Configurazione dell'autenticazione 802.1X con PEAP, ISE 2.1 e WLC 8.3

Sommario

Introduzione

In questo documento viene descritto come configurare una rete WLAN (Wireless Local Area Network) con sicurezza 802.1x e override della VLAN (Virtual Local Area Network).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- 802.1x
- PEAP (Protected Extensible Authentication Protocol)
- CA (Certification Authority)
- Certificati

Componenti usati

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

- WLC v8.3.102.0

- Identity Service Engine (ISE) v2.1
- Notebook Windows 10

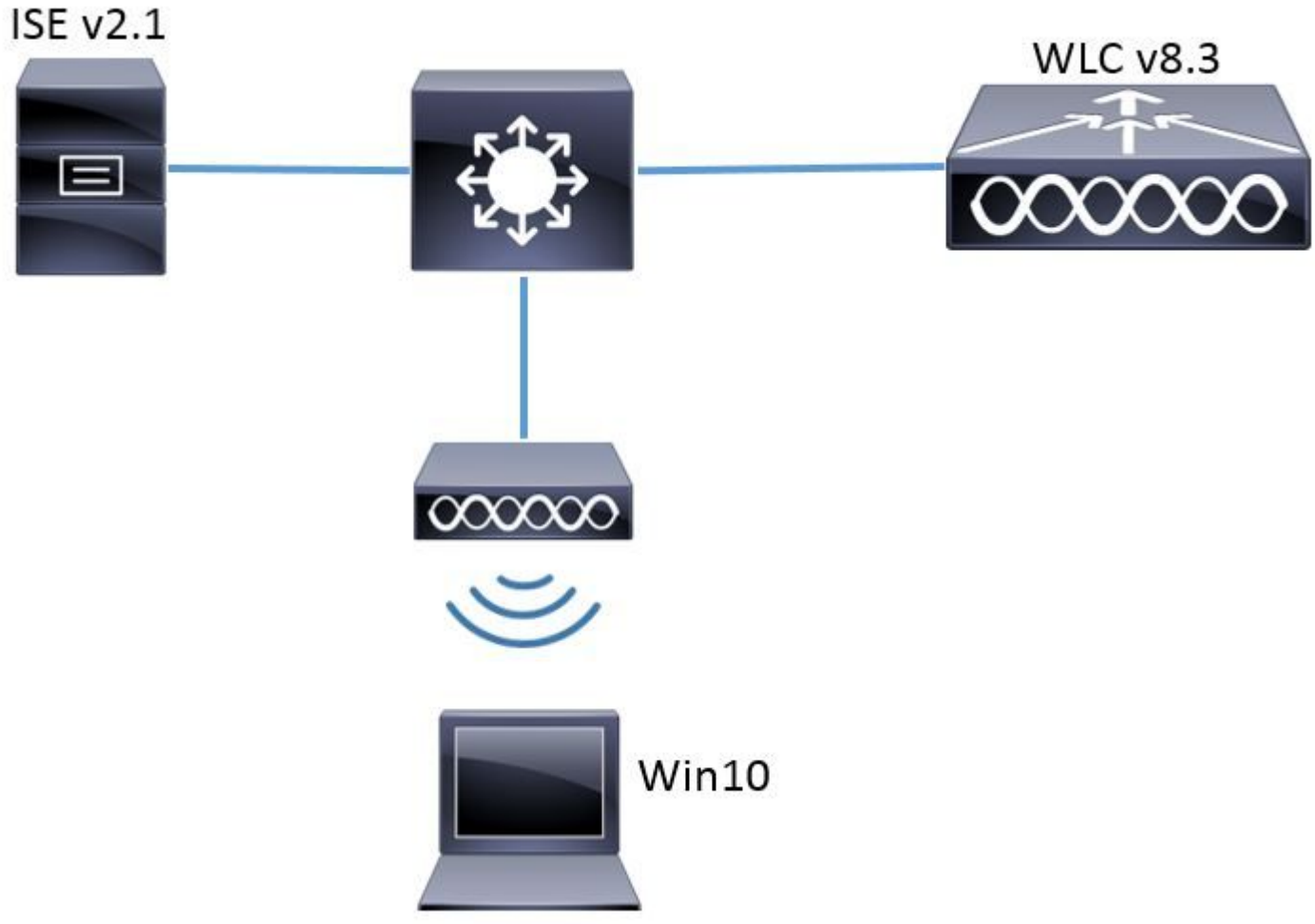
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Quando si configura una WLAN con sicurezza 802.1x e VLAN, è possibile ignorare il protocollo EAP (Protected Extensible Authentication Protocol).

Configurazione

Esempio di rete



Configurazione

Le fasi generali sono le seguenti:

1. Dichiarare il server RADIUS su WLC e viceversa per consentire la comunicazione reciproca.
2. Creare l'SSID (Service Set Identifier) nel WLC.
3. Creare la regola di autenticazione in ISE.

4. Creare il profilo di autorizzazione su ISE.
5. Creare la regola di autorizzazione in ISE.
6. Configurare l'endpoint.

Dichiara server RADIUS su WLC

Per consentire la comunicazione tra il server RADIUS e il WLC, è necessario registrare il server RADIUS sul WLC e viceversa.

GUI:

Passaggio 1. Aprire la GUI del WLC e selezionare **SECURITY > RADIUS > Authentication > New** (SICUREZZA > RADIUS > Autenticazione > Nuovo), come mostrato nell'immagine.

Passaggio 2. Immettere le informazioni sul server RADIUS come mostrato nell'immagine.

CLI:

```
> config radius auth add <index> <a.b.c.d> 1812 ascii <shared-key>
```

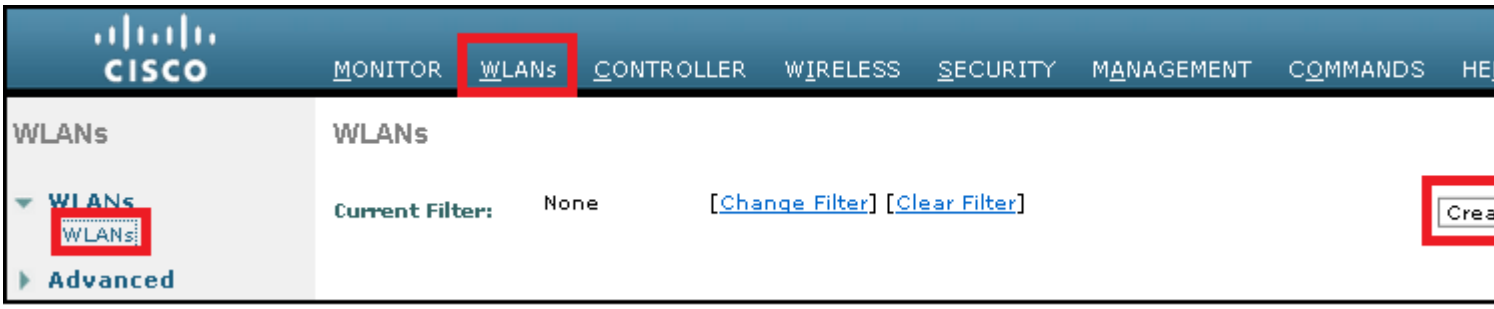
```
> config radius auth disable <index>
> config radius auth retransmit-timeout <index> <timeout-seconds>
> config radius auth enable <index>
```

<a.b.c.d> corrisponde al server RADIUS.

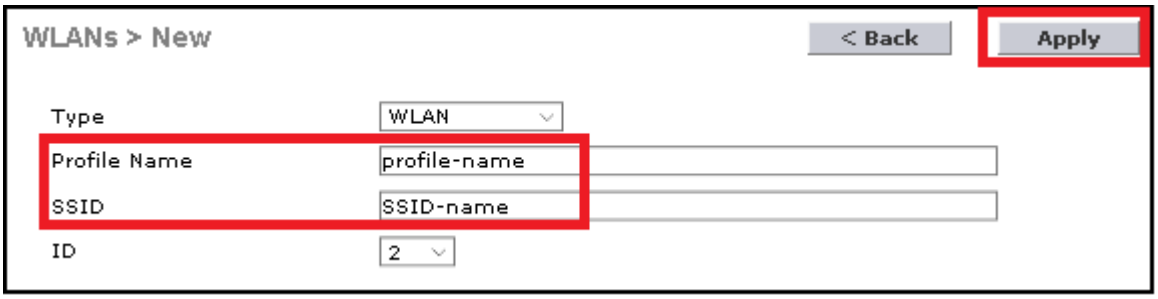
Crea SSID

GUI:

Passaggio 1. Aprire la GUI del WLC e selezionare **WLAN > Create New > Go** (WLAN > Crea nuovo > Vai), come mostrato nell'immagine.



Passaggio 2. Scegliere un nome per il SSID e il profilo, quindi fare clic su **Apply** (Applica) come mostrato nell'immagine.



CLI:

```
> config wlan create <id> <profile-name> <ssid-name>
```

Passaggio 3. Assegnare il server RADIUS alla WLAN.

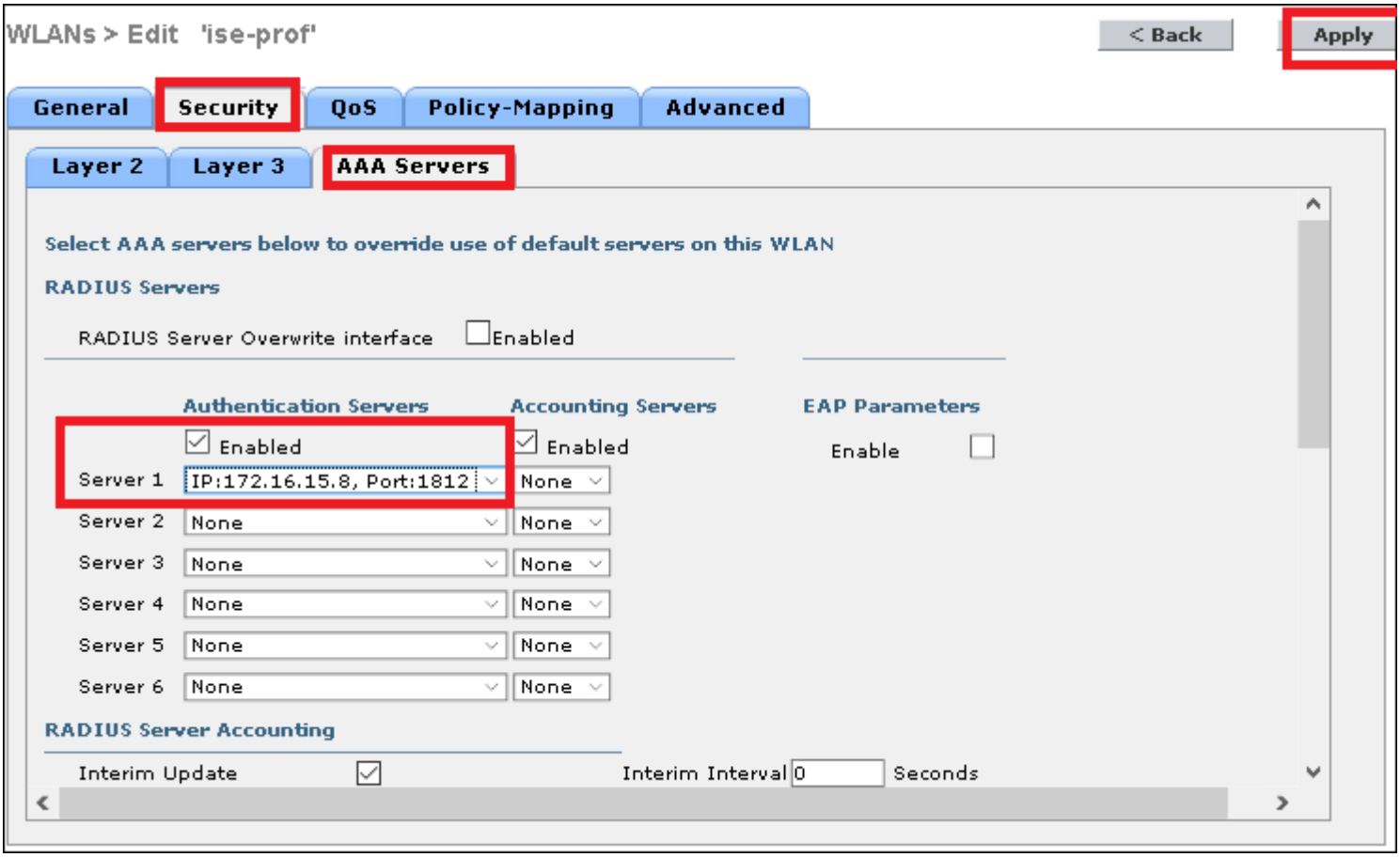
CLI:

```
> config wlan radius_server auth add <wlan-id> <radius-index>
```

GUI:

Passare a **Sicurezza > Server AAA** e scegliere il server RADIUS desiderato, quindi fare clic su **Applica**

come mostrato nell'immagine.



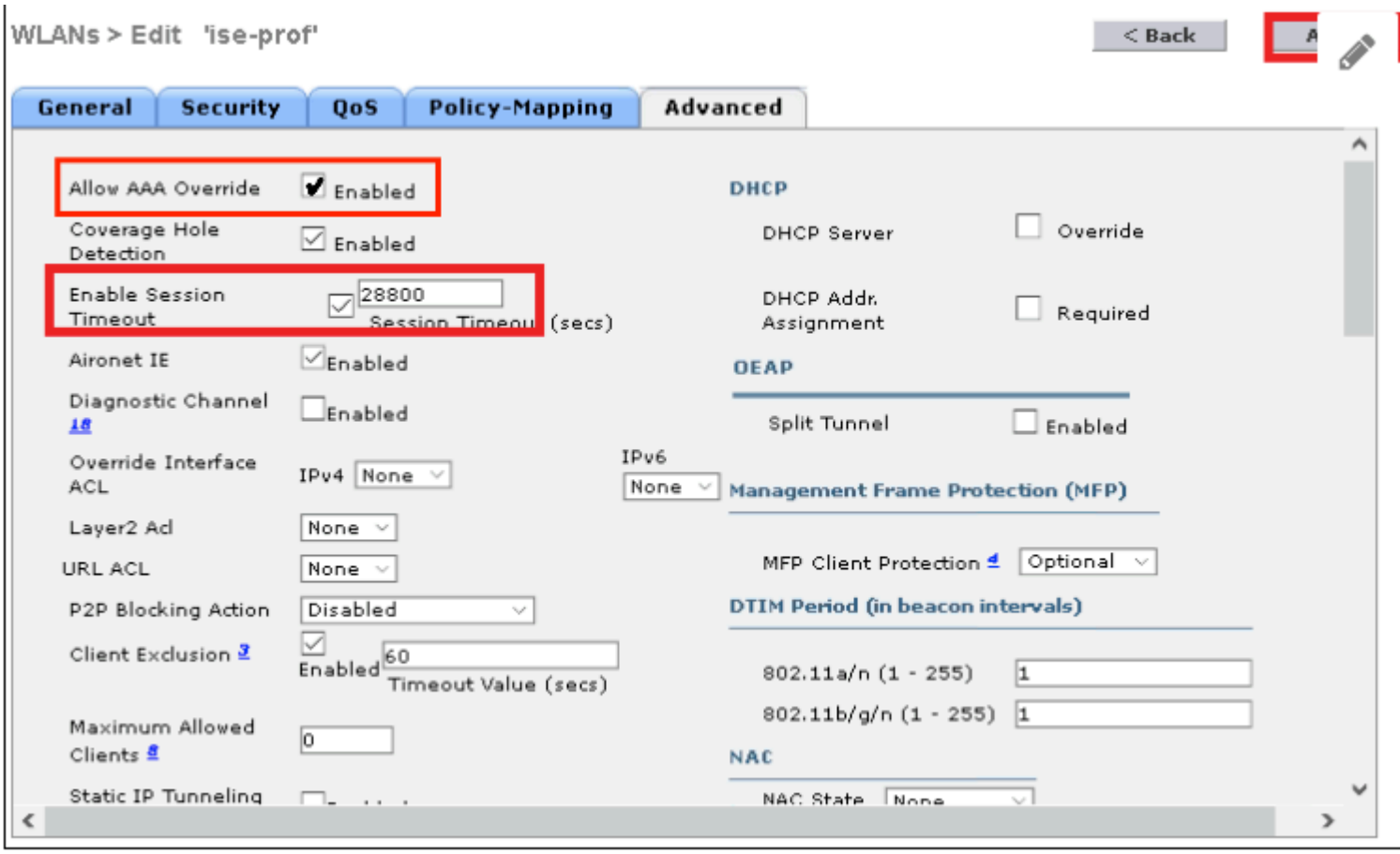
Passaggio 4. Abilitare **Consenti sostituzione AAA** e, facoltativamente, aumentare il timeout della sessione

CLI:

```
> config wlan aaa-override enable <wlan-id>
> config wlan session-timeout <wlan-id> <session-timeout-seconds>
```

GUI:

Selezionare **WLAN > ID WLAN > Avanzate** e abilitare **Consenti sostituzione AAA**. Facoltativamente, specificare il timeout della sessione come mostrato nell'immagine.



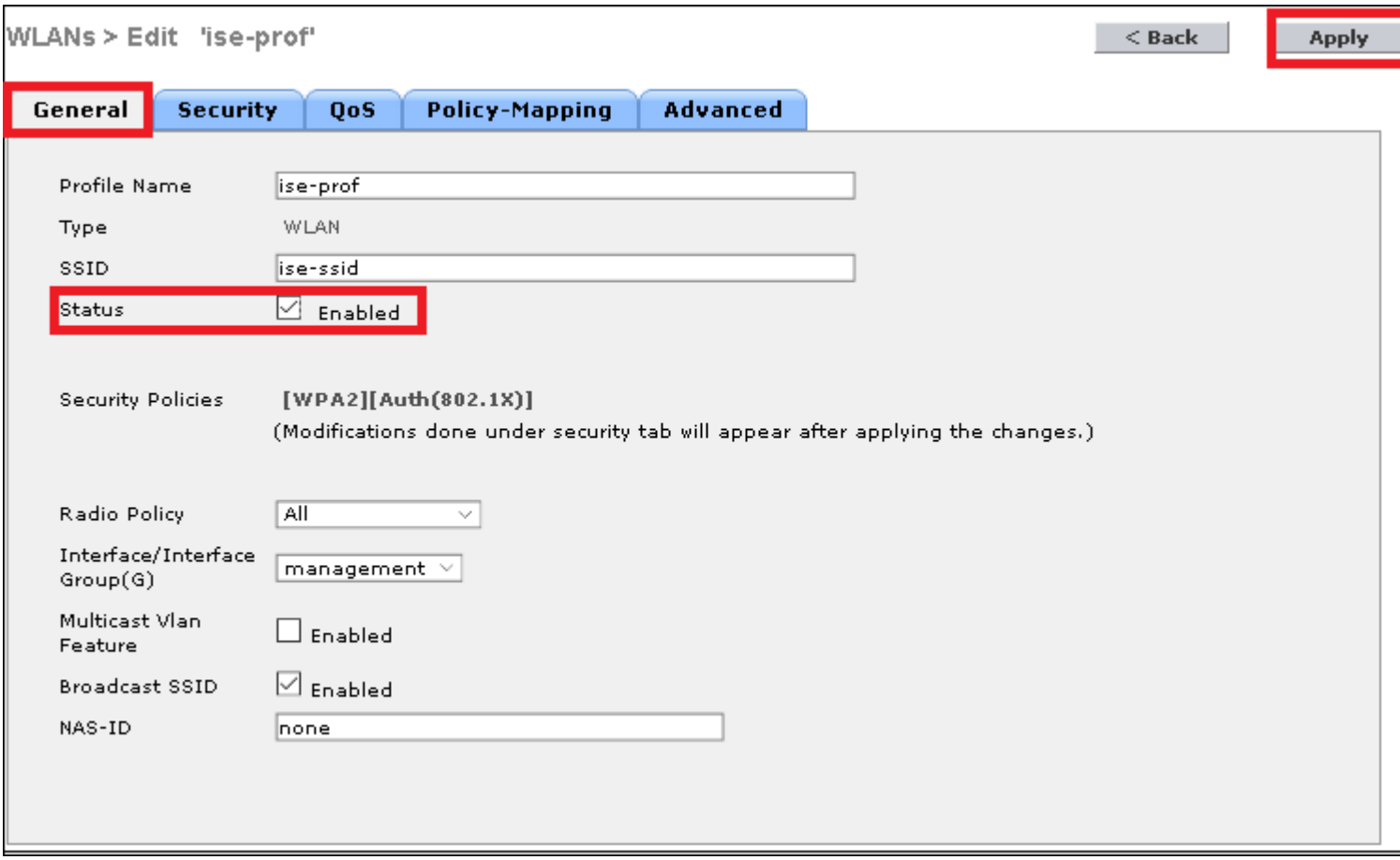
Passaggio 5. Abilitare la WLAN.

CLI:

```
> config wlan enable <wlan-id>
```

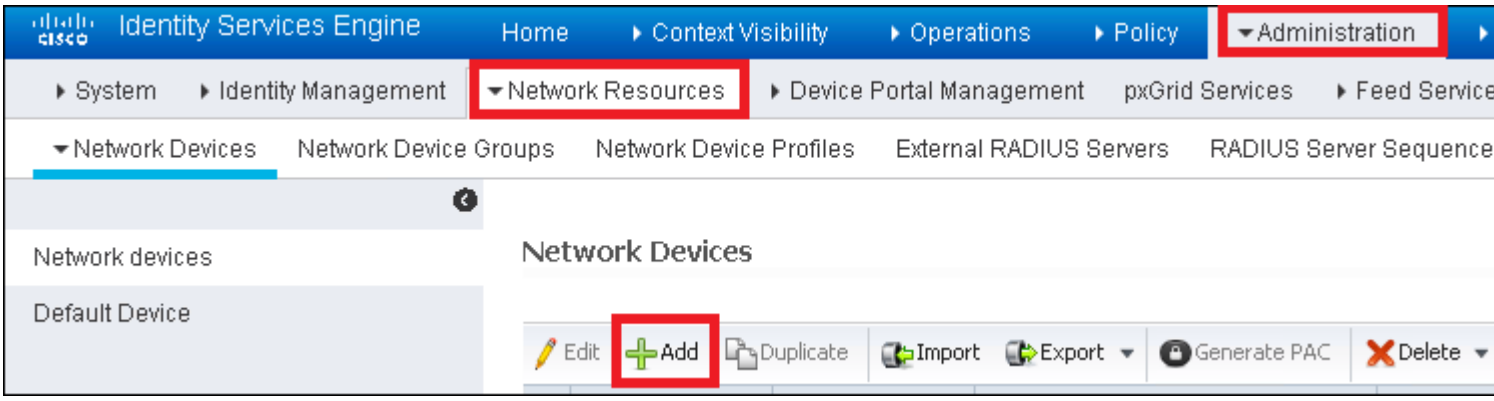
GUI:

Selezionare **WLAN > ID WLAN > Generale** e abilitare l'SSID come mostrato nell'immagine.



Dichiarare WLC su ISE

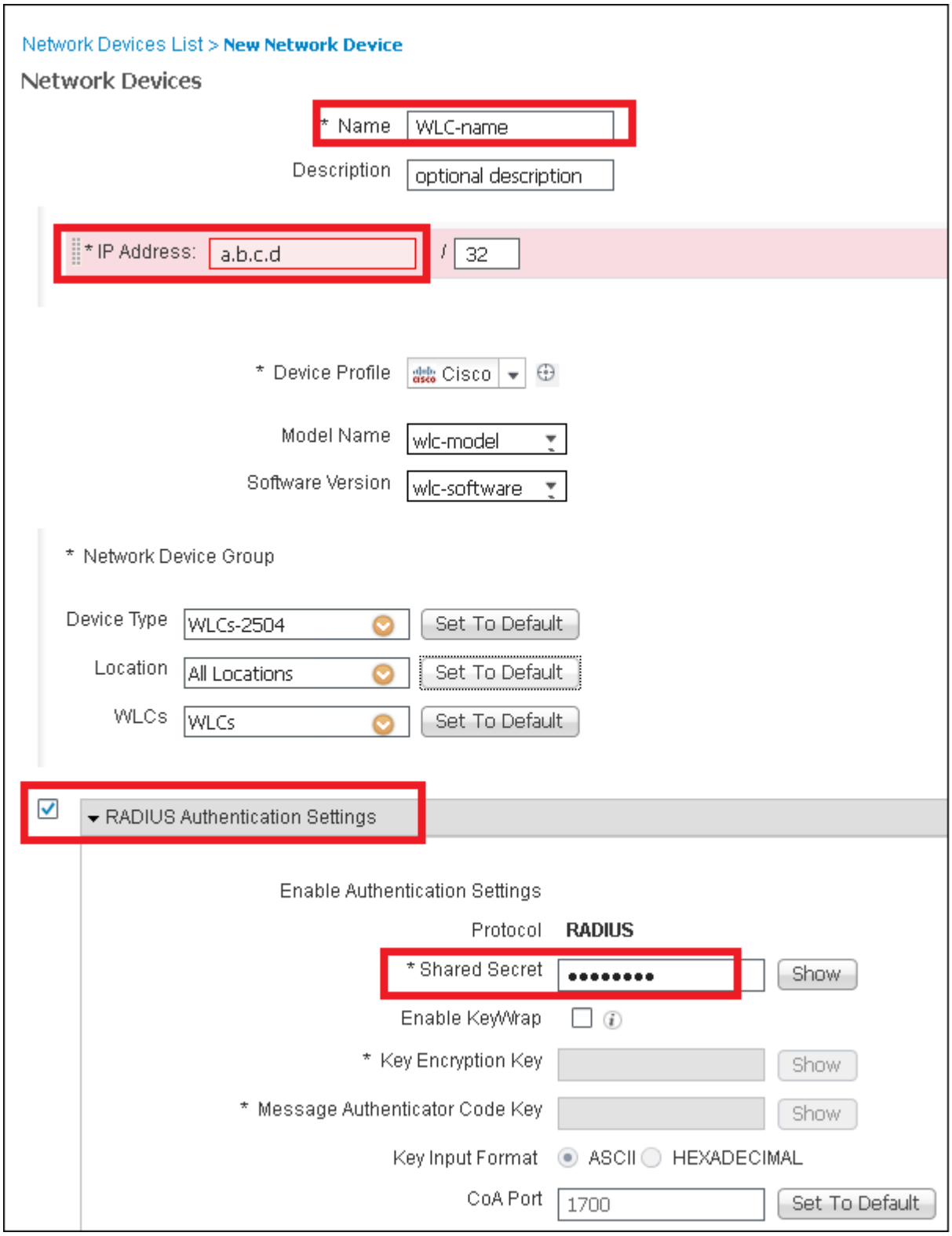
Passaggio 1. Aprire la console ISE e selezionare **Amministrazione > Risorse di rete > Dispositivi di rete > Aggiungi**, come mostrato nell'immagine.



Passaggio 2. Immettere i valori.

Facoltativamente, può corrispondere a un nome di modello, una versione del software, una descrizione e l'assegnazione di gruppi di dispositivi di rete in base al tipo di dispositivo, alla posizione o ai WLC.

a.b.c.d corrisponde all'interfaccia WLC che invia l'autenticazione richiesta. Per impostazione predefinita, si tratta dell'interfaccia di gestione, come illustrato nell'immagine.

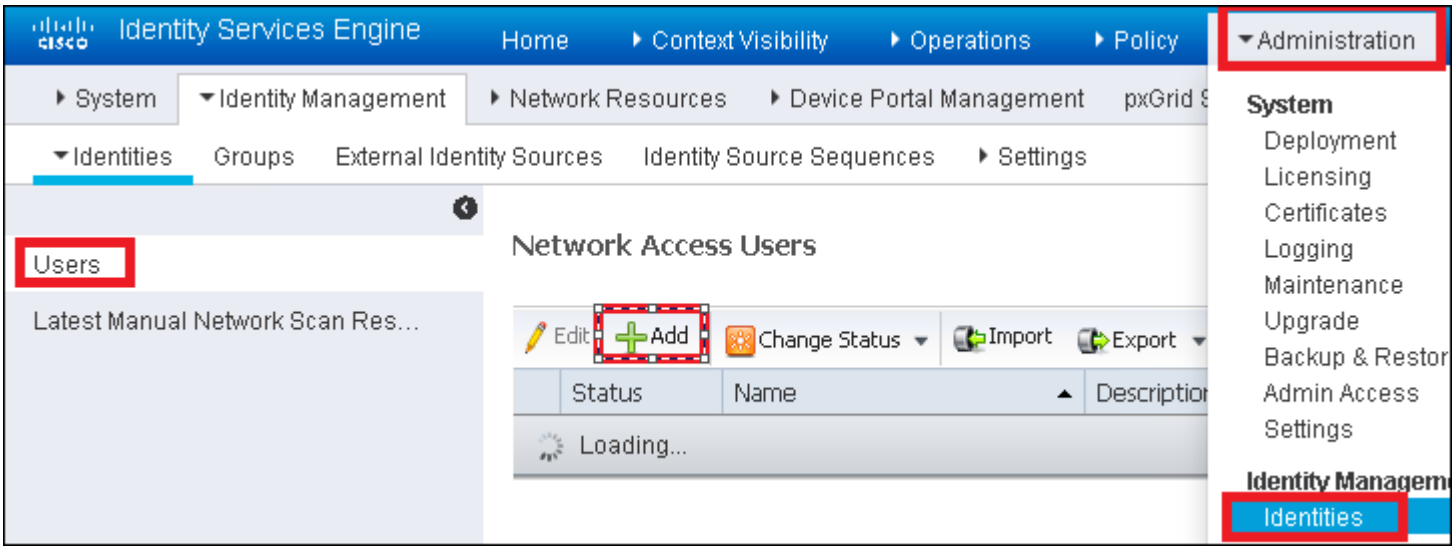


Per ulteriori informazioni sui gruppi di dispositivi di rete:

ISE - Gruppi di dispositivi di rete

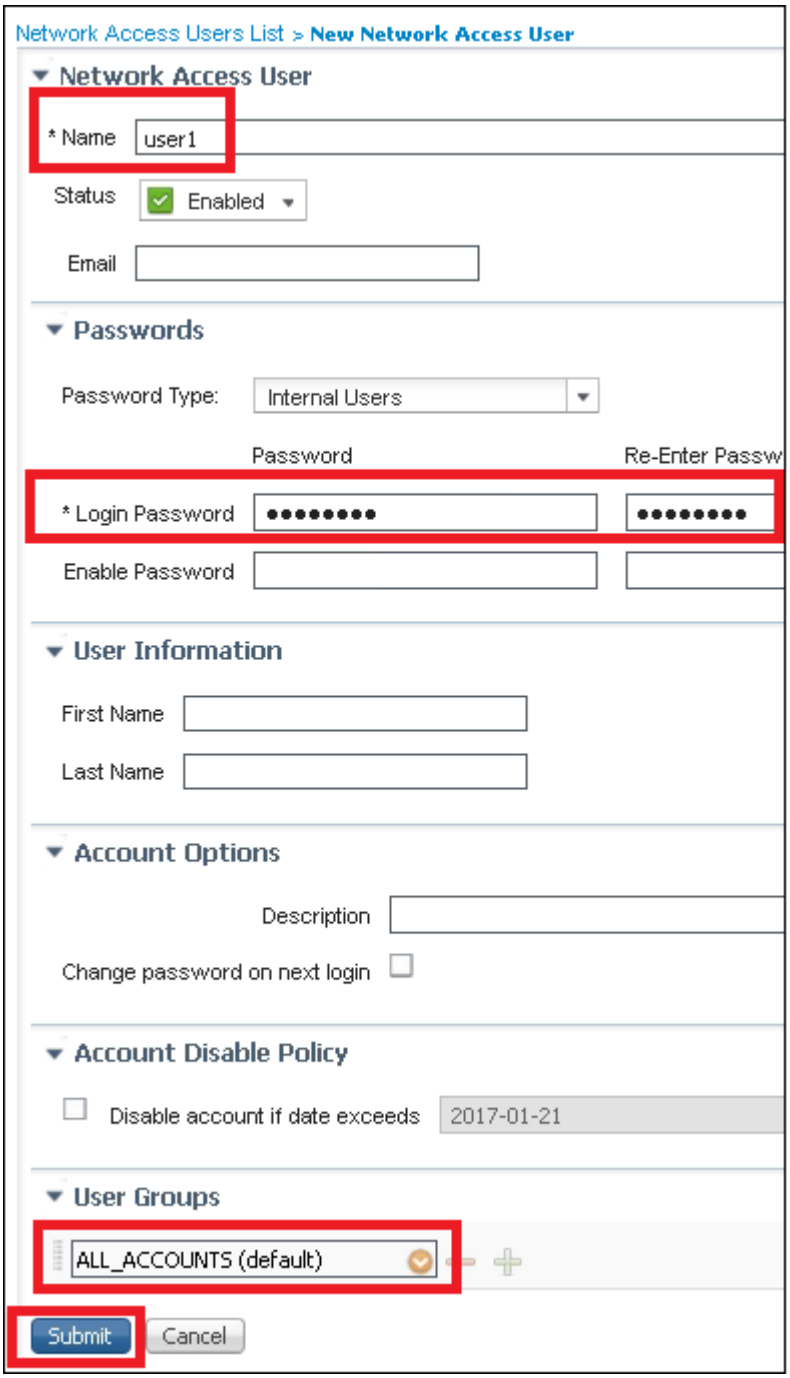
Creazione di un nuovo utente in ISE

Passaggio 1. Passare a **Amministrazione > Gestione delle identità > Identità > Utenti > Aggiungi** come mostrato nell'immagine.



Passaggio 2. Immettere le informazioni.

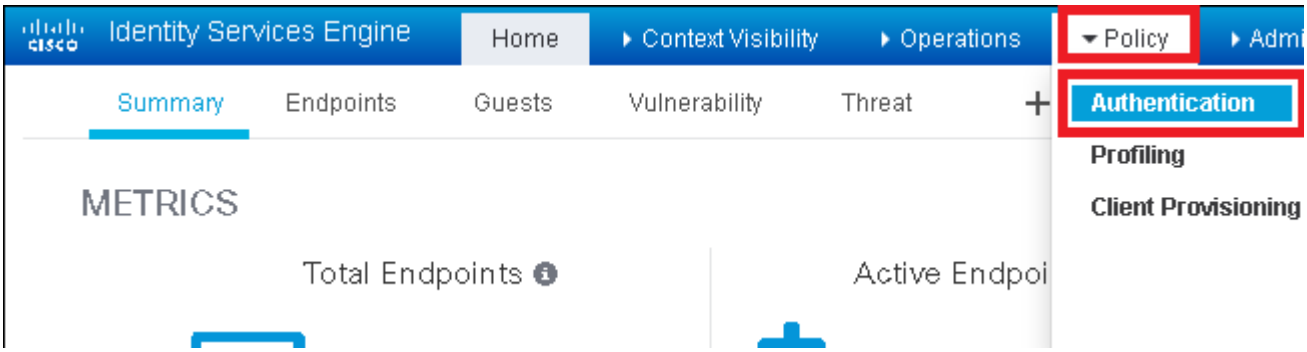
In questo esempio, l'utente appartiene a un gruppo denominato ALL_ACCOUNTS, ma può essere regolato in base alle esigenze, come mostrato nell'immagine.



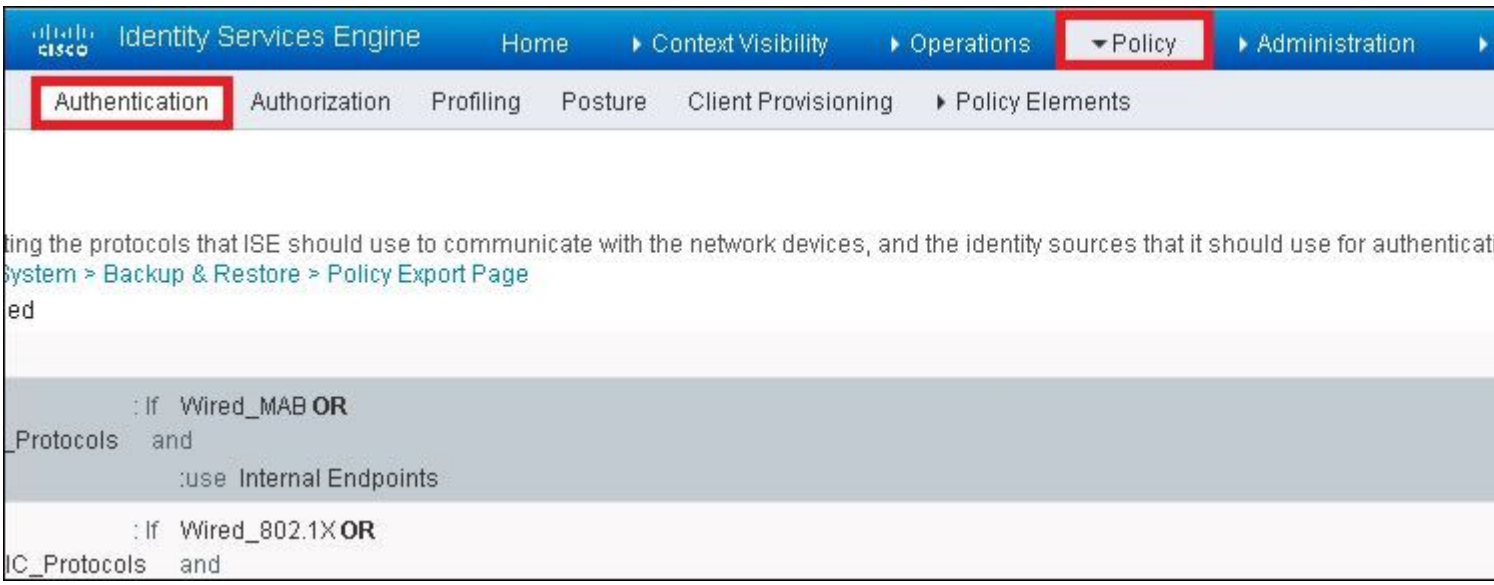
Crea regola di autenticazione

Le regole di autenticazione vengono utilizzate per verificare se le credenziali degli utenti sono corrette, ovvero per verificare se l'utente è effettivamente l'utente che dichiara di essere, e per limitare i metodi di autenticazione che possono essere utilizzati dall'utente.

Passaggio 1. Passare a **Criteri > Autenticazione** come mostrato nell'immagine.

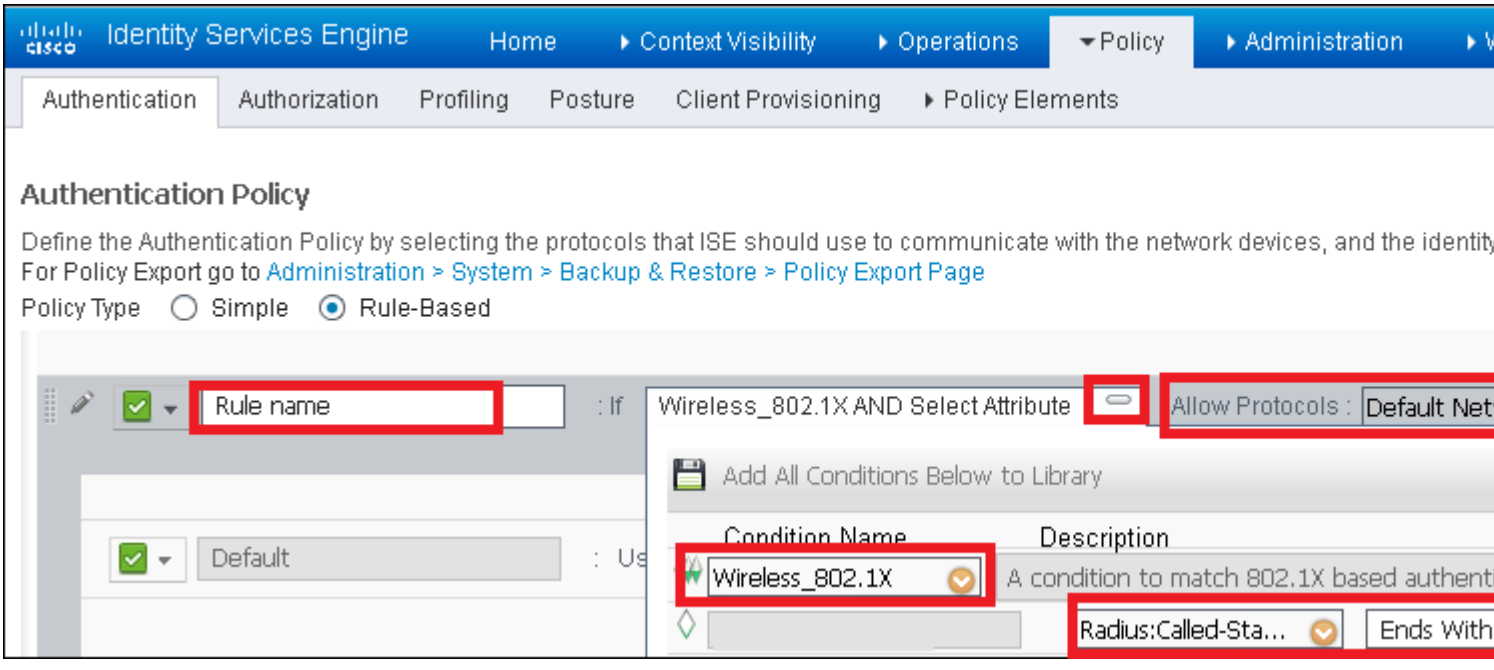


Passaggio 2. Inserire una nuova regola di autenticazione come illustrato nell'immagine.

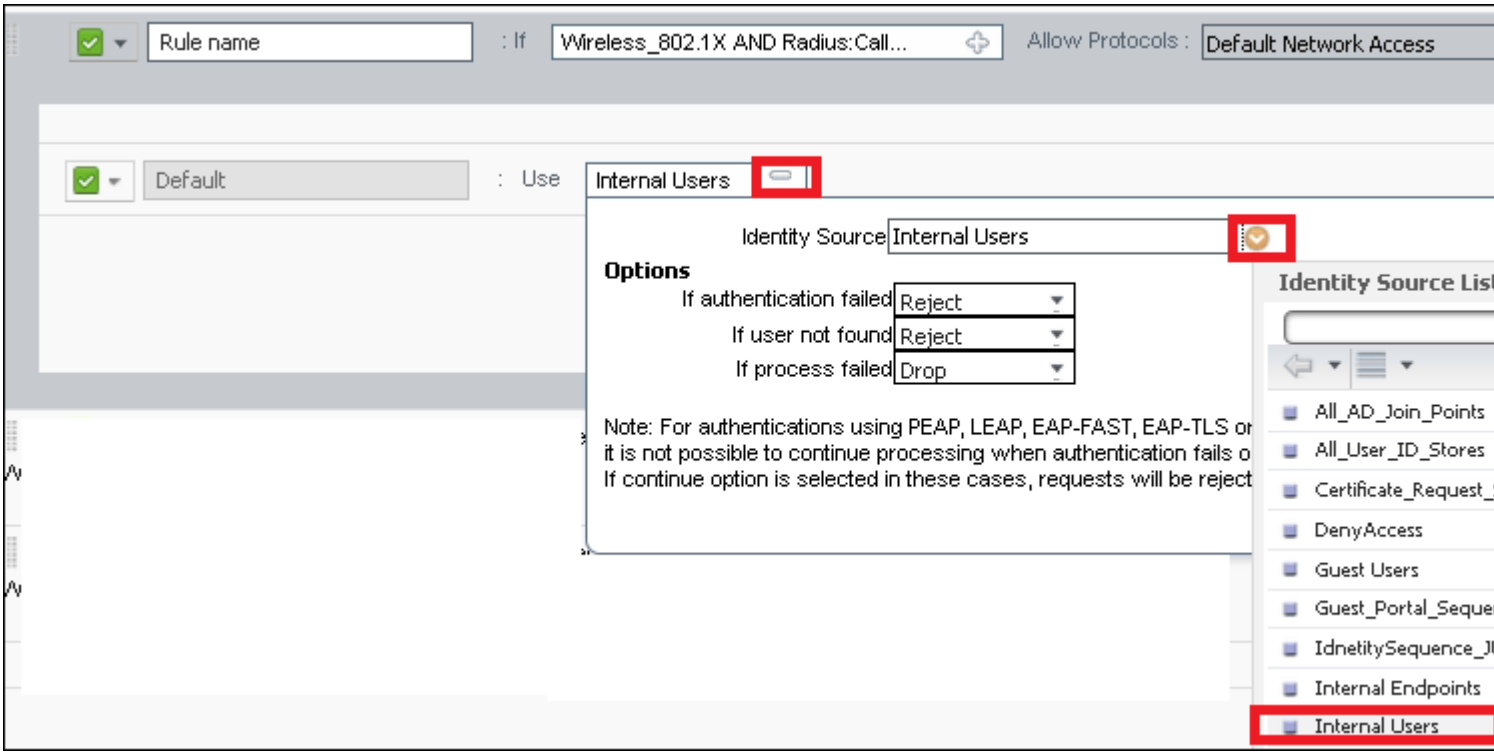


Passaggio 3. Immettere i valori.

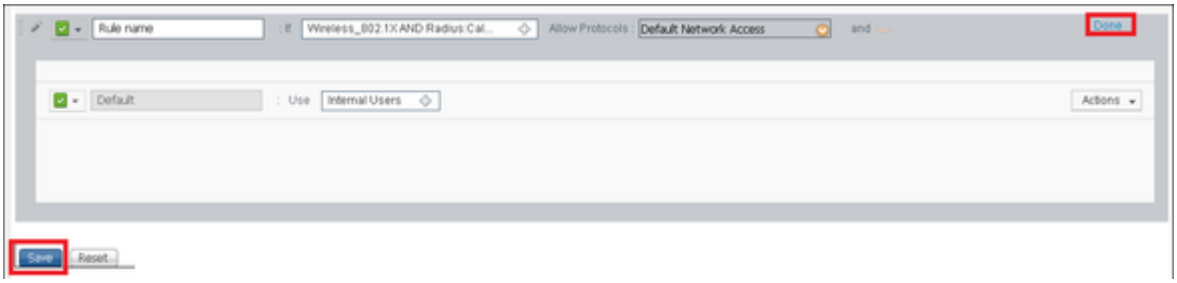
Questa regola di autenticazione consente tutti i protocolli elencati nell'elenco Accesso di rete predefinito. Questo vale per la richiesta di autenticazione per client Wireless 802.1x e con ID stazione chiamata e termina con ise-ssid come mostrato nell'immagine.



Scegliere inoltre l'origine di identità per i client che soddisfano questa regola di autenticazione. In questo esempio viene utilizzato l'elenco delle origini dell'identità degli utenti interni, come illustrato nell'immagine.



Al termine, fate clic su **Fatto (Done)** e su **Salva (Save**), come mostrato nell'immagine.



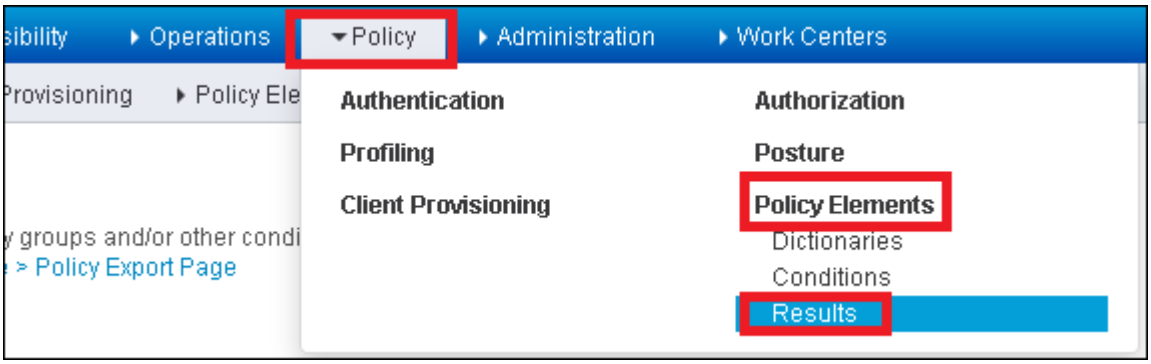
Per ulteriori informazioni sulle origini di identità, vedere questo collegamento:

Crea un gruppo di identità utente

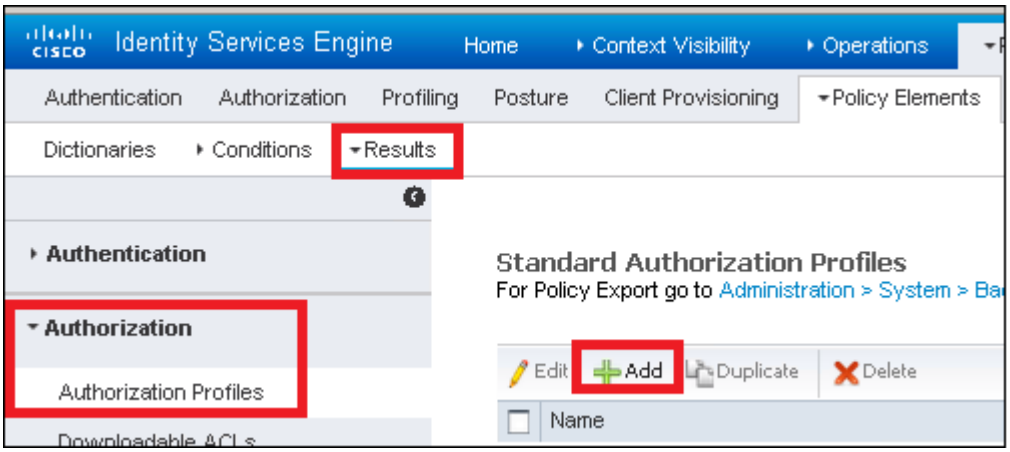
Creazione del profilo di autorizzazione

Il profilo di autorizzazione determina se l'utente ha accesso alla rete. Push Access Control Lists (ACLs), override VLAN o qualsiasi altro parametro. Il profilo di autorizzazione mostrato in questo esempio invia un messaggio di accettazione dell'accesso all'utente e assegna la VLAN 2404.

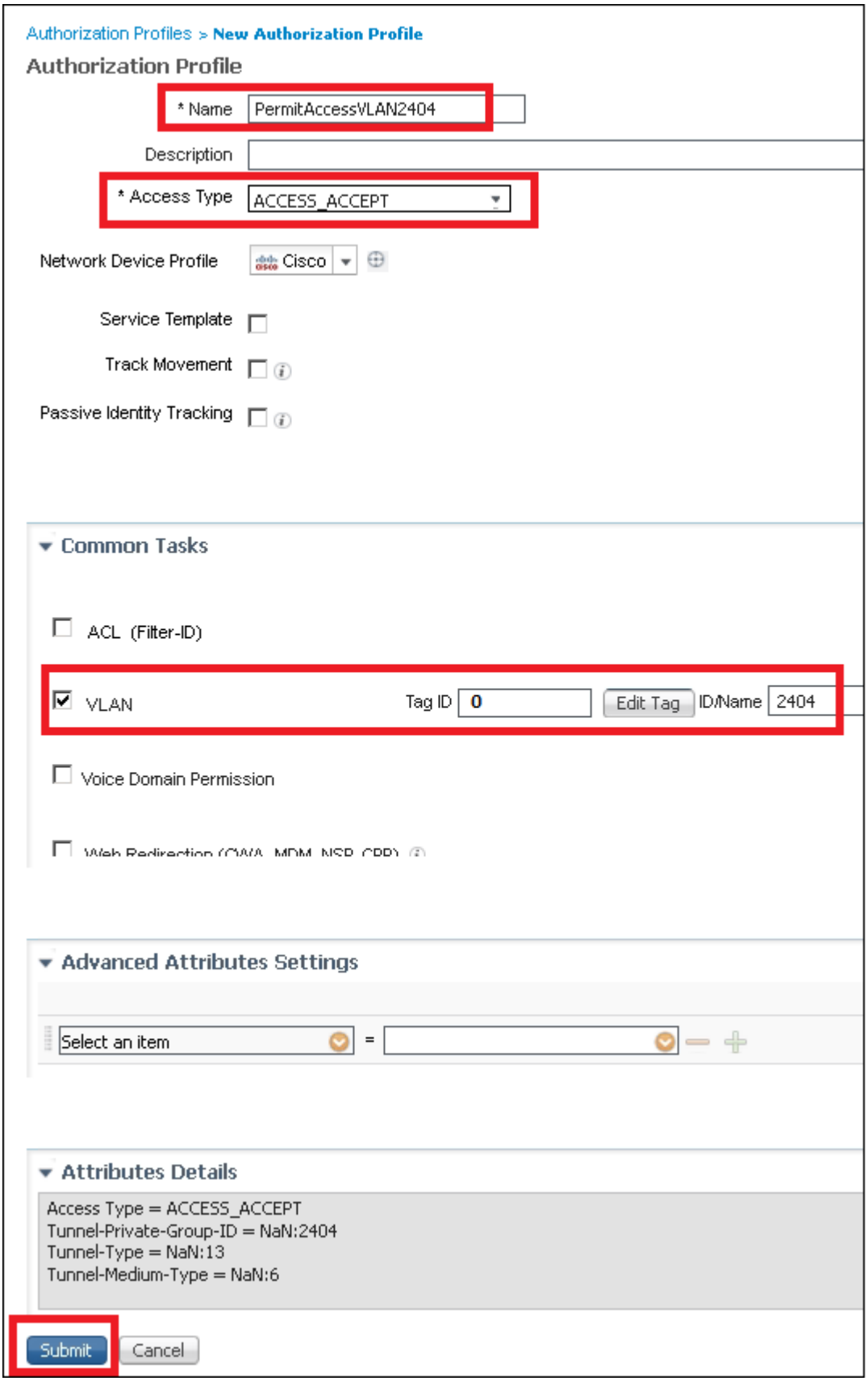
Passaggio 1. Passare a **Criterio > Elementi criteri > Risultati**, come mostrato nell'immagine.



Passaggio 2. Aggiungere un nuovo profilo di autorizzazione. Passare a **Autorizzazione > Profili di autorizzazione > Aggiungi** come mostrato nell'immagine.



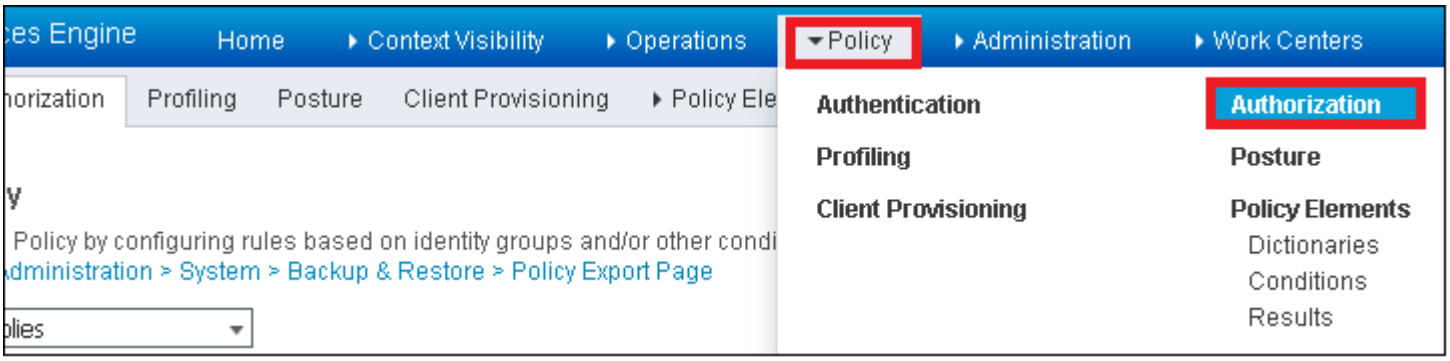
Passaggio 3. Immettete i valori come mostrato nell'immagine.



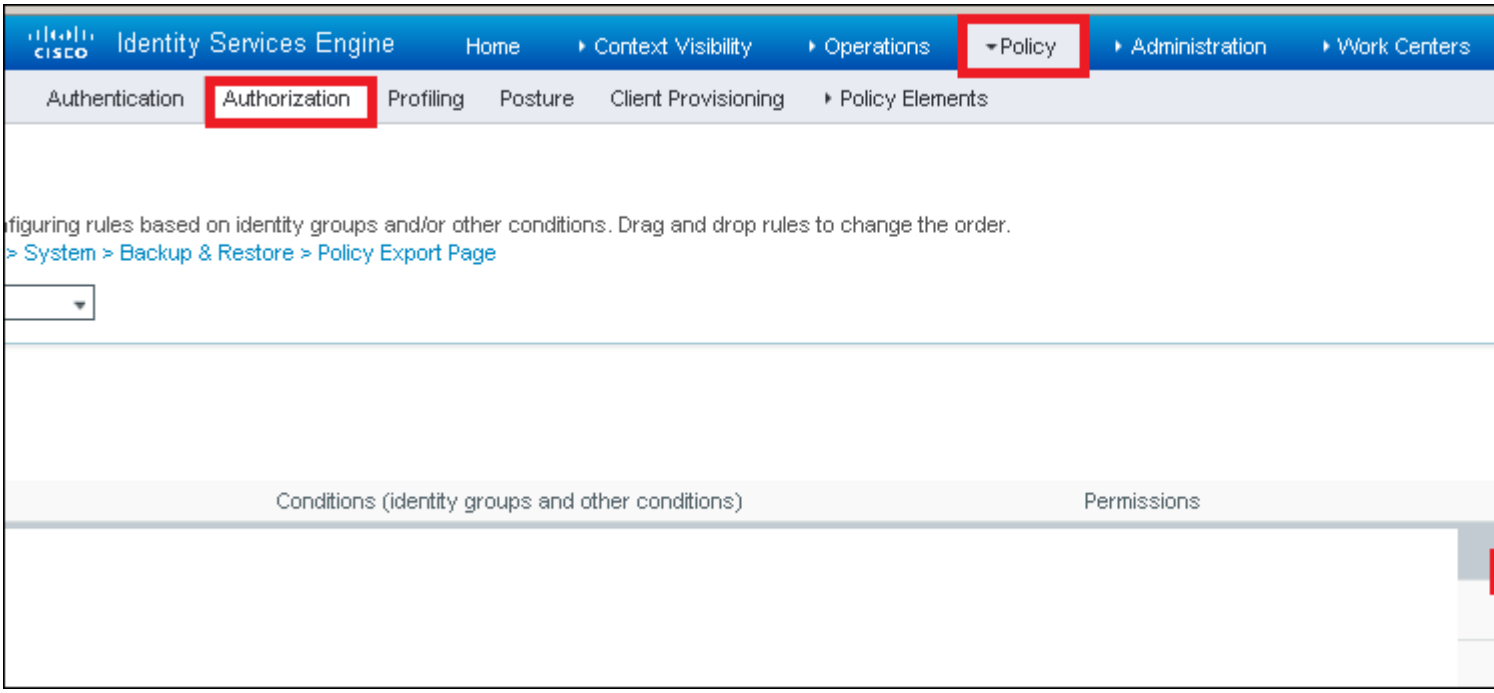
Crea regola di autorizzazione

La regola di autorizzazione è quella incaricata di determinare il risultato delle autorizzazioni (il profilo di autorizzazione) da applicare all'utente.

Passaggio 1. Passare a **Criteri > Autorizzazione** come mostrato nell'immagine.

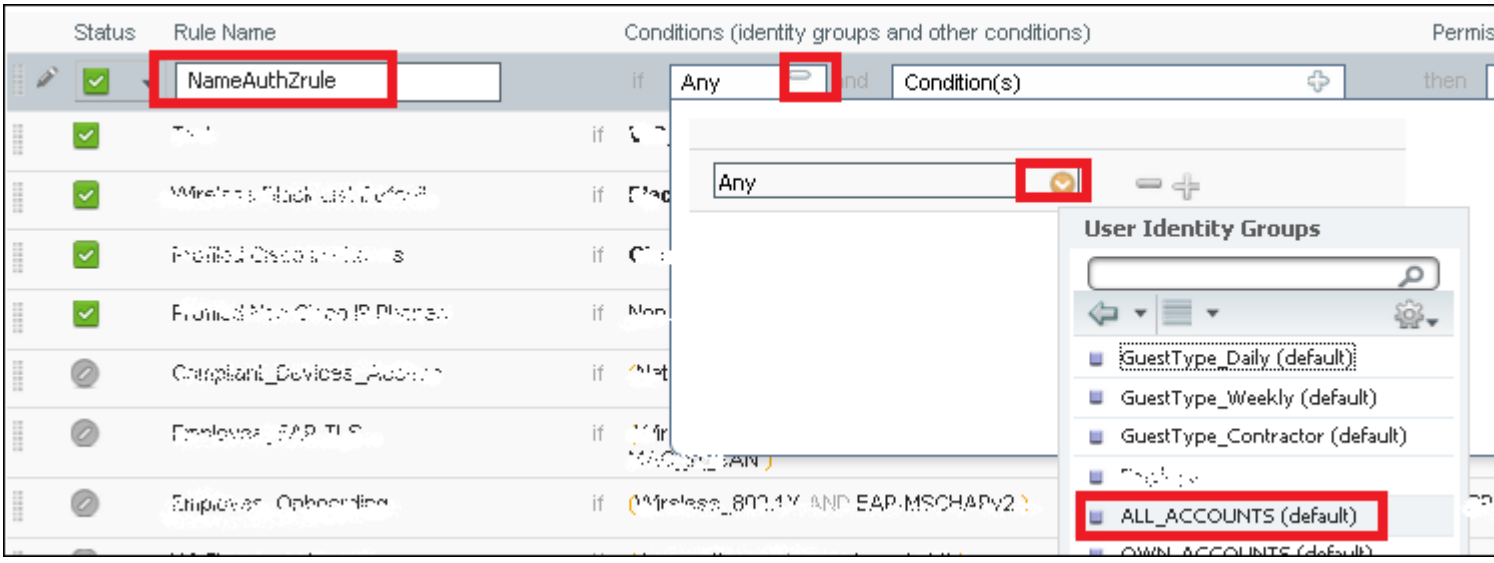


Passaggio 2. Inserite una nuova regola come mostrato nell'immagine.

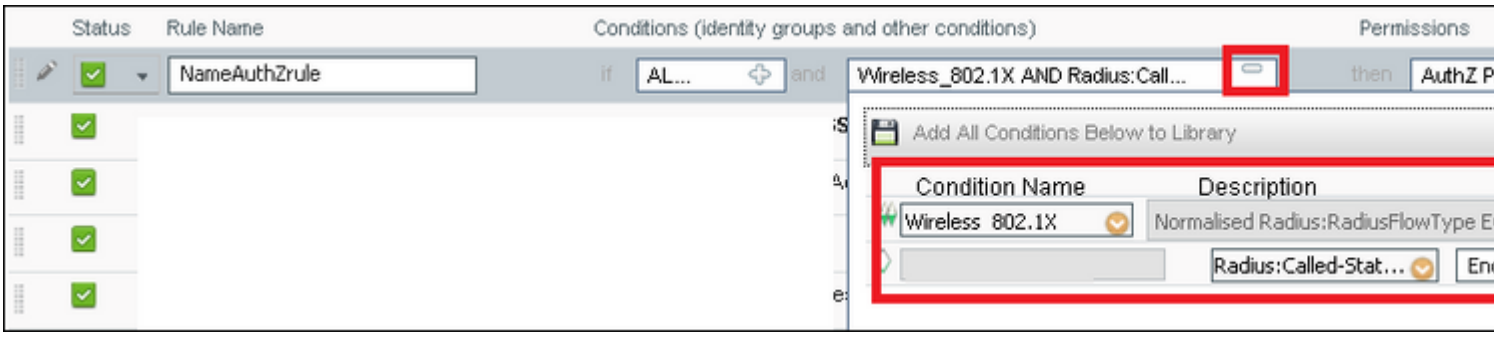


Passaggio 3. Immettere i valori.

Selezionare innanzitutto un nome per la regola e il gruppo di identità in cui è memorizzato l'utente (ALL_ACCOUNTS), come illustrato nell'immagine.



Quindi, selezionare altre condizioni che fanno rientrare il processo di autorizzazione in questa regola. Nell'esempio, il processo di autorizzazione soddisfa questa regola se utilizza una connessione wireless 802.1x e l'ID della stazione chiamata termina con ise-ssid, come mostrato nell'immagine.



Infine, selezionare il profilo di autorizzazione assegnato che corrisponde alla regola. Selezionate **Fatto (Done)** e **Salva (Save)** come mostrato nell'immagine.

Configurazione del dispositivo finale

Configurare un computer portatile Windows 10 per la connessione a un SSID con autenticazione 802.1x e PEAP/MS-CHAPv2 (versione Microsoft del protocollo di autenticazione Challenge-Handshake) versione 2.

Nell'esempio di configurazione, ISE usa il proprio certificato autofirmato per eseguire l'autenticazione.

Per creare il profilo WLAN sul computer Windows, sono disponibili due opzioni:

1. Installare il certificato autofirmato nel computer per convalidare e considerare attendibile il server ISE per completare l'autenticazione.
2. Ignorare la convalida del server RADIUS e considerare attendibile qualsiasi server RADIUS utilizzato per eseguire l'autenticazione (scelta non consigliata, in quanto può diventare un problema di sicurezza).

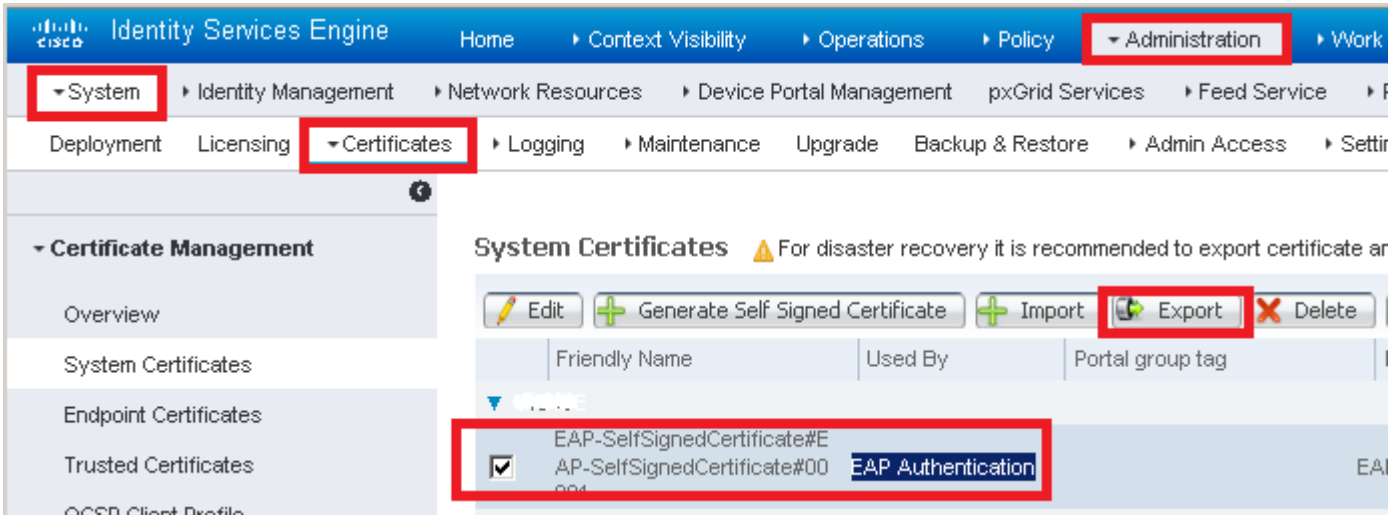
La configurazione di queste opzioni è spiegata in Configurazione del dispositivo terminale - Creazione del profilo WLAN - Passaggio 7.

Fine configurazione dispositivo - Installazione certificato autofirmato ISE

Passaggio 1. Esporta certificato autofirmato.

Accedere ad ISE e selezionare **Amministrazione > Sistema > Certificati > Certificati di sistema**.

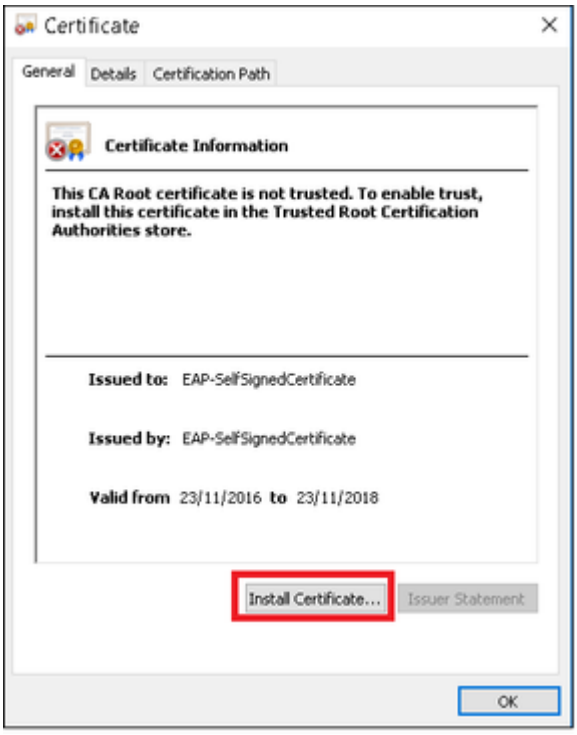
Scegliere quindi il certificato utilizzato per l'**autenticazione EAP** e fare clic su **Esporta**, come mostrato nell'immagine.



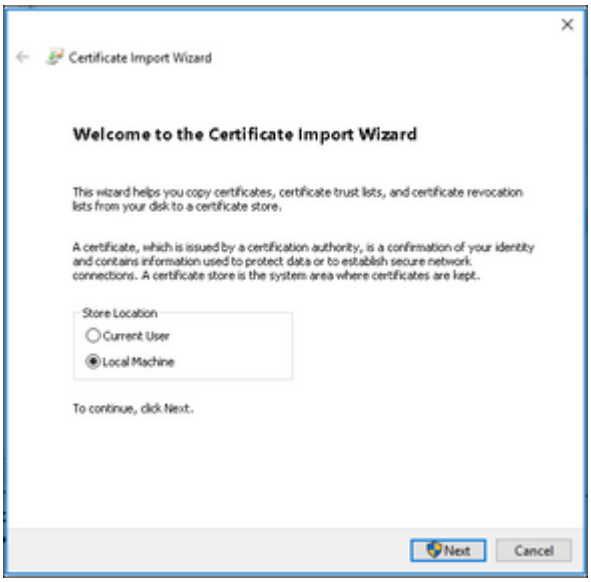
Salvare il certificato nella posizione desiderata. Tale certificato deve essere installato nel computer Windows come illustrato nell'immagine.

Passaggio 2. Installare il certificato nel computer Windows.

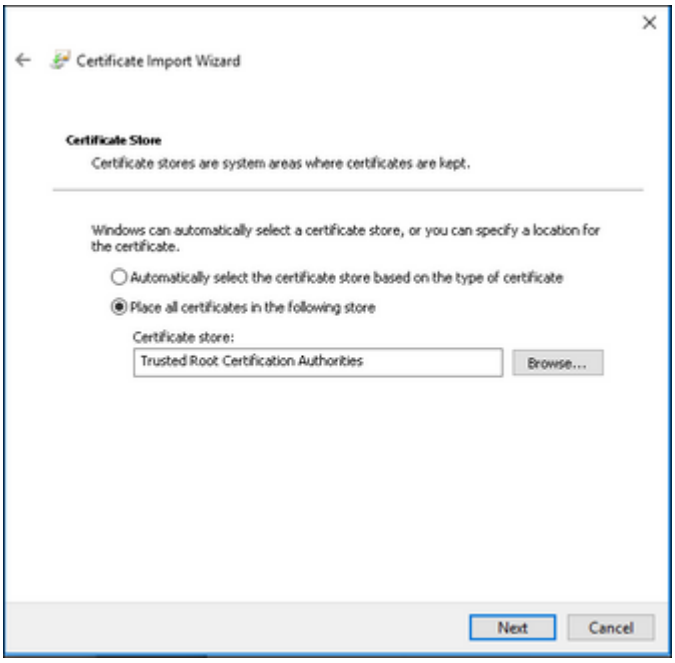
Copiare il certificato esportato da ISE nel computer Windows, modificare l'estensione del file da .pem a .crt, quindi fare doppio clic per installarlo come mostrato nell'immagine.



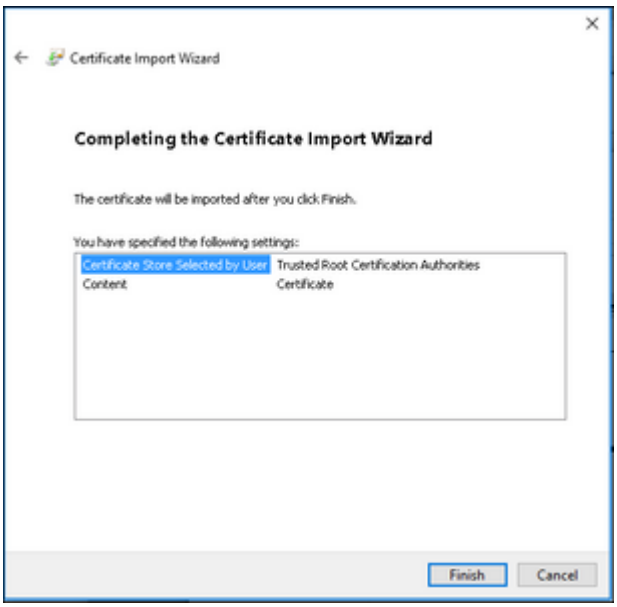
Passaggio 3. Selezionare Installa nel **computer locale** e fare clic su **Avanti**, come mostrato nell'immagine.



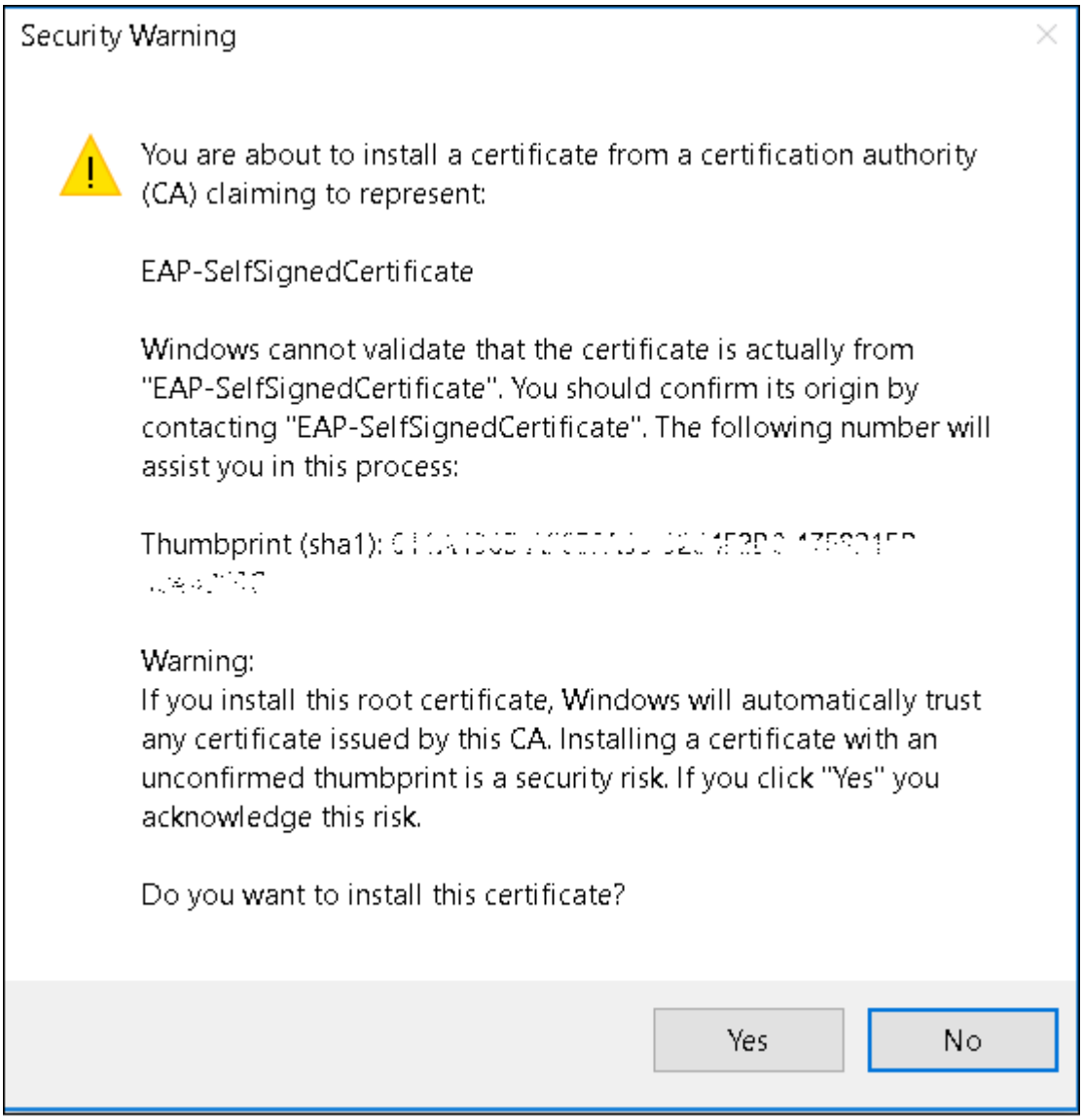
Passaggio 4. Selezionare **Colloca tutti i certificati nell'archivio**, quindi individuare e selezionare **Autorità di certificazione radice attendibili.** Quindi, fare clic su **Next** (Avanti) come mostrato nell'immagine.



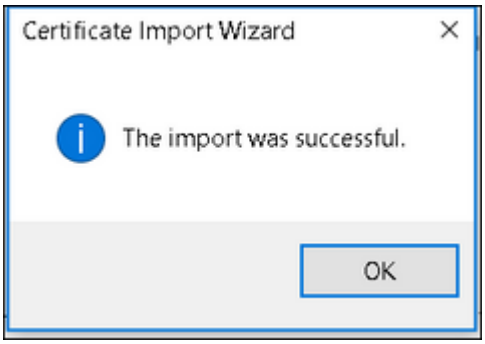
Passaggio 5. Quindi, fare clic su **Finish** (Fine) come mostrato nell'immagine.



Passaggio 6. Confermare l'installazione del certificato. Fare clic su **Yes** (Sì) come illustrato nell'immagine.

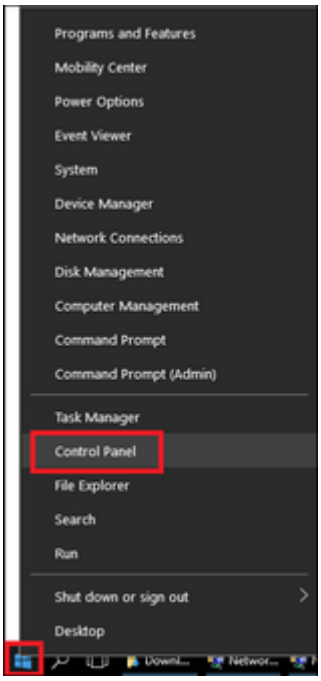


Passaggio 7. Infine, fare clic su **OK** come mostrato nell'immagine.

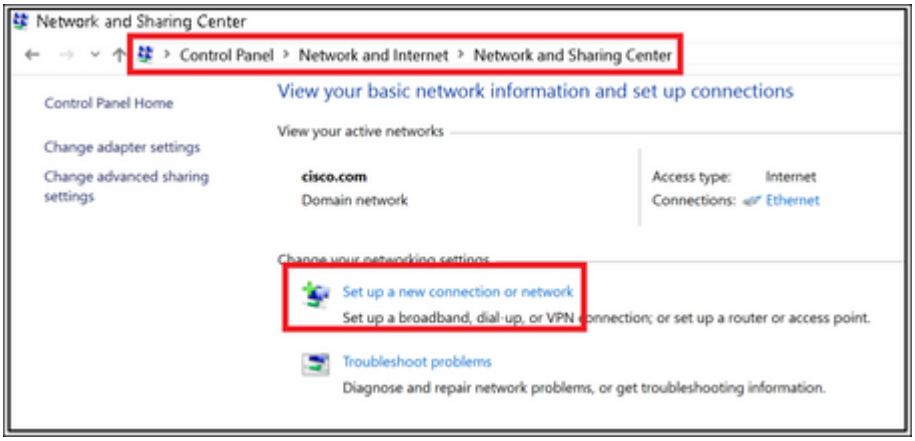


End Device Configuration - Creazione del profilo WLAN

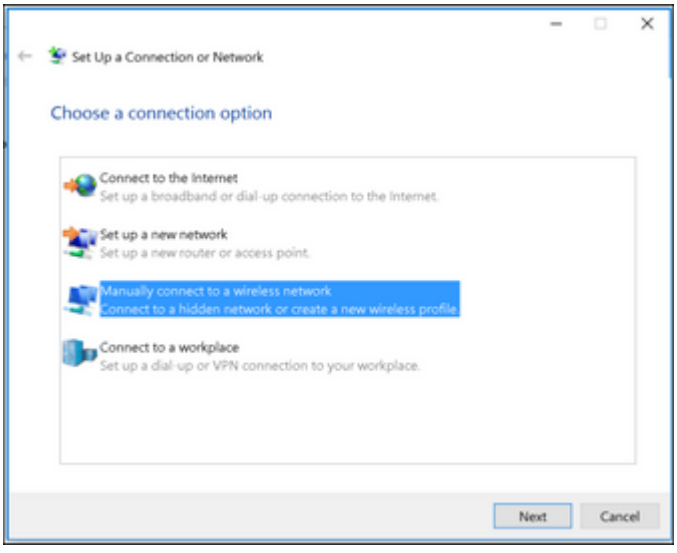
Passaggio 1. Fare clic con il pulsante destro del mouse sull'icona **Start** e selezionare **Pannello di controllo**, come mostrato nell'immagine.



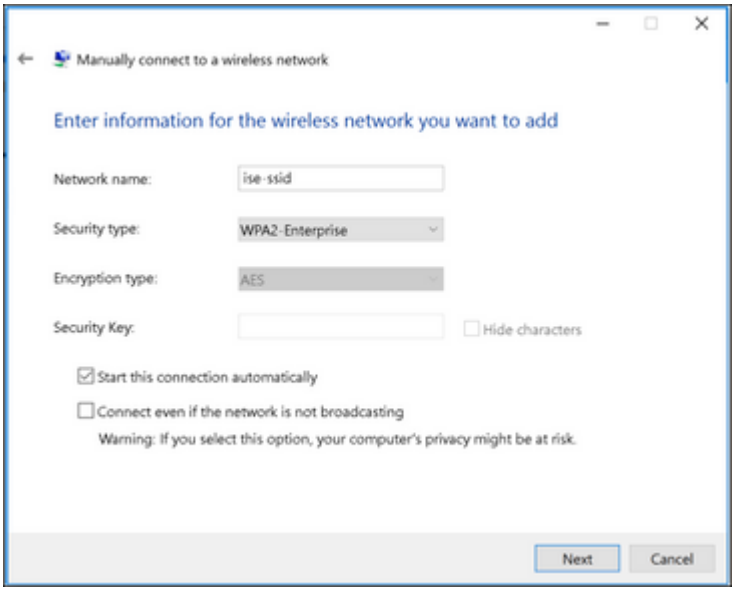
Passaggio 2. Passare a **Rete e Internet** e quindi a **Centro connessioni di rete e condivisione** e fare clic su **Configura nuova connessione o rete** come mostrato nell'immagine.



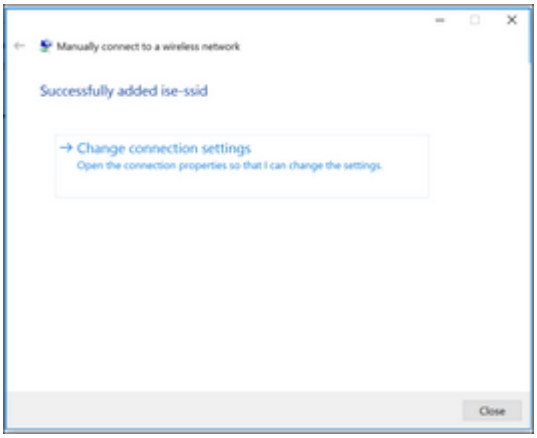
Passaggio 3. Selezionare **Connetti manualmente a una rete wireless**, quindi fare clic su **Avanti** come mostrato nell'immagine.



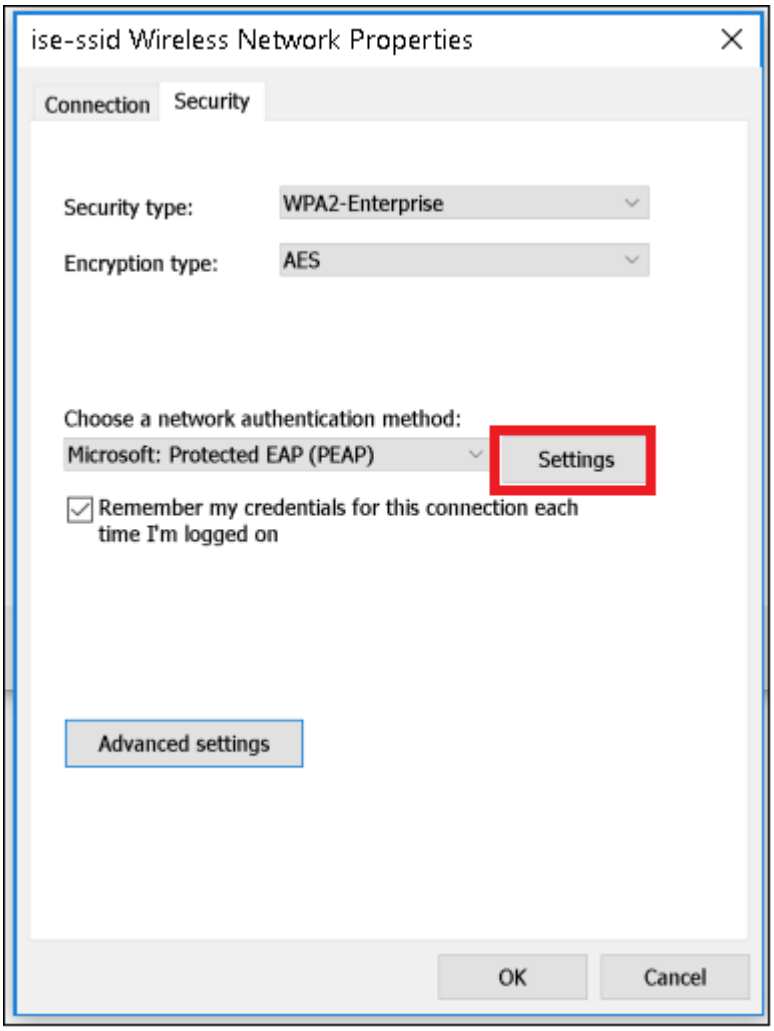
Passaggio 4. Immettere le informazioni con il nome del SSID e il tipo di protezione WPA2-Enterprise e fare clic su **Avanti**, come mostrato nell'immagine.



Passaggio 5. Per personalizzare la configurazione del profilo WLAN, selezionare **Change connection settings** (Cambia impostazioni di connessione)come mostrato nell'immagine.



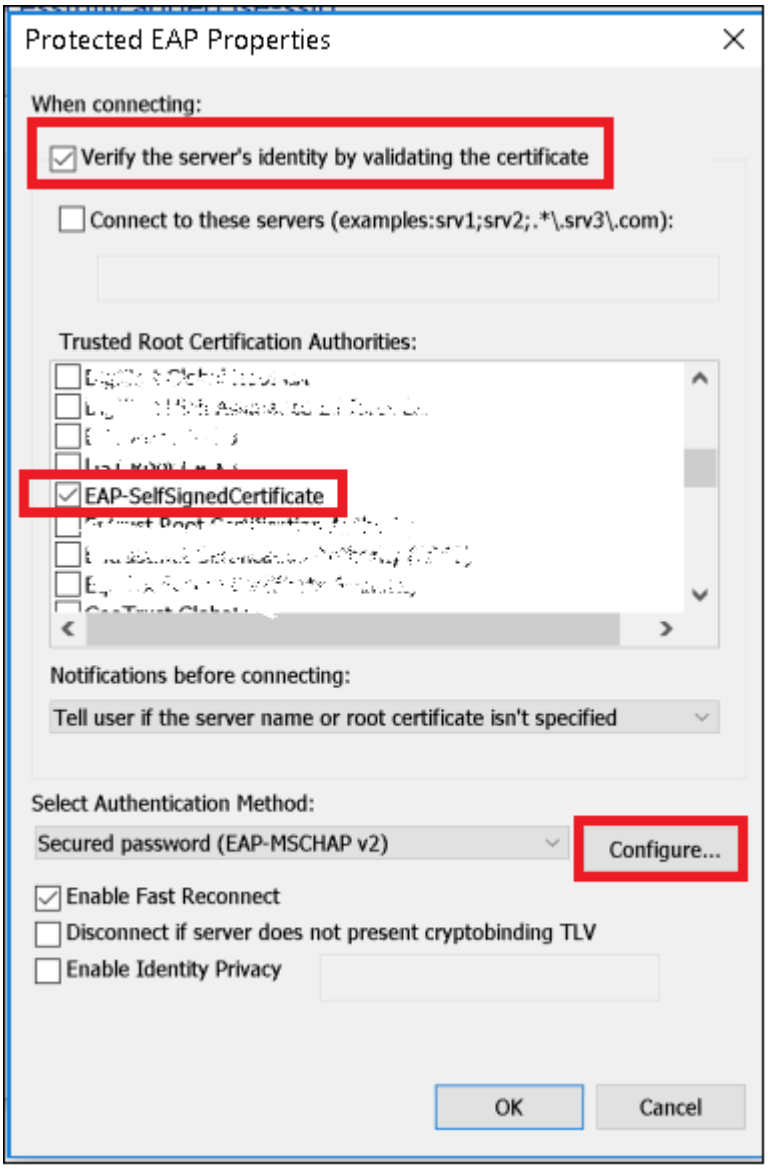
Passaggio 6. Passare alla scheda **Protezione** e fare clic su **Impostazioni** come mostrato nell'immagine.

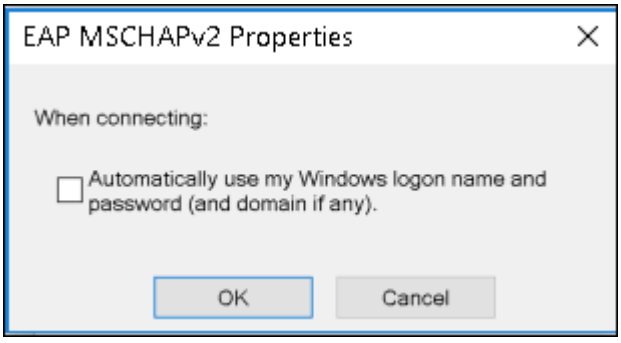


Passaggio 7. Selezionare se il server RADIUS è convalidato o meno.

In caso affermativo, abilitare **Verifica dell'identità del server convalidando il certificato** e dall'elenco **Autorità di certificazione radice attendibili** selezionare il certificato autofirmato ISE.

Quindi selezionare **Configure** and disable **Automatically use my Windows logon name and password...**, quindi fare clic su **OK** come mostrato nelle immagini.

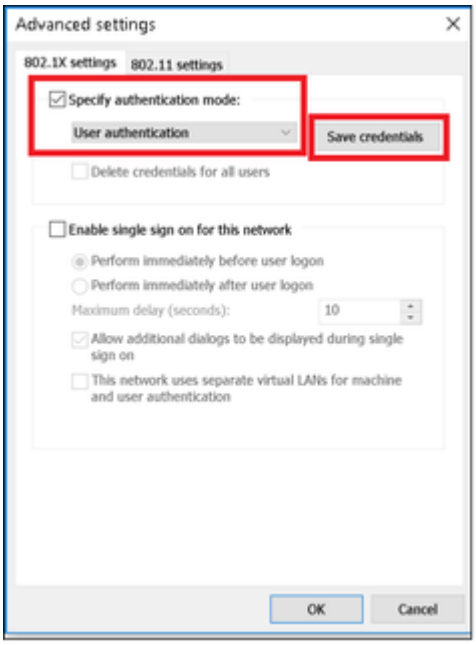


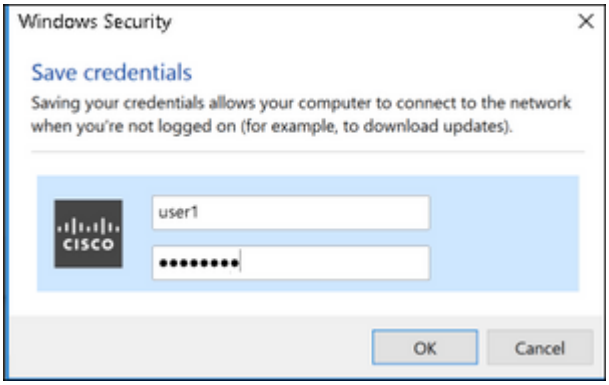


Passaggio 8. Configurare le credenziali utente.

Una volta tornata alla scheda **Sicurezza**, selezionare **Impostazioni avanzate**, specificare la modalità di autenticazione come Autenticazione utente e **salvare** le credenziali configurate su ISE per autenticare l'utente come mostrato nelle immagini.


ise-ssid Wireless Network Properties
Connection
Security
Security type:
WPA2-Enterprise
Encryption type:
AES
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)
Settings
Remember my credentials for this connection each time I'm logged on
Advanced settings
OK
Cancel


Advanced settings
802.1X settings
802.11 settings
Specify authentication mode:
User authentication
Save credentials
Delete credentials for all users
Enable single sign on for this network
Perform immediately before user logon
Perform immediately after user logon
Maximum delay (seconds):
10
Allow additional dialogs to be displayed during single sign on
This network uses separate virtual LANs for machine and user authentication
OK
Cancel


Windows Security
Save credentials
Saving your credentials allows your computer to connect to the network when you're not logged on (for example, to download updates).
user1
OK
Cancel

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Il flusso di autenticazione può essere verificato dal WLC o dalla prospettiva ISE.

Processo di autenticazione su WLC

Per monitorare il processo di autenticazione per un utente specifico, eseguire i comandi seguenti:

```
> debug client <mac-add-client>
> debug dot1x event enable
> debug dot1x aaa enable
```

Esempio di autenticazione riuscita (alcuni output sono stati omessi):

<#root>

```
*apfMsConnTask_1: Nov 24 04:30:44.317:

e4:b3:18:7c:30:58 Processing assoc-req station:e4:b3:18:7c:30:58 AP:00:c8:8b:26:2c:d0-00

 thread:1a5cc288
*apfMsConnTask_1: Nov 24 04:30:44.317: e4:b3:18:7c:30:58 Reassociation received from mobile on BSSID 00:
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying Interface(management) policy on Mobile
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying site-specific Local Bridging override
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying Local Bridging Interface Policy for st
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 RSN Capabilities:  60
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Marking Mobile as non-

e4:b3:18:7c:30:58 Received 802.11i 802.1X key management suite, enabling dot1x Authentication

11w Capable
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Received RSN IE with 1 PMKIDs from mobile e4:b3
*apfMsConnTask_1: Nov 24 04:30:44.319: Received PMKID:  (16)
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Searching for PMKID in MSCB PMKID cache for mob
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 No valid PMKID found in the MSCB PMKID cache fo
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 0.0.0.0 START (0) Initializing policy
*apfMsConnTask_1: Nov 24 04:30:44.319:

e4:b3:18:7c:30:58 0.0.0.0 START (0) Change state to AUTHCHECK (2) last state START (0)

*apfMsConnTask_1: Nov 24 04:30:44.319:

e4:b3:18:7c:30:58 0.0.0.0 AUTHCHECK (2) Change state to 8021X_REQD (3) last state AUTHCHECK (2)

*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 0.0.0.0 8021X_REQD (3) Plumbed mobile LWAPP rul
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfMsAssoStateInc
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfPemAddUser2 (apf_policy.c:437) Changing stat
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfPemAddUser2:session timeout forstation e4:b3
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Stopping deletion of Mobile Station: (callerId:
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Func: apfPemAddUser2, Ms Timeout = 0, Session T
*apfMsConnTask_1: Nov 24 04:30:44.320: e4:b3:18:7c:30:58 Sending Assoc Response to station on BSSID 00:c
*spamApTask2: Nov 24 04:30:44.323: e4:b3:18:7c:30:58 Successful transmission of LWAPP Add-Mobile to AP 0
*spamApTask2: Nov 24 04:30:44.325: e4:b3:18:7c:30:58 Received ADD_MOBILE ack - Initiating 1x to STA e4:b
*spamApTask2: Nov 24 04:30:44.325: e4:b3:18:7c:30:58

Sent dot1x auth initiate message for mobile e4:b3:18:7c:30:58

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 reauth_sm state transition 0 ---> 1 for mobi
```

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 EAP-PARAM Debug - eap-params for Wlan-Id :2
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Disable re-auth, use PMK lifetime.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Station e4:b3:18:7c:30:58 setting dot1x reau
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Stopping reauth timeout for e4:b3:18:7c:30:5
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 into
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326:
```

e4:b3:18:7c:30:58 Sending EAP-Request/Identity to mobile e4:b3:18:7c:30:58 (EAP Id 1)

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Received EAPOL EAPPKT from mobile e4:b3:18:7
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Received Identity Response (count=1) from mo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Resetting reauth count 1 to 0 for mobile e4:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 EAP State update from Connecting to Authenti
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 into
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Entering Backend Auth Response state for mob
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Created Acct-Session-ID (58366cf4/e4:b3:18:7
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.386: e4:b3:18:7c:30:58 Processing Access-Challenge for mobile e4:b3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Entering Backend Auth Req state (id=215) for
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 WARNING: updated EAP-Identifier 1 ===> 215 f
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Sending EAP Request from AAA to mobile e4:b3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Allocating EAP Pkt for retransmission to mob
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Received EAPOL EAPPKT from mobile e4:b3:18:7
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Received EAP Response from mobile e4:b3:18:7
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Resetting reauth count 0 to 0 for mobile e4:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Entering Backend Auth Response state for mob
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Processing Access-Challenge for mobile e4:b3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Entering Backend Auth Req state (id=216) for
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Sending EAP Request from AAA to mobile e4:b3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Reusing allocated memory for  EAP Pkt for re
.
.
.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530:
```

e4:b3:18:7c:30:58 Processing Access-Accept for mobile e4:b3:18:7c:30:58

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Resetting web IPv4 acl from 255 to 255
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Resetting web IPv4 Flex acl from 65535 to 65
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530:
```

e4:b3:18:7c:30:58 Username entry (user1) created for mobile, length = 253

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530:
```

e4:b3:18:7c:30:58 Found an interface name:'vlan2404' corresponds to interface name received: vlan2404

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 override for default ap group, marking intgr
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Applying Interface(management) policy on Mob
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Re-applying interface policy for client
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 apfApplyWlanPolicy: Apply WLAN Policy over P
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531:
```

e4:b3:18:7c:30:58 Inserting AAA Override struct for mobile

```
        MAC: e4:b3:18:7c:30:58, source 4
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Applying override policy from source Overrid
*Dot1x_NW_MsgTask_0: Nov 24
```

04:30:44.531: e4:b3:18:7c:30:58 Found an interface name:'vlan2404' corresponds to interface name receive

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Applying Interface(vlan2404) policy on Mobil
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Re-applying interface policy for client
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Setting re-auth timeout to 0 seconds, got fr
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Station e4:b3:18:7c:30:58 setting dot1x reau
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Stopping reauth timeout for e4:b3:18:7c:30:5
```

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Creating a PKC PMKID Cache entry for station
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Resetting MSCB PMK Cache Entry 0 for station
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Adding BSSID 00:c8:8b:26:2c:d1 to PMKID cach
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: New PMKID: (16)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531:      [0000] cc 3a 3d 26 80 17 8b f1 2d c5 cd fd a0 8a c4 39
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 unsetting PmkIdValidatedByAp
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Updating AAA Overrides from local for static
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Adding Audit session ID payload in Mobility
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 0 PMK-update groupcast messages sent
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 PMK sent to mobility group
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Disabling re-auth since PMK lifetime can tak
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Sending EAP-Success to mobile e4:b3:18:7c:30
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Freeing AAACB from Dot1xCB as AAA auth is do
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Found an cache entry for BSSID 00:c8:8b:26:2
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: Including PMKID in M1  (16)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:      [0000] cc 3a 3d 26 80 17 8b f1 2d c5 cd fd a0 8a c4 39
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: M1 - Key Data: (22)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:      [0000] dd 14 00 0f ac 04 cc 3a 3d 26 80 17 8b f1 2d c5
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:      [0016] cd fd a0 8a c4 39
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:
```

e4:b3:18:7c:30:58 Starting key exchange to mobile e4:b3:18:7c:30:58, data packets will be dropped

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:
```

e4:b3:18:7c:30:58 Sending EAPOL-Key Message to mobile e4:b3:18:7c:30:58

```
state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Reusing allocated memory for  EAP Pkt for re
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Entering Backend Auth Success state (id=223)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Received Auth Success while in Authenticatin
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 into
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 Received EAPOL-Key from mobile e4:b3:18:7c:3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 Ignoring invalid EAPOL version (1) in EAPOL-
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547:
```

e4:b3:18:7c:30:58 Received EAPOL-key in PTK_START state (message 2) from mobile

```
 e4:b3:18:7c:30:58
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Successfully computed PTK from PMK!!!
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Received valid MIC in EAPOL Key Message M2!!
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Not Flex client. Do not distribute PMK Key c
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Stopping retransmission timer for mobile e4:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Sending EAPOL-Key Message to mobile e4:b3:18
state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Reusing allocated memory for  EAP Pkt for re
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Received EAPOL-Key from mobile e4:b3:18:7c:3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Ignoring invalid EAPOL version (1) in EAPOL-
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555:
```

e4:b3:18:7c:30:58 Received EAPOL-key in PTKINITNEGOTIATING state (message 4)

```
 from mobile e4:b3:18:7c:30:58
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Stopping retransmission timer for mobile e4:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Freeing EAP Retransmit Bufer for mobile e4:b
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMs1xStateInc
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMsPeapSimReqCntInc
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMsPeapSimReqSuccessCntInc
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555:
```

e4:b3:18:7c:30:58 0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last state 8021X_REQD (3)

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Mobility query, PEM State: L2AUTHCOMPLETE
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Building Mobile Announce :
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58   Building Client Payload:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     Client Ip: 0.0.0.0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     Client Vlan Ip: 172.16.0.134, Vlan mask
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     Client Vap Security: 16384
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     Virtual Ip: 10.10.10.10
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     ssid: ise-ssid
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58   Building VlanIpPayload.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Not Using WMM Compliance code qosCap 00
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile LW
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556:
```

e4:b3:18:7c:30:58 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6677,
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Adding Fast Path rule
  type = Airespace AP - Learn IP address
  on AP 00:c8:8b:26:2c:d0, slot 0, interface = 1, QOS = 0
  IPv4 ACL ID = 255, IPv
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Successfully plumbed m
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Successfully Plumbed PTK session Keysfor mob
*spamApTask2: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Successful transmission of LWAPP Add-Mobile to AP 0
*pemReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) mobility role update reque
  Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 172.16.0.3
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) State Update from Mobility
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6315, Add
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Replacing Fast Path rule
  IPv4 ACL ID = 255,
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...)
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...)
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobil
*pemReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 Sent an XID frame
*dtlArpTask: Nov 24 04:30:47.932: e4:b3:18:7c:30:58 Static IP client associated to interface vlan2404 wh
*dtlArpTask: Nov 24 04:30:47.933: e4:b3:18:7c:30:58 apfMsRunStateInc
*dtlArpTask: Nov 24 04:30:47.933:
```

e4:b3:18:7c:30:58 172.16.0.151 DHCP_REQD (7) Change state to RUN (20)

```
 last state DHCP_REQD (7)
```

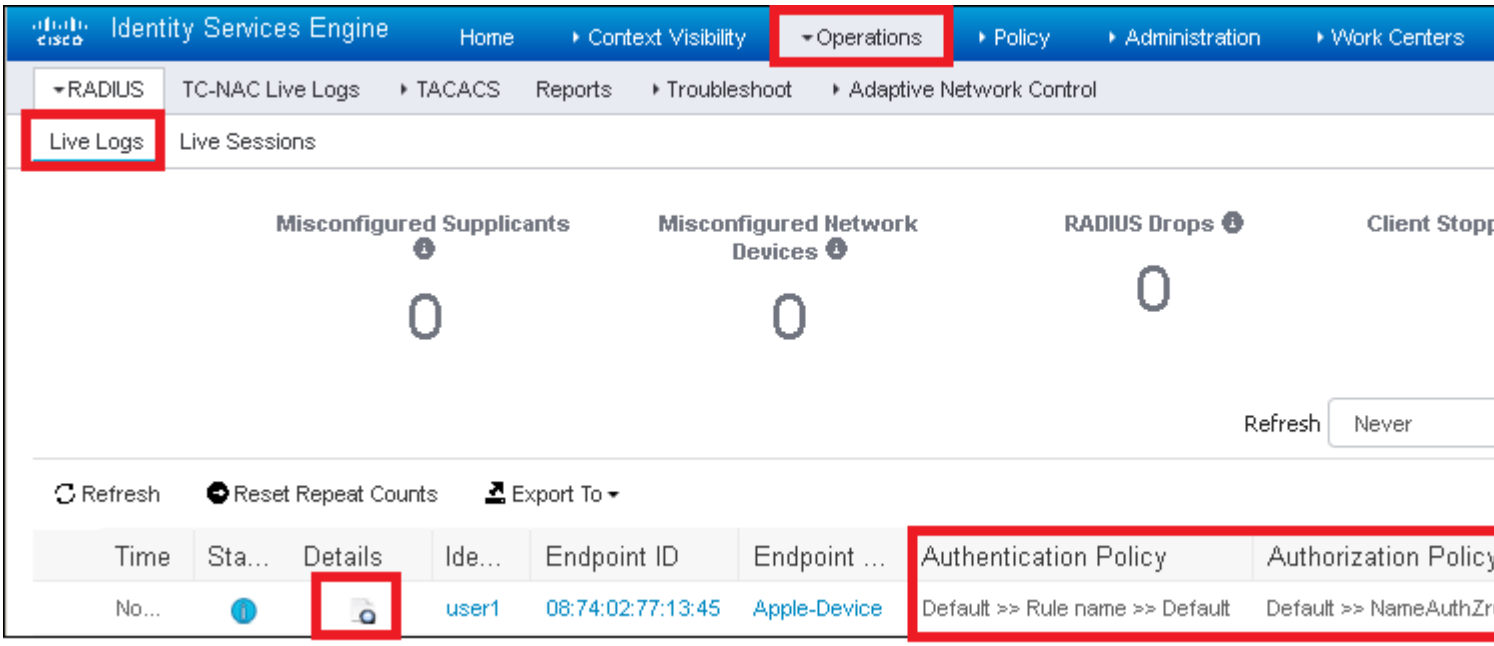
Per leggere facilmente gli output dei client di debug, usare lo strumento Wireless debug analyzer:

Wireless Debug Analyzer

Processo di autenticazione su ISE

Passare a **Operazioni > RADIUS > Live Log** per verificare quale criterio di autenticazione, criterio di autorizzazione e profilo di autorizzazione sono stati assegnati all'utente.

Per ulteriori informazioni, fare clic su **Details** (Dettagli) per visualizzare un processo di autenticazione più dettagliato, come mostrato nell'immagine.



Risoluzione dei problemi

Non sono attualmente disponibili informazioni specifiche per risolvere i problemi relativi a questa configurazione.

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).