

Autenticazione EAP-FAST con Wireless LAN Controller e Identity Services Engine

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Premesse](#)

[PAC](#)

[Modalità di provisioning PAC](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configurazione del WLC per l'autenticazione EAP-FAST](#)

[Configurazione del WLC per l'autenticazione RADIUS tramite un server RADIUS esterno](#)

[Configurazione della WLAN per l'autenticazione EAP-FAST](#)

[Configurazione del server RADIUS per l'autenticazione EAP-FAST](#)

[Creazione di un database utenti per autenticare i client EAP-FAST](#)

[Aggiungere il WLC come client AAA al server RADIUS](#)

[Configurazione dell'autenticazione EAP-FAST sul server RADIUS con provisioning PAC in banda anonimo](#)

[Configurazione dell'autenticazione EAP-FAST sul server RADIUS con provisioning della PAC in-band autenticato](#)

[Verifica](#)

[Configurazione profilo NAM](#)

[Verificare la connettività a SSID utilizzando l'autenticazione EAP-FAST.](#)

[Log di autenticazione ISE](#)

[Debug lato WLC sul flusso EAP-FAST completato](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene spiegato come configurare il controller WLC (Wireless LAN Controller) per l'autenticazione EAP (Extensible Authentication Protocol) - Autenticazione flessibile tramite autenticazione FAST (Secure Tunneling) con l'utilizzo di un server RADIUS esterno. In questo esempio di configurazione viene utilizzato Identity Services Engine (ISE) come server RADIUS esterno per autenticare il client wireless.

In questo documento viene illustrato come configurare ISE per la configurazione delle credenziali di accesso protetto (PAC) in banda anonime e autenticate per i client wireless.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Conoscenze base della configurazione dei Lightweight Access Point (LAP) e dei Cisco WLC
- Conoscenze base del protocollo CAPWAP
- Informazioni su come configurare un server RADIUS esterno, ad esempio Cisco ISE
- Conoscenze funzionali del quadro generale EAP
- Conoscenze base dei protocolli di sicurezza, ad esempio MS-CHAPv2 e EAP-GTC, e conoscenze dei certificati digitali

Componenti usati

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

- Cisco serie 5520 WLC con firmware versione 8.8.11.0 Cisco serie 4800 APAnyconnect NAM. Cisco Secure ISE versione 2.3.0.298 Cisco serie 3560-CX Switch con versione 15.2(4)E1

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.

Convenzioni

Fare riferimento a [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.](#)

Premesse

Il protocollo EAP-FAST è un tipo EAP IEEE 802.1X accessibile al pubblico sviluppato da Cisco per supportare i clienti che non possono applicare policy per la password complesse e desiderano distribuire un tipo EAP 802.1X che non richiede certificati digitali.

Il protocollo EAP-FAST è un'architettura di sicurezza client-server che cripta le transazioni EAP con un tunnel TLS (Transport Level Security). La creazione del tunnel EAP-FAST si basa su segreti sicuri specifici degli utenti. Questi segreti si chiamano PAC, che l'ISE genera utilizzando una chiave master nota solo all'ISE.

EAP-FAST si articola in tre fasi:

- **Fase zero (fase di preparazione automatica della PAC)** - Fase zero di EAP-FAST, una fase opzionale è un mezzo protetto dal tunnel per fornire a un client utente finale EAP-FAST una PAC per l'utente che richiede l'accesso alla rete. **L'unico scopo della fase zero è fornire una PAC al client dell'utente finale.** Nota: la fase zero è facoltativa in quanto le PAC possono

anche essere assegnate manualmente ai client anziché utilizzare la fase zero. Per ulteriori informazioni, vedere la sezione [Modalità di provisioning PAC](#) di questo documento.

- **Fase 1:** nella fase 1, l'ISE e il client dell'utente finale stabiliscono un tunnel TLS in base alle credenziali PAC dell'utente. Questa fase richiede che il client dell'utente finale disponga di una PAC per l'utente che sta tentando di ottenere l'accesso alla rete e che la PAC sia basata su una chiave master non scaduta. Nessun servizio di rete abilitato dalla fase uno di EAP-FAST.
- **Fase due:** nella fase due, le credenziali di autenticazione utente vengono passate in modo sicuro utilizzando un metodo EAP interno supportato da EAP-FAST all'interno del tunnel TLS al RADIUS creato utilizzando la PAC tra il client e il server RADIUS. EAP-GTC, TLS e MS-CHAP sono supportati come metodi EAP interni. Per EAP-FAST non sono supportati altri tipi di EAP.

Per ulteriori informazioni, fare riferimento a [Come funziona EAP-FAST](#).

PAC

Le PAC sono importanti segreti condivisi che consentono all'ISE e al client dell'utente finale EAP-FAST di autenticarsi a vicenda e stabilire un tunnel TLS da utilizzare nella seconda fase di EAP-FAST. L'ISE genera PAC utilizzando la chiave master attiva e un nome utente.

Il PAC comprende:

- **PAC-Key:** segreto condiviso associato a un'identità client (e di dispositivo client) e server.
- **PAC opaco:** campo opaco che il client memorizza nella cache e passa al server. Il server recupera la PAC-Key e l'identità del client per autenticarsi reciprocamente con il client.
- **PAC-Info:** include almeno l'identità del server per consentire al client di memorizzare nella cache PAC diverse. Facoltativamente, include altre informazioni quali l'ora di scadenza del PAC.

Modalità di provisioning PAC

Come accennato in precedenza, la fase zero è una fase facoltativa.

EAP-FAST offre due opzioni per il provisioning di un client con una PAC:

- **Preparazione automatica della PAC (fase 0 di EAP-FAST o preparazione della PAC in banda)**
- **Preparazione manuale della PAC (fuori banda)**

La **preparazione automatica della PAC in banda** invia una nuova PAC al client dell'utente finale tramite una connessione di rete protetta. La preparazione automatica delle credenziali di accesso protette non richiede l'intervento dell'utente di rete o di un amministratore ISE, a condizione che l'ISE e il client dell'utente finale siano configurati in modo da supportare la preparazione automatica.

L'ultima versione di EAP-FAST supporta due diverse opzioni di configurazione della preparazione della PAC in banda:

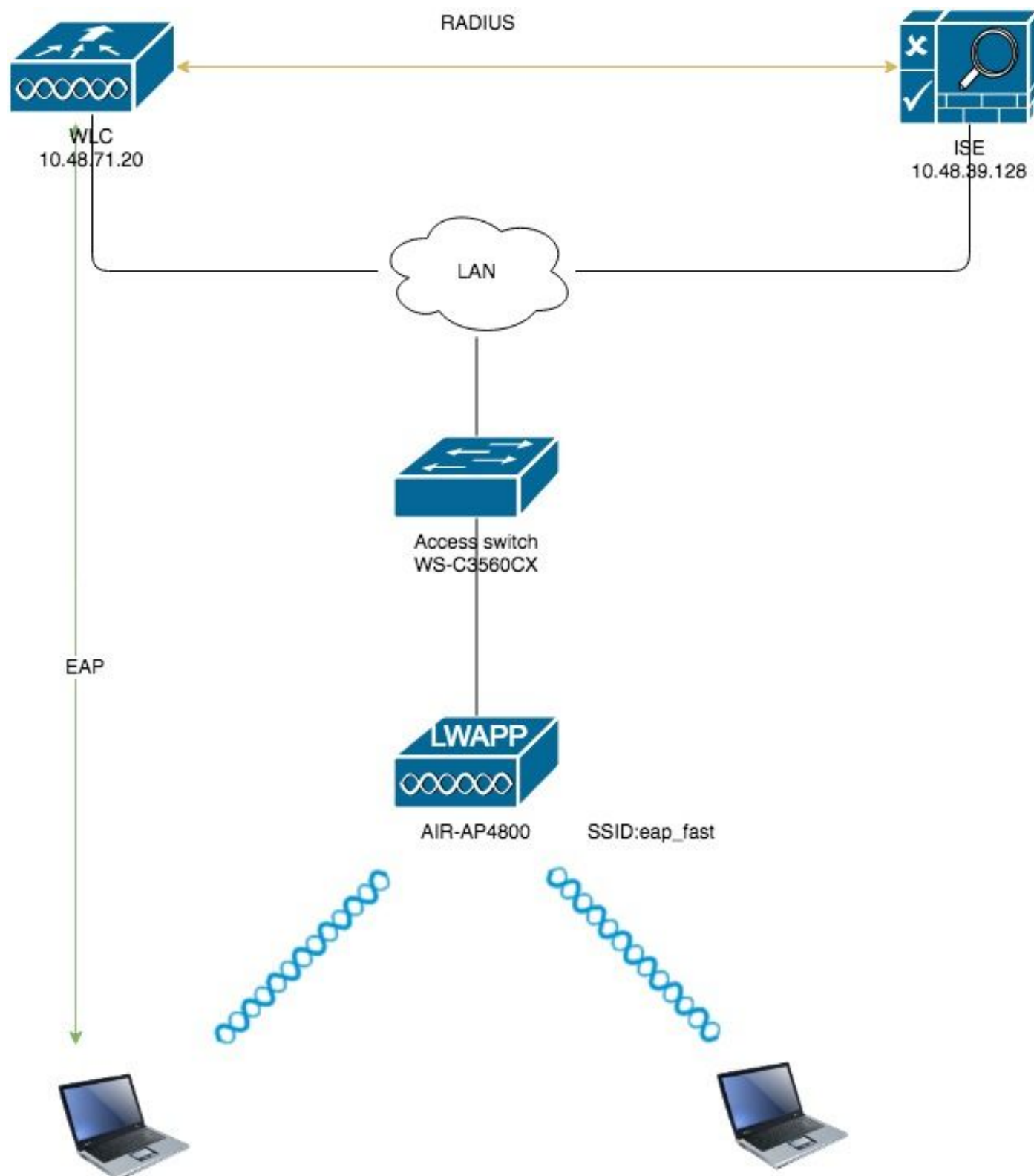
- **Preparazione PAC in banda anonima**
- **Provisioning PAC in banda autenticato**

Nota: in questo documento vengono descritti i metodi di preparazione della PAC in banda e la relativa configurazione.

La preparazione manuale/fuori banda della PAC richiede che un amministratore ISE generi i file PAC, che devono quindi essere distribuiti agli utenti della rete interessati. Gli utenti devono configurare i client degli utenti finali con i relativi file PAC.

Configurazione

Esempio di rete



Configurazioni

Configurazione del WLC per l'autenticazione EAP-FAST

Per configurare il WLC per l'autenticazione EAP-FAST, eseguire la procedura seguente:

1. Configurazione del WLC per l'autenticazione RADIUS tramite un server RADIUS esterno
2. Configurazione della WLAN per l'autenticazione EAP-FAST

Configurazione del WLC per l'autenticazione RADIUS tramite un server RADIUS esterno

È necessario configurare il WLC per inoltrare le credenziali dell'utente a un server RADIUS esterno. Il server RADIUS esterno convalida quindi le credenziali utente utilizzando EAP-FAST e fornisce l'accesso ai client wireless.

Per configurare il WLC per un server RADIUS esterno, completare la procedura seguente:

1. Scegliere **Sicurezza e Autenticazione RADIUS** dall'interfaccia utente del controller per visualizzare la pagina Server di autenticazione RADIUS. Quindi, fare clic su **New** (Nuovo) per definire un server RADIUS.
2. Definire i parametri del server RADIUS nella pagina **Server di autenticazione RADIUS > Nuovo**. Questi parametri includono: Indirizzo IP server RADIUS, Segreto condiviso, Numero porta, Stato server. Nel documento viene usato il server ISE con indirizzo IP 10.48.39.128.

The screenshot shows the Cisco WLC configuration interface for a new RADIUS Authentication Server. The interface is titled "RADIUS Authentication Servers > New". The configuration parameters are as follows:

Parameter	Value
Server Index (Priority)	2
Server IP Address (Ipv4/Ipv6)	10.48.39.128
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Apply Cisco ISE Default settings	<input checked="" type="checkbox"/>
Apply Cisco ACA Default settings	<input type="checkbox"/>
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for CoA	Enabled
Server Timeout	5 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	<input type="checkbox"/> Enable
PAC Provisioning	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable
Cisco ACA	<input type="checkbox"/> Enable

3. Clic **Applica**.

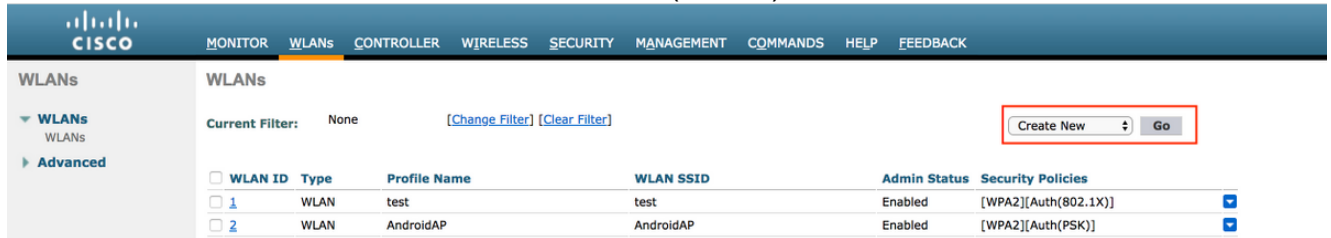
Configurazione della WLAN per l'autenticazione EAP-FAST

Configurare quindi la WLAN utilizzata dai client per connettersi alla rete wireless per l'autenticazione EAP-FAST e assegnarla a un'interfaccia dinamica. Il nome WLAN configurato in

questo esempio è **eap fast**. In questo esempio la WLAN viene assegnata all'interfaccia di gestione.

Completare questa procedura per configurare la WLAN **eap fast** e i relativi parametri:

1. Fare clic su **WLAN** dalla GUI del controller per visualizzare la pagina WLAN. In questa pagina vengono elencate le WLAN esistenti sul controller.
2. Per creare una nuova WLAN, fare clic su **New** (Nuovo).



3. Configurare il nome SSID della WLAN **eap_fast**, il nome del profilo e l'ID della WLAN nella pagina WLAN > Nuovo. Quindi fare clic su **Apply** (Applica).



4. Dopo aver creato una nuova WLAN, viene visualizzata la pagina **WLAN > Modifica** per la nuova WLAN. In questa pagina è possibile definire vari parametri specifici per la WLAN. Sono inclusi i criteri generali, i server RADIUS, i criteri di sicurezza e i parametri 802.1x.
5. Per abilitare la WLAN, selezionare la casella di controllo **Admin Status** (Stato amministratore) nella scheda **General Policies** (Criteri generali). Se si desidera che l'access point trasmetta il SSID nei frame del beacon, selezionare la casella di controllo **Broadcast SSID**.

WLANs > Edit 'eap_fast'

The screenshot shows the 'WLANs > Edit 'eap_fast'' configuration page. The top navigation bar is the same as the previous screenshots. The main content area has a 'WLANs > Edit 'eap_fast'' title and a '< Back' button. The configuration is organized into tabs: 'General', 'Security', 'QoS', 'Policy-Mapping', and 'Advanced'. The 'General' tab is selected. The configuration fields are: 'Profile Name' (eap_fast), 'Type' (WLAN), 'SSID' (eap_fast), 'Status' (Enabled, checked), 'Security Policies' ([WPA2][Auth(802.1X)]), 'Radio Policy' (All), 'Interface/Interface Group(G)' (vlan1477), 'Multicast Vlan Feature' (Enabled, unchecked), 'Broadcast SSID' (Enabled, checked), and 'NAS-ID' (none). Red boxes highlight the 'Status' checkbox and the 'Broadcast SSID' checkbox.

6. In "WLAN -> Modifica -> Sicurezza -> Layer 2" selezionare WPA/WPA2 parameters e selezionare dot1x per AKM.

In questo esempio viene usato WPA2/AES + dot1x come protezione di layer 2 per questa WLAN. Gli altri parametri possono essere modificati in base ai requisiti della rete WLAN.

The screenshot shows the configuration page for a WLAN named 'eap_fast'. The 'Security' tab is active, and the 'Layer 2' sub-tab is selected. The 'Layer 2 Security' dropdown is set to 'WPA+WPA2'. Below it, 'MAC Filtering' is disabled. The 'Fast Transition' is set to 'Disable'. The 'Protected Management Frame' (PMF) is set to 'Disabled'. Under 'WPA+WPA2 Parameters', 'WPA2 Policy' is checked, and 'WPA2 Encryption' is set to 'AES'. Other encryption options like TKIP, CCMP256, and GCMP128 are unchecked. Under 'Authentication Key Management', '802.1X' is checked and set to 'Enable', while 'CCKM', 'PSK', and 'FT 802.1X' are unchecked.

7. Nella scheda "WLAN -> Modifica -> Protezione -> Server AAA" scegliere il server RADIUS appropriato dal menu a discesa in Server RADIUS.

WLANs > Edit 'eap_fast'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

RADIUS Server Overwrite interface Enabled
 Apply Cisco ISE Default Settings Enabled

	Authentication Servers	Accounting Servers	EAP Paramet
Server 1	<input checked="" type="checkbox"/> Enabled IP:10.48.39.128, Port:1812	<input checked="" type="checkbox"/> Enabled None	Enable
Server 2	None	None	
Server 3	None	None	
Server 4	None	None	
Server 5	None	None	
Server 6	None	None	

Authorization ACA Server Enabled
 Server None

Accounting ACA Server Enabled
 Server None

8. Fare clic su **Apply** (Applica). **Nota:** questa è l'unica impostazione EAP da configurare sul controller per l'autenticazione EAP. Tutte le altre configurazioni specifiche di EAP-FAST devono essere eseguite sul server RADIUS e sui client da autenticare.

Configurazione del server RADIUS per l'autenticazione EAP-FAST

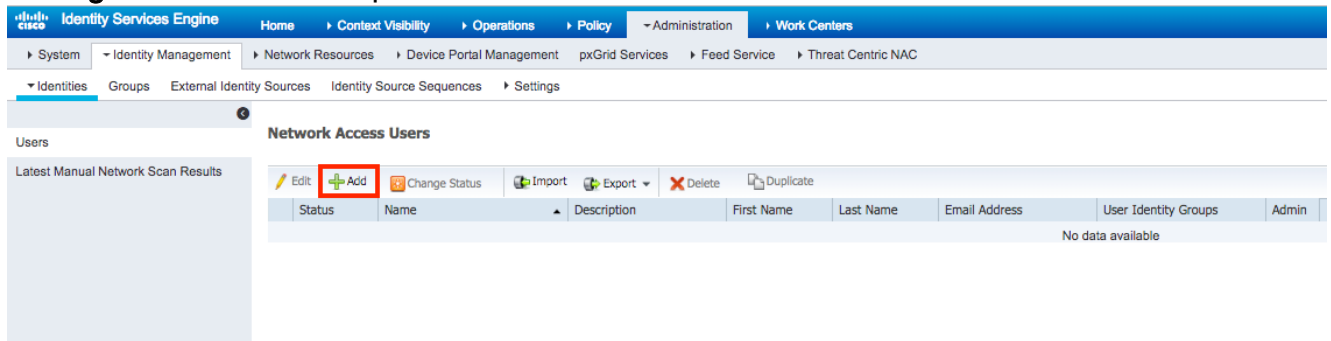
Per configurare il server RADIUS per l'autenticazione EAP-FAST, attenersi alla procedura seguente:

1. Creazione di un database utenti per autenticare i client EAP-FAST
2. Aggiungere il WLC come client AAA al server RADIUS
3. Configurazione dell'autenticazione EAP-FAST sul server RADIUS con provisioning PAC in banda anonimo
4. Configurazione dell'autenticazione EAP-FAST sul server RADIUS con provisioning della PAC in-band autenticato

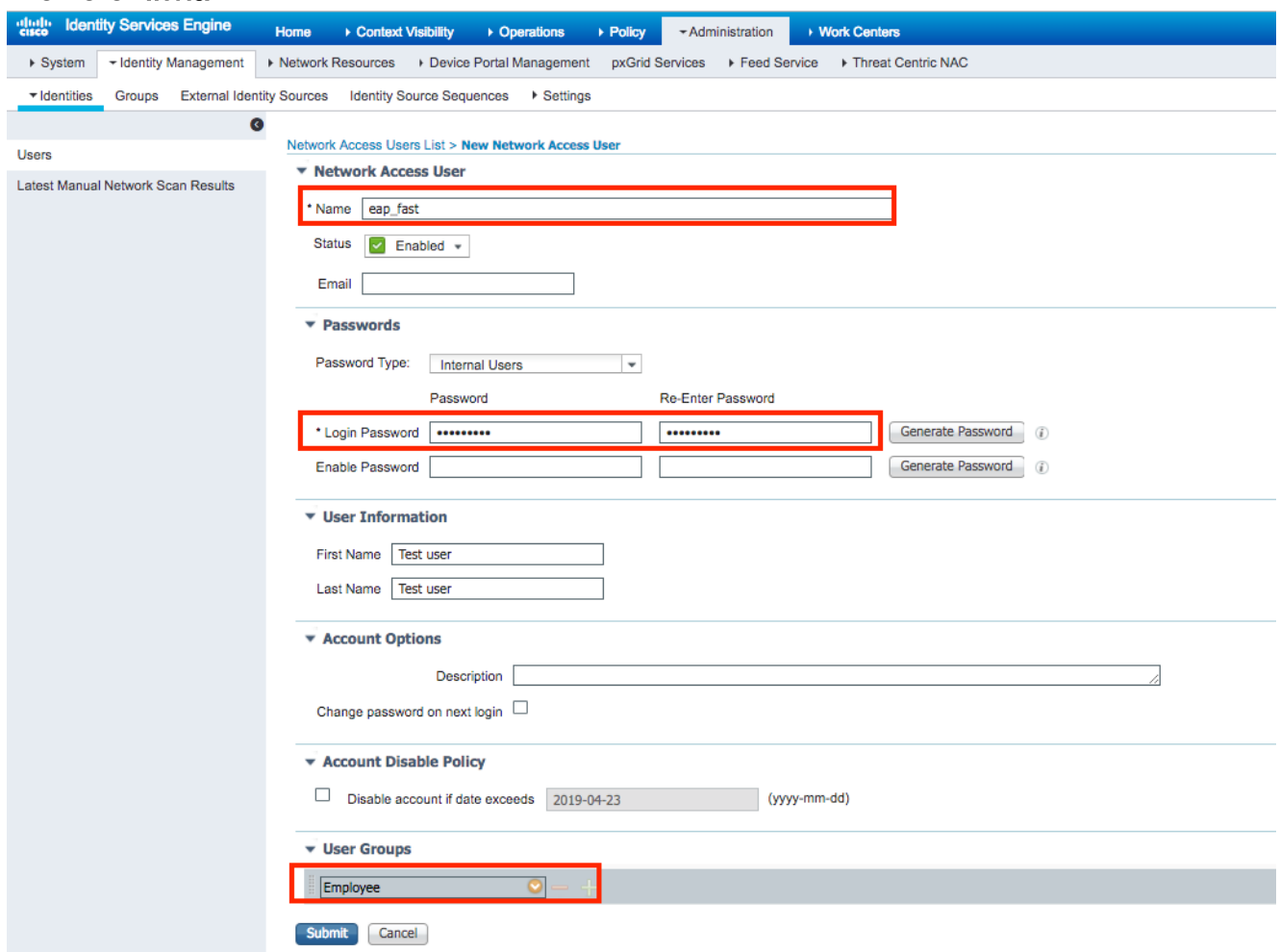
Creazione di un database utenti per autenticare i client EAP-FAST

Nell'esempio, il nome utente e la password del client EAP-FAST sono configurati rispettivamente come `<eap_fast>` e `<EAP-fast1>`.

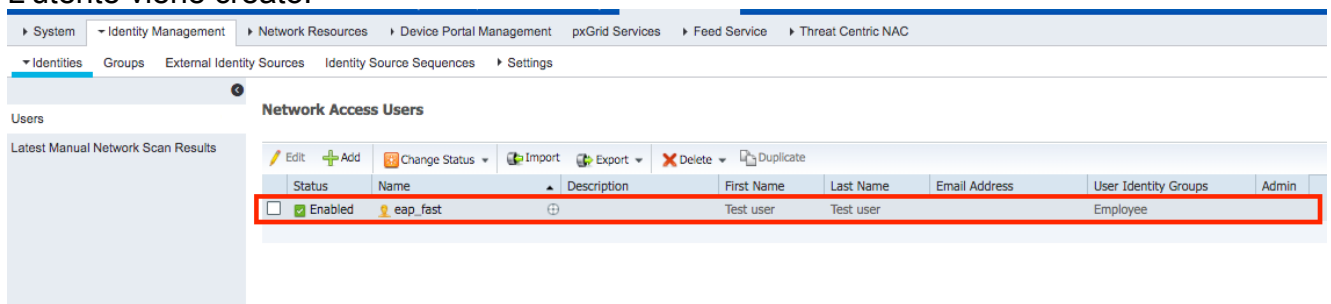
1. Nell'interfaccia utente di ISE Web admin, selezionare **"Administration -> Identity Management -> Users"** e premere l'icona **"Add"**.



2. Compilare i moduli obbligatori per la creazione dell'utente - **"Nome"** e **"Password di accesso"** e selezionare **"Gruppo utenti"** dall'elenco a discesa; [facoltativamente è possibile compilare altre informazioni per l'account utente]
Premere **"Invia"**



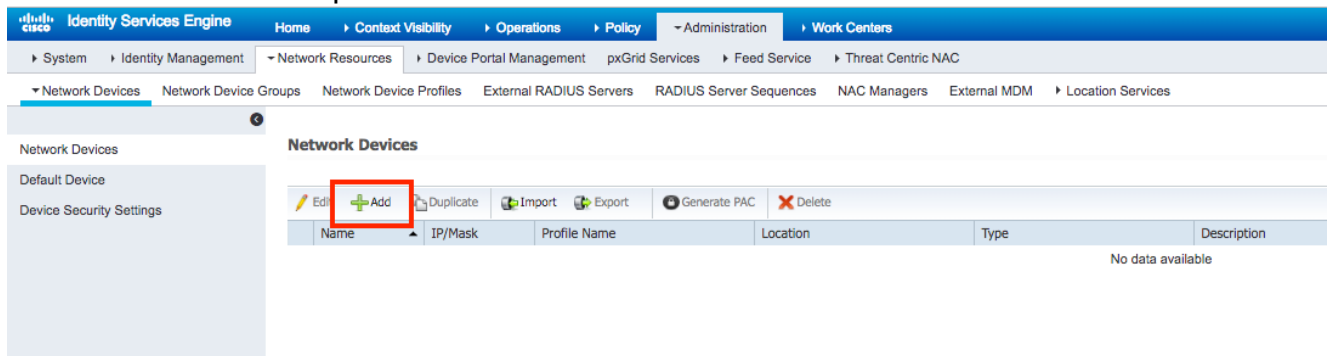
3. L'utente viene creato.



Aggiungere il WLC come client AAA al server RADIUS

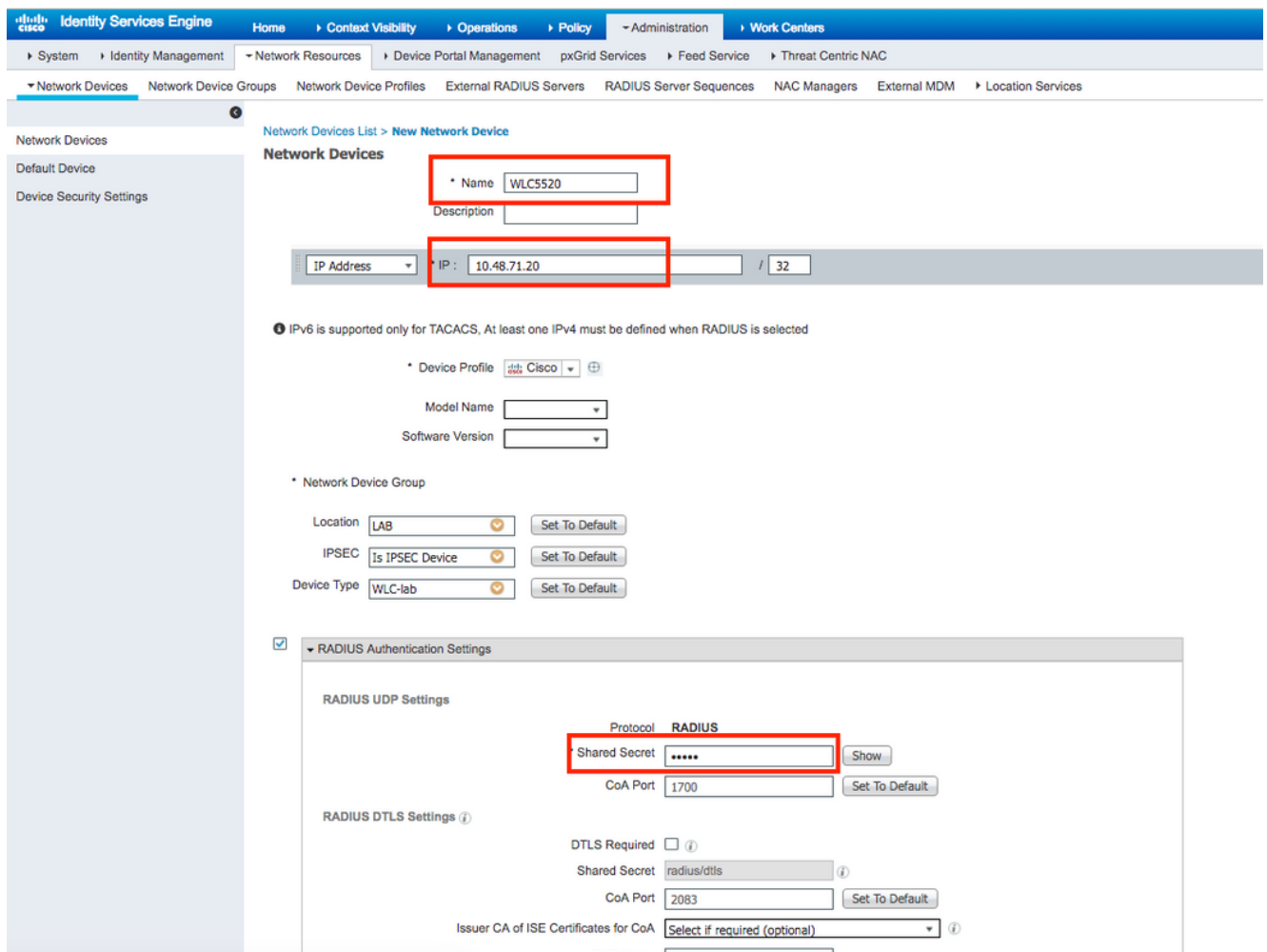
Completare questa procedura per definire il controller come client AAA sul server ACS:

1. Nell'interfaccia utente di ISE Web admin, selezionare **"Administration -> Network Resources -> Network Devices"** e premere l'icona **"Add"**.

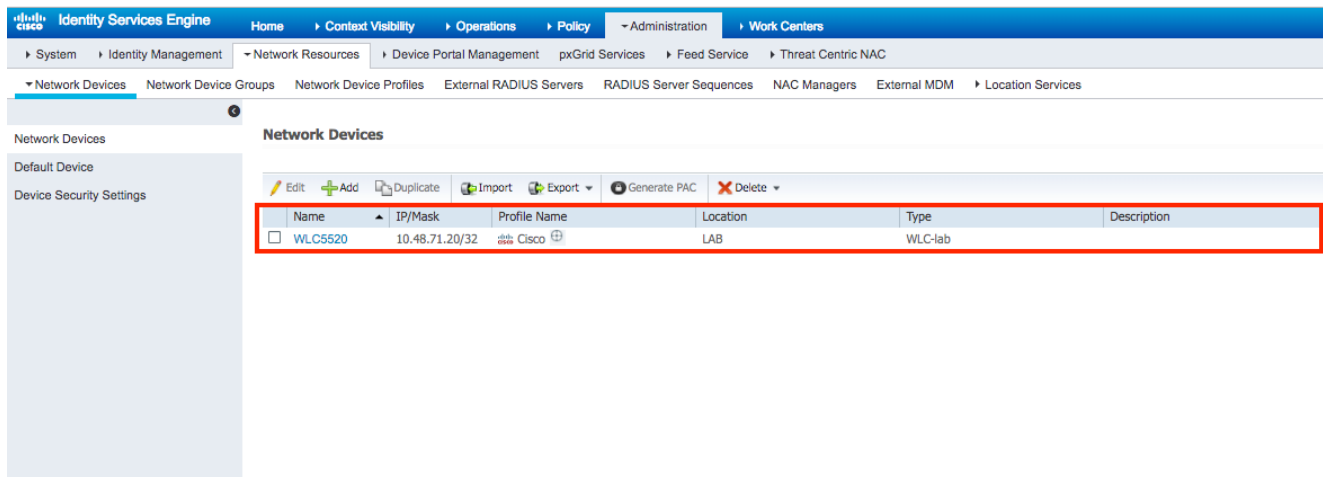


2. Compilare i moduli richiesti per il dispositivo da aggiungere - **"Nome"**, **"IP"** e configurare la stessa password segreta condivisa, come configurato sul WLC nella sezione precedente, nel modulo **"Segreto condiviso"** [facoltativamente è possibile compilare altre informazioni per il dispositivo come posizione, gruppo, ecc.].

Premere **"Invia"**



3. La periferica viene aggiunta all'elenco delle periferiche di accesso alla rete ISE. (AND)

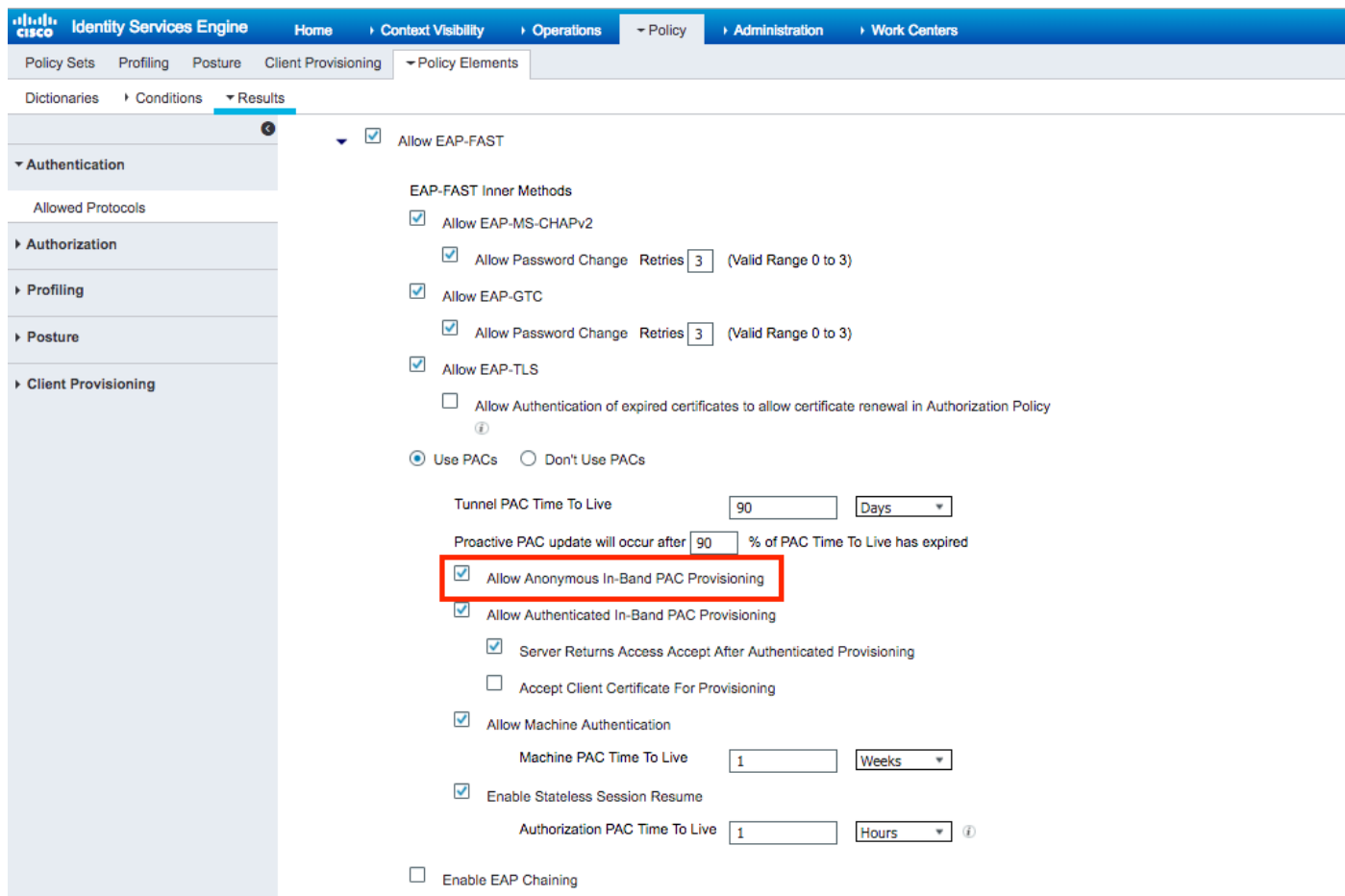


Configurazione dell'autenticazione EAP-FAST sul server RADIUS con provisioning PAC in banda anonimo

In genere si preferisce utilizzare questo tipo di metodo nel caso in cui non sia disponibile un'infrastruttura PKI nella distribuzione.

Questo metodo funziona all'interno di un tunnel ADHP (Authenticated Diffie-Hellman Key Agreement Protocol) prima che il peer autentichi il server ISE.

Per supportare questo metodo, è necessario abilitare **"Allow Anonymous In-band PAC Provisioning"** (Consenti provisioning PAC in-band anonimo) su ISE in **"Authentication Allowed Protocols"** (Protocolli autorizzati per l'autenticazione):



Nota: accertarsi di aver consentito l'autenticazione del tipo di password, come EAP-MS-CHAPv2

per il metodo interno EAP-FAST, poiché ovviamente con il provisioning in banda anonimo non è possibile utilizzare alcun certificato.

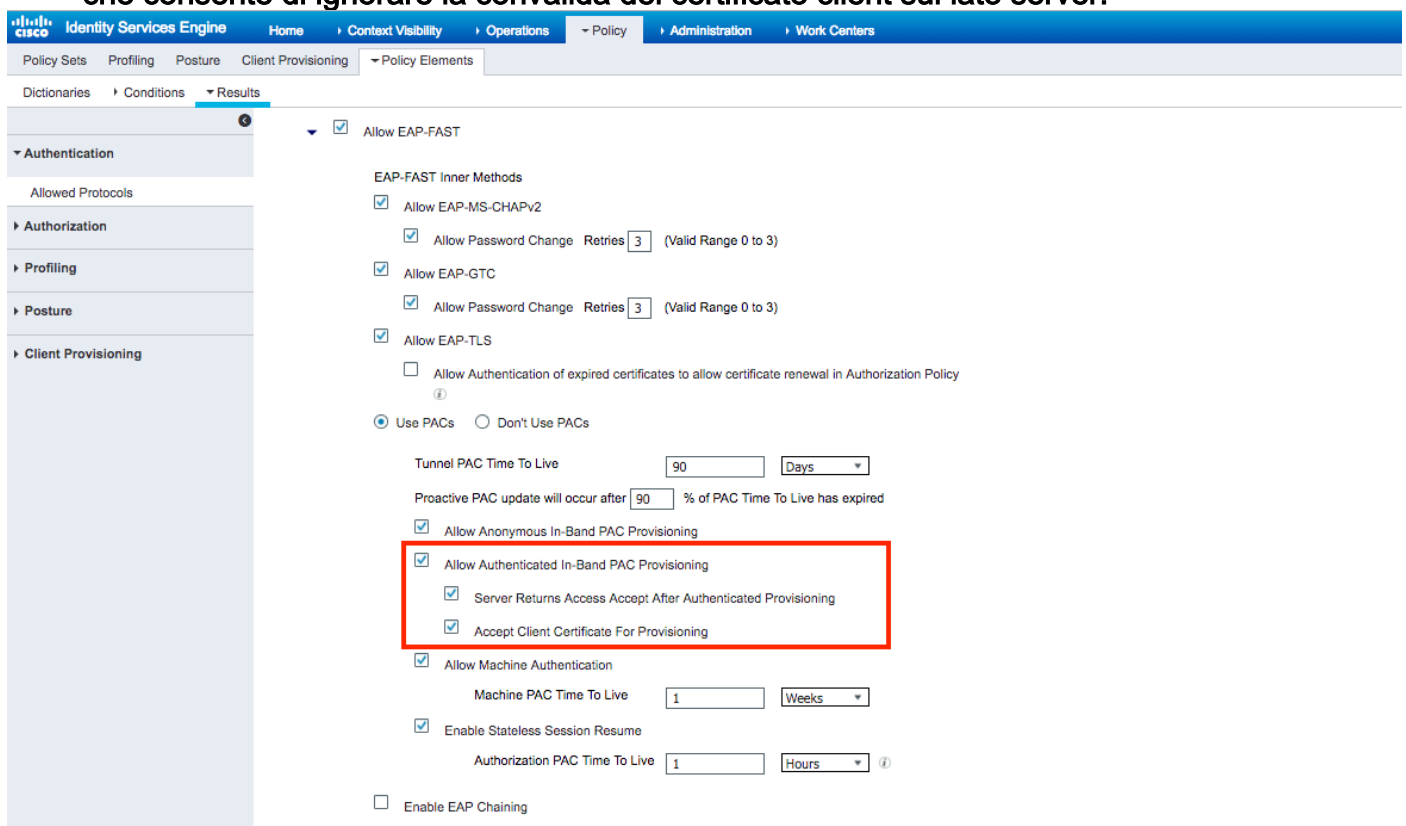
Configurazione dell'autenticazione EAP-FAST sul server RADIUS con provisioning della PAC in-band autenticato

Si tratta dell'opzione più sicura e consigliata. Il tunnel TLS viene creato in base al certificato del server convalidato dal richiedente e il certificato del client viene convalidato da ISE (impostazione predefinita).

Questa opzione richiede un'infrastruttura PKI per client e server, anche se può essere limitata al solo lato server o ignorata su entrambi i lati.

ISE offre due opzioni aggiuntive per il provisioning in-band autenticato:

1. **"Server Returns Access Accept After Authenticated Provisioning"** - In genere, dopo la preparazione della PAC, è necessario inviare un messaggio di rifiuto dell'accesso che impone al richiedente di rieseguire l'autenticazione utilizzando le PAC. Tuttavia, poiché la preparazione della PAC viene eseguita in un tunnel TLS autenticato, è possibile rispondere immediatamente con Access-Accept per ridurre al minimo i tempi di autenticazione. In questo caso, verificare di disporre di certificati attendibili sul lato client e server.
2. **"Accetta certificato client per provisioning"** - se non si desidera fornire l'infrastruttura PKI ai dispositivi client e si dispone solo di un certificato attendibile su ISE, abilitare questa opzione, che consente di ignorare la convalida del certificato client sul lato server.



The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The navigation pane on the left includes sections for Authentication, Authorization, Profiling, Posture, and Client Provisioning. The main content area is titled 'Policy Elements' and shows the configuration for 'Allow EAP-FAST'. Under the 'EAP-FAST Inner Methods' section, several options are checked, including 'Allow EAP-MS-CHAPv2', 'Allow EAP-GTC', and 'Allow EAP-TLS'. The 'Use PACs' radio button is selected. Below this, the 'Tunnel PAC Time To Live' is set to 90 days, and the 'Proactive PAC update' is set to occur after 90% of the PAC Time To Live has expired. A red box highlights three specific options under 'Allow Anonymous In-Band PAC Provisioning': 'Allow Authenticated In-Band PAC Provisioning', 'Server Returns Access Accept After Authenticated Provisioning', and 'Accept Client Certificate For Provisioning', all of which are checked. Other options like 'Allow Machine Authentication' and 'Enable Stateless Session Resume' are also visible.

Su ISE definiamo anche criteri di autenticazione semplici impostati per gli utenti wireless, qui di seguito esempio sta utilizzando come parametro di condizione tipo di dispositivo e posizione e tipo di autenticazione, il flusso di autenticazione corrispondente a quella condizione sarà convalidato rispetto al database degli utenti interni.



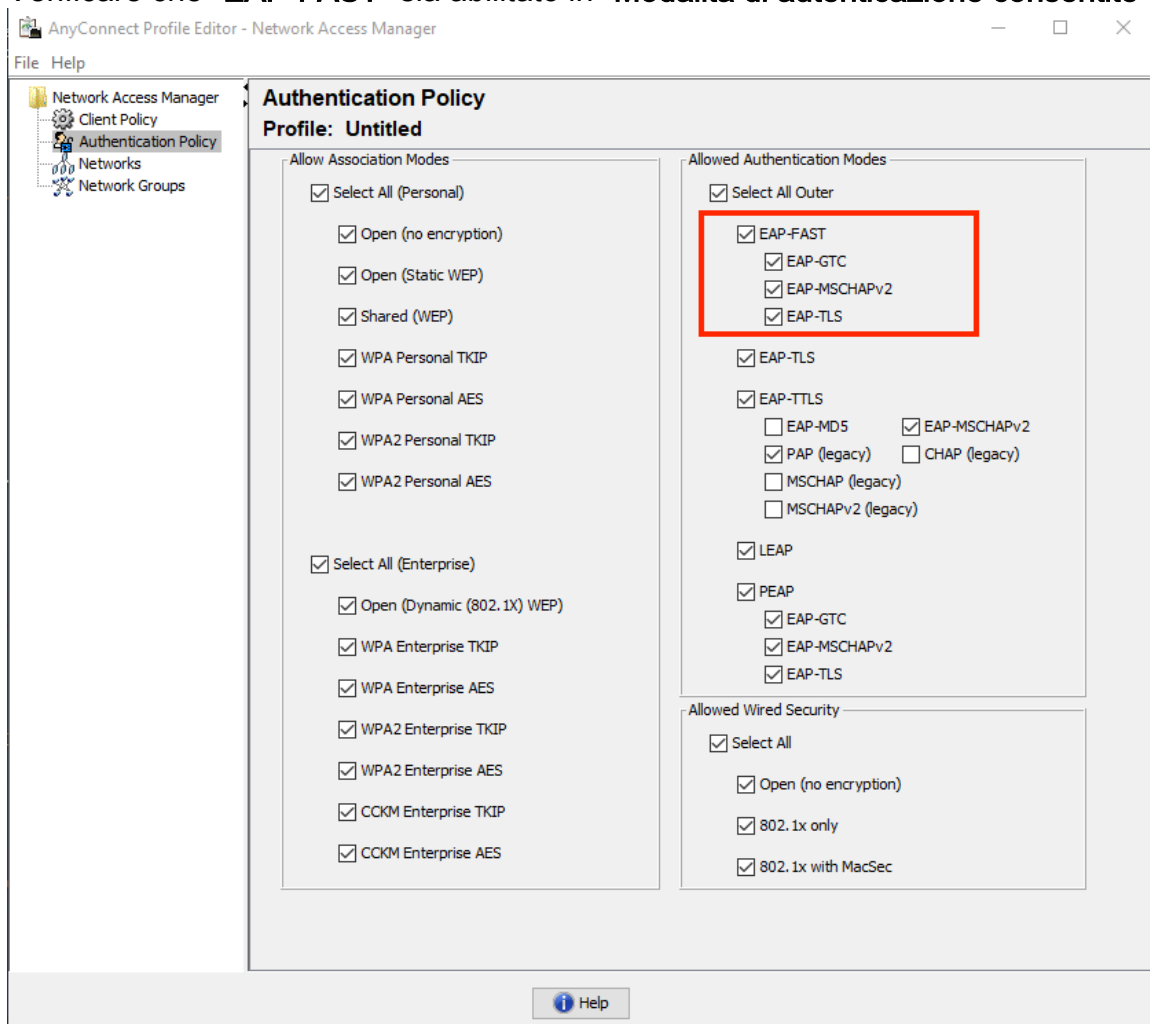
Verifica

In questo esempio vengono mostrati il flusso di provisioning della PAC in banda autenticata e le impostazioni di configurazione di Network Access Manager (NAM) insieme ai rispettivi debug WLC.

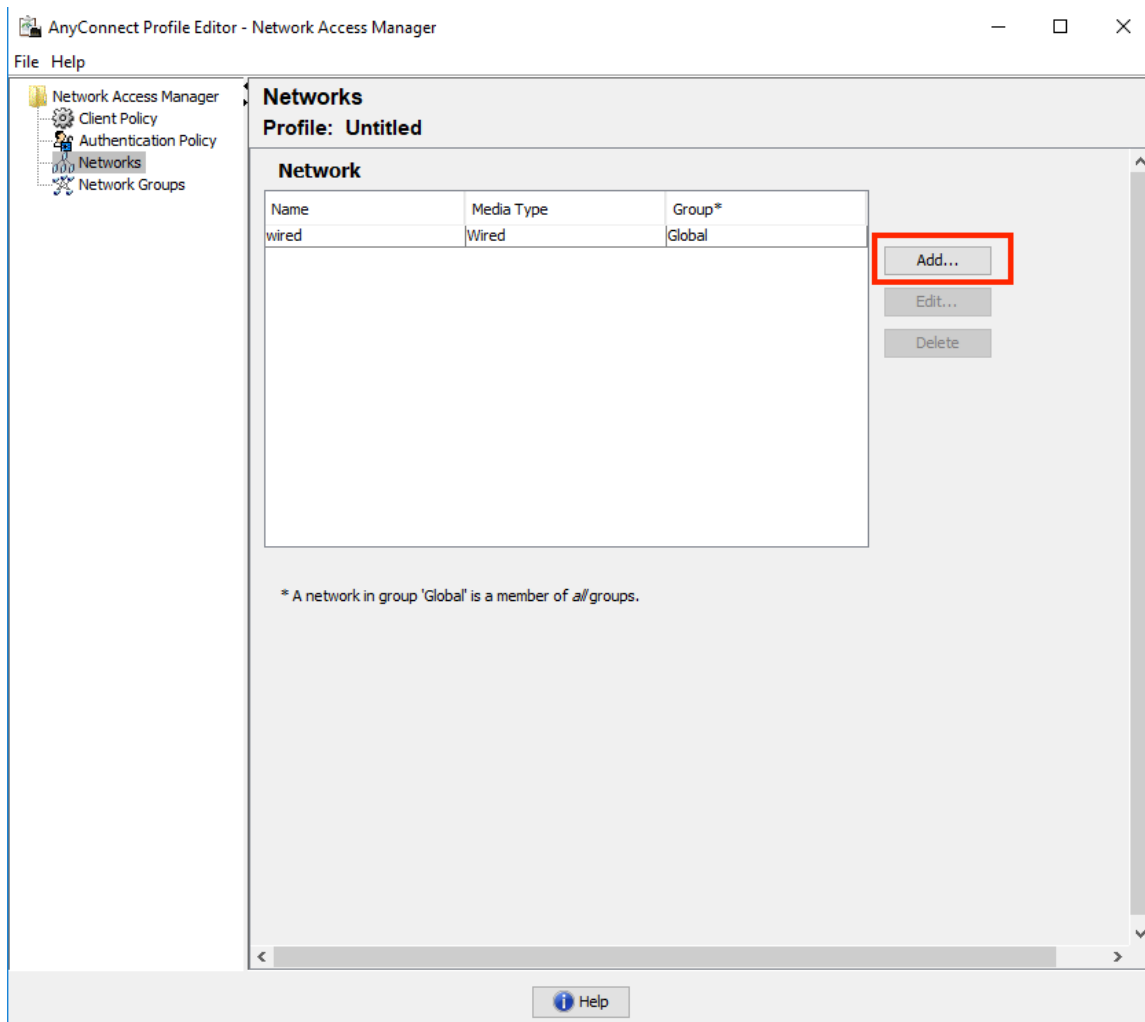
Configurazione profilo NAM

Per configurare il profilo Anyconnect NAM in modo che autentichi la sessione utente con ISE usando EAP-FAST, è necessario eseguire le seguenti operazioni:

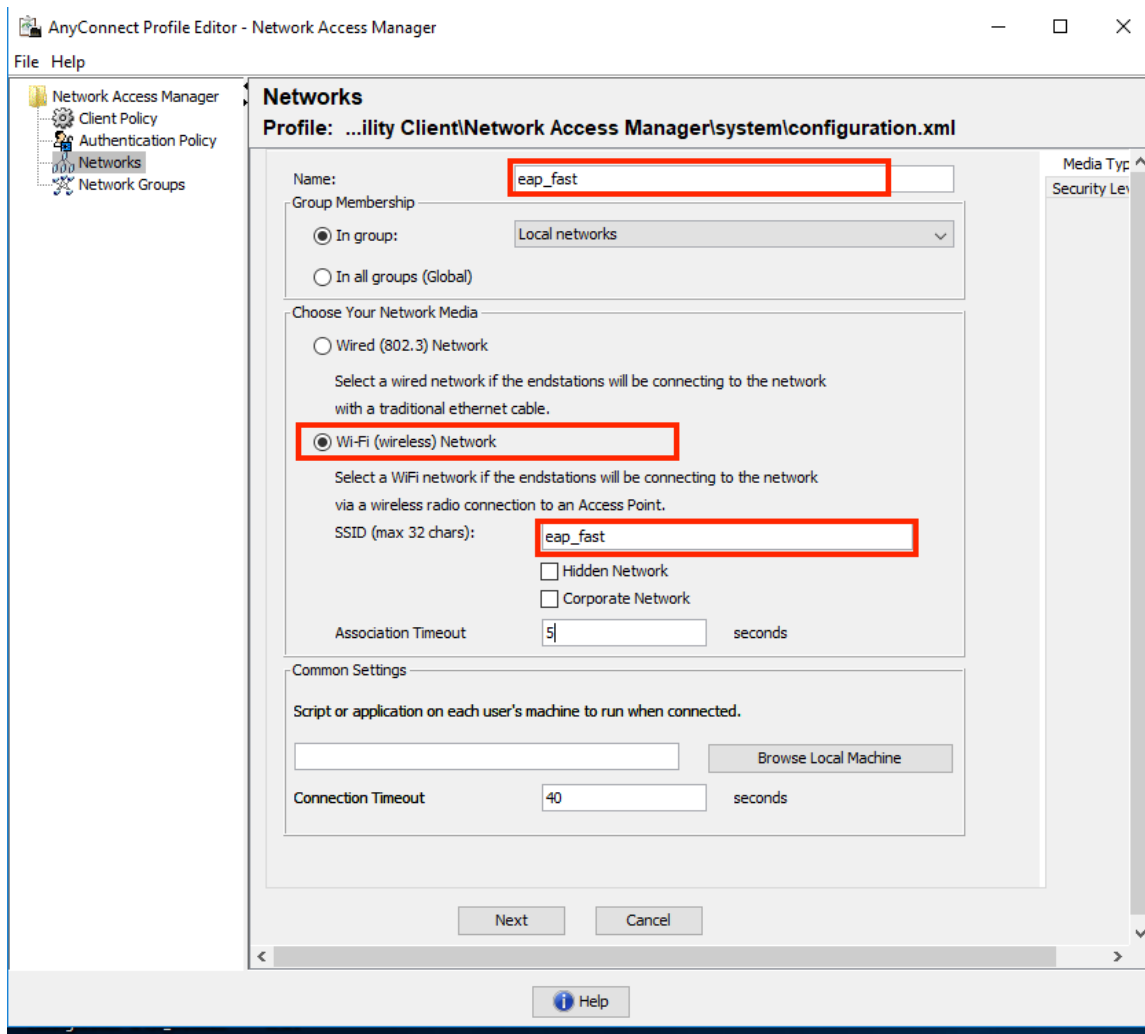
1. Aprire l'Editor profili di Network Access Manager e caricare il file di configurazione corrente.
2. Verificare che "EAP-FAST" sia abilitato in "Modalità di autenticazione consentite"



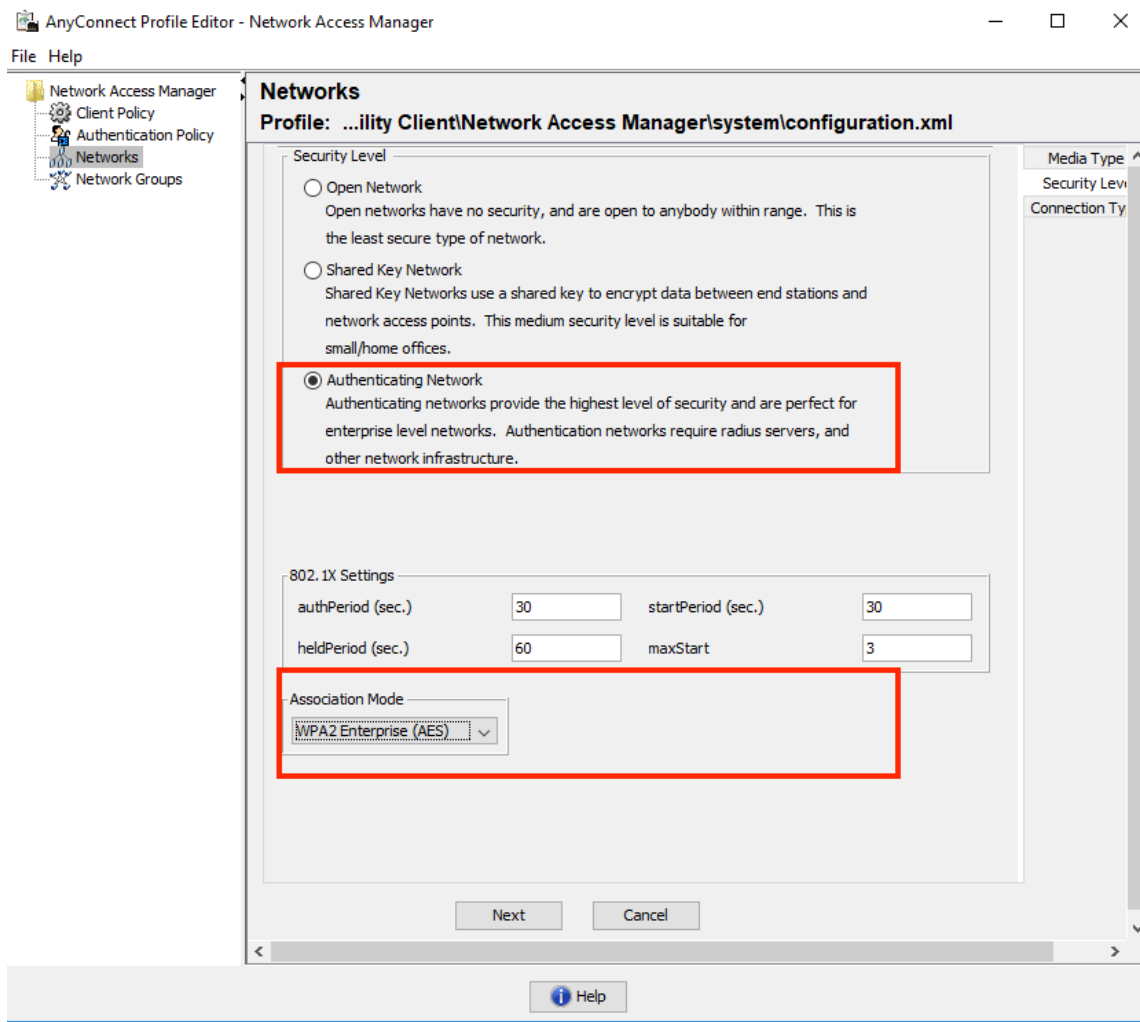
3. "Aggiungi" un nuovo profilo di rete:



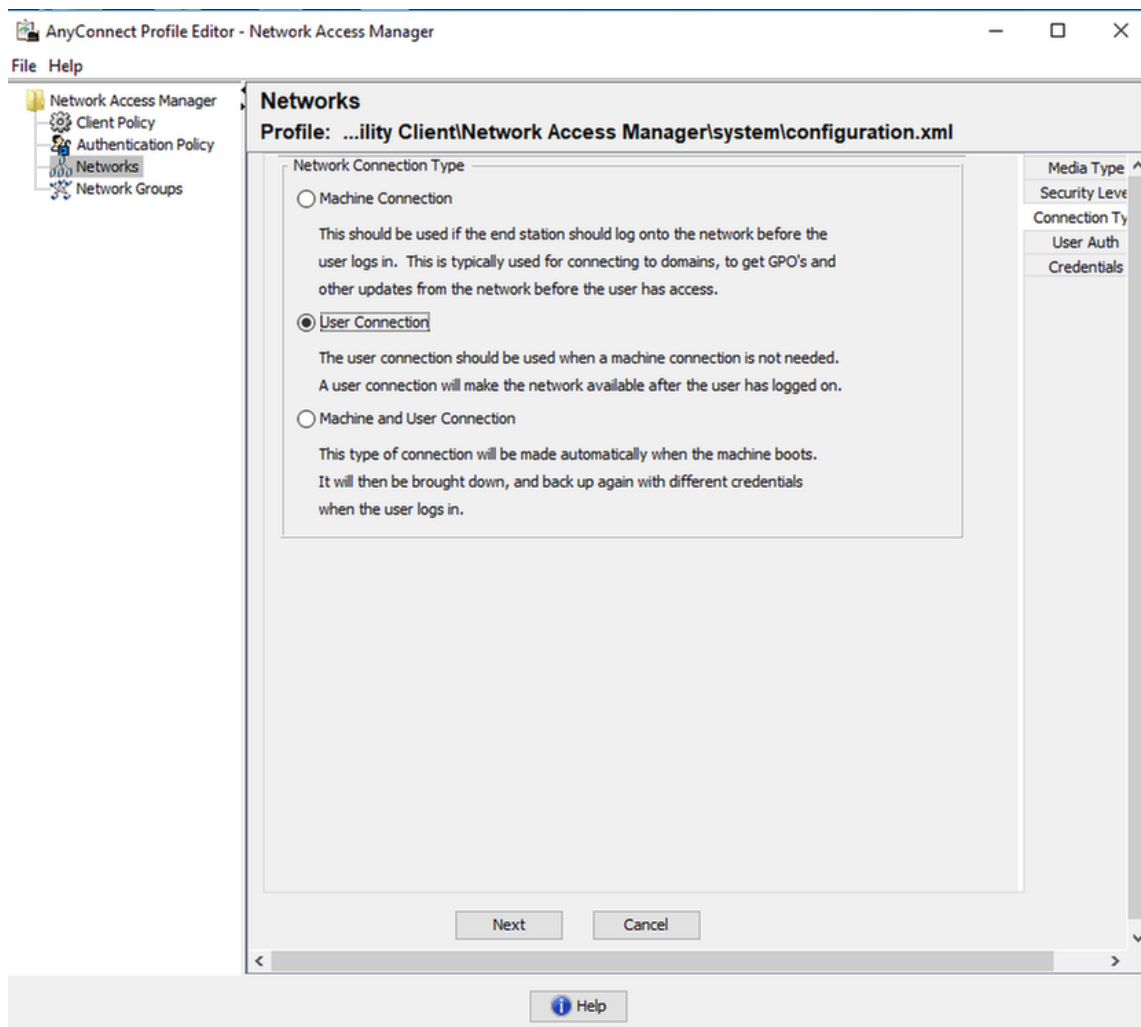
4. Nella sezione di configurazione "**Tipo di supporto**" definire il profilo "**Nome**", wireless come tipo di rete multimediale e specificare il nome SSID.



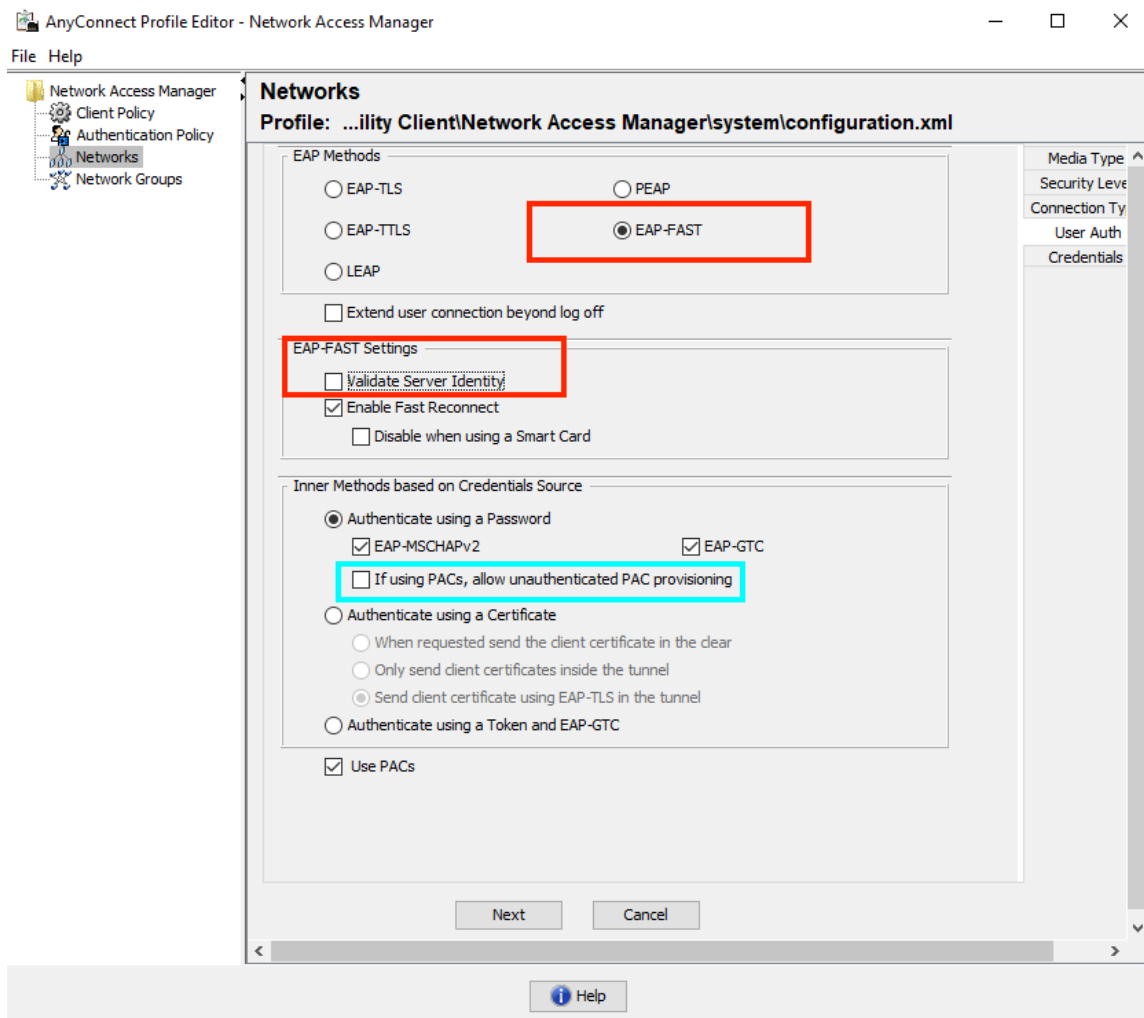
5. Nella scheda di configurazione "**Livello di protezione**" selezionare "Autenticazione rete" e specificare la modalità di associazione come WPA2 Enterprise (AES)



6. In questo esempio viene utilizzata l'autenticazione basata sul tipo di utente, quindi nella scheda successiva "Tipo di connessione" selezionare "Connessione utente"



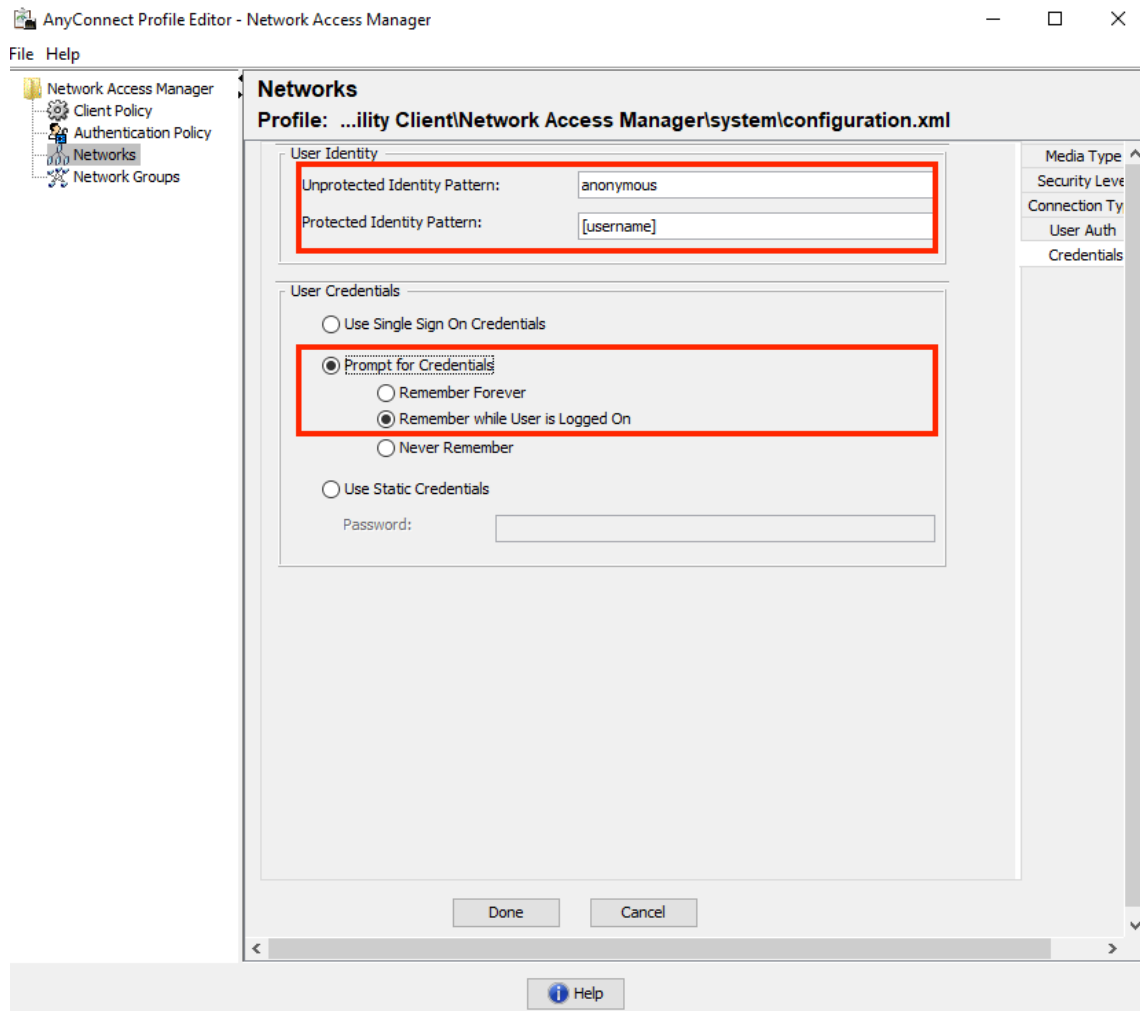
7. Nella scheda "**Autenticazione utente**" specificare EAP-FAST come metodo di autenticazione consentito e disattivare la convalida dei certificati del server, poiché in questo esempio non vengono utilizzati certificati protetti.



Nota: in un ambiente di produzione reale assicurarsi di avere un certificato attendibile installato su ISE e mantenere l'opzione di convalida del certificato server abilitata nelle impostazioni NAM.

Nota: L'opzione "Se si utilizzano PAC, consenti preparazione PAC non autenticata" deve essere selezionata solo in caso di preparazione PAC in banda anonima.

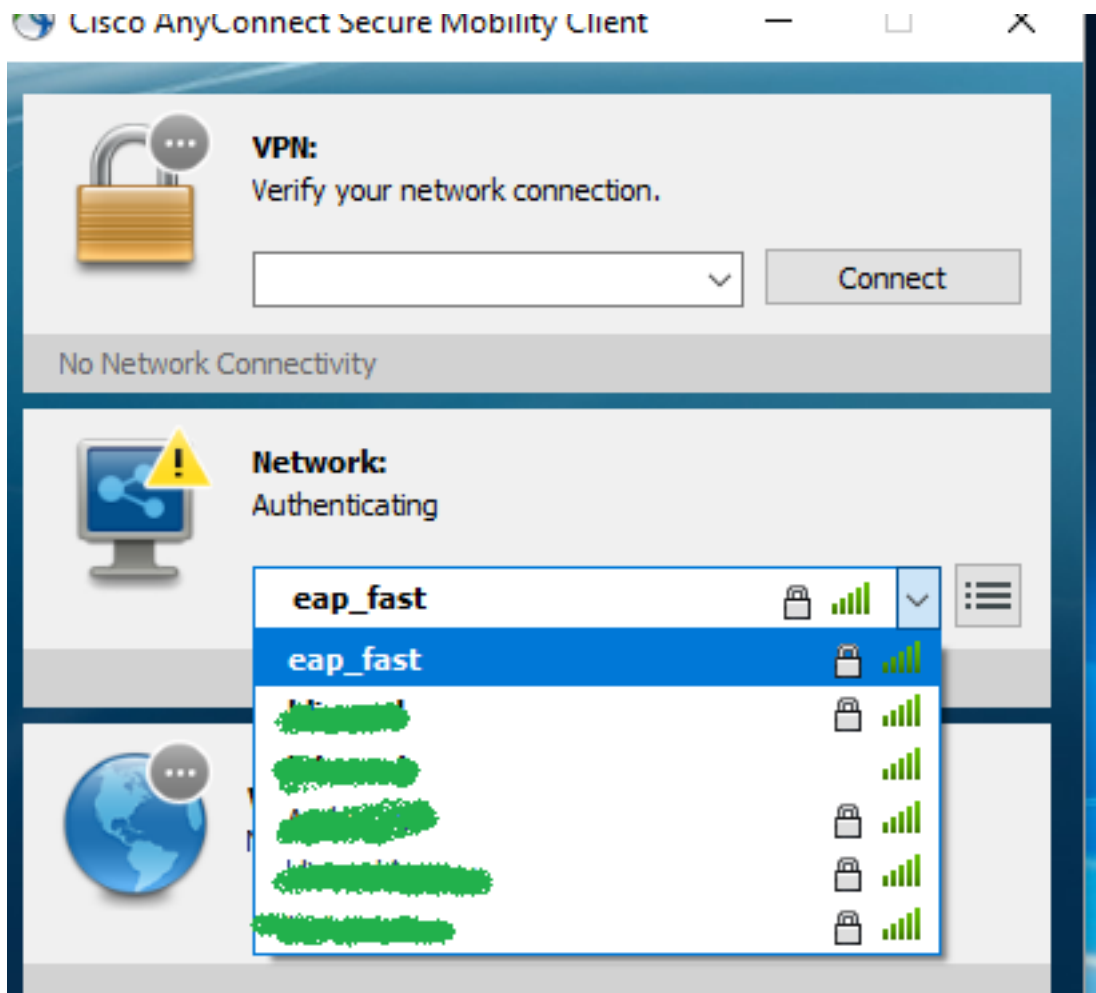
8. Definire le credenziali utente come SSO se si desidera utilizzare le stesse credenziali utilizzate per l'accesso, selezionare "Richiedi credenziali" se si desidera che all'utente vengano richieste le credenziali durante la connessione alla rete oppure definire credenziali statiche per il tipo di accesso. In questo esempio vengono richieste le credenziali dell'utente al tentativo di connessione alla rete.



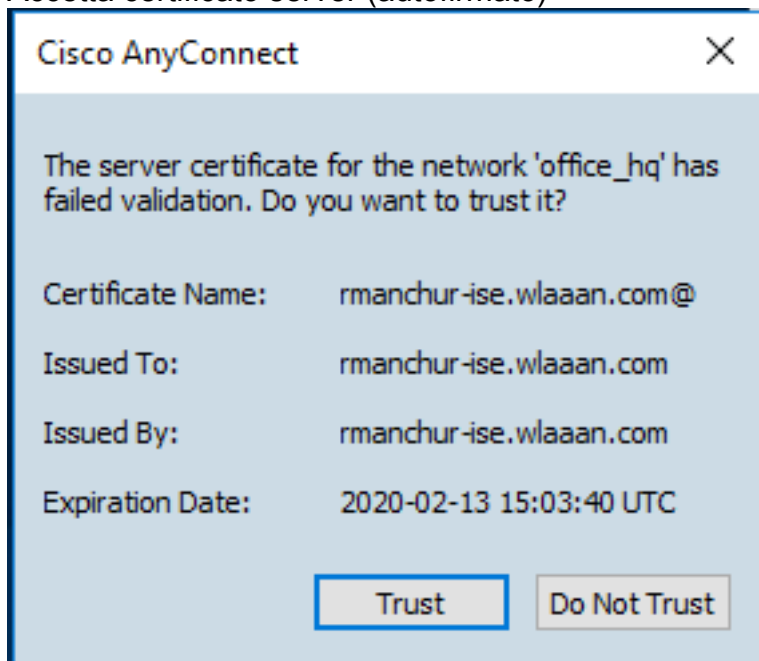
9. Salvare il profilo configurato nella cartella NAM corrispondente.

Verificare la connettività a SSID utilizzando l'autenticazione EAP-FAST.

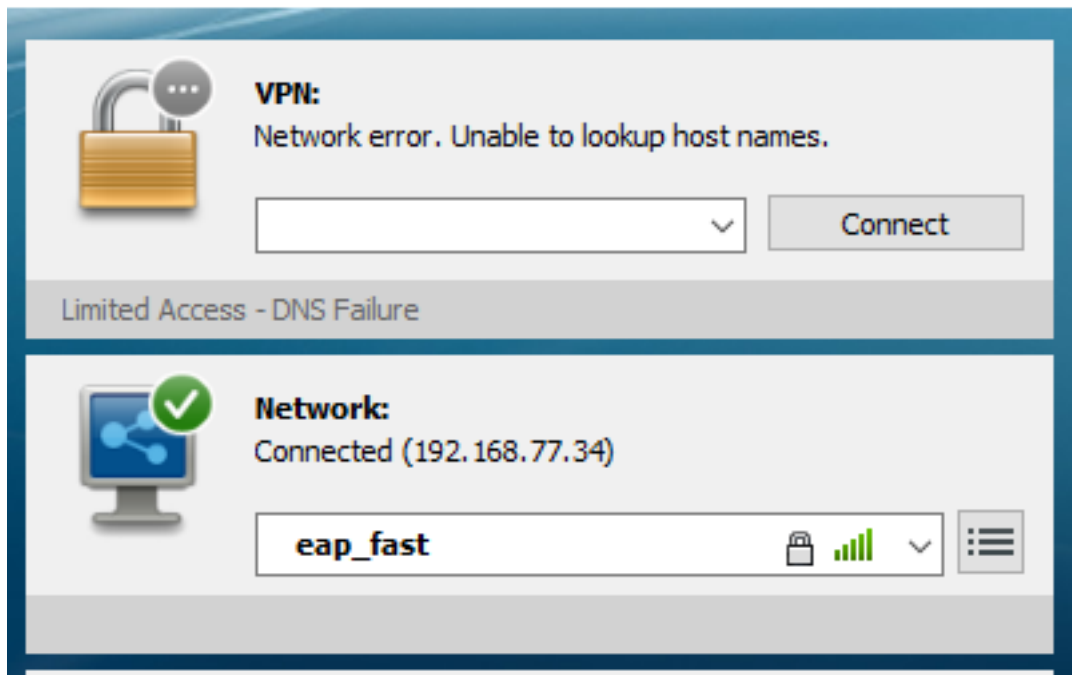
1. Seleziona il profilo corrispondente dall'elenco delle reti Anyconnect



2. Immettere il nome utente e la password necessari per l'autenticazione
3. Accetta certificato server (autofirmato)



4. Fine



Log di autenticazione ISE

I log di autenticazione ISE che mostrano il flusso di provisioning EAP-FAST e PAC possono essere visualizzati in "Operations -> RADIUS -> Live Logs" (Operazioni -> RAGGIO -> Live Logs) e consultati in maggior dettaglio usando l'icona "Zoom" (Zoom):

1. Il client ha avviato l'autenticazione e ISE ha proposto EAP-TLS come metodo di autenticazione, ma il client ha rifiutato e ha proposto EAP-FAST; questo è stato il metodo accettato sia dal client che da ISE.

Steps

11001 Received RADIUS Access-Request
11017 RADIUS created a new session
15049 Evaluating Policy Group
15008 Evaluating Service Selection Policy
11507 Extracted EAP-Response/Identity
12500 Prepared EAP-Request proposing EAP-TLS with challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12101 Extracted EAP-Response/NAK requesting to use EAP-FAST instead
12100 Prepared EAP-Request proposing EAP-FAST with challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12102 Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated

2. L'handshake TLS è stato avviato tra il client e il server per fornire l'ambiente protetto per lo scambio PAC ed è stato completato.

12800 Extracted first TLS record; TLS handshake started

12805 Extracted TLS ClientHello message

12806 Prepared TLS ServerHello message

12807 Prepared TLS Certificate message

12808 Prepared TLS ServerKeyExchange message

12810 Prepared TLS ServerDone message

12811 Extracted TLS Certificate message containing client certificate

12105 Prepared EAP-Request with another EAP-FAST challenge

11006 Returned RADIUS Access-Challenge

11001 Received RADIUS Access-Request

11018 RADIUS is re-using an existing session

12104 Extracted EAP-Response containing EAP-FAST challenge-response

12105 Prepared EAP-Request with another EAP-FAST challenge

11006 Returned RADIUS Access-Challenge

11001 Received RADIUS Access-Request (🕒 Step latency=13317 ms)

11018 RADIUS is re-using an existing session

12104 Extracted EAP-Response containing EAP-FAST challenge-response

12812 Extracted TLS ClientKeyExchange message

12813 Extracted TLS CertificateVerify message

12804 Extracted TLS Finished message

12801 Prepared TLS ChangeCipherSpec message

~~12802 Prepared TLS Finished message~~

12816 TLS handshake succeeded

3. Autenticazione interna avviata e credenziali utente convalidate da ISE con MS-CHAPv2 (autenticazione basata su nome utente/password)

