Configurazione di ISE BYOD con Single e Dual SSID in ISE 3.3

Sommario

Introduzione

Nel documento viene descritto come configurare ISE e risolvere i problemi relativi a BYOD.

Introduzione

BYOD è una funzione che permette agli utenti di integrare i propri dispositivi personali su ISE in modo che possano utilizzare le risorse di rete sull'ambiente. Consente inoltre all'amministratore di rete di impedire all'utente di accedere alla risorsa critica dai dispositivi personali.

A differenza del flusso guest, in cui il dispositivo viene autenticato con la pagina Guest tramite il punto vendita interno o Active Directory su ISE. Il BYOD consente all'amministratore di rete di installare un profilo dell'endpoint sull'endpoint per scegliere il tipo di metodo EAP. In scenari come EAP-TLS, il certificato client viene firmato dall'ISE stessa per creare un trust tra l'endpoint e ISE.

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- controller WLC
- Conoscenze base di ISE

Componente utilizzato

I dispositivi utilizzati non sono limitati a una particolare versione per il flusso BYOD:

- Catalyst 9800-CL Wireless Controller (17.12.3)
- ISE Virtual Machine (3.3)

Che cos'è Single SSID e Dual SSID BYOD su ISE?

Single SSID BYOD

In una configurazione BYOD a un solo SSID, gli utenti connettono i propri dispositivi personali direttamente alla rete wireless aziendale. Il processo di caricamento si verifica sullo stesso SSID, dove ISE semplifica la registrazione dei dispositivi, il provisioning e l'applicazione delle policy. Questo approccio semplifica l'esperienza dell'utente, ma richiede l'accesso sicuro e metodi di autenticazione appropriati per garantire la sicurezza della rete.

Doppio SSID BYOD

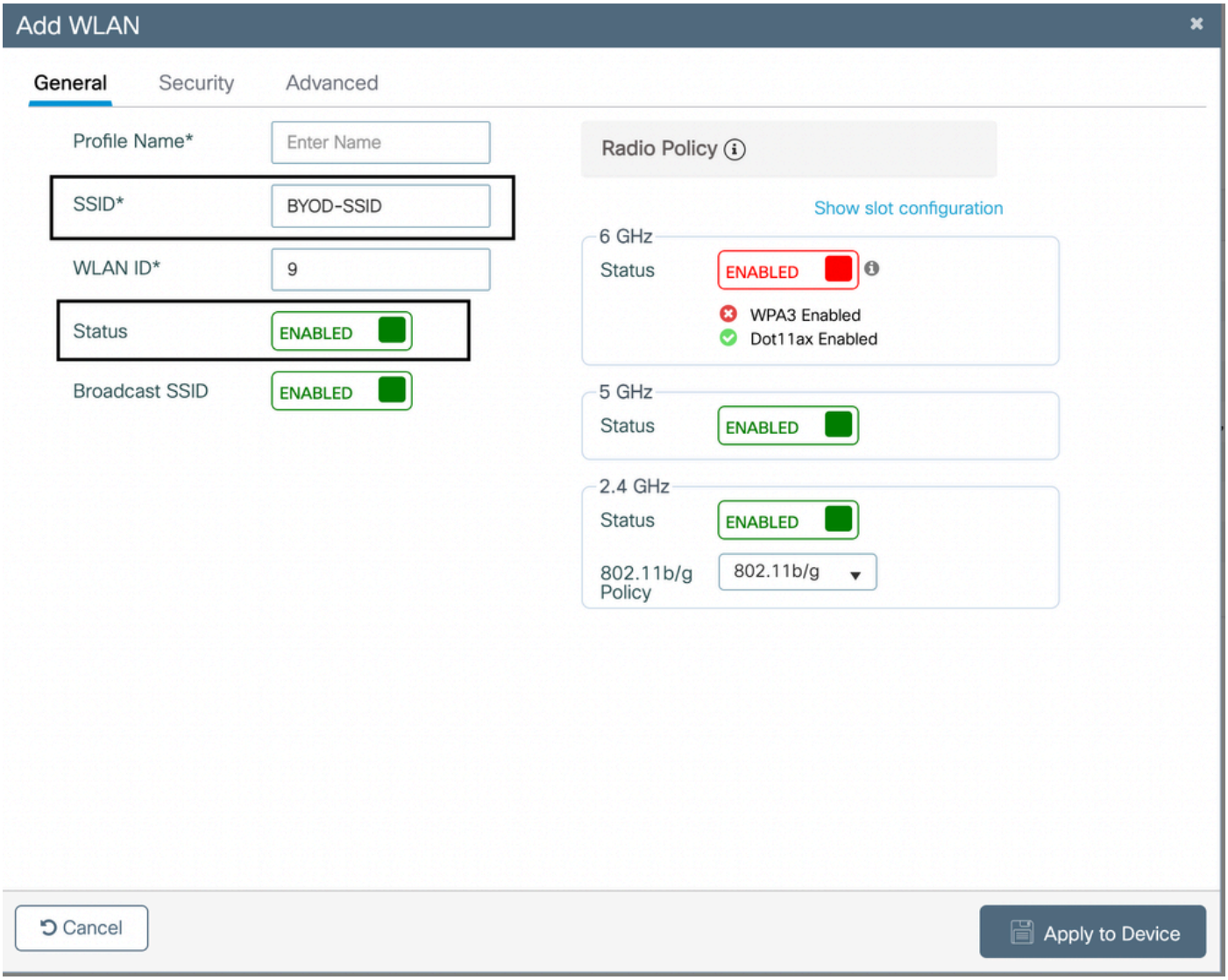
In una configurazione BYOD con due SSID, vengono utilizzati due SSID distinti: una per l'onboarding (accesso non protetto o limitato) e un'altra per accedere alla rete aziendale. Inizialmente gli utenti si connettono all'SSID caricato, completano la registrazione del dispositivo e il provisioning tramite ISE, quindi passano all'SSID aziendale sicuro per l'accesso alla rete. Questo fornisce un ulteriore livello di sicurezza separando il traffico in entrata dal traffico di produzione.

Configurazione WLC

Creazione di una WLAN per CWA

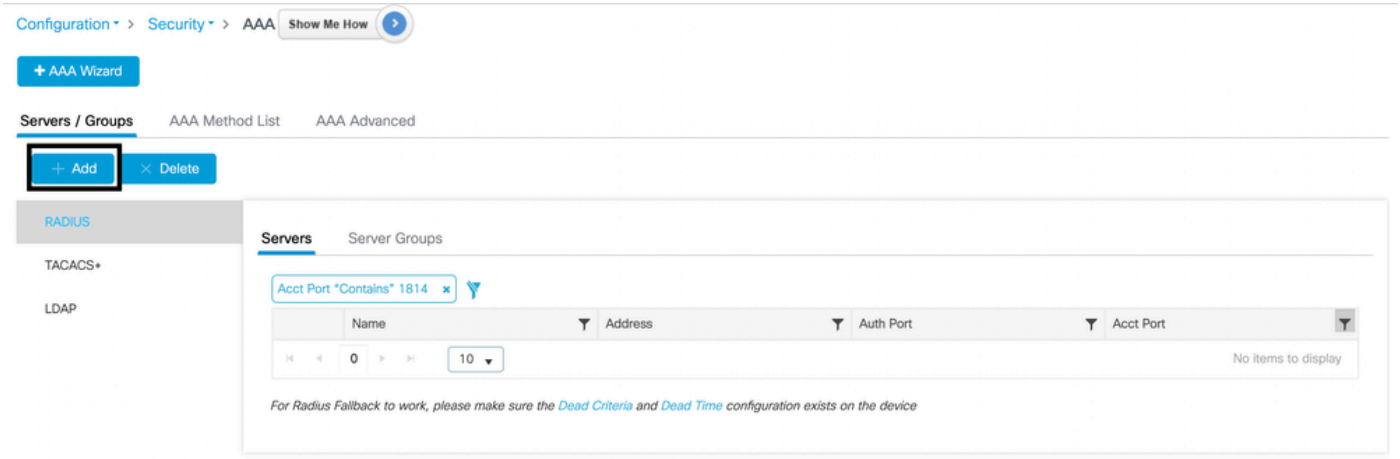
1. Selezionare Configurazione > Tag e profili > WLAN.
2. Fare clic su Add (Aggiungi) per creare una nuova WLAN.

    - Impostare un nome WLAN e un SSID (ad esempio, BYOD-WiFi).
    - Abilitare la WLAN.

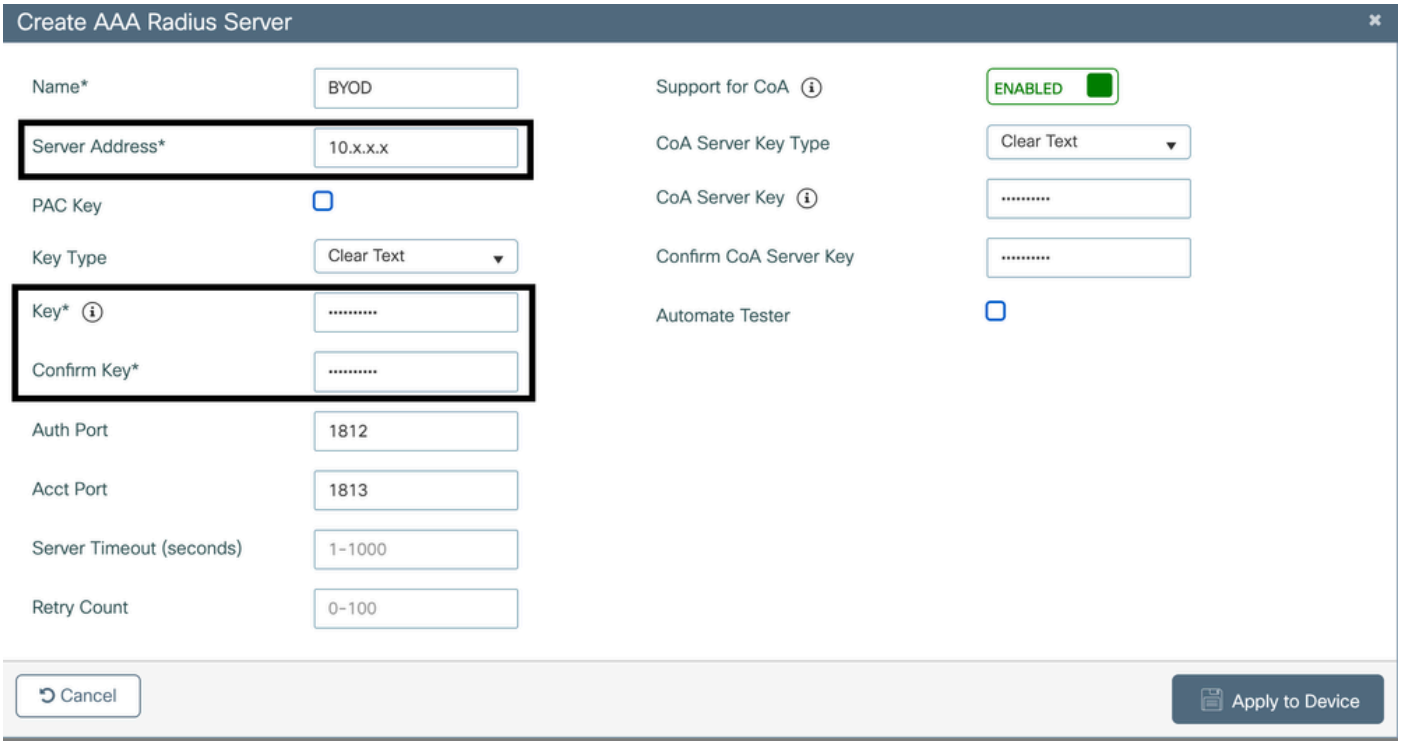


Configurazione server RADIUS

1. Selezionare Configurazione > Sicurezza > AAA > RADIUS > Server.

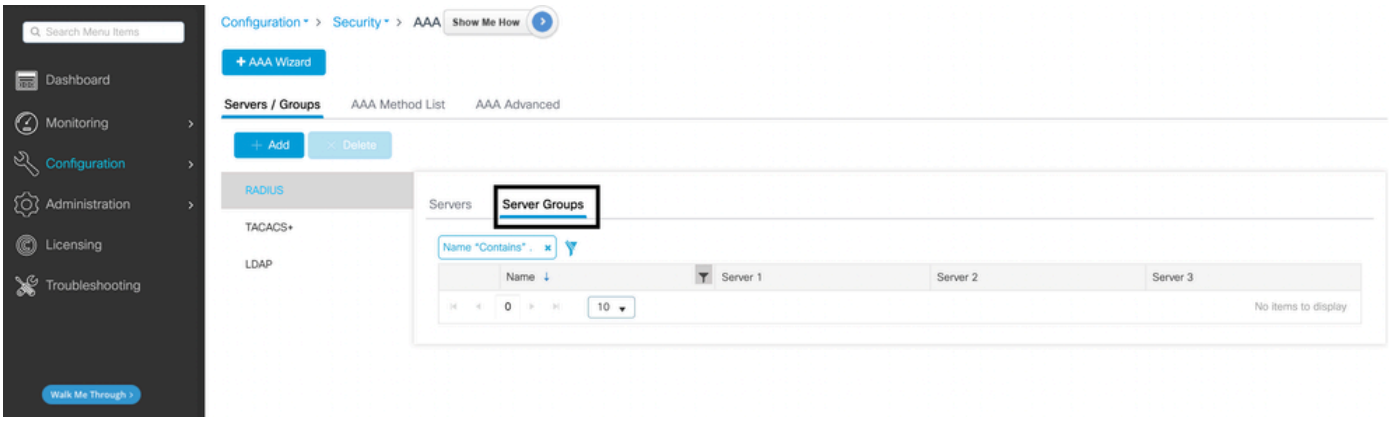


2. Fare clic su Add (Aggiungi) per configurare ISE come server RADIUS:
    - IP server: Indirizzo IP dell'ISE.
    - Segreto condiviso: Trova la corrispondenza con il segreto condiviso configurato su ISE.

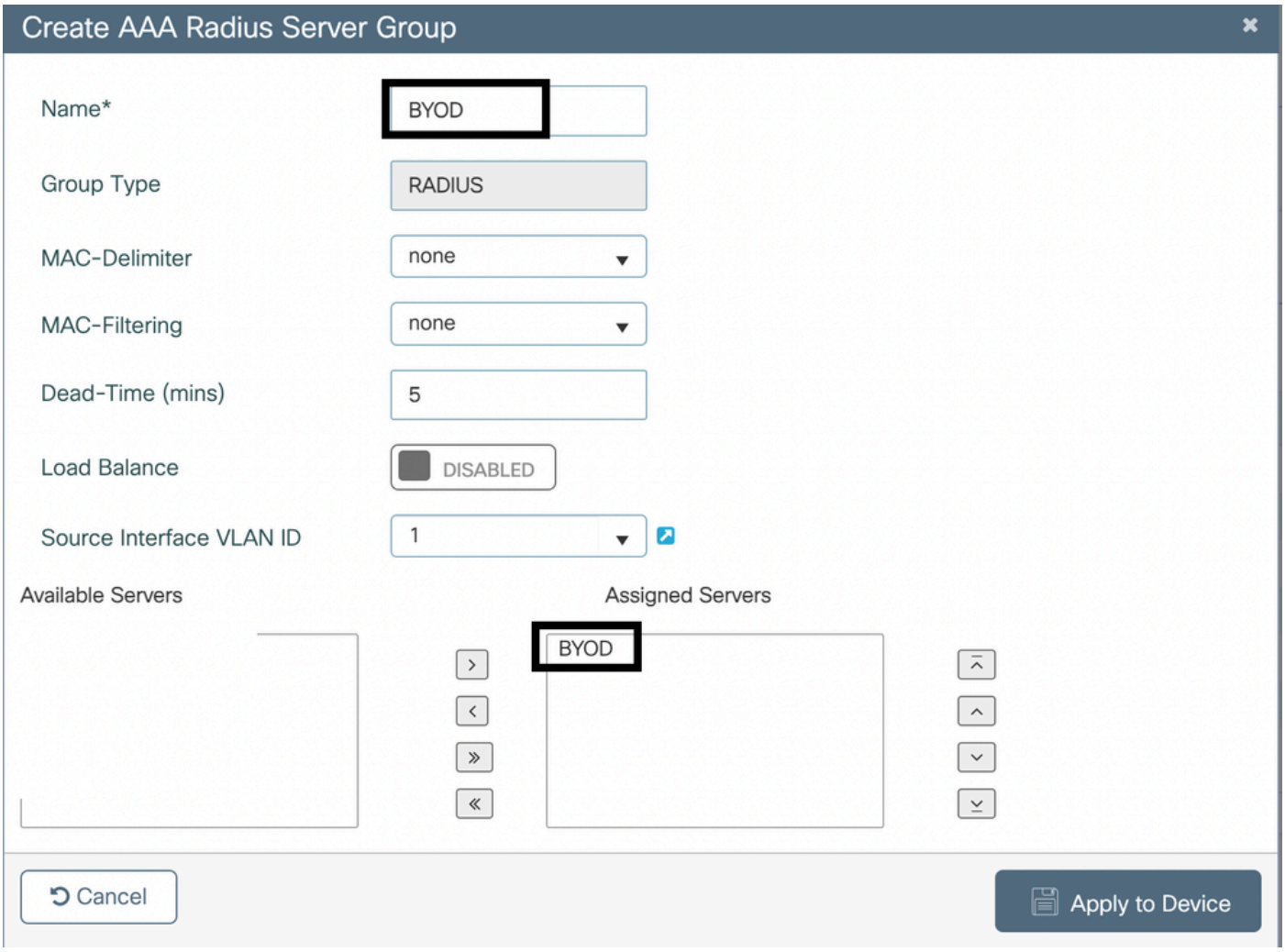


Configurazione dei server AAA

1. Passare a Configurazione > Sicurezza > AAA > Server/Gruppi.



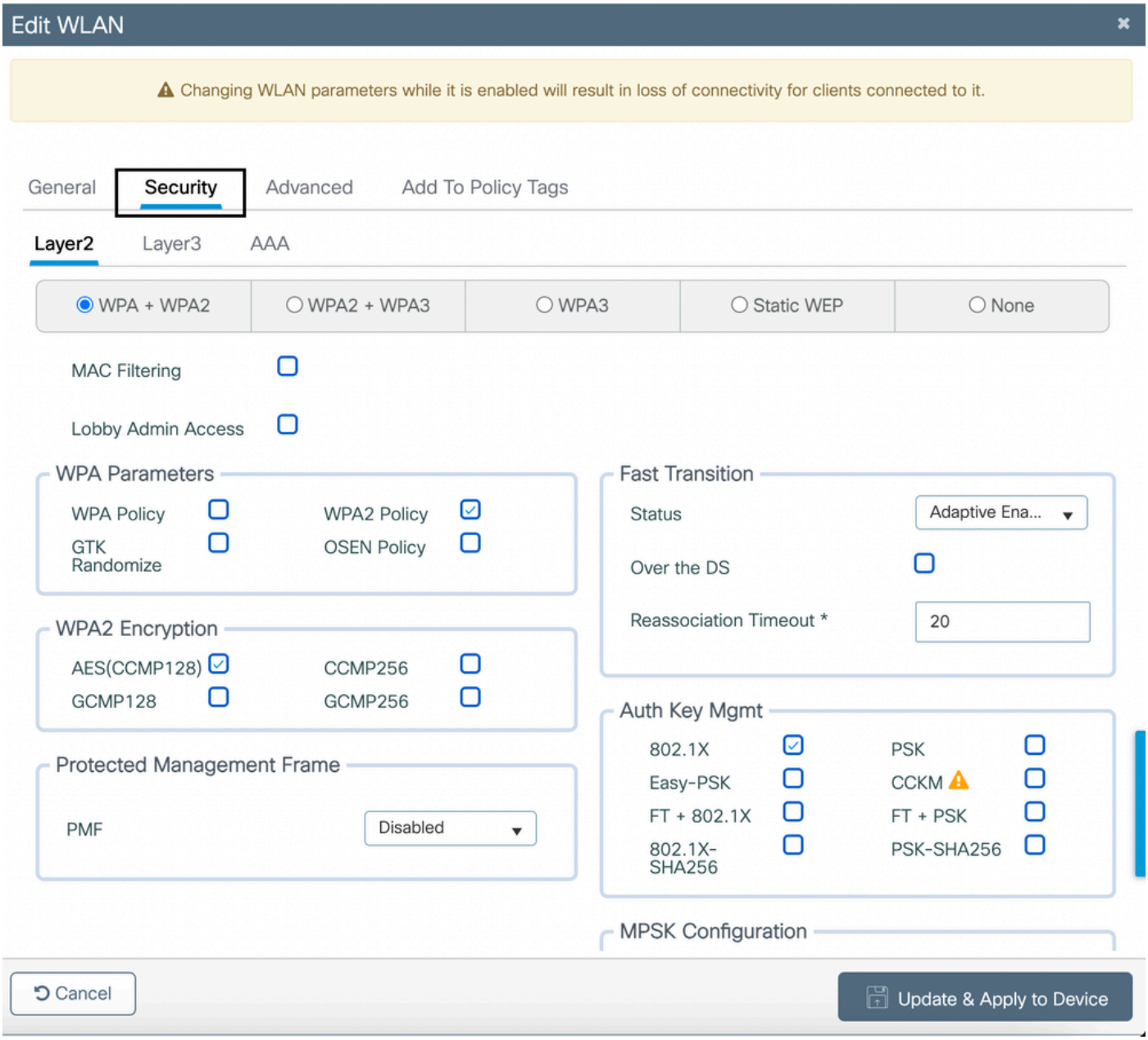
2. Assegnare il server RADIUS a un gruppo di server nuovo o esistente.



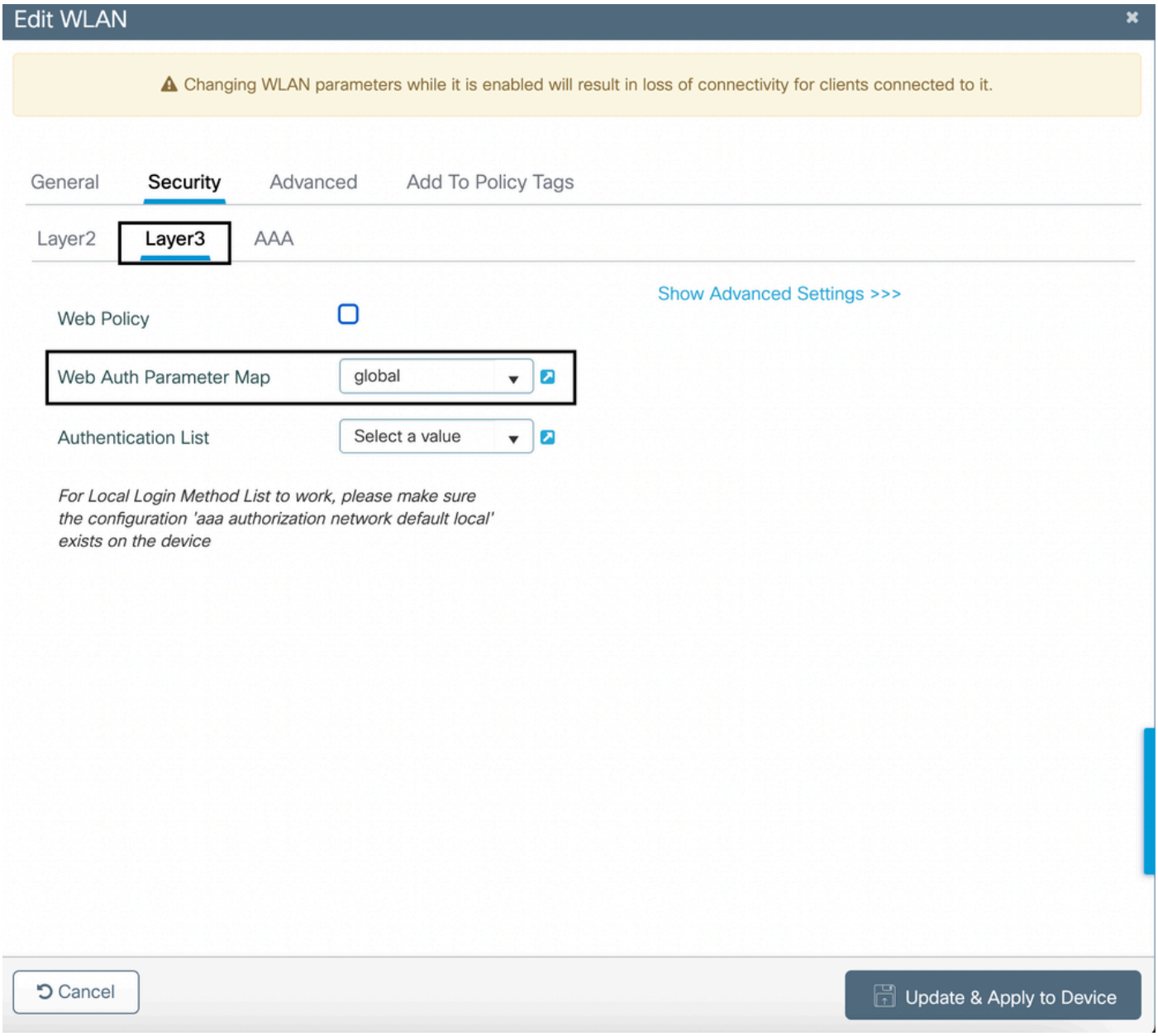
Configurazione dei criteri di sicurezza per la WLAN

1. Selezionare Configurazione > Tag e profili > WLAN. Modificare la WLAN creata in precedenza.

2. Nella scheda Protezione > Livello 2:
   - Abilita WPA+WPA2
   - Impostazione di AES(CCMP128) con la crittografia WPA2
   - Gestione chiavi di autenticazione come 802.1X



3. Nella scheda Protezione > Livello 3, selezionare globale dall'elenco a discesa Mappa parametri autenticazione Web.



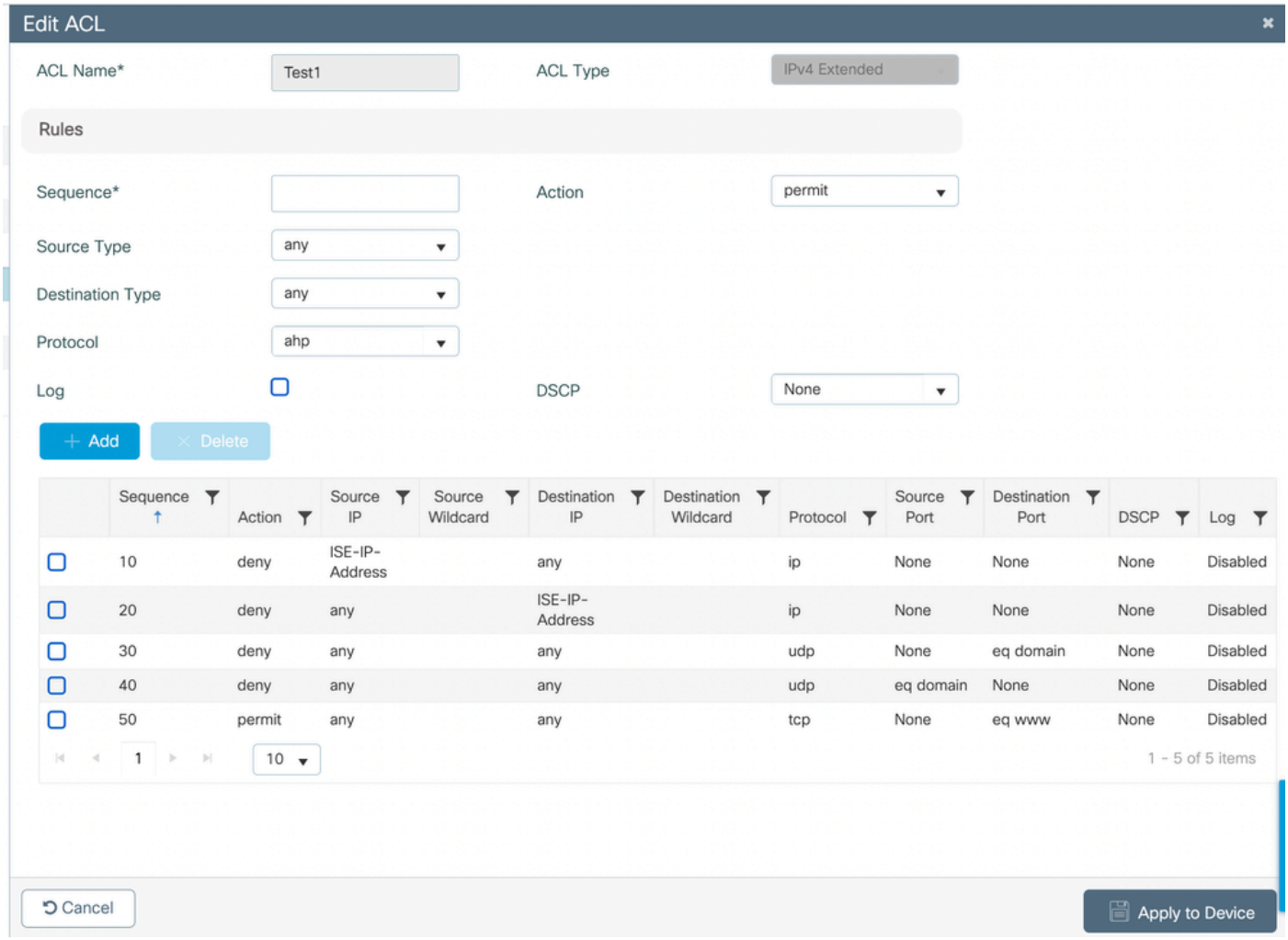
Configurazione dell'ACL di preautenticazione

Creare un ACL per consentireUsa azioni per il reindirizzamento:

- traffico DNS.
- HTTP/HTTPS sul portale ISE.
- Tutti i servizi back-end necessari.

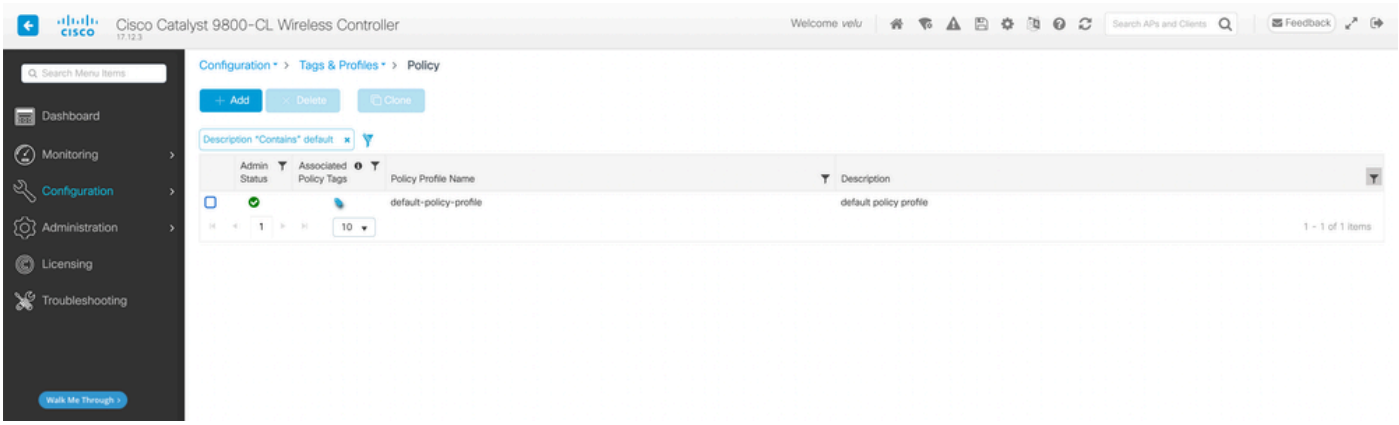
A tale scopo:

1. Selezionare Configurazione > Sicurezza > ACL > Access Control Lists.
2. Creare un nuovo ACL con le regole per autorizzare il traffico necessario.

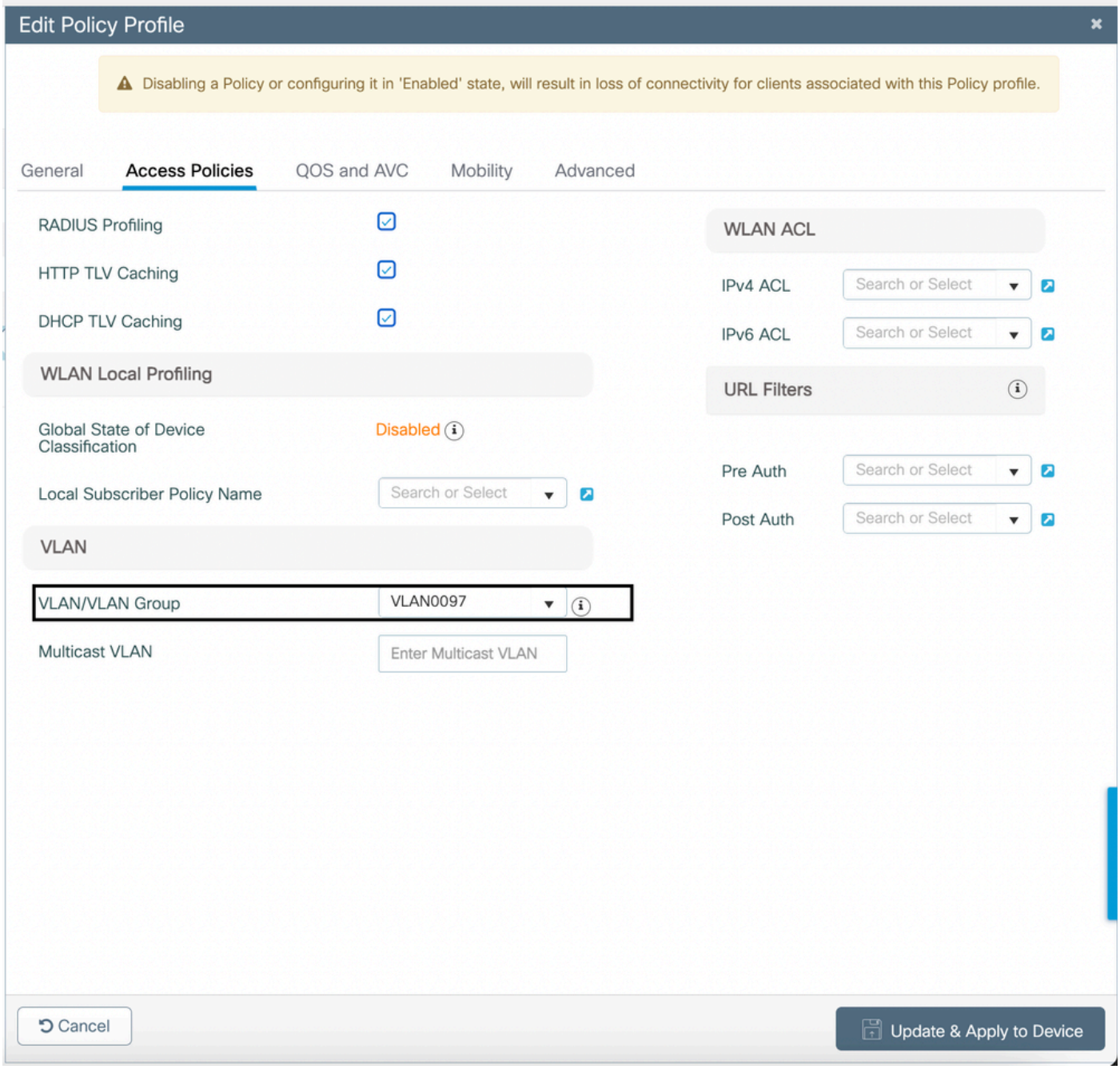


Configura profilo criteri

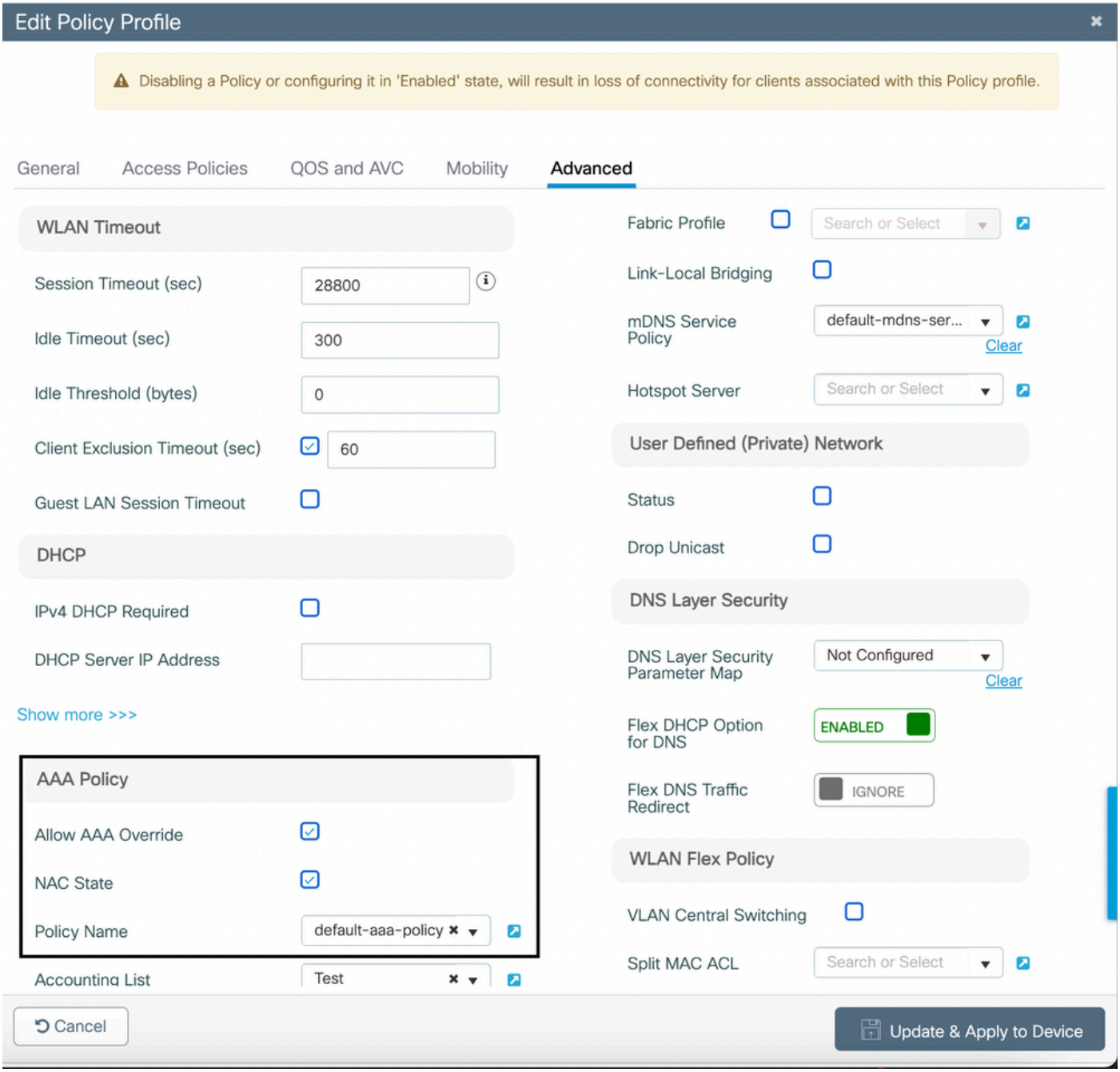
1. Selezionare Configurazione > Tag e profili > Criterio. È possibile creare o utilizzare il criterio predefinito



2. Assegnare la VLAN appropriata in Criteri di accesso

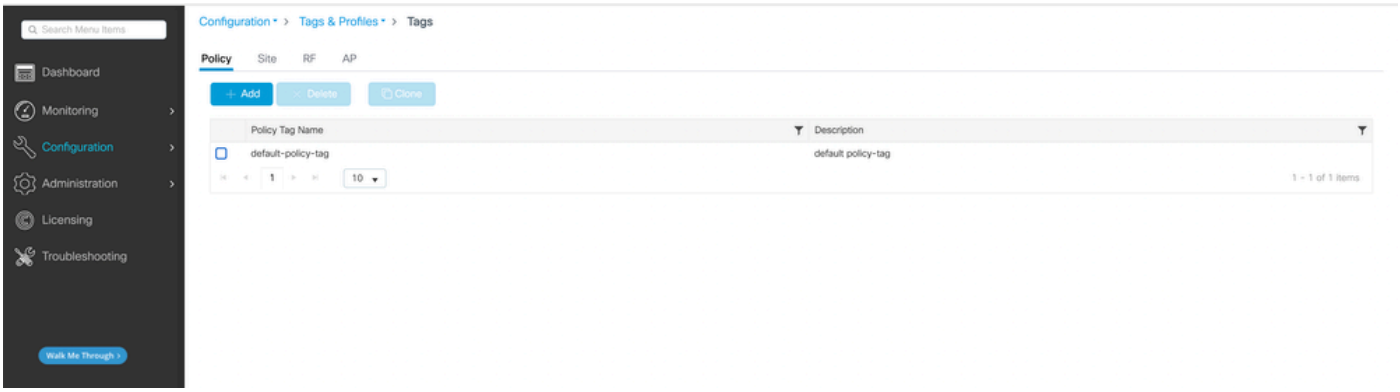


3. Abilitare anche Consenti sostituzione AAA e stato NAC in Avanzate del criterio.



Applica tag e distribuisci

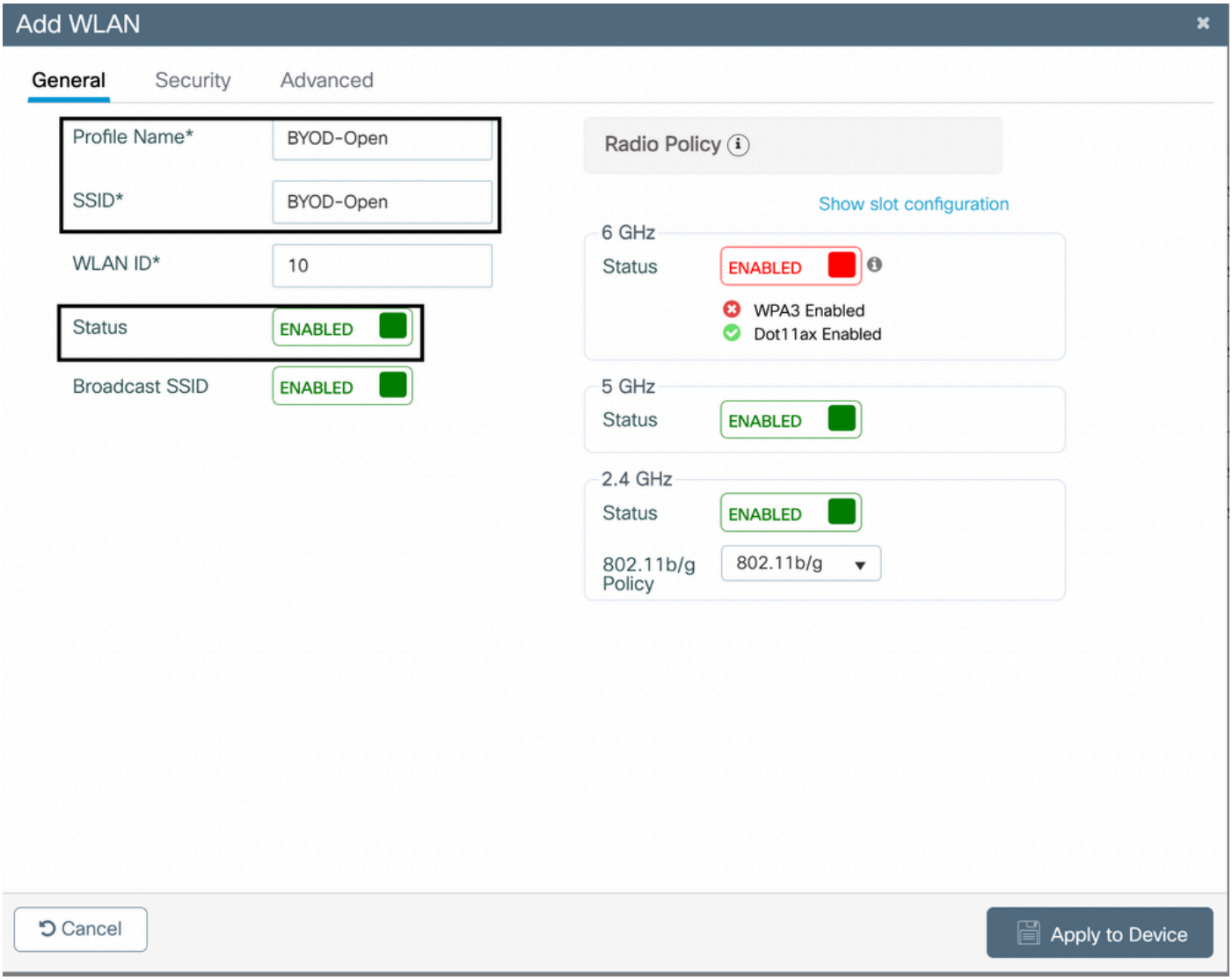
- Selezionare Configurazione > Tag e profili > Tag.
- Creare o modificare un tag per includere il profilo WLAN e delle policy.
- Assegnare il tag ai punti di accesso.



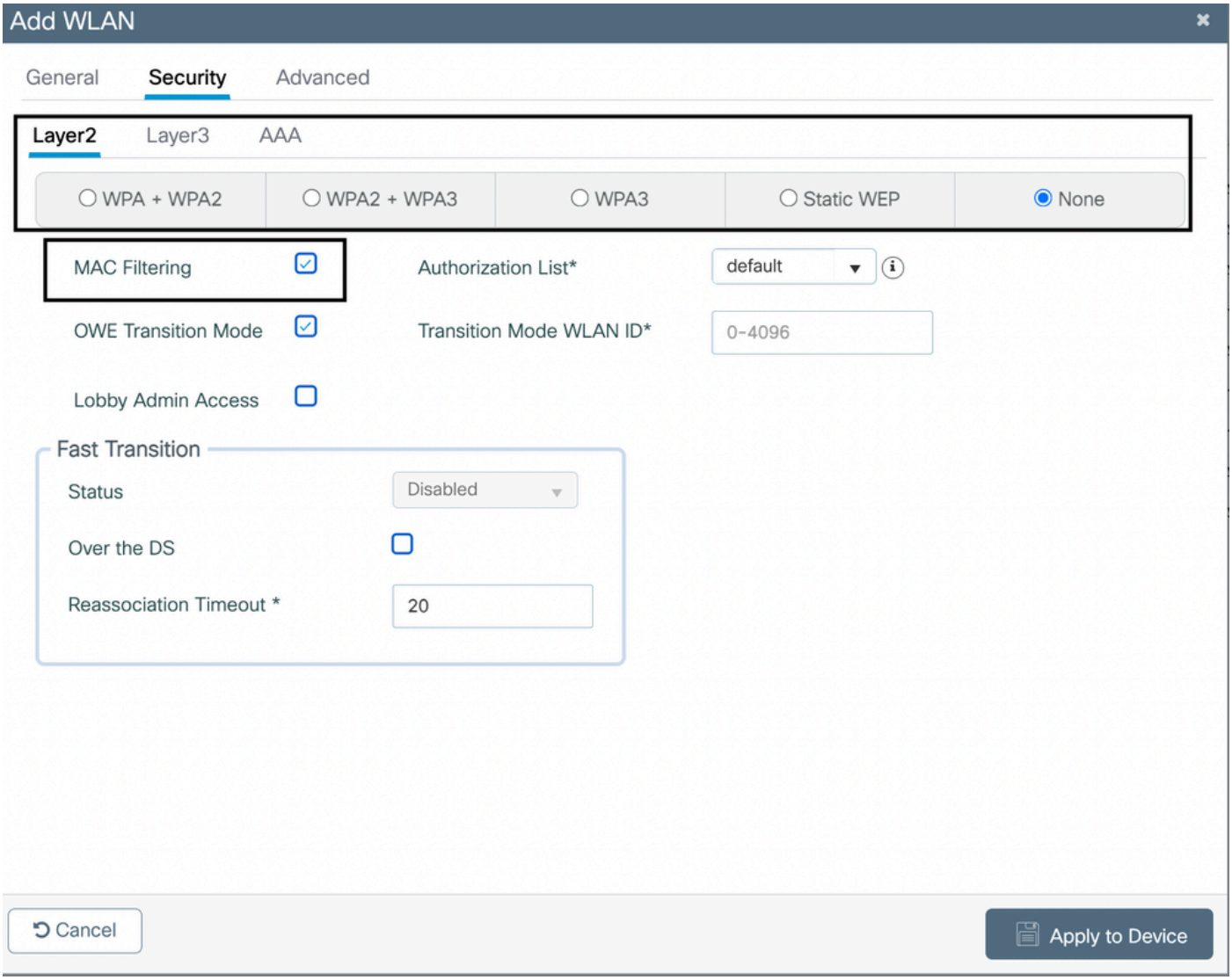
Configurare un SSID aperto/non protetto

Open SSID viene creato solo quando si decide di avere una configurazione BYOD a doppio SSID nel proprio ambiente.

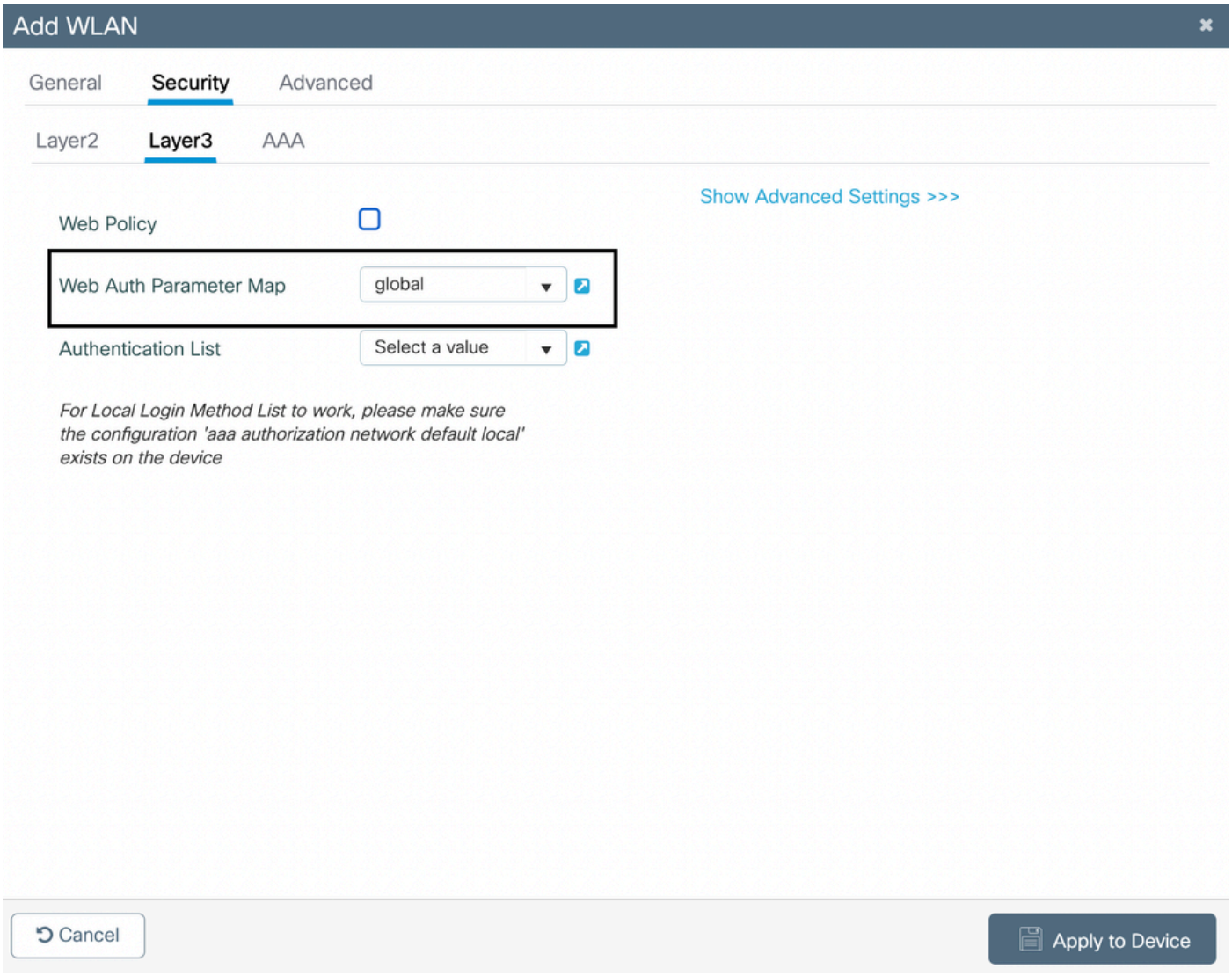
1. Selezionare Configurazione > Tag e profili > WLAN. Fare clic sul pulsante Aggiungi.
2. Specificare un nome SSID nella scheda Generale e abilitare il pulsante WLAN.



3. Fare clic sulla scheda Protezione nella stessa finestra. Selezionare il pulsante di scelta Nessuno e abilitare il filtro Mac.



4. Nel layer 3, in Protezione, selezionare l'impostazione globale per Mappa parametri autenticazione Web. Se sul WLC è configurato un altro profilo di autenticazione Web, è possibile mapparlo anche qui:



Configurazione di ISE

Prerequisiti

- Verificare che Cisco ISE sia installato e concesso in licenza per la funzionalità BYOD.
- Aggiungere il WLC all'ISE come dispositivo di rete con il segreto condiviso RADIUS.

Certificati

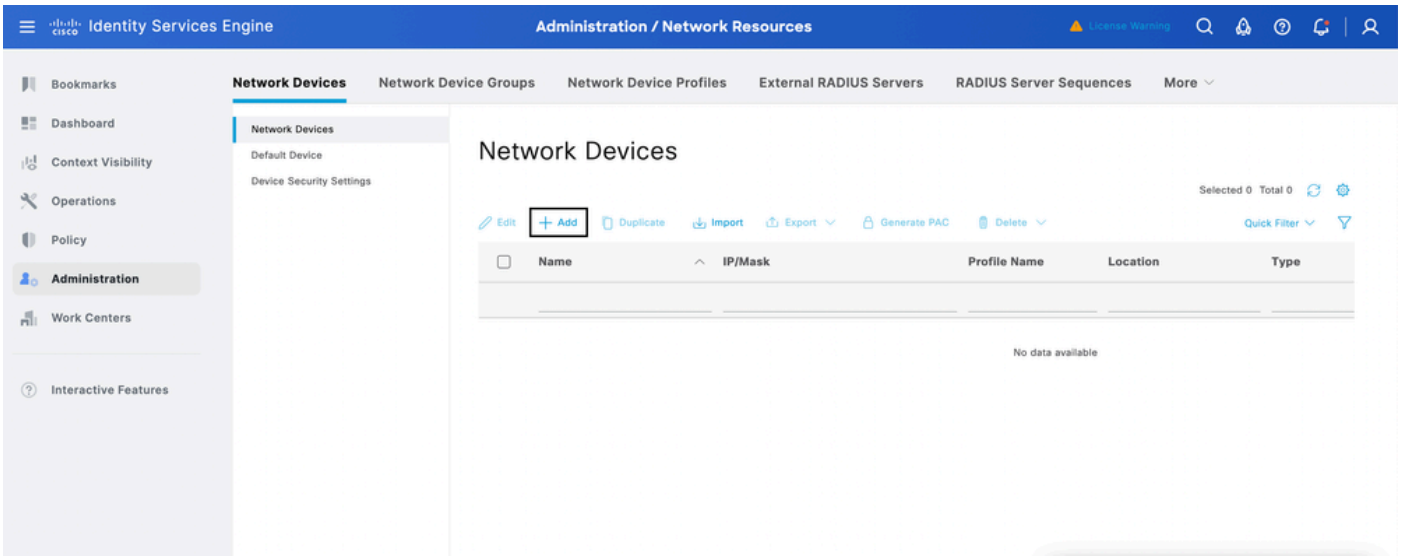
- Installare un certificato server valido su ISE per evitare la visualizzazione di avvisi di protezione del browser.
- Verificare che il certificato sia considerato attendibile dagli endpoint (firmati da una CA nota o da una CA interna con radice attendibile).

Configurazione DNS

- Accertarsi che il DNS risolva il nome host ISE per il portale BYOD.

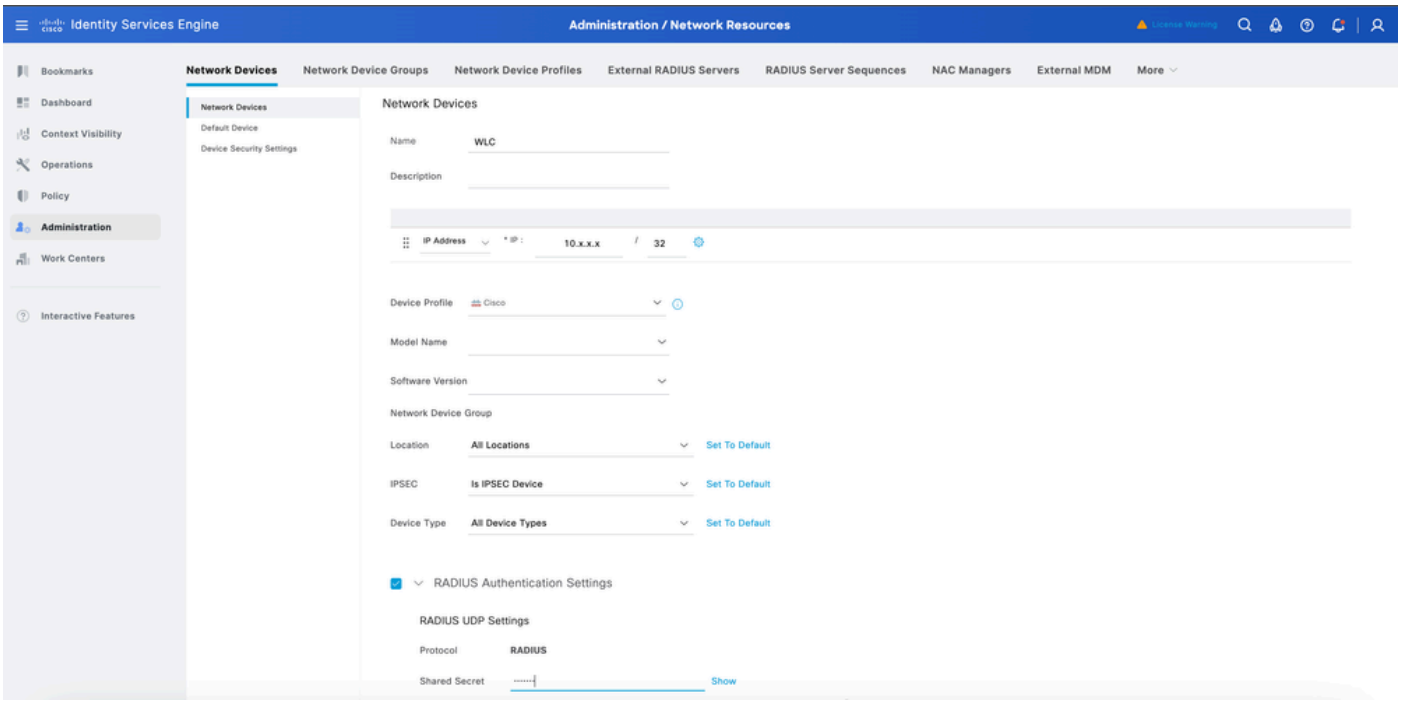
Configura dispositivo di rete ISE

1. Accedere all'interfaccia utente Web di ISE.
2. Selezionare Amministrazione > Risorse di rete > Dispositivi di rete.



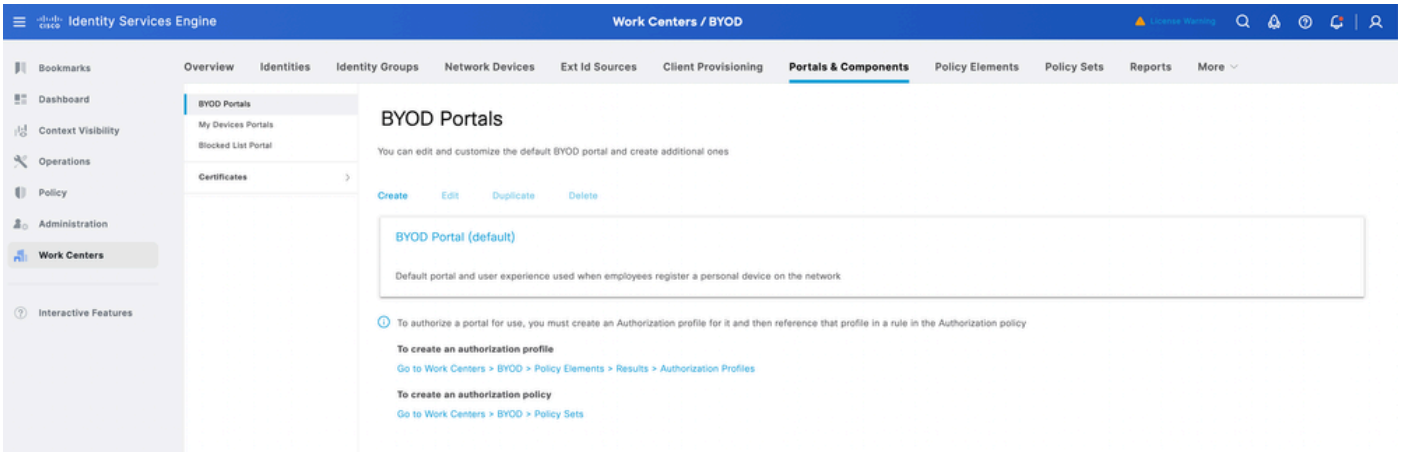
3. Aggiungere il WLC come dispositivo di rete:

- Nome: Immettere un nome per il WLC.
- Indirizzo IP: Immettere l'IP di gestione WLC.
- Segreto condiviso RADIUS: Immettere lo stesso segreto condiviso configurato sul WLC.
- Fare clic su Invia.



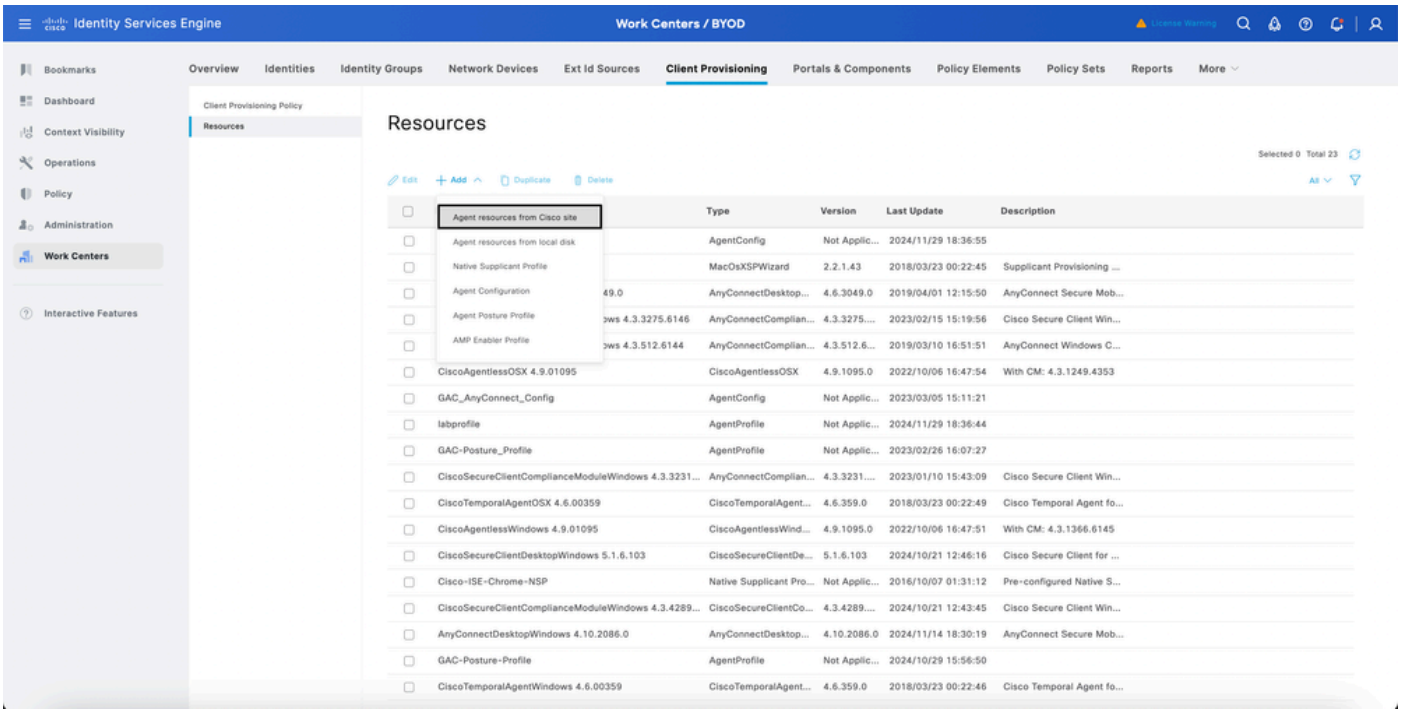
Creazione di un portale BYOD

1. Passare a Centri di lavoro > BYOD > Impostazioni > Portali e componenti > Portali BYOD.
2. Fare clic su Add (Aggiungi) per creare un portale BYOD o è possibile utilizzare il portale predefinito esistente su ISE.



Scarica l'ultima versione di Cisco IOS®

1. Passare a Centri di lavoro > BYOD > Provisioning client > Risorse.
2. Fare clic sul pulsante Add (Aggiungi) e selezionare le risorse agente dal sito Cisco.



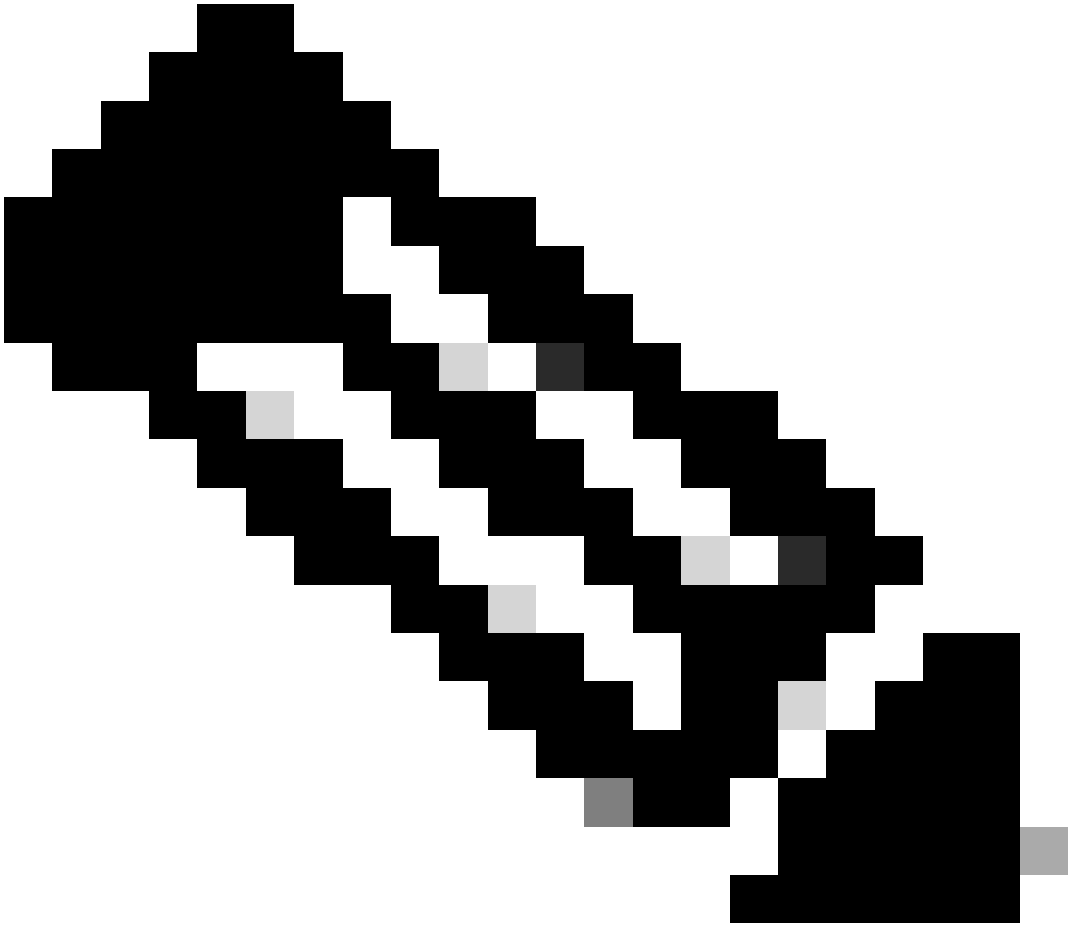
3. Nell'elenco del software, selezionare la versione più recente di Cisco IOS da scaricare.

Download Remote Resources

	Name	Description
☐	MacOsXSPWizard 2.7.0.1	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	MacOsXSPWizard 3.1.0.1	Supplicant Provisioning Wizard for MAC OSX Version 3.1.0.1
☐	MacOsXSPWizard 3.1.0.2	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	MacOsXSPWizard 3.2.0.1	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	MacOsXSPWizard 3.4.0.0	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	WinSPWizard 3.0.0.2	Supplicant Provisioning Wizard for Windows (ISE 2.x and Above)
☑	WinSPWizard 3.0.0.3	Supplicant Provisioning Wizard for Windows (ISE 2.x and Above)

For Agent software, please download from http://cisco.com/go/ciscosecureclient. Use the "Agent resource from local disk" add option, to import into ISE

Cancel Save

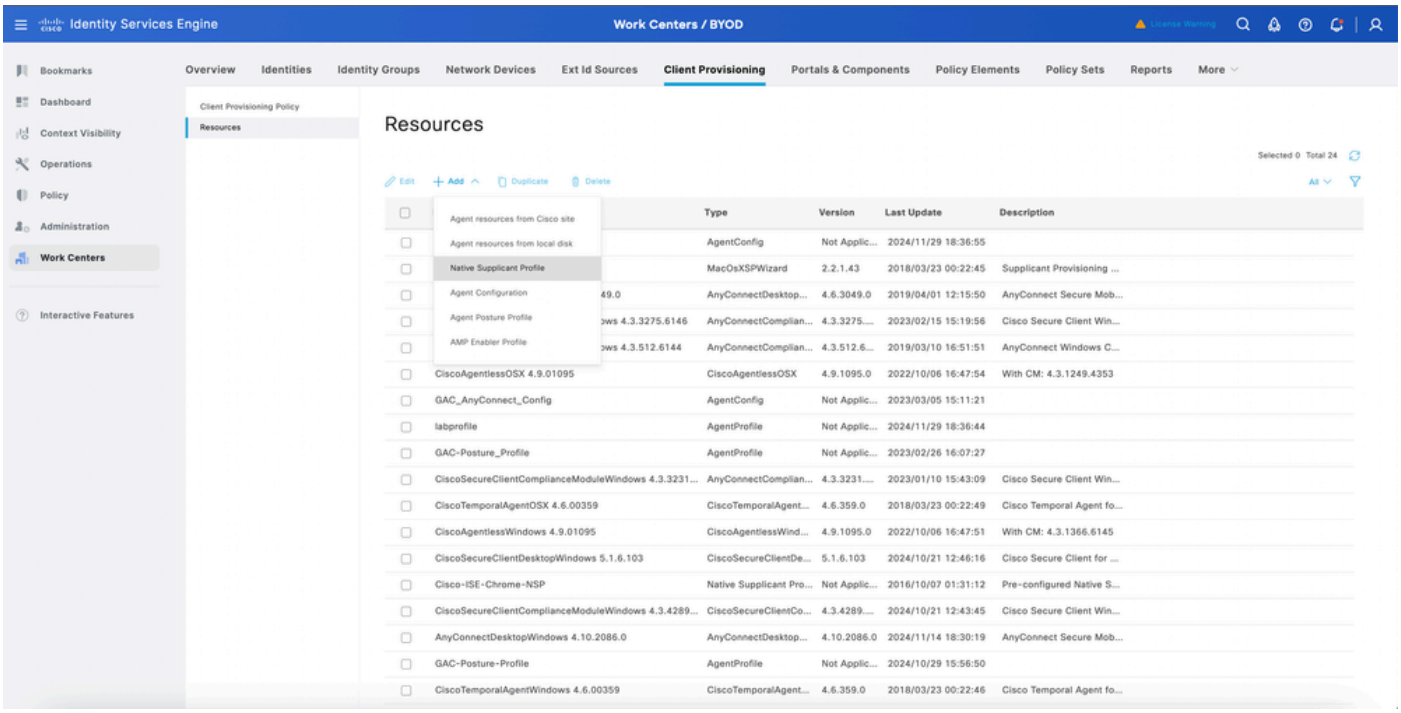


Nota: Il software Cisco IOS viene scaricato sull'ISE per gli endpoint Windows e MacOS. Per Apple iPhone IOS, utilizza un supplicant nativo per effettuare il provisioning del dispositivo e Per il dispositivo android, si dispone di Network setup assistant che deve essere scaricato da Play Store.

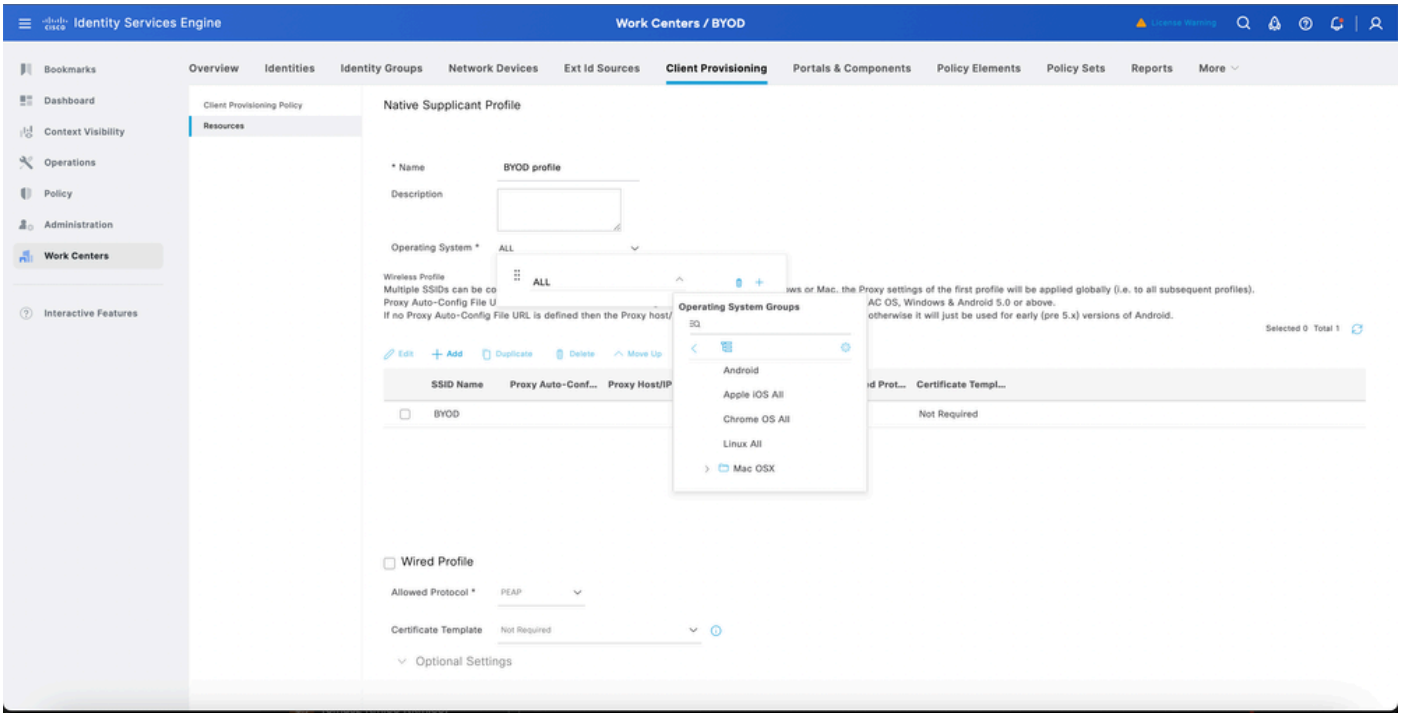
Creazione di un profilo di endpoint

1. Passare a Centri di lavoro > BYOD > Provisioning client > Risorse.

2. Fare clic su Aggiungi, quindi selezionare Profilo supplicant nativo dal menu a discesa.



3. Sotto l'elenco a discesa Sistema operativo, selezionare il sistema operativo richiesto che si desidera incorporare il dispositivo o impostarlo come ALL per tutti gli endpoint presenti nell'ambiente:



4. Fare clic su Add dalla pagina per creare il profilo dell'endpoint e configurare 802.1X per l'endpoint:

Wireless Profile(s)

SSID Name * BYOD

Proxy Auto-Config File URL

Proxy Host/IP

Proxy Port

Security * WPA2 Enterprise

Allowed Protocol * PEAP

Certificate Template Not Required

Optional Settings

Windows Settings

Authentication Mode User or Computer

- [ ] Automatically use logon name and password (and domain if any)
- [x] Enable fast reconnect
- [ ] Enable quarantine checks
- [ ] Disconnect if server does not present cryptobinding TLV
- [ ] Do not prompt user to authorize new servers or trusted certification authorities
- [x] Connect even if the network is not broadcasting its name (SSID)

iOS Settings

- [ ] Enable if target network is hidden

Android Settings

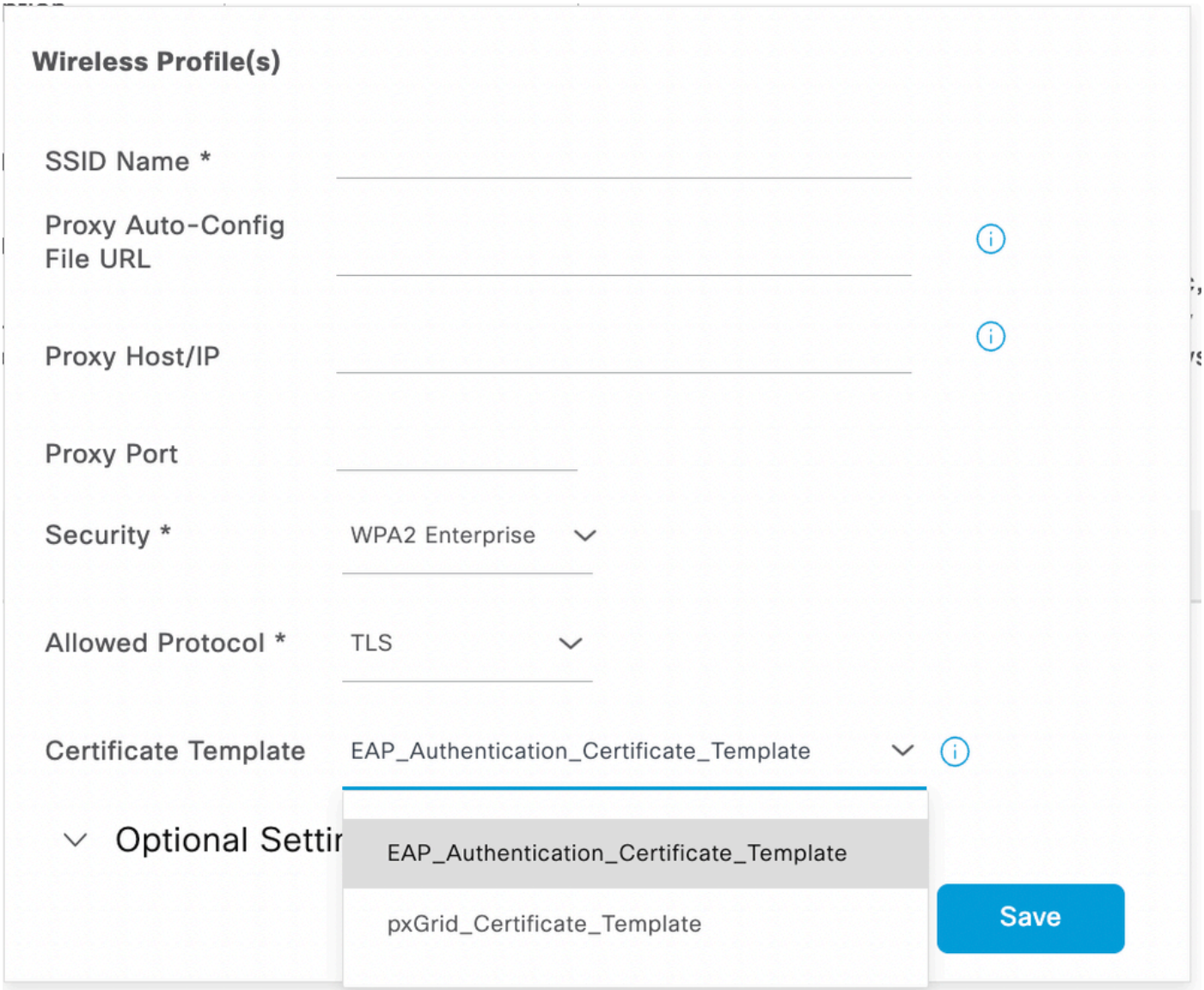
Certificate Enrollment Protocol:

A seconda delle esigenze, configurare il profilo dell'endpoint per l'endpoint nell'ambiente. Il profilo degli endpoint consente di configurare EAP-PEAP, EAP-TLS.

5. Fare clic su Save, quindi su Submit (Invia) nel profilo dell'endpoint.

Modello di certificato

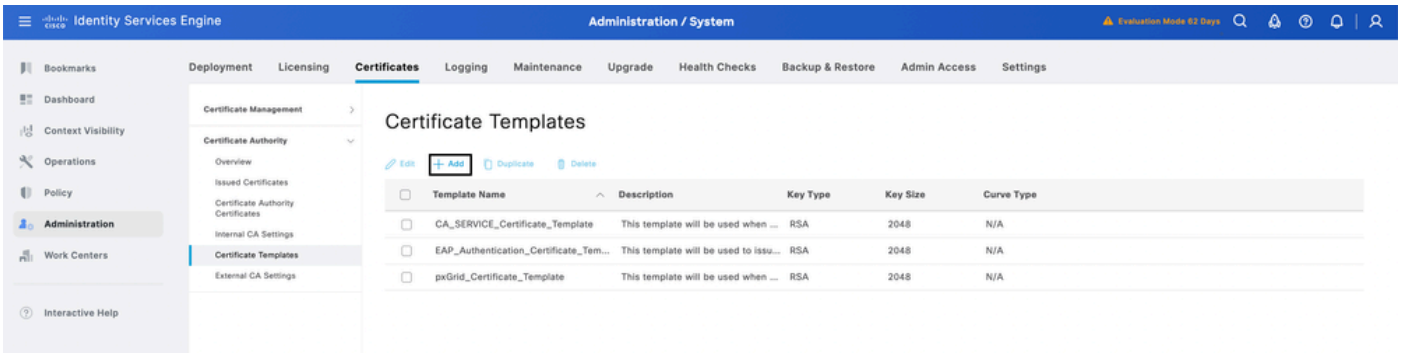
Il profilo dell'endpoint è preconfigurato per eseguire EAP-TLS. È necessario aggiungere un modello di certificato al profilo. Per impostazione predefinita, ISE ha due modelli predefiniti che possono essere scelti dal menu a discesa.



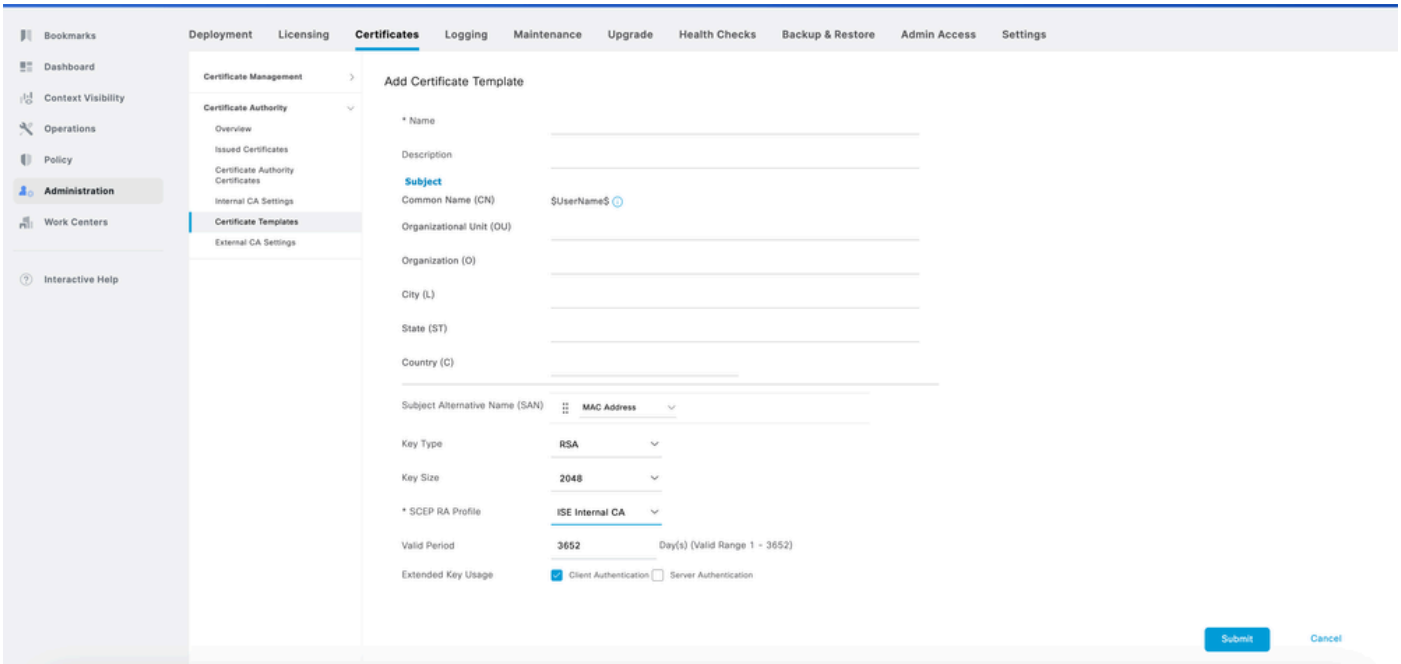
Per creare un nuovo modello di certificato, eseguire la procedura seguente:

1. Passare a Amministrazione > Sistema > Certificati > Autorità di certificazione > Modelli di certificato.

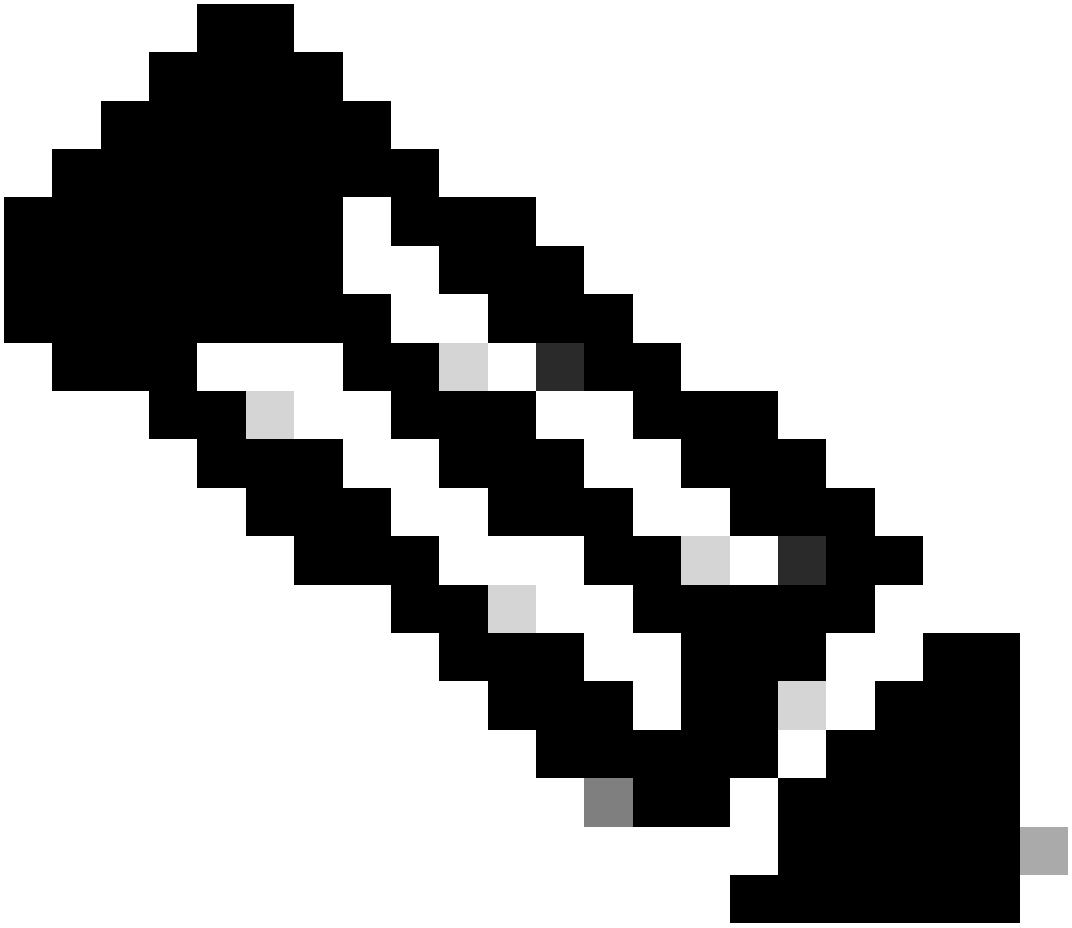
2. Fare clic sul pulsante Aggiungi nella pagina.



3. Inserire i dettagli adatti alle esigenze specifiche dell'organizzazione.



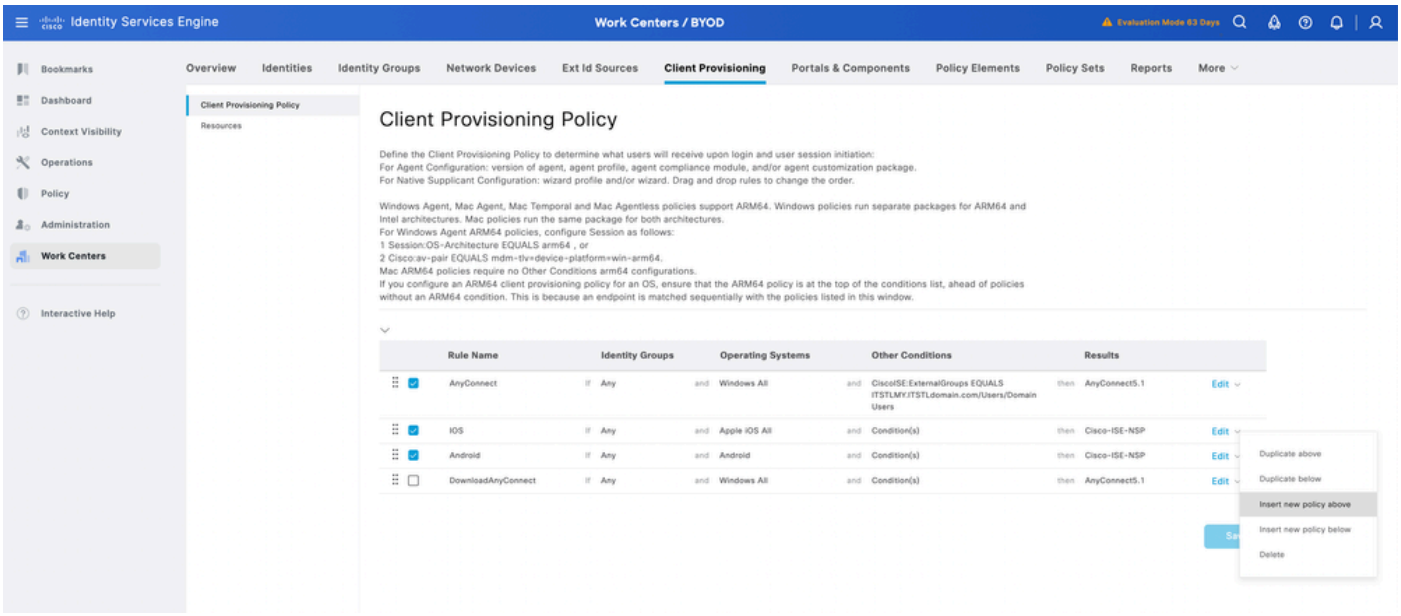
4. Fare clic su Sottometti per salvare le modifiche.



Nota: Il modello di certificato può essere utile in scenari in cui sono presenti domini diversi e l'utente viene segmentato aggiungendo un valore diverso nell'unità organizzativa del certificato.

Mappare un profilo di endpoint al portale di provisioning client

1. Passare a Centri di lavoro > BYOD > Provisioning client > Criteri di provisioning client.
2. Fare clic su v in una delle regole per creare una nuova regola di provisioning client.

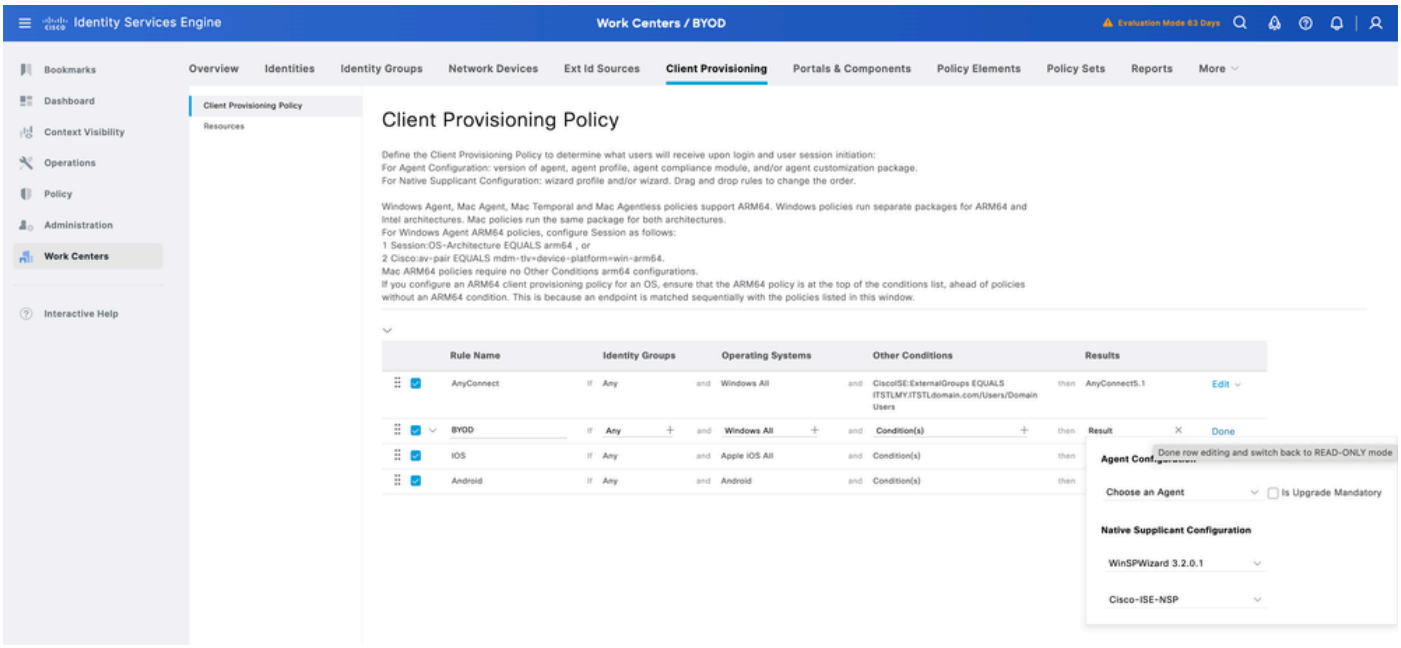


3. Contabilizzazione della creazione della nuova regola nella pagina

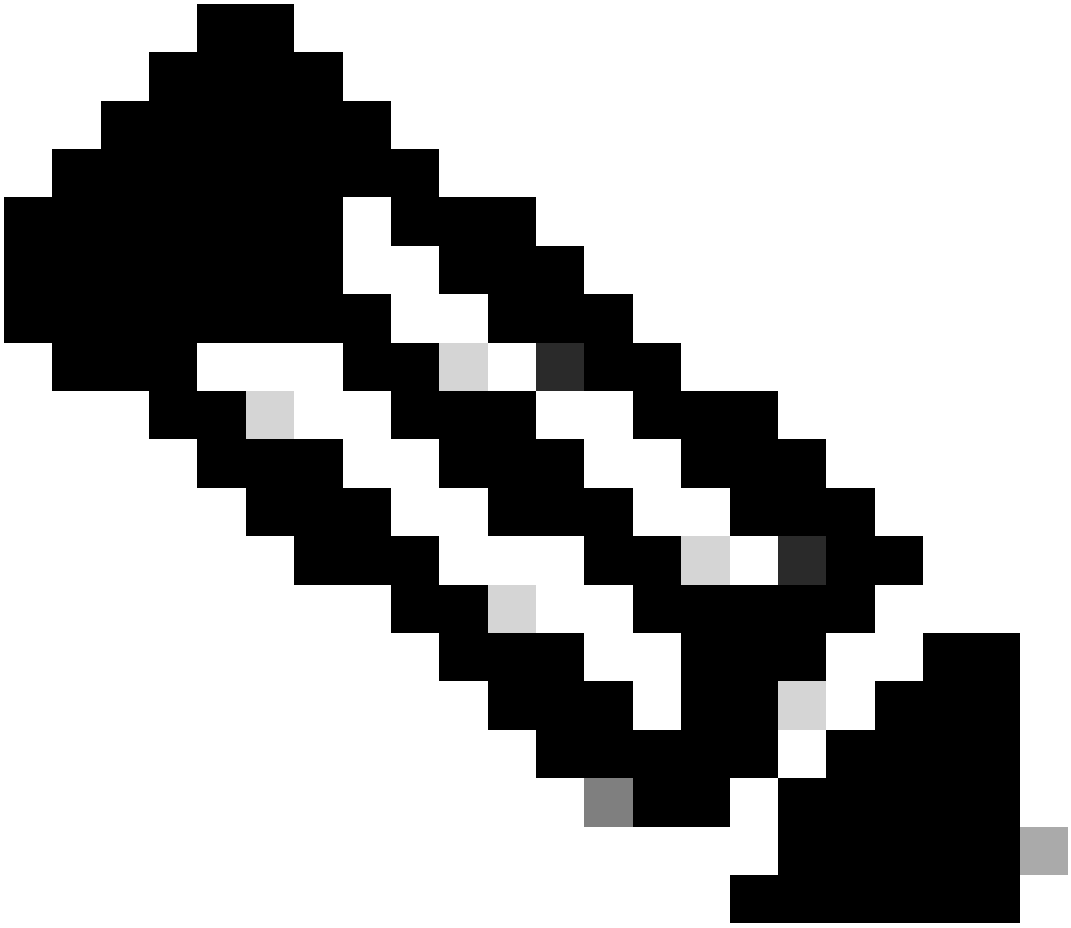
4. Aggiungere il gruppo di identità se si desidera limitare l'utilizzo del portale BYOD a determinati utenti

5. Aggiungere il sistema operativo che si desidera avere accesso al portale BYOD

6. Mappare la versione di Cisco IOS dall'elenco a discesa e selezionare anche il profilo dell'endpoint creato dal risultato



7. Fare clic su Fine, quindi sul pulsante Salva.

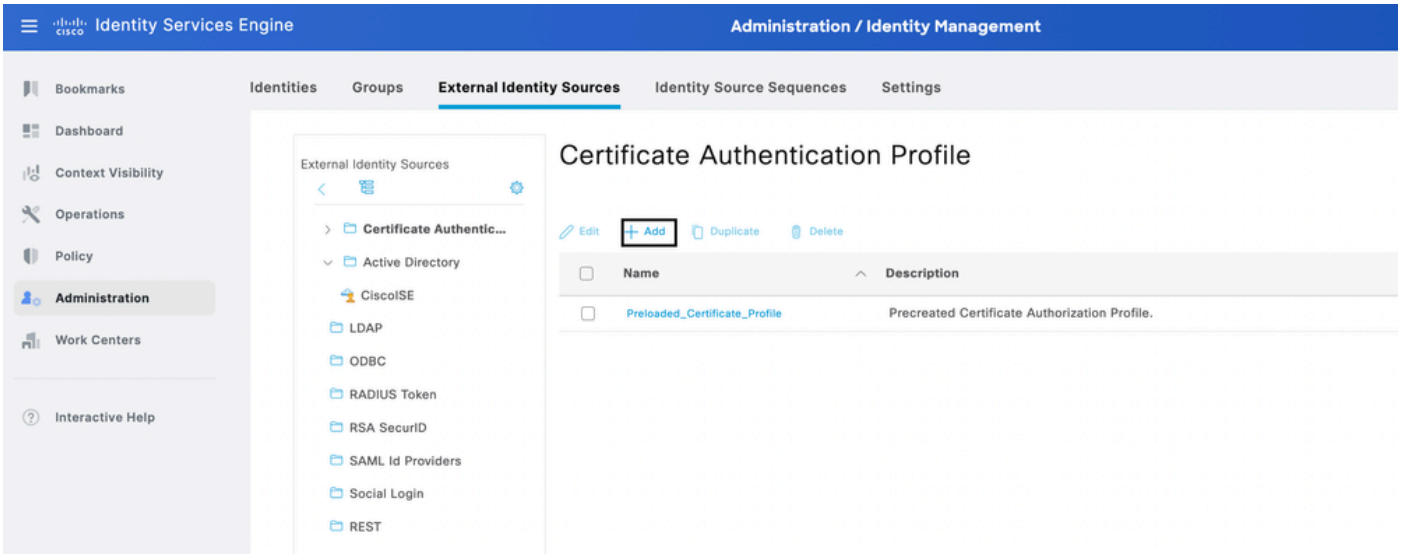


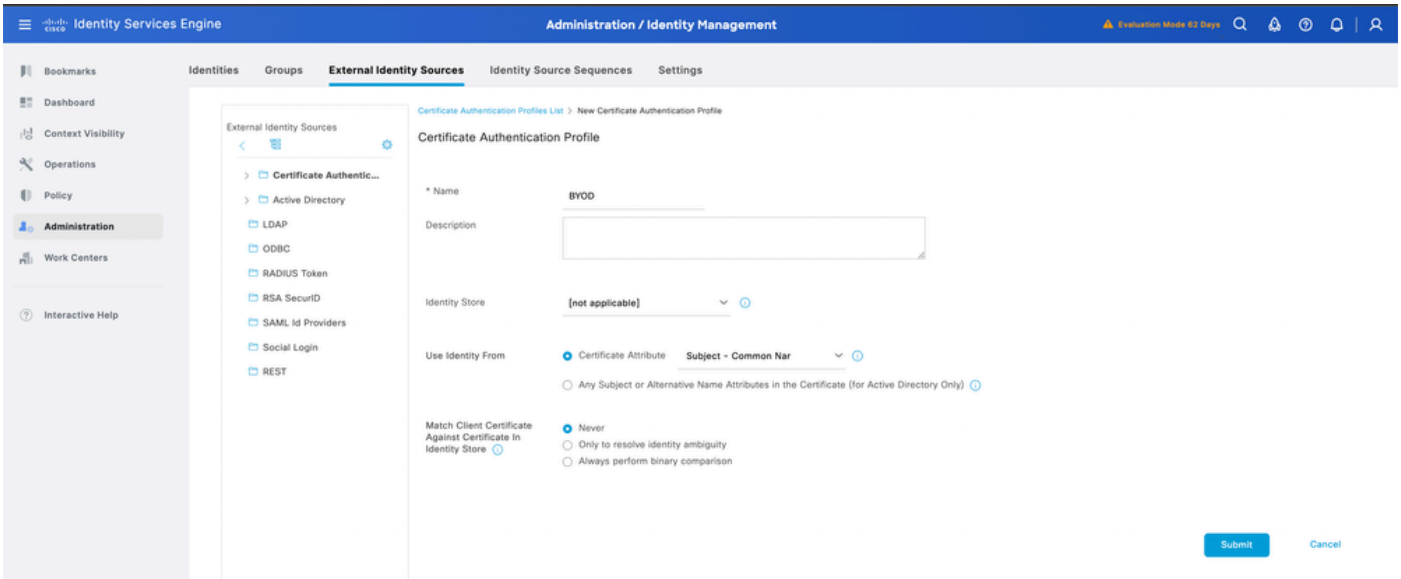
Nota: Questo criterio influisce sia sul provisioning del client di postura che sul provisioning BYOD, dove la sezione Configurazione agente determina l'agente di postura e il modulo di conformità applicati per i controlli di postura, mentre la sezione Configurazione richiedente nativo gestisce le impostazioni per i flussi di provisioning BYOD

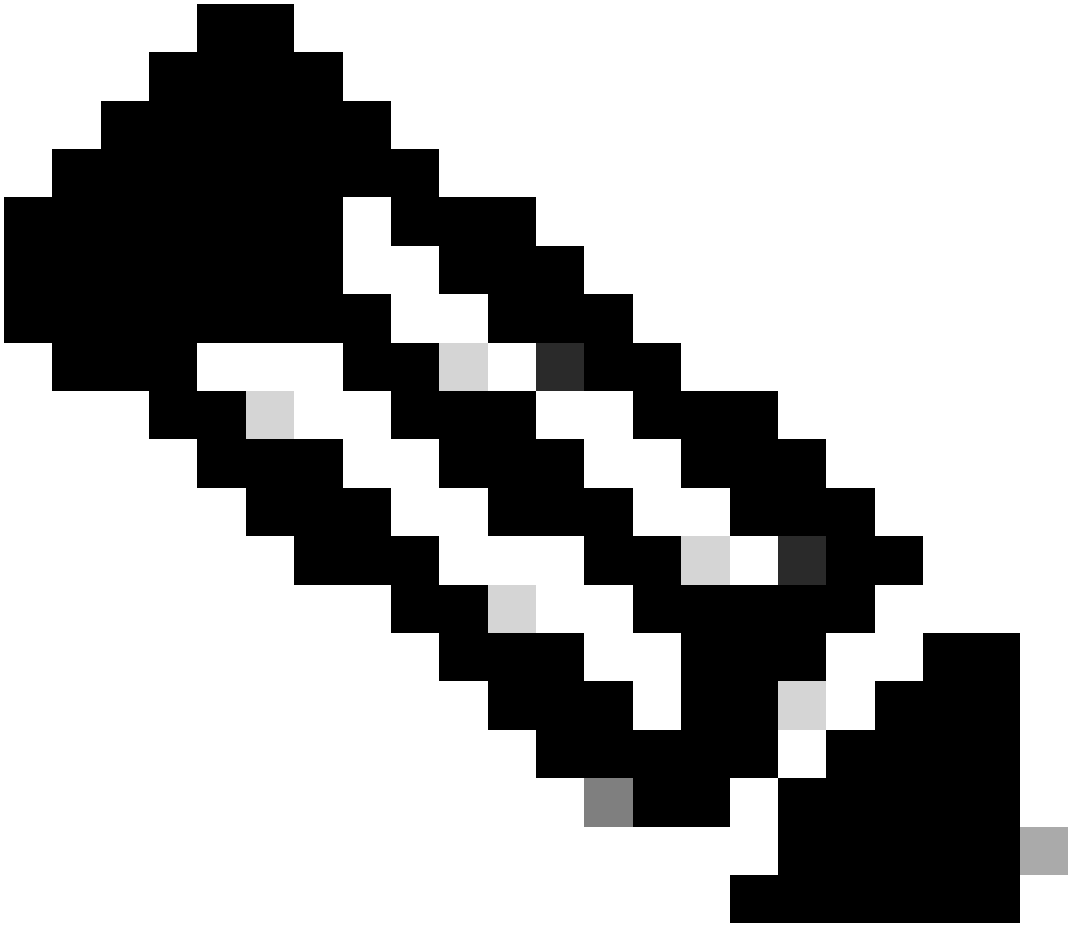
Configurazione dei set di criteri ISE per Single SSID BYOD

1. Selezionare Policy > Policy Set (Policy > Set) e creare una policy per il flusso BYOD sull'ISE:

2. Passare quindi a Amministrazione > Gestione delle identità > Origini identità esterne > Profilo di autenticazione certificato. Fare clic sul pulsante Aggiungi per creare il profilo del certificato:

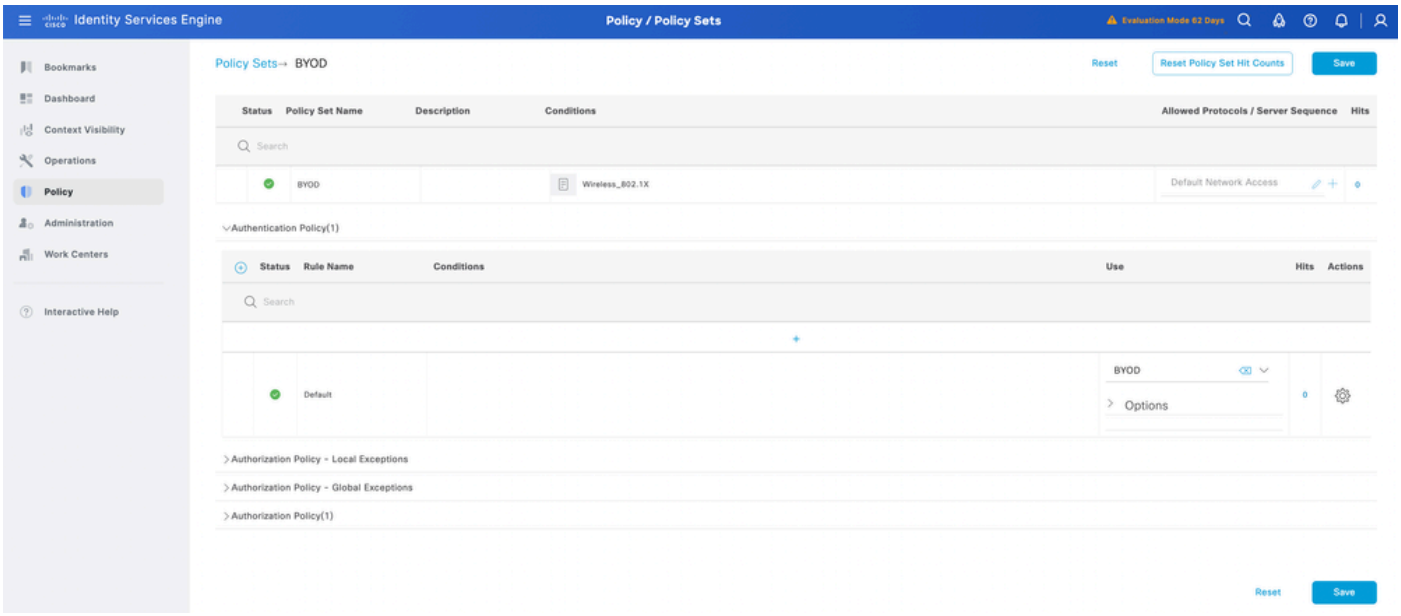






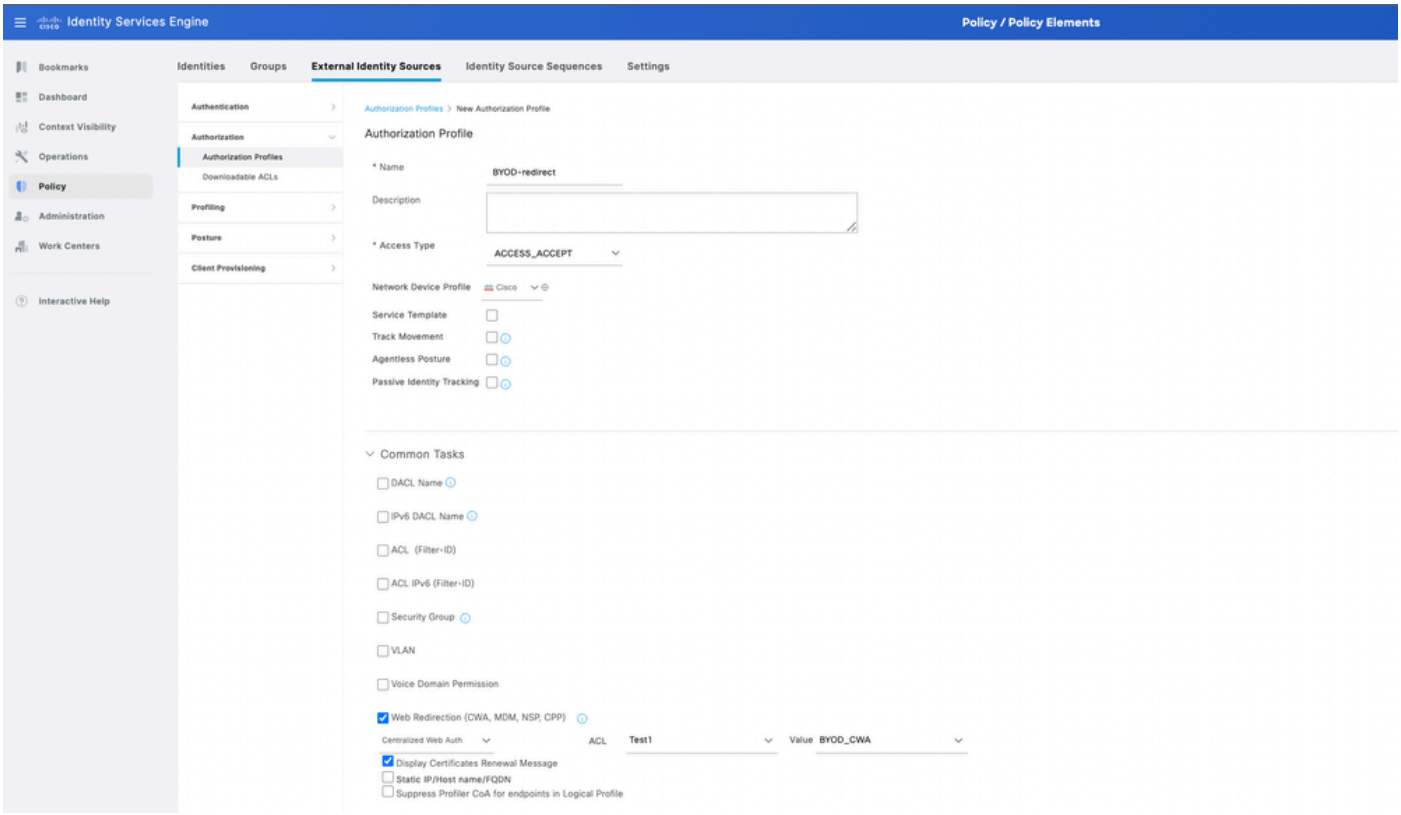
Nota: Nell'Identity Store è sempre possibile selezionare Active Directory integrato in ISE per eseguire una ricerca utente dal certificato per una maggiore sicurezza.

3. Fare clic su Sottometti per salvare la configurazione. Mappare quindi il profilo del certificato al criterio impostato per BYOD:

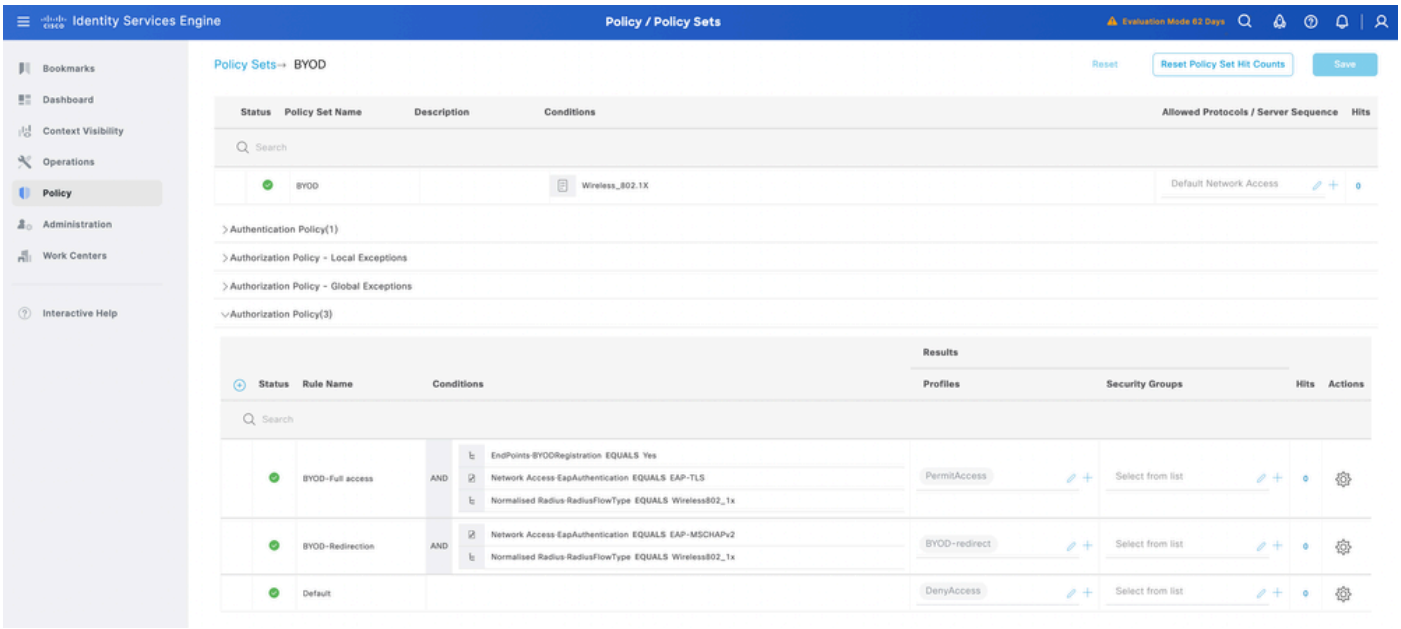


4. Configurare il profilo di autorizzazione per il reindirizzamento BYOD e l'accesso completo dopo il flusso BYOD. Passare a Criterio > Elementi criteri > Risultati > Autorizzazione > Profili di autorizzazione.

5. Fare clic su Add (Aggiungi) e creare un profilo di autorizzazione. Controllare il reindirizzamento Web (CWA,MDM,NSP,CPP) ed eseguire il mapping della pagina del portale BYOD. Inoltre, aggiungere il nome ACL di reindirizzamento dal WLC al profilo. Per il profilo di accesso completo, configurare un'autorizzazione di accesso con la rispettiva VLAN aziendale nel profilo.



6. Mappare il profilo di autorizzazione alla regola di autorizzazione. L'accesso completo BYOD deve avere la regola EndPoints·BYODRegistration uguale a yes in modo che l'utente ottenga l'accesso completo alla rete dopo il flusso BYOD.

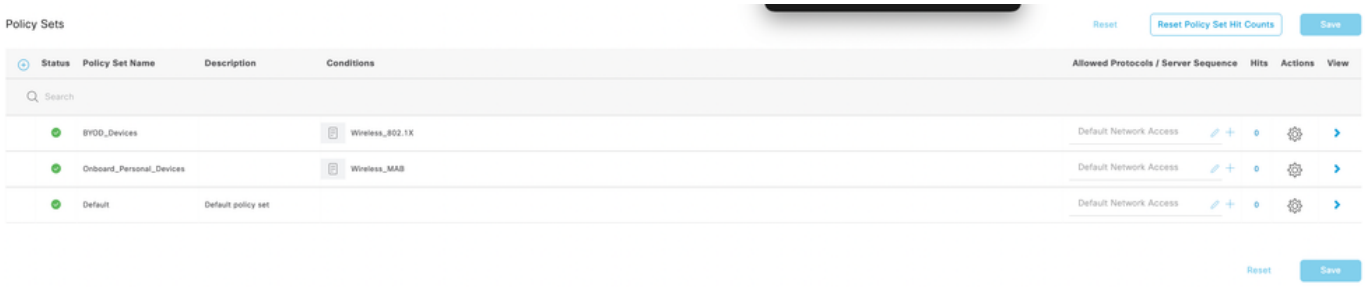


Configurazione dei set di criteri ISE per Dual SSID BYOD

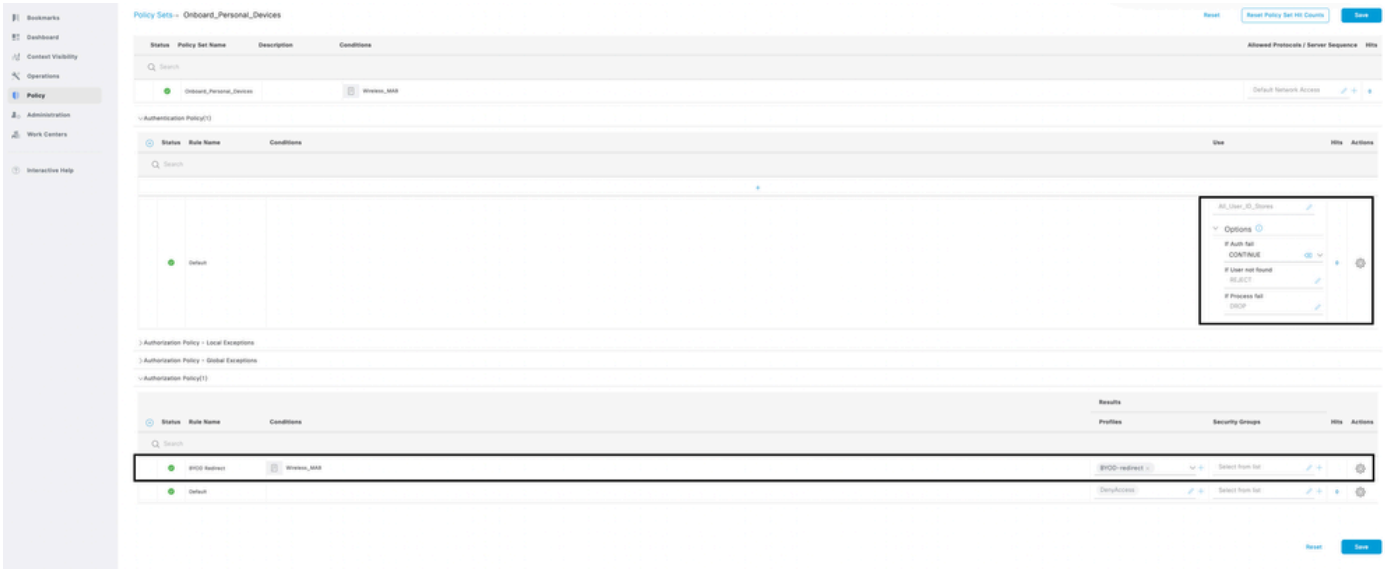
Nella configurazione Dual SSID BYOD, il set di due regole è configurato su ISE. Il primo set di criteri è per il SSID aperto/non protetto, in cui la configurazione del set di criteri reindirizza l'utente alla pagina BYOD al momento della connessione al SSID aperto/non protetto

1. Selezionare Policy > Policy Set e creare una policy per il flusso BYOD sull'ISE.

2. Creare un set di criteri per SSID aperto/non protetto e SSID aziendale che autentichi l'utente BYOD registrato su ISE.

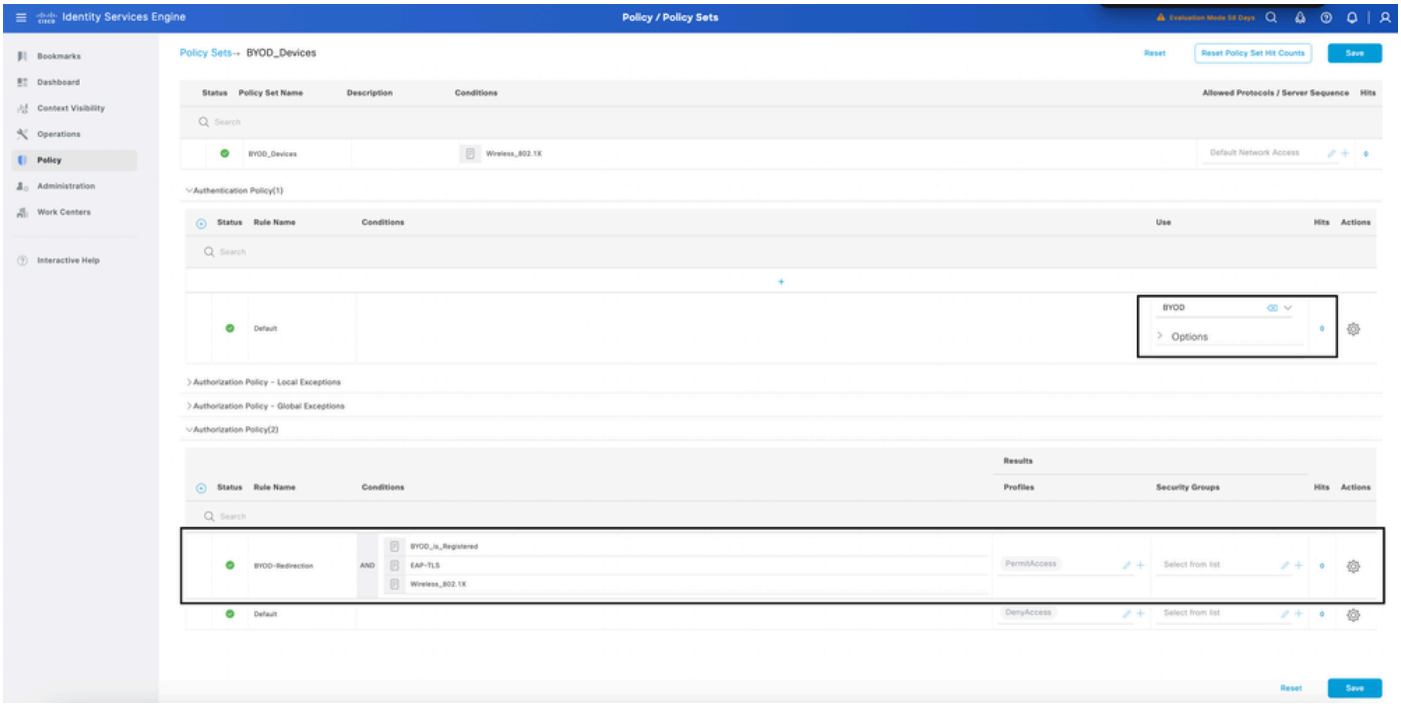


3. Nell'insieme di criteri di caricamento, trova Continua selezionato nelle opzioni. Per il criterio di autorizzazione, creare una condizione e mappare il profilo di autorizzazione di reindirizzamento. Gli stessi passaggi sono previsti per la creazione del profilo di autorizzazione, come indicato al punto 4.



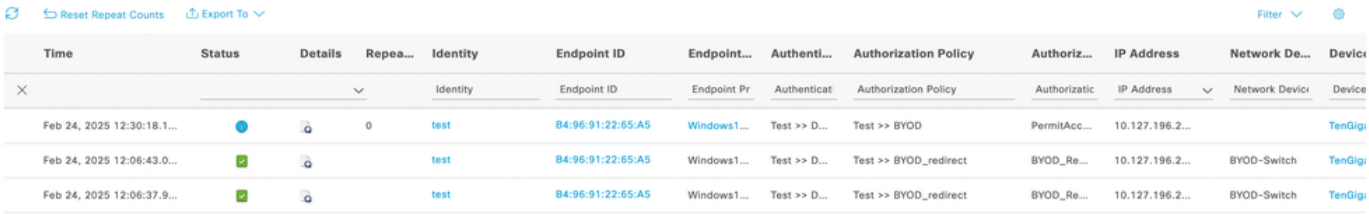
4. Nel set di criteri registrati BYOD, configurare il criterio di autenticazione con il profilo del certificato trovato.

in Configure ISE Policy Sets for Single SSID BYOD al punto 2. Creare inoltre una condizione per il criterio di autorizzazione e mappare il profilo di accesso completo al criterio.

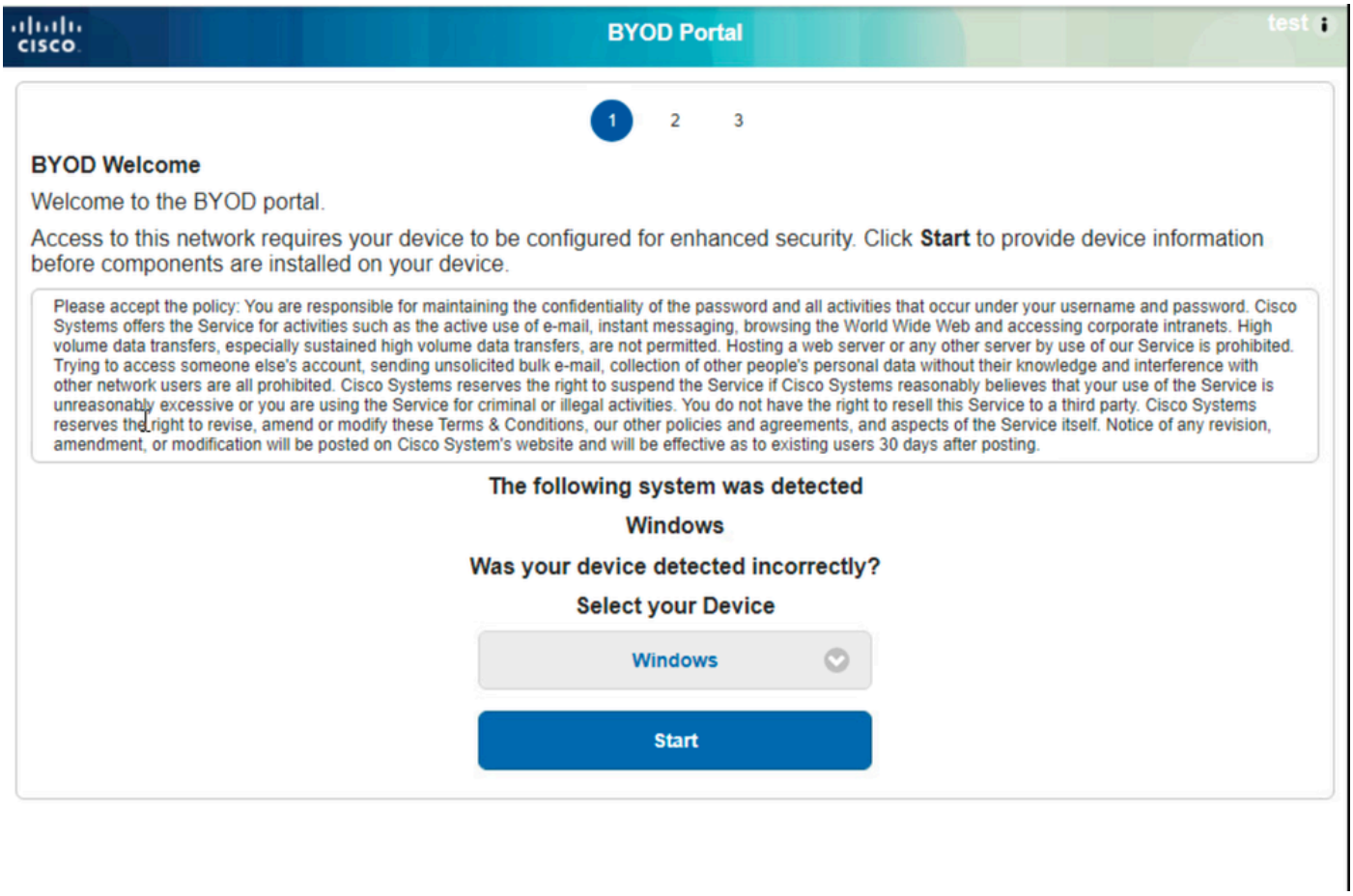


Registrazione

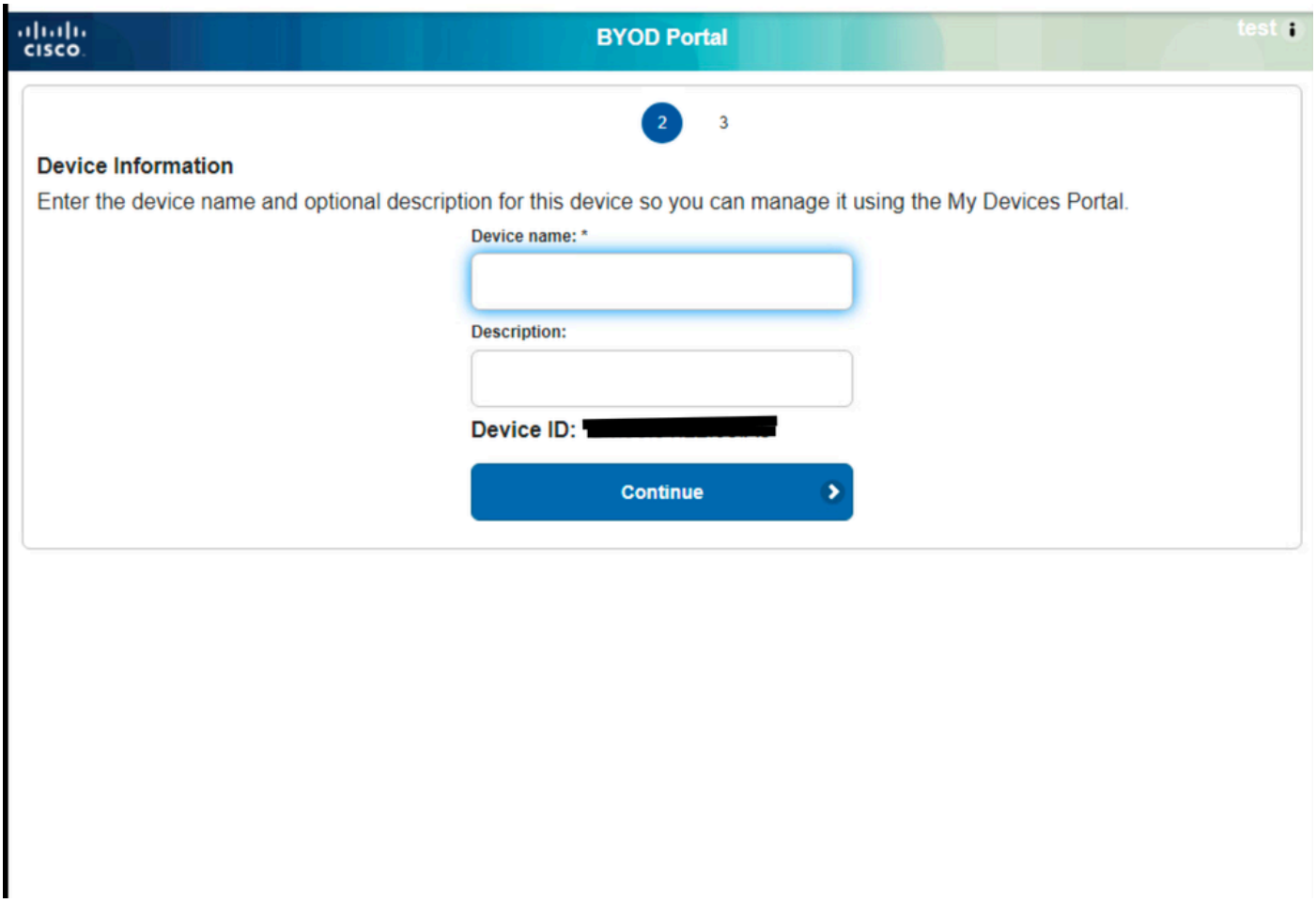
Dal live log di ISE, l'autenticazione utente avrà esito positivo e verrà reindirizzata alla pagina del portale BYOD. Dopo aver completato il flusso BYOD, all'utente viene concesso l'accesso alla rete



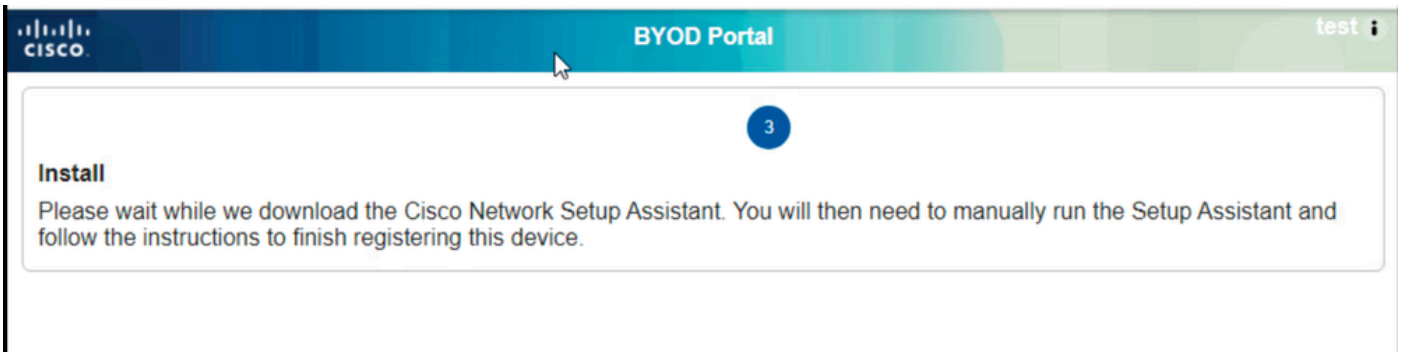
Dal punto di vista dell'utente, vengono prima reindirizzati alla pagina BYOD e il dispositivo appropriato deve essere selezionato dalla pagina Web. Per il test di un dispositivo Windows 10 è stato utilizzato



Dopo aver fatto clic sul pulsante Next (Avanti), viene visualizzata una pagina in cui l'utente deve inserire il nome del dispositivo e la descrizione

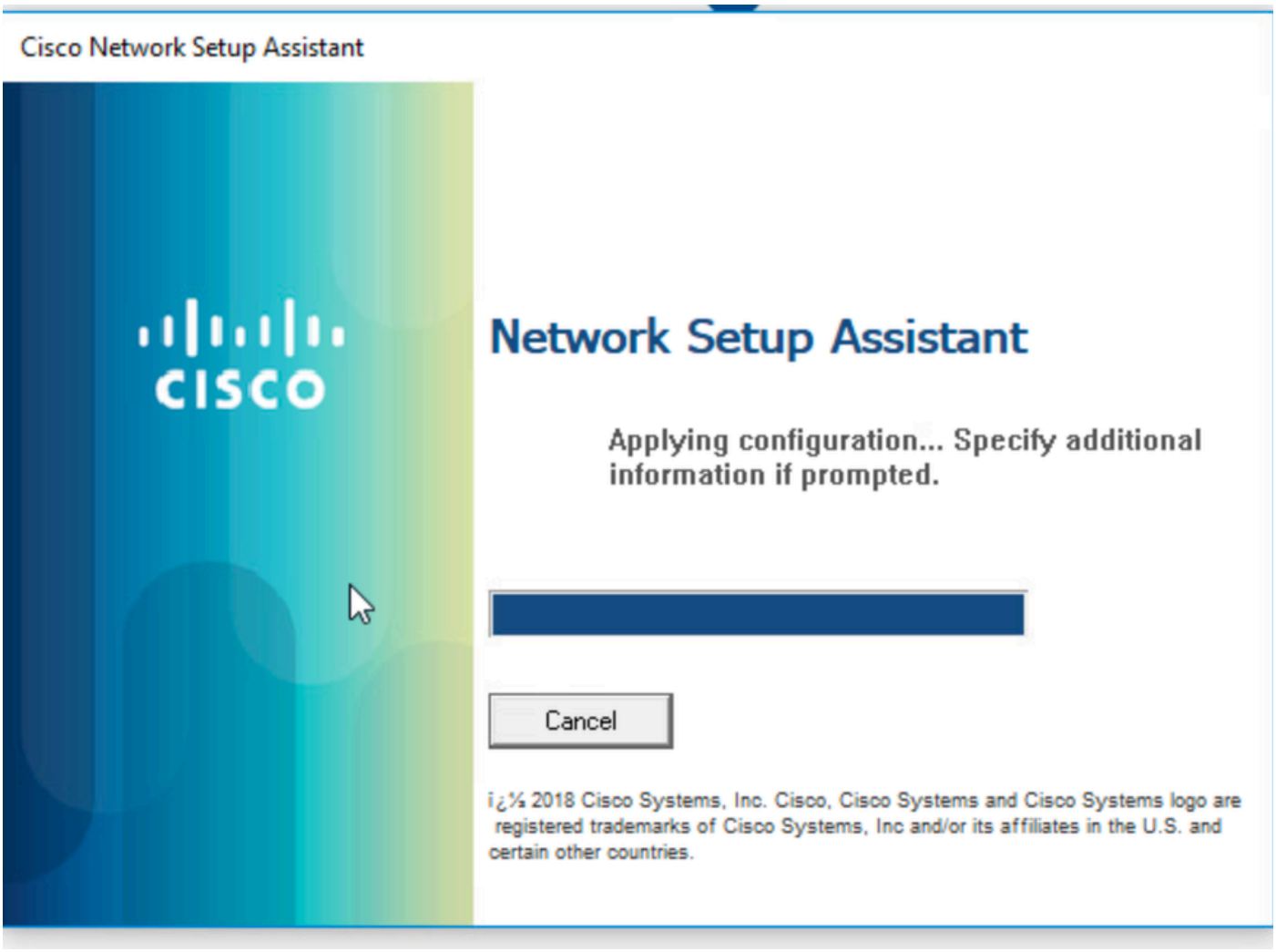


Indica che all'utente verrà richiesto di scaricare lo strumento Network Assistant per il download del profilo dell'endpoint e del certificato EAP TLS per l'autenticazione se il profilo è configurato per eseguire l'autenticazione EAP-TLS



Eseguire l'applicazione Network Assistant con privilegi di amministratore e fare clic sul pulsante Start per avviare il flusso di caricamento:


Cisco Network Setup Assistant
Network Setup Assistant
This application automatically configures network settings.
Start
Quit
i¿¼ 2018 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.



L'utente è stato correttamente connesso alla rete con il proprio dispositivo personale per accedere alle risorse.

Risoluzione dei problemi

Per risolvere il problema con BYOD, abilitare il debug su ISE

Attributi da impostare sul livello di debug:

- client (guest.log)
- client-webapp (guest.log)
- scep (ise-psc.log)
- ca-service (ise-psc.log)
- admin-ca (ise-psc.log)
- runtime-AAA (prt-server.log)
- nsf (ise-psc.log)
- sessione nsf (ise-psc.log)
- profiler (profiler.log)

Frammento di log

Log Guest

Questi log indicano che l'utente ha eseguito correttamente il reindirizzamento alla pagina e ha scaricato l'applicazione Network Assistant:

2025-02-24 12:06:08,053 INFO [https-jsse-nio-10.127.196.172-8443-exec-4][] portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:0000000000000000B30D555::::- percorso di mapping trovato in azione-inoltro, inoltro a: pages/byodWelcome.jsp // Pagina iniziale BYOD
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[]] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5::test: di pTransSteps:1
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[]] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5::test: NextFlowStep, pTransSteps:[id: d2513b7b-7249-4bc3-a423-0e7d9a0b2500]
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[]] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5::test: NextFlowStep, stepTran:d2513b7b-7249-4bc3-a423-0e7d9a0b2500
2025-02-24 12:06:09,979 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][] portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:0000000000000000B30D59CC5::::- percorso di mapping trovato in inoltri azione, inoltro a: pages/byodRegistration.jsp
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][[]] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5::test: di pTransSteps:1
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][[]] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5::test: NextFlowStep, pTransSteps:[id: f203b757-9e8a-473e-abdc-879d0cd37491]
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][[]] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5::test: NextFlowStep, stepTran:f203b757-9e8a-473e-abdc-879d0cd37491
2025-02-24 12:06:14,647 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][] portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:0000000000000000B30D59CC5::::- percorso di mapping trovato in inoltri azione, inoltro a: pages/byodInstall.jsp
2025-02-24 12:06:14,713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][] cisco.cpm.client.provisioning.StreamingServlet -:000000000000000B30D59CC5::: Session = null
2025-02-24 12:06:14,713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][] cisco.cpm.client.provisioning.StreamingServlet -:000000000000000B30D59CC5::: portalSessionId = null
2025-02-24 12:06:14.713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][[]] cisco.cpm.client.provisioning.StreamingServlet -:000000000000000B30D59CC5::::- StreamingServlet URI:/auth/provisioning/download/f6b73ef8-4502-4d50-81aa-bbb91e8828da/NetworkSetupAssistant.exe // L'applicazione Assistenza di rete è stata inviata all'endpoint

Registri Ise-Psc

Quando l'applicazione viene scaricata sull'endpoint, l'applicazione avvia un flusso SCEP per ottenere il certificato client da ISE.

2025-02-24 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- CertStore contiene 4 certificati:
2025-02-24 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- 1. '[issuer=CN=Certificate Services Root CA - iseguest; serial=322815127387689606282525327846633020 89]'
2025-02-24 12:04:39,808 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- 2. '[issuer=CN=Certificate Services Endpoint Sub CA - iseguest; serial=131900858749761727853768227590303808637]'
2025-02-24 12:04:39,810 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- 3. '[issuer=CN=Certificate Services Root CA - iseguest; serial=686276201605863086858498187751006982 24]'
2025-02-24 12:04:39,810 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- 4. '[issuer=CN=Certificate Services Node CA - iseguest; serial=729347676986030971539324822275488749 53]'
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Selezione del certificato di crittografia
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Selezione del certificato con chiaveEncipherment keyUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Trovato 1 certificato/i con chiaveEncipherment keyUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Utilizzando [issuer=CN=Certificate Services Endpoint Sub CA - iseguest; serial=131900858749761727853768275903038086 37] per la crittografia dei messaggi
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Selezione del certificato del verificatore
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Selezione del certificato con la chiave digitalSignatureUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Trovato 1 certificato/i con chiave digitalSignatureUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Utilizzando [issuer=CN=Certificate Services Endpoint Sub CA - iseguest; serial=131900858749761727853768275903038086 37] per la verifica dei messaggi
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Selezione del certificato emittente
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Selezione di un certificato con BasicConstraints
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]

org.jscep.client.CertStoreInspector -::::- Trovati 3 certificati con BasicConstraints
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Utilizzando [issuer=CN=Certificate Services Endpoint Sub CA - iseguest; serial=131900858749761727853768227590303808637] per l'emittente
2025-02-24 12:04:39,812 DEBUG [DefaultQuarzScheduler_Worker-5][[]]
com.cisco.cpm.scep.PKIServerLoadBalancer -:::::- Metriche delle prestazioni dei server SCEP : name[attivo/inattivo, richieste totali, errori totali, richieste in esecuzione, RTT medio] http://127.0.0.1:9444/caservice/scep[live,96444,1,0,120]

Download profilo endpoint

Dopo il completamento del processo SCEP e l'installazione del certificato da parte dell'endpoint, l'applicazione scarica il profilo dell'endpoint per l'autenticazione futura che verrà eseguita dal dispositivo:

2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::::- Riferimento = Windows // È stato rilevato il dispositivo Windows in base alla pagina Web
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::::- Sessione = 00000000000000000B30D59CC5
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::::- Sessione = 00000000000000000B30D59CC5
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -:::- provisioning profilo nsp
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- Sessione = 00000000000000000B30D59CC5
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- portalSessionId = null
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- StreamingServlet URI:/auth/provisioning/download/b8ce01e6-b150-4d4e-9698-40e48d5e0197/Cisco-ISE-NSP.xml//Il profilo NSP viene scaricato sull'endpoint
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- Streaming su ip: tipo di file: Nome file NativeSPProfile:Cisco-ISE-NSP.xml //Applicazione Network Assistant
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- BYODStatus:INIT_PROFILE
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- userId è stato impostato su test
2025-02-24 12:06:26,558 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -:::: - tipo di reindirizzamento: SUCCESS_PAGE, URL di reindirizzamento: per mac:

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).