

Comprendere e configurare EAP-TLS con Mobility Express e ISE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Flusso EAP-TLS](#)

[Fasi del flusso EAP-TLS](#)

[Configurazione](#)

[Cisco Mobility Express](#)

[ISE con Cisco Mobility Express](#)

[Impostazioni EAP-TLS](#)

[Impostazioni di Mobility Express su 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

In questo documento viene descritto come configurare una rete WLAN (Wireless Local Area Network) con sicurezza 802.1x in un controller Mobility Express. Questo documento spiega anche l'uso del protocollo EAP (Extensible Authentication Protocol) - TLS (Transport Layer Security) in particolare.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione iniziale di Mobility Express
- processo di autenticazione 802.1x
- Certificati

Componenti usati

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

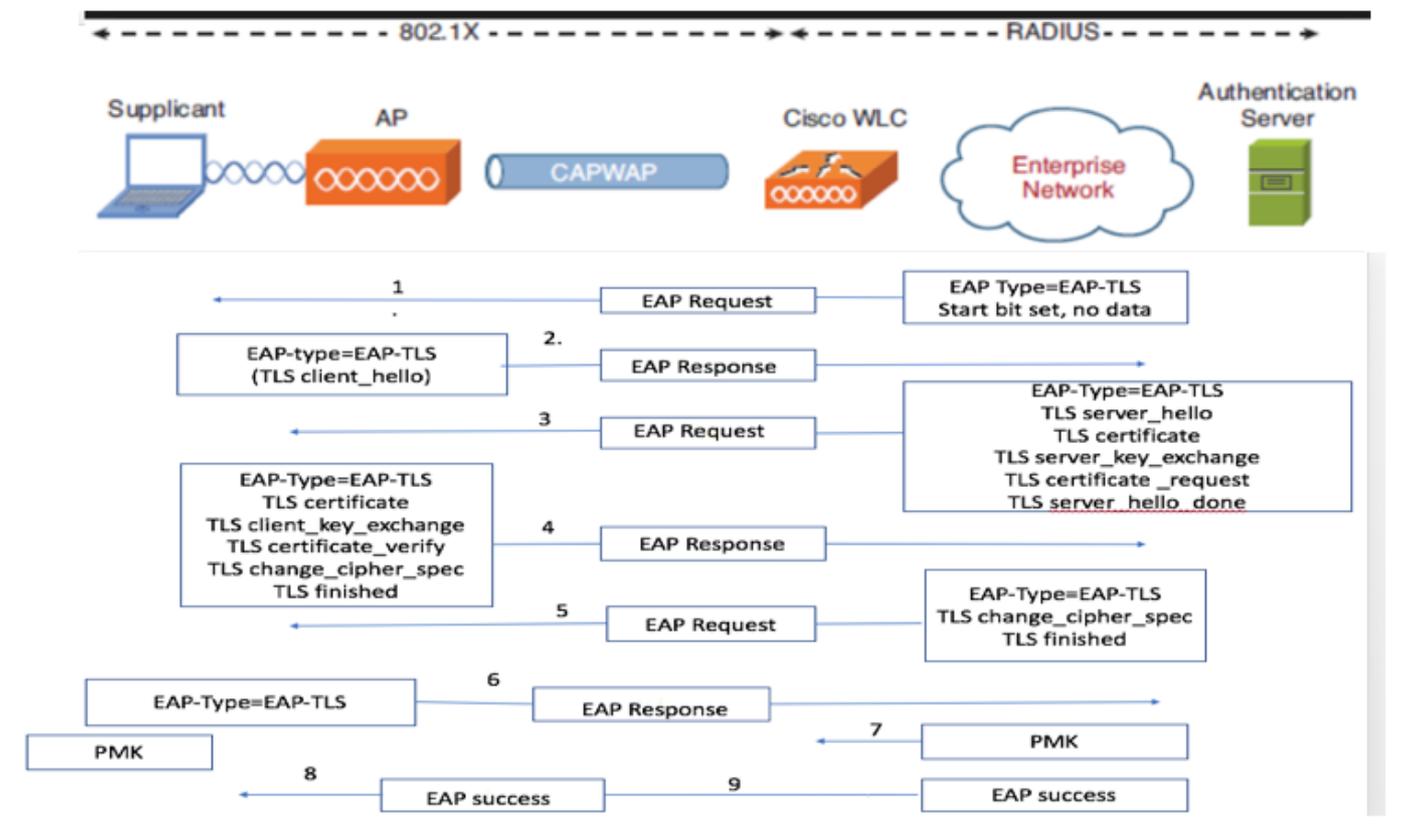
hardware:

- WLC 5508 versione 8.5
- Identity Services Engine (ISE) versione 2.1

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

6. 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.
```

7. 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
```

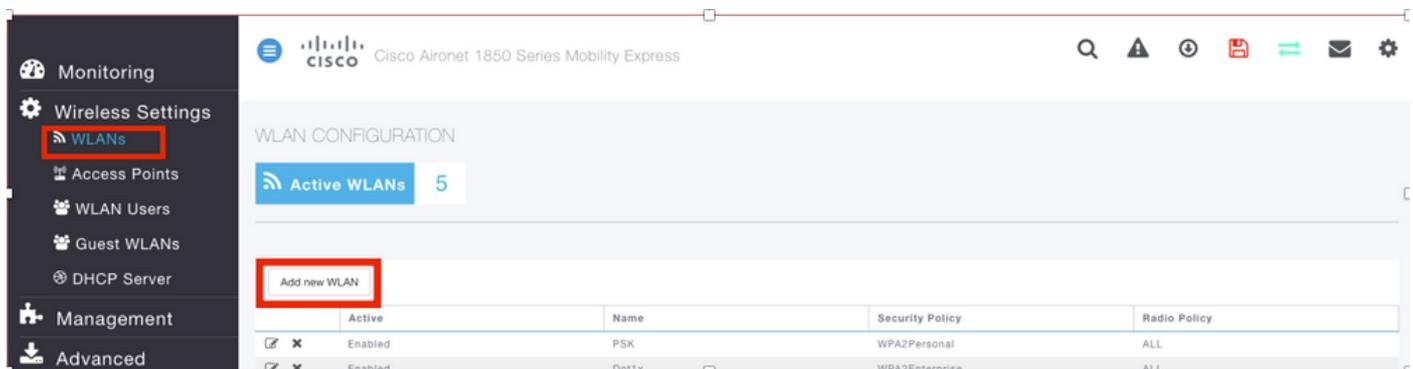
8. Una volta completata l'autenticazione del client, il server RADIUS risponde con una richiesta di verifica di accesso, contenente il messaggio "change_cipher_spec" e il messaggio di completamento dell'handshake. Alla ricezione di questo messaggio, il client verifica l'hash per autenticare il server RADIUS. Una nuova chiave di crittografia viene derivata in modo dinamico dal segreto durante l'handshake TLS.

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

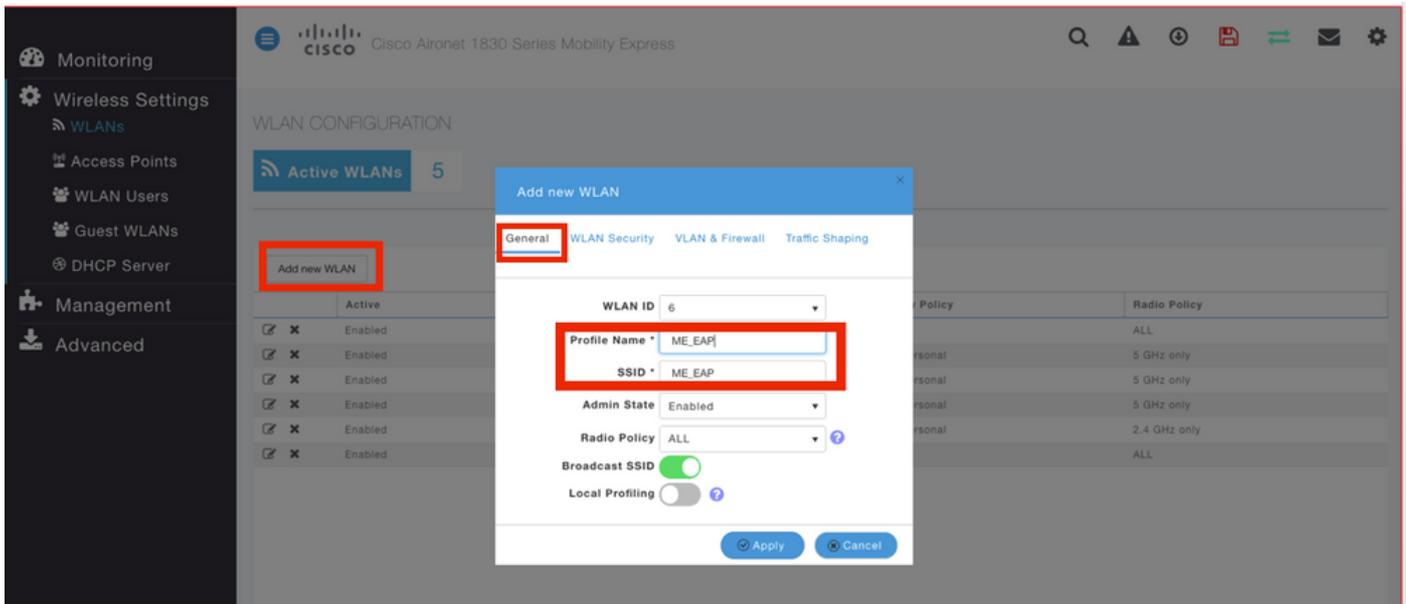
Configurazione

Cisco Mobility Express

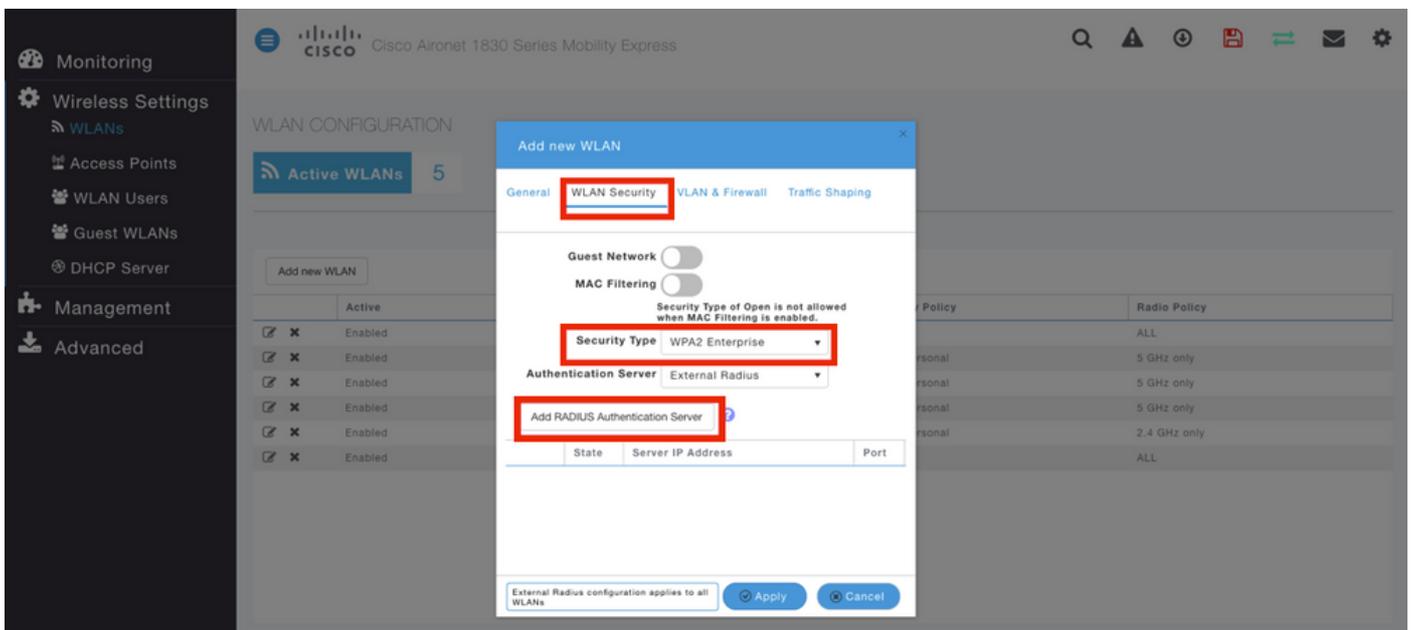
Passaggio 1. Il primo passaggio consiste nella creazione di una WLAN su Mobility Express. Per creare una WLAN, selezionare **WLAN > Add new WLAN** (Aggiungi nuova WLAN), come mostrato nell'immagine.



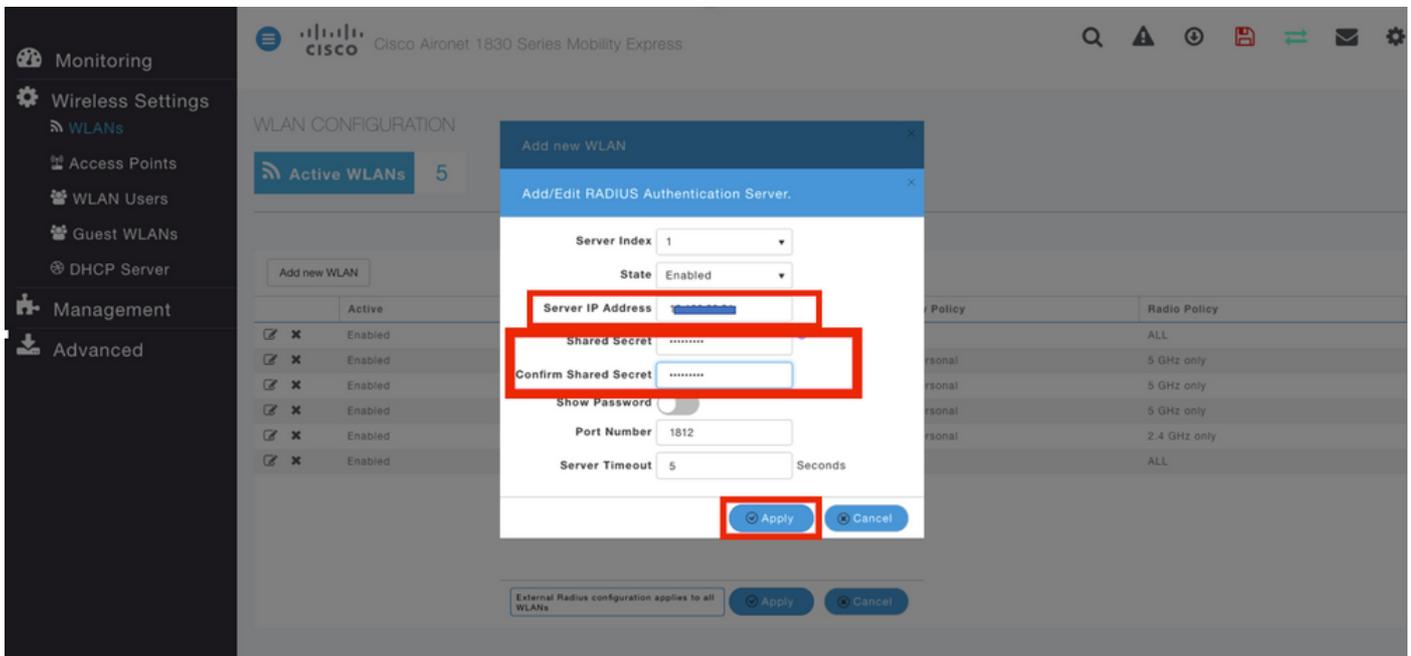
Passaggio 2. Una volta fatto clic su **Add new WLAN**, viene visualizzata una nuova finestra popup. Per creare un nome di profilo, selezionare **Add new WLAN > General** (Aggiungi nuova WLAN > Generale), come mostrato nell'immagine.



Passaggio 3. Configurare il tipo di autenticazione come WPA Enterprise per 802.1x e configurare il server RADIUS in **Aggiungi nuova WLAN > Sicurezza WLAN**, come mostrato nell'immagine.



Passaggio 4. Fare clic su **Add RADIUS Authentication Server** (Aggiungi server di autenticazione RADIUS) e fornire l'indirizzo IP del server RADIUS e il segreto condiviso che devono corrispondere esattamente a quello configurato su ISE, quindi fare clic su **Apply** (Applica), come mostrato nell'immagine.



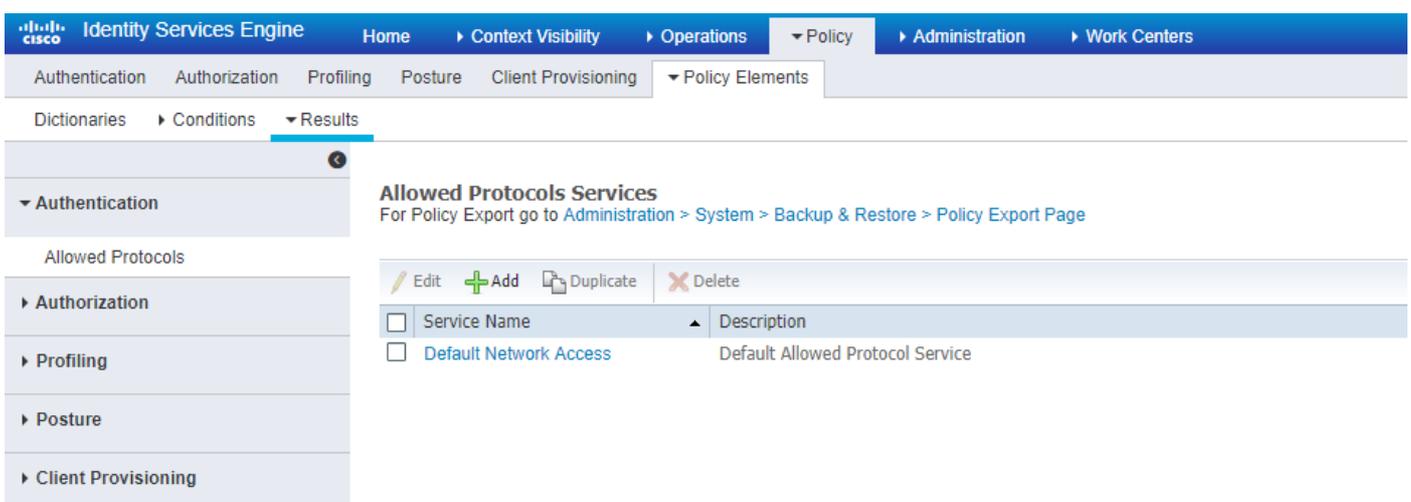
ISE con Cisco Mobility Express

Impostazioni EAP-TLS

Per creare il criterio, è necessario creare l'elenco dei 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 potrebbe non essere preferibile 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 deselectionate, come mostrato nell'immagine.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main menu includes Authentication, Authorization, Profiling, Posture, Client Provisioning, and Policy Elements. The left sidebar shows a tree view with Authentication selected, containing sub-items: Allowed Protocols, Authorization, Profiling, Posture, and Client Provisioning. The main content area is titled "Allowed Protocols Services List > New Allowed Protocols Service". The "Allowed Protocols" section has a "Name" field containing "EAP-TLS" and an empty "Description" field. Below this, the "Allowed Protocols" list is expanded to show "Authentication Bypass" (Process Host Lookup), "Authentication Protocols" (Allow PAP/ASCII, Allow CHAP, Allow MS-CHAPv1, Allow MS-CHAPv2, Allow EAP-MD5, Allow EAP-TLS), and "PEAP Inner Methods" (Allow EAP-MS-CHAPv2, Allow Password Change, Allow EAP-GTC, Allow Password Change, Allow EAP-TLS, Allow Authentication of expired certificates, Require cryptobinding TLV). The "Allow EAP-TLS" checkbox is checked. The "Session ticket time to live" is set to 2 hours, and the "Proactive session ticket update" is set to occur after 10% of the Time To Live has expired.

Impostazioni di Mobility Express su ISE

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

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface for Network Devices. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main menu includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, PassiveID, and Threat Centric NAC. The left sidebar shows a tree view with Network Resources selected, containing sub-items: Network Devices, Network Device Groups, Network Device Profiles, External RADIUS Servers, RADIUS Server Sequences, NAC Managers, External MDM, and Location Services. The main content area is titled "Network Devices". The "Network devices" section is highlighted with a red box. Below this, the "Default Device" section is visible. The "Add" button is highlighted with a red box. The table below shows columns for Name, IP/Mask, Profile Name, Location, Type, and Description.

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

The screenshot shows the 'New Network Device' configuration page in Cisco ISE. The 'RADIUS Authentication Settings' section is expanded, showing the following fields:

- Enable Authentication Settings:
- Protocol: RADIUS
- Shared Secret: (with a 'Show' button)
- Enable KeyWrap:
- Key Encryption Key: (with a 'Show' button)
- Message Authenticator Code Key: (with a 'Show' button)
- Key Input Format: ASCII HEXADECIMAL
- CoA Port: 1700 (with a 'Set To Default' button)

Below the RADIUS settings, there are three sections that are collapsed:

- TACACS Authentication Settings
- SNMP Settings
- Advanced TrustSec Settings

At the bottom, there are 'Submit' and 'Cancel' buttons. The 'Submit' button is highlighted with a red box.

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. A tale scopo, è necessario 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.

The screenshot shows the 'Certificate Signing Requests' page in Cisco ISE. The page displays a table of CSR requests. The table has the following columns: Friendly Name, Certificate Subject, Key Length, Portal group tag, Timestamp, and Host. One request is listed with the following details:

Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp	Host
<input type="checkbox"/> ise#EAP Authentication	CN#ise.c.com	2048	ise	Wed, 11 Jul 2018	ise

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

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

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**.

Dall'opzione a discesa **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.

Certificate Issued

The certificate you requested was issued to you.

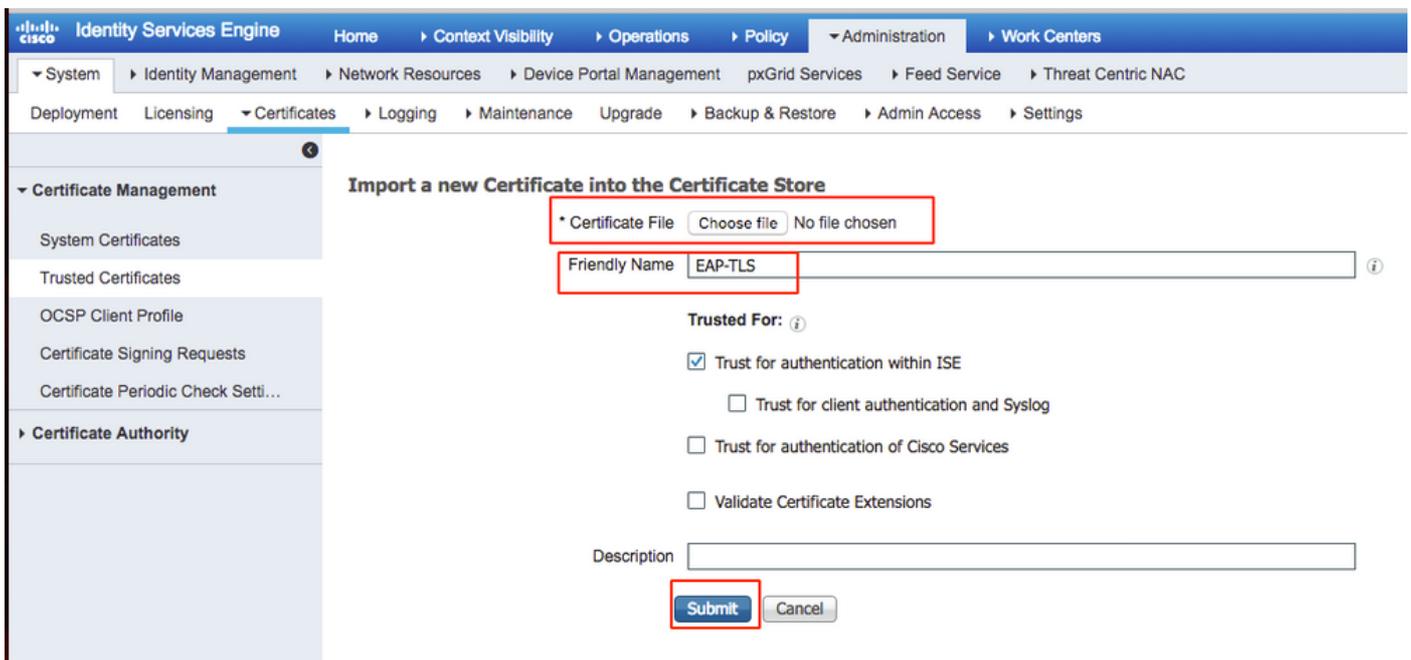
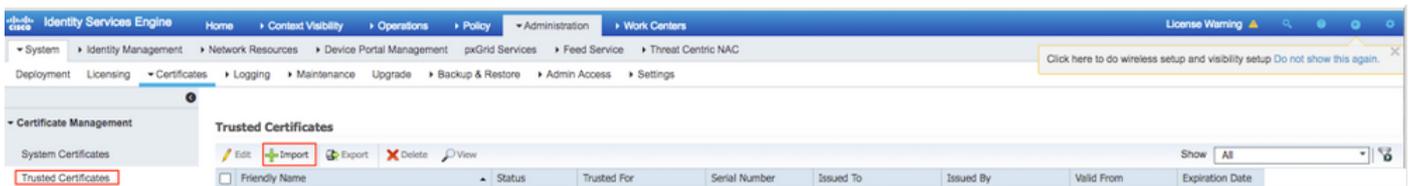
DER encoded or Base 64 encoded



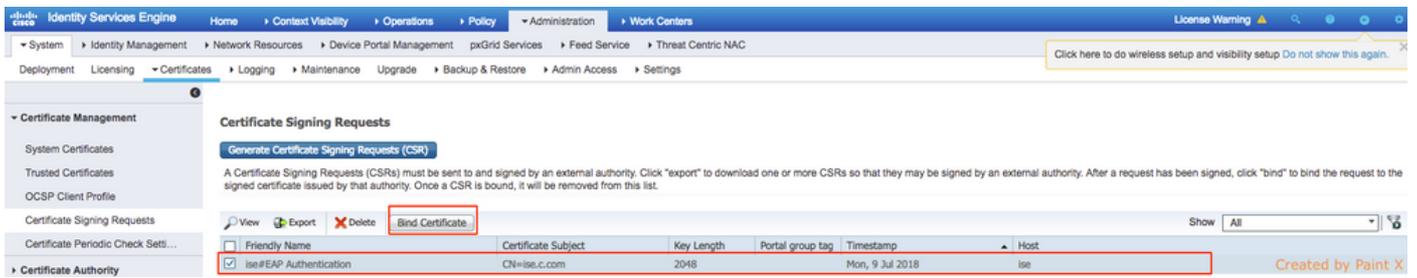
[Download certificate](#)

[Download certificate chain](#)

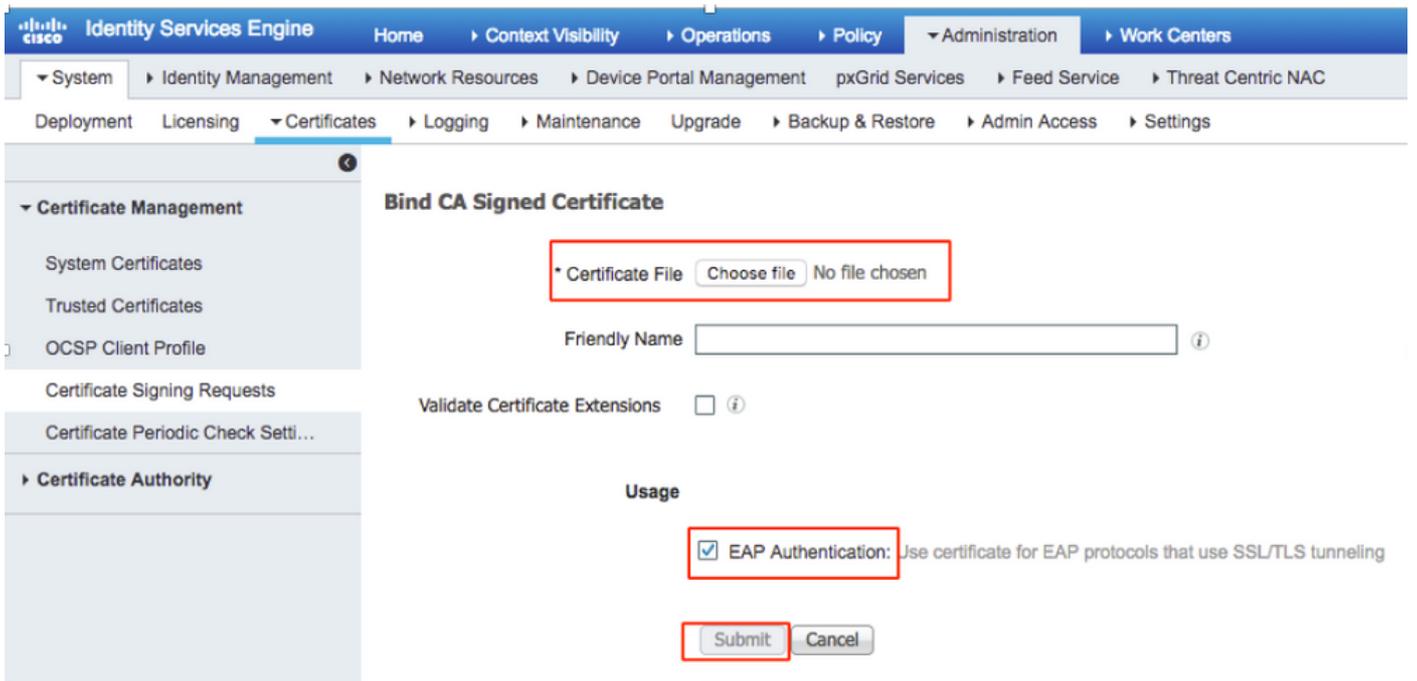
Passaggio 9. Il download del certificato per il server ISE è completato. È possibile estrarre il certificato. Il certificato conterrà due certificati, un certificato radice e un altro intermedio. Il certificato radice può essere importato in **Amministrazione > Certificati > Certificati attendibili >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



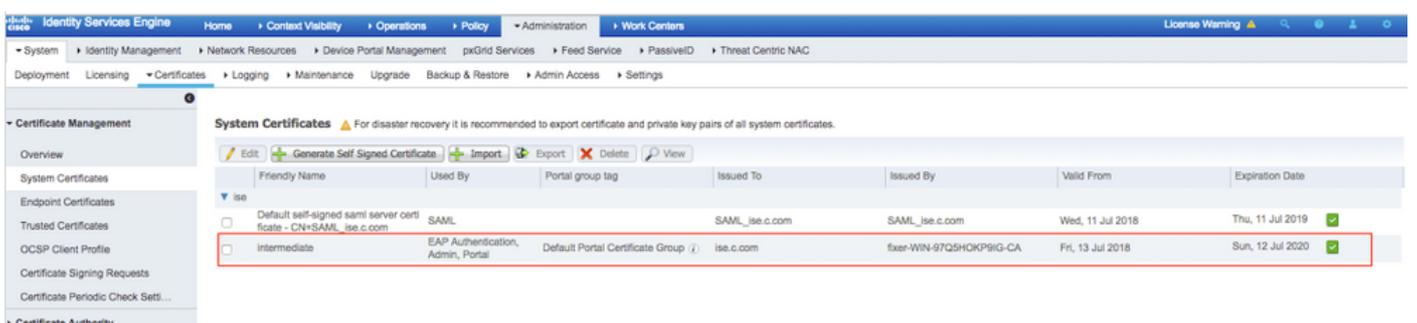
Passaggio 10. Dopo aver fatto clic su **Invia**, il certificato viene aggiunto all'elenco dei certificati attendibili. Inoltre, il certificato intermedio è necessario per il collegamento con CSR, come mostrato nell'immagine.



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.

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

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  
aF4l2aLpmDFp1PfvZ3VaP6Oa/mej3IXh0RFxBUII  
weOh06+V+eh7ljeTgiwzEZGr/ceYJIakco5zLjgR  
dD7LeujkxFlj3SwvLTKLDJq+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**.

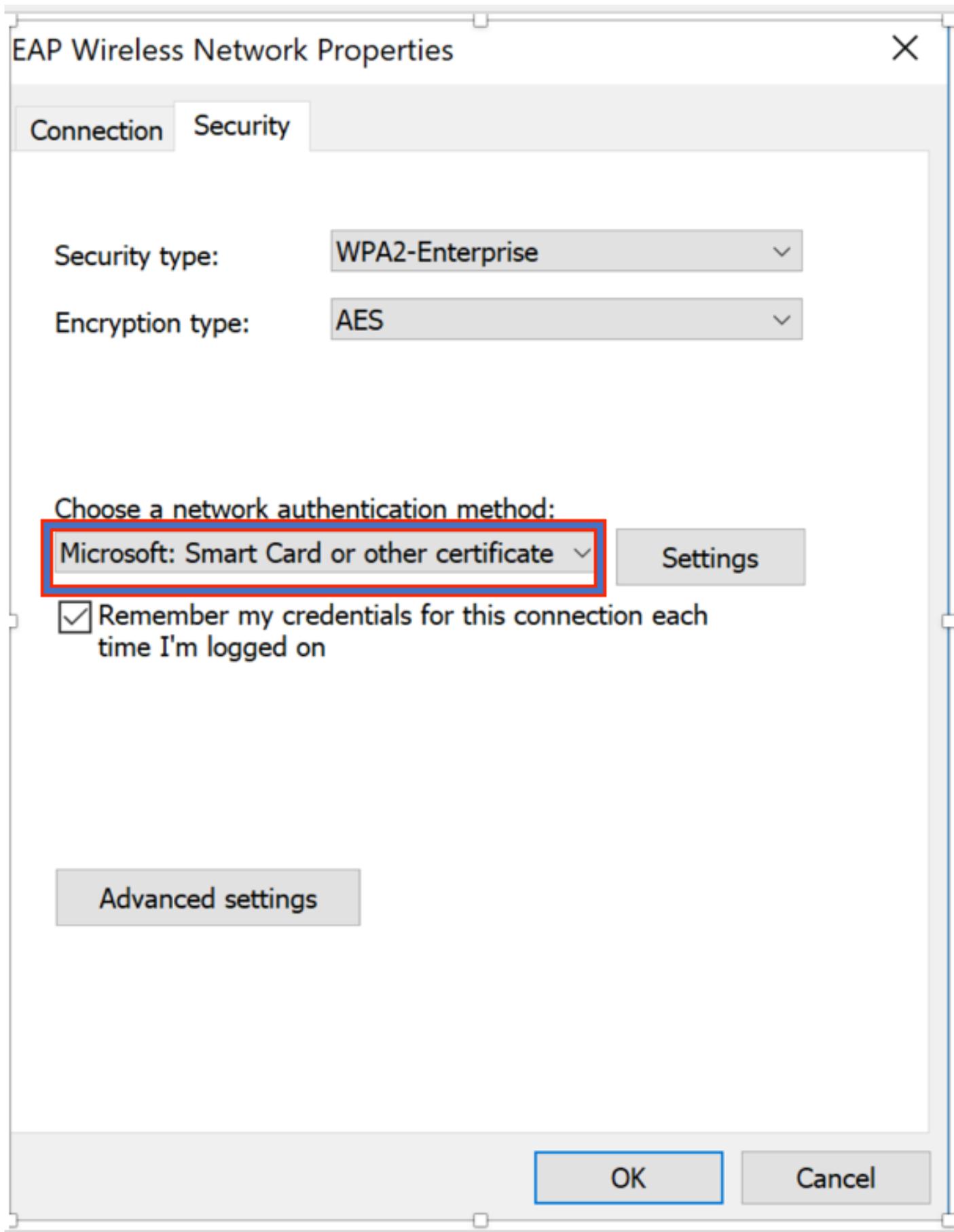
7. Fare clic su **[+]** accanto a **Certificati > Personali > Certificati**.
8. Fare clic con il pulsante destro del mouse su **Certificati** e selezionare **Tutte le attività > Importa**.
9. Fare clic su **Next** (Avanti).
10. Fare clic su **Sfogli**.
11. Selezionare il file **.cer, .crt o .pfx** che 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 PEAP (Protected Extensible Authentication Protocol) in modo da utilizzare EAP-TLS. Fare clic su **EAP Wireless Profile**.

Passaggio 2. Selezionare **Microsoft: Smart Card o altro certificato** e fare clic su **OK**, come mostrato 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

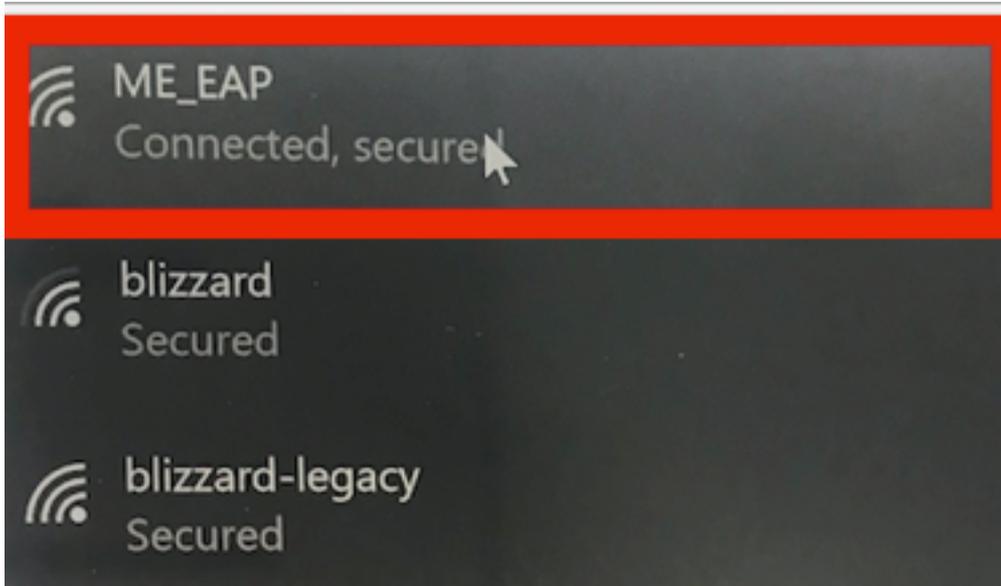
Maximum delay (seconds):

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. Il tipo EAP del client deve essere EAP-TLS. Ciò significa che il client ha completato l'autenticazione, con l'uso di EAP-TLS, ha ottenuto l'indirizzo IP ed è pronto a passare il traffico, come mostrato nelle immagini.

The screenshot displays a network management interface with a sidebar on the left and a main content area. The sidebar includes sections for Monitoring, Applications, Rogues, Interferers, Wireless Dashboard, Best Practices, Wireless Settings, Management, and Advanced. The main content area is titled 'CLIENT VIEW' and shows details for a client with SSID 'ME_EAP'. The 'GENERAL' section includes fields for User Name (Administrator), Host Name (Unknown), MAC Address (34:02:86:96:2f:b7), Uptime (Associated since 37 Seconds), AP Name (AP442b.03a9.7f72 (Ch 56)), Nearest APs, Device Type, Performance (Signal Strength: 0 dBm, Signal Quality: 0 dB, Connection Speed: 0, Channel Width: 40 MHz), Capabilities (802.11n (5GHz) Spatial Stream: 0), Cisco Compatible (Supported (CCX v 4)), and Connection Score (0%). The 'CONNECTIVITY' section shows a flow diagram with steps: Start, Association, Authentication, DHCP, and Online. The 'TOP APPLICATIONS' section shows a table with columns for Name, Usage, and % Usage, with the message 'No Data Available!'. The 'MOBILITY STATE' section shows a diagram of the network path: WLC (LOCAL) -> Wired (CAP-WAP) -> AP (FlexConnect) -> Wireless (802.11n (5GHz)) -> Client (VLAN1).

The screenshot displays the Cisco ISE GUI for a client's configuration. The left sidebar shows navigation options like 'Monitoring', 'Wireless Settings', and 'Management'. The main area is divided into several sections:

- MOBILITY STATE:** A diagram showing the client's path from WLC (LOCAL) through Wired (CAPWAP) and AP (FlexConnect) to Wireless (802.11n (5GHz)) and finally to the Client (VLAN1).
- NETWORK & QOS:** A table listing network parameters such as IP Address (10.127.209.55), IPv6 Address (fe80::2818:15a4:65f9:842), VLAN (1), and QoS Level (Silver).
- SECURITY & POLICY:** A table showing security settings. Two rows are highlighted with red boxes: 'Key Management' with status '802.1x' and 'EAP Type' with status 'EAP-TLS'.
- CLIENT TEST:** A section with tabs for 'PING TEST', 'CONNECTION', 'EVENT LOG', and 'PACKET CAPTURE'.

Passaggio 2. Ecco i dettagli del client dalla CLI del controller (output troncato):

```
(Cisco Controller) > show client detail 34:02:86:96:2f:b7
Client MAC Address..... 34:02:86:96:2f:b7
Client Username ..... Administrator
AP MAC Address..... c8:f9:f9:83:47:b0
AP Name..... AP442b.03a9.7f72
AP radio slot Id..... 1
Client State..... Associated
Client User Group..... Administrator
Client NAC OOB State..... Access
Wireless LAN Id..... 6
Wireless LAN Network Name (SSID)..... ME_EAP
Wireless LAN Profile Name..... ME_EAP
Hotspot (802.11u)..... Not Supported
BSSID..... c8:f9:f9:83:47:ba
Connected For ..... 18 secs
Channel..... 56
IP Address..... 10.127.209.55
Gateway Address..... 10.127.209.49
Netmask..... 255.255.255.240
IPv6 Address..... fe80::2818:15a4:65f9:842
--More-- or (q)uit
Security Policy Completed..... Yes
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 3. Su ISE, selezionare **Context Visibility > End Points > Attributes**, come mostrato nelle immagini.

Endpoints > 34:02:86:96:2F:B7

34:02:86:96:2F:B7   



MAC Address: 34:02:86:96:2F:B7
Username: Administrator@fixer.com
Endpoint Profile: Intel-Device
Current IP Address:
Location:

Attributes Authentication Threats Vulnerabilities

General Attributes

Description

Static Assignment	false
Endpoint Policy	Intel-Device
Static Group Assignment	false
Identity Group Assignment	Profiled

Custom Attributes

Filter 

Attribute Name	Attribute Value
x <input type="text" value="Attribute Name"/>	<input type="text" value="Attribute Value"/>

No data found. Add custom attributes here.

Other Attributes

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	6
AllowedProtocolMatchedRule	Dot1X
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	x509_PKI
AuthorizationPolicyMatchedRule	Basic_Authenticated_Access

BYODRegistration	Unknown
Called-Station-ID	c8-f9-f9-83-47-b0:ME_EAP
Calling-Station-ID	34-02-86-96-2f-b7
Days to Expiry	344
DestinationIPAddress	10.106.32.31
DestinationPort	1812
DetailedInfo	Invalid username or password specified
Device IP Address	10.127.209.56
Device Port	32775
Device Type	Device Type#All Device Types
DeviceRegistrationStatus	NotRegistered
ElapsedDays	21
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, 1.3.6.1.4.1.311.1f
FailureReason	12935 Supplicant stopped responding to ISE during
IdentityGroup	Profiled
InactiveDays	0
IsThirdPartyDeviceFlow	false
Issuer	CN=fixer-WIN-97Q5HOKP9IG-CA,DC=fixer,DC=cc
Issuer - Common Name	fixer-WIN-97Q5HOKP9IG-CA
Issuer - Domain Component	fixer, com
Key Usage	0, 2
Location	Location#All Locations
MACAddress	34:02:86:96:2F:B7

MatchedPolicy	Intel-Device
MessageCode	5411
NAS-IP-Address	10.127.209.56
NAS-Identifier	ryo_ap
NAS-Port	1
NAS-Port-Type	Wireless - IEEE 802.11
Network Device Profile	Cisco
NetworkDeviceGroups	Location#All Locations, Device Type#All Device Types
NetworkDeviceName	ryo_ap
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"
OpenSSLStack	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	Drop
SSID	c8-f9-f9-83-47-b0:ME_EAP
SelectedAccessService	Default Network Access
SelectedAuthenticationIdentityStores	EAPTLS
SelectedAuthorizationProfiles	PermitAccess
Serial Number	10 29 41 78 00 00 00 00 11
Service-Type	Framed
StaticAssignment	false
StaticGroupAssignment	false
StepData	4=Dot1X

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.