Configurazione e risoluzione dei problemi di autenticazione Web esterna su 9800 WLC

Sommario

Introduzione

In questo documento viene descritto come configurare e risolvere i problemi di autenticazione Web esterna (EWA) su un controller Catalyst 9800 Wireless LAN Controller (WLC).

Prerequisiti

In questo documento si presume che il server Web sia configurato correttamente per consentire le comunicazioni esterne e che la pagina Web sia configurata correttamente per inviare tutti i parametri necessari al WLC per autenticare l'utente e spostare le sessioni client allo stato RUN.

Nota: poiché l'accesso alle risorse esterne è limitato dal WLC attraverso le autorizzazioni dell'elenco degli accessi, tutti gli script, i tipi di carattere, le immagini e così via. che vengono utilizzati nella pagina Web devono essere scaricati e rimanere locali sul server Web.

I parametri necessari per l'autenticazione dell'utente sono:

- buttonClicked: per consentire al WLC di rilevare l'azione come tentativo di autenticazione, questo parametro deve essere impostato sul valore "4".
- redirectUrl: il valore di questo parametro viene utilizzato dal controller per indirizzare il client a un sito Web specifico dopo la corretta autenticazione.
- err_flag: questo parametro viene utilizzato per indicare alcuni errori, ad esempio informazioni incomplete o credenziali non corrette. In caso di autenticazioni riuscite, viene impostato su "0".
- username: questo parametro viene utilizzato solo per le mappe di parametri webauth. Se la mappa di parametri è impostata su consenso, può essere ignorata. Deve essere compilato con il nome utente del client wireless.
- password: questo parametro viene utilizzato solo per le mappe di parametri webauth. Se la mappa di parametri è impostata su Consenso, può essere ignorata. Deve essere compilato con la password del client wireless.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Sviluppo Web Hyper Text Markup Language (HTML)
- Funzioni wireless Cisco IOS®-XE
- Strumenti di sviluppo per browser Web

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- C9800-CL WLC Cisco IOS®-XE versione 17.3.3
- Microsoft Windows Server 2012 con funzionalità di Internet Information Services (IIS)
- Access point 2802 e 9117

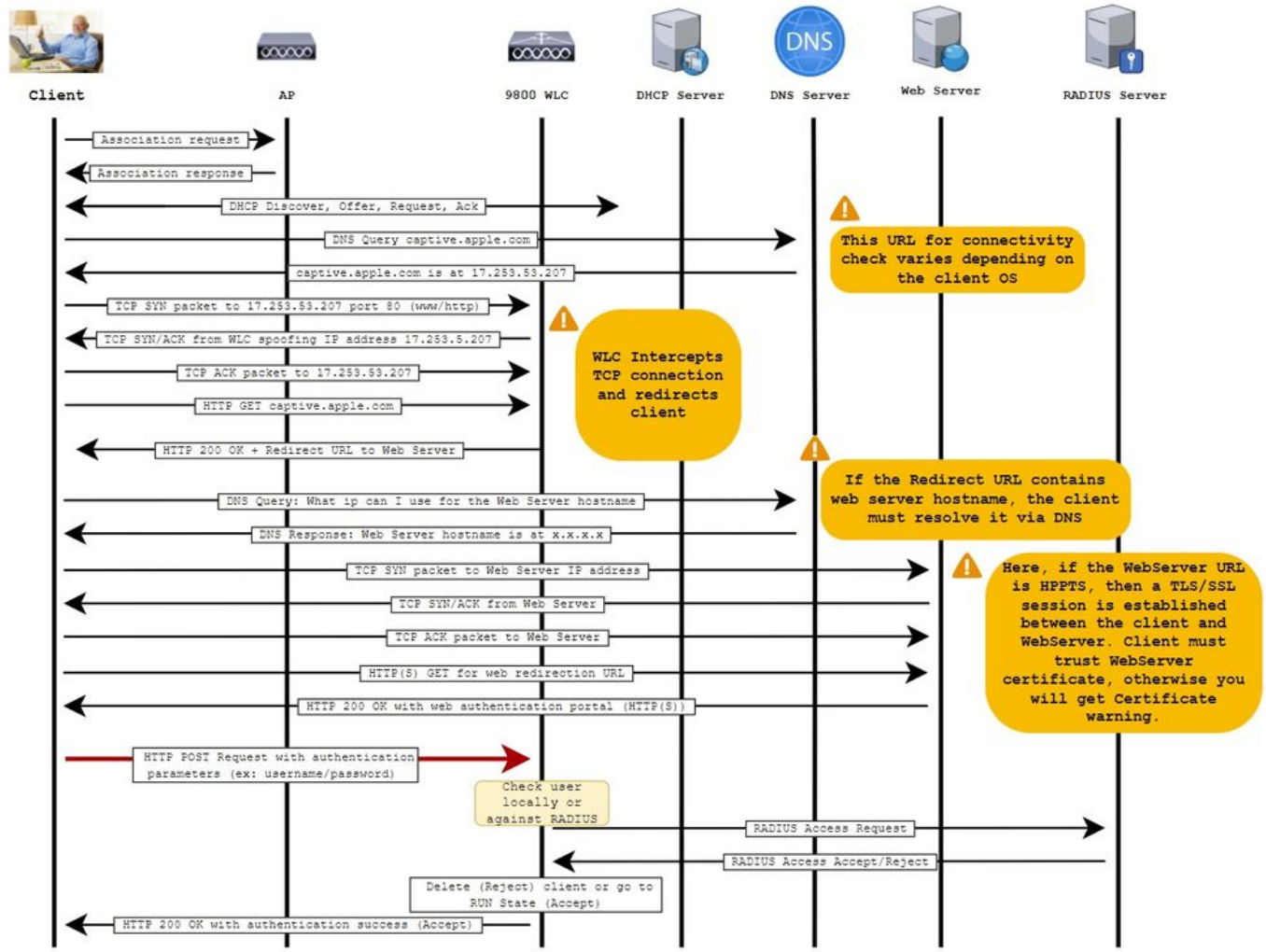
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

L'autenticazione Web esterna sfrutta un portale Web ospitato al di fuori del WLC su un server Web dedicato o su server multifunzione come Identity Services Engine (ISE) che consentono l'accesso granulare e la gestione dei componenti Web. Nell'immagine viene eseguito il rendering dell'handshake relativo alla connessione di un client a una WLAN di autenticazione Web esterna. Nell'immagine sono elencate le interazioni sequenziali tra client wireless, WLC, server DNS (Domain Name System) che risolve URL (Uniform Resource Location) e server Web in cui WLC convalida le credenziali utente localmente. Questo flusso di lavoro è utile per risolvere eventuali

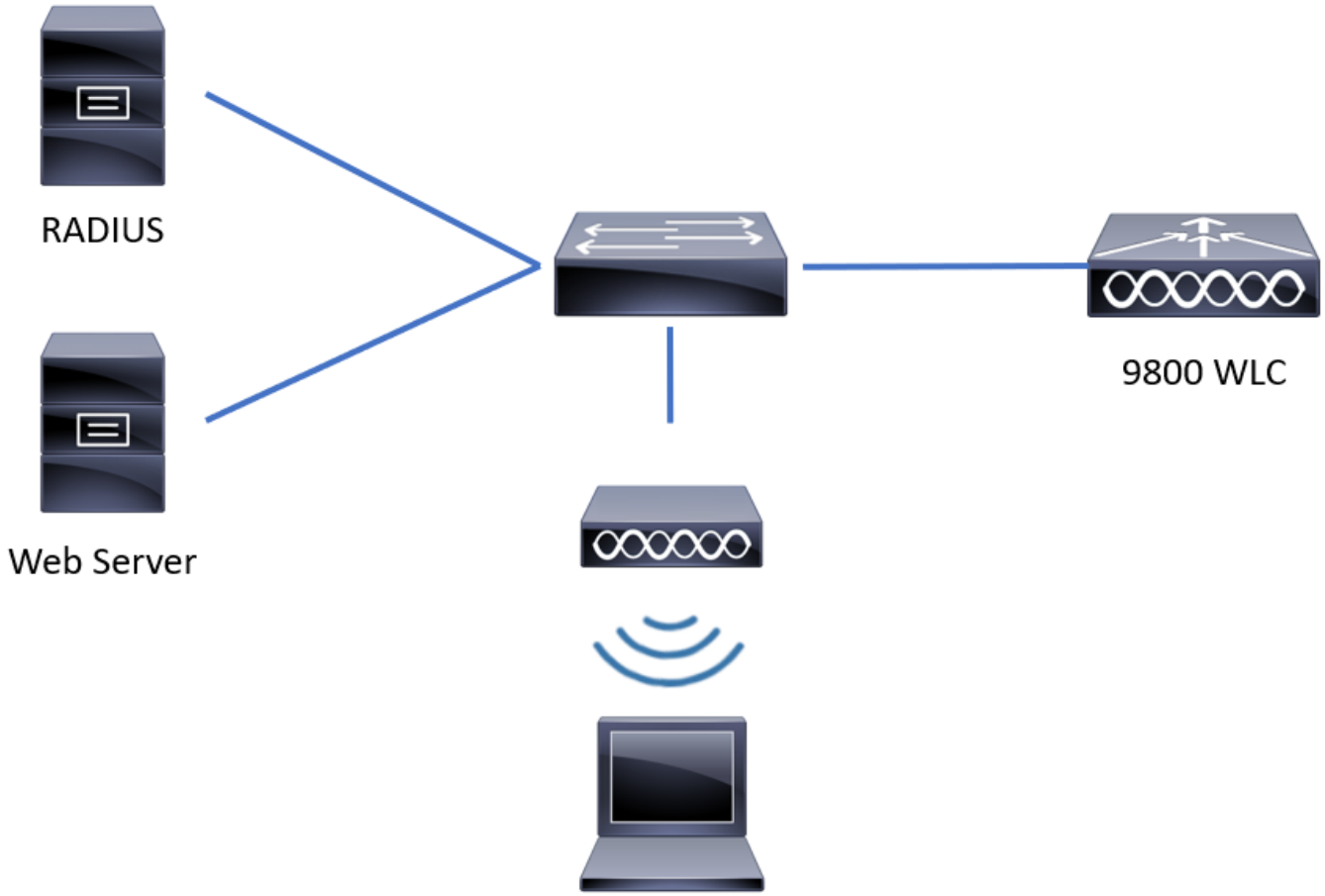
problemi di errore.

Nota: prima della chiamata HTTP POST dal client al WLC, se nella mappa dei parametri è abilitata l'autenticazione Web sicura e il WLC non ha un trust point firmato da un'Autorità di certificazione attendibile, nel browser viene visualizzato un avviso di sicurezza. Il client deve ignorare questo avviso e accettare il reinvio del modulo affinché il controller possa mettere le sessioni client in stato RUN.



Configurazione

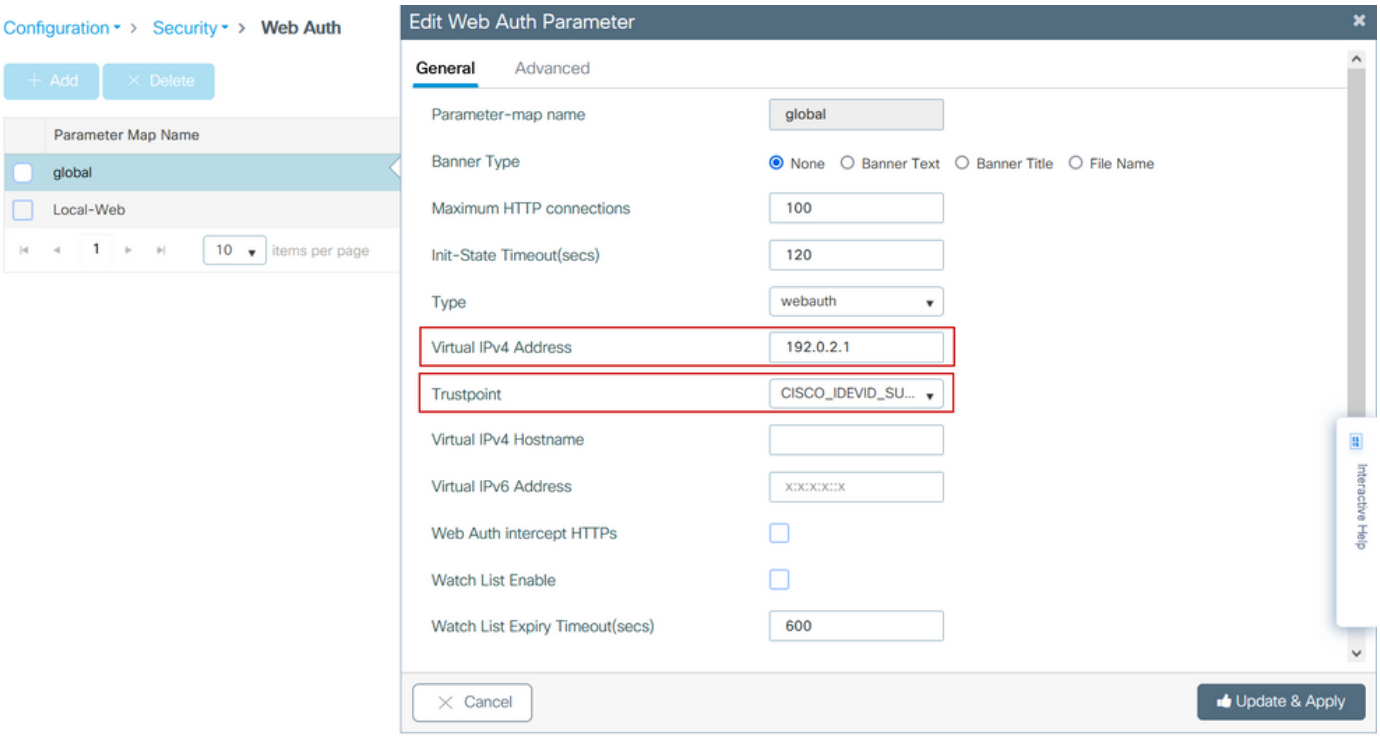
Esempio di rete



Configura impostazioni parametri Web

Passaggio 1. Passare a Configurazione > Sicurezza > Web Auth e scegliere la mappa dei parametri globali. Verificare che l'indirizzo IPv4 virtuale e il trust point siano configurati in modo da fornire le funzionalità di reindirizzamento appropriate.

Nota: per impostazione predefinita, i browser utilizzano un sito Web HTTP per avviare il processo di reindirizzamento. Se è necessario il reindirizzamento HTTPS, è necessario controllare l'intercettazione HTTP da parte dell'autenticazione Web. Questa configurazione non è tuttavia consigliata in quanto aumenta l'utilizzo della CPU.

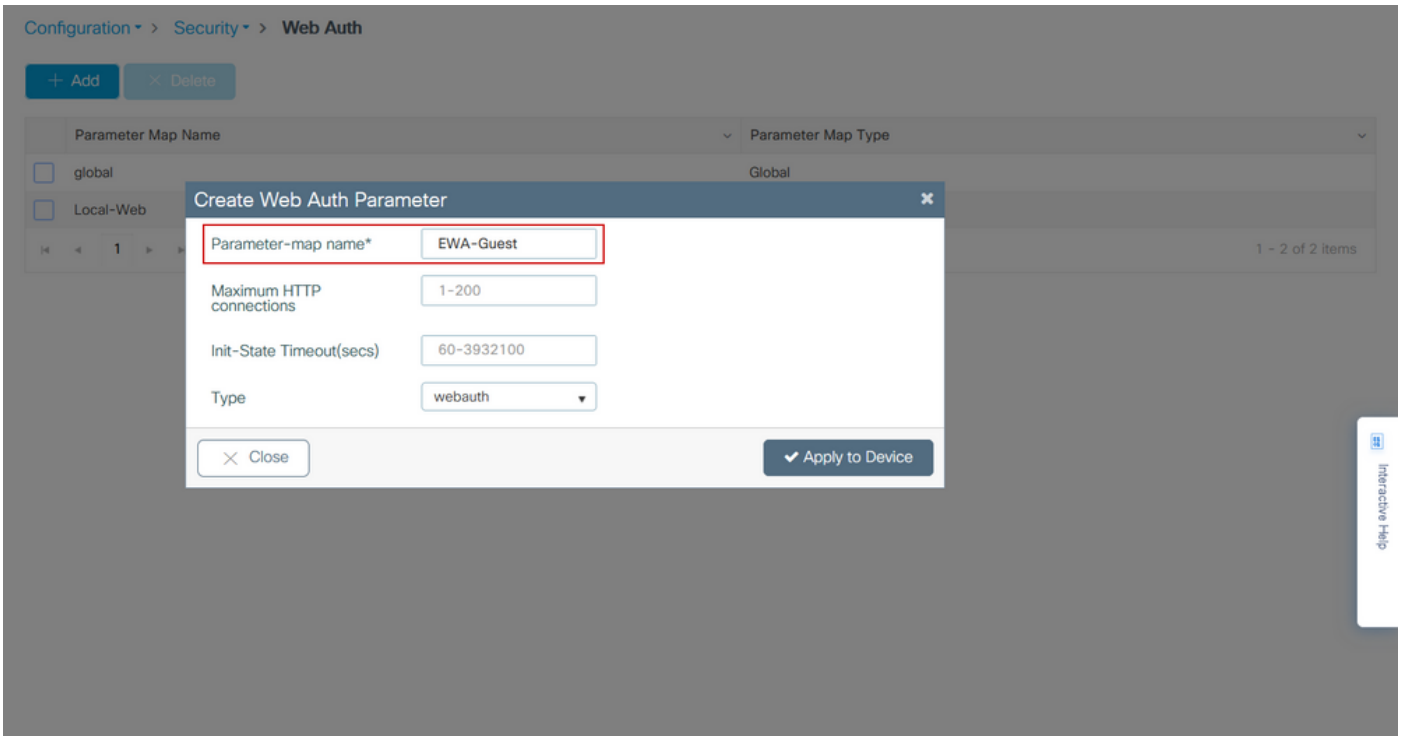


Configurazione dalla CLI:

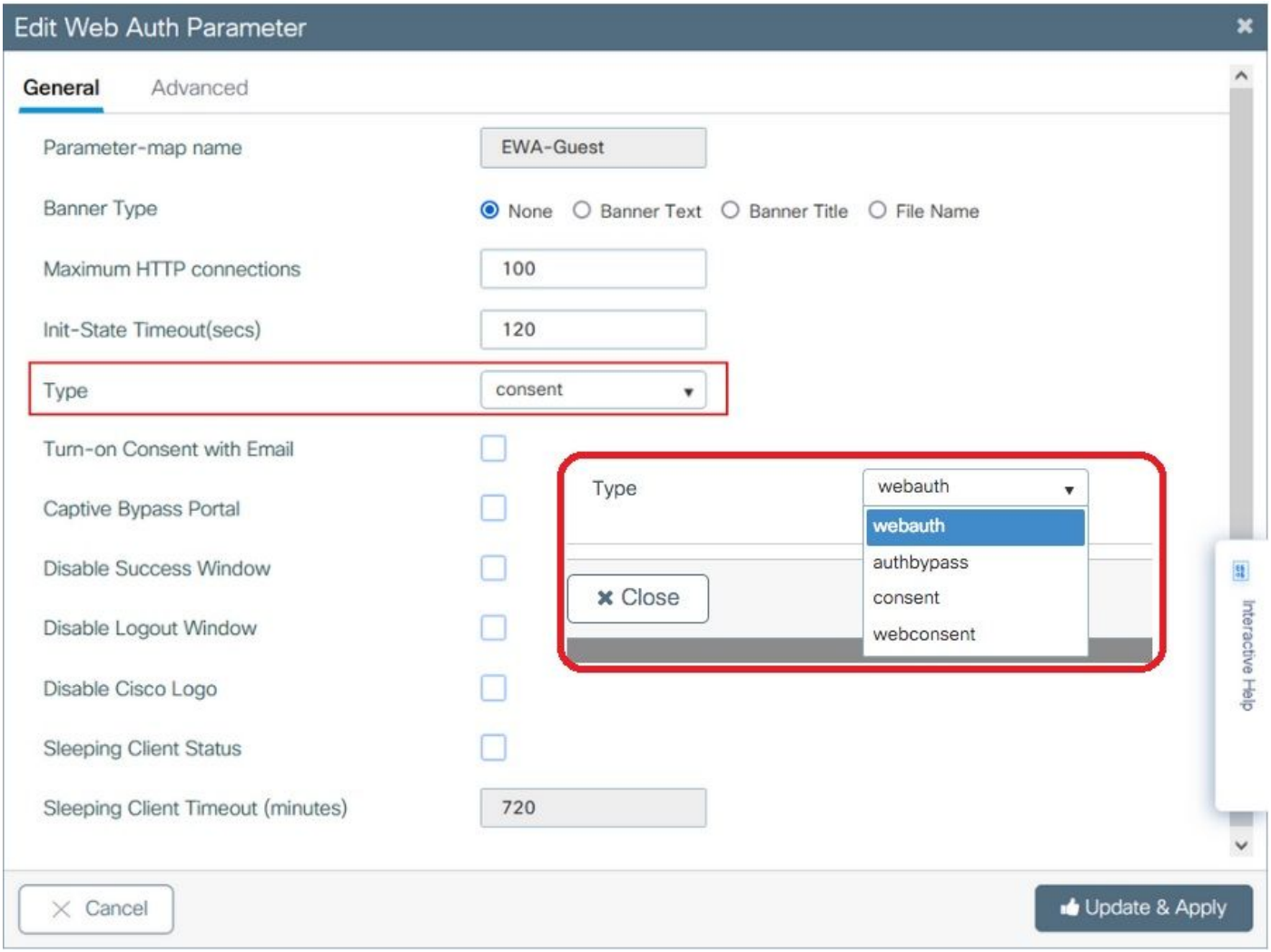
<#root>

```
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
```

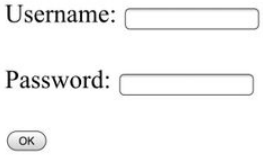
Passaggio 2. Selezionare + Aggiungi e configurare un nome per la nuova mappa dei parametri che punta al server esterno. Facoltativamente, configurare il numero massimo di errori di autenticazione HTTP prima che il client venga escluso e il tempo (in secondi) per cui un client può rimanere nello stato di autenticazione Web.



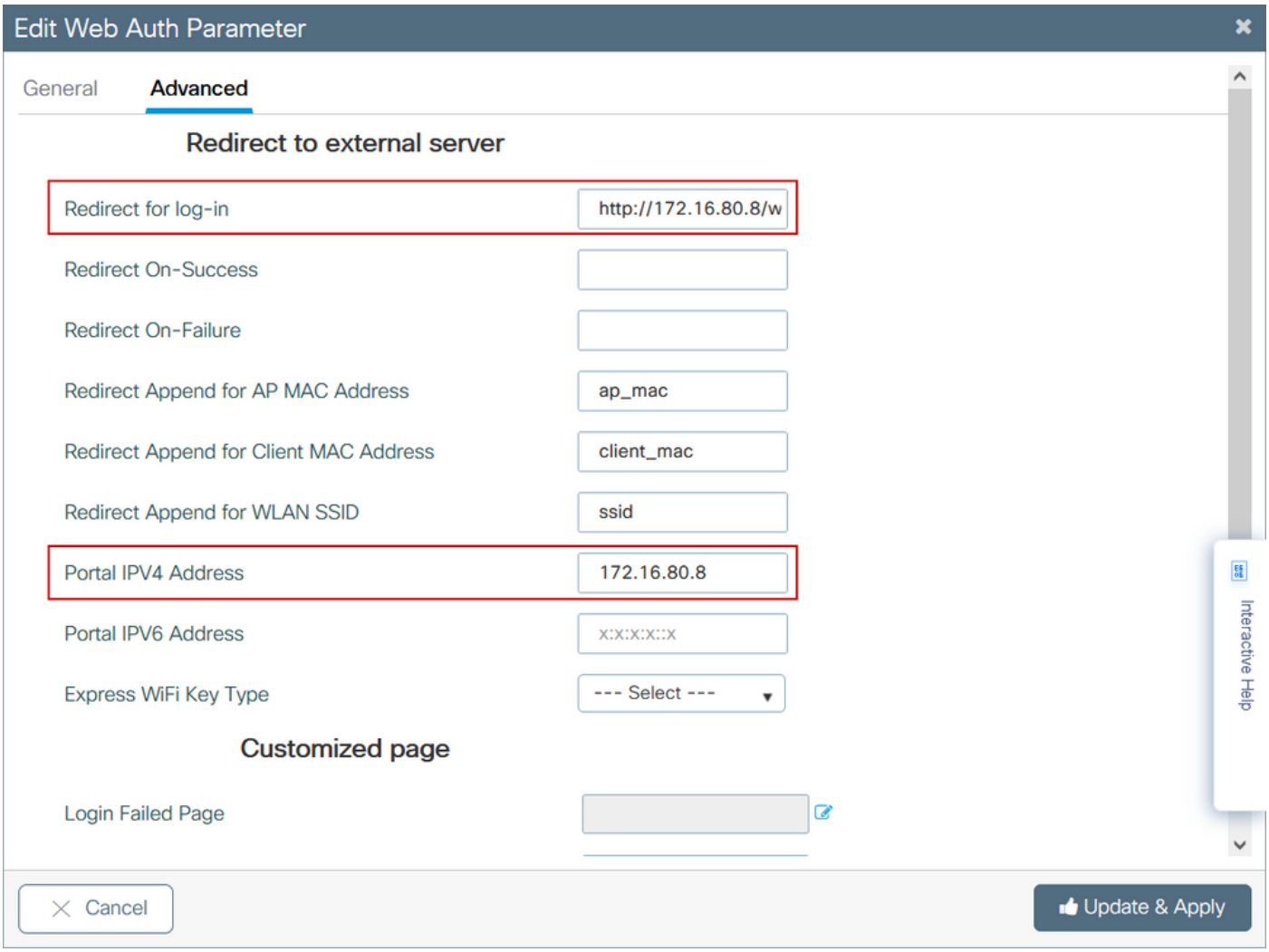
Passaggio 3. Selezionare la mappa dei parametri appena creata nella scheda Generale e configurare il tipo di autenticazione dall'elenco a discesa Tipo.



- Parameter-map name = Nome assegnato alla mappa Parameter WebAuth
- Numero massimo di connessioni HTTP = Numero di errori di autenticazione prima che il client venga escluso
- Timeout stato inizializzazione (sec) = secondi in cui un client può trovarsi nello stato di autenticazione Web
- Tipo = Tipo di autenticazione Web

webauth	authbypass	consenso	consenso Web
	Il client si connette al SSID e ottiene un indirizzo IP, quindi il WLC 9800 verifica se l'indirizzo MAC è autorizzato ad accedere al rete, se sì, viene spostata allo stato RUN, se non è non è autorizzato a partecipare. (non fallback all'autenticazione Web)		

Passaggio 4. Dalla scheda Advanced (Avanzate)configurare il reindirizzamento per l'indirizzo IPV4 di accesso e l'indirizzo IP del sito del server specifico rispettivamente.



Configurazione CLI per i passaggi 2, 3 e 4:

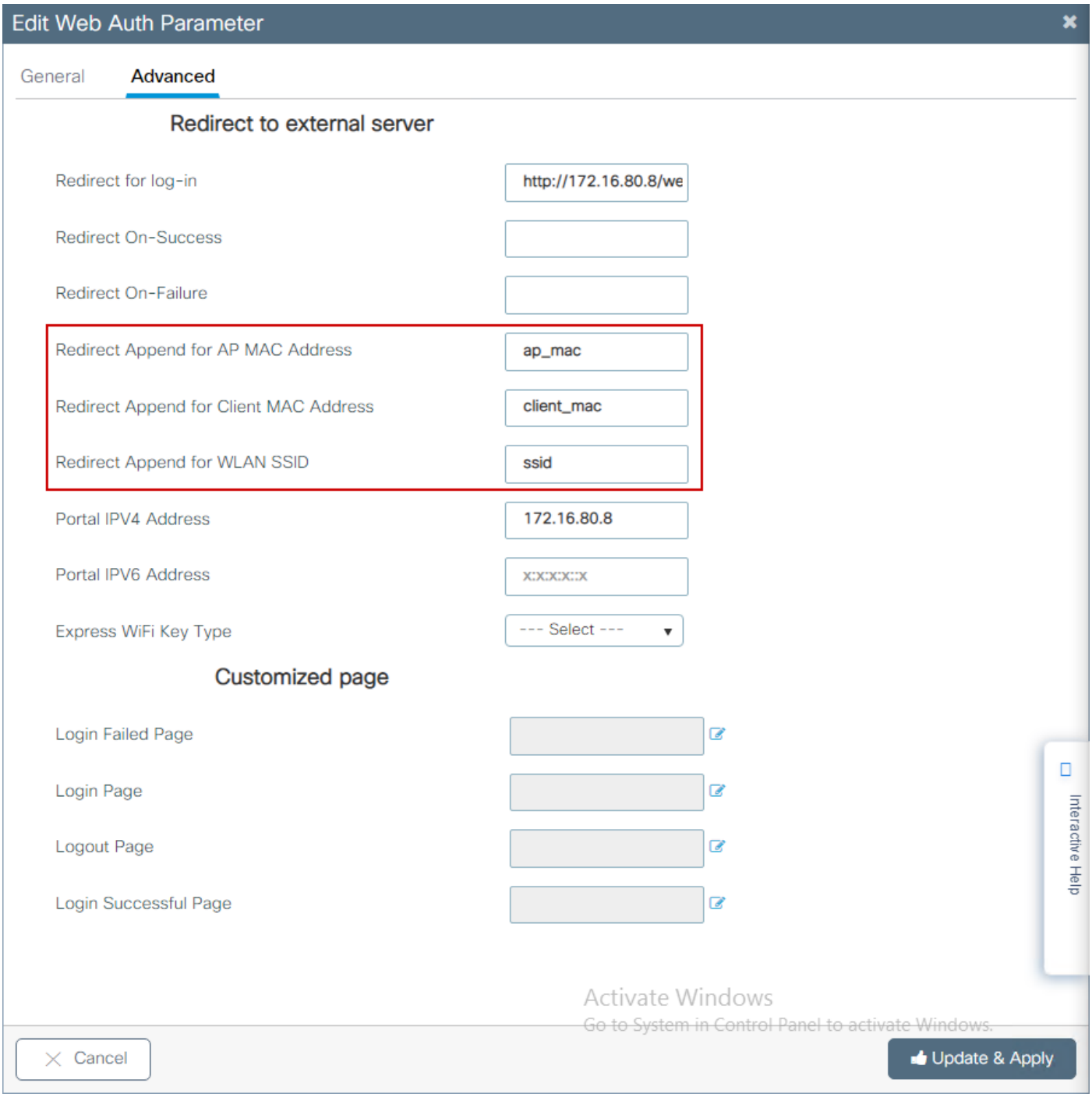
<#root>

```
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
```

Passaggio 5. (Facoltativo) Il WLC può inviare i parametri aggiuntivi tramite la stringa di query. Questa operazione è spesso necessaria per rendere 9800 compatibile con portali esterni di terze parti. I campi "Redirect Append for AP MAC Address", "Redirect Append for Client MAC Address" e "Redirect Append for WLAN SSID" consentono di aggiungere parametri aggiuntivi all'ACL di

reindirizzamento con un nome personalizzato. Selezionare la mappa dei parametri appena creata e passare alla scheda Avanzate, quindi configurare il nome dei parametri necessari. I parametri disponibili sono:

- Indirizzo MAC AP (in formato aa:bb:cc:dd:ee:ff)
- Indirizzo MAC client (in formato aa:bb:cc:dd:ee:ff)
- Nome SSID



Configurazione dalla CLI:

<#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
```

Per questo esempio, l'URL di reindirizzamento inviato al client determina:

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

Nota: quando si aggiungono le informazioni sull'indirizzo IPV4 del portale, viene aggiunto automaticamente un ACL che consente il traffico HTTP e HTTPS dai client wireless al server di autenticazione Web esterno, quindi non è necessario configurare altri ACL di pre-autenticazione. Se si desidera consentire l'utilizzo di più indirizzi IP o URL, l'unica opzione disponibile è configurare un filtro URL in modo che vengano consentiti tutti gli IP corrispondenti agli URL specificati prima dell'autenticazione. Non è possibile aggiungere staticamente più indirizzi IP di un portale a meno che non si utilizzino filtri URL.

Nota: la mappa dei parametri globali è l'unica in cui è possibile definire l'indirizzo IPv4 e IPv6 virtuale, HTTP intercettati da Webauth, portale di bypass vincolato, impostazioni di timeout di attivazione e scadenza dell'elenco di controllo.

Riepilogo della configurazione CLI:

Server Web locale

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

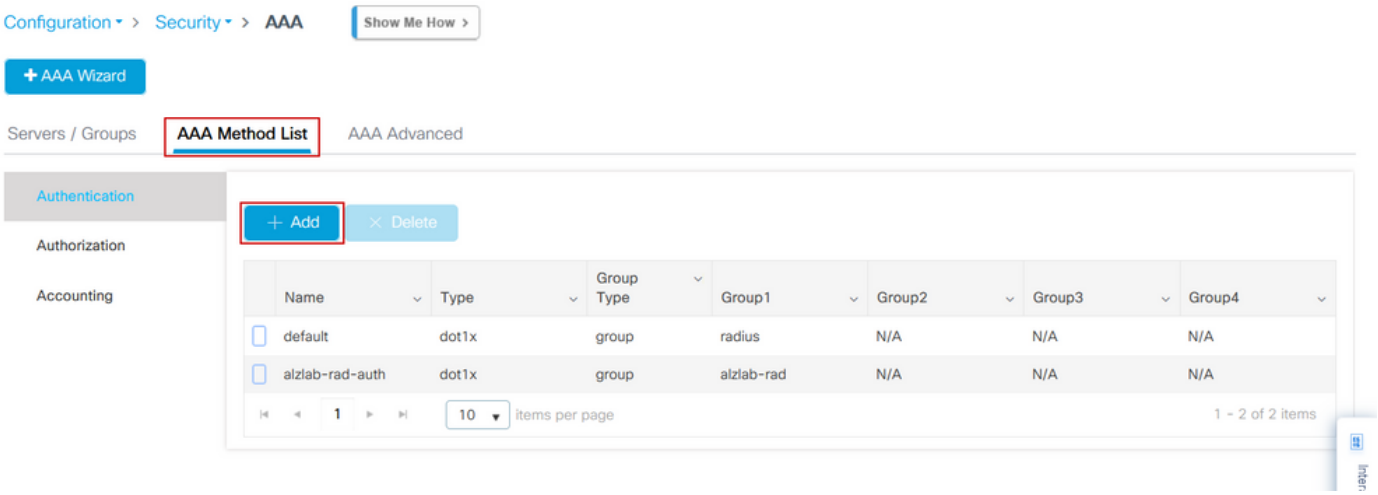
Server Web esterno

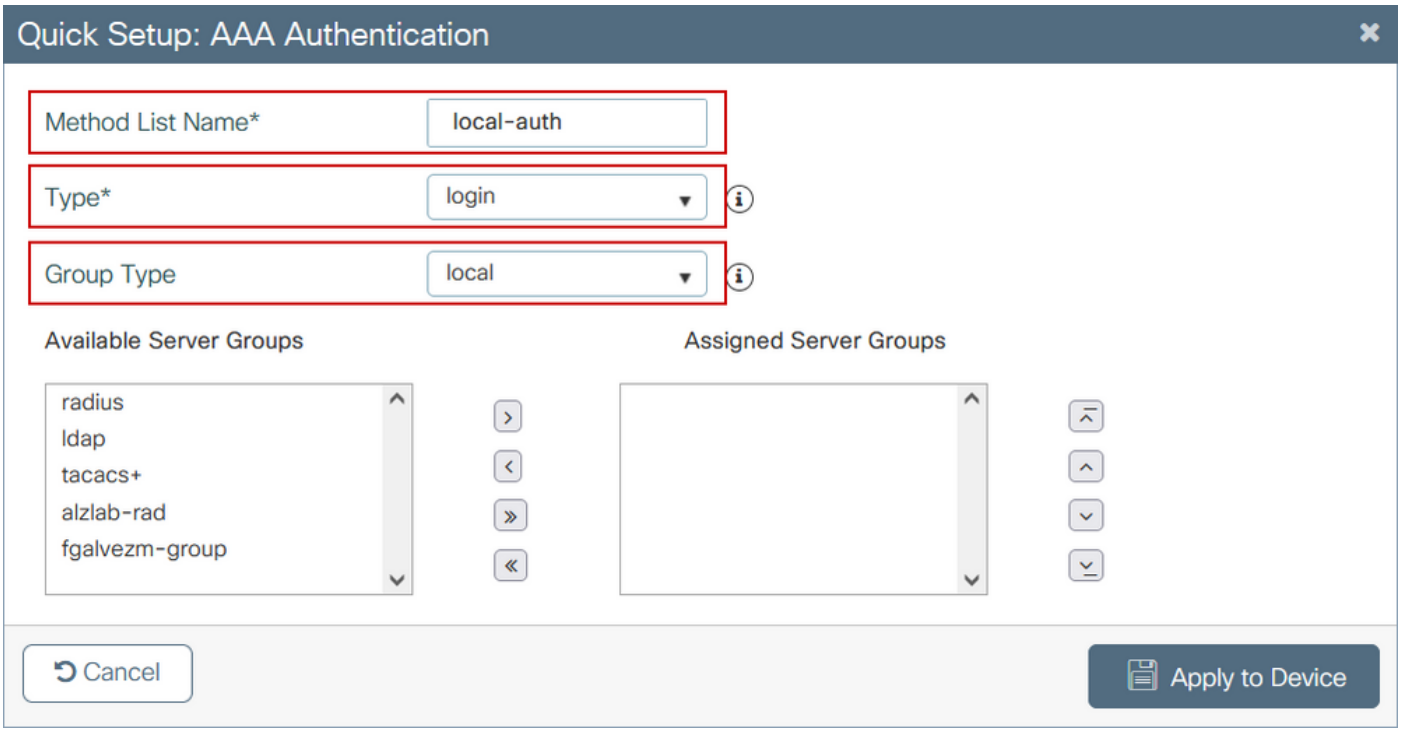
```
parameter-map type webauth <web-parameter-map-name>
 type webauth
 timeout init-state sec 300
 redirect for-login <URL-for-webauth>
 redirect portal ipv4 <external-server's-IP
 max-http-conns 10
```

Configurazione delle impostazioni AAA

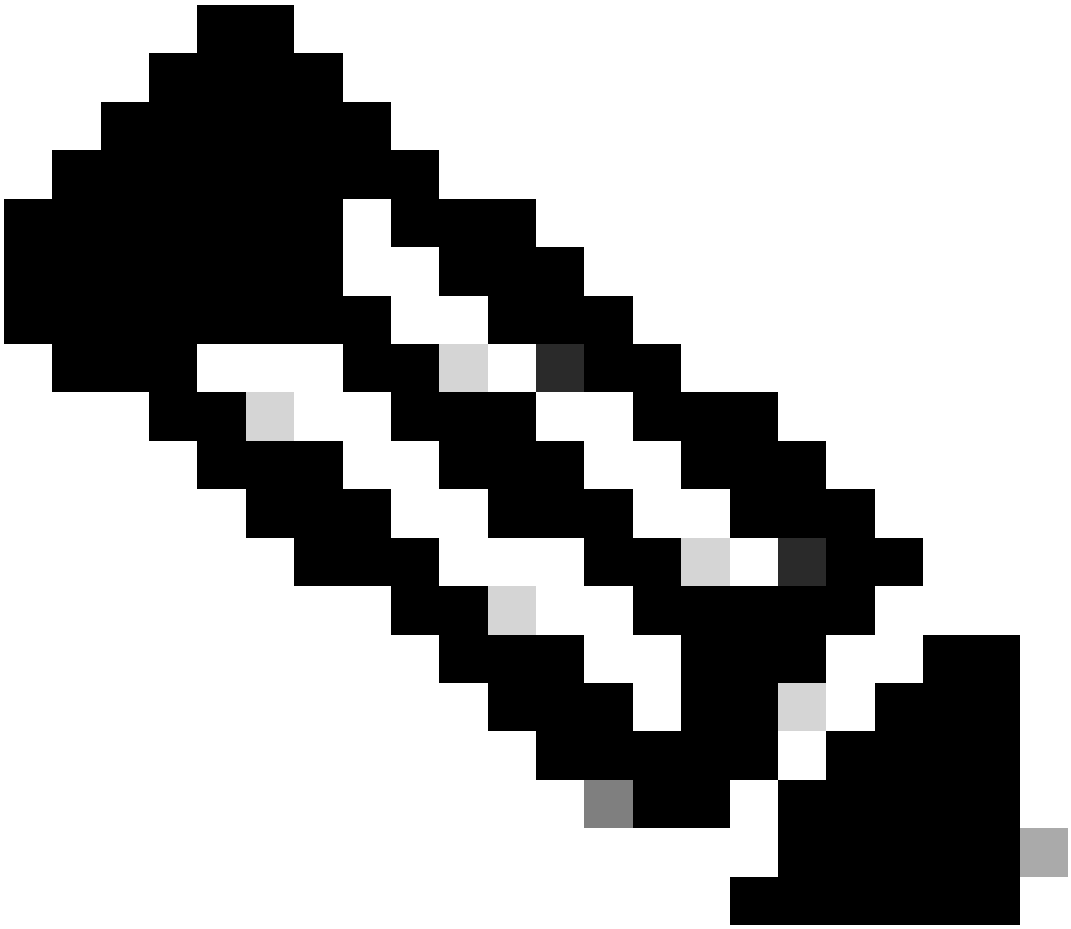
Questa sezione di configurazione è necessaria solo per le mappe di parametri configurate per il tipo di autenticazione webauth o webconsence.

Passaggio 1. Passare a Configurazione > Sicurezza > AAA, quindi selezionare Elenco metodi AAA. Configurare un nuovo elenco di metodi, selezionare + Aggiungi e inserire i dettagli dell'elenco; assicurarsi che Type sia impostato su "login" come mostrato nell'immagine.

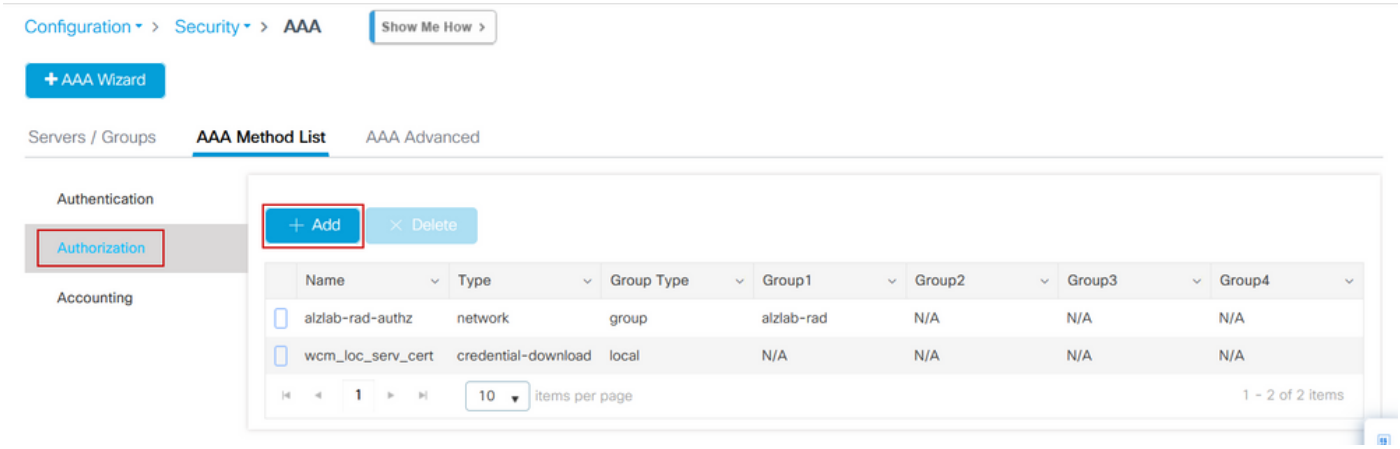


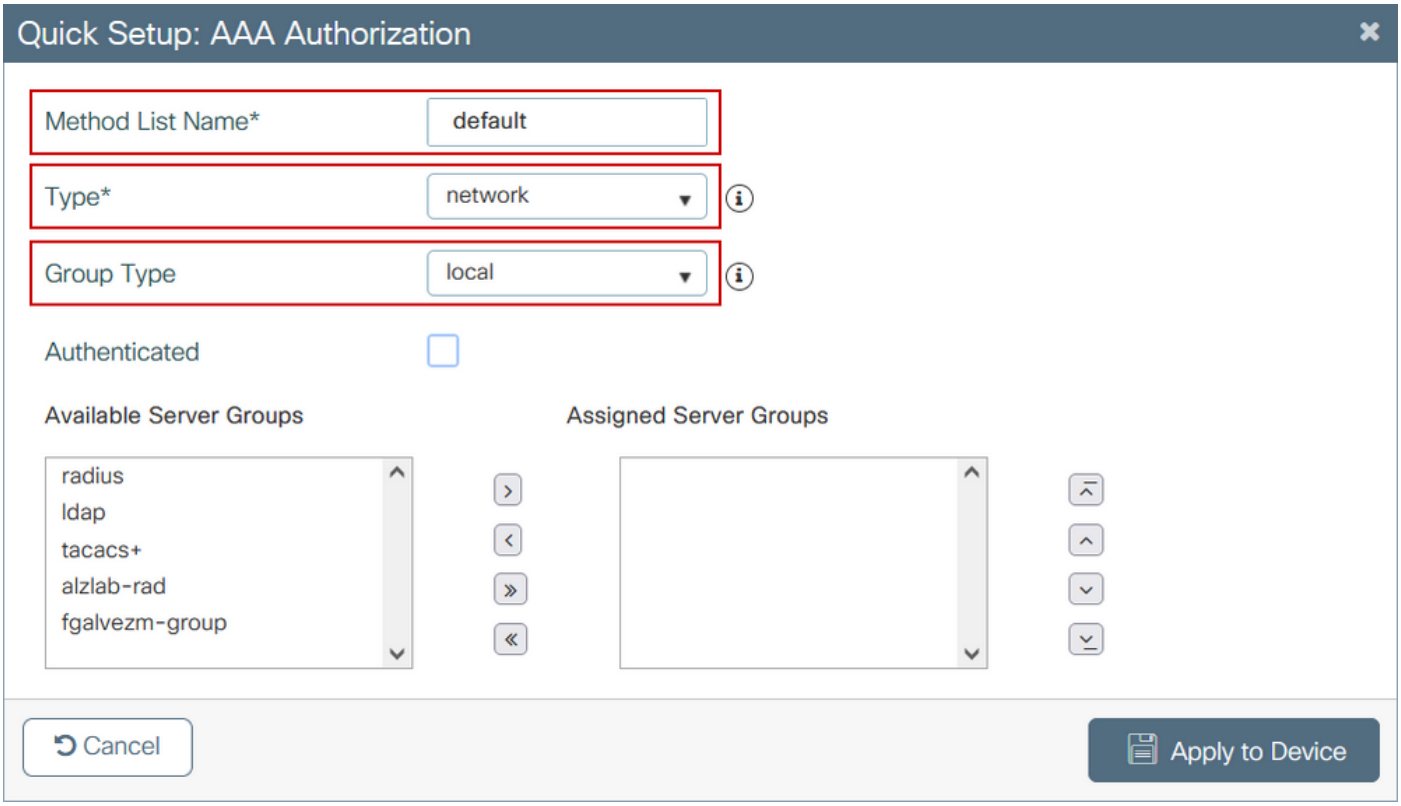


Passaggio 2. Selezionare Authorization (Autorizzazione), quindi selezionare + Add (Aggiungi) per creare un nuovo elenco di metodi. Assegnare al nome il nome predefinito con Tipo come rete, come mostrato nell'immagine.



Nota: come viene annunciato dal controller durante la configurazione della protezione WLAN di layer 3: per il corretto funzionamento dell'elenco dei metodi di accesso locale, verificare che nel dispositivo sia presente la configurazione 'aaa authorization network default local'. È quindi necessario definire l'elenco dei metodi di autorizzazione con il nome predefinito per configurare correttamente l'autenticazione Web locale. In questa sezione è configurato questo particolare elenco di metodi di autorizzazione.





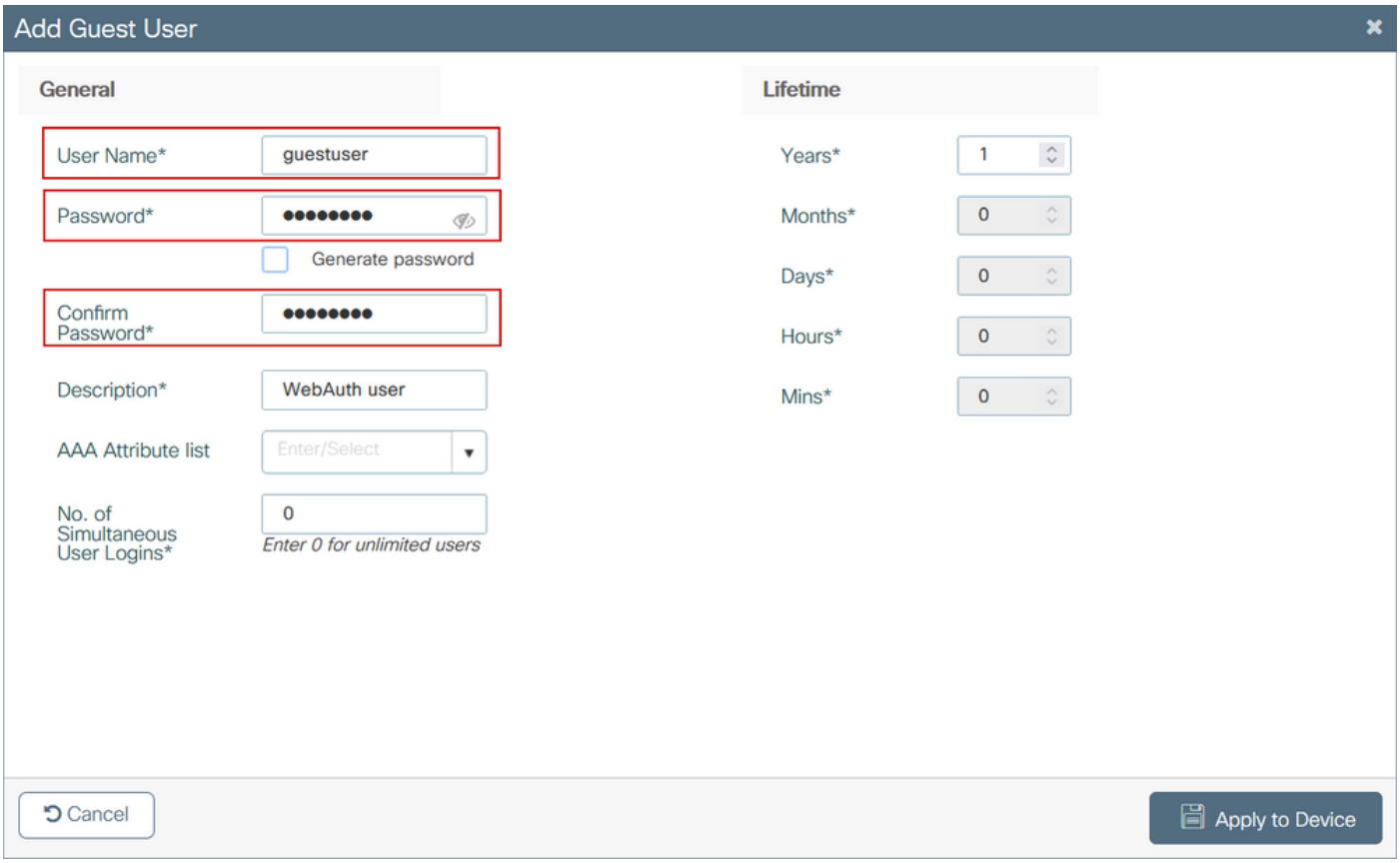
Configurazione CLI per i passaggi 1 e 2:

<#root>

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

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

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

Nota: se è necessaria l'autenticazione RADIUS esterna, leggere le seguenti istruzioni relative alla configurazione del server RADIUS su WLC 9800: configurazione AAA su WLC 9800. Verificare che per l'elenco dei metodi di autenticazione sia impostato il tipo "login" anziché il tipo dot1x.

Passaggio 3. Passare a Configurazione > Protezione > Utente guest. Selezionare + Aggiungi e configura i dettagli dell'account utente guest.



Configurazione dalla CLI:

<#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>
```

Passaggio 4. (Facoltativo) Quando si definisce la mappa dei parametri, vengono creati automaticamente un paio di elenchi di controllo di accesso (ACL). Questi ACL vengono usati per definire il traffico che attiva un reindirizzamento al server Web e il traffico che può passare. Se esistono requisiti specifici, ad esempio più indirizzi IP o filtri URL di server Web, selezionare Configurazione > Sicurezza > ACL select + Add and define needed rules; le istruzioni di autorizzazione vengono reindirizzate mentre le istruzioni di negazione definiscono il traffico che passa.

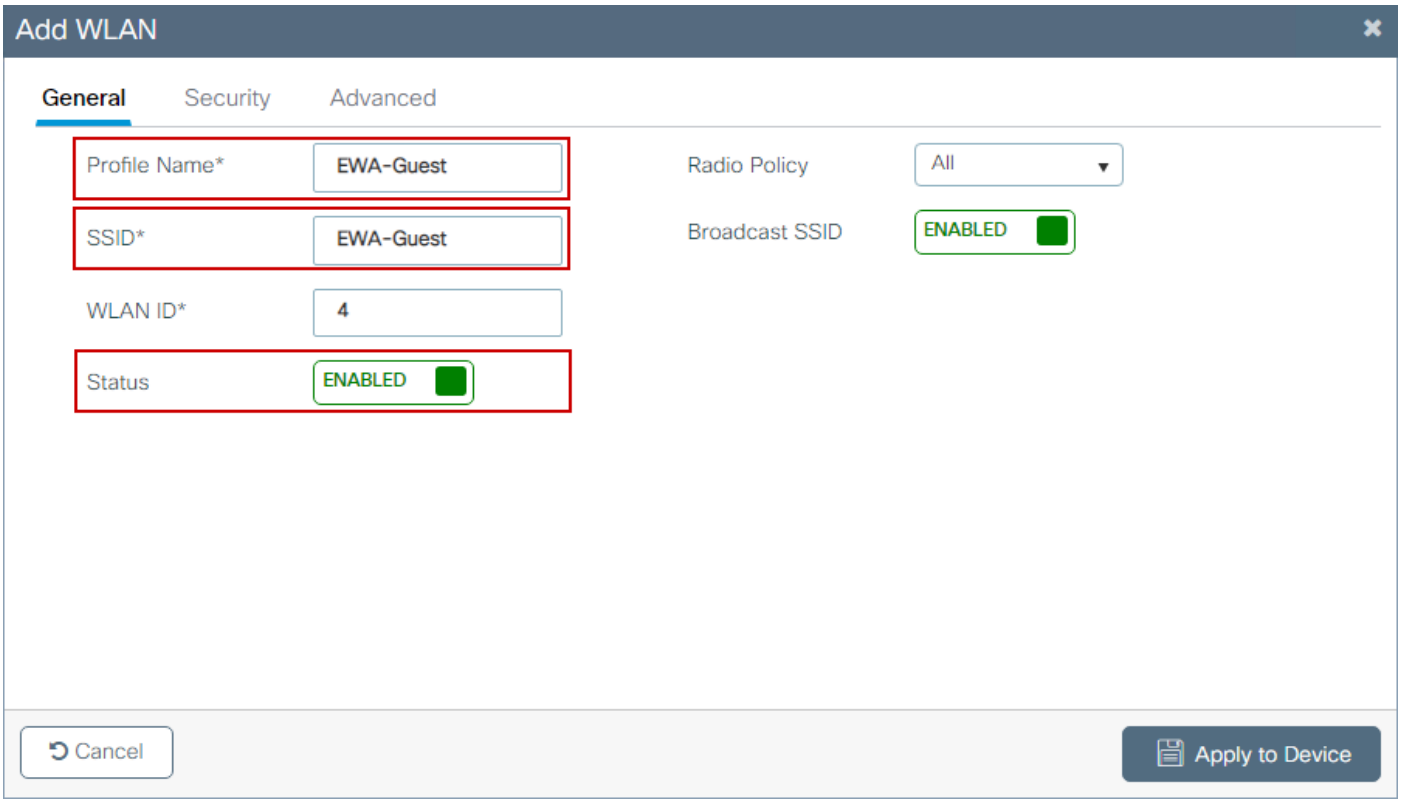
Le regole ACL create automaticamente sono:

<#root>

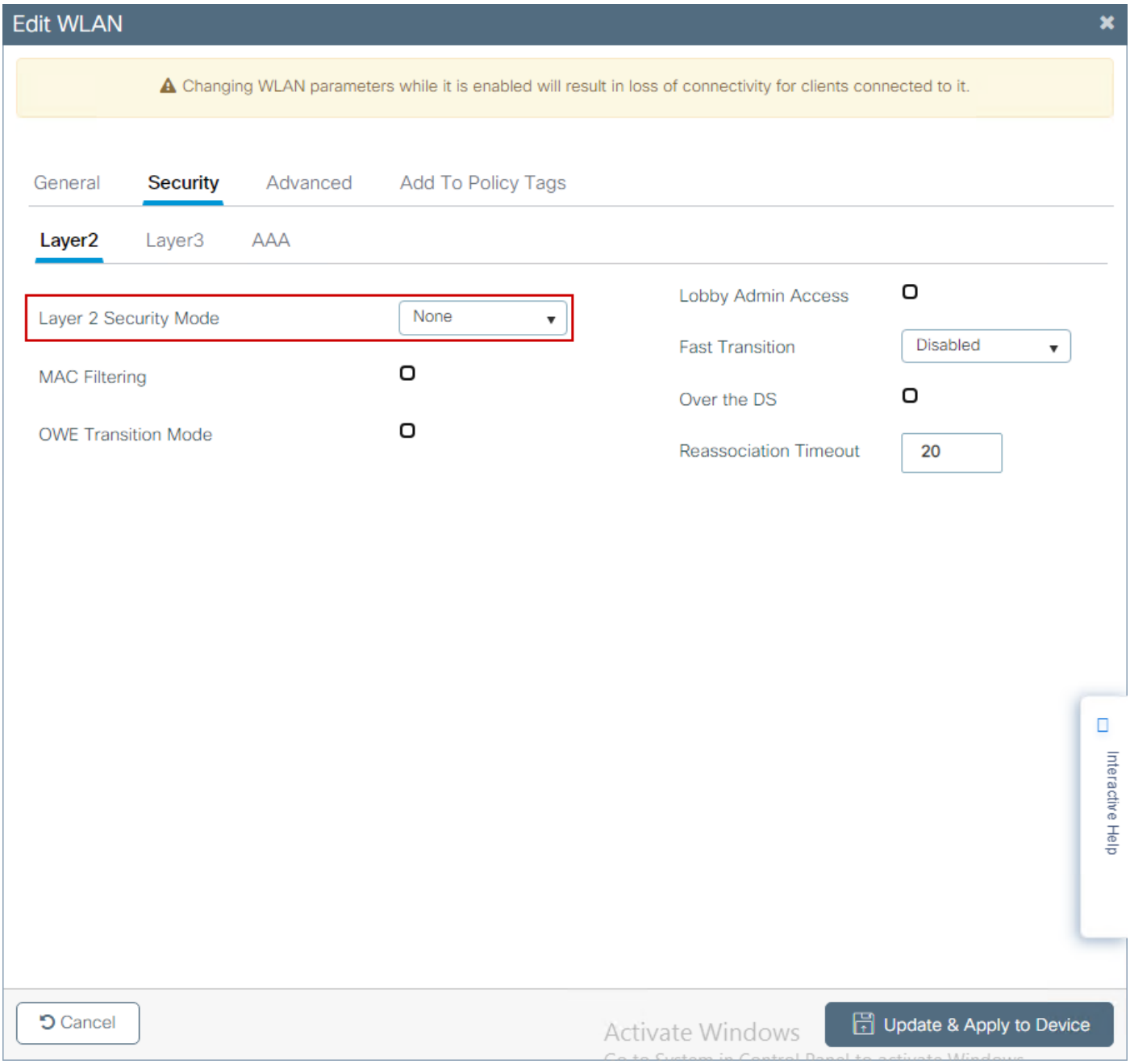
```
alz-9800#

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
```

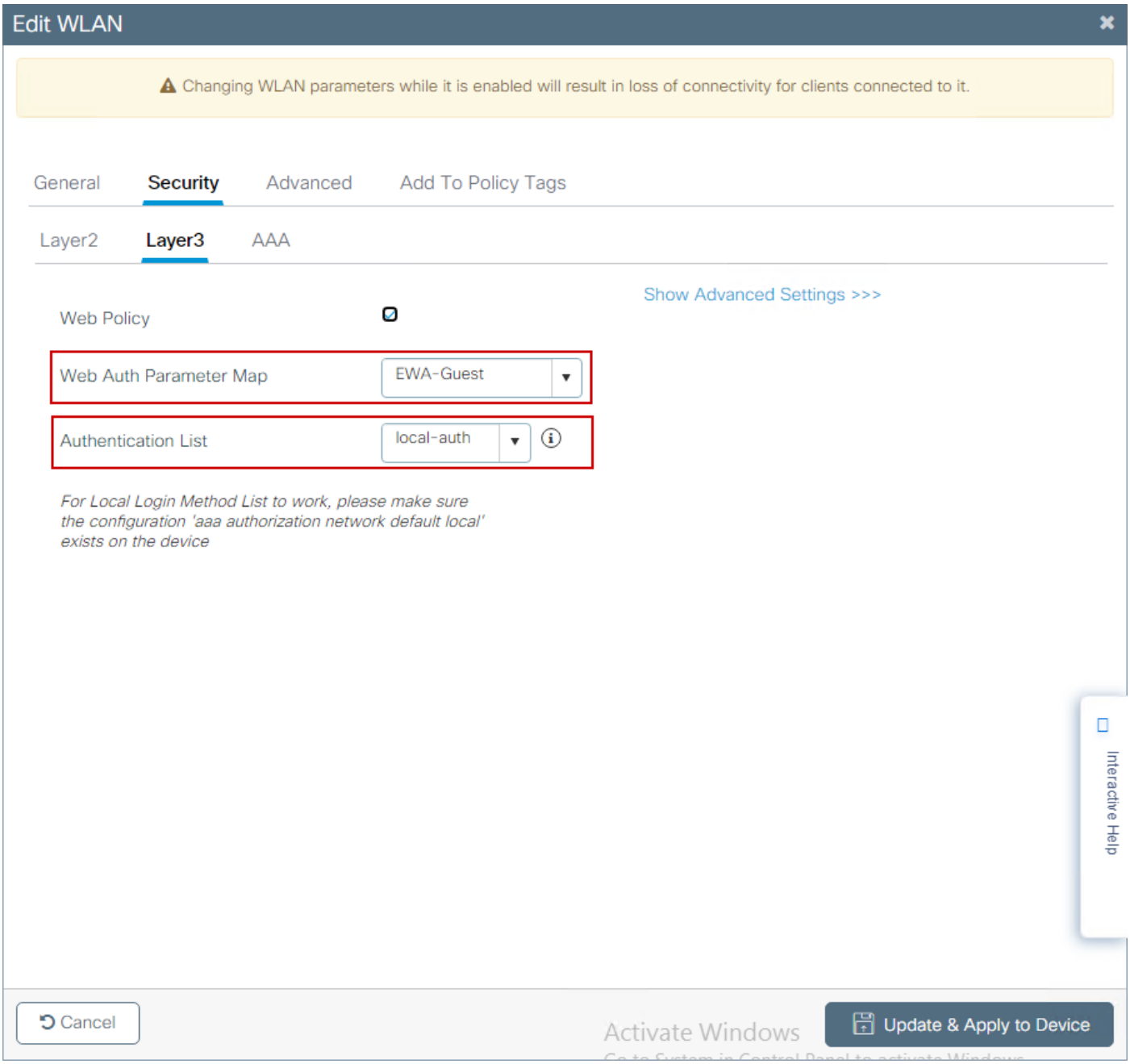
Configura criteri e tag

Passaggio 1. Selezionare Configurazione > Tag e profili > WLAN, quindi selezionare + Aggiungi per creare una nuova WLAN. Definire il nome e lo stato del profilo e dell'SSID nella scheda Generale.



Passaggio 2. Selezionare la scheda Sicurezza e impostare l'autenticazione di livello 2 su Nessuno se non è necessario alcun meccanismo di crittografia via etere. Nella scheda Layer 3, selezionare la casella di controllo Criteri Web, selezionare la mappa dei parametri dal menu a discesa e scegliere l'elenco di autenticazione dal menu a discesa. Facoltativamente, se in precedenza è stato definito un ACL personalizzato, selezionare Show Advanced Settings (Mostra impostazioni avanzate) e selezionare l'ACL appropriato dal menu a discesa.


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



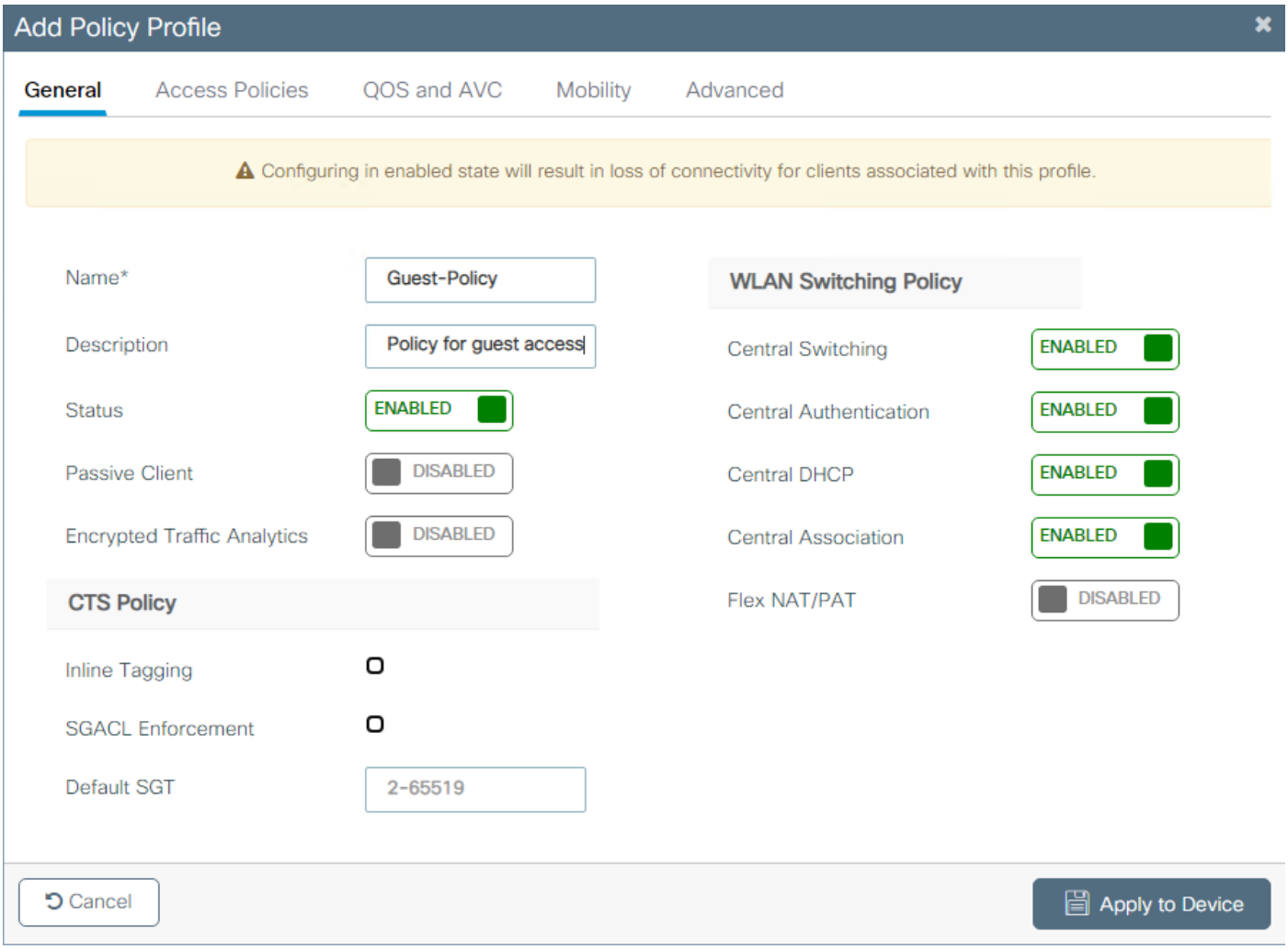
Configurazioni CLI:

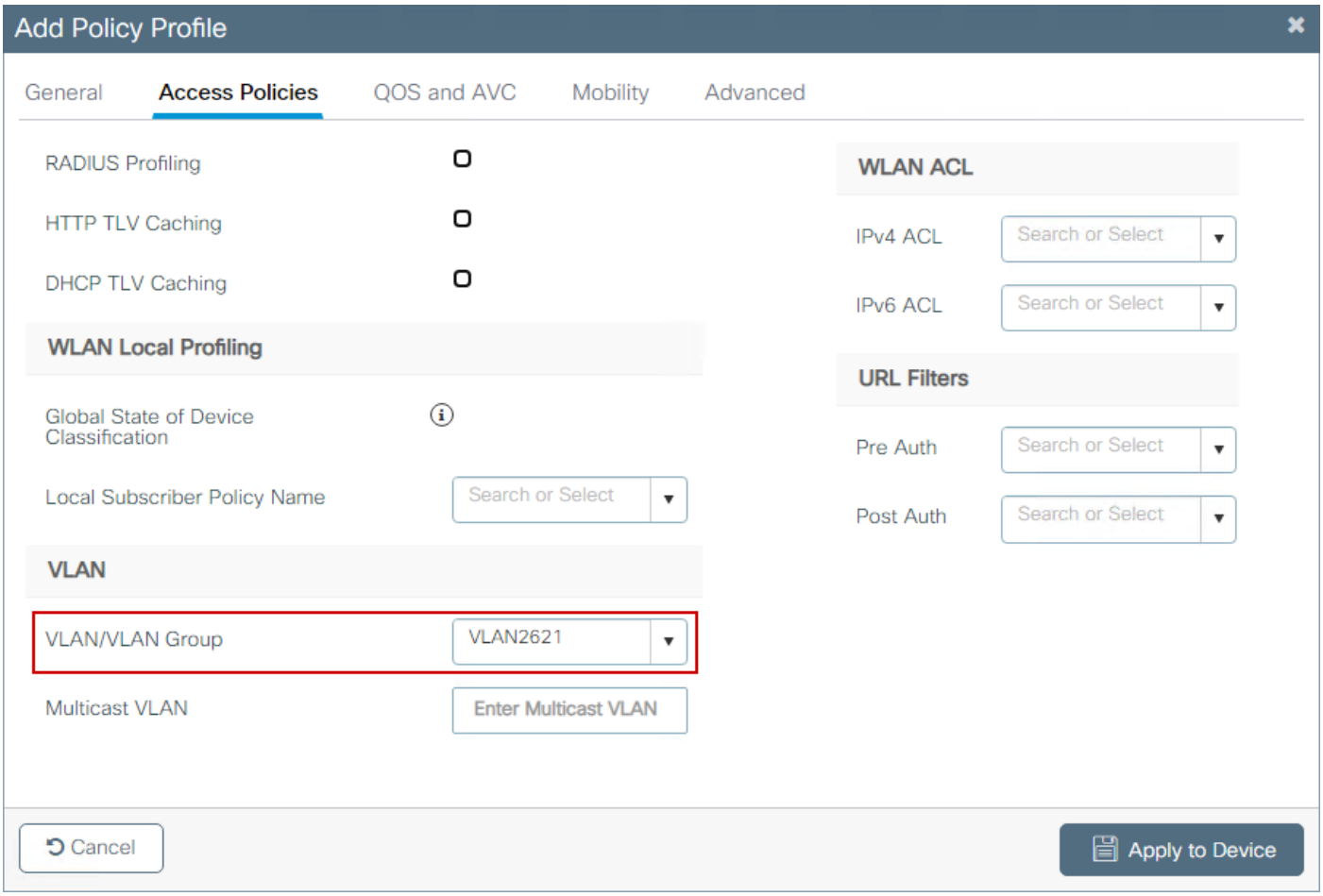
<#root>

```
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
```

Passaggio 3. Passare a Configurazione > Tag e profili > Criterio e selezionare + Aggiungi. Definire il nome e lo stato del criterio; verificare che le impostazioni centrali in Criteri di switching WLAN siano abilitate per i punti di accesso in modalità locale. Nella scheda Access Policies (Criteri di accesso), selezionare la VLAN corretta dal menu a discesa VLAN/VLAN Group (Gruppo di VLAN/VLAN), come mostrato nell'immagine.


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

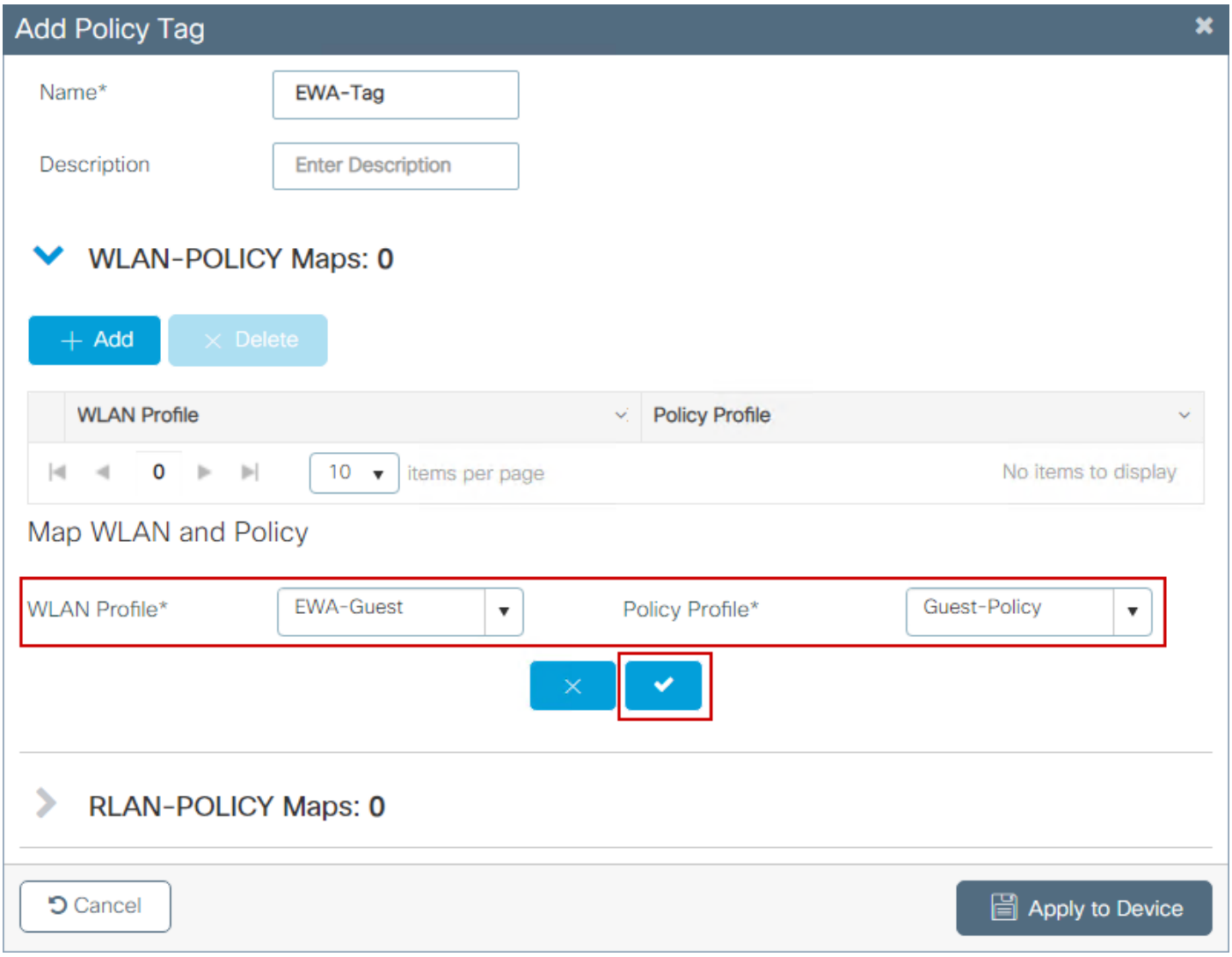


Configurazione dalla CLI:

<#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
```

Passaggio 4. Passare a Configurazione > Tag e profili > Tag, all'interno della scheda Criterio selezionare + Aggiungi. Definire un nome di tag, quindi in Mappe WLAN-POLICY selezionare + Aggiungi e aggiungere il profilo WLAN e policy creato in precedenza.

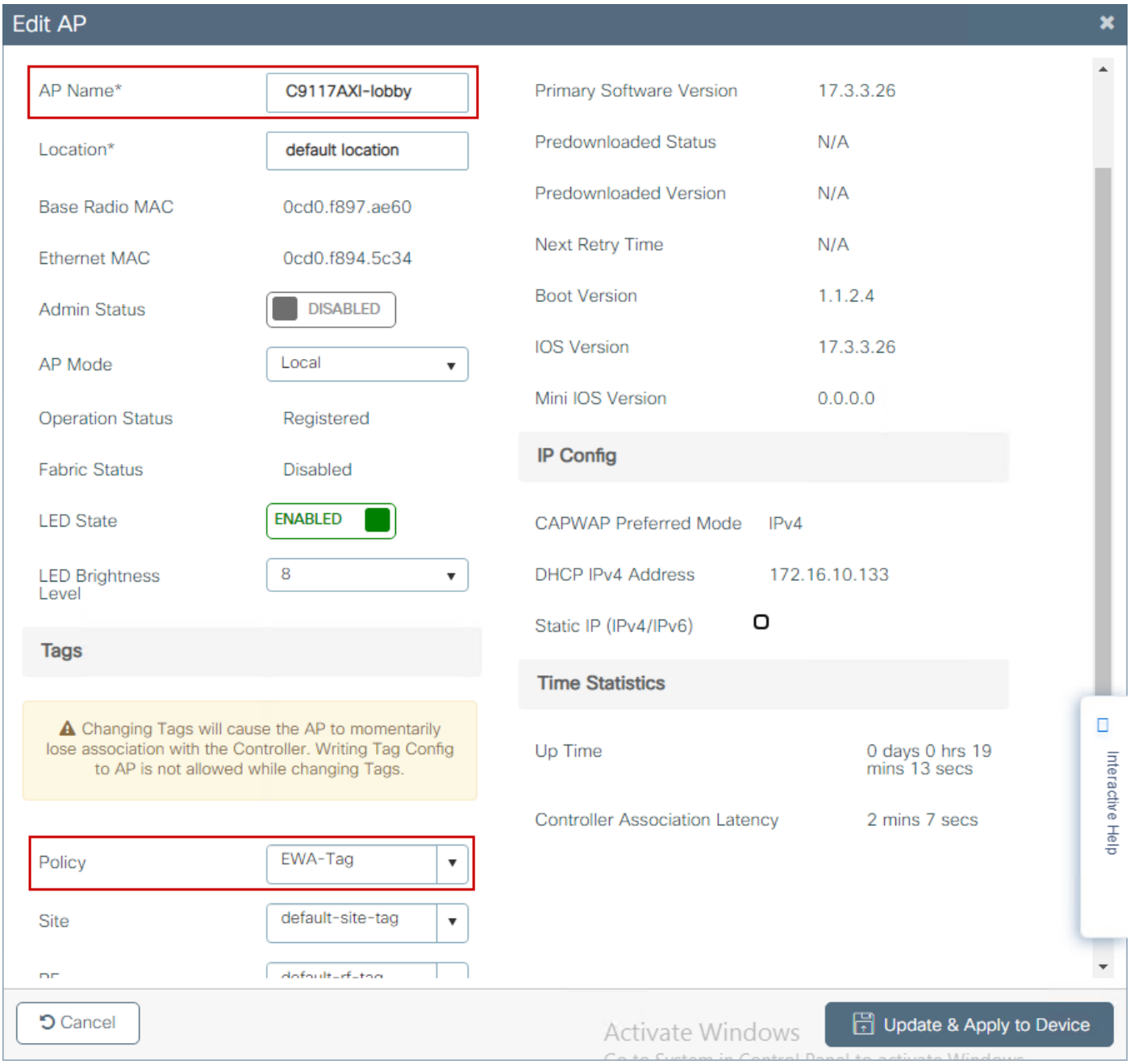


Configurazione dalla CLI:

<#root>

```
9800(config)#

wireless tag policy EWA-Tag


9800(config-policy-tag)#

wlan EWA-Guest policy Guest-Policy
```

Passaggio 5. Passare a Configurazione > Wireless > Access Point e selezionare l'access point utilizzato per trasmettere questo SSID. Dal menu Modifica punto di accesso, selezionare il tag appena creato dal menu a discesa Criterio.



Se è necessario associare tag a più access point contemporaneamente, sono disponibili due opzioni:

Opzione A. Passare a Configurazione > Installazione wireless > Avanzate da qui selezionare Avvia ora per visualizzare l'elenco dei menu di configurazione. Selezionare l'icona di elenco accanto a Tag AP, per visualizzare l'elenco di tutti gli AP nello stato di join, selezionare gli AP necessari, quindi selezionare + Tag AP, quindi selezionare il tag di criterio creato dal menu a discesa.

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

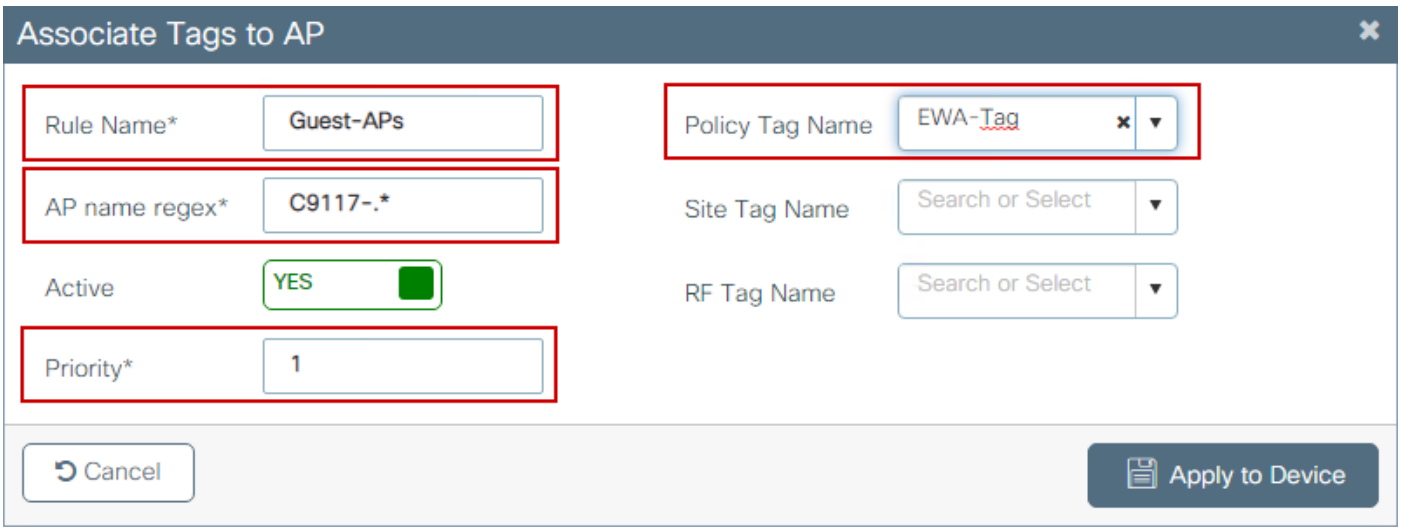
Radio Policy - Radio Characteristics

ACTIONS

Go to List View

Create New

. Definire il nome della regola, il nome dell'access point regex (questa impostazione consente al controller di definire quali access point sono contrassegnati), la priorità (i numeri più bassi hanno una priorità maggiore) e i tag necessari.



Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente:

<#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>

Verificare lo stato e la disponibilità del server http tramite il comando 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

Verificare il plumbing ACL nella sessione client con questi comandi:

<#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
```

Risoluzione dei problemi

Traccia sempre attiva

WLC 9800 offre funzionalità di traccia ALWAYS-ON. In questo modo, tutti gli errori relativi alla connettività del client, gli avvisi e i messaggi a livello di avviso vengono costantemente registrati ed è possibile visualizzare i registri di un evento imprevisto o di una condizione di errore dopo che si è verificato.

Nota: in base al volume dei log generati, è possibile tornare indietro da alcune ore a diversi giorni.

Per visualizzare le tracce raccolte per impostazione predefinita dal 9800 WLC, è possibile connettersi al 9800 WLC tramite SSH/Telnet e leggere i seguenti passaggi (verificare di aver registrato la sessione su un file di testo).

Passaggio 1. Controllare l'ora corrente del controller in modo da poter tenere traccia dei log nel tempo che intercorre tra il momento in cui si è verificato il problema.

```
<#root>

9800#

show clock
```

Passaggio 2. Raccogliere syslog dal buffer del controller o dal syslog esterno in base alla configurazione del sistema. In questo modo è possibile visualizzare rapidamente lo stato del sistema e gli eventuali errori.

```
<#root>

9800#

show logging
```

Passaggio 3. Verificare se sono abilitate le condizioni di debug.

<#root>

9800#

show debugging

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

Nota: se nell'elenco è presente una condizione, le tracce vengono registrate a livello di debug per tutti i processi che soddisfano le condizioni abilitate (indirizzo MAC, indirizzo IP e così via). Ciò aumenta le dimensioni dei log. È pertanto consigliabile cancellare tutte le condizioni quando non si esegue il debug attivo.

Passaggio 4. con il presupposto che l'indirizzo MAC in fase di test non è elencato come condizione nel passaggio 3. Raccogliere le tracce del livello di avviso sempre attive per l'indirizzo MAC specifico.

<#root>

9800#

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

È possibile visualizzare il contenuto della sessione oppure copiare il file su un server TFTP esterno.

<#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>

Debug condizionale e traccia Radioactive (RA)

Se le tracce sempre attive non forniscono informazioni sufficienti per determinare il trigger del problema in esame, è possibile abilitare il debug condizionale e acquisire la traccia Radio attiva (RA), che fornisce le tracce dei livelli di debug per tutti i processi che interagiscono con la condizione specificata (in questo caso l'indirizzo MAC del client). Per abilitare il debug

condizionale, leggere i passaggi seguenti.

Passaggio 1. Accertarsi che non vi siano condizioni di debug abilitate.

<#root>

9800#

clear platform condition all

Passaggio 2. Abilitare la condizione di debug per l'indirizzo MAC del client wireless che si desidera monitorare.

Questi comandi iniziano a monitorare l'indirizzo MAC fornito per 30 minuti (1800 secondi). È possibile aumentare questo tempo fino a 2085978494 secondi.

<#root>

9800#

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

Nota: per monitorare più client alla volta, eseguire il comando debug wireless mac per indirizzo MAC.

Nota: l'attività del client wireless non viene visualizzata nella sessione del terminale in quanto tutti i registri vengono memorizzati nel buffer interno in modo da poter essere visualizzati in un secondo momento.

Passaggio 3. Riprodurre il problema o il comportamento che si desidera monitorare.

Passaggio 4. Interrompere i debug se il problema viene riprodotto prima che il tempo di monitoraggio predefinito o configurato sia attivo.

<#root>

9800#

no debug wireless mac <aaaa.bbbb.cccc>

Una volta trascorso il tempo di monitoraggio o interrotto il debug wireless, il controller 9800 WLC genera un file locale con il nome:

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Passaggio 5. Recuperare il file dell'attività dell'indirizzo MAC. È possibile copiare la traccia RA .log su un server esterno o visualizzare l'output direttamente sullo schermo.

Controllare il nome del file delle tracce RA.

<#root>

9800#

dir bootflash: | inc ra_trace

Copiare il file su un server esterno:

<#root>

9800#

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

Visualizzare il contenuto:

<#root>

9800#

more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Passaggio 6. Se la causa principale non è ancora ovvia, raccogliere i log interni che offrono una visualizzazione più dettagliata dei log del livello di debug. non è necessario eseguire di nuovo il debug del client, in quanto il comando fornisce log di debug già raccolti e archiviati internamente.

<#root>

9800#

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

---

Nota: questo output del comando restituisce tracce per tutti i livelli di registrazione per tutti i processi ed è piuttosto voluminoso. Per analizzare queste tracce, contattare Cisco TAC.

<#root>

9800#

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

Visualizzare il contenuto:

<#root>

```
9800#
more bootflash:ra-internal-<FILENAME>.txt
```

Passaggio 7. Rimuovere le condizioni di debug.

Nota: assicurarsi di rimuovere sempre le condizioni di debug dopo una sessione di risoluzione dei problemi.

Acquisizioni pacchetti incorporate

I controller 9800 possono eseguire l'analisi nativa dei pacchetti; ciò consente una più semplice risoluzione dei problemi come la visibilità dell'elaborazione dei pacchetti del control plane.

Passaggio 1. Definire un ACL per filtrare il traffico di interesse. Per l'autenticazione Web, si consiglia di consentire il traffico da e verso il server Web, nonché il traffico da e verso un paio di punti di accesso a cui i client sono connessi.

<#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
```

Passaggio 2. Definire i parametri di acquisizione del monitor. Verificare che il traffico del control plane sia abilitato in entrambe le direzioni. L'interfaccia fa riferimento all'uplink fisico del controller.

<#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)
```

Passaggio 3. Avviare l'acquisizione del monitor e riprodurre il problema.

<#root>

```
9800#
```

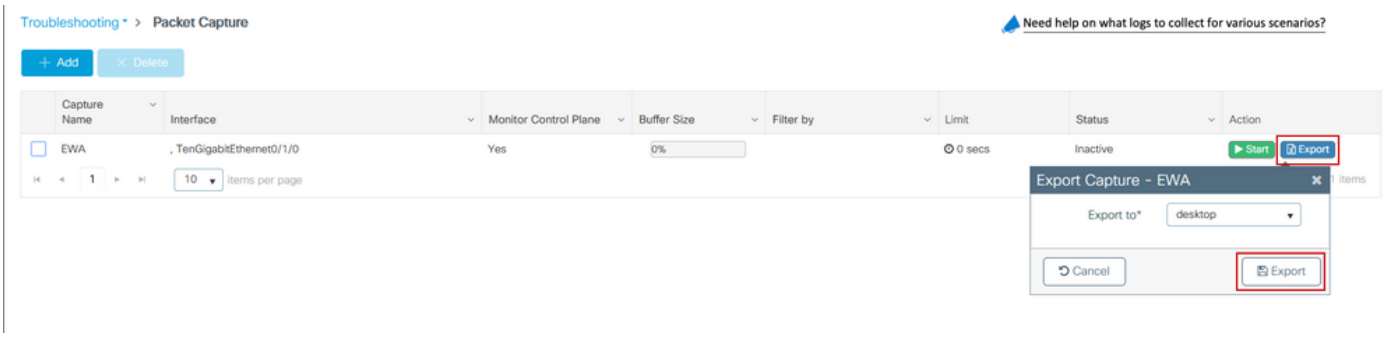
```
monitor capture EWA start

Started capture point : EWA
```

Passaggio 4. Interrompere l'acquisizione ed esportazione del monitor.

<#root>

```
9800#
monitor capture EWA stop

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

In alternativa, è possibile scaricare l'acquisizione dalla GUI, selezionare Risoluzione dei problemi > Packet Capture (Acquisizione pacchetti) e selezionare Export (Esporta) sull'acquisizione configurata. Selezionare Desktop dal menu a discesa per scaricare l'acquisizione tramite HTTP nella cartella desiderata.



Risoluzione dei problemi sul lato client

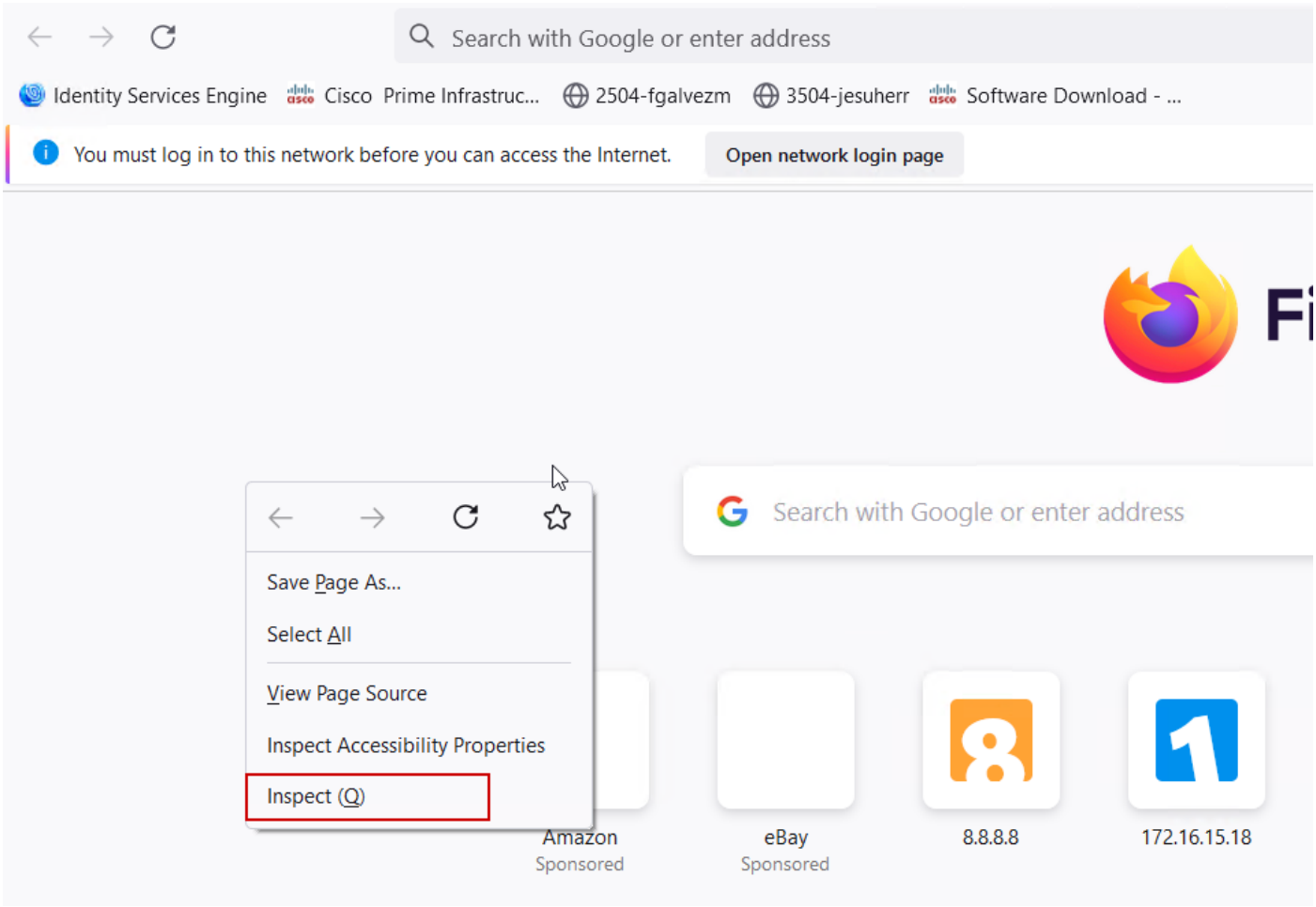
Le WLAN di autenticazione Web dipendono dal comportamento del client. Su questa base, la conoscenza del comportamento del client e le informazioni sono fondamentali per identificare la root cause dei comportamenti errati di autenticazione Web.

Risoluzione problemi browser HAR

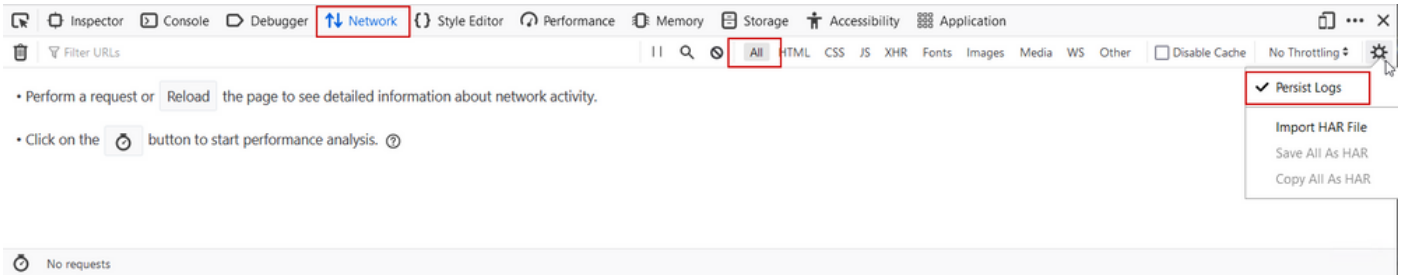
Molti browser moderni, come Mozilla Firefox e Google Chrome, forniscono strumenti di sviluppo della console per eseguire il debug delle interazioni delle applicazioni Web. I file HAR sono record di interazioni client-server e forniscono una linea temporale di interazioni HTTP insieme a informazioni su richieste e risposte (intestazioni, codice di stato, parametri e così via).

I file HAR possono essere esportati dal browser client e importati in un browser diverso per un'ulteriore analisi. Questo documento descrive come raccogliere il file HAR da Mozilla Firefox.

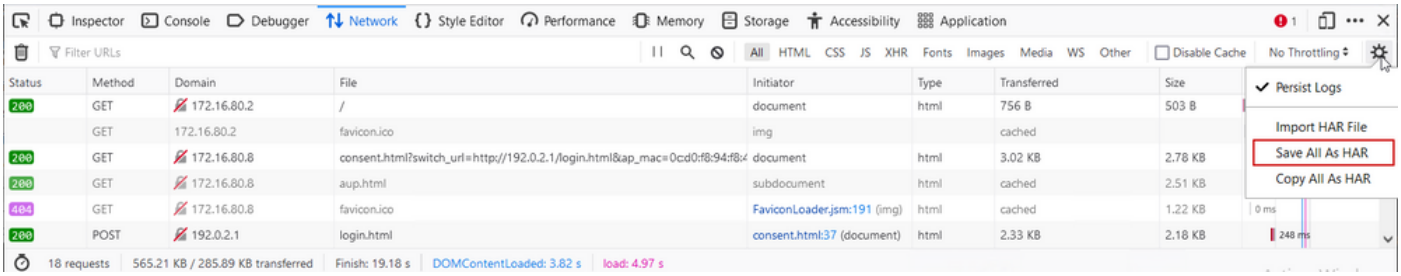
Passaggio 1. Aprire Strumenti di sviluppo Web con Ctrl + Maiusc + I, in alternativa fare clic con il pulsante destro del mouse nel contenuto del browser e selezionare Ispeziona.



Passaggio 2. Passare alla rete e assicurarsi che sia selezionato "Tutto" per acquisire tutti i tipi di richiesta. Selezionare l'icona a forma di ingranaggio e assicurarsi che accanto a Registri persistenti sia presente una freccia, altrimenti le richieste di registrazione vengono cancellate ogni volta che viene attivata una modifica al dominio.



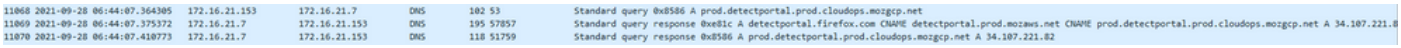
Passaggio 3. Riprodurre il problema, verificare che tutte le richieste vengano registrate nel browser. Una volta, il problema viene riprodotto arrestare la registrazione di rete, quindi selezionare sull'icona ingranaggio e selezionare Salva tutto come HAR.



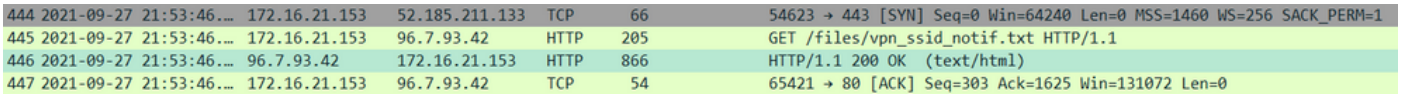
Acquisizione pacchetti lato client

I client wireless con sistemi operativi quali Windows o MacOS possono eseguire l'analisi dei pacchetti sulla scheda di rete wireless. Pur non sostituendo direttamente le acquisizioni di pacchetti via etere, possono fornire uno sguardo sul flusso complessivo dell'autenticazione Web.

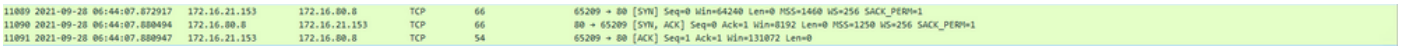
Richiesta DNS:



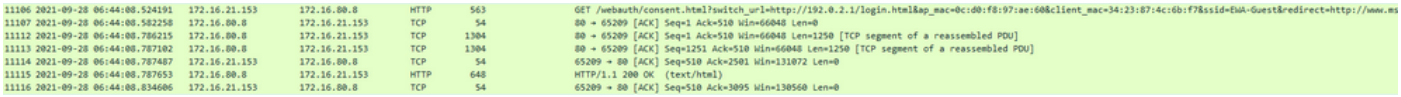
Handshake TCP iniziale e HTTP GET per il reindirizzamento:



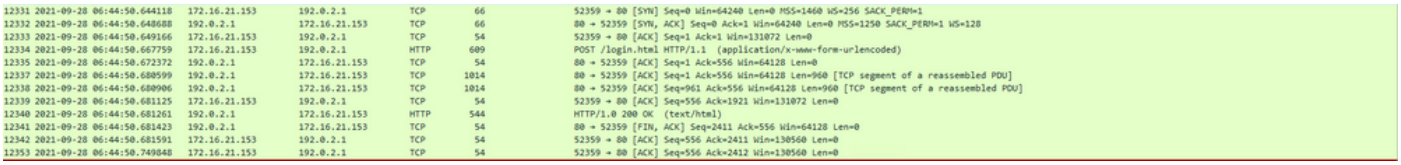
Handshake TCP con server esterno:



HTTP GET al server esterno (richiesta di portale captive):



HTTP POST su IP virtuale per autenticazione:



Esempio di tentativo riuscito

Questo è l'output di un tentativo di connessione riuscito dalla prospettiva di traccia attiva radio. Usare questo come riferimento per identificare le fasi della sessione client per i client che si connettono a un SSID di autenticazione Web di layer 3.

autenticazione e associazione 802.11:

<#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.

Autenticazione di livello 2 ignorata:

<#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

Piombo ACL:

<#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
```

Processo di apprendimento IP:

<#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 cap
[...]
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

Processo di autenticazione e reindirizzamento di livello 3:

<#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

Transizione allo stato RUN:

<#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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).