Configurazione dell'autenticazione computer e utente con EAP-TTLS

Sommario

Introduzione

In questo documento viene descritto come configurare l'autenticazione computer e utente con EAP-TTLS (EAP-MSCHAPv2) su Secure Client NAM e Cisco ISE.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti prima di procedere con questa distribuzione:

- Cisco Identity Services Engine (ISE)
- NAM (Secure Client Network Analysis Module)
- Protocolli EAP

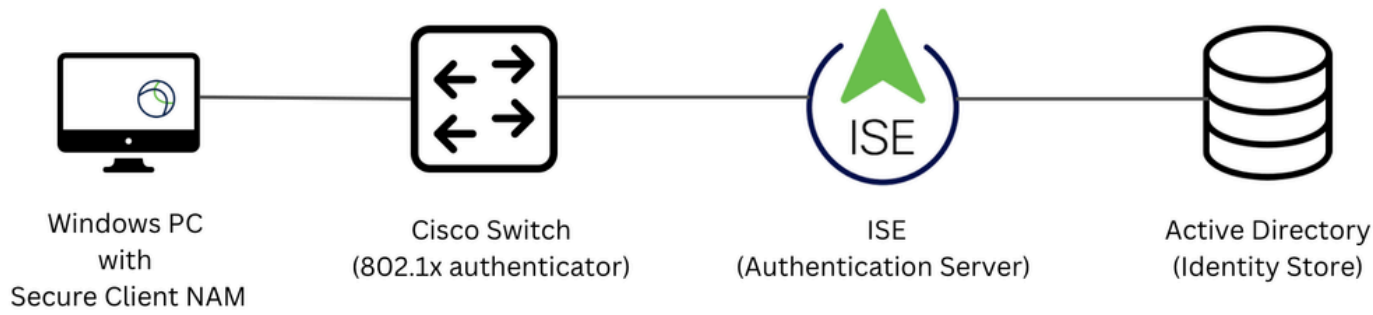
Componenti usati

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

- Identity Services Engine (ISE) versione 3.4
- Switch C9300 con software Cisco IOS® XE, versione 16.12.01
- Windows 10 Pro versione 22H2 19045.3930

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.

Topologia della rete



Topologia della rete

Configurazione

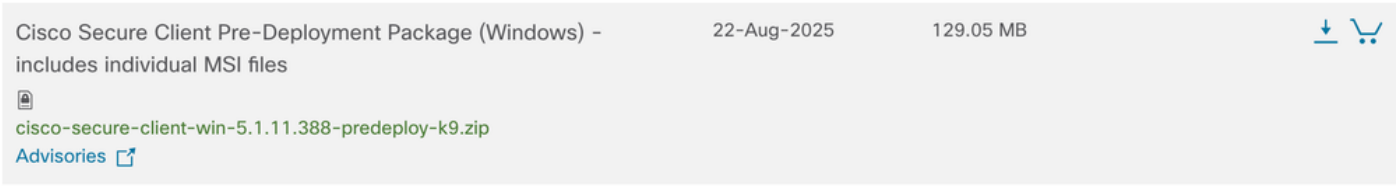
Configurazioni

Parte 1: Scaricare e installare Secure Client NAM (Network Access Manager)

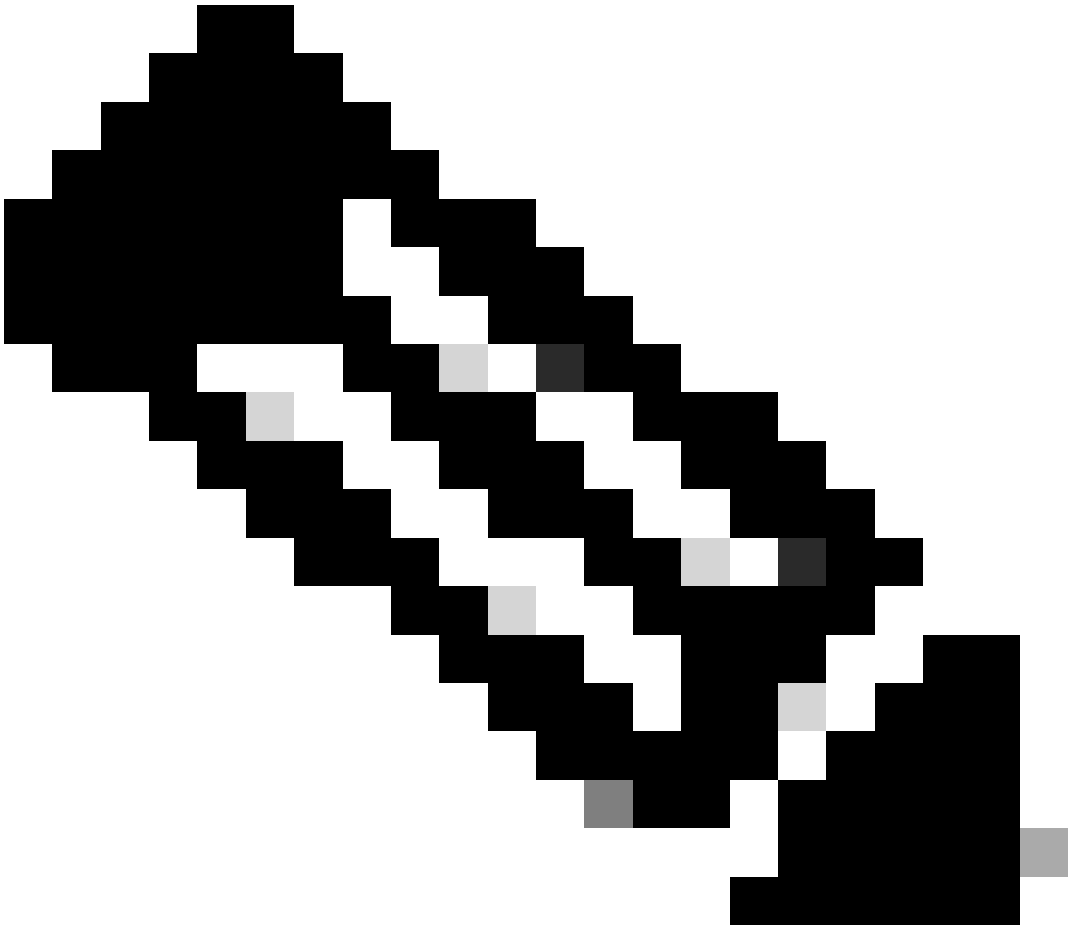
Passaggio 1. Andare a Cisco Software Download. Nella barra di ricerca del prodotto, immettere Secure Client 5.

In questo esempio di configurazione viene utilizzata la versione 5.1.11.388. L'installazione viene eseguita utilizzando il metodo pre-distribuzione.

Nella pagina di download, individuare e scaricare Cisco Secure Client Pre-Deployment Package (Windows).

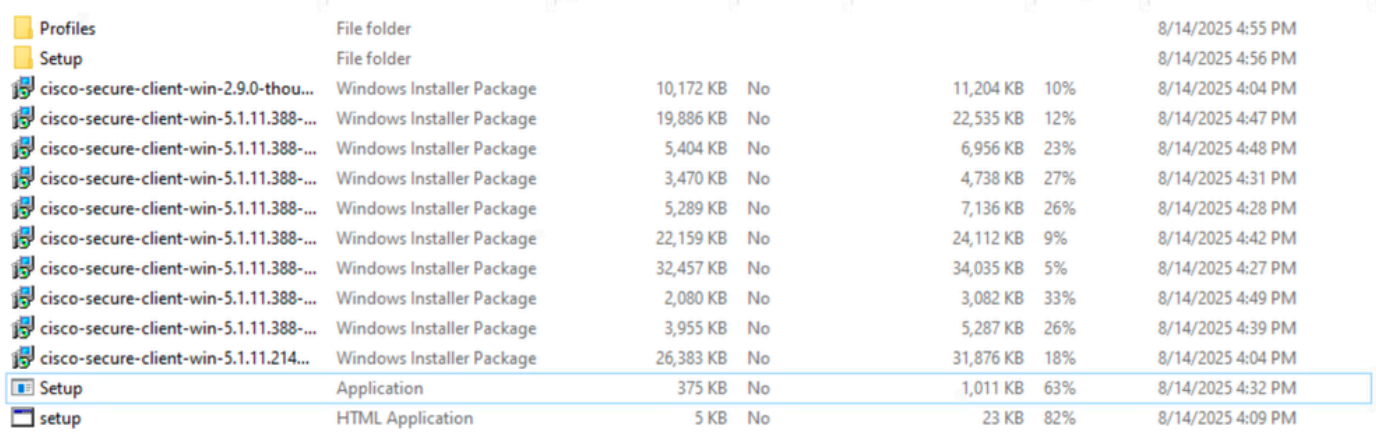


File zip pre-distribuzione



Nota: Cisco AnyConnect è stato dichiarato obsoleto e non è più disponibile sul sito di download del software Cisco.

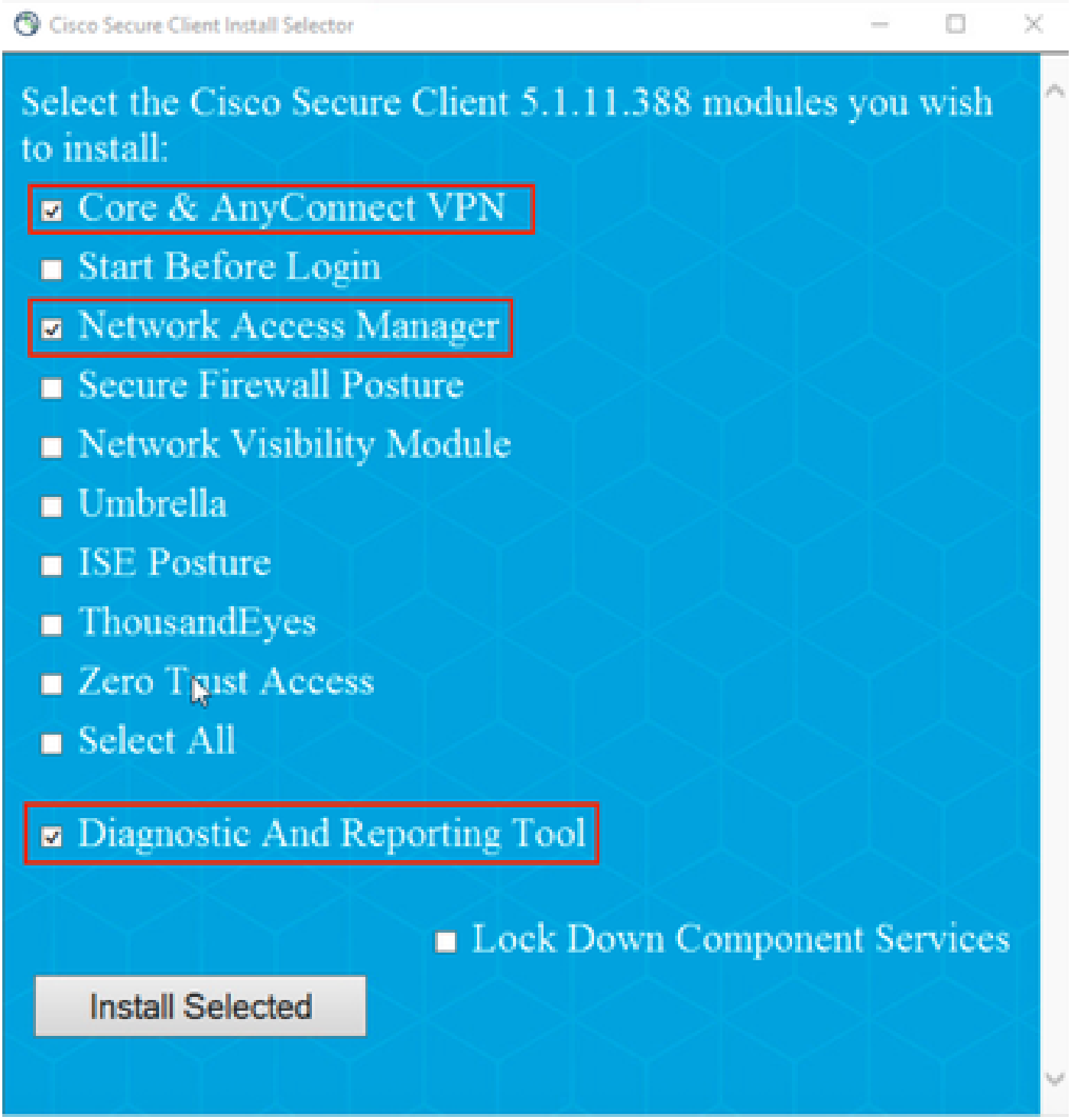
Passaggio 2. Una volta scaricati ed estratti, fare clic su Setup.



Profiles	File folder					8/14/2025 4:55 PM
Setup	File folder					8/14/2025 4:56 PM
cisco-secure-client-win-2.9.0-thou...	Windows Installer Package	10,172 KB	No	11,204 KB	10%	8/14/2025 4:04 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	19,886 KB	No	22,535 KB	12%	8/14/2025 4:47 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	5,404 KB	No	6,956 KB	23%	8/14/2025 4:48 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	3,470 KB	No	4,738 KB	27%	8/14/2025 4:31 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	5,289 KB	No	7,136 KB	26%	8/14/2025 4:28 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	22,159 KB	No	24,112 KB	9%	8/14/2025 4:42 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	32,457 KB	No	34,035 KB	5%	8/14/2025 4:27 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	2,080 KB	No	3,082 KB	33%	8/14/2025 4:49 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	3,955 KB	No	5,287 KB	26%	8/14/2025 4:39 PM
cisco-secure-client-win-5.1.11.214...	Windows Installer Package	26,383 KB	No	31,876 KB	18%	8/14/2025 4:04 PM
Setup	Application	375 KB	No	1,011 KB	63%	8/14/2025 4:32 PM
setup	HTML Application	5 KB	No	23 KB	82%	8/14/2025 4:09 PM

File Zip Predeployment

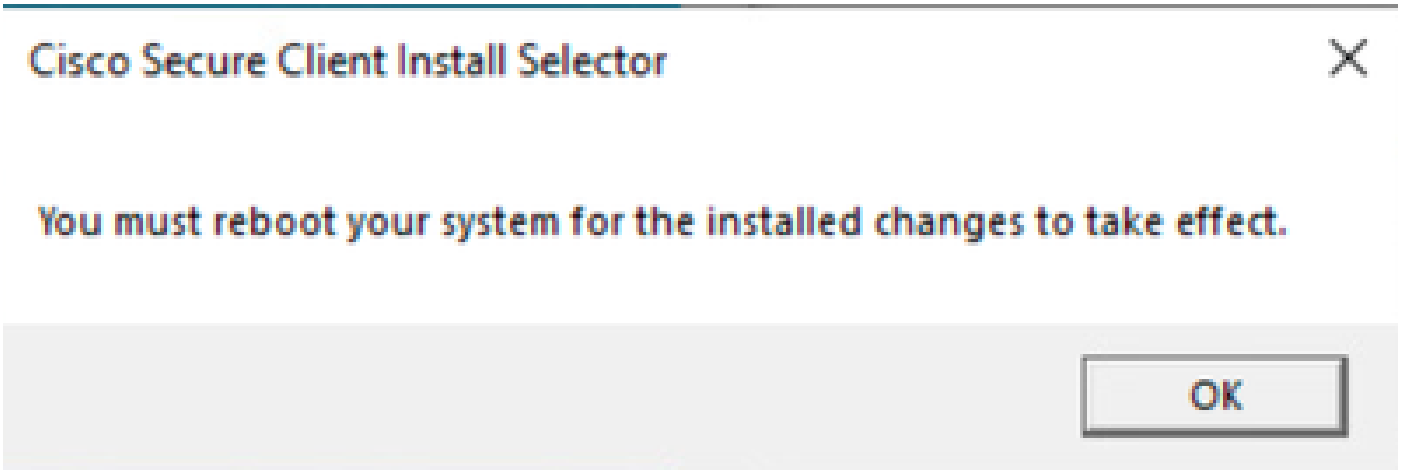
Passaggio 3. Installare i moduli Core e AnyConnect VPN, Network Access Manager e i moduli Diagnostica e Report.



Secure Client Installer

Fare clic su Install Selected (Installa selezionati).

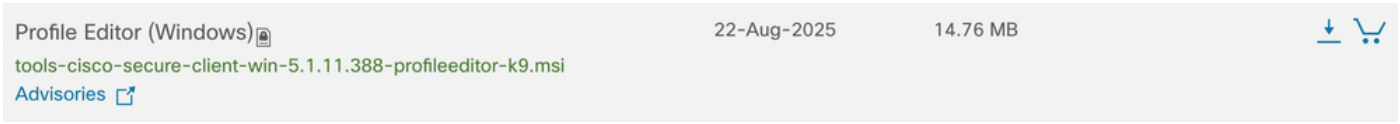
Passaggio 4. Dopo l'installazione è necessario riavviare il sistema. Fare clic su OK e riavviare il dispositivo.



Popup richiesto Riavvio

Parte 2: Scarica e installa l'Editor di profili Secure Client NAM

Passaggio 1. L'Editor di profili si trova nella stessa pagina di download di Secure Client. In questo esempio di configurazione viene utilizzata la versione 5.1.11.388.



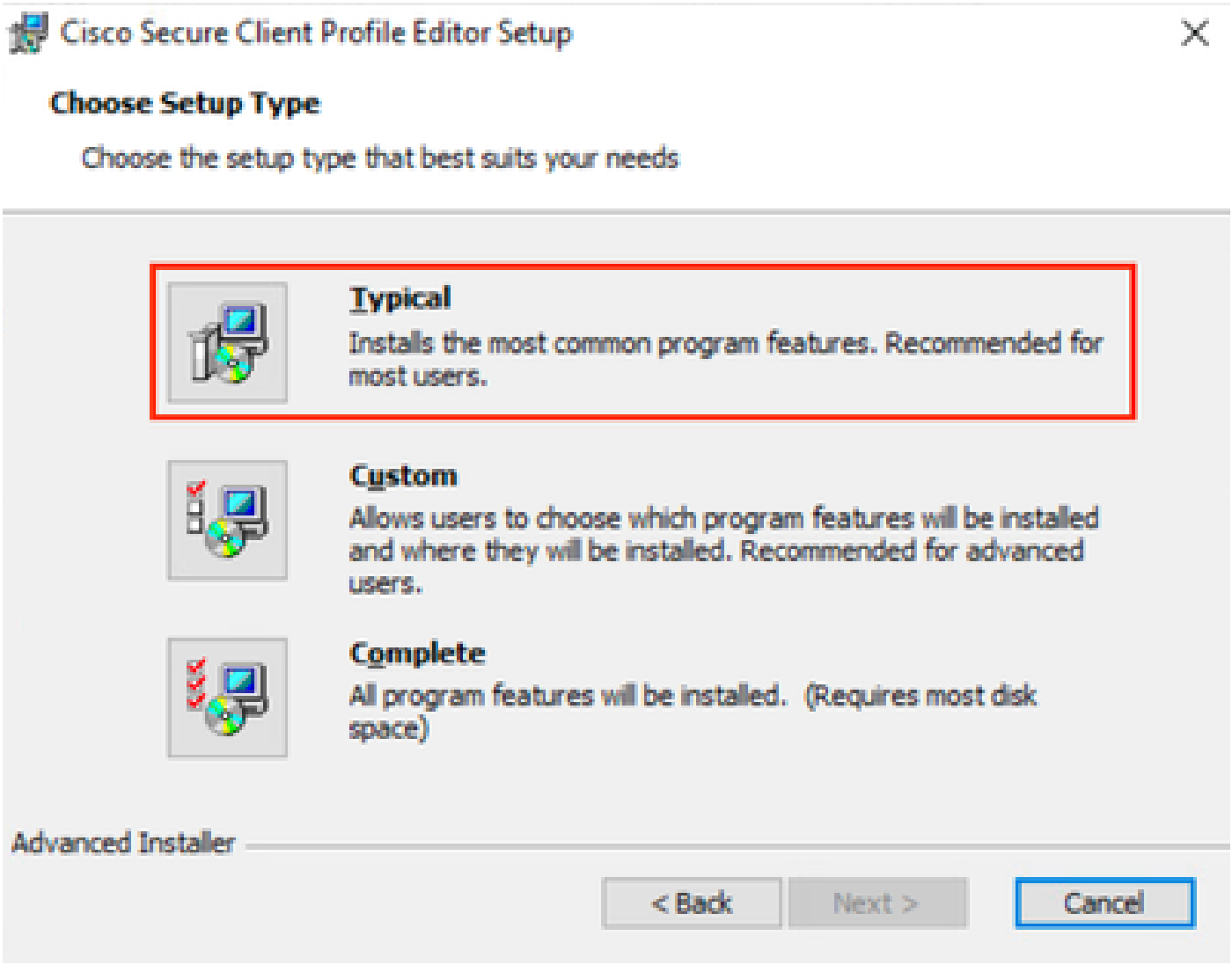
Editor di profili

Scaricare e installare l'Editor di profili.

Passaggio 2. Eseguire il file MSI.

Avvio installazione Editor di profili

Passaggio 3. Utilizzare l'opzione di installazione Tipica e installare NAM Profile Editor.

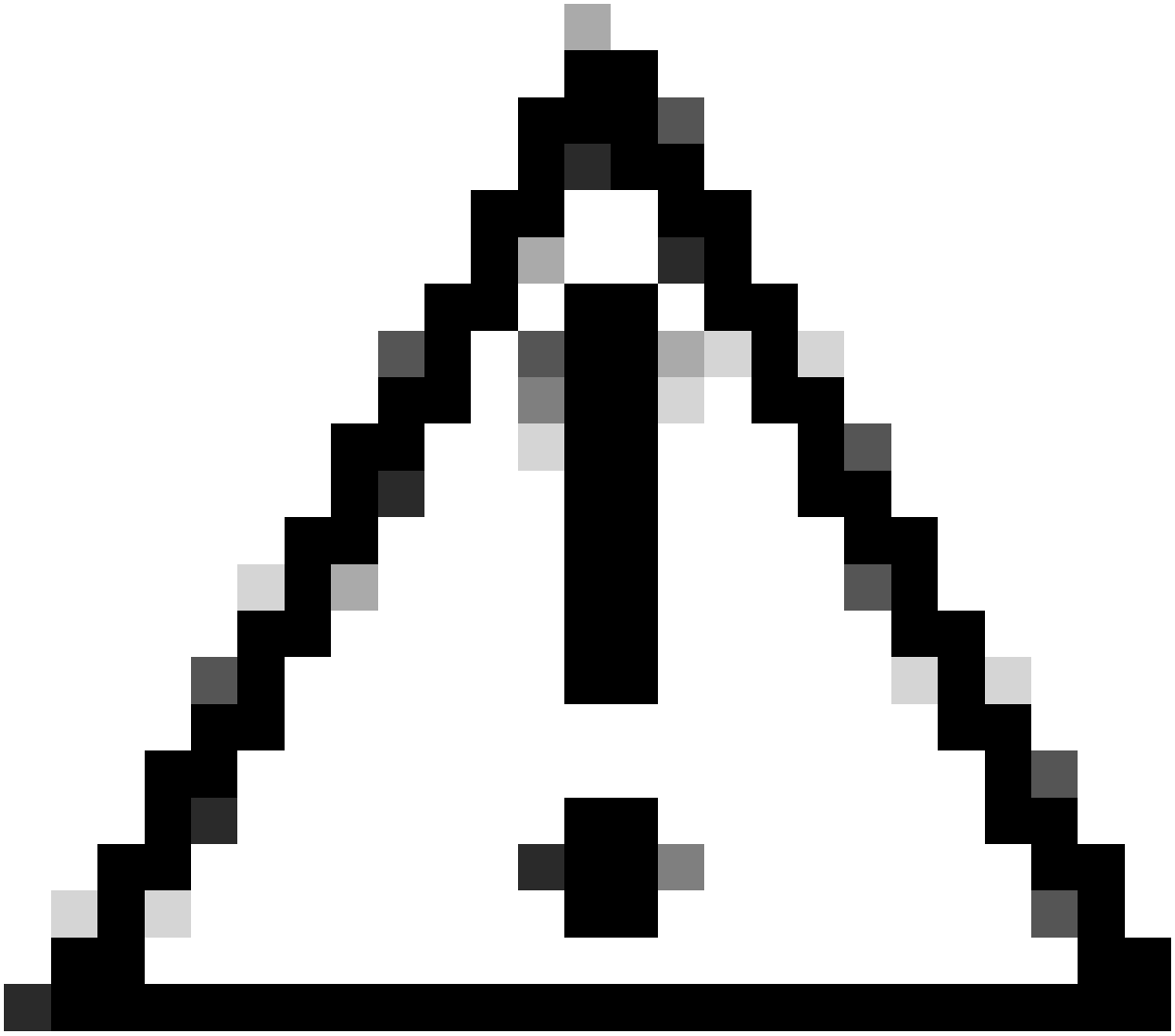


Installazione dell'Editor di profili

Parte 3: Consenti accesso alle credenziali della cache di Windows da parte di NAM

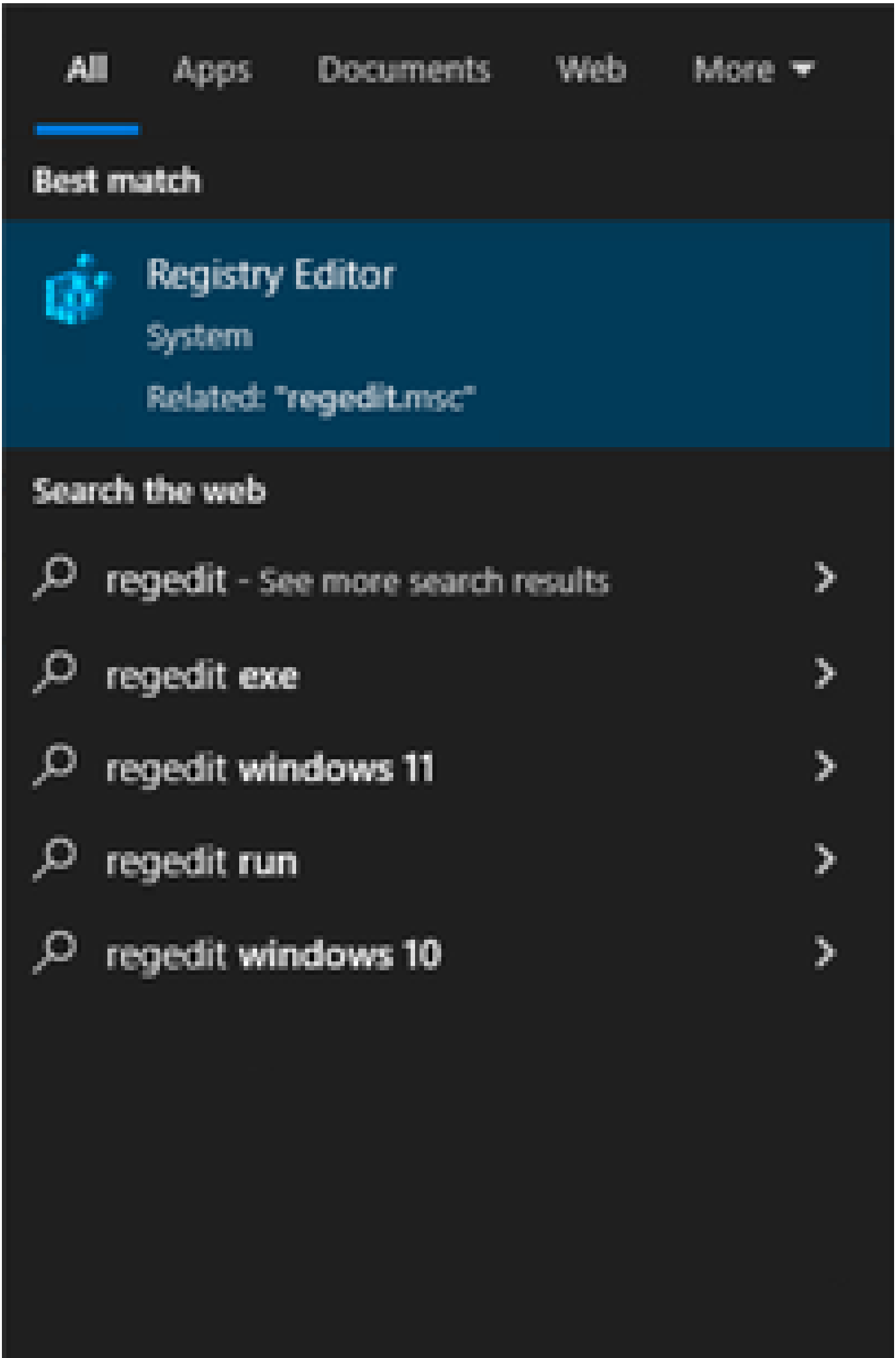
Per impostazione predefinita, in Windows 10, Windows 11 e Windows Server 2012 il sistema operativo impedisce a Network Access Manager (NAM) di recuperare la password del computer necessaria per l'autenticazione del computer. Di conseguenza, l'autenticazione del computer tramite la password del computer non funziona a meno che non venga applicata una correzione del Registro di sistema.

Per consentire a NAM di accedere alle credenziali del computer, applicare la correzione dell'KB 2743127 Microsoft sul desktop del client.



Attenzione: La modifica non corretta del Registro di sistema di Windows può causare gravi problemi. Assicurarsi di eseguire il backup del Registro di sistema prima di apportare modifiche.

Passaggio 1. Nella barra di ricerca di Windows, immettere regedit, quindi fare clic su Editor del Registro di sistema.

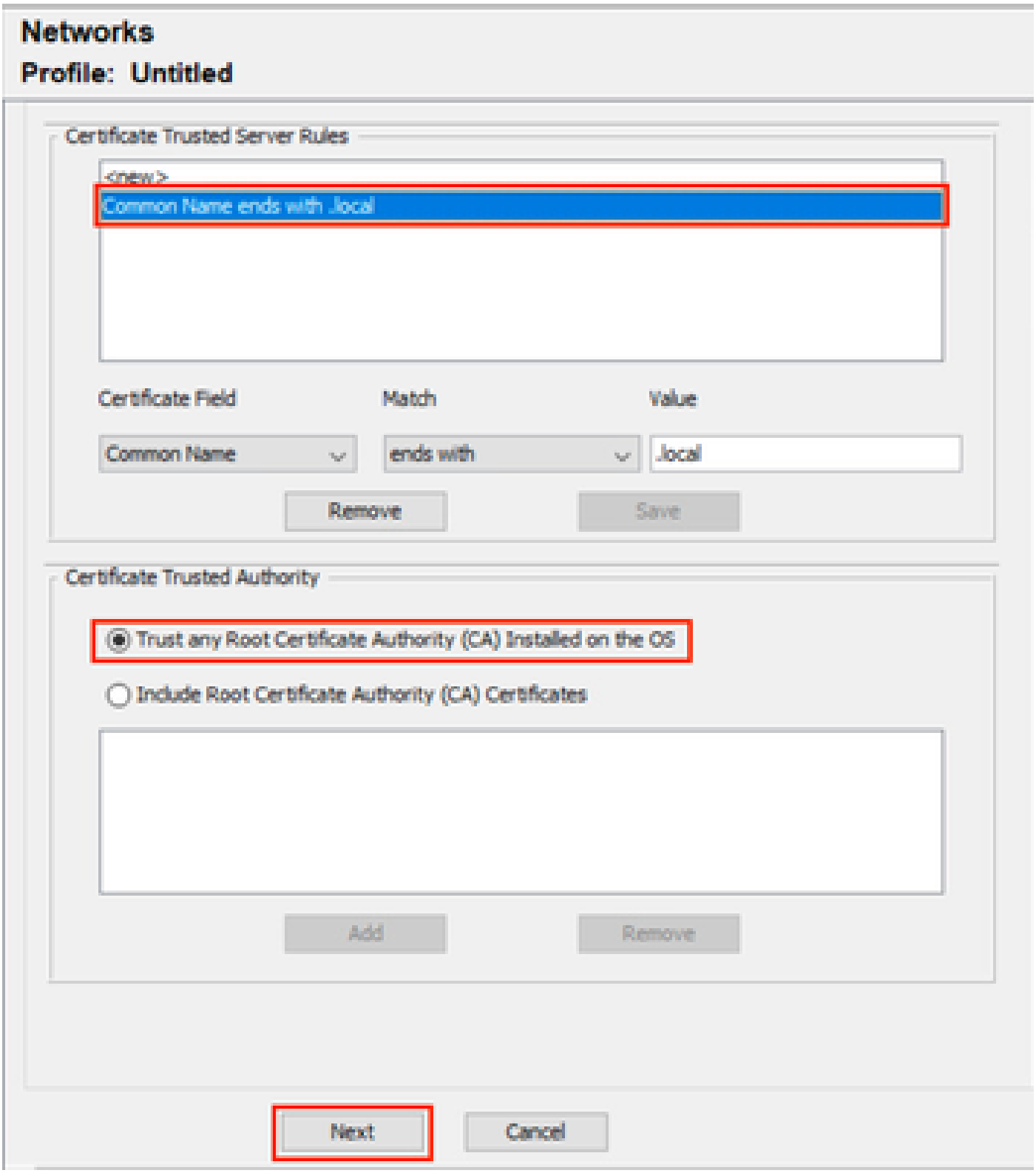

All
Apps
Documents
Web
More
Best match
Registry Editor
System
Related: "regedit.msc"
Search the web
regedit - See more search results
regedit exe
regedit windows 11
regedit run
regedit windows 10

In questo esempio, il certificato del nodo PSN viene emesso da varshaah.varshaah.local. Pertanto, viene utilizzata la regola Nome comune termina con .local. Questa regola convalida il certificato presentato dal server durante il flusso EAP-TTLS.

È inoltre possibile specificare il nome comune del certificato di autenticazione EAP Policy Service Node (PSN).

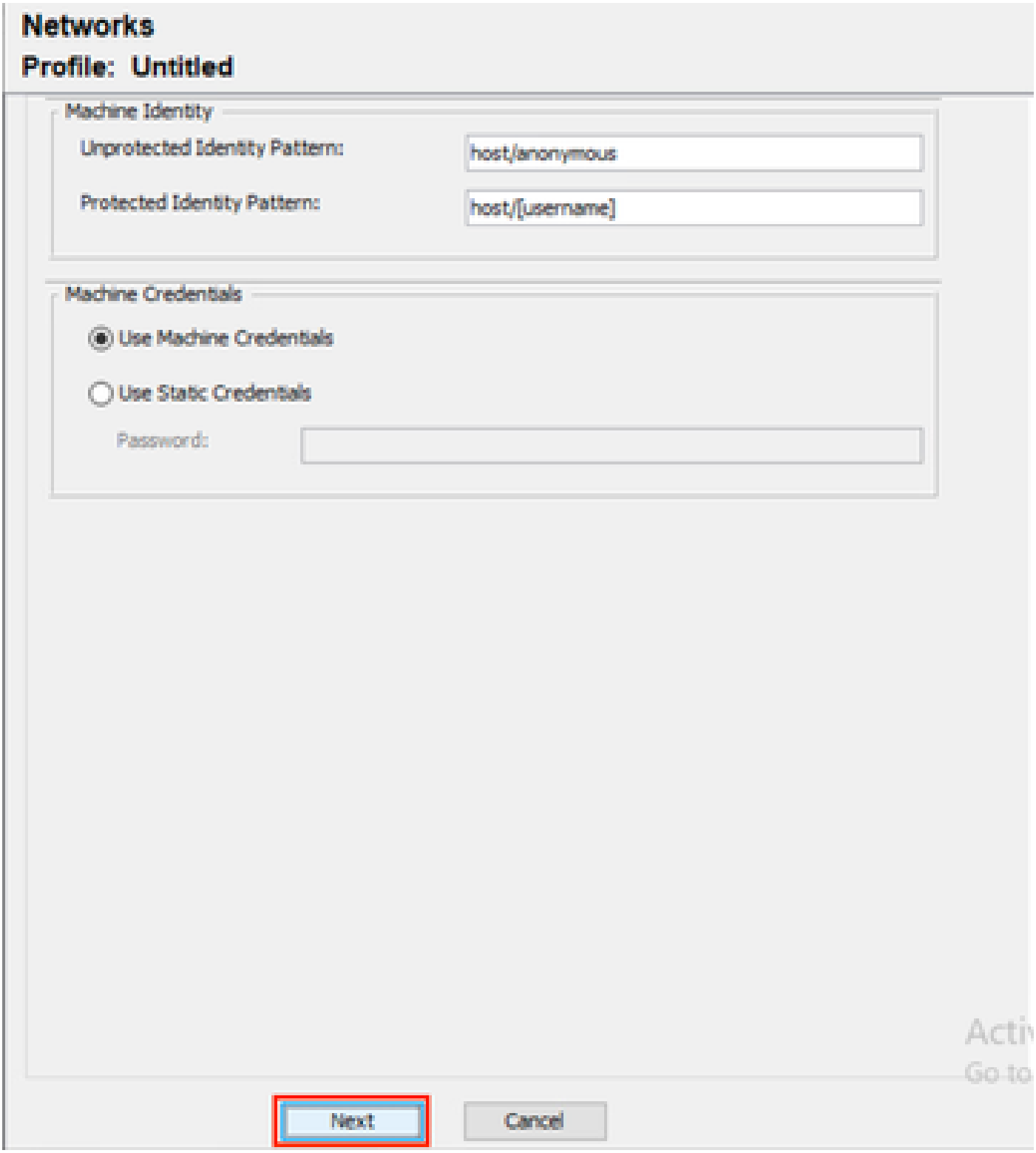
- In Autorità di certificazione attendibile sono disponibili due opzioni.
  In questo scenario viene utilizzata l'opzione Considera attendibile qualsiasi CA radice installata nel sistema operativo anziché aggiungere un certificato CA specifico.

  Con questa opzione, il dispositivo Windows considera attendibile qualsiasi certificato EAP firmato da un certificato incluso in Certificati - Utente corrente > Autorità di certificazione radice attendibili > Certificati (gestiti dal sistema operativo).
- Fare clic su Avanti per continuare.



Certificati dell'Editor di profili NAM

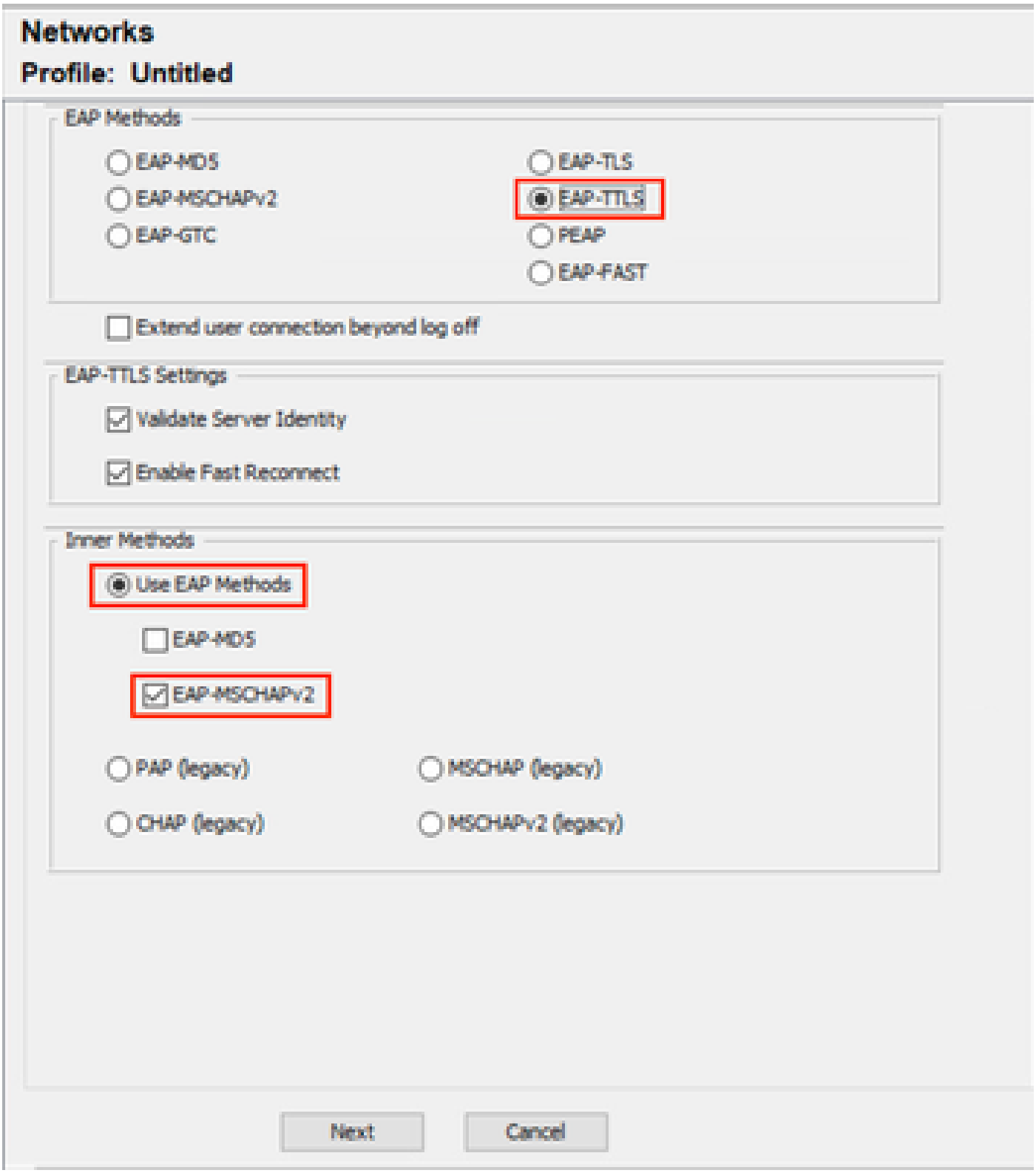
Passaggio 6. Nella sezione Credenziali computer, selezionare Usa credenziali computer, quindi fare clic su Avanti.



Credenziali dell'editor di profili NAM

Passaggio 7. Sezione Configurazione autenticazione utente.

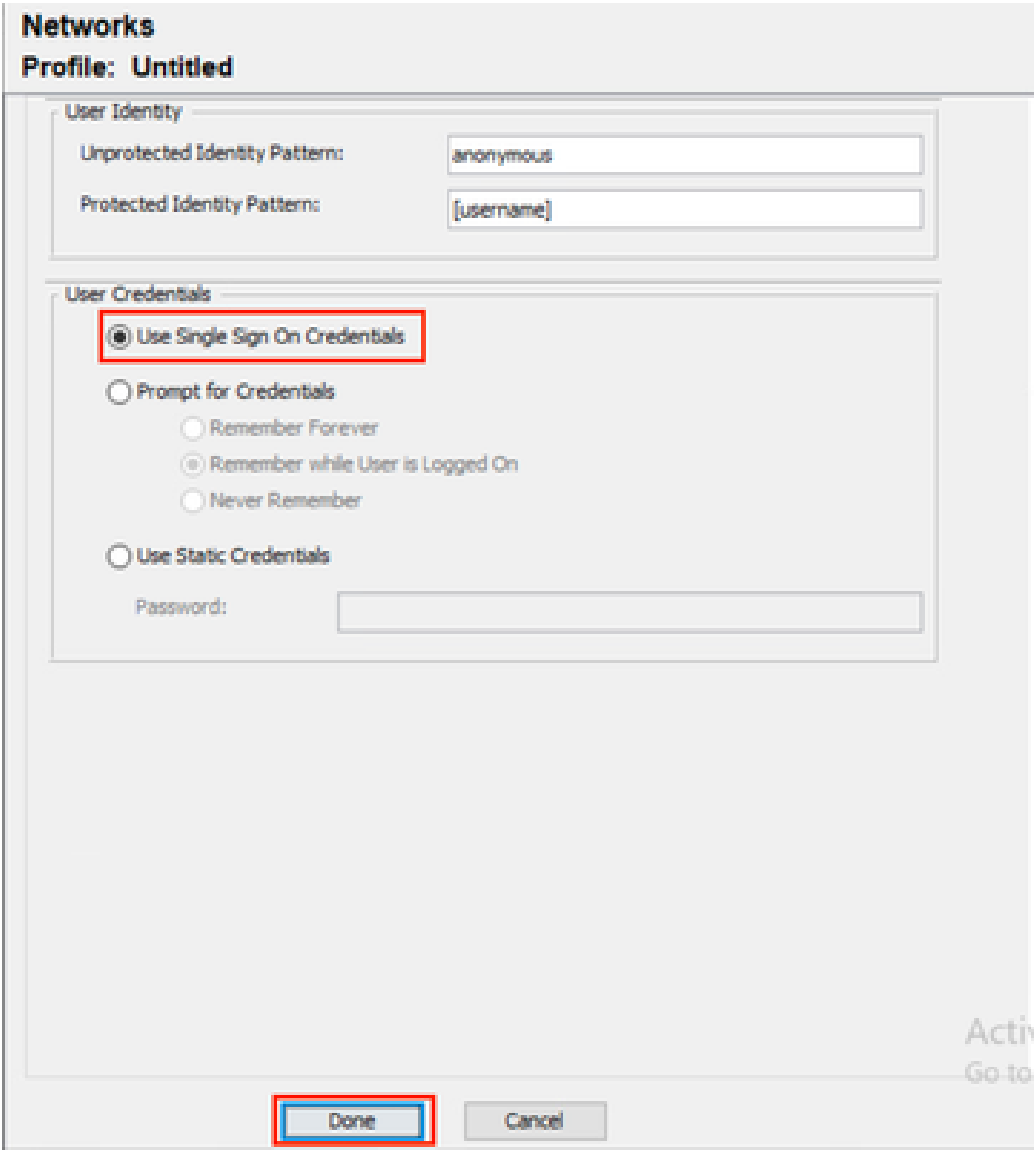
- Selezionare EAP-TTLS in Metodi EAP.
- In Metodi interni, selezionare Usa metodi EAP, quindi selezionare EAP-MSCHAPv2.
- Fare clic su Next (Avanti).



Autenticazione utente editor profili NAM

Passaggio 8. In Certificati, configurare le stesse regole di convalida dei certificati descritte nel passaggio 5.

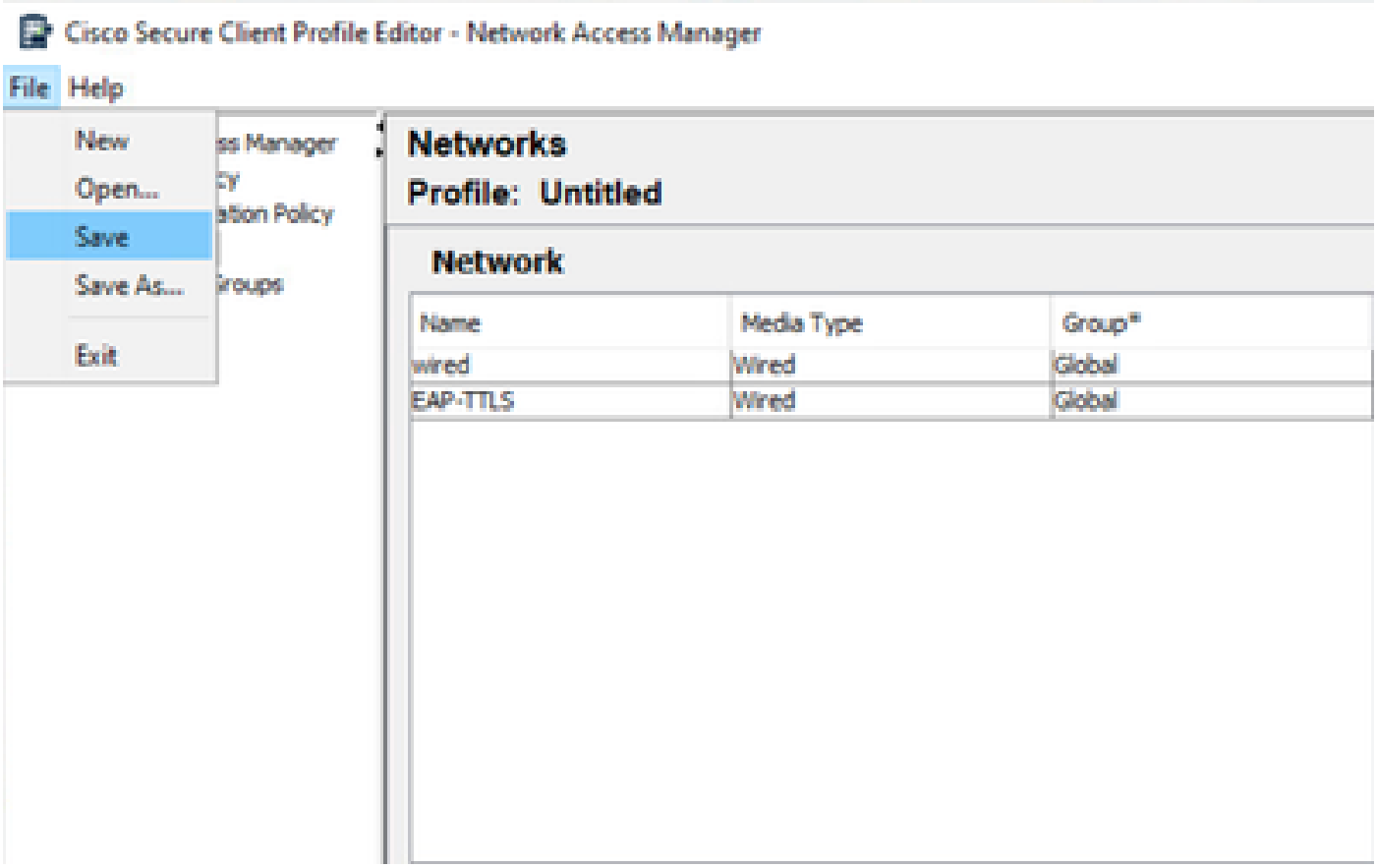
Passaggio 9. In Credenziali utente, selezionare Usa credenziali Single Sign-On, quindi fare clic su Fine.



Credenziali utente dell'Editor di profili NAM

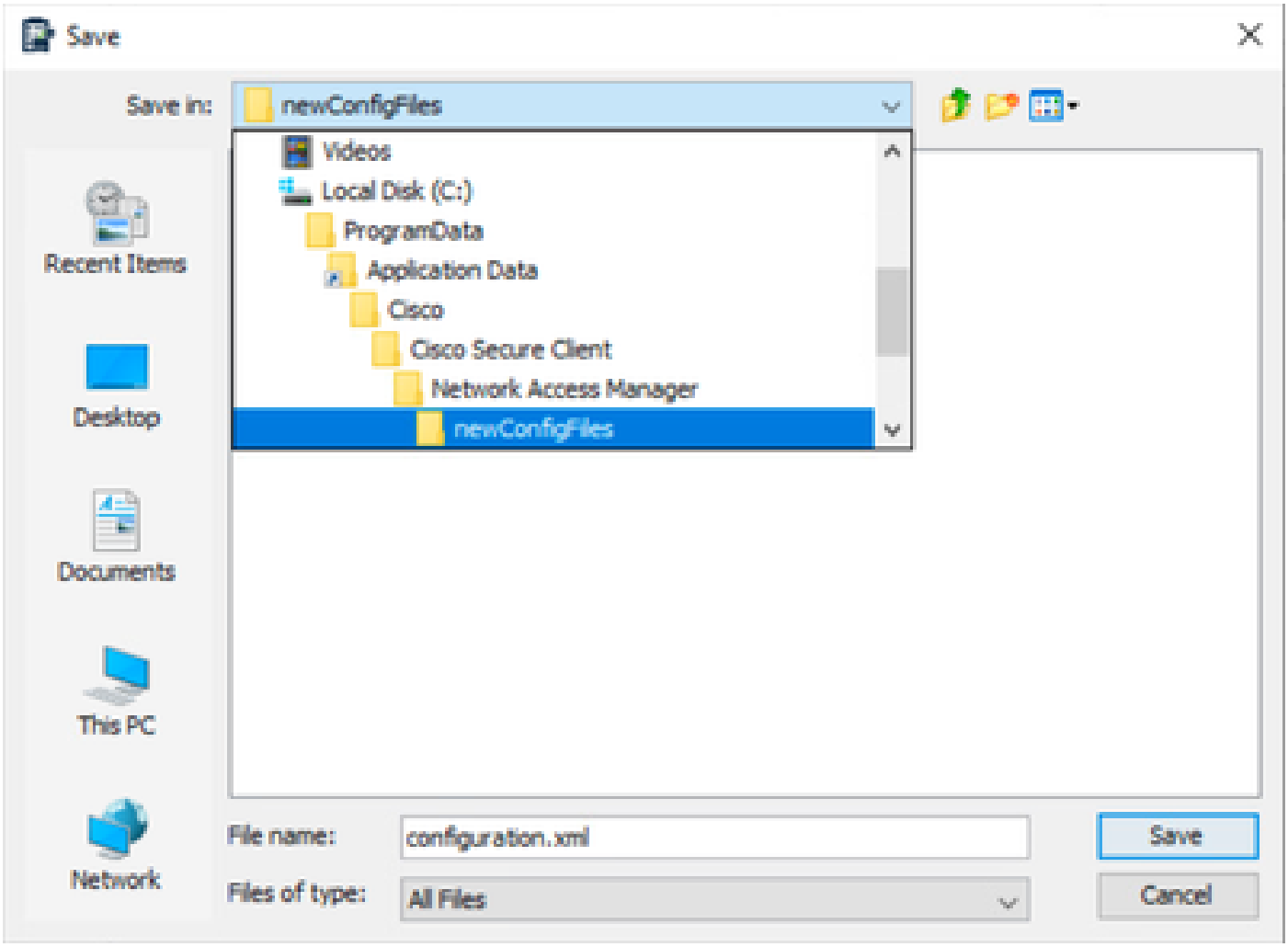
Parte 6: Salvataggio del file di configurazione di rete

Passaggio 1. Fare clic su File > Salva.



Configurazione di rete salvata dall'Editor profili NAM

Passaggio 2. Salvare il file come configuration.xml nella cartella newConfigFiles.

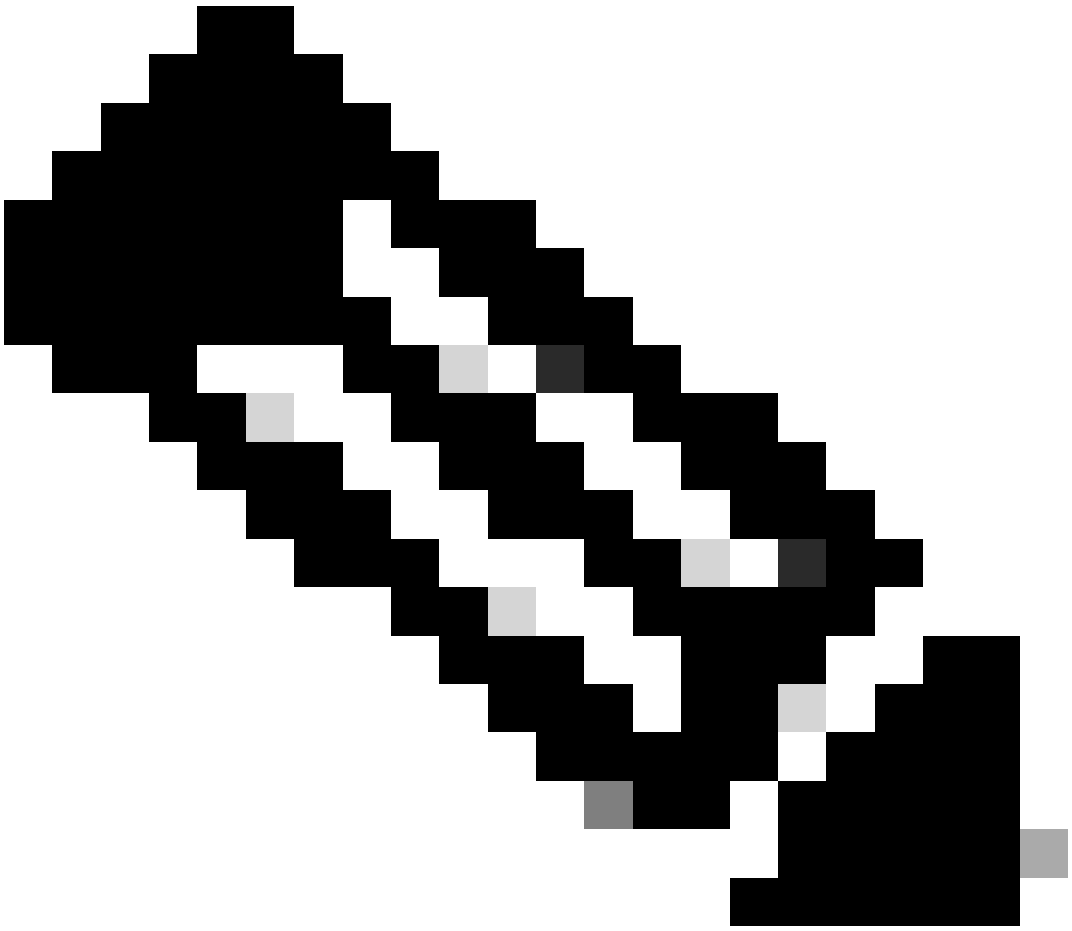


Salva configurazione di rete

Parte 7: Configurazione del server AAA sullo switch

```
C9300-1#sh run aaa
!
aaa authentication dot1x default group labgroup
aaa authorization network default group labgroup
aaa accounting dot1x default start-stop group labgroup
aaa accounting update newinfo periodic 2880
!
!
!
!
aaa server radius dynamic-author
 client 10.76.112.135 server-key cisco
!
!
radius server labserver
 address ipv4 10.76.112.135 auth-port 1812 acct-port 1813
 key cisco
!
!
aaa group server radius labgroup
 server name labserver
!
```

```
!
!
!
aaa new-model
aaa session-id common
!
!



C9300-1(config)#dot1x system-auth-control
```



> Nota: il comando dot1x system-auth-control non viene visualizzato nell'output show running-config, ma è necessario per abilitare 802.1X a livello globale.

Configurare l'interfaccia dello switch per 802.1X:

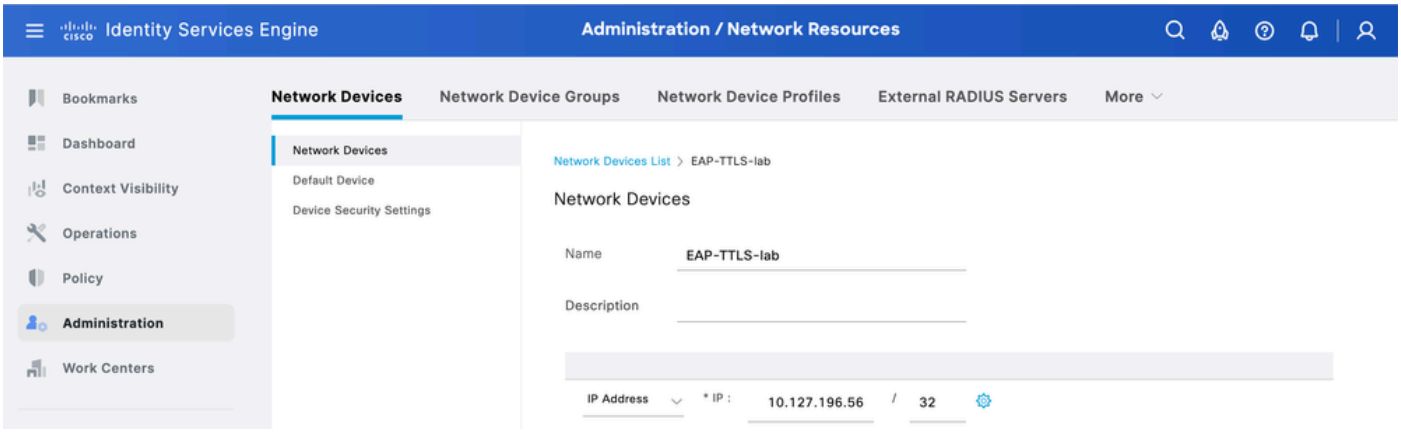
```
C9300-1(config)#do sh run int gig1/0/44
Building configuration...

Current configuration : 242 bytes
!
interface GigabitEthernet1/0/44
 switchport access vlan 96
 switchport mode access
 device-tracking
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication host-mode multi-auth
 authentication periodic

 mab
 dot1x pae authenticator
end
```

Parte 8: Configurazioni ISE

Passaggio 1. Configurare lo switch su ISE.

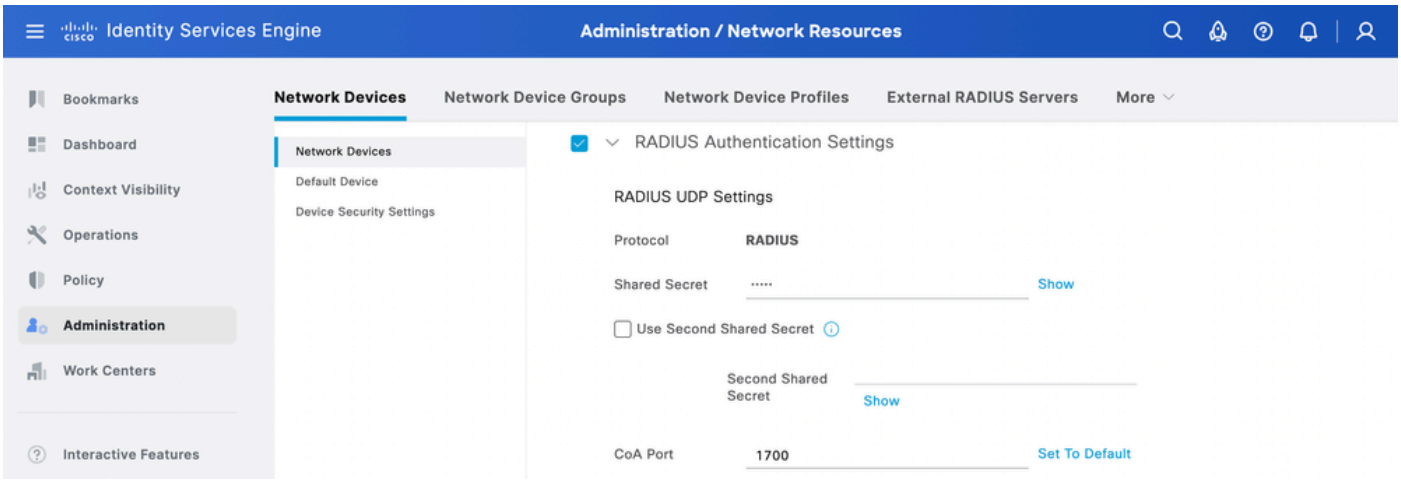
Selezionare Amministrazione > Risorse di rete > Dispositivi di rete e fare clic su Aggiungi.

Immettere qui il nome dello switch e l'indirizzo IP.



Aggiunta del dispositivo di rete ISE

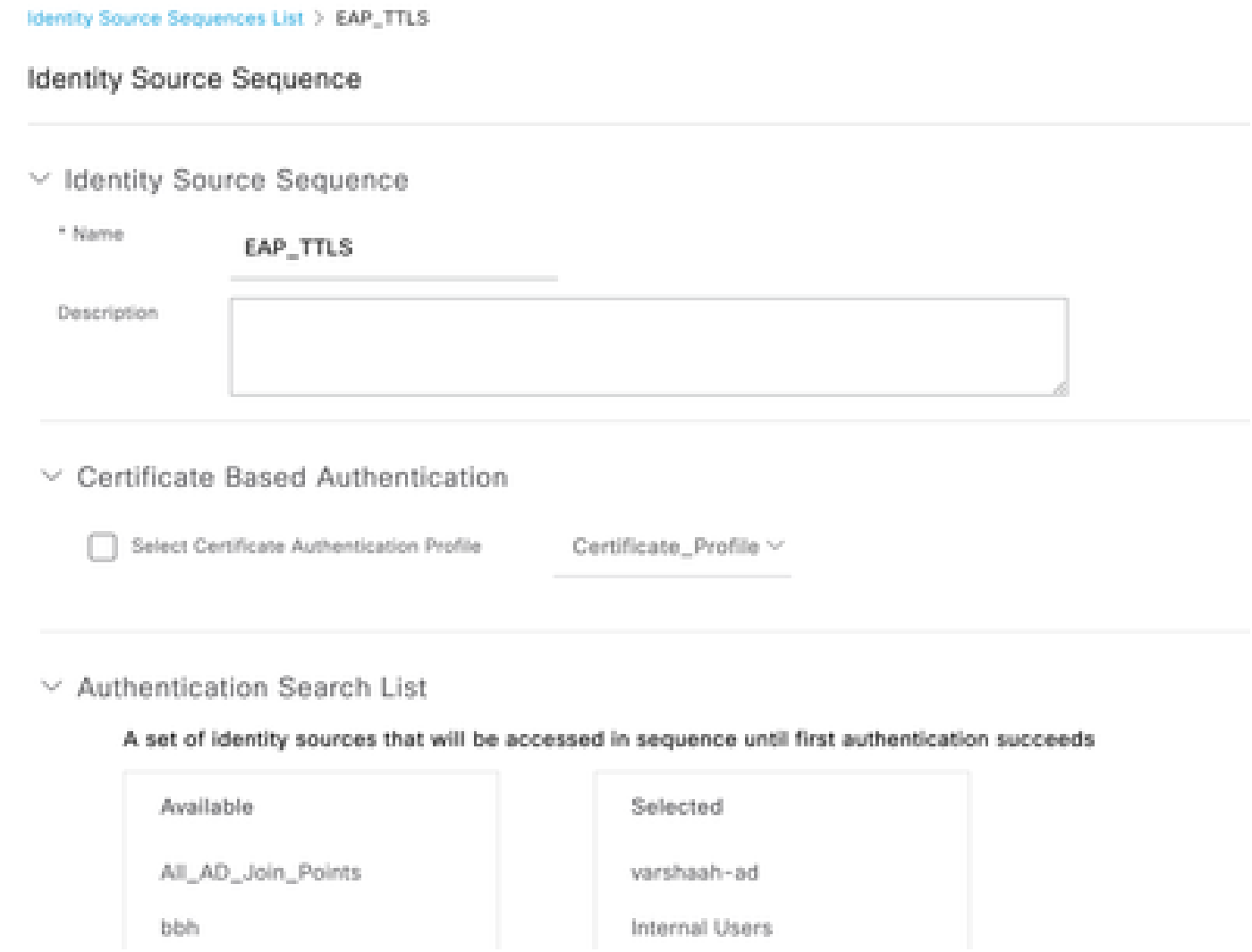
Immettere il segreto condiviso RADIUS, lo stesso di quello configurato in precedenza sullo switch.



RADIUS Shared Secret ISE

Passaggio 2. Configurare la sequenza di origine dell'identità.

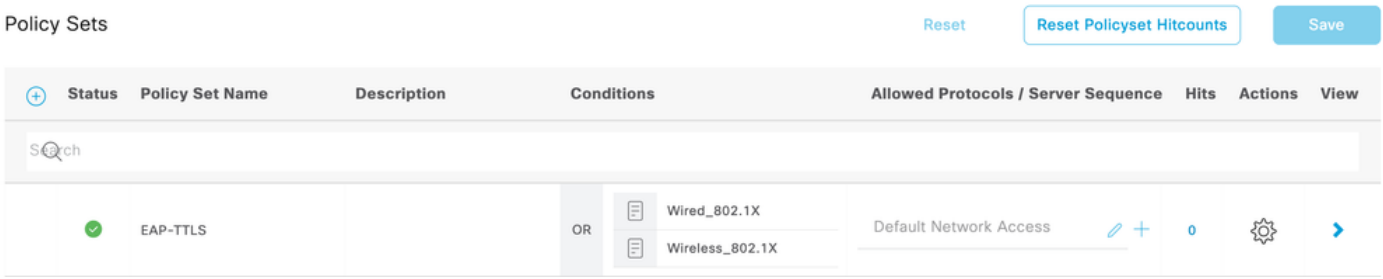
- Passare a Amministrazione > Gestione delle identità > Sequenze origini identità.
- Fare clic su Aggiungi per creare una nuova sequenza di origine identità.
- Configurare le origini di identità nell'elenco di ricerca autenticazione.



ISE Identity Source Sequence

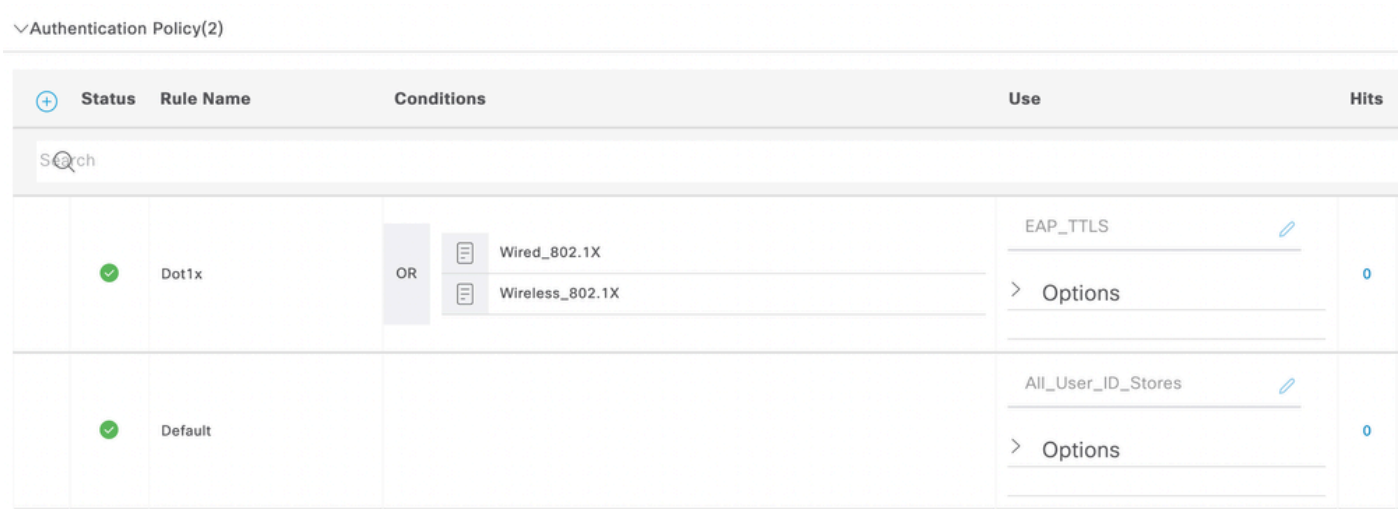
Passaggio 3. Configurare il set di criteri.

Passare a Criterio > Set di criteri e creare un nuovo set di criteri. Configurare le condizioni come Wired_802.1x O Wireless_802.1x. Per Protocolli consentiti, scegliere Accesso di rete predefinito:



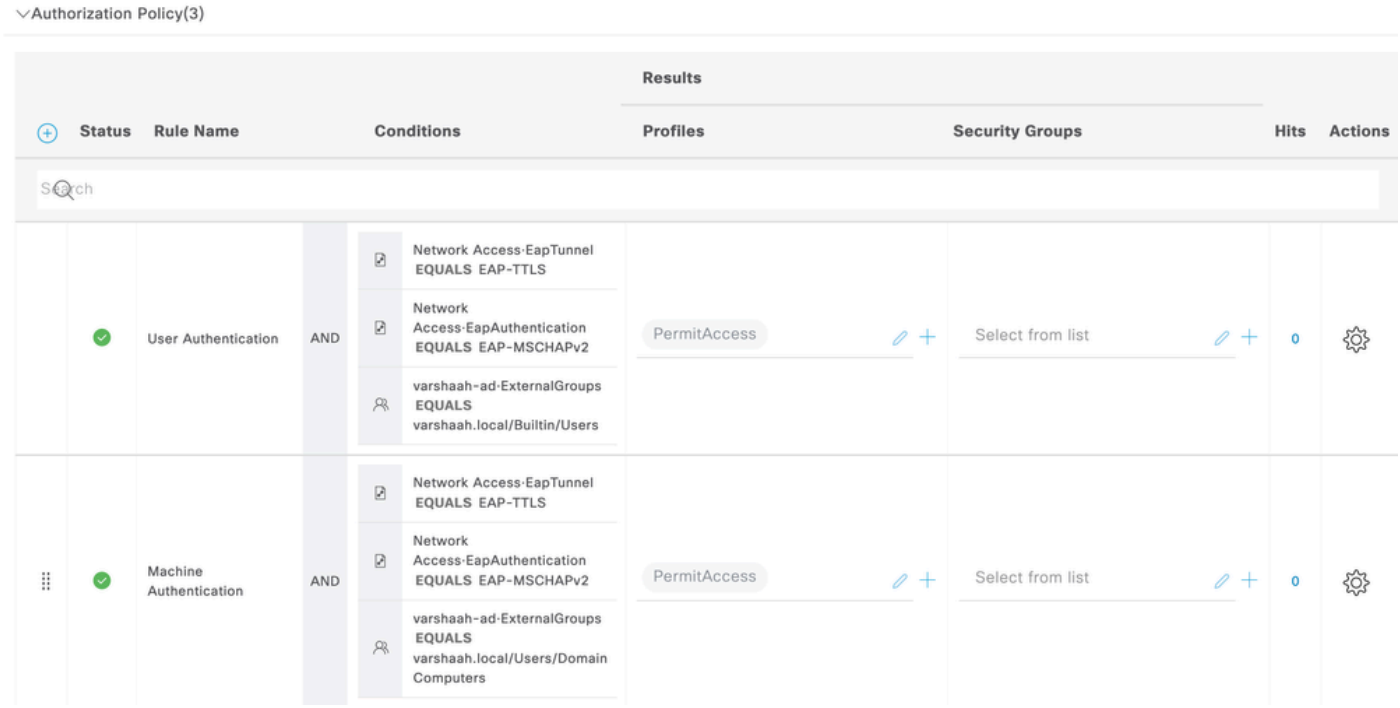
Set di criteri EAP-TTLS

Creare il criterio di autenticazione per dot1x e scegliere la sequenza di origine dell'identità creata al passaggio 4.



Criterio di autenticazione EAP-TTLS

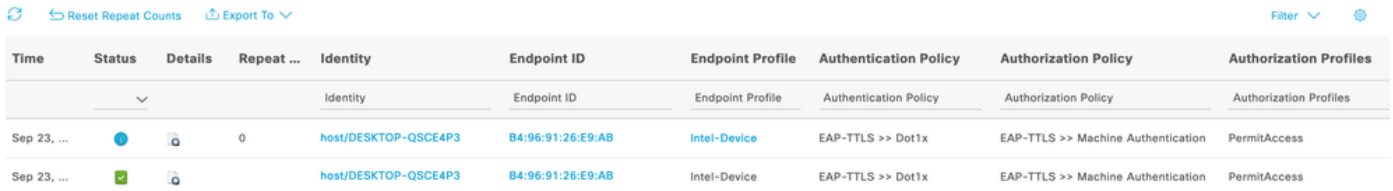
Per i criteri di autorizzazione, creare la regola con tre condizioni. La prima condizione verifica la condizione di utilizzo del tunnel EAP-TTLS. La seconda condizione verifica che EAP-MSCHAPv2 sia utilizzato come metodo EAP interno. La terza condizione verifica il rispettivo gruppo AD.



Criteri di autorizzazione dot1x

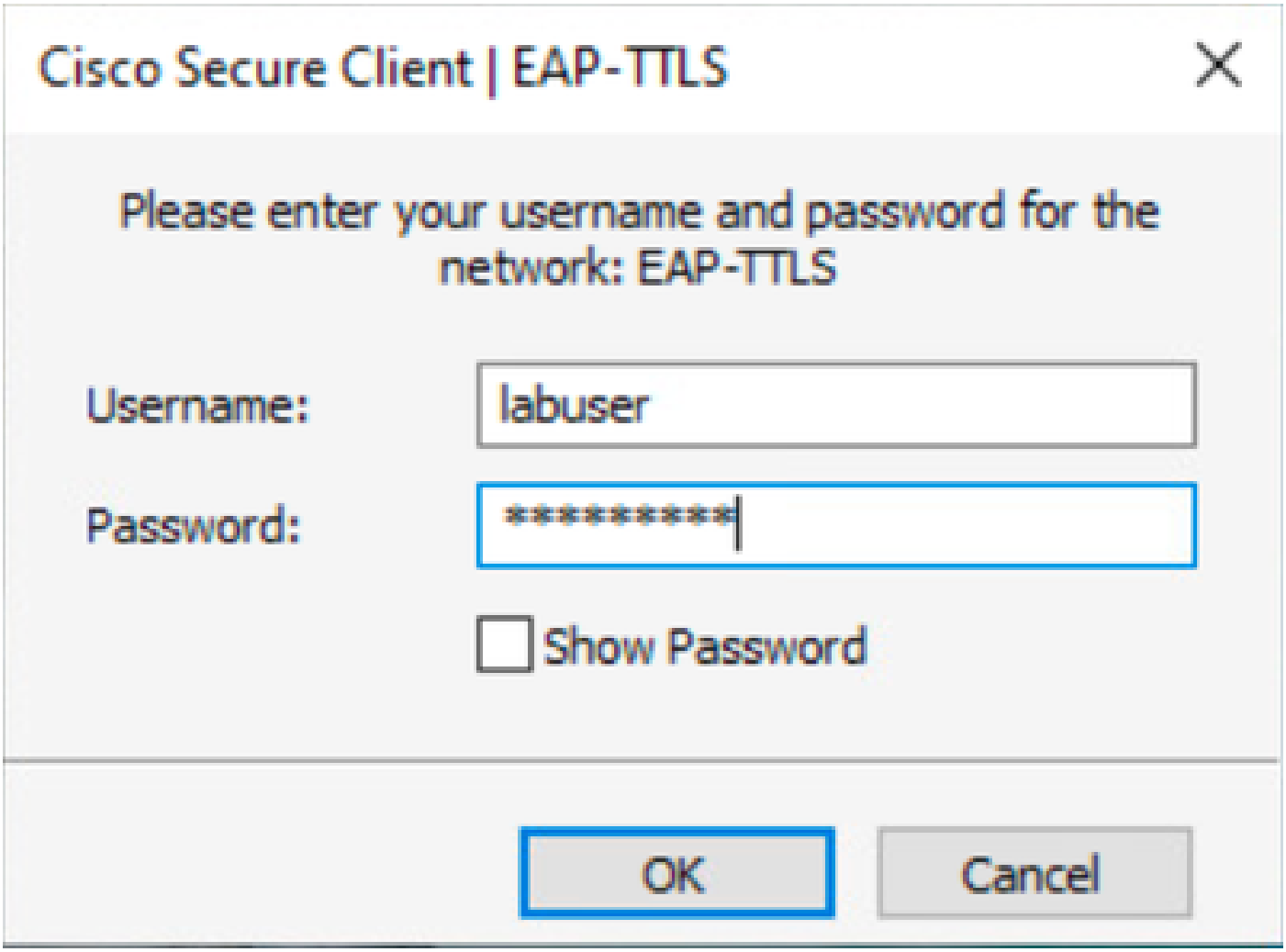
Verifica

È possibile riavviare il computer con Windows 10 oppure disconnettersi e accedere. Ogni volta che viene visualizzata la schermata di accesso a Windows, viene attivata l'autenticazione del computer.

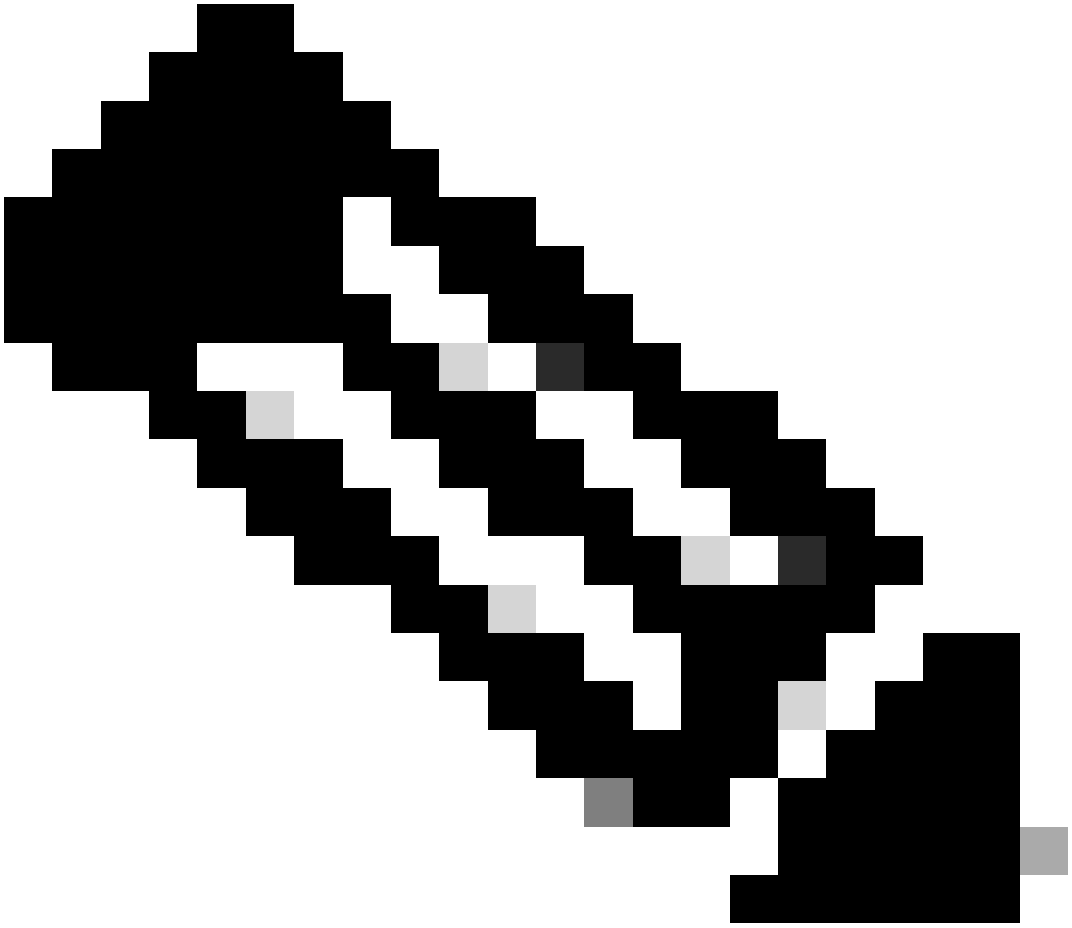


Autenticazione Live Log Machine

Quando si accede al PC con le credenziali, viene attivata l'autenticazione dell'utente.

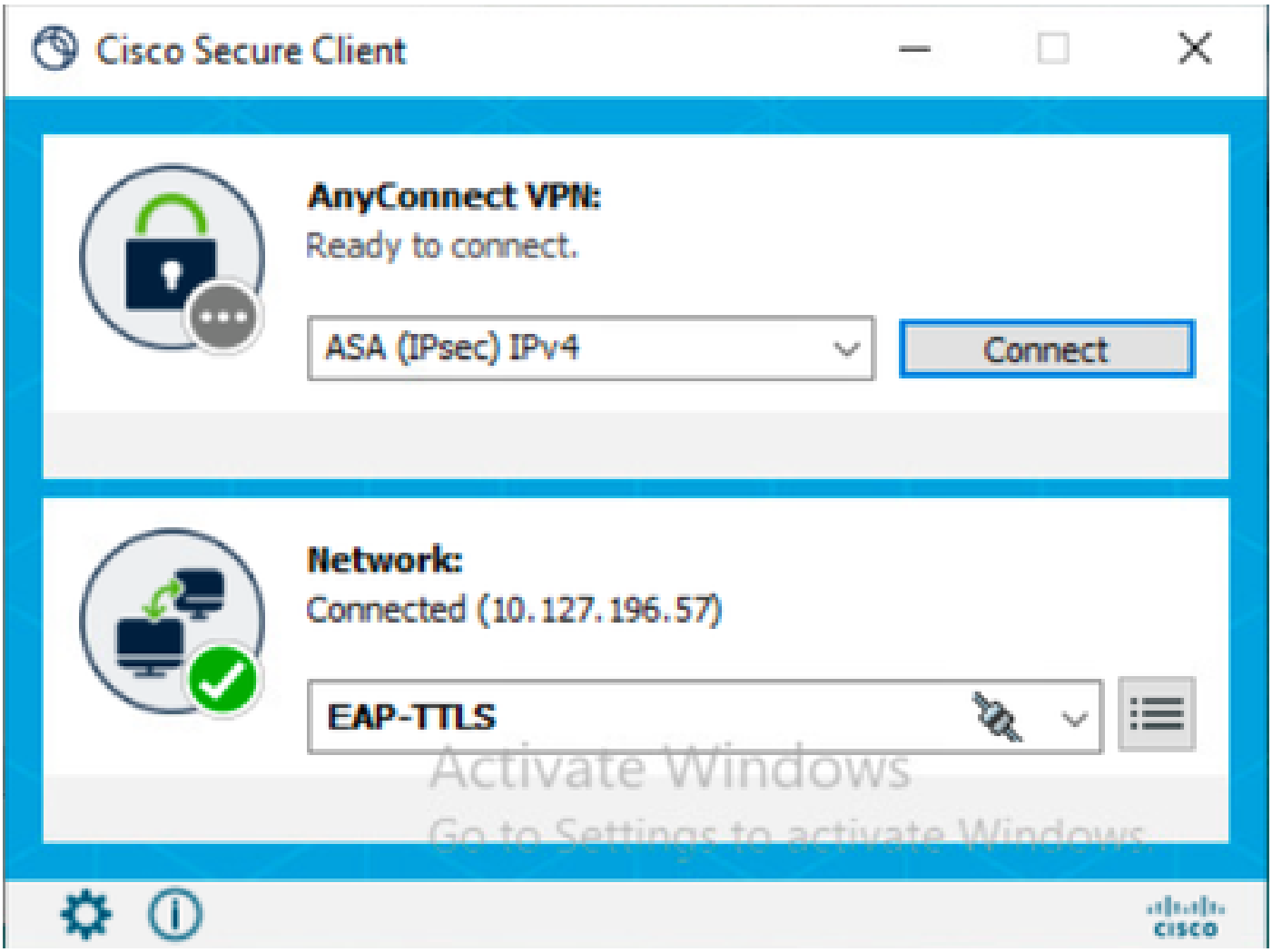


Credenziali di autenticazione utente

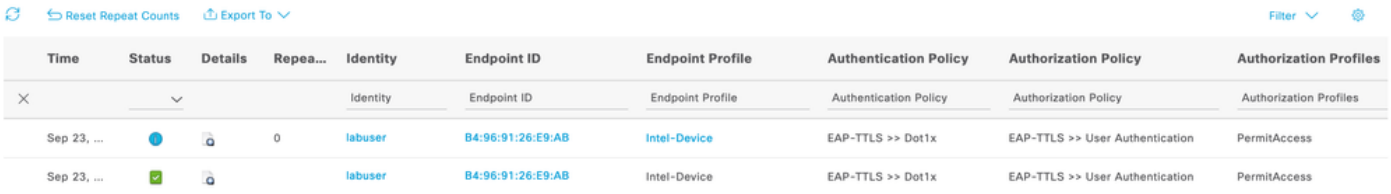


Nota: In questo esempio vengono utilizzate le credenziali utente di Active Directory per l'autenticazione. In alternativa, è possibile creare un utente interno in Cisco ISE e usare le credenziali per eseguire l'accesso.

Dopo l'immissione e la verifica delle credenziali, l'endpoint viene connesso alla rete con l'autenticazione dell'utente.



EAP-TTLS connesso



Autenticazione utente Live Log

Analisi dei Live Log ISE RADIUS

In questa sezione vengono illustrate le voci del registro attivo RADIUS per la corretta autenticazione del computer e dell'utente.

Autenticazione computer

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ... 11507 Extracted EAP-Response/Identity **12983 Prepared EAP-Request proposing EAP-TTLS with challenge** ... ... **12978 Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated** 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 ... ... 12803 Extracted TLS ChangeCipherSpec message 12804 Extracted TLS Finished message

12801 Prepared TLS ChangeCipherSpec message 12802 Prepared TLS Finished message **12816 TLS handshake succeeded** ... ... **11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge** 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response **11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated** ... ... 24431 Authenticating machine against Active Directory - varshaah-ad 24325 Resolving identity - host/DESKTOP-QSCE4P3 ... ... 24343 RPC Logon request succeeded - DESKTOP-QSCE4P3$@varshaah.local **24470 Machine authentication against Active Directory is successful - varshaah-ad** 22037 Authentication Passed ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response 11810 Extracted EAP-Response for inner method containing MSCHAP challenge-response 11814 Inner EAP-MSCHAP authentication succeeded 11519 Prepared EAP-Success for inner EAP method **12975 EAP-TTLS authentication succeeded** ... ... 15036 Evaluating Authorization Policy 24209 Looking up Endpoint in Internal Endpoints IDStore - host/DESKTOP-QSCE4P3 24211 Found Endpoint in Internal Endpoints IDStore 15048 Queried PIP - Network Access.Device IP Address 15048 Queried PIP - Network Access.EapTunnel **15016 Selected Authorization Profile - PermitAccess** ... ... 11002 Returned RADIUS Access-Accept

Autenticazione utente

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ... 11507 Extracted EAP-Response/Identity **12983 Prepared EAP-Request proposing EAP-TTLS with challenge** ... ... **12978 Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated** 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 ... ... 12812 Extracted TLS ClientKeyExchange message 12803 Extracted TLS ChangeCipherSpec message 12804 Extracted TLS Finished message 12801 Prepared TLS ChangeCipherSpec message 12802 Prepared TLS Finished message **12816 TLS handshake succeeded** ... ... **11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge** 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response **11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated** ... ... 24430 Authenticating user against Active Directory - varshaah-ad 24325 Resolving identity - labuser@varshaah.local ... ... 24343 RPC Logon request succeeded - labuser@varshaah.local **24402 User authentication against Active Directory succeeded - varshaah-ad** 22037 Authentication Passed ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response 11810 Extracted EAP-Response for inner method containing MSCHAP challenge-response 11814 Inner EAP-MSCHAP authentication succeeded 11519 Prepared EAP-Success for inner EAP method **12975 EAP-TTLS authentication succeeded** ... ... 15036 Evaluating Authorization Policy 24209 Looking up Endpoint in Internal Endpoints IDStore - labuser 24211 Found Endpoint in Internal Endpoints IDStore 15048 Queried PIP - Network Access.Device IP Address 15048 Queried PIP - Network Access.EapTunnel **15016 Selected Authorization Profile - PermitAccess** ... ... 11002 Returned RADIUS Access-Accept

Analizza registri NAM

I registri NAM, soprattutto dopo aver attivato la registrazione estesa, contengono una grande quantità di dati, la maggior parte dei quali sono irrilevanti e possono essere ignorati. In questa sezione vengono elencate le righe di debug per illustrare i passaggi eseguiti da NAM per stabilire una connessione di rete. Quando si analizza un registro, queste frasi chiave possono essere utili per individuare una parte del registro relativa al problema.

Autenticazione computer

```
2160: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11812][comp=SAE]: 80
```

Il client riceve un pacchetto EAP-TTLS dallo switch di rete, avviando la sessione EAP-TTLS. Questo è il punto di partenza per il tunnel di autenticazione del computer.

```
2171: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11812][comp=SAE]: EA
2172: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11812][comp=SAE]: CER
2173: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11812][comp=SAE]: CER
```

Il client riceve il file Server Hello da ISE e inizia a convalidare il certificato del server (CN=varshaah.varshaah.local). Il certificato viene trovato nell'archivio di attendibilità del client e aggiunto per la convalida.

```
2222: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11768]: Validating th
2223: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11768]: Server certif
```

Convalida del certificato del server completata. Creazione del tunnel TLS.

```
2563: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.789 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2564: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.789 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11812][comp=SAE]: NE
2565: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.789 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
```

Segnali client passati dall'autenticazione. L'interfaccia viene sbloccata e la macchina a stati interni passa a USER_T_NOT_DISCONNECTED, a indicare che la macchina può ora passare il traffico.

```
2609: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2610: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11824][comp=SAE]: NE
2611: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2612: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11824][comp=SAE]: NE
2613: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2614: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11824][comp=SAE]: NE
2615: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
```

L'adattatore segnala l'autenticazione e il NAM AccessStateMachine passa ad ACCESS_AUTHENTICATED. Conferma che l'autenticazione del computer è stata completata e che il computer dispone dell'accesso completo alla rete.

Autenticazione utente

```
100: DESKTOP-QSCE4P3: Sep 25 2025 14:01:26.669 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9664]: Network EAP-TT
```

Il client NAM avvia il processo di connessione EAP-TTLS.

```
195: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3252]: Binding adapte
198: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3252]: Network EAP-TT
```

NAM associa la scheda fisica alla rete EAP-TTLS e passa allo stato ACCESS_ATTACHED, verificando che la scheda sia pronta per l'autenticazione.

```
204: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3252]: Network EAP-TT
247: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3680][comp=SAE]: STAT
```

Il client passa da ATTACHED a CONNECTING, iniziando lo scambio 802.1X.

```
291: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.388 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: 8021
```

Il client invia un comando EAPOL-Start per attivare il processo di autenticazione.

```
331: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.435 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: PORT
332: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.435 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: 8021
340: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.435 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: EAP
```

Lo switch richiede un'identità e il client si prepara a rispondere con un'identità esterna.

```
402: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.685 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9580]: EAP-CB: creden
422: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.685 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: processin
460: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.685 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: credentia
```

Il NAM invia l'identità esterna. Per impostazione predefinita, questo valore è anonimo, a indicare che lo scambio è per l'autenticazione utente (non computer).

```
488: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-6-INFO_MSG: %[tid=6088]: EAP: EAP sugges
489: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-6-INFO_MSG: %[tid=6088]: EAP: EAP reques
490: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: EAP metho
```

```
491: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: credentia
```

Sia il client che il server concordano di utilizzare EAP-TTLS come metodo esterno.

```
660: DESKTOP-QSCE4P3: Sep 25 2025 14:01:27.185 +0900: %csc_nam-7-DEBUG_MSG: %[tid=8296][comp=SAE]: EAP
661: DESKTOP-QSCE4P3: Sep 25 2025 14:01:27.185 +0900: %csc_nam-7-DEBUG_MSG: %[tid=8296][comp=SAE]: EAP
```

Il client invia Client Hello e riceve Server Hello, che include il certificato ISE.

```
706: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.967 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: 802
717: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.967 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EAP
718: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.967 +0900: %csc_nam-6-INFO_MSG: %[tid=11932][comp=SAE]: CERT
719: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-6-INFO_MSG: %[tid=11932][comp=SAE]: CERT
726: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EAP
```

Viene presentato il certificato del server. Il client cerca il file CN varshaah.varshaah.local, trova una corrispondenza e convalida il certificato. L'handshake viene sospeso durante il controllo del certificato X.509.

```
729: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EAP
730: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11916][comp=SAE]: EAP
1110: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.044 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
1111: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.044 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
```

Il tunnel è stato stabilito. NAM richiede e prepara l'identità e le credenziali protette per l'autenticazione interna.

```
1527: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.169 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11916][comp=SAE]: EA
1528: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.169 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11916][comp=SAE]: EA
1573: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.184 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EA
1574: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.184 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EA
1575: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.184 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EA
```

Handshake TLS completato. È stato stabilito un tunnel sicuro per l'autenticazione interna.

```
1616: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.262 +0900: %csc_nam-6-INFO_MSG: %[tid=9664]: Protected iden
1620: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9664]: Auth[EAP-TTLS
1689: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.277 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9664]: Auth[EAP-TTLS
```

L'identità protetta (nome utente) viene inviata e accettata da ISE.

```
1708: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.277 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9456][comp=SAE]: EAP
1738: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.758 +0900: %csc_nam-6-INFO_MSG: %[tid=11768]: Protected pas
1741: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.200 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
```

ISE richiede la password. NAM invia la password protetta all'interno del tunnel TLS.

```
1851: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
1852: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: STA
1853: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
1854: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: STA
1855: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: STA
```

ISE convalida la password, invia EAP-Success e le transizioni NAM a AUTHENTICATED. A questo punto, l'autenticazione dell'utente è completa e al client è consentito l'accesso alla rete.

Risoluzione dei problemi

Per risolvere i problemi di Network Access Manager (NAM) con Cisco ISE e l'integrazione dello switch, è necessario raccogliere i log da tutti e tre i componenti: Secure Client (NAM), Cisco ISE e lo switch.

Registri Secure Client (NAM)

1. Abilitare la registrazione estesa NAM attenendosi alla seguente procedura.
2. Riprodurre il problema. Se il profilo di rete non è applicabile, eseguire Ripristino configurazione di rete in Client protetto.
3. Raccogliere il bundle DART utilizzando lo strumento di diagnostica e reporting (DART).

Registri Cisco ISE

Abilitare questi debug su ISE per acquisire l'autenticazione e le interazioni delle directory:

- runtime-AAA
- nsf
- sessione nsf

Cambia log

Debug di base

```
request platform software trace rotate all
set platform software trace smd switch active R0 radius debug
set platform software trace smd switch active R0 aaa debug
set platform software trace smd switch active R0 dot1x-all debug
set platform software trace smd switch active R0 eap-all debug
debug radius all
```

Debug avanzati (se necessario)

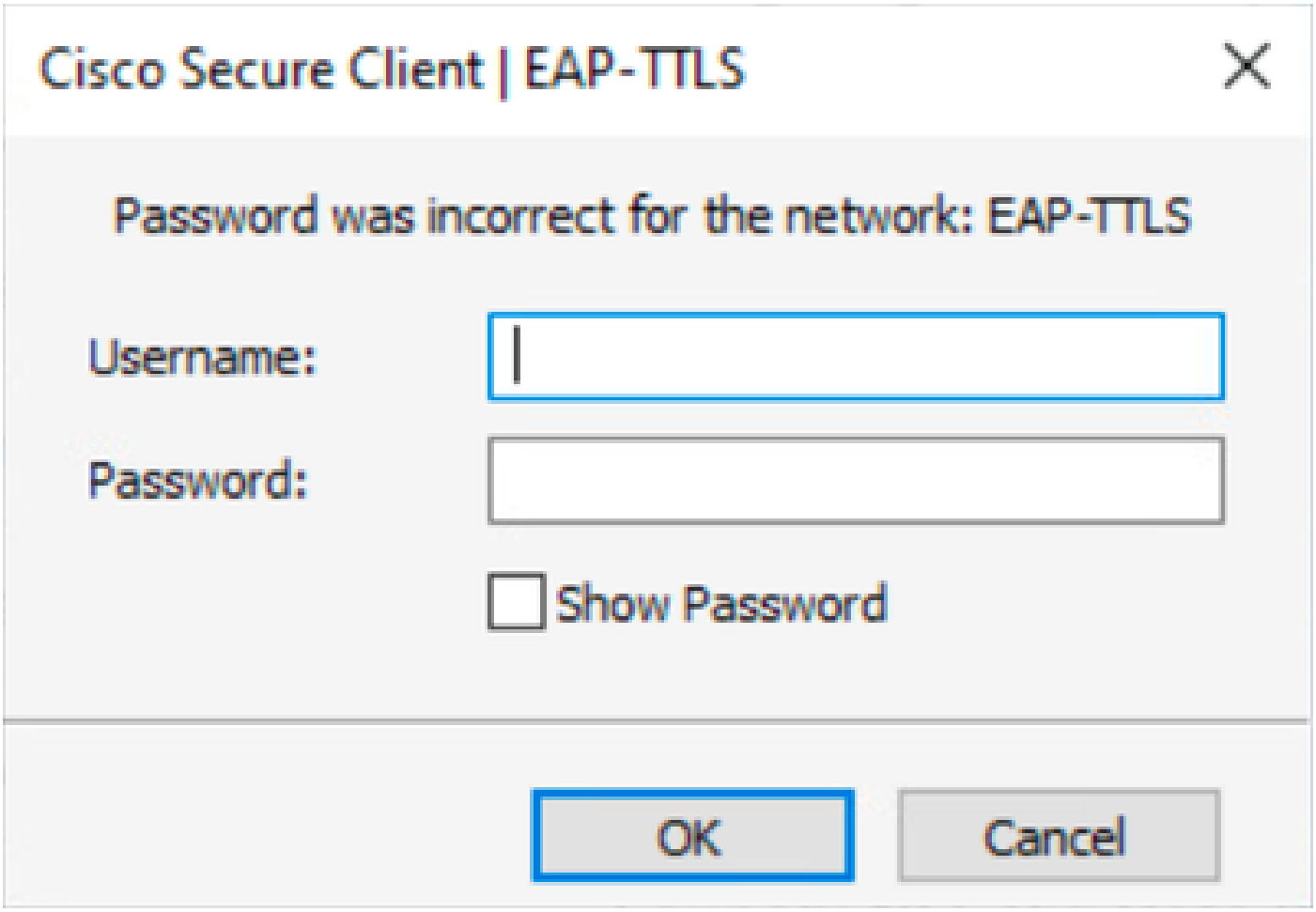
```
set platform software trace smd switch active R0 epm-all debug
set platform software trace smd switch active R0 pre-all debug
```

Comandi show

```
show version
show debugging
show running-config aaa
show authentication session interface gix/x details
show dot1x interface gix/x
show aaa servers
show platform software trace message smd switch active R0
```

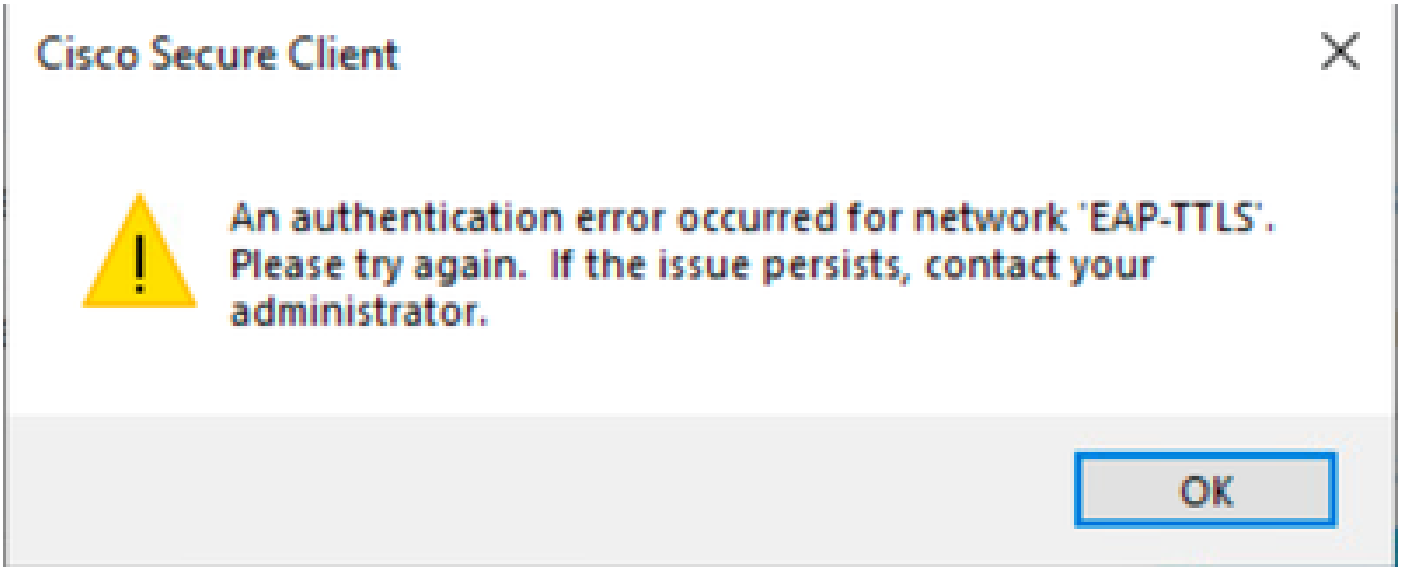
Errore di autenticazione utente a causa di credenziali non valide

Quando un utente immette credenziali non corrette, Secure Client visualizza una password generica non corretta per la rete: Messaggio EAP-TTLS. L'errore visualizzato sullo schermo non specifica se il problema è dovuto a un nome utente o a una password non validi.



Errore di password non corretta

Se l'autenticazione non riesce due volte consecutivamente, Secure Client visualizza questo messaggio: Si è verificato un errore di autenticazione per la rete 'EAP-TTLS'. Riprova. Se il problema persiste, contattare l'amministratore.



Problema di autenticazione utente

Per identificare la causa, esaminare i registri NAM.

1. Password non corretta:

Quando un utente immette una password non corretta, nei log NAM vengono visualizzate voci simili a questo output:

```
3775: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.921 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
3776: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.921 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
3777: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.922 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
```

Nei log live di Cisco ISE, l'evento corrispondente viene visualizzato come:

Event	5400 Authentication failed
Failure Reason	24408 User authentication against Active Directory failed since user has entered the wrong password
Resolution	Check the user password credentials. If the RADIUS request is using PAP for authentication, also check the Shared Secret configured for the Network Device
Root cause	User authentication against Active Directory failed since user has entered the wrong password

Password non corretta

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ... 11507 Extracted EAP-Response/Identity 10 **12983 Prepared EAP-Request proposing EAP-TTLS with challenge** ... ... **12978 Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated** 12800 Extracted first TLS record; TLS handshake started ... ... 12810 Prepared TLS ServerDone message ... ... 12812 Extracted TLS ClientKeyExchange message 12803 Extracted TLS ChangeCipherSpec message ... ... **12816 TLS handshake succeeded** ... ... **11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge 0** 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 Returned RADIUS Access-Challenge 0 11001 Received RADIUS Access-Request ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response 0 **11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated** ... ... 15013 Selected Identity Source - varshaah-ad 0 24430 Authenticating user against Active Directory - varshaah-ad 0 24325 Resolving identity - labuser@varshaah.local 4 24313 Search for matching accounts at join point - varshaah.local 0 24319 Single matching account found in forest - varshaah.local 0 24323 Identity resolution detected single matching account 0 **24344 RPC Logon request failed - STATUS_WRONG_PASSWORD, ERROR_INVALID_PASSWORD, labuser@varshaah.local 20 24408 User authentication against Active Directory failed since user has entered the wrong password - varshaah-ad 1** ... ... 11823 EAP-MSCHAP authentication attempt failed ... ... 11815 Inner EAP-MSCHAP authentication failed 0 ... ... 12976 EAP-TTLS authentication failed 0 ... ... 11003 Returned RADIUS Access-Reject

2. Nome utente errato:

Quando un utente immette un nome utente non corretto, nei log NAM vengono visualizzate voci simili a questo output:

```
3788: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.923 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
3789: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.923 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300]: EAP-CB: EAP
```

Nei log live di Cisco ISE, l'evento corrispondente viene visualizzato come:

Event	5400 Authentication failed
Failure Reason	22056 Subject not found in the applicable identity store(s)
Resolution	Check whether the subject is present in any one of the chosen identity stores. Note that some identity stores may have been skipped due to identity resoultion settings or if they do not support the current authentication protocol.
Root cause	Subject not found in the applicable identity store(s).

Nome utente non corretto

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ... 11507 Extracted EAP-Response/Identity **12983 Prepared EAP-Request proposing EAP-TTLS with challenge** ... ... **12978 Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated** 12800 Extracted first TLS record; TLS handshake started ... ... 12810 Prepared TLS ServerDone message ... ... 12812 Extracted TLS ClientKeyExchange message 12803 Extracted TLS ChangeCipherSpec message ... ... **12816 TLS handshake succeeded** ... ... **11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge** 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response **11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated** ... ... 15013 Selected Identity Source - All_AD_Join_Points 24430 Authenticating user against Active Directory - varshaah-ad 24325 Resolving identity - user@varshaah.local 24313 Search for matching accounts at join point - varshaah.local ... ... 24352 Identity resolution failed - ERROR_NO_SUCH_USER **24412 User not found in Active Directory - varshaah-ad** ... ... 15013 Selected Identity Source - Internal Users 24210 Looking up User in Internal Users IDStore - user **24216 The user is not found in the internal users identity store** ... ... 22056 Subject not found in the applicable identity store(s) 22058 The advanced option that is configured for an unknown user is used 22061 The 'Reject' advanced option is configured in case of a failed authentication request **11823 EAP-MSCHAP authentication attempt failed** ... ... **11815 Inner EAP-MSCHAP authentication failed** ... ... 12976 EAP-TTLS authentication failed 0 ... ... 11504 Prepared EAP-Failure 1 **11003 Returned RADIUS Access-Reject**

Difetti noti

ID bug	Descrizione
Cisco bug ID 63395	ISE 3.0: impossibile individuare l'archivio ID REST dopo il riavvio dei servizi

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).