
Best-Practices
Sichere Wi-Fi Netze einrichten mit Discover

WatchGuard Wi-Fi Cloud

- Skalierbares Cloud management
- Patentierte WIPS Funtkionalität
- Intelligent Network Visibility und Troubleshooting
- Interaktion mit Gästen (Hotspot)
- Location-based analytics
- Reporting und Visibility

Wi-Fi Subscriptions

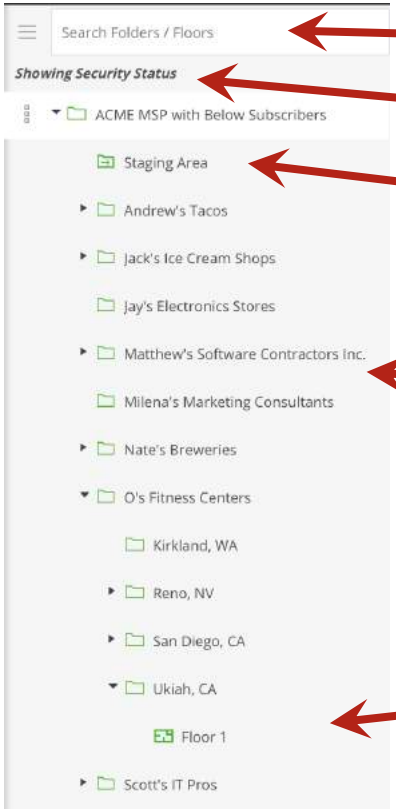
WatchGuard Wi-Fi Solution	Total Wi-Fi	Secure Wi-Fi	Basic Wi-Fi
Management Platform	Wi-Fi Cloud	Wi-Fi Cloud	Firebox Appliance*
Scalability Number of managed access points.	Unlimited	Unlimited	Limited**
Configuration and Management SSID configuration with VLAN support, band steering, smart steering, fast roaming, user bandwidth control, Wi-Fi traffic dashboard.	✓	✓	✓
Additional Wi-Fi Cloud-based Management Radio Resource Management, Hotspot 2.0, enhanced client roaming, nested folders for configuration before deployment, integration with 3rd party WLAN controllers.	✓	✓	
Intelligent Network Visibility and Troubleshooting Pinpoint meaningful network problems and application issues by seeing when an anomaly occurs above baseline thresholds and remotely troubleshoot.	✓	✓	
Verified Comprehensive Security A patented WIPS technology defends your business from the six known Wi-Fi threat categories, enabling a Trusted Wireless Environment.	✓	✓	
GO Mobile Web App Quickly and easily set-up your WLAN network from any mobile device.	✓	✓	
Guest Engagement Tools Splash pages, social media integrations, surveys, coupons, videos, and so much more.	✓		
Location-based Analytics Leverage metrics like footfall, dwell time, and conversion to drive business decisions and create customizable reports.	✓		
Support Hardware warranty with advance hardware replacement, customer support, and software updates	Standard	Standard	Standard

***20 access points recommended for each Firebox model. 4 access points are recommended for the T-15 Firebox model.*
**Requires Firebox with active support contract.*

Konfiguration mit Discover

WatchGuard Training

Navigator — Location Hierarchy



Search the Locations tree

Turn on/off security status

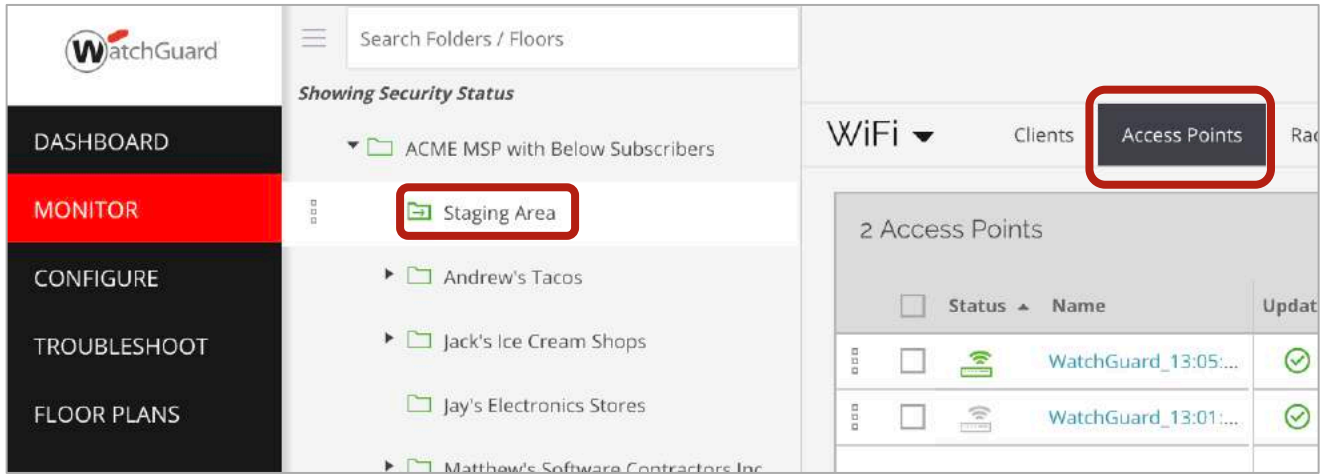
Default folder for all newly activated APs

Use folders to group objects by location, configuration, setup, or other attributes

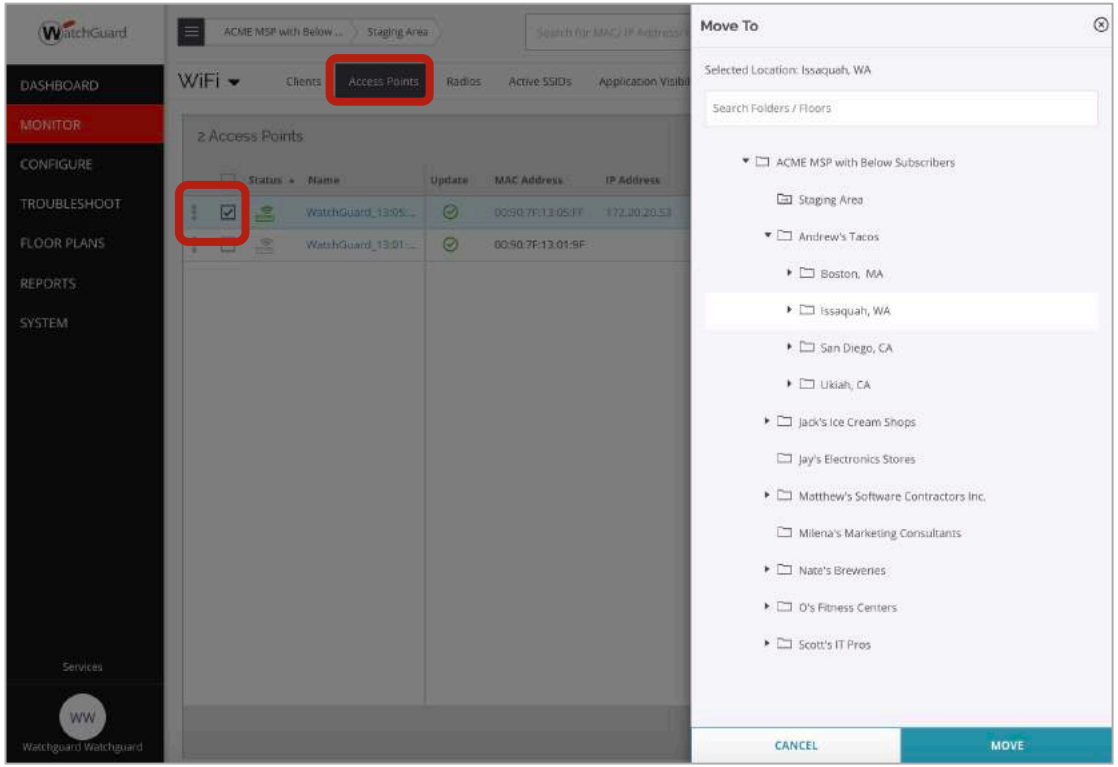
Nodes are at the lowest level in the tree and represent floors

Neue Accesspoints hinzufügen

- Nach Aktivierung eines neuen Accesspoints wird dieser in **Staging Area** dargestellt.
- Der Status kann unter **Monitor > Wi-Fi > Access Points** in der **Staging Area** angezeigt werden



Verschieben von Accesspoints

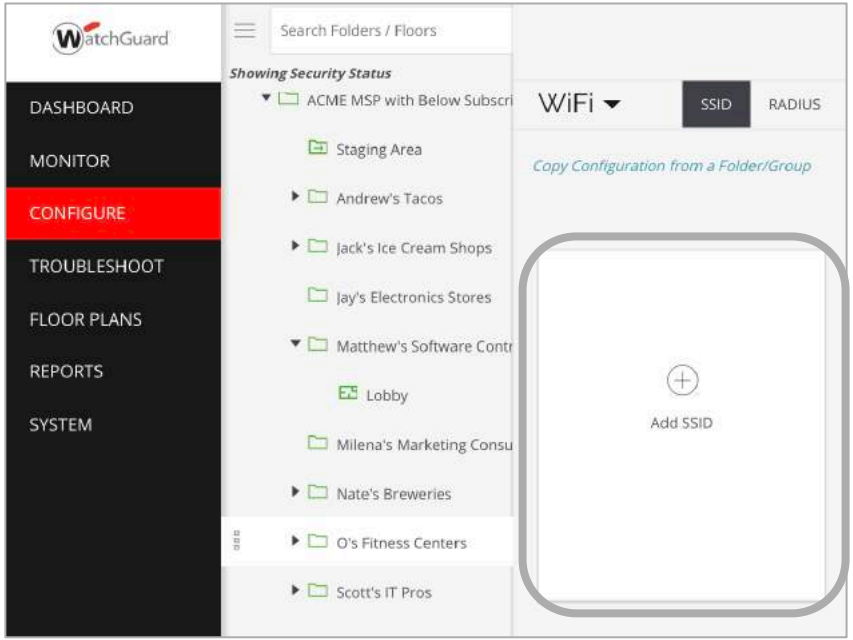


Erzeugen von SSIDs in Discover

WatchGuard Training

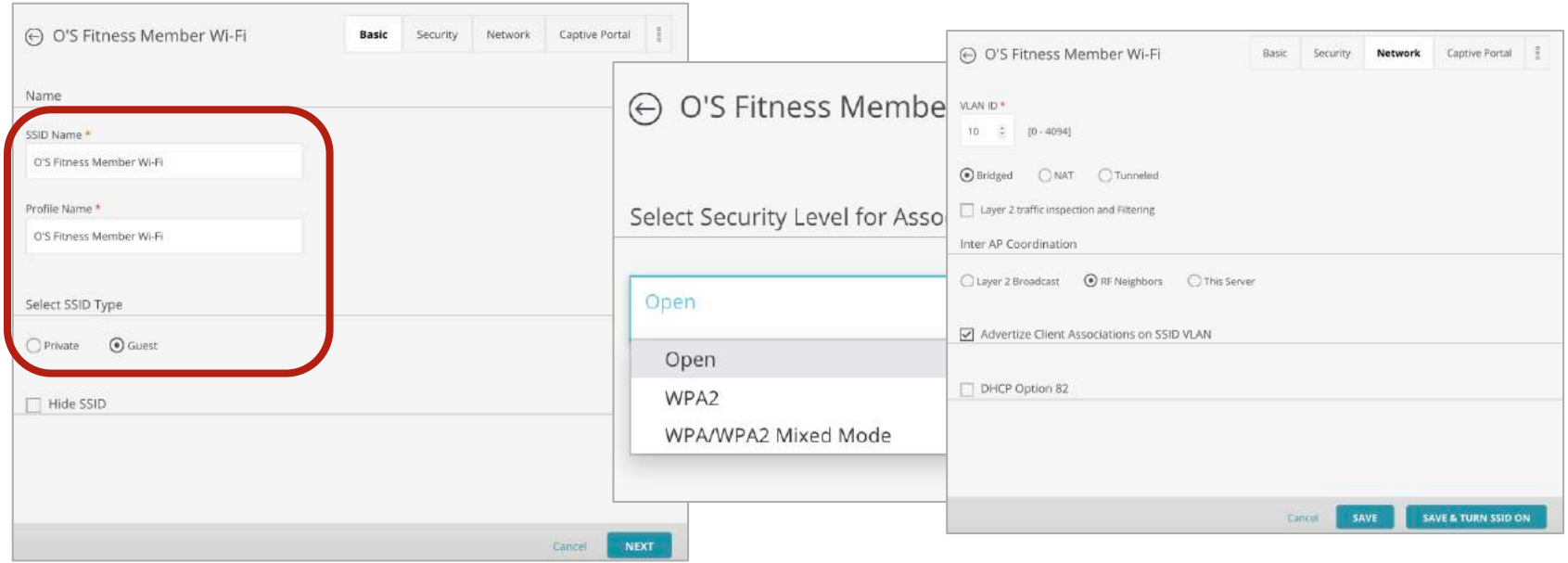
Create a New SSID

- Die Location wird festgelegt und über **Configure > WiFi > SSID**, per **Add SSID** eine neue SSID hinzugefügt.



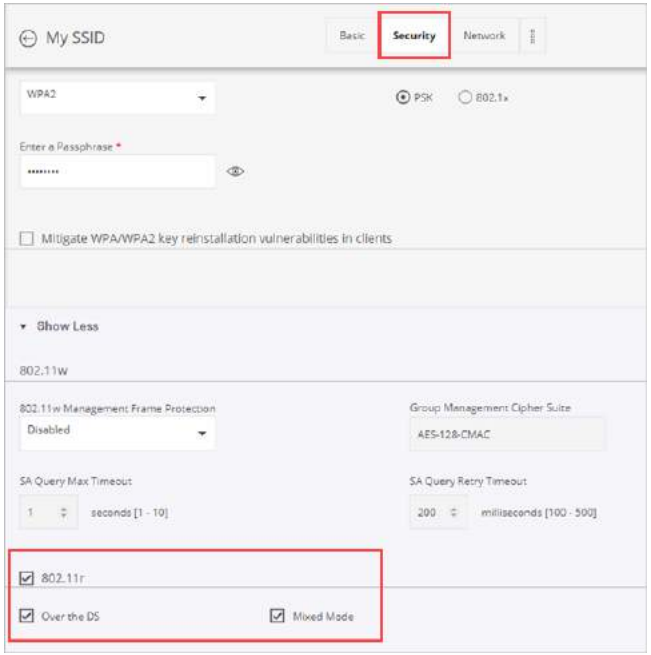
SSID Configuration

- Ein Wizard leitet durch die Schritte der Einrichtung

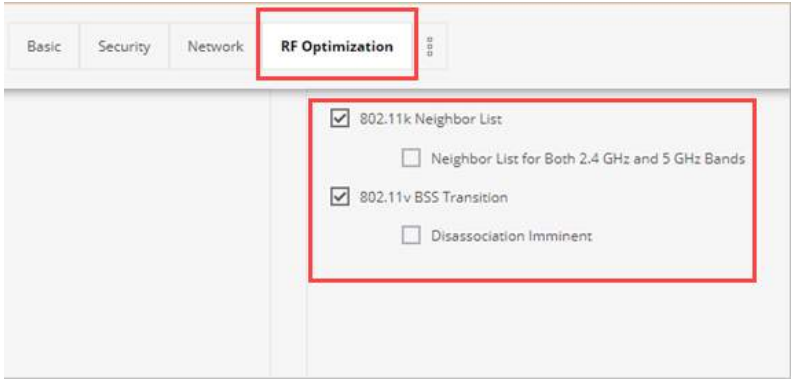


Roaming unterstützende Funktionen

802.11r Fast Roaming

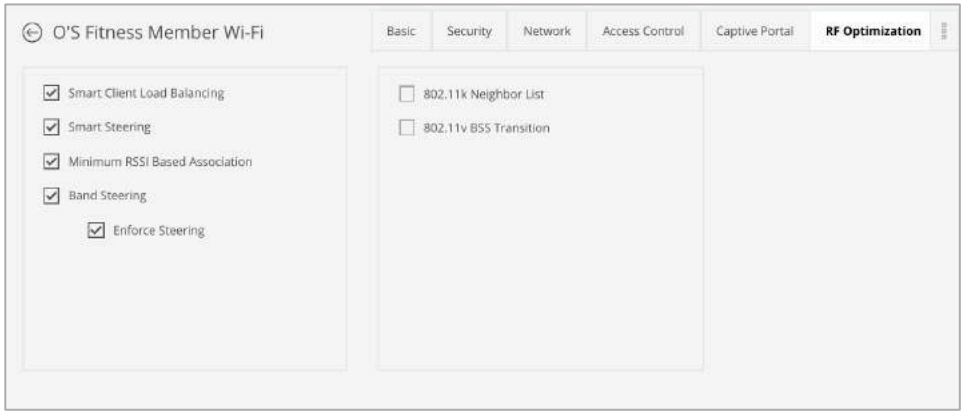


802.11k und 802.11v (für neuere Clients)



RF Optimizations

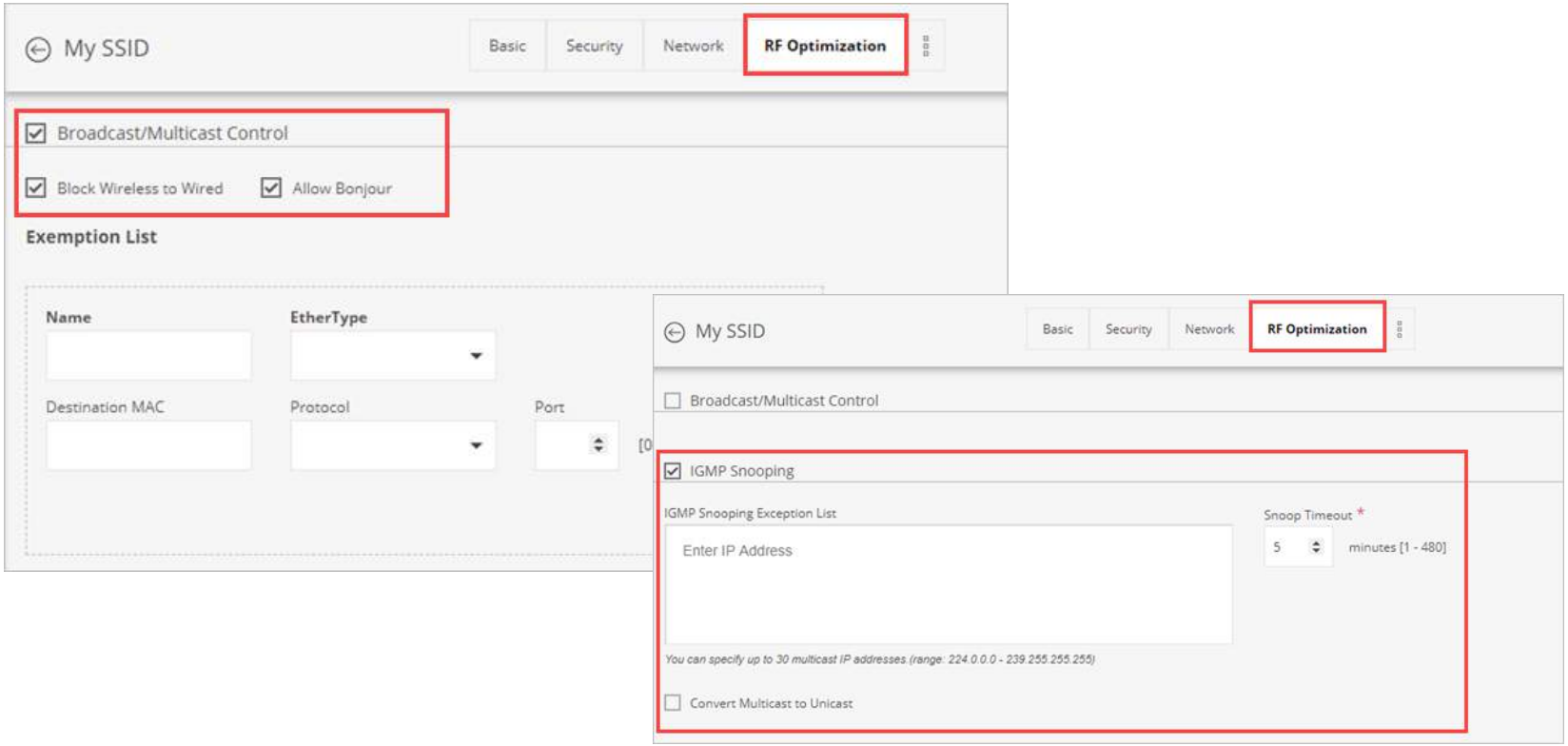
- **Smart Client Load Balancing** – intelligente Verteilung der Clients
- **Smart Steering** – Clients mit “schlechtem Empfang” werden aktiv abgemeldet durch den Accesspoint
- **Min Association RSSI** – Anmeldeversuche von Clients mit “schlechtem Empfang” werden abgewiesen.



RF Optimizations

- **Band Steering** – 5 GHz fähige Clients werden priorisiert in diesem Frequenzbereich angemeldet.
- **Enforce Steering** – zusätzliche Pakete stellen sicher, dass der Client nach Möglichkeit 5 GHz nutzt.

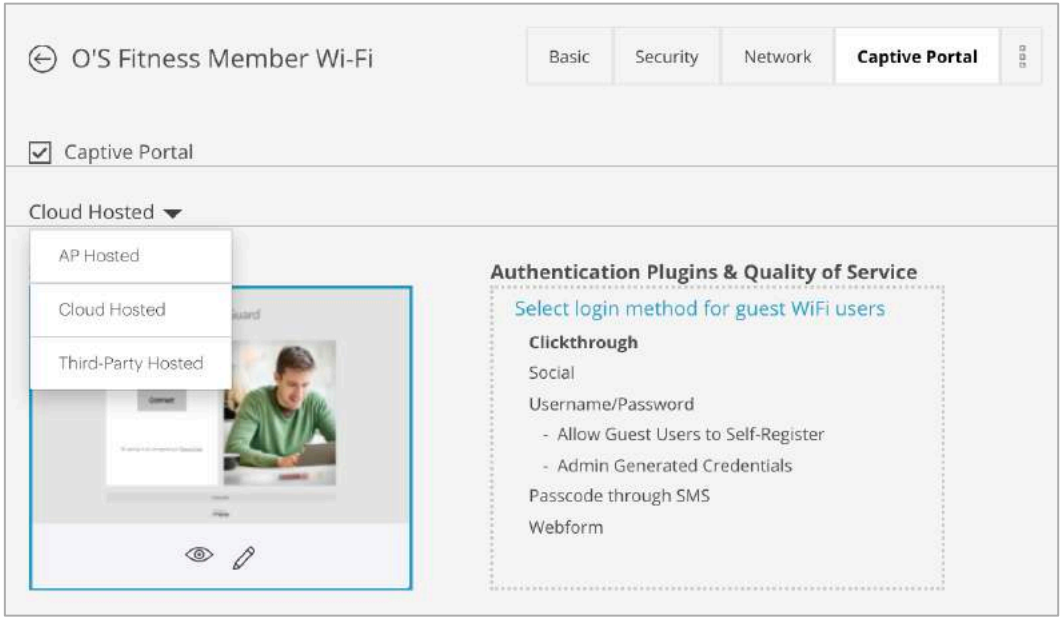
Broadcast/Multicast Control



Traffic Shaping & QoS

- Parameter zu Multicast und Unicast Data Rate anpassen

Captive Portal Konfiguration



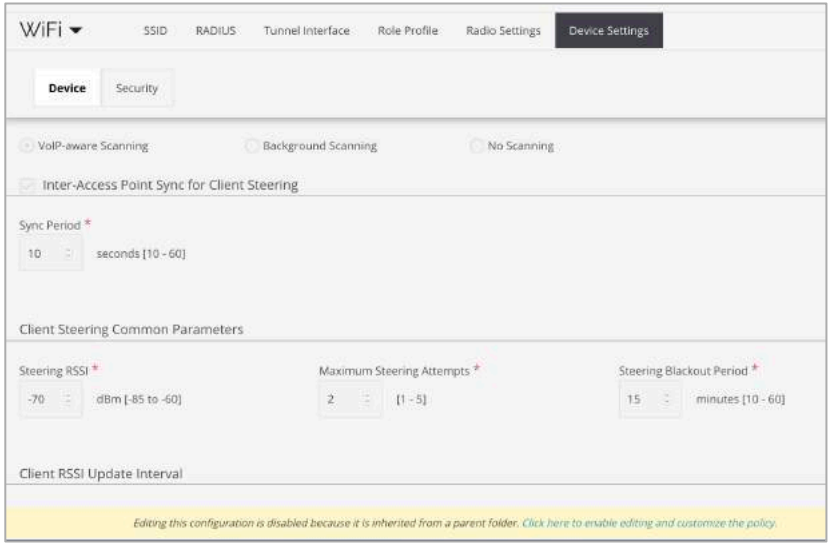
Device and Radio Settings

WatchGuard Training

Device Settings

Device Settings dienen der Accesspoint Anpassung im Sinne von Operating Mode, Steering Parametern, etc.

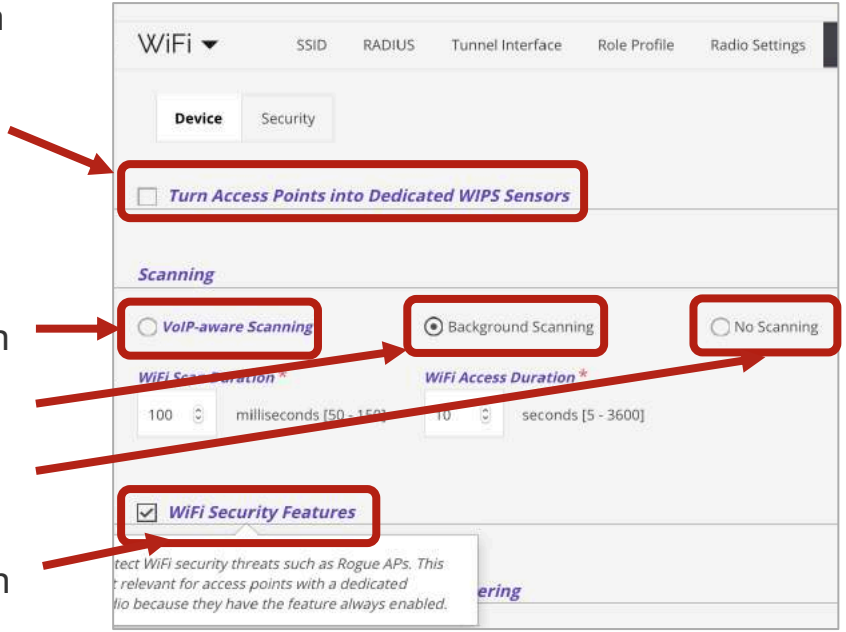
- Device Settings werden automatisiert von übergeordneten Locations geerbt
- Die Vererbung kann aufgehoben werden
- Farblicher Indikator in den Device Settings
- Ein “Rollback” auf die Einstellungen der übergeordneten Struktur ist möglich



Scanning Settings for WIPS and RF

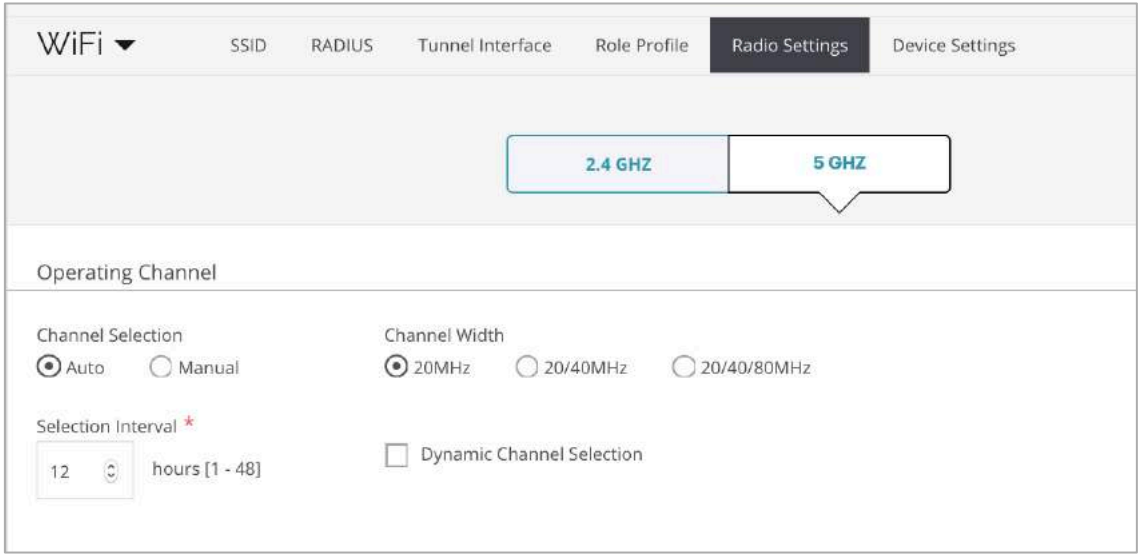
- Accesspoints mit 2 Radio Modulen werden als dedizierte WIPS Sensoren genutzt.”Overlay” – schützt auch bestehende Wi-Fi (3rd Party) Infrastruktur.

- Background scanning Optionen bei dual radio APs:
  - Kurzer Scan um VoIP Kommunikation weniger zu beinträchtigen.
  - “Standard” background Scan
  - Verzicht auf die WIPS Funktion und auf Background Scanning.
  - Aktiviert die WIPS Sicherheitsfunktion im Background Scanning Modus



Radio Settings

- Konfiguration der Einstellungen für 2.4 GHz and 5 GHz
- Optional kann ”Dynamic Channel Selection” aktiviert werden



Authorized Wi-Fi Policy

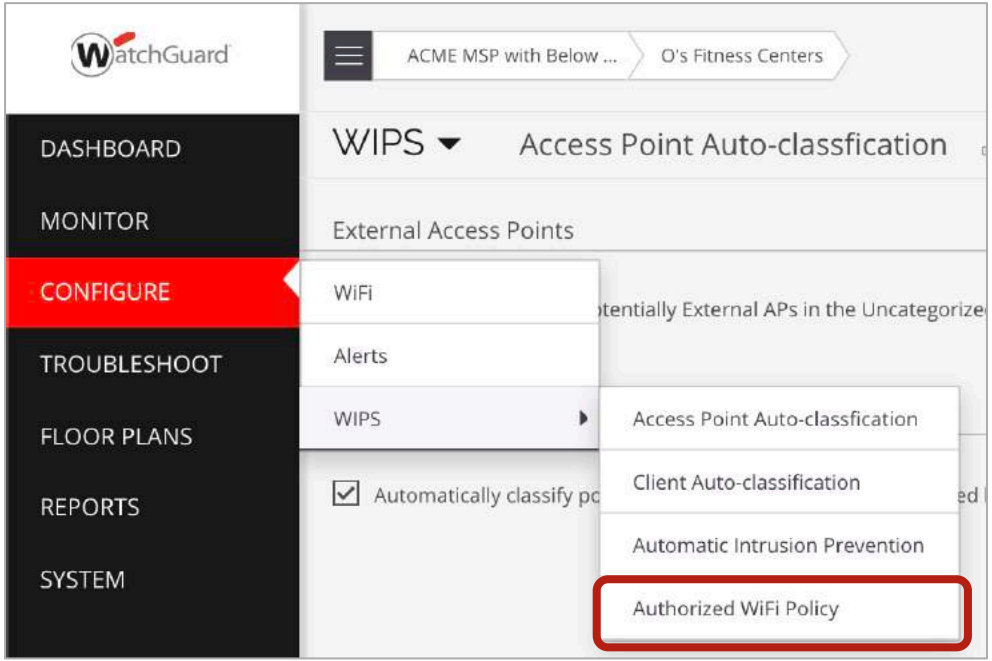
WatchGuard Training

Authorized WiFi Policy

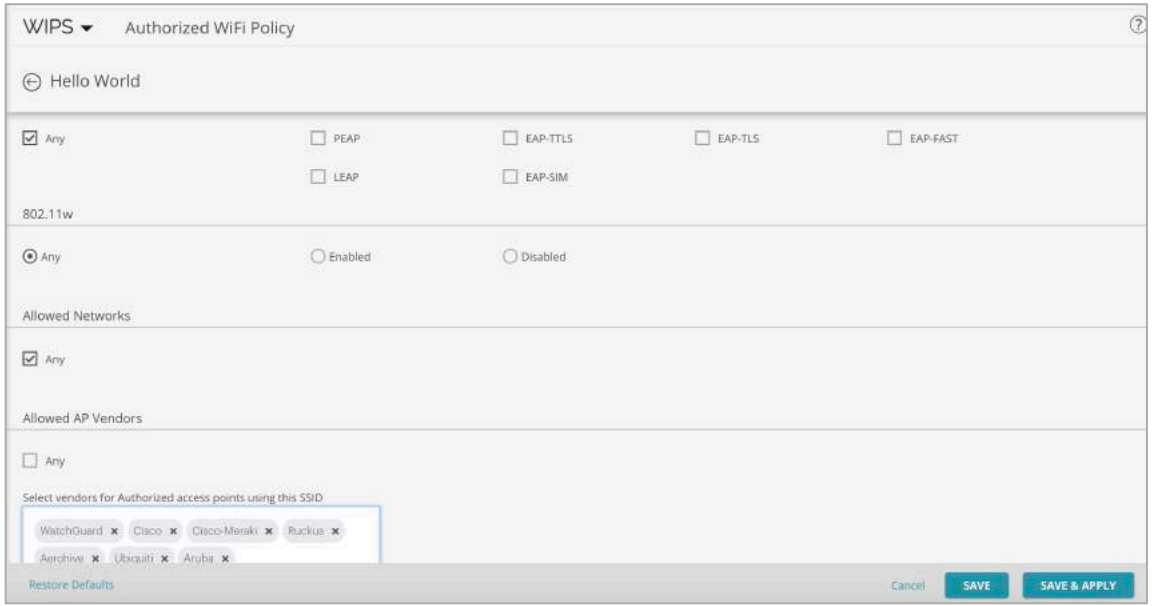
- Festlegung der WiFi Richtlinien pro Location (Vererbung in untergeordnete Locations)
  - Z.B. SSID Name, Security Parameter, Wi-Fi Vendor, etc.
- Verstößt ein Accesspoint gegen die zugewiesene Authorized WiFi Policy, so gilt dieser Accesspoint als “misconfigured”
- Ermöglicht aktive “Überprüfung” der Richtlinieneinhaltung – auch bei 3rd Party Accesspoints.

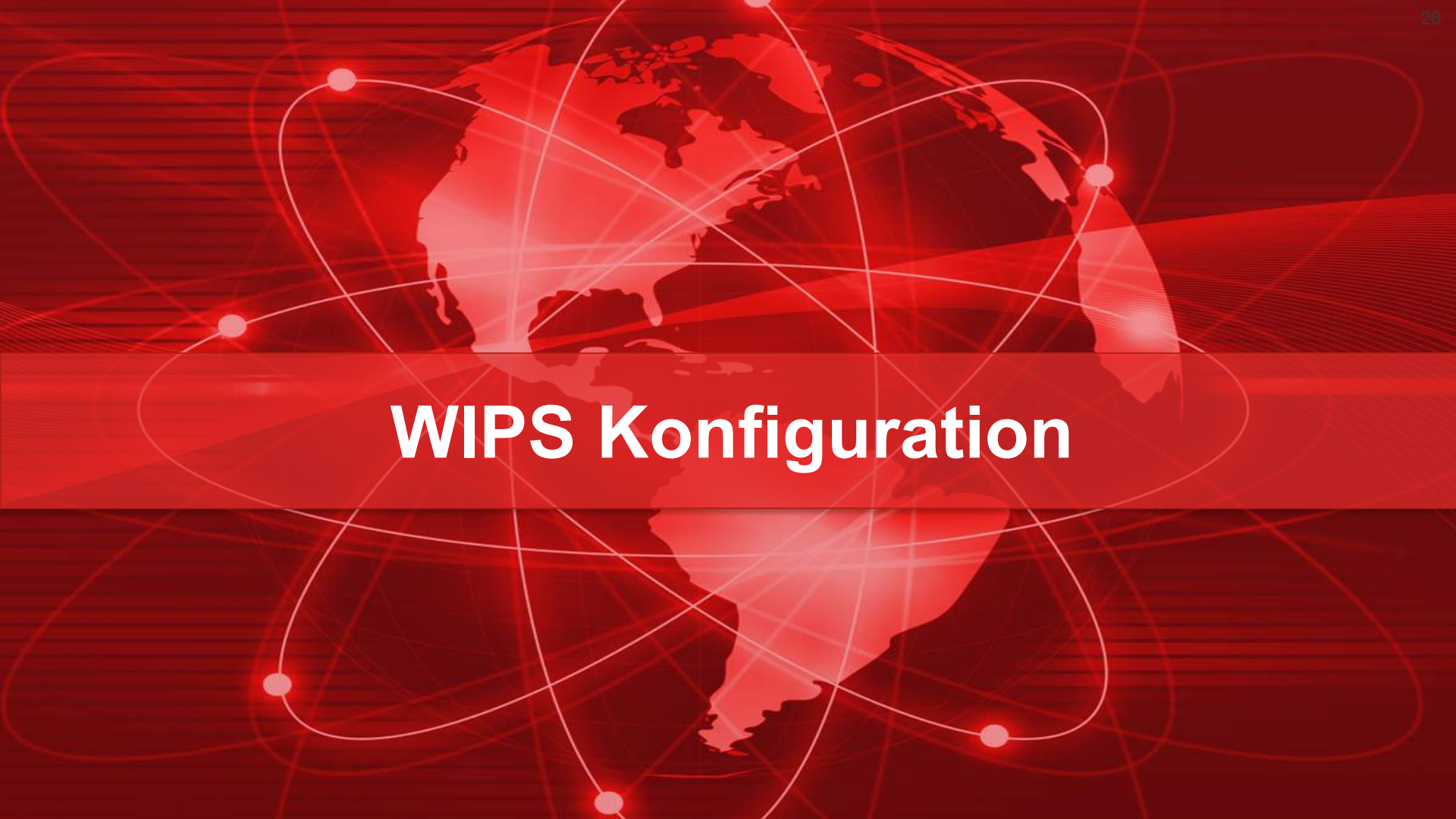
Authorized WiFi Policy

- **Configure > WIPS > Authorized WiFi Policy**



Configure > WIPS > Authorized WiFi Policy

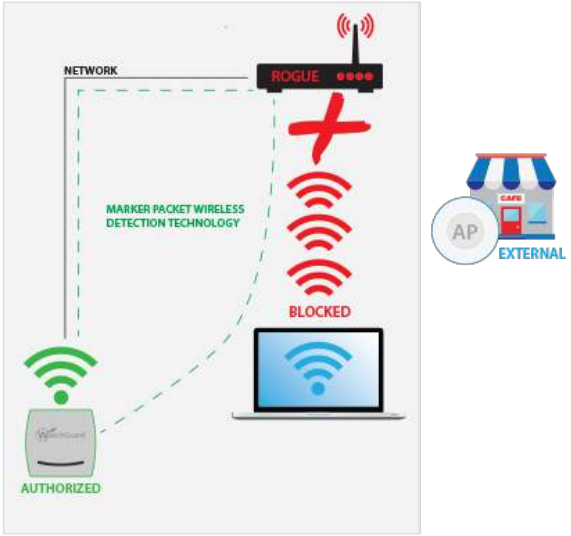




WIPS Konfiguration

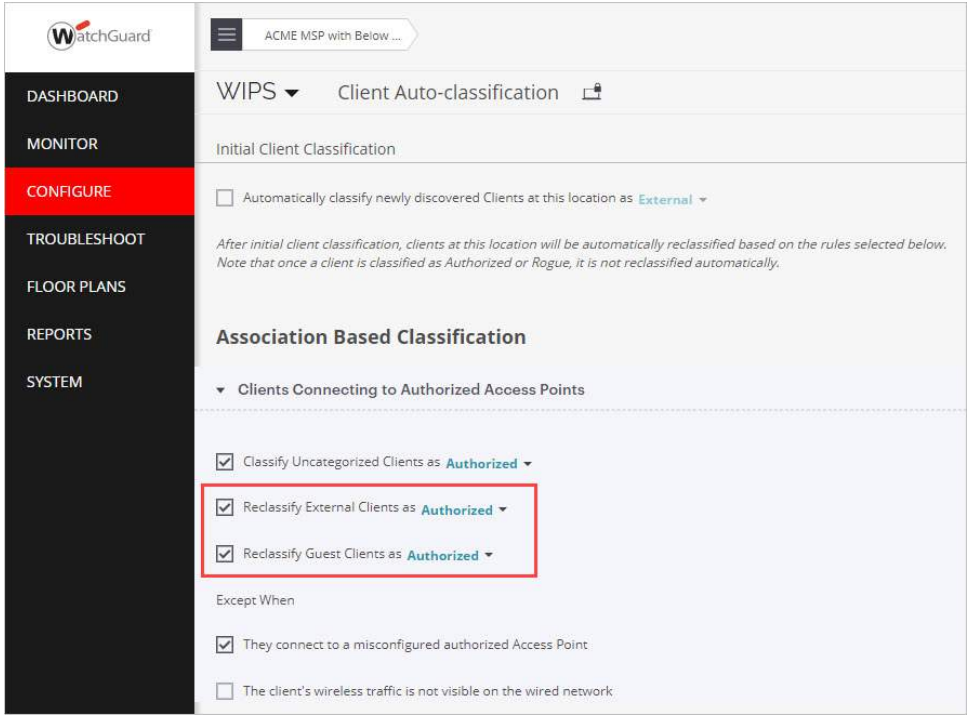
Wireless Intrusion Prevention System (WIPS)

- Access Point überwacht die Wi-Fi Umgebung auf schädliche Aktivitäten
- WIPS Technologie blockiert die Gefahr automatisch
- “Sicherheits Schild” für Ihr Unternehmen und die Nutzer



Client Auto-classification

- Empfohlene Anpassung der Default Konfiguration
  - Reclassify External Clients as “Authorized”.
  - Reclassify Guest Clients as “Authorized”.

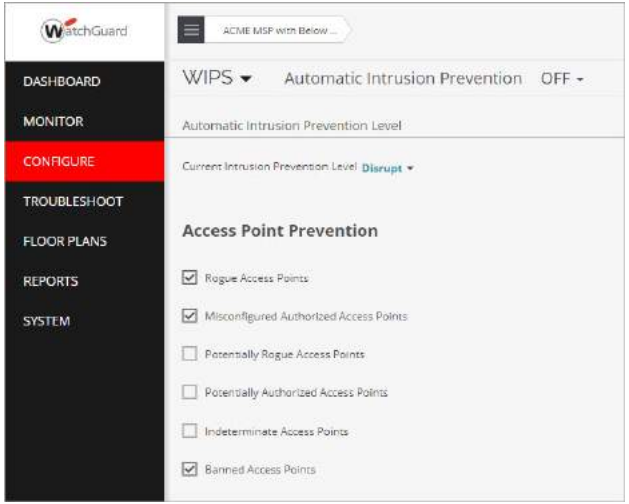


WIPS Konfiguration

- Die aktive und automatischen Abwehr von gefährlichen Aktivitäten wird hier festgelegt

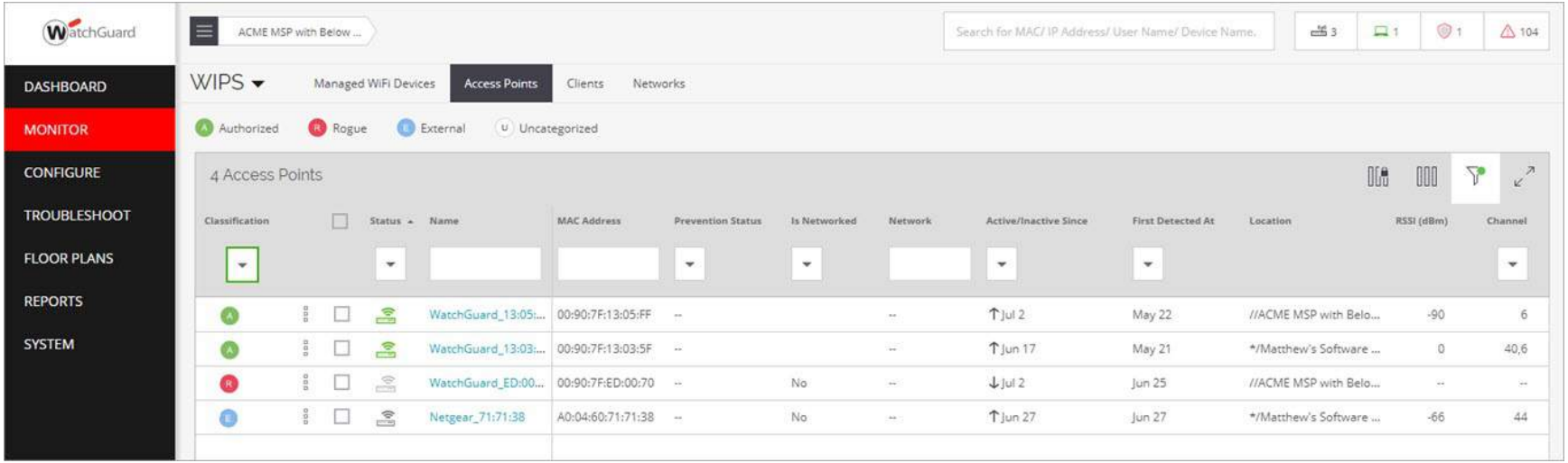
- Bitte in Zusammenhang mit der geplanten Installation prüfen

- Empfohlene Anpassungen der Default Konfiguration:
  - „MAC Spoofing“ aktivieren



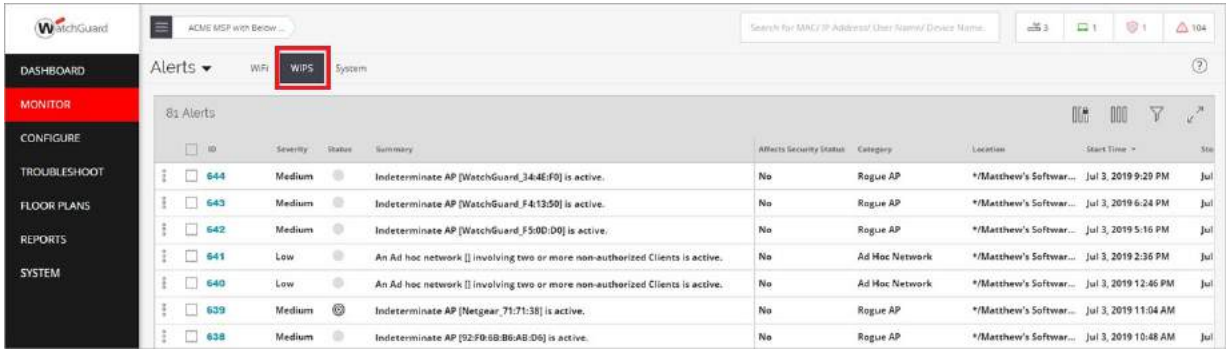
WIPS Klassifikation prüfen

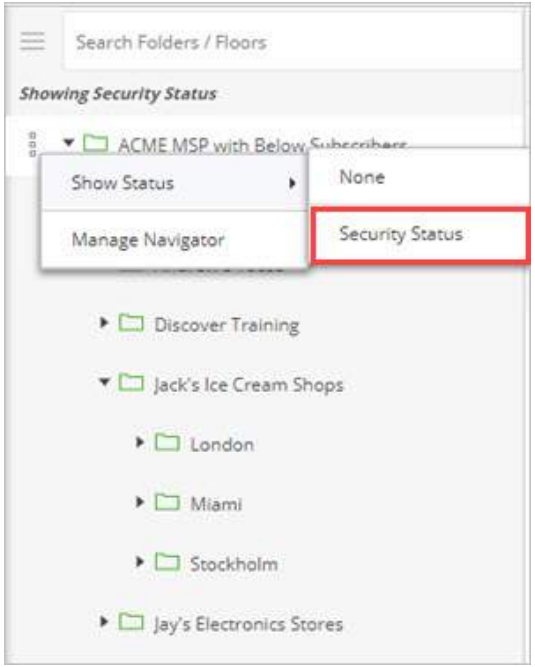
- In Monitor WIPS sollte die Klassifikation der Accesspoints und Clients geprüft werden.



Prüfen der Alarme und des Security Status

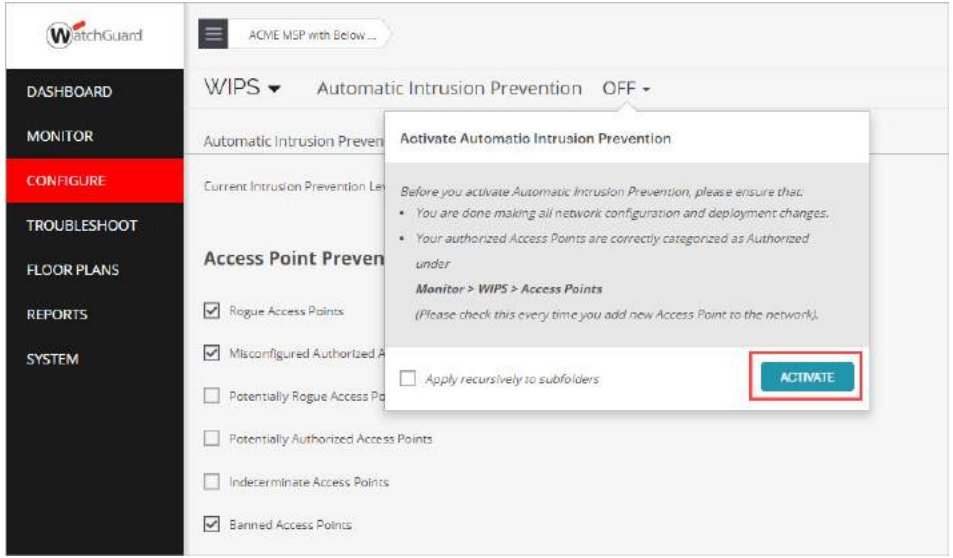
- Überprüfen auf offene Alarme und Events im Zusammenhang mit der WIPS Funktion





Aktivieren von WIPS

- „Scharfschaltung“
  - Ab jetzt werden automatische Abwehrmechanismen angewendet



Weitere Ressourcen – Deployment Guides

- https://www.watchguard.com/help/docs/Wi-Fi_Cloud/en-US/WatchGuard_Wi-Fi-Cloud_AP-Deployment-Guide.pdf

- https://www.watchguard.com/help/docs/Wi-Fi_Cloud/en-US/Wi-Fi-Cloud_WIPS_Trusted_Wireless_Environment.pdf

Let’s Make Wi-Fi Security a Global Standard!

www.trustedwirelessenvironment.com