Discover the Answer to Happy Users and Productive IT

"Why is the Wi-Fi not working?"

If this comment sounds all too familiar, you're not alone. Whenever a user experiences a problem, they will often blame Wi-Fi. They simply assume that since their laptop or smartphone is connected over Wi-Fi, the issue must be in the air. In many cases, the root cause arises from the LAN connection or application. Most Wi-Fi solutions do not give IT administrators the ability to appropriately determine where the problem is on the network and to fix it quickly. Admins need access to better answers.

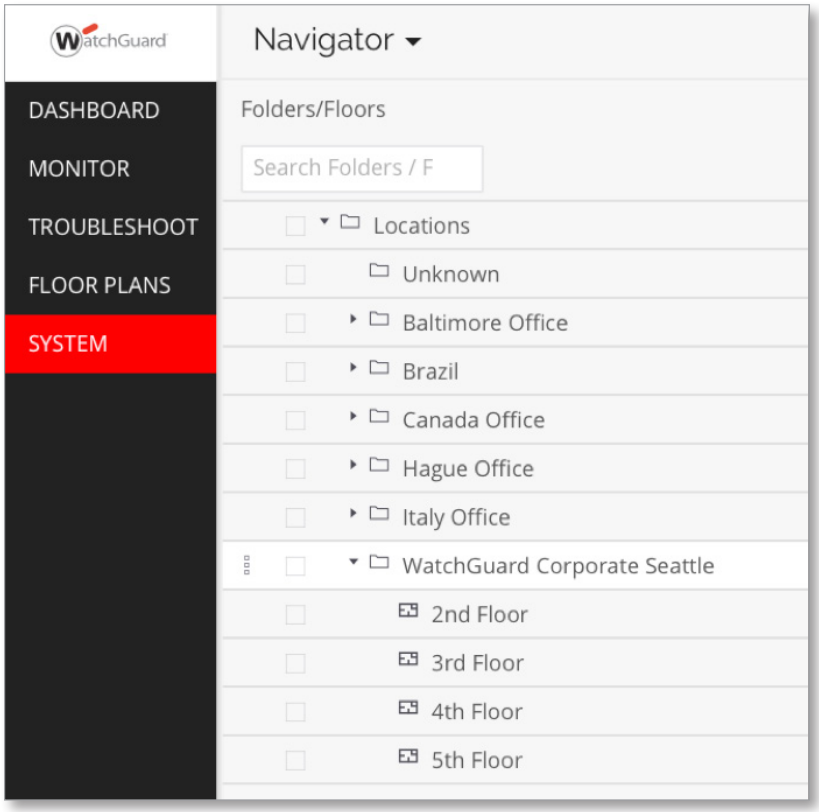
DISCOVER is the answer!

WatchGuard's Wi-Fi Cloud now includes the Discover app. Discover brings the most complete set of Wi-Fi **visibility, troubleshooting,** and **network health** features ever introduced to the market. After configuring your Wi-Fi settings in **Manage,** you'll find useful treasures inside Discover to:

- View a live snapshot of the **Client Journey** across all your locations
- Drill down into events to get clear answers to "**Why is the Wi-Fi not working?**"
- View **baselines** of performance data and more
- Receive **Alerts** when a network anomaly occurs above baseline thresholds
- Perform **Client Connectivity Tests** using WatchGuard access points with a 3rd radio
- Remotely troubleshoot problems with live **Spectrum Analysis** and live **Client Debugging**

Location-Based Information

Leveraging WatchGuard's Wi-Fi Cloud hierarchy-based management, Discover evaluates and displays metrics at the level selected, allowing views of the whole organization, site, or of a specific location.



Discover dashboard focuses on each type of problem:

- Connectivity
- Performance
- Applications

User Connections

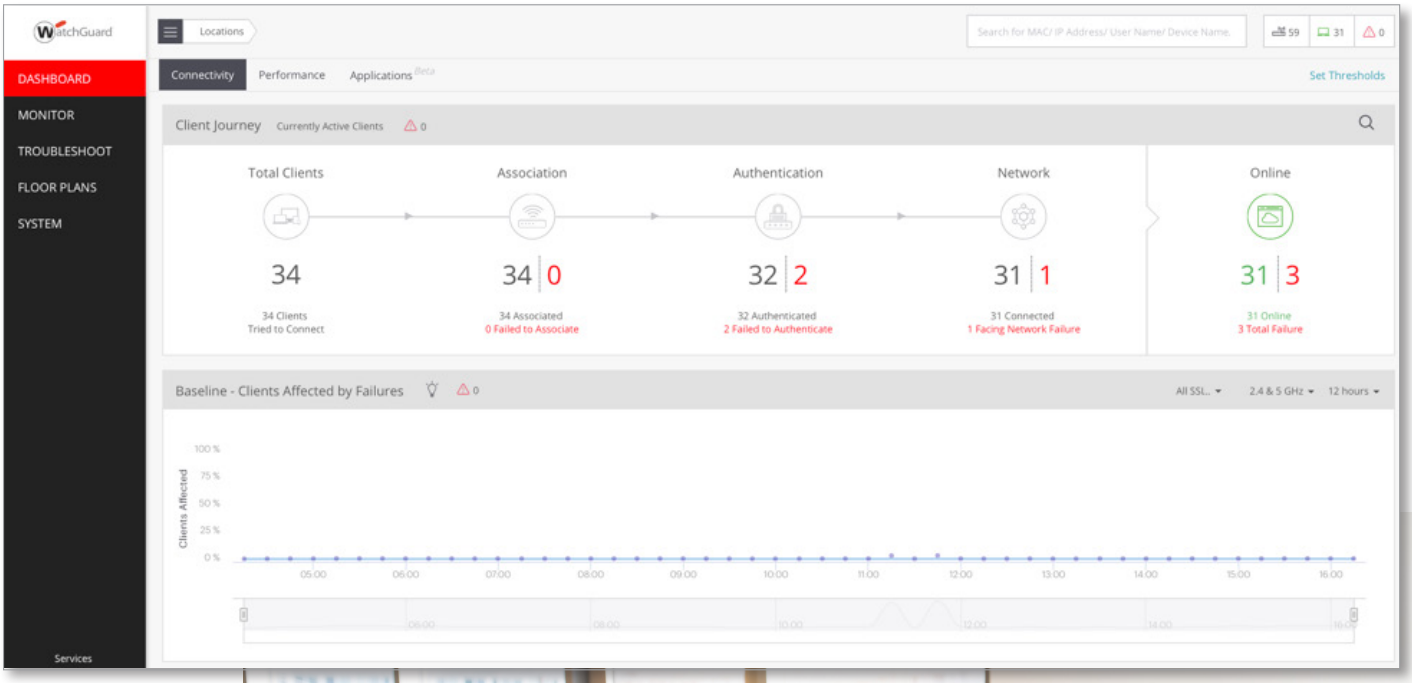
The Connectivity dashboard summarizes and highlights problems that may degrade the Wi-Fi user experience and require attention. It also builds a baseline of key metrics for each network and highlights anomalies that vary significantly from the baseline. Deeper insights can be found by a simple mouse-hover or by clicking and drilling down on specific Wi-Fi clients, APs, applications, or charts.

WatchGuard APs intelligently monitor clients as they connect to the Wi-Fi network. If a problem occurs, the AP detects it, automatically captures the clients' packets, performs a root cause analysis, and delivers the root cause with the packet capture to WatchGuard Wi-Fi Cloud. Client connection assessments (root cause analysis and packet capture) are available via the Cloud within seconds of a failed connection attempt and are maintained historically for investigation if needed.

Client Journey Location and Individual Client

The **Client Journey** is the main view of the Discover dashboard, which provides a real-time overview of the network's client connection problems. It is segmented into the stages each client goes through to connect to the WLAN: Association, Authentication, and Network (DHCP and DNS).

Each connection segment displays the number of clients that have succeeded or failed. Hovering over the failure (red) number in the stage summarizes the failures by root cause. Clicking drills down to provide more details on the clients. Clicking on a client drills deeper to show the connection logs. The packet trace of the event can be automatically opened in Packets for graphical analysis or downloaded locally for analysis in a packet analyzer like Wireshark. All of this is done within seconds of the connection problem occurring. The Client Journey section has its own search function that can be used to quickly find and view the connection information of a specific user. Search using MAC address, IP address, username, or device name to see the details of the last connection. Click to drill down to view a client's connection logs for the last month.

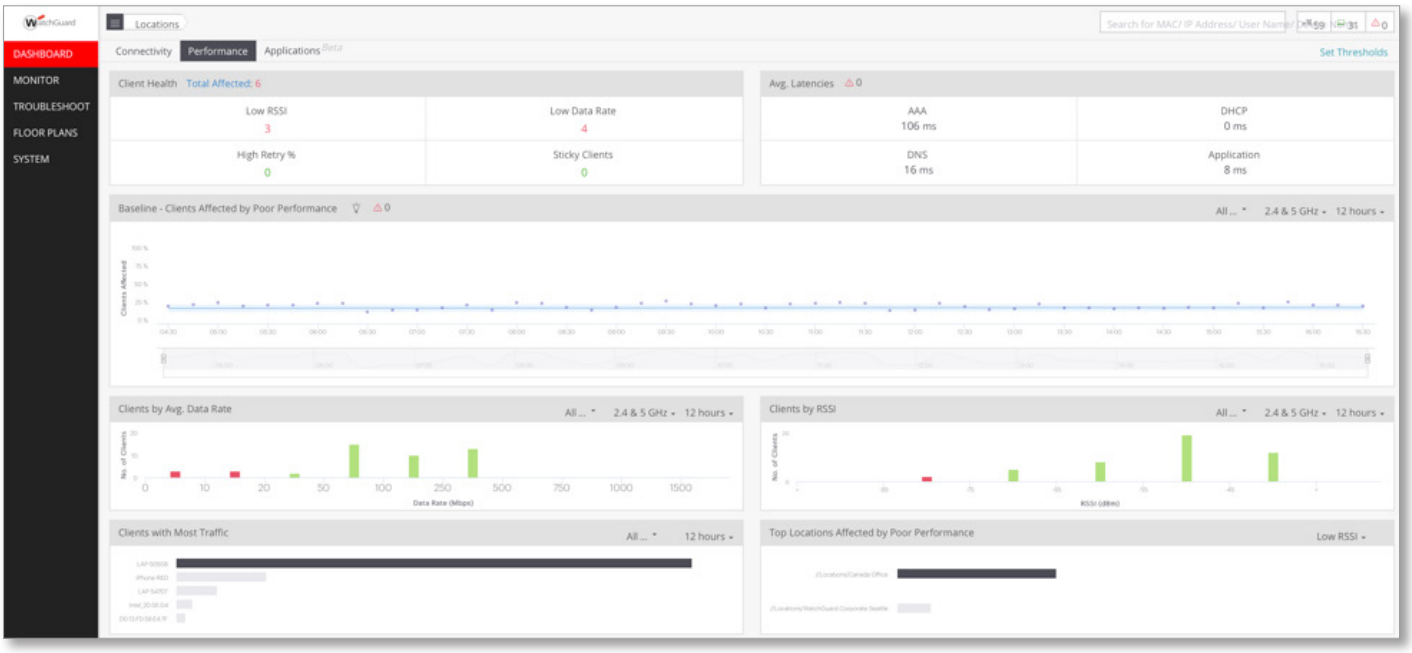


The Client Journey is the main view of the Discover dashboard

Performance

The user experience and application performance depend largely on the quality of a client's network health. The Discover application provides direct insight into the clients' network health and reports on both Wi-Fi and non-Wi-Fi issues that may cause poor application performance and poor user experience.

Provides direct insight into the clients' network health and reports on both Wi-Fi and non-Wi-Fi issues



Baselines and Anomalies

Traditional network monitoring systems use thresholds to evaluate key health and performance metrics. These thresholds are manually set and must be tuned because each network has different characteristics. Network managers typically disable threshold-based warning messages because they produce a significant number of false negatives and false positives.

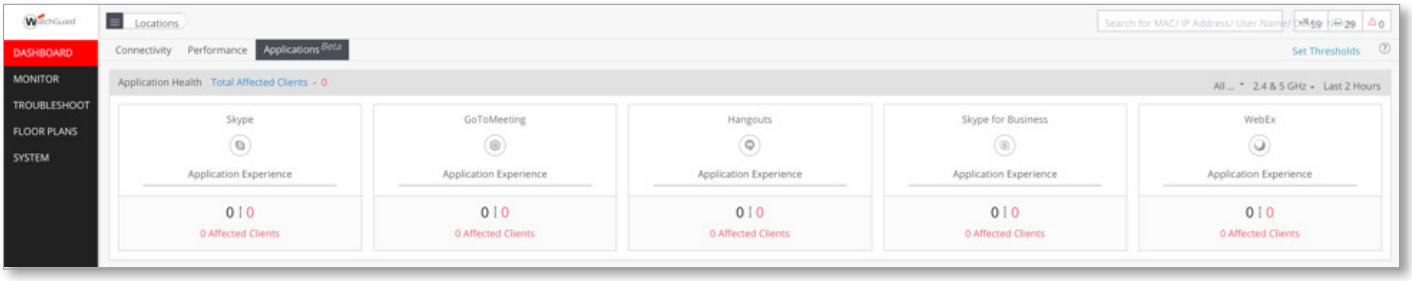
Wi-Fi Cloud Discover uses a different approach. It monitors ~300 variables and determines what is normal for each environment, draws baselines for the behavior, and highlights anomalous behavior to focus on what is important. Baselines are provided for critical Wi-Fi factors such as client connectivity, poor performance, data rates, latency, and applications.

Baselines are dynamic and adjust as the network characteristics change. Each baseline graph contains three components that make normal and unusual behavior easy to see:

- Baseline – dark blue line – weighted average that shows normal behavior
- Deviation range – blue area – normal range
- Anomalies – red dots – events significantly away from the baseline

Application Latency

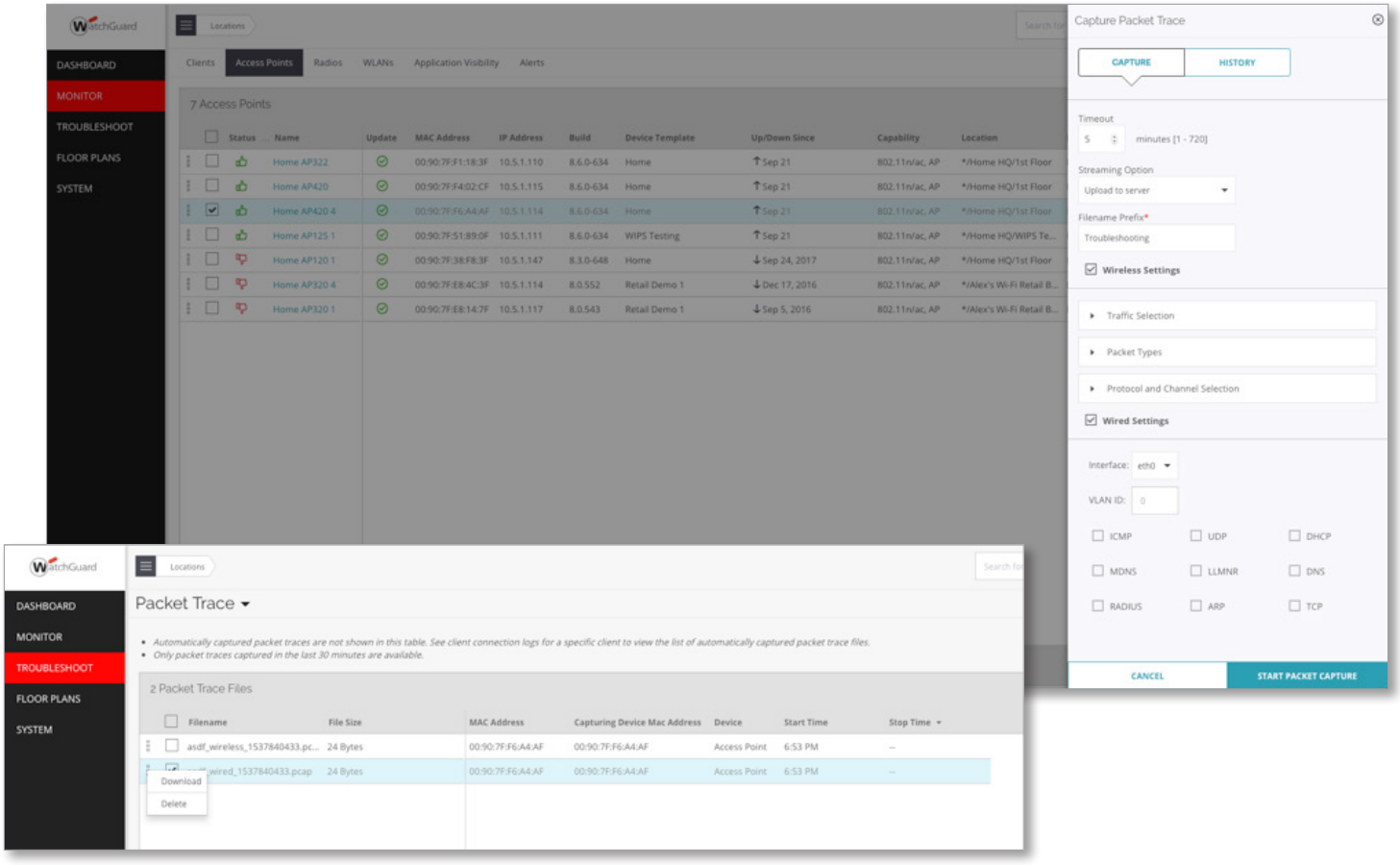
End-to-end application performance depends on both Wi-Fi and wired networks over which packets traverse. Users often blame Wi-Fi for performance problems when there could be a problem with the wired side of the network. Using deep packet inspection (DPI), WatchGuard parses all TCP connections for the network and separates them into wired and wireless components. The Application Latency baseline graph displays the wired and wireless components of TCP latency. Comparing these baselines allows you to narrow down the troubleshooting focus to the wired or wireless part of the network.



Troubleshooting

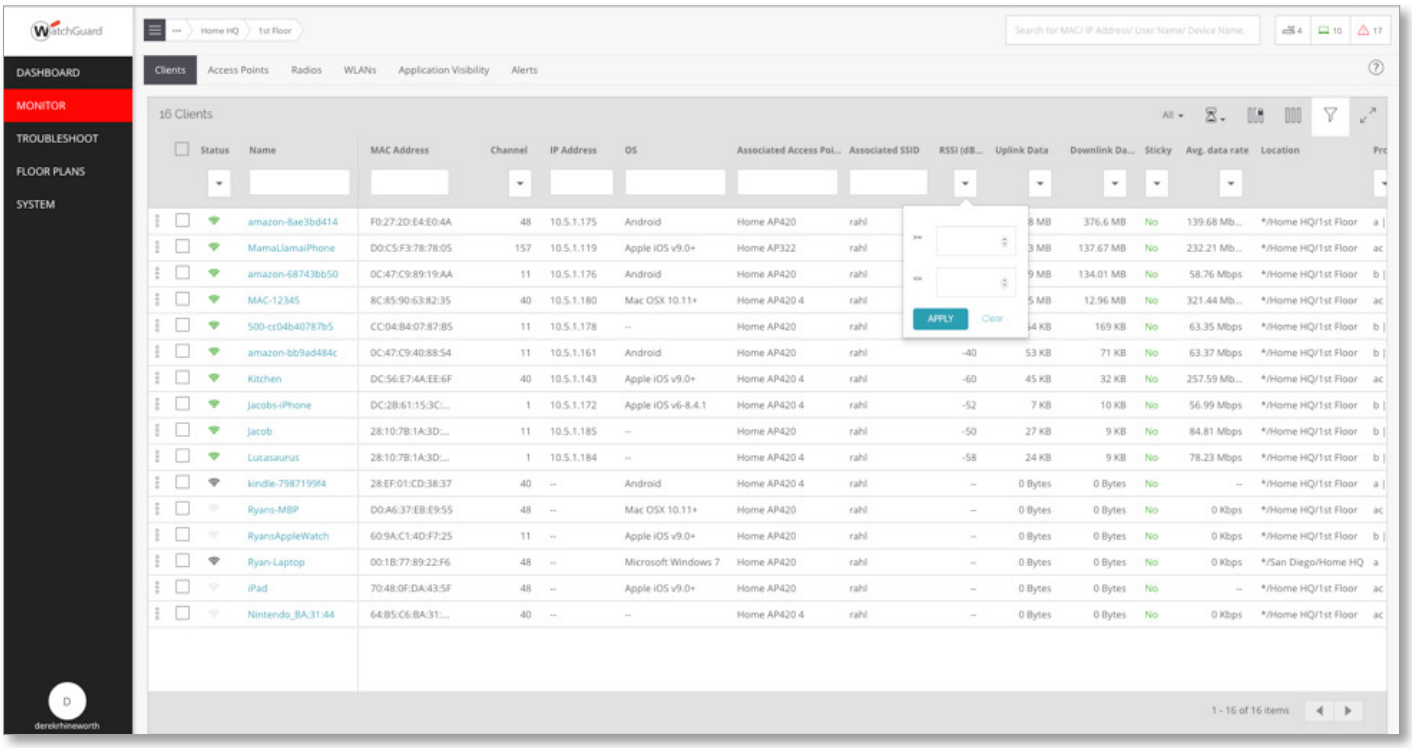
Traditionally, advanced Wi-Fi troubleshooting is a painstaking process, often requiring personnel to travel to the site, set up test gear, attempt to reproduce the problem and collect relevant information. Even when everything goes as planned, it is a tedious time-consuming process.

Discover app takes the pain out of troubleshooting by automating detection and root cause analysis of failures and anomalies. It can even help when the problem is not a Wi-Fi issue. If deeper analysis is necessary, Discover automatically captures the packet of connection problems and makes them available in the Troubleshoot tab (Packet Trace) or for download. Two of the Wi-Fi troubleshooting features available with Discover are Auto Packet Capture and using an AP's 3rd radio as a client of a neighboring AP.



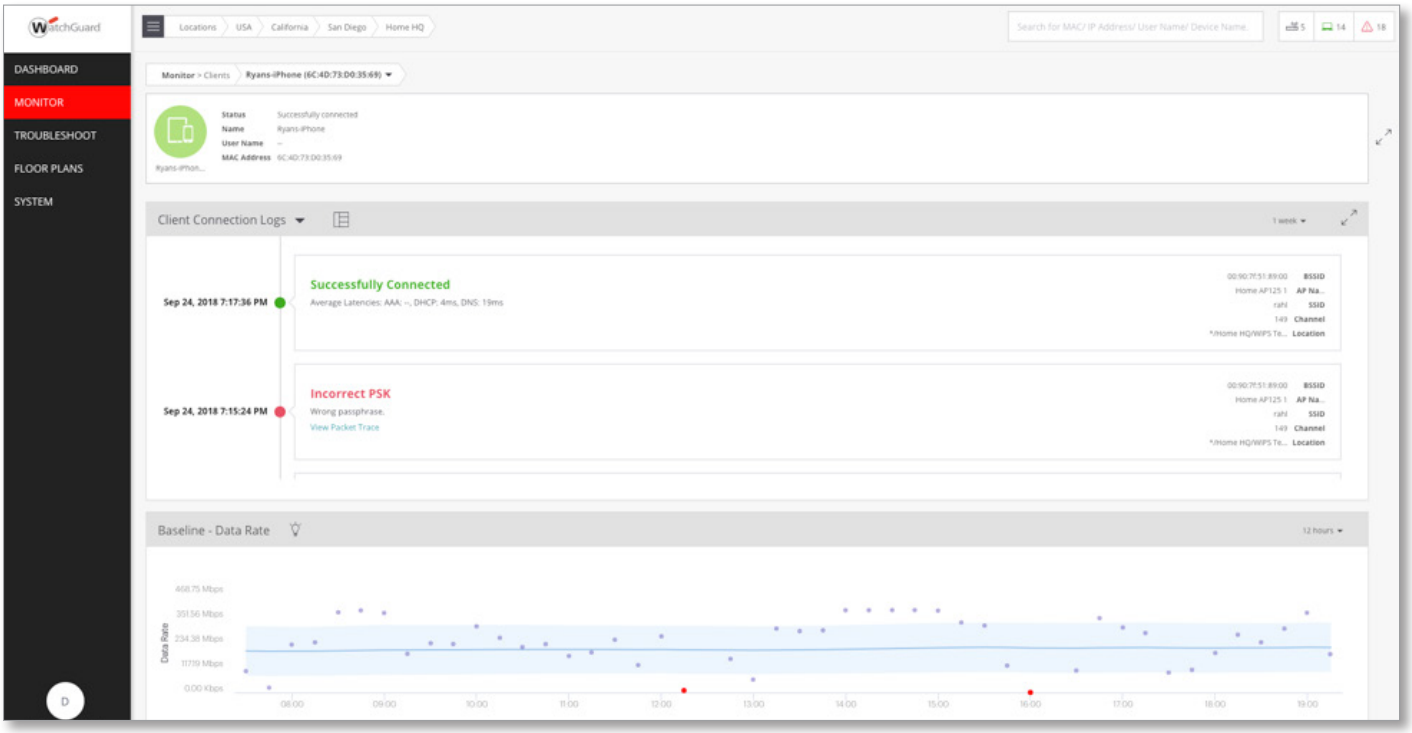
User Connections

The first step in troubleshooting a user-reported Wi-Fi issue is locating the user's information. Discover minimizes the pain of finding a troubled client by providing global, dynamic search capabilities for clients on the network. The main search bar is readily accessible at the top of the dashboard and it dynamically searches for clients based on their MAC or IP address, or by user (802.1x) or device name. The search refines as information is entered, character by character.



Root Cause Analysis Engine

Discover automatically detects and classifies in real time when Wi-Fi clients fail to connect and pinpoints the root cause (whether it's related to Wi-Fi, network service, or a client device and/or application). Similarly, it automates root cause analysis of poor performance, e.g., poor coverage, high retry rate, sticky clients.

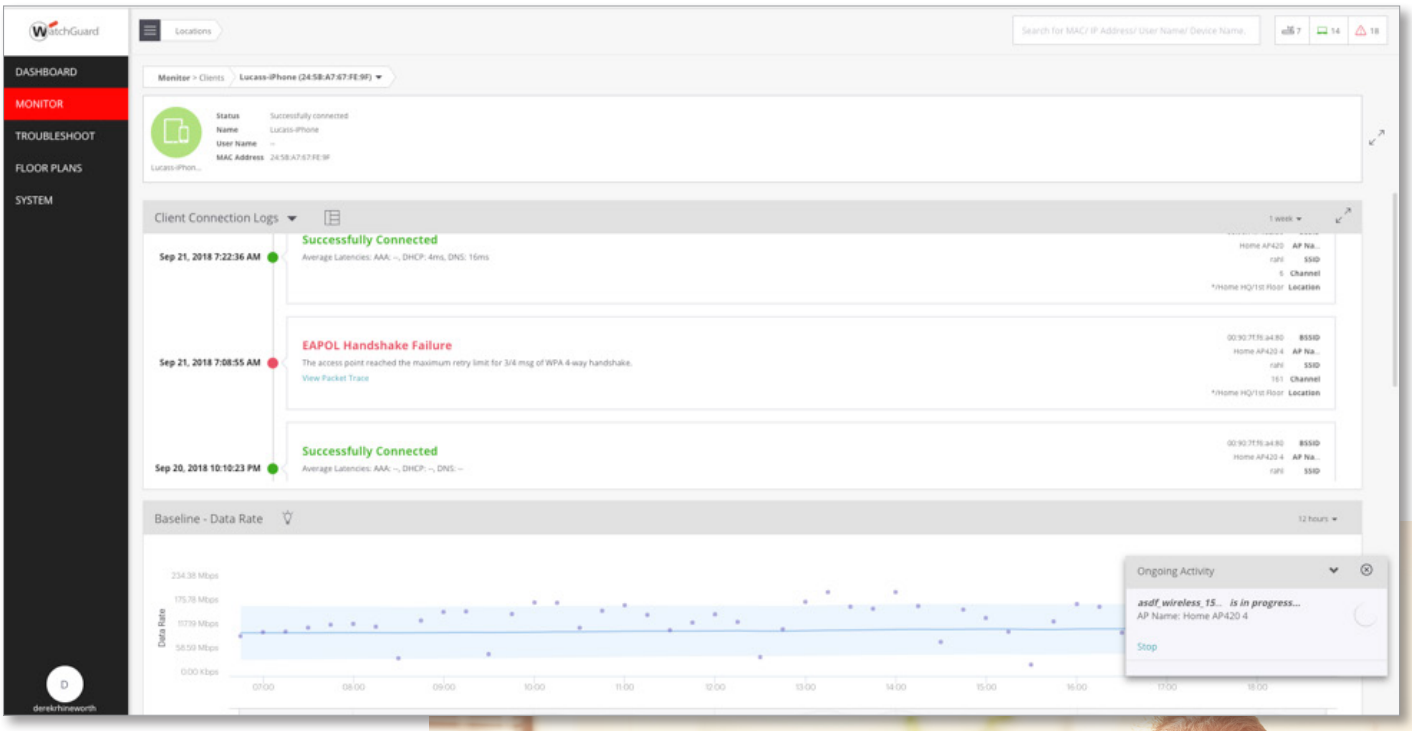


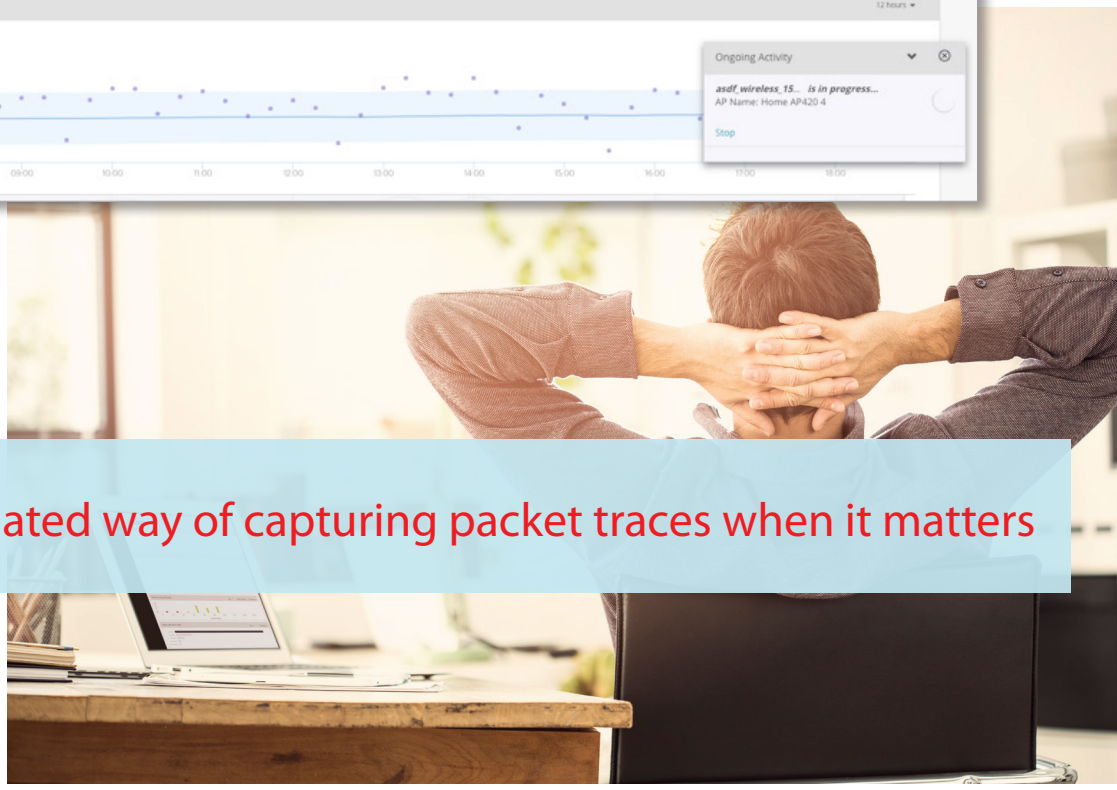
Automatic Packet Capture

Network troubleshooters often rely on capturing packet traces for advanced Wi-Fi problem solving. Most of the time a packet capture tool is not running when a problem occurs, so the administrator must coordinate with the user(s) that experienced the problem and seek their help to reproduce so that it can be captured in a packet trace. Special tools for Wi-Fi packet capture and analysis, and the presence of on-site Wi-Fi experts are often needed.

Discover provides a smarter, automated way of capturing packet traces when it matters. Each WatchGuard AP captures packets for each client as it connects to the network. When a problem occurs, the AP detects the problem, performs root cause analysis, saves the captured packets, and reports all that information to the Cloud.

All necessary information is captured in real time, as the problem occurs and is available in the Discover UI within seconds. The packets are captured in the context of the troubled Wi-Fi client that experienced the problem. The inconvenience of travel and problem reproduction is avoided. Reviewing the trace is as easy as downloading the packet capture and viewing it in popular packet-viewing tools.

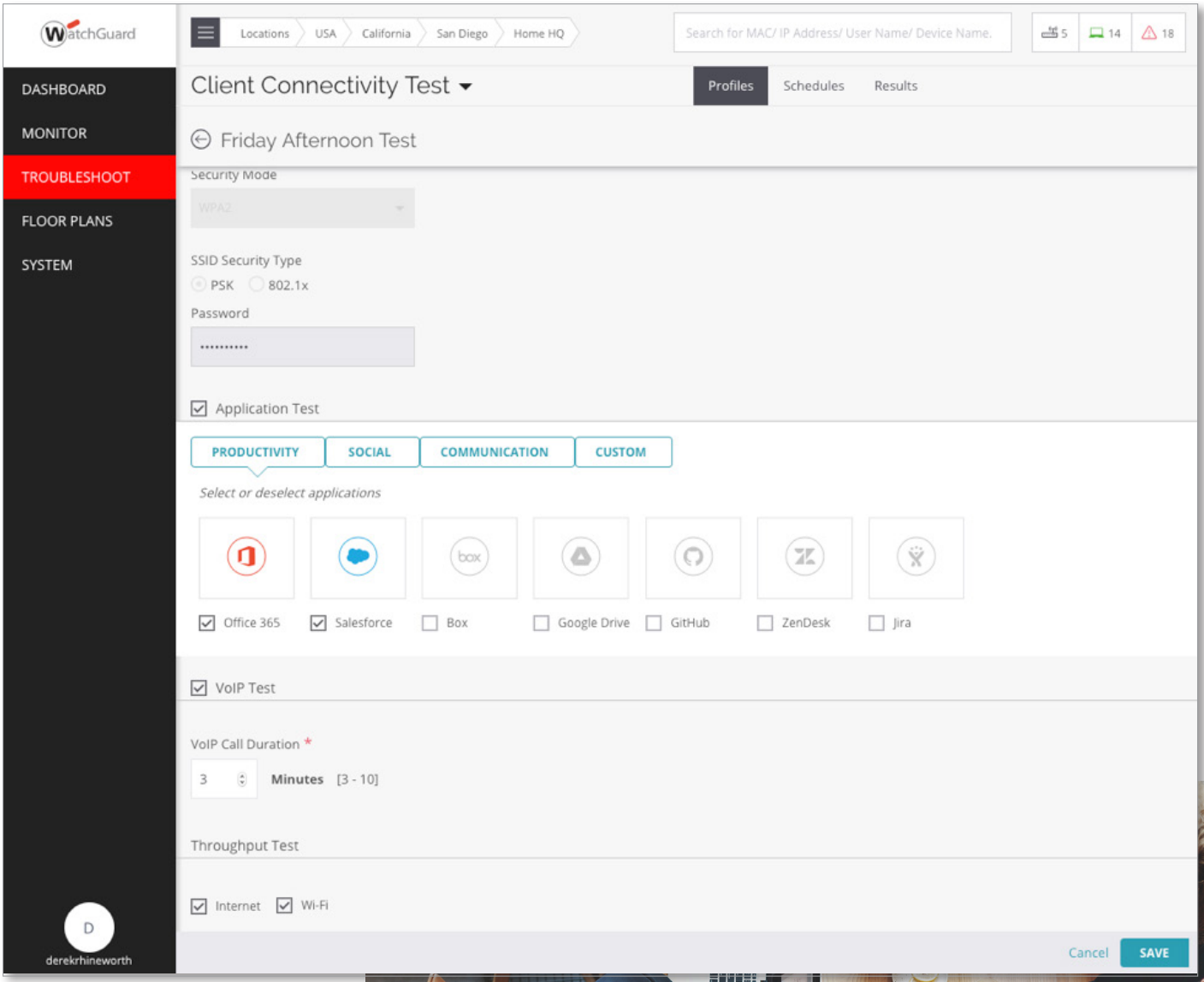


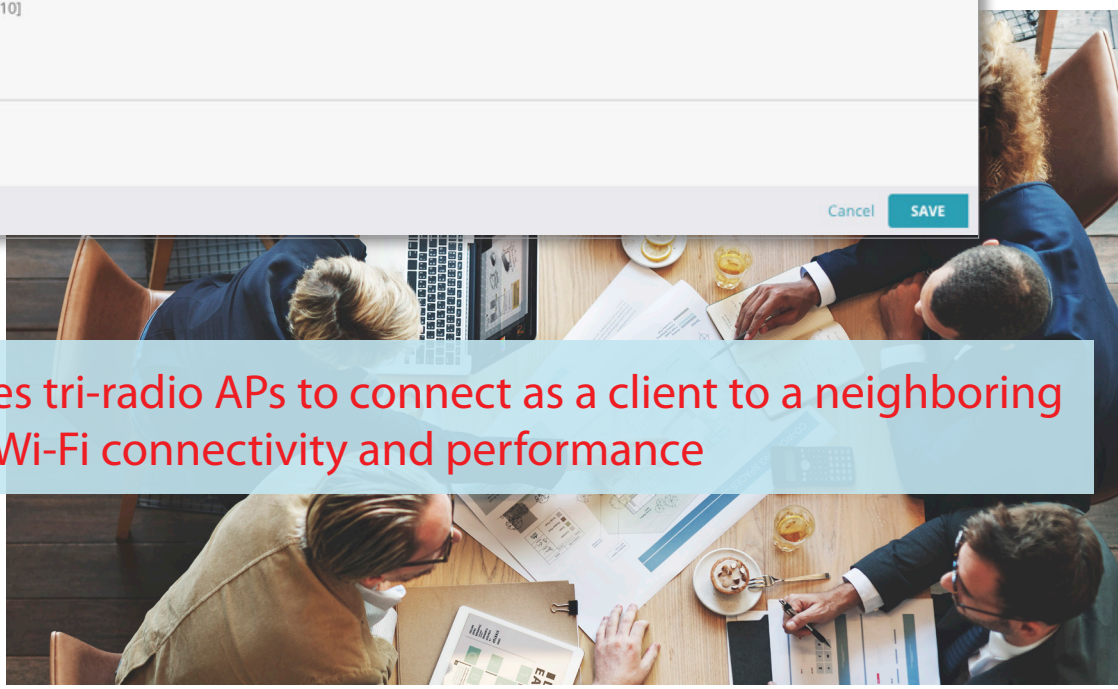


Smarter, automated way of capturing packet traces when it matters

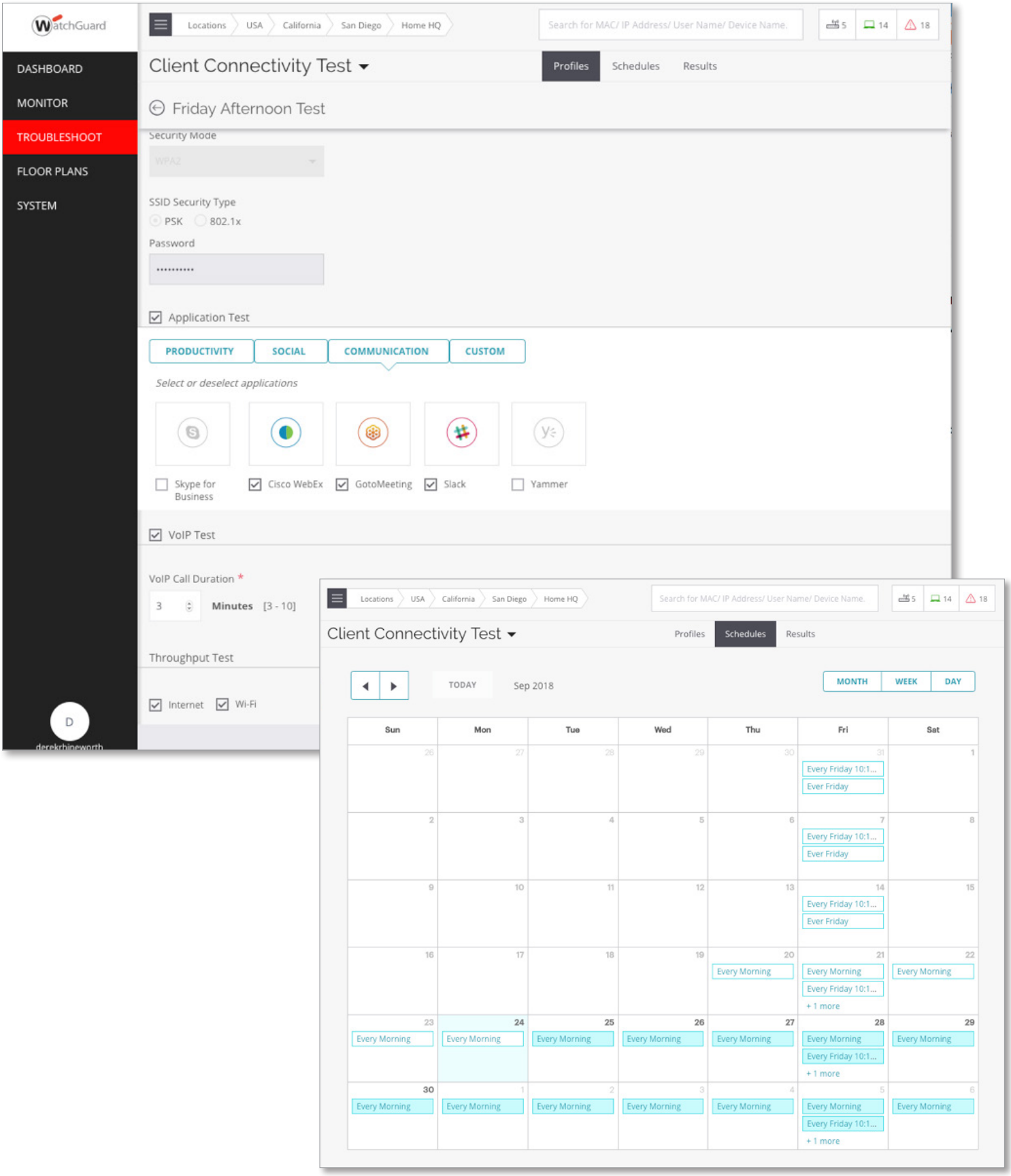
Client Emulation and Network Profiling

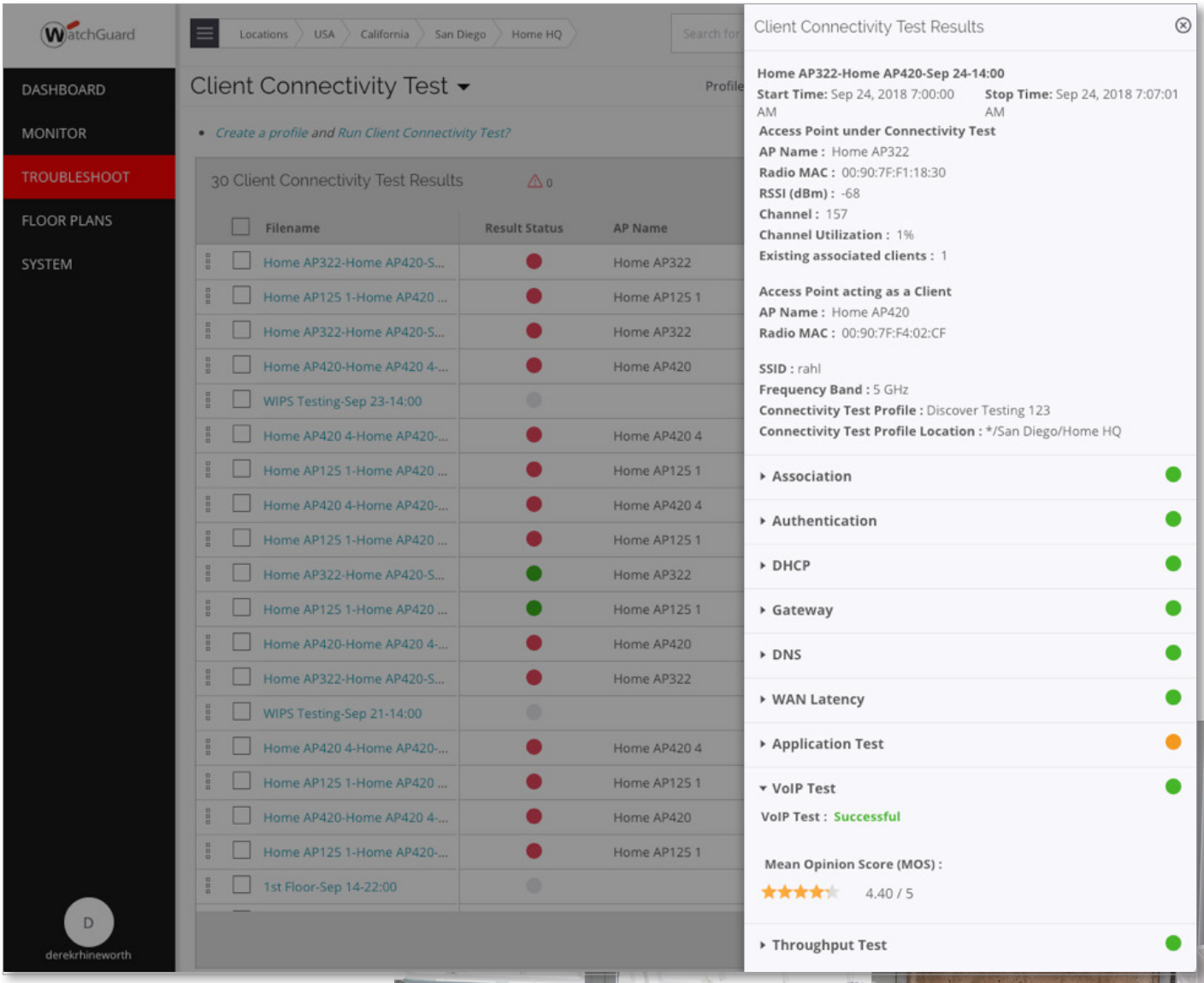
Discover enables tri-radio APs (AP325 and AP420) to connect as a client to a neighboring AP to evaluate Wi-Fi connectivity and performance. Tests can be run on demand or can be scheduled and repeated. To run on demand, right-click on the AP, select a test profile and frequency band and the neighboring tri-radio AP to connect as a client. Each run tests Wi-Fi, network, and Internet connectivity. Application, VoIP, and throughput tests can be included in the test template as desired.

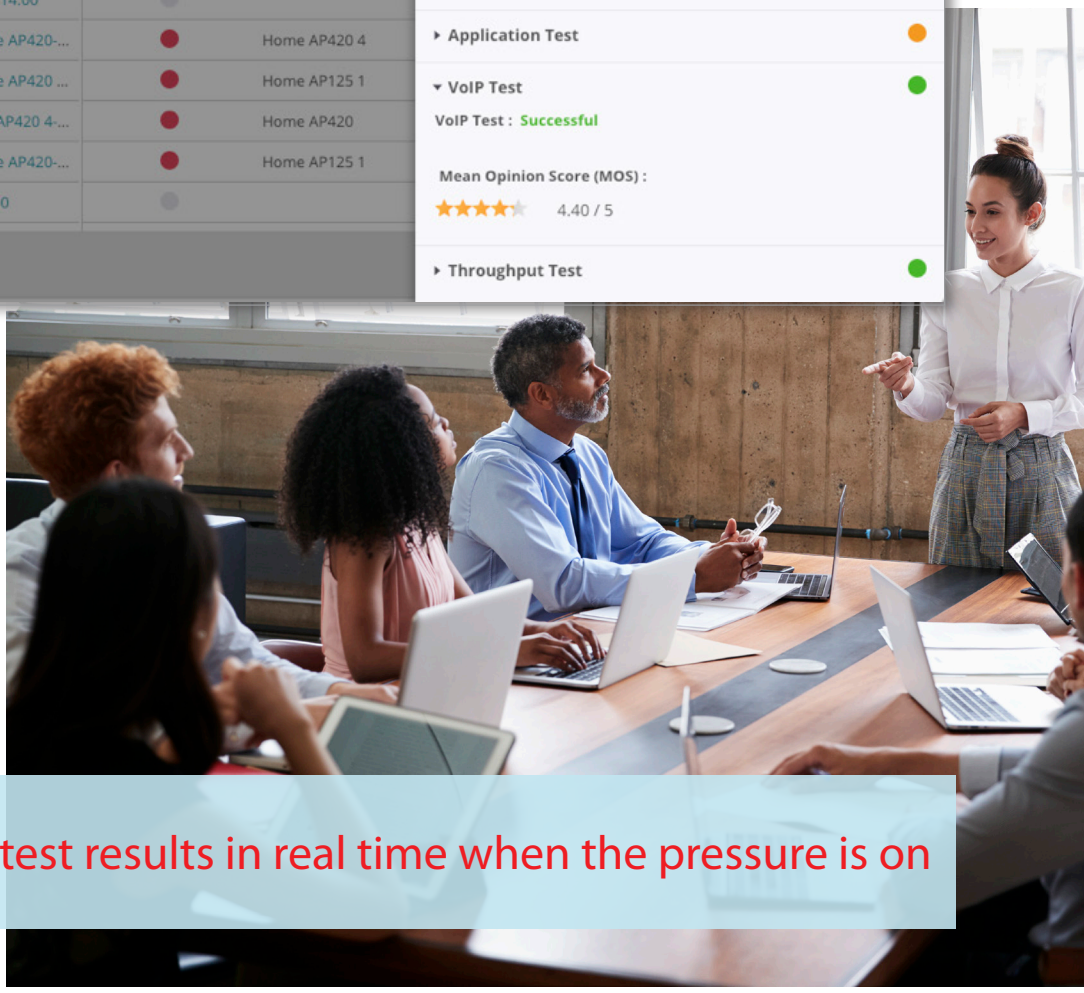




Discover enables tri-radio APs to connect as a client to a neighboring AP to evaluate Wi-Fi connectivity and performance


WatchGuard
DASHBOARD
MONITOR
TROUBLESHOOT
FLOOR PLANS
SYSTEM
Locations
USA
California
San Diego
Home HQ
Search for MAC/ IP Address/ User Name/ Device Name.
5
14
18
Client Connectivity Test
Profiles
Schedules
Results
Friday Afternoon Test
Security Mode
WPA2
SSID Security Type
PSK
802.1x
Password
Application Test
PRODUCTIVITY
SOCIAL
COMMUNICATION
CUSTOM
Select or deselect applications
Skype for Business
Cisco WebEx
GotoMeeting
Slack
Yammer
VoIP Test
VoIP Call Duration *
3
Minutes [3 - 10]
Throughput Test
Internet
Wi-Fi
D
derekrhineworth
TODAY
Sep 2018
MONTH
WEEK
DAY
Sun
Mon
Tue
Wed
Thu
Fri
Sat
Every Friday 10:1...
Ever Friday
Every Morning
+ 1 more

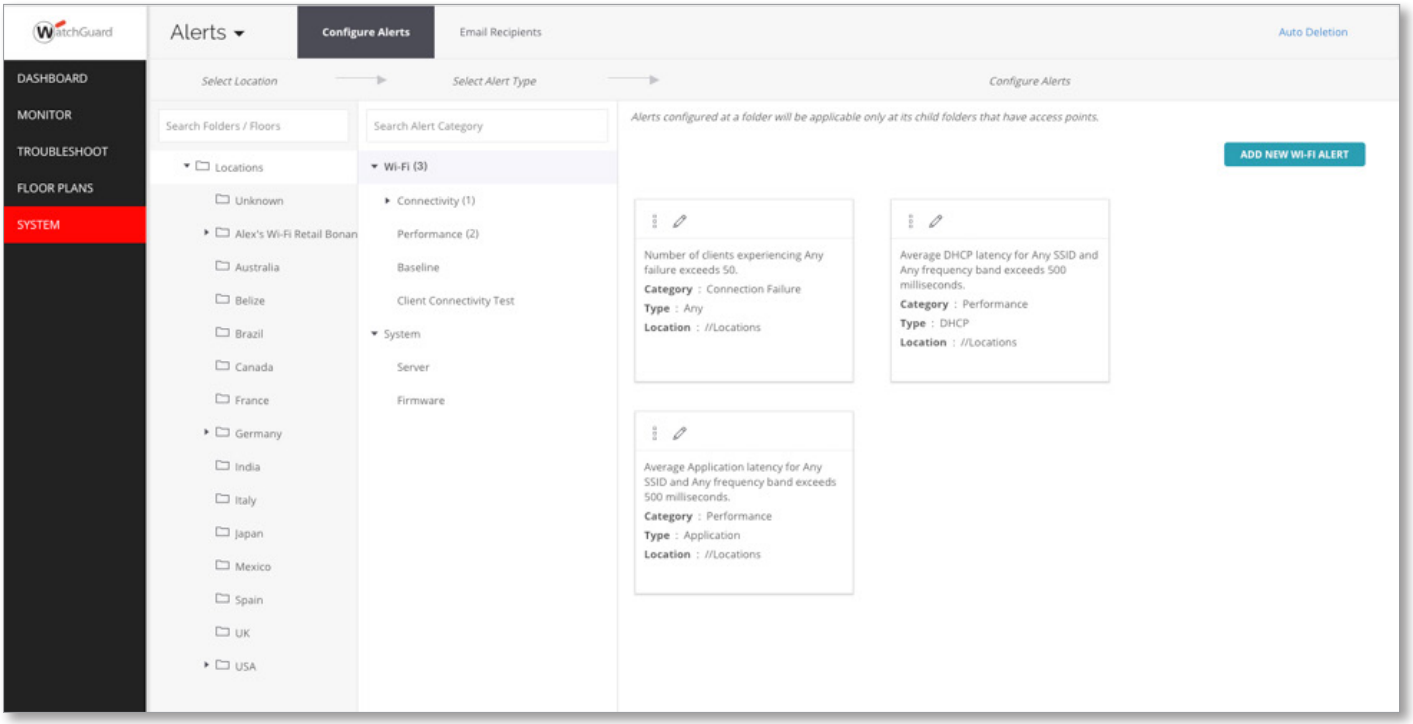


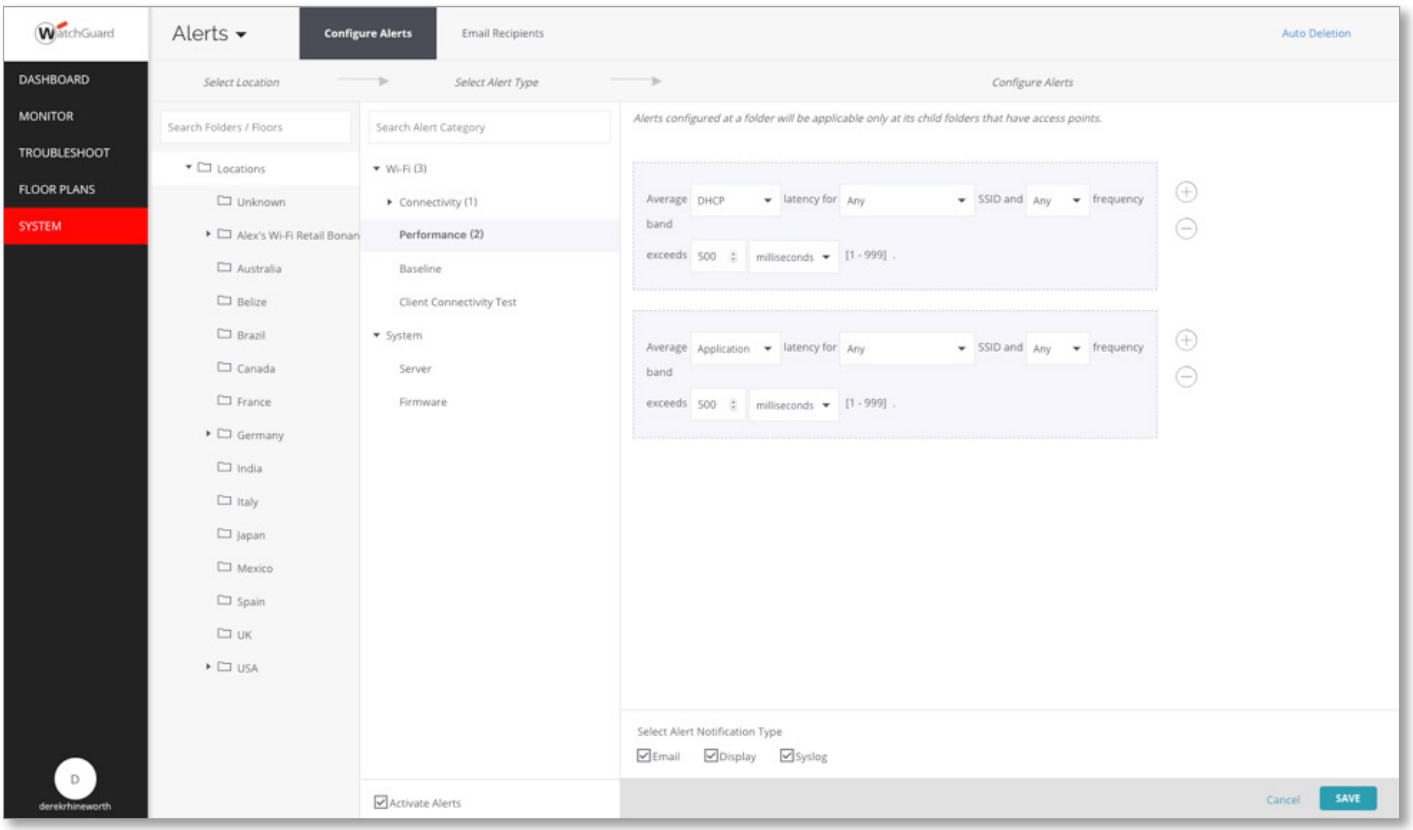


Quickly see your test results in real time when the pressure is on

Alerts

Maintaining Service Level Agreements (SLAs) is a breeze using the Alerts feature within Discover. Maintain SLAs and keep your Wi-Fi network running smooth. Have an option to configure alerts to be sent to your PSA tool ticketing system via email, to the Discover UI, and optionally to the Syslog stream output. Alerts can be configured to monitor client connectivity, network services performance, a variety of anomalies above baseline thresholds, or any of your configured Client Connectivity Tests.

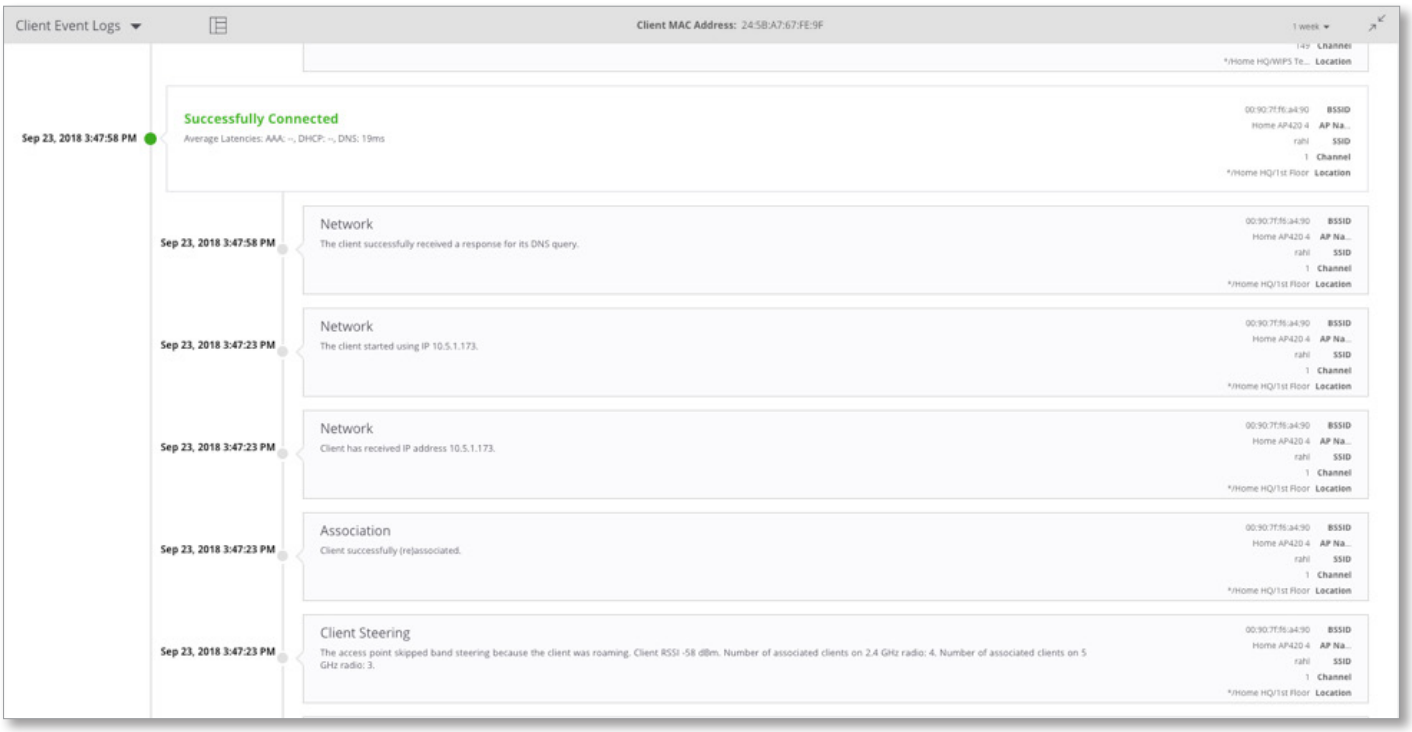




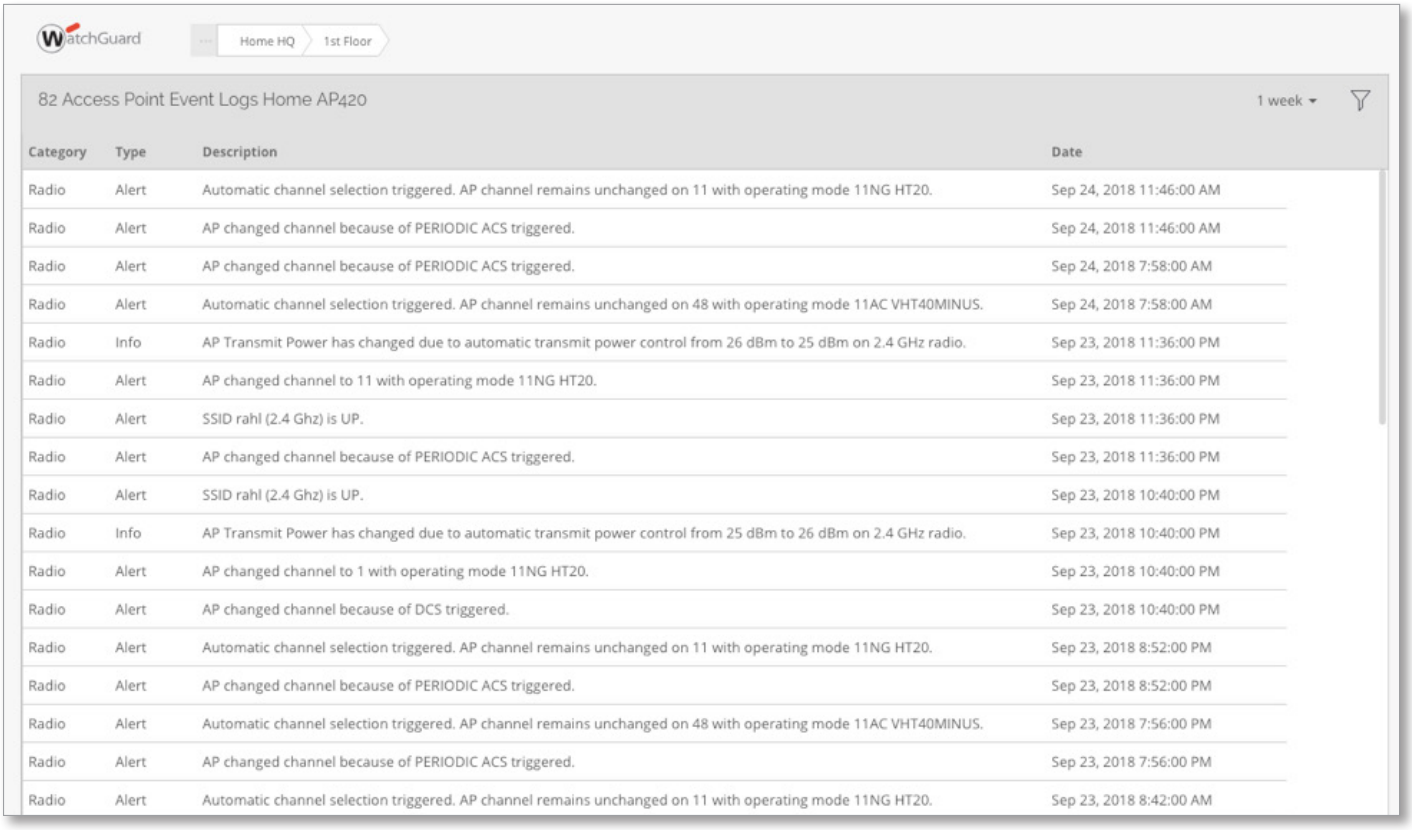
Client and AP Event Logging

Discover offers a number of ways to view what is going on with a client or the access point. See the full story over time of any access point or client and events that happen during the connection: channels changed, transmit power adjusted, roaming initiated and much more. This critical information can fill in the gaps to answer, "what changed?".

Client Event Log



AP Event Log



Category	Type	Description	Date
Radio	Alert	Automatic channel selection triggered. AP channel remains unchanged on 11 with operating mode 11NG HT20.	Sep 24, 2018 11:46:00 AM
Radio	Alert	AP changed channel because of PERIODIC ACS triggered.	Sep 24, 2018 11:46:00 AM
Radio	Alert	AP changed channel because of PERIODIC ACS triggered.	Sep 24, 2018 7:58:00 AM
Radio	Alert	Automatic channel selection triggered. AP channel remains unchanged on 48 with operating mode 11AC VHT40MINUS.	Sep 24, 2018 7:58:00 AM
Radio	Info	AP Transmit Power has changed due to automatic transmit power control from 26 dBm to 25 dBm on 2.4 GHz radio.	Sep 23, 2018 11:36:00 PM
Radio	Alert	AP changed channel to 11 with operating mode 11NG HT20.	Sep 23, 2018 11:36:00 PM
Radio	Alert	SSID rahl (2.4 Ghz) is UP.	Sep 23, 2018 11:36:00 PM
Radio	Alert	AP changed channel because of PERIODIC ACS triggered.	Sep 23, 2018 11:36:00 PM
Radio	Alert	SSID rahl (2.4 Ghz) is UP.	Sep 23, 2018 10:40:00 PM
Radio	Info	AP Transmit Power has changed due to automatic transmit power control from 25 dBm to 26 dBm on 2.4 GHz radio.	Sep 23, 2018 10:40:00 PM
Radio	Alert	AP changed channel to 1 with operating mode 11NG HT20.	Sep 23, 2018 10:40:00 PM
Radio	Alert	AP changed channel because of DCS triggered.	Sep 23, 2018 10:40:00 PM
Radio	Alert	Automatic channel selection triggered. AP channel remains unchanged on 11 with operating mode 11NG HT20.	Sep 23, 2018 8:52:00 PM
Radio	Alert	AP changed channel because of PERIODIC ACS triggered.	Sep 23, 2018 8:52:00 PM
Radio	Alert	Automatic channel selection triggered. AP channel remains unchanged on 48 with operating mode 11AC VHT40MINUS.	Sep 23, 2018 7:56:00 PM
Radio	Alert	AP changed channel because of PERIODIC ACS triggered.	Sep 23, 2018 7:56:00 PM
Radio	Alert	Automatic channel selection triggered. AP channel remains unchanged on 11 with operating mode 11NG HT20.	Sep 23, 2018 8:42:00 AM

Live Client Debugging

Save time and expense in sending technical resources onsite to troubleshoot client issues when you can remotely monitor detailed WLAN debugging frames with clients. It is as easy as right-clicking on a client to start collecting debug logs in real time while the client is live on the network.

WatchGuard Live Client Debugging - Ryans-iPhone Download STOP

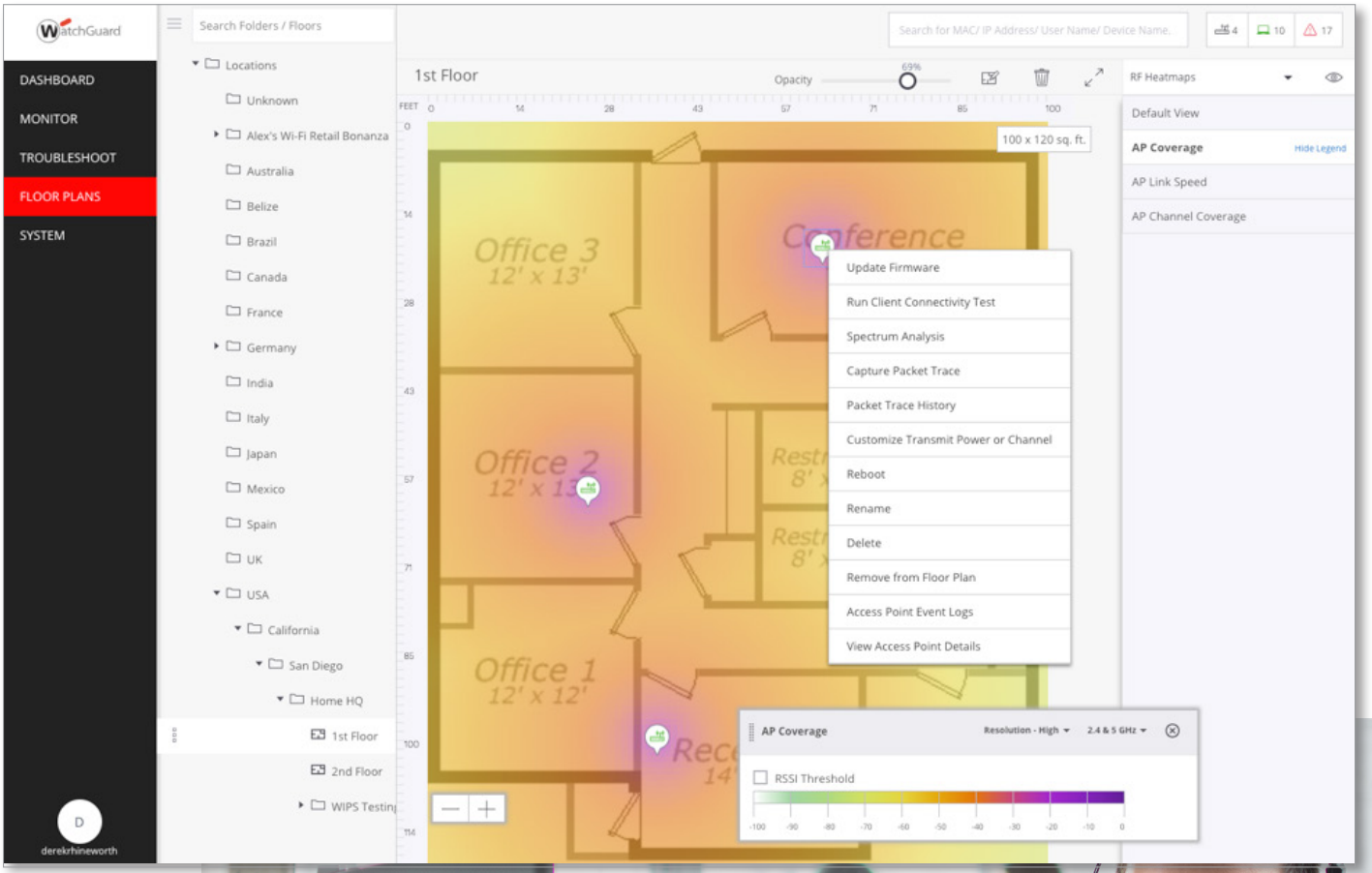
Download log file to view historical log entries from start time till now. **Remaining Time**: 00:04:34 Minutes

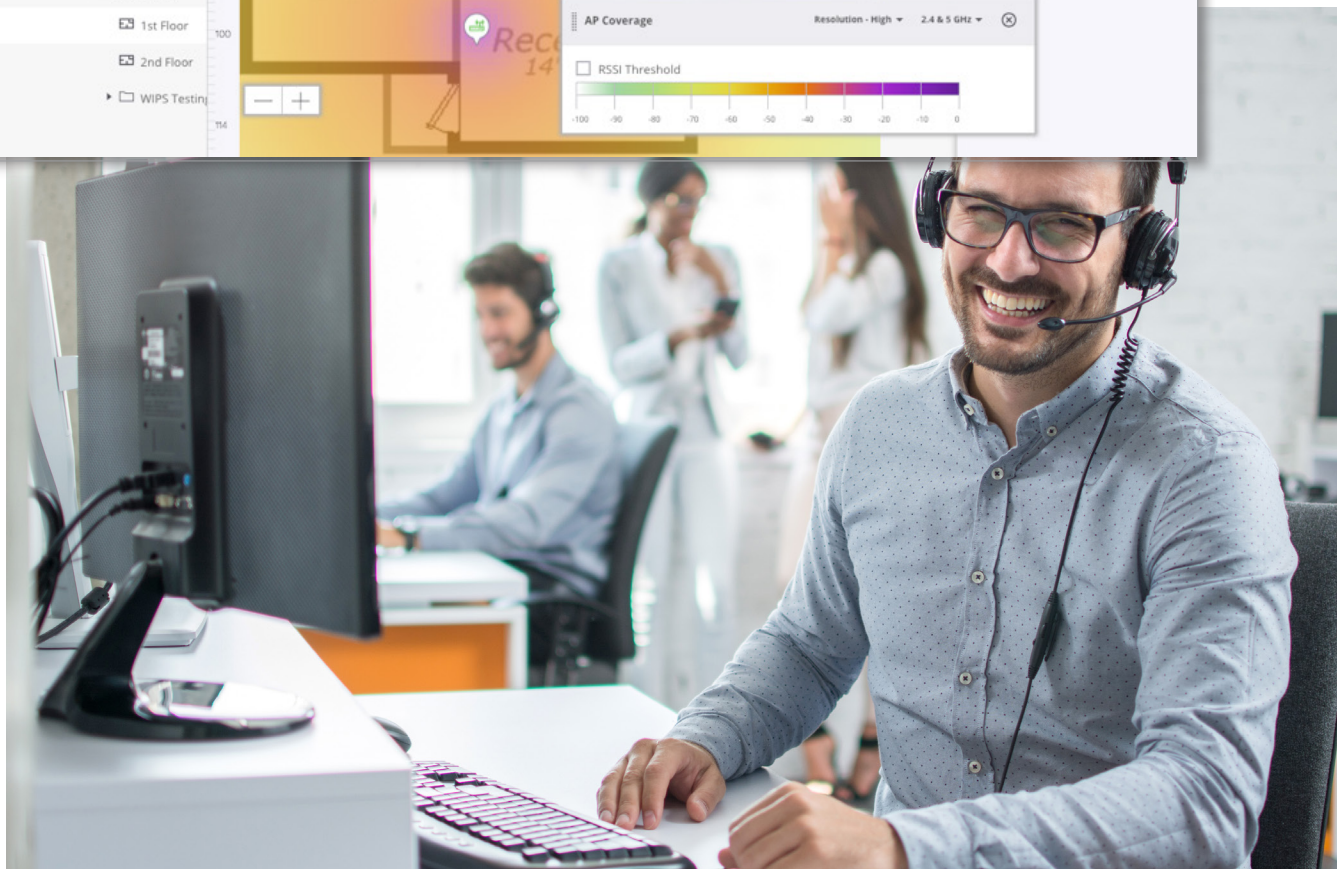
```
SSID    : rahl
BSSID   : 00:90:7F:F6:A4:80
AP NAME : Home AP420 4
Chan    : 40
Time    : 2018.09.24 19:04:20 (America/Los_Angeles)
Tdiff(msec)     Timestamp           Event
        0       2018.09.24 19:04:20     Disassociation received from client because sending STA is leaving (or has left) BSS
        6       2018.09.24 19:04:20     Node Left
SSID    : rahl
BSSID   : 00:90:7F:51:89:00
AP NAME : Home AP125 1
Chan    : 149
Time    : 2018.09.24 19:04:28 (America/Los_Angeles)
Tdiff(msec)     Timestamp           Event
        0       2018.09.24 19:04:28     AP received authentication request from client at [-62]db
        0       2018.09.24 19:04:28     Client successfully authenticated
        0       2018.09.24 19:04:28     AP received (re)association request from client
        0       2018.09.24 19:04:28     Signals a new WPA or WPA2 exchange
        6       2018.09.24 19:04:28     Setting PMK from PSK as this is a WPA or WPA2 PSK authentication
        6       2018.09.24 19:04:28     Client successfully (re)associated
        6       2018.09.24 19:04:28     First phase of WPA/WPA2 4-Way Handshake Completed
       12       2018.09.24 19:04:28     Second phase of WPA/WPA2 4-Way Handshake Completed
       12       2018.09.24 19:04:28     Third phase of WPA/WPA2 4-Way Handshake Completed
       12       2018.09.24 19:04:28     Node Authorized
       34       2018.09.24 19:04:28     Fourth phase of WPA/WPA2 4-Way Handshake Completed
      272       2018.09.24 19:04:28     Client sent DHCP REQUEST
      272       2018.09.24 19:04:28     DHCP ACK sent to Client from [10.5.1.253]
      272       2018.09.24 19:04:28     Client has received IP [10.5.1.177]
      389       2018.09.24 19:04:28     Client has received IP [fe80::18bf:c5cc:2345:106]
```

Save time and expense using remote monitoring

Floor Plans and RF Heatmaps

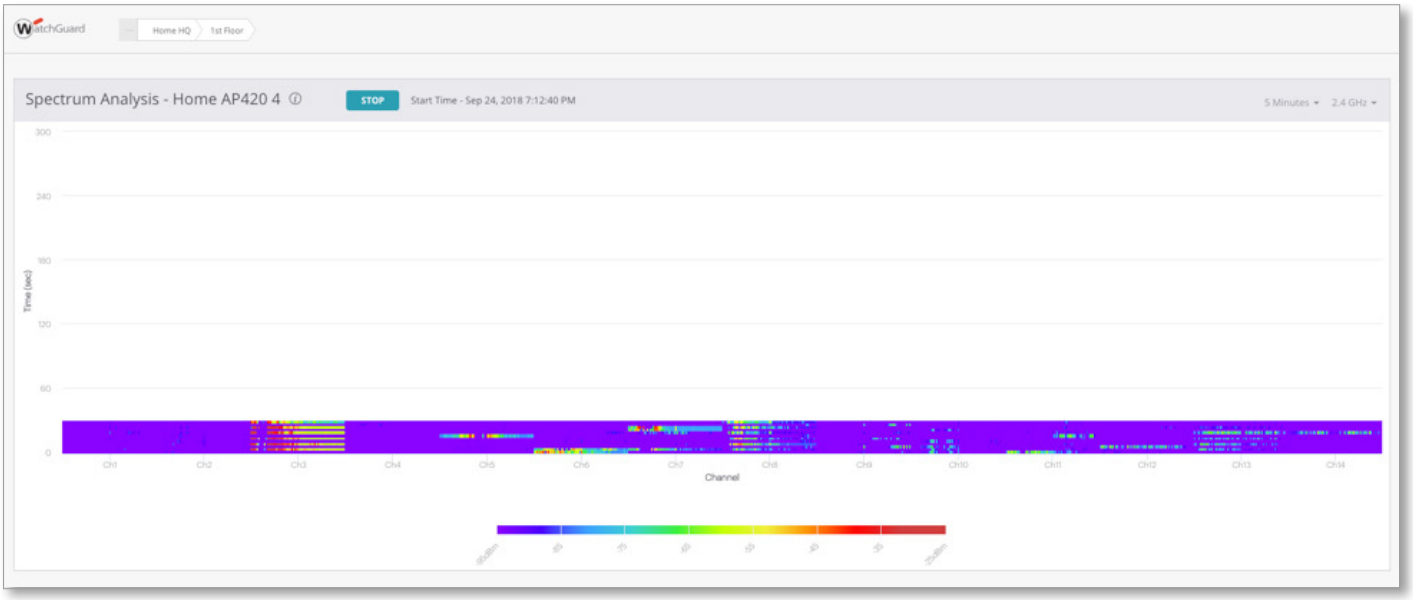
Standard image files of floor plans are easily imported for each location. Once added, a right-click on the AP provides all management and troubleshooting functions for each AP. Heatmaps show AP Coverage, Link Speed, and Channel Coverage. Each map can be viewed for 2.4 GHz or 5 GHz, or 2.4 & 5 GHz bands combined.





Remote Spectrum Analysis

The 3rd radio on select access point models (AP325 and AP420) dedicated for scanning provides unparalleled visibility in both 2.4 GHz and 5 GHz and enables automatic RF optimizations such as band steering, smart steering, auto channel selection or auto transmit power control, delivering best performance. This can all be done remotely without ever having to deploy technical resources onsite.



Learn more: www.watchguard.com/wifi

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by nearly 10,000 security resellers and service providers to protect more than 80,000 customers. WatchGuard'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. The company 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.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com