Configurazione di EAP-TLS su 9800 WLC con ISE Internal CA

Sommario

- Introduzione
- Prerequisiti
  - Componenti usati
  - Premesse
  - Flusso di autenticazione EAP-TLS
  - Fasi del flusso EAP-TLS
- Configurazione
  - Esempio di rete
  - Configurazioni
  - Configurazione di ISE
  - Aggiunta di un dispositivo di rete
  - Verifica CA interna
  - Aggiungi metodo di autenticazione
  - Specifica modello di certificato
  - Crea portale certificati
  - Aggiungi utente interno
  - Configurazione del portale di provisioning dei certificati ISE e dei criteri RADIUS
- Configurazione 9800 WLC
  - Aggiunta di ISE Server a 9800 WLC
  - Aggiungi gruppo di server su 9800 WLC
  - Configurazione dell'elenco dei metodi AAA su 9800 WLC
  - Configura elenco metodi di autorizzazione su 9800 WLC
  - Crea un profilo criteri su 9800 WLC
  - Creazione di una WLAN su 9800 WLC
  - Mappa WLAN con profilo criterio su 9800 WLC
  - Mappa il tag criteri al punto di accesso su 9800 WLC
  - Esecuzione della configurazione del WLC dopo il completamento dell'installazione
- Crea e scarica il certificato per l'utente
- Installazione certificato su un computer con Windows 10
  - Verifica
- Risoluzione dei problemi
- Riferimenti

Introduzione

In questo documento viene descritta l'autenticazione EAP-TLS che utilizza Certificate Authority of

Identity Services Engine per autenticare gli utenti.

Prerequisiti

Componenti usati

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

- Controller wireless: C9800-40-K9 con 17.09.04a
- Cisco ISE Esecuzione della patch versione 3 4
- Modello AP: C9130AXI-D
- Switch: 9200-24P

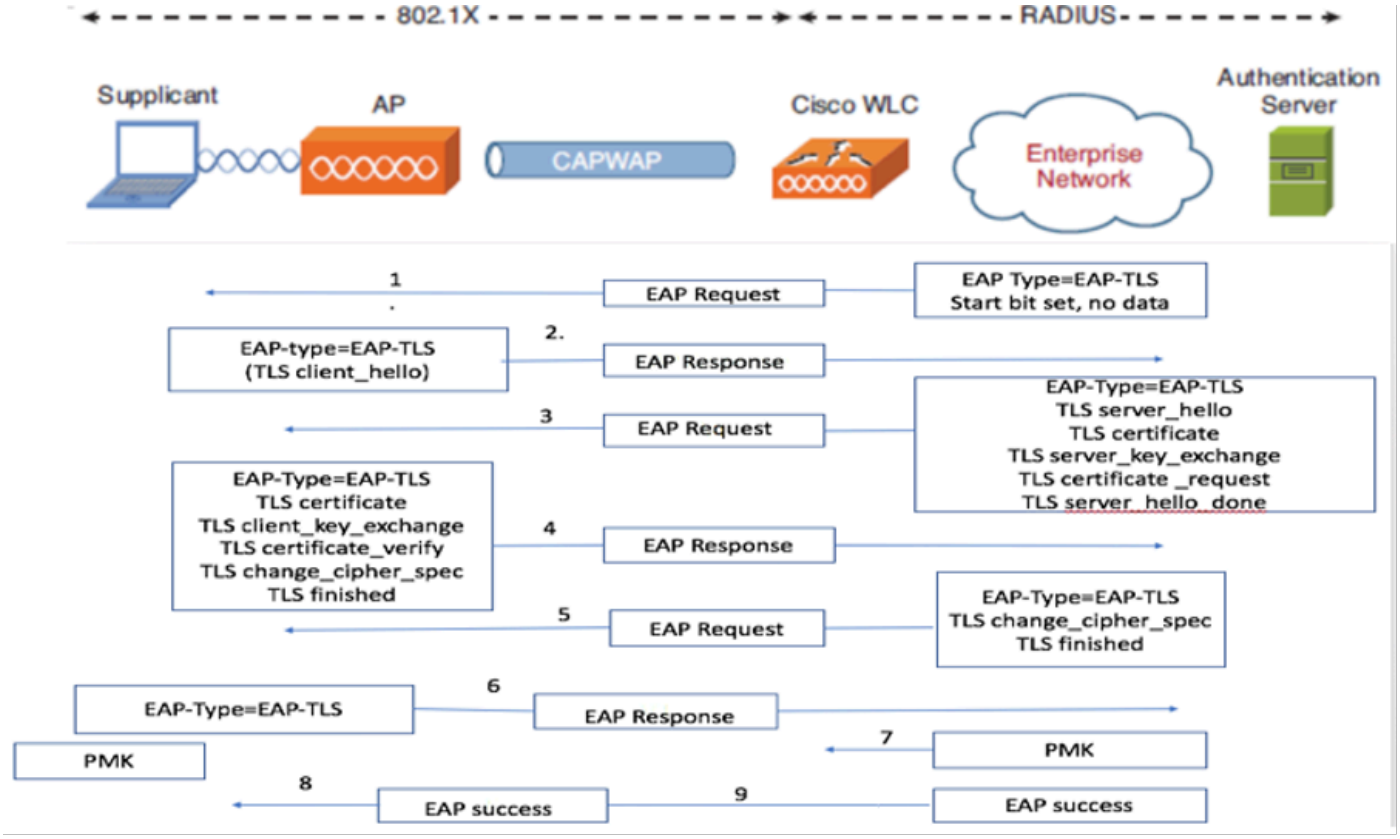
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Premesse

La maggior parte delle organizzazioni dispone di una propria CA che rilascia certificati agli utenti finali per l'autenticazione EAP-TLS. ISE include un'autorità di certificazione incorporata che può essere utilizzata per generare certificati per gli utenti da utilizzare nell'autenticazione EAP-TLS. Quando l'utilizzo di una CA completa non è fattibile, l'utilizzo della CA ISE per l'autenticazione utente risulta vantaggioso.

In questo documento viene descritta la procedura di configurazione necessaria per utilizzare in modo efficace l'autorità di certificazione ISE per autenticare gli utenti wireless. Flusso di autenticazione EAP-TLS

Flusso di autenticazione EAP-TLS



Flusso di autenticazione EAP-TLS

Fasi del flusso EAP-TLS

1. Il client wireless viene associato al punto di accesso (AP).
2. In questa fase, il punto di accesso non consente la trasmissione dei dati e invia una richiesta di autenticazione.
3. Il client, agendo come supplicant, risponde con un'identità di risposta EAP.
4. Il controller WLC (Wireless LAN Controller) inoltra le informazioni sull'ID utente al server di autenticazione.
5. Il server RADIUS risponde al client con un pacchetto di avvio EAP-TLS.
6. La conversazione EAP-TLS inizia da questo punto.
7. Il client invia una risposta EAP al server di autenticazione, incluso un messaggio di handshake client_hello con una cifratura impostata su NULL.
8. Il server di autenticazione risponde con un pacchetto Access-Challenge contenente:

```
TLS server_hello
Handshake message
Certificate
Server_key_exchange
Certificate request
Server_hello_done
```

9. Il client risponde con un messaggio di risposta EAP che include:

```
Certificate (for server validation)
Client_key_exchange
Certificate_verify (to verify server trust)
Change_cipher_spec
TLS finished
```

10. Una volta completata l'autenticazione del client, il server RADIUS invia un messaggio di richiesta di verifica di accesso contenente:

```
Change_cipher_spec
Handshake finished message
```

11. Il client verifica l'hash per autenticare il server RADIUS.

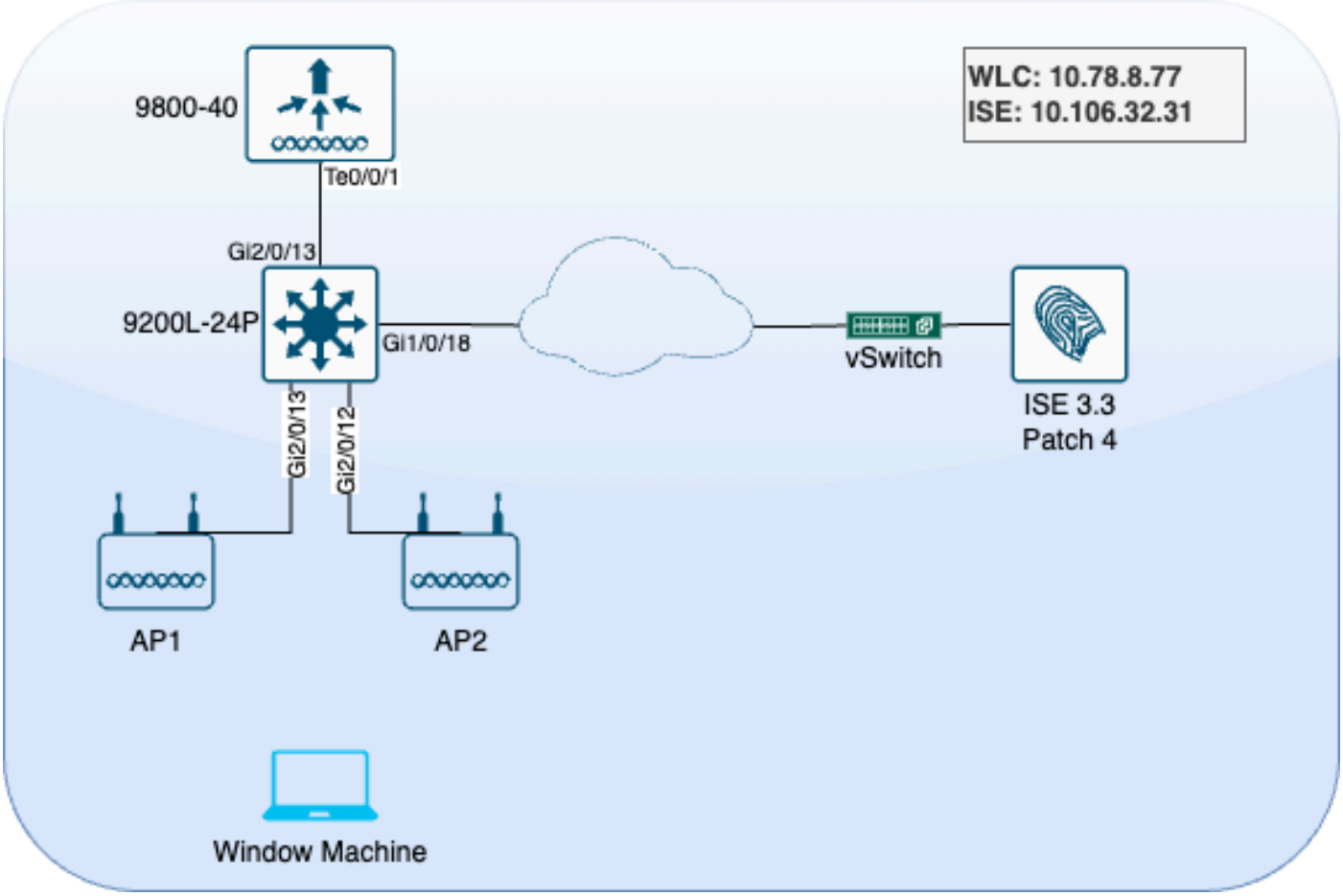
12. Una nuova chiave di crittografia viene derivata in modo dinamico dal segreto durante l'handshake TLS.

13. Un messaggio EAP-Success viene inviato dal server all'autenticatore e quindi al supplicant.

14. Il client wireless abilitato per EAP-TLS può ora accedere alla rete wireless.

Configurazione

Esempio di rete



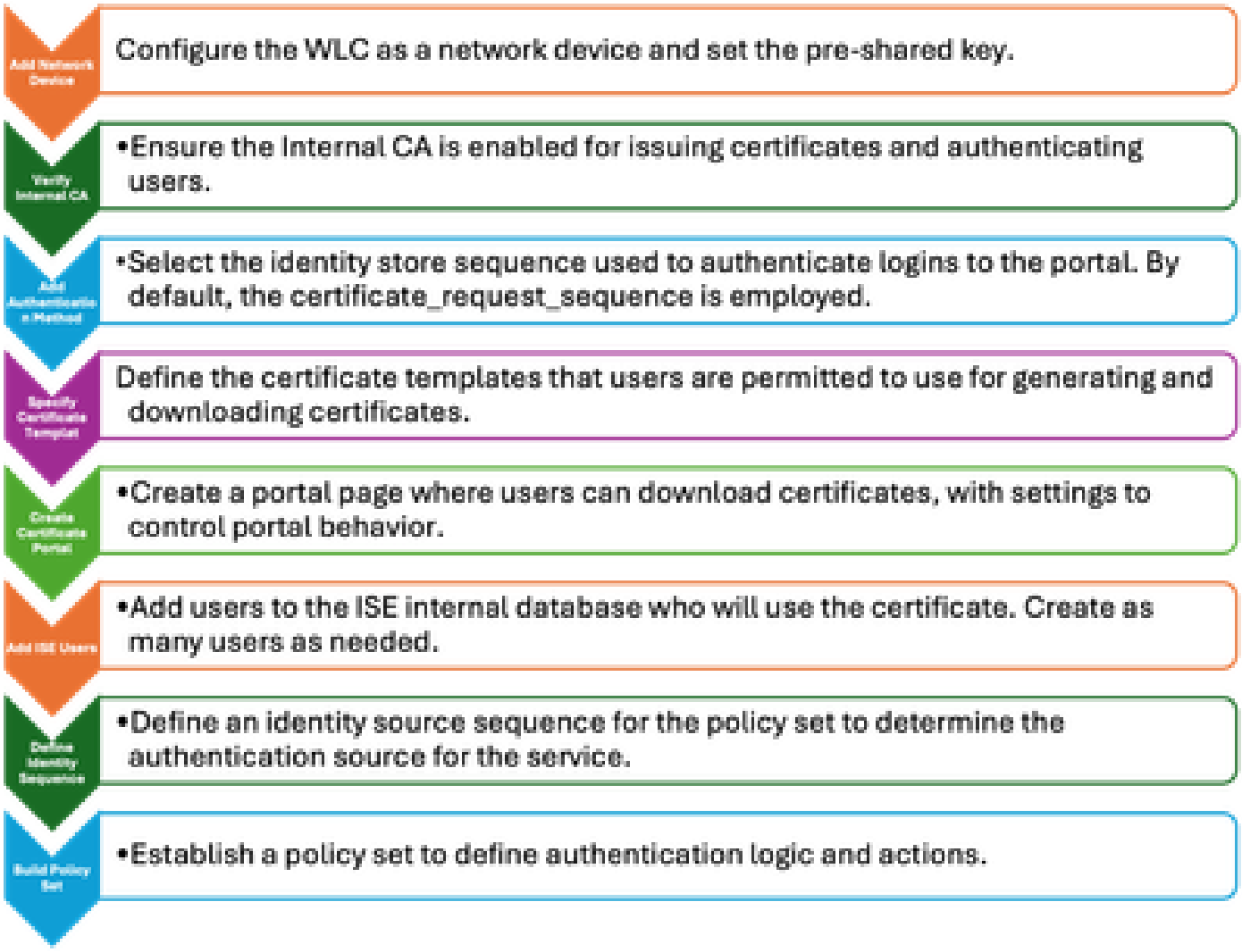
Topologia LAB

Configurazioni

In questa sezione vengono configurati due componenti: ISE e 9800 WLC.

Configurazione di ISE

Di seguito viene riportata la procedura di configurazione per il server ISE. Ciascuna procedura è accompagnata da uno screenshot in questa sezione per fornire una guida visiva.

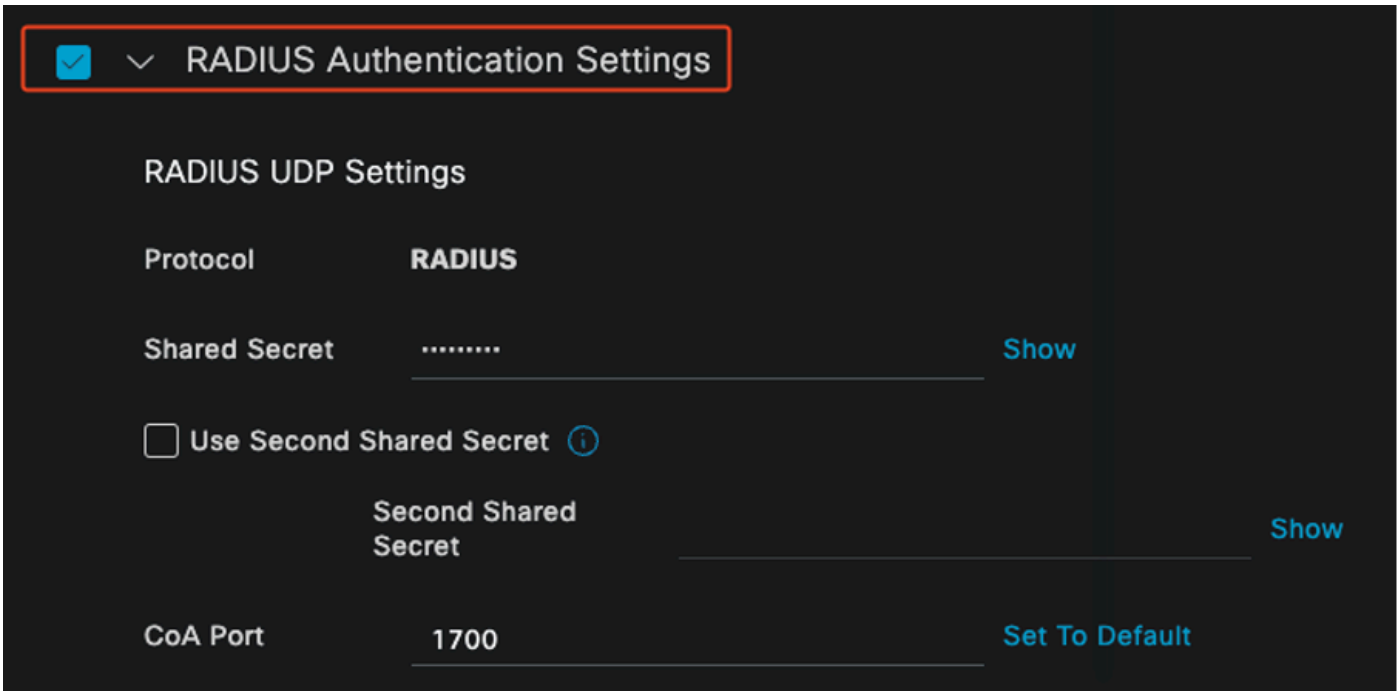


Procedura di configurazione del server ISE

Aggiunta di un dispositivo di rete

Per aggiungere il controller WLC come dispositivo di rete, attenersi alle seguenti istruzioni:

1. Selezionare Amministrazione > Risorse di rete > Dispositivi di rete.
2. Fare clic sull'icona +Add per avviare il processo di aggiunta del WLC.
3. Verificare che la chiave precondivisa corrisponda sia al WLC che al server ISE per consentire una corretta comunicazione.
4. Dopo aver immesso correttamente tutti i dettagli, fare clic su Submit (Invia) nell'angolo inferiore sinistro per salvare la configurazione

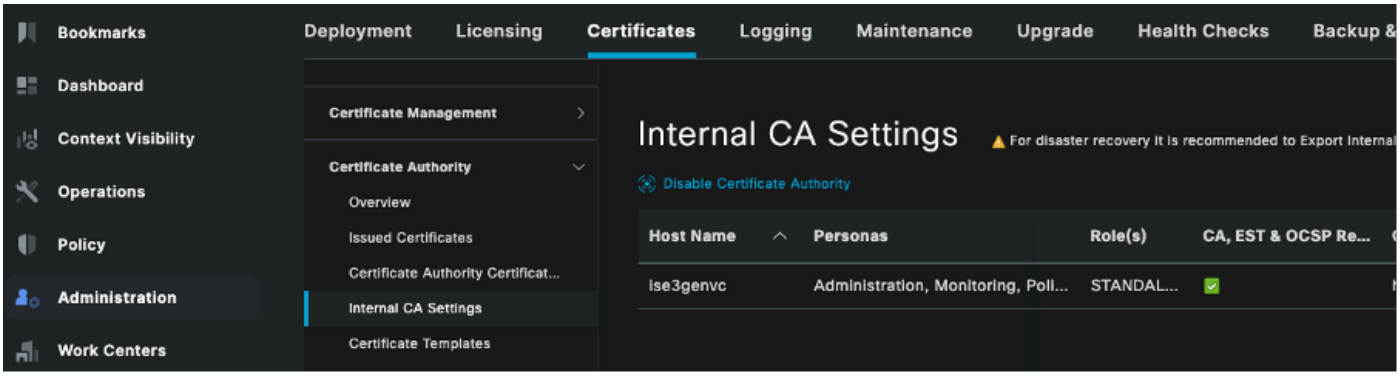


Aggiunta di un dispositivo di rete

Verifica CA interna

Per verificare le impostazioni dell'Autorità di certificazione interna (CA), eseguire la procedura seguente:

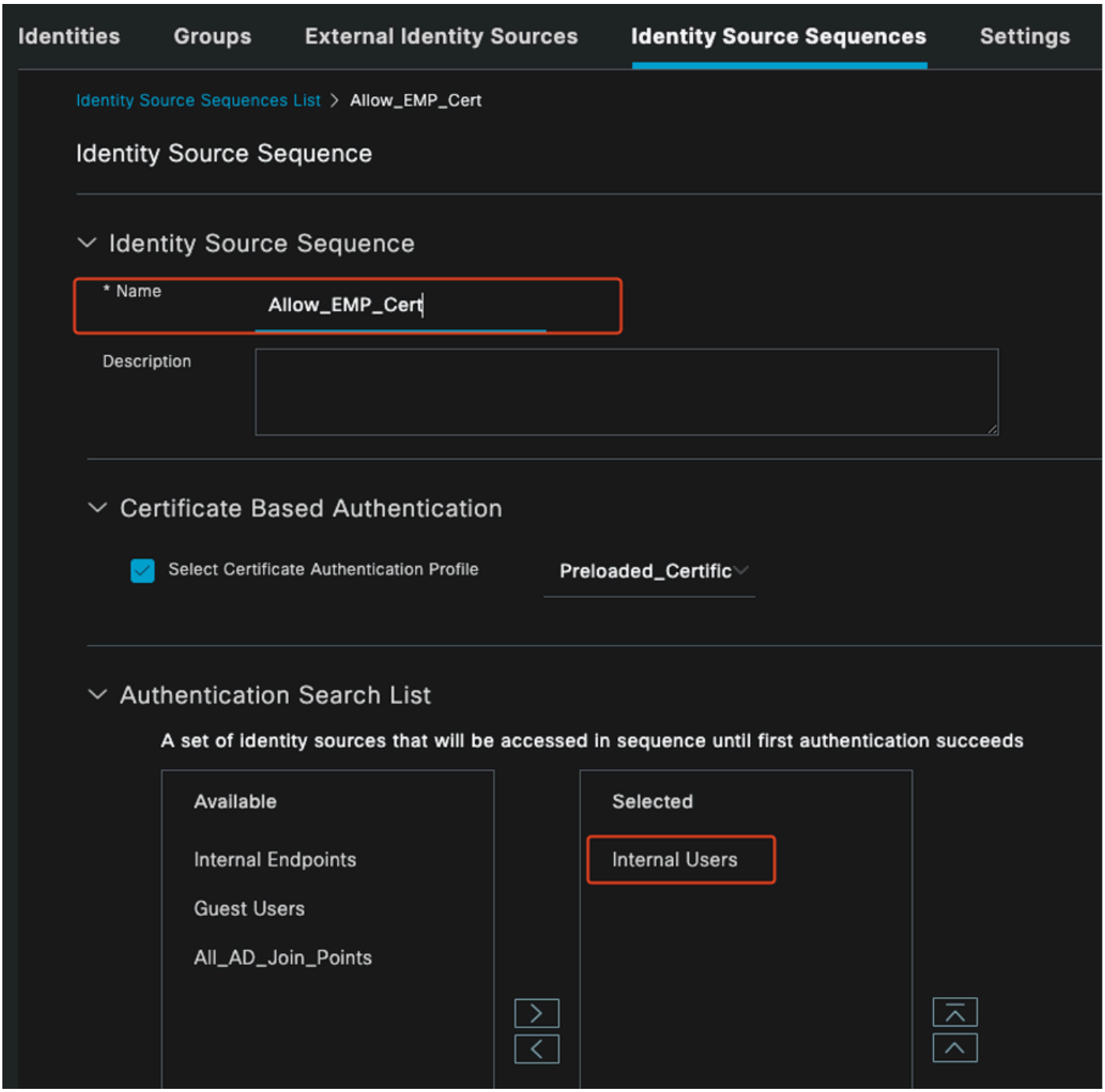
1. Selezionare Amministrazione > Sistema > Certificati > Autorità di certificazione > Impostazioni CA interne.
2. Verificare che la colonna CA sia abilitata per verificare che la CA interna sia attiva.



Verifica CA interna

Aggiungi metodo di autenticazione

Passare a Amministrazione > Gestione delle identità > Sequenze origini identità. Aggiungere una sequenza di identità personalizzata per controllare l'origine di accesso al portale.



Metodo di autenticazione

Specifica modello di certificato

Per specificare un modello di certificato, eseguire la procedura seguente:

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

Passaggio 2. Fare clic sull'icona +Aggiungi per creare un nuovo modello di certificato:

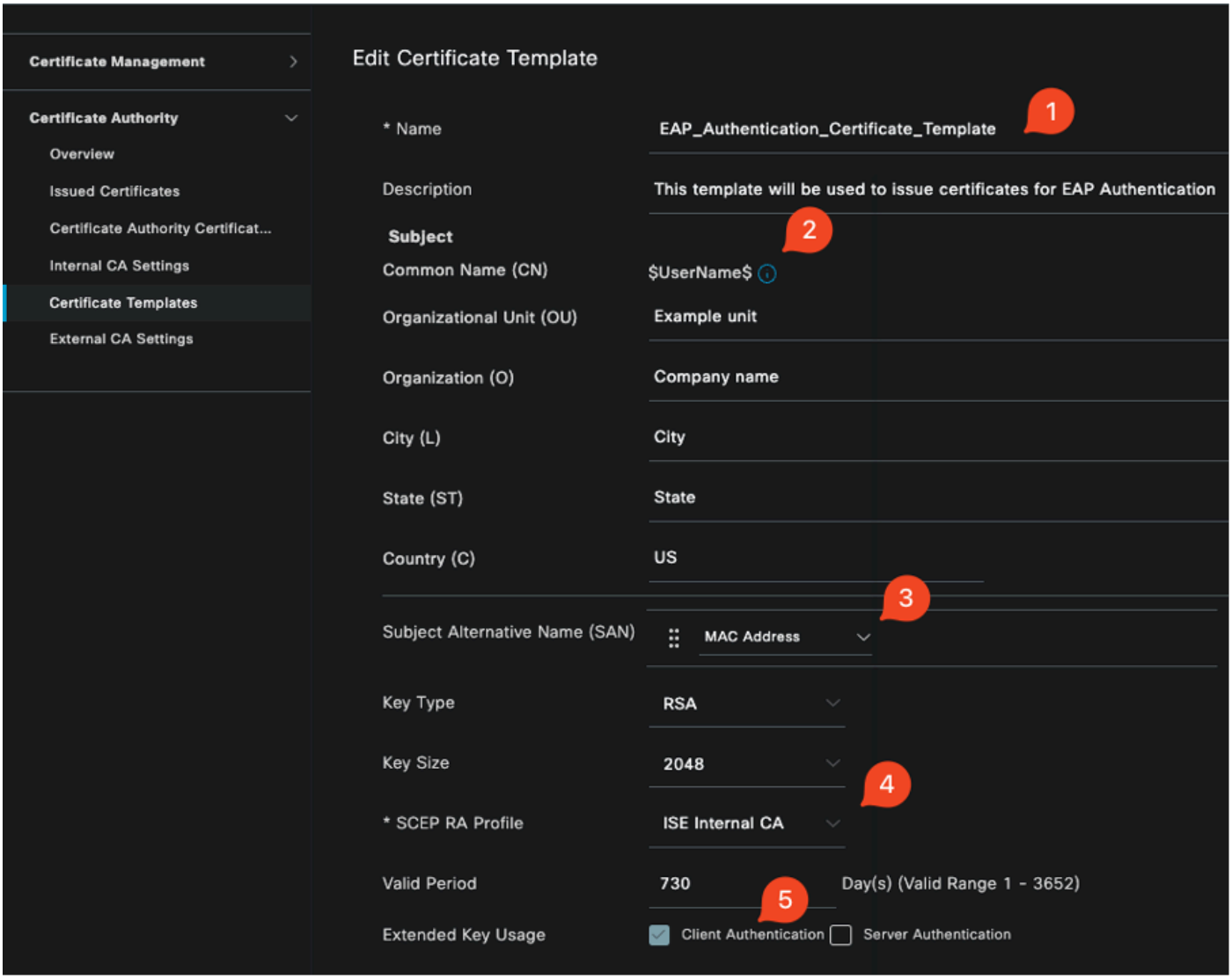
2.1 Assegnare un nome univoco locale al server ISE per il modello.

2.2 Assicurarsi che il nome comune (CN) sia impostato su $UserName$.

2.3 Verificare che il nome alternativo del soggetto (SAN) sia mappato all'indirizzo MAC.

2.4 Impostare il profilo SCEP RA su ISE Internal CA.

2.5 Nella sezione utilizzo chiavi esteso abilitare l'autenticazione client.



Modello di certificato

Crea portale certificati

Per creare un portale certificati per la generazione di certificati client, eseguire la procedura seguente:

Passaggio 1. Passare a Amministrazione > Gestione portale dispositivi > Provisioning certificati.

Passaggio 2. Fare clic su Crea per impostare una nuova pagina del portale.

Passaggio 3. Fornire un nome univoco per il portale per identificarlo facilmente.

3.1. Scegliere il numero di porta su cui deve operare il portale; impostate questo valore su

8443.

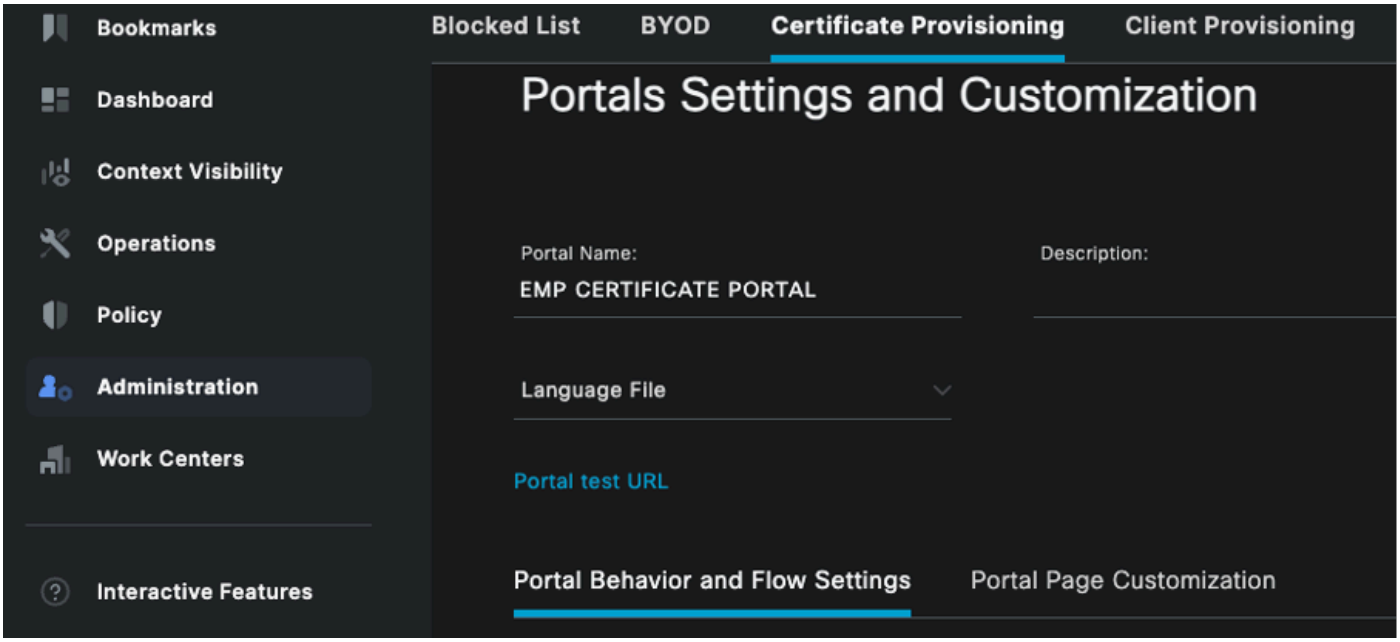
3.2. Specificare le interfacce su cui ISE è in ascolto per questo portale.

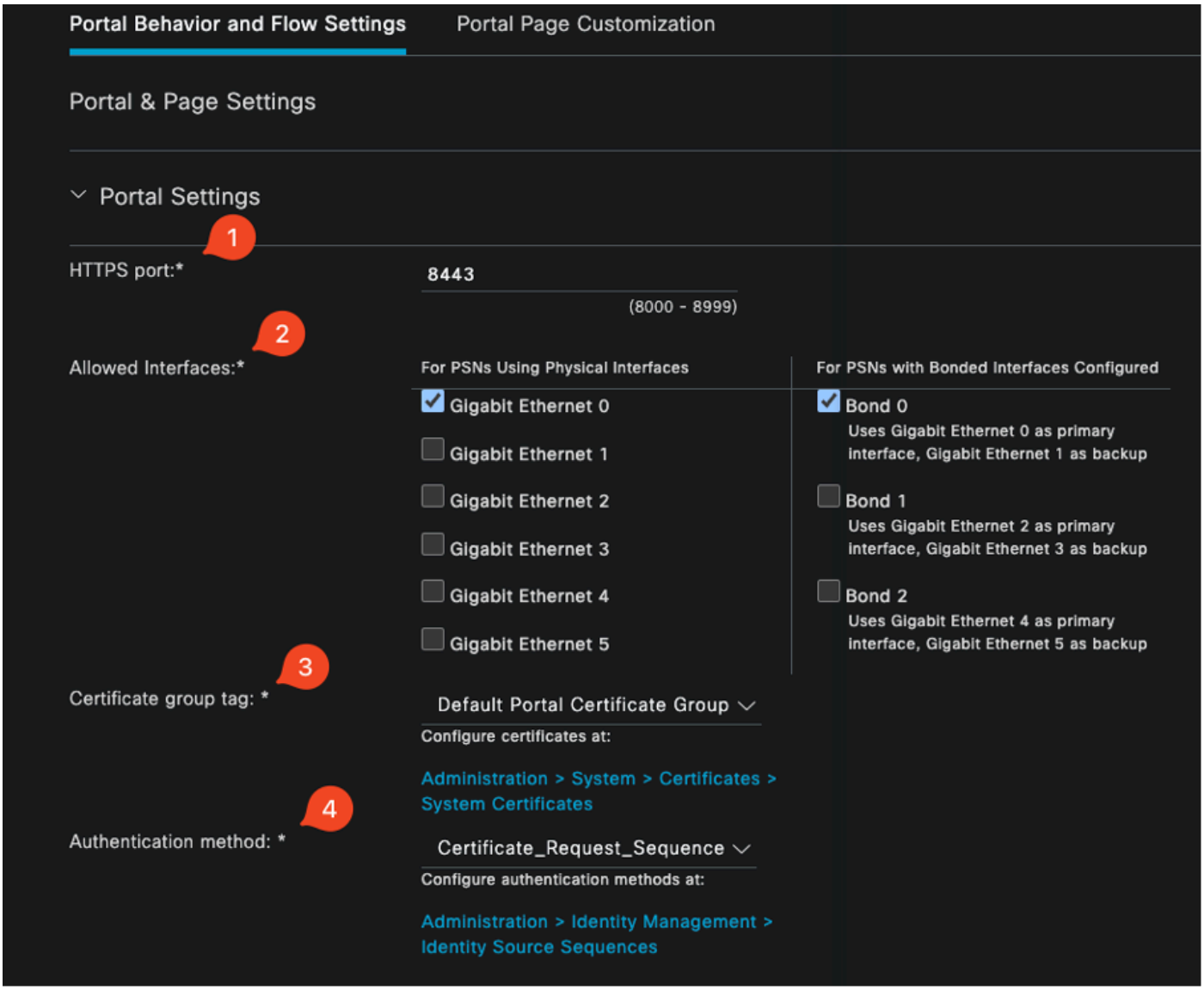
3.3. Selezionare il tag del gruppo di certificati come gruppo di certificati predefinito del portale.

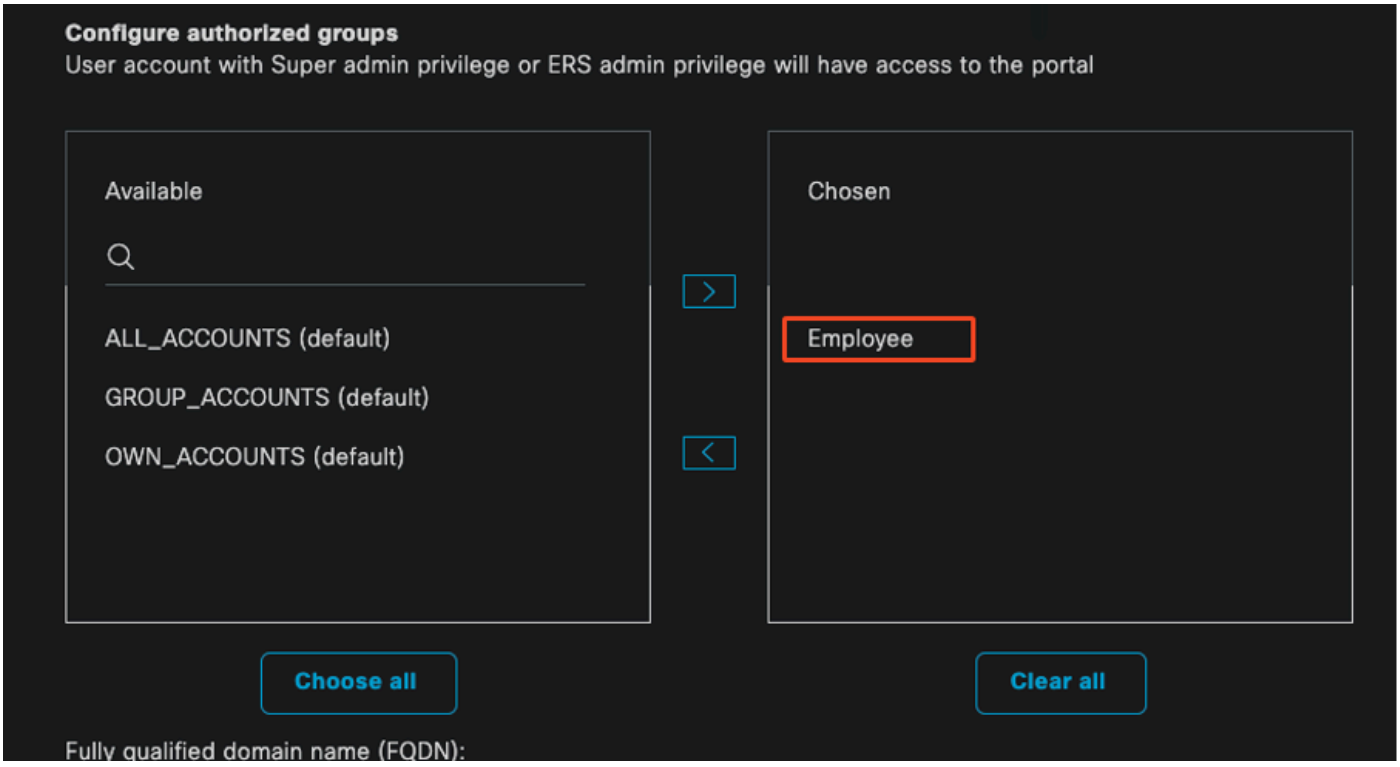
3.4. Selezionare il metodo di autenticazione, che indica la sequenza di archivi di identità utilizzata per autenticare l'accesso a questo portale.

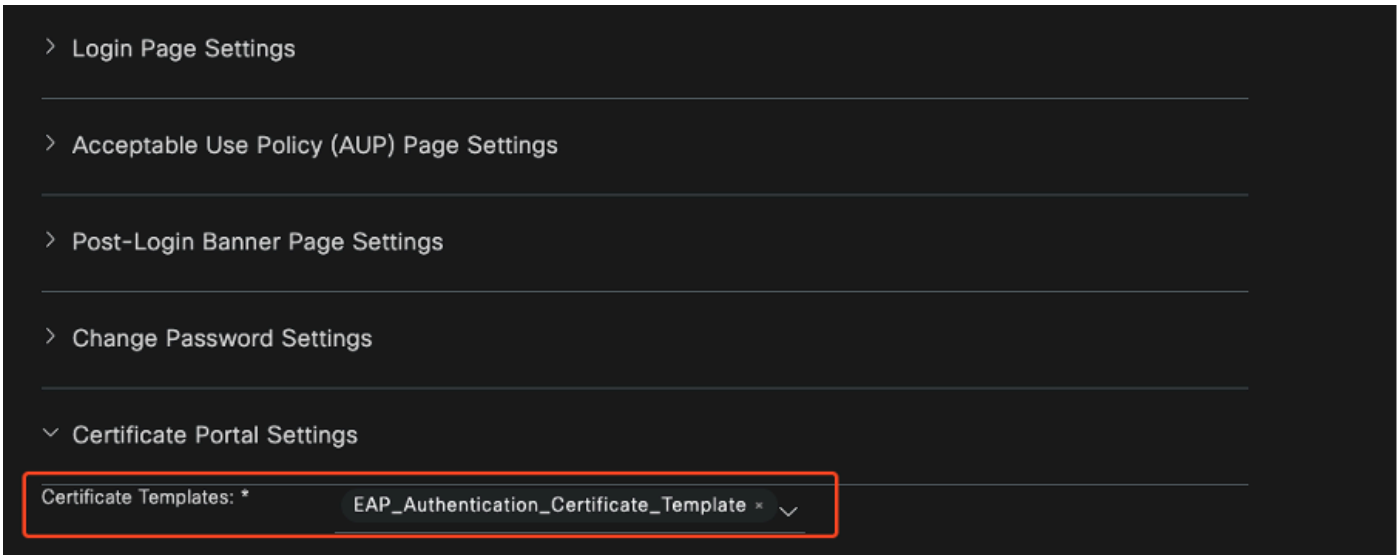
3.5. Includere i gruppi autorizzati i cui membri possono accedere al portale. Ad esempio, selezionare il gruppo utenti Dipendenti se gli utenti appartengono a questo gruppo.

3.6. Definire i modelli di certificato consentiti dalle impostazioni di Provisioning certificati.



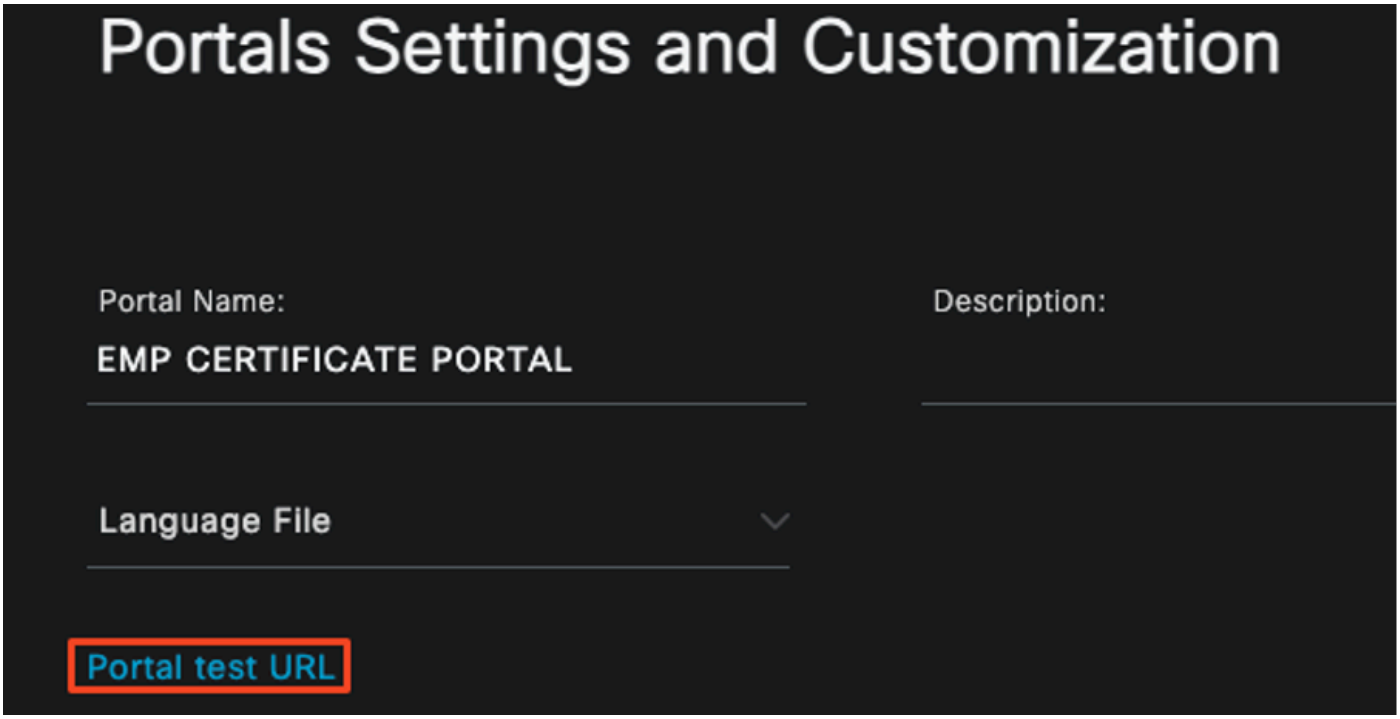

Portal Behavior and Flow Settings
Portal Page Customization
Portal & Page Settings
Portal Settings
1
HTTPS port:*
8443
(8000 - 8999)
2
Allowed Interfaces:*
For PSNs Using Physical Interfaces
Gigabit Ethernet 0
Gigabit Ethernet 1
Gigabit Ethernet 2
Gigabit Ethernet 3
Gigabit Ethernet 4
Gigabit Ethernet 5
For PSNs with Bonded Interfaces Configured
Bond 0
Uses Gigabit Ethernet 0 as primary interface, Gigabit Ethernet 1 as backup
Bond 1
Uses Gigabit Ethernet 2 as primary interface, Gigabit Ethernet 3 as backup
Bond 2
Uses Gigabit Ethernet 4 as primary interface, Gigabit Ethernet 5 as backup
3
Certificate group tag: *
Default Portal Certificate Group
Configure certificates at:
Administration > System > Certificates > System Certificates
4
Authentication method: *
Certificate_Request_Sequence
Configure authentication methods at:
Administration > Identity Management > Identity Source Sequences


Configure authorized groups
User account with Super admin privilege or ERS admin privilege will have access to the portal
Available
ALL_ACCOUNTS (default)
GROUP_ACCOUNTS (default)
OWN_ACCOUNTS (default)
Chosen
Employee
Choose all
Clear all
Fully qualified domain name (FQDN):

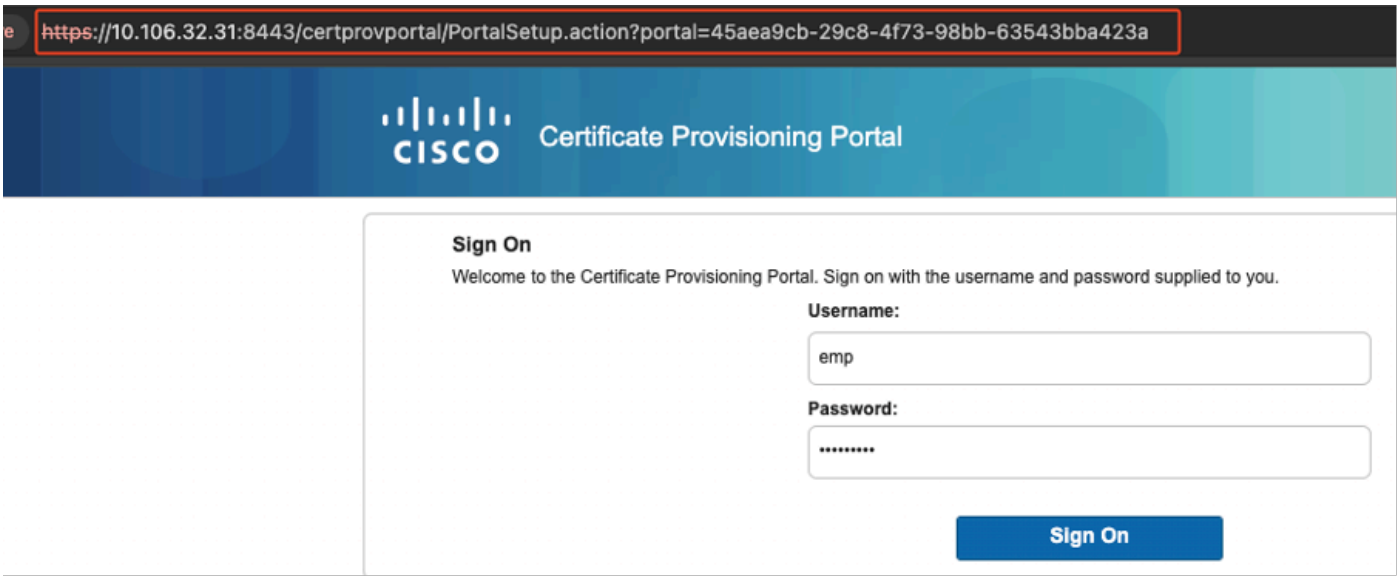


Configurazione portale certificati

Al termine dell'installazione, è possibile eseguire il test del portale facendo clic sull'URL di test del portale. Verrà aperta la pagina del portale.



Test URL pagina portale

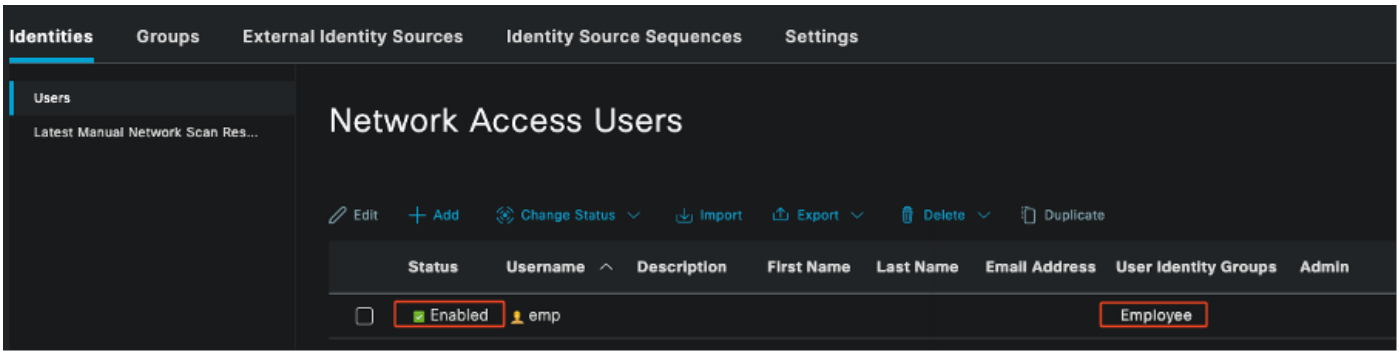


Pagina portale

Aggiungi utente interno

Per creare un utente per l'autenticazione tramite il portale certificati, eseguire la procedura seguente:

1. Andare a Amministrazione > Gestione delle identità > Identità > Utenti.
2. Fare clic sull'opzione per aggiungere un utente al sistema.
3. Selezionare i gruppi di identità utente a cui appartiene l'utente. Per questo esempio, assegnare l'utente al gruppo Employee.



Aggiunta utente interno

Configurazione del portale di provisioning dei certificati ISE e dei criteri RADIUS

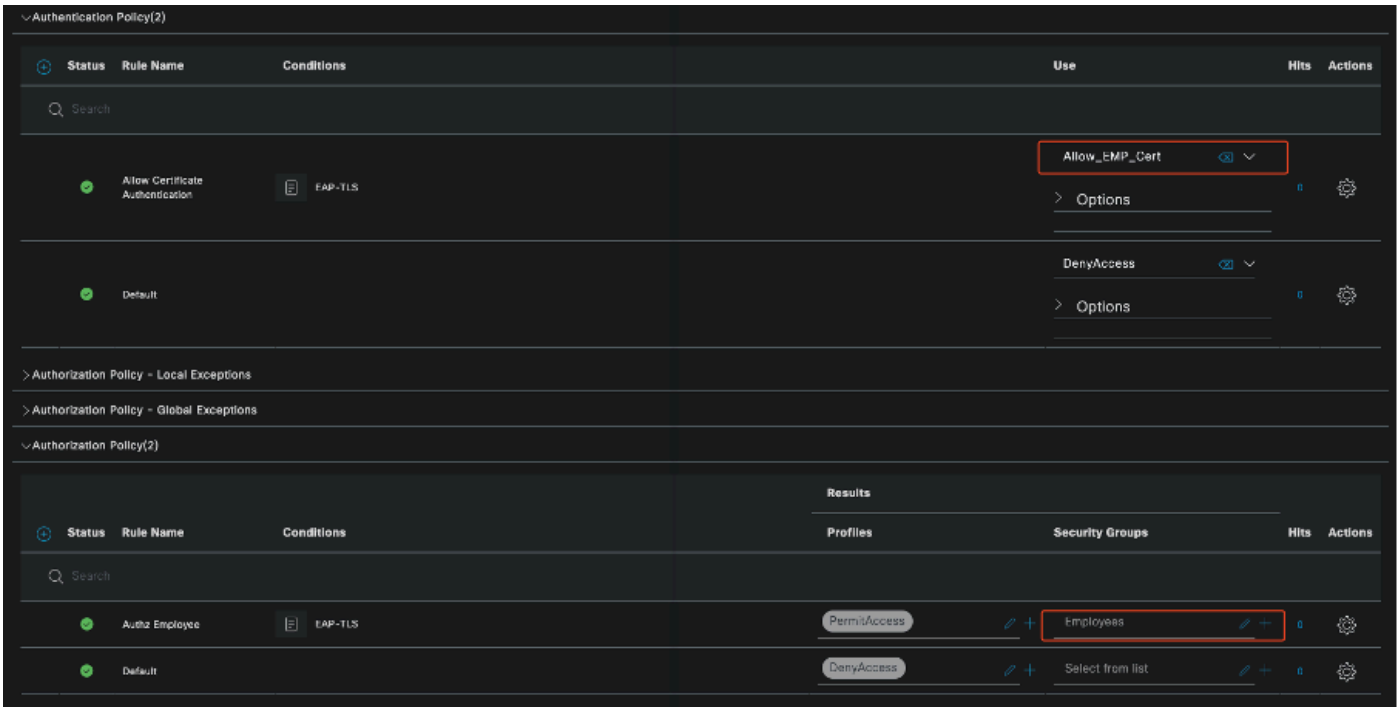
La sezione precedente riguardava la configurazione del portale di provisioning dei certificati ISE. A questo punto, i set di criteri ISE RADIUS vengono configurati in modo da consentire l'autenticazione dell'utente.

1. Configura set di criteri ISE RADIUS
2. Passare a Criterio > Set di criteri.
3. Fare clic sul segno più (+) per creare un nuovo set di criteri.

In questo esempio, impostare un set di criteri semplice progettato per autenticare gli utenti

utilizzando i certificati.

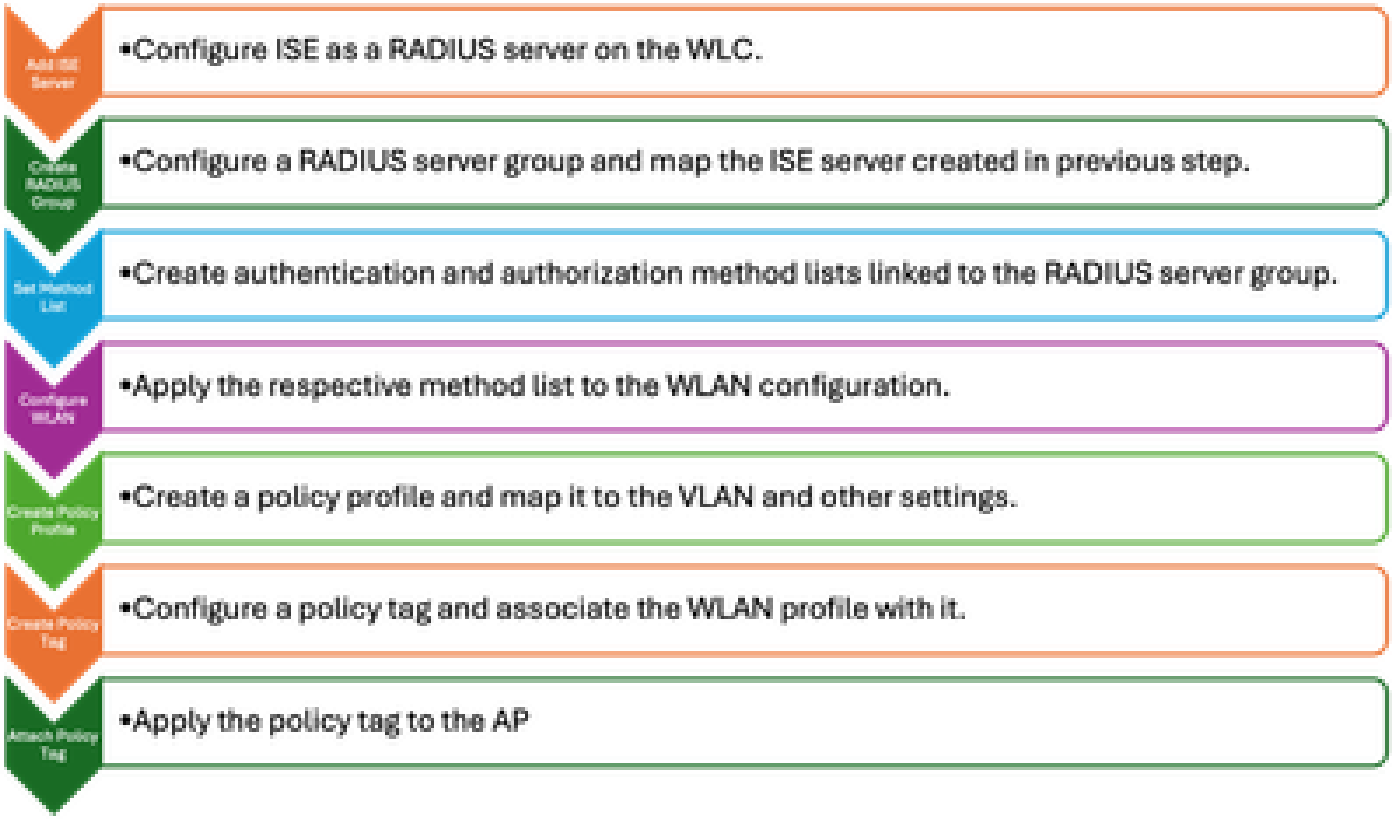
Set di criteri



Set di criteri che mostra i criteri di autenticazione e autorizzazione

Configurazione 9800 WLC

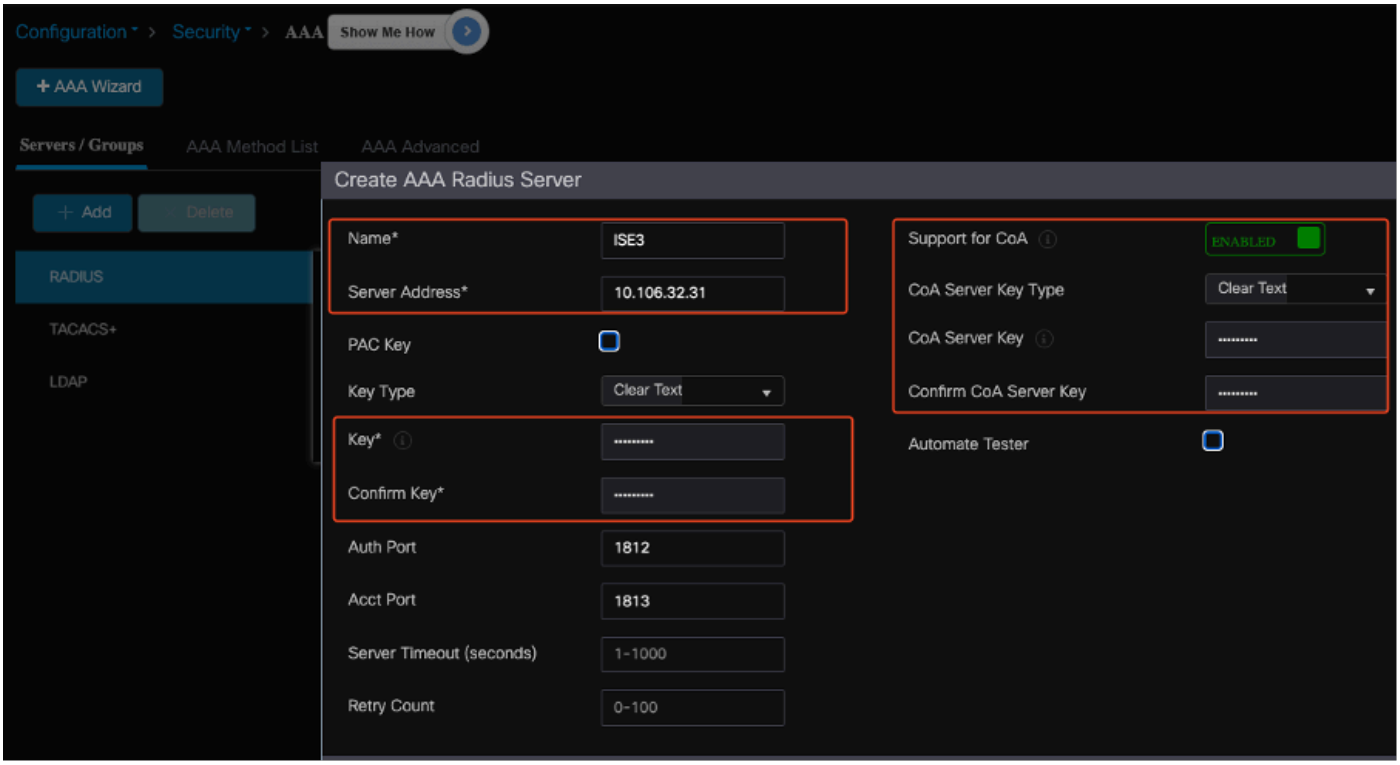
Di seguito sono riportati i passaggi di configurazione per il WLC 9800. Ciascun passaggio è accompagnato da schermate in questa sezione per fornire una guida visiva.



Passaggi della configurazione WLC

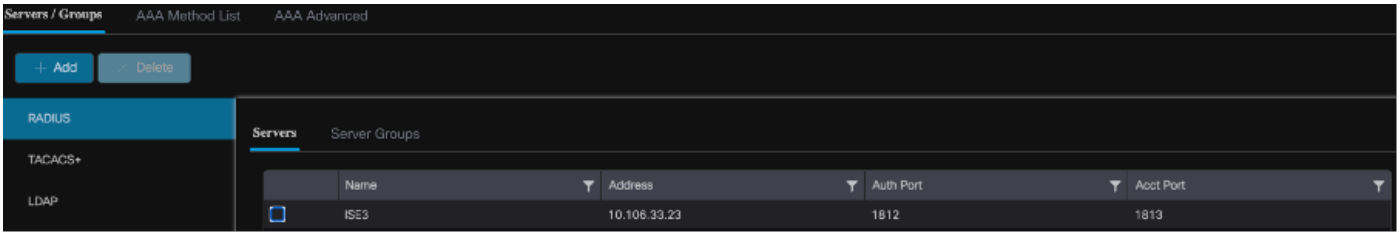
Aggiunta di ISE Server a 9800 WLC

1. Per integrare il server ISE con il controller WLC (Wireless LAN Controller) 9800, attenersi alla seguente procedura:
2. Andare a Configurazione > Sicurezza > AAA.
3. Fare clic sul pulsante Add (Aggiungi) per includere il server ISE nella configurazione WLC.



Aggiunta di ISE Server al WLC

Una volta aggiunto, il server viene visualizzato nell'elenco dei server.

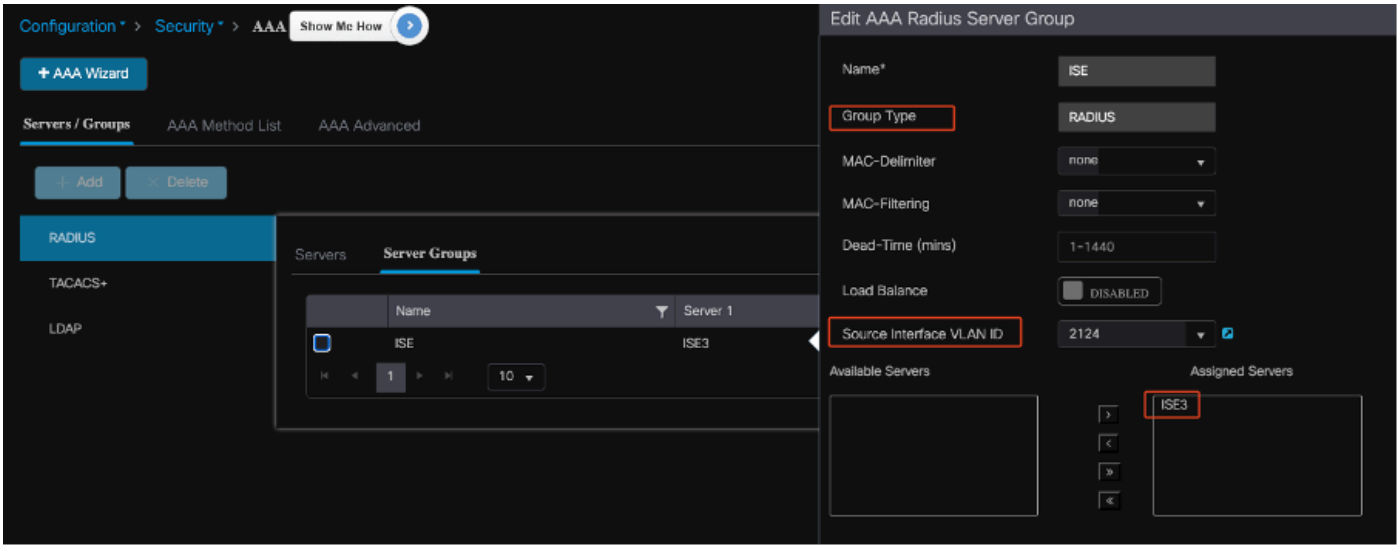


Visualizzazione dei server Radius

Aggiungi gruppo di server su 9800 WLC

Per aggiungere un gruppo di server sul controller LAN wireless 9800, attenersi alla seguente procedura:

1. Selezionare Configurazione > Sicurezza > AAA.
2. Fare clic sulla scheda Gruppo server, quindi su Aggiungi per creare un nuovo gruppo di server.

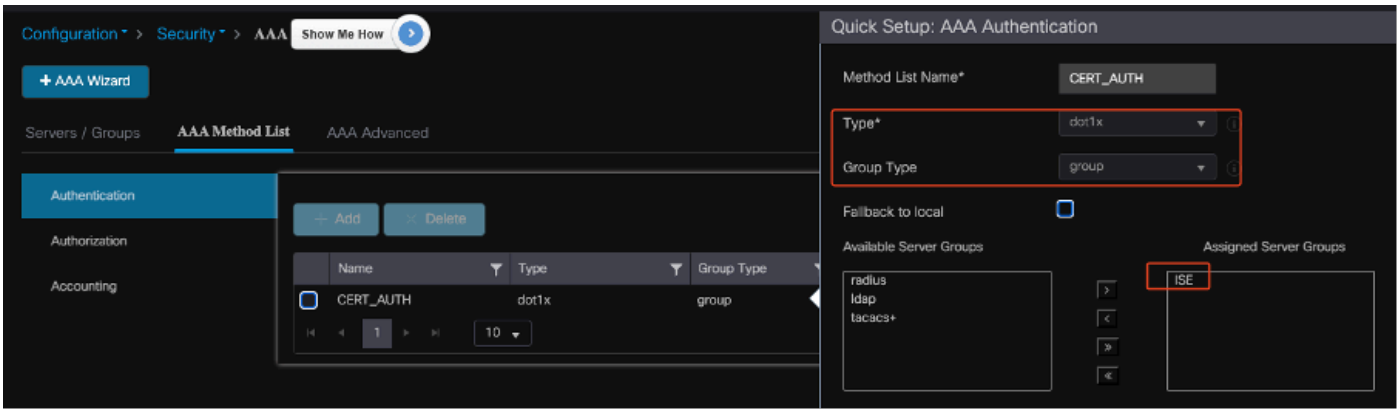


Mappatura dei server ISE a un gruppo di server Radius

Configurazione dell'elenco dei metodi AAA su 9800 WLC

Dopo aver creato il gruppo di server, configurare l'elenco dei metodi di autenticazione attenendosi alla procedura seguente:

1. Passare a Configurazione > Sicurezza > AAA > Elenco metodi AAA.
2. Nella scheda Autenticazione aggiungere un nuovo elenco di metodi di autenticazione.
3. Impostate il tipo su dot1x.
4. Selezionate gruppo (group) come tipo di gruppo.
5. Includere i gruppi di server ISE creati in precedenza come gruppi di server.

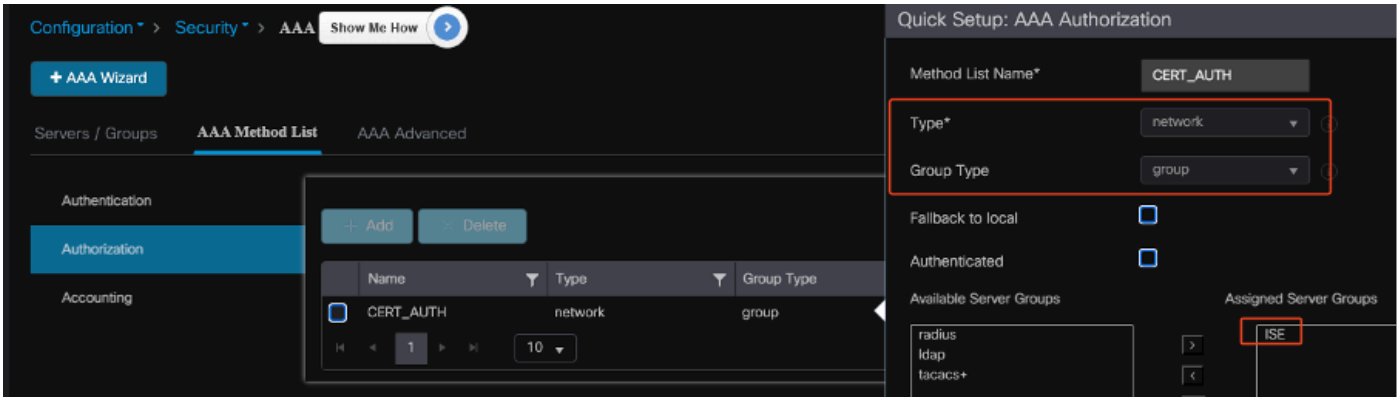


Creazione di elenchi di metodi di autenticazione

Configura elenco metodi di autorizzazione su 9800 WLC

Per impostare l'elenco dei metodi di autorizzazione, eseguire la procedura seguente:

1. Passare alla scheda Autorizzazione nella sezione Lista metodi AAA.
2. Fare clic su Aggiungi per creare un nuovo elenco di metodi di autorizzazione.
3. Selezionate network come tipo.
4. Selezionate gruppo (group) come tipo di gruppo.
5. Includere il gruppo di server ISE come gruppo di server.

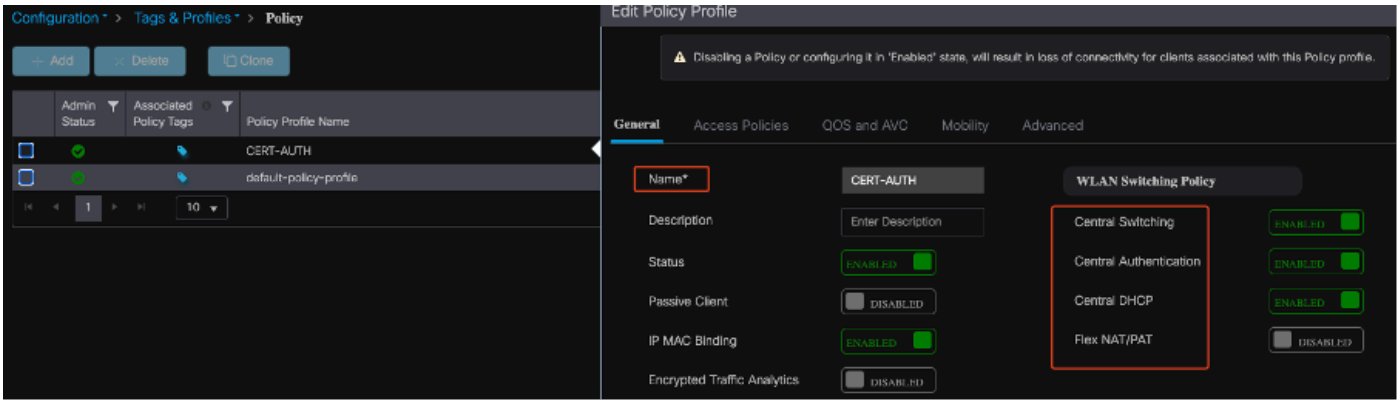


Aggiunta dell'elenco dei metodi di autorizzazione

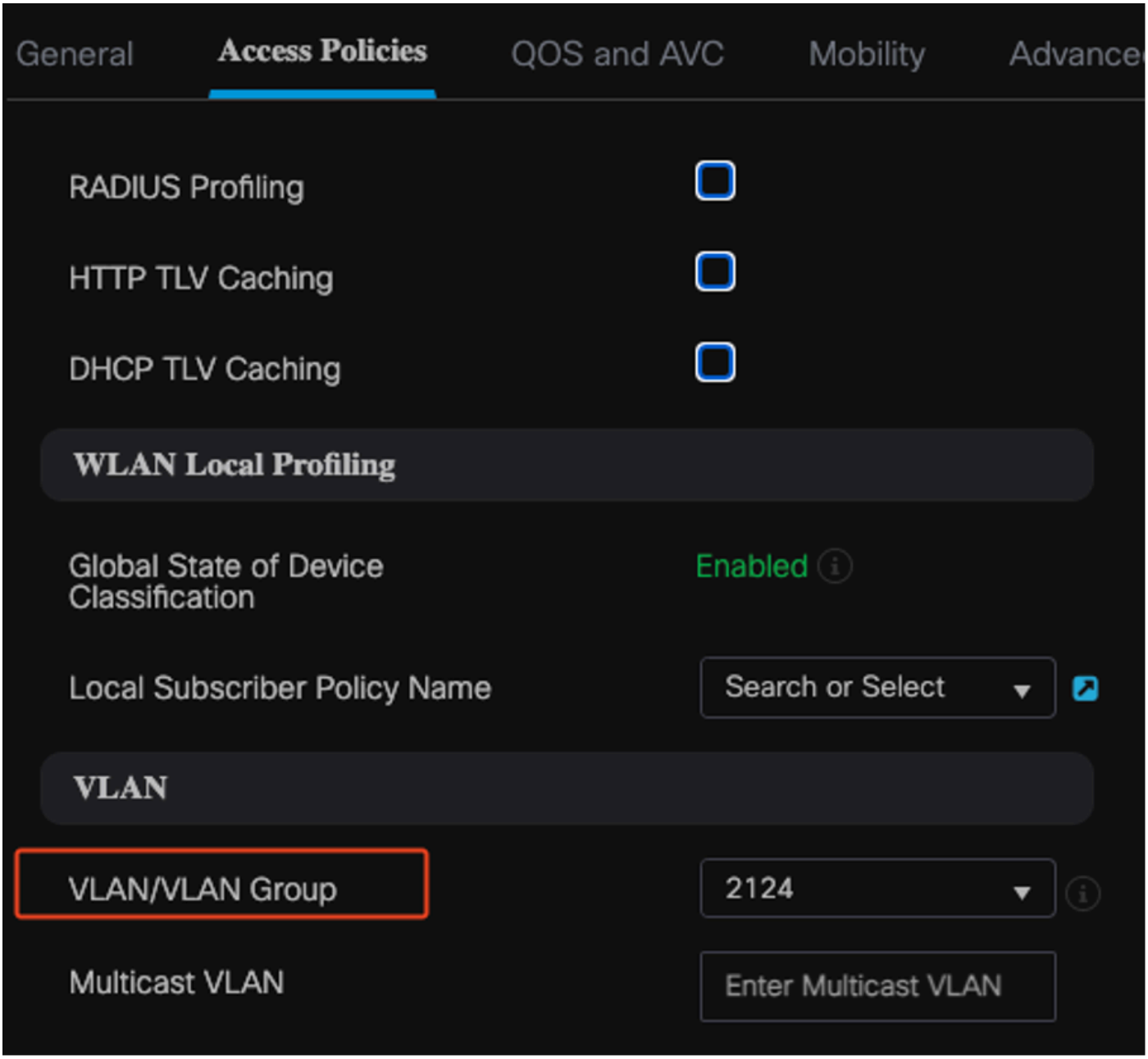
Crea un profilo criteri su 9800 WLC

Al termine della configurazione del gruppo RADIUS, procedere con la creazione di un profilo dei criteri:

1. Selezionare Configurazione > Tag e profili > Criterio.
2. Fare clic su Aggiungi per creare un nuovo profilo criteri.
3. Scegliere i parametri appropriati per il profilo dei criteri. Nell'esempio, tutto è centrale e la VLAN LAB viene usata come VLAN client.



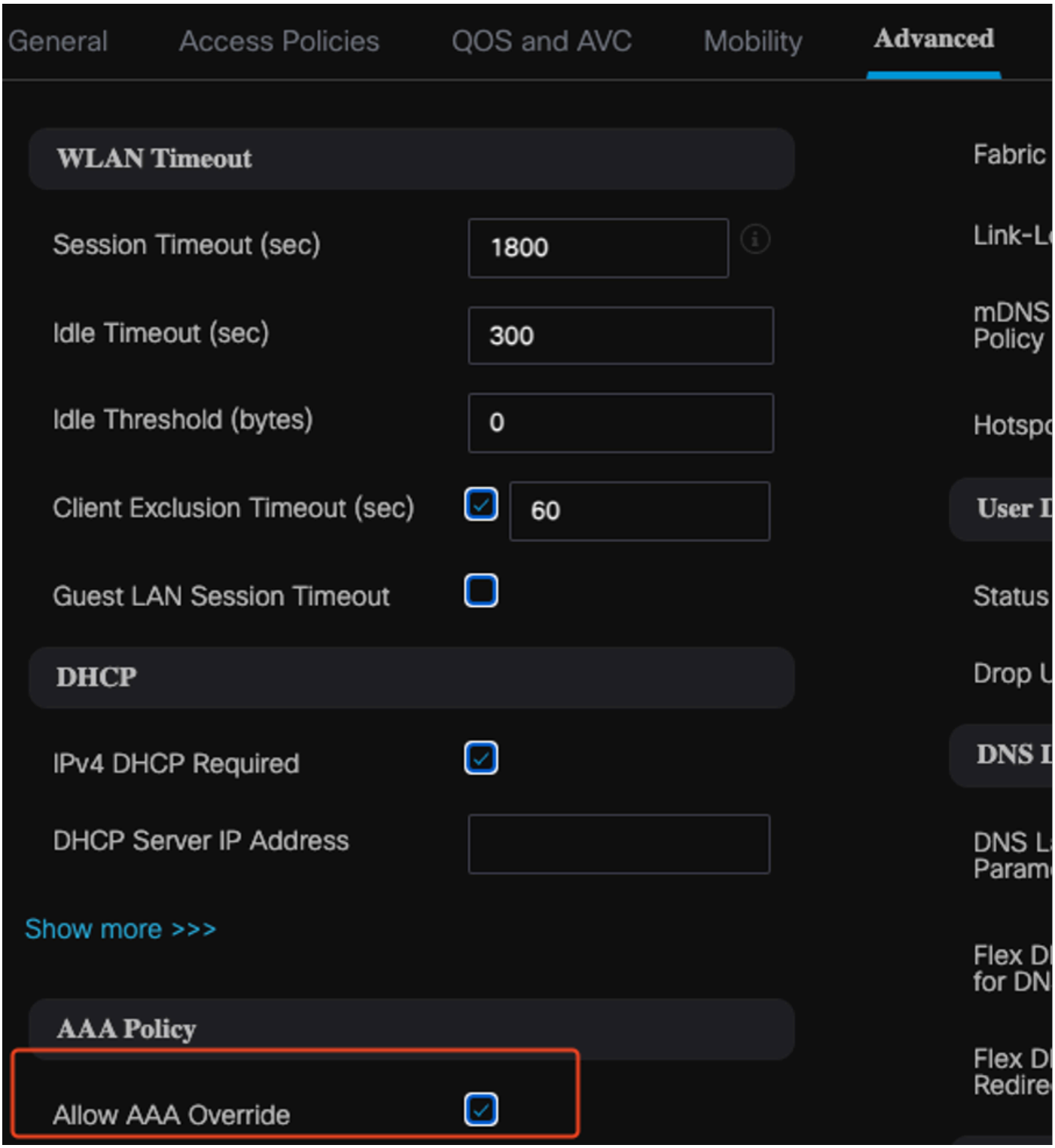
Configurazione del profilo dei criteri



Mappatura da VLAN a policy

Quando si configura l'autorizzazione RADIUS, verificare che l'opzione AAA Override sia abilitata nella scheda Advanced (Avanzate) delle impostazioni del profilo dei criteri. Questa impostazione

consente al controller LAN wireless di applicare criteri di autorizzazione basati su RADIUS a utenti e dispositivi.



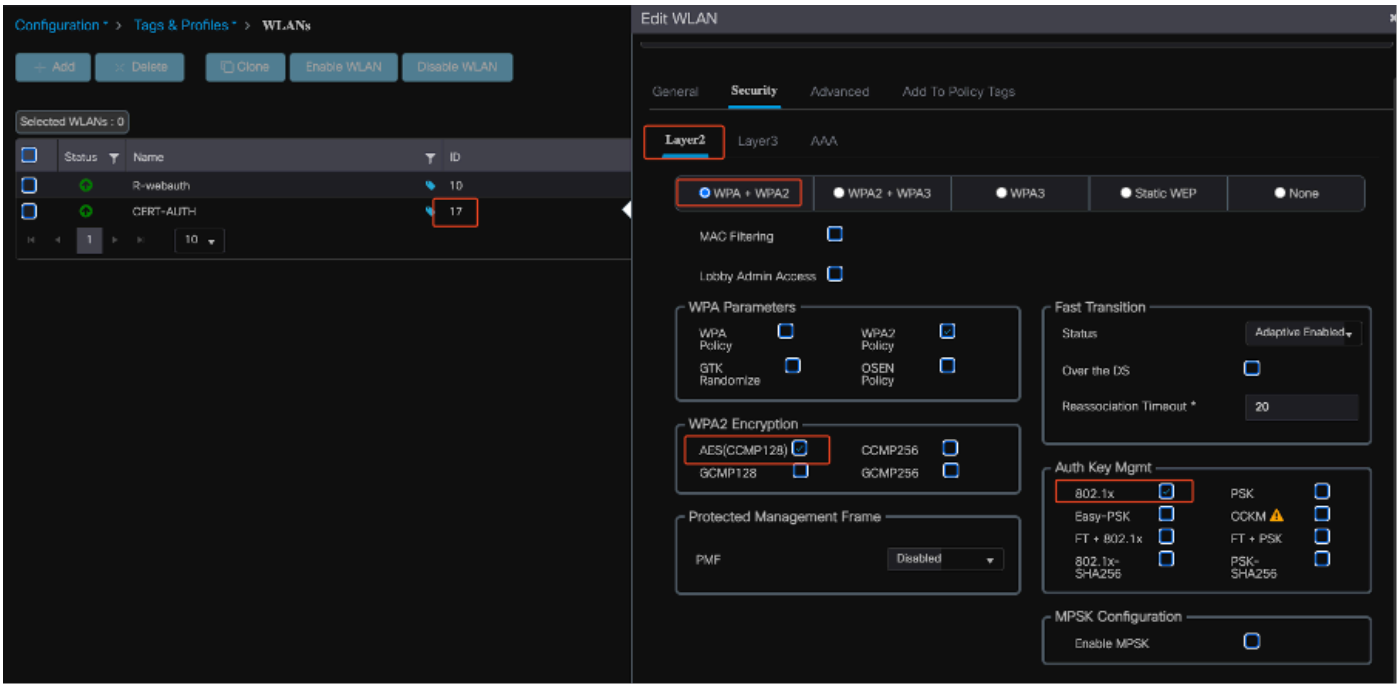
Override AAA

Creazione di una WLAN su 9800 WLC

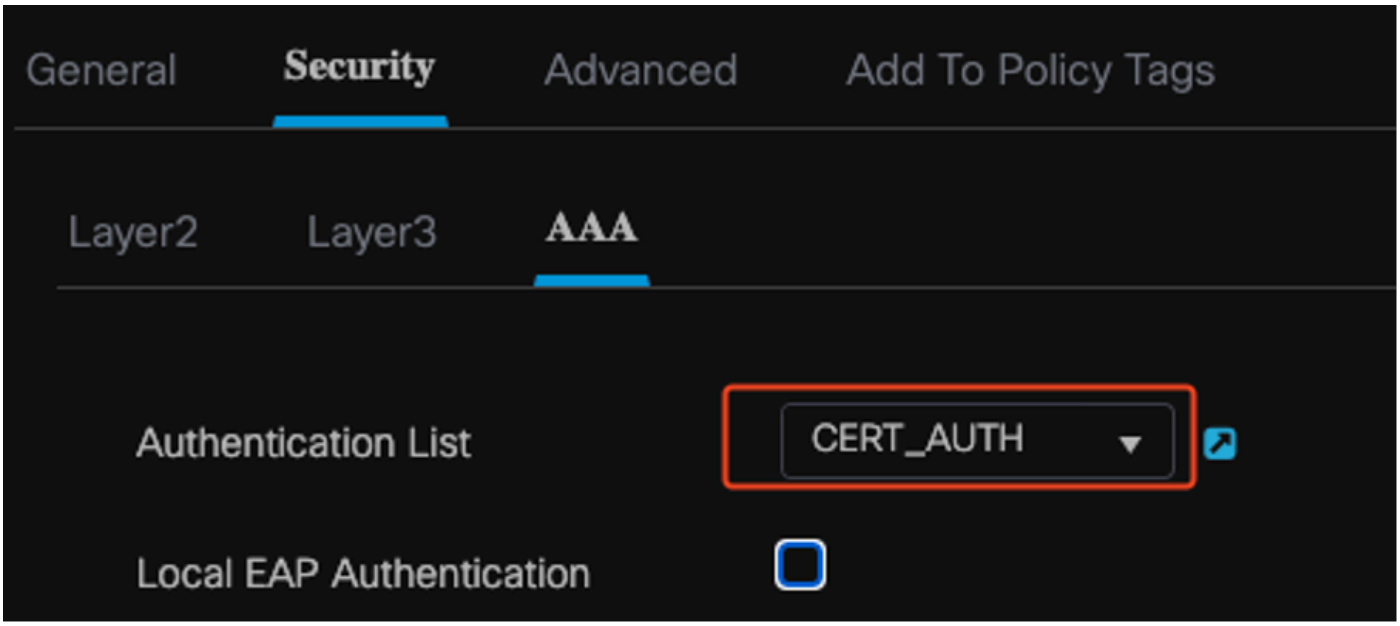
Per configurare una nuova WLAN con autenticazione 802.1x, attenersi alla seguente procedura:

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

3. Selezionare le impostazioni di autenticazione di layer 2 e abilitare l'autenticazione 802.1x.



Configurazione del profilo WLAN

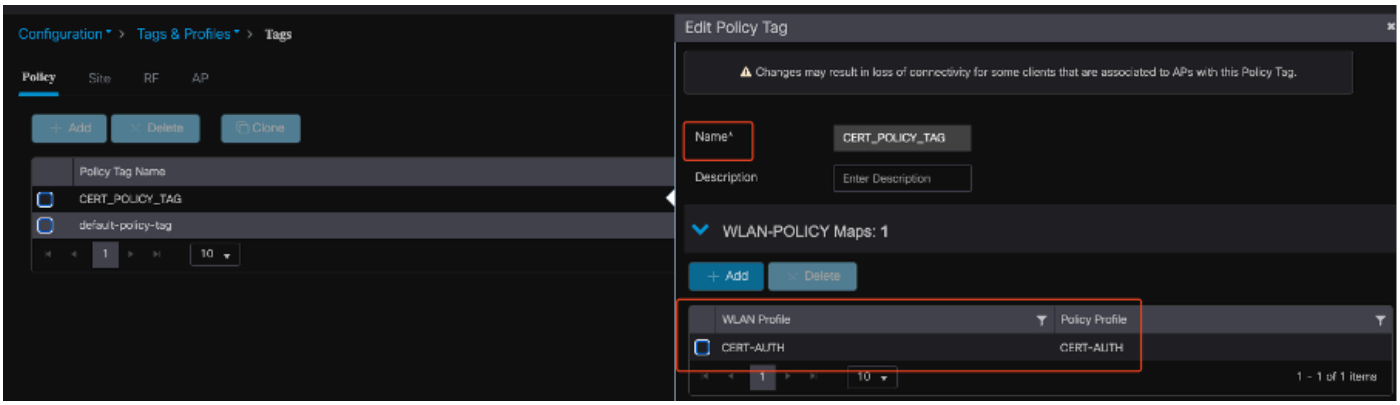


Mappa da profilo WLAN a elenco metodi

Mappa WLAN con profilo criterio su 9800 WLC

Per associare la WLAN a un profilo di criteri, eseguire la procedura seguente:

1. Selezionare Configurazione > Tag e profili > Tag.
2. Fare clic su Add (Aggiungi) per aggiungere un nuovo tag.
3. Nella sezione WLAN-POLICY, mappare la WLAN appena creata al profilo della policy appropriato.

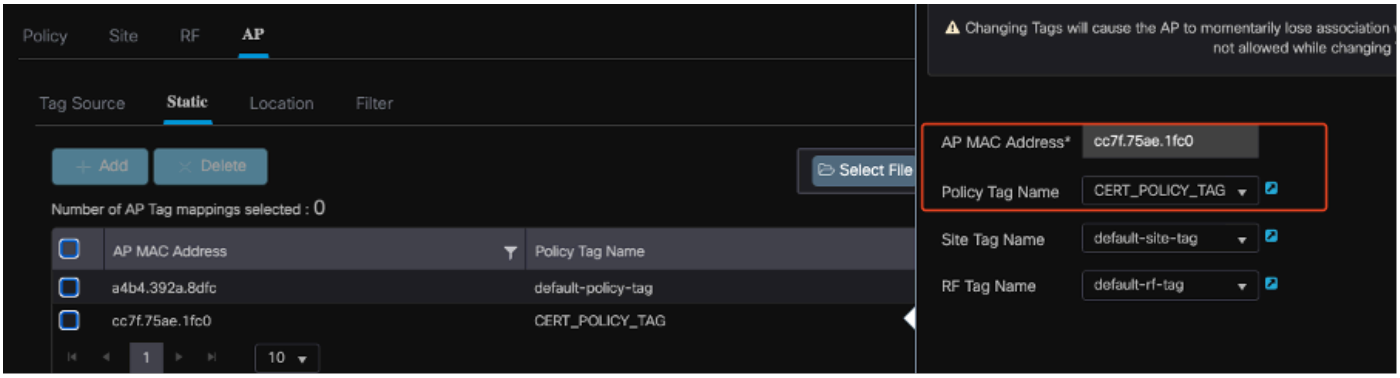


Configurazione del tag di policy

Mappa il tag criteri al punto di accesso su 9800 WLC

Per assegnare il tag di criterio a un punto di accesso, attenersi alla seguente procedura:

1. Selezionare Configurazione > Tag e profili > Tag > punto di accesso.
2. Andare alla sezione Static all'interno della configurazione AP.
3. Fare clic sull'access point specifico da configurare.
4. Assegnare il tag di criterio creato al punto di accesso selezionato.



Assegnazione tag PA

Esecuzione della configurazione del WLC dopo il completamento dell'installazione

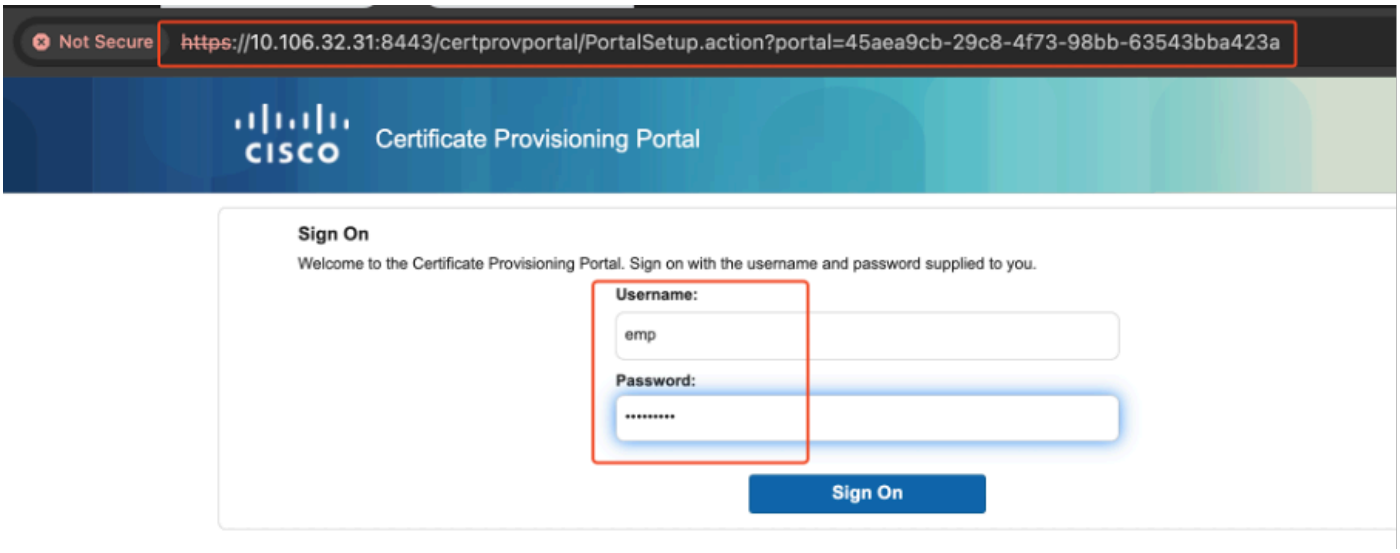
```
aaa group server radius ISE
 server name ISE3
 ip radius source-interface Vlan2124
aaa authentication dot1x CERT_AUTH group ISE
aaa authorization network CERT_AUTH group ISE
aaa server radius dynamic-author
 client 10.106.32.31 server-key Cisco!123
!

wireless profile policy CERT-AUTH
 aaa-override
 ipv4 dhcp required
 vlan 2124
 no shutdown
 wlan CERT-AUTH policy CERT-AUTH
wlan CERT-AUTH 17 CERT-AUTH
```

```
 security dot1x authentication-list CERT_AUTH
 no shutdown
!
wireless tag policy CERT_POLICY_TAG
 wlan CERT-AUTH policy CERT-AUTH
```

Crea e scarica il certificato per l'utente

Per creare e scaricare un certificato per un utente, eseguire la procedura seguente:

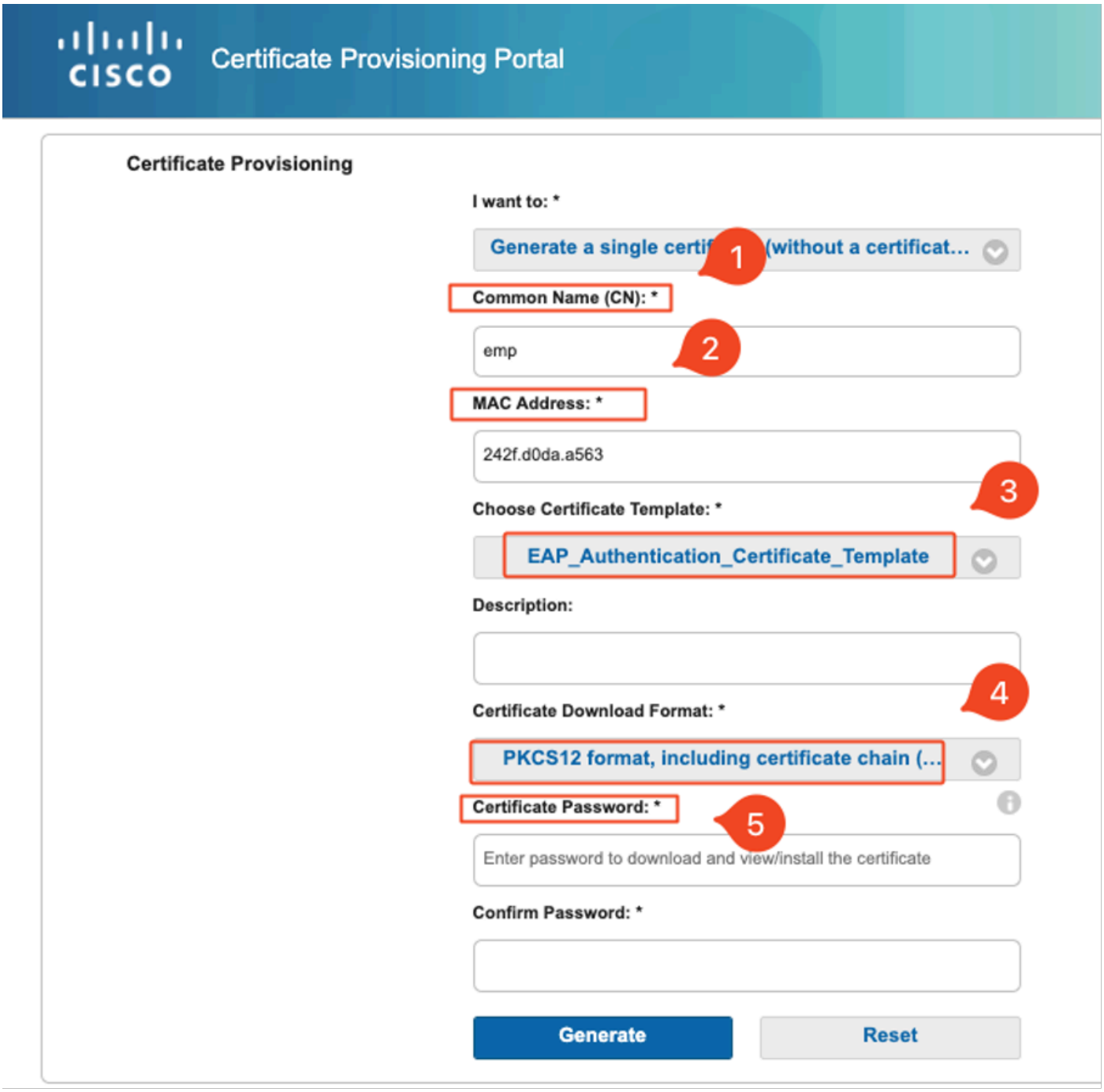
1. Chiedere all'utente di accedere al portale certificati configurato in precedenza.



Accesso al portale certificati

2. Accettare la politica d'uso accettabile (AUP). L'ISE quindi presenta una pagina per la generazione del certificato.

3. Selezionare Genera un singolo certificato (senza una richiesta di firma del certificato).



Generazione del certificato

Per generare un certificato tramite il portale di provisioning dei certificati, verificare che i seguenti campi obbligatori siano compilati:

- CN: Il server di autenticazione utilizza il valore presente nel campo Nome comune nel certificato client per autenticare un utente. Nel campo Nome comune immettere il nome utente utilizzato per accedere al portale di provisioning dei certificati.
- Indirizzo MAC: Nomi alternativi soggetto (SAN, Subject Alternative Names) è un'estensione X.509 che consente l'associazione di vari valori a un certificato di protezione. Cisco ISE, release 2.0 supporta solo indirizzi MAC. Quindi, nel campo dell'indirizzo SAN/MAC.
    - Modello di certificato: Il modello di certificato definisce un set di campi utilizzati dalla CA per convalidare una richiesta e rilasciare un certificato. Campi quali il nome comune (CN) vengono utilizzati per convalidare la richiesta (CN deve corrispondere al

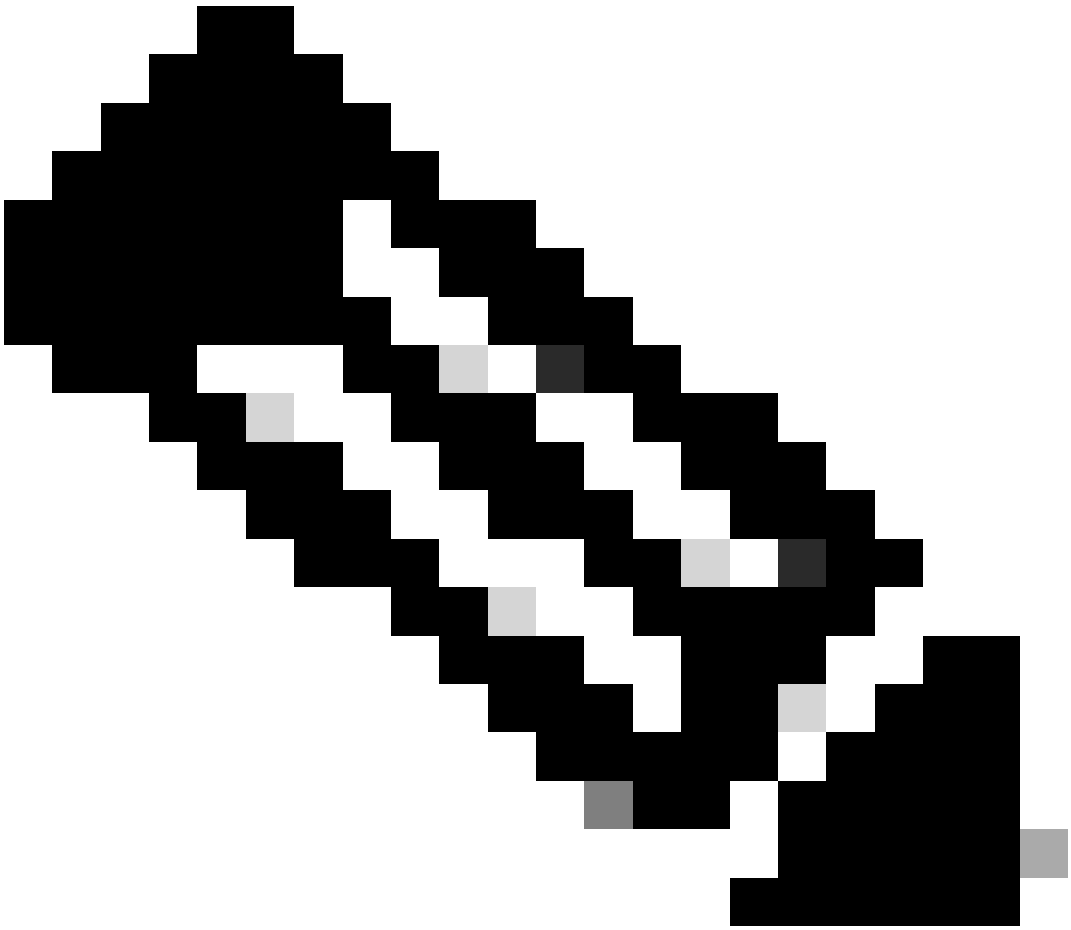
nome utente). Altri campi vengono utilizzati dalla CA durante il rilascio del certificato.

- Password certificato: Per proteggere il certificato è necessaria una password. È necessario specificare la password del certificato per visualizzare il contenuto del certificato e per importare il certificato in un dispositivo.
- La password deve essere conforme alle seguenti regole:
- La password deve contenere almeno una lettera maiuscola, una lettera minuscola e una cifra
    - La password deve contenere da 8 a 15 caratteri
    - I caratteri consentiti includono A-Z, a-z, 0-9, _, #

Una volta compilati tutti i campi, selezionare Genera per creare e scaricare il certificato.

Installazione certificato su un computer con Windows 10

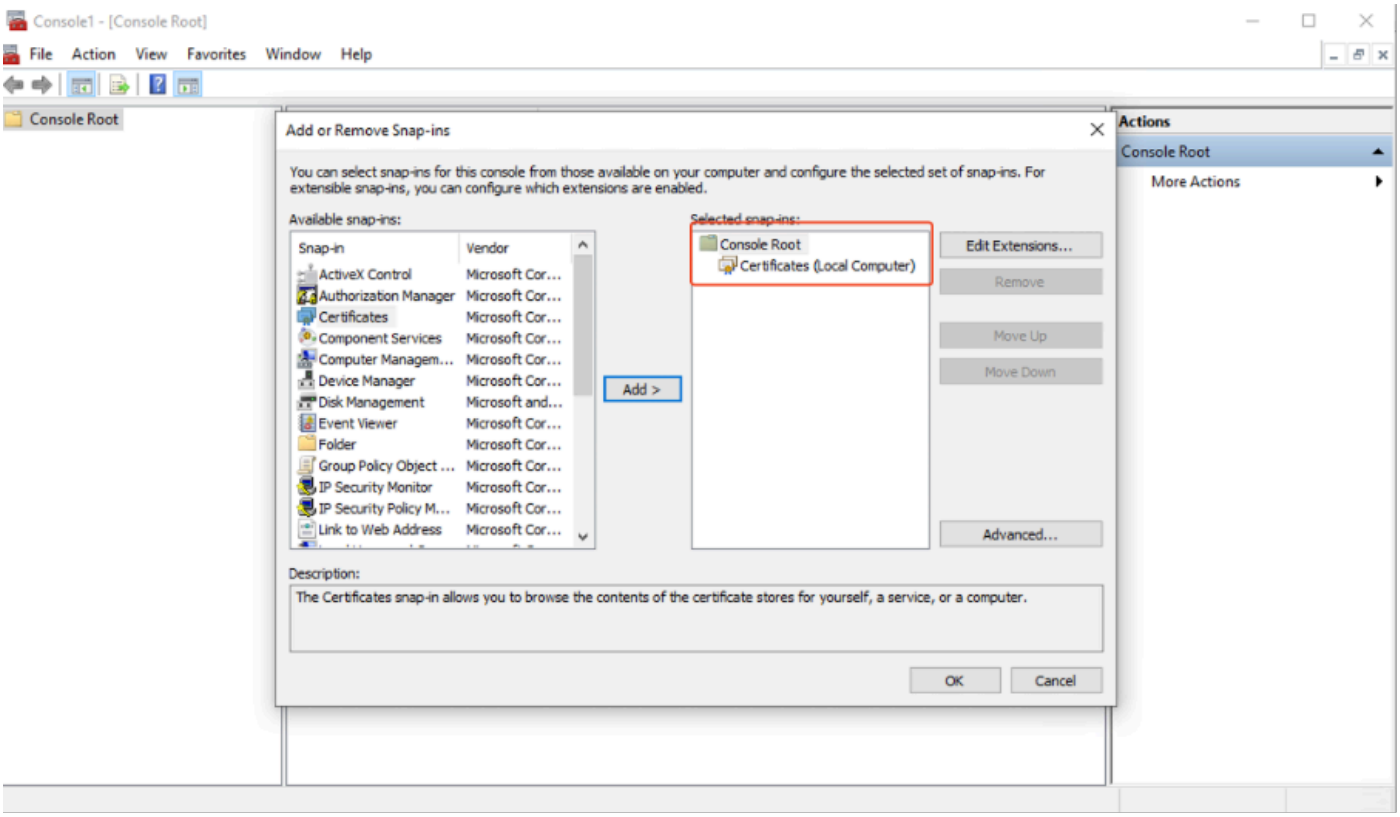
Per installare un certificato in un computer Windows 10, aprire Microsoft Management Console (MMC) eseguendo la procedura seguente:



Nota: Poiché queste istruzioni possono variare in base all'installazione di Windows, si consiglia di consultare la documentazione di Microsoft per informazioni specifiche.

1. Fare clic su Start e quindi su Esegui.
2. Digitare mmc nella casella Esegui e premere Invio. Verrà aperta Microsoft Management Console.
3. Aggiungi snap-in certificato:
4. Selezionare File > Aggiungi/Rimuovi snap-in.
5. Selezionare Aggiungi, quindi scegliere Certificati e fare clic su Aggiungi.
6. Selezionare Account computer, quindi Computer locale e fare clic su Fine.

Questa procedura consente di gestire i certificati nel computer locale.



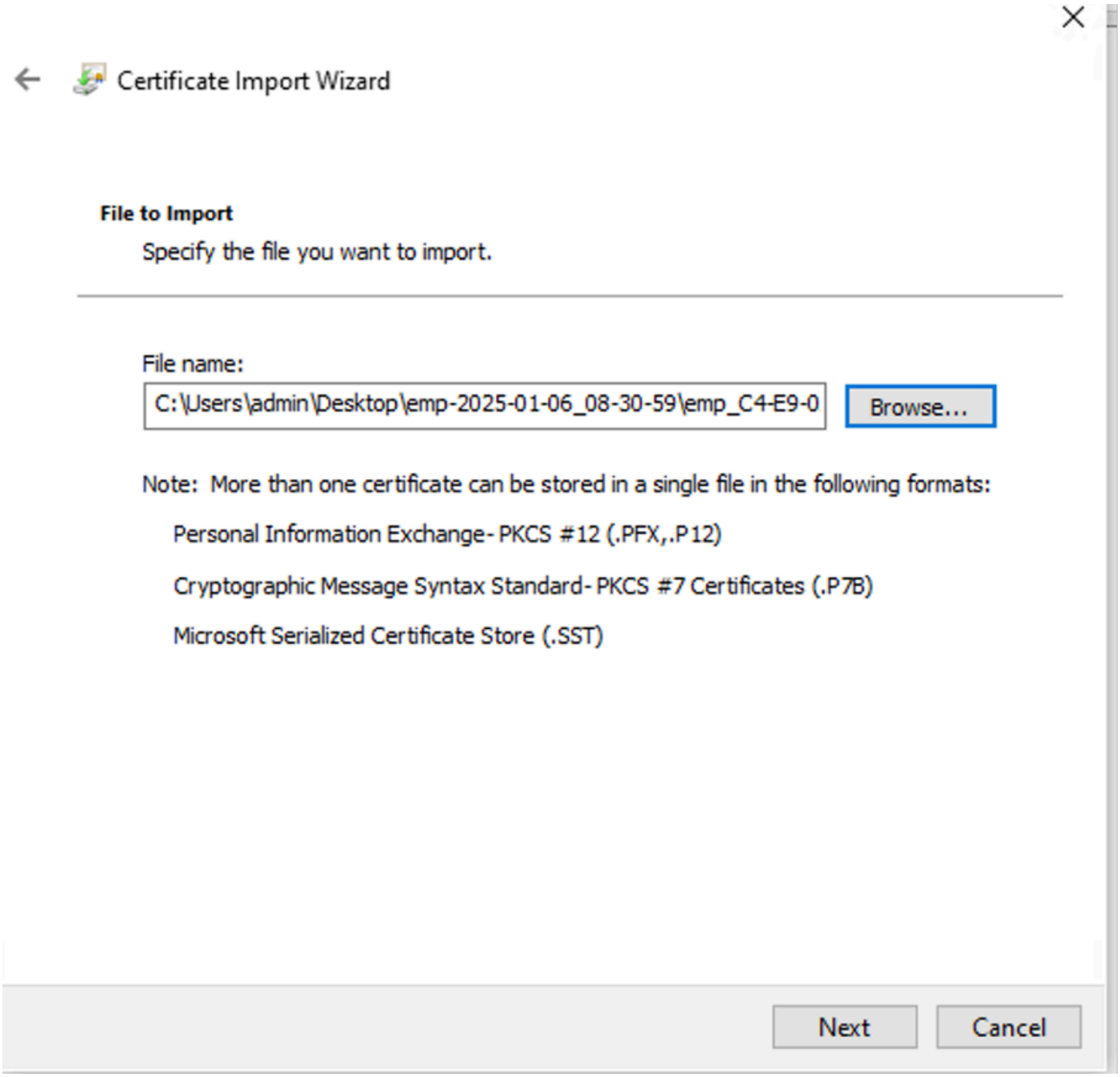
Console MMC di Windows

Passaggio 1. Importare il certificato:

1.1. Fare clic su Azione nel menu.

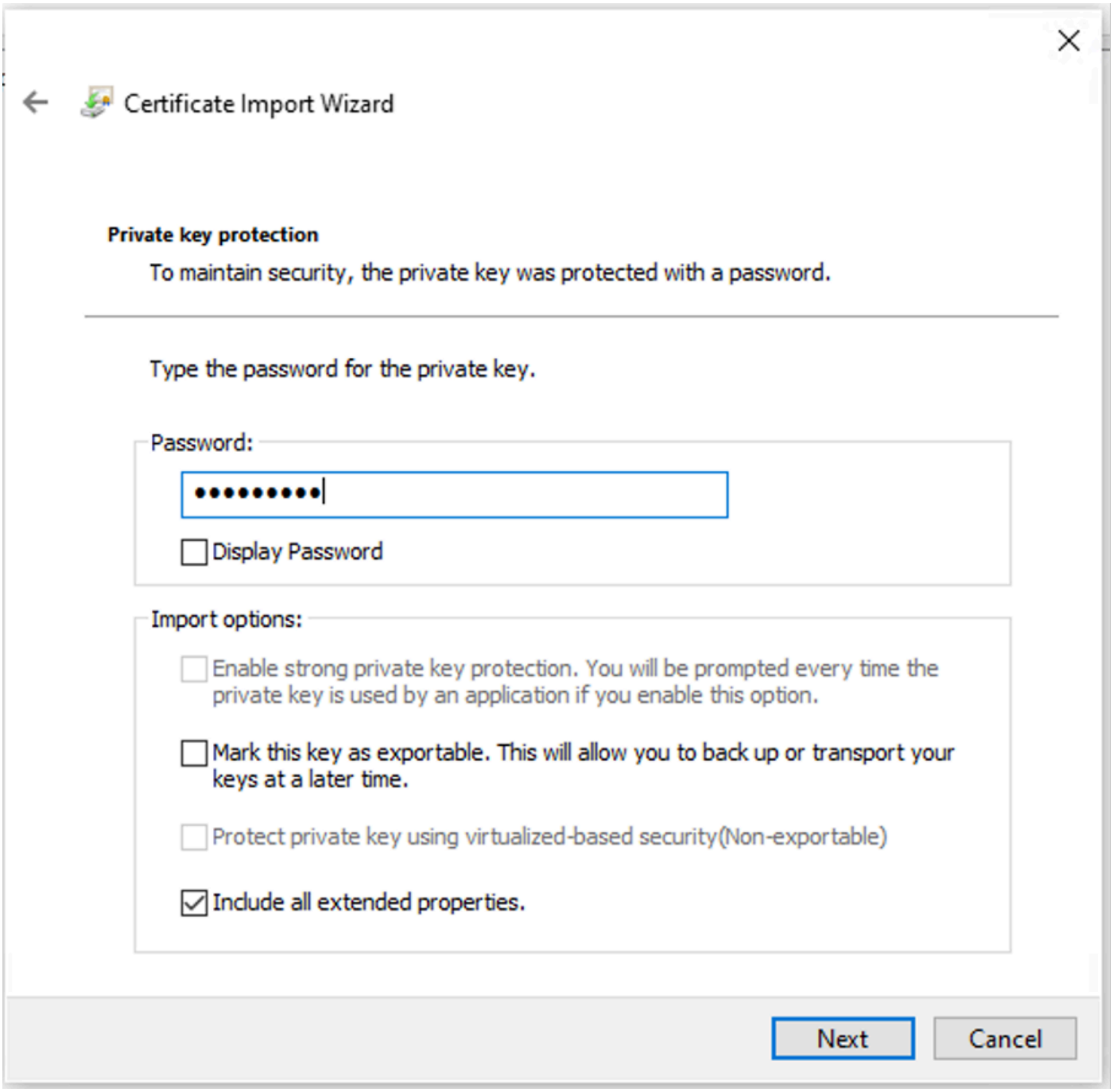
1.2. Andare a Tutte le attività, quindi selezionare Importa.

1.3. Procedere attraverso le richieste per individuare e selezionare il file di certificato archiviato nel computer.



Importazione del certificato

Durante il processo di importazione del certificato, viene richiesto di immettere la password creata durante la generazione del certificato nel portale. Assicurarsi di immettere questa password in modo corretto per importare e installare il certificato nel computer.



Immissione della password del certificato

Passaggio 2. Spostare i certificati nelle cartelle appropriate:

2.1. Aprire Microsoft Management Console (MMC) e selezionare la cartella Certificati (Computer locale) > Personale.

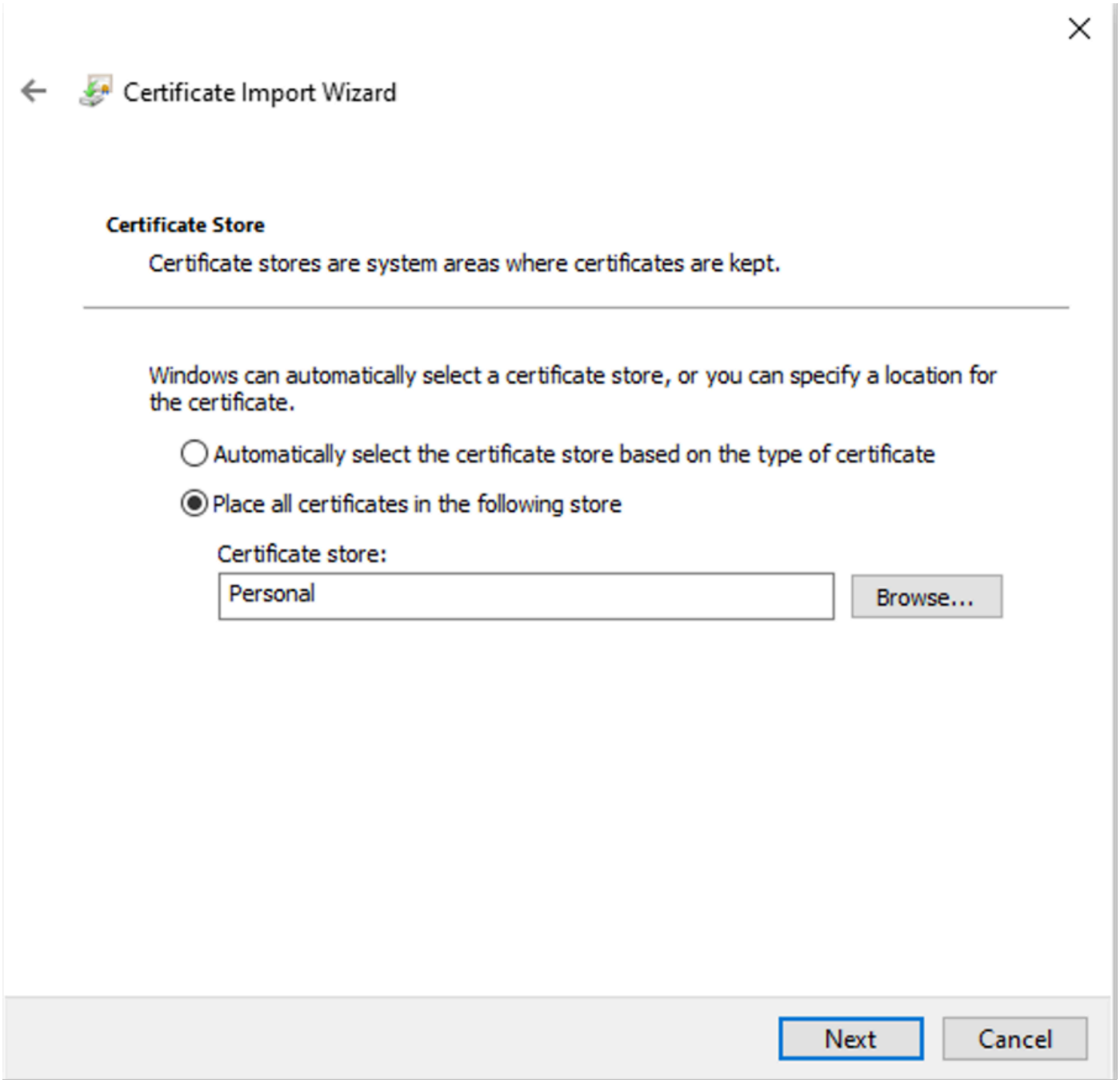
2.2. Esaminare i certificati e determinarne i tipi (ad esempio, CA radice, CA intermedia o personale).

2.3. Spostare ciascun certificato nell'archivio appropriato:

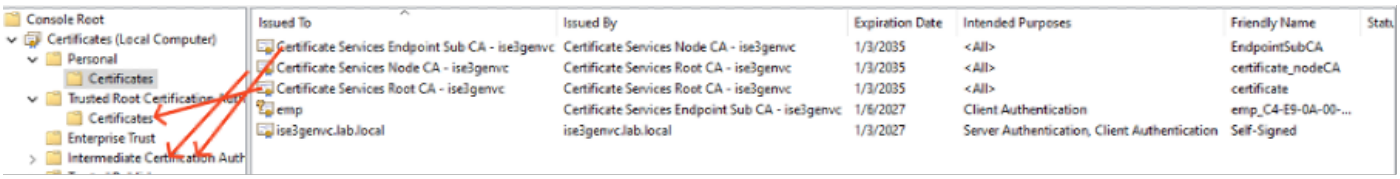
2.4. Certificati CA radice: Passare ad Autorità di certificazione radice attendibili.

2.5. Certificati CA intermedi: Passare alle Autorità di certificazione intermedie.

2.6. Certificati personali: Lasciare nella cartella Personale.



Archiviazione dei certificati nella cartella personale

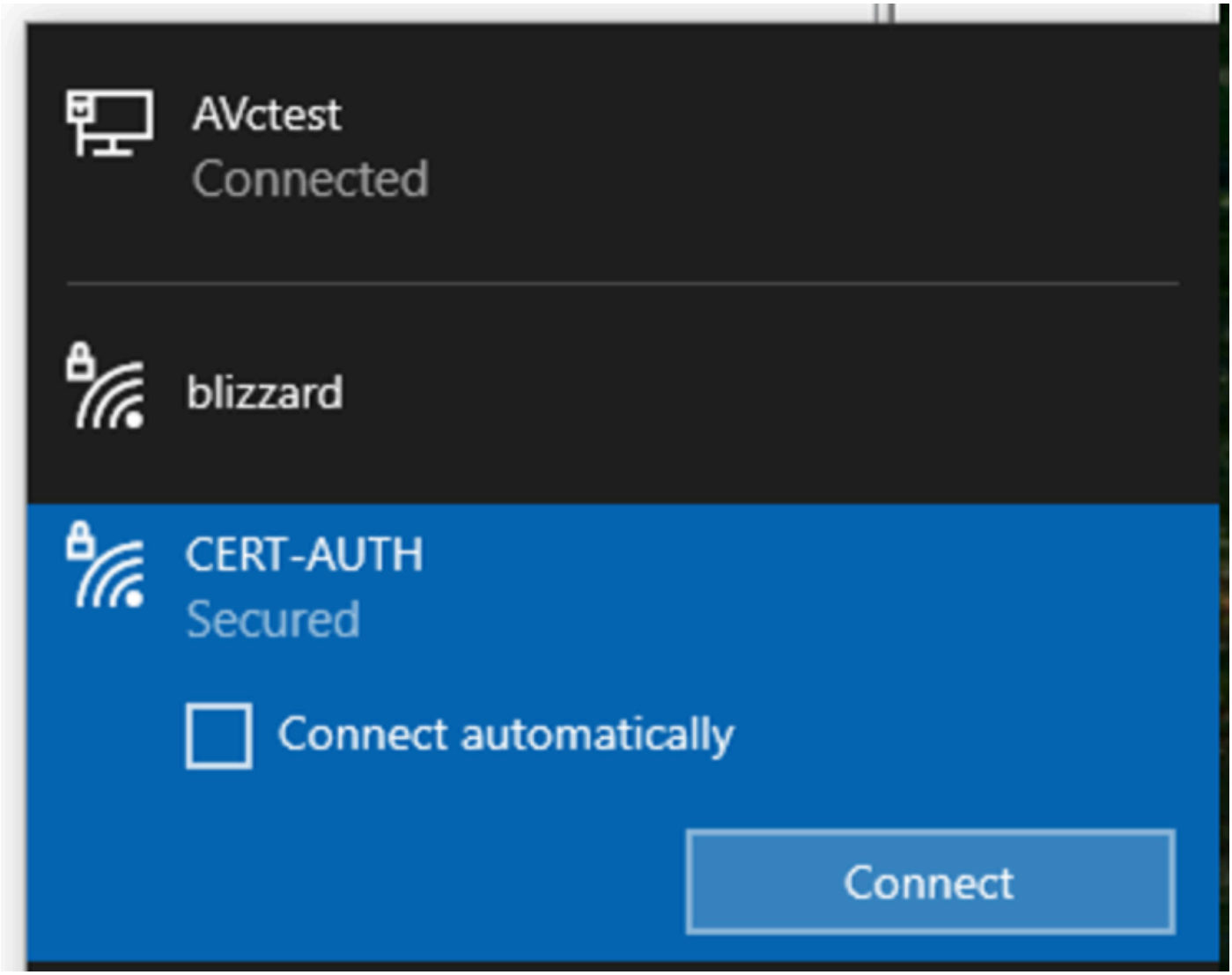


Spostamento dei certificati nei relativi archivi

Collegamento del computer Windows

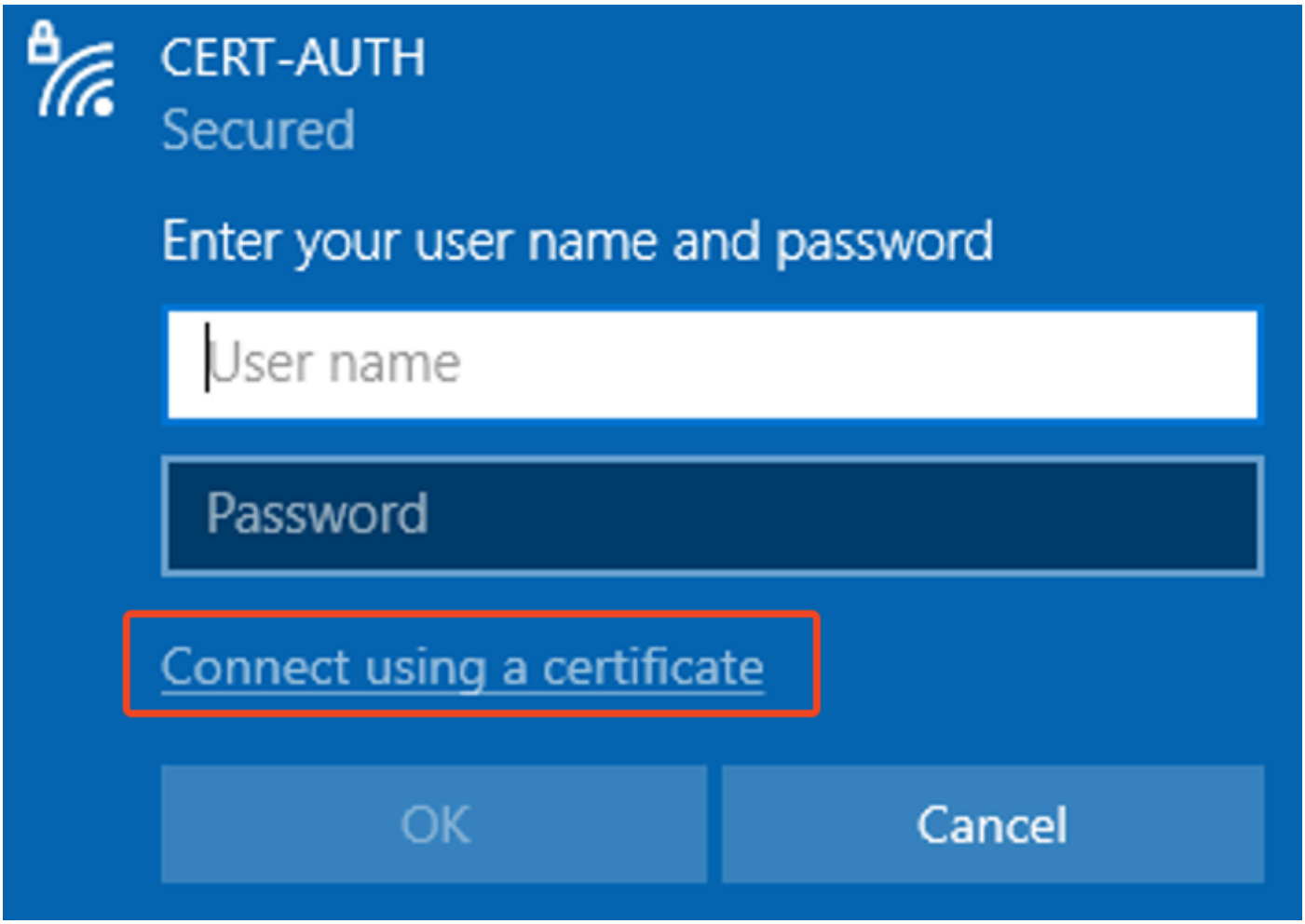
Dopo aver spostato i certificati negli archivi corretti, eseguire la procedura seguente per connettersi alla WLAN:

1. Per visualizzare le reti wireless disponibili, fare clic sull'icona rete nella barra delle applicazioni.
2. Trova e fai clic sul nome della WLAN a cui vuoi connetterti.
3. Fare clic su Connetti e continuare con eventuali richieste aggiuntive per completare il processo di connessione utilizzando il certificato per l'autenticazione.



Connessione alla rete wireless

Quando richiesto durante il processo di connessione alla WLAN, selezionare l'opzione per la connessione utilizzando un certificato.



Utilizzo del certificato come credenziale

In questo modo è possibile connettersi alla rete wireless utilizzando il certificato.

```
C:\>netsh wlan  show interface

There is 1 interface on the system:

    Name                   : Wi-Fi 3
    Description            : TP-Link Wireless USB Adapter
    GUID                   : ee5d1c47-43cc-4873-9ae6-99e2e43c39ea
    Physical address       : 24:2f:d0:da:a5:63
    State                  : connected
    SSID                   : CERT-AUTH
    BSSID                  : a4:88:73:9e:8d:af
    Network type           : Infrastructure
    Radio type             : 802.11ac
    Authentication         : WPA2-Enterprise
    Cipher                 : CCMP
    Connection mode        : Profile
    Channel                : 36
    Receive rate (Mbps)    : 360
    Transmit rate (Mbps)   : 360
    Signal                 : 100%
    Profile                : CERT-AUTH

    Hosted network status  : Not available


C:\>netsh wlan show profiles CERT-AUTH | find "Smart"
    EAP type               : Microsoft: Smart Card or other certificate
```

Verifica profilo wireless

Verifica

Verificare che la WLAN sia trasmessa dal WLC:

<#root>

```
POD6_9800#show wlan summ
Number of WLANs: 2
ID Profile Name SSID Status Security
-----------------------------------------------------------------------------------------------------------------
```

17

CERT-AUTH

CERT-AUTH

UP [WPA2][802.1x][AES]

Verificare che l'access point sia attivo sul WLC:

```
POD6_9800#show ap summ
Number of APs: 1
CC = Country Code
RD = Regulatory Domain
AP Name Slots AP Model Ethernet MAC Radio MAC CC RD IP Address State Location
-------------------------------------------------------------------------------------------------
AP1 3 C9130AXI-D cc7f.75ae.1fc0 a488.739e.8da0 IN -D 10.78.8.78 Registered default location
```

Verificare che l'access point stia trasmettendo la WLAN:

<#root>

```
POD6_9800#show ap name AP1 wlan dot11 24ghz
Slot id : 0
WLAN ID BSSID
------------------------
17 a488.739e.8da0

POD6_9800#show ap name AP1 wlan dot11 5ghz
Slot id : 1
WLAN ID BSSID
------------------------
```

17

```
 a488.739e.8daf
```

Client connesso tramite EAP-TLS:

<#root>

```
POD6_9800#show wire cli summ
Number of Clients: 1
MAC Address AP Name Type ID State Protocol Method Role
-----------------------------------------------------------------------------------------------------
242f.d0da.a563 AP1 WLAN
```

17

```
 IP Learn 11ac
```

Dot1x

```
 Local

POD6_9800#sho wireless client mac-address 242f.d0da.a563 detail | in username|SSID|EAP|AAA|VLAN
```

Wireless LAN Network Name (SSID): CERT-AUTH

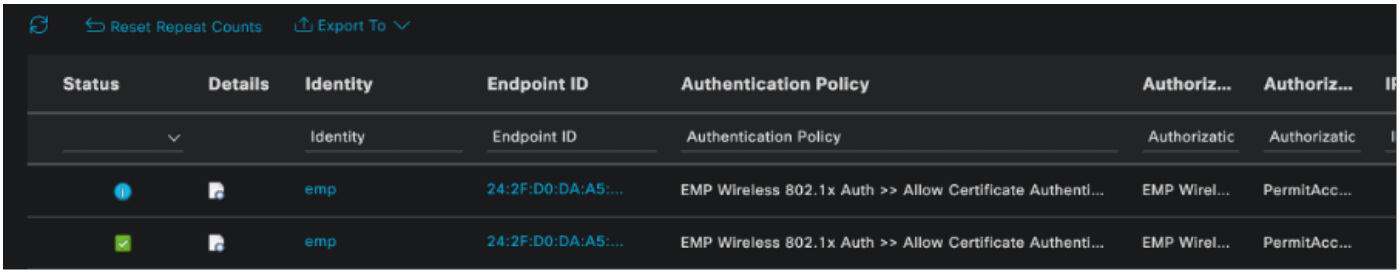
```
BSSID : a488.739e.8daf
```

EAP Type : EAP-TLS

```
VLAN : 2124
Multicast VLAN : 0
```

VLAN : 2124

Log live Cisco Radius ISE:

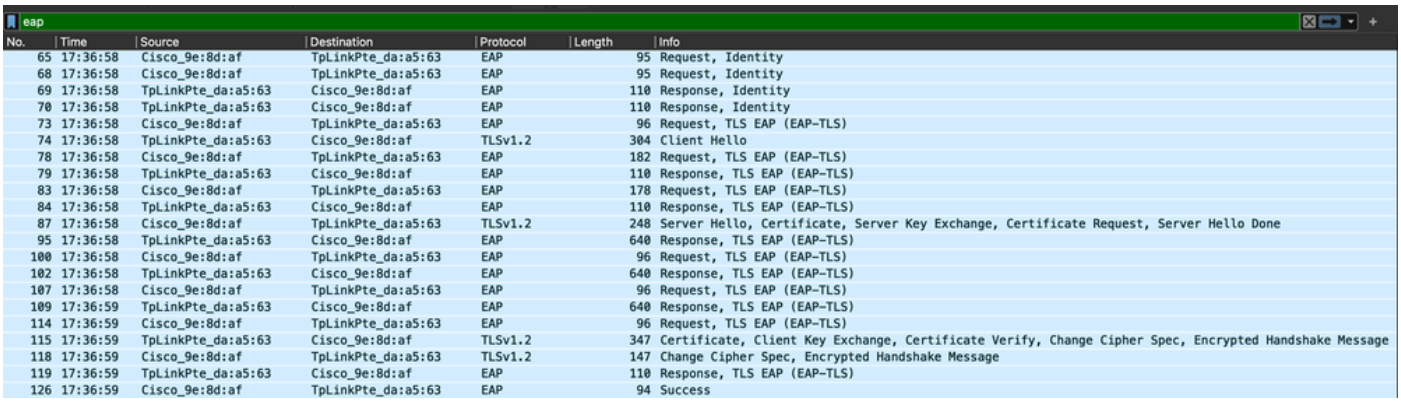


Registri live ISE Radius

Tipo di autenticazione dettagliata:

Log dettagliati ISE

WLC EPC Capture con i pacchetti EAP-TLS:



eap

No.	Time	Source	Destination	Protocol	Length	Info
65	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity
68	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity
69	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity
70	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity
73	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
74	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLSv1.2	304	Client Hello
78	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	182	Request, TLS EAP (EAP-TLS)
79	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
83	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	178	Request, TLS EAP (EAP-TLS)
84	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
87	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLSv1.2	248	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
95	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
100	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
102	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
107	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
109	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
114	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
115	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLSv1.2	347	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
118	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLSv1.2	147	Change Cipher Spec, Encrypted Handshake Message
119	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
126	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	94	Success

Acquisizione WLC che mostra la transazione EAP

- Il numero di pacchetto 87 corrisponde al passaggio 8 nel flusso EAP-TLS descritto all'inizio del documento.
- Il numero di pacchetto 115 corrisponde al passaggio 9 nel flusso EAP-TLS descritto all'inizio del documento.
- Il numero di pacchetto 118 corrisponde al passaggio 10 nel flusso EAP-TLS descritto all'inizio del documento.

Traccia Radio Active (RA) con connessione client: Questa traccia dell'Autorità registrazione è filtrata per visualizzare alcune delle righe rilevanti della transazione di autenticazione.

2025/01/08 11 58 20.816875191 {wncd_x_R0-2}{1} [ewlc-capwapmsg-sess] [15655] (debug) Invio di messaggi DTLS crittografati. Dest IP 10.78.8.78[5256], lunghezza 499
2025/01/08 11 58 20.851392112 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Invia richiesta di accesso a 10.106.33.23 1812 id 0/25, len 390
2025/01/08 11 58 20.871842938 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Ricevuto da id 1812/25 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.872246323 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Inviato pacchetto EAPOL - Versione 3,EAPOL Tipo EAP, Payload Lunghezza 6, EAP-Tipo = EAP LS
2025/01/08 11 58 20.881960763 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Ricevuto pacchetto EAPOL - Versione 1,EAPOL Tipo EAP, Payload Lunghezza 204, EAP-Type = EAP-TLS
2025/01/08 11 58 20.882292551 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Invia richiesta di accesso a 10.106.33.23 1812 id 0/26, len 663
2025/01/08 11 58 20.926204990 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Ricevuto da id 1812/26 10.106.33.23 0, Access-Challenge, len 1135
2025/01/08 11 58 20.927390754 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Inviato pacchetto EAPOL - Versione 3,EAPOL Tipo EAP, Lunghezza payload 1012, EAP Tipo = EAP-TLS
2025/01/08 11 58 20.935081108 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Ricevuto pacchetto EAPOL - Versione 1,EAPOL Tipo EAP, Payload Lunghezza 6, EAP-Tipo = EAP LS
2025/01/08 11 58 20.935405770 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Invia richiesta di accesso a 10.106.33.23 1812 id 0/27, len 465
2025/01/08 11 58 20.938485635 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Ricevuto da id

1812/27 10.106.33.23 0, Access-Challenge, len 1131
2025/01/08 11 58 20.939630108 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Inviato pacchetto EAPOL - Versione 3,EAPOL Tipo EAP, Lunghezza payload 1008, EAP Tipo = EAP-TLS
2025/01/08 11 58 20.947417061 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Ricevuto pacchetto EAPOL - Versione 1,EAPOL Tipo EAP, Payload Lunghezza 6, EAP-Tipo = EAP LS
2025/01/08 11 58 20.947722851 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Invia richiesta di accesso a 10.106.33.23 1812 id 0/28, len 465
2025/01/08 11 58 20.949913199 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Ricevuto da id 1812/28 10.106.33.23 0, Access-Challenge, len 275
2025/01/08 11 58 20.950432303 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Inviato pacchetto EAPOL - Versione 3,EAPOL Tipo EAP, Lunghezza payload 158, Tipo EAP EAP-TLS
2025/01/08 11 58 20.966862562 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Ricevuto pacchetto EAPOL - Versione 1,EAPOL Tipo EAP, Lunghezza payload 1492, EAP Tipo = EAP-TLS
2025/01/08 11 58 20.967209224 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Invia richiesta di accesso a 10.106.33.23 1812 id 0/29, len 1961
2025/01/08 11 58 20.971337739 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Ricevuto da id 1812/29 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.971708100 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Inviato pacchetto EAPOL - Versione 3,EAPOL Tipo EAP, Payload Lunghezza 6, EAP-Tipo = EAP LS
2025/01/08 11 58 20.978742828 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Ricevuto pacchetto EAPOL - Versione 1,EAPOL Tipo EAP, Lunghezza payload 1492, EAP Tipo = EAP-TLS
2025/01/08 11 58 20.979081544 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Invia richiesta di accesso a 10.106.33.23 1812 id 0/30, len 1961
2025/01/08 11 58 20.982535977 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Ricevuto da id 1812/30 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.982907200 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Inviato pacchetto EAPOL - Versione 3,EAPOL Tipo EAP, Payload Lunghezza 6, EAP-Tipo = EAP LS
2025/01/08 11 58 20.990141062 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Ricevuto pacchetto EAPOL - Versione 1,EAPOL Tipo EAP, Lunghezza payload 1492, EAP Tipo = EAP-TLS
2025/01/08 11 58 20.990472026 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Invia richiesta di accesso a 10.106.33.23 1812 id 0/31, len 1961
2025/01/08 11 58 20.994358525 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Ricevuto da id 1812/31 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.994722151 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Inviato pacchetto EAPOL - Versione 3,EAPOL Tipo EAP, Payload Lunghezza 6, EAP-Tipo = EAP LS
2025/01/08 11 58 21.00173553 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Ricevuto pacchetto EAPOL - Versione 1,EAPOL Tipo EAP, Lunghezza

payload 247, EAP-Type = EAP-TLS
2025/01/08 11 58 21.002076369 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Invia richiesta di accesso a 10.106.33.23 1812 id 0/32, len 706
2025/01/08 11 58 21.013571608 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Ricevuto da id 1812/32 10.106.33.23 0, Access-Challenge, len 174
2025/01/08 11 58 21.013987785 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Inviato pacchetto EAPOL - Versione 3,EAPOL Tipo EAP, Payload Lunghezza 57, EAP-Type = EAP -TLS
2025/01/08 11 58 21.024429150 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Ricevuto pacchetto EAPOL - Versione 1,EAPOL Tipo EAP, Payload Lunghezza 6, EAP-Type = EAP LS
2025/01/08 11 58 21.024737996 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Invia richiesta di accesso a 10.106.33.23 1812 id 0/33, len 465
2025/01/08 11 58 21.057794929 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Ricevuto da id 1812/33 10.106.33.23 0, Access-Accept, len 324
2025/01/08 11 58 21.058149893 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Generato evento di aggiornamento identità per il metodo EAP-TLS

Risoluzione dei problemi

Per questo problema non sono disponibili procedure specifiche di risoluzione oltre a quelle tipiche per la risoluzione dei problemi di Wireless 802.1x:

1. Eseguire i debug di traccia RA del client per controllare il processo di autenticazione.
2. Eseguire un'acquisizione EPC WLC per esaminare i pacchetti tra il client, il WLC e il server RADIUS.
3. Controllare i log attivi ISE per verificare che la richiesta corrisponda al criterio corretto.
4. Verificare sull'endpoint di Windows che il certificato sia installato correttamente e che sia presente l'intera catena di attendibilità.

Riferimenti

- Domande frequenti sul portale di provisioning dei certificati, release 3.2
- Informazioni sui servizi ISE Internal Certificate Authority
- Comprensione e configurazione di EAP-TLS con WLC e ISE

Informazioni su questa traduzione

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