

Configurazione dell'autenticazione Web centrale (CWA) su Catalyst 9800 WLC e ISE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione AAA sui controller 9800 WLC](#)

[Configurazione della WLAN](#)

[Configurazione del profilo di policy](#)

[Configurazione del tag di policy](#)

[Assegnazione di un tag di policy](#)

[Configurazione degli ACL di reindirizzamento](#)

[Abilita reindirizzamento per HTTP o HTTPS](#)

[Configurazione di ISE](#)

[Aggiunta di controller 9800 WLC a ISE](#)

[Creazione di un nuovo utente in ISE](#)

[Creazione del profilo di autorizzazione](#)

[Configurazione della regola di autenticazione](#)

[Configurazione delle regole di autorizzazione](#)

[SOLO FlexConnect Access Point con switching locale](#)

[Certificati](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Elenco di controllo](#)

[Supporto porta servizio per RADIUS](#)

[Raccogli debug](#)

[Esempi](#)

Introduzione

Questo documento descrive come configurare una LAN wireless CWA su uno switch Catalyst 9800 WLC e ISE.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza della configurazione dei Wireless LAN Controller (WLC) 9800.

Componenti usati

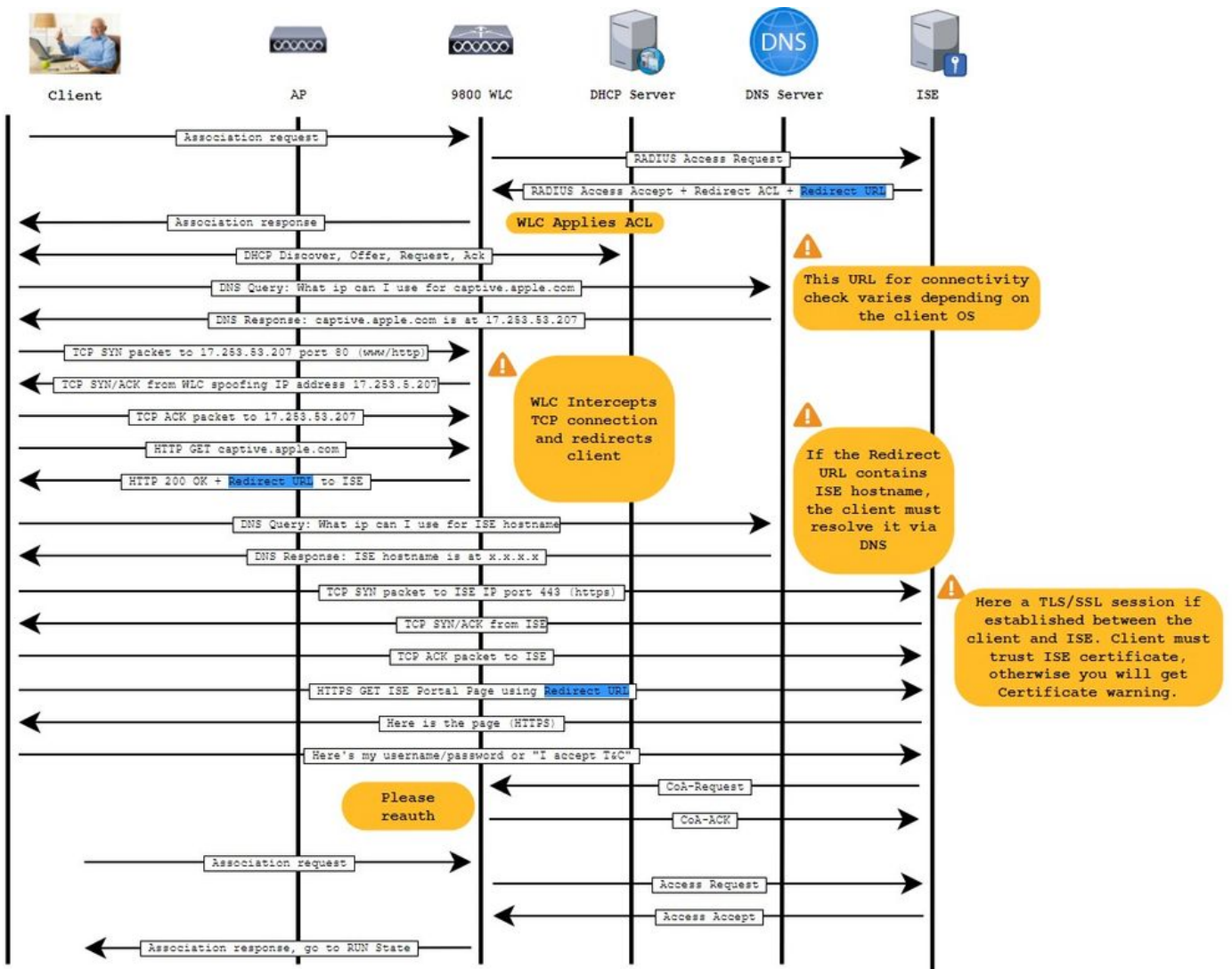
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- 9800 WLC Cisco IOS® XE Gibraltar v17.6.x
- Identity Service Engine (ISE) v3.0

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.

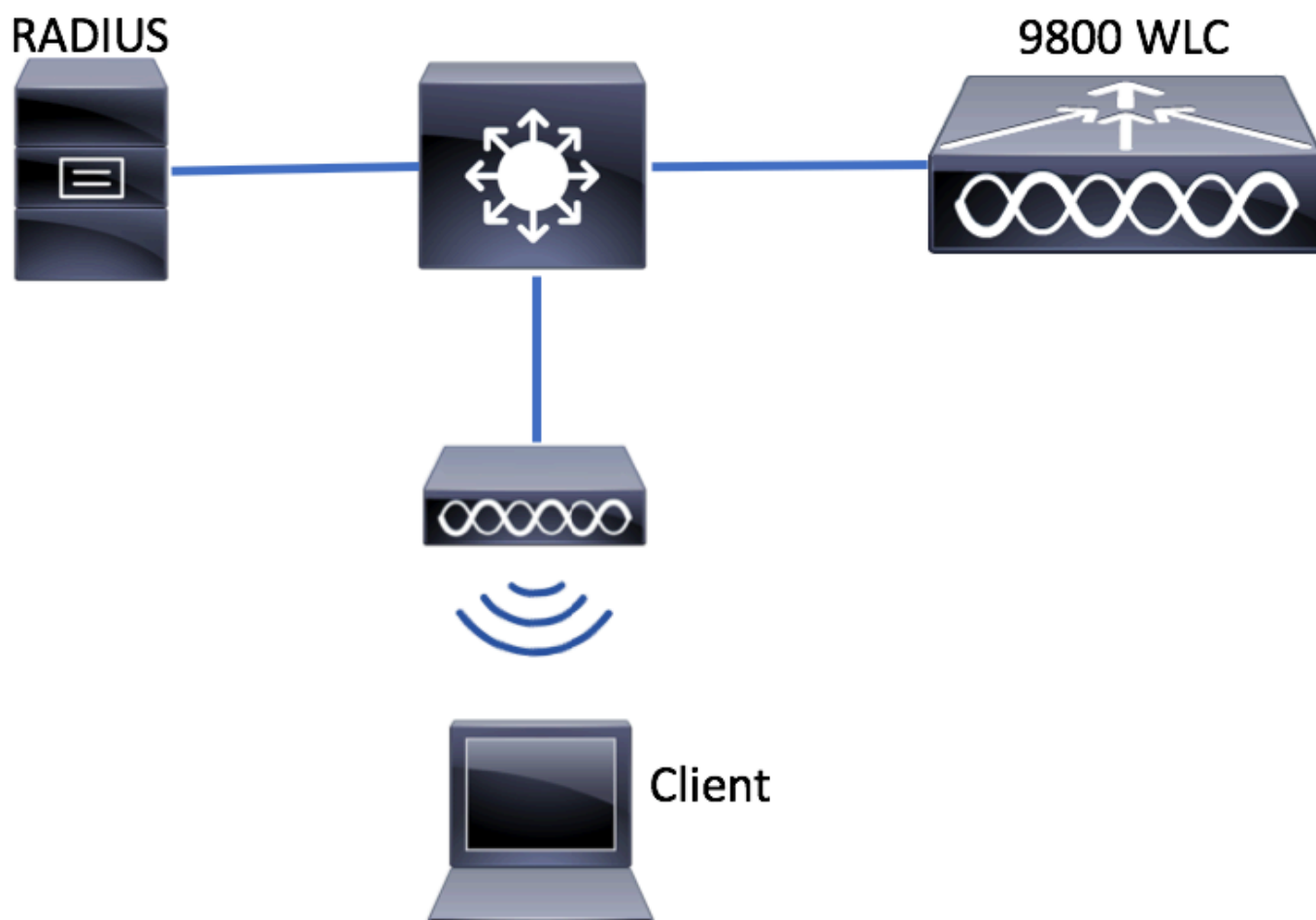
Premesse

Il processo CWA è illustrato di seguito, ad esempio il processo CWA di un dispositivo Apple:



Configurazione

Esempio di rete



Configurazione AAA sui controller 9800 WLC

Passaggio 1. Aggiungere il server ISE alla configurazione WLC 9800.

Individuare Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add e immettere le informazioni sul server RADIUS come mostrato nelle immagini.

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add × Delete

RADIUS

TACACS+

LDAP

Servers Server Groups

Name	Address
0 items per page	

Verificare che l'opzione Support for CoA (Supporto per CoA) sia abilitata se si pensa di usare in futuro l'autenticazione Web centralizzata o altro tipo di sicurezza che richieda una modifica di autorizzazione, o CoA (Change of Authorization).

Create AAA Radius Server

Name* ISE-server

Server Address* [Redacted]

PAC Key

Key Type Clear Text

Key* [Redacted]

Confirm Key* [Redacted]

Auth Port 1812

Acct Port 1813

Server Timeout (seconds) 1-1000

Retry Count 0-100

Support for CoA ENABLED

CoA Server Key Type Clear Text

CoA Server Key [Redacted]

Confirm CoA Server Key [Redacted]

Automate Tester

Cancel Apply to Device



Nota: nella versione 17.4.X e successive, assicurarsi di configurare anche la chiave del server CoA quando si configura il server RADIUS. Utilizzare la stessa chiave del segreto condiviso (per impostazione predefinita, sono le stesse in ISE). Lo scopo è quello di configurare facoltativamente una chiave diversa per il certificato di autenticità (CoA) rispetto al segreto condiviso, se questo è ciò che è stato configurato dal server RADIUS. In Cisco IOS XE 17.3, l'interfaccia utente Web ha semplicemente utilizzato lo stesso segreto condiviso della chiave CoA.

Passaggio 2. Creare un elenco di metodi di autorizzazione.

Passare a Configuration > Security > AAA > AAA Method List > Authorization > + Add come mostrato nell'immagine.

Search Menu Items

- Dashboard
- Monitoring
- Configuration**
- Administration
- Troubleshooting

Authentication Authorization and Accounting

+ AAA Wizard

AAA Method List Servers / Groups AAA Advanced

General

Authentication

Authorization

Accounting

+ Add **x Delete**

Name	Type	Group Type	Group
<input type="checkbox"/> default	network	local	N/A

10 items per page

Quick Setup: AAA Authorization

Method List Name* **CWAauthz**

Type* network

Group Type group

Fallback to local

Authenticated

Available Server Groups **Assigned Server Groups**

ldap
tacacs+

>
<
>>
<<

radius

^
^
v
v

Passaggio 3. (Facoltativo) Creare un elenco di metodi contabili come mostrato nell'immagine.

Quick Setup: AAA Accounting

Method List Name*

Type*

Available Server Groups: ldap, tacacs+

Assigned Server Groups: radius

Buttons: Cancel, Apply to Device

Nota: CWA non funziona se si decide di bilanciare il carico (dalla configurazione CLI di Cisco IOS XE) dei server radius a causa dell'ID bug Cisco [CSCvh03827](https://cisco.com/cisco/webbugtool/CSCvh03827). L'utilizzo dei servizi di bilanciamento del carico esterni è corretto. Verificare tuttavia che il servizio di bilanciamento del carico funzioni per client utilizzando l'attributo RADIUS id stazione chiamante. L'utilizzo della porta di origine UDP non è un meccanismo supportato per il bilanciamento delle richieste RADIUS provenienti da 9800.

Passaggio 4. (Facoltativo) È possibile definire la policy AAA per inviare il nome SSID come attributo ID stazione chiamata. Questa condizione può essere utile se si desidera sfruttare questa condizione su ISE in un secondo momento del processo.

Individuare Configuration > Security > Wireless AAA Policy il criterio AAA predefinito e modificarlo oppure crearne uno nuovo.

- Dashboard
- Monitoring >
- Configuration** >
- Administration >
- Troubleshooting

Configuration > Security > **Wireless AAA Policy**

+ Add
× Delete

Policy Name
<input type="checkbox"/> default-aaa-policy

⏪
⏩
1
⏪
⏩
10 items per page

L'opzione 1 può essere selezionata SSID. Tenere presente che anche quando si sceglie solo SSID, l'ID stazione chiamato continua ad aggiungere l'indirizzo MAC AP al nome SSID.

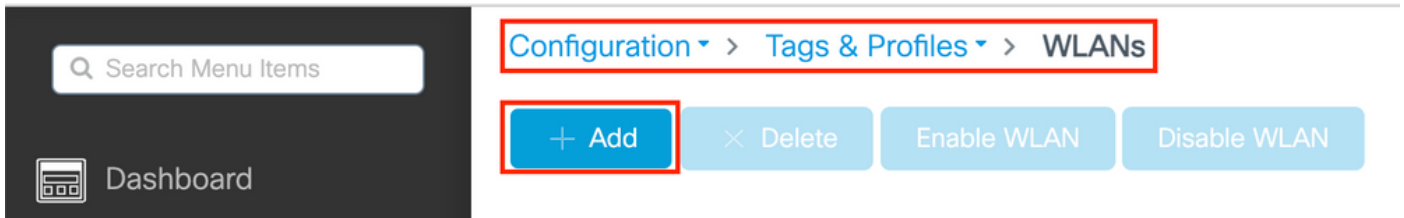
Edit Wireless AAA Policy

Policy Name*	<input style="width: 90%; border: 1px solid #ccc;" type="text" value="default-aaa-policy"/>
Option 1	<input style="width: 90%; border: 1px solid #ccc;" type="text" value="SSID"/>
Option 2	<input style="width: 90%; border: 1px solid #ccc;" type="text" value="Not Configured"/>
Option 3	<input style="width: 90%; border: 1px solid #ccc;" type="text" value="Not Configured"/>

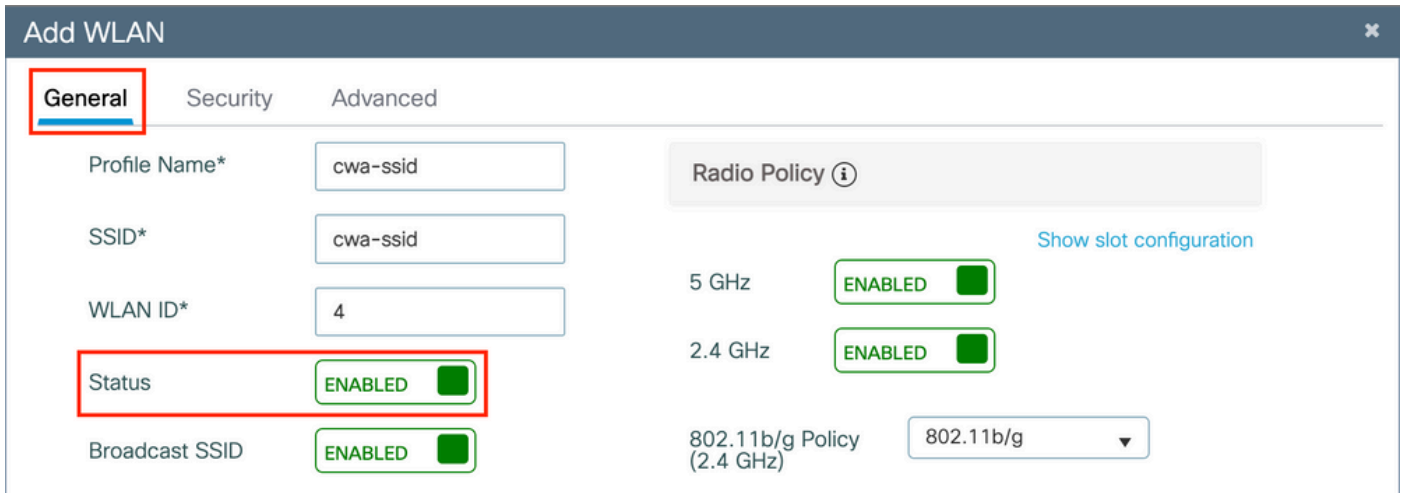
Configurazione della WLAN

Passaggio 1. Creare la WLAN.

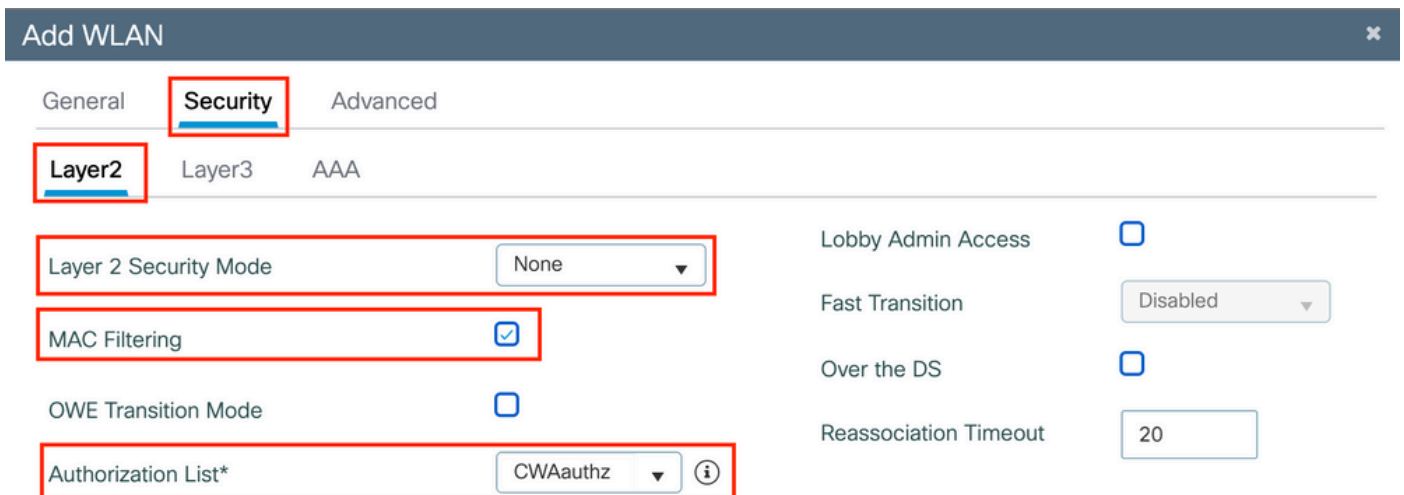
Passare alla rete Configuration > Tags & Profiles > WLANs > + Add e configurarla in base alle esigenze.



Passaggio 2. Immettere le informazioni generali sulla WLAN.



Passaggio 3. Passare alla Security scheda e scegliere il metodo di protezione desiderato. In questo caso, sono necessari solo il filtro MAC e l'elenco di autorizzazioni AAA (creato nel Passaggio 2. della AAA Configuration sezione).



CLI:

```
#config t
(config)#wlan cwa-ssid 4 cwa-ssid
(config-wlan)#mac-filtering CWAauthz
(config-wlan)#no security ft adaptive
(config-wlan)#no security wpa
(config-wlan)#no security wpa wpa2
```

```
(config-wlan)#no security wpa wpa2 ciphers aes
(config-wlan)#no security wpa akm dot1x
(config-wlan)#no shutdown
```

Configurazione del profilo di policy

All'interno di un profilo di policy, è possibile decidere di assegnare ai client la VLAN desiderata, tra le altre impostazioni (ad esempio, Access Controls List (ACL), Quality of Service (QoS), Mobility Anchor, Timer e così via).

È possibile usare il profilo di policy predefinito oppure crearne uno nuovo.

GUI:

Passaggio 1. Crea un nuovo Policy Profile oggetto.

Passare a Configuration > Tags & Profiles > Policy e configurare default-policy-profile o crearne uno nuovo.

Policy Profile

+ Add x Delete

Policy Profile Name	Description
<input type="checkbox"/> voice	
<input type="checkbox"/> default-policy-profile	default policy profile

1 10 items per page

Verificare che il profilo sia abilitato.

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

Description

Status ENABLED

Passive Client DISABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

WLAN Switching Policy

Central Switching ENABLED

Central Authentication ENABLED

Central DHCP ENABLED

Flex NAT/PAT DISABLED

Passaggio 2. Selezionare la VLAN.

Passare alla Access Policies scheda e scegliere il nome della VLAN dall'elenco a discesa o digitare manualmente l'ID della VLAN. Non configurare un ACL nel profilo di policy.

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select ▼

VLAN

VLAN/VLAN Group

VLAN1416 ▼

Multicast VLAN

Enter Multicast VLAN

WLAN ACL

IPv4 ACL

Search or Select ▼

IPv6 ACL

Search or Select ▼

URL Filters

Pre Auth

Search or Select ▼

Post Auth

Search or Select ▼

Passaggio 3. Configurare il profilo della policy in modo che accetti le sostituzioni ISE (consenti override AAA) e la modifica dell'autorizzazione (CoA) (stato NAC). È possibile anche specificare un metodo di accounting.

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

AAA Policy

Allow AAA Override

NAC State

NAC Type

Policy Name

Accounting List ⓘ ✕

WGB Parameters

Broadcast Tagging

WGB VLAN

Policy Proxy Settings

ARP Proxy DISABLED

IPv6 Proxy

Fabric Profile

Link-Local Bridging

mDNS Service Policy [Clear](#)

Hotspot Server

User Defined (Private) Network

Status

Drop Unicast

DNS Layer Security

DNS Layer Security Parameter Map [Clear](#)

Flex DHCP Option for DNS ENABLED

Flex DNS Traffic Redirect IGNORE

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Air Time Fairness Policies

2.4 GHz Policy

5 GHz Policy

EoGRE Tunnel Profiles


Tunnel Profile

CLI:

```
# config # wireless profile policy <policy-profile-name> # aaa-override
# nac
# vlan <vlan-id_or_vlan-name>
# accounting-list <acct-list>
# no shutdown
```

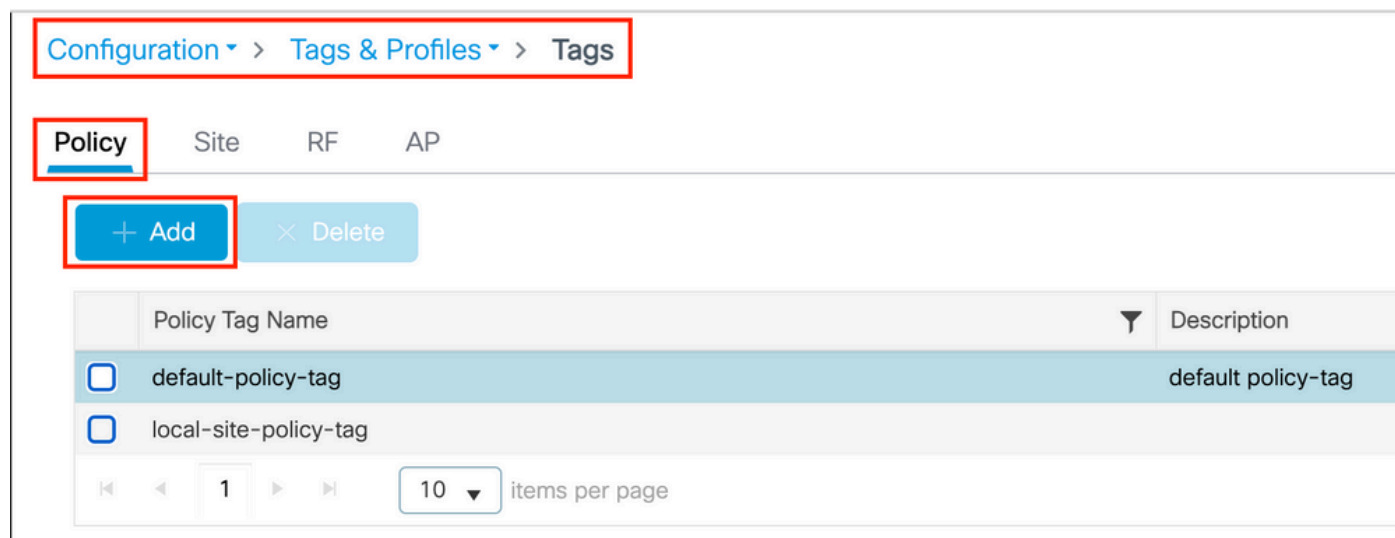
Configurazione del tag di policy

Il tag di policy permette di collegare l'SSID al profilo di policy. È possibile creare un nuovo tag o utilizzare il tag predefinito.

 **Nota:** il tag default-policy mappa automaticamente qualsiasi SSID con ID WLAN compreso tra 1 e 16 al profilo default-policy. Non può essere modificata o eliminata. Se si dispone di una WLAN con ID 17 o successivo, il tag default-policy non può essere utilizzato.

GUI:

Individuate Configuration > Tags & Profiles > Tags > Policy e aggiungetene una nuova, se necessario, come mostrato nell'immagine.



Configuration > Tags & Profiles > Tags

Policy Site RF AP

+ Add × Delete

Policy Tag Name	Description
<input type="checkbox"/> default-policy-tag	default policy-tag
<input type="checkbox"/> local-site-policy-tag	

1 10 items per page

Associare il profilo WLAN al profilo di policy desiderato.

Add Policy Tag ✕

Name*

Description

▼ **WLAN-POLICY Maps: 1**

+ Add
✕ Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> cwa-ssid	default-policy-profile

◀ ◁ 1 ▷ ▶ 10 items per page 1 - 1 of 1 items

➤ **RLAN-POLICY Maps: 0**

↶ Cancel
📄 Apply to Device

CLI:

```
# config t # wireless tag policy <policy-tag-name> # wlan <profile-name> policy <policy-profile-name>
```

Assegnazione di un tag di policy

Assegnare il tag di policy agli access point desiderati.


GUI:

Per assegnare il tag a un punto di accesso, passare a Configuration > Wireless > Access Points > AP Name > General Tags, effettuare l'assegnazione necessaria e quindi fare clic su Update & Apply to Device.

Edit AP

- General**
- Interfaces
- High Availability
- Inventory
- ICap
- Advanced
- Support Bundle

General	Tags
AP Name*	⚠ Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.
Location*	
Base Radio MAC	Policy <input type="text" value="cwa-policy-tag"/>
Ethernet MAC	Site <input type="text" value="default-site-tag"/>
Admin Status <input checked="" type="checkbox"/>	RF <input type="text" value="default-rf-tag"/>
AP Mode <input type="text" value="Local"/>	Write Tag Config to AP <input type="checkbox"/>
Operation Status <input type="text" value="Registered"/>	

 **Nota:** dopo aver modificato il tag di policy su un access point, quest'ultimo perde l'associazione con il WLC 9800 e si unisce di nuovo entro circa 1 minuto.

Per assegnare lo stesso tag di policy a più access point, passare a Configuration > Wireless > Wireless Setup > Advanced > Start Now.

Start

Tags & Profiles



WLAN Profile



Policy Profile



Policy Tag



AP Join Profile



Flex Profile



Site Tag



RF Profile



RF Tag



Apply

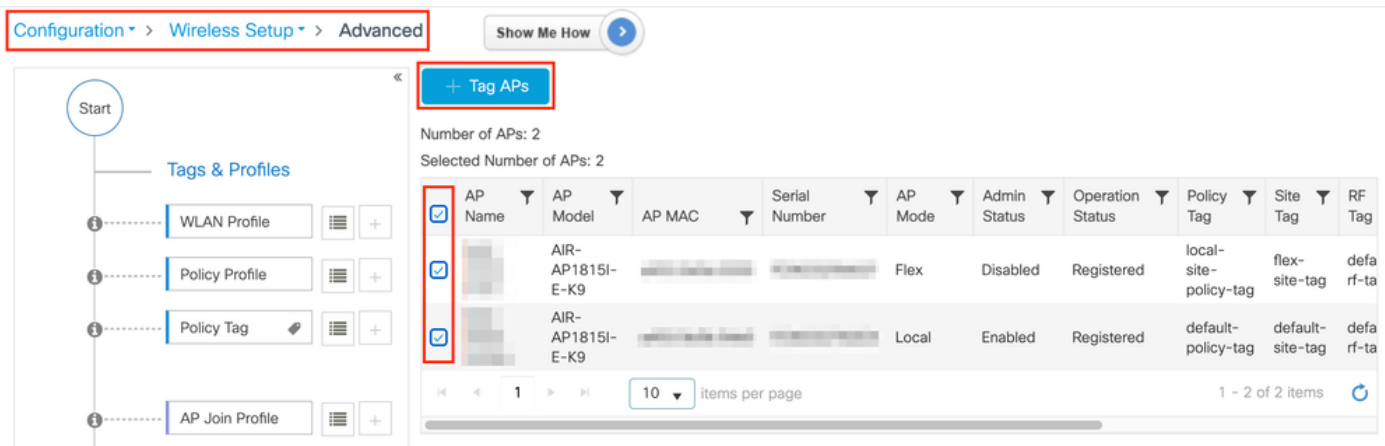


Tag APs

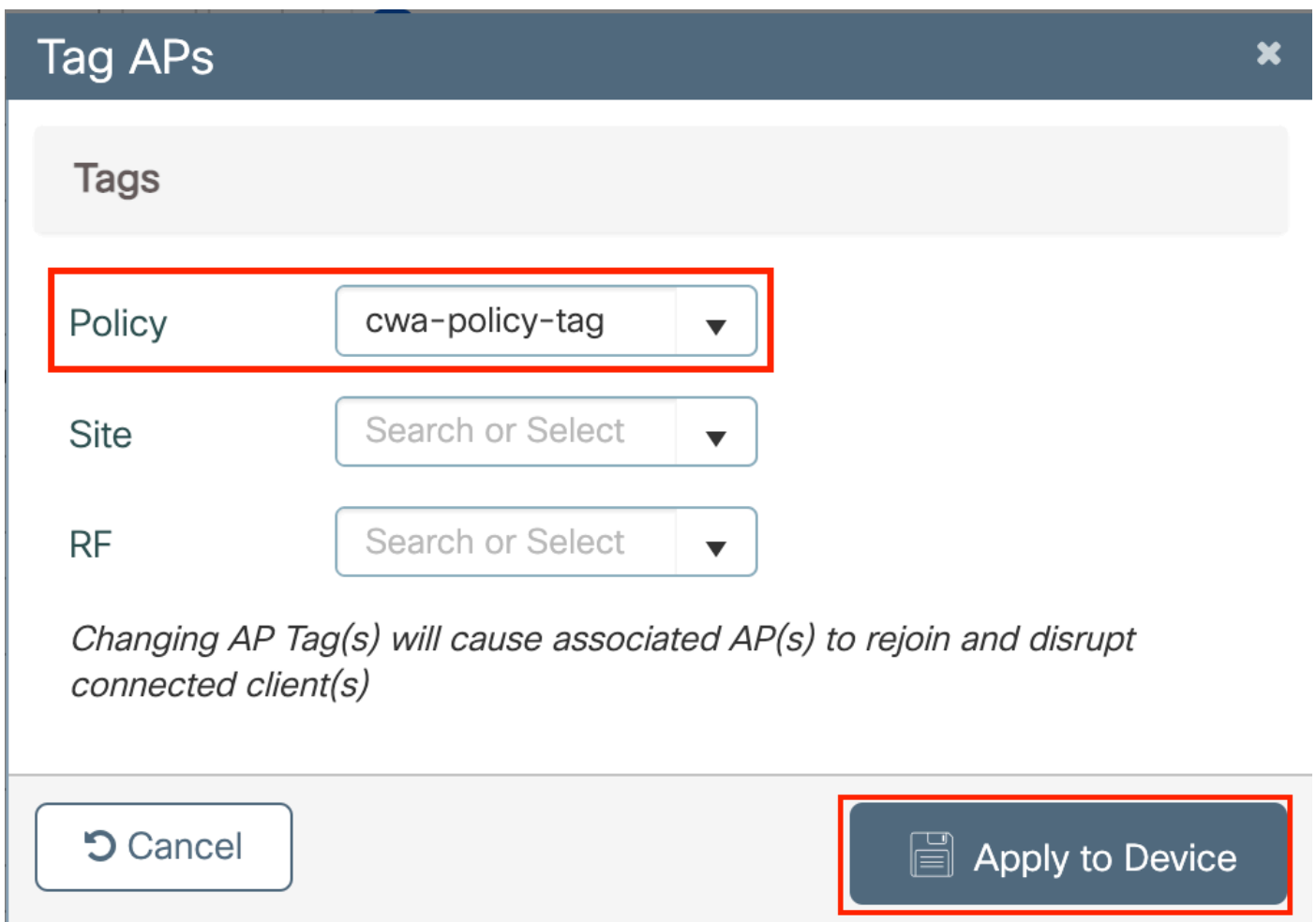


Start Now →

Done



Scegliete il tag desiderato e fate clic su Save & Apply to Device come mostrato nell'immagine.



CLI:

```
# config t # ap <ethernet-mac-addr> # policy-tag <policy-tag-name> # end
```

Configurazione degli ACL di reindirizzamento

Passaggio 1. Per creare un nuovo ACL, Configuration > Security > ACL > + Add passare a.

Scegliere un nome per l'ACL, IPv4 Extended digitare e aggiungere tutte le regole come sequenza, come mostrato nell'immagine.

Add ACL Setup ✕

ACL Name* ACL Type

Rules

Sequence* Action

Source Type

Destination Type Host Name* ! This field is mandatory

Protocol

Log DSCP

+ Add
✕ Delete

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
0										

No items to display

↶ Cancel
Apply to Device

È necessario bloccare il traffico diretto ai nodi ISE PSN e al DNS; tutto il resto del traffico può essere autorizzato. Questo ACL di reindirizzamento non è un ACL di sicurezza, ma un ACL punt che definisce il traffico diretto alla CPU (sui permessi) per un ulteriore trattamento (come il reindirizzamento) e il traffico rimanente sul piano dati (su rifiuto) e impedisce il reindirizzamento.

L'ACL deve essere simile al seguente (sostituire 10.48.39.28 con l'indirizzo IP ISE nell'esempio):


Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
<input type="checkbox"/> 10	deny	any		10.48.39.28		ip			None	Disabled
<input type="checkbox"/> 20	deny	10.48.39.28		any		ip			None	Disabled
<input type="checkbox"/> 30	deny	any		any		udp		eq domain	None	Disabled
<input type="checkbox"/> 40	deny	any		any		udp	eq domain		None	Disabled
<input type="checkbox"/> 50	permit	any		any		tcp		eq www	None	Disabled

1 - 5 of 5 items

Nota: per l'ACL di reindirizzamento, considerare l'azione come un reindirizzamento delladeny negazione (non della negazione del traffico) e l'azione come un reindirizzamento dellapermit autorizzazione. Il WLC analizza solo il traffico che può reindirizzare (per impostazione predefinita, le porte 80 e 43).

CLI:

```
ip access-list extended REDIRECT
deny ip any host <ISE-IP>
deny ip host<ISE-IP> any
deny udp any any eq domain
deny udp any eq domain any
permit tcp any any eq 80
```

 **Nota:** se si termina l'ACL con un permit ip any any permesso anziché con un permesso basato sulla porta 80, il WLC reindirizza anche il protocollo HTTPS, che spesso non è consigliabile in quanto deve fornire il proprio certificato e crea sempre una violazione del certificato. Questa è l'eccezione alla dichiarazione precedente che dice che non è necessario un certificato sul WLC nel caso di CWA: ne serve uno se l'intercettazione HTTPS è abilitata, ma non è mai considerata valida in ogni caso.

È possibile migliorare l'ACL intervenendo per negare solo la porta guest 8443 al server ISE.

Abilita reindirizzamento per HTTP o HTTPS

La configurazione del portale di amministrazione Web è collegata alla configurazione del portale di autenticazione Web e deve essere in ascolto sulla porta 80 per poter essere reindirizzata. Per il corretto funzionamento del reindirizzamento, è pertanto necessario attivare il protocollo HTTP. È possibile scegliere di attivarlo globalmente (con l'uso del comando ip http server) oppure HTTP solo per il modulo di autenticazione Web (con l'uso del comando webauth-http-enable nella mappa dei parametri).



Nota: il reindirizzamento del traffico HTTP avviene all'interno di CAPWAP, anche in caso di switching locale FlexConnect. Poiché è il WLC a eseguire l'intercettazione, l'AP invia i pacchetti HTTP(S) all'interno del tunnel CAPWAP e riceve il reindirizzamento dal WLC in CAPWAP

Se si desidera essere reindirizzati quando si tenta di accedere a un URL HTTPS, aggiungere il comando `intercept-https-enable` nella mappa dei parametri ma questa non è una configurazione ottimale, poiché influisce sulla CPU del WLC e genera comunque errori di certificato:

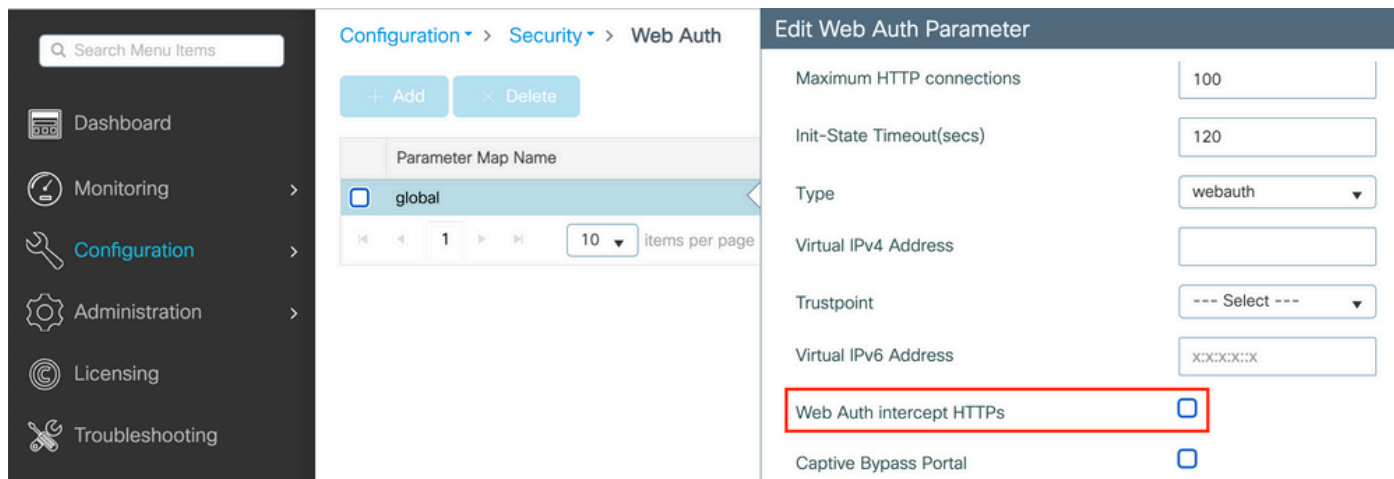
`<#root>`

```
parameter-map type webauth global
type webauth
```

`intercept-https-enable`

`trustpoint xxxxx`

È possibile farlo anche tramite la GUI con l'opzione 'Web Auth intercept HTTPS' selezionata nella mappa dei parametri (Configuration > Security > Web Auth).



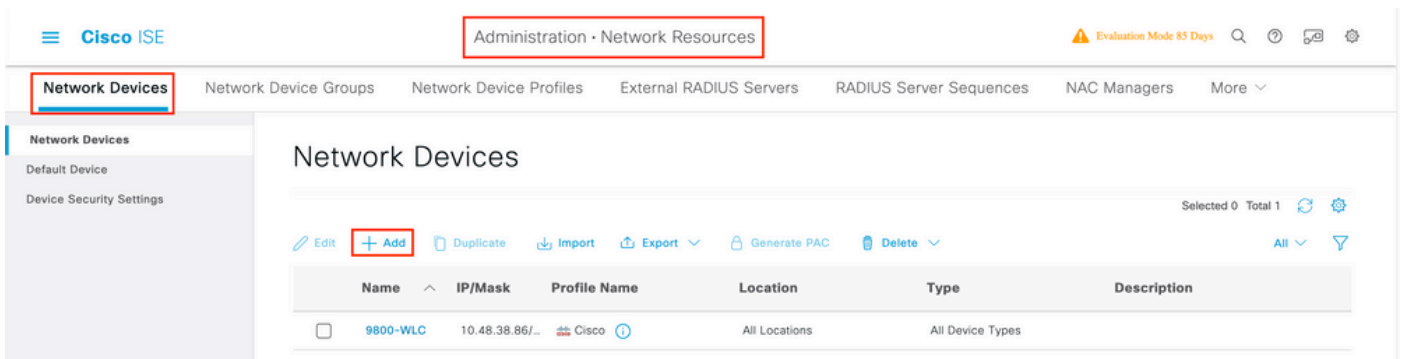


Nota: per impostazione predefinita, i browser utilizzano un sito Web HTTP per avviare il processo di reindirizzamento. Se è necessario il reindirizzamento HTTPS, è necessario controllare l'intercettazione HTTPS di Web Auth. Questa configurazione non è tuttavia consigliata in quanto aumenta l'utilizzo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

Configurazione di ISE

Aggiunta di controller 9800 WLC a ISE

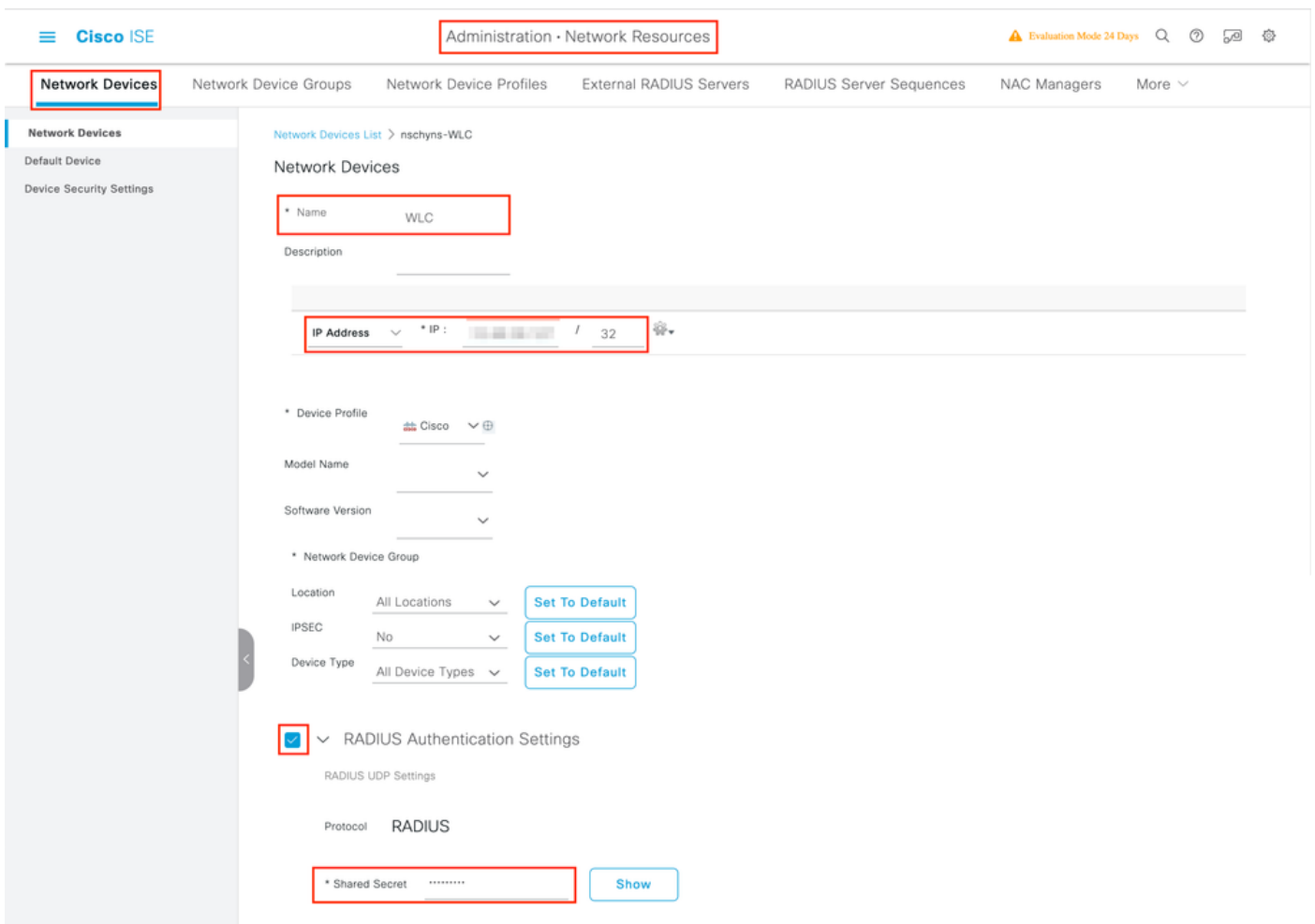
Passaggio 1. Aprire la console ISE e passare `Administration > Network Resources > Network Devices > Add` a come mostrato nell'immagine.



Passaggio 2. Configurare il dispositivo di rete.

Facoltativamente, è possibile specificare il nome del modello, la versione del software e la descrizione, nonché assegnare gruppi di dispositivi di rete in base al tipo di dispositivo, alla posizione o ai WLC.

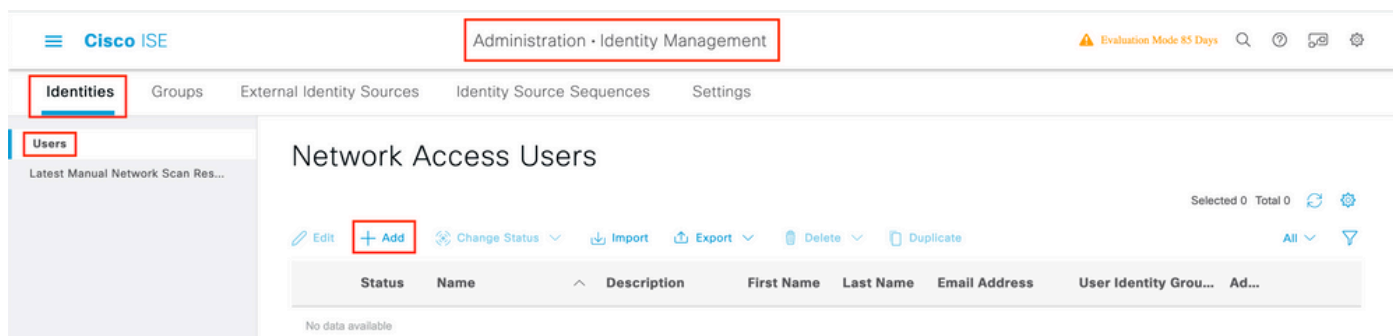
L'indirizzo IP corrisponde all'interfaccia WLC che invia le richieste di autenticazione. Per impostazione predefinita è l'interfaccia di gestione, come mostrato nell'immagine:



Per ulteriori informazioni sui gruppi di dispositivi di rete, vedere il capitolo della guida per l'amministratore di ISE: [Manage Network Devices: ISE - Network Device Groups](#).

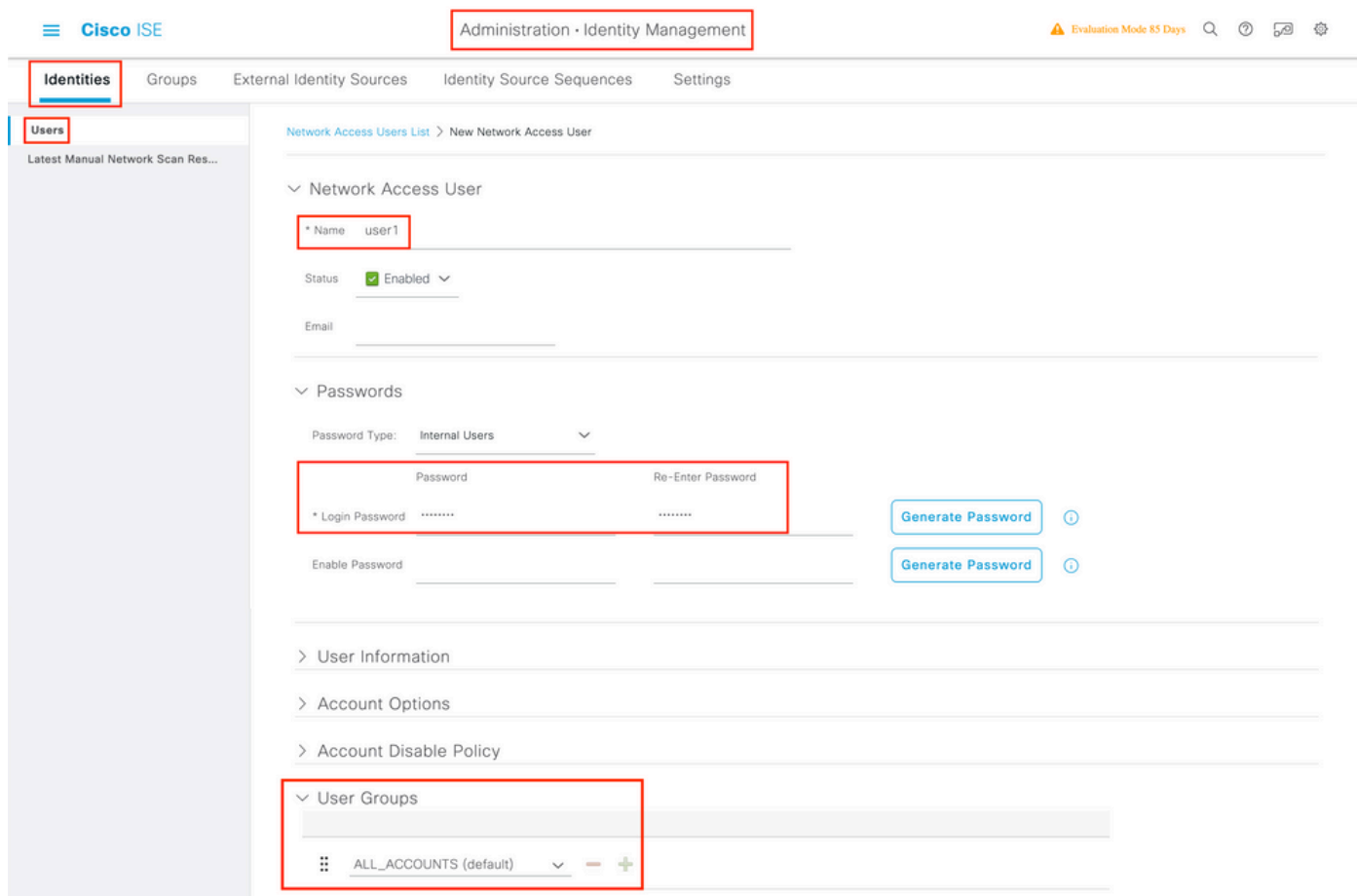
Creazione di un nuovo utente in ISE

Passaggio 1. Passare a Administration > Identity Management > Identities > Users > Add come mostrato nell'immagine.



Passaggio 2. Immettere le informazioni.

In questo esempio, l'utente appartiene a un gruppo denominato ALL_ACCOUNTS ma può essere regolato in base alle esigenze, come mostrato nell'immagine.



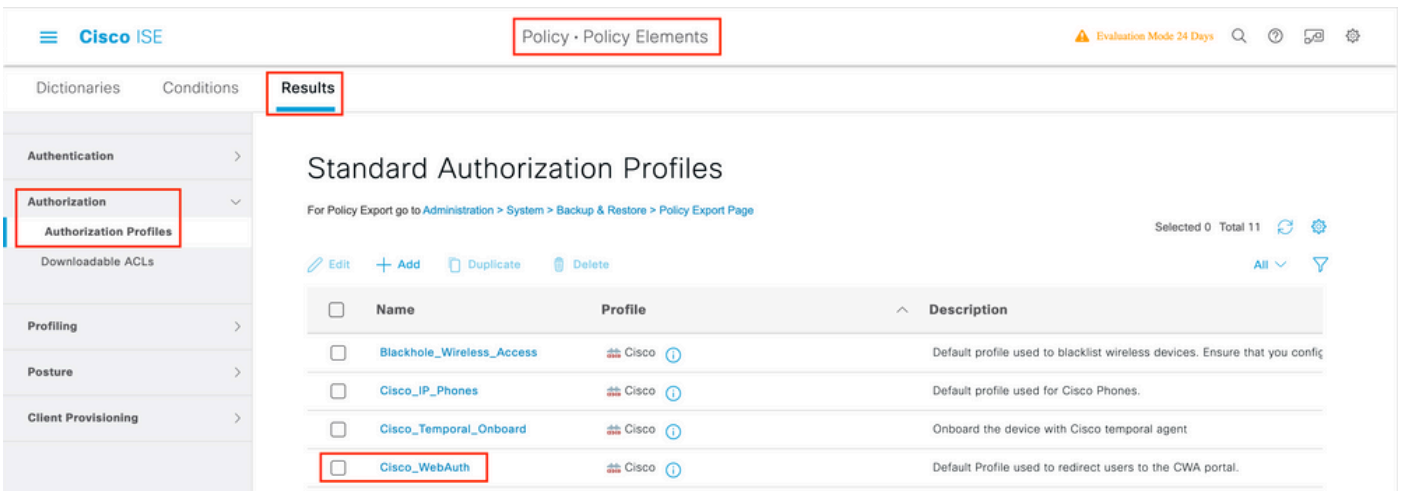
Creazione del profilo di autorizzazione

Il profilo dei criteri è il risultato assegnato a un client in base ai relativi parametri, ad esempio indirizzo MAC, credenziali, WLAN utilizzata e così via. Può assegnare impostazioni specifiche come VLAN (Virtual Local Area Network), elenchi di controllo di accesso (ACL), reindirizzamenti URL (Uniform Resource Locator) e così via.

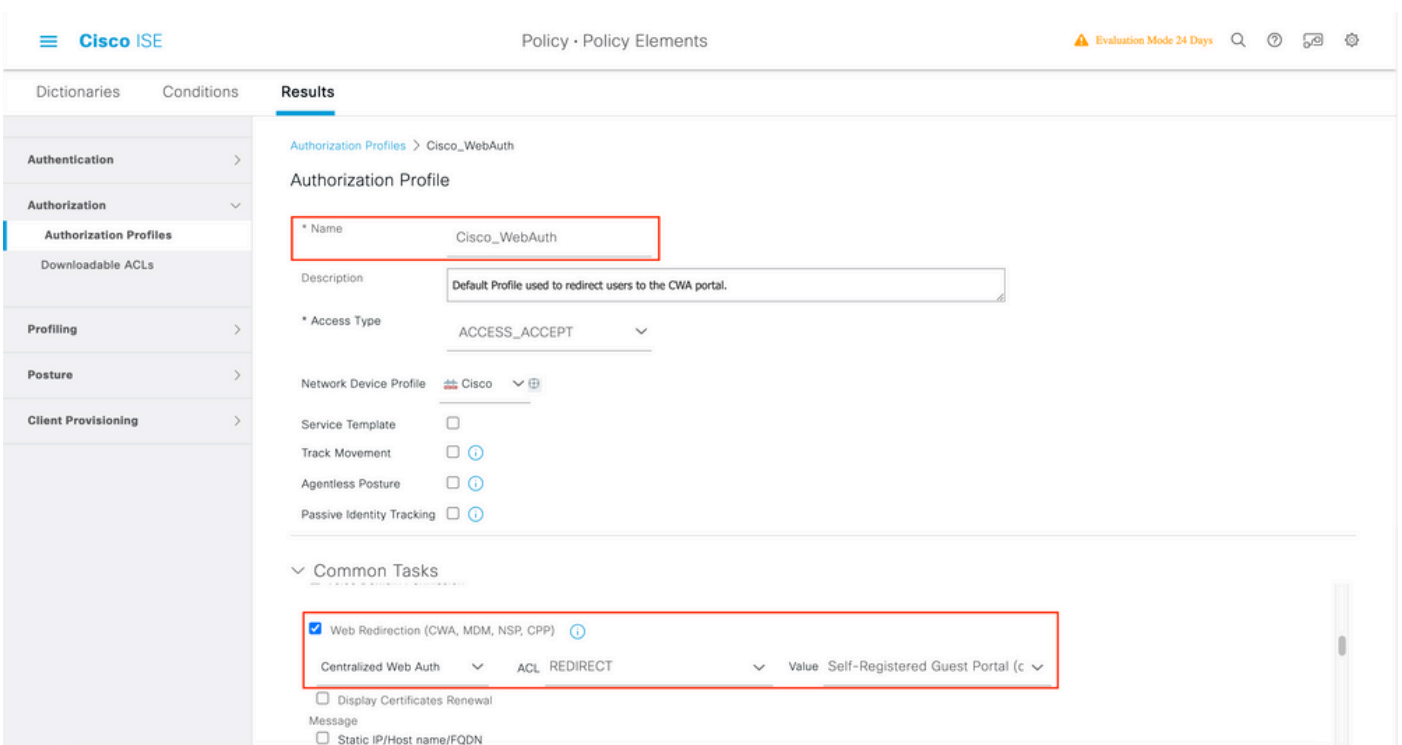
Tenere presente che nelle versioni recenti di ISE esiste già un profilo di autorizzazione Cisco_Webauth. Qui è possibile modificarlo per

cambiare il nome dell'ACL di reindirizzamento in modo che corrisponda a quello configurato nel WLC.

Passaggio 1. Passare a Policy > Policy Elements > Results > Authorization > Authorization Profiles. Fare clic su add per creare il proprio risultato o modificare quello Cisco_Webauth predefinito.

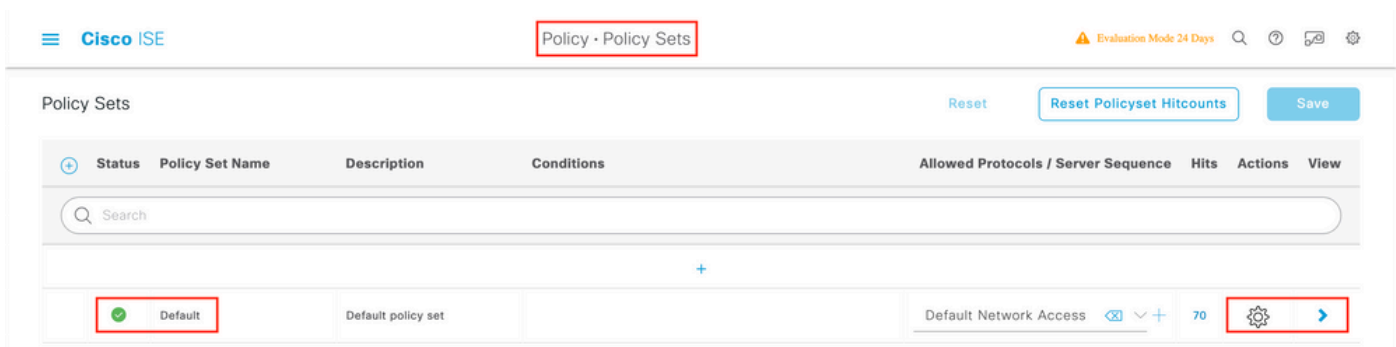


Passaggio 2. Immettere le informazioni di reindirizzamento. Verificare che il nome ACL sia lo stesso di quello configurato sul WLC 9800.

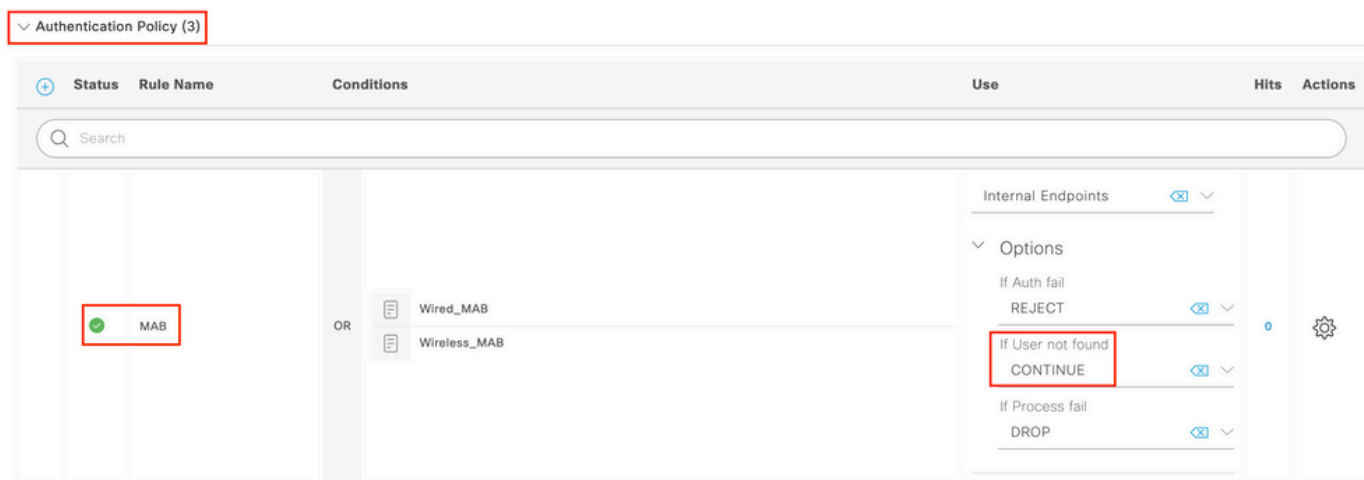


Configurazione della regola di autenticazione

Passaggio 1. Un set di criteri definisce un insieme di regole di autenticazione e autorizzazione. Per crearne uno, passare Policy > Policy Sets a, fare clic sull'ingranaggio del primo set di criteri nell'elenco e Insert new row scegliere o fare clic sulla freccia blu a destra per scegliere il set di criteri predefinito.



Passaggio 2. Espandere Authentication criteri. Per la MAB regola (corrispondenza su MAB cablato o wireless), espandere Options e scegliere l'opzione nel caso in cui venga visualizzato 'Se l'utente non è stato trovato' nelCONTINUE campo.



Passaggio 3. Fare clic su Save per salvare le modifiche.

Configurazione delle regole di autorizzazione

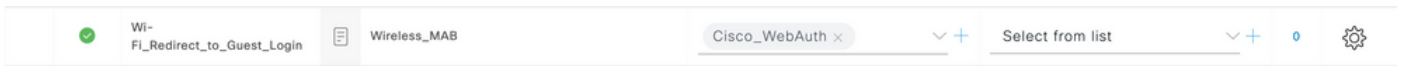
La regola di autorizzazione permette di stabilire quali autorizzazioni (ovvero quale profilo di autorizzazione) vengono applicate al client.

Passaggio 1. Nella stessa pagina di set di criteri, chiudere il Authentication Policy e espandere Authorziation Policy come mostrato nell'immagine.

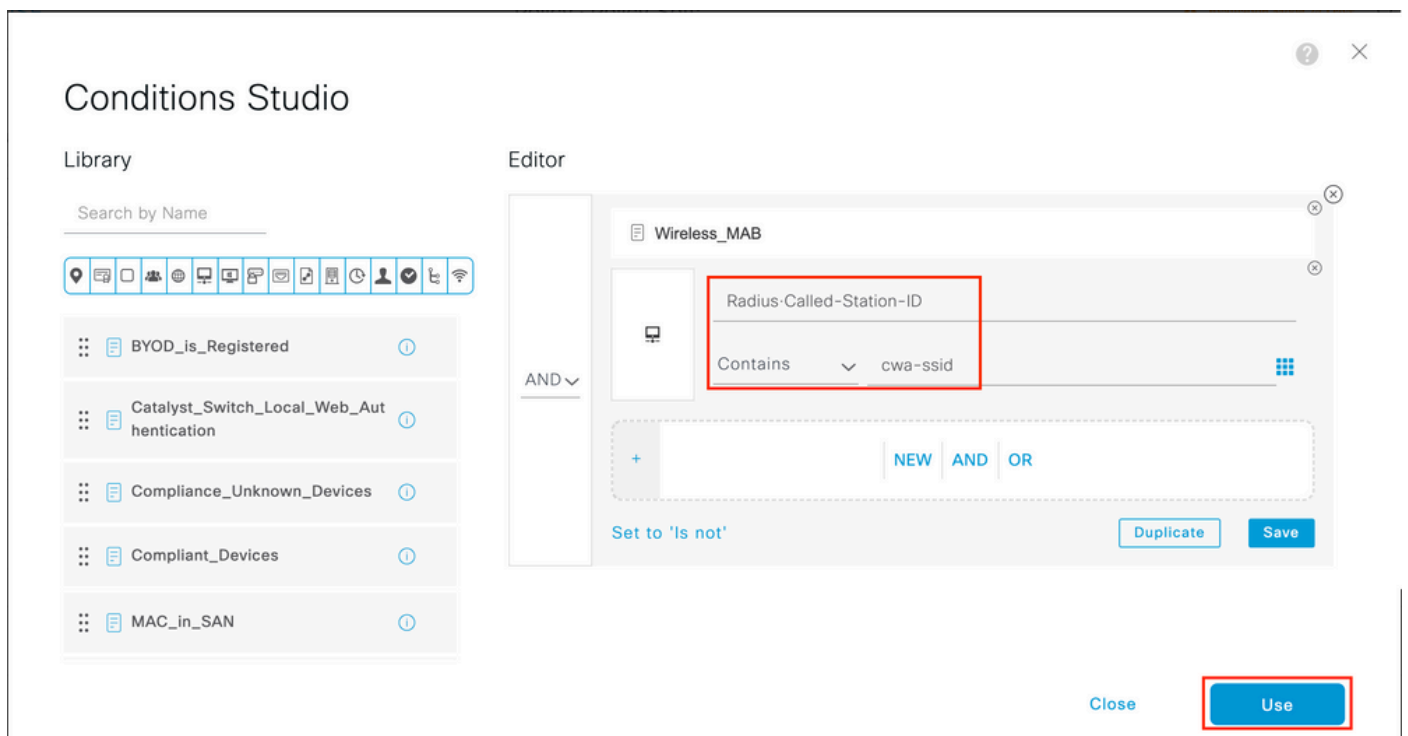


Passaggio 2. Le versioni più recenti di ISE iniziano con una regola pre-creata, chiamataWifi_Redirect_to_Guest_Login "equalizzatori", che

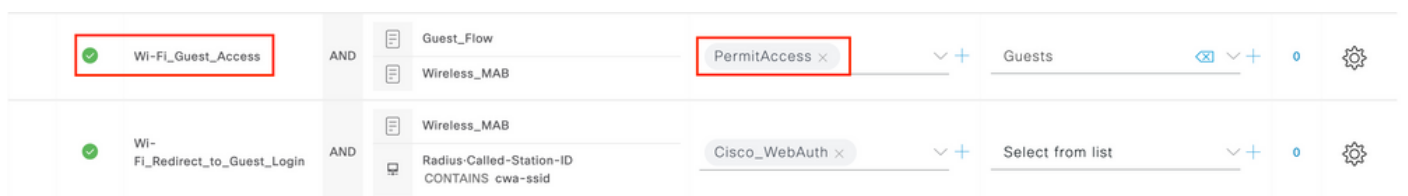
soddisfa soprattutto le nostre esigenze. Ruotare il simbolo grigio a sinistra su enable.



Passaggio 3. Questa regola corrisponde solo a Wireless_MAB e restituisce gli attributi di reindirizzamento CWA. Ora, è possibile aggiungere una piccola torsione e far corrispondere solo l'SSID specifico. Scegliere la condizione (Wireless_MAB a partire da questo momento) per visualizzare Conditions Studio (Studio condizioni). Aggiungere una condizione a destra e scegliere il Radius dizionario con l'Called-Station-ID attributo. facendo corrispondere la condizione al nome SSID. Eseguire la convalida con il simbolo Use nella parte inferiore dello schermo, come illustrato nell'immagine.



Passaggio 4. È ora necessaria una seconda regola, definita con una priorità più alta, che soddisfi la condizione per restituire i dettagli di accesso alla rete dopo l'autenticazione dell'utente sul portale Guest Flow. È possibile usare la regola Wifi Guest Access che è stata creata in precedenza sulle versioni ISE recenti. Per abilitare la regola, è sufficiente inserire un segno di spunta verde a sinistra. È possibile restituire il valore predefinito di PermitAccess o configurare restrizioni più precise per gli elenchi degli accessi.



Passaggio 5. Salvate le regole.

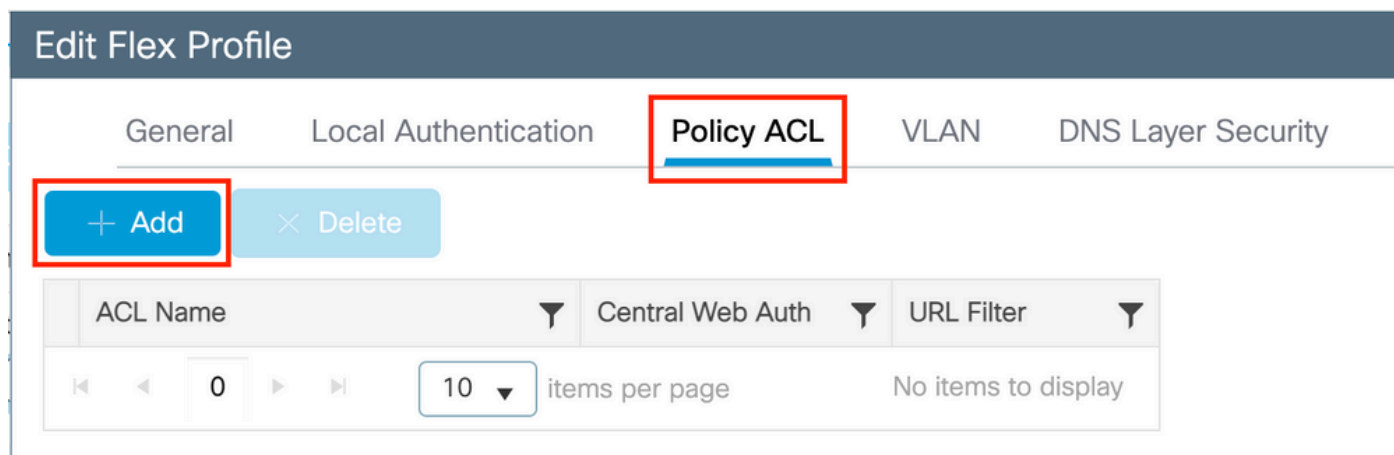
Fare clic Save in fondo alle regole.

SOLO FlexConnect Access Point con switching locale

Qual è la procedura per i FlexConnect Access Point con switching locale e WLAN? Le sezioni precedenti sono ancora valide. Tuttavia, è necessario un passaggio aggiuntivo per eseguire il push dell'ACL di reindirizzamento agli access point in anticipo.


Individuate Configuration > Tags & Profiles > Flex il profilo Flex e sceglietelo. Passare quindi alla Policy ACL scheda.

Fare clic Add come mostrato nell'immagine.

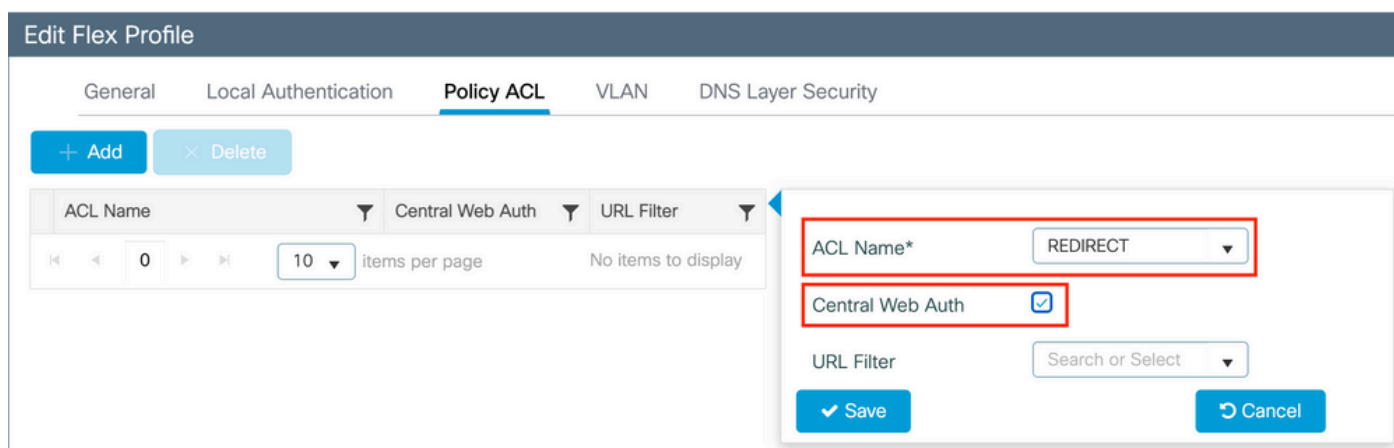


The screenshot shows the 'Edit Flex Profile' interface with the 'Policy ACL' tab selected. A red box highlights the '+ Add' button. Below the tabs, there are 'Add' and 'Delete' buttons. A table header shows 'ACL Name', 'Central Web Auth', and 'URL Filter'. Below the table, there are navigation arrows, a page number '0', a dropdown for '10 items per page', and the text 'No items to display'.

Scegliere il nome dell'ACL di reindirizzamento e abilitare l'autenticazione Web centrale. Questa casella di controllo inverte automaticamente l'ACL sull'access point (in quanto un'istruzione 'deny' significa 'non reindirizzare a questo IP' sul WLC in Cisco IOS XE). Tuttavia, nell'AP l'istruzione 'deny' significa il contrario. Pertanto, questa casella di controllo scambia automaticamente tutti i permessi e li nega quando esegue il push nell'access point. È possibile verificarlo con un show ip access list comando da AP (CLI).

 **Nota:** nello scenario di switching locale per Flexconnect, l'ACL deve menzionare specificamente le istruzioni return (che non sono necessariamente richieste in modalità locale), in modo che tutte le regole ACL coprano entrambe le modalità di traffico (ad esempio, da e verso l'ISE).

Non dimenticare di colpire Save e poi Update and apply to the device.



The screenshot shows the 'Edit Flex Profile' interface with the 'Policy ACL' tab selected. A modal dialog is open for adding a new ACL. The 'ACL Name*' field is set to 'REDIRECT' and the 'Central Web Auth' checkbox is checked. The 'URL Filter' field is set to 'Search or Select'. The 'Save' and 'Cancel' buttons are visible.

Certificati

Affinché il client consideri attendibile il certificato di autenticazione Web, non è necessario installare alcun certificato sul WLC, poiché l'unico certificato presentato è il certificato ISE (che deve essere considerato attendibile dal client).

Verifica

Usare questi comandi per verificare la configurazione corrente.

<#root>

```
# show run wlan # show run aaa # show aaa servers # show ap config general # show ap name <ap-name> config general
# show ap tag summary
# show ap name <AP-name> tag detail
# show wlan { summary | id | nme | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

Di seguito è riportata la parte pertinente della configurazione del WLC che corrisponde al presente esempio:

<#root>

```
aaa new-model !
aaa authorization network CWAauthz group radius aaa accounting identity CWAacct start-stop group radius ! aaa server radius dynamic-author client <ISE>
mac-filtering CWAauthz
no security ft adaptive
no security wpa
no security wpa wpa2
no security wpa wpa2 ciphers aes
no security wpa akm dot1x
no shutdown
ip http server (or "webauth-http-enable" under the parameter map)
ip http secure-server
```

Risoluzione dei problemi

Elenco di controllo

- Verificare che il client si connetta e ottenga un indirizzo IP valido.
- Se il reindirizzamento non è automatico, aprire un browser e provare con un indirizzo IP casuale. Ad esempio, 10.0.0.1. Se il reindirizzamento funziona, è possibile che si sia verificato un problema di risoluzione DNS. Verificare di disporre di un server DNS

valido fornito tramite DHCP e che sia in grado di risolvere i nomi host.

- Verificare che il comando `ip http server` sia configurato per il reindirizzamento su HTTP. La configurazione del portale di amministrazione Web è collegata alla configurazione del portale di autenticazione Web e deve essere elencata sulla porta 80 per poter essere reindirizzata. È possibile scegliere di attivarlo globalmente (con l'uso del comando `ip http server`) oppure HTTP solo per il modulo di autenticazione Web (con l'uso del comando `webauth-http-enable` nella mappa dei parametri).
- Se non si viene reindirizzati quando si tenta di accedere a un URL HTTPS e questo è obbligatorio, verificare di disporre del comando `intercept-https-enable` nella mappa dei parametri:

<#root>

```
parameter-map type webauth global  
type webauth
```

```
intercept-https-enable
```

```
trustpoint xxxxxx
```

È inoltre possibile verificare tramite la GUI che l'opzione 'Web Auth intercept HTTPS' sia selezionata nella mappa dei parametri:

The screenshot shows the Cisco Catalyst GUI configuration interface. On the left is a navigation menu with options like Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main area is titled 'Configuration > Security > Web Auth'. Below this, there's a table of 'Parameter Map Name' with one entry 'global'. To the right, the 'Edit Web Auth Parameter' form is visible, containing fields for 'Maximum HTTP connections' (100), 'Init-State Timeout(secs)' (120), 'Type' (webauth), 'Virtual IPv4 Address', 'Trustpoint' (--- Select ---), 'Virtual IPv6 Address' (xxxxxx), and two checkboxes: 'Web Auth intercept HTTPS' (checked) and 'Captive Bypass Portal' (unchecked). The 'Web Auth intercept HTTPS' checkbox is highlighted with a red border.

Supporto porta servizio per RADIUS

Cisco Catalyst serie 9800 Wireless Controller ha una porta servizio che viene indicata come GigabitEthernet 0porta. A partire dalla versione 17.6.1, questa porta supporta RADIUS (che include CoA).

Se si desidera utilizzare la porta di servizio per RADIUS, è necessaria la configurazione seguente:

<#root>

```
aaa server radius dynamic-author
client 10.48.39.28

vrf Mgmt-intf

    server-key cisco123

interface GigabitEthernet0

vrf forwarding Mgmt-intf

    ip address x.x.x.x x.x.x.x

!if using aaa group server:
aaa group server radius group-name
    server name nicoISE

    ip vrf forwarding Mgmt-intf

    ip radius source-interface GigabitEthernet0
```

Raccogli debug

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



Nota: è possibile tornare indietro di alcune ore a diversi giorni nei log, ma dipende dal volume dei log generati.

Per visualizzare le tracce raccolte per impostazione predefinita dal protocollo 9800 WLC, è possibile connettersi al protocollo 9800 WLC tramite SSH/Telnet e procedere come segue (accertarsi di registrare la sessione su un file di testo).

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

```
<#root>
```

```
# show clock
```

Passaggio 2. Raccogliere i syslog dal buffer WLC 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>
```

```
# show logging
```

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

```
<#root>
```

```
# show debugging Cisco IOS XE Conditional Debug Configs: Conditional Debug Global State: Stop Cisco IOS XE Packet Tracing Configs: Packet Infra d
```

 **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). In questo modo si aumenta il volume dei registri. Pertanto, si consiglia di cancellare tutte le condizioni quando non si esegue il debug attivo.

Passaggio 4. Supponendo che l'indirizzo MAC in fase di test non sia stato elencato come condizione nel passaggio 3., raccogliere le tracce del livello di avviso always on per l'indirizzo MAC specifico.

```
<#root>
```

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-<FILENAME.txt>
```

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

```
<#root>
```

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

```
or
```

```
# 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 a livello 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, procedere come segue.

Passaggio 5. Verificare che non vi siano condizioni di debug abilitate.

```
<#root>
```

```
# clear platform condition all
```

Passaggio 6. 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>
```

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



Nota: per monitorare più client alla volta, eseguire il comando debug wireless mac<aaaa.bbbb.cccc> per indirizzo MAC.



Nota: non è possibile visualizzare l'output dell'attività del client nella sessione terminale, in quanto tutto viene memorizzato internamente nel buffer per essere visualizzato successivamente.

Passaggio 7". Riprodurre il problema o il comportamento che si desidera monitorare.

Passaggio 8. Interrompere i debug se il problema viene riprodotto prima che il tempo di monitoraggio predefinito o configurato sia attivo.

```
<#root>
```

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

Allo scadere del tempo di monitoraggio o dopo aver interrotto il debug wireless, il WLC 9800 genera un file locale con il nome:

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Passaggio 9. Raccogliere il file dell'attività dell'indirizzo MAC. È possibile copiare il filera trace .log su un server esterno oppure visualizzarlo

direttamente sullo schermo.

Controllare il nome del file delle tracce RA.

```
<#root>
```

```
# dir bootflash: | inc ra_trace
```

Copiare il file su un server esterno:

```
<#root>
```

```
# copy bootflash: ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.d/ra-FILENAME.txt
```

Visualizzare il contenuto:


```
<#root>
```

```
# more bootflash: ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Passaggio 10. Se la causa principale non è ancora ovvia, raccogliere i log interni che offrono una visualizzazione più dettagliata dei log a livello di debug. non è necessario eseguire di nuovo il debug del client. Per ulteriori informazioni, vedere i log di debug già raccolti e archiviati internamente.

```
<#root>
```

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file ra-internal-<FILENAME>.txt
```

 **Nota:** questo output del comando restituisce tracce per tutti i livelli di log per tutti i processi ed è piuttosto voluminoso. Coinvolgere Cisco TAC per analizzare queste tracce.

È possibile copiare il filera-internal-FILENAME.txt su un server esterno oppure visualizzarlo direttamente sullo schermo.

Copiare il file su un server esterno:

<#root>

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

Visualizzare il contenuto:

<#root>

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

Passaggio 11. Rimuovere le condizioni di debug.

<#root>

```
# clear platform condition all
```



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

Esempi

Se il risultato dell'autenticazione non è quello previsto, è importante andare alla pagina ISE Operations > Live logs e ottenere i dettagli del risultato.

Viene visualizzato il motivo dell'errore (se si verifica un errore) e tutti gli attributi Radius ricevuti da ISE.

Nell'esempio seguente, ISE ha rifiutato l'autenticazione perché non ha trovato una regola di autorizzazione corrispondente. Questo perché l'attributo ID stazione chiamata viene inviato come nome SSID aggiunto all'indirizzo MAC dell'access point, mentre l'autorizzazione corrisponde esattamente al nome SSID. Viene corretto quando la regola viene modificata in 'contains' anziché 'equal'.

Event	5400 Authentication failed
Failure Reason	15039 Rejected per authorization profile
Resolution	Authorization Profile with ACCESS_REJECT attribute was selected as a result of the matching authorization rule. Check the appropriate Authorization policy rule-results.
Root cause	Selected Authorization Profile contains ACCESS_REJECT attribute
Username	E8:36:17:1F:A1:62

```
15048 Queried PIP - Radius.NAS-Port-1-type
15048 Queried PIP - Network Access.UserName
15048 Queried PIP - IdentityGroup.Name (2 times)
15048 Queried PIP - EndPoints.LogicalProfile
15048 Queried PIP - Radius.Called-Station-ID
15048 Queried PIP - Network Access.AuthenticationStatus
15016 Selected Authorization Profile - DenyAccess
15039 Rejected per authorization profile
11003 Returned RADIUS Access-Reject
```


Other Attributes

ConfigVersionId	140
Device Port	58209
DestinationPort	1812
RadiusPacketType	AccessRequest
Protocol	Radius
NAS-Port	71111
Framed-MTU	1485
OriginalUserName	e836171fa162
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	nicolse26/356963261/1
UseCase	Host Lookup
SelectedAuthenticationIdentityStores	Internal Endpoints
IdentityPolicyMatchedRule	MAB
AuthorizationPolicyMatchedRule	Default
EndPointMACAddress	E8-36-17-1F-A1-62
ISEPolicySetName	Default
IdentitySelectionMatchedRule	MAB
DTLSSupport	Unknown
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
RADIUS Username	E8:36:17:1F:A1:62
NAS-Identifler	cwa-ssid
Device IP Address	10.48.71.120
CPMSessionID	7847300A0000012DFC227BF1
Called-Station-ID	00-27-e3-8f-33-a0:cwa-ssid
CiscoAVPair	service-type=Call Check, audit-session-id=7847300A0000012DFC227BF1, method=mab, client-if-id=3003124185, vlan-id=1468, cisco-wlan-ssid=cwa-ssid

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Troubleshooting

Troubleshooting > Radioactive Trace

Conditional Debug Global State: **Stopped**

+ Add - Delete Start Stop

MAC/IP Address	Trace file
<input type="checkbox"/> e836.171f.a162	debugTrace_e836.171f.a162.txt Download

1 10 Items per page 1 - 1 of 1 items

Generate

In questo caso, il problema è che è stato digitato un nome ACL non corrispondente al nome ACL restituito dall'ISE oppure il WLC lamenta che non esiste alcun ACL come quello richiesto da ISE:

<#root>

2019/09/04 12:00:06.507 {wncd_x_R0-0}{1}: [client-auth] [24264]: (ERR): MAC: e836.171f.a162 client authz result: FAILURE 2019/09/04 12:00:06.51

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).