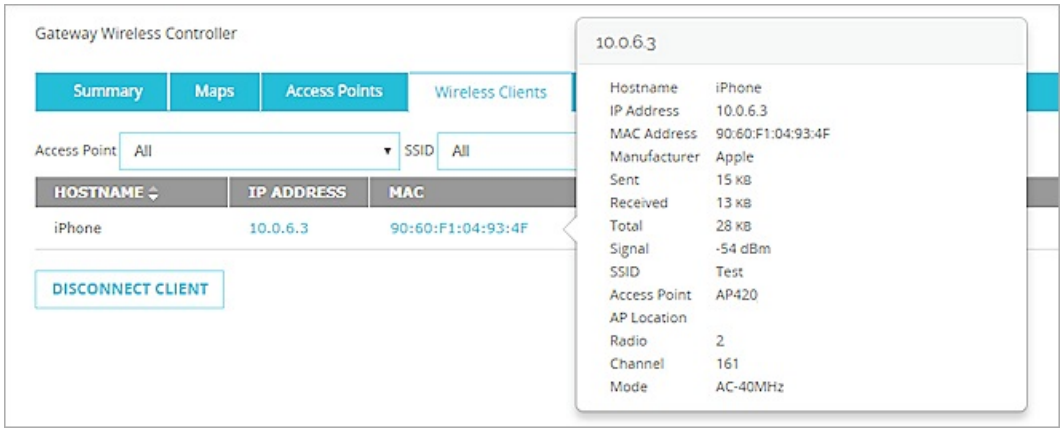
You can see and monitor the wireless clients that are connected to your WatchGuard APs. You can also disconnect a wireless client from an AP.

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.



- To see only wireless clients that are connected to a specific AP, from the **Access Point** drop-down list, select an AP .
- To see only wireless clients that are connected to a specific SSID, from the **SSID** drop-down list, select an SSID.
- To disconnect a wireless client, select the client and click **Disconnect Client**.
- To see statistics for a wireless client in FireWatch or Traffic Monitor, select an IP address.
- To see a pop-up window with detailed information about a client, click the MAC address.



Reset a WatchGuard AP

You can use any of these methods to reset a WatchGuard AP to factory-default settings:

- Reset the AP from the Gateway Wireless Controller
- Press the reset button on the AP
- Unpair an AP
- Disable automatic deployment for automatically deployed APs
- Reset the AP from the access point's local web UI

When you reset an AP to factory default settings, you must discover and pair the AP again

Reset a WatchGuard AP from the Gateway Wireless Controller

To reset the AP from the Gateway Wireless Controller, your Firebox must run Fireware v11.11.4 or higher.

To reset the AP, from Fireware Web UI:

1. Select **Dashboard > Gateway Wireless Controller**.
2. Select the **Access Points** tab.
3. Select an Access Point.
4. From the **Actions** drop-down list, select **Reset to Factory Default**.

To reset the AP, from Firebox System Manager:

1. Select the **Gateway Wireless Controller** tab.
2. Select the **Access Points** tab.
3. Select an Access Point.
4. From the **Actions** drop-down list, select **Reset to Factory Default**.

Reset a WatchGuard AP with the Reset Button

The reset procedure you can choose depends on the firmware version on your AP or your AP model.

To reset an AP100, AP102, AP200, or AP300 with firmware v1.2.9.2 or higher:

1. With the AP powered on, press and hold the reset button.
2. After 5 seconds, release the reset button.
   If you press the reset button briefly and then release the button (less than 5 seconds), the AP reboots, but it is not reset to factory-default settings.

To reset an AP100, AP102, AP200, or AP300 with firmware v1.2.9.1 or lower:

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

To reset an AP120, AP320, or AP322:

1. Remove the power cable or Ethernet cable connected to PoE power.
2. Insert a pin or paperclip into the Reset button hole.
3. While you press and hold the reset button, plug the power cable in.
4. Continue pressing the reset button for at least 60 seconds until the Power, LAN, and 2.4 GHz indicators are green.

To reset an AP125, AP225W, AP325, AP420, or AP327X:

1. Insert a pin or paperclip into the Reset button hole.
2. Press and hold the reset button for up to 10 seconds until all LEDs go off to indicate that the AP has rebooted.

Plan your Wireless AP Deployment

Before you deploy WatchGuard APs 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 Placement** – Determine the best location and placement of your WatchGuard APs.
- **Wireless Deployment Maps** – Use the Wireless Deployment Maps feature on the Gateway Wireless Controller to help deploy your WatchGuard APs, 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 APs 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.

- 2.4 GHz band – Supports 802.11b, 802.11g and 802.11n
- 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	1300 - 1733 Mbps	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, we recommend that you configure your WatchGuard AP to use mixed protocol modes.

If you choose a wireless mode that supports more than one 802.11 standard, the overall performance can be impacted. This is in part because of backward compatibility requirements 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 those devices.

Range

The 5GHz band is less congested and provides faster data rates than 2.4GHz, but it also 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 reduce your effective wireless range and data speeds.

Channels

A wireless channel is a specific division of frequencies in a specific wireless band.

2.4GHz Band

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 APs, use different channels for each AP and place them so that different channels are used in locations that do not overlap.

5GHz Band

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

Channel Width	Valid Channel Numbers
20 MHz	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 161, 165, 169
40 MHz	38, 46, 54, 62, 102, 110, 118, 126, 134, 142, 151, 159
80 MHz	42, 58, 106, 122, 138, 155
160 MHz	50, 114

About DFS Channels

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

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 APs being slow to connect on the wireless network.

AP Channel Selection

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

You can also manually set your preferred channel.

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, 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.

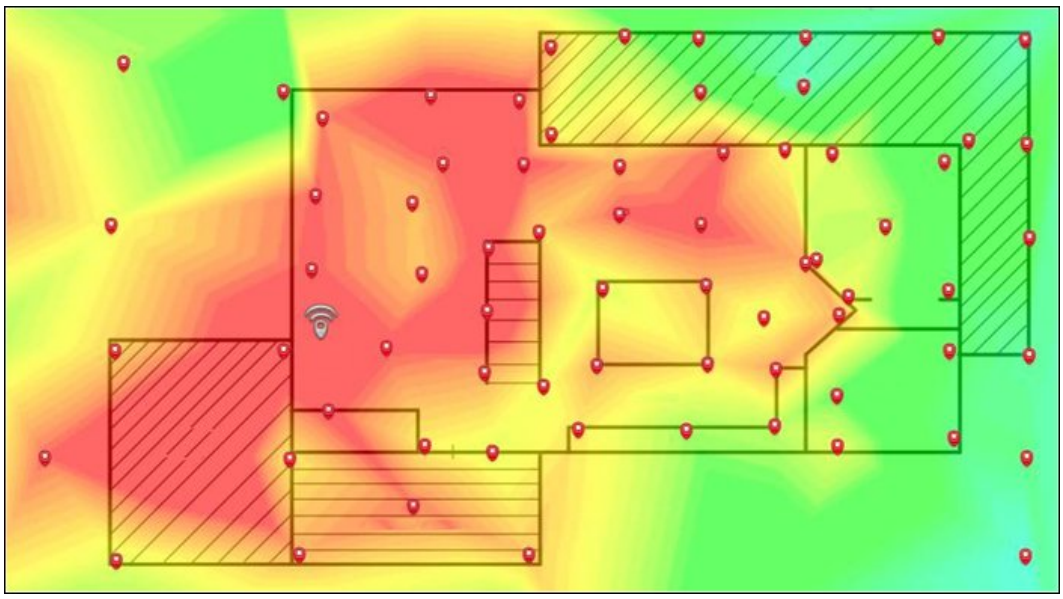
Site survey results can help you determine this information:

- Number of wireless clients that must be supported
- Airtime utilization and demand of wireless clients and applications
- Areas of coverage and number of APs required
- Best physical placement of APs
- Range from clients to each AP
- 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 APs, 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 APs 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 path loss and attenuation of your wireless signals as a result of these factors.

Walls and ceilings

Walls and ceilings between the AP 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.

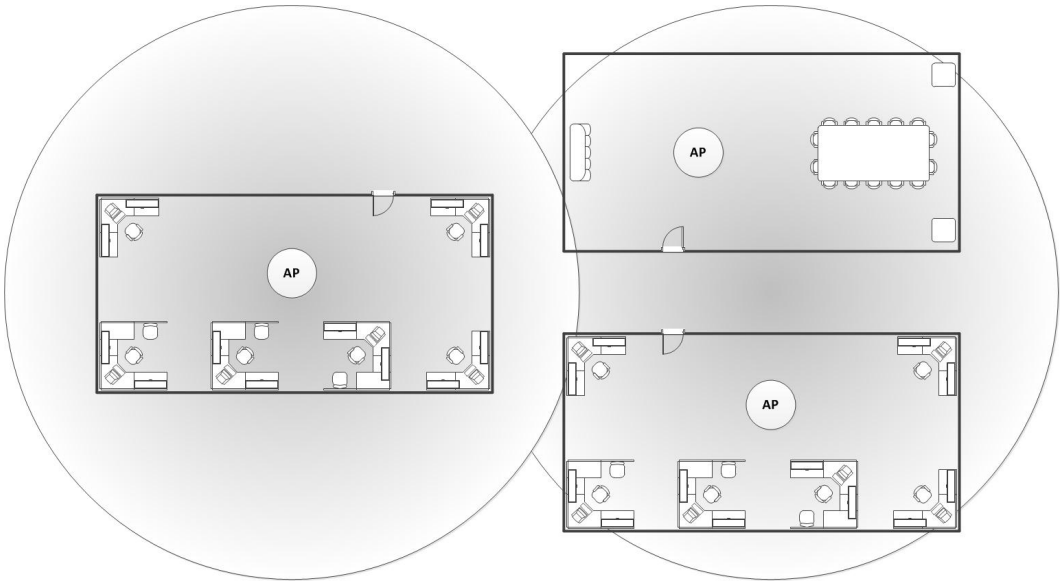
Distance

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

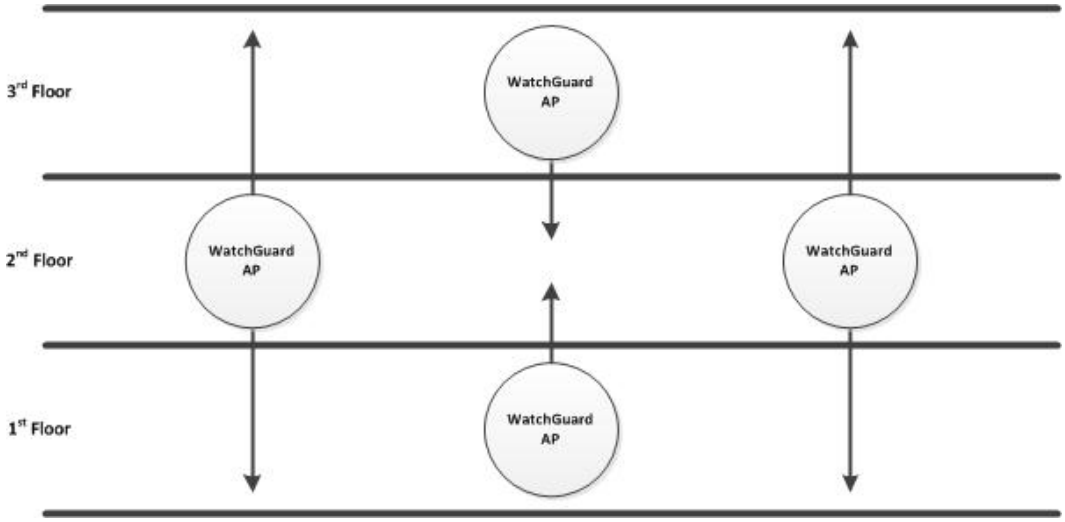
For full wireless coverage and to make sure that all users in your environment receive a strong wireless signal, consider these guidelines for the location and placement of your WatchGuard APs:

- Place your APs in a central location away from any corners, walls, or other physical obstructions to provide maximum signal coverage.
- Place your APs in a high location to provide the overall best signal strength reception and performance for your wireless network.
- In general, one AP can cover up to approximately 2000 ft^2 depending on the physical environment and wireless interference.



- Make sure you do not install an AP 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, 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 APs, 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 external BSSIDs (Broadcast SSID)
- Find rogue access points.

You can select two views:

- **Wireless Coverage Map** – Shows the location of your APs in relation to one another, and shows the connection quality and any channel conflicts between your APs.
- **Channel Conflict Map** – Shows the location of your APs 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.

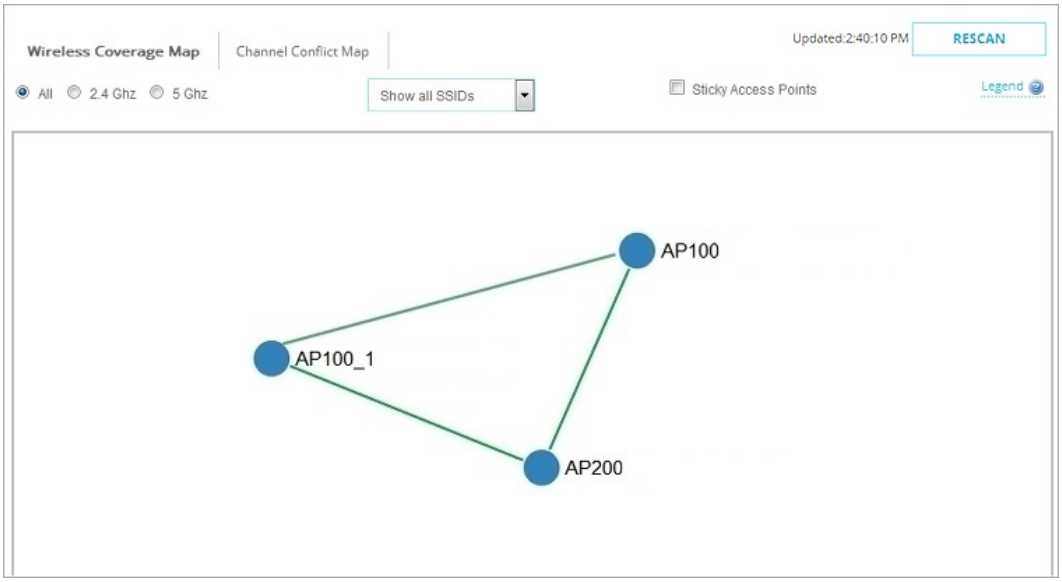
Use Maps for AP Placement

You can use the *Wireless Coverage Map* to provide a simulated physical view of your wireless network to help you place the APs in optimal locations for maximum coverage. After the initial scan, the maps display the relative location of each WatchGuard AP. Because the Wireless Coverage Map is a two-dimensional representation of your environment, APs 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 APs.

In an ideal deployment, your APs 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 APs for uninterrupted roaming for wireless clients.

For example, in this simple wireless network:

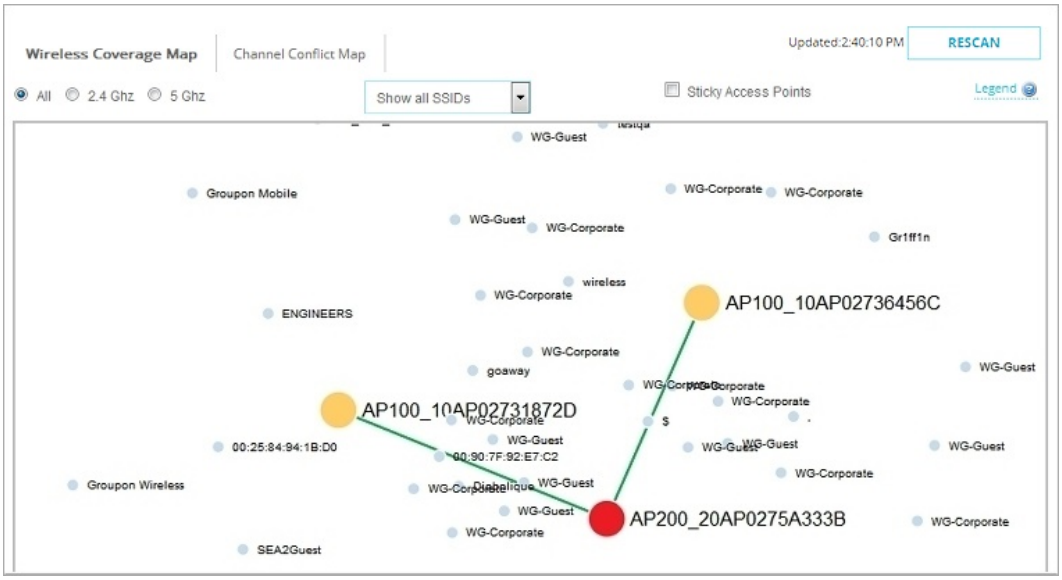
- There are three WatchGuard APs managed by this Gateway Wireless Controller.
- The APs are well positioned for maximum coverage.
- Wireless users have no interruptions when they roam from one AP to another.
- The solid green lines indicate a strong wireless connection with no channel conflicts between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



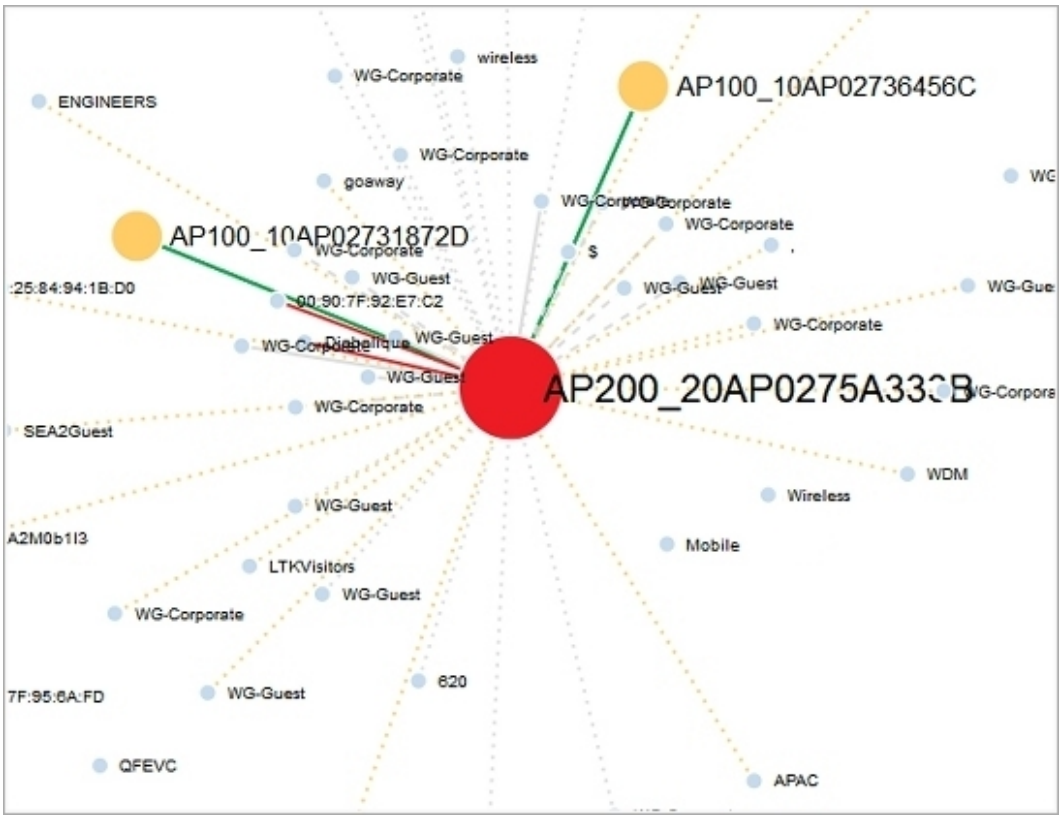
See Wireless Channel Conflicts

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 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 APs are green that indicates any wireless conflicts are with external devices, not with other WatchGuard APs in your network.

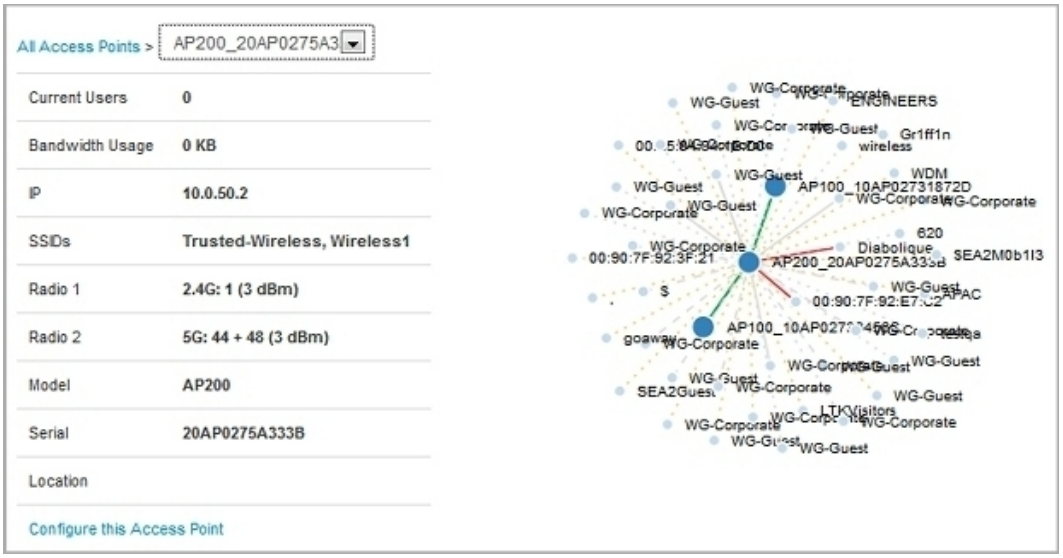


To see more detailed information on connections to other wireless devices, including external devices that are not other WatchGuard APs in your network, hover your mouse pointer over the AP200 device. The color and line detail indicate the severity of the conflict and signal loss.



To see more detailed information about the AP and any channel conflicts, right-click an AP 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, 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. 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, click **Configure this Access Point**.

If your **Preferred Channel** selection is set to **Auto**, the AP selects an appropriate channel when it reboots.

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

Find Rogue Access Points

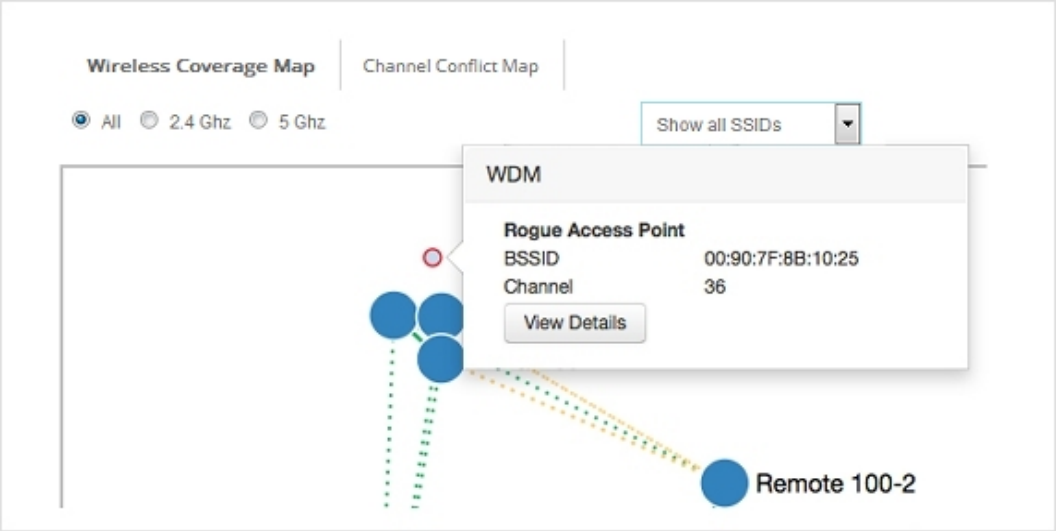
You can use the Wireless Deployment Maps to scan your network for all external wireless access points that operate within range of your managed APs. Some of these external access points could be rogue access points.

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.

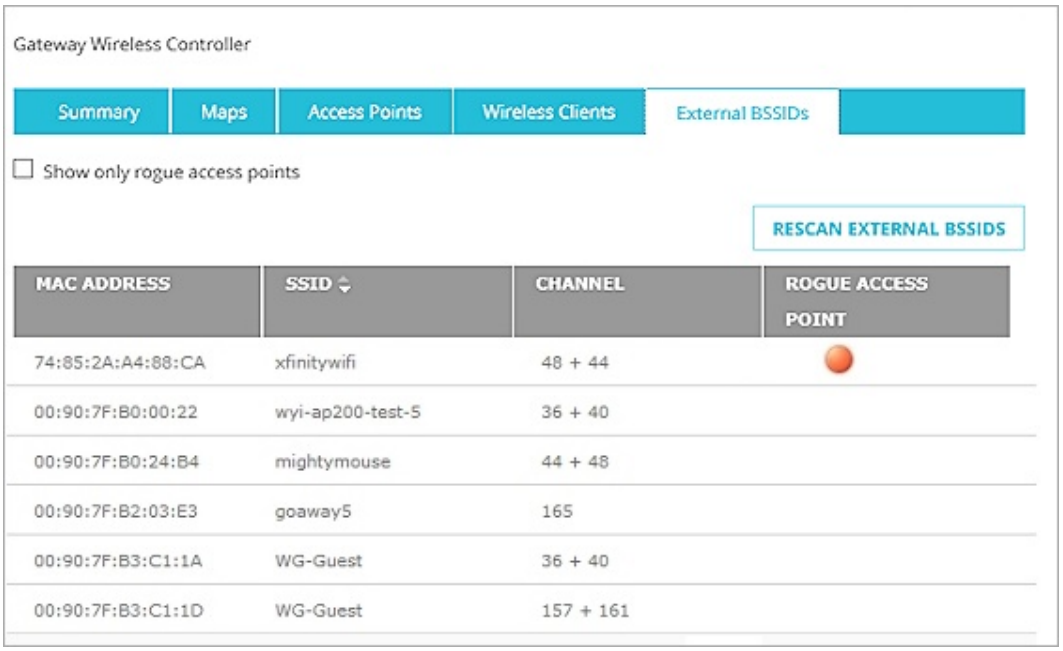
The Gateway Wireless Controller scans the wireless network on all wireless modes and channels within range for other wireless devices.

In the Wireless Deployment Maps, you can see all wireless devices and access points. This includes the APs managed by your Gateway Wireless Controller in the Wireless Coverage Map, and all external 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 external device in relation to your other devices on the network. You can also click any external device in the map and examine wireless details for that device.

Select the **External BSSIDs** tab to see all SSIDs broadcast by unknown APs (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.



Additional Resources

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

For information about your AP 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 configuration examples, see *Fireware Help*.

You can see and download the most current documentation for your WatchGuard AP on the WatchGuard website Documentation page.