

Override 802.1x WLAN + VLAN con Mobility Express (ME) 8.2 e ISE 2.1

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configurazione su ME](#)

[Dichiaratemi ad ISE](#)

[Crea un nuovo utente su ISE](#)

[Creare la regola di autenticazione](#)

[Creare la regola di autorizzazione](#)

[Configurazione del dispositivo terminale](#)

[Verifica](#)

[Processo di autenticazione in ME](#)

[Processo di autenticazione su ISE](#)

Introduzione

In questo documento viene descritto come configurare una WLAN (Wireless Local Area Network) con protezione aziendale Wi-Fi Protected Access 2 (WPA2) con un controller Mobility Express e un server esterno RADIUS (Remote Authentication Dial-In User Service). Identity Service Engine (ISE) è utilizzato come esempio di server RADIUS esterni.

Il protocollo EAP (Extensible Authentication Protocol) utilizzato in questa guida è PEAP (Protected Extensible Authentication Protocol). Inoltre, il client è assegnato a una VLAN specifica (diversa da quella assegnata alla WLAN per impostazione predefinita).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- 802.1x
- PEAP
- CA (Certification Authority)
- Certificati

Componenti usati

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

ME v8.2

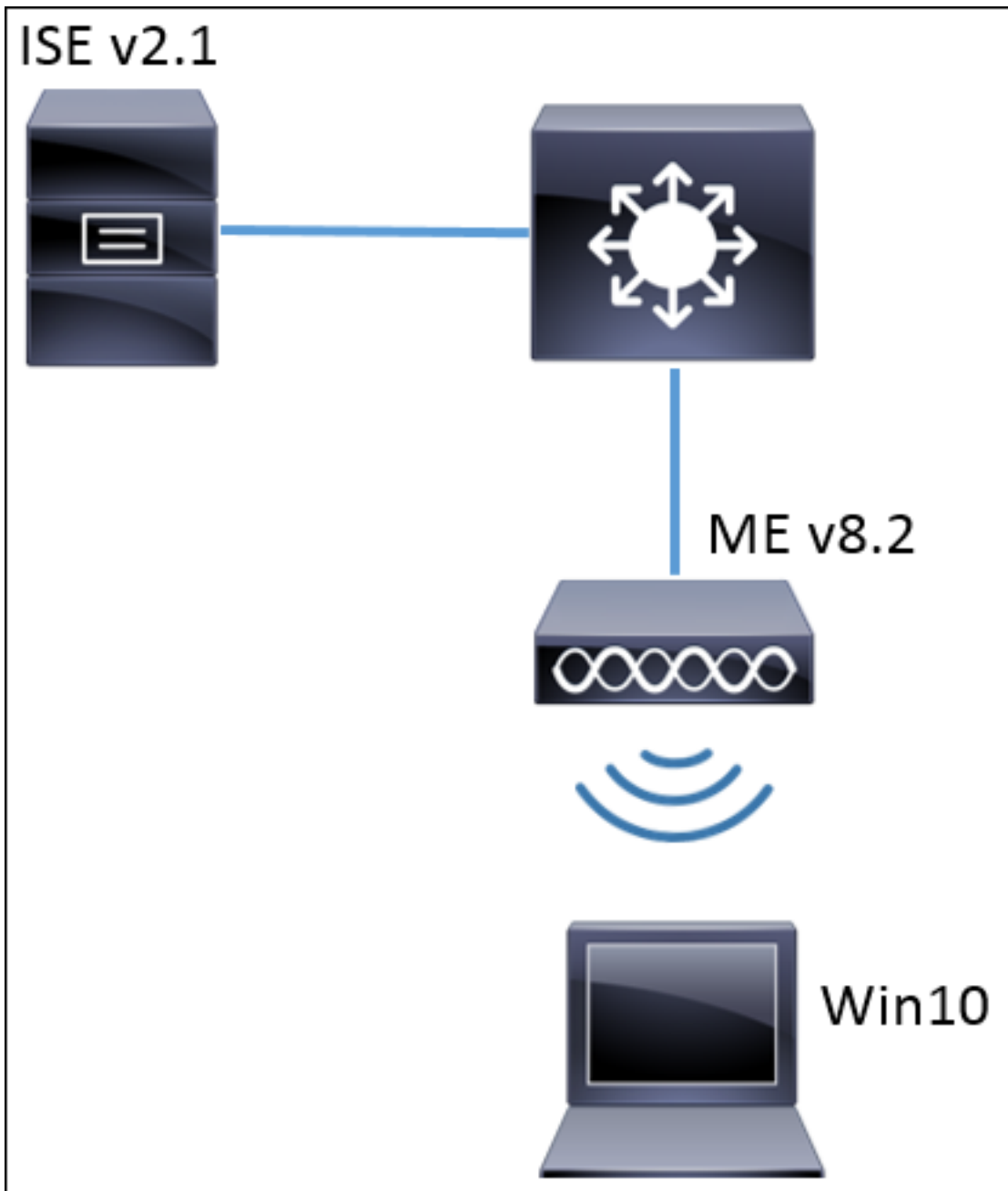
ISE v2.1

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.

Configurazione

Esempio di rete



Configurazioni

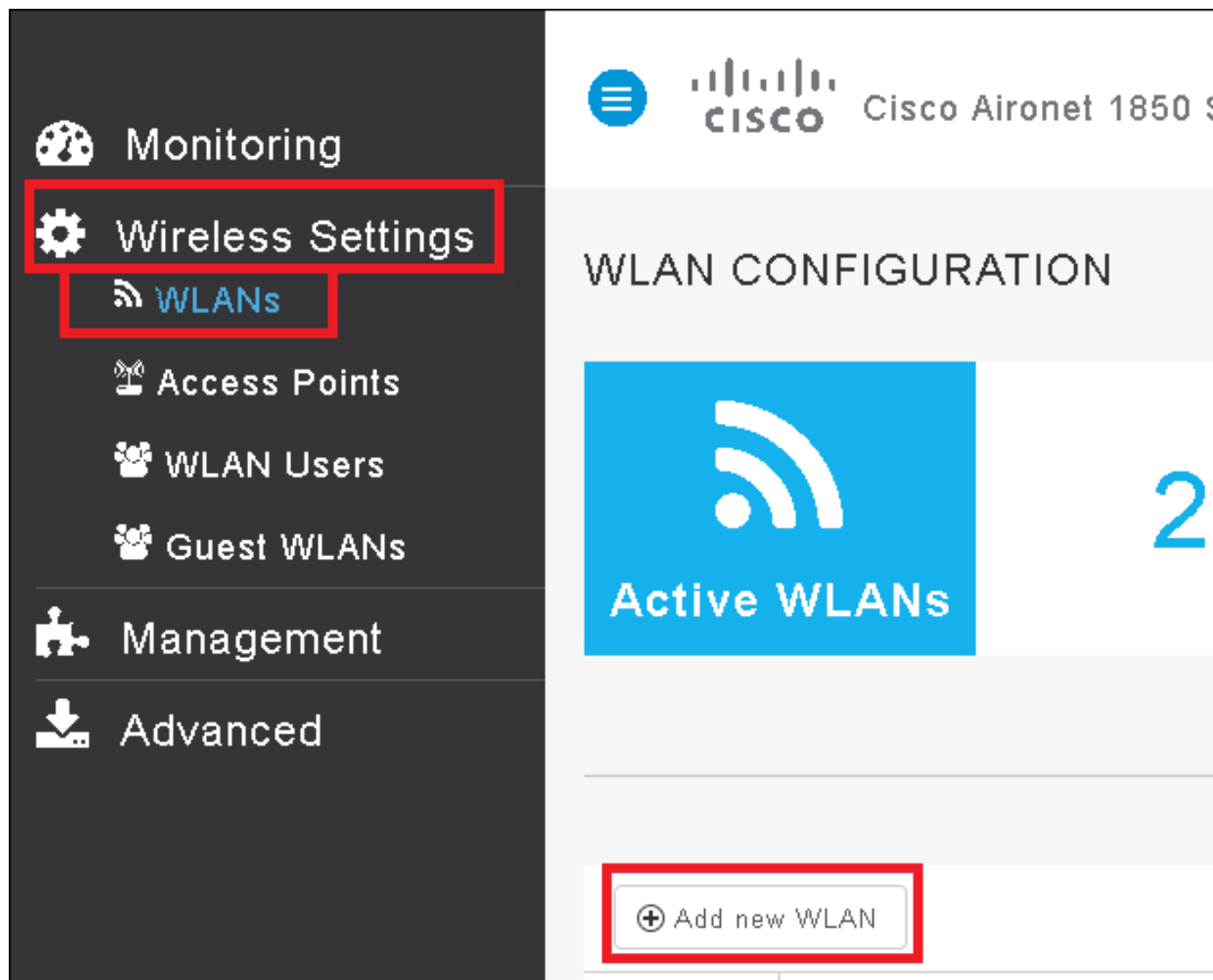
Le fasi generali sono:

1. Creare il Service Set Identifier (SSID) in ME e dichiarare il server RADIUS (ISE in questo esempio) in ME
2. Dichiarare ME su server RADIUS (ISE)
3. Creare la regola di autenticazione su ISE
4. Creare la regola di autorizzazione in ISE
5. Configurare l'endpoint

Configurazione su ME

Per consentire la comunicazione tra il server RADIUS e ME è necessario registrare il server RADIUS su ME e viceversa. In questo passaggio viene illustrato come registrare il server RADIUS su ME.

Passaggio 1. Aprire la GUI di ME e passare a **Wireless Settings (Impostazioni wireless) > WLAN > Add new WLAN (Aggiungi nuova WLAN)**.



Passaggio 2. Selezionare un nome per la WLAN.

Add New WLAN ✕

General **WLAN Security** VLAN & Firewall QoS

WLAN Id 3 ▼

Profile Name * me-ise|

SSID * me-ise

Admin State Enabled ▼

Radio Policy ALL ▼

✓ Apply ✕ Cancel

Passaggio 3. Specificare la configurazione di protezione nella scheda **Protezione WLAN**.

Scegliere **WPA2 Enterprise**, per il server di autenticazione scegliere **RAGGIO esterno**. Fare clic sull'opzione di modifica per aggiungere l'indirizzo IP del RADIUS e scegliere una chiave **segreta condivisa**.



Add New WLAN



General WLAN Security VLAN & Firewall QoS

Security WPA2 Enterprise ▼

Authentication Server External Radius ▼

	Radius IP ▲	Radius Port	Shared Secret	
		1812	*****	▲
		1812	*****	▼

External Radius configuration applies to all WLANs

Apply

Cancel

Add New WLAN

General WLAN Security VLAN & Firewall QoS

Security WPA2 Enterprise ▼

Authentication Server External Radius ▼

Radius IP ▲	Radius Port	Shared Secret
a.b.c.d	1812

ⓧ Please enter valid IPv4 address

External Radius configuration applies to all WLANs

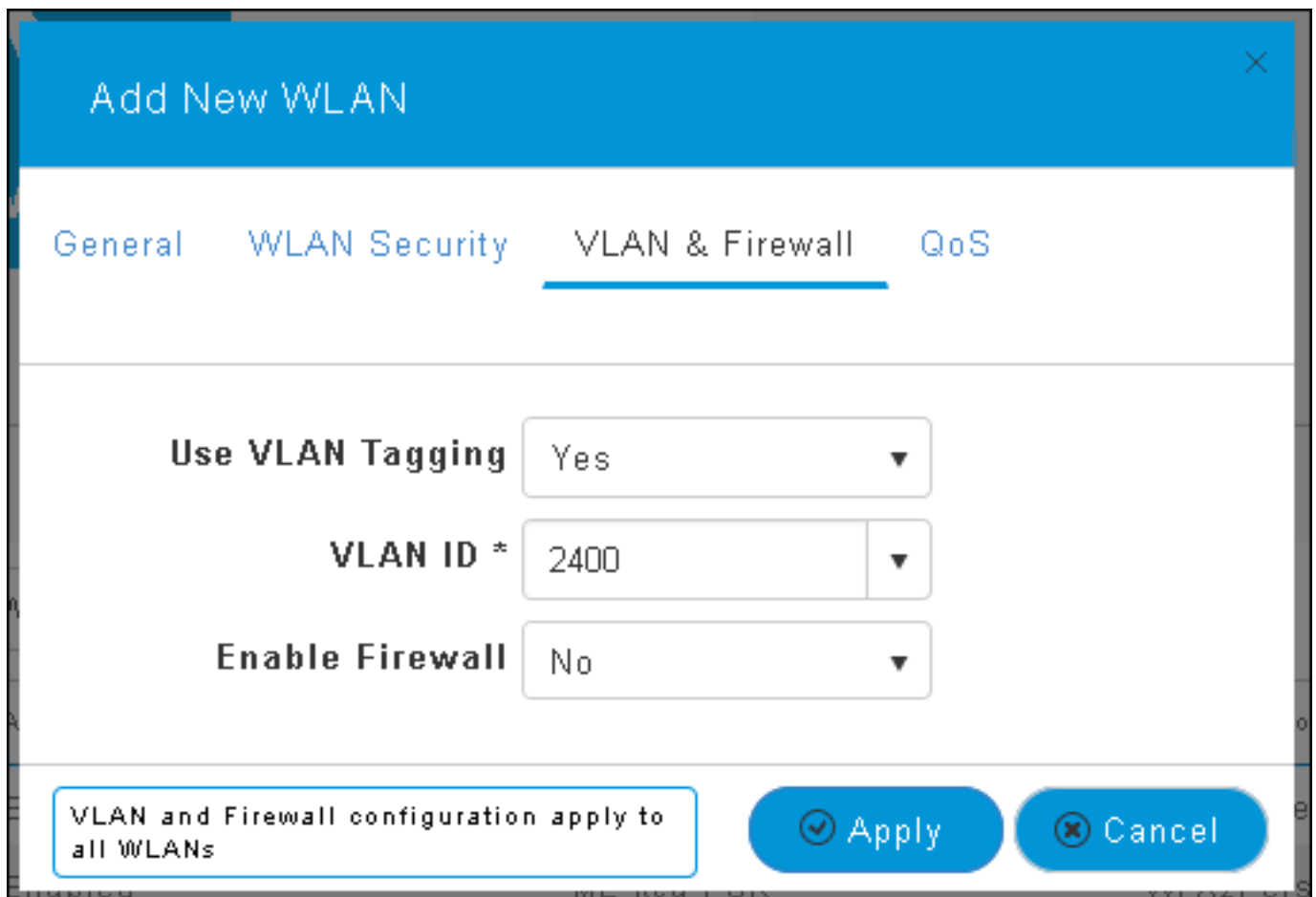
Apply Cancel

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

Passaggio 4. Assegnare una VLAN all'SSID.

Se l'SSID deve essere assegnato alla VLAN dell'access point, questo passaggio può essere ignorato.

Per assegnare gli utenti per questo SSID a una VLAN specifica (diversa dalla VLAN dell'access point), abilitare **Use VLAN Tagging** e assegnare l'**ID VLAN** desiderato.



Add New WLAN

General WLAN Security **VLAN & Firewall** QoS

Use VLAN Tagging Yes ▼

VLAN ID * 2400 ▼

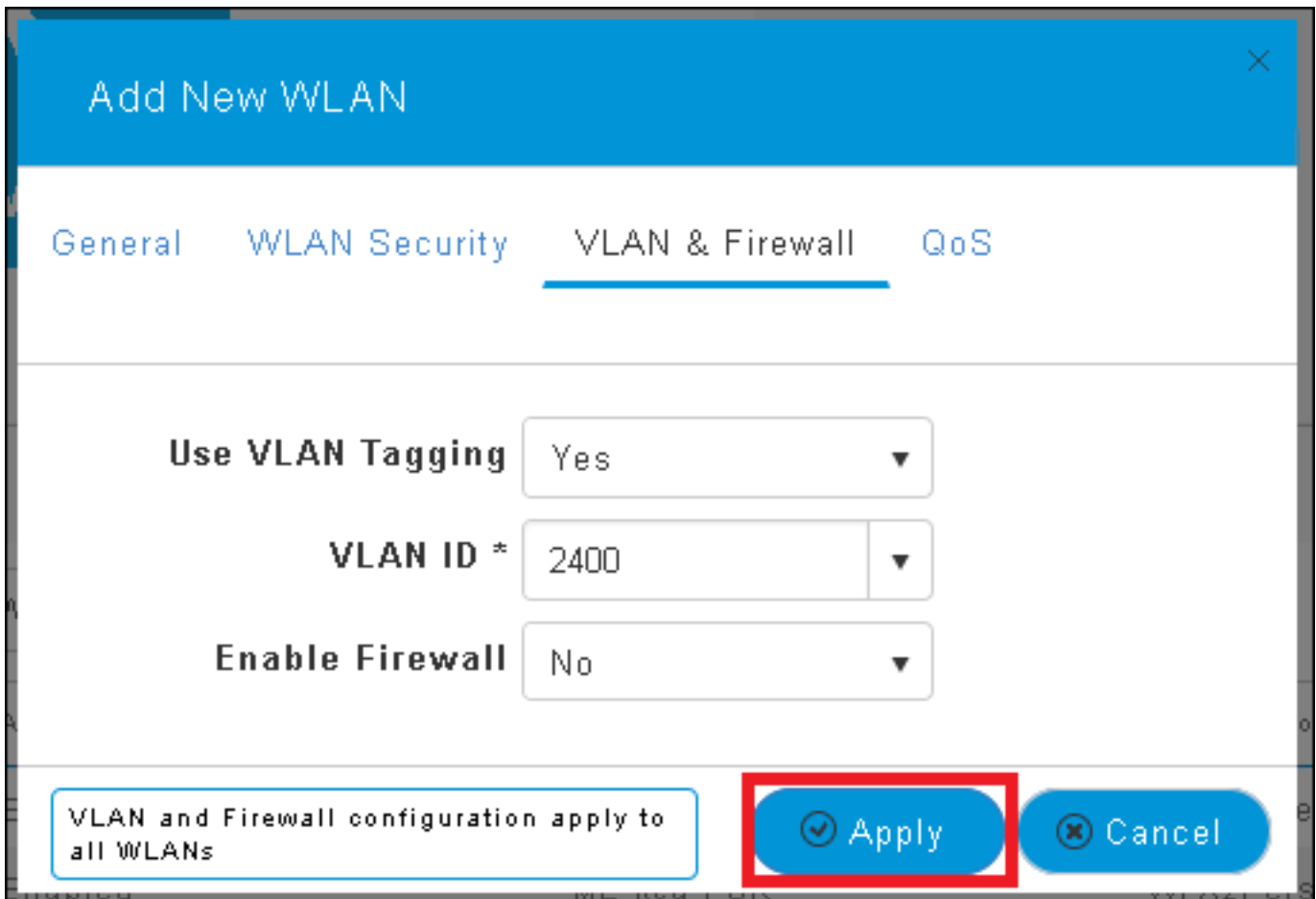
Enable Firewall No ▼

VLAN and Firewall configuration apply to all WLANs

Apply Cancel

Nota: Se si usa il tagging VLAN, verificare che la porta dello switch a cui è connesso il punto di accesso sia configurata come porta trunk e che la VLAN dell'access point sia configurata come nativa.

Passaggio 5. Fare clic su **Apply** (Applica) per completare la configurazione.



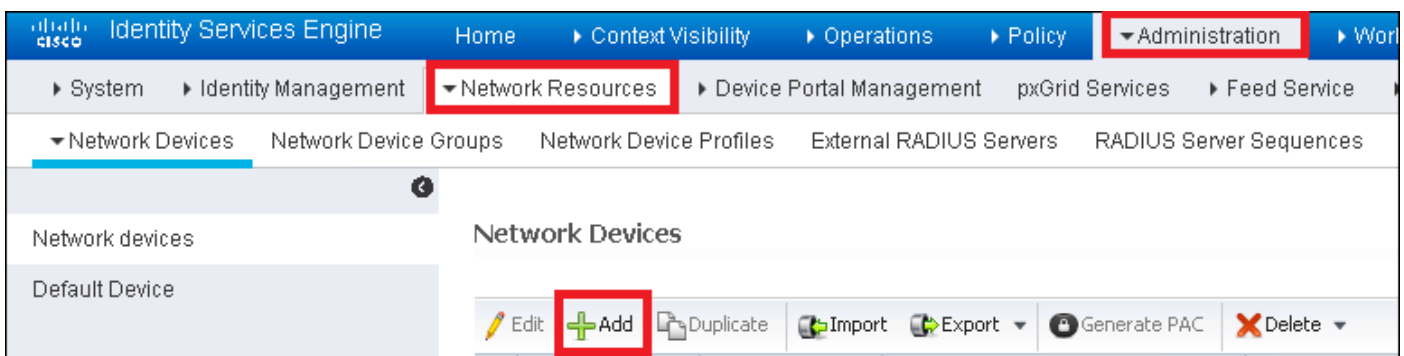
Passaggio 6. Facoltativo, configurare la WLAN in modo che accetti l'override della VLAN.

Abilitare l'override AAA sulla WLAN e aggiungere le VLAN necessarie. A tale scopo, è necessario aprire una sessione CLI sull'interfaccia di gestione ME ed eseguire i seguenti comandi:

```
>config wlan disable <wlan-id>  
>config wlan aaa-override enable <wlan-id>  
>config wlan enable <wlan-id>  
>config flexconnect group default-flexgroup vlan add <vlan-id>
```

Dichiaratemi ad ISE

Passaggio 1. Aprire la console ISE e selezionare **Amministrazione > Risorse di rete > Dispositivi di rete > Aggiungi**.



Passaggio 2. Immettere le informazioni.

Facoltativamente, è possibile specificare il nome del modello, la versione del software, la

descrizione e assegnare i gruppi di dispositivi di rete in base al tipo di dispositivo, alla posizione o ai WLC.

a.b.c.d corrisponde all'indirizzo IP dell'utente corrente.

Network Devices List > **New Network Device**

Network Devices

* Name

Description

* IP Address: /

* Device Profile

Model Name

Software Version

* Network Device Group

Device Type

Location

WLCs

RADIUS Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret

Enable KeyWrap

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

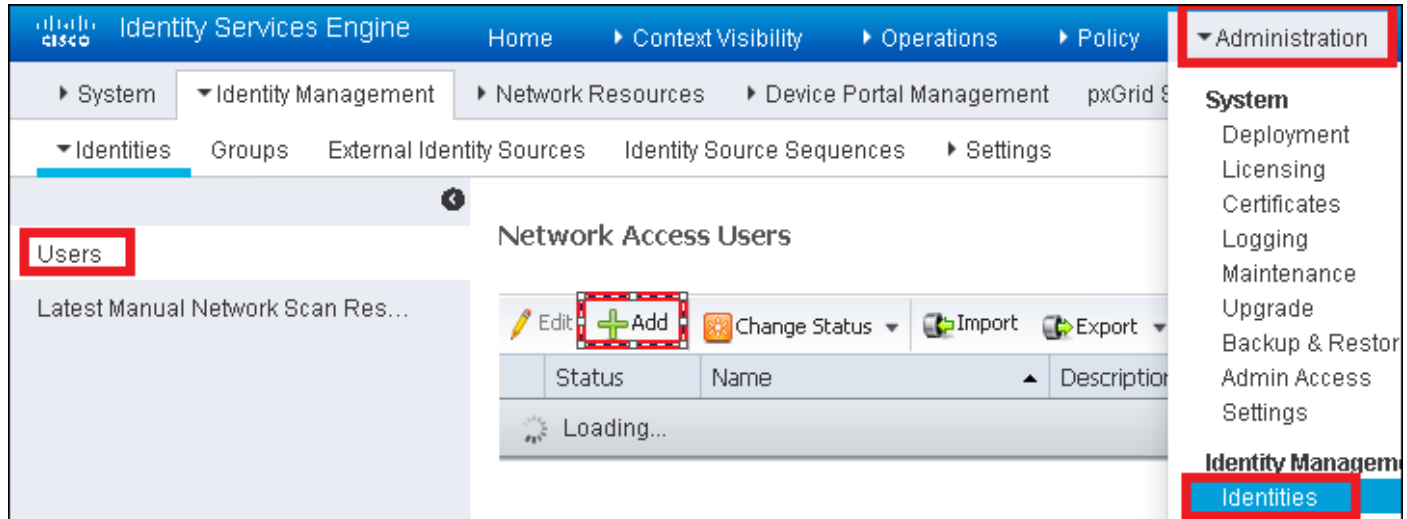
CoA Port

Per ulteriori informazioni sui gruppi di dispositivi di rete, vedere questo collegamento:

[ISE - Gruppi di dispositivi di rete](#)

Crea un nuovo utente su ISE

Passaggio 1. Passare a **Amministrazione > Gestione delle identità > Identità > Utenti > Aggiungi**.



Passaggio 2. Immettere le informazioni.

In questo esempio l'utente appartiene a un gruppo denominato ALL_ACCOUNTS ma può essere adeguato in base alle esigenze.

▼ **Network Access User**

* Name

Status Enabled ▼

Email

▼ **Passwords**

Password Type: ▼

Password

Re-Enter Passw

* Login Password

Enable Password

▼ **User Information**

First Name

Last Name

▼ **Account Options**

Description

Change password on next login

▼ **Account Disable Policy**

Disable account if date exceeds

▼ **User Groups**

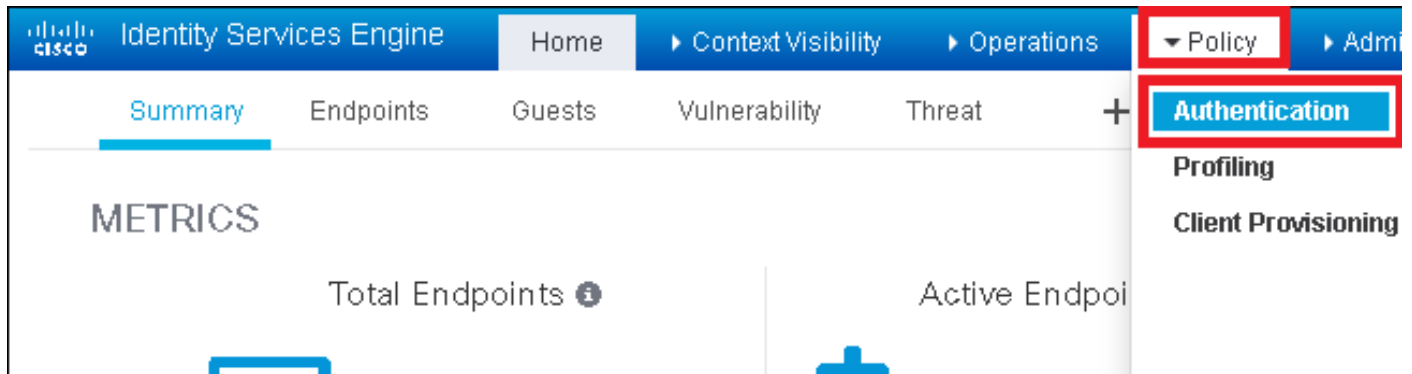
+

Creare la 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 a cui sono state assegnate, e

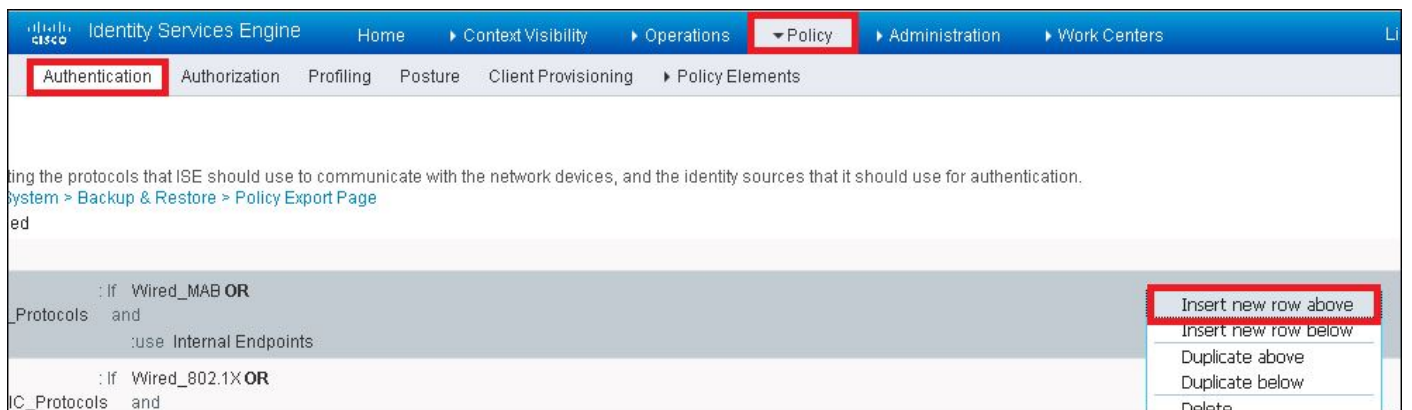
per limitare i metodi di autenticazione consentiti.

Passaggio 1. Naviga in **Criteri > Autenticazione**.



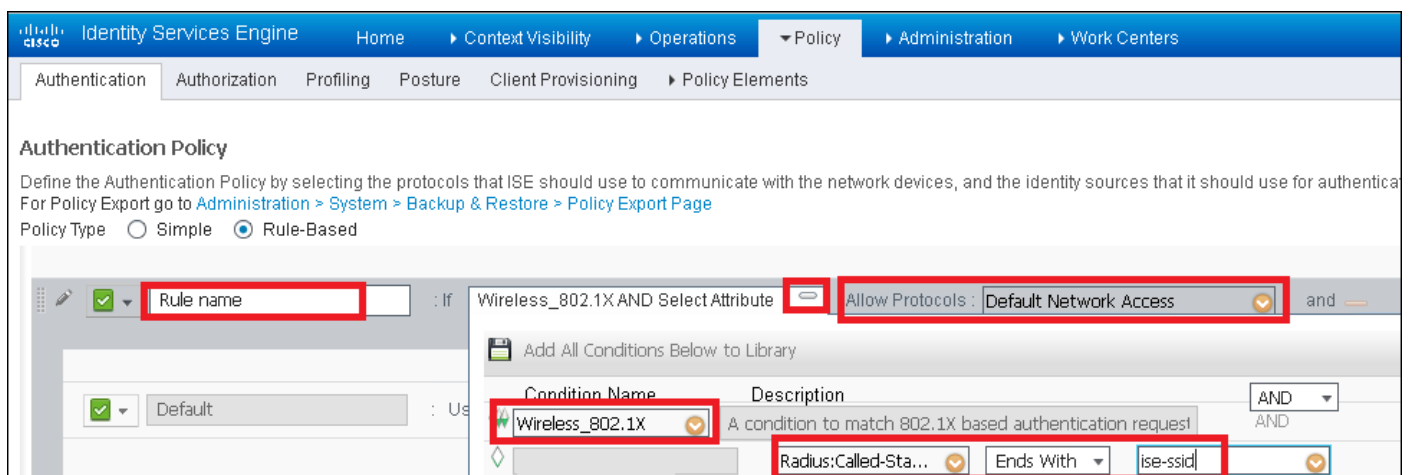
Passaggio 2. Inserire una nuova regola di autenticazione.

A tale scopo, passare a **Criterio > Autenticazione > Inserisci nuova riga sopra/sotto**.

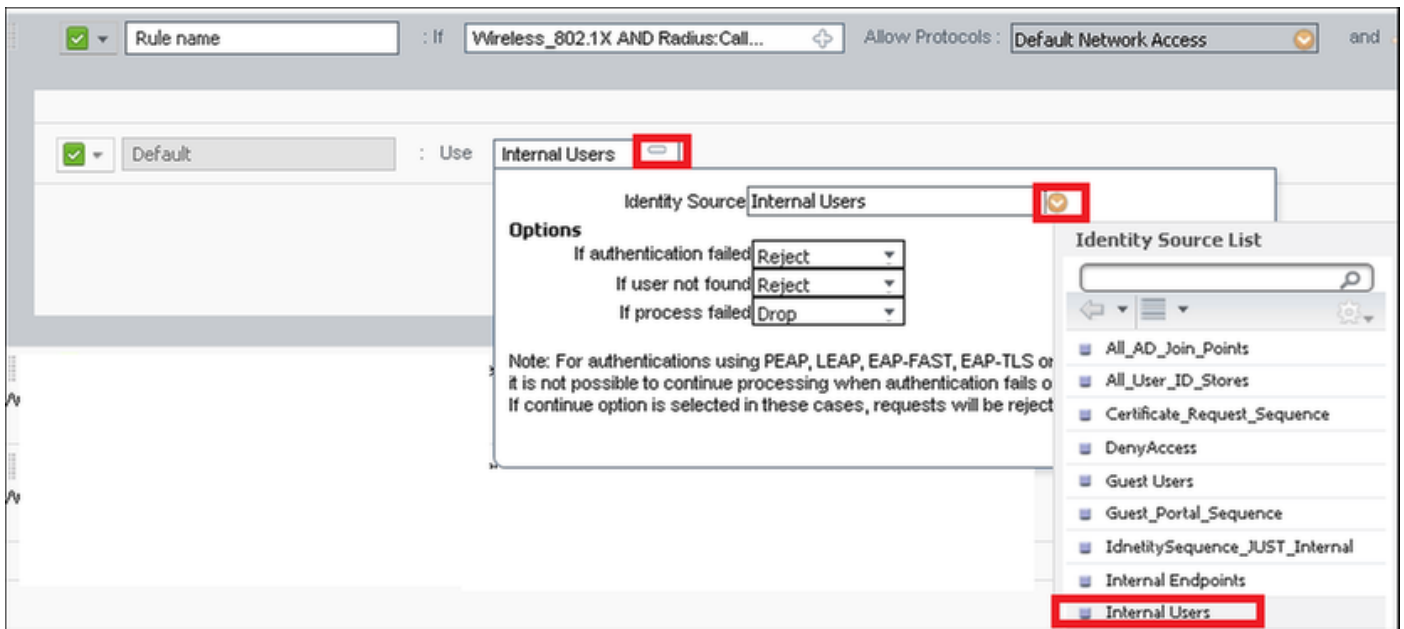


Passaggio 3. Inserire le informazioni necessarie

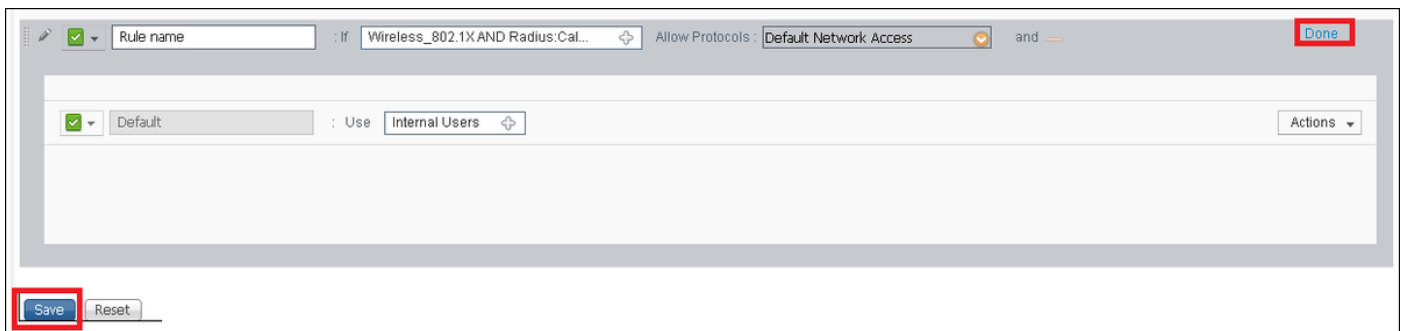
Questo esempio di regola di autenticazione consente di utilizzare tutti i protocolli elencati nell'elenco **Accesso alla rete predefinito**, applicabile alla richiesta di autenticazione per i client Wireless 802.1x e con ID stazione chiamata e terminante con *ise-ssid*.



Scegliere inoltre l'origine Identità per i client che soddisfano questa regola di autenticazione. In questo esempio viene utilizzato *Utenti interni*



Al termine, fate clic su **Fatto (Done)** e **Salva (Save)**



Per ulteriori informazioni su Consenti criteri protocolli, vedere questo collegamento:

[Servizio Protocolli consentiti](#)

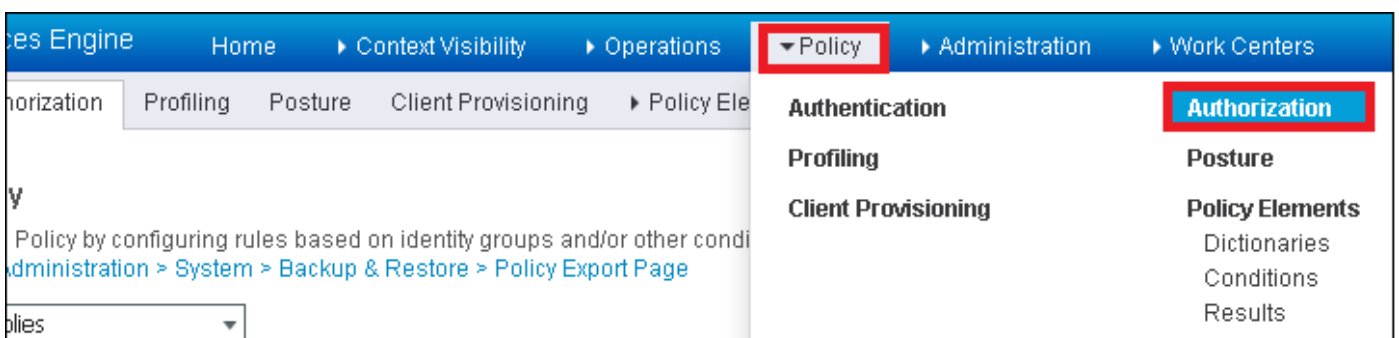
Per ulteriori informazioni sulle origini di identità, vedere questo collegamento:

[Crea un gruppo di identità utente](#)

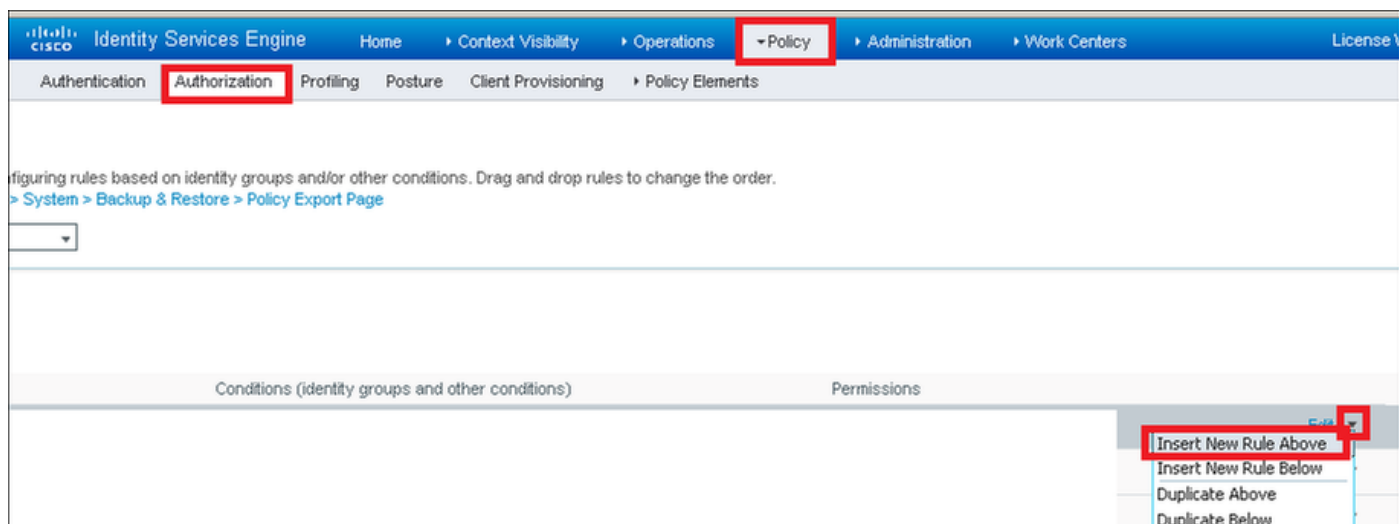
Creare la regola di autorizzazione

La regola di autorizzazione è quella incaricata di determinare se al client è consentito o meno connettersi alla rete

Passaggio 1. Passare a **Criterio > Autorizzazione**.

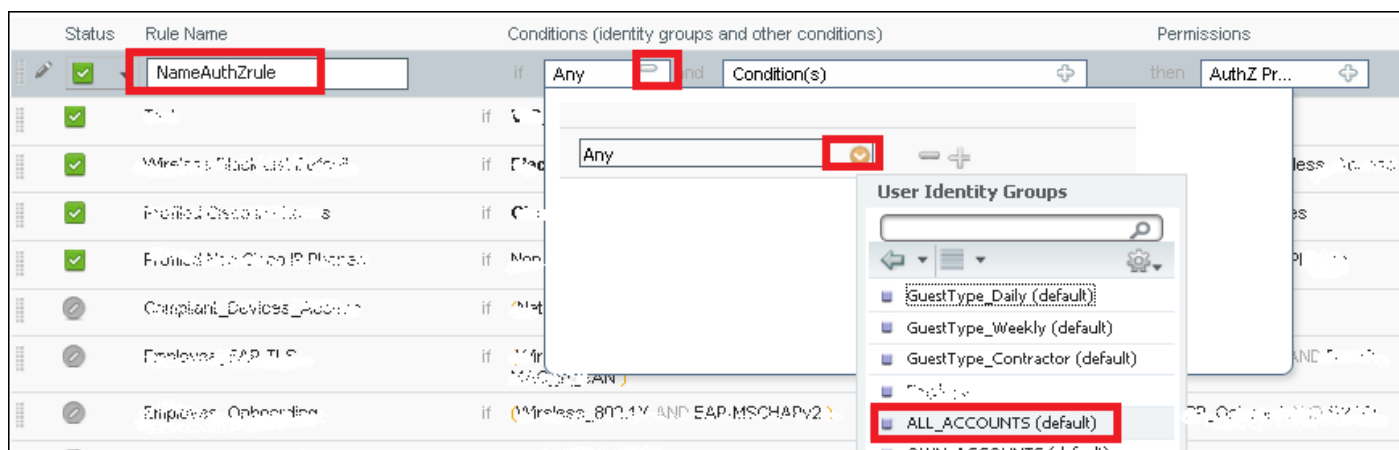


Passaggio 2. Inserire una nuova regola. Passare a **Criterio > Autorizzazione > Inserisci nuova regola sopra/sotto**.

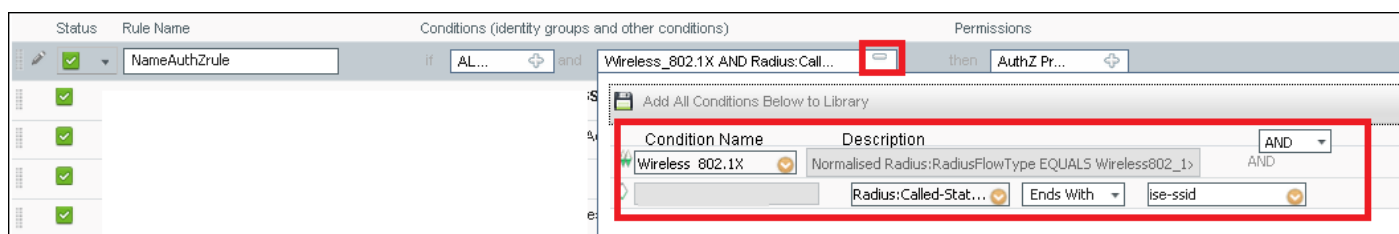


Passaggio 3. Immettere le informazioni.

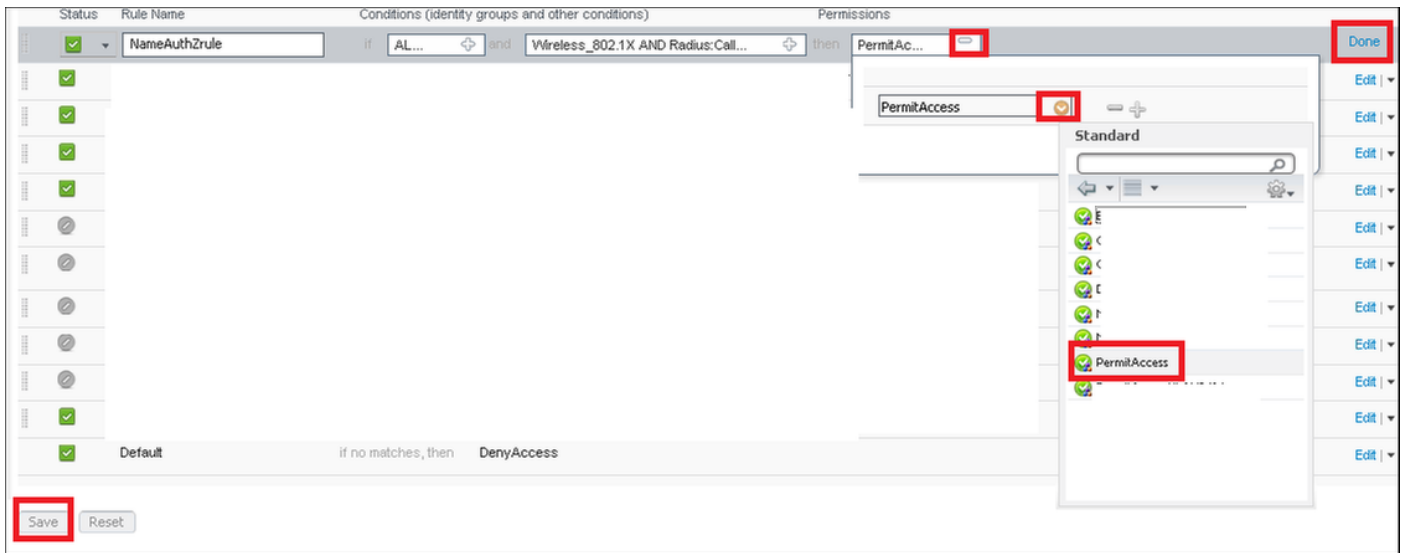
Scegliere innanzitutto un nome per la regola e i gruppi di identità in cui è memorizzato l'utente. In questo esempio l'utente è memorizzato nel gruppo **ALL_ACCOUNTS**.



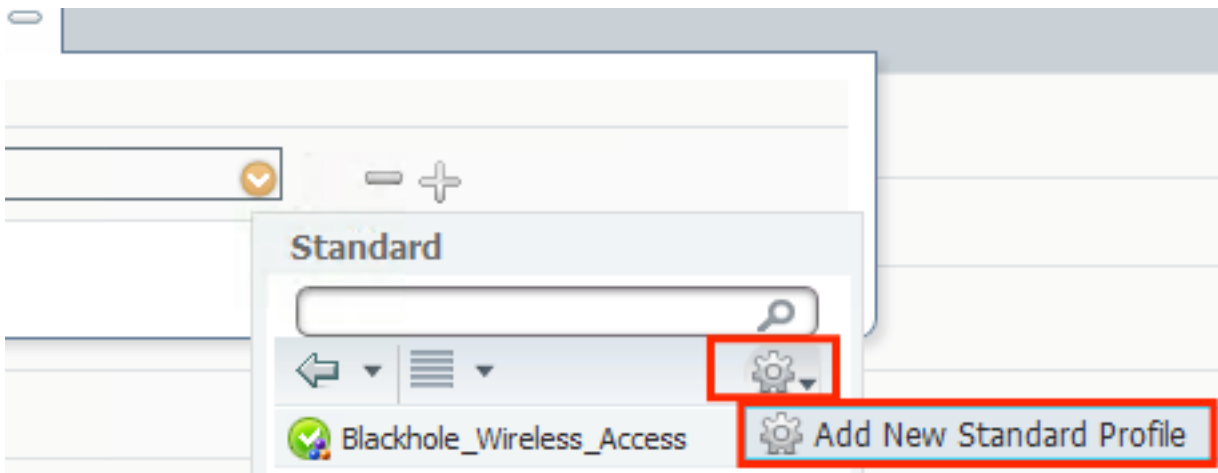
In seguito scegliere altre condizioni che fanno rientrare il processo di autorizzazione in questa regola. In questo esempio il processo di autorizzazione rileva questa regola se utilizza una connessione wireless 802.1x e viene chiamato ID stazione e termina con *ise-ssid*.



Infine, scegliere il profilo di autorizzazione che consente ai clienti di connettersi alla rete, fare clic su **Fine** e **Salva**.



Facoltativamente, creare un nuovo profilo di autorizzazione che assegni il client wireless a una VLAN diversa:



Immettere le informazioni:

Add New Standard Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

DAACL Name

ACL (Filter-ID)

VLAN Tag ID IDName

Voice Domain Permission

Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:vlan-id
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6

Configurazione del dispositivo terminale

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

In questo esempio di configurazione, ISE utilizza il proprio certificato autofirmato per eseguire l'autenticazione.

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

1. Installa il certificato autofirmato nel computer per convalidare e considerare attendibile il server ISE per completare l'autenticazione
2. Ignora la convalida del server RADIUS e considera 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 - Installa certificato autofirmato ISE

Passaggio 1. Esportare il certificato autofirmato da ISE.

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

Selezionare quindi il certificato utilizzato per l'autenticazione **EAP** e fare clic su **Esporta**.

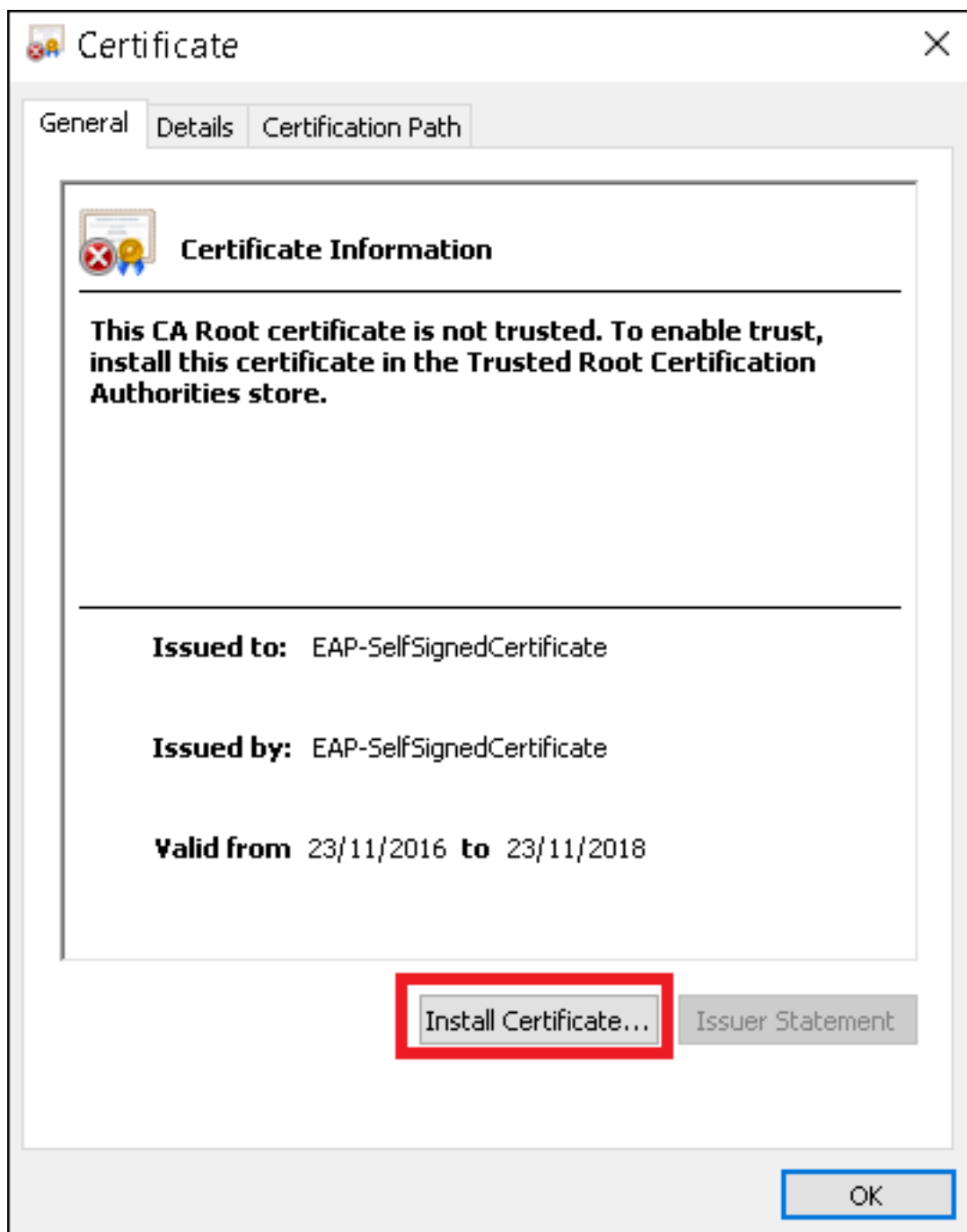
The screenshot shows the Cisco Identity Services Engine Administration interface. The navigation menu includes 'Administration' (highlighted), 'System' (highlighted), and 'Certificates' (highlighted). The main content area is titled 'System Certificates' and includes a warning: 'For disaster recovery it is recommended to export certificate ar'. Below this are buttons for 'Edit', 'Generate Self Signed Certificate', 'Import', 'Export' (highlighted), and 'Delete'. A table below lists certificates with columns for 'Friendly Name', 'Used By', and 'Portal group tag'. One certificate is selected and highlighted: 'EAP-SelfSignedCertificate#EAP Authentication'.

Salvare il certificato nella posizione desiderata. Il certificato è installato nel computer Windows.

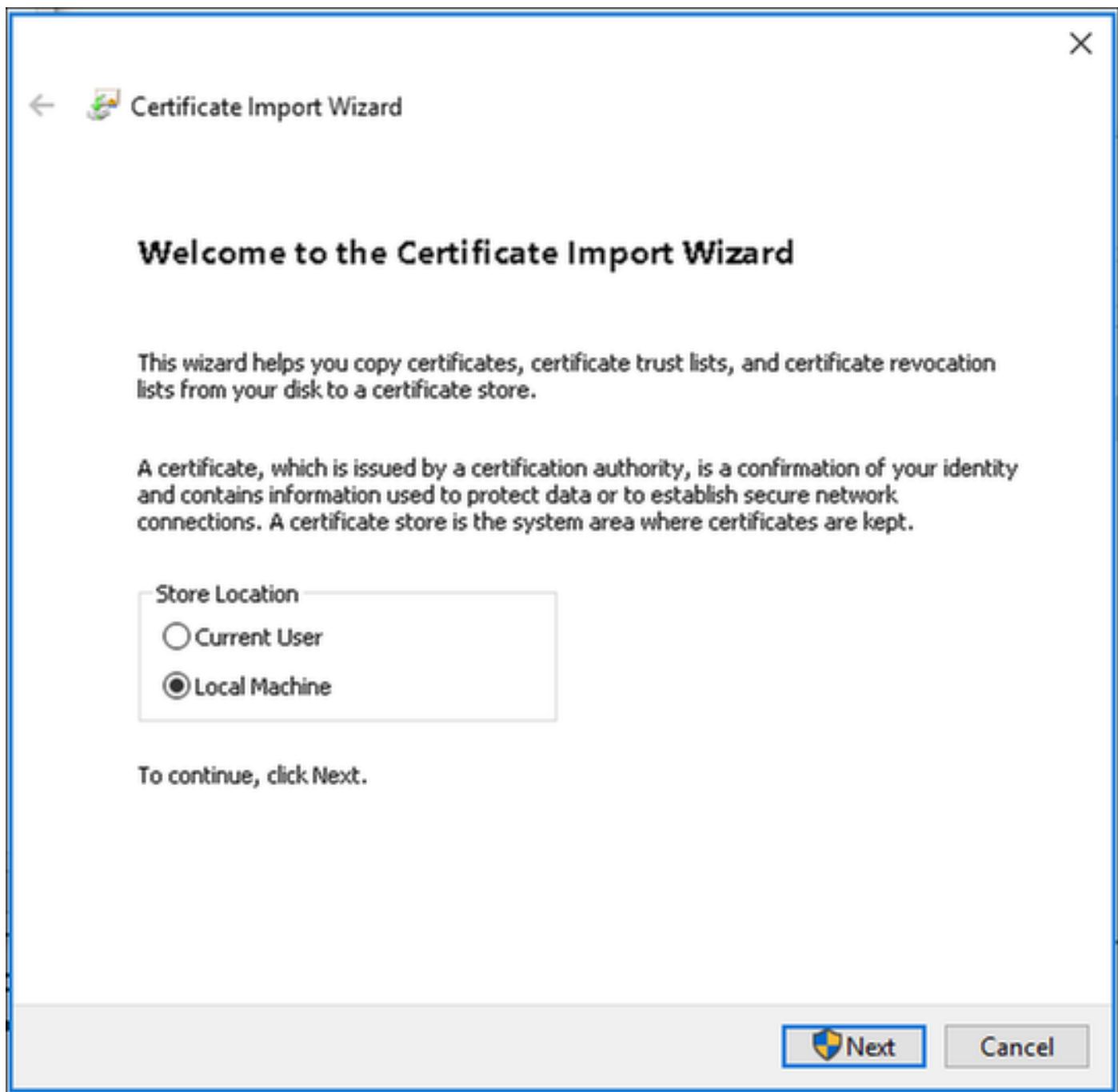
The screenshot shows the 'Export Certificate' dialog box. The title is 'Export Certificate 'EAP-SelfSignedCertificate#EAP-SelfSignedCertificate#00001''. There are two radio buttons: 'Export Certificate Only' (selected and highlighted) and 'Export Certificate and Private Key'. Below these are input fields for '*Private Key Password' and '*Confirm Password'. A warning message is displayed: 'Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.' The 'Export' button is highlighted.

Passaggio 2. Installare il certificato nel computer Windows.

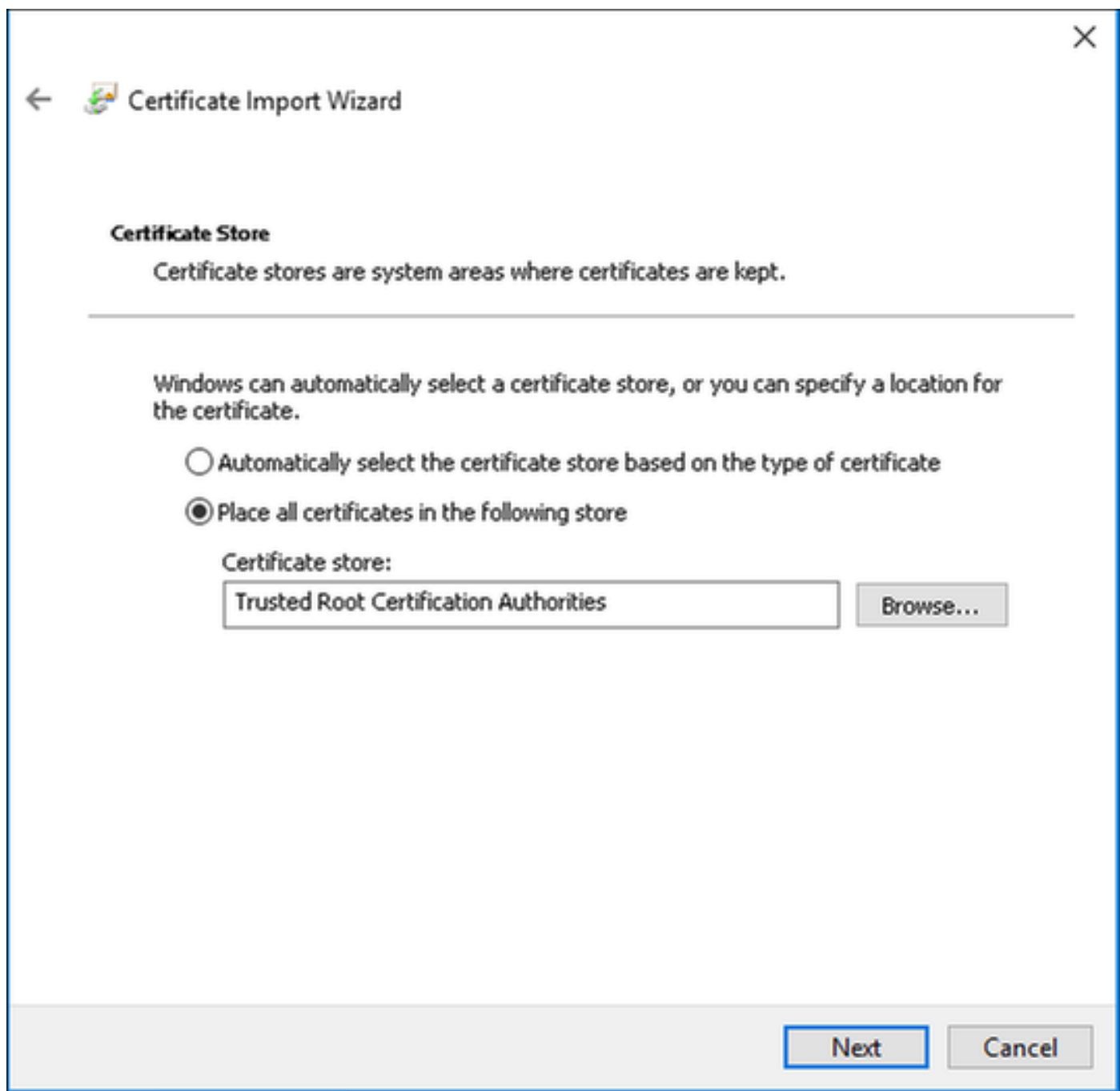
Copiare il certificato esportato in precedenza nel computer Windows, modificare l'estensione del file da .pem a .crt, dopo che il doppio clic su di esso e selezionare **Installa certificato....**



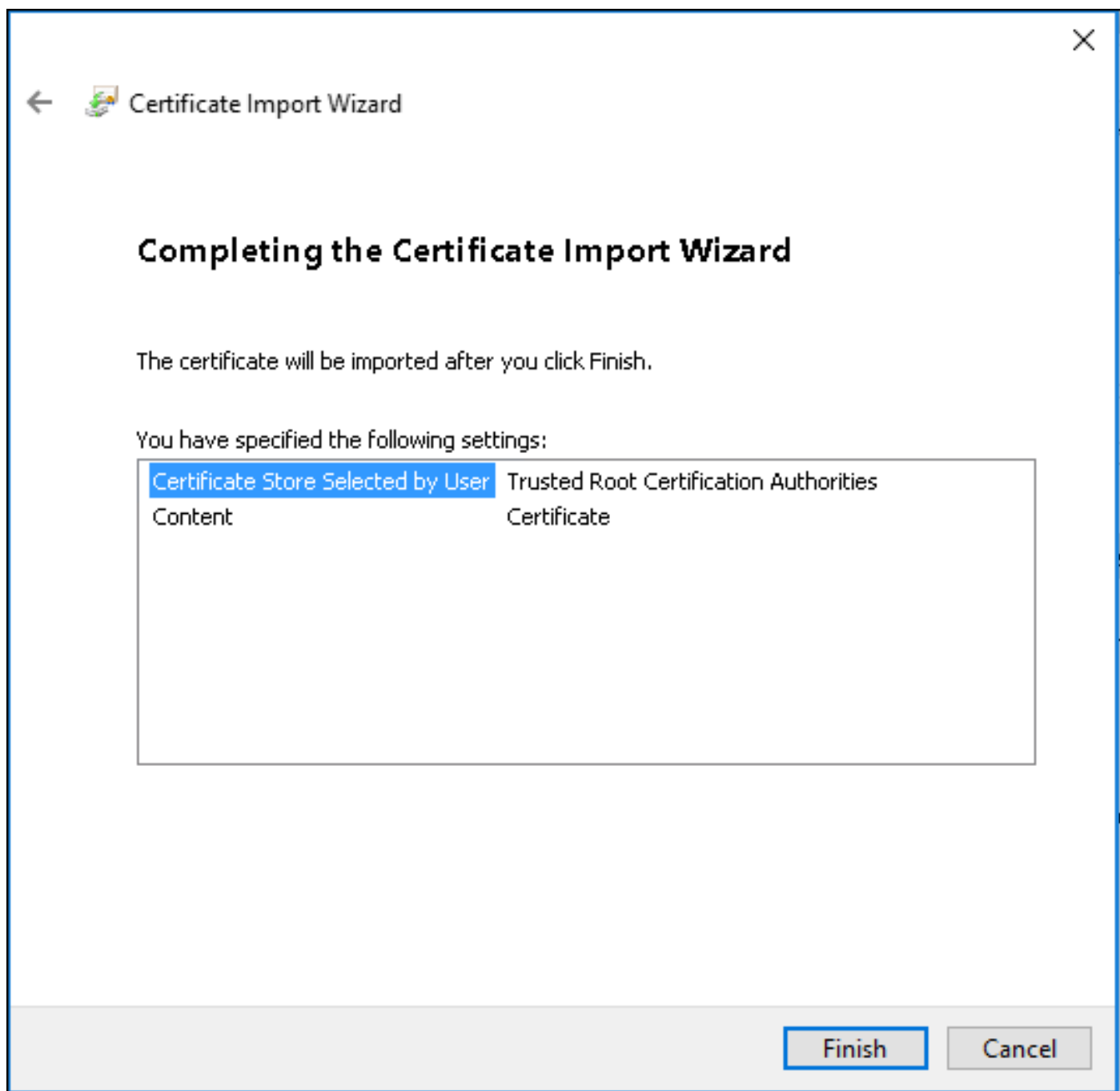
Scegliere di installarlo nel **computer locale**, quindi fare clic su **Avanti**.



Selezionare **Colloca tutti i certificati nel seguente archivio**, quindi individuare e scegliere **Autorità di certificazione radice attendibili**. Quindi, fare clic su Next (Avanti).



Quindi fare clic su **Fine**.



Alla fine fare clic su **Sì** per confermare l'installazione del certificato.

Security Warning



You are about to install a certificate from a certification authority (CA) claiming to represent:

EAP-SelfSignedCertificate

Windows cannot validate that the certificate is actually from "EAP-SelfSignedCertificate". You should confirm its origin by contacting "EAP-SelfSignedCertificate". The following number will assist you in this process:

Thumbprint (sha1): 011A193D 700E713D 0204E3D0 4759215D
4294213C

Warning:

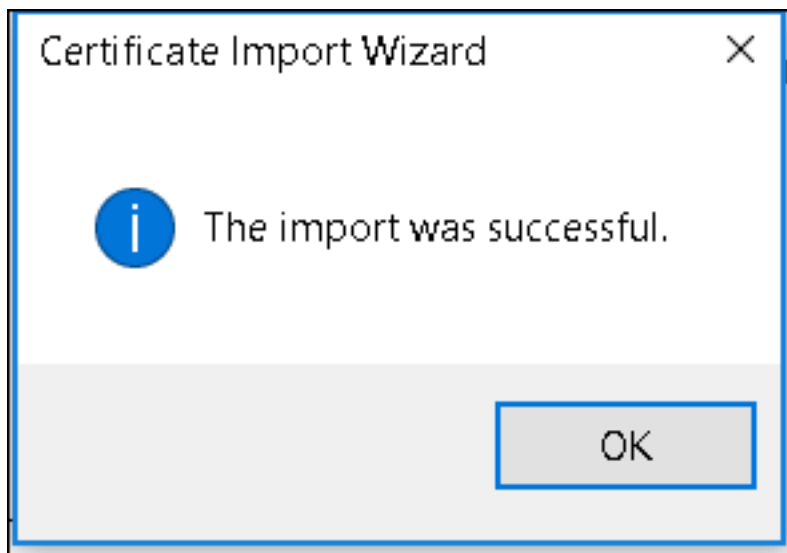
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Yes

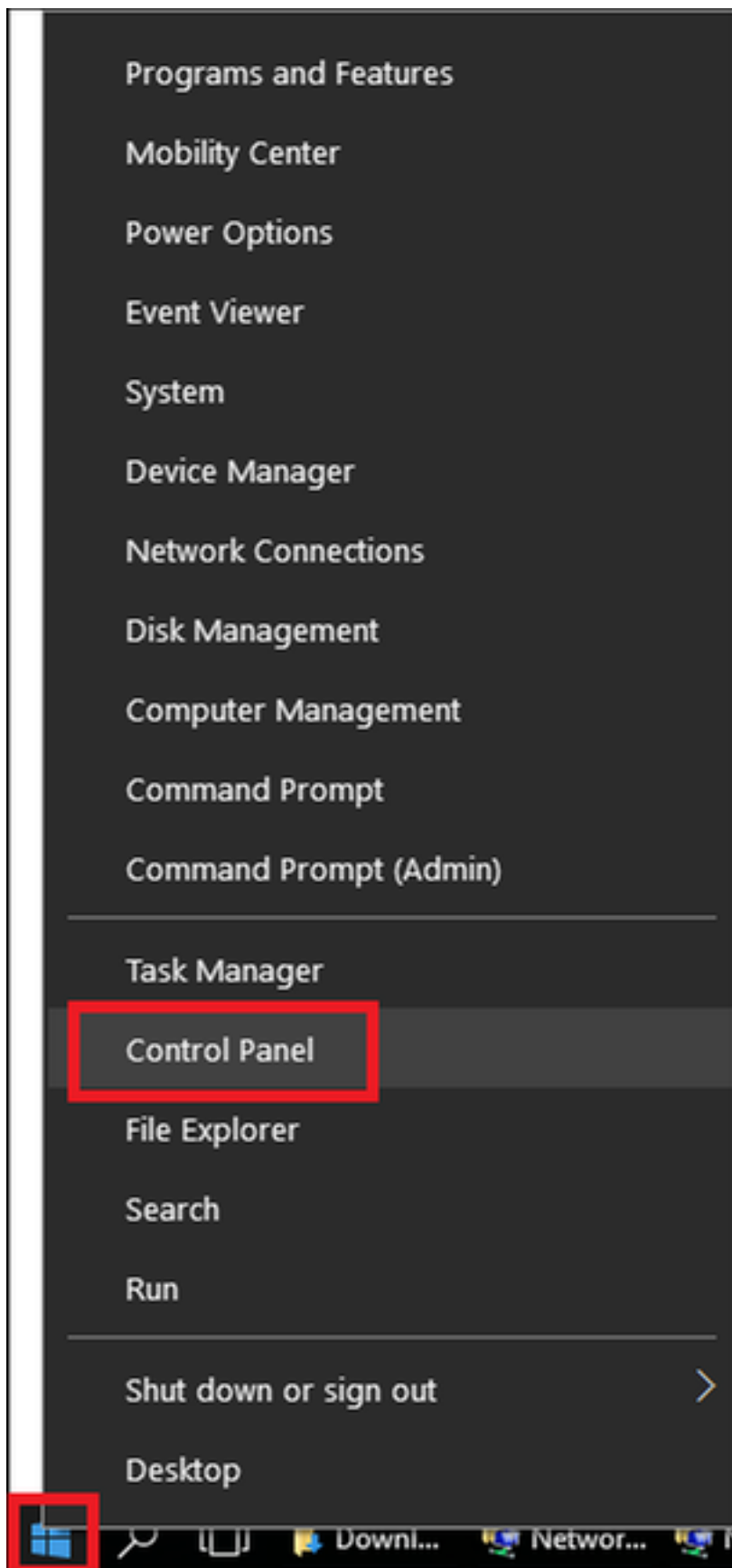
No

Infine fare clic su **OK**.

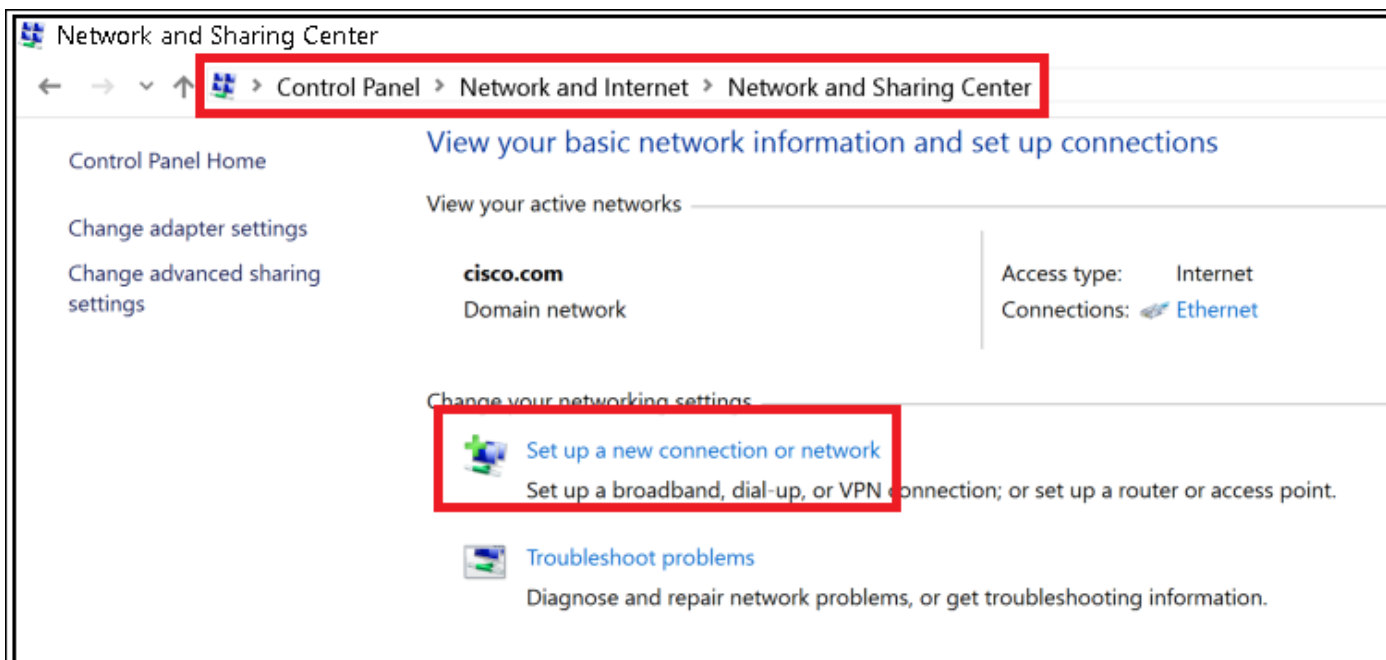


Fine configurazione dispositivo - Creazione del profilo WLAN

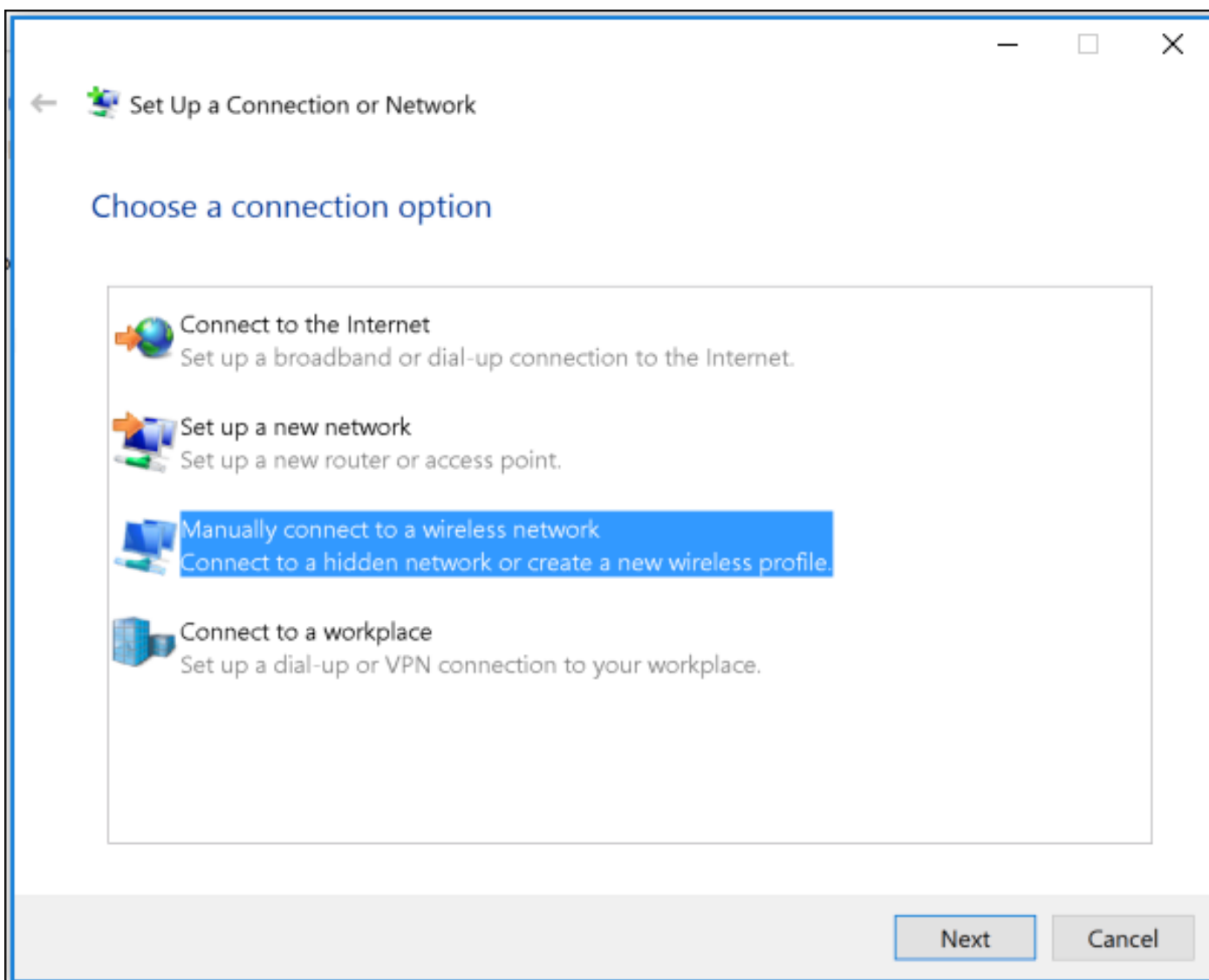
Passaggio 1. Fare clic con il pulsante destro del mouse sull'icona **Start** e selezionare **Pannello di controllo**.



Passaggio 2. Passare a **Rete e Internet**, quindi a **Centro connessioni di rete e condivisione** e fare clic su **Configura nuova connessione o rete**.



Passaggio 3. Selezionare **Connetti manualmente a una rete wireless** e fare clic su **Avanti**.



Passaggio 4. Immettere le informazioni con il nome del SSID e il tipo di protezione WPA2-Enterprise e fare clic su **Avanti**.

← Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name:

Security type:

Encryption type:

Security Key: Hide characters

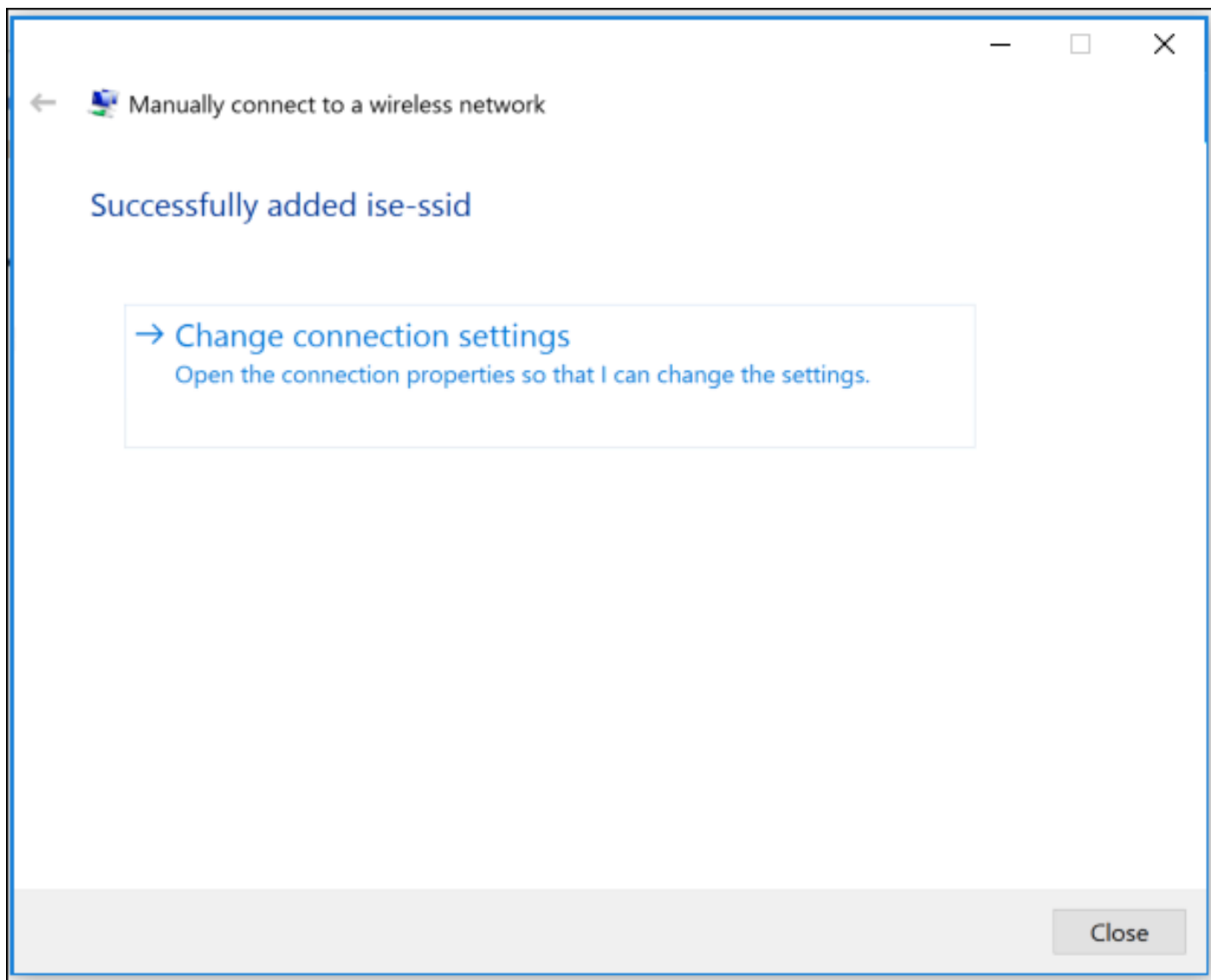
Start this connection automatically

Connect even if the network is not broadcasting

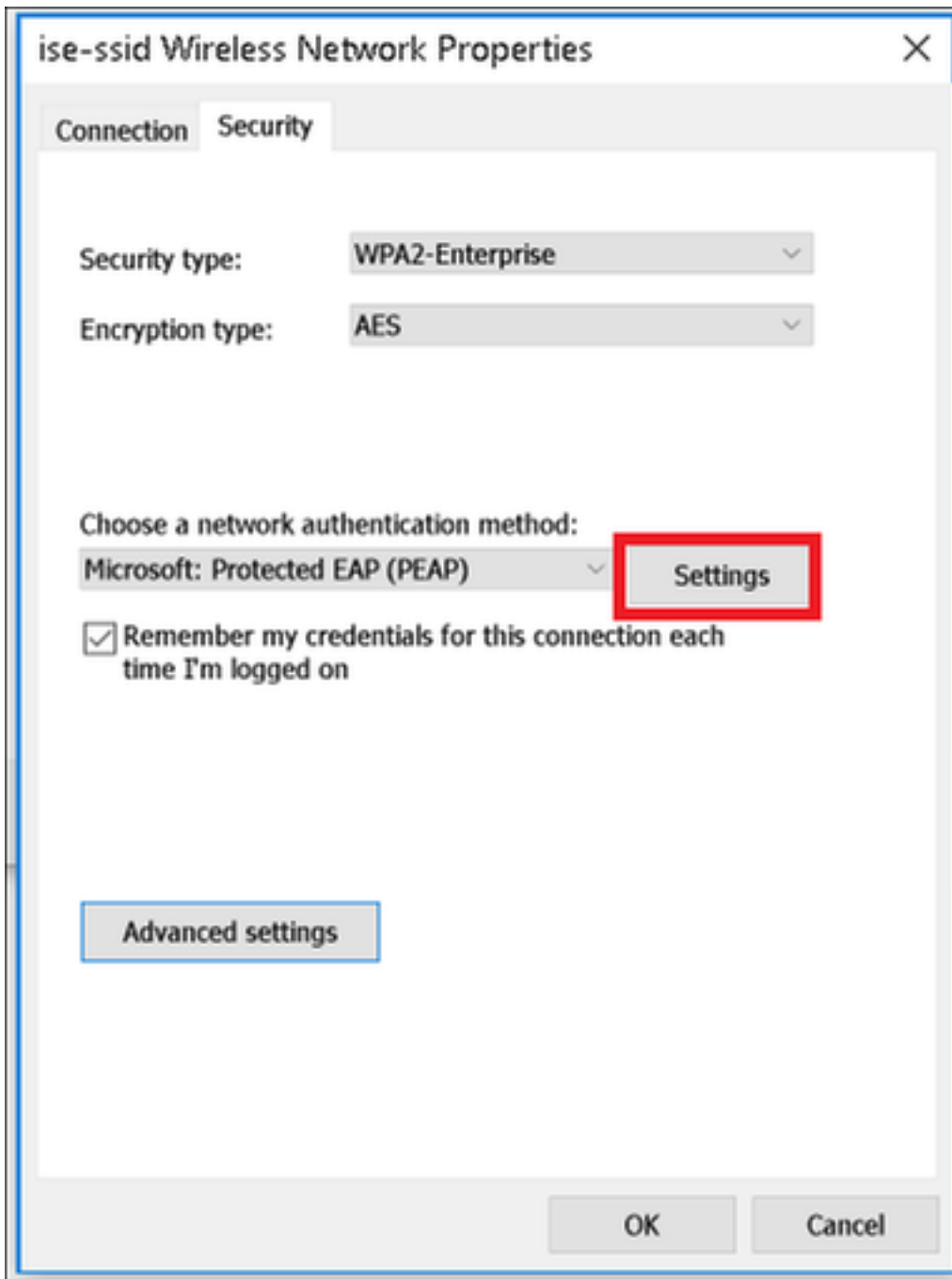
Warning: If you select this option, your computer's privacy might be at risk.

Next Cancel

Passaggio 5. Selezionare **Change connection settings** per personalizzare la configurazione del profilo WLAN.



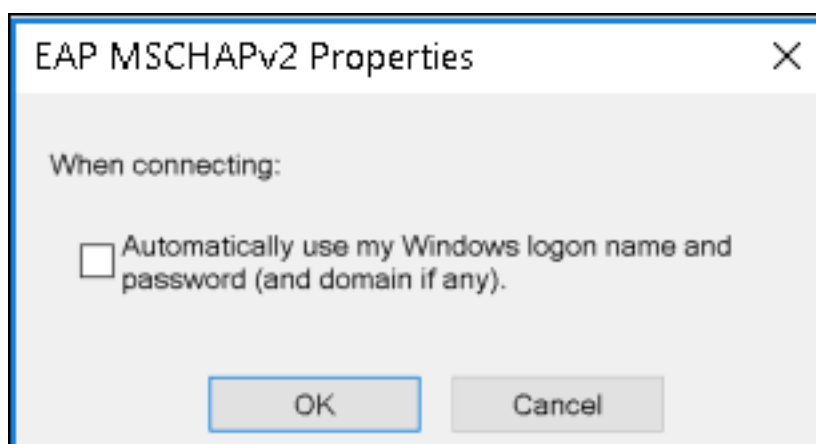
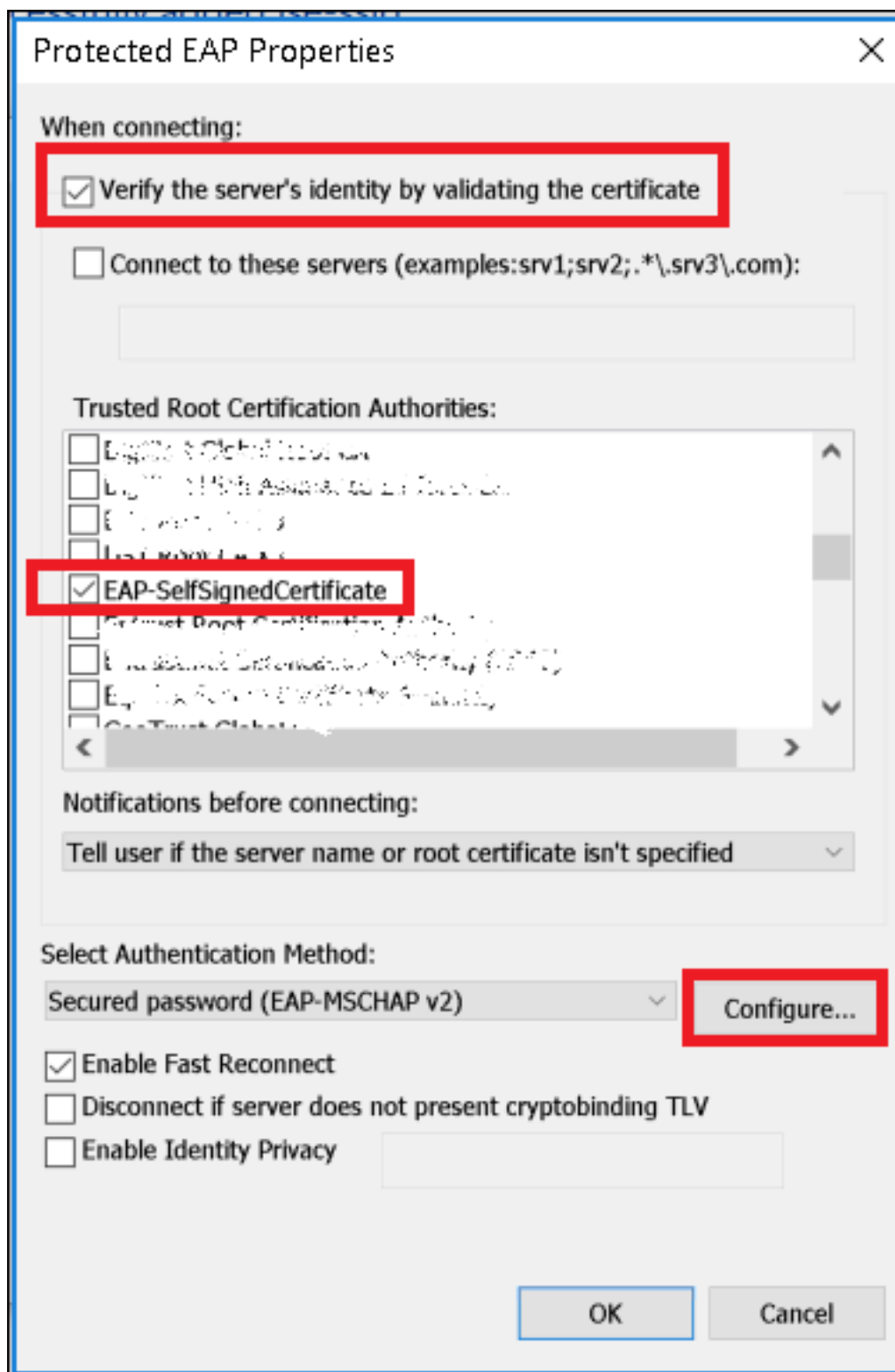
Passaggio 6. Passare alla scheda **Protezione** e fare clic su **Impostazioni**.



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

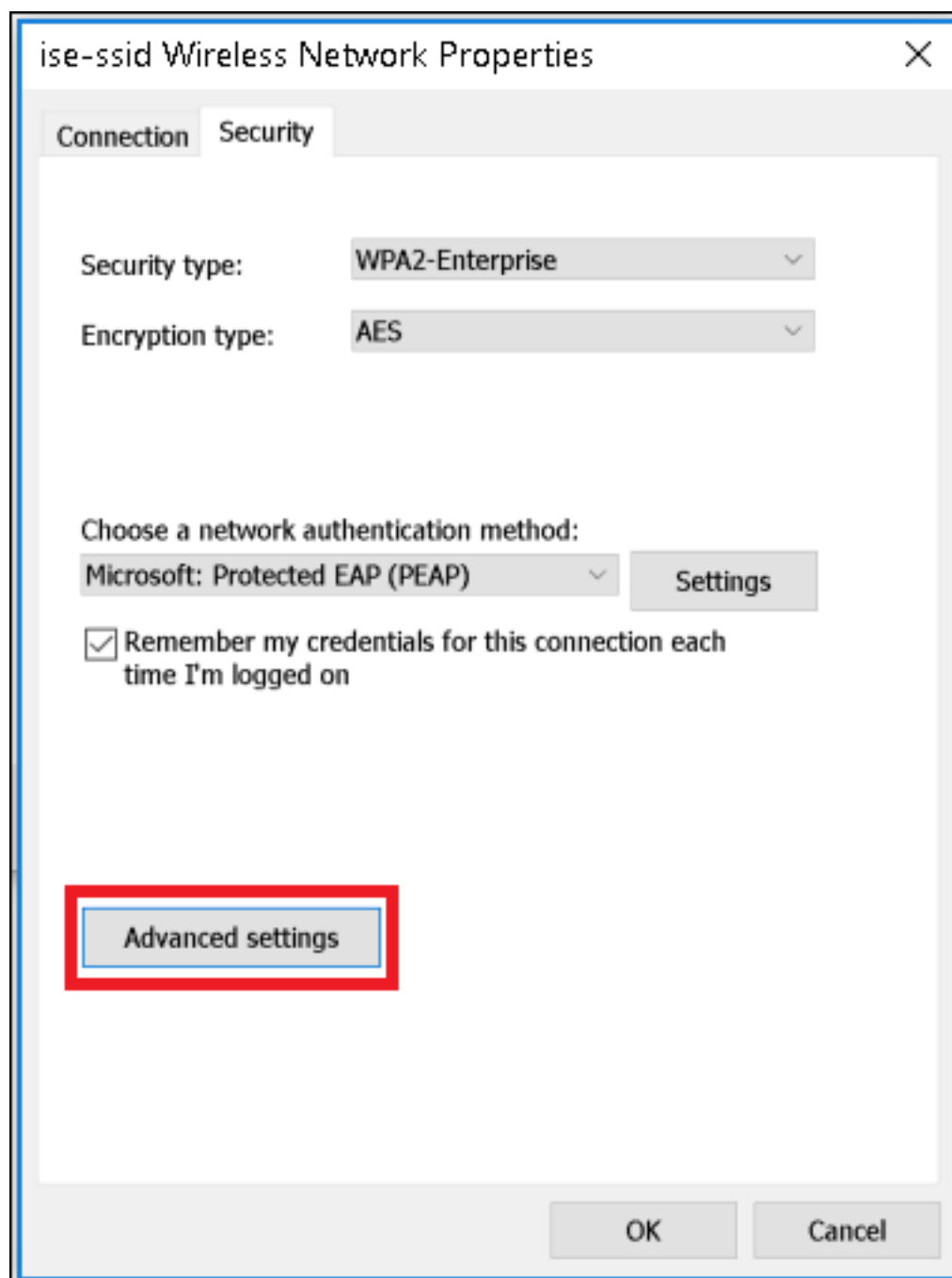
In caso affermativo, abilitare **Verifica dell'identità del server convalidando il certificato** e dall'elenco **Autorità di certificazione fonti attendibili** selezionare il certificato autofirmato ISE.

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



Passaggio 8. Configurare le credenziali utente

Una volta tornati 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.



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):

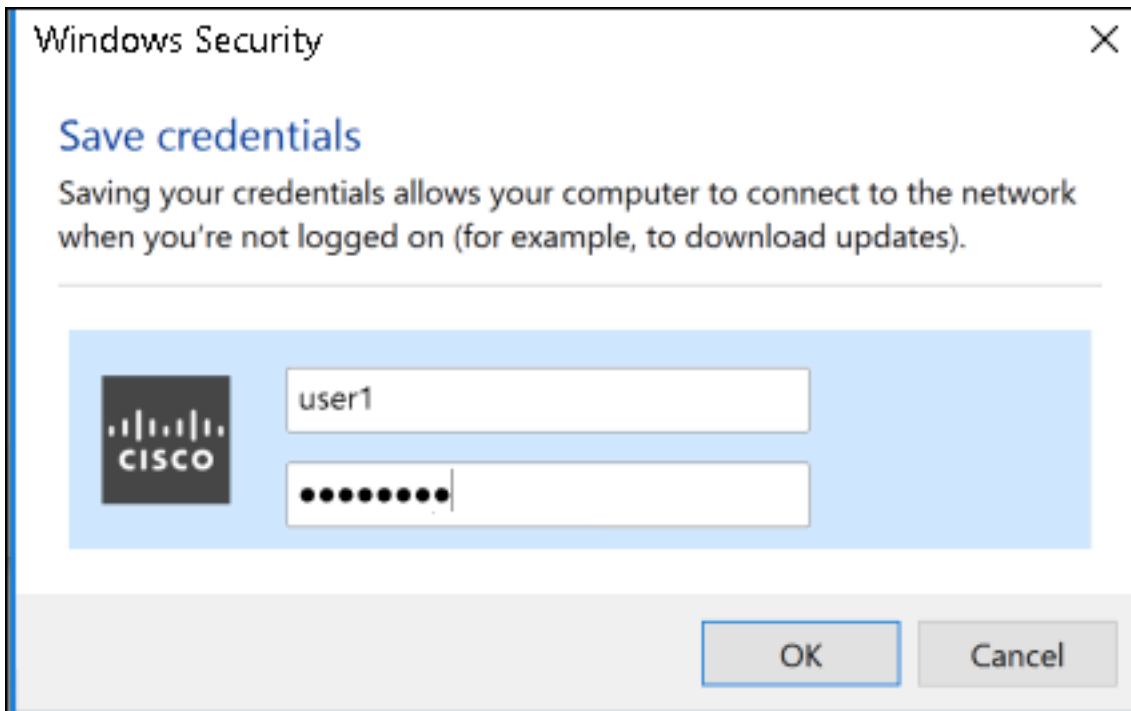
10

Allow additional dialogs to be displayed during single sign on

This network uses separate virtual LANs for machine and user authentication

OK

Cancel



Verifica

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

Processo di autenticazione in ME

Eseguire questo comando per monitorare il processo di autenticazione per un utente specifico:

```
> debug client <mac-add-client>
```

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

```
*apfMsConnTask_0: Nov 25 16:36:24.333: 08:74:02:77:13:45 Processing assoc-req
station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 thread:669ba80
*apfMsConnTask_0: Nov 25 16:36:24.333: 08:74:02:77:13:45 Association received from mobile on
BSSID 38:ed:18:c6:7b:4d AP 1852-4
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying site-specific Local Bridging
override for station 08:74:02:77:13:45 - vapId 3, site 'FlexGroup', interface 'management'
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying Local Bridging Interface
Policy for station 08:74:02:77:13:45 - vlan 0, interface id 0, interface 'management'
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Set Clinet Non AP specific
apfMsAccessVlan = 2400
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 This apfMsAccessVlan may be changed
later from AAA after L2 Auth
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Received 802.11i 802.1X key management
suite, enabling dot1x Authentication
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 START (0) Change state to
AUTHCHECK (2) last state START (0)
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 AUTHCHECK (2) Change state to
8021X_REQD (3) last state AUTHCHECK (2)
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 8021X_REQD (3) DHCP required on
```

AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this client

*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 apfPemAddUser2:session timeout forstation 08:74:02:77:13:45 - Session Tout 0, apfMsTimeOut '0' and sessionTimerRunning flag is 0

*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Stopping deletion of Mobile Station: (callerId: 48)

*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Func: apfPemAddUser2, Ms Timeout = 0, Session Timeout = 0

*apfMsConnTask_0: Nov 25 16:36:24.335: **08:74:02:77:13:45 Sending assoc-resp with status 0 station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 on apVapId 3**

*apfMsConnTask_0: Nov 25 16:36:24.335: **08:74:02:77:13:45 Sending Assoc Response to station on BSSID 38:ed:18:c6:7b:4d (status 0) ApVapId 3 Slot 1**

*spamApTask0: Nov 25 16:36:24.341: 08:74:02:77:13:45 Sent dot1x auth initiate message for mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 reauth_sm state transition 0 ---> 1 for mobile 08:74:02:77:13:45 at 1x_reauth_sm.c:47

*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 EAP-PARAM Debug - eap-params for Wlan-Id :3 is disabled - applying Global eap timers and retries

*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Disable re-auth, use PMK lifetime.

*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting dot1x reauth timeout = 1800

*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 dot1x - moving mobile 08:74:02:77:13:45 into Connecting state

*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: **08:74:02:77:13:45 Sending EAP-Request/Identity to mobile 08:74:02:77:13:45 (EAP Id 1)**

*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.401: **08:74:02:77:13:45 Received EAPOL EAPPKT from mobile 08:74:02:77:13:45**

*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.401: **08:74:02:77:13:45 Received Identity Response (count=1) from mobile 08:74:02:77:13:45**

.

.

.

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: **08:74:02:77:13:45 Processing Access-Accept for mobile 08:74:02:77:13:45**

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: **08:74:02:77:13:45 Username entry (user1) created in mscb for mobile, length = 253**

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting dot1x reauth timeout = 1800

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Creating a PKC PMKID Cache entry for station 08:74:02:77:13:45 (RSN 2)

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding BSSID 38:ed:18:c6:7b:4d to PMKID cache at index 0 for station 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: New PMKID: (16)

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding Audit session ID payload in Mobility handoff

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 0 PMK-update groupcast messages sent

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 PMK sent to mobility group

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Disabling re-auth since PMK lifetime can take care of same.

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Sending EAP-Success to mobile 08:74:02:77:13:45 (EAP Id 70)

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Freeing AAACB from Dot1xCB as AAA auth is done for mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID 38:ed:18:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID 38:ed:18:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: Including PMKID in M1 (16)

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: M1 - Key Data: (22)

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] dd 14 00 0f ac 04 80 3a 20 8c 8f c2 4c 18 7d 4c

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0016] 28 e7 7f 10 11 03

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: **08:74:02:77:13:45 Starting key exchange to mobile**

08:74:02:77:13:45, data packets will be dropped

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Sending EAPOL-Key Message to mobile

08:74:02:77:13:45

state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt for retransmission to mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Entering Backend Auth Success state (id=70) for mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Received Auth Success while in Authenticating state for mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 dot1x - moving mobile 08:74:02:77:13:45 into Authenticated state

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received EAPOL-Key from mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received EAPOL-key in PTK_START state (message 2) from mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Successfully computed PTK from PMK!!!

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received valid MIC in EAPOL Key Message M2!!!!!!

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000000: 30 14 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 0.....

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000010: 00 0f ac 01 0c 00

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000000: 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 00 0f

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000010: ac 01 0c 00

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 PMK: Sending cache add

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Stopping retransmission timer for mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Sending EAPOL-Key Message to mobile 08:74:02:77:13:45

state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt for retransmission to mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Received EAPOL-key in

PTKINITNEGOTIATING state (message 4) from mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Stopping retransmission timer for mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last state 8021X_REQD (3)

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Mobility query, PEM State: L2AUTHCOMPLETE

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Mobile Announce :

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Client Payload:

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Ip: 0.0.0.0

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vlan Ip: 172.16.0.136, Vlan mask : 255.255.255.224

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vap Security: 16384

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Virtual Ip: 192.0.2.1

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 ssid: ise-ssid

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building VlanIpPayload.

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) DHCP required on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this client

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Not Using WMM Compliance code qosCap 00

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3 flex-acl-name:

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7)

pemAdvanceState2 6623, Adding TMP rule

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Adding Fast Path rule

type = Airespace AP - Learn IP address

```

on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0
IPv4 ACL ID = 255, IPv
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) mobility role
update request from Unassociated to Local
Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 172.16.0.136
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) State Update from
Mobility-Incomplete to Mobility-Complete, mobility role=Local, client
state=APF_MS_STATE_ASSOCIATED
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) pemAdvanceState2
6261, Adding TMP rule
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Replacing Fast
Path rule
type = Airespace AP - Learn IP address
on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0
IPv4 ACL ID = 255,
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Successfully
plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9,
dtlFlags 0x0
*pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9,
dtlFlags 0x0
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB
ip_learn_type 1, add_or_delete 1
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 In apfRegisterIpAddrOnMscb_debug:
regType=1 Invalid src IP address, 0.0.0.0 is part of reserved ip address range (caller
apf_ms.c:3593)
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0
*apfReceiveTask: Nov 25 16:36:27.840: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB
ip_learn_type 1, add_or_delete 1
*apfReceiveTask: Nov 25 16:36:27.841: 08:74:02:77:13:45 172.16.0.16 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 il criterio di autenticazione, il criterio di autorizzazione e il profilo di autorizzazione assegnati all'utente.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Operations' menu is expanded, showing 'RADIUS', 'TC-NAC Live Logs', 'TACACS', 'Reports', 'Troubleshoot', and 'Adaptive Network Control'. The 'RADIUS' menu is further expanded to show 'Live Logs' and 'Live Sessions'. The 'Live Logs' section displays several metrics: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (0), and Client Stopped Responding (4). Below these metrics, there are buttons for 'Refresh', 'Reset Repeat Counts', and 'Export To'. A table of log entries is shown, with the first entry highlighted. The table has columns for 'Time', 'Sta...', 'Details', 'Ide...', 'Endpoint ID', 'Endpoint ...', 'Authentication Policy', 'Authorization Policy', and 'Authorization Profiles'. The 'Details' column for the first entry is highlighted with a red box, showing 'Default >> Rule name >> Default' for Authentication Policy, 'Default >> NameAuthZrule' for Authorization Policy, and 'PermitAccess' for Authorization Profiles.

Time	Sta...	Details	Ide...	Endpoint ID	Endpoint ...	Authentication Policy	Authorization Policy	Authorization Profiles
No...			user1	08:74:02:77:13:45	Apple-Device	Default >> Rule name >> Default	Default >> NameAuthZrule	PermitAccess

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