

A large, detailed image of a lion's head and shoulders, rendered with a red color cast. The lion is looking slightly to the right with a serious expression. The background is white.

# Best Practices – Gateway Wireless Controller Wi-Fi Accesspoints mit Firebox verwalten

Jonas Spieckermann  
Senior Sales Engineer

[Jonas.Spieckermann@watchguard.com](mailto:Jonas.Spieckermann@watchguard.com)



# Grundlagen

# Firebox Wi-Fi und Accesspoints

- Firebox Wireless:
  - Ein Radio Modul mit maximal 3 SSIDs
  - Nutzbar als Wireless Client (WLAN = External Interface)
  - Der Accesspoint oder Wireless Client wird als Netzwerk Interface eingerichtet
  
- WatchGuard APs:
  - Jeder Accesspoint nutzt 2 Radio Module
  - Verwaltung über WatchGuard Firebox
    - Verbunden an Trusted, Optional, oder Custom Interface
    - 1 Firebox kann viele Accesspoints vewalten
    - Eine SSID kann für mehrere Accesspoints zur besseren WLAN Abdeckung genutzt werden

# AP120, AP320, AP322, and AP420 Devices

- AP120 — Concurrent 2x2 MIMO capability and a dual radio that supports 2.4GHz (802.11b/g/n) and 5GHz (11a/n/ac)
- AP320 — 3x3 MIMO capability and a dual radio that supports 2.4GHz (802.11b/g/n) and 5GHz (11a/n/ac)
- AP322 — outdoor model, 3x3 MIMO capability and a dual radio that supports 2.4GHz (802.11b/g/n) and 5GHz (11a/n/ac)
- AP420 — High performance enterprise AP device with 4x4:4 MU-MIMO 802.11ac Wave 2 capabilities



# WatchGuard AP Wi-Fi Solutions

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	✓	✓	
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	✓		
GO Mobile Web App Easily set-up your network and configuration from any mobile device	✓		
Firebox Gateway Wireless Controller			✓
Standard 24x7 Support Hardware warranty with advance hardware replacement, customer support, and software updates	✓	✓	✓

# Vorbereitung der WLAN Installation

- Welche Wi-Fi Protokolle sollen unterstützt werden (802.11a/b/g/n/ac)?
  - Was für Wi-Fi Clients werden genutzt und müssen unterstützt werden?
- Welche SSIDs sind nötig und wie sind die Netzwerkzuordnungen?
  - Unterschiedliche Gruppen mit differenzierten Zugriffsrechten?
  - Wird ein Gast-Netzwerk benötigt?
- Physikalische Positionierung der Accesspoints?
  - Wie ist die Lokation/das Gebäude?
  - Welche Bereiche sollen mit Wi-Fi ausgestattet werden?
  - Durchführung eines Site-Surveys?

# Positionierung der Accesspoints

- Zentrale Positionierung der Accesspoints (keine Hindernisse, Ecken, etc. )
- Erhöhte Montage bietet optimierte Signal-Stärke und Reichweite
- Vermeiden Sie möglichst eine Positionierung neben anderen elektrischen Geräte oder potentiellen Störquellen
- Accesspoints nicht zu nah nebeneinander platzieren.
  - Bei mehreren Etagen auch Überlappungen zwischen den Etagen berücksichtigen

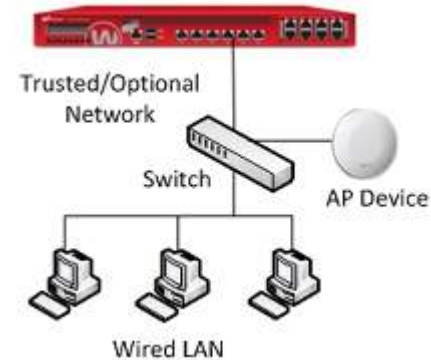
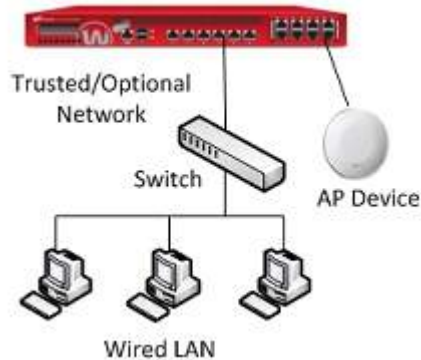
# Grundlagen

- Durch Accesspoints kann ein Firebox geschütztes Netzwerk leicht um Wi-Fi Zugriffe erweitert werden

*Direkte Verbindung der  
Accesspoints mit Firebox*

**oder**

*Verbindung der Accesspoints  
über einen Switch*





# Accesspoint-Deployment

- Folgende Schritte sind notwendig:
  - Aktivierung des Gateway Wireless Controller auf Ihrer Firebox.
  - Anschließen des Accesspoints
  - Pairing des AP mit Ihrer Firebox.
  - Konfiguration der AP Einstellungen.
  - Konfiguration der SSIDs.
- Automatic Deployment
  - Firebox Gateway Wireless Controller unterstützt “automatic deployment”. Hierüber können automatisch festgelegte SSIDs auf neu im Netzwerk aufgenommen Accesspoints angewendet werden.

# Accesspoint Deployment mit VLANs

- Bei Verwendung von VLANs sind folgenden Schritte zusätzlich erforderlich:
  - Konfiguration der VLANs (tagged) für die SSIDs.
  - Konfiguration eines VLANs (untagged) für die Verwaltung der Accesspoints .
  - Ggf. Anpassung der Switchkonfiguration

A detailed illustration of a lion, colored in a monochromatic red hue, standing and looking towards the viewer. The lion's mane is thick and textured, and its body is muscular. A semi-transparent red horizontal bar is overlaid across the middle of the image, containing the title text.

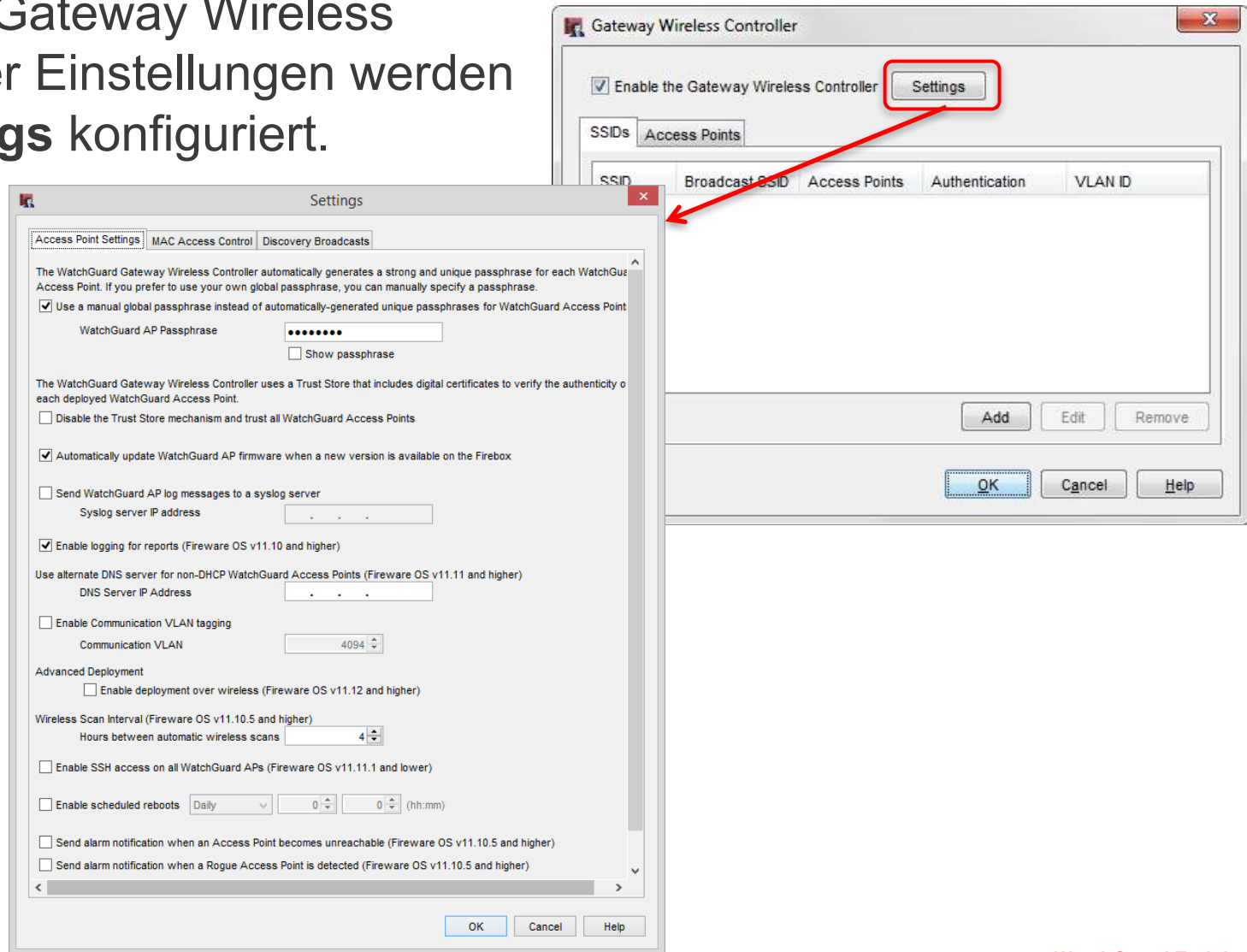
# Einrichtung des Gateway Wireless Controller

# Gateway Wireless Controller

- Gateway Wireless Controller settings
  - Einstellungen für alle Accesspoints
- AP device settings
  - Einstellungen für einen einzelnen Accesspoint
- SSIDs
  - Einstellungen zu den verwendeten SSIDs zu denen Endgeräte sich verbinden werden.
  - SSIDs können von mehreren APs verwendet werden.
- Trusted APs
  - Der Trust-Store des Gateway Wireless Controllers verhindert das nicht-vertrauenswürdige Accesspoints Konfigurationen erhalten/synchronisieren.

# Konfiguration der GWC Einstellungen

- Globale Gateway Wireless Controller Einstellungen werden in **Settings** konfiguriert.



# Passphrase

- Konfiguration des WatchGuard AP Passphrase
  - Sie können ein manuell definiertes globales Passwort verwenden, oder die automatische Passwortverwaltung wählen. Das Passphrase sichert die Kommunikation zwischen Accesspoint und GWC
- Standard: Manual global AP passphrase

Settings

Access Point Settings | MAC Access Control | Discovery Broadcasts

The WatchGuard Gateway Wireless Controller will automatically generate a strong and unique passphrase for each WatchGuard AP Device. If you prefer to use a manual, global passphrase instead, you may supply it below.

Use a manual, global passphrase instead of automatically-generated unique passphrases for WatchGuard AP Devices

WatchGuard AP Passphrase:

Show passphrase

The WatchGuard Gateway Wireless Controller uses a Trust Store including digital certificates to verify the authenticity of each deployed WatchGuard AP Device.

Disable the Trust Store mechanism; all WatchGuard AP Devices will always be trusted

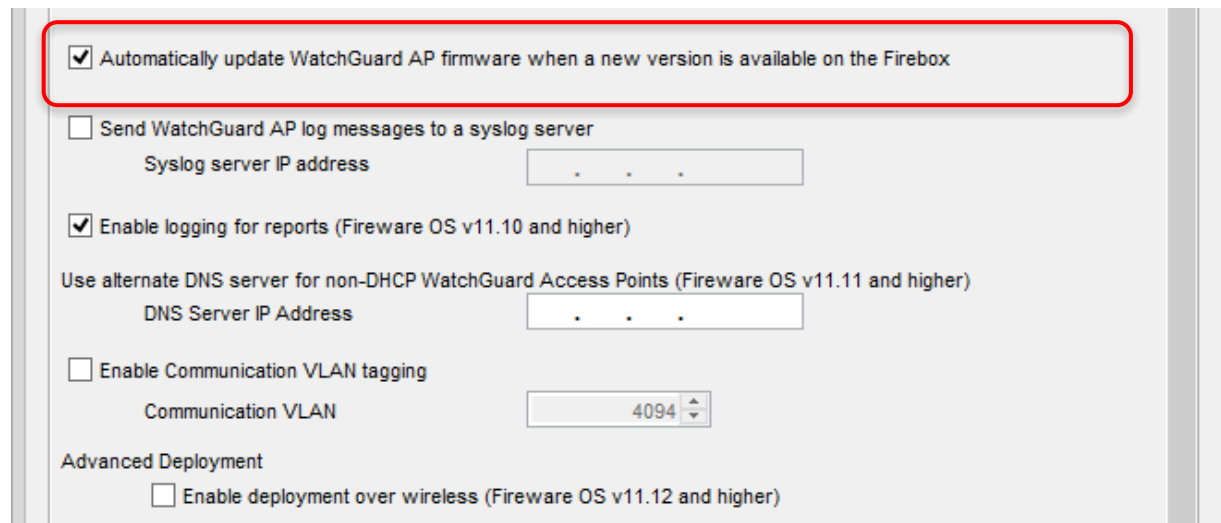
# Automatic Passphrase Management

- Automatic Passphrase Management
  - Optionaler Automatismus zur Verwendung von zufällig generierten Passphrases pro Accespoint
  - Die Passphrase wird nur geändert wenn der AP auf Factory Default zurückgesetzt wird
  - Die Passphrase ist in den Gateway Wireless Controller Dashboards einsehbar.

**Hinweis: automatisch generierte AP Passphrases werden nicht gesichert und können nicht widerhergestellt werden (z.B. bei Hardware defekten des GWC).**

# GWC Einstellungen

- Automatische Firmware Updates
  - Accesspoints werden automatisch (nacheinander) aktualisiert wenn eine neue Firmware verfügbar ist (im GWC)
  - Automatische Updates erfolgen zwischen 00:00 und 04:00 Uhr
    - Zeit-Einstellungen der Firebox prüfen (NTP ermöglichen)



The screenshot shows a configuration page for WatchGuard AP firmware updates. The first option, "Automatically update WatchGuard AP firmware when a new version is available on the Firebox", is checked and highlighted with a red box. Other options include sending log messages to a syslog server, enabling logging for reports, using an alternate DNS server, enabling communication VLAN tagging, and enabling deployment over wireless.

Automatically update WatchGuard AP firmware when a new version is available on the Firebox

Send WatchGuard AP log messages to a syslog server  
Syslog server IP address

Enable logging for reports (Fireware OS v11.10 and higher)

Use alternate DNS server for non-DHCP WatchGuard Access Points (Fireware OS v11.11 and higher)  
DNS Server IP Address

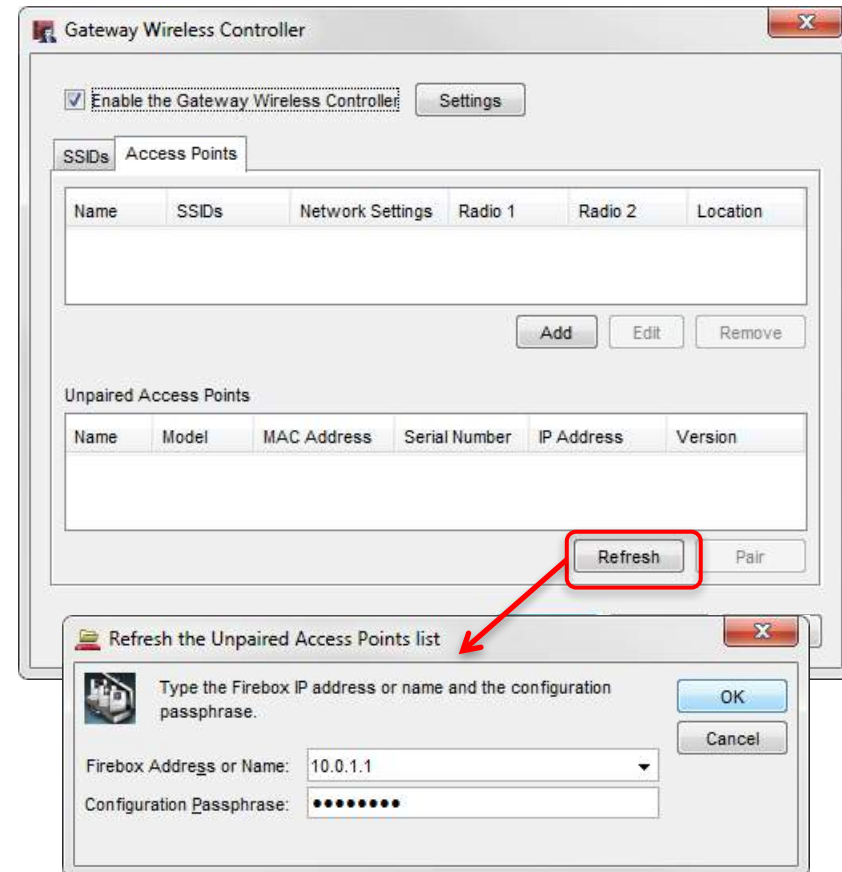
Enable Communication VLAN tagging  
Communication VLAN

Advanced Deployment  
 Enable deployment over wireless (Fireware OS v11.12 and higher)



# Pairing

- Einbindung eines Accesspoints:
  1. **Network > Gateway Wireless Controller.**
  2. Auswahl **Access Points.**
  3. **Refresh.**
  4. Eingabe von Kennwort und IP der Firebox.
    - Firebox versendet einen Broadcast auf UDP port 2529 (alle 30 Sekunden) um noch nicht eingebundene Accesspoints zu ermitteln.

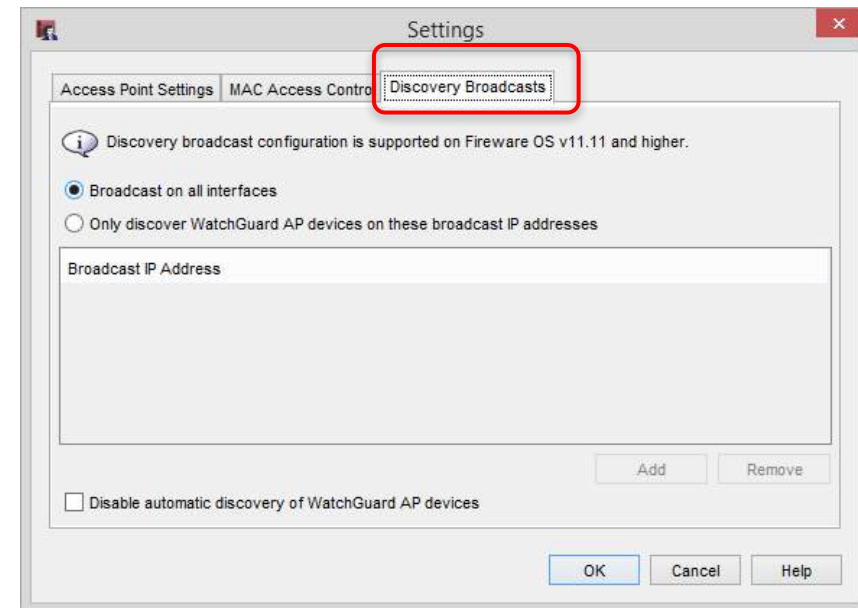


# Discovery Broadcasts

- Der Gateway Wireless Controller nutzt einen UDP Broadcast auf allen lokal verfügbaren Netzwerken um neue Accesspoints zu ermitteln.
- Der Discovery Broadcast kann eingeschränkt werden auf spezielle Netzwerke oder gänzlich unterbunden werden.
  - Nützlich bei Verwendung von “automatic deployment”
  - Es ist nicht empfohlen die Funktion zu deaktivieren, wenn Accesspoints wechselnde DHCP Adressen erhalten.
    - Es könnte sonst zu Kommunikationsverlust zwischen Accesspoints und GWC kommen.

# Discovery Broadcasts

- Einschränkungen des **Discovery Broadcasts** können definiert werden
  - Hinzufügen eines Broadcast Network.
  - Z.B. ist für das Netzwerk 10.0.0.1/24, die Broadcast IP 10.0.0.255 einzutragen.
  - Zusätzlich kann “automatic discovery” deaktiviert werden
    - Neue Accesspoints müssen dann manuell über **Refresh** im **GWC Access Points** Menu erkannt werden



# Pairing

- Wird die Konfiguration nach einem Pairing Vorgang gespeichert:
  - Die Firebox nutzt das Management Passphrase zur Verbindung zum Accesspoint.
  - Die Firebox sendet die Konfiguration an den AP.
  - Die Firebox aktiviert den Accesspoint online
    - Benötigt Port 443 Zugriff zu WatchGuard
    - Der Aktivierungsstatus wirkt sich nicht auf die AP Funktionalität aus
  - Der Accesspoint rebootet.

# Hinweis für AP120/AP320/AP322/AP420

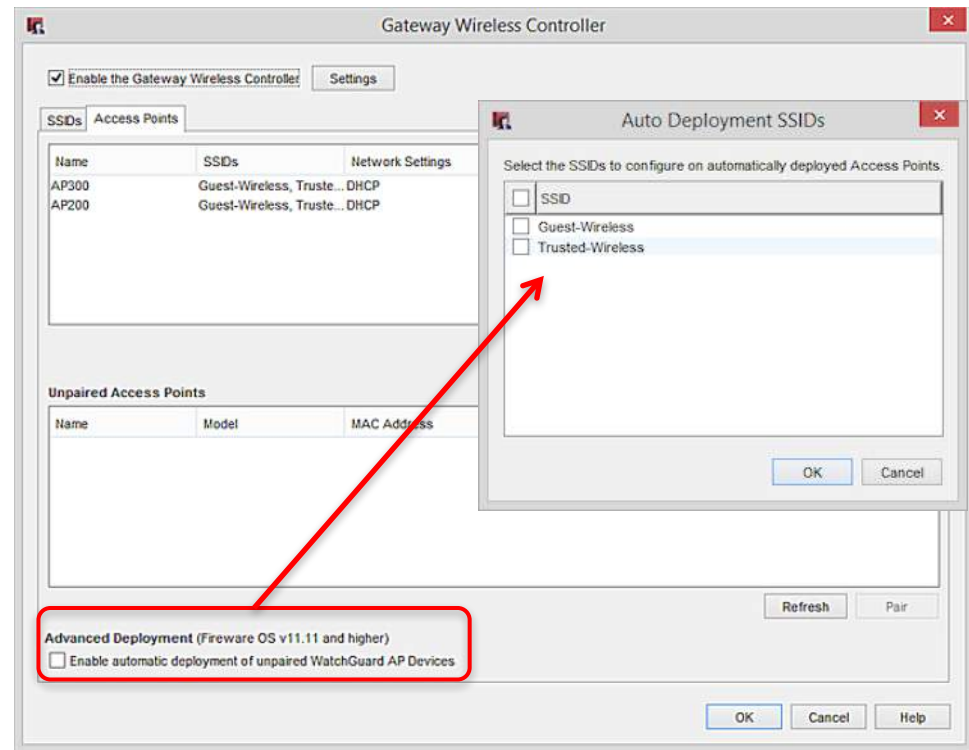
- AP120, AP320, AP322 und AP420 Systeme bauen im Factory-Default zunächst eine Verbindung zur WatchGuard Wi-Fi Cloud auf
  - Auch wenn ein AP nicht für die Wi-Fi Cloud aktiviert ist, versucht er wenige Minuten diese zu erreichen.
  - Nach dem Timeout ist der Accesspoint bereit für das lokale Pairing mit dem GWC der Firebox
  - Tipp: Blockieren Sie den Zugriff aus dem “Deployment Netz” zur Wi-Fi Cloud um den Vorgang zu beschleunigen.
- Nach einem erfolgreichen Pairing versucht der Accesspoint nicht mehr die Wi-Fi Cloud zu erreichen.

# AP120/AP320/AP322/AP420 Limitierungen

- Folgende Funktionen sind für per GWC verwaltete AP120 / AP320 / AP322 / AP420 nicht verfügbar:
  - LED controls
  - Fast Handover
  - Client limits
  - External syslog support
  - Local Web UI access
  - AP420 third scanning radio

# Automatic Deployment

- Für Umgebungen mit einer großen Anzahl Accesspoints, die die gleiche(n) SSID(s) nutzen werden.
- Konfiguration:
  - Aktivierung der Funktion in den GWC Einstellungen.
  - Auswahl der SSIDs für automatic deployment.



# Trust Store

- Der Trust Store gewährleistet, dass keine Konfigurationen mit “nicht vertrauenswürdigen” Accesspoints synchronisiert werden
  - z.B. bei nicht autorisiertem Factory Default oder bei kompromitierten Accesspoints.
- Für jeden verwalteten Accesspoint wird IP-bezogen ein Trust-Record erzeugt
  - Gateway Wireless Controller kommuniziert nicht mit Accesspoints ohne Trust-Record
  - Die WLAN Funktion von Accesspoints ist unabhängig vom Trust-Store Status
- **Empfehlung: DHCP Reservierungen oder statische IP Adressen sollten für Accesspoints genutzt werden um den Trust Store effektiv zu nutzen.**



# AP Device Trust Store

- Alle Accesspoints ohne Trust-Record werden als **Not Trusted** im Gateway Wireless Controller dargestellt.

Gateway Wireless Controller

Summary Maps Access Points Wireless Clients Foreign BSSIDs

ACTION ▾

<input type="checkbox"/>	NAME	STATUS	BYTES ▾	USER	SSIDS	IP ADDRESS	RADIO 1	RADIO 2	VERS	MODE	UPTIME
<input type="checkbox"/>	AP120_M001174	Online	0 KB	0	AutoDeploy	10.0.5.128	2.4G: 1 (	5G: 36 +	8.0.54	AP120	1 day 02:
<input type="checkbox"/>	AP200_20AP027	Online	51 KB	1	AutoDeploy	10.0.8.129	2.4G: 9 (	5G: 100 ·	1.2.9.1	AP200	27 days 2
<input type="checkbox"/>	AP300	Not Trusted	0 KB	0	linker 2, linker 1, linker	10.0.8.144		5G: 116 ·	2.0.0.6	AP300	0 days 07

# AP Device Trust Store

- Um den Trust-Record zu erzeugen:
  - Auswahl eines oder mehrere Accesspoints
  - Auswahl von **Action** und **Mark Trusted**
  - Der Accesspoint verändert den Status von **Not Trusted** zu **Online**

The screenshot displays the 'Gateway Wireless Controller' interface. At the top, there are three tabs: 'Summary', 'Maps', and 'Access Points'. Below the tabs is an 'ACTION' dropdown menu. The menu options are: Site Survey, Log Messages, Network Statistics, Flash Power LED, Restart Wireless, Reboot, Upgrade, **Mark Trusted** (highlighted with a red box), and Show Password. To the right of the menu, there is a table with columns for 'STATUS' and 'BYTES'. The table shows three rows of data:

STATUS	BYTES
ne	959 KB
ne	439 KB
ne	0 KB

# Reset Trust Store

- Bei Verdacht einer Kompromittierung
  - Der Trust Store kann nur global zurückgesetzt werden.
  - Vertrauenswürdige Accesspoints müssen erneut in Trust Store aufgenommen werden.
  
- Eine generelle Deaktivierung des Trust Store ist ebenfalls möglich.

Enable the Gateway Wireless Controller

Access Points | **SSIDs** | Settings | Notification

### Deployment Security Settings

The WatchGuard Gateway Wireless Controller automatically generates a strong and unique passphrase for each WatchGuard AP Device. If you prefer to use your own global passphrase, you can manually specify a passphrase.

Use a manual global passphrase instead of automatically-generated unique passphrases for WatchGuard AP Devices

Global AP Passphrase

Show passphrase

The WatchGuard Gateway Wireless Controller uses a Trust Store that includes digital certificates to verify the authenticity of each deployed WatchGuard AP Device. If you believe any of your AP Devices have been tampered with or are no longer under your control, you can manually reset the Trust Store on the Gateway Wireless Controller.

**RESET TRUST STORE**

Disable the Trust Store mechanism and trust all WatchGuard AP Devices

Detail

Access Points | **Wireless Clients** | Foreign BSSIDs

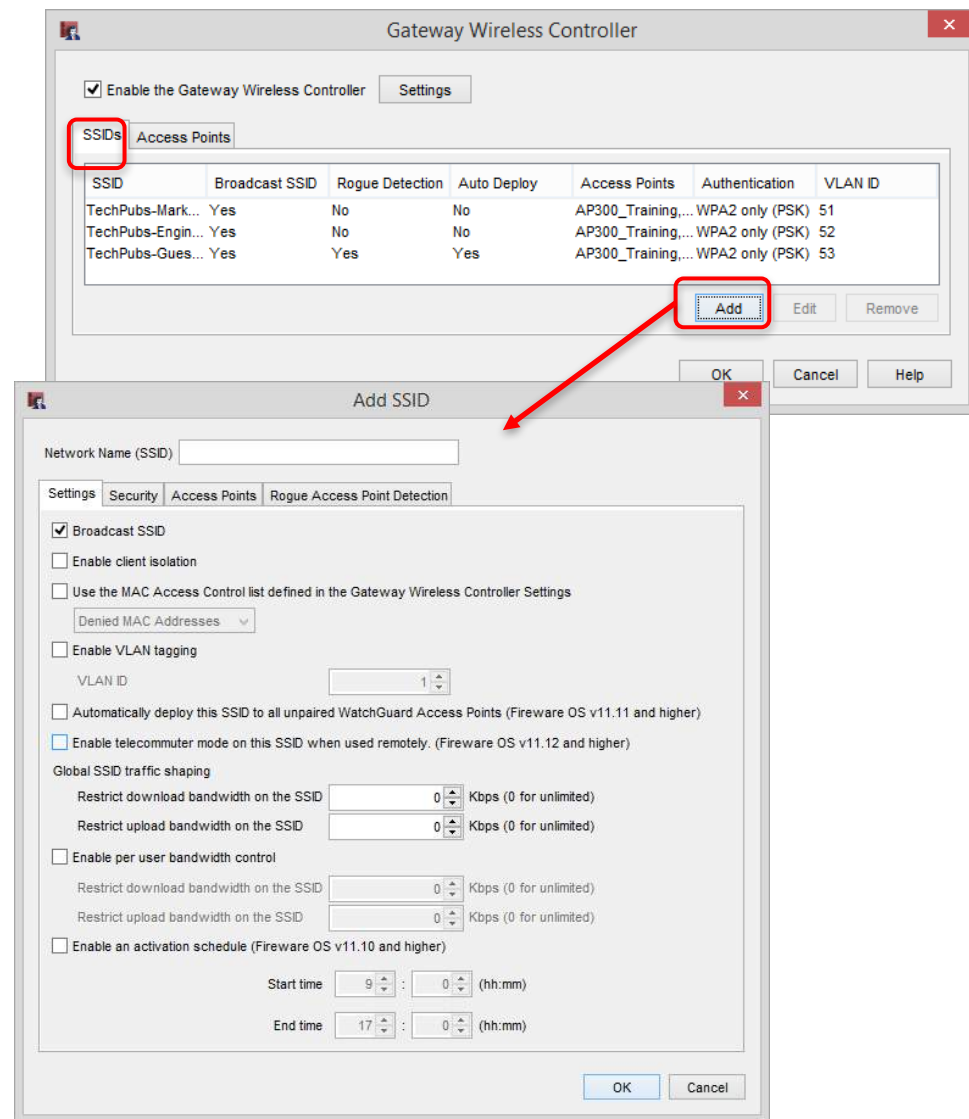
Name	Status	Bytes	Clients	SSIDs	IP Address	Port
AP200_Sales	Online	0 KB	0	TechPubs-Marketing-WiFi, TechPubs-Engineering-WiFi, TechPubs-GuestNet-WiFi	10.0.50.210	
AP300_Training	Online	0 KB	0	TechPubs-Marketing-WiFi, TechPubs-Engineering-WiFi, TechPubs-GuestNet-WiFi	10.0.50.220	

Trust Store: **Reset** ⓘ

Refresh Interval: 30 seconds

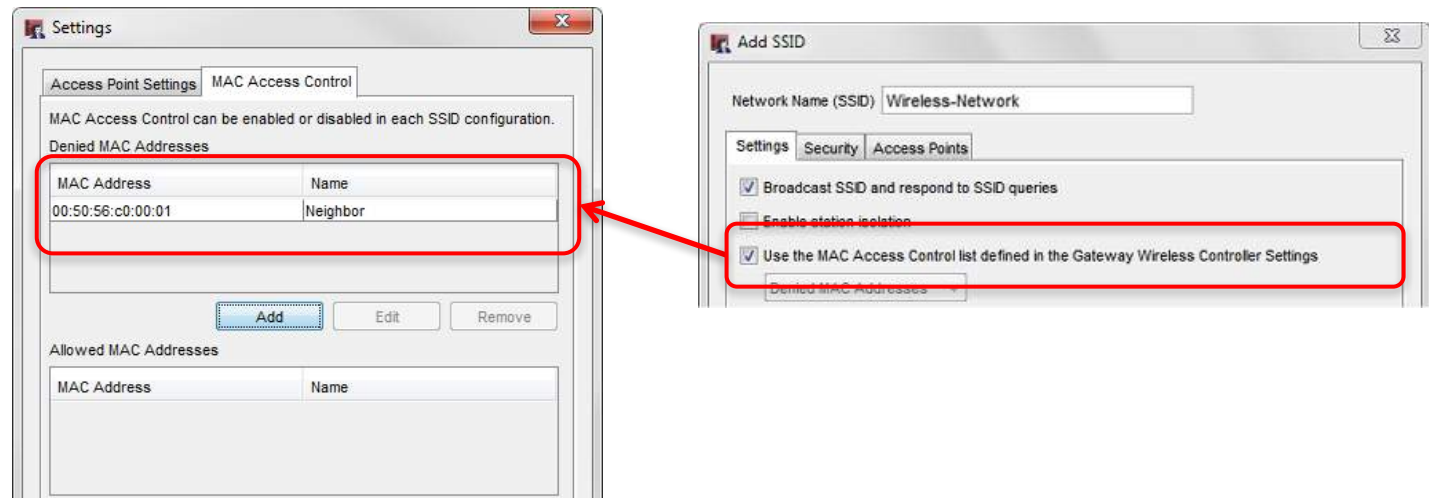
# Konfiguration der SSIDs

- Verwaltung der SSIDs erfolgt im Gateway Wireless Controller.
  - Roaming ist unterstützt durch Zuweisung der SSID zu mehreren Accesspoints und Radio Modulen.
- Hinzufügen einer neuen SSID über **Add**.



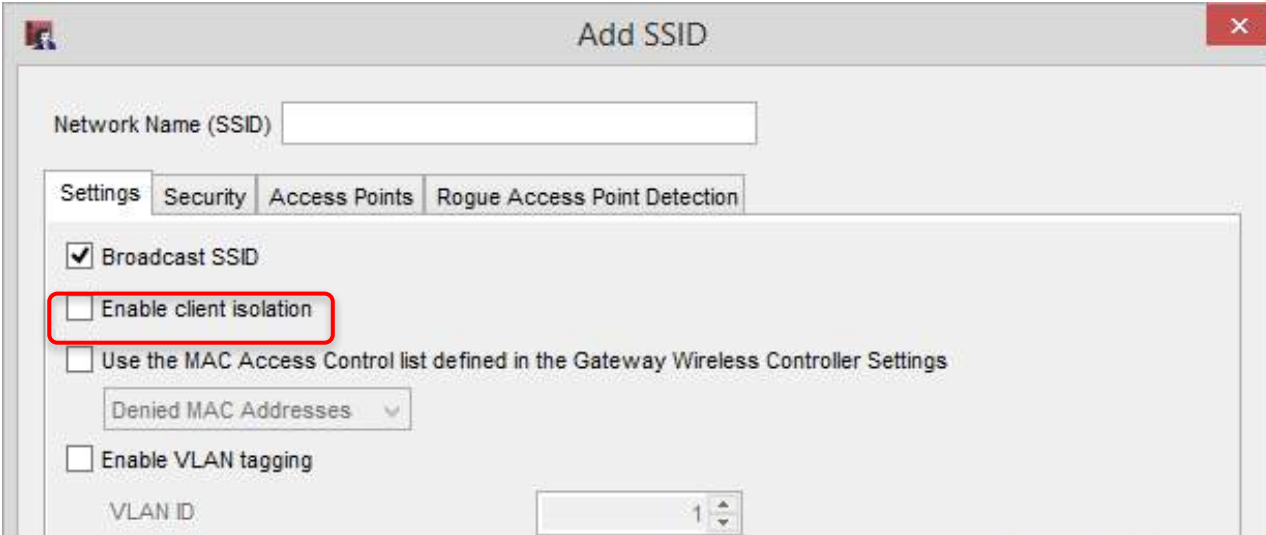
# MAC Access Control

- Die MAC Access Control Listen werden in den globalen Gateway Wireless Controller Einstellungen definiert.
- Für eine SSID kann die Funktion anschließend aktiviert und eine anwendbare Liste ausgewählt werden:
  - Denied MAC Addresses oder Allowed MAC Addresses



# Client Isolation

- Client Isolation
  - Mit Client Isolation wird die direkte Kommunikation zwischen Wi-Fi Clients innerhalb einer SSID des elben Radio-Moduls unterbunden.
  - Empfohlen für Gast-Netze und andere Bereiche in denen Clients isoliert sein sollen.



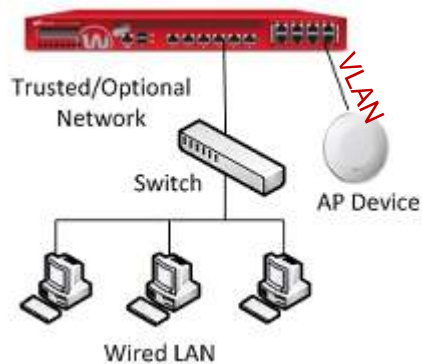
The screenshot shows the 'Add SSID' configuration window. The 'Settings' tab is active, and the 'Enable client isolation' checkbox is highlighted with a red box. Other visible options include 'Broadcast SSID' (checked), 'Use the MAC Access Control list defined in the Gateway Wireless Controller Settings' (unchecked), and 'Enable VLAN tagging' (unchecked). A 'Denied MAC Addresses' dropdown menu and a 'VLAN ID' spinner are also visible.



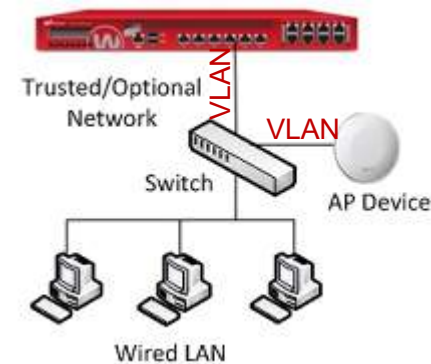
# Accesspoints & VLANs

# Accesspoints & VLANs

- Zwei gängige Szenarien werden unterstützt:
  - Direkte Verbindung der Accesspoints an einem VLAN Interface der Firebox.
  - Zwischen Accesspoints & Firebox werden VLAN fähige Switche verwendet.
- Bei Verwendung von Switchen müssen die VLANs eingerichtet und als tagged/untagged dem Switchport zugewiesen werden.



OR





# VLAN Konfiguration Firebox

The image displays three overlapping screenshots of the WatchGuard Firebox configuration interface, showing the configuration for three different VLANs. Each window has tabs for IPv4, IPv6, and Secondary.

**Edit VLAN: AP-Mgmt-VLAN**

- Name (Alias): AP-Mgmt-VLAN
- Description: VLAN for AP Mgmt
- VLAN ID: 30
- Security Zone: Trusted
- IP Address: 10.0.30.1/24
- Disable DHCP
- Use DHCP Server
- You can configure a maximum of six address ranges.
- Address Pool:
 

Starting IP	Ending IP
10.0.30.2	

**Edit VLAN: Guest-VLAN**

- Name (Alias): Guest-VLAN
- Description: VLAN for AP SSID Guest-W
- VLAN ID: 20
- Security Zone: Custom
- IP Address: 10.0.20.1/24
- Disable DHCP
- Use DHCP Server
- You can configure a maximum of six address ranges.
- Address Pool:
 

Starting IP	Ending IP
10.0.20.2	

**Edit VLAN: Trusted-VLAN**

- Name (Alias): Trusted-VLAN
- Description: VLAN for Trusted
- VLAN ID: 10
- Security Zone: Trusted
- IP Address: 10.0.10.1/24
- Disable DHCP
- Use DHCP Server
- You can configure a maximum of six address ranges.
- Address Pool:
 

Starting IP	Ending IP
10.0.10.2	10.0.10.100

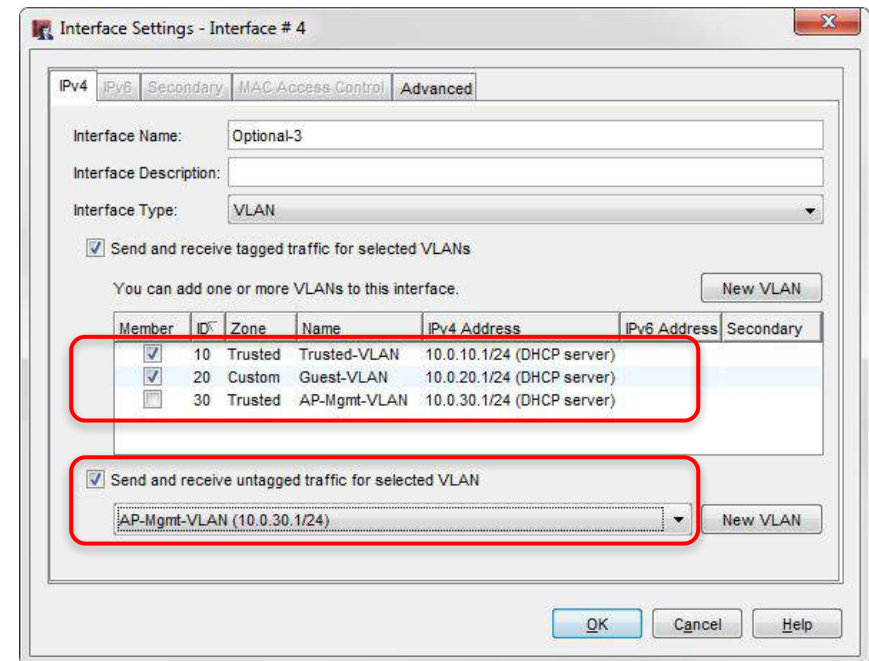
VLAN ID 30

VLAN ID 20

VLAN ID 10

# VLAN Interface - Firebox

- Konfiguration des VLAN Interface.
  - **Interface Type** VLAN muss in der Network Konfiguration eingerichtet werden.
    - Send and receive **tagged** traffic for the VLANs for each SSID (VLAN IDs 10 and 20).
    - Send and received **untagged** traffic for the VLAN for AP management connections (VLAN ID 30).
  - Speichern der Konfiguration
  - Anschließen des Accesspoints oder Switch-Uplinks an den Firebox Port



A detailed illustration of a lion, colored in a monochromatic red hue. The lion is shown in profile, facing right, with its head slightly lowered. It has a thick, textured mane and a focused expression. The background is plain white.

# Monitoring der Accesspoints

# Monitor APs in Firebox System Manager

## Übersicht der Access Points:

- AP name
- AP device status
- SSIDs
- IP address
- Radio band & channel
- Firmware version
- AP model
- Activation status
- Uptime

Firebox System Manager - 192.168.43.144 [Connected]

File View Tools Help

Front Panel | Traffic Monitor | Bandwidth Meter | Service Watch | Status Report  
 Authentication List | Blocked Sites | Subscription Services | Gateway Wireless Controller | Traffic Management

Summary

Online Access Points: 3      Available SSIDs: 2  
 Offline Access Points: 0      Connected Clients: 0

WAP Firmware Available

AP100: 1.2.9.1AP102: 1.2.9.1      AP200: 1.2.9.1

Detail

Access Points | **Wireless Clients**

Name	Status	SSIDs	IP Addr...	Radio1	Radio2	Version	Model	LiveSecu...	Uptime
AP100_10AP02736...	Online	Wireless1	10.0.30.2	5G: 60 + 64 (3 ...		1.2.9.1	AP100	Activated	29d 20h 38m ...
AP200_20AP0275A...	Online	Trusted-Wireless, Wire...	10.0.50.2	2.4G: 1 (3 dBm)	5G: 44 + 48 (3 ...	1.2.9.1	AP200	Activated	13d 3h 16m 56s
AP100_10AP02731...	Online	Trusted-Wireless	10.0.40.2	2.4G: 11 (3 dBm)		1.2.9.1	AP100	Activated	29d 2h 38m 49s

# AP Device Status — Unreachable

- Kann die Firebox einen Accesspoint nicht erreichen/kontaktieren so ist der Status **Unreachable**.
- Bei Reboot des Accesspoints ist temporär der Status **Unreachable** dargestellt.

Detail

Access Points Wireless Clients Foreign BSSIDs

Name	Status	Bytes	Clients	SSIDs	IP Address
AP200_Sales	Unreachable	0 KB	0	TechPubs-Marketing-WiFi, TechPubs-Engineering-WiFi, TechPubs-GuestNet-WiFi	10.0.50.2
AP300_Training	Unreachable	0 KB	0	TechPubs-Marketing-WiFi, TechPubs-Engineering-WiFi, TechPubs-GuestNet-WiFi	10.0.50.2

# AP Status — Not Trusted

- Accesspoints ohne Trust-Record werden als **Not Trusted** dargestellt.
- Alle Accesspoints sollten dem Trust-Store hinzugefügt werden (wenn diese Funktion genutzt wird)

Gateway Wireless Controller

Summary Maps Access Points Wireless Clients Foreign BSSIDs

ACTION ▾

	NAME	STATUS	BYTES	USER	SSIDS	IP ADDRESS	RADIO 1	RADIO 2	VERS	MODE	UPTIME
<input type="checkbox"/>	AP120_M001174	Online	0 KB	0	AutoDeploy	10.0.5.128	2.4G: 1 (	5G: 36 +	8.0.54	AP120	1 day 02:
<input type="checkbox"/>	AP200_20AP027	Online	51 KB	1	AutoDeploy	10.0.8.129	2.4G: 9 (	5G: 100 ·	1.2.9.1	AP200	27 days 2
<input type="checkbox"/>	AP300	Not Trusted	0 KB	0	linker 2, linker 1, linker	10.0.8.144		5G: 116 ·	2.0.0.6	AP300	0 days 07

# AP Status — Authenticating

- **Authenticating** bedeutet, dass ein Anmeldeversuch von Accesspoint und Gateway Wireless Controller stattfindet.
- Sollte der Status **Authenticating** nicht in wenigen Minuten auf **Online** wechseln, liegt ggf. ein Passphrase Mismatch vor
  - Lösen eines solchen Problems (sollte das Passphrase unbekannt sein):
    - Löschen des Accesspoints über den Gateway Wireless Controller
    - Manueller Factory Default des Accesspoints.
    - Erneute Aufnahme des Accesspoints per Discover und Pairing.

# Monitoring — Connected Wireless Clients

- Informationen über **Wireless Clients** werden dargestellt:
  - Host name and IP address if DHCP enabled
  - MAC Address
  - The SSID, AP, and radio the client is connected to
  - Data sent and received through the AP device
  - Signal strength
  - Last activity
  - Client PHY Mode indicates b, g, a, n, n40, ac80, etc.
  - Location derived from AP device client is connected to

The screenshot shows the Firebox System Manager interface for IP 10.138.109.51. The 'Wireless Clients' tab is selected in the 'Detail' section. The interface displays the following information:

**Summary:**  
 Access Points: 3 (0 Unreachable)  
 Available SSIDs: 2  
 Connected Clients: 5  
 Bytes Sent/Received: 1 MB / 177 KB

**WAP Firmware Available:**  
 AP100: 1.2.9.11 build-170118 (5b39d5a3)  
 AP200: 1.2.9.11 build-170118 (5b39d5a3)  
 AP320: 8.0.564

**Detail - Wireless Clients:**

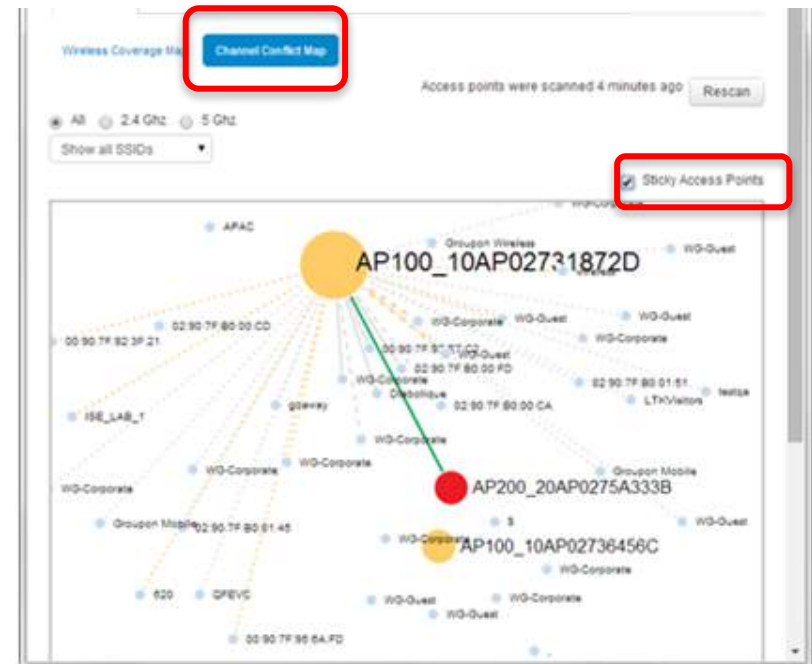
Filter By AP	Filter By SSID	Hostname	IP Address	Client	Sent	Received	Signal	SSID	Access Point	Radio	Last Activity	Mode	Location
AP	All	LAP-53982	172.16.200.192	60:57:18:A2:62:23	828 KB	40 KB		WG-Guest	AP100_10AP02FEFDA1B	1 (11)	0d 0h 0m 0s	N	5th Floor

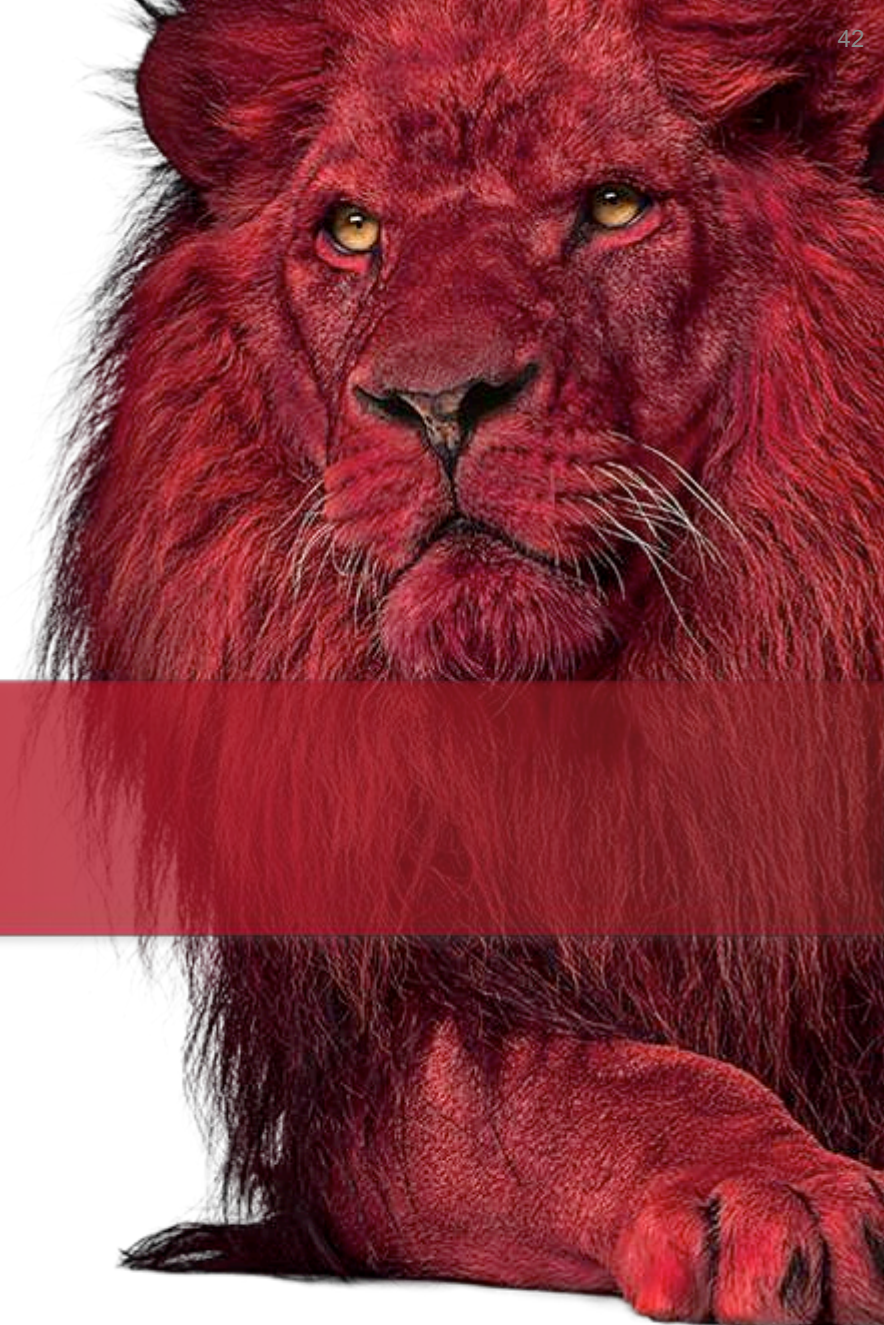
Refresh Interval: 30 seconds | Pause



# Gateway Wireless Controller Maps

- **Channel Conflict Map**
  - Stellt die Verteilung der Accesspoints visuell dar
  - Weitere Details können per Rechtsklick und **View Details** eingesehen werden.
- Automatische Verteilung der APs anhand der Signalstärke.
  - **Sticky Access Points** ermöglicht eine manuelle Positionierung auf dem Dashboard.





# Live Demo



**Vielen Dank!**

***NOTHING GETS  
PAST RED.***



**WatchGuard Training**

Copyright ©2017 WatchGuard Technologies, Inc. All Rights Reserved