Externe Web-Authentifizierung am 9800 WLC konfigurieren und Fehlerbehebung dafür durchführen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die externe Webauthentifizierung (EWA) auf einem Catalyst 9800 Wireless LAN Controller (WLC) konfigurieren und Fehler bei dieser beheben.

Voraussetzungen

In diesem Dokument wird davon ausgegangen, dass der Webserver für die externe Kommunikation richtig konfiguriert ist und dass die Webseite ordnungsgemäß konfiguriert ist, um alle erforderlichen Parameter für den WLC zu senden, damit der Benutzer authentifiziert und Clientsitzungen in den RUN-Status verschoben werden können.

Hinweis: Da der Zugriff auf externe Ressourcen durch den WLC über Zugriffslistenberechtigungen eingeschränkt wird, müssen alle Skripte, Schriftarten, Bilder usw., die auf der Webseite verwendet werden, heruntergeladen werden und lokal auf dem Webserver verbleiben.

Die erforderlichen Parameter für die Benutzerauthentifizierung sind:

- buttonClicked: Dieser Parameter muss auf den Wert "4" gesetzt werden, damit der WLC die Aktion als Authentifizierungsversuch erkennen kann.
- redirectUrl: Der Wert in diesem Parameter wird vom Controller verwendet, um den Client bei erfolgreicher Authentifizierung an eine bestimmte Website weiterzuleiten.
- err_flag: Dieser Parameter wird verwendet, um auf Fehler hinzuweisen, z. B. unvollständige Informationen oder falsche Anmeldeinformationen. Bei erfolgreichen Authentifizierungen wird er auf "0" gesetzt.
- username: Dieser Parameter wird nur für Webauth-Parameterzuordnungen verwendet. Wenn die Parameterzuordnung auf "agree" festgelegt ist, kann sie ignoriert werden. Sie muss mit dem Benutzernamen des Wireless-Clients ausgefüllt werden.
- password: Dieser Parameter wird nur für Webauth-Parameterzuordnungen verwendet. Wenn die Parameterzuordnung auf "agree" festgelegt ist, kann sie ignoriert werden. Sie muss mit dem Kennwort des Wireless-Clients ausgefüllt werden.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Hypertext Markup Language (HTML)-Webentwicklung
- Cisco IOS®-XE Wireless-Funktionen
- Webbrowser-Entwicklungstools

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- C9800-CL WLC Cisco IOS®-XE Version 17.3.3
- Microsoft Windows Server 2012 mit Internetinformationsdienste (IIS)
- Access Points 2802 und 9117

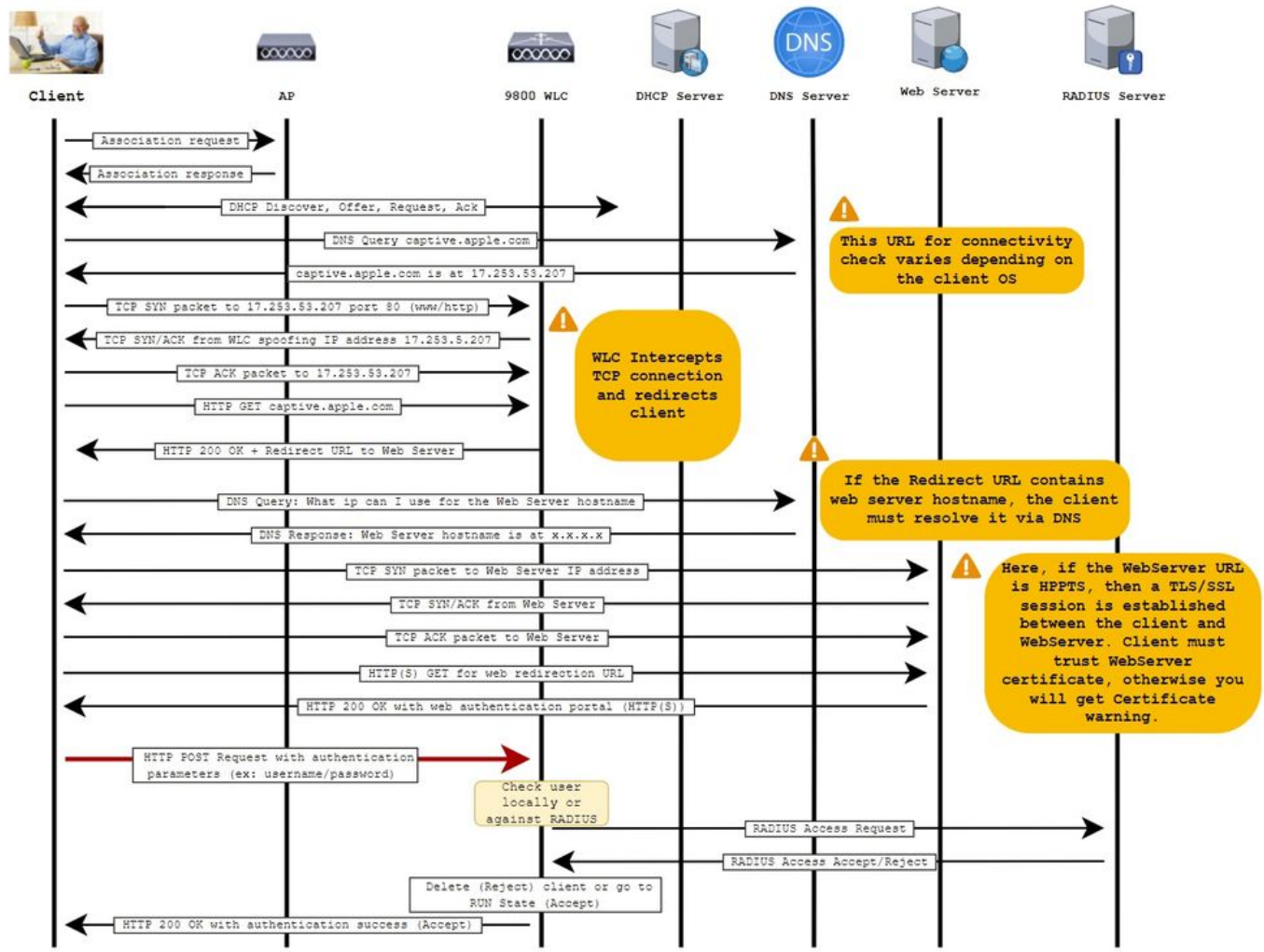
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Bei der externen Webauthentifizierung wird ein Webportal genutzt, das außerhalb von WLC auf

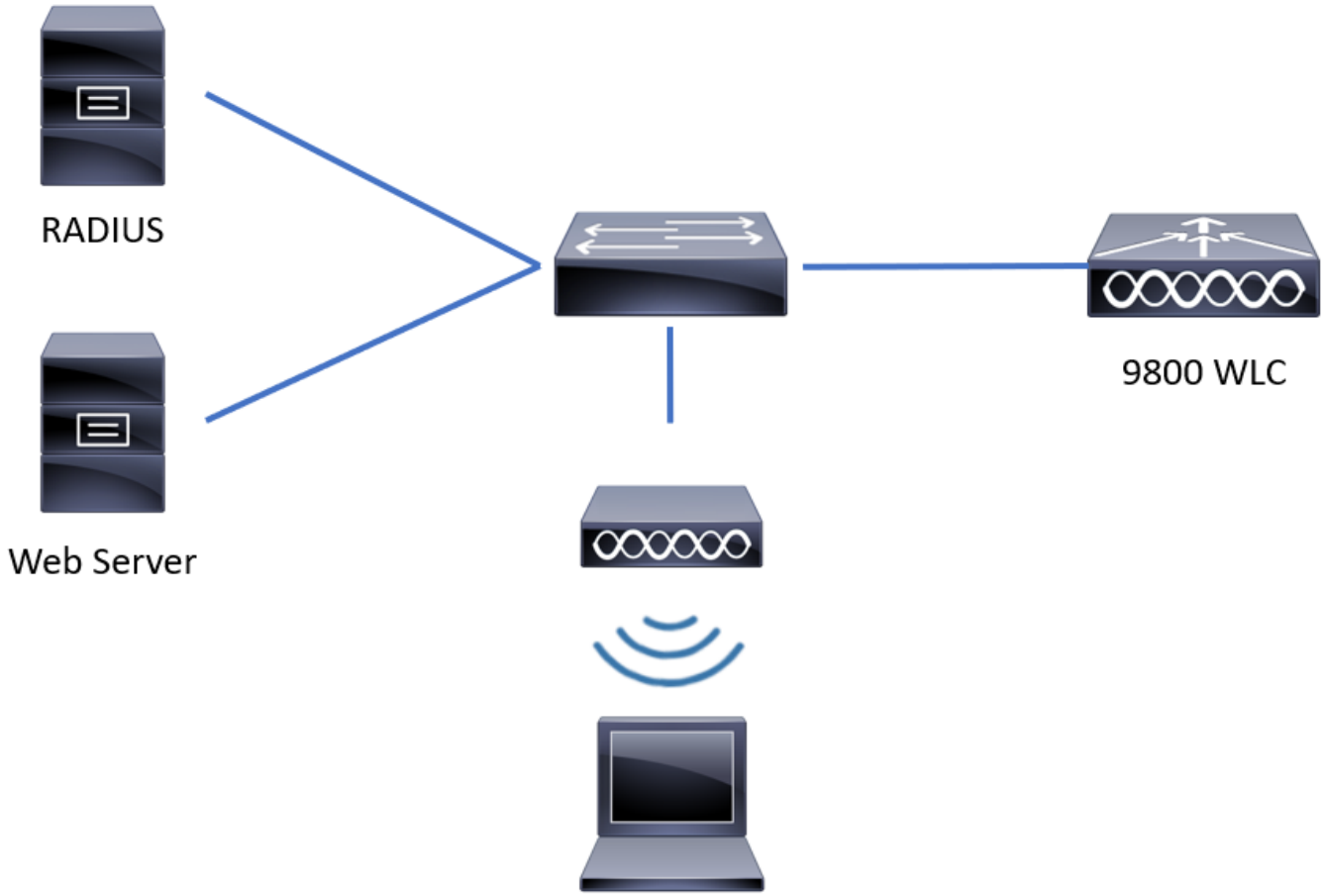
einem dedizierten Webserver oder auf Mehrzweckservern wie Identity Services Engine (ISE) gehostet wird und einen granularen Zugriff und eine präzise Verwaltung von Webkomponenten ermöglicht. Der Handshake, der erforderlich ist, um einen Client erfolgreich in ein externes Web-Authentifizierungs-WLAN zu integrieren, wird im Bild dargestellt. Das Image listet sequenzielle Interaktionen zwischen Wireless-Client, WLC, DNS-Server (Domain Name System) auf, der die URL (Uniform Resource Location) und den Webserver auflöst, auf dem WLC die Benutzeranmeldeinformationen lokal überprüft. Dieser Workflow ist hilfreich bei der Fehlerbehebung.

Hinweis: Wenn vor dem HTTP-POST-Aufruf vom Client an den WLC die sichere Web-Authentifizierung in der Parameterzuordnung aktiviert ist und der WLC keinen von einer vertrauenswürdigen Zertifizierungsstelle signierten Vertrauenspunkt hat, wird im Browser eine Sicherheitswarnung angezeigt. Der Client muss diese Warnung umgehen und das erneute Einsenden des Formulars akzeptieren, damit der Controller die Client-Sitzungen in den RUN-Status versetzen kann.



Konfigurieren

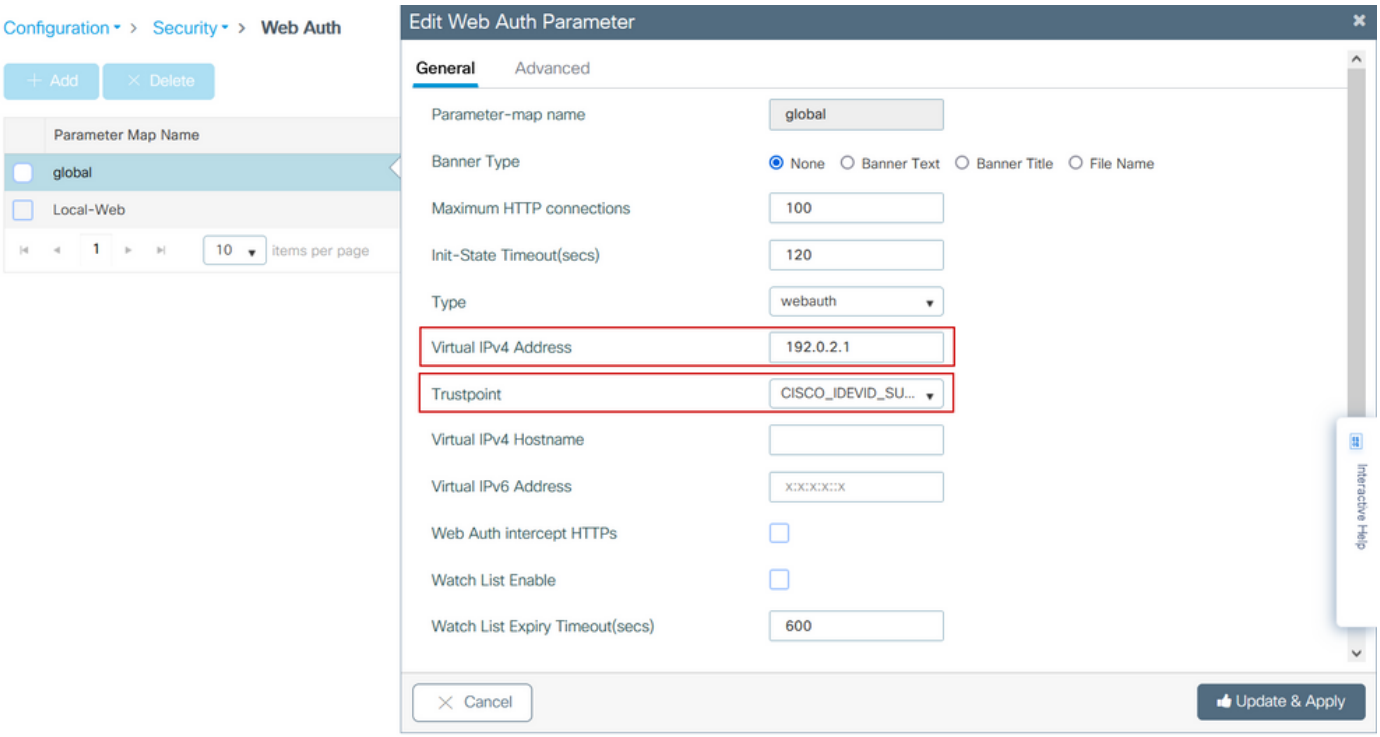
Netzwerkdiagramm



Webparametereinstellungen konfigurieren

Schritt 1: Navigieren Sie zu Configuration > Security > Web Auth, und wählen Sie die globale Parameterzuordnung aus. Vergewissern Sie sich, dass die virtuelle IPv4-Adresse und der Vertrauenspunkt konfiguriert sind, um die richtigen Umleitungsfunktionen bereitzustellen.

Hinweis: Browser verwenden standardmäßig eine HTTP-Website, um den Umleitungsprozess zu starten. Wenn eine HTTPS-Umleitung erforderlich ist, müssen Web Auth Intercept-HTTPs überprüft werden. Diese Konfiguration wird jedoch nicht empfohlen, da sie die CPU-Auslastung erhöht.

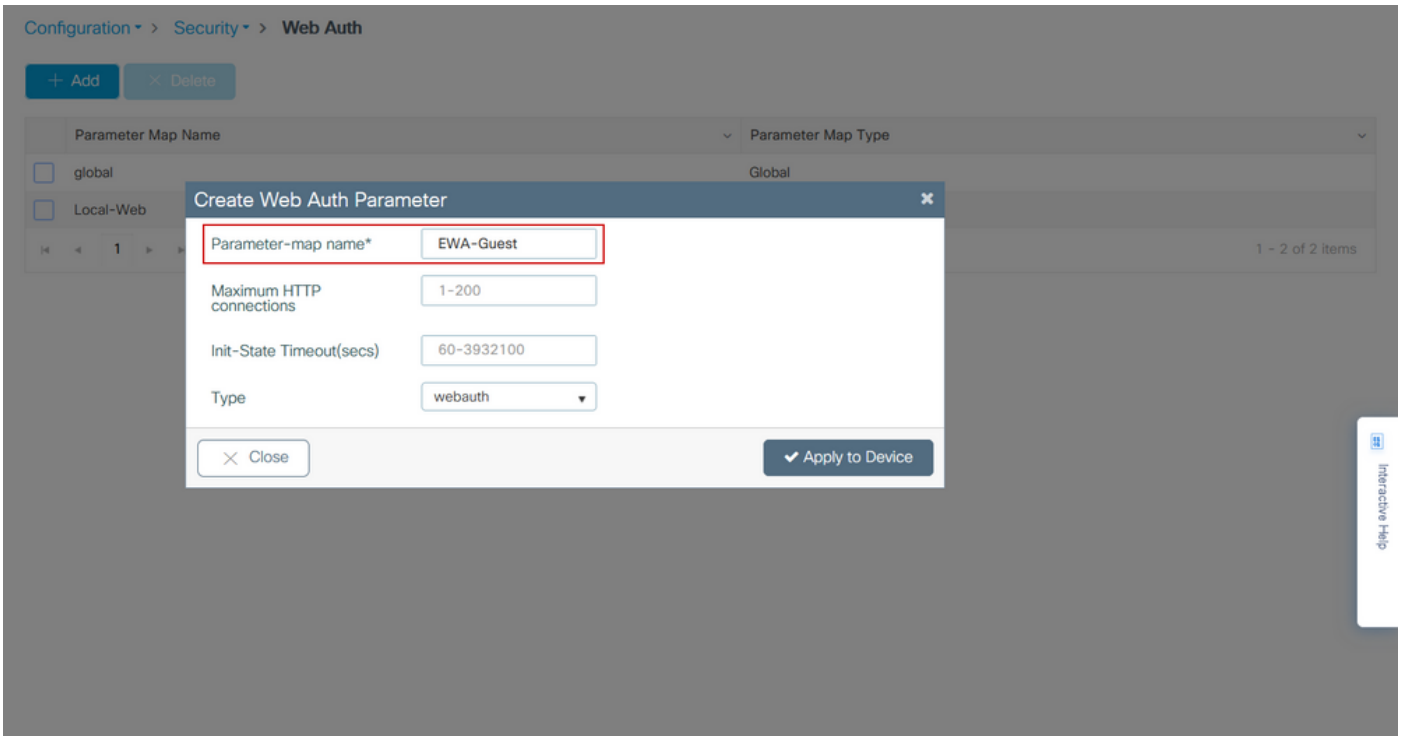


CLI-Konfiguration:

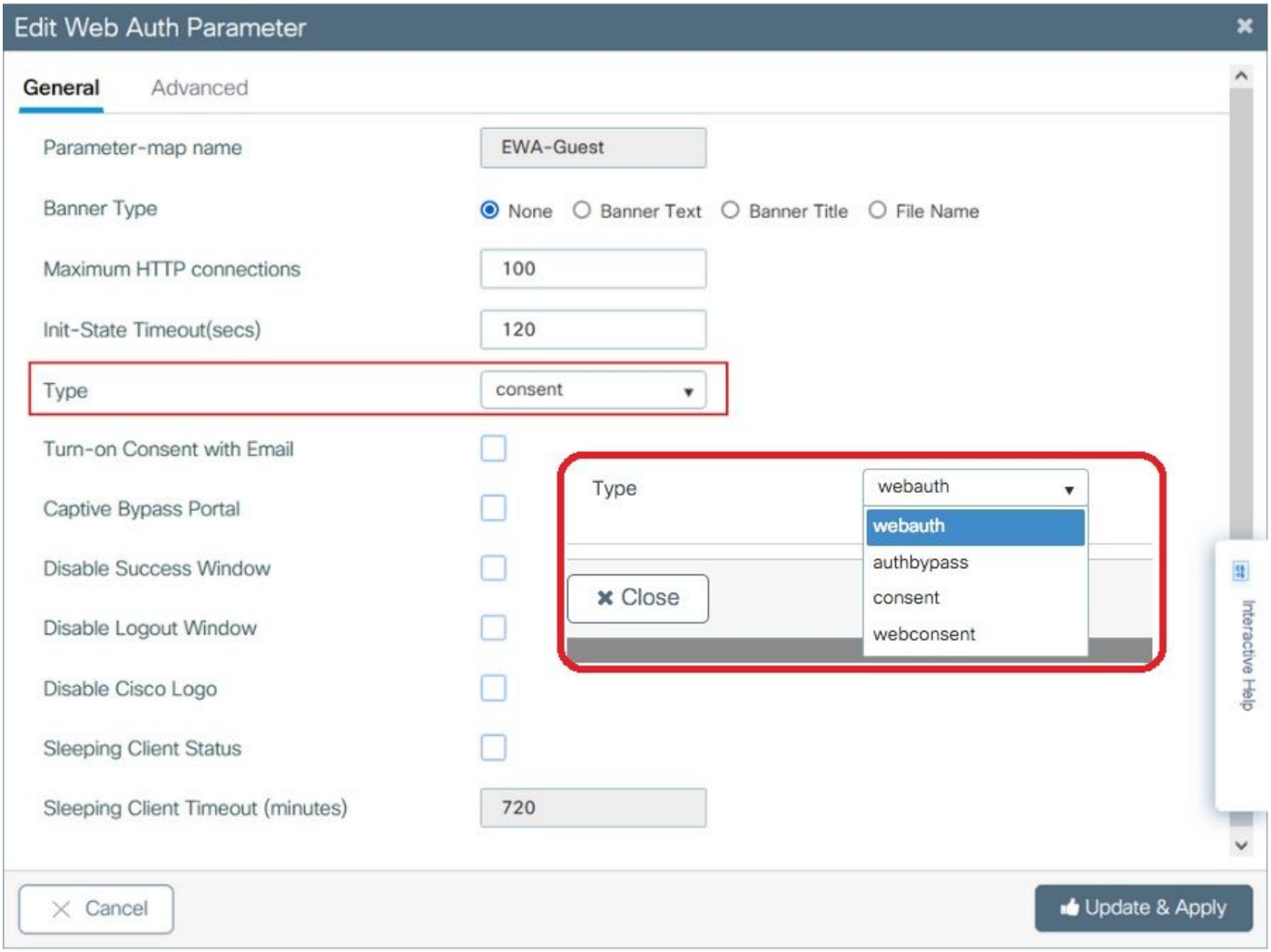
<#root>

```
9800#

configure terminal

9800(config)#

parameter-map type webauth global

9800(config-params-parameter-map)#

virtual-ip ipv4 192.0.2.1

9800(config-params-parameter-map)#

trustpoint CISCO_IDEVID_SUDI


9800(config-params-parameter-map)#

secure-webauth-disable


9800(config-params-parameter-map)#

webauth-http-enable
```

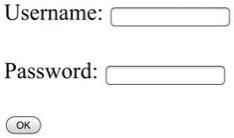
Schritt 2: Wählen Sie + Hinzufügen und konfigurieren Sie einen Namen für die neue Parameterzuordnung, die auf den externen Server verweist. Optional können Sie die maximale Anzahl von HTTP-Authentifizierungsfehlern konfigurieren, bevor der Client ausgeschlossen wird, sowie die Zeit (in Sekunden), die ein Client im Web-Authentifizierungsstatus verbleiben kann.



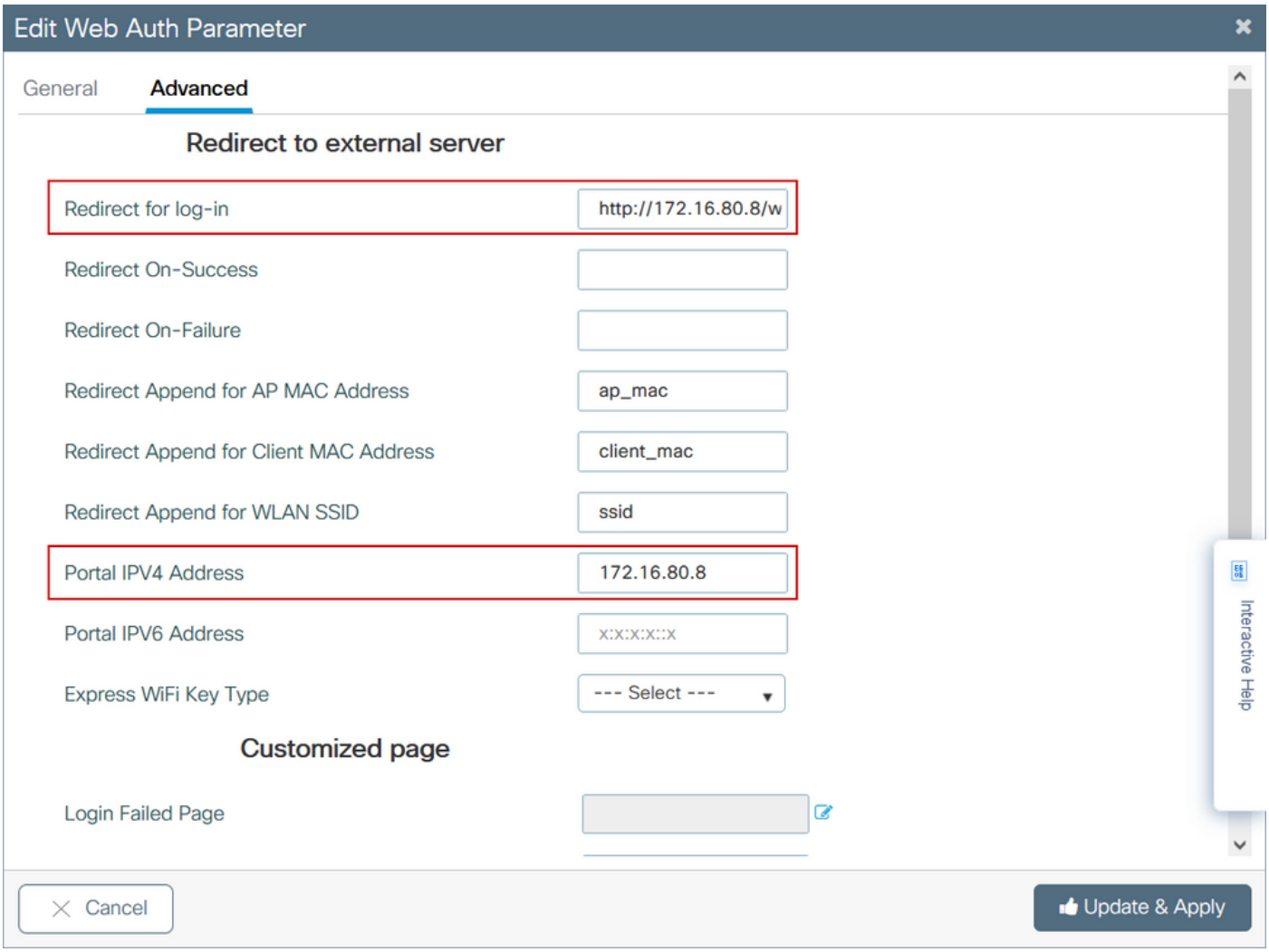
Schritt 3: Wählen Sie die neu erstellte Parameterzuordnung aus. Konfigurieren Sie auf der Registerkarte Allgemein den Authentifizierungstyp aus der Dropdown-Liste Typ.



- Name der Parameterzuordnung = Name, der der WebAuth-Parameterzuordnung zugewiesen ist
- Maximale HTTP-Verbindungen = Anzahl der Authentifizierungsfehler, bevor der Client ausgeschlossen wird
- Init-State Timeout (Sek.) = Sekunden, die ein Client im Web-Authentifizierungsstatus haben kann
- Typ = Typ der Webauthentifizierung

Webauth	Authbypass	Einwilligung	Webkonvention
	Client stellt Verbindung mit dem SSID festgelegt und erhält eine IP-Adresse, dann den 9800 WLC überprüft, ob die MAC-Adresse darf in das Netzwerk, falls ja, wird verschoben in den Status "RUN", wenn dies nicht der Fall ist, nicht teilzunehmen. (Es geht nicht auf die Web-Authentifizierung zurück.)		

Schritt 4: Konfigurieren Sie auf der Registerkarte Advanced (Erweitert) die Umleitung für die Anmeldung und die Portal-IPv4-Adresse mit der spezifischen URL der Serversite bzw. der IP-Adresse.



CLI-Konfiguration für die Schritte 2, 3 und 4:

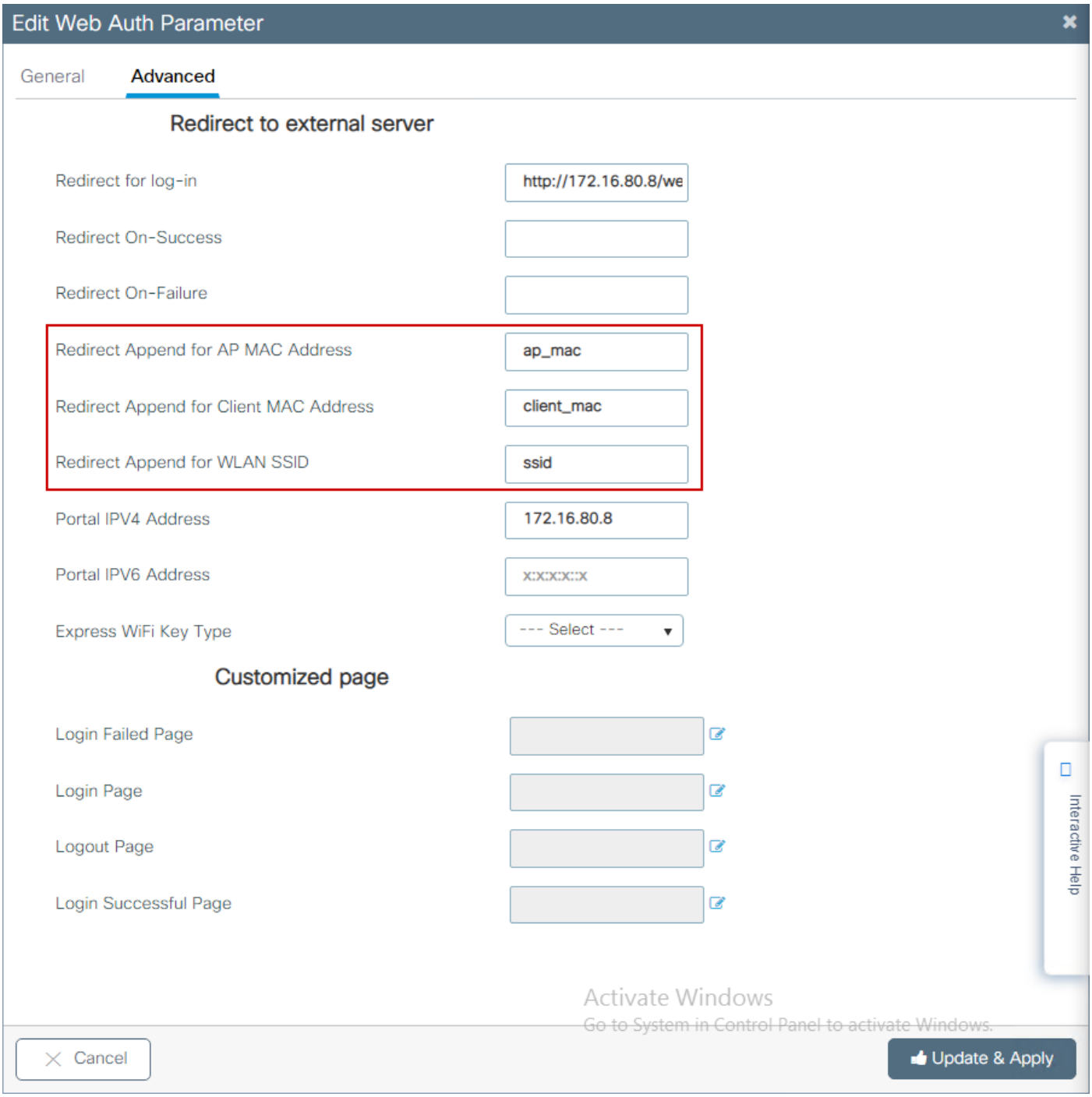
<#root>

```
9800(config)#

parameter-map type webauth EWA-Guest

9800(config-params-parameter-map)#

type consent

9800(config-params-parameter-map)#

redirect for-login http://172.16.80.8/webauth/login.html

9800(config-params-parameter-map)#

redirect portal ipv4 172.16.80.8
```

Schritt 5: (Optional) WLC kann die zusätzlichen Parameter über Query String senden. Dies wird häufig benötigt, um 9800 mit externen Drittanbieter-Portalen kompatibel zu machen. Mit den Feldern "Redirect Append for AP MAC Address", "Redirect Append for Client MAC Address" und "Redirect Append for WLAN SSID" können zusätzliche Parameter mit einem benutzerdefinierten

Namen an die Redirect ACL angehängt werden. Wählen Sie die neu erstellte Parameterzuordnung aus, und navigieren Sie zur Registerkarte Erweitert, und konfigurieren Sie den Namen für die erforderlichen Parameter. Verfügbare Parameter:

- AP-MAC-Adresse (im Format aa:bb:cc:dd:ee:ff)
- Client-MAC-Adresse (im Format aa:bb:cc:dd:ee:ff)
- SSID-Name



CLI-Konfiguration:

<#root>

```
9800(config)#
```

```
parameter-map type webauth EWA-Guest

9800(config-params-parameter-map)#
redirect append ap-mac tag ap_mac

9800(config-params-parameter-map)#
redirect append wlan-ssid tag ssid

9800(config-params-parameter-map)#
redirect append client-mac tag client_mac
```

Für dieses Beispiel ergibt die an den Client gesendete Umleitungs-URL Folgendes:

```
http://172.16.80.8/webauth/consent.html?switch_url=http://192.0.2.1/login.html&ap_mac=&ssid=&client_mac
```

Hinweis: Wenn Sie die Portal IPV4-Adressinformationen hinzufügen, wird automatisch eine ACL hinzugefügt, die den HTTP- und HTTPS-Verkehr von den Wireless-Clients zum externen Web-Authentifizierungsserver zulässt, sodass Sie keine zusätzliche Pre-Auth-ACL konfigurieren müssen. Falls Sie mehrere IP-Adressen oder URLs zulassen möchten, ist die einzige Option, einen URL-Filter zu konfigurieren, sodass alle IP-passenden URLs vor der Authentifizierung zugelassen werden. stattfindet. Es ist nicht möglich, statisch mehr als eine Portal-IP-Adresse hinzuzufügen, es sei denn, Sie verwenden URL-Filter.

Hinweis: Globale Parameterzuordnung ist die einzige, in der Sie virtuelle IPv4- und IPv6-Adressen, Webauth-Intercept-HTTPs, Captive-Bypass-Portal, Watchlist-Aktivierung und Watchlist-Timeout-Einstellungen definieren können.

Zusammenfassung der CLI-Konfiguration:

Lokaler Webserver

```
parameter-map type webauth <web-parameter-map-name>
 type { webauth | authbypass | consent | webconsent }
 timeout init-state sec 300
 banner text ^Cbanner login^C
```

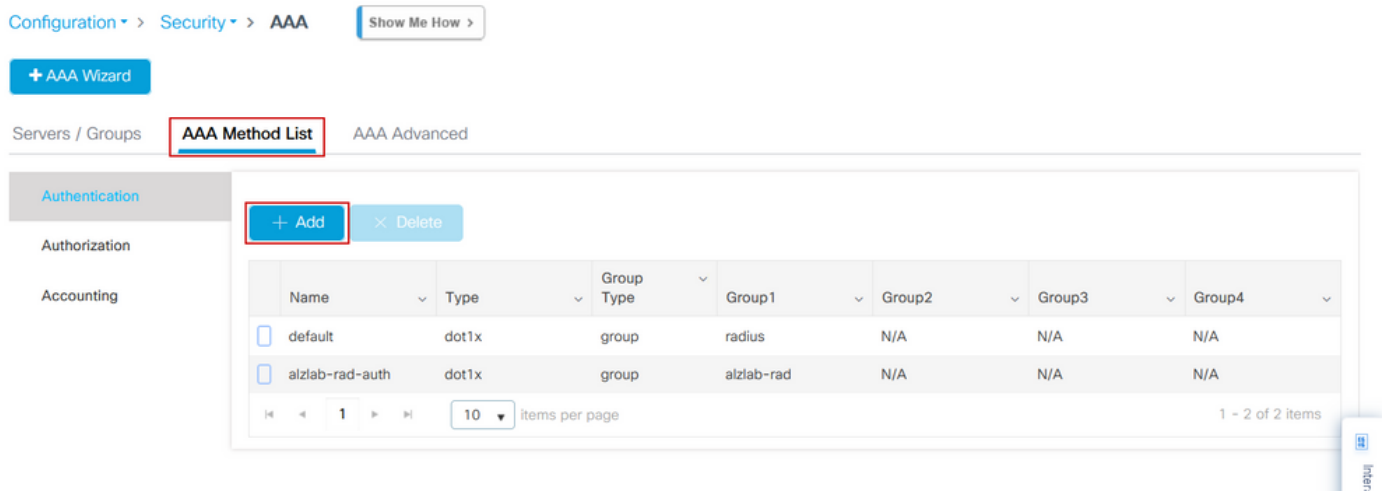
Externer Webserver

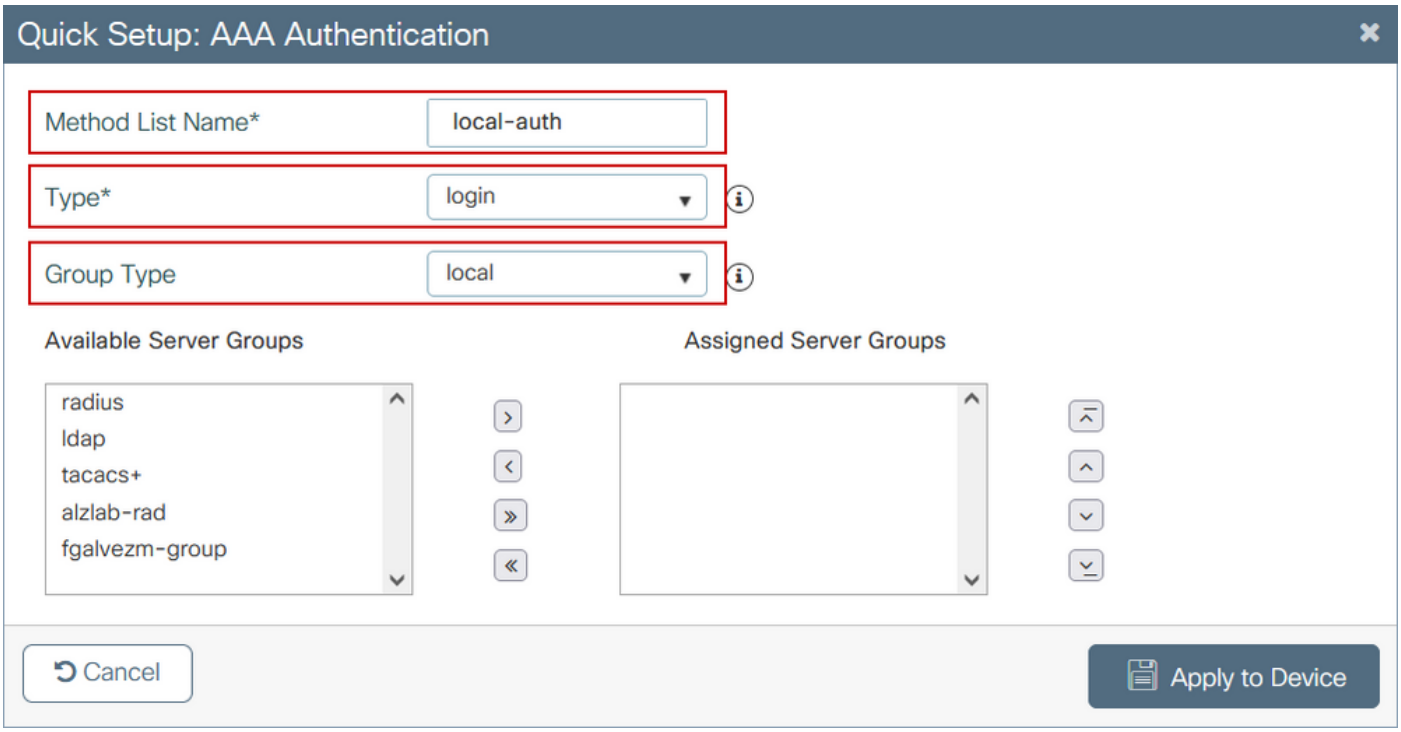
```
parameter-map type webauth <web-parameter-map-name>
 type webauth
 timeout init-state sec 300
 redirect for-login <URL-for-webauth>
 redirect portal ipv4 <external-server's-IP
 max-http-conns 10
```

AAA-Einstellungen konfigurieren

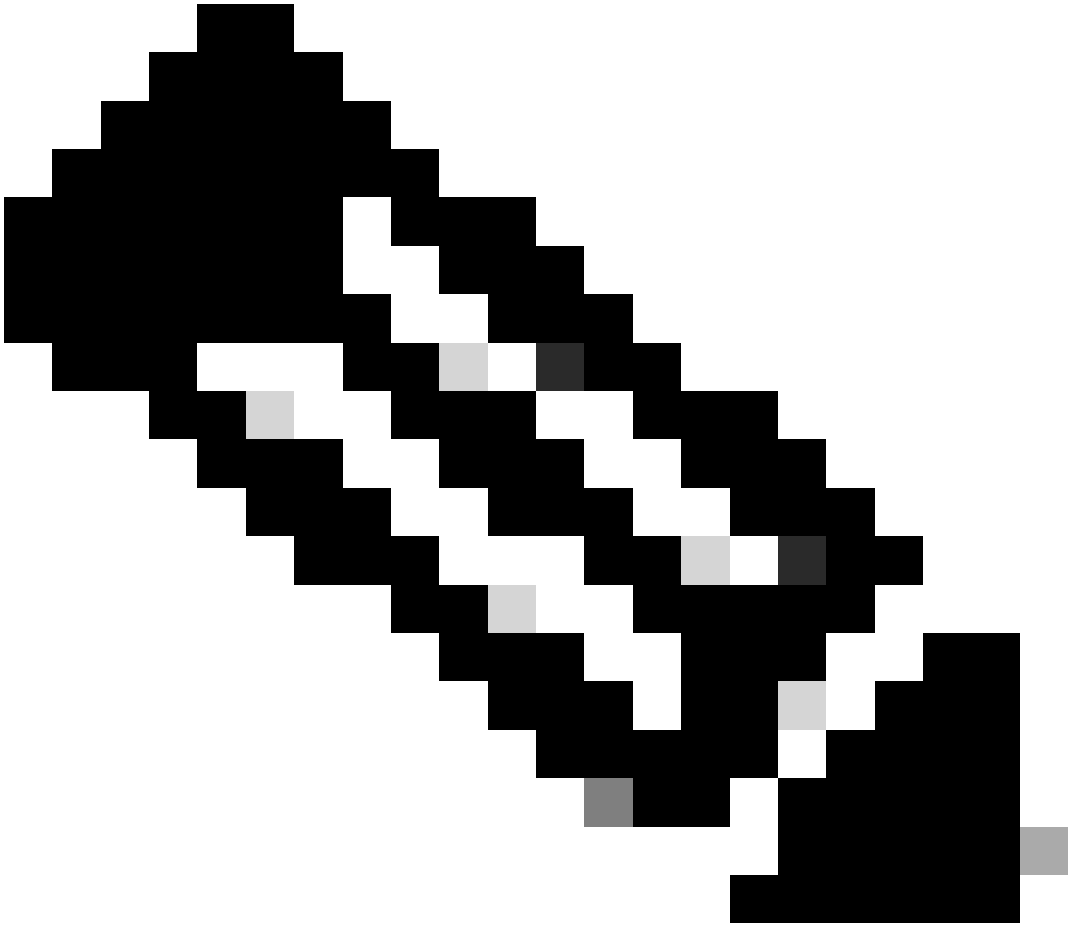
Dieser Konfigurationsabschnitt wird nur für Parameterzuordnungen benötigt, die entweder für den Webauthentifizierungstyp oder für den Webgenehmigungs-Authentifizierungstyp konfiguriert wurden.

Schritt 1: Navigieren Sie zu Configuration > Security > AAA, und wählen Sie dann AAA Method List aus. Konfigurieren Sie eine neue Methodenliste, wählen Sie + Hinzufügen und füllen Sie die Listendetails aus. Stellen Sie sicher, dass Type auf "login" gesetzt ist, wie im Bild gezeigt.

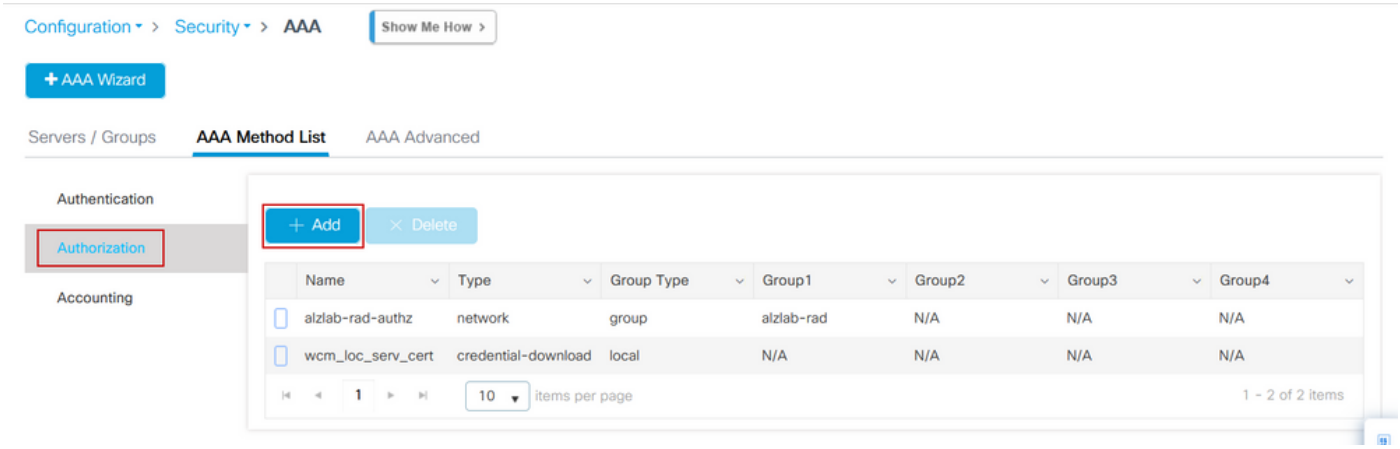


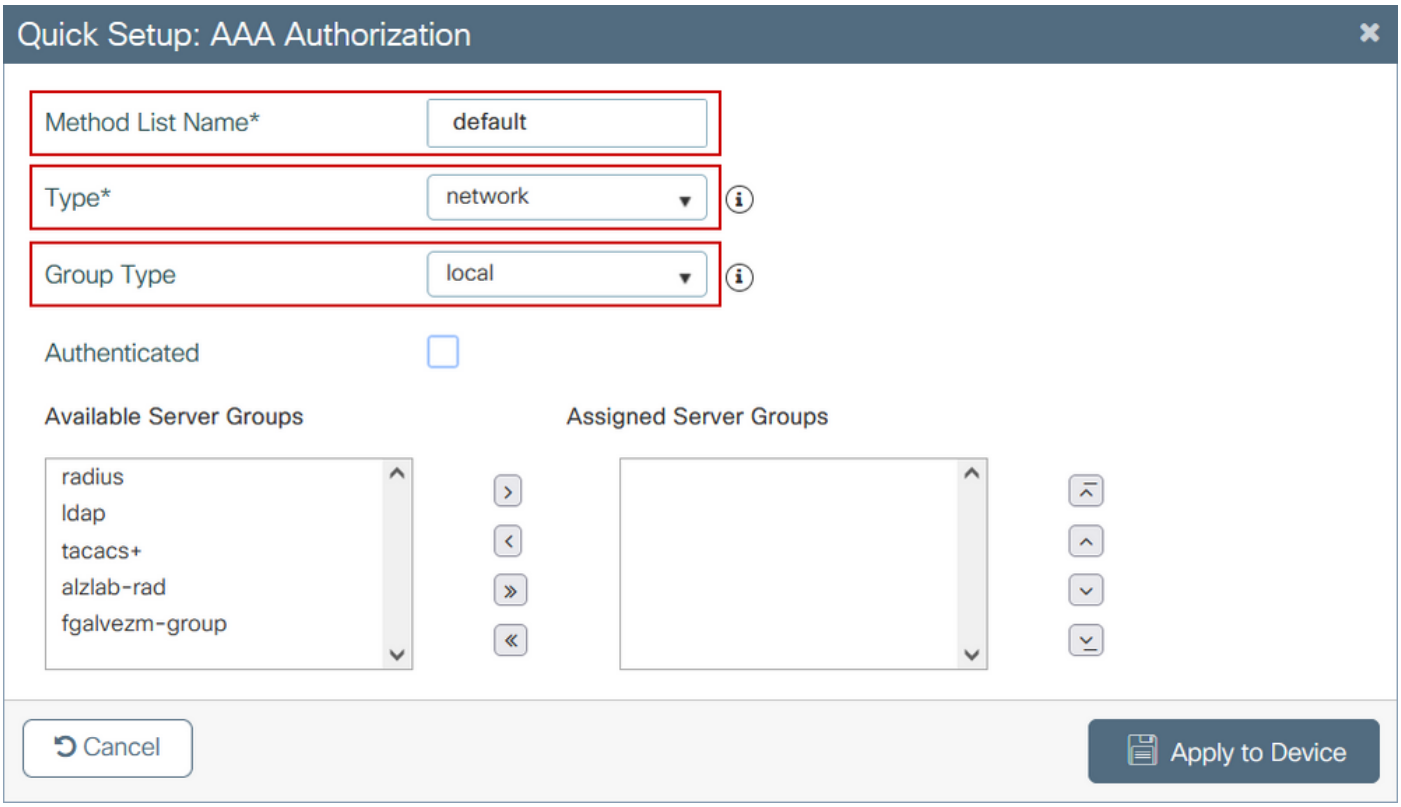


Schritt 2: Wählen Sie Authorization (Autorisierung) und anschließend + Add (Hinzufügen) aus, um eine neue Methodenliste zu erstellen. Nennen Sie es standardmäßig mit Type as network (Netzwerktyp), wie im Bild dargestellt.



Hinweis: Wie vom Controller während der Sicherheitskonfiguration für WLAN Layer 3 angekündigt: Damit die Liste der lokalen Anmeldemethoden funktioniert, stellen Sie sicher, dass die Konfiguration "aaa Authorization Network Default Local" auf dem Gerät vorhanden ist. Dies bedeutet, dass die Autorisierungsmethodenliste mit dem Standardnamen definiert werden muss, um die lokale Webauthentifizierung richtig zu konfigurieren. In diesem Abschnitt wird diese Liste der Autorisierungsmethoden konfiguriert.





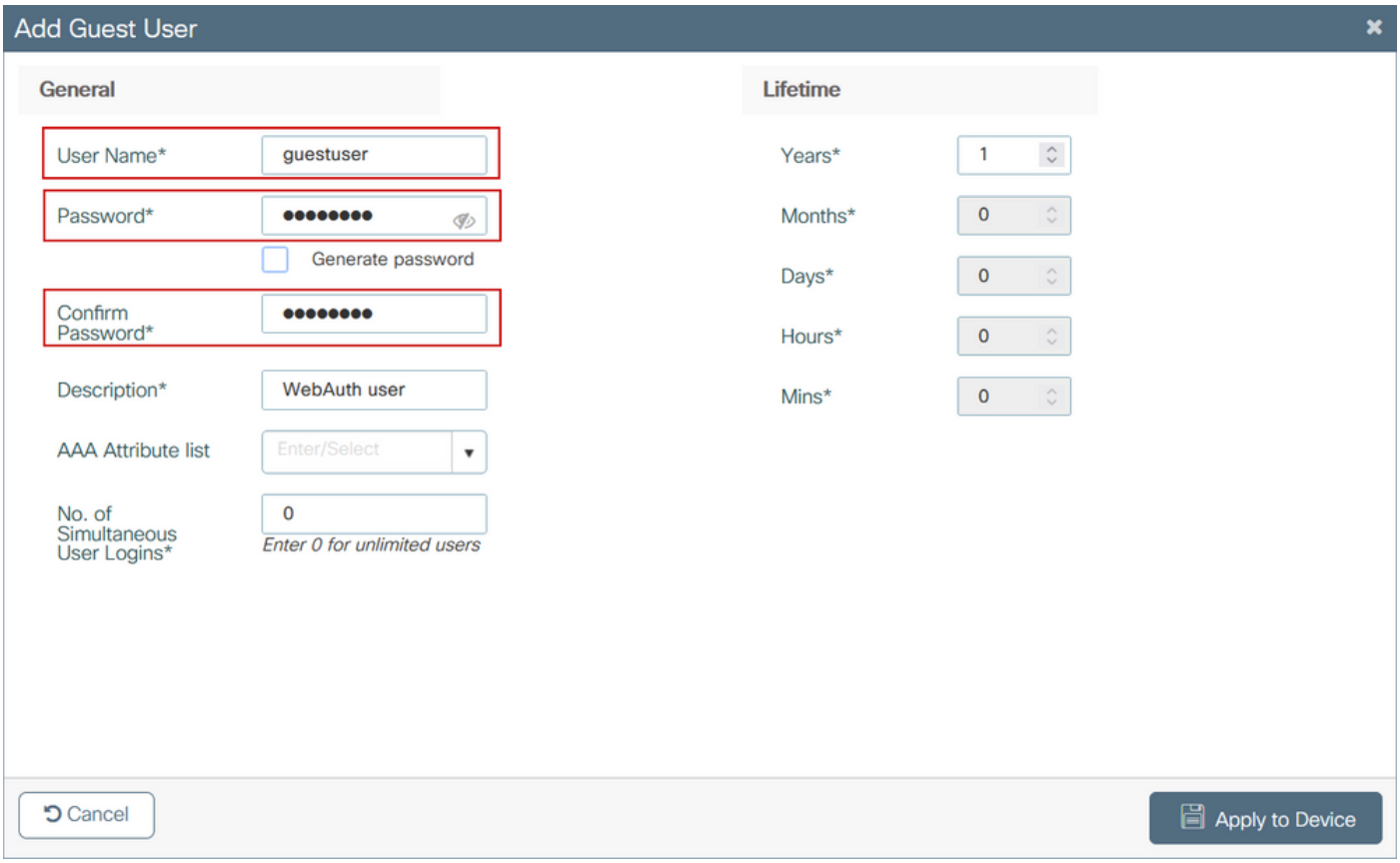
CLI-Konfiguration für Schritt 1 und 2:

<#root>

```
9800(config)#
aaa new-model

9800(config)#
aaa authentication login local-auth local

9800(config)#
aaa authorization network default local
```

Hinweis: Wenn eine externe RADIUS-Authentifizierung erforderlich ist, lesen Sie bitte die folgenden Anweisungen zur RADIUS-Serverkonfiguration auf 9800-WLCs: AAA-Konfiguration auf 9800-WLC. Stellen Sie sicher, dass in der Liste der Authentifizierungsmethoden "login" als Typ und nicht als dot1x festgelegt ist.

Schritt 3: Navigieren Sie zu Konfiguration > Sicherheit > Gastbenutzer. Wählen Sie + Details zum Gastbenutzerkonto hinzufügen und konfigurieren.



CLI-Konfiguration:

<#root>

```
9800(config)#

user-name guestuser

9800(config-user-name)#

description "WebAuth user"

9800(config-user-name)#

password 0 <password>

9800(config-user-name)#

type network-user description "WebAuth user" guest-user lifetime year 1
```

If permanent users are needed then use this command:
9800(config)#

username guestuserperm privilege 0 secret 0 <password>

Schritt 4: (Optional) Bei der Definition der Parameterzuordnung werden automatisch mehrere Zugriffskontrolllisten (ACLs) erstellt. Diese ACLs werden verwendet, um festzulegen, welcher Datenverkehr eine Umleitung an den Webserver auslöst und welcher Datenverkehr durchgelassen wird. Wenn bestimmte Anforderungen, z. B. mehrere Webserver-IP-Adressen oder URL-Filter, vorhanden sind, navigieren Sie zu Configuration > Security > ACL (Konfiguration > Sicherheit > ACL) select + Add (Hinzufügen) und definieren die erforderlichen Regeln; permit-Anweisungen werden umgeleitet, während deny-Anweisungen die Weiterleitung von Datenverkehr definieren.

Regeln für automatisch erstellte Zugriffskontrolllisten sind:

<#root>

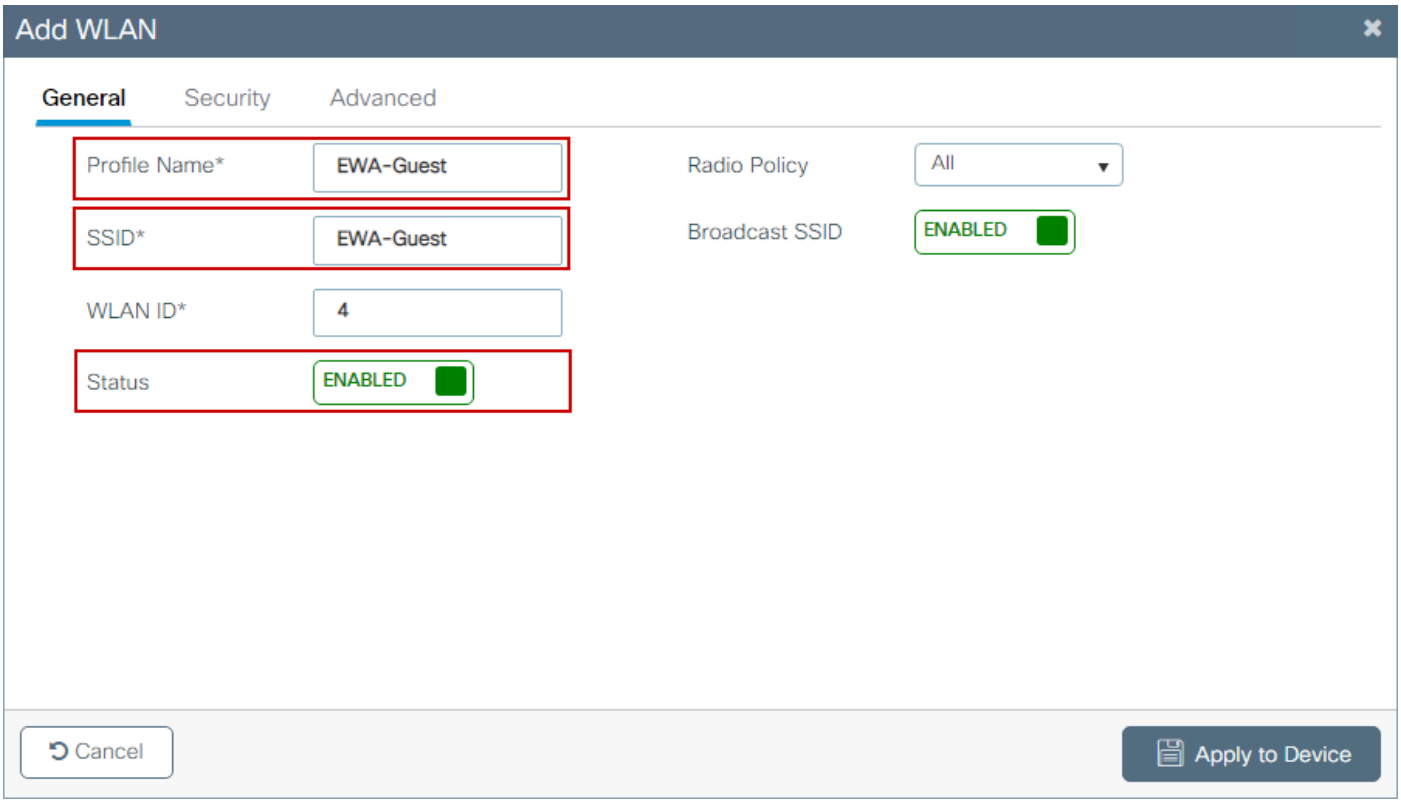
alz-9800#

show ip access-list

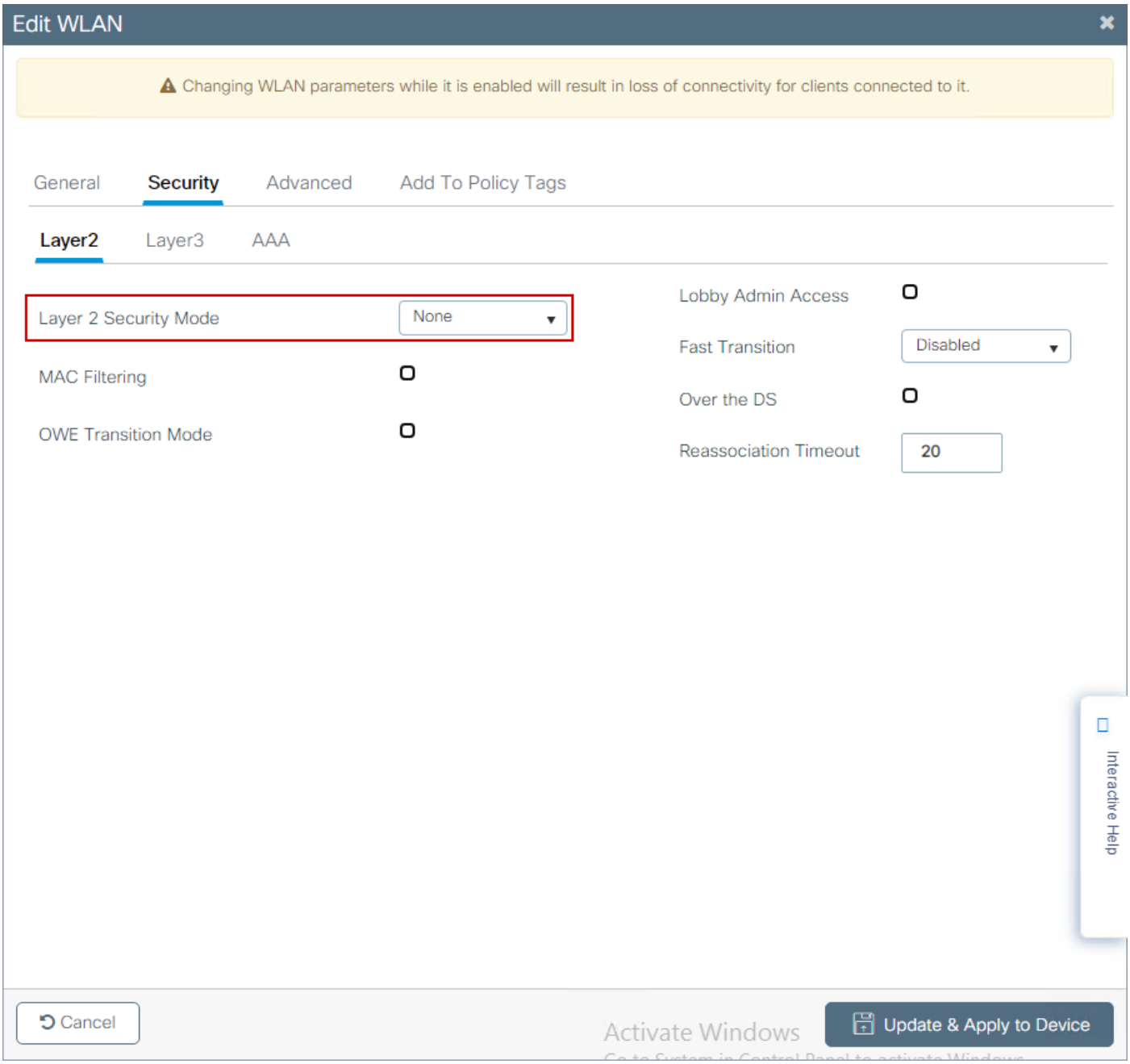
```
Extended IP access list WA-sec-172.16.80.8
10 permit tcp any host 172.16.80.8 eq www
20 permit tcp any host 172.16.80.8 eq 443
30 permit tcp host 172.16.80.8 eq www any
40 permit tcp host 172.16.80.8 eq 443 any
50 permit tcp any any eq domain
60 permit udp any any eq domain
70 permit udp any any eq bootpc
80 permit udp any any eq bootps
90 deny ip any any (1288 matches)
Extended IP access list WA-v4-int-172.16.80.8
10 deny tcp any host 172.16.80.8 eq www
20 deny tcp any host 172.16.80.8 eq 443
30 permit tcp any any eq www
40 permit tcp any host 192.0.2.1 eq 443
```

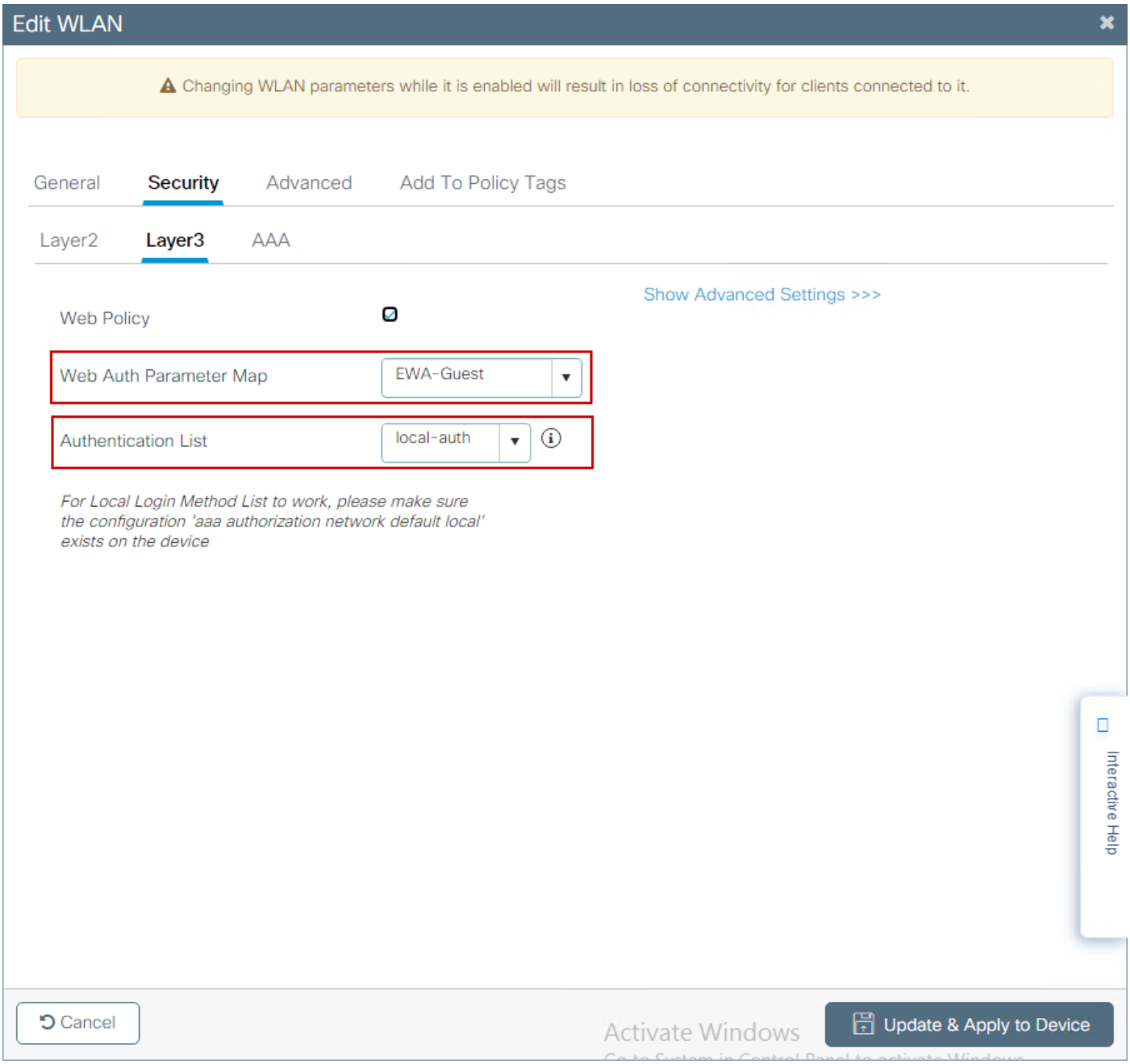
Konfigurieren von Richtlinien und Tags

Schritt 1: Navigieren Sie zu Configuration > Tags & Profiles > WLANs, und wählen Sie + Add aus, um ein neues WLAN zu erstellen. Auf der Registerkarte Allgemein können Sie den Profil- und SSID-Namen sowie den Status definieren.



Schritt 2: Wählen Sie die Registerkarte Sicherheit, und legen Sie die Layer-2-Authentifizierung auf Keine fest, wenn Sie keine Verschlüsselung per Funk benötigen. Aktivieren Sie auf der Registerkarte Layer 3 das Kontrollkästchen Web Policy, wählen Sie die Parameterzuordnung aus dem Dropdown-Menü aus, und wählen Sie die Authentifizierungsliste aus dem Dropdown-Menü aus. Wenn zuvor eine benutzerdefinierte ACL definiert wurde, können Sie optional die Option Erweiterte Einstellungen anzeigen und die entsprechende ACL aus dem Dropdown-Menü auswählen.


Edit WLAN
Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.
General
Security
Advanced
Add To Policy Tags
Layer2
Layer3
AAA
Layer 2 Security Mode
None
MAC Filtering
OWE Transition Mode
Lobby Admin Access
Fast Transition
Disabled
Over the DS
Reassociation Timeout
20
Interactive Help
Cancel
Activate Windows
Update & Apply to Device



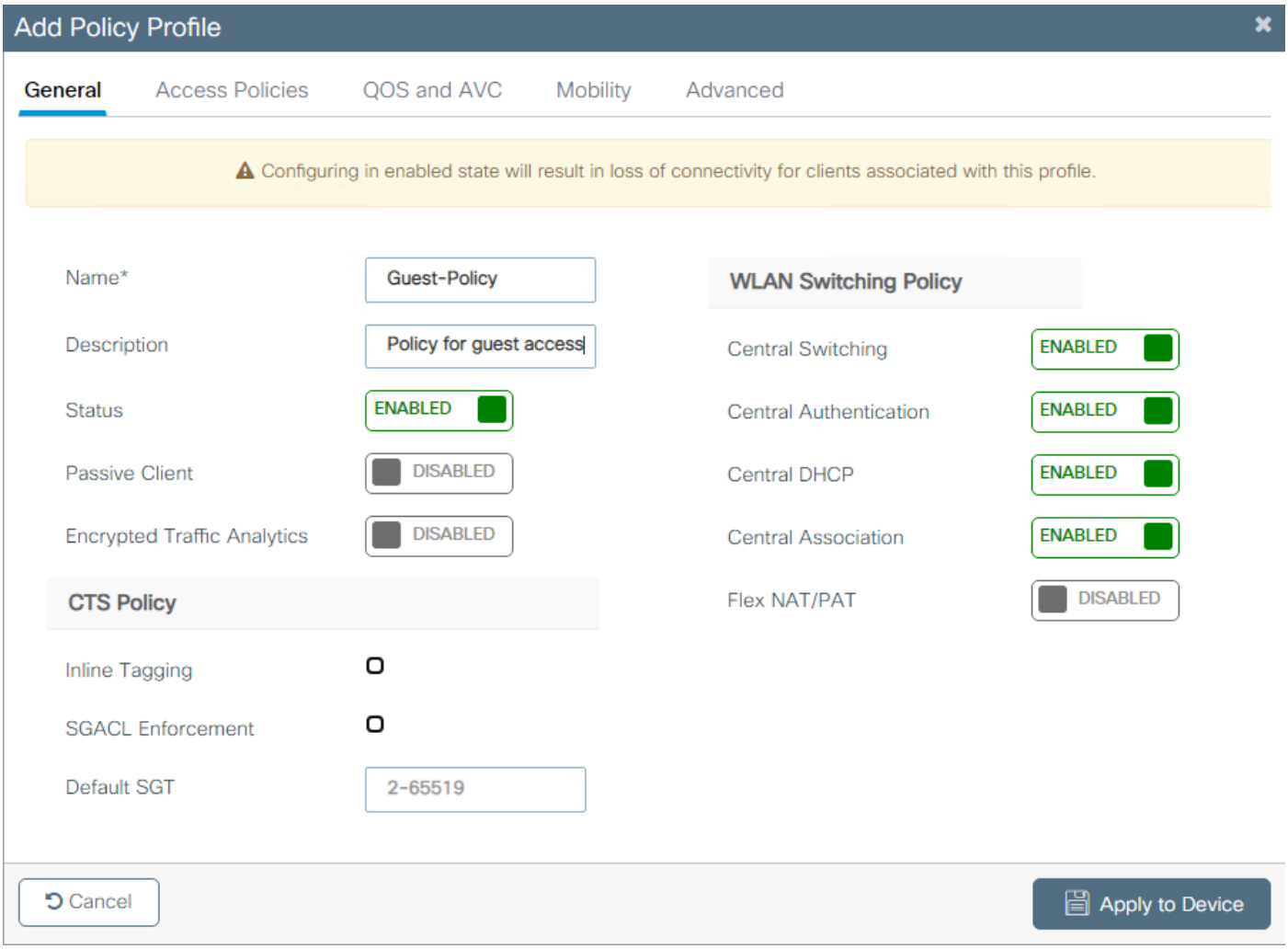
CLI-Konfigurationen:

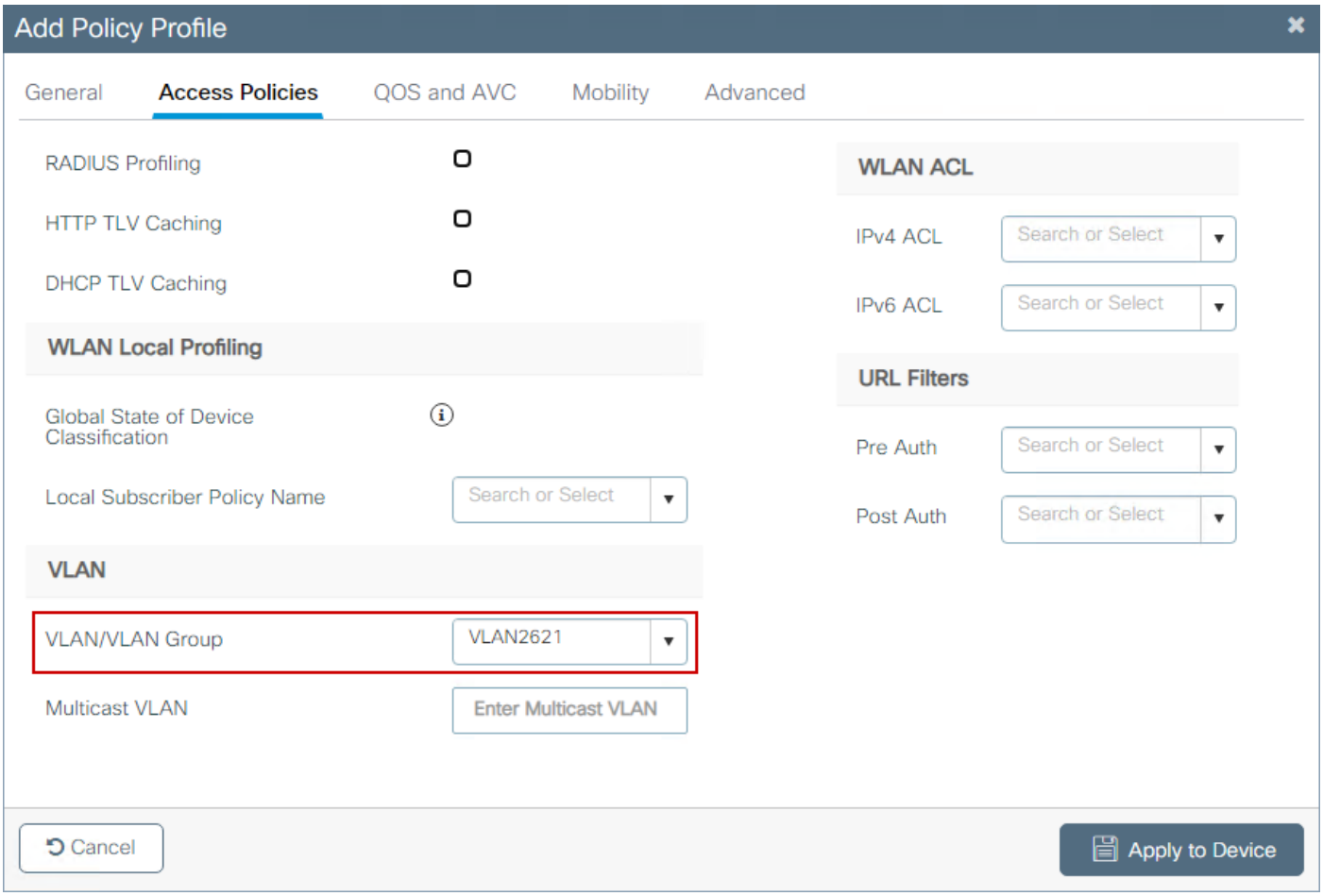
<#root>

```
9800(config)#

wlan EWA-Guest 4 EWA-Guest

9800(config-wlan)#

no security ft adaptive

9800(config-wlan)#

no security wpa

9800(config-wlan)#
```

```
no security wpa wpa2

9800(config-wlan)#
no security wpa wpa2 ciphers aes

9800(config-wlan)#
no security wpa akm dot1x

9800(config-wlan)#
security web-auth

9800(config-wlan)#
security web-auth authentication-list local-auth

9800(config-wlan)#
security web-auth parameter-map EWA-Guest

9800(config-wlan)#
 no shutdown
```

Schritt 3: Navigieren Sie zu Konfiguration > Tags und Profile > Richtlinie, und wählen Sie + Hinzufügen aus. Definieren Sie den Richtliniennamen und -status. Stellen Sie sicher, dass die zentralen Einstellungen unter "WLAN Switching Policy" (WLAN-Switching-Richtlinie) für die APs im lokalen Modus aktiviert sind. Wählen Sie auf der Registerkarte Access Policies (Zugriffsrichtlinien) das richtige VLAN aus dem Dropdown-Menü VLAN/VLAN Group (VLAN/VLAN-Gruppe) aus, wie im Bild gezeigt.


Add Policy Profile
General
Access Policies
QOS and AVC
Mobility
Advanced
Configuring in enabled state will result in loss of connectivity for clients associated with this profile.
Name*
Guest-Policy
Description
Policy for guest access
Status
ENABLED
Passive Client
DISABLED
Encrypted Traffic Analytics
DISABLED
CTS Policy
Inline Tagging
SGACL Enforcement
Default SGT
2-65519
WLAN Switching Policy
Central Switching
ENABLED
Central Authentication
ENABLED
Central DHCP
ENABLED
Central Association
ENABLED
Flex NAT/PAT
DISABLED
Cancel
Apply to Device

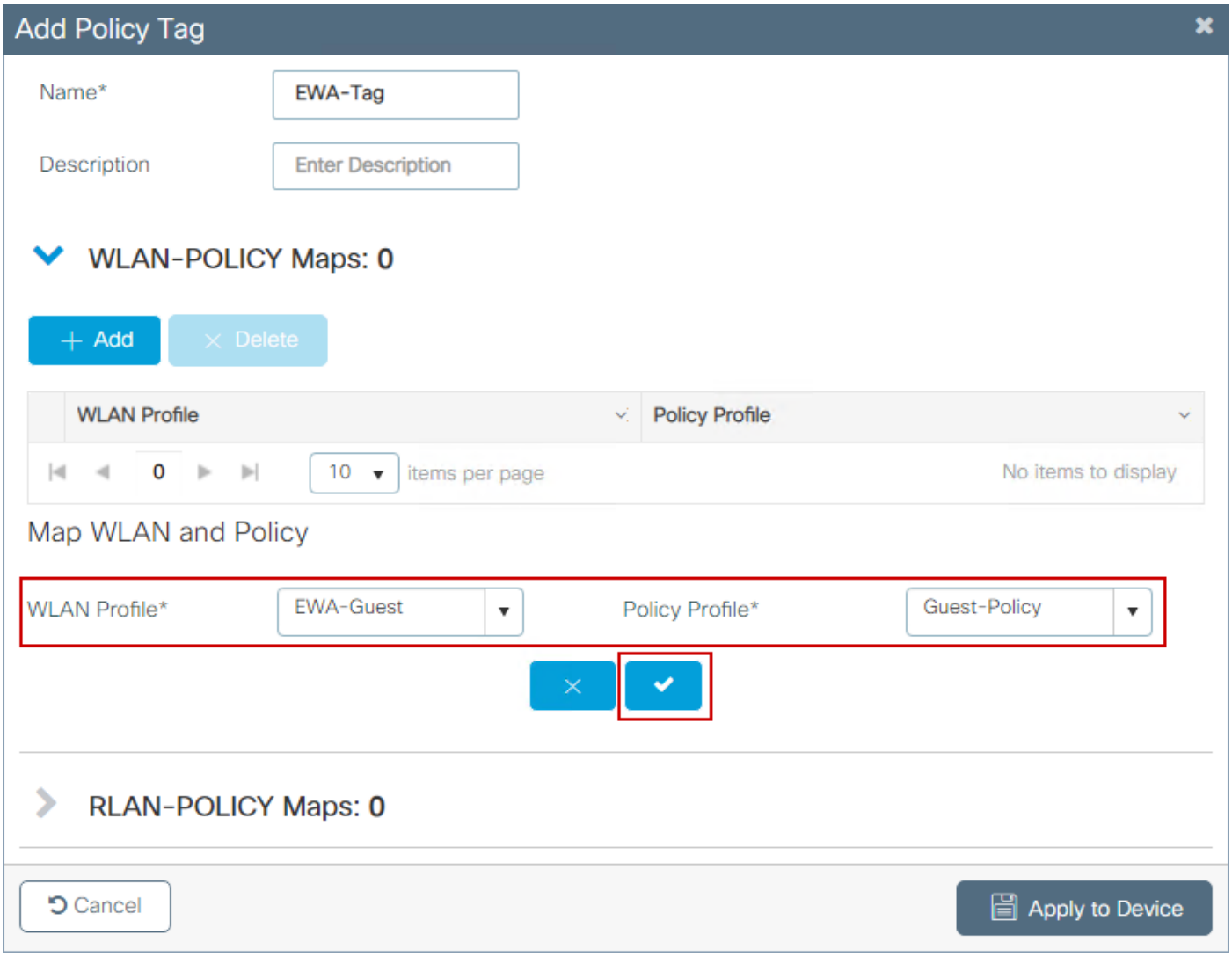


CLI-Konfiguration:

<#root>

```
9800(config)#

wireless profile policy Guest-Policy

9800(config-wireless-policy)#

description "Policy for guest access"

9800(config-wireless-policy)#

vlan VLAN2621

9800(config-wireless-policy)#

no shutdown
```

Schritt 4: Navigieren Sie zu Configuration > Tags & Profiles > Tags, und wählen Sie auf der Registerkarte Policy (Richtlinie) + Add (Hinzufügen). Definieren Sie einen Tag-Namen, wählen Sie dann unter WLAN-POLICY Maps + Add aus, und fügen Sie das zuvor erstellte WLAN und Richtlinienprofil hinzu.

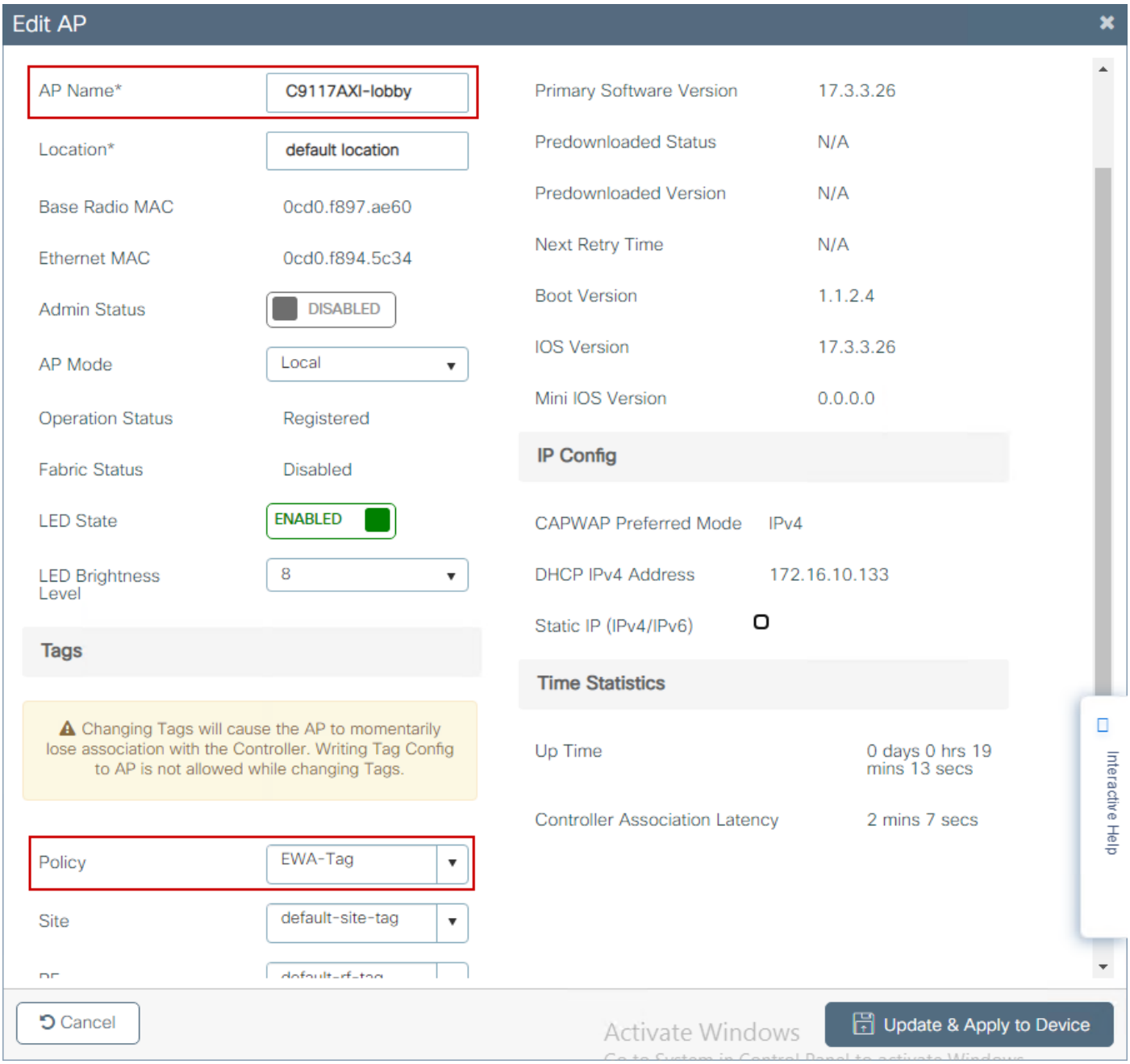


CLI-Konfiguration:

<#root>

```
9800(config)#

wireless tag policy EWA-Tag


9800(config-policy-tag)#

wlan EWA-Guest policy Guest-Policy
```

Schritt 5: Navigieren Sie zu Configuration > Wireless > Access Points, und wählen Sie den AP aus, der zum Senden dieser SSID verwendet wird. Wählen Sie im Menü Edit AP (Access Point bearbeiten) das neu erstellte Tag aus dem Dropdown-Menü Policy (Richtlinie) aus.



Wenn mehrere APs gleichzeitig gekennzeichnet werden müssen, stehen zwei Optionen zur Verfügung:

Option A. Navigieren Sie zu Configuration > Wireless Setup > Advanced (Konfiguration > Wireless-Einrichtung > Erweitert), und wählen Sie dort Start Now (Jetzt starten) aus, um die Liste im Konfigurationsmenü anzuzeigen. Wählen Sie das Listensymbol neben Tag APs aus, um die Liste aller APs im Join-Status anzuzeigen, überprüfen Sie die erforderlichen APs, und wählen Sie dann + Tag APs aus, wählen Sie im Dropdown-Menü den erstellten Policy Tag aus.

Wireless Setup Flow Overview

This screen allows you to design Wireless LAN Configuration. It involves creating Policies and Tags. Once the design is completed, they can be deployed to the Access Points right here.

DESIGN PHASE

Tags & Profiles

WLAN Policy (Mandatory)	Site Policy (Optional)	Radio Policy (Optional)
WLAN Profile	AP Join Profile	RF Profile
Policy Profile	Flex Profile	RF Tag
Policy Tag	Site Tag	

DEPLOY PHASE

Apply to APs

(Mandatory)

Tag APs

Select APs and push configuration to them

TERMINOLOGY

Tag

WLAN Policy, Policy Profile

Site Policy - AP Profile, Site Profile

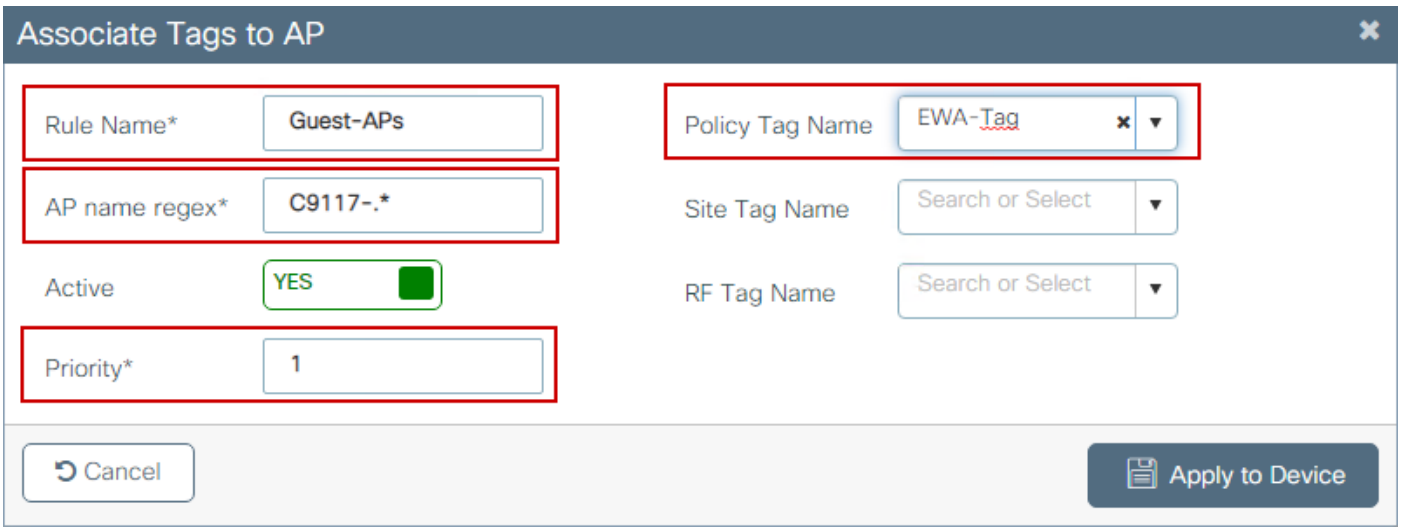
Radio Policy - Radio Characteristics

ACTIONS

Go to List View

Create New

. Definieren Sie einen Regelnamen, einen regulären AP-Namen (mit dieser Einstellung kann der Controller definieren, welche APs gekennzeichnet sind), eine Priorität (niedrigere Nummern haben eine höhere Priorität) und erforderliche Tags.



Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert:

<#root>

9800#

show running-config wlan

9800#

show running-config aaa

9800#

show aaa servers

9800#

show ap tag summary

9800#

show ap name <ap-name> config general

9800#

show ap name <ap-name> tag detail

9800#

show wlan [summary | id | name | all]

9800#

show wireless tag policy detailed <policy-tag name>

9800#

show wireless profile policy detailed <policy-profile name>

Überprüfen Sie den HTTP-Serverstatus und die Verfügbarkeit mit show ip http server status:

<#root>

9800#

show ip http server status

HTTP server status: Enabled

HTTP server port: 80

HTTP server active supplementary listener ports: 21111
HTTP server authentication method: local
HTTP server auth-retry 0 time-window 0
HTTP server digest algorithm: md5
HTTP server access class: 0

HTTP server IPv4 access class: None

HTTP server IPv6 access class: None

[...]
HTTP server active session modules: ALL
HTTP secure server capability: Present

HTTP secure server status: Enabled

HTTP secure server port: 443

HTTP secure server ciphersuite: rsa-aes-cbc-sha2 rsa-aes-gcm-sha2
dhe-aes-cbc-sha2 dhe-aes-gcm-sha2 ecdhe-rsa-aes-cbc-sha2
ecdhe-rsa-aes-gcm-sha2 ecdhe-ecdsa-aes-gcm-sha2
HTTP secure server TLS version: TLSv1.2 TLSv1.1
HTTP secure server client authentication: Disabled
HTTP secure server PIV authentication: Disabled
HTTP secure server PIV authorization only: Disabled

HTTP secure server trustpoint: CISCO_IDEVID_SUDI

HTTP secure server peer validation trustpoint:

```
HTTP secure server ECDHE curve: secp256r1
HTTP secure server active session modules: ALL
```

Überprüfen Sie die Zugriffskontrolllisten-Piumb für die Client-Sitzung mithilfe der folgenden Befehle:

<#root>

```
9800#
show platform software wireless-client chassis active R0 mac-address <Client mac in aaaa.bbbb.cccc forma

ID : 0xa0000002
MAC address : aaaa.bbbb.cccc
Type : Normal
Global WLAN ID : 4
SSID : EWA-Guest

Client index : 0
Mobility state : Local
Authentication state : L3 Authentication

VLAN ID : 2621
[...]
Disable IPv6 traffic : No
Dynamic policy template : 0x7b 0x73 0x0b 0x1e 0x46 0x2a 0xd7 0x8f 0x23 0xf3 0xfe 0x9e 0x5c 0xb0 0xeb 0xf

9800#
show platform software cgacl chassis active F0

Template ID
Group Index
 Lookup ID Number of clients
-----------------------------------------------------------------------------------------------------------
0x7B 0x73 0x0B 0x1E 0x46 0x2A 0xD7 0x8F 0x23 0xF3 0xFE 0x9E 0x5C 0xB0 0xEB 0xF8 0x0000000a

0x0000001a 1

9800#
show platform software cgacl chassis active F0 group-idx <group index> acl

Acl ID Acl Name CGACL Type Protocol Direction Sequence
-----------------------------------------------------------------------------------------------------------
16 IP-Adm-V6-Int-ACL-global Punt IPv6 IN 1
```

```
25 WA-sec-172.16.80.8 Security IPv4 IN 2


26 WA-v4-int-172.16.80.8 Punt IPv4 IN 1


19 implicit_deny Security IPv4 IN 3
21 implicit_deny_v6 Security IPv6 IN 3
18 preauth_v6 Security IPv6 IN 2
```

Fehlerbehebung

Stets verfügbare Ablaufverfolgung

Der WLC 9800 bietet IMMER-EIN-Ablaufverfolgungsfunktionen. So wird sichergestellt, dass alle verbindungsbezogenen Fehler, Warnungen und Meldungen auf Benachrichtigungsebene ständig protokolliert werden und Sie Protokolle zu Vorfällen oder Ausfällen anzeigen können, nachdem diese aufgetreten sind.

Hinweis: Je nach Umfang der generierten Protokolle können Sie von wenigen Stunden auf mehrere Tage zurückgehen.

Um die Traces anzuzeigen, die 9800 WLC standardmäßig gesammelt hat, können Sie sich über SSH/Telnet mit dem 9800 WLC verbinden und diese Schritte lesen (stellen Sie sicher, dass Sie die Sitzung in einer Textdatei protokollieren).

Schritt 1: Überprüfen Sie die aktuelle Uhrzeit des Controllers, damit Sie die Protokolle bis zum Auftreten des Problems nachverfolgen können.

```
<#root>

9800#

show clock
```

Schritt 2: Erfassen Sie die Syslogs aus dem Controller-Puffer oder dem externen Syslog gemäß der Systemkonfiguration. Dadurch erhalten Sie eine Kurzübersicht über den Systemstatus und etwaige Fehler.

```
<#root>

9800#

show logging
```

Schritt 3: Überprüfen Sie, ob Debug-Bedingungen aktiviert sind.

<#root>

```
9800#

show debugging

IOSXE Conditional Debug Configs:
Conditional Debug Global State: Stop
IOSXE Packet Tracing Configs:
Packet Infra debugs:
Ip Address                                              Port
------------------------------------------------------|----------
```

Hinweis: Wenn eine Bedingung aufgeführt wird, bedeutet dies, dass die Ablaufverfolgungen für alle Prozesse, bei denen die aktivierten Bedingungen auftreten (MAC-Adresse, IP-Adresse usw.) protokolliert werden. Dies würde das Protokollvolumen erhöhen. Daher wird empfohlen, alle Bedingungen zu löschen, wenn gerade kein Debugging aktiv ist.

Schritt 4: Unter der Annahme, dass die zu testende MAC-Adresse nicht als Bedingung in Schritt 3 aufgeführt wurde. Sammeln Sie die stets verfügbaren Ablaufverfolgungen für die jeweilige MAC-Adresse.

<#root>

```
9800#

show logging profile wireless filter [mac | ip] [<aaaa.bbbb.cccc> | <a.b.c.d>] to-file always-on-<FILENA
```

Sie können entweder den Inhalt der Sitzung anzeigen oder die Datei auf einen externen TFTP-Server kopieren.

<#root>

```
9800#

 more bootflash:always-on-<FILENAME.txt>
```

or

```
9800#

copy bootflash:always-on-<FILENAME.txt> tftp://<a.b.c.d>/<path>/always-on-<FILENAME.txt>
```

Bedingtes Debugging und Radio Active Tracing

Wenn die stets verfügbaren Ablaufverfolgungen nicht genügend Informationen liefern, um den Auslöser für das zu untersuchende Problem zu bestimmen, können Sie bedingtes Debuggen aktivieren und die Radio Active (RA)-Ablaufverfolgung erfassen, die Ablaufverfolgungen auf Debugebene für alle Prozesse bereitstellt, die mit der angegebenen Bedingung interagieren (in diesem Fall Client-MAC-Adresse). Lesen Sie diese Schritte, um das bedingte Debuggen zu aktivieren.

Schritt 1: Stellen Sie sicher, dass keine Debug-Bedingungen aktiviert sind.

```
<#root>

9800#

clear platform condition all
```

Schritt 2: Aktivieren Sie die Debug-Bedingung für die MAC-Adresse des Wireless-Clients, die Sie überwachen möchten.

Mit diesen Befehlen wird die angegebene MAC-Adresse 30 Minuten (1800 Sekunden) lang überwacht. Sie können diese Zeit optional auf bis zu 2085978494 Sekunden erhöhen.

```
<#root>

9800#

debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

Hinweis: Führen Sie den Befehl debug wireless mac pro MAC-Adresse aus, um mehr als einen Client gleichzeitig zu überwachen.

Hinweis: Die Wireless-Client-Aktivität wird in der Terminalsitzung nicht angezeigt, da alle Protokolle intern gepuffert werden, um zu einem späteren Zeitpunkt angezeigt zu werden.

Schritt 3: Reproduzieren Sie das Problem oder Verhalten, das Sie überwachen möchten.

Schritt 4: Stoppen Sie die Debugs, wenn das Problem reproduziert wird, bevor die standardmäßige oder konfigurierte Monitoring-Zeit abgelaufen ist.

```
<#root>

9800#

no debug wireless mac <aaaa.bbbb.cccc>
```

Sobald die Monitoring-Zeit abgelaufen ist oder das Wireless-Debugging beendet wurde, generiert der 9800 WLC eine lokale Datei mit dem Namen:

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Schritt 5: Rufen Sie die Datei mit der MAC-Adressaktivität ab. Sie können entweder die Datei „ra trace.log“ auf einen externen Server kopieren oder die Ausgabe direkt auf dem Bildschirm anzeigen.

Überprüfen Sie den Namen der RA-Tracing-Datei.

<#root>

9800#

dir bootflash: | inc ra_trace

Datei auf externen Server kopieren:

<#root>

9800#

copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://<a.b.c.d>

Inhalt anzeigen:

<#root>

9800#

more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Schritt 6: Wenn die Ursache immer noch nicht offensichtlich ist, rufen Sie die internen Protokolle ab, die eine ausführlichere Ansicht der Protokolle auf Debug-Ebene darstellen. Sie müssen den Client nicht erneut debuggen, da der Befehl Debugprotokolle bereitstellt, die bereits gesammelt und intern gespeichert wurden.

<#root>

9800#

show logging profile wireless internal filter [mac | ip] [<aaaa.bbbb.cccc> | <a.b.c.d>] to-file ra-inter

Hinweis: Diese Befehlsausgabe gibt Traces für alle Protokollierungsebenen für alle Prozesse zurück und ist sehr umfangreich. Wenden Sie sich an das Cisco TAC, um diese Traces zu analysieren.

<#root>

9800#

copy bootflash:ra-internal-<FILENAME>.txt tftp://<a.b.c.d>/ra-internal-<FILENAME>.txt

Inhalt anzeigen:

<#root>

9800#

more bootflash:ra-internal-<FILENAME>.txt

Schritt 7. Entfernen Sie die Debug-Bedingungen.

Hinweis: Stellen Sie sicher, dass die Debug-Bedingungen nach einer Fehlerbehebungssitzung immer entfernt werden.

Integrierte Paketerfassung

9.800 Controller können Pakete nativ erkennen, was die Fehlerbehebung vereinfacht, da die Paketverarbeitung auf der Kontrollebene transparent ist.

Schritt 1: Definieren einer ACL zum Filtern des relevanten Datenverkehrs Für die Webauthentifizierung wird empfohlen, Datenverkehr vom und zum Webserver sowie Datenverkehr von und zu einigen APs zuzulassen, an denen Clients angeschlossen sind.

<#root>

9800(config)#

ip access-list extended EWA-pcap

9800(config-ext-nacl)#

permit ip any host <web server IP>

9800(config-ext-nacl)#

permit ip host <web server IP> any

```
9800(config-ext-nacl)#
permit ip any host <AP IP>

9800(config-ext-nacl)#
permit ip host <AP IP> any
```

Schritt 2: Definieren der Parameter für die Monitorerfassung Stellen Sie sicher, dass der Steuerungsebenen-Datenverkehr in beide Richtungen aktiviert ist. Die Schnittstelle bezieht sich auf den physischen Uplink des Controllers.

<#root>

```
9800#
monitor capture EWA buffer size <buffer size in MB>

9800#
monitor capture EWA access-list EWA-pcap

9800#
monitor capture EWA control-plane both interface <uplink interface> both
```

<#root>

```
9800#
show monitor capture EWA

Status Information for Capture EWA
Target Type:
Interface: Control Plane, Direction: BOTH
Interface: TenGigabitEthernet0/1/0, Direction: BOTH

Status : Inactive
Filter Details:
Access-list: EWA-pcap

Inner Filter Details:
Buffer Details:
Buffer Type: LINEAR (default)
Buffer Size (in MB): 100

Limit Details:
Number of Packets to capture: 0 (no limit)
Packet Capture duration: 0 (no limit)
```

```
Packet Size to capture: 0 (no limit)
Packet sampling rate: 0 (no sampling)
```

Schritt 3: Starten Sie die Monitorerfassung, und reproduzieren Sie das Problem.

<#root>

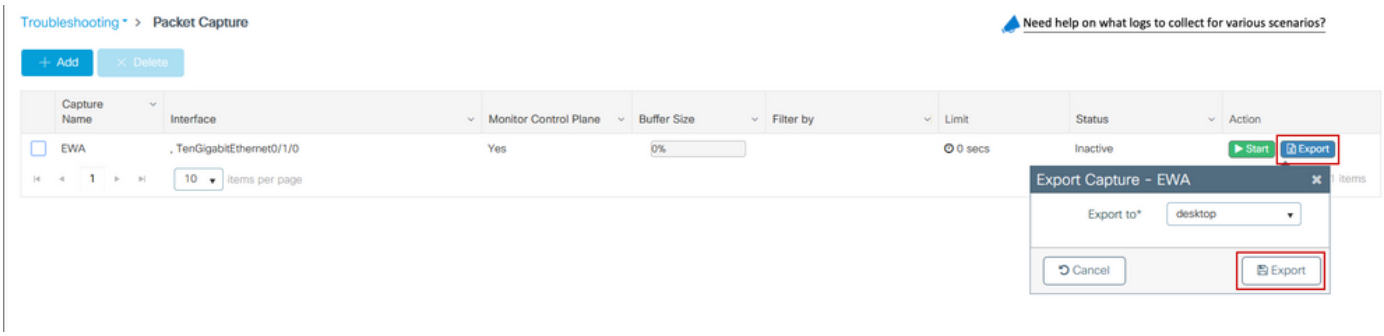
```
9800#

monitor capture EWA start


Started capture point : EWA
```

Schritt 4: Beenden Sie die Monitorerfassung, und exportieren Sie sie.

<#root>

```
9800#

monitor capture EWA stop


Stopped capture point : EWA
9800#monitor capture EWA export tftp://<a.b.c.d>/EWA.pcap
```

Alternativ kann die Erfassung auch über die GUI heruntergeladen werden. Navigieren Sie zu Troubleshooting > Packet Capture, und wählen Sie Export für die konfigurierte Erfassung aus. Wählen Sie Desktop aus dem Dropdown-Menü aus, um die Erfassung über HTTP in den gewünschten Ordner herunterzuladen.



Client-seitige Fehlerbehebung

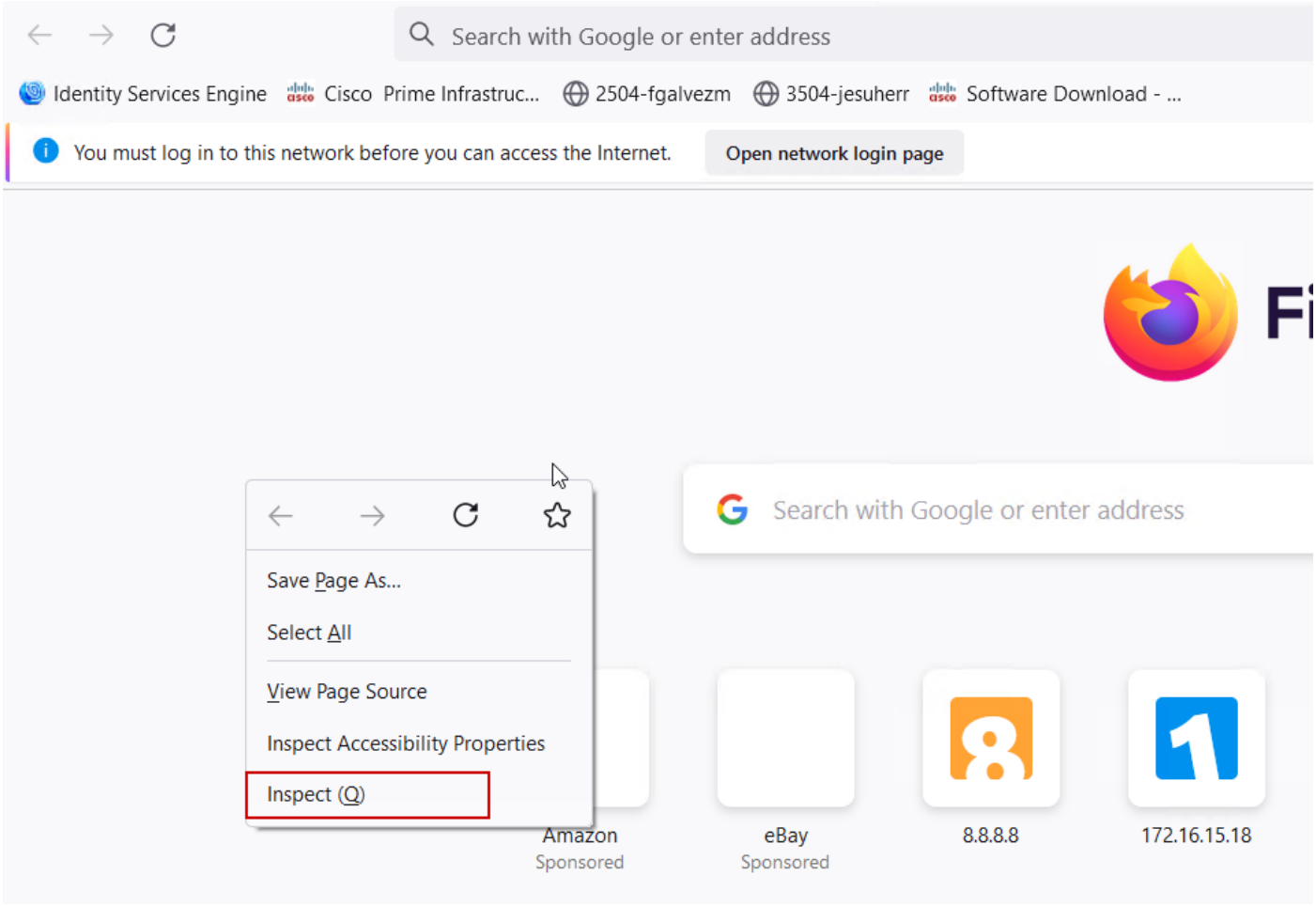
Webauthentifizierungs-WLANs sind vom Verhalten des Clients abhängig. Auf dieser Grundlage sind Kenntnisse und Informationen zum Verhalten des Clients der Schlüssel zur Identifizierung der Ursache für fehlerhafte Webauthentifizierungen.

Fehlerbehebung bei HAR-Browser

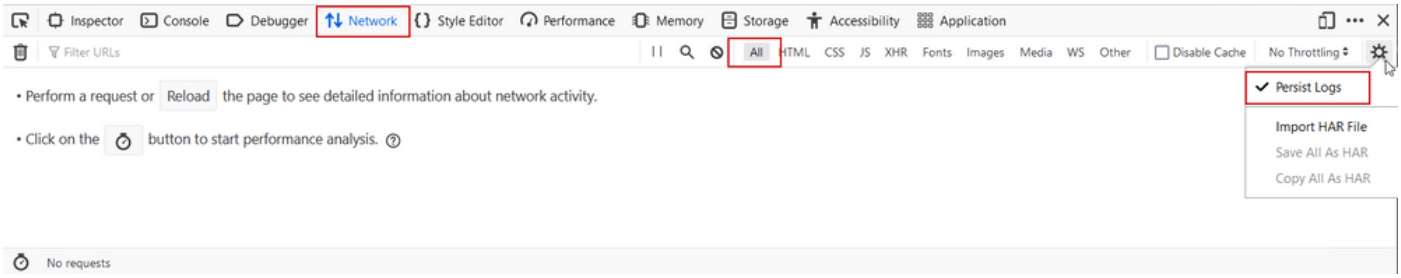
Viele moderne Browser, wie Mozilla Firefox und Google Chrome, bieten Konsolenentwicklungstools zum Debuggen von Interaktionen mit Webanwendungen. HAR-Dateien sind Datensätze mit Client-Server-Interaktionen und bieten eine Zeitleiste mit HTTP-Interaktionen sowie Anforderungs- und Antwortinformationen (Header, Statuscode, Parameter usw.).

HAR-Dateien können aus dem Client-Browser exportiert und zur weiteren Analyse in einen anderen Browser importiert werden. Dieses Dokument beschreibt, wie die HAR-Datei von Mozilla Firefox zu sammeln.

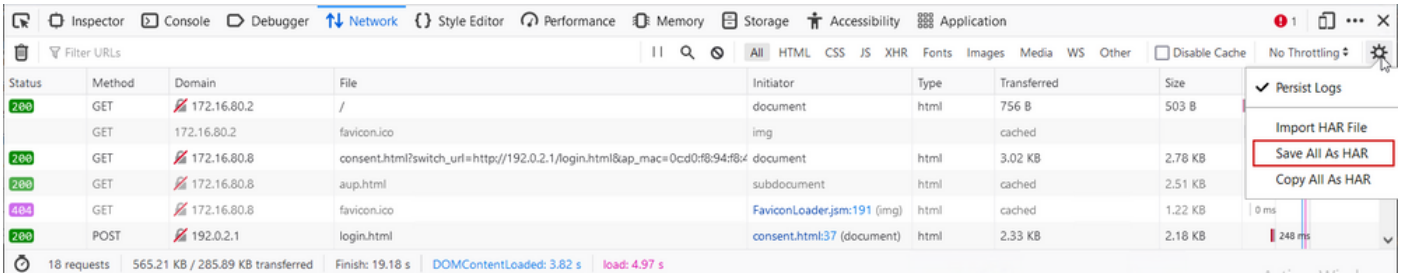
Schritt 1: Öffnen Sie Web Developer Tools mit Strg + Umschalt + I, oder klicken Sie mit der rechten Maustaste in den Browserinhalt und wählen Sie Inspizieren.



Schritt 2: Navigieren Sie zu Netzwerk, und stellen Sie sicher, dass "Alle" ausgewählt ist, um alle Anforderungstypen zu erfassen. Wählen Sie das Zahnrad-Symbol aus, und stellen Sie sicher, dass Persist Logs einen Pfeil daneben hat, andernfalls werden Loganforderungen gelöscht, wenn eine Domänenänderung ausgelöst wird.



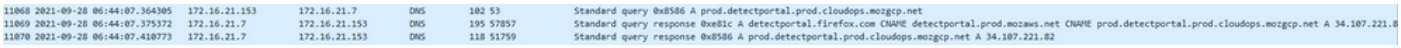
Schritt 3: Reproduzieren Sie das Problem, stellen Sie sicher, dass der Browser alle Anforderungen protokolliert. Sobald das Problem reproduziert wird, stoppen Sie die Netzwerkprotokollierung, wählen Sie dann auf dem Zahnrad-Symbol aus, und wählen Sie Alle als HAR speichern.



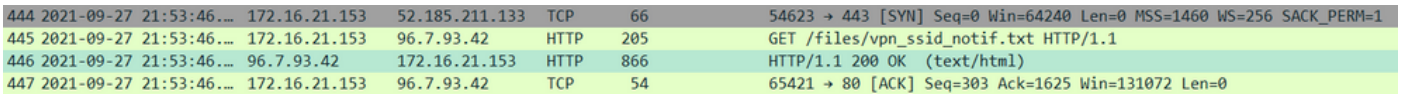
Clientseitige Paketerfassung

Wireless-Clients mit Betriebssystemen wie Windows oder MacOS können Pakete auf ihrem Wireless-Karten-Adapter abhören. Obwohl es sich hierbei nicht um einen direkten Ersatz für die drahtlose Paketerfassung handelt, können sie einen Blick auf den gesamten Web-Authentifizierungsfluss gewähren.

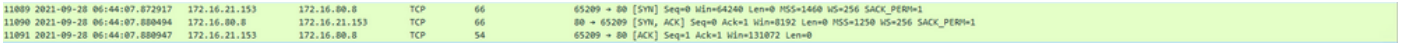
DNS-Anforderung:



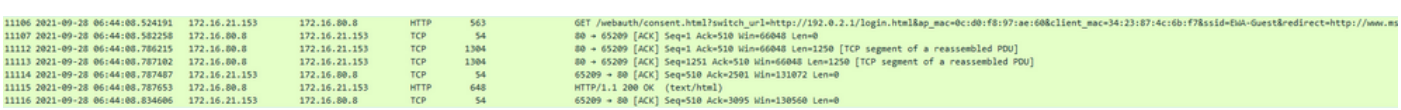
Anfänglicher TCP-Handshake und HTTP GET für die Umleitung:



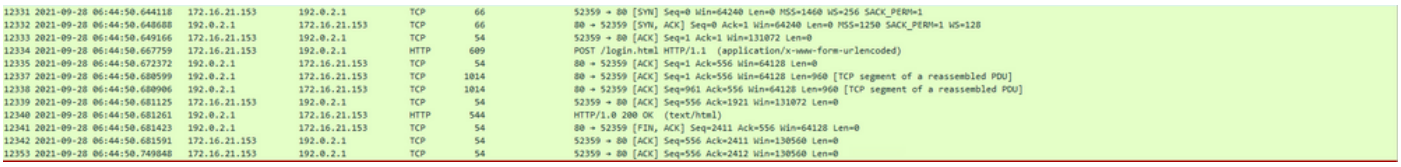
TCP-Handshake mit externem Server:



HTTP GET zu externem Server (Captive Portal Request):



HTTP POST an virtuelle IP zur Authentifizierung:



Beispiel eines erfolgreichen Versuchs

Dies ist die Ausgabe eines erfolgreichen Verbindungsversuchs aus Sicht von Radio Active Trace. Verwenden Sie diesen als Referenz, um Client-Sitzungsstufen für Clients zu identifizieren, die eine Verbindung zu einer Layer-3-Webauthentifizierungs-SSID herstellen.

802.11-Authentifizierung und -Zuordnung:

<#root>

```
2021/09/28 12:59:51.781967 {wncd_x_R0-0}{1}: [client-orch-sm] [26328]: (note): MAC: 3423.874c.6bf7 Asso
2021/09/28 12:59:51.782009 {wncd_x_R0-0}{1}: [client-orch-sm] [26328]: (debug): MAC: 3423.874c.6bf7

Received Dot11 association request.

 Processing started,

SSID: EWA-Guest, Policy profile: Guest-Policy

, AP Name: C9117AXI-lobby, Ap Mac Address: 0cd0.f897.ae60 BSSID MAC0000.0000.0000 wlan ID: 4RSSI: -39,
2021/09/28 12:59:51.782152 {wncd_x_R0-0}{1}: [client-orch-state] [26328]: (note): MAC: 3423.874c.6bf7 C
2021/09/28 12:59:51.782357 {wncd_x_R0-0}{1}: [dot11-validate] [26328]: (info): MAC: 3423.874c.6bf7 WiFi
2021/09/28 12:59:51.782480 {wncd_x_R0-0}{1}: [dot11] [26328]: (debug): MAC: 3423.874c.6bf7 dot11 send a

Sending association response with resp_status_code: 0


2021/09/28 12:59:51.782483 {wncd_x_R0-0}{1}: [dot11] [26328]: (debug): MAC: 3423.874c.6bf7 Dot11 Capabi
2021/09/28 12:59:51.782509 {wncd_x_R0-0}{1}: [dot11-frame] [26328]: (info): MAC: 3423.874c.6bf7 WiFi di
2021/09/28 12:59:51.782519 {wncd_x_R0-0}{1}: [dot11] [26328]: (info): MAC: 3423.874c.6bf7 dot11 send as
2021/09/28 12:59:51.782611 {wncd_x_R0-0}{1}: [dot11] [26328]: (note): MAC: 3423.874c.6bf7

Association success. AID 1

, Roaming = False, WGB = False, 11r = False, 11w = False
2021/09/28 12:59:51.782626 {wncd_x_R0-0}{1}: [dot11] [26328]: (info): MAC: 3423.874c.6bf7 DOT11 state t
2021/09/28 12:59:51.782676 {wncd_x_R0-0}{1}: [client-orch-sm] [26328]: (debug): MAC: 3423.874c.6bf7

Station Dot11 association is successful.
```

Layer-2-Authentifizierung übersprungen:

<#root>

```
2021/09/28 12:59:51.782727 {wncd_x_R0-0}{1}: [client-orch-sm] [26328]: (debug): MAC: 3423.874c.6bf7 Sta
2021/09/28 12:59:51.782745 {wncd_x_R0-0}{1}: [client-orch-state] [26328]: (note): MAC: 3423.874c.6bf7 C
2021/09/28 12:59:51.782785 {wncd_x_R0-0}{1}: [client-auth] [26328]: (note): MAC: 3423.874c.6bf7

L2 Authentication initiated. method WEBAUTH

, Policy VLAN 2621,AAA override = 0
```

```
2021/09/28 12:59:51.782803 {wncd_x_R0-0}{1}: [sanet-shim-translate] [26328]: (ERR): 3423.874c.6bf7 wlan
[...]
2021/09/28 12:59:51.787912 {wncd_x_R0-0}{1}: [client-auth] [26328]: (info): MAC: 3423.874c.6bf7 Client
2021/09/28 12:59:51.787953 {wncd_x_R0-0}{1}: [client-auth] [26328]: (info): MAC: 3423.874c.6bf7 Client
2021/09/28 12:59:51.787966 {wncd_x_R0-0}{1}: [client-orch-sm] [26328]: (debug): MAC: 3423.874c.6bf7
```

L2 Authentication of station is successful., L3 Authentication : 1

ACL-Plumb:

<#root>

```
2021/09/28 12:59:51.785227 {wncd_x_R0-0}{1}: [webauth-sm] [26328]: (info): [ 0.0.0.0]Starting Webauth,
2021/09/28 12:59:51.785307 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [26328]: (info): [0000.0000.0000:
2021/09/28 12:59:51.785378 {wncd_x_R0-0}{1}: [webauth-acl] [26328]: (info): capwap_9000000b[3423.874c.6
```

Applying IPv4 intercept ACL via SVM, name: WA-v4-int-172.16.80.8

```
, priority: 50, IIF-ID: 0
2021/09/28 12:59:51.785738 {wncd_x_R0-0}{1}: [epm-redirect] [26328]: (info): [0000.0000.0000:unknown]
```

URL-Redirect-ACL = WA-v4-int-172.16.80.8

```
2021/09/28 12:59:51.786324 {wncd_x_R0-0}{1}: [webauth-acl] [26328]: (info): capwap_9000000b[3423.874c.6
```

Applying IPv6 intercept ACL via SVM, name: IP-Adm-V6-Int-ACL-global, priority: 52

```
, IIF-ID: 0
2021/09/28 12:59:51.786598 {wncd_x_R0-0}{1}: [epm-redirect] [26328]: (info): [0000.0000.0000:unknown]
```

URL-Redirect-ACL = IP-Adm-V6-Int-ACL-global

```
2021/09/28 12:59:51.787904 {wncd_x_R0-0}{1}: [client-auth] [26328]: (info): MAC: 3423.874c.6bf7 Client
```

IP-Lernprozess:

<#root>

```
2021/09/28 12:59:51.799515 {wncd_x_R0-0}{1}: [client-orch-state] [26328]: (note): MAC: 3423.874c.6bf7 C
2021/09/28 12:59:51.799716 {wncd_x_R0-0}{1}: [client-iplearn] [26328]: (info): MAC: 3423.874c.6bf7
```

IP-learn state transition: S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS

```
2021/09/28 12:59:51.802213 {wncd_x_R0-0}{1}: [client-auth] [26328]: (info): MAC: 3423.874c.6bf7 Client
2021/09/28 12:59:51.916777 {wncd_x_R0-0}{1}: [sisf-packet] [26328]: (debug): RX: ARP from interface capw
[...]
2021/09/28 12:59:52.810136 {wncd_x_R0-0}{1}: [client-iplearn] [26328]: (note): MAC: 3423.874c.6bf7
```

Client IP learn successful. Method: ARP IP: 172.16.21.153

```
2021/09/28 12:59:52.810185 {wncd_x_R0-0}{1}: [epm] [26328]: (info): [0000.0000.0000:unknown] HDL = 0x0
2021/09/28 12:59:52.810404 {wncd_x_R0-0}{1}: [auth-mgr] [26328]: (info): [3423.874c.6bf7:capwap_900000
2021/09/28 12:59:52.810794 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [26328]: (info): [0000.0000.0000:
2021/09/28 12:59:52.810863 {wncd_x_R0-0}{1}: [client-iplearn] [26328]: (info): MAC: 3423.874c.6bf7
```

IP-learn state transition: S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE

Layer-3-Authentifizierungs- und Umleitungsprozess:

<#root>

2021/09/28 12:59:52.811141 {wncd_x_R0-0}{1}: [client-auth] [26328]: (note): MAC: 3423.874c.6bf7

L3 Authentication initiated. LWA

2021/09/28 12:59:52.811154 {wncd_x_R0-0}{1}: [client-auth] [26328]: (info): MAC: 3423.874c.6bf7 Client
2021/09/28 12:59:55.324550 {wncd_x_R0-0}{1}: [webauth-httpd] [26328]: (info): capwap_9000000b[3423.874c
2021/09/28 12:59:55.324565 {wncd_x_R0-0}{1}: [webauth-httpd] [26328]: (info): capwap_9000000b[3423.874c

HTTP GET request

2021/09/28 12:59:55.324588 {wncd_x_R0-0}{1}: [webauth-httpd] [26328]: (info): capwap_9000000b[3423.874c
[...]
2021/09/28 13:01:29.859434 {wncd_x_R0-0}{1}: [webauth-httpd] [26328]: (info): capwap_9000000b[3423.874c

POST rcvd when in LOGIN state

2021/09/28 13:01:29.859636 {wncd_x_R0-0}{1}: [webauth-acl] [26328]: (info): capwap_9000000b[3423.874c.6
2021/09/28 13:01:29.860335 {wncd_x_R0-0}{1}: [webauth-acl] [26328]: (info): capwap_9000000b[3423.874c.6
2021/09/28 13:01:29.861092 {wncd_x_R0-0}{1}: [auth-mgr] [26328]: (info): [3423.874c.6bf7:capwap_900000

Authc success from WebAuth, Auth event success

2021/09/28 13:01:29.861151 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [26328]: (note): Authentication Success.
2021/09/28 13:01:29.862867 {wncd_x_R0-0}{1}: [client-auth] [26328]: (note): MAC: 3423.874c.6bf7

L3 Authentication Successful.

ACL:[]
2021/09/28 13:01:29.862871 {wncd_x_R0-0}{1}: [client-auth] [26328]: (info): MAC: 3423.874c.6bf7

Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH_DONE

Übergang in den RUN-Status:

<#root>

2021/09/28 13:01:29.863176 {wncd_x_R0-0}{1}: [client-auth] [26328]: (note): MAC: 3423.874c.6bf7 ADD MOB
2021/09/28 13:01:29.863272 {wncd_x_R0-0}{1}: [errmsg] [26328]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_

Username entry (3423.874C.6BF7) joined with ssid (EWA-Guest) for device with MAC: 3423.874c.6bf7

2021/09/28 13:01:29.863334 {wncd_x_R0-0}{1}: [aaa-attr-inf] [26328]: (info): [Applied attribute :bsn-v
2021/09/28 13:01:29.863336 {wncd_x_R0-0}{1}: [aaa-attr-inf] [26328]: (info): [Applied attribute : time
2021/09/28 13:01:29.863343 {wncd_x_R0-0}{1}: [aaa-attr-inf] [26328]: (info): [Applied attribute : url-
2021/09/28 13:01:29.863387 {wncd_x_R0-0}{1}: [ewlc-qos-client] [26328]: (info): MAC: 3423.874c.6bf7 Cli
2021/09/28 13:01:29.863409 {wncd_x_R0-0}{1}: [rog-proxy-capwap] [26328]: (debug):

Managed client RUN state notification

: 3423.874c.6bf7
2021/09/28 13:01:29.863451 {wncd_x_R0-0}{1}: [client-orch-state] [26328]: (note): MAC: 3423.874c.6bf7

Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.