



# **Best-Practices**

## **Sichere Wi-Fi Netze einrichten mit Discover**

# WatchGuard Wi-Fi Cloud

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



# Wi-Fi Subscriptions

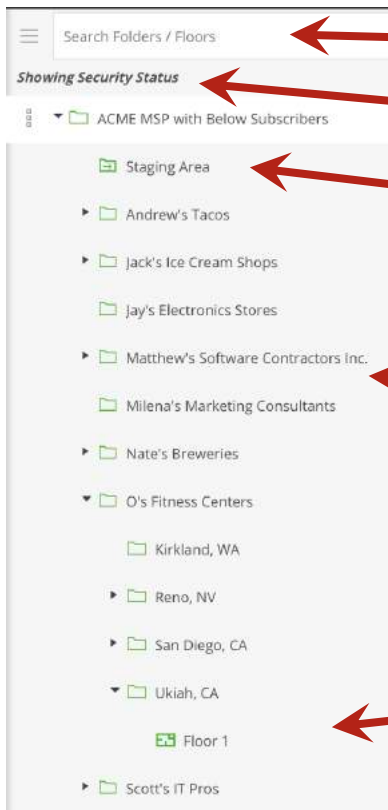
WatchGuard Wi-Fi Solution	Total Wi-Fi	Secure Wi-Fi	Basic Wi-Fi
<b>Management Platform</b>	Wi-Fi Cloud	Wi-Fi Cloud	Firebox Appliance*
<b>Scalability</b> Number of managed access points.	Unlimited	Unlimited	Limited**
<b>Configuration and Management</b> SSID configuration with VLAN support, band steering,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

# 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

The screenshot displays the WatchGuard web interface. On the left is a navigation sidebar with the following menu items: DASHBOARD, MONITOR (highlighted in red), CONFIGURE, TROUBLESHOOT, and FLOOR PLANS. The main content area is titled 'Showing Security Status' and shows a tree view of folders under 'ACME MSP with Below Subscribers'. The 'Staging Area' folder is highlighted with a red box. To the right, the 'WiFi' section is active, with 'Access Points' selected in a dropdown menu (also highlighted with a red box). Below this, a table shows '2 Access Points' with columns for Status, Name, and Update. Two access points are listed, both with a green checkmark in the Update column.

Status	Name	Update
<input type="checkbox"/>	WatchGuard_13:05:...	✓
<input type="checkbox"/>	WatchGuard_13:01:...	✓

# Verschieben von Accesspoints

The screenshot displays the WatchGuard management interface. The left sidebar contains navigation options: DASHBOARD, MONITOR (highlighted in red), CONFIGURE, TROUBLESHOOT, FLOOR PLANS, REPORTS, and SYSTEM. The main content area shows the 'Access Points' tab, with a table listing two access points. The first access point, 'WatchGuard\_13:05...', is selected with a checkmark in a red-bordered box. A 'Move To' dialog is open on the right, showing a tree view of folders. The 'Issaquah, WA' folder is highlighted in yellow. The dialog includes a search field, a 'Selected Location' field, and 'CANCEL' and 'MOVE' buttons at the bottom.

Status	Name	Update	MAC Address	IP Address
<input checked="" type="checkbox"/>	WatchGuard_13:05...		00:90:7F:13:05:FF	172.20.20.53
<input type="checkbox"/>	WatchGuard_13:01...		00:90:7F:13:01:9F	

Move To dialog details:

- Selected Location: Issaquah, WA
- Search Folders / Floors: [input field]
- ACME MSP with Below Subscribers
  - Staging Area
  - Andrew's Tacos
    - Boston, MA
    - Issaquah, WA (highlighted)
    - San Diego, CA
    - Likiah, CA
  - Jack's Ice Cream Shops
  - Jay's Electronics Stores
  - Matthew's Software Contractors Inc.
  - Milena's Marketing Consultants
  - Nate's Breweries
  - O's Fitness Centers
  - Scott's IT Pros

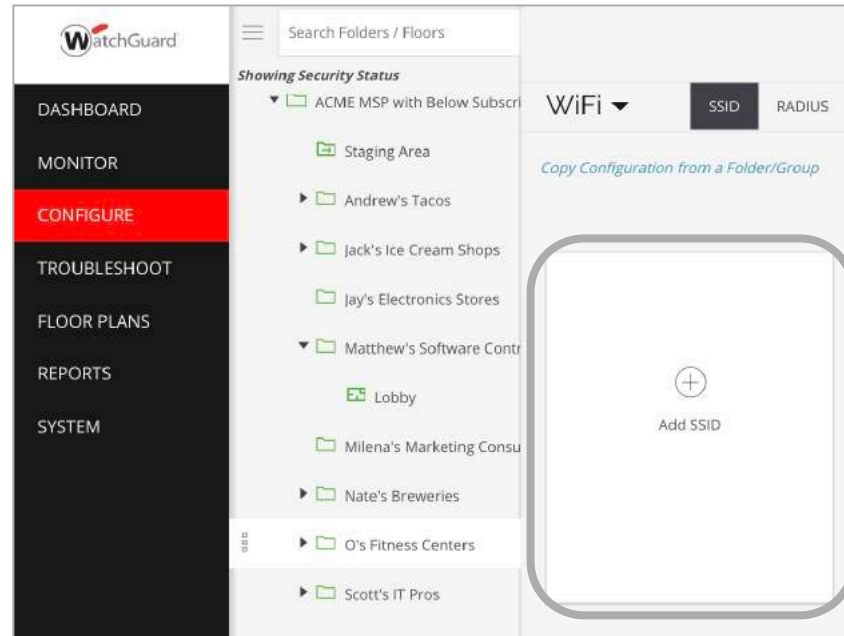


# Erzeugen von SSIDs in Discover



# 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

The image displays a multi-step configuration wizard for an SSID named "O'S Fitness Member Wi-Fi".

- Basic Step:** Shows fields for "SSID Name" (O'S Fitness Member Wi-Fi) and "Profile Name" (O'S Fitness Member Wi-Fi). The "Select SSID Type" section has "Guest" selected. A red rounded rectangle highlights these fields.
- Security Step:** A modal dialog titled "Select Security Level for Association" is shown, with a list containing "Open", "WPA2", and "WPA/WPA2 Mixed Mode".
- Network Step:** Shows "VLAN ID" set to 10. "Bridged" is selected under "Inter AP Coordination". "Advertise Client Associations on SSID VLAN" is checked.

Buttons at the bottom include "Cancel", "NEXT", "SAVE", and "SAVE & TURN SSID ON".

# Roaming unterstützende Funktionen

## 802.11r Fast Roaming

My SSID

Basic **Security** Network

WPA2  PSK  802.1x

Enter a Passphrase \*

Mitigate WPA/WPA2 key reinstallation vulnerabilities in clients.

▼ Show Less

802.11w

802.11w Management Frame Protection: Disabled

Group Management Cipher Suite: AES-128-CCMP

SA Query Max Timeout: 1 seconds [1 - 10]

SA Query Retry Timeout: 200 milliseconds [100 - 500]

802.11r

Over the DS  Mixed Mode

## 802.11k und 802.11v (für neuere Clients)

Basic Security Network **RF Optimization**

802.11k Neighbor List

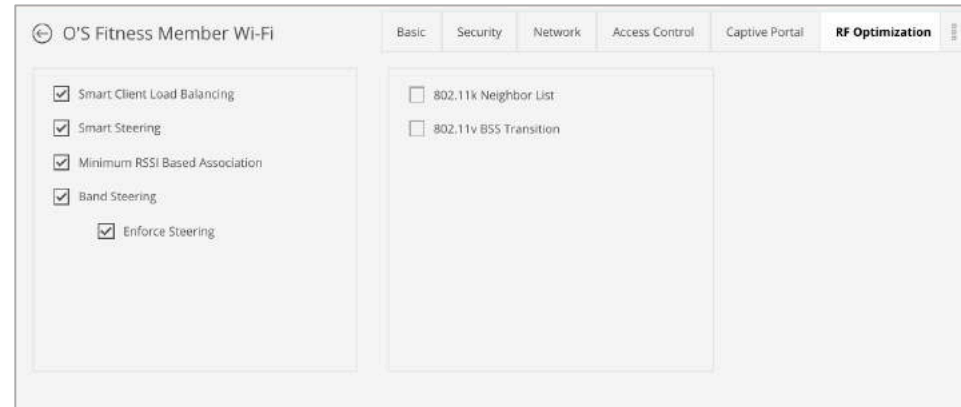
Neighbor List for Both 2.4 GHz and 5 GHz Bands

802.11v BSS Transition

Disassociation Imminent

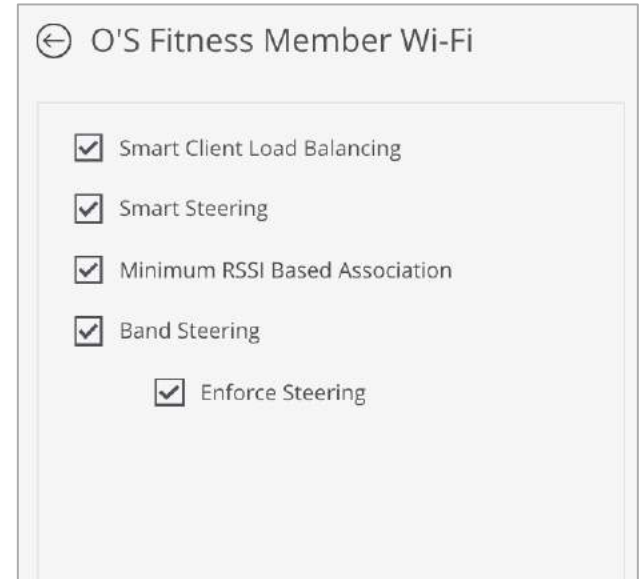
# RF Optimizations

- **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

The image displays two screenshots of a network configuration interface, likely from a WatchGuard device, showing the 'RF Optimization' tab for a 'My SSID'.

**Left Screenshot:** Shows the 'Broadcast/Multicast Control' section. The 'Broadcast/Multicast Control' checkbox is checked. Below it, 'Block Wireless to Wired' and 'Allow Bonjour' are also checked. An 'Exemption List' section is visible, containing fields for Name, EtherType, Destination MAC, Protocol, and Port.

**Right Screenshot:** Shows the 'IGMP Snooping' section. The 'IGMP Snooping' checkbox is checked. Below it, there is an 'IGMP Snooping Exception List' with a text input field labeled 'Enter IP Address'. To the right, the 'Snoop Timeout' is set to 5 minutes. Below the input field, a note states: 'You can specify up to 30 multicast IP addresses. (range: 224.0.0.0 - 239.255.255.255)'. At the bottom, the 'Convert Multicast to Unicast' checkbox is unchecked.

# Traffic Shaping & QoS

- Parameter zu Multicast und Unicast Data Rate anpassen

Multicast, Broadcast and Management Rate Control

Set the data rate for multicast, broadcast and management traffic to

24  Mbps [0 - 54]

Unicast Rate Control

Limit the maximum unicast traffic data rate to

0  Mbps [0 - 54]

Apply to all clients including 802.11n and 802.11ac

Limit the minimum unicast traffic data rate to

24  Mbps [0 - 54]

# Captive Portal Configuration

The screenshot shows the configuration page for 'O'S Fitness Member Wi-Fi'. At the top, there are navigation tabs: Basic, Security, Network, and Captive Portal (which is selected). Below the tabs, there is a checkbox for 'Captive Portal' which is checked. Underneath, a dropdown menu is open for 'Cloud Hosted', showing three options: 'AP Hosted', 'Cloud Hosted', and 'Third-Party Hosted'. The 'Cloud Hosted' option is selected, and a preview window shows a login page with a user image and a 'Login' button. To the right of the preview, there is a section titled 'Authentication Plugins & Quality of Service' with a dashed border. This section contains a link 'Select login method for guest WiFi users' and a list of authentication methods: Clickthrough, Social, Username/Password (with sub-options: Allow Guest Users to Self-Register and Admin Generated Credentials), Passcode through SMS, and Webform.

← O'S Fitness Member Wi-Fi

Basic Security Network **Captive Portal**

Captive Portal

Cloud Hosted ▼

- AP Hosted
- Cloud Hosted
- Third-Party Hosted

**Authentication Plugins & Quality of Service**

Select login method for guest WiFi users

- Clickthrough**
- Social
- Username/Password
  - Allow Guest Users to Self-Register
  - Admin Generated Credentials
- Passcode through SMS
- Webform





# Device and Radio Settings

# 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

The screenshot shows the 'Device Settings' tab for a WiFi network. The 'Device' tab is selected, and the 'Security' sub-tab is active. The settings include:

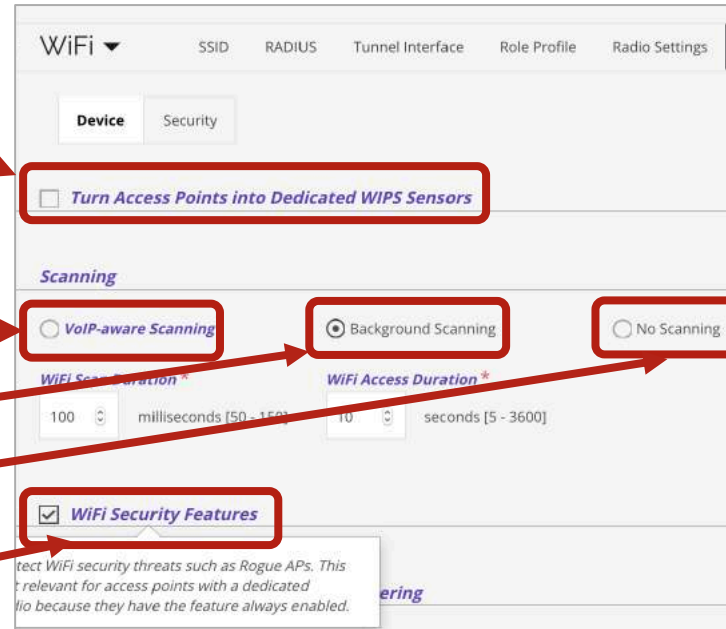
- Scanning options:  VoIP-aware Scanning,  Background Scanning,  No Scanning.
- Inter-Access Point Sync for Client Steering.
- Sync Period: 10 seconds [10 - 60].
- Client Steering Common Parameters:
  - Steering RSSI: -70 dBm [-85 to -60].
  - Maximum Steering Attempts: 2 [1 - 5].
  - Steering Blackout Period: 15 minutes [10 - 60].
- Client RSSI Update Interval: (empty field).

A yellow banner at the bottom of the interface reads: "Editing this configuration is disabled because it is inherited from a parent folder. Click here to enable editing and customize the policy."

Configuration is customized at the selected folder. [Inherit configuration from parent folder?](#)

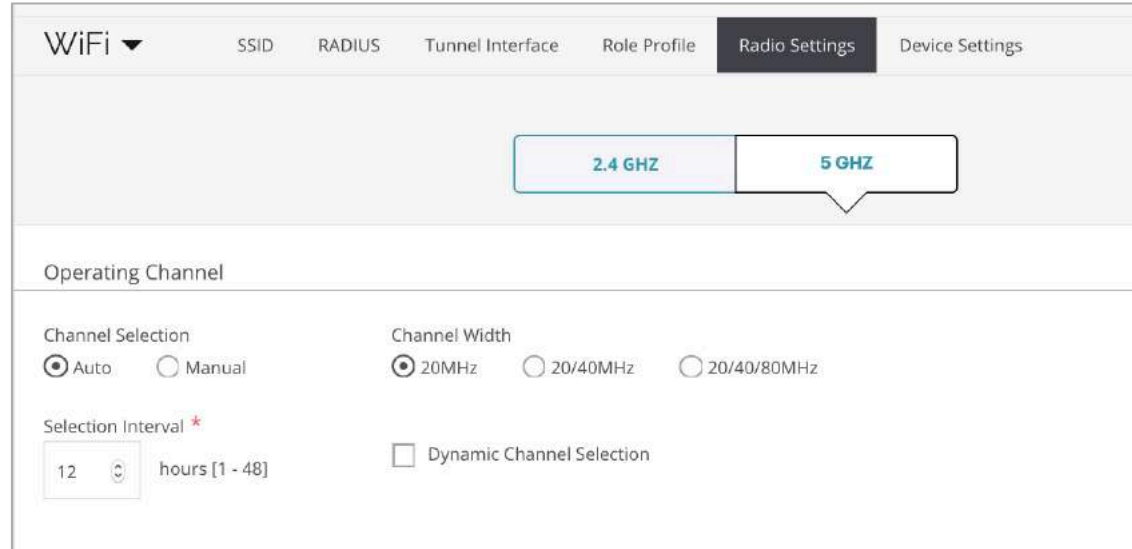
# Scanning Settings for WIPS and RF

- Accesspoints mit 2 Radio Modulen werden als dedizierte WIPS Sensoren genutzt. "Overlay" – schützt auch bestehende Wi-Fi (3<sup>rd</sup> Party) Infrastruktur.
- Background scanning Optionen bei dual radio APs:
  - Kurzer Scan um VoIP Kommunikation weniger zu beeinträchtigen.
  - "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



WiFi ▾ SSID RADIUS Tunnel Interface Role Profile **Radio Settings** Device Settings

2.4 GHZ 5 GHZ

Operating Channel

Channel Selection  
 Auto  Manual

Channel Width  
 20MHz  20/40MHz  20/40/80MHz

Selection Interval \*  
12 hours [1 - 48]

Dynamic Channel Selection



# Authorized Wi-Fi Policy

# 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 3<sup>rd</sup> Party Accesspoints.

# Authorized WiFi Policy

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

The screenshot displays the WatchGuard web interface. On the left is a dark navigation sidebar with the following menu items: DASHBOARD, MONITOR, CONFIGURE (highlighted in red), TROUBLESHOOT, FLOOR PLANS, REPORTS, and SYSTEM. The main content area shows a breadcrumb trail: ACME MSP with Below ... > O's Fitness Centers. Below this, there is a 'WIPS' dropdown menu with a downward arrow, followed by 'Access Point Auto-classification'. Underneath, there is a section for 'External Access Points'. A 'WIFI' dropdown menu is open, showing options: Alerts, WIPS (with a rightward arrow), and a checked checkbox for 'Automatically classify po...'. The 'WIPS' dropdown is further expanded to show: Access Point Auto-classification, Client Auto-classification, Automatic Intrusion Prevention, and Authorized WiFi Policy. The 'Authorized WiFi Policy' option is highlighted with a red rectangular box.

# Configure > WIPS > Authorized WiFi Policy

WIPS ▾ Authorized WiFi Policy ?

⊖ Hello World

Any  PEAP  EAP-TTLS  EAP-TLS  EAP-FAST  
 LEAP  EAP-SIM

802.11w

Any  Enabled  Disabled

Allowed Networks

Any

Allowed AP Vendors

Any

Select vendors for Authorized access points using this SSID

WatchGuard x Cisco x Cisco-Meraki x Ruckus x  
Aerohive x Ubiquiti x Aruba x

Restore Defaults Cancel SAVE SAVE & APPLY

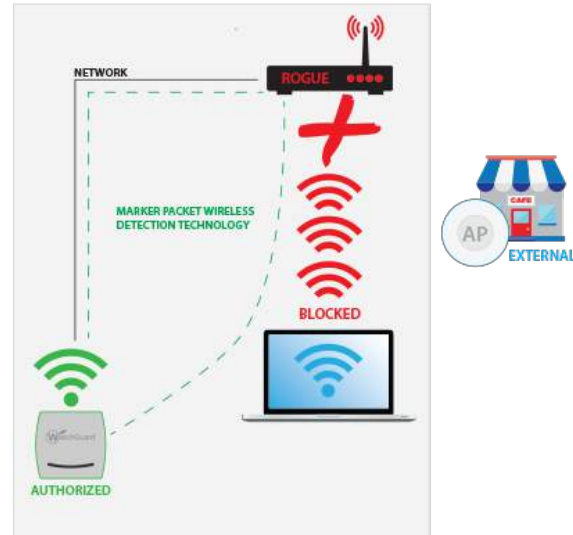




# WIPS Konfiguration

# Wireless Intrusion Prevention System (WIPS)

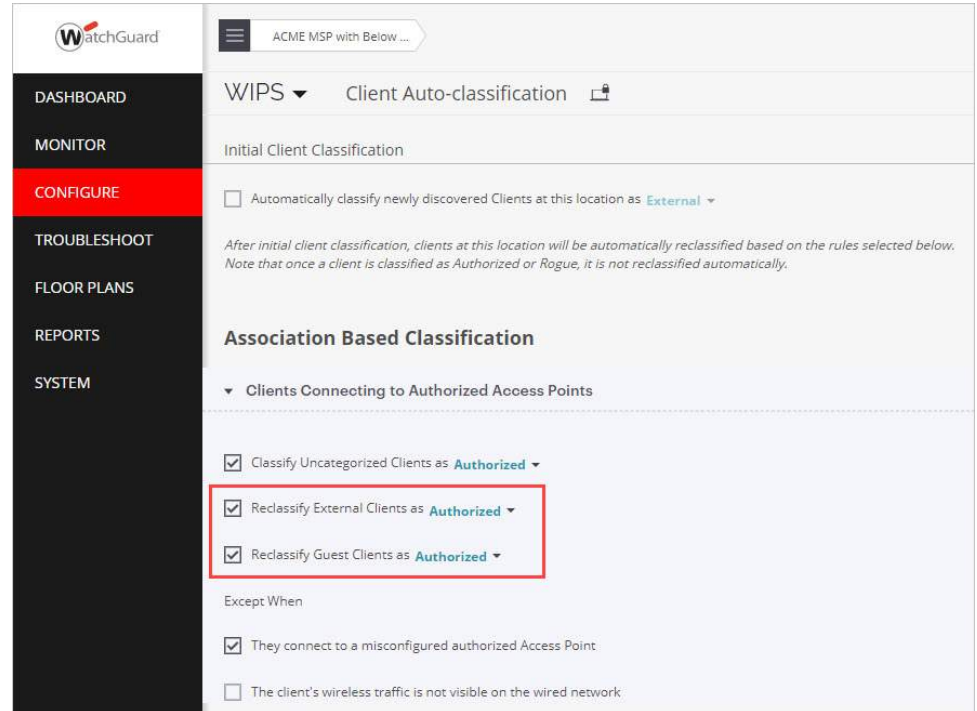
- Access Point überwacht die Wi-Fi Umgebung auf schädliche Aktivitäten
- WIPS Technologie blockiert die Gefahr automatisch
- “Sicherheits Schild” für Ihr Unternehmen und die Nutzer



# Client Auto-classification

- Empfohlene Anpassung der Default Konfiguration

- Reclassify External Clients as “Authorized”.
- Reclassify Guest Clients as “Authorized”.



WatchGuard

ACME MSP with Below ...

WIPS Client Auto-classification

Initial Client Classification

Automatically classify newly discovered Clients at this location as **External**

*After initial client classification, clients at this location will be automatically reclassified based on the rules selected below. Note that once a client is classified as Authorized or Rogue, it is not reclassified automatically.*

**Association Based Classification**

▼ Clients Connecting to Authorized Access Points

Classify Uncategorized Clients as **Authorized**

Reclassify External Clients as **Authorized**

Reclassify Guest Clients as **Authorized**

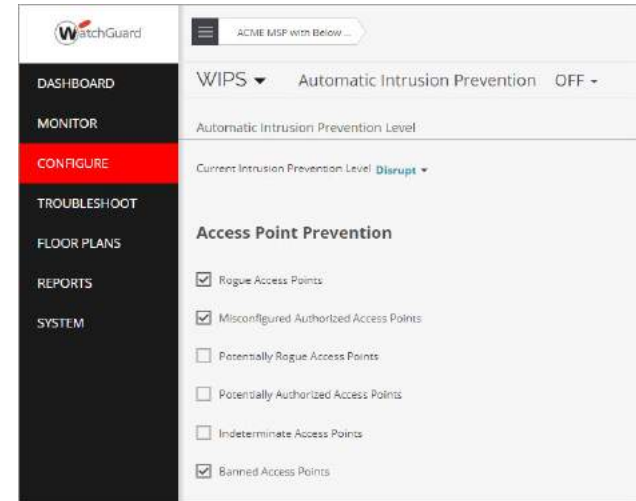
Except When

They connect to a misconfigured authorized Access Point

The client's wireless traffic is not visible on the wired network

# WIPS Konfiguration

- Die aktive und automatische 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.

The screenshot displays the WatchGuard WIPS monitoring interface. The left sidebar contains navigation options: DASHBOARD, MONITOR (highlighted), CONFIGURE, TROUBLESHOOT, FLOOR PLANS, REPORTS, and SYSTEM. The main content area shows the 'WIPS' section with tabs for 'Managed WiFi Devices', 'Access Points', 'Clients', and 'Networks'. The 'Access Points' tab is active, showing 4 Access Points. The interface includes a search bar, a filter icon, and a table of data.

Classification	Status	Name	MAC Address	Prevention Status	Is Networked	Network	Active/Inactive Since	First Detected At	Location	RSSI (dBm)	Channel
	<input type="checkbox"/>	WatchGuard_13:05:...	00:90:7F:13:05:FF	--	--	--	↑ Jul 2	May 22	//ACME MSP with Belo...	-90	6
	<input type="checkbox"/>	WatchGuard_13:03:...	00:90:7F:13:03:5F	--	--	--	↑ Jun 17	May 21	*//Matthew's Software ...	0	40,6
	<input type="checkbox"/>	WatchGuard_ED:00:...	00:90:7F:ED:00:70	--	No	--	↓ Jul 2	Jun 25	//ACME MSP with Belo...	--	--
	<input type="checkbox"/>	Netgear_71:71:38	A0:04:60:71:71:38	--	No	--	↑ Jun 27	Jun 27	*//Matthew's Software ...	-66	44

# Prüfen der Alarme und des Security Status

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

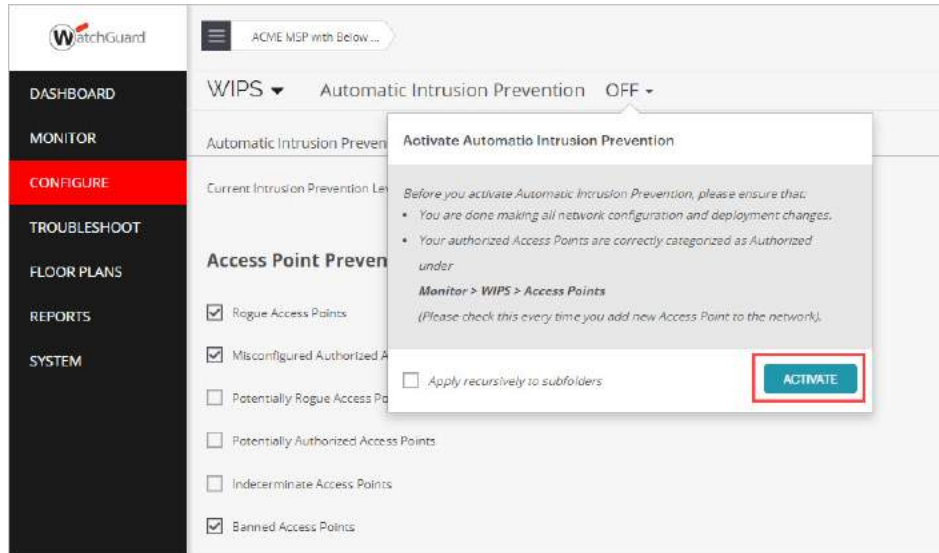
The screenshot shows the WatchGuard WIPS interface. The left sidebar contains navigation options: DASHBOARD, MONITOR (highlighted), CONFIGURE, TROUBLESHOOT, FLOOR PLANS, REPORTS, and SYSTEM. The main area displays a table of alerts for 'ACME MSP with Below...'. The 'WIPS' tab is selected and highlighted with a red box. The table lists several alerts with columns for ID, Severity, Status, Summary, Affects Security Status, Category, Location, and Start Time.

ID	Severity	Status	Summary	Affects Security Status	Category	Location	Start Time	Site
644	Medium	●	Indeterminate AP [WatchGuard_344E:F9] is active.	No	Rogue AP	*Matthew's Softwar...	Jul 3, 2019 9:29 PM	Jul
643	Medium	●	Indeterminate AP [WatchGuard_F4:13:50] is active.	No	Rogue AP	*Matthew's Softwar...	Jul 3, 2019 6:24 PM	Jul
642	Medium	●	Indeterminate AP [WatchGuard_F5:0D:D0] is active.	No	Rogue AP	*Matthew's Softwar...	Jul 3, 2019 5:16 PM	Jul
641	Low	●	An Ad hoc network [] involving two or more non-authorized Clients is active.	No	Ad Hoc Network	*Matthew's Softwar...	Jul 3, 2019 2:36 PM	Jul
640	Low	●	An Ad hoc network [] involving two or more non-authorized Clients is active.	No	Ad Hoc Network	*Matthew's Softwar...	Jul 3, 2019 12:46 PM	Jul
639	Medium	⊙	Indeterminate AP [Netgear_71:71:38] is active.	No	Rogue AP	*Matthew's Softwar...	Jul 3, 2019 11:04 AM	Jul
638	Medium	●	Indeterminate AP [92:F0:6B:B6:AB:D6] is active.	No	Rogue AP	*Matthew's Softwar...	Jul 3, 2019 10:48 AM	Jul

The screenshot shows a dropdown menu for 'ACME MSP with Below...'. The menu options are 'Show Status' (with a sub-menu arrow), 'Manage Navigator', and 'Security Status' (highlighted with a red box). The sub-menu for 'Show Status' shows 'None' as the selected option.

# 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/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](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](http://www.trustedwirelessenvironment.com)

A red-tinted graphic featuring a globe with a network of white lines and glowing nodes, symbolizing global connectivity or technology.

**Vielen Dank!**