



Best Practices – Wi-Fi Cloud

Jonas Spieckermann
Senior Sales Engineer

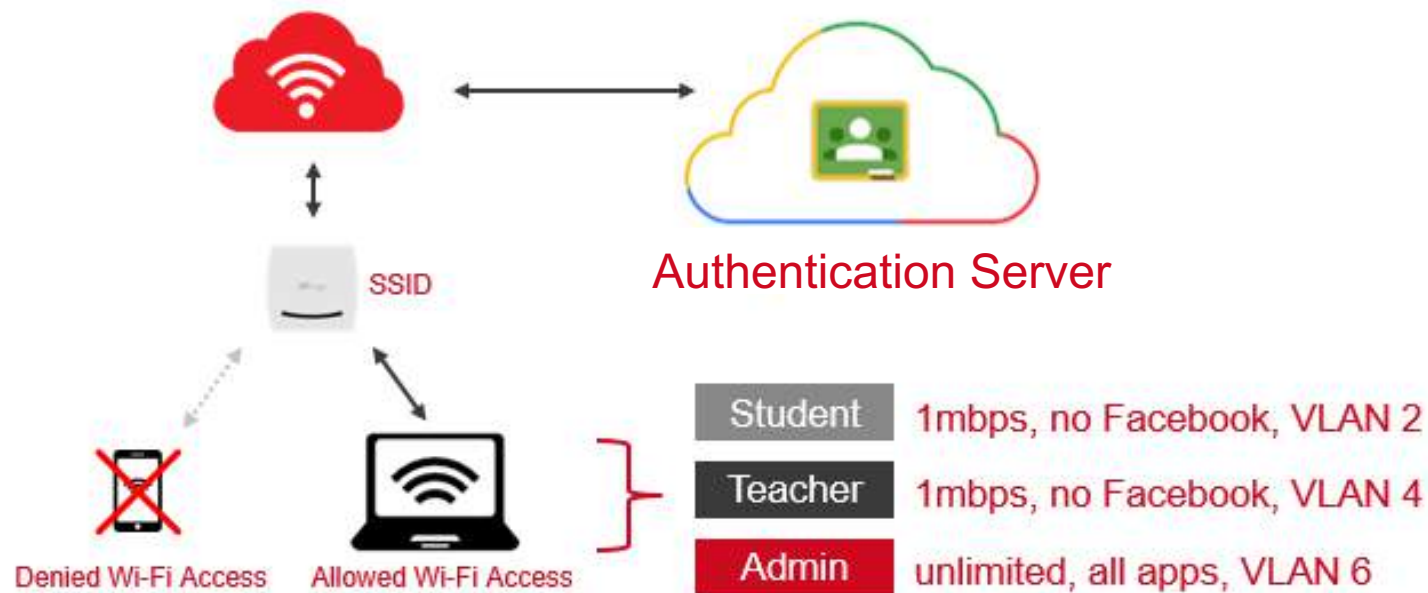
Jonas.Spieckermann@watchguard.com

Mit Rolebased Control WLAN-Zugriffsrichtlinien bei gleichbleibender SSID definieren



Grundlage

- Authentifizierung der User/Clients
- Zuweisung von Rollen / Zugriffsprofilen



Role-Based Control

- Um Einschränkungen für Benutzer und Clients durchzusetzen, können spezifische Zugriffs-Regeln in Rollen festgelegt werden.
- Eine oder mehrere Rollen können authentifizierten Usern und Clients zugeordnet werden.
- Bei der Anmeldung an einer SSID, authentifiziert sich der Benutzer per RADIUS oder Google Authentication. Basierend auf den eingerichteten Regeln wird die festgelegte Rolle der User Session zugewiesen.
- Die Rollenzuweisung erfolgt über:
 - 802.1x VSA (Vendor Specific Attribute)
 - Google OU

Role Profiles

- Ein Role Profile ermöglicht Einschränkungen durch die folgenden Funktionen:
 - VLAN access
 - Firewall rules
 - Bandwidth control for each user
 - Redirection portal URL and Walled Garden sites

Schritt 1: Definition Role Profiles

- Role Profiles werden in **Configuration > Device Configuration > Role Profiles** festgelegt

Add Role Profile

Profile Name: Role: Inherit From SSID:

VLAN

VLAN
VLAN ID:

Firewall

Enable Firewall
[Add New Rule](#)

Rule Name: Host: Port:
Action: Protocol: Direction: [Delete](#)

Application Firewall
Default Rule:

Bandwidth

Enable per user bandwidth control
Restrict user upload bandwidth to: [0 - 1024]
Restrict user download bandwidth to: [0 - 1024]

Redirection Redirection - Disabled

Schritt 2: Role-Based Control Aktivierung

- Aktivierung erfolgt in SSID profile über **Enable Role Based Control**
- **Add New Rule** ermöglicht die Entscheidung ob 802.1x VSA, oder Google Authentication genutzt werden
 - Google OU kann nicht mit VSA Rules kombiniert werden

▼ Role Based Control

One or more role profiles defined under Device Configuration > Role Profiles can be associated with specific Mojo/Custom VSA rules or Google OU rules to enforce restrictions on c rules, ensure that Secondary Authentication is enabled and Google Device Authorization is selected under the Security section. For Mojo/Custom VSA rules, ensure that the Security Mixed mode" and "802.1x" is selected.

▪ Enable Role Based Control



Role Based Control is supported only on 802.11ac platforms. This setting is ignored on 802.11n platforms.

[Add New Rule](#)



Rules are compared from top to bottom till the first match. Drag rules to reorder. You can add either Google OU rules or a combination of Mojo VSA and Custom VSA rules.

Role-Based Control — Wi-Fi Cloud / Custom

- Für RADIUS VSA Rules muss in der **Security** des SSID Profile folgendes definiert sein:
 - Security Mode — **WPA2** or **WPA and WPA2 Mixed mode**
 - Security option — **802.1X**

Add Wi-Fi Profile

WLAN Hotspot 2.0

Profile Name WatchGuard SSID WatchGuard

Broadcast SSID Application Visibility Association Analytics

Security


Security Mode WPA2

PSK 802.1X


Add Rule — 802.1x VSA

- Die Festlegung der RADIUS Attribute zu konfigurierten Roles wird im **Select Role** drop-down Menu durchgeführt:
 - **Use Role Name**
 - Die Namensgebung für RADIUS Attribut oder Google OU ist identisch zu den Namen der Role Profiles
 - **Custom Role Name**
 - Abweichungen des RADIUS Attributs oder der Google OU zu den verwendeten Namen Role Profiles sind möglich.

▪ **Enable Role Based Control**

 Role Based Control is supported only on 802.11ac platforms. This setting is ignored on 802.11n platforms.

[Add New Rule](#)

 Rules are compared from top to bottom till the first match. Drag rules to reorder. You can add either Google OU rules or a combination of Mojo VSA and Custom VSA rules.

802.1x Mojo VSA	Vendor Id <input type="text" value="16901"/>	Attribute Id <input type="text" value="7"/>
Select Role <input type="text"/>	Role <input type="text"/>	Enter Name <input type="text"/>

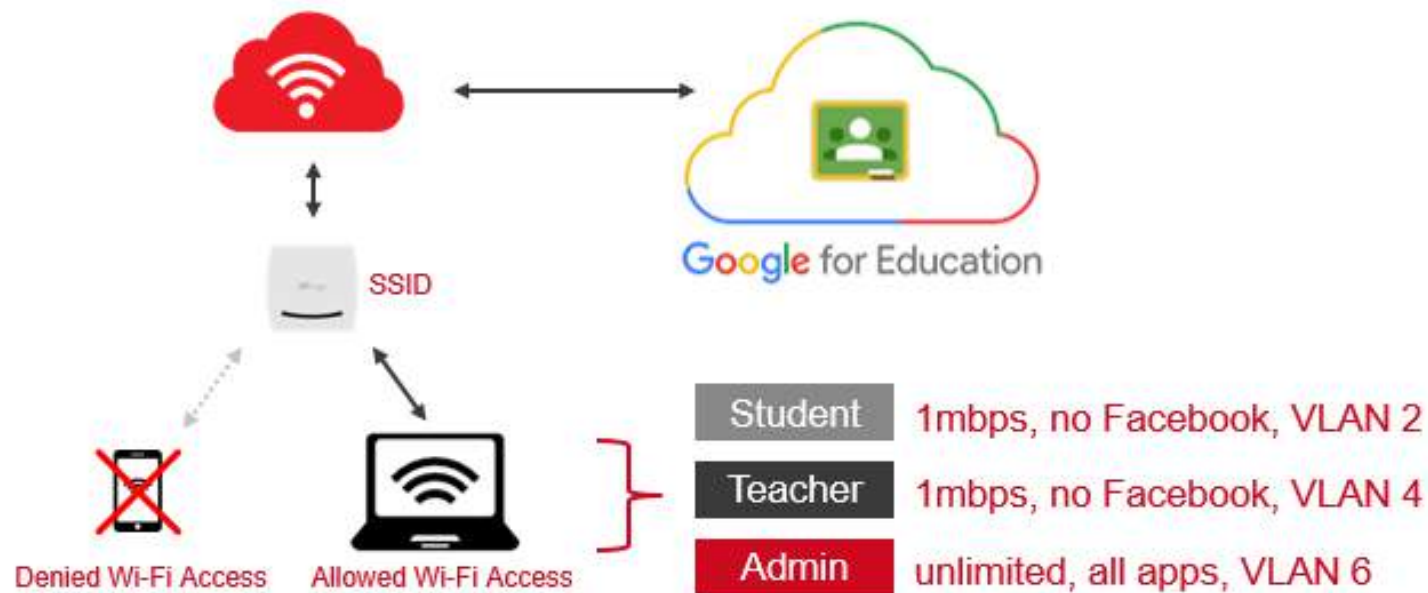
[Delete](#)

Google Integration and Device Authorization

- Google stellt für Unternehmen und Bildungseinrichtungen einen Authentifizierungs-Service zur Verfügung.
- Dieser ermöglicht eine Benutzer/Geräte Verwaltung und die Verwendung von Organizational Units zur Zuweisung von Einstellungen und Richtlinien (für Geräte und Benutzer)
 - *User Directory* ermöglicht single sign-on für alle Google Applikationen
 - *Device Management* ermöglicht Kontrolle über authorisierte Systeme und Zuweisung von Netzwerk-Richtlinien
- Bei der Anmeldung eines Benutzers kann die MAC Adresse des Systems zur Device Management Liste hinzugefügt werden, um spezifische Geräte zu erlauben oder zu verbieten.

Google for Education Example

- Schulen, die Google for Education nutzen, können kontrollieren welche Geräte Zugriff auf die definierten SSIDs erhalten und welche Zugriffs-Richtlinie zugewiesen wird.



Role-Based Control — Google OU

- Zur Verwendung von Google OU rules muss in den **Security** Einstellungen des SSID Profile folgendes definiert sein:
 - **Secondary Authentication**
 - **Google Device Authorization**

▼ Security

Security Mode

PSK 802.1X

Passphrase

▶ 802.11w Settings

▶ 802.11r Settings

Client Isolation

Secondary Authentication

Google Device Authorization RADIUS MAC Authentication


If the client authorization fails :

Disconnect Assign Role Select Role:


Add Rule — Google OU

- Für Google OU Rules muss der Role Name mit dem Namen der OU als **Matching OU** verknüpft werden
- Ist der Role Name identisch, so wird das Role Profile der aktiven Verbindung zugewiesen.

■ **Enable Role Based Control**

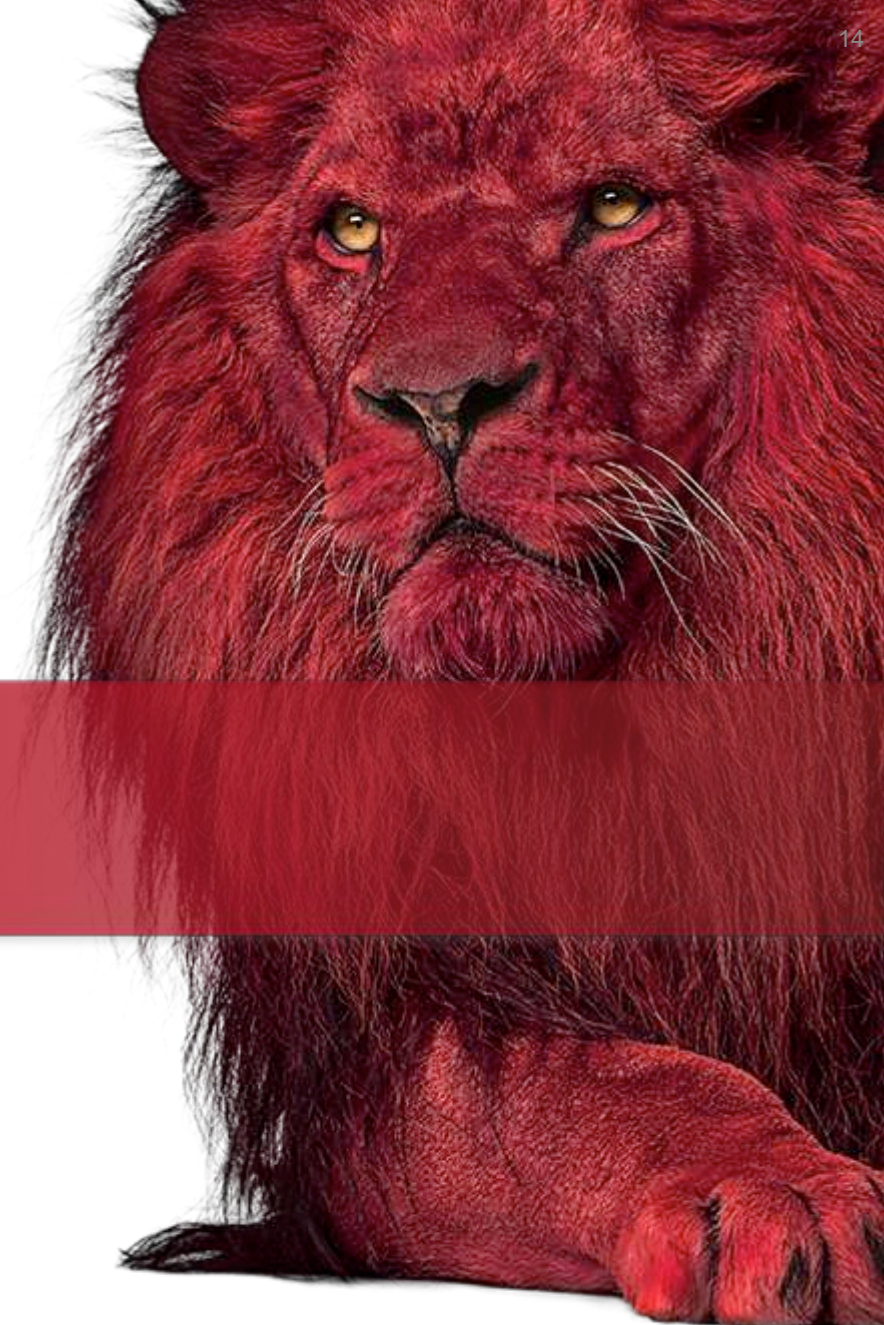
 Role Based Control is supported only on 802.11ac platforms. This setting is ignored on 802.11n platforms.

[Add New Rule](#)

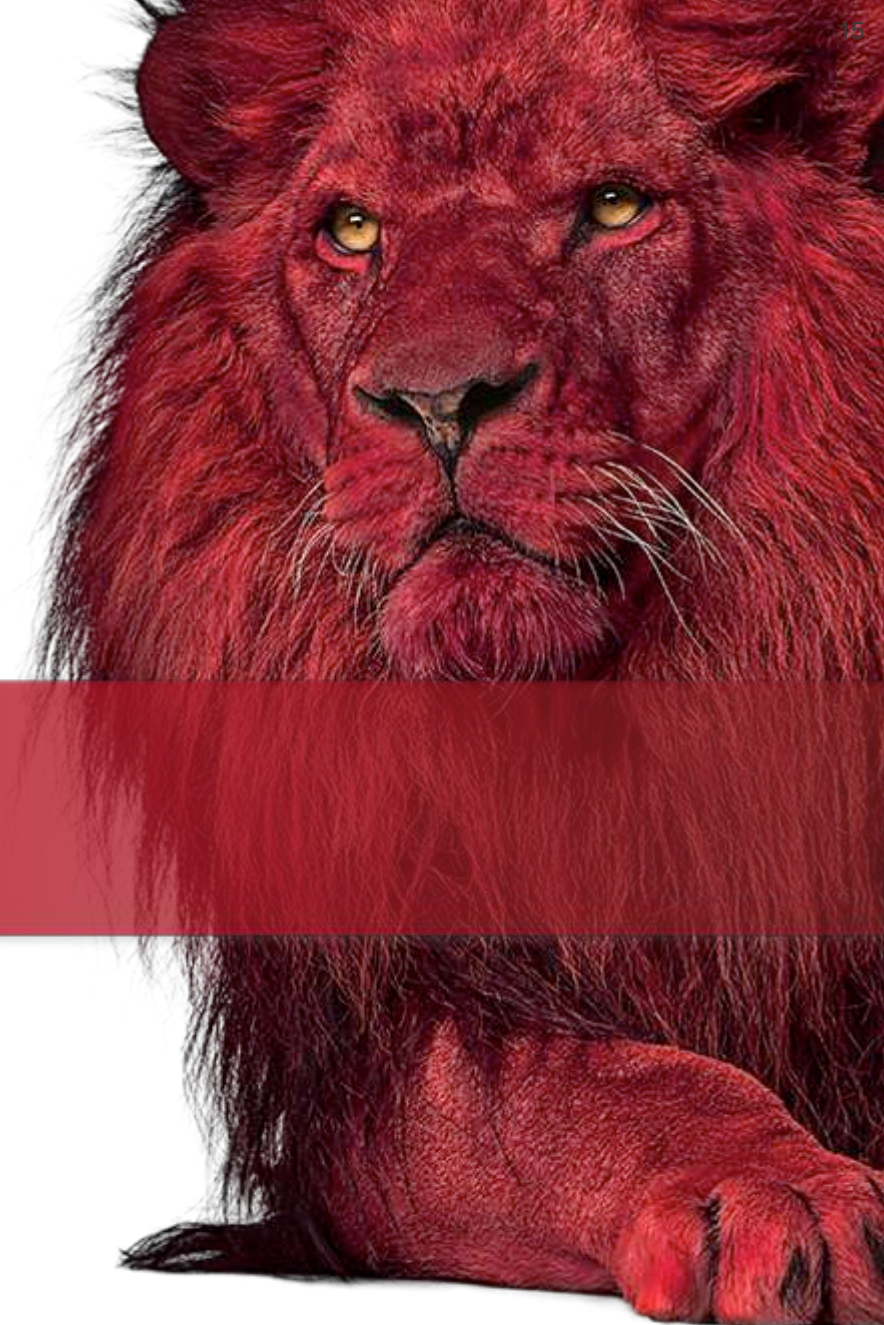
 Rules are compared from top to bottom till the first match. Drag rules to reorder. You can add either Google OU rules or a combination of Mojo VSA and Custom VSA rules.

Google OU

Select Role Role Matching OU [Delete](#)



Live Demo



Vielen Dank!

***NOTHING GETS
PAST RED.***



WatchGuard Training

Copyright ©2017 WatchGuard Technologies, Inc. All Rights Reserved