Configurazione di Secure Client NAM per Dot1x con Windows e ISE 3.2

Sommario

Introduzione

In questo documento viene descritto come configurare Secure Client Network Analysis Module (NAM) su Windows.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza di base di un supplicant RADIUS
- Punto1x
- PEAP
- PKI

Componenti usati

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

- Windows 10 Pro versione 22H2 19045.3930
- ISE 3.2
- Software Cisco IOS® XE C117, versione 17.12.02
- Active Directory 2016

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

In questo documento viene descritto come configurare Secure Client NAM su Windows. Vengono utilizzati l'opzione di predistribuzione e l'Editor di profili per eseguire l'autenticazione dot1x. Vengono inoltre forniti alcuni esempi di come questo obiettivo viene raggiunto.

In rete, un supplicant è un'entità a un'estremità di un segmento LAN point-to-point che cerca di essere autenticato da un autenticatore collegato all'altra estremità del collegamento. Lo standard IEEE 802.1X utilizza il termine supplicant per riferirsi sia all'hardware che al software. In pratica, un richiedente è un'applicazione software installata su un computer dell'utente finale. L'utente richiama il supplicant e invia le credenziali per connettere il computer a una rete protetta. Se l'autenticazione ha esito positivo, in genere l'autenticatore consente al computer di connettersi alla rete.

Informazioni su Network Access Manager

Network Access Manager è un software client che fornisce una rete di layer 2 protetta in conformità alle relative policy. Rileva e seleziona la rete di accesso di livello 2 ottimale ed esegue l'autenticazione dei dispositivi per l'accesso alle reti cablate e wireless. Network Access Manager gestisce l'identità di utenti e dispositivi e i protocolli di accesso alla rete necessari per l'accesso protetto. Funziona in modo intelligente per impedire agli utenti finali di stabilire connessioni che violano le policy definite dagli amministratori.

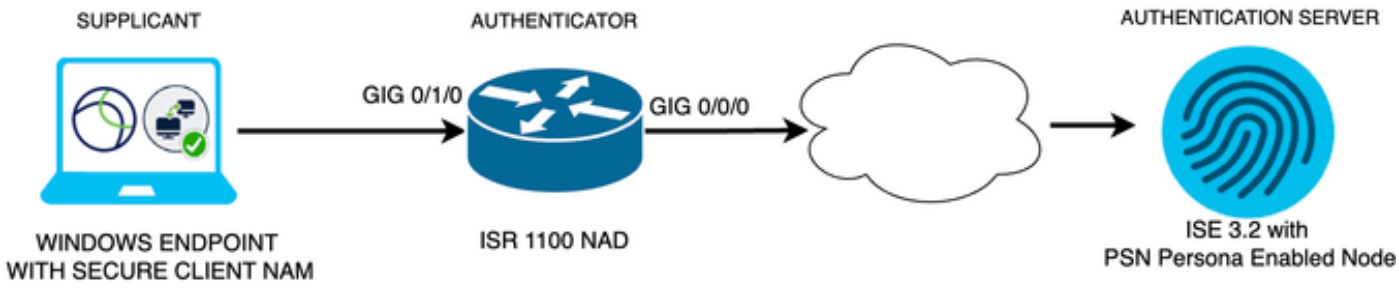
Network Access Manager è stato progettato per essere installato in un'unica postazione, in modo da consentire una sola connessione di rete alla volta. Inoltre, le connessioni cablate hanno una priorità più alta rispetto alle connessioni wireless, quindi se si è collegati alla rete con una connessione cablata, la scheda di rete wireless viene disabilitata senza indirizzo IP.

Configurazione

Esempio di rete

È fondamentale comprendere che per le autenticazioni dot1x sono necessarie 3 parti: il supplicant che può fare dot1x, l'autenticatore noto anche come NAS/NAD che funge da proxy incapsulando il traffico dot1x all'interno di RADIUS e il server di autenticazione.

In questo esempio, il supplicant viene installato e configurato in modi diversi. Successivamente, verrà visualizzato uno scenario con la configurazione del dispositivo di rete e il server di autenticazione.



Esempio di rete

Configurazioni

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

2. Scaricare e installare l'editor di profili Secure Client NAM.
3. Configurazioni generali predefinite
4. Scenario 1: configurare il richiedente Secure Client NAM per l'autenticazione utente PEAP (MS-CHAPv2).
5. Scenario 2: configurare il richiedente Secure Client NAM per EAP-FAST simultaneamente alla configurazione dell'autenticazione di computer e utente.
6. Scenario 3 parte 1: configurare il richiedente Secure Client NAM per EAP-TLS.
7. Scenario 3 parte 2: configurare la dimostrazione di NAD e ISE.

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

Download del software Cisco

Nella barra di ricerca del nome del prodotto, digitare Secure Client 5.

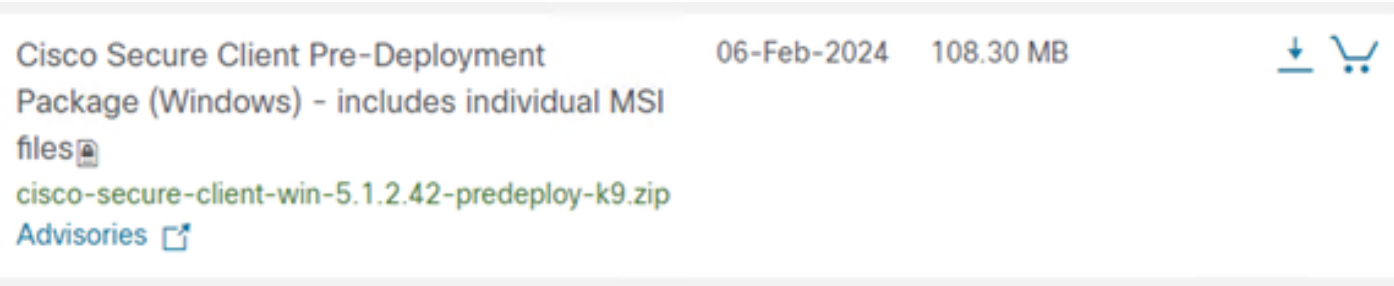
Download Home > Sicurezza > Client VPN e per la sicurezza degli endpoint > Client sicuro (AnyConnect inclusa) > Secure Client 5 > Software client VPN AnyConnect.

Nell'esempio di configurazione, viene utilizzata la versione 5.1.2.42.

Esistono diversi modi per distribuire Secure Client ai dispositivi Windows: da SCCM, dal motore

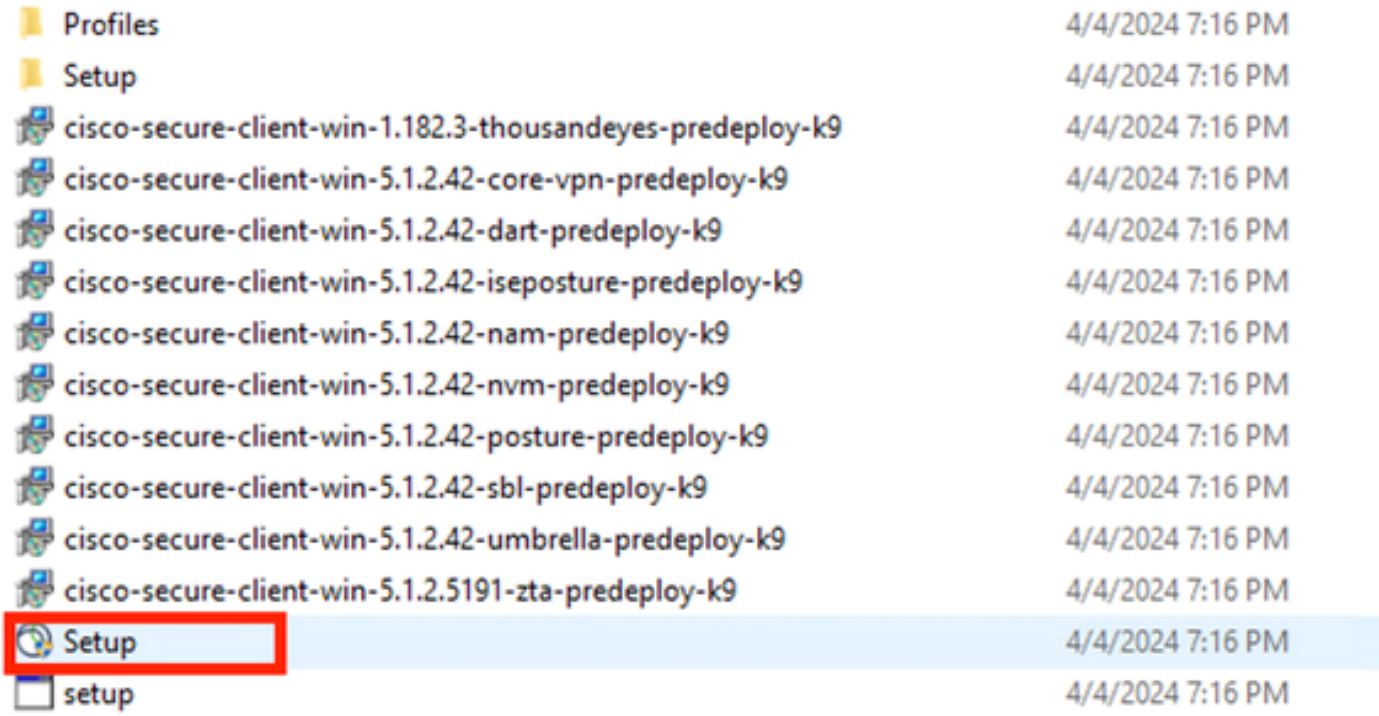
dei servizi di identità e dall'headend VPN. Tuttavia, in questo articolo, il metodo di installazione utilizzato è il metodo pre-distribuzione.

Nella pagina cercare il file Cisco Secure Client Headend Deployment Package (Windows).



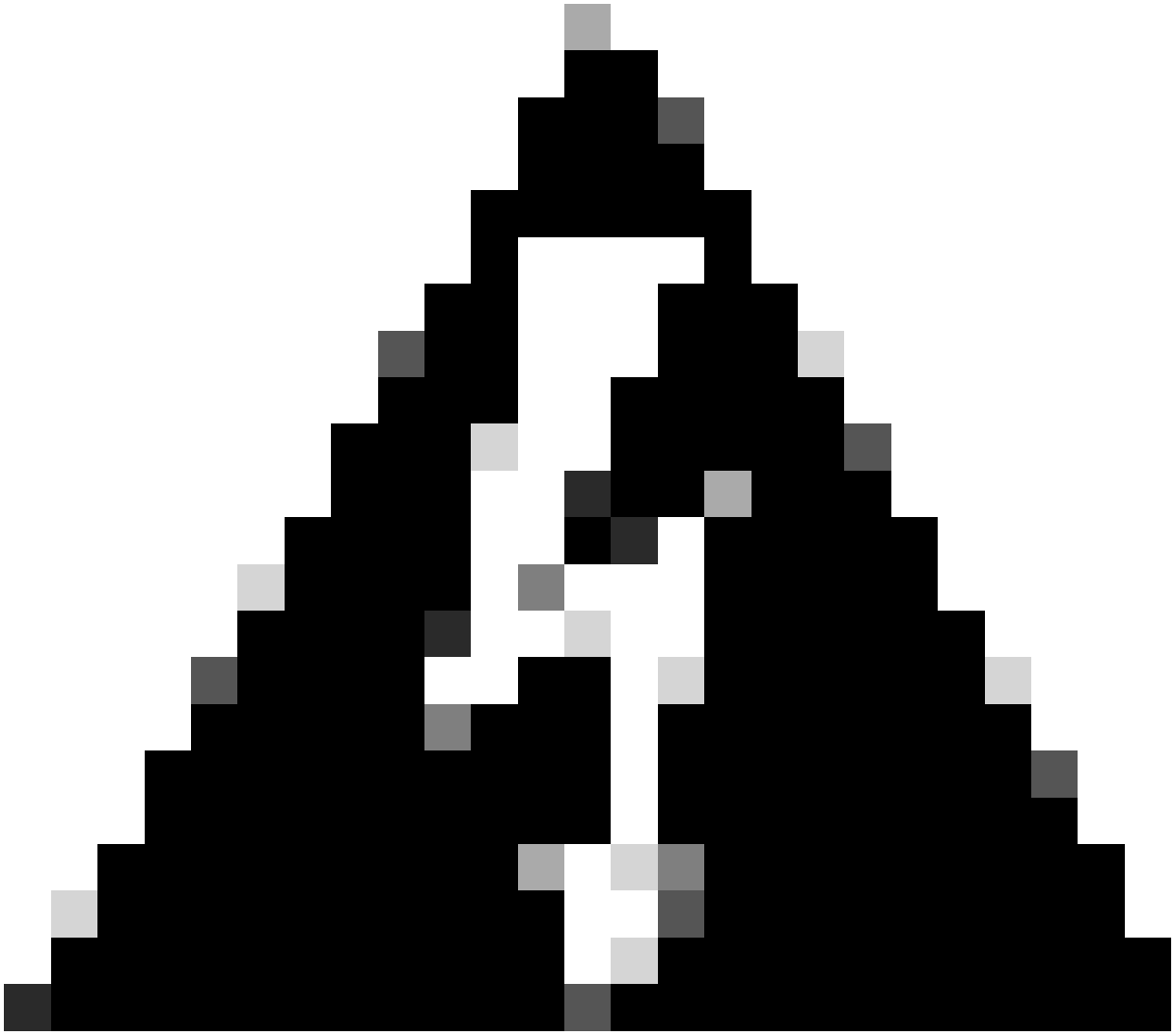
File zip Msi

Una volta scaricati ed estratti, fare clic su Setup (Imposta).

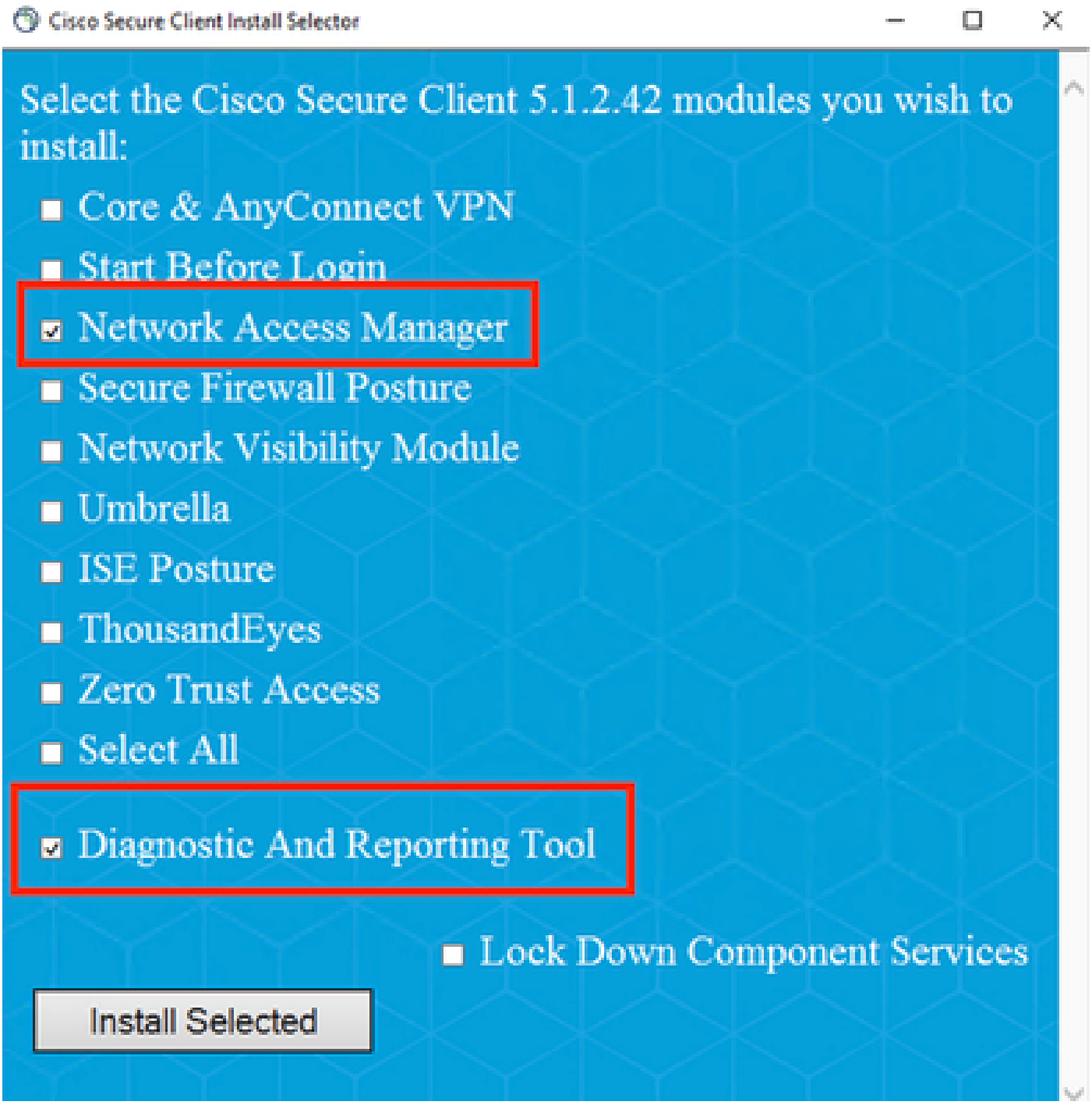


Protezione dei file client

Installare i moduli Network Access Manager e Diagnostics and Reporting Tool.



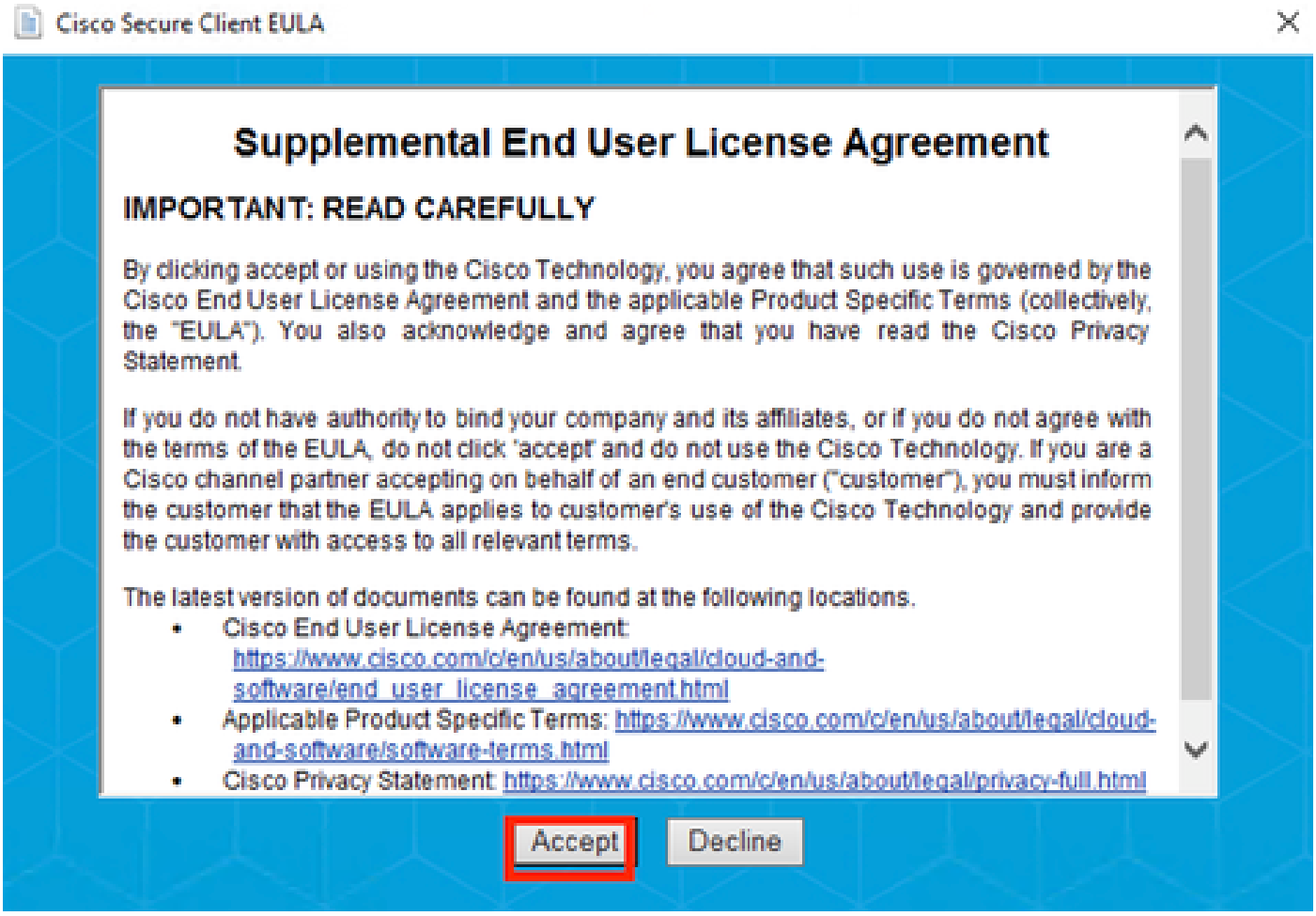
Avviso: se si utilizza la procedura guidata Cisco Secure Client, il modulo VPN viene installato automaticamente e nascosto nell'interfaccia utente. NAM non funziona se il modulo VPN non è installato. Se si utilizzano singoli file MSI o un metodo di installazione diverso, assicurarsi di installare il modulo VPN.



Selettore di installazione

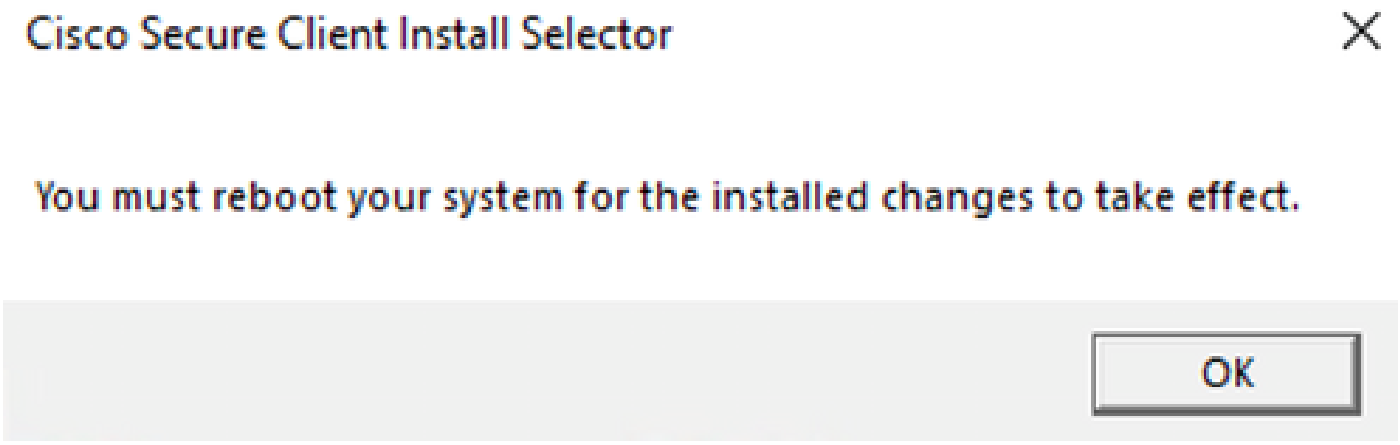
Fare clic su Install Selected (Installa selezionati).

Accettare il Contratto.



Finestra EULA

Dopo l'installazione di NAM è necessario riavviare il sistema.



Finestra Requisiti per il riavvio

Una volta installato, può essere individuato e aperto dalla barra di ricerca di Windows.

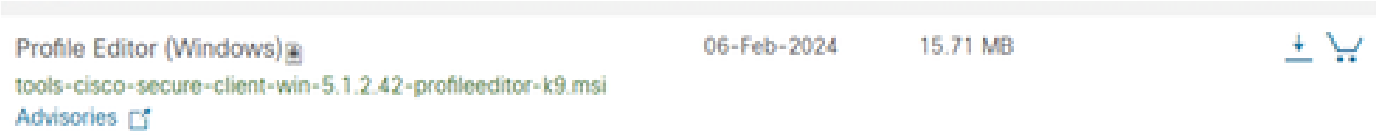
Programma Secure Client

2. Scaricare e installare Secure Client NAM Profile Editor.

Per configurare le preferenze Dot1x, è necessario Cisco Network Access Manager Profile Editor.

Dalla stessa pagina in cui è stato scaricato Secure Client, è disponibile l'opzione Editor di profili.

In questo esempio viene utilizzata l'opzione con la versione 5.1.2.42.



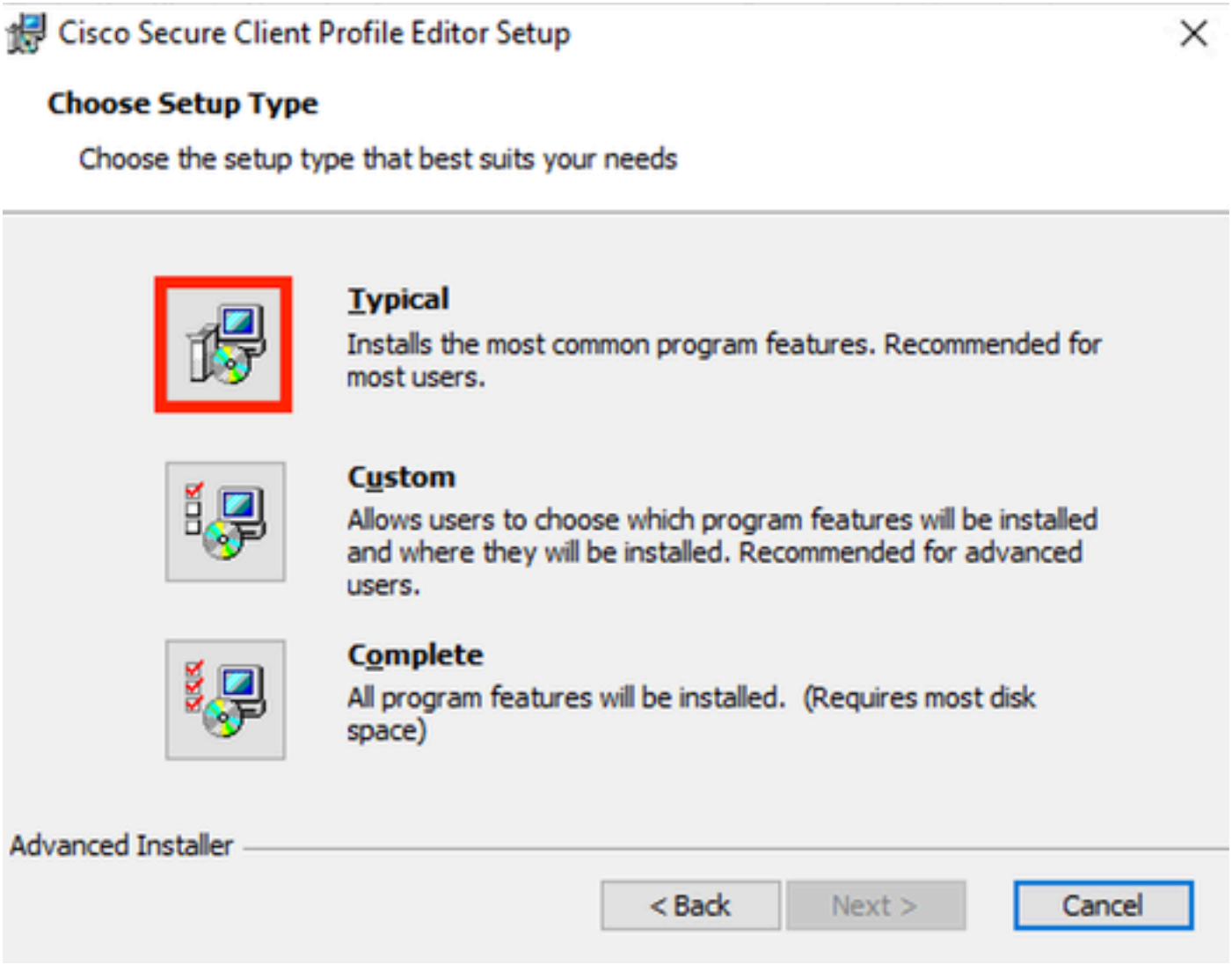
Editor di profili

Una volta scaricato, procedere con l'installazione.

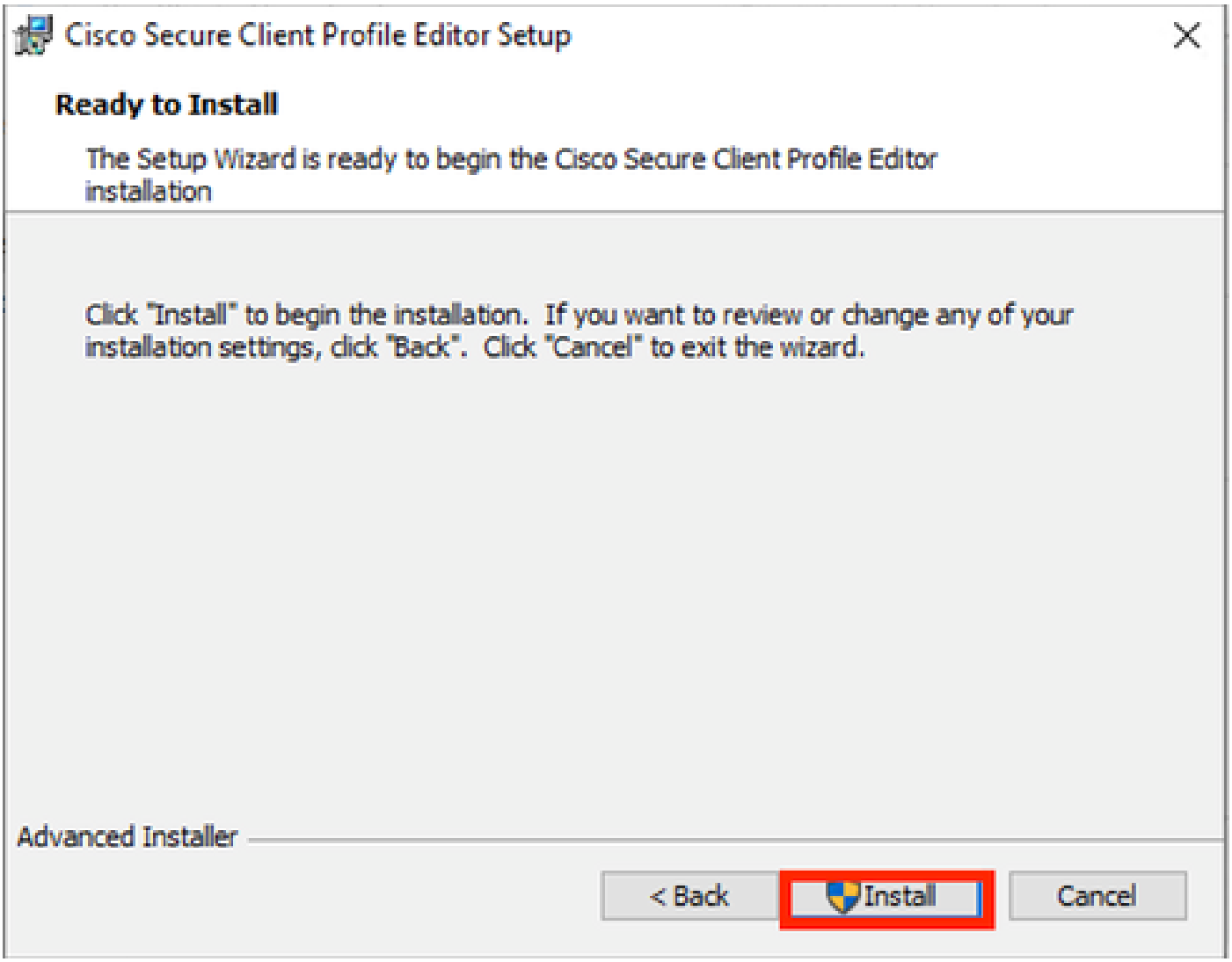
Eseguire il file msi.

Finestra di impostazione dell'Editor di profili

Utilizzare l'opzione di impostazione Tipica.

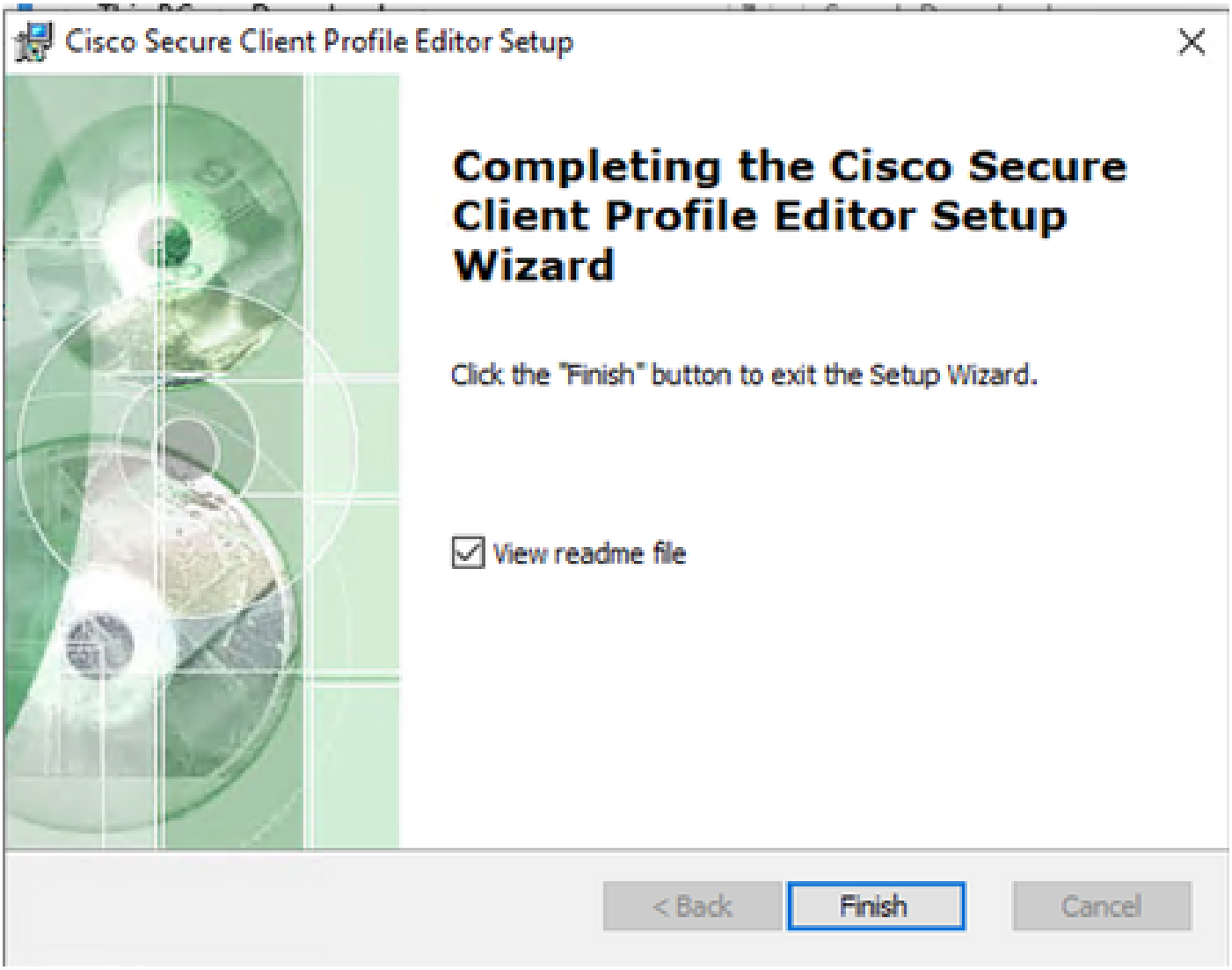


Installazione dell'Editor di profili



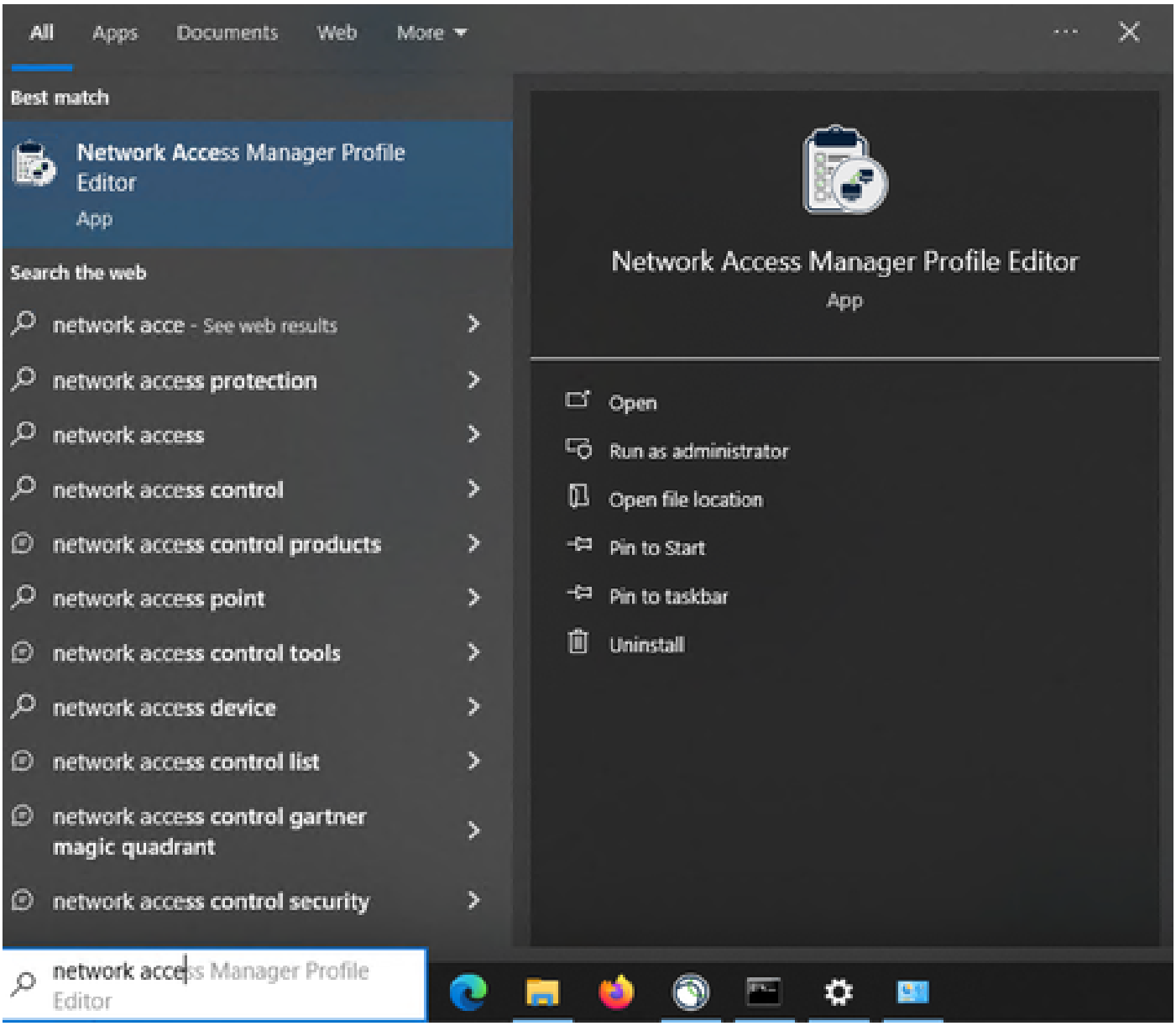
Finestra di installazione

Fare clic su Finish (Fine).



Fine installazione editor di profili

Una volta installato, aprire Editor profili di Network Access Manager dalla barra di ricerca.



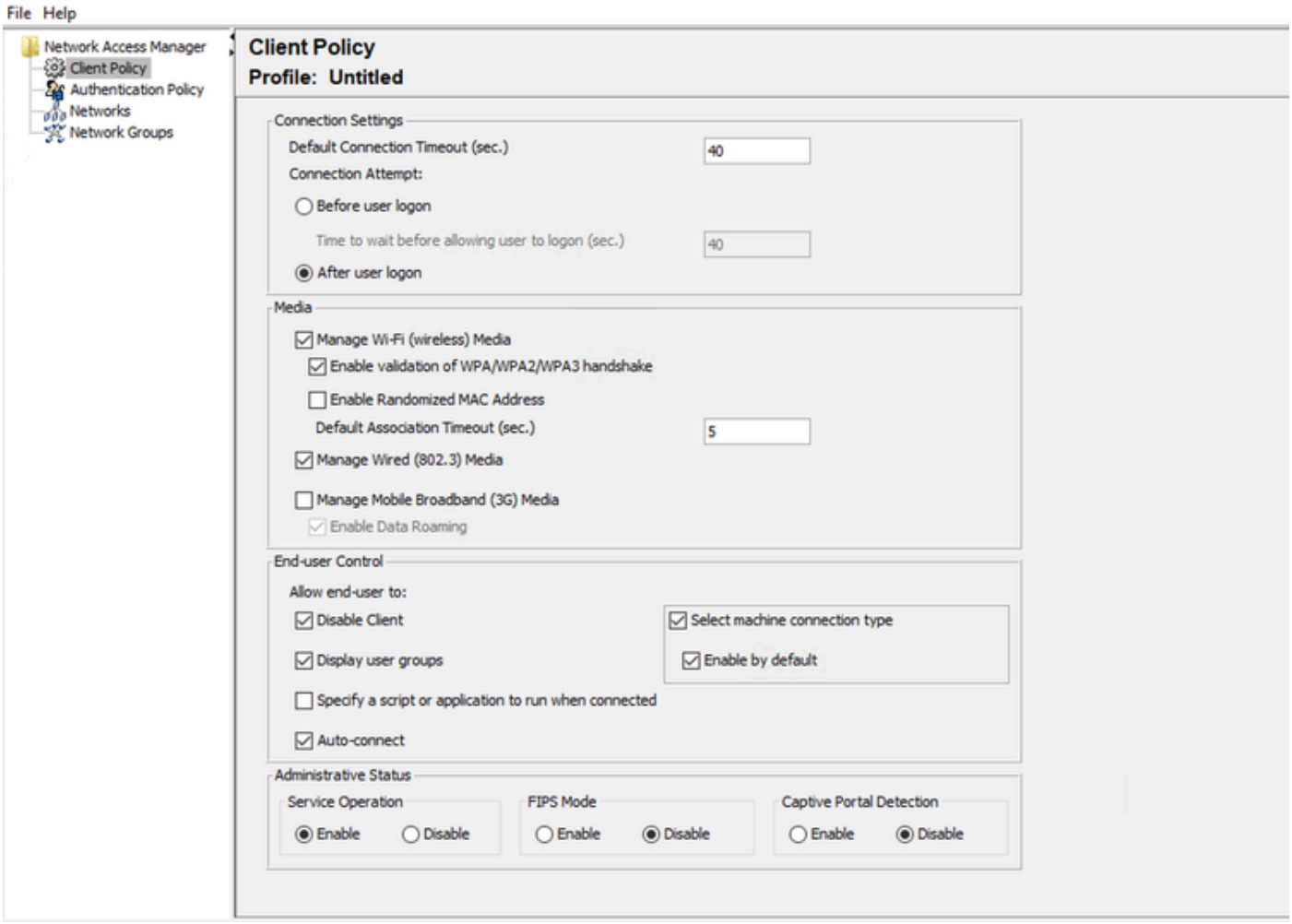
Editor di profili per NAM sulla barra di ricerca

Installazione di Network Access Manager e dell'Editor di profili completata.

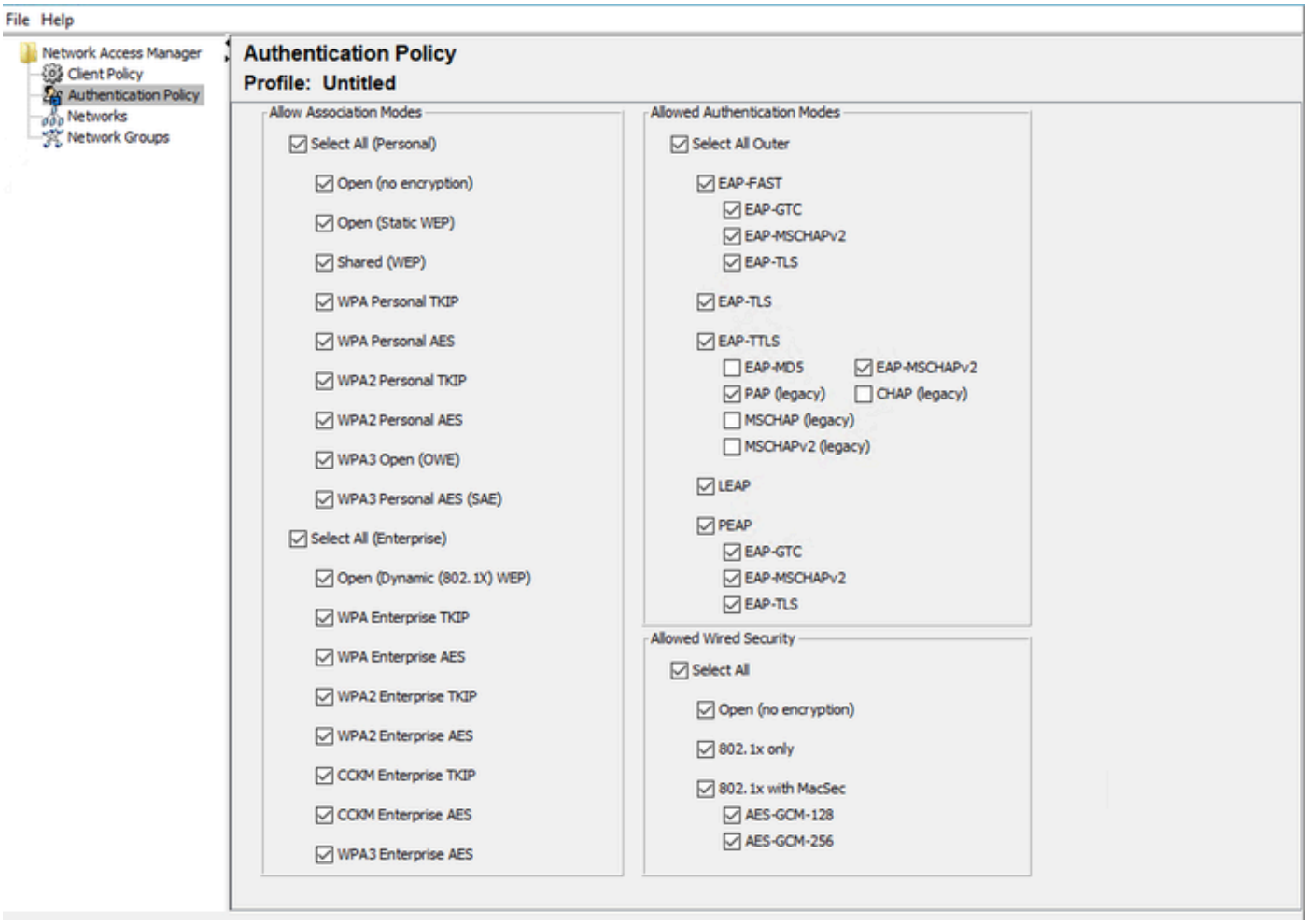
3. Configurazioni generali predefinite

Tutti gli scenari presentati in questo articolo contengono configurazioni per:

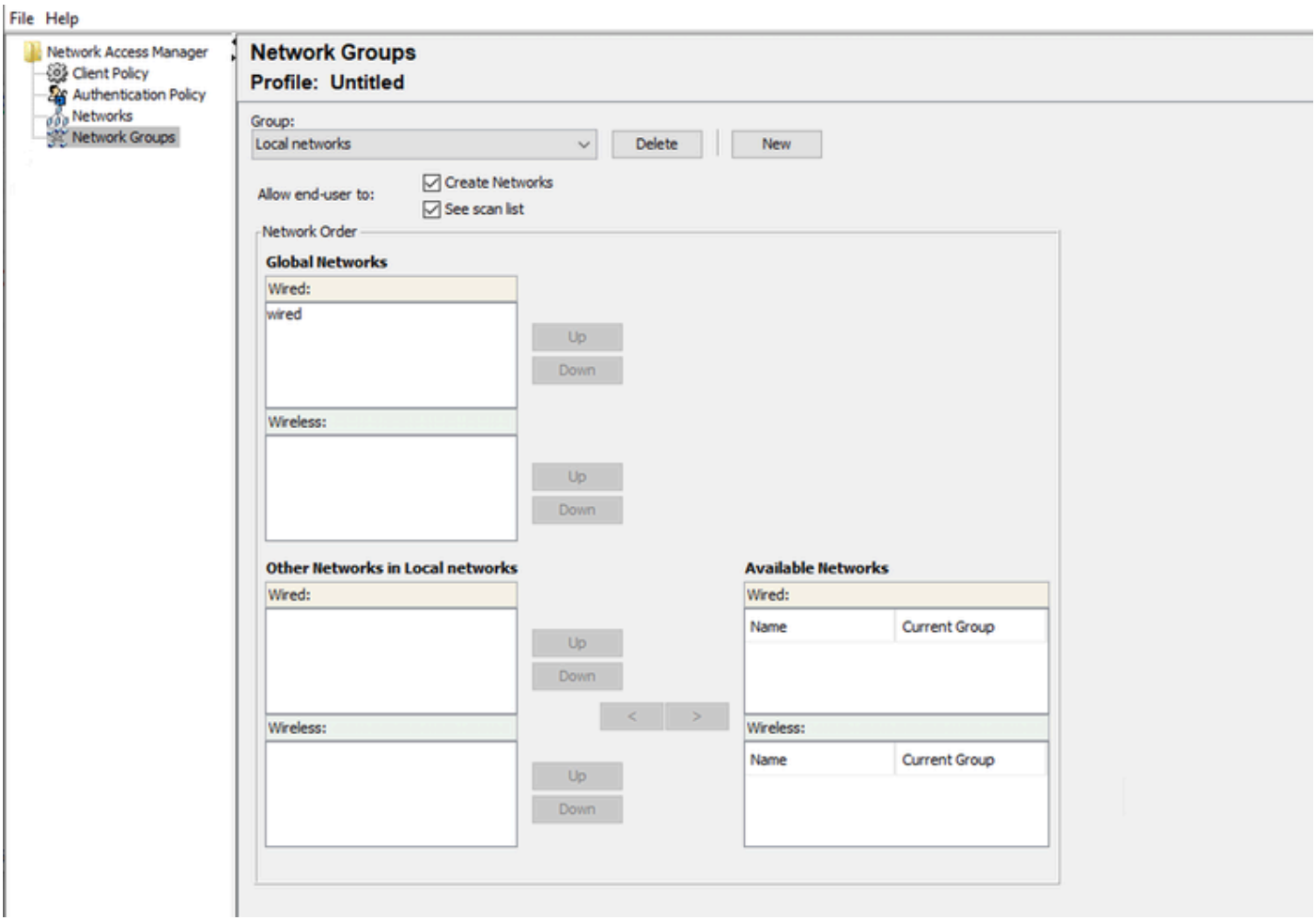
- Criterio client
- Criterio di autenticazione
- Gruppi di rete



Criterio client Editor profili NAM



Criterio di autenticazione dell'Editor di profili NAM



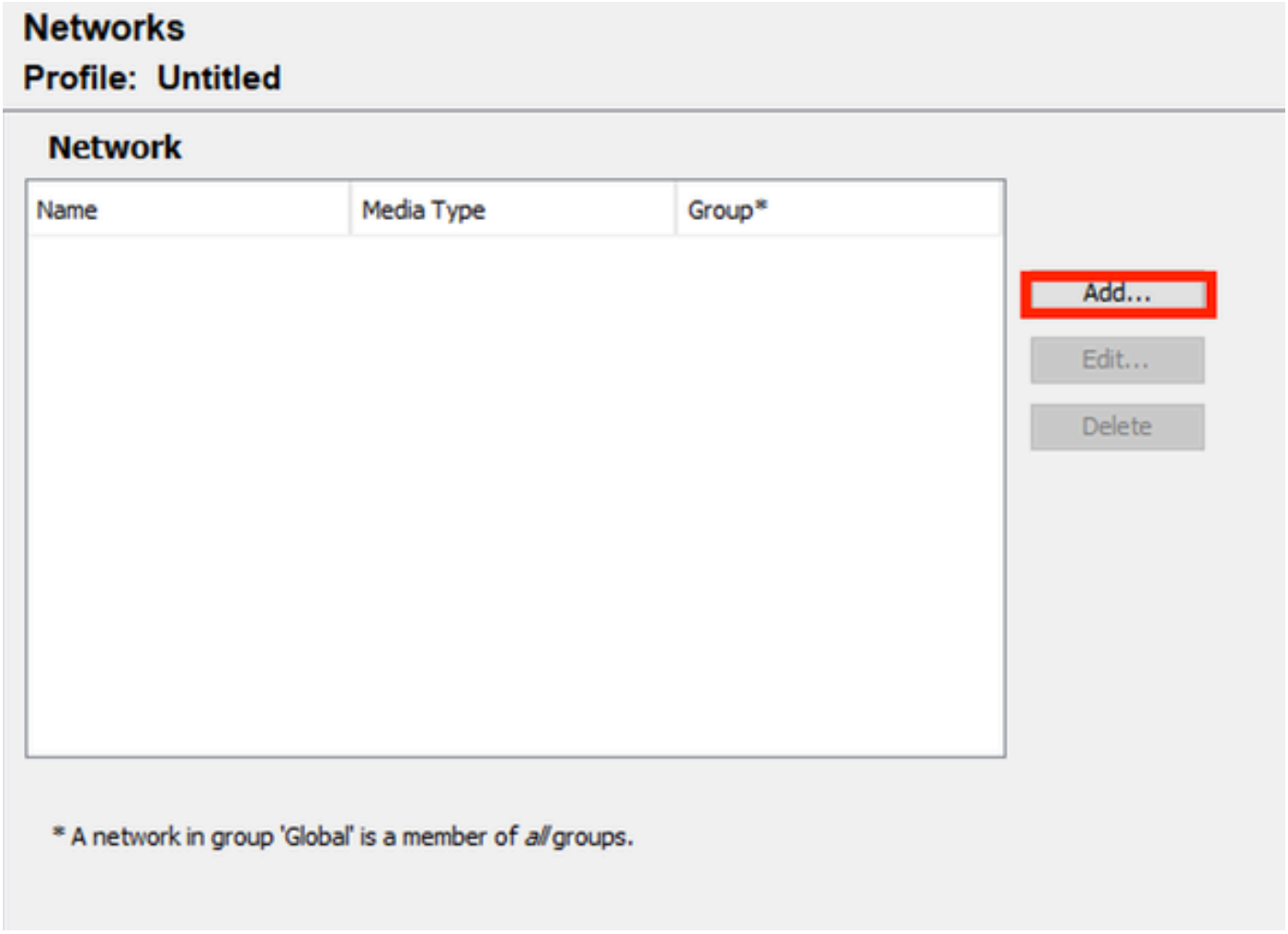
Scheda Gruppi di rete

4. Scenario 1: configurazione del richiedente Secure Client NAM per l'autenticazione utente PEAP (MS-CHAPv2)

Passare alla sezione Reti.

È possibile eliminare il profilo di rete predefinito.

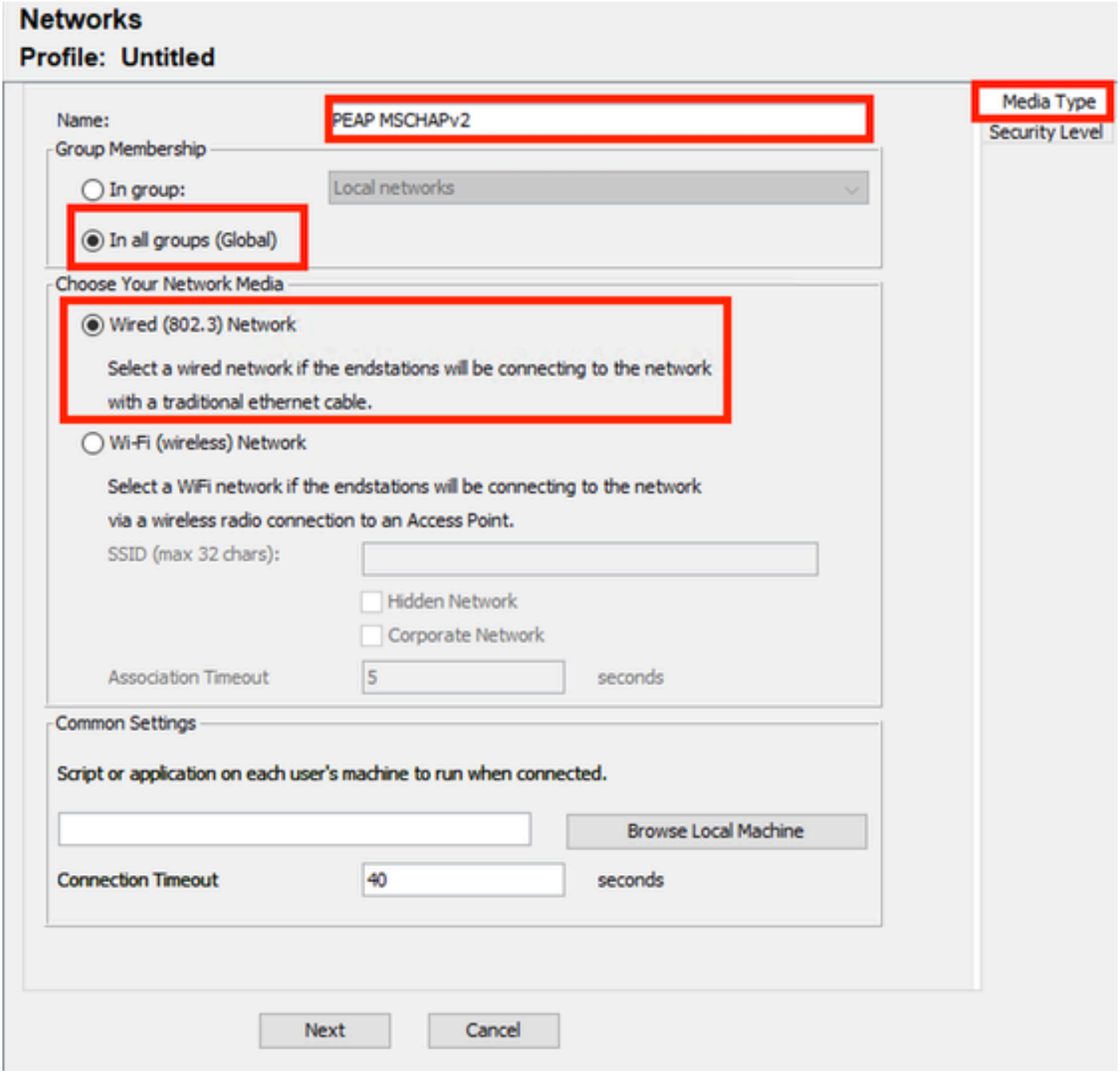
Fare clic su Add.



Creazione profilo di rete

Assegnare un nome al profilo di rete.

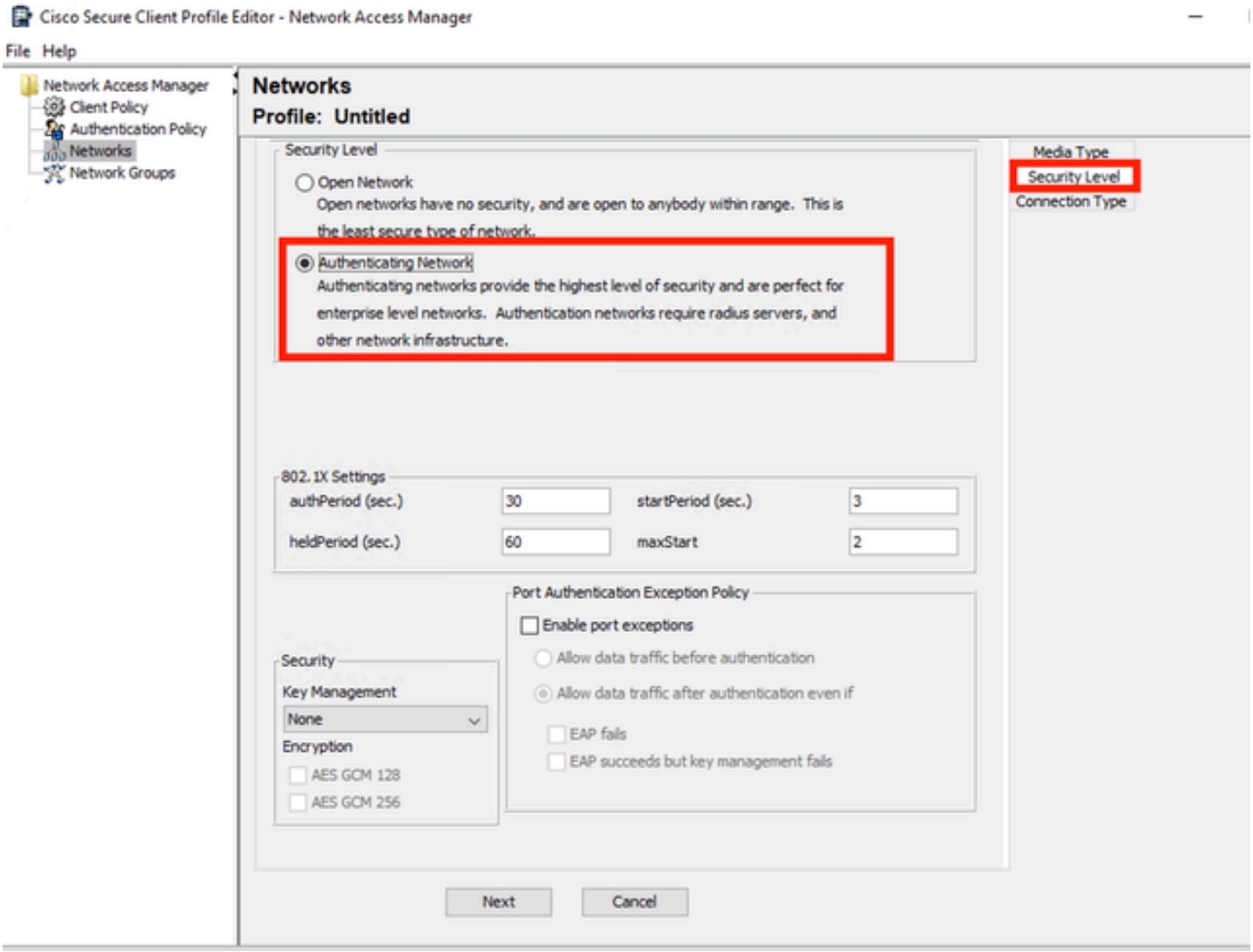
Selezionare Globale per l'appartenenza al gruppo. Selezionare Supporto di rete cablata.



Sezione Tipo di supporto del profilo di rete

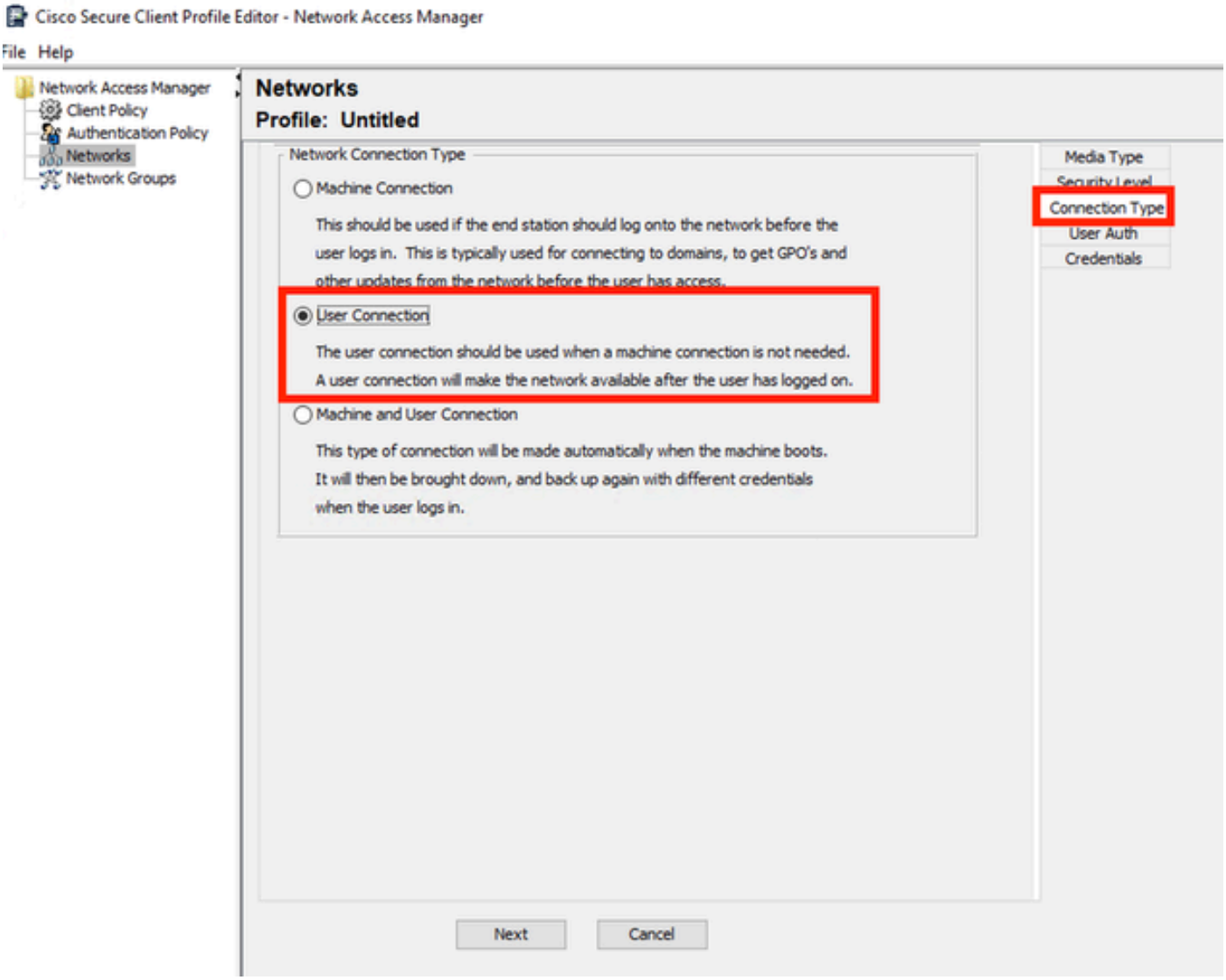
Fare clic su Next (Avanti).

Selezionare Autenticazione rete e utilizzare l'impostazione predefinita per le altre opzioni della sezione Livello di protezione.



Livello di protezione profilo di rete

Fare clic su Avanti per continuare con la sezione Tipo di connessione.

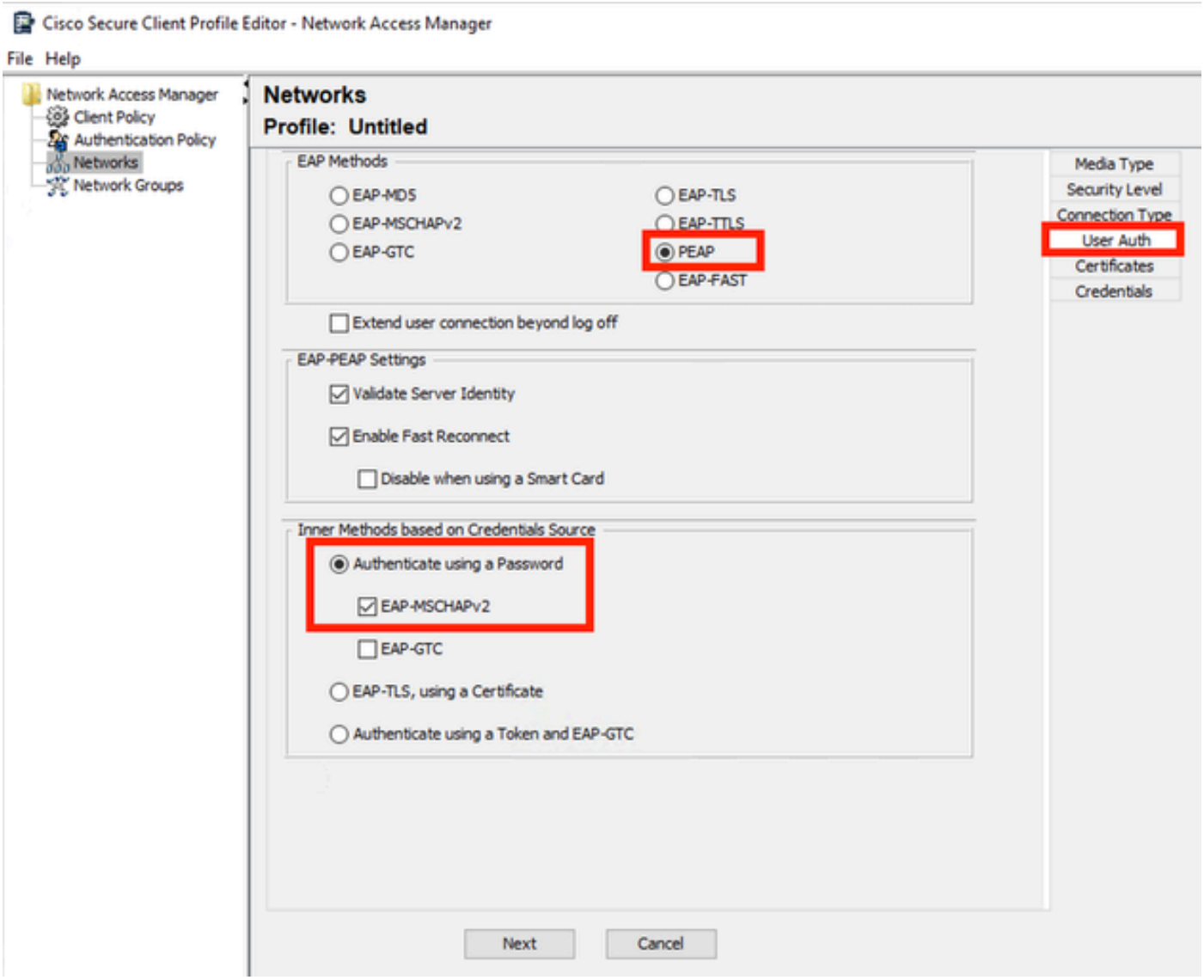


Tipo di connessione profilo di rete

Selezionare il tipo di connessione Connessione utente.

Fare clic su Avanti per continuare con la sezione Autenticazione utente, che è ora disponibile.

Selezionare PEAP come metodo EAP generale.



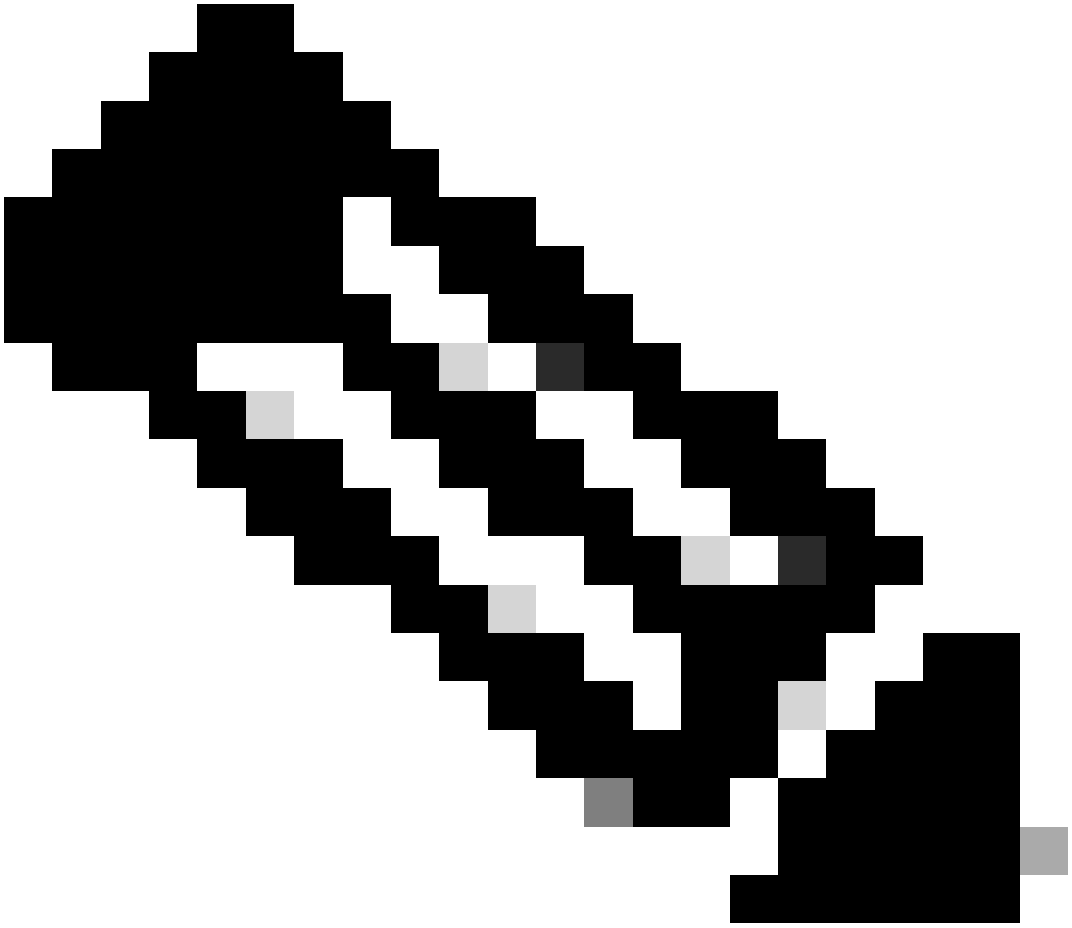
Autenticazione utente profilo di rete

Non modificare i valori predefiniti in Impostazioni EAP-PEAP.

Continuare con la sezione Metodi interni basati sull'origine credenziali.

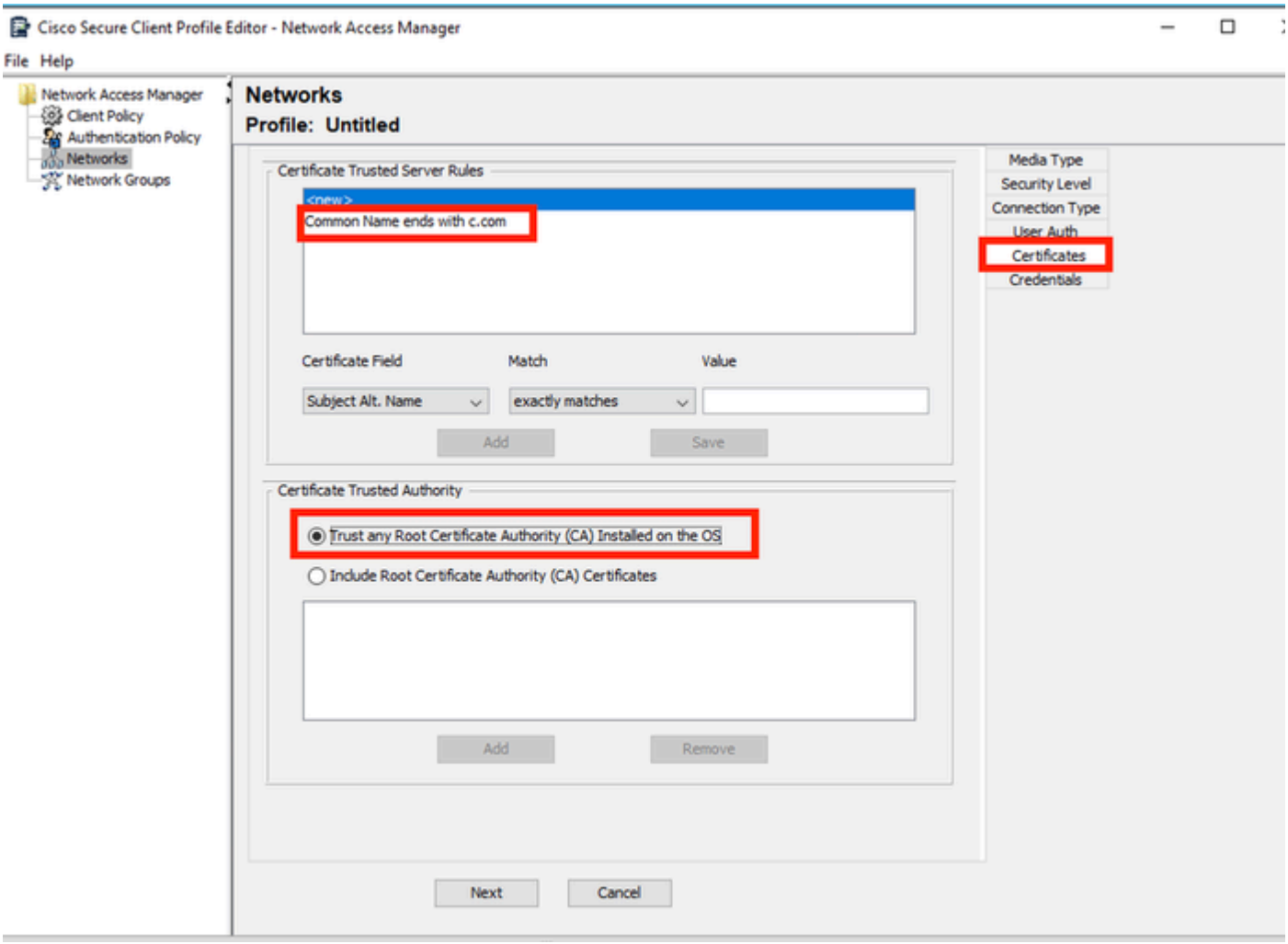
Tra i vari metodi interni esistenti per EAP PEAP, selezionare Autentica tramite password e selezionare EAP-MSCHAPv2.

Fare clic su Avanti per passare alla sezione Certificato.



Nota: la sezione Certificato viene visualizzata perché l'opzione Convalida identità server in Impostazioni EAP-PEAP è selezionata. Per EAP PEAP, esegue l'incapsulamento utilizzando il certificato del server.

Nella sezione Certificati, in Regole server trusted per certificati, la regola Nome comune termina con c.com. Questa sezione della configurazione fa riferimento al certificato utilizzato dal server durante il flusso PEAP EAP. Se nell'ambiente viene utilizzato Identity Service Engine (ISE), è possibile utilizzare il nome comune del certificato EAP del nodo di Policy Server.

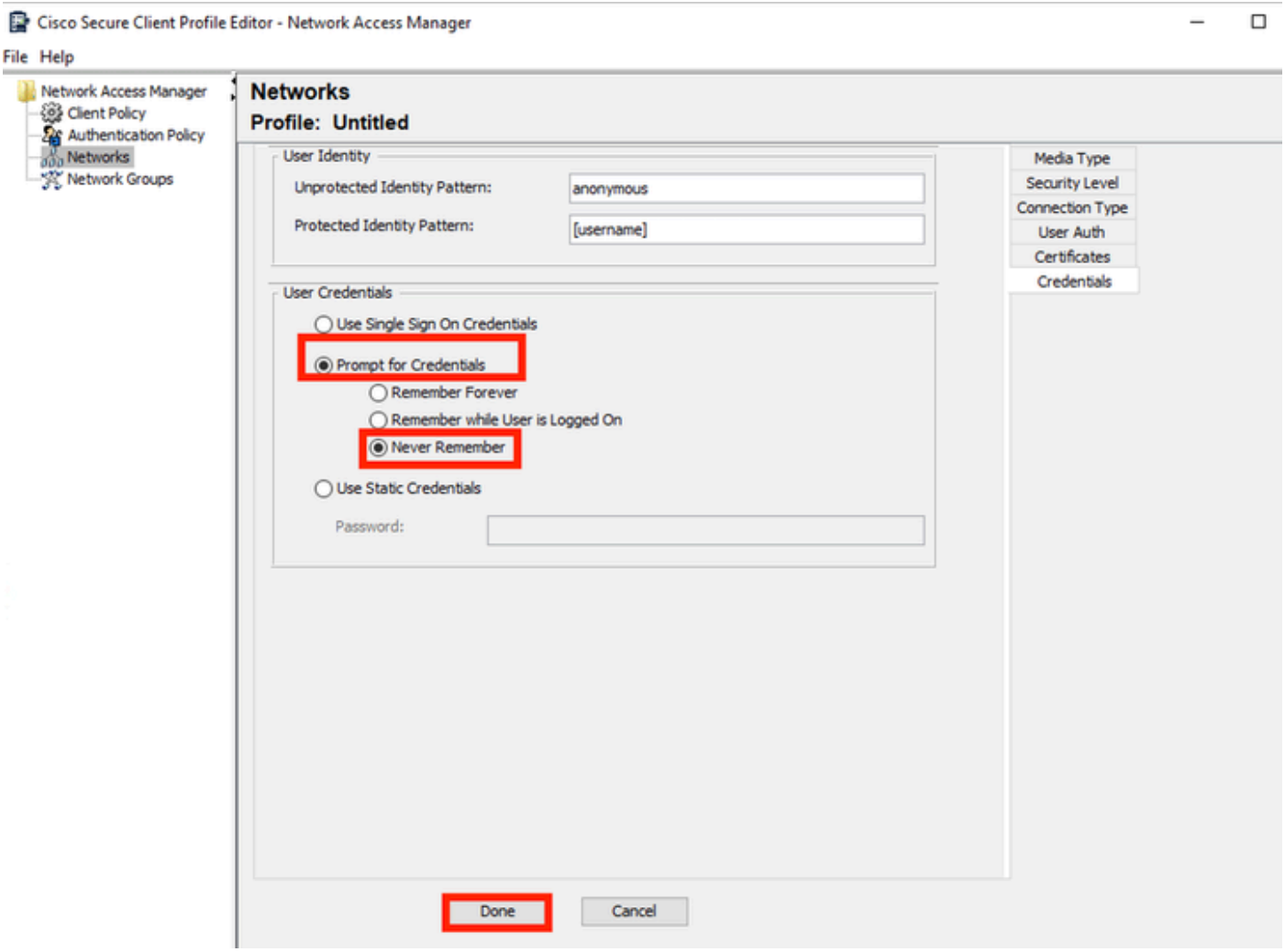


Sezione Certificato profilo di rete

In Autorità di certificazione attendibile è possibile selezionare due opzioni. Per questo scenario, anziché aggiungere un certificato CA specifico che firmi il certificato RADIUS EAP, viene utilizzata l'opzione Considera attendibile qualsiasi autorità di certificazione (CA) radice installata nel sistema operativo.

Con questa opzione il dispositivo Windows considera attendibile qualsiasi certificato EAP firmato da un certificato incluso nel programma Certificati del programma Gestione certificati utente — Utente corrente > Autorità di certificazione radice attendibili > Certificati.

Fare clic su Next (Avanti).



Sezione Credenziali profilo di rete

Nella sezione Credenziali viene modificata solo la sezione Credenziali utente.

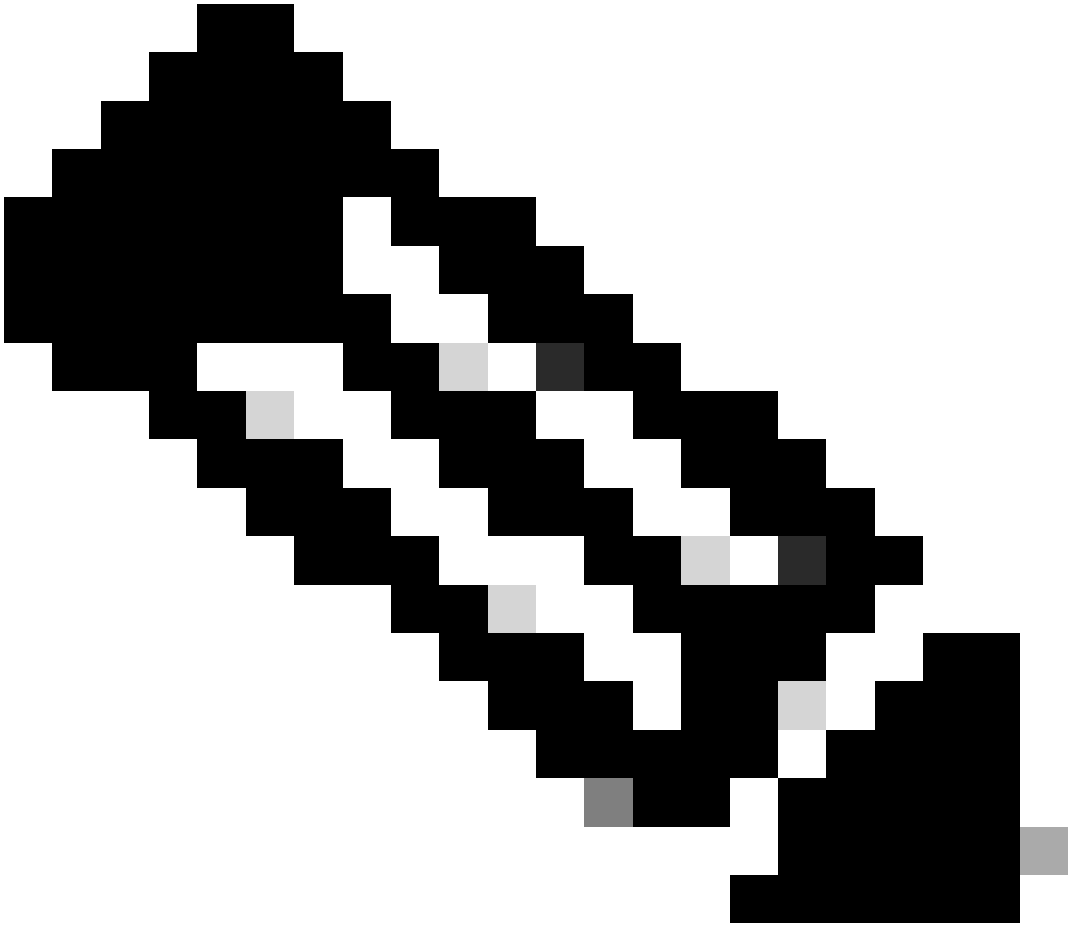
L'opzione Richiedi credenziali > Non ricordare mai è selezionata, quindi in ogni autenticazione l'utente che effettua l'autenticazione deve immettere le proprie credenziali.

Selezionate Fatto (Done).

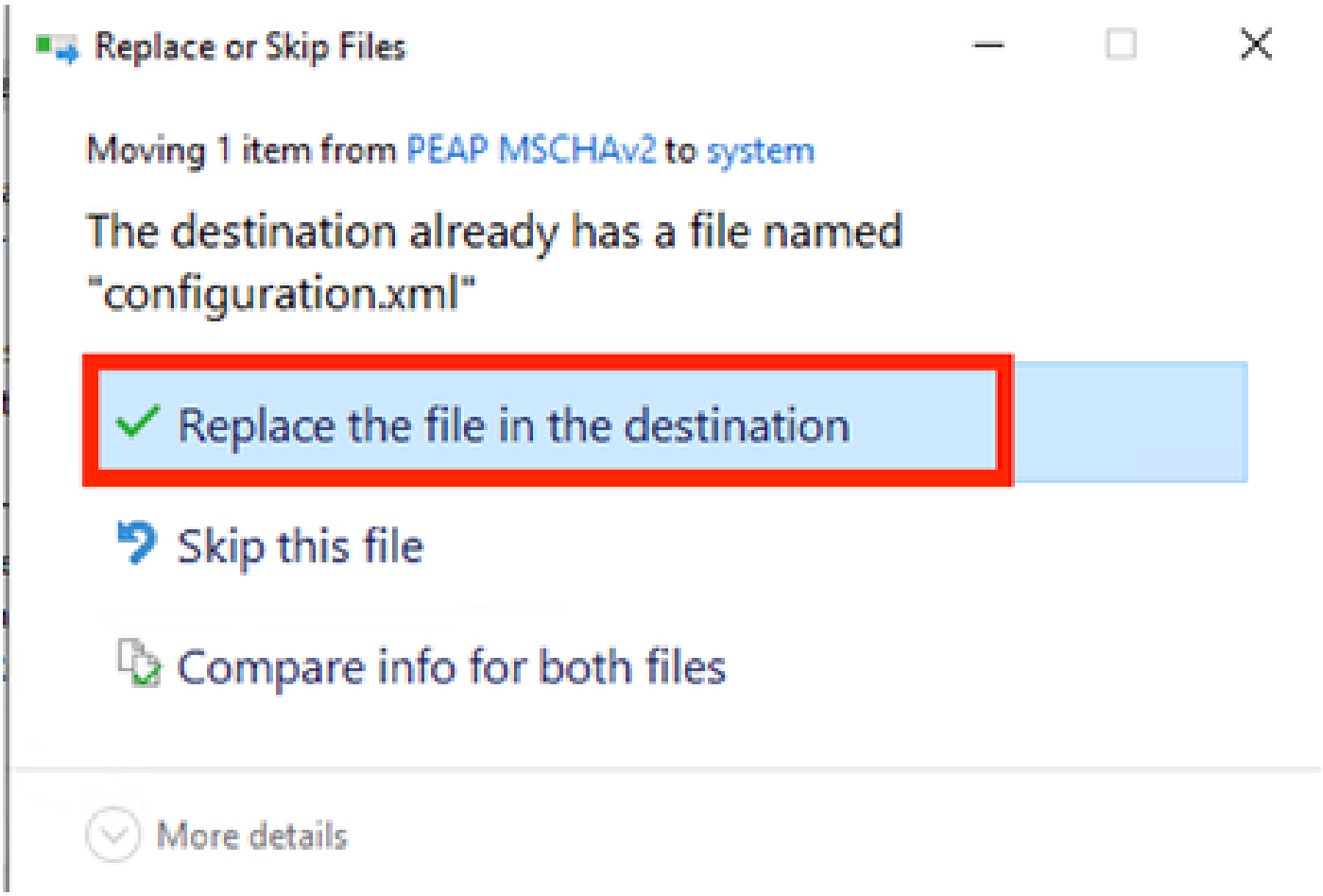
Salvare il profilo di Secure Client Network Access Manager come configuration.xml con l'opzione File > Salva con nome.

Per fare in modo che Secure Client Network Access Manager utilizzi il profilo appena creato, sostituire il file configuration.xml nella directory successiva con quello nuovo:

C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system



Nota: il nome del file deve essere configuration.xml, altrimenti il file non funzionerà.

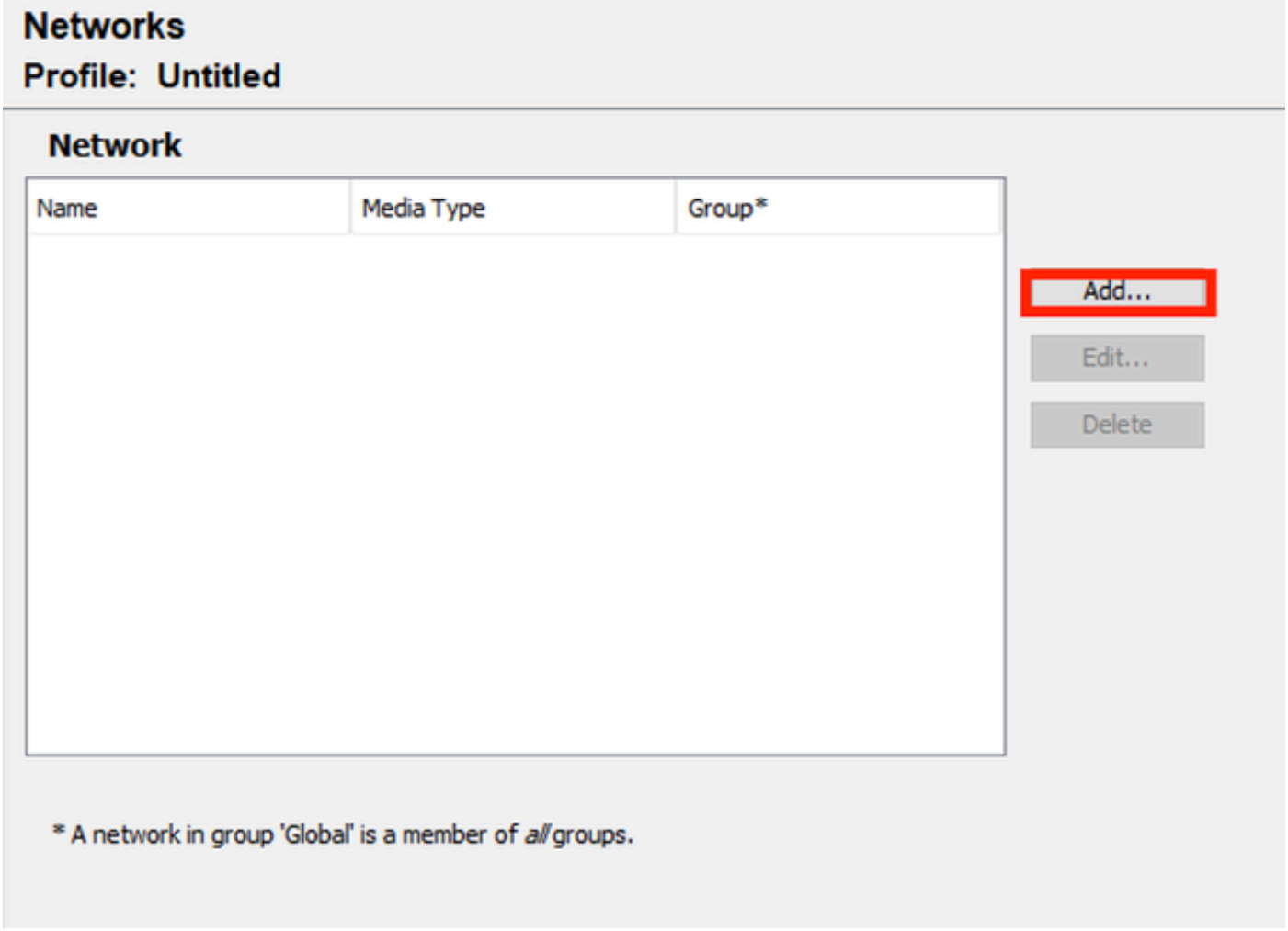


Sezione Sostituisci file

5. Scenario 2: configurazione del richiedente Secure Client NAM per l'autenticazione simultanea di computer e utente EAP-FAST

Aprire NAM Profile Editor e passare alla sezione Reti.

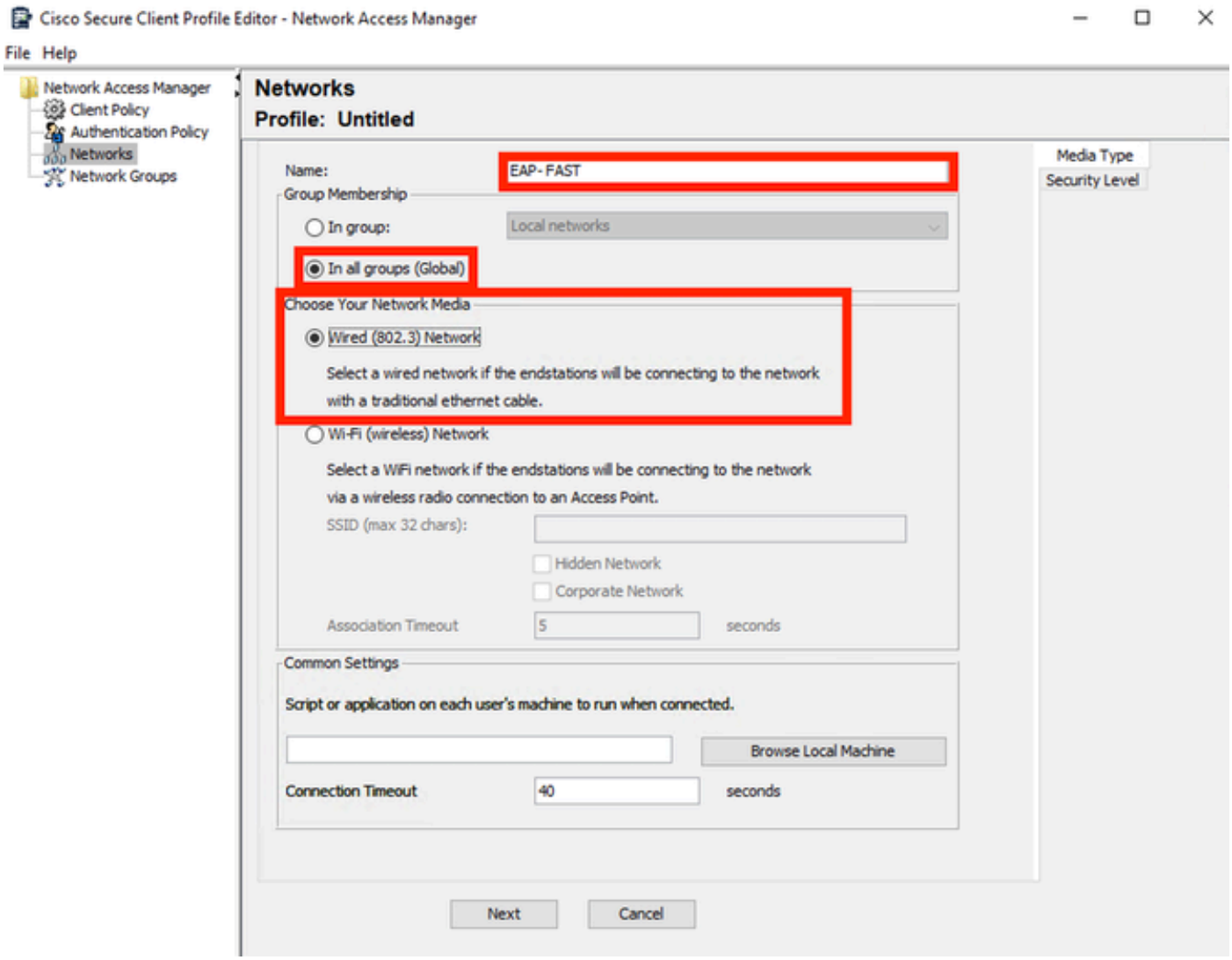
Fare clic su Add.



Scheda Rete dell'Editor di profili NAM

Immettere un nome nel profilo di rete.

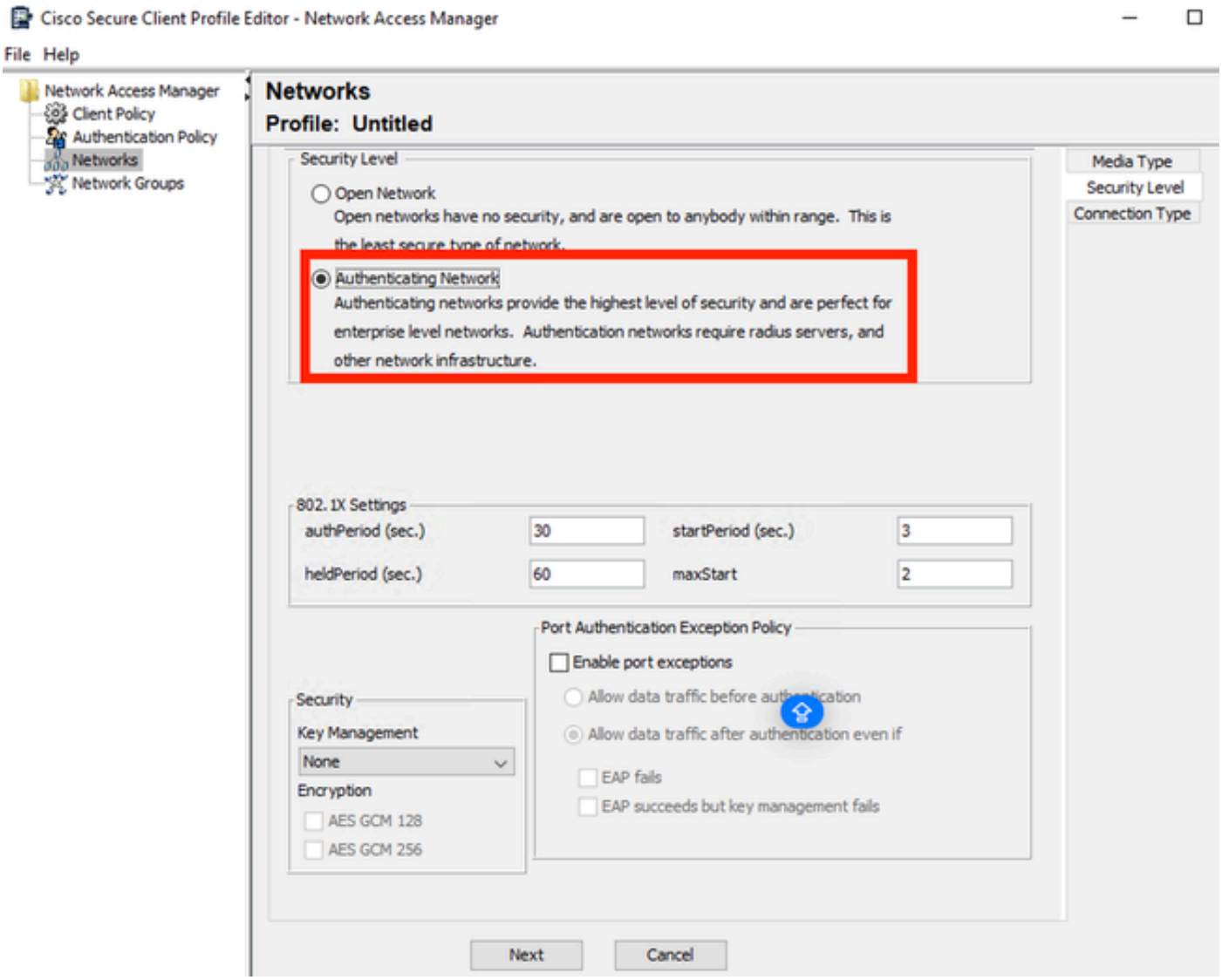
Selezionare Globale per l'appartenenza al gruppo. Selezionare Wired Network Media.



Sezione tipo di supporto

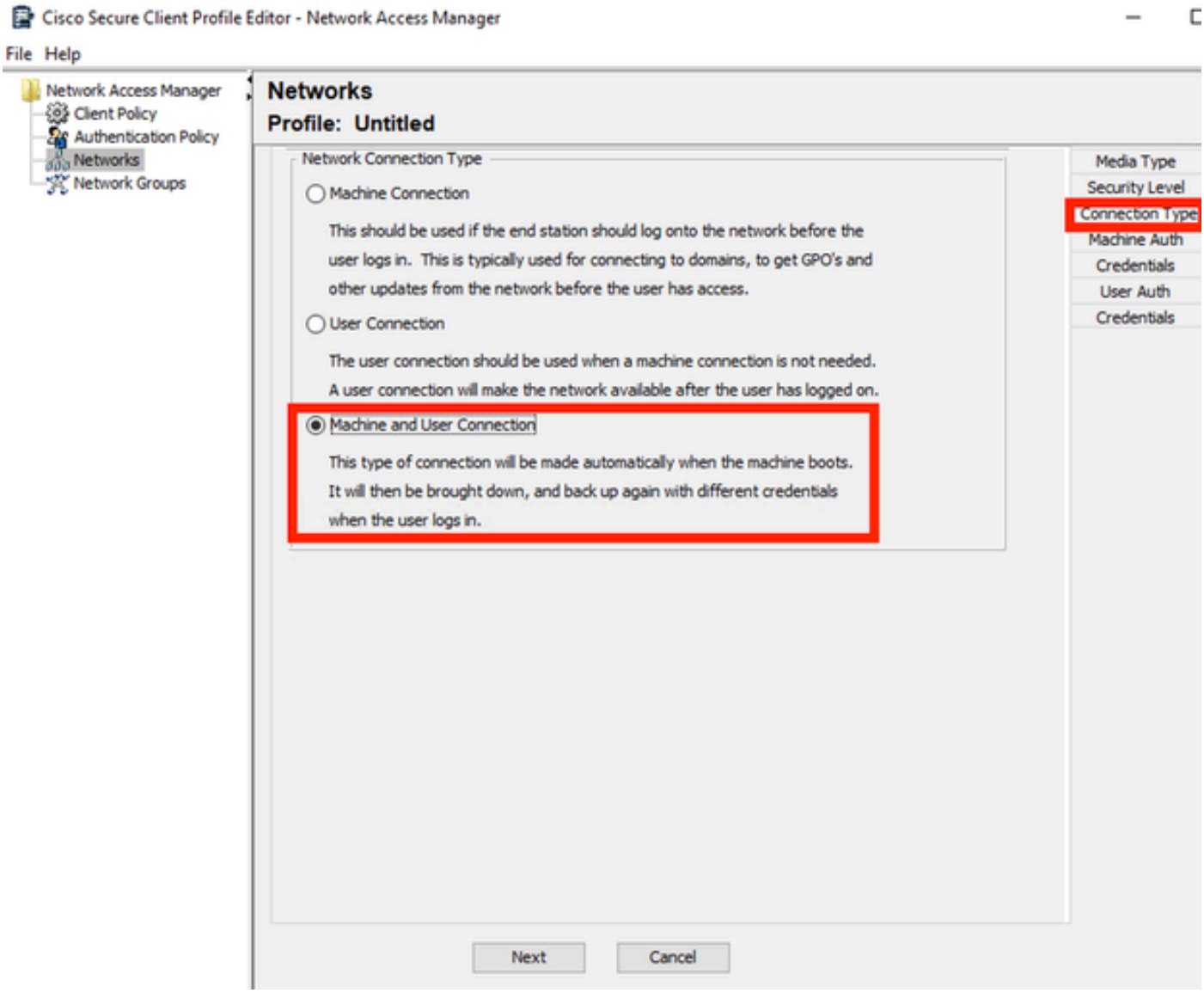
Fare clic su Next (Avanti).

Selezionare Autenticazione rete e non modificare i valori predefiniti per le altre opzioni di questa sezione.



Sezione Editor di profili del livello di protezione

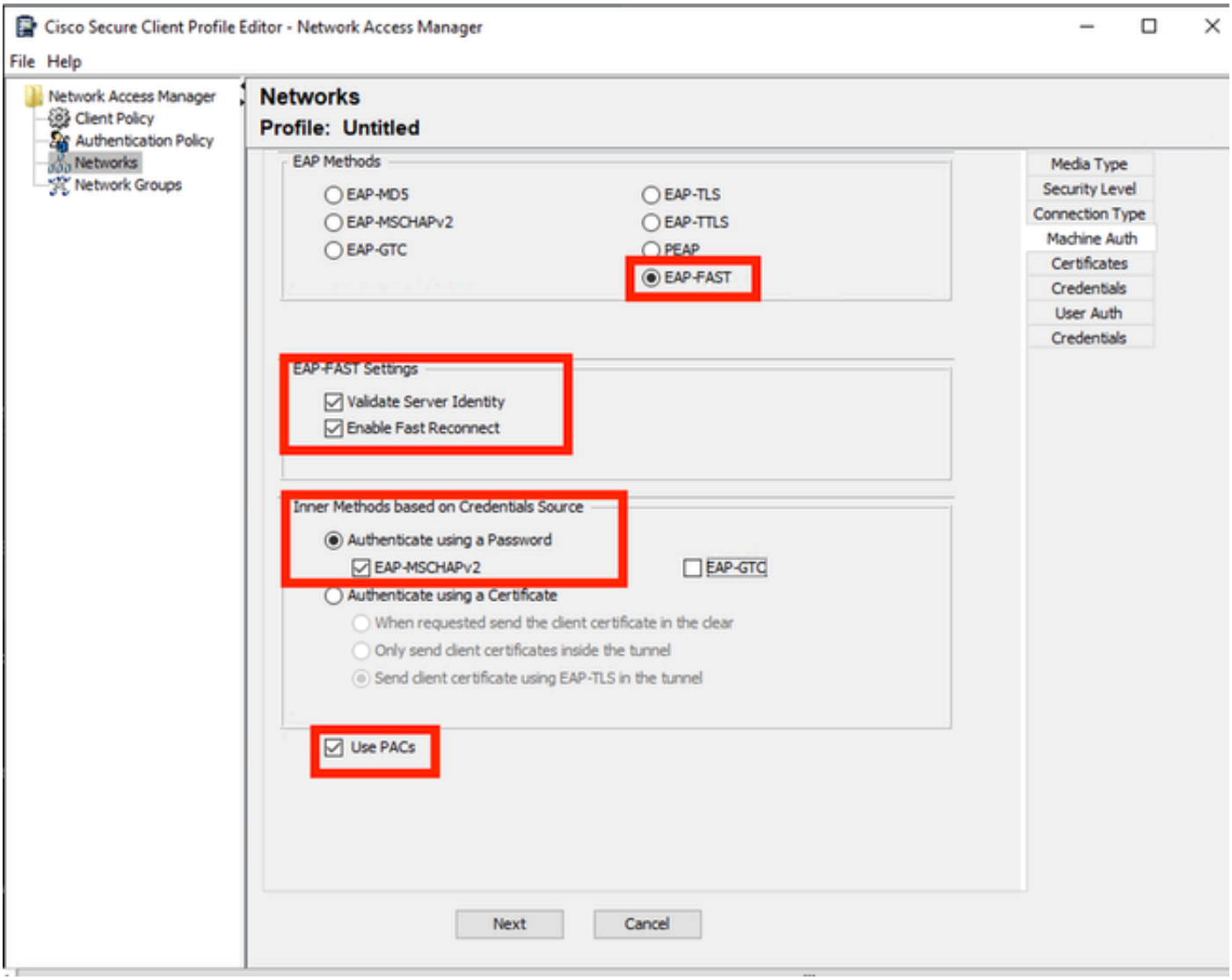
Fare clic su Avanti per continuare con la sezione Tipo di connessione.



Sezione Tipo di connessione

Configurare l'autenticazione di computer e utente contemporaneamente selezionando la terza opzione.

Fare clic su Next (Avanti).

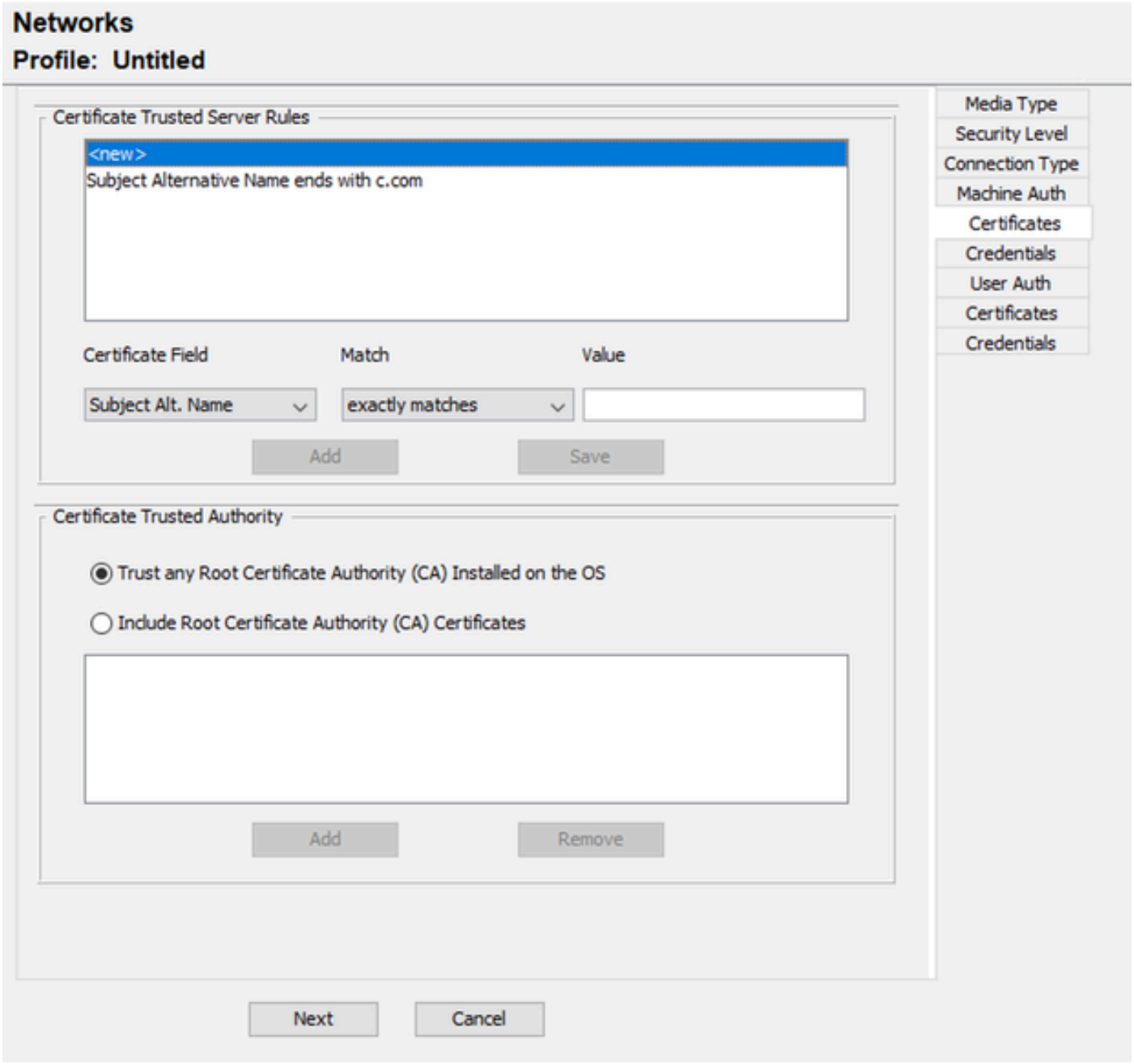


Sezione Machine Auth

Nella sezione Machine Auth (Autenticazione macchina) selezionare EAP-FAST come metodo EAP. Non modificare i valori predefiniti delle impostazioni FAST EAP. Per la sezione Metodi interni basati su origine credenziali selezionare Autentica utilizzando una password e EAP-MSCHAPv2 come metodo. Selezionare quindi l'opzione Usa PAC.

Fare clic su Next (Avanti).

Nella sezione Certificati, in Regole server trusted certificato il nome comune della regola termina con c.com. Questa sezione fa riferimento al certificato utilizzato dal server durante il flusso PEAP EAP. Se nell'ambiente viene utilizzato Identity Service Engine (ISE), è possibile utilizzare il nome comune del certificato EAP del nodo di Policy Server.

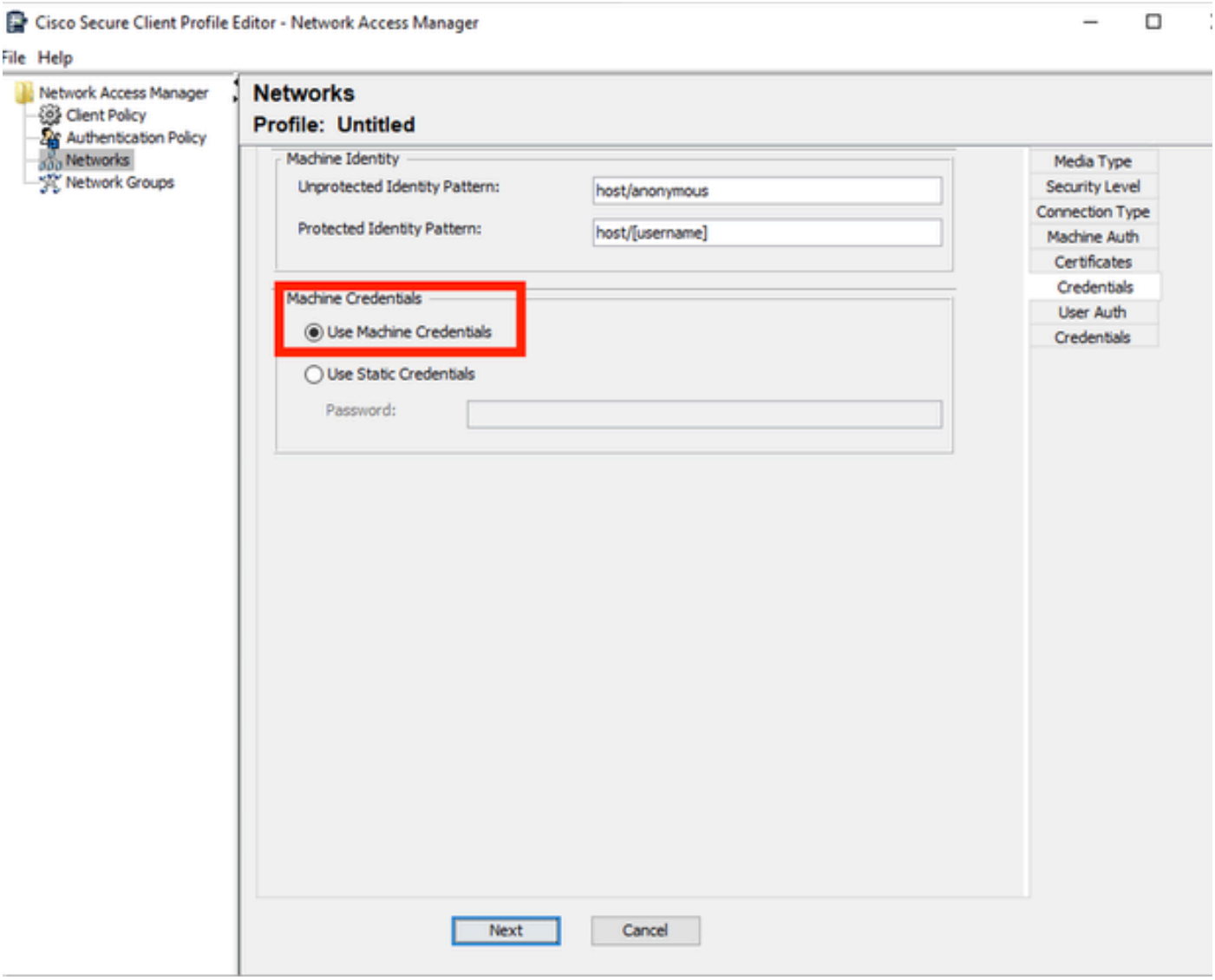


Sezione Attendibilità certificato server di autenticazione computer

In Autorità di certificazione attendibile è possibile selezionare due opzioni. Per questo scenario, anziché aggiungere un certificato CA specifico che firmi il certificato RADIUS EAP, utilizzare l'opzione Considera attendibile qualsiasi autorità di certificazione (CA) radice installata nel sistema operativo.

Con questa opzione, Windows considera attendibile qualsiasi certificato EAP firmato da un certificato incluso nel programma Gestisci certificati utente (Utente corrente > Autorità di certificazione principali attendibili > Certificati).

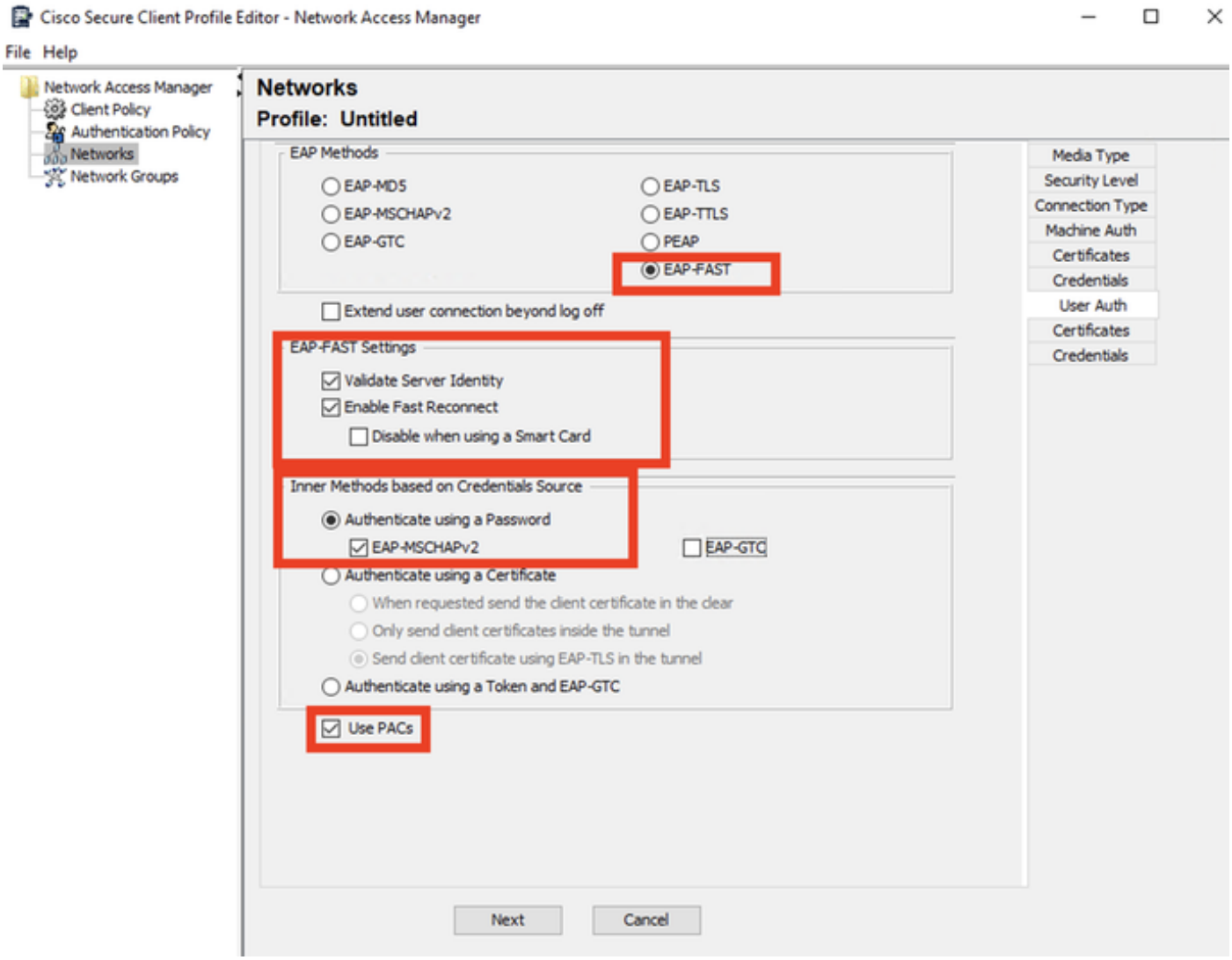
Fare clic su Next (Avanti).



Sezione Credenziali autenticazione computer

Selezionare Usa credenziali computer nella sezione Credenziali computer.

Fare clic su Next (Avanti).



Sezione Autenticazione utente

Per Autenticazione utente, selezionare EAP-FAST come metodo EAP.

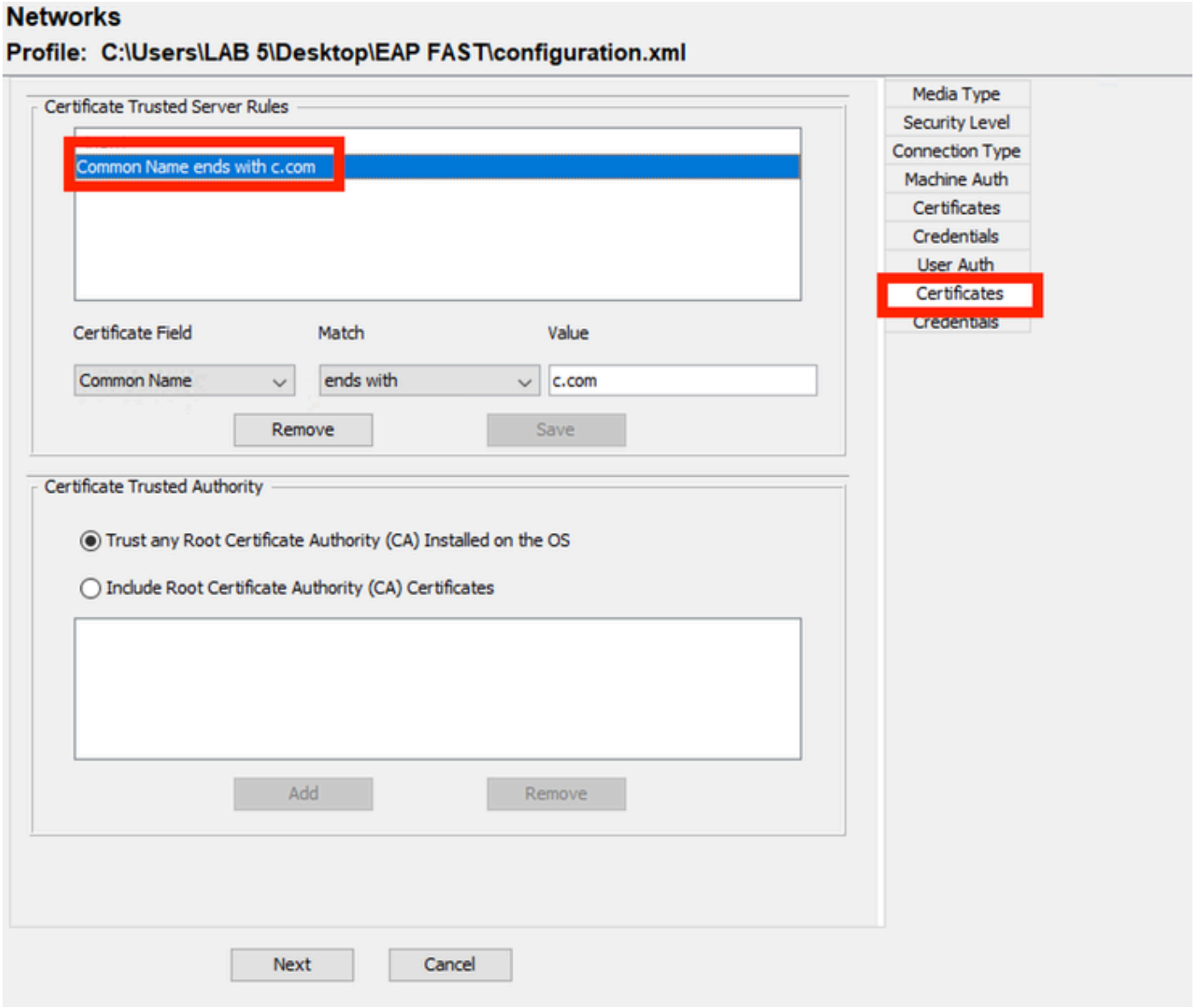
Non modificare i valori predefiniti nella sezione delle impostazioni EAP-FAST.

Per la sezione Metodo interno basato su origine credenziali, selezionare Autentica utilizzando una password e EAP-MSCHAPv2 come metodo.

Selezionare Usa PAC.

Fare clic su Next (Avanti).

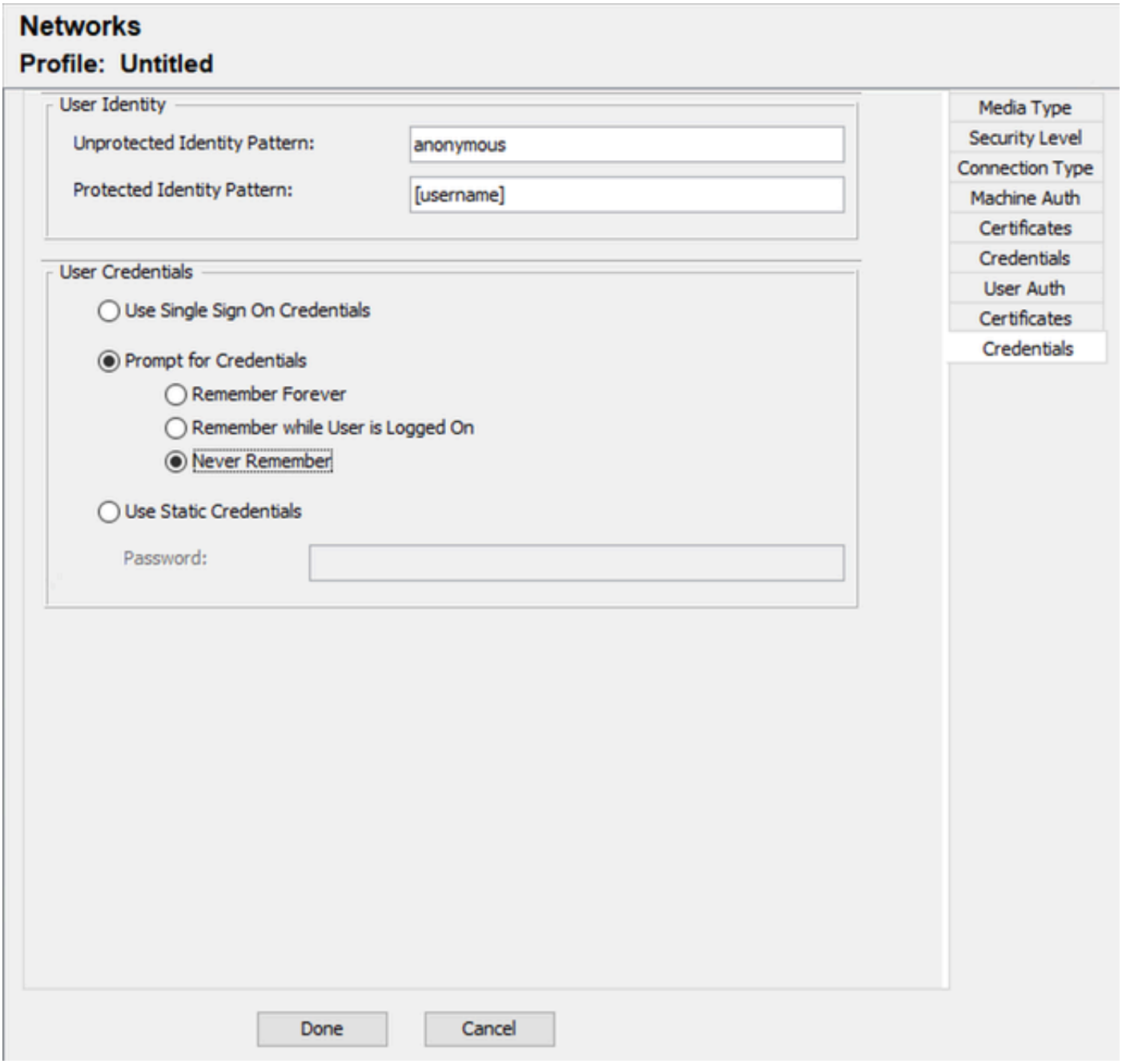
Nella sezione Certificati, in Regole server trusted certificato, la regola è Nome comune (Common Name) che termina con c.com. Queste configurazioni sono per il certificato utilizzato dal server durante il flusso PEAP EAP. Se nell'ambiente viene utilizzato ISE, è possibile utilizzare il nome comune del certificato EAP del nodo di Policy Server.



Sezione User Auth Server Certificate Trust

In Autorità di certificazione attendibile è possibile selezionare due opzioni. Per questo scenario, anziché aggiungere un certificato CA specifico che firmi il certificato RADIUS EAP, viene utilizzata l'opzione Considera attendibile qualsiasi autorità di certificazione (CA) radice installata nel sistema operativo.

Fare clic su Next (Avanti).



Credenziali autenticazione utente

Nella sezione Credenziali viene modificata solo la sezione Credenziali utente.

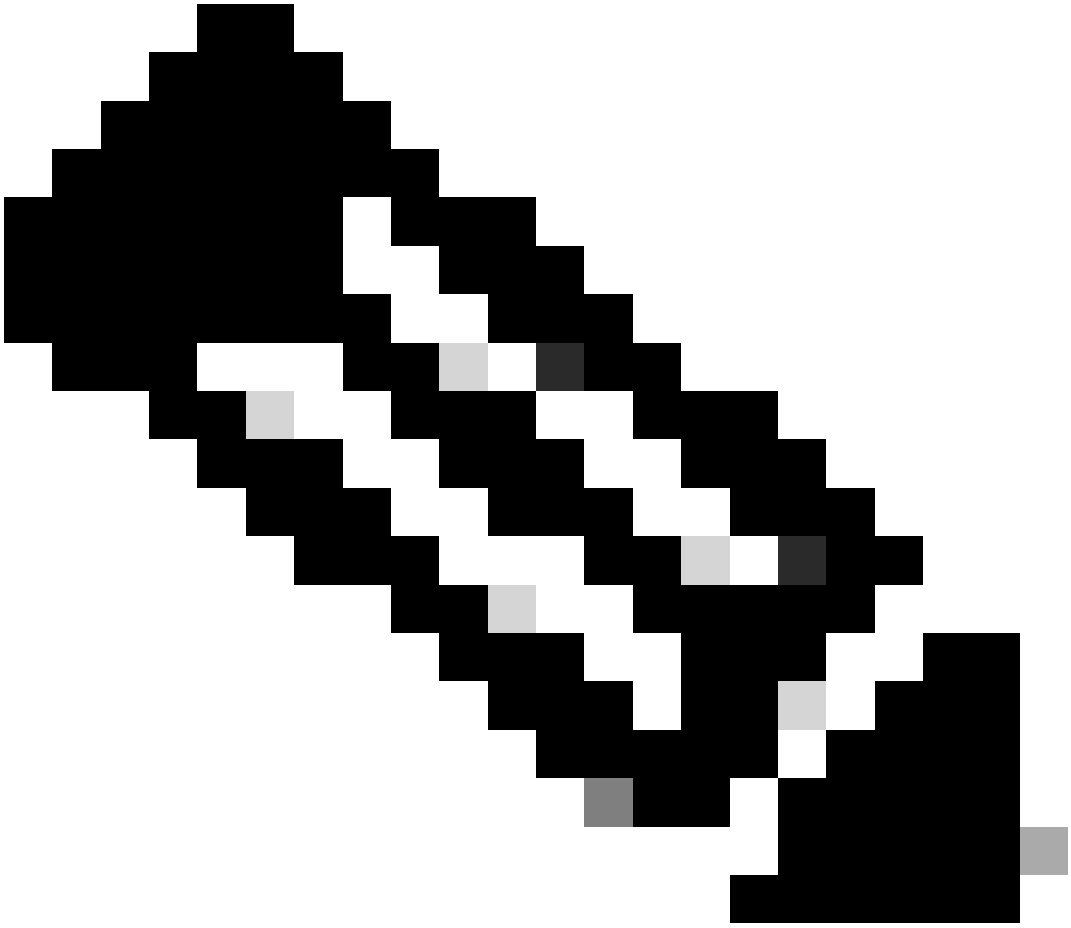
L'opzione Richiedi credenziali > Non ricordare mai è selezionata. Pertanto, in ogni autenticazione, l'utente che esegue l'autenticazione deve immettere le proprie credenziali.

Fare clic sul pulsante Chiudi.

Selezionare File > Salva con nome e salvare il profilo di Secure Client Network Access Manager come configuration.xml.

Per fare in modo che Secure Client Network Access Manager utilizzi il profilo appena creato, sostituire il file configuration.xml nella directory successiva con quello nuovo:

C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system

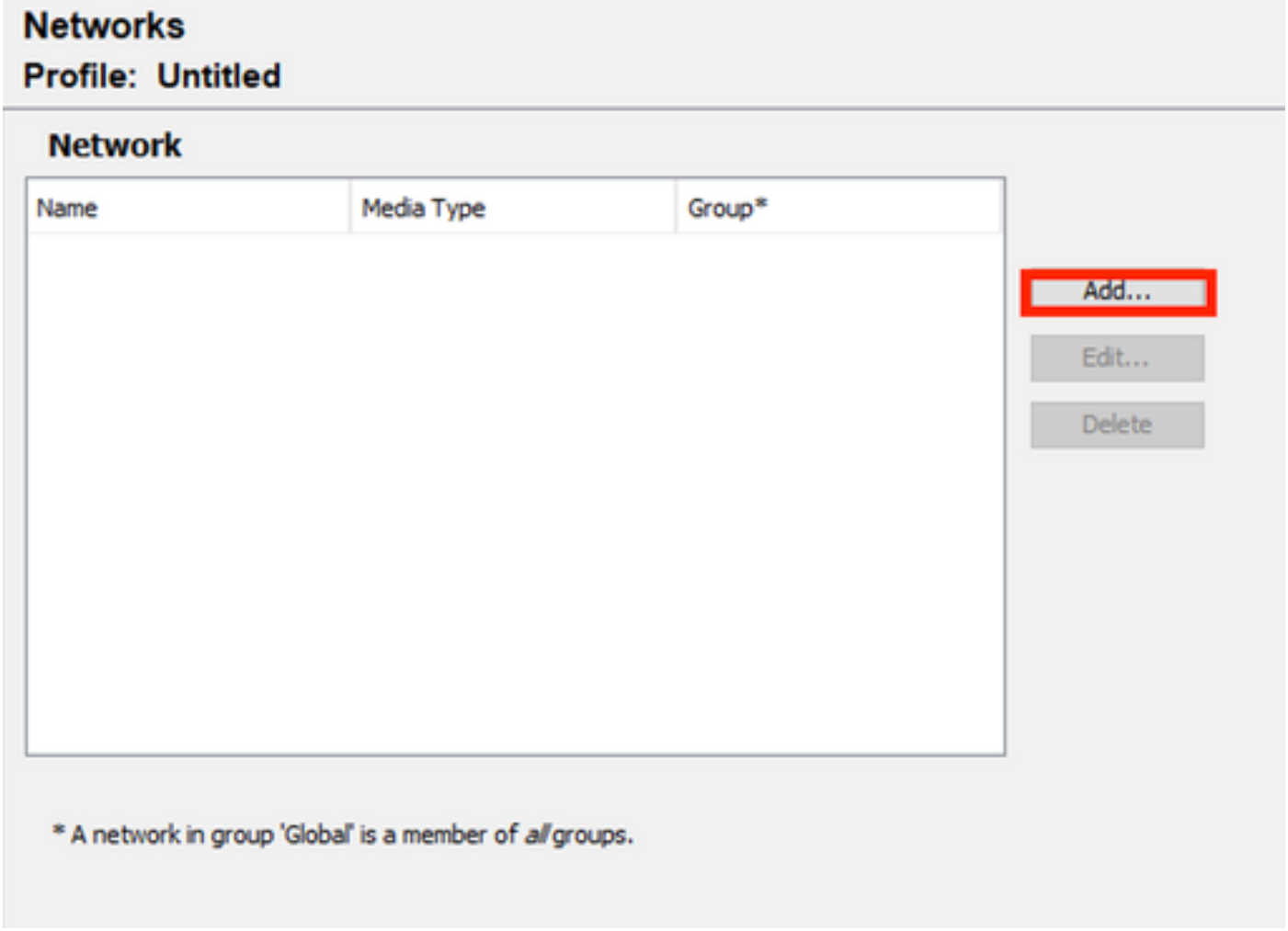


Nota: il nome del file deve essere configuration.xml, altrimenti il file non funzionerà.

6. Scenario 3: configurazione del richiedente Secure Client NAM per l'autenticazione del certificato utente EAP TLS

Aprire NAM Profile Editor e passare alla sezione Reti.

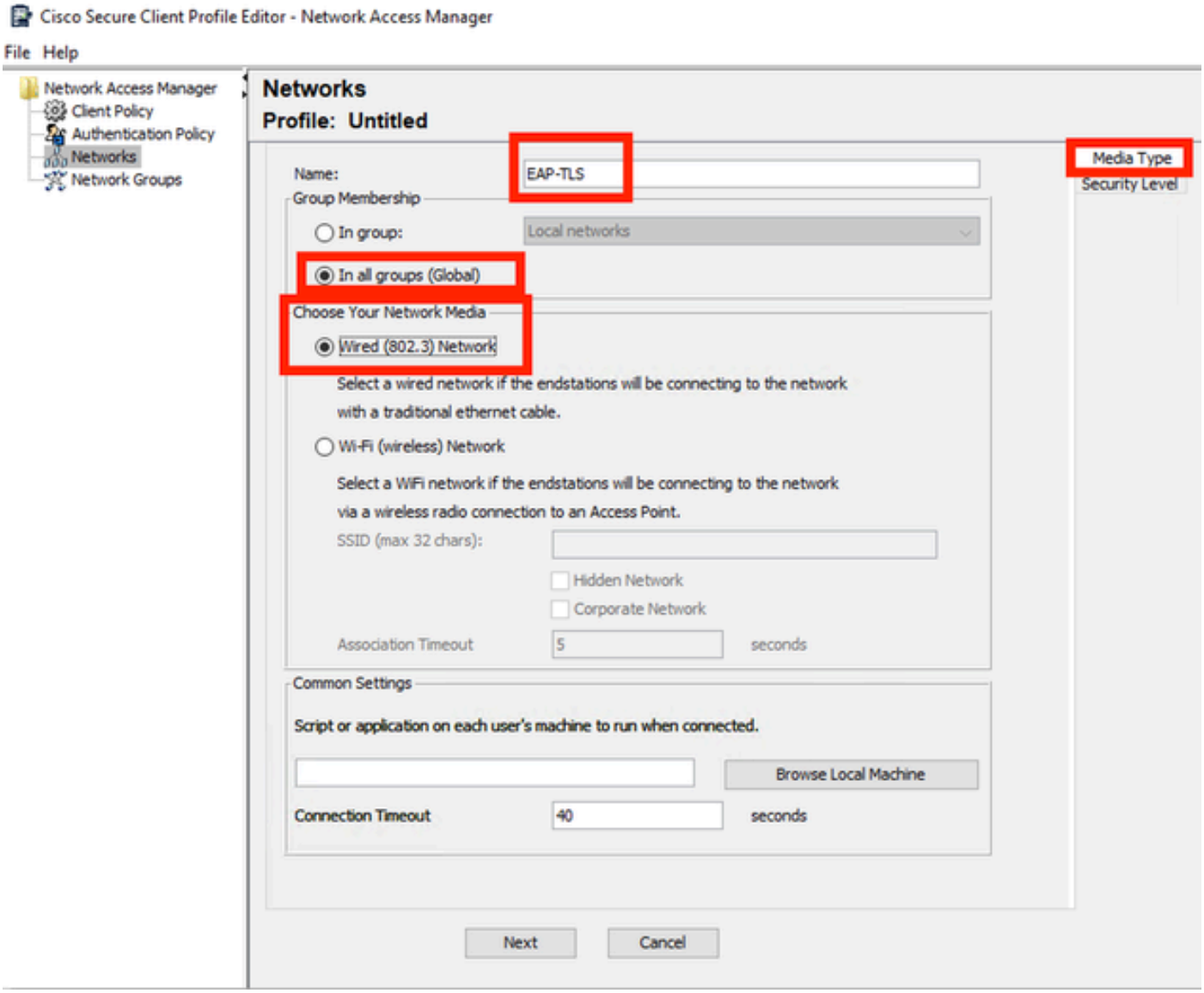
Fare clic su Add.



Sezione Creazione rete

Assegnare un nome al profilo di rete, in questo caso il nome corrisponde al protocollo EAP utilizzato per questo scenario.

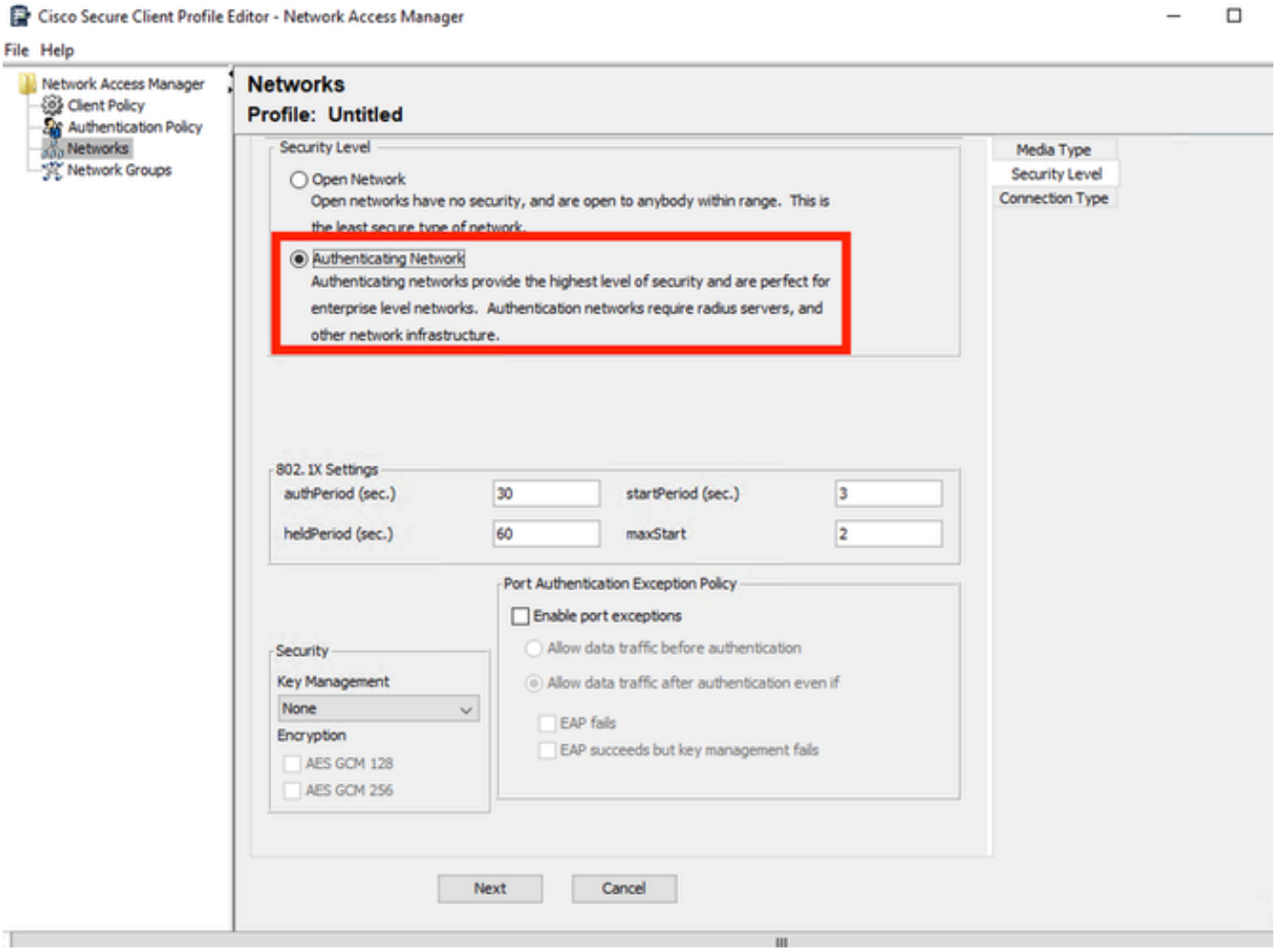
Selezionare Globale per l'appartenenza al gruppo. E Supporti Di Rete Cablati.



Sezione tipo di supporto

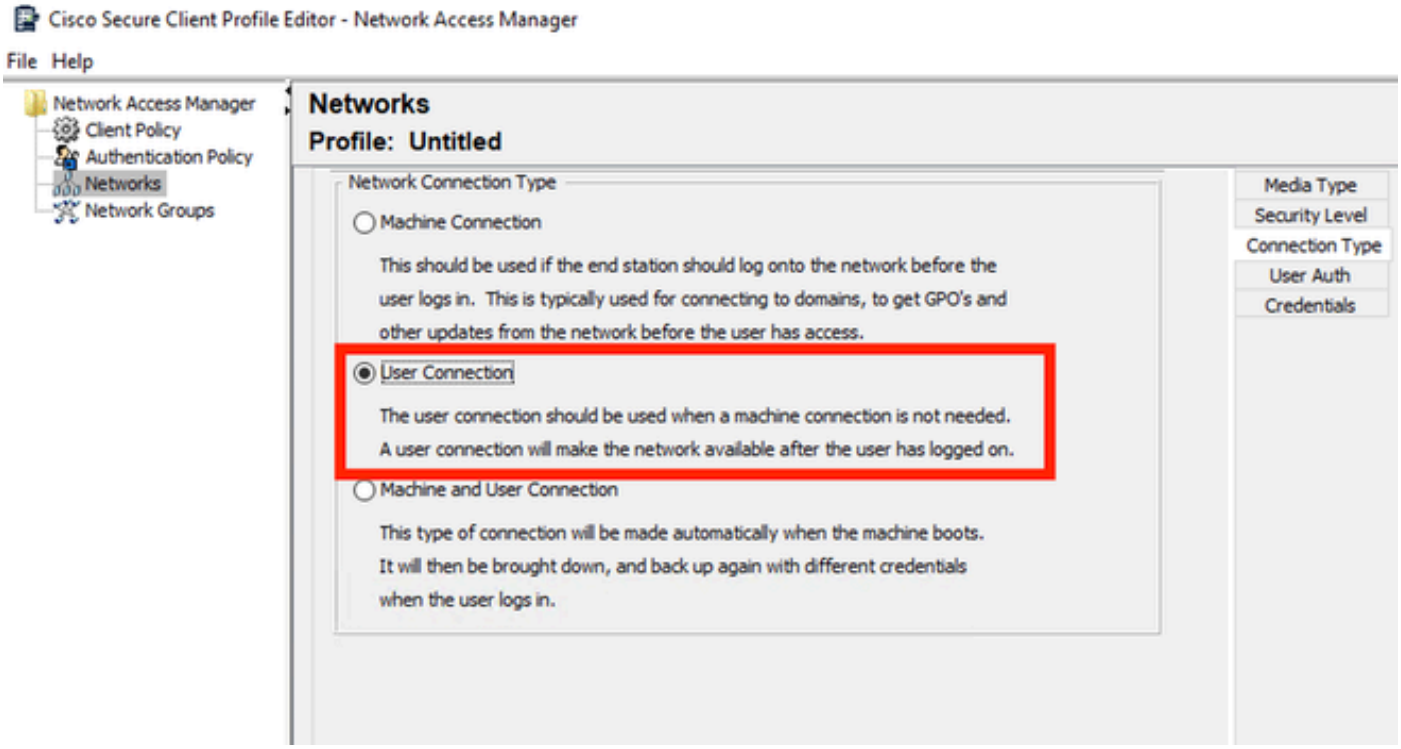
Fare clic su Next (Avanti).

Selezionare Autenticazione della rete e non modificare i valori predefiniti per le altre opzioni nella sezione Livello di protezione.



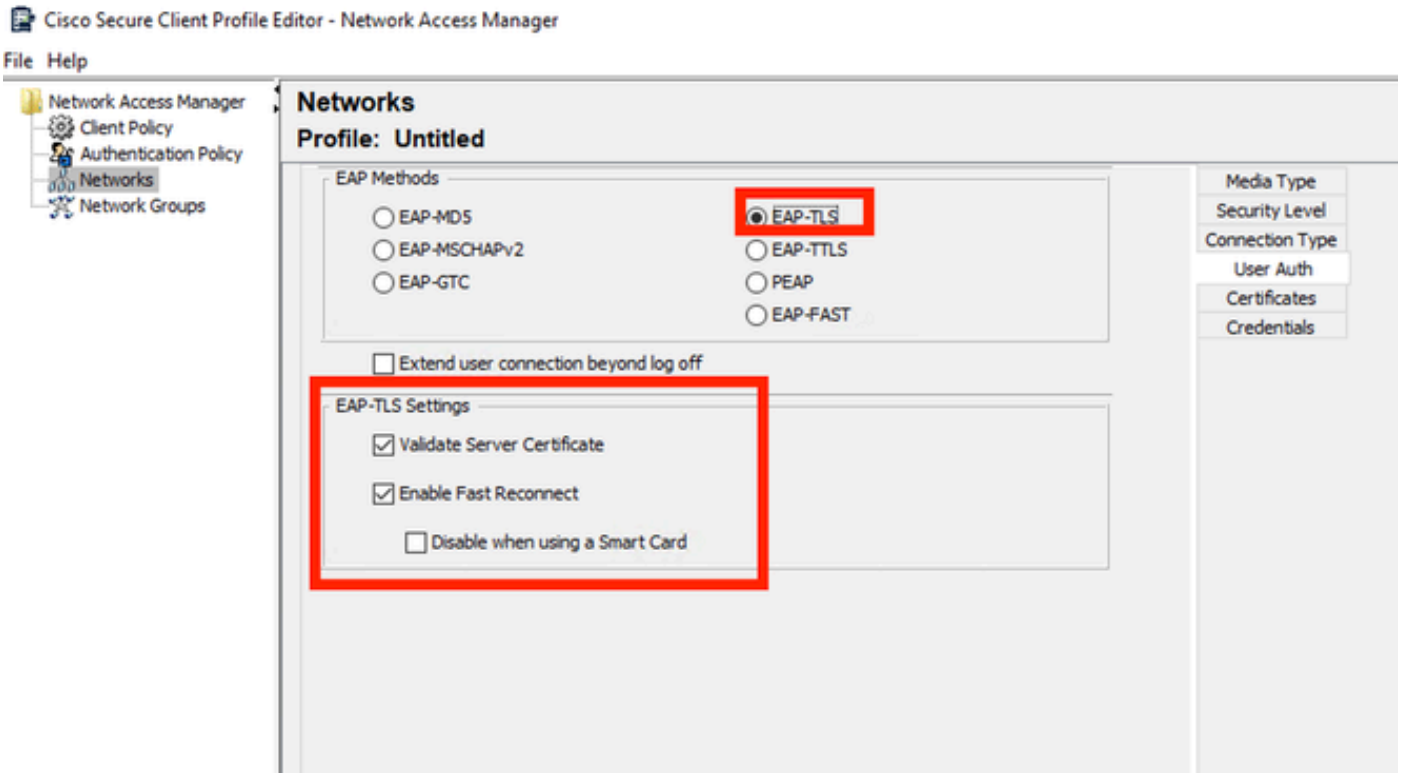
Livello di protezione

Scenario per l'autenticazione utente tramite un certificato. Per questo motivo viene utilizzata l'opzione Connessione utente.



Tipo di connessione

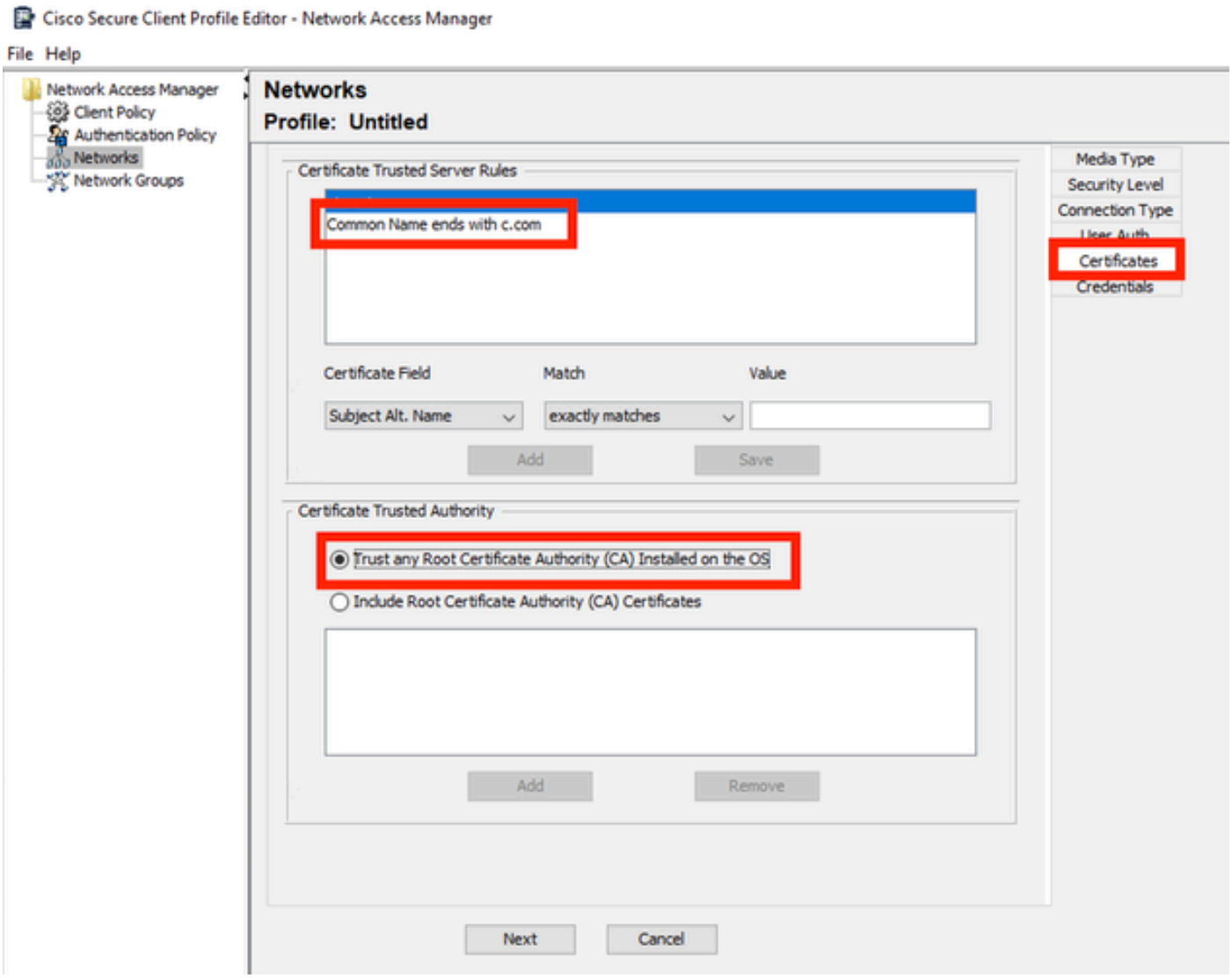
Configurare EAP-TLS come metodo EAP. Non modificare i valori predefiniti nella sezione Impostazioni EAP-TLS.



Sezione Autenticazione utente

Per la sezione Certificati, creare una regola che corrisponda al certificato AAA EAP-TLS. Se si utilizza ISE, trovare questa regola nella sezione Amministrazione > Sistema > Certificati.

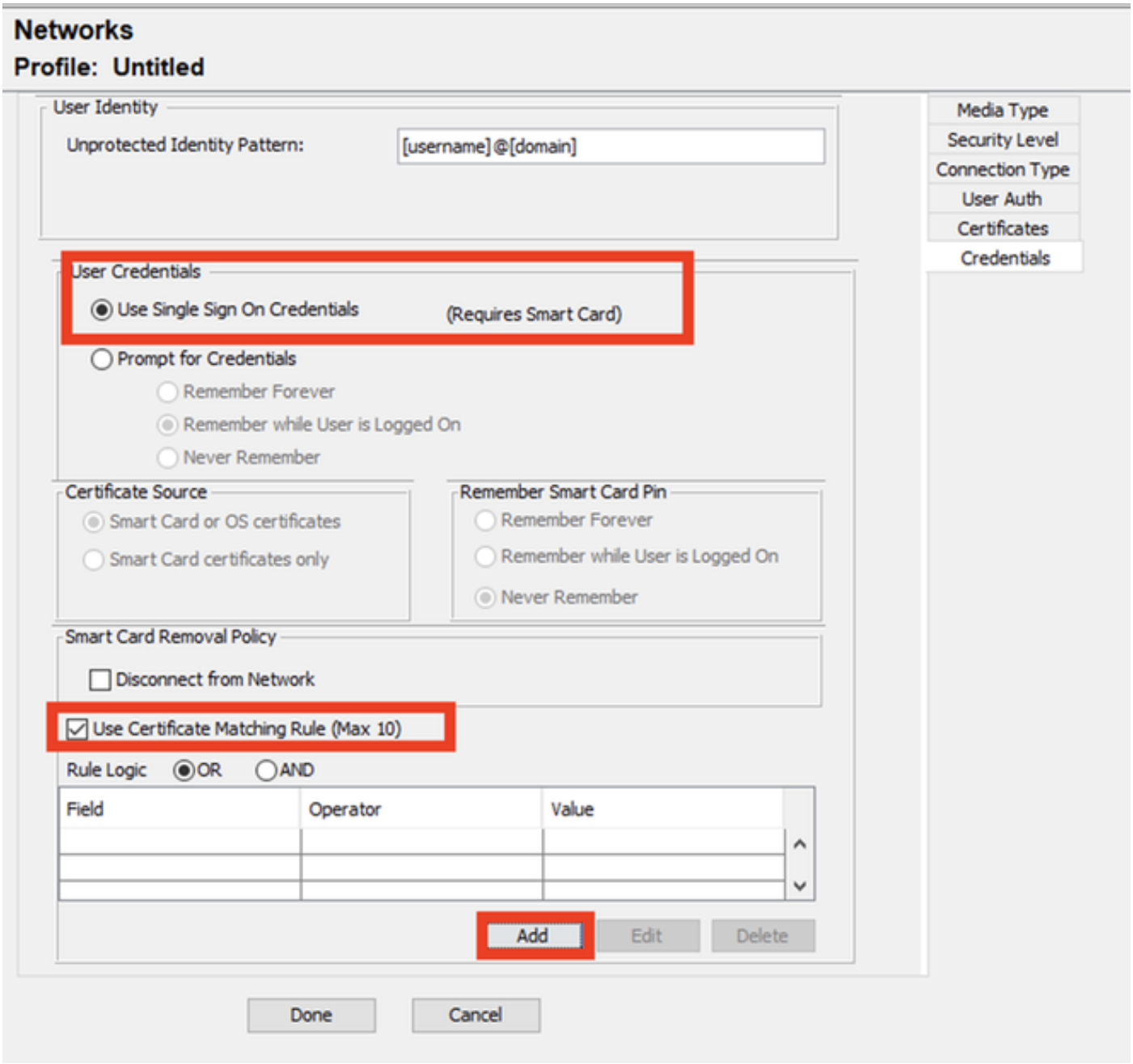
Per la sezione Autorità di certificazione attendibile selezionare Considera attendibile qualsiasi autorità di certificazione (CA) radice installata nel sistema operativo.



Impostazioni di attendibilità del certificato del server di autenticazione utente

Fare clic su Next (Avanti).

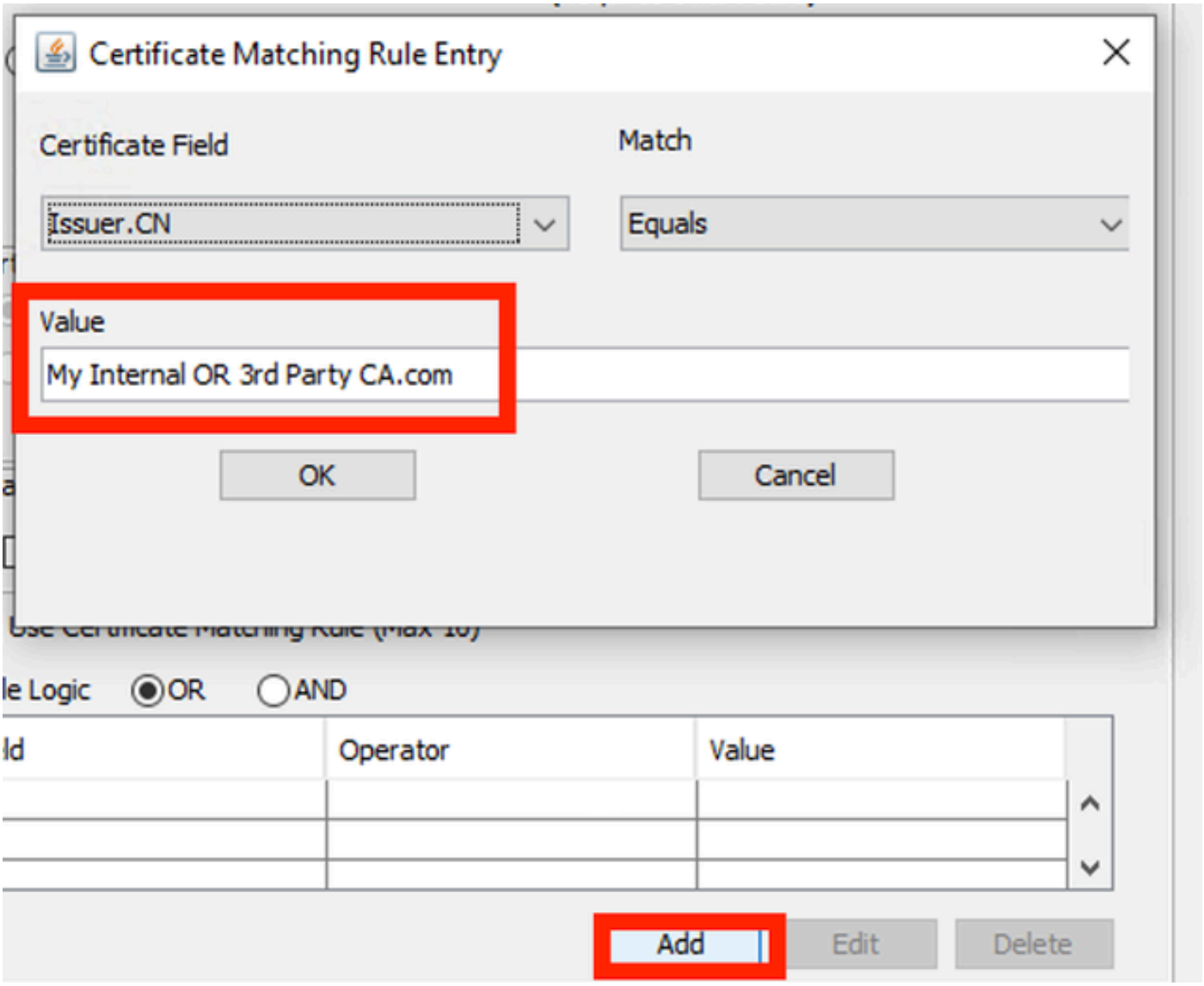
Per la sezione Credenziali utente, non modificare i valori predefiniti nella prima parte.



Sezione Credenziali autenticazione utente

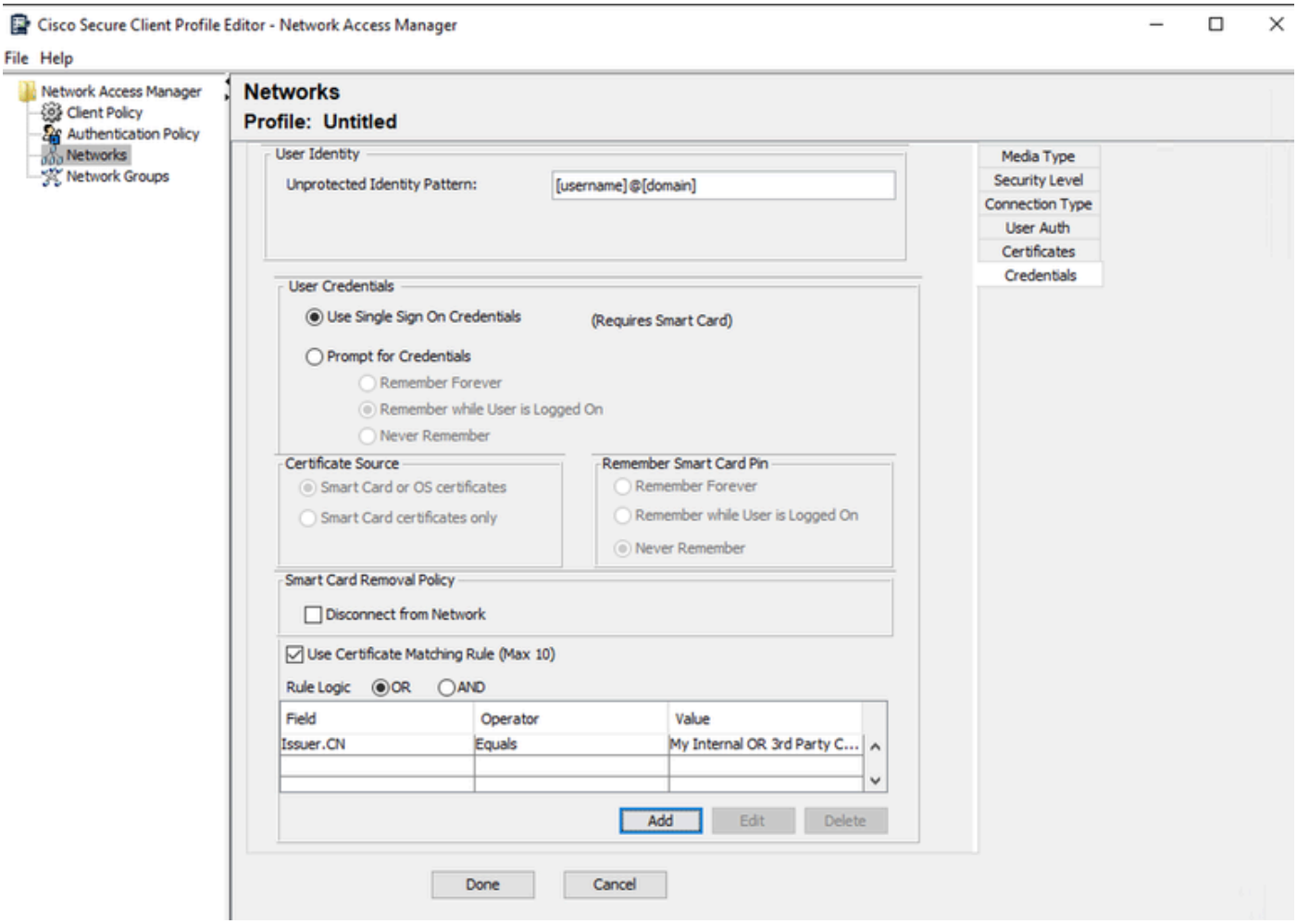
È importante configurare una regola corrispondente al certificato di identità inviato dall'utente durante il processo TLS EAP. A tale scopo, fare clic sulla casella di spunta accanto a Usa regola di corrispondenza certificati (max 10).

Fare clic su Add.



Finestra Regola di corrispondenza certificato

Sostituire il valore My Internal OR 3rd Party CA.com string con il CN del certificato utente.



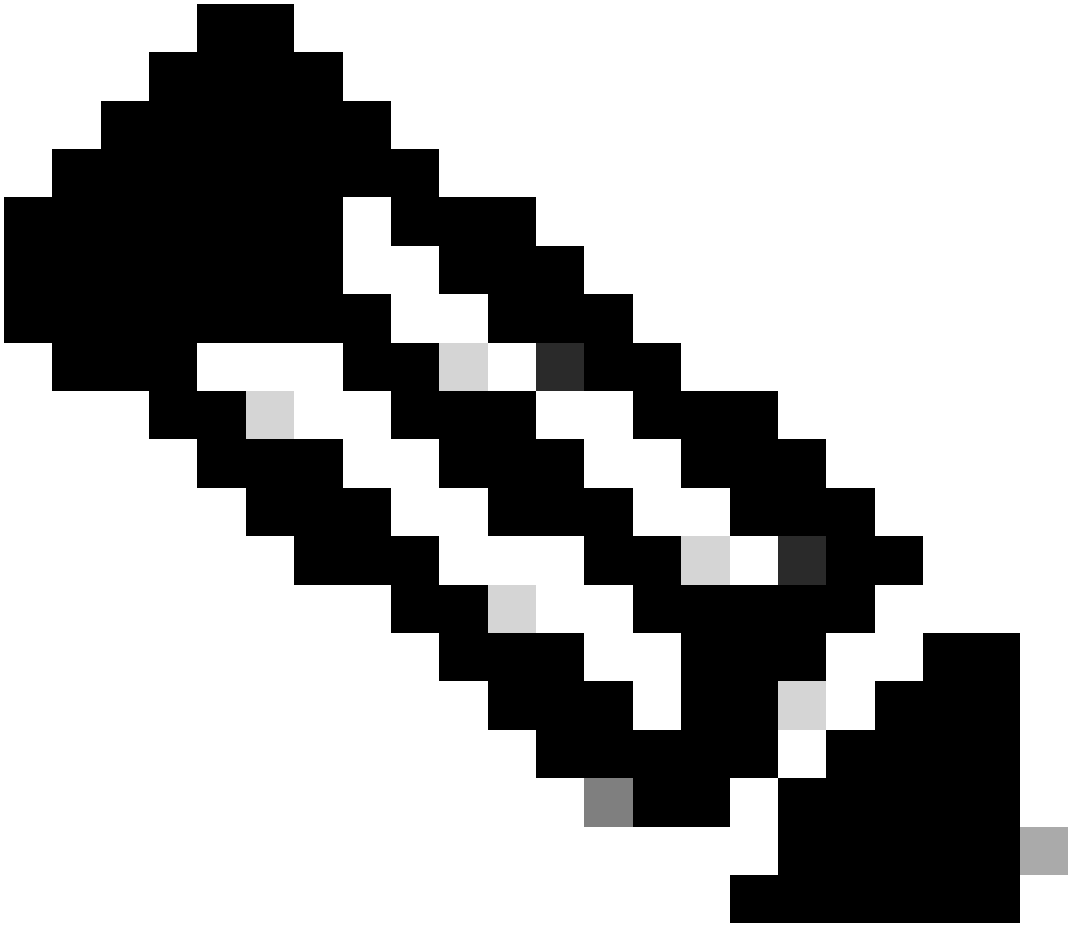
Sezione Credenziali certificato di autenticazione utente

Fate clic su Fatto (Done) per completare la configurazione.

Selezionare File > Salva con nome per salvare il profilo di Secure Client Network Access Manager come configuration.xml.

Per fare in modo che Secure Client Network Access Manager utilizzi il profilo appena creato, sostituire il file configuration.xml nella directory successiva con quello nuovo:

C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system

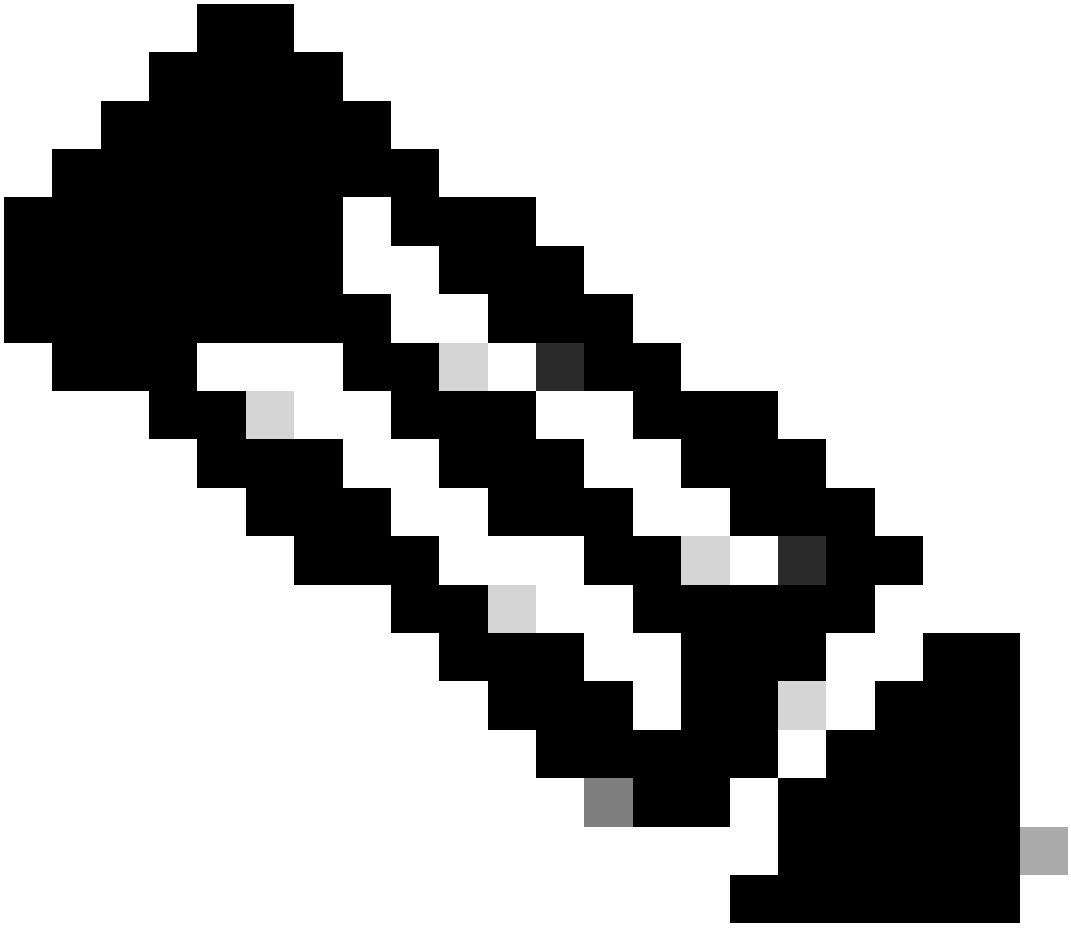


Nota: il nome del file deve essere configuration.xml, altrimenti il file non funzionerà.

7. Configurare ISR 1100 e ISE in modo da consentire le autenticazioni basate sullo scenario 1 PEAP MSCHAPv2

Configurare il router ISR 1100.

In questa sezione viene illustrata la configurazione di base necessaria per il funzionamento di dot1x da parte di NAD.



Nota: per la distribuzione ISE a più nodi, puntare a qualsiasi nodo con la persona nodo di Policy Server abilitata. Per verificare questa condizione, accedere ad ISE nella scheda Amministrazione > Sistema >Distribuzione.

```
aaa new-model
aaa session-id common
!
aaa authentication dot1x default group ISE-CLUSTER
aaa authorization network default group ISE-CLUSTER
aaa accounting system default start-stop group ISE-CLUSTER
aaa accounting dot1x default start-stop group ISE-CLUSTER
!
aaa server radius dynamic-author
 client A.B.C.D server-key  <Your shared secret>
!
!
radius server  ISE-PSN-1
 address ipv4 A.B.C.D auth-port 1645 acct-port 1646
 timeout 15
 key <Your shared secret>
```

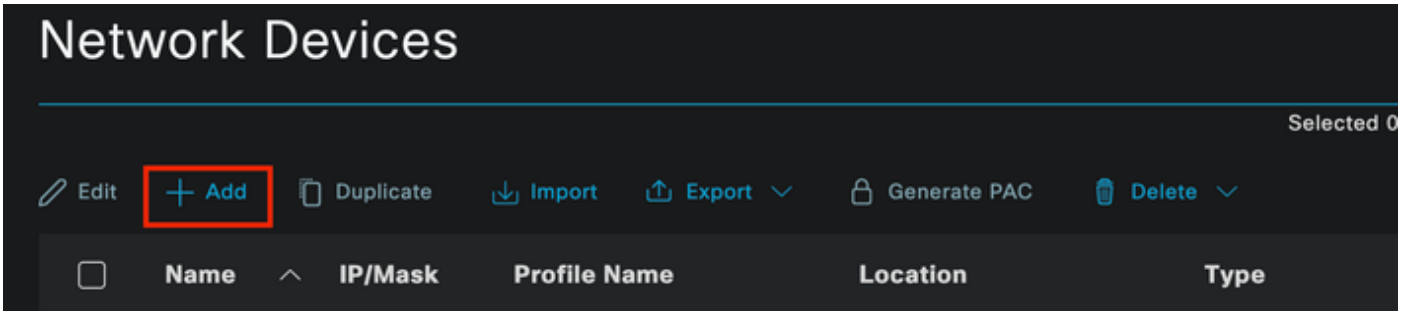
```
!
!
aaa group server radius ISE-CLUSTER
 server name ISE-PSN-1
!
interface GigabitEthernet0/1/0
 description "Endpoint that supports dot1x"
 switchport access vlan 15
 switchport mode access
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast
```

Configurare Identity Service Engine 3.2.

Configurare il dispositivo di rete.

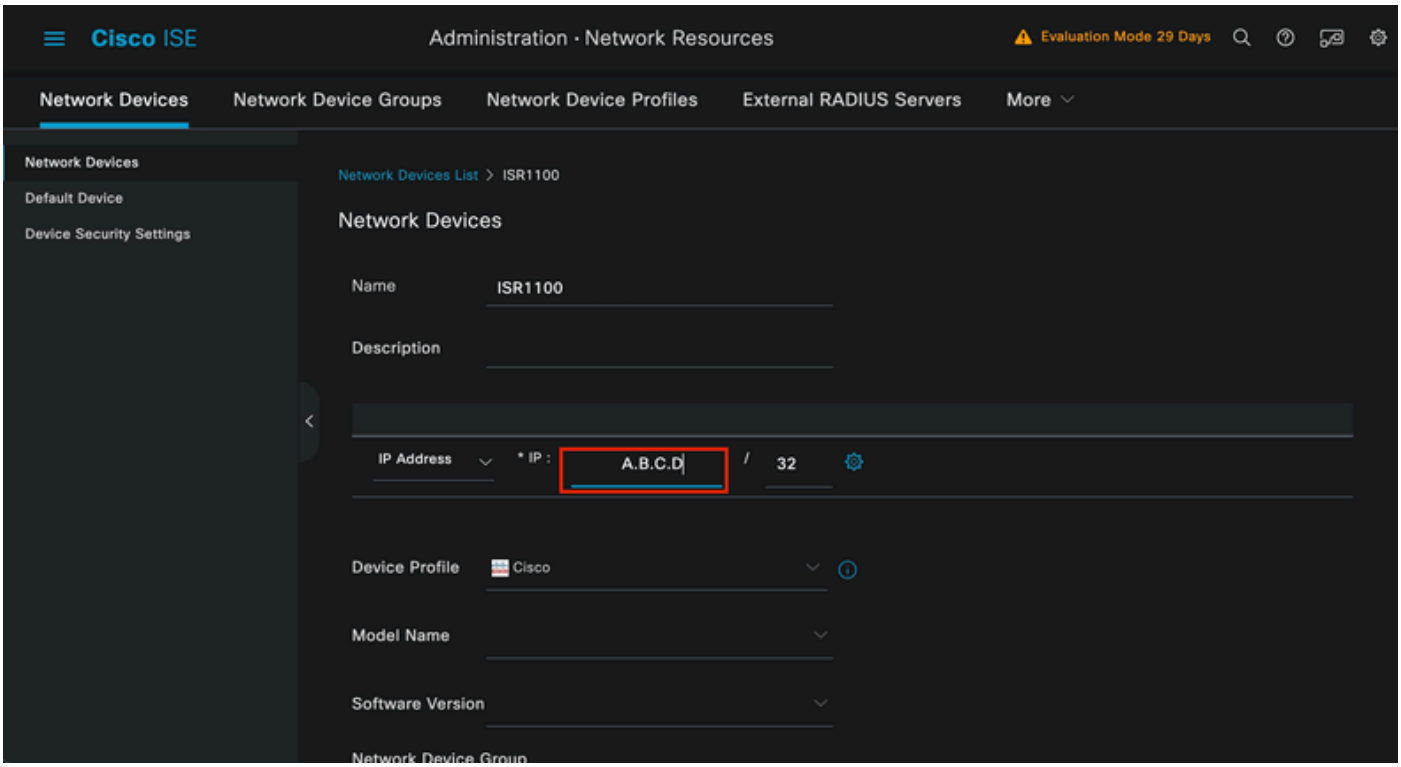
Aggiungere ISR e ISE ad Amministrazione > Risorse di rete > Dispositivi di rete.

Fare clic su Add.



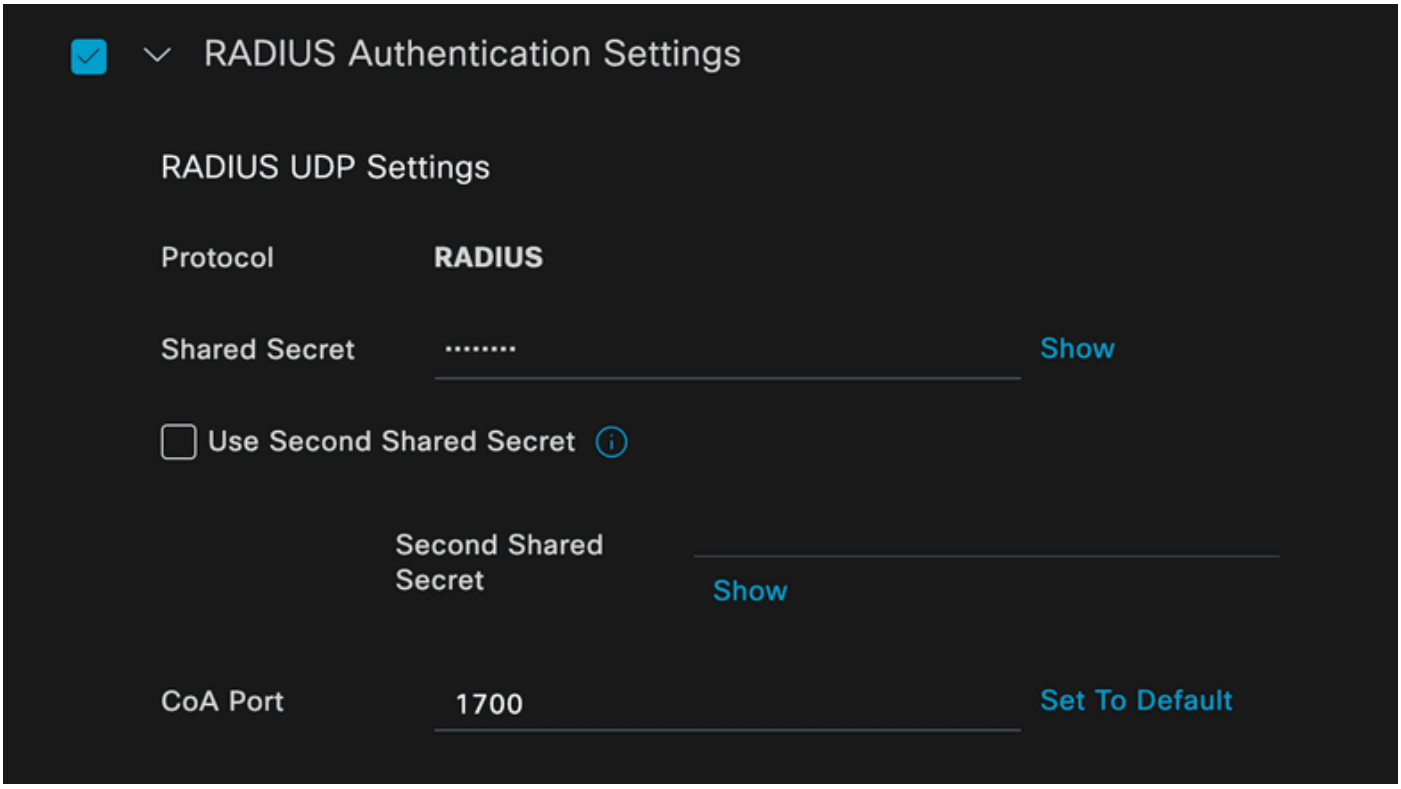
Sezione Periferica di rete

Assegnare un nome al file NAD che si sta creando. Aggiungere l'indirizzo IP del dispositivo di rete.



Creazione di dispositivi di rete

Nella parte inferiore della stessa pagina aggiungere lo stesso segreto condiviso utilizzato nella configurazione del dispositivo di rete.



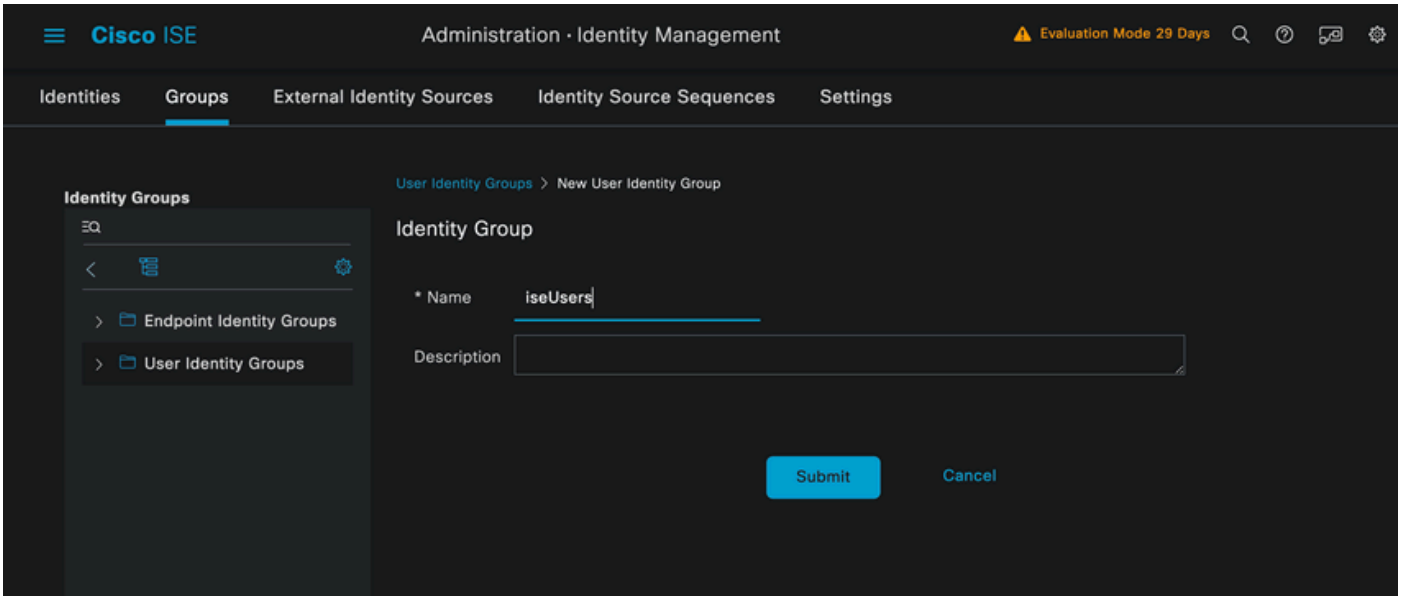
Impostazioni raggio dispositivo di rete

Salvare le modifiche.

Configurare l'identità utilizzata per autenticare l'endpoint.

Viene utilizzata l'autenticazione ISE locale. In questo articolo non viene fornita alcuna spiegazione sull'autenticazione ISE esterna.

Passare alla scheda Amministrazione > Gestione delle identità > Gruppi e creare il gruppo di cui fa parte l'utente. Il gruppo di identità creato per questa dimostrazione è iseUsers.

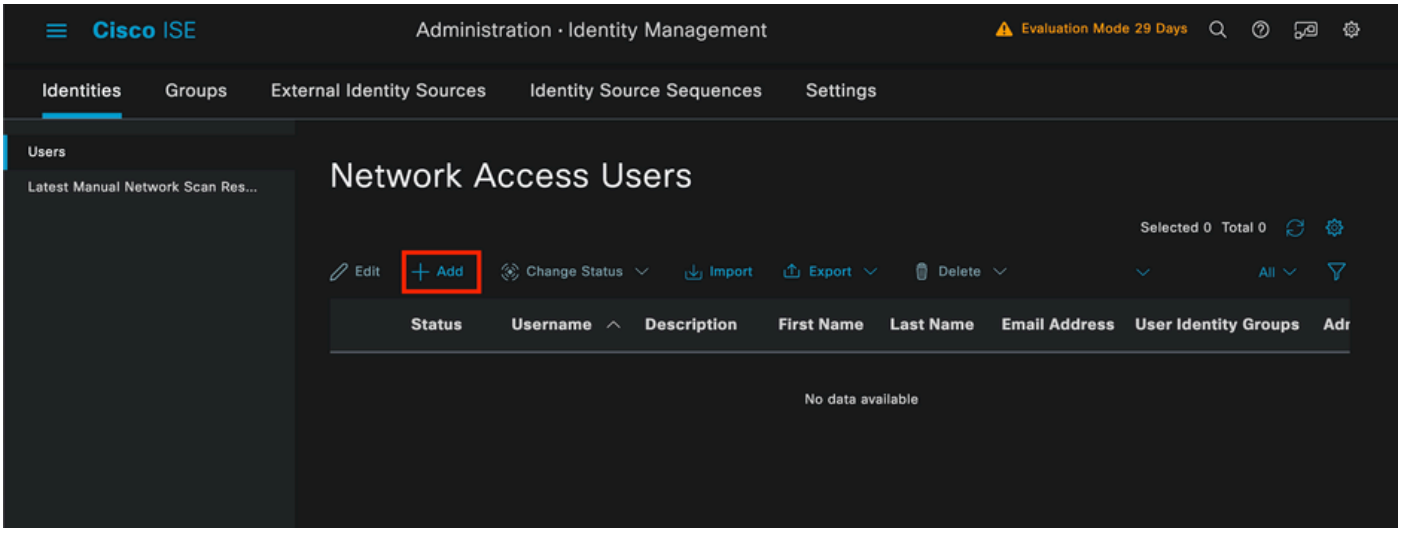


Creazione gruppo di identità

Fare clic su Invia.

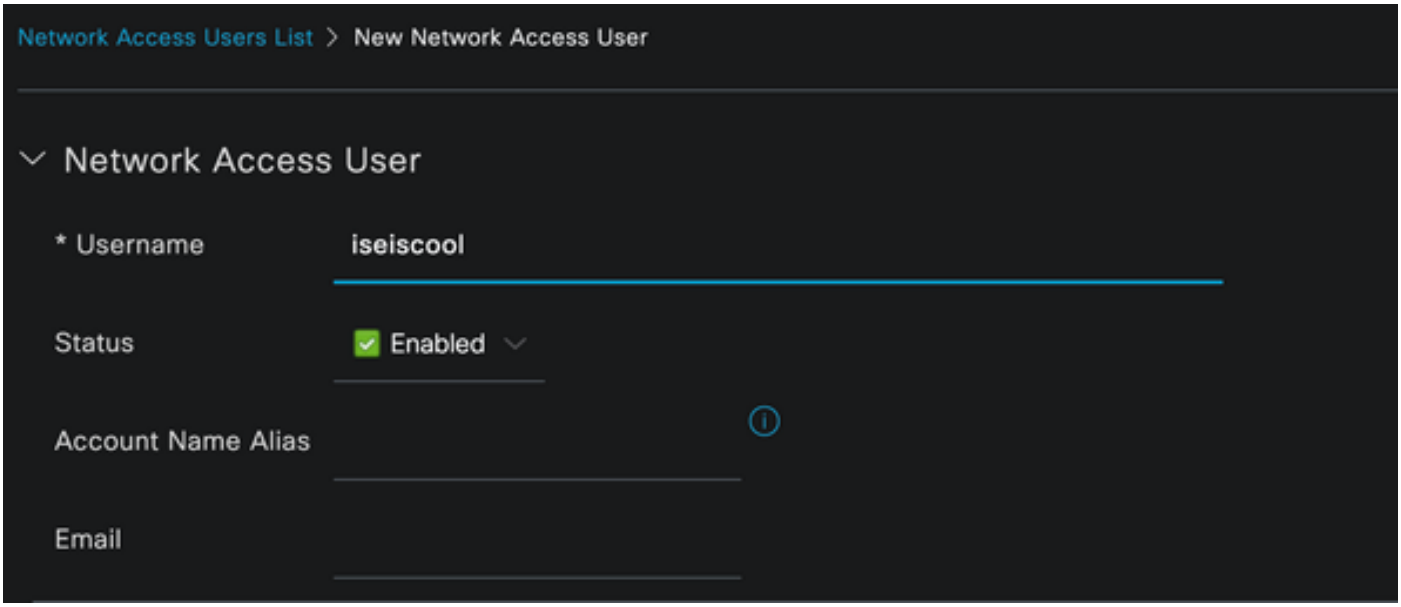
Passare a Amministrazione > Gestione delle identità > Scheda Identità.

Fare clic su Add.



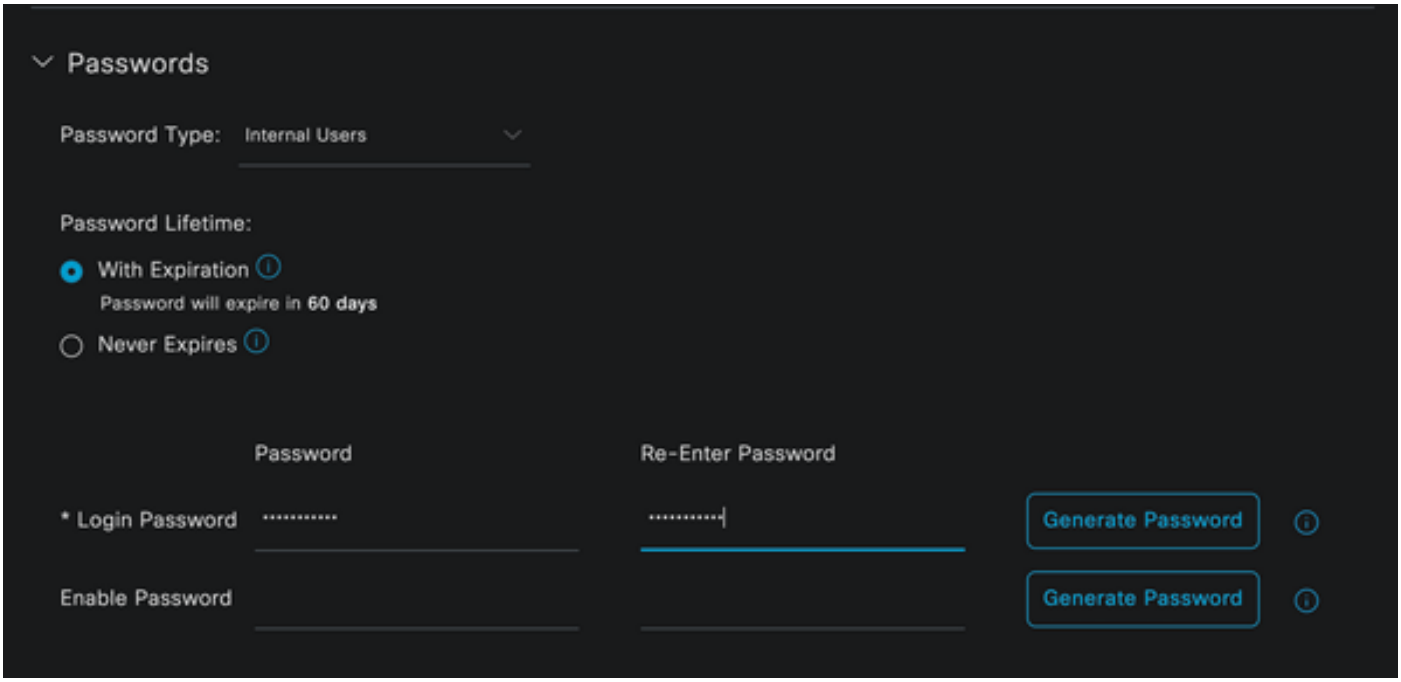
Sezione Utenti accesso alla rete

I campi obbligatori iniziano con il nome dell'utente. Nell'esempio riportato viene utilizzato il nome utente iseiscool.



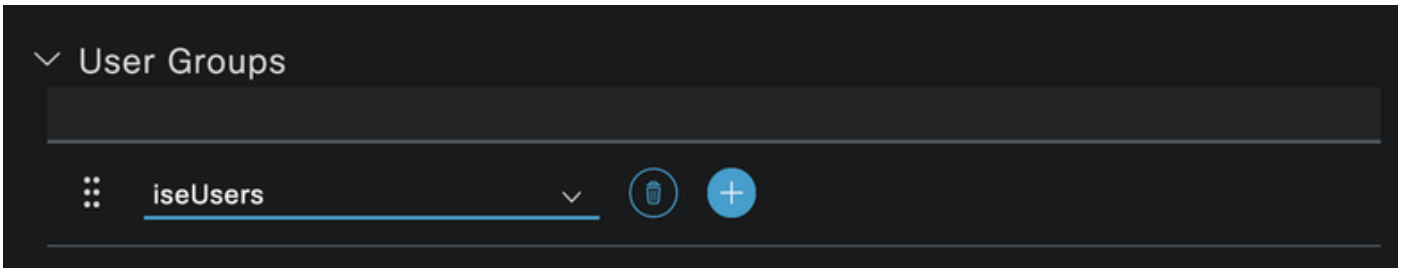
Creazione utente di accesso alla rete

Assegnare una password all'utente. Si utilizza VainillaISE97.



Sezione Password di creazione utente

Assegnare l'utente al gruppo iseUsers.

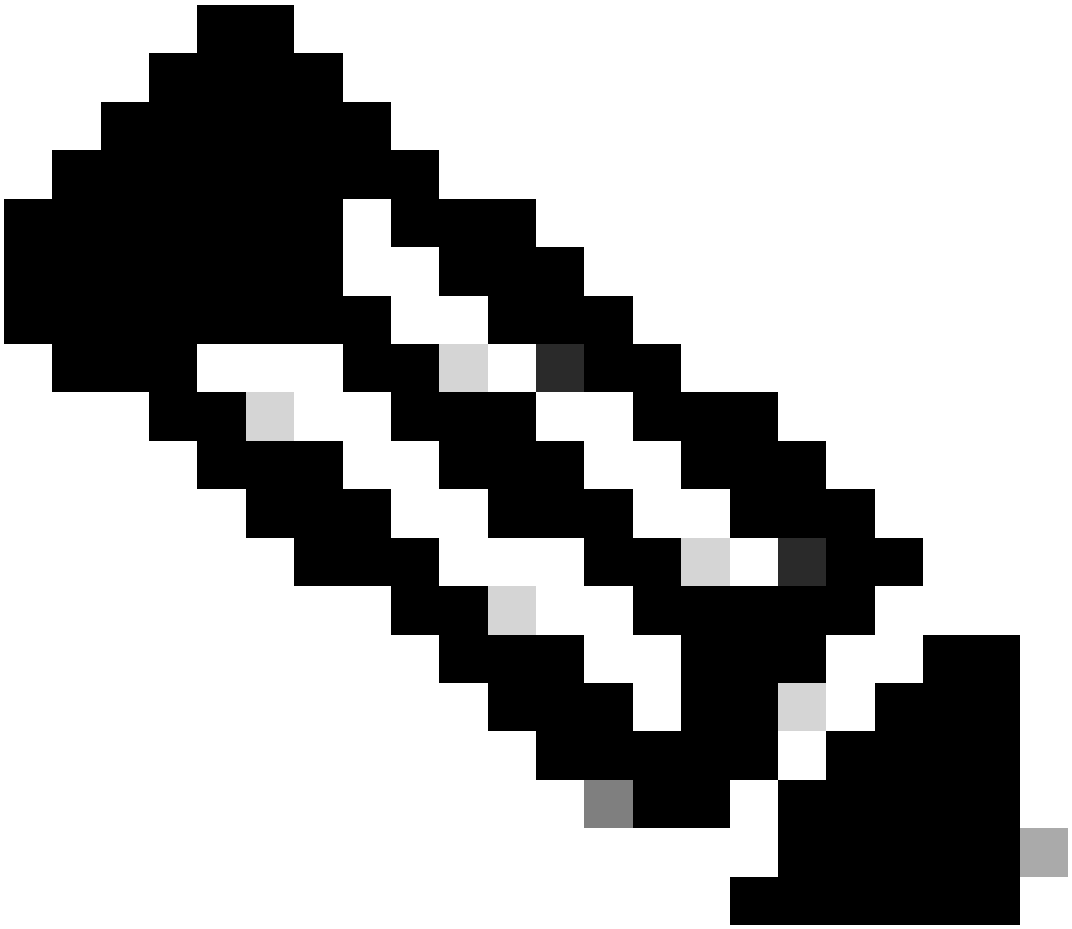


Assegnazione gruppo utenti

Configurare il set di criteri.

Selezionare Menu ISE > Policy > Policy Sets.

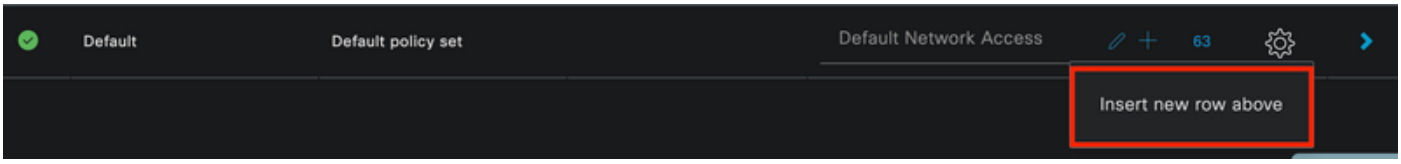
È possibile utilizzare il set di criteri predefinito. Tuttavia, per questo esempio viene creato un elemento denominato Wired.



Nota: la classificazione e la differenziazione dei set di criteri facilita la risoluzione dei problemi,

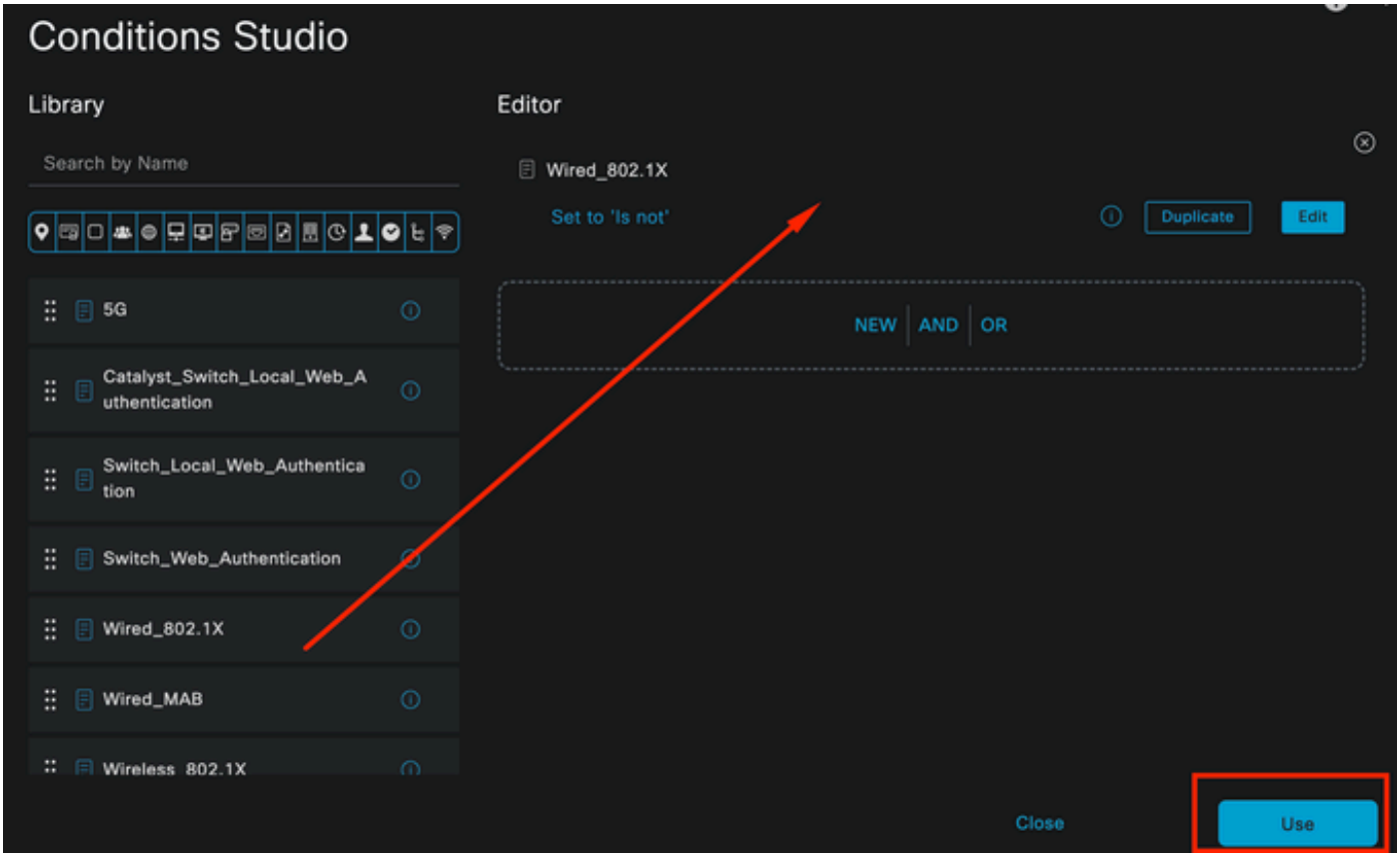
---

Nota: se l'icona Aggiungi o Più non è visibile, è possibile fare clic sull'icona Ingranaggio di qualsiasi set di criteri, quindi selezionare Inserisci nuova riga sopra.



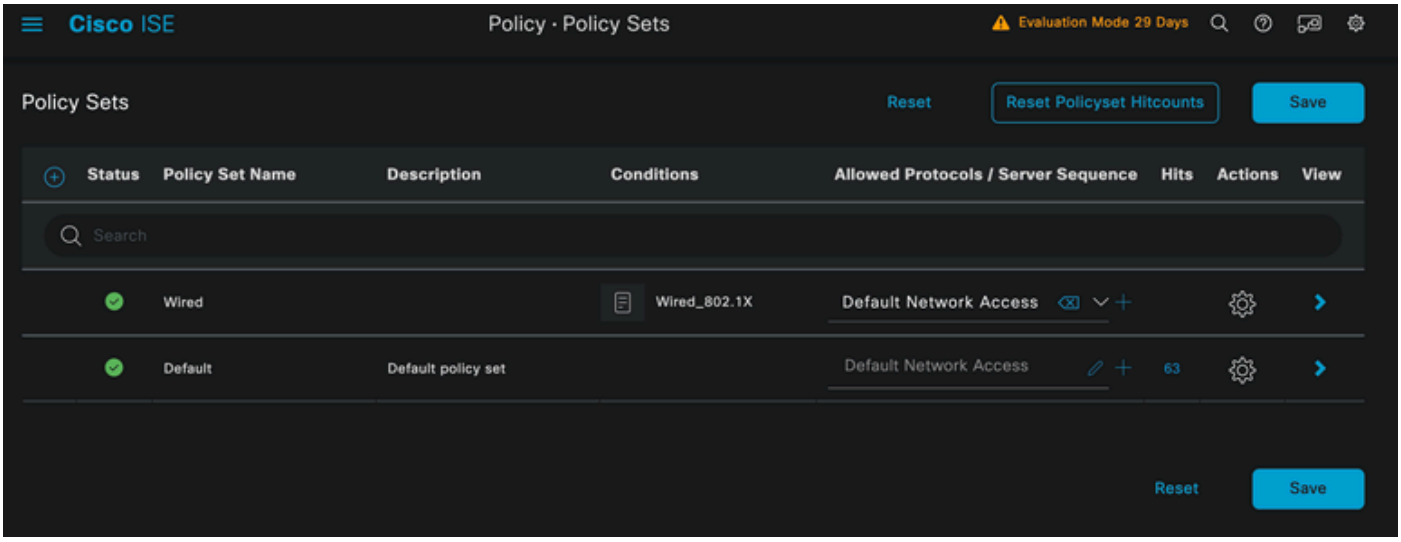
Opzioni icona ingranaggio

La condizione utilizzata è Wired 8021x. Trascinarlo, quindi fare clic su Usa.



Studio condizione criteri di autenticazione

Selezionare Accesso alla rete predefinito nella sezione Protocolli consentiti.

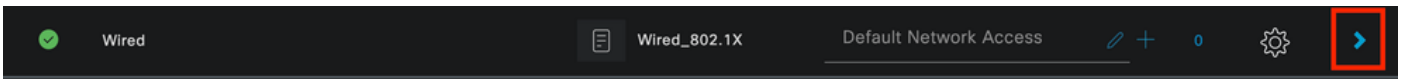


Visualizzazione generale set di criteri

Fare clic su Save (Salva).

2.d. Configurare i criteri di autenticazione e autorizzazione.

Fare clic sull'icona >.



Set di criteri per reti cablate

Espandere la sezione Criteri di autenticazione.

Fare clic sull'icona +.

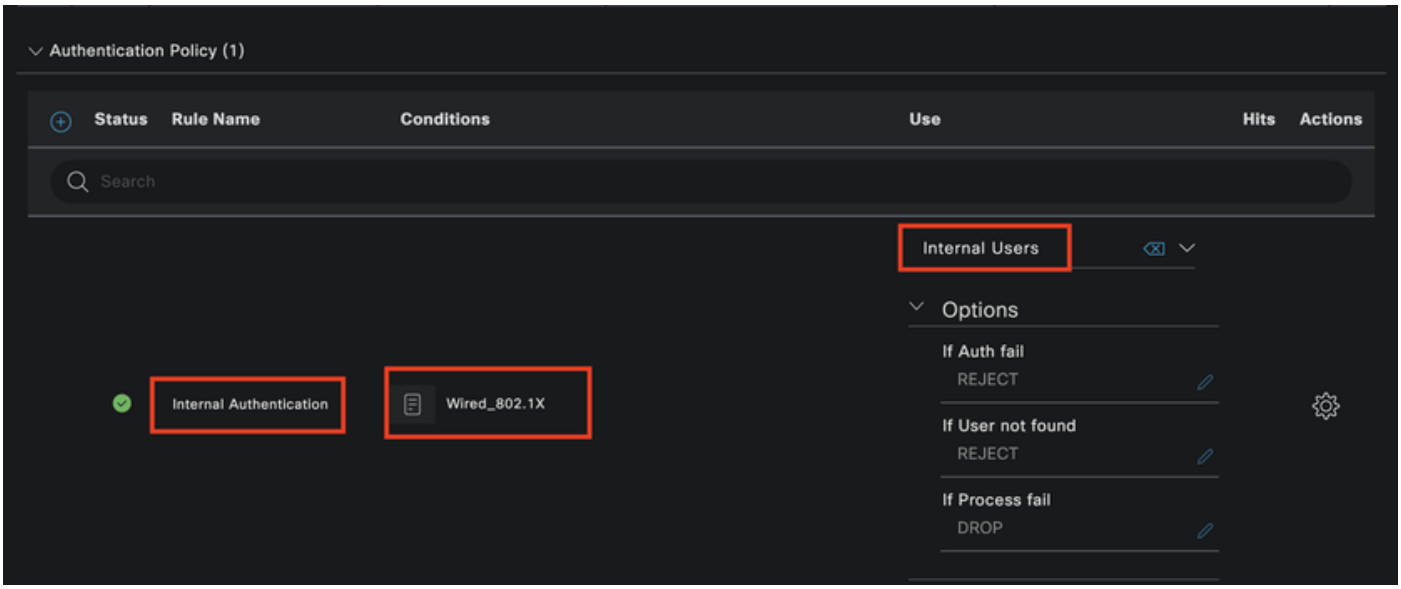
Criterio di autenticazione

Assegnare un nome al criterio di autenticazione. Nell'esempio viene utilizzata l'autenticazione interna.

Fare clic sull'icona + nella colonna Condizioni per questo nuovo criterio di autenticazione.

Viene utilizzata la condizione preconfigurata Wired Dot1x.

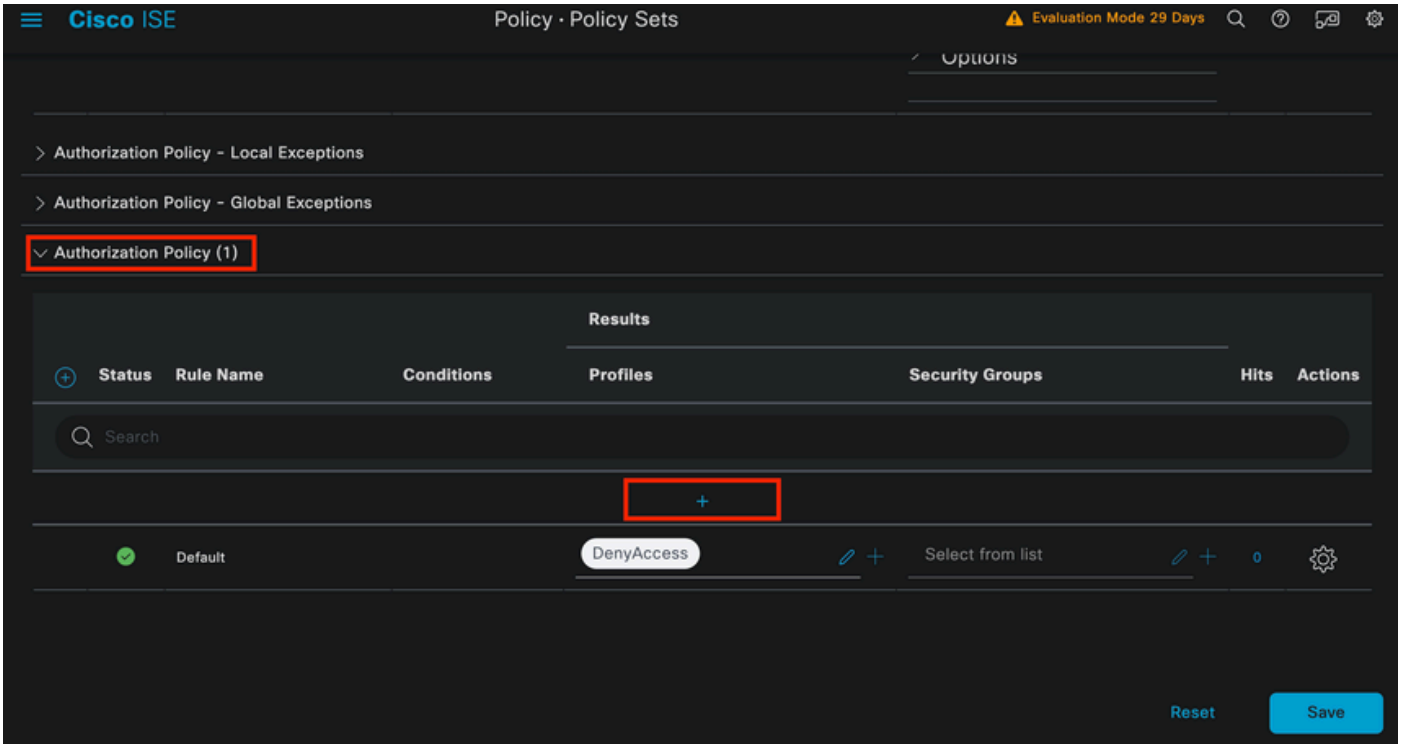
Infine, nella colonna Utilizza selezionare Utenti interni.



Criterio di autenticazione

Criteri di autorizzazione.

La sezione Criteri di autorizzazione si trova nella parte inferiore della pagina. Espanderlo e fare clic sull'icona +.



Criteri di autorizzazione

Assegnare un nome al criterio di autorizzazione creato di recente. Nell'esempio di configurazione, viene usato il nome Internal ISE Users.

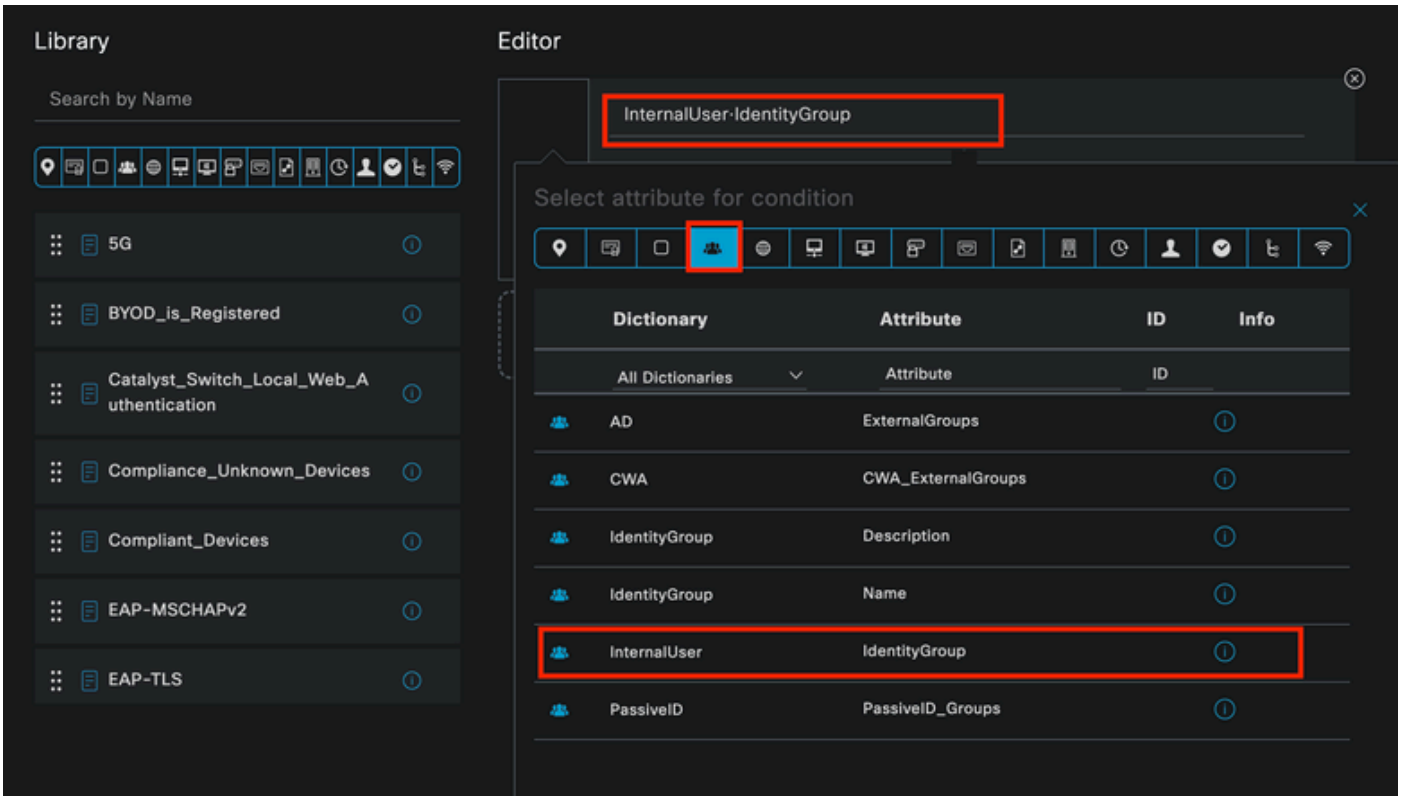
Per creare una condizione per il criterio di autorizzazione, fare clic sull'icona + nella colonna Condizioni.

Viene utilizzato il gruppo IseUsers.

Fare clic sulla sezione Attributo.

Selezionare l'icona IdentityGroup.

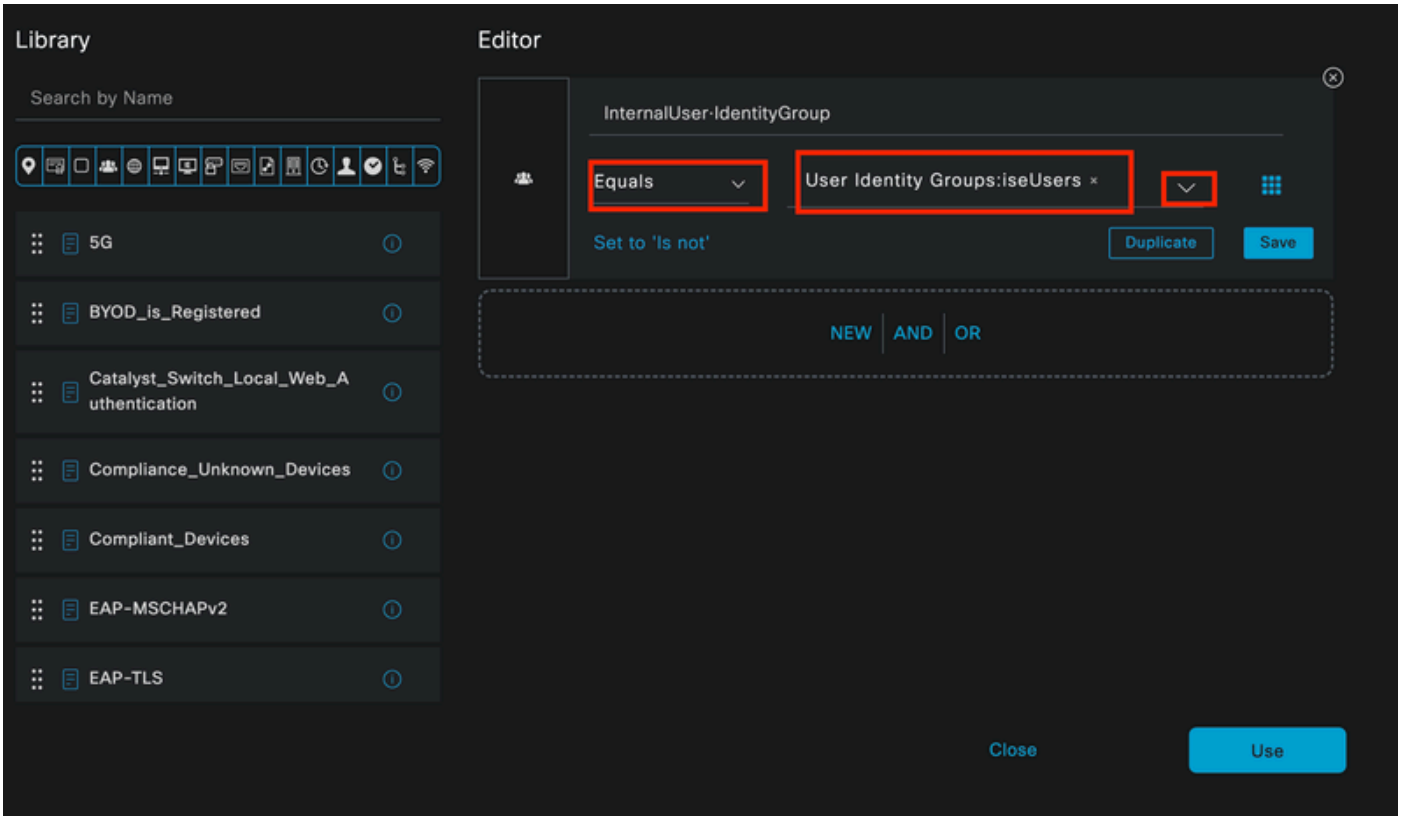
Dal dizionario selezionare il dizionario InternalUser fornito con l'attributo IdentityGroup.



Creazione di condizioni

Selezionare l'operatore Uguale a.

In Gruppi identità utente, selezionare il gruppo IseUsers.

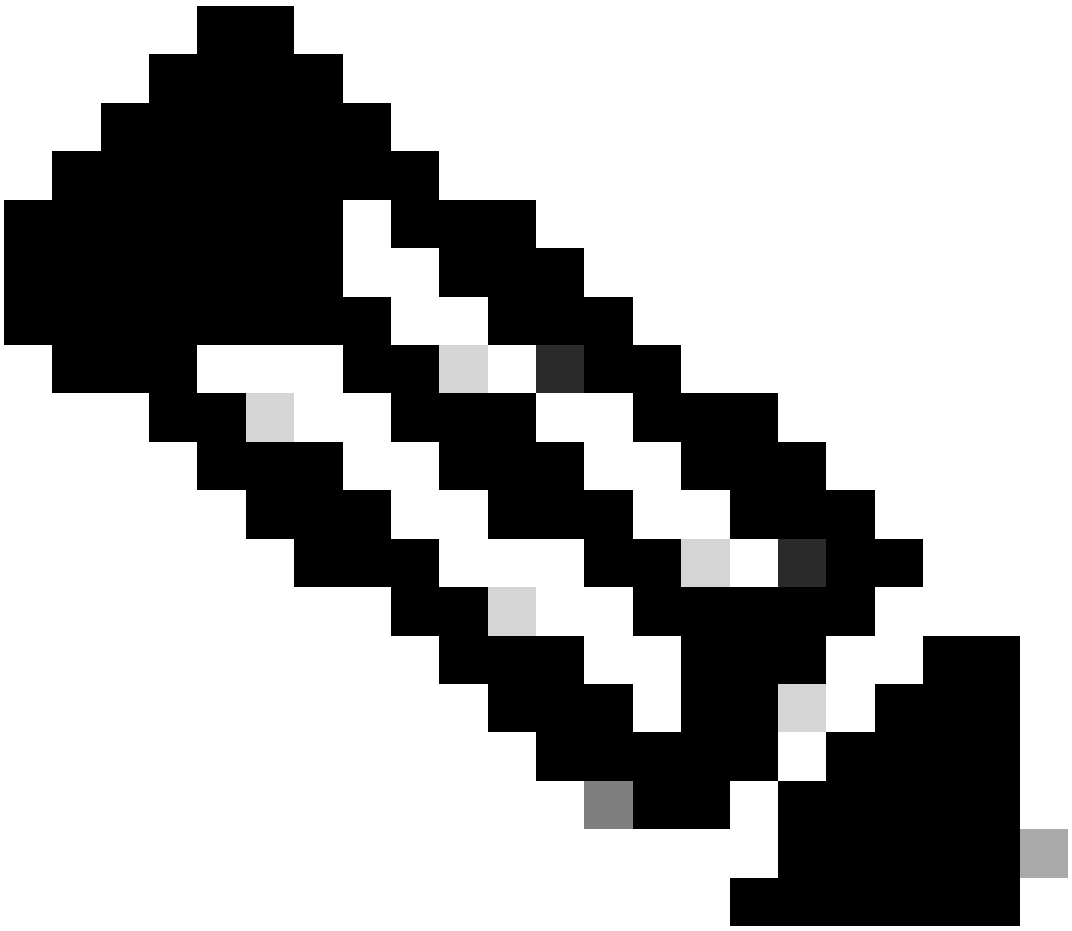


Creazione di condizioni

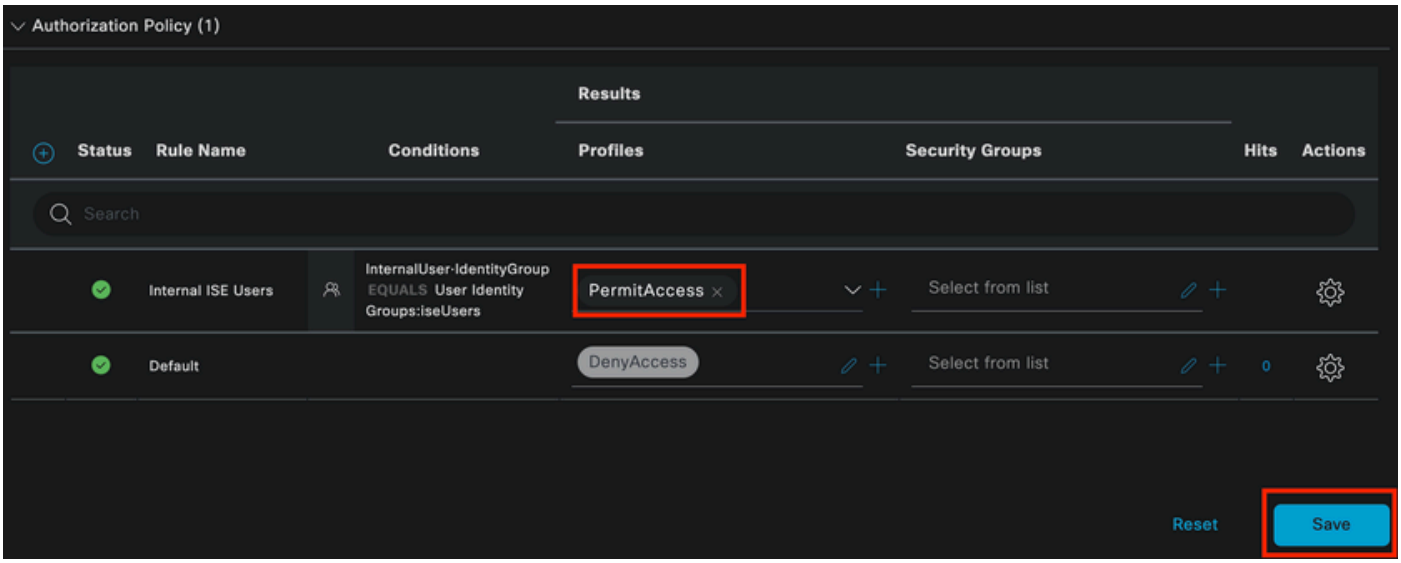
Fare clic su Usa.

Aggiungere il profilo di autorizzazione dei risultati.

Viene utilizzato il profilo preconfigurato Permit Access.



Nota: le autenticazioni che arrivano a ISE e che colpiscono questo set di criteri Dot1x cablato che non fanno parte del gruppo di identità utenti ISEUsers, raggiungono i criteri di autorizzazione predefiniti, che hanno il risultato DenyAccess.



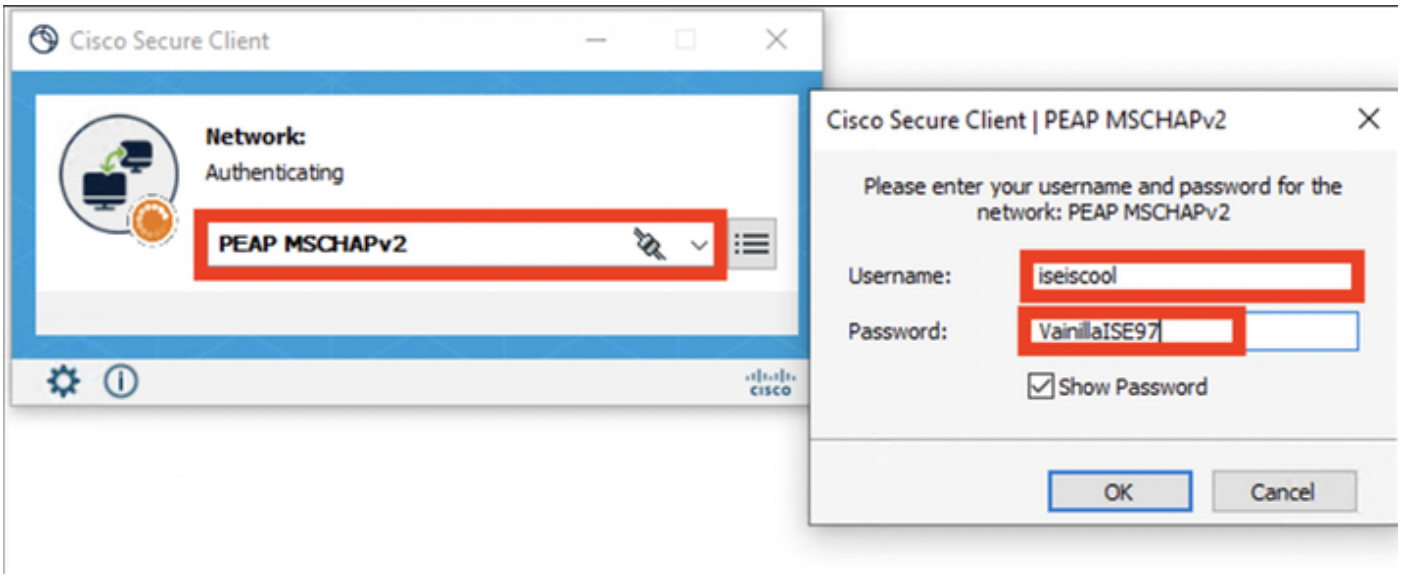
Criteri di autorizzazione

Fare clic su Save (Salva).

Verifica

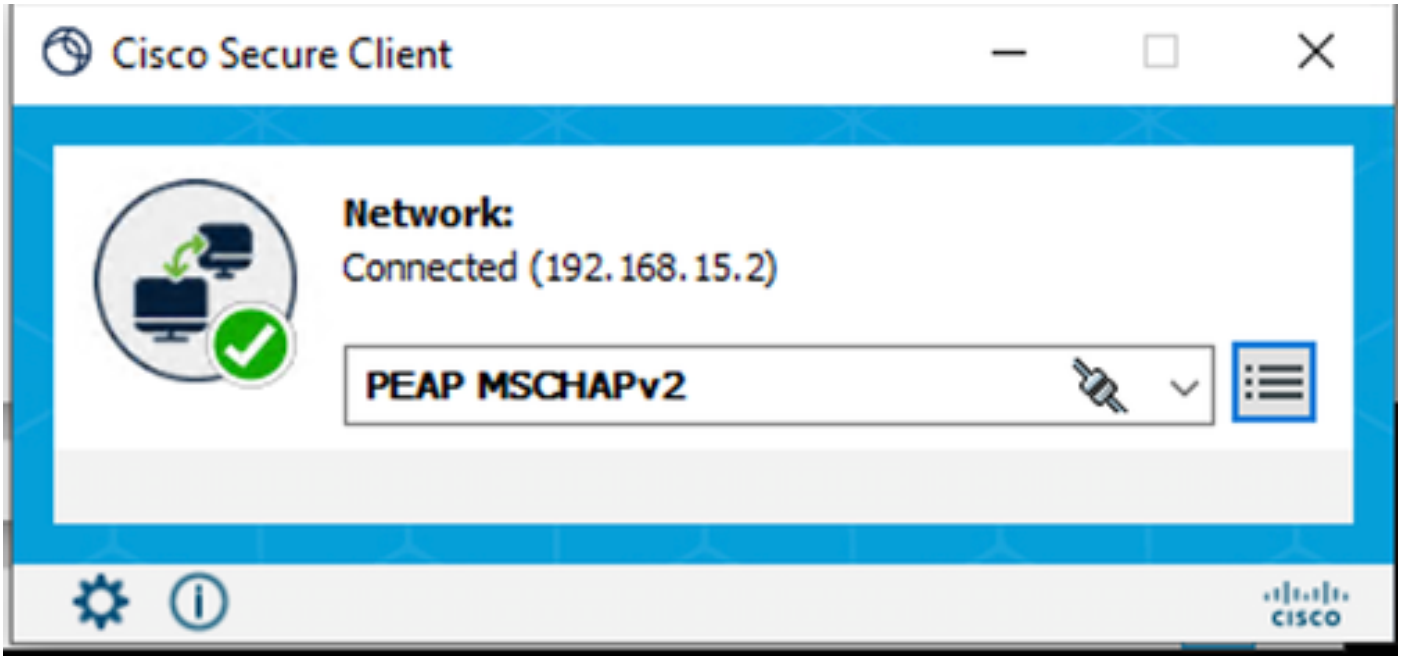
Al termine della configurazione, Secure Client richiede le credenziali e specifica l'utilizzo del profilo PEAP MSCHAPv2.

Verranno immesse le credenziali create in precedenza.



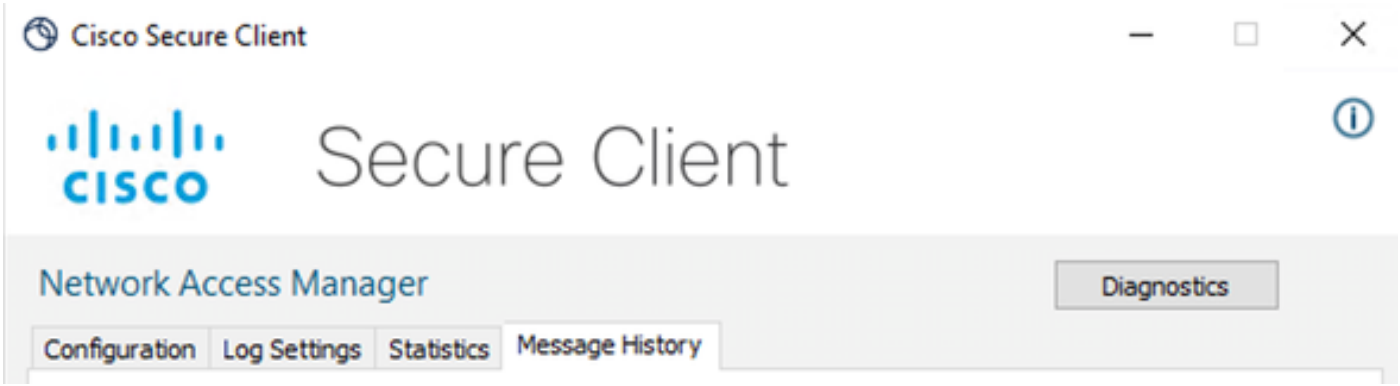
Secure Client NAM

Se l'endpoint viene autenticato correttamente,. NAM indica che è connesso.

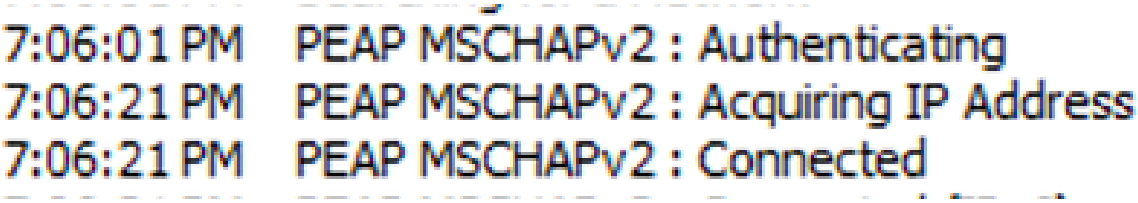


Secure Client NAM

Facendo clic sull'icona delle informazioni e passando alla sezione Cronologia messaggi, vengono visualizzati i dettagli di ogni passaggio eseguito da NAM.



Cronologia messaggi client sicuri



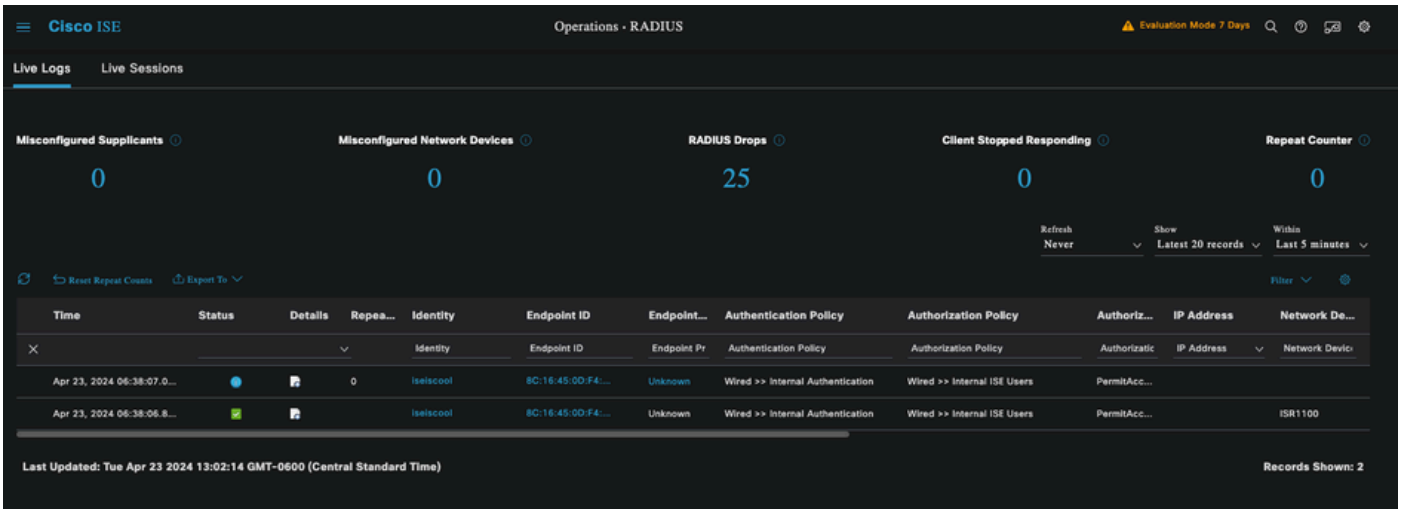
Cronologia messaggi client sicuri

Da ISE selezionare Operations > Radius LiveLogs per visualizzare i dettagli dell'autenticazione. Come mostrato nell'immagine seguente, viene visualizzato il nome utente utilizzato.

Altri dettagli sono:

- Timestamp (Data e ora).
- Indirizzo MAC.
- Set di criteri utilizzato.
- Criteri di autenticazione.

- Criteri di autorizzazione.
- Altre informazioni pertinenti.



Live log ISE RADIUS

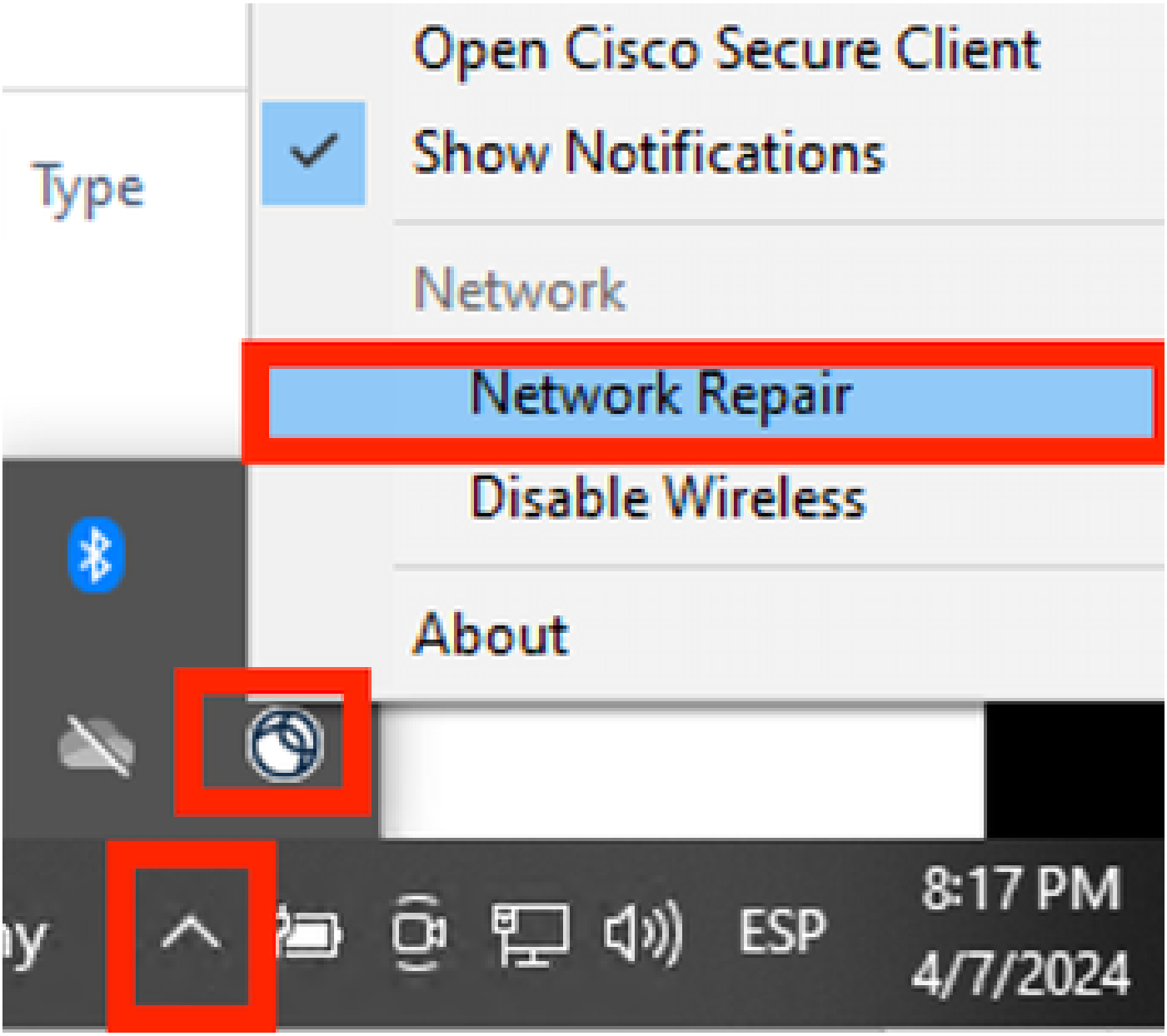
Dal momento che è possibile verificare che la configurazione rispetta i criteri corretti e che lo stato di autenticazione ha esito positivo, si può concludere che la configurazione è corretta.

Risoluzione dei problemi

Problema: il profilo NAM non è utilizzato da Secure Client.

Se il nuovo profilo creato nell'editor dei profili non è utilizzato da NAM, utilizzare l'opzione Ripristino configurazione di rete per Secure Client.

Per individuare questa opzione, spostarsi sulla barra di Windows > Fare clic sull'icona con la circonferenza > Fare clic con il pulsante destro del mouse sull'icona Secure Client > Fare clic su Ripristino rete.



Sezione Ripristino configurazione di rete

Problema 2: è necessario raccogliere i registri per un'ulteriore analisi.

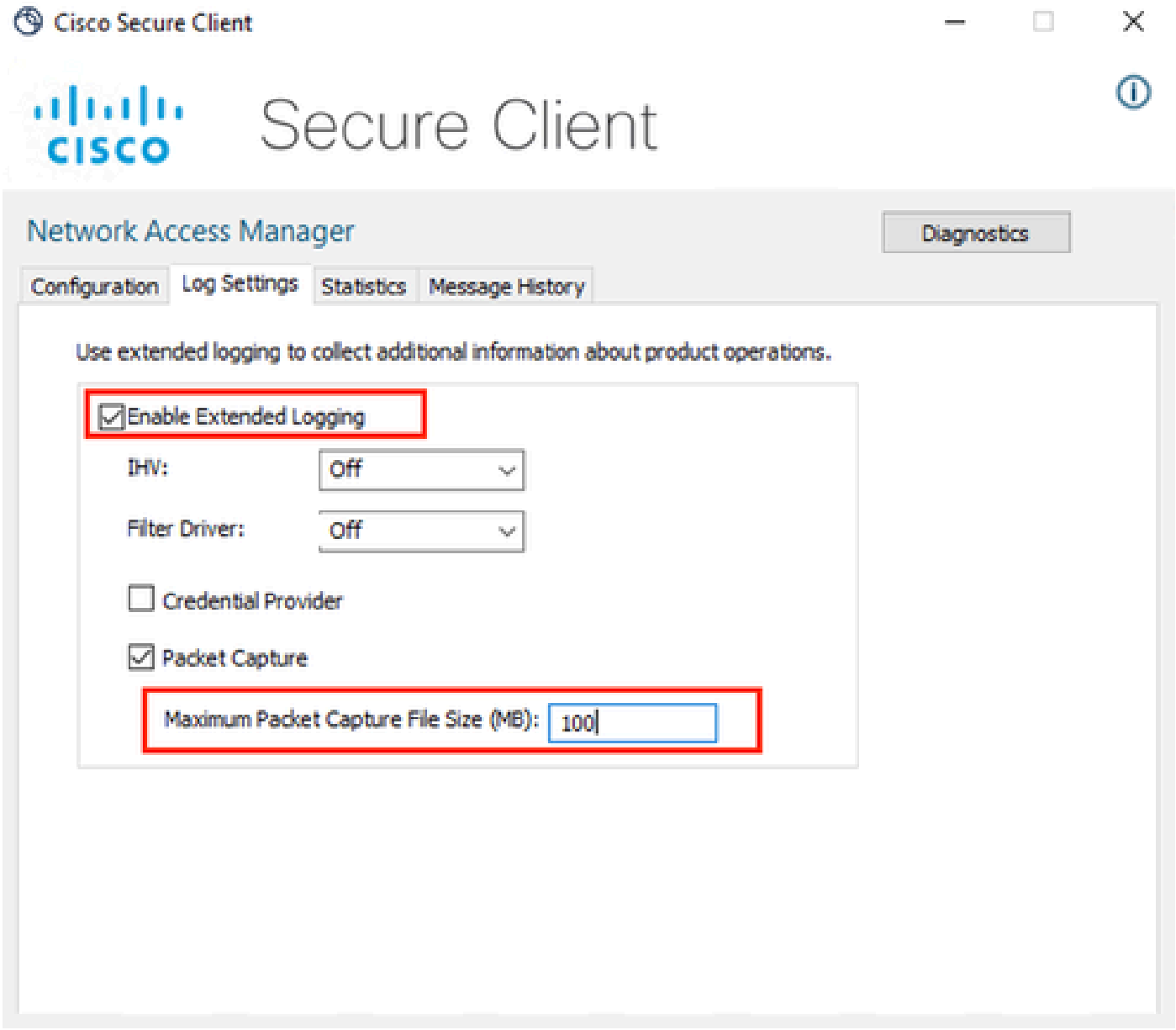
1. Abilita registrazione estesa NAM

Aprite NAM e fate clic sull'icona ingranaggio.

Interfaccia NAM

Passare alla scheda Impostazioni log. Selezionare la casella di controllo Abilita registrazione estesa.

Impostare Packet Capture File Size (Dimensioni file di acquisizione pacchetto) su 100 MB.



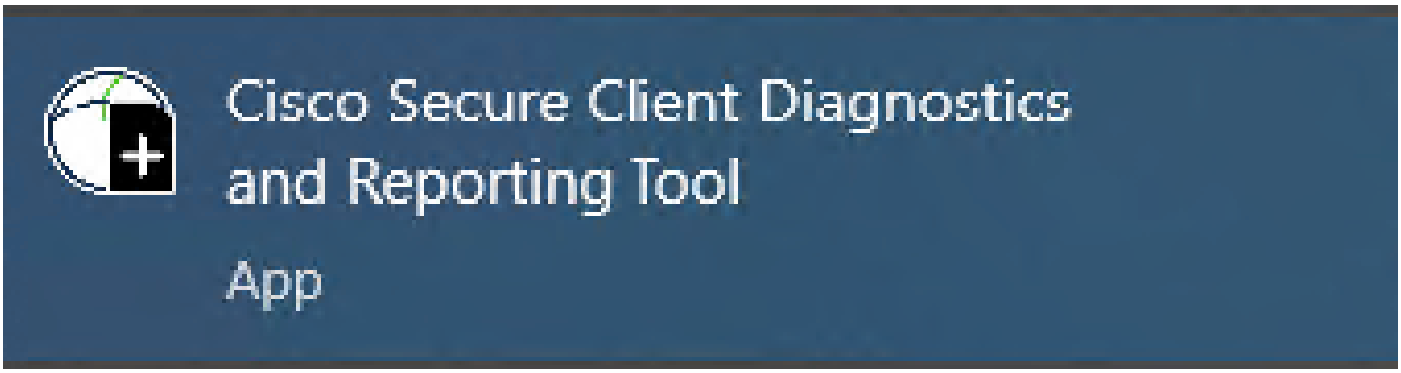
Impostazioni registro NAM client protetto

2. Riprodurre il problema.

Dopo aver abilitato la registrazione estesa, riprodurre il problema più volte per assicurarsi che i log vengano generati e che il traffico venga acquisito.

3. Raccogliere il bundle Secure Client DART.

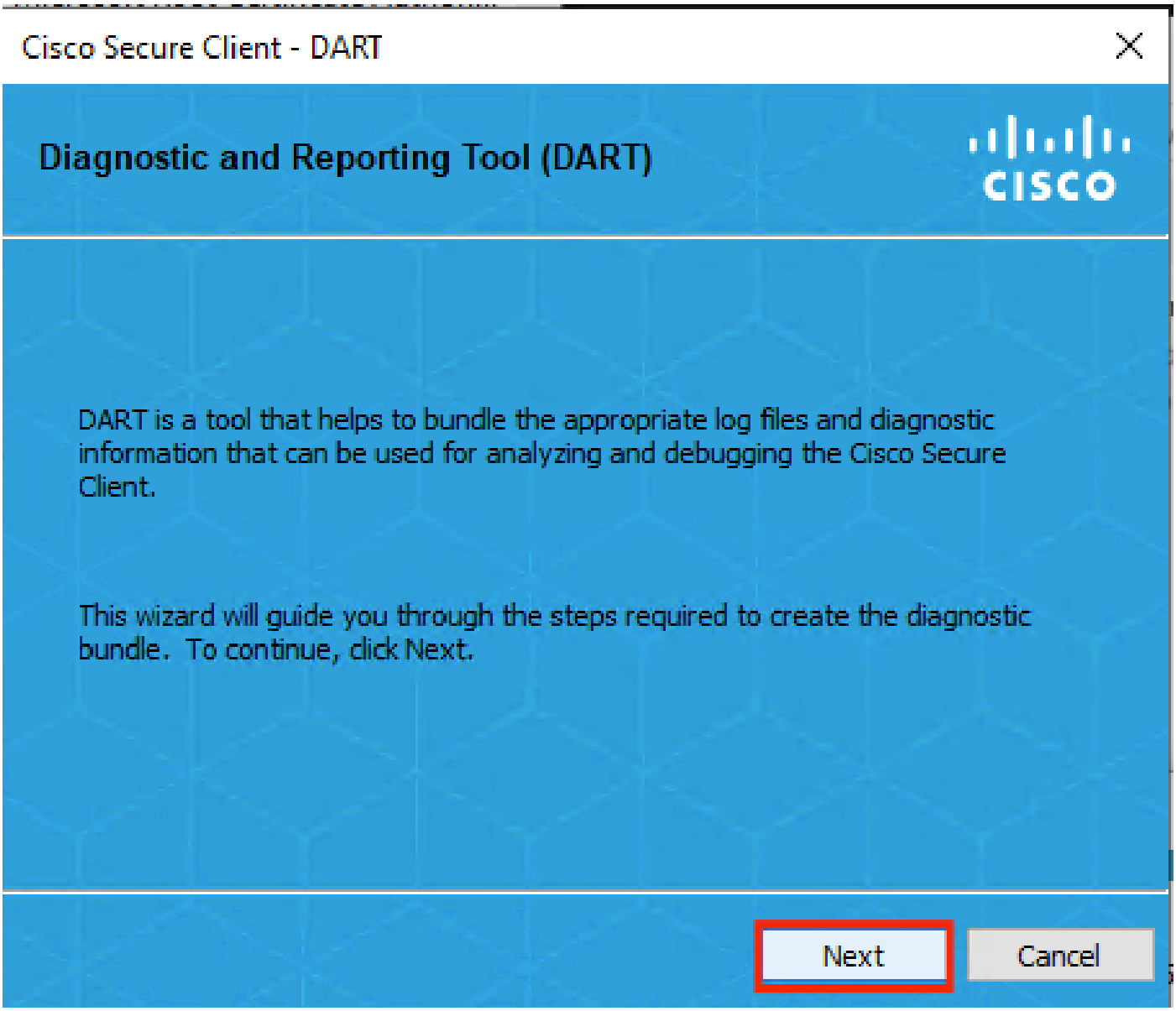
Da Windows, passare alla barra di ricerca e digitare Cisco Secure Client Diagnostics and Reporting Tool.



Modulo DART

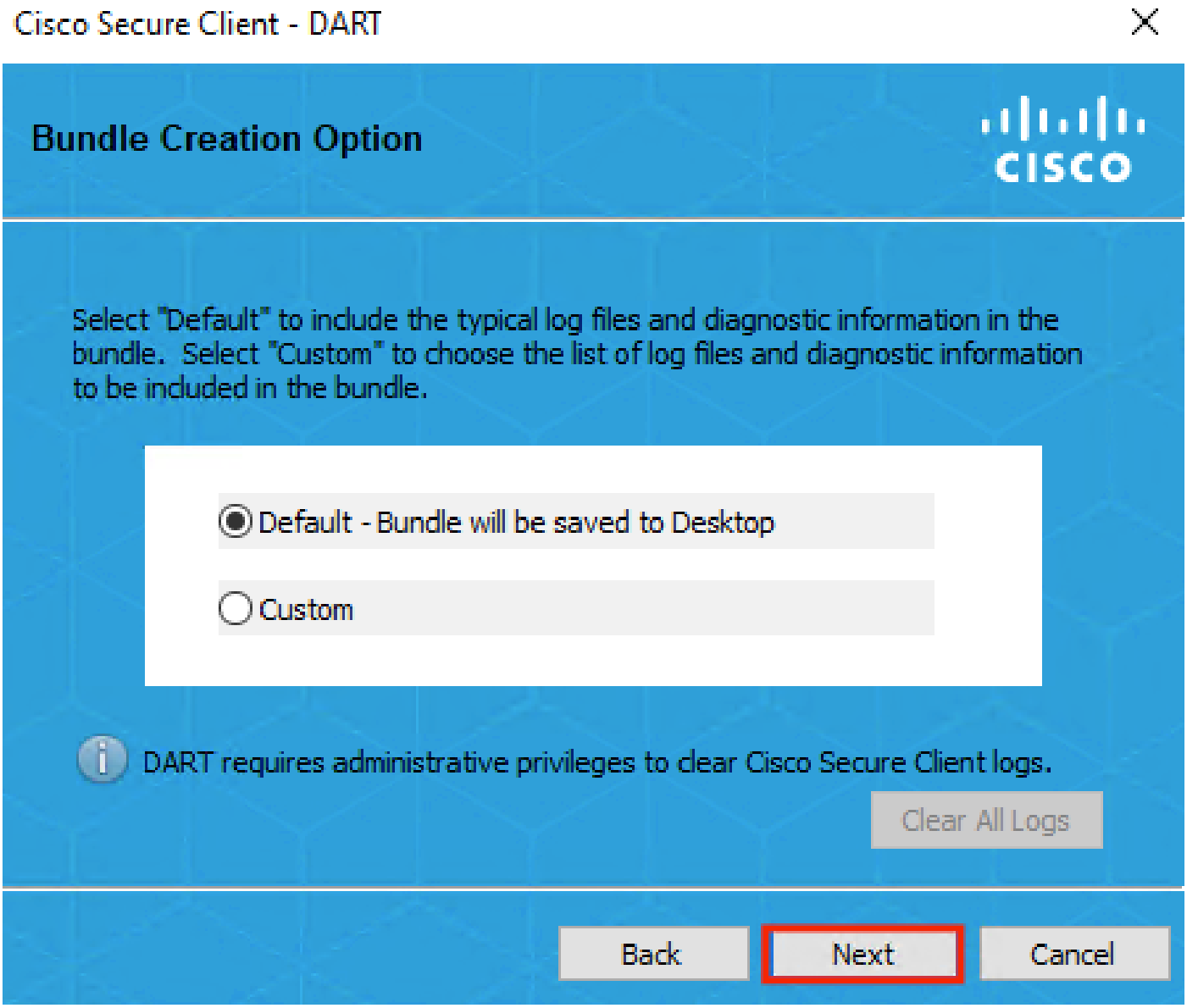
Durante il processo di installazione, è stato installato anche questo modulo. Si tratta di uno strumento che facilita il processo di risoluzione dei problemi raccogliendo i registri e le informazioni rilevanti sulla sessione dot1x.

Fare clic su Avanti nella prima finestra.



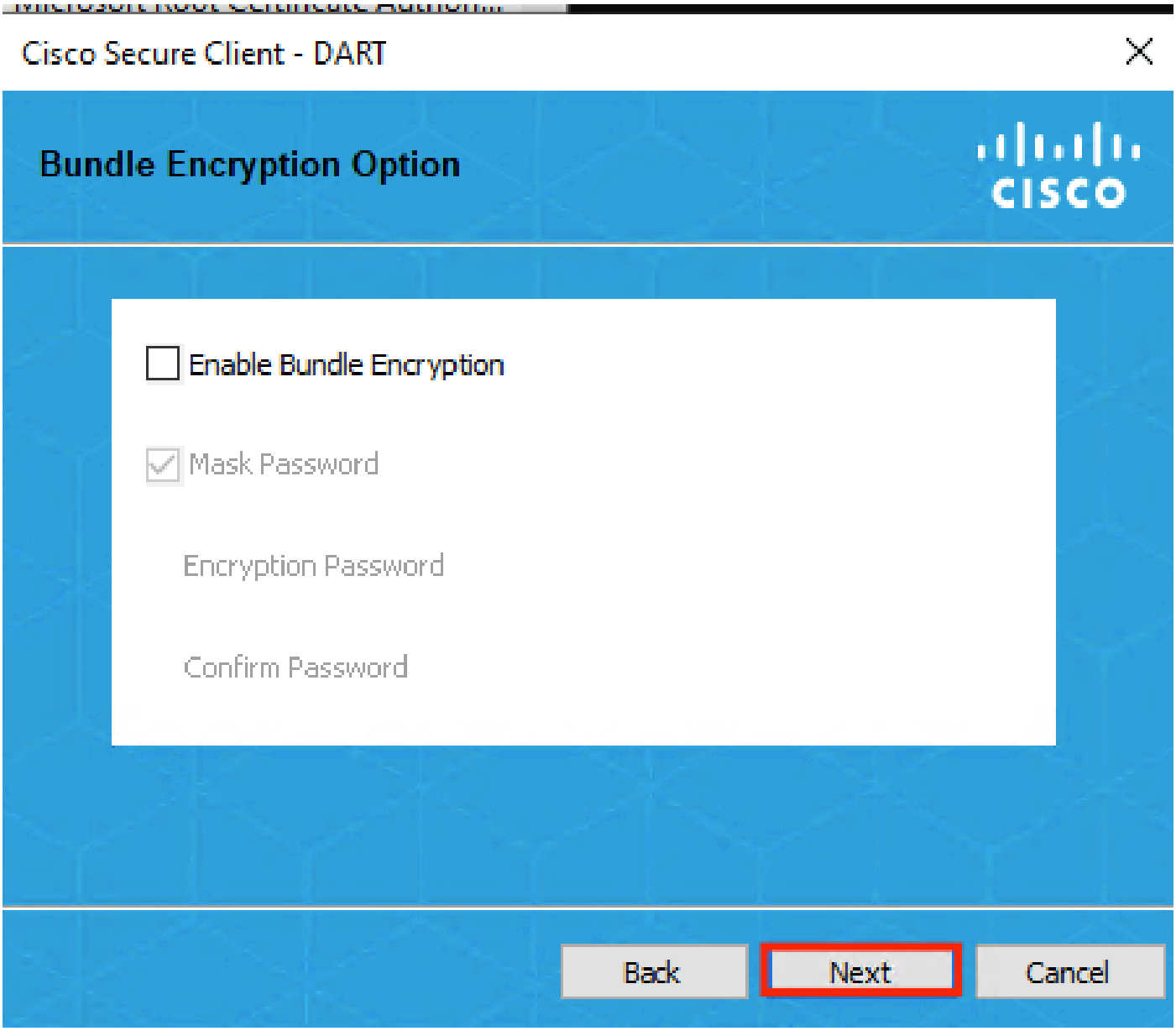
Modulo DART

Fare nuovamente clic su Avanti per salvare il bundle di log sul desktop.



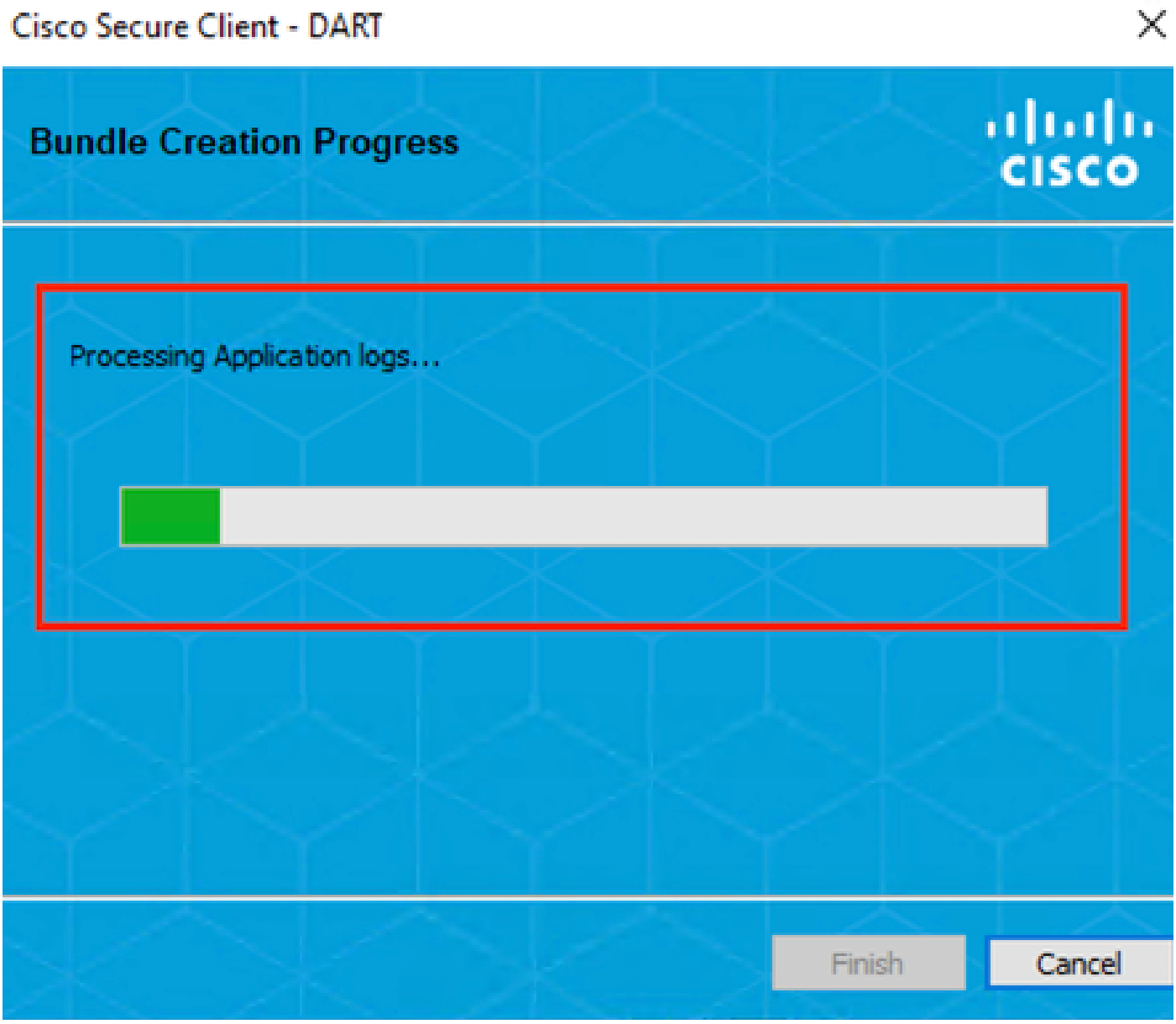
Modulo DART

Se necessario, selezionare la casella di spunta Enable Bundle Encryption (Abilita crittografia bundle).



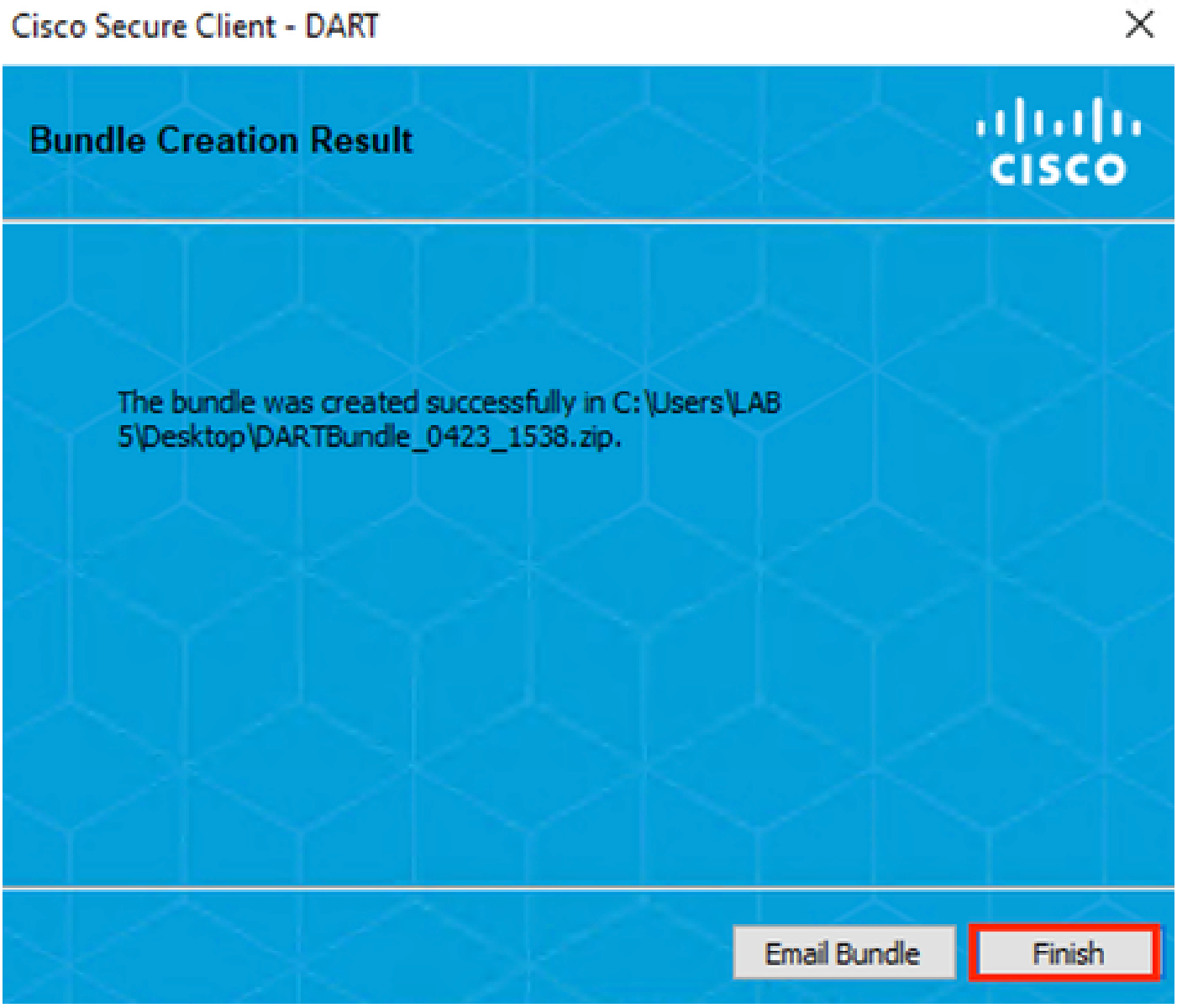
Modulo DART

Verrà avviata la raccolta di log DART.



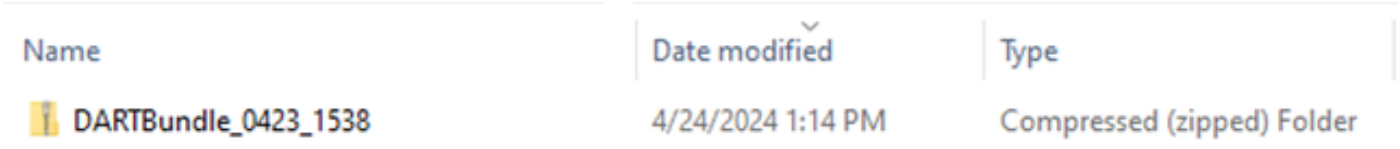
Raccolta di log DART

Possono essere necessari 10 minuti o più per completare il processo.



Risultato creazione bundle DART

Il file dei risultati DART è disponibile nella directory del desktop.



File di risultati DART

Informazioni correlate

- Supporto tecnico Cisco e download

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).