Configurazione dell'autenticazione Web locale con autenticazione esterna

Sommario

Introduzione

In questo documento viene descritto come configurare l'autenticazione Web locale con autenticazione locale su un controller WLC (Wireless LAN Controller) 9800.

Prerequisiti

Cisco raccomanda la conoscenza del modello di configurazione WLC 9800.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco WLC serie 9800.
- Conoscenza completa dell'autenticazione Web.

Componenti usati

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

- 9800-CL WLC Cisco IOS® XE versione 17.12.5
- Access point Cisco C9117AXI.

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

Local Web Authentication (LWA) è un metodo di autenticazione Wireless Local Area Network (WLAN) che può essere configurato sul WLC. Quando un utente seleziona la WLAN dall'elenco delle reti disponibili, viene reindirizzato a un portale Web. In questo portale, a seconda della configurazione, è possibile che all'utente venga richiesto di immettere un nome utente e una password, di accettare un criterio di utilizzo accettabile (Acceptable Use Policy, AUP) o una combinazione di entrambe le azioni per completare la connessione.

Per informazioni sui quattro tipi di pagine di autenticazione Web presentati durante il processo di accesso, consultare la guida alla configurazione dell'autenticazione Web locale e rivedere le opzioni disponibili per il tipo di autenticazione Web. È inoltre possibile consultare la guida alla configurazione dell'autenticazione Web locale con autenticazione esterna nella sezione Tipi di autenticazione.

Mappa parametri

La mappa dei parametri è un elemento di configurazione essenziale in un WLC che abilita l'autenticazione Web. È costituito da un insieme di impostazioni che gestiscono vari aspetti del processo di autenticazione Web, tra cui il tipo di autenticazione, gli URL di reindirizzamento, i parametri aggiunti, i timeout e le pagine Web personalizzate. Per attivare e gestire l'autenticazione basata sul Web per un determinato SSID, questa mappa deve essere collegata al profilo WLAN.

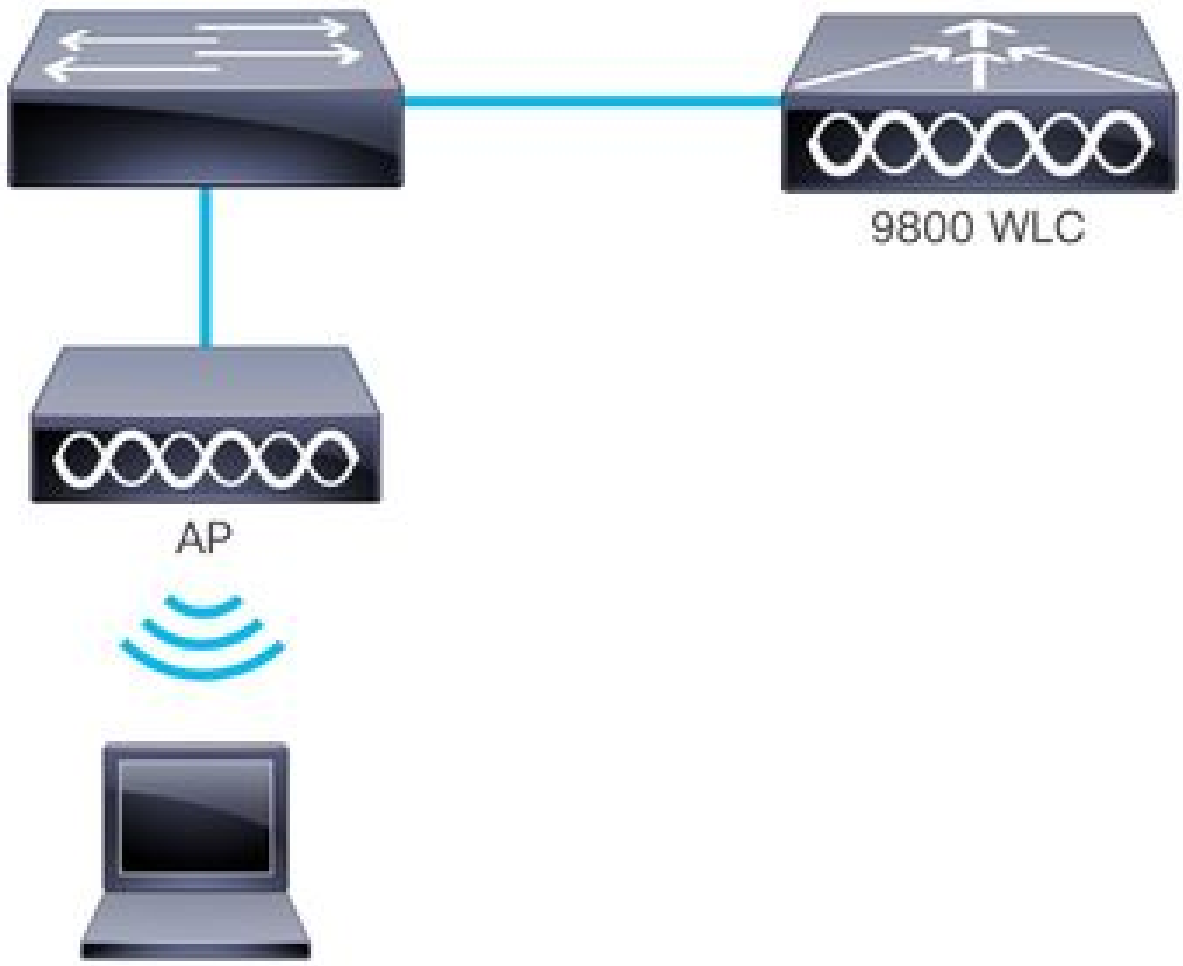
Il controller LAN wireless viene fornito con una mappa dei parametri globale predefinita, ma gli amministratori hanno la possibilità di creare mappe dei parametri personalizzate per personalizzare il comportamento dell'autenticazione Web in base alle esigenze specifiche.

Database per autenticazione

Se la mappa dei parametri è configurata per l'utilizzo di un nome utente e di una password, è necessario definire le credenziali di autenticazione, memorizzate localmente sul WLC. Quando si crea un account utente guest tramite la GUI, è possibile impostare il numero massimo di accessi simultanei consentiti per ogni account guest. I valori validi sono compresi tra 0 e 64, dove 0 indica che sono consentiti accessi simultanei illimitati per l'utente guest.

LWA è destinato principalmente a piccole distribuzioni. Se supporta l'integrazione con altri metodi di autenticazione, è possibile controllare la Combinazione di autenticazioni supportata per un client per ulteriori informazioni.

L'immagine rappresenta una topologia generica di LWA:



Topologia generica di LWA con autenticazione locale

Dispositivi nella topologia di rete di LWA:

- Client/Supplicant: avvia la richiesta di connessione alla WLAN, in seguito ai server DHCP e DNS, e risponde alle comunicazioni dal WLC.
- Access Point: collegato a uno switch, trasmette la WLAN guest e fornisce connettività wireless ai dispositivi guest. Consente il traffico DHCP e DNS prima che l'utente guest completi l'autenticazione immettendo credenziali valide, accetti un'autenticazione automatica o una combinazione di entrambe le azioni.
- WLC/autenticatore: Gestisce i punti di accesso e i dispositivi client. Il WLC ospita l'URL di reindirizzamento e applica l'elenco di controllo di accesso (ACL) che controlla il traffico e i

relativi elementi creati per impostazione predefinita durante la configurazione della mappa dei parametri. Intercetta le richieste HTTP degli utenti guest e le reindirizza a un portale Web (pagina di accesso) in cui gli utenti devono eseguire l'autenticazione. Il WLC acquisisce le credenziali utente, autentica i guest e controlla il database locale per verificare la validità delle credenziali.

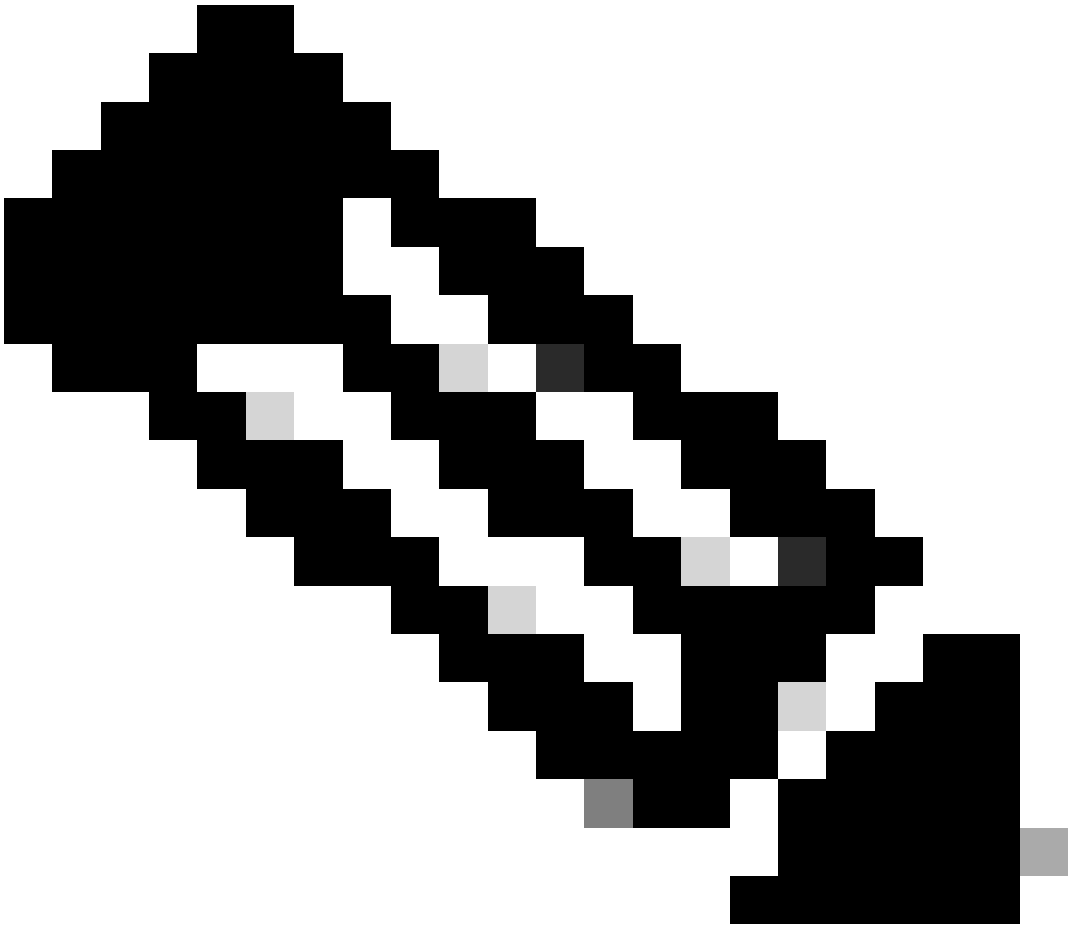
- Server di autenticazione: in questo scenario, il WLC funziona come server di autenticazione. Convalida le credenziali utente guest e concede o nega l'accesso alla rete di conseguenza.

Configurazione

Autenticazione Web locale con autenticazione locale sulla CLI

Elenchi di metodi per autenticazione locale

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#aaa new-model
9800WLC(config)#aaa authentication login LWA_AUTHENTICATION local
9800WLC(config)#aaa authorization network default local
9800WLC(config)#end
```



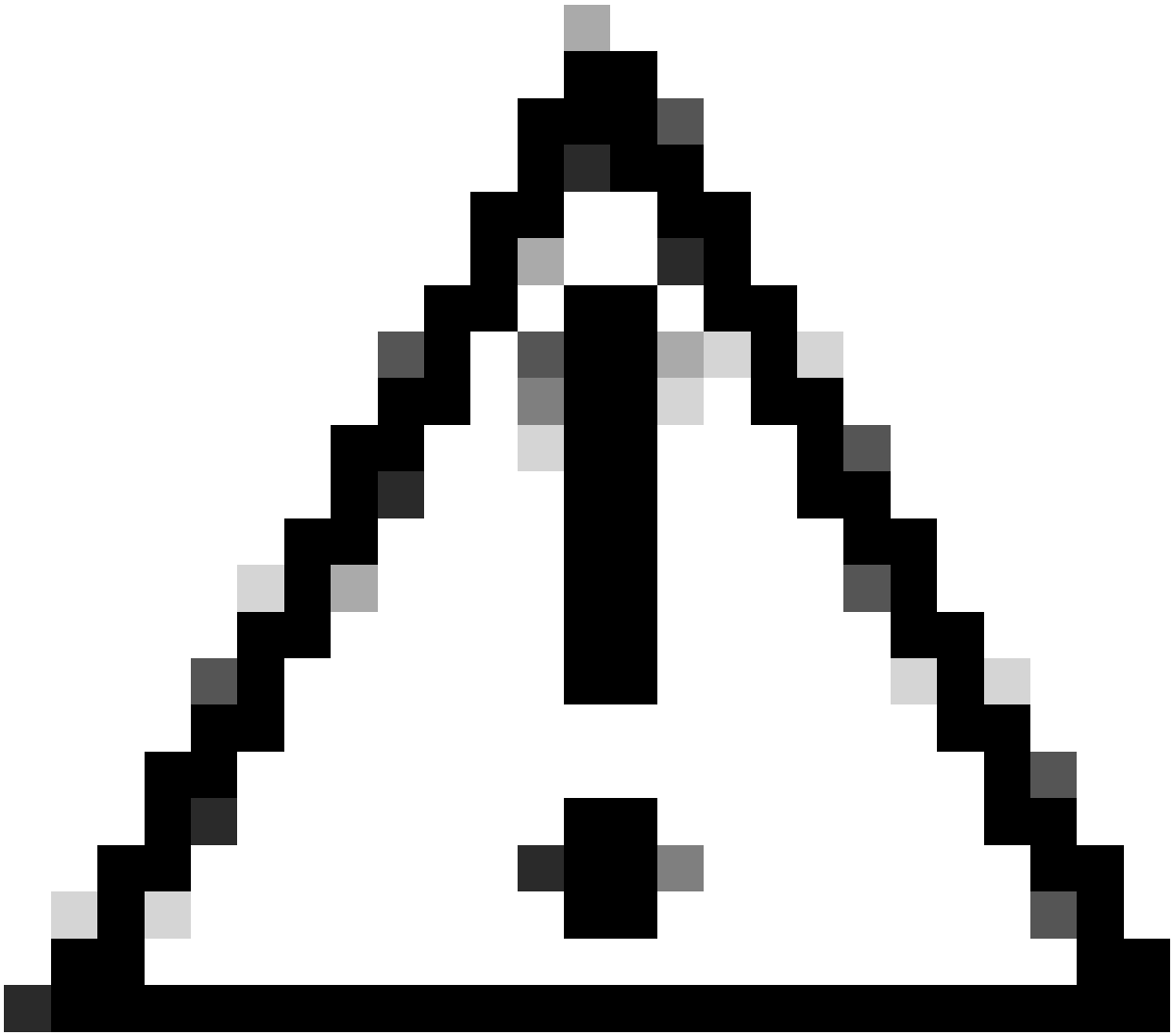
Nota: Affinché Local Login Method List funzioni, verificare che la configurazione aaa authorization network default esista sul WLC. Questa operazione è necessaria in quanto il WLC autorizza l'utente ad accedere alla rete.

Mappe parametri

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#parameter-map type webauth global
9800WLC(config-params-parameter-map)#type webauth
9800WLC(config-params-parameter-map)#virtual-ip ipv4 192.0.2.1
9800WLC(config-params-parameter-map)#trustpoint
```

```
9800WLC(config-params-parameter-map)#webauth-http-enable
```

```
9800WLC(config-params-parameter-map)#end
```



Attenzione: L'indirizzo IP virtuale deve essere un indirizzo non instradabile proposto nella RFC 5737. Per impostazione predefinita, è impostato IP 192.0.2.1. Per ulteriori informazioni sull'indirizzo IP virtuale, consultare il documento Cisco Catalyst serie 9800 Configuration Best Practices. Su AireOs, per la maggior parte del tempo il valore IP utilizzato è 1.1.1.1. Questa opzione non è più consigliata in quanto è diventata un valore IP pubblico.

La capacità di creare più mappe di parametri consente flussi personalizzati: pagine Web personalizzate e parametri di presentazione specifici per ciascuna WLAN. La mappa dei parametri globali determina il Trustpoint e quindi il certificato che il WLC presenta al client sul portale di

reindirizzamento. Controlla inoltre i tipi di traffico client intercettato, ad esempio HTTP/HTTPS per il portale di reindirizzamento, la risoluzione del dominio o del nome host per l'indirizzo IP virtuale. Questa separazione consente alla mappa globale di gestire le impostazioni generali, ad esempio la presentazione dei certificati e l'intercettazione del traffico, mentre le mappe dei parametri definite dall'utente forniscono un'esperienza granulare per ciascuna WLAN.

Parametri di sicurezza WLAN

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#wlan LWA_LA 1 "LWA LA"
9800WLC(config-wlan)#no security wpa
9800WLC(config-wlan)#no security wpa wpa2
9800WLC(config-wlan)#no security wpa wpa2 ciphers aes
9800WLC(config-wlan)#no security wpa akm dot1x
9800WLC(config-wlan)#security web-auth
9800WLC(config-wlan)#security web-auth authentication-list LWA_AUTHENTICATION
9800WLC(config-wlan)#security web-auth parameter-map global
9800WLC(config-wlan)#no shutdown
9800WLC(config-wlan)#end
```

Crea un profilo criteri

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#wireless profile policy
```

```
9800WLC(config-wireless-policy)#vlan
```

```
9800WLC(config-wireless-policy)#no shutdown
```

```
9800WLC(config-wireless-policy)#end
```

Crea un tag di criteri

```
9800WLC>enable
```

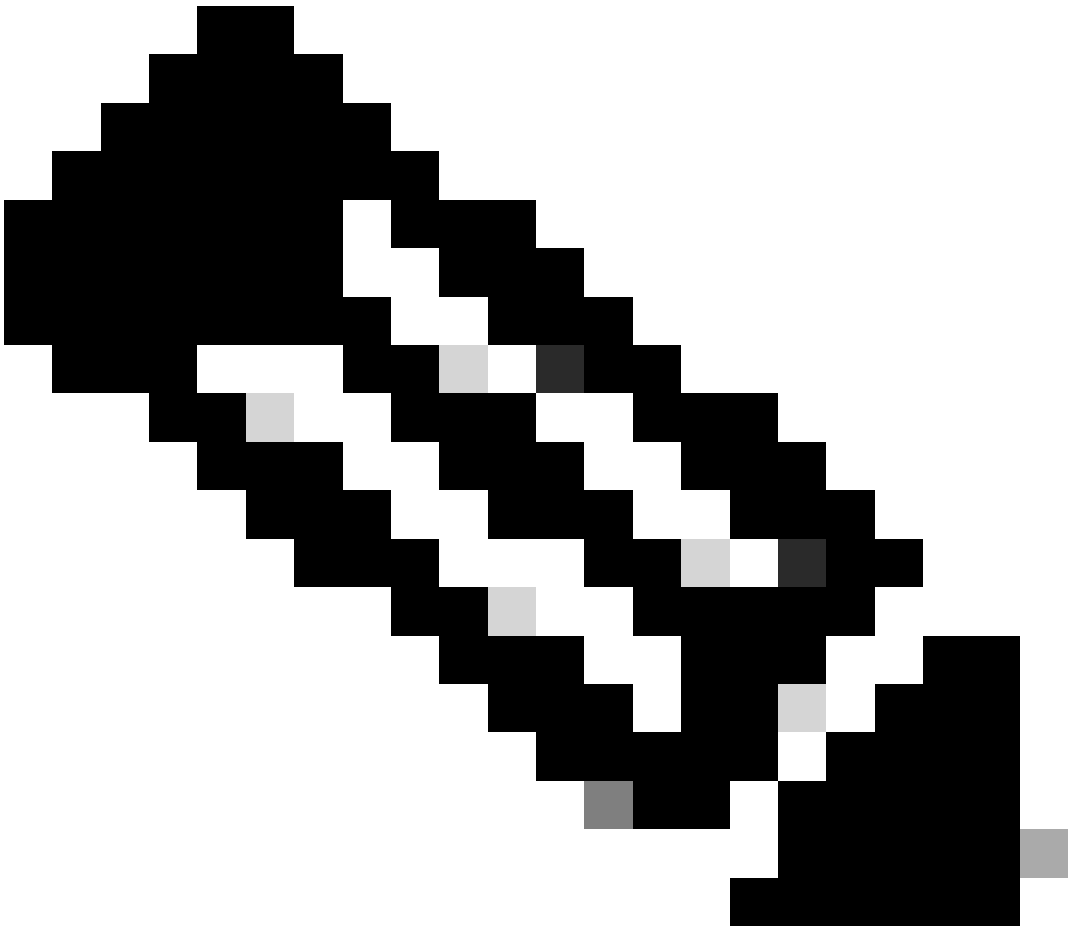
```
9800WLC#configure terminal
9800WLC(config)#wireless tag policy



9800WLC(config-policy-tag)#wlan LWA_LA policy



9800WLC(config-policy-tag)# end
```

Assegnazione di un tag di criterio a un punto di accesso

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#ap


       >


9800WLC(config-ap-tag)#policy-tag POLICY_TAG


9800WLC(config-ap-tag)#end
```

Crea nome utente guest

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#user-name johndoe
9800WLC(config-user-name)#description Guest-User
9800WLC(config-user-name)#password 0 Cisco123
9800WLC(config-user-name)#type network-user description


        guest-user lifetime year 0 month 11 day 30 hour 23


9800WLC(config-user-name)#end
```

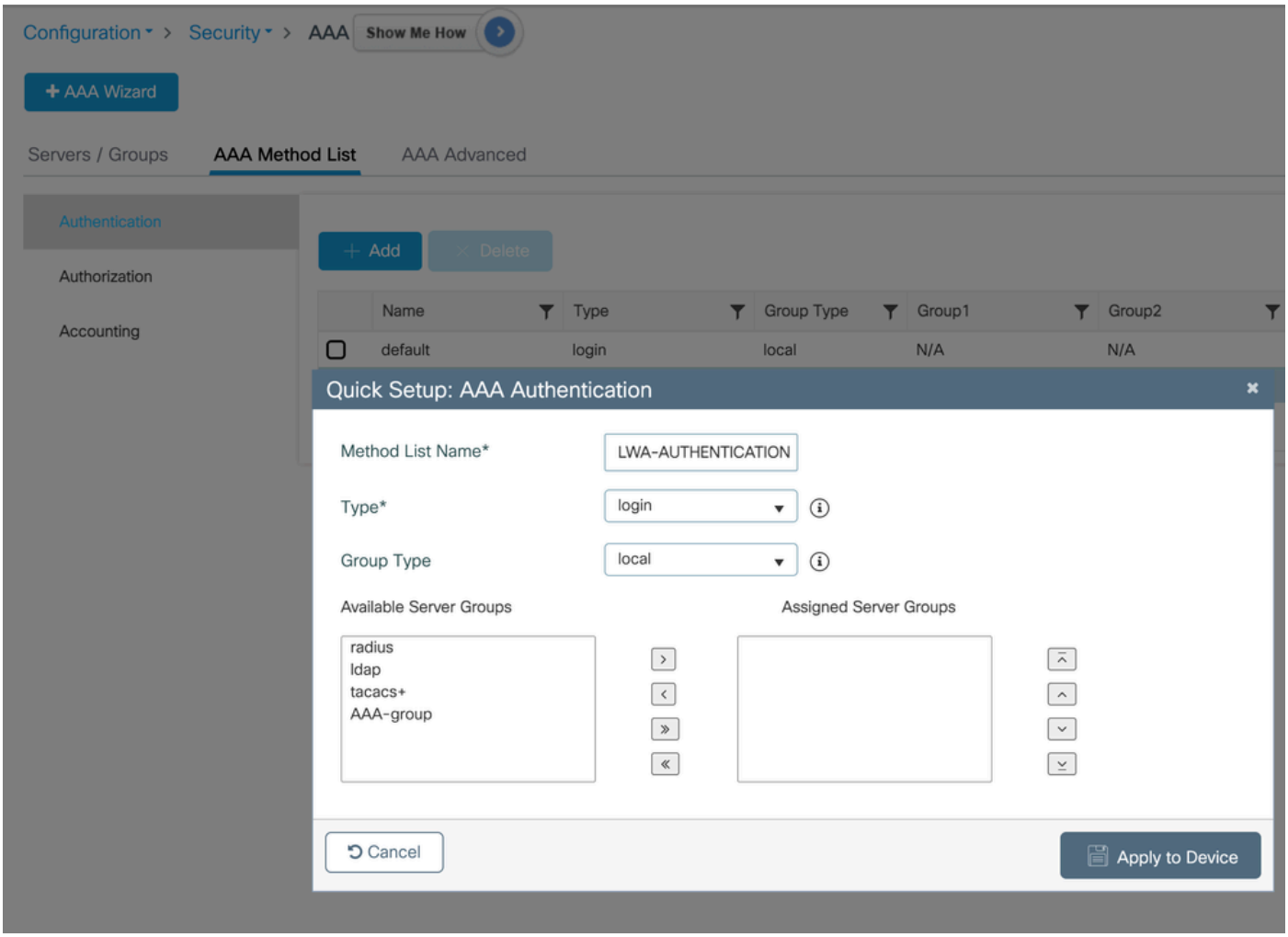


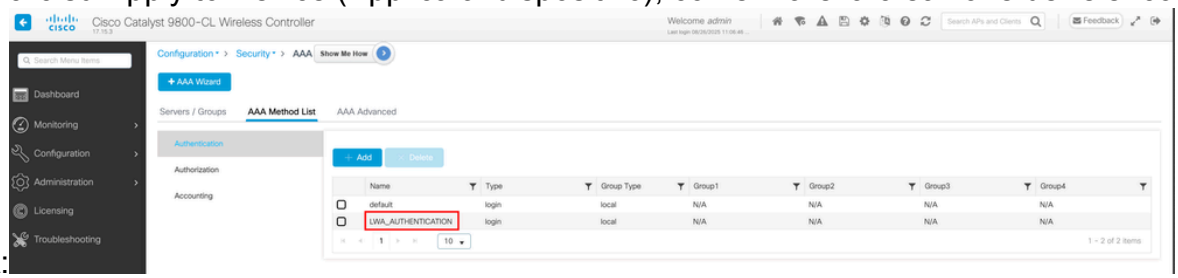
Nota: Quando si imposta la durata per l'utente guest, se l'anno è impostato su 1, non è possibile specificare i parametri successivi, ovvero mesi, giorni, ore e minuti, poiché la durata massima è 1 anno.

Autenticazione Web locale con autenticazione locale tramite WebUI

Elenchi di metodi per autenticazione locale

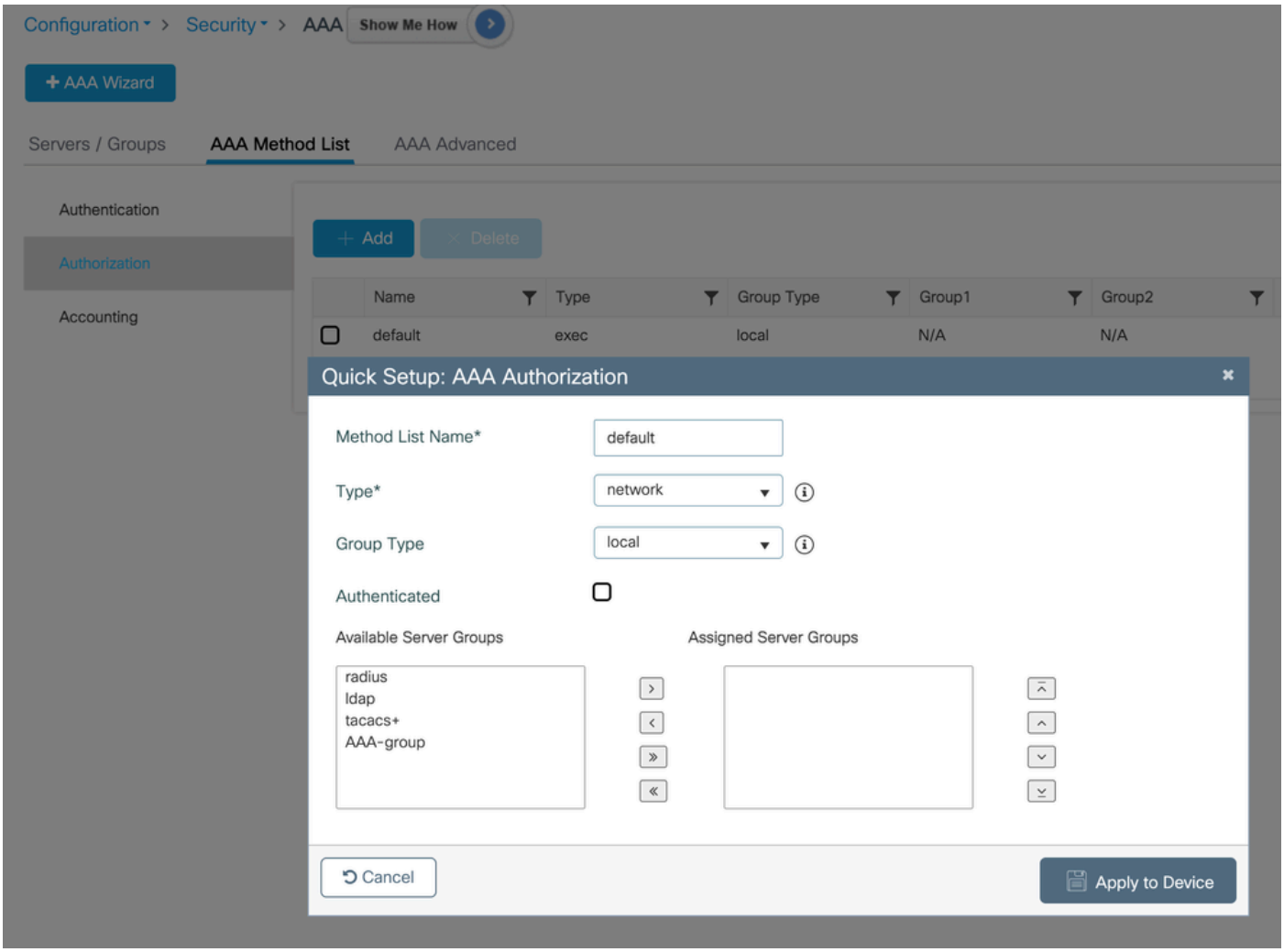
Selezionare Configurazione > Sicurezza > AAA > Elenco metodi AAA > Autenticazione > Aggiungi per creare l'elenco dei metodi da utilizzare successivamente nella configurazione WLAN.



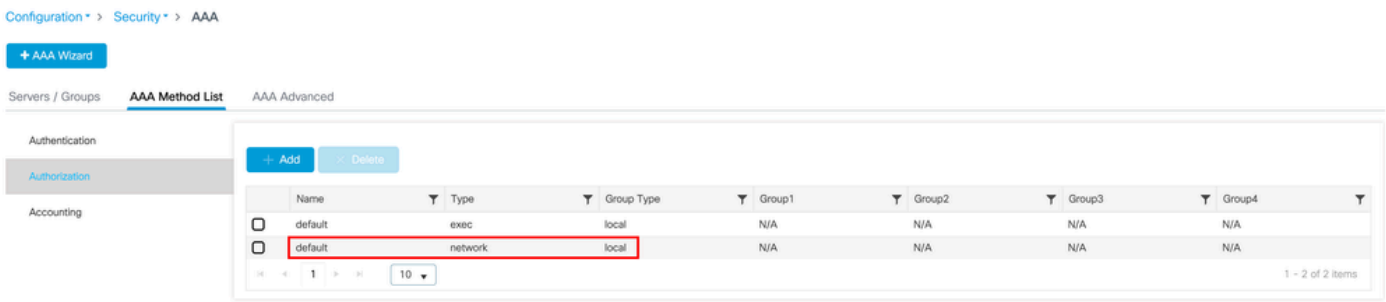
Dopo aver fatto clic su Apply to Device (Applica al dispositivo), confermare la creazione dell'elenco dei metodi AAA: 

Verificare che esista un elenco di metodi di autorizzazione locale. Questo è un requisito per il funzionamento dell'elenco di metodi di accesso locale creato.

Configurazione > Sicurezza > AAA > Elenco metodi AAA > Autorizzazione > Aggiungi

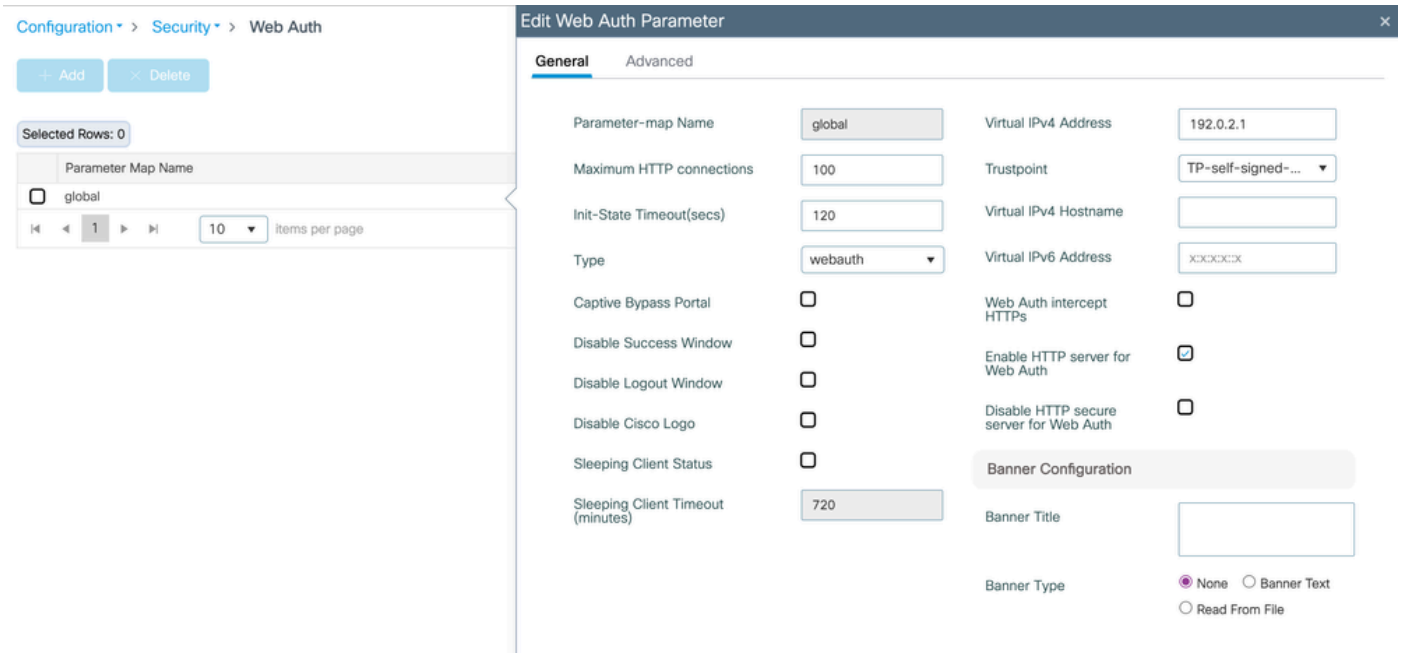


Dopo aver fatto clic su Apply to Device (Applica al dispositivo), confermare la creazione dell'elenco dei metodi AAA:

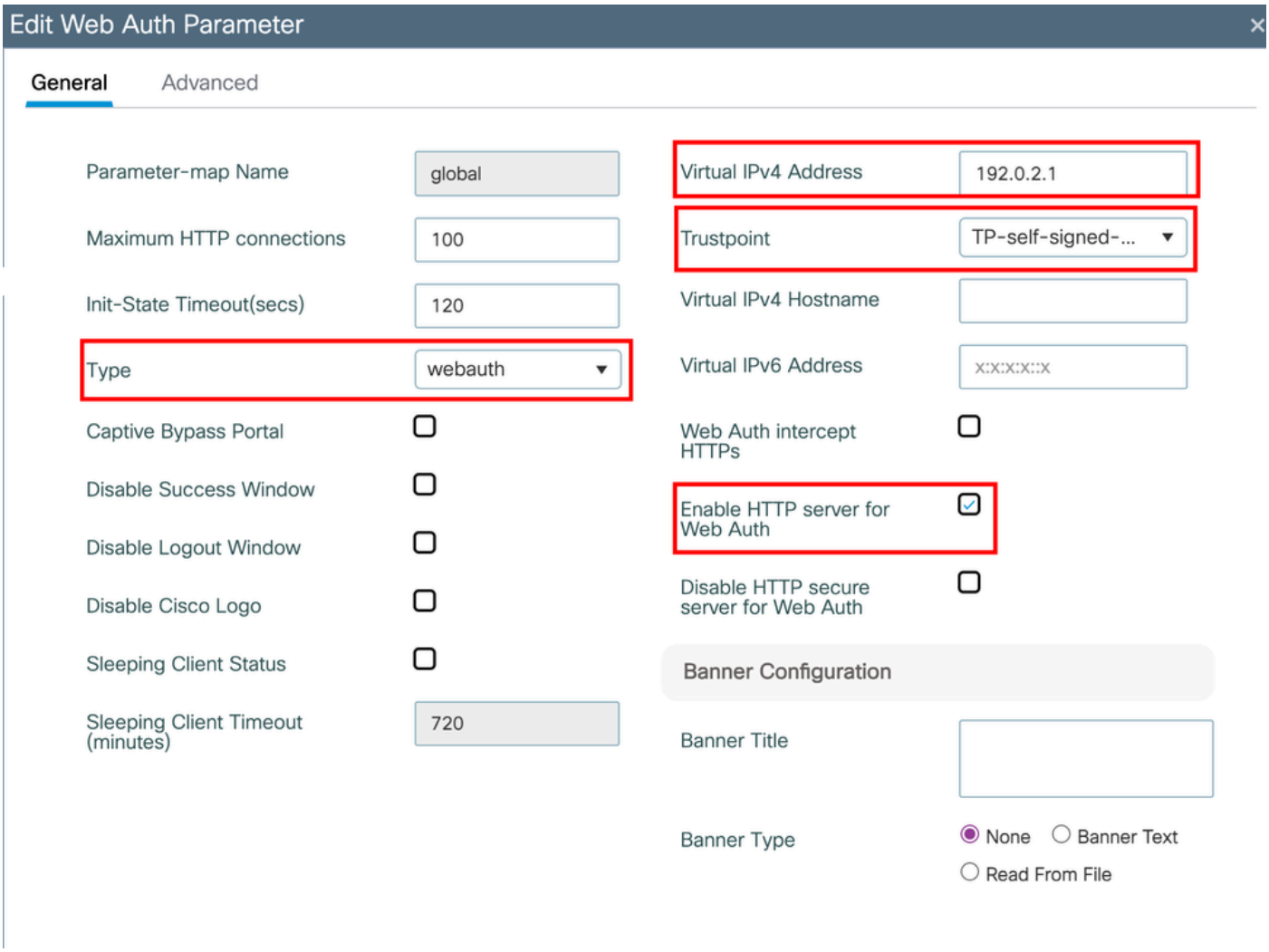


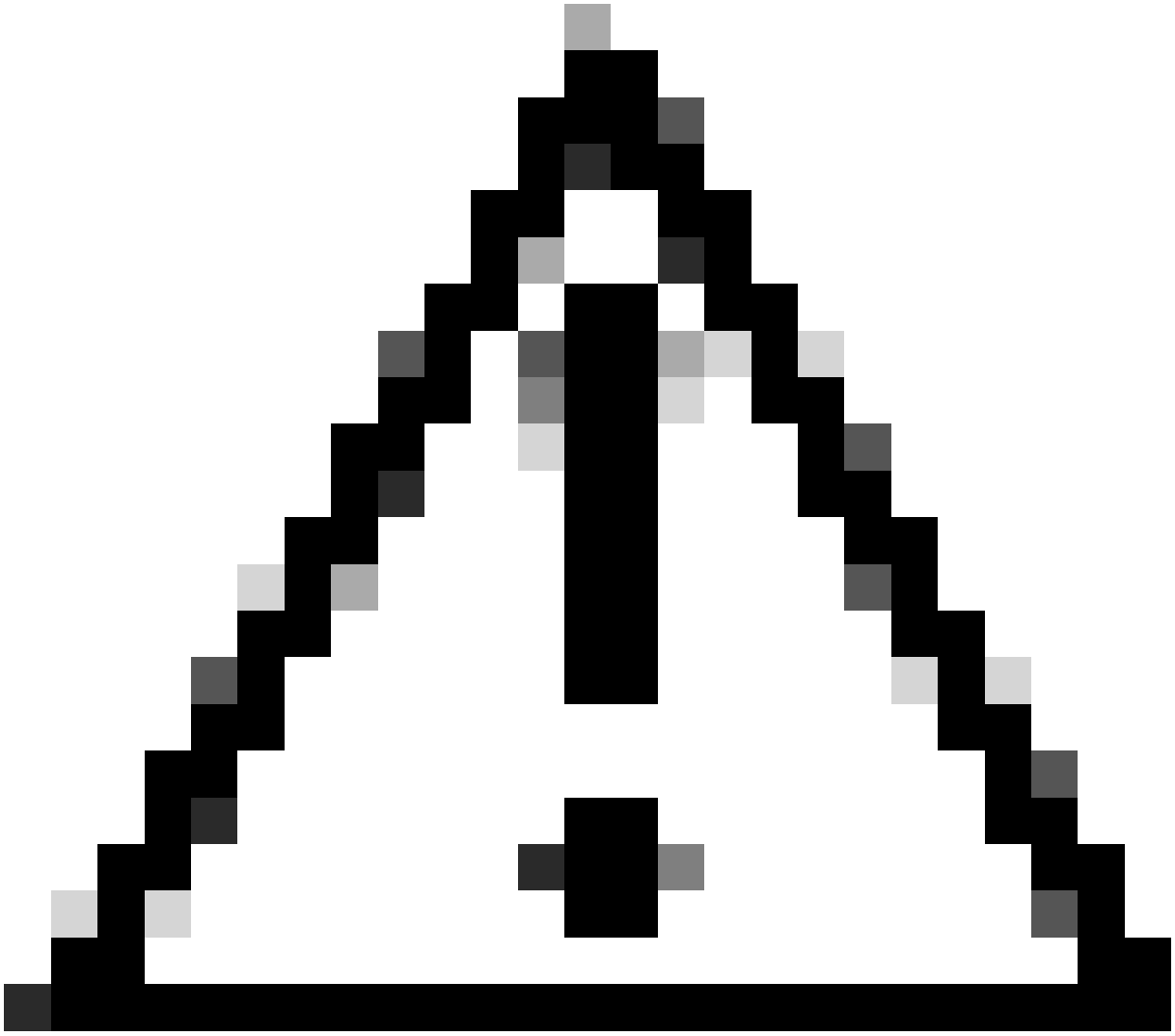
Mappe parametri

Modifica la mappa dei parametri globali in Configurazione > Sicurezza > Autenticazione Web



Selezionare il tipo di autenticazione Web da utilizzare, IP virtuale e il Trustpoint che il WLC presenta sul portale Web. In questo caso, il certificato autofirmato è selezionato ed è probabile che causi una dichiarazione di non responsabilità del tipo "la connessione non è una rete privata::ERR_CERT_AUTHORITY_INVALID" poiché si tratta di un certificato LSC (Locally Significant Certificate) e non è firmato da una CA riconoscibile su Internet. Per modificare questa impostazione, utilizzare un certificato firmato da terze parti. I dettagli sono illustrati in Generate and Download CSR Certificates on Catalyst 9800 WLCs o è disponibile un'opzione video che illustra il caricamento e la creazione di Truspoint. Rinnovare i certificati per WebAuth e WebAdmin su Cisco 9800 WLC | Installazione di Secure Wireless LAN Controller.

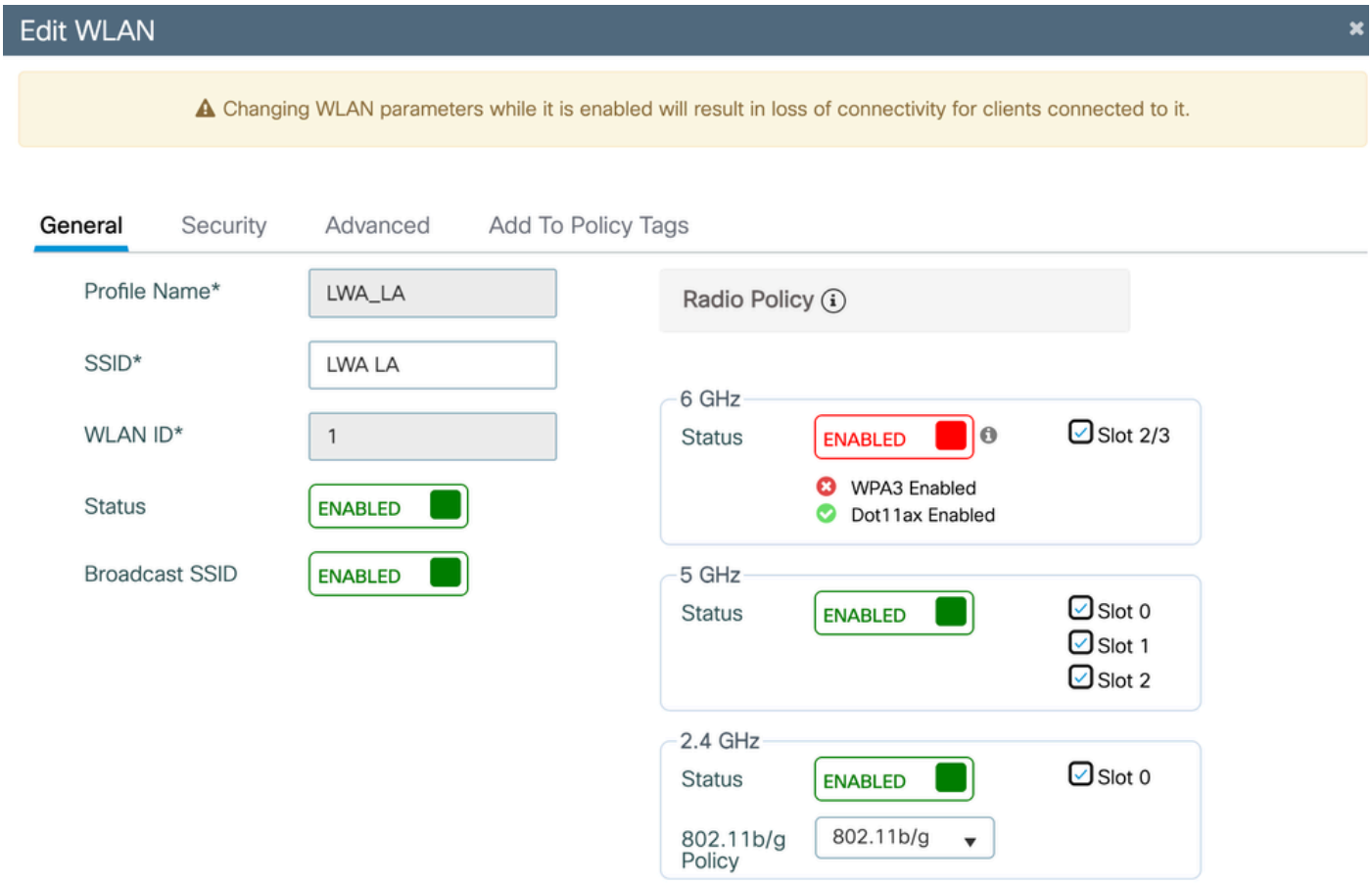

Edit Web Auth Parameter
General
Advanced
Parameter-map Name
global
Maximum HTTP connections
100
Init-State Timeout(secs)
120
Type
webauth
Captive Bypass Portal
Disable Success Window
Disable Logout Window
Disable Cisco Logo
Sleeping Client Status
Sleeping Client Timeout (minutes)
720
Virtual IPv4 Address
192.0.2.1
Trustpoint
TP-self-signed-...
Virtual IPv4 Hostname
Virtual IPv6 Address
x:x:x:x::x
Web Auth intercept HTTPs
Enable HTTP server for Web Auth
Disable HTTP secure server for Web Auth
Banner Configuration
Banner Title
Banner Type
None
Banner Text
Read From File



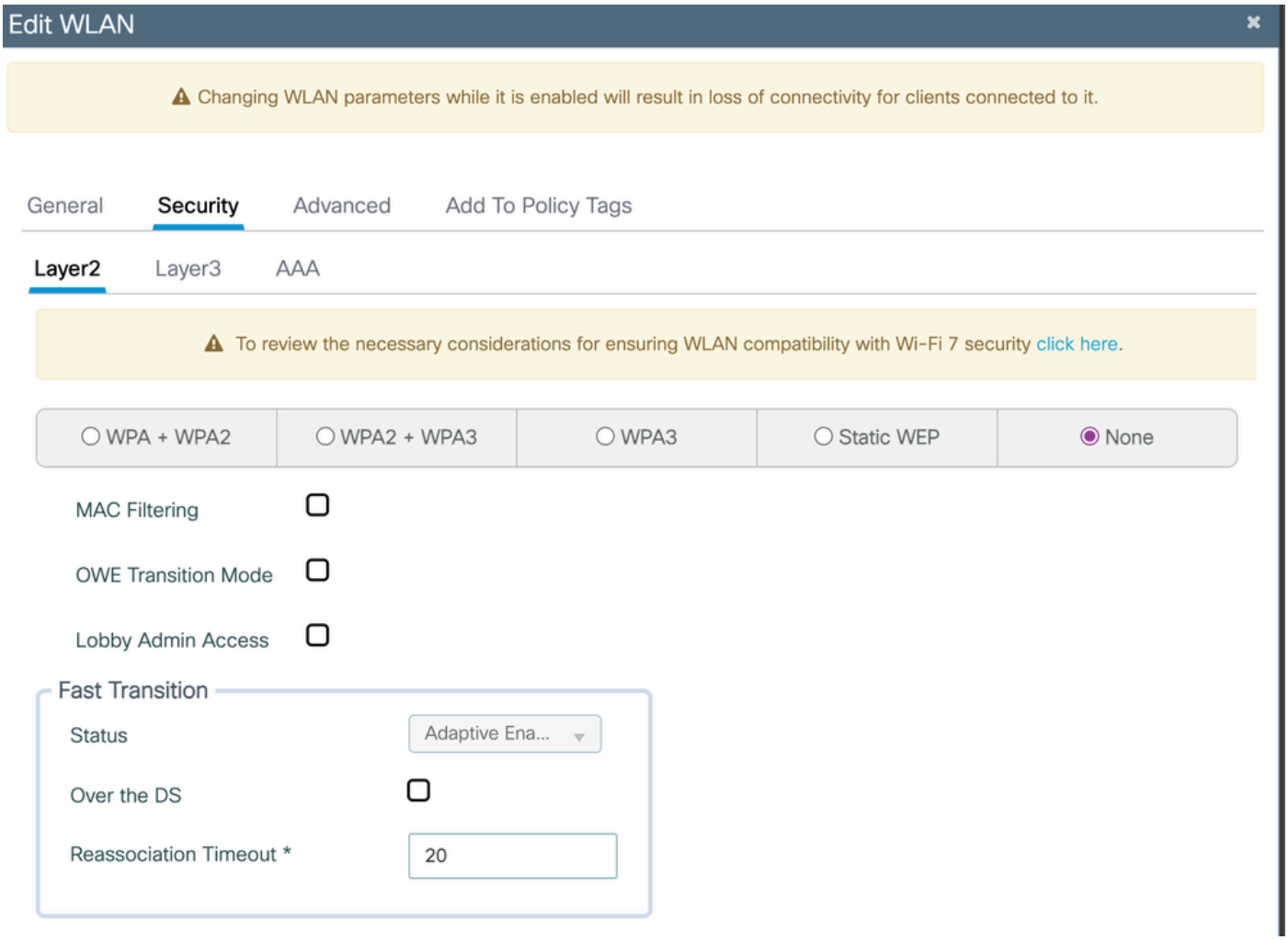
Attenzione: Se il protocollo HTTP è stato disabilitato a livello globale sul router 9800, verificare che l'opzione Abilita server HTTP per autenticazione Web sia selezionata in quanto Cisco ha separato la dipendenza di questi processi. I client o i supplicant devono avviare un processo di connessione HTTP e tale sessione viene intercettata dal controller per la presentazione del portale Web. Per questo motivo non è consigliabile abilitare Web Auth Intercept HTTPS a meno che non sia assolutamente necessario, in quanto questa impostazione non è necessaria per la maggior parte delle distribuzioni e può aumentare l'utilizzo della CPU del controller, con un potenziale impatto sulle prestazioni.

Parametri di sicurezza WLAN

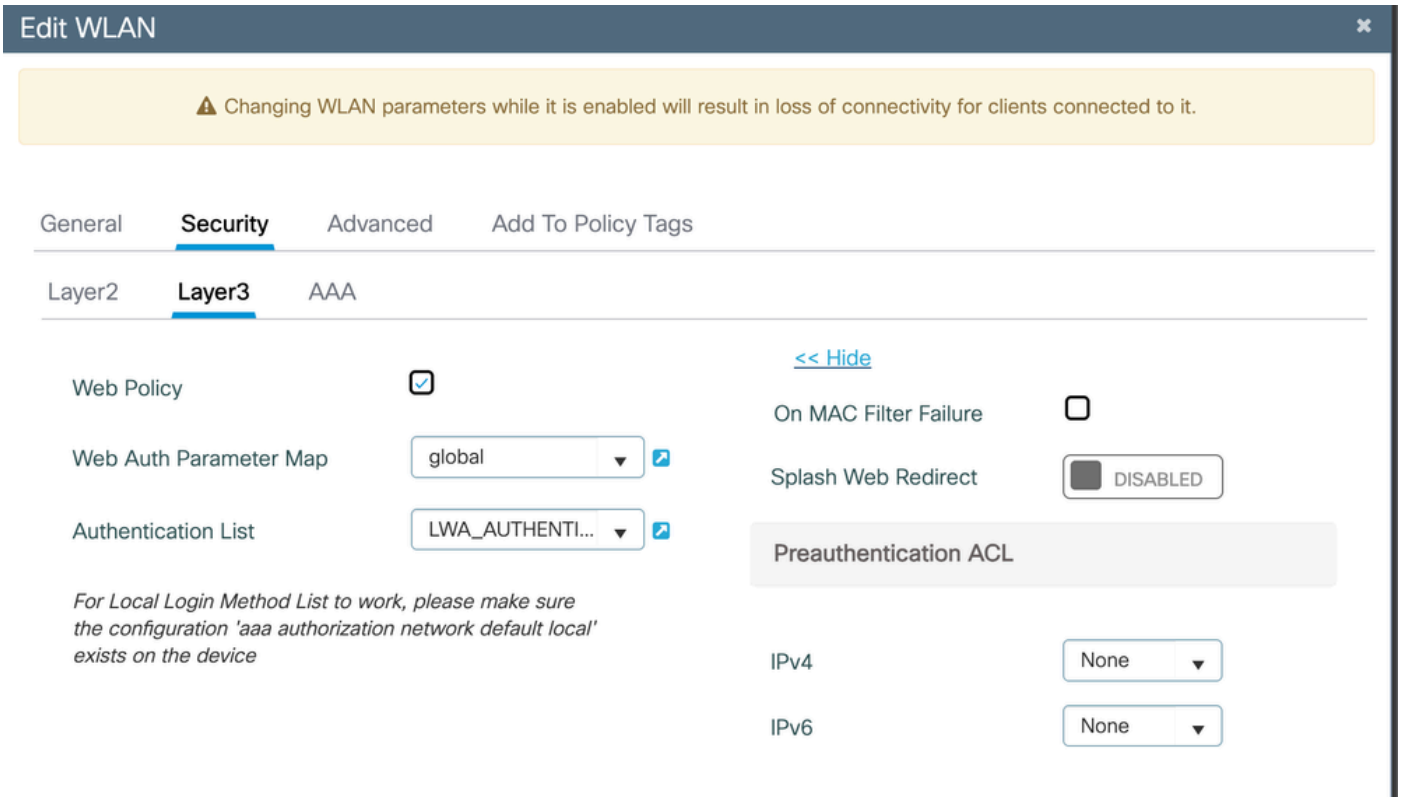
Selezionare Configurazione > Tag e profili > WLAN, quindi fare clic su Aggiungi.



Nella scheda Protezione selezionare Nessuno per Layer2.

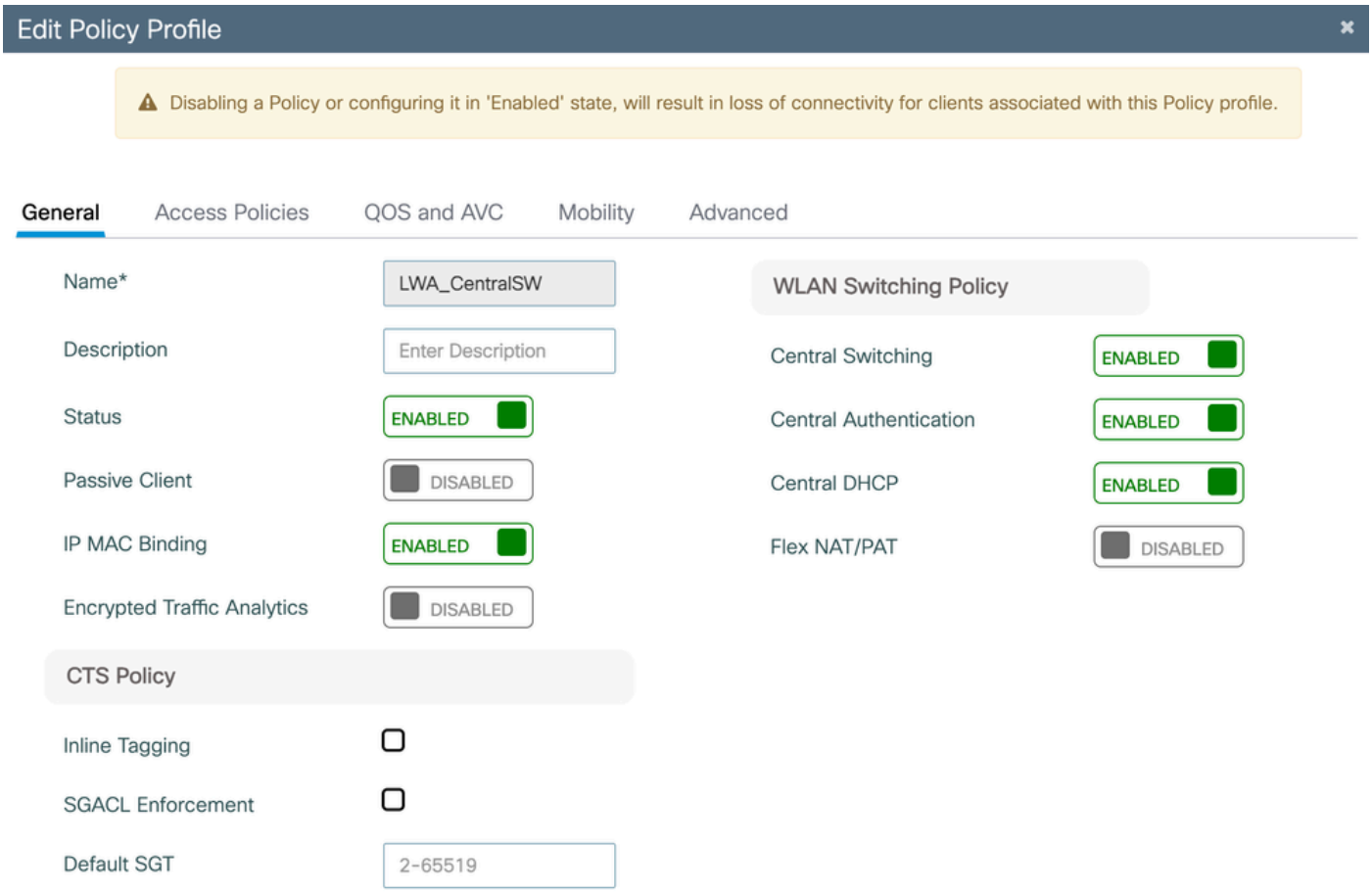


Nella scheda Protezione selezionare la casella Criteri Web nella casella Livello3, quindi selezionare la mappa dei parametri precedentemente configurata dal menu a discesa e dall'elenco di autenticazione.

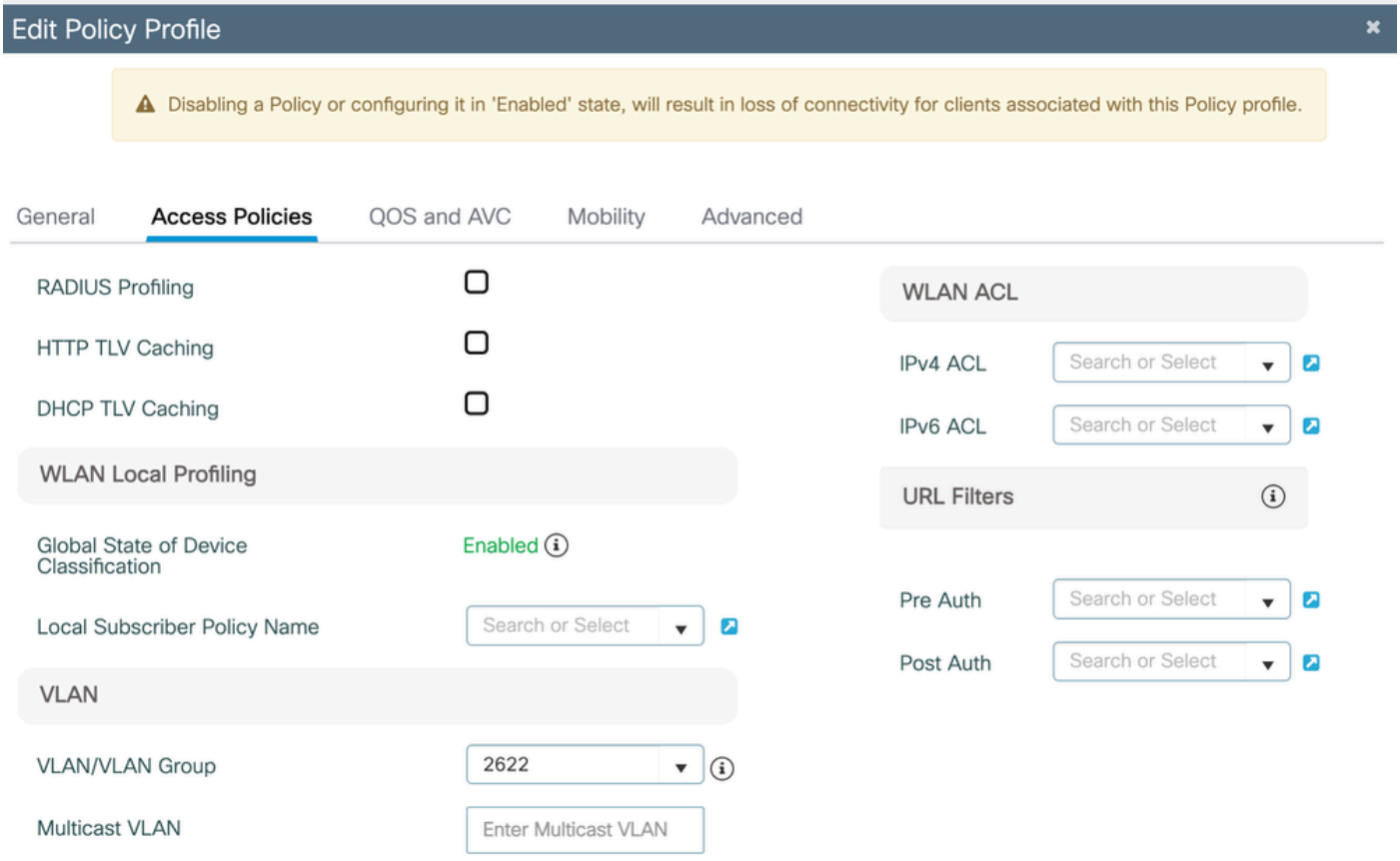


Crea un profilo criteri

Per creare il profilo della policy da collegare al profilo WLAN, selezionare Configurazione > Tag e profili > Policy.

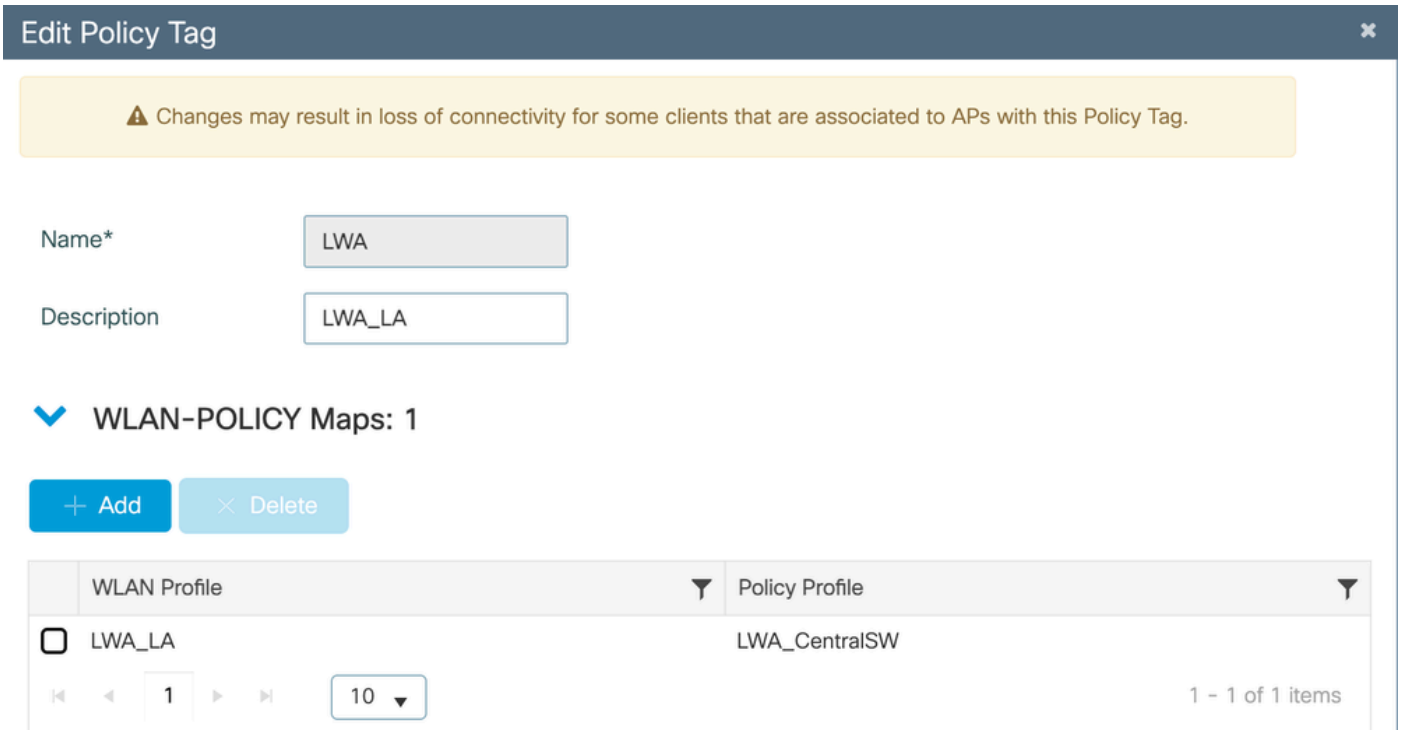


Nella scheda Access Policies (Criteri di accesso), selezionare la VLAN da cui i client/richiedenti devono richiedere un indirizzo IP.



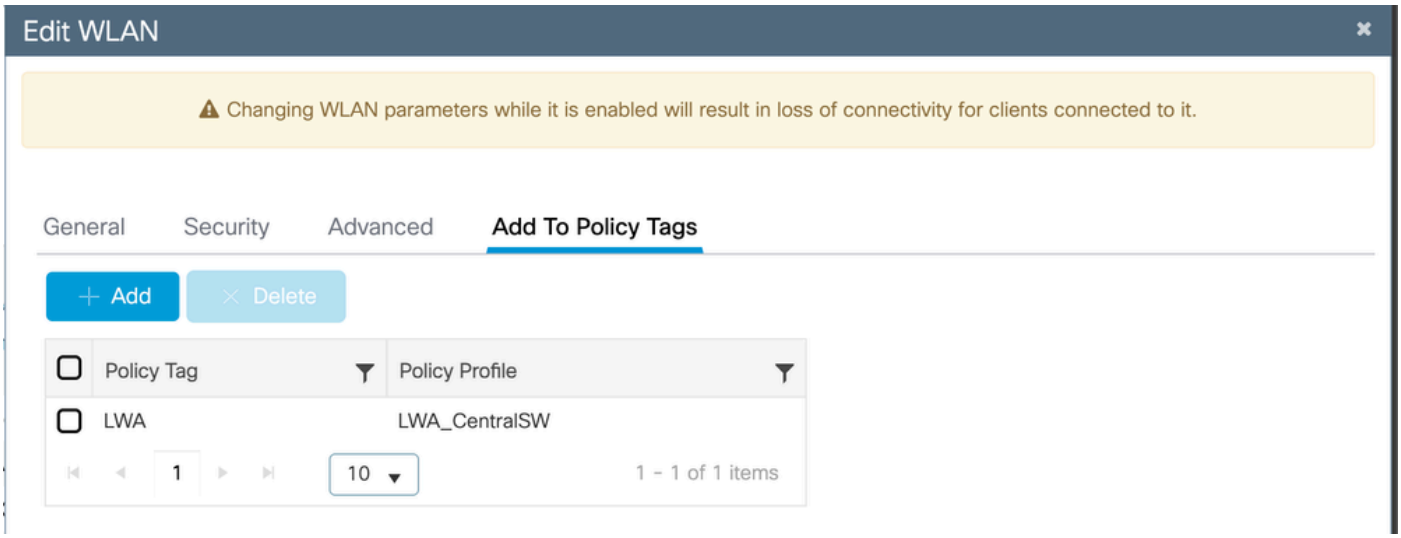
Crea un tag di criteri

Per questa guida alla configurazione è stato creato un tag di criterio personalizzato denominato LWA.



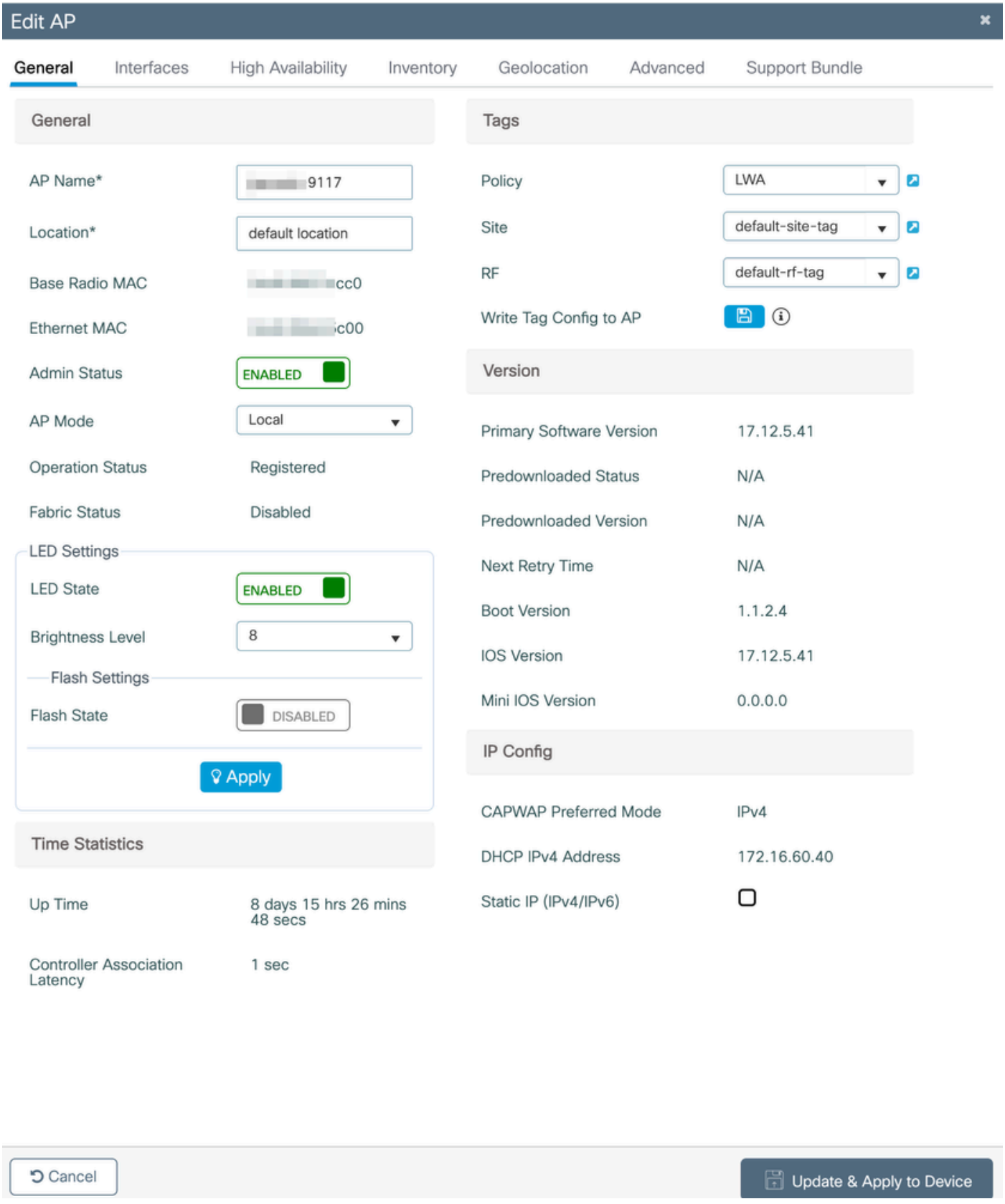
Associare il profilo WLAN e criteri

Per collegare le policy di switching dal Profilo policy alla WLAN, selezionare Configurazione > Tag e profili > WLAN, selezionare il Profilo WLAN, fare clic su Aggiungi a tag policy.



Assegnazione di un tag di criterio a un punto di accesso

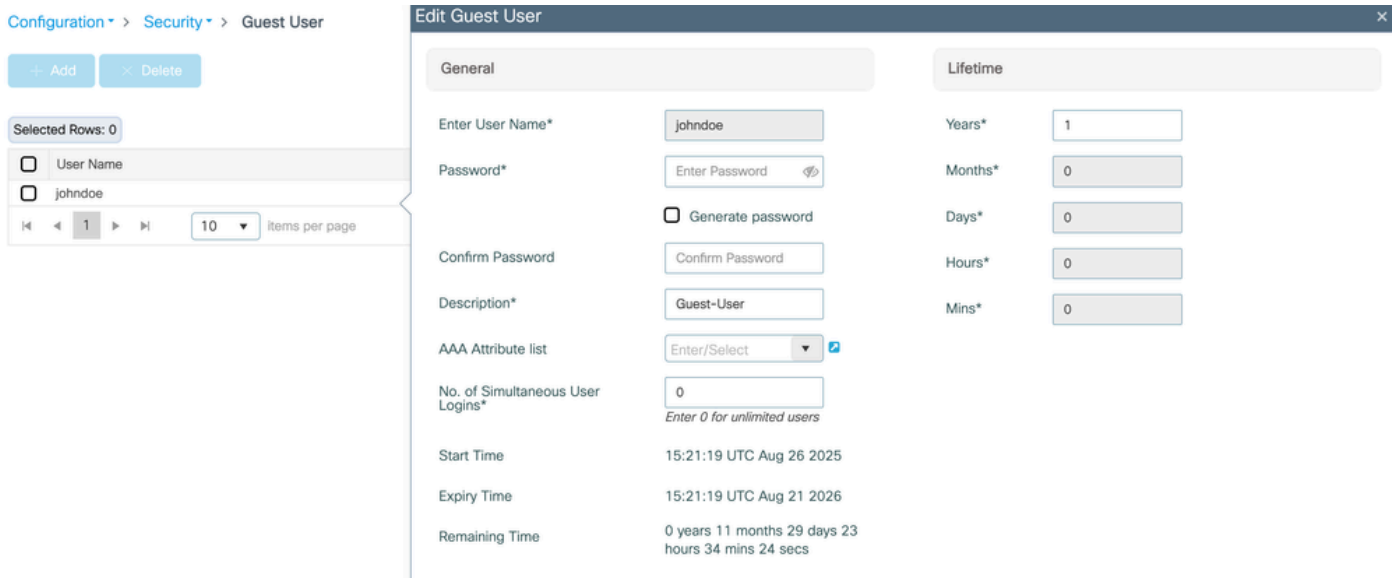
Per associare un tag all'access point con il tag della policy creato, selezionare Configurazione > Wireless > Access Point, selezionare l'access point e nella scheda Generale, a destra, sono presenti i tag utilizzati dall'access point.



Crea nome utente guest

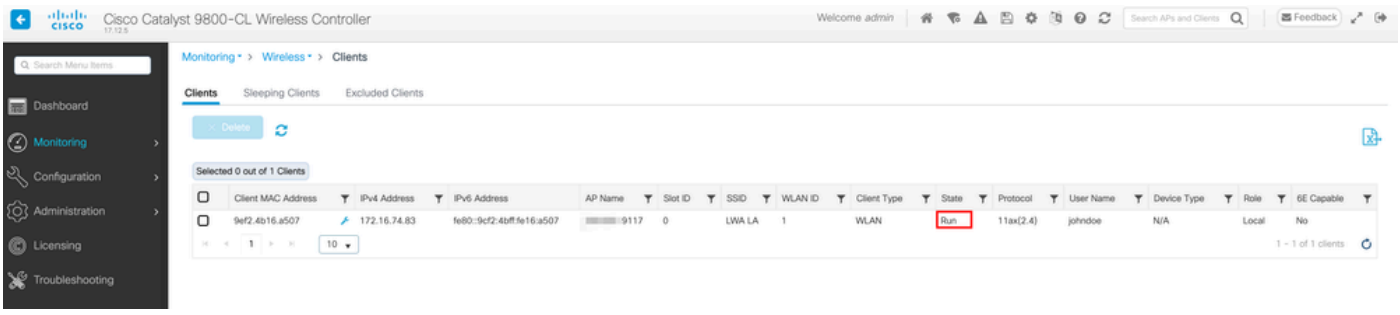
Se è stato selezionato il tipo webauth nella mappa dei parametri, è necessario un nome utente guest per crearlo. Passare a Configurazione > Protezione > Utente guest.

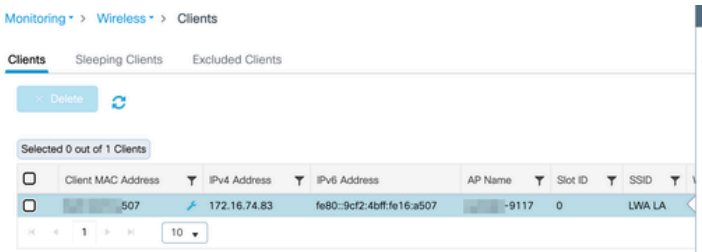
La durata massima dell'utente è di 1 anno. È possibile specificare un valore diverso con le opzioni disponibili.

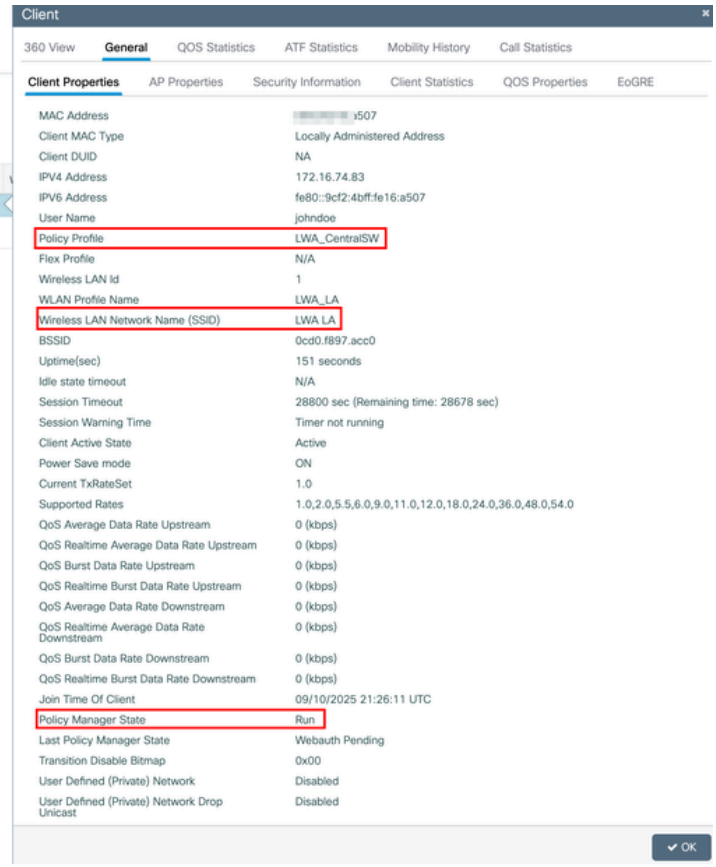


Verifica

Tramite GUI







Tramite CLI

```
9800WLC>enable
9800WLC#show wireless client summary
Number of Clients: 1
MAC Address      AP Name       Type ID State Protocol  Method    Role
-------------------------------------------------------------------------------------------------------------
9ef2.4b16.a507   xxxxx-9117 WLAN 1  Run   11ax(2.4) Web Auth  Local
9800WLC#show wireless client mac-address


        detail


Client MAC Address : 9ef2.4b16.a507


Client MAC Type : Locally Administered Address


Client DUID: NA


Client IPv4 Address : 172.16.74.83


Client IPv6 Addresses : fe80::9cf2:4bff:fe16:a507


Client Username : johndoe
```

AP MAC Address : 0cd0.f897.acc0

AP Name: xxxxx-9117

AP slot : 0

Client State : Associated

Policy Profile : LWA_CentralSW

Flex Profile : N/A

Wireless LAN Id: 1

WLAN Profile Name: LWA_LA

Wireless LAN Network Name (SSID): LWA LA

BSSID : 0cd0.f897.acc0

Connected For : 392 seconds

Protocol : 802.11ax - 2.4 GHz

Channel : 11

Client IIF-ID : 0xa0000002

Association Id : 1

Authentication Algorithm : Open System

Idle state timeout : N/A

Session Timeout : 28800 sec (Remaining time: 28455 sec)

Session Warning Time : Timer not running

Input Policy Name : None

Input Policy State : None

Input Policy Source : None

Output Policy Name : None

Output Policy State : None

Output Policy Source : None

WMM Support : Enabled

U-APSD Support : Disabled

Fastlane Support : Disabled

Client Active State : Active

Power Save : ON

Current Rate : m0 ss2

Supported Rates : 1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0

AAA QoS Rate Limit Parameters:

QoS Average Data Rate Upstream : 0 (kbps)

QoS Realtime Average Data Rate Upstream : 0 (kbps)

QoS Burst Data Rate Upstream : 0 (kbps)

QoS Realtime Burst Data Rate Upstream : 0 (kbps)

QoS Average Data Rate Downstream : 0 (kbps)

QoS Realtime Average Data Rate Downstream : 0 (kbps)

QoS Burst Data Rate Downstream : 0 (kbps)

QoS Realtime Burst Data Rate Downstream : 0 (kbps)

Mobility:

Move Count : 0

Mobility Role : Local

Mobility Roam Type : None

Mobility Complete Timestamp : 09/10/2025 21:41:11 UTC

Client Join Time:

Join Time Of Client : 09/10/2025 21:41:11 UTC

Client State Servers : None

Client ACLs : None

Policy Manager State: Run

Last Policy Manager State : Webauth Pending

Client Entry Create Time : 392 seconds

Policy Type : N/A

Encryption Cipher : None

Transition Disable Bitmap : 0x00

User Defined (Private) Network : Disabled

User Defined (Private) Network Drop Unicast : Disabled

Encrypted Traffic Analytics : No

Protected Management Frame - 802.11w : No

EAP Type : Not Applicable

VLAN Override after Webauth : No

VLAN : 2667

Multicast VLAN : 0

VRF Name : N/A

WiFi Direct Capabilities:

WiFi Direct Capable : No

Central NAT : DISABLED

Session Manager:

Point of Attachment : capwap_90400005

IIF ID : 0x90400005

Authorized : TRUE

Session timeout : 28800

Common Session ID: 044A10AC0000000F359351E3

Acct Session ID : 0x00000000

Auth Method Status List

Method : Web Auth

Webauth State : Authz

Webauth Method : Webauth

Local Policies:

Service Template : IP-Adm-V4-LOGOUT-ACL (priority 100)

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

Service Template : wlan_svc_LWA_CentralSW_local (priority 254)

VLAN : 2667

Absolute-Timer : 28800

Server Policies:

Resultant Policies:

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

VLAN Name : xxxxx

VLAN : 2667

Absolute-Timer : 28800

DNS Snooped IPv4 Addresses : None

DNS Snooped IPv6 Addresses : None

Client Capabilities

CF Pollable : Not implemented

CF Poll Request : Not implemented

Short Preamble : Not implemented

PBCC : Not implemented

Channel Agility : Not implemented

Listen Interval : 0

Fast BSS Transition Details :

Reassociation Timeout : 0

11v BSS Transition : Implemented

11v DMS Capable : No

QoS Map Capable : Yes

FlexConnect Data Switching : N/A

FlexConnect Dhcp Status : N/A

FlexConnect Authentication : N/A

Client Statistics:

Number of Bytes Received from Client : 111696

Number of Bytes Sent to Client : 62671

Number of Packets Received from Client : 529

Number of Packets Sent to Client : 268

Number of Data Retries : 136

Number of RTS Retries : 0

Number of Tx Total Dropped Packets : 1

Number of Duplicate Received Packets : 0

Number of Decrypt Failed Packets : 0

Number of Mic Failured Packets : 0

Number of Mic Missing Packets : 0

Number of Policy Errors : 0

Radio Signal Strength Indicator : -61 dBm

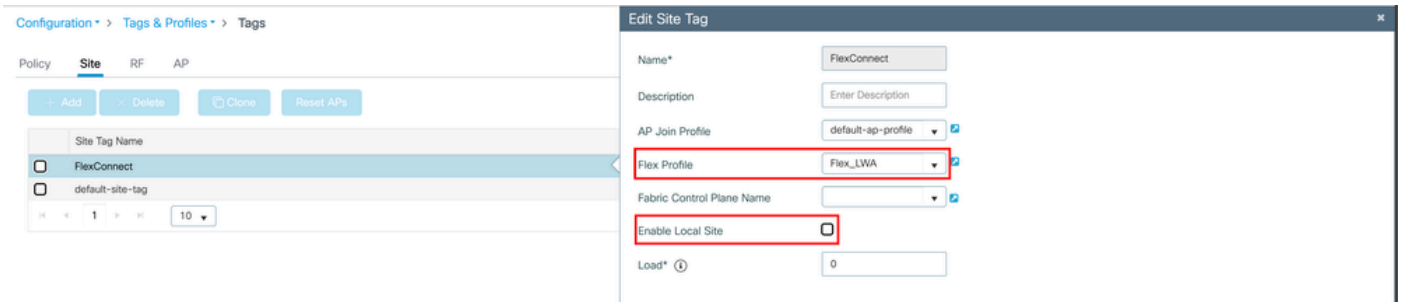
Signal to Noise Ratio : 4 dB

Fabric status : Disabled

```
Radio Measurement Enabled Capabilities

Capabilities: Link Measurement, Neighbor Report, Repeated Measurements, Passive Beacon Measurement, Act

Client Scan Report Time : Timer not running

Client Scan Reports

Assisted Roaming Neighbor List

Nearby AP Statistics:

EoGRE : Pending Classification

Max Client Protocol Capability: Wi-Fi6 (802.11ax)

WiFi to Cellular Steering : Not implemented

Cellular Capability : N/A

Advanced Scheduling Requests Details:

Apple Specific Requests(ASR) Capabilities/Statistics:

Regular ASR support: DISABLED
```

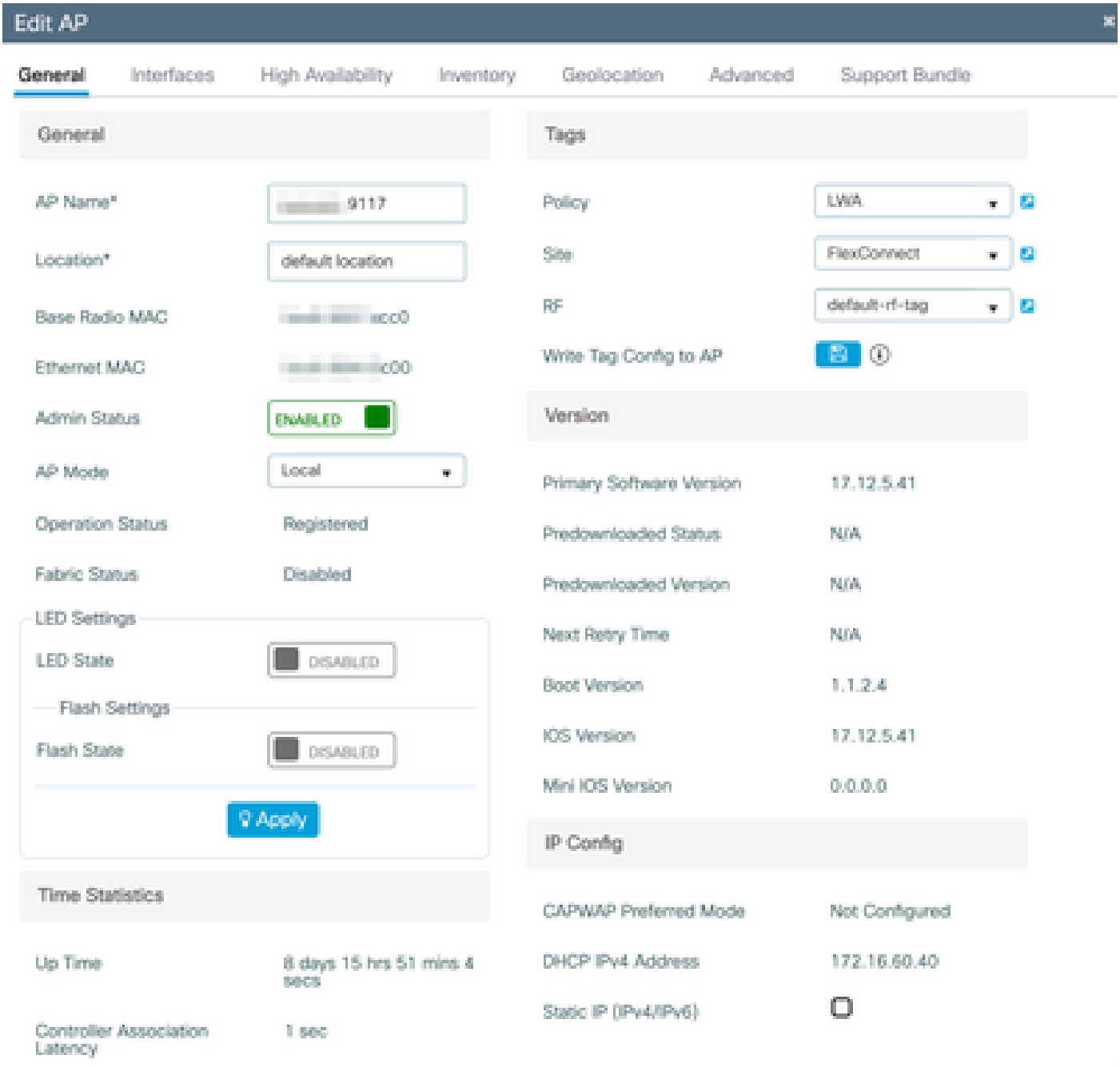
Autenticazione Web locale su switching locale FlexConnect

In questo scenario, si presume che l'access point sia in modalità FlexConnect. Affinché un punto di accesso sia in modalità FlexConnect, è necessario che sia associato un profilo Flex nel tag del sito, dove la casella di controllo Abilita sito locale è disabilitata. In questo tag del sito vengono utilizzati l'associazione predefinita e il nome del profilo flessibile personalizzato Flex_LWA:

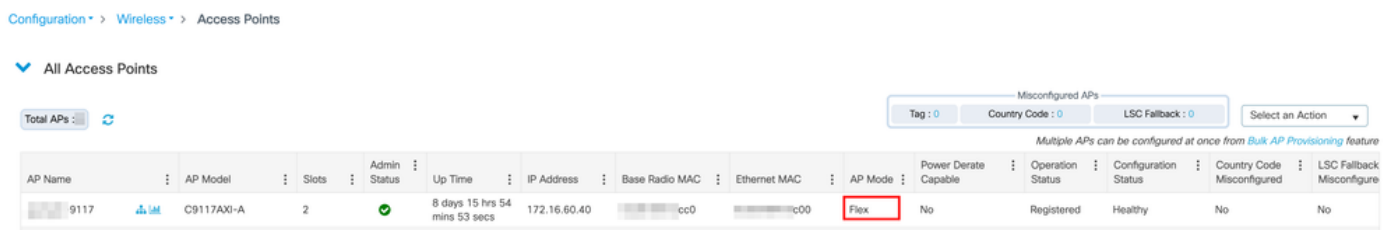


Assegnazione di un tag di criterio a un punto di accesso

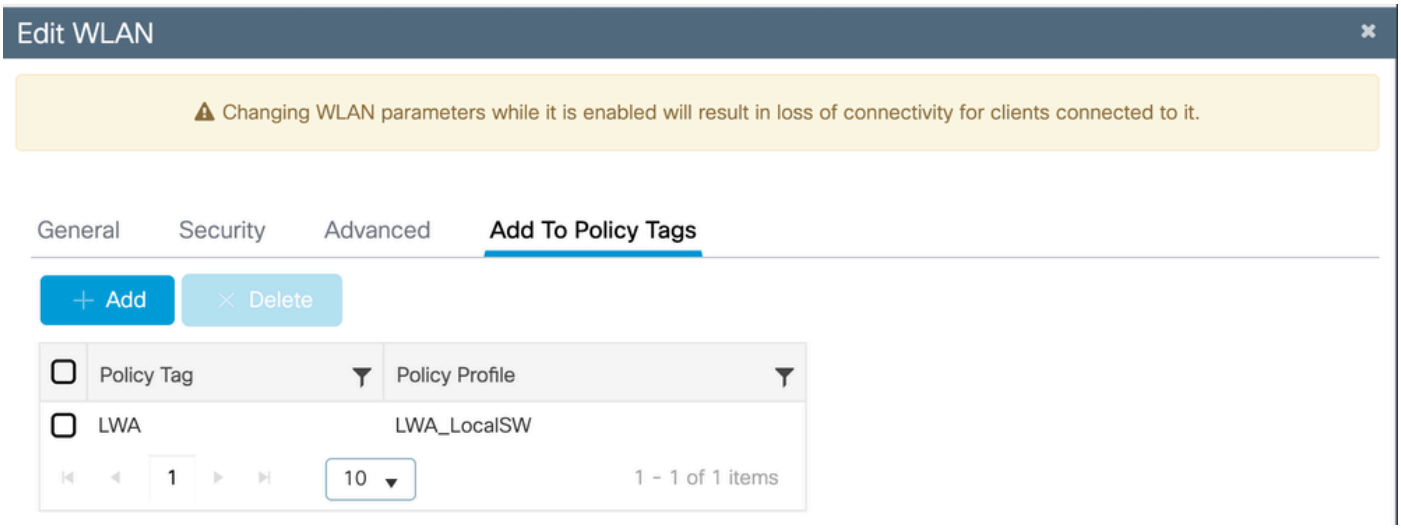
Passare a Configurazione > Wireless > Access Point, selezionare l'access point e nella scheda Generale, a destra, sono presenti i tag utilizzati dall'access point.

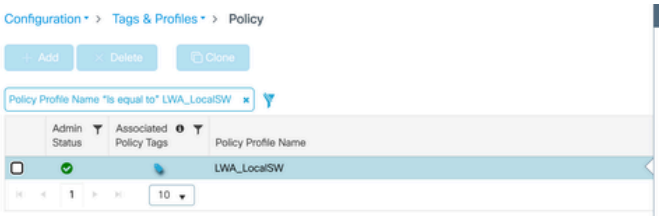


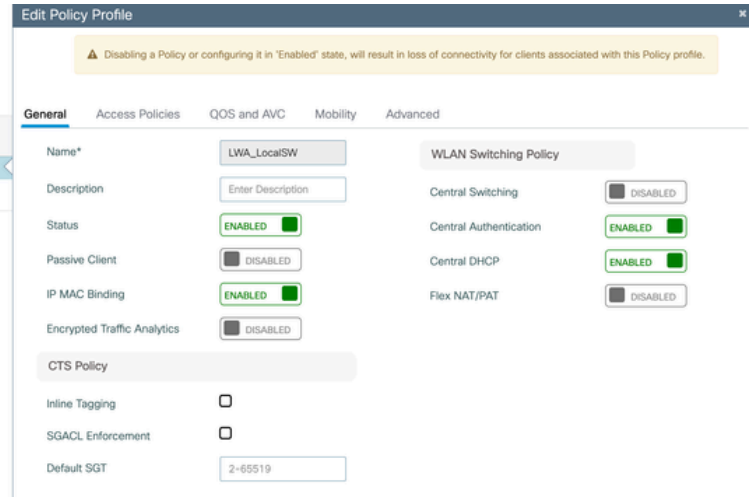
Avviso: La modifica dei tag determina la disconnessione dell'access point dal WLC.



Il profilo della policy associato alla WLAN è Switching locale







Verifica

```
9800WLC>enable
9800WLC#show wireless client summary
Number of Clients: 1
MAC Address      AP Name        Type ID  State Protocol  Method    Role
---------------------------------------------------------------------------------------------
9ef2.4b16.a507 xxxxx-9117 WLAN 1 Run 11ax(2.4) Web Auth Local

9800WLC#show wireless client mac-address


        detail


Client MAC Address :



Client MAC Type : Locally Administered Address


Client DUID: NA
```

Client IPv4 Address : 172.16.74.83

Client IPv6 Addresses : fe80::9cf2:4bff:fe16:a507

Client Username : johndoe

AP MAC Address : xxxx.xxxx.xcc0

AP Name: xxxxxx-9117

AP slot : 0

Client State : Associated

Policy Profile : LWA_LocalSW

Flex Profile : Flex_LWA

Wireless LAN Id: 1

WLAN Profile Name: LWA_LA

Wireless LAN Network Name (SSID): LWA LA

BSSID : 0cd0.f897.acc0

Connected For : 315 seconds

Protocol : 802.11ax - 2.4 GHz

Channel : 6

Client IIF-ID : 0xa0000004

Association Id : 1

Authentication Algorithm : Open System

Idle state timeout : N/A

Session Timeout : 28800 sec (Remaining time: 28525 sec)

Session Warning Time : Timer not running

Input Policy Name : None

Input Policy State : None

Input Policy Source : None

Output Policy Name : None

Output Policy State : None

Output Policy Source : None

WMM Support : Enabled

U-APSD Support : Disabled

Fastlane Support : Disabled

Client Active State : Active

Power Save : ON

Current Rate : m11 ss2

Supported Rates : 1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0

AAA QoS Rate Limit Parameters:

QoS Average Data Rate Upstream : 0 (kbps)

QoS Realtime Average Data Rate Upstream : 0 (kbps)

QoS Burst Data Rate Upstream : 0 (kbps)

QoS Realtime Burst Data Rate Upstream : 0 (kbps)

QoS Average Data Rate Downstream : 0 (kbps)

QoS Realtime Average Data Rate Downstream : 0 (kbps)

QoS Burst Data Rate Downstream : 0 (kbps)

QoS Realtime Burst Data Rate Downstream : 0 (kbps)

Mobility:

Move Count : 0

Mobility Role : Local

Mobility Roam Type : None

Mobility Complete Timestamp : 09/11/2025 17:38:26 UTC

Client Join Time:

Join Time Of Client : 09/11/2025 17:38:26 UTC

Client State Servers : None

Client ACLs : None

Policy Manager State: Run

Last Policy Manager State : Webauth Pending

Client Entry Create Time : 315 seconds

Policy Type : N/A

Encryption Cipher : None

Transition Disable Bitmap : 0x00

User Defined (Private) Network : Disabled

User Defined (Private) Network Drop Unicast : Disabled

Encrypted Traffic Analytics : No

Protected Management Frame - 802.11w : No

EAP Type : Not Applicable

VLAN Override after Webauth : No

VLAN : 2667

Multicast VLAN : 0

VRF Name : N/A

WiFi Direct Capabilities:

WiFi Direct Capable : No

Central NAT : DISABLED

Session Manager:

Point of Attachment : capwap_90400005

IIF ID : 0x90400005

Authorized : TRUE

Session timeout : 28800

Common Session ID: 044A10AC0000002A39DB6F52

Acct Session ID : 0x00000000

Auth Method Status List

Method : Web Auth

Webauth State : Authz

Webauth Method : Webauth

```
Local Policies:

Service Template : IP-Adm-V4-LOGOUT-ACL (priority 100)

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

Service Template : wlan_svc_LWA_LocalSW (priority 254)

VLAN : 2667

Absolute-Timer : 28800

Server Policies:

Resultant Policies:

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

VLAN Name : xxxxx

VLAN : 2667

Absolute-Timer : 28800

DNS Snooped IPv4 Addresses : None

DNS Snooped IPv6 Addresses : None

Client Capabilities

CF Pollable : Not implemented

CF Poll Request : Not implemented

Short Preamble : Not implemented

PBCC : Not implemented

Channel Agility : Not implemented

Listen Interval : 0
```

Fast BSS Transition Details :

Reassociation Timeout : 0

11v BSS Transition : Implemented

11v DMS Capable : No

QoS Map Capable : Yes

FlexConnect Data Switching : Local

FlexConnect Dhcp Status : Central

FlexConnect Authentication : Central

Client Statistics:

Number of Bytes Received from Client : 295564

Number of Bytes Sent to Client : 90146

Number of Packets Received from Client : 1890

Number of Packets Sent to Client : 351

Number of Data Retries : 96

Number of RTS Retries : 0

Number of Tx Total Dropped Packets : 0

Number of Duplicate Received Packets : 0

Number of Decrypt Failed Packets : 0

Number of Mic Failured Packets : 0

Number of Mic Missing Packets : 0

Number of Policy Errors : 0

Radio Signal Strength Indicator : -34 dBm

Signal to Noise Ratio : 31 dB

Fabric status : Disabled

Radio Measurement Enabled Capabilities

Capabilities: Link Measurement, Neighbor Report, Repeated Measurements, Passive Beacon Measurement, Act

Client Scan Report Time : Timer not running

Client Scan Reports

Assisted Roaming Neighbor List

Nearby AP Statistics:

EoGRE : Pending Classification

Max Client Protocol Capability: Wi-Fi6 (802.11ax)

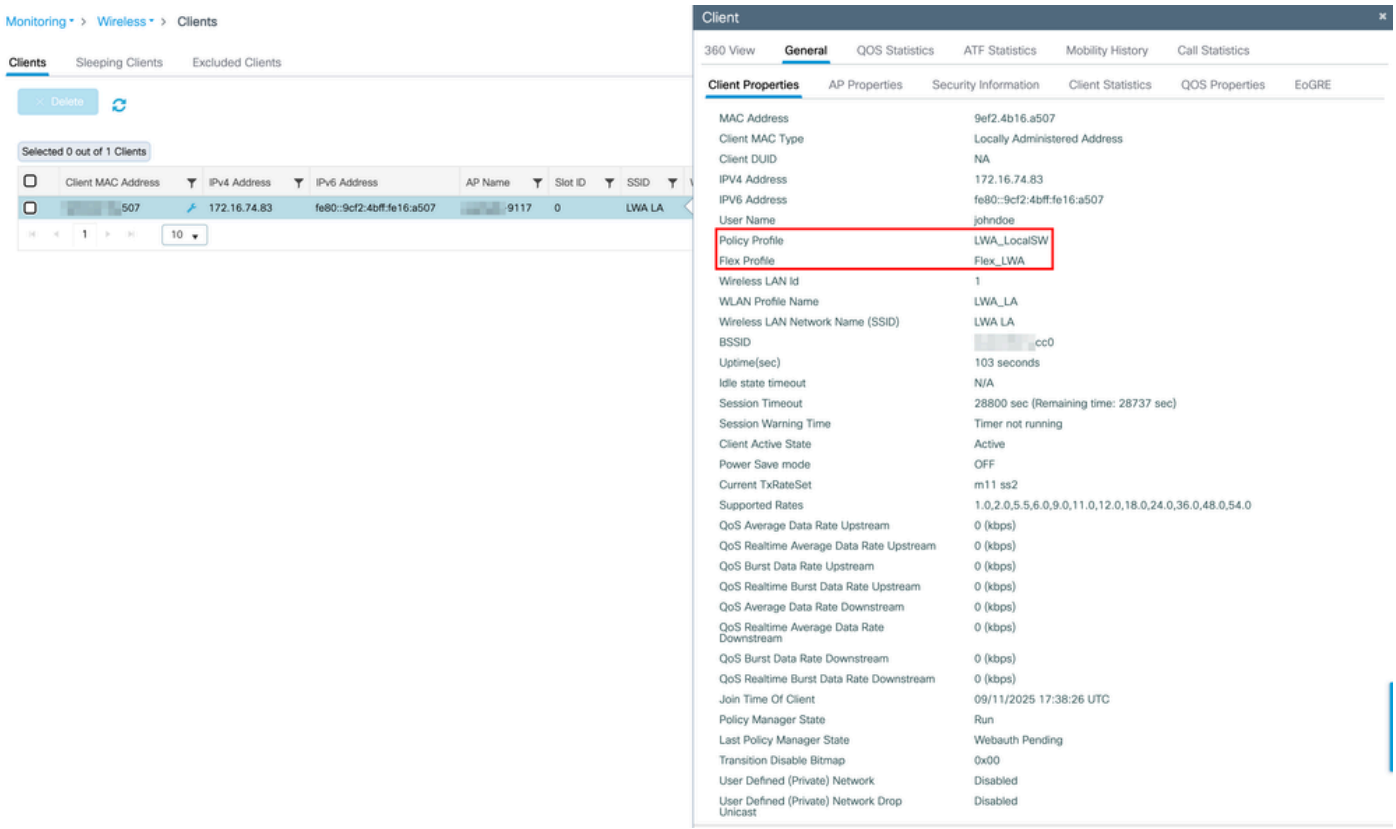
WiFi to Cellular Steering : Not implemented

Cellular Capability : N/A

Advanced Scheduling Requests Details:

Apple Specific Requests(ASR) Capabilities/Statistics:

Regular ASR support: DISABLED



Risoluzione dei problemi

Lo stato "Web Auth Pending" (Autenticazione Web in sospeso) indica che il client è stato associato al punto di accesso ma non ha ancora completato il processo di autenticazione Web. Durante questo stato, il controller intercetta il traffico HTTP del client e lo reindirizza a un portale di autenticazione Web per l'accesso utente o l'accettazione dei termini. Il client rimane in questo stato fino al completamento dell'autenticazione Web, dopodiché lo stato di Gestione criteri client passa a "Esegui" e viene concesso l'accesso completo alla rete.

per visualizzare il flusso della connessione client, verificare il flusso LWA da Configura autenticazione Web locale con autenticazione esterna.

Le fasi sottomesse dal client dal punto di vista del client sono descritte in Risoluzione dei problemi comuni con LWA su 9800 WLC.

- Documentazione e supporto tecnico – Cisco Systems

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).