Configurazione dell'autenticazione locale in modalità FlexConnect

Sommario

- Introduzione
  - Premesse
    - Panoramica e requisiti di FlexConnect
    - Modalità di funzionamento
    - Roaming sicuro e rapido
    - Modalità alta scala FlexConnect
    - Supporto Wi-Fi 7 FlexConnect
    - Scenari di resilienza di FlexConnect
- Prerequisiti
  - Requisiti
  - Componenti usati
- Configurazione
  - Esempio di rete
  - Configurazione dei server AAA
  - Configurazione della modalità FlexConnect sul sito remoto
  - Configurazione di una WLAN 802.1x con autenticazione locale tramite un server RADIUS esterno
  - Configurare ISE
  - Configurazione della WLAN della chiave pubblica con autenticazione locale
- Verifica
- Risoluzione dei problemi
  - Scenario autonomo
- Informazioni correlate

Introduzione

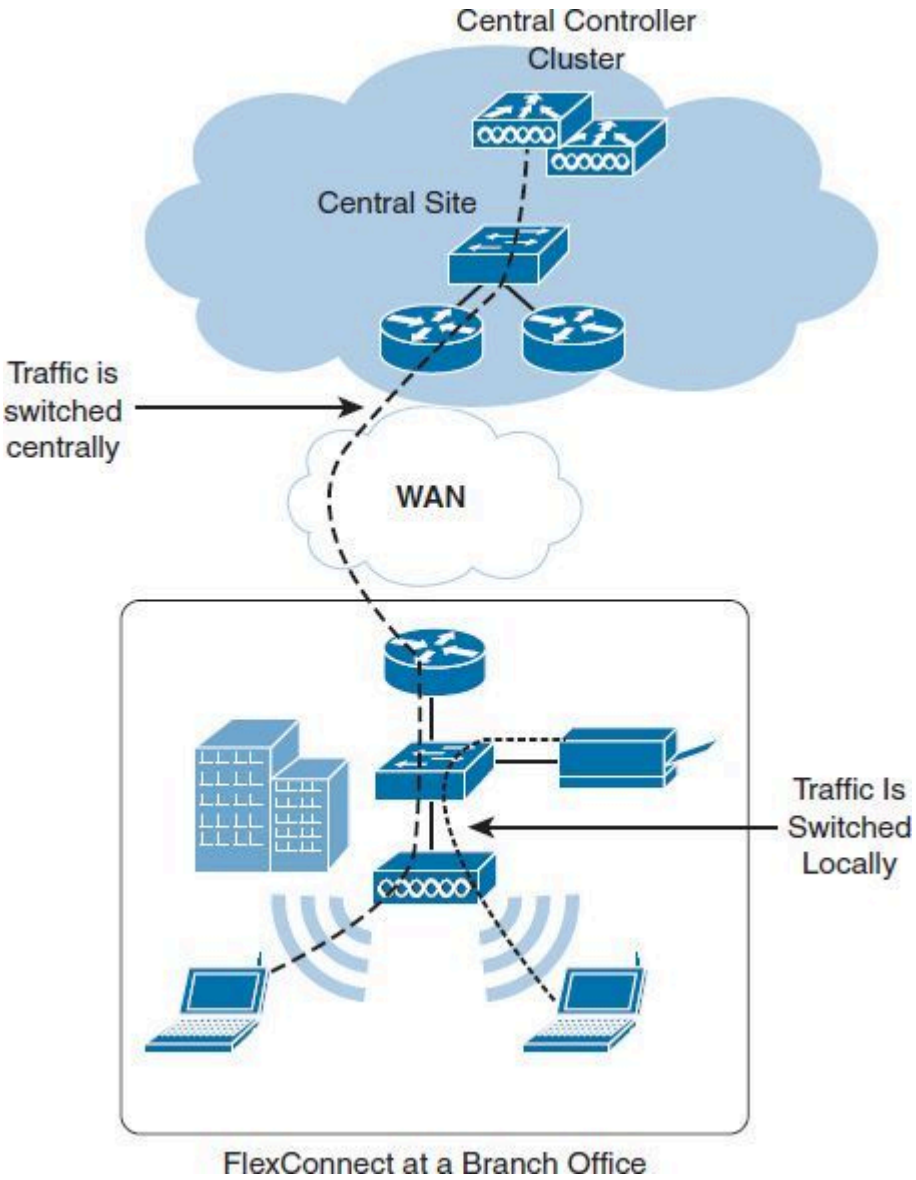
Questo documento descrive il funzionamento dell'autenticazione locale FlexConnect e come configurarla con Cisco Catalyst serie 9800 Wireless Controller (WLC)

Premesse

Panoramica e requisiti di FlexConnect

FlexConnect consente al punto di accesso (AP) di uffici remoti o filiali di connettersi a un controller centralizzato e al tempo stesso consente l'elaborazione locale del traffico wireless. A differenza delle tradizionali installazioni wireless centralizzate, in cui tutto il traffico wireless viene tunneling al controller tramite CAPWAP (Control and Provisioning of Wireless Access Point), FlexConnect consente di commutare e gestire il traffico a livello locale direttamente dal punto di accesso della filiale. Questa commutazione locale fornisce all'access point un grado di autonomia che consente ai servizi chiave, quali sicurezza, roaming e QoS (Quality of Service), di funzionare in modo indipendente dal controller.

Sebbene FlexConnect sia progettato principalmente per la commutazione del traffico locale, offre anche la flessibilità di commutare centralmente SSID specifici (Service Set Identifier) quando necessario. Ad esempio, se un determinato traffico deve passare attraverso un firewall centrale, gli SSID possono essere rimandati al controller tramite CAPWAP per lo switching centralizzato. Questa doppia funzionalità consente a un singolo punto di accesso FlexConnect di supportare contemporaneamente le WLAN (Wireless Local Area Network) commutate sia localmente che centralmente.



FlexConnect at a Branch Office

Modalità di funzionamento

I punti di accesso FlexConnect funzionano in due modalità: modalità connessa e modalità standalone.

- Connesso, l'access point mantiene una connessione attiva al controller tramite il canale di controllo CAPWAP.
- La modalità standalone è uno stato di fallback che si verifica quando l'access point perde la connettività al controller.

In condizioni normali, i punti di accesso FlexConnect funzionano in modalità connessa, in cui il controller gestisce servizi critici quali l'autenticazione centralizzata, la profilatura dei client e la gestione delle risorse radio (RRM). Mentre si prevede che l'access point rimanga in questa modalità per la maggior parte del tempo, passa automaticamente alla modalità standalone se la comunicazione con il controller viene persa. In modalità standalone, l'access point continua a funzionare, commutando il traffico a livello locale e consentendo ai client di rimanere connessi. Gli access point autenticano i client in modo indipendente senza inoltrare le richieste di autenticazione a un controller centrale. Tuttavia, alcuni servizi dipendenti dai controller, ad esempio RRM e l'autenticazione client centralizzata, diventano temporaneamente non disponibili.

Ad esempio, se un'interruzione della rete WAN (Wide Area Network) interrompe la connessione tra il punto di accesso e il controller ma l'accesso a Internet rimane attivo, il punto di accesso passa alla modalità standalone e continua a elaborare il traffico commutato localmente senza interruzioni. I client esistenti rimangono connessi, ma i nuovi client che richiedono l'autenticazione centrale non possono unirsi alla rete, a meno che non sia configurata l'autenticazione locale. I punti di accesso FlexConnect possono essere configurati in modo da eseguire l'autenticazione locale durante gli errori della WAN, garantendo un servizio continuo anche quando il controller non è raggiungibile.

In modalità standalone, l'access point non dispone delle seguenti funzionalità:

- Autenticazione Web client
- Autenticazione Guest (reindirizzamento portale)
- Qualsiasi SSID commutato centralmente
- RRM
- Mobilità Layer-3 IPv6

- Profilatura nativa
- Classificazione criteri
- Service Discovery Gateway
- Aggiornamenti della configurazione

Per un elenco completo delle funzionalità e delle configurazioni WLAN supportate in modalità standalone (autenticazione locale), vedere la matrice delle funzionalità: Matrice di funzionalità per i Cisco Wireless Access Point

Uno scenario di errore comune di FlexConnect implica una perdita completa o un peggioramento significativo della WAN, che interrompe il canale di controllo CAPWAP. Quando l'access point perde la connettività al controller a causa di problemi della WAN, passa immediatamente alla modalità standalone.

L'obiettivo principale durante un guasto della WAN è ripristinare la comunicazione con il controller il più rapidamente possibile per ripristinare la piena funzionalità.

Quando un access point FlexConnect entra in modalità standalone a causa di un errore della WAN, i client attivi rimangono connessi e possono spostarsi senza problemi tra gli access point all'interno del tag dominio/sito FlexConnect, ma il roaming tra tag sito FlexConnect diversi può richiedere la riautenticazione completa. Tuttavia, i nuovi client che tentano di collegarsi alla WLAN commutata localmente non sono in grado di eseguire l'autenticazione perché il server AAA (Authentication, Authorization, and Accounting Server) nella posizione centrale non è raggiungibile.

Roaming sicuro e rapido

L'autenticazione EAP (Extensible Authentication Protocol) introduce una latenza più elevata rispetto all'autenticazione PSK (Pre-Shared Key) a causa dello scambio di frame EAP con il server AAA. Tuttavia, con il roaming veloce e sicuro, un client viene sottoposto a un'autenticazione 802.1X/EAP completa solo durante la sua associazione iniziale alla rete. Nei roam successivi verso gli access point adiacenti, lo scambio EAP viene ignorato, lasciando solo l'handshake a quattro vie, che è notevolmente più veloce in quanto non coinvolge il server AAA. Questa tabella descrive i vari metodi di roaming veloce e sicuro supportati dal WLC 9800 sia in modalità locale che nelle distribuzioni FlexConnect.

Funzionalità	Modalità locale	FlexConnect (modalità connessa;	FlexConnect (modalità connessa -	FlexConnect (autonomo)

		autenticazione centralizzata)	autenticazione locale)	
SKC (Sticky Key Caching)	Non supportata	Non supportata	Non supportata	Non supportata
OKC (Opportunistic Key Caching)	Supportato	Supportato	Supportato	Supportato (fino alla scadenza della sessione client)
Gestione centralizzata delle chiavi (CCKM) Cisco	Supportato	Supportato	Supportato	Non supportata
FT-802.11r/ Adaptive 11r (Transizione rapida) (via etere)	Supportato	Supportato	Supportato	Supportato (fino alla scadenza della sessione client)
FT-802.11r/ Adaptive 11r (Fast Transition) (su DS)	Supportato	Supportato	Non supportata	Non supportata

In modalità standalone, il roaming veloce dipende dal fatto che il materiale della chiave memorizzato nella cache rimanga valido. Alla scadenza della chiave PMK (Pairwise Master Key) o della sessione memorizzata nella cache, l'access point non può ottenere nuove informazioni sulla chiave derivata dal controller finché la connettività al controller non viene ripristinata.

Modalità alta scala FlexConnect

A partire da Cisco IOS XE 17.8.1, la capacità del sito flessibile è stata aumentata per supportare 300 AP e 3000 802.1x client.

La propagazione PMK consente agli access point nello stesso sito FlexConnect di condividere le informazioni PMK, riducendo la necessità di uno scambio EAP completo durante il roaming. Per impostazione predefinita, la propagazione PMK non è attivata.

Utilizzare questi comandi per verificare la propagazione PMK e per abilitarla:

- show wireless stats pmk-propagation
- propagazione pmk

Supporto Wi-Fi 7 FlexConnect

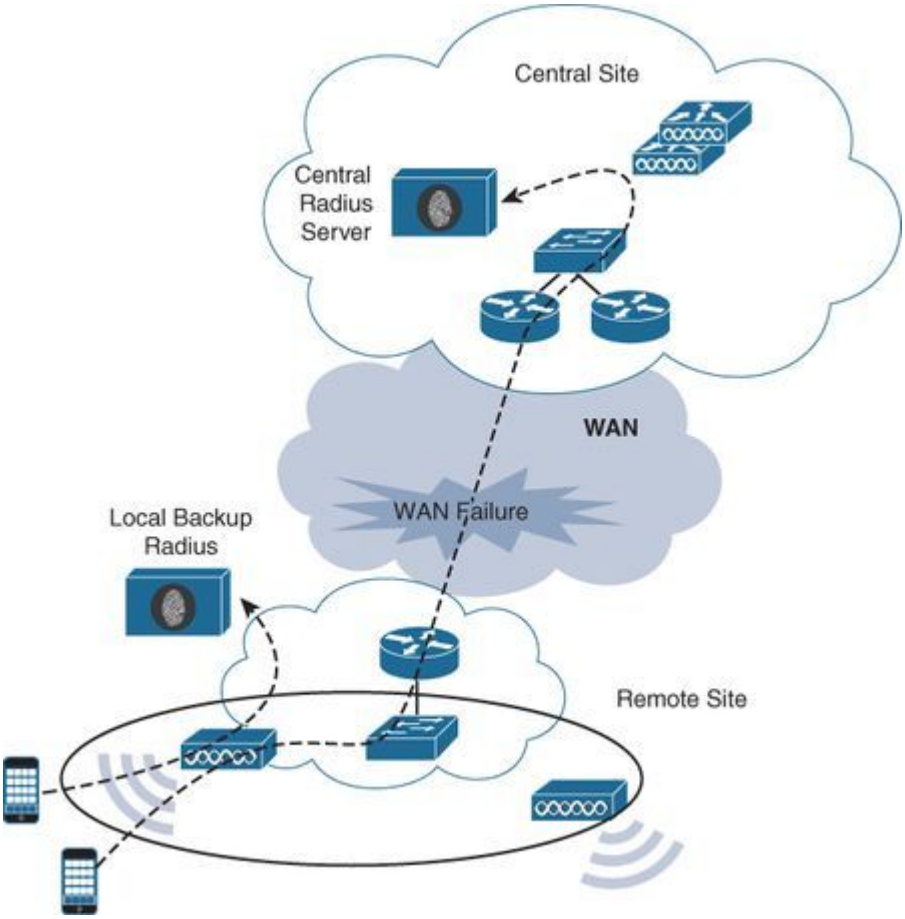
La tabella riepiloga le funzionalità di FlexConnect supportate nella famiglia di access point Wi-Fi 7 CW917x.

Funzionalità	Supporto
Switching locale	Supportato
Switching centrale	Supportato
Mappatura WLAN-VLAN	Supportato
Autenticazione locale con RADIUS esterno	Supportato
WPA3-Enterprise	Supportato
FT-802.11r Fast Roaming	Supportato
MLO (Multi Link Operation)	Supportato
Autenticazione locale con RADIUS interno	Non supportata
WPA3-Enterprise-192	Non supportata

Scenari di resilienza di FlexConnect

1. In un'impostazione di resilienza N+1, più controller attivi condividono un controller di backup comune che assume il controllo in caso di guasto di uno dei controller attivi. Quando un controller primario passa alla modalità offline, i punti di accesso FlexConnect passano immediatamente alla modalità standalone e iniziano la ricerca del controller di backup. Durante questo periodo di disconnessione, i client a commutazione centrale vengono disconnessi dai punti di accesso. Una volta che gli access point sono stati individuati e sincronizzati con il controller di backup, i client che richiedono l'accesso agli SSID commutati centralmente vengono riconnessi. Nel frattempo, i client commutati localmente non subiscono modifiche e continuano a funzionare senza notare l'interruzione del servizio.
2. Fornire un server AAA di backup nella postazione remota, accessibile dal gruppo FlexConnect. Se l'autenticazione locale è abilitata, il server RADIUS di backup viene utilizzato solo quando i punti di accesso entrano in modalità standalone e rimane inattivo mentre i punti di accesso sono in modalità connessa. Quando i punti di accesso FlexConnect utilizzano il server AAA di backup locale per l'autenticazione, le chiavi di autenticazione vengono distribuite su tutti i punti di accesso del gruppo FlexConnect, come se si trattasse di un server AAA centralizzato. Ciò garantisce che i nuovi client possano comunque eseguire il roaming senza problemi tra i punti di accesso senza dover ripetere

l'autenticazione, anche quando il server RADIUS di backup è in uso.
3. Qualsiasi metodo presente nella Feature Matrix per i Cisco Wireless Access Point che consente l'autenticazione locale.



I client eseguono l'autenticazione su un server AAA di backup locale quando il server AAA centrale diventa non disponibile a causa di un errore della WAN

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

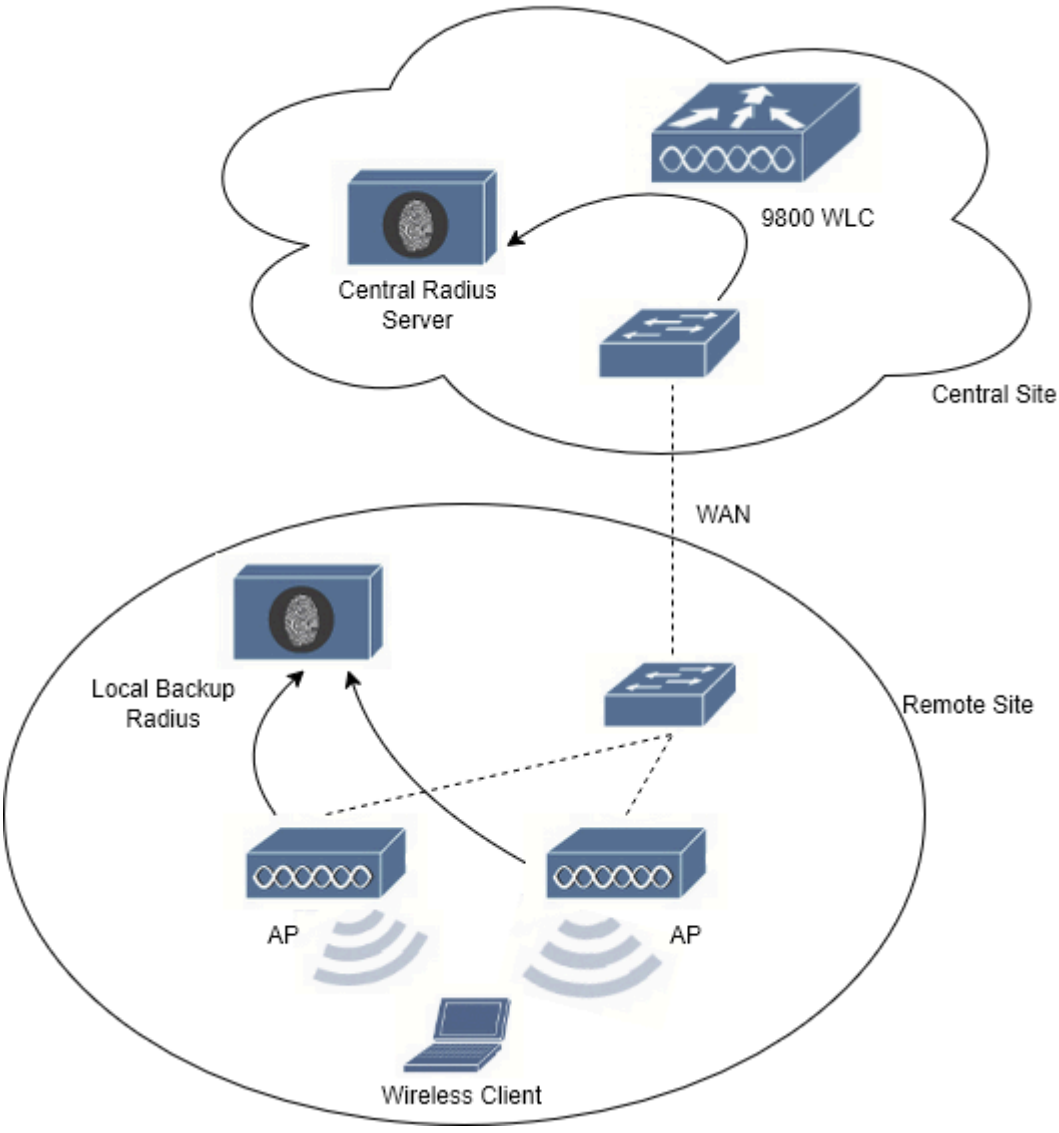
- Catalyst C9800-CL Wireless Controller per cloud con Cisco IOS® XE Dublin 17.18.3

- Access point Catalyst CW9164I-ROW v17.18.3.18
- Access point Aironet® AIR-AP2802I-E-K9 versione 17.18.3.18
- 2 Identity Services Engine v3.2.0.542

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.

Configurazione

Esempio di rete



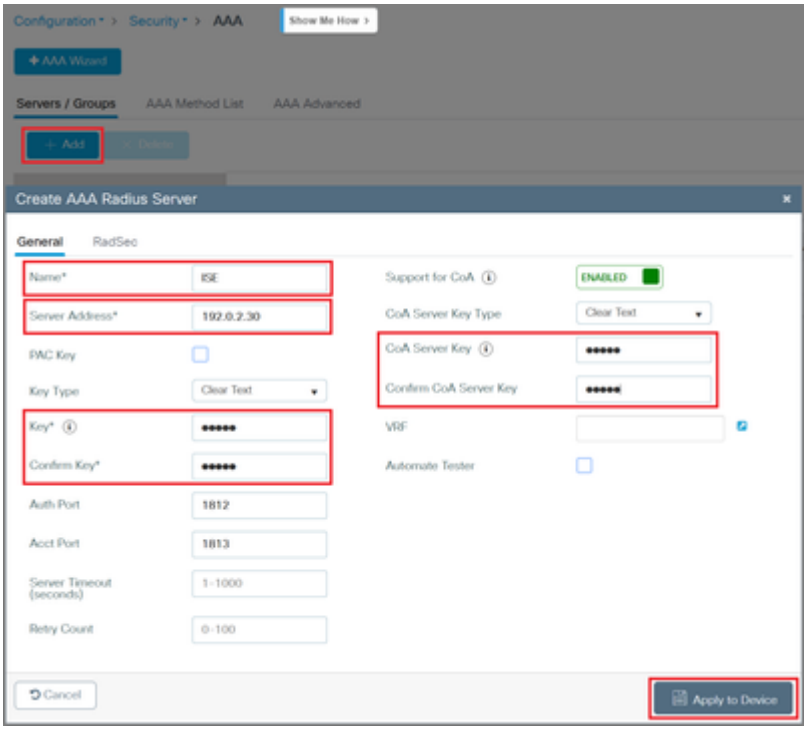
Esempio di rete

Configurazione dei server AAA

Passaggio 1. Per configurare una WLAN 802.1x, è necessario creare il gruppo di server AAA sul WLC 9800.

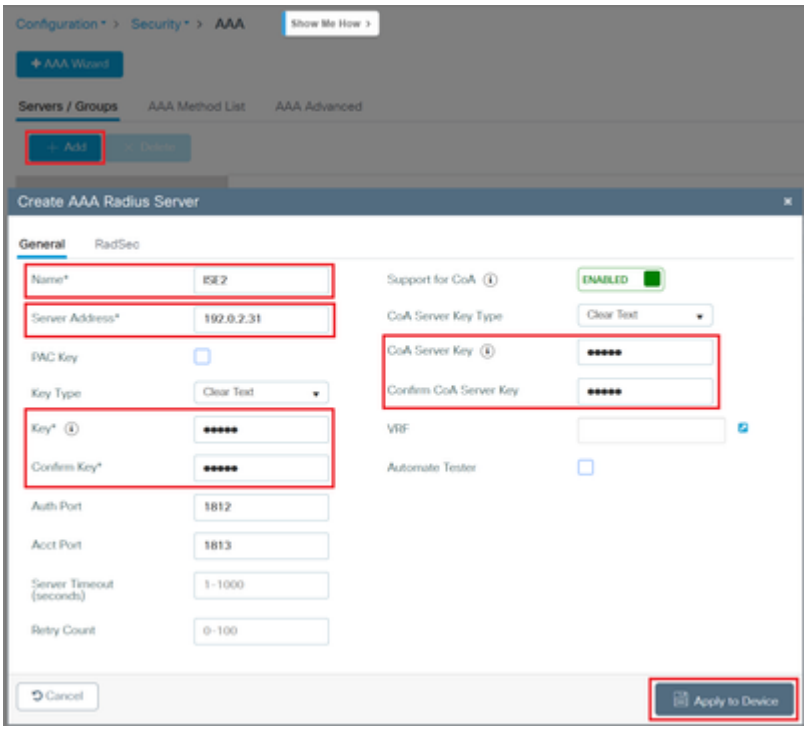
Creare un server AAA per ciascun sito, quello sul sito centrale e l'altro sul sito remoto.

Passare a Configurazione > Sicurezza > AAA > Server/Gruppi > Server e selezionare +Aggiungi. Assegnare un nome al server, il relativo indirizzo IP, la chiave (e la chiave di conferma), attivare il supporto per la modifica dell'autorizzazione e immettere la chiave del server CoA (e confermare la chiave del server CoA). Le chiavi devono essere uguali.



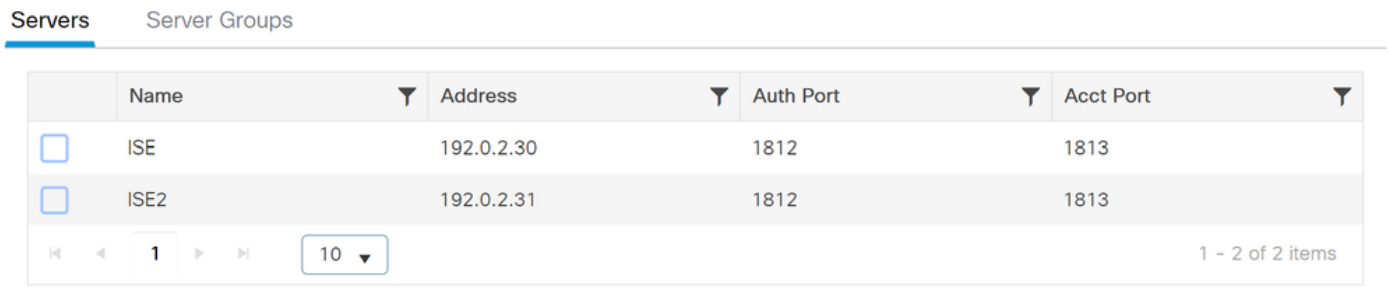
Fare clic su Applica alla periferica.

Passaggio 2. Creare l'altro server AAA:

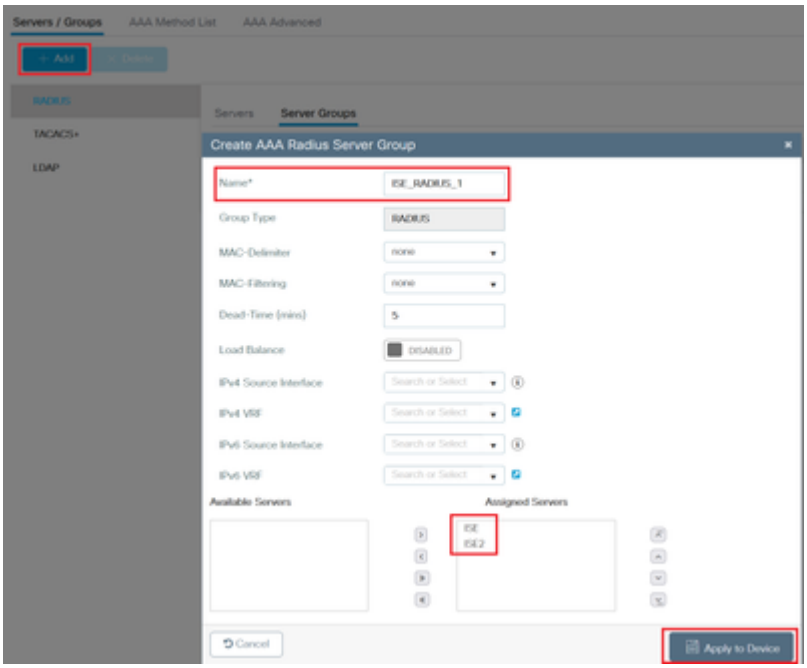


Fare clic su Applica alla periferica.

A questo punto, i server AAA sono configurati:

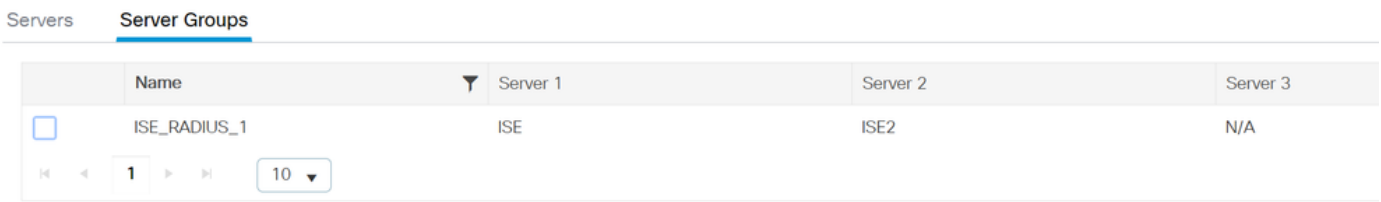


Passaggio 3. Passare a Configurazione > Sicurezza > AAA > Server/Gruppi > Gruppi di server e selezionare +Aggiungi. Assegnare un nome al server del gruppo e selezionare i server AAA creati in precedenza nella colonna Server assegnati:



Fare clic su Applica alla periferica.

Viene quindi visualizzato il gruppo di server AAA configurato:



CLI:

```
aaa new-model
!
radius server ISE
address ipv4 192.0.2.30 auth-port 1812 acct-port 1813
key keystring
!
radius server ISE2
address ipv4 192.0.2.31 auth-port 1812 acct-port 1813
key keystring
!
aaa server radius dynamic-author
client 192.0.2.30 server-key keystring
client 192.0.2.31 server-key keystring
!
aaa group server radius ISE_RADIUS_1
server name ISE
server name ISE2
deadtime 5
```

Configurazione della modalità FlexConnect sul sito remoto

Passaggio 1. Il primo passaggio consiste nella configurazione di FlexConnect sul sito remoto.

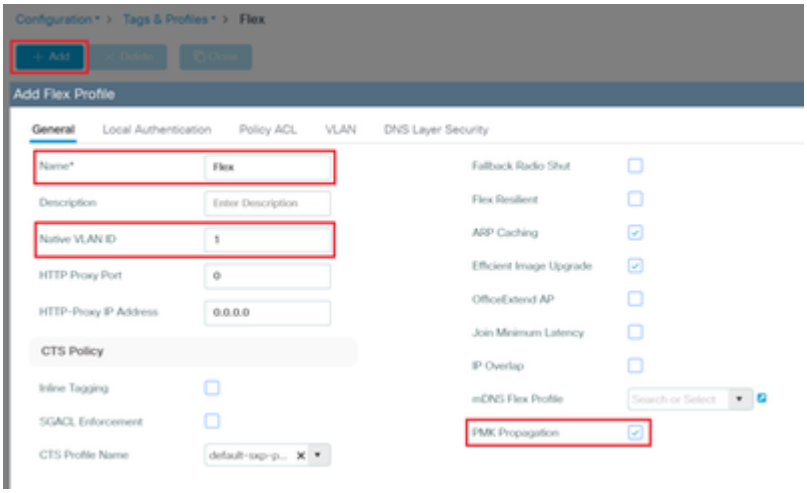
Utilizzare questa guida per modificare la modalità dei punti di accesso in Flex: informazioni su FlexConnect sul controller wireless Catalyst 9800.

Gli access point in questa guida/esercitazione utilizzano lo stesso Flex Profile.

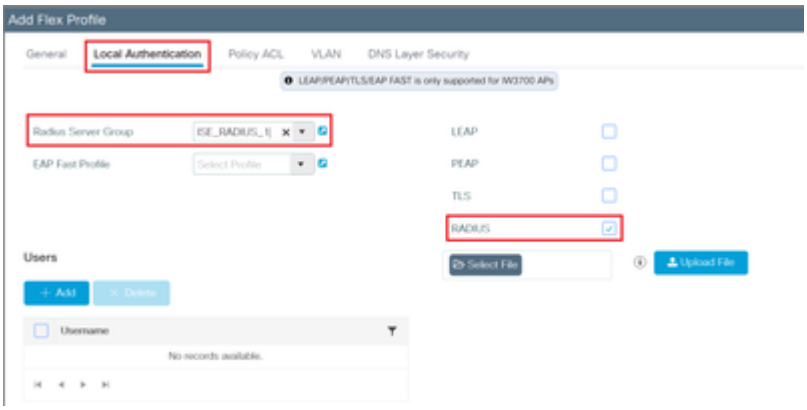
Passaggio 2. Passare a Configurazione > Tag e profili > Flex.

Creare un nuovo nome di profilo Flex con +Add. Nella scheda General (Generale), assegnare un nome al profilo, immettere l'ID della VLAN nativa (Virtual Local Area Network) e abilitare la propagazione PMK.

Abilitare la propagazione PMK per semplificare il roaming dei client wireless condividendo le informazioni PMK tra più punti di accesso all'interno di un singolo sito.

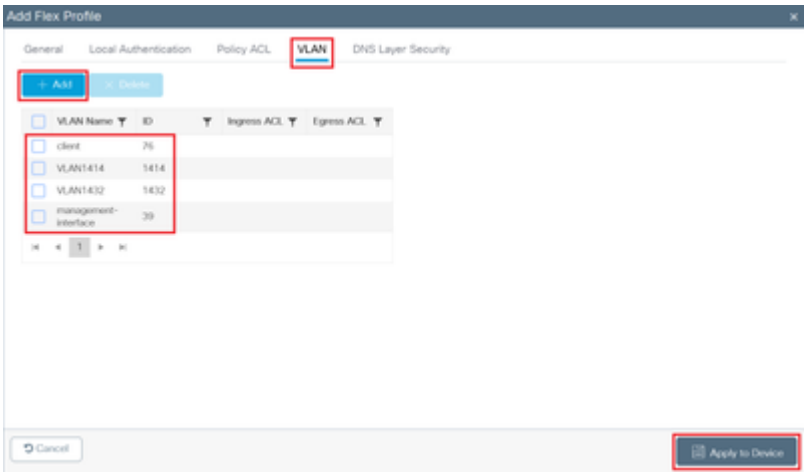


Passaggio 3. Per la rete WLAN 802.1x, nella scheda Autenticazione locale selezionare il gruppo di server Radius e abilitare RADIUS:



Suggerimento: Per una WLAN PSK, non è necessario aggiungere nulla in questa scheda.

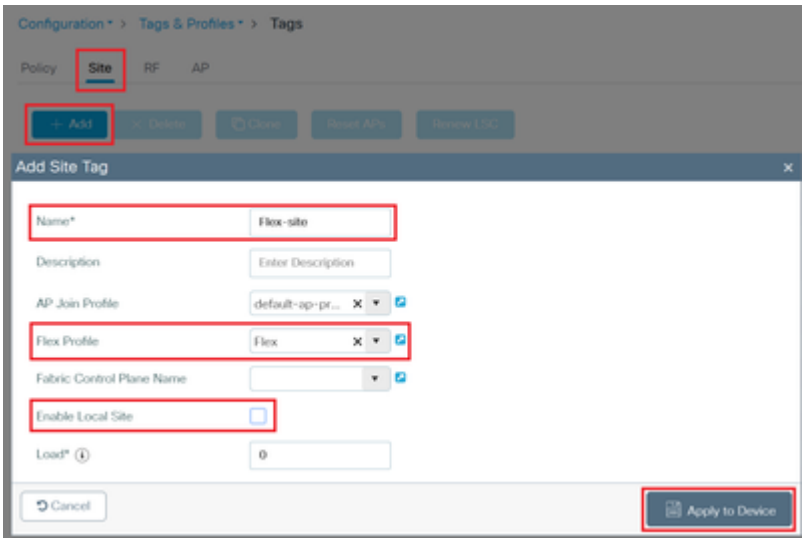
Passaggio 4. Nella scheda VLAN, aggiungere tutte le VLAN usate dai client, dai punti di accesso e dal server RADIUS. Verificare di aver creato la corrispondenza corretta tra il nome di ciascuna VLAN e l'ID VLAN corretto:



Alla fine fare clic su Update & Apply to Device (Aggiorna e applica al dispositivo).

Passaggio 5. Passare a Configurazione > Tag e profili > Tag > Sito e selezionare +Aggiungi.

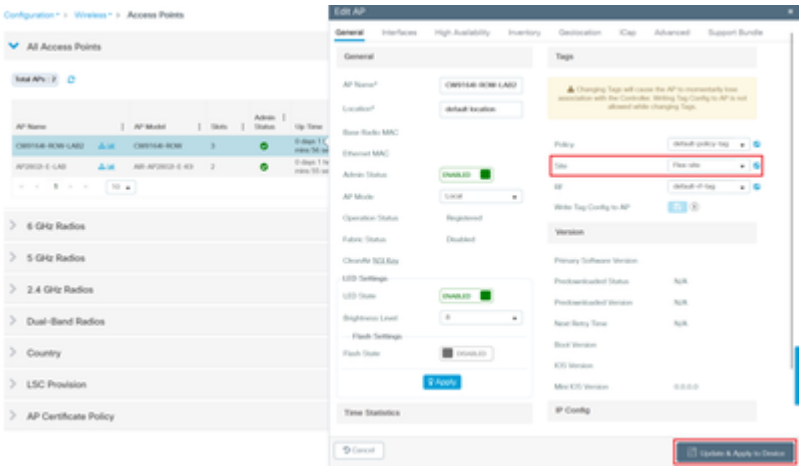
Creare il tag del sito con il profilo Flex creato in precedenza. Assegnate un nome, selezionate il profilo Flex corretto e disattivate Attiva sito locale. Verificare che il profilo di join AP sia quello corretto.



Fare clic su Applica alla periferica.

Passaggio 6. Passare a Configurazione > Wireless > Access Point.

Selezionare l'access point, in Generale > Tag modificare il tag del sito con il tag configurato in precedenza:



Fare clic su Update & Apply to Device (Aggiorna e applica al dispositivo).

L'access point si disconnette dal WLC e si unisce nuovamente alla modalità Flex AP.

Nella stessa pagina, quando l'access point si ricongiunge, è possibile controllare la modalità AP nella colonna Modalità AP.

Se si seleziona il punto di accesso, viene visualizzato il nuovo tag Sito:



CLI:

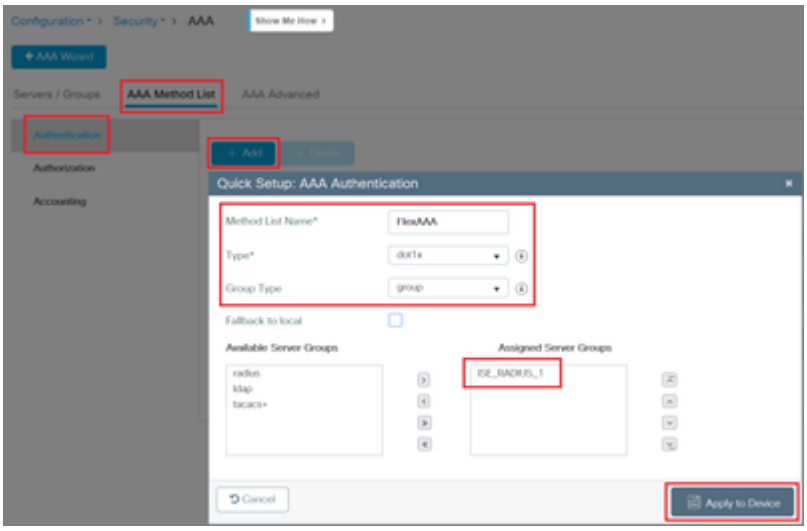
```
wireless profile flex Flex
ip http client proxy 0.0.0.0 0
local-auth radius-server-group ISE_RADIUS_1
vlan-name client
vlan-id 76
vlan-name VLAN1414
vlan-id 1414
vlan-name VLAN1432
vlan-id 1432
vlan-name management-interface
vlan-id 39
pmk propagate
!
wireless tag site Flex-site
ap-profile default-ap-profile
no local-site
flex-profile Flex
!
ap h.h.h (AP Radio MAC address)
policy-tag default-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

Configurazione della WLAN 802.1x con l'autenticazione locale tramite un server RADIUS esterno

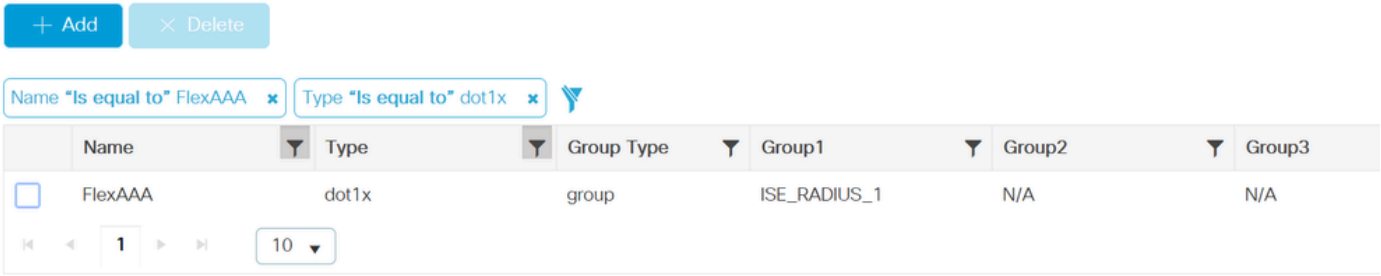
Passaggio 1. Creare l'elenco dei metodi di autenticazione.

Selezionare Configurazione > Sicurezza > AAA, in Elenco metodi AAA > scheda Autenticazione.

Selezionare +Aggiungi, assegnare un nome al nome dell'elenco di metodi, selezionare dot1x come tipo, selezionare group come tipo di gruppo e assegnare il gruppo di server AAA nella colonna Assigned Server Groups:



Viene visualizzato l'elenco dei metodi AAA creati:



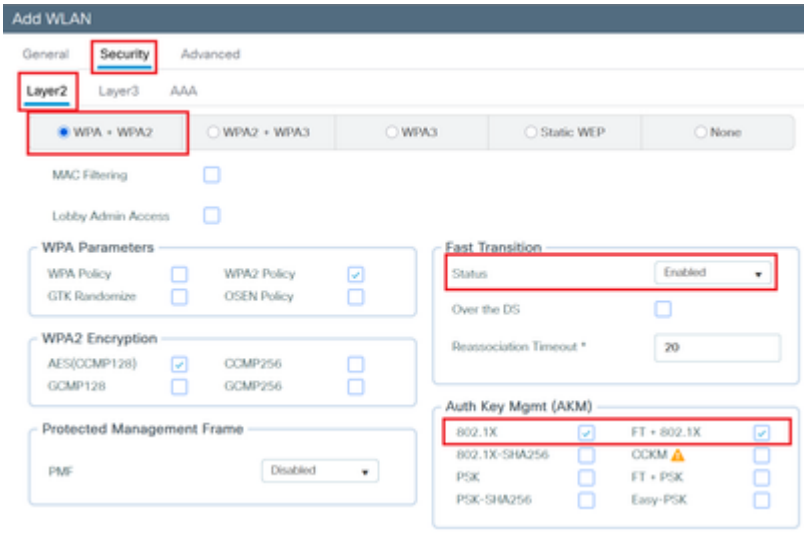
Passaggio 2. Creare la WLAN.

Selezionare Configurazione > Tag e profili > WLAN, quindi selezionare +Aggiungi.

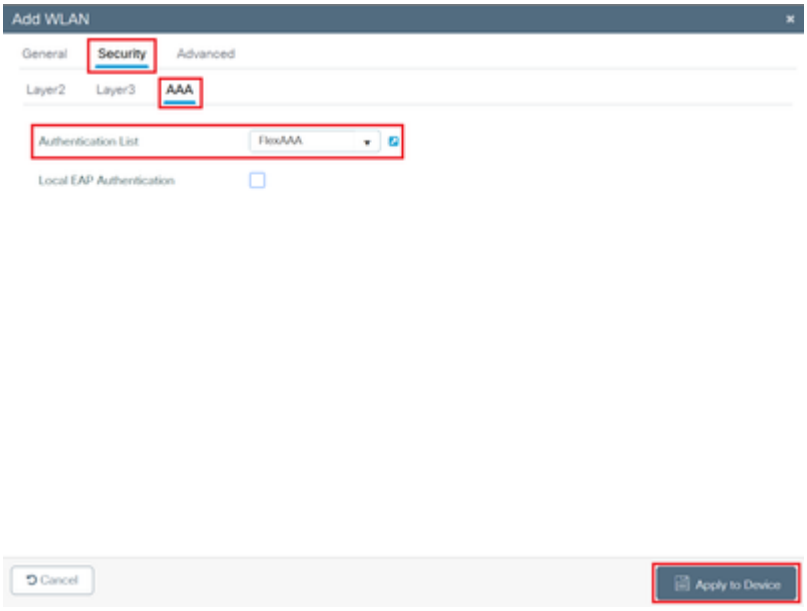
Su tag General creare un nome per Nome profilo, SSID e Stato abilitazione:



Passaggio 3. Passare a Sicurezza > scheda Layer 2, selezionare WPA+WPA2 (Wi-Fi Protected Access), Fast Transition as Enabled, Auth Key Mgmt 802.1X e FT+802.1X:



Passaggio 4. Passare alla scheda Sicurezza > AAA, nel menu a discesa Authentication List (Elenco autenticazione) selezionare l'elenco creato in precedenza:



Fare clic su Update & Apply to Device (Aggiorna e applica al dispositivo).

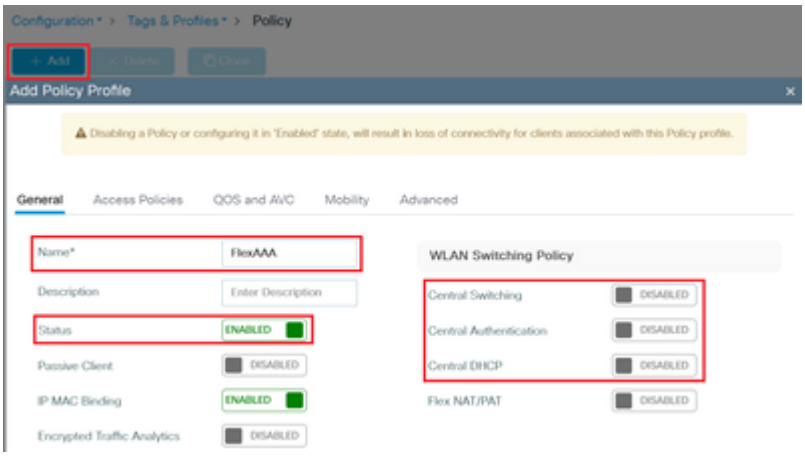
Viene quindi visualizzata la WLAN creata:



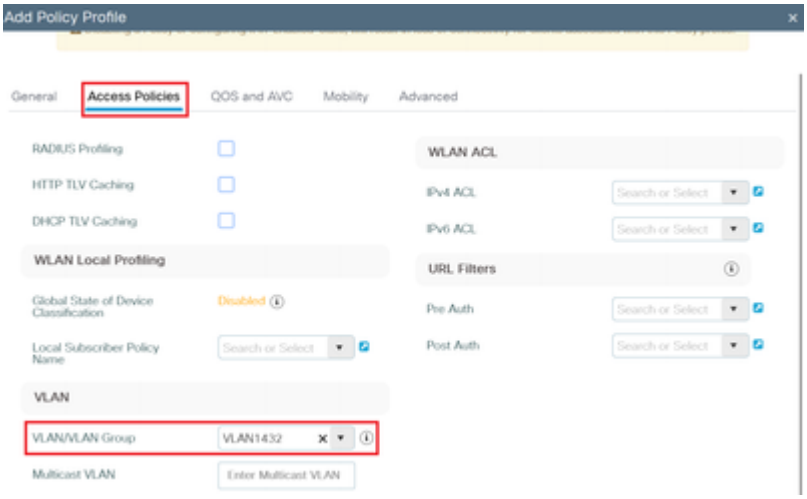
Passaggio 5. Creare il profilo dei criteri.

Selezionare Configurazione > Tag e profili > Criterio.

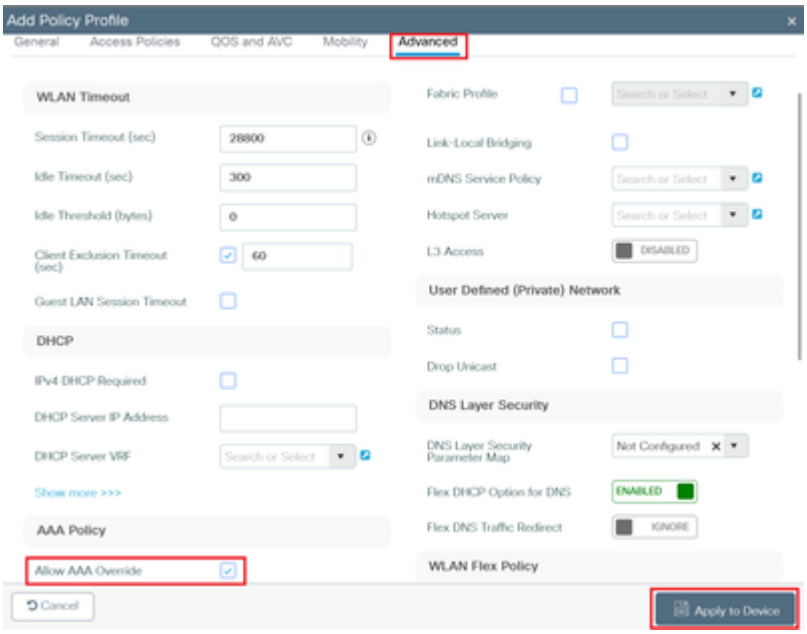
Selezionare +Aggiungi e nella scheda Generale assegnare un nome al profilo del criterio, abilitare lo stato e disabilitare la commutazione centrale, l'autenticazione centrale e il protocollo DHCP (Dynamic Host Configuration Protocol) centrale:



Passaggio 6. Passare alla scheda Criteri di accesso, selezionare la VLAN:

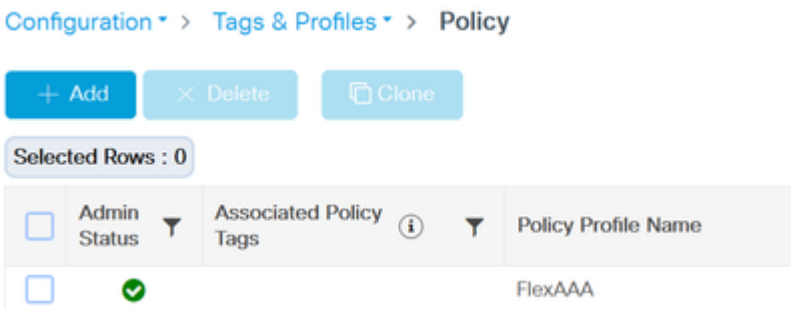


Passaggio 7. Passare alla scheda Avanzate, abilitare Consenti sostituzione AAA.:



Fare clic su Aggiorna e applica al dispositivo.

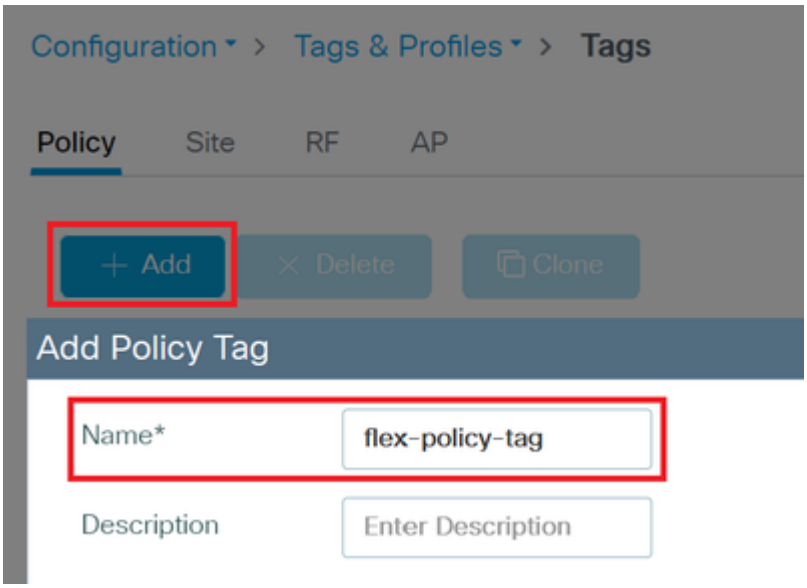
È possibile visualizzare il profilo dei criteri nell'elenco:



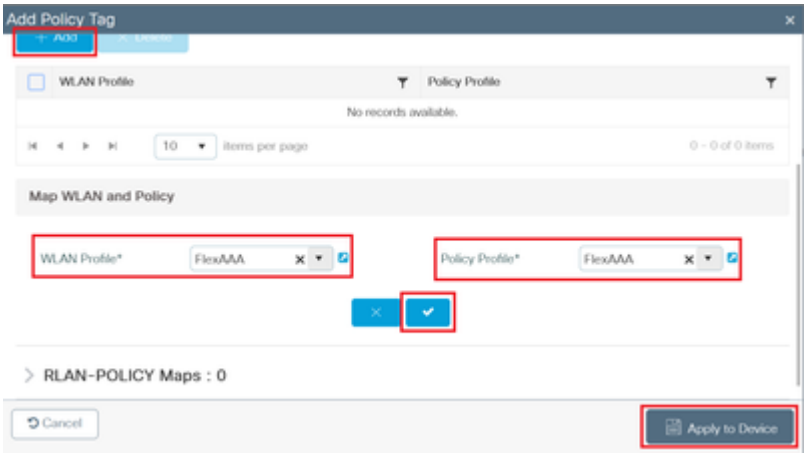
Passaggio 8. Creazione del tag dei criteri.

Selezionare Configurazione > Tag e profili > Tag

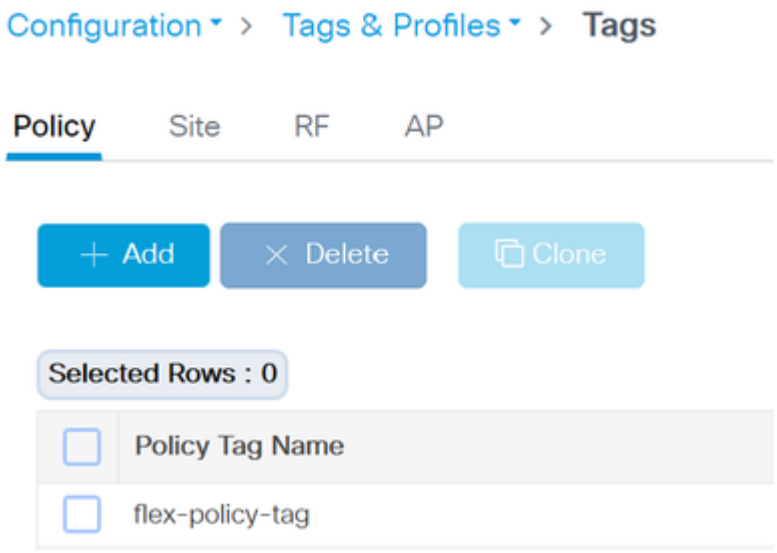
Nella scheda Criterio selezionare +Aggiungi. Assegnare un nome al tag del criterio:



Scorrere verso il basso e selezionare +Add in WLAN-POLICY Maps. In Profilo WLAN selezionare dal menu a discesa la WLAN creata in precedenza. In Profilo criterio selezionare il Profilo criterio creato in precedenza dal menu a discesa. Fare clic sul pulsante di controllo e quindi su Applica a dispositivo:

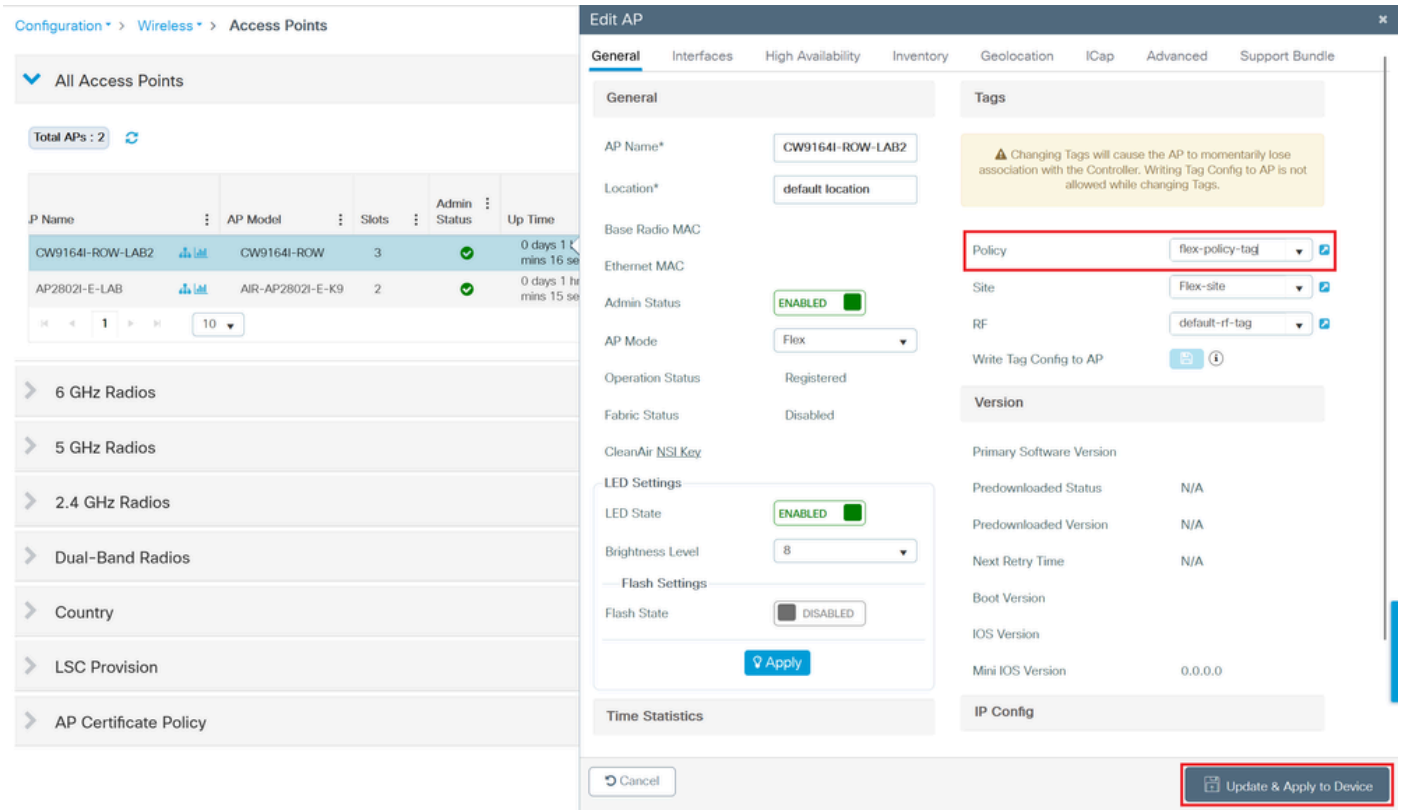


Nell'elenco è possibile visualizzare il tag relativo ai criteri:



Passaggio 9. Assegnare il tag dei criteri sul tag AP.

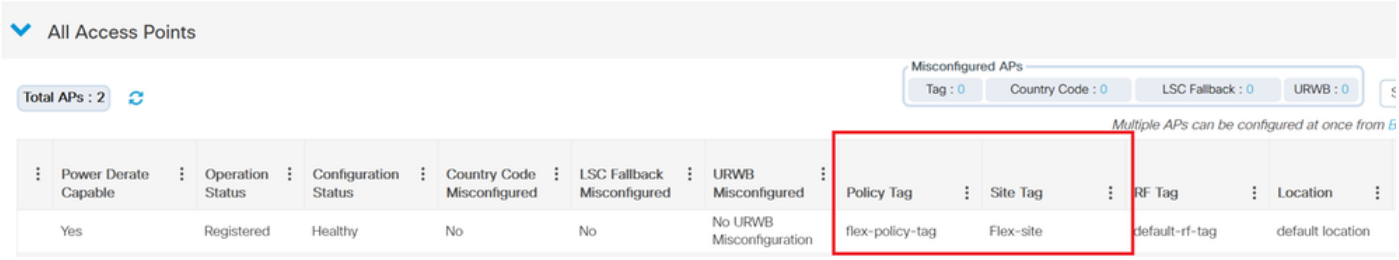
Selezionare Configurazione > Wireless > Access Point. Selezionare l'access point per modificare il tag.



Fare clic su Update & Apply to Device (Aggiorna e applica al dispositivo).

L'access point si separa e si unisce di nuovo con il nuovo tag dei criteri.

Quando l'access point si unisce nuovamente, è possibile controllare l'elenco Access Point, verificare che l'access point sia in modalità Flex e i tag assegnati:



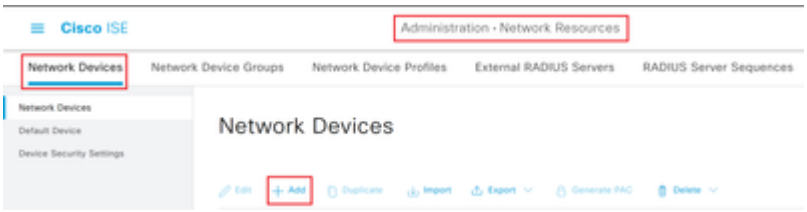
CLI:

```
aaa authentication dot1x FlexAAA group ISE_RADIUS_1
!
wlan FlexAAA 4 FlexAAA
radio policy dot11 24ghz
radio policy dot11 5ghz
security ft
security wpa akm ft dot1x
security dot1x authentication-list FlexAAA
no shutdown
!
wireless profile policy FlexAAA
aaa-override
no central authentication
no central dhcp
no central switching
vlan VLAN1432
no shutdown
!
wireless tag policy flex-policy-tag
wlan FlexAAA policy FlexAAA
!
ap h.h.h (AP Radio MAC address)
policy-tag flex-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

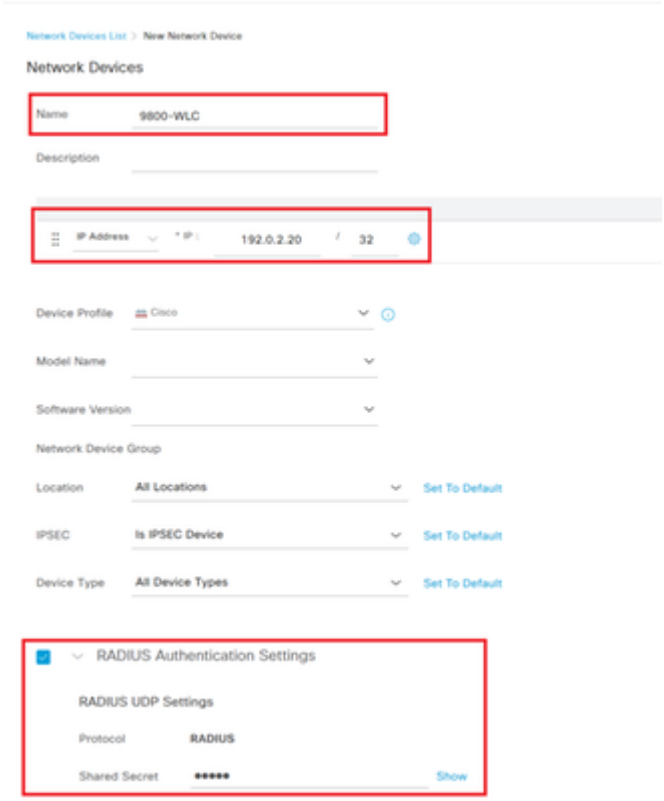
Configurare ISE

A questo punto, è necessario configurare ISE in modo che sia in grado di autenticare i client quando si trovano nell'autenticazione locale.

Passaggio 1. Passare a Amministrazione > Risorse di rete > Dispositivi di rete. Selezionare +Aggiungi.



Passaggio 2. Aggiungere il WLC 9800. Assegnare un nome, aggiungere il relativo indirizzo IP, abilitare le impostazioni di autenticazione RADIUS e aggiungere la chiave privata condivisa. Questa chiave deve essere la stessa chiave configurata in precedenza quando sono stati creati i server AAA sul WLC 9800.



Nell'angolo in basso a destra, fare clic su Save (Salva).

Passaggio 3. È necessario aggiungere gli access point all'elenco dei dispositivi di rete in modo che possano agire come autenticatori/server d'inoltro AAA quando il sito remoto perde il collegamento WAN (e quando gli access point passano alla modalità standalone).

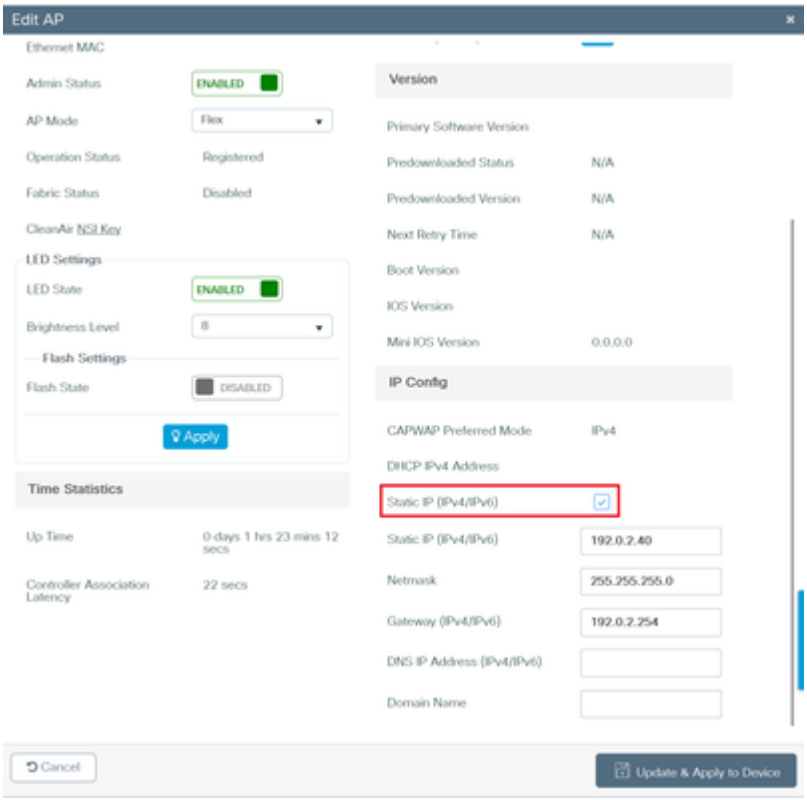
Selezionare Configuration > Wireless > Access Point sulla GUI del WLC 9800 e prendere nota di ciascun indirizzo IP dell'access point.

Nota: Configurare l'indirizzo IP di ciascun Flex AP su Static. Quando gli access point

---

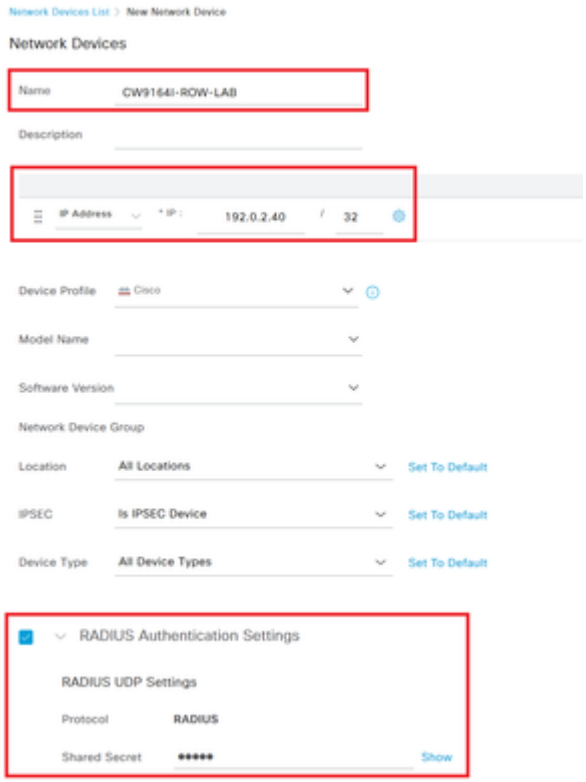
perdono e riprendono la connessione al WLC 9800, possono tornare con un indirizzo IP diverso da DHCP, perdendo così la comunicazione con ISE.

Abilitare IP statico (IPv4/IPv6). Fare clic su Aggiorna e applica al dispositivo:



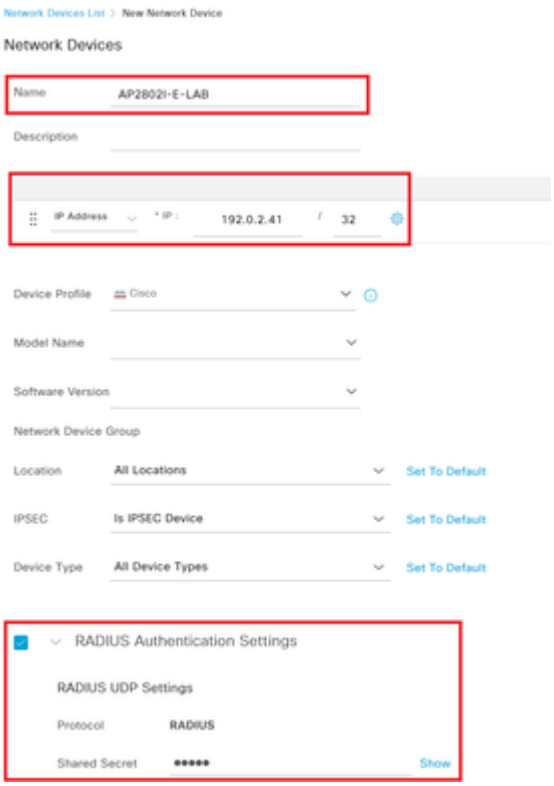
Passaggio 4. Tornando ad ISE, selezionare Administration > Network Resources > Network Devices (Amministrazione > Risorse di rete > Dispositivi di rete). Selezionare +Aggiungi.

Aggiungere i punti di accesso come dispositivi di rete, con la stessa configurazione del WLC 9800:



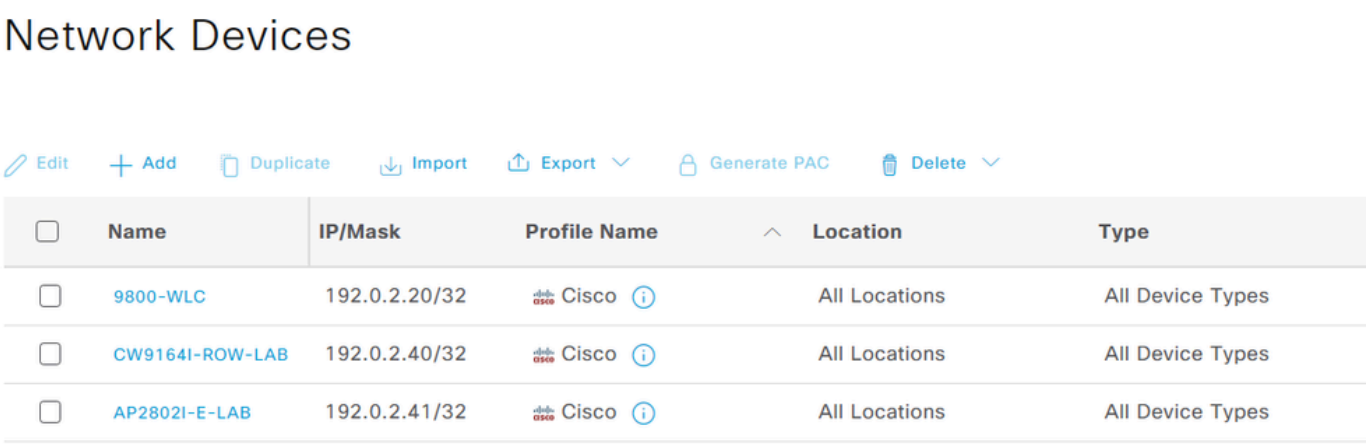
Nell'angolo in basso a destra, fare clic su Save (Salva).

Per il secondo punto di accesso:



Nell'angolo in basso a destra, fare clic su Save (Salva).

È possibile visualizzare questo elenco di dispositivi di rete:

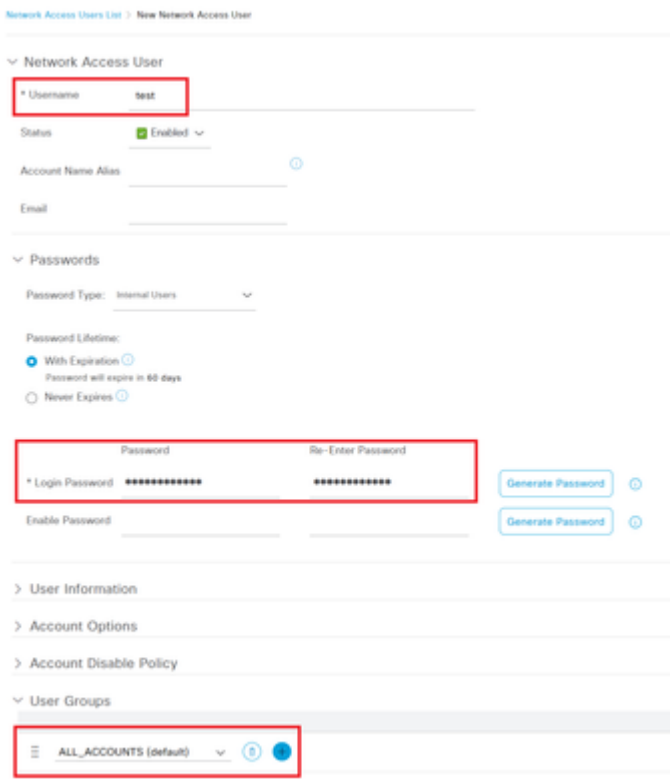


Se i punti di accesso si trovano in intervalli IP contigui, è possibile utilizzare la funzione di maschera per configurare una singola voce che definisca il segreto condiviso per un intero gruppo (se non tutti) di punti di accesso. Ad ISE non è necessario configurare un dispositivo di rete per ciascun access point. Si noti, tuttavia, che l'utilizzo di caratteri jolly e maschere consente a un dispositivo non autorizzato di fungere da server di inoltro per ISE.

Passaggio 5. Passare a Amministrazione > Gestione delle identità > Identità, nella scheda Utenti, e creare un utente per l'autenticazione 802.1x. Seleziona +Aggiungi:

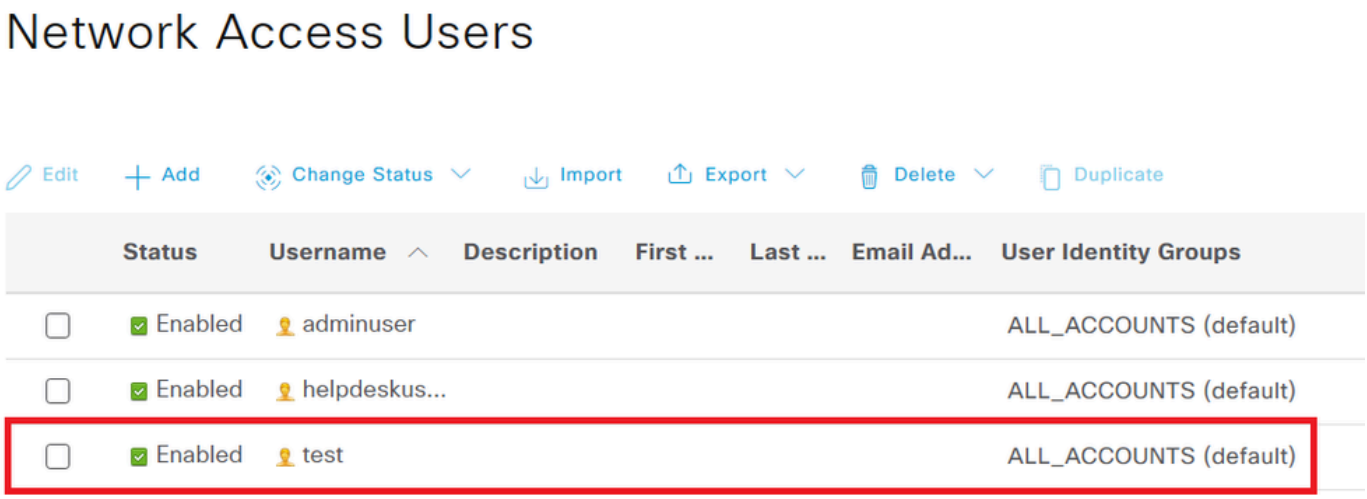


Creare un nome utente, la password (e digitare la stessa password quando si immette nuovamente la password) e selezionare ALL_ACCOUNTS (impostazione predefinita) dal menu a discesa Gruppi di utenti:

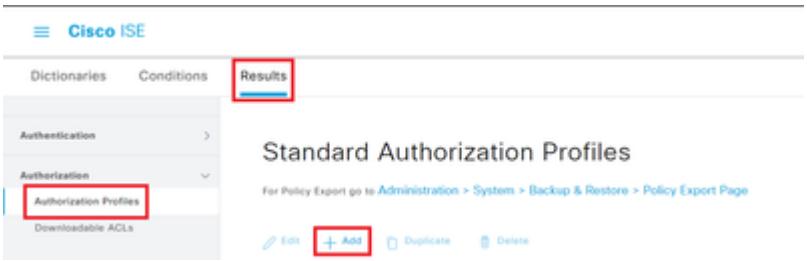


Nell'angolo in basso a destra, fare clic su Submit (Invia).

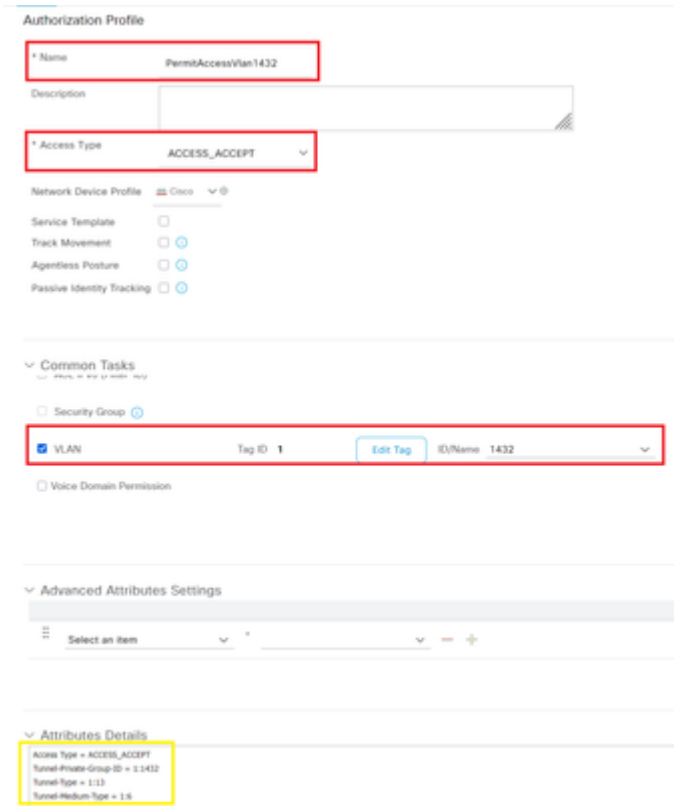
È possibile visualizzare l'utente nell'elenco Utenti accesso alla rete:



Passaggio 6. Passare a Criterio > Elementi criteri > Risultati. Nella scheda Autorizzazione > Profili di autorizzazione, selezionare +Aggiungi.



Creare il profilo di autorizzazione per la VLAN a cui sono assegnati i client di autenticazione locale:

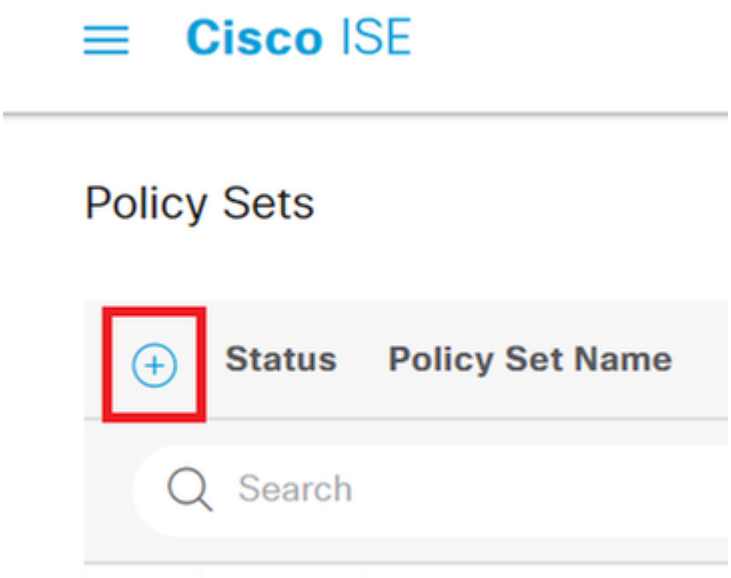


Nell'angolo in basso a destra, fare clic su Submit (Invia).

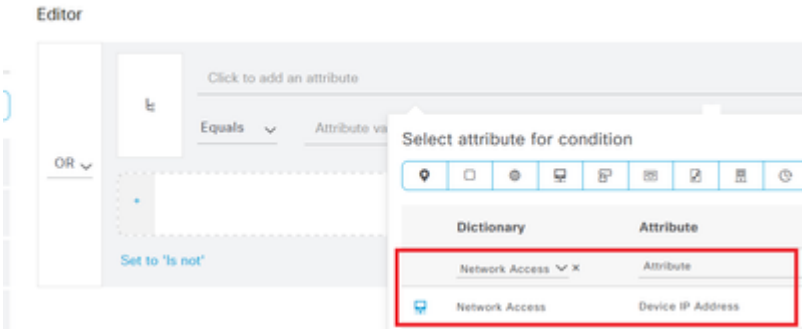
In uno scenario di successo, è possibile visualizzare i dettagli degli attributi che ISE invia ai WLC/AP.

Passaggio 7. Andare a Policy > Policy Sets (Policy > Set di policy). Crea un nuovo set di criteri.

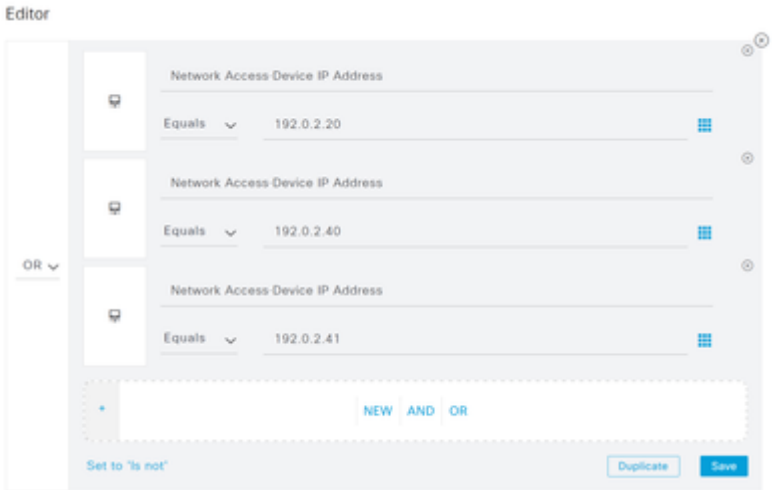
Fare clic sul segno +:



Assegnare un nome al set di criteri. Nella colonna Condizioni aggiungere la regola OR e aggiungere il dizionario Accesso di rete, con l'attributo Indirizzo IP periferica, selezionare Uguale a:

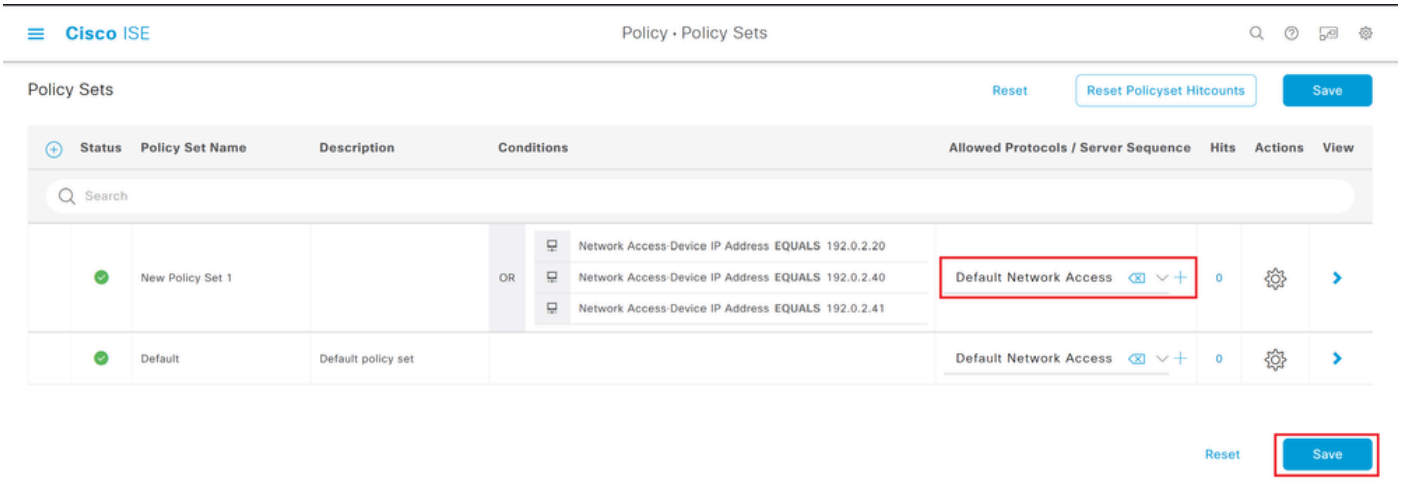


Aggiungere il WLC 9800 e gli indirizzi IP degli access point:

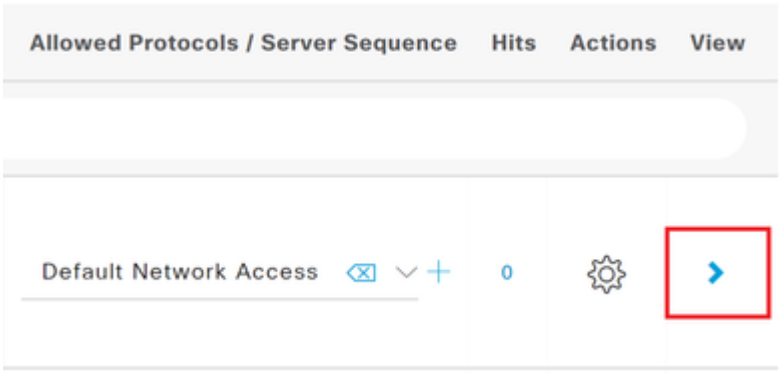


Nell'angolo in basso a destra, fare clic su Use (Usa).

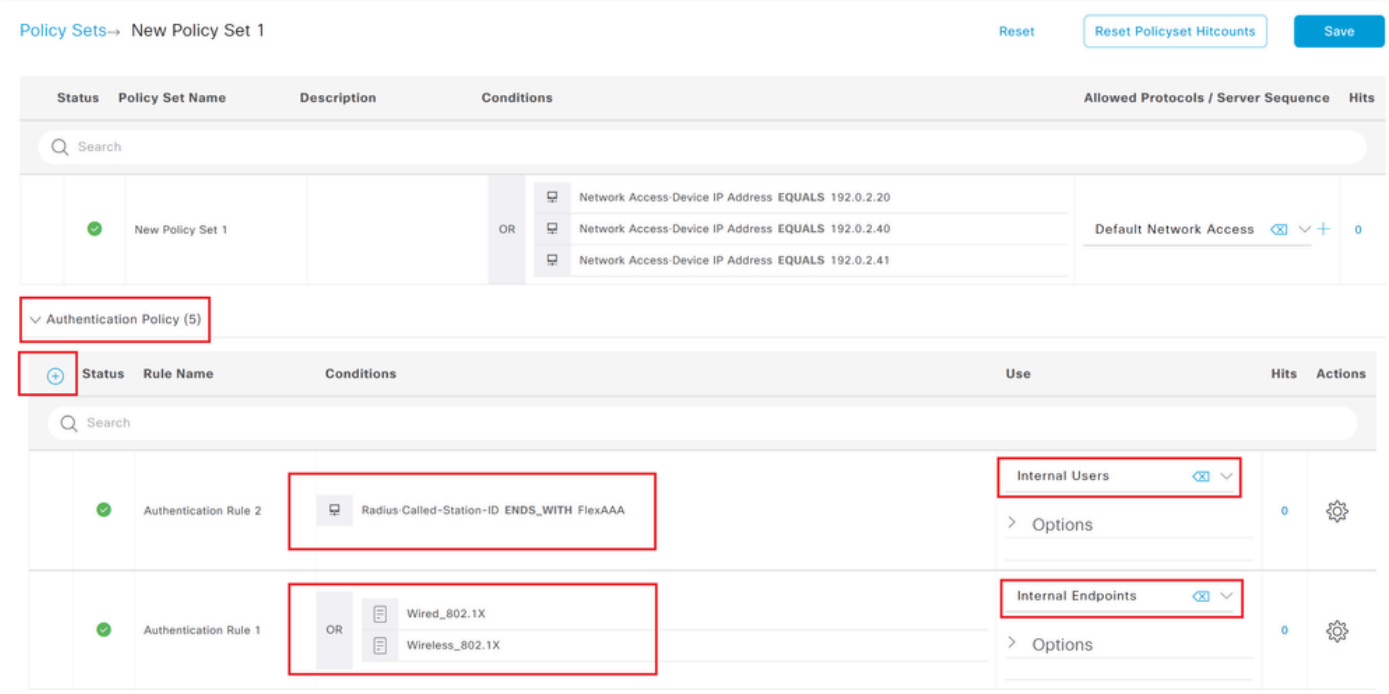
Passaggio 8. Nella colonna Protocolli consentiti selezionare Accesso di rete predefinito. Alla fine, fare clic su Save (Salva):



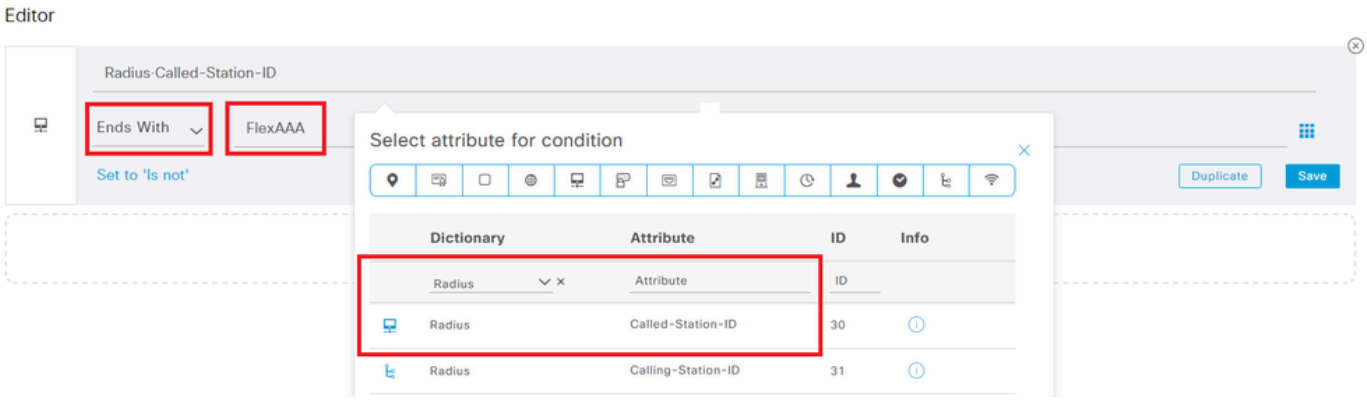
Passaggio 9. Nella colonna Visualizza fare clic sul segno di freccia:



Passaggio 10. Espandere Criteri di autenticazione, creare due nuovi criteri: uno per il nome WLAN, l'altro per la configurazione 802.1X:

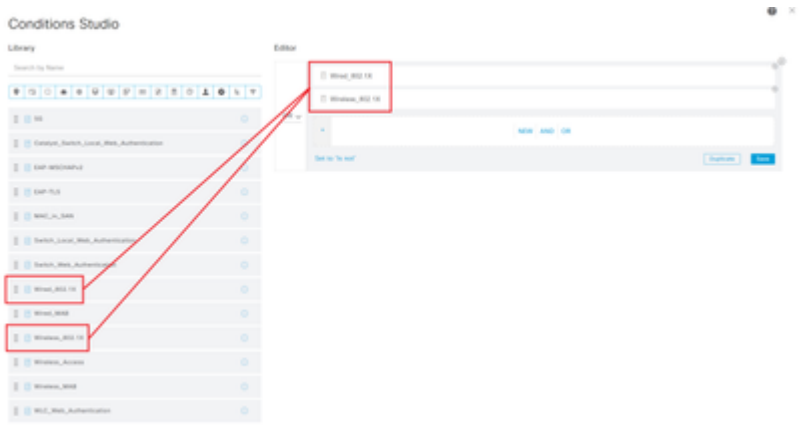


Per il nome della WLAN, creare la condizione con il dizionario Radius e l'attributo Called-Station-ID. Selezionare Termina con e digitare il nome della WLAN:



Nell'angolo in basso a destra, fare clic su Use (Usa). Per questo criterio, nella colonna Utilizza, selezionare Utenti interni.

Passaggio 11. Per il criterio 802.1X, creare la condizione con la libreria Wired_802.1X e Wireless_802.1X disponibile su ISE. È possibile trascinare questi elementi e selezionare la condizione OR:



Nell'angolo in basso a destra, fare clic su Use (Usa). Per questo criterio, nella colonna Utilizza, selezionare Endpoint interni.

Passaggio 12. Scorrere fino a Criteri di autorizzazione e creare un nuovo criterio. Assegnare un nome alla rete e creare la stessa condizione creata per il nome della rete WLAN nei criteri di autenticazione.

Nella colonna Profili selezionare dal menu a discesa il profilo PermitAccessVlan1432:



Nell'angolo in basso a destra, fare clic su Save (Salva).

Configurazione della WLAN della chiave pubblica con autenticazione locale

Passaggio 1. Configurare innanzitutto gli access point in modalità Flex come descritto nella sezione Configurazione della modalità FlexConnect sul sito remoto.

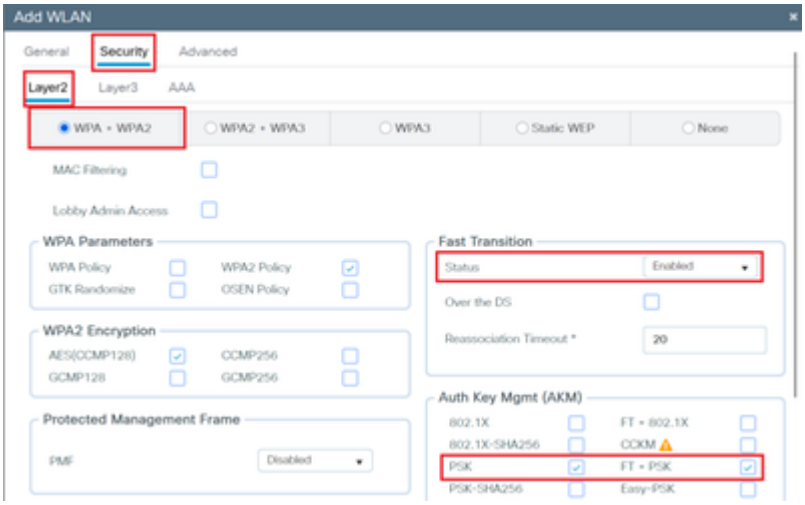
Passaggio 2. Creare la WLAN.

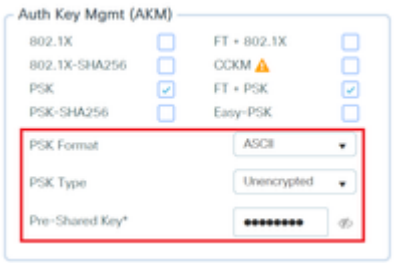
Selezionare Configurazione > Tag e profili > WLAN, quindi selezionare +Aggiungi.

Su tag General creare un nome per Nome profilo, SSID e Stato abilitazione:



Passaggio 3. Passare a Sicurezza > Scheda Layer 2 selezionare WPA+WPA2, Transizione rapida come abilitata, Auth Key Mgmt PSK e FT+PSK, scegliere il formato PSK e il tipo di chiave già condivisa che si desidera utilizzare per i client:





Fare clic su Update & Apply to Device (Aggiorna e applica al dispositivo).

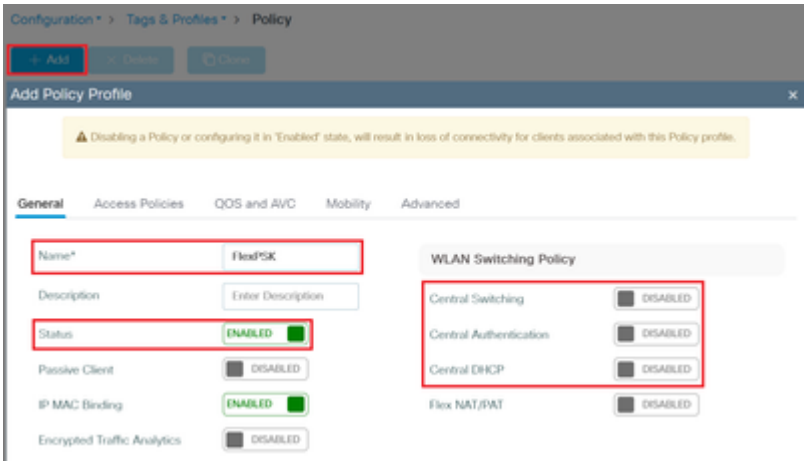
La WLAN creata è visibile:



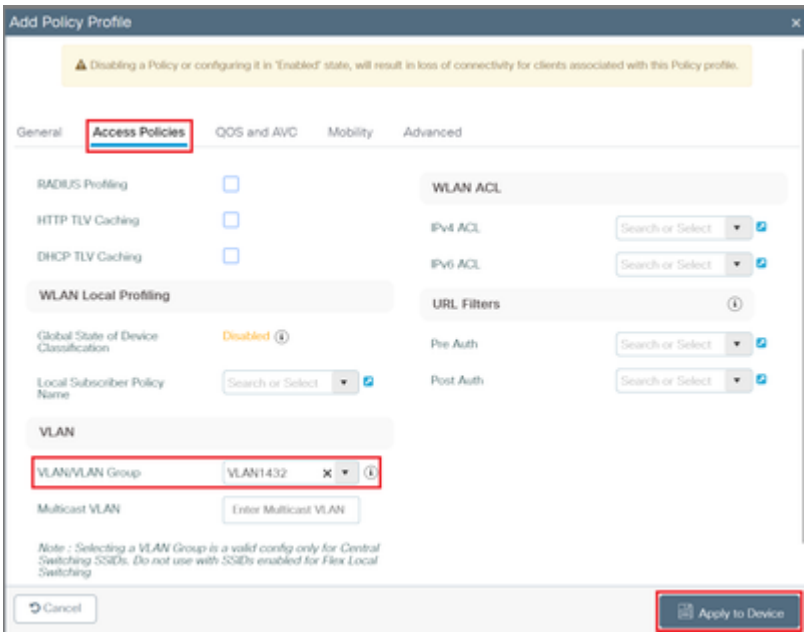
Passaggio 4. Creare il profilo dei criteri.

Selezionare Configurazione > Tag e profili > Criterio.

Selezionare +Aggiungi e nella scheda Generale assegnare un nome al profilo del criterio, abilitare lo stato e disabilitare la commutazione centrale, l'autenticazione centrale e DHCP centrale:

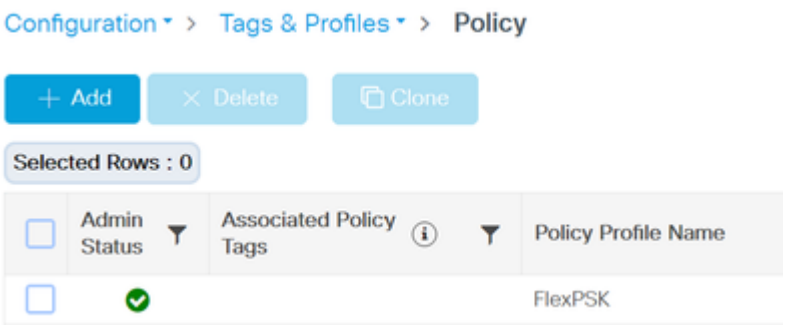


Passaggio 5. Passare alla scheda Criteri di accesso, quindi selezionare la VLAN:



Fare clic su Update & Apply to Device (Aggiorna e applica al dispositivo).

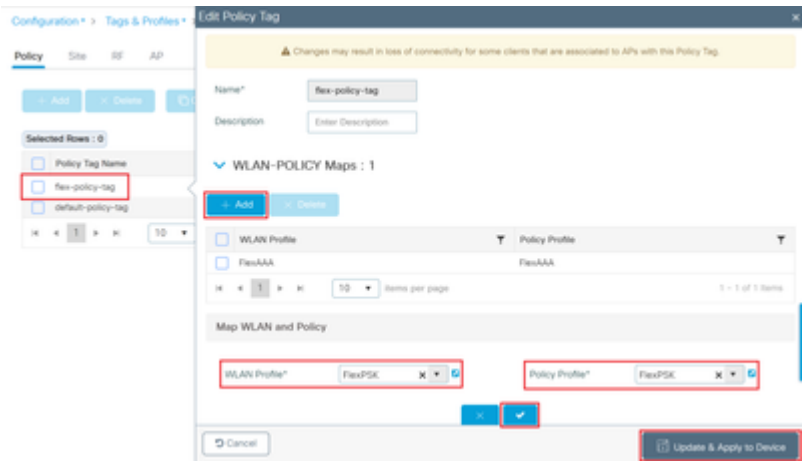
È possibile visualizzare il profilo dei criteri nell'elenco:



Passaggio 6. È possibile creare un nuovo tag di criterio o modificare quello esistente.

Passare a Configurazione > Tag e profili > Tag per modificare il tag di criterio esistente. Selezionare il tag da modificare.

Selezionare +Add in WLAN-POLICY Maps. In Profilo WLAN selezionare dal menu a discesa la WLAN creata in precedenza. In Profilo criterio selezionare il Profilo criterio creato in precedenza dal menu a discesa. Fare clic sul pulsante di controllo e quindi su Applica a dispositivo:



Se il tag dei criteri è già assegnato all'access point, non è necessario eseguire altre operazioni.

In caso contrario, assegnare il tag di criterio sul tag AP. Passare a Configurazione > Wireless > Access Point. Selezionare l'access point per modificare il tag della policy e fare clic su "Aggiorna e applica al dispositivo".

L'access point si disgiunge e si unisce di nuovo con il nuovo tag dei criteri.

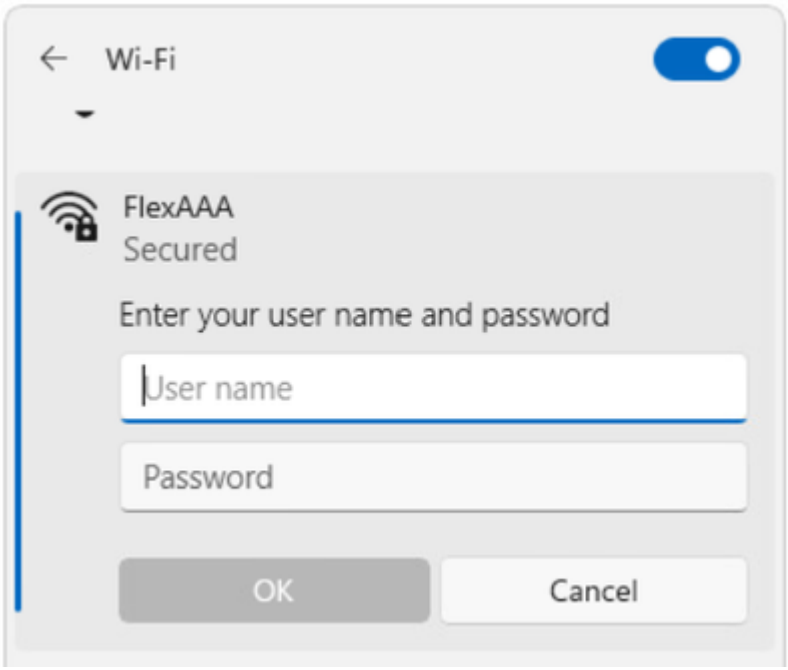
Quando l'access point si unisce nuovamente, è possibile controllare l'elenco dei punti di accesso, verificare che l'access point sia in modalità Flex e che abbia i tag assegnati corretti.

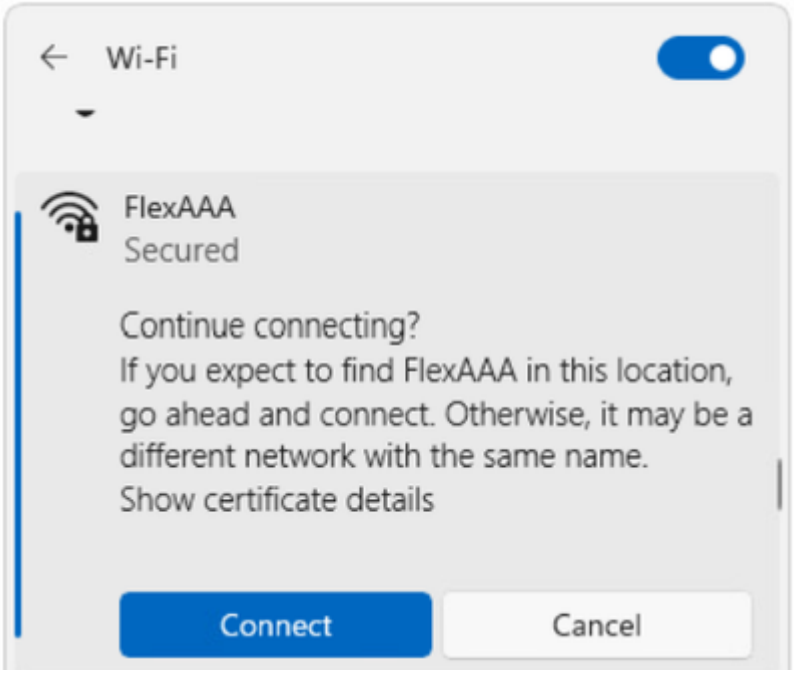
CLI:

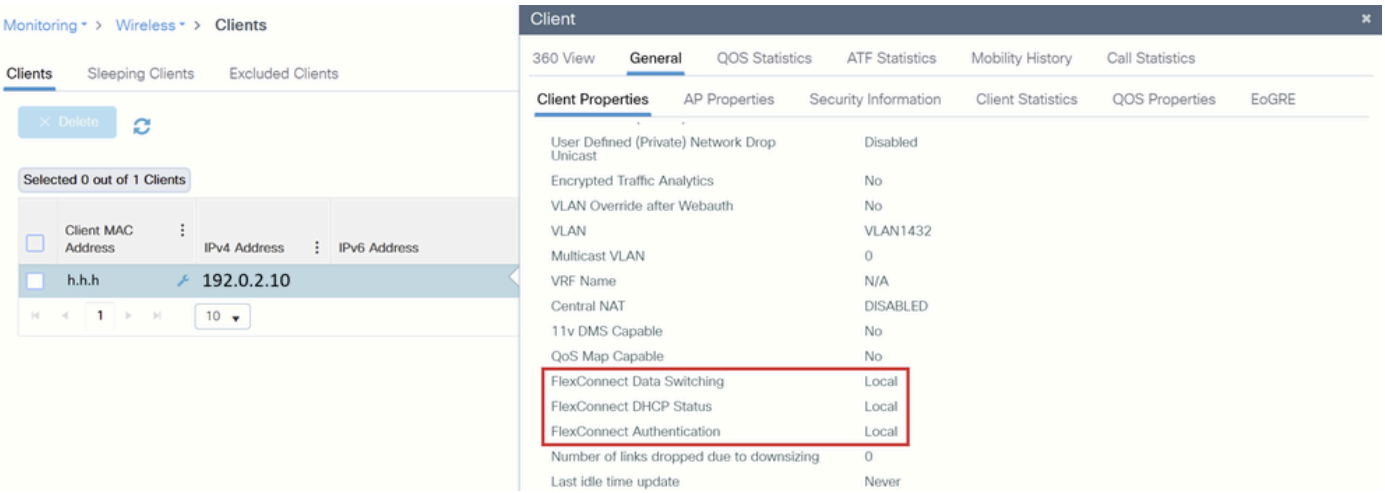
```
wlan FlexPSK 5 FlexPSK
radio policy dot11 24ghz
radio policy dot11 5ghz
security ft
security wpa psk set-key ascii 0 Password123
no security wpa akm dot1x
security wpa akm ft psk
security wpa akm psk
no shutdown
!
wireless profile policy FlexPSK
no central authentication
no central dhcp
no central switching
vlan VLAN1432
no shutdown
!
wireless tag policy flex-policy-tag
wlan FlexAAA policy FlexAAA
wlan FlexPSK policy FlexPSK
!
ap h.h.h (AP Radio MAC address)
policy-tag flex-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

Verifica

Per WLAN 802.1x:


Wi-Fi
FlexAAA
Secured
Enter your user name and password
User name
Password
OK
Cancel


Wi-Fi
FlexAAA
Secured
Continue connecting?
If you expect to find FlexAAA in this location, go ahead and connect. Otherwise, it may be a different network with the same name.
Show certificate details
Connect
Cancel


Monitoring > Wireless > Clients
Clients
Sleeping Clients
Excluded Clients
Delete
Selected 0 out of 1 Clients
Client MAC Address
IPv4 Address
IPv6 Address
h.h.h
192.0.2.10
1
10
Client
360 View
General
QOS Statistics
ATF Statistics
Mobility History
Call Statistics
Client Properties
AP Properties
Security Information
Client Statistics
QOS Properties
EoGRE
User Defined (Private) Network Drop Unicast
Disabled
Encrypted Traffic Analytics
No
VLAN Override after Webauth
No
VLAN
VLAN1432
Multicast VLAN
0
VRF Name
N/A
Central NAT
DISABLED
11v DMS Capable
No
QoS Map Capable
No
FlexConnect Data Switching
Local
FlexConnect DHCP Status
Local
FlexConnect Authentication
Local
Number of links dropped due to downsizing
0
Last idle time update
Never

CLI:

```
C9800-1#show wireless client mac-address      h.h.h        detail

Client MAC Address : h.h.h
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address :192.0.2.10
Client IPv6 Addresses :
Client Username : test
AP MAC Address :
AP Name: CW9164I-ROW-LAB2
AP slot : 1
Client State : Associated
Policy Profile : FlexAAA
Flex Profile : Flex
Wireless LAN Id: 4
WLAN Profile Name: FlexAAA
Wireless LAN Network Name (SSID): FlexAAA
BSSID :
Connected For : 134 seconds
Protocol : 802.11ac
Channel : 48
Client IIF-ID : 0xa0000001
Association Id : 33
```

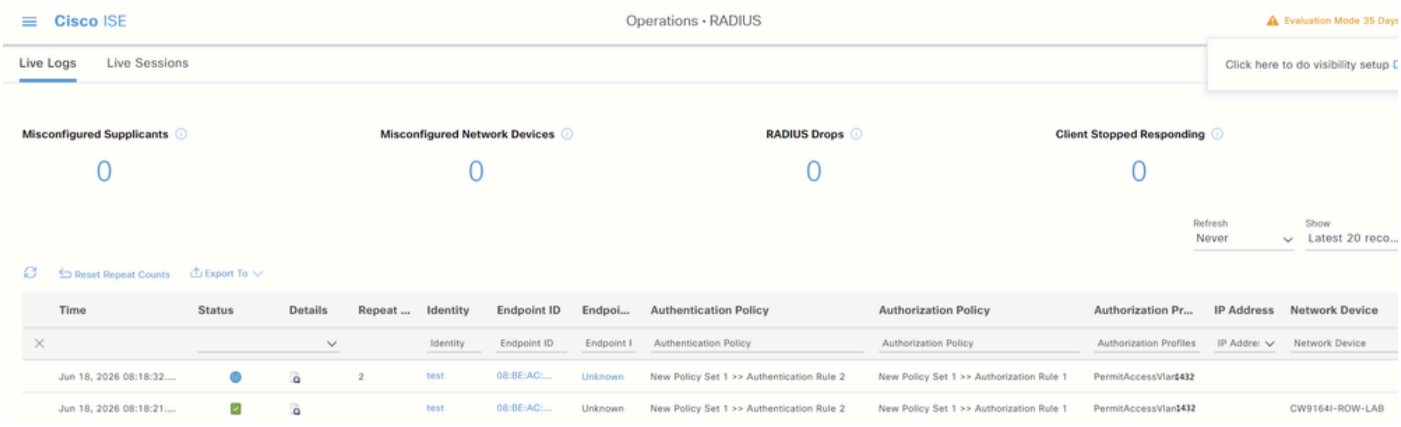
```
QoS Map Capable : No
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Local
Client Statistics:
```

Dalla CLI dell'access point:

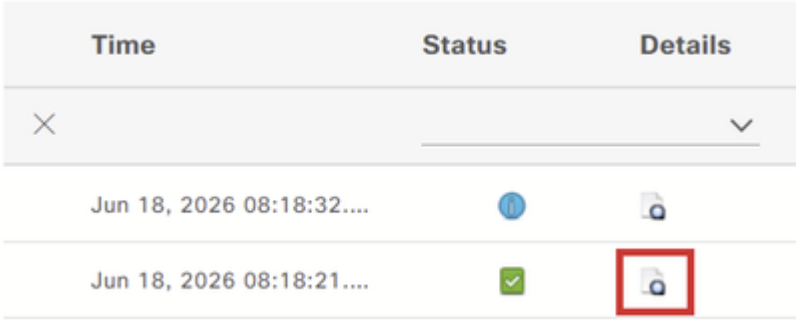
```
CW9164I-ROW-LAB#show dot11 clients

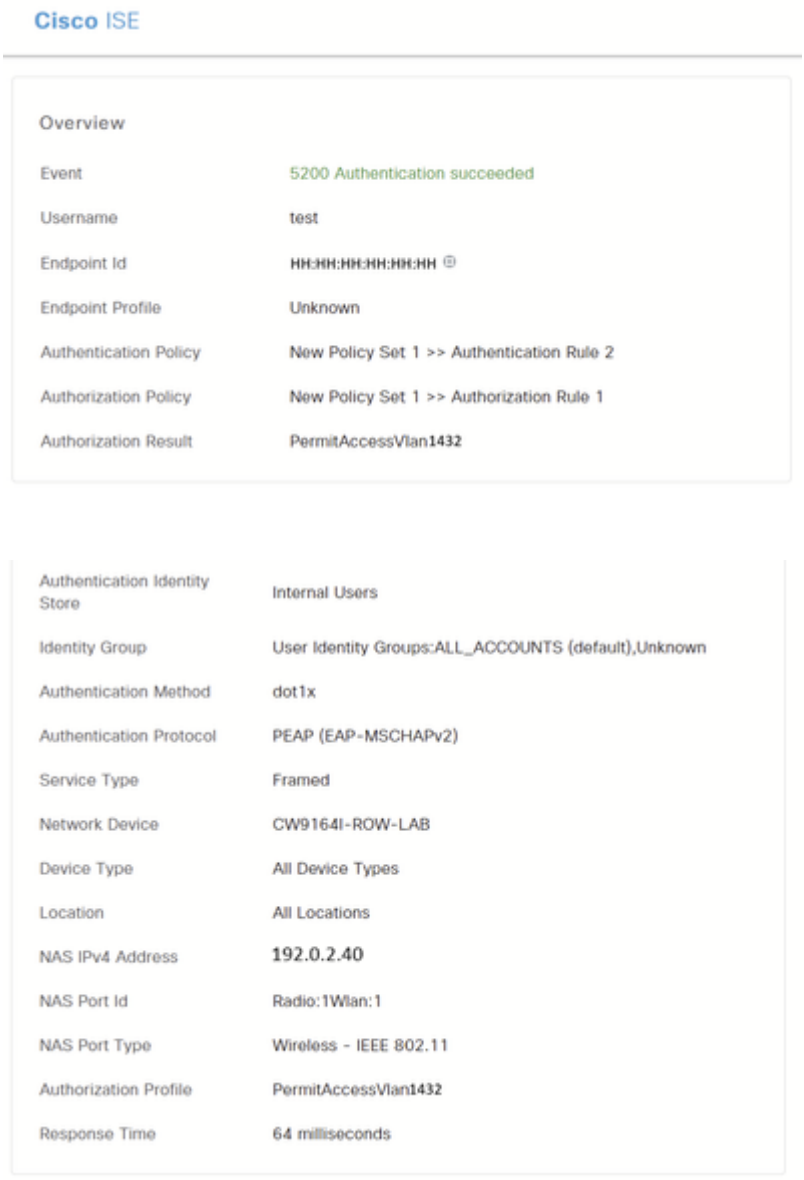
Total dot11 clients: 1
      Client MAC    Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH           1       1  33   FlexAAA  -45 MCS9ISS           No         No
```

ISE

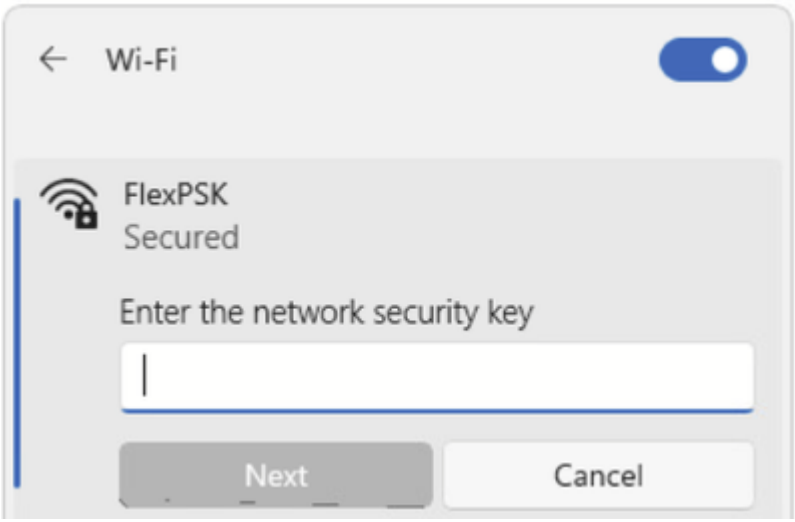


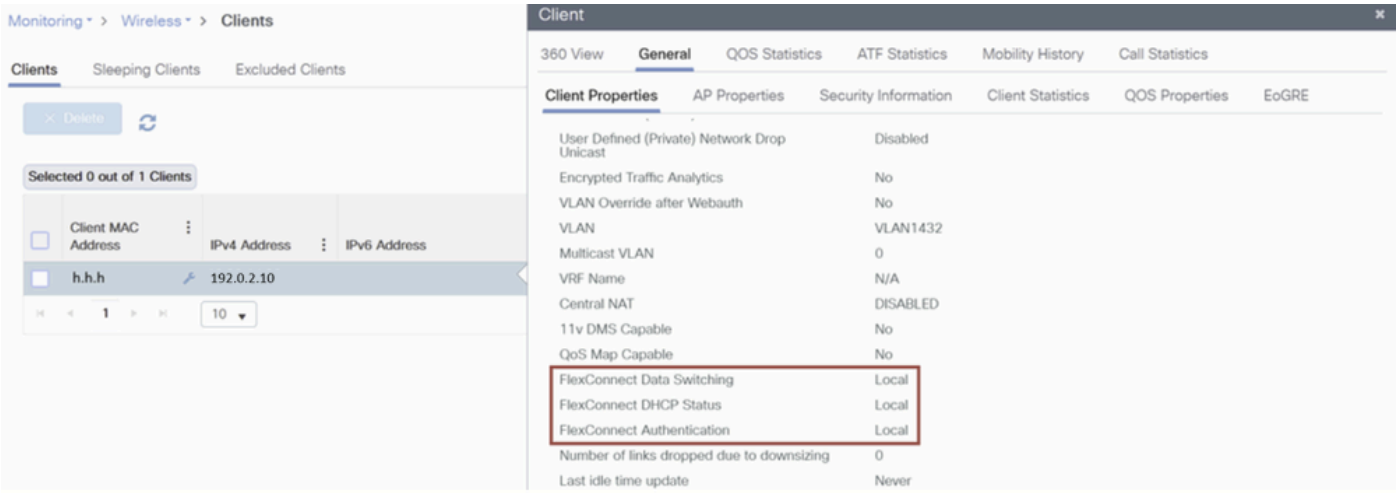
IP Address	Network Device	Device Port	Identity Group	Posture ...	Server
IP Addre:	Network Device	Device Port	Identity Group	Posture Sta	Server
		Radio:1Wlan:1			ISE1
	CW9164I-ROW-LAB	Radio:1Wlan:1	User Identity Groups:ALL_ACCOUNTS (default),Unknown		ISE1


Time
Status
Details
Jun 18, 2026 08:18:32....
Jun 18, 2026 08:18:21....


Cisco ISE
Overview
Event
5200 Authentication succeeded
Username
test
Endpoint Id
HH:HH:HH:HH:HH:HH
Endpoint Profile
Unknown
Authentication Policy
New Policy Set 1 >> Authentication Rule 2
Authorization Policy
New Policy Set 1 >> Authorization Rule 1
Authorization Result
PermitAccessVlan1432
Authentication Identity Store
Internal Users
Identity Group
User Identity Groups:ALL_ACCOUNTS (default),Unknown
Authentication Method
dot1x
Authentication Protocol
PEAP (EAP-MSCHAPv2)
Service Type
Framed
Network Device
CW9164I-ROW-LAB
Device Type
All Device Types
Location
All Locations
NAS IPv4 Address
192.0.2.40
NAS Port Id
Radio:1Wlan:1
NAS Port Type
Wireless - IEEE 802.11
Authorization Profile
PermitAccessVlan1432
Response Time
64 milliseconds

Per PSK WLAN:





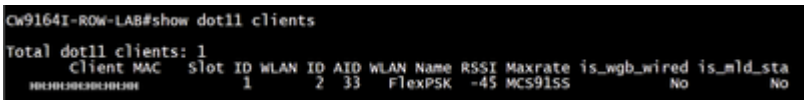
CLI:

```
C9800-1#show wireless client mac-address h.h.h detail

Client MAC Address : h.h.h
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : 192.0.2.10
Client IPv6 Addresses :
Client Username: N/A
AP MAC Address :
AP Name: CW9164I-ROW-LAB2
AP slot : 1
Client State : Associated
Policy Profile : FlexPSK
Flex Profile : Flex
Wireless LAN Id: 5
WLAN Profile Name: FlexPSK
Wireless LAN Network Name (SSID): FlexPSK
BSSID :
Connected For : 116 seconds
Protocol : 802.11ac
Channel : 48
Client IIF-ID : 0xa0000001
Association Id : 33
```

```
QoS Map Capable : No
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Local
Client Statistics:
```

Su CLI AP:



Risoluzione dei problemi

Abilita debug AP e traccia RA con l'indirizzo MAC del client, in sincronia.

Nell'access point abilitare i seguenti debug:

debug evento flexconnect
debug flexconnect pmk
debug flexconnect dot11r
informazioni di gestione client debug dot11
debug dot11 client management critical
errori di gestione client debug dot11
debug dot11 eventi di gestione client

Per WLAN 802.1x:

Registri di debug AP con autenticazione riuscita:

L'access point gestisce il computer di stato 802.11 e la gestione delle chiavi locali.
L'access point elabora l'associazione e prepara il client per l'autenticazione.

```
[*06/19/2026 06:49:00.1836] CLSM[HH:HH:HH:HH:HH:HH]: client moved from UNASSOC to AUTH
[*06/19/2026 06:49:00.1890] wcp/flex_roam_st :: Flexconnect 11r enabled for client HH:HH:HH:HH:HH:HH
[*06/19/2026 06:49:00.1908] CLSM[HH:HH:HH:HH:HH:HH]: client moved from AUTH to ASSOC
[*06/19/2026 06:49:00.1909] Sending ADD MOBILE to client SM for local auth client mac HH:HH:HH:HH:HH:HH
[*06/19/2026 06:49:00.1931] CLSM[HH:HH:HH:HH:HH:HH]: client moved from ASSOC to 8021X
```

L'access point elabora l'autorizzazione, applica l'override VLAN e sposta il client nello stato FWD (Inoltro).

```
[*06/19/2026 06:49:20.3601] received WCP_EVENT_CLIENT_AUTHORIZE (non) roaming case clearing roam flags
[*06/19/2026 06:49:20.3601] CLSM[HH:HH:HH:HH:HH:HH]: WCP_EVENT_CLIENT_AUTHORIZE : Plumbing key info to
[*06/19/2026 06:49:20.3612] wcp/flex_roam_st :: Flexconnect AAA Override Vlan with WLAN mapping: 1432 f
```

```
[*06/19/2026 06:49:20.3625] CLSM[HH:HH:HH:HH:HH:HH]: client moved from 8021X to IPLEARN_PENDING
[*06/19/2026 06:49:20.3627] wcp/flex_roam_st :: Flexconnect Sending HREAP_APAUTH_CLIENT_ADD
[*06/19/2026 06:49:20.3627] CLSM[HH:HH:HH:HH:HH:HH]: Retrieved key for FT+FT_DOT1X algono: 8, vlanId: 1
[*06/19/2026 06:49:20.3627] CLSM[HH:HH:HH:HH:HH:HH]: Local auth (Add) on radio 1 Vap 0 reported to WLC
[*06/19/2026 06:49:20.3701] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*06/19/2026 06:49:20.4313] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr1v0
[*06/19/2026 06:49:20.4317] CLSM[HH:HH:HH:HH:HH:HH]: Local auth on radio 1 Vap 0 IP 192.0.2.10 updatere
[*06/19/2026 06:49:20.4318] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD
```

Registri di traccia RA per la stessa autenticazione riuscita:

La traccia RA registra l'orchestrazione della sessione da parte del WLC. Il WLC convalida l'identità e il criterio del client.
WLC riconosce l'associazione FlexConnect.

```
2026/06/19 06:49:20.934325580 {wncd_x_R0-1}{1}: [client-orch-sm] [18318]: (note): MAC: hhhh.hhhh.hhhh H
2026/06/19 06:49:20.936543415 {wncd_x_R0-1}{1}: [dot1x] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040000
2026/06/19 06:49:20.936579730 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.936600851 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.936654791 {wncd_x_R0-1}{1}: [ewlc-infra-evq] [18318]: (note): Authentication Succes
2026/06/19 06:49:20.936769433 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
```

WLC invia il criterio all'access point.

```
2026/06/19 06:49:20.937447786 {wncd_x_R0-1}{1}: [svm] [18318]: (info): [hhhh.hhhh.hhhh] Applied User Pr
2026/06/19 06:49:20.937451734 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: c
2026/06/19 06:49:20.937452534 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937455590 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: v
2026/06/19 06:49:20.937456177 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: m
2026/06/19 06:49:20.937458436 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: u
2026/06/19 06:49:20.937462127 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile:tu
2026/06/19 06:49:20.937462755 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937463426 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937464035 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
```

Autorizzazione riuscita.

```
2026/06/19 06:49:20.937594042 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.937597878 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
```

Parametri client.
2026/06/19 06:49:20.939394217 {wncd_x_R0-1}{1}: [dot11] [18318]: Nota: MAC: hhhh.hhh.hhh

Parametri voce datapath client - ssid:FlexAAA,slot_id:1 bssid ifid: 0x0, id_radio: 0x90400008, wlan_id: 0xf0400004

WLC apprende l'IP tramite il protocollo DHCP/ARP locale.
2026/06/19 06:49:21.001000218 {wncd_x_R0-1}{1}: [client-iplearn] [18318]: Nota: MAC: hhhh.hhh.hhhh L'IP del client è stato identificato correttamente. Metodo: IP Snooping IP: 192.0.2.10

Il client è completamente connesso.
2026/06/19 06:49:21.002363496 {wncd_x_R0-1}{1}: [errmsg] [18318]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: R0/1: wncd: Voce del nome utente (test) unita al ssid (FlexAAA) per il dispositivo con MAC: hhh.hhh.hhh sul canale (48)
2026/06/19 06:49:21.002795009 {wncd_x_R0-1}{1}: [stato-orch-client] [18318]: Nota: MAC: hhh.hhh.hhh Transizione stato client: S_CO_IP_LEARN_IN_PROGRESS -> ESEGUI_CO

Scenario autonomo

Comportamento durante la perdita della connettività AP-WLC e il successivo ripristino.

L'access point è unito al WLC. Il client esegue correttamente l'autenticazione 802.1X e l'access point passa allo stato FWD (inoltro).

Sui Live Log ISE RADIUS vediamo la sessione del client.

```
[*07/06/2026 20:26:05.8590] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr0v0
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: Local auth on radio 0 Vap 0 IP 192.0.2.10 updatere
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD


CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 No No
```

L'access point non riesce a raggiungere il WLC, esaurisce il numero di ritrasmissioni e passa alla modalità standalone. I client esistenti rimangono connessi localmente.

```
[*07/06/2026 20:28:47.0840] Re-Tx Count=1, Max Re-Tx Value=5, SendSeqNum=33, NumofPendingMsgs=4
[*07/06/2026 20:28:50.0860] Re-Tx Count=2, Max Re-Tx Value=5, SendSeqNum=34, NumofPendingMsgs=5
```

```
[*07/06/2026 20:28:53.0870] Re-Tx Count=3, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:28:56.0990] Re-Tx Count=4, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:28:59.1000] Re-Tx Count=5, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:29:02.1010] Max retransmission count exceeded, going back to DISCOVER mode.
[*07/06/2026 20:29:02.1020] Flexconnect Switching to Standalone Mode!
[*07/06/2026 20:29:02.2170] CAPWAP State: DTLS Teardown
```

Ma il client è ancora connesso:

CW9164I-ROW-LAB2#show dot11 client

Totale client dot11: 1
ID slot MAC client ID WLAN ID ID ID WLAN Nome WLAN RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 No No

Quando il client esegue il roaming a un altro punto di accesso in modalità standalone, l'handshake EAP ha esito negativo a causa dell'impossibilità di raggiungere il server RADIUS. Il client non è autorizzato e viene rimosso dall'access point.

```
[*07/06/2026 20:34:44.7240] CLSM[HH:HH:HH:HH:HH:HH]: Session timeout
[*07/06/2026 20:36:15.2670] hostapd:apr0v0: CTRL-EVENT-EAP-RETRANSMIT hh:hh:hh:hh:hh:hh
[*07/06/2026 20:36:15.2670] hostapd:apr0v0: CTRL-EVENT-EAP-TIMEOUT-FAILURE hh:hh:hh:hh:hh:hh
[*07/06/2026 20:36:15.2680] wcp/flex_roam_st :: Flexconnect hapdev: Received UNAUTHORIZE for hh:hh:hh:h
[*07/06/2026 20:36:15.2680] wcp/flex_roam_st :: Flexconnect hapdev: recv'd UNAUTH with DISCONNECT REQUE
[*07/06/2026 20:36:15.2680] CLSM[HH:HH:HH:HH:HH:HH]: Client delete initiated with timeout of 10 seconds
[*07/06/2026 20:36:15.2770] CLSM[HH:HH:HH:HH:HH:HH]: Remove success from ClientIPTable on apr0v0
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: Not sending DELETE to cont, reason CLIENT_DEL_EAP_
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: Deauthorize succeeded to radio intf apr0v0
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: client moved from FWD to DELETE_PENDING
[*07/06/2026 20:36:15.2880] CLSM[HH:HH:HH:HH:HH:HH]: Send Deauth with reason 2 force 1 - Radio 0 Vap 0
[*07/06/2026 20:36:25.0830] CLSM[HH:HH:HH:HH:HH:HH]: Delete timeout
[*07/06/2026 20:36:25.0830] CLSM[HH:HH:HH:HH:HH:HH]: Delete client reassoc 0 succeeded to radio intf ap
```

AP invia la sessione client al server RADIUS di backup.

L'access point riacquista la connettività al WLC. L'access point torna alla modalità connessa e sincronizza le informazioni sulla sessione client locale con il WLC.

La sessione client esegue la transizione tra i nodi ISE primario e di backup in base allo stato di connettività dell'access point.

L'access point e il client risultano connessi sul WLC e il client non ha rilevato alcuna disconnessione o flap quando la connettività tra l'access point e il WLC non è attiva.

```
CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 0


Upon roaming back, the client undergoes local authentication. The AP processes the association and move

[*07/06/2026 20:48:49.2830] CLSM[HH:HH:HH:HH:HH:HH]: US Auth(b0) seq 2653 IF 23 slot 0 vap 0 len 30 sta
[*07/06/2026 20:48:49.2840] CLSM[HH:HH:HH:HH:HH:HH]: DS Auth len 30 slot 0 vap 0
[*07/06/2026 20:48:49.2850] CLSM[HH:HH:HH:HH:HH:HH]: Driver send mgmt frame success Radio 0 Vap 0
[*07/06/2026 20:48:49.2850] CLSM[HH:HH:HH:HH:HH:HH]: client moved from UNASSOC to AUTH
[*07/06/2026 20:48:49.2920] CLSM[HH:HH:HH:HH:HH:HH]: US Reassoc Req(20) seq 2654 IF 23 slot 0 vap 0 len
[*07/06/2026 20:48:49.2930] CLSM[HH:HH:HH:HH:HH:HH]: AUTH TYPE RSNIE DOT1X
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: Populate client capability: cap_from_click=true, ma
[*07/06/2026 20:48:49.2940] Flexconnect local_auth 1 local_assoc 1 frame subtype 32
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: radio id: 0, vap id: 0, max clients for this wlan:
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: radio state: 1, client state: 1, max_client_per_ra
[*07/06/2026 20:48:49.2940] Adding RM Capable IE - Len = 5, RRM[0] = 73, RRM[1] = c0
[*07/06/2026 20:48:49.2940] DS [re]Assoc 1 req_len=201 resp_len=146 11r_len=0 cckm 0 qos_flag 1 status
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: DS Reassoc Resp(30) IF 0 slot 0 vap 0 state AUTH,
[*07/06/2026 20:48:49.2950] CLSM[HH:HH:HH:HH:HH:HH]: Driver send mgmt frame success Radio 0 Vap 0
[*07/06/2026 20:48:49.2950] CLSM[HH:HH:HH:HH:HH:HH]: client moved from AUTH to ASSOC
[*07/06/2026 20:48:49.2950] Sending ADD MOBILE to client SM for local auth client mac HH:HH:HH:HH:HH:HH
[*07/06/2026 20:48:49.2960] wcp/flex_roam_st :: Flexconnect Sending ADD_MOBILE_PAYLOAD (v4-client-acl-na
[*07/06/2026 20:48:49.2960] wcp/flex_roam_st :: Flexconnect encode_and_send_add_mobile_to_dott11_client_
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: ADD_MOBILE AID 1
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: Driver Add Client success AID 1 Radio 0 Vap 0 Enc
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: Added to ClientIPTable on apr0v0
[*07/06/2026 20:48:49.2970] CLSM[HH:HH:HH:HH:HH:HH]: client moved from ASSOC to 8021X
[*07/06/2026 20:48:49.2970] CLSM[HH:HH:HH:HH:HH:HH]: Added to WCP client table AID 1 Radio 0 Vap 0 Enc
[*07/06/2026 20:48:49.2980] wcp/flex_roam_st :: Flexconnect hapdev: client WCP_EVENT_CLIENT_ASSOC/REASSO
[*07/06/2026 20:48:49.6360] received WCP_EVENT_CLIENT_AUTHORIZE (non) roaming case clearing roam flags
[*07/06/2026 20:48:49.6360] wcp/flex_roam_st :: Flexconnect (AUTHORIZE) received PTK thru wcp_event
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect HH:HH:HH:HH:HH:HH client ACL , Qos Profile:
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect AAA Override Vlan with WLAN mapping: 1432 fo
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect Sending ADD_MOBILE_PAYLOAD (v4-client-acl-na
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect encode_and_send_add_mobile_to_dott11_client_
[*07/06/2026 20:48:49.6370] CLSM[HH:HH:HH:HH:HH:HH]: ADD_MOBILE AID 1
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: check vlan override vlan 1432
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: Client ADD Encrypt Key success AID 1 Radio 0 Enc 4
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: client moved from 8021X to IPLEARN_PENDING
[*07/06/2026 20:48:49.6390] wcp/flex_roam_st :: Flexconnect Sending HREAP_APAUTH_CLIENT_ADD
[*07/06/2026 20:48:49.6900] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr0v0
[*07/06/2026 20:48:49.6910] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD


CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -39 M7 No No

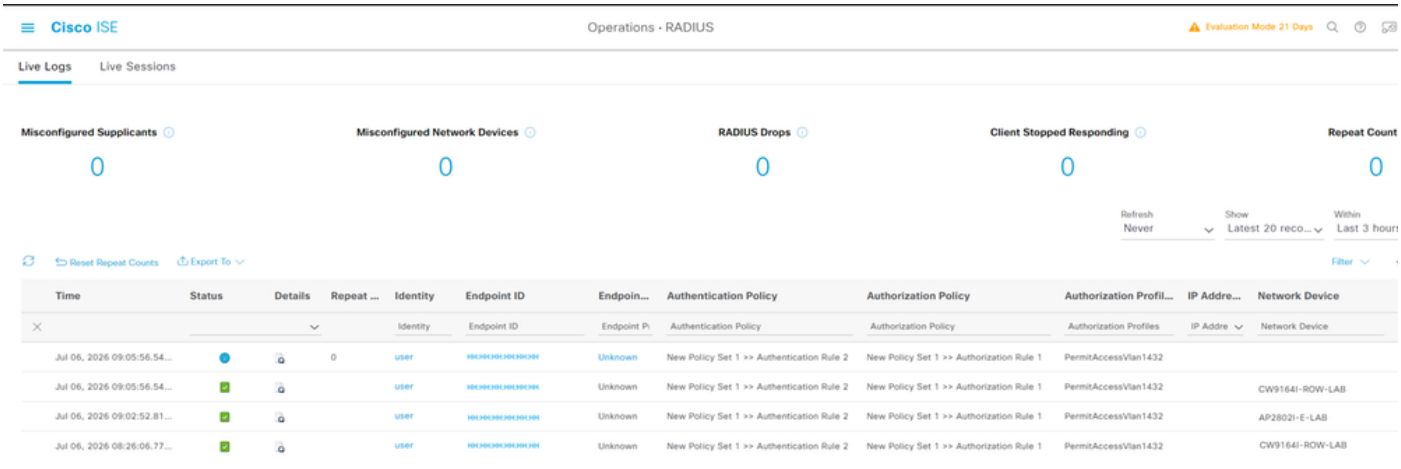



*07/06/2026 20:59:57.7690] Discovery Response from 192.0.2.20
[*07/06/2026 21:00:08.0080] CAPWAP State: DTLS Setup
[*07/06/2026 21:00:08.4820] CAPWAP State: Join
[*07/06/2026 21:00:09.3740] Sending Join request to 192.0.2.20 through port 5253, packet size 1376
[*07/06/2026 21:00:09.3780] Join Response from 192.0.2.20, packet size 1397
[*07/06/2026 21:00:09.4040] CAPWAP State: Image Data
```

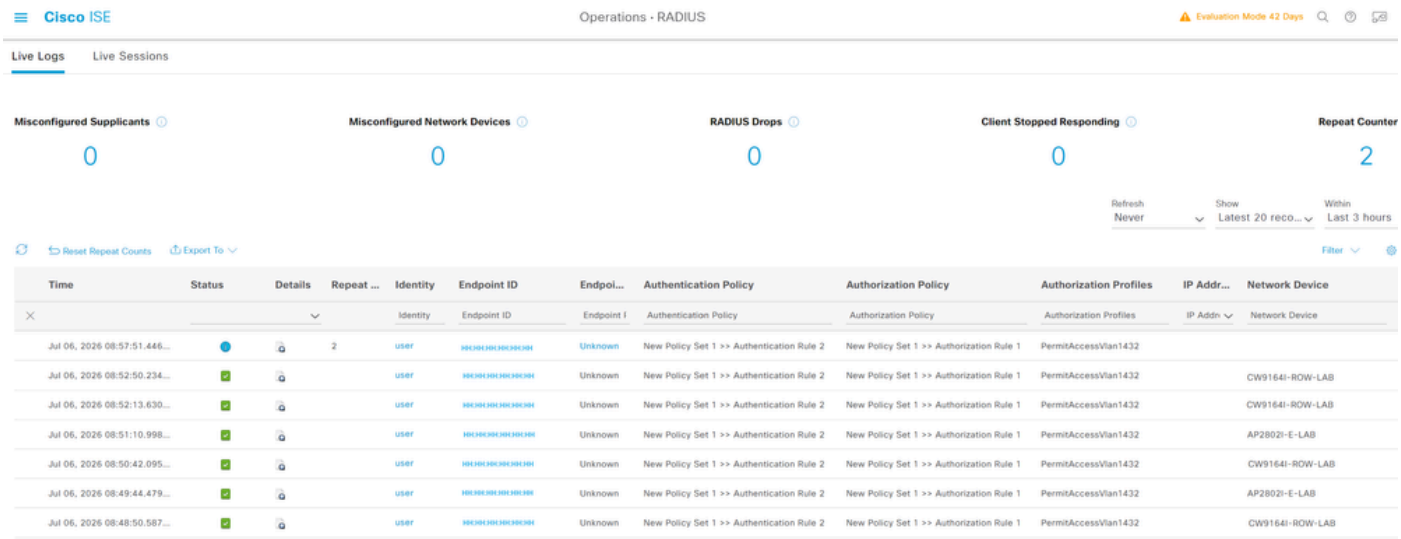
```
[*07/06/2026 21:00:09.5020] CAPWAP State: Configure
[*07/06/2026 21:00:12.5510] CAPWAP State: Run
[*07/06/2026 21:00:12.6480] AP has joined controller C9800-1
[*07/06/2026 21:00:12.6490] Flexconnect Switching to Connected Mode!
[*07/06/2026 21:00:12.6520] CLSM[HH:HH:HH:HH:HH:HH]: AP_REAP_CLIENT_INFO_PAYLOAD Client MAC HH:HH:HH:HH
[*07/06/2026 21:00:12.6520] AssocTimeAtAP 1783371169 clientBitmap=0x13
[*07/06/2026 21:00:12.6520] CLSM[00:00:00:00:00:00]: Numbers of Local Switching clients to report : 1
[*07/06/2026 21:00:14.8270] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 21:00:14.8270] chatter: bssid BB:BB:BB:BB:BB:BB, life_time 1783371774, created_at 17833716
[*07/06/2026 21:00:14.8280] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 21:00:14.8280] chatter: bssid BB:BB:BB:BB:BB:BB, life_time 1783371774, created_at 17833716
```

```
CW9164I-ROW-LAB2# show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 No No
```



ISE principale: Registra la sessione iniziale (08:26:06) e la sessione ripresa dopo il ripristino della connettività WLC (09:02:52).



Backup ISE: Acquisisce l'attività della sessione (08:48:50 - 08:57:51) mentre l'access point funzionava in modalità standalone.

La prima sessione è stata alle 08:26:06, dopo che l'access point ha perso la connettività al WLC e si è spostato in modalità standalone.

La sessione 09:02:52 è la prima sessione dopo che l'AP ha ristabilito la connettività con il WLC.

Informazioni correlate

- CCNP Enterprise Wireless Design ENWLSD 300-425 e Implementation ENWLSI 300-430 - Guida ufficiale ai certificati, seconda edizione
- Guida alla configurazione del software Cisco Catalyst serie 9800 Wireless Controller, Cisco IOS XE 17.8.x - Capitolo: FlexConnect
- Note sulla versione di Cisco Catalyst serie 9800 Wireless Controller, Cisco IOS XE Cupertino release 17.8.x
- Matrice di funzionalità per i Cisco Wireless Access Point
- Supporto tecnico Cisco e download

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).