

Guida all'implementazione di Wireless BYOD per FlexConnect

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Topologia](#)

[Registrazione dei dispositivi e provisioning dei supplicant](#)

[Portale registrazione asset](#)

[Portale di autoregistrazione](#)

[Autenticazione e provisioning](#)

[Provisioning per iOS \(iPhone/iPad/iPod\)](#)

[Provisioning per Android](#)

[Doppia registrazione SSID wireless BYOD](#)

[Registrazione singola BYOD wireless SSID](#)

[Configurazione funzionalità](#)

[Configurazione della WLAN](#)

[Configurazione punto di accesso FlexConnect](#)

[Configurazione di ISE](#)

[Esperienza utente - Provisioning iOS](#)

[SSID doppio](#)

[SSID singolo](#)

[Esperienza utente - Provisioning di Android](#)

[SSID doppio](#)

[Portale I miei dispositivi](#)

[Riferimento - Certificati](#)

[Informazioni correlate](#)

Introduzione

I dispositivi mobili stanno diventando sempre più potenti dal punto di vista computazionale e popolari tra i consumatori. Milioni di questi dispositivi sono venduti ai consumatori con Wi-Fi ad alta velocità in modo che gli utenti possano comunicare e collaborare. I consumatori sono ormai abituati all'aumento della produttività che questi dispositivi mobili portano nelle loro vite e stanno cercando di portare la loro esperienza personale nello spazio di lavoro. In questo modo si creano le esigenze di funzionalità di una soluzione BYOD (Bring Your Own Device) sul posto di lavoro.

Questo documento fornisce la distribuzione di filiali per la soluzione BYOD. Un dipendente si

connette a un SSID (Service Set Identifier) aziendale con il suo nuovo iPad e viene reindirizzato a un portale di registrazione automatica. Cisco Identity Services Engine (ISE) autentica l'utente in Active Directory (AD) aziendale e scarica un certificato con un indirizzo MAC iPad incorporato e un nome utente nell'iPad, insieme a un profilo richiedente che impone l'uso di EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) come metodo per la connettività dot1x. In base alla policy di autorizzazione dell'ISE, l'utente può connettersi usando il dot1x e accedere alle risorse appropriate.

Le funzionalità ISE delle versioni software Cisco Wireless LAN Controller precedenti alla 7.2.110.0 non supportavano i client di switching locale associati tramite i punti di accesso (AP) FlexConnect. La versione 7.2.10.0 supporta queste funzionalità ISE per i FlexConnect AP per lo switching locale e i client autenticati centralmente. Inoltre, la release 7.2.110.0 integrata con ISE 1.1.1 fornisce (ma non si limita a) queste funzionalità della soluzione BYOD per il wireless:

- Profilatura e postura del dispositivo
- Registrazione dei dispositivi e provisioning dei supplicant
- Caricamento di dispositivi personali (provisioning di dispositivi iOS o Android)

Nota: anche se supportati, altri dispositivi, come laptop e workstation wireless PC o Mac, non sono inclusi in questa guida.

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:

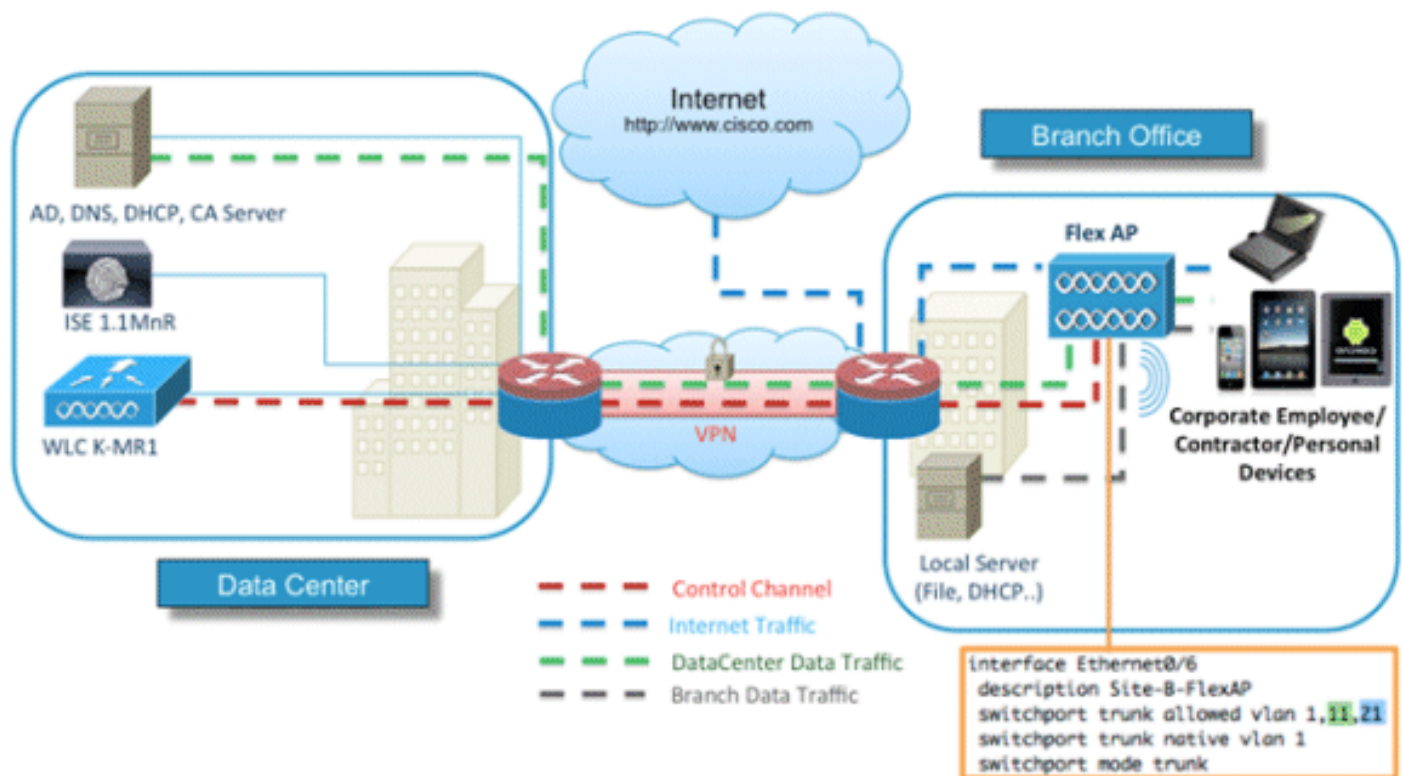
- Switch Cisco Catalyst
- Controller Cisco Wireless LAN (WLAN)
- Software Cisco WLAN Controller (WLC) versione 7.2.10.0 e successive
- AP 802.11n in modalità FlexConnect
- Software Cisco ISE release 11.1.1 e successive
- Windows 2008 AD con CA (Certification Authority)
- server DHCP
- Server DNS (Domain Name System)
- Protocollo NTP (Network Time Protocol)
- Notebook, smartphone e tablet client wireless (Apple iOS, Android, Windows e Mac)

Nota: per informazioni importanti su questa versione del software, consultare le [note di versione per Cisco Wireless LAN Controller e Lightweight Access Point](#) per la [versione 7.2.10.0](#). Accedere al sito Cisco.com per ottenere le note sulla versione più recenti prima di caricare e testare il software.

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.

Topologia

Per implementare e testare correttamente le seguenti funzionalità, è necessaria una configurazione di rete minima, come mostrato nel diagramma:



Per questa simulazione, è necessaria una rete con un punto di accesso FlexConnect, un sito locale/remoto con DHCP locale, DNS, WLC e ISE. L'access point FlexConnect è collegato a un trunk per verificare la commutazione locale con più VLAN.

Registrazione dei dispositivi e provisioning dei supplicant

È necessario registrare un dispositivo in modo che il relativo supplicant nativo possa eseguire il provisioning per l'autenticazione dot1x. In base al criterio di autenticazione corretto, l'utente viene reindirizzato alla pagina guest e autenticato dalle credenziali del dipendente. L'utente visualizza la pagina di registrazione del dispositivo, in cui vengono richieste le informazioni sul dispositivo. Il processo di provisioning dei dispositivi viene quindi avviato. Se il sistema operativo non è supportato per il provisioning, l'utente viene reindirizzato al portale di registrazione degli asset per contrassegnare il dispositivo per l'accesso MAB (MAC Authentication Bypass). Se il sistema operativo è supportato, viene avviato il processo di registrazione e viene configurato il supplicant nativo del dispositivo per l'autenticazione dot1x.

Portale registrazione asset

Il portale di registrazione degli asset è l'elemento della piattaforma ISE che consente ai dipendenti di avviare l'onboarding degli endpoint tramite un processo di autenticazione e registrazione.

Gli amministratori possono eliminare le risorse dalla pagina Identità endpoint. Ogni dipendente è in grado di modificare, eliminare ed inserire in una lista nera le risorse registrate. Gli endpoint della lista nera vengono assegnati a un gruppo di identità della lista nera e viene creato un criterio di autorizzazione per impedire l'accesso alla rete da parte degli endpoint della lista nera.

Portale di autoregistrazione

Nel flusso CWA (Central Web Authentication) i dipendenti vengono reindirizzati a un portale che consente di immettere le credenziali, eseguire l'autenticazione e immettere le specifiche della risorsa specifica che si desidera registrare. Questo portale è denominato Portale self-provisioning ed è simile al Portale di registrazione dei dispositivi. Consente ai dipendenti di immettere l'indirizzo MAC e una descrizione significativa dell'endpoint.

Autenticazione e provisioning

Dopo aver selezionato il portale di autoregistrazione, i dipendenti devono fornire un insieme di credenziali valide per passare alla fase di attivazione. Dopo l'autenticazione, è possibile eseguire il provisioning dell'endpoint nel database degli endpoint e generare un certificato per l'endpoint. Un link nella pagina consente al dipendente di scaricare la procedura guidata del programma pilota per i supplicant (SPW).

Nota: per visualizzare la [matrice delle](#) funzionalità FlexConnect per BYOD, consultare l'articolo di Cisco sulla matrice delle funzionalità di FlexConnect.

Provisioning per iOS (iPhone/iPad/iPod)

Per la configurazione EAP-TLS, ISE segue il processo di registrazione OTA (Over-the-Air) di Apple:

- Una volta completata l'autenticazione, il motore di valutazione valuta i criteri di provisioning del client, generando un profilo supplicant.
- Se il profilo supplicant è per l'impostazione EAP-TLS, il processo OTA determina se l'ISE utilizza la firma automatica o la firma di una CA sconosciuta. Se una delle condizioni è vera, all'utente viene richiesto di scaricare il certificato di ISE o CA prima di poter iniziare il processo di registrazione.
- Per altri metodi EAP, ISE spinge il profilo finale dopo la corretta autenticazione.

Provisioning per Android

Per motivi di sicurezza, l'agente Android deve essere scaricato dal sito Marketplace Android e non può essere eseguito il provisioning da ISE. Cisco carica una versione finale della procedura guidata nel marketplace Android tramite l'account Cisco Android Marketplace Publisher.

Questo è il processo di provisioning Android:

1. Cisco utilizza il Software Development Kit (SDK) per creare il pacchetto Android con estensione .apk.
2. Cisco carica un pacchetto nel marketplace Android.
3. L'utente configura il criterio nel provisioning del client con i parametri appropriati.
4. Dopo la registrazione del dispositivo, l'utente finale viene reindirizzato al servizio di provisioning client quando l'autenticazione dot1x non riesce.
5. La pagina del portale di provisioning fornisce un pulsante che reindirizza gli utenti al portale del marketplace Android, dove possono scaricare l'SPW.
6. Viene avviato Cisco SPW che esegue il provisioning del richiedente: SPW rileva l'ISE e scarica il profilo da ISE.SPW crea una coppia certificato/chave per EAP-TLS.SPW effettua una chiamata di richiesta proxy SCEP (Simple Certificate Enrollment Protocol) ad ISE e ottiene il certificato.I profili wireless vengono applicati da SPW.Se i profili vengono applicati correttamente, SPW attiva la riautenticazione.L'SPW si chiude.

Doppia registrazione SSID wireless BYOD

Questo è il processo per la registrazione automatica della doppia SSID wireless BYOD:

1. L'utente viene associato all'SSID guest.
2. L'utente apre un browser e viene reindirizzato al portale per gli ospiti di ISE CWA.
3. L'utente immette il nome utente e la password di un dipendente nel portale guest.
4. ISE autentica l'utente e, in base al fatto che si tratta di un dipendente e non di un ospite, reindirizza l'utente alla pagina guest di registrazione del dispositivo dipendente.
5. L'indirizzo MAC è precompilato nella pagina guest di registrazione del dispositivo per DeviceID. L'utente immette una descrizione e accetta la politica d'uso accettabile (AUP, Acceptable Use Policy) se necessario.
6. L'utente seleziona **Accetta** e inizia a scaricare e installare l'SPW.
7. Il provisioning del richiedente per il dispositivo dell'utente viene eseguito insieme a tutti i certificati.
8. Si verifica il CoA e il dispositivo si riassocia all'SSID aziendale (CORP) e si autentica con EAP-TLS (o altro metodo di autorizzazione in uso per il richiedente).

Registrazione singola BYOD wireless SSID

In questo scenario, esiste un singolo SSID per l'accesso aziendale (CORP) che supporta sia PEAP (Protected Extensible Authentication Protocol) che EAP-TLS. Nessun SSID guest.

Questo è il processo per la registrazione automatica della BYOD wireless con un solo SSID:

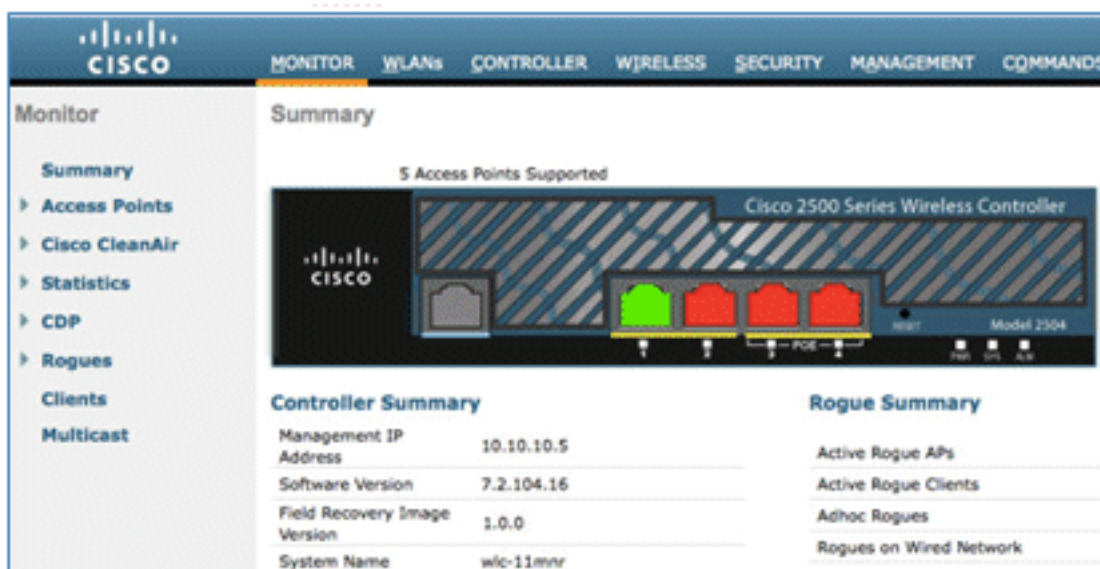
1. L'utente viene associato a CORP.
2. L'utente immette un nome utente e una password dipendente nel applicant per l'autenticazione PEAP.
3. ISE autentica l'utente e, in base al metodo PEAP, fornisce una policy di autorizzazione di accettazione con reindirizzamento alla pagina guest di registrazione del dispositivo dipendente.

4. L'utente apre un browser e viene reindirizzato alla pagina guest di Registrazione dispositivo dipendente.
5. L'indirizzo MAC è precompilato nella pagina guest di registrazione del dispositivo per DeviceID. L'utente immette una descrizione e accetta le CDS.
6. L'utente seleziona **Accetta** e inizia a scaricare e installare l'SPW.
7. Il provisioning del richiedente per il dispositivo dell'utente viene eseguito insieme a tutti i certificati.
8. Si verifica il CoA e il dispositivo si riassocia all'SSID CORP e si autentica con EAP-TLS.

Configurazione funzionalità

Per iniziare la configurazione, completare i seguenti passaggi:

1. Per questa guida, verificare che la versione del WLC sia 7.2.10.0 o successiva.



2. Passare a **Sicurezza > RADIUS > Autenticazione** e aggiungere il server RADIUS al WLC.



3. Aggiungere ISE 1.1.1 al WLC:

Immettere un segreto condiviso. Impostare il supporto per RFC 3576 su **Enabled**.

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

RADIUS Authentication Servers > Edit

Server Index	1
Server Address	10.10.10.60
Shared Secret Format	ASCII
Shared Secret	***
Confirm Shared Secret	***
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

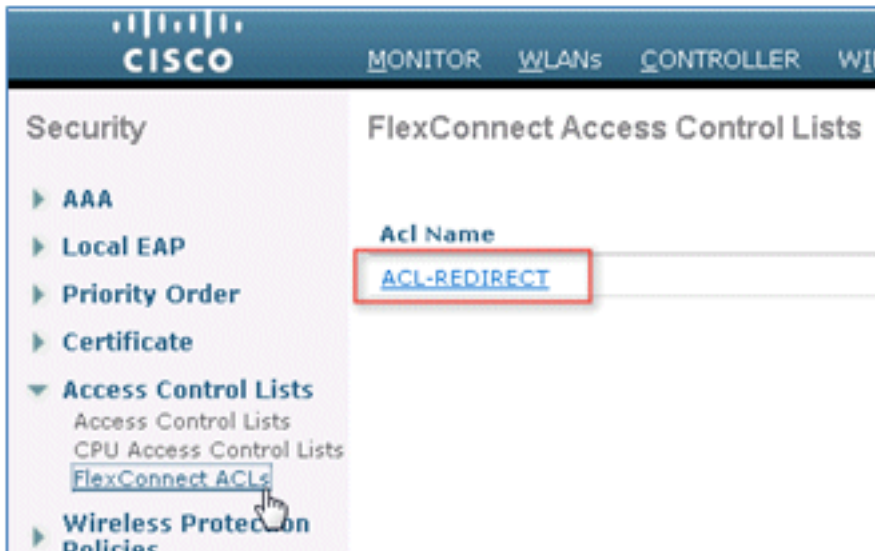
4. Aggiungere lo stesso server ISE come server di accounting RADIUS.

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANA

RADIUS Accounting Servers > Edit

Server Index	1
Server Address	10.10.10.60
Shared Secret Format	ASCII
Shared Secret	***
Confirm Shared Secret	***
Port Number	1813
Server Status	Enabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

5. Creare un ACL WLC Pre-Auth da usare nella policy ISE in un secondo momento. Selezionare WLC > Security > Access Control Lists > ACL FlexConnect, quindi creare un nuovo ACL FlexConnect denominato ACL-REDIRECT (nell'esempio).



6. Nelle regole ACL, autorizzare tutto il traffico da/verso l'ISE e autorizzare il traffico dei client durante il provisioning del supplicant.

Per la prima regola (sequenza 1):

Impostare Source (Origine) su **Any (Qualsiasi)**. Impostare IP (indirizzo ISE)/ Netmask **255.255.255.255**. Impostare Action su **Permit**.

Access Control Lists > Rules > Edit

Sequence:

Source:

Destination: IP Address: Netmask:

Protocol:

DSCP:

Direction:

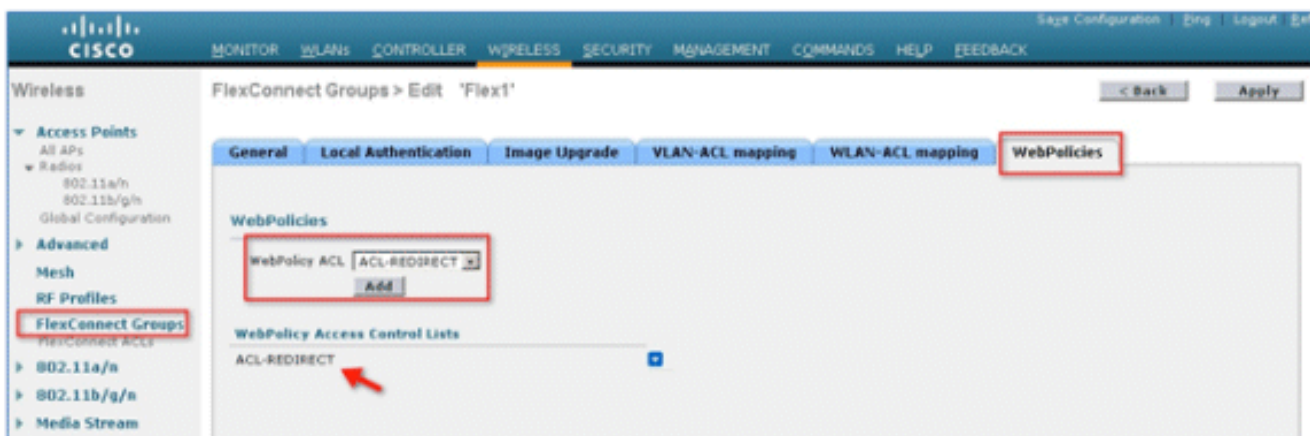
Action:

Per la seconda regola (sequenza 2), impostare source IP (indirizzo ISE)/ mask 255.255.255.255 su **Any** and Action to **Permit**.

General							
Access List Name		ACL-REDIRECT					
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
1	Permit	0.0.0.0 0.0.0.0	/ 10.10.10.60 255.255.255.255	/ Any	Any	Any	Any <input checked="" type="checkbox"/>
2	Permit	10.10.10.60 255.255.255.255	/ 0.0.0.0 0.0.0.0	/ Any	Any	Any	Any <input checked="" type="checkbox"/>

7. Creare un nuovo gruppo FlexConnect denominato Flex1 (in questo esempio):

Passare alla scheda **Gruppo FlexConnect > Criteri Web**. Nel campo ACL WebPolicy, fare clic su **Add**, quindi selezionare **ACL-REDIRECT** o l'ACL FlexConnect creato in precedenza. Confermare che popola il campo **Elenchi di controllo di accesso di WebPolicy**.



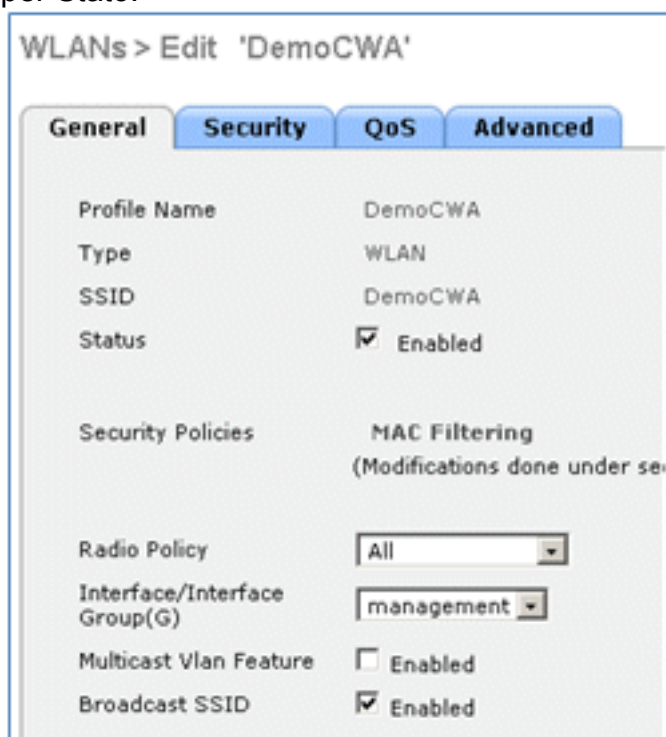
8. Fare clic su **Apply and Save Configuration** (Applica e salva configurazione).

Configurazione della WLAN

Per configurare la WLAN, effettuare i seguenti passaggi:

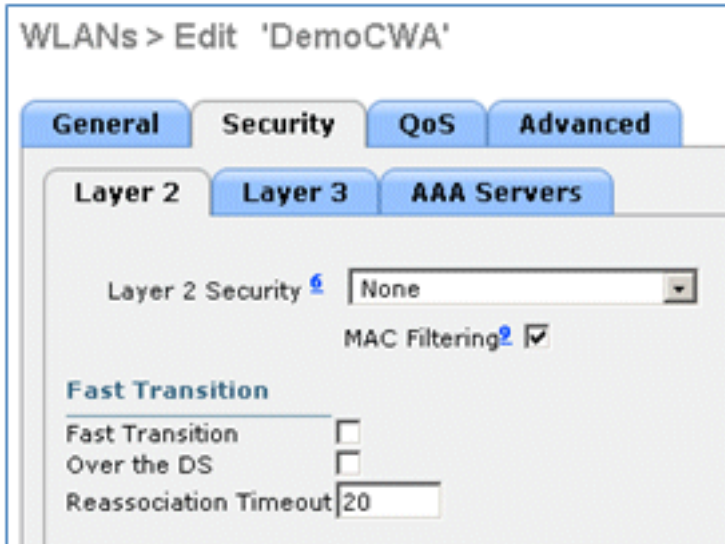
1. Creare un SSID WLAN aperto per l'esempio di SSID doppio:

Immettere il nome di una WLAN: **DemoCWA** (nell'esempio). Selezionare l'opzione **Abilitato** per Stato.



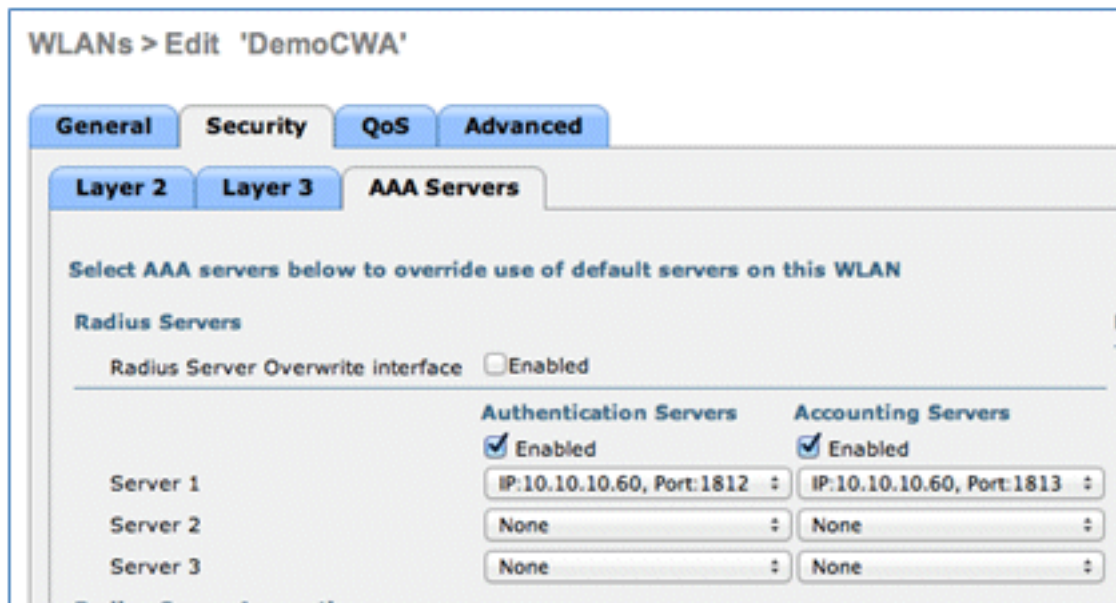
2. Passare alla scheda **Sicurezza > scheda Layer 2** e impostare i seguenti attributi:

Sicurezza di livello 2: **nessuna**Filtro MAC: **Abilitato** (casella selezionata)Transizione rapida: **disabilitata** (casella non selezionata)

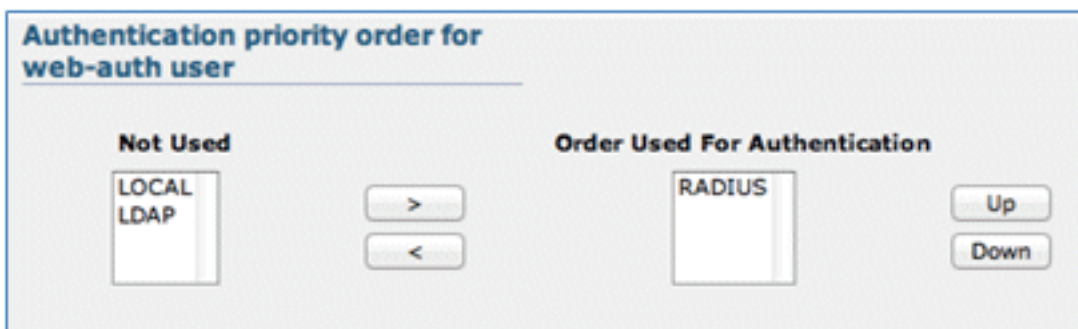


3. Andare alla scheda **AAA Server** e impostare i seguenti attributi:

Autenticazione e server account: **Abilitato**Server 1: *<ISE IP address>*

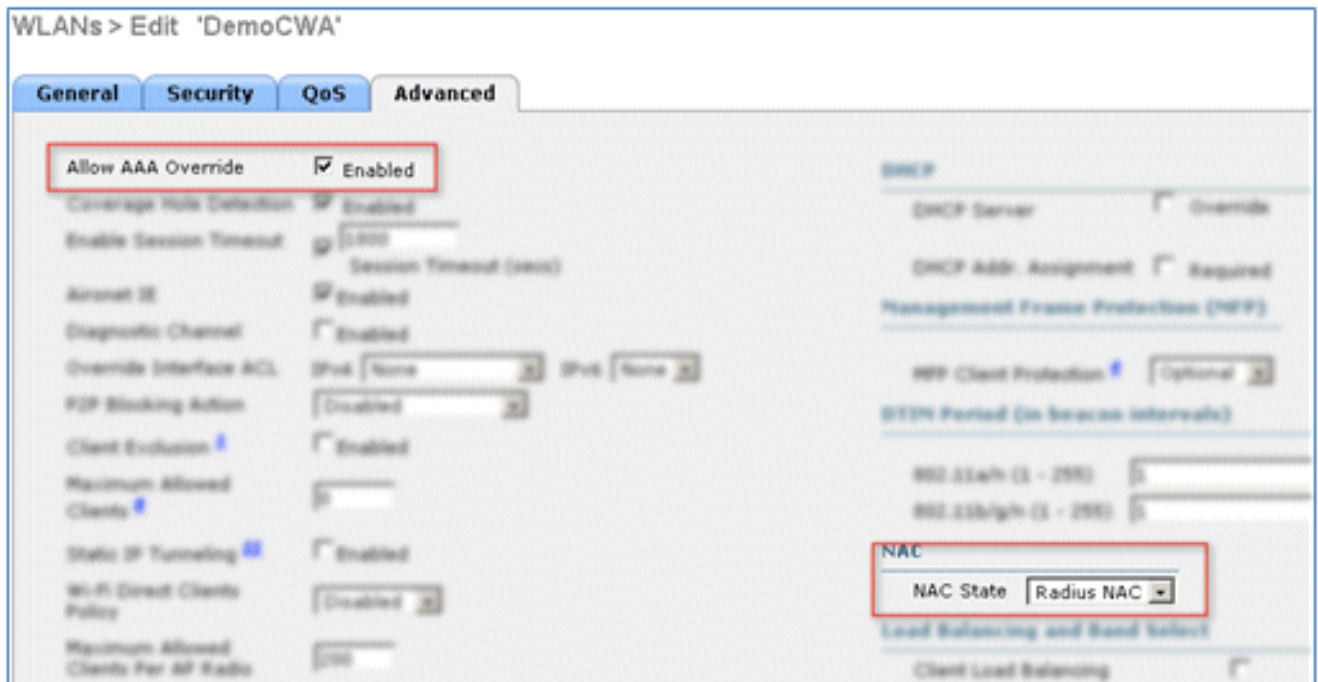


4. Scorrere verso il basso dalla scheda **Server AAA**. In Ordine di priorità autenticazione per l'utente con autenticazione Web verificare che **RADIUS** sia utilizzato per l'autenticazione e che gli altri non siano utilizzati.



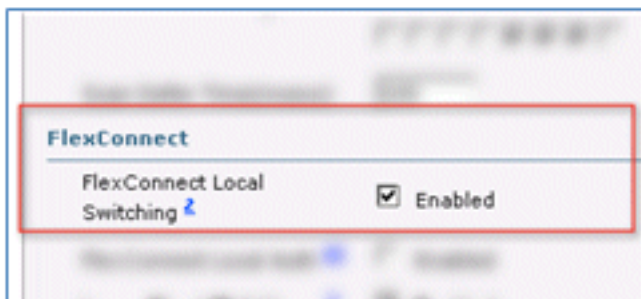
5. Andare alla scheda **Advanced** (Avanzate) e impostare i seguenti attributi:

Consenti sostituzione AAA: **abilitata** Stato NAC: **Radius NAC**



Nota: RADIUS Network Admission Control (NAC) non è supportato quando FlexConnect AP è in modalità disconnessa. Pertanto, se l'access point FlexConnect è in modalità standalone e perde la connessione al WLC, tutti i client vengono disconnessi e l'SSID non viene più annunciato.

6. Scorrere verso il basso nella scheda **Advanced** e impostare FlexConnect Local Switching su **Enabled**.



7. Fare clic su **Apply** and **Save Configuration** (Applica e salva configurazione).



8. Creare un SSID WLAN 802.1X denominato **Demo1x** (nell'esempio) per gli scenari a SSID singolo e doppio.

WLANs > Edit 'Demo1x'

General | **Security** | QoS | Advanced

Profile Name: Demo1x
 Type: WLAN
 SSID: Demo1x
 Status: Enabled

Security Policies: [WPA2][Auth(802.1X)]
 (Modifications done under secu

Radio Policy: All
 Interface/Interface Group(G): management
 Multicast Vlan Feature: Enabled
 Broadcast SSID: Enabled

9. Passare alla scheda **Sicurezza** > scheda **Layer 2** e impostare i seguenti attributi:

Sicurezza di layer 2: **WPA+WPA2** Transizione rapida: **disabilitata** (casella non selezionata) Gestione chiavi di autenticazione: 802.IX: **Abilita**

WLANs > Edit 'Demo1x'

General | **Security** | QoS | Advanced

Layer 2 | Layer 3 | AAA Servers

Layer 2 Security: WPA+WPA2
 MAC Filtering:

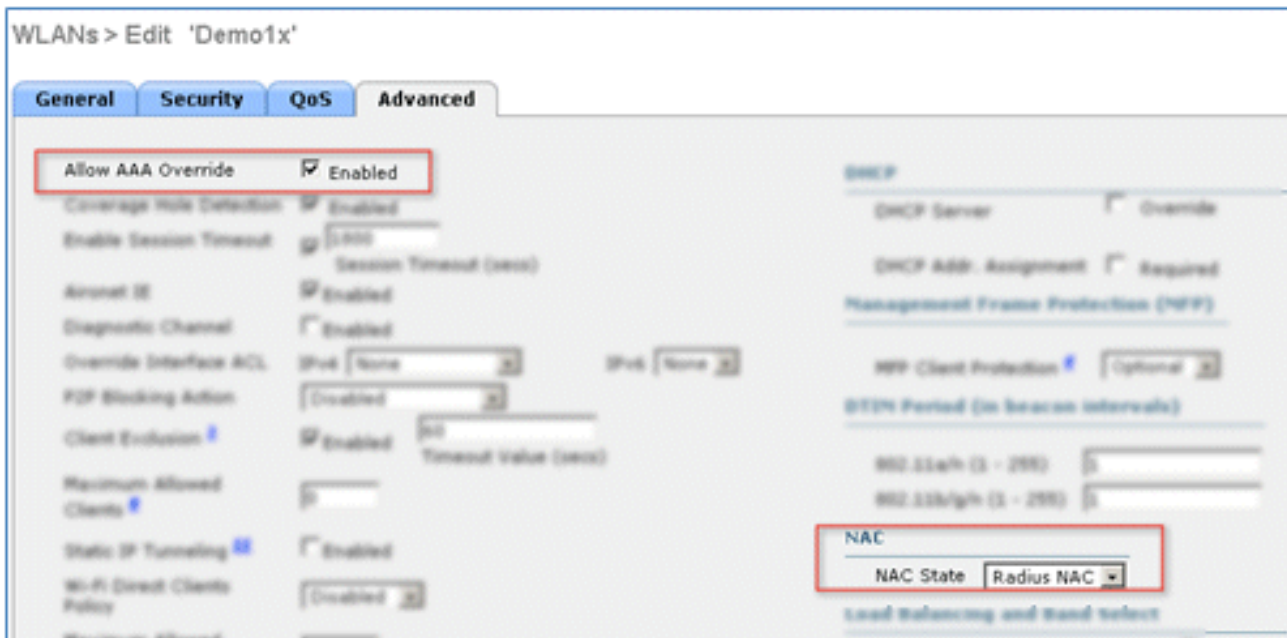
Fast Transition
 Fast Transition:
 Over the DS:
 Reassociation Timeout: 20

WPA+WPA2 Parameters
 WPA Policy:
 WPA2 Policy:
 WPA2 Encryption: AES TKIP

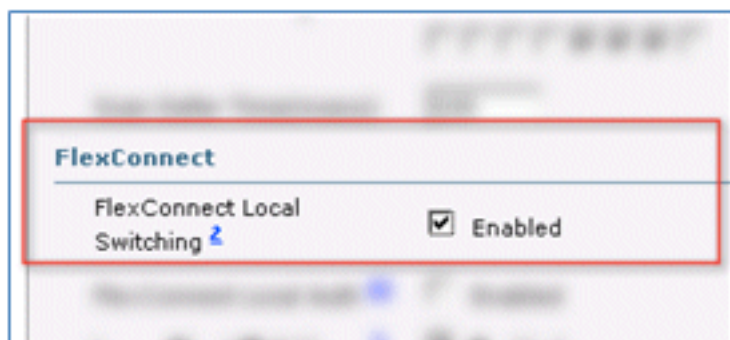
Authentication Key Management
 802.1X: Enable
 CCKM: Enable
 PSK: Enable

10. Andare alla scheda **Advanced** (Avanzate) e impostare i seguenti attributi:

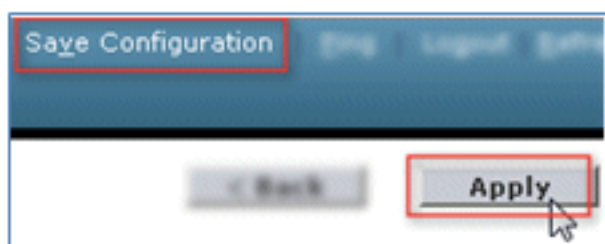
Consenti sostituzione AAA: **abilitata** Stato NAC: **Radius NAC**



11. Scorrere verso il basso la scheda **Advanced** (Avanzate) e impostare FlexConnect Local Switching su **Enabled** (Abilitato).



12. Fare clic su **Apply** and **Save Configuration** (Applica e salva configurazione).



13. Confermare che entrambe le nuove WLAN sono state create.

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	802x	802x	Disabled	[WPA2][Auth(802.1X)]
2	WLAN	Demo1x	Demo1x	Enabled	[WPA2][Auth(802.1X)]
4	WLAN	DemoCWA	DemoCWA	Enabled	MAC Filtering
5	WLAN	Flex	Flex	Disabled	Web-Auth

Configurazione punto di accesso FlexConnect

Per configurare l'access point FlexConnect, completare i seguenti passaggi:

1. Passare a **WLC > Wireless** e fare clic sull'access point FlexConnect di destinazione.

AP Name	AP Model
Site-B-FlexAP	AIR-LAP1262N-A-K

2. Fare clic sulla scheda **FlexConnect**.

General	Credentials	Interfaces	High Availability	Inventory	FlexConnect	Advanced
---------	-------------	------------	-------------------	-----------	-------------	----------

3. Abilitare il supporto VLAN (la casella è selezionata), impostare l'ID VLAN nativo e fare clic su **Mapping VLAN**.

VLAN Support

Native VLAN ID **VLAN Mappings**

FlexConnect Group Name Not Configured

4. Impostare l'ID VLAN su 21 (in questo esempio) per l'SSID per la commutazione locale.

MONITOR WLANs CONTROLLER WIRELESS SECURITY M

All APs > Site-B-FlexAP > VLAN Mappings

AP Name Site-B-FlexAP

Base Radio MAC e8:04:62:0a:68:80

WLAN Id	SSID	VLAN ID
3	Demo1x	<input type="text" value="21"/>
4	DemoCWA	<input type="text" value="21"/>

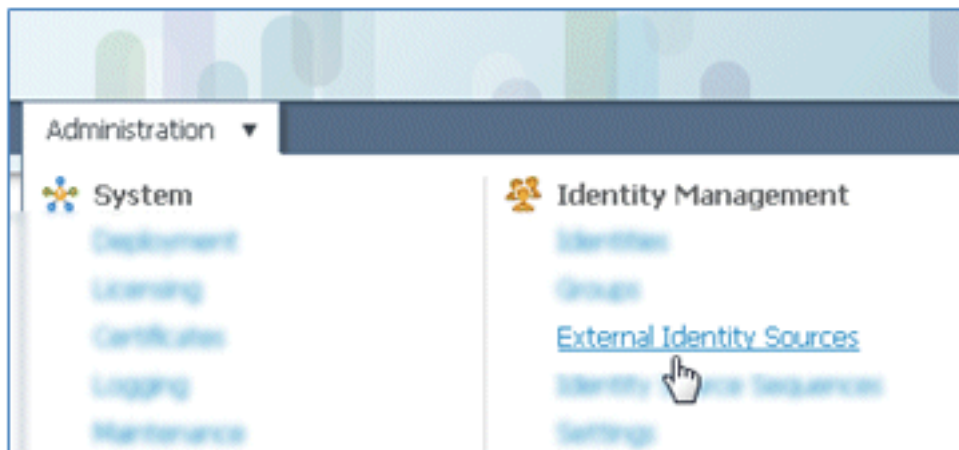
5. Fare clic su **Apply and Save Configuration** (Applica e salva configurazione).

Configurazione di ISE

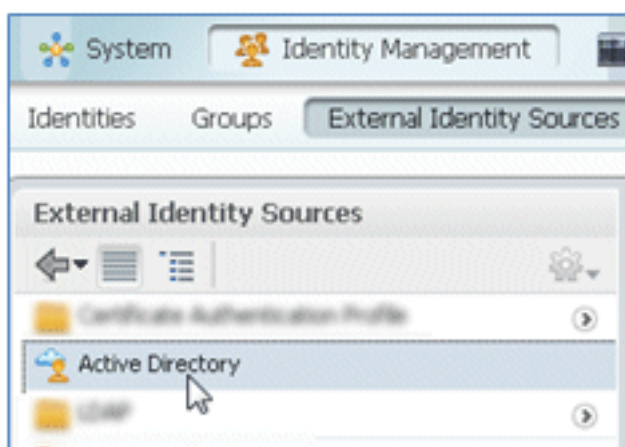
Per configurare l'ISE, completare la procedura seguente:

1. Accedere al server ISE: <https://ise>.

2. Passare a **Amministrazione > Gestione identità > Origini identità esterne**.

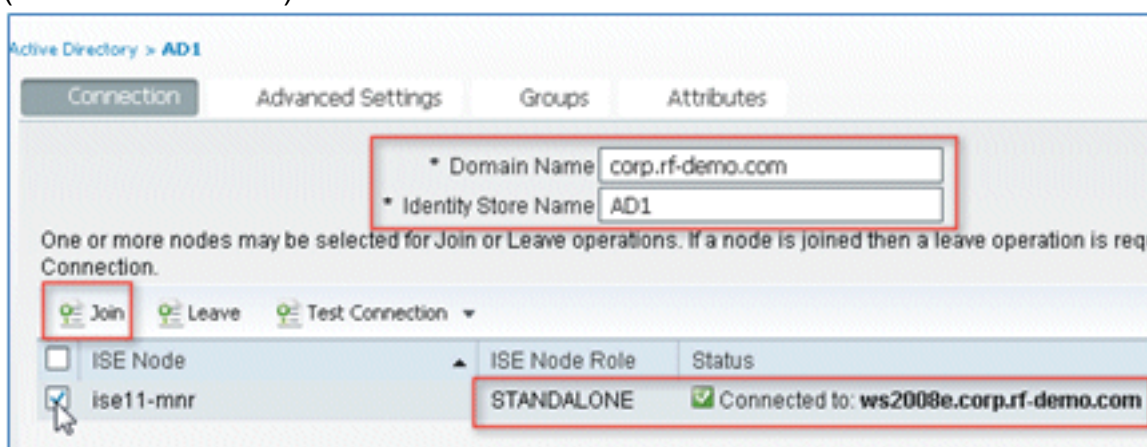


3. Fare clic su **Active Directory**.

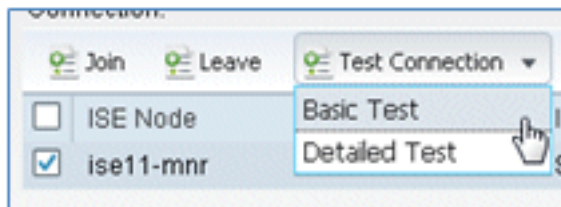


4. Nella scheda Connessione:

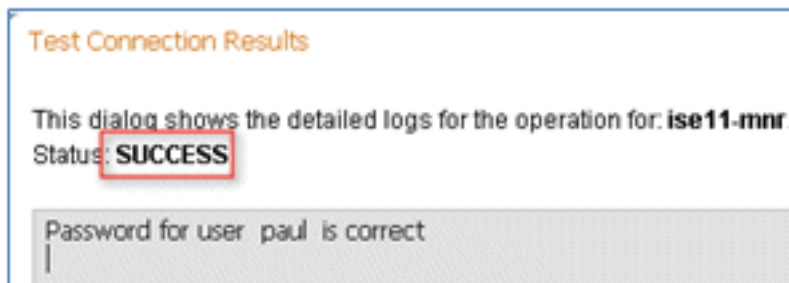
Aggiungere il nome di dominio di **corp.rf-demo.com** (in questo esempio) e impostare il nome predefinito dell'archivio identità su **AD1**. Fare clic su **Salva configurazione**. Fare clic su **Partecipa** e specificare il nome utente e la password dell'account dell'amministratore di Active Directory necessari per l'aggiunta. Lo stato deve essere verde. Abilita **Connesso a:** (casella selezionata).



5. Eseguire un test di connessione di base ad Active Directory con un utente del dominio corrente.

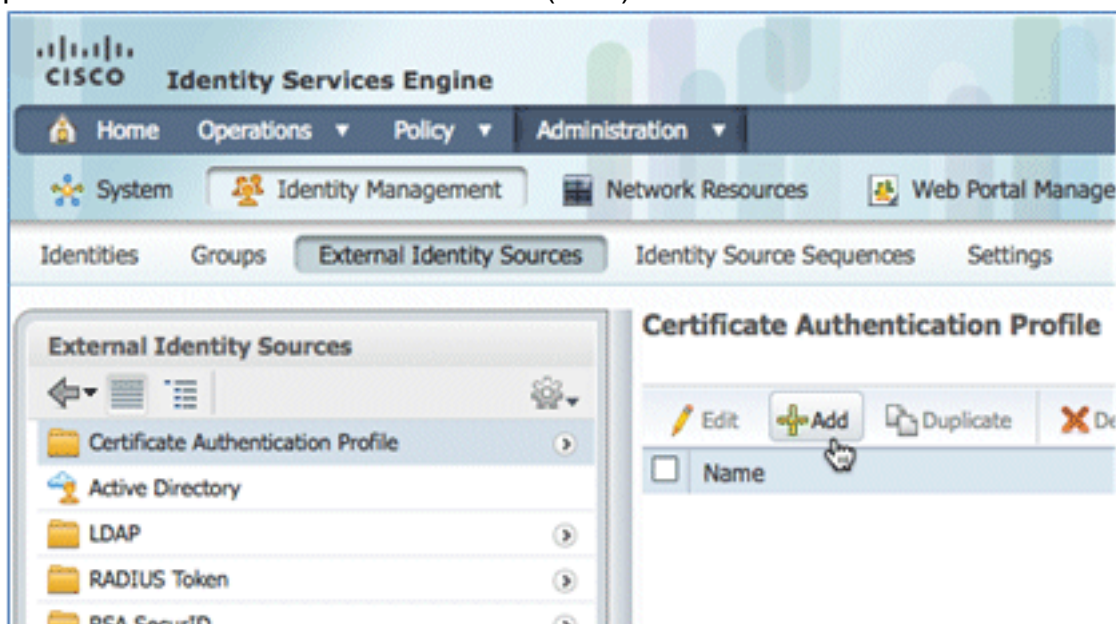


6. Se la connessione ad Active Directory ha esito positivo, una finestra di dialogo conferma che la password è corretta.



7. Passare a **Amministrazione > Gestione identità > Origini identità esterne**:

Fare clic su **Profilo di autenticazione certificato**. Fare clic su **Add** (Aggiungi) per un nuovo profilo di autenticazione del certificato (CAP).



8. Immettere il nome **CertAuth** (in questo esempio) per il criterio di autorizzazione delle connessioni; per l'attributo Nome utente principale X509, selezionare **Nome comune**, quindi fare clic su **Invia**.

Certificate Authentication Profiles List > New Certificate Authentication Profile

Certificate Authentication Profile

* Name

Description

Principal Username X509 Attribute

Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory

LDAP/AD Instance Name

9. Confermare l'aggiunta del nuovo criterio di autorizzazione delle connessioni.

CISCO Identity Services Engine

Home Operations Policy Administration

System Identity Management Network Resources Web Portal Management

Identities Groups External Identity Sources Identity Source Sequences Settings

External Identity Sources

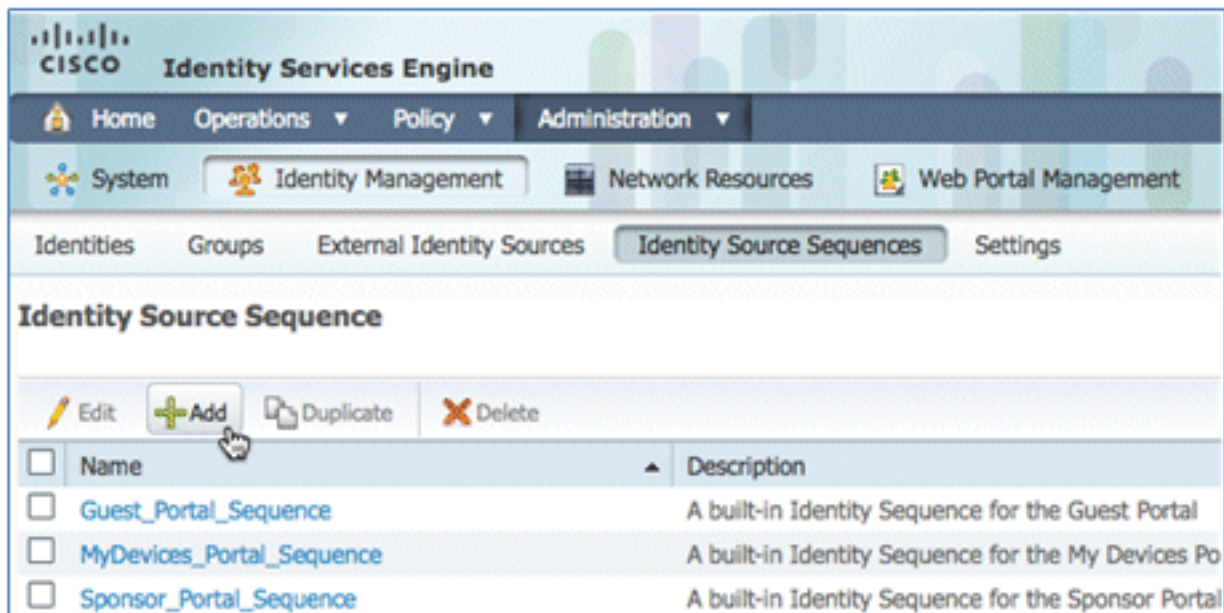
- Certificate Authentication Profile
- Active Directory
- LDAP
- RADIUS Token
- RSA SecurID

Certificate Authentication Profile

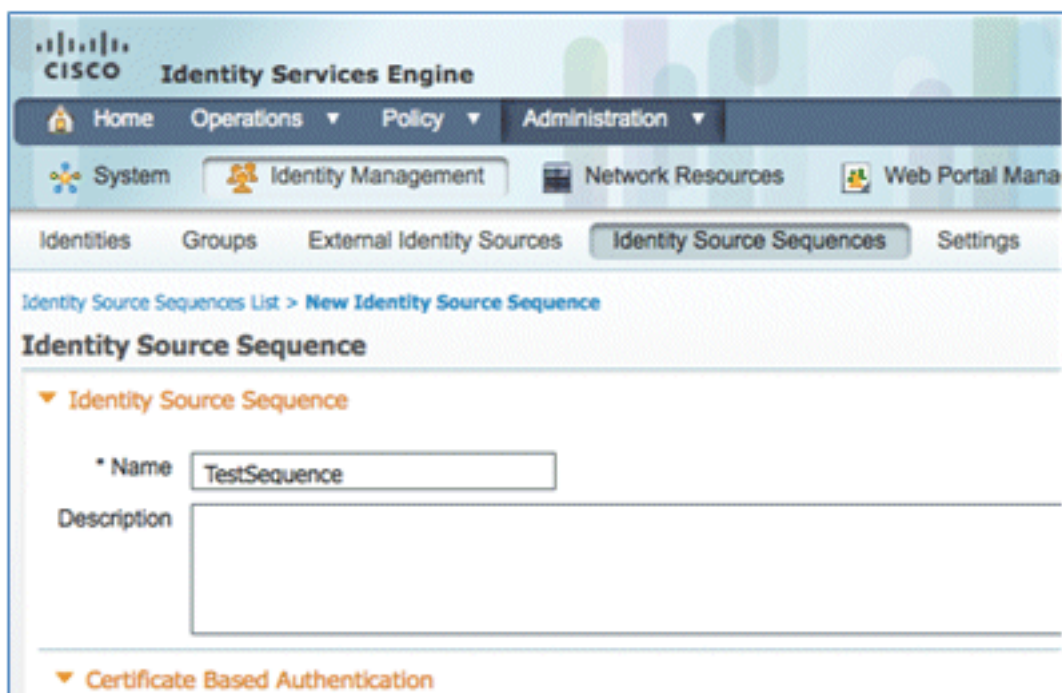
Edit Add Duplicate Delete

<input type="checkbox"/>	Name
<input type="checkbox"/>	CertAuth

10. Passare a **Amministrazione > Gestione identità > Sequenze origine identità** e fare clic su **Aggiungi**.

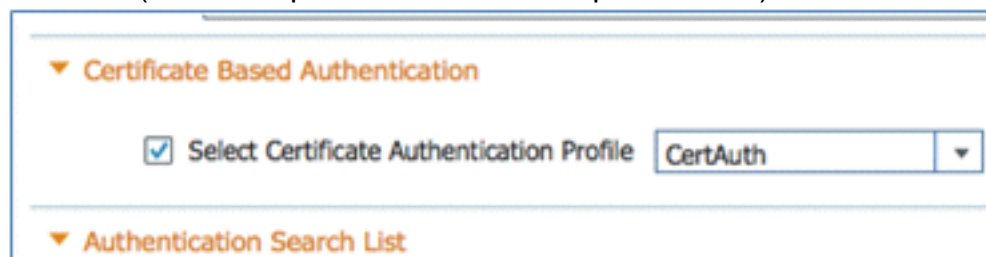


11. Assegnare alla sequenza il nome **TestSequence** (nell'esempio).



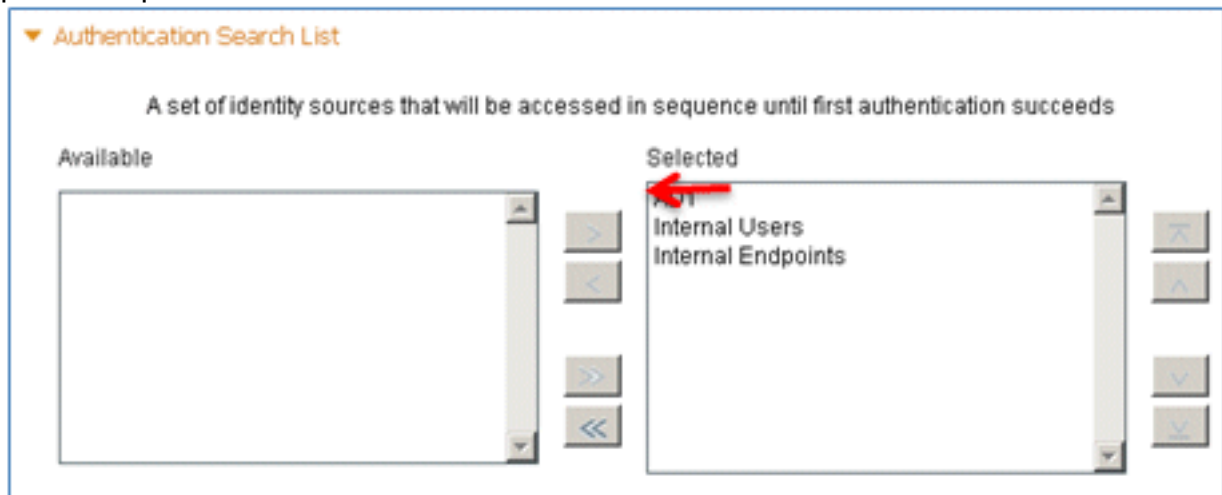
12. Scorrere fino a **Autenticazione basata su certificato**:

Abilitare **Seleziona profilo di autenticazione certificato** (la casella è selezionata). Selezionare **CertAuth** (o un altro profilo CAP creato in precedenza).

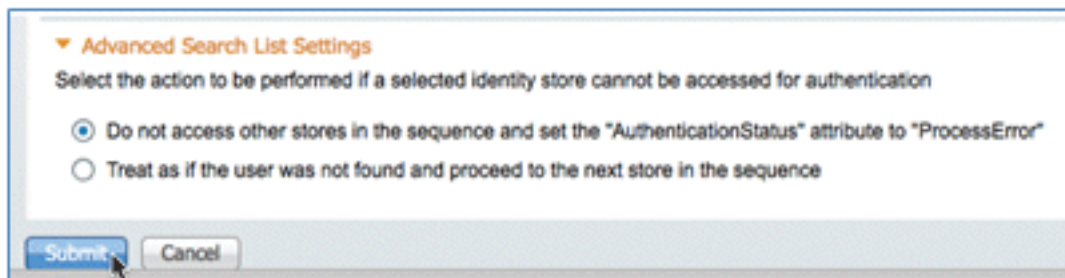


13. Scorri verso il basso fino all'**elenco di ricerca autenticazione**:

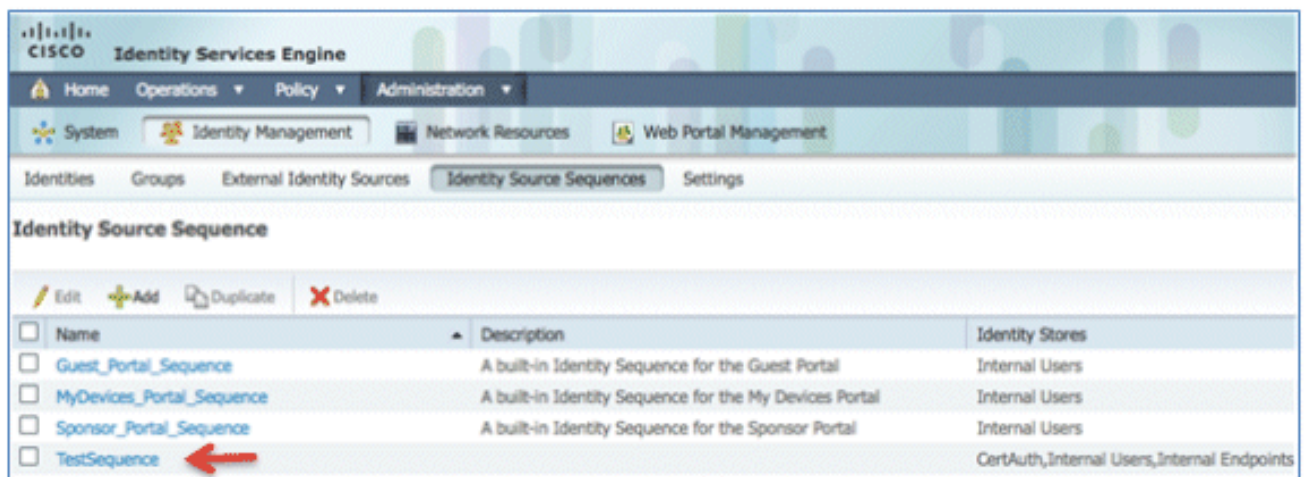
Sposta AD1 da Disponibile a Selezionato. Fare clic sul pulsante su per spostare AD1 alla priorità superiore.



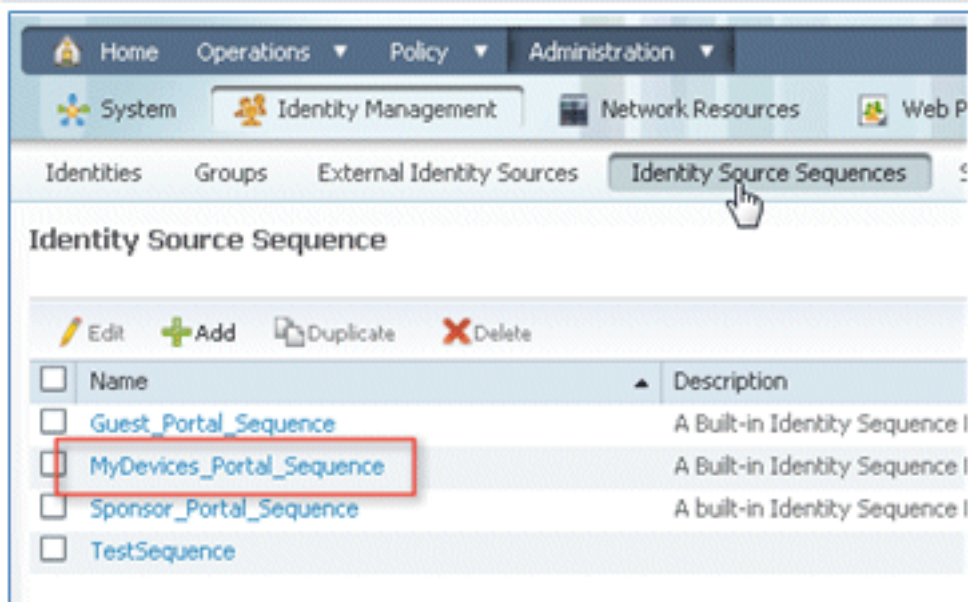
14. Per salvare, fare clic su **Submit** (Invia).



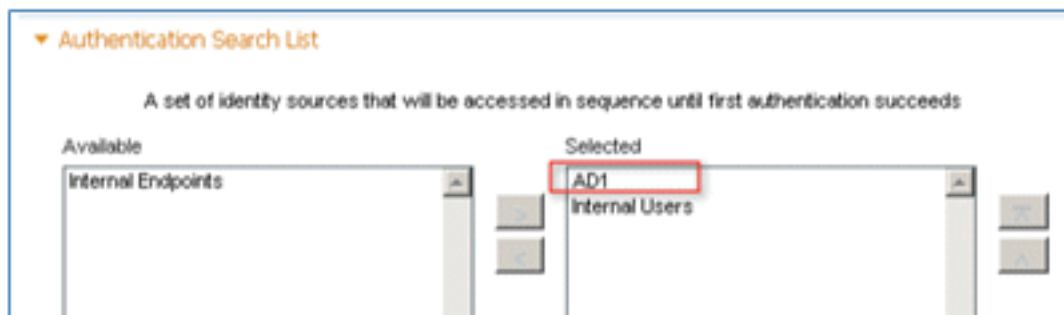
15. Confermare l'aggiunta della nuova sequenza di origine identità.



16. Utilizzare AD per autenticare il portale dei dispositivi personali. Selezionare ISE > Amministrazione > Gestione identità > Sequenza origine identità, quindi modificare MyDevices_Portal_Sequence.



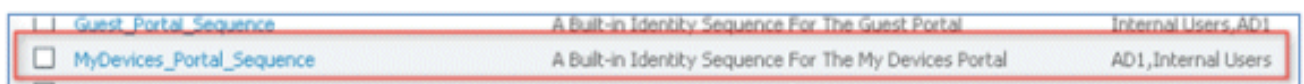
17. Aggiungere **AD1** all'elenco Selezionati e fare clic sul pulsante su per spostare AD1 alla priorità superiore.



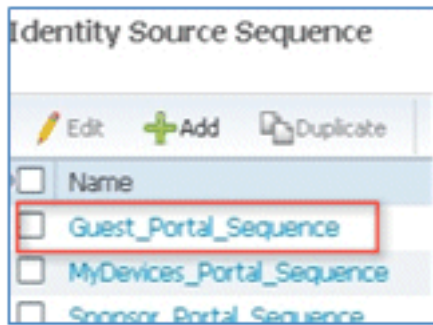
18. Fare clic su **Salva**.



19. Confermare che la sequenza dell'archivio identità per MyDevices_Portal_Sequence contenga **AD1**.



20. Ripetere i passaggi da 16 a 19 per aggiungere AD1 per Guest_Portal_Sequence e fare clic su **Salva**.



21. Confermare che Guest_Portal_Sequence contenga **AD1**.

<input type="checkbox"/>	Name	Description	Identity Stores
<input type="checkbox"/>	Guest_Portal_Sequence	A Built-in Identity Sequence For The Guest Portal	Internal Users,AD1

22. Per aggiungere il WLC al dispositivo di accesso alla rete (WLC), selezionare **Amministrazione > Risorse di rete > Dispositivi di rete**, quindi fare clic su **Aggiungi**.



23. Aggiungere il nome del WLC, l'indirizzo IP, la subnet mask e così via.

Network Devices List > New Network Device

Network Devices

* Name

Description

* IP Address: /

Model Name

Software Version

* Network Device Group

Location

Device Type

24. Scorrere fino a Impostazioni di autenticazione e immettere il segreto condiviso. Deve corrispondere al segreto condiviso del RADIUS del WLC.

Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret

Enable KeyWrap ⓘ

* Key Encryption Key

* Message Authenticator Code Key

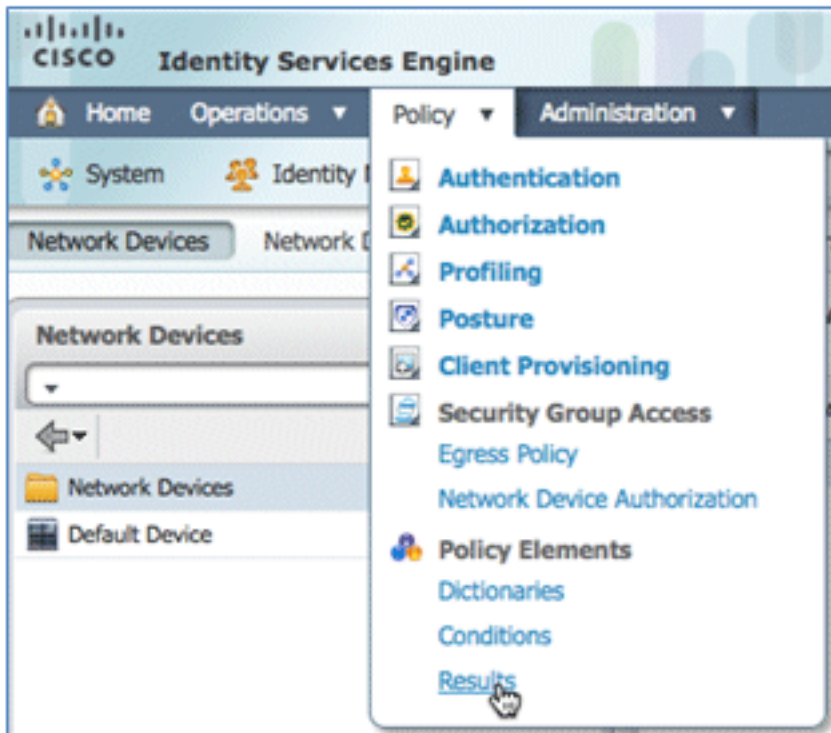
Key Input Format ASCII HEXADECIMAL

▶ SNMP Settings

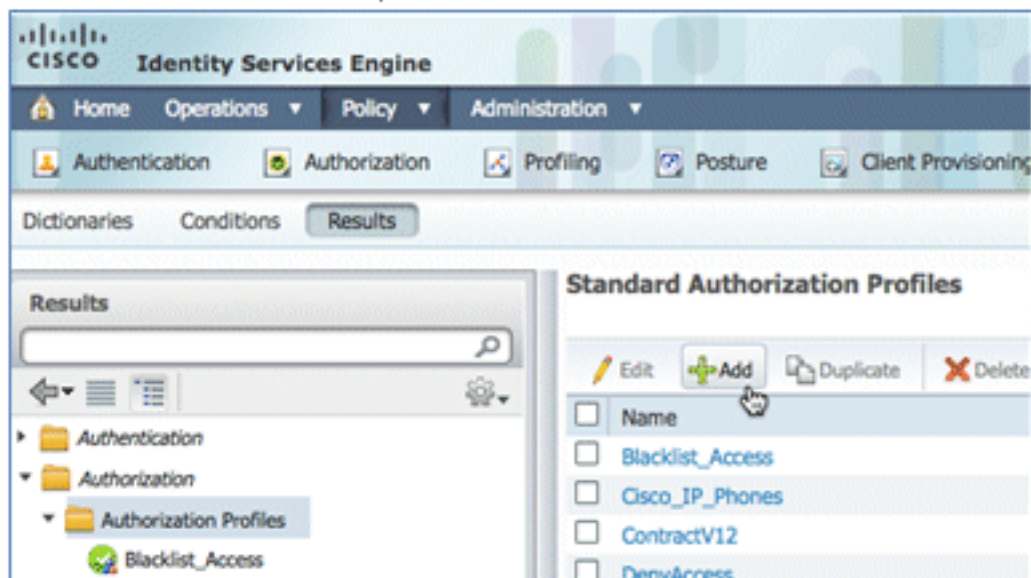
▶ SGA Attributes

25. Fare clic su **Invia**.

26. Selezionare **ISE > Policy > Policy Elements > Results** (Risultati criteri).



27. Espandere **Risultati e autorizzazione**, fare clic su **Profili di autorizzazione**, quindi fare clic su **Aggiungi** per un nuovo profilo.



28. Assegna al profilo i seguenti valori:

Nome: **CWA**

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type

Abilita autenticazione Web (casella selezionata):

Autenticazione Web: **centralizzata**ACL: **ACL-REDIRECT** (deve corrispondere al nome dell'ACL di preautenticazione WLC).Reindirizzamento: **predefinito**

Common Tasks

DACL Name

VLAN

Voice Domain Permission

Web Authentication ACL Redirect

29. Fare clic su **Invia** e verificare che il profilo di autorizzazione CWA sia stato aggiunto.

Standard Authorization Profiles

Edit Add Duplicate Delete

Name

Blacklist_Access

CWA

Cisco_IP_Phones

30. Per creare un nuovo profilo di autorizzazione, fare clic su **Add** (Aggiungi).

Standard Authorization Profiles

Edit Add Duplicate Delete

Name

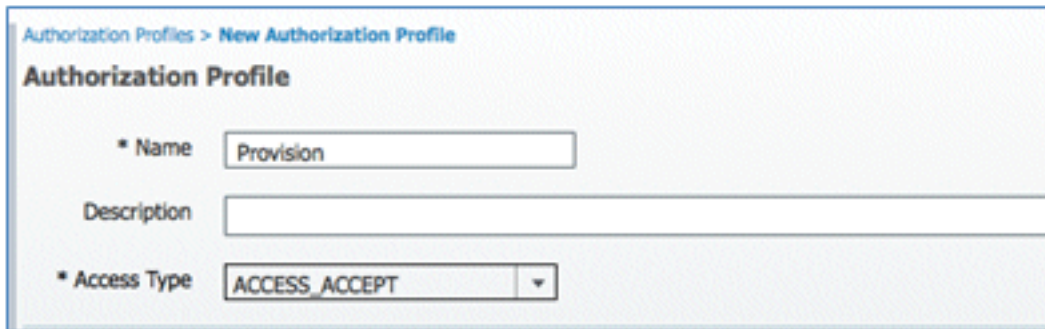
Blacklist_Access

CWA

Cisco_IP_Phones

31. Assegna al profilo i seguenti valori:

Nome: **Provisioning**



Authorization Profiles > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type

Abilita autenticazione Web (casella selezionata):

Valore autenticazione Web: **provisioning supplicant**



Common Tasks

DACL Name

VLAN

Voice Domain Permission

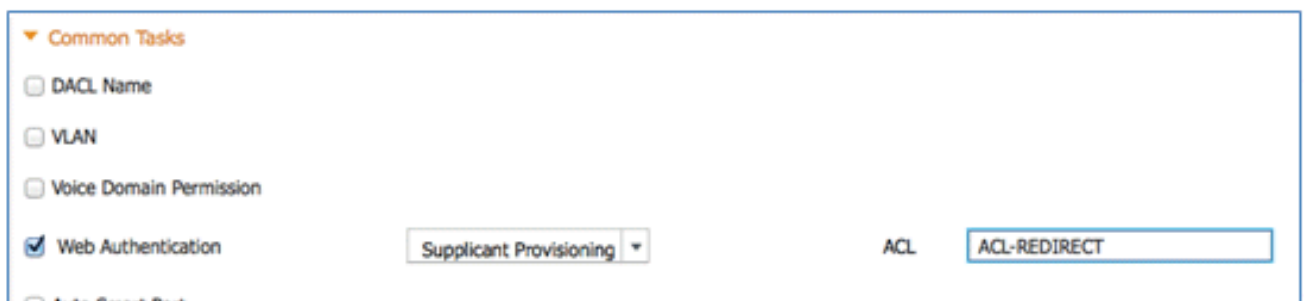
Web Authentication ACL

Auto Smart Port

Filter-ID

Centralized
Device Registration
Posture Discovery
Supplicant Provisioning

ACL: **ACL-REDIRECT** (deve corrispondere al nome dell'ACL di preautenticazione WLC).



Common Tasks

DACL Name

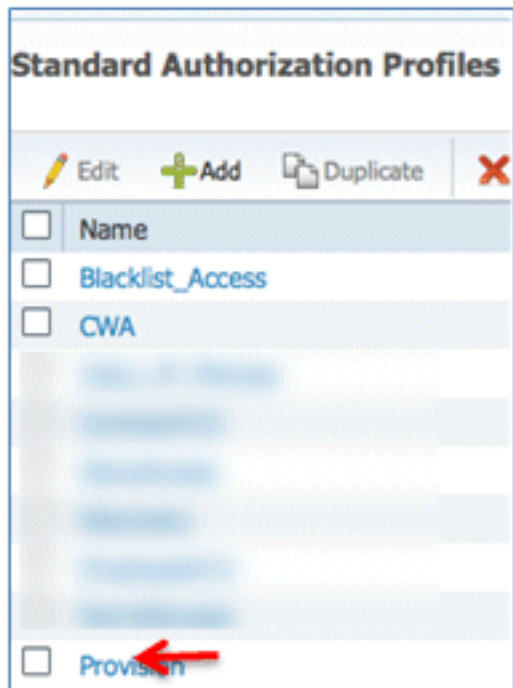
VLAN

Voice Domain Permission

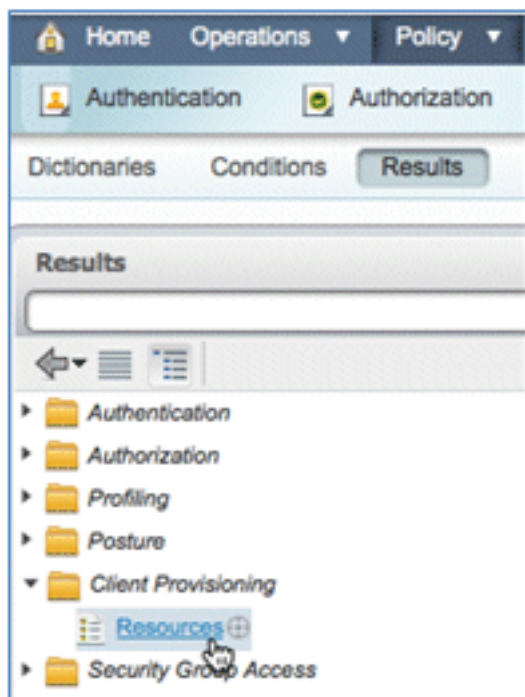
Web Authentication ACL

Auto Smart Port

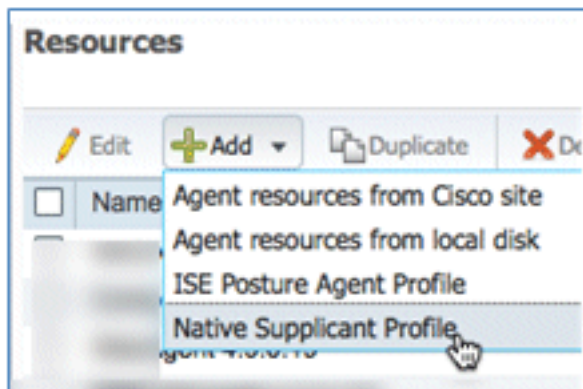
32. Fare clic su **Invia** e confermare che il profilo di autorizzazione del provisioning è stato aggiunto.



33. Scorrere verso il basso in Risultati, espandere **Provisioning client** e fare clic su **Risorse**.



34. Selezionare **Profilo supplicat nativo**.



35. Assegnare al profilo il nome **WirelessSP** (in questo esempio).

Native Supplicant Profile

* Name

Description

36. Immettere i seguenti valori:

Tipo di connessione: **wirelessSSID: Demo1x** (questo valore deriva dalla configurazione WLC 802.1x WLAN) Protocollo consentito: **TLS** Dimensioni della chiave: **1024**

* Operating System

* Connection Type Wired Wireless

* SSID

Security

* Allowed Protocol

Optional Settings

- TLS
- PEAP

Submit Cancel

37. Fare clic su **Invia**.

38. Fare clic su **Salva**.

* Allowed Protocol

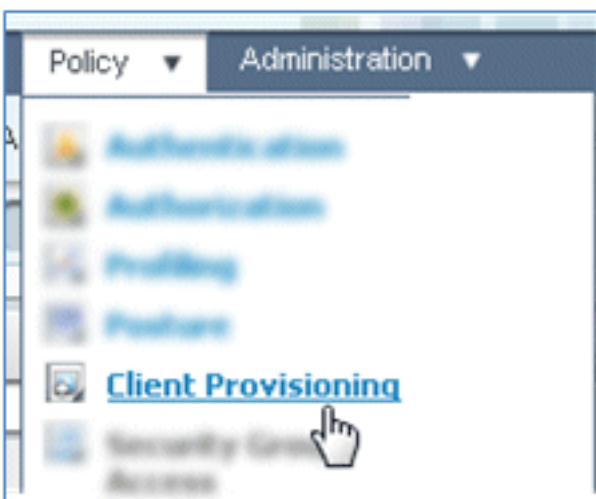
* Key Size

39. Confermare che il nuovo profilo è stato aggiunto.

Resources

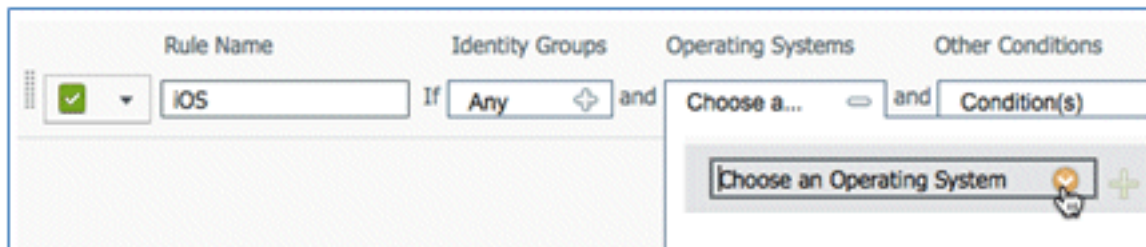
<input type="checkbox"/>	Name	Type
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>	WirelessS...	NativeSPProfile

40. Passare a **Policy > Client Provisioning**.

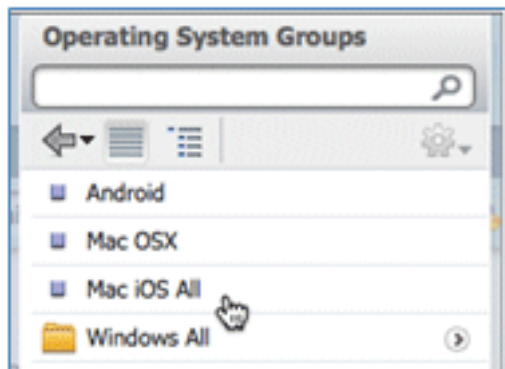


41. Immettere i seguenti valori per la regola di provisioning dei dispositivi iOS:

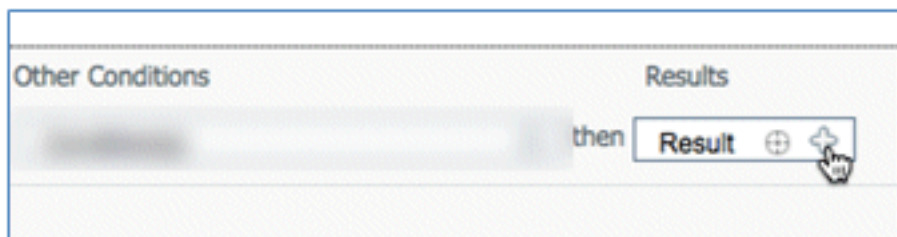
Nome regola: **iOS** Gruppi di identità: **qualsiasi**



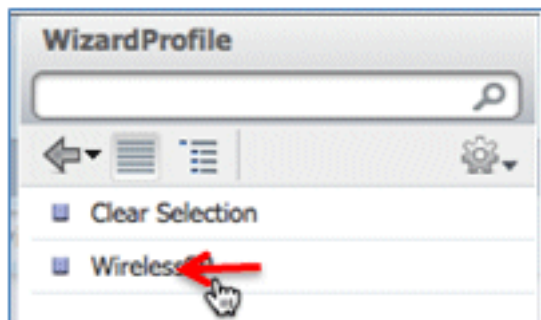
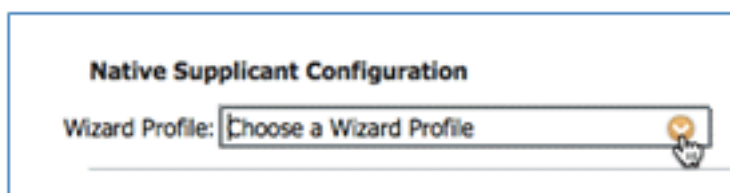
Sistemi operativi: **Mac iOS All**



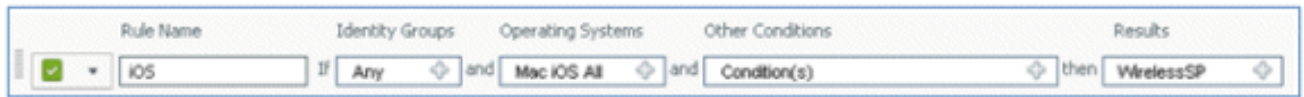
Risultati: **WirelessSP** (profilo supplicant nativo creato in precedenza)



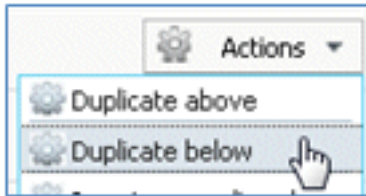
Passare a **Risultati** > **Profilo procedura guidata** (elenco a discesa) > **WirelessSP**.



42. Confermare che il profilo di provisioning iOS è stato aggiunto.



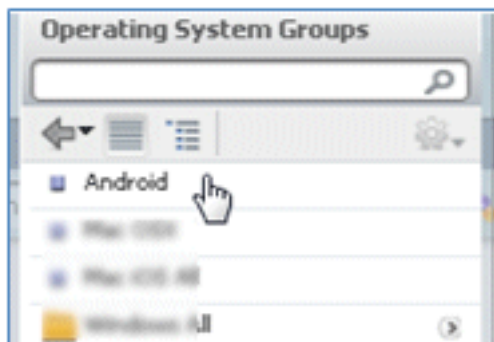
43. Sul lato destro della prima regola, individuare l'elenco a discesa Azioni e selezionare **Duplica sotto** o sopra.



44. Modificare il nome della nuova regola in **Android**.



45. Cambiare i sistemi operativi in **Android**.

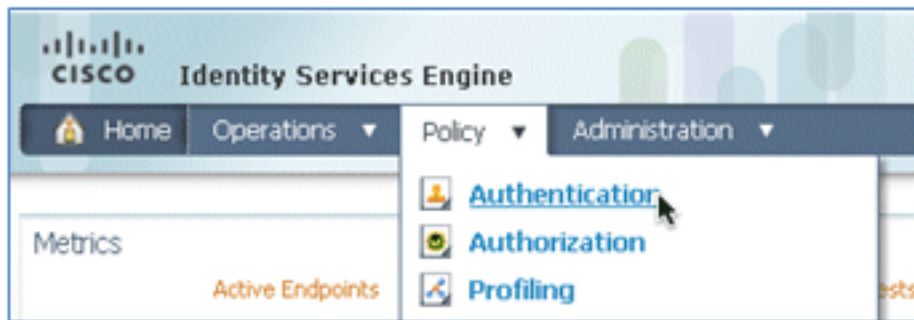


46. Non modificare altri valori.

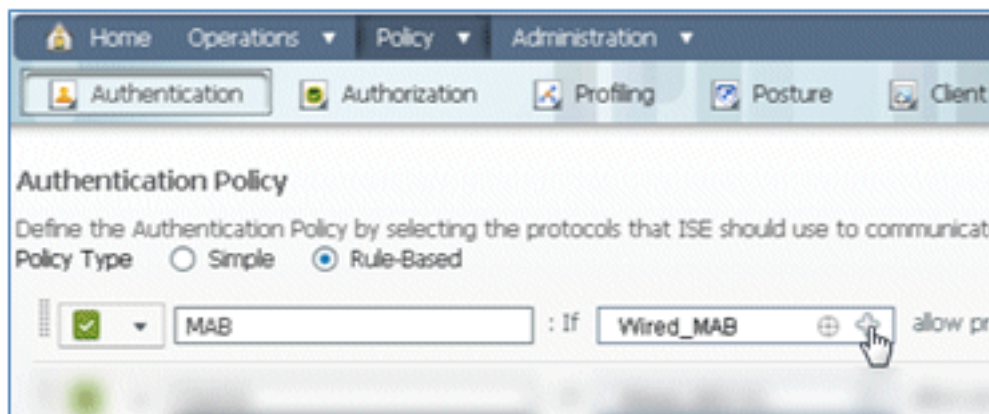
47. Fare clic su **Save** (schermata in basso a sinistra).



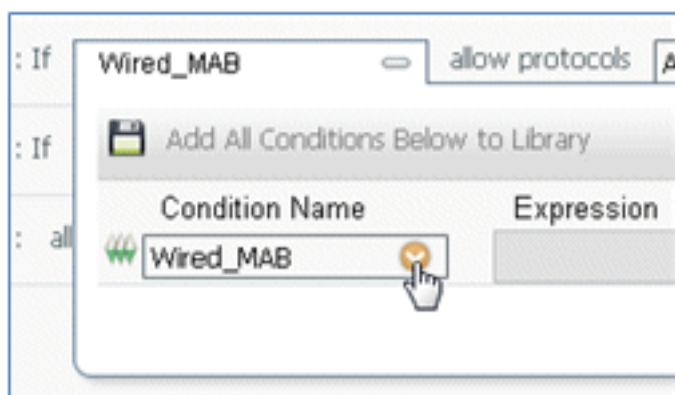
48. Selezionare **ISE > Policy > Authentication** (Autenticazione).



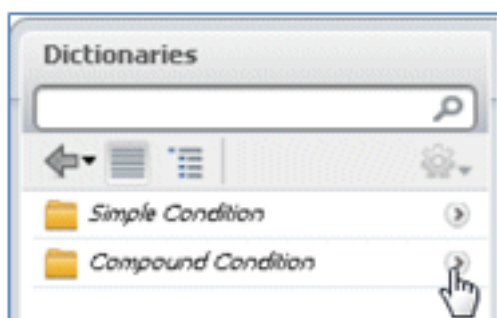
49. Modificare la condizione in modo da includere Wireless_MAB ed espandere **Wired_MAB**.



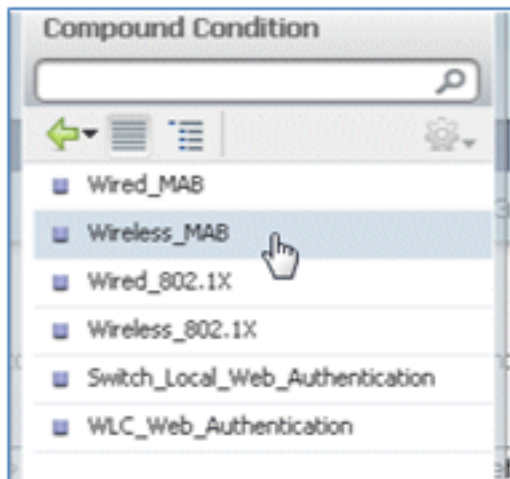
50. Fare clic sull'elenco a discesa **Nome condizione**.



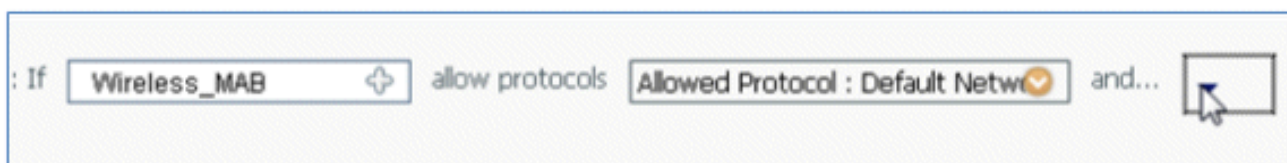
51. Selezionare **Dizionari > Condizione composta**.



52. Selezionare **Wireless_MAB**.

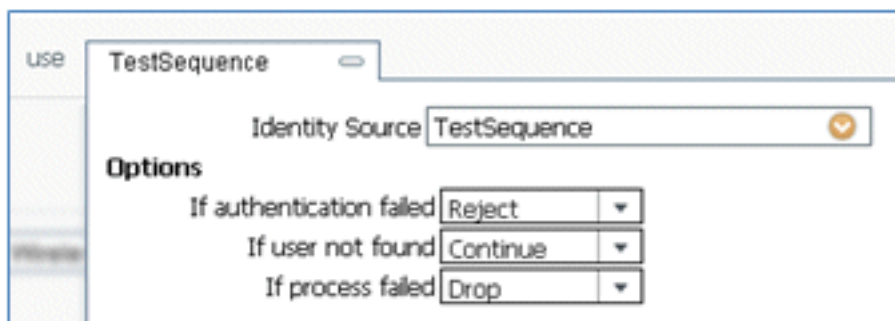


53. A destra della regola, selezionare la freccia da espandere.

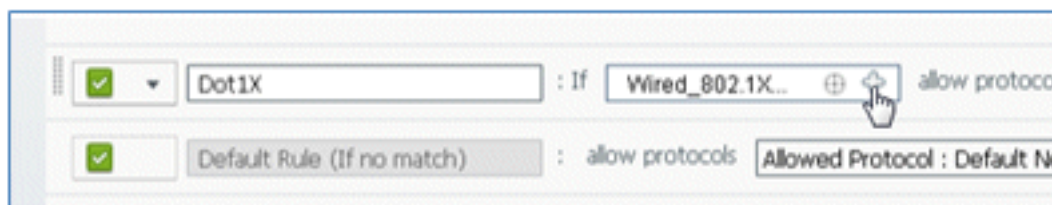


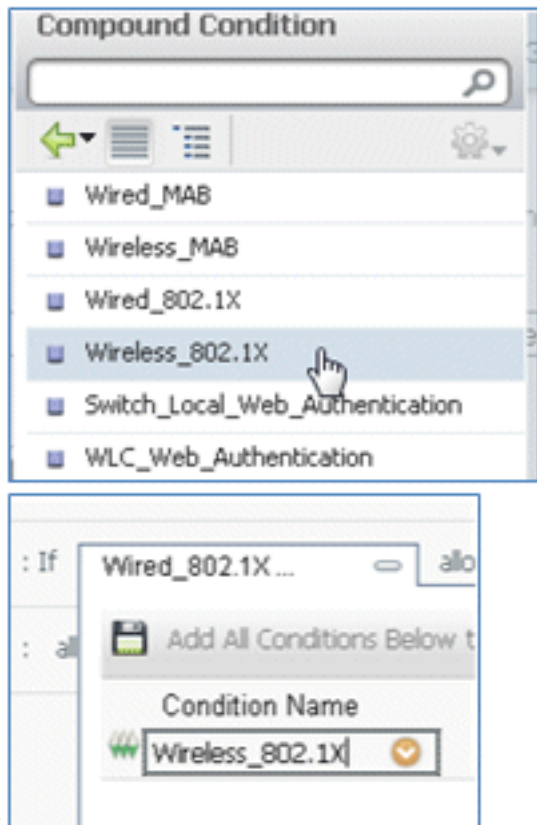
54. Selezionare i valori seguenti dall'elenco a discesa:

Origine identità: **TestSequence** (valore creato in precedenza)
 Se l'autenticazione non è riuscita: **Rifiuta**
 Se l'utente non è stato trovato: **Continua**
 Se il processo non è riuscito: **Elimina**



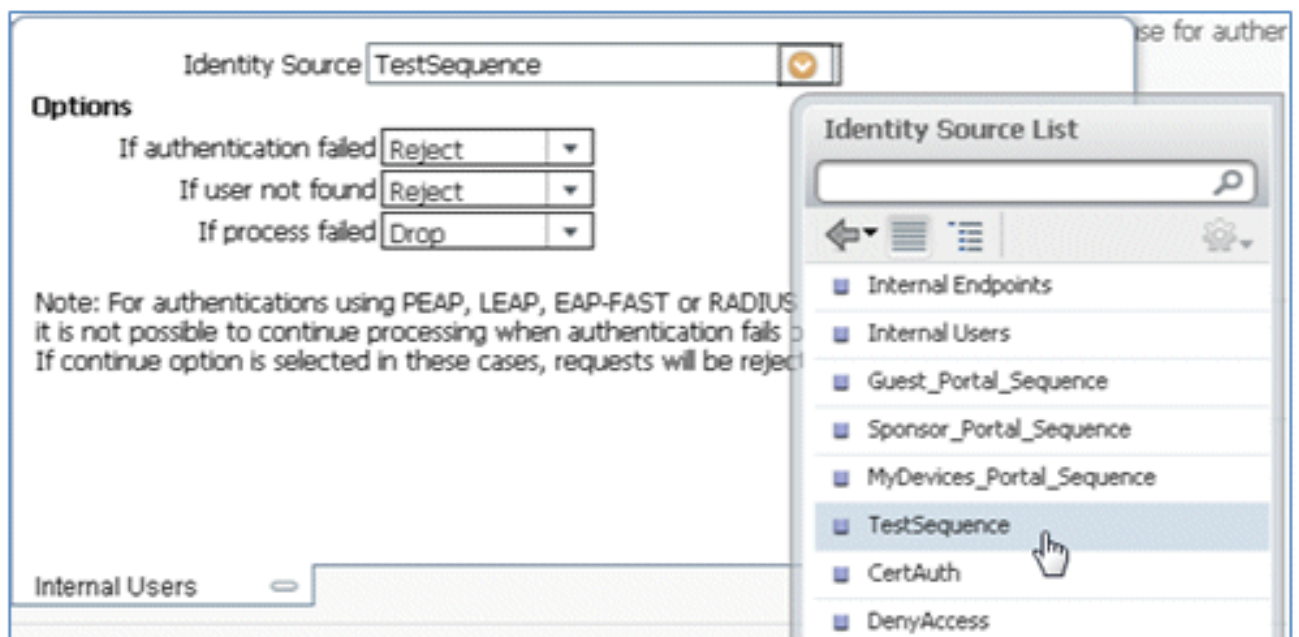
55. Passare alla regola **Dot1X** e modificare i valori seguenti:





Condizione: **Wireless_802.1X**

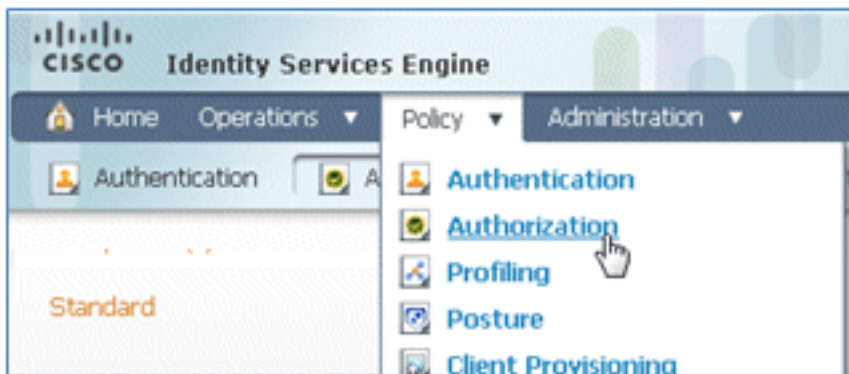
Origine identità: **TestSequence**



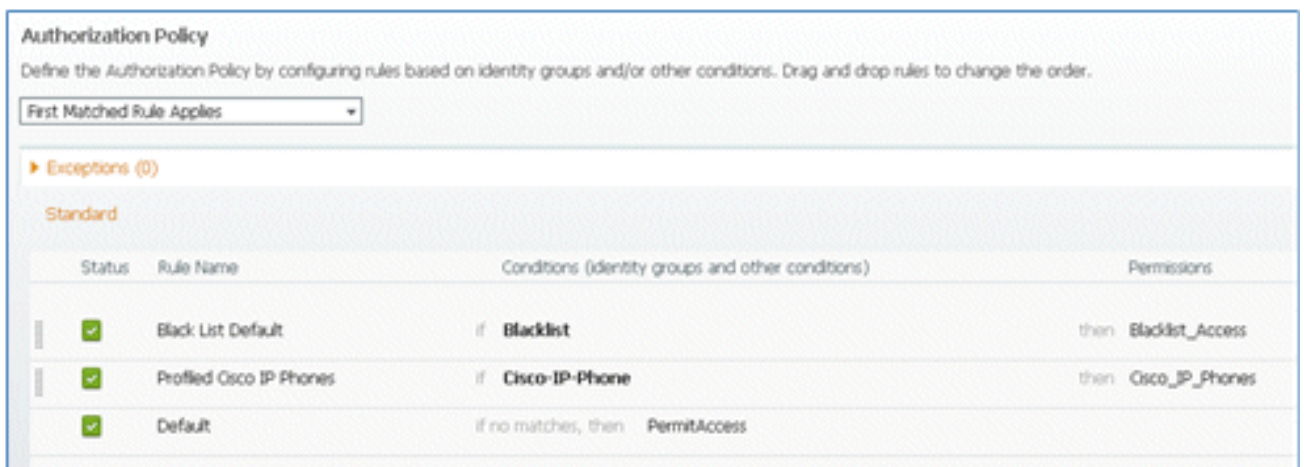
56. Fare clic su **Salva**.



57. Selezionare **ISE > Policy > Authorization** (Policy > Autorizzazione).



58. Le regole predefinite (ad esempio Black List Default, Profiled e Default) sono già configurate dall'installazione; le prime due possono essere ignorate; la regola predefinita verrà modificata in seguito.



59. A destra della seconda regola (Telefoni IP Cisco con profilo), fare clic sulla freccia in giù accanto a Modifica e selezionare **Inserisci nuova regola sotto**.



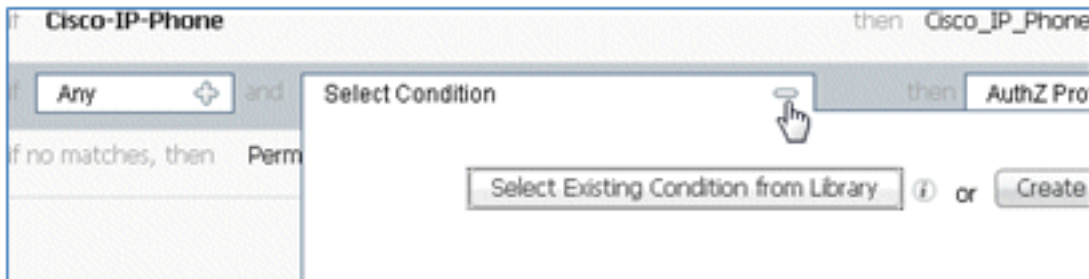
Viene aggiunto un nuovo numero di regola standard.



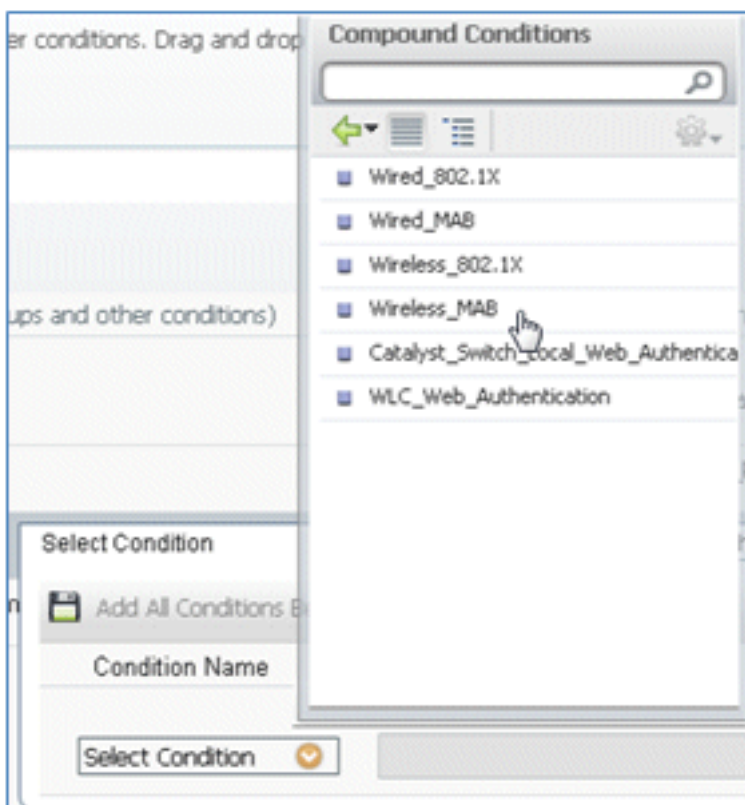
60. Modificare il nome della regola da Standard Rule # a **OpenCWA**. Questa regola avvia il processo di registrazione sulla WLAN aperta (SSID doppio) per gli utenti che vengono alla rete guest per eseguire il provisioning dei dispositivi.



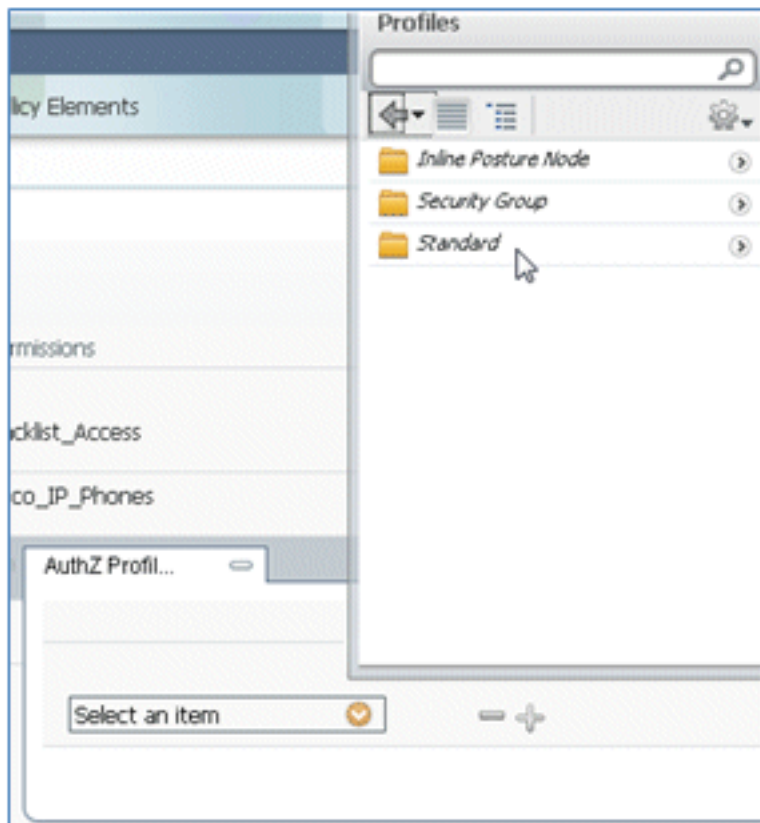
61. Fare clic sul segno più (+) per Condizione/i, quindi fare clic su **Seleziona condizione esistente dalla libreria**.



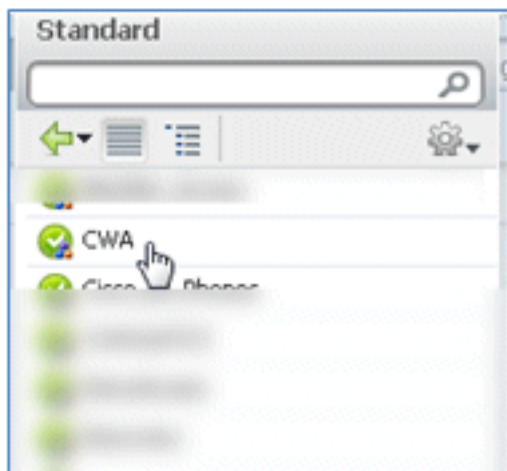
62. Selezionare **Condizioni composte > Wireless_MAB**.



63. Nel Profilo AuthZ, fare clic sul segno più (+), quindi selezionare **Standard**.



64. Selezionare il **CWA** standard (profilo di autorizzazione creato in precedenza).



65. Confermare che la regola sia stata aggiunta con le condizioni e l'autorizzazione corrette.



66. Fare clic su **Done** (sul lato destro della regola).

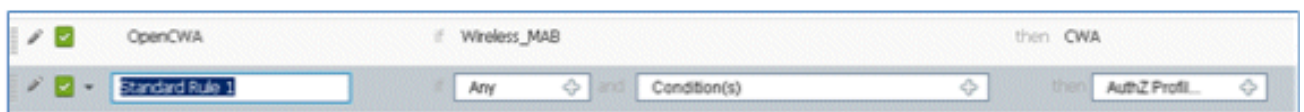


67. A destra della stessa regola, fare clic sulla freccia in giù accanto a Modifica e selezionare

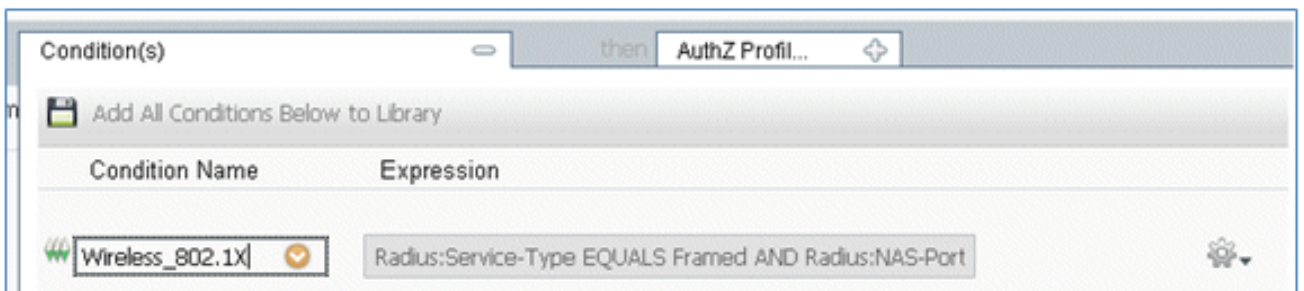
Inserisci nuova regola sotto.



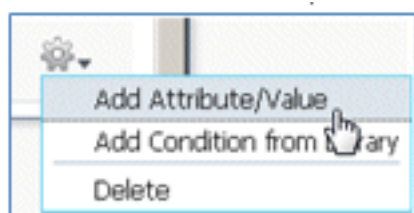
68. Modificare il nome della regola da Standard Rule # a **PEAPrule** (in questo esempio). Questa regola viene utilizzata per PEAP (utilizzato anche per uno scenario SSID singolo) per verificare che l'autenticazione di 802.1X senza Transport Layer Security (TLS) e il provisioning del supplicant di rete vengano avviati con il profilo di autorizzazione del provisioning creato in precedenza.



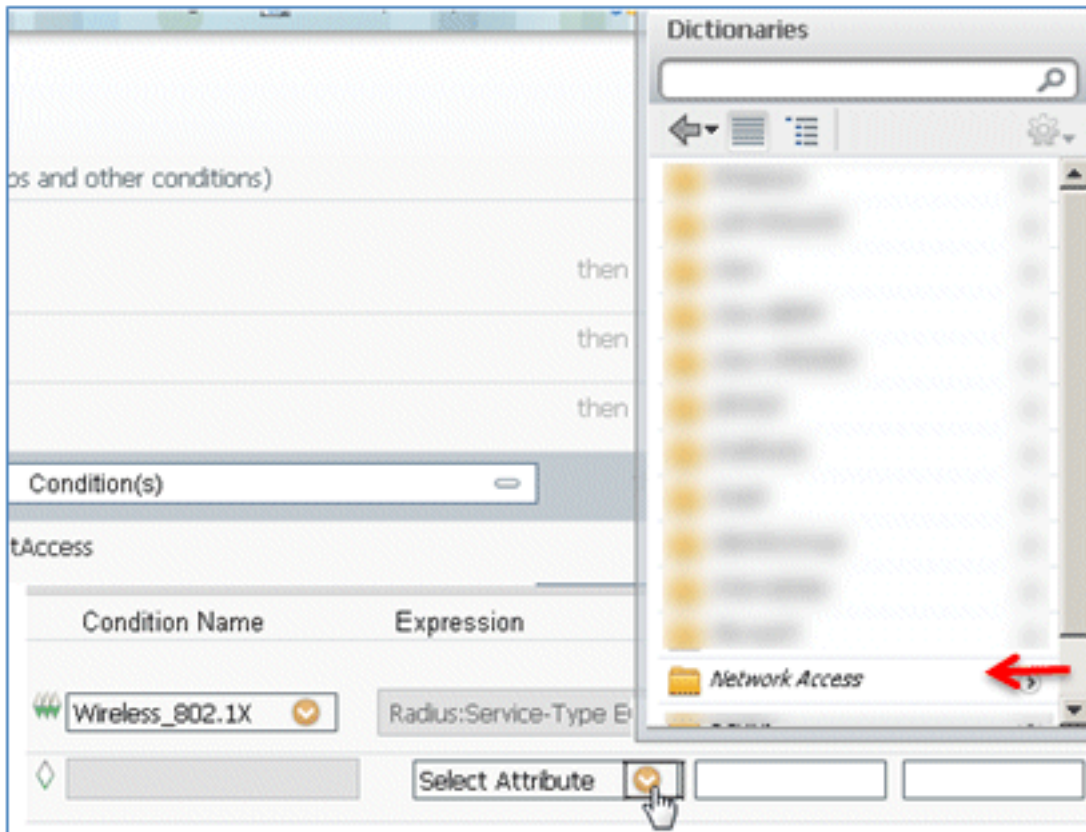
69. Modificare la condizione in **Wireless_802.1X**.



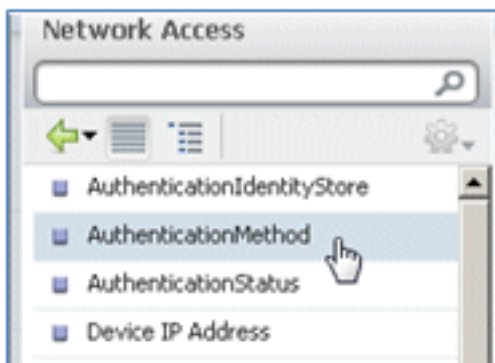
70. Fare clic sull'icona dell'ingranaggio sul lato destro della condizione e selezionare **Aggiungi attributo/valore**. Condizione 'and', non 'or'.



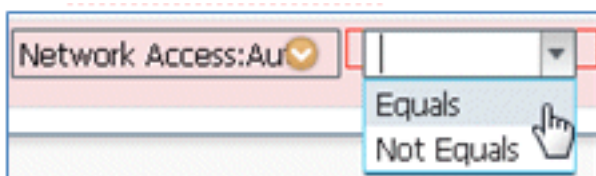
71. Individuare e selezionare **Accesso alla rete**.



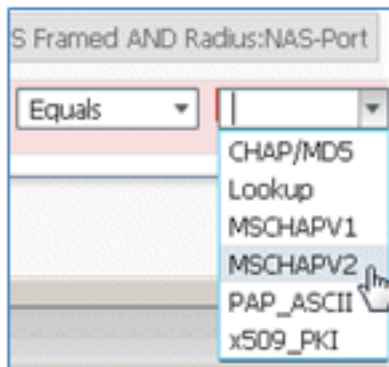
72. Selezionare **AuthenticationMethod** e immettere i seguenti valori:



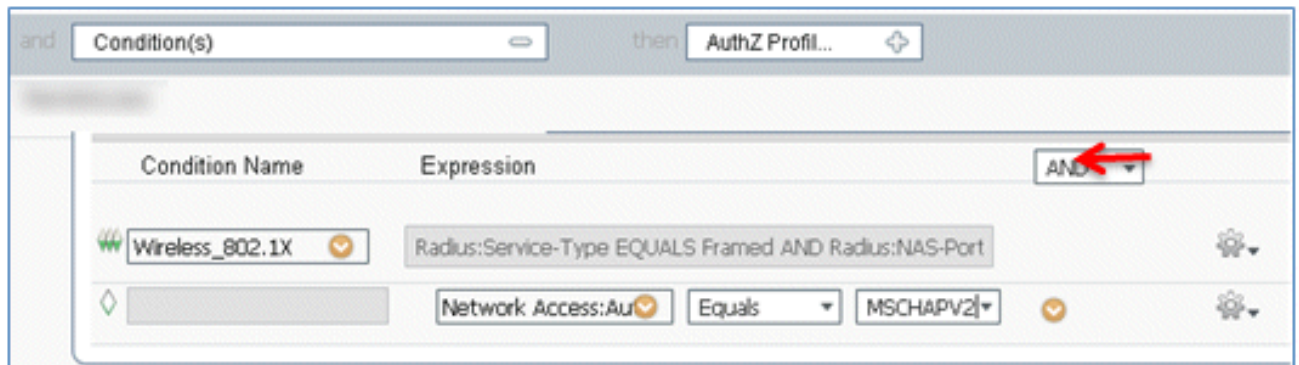
AuthenticationMethod: **uguale a**



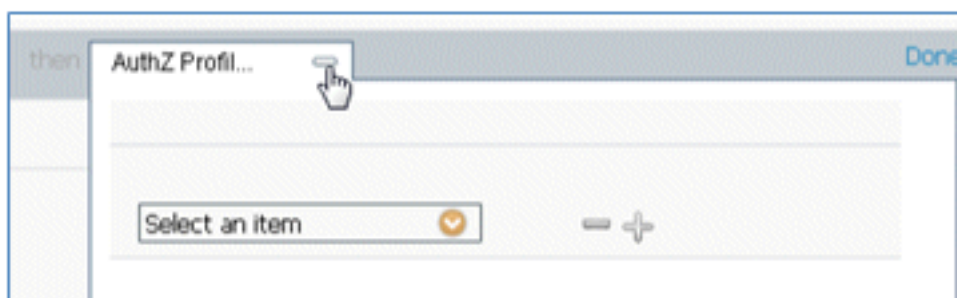
Selezionare **MSCHAPV2**.

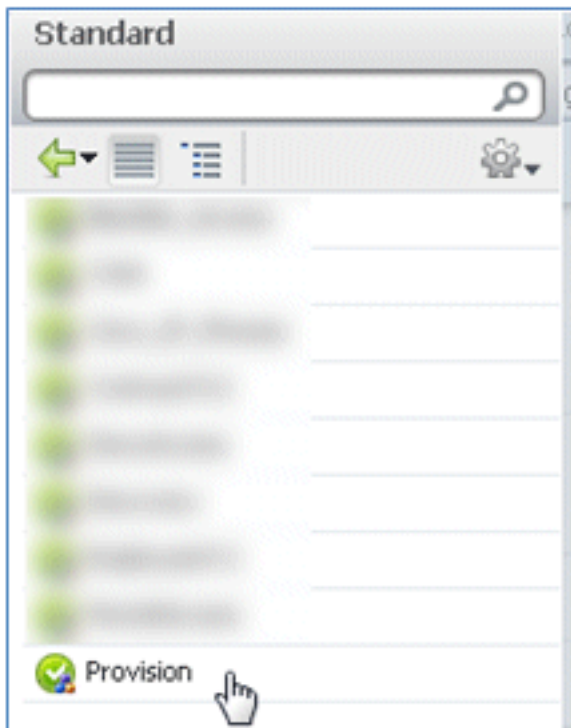


Questo è un esempio della regola. Accertarsi che la condizione sia AND.

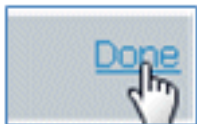


73. In Profilo AuthZ, selezionare **Standard > Provisioning** (profilo di autorizzazione creato in precedenza).





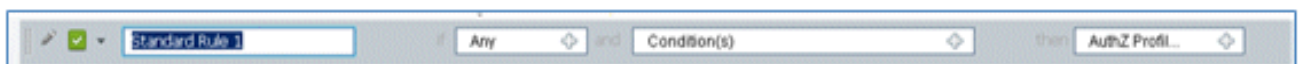
74. Selezionate **Fatto (Done)**.



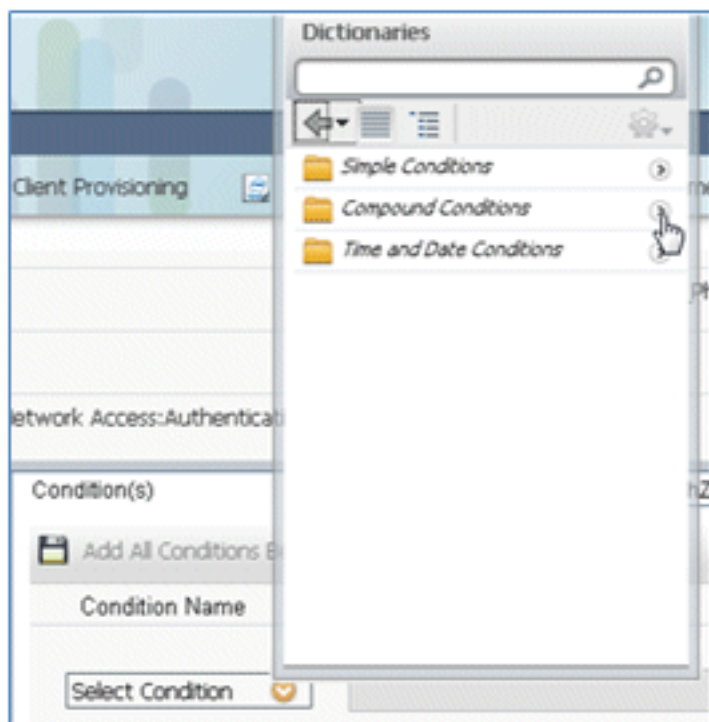
75. A destra della regola PEAP, fare clic sulla freccia in giù accanto a Modifica e selezionare **Inserisci nuova regola sotto**.



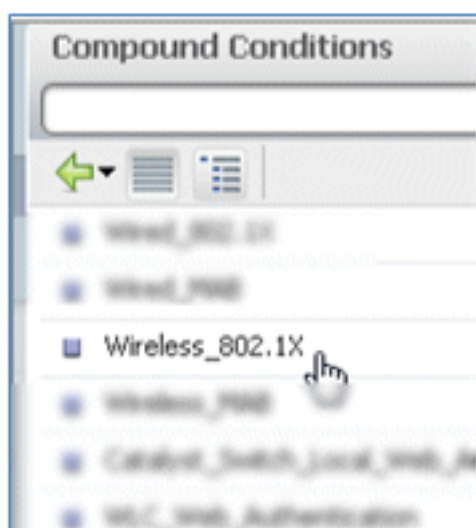
76. Modificare il nome della regola da Standard Rule # a **AllowRule** (in questo esempio). Questa regola verrà utilizzata per consentire l'accesso alle periferiche registrate con certificati installati.



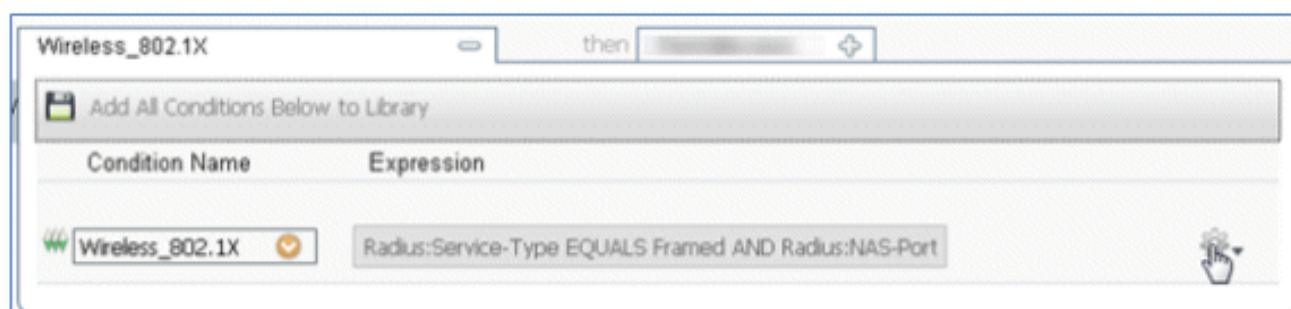
77. In Condizioni selezionare **Condizioni composte**.



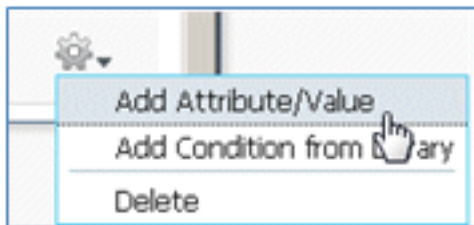
78. Selezionare **Wireless_802.1X**.



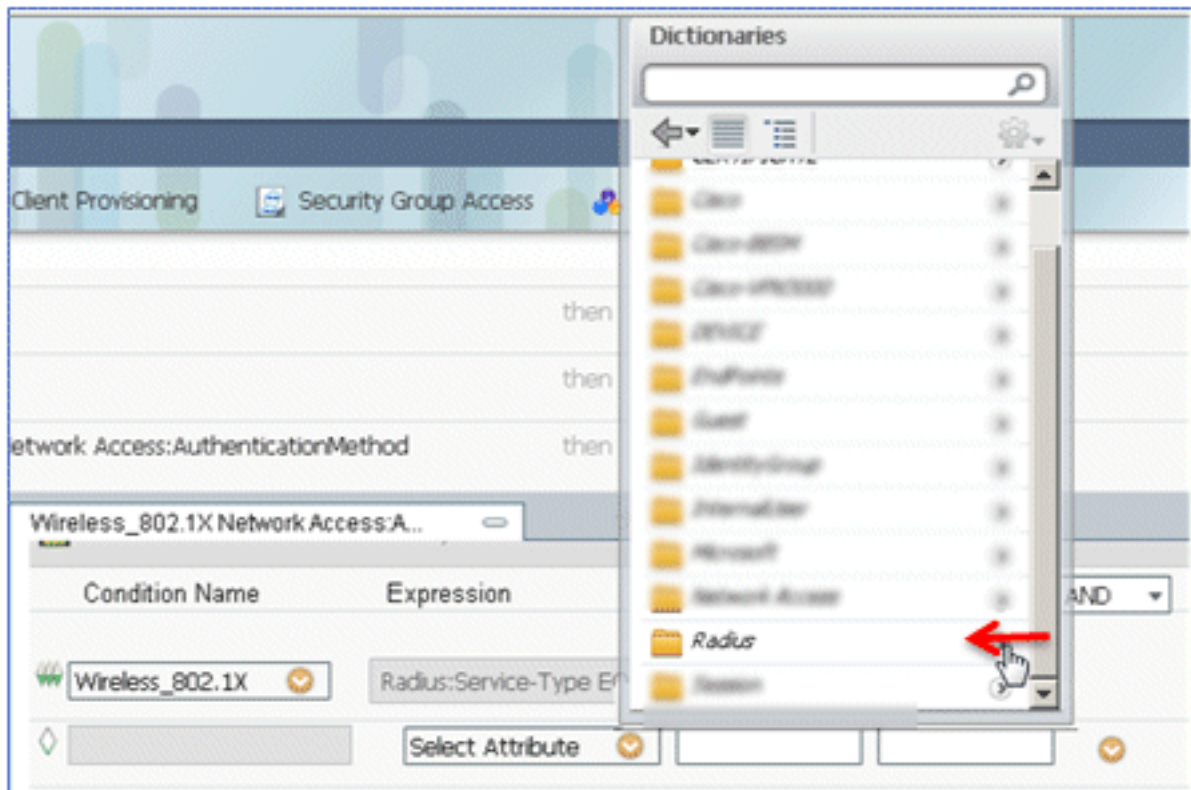
79. Aggiungere un attributo AND.



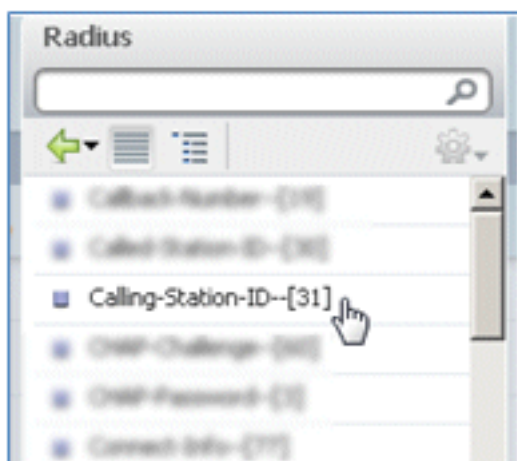
80. Fare clic sull'icona dell'ingranaggio sul lato destro della condizione e selezionare **Aggiungi attributo/valore**.



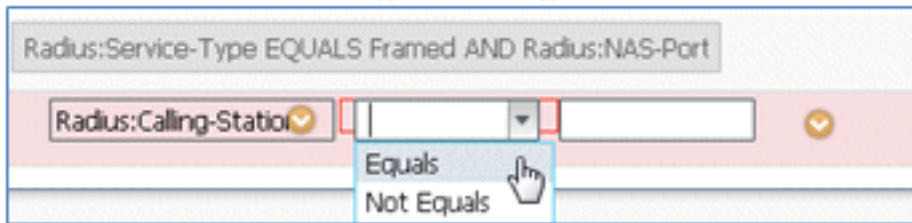
81. Individuate e selezionate **Raggio (Radius)**.



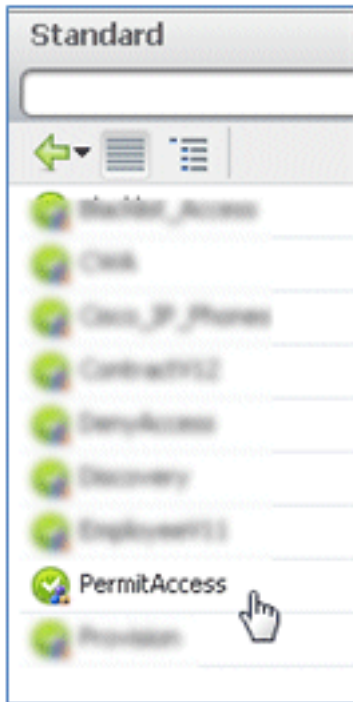
82. Selezionare **Calling-Station-ID--[31]**.



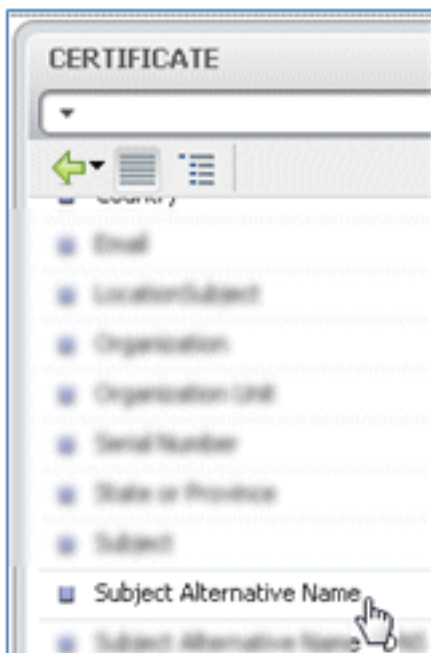
83. Selezionare **Uguale a**.



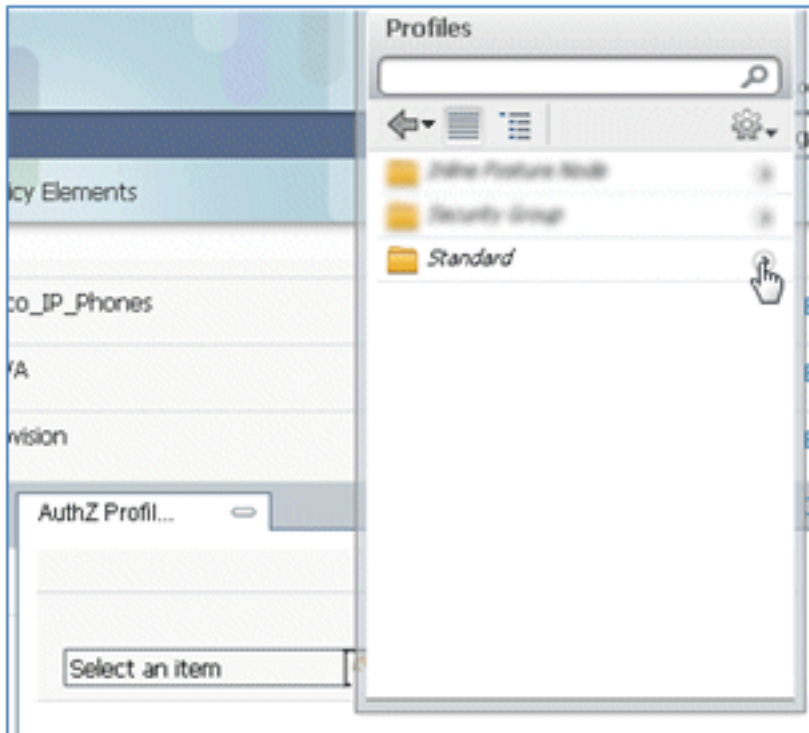
84. Passare a **CERTIFICATO** e fare clic sulla freccia destra.



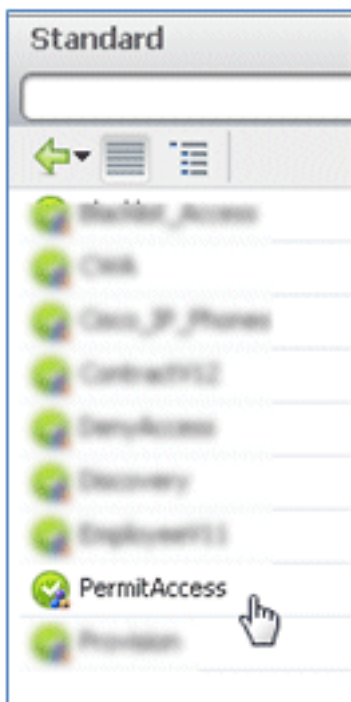
85. Selezionare **Nome alternativo soggetto**.



86. Per il profilo AuthZ, selezionare **Standard**.



87. Selezionare **Permit Access**.



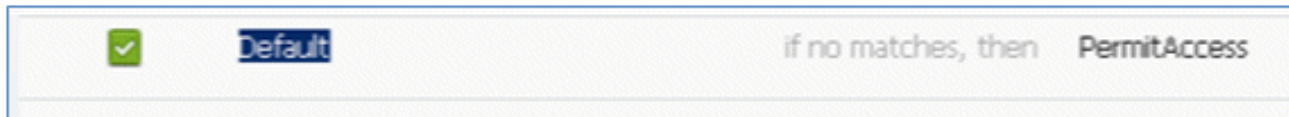
88. Selezionate **Fatto (Done)**.



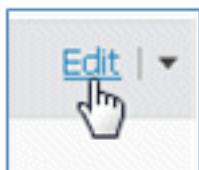
Questo è un esempio della regola:

	OpenCWA	Wireless_M40	then: Deny
	PerfHub	Wireless_802.1X (1): Network-Access:AuthenticationMethod EQUALS RADIUS(2)	then: Permit
	AllowRule	Wireless_802.1X Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject.AltitudeName	then: PermitAccess

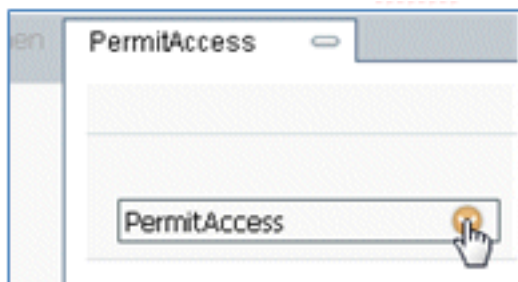
89. Individuare la regola predefinita per modificare PermitAccess in DenyAccess.



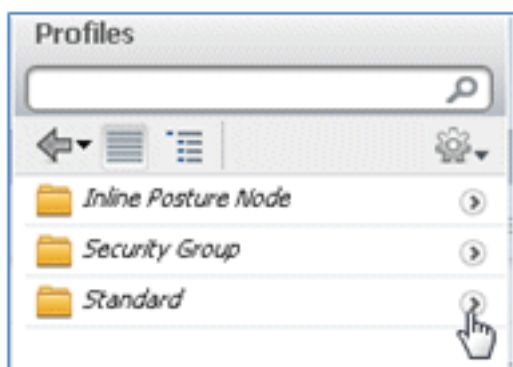
90. Per modificare la regola predefinita, fare clic su **Modifica**.



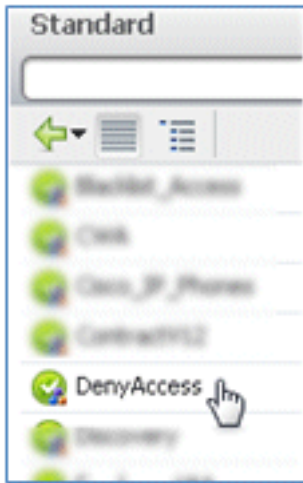
91. Passare al profilo AuthZ esistente di PermitAccess.



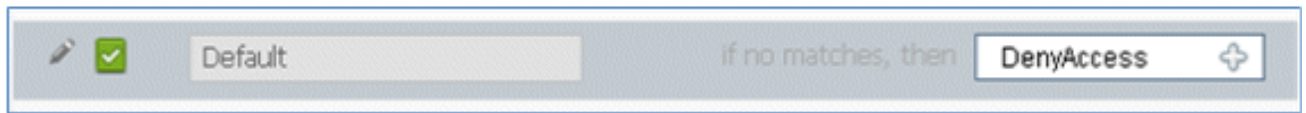
92. Selezionare **Standard**.



93. Selezionare **DenyAccess**.



94. Confermare che la regola predefinita disponga di DenyAccess se non vengono trovate corrispondenze.



95. Selezionate **Fatto (Done)**.



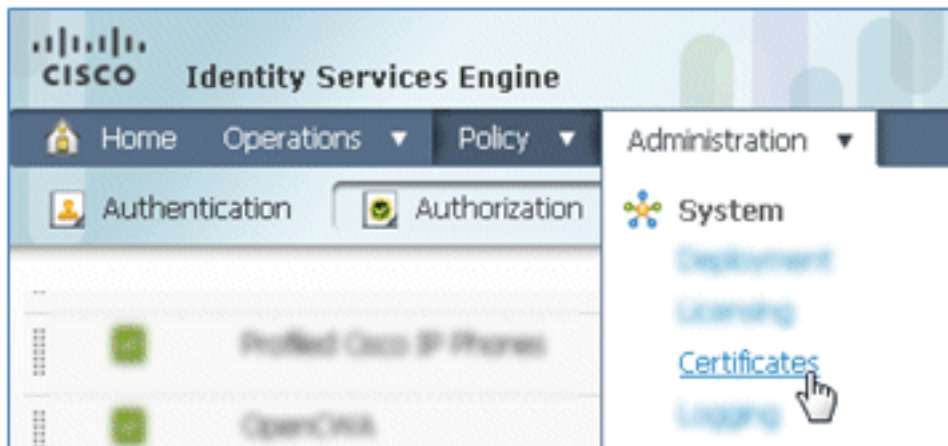
Questo è un esempio delle regole principali richieste per il test e sono applicabili per uno scenario SSID singolo o SSID doppio.

<input checked="" type="checkbox"/>	OpenCWA	if Wireless_MAB	then CWA
<input checked="" type="checkbox"/>	PEAPrule	if (Wireless_802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	then Provision
<input checked="" type="checkbox"/>	AllowRule	if (Wireless_802.1X AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name)	then PermitAccess
<input checked="" type="checkbox"/>	Default	if no matches, then	DenyAccess

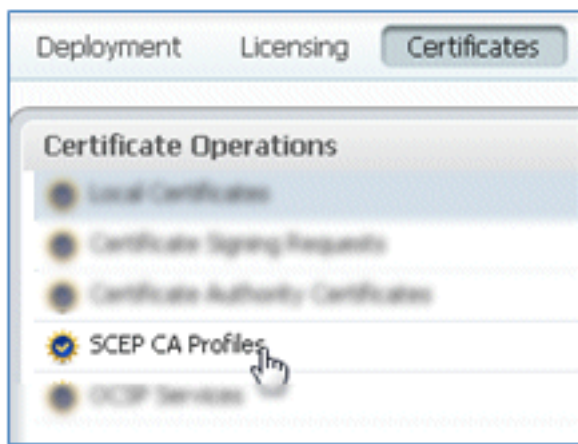
96. Fare clic su **Salva**.



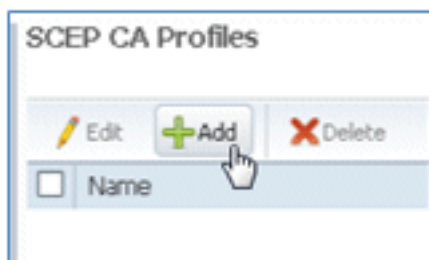
97. Per configurare il server ISE con un profilo SCEP, selezionare **ISE > Administration > System > Certificates**.



98. In Operazioni certificato fare clic su **Profili CA SCEP**.



99. Fare clic su **Add**.



100. Immettere i seguenti valori per il profilo:

Nome: **mySCEP** (in questo esempio) URL: **https://<ca-server>/CertSrv/mscep/** (verificare la configurazione del server CA per l'indirizzo corretto).

SEP Certificate Authority Certificates > New SCEP Profile

Edit Certificate

SEP Certificate Authority

* Name

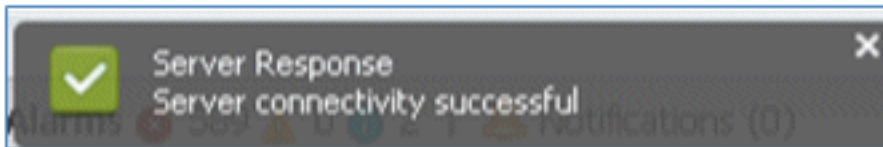
Description

* URL

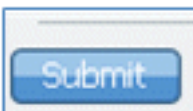
101. Fare clic su **Test connettività** per verificare la connettività della connessione SCEP.



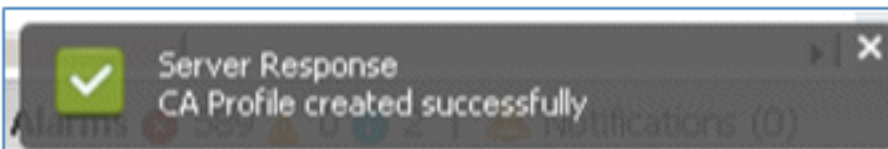
102. Questa risposta indica che la connettività del server è riuscita.



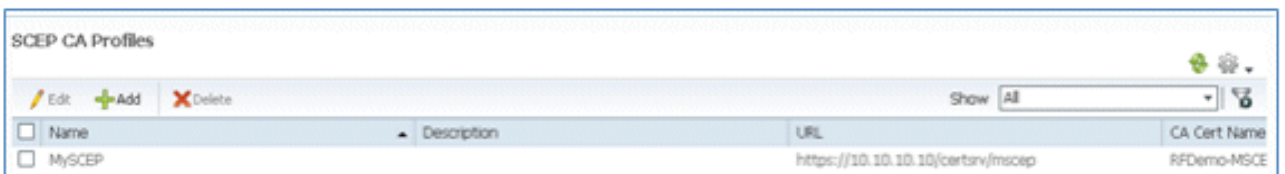
103. Fare clic su **Invia**.



104. Il server risponde che il profilo CA è stato creato correttamente.



105. Confermare che il profilo CA SCEP sia stato aggiunto.



Esperienza utente - Provisioning iOS

SSID doppio

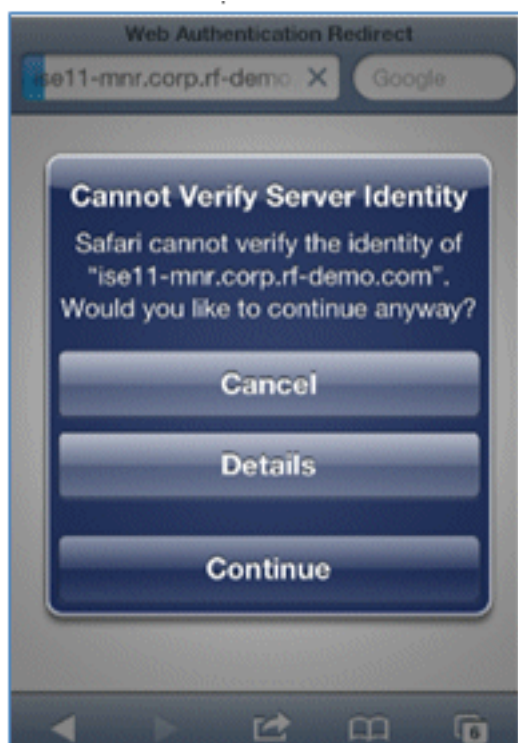
In questa sezione vengono illustrati due SSID e viene descritto come connettersi al guest di cui eseguire il provisioning e come connettersi a una WLAN 802.1x.

Completare questi passaggi per effettuare il provisioning di iOS nello scenario con doppio SSID:

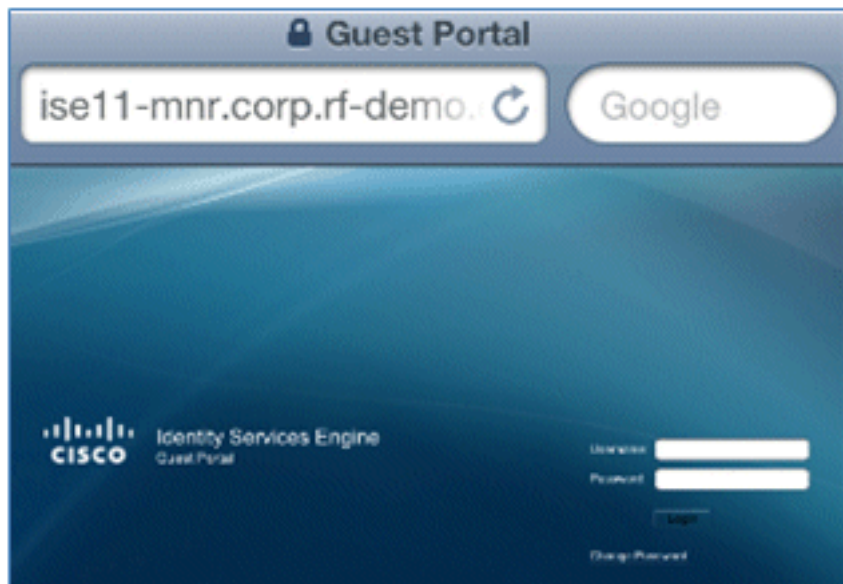
1. Sul dispositivo iOS, andare su **Reti Wi-Fi** e selezionare **DemoCWA** (configurato per aprire WLAN su WLC).



2. Aprire il browser Safari sul dispositivo iOS e visitare un URL raggiungibile (ad esempio, server Web interno/esterno). L'ISE vi reindirizza al portale. Fare clic su **Continue** (Continua).



3. Viene eseguito il reindirizzamento al portale per l'accesso.



4. Accedere con un account utente e una password di Active Directory. Installare il profilo CA quando richiesto.



5. Fare clic su **Installa** certificato protetto del server CA.



6. Fare clic su **Fine** una volta completata l'installazione del profilo.



7. Tornare al browser e fare clic su **Registra**. Prendere nota dell'ID dispositivo che contiene l'indirizzo MAC del dispositivo.



8. Per installare il profilo verificato, fare clic su **Installa**.



9. Fare clic su **Installa**.



10. Al termine del processo, il profilo WirelessSP conferma che il profilo è installato. Selezionate **Fatto (Done)**.



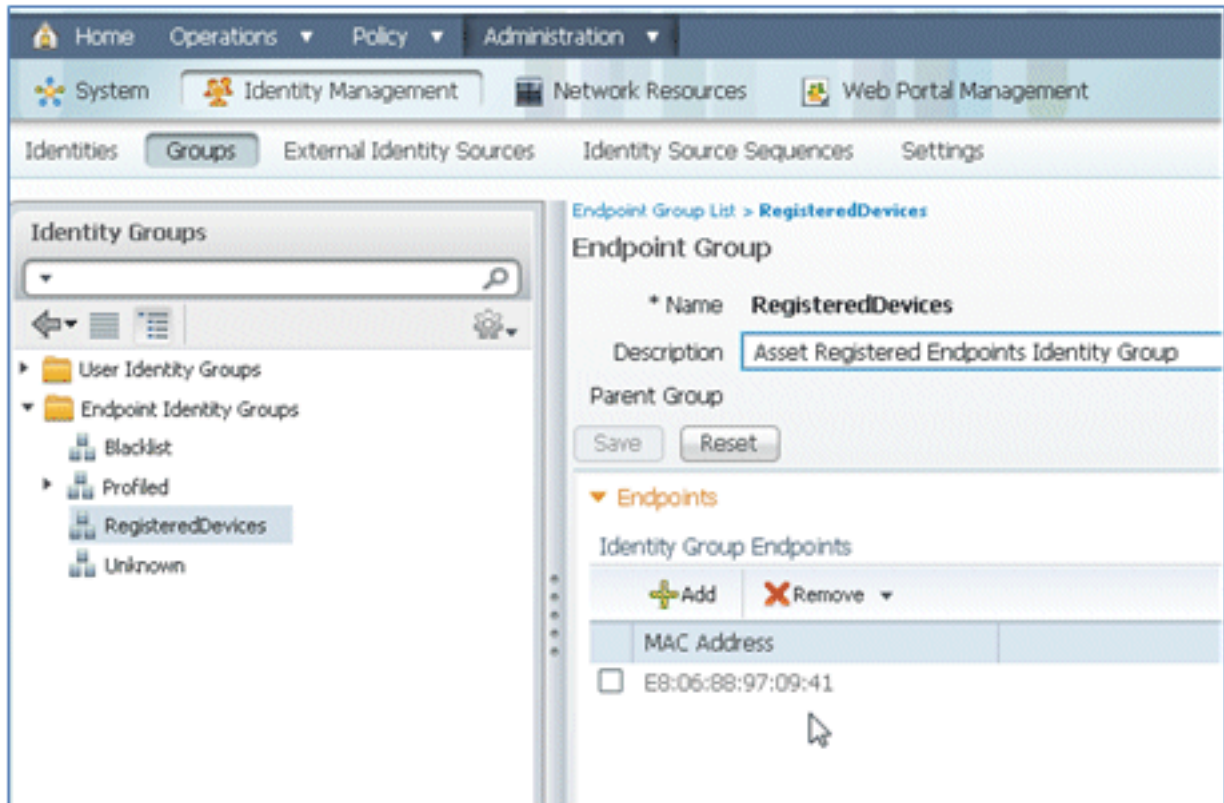
11. Accedere a **Reti Wi-Fi** e modificare la rete in **Demo1x**. Il dispositivo è ora connesso e utilizza TLS.



12. In ISE, selezionare **Operations > Authentications** (Operazioni > Autenticazioni). Gli eventi mostrano il processo in cui il dispositivo è connesso alla rete guest aperta, passa attraverso il processo di registrazione con il provisioning del richiedente e viene consentito l'accesso dopo la registrazione.

Time	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25, 12 12:27:57.052 AM	✓	🔒	paul	EE-06-80-97-09-41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25, 12 12:27:21.714 AM	✓	🔒	EE-06-80-97-09-41	EE-06-80-97-09-41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25, 12 12:27:20.438 AM	✓	🔒			WLC				Dynamic Authorization succeeded
Mar 25, 12 12:26:56.187 AM	✓	🔒	paul	EE-06-80-97-09-41	WLC	CWA	Any,Profiled Apple-Ipad	Pending	

13. Passare a ISE > Amministrazione > Gestione identità > **Gruppi** > **Gruppi di identità degli endpoint** > **Dispositivi registrati**. L'indirizzo MAC è stato aggiunto al database.

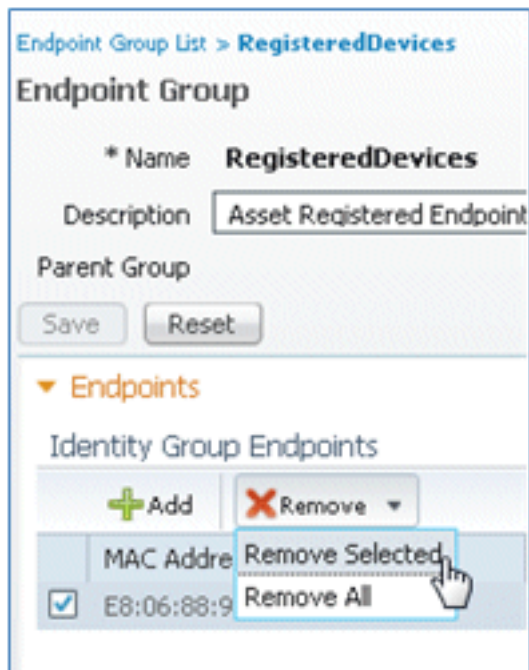


SSID singolo

In questa sezione viene descritto un singolo SSID e viene descritto come connettersi direttamente a una WLAN 802.1x, fornire nome utente e password di Active Directory per l'autenticazione PEAP, effettuare il provisioning tramite un account guest e riconnettersi a TLS.

Completare questi passaggi per eseguire il provisioning di iOS nello scenario SSID singolo:

1. Se si utilizza lo stesso dispositivo iOS, rimuovere l'endpoint dai dispositivi registrati.



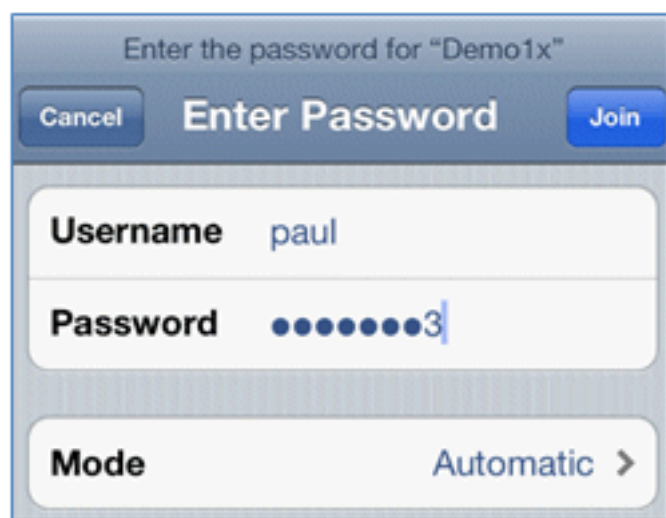
2. Sul dispositivo iOS, selezionare **Settings > General > Profiles** (Impostazioni > Generali > Profili). Rimuovere i profili installati in questo esempio.



3. Per rimuovere i profili precedenti, fare clic su **Rimuovi**.



4. Connettersi direttamente a 802.1x con il dispositivo esistente (cancellato) o con un nuovo dispositivo iOS.
5. Connetti a **Dot1x**, immetti un nome utente e una password e fai clic su **Partecipa**.



6. Ripetere i passaggi da 90 a 90 dalla sezione [Configurazione ISE](#) fino al completamento

dell'installazione dei profili appropriati.

7. Per controllare il processo, selezionare **ISE > Operations > Authentications**. Nell'esempio viene mostrato il client connesso direttamente alla WLAN 802.1X quando viene attivato, disconnesso e riconnesso alla stessa WLAN con l'uso di TLS.

Time	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25,12 12:40:03.593 AM	✓		paul	EB:06:98:97:09:41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25,12 12:39:53.353 AM	✓		EB:06:98:97:09:41	EB:06:98:97:09:41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25,12 12:39:08.967 AM	✓		paul	EB:06:98:97:09:41	WLC	Provision	RegisteredDevices	Pending	Authentication succeeded

8. Passare a **WLC > Monitor > [MAC client]**. Nel dettaglio del client, notare che il client si trova nello stato RUN, il relativo Data Switching è impostato su local e l'autenticazione è Central. Ciò vale per i client che si connettono a FlexConnect AP.

Time	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25,12 12:40:03.593 AM	✓		paul	EB:06:98:97:09:41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25,12 12:39:53.353 AM	✓		EB:06:98:97:09:41	EB:06:98:97:09:41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25,12 12:39:08.967 AM	✓		paul	EB:06:98:97:09:41	WLC	Provision	RegisteredDevices	Pending	Authentication succeeded

Esperienza utente - Provisioning di Android

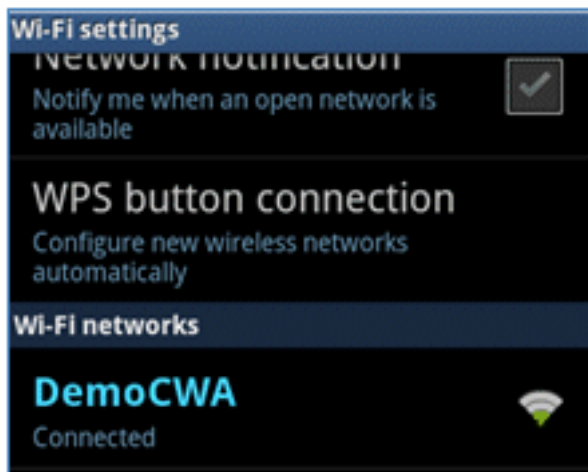
SSID doppio

In questa sezione vengono illustrati due SSID e viene descritto come connettersi al guest di cui eseguire il provisioning e come connettersi a una WLAN 802.1x.

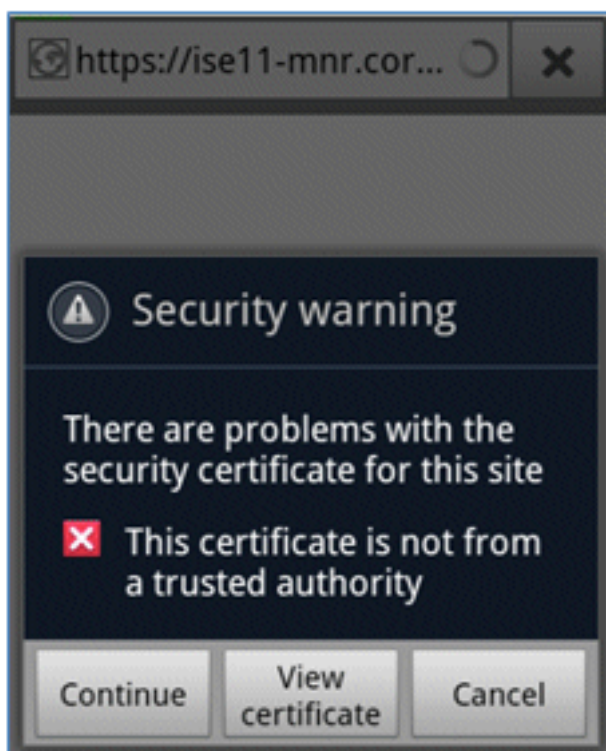
Il processo di connessione per il dispositivo Android è molto simile a quello per un dispositivo iOS (singolo o doppio SSID). Tuttavia, una differenza importante è che il dispositivo Android richiede l'accesso a Internet per accedere a Google Marketplace (ora Google Play) e scaricare l'agente supplicant.

Completare questi passaggi per effettuare il provisioning di un dispositivo Android (come il Samsung Galaxy in questo esempio) nello scenario con doppio SSID:

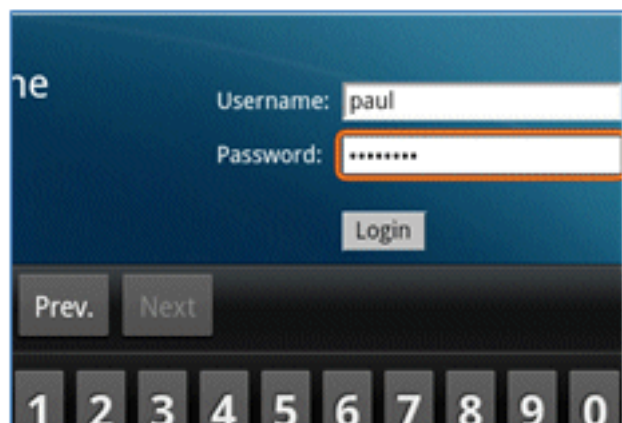
1. Nel dispositivo Android, usare Wi-Fi per collegarsi a **DemoCWA** e aprire la WLAN guest.



2. Accettare tutti i certificati per collegarsi all'ISE.

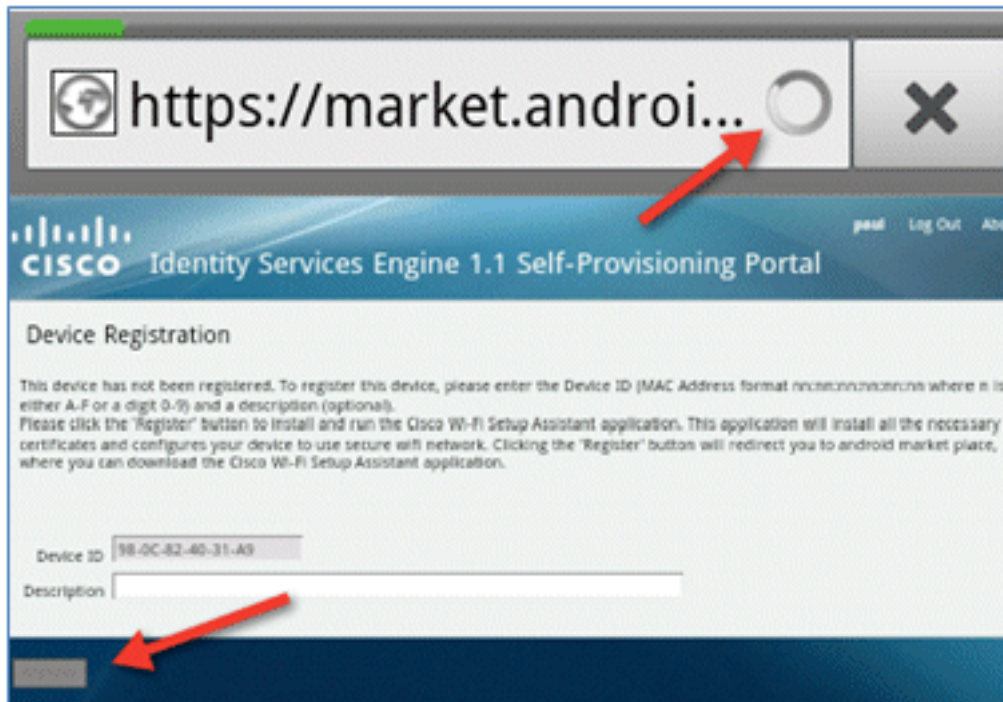


3. Immettere un nome utente e una password nel portale guest per eseguire il login.

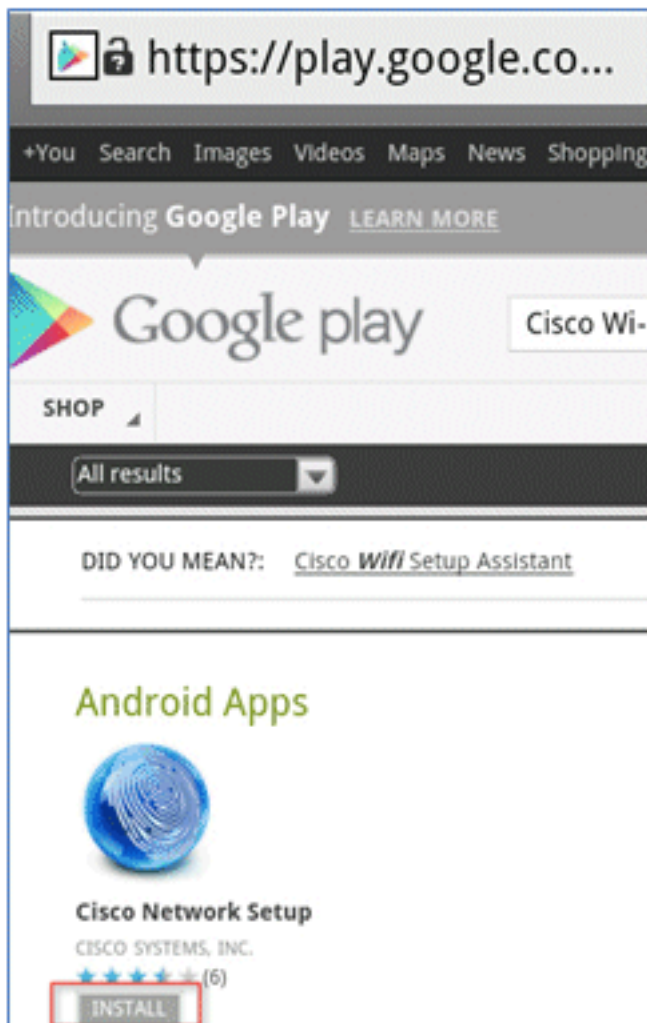


4. Fare clic su **Registra**. Il dispositivo tenta di raggiungere Internet per accedere a Google

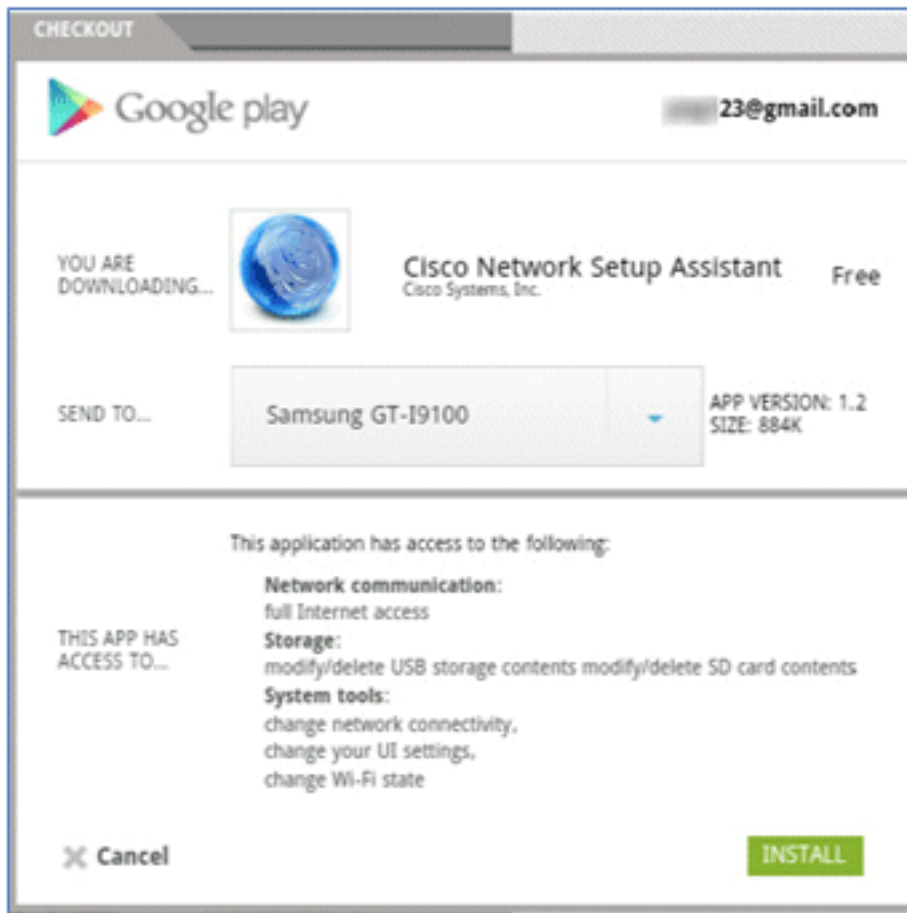
Marketplace. Aggiungere eventuali regole aggiuntive all'ACL di pre-autenticazione (ad esempio, ACL-REDIRECT) nel controller per consentire l'accesso a Internet.



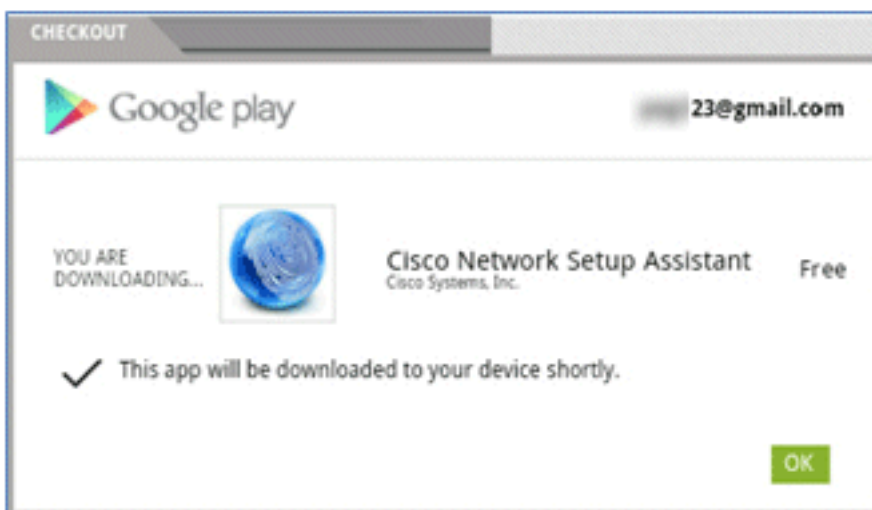
5. Google elenca Cisco Network Setup come app per Android. Fare clic su **INSTALLA**.



6. Accedere a Google e fare clic su **INSTALL** (INSTALLA).



7. Fare clic su **OK**.



8. Sul dispositivo Android, trovare l'app **Cisco SPW** installata e aprirla.



9. Verificare di aver ancora eseguito l'accesso al portale guest dal dispositivo Android.

10. Per avviare l'Assistente installazione Wi-Fi, fare clic su **Start**.



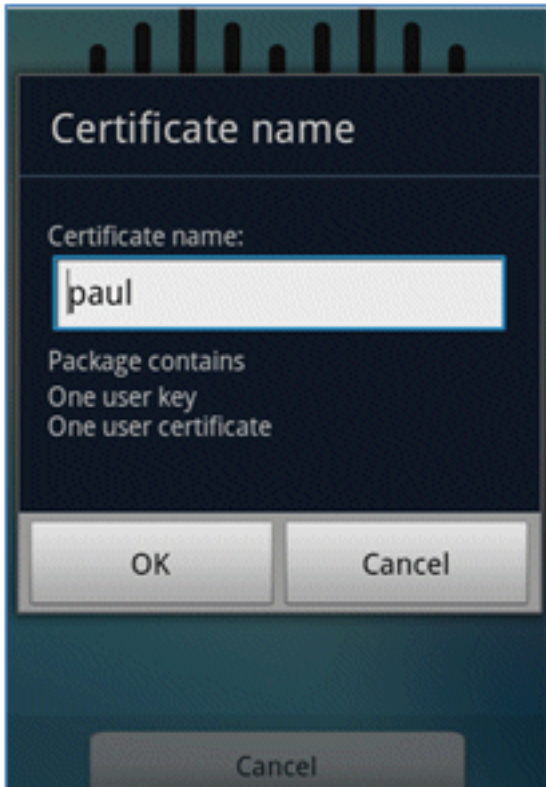
11. L'SPW Cisco inizia a installare i certificati.



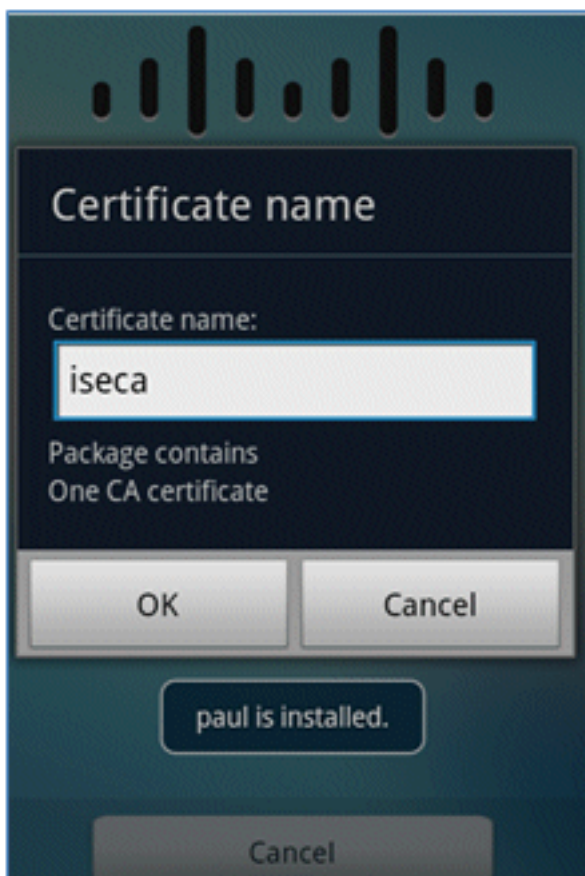
12. Quando richiesto, impostare una password per l'archiviazione delle credenziali.



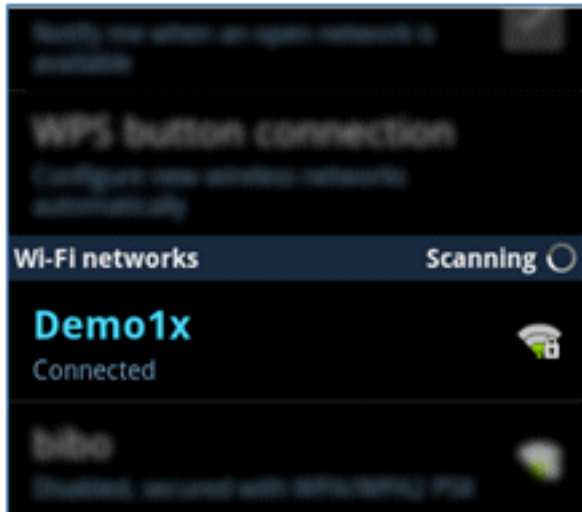
13. L'SPW Cisco restituisce un nome di certificato, che contiene la chiave utente e il certificato utente. Per confermare, fare clic su **OK**.



14. Cisco SPW continua e richiede un altro nome di certificato, che contiene il certificato CA. Immettere il nome **iseca** (in questo esempio), quindi fare clic su **OK** per continuare.



15. Il dispositivo Android è ora connesso.

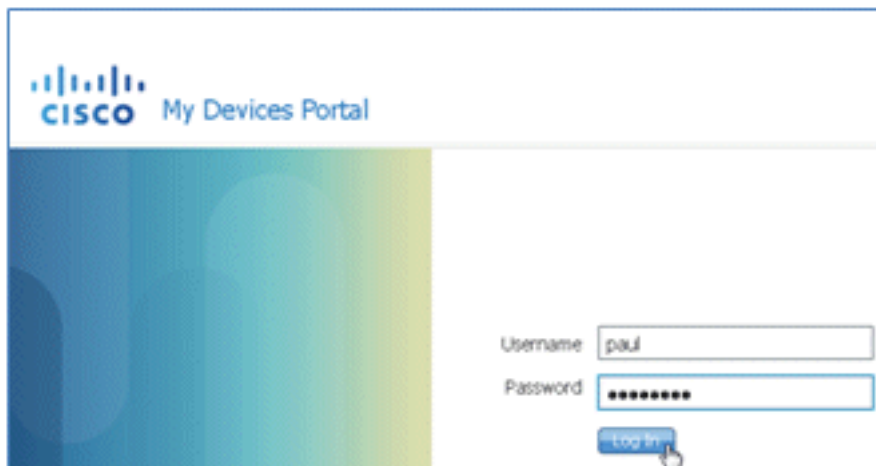


Portale I miei dispositivi

My Devices Portal consente agli utenti di inserire nella blacklist i dispositivi registrati in precedenza in caso di smarrimento o furto di un dispositivo. Consente inoltre agli utenti di reinserirsi, se necessario.

Per mettere in blacklist un dispositivo, completare i seguenti passaggi:

1. Per accedere al portale I miei dispositivi, apri un browser, connettiti a <https://ise-server:8443/mydevices> (nota il numero di porta 8443) e accedi con un account AD.



2. Individuare il dispositivo in ID dispositivo e fare clic su **Lost?** per avviare la creazione della blacklist di un dispositivo.

Add a New Device

To add a device, please enter the Device ID (MAC Address) and a description (optional); then click submit to add the device.

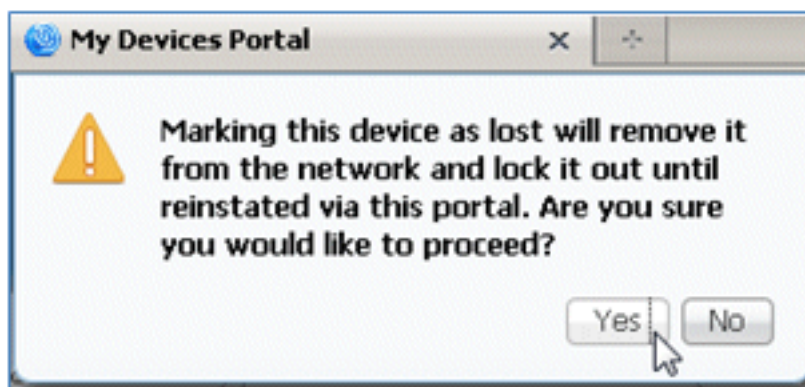
* Device ID

Description

Your Devices

State	Device ID	Description	Action
	EB:06:88:97:09:41		Edit Log2

3. Quando l'ISE chiede un avviso, fare clic su **Yes** (Sì) per procedere.



4. ISE conferma che il dispositivo è contrassegnato come **perso**.



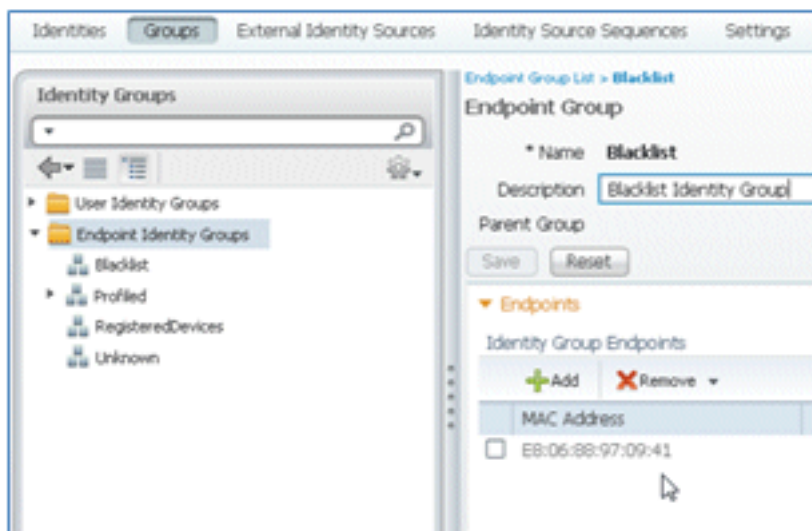
5. Qualsiasi tentativo di connessione alla rete con il dispositivo registrato in precedenza è ora bloccato, anche se è installato un certificato valido. Questo è un esempio di un dispositivo in blacklist che non riesce ad autenticarsi:

Live Authentications

Refresh: Every 3 seconds | Show: Latest 20 records

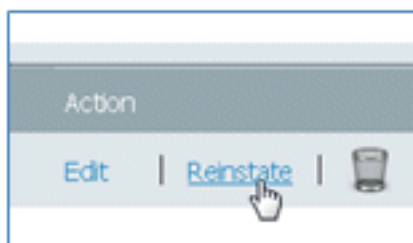
Time	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25, 12:49:07.851 AM			pa.j	EB:06:88:97:09:41	WLC	Blacklist_Access	Blacklist		Authentication failed
Mar 25, 12:48:59.057 AM			EB:06:88:97:09:41	EB:06:88:97:09:41	WLC	Blacklist_Access	Blacklist		Authentication failed
Mar 25, 12:48:54.137 AM			pa.j	EB:06:88:97:09:41	WLC	Blacklist_Access	Blacklist		Authentication failed

6. Un amministratore può passare a ISE > Amministrazione > Gestione identità > **Gruppi**, fare clic su **Gruppi di identità degli endpoint > Lista nera**, e vedere il dispositivo è in blacklist.

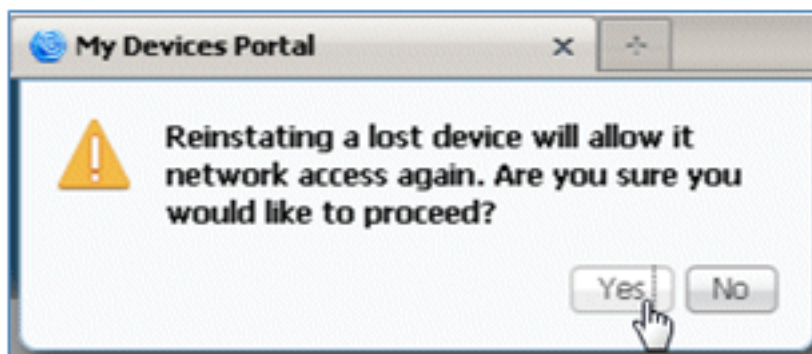


Per ripristinare un dispositivo in lista nera, completare i seguenti passaggi:

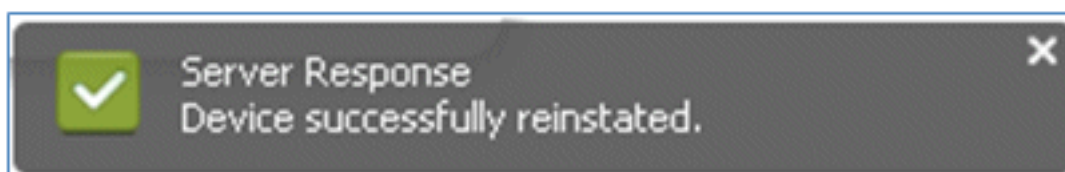
1. Dal portale I miei dispositivi, fare clic su **Reintegra** per il dispositivo.



2. Quando ISE chiede un avviso, fare clic su **Sì** per procedere.



3. ISE conferma che il dispositivo è stato ripristinato. Collegare il dispositivo reinstallato alla rete per verificare che sia autorizzato.

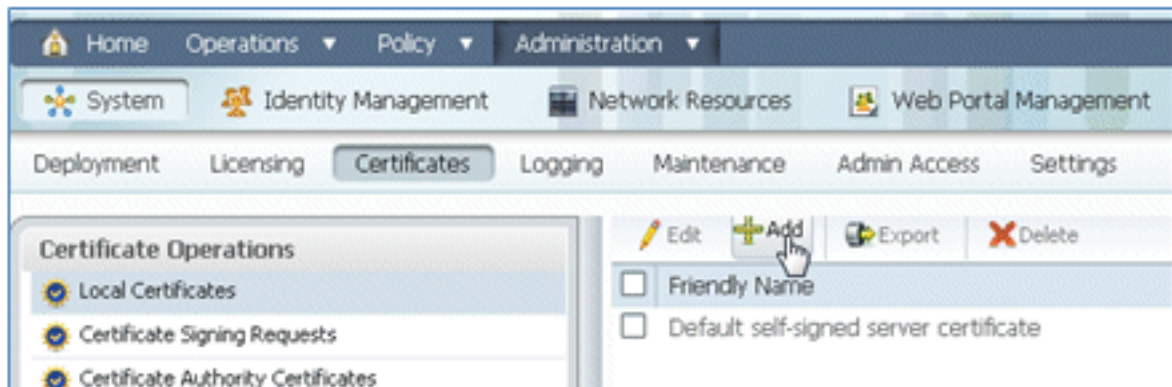


Riferimento - Certificati

ISE richiede non solo un certificato radice CA valido, ma anche un certificato valido firmato da CA.

Completare questa procedura per aggiungere, associare e importare un nuovo certificato CA attendibile:

1. Selezionare ISE > Administration > System > **Certificates**, fare clic su **Local Certificates**, quindi fare clic su **Add**.



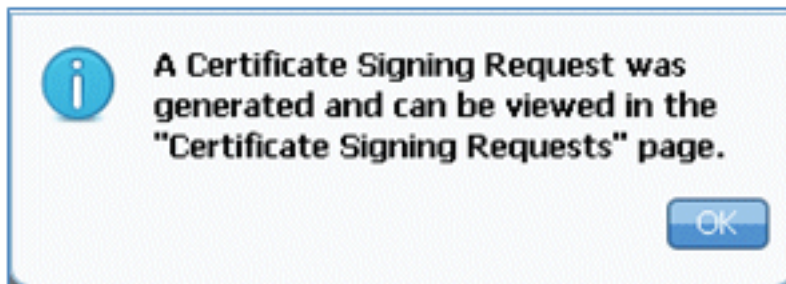
2. Selezionare **Genera richiesta di firma del certificato (CSR)**.



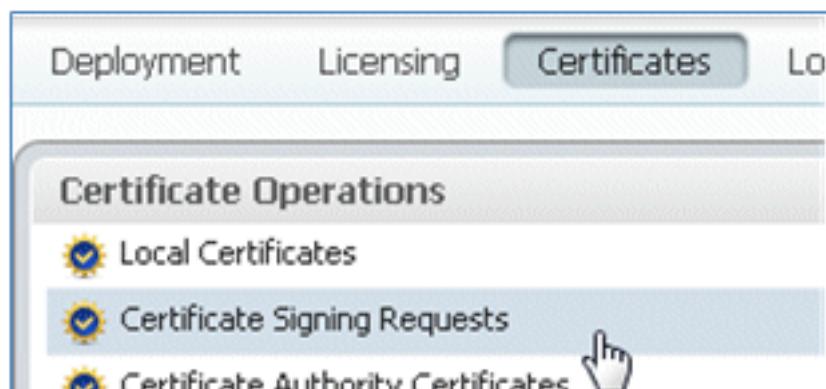
3. Immettere il **CN** del soggetto del certificato=**<ISE-SERVER nomehost.FQDN>**. Per gli altri campi, è possibile utilizzare il valore predefinito o i valori richiesti dall'impostazione della CA. Fare clic su **Invia**.

The screenshot shows the 'Generate Certificate Signing Request' form. The title is 'Local Certificates > Generate Certificate Signing Request'. Under the 'Certificate' section, there are three fields: '* Certificate Subject' with the value 'CN=ise11-mnr.corp.rf-demo.com', '* Key Length' with a dropdown menu set to '2048', and '* Digest to Sign With' with a dropdown menu set to 'SHA-256'. At the bottom, there are 'Submit' and 'Cancel' buttons.

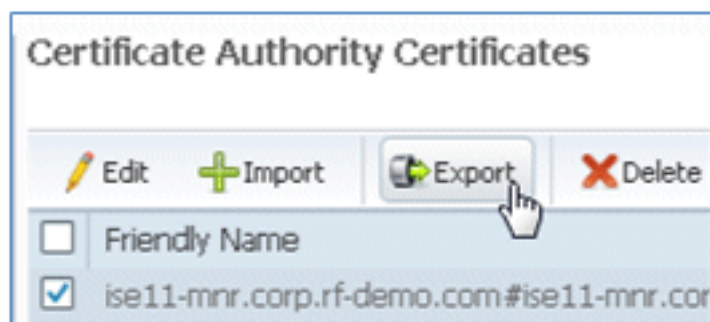
4. ISE verifica che il CSR sia stato generato.



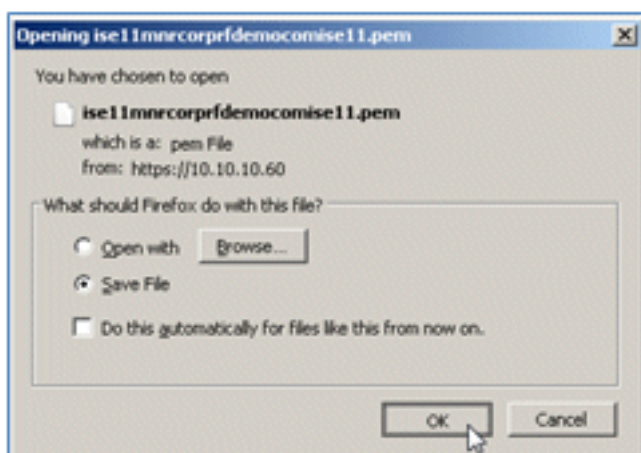
5. Per accedere al CSR, fare clic sulle operazioni **Richieste di firma certificato**.



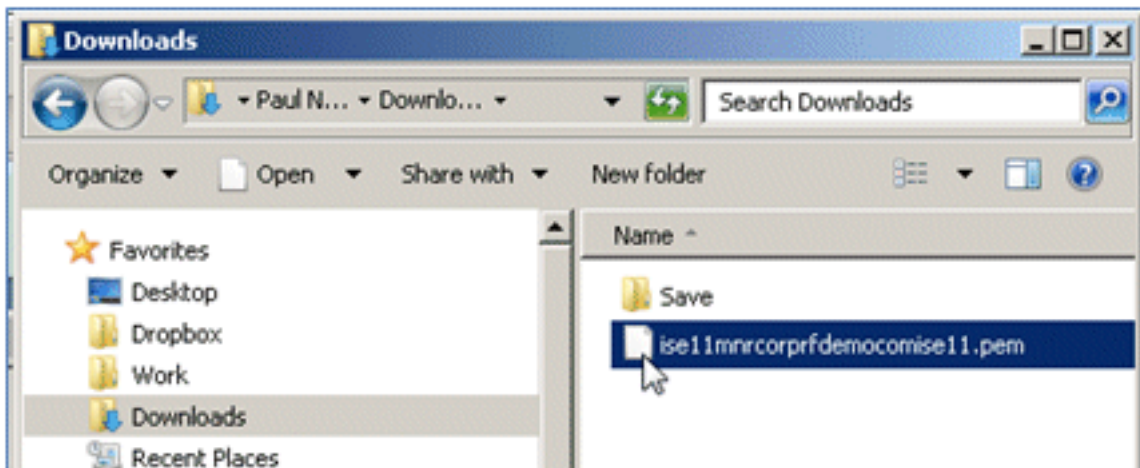
6. Selezionare il CSR creato di recente, quindi fare clic su **Esporta**.



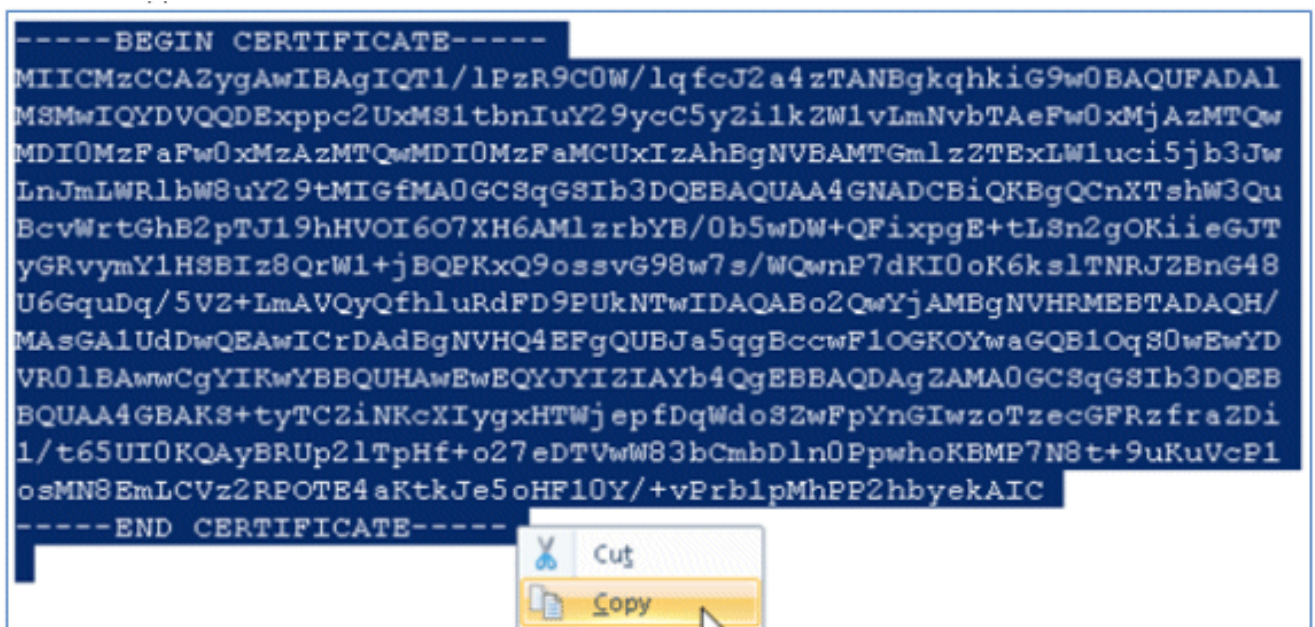
7. ISE esporta il CSR in un file .pem. Per salvare il file sul computer locale, fare clic su **Salva file**, quindi su **OK**.



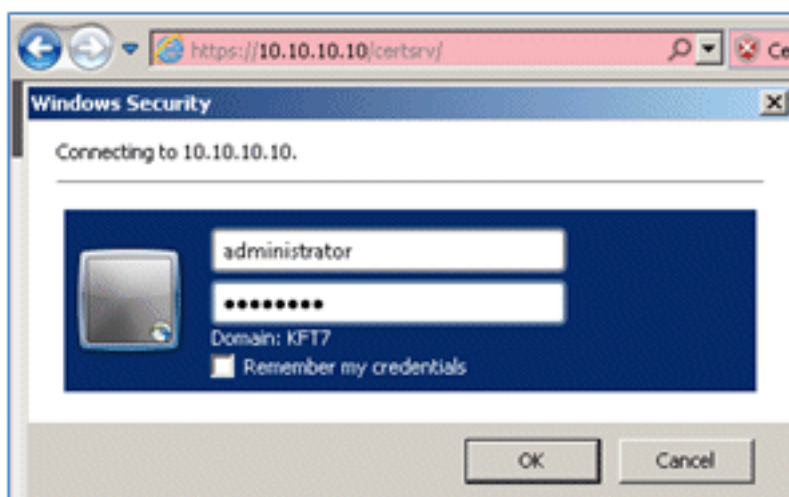
8. Individuare e aprire il file del certificato ISE con un editor di testo.



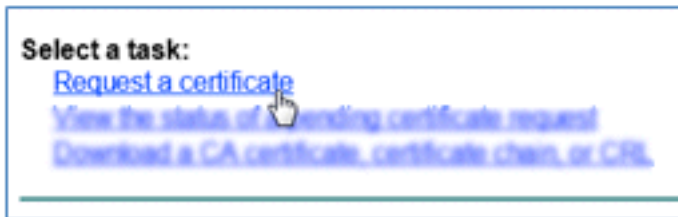
9. Copiare l'intero contenuto del certificato.



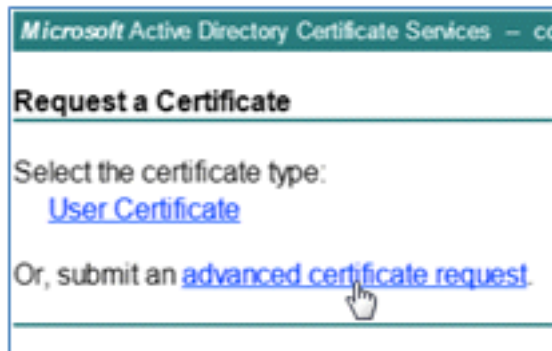
10. Connettersi al server CA e accedere con un account amministratore. Il server è una CA di Microsoft 2008 all'indirizzo <https://10.10.10.10/certsrv> (in questo esempio).



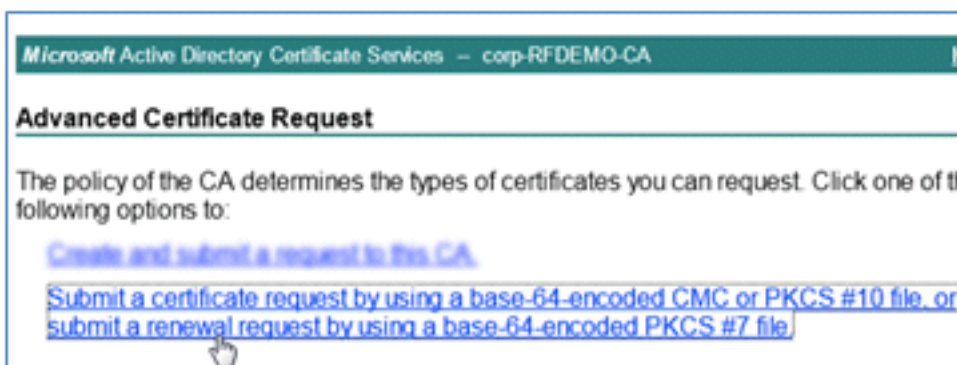
11. Fare clic su **Richiedi certificato**.



12. Fare clic su **Richiesta avanzata di certificati**.



13. Fare clic sulla seconda opzione per **inviare una richiesta di certificato utilizzando un CMC con codifica Base 64 o ...**



14. Incollare il contenuto del file del certificato ISE (.pem) nel campo Richiesta salvata, verificare che il modello di certificato sia **Server Web**, quindi fare clic su **Invia**.

Microsoft Certificate Services -- labsrv.corp.rf-demo.com

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CM Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
MAAGAlUdDwQEAvICrDAdBgNVHQ4EFgQUBJa5qgBc
VRO1BAwvCgYIKwYBBQUHAvEwEQYJYIZIAAYb4QgEB
BQUAA4GBAKS+tyTCZ1NKcXIyqxHTWjepfDqVdoS2
1/t6SUIORQayBRUp21TpHf+o27eDTVwW83bCmbD1
oaMNBEmLCVz2RPOTE4aKtkJe5oHF10Y/+vPrb1pM
-----END CERTIFICATE-----
```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >


15. Fare clic su **Scarica certificato**.

Microsoft Active Directory Certificate Services -- corp-RFDEMO-CA

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded

 [Download certificate](#)

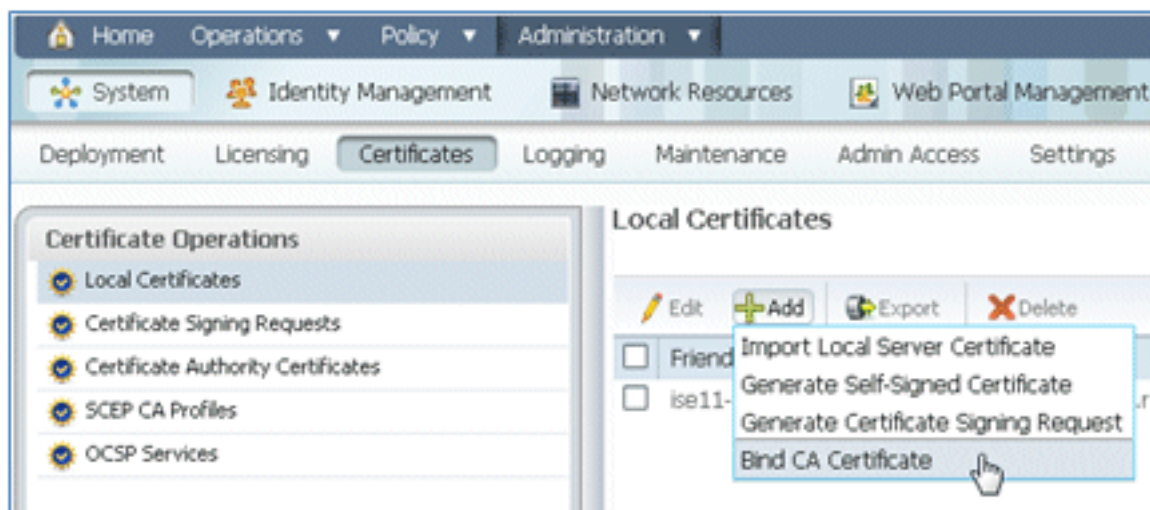
[Download certificate chain](#)

16. Salvare il file certnew.cer che verrà utilizzato in seguito per il binding all'ISE.

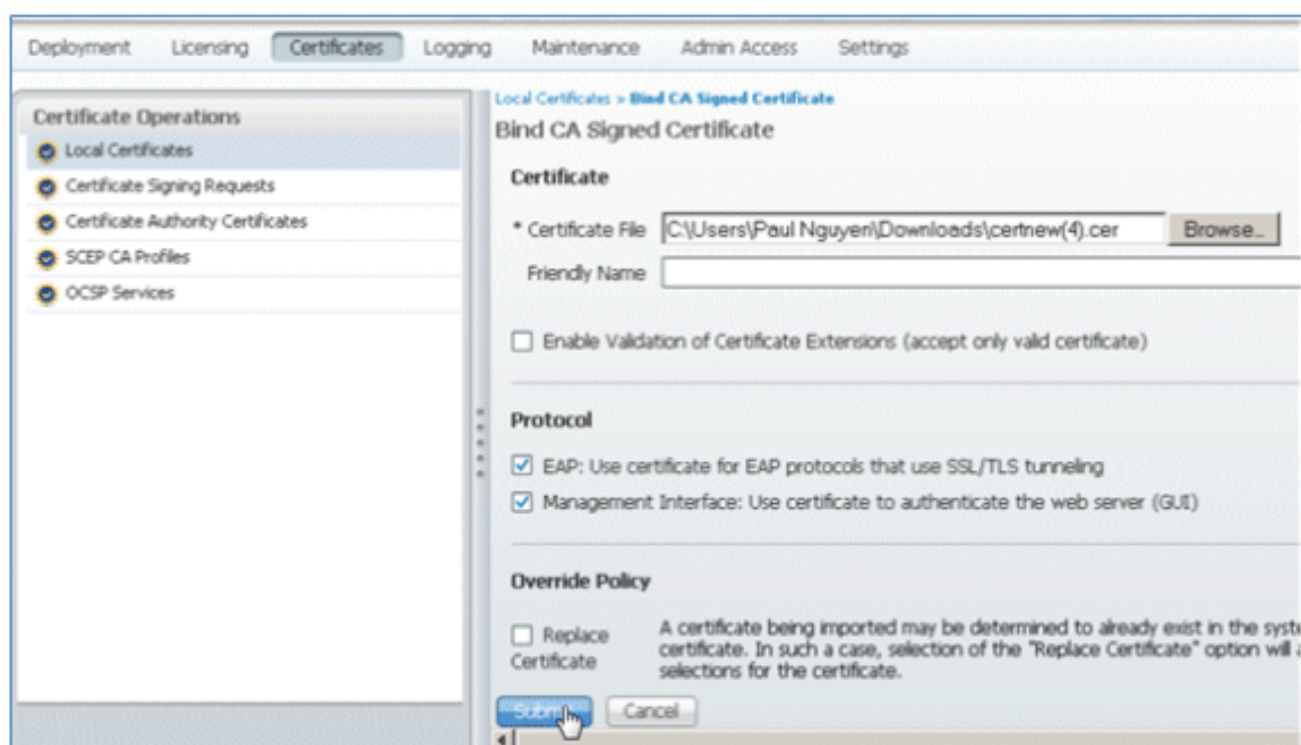
Do you want to open or save certnew.cer (921 bytes) from 10.10.10.10?

Open Save

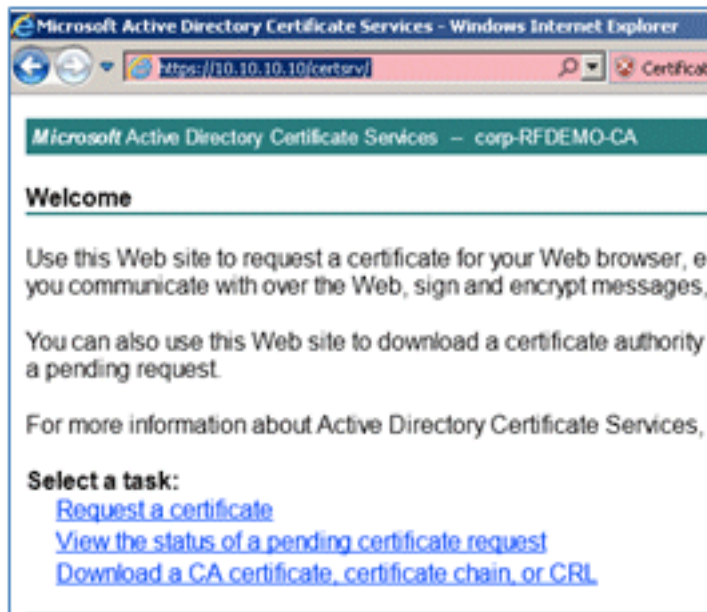
17. Da **Certificati ISE**, passare a **Certificati locali** e fare clic su **Add > Bind CA Certificate** (Aggiungi > **Certificato CA binding**).



18. Individuare il certificato salvato nel computer locale nel passaggio precedente, abilitare entrambi i protocolli **EAP** e **Management Interface** (le caselle sono selezionate) e fare clic su **Invia**. ISE potrebbe richiedere alcuni minuti o più per riavviare i servizi.



19. Tornare alla pagina iniziale della CA (<https://CA/certsrv/>) e fare clic su **Scarica certificato CA, catena di certificati o CRL**.



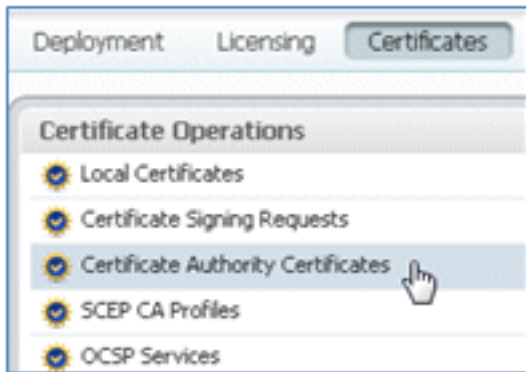
20. Fare clic su **Scarica certificato CA**.



21. **Salvare** il file nel computer locale.



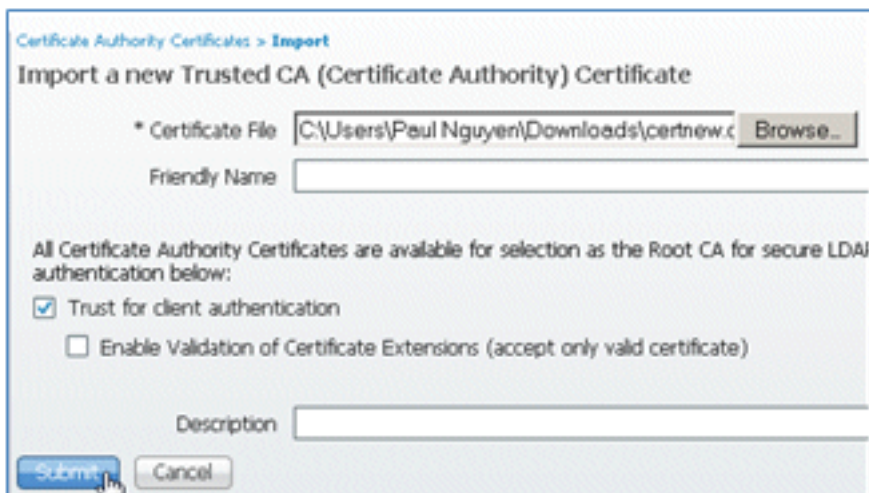
22. Con il server ISE in linea, andare su **Certificati**, quindi fare clic su **Certificati Autorità di certificazione**.



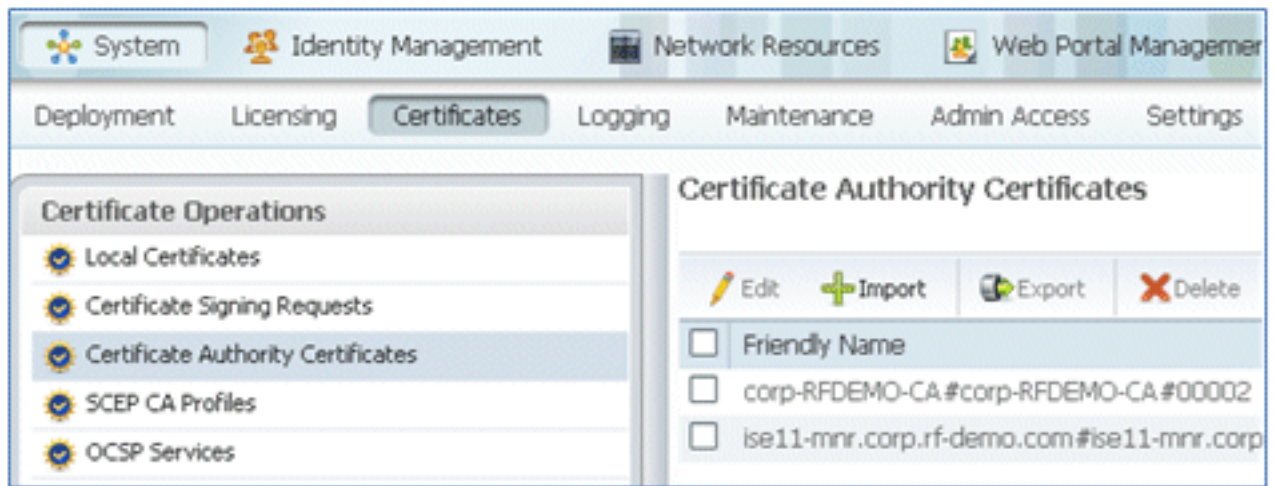
23. Fare clic su **Import** (Importa).



24. Cercare il certificato CA, abilitare l'opzione **Attendibilità per l'autenticazione client** (casella selezionata) e fare clic su **Invia**.



25. Confermare l'aggiunta del nuovo certificato CA attendibile.



Informazioni correlate

- [Guida all'installazione dell'hardware di Cisco Identity Services Engine, versione 1.0.4](#)
- [Cisco serie 2000 Wireless LAN Controller](#)
- [Cisco serie 4400 Wireless LAN Controller](#)
- [Cisco Aironet serie 3500](#)
- [Guida all'installazione di Flex 7500 Wireless Branch Controller](#)
- [Personalizzazione del dispositivo - Autenticazione unificata del dispositivo ed esperienza di accesso coerente](#)
- [BYOD wireless con Identity Services Engine](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).