Comprensione e configurazione di EAP-TLS con WLC e ISE

Sommario

Introduzione

Questo documento descrive come configurare una rete WLAN (Wireless Local Area Network) con 802.1X e il protocollo di autenticazione estendibile EAP-TLS

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Processo di autenticazione 802.1X
- Certificati

Componenti usati

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

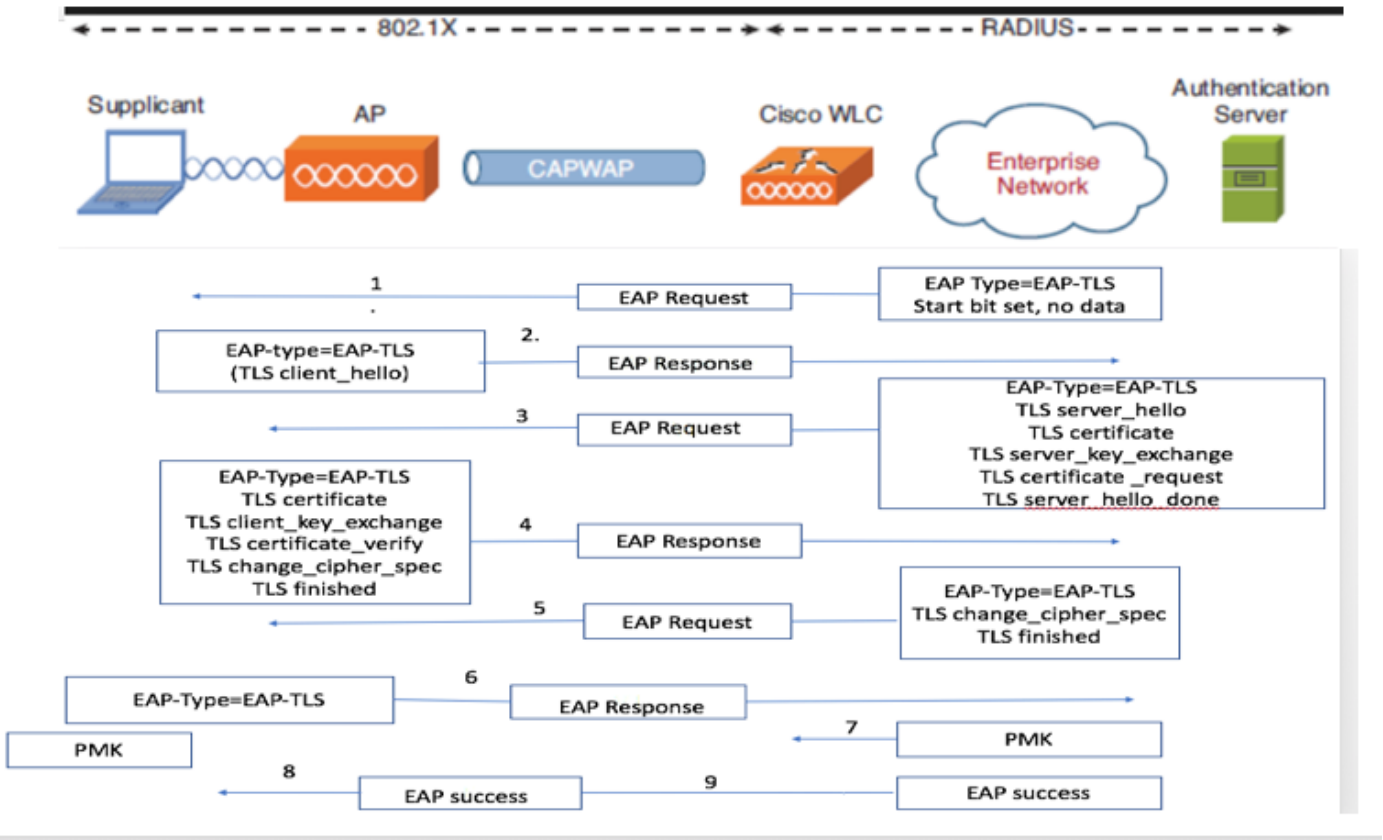
hardware:

- WLC 3504 versione 8.10
- Identity Services Engine (ISE) versione 2.7

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

Flusso EAP-TLS



Fasi del flusso EAP-TLS

1. Il client wireless viene associato al punto di accesso (AP). AP non consente al client di inviare dati a questo punto e invia una richiesta di autenticazione. Il richiedente risponde quindi con un'identità di risposta EAP. Il WLC comunica quindi le informazioni sull'ID utente al server di autenticazione. Il server RADIUS risponde al client con un pacchetto di avvio EAP-TLS. A questo punto inizia la conversazione EAP-TLS.
2. Il peer invia una risposta EAP al server di autenticazione che contiene un messaggio di handshake "client_hello", una cifratura impostata per NULL
3. Il server di autenticazione risponde con un pacchetto di richiesta di accesso contenente:

```
TLS server_hello
handshake message
certificate
```

```
server_key_exchange
certificate request
server_hello_done.
```

4. Il client risponde con un messaggio di risposta EAP che contiene:

```
Certificate ¬ Server can validate to verify that it is trusted.

client_key_exchange

certificate_verify ¬ Verifies the server is trusted

change_cipher_spec

TLS finished
```

5. Una volta completata l'autenticazione del client, il server RADIUS risponde con una richiesta di verifica di accesso contenente il messaggio "change_cipher_spec" e l'handshake completato.

6.Quando riceve questo messaggio, il client verifica l'hash per autenticare il server radius.

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

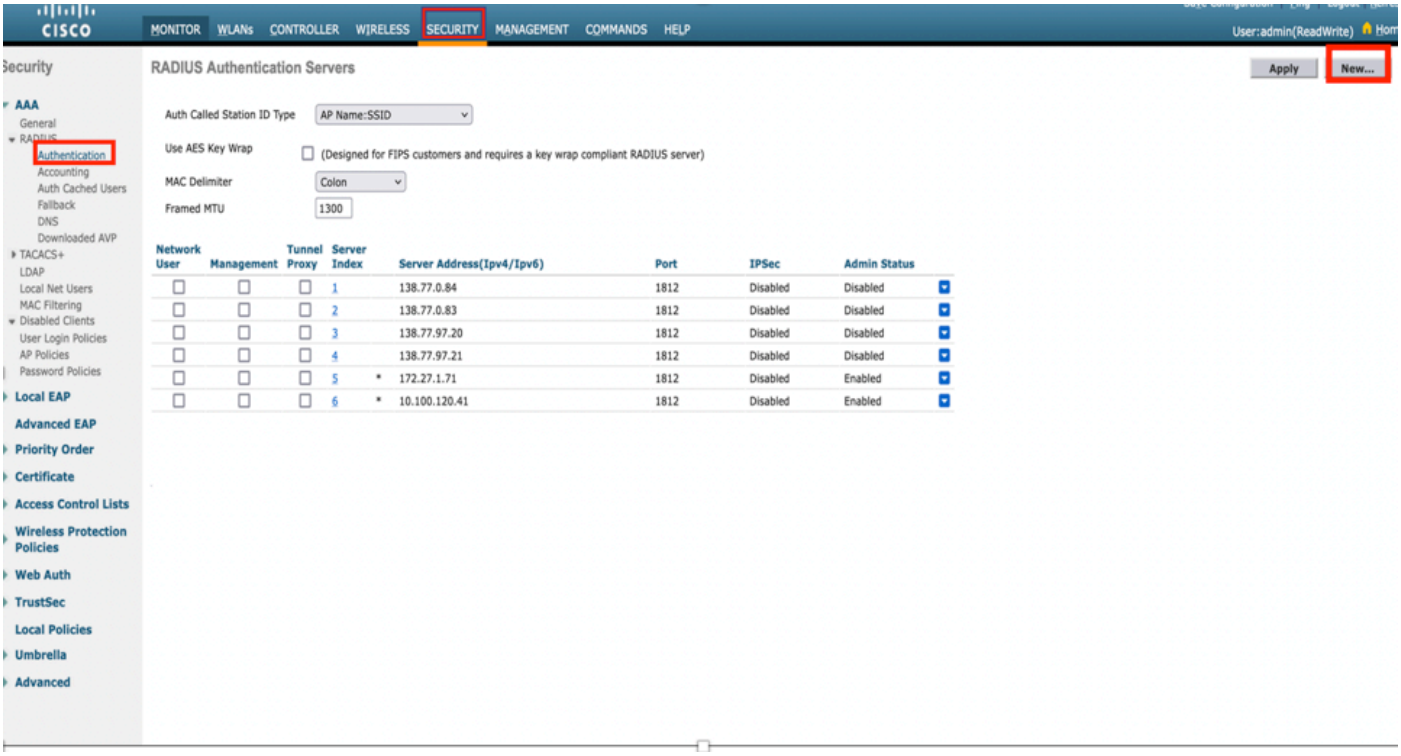
8/9.EAP-Success viene infine inviato dal server all'autenticatore che viene quindi passato al supplicant.

A questo punto, il client wireless abilitato per EAP-TLS può accedere alla rete wireless.

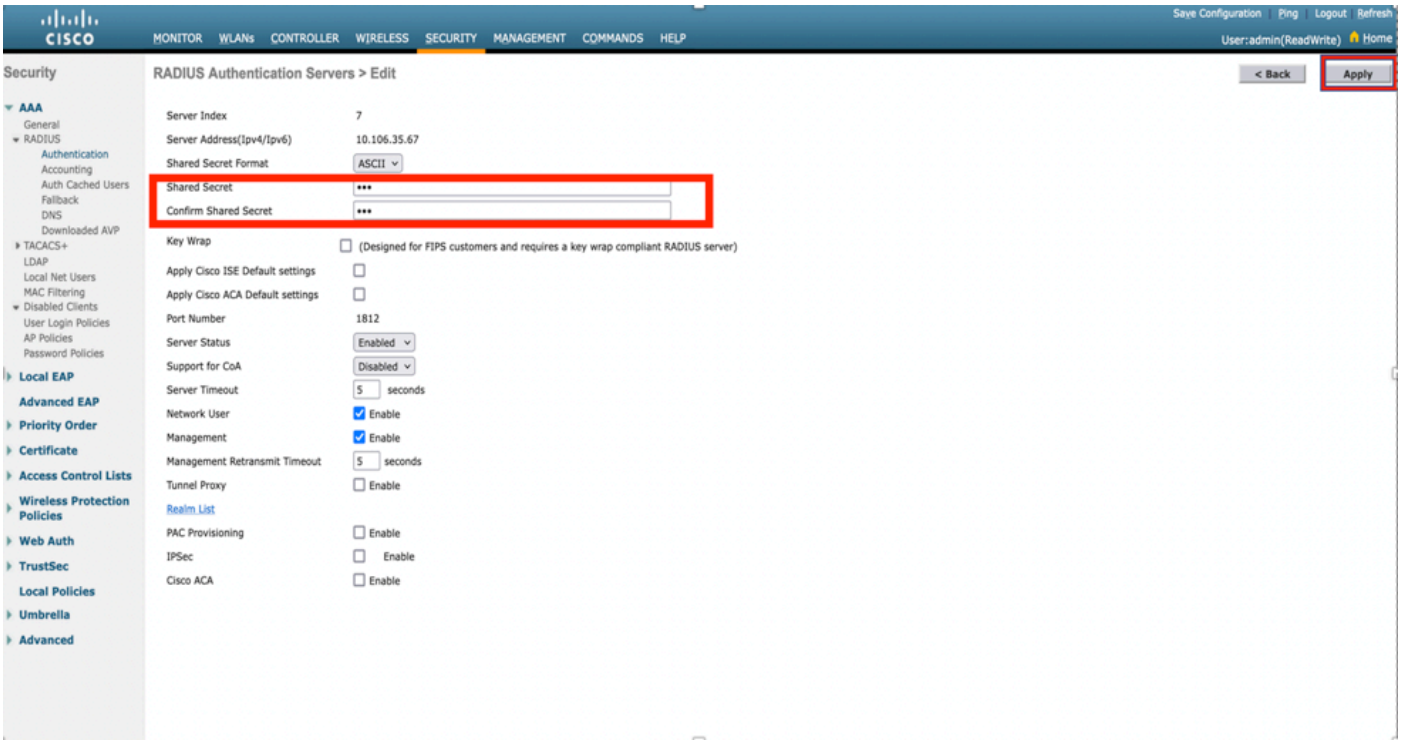
Configurazione

Cisco Wireless LAN Controller

Passaggio 1. Il primo passaggio consiste nella configurazione del server RADIUS sul WLC Cisco. Per aggiungere un server RADIUS, selezionare **Sicurezza > RADIUS > Autenticazione**. Fare clic su **New** (Nuovo) come mostrato nell'immagine.



Passaggio 2. Qui, è necessario immettere l'indirizzo IP e il segreto condiviso <password> usato per convalidare il WLC sull'ISE. Per continuare, fare clic su **Apply** (Applica) come mostrato nell'immagine.

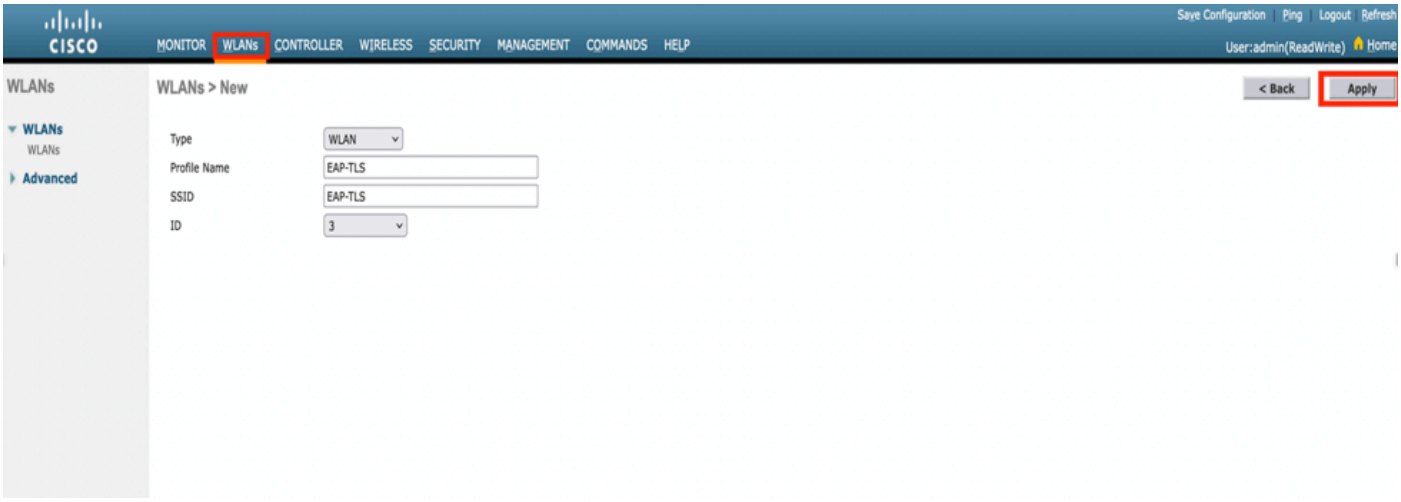


Passaggio 3. Creazione di una WLAN per l'autenticazione RADIUS.

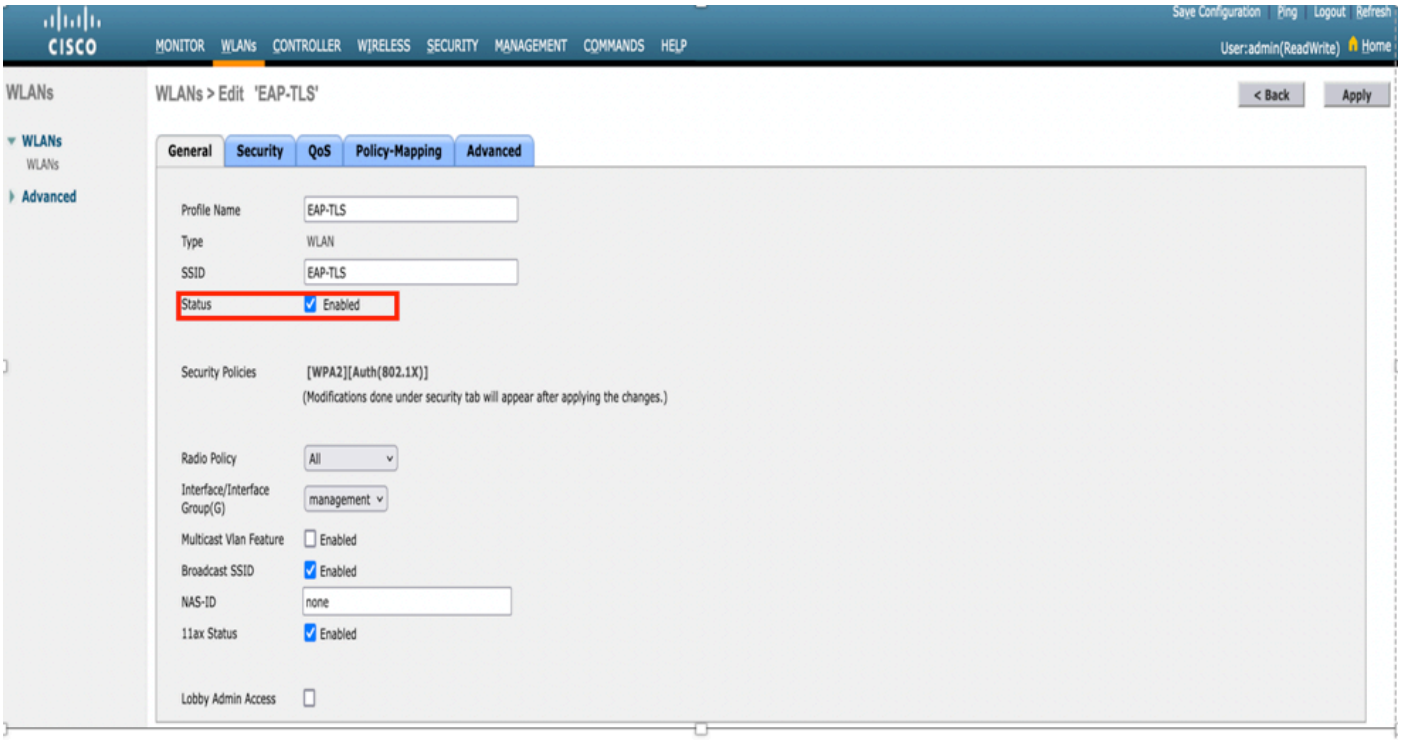
A questo punto è possibile creare una nuova WLAN e configurarla in modo che utilizzi la modalità WPA-enterprise, in modo che possa utilizzare RADIUS per l'autenticazione.

Passaggio 4. Selezionare **WLAN** dal menu principale, scegliere **Crea nuovo** e fare clic su **Go** (Vai), come mostrato nell'immagine.

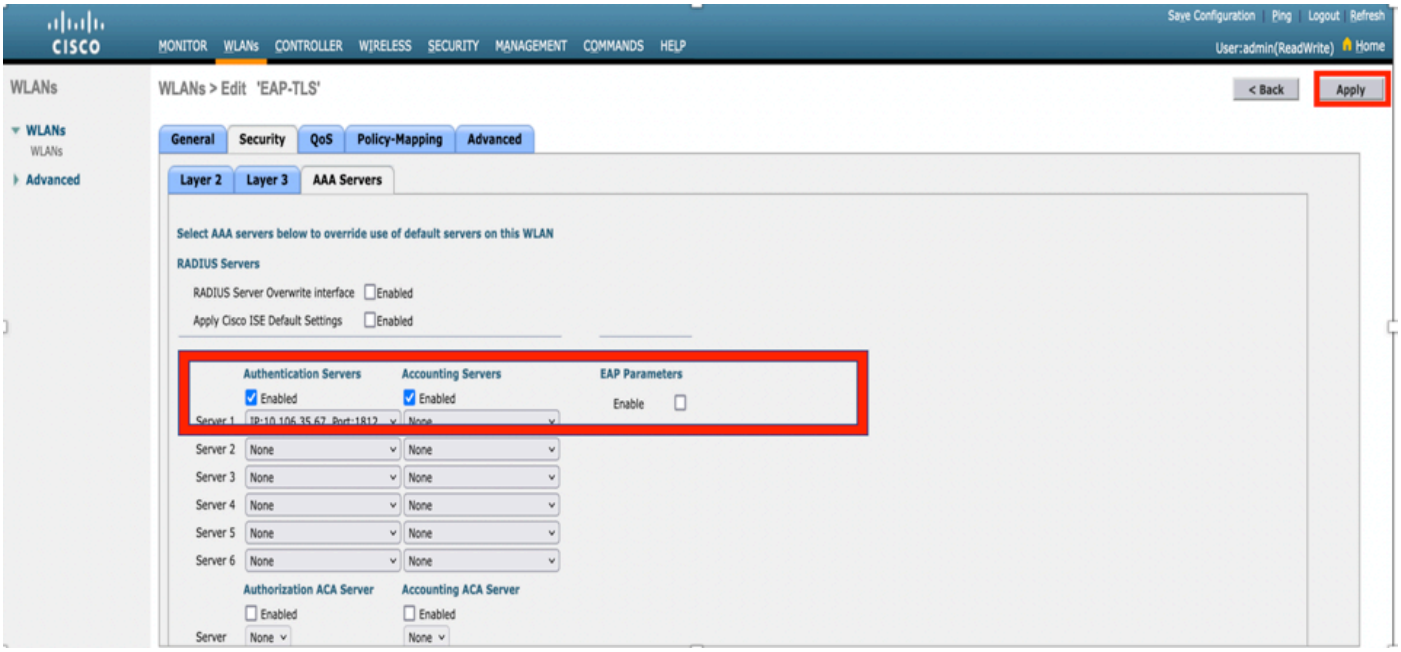
Passaggio 5. Assegnare un nome al nuovo WLAN **EAP-TLS**. Per continuare, fare clic su **Apply** (Applica) come mostrato nell'immagine.



Passaggio 6. Fare clic su **Generale** e verificare che lo stato sia **Abilitato**. I criteri di sicurezza predefiniti sono l'autenticazione 802.1X e WPA2, come mostrato nell'immagine.



Passaggio 7. Passare alla scheda **Sicurezza > Server AAA**, quindi selezionare il server RADIUS appena configurato e come mostrato nell'immagine.



Nota: È consigliabile verificare di poter raggiungere il server RADIUS dal WLC prima di continuare. RADIUS utilizza la porta UDP 1812 (per l'autenticazione), quindi è necessario verificare che il traffico non venga bloccato in alcun punto della rete.

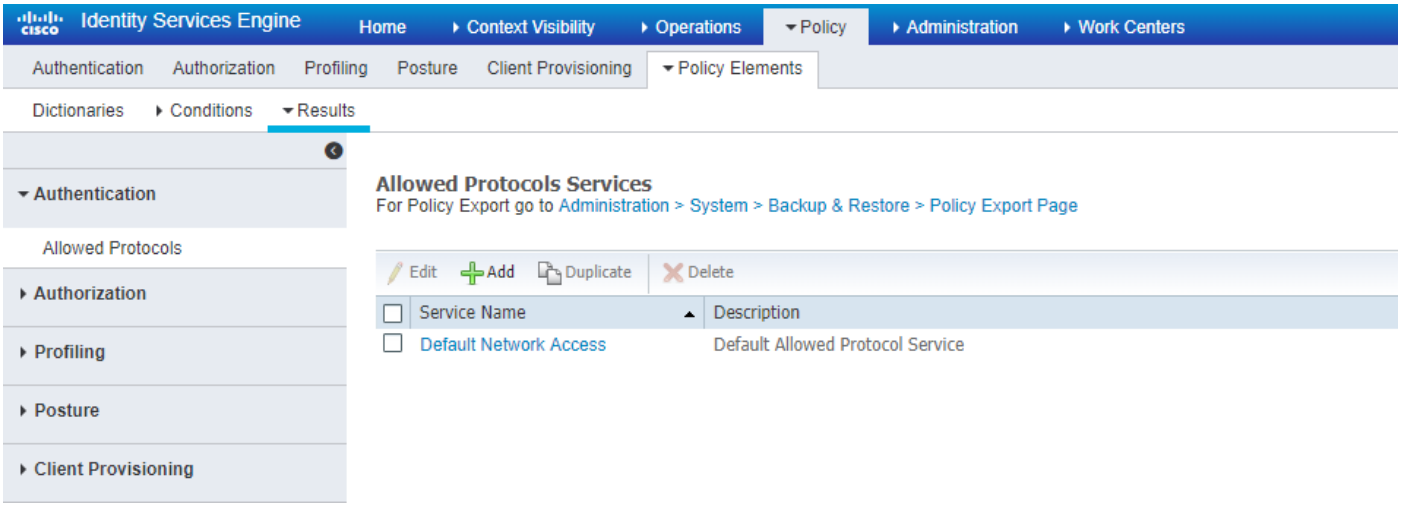
ISE con Cisco WLC

Impostazioni EAP-TLS

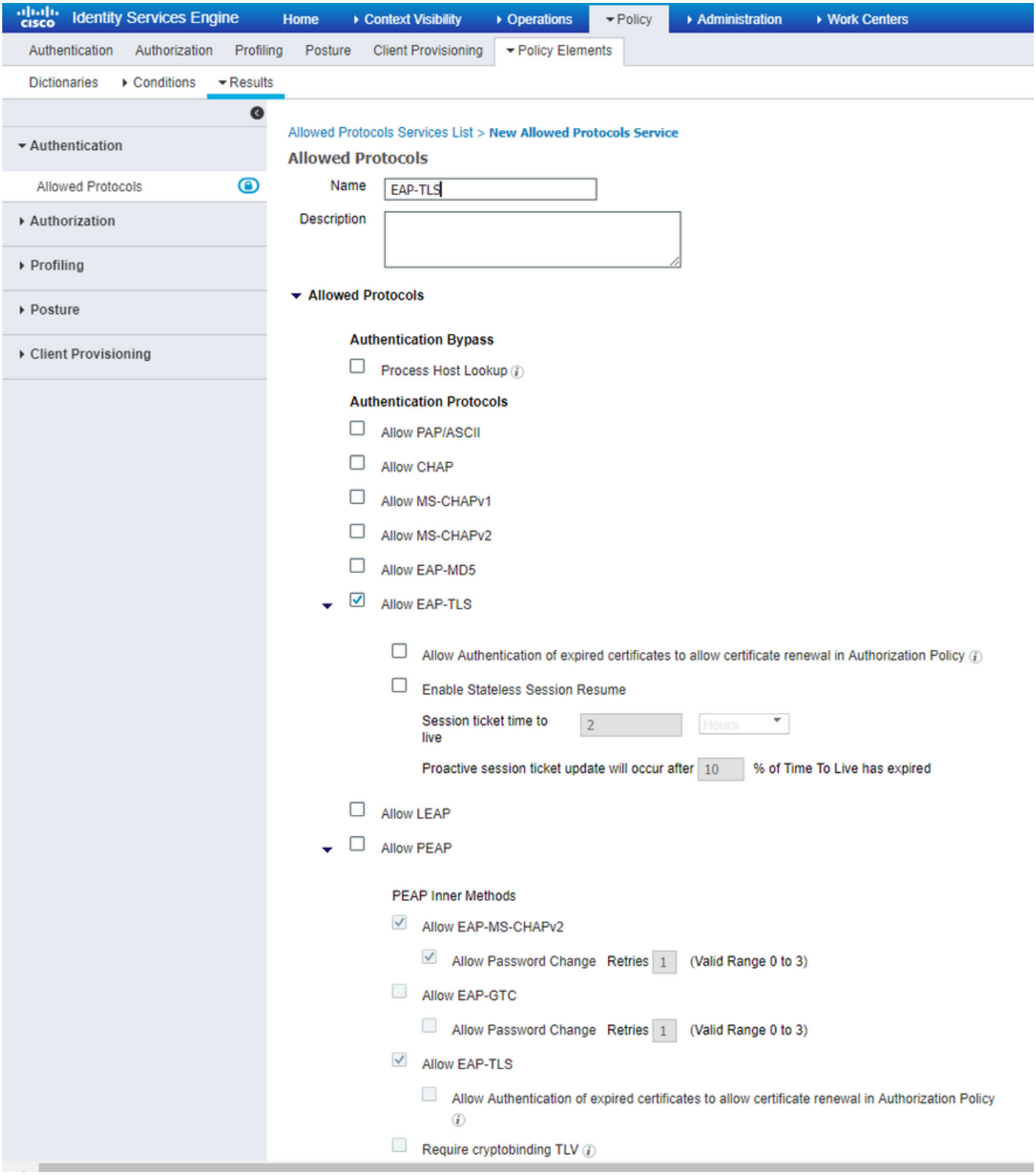
Per creare il criterio, è necessario creare l'elenco di protocolli consentiti da utilizzare nel criterio. Poiché viene scritto un criterio dot1x, specificare il tipo EAP consentito in base alla configurazione del criterio.

Se si utilizza l'impostazione predefinita, è possibile consentire la maggior parte dei tipi EAP per l'autenticazione, che non sono consigliati se è necessario bloccare l'accesso a un tipo EAP specifico.

Passaggio 1. Passare **a Criterio > Elementi criteri > Risultati > Autenticazione >** Protocolli **consentiti** e **fare clic su Aggiungi** come mostrato nell'immagine.

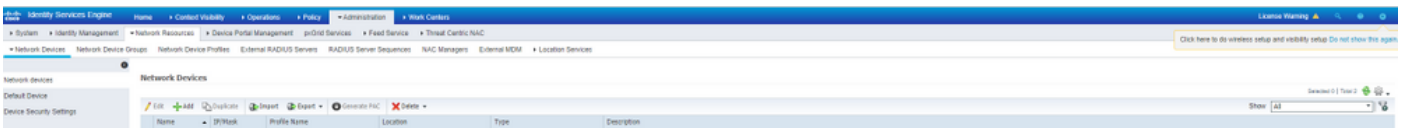


Passaggio 2. In questo elenco di protocolli consentiti, è possibile immettere il nome dell'elenco. In questo caso, la casella **Consenti EAP-TLS** è selezionata e le altre caselle sono deselezionate, come mostrato nell'immagine.

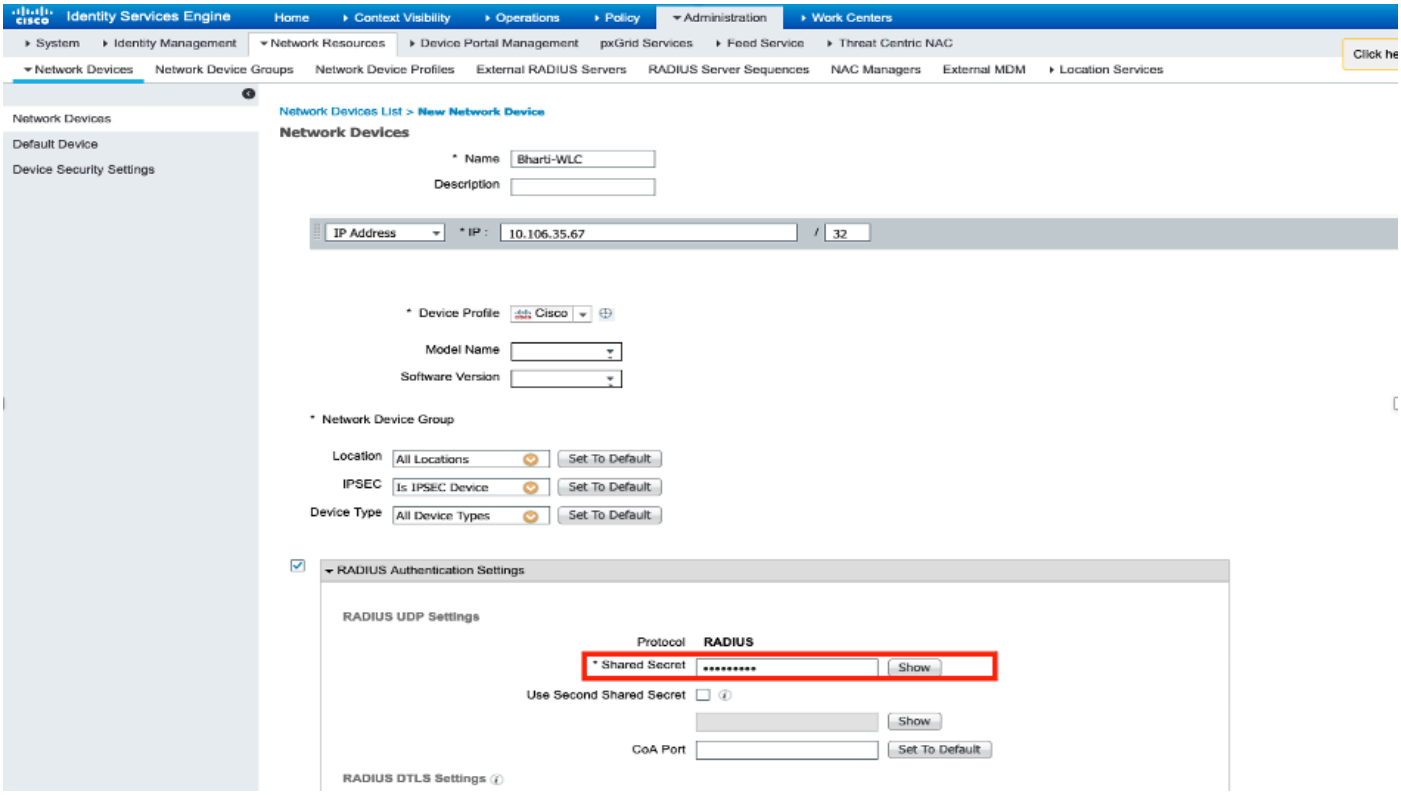


Impostazioni WLC su ISE

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

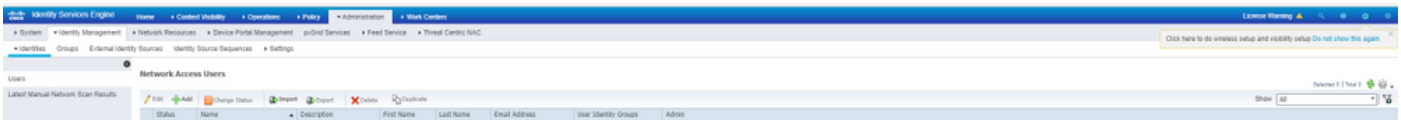


Passaggio 2. Inserire i valori come indicato nell'immagine.

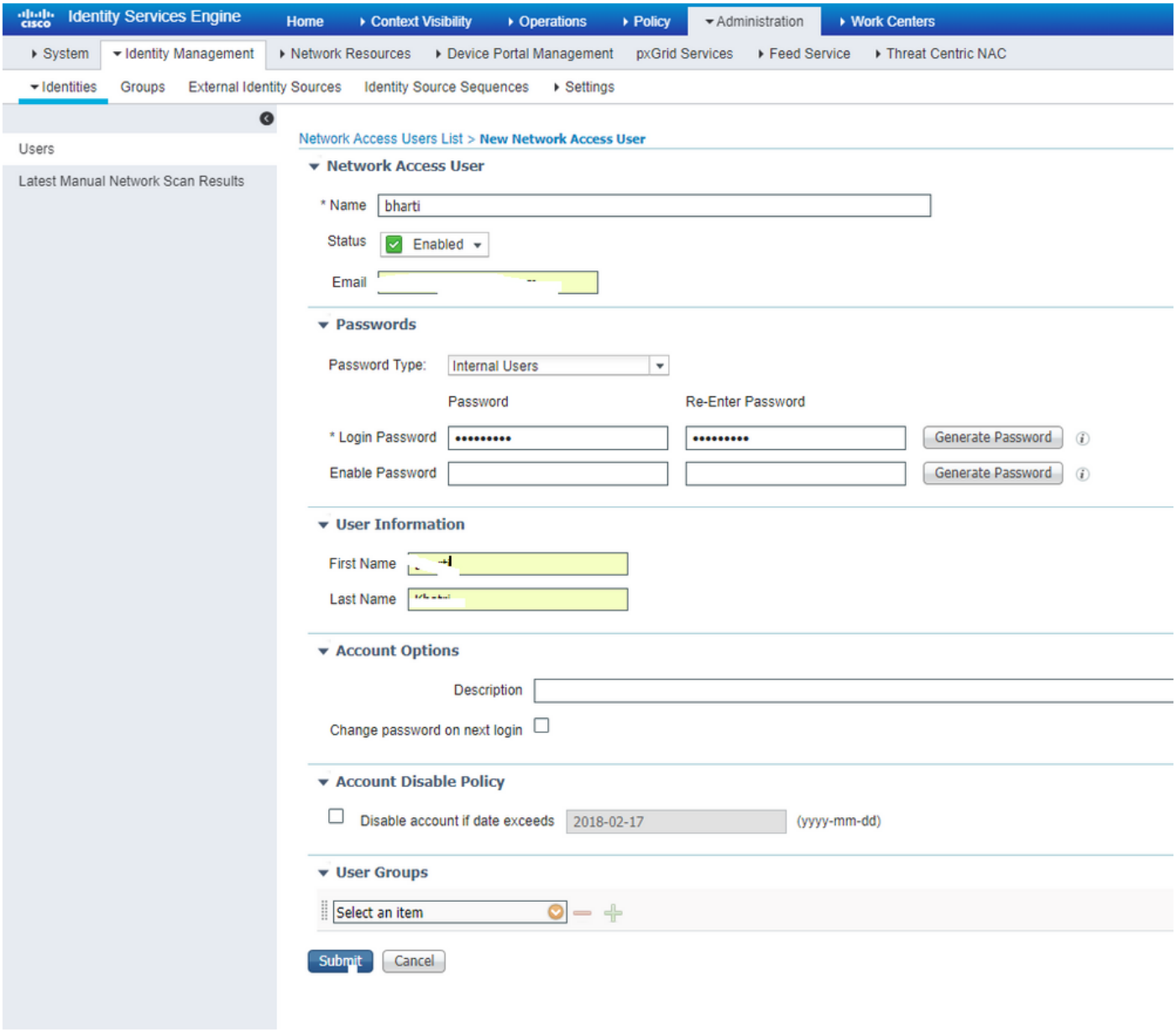


Creazione di un nuovo utente in ISE

Passaggio 1. Accedere a Administration > Identity Management > Identities > Users > Add (Amministrazione > Gestione delle identità > Identità > Utenti > Aggiungi) come mostrato nell'immagine.



Passaggio 2. Inserire le informazioni come illustrato nell'immagine.

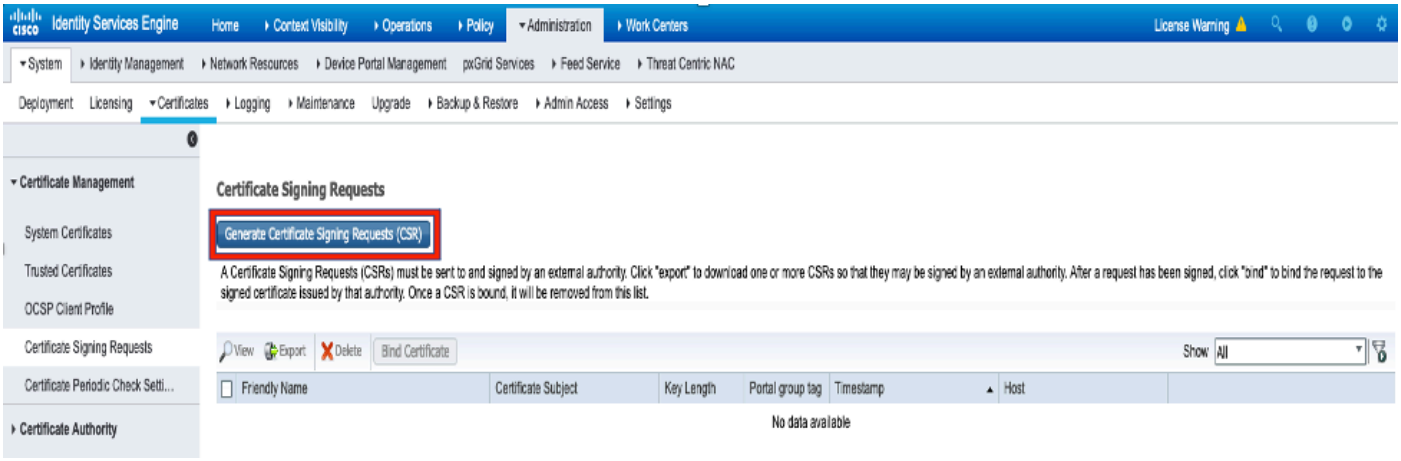


Certificato di attendibilità per ISE

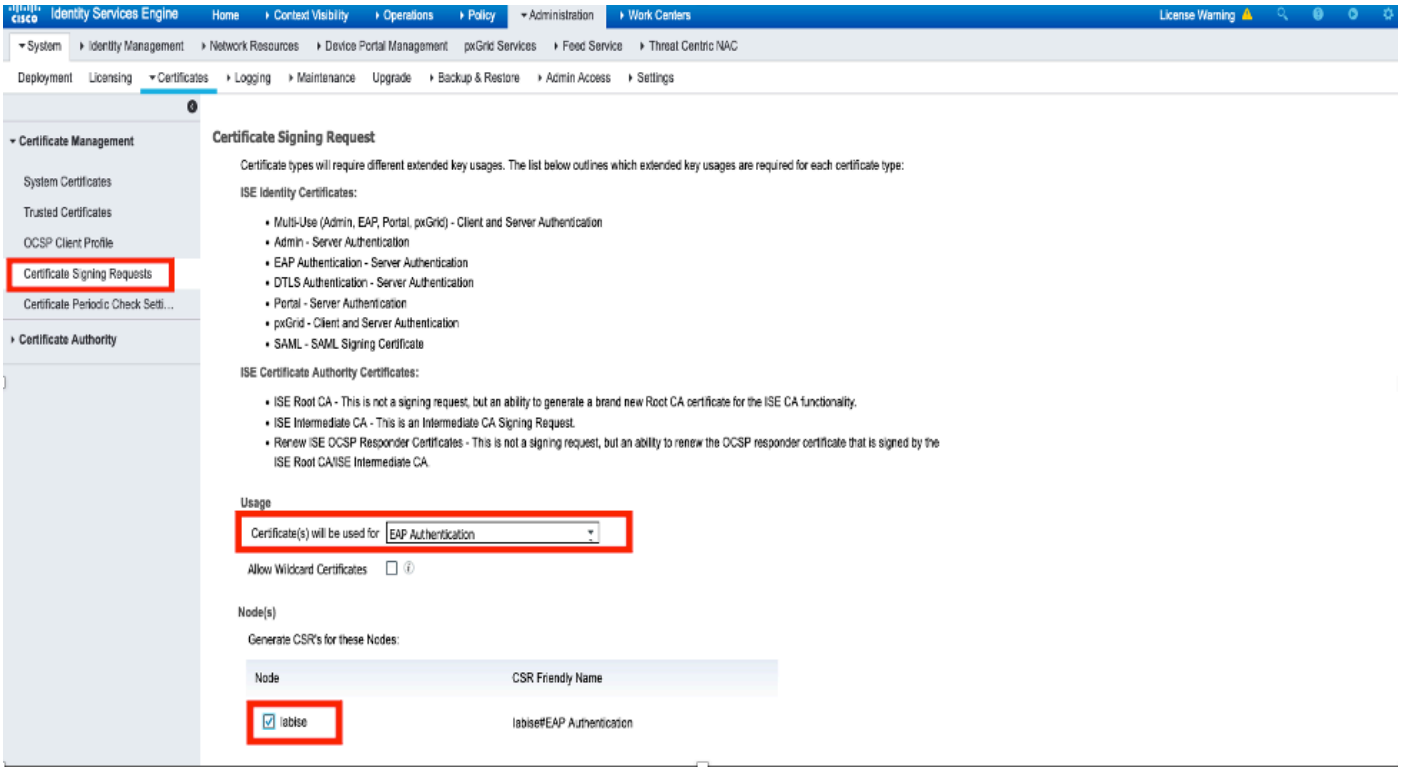
Passaggio 1. Passare ad **Amministrazione > Sistema > Certificati > Gestione certificati > Certificati attendibili**.

Per importare un certificato in ISE, fare clic su **Import** (Importa). Una volta aggiunto un WLC e creato un utente su ISE, è necessario fare la parte più importante di EAP-TLS che è quella di considerare attendibile il certificato su ISE. Per questo dobbiamo generare la RSI.

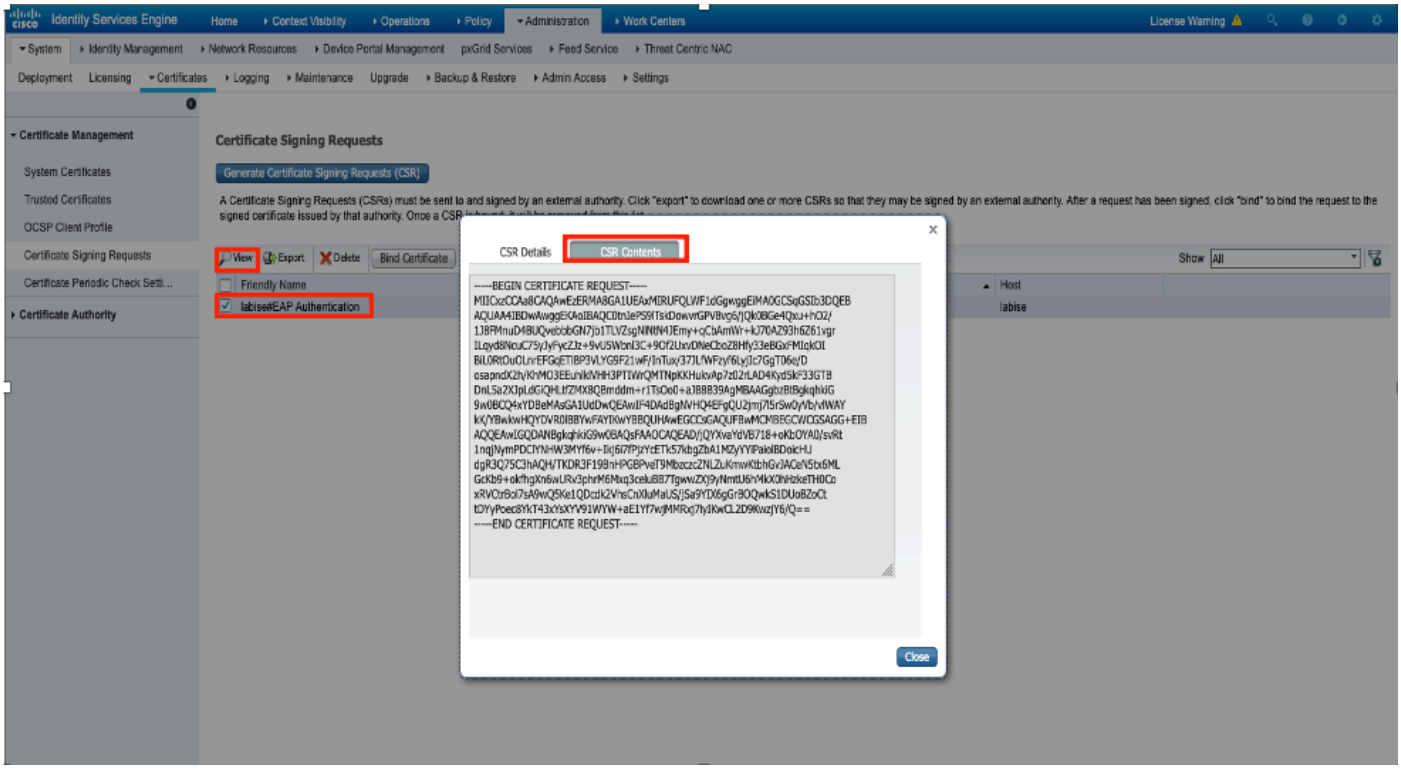
Passaggio 2. Passare a **Amministrazione > Certificati > Richieste di firma del certificato > Genera richieste di firma del certificato (CSR)** come mostrato nell'immagine.



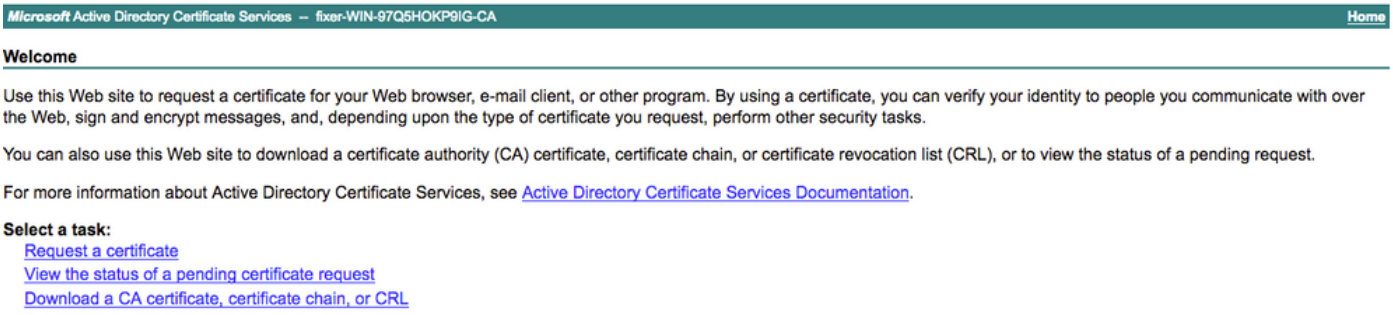
Passaggio 3. Per generare CSR, passare a **Uso** e da **Certificati utilizzati per** le opzioni di elenco a discesa selezionare **Autenticazione EAP** come mostrato nell'immagine.



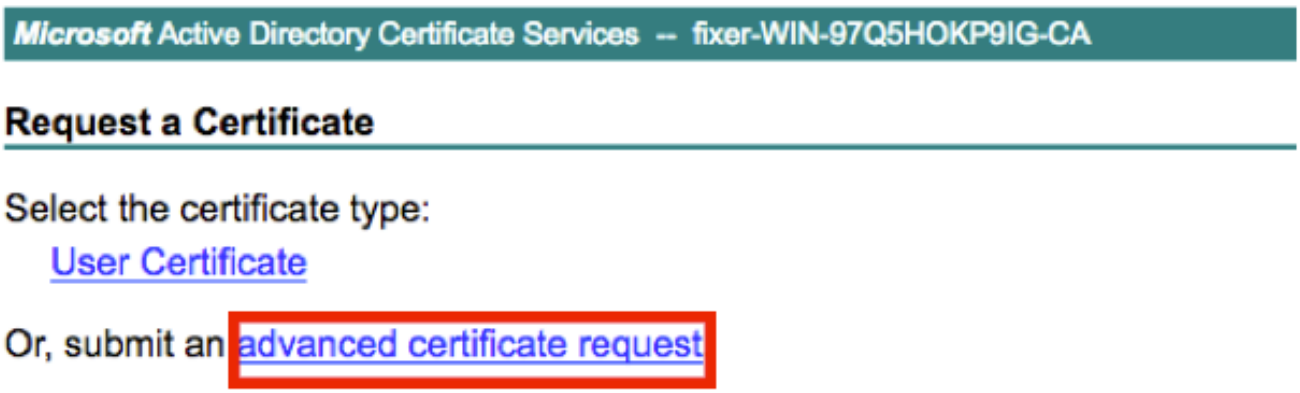
Passaggio 4. È possibile visualizzare il file CSR generato ad ISE. Fare clic su **Visualizza** come illustrato nell'immagine.



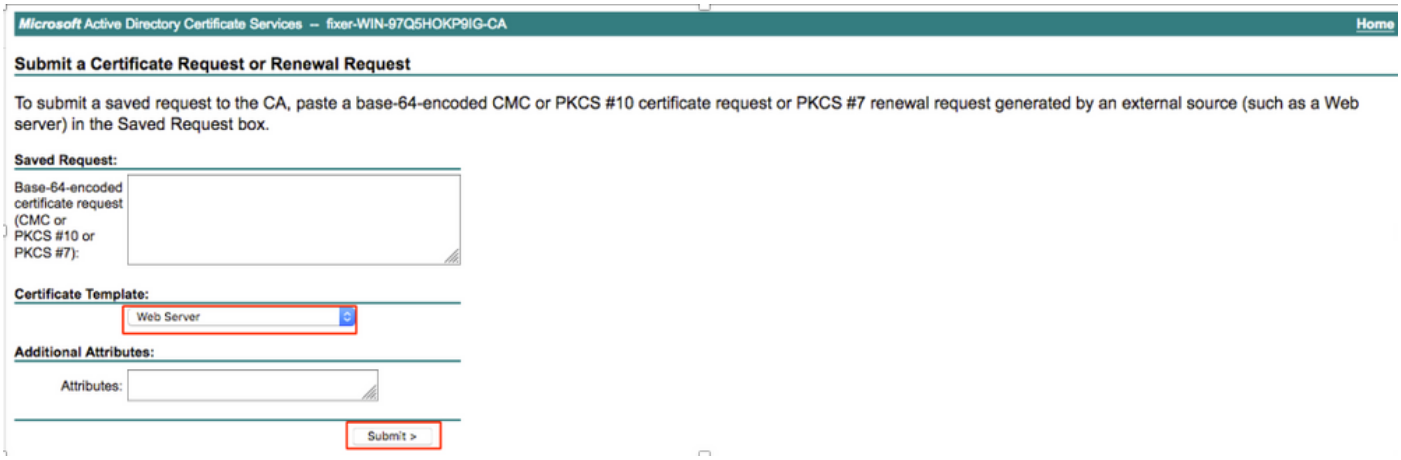
Passaggio 5. Dopo aver generato CSR, individuare il server CA e fare clic su **Request a certificate** (Richiedi **certificato)** come mostrato nell'immagine:



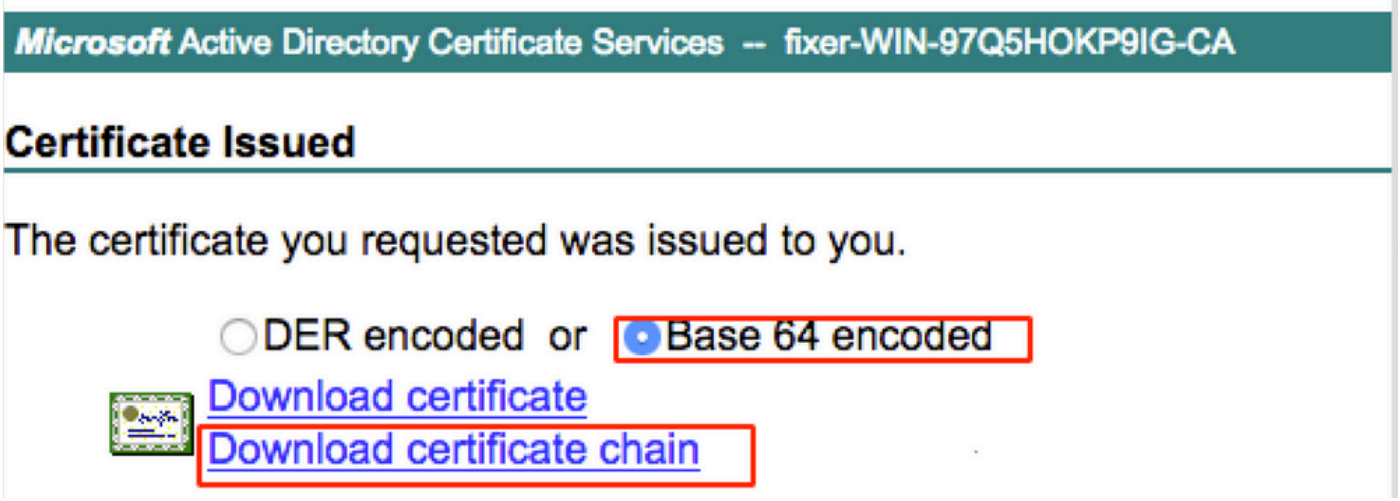
Passaggio 6. Dopo aver richiesto un certificato, si ottengono le opzioni **Certificato utente** e **Richiesta di certificato avanzata**, fare clic su **Richiesta di certificato avanzata** come mostrato nell'immagine.



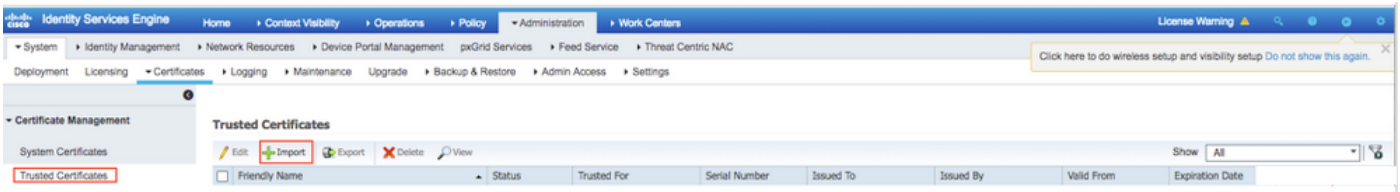
Passaggio 7. Incollare il CSR generato nella **richiesta di certificato con codifica Base 64**. Dal **modello** di **certificato:** scegliere **Server Web** e fare clic su **Invia**, come mostrato nell'immagine.

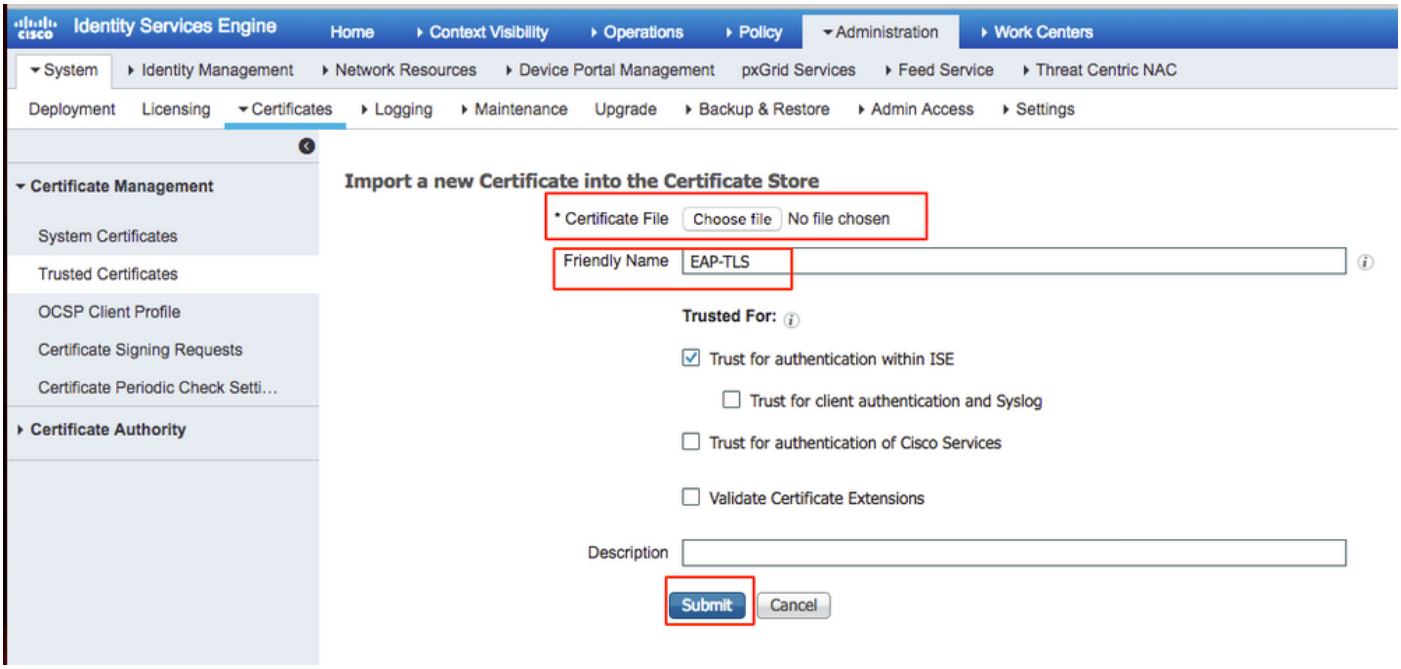


Passaggio 8. Dopo aver fatto clic su **Invia**, è possibile scegliere il tipo di certificato, selezionare **Codificato Base 64** e fare clic su **Scarica catena di certificati**, come mostrato nell'immagine.

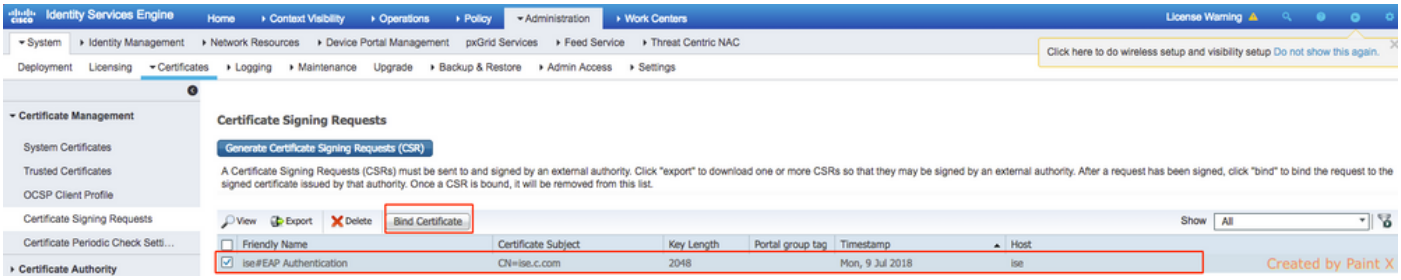


Passaggio 9. Il download del certificato per il server ISE è completato. È possibile estrarre il certificato, il certificato contiene due certificati, un certificato radice e un altro intermedio. Il certificato radice può essere importato in **Amministrazione > Certificati > Certificati attendibili > Importa** come mostrato nelle immagini.

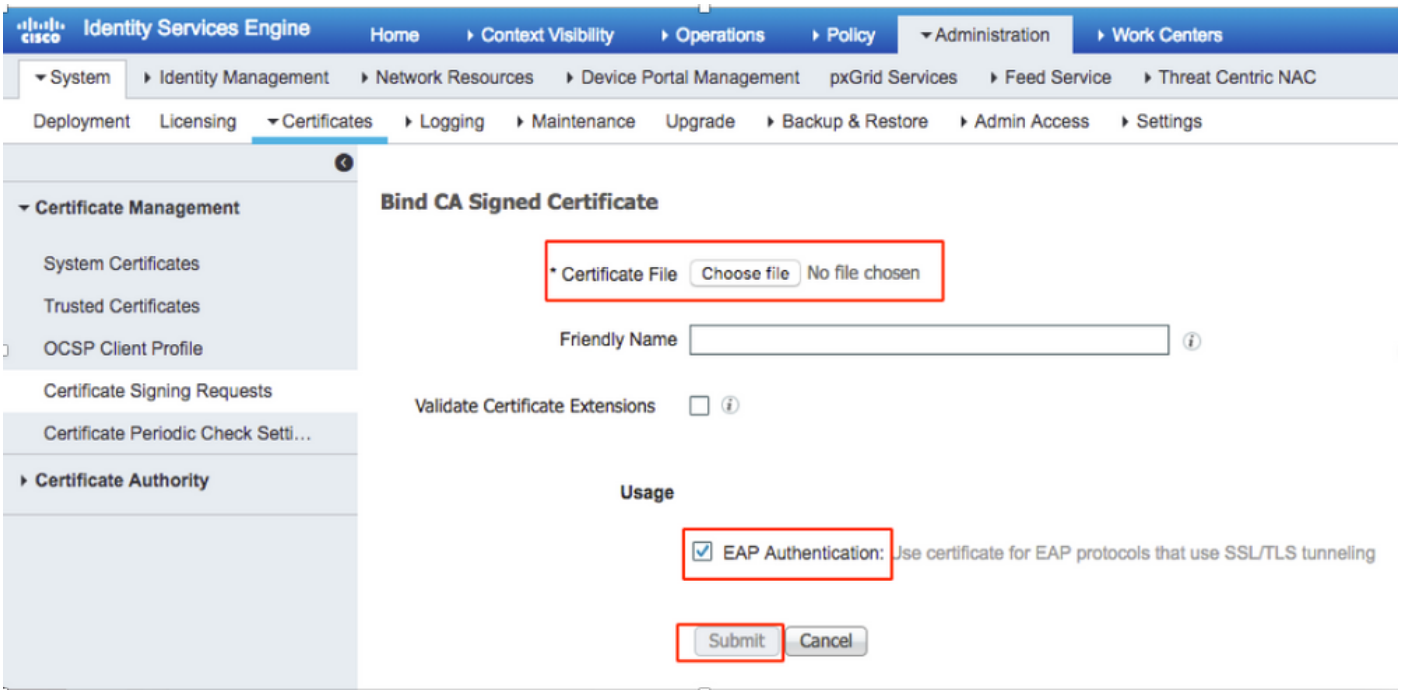




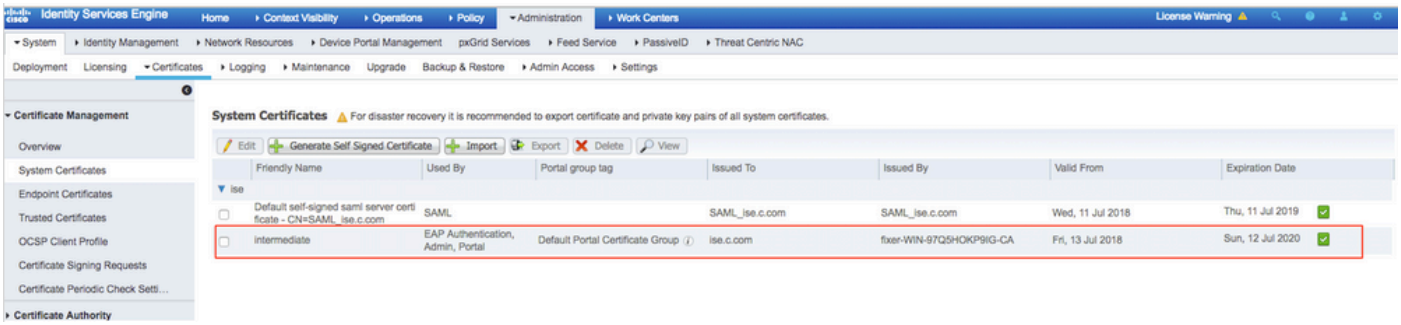
Passaggio 10. Dopo aver fatto clic su **Invia**, il certificato viene aggiunto all'elenco dei certificati attendibili. Inoltre, il certificato intermedio è necessario per il collegamento con CSR, come mostrato nell'immagine.



Passaggio 11. Dopo aver fatto clic su **Associa certificato**, è possibile scegliere il file di certificato salvato sul desktop. Individuare il certificato intermedio e fare clic su **Invia**, come mostrato nell'immagine.



Passaggio 12. Per visualizzare il certificato, selezionare **Amministrazione > Certificati > Certificati di sistema**, come mostrato nell'immagine.



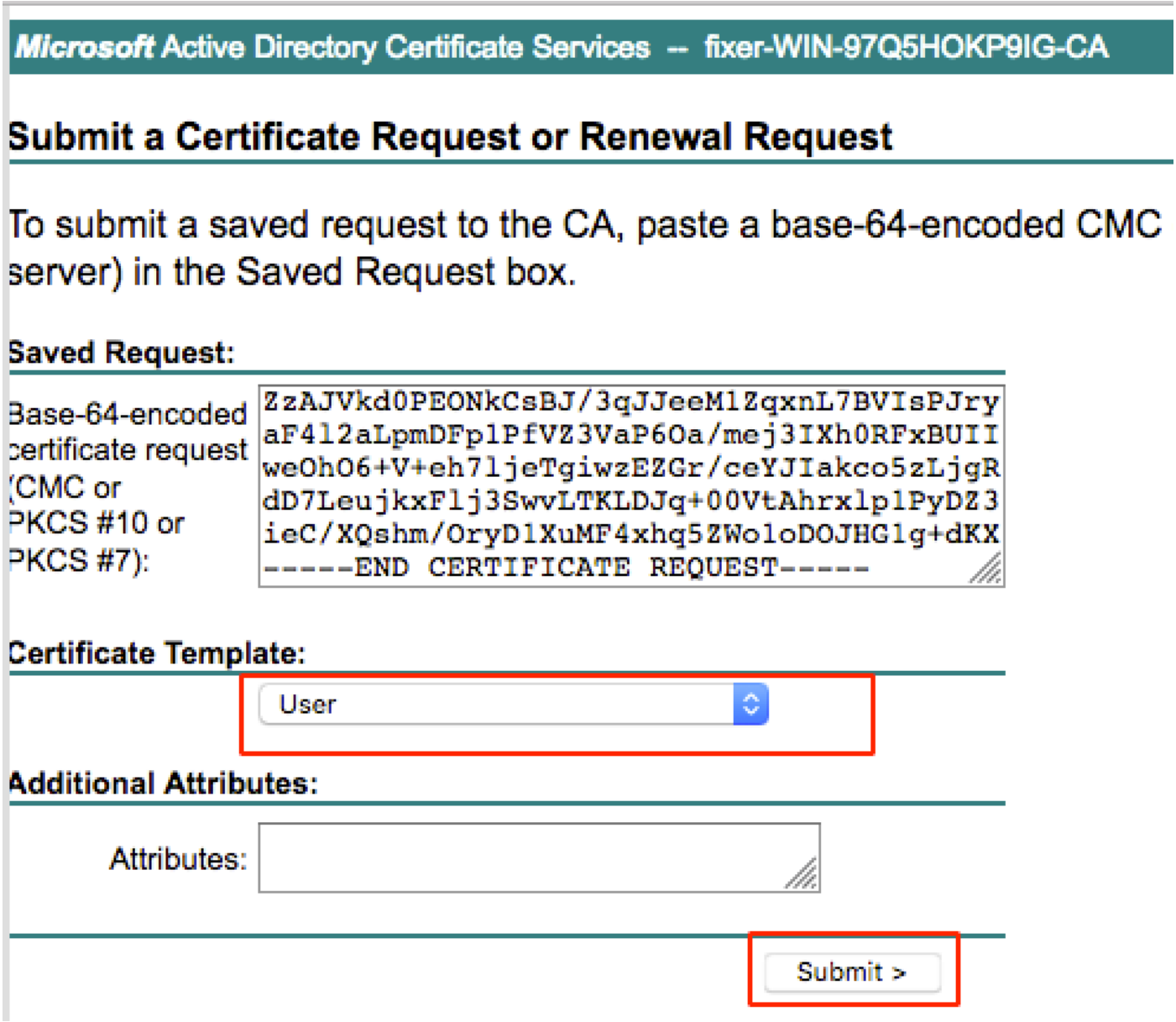
Client per EAP-TLS

Scarica certificato utente sul computer client (Windows Desktop)

Passaggio 1. Per autenticare un utente wireless tramite EAP-TLS, è necessario generare un certificato client. Connettere il computer Windows alla rete in modo da poter accedere al server. Apri un browser Web e immetti questo indirizzo: https://sever ip addr/certsrv—

Passaggio 2. Notare che la CA deve essere la stessa con cui è stato scaricato il certificato per ISE.

A tale scopo, è necessario cercare lo stesso server CA utilizzato per scaricare il certificato per il server. Nella stessa CA fare clic su **Richiedi un certificato** come in precedenza, ma questa volta è necessario selezionare **Utente** come modello di certificato, come mostrato nell'immagine.



Passaggio 3. Fare quindi clic su **scarica catena di certificati** come in precedenza per il server.

Dopo aver ottenuto i certificati, eseguire la procedura seguente per importare il certificato in Windows laptop:

Passaggio 4. Per importare il certificato, è necessario accedervi da Microsoft Management Console (MMC).

1. Per aprire MMC, selezionare **Start > Esegui > MMC**.
2. Selezionare **File > Aggiungi/Rimuovi snap-in**
3. Fare doppio clic su **Certificati**.
4. **Selezionare Account computer**.
5. Selezionare **Computer locale > Fine**
6. Per uscire dalla finestra Snap-in, fare clic su **OK**.
7. Fare clic su **[+]** accanto a **Certificati > Personali > Certificati**.
8. Fare clic con il pulsante destro del mouse su **Certificati** e selezionare **Tutte le attività > Importa**.
9. Fare clic su **Next** (Avanti).
10. Fare clic su **Sfoglia**.

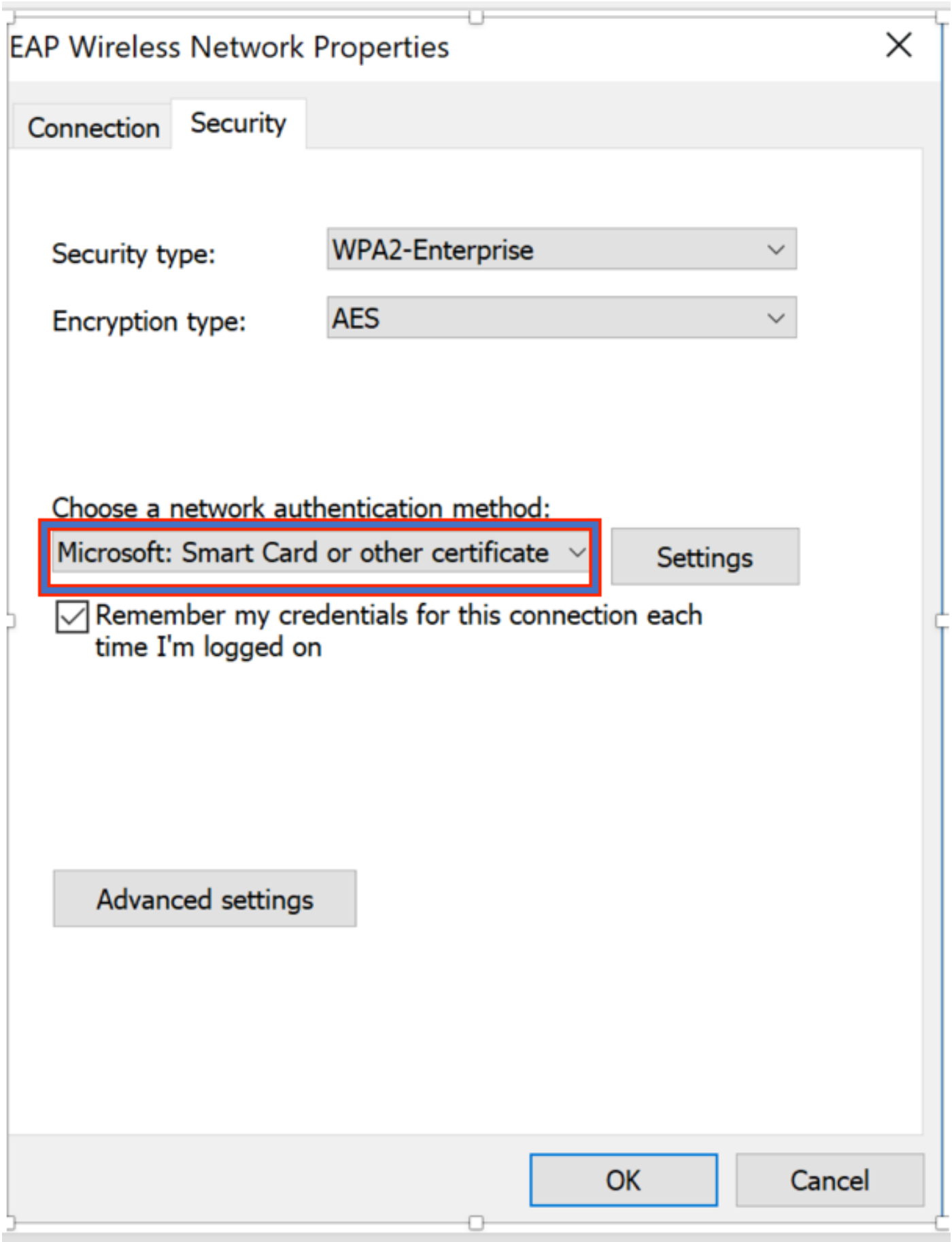
11. Selezionare il file **.cer, .crt o .pfx** che si desidera importare.
12. Fare clic su **Apri**.
13. Fare clic su **Next** (Avanti).
14. Selezionare **Seleziona automaticamente l'archivio certificati in base al tipo di certificato**.
15. Fare clic su **Fine e OK**

Al termine dell'importazione del certificato, è necessario configurare il client wireless (desktop di Windows in questo esempio) per EAP-TLS.

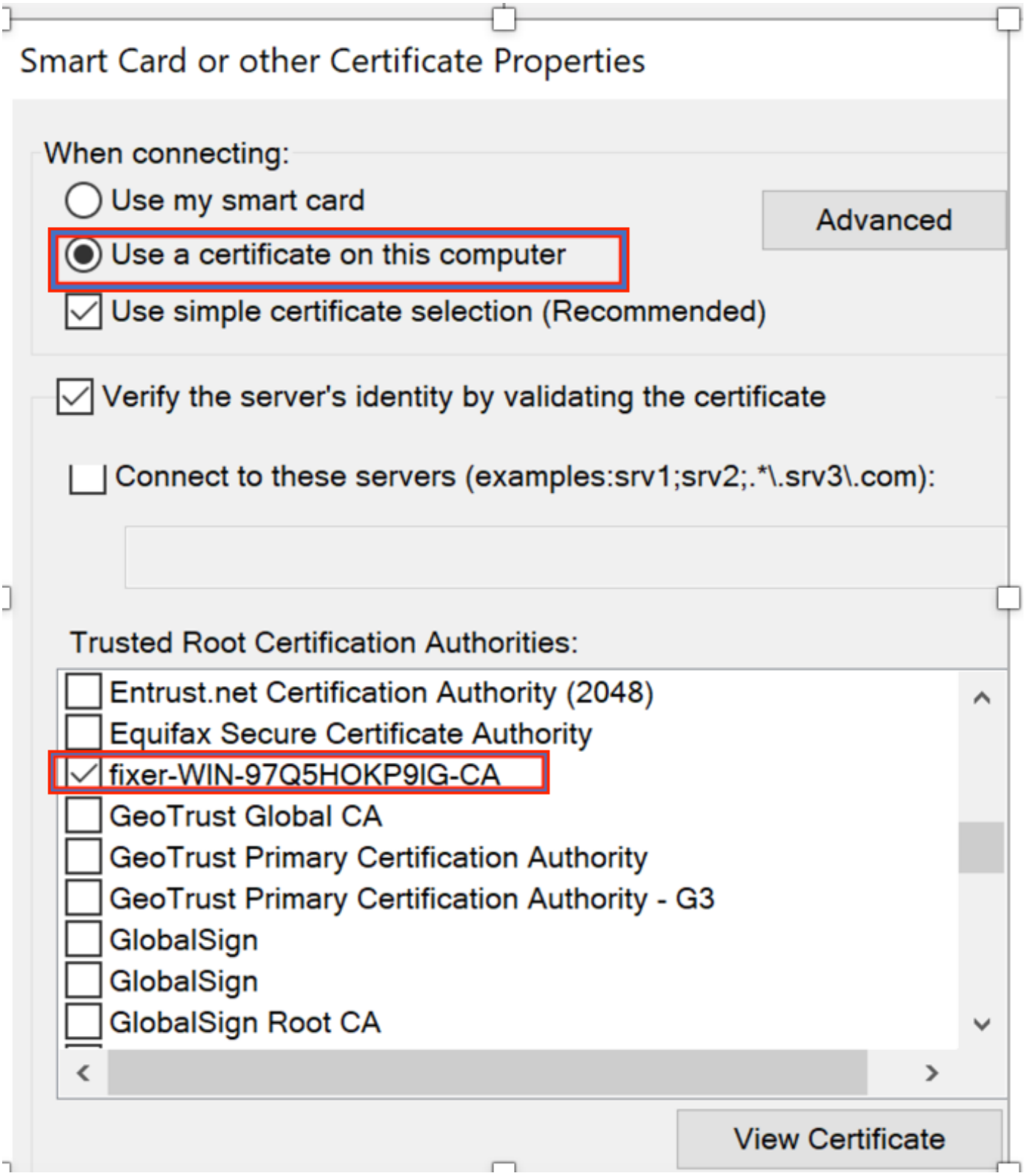
Profilo wireless per EAP-TLS

Passaggio 1. Modificare il profilo wireless creato in precedenza per il protocollo PEAP (Protected Extensible Authentication Protocol) in modo da utilizzare il protocollo EAP-TLS. Fare clic su **Profilo wireless EAP**.

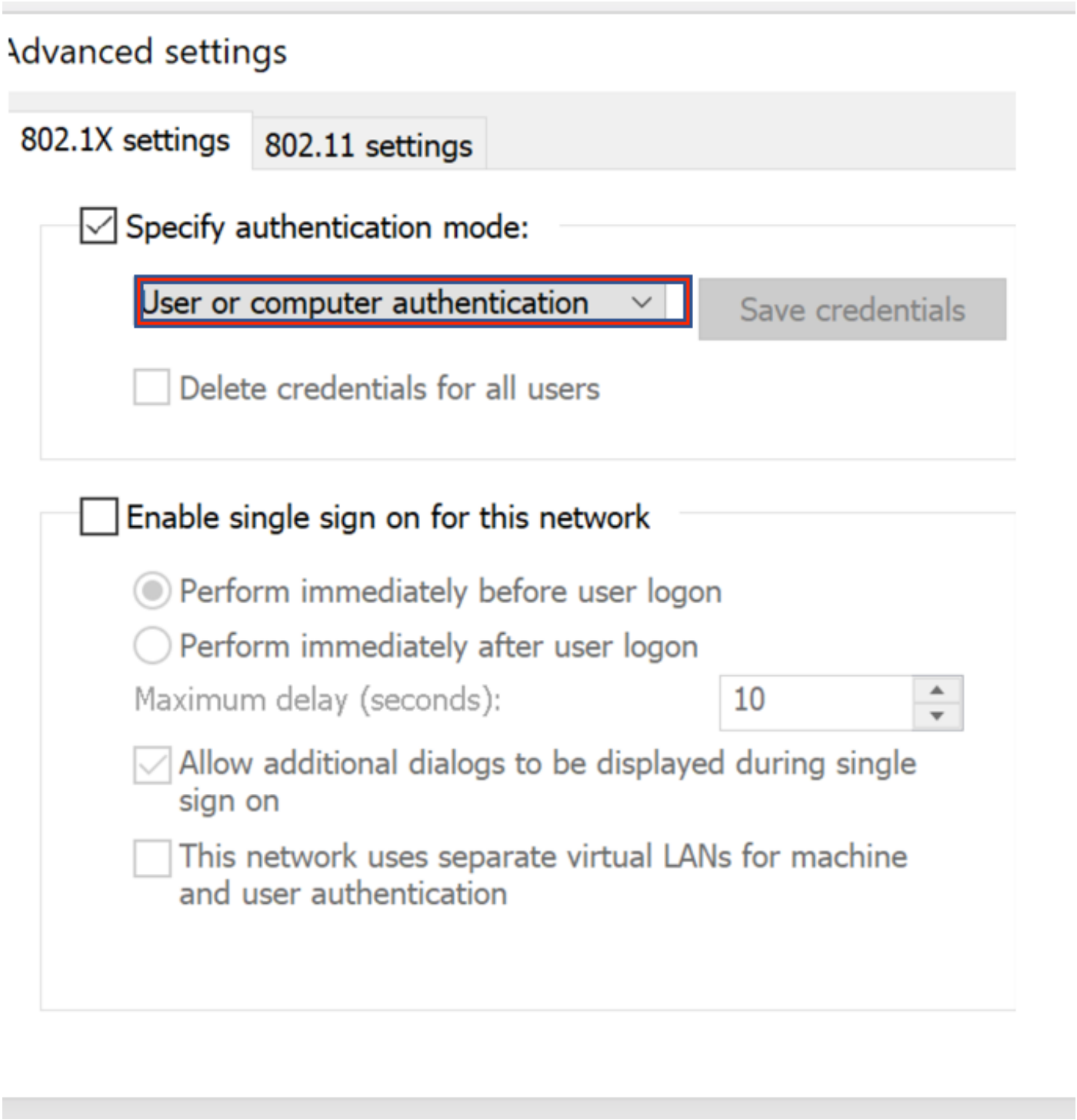
Passaggio 2. Selezionare **Microsoft: Smart Card o altro certificato** e fare clic su **OK** nell'immagine.



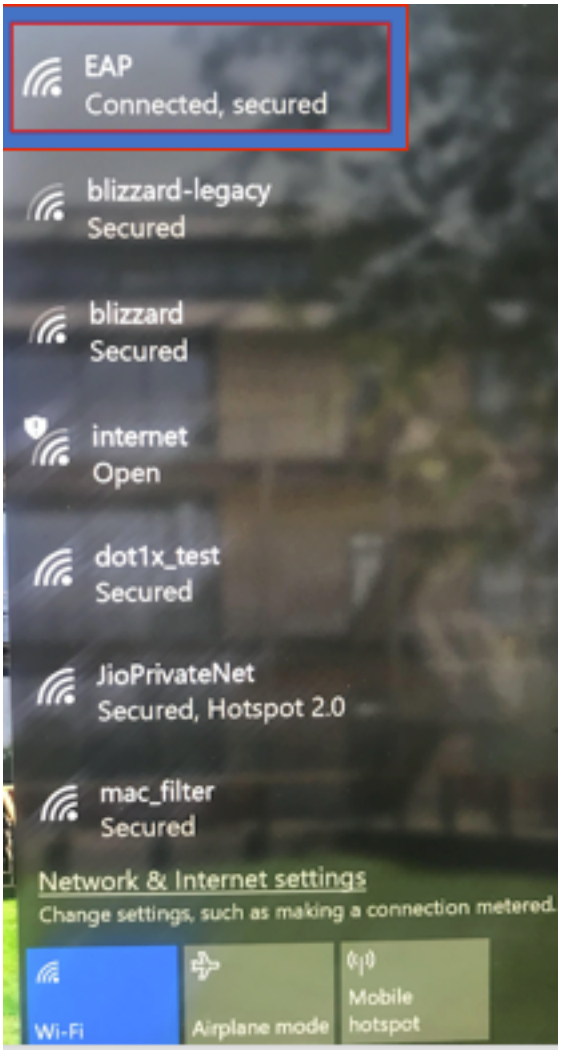
Passaggio 3. Fare clic su **impostazioni** e selezionare il certificato radice rilasciato dal server CA come mostrato nell'immagine.



Passaggio 4. Fare clic su **Impostazioni avanzate** e selezionare **Autenticazione utente o computer** dalla scheda Impostazioni 802.1x, come mostrato nell'immagine.



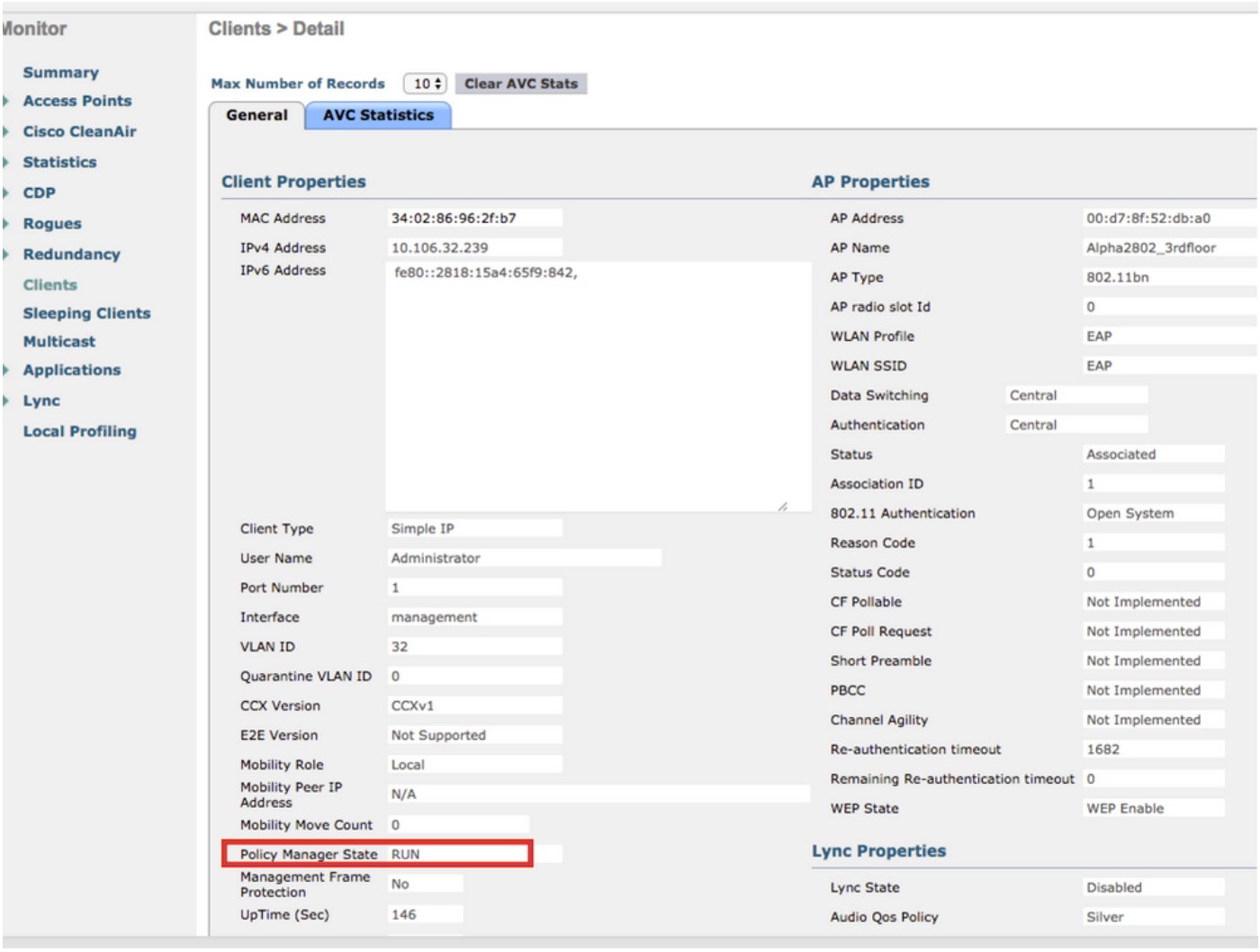
Passaggio 5. A questo punto, provare di nuovo a connettersi alla rete wireless, selezionare il profilo corretto (in questo esempio EAP) e **Connetti**. Si è connessi alla rete wireless come mostrato nell'immagine.



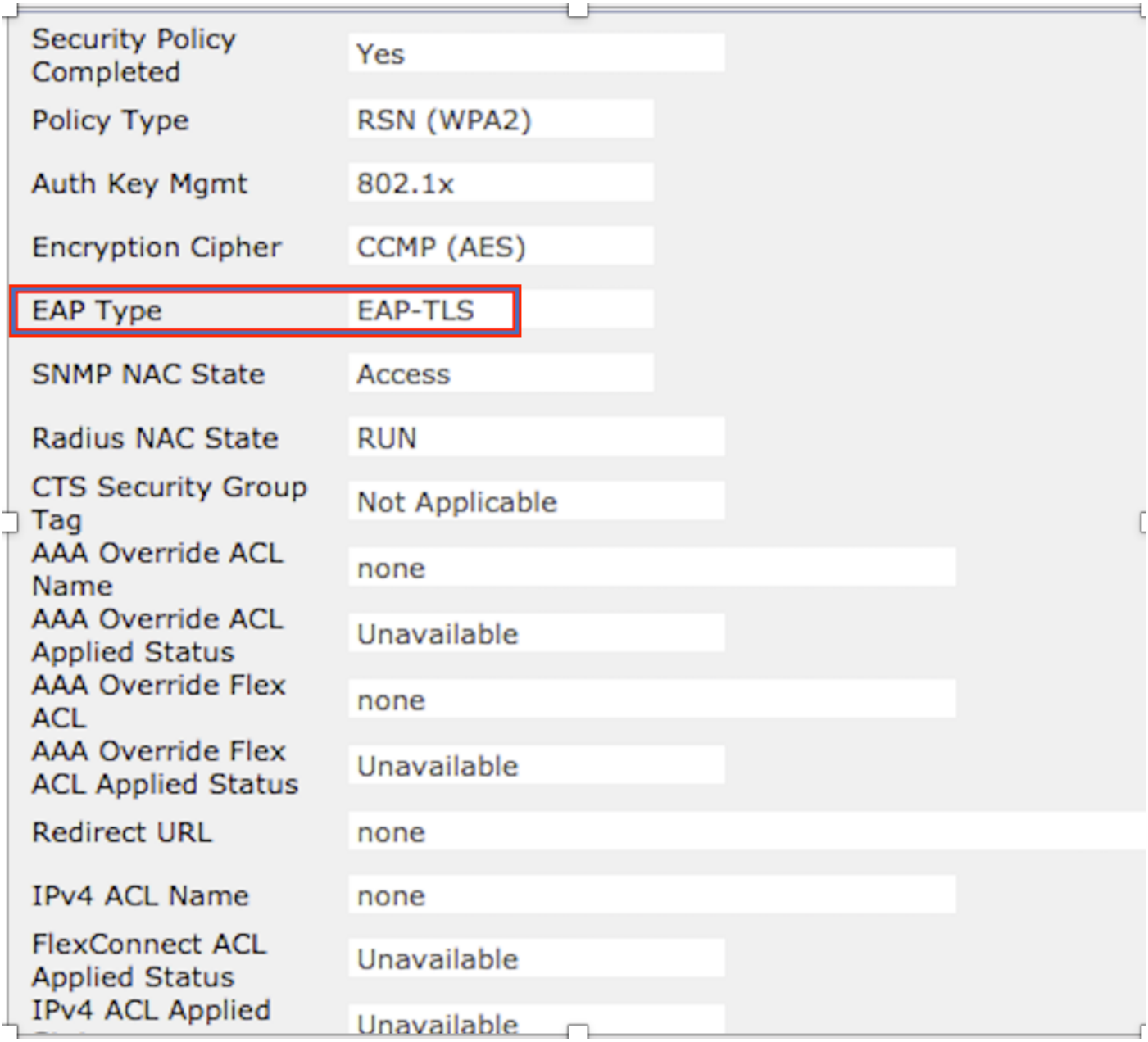
Verifica

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

Passaggio 1. Lo stato di gestione dei criteri client deve essere **RUN**. Ciò significa che il client ha completato l'autenticazione, ha ottenuto l'indirizzo IP ed è pronto a trasmettere il traffico mostrato nell'immagine.



Passaggio 2. Verificare inoltre il metodo EAP corretto sul WLC nella pagina dei dettagli del client, come mostrato nell'immagine.

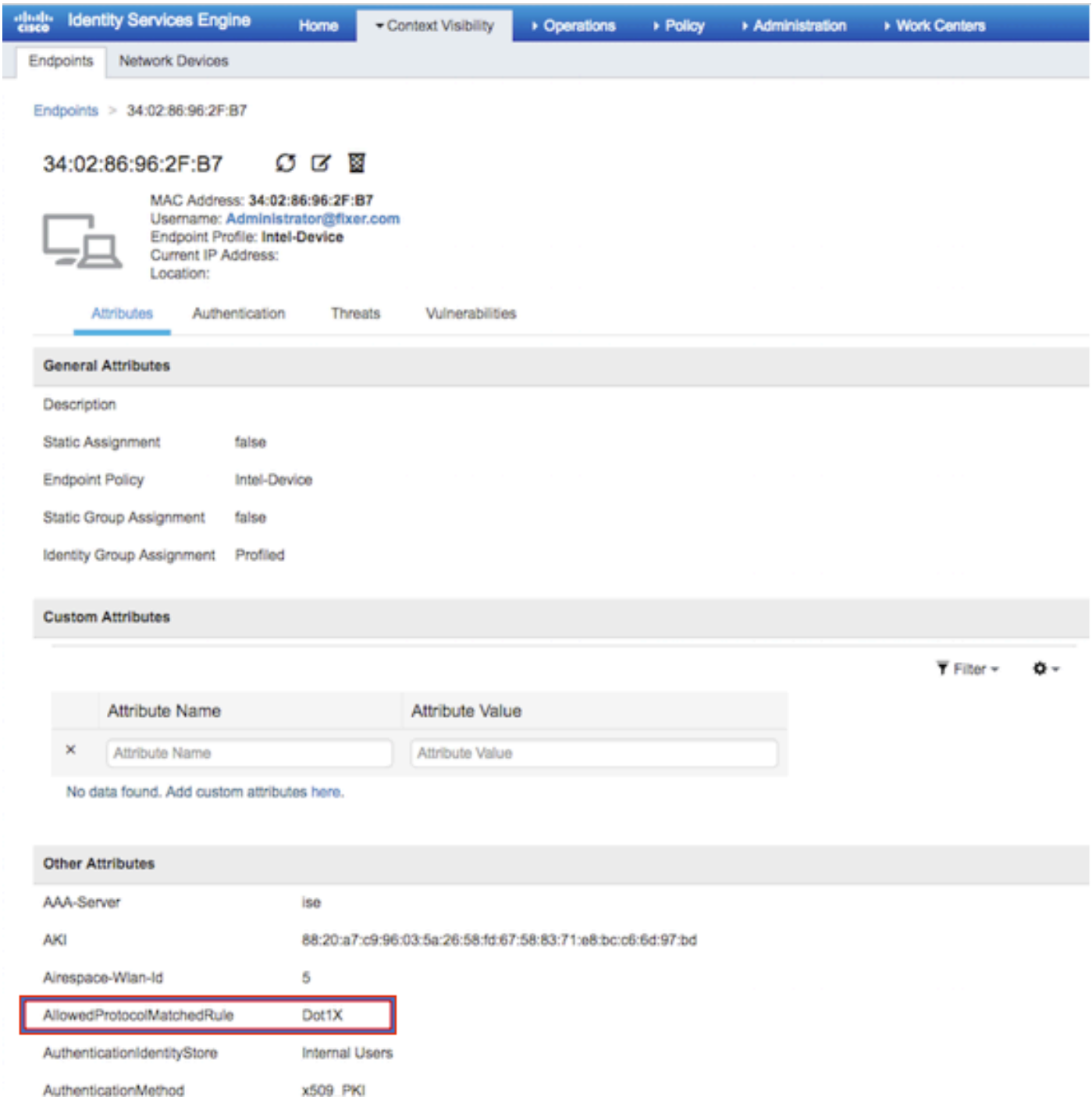


Passaggio 3. Ecco i dettagli del client dalla CLI del controller (output troncato):

```
(Cisco Controller-Standby) >show client detail 34:02:86:96:2f:b7
Client MAC Address.............................. 34:02:86:96:2f:b7
Client Username ................................ Administrator
AP MAC Address.................................. 00:d7:8f:52:db:a0
AP Name......................................... Alpha2802_3rdfloor
AP radio slot Id................................ 0
Client State.................................... Associated
Wireless LAN Id................................. 5
Wireless LAN Network Name (SSID)................ EAP
Wireless LAN Profile Name....................... EAP
Hotspot (802.11u)............................... Not Supported
BSSID........................................... 00:d7:8f:52:db:a4
Connected For .................................. 48 secs
Channel......................................... 1
IP Address...................................... 10.106.32.239
Gateway Address................................. 10.106.32.1
Netmask......................................... 255.255.255.0
Policy Manager State............................ RUN
Policy Type..................................... WPA2
Authentication Key Management................... 802.1x
```

```
Encryption Cipher.............................. CCMP-128 (AES)
Protected Management Frame ..................... No
Management Frame Protection..................... No
EAP Type....................................... EAP-TLS
```

Passaggio 4. Su ISE, selezionare **Context Visibility > End Points > Attributes**, come mostrato nelle immagini.



BYODRegistration	Unknown
Called-Station-ID	00-d7-8f-52-db-a0:EAP
Calling-Station-ID	34-02-86-96-2f-b7
Days to Expiry	363
DestinationIPAddress	10.106.32.31
DestinationPort	1812
DetailedInfo	Invalid username or password specified
Device IP Address	10.106.32.223
Device Port	32775
Device Type	Device Type#All Device Types
DeviceRegistrationStatus	NotRegistered
ElapsedDays	7
EnableFlag	Enabled
EndPointMACAddress	34-02-86-96-2F-B7
EndPointPolicy	Intel-Device
EndPointProfilerServer	ise.c.com
EndPointSource	RADIUS Probe
Extended Key Usage - Name	130, 132, 138
Extended Key Usage - OID	1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.4, 1.3.6.1.4.1.311.1
FailureReason	-
IdentityGroup	Profiled
InactiveDays	5
IsThirdPartyDeviceFlow	false
Issuer	CN=fixer-WIN-97Q5HOKP9IG-CA\,DC=fixer\,DC=c
Issuer - Common Name	fixer-WIN-97Q5HOKP9IG-CA
Issuer - Domain Component	fixer, com

Location	Location#All Locations
MACAddress	34:02:86:96:2F:B7
MatchedPolicy	Intel-Device
MessageCode	5200
NAS-IP-Address	10.106.32.223
NAS-Identifier	HA_Pri
NAS-Port	1
NAS-Port-Type	Wireless - IEEE 802.11
Network Device Profile	Cisco
NetworkDeviceGroups	Location#All Locations, Device Type#All Device Types
NetworkDeviceName	HA_Pri
NetworkDeviceProfileId	403ea8fc-7a27-41c3-80bb-27964031a08d
NetworkDeviceProfileName	Cisco
OUI	Intel Corporate
OpenSSLErrorMessage	SSL alert: code=0x230=560 \; source=local \; type=fatal \; message="Unknown CA - error unable to get issuer certificate locally"
OpenSSLErrorStack	140160653813504:error:140890B2:SSL routines:SSL3_GET_CLIENT_CERTIFICATE:no certificate returned:s3_srvr.c:3370:
PolicyVersion	0
PostureApplicable	Yes
PostureAssessmentStatus	NotApplicable
RadiusFlowType	Wireless802_1x
RadiusPacketType	AccessRequest
SSID	00-d7-8f-52-db-a0:EAP
SelectedAccessService	Default Network Access
SelectedAuthenticationIdentityStores	EAPTLS
SelectedAuthorizationProfiles	PermitAccess
Serial Number	10 29 41 78 00 00 00 00 00 11

Risoluzione dei problemi

Non sono attualmente disponibili informazioni specifiche per la risoluzione dei problemi per 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).