# Configurazione della postura sui switch Catalyst 9800 WLC e ISE

## Sommario



## Introduzione

Questo documento descrive come configurare una WLAN di postura su un Catalyst 9800 WLC e ISE tramite l'interfaccia grafica utente (GUI).

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- 9800 WLC - configurazione generale
- Configurazione di profili e policy ISE

### Componenti usati

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

- 9800 WLC Cisco IOS® XE Cupertino v17.9.5
- Identity Service Engine (ISE) v3.2
- Notebook per Windows 10 Enterprise

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

Flusso delle funzionalità RADIUS NAC e CoA del controller LAN wireless

1. Il client esegue l'autenticazione con dot1x.

2. L'accettazione dell'accesso RADIUS porta l'URL reindirizzato per la porta 80 e gli ACL di pre-autenticazione, che includono la possibilità di usare indirizzi IP e porte o di mettere in quarantena le VLAN.

3. Il client viene reindirizzato all'URL fornito in access accept (Accetta accesso) e messo in un nuovo stato fino a quando non viene eseguita la convalida della postura. In questo stato, il client comunica con il server ISE e si convalida rispetto alle policy configurate sul server ISE NAC.

4. L'agente NAC sul client avvia la convalida della postura (traffico verso la porta 80): L'agente invia una richiesta di individuazione HTTP alla porta 80, che il controller reindirizza all'URL specificato in Accetta. L'ISE sa che il cliente cerca di raggiungere il cliente e risponde direttamente a quest'ultimo. In questo modo il client viene a conoscenza dell'IP del server ISE e da ora in poi comunica direttamente con il server ISE.

5. Il WLC consente questo traffico perché l'ACL è configurato per consentire questo traffico. In caso di override della VLAN, il traffico viene bloccato in modo che raggiunga il server ISE.

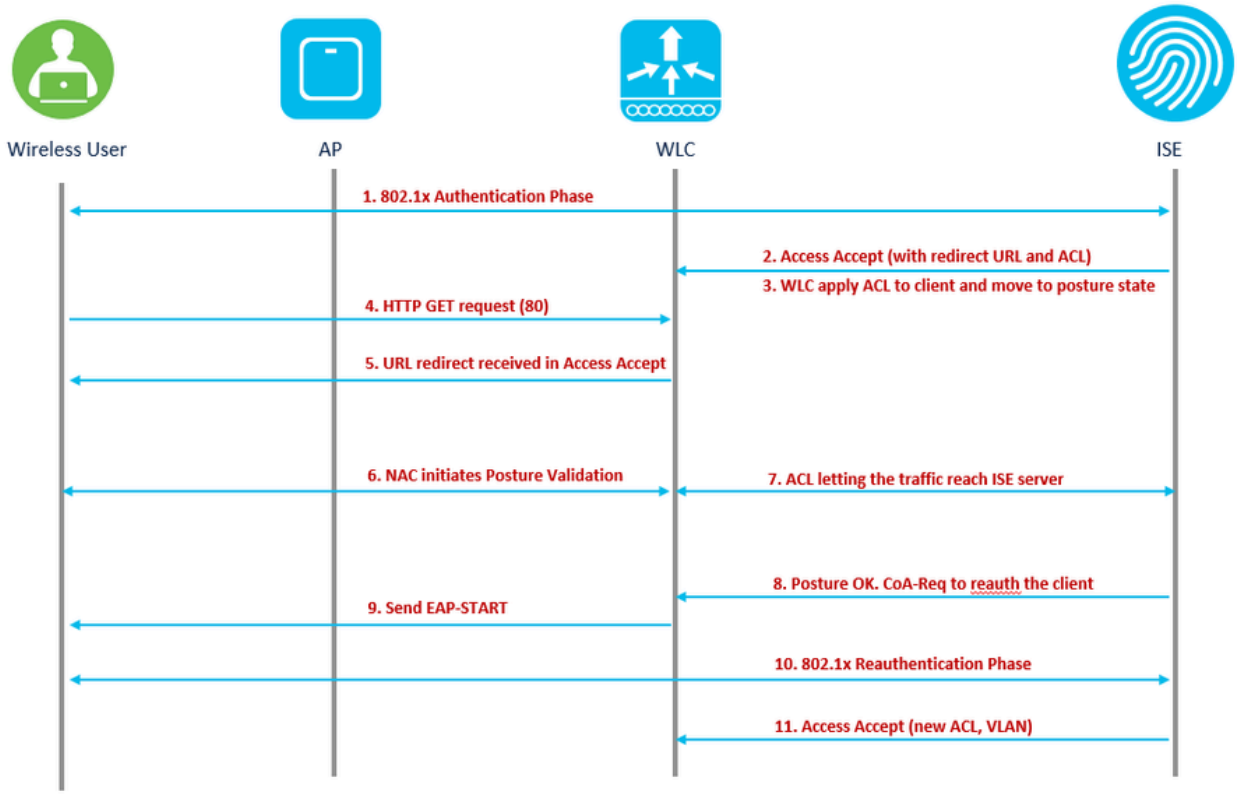
6. Una volta che ISE-client ha completato la valutazione, un CoA-Req RADIUS con servizio di riautenticazione viene inviato al WLC. In questo modo viene avviata la riautenticazione del client (inviando EAP-START). Se la riautenticazione ha esito positivo, ISE invia un messaggio di accettazione dell'accesso con un nuovo ACL (se presente) e senza reindirizzamento dell'URL o accesso alla VLAN.

7. Il WLC supporta CoA-Req e Disconnect-Req in base alla RFC 3576. Il WLC deve supportare CoA-Req per il servizio di riautenticazione, come da RFC 5176.

8. Anziché ACL scaricabili, sul WLC vengono utilizzati ACL preconfigurati. Il server ISE invia semplicemente il nome ACL, già configurato nel controller.

9. Questa progettazione è valida sia per le VLAN che per gli ACL. In caso di override della VLAN, è sufficiente reindirizzare la porta 80 per consentire al resto del traffico sulla VLAN di quarantena. Per l'ACL, viene applicato l'ACL di preautenticazione ricevuto in accettazione dell'accesso.

La figura seguente fornisce una rappresentazione visiva di questo flusso di funzionalità:



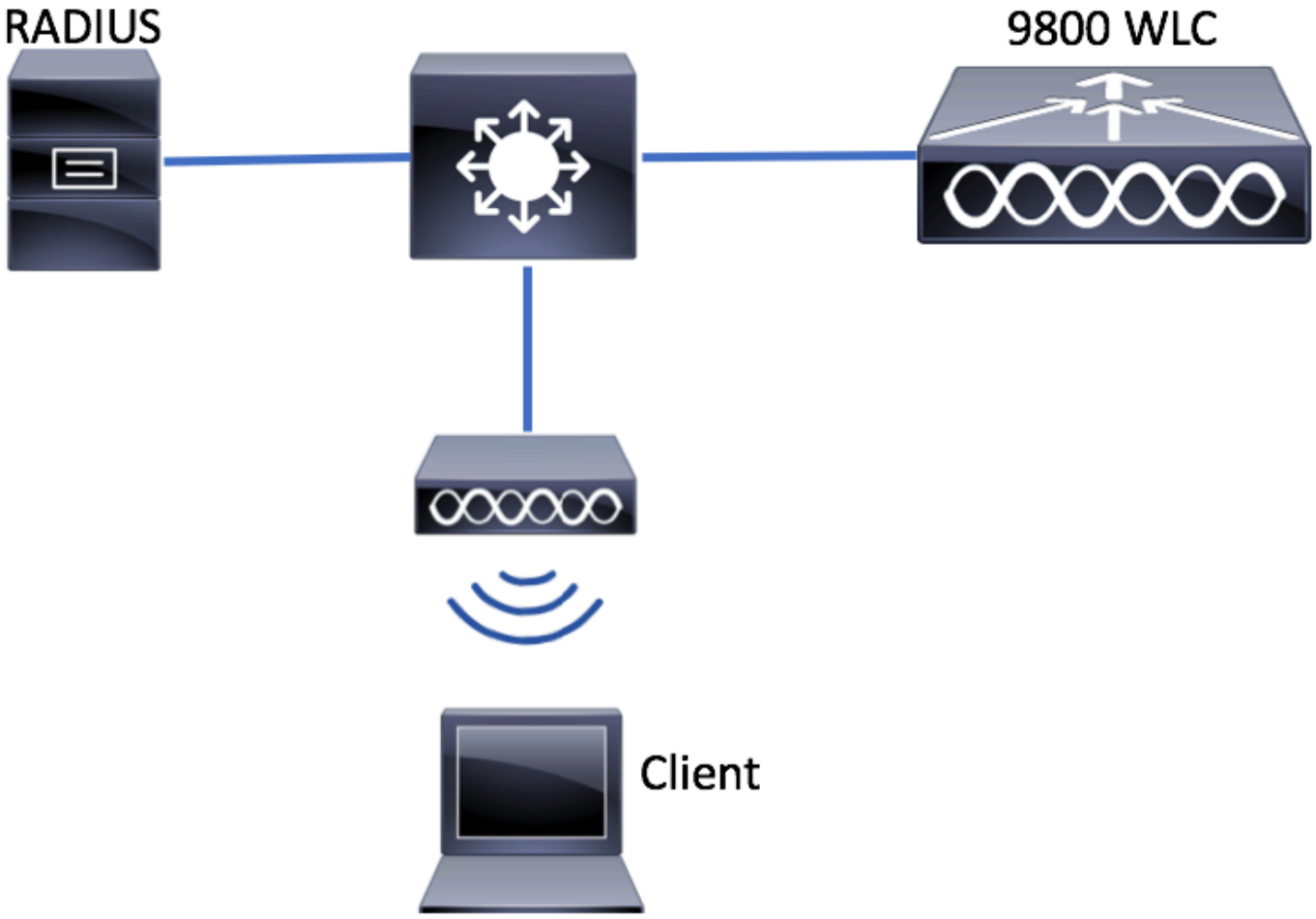

flusso di lavoro delle funzionalità

In questo caso, un SSID utilizzato solo per gli utenti aziendali è abilitato per la postura. In questo SSID non sono presenti altri scenari di utilizzo, ad esempio BYOD, Guest o altri.

Quando un client wireless si connette a Posture SSID per la prima volta, deve scaricare e installare il modulo Posture sul portale reindirizzato dell'ISE e infine deve essere applicato con gli ACL pertinenti in base al risultato della verifica della postura (conforme/non conforme).

# Configurazione

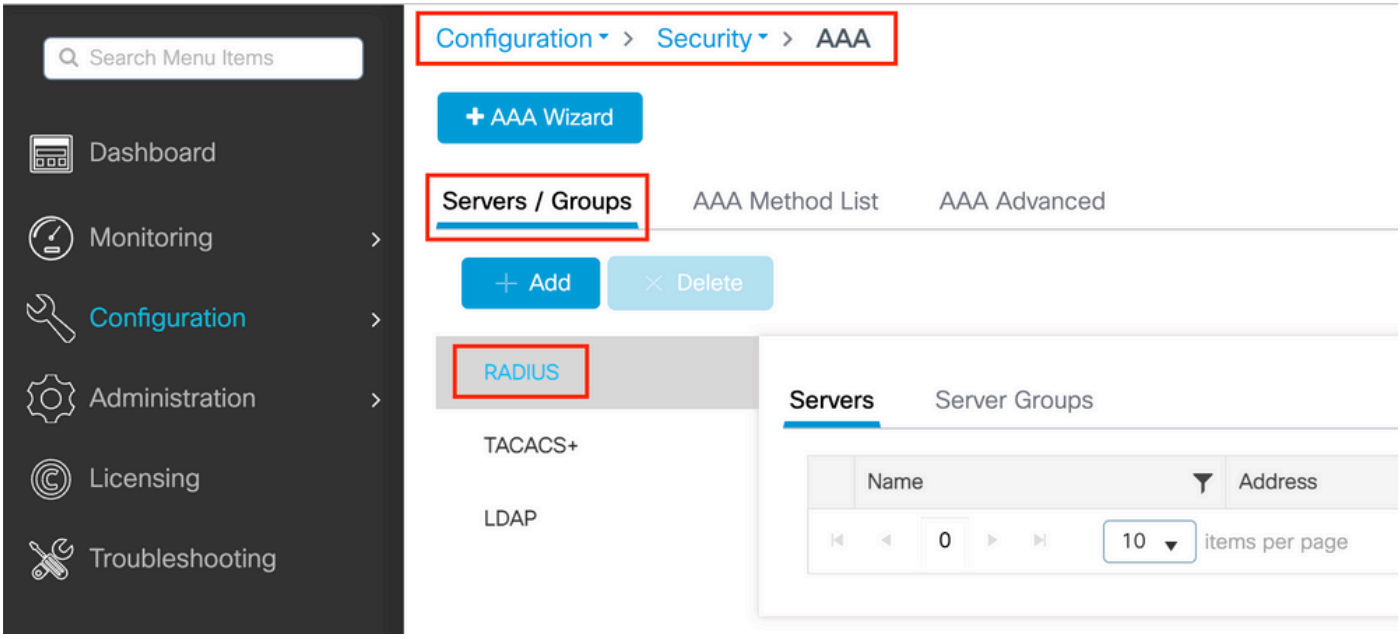
## Esempio di rete



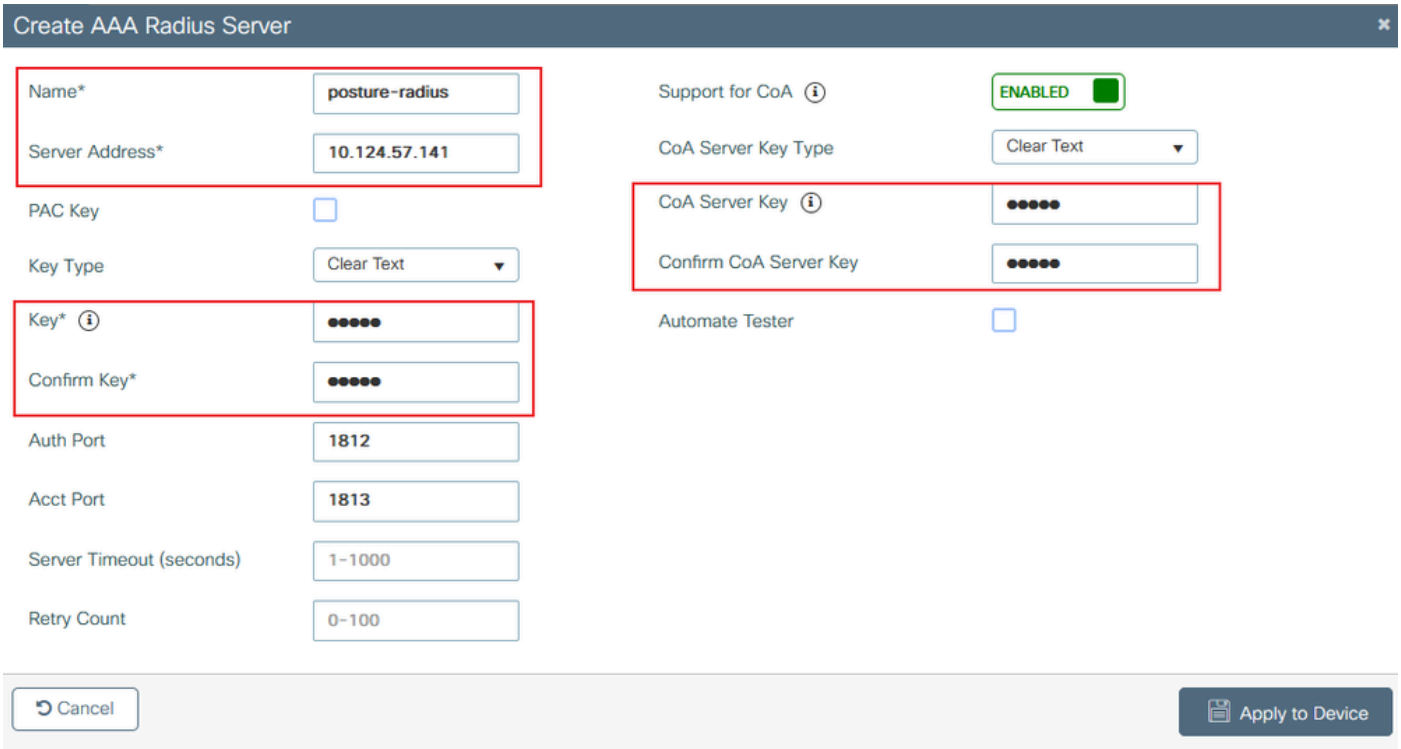

Esempio di rete

## Configurazione AAA sui controller 9800 WLC

Passaggio 1. Aggiungere il server ISE alla configurazione WLC 9800. Passare a Configurazione > Sicurezza > AAA > Server/Gruppi > RADIUS > Server > + Aggiungi e immettere le informazioni sul server RADIUS come mostrato nelle immagini. Assicurarsi che il supporto per CoA sia abilitato per la postura NAC.

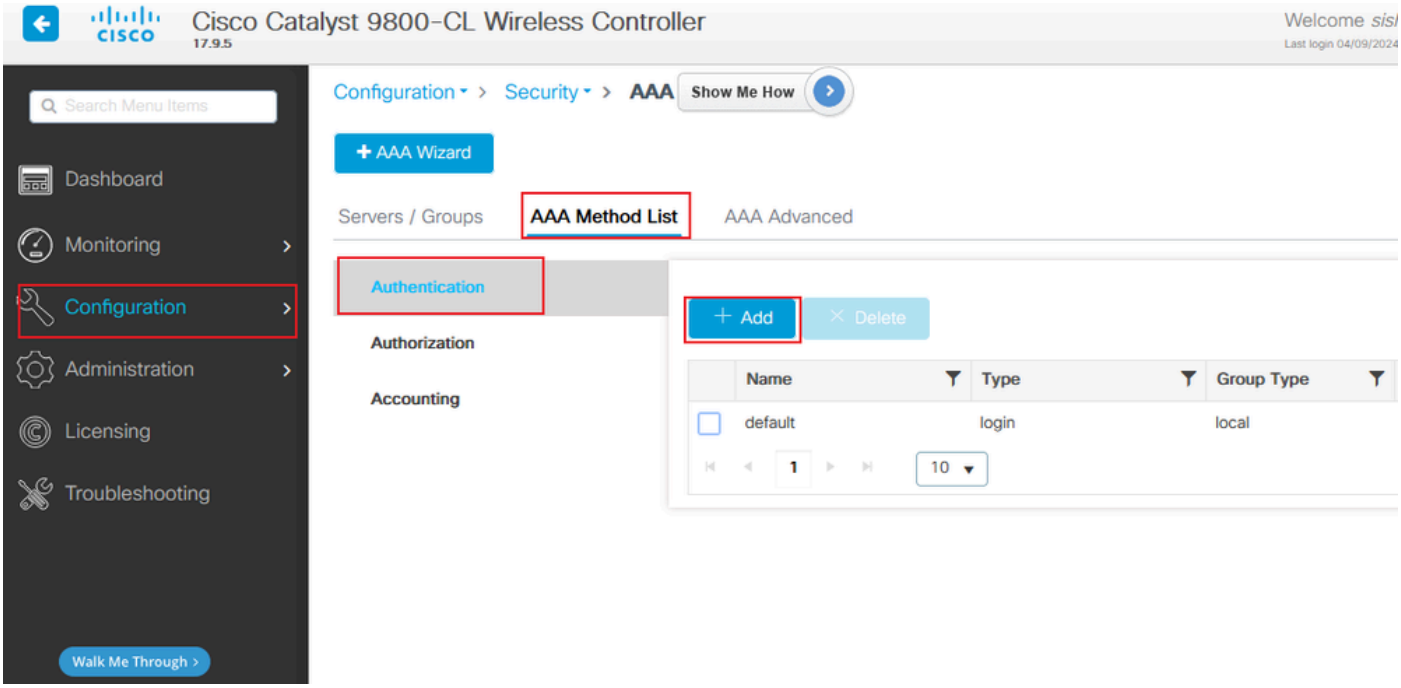



9800 create radius server

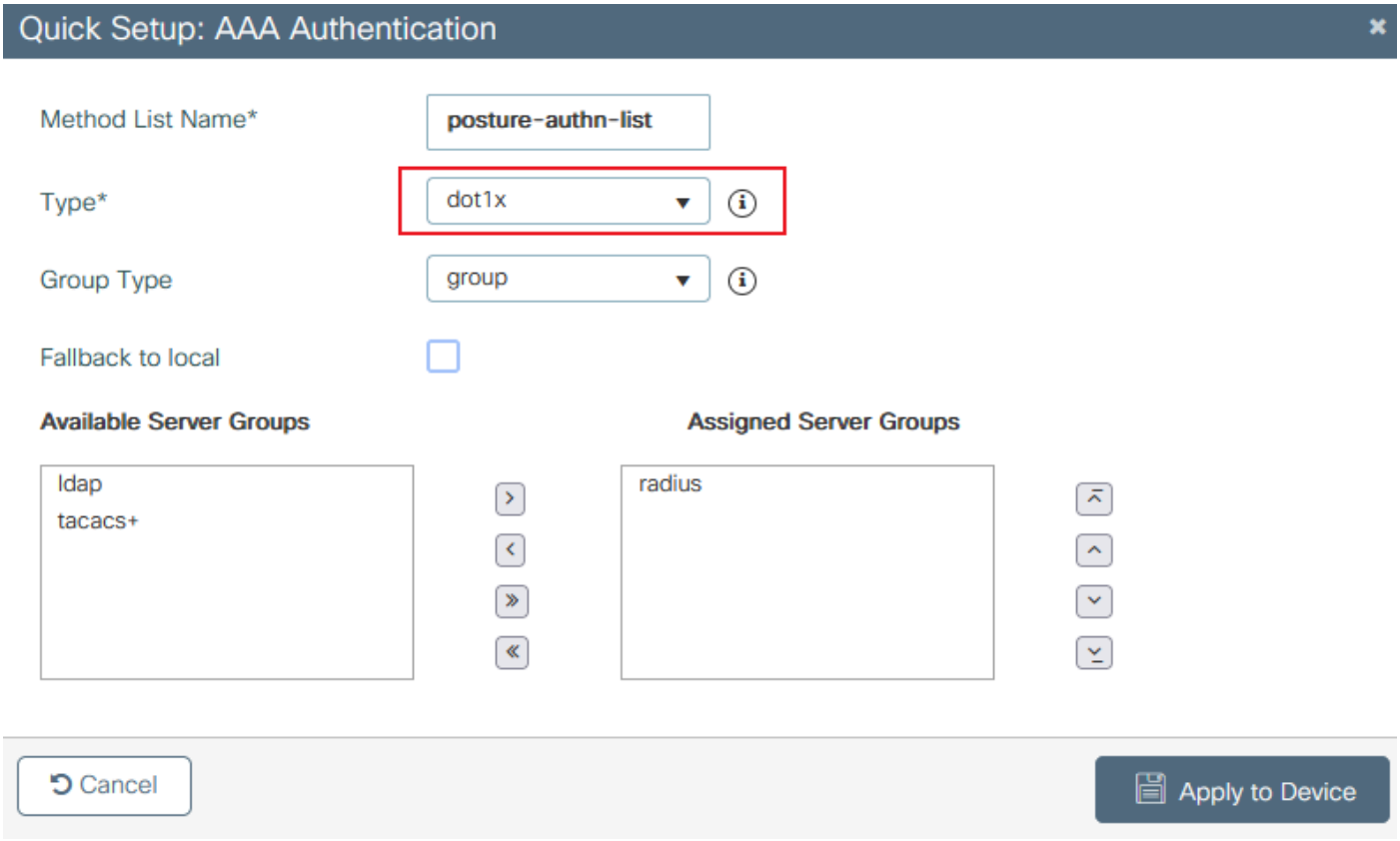



9800 - crea dettagli raggio

Passaggio 2. Creare un elenco di metodi di autenticazione. Passare a Configurazione > Sicurezza > AAA > Elenco metodi AAA > Autenticazione > + Aggiungi come mostrato nell'immagine:

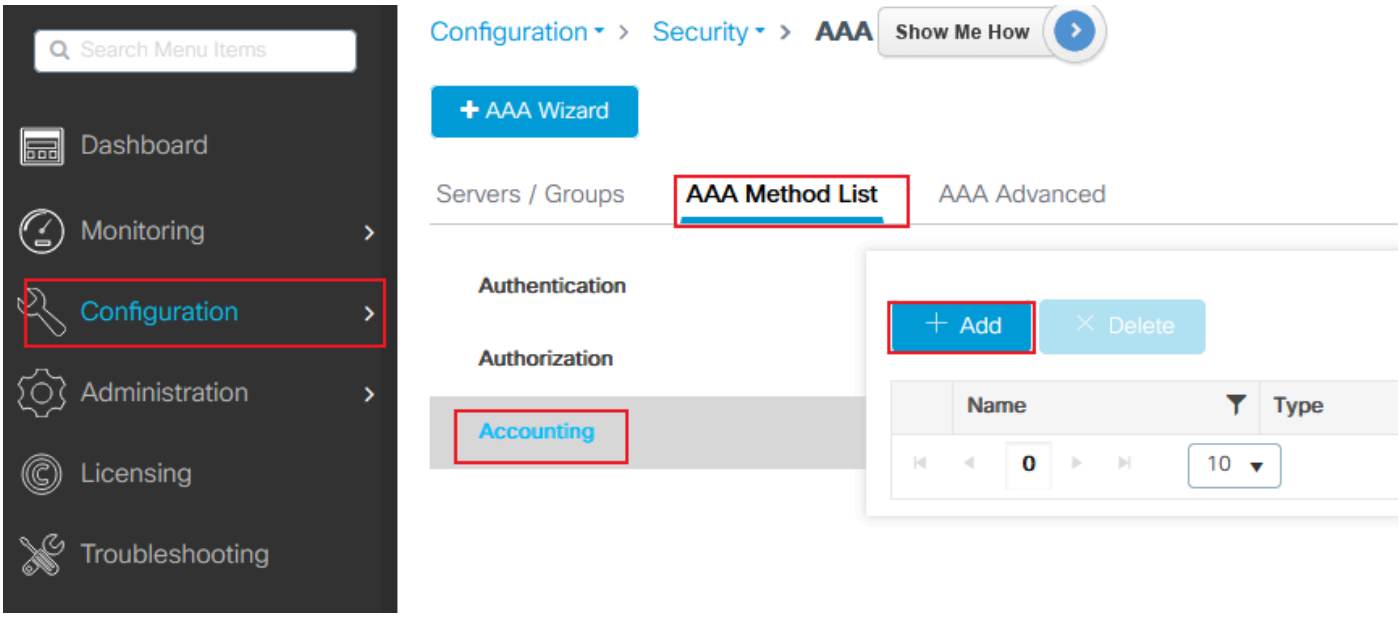



9800 add auth list

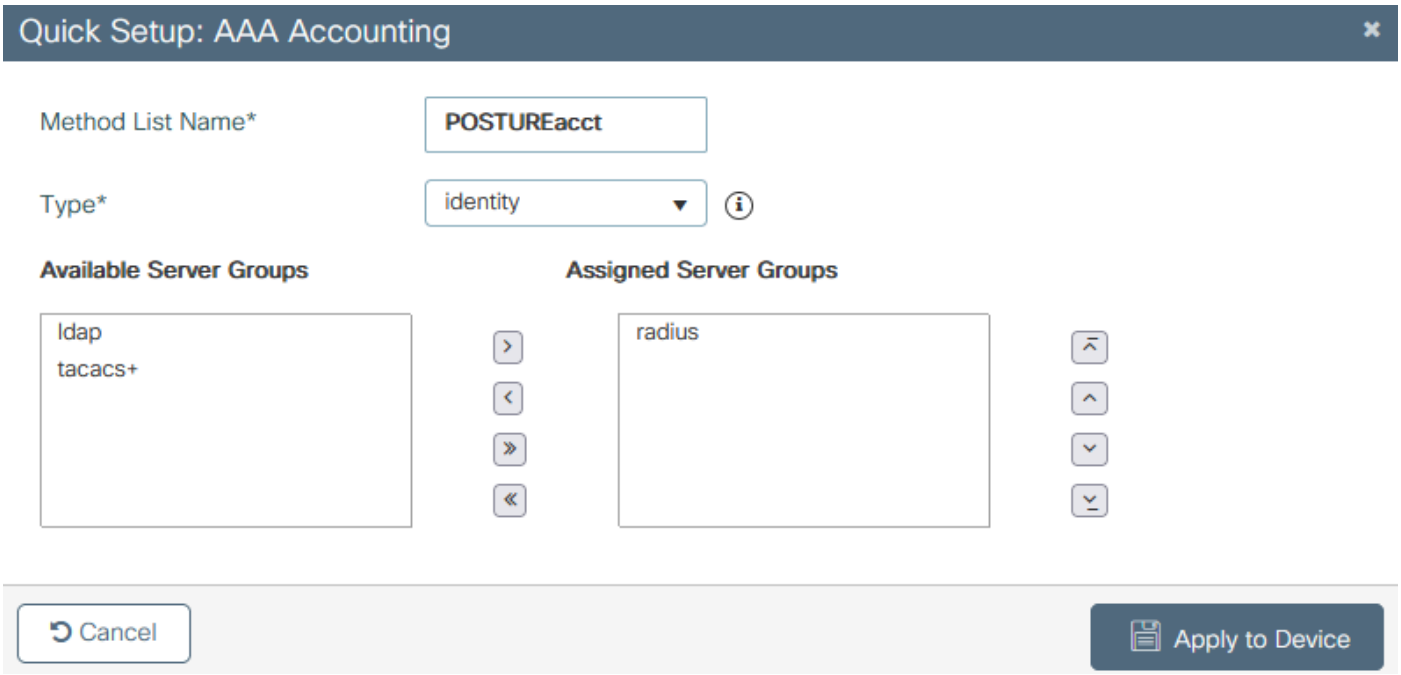



9800 - crea dettagli elenco di autenticazione

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



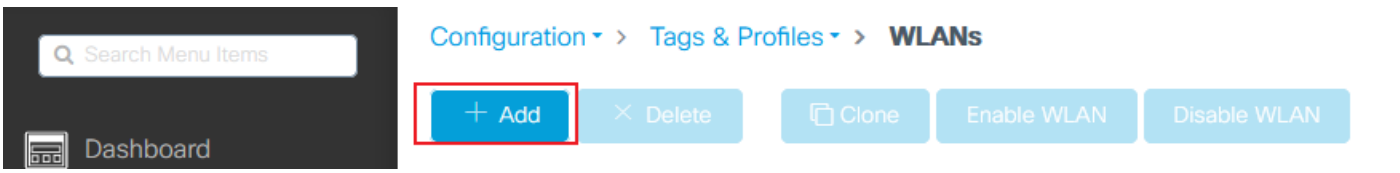

9800 aggiungi elenco account




9800 - crea dettagli elenco acct

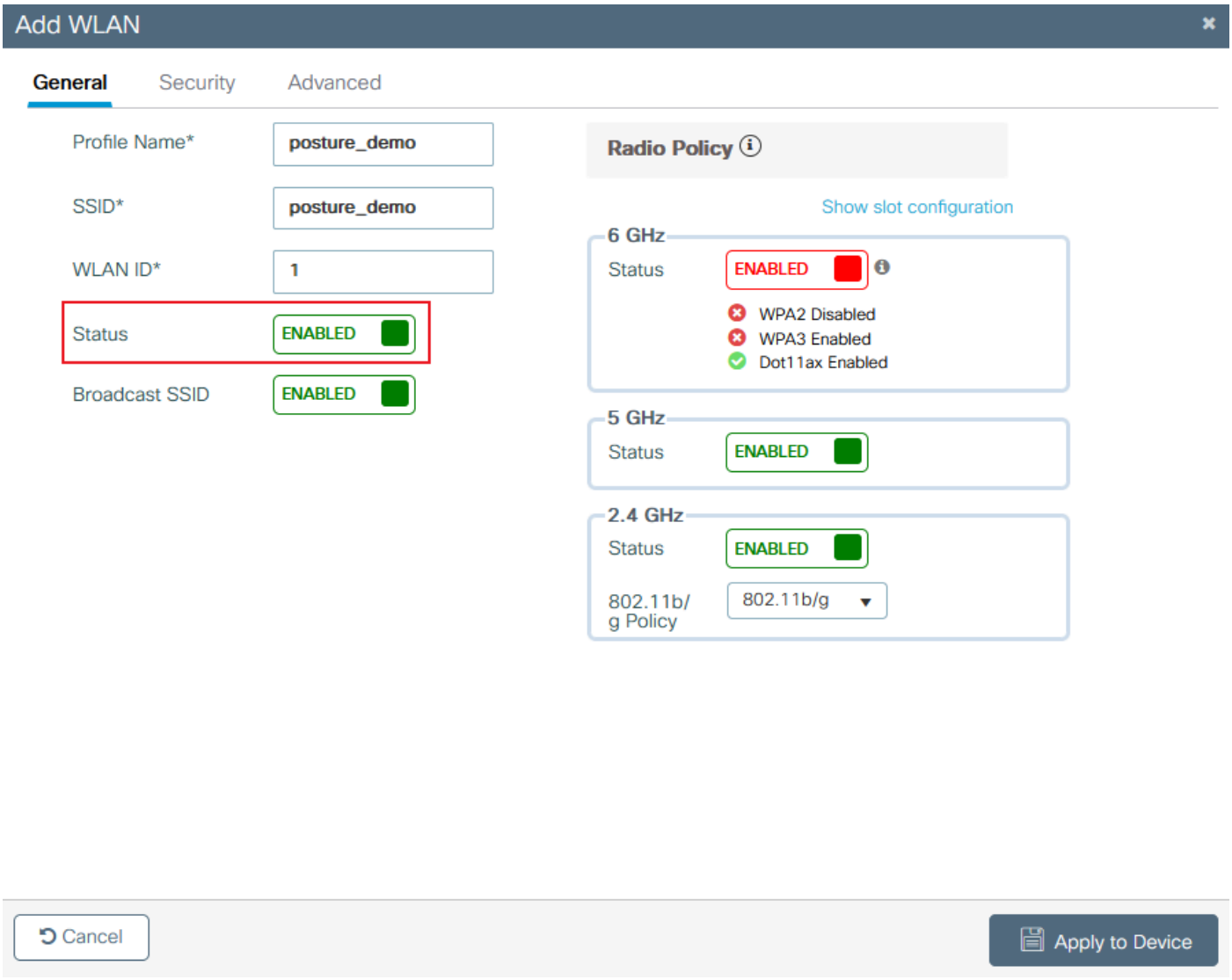
## Configurazione della WLAN

Passaggio 1. Creare la WLAN. Selezionare Configurazione > Tag e profili > WLAN > + Aggiungi e configura la rete come necessario:



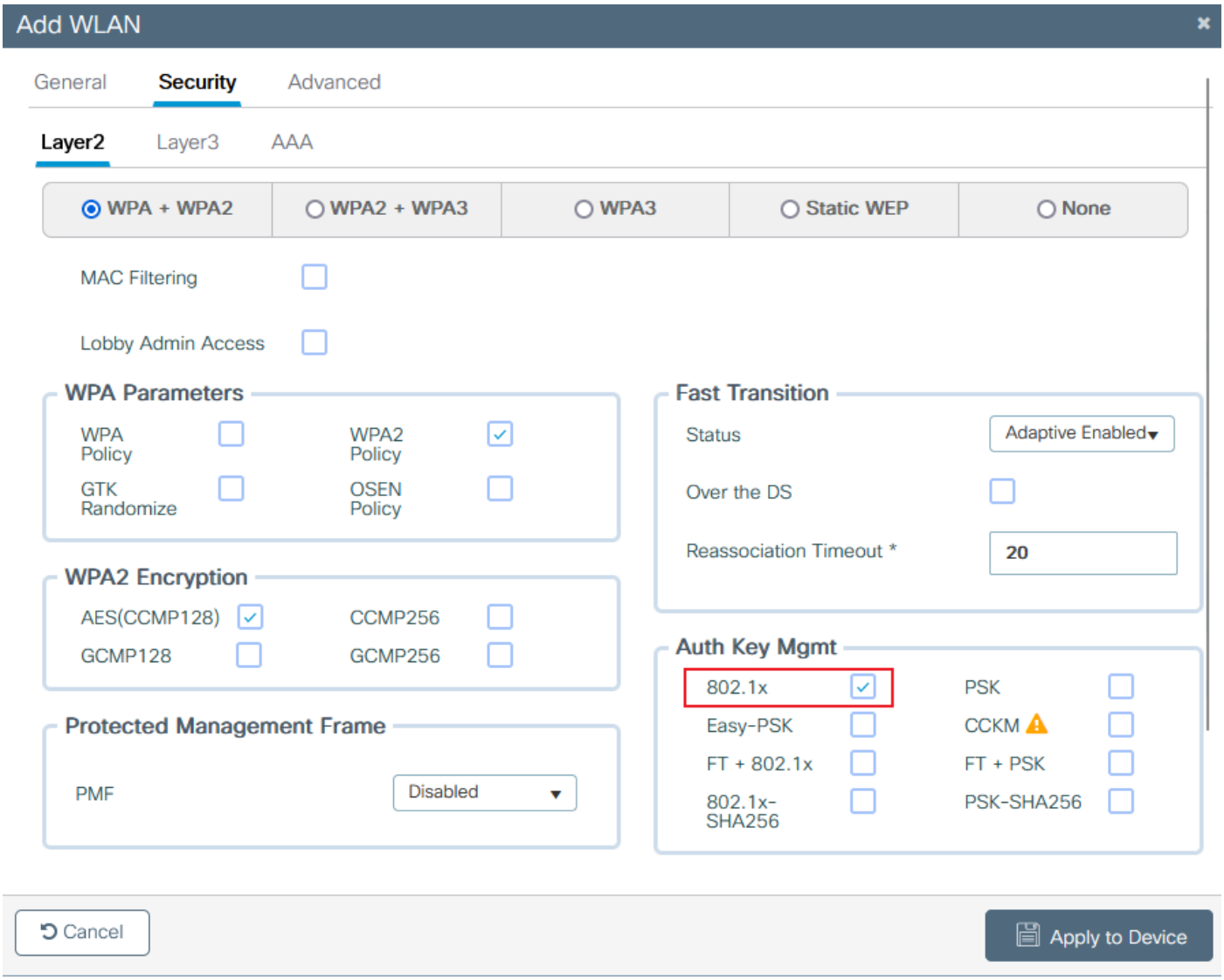

9800 WLAN add

Passaggio 2. Inserire le informazioni generali sulla WLAN.

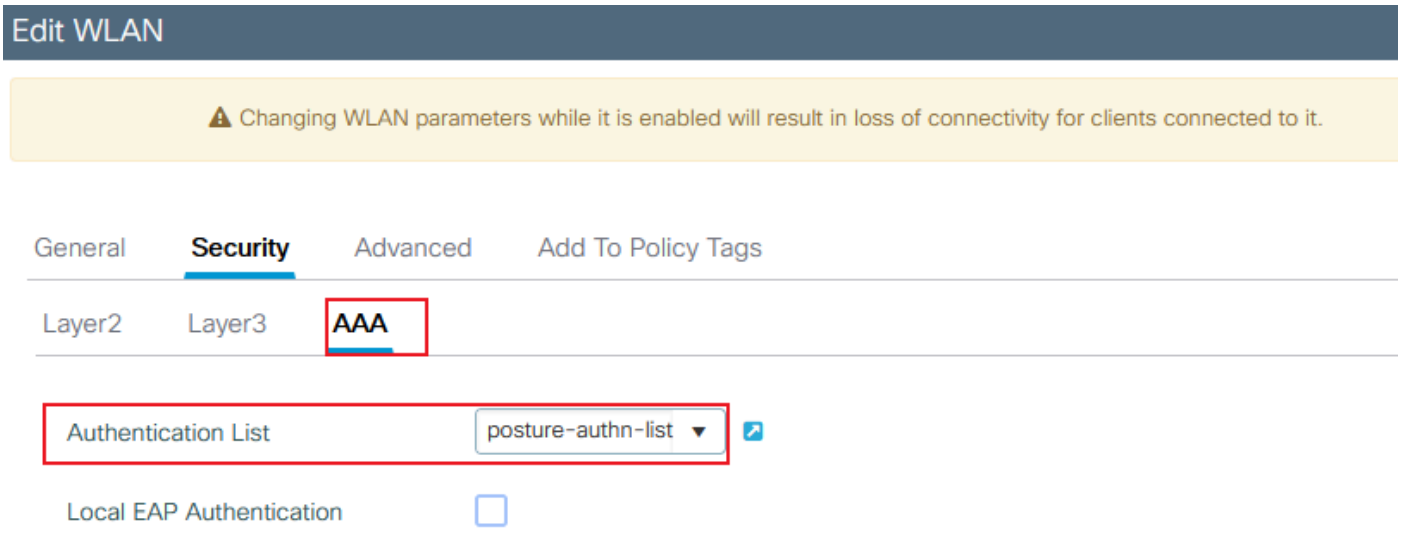



9800: creazione di una WLAN generale

Passaggio 3. Passare alla scheda Protezione e scegliere il metodo di protezione desiderato. In questo caso, scegliere '802.1x' e l'elenco di autenticazione AAA (creato nel passaggio 2. nella sezione Configurazione AAA) sono obbligatori:




9800: creazione della sicurezza WLAN L2

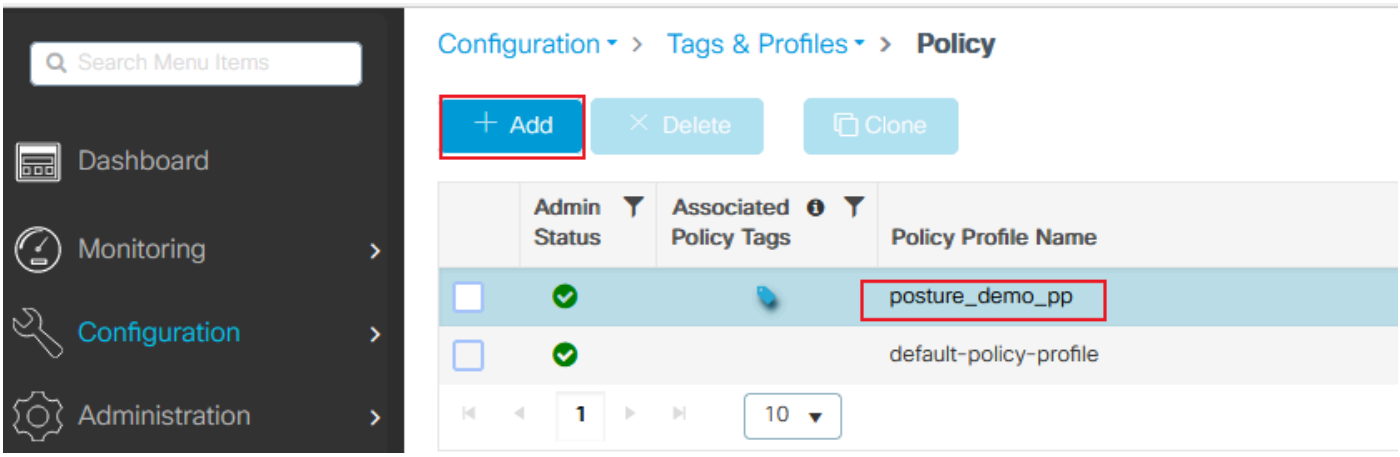



9800: creazione di AAA per la sicurezza WLAN

## Configurazione del profilo di policy

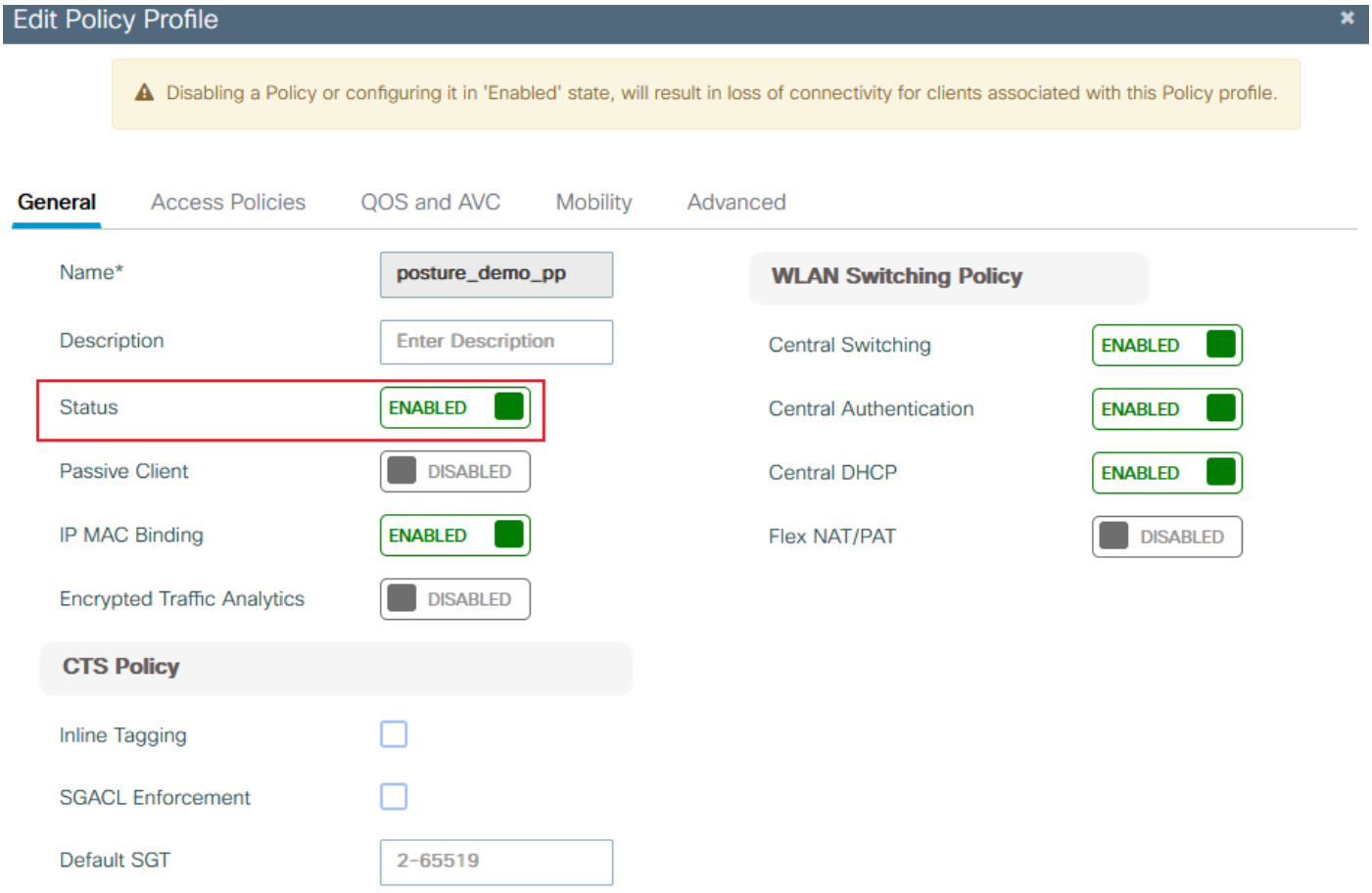
All'interno di un profilo di policy, è possibile decidere di assegnare ai client la VLAN desiderata, tra le altre impostazioni (ad esempio, Access Controls List (ACL), Quality of Service (QoS), Mobility Anchor, Timer e così via). È possibile usare il profilo di policy predefinito oppure crearne uno nuovo.

Passaggio 1. Creare un nuovo Policy Profile (Profilo di policy). Passare a Configurazione > Tag e profili > Criterio e crearne uno nuovo:



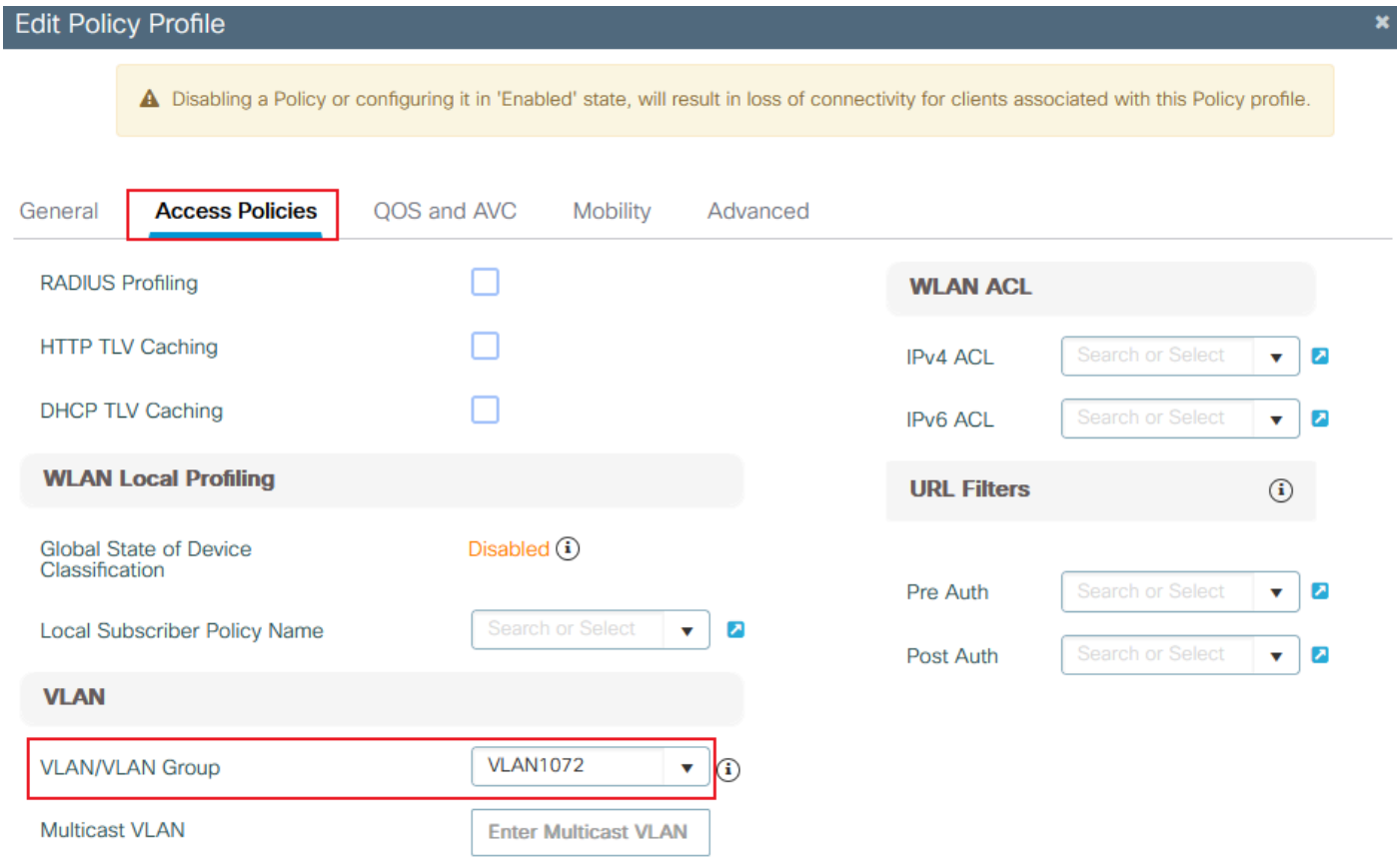

9800 add policy profile

Verificare che il profilo sia abilitato.



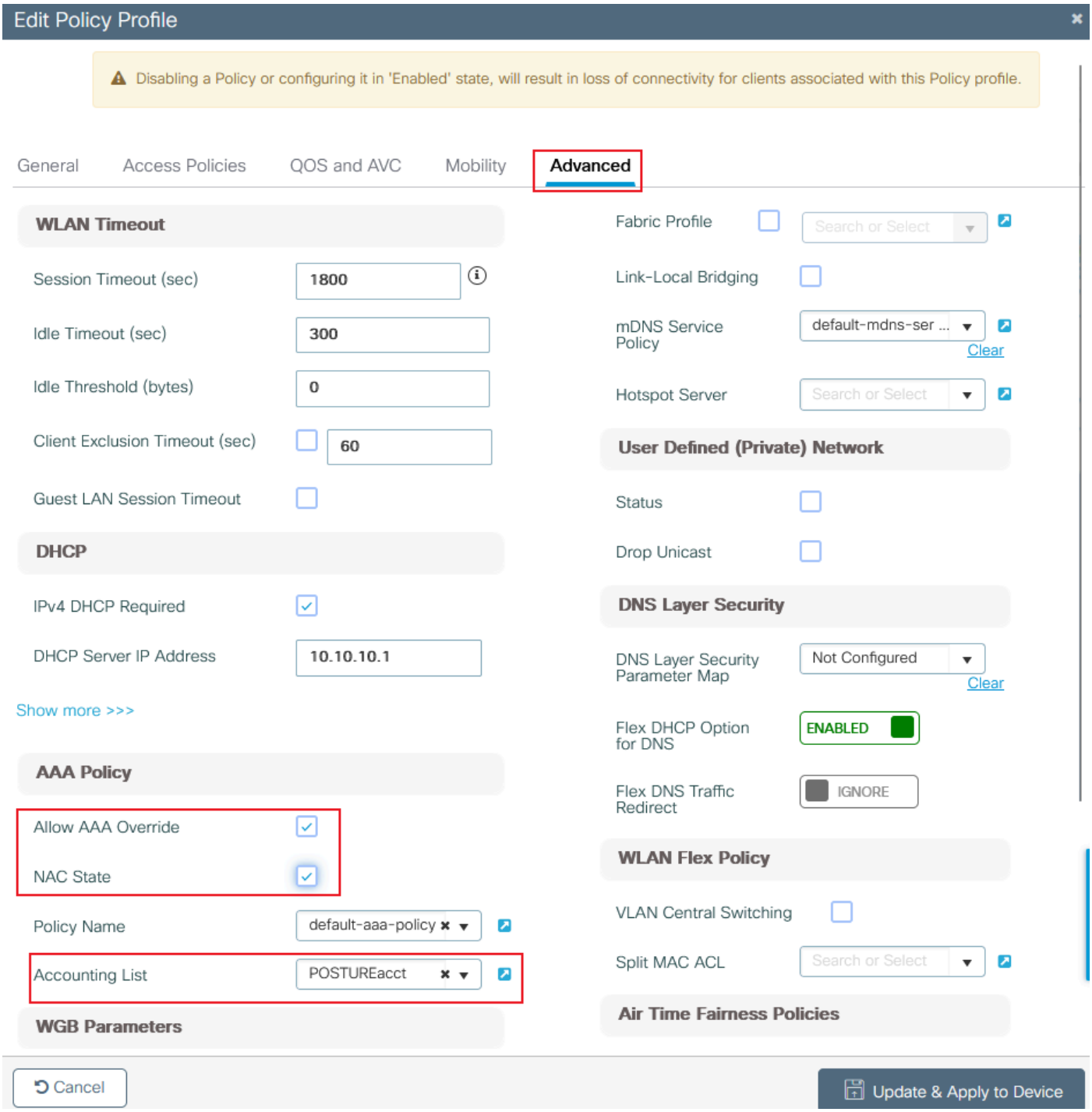

9800 create policy profile general

Passaggio 2. Selezionare la VLAN. Passare alla scheda Access Policies (Criteri di accesso) 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:




9800: creazione della VLAN del profilo della policy

Passaggio 3. Configurare il profilo di policy per accettare le sostituzioni ISE (Allow AAA Override) e le modifiche di autorizzazione, o CoA (Change of Authorization) (stato NAC). È possibile anche specificare un metodo di accounting:

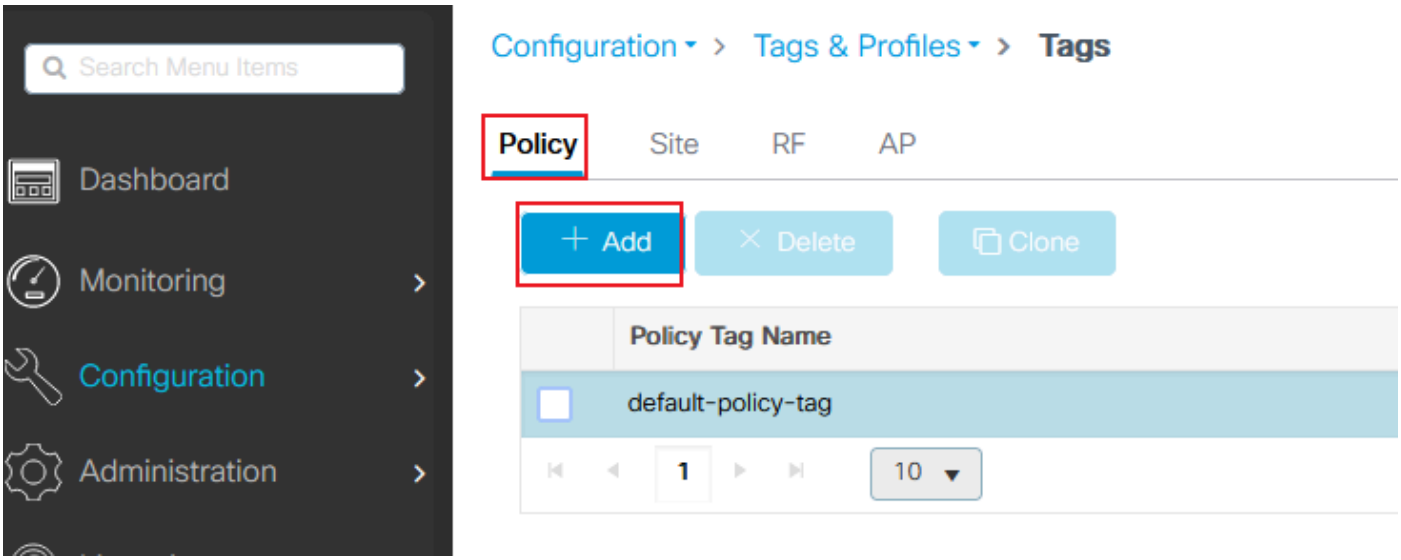



9800 create policy profile Advance

## 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.

Passare a Configurazione > Tag e profili > Tag > Criteri e aggiungerne uno nuovo, se necessario, come mostrato nell'immagine:



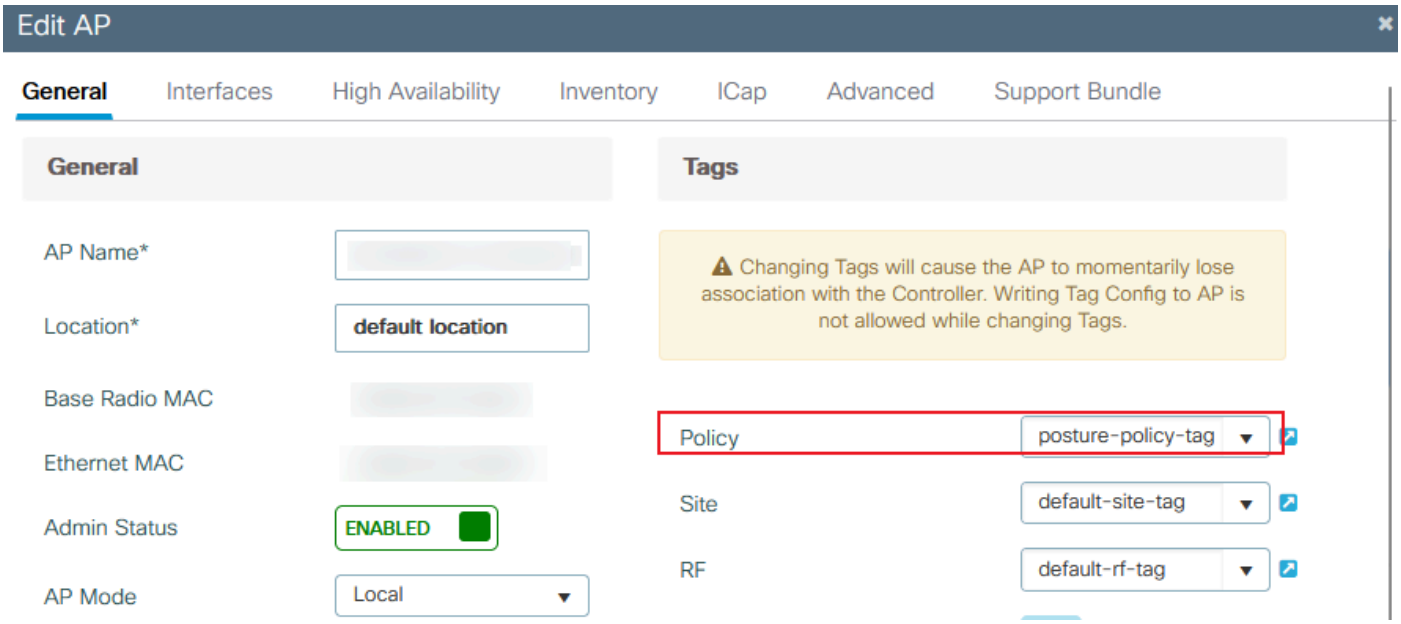

9800 policy tag add

Associare il profilo WLAN al profilo di policy desiderato:


Dettagli tag criteri 9800

## Assegnazione di un tag di policy

Assegnare il tag di policy agli access point desiderati. Selezionare Configurazione > Wireless > Access Point > Nome access point > Tag generali , effettuare l'assegnazione necessaria, quindi fare clic su Aggiorna e applica al dispositivo.



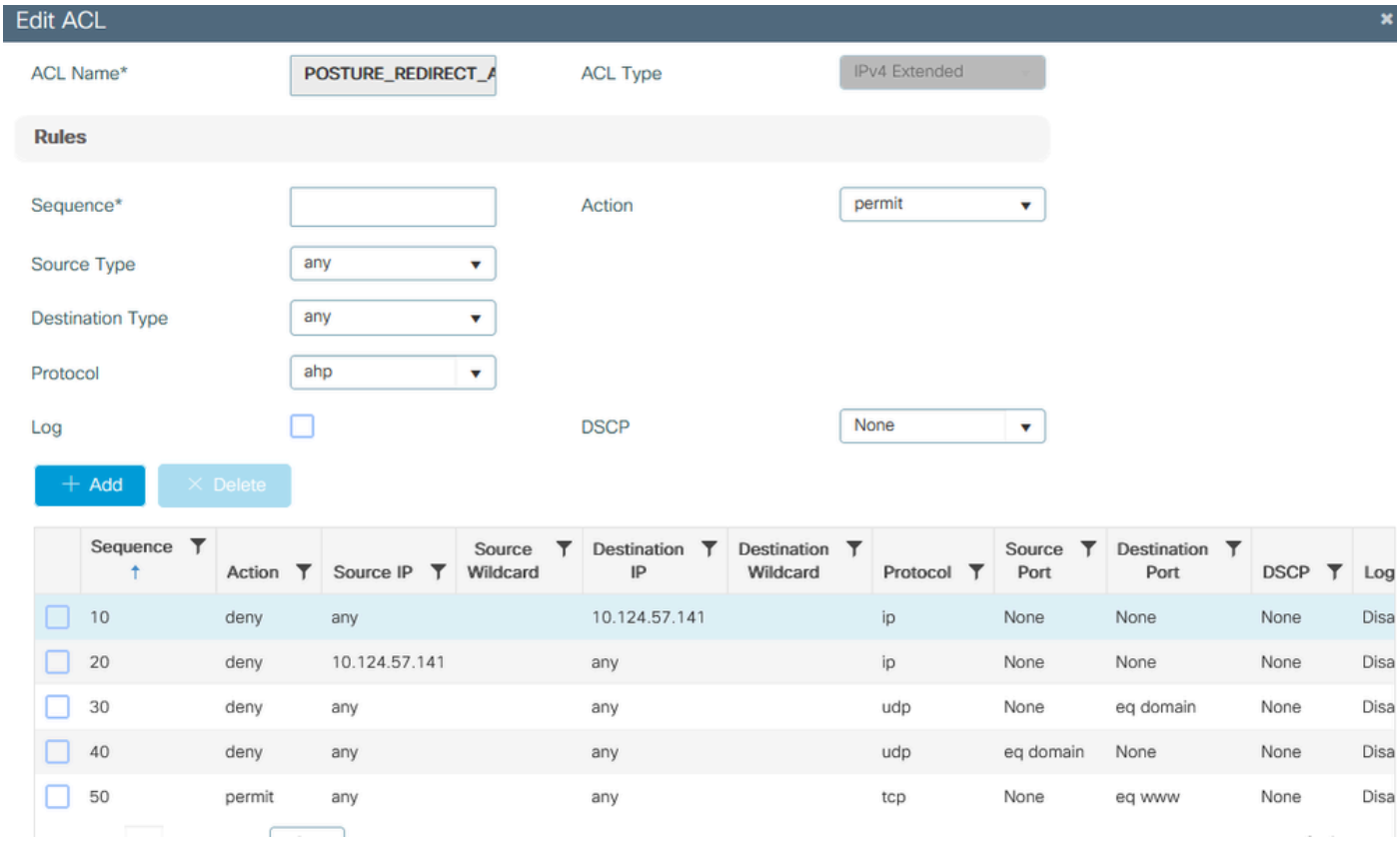

9800 assegnazione di tag ai criteri

## Configurazione degli ACL di reindirizzamento

Per creare un nuovo ACL, selezionare Configurazione > Sicurezza > ACL > + Aggiungi.

L'ACL utilizzato per il reindirizzamento del portale delle posture ha gli stessi requisiti di CWA (Central Web Authentication).

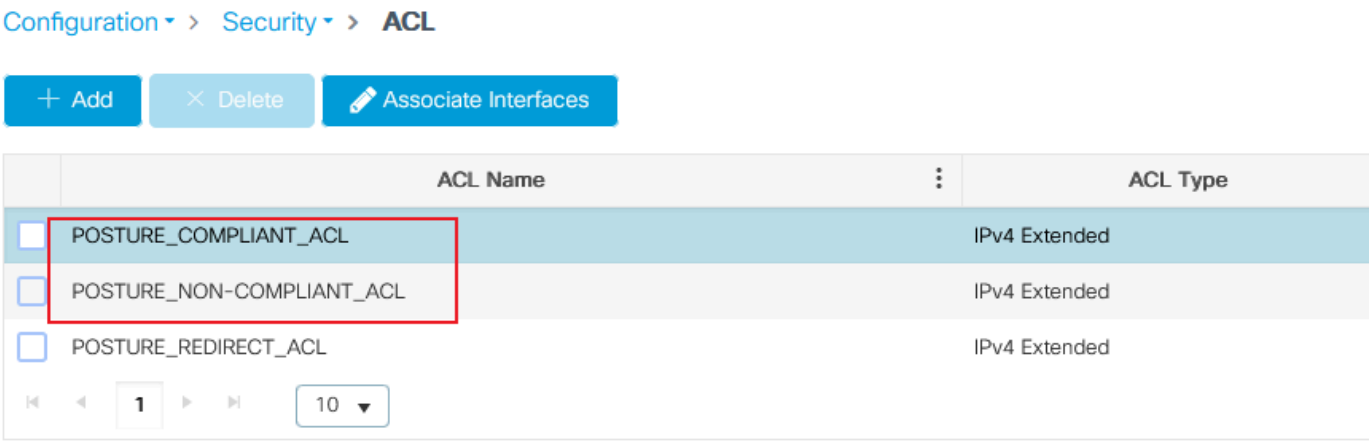
È necessario bloccare il traffico diretto ai nodi ISE PSN e al DNS; tutto il resto del traffico può essere autorizzato. Questo ACL di reindirizzamento non è un ACL di sicurezza, ma un ACL punt che definisce il traffico diretto alla CPU (sui permessi) per un ulteriore trattamento (come il reindirizzamento) e il traffico rimanente sul piano dati (su rifiuto) e impedisce il reindirizzamento. L'ACL deve avere questo aspetto (sostituire 10.124.57.141 con l'indirizzo IP ISE nell'esempio):




Dettagli ACL di reindirizzamento 9800

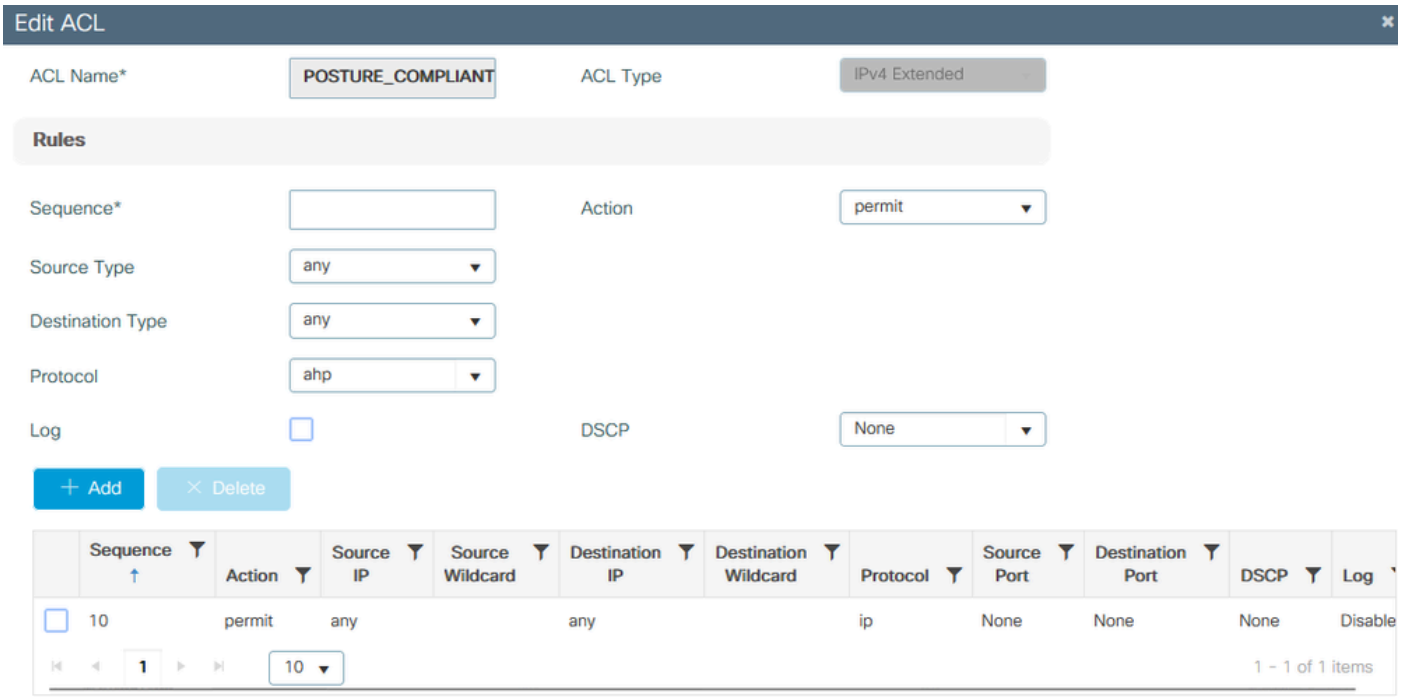
## Configurazione ACL del criterio

In questo caso, è necessario definire ACL separati su 9800 WLC per ISE per autorizzare gli scenari di conformità e non conformità in base ai risultati del controllo di postura.



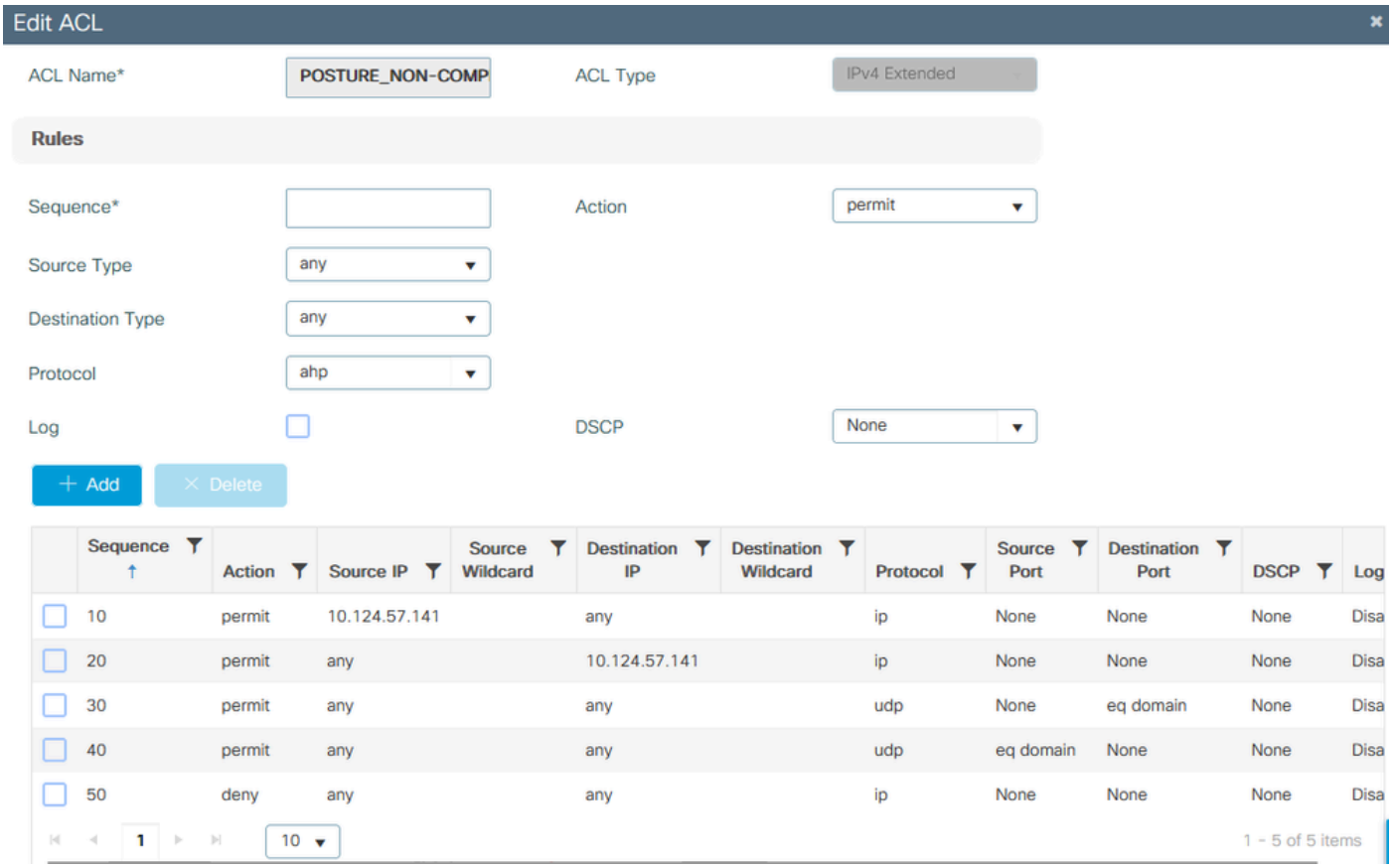

9800 ACL - Generale

Per lo scenario conforme, utilizzare semplicemente consenti tutto in questo caso. Come altra configurazione comune, l'ISE può decidere di non autorizzare alcun ACL nel risultato conforme, il che equivale a permettere tutto sul lato 9800:




9800 ACL - Conforme

In uno scenario non conforme, il client consente l'accesso solo a determinate reti, in genere il server di monitoraggio e aggiornamento (in questo caso ISE):

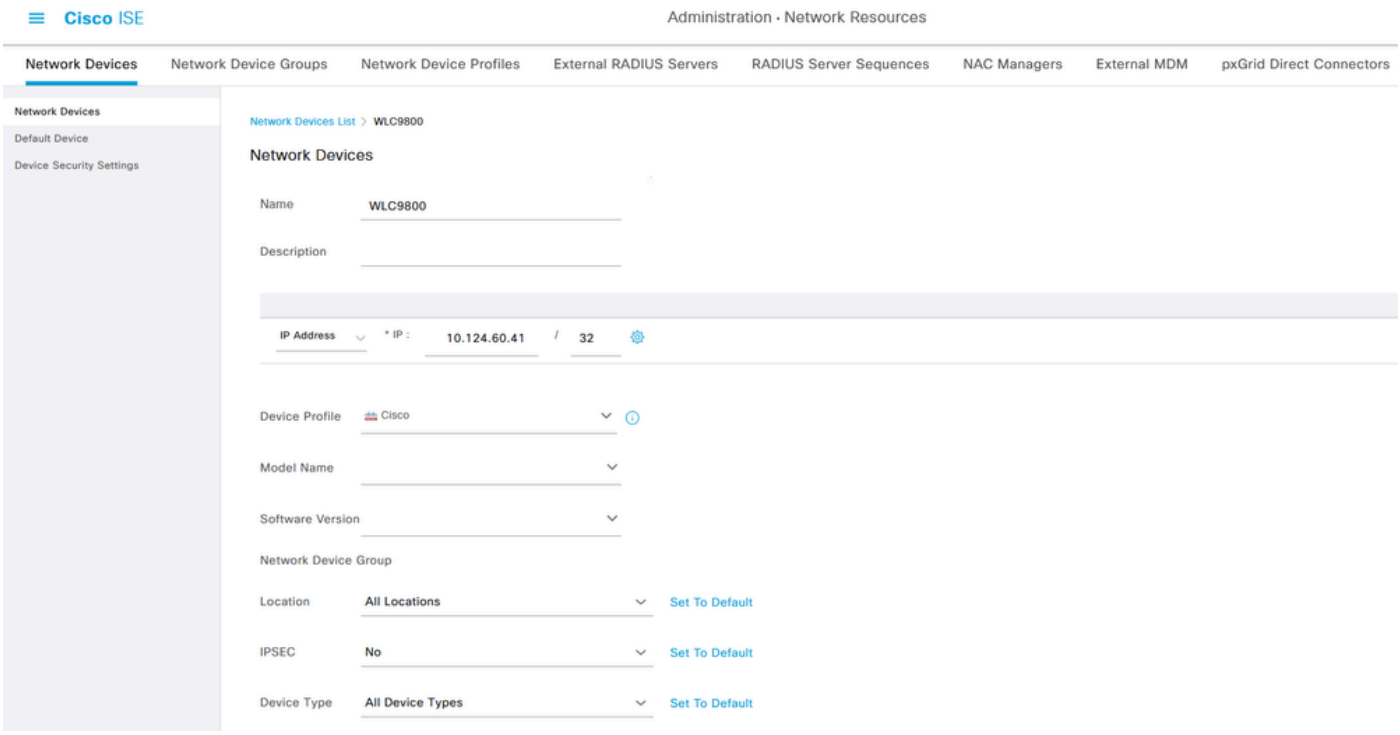



9800 ACL - Non conforme

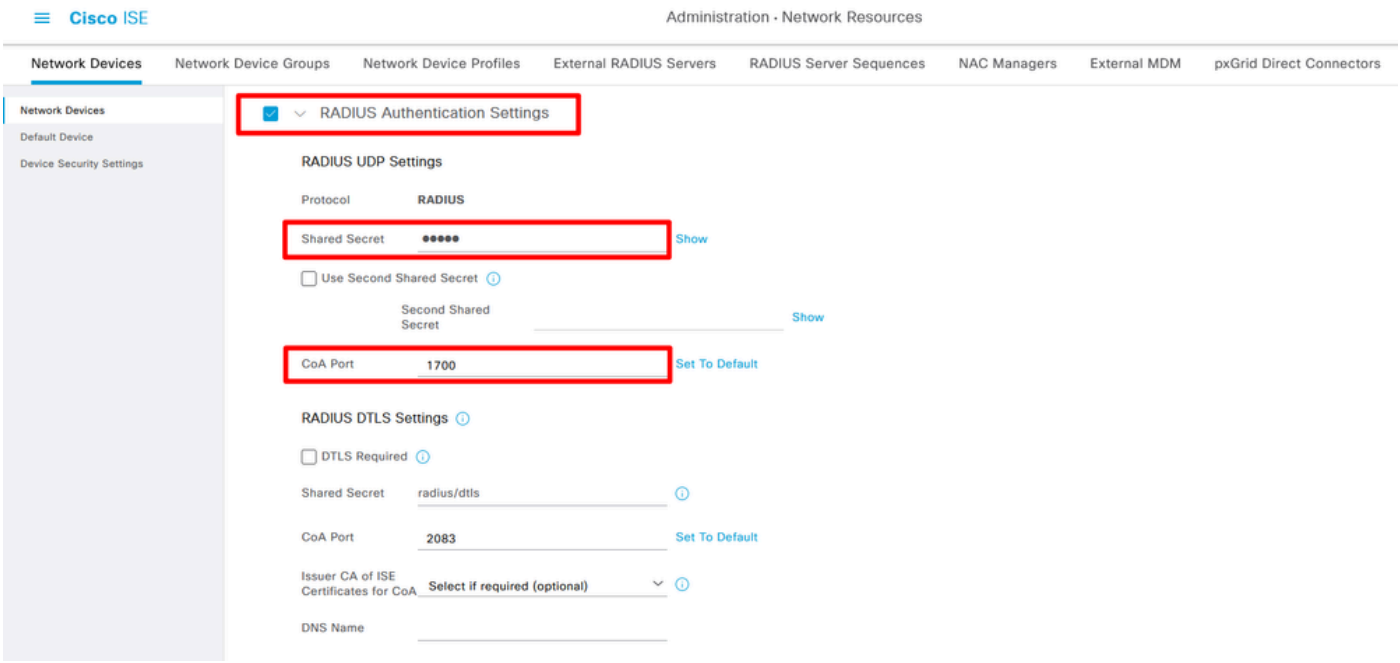
## Configurazione AAA e impostazione della postura su ISE

Requisito postura: In questo esempio, il requisito per determinare la conformità è rilevare se un file di test specifico esiste sul desktop utilizzato per testare il PC Windows.

Passaggio 1. Aggiungere WLC 9800 come AND sull'ISE. Selezionare Amministrazione > Risorse di rete > Dispositivi di rete > Aggiungi:



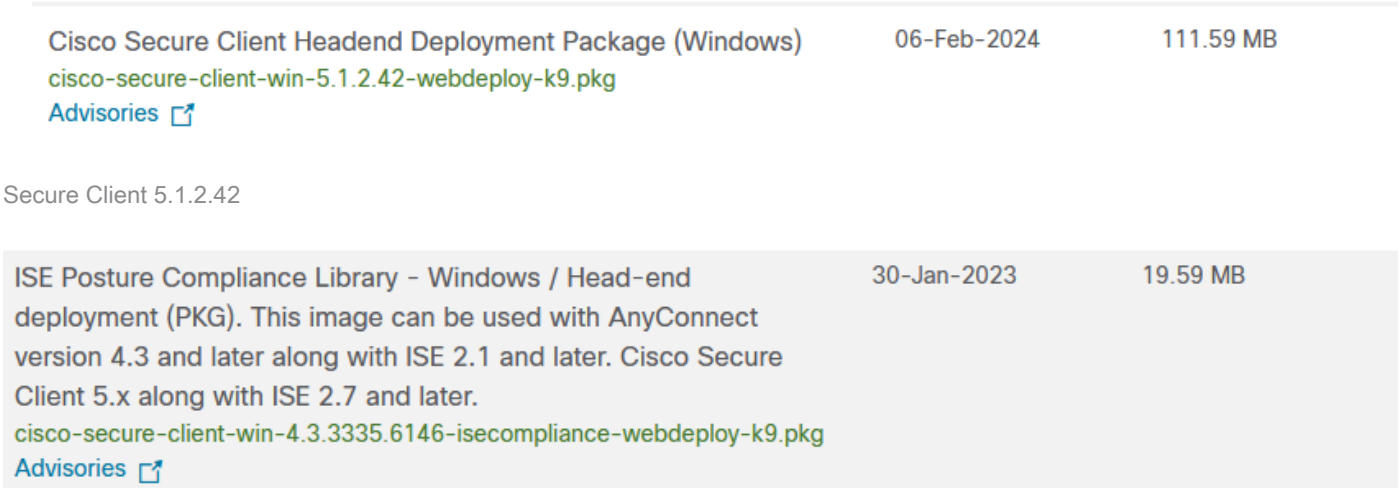

Aggiungi dispositivo di rete 01




Aggiungi dispositivo di rete 02

Passaggio 2. Scaricare il pacchetto di distribuzione e il modulo di conformità dell'headend Cisco Secure Client sul sito Web CCO per il software Cisco.

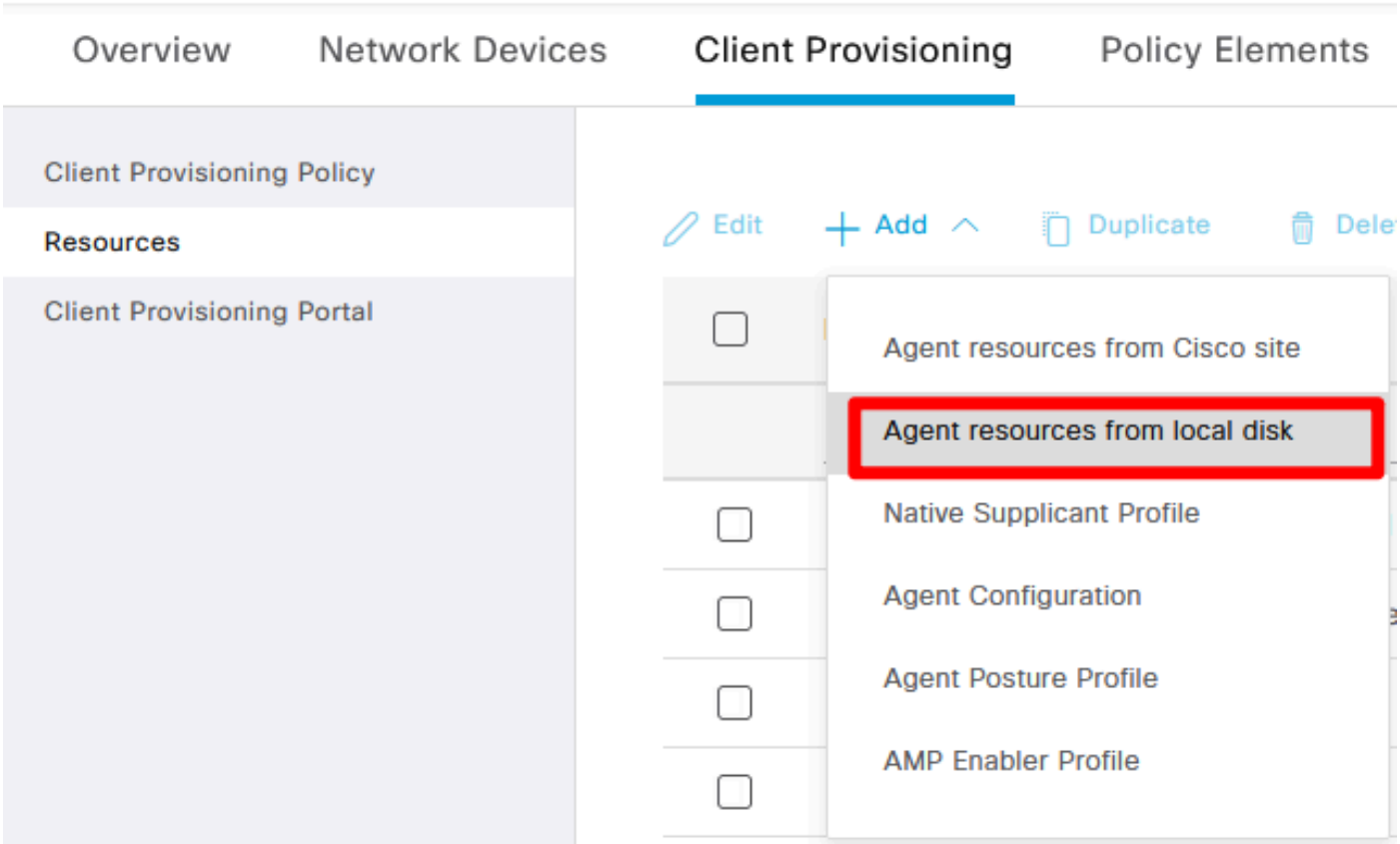
Accesso e ricerca in Cisco Secure Client:



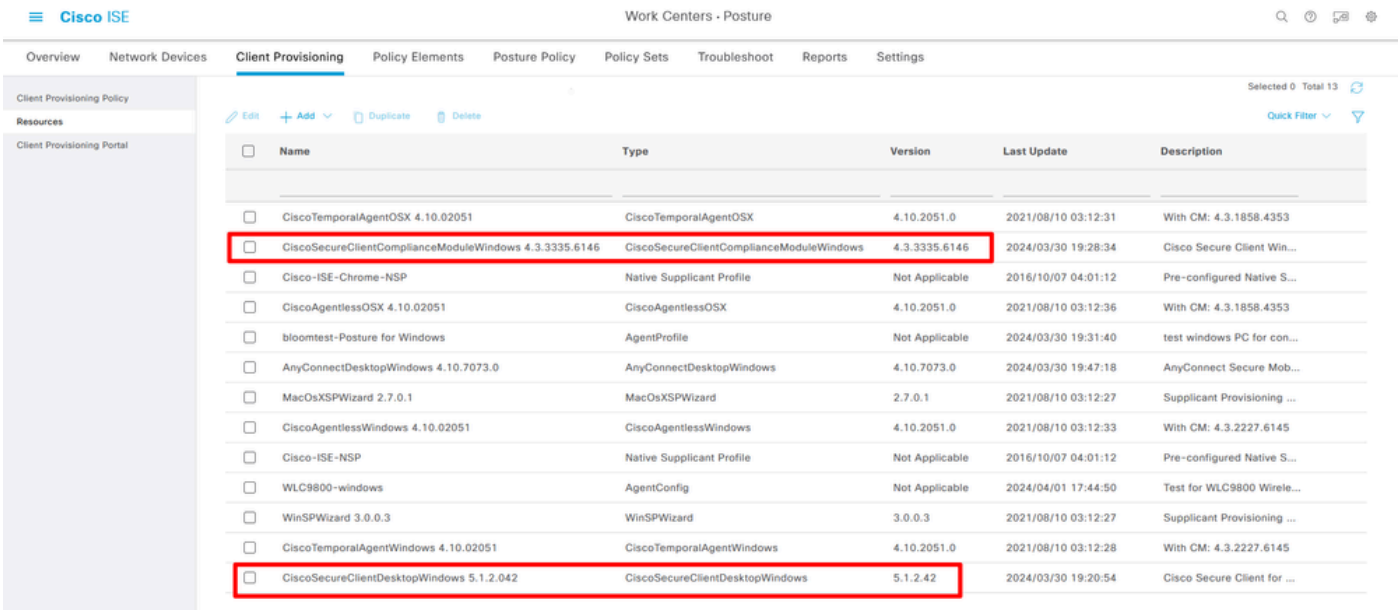

Secure Client 5.1.2.42

ISE Compliance Module 4.3

Passaggio 3. Caricare il pacchetto del pacchetto di distribuzione headend Cisco Secure Client e il pacchetto del modulo di conformità in ISE Client Provisioning. Passare a Centri di lavoro> Postura> Provisioning client> Risorse. Fare clic su Aggiungi, Scegliere Risorse agente dal disco locale dalla casella a discesa:

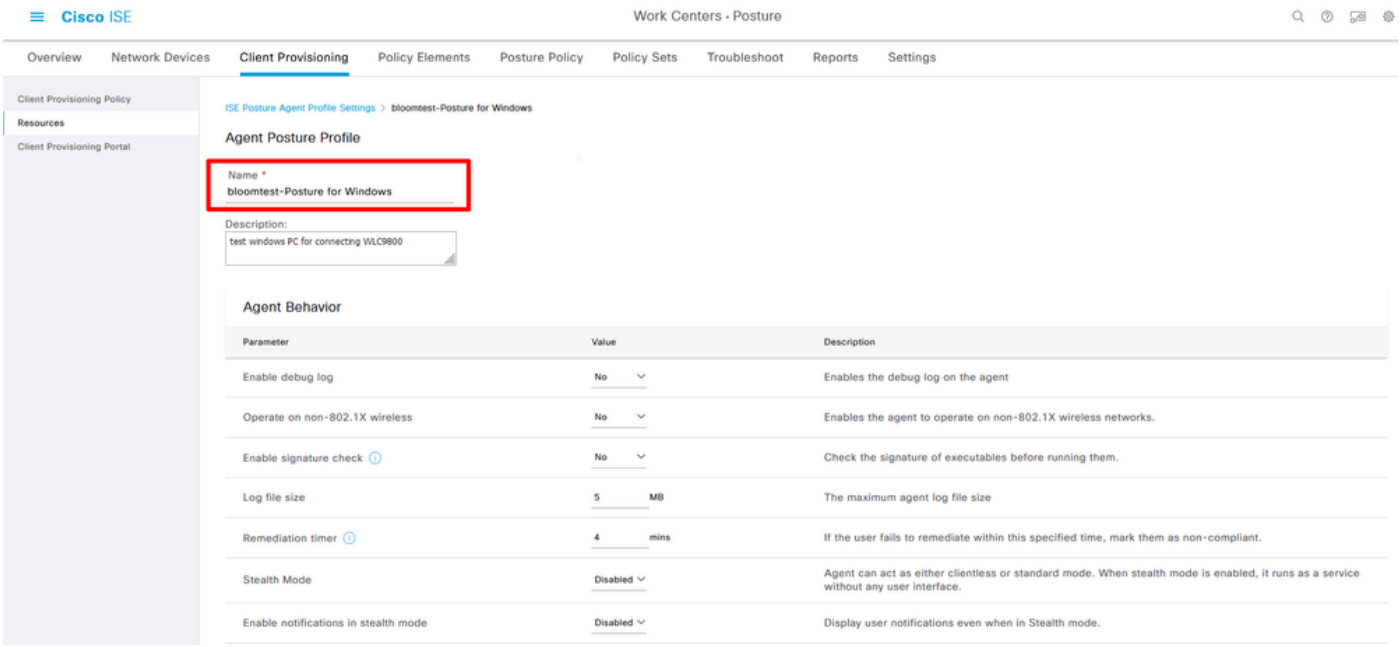



Upload Secure Client



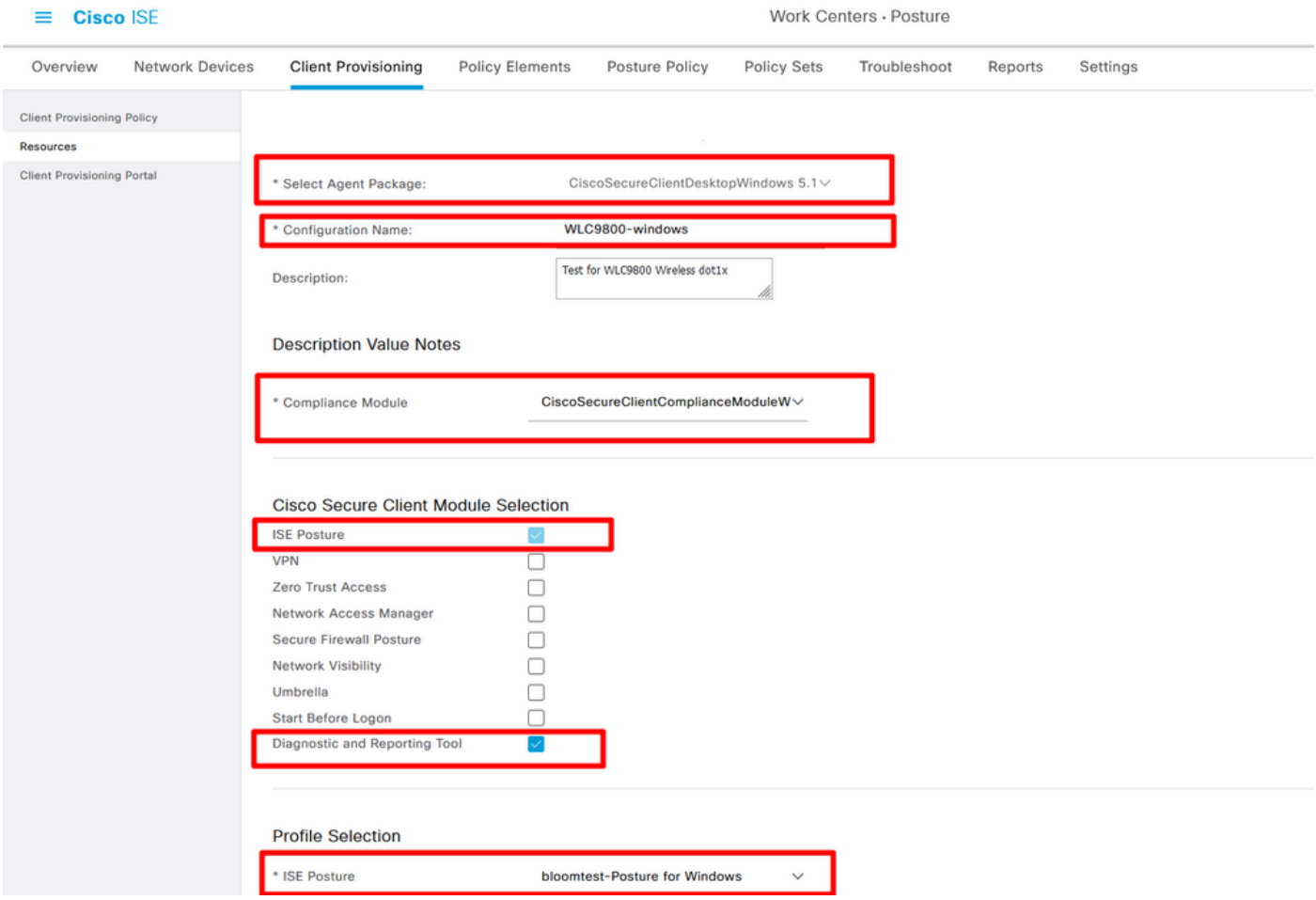

Caricamento del client sicuro e del modulo di conformità completato

Passaggio 4. Crea profilo postura agente Passare a Centri di lavoro> Postura> Provisioning client> Risorse> Aggiungi> Profilo postura agente:




Profilo postura agente

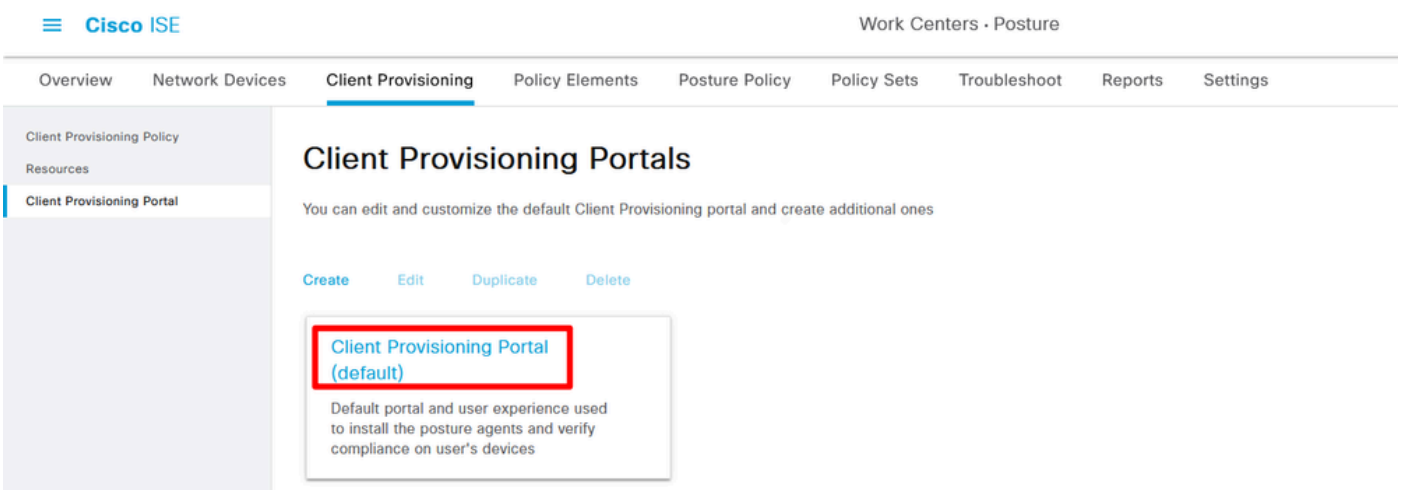
Passaggio 5. Creare la configurazione dell'agente Passare a Centri di lavoro> Postura> Provisioning client> Risorse> Aggiungi> Configurazione agente:



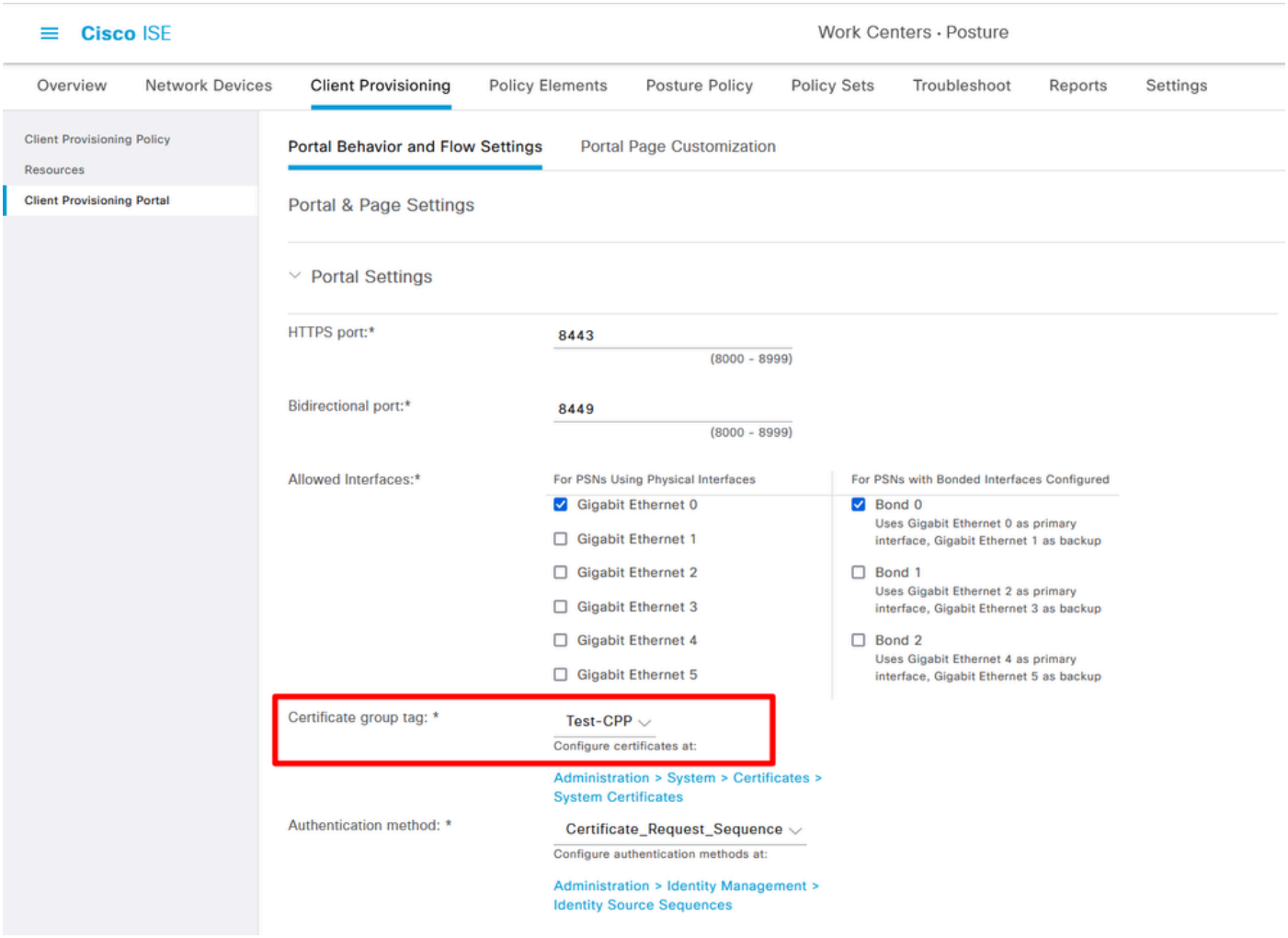

Aggiungi configurazione agente

Passaggio 6. Verificare che il portale di provisioning client sia corretto. Utilizzare il portale predefinito per il testing. (Generare CSR e richiedere un certificato SSL dal server CA e sostituire il tag Gruppo di certificati in queste impostazioni del portale. In caso contrario, durante il processo di test verrà visualizzato un avviso di certificato non attendibile.)

Passare a Centri di lavoro> Postura> Provisioning client> Portali provisioning client:

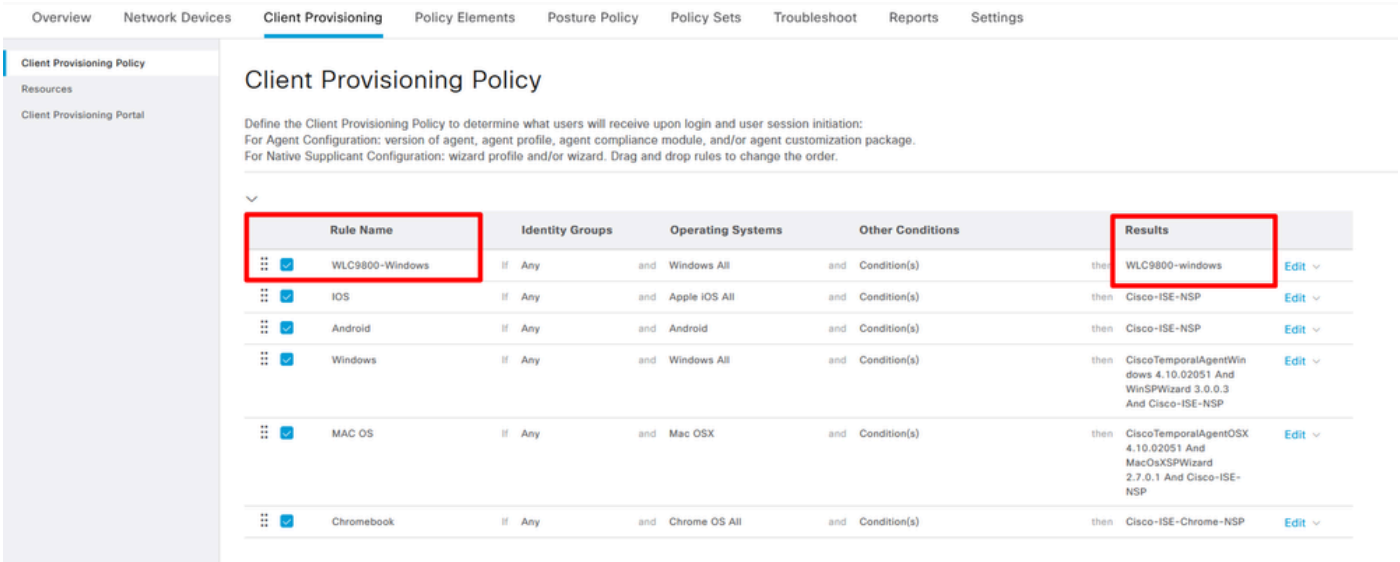



Scegli portale di provisioning client 01



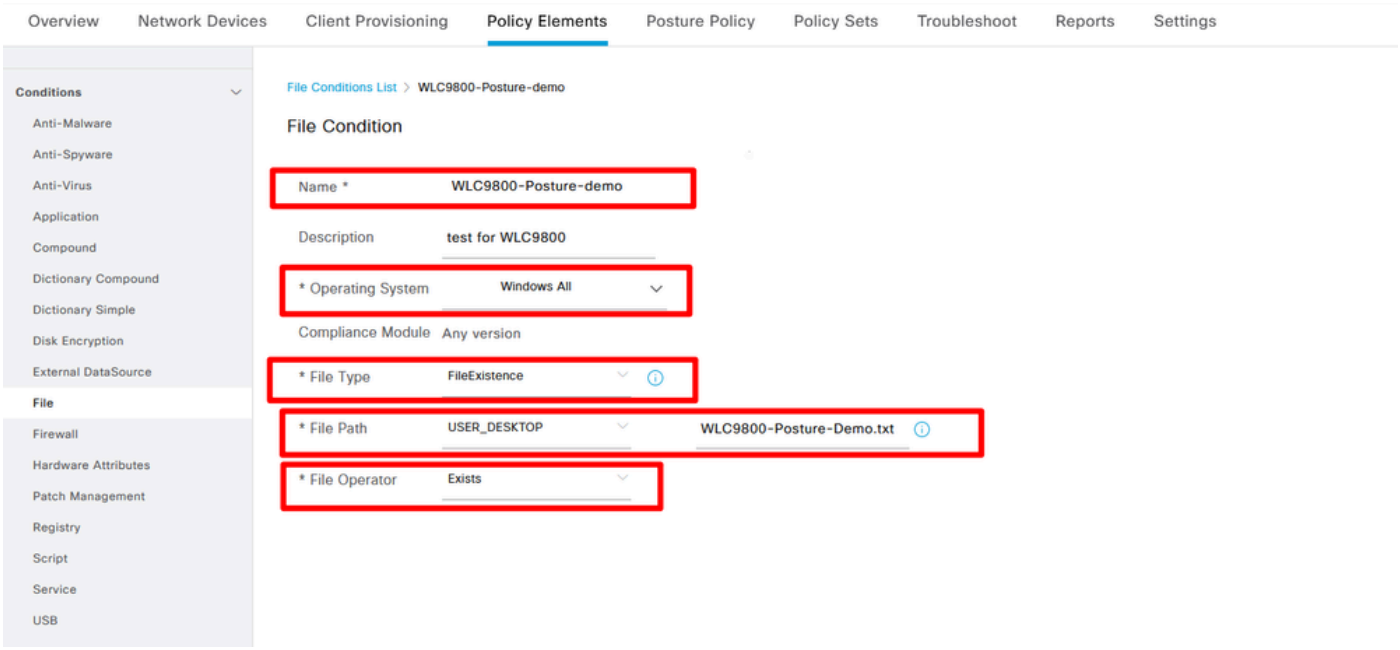

Scegli portale di provisioning client 02

Passaggio 7. Creazione dei criteri di provisioning client. Passare a Centri di lavoro> Postura> Provisioning client> Criterio di provisioning client > Modifica> inserire un nuovo criterio sopra.



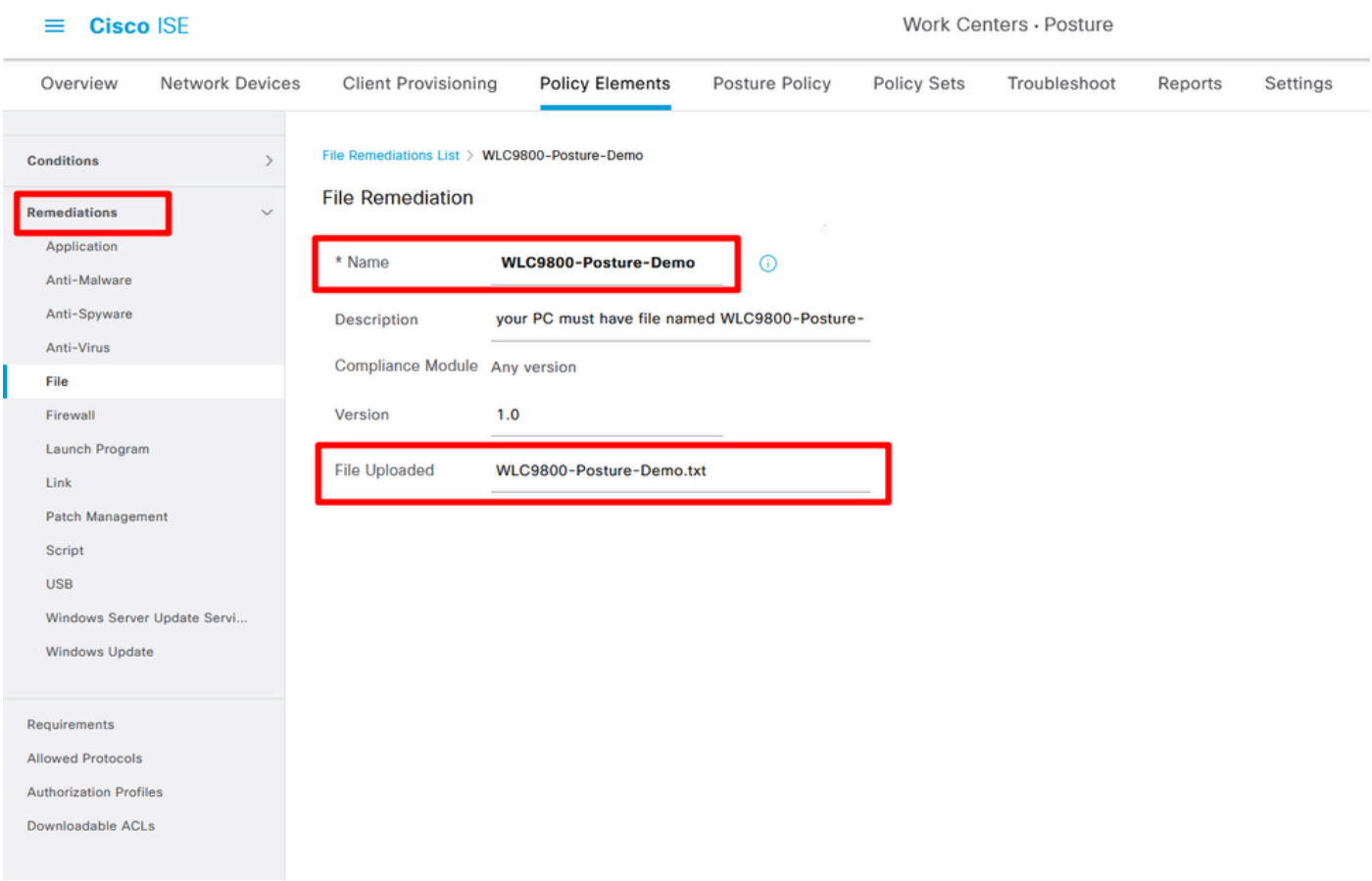

Crea criterio di provisioning client

Passaggio 8. Creazione delle condizioni del file. Passare a Centri di lavoro> Postura> Elementi della policy> Condizioni> File > Condizioni file> Aggiungi:



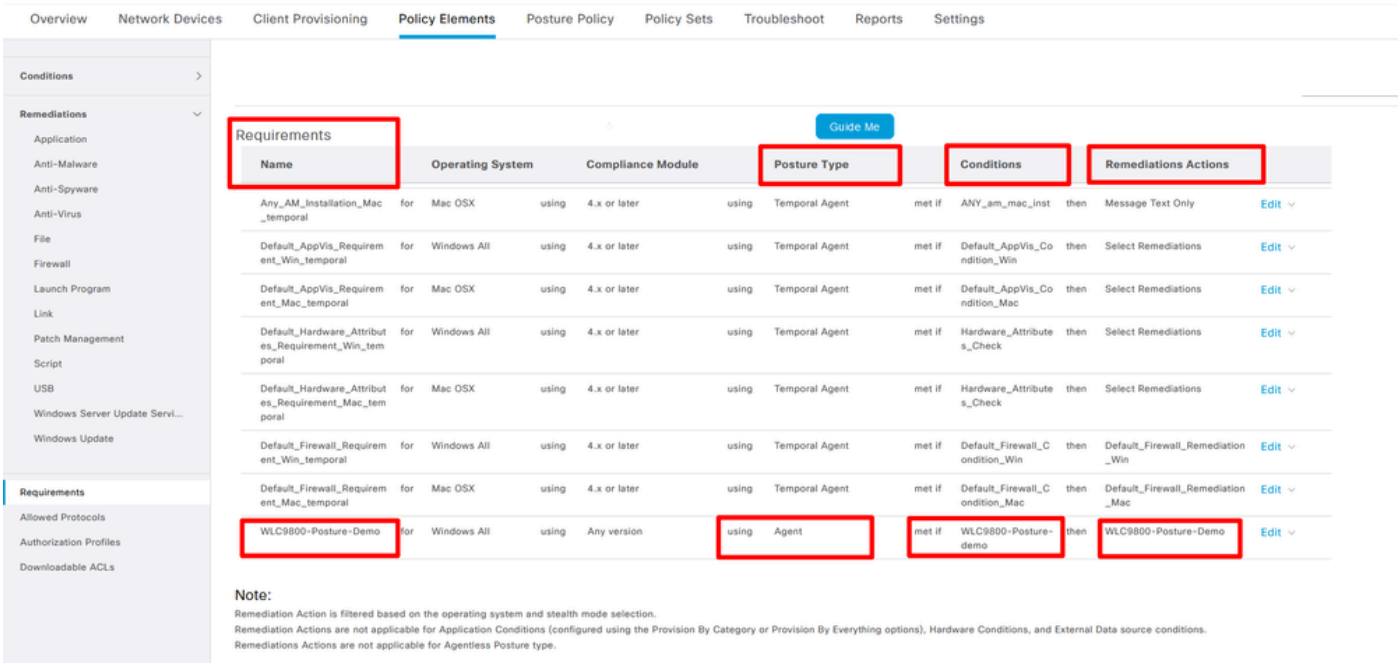

Crea condizione file

Passaggio 9. Creazione di soluzioni Passare a Centri di lavoro> Postura> Elementi dei criteri> Risoluzioni > File> Aggiungi:



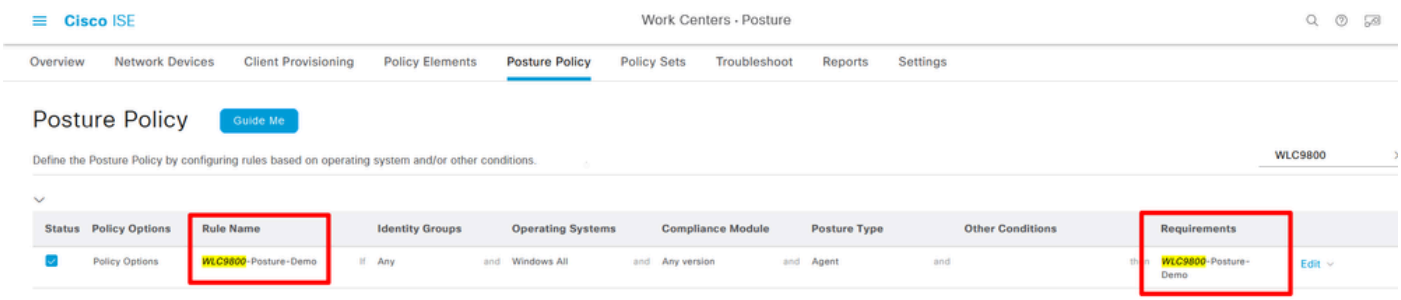

Crea risoluzione file

Passaggio 10. Creazione del fabbisogno. Passare a Centri di lavoro> Postura> Elementi criteri> Requisiti> Inserisci nuovo requisito:



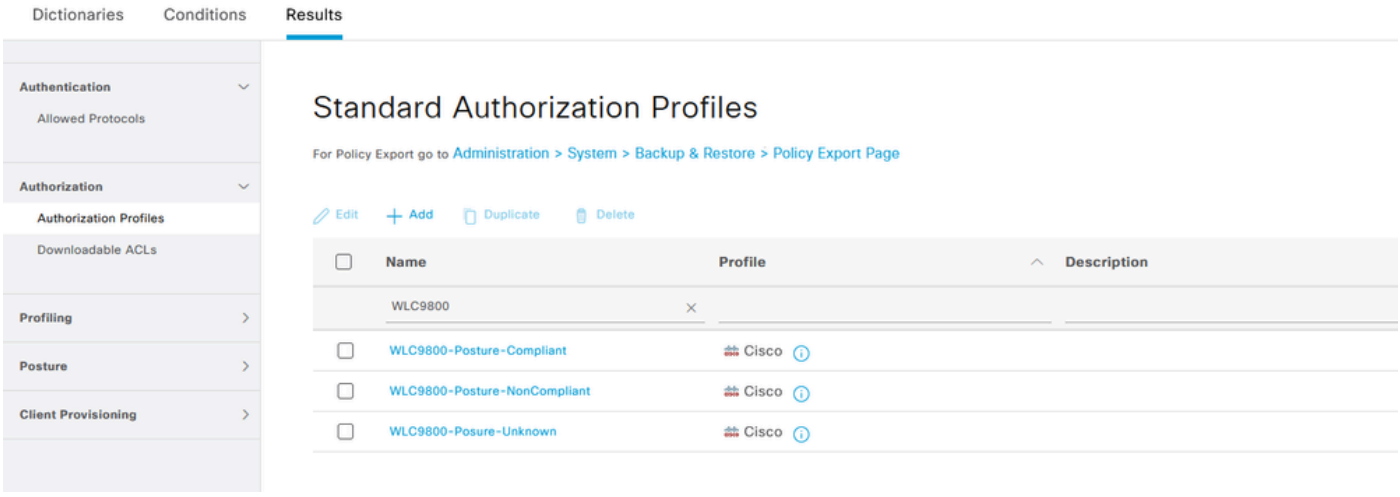

Crea requisito postura

Passaggio 11. Creazione dei criteri di postura. Passare a Centri di lavoro> Postura> Inserisci nuovo criterio:

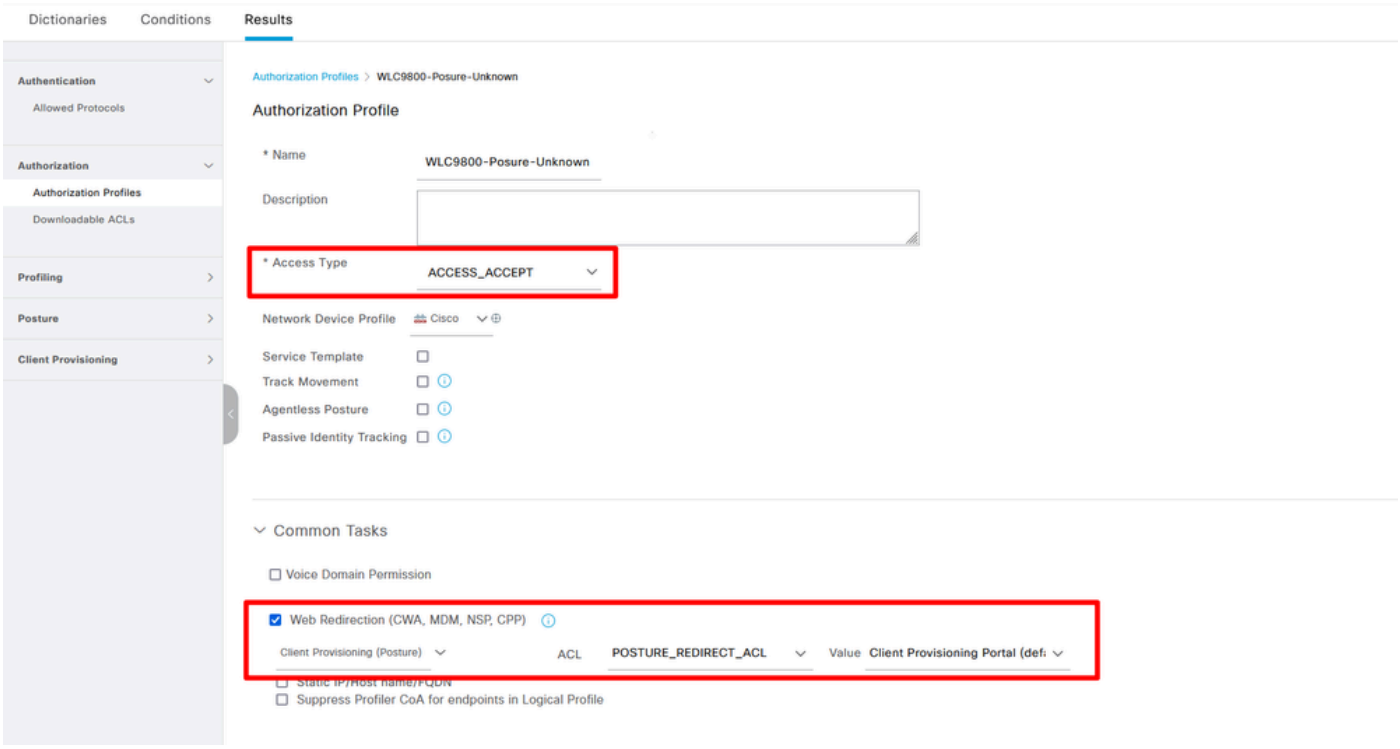



Crea criterio di postura

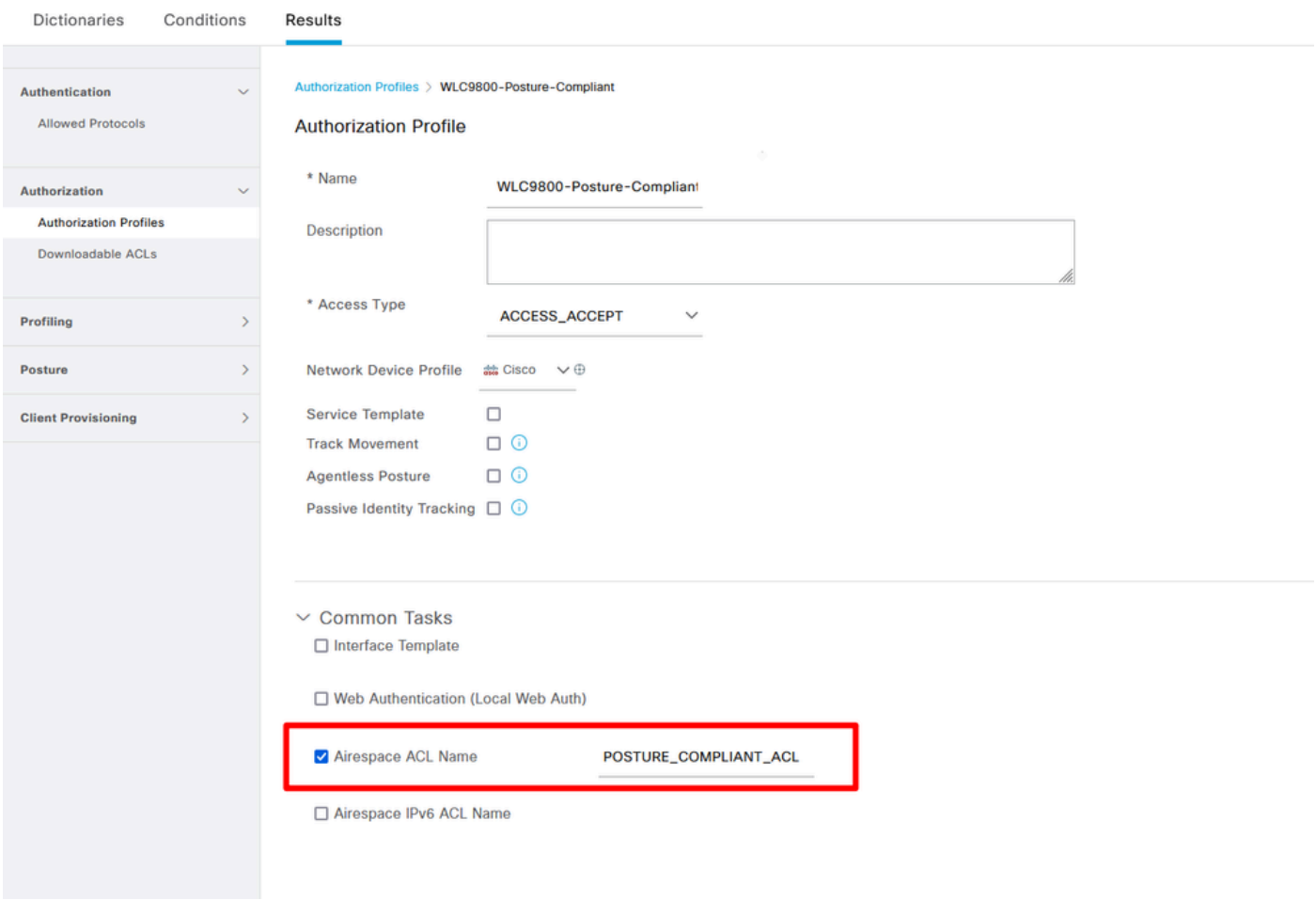
Passaggio 12. Creare tre profili di autorizzazione: Stato della postura sconosciuto; lo stato della postura non è conforme; Lo stato della postura è conforme. Passare a Criterio> Elementi dei criteri> Risultati> Autorizzazione> Profili di autorizzazione> Aggiungi:



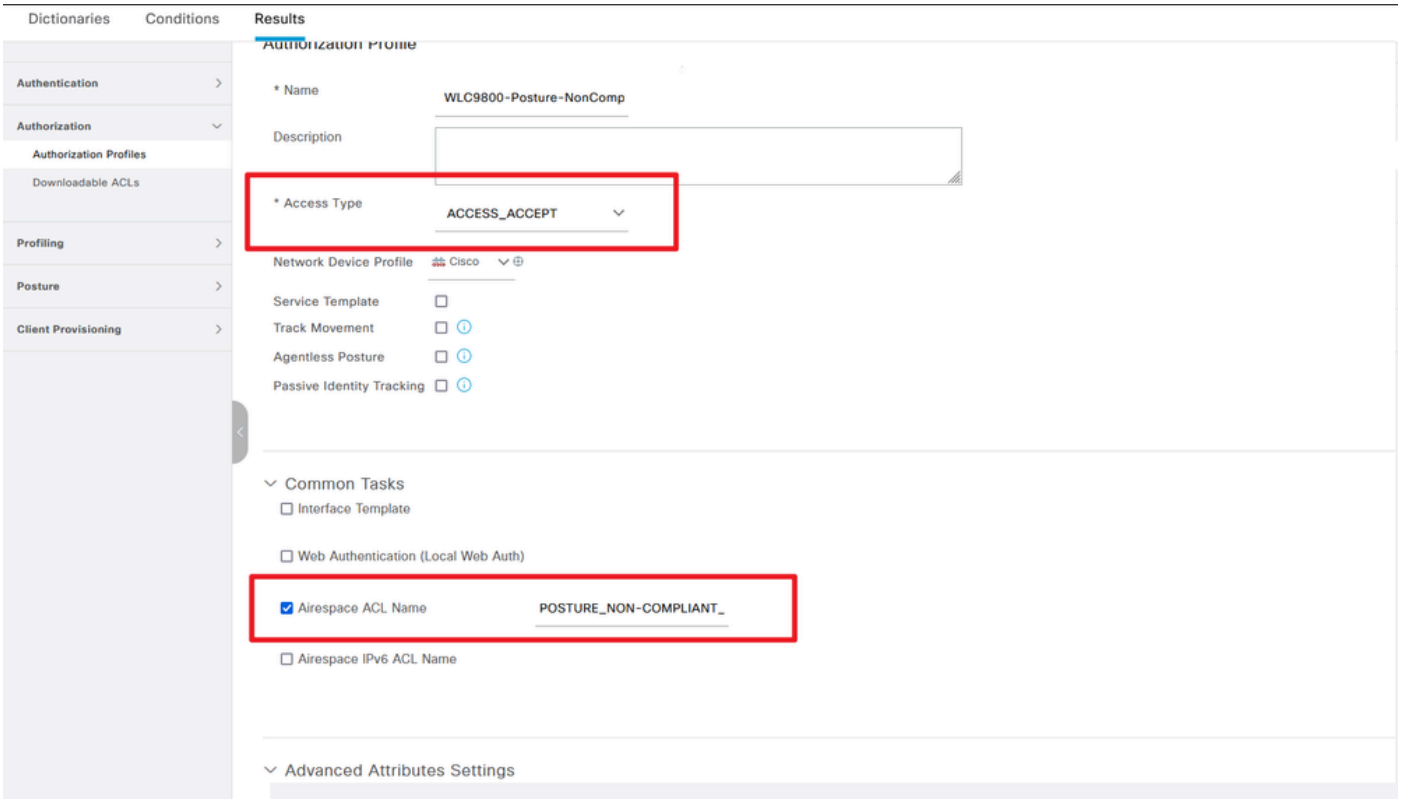
Crea profili di autorizzazione 01



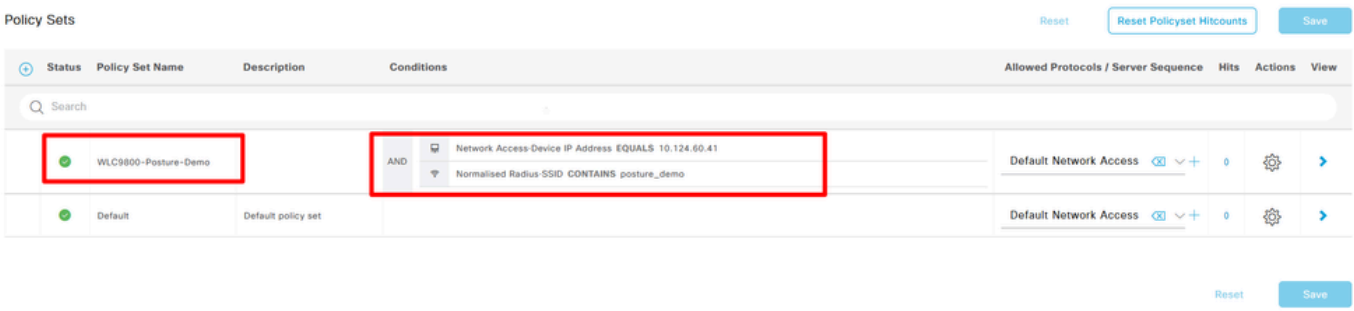

Crea profili di autorizzazione 02




Crea profili di autorizzazione 03



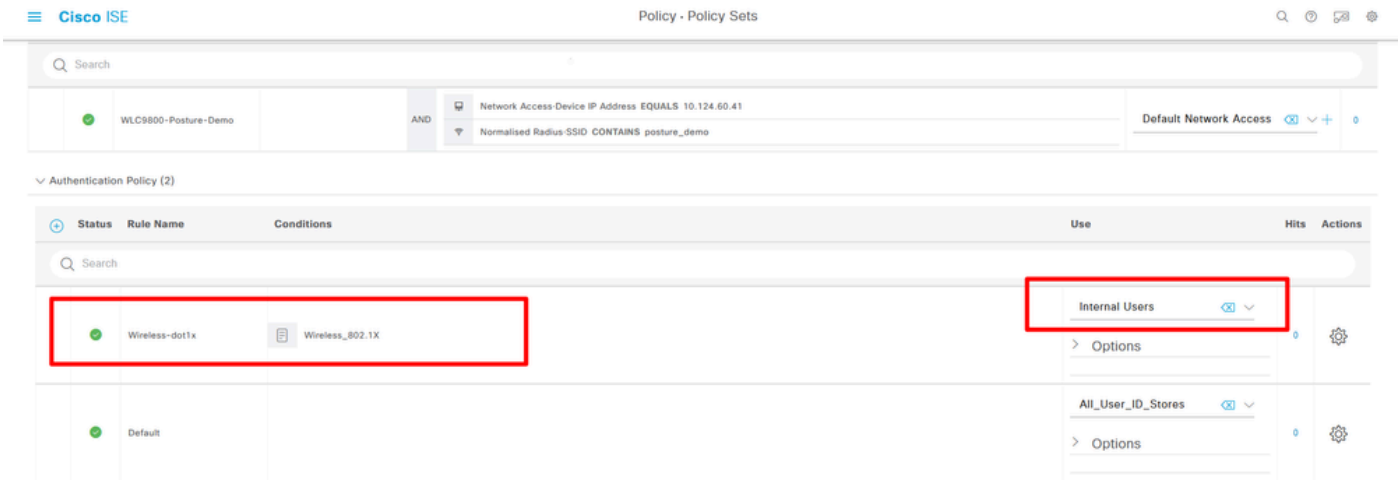

Passaggio 13. Creazione di set di criteri. Passa a Criterio > Criterio




Crea set di criteri

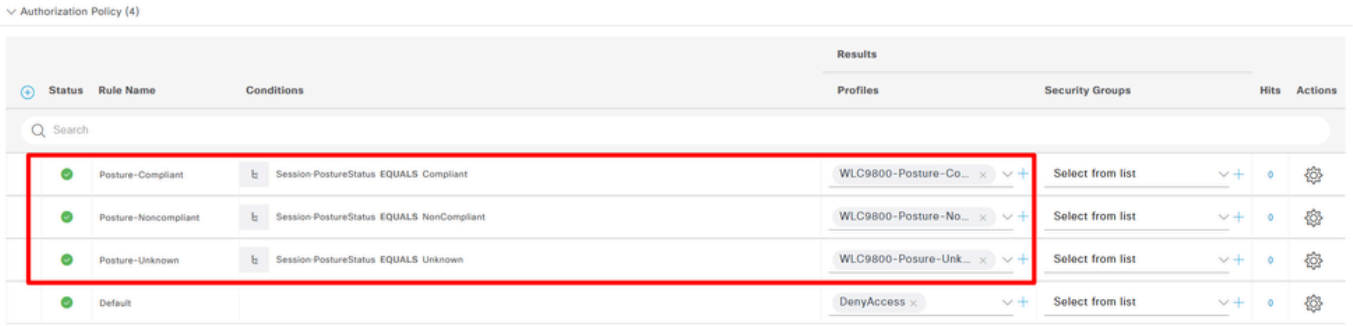
Sets> Aggiungi icona:

Passaggio 14. Creazione del criterio di autenticazione Passare a Criterio> Set di criteri> Espandere "WLC9800-Posture-Demo"> Criteri di autenticazione> Aggiungi:




Crea criterio di autenticazione

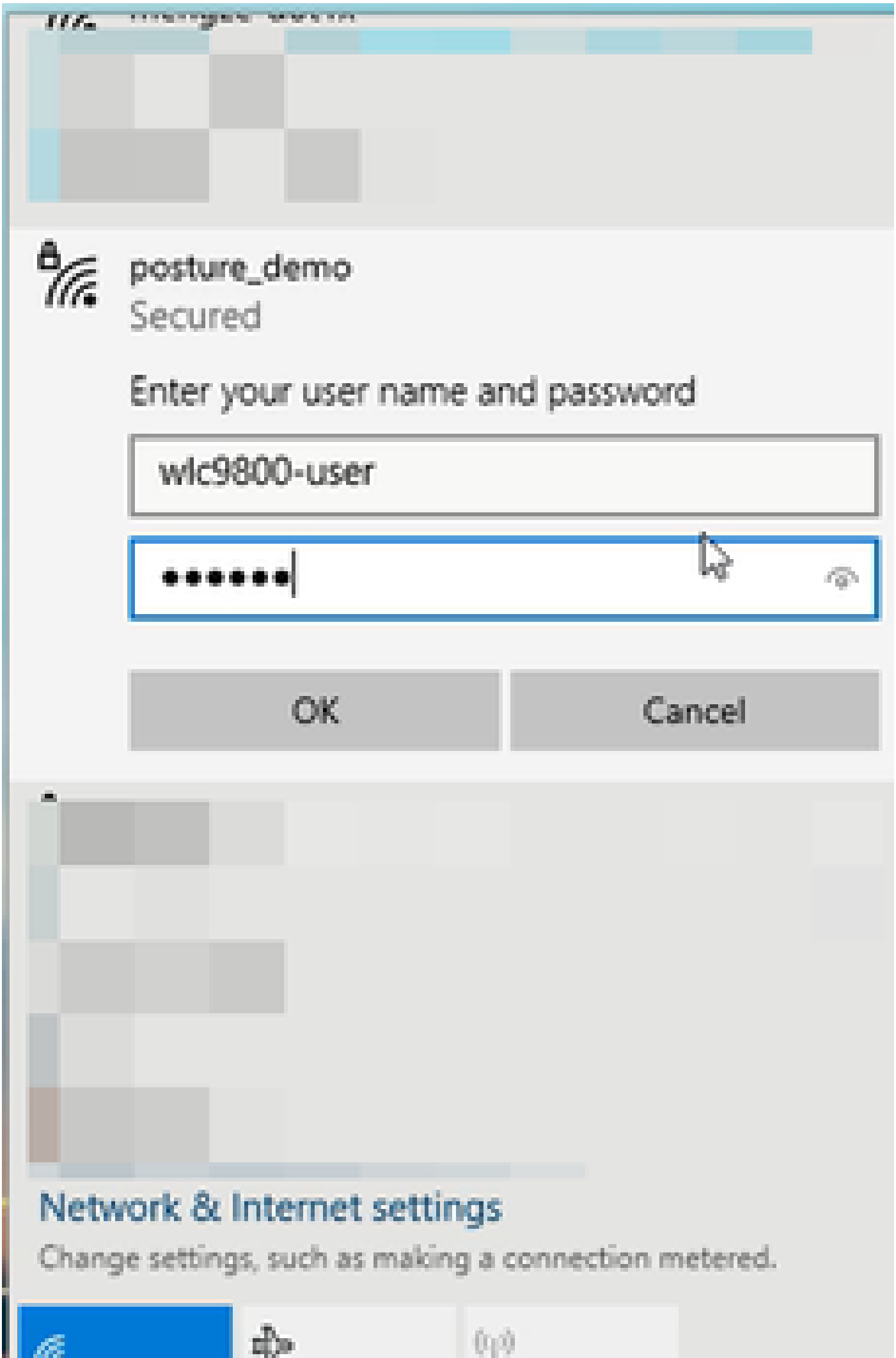
Passaggio 15. Creazione del criterio di autorizzazione Passare a Criterio> Set di criteri> Espandere "WLC9800-Posture-Demo"> Criterio di autorizzazione> Aggiungere:



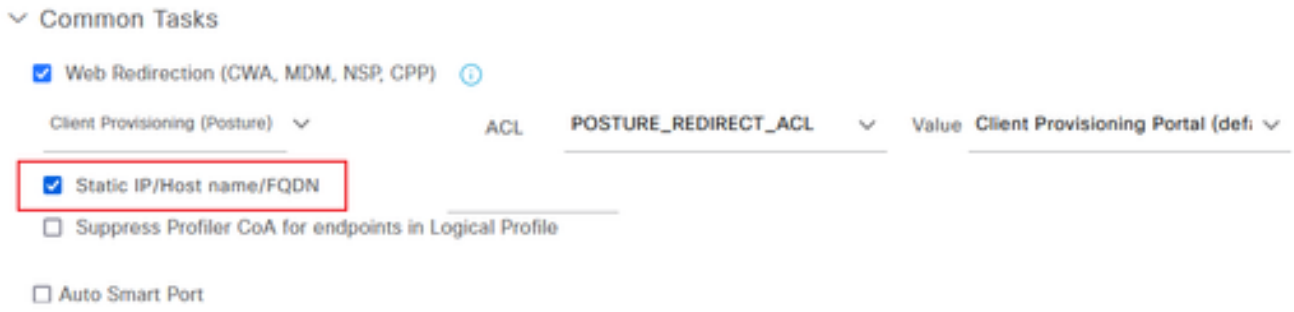

Crea criterio di autorizzazione

# Esempi

1. Test connesso SSID posture_demo con credenziali 802.1X corrette.


posture_demo
Secured
Enter your user name and password
wlc9800-user
OK
Cancel
Network & Internet settings
Change settings, such as making a connection metered.

- Se il browser è stato reindirizzato all'URL del portale ISE ma non è possibile caricare la pagina, verificare se il nome di dominio ISE non è stato aggiunto al server DNS e il client non è in grado di risolvere l'URL del portale. Per risolvere rapidamente il problema, controllare il nome IP/host statico/FQDN nel profilo di autorizzazione per fornire l'indirizzo IP nell'URL di reindirizzamento. Tuttavia, questo problema può riguardare la sicurezza in quanto espone l'indirizzo IP dell'ISE.




## Raccogli debug

Abilita debug su C9800

Abilita debug su ISE

## Riferimenti

- Configurazione di CWA su Catalyst 9800 WLC e ISE - Cisco
- BYOD wireless con Identity Services Engine
- Implementazione della postura ISE
- Risoluzione dei problemi di gestione e postura delle sessioni ISE
- Confronta il flusso di reindirizzamento della postura ISE con il flusso di reindirizzamento della postura ISE

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).