

# Comprensione e configurazione di EAP-TLS con WLC e ISE

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Flusso EAP-TLS](#)

[Fasi del flusso EAP-TLS](#)

[Configurazione](#)

[Cisco Wireless LAN Controller](#)

[ISE con Cisco WLC](#)

[Impostazioni EAP-TLS](#)

[Impostazioni WLC su ISE](#)

[Creazione di un nuovo utente in ISE](#)

[Certificato di attendibilità per ISE](#)

[Client per EAP-TLS](#)

[Scarica certificato utente sul computer client \(Windows Desktop\)](#)

[Profilo wireless per EAP-TLS](#)

[Verifica](#)

[Risoluzione dei problemi](#)

## 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

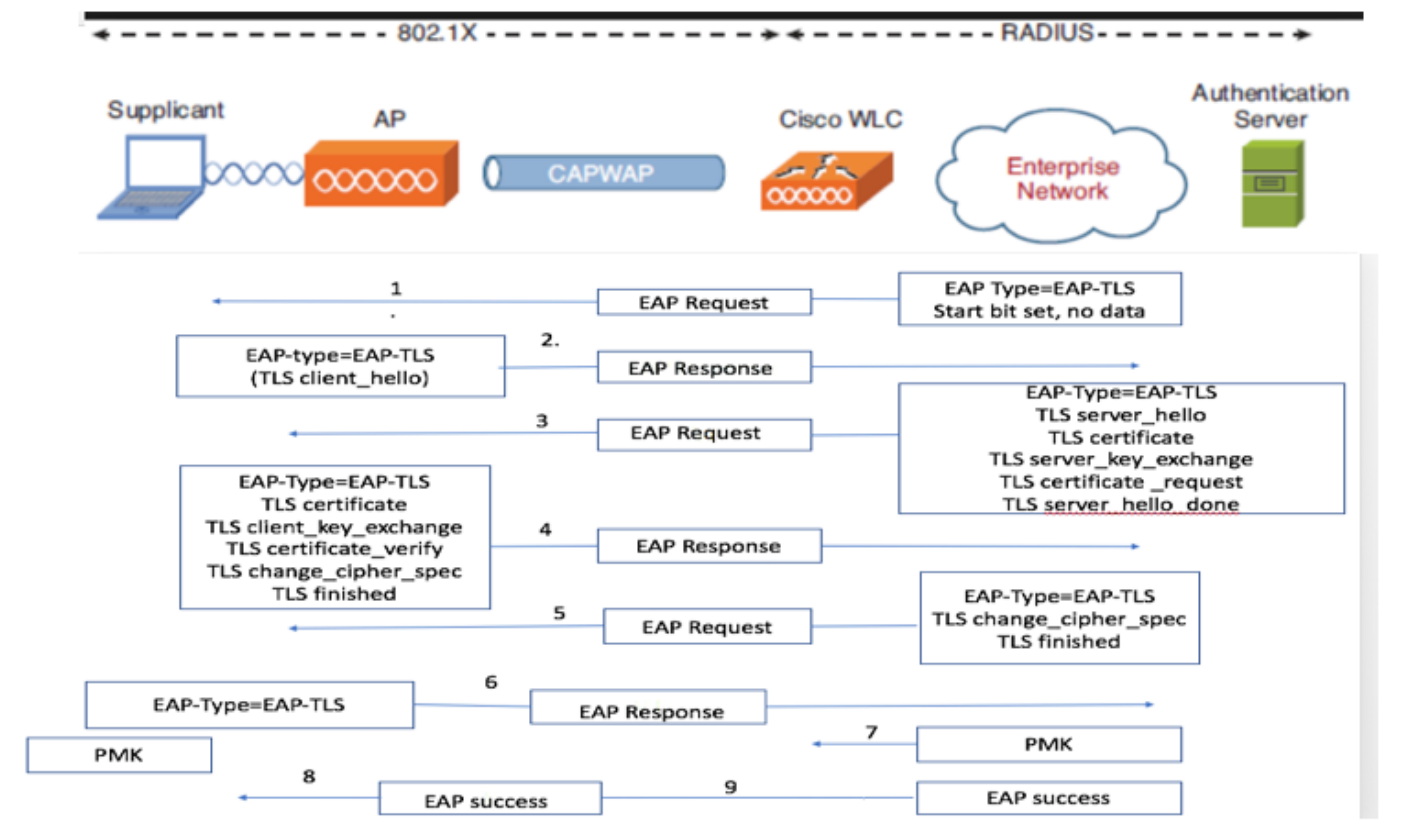
hardware:

- 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.

Security

RADIUS Authentication Servers

Auth Called Station ID Type: AP Name:SSID

Use AES Key Wrap:  (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter: Colon

Framed MTU: 1300

Network User	Management	Tunnel Proxy	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	138.77.0.84	1812	Disabled	Disabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2	138.77.0.83	1812	Disabled	Disabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	3	138.77.97.20	1812	Disabled	Disabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	4	138.77.97.21	1812	Disabled	Disabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5	* 172.27.1.71	1812	Disabled	Enabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	6	* 10.100.120.41	1812	Disabled	Enabled

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.

Security

RADIUS Authentication Servers > Edit

Server Index: 7

Server Address(Ipv4/Ipv6): 10.106.35.67

Shared Secret Format: ASCII

Shared Secret: \*\*\*

Confirm Shared Secret: \*\*\*

Key Wrap:  (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Apply Cisco ISE Default settings:

Apply Cisco ACA Default settings:

Port Number: 1812

Server Status: Enabled

Support for CoA: Disabled

Server Timeout: 5 seconds

Network User:  Enable

Management:  Enable

Management Retransmit Timeout: 5 seconds

Tunnel Proxy:  Enable

Realm List

PAC Provisioning:  Enable

IPSec:  Enable

Cisco ACA:  Enable

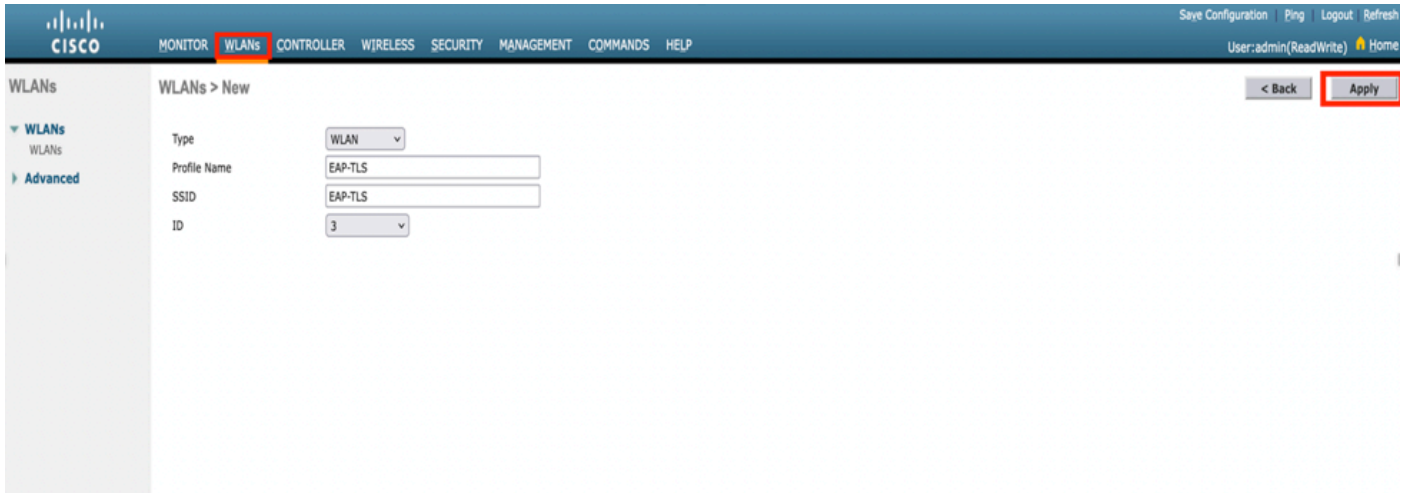
Passaggio 3. Creazione di una WLAN per l'autenticazione RADIUS.

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.

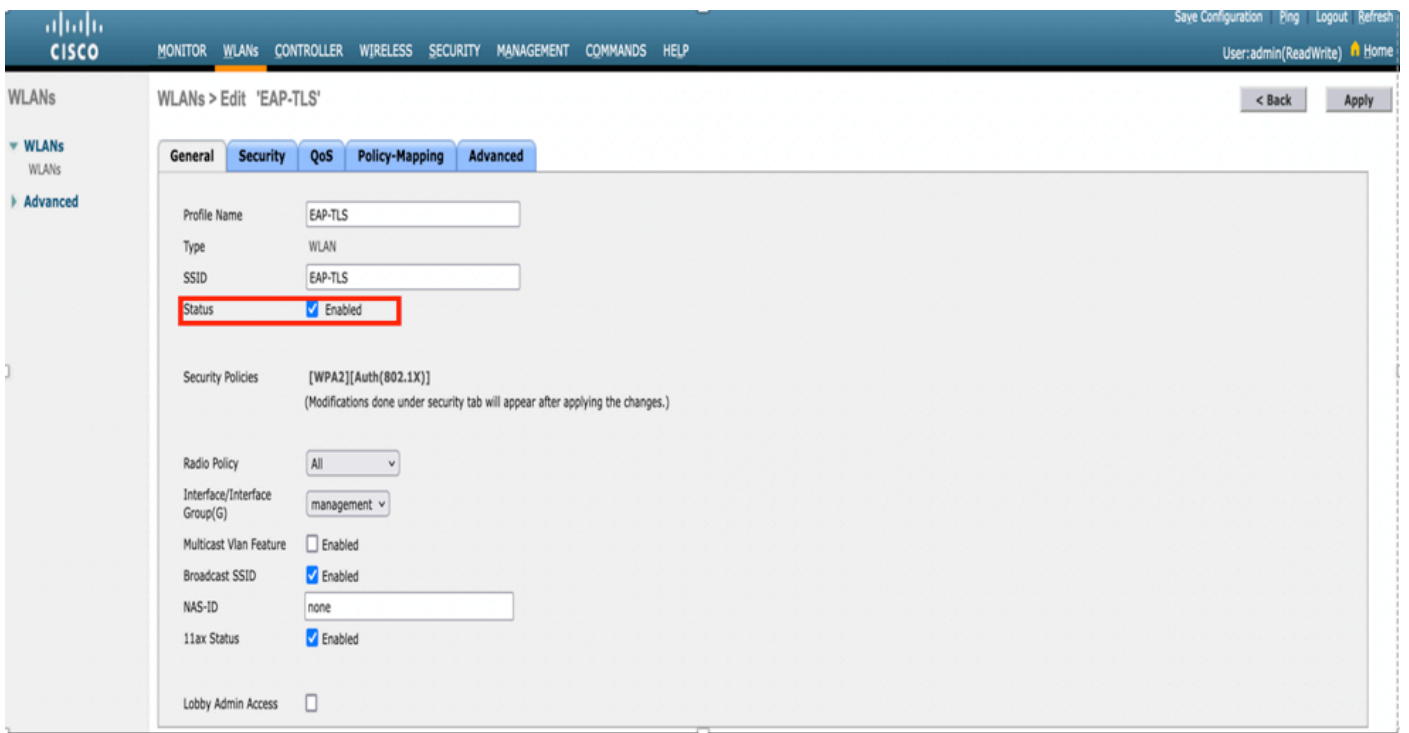
Passaggio 4. Selezionare **WLAN** dal menu principale, scegliere **Crea nuovo** e fare clic su **Go** (Vai), come mostrato nell'immagine.



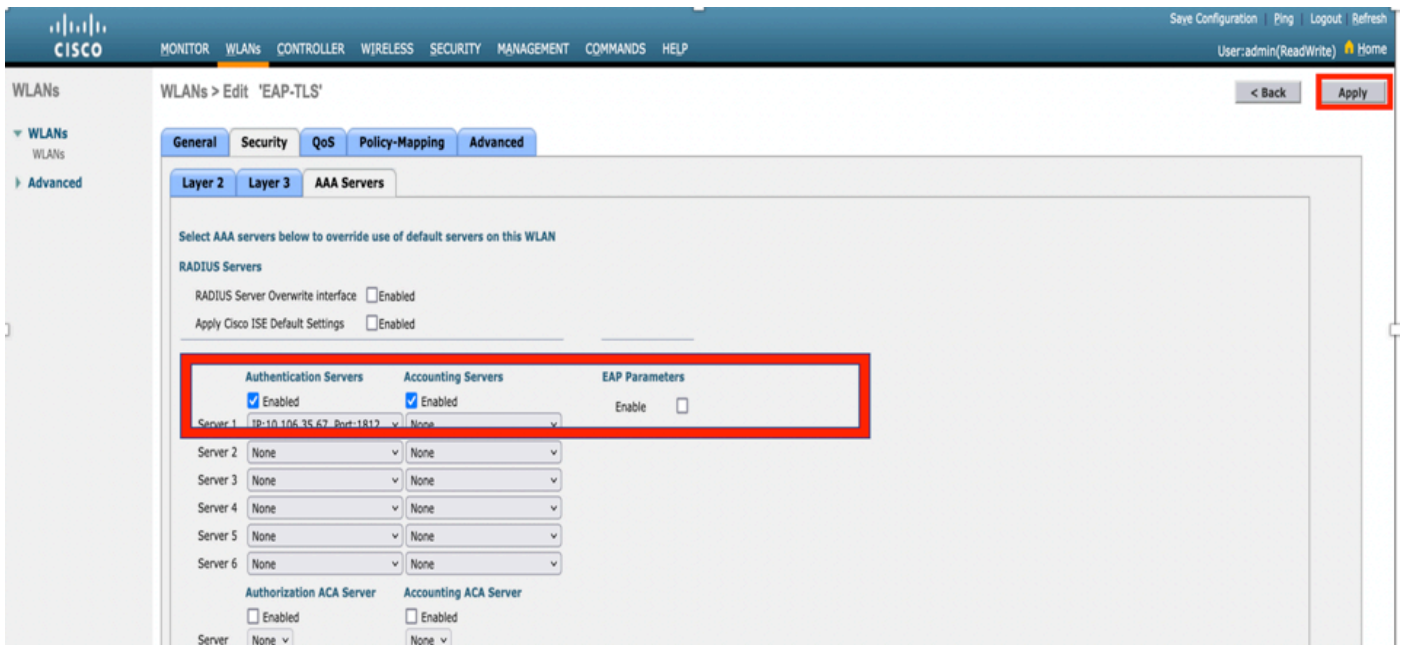
Passaggio 5. Assegnare un nome al nuovo WLAN **EAP-TLS**. Per continuare, fare clic su **Apply** (Applica) come mostrato nell'immagine.



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.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionaries Conditions Results

Authentication

Allowed Protocols

Authorization

Profiling

Posture

Client Provisioning

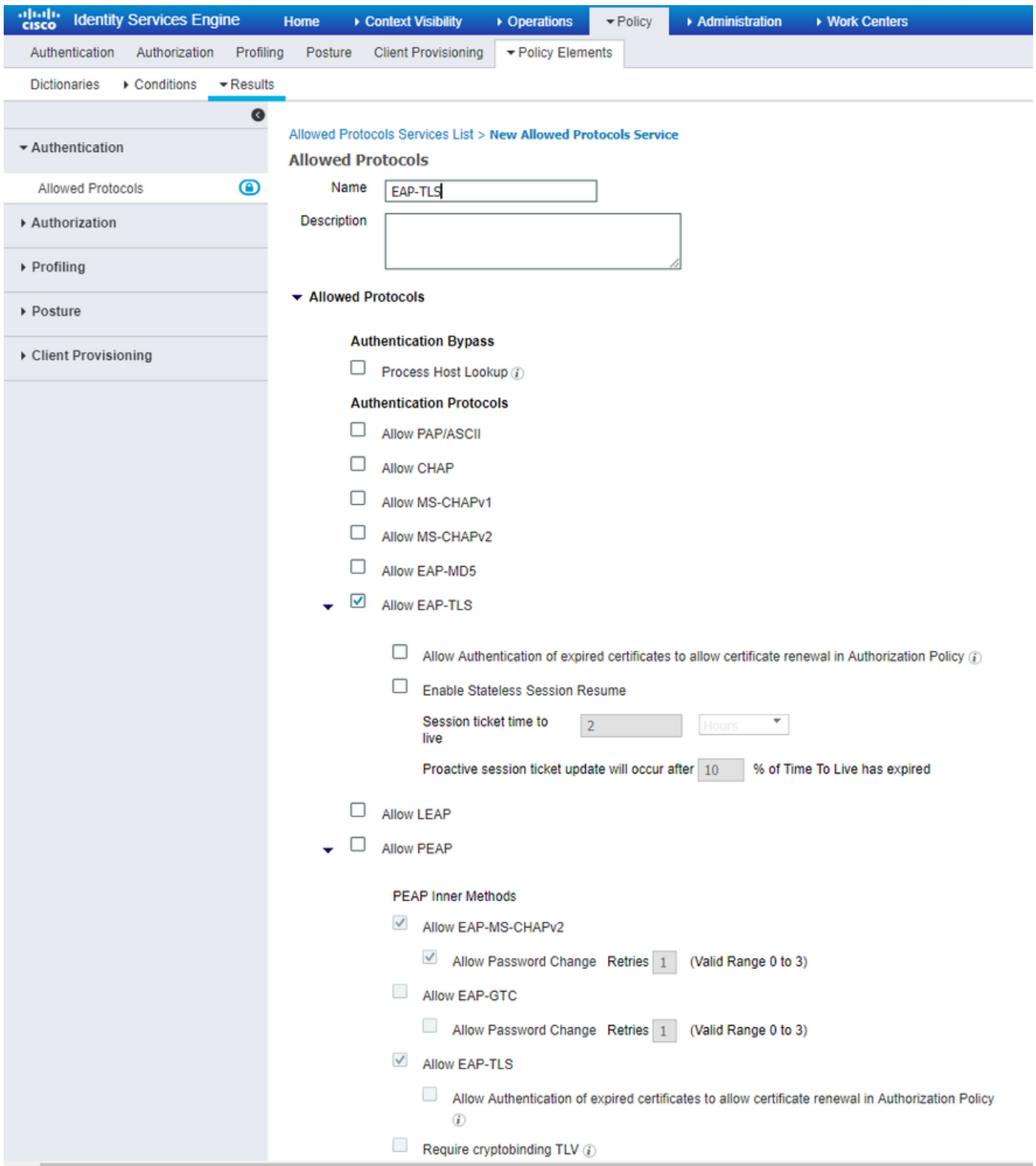
### Allowed Protocols Services

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Edit Add Duplicate Delete

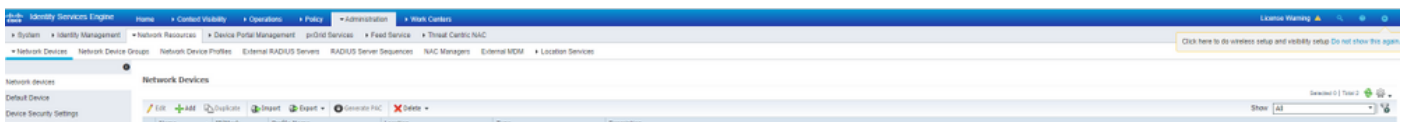
<input type="checkbox"/>	Service Name	Description
<input type="checkbox"/>	Default Network Access	Default Allowed Protocol Service

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 deselectionate, come mostrato nell'immagine.



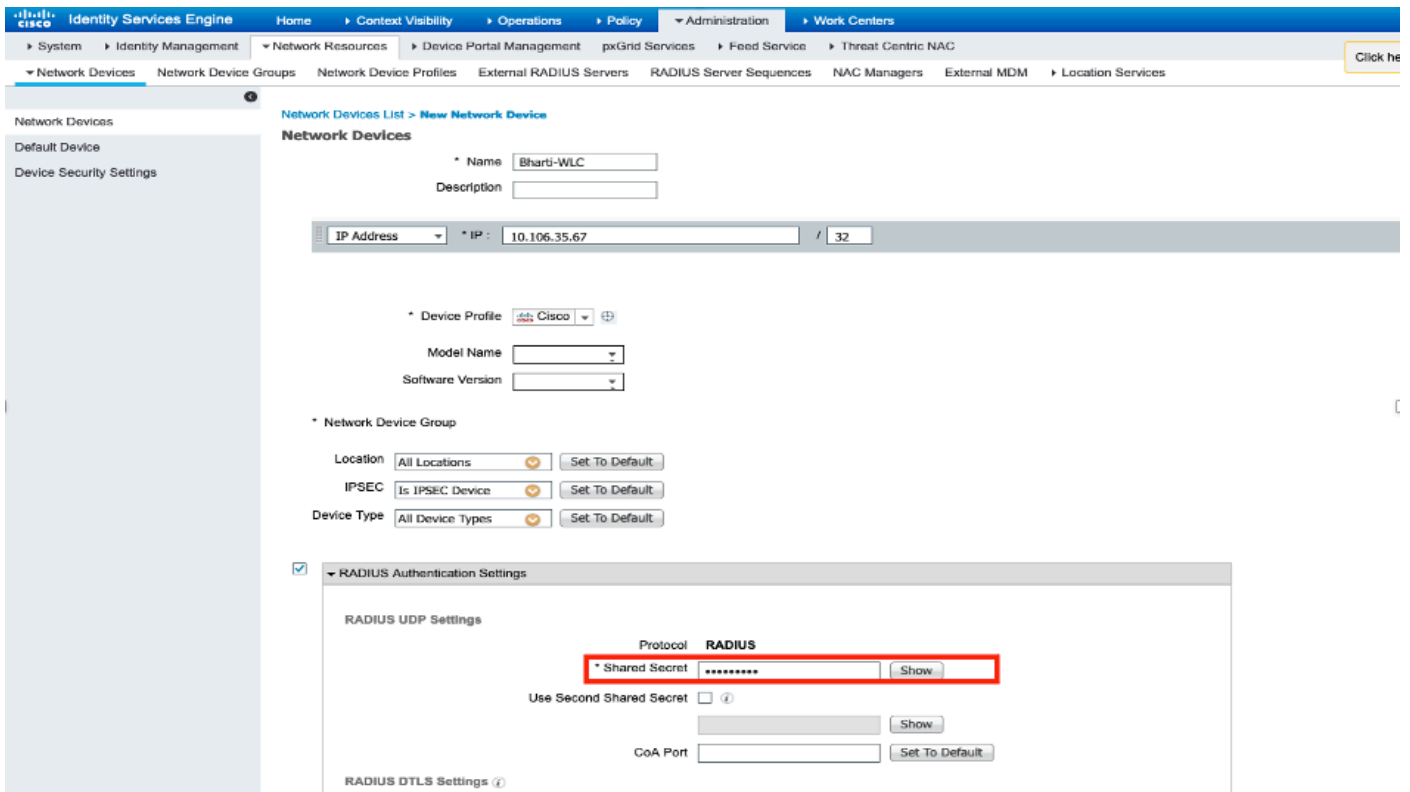
## Impostazioni WLC su ISE

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



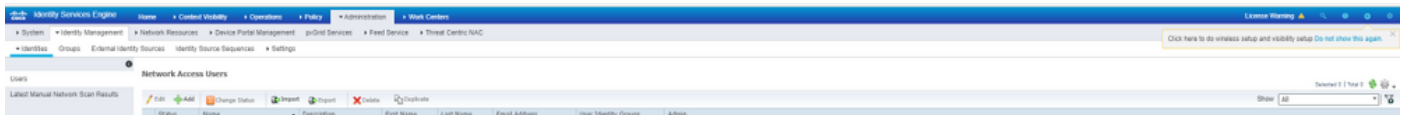
Passaggio 2. Inserire i valori come indicato nell'immagine.





## 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.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users List > New Network Access User

**Network Access User**

\* Name

Status  Enabled

Email

**Passwords**

Password Type:

Password Re-Enter Password

\* 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  (yyyy-mm-dd)

**User Groups**

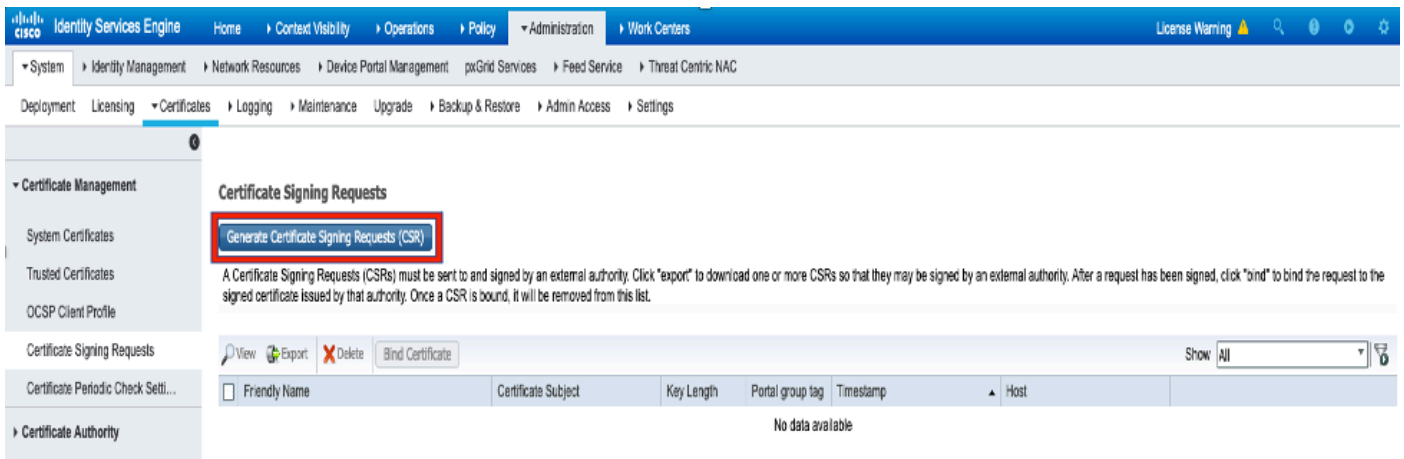
Select an item

## Certificato di attendibilità per ISE

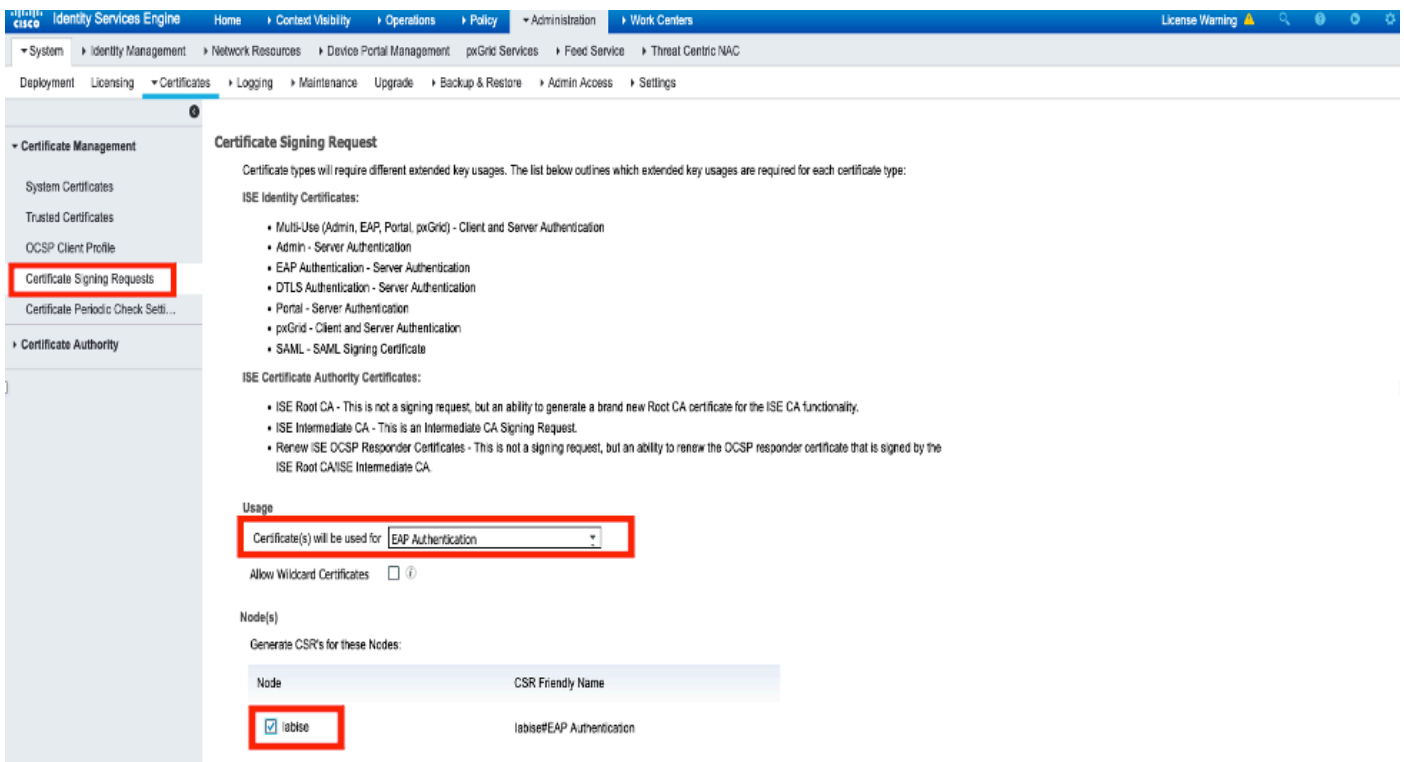
Passaggio 1. Passare ad **Amministrazione > Sistema > Certificati > Gestione certificati > Certificati attendibili**.

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.

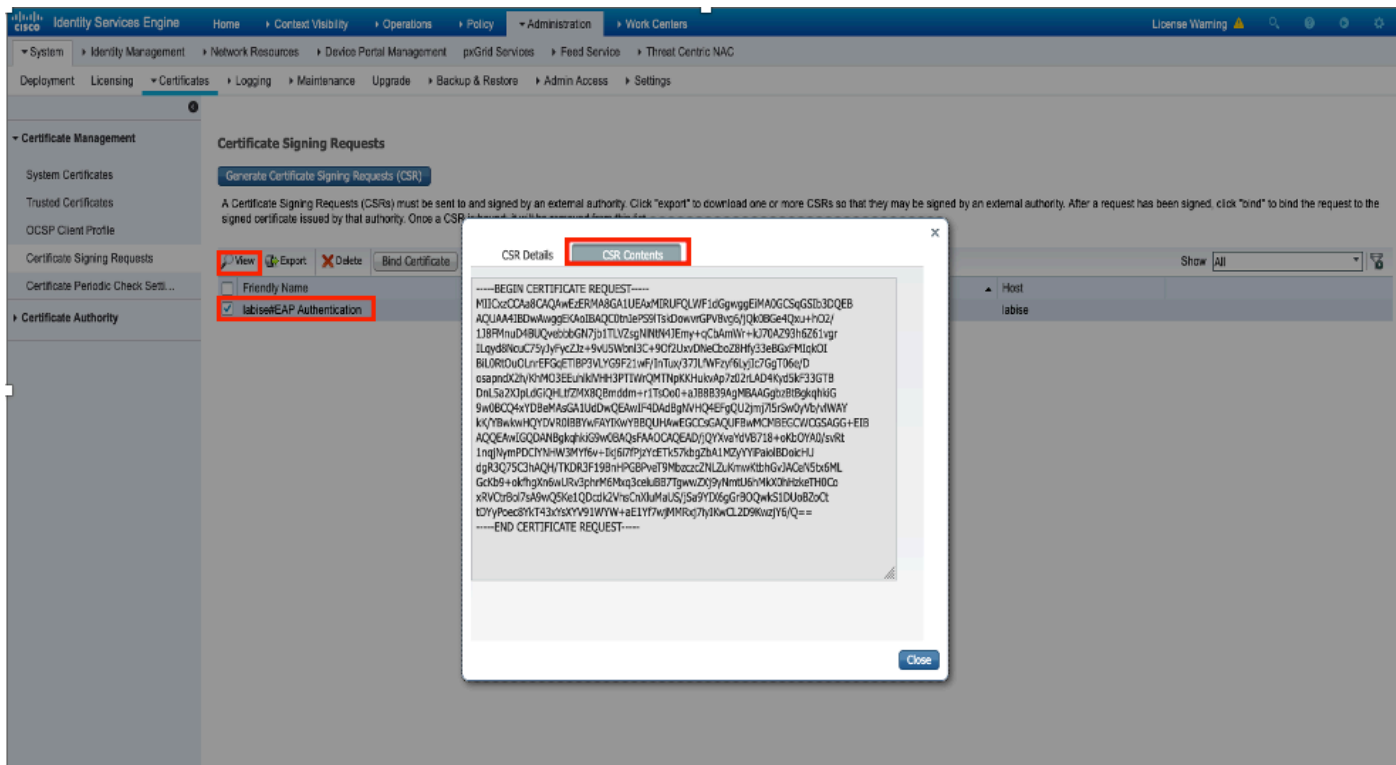
Passaggio 2. Passare a **Amministrazione > Certificati > Richieste di firma del certificato > Genera richieste di firma del certificato (CSR)** come mostrato nell'immagine.



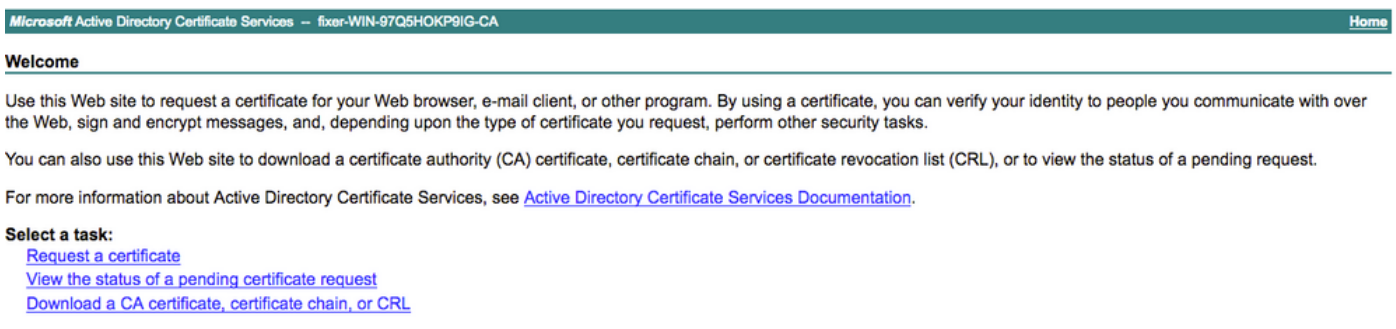
Passaggio 3. Per generare CSR, passare a **Uso** e da **Certificati utilizzati per** le opzioni di elenco a discesa selezionare **Autenticazione EAP** come mostrato nell'immagine.



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.

Microsoft Active Directory Certificate Services -- fixer-WIN-97Q5HOKP9IG-CA

## Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#)

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.

Microsoft Active Directory Certificate Services -- fixer-WIN-97Q5HOKP9IG-CA Home

### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

**Saved Request:**

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

**Certificate Template:**

**Additional Attributes:**

Attributes:


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.

Microsoft Active Directory Certificate Services -- fixer-WIN-97Q5HOKP9IG-CA

## Certificate Issued

The certificate you requested was issued to you.

DER encoded or  **Base 64 encoded**

 [Download certificate](#)  
[Download certificate chain](#)

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.

Identity Services Engine License Warning

Home > Context Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC

Deployment > Licensing > **Certificates** > Logging > Maintenance > Upgrade > Backup & Restore > Admin Access > Settings

Click here to do wireless setup and visibility setup. Do not show this again.

**Certificate Management**

System Certificates

**Trusted Certificates**

Edit Import Export Delete View

Show All

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date
---------------	--------	-------------	---------------	-----------	-----------	------------	-----------------

**Import a new Certificate into the Certificate Store**

\* Certificate File  No file chosen

Friendly Name

**Trusted For:**

Trust for authentication within ISE

Trust for client authentication and Syslog

Trust for authentication of Cisco Services

Validate Certificate Extensions

Description

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.

**Certificate Signing Requests**

[Generate Certificate Signing Requests \(CSR\)](#)

A Certificate Signing Request (CSR) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

<input type="checkbox"/>	Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp	Host
<input checked="" type="checkbox"/>	ise#EAP Authentication	CN=ise.c.com	2048	ise	Mon, 9 Jul 2018	ise

Created by Paint X

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.

**Bind CA Signed Certificate**

\* Certificate File  No file chosen

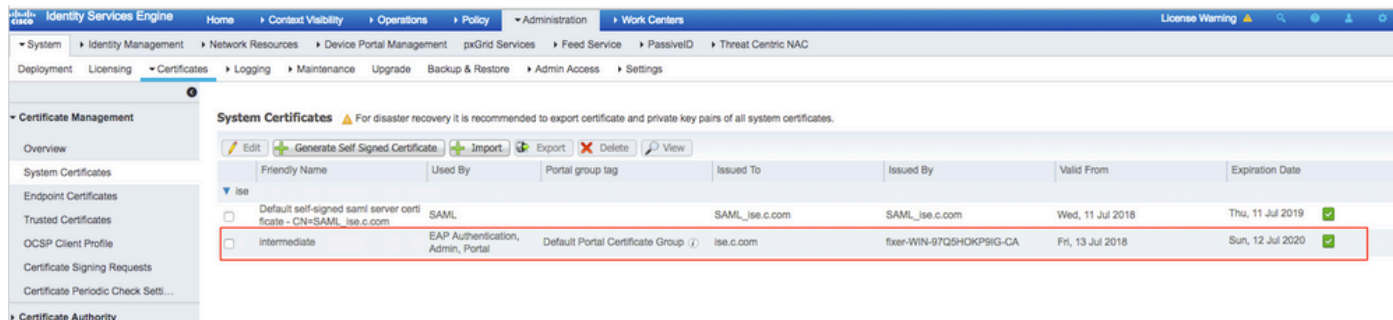
Friendly Name

Validate Certificate Extensions

**Usage**

EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling

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://server 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.

## Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC server) in the Saved Request box.

### Saved Request:

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

```
ZzAJVkd0PEONkCsBJ/3qJJeeM1ZqxnL7BVIspJry  
aF412aLpmDFp1PfVZ3VaP6Oa/mej3IXh0RFxBUII  
weOh06+V+eh7ljeTgiwzEZGr/ceYJIakco5zLjgR  
dD7LeujkxF1j3SwvLTKLDJq+00VtAhrxlp1PyDZ3  
ieC/XQshm/OryD1XuMF4xhq5ZWoloDOJHG1g+dKX  
-----END CERTIFICATE REQUEST-----
```

### Certificate Template:

User

### Additional Attributes:

Attributes:

Submit >

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 **Sfoggia**.



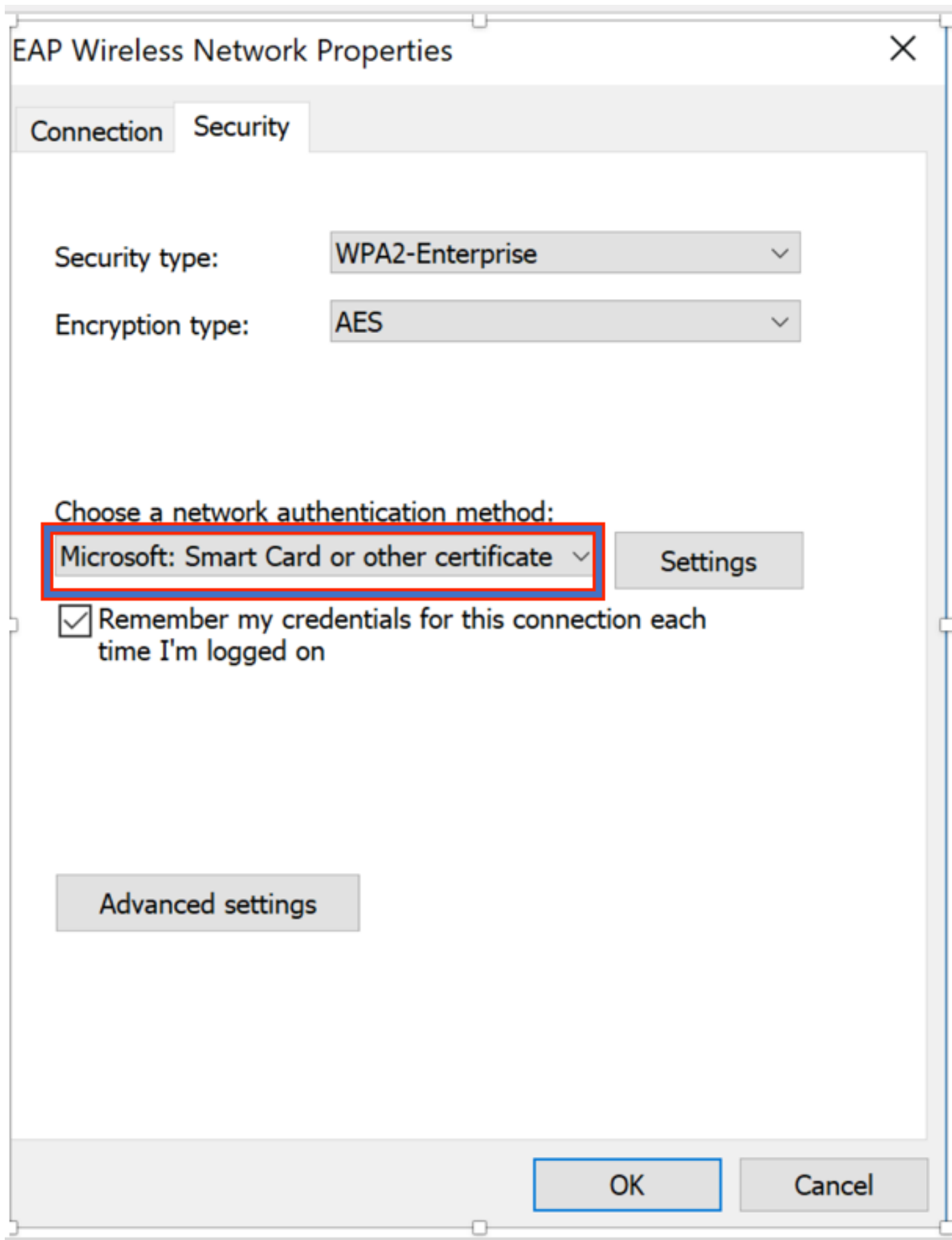
11. Selezionare il file **.cer**, **.crt** o **.pfx** che si desidera importare.
12. Fare clic su **Apri**.
13. Fare clic su **Next** (Avanti).
14. Selezionare **Seleziona automaticamente l'archivio certificati in base al tipo di certificato**.
15. Fare clic su **Fine e OK**

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.

## Smart Card or other Certificate Properties

When connecting:

Use my smart card

Use a certificate on this computer

Advanced

Use simple certificate selection (Recommended)

Verify the server's identity by validating the certificate

Connect to these servers (examples: srv1; srv2; \*.srv3.com):

Trusted Root Certification Authorities:

Entrust.net Certification Authority (2048)

Equifax Secure Certificate Authority

fixer-WIN-97Q5HOKP9IG-CA

GeoTrust Global CA

GeoTrust Primary Certification Authority

GeoTrust Primary Certification Authority - G3

GlobalSign

GlobalSign

GlobalSign Root CA



View Certificate

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

## Advanced settings

802.1X settings

802.11 settings

Specify authentication mode:

User or computer 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

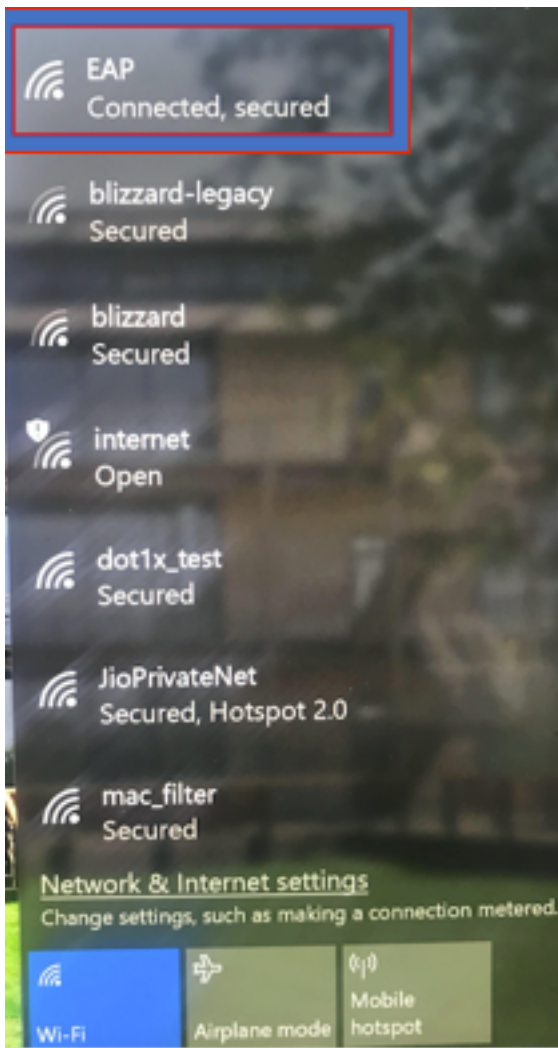
Maximum delay (seconds):

10

Allow additional dialogs to be displayed during single sign on

This network uses separate virtual LANs for machine and user authentication

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.

Monitor

Summary

- Access Points
- Cisco CleanAir
- Statistics
- CDP
- Rogues
- Redundancy
- Clients
  - Sleeping Clients
  - Multicast
  - Applications
  - Lync
  - Local Profiling

Clients > Detail

Max Number of Records  Clear AVC Stats

General **AVC Statistics**

Client Properties		AP Properties	
MAC Address	34:02:86:96:2f:b7	AP Address	00:d7:8f:52:db:a0
IPv4 Address	10.106.32.239	AP Name	Alpha2802_3rdfloor
IPv6 Address	fe80::2818:15a4:65f9:842,	AP Type	802.11bn
		AP radio slot Id	0
		WLAN Profile	EAP
		WLAN SSID	EAP
		Data Switching	Central
		Authentication	Central
		Status	Associated
		Association ID	1
		802.11 Authentication	Open System
Client Type	Simple IP	Reason Code	1
User Name	Administrator	Status Code	0
Port Number	1	CF Pollable	Not Implemented
Interface	management	CF Poll Request	Not Implemented
VLAN ID	32	Short Preamble	Not Implemented
Quarantine VLAN ID	0	PBCC	Not Implemented
CCX Version	CCXv1	Channel Agility	Not Implemented
E2E Version	Not Supported	Re-authentication timeout	1682
Mobility Role	Local	Remaining Re-authentication timeout	0
Mobility Peer IP Address	N/A	WEP State	WEP Enable
Mobility Move Count	0		
<b>Policy Manager State</b>	<b>RUN</b>		
Management Frame Protection	No		
UpTime (Sec)	146		

**Lync Properties**

Lync State	Disabled
Audio Qos Policy	Silver

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

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Auth Key Mgmt	802.1x
Encryption Cipher	CCMP (AES)
<b>EAP Type</b>	<b>EAP-TLS</b>
SNMP NAC State	Access
Radius NAC State	RUN
CTS Security Group Tag	Not Applicable
AAA Override ACL Name	none
AAA Override ACL Applied Status	Unavailable
AAA Override Flex ACL	none
AAA Override Flex ACL Applied Status	Unavailable
Redirect URL	none
IPv4 ACL Name	none
FlexConnect ACL Applied Status	Unavailable
IPv4 ACL Applied	Unavailable

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.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The breadcrumb navigation is: Endpoints > 34:02:86:96:2F:B7. The main header includes 'Identity Services Engine' and navigation tabs for 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. Below the header, there are tabs for 'Endpoints' and 'Network Devices'. The main content area shows the endpoint details for MAC address 34:02:86:96:2F:B7, including fields for MAC Address, Username (Administrator@flxer.com), Endpoint Profile (Intel-Device), Current IP Address, and Location. Below this, there are tabs for 'Attributes', 'Authentication', 'Threats', and 'Vulnerabilities'. The 'Attributes' tab is active, showing 'General Attributes' and 'Custom Attributes'. The 'General Attributes' section includes a description and several key-value pairs: Static Assignment (false), Endpoint Policy (Intel-Device), Static Group Assignment (false), and Identity Group Assignment (Profiled). The 'Custom Attributes' section is empty, with a message 'No data found. Add custom attributes here.' and a 'Filter' button. Below this, there is a table for 'Other Attributes' with the following entries:

Attribute Name	Attribute Value
AAA-Server	ise
AKI	88:20:a7:c9:96:03:5a:26:58:fd:67:58:83:71:e8:bc:c6:6d:97:bd
Airespace-Wlan-Id	5
AllowedProtocolMatchedRule	Dot1X
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	x509 PKI



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 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).