

Discover - Für zufriedene Benutzer und eine produktive IT



„Warum funktioniert das WLAN nicht?“

Diese Frage kommt nicht nur Ihnen allzu bekannt vor. Wann immer Benutzer ein Problem feststellen, gehen sie in der Regel davon aus, dass dieses auf das WLAN zurückzuführen ist. Da ihre Notebooks und Smartphones über WLAN verbunden sind, glauben sie ganz einfach, dass dieses auch das Problem sein muss. In vielen Fällen ist die Ursache die LAN-Verbindung oder die Anwendung. Bei den meisten WLAN-Lösungen können IT-Administratoren nicht lokalisieren, wo genau das Problem im Netzwerk besteht, und können es deshalb auch nicht so schnell beheben. Administratoren benötigen daher einen besseren Überblick.

DISCOVER umfangreiches Management!

Wi-Fi Cloud von WatchGuard enthält nun auch die Discover-App. Discover bietet die umfassendste Auswahl an Funktionen für **WLAN-Transparenz, Fehlerbehebung** und **Netzwerkzustand**, die je auf dem Markt verfügbar gewesen ist. Nach der Konfiguration der WLAN-Einstellungen unter **Manage** bietet Ihnen Discover nützliche Funktionen für folgende Aufgaben:

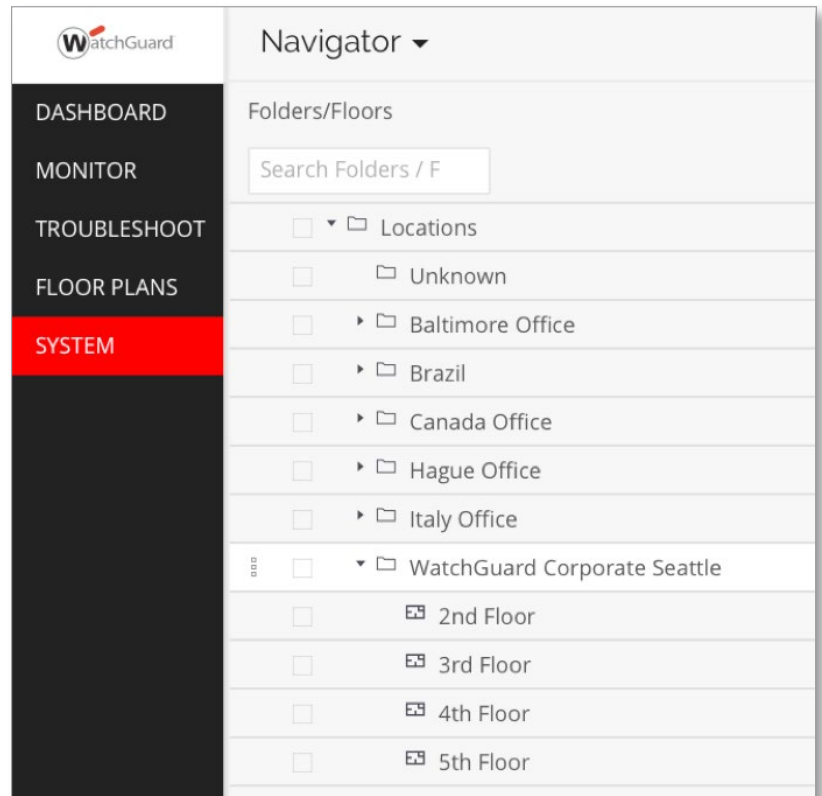
- Anzeige eines Live-Snapshots zur **Client Journey** für all Ihre Standorte
- Detailanalyse von Ereignissen, um klare Antworten auf die Frage zu erhalten, **warum das WLAN nicht funktioniert**
- Anzeigen von **Baselines** für Leistungsdaten und mehr
- Empfang von **Warnmeldungen**, wenn Netzwerkanomalien Baseline-Schwellenwerte übersteigen
- Durchführen von **Client-Konnektivitätstests** mithilfe von WatchGuard-Access Points mit einem dritten Funksystem
- Remote-Behebung von Problemen mit Live-**Spektrumsanalysen** und Live-**Client-Debugging**

Standortbasierte Informationen

Unter Verwendung der hierarchiebasierten Verwaltungsfunktion von WatchGuard Wi-Fi Cloud bewertet Discover Metriken auf der ausgewählten Ebene und zeigt diese an, sodass Sie über Ansichten der gesamten Organisation, des gesamten Standorts oder einer bestimmten Lokation verfügen.

Das Discover-Dashboard befasst sich mit jedem Problemtyp:

- **Konnektivität**
- **Leistung**
- **Anwendungen**



Benutzerverbindungen

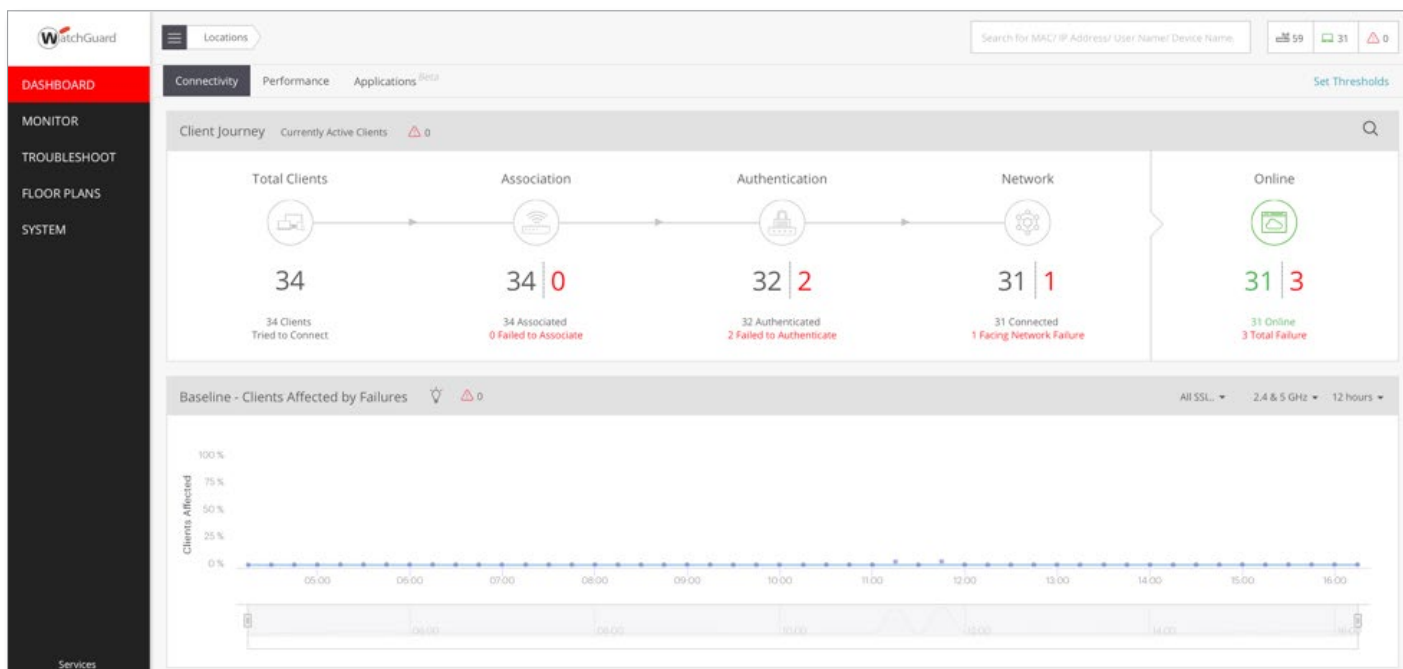
Im Konnektivitäts-Dashboard werden Probleme zusammengefasst und hervorgehoben, die sich negativ auf die WLAN-Benutzererfahrung auswirken können und behoben werden müssen. Außerdem erstellt es eine Baseline der wichtigsten Metriken für jedes Netzwerk und hebt Anomalien hervor, die deutlich von der Baseline abweichen. Tiefgreifende Einblicke erhalten Sie, indem Sie ganz einfach mit dem Mauszeiger über bestimmte WLAN-Clients, Zugriffspunkte, Anwendungen oder Diagramme fahren oder auf diese klicken, um weitere Informationen anzuzeigen.

WatchGuard Access-Points sorgen für eine intelligente Überwachung von Clients, während diese eine Verbindung zum WLAN-Netzwerk herstellen. Wenn ein Problem auftritt, wird es vom Access-Point erkannt, der dann automatisch die Pakete des Clients erfasst, eine Ursachenanalyse durchführt und diese zusammen mit den erfassten Paketen an die WatchGuard Wi-Fi Cloud weiterleitet. Client-Verbindungsbewertungen (Ursachenanalysen und erfasste Pakete) stehen innerhalb von Sekunden nach einem fehlgeschlagenen Verbindungsversuch über die Cloud zur Verfügung und werden verlaufs basiert für den Fall gespeichert, dass eine Überprüfung notwendig ist.

Client-Journey-Standort und einzelner Client

Die **Client Journey** ist die Hauptansicht des Discover-Dashboards und bietet einen Echtzeit-Überblick über die Client-Verbindungsprobleme des Netzwerks. Sie ist in Phasen unterteilt, die jeder Client bei der Herstellung einer Verbindung zum WLAN durchläuft: Zuordnung, Authentifizierung und Netzwerk (DHCP und DNS).

Jedes Verbindungssegment zeigt die Anzahl der Clients an, deren Verbindung erfolgreich war oder fehlgeschlagen ist. Wenn Sie mit dem Mauszeiger über die Anzahl (rot) der fehlgeschlagenen Versuche in dieser Phase fahren, werden diese nach Ursache zusammengefasst. Durch Klicken auf die Anzahl erhalten Sie weitere Informationen zu den Clients. Klicken Sie auf einen der Clients, werden die Verbindungsprotokolle angezeigt. Das Paketprotokoll des Ereignisses lässt sich automatisch unter „Packets“ öffnen, sodass Sie eine grafische Analyse durchführen oder eine lokale Kopie herunterladen können, um eine Analyse in einem Paketanalyse-Tool wie Wireshark durchzuführen. All dies erfolgt innerhalb von Sekunden nach dem Auftreten des Verbindungsproblems. Der Abschnitt „Client Journey“ verfügt über eine eigene Suchfunktion, mit der Sie schnell die Verbindungsinformationen eines bestimmten Benutzers suchen und anzeigen können. Suchen Sie anhand von MAC-Adresse, IP-Adresse, Benutzername oder Gerätenamen, um die Details der letzten Verbindung anzuzeigen. Klicken Sie, um die Verbindungsprotokolle des letzten Monats anzuzeigen.

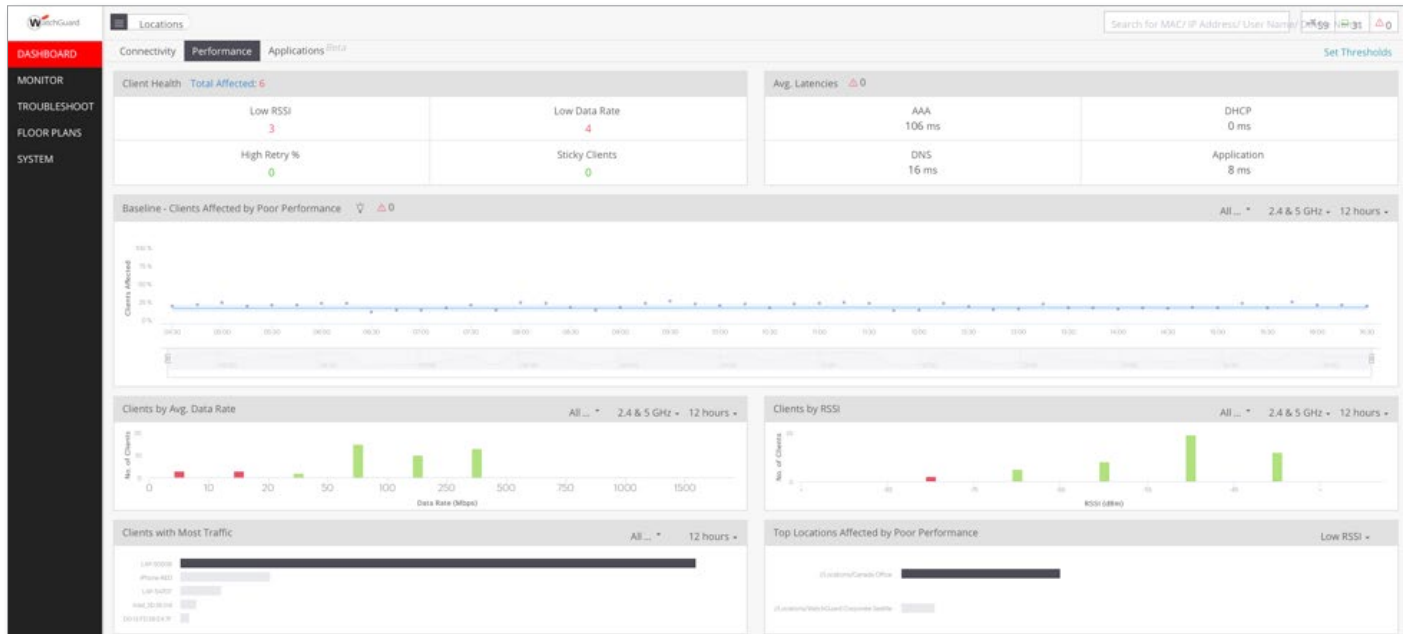


Die Client Journey ist die Hauptansicht des Discover-Dashboards

Leistung

Die Benutzererfahrung und die Anwendungsleistung hängen in großem Maß vom Netzwerkstatus des Clients ab. Die Discover-Anwendung bietet direkte Einblicke und meldet sowohl Probleme, die im Zusammenhang mit dem WLAN stehen, als auch andere, die zu einer schlechten Anwendungsleistung und Benutzererfahrung führen können.

Bietet direkten Blick auf den Netzwerkstatus und meldet Probleme inner- und außerhalb des WLAN



Baselines und Anomalien

Herkömmliche Netzwerküberwachungssysteme nutzen Schwellenwerte, um die wichtigsten Zustands- und Leistungsmetriken zu bewerten. Diese Schwellenwerte werden manuell festgelegt und müssen angepasst werden, da jedes Netzwerk unterschiedliche Merkmale aufweist. Netzwerkmanager deaktivieren schwellenwertbasierte Warnmeldungen in der Regel, da sie zu einer großen Anzahl von falschen Negativ- und falschen Positivergebnissen führen.

Wi-Fi Cloud Discover verfolgt einen anderen Ansatz. Die Lösung überwacht ca. 300 Variablen und bestimmt den Normalzustand für eine Umgebung, legt Baselines für das Verhalten fest und hebt Anomalien vor, damit Sie sich auf die wichtigen Dinge konzentrieren können. Baselines werden für wichtige WLAN-Faktoren wie Client-Konnektivität, schlechte Leistung, Datenraten, Latenz und Anwendungen bereitgestellt.

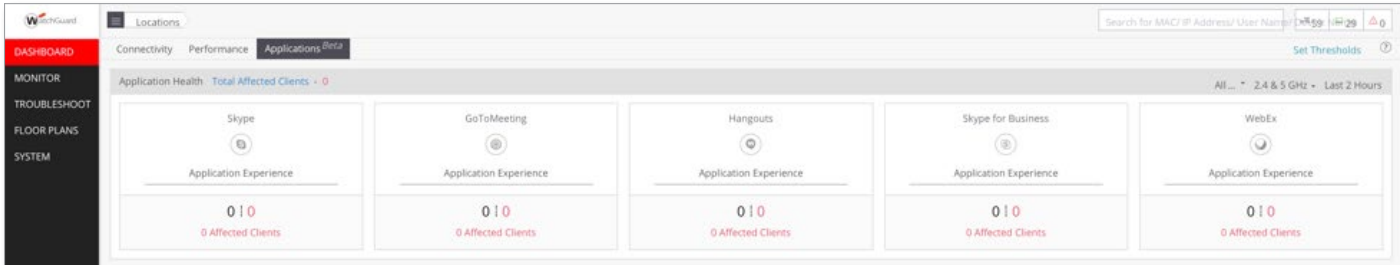
Sie sind dynamisch und werden angepasst, sobald sich die Netzwerkmerkmale ändern. Jede Baseline-Grafik besteht aus drei Komponenten, anhand derer Sie normales und abweichendes Verhalten einfach erkennen können:

- Baseline (dunkelblaue Linie) – gewichteter Durchschnitt, der normales Verhalten zeigt
- Abweichungsbereich (blauer Bereich) – normaler Bereich
- Anomalien (rote Punkte) – Ereignisse, die deutlich von der Baseline abweichen



Anwendungslatenz

Die durchgängige Anwendungsleistung hängt sowohl von den WLAN- als auch von den kabelgebundenen Netzwerken ab, über die Pakete weitergeleitet werden. Benutzer geben häufig dem WLAN die Schuld für Leistungsprobleme, obwohl genauso gut ein Problem mit der kabelgebundenen Seite des Netzwerks bestehen könnte. Mithilfe von Deep Packet Inspection (DPI) analysiert WatchGuard alle TCP-Verbindungen für das Netzwerk und unterteilt sie in kabelgebundene und kabellose Komponenten. Die Grafik zur Anwendungslatenz-Baseline zeigt die kabelgebundenen und kabellosen Komponenten im Hinblick auf TCP-Latenz. Durch den Vergleich dieser Baselines können Sie den Fokus bei der Fehlerbehebung auf den kabelgebundenen oder den kabellosen Teil des Netzwerks eingrenzen.



Fehlerbehebung

Ursprünglich ist die WLAN-Fehlerbehebung ein aufwändiger Prozess, bei dem Mitarbeiter häufig am Ort des Geschehens Testausrüstung einrichten, das Problem reproduzieren und relevante Informationen erfassen müssen. Auch wenn alles wie geplant verläuft, handelt es sich um einen langwierigen, zeitaufwändigen Vorgang.

Die Discover-App vereinfacht die Fehlerbehebung durch die Automatisierung der Erkennung und Ursachenanalyse von Fehlern und Anomalien. Sie kann auch dann helfen, wenn das Problem nicht mit dem WLAN zusammenhängt. Wenn tiefgreifende Analysen erforderlich sind, erfasst Discover automatisch die Pakete von Verbindungsproblemen und stellt diese auf der Registerkarte „Troubleshoot“ (Paketprotokoll) oder zum Download bereit. Zwei der WLAN-Fehlerbehebungsfunktionen von Discover sind die automatische Paketerfassung und die Nutzung des dritten Funksystems eines Zugriffspunkts als Client eines benachbarten Zugriffspunkts.

Access Points Table:

Status	Name	Update	MAC Address	IP Address	Build	Device Template	Up/Down Since	Capability	Location
🟢	Home AP322	🟢	00:90:7F:F1:18:3F	10.5.1.110	8.6.0-634	Home	↑ Sep 21	802.11n/ac, AP	*Home HQ/1st Floor
🟢	Home AP420	🟢	00:90:7F:F4:02:CF	10.5.1.115	8.6.0-634	Home	↑ Sep 21	802.11n/ac, AP	*Home HQ/1st Floor
🟢	Home AP420.4	🟢	00:90:7F:F6:A4:AF	10.5.1.114	8.6.0-634	Home	↑ Sep 21	802.11n/ac, AP	*Home HQ/1st Floor
🟢	Home AP125.1	🟢	00:90:7F:51:89:0F	10.5.1.111	8.6.0-634	WIPS Testing	↑ Sep 21	802.11n/ac, AP	*Home HQ/WIPS Te...
🟢	Home AP120.1	🟢	00:90:7F:38:F8:3F	10.5.1.147	8.3.0-648	Home	↓ Sep 24, 2017	802.11n/ac, AP	*Home HQ/1st Floor
🟢	Home AP320.4	🟢	00:90:7F:ER-AC:3F	10.5.1.114	8.0.552	Retail Demo 1	↓ Dec 17, 2016	802.11n/ac, AP	*Alex's Wi-Fi Retail B...
🟢	Home AP320.1	🟢	00:90:7F:ER-14:7F	10.5.1.117	8.0.543	Retail Demo 1	↓ Sep 5, 2016	802.11n/ac, AP	*Alex's Wi-Fi Retail B...

Packet Trace Table:

Filename	File Size	MAC Address	Capturing Device Mac Address	Device	Start Time	Stop Time
asdf_wireless_1537840433.pcap...	24 Bytes	00:90:7F:F6:A4:AF	00:90:7F:F6:A4:AF	Access Point	6:53 PM	--
wired_1537840433.pcap	24 Bytes	00:90:7F:F6:A4:AF	00:90:7F:F6:A4:AF	Access Point	6:53 PM	--

Capture Packet Trace Settings:

- Timeout: 5 minutes [1 - 720]
- Streaming Option: Upload to server
- Filename Prefix: Troubleshooting
- Wireless Settings
 - Traffic Selection
 - Packet Types
 - Protocol and Channel Selection
- Wired Settings
 - Interface: eth0
 - VLAN ID: 0
 - ICMP UDP DHCP
 - MDNS LLNMR DNS
 - RADIUS ARP TCP

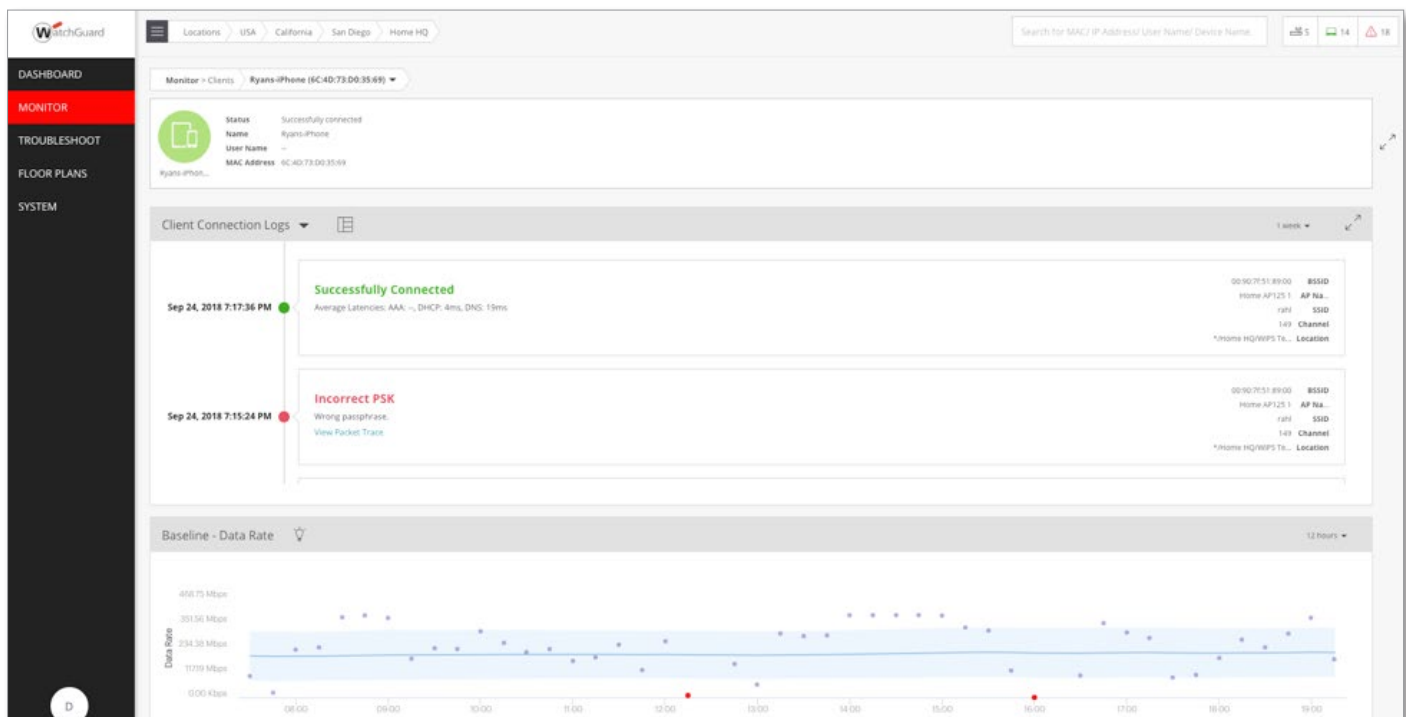
Benutzerverbindungen

Der erste Schritt bei der Behebung eines von einem Benutzer gemeldeten WLAN-Problems ist die Lokalisierung der Benutzerinformationen. Discover minimiert den Aufwand für die Suche nach einem problembehafteten Client durch die Bereitstellung von globalen, dynamischen Suchfunktionen für Clients im Netzwerk. Die Hauptsuchleiste befindet sich oben im Dashboard und ermöglicht eine dynamische Suche nach Clients basierend auf der MAC- oder IP-Adresse oder nach Benutzer- (802.1x) oder Gerätenamen. Die Suche wird durch jedes eingegebene Zeichen weiter verfeinert.

Status	Name	MAC Address	Channel	IP Address	OS	Associated Access Poi...	Associated SSID	RSSI (dB...	Uplink Data	Downlink Da...	Sticky	Avg. data rate	Location
✓	amazon-lac3bd414	F0:27:2D:E4:E0:4A	48	10.5.1.175	Android	Home AP420	rahl		8 MB	376.6 MB	No	139.68 Mb...	*/Home HQ/1st Floor
✓	MamaLiamiPhone	D0:C5:F3:78:78:05	157	10.5.1.119	Apple iOS v9.0+	Home AP322	rahl		3 MB	137.67 MB	No	232.21 Mb...	*/Home HQ/1st Floor
✓	amazon-68743b650	0C:47:C9:89:19:AA	11	10.5.1.176	Android	Home AP420	rahl		9 MB	134.01 MB	No	58.76 Mbps	*/Home HQ/1st Floor
✓	MAC-12345	8C:85:90:63:82:35	40	10.5.1.180	Mac OSX 10.11+	Home AP420 4	rahl		5 MB	12.96 MB	No	321.44 Mb...	*/Home HQ/1st Floor
✓	500-cc4b40787b5	CC:04:84:07:87:85	11	10.5.1.178	--	Home AP420	rahl		4 KB	169 KB	No	63.35 Mbps	*/Home HQ/1st Floor
✓	amazon-bb9ad484c	DC:47:C9:40:88:54	11	10.5.1.161	Android	Home AP420	rahl	-40	53 KB	71 KB	No	63.37 Mbps	*/Home HQ/1st Floor
✓	Kitchen	DC:56:E7:4A:EE:6F	40	10.5.1.143	Apple iOS v9.0+	Home AP420 4	rahl	-60	45 KB	32 KB	No	257.59 Mb...	*/Home HQ/1st Floor
✓	Jacobs-iPhone	DC:2B:61:15:3C:...	1	10.5.1.172	Apple iOS v6-8.4.1	Home AP420 4	rahl	-52	7 KB	10 KB	No	56.99 Mbps	*/Home HQ/1st Floor
✓	Jacob	28:10:7B:1A:3D:...	11	10.5.1.185	--	Home AP420	rahl	-50	27 KB	9 KB	No	84.81 Mbps	*/Home HQ/1st Floor
✓	Lucasaaurus	28:10:7B:1A:3D:...	1	10.5.1.184	--	Home AP420 4	rahl	-58	24 KB	9 KB	No	78.23 Mbps	*/Home HQ/1st Floor
✓	kindle-7987199f4	28:EF:01:CD:38:37	40	--	Android	Home AP420 4	rahl	--	0 Bytes	0 Bytes	No	--	*/Home HQ/1st Floor
✓	Ryans-MBP	D0:A6:37:EB:E9:55	48	--	Mac OSX 10.11+	Home AP420	rahl	--	0 Bytes	0 Bytes	No	0 Kbps	*/Home HQ/1st Floor
✓	RyansAppleWatch	60:9A:C1:4D:F7:25	11	--	Apple iOS v9.0+	Home AP420	rahl	--	0 Bytes	0 Bytes	No	0 Kbps	*/Home HQ/1st Floor
✓	Ryan-Laptop	00:1B:77:89:22:F6	48	--	Microsoft Windows 7	Home AP420	rahl	--	0 Bytes	0 Bytes	No	0 Kbps	*/San Diego/Home HQ
✓	iPad	70:48:0F:DA:43:5F	48	--	Apple iOS v9.0+	Home AP420	rahl	--	0 Bytes	0 Bytes	No	--	*/Home HQ/1st Floor
✓	Nintendo_BIA31:44	64:85:C6:BA:31:...	40	--	--	Home AP420 4	rahl	--	0 Bytes	0 Bytes	No	0 Kbps	*/Home HQ/1st Floor

Engine für die Ursachenanalyse

Discover sorgt für eine automatische Erkennung und Klassifizierung in Echtzeit, wenn die Verbindungsherstellung bei WLAN-Clients fehlschlägt, und identifiziert die Ursache (das heißt, ob das Problem mit dem WLAN, Netzwerkdienst oder einem Client-Gerät und/oder einer Client-Anwendung zusammenhängt). Gleichzeitig automatisiert die Lösung die Analyse der Ursache für die schlechte Leistung, zum Beispiel schlechter Empfang, hohe Wiederholungsraten oder Sticky Clients.

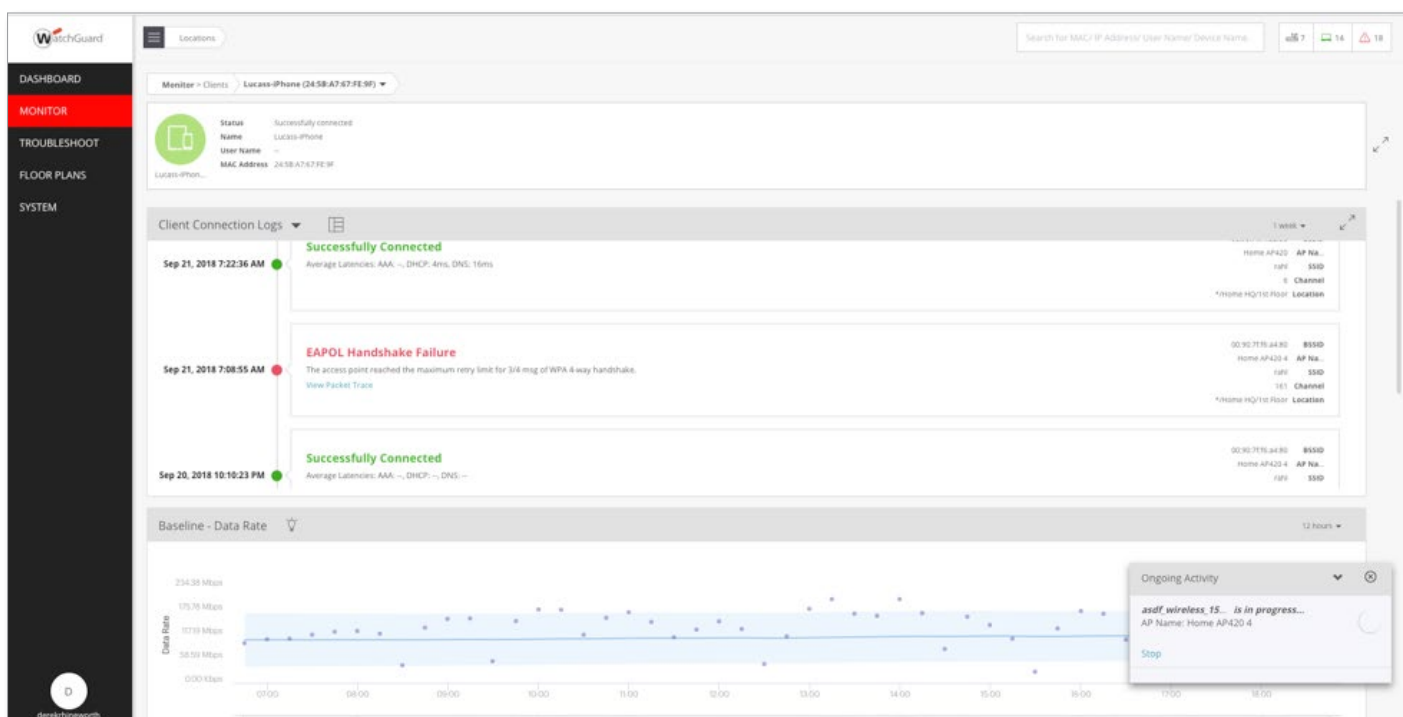


Automatische Paketerfassung

Personen, die Netzwerkfehler beheben, verlassen sich bei der erweiterten Behebung von WLAN-Problemen häufig auf die Erfassung von Paketprotokollen. In den meisten Fällen wird gerade kein Tool für die Paketerfassung ausgeführt, wenn ein Problem auftritt. Daher müssen Administratoren sich mit den Benutzern abstimmen, bei denen das Problem aufgetreten ist, und sie um Hilfe bei der Reproduktion des Problems bitten, damit sie es in einem Paketprotokoll erfassen können. Dafür sind häufig spezielle Tools für die WLAN-Paketerfassung und -analyse sowie WLAN-Experten vor Ort erforderlich.

Discover bietet Ihnen im Bedarfsfall eine intelligenterere und automatisierte Lösung für die Erfassung von Paketprotokollen. Jeder WatchGuard-Zugriffspunkt erfasst Pakete für jeden Client, der eine Verbindung zum Netzwerk herstellt. Wenn ein Problem auftritt, erkennt der Zugriffspunkt das Problem, führt eine Ursachenanalyse durch, speichert die erfassten Pakete und gibt all diese Informationen an die Cloud weiter.

Alle erforderlichen Informationen werden in Echtzeit erfasst, während das Problem auftritt, und innerhalb von Sekunden in der Discover-UI zur Verfügung gestellt. Die Pakete werden im Kontext eines WLAN-Clients erfasst, bei dem ein Problem aufgetreten ist. Somit müssen Mitarbeiter nicht vor Ort sein und das Problem aufwändig reproduzieren. Um das Protokoll zu überprüfen, müssen nur die erfassten Pakete heruntergeladen und in einem der beliebigen Tools zum Anzeigen von Paketen angezeigt werden.



Intelligenterere und automatisierte Lösung für die Erfassung von Paketprotokollen im Bedarfsfall

Client-Emulation und Netzwerk-Profiling

Discover ermöglicht Zugriffspunkten mit drei Funksystemen (AP325 und AP420) die Herstellung einer Verbindung als Client zu einem benachbarten Zugriffspunkt, um die WLAN-Verbindung und -Leistung zu bewerten. Tests können on demand durchgeführt oder geplant und wiederholt werden. Zur On-Demand-Ausführung klicken Sie mit der rechten Maustaste auf den Zugriffspunkt und wählen Sie ein Testprofil, ein Frequenzband und den benachbarten Zugriffspunkt mit drei Funksystemen aus, zu dem eine Verbindung als Client hergestellt werden soll. Bei jedem Lauf werden WLAN-, Netzwerk- und Internetverbindung getestet. Anwendungs-, VoIP- und Durchsatztests können bei Bedarf zur Testvorlage hinzugefügt werden.

Discover ermöglicht Zugriffspunkten mit drei Funksystemen die Herstellung einer Verbindung als Client zu einem benachbarten Zugriffspunkt, um die WLAN-Verbindung und -Leistung zu bewerten.



Client Connectivity Test ▾ Profiles Schedules Results

← Friday Afternoon Test

Security Mode
WPA2

SSID Security Type
 PSK 802.1x

Password

Application Test

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

Client Connectivity Test ▾ Profiles Schedules Results

← TODAY Sep 2018 MONTH WEEK DAY

Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	31 Every Friday 10:1... Ever Friday	1
2	3	4	5	6	7 Every Friday 10:1... Ever Friday	8
9	10	11	12	13	14 Every Friday 10:1... Ever Friday	15
16	17	18	19	20 Every Morning	21 Every Morning Every Friday 10:1... + 1 more	22 Every Morning
23 Every Morning	24 Every Morning	25 Every Morning	26 Every Morning	27 Every Morning	28 Every Morning Every Friday 10:1... + 1 more	29 Every Morning
30 Every Morning	1 Every Morning	2 Every Morning	3 Every Morning	4 Every Morning	5 Every Morning Every Friday 10:1... + 1 more	6 Every Morning

The screenshot displays the WatchGuard Client Connectivity Test interface. On the left is a navigation sidebar with options: DASHBOARD, MONITOR, TROUBLESHOOT (highlighted), FLOOR PLANS, and SYSTEM. The main area shows a breadcrumb trail: Locations > USA > California > San Diego > Home HQ. Below this is a search bar and a 'Client Connectivity Test' dropdown menu. A link says 'Create a profile and Run Client Connectivity Test?'. A table titled '30 Client Connectivity Test Results' shows columns for 'Filename', 'Result Status', and 'AP Name'. The table contains 30 rows with various test names and AP names, and result status indicators (red, green, grey). On the right, a detailed view for 'Home AP322-Home AP420-Sep 24-14:00' is shown. It includes start and stop times, test details, and a list of test categories with their status: Association (green), Authentication (green), DHCP (green), Gateway (green), DNS (green), WAN Latency (green), Application Test (orange), VoIP Test (green), and Throughput Test (green). The VoIP Test section shows a 'Successful' result and a Mean Opinion Score (MOS) of 4.40 / 5, represented by five stars.



Wenn die Zeit drängt, können Sie die Testergebnisse in Echtzeit anzeigen

Warnmeldungen

Mit der Warnmeldfunktion von Discover ist die Erfüllung von Service Level Agreements (SLAs) ein Kinderspiel. Erfüllen Sie SLAs und sorgen Sie dafür dass Ihr WLAN-Netzwerk reibungslos läuft. Sie können bei Bedarf festlegen, dass Warnmeldungen per E-Mail an Ihr PSA-Tool-Ticketing-System, an die Discover-UI und optional an die Syslog-Stream-Ausgabe gesendet werden. Warnmeldungen können so konfiguriert werden, dass die Client-Konnektivität, die Netzwerkdienstleistung, verschiedene Anomalien, die Baseline-Schwellenwerte übersteigen, oder Ihre konfigurierten Client-Konnektivitätstests überwacht werden.

The screenshot shows the 'Configure Alerts' page in the WatchGuard interface. On the left, there is a navigation menu with 'SYSTEM' selected. The main area is divided into three sections: 'Select Location', 'Select Alert Type', and 'Configure Alerts'. Under 'Select Location', a tree view shows various geographical locations like 'Alex's Wi-Fi Retail Bonan', 'Australia', 'Brazil', etc. Under 'Select Alert Type', 'Wi-Fi (3)' is selected, showing sub-categories like 'Connectivity (1)', 'Performance (2)', and 'System'. The 'Configure Alerts' section displays three configured alerts:

- Alert 1:** Number of clients experiencing Any failure exceeds 50. Category: Connection Failure, Type: Any, Location: //Locations.
- Alert 2:** Average DHCP latency for Any SSID and Any frequency band exceeds 500 milliseconds. Category: Performance, Type: DHCP, Location: //Locations.
- Alert 3:** Average Application latency for Any SSID and Any frequency band exceeds 500 milliseconds. Category: Performance, Type: Application, Location: //Locations.

An 'ADD NEW WI-FI ALERT' button is visible in the top right of the alert configuration area.

This screenshot shows the configuration details for a new alert. The 'Alert Type' is 'Performance (2)'. The configuration fields are as follows:

- Alert 1 (DHCP Latency):** Average DHCP latency for Any SSID and Any frequency band exceeds 500 milliseconds [1 - 999].
- Alert 2 (Application Latency):** Average Application latency for Any SSID and Any frequency band exceeds 500 milliseconds [1 - 999].

At the bottom, there are checkboxes for 'Select Alert Notification Type': Email, Display, and Syslog. There is also an 'Activate Alerts' checkbox at the bottom left and 'Cancel' and 'SAVE' buttons at the bottom right.

Client- und Zugriffspunkt-Ereignisprotokollierung

Discover bietet mehrere Möglichkeiten, um den Zustand eines Clients oder Access Points anzuzeigen. Sie können den vollständigen Verlauf eines Access Points oder Clients anzeigen sowie Ereignisse, die während der Verbindungsherstellung auftreten: Änderung von Kanälen, Anpassung der Übertragungsleistung, Initiierung von Roaming und vieles mehr. Diese wichtigen Informationen füllen die Lücken, sodass Sie wissen, was sich geändert hat.

Client-Ereignisprotokoll

Client Event Logs - Client MAC Address: 24:5B:A7:67:FE:9F

1 week

Successfully Connected
Average Latencies: AAA- -, DHCP: -, DNS: 19ms

Sep 23, 2018 3:47:58 PM

Network
The client successfully received a response for its DNS query.

Sep 23, 2018 3:47:23 PM

Network
The client started using IP 10.5.1.173.

Sep 23, 2018 3:47:23 PM

Network
Client has received IP address 10.5.1.173.

Sep 23, 2018 3:47:23 PM

Association
Client successfully (re)associated.

Sep 23, 2018 3:47:23 PM

Client Steering
The access point skipped band steering because the client was roaming. Client RSSI: -58 dBm. Number of associated clients on 2.4 GHz radio: 4. Number of associated clients on 5 GHz radio: 3.

00:90:7f:8e:a4:90 BSSID
Home AP420-4 AP Na...
rahl SSID
1 Channel
*Home HQ/1st Floor Location

Access Point-Ereignisprotokoll


WatchGuard Home HQ 1st Floor

82 Access Point Event Logs Home AP420 1 week

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

Technische Ressourcen müssen Probleme mit Clients nicht mehr vor Ort beheben, da Sie detaillierte WLAN-Debugging-Frames mit Clients ganz einfach remote überwachen können. Auf diese Weise sparen Sie nicht nur Zeit, sondern auch Kosten. Zur Erfassung von Debug-Protokollen in Echtzeit müssen Sie einfach nur mit der rechten Maustaste auf einen Client klicken – und das, während er live im Netzwerk ist.

 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

```

1  SSID      : rahl
2  BSSID    : 00:90:7F:F6:A4:80
3  AP NAME  : Home AP420 4
4  Chan     : 40
5  Time    : 2018.09.24 19:04:20 (America/Los_Angeles)
6  Tdiff(msec)  Timestamp      Event
7  |         | 2018.09.24 19:04:20  Disassociation received from client because sending STA is leaving (or has left) BSS
8  |         | 2018.09.24 19:04:20  Node Left
9  SSID      : rahl
10 BSSID    : 00:90:7F:51:89:00
11 AP NAME  : Home AP125 1
12 Chan     : 149
13 Time    : 2018.09.24 19:04:28 (America/Los_Angeles)
14 Tdiff(msec)  Timestamp      Event
15 |         | 2018.09.24 19:04:28  AP received authentication request from client at [-62]db
16 |         | 2018.09.24 19:04:28  Client successfully authenticated
17 |         | 2018.09.24 19:04:28  AP received (re)association request from client
18 |         | 2018.09.24 19:04:28  Signals a new WPA or WPA2 exchange
19 |         | 2018.09.24 19:04:28  Setting PMK from PSK as this is a WPA or WPA2 PSK authentication
20 |         | 2018.09.24 19:04:28  Client successfully (re)associated
21 |         | 2018.09.24 19:04:28  First phase of WPA/WPA2 4-Way Handshake Completed
22 |         | 2018.09.24 19:04:28  Second phase of WPA/WPA2 4-Way Handshake Completed
23 |         | 2018.09.24 19:04:28  Third phase of WPA/WPA2 4-Way Handshake Completed
24 |         | 2018.09.24 19:04:28  Node Authorized
25 |         | 2018.09.24 19:04:28  Fourth phase of WPA/WPA2 4-Way Handshake Completed
26 |         | 2018.09.24 19:04:28  Client sent DHCP REQUEST
27 |         | 2018.09.24 19:04:28  DHCP ACK sent to Client from [10.5.1.253]
28 |         | 2018.09.24 19:04:28  Client has received IP [10.5.1.177]
29 |         | 2018.09.24 19:04:28  Client has received IP [fe80::18bf:c5cc:2345:106]
30

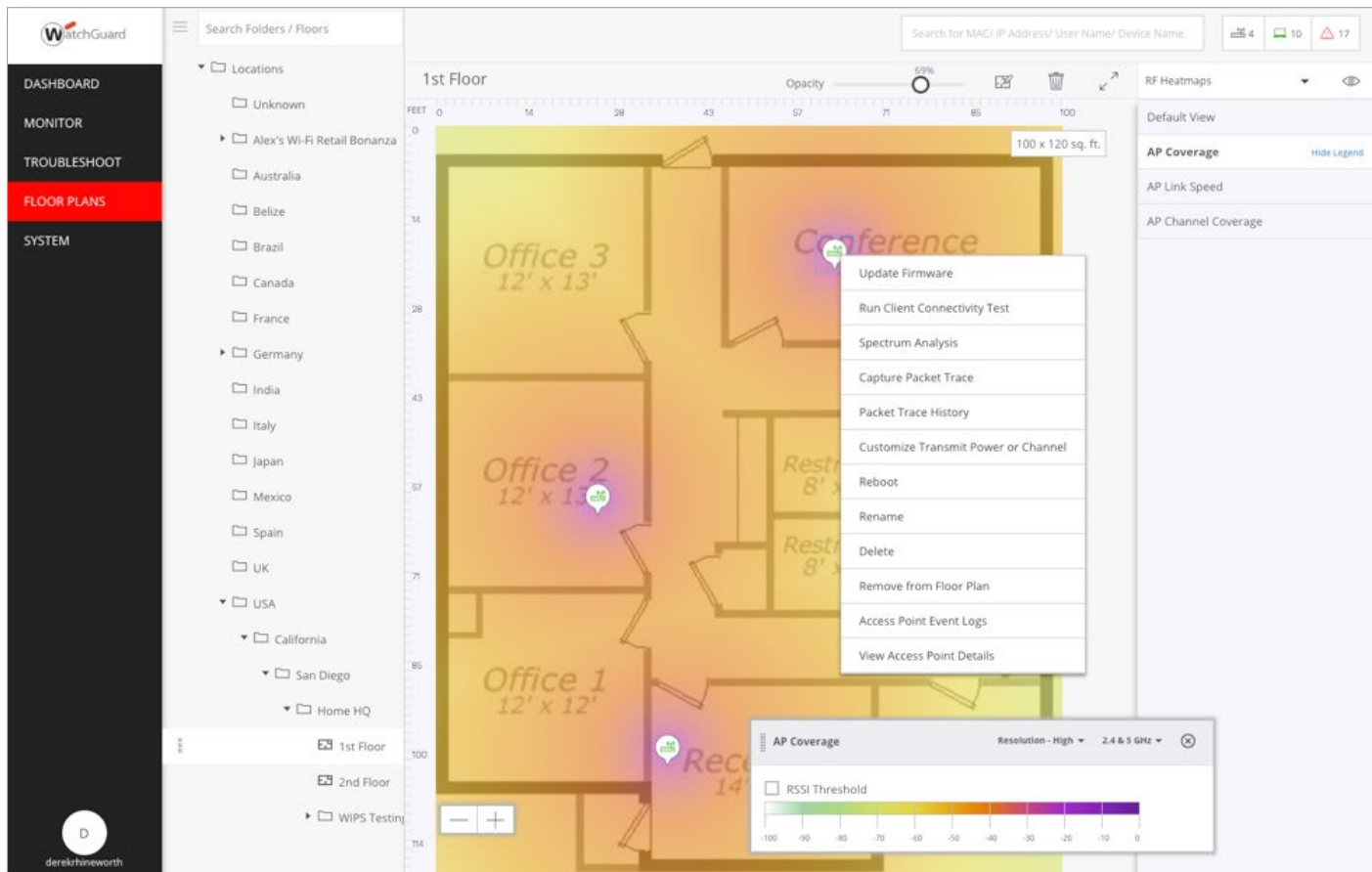
```



Zeit und Kosten durch Remote-Überwachung sparen

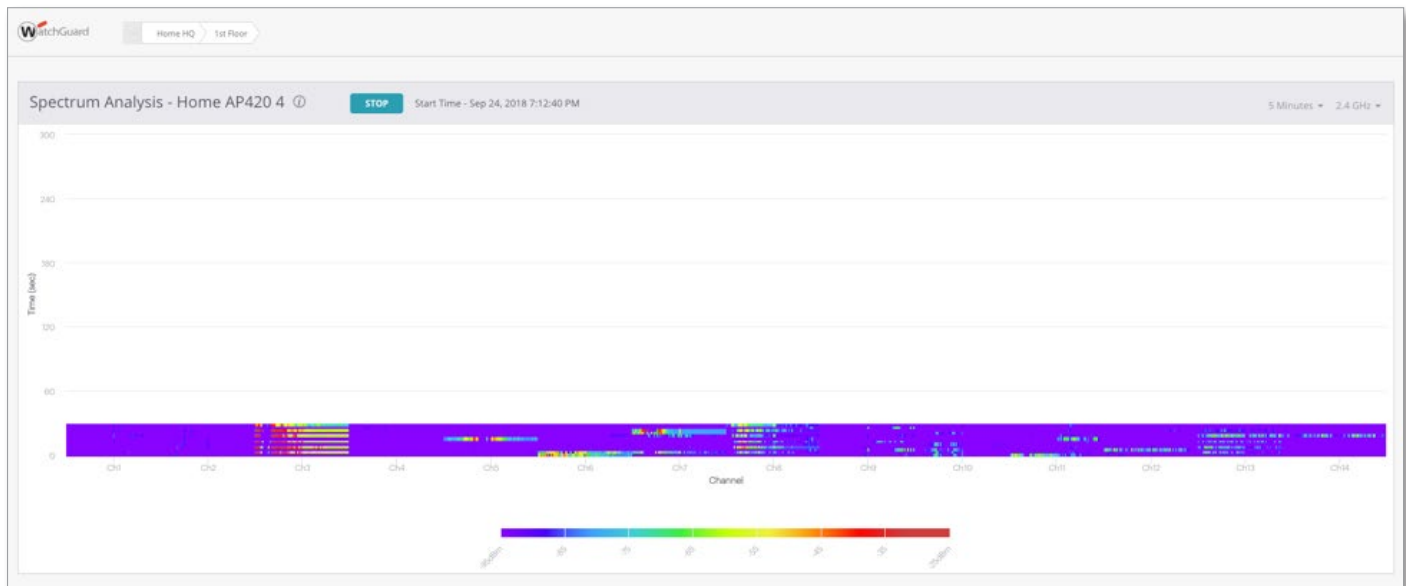
Etagengrundrisse und Funk-Heatmaps

Sie können standardmäßige Bilddateien für Etagengrundrisse ganz einfach für jeden Standort importieren. Nach dem Hinzufügen können Sie per rechtem Mausklick auf alle Verwaltungs- und Fehlerbehebungsfunktionen für jeden Zugriffspunkt zugreifen. Heatmaps zeigen die Access Point-Abdeckung, die Verbindungsgeschwindigkeit und die Kanalabdeckung. Jede Heatmap kann für 2,4-GHz- oder 5-GHz- oder für 2,4- und 5-GHz-Bänder zusammen angezeigt werden.



Remote-Spektrumsanalyse

Das dritte Funkmodul überwacht ausgewählten Access Point-Modellen (AP325 und AP420) dediziert die Umgebung und ermöglicht eine Visualisierung der 2,4-GHz- und 5-GHz-Frequenzbänder und automatische Funk-Optimierung, wie beispielsweise Band Steering, intelligentes Steering, automatische Kanalauswahl oder Automatic Transmit Power Control, für optimale Leistung. All dies kann remote erfolgen, ohne dass technische Ressourcen vor Ort sein müssen.



Weitere Informationen finden Sie unter: www.watchguard.com/wifi

Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Netzwerksicherheit, sicheres WLAN, Multifaktor-Authentifizierung und Network Intelligence. Beinahe 10.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Dienste des Unternehmens, um mehr als 80.000 Kunden zu schützen. Die Philosophie von WatchGuard ist es, Sicherheit auf Enterprise-Niveau für Unternehmen jeder Größenordnung und Art zu realisieren. Das macht WatchGuard insbesondere für kleine und mittlere sowie dezentral aufgestellte Unternehmen zum idealen Anbieter. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter WatchGuard.de.

Wenn Sie mehr über WatchGuard, unsere Werbeaktionen und Updates erfahren möchten, folgen Sie uns auf Twitter @WatchGuard, auf Facebook oder auf unserer Seite auf LinkedIn. Lesen Sie auch unseren InfoSec-Blog Secplicity. Darin wird einfach und nachvollziehbar beschrieben, wie Sie den neuesten Bedrohungen am besten begegnen. Hier geht's zum Blog: www.secplicity.org.

