

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

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

- [1. Scaricare e installare Secure Client NAM \(Network Access Manager\)](#)
- [2. Scaricare e installare Secure Client NAM Profile Editor.](#)
- [3. Configurazioni generali predefinite](#)
- [4. Scenario 1: configurazione del richiedente Secure Client NAM per l'autenticazione utente PEAP \(MS-CHAPv2\)](#)
- [5. Scenario 2: configurazione del richiedente Secure Client NAM per l'autenticazione simultanea di computer e utente EAP-FAST](#)
- [6. Scenario 3: configurazione del richiedente Secure Client NAM per l'autenticazione del certificato utente EAP-TLS](#)
- [7. Configurare ISR 1100 e ISE in modo da consentire le autenticazioni basate sullo scenario 1 PEAP MSCHAPv2](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Problema: il profilo NAM non è utilizzato da Secure Client.](#)

[Problema 2: è necessario raccogliere i registri per un'ulteriore analisi.](#)

- [1. Abilita registrazione estesa NAM](#)
- [2. Riprodurre il problema.](#)
- [3. Raccogliere il bundle Secure Client DART.](#)

[Informazioni correlate](#)

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.

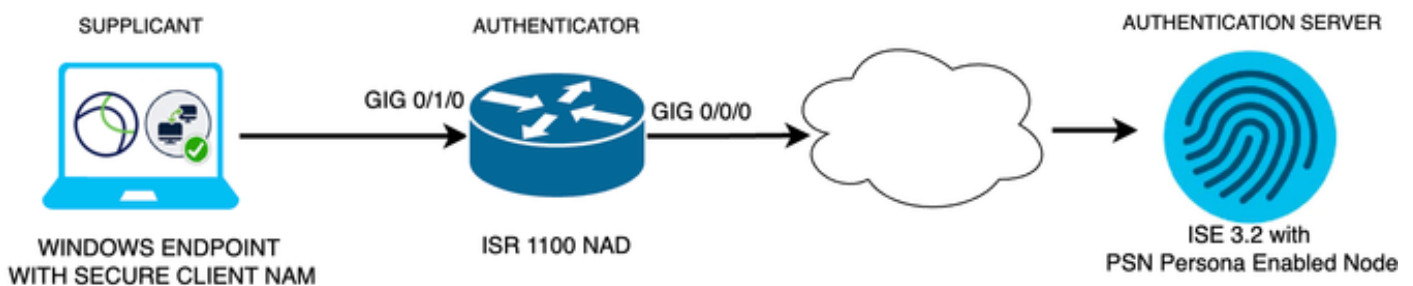
Network Access Manager è stato progettato per essere installato in un'unica postazione, in modo da consentire una sola connessione di rete alla volta. Inoltre, le connessioni cablate hanno una priorità più alta rispetto alle connessioni wireless, quindi se si è collegati alla rete con una connessione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















Cisco Secure Client Pre-Deployment Package (Windows) - includes individual MSI files  06-Feb-2024 108.30 MB  

[cisco-secure-client-win-5.1.2.42-predeploy-k9.zip](#)

[Advisories](#) 

File zip Msi

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

 Profiles	4/4/2024 7:16 PM
 Setup	4/4/2024 7:16 PM
 cisco-secure-client-win-1.182.3-thousandeyes-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-core-vpn-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-dart-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-iseposture-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-nam-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-nvm-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-posture-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-sbl-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.42-umbrella-predeploy-k9	4/4/2024 7:16 PM
 cisco-secure-client-win-5.1.2.5191-zta-predeploy-k9	4/4/2024 7:16 PM
 Setup	4/4/2024 7:16 PM
 setup	4/4/2024 7:16 PM

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.

Select the Cisco Secure Client 5.1.2.42 modules you wish to install:

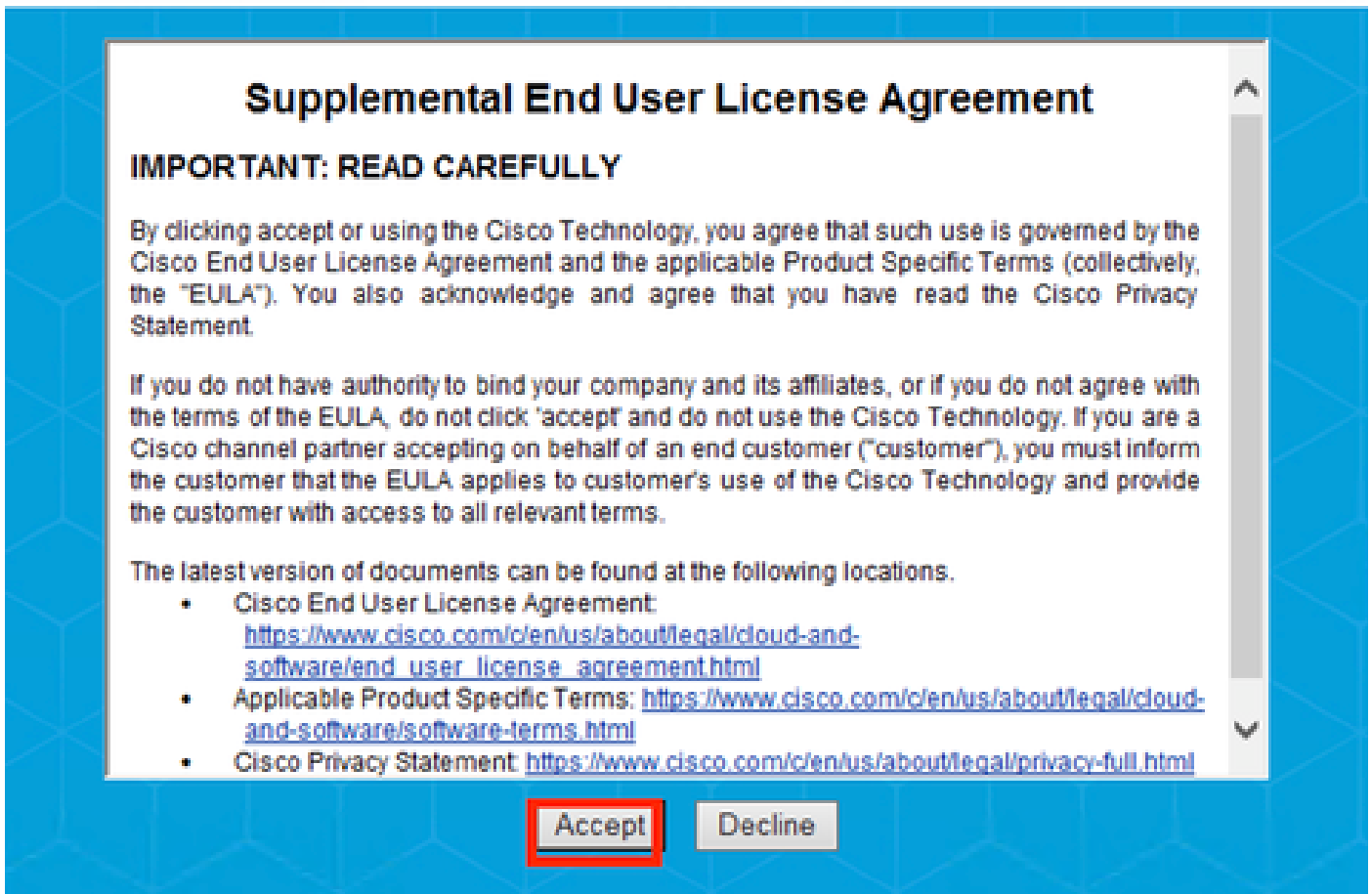
- Core & AnyConnect VPN
- Start Before Login
- Network Access Manager
- Secure Firewall Posture
- Network Visibility Module
- Umbrella
- ISE Posture
- ThousandEyes
- Zero Trust Access
- Select All
- Diagnostic And Reporting Tool
- Lock Down Component Services

Install Selected

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.

Cisco Secure Client Install Selector

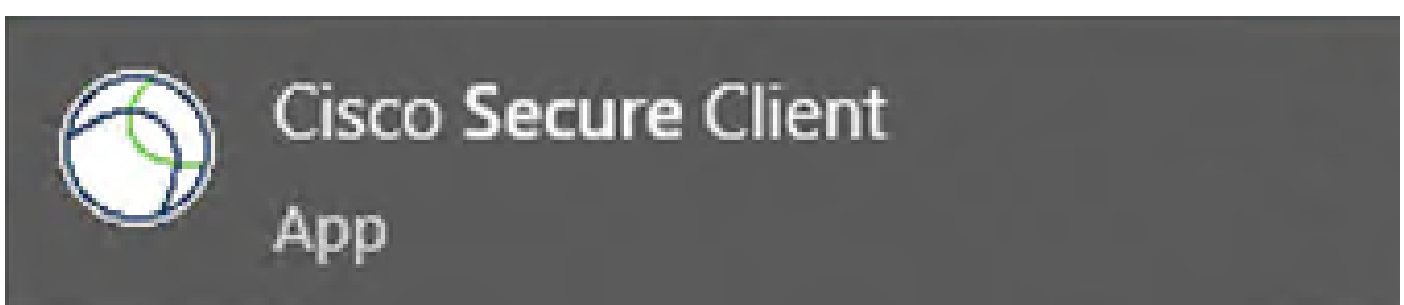


You must reboot your system for the installed changes to take effect.

OK

Finestra Requisiti per il riavvio

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

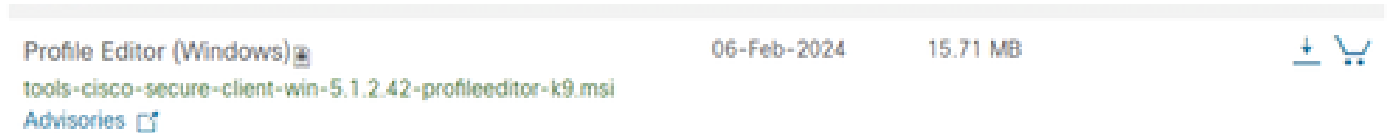


2. Scaricare e installare Secure Client NAM Profile Editor.

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.

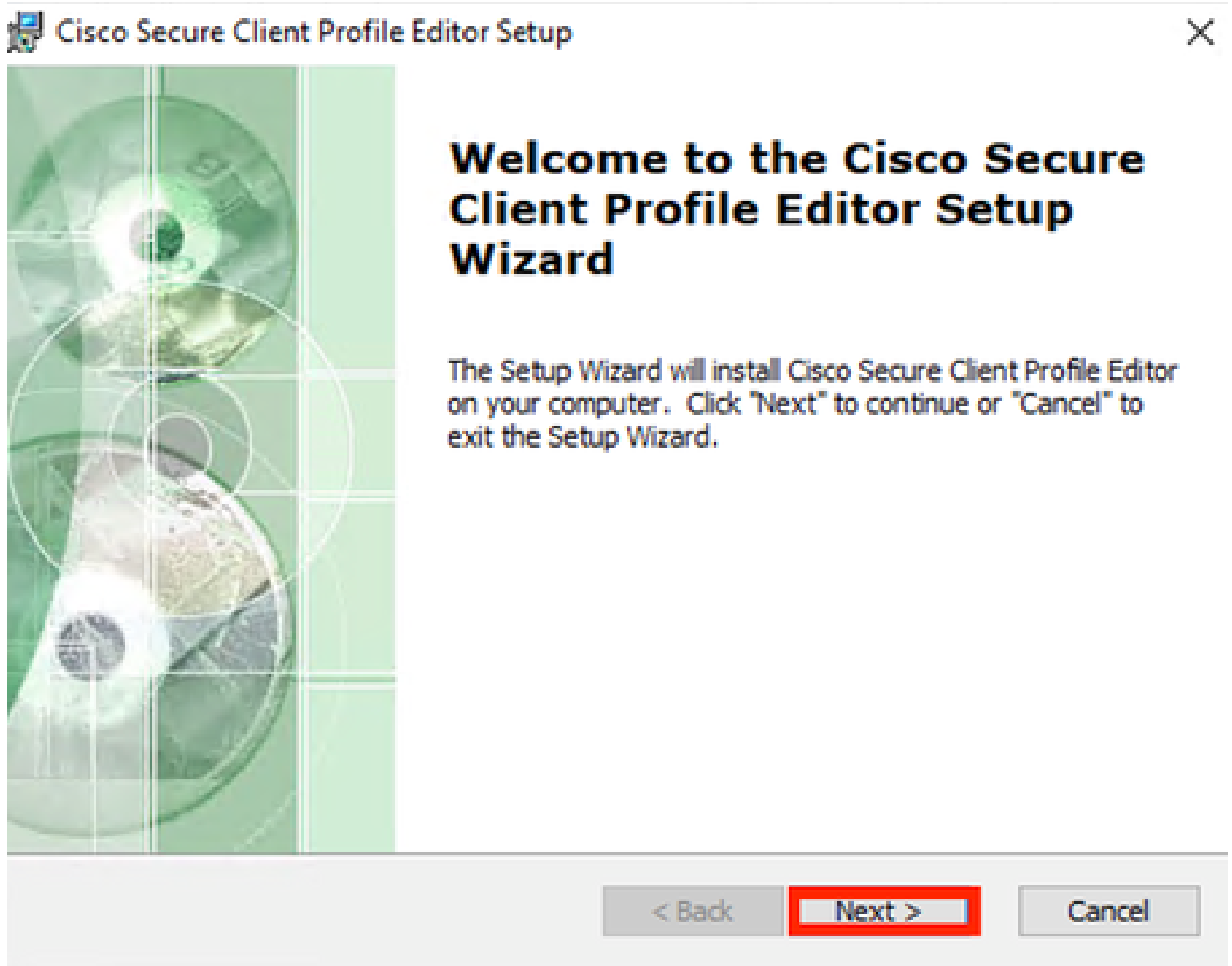
In questo esempio viene utilizzata l'opzione con la versione 5.1.2.42.



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.

Cisco Secure Client Profile Editor Setup

Choose Setup Type

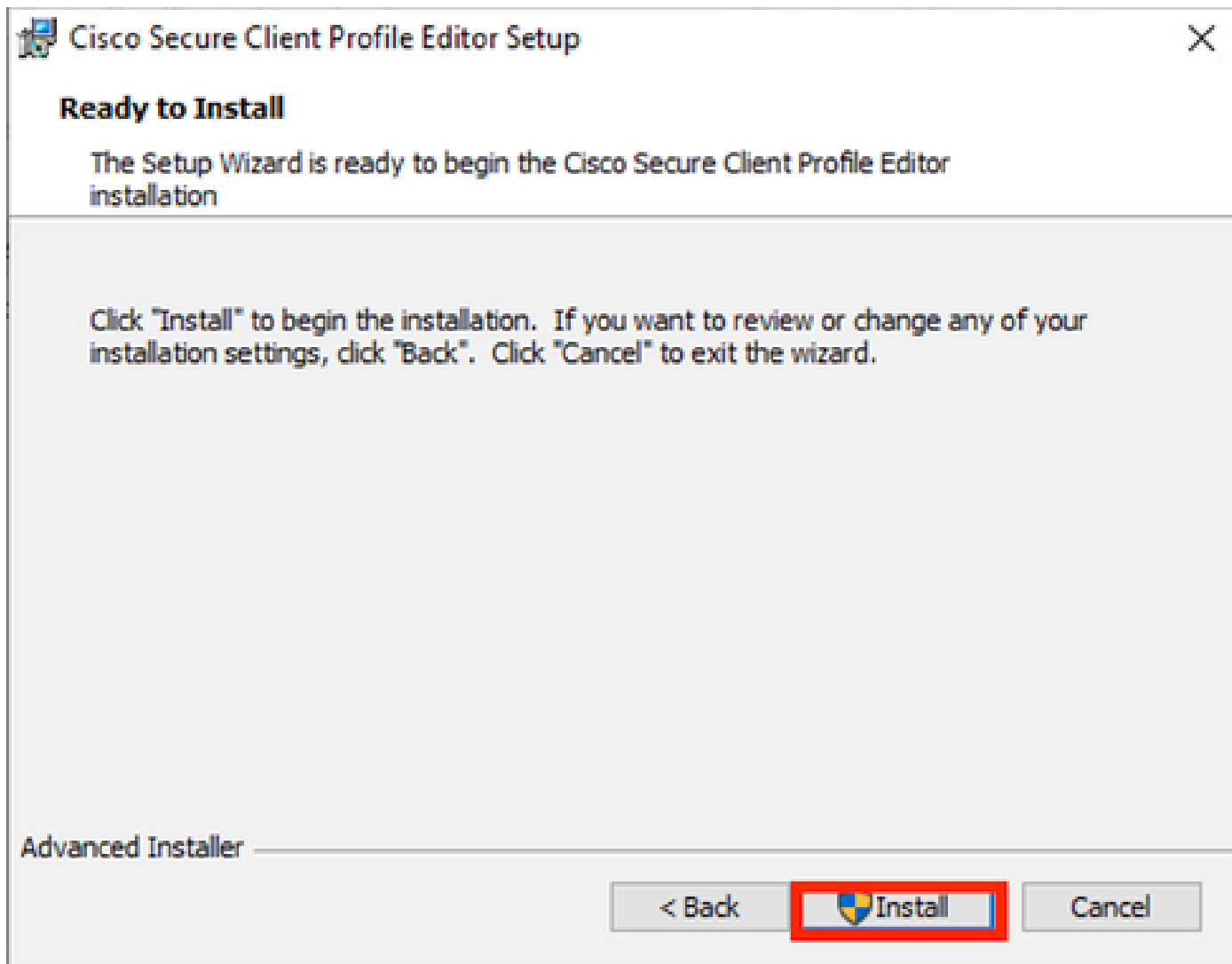
Choose the setup type that best suits your needs

	Typical Installs the most common program features. Recommended for most users.
	Custom Allows users to choose which program features will be installed and where they will be installed. Recommended for advanced users.
	Complete All program features will be installed. (Requires most disk space)

Advanced Installer

< Back Next > Cancel

Installazione dell'Editor di profili



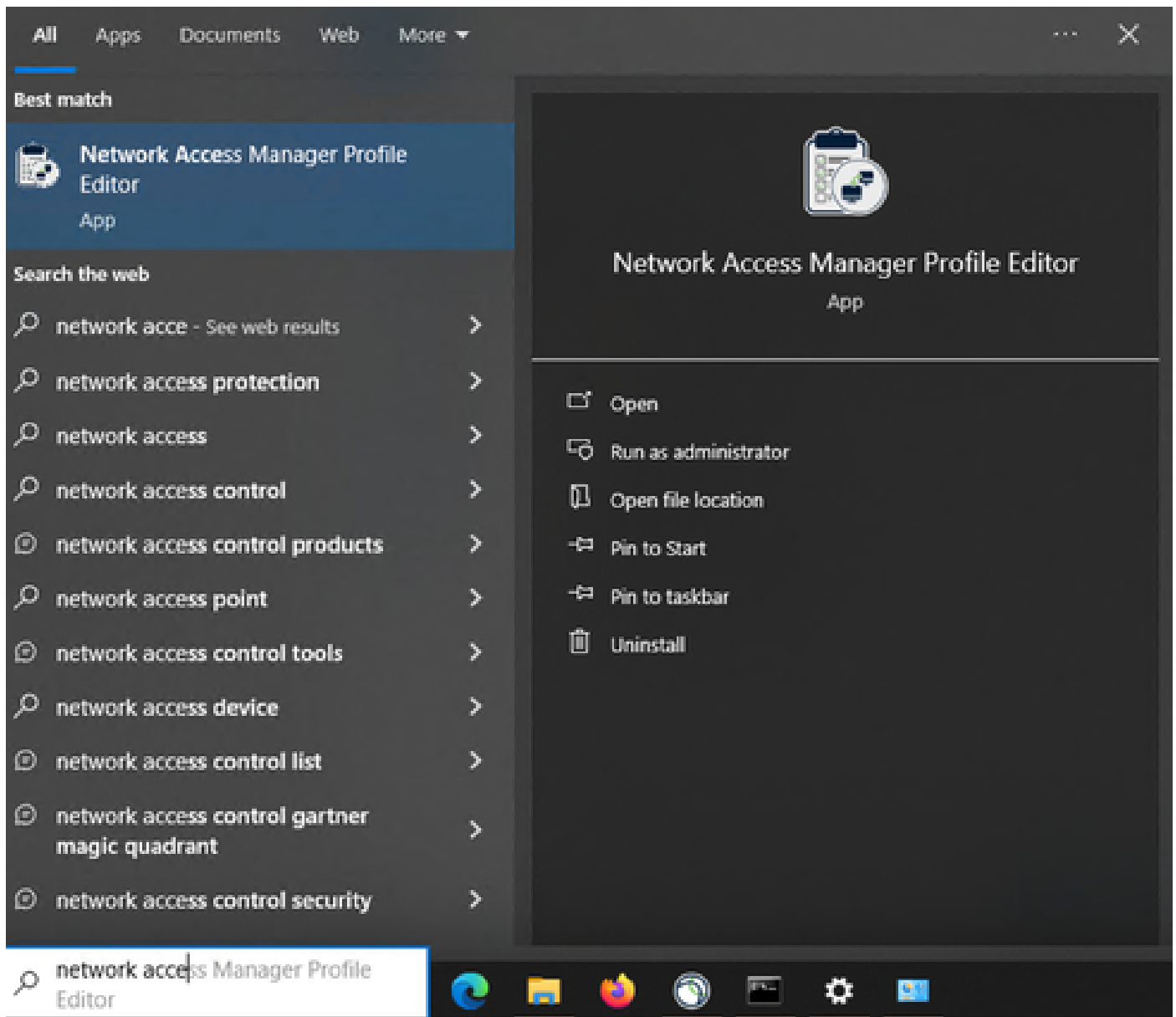
Finestra di installazione

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

- Network Access Manager
 - Client Policy
 - Authentication Policy
 - Networks
 - Network Groups

Client Policy

Profile: Untitled

Connection Settings

Default Connection Timeout (sec.)

Connection Attempt:

Before user logon

Time to wait before allowing user to logon (sec.)

After user logon

Media

Manage Wi-Fi (wireless) Media

Enable validation of WPA/WPA2/WPA3 handshake

Enable Randomized MAC Address

Default Association Timeout (sec.)

Manage Wired (802.3) Media

Manage Mobile Broadband (3G) Media

Enable Data Roaming

End-user Control

Allow end-user to:

Disable Client Select machine connection type

Display user groups Enable by default

Specify a script or application to run when connected

Auto-connect

Administrative Status

Service Operation Enable Disable

FIPS Mode Enable Disable

Captive Portal Detection Enable Disable

Criteria client Editor profili NAM

Authentication PolicyProfile: **Untitled**

Allow Association Modes

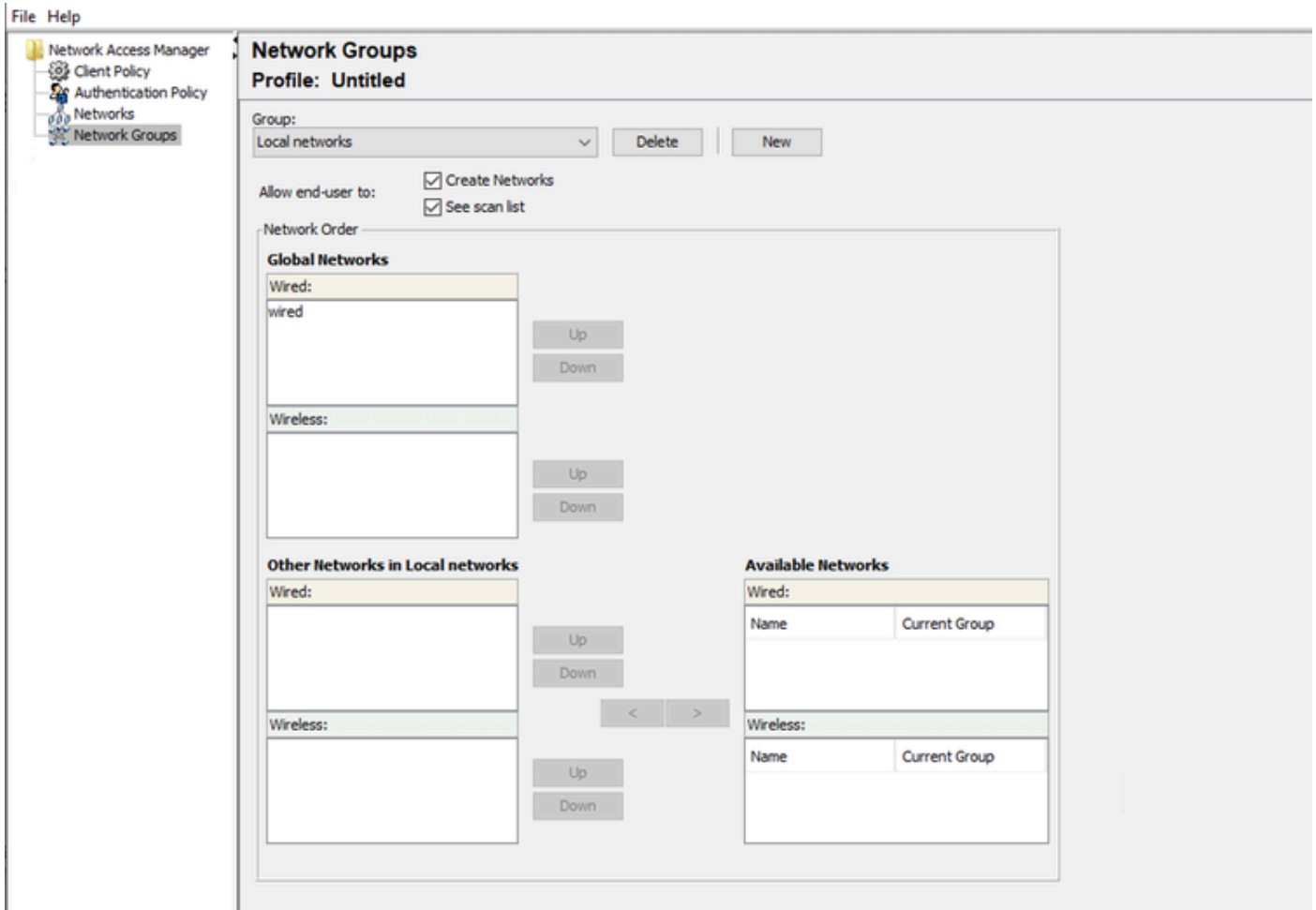
- Select All (Personal)
 - Open (no encryption)
 - Open (Static WEP)
 - Shared (WEP)
 - WPA Personal TKIP
 - WPA Personal AES
 - WPA2 Personal TKIP
 - WPA2 Personal AES
 - WPA3 Open (OWE)
 - WPA3 Personal AES (SAE)
- Select All (Enterprise)
 - Open (Dynamic (802.1X) WEP)
 - WPA Enterprise TKIP
 - WPA Enterprise AES
 - WPA2 Enterprise TKIP
 - WPA2 Enterprise AES
 - CKM Enterprise TKIP
 - CKM Enterprise AES
 - WPA3 Enterprise AES

Allowed Authentication Modes

- Select All Outer
 - EAP-FAST
 - EAP-GTC
 - EAP-MSCHAPv2
 - EAP-TLS
 - EAP-TLS
 - EAP-TTLS
 - EAP-MD5
 - EAP-MSCHAPv2
 - PAP (legacy)
 - CHAP (legacy)
 - MSCHAP (legacy)
 - MSCHAPv2 (legacy)
 - LEAP
 - PEAP
 - EAP-GTC
 - EAP-MSCHAPv2
 - EAP-TLS

Allowed Wired Security

- Select All
 - Open (no encryption)
 - 802.1x only
 - 802.1x with MacSec
 - AES-GCM-128
 - AES-GCM-256



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.

Networks

Profile: Untitled

Network

Name	Media Type	Group*
------	------------	--------

Add...

Edit...

Delete

* A network in group 'Global' is a member of *all* groups.

Creazione profilo di rete

Assegnare un nome al profilo di rete.

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

Networks

Profile: Untitled

Name:	<input type="text" value="PEAP MSCHAPv2"/>	Media Type
Group Membership	<input type="radio"/> In group: <input type="text" value="Local networks"/>	Security Level
	<input checked="" type="radio"/> In all groups (Global)	
Choose Your Network Media	<input checked="" type="radio"/> Wired (802.3) Network Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.	
	<input type="radio"/> Wi-Fi (wireless) Network Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point. SSID (max 32 chars): <input type="text"/> <input type="checkbox"/> Hidden Network <input type="checkbox"/> Corporate Network Association Timeout: <input type="text" value="5"/> seconds	
Common Settings	Script or application on each user's machine to run when connected. <input type="text"/> <input type="button" value="Browse Local Machine"/> Connection Timeout: <input type="text" value="40"/> seconds	
<input type="button" value="Next"/> <input type="button" value="Cancel"/>		

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.

Networks
Profile: Untitled

Security Level

Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

Authenticating Network
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

802.1X Settings

authPeriod (sec.)	<input type="text" value="30"/>	startPeriod (sec.)	<input type="text" value="3"/>
heldPeriod (sec.)	<input type="text" value="60"/>	maxStart	<input type="text" value="2"/>

Security

Key Management
None

Encryption

AES GCM 128
 AES GCM 256

Port Authentication Exception Policy

Enable port exceptions

Allow data traffic before authentication
 Allow data traffic after authentication even if

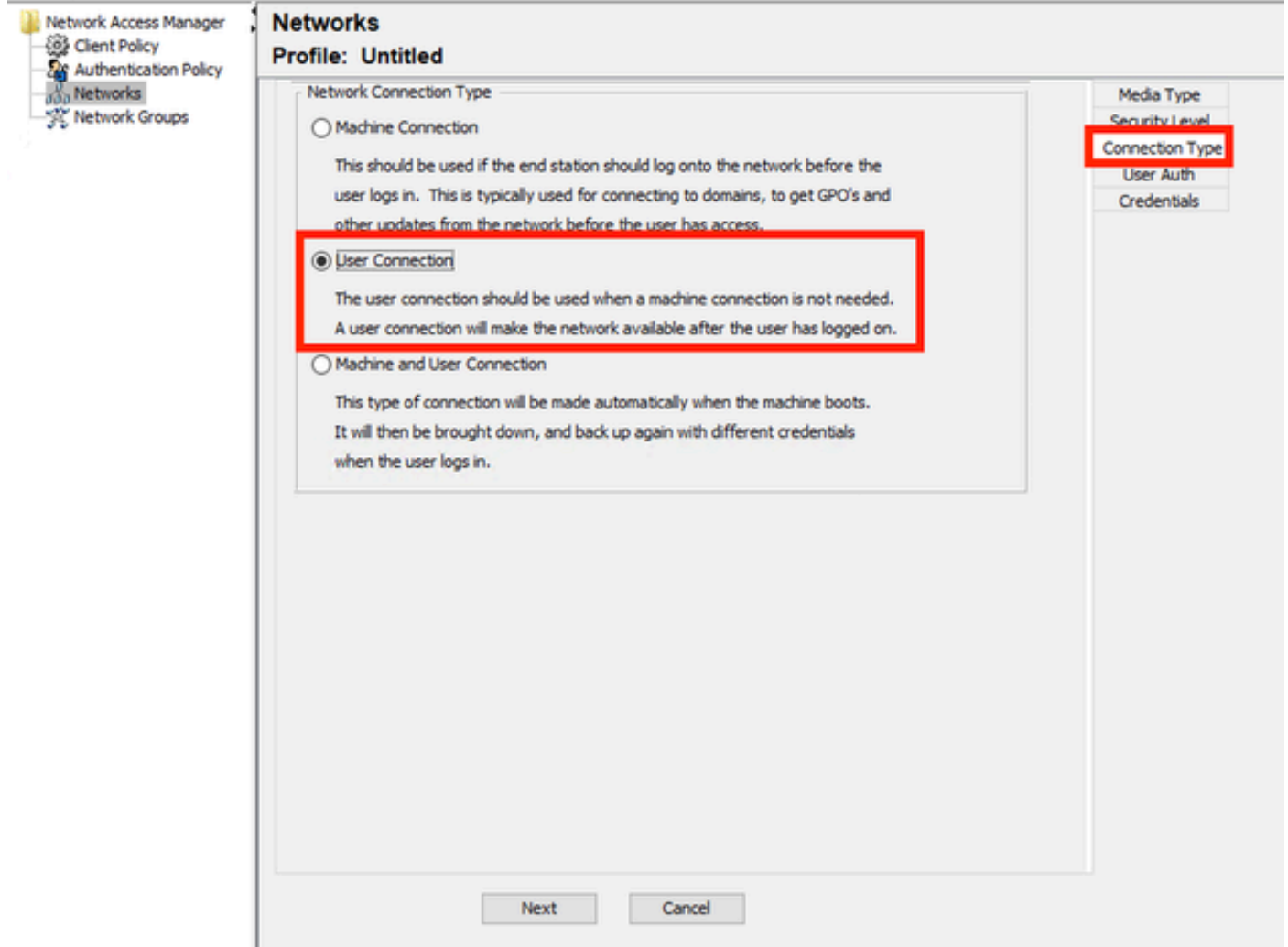
EAP fails
 EAP succeeds but key management fails

Media Type
Security Level
Connection Type

Next Cancel

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.

Networks
Profile: Untitled

EAP Methods

- EAP-MD5
- EAP-MSCHAPv2
- EAP-GTC
- EAP-TLS
- EAP-TTLS
- PEAP
- EAP-FAST

Extend user connection beyond log off

EAP-PEAP Settings

- Validate Server Identity
- Enable Fast Reconnect
- Disable when using a Smart Card

Inner Methods based on Credentials Source

- Authenticate using a Password
 - EAP-MSCHAPv2
 - EAP-GTC
- EAP-TLS, using a Certificate
- Authenticate using a Token and EAP-GTC

Media Type
Security Level
Connection Type
User Auth
Certificates
Credentials

Next Cancel

Autenticazione utente profilo di rete

Non modificare i valori predefiniti in Impostazioni EAP-PEAP.

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

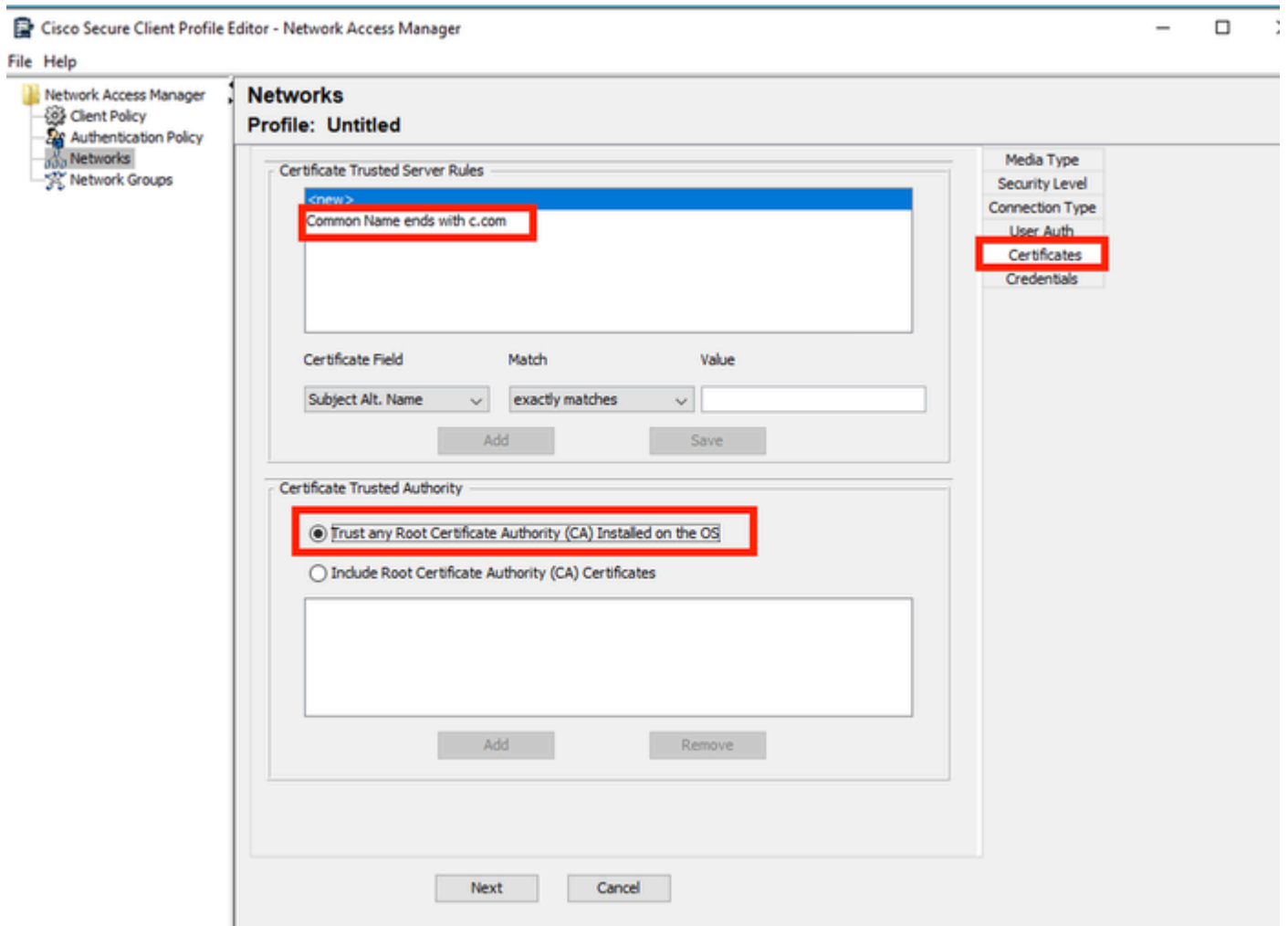
Tra i vari metodi interni esistenti per EAP PEAP, selezionare Autentica tramite password e selezionare EAP-MSCHAPv2.

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.

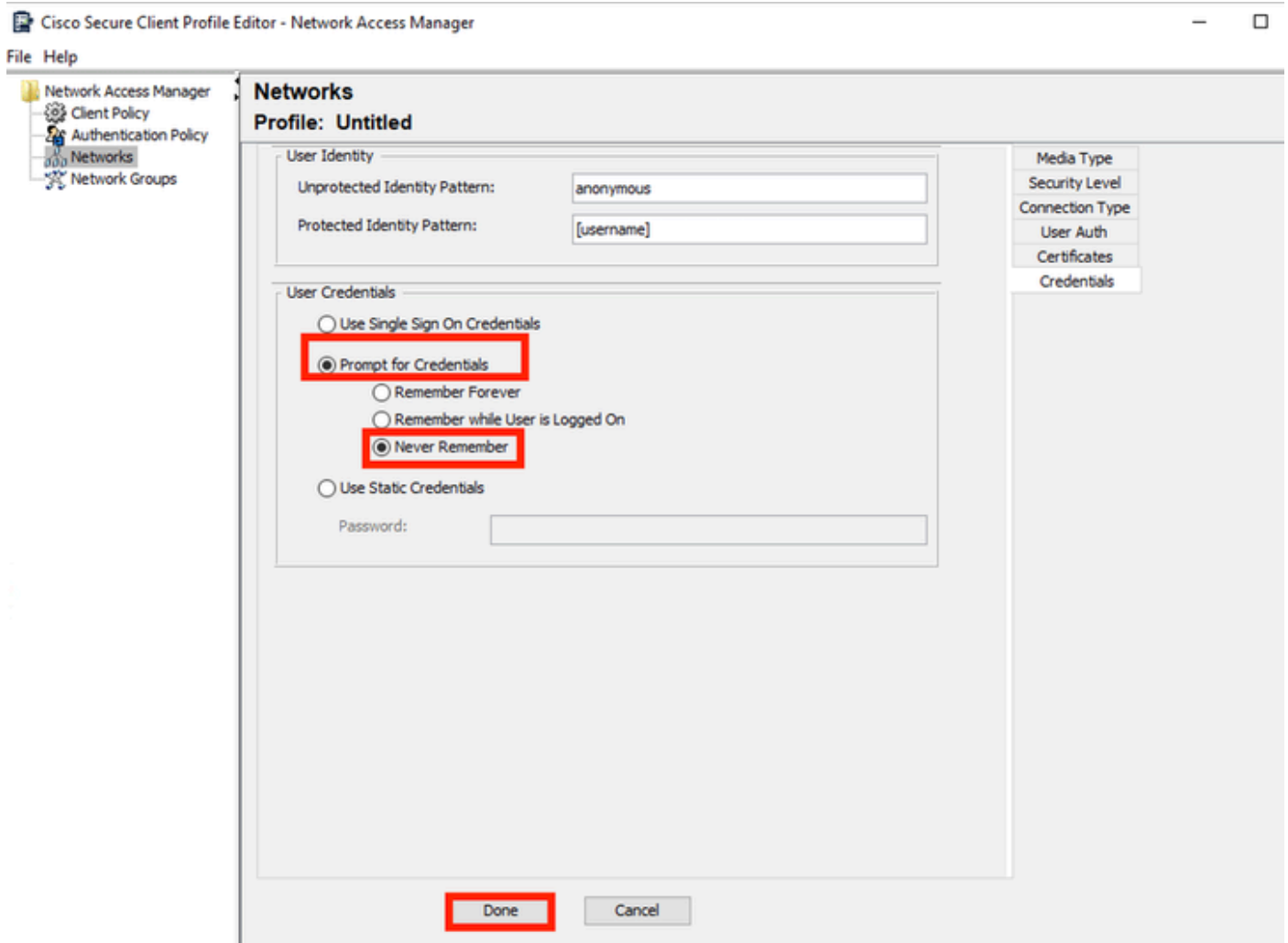


Sezione Certificato profilo di rete

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.

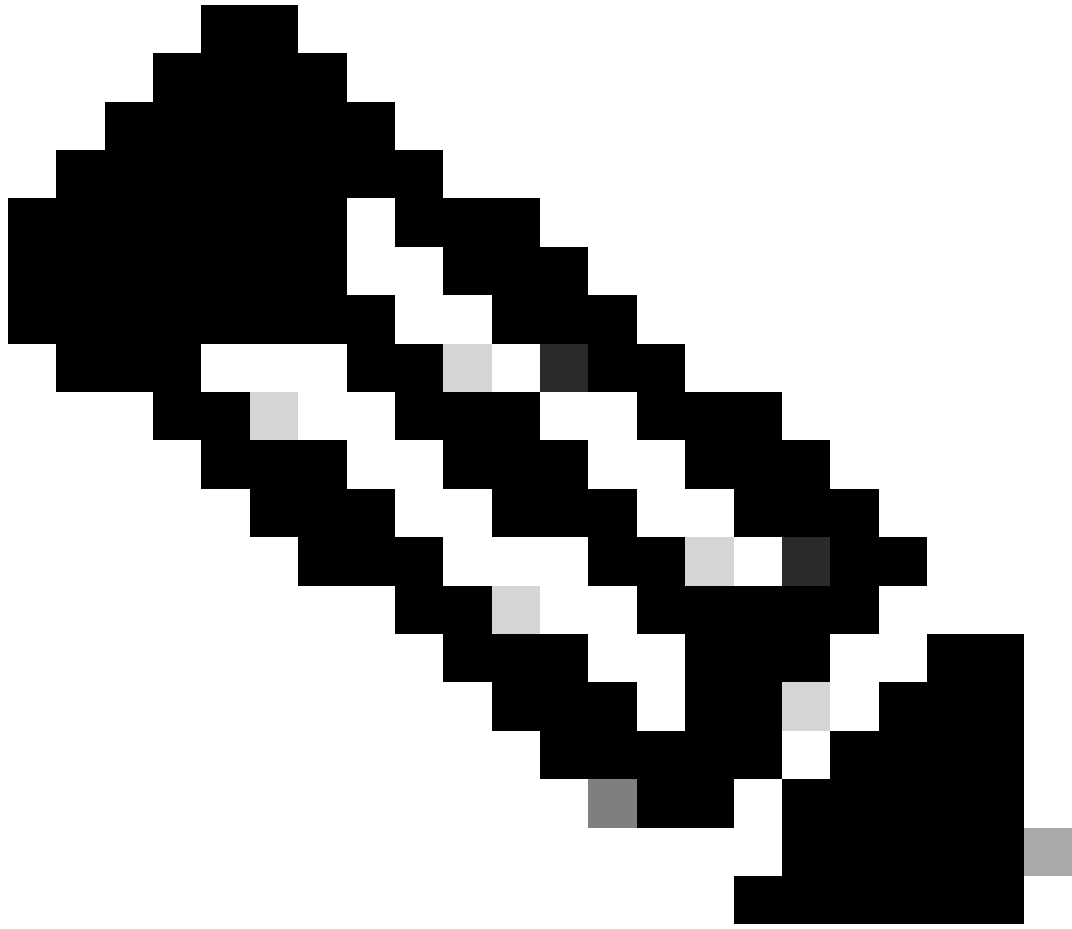
L'opzione Richiedi credenziali > Non ricordare mai è selezionata, quindi in ogni autenticazione l'utente che effettua l'autenticazione deve immettere le proprie credenziali.

Selezionate Fatto (Done).

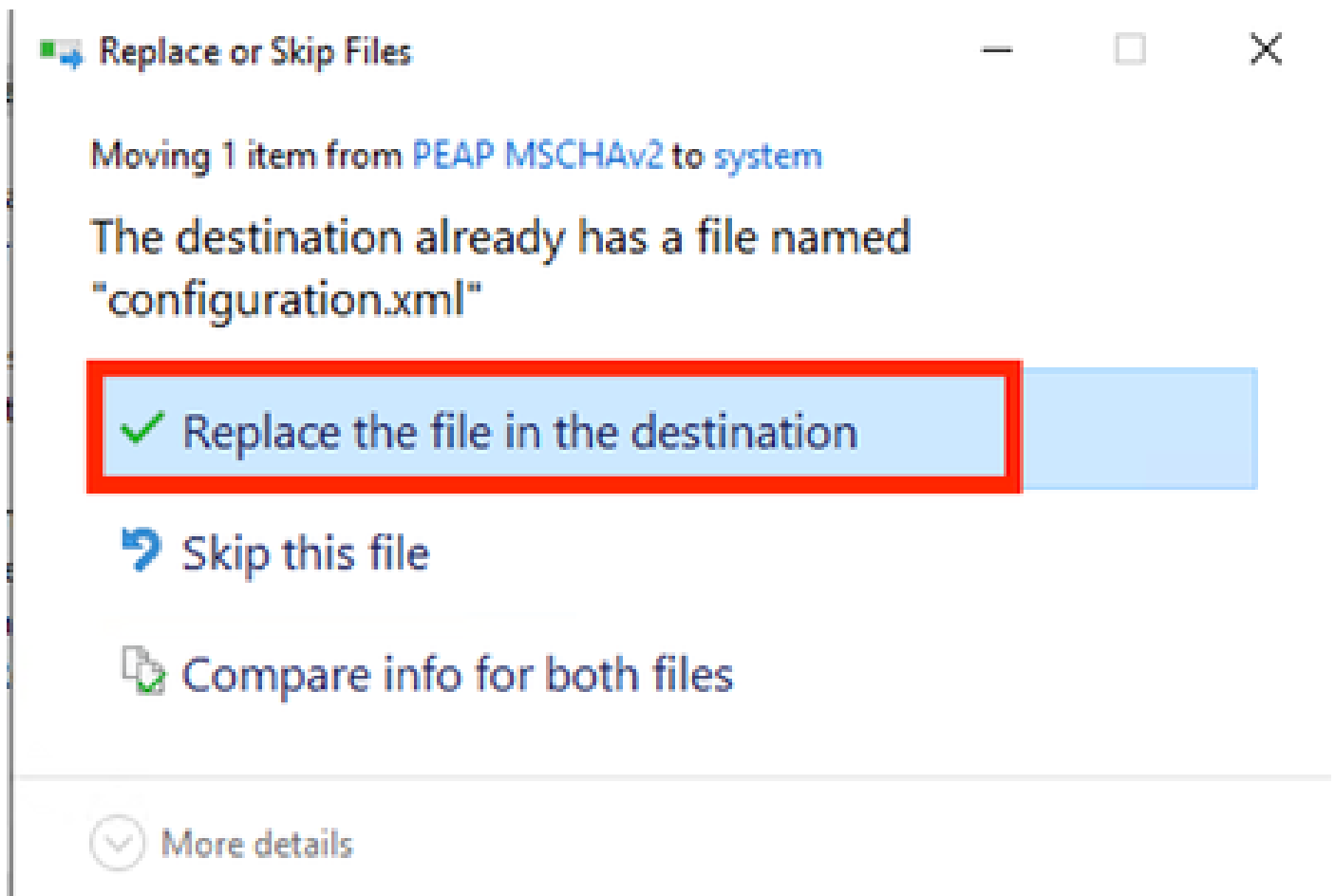
Salvare il profilo di Secure Client Network Access Manager come configuration.xml con l'opzione File > Salva con nome.

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.

Networks

Profile: Untitled

Network

Name	Media Type	Group*
------	------------	--------

Add...

Edit...

Delete

* A network in group 'Global' is a member of *all* groups.

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.

File Help

Networks
Profile: Untitled

Name: **EAP-FAST**

Group Membership

In group: Local networks

In all groups (Global)

Choose Your Network Media

Wired (802.3) Network
Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.

Wi-Fi (wireless) Network
Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.

SSID (max 32 chars):

Hidden Network
 Corporate Network

Association Timeout: seconds

Common Settings

Script or application on each user's machine to run when connected.

Connection Timeout: seconds

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.

File Help

Networks
Profile: Untitled

Security Level

Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

Authenticating Network
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

802.1X Settings

authPeriod (sec.)	<input type="text" value="30"/>	startPeriod (sec.)	<input type="text" value="3"/>
heldPeriod (sec.)	<input type="text" value="60"/>	maxStart	<input type="text" value="2"/>

Security

Key Management
None

Encryption

AES GCM 128
 AES GCM 256

Port Authentication Exception Policy

Enable port exceptions

Allow data traffic before authentication

Allow data traffic after authentication even if

EAP fails
 EAP succeeds but key management fails

Next Cancel

Sezione Editor di profili del livello di protezione

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

File Help

Networks
Profile: Untitled

Network Connection Type

Machine Connection

This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.

User Connection

The user connection should be used when a machine connection is not needed. A user connection will make the network available after the user has logged on.

Machine and User Connection

This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.

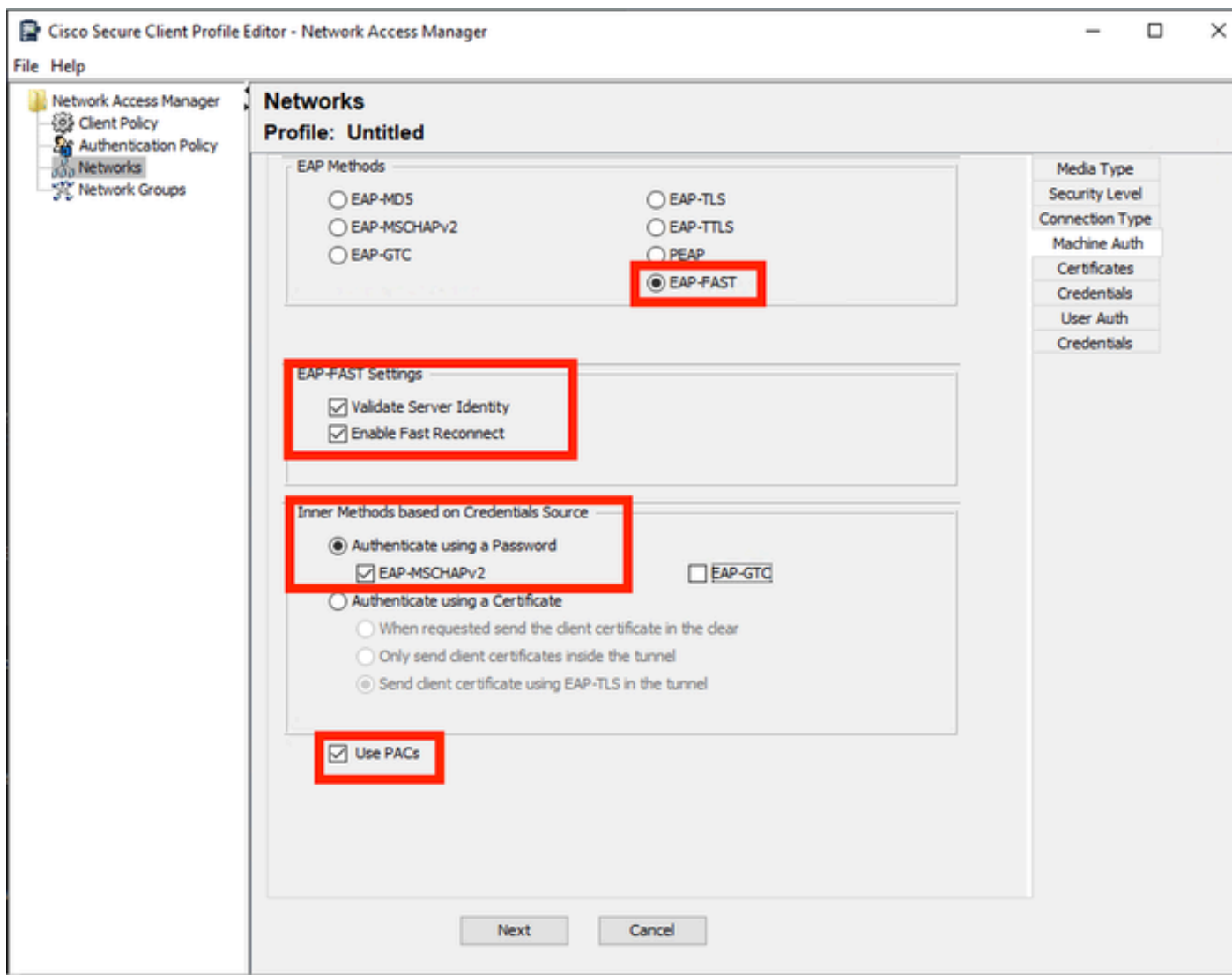
Media Type
Security Level
Connection Type
Machine Auth
Credentials
User Auth
Credentials

Next Cancel

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.

Networks

Profile: Untitled

Certificate Trusted Server Rules

<new>
Subject Alternative Name ends with c.com

Certificate Field	Match	Value
Subject Alt. Name	exactly matches	

Add Save

Certificate Trusted Authority

Trust any Root Certificate Authority (CA) Installed on the OS

Include Root Certificate Authority (CA) Certificates

--

Add Remove

Next Cancel

Media Type

Security Level

Connection Type

Machine Auth

Certificates

Credentials

User Auth

Certificates

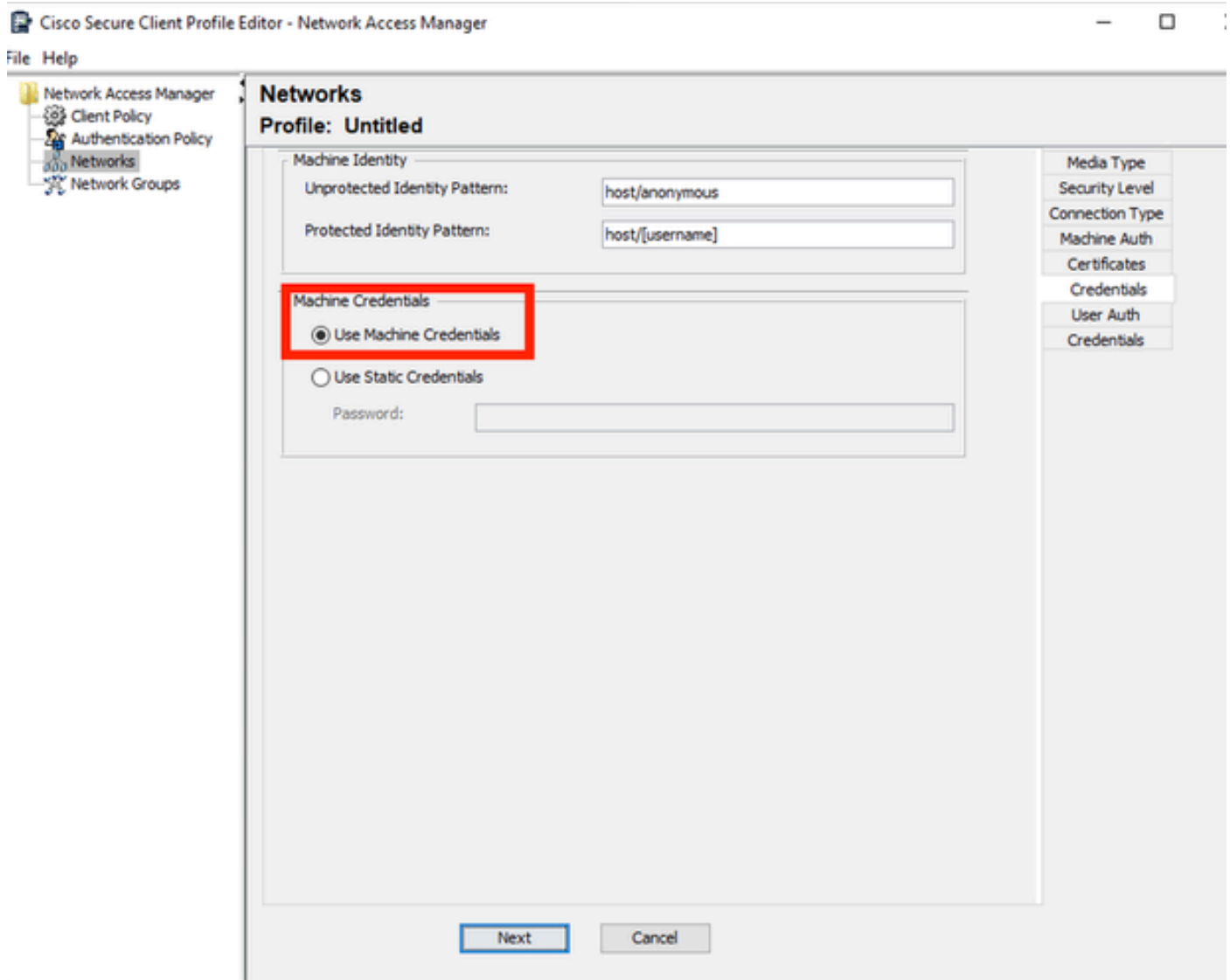
Credentials

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).

File Help

Networks
Profile: Untitled

EAP Methods

EAP-MD5
 EAP-TLS
 EAP-MSCHAPv2
 EAP-TTLS
 EAP-GTC
 PEAP
 EAP-FAST

Extend user connection beyond log off

EAP-FAST Settings

Validate Server Identity
 Enable Fast Reconnect
 Disable when using a Smart Card

Inner Methods based on Credentials Source

Authenticate using a Password
 EAP-MSCHAPv2
 EAP-GTC
 Authenticate using a Certificate
 When requested send the client certificate in the clear
 Only send client certificates inside the tunnel
 Send client certificate using EAP-TLS in the tunnel
 Authenticate using a Token and EAP-GTC

Use PACs

Media Type
Security Level
Connection Type
Machine Auth
Certificates
Credentials
User Auth
Certificates
Credentials

Next Cancel

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.

Networks

Profile: C:\Users\LAB 5\Desktop\EAP FAST\configuration.xml

The screenshot displays the 'Certificate Trusted Server Rules' section of a network configuration wizard. A rule is defined with the field 'Common Name', the match 'ends with', and the value 'c.com'. Below this, the 'Certificate Trusted Authority' section is shown with two radio button options: 'Trust any Root Certificate Authority (CA) Installed on the OS' (selected) and 'Include Root Certificate Authority (CA) Certificates'. A vertical sidebar on the right contains a list of configuration categories: Media Type, Security Level, Connection Type, Machine Auth, Certificates, Credentials, User Auth, Certificates, and Credentials. The 'Certificates' item in the second row is highlighted with a red box. At the bottom of the wizard, 'Next' and 'Cancel' buttons are visible.

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).

Networks

Profile: Untitled

User Identity

Unprotected Identity Pattern:

Protected Identity Pattern:

User Credentials

Use Single Sign On Credentials

Prompt for Credentials

Remember Forever

Remember while User is Logged On

Never Remember

Use Static Credentials

Password:

Media Type

Security Level

Connection Type

Machine Auth

Certificates

Credentials

User Auth

Certificates

Credentials

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.

Networks

Profile: Untitled

Network

Name	Media Type	Group*
------	------------	--------

Add...

Edit...

Delete

* A network in group 'Global' is a member of *all* groups.

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.

Networks
Profile: Untitled

Name:

Group Membership

In group:

In all groups (Global)

Choose Your Network Media

Wired (802.3) Network

Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.

Wi-Fi (wireless) Network

Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.

SSID (max 32 chars):

Hidden Network

Corporate Network

Association Timeout: seconds

Common Settings

Script or application on each user's machine to run when connected.

Connection Timeout: seconds

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.

Networks
Profile: Untitled

Security Level

Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

Authenticating Network
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

802.1X Settings

authPeriod (sec.) startPeriod (sec.)

heldPeriod (sec.) maxStart

Port Authentication Exception Policy

Enable port exceptions

Allow data traffic before authentication

Allow data traffic after authentication even if

EAP fails

EAP succeeds but key management fails

Security

Key Management
None

Encryption

AES GCM 128

AES GCM 256

Media Type

Security Level

Connection Type

Next Cancel

Livello di protezione

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

Networks
Profile: Untitled

Network Connection Type

Machine Connection
This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.

User Connection
The user connection should be used when a machine connection is not needed. A user connection will make the network available after the user has logged on.

Machine and User Connection
This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.

Media Type

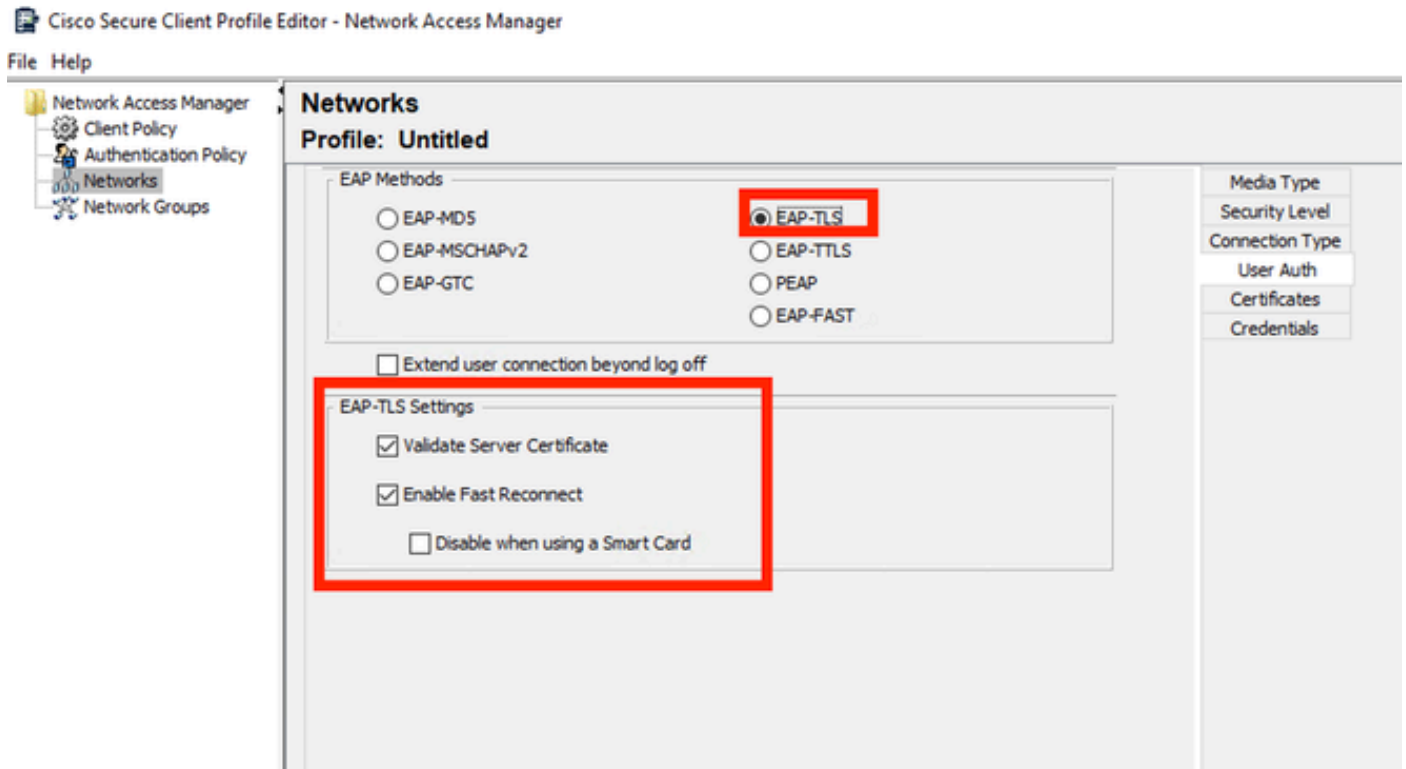
Security Level

Connection Type

User Auth

Credentials

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.

Networks
Profile: Untitled

Certificate Trusted Server Rules

Common Name ends with c.com

Certificate Field	Match	Value
Subject Alt. Name	exactly matches	

Buttons: Add, Save

Certificate Trusted Authority

Trust any Root Certificate Authority (CA) Installed on the OS

Include Root Certificate Authority (CA) Certificates

Buttons: Add, Remove

Buttons: Next, Cancel

Media Type
Security Level
Connection Type
User Auth
Certificates
Credentials

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.

Networks

Profile: Untitled

User Identity

Unprotected Identity Pattern:

User Credentials

Use Single Sign On Credentials (Requires Smart Card)

Prompt for Credentials

- Remember Forever
- Remember while User is Logged On
- Never Remember

Certificate Source

Smart Card or OS certificates

Smart Card certificates only

Remember Smart Card Pin

Remember Forever

Remember while User is Logged On

Never Remember

Smart Card Removal Policy

Disconnect from Network

Use Certificate Matching Rule (Max 10)

Rule Logic OR AND

Field	Operator	Value

Media Type

Security Level

Connection Type

User Auth

Certificates

Credentials

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.

Certificate Matching Rule Entry [X]

Certificate Field: Issuer.CN Match: Equals

Value: My Internal OR 3rd Party CA.com

OK Cancel

Use Certificate Matching Rule (Max 10)

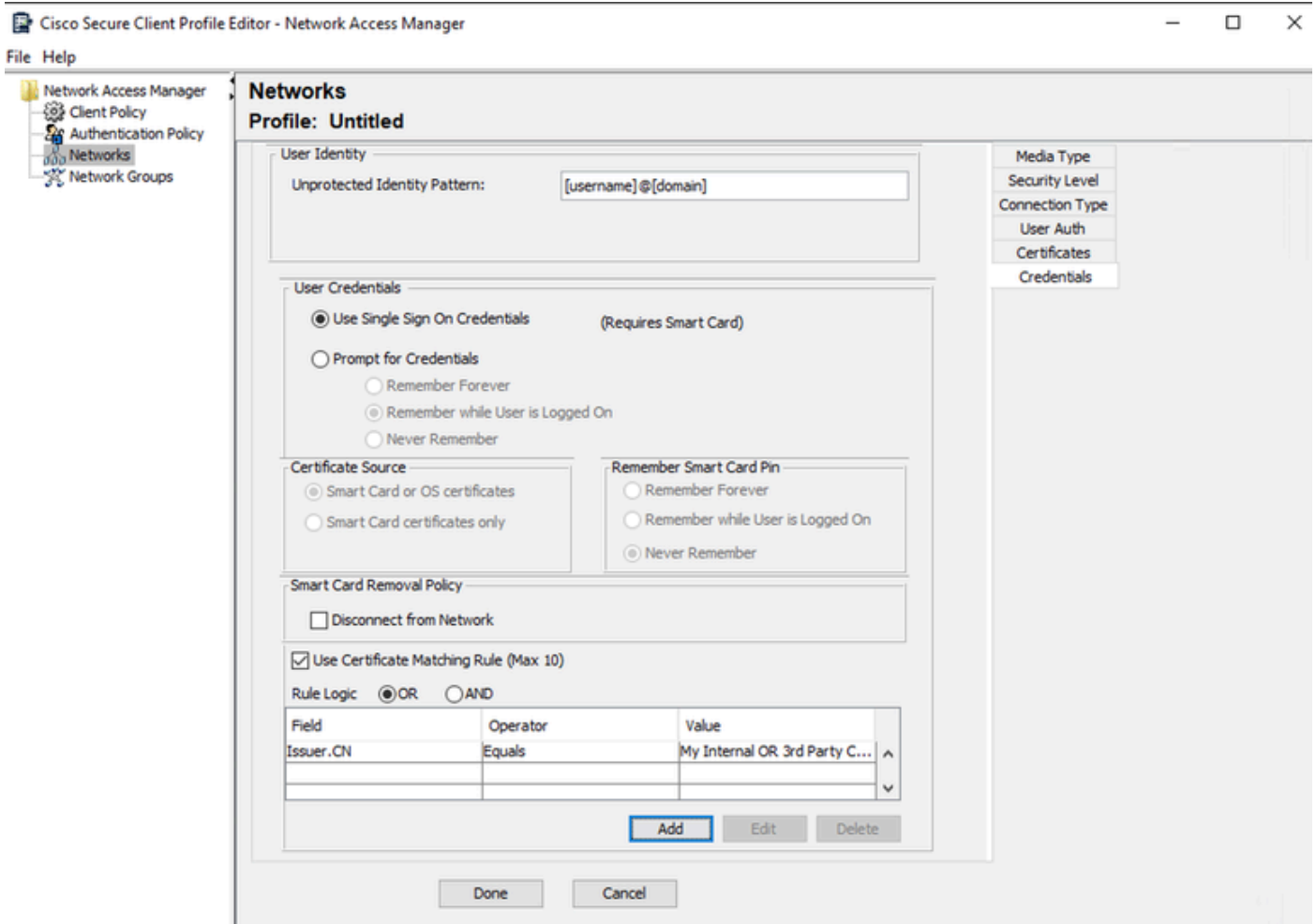
Logic: OR AND

Id	Operator	Value

Add Edit Delete

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>
```

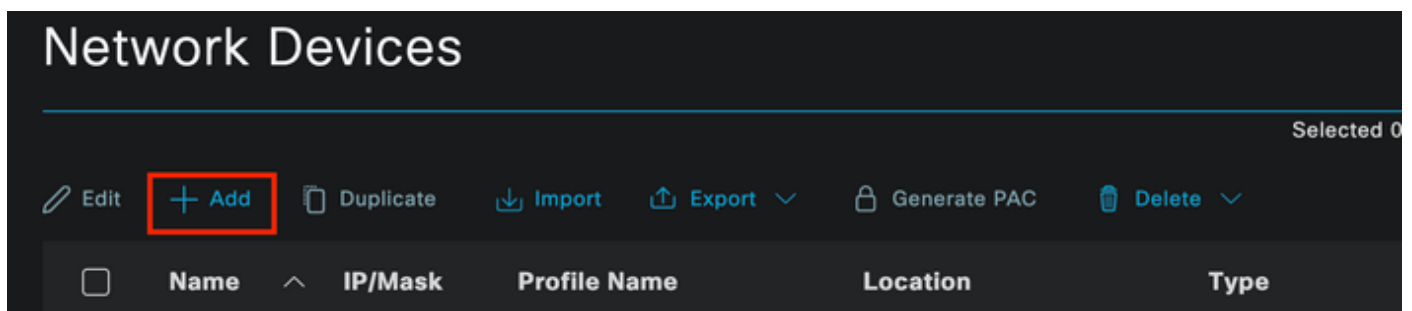
```
!  
!  
aaa group server radius ISE-CLUSTER  
  server name ISE-PSN-1  
!  
interface GigabitEthernet0/1/0  
  description "Endpoint that supports dot1x"  
  switchport access vlan 15  
  switchport mode access  
  authentication host-mode multi-auth  
  authentication order dot1x mab  
  authentication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

Configurare Identity Service Engine 3.2.

Configurare il dispositivo di rete.

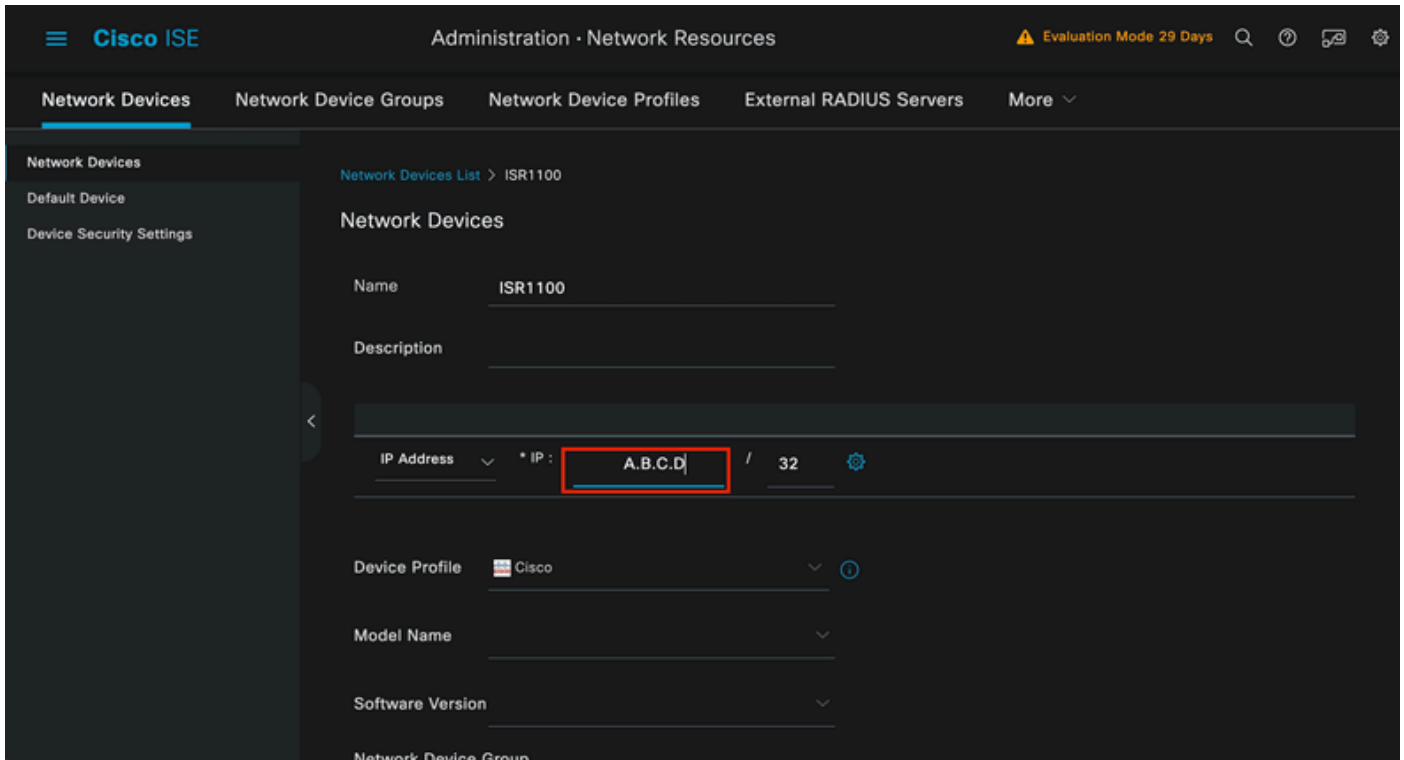
Aggiungere ISR e ISE ad Amministrazione > Risorse di rete > Dispositivi di rete.

Fare clic su Add.



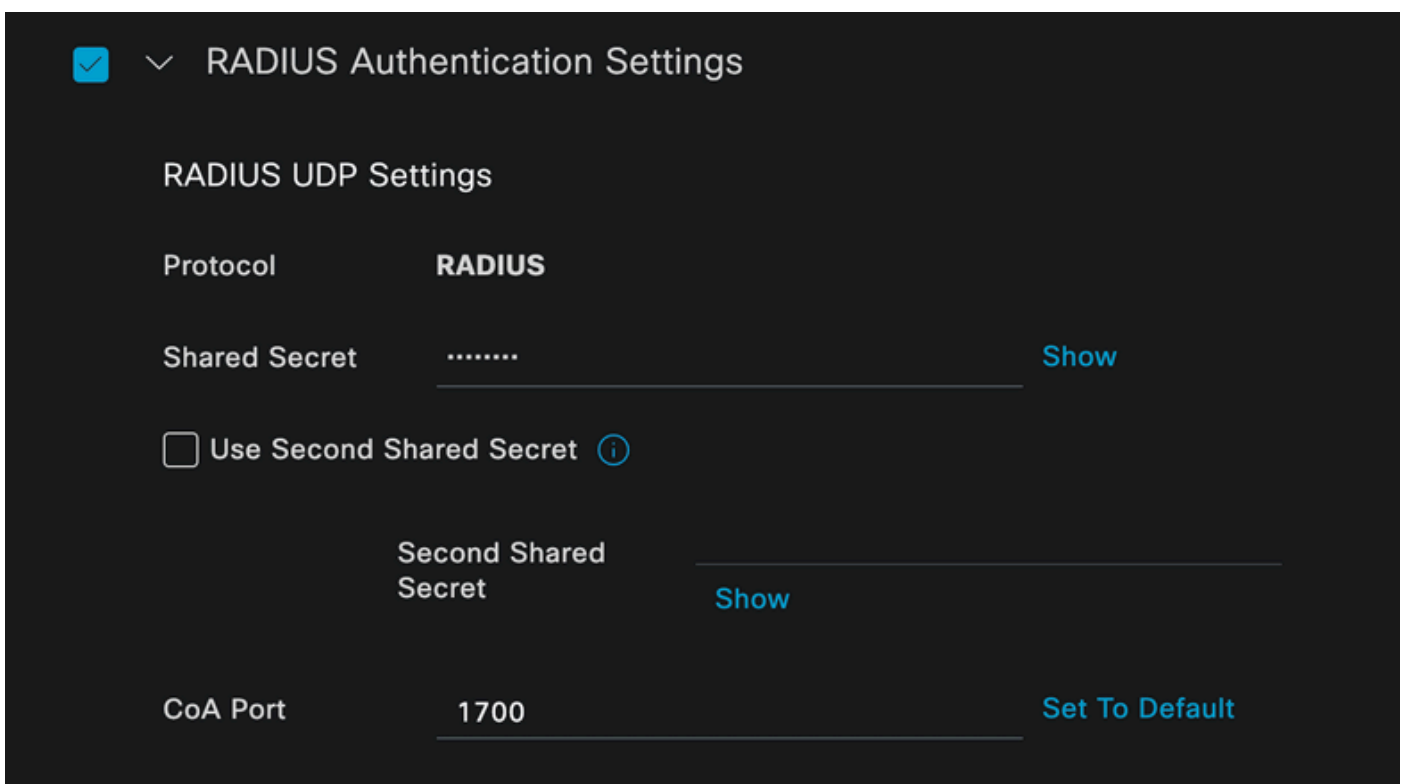
Sezione Periferica di rete

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.



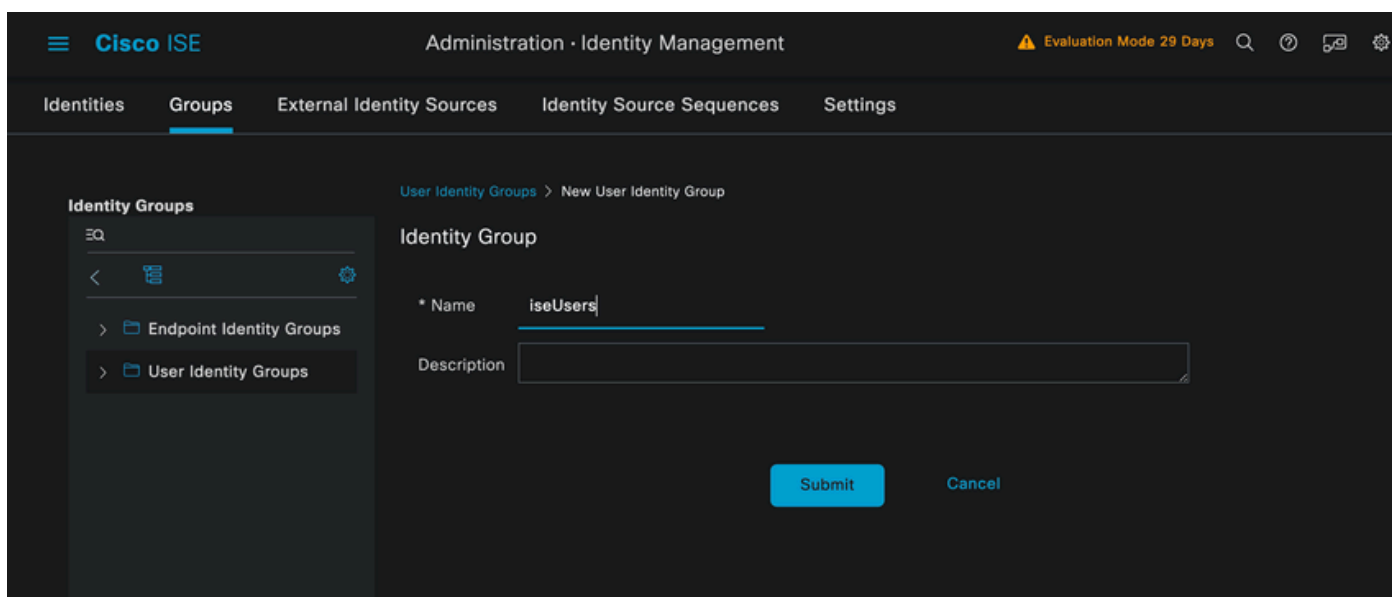
Impostazioni raggio dispositivo di rete

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.



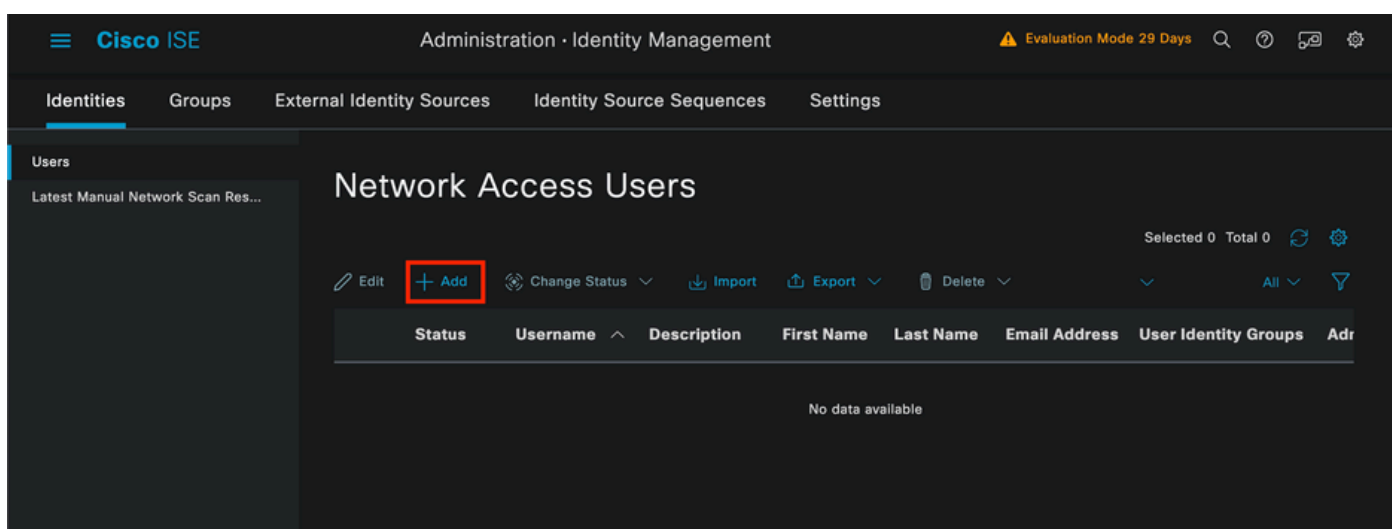
The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE', 'Administration · Identity Management', and 'Evaluation Mode 29 Days'. The main navigation menu has 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'Groups' tab is selected. On the left, the 'Identity Groups' sidebar shows 'Endpoint Identity Groups' and 'User Identity Groups'. The main area is titled 'User Identity Groups > New User Identity Group'. The 'Identity Group' form has a '* Name' field containing 'iseUsers' and an empty 'Description' field. At the bottom right, there are 'Submit' and 'Cancel' buttons.

Creazione gruppo di identità

Fare clic su Invia.

Passare a Amministrazione > Gestione delle identità > Scheda Identità.

Fare clic su Add.



The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE', 'Administration · Identity Management', and 'Evaluation Mode 29 Days'. The main navigation menu has 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'Identities' tab is selected. On the left, the 'Users' sidebar shows 'Latest Manual Network Scan Res...'. The main area is titled 'Network Access Users'. Above the table, there are 'Selected 0 Total 0' and icons for refresh and settings. Below this, there are action buttons: 'Edit', '+ Add' (highlighted with a red box), 'Change Status', 'Import', 'Export', and 'Delete'. The table has columns: 'Status', 'Username', 'Description', 'First Name', 'Last Name', 'Email Address', 'User Identity Groups', and 'Adr'. The table is currently empty, showing 'No data available'.

Sezione Utenti accesso alla rete

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

Network Access User

* Username

Status Enabled ▼

Account Name Alias ⓘ

Email

Creazione utente di accesso alla rete

Assegnare una password all'utente. Si utilizza VainillaISE97.

Passwords

Password Type: ▼

Password Lifetime:

- With Expiration ⓘ
Password will expire in 60 days
- Never Expires ⓘ

Password

Re-Enter Password

* Login Password

Generate Password ⓘ

Enable Password

Generate Password ⓘ

Sezione Password di creazione utente

Assegnare l'utente al gruppo iseUsers.

User Groups



iseUsers ▼

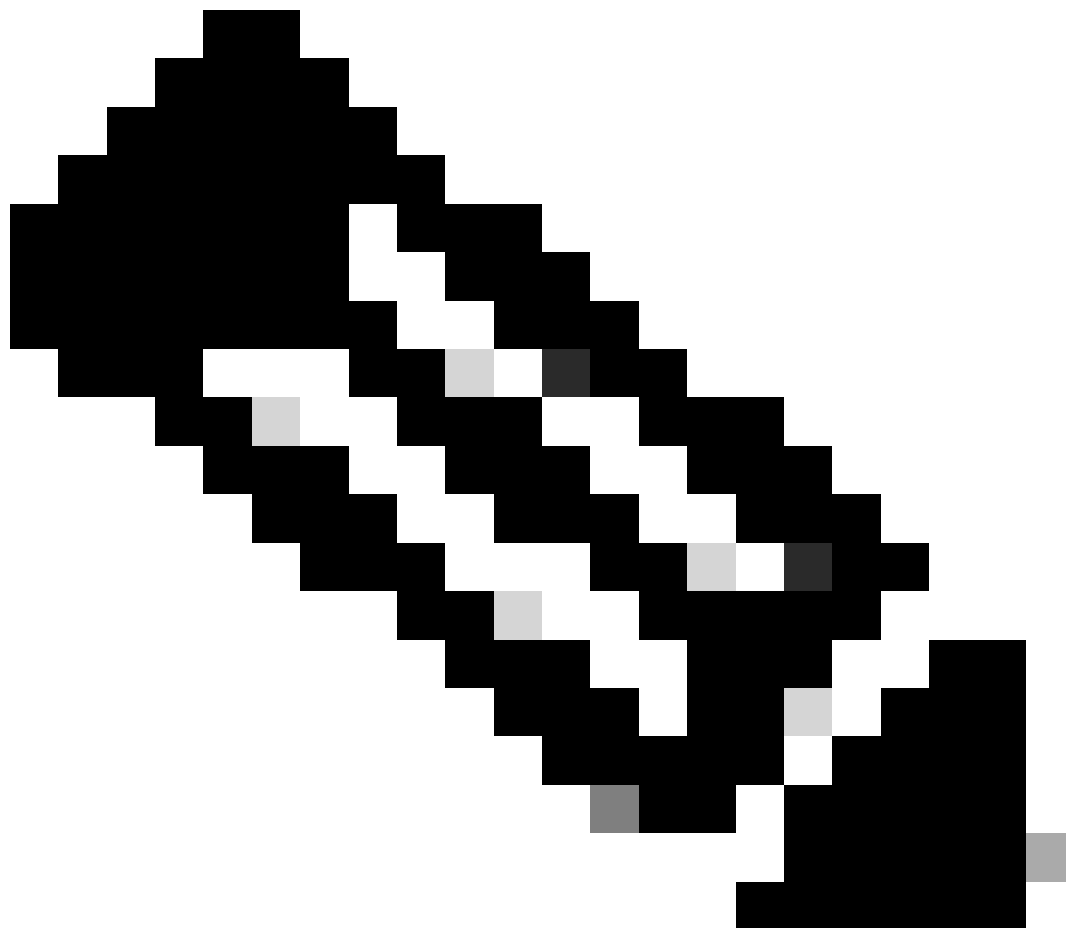


Assegnazione gruppo utenti

Configurare il set di criteri.

Selezionare Menu ISE > Policy > Policy Sets.

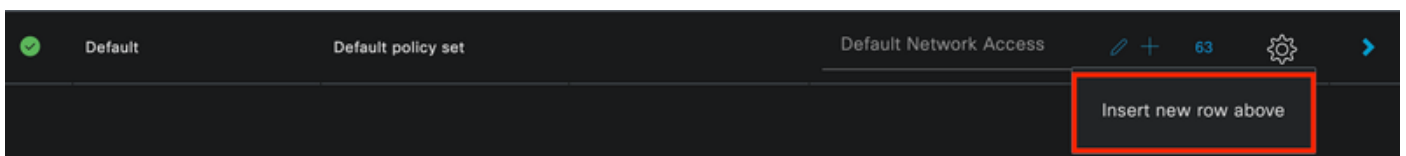
È possibile utilizzare il set di criteri predefinito. Tuttavia, per questo esempio viene creato un elemento denominato Wired.



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

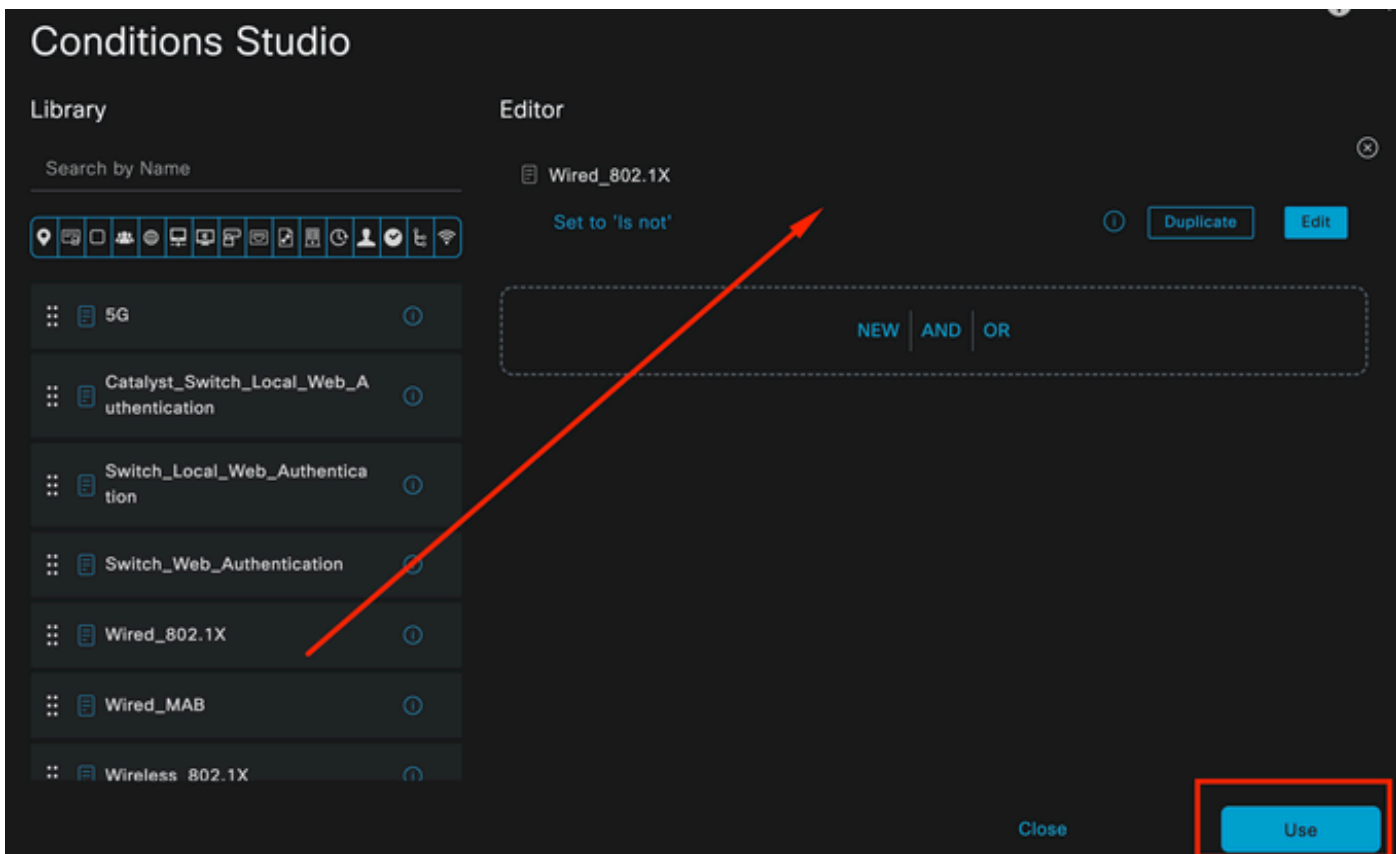


Nota: se l'icona Aggiungi o Più non è visibile, è possibile fare clic sull'icona Ingranaggio di qualsiasi set di criteri, quindi selezionare Inserisci nuova riga sopra.



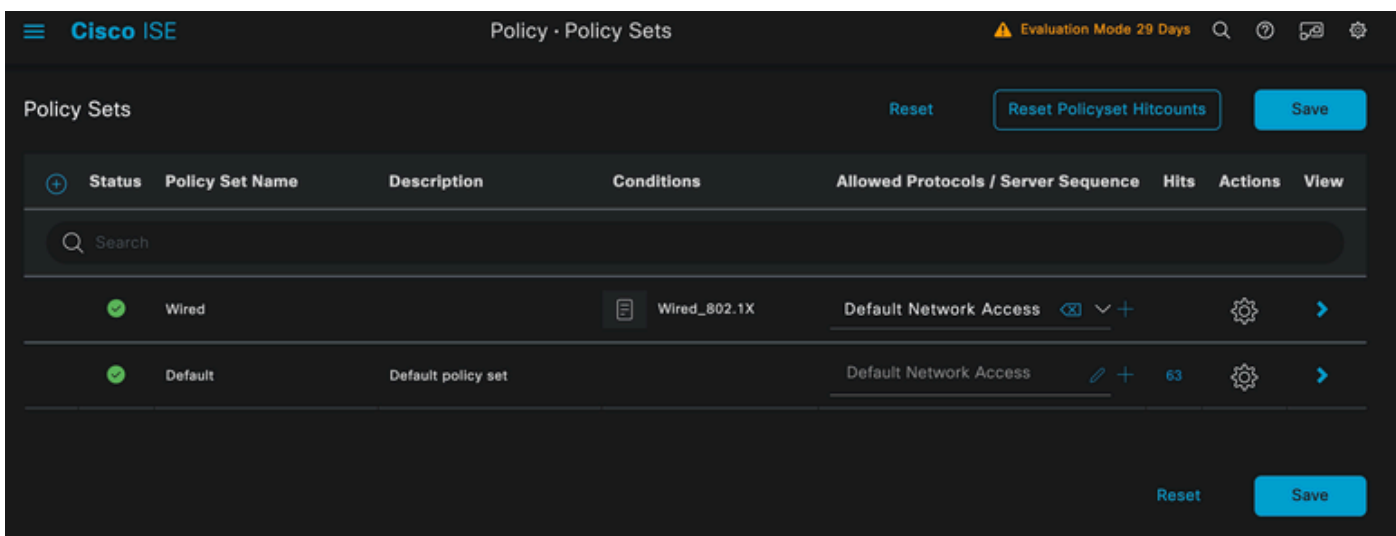
Opzioni icona ingranaggio

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.

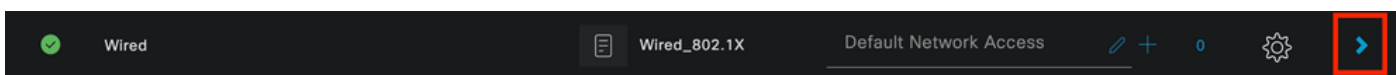


Visualizzazione generale set di criteri

Fare clic su Save (Salva).

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

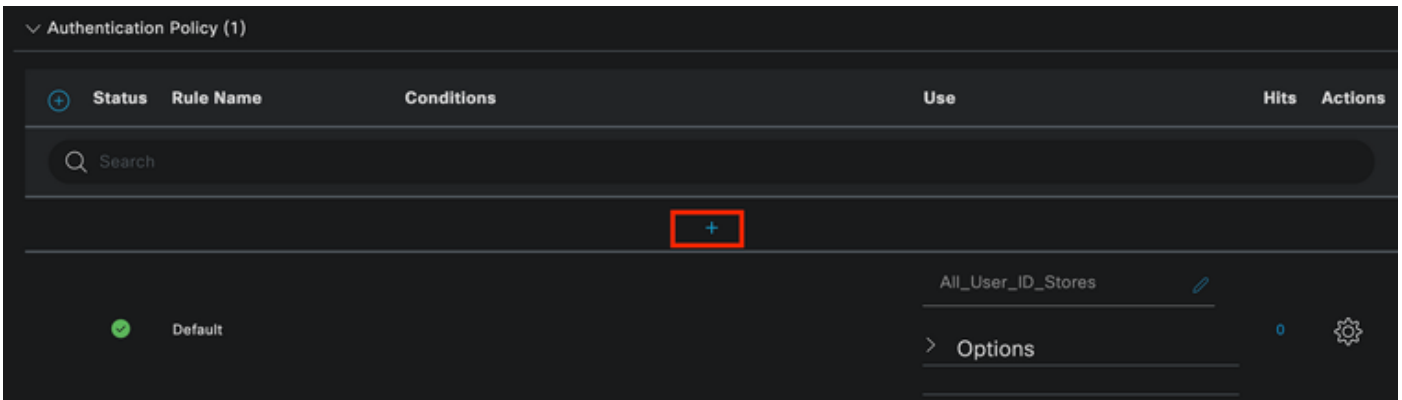
Fare clic sull'icona >.



Set di criteri per reti cablate

Espandere la sezione Criteri di autenticazione.

Fare clic sull'icona +.



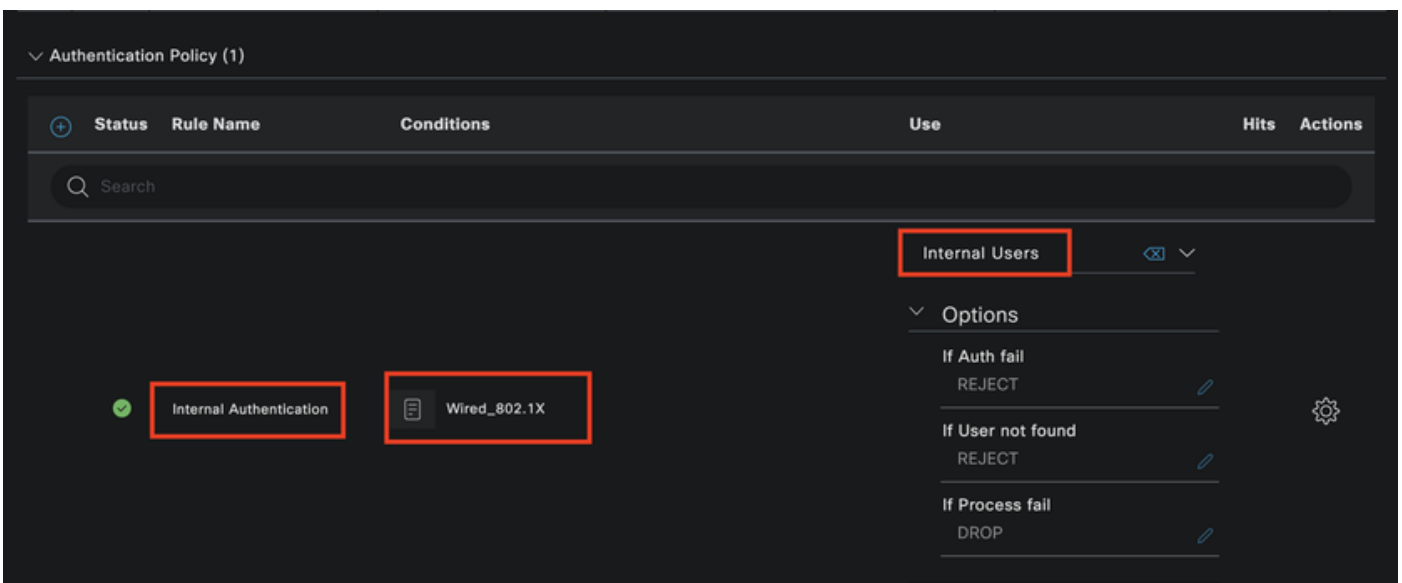
Criterio di autenticazione

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.

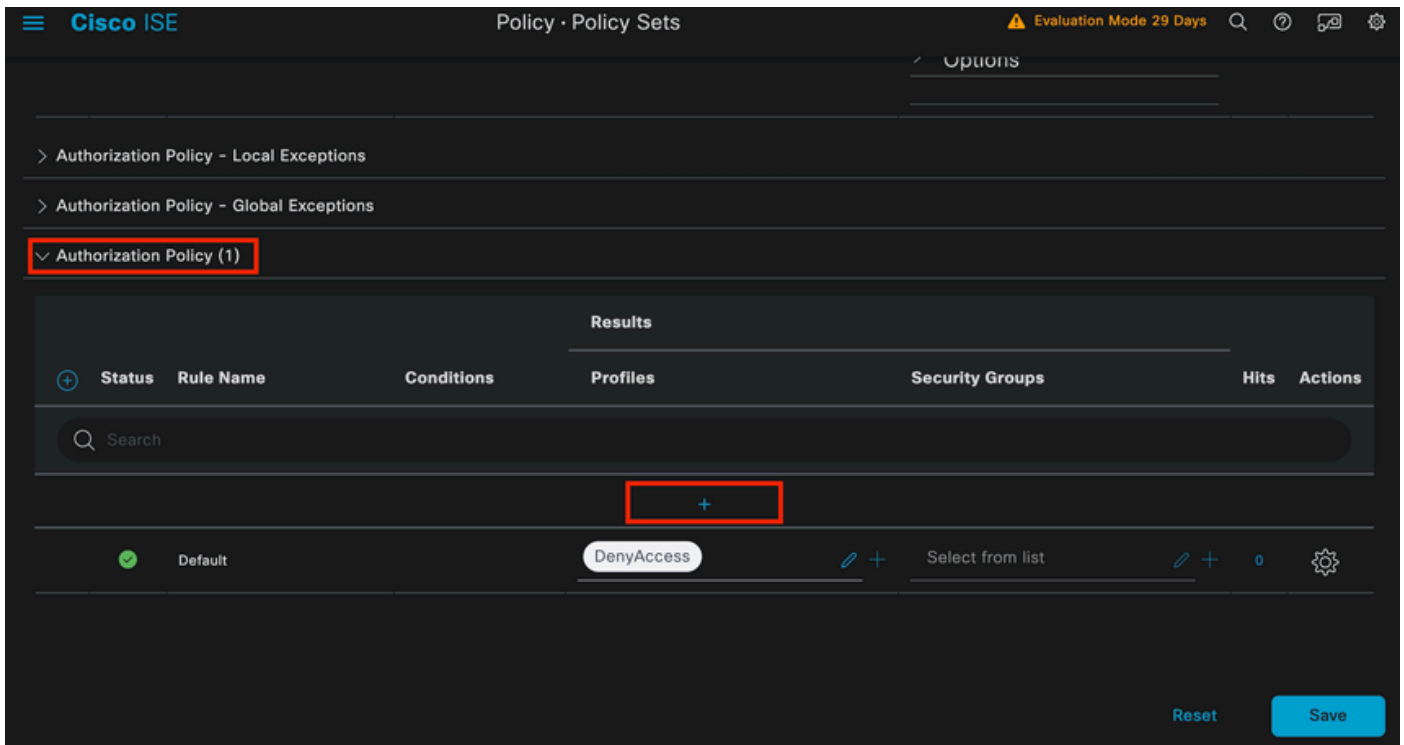
Infine, nella colonna Utilizza selezionare Utenti interni.



Criterio di autenticazione

Criteri di autorizzazione.

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



Criteria di autorizzazione

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

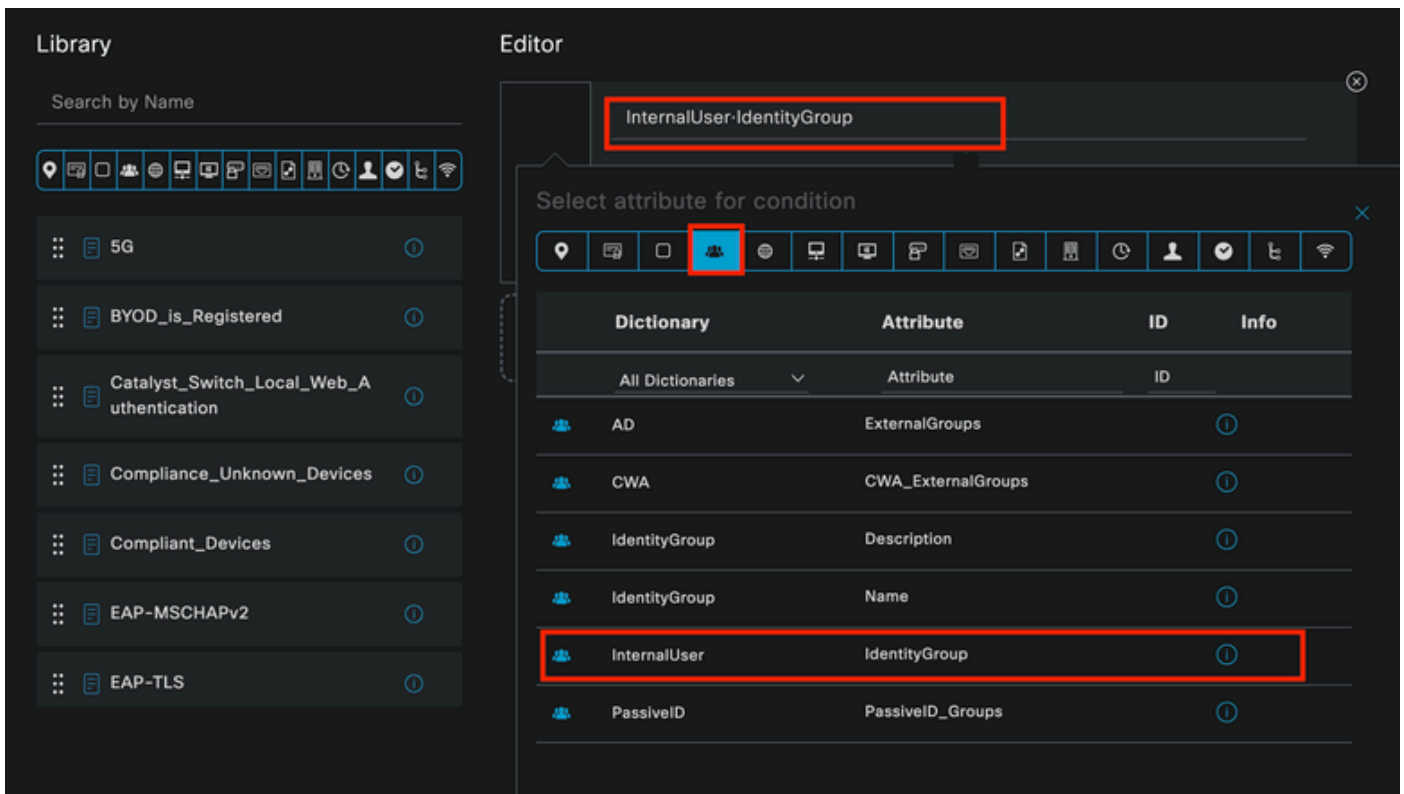
Per creare una condizione per il criterio di autorizzazione, fare clic sull'icona + nella colonna Condizioni.

Viene utilizzato il gruppo IseUsers.

Fare clic sulla sezione Attributo.

Selezionare l'icona IdentityGroup.

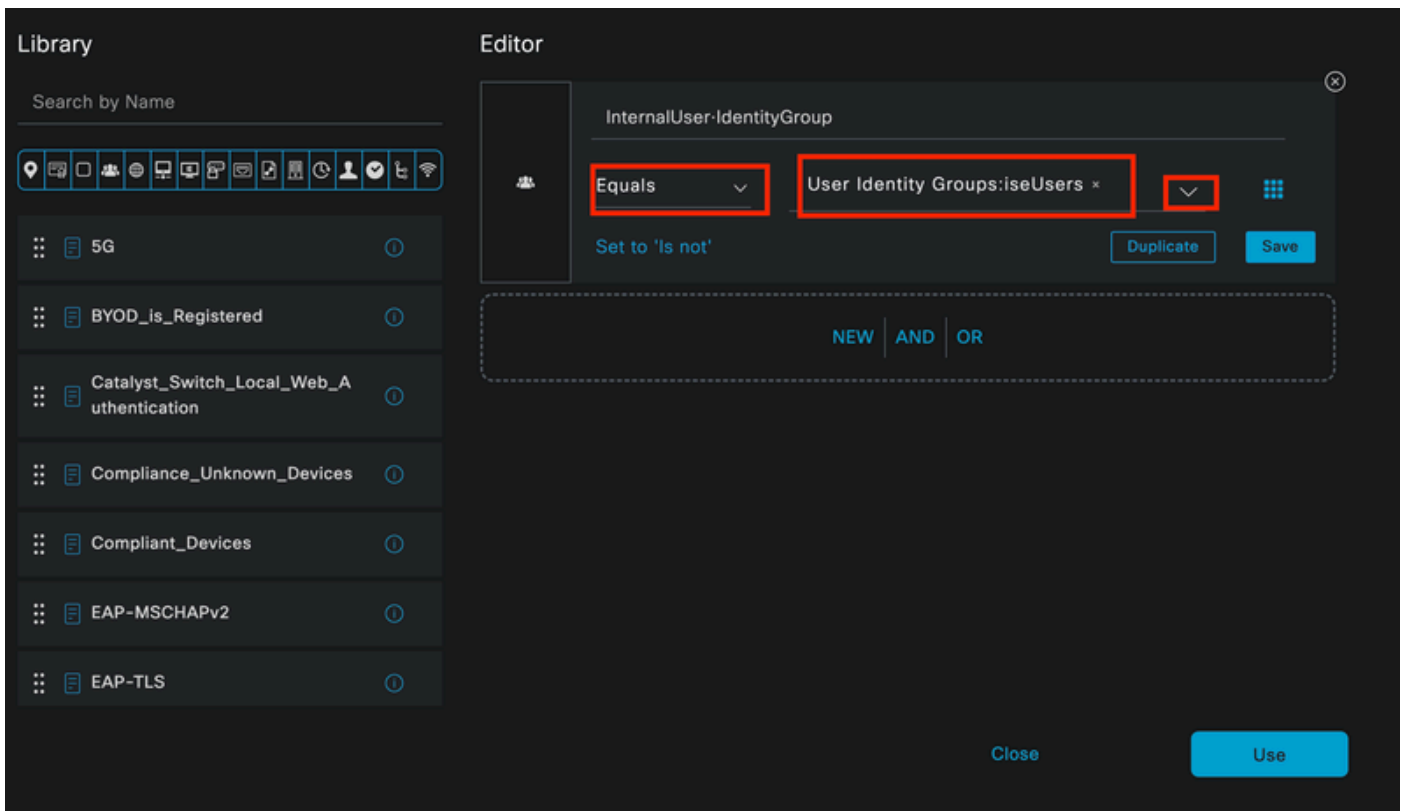
Dal dizionario selezionare il dizionario InternalUser fornito con l'attributo IdentityGroup.



Creazione di condizioni

Selezionare l'operatore Uguale a.

In Gruppi identità utente, selezionare il gruppo IseUsers.

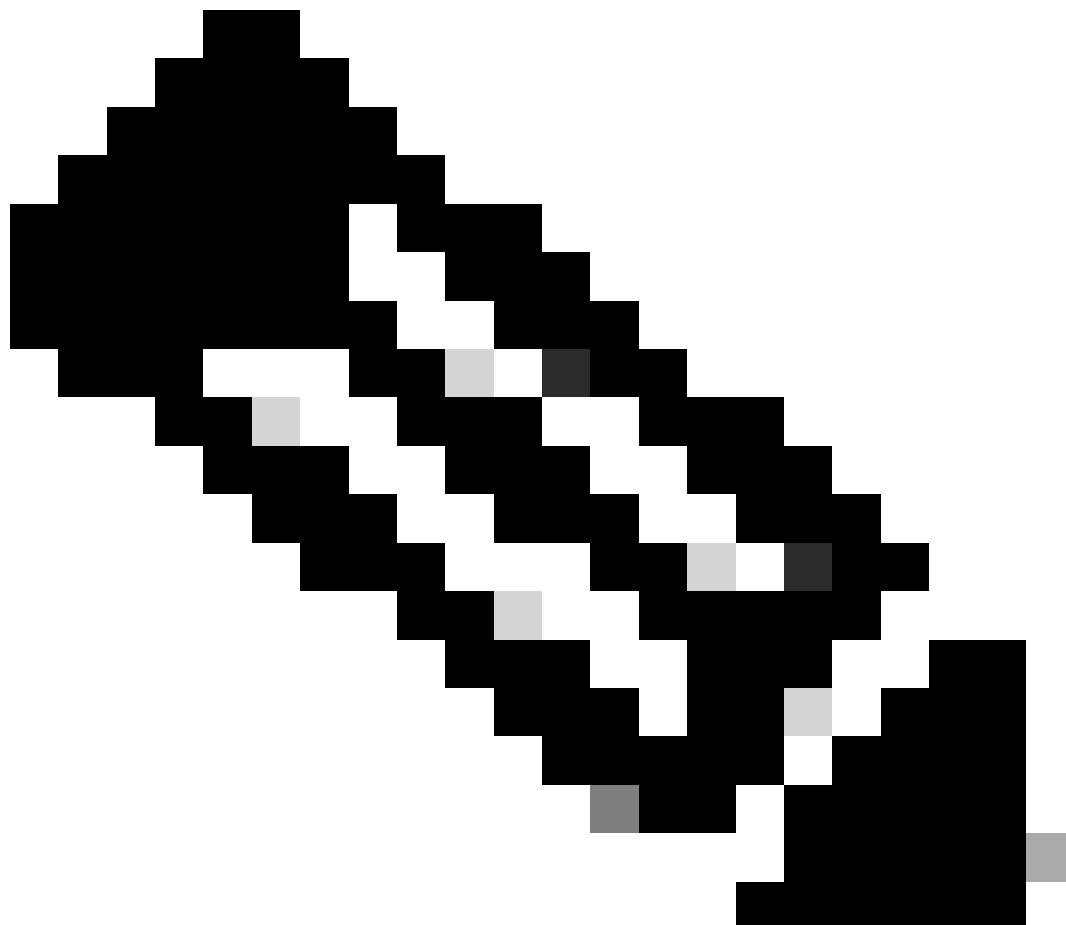


Creazione di condizioni

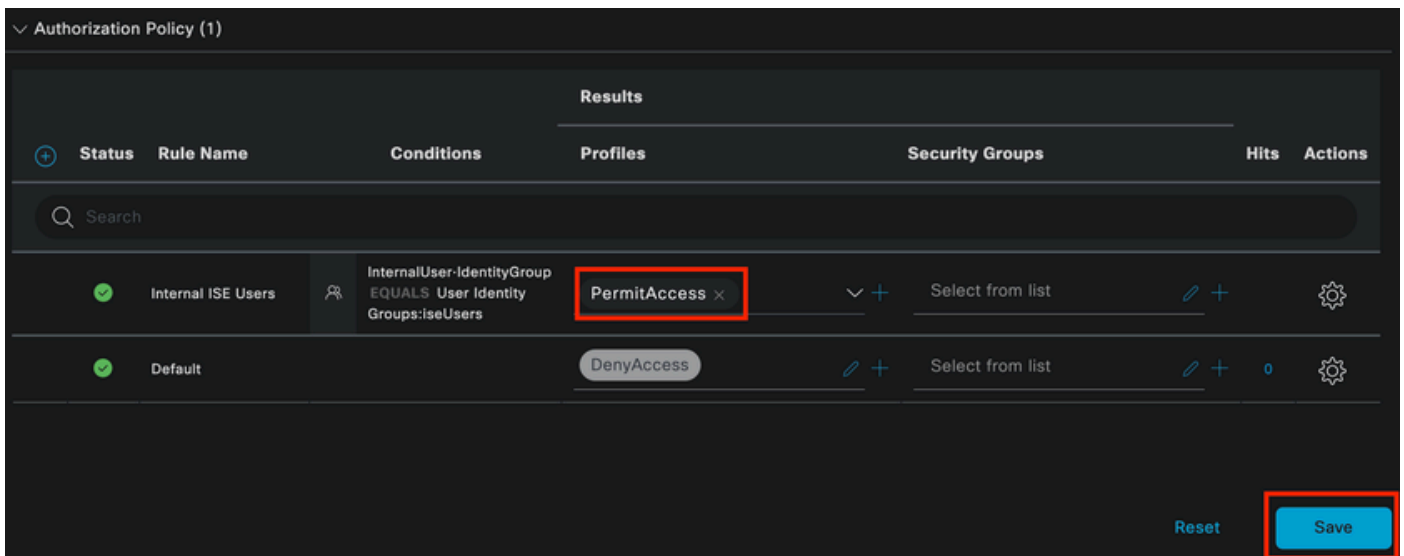
Fare clic su Usa.

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.



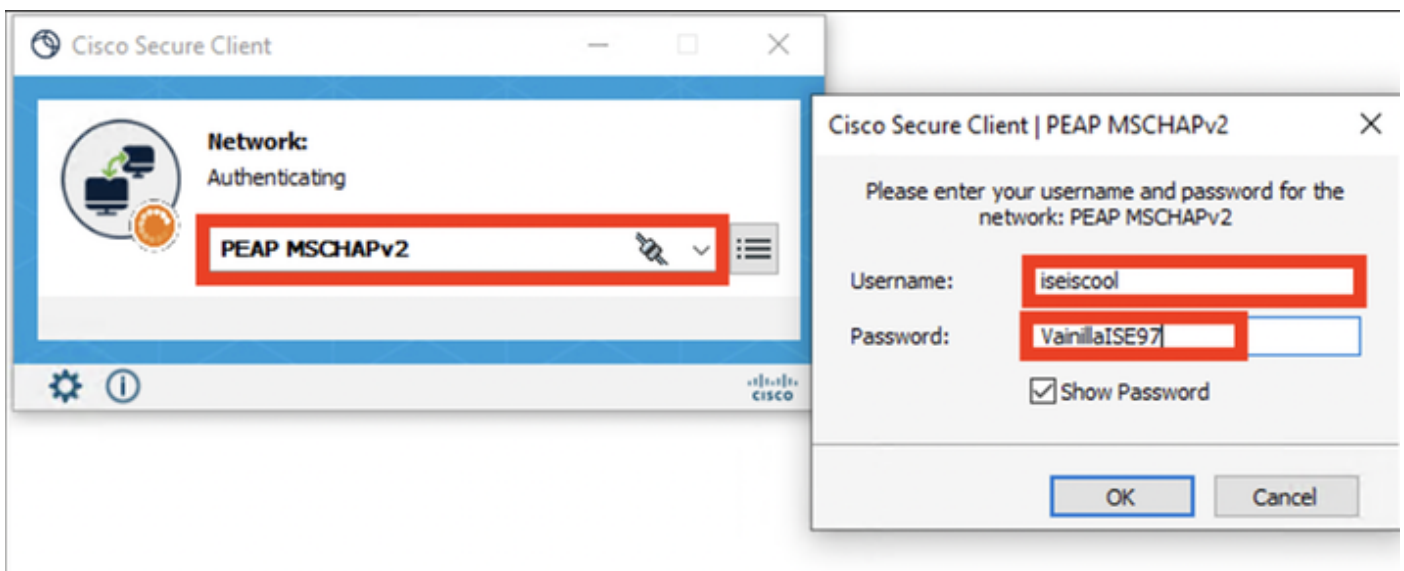
Criteria di autorizzazione

Fare clic su Save (Salva).

Verifica

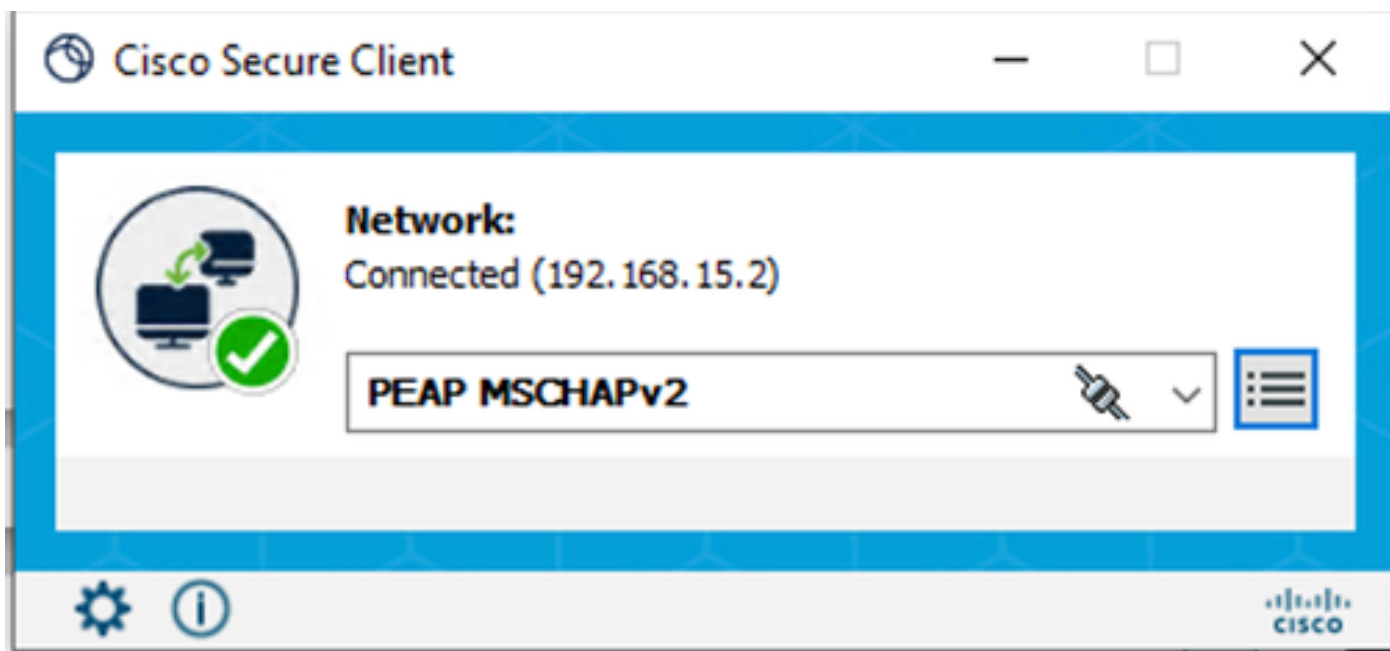
Al termine della configurazione, Secure Client richiede le credenziali e specifica l'utilizzo del profilo PEAP MSCHAPv2.

Verranno immesse le credenziali create in precedenza.



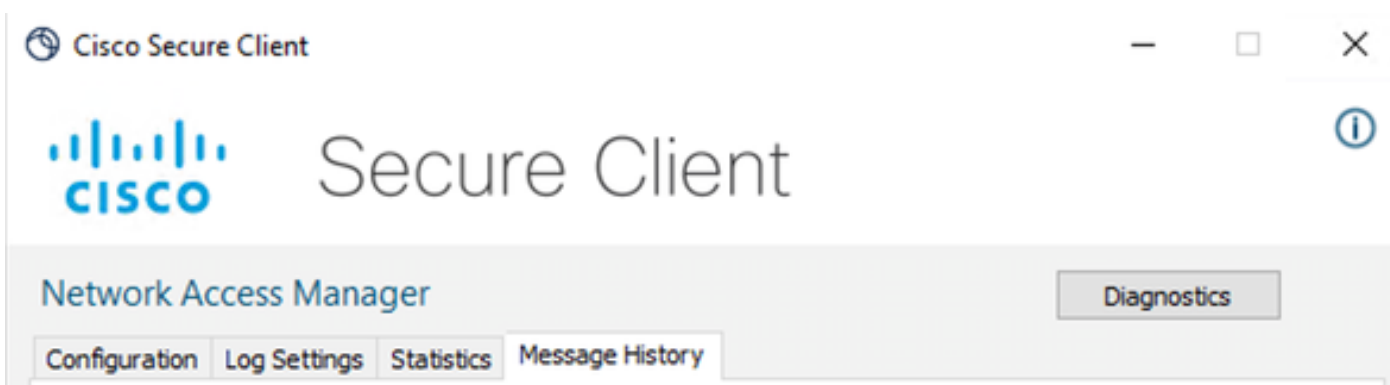
Secure Client NAM

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

```
7:06:01 PM PEAP MSCHAPv2 : Authenticating
7:06:21 PM PEAP MSCHAPv2 : Acquiring IP Address
7:06:21 PM PEAP MSCHAPv2 : Connected
```

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.

The screenshot shows the Cisco ISE Operations - RADIUS interface. At the top, there are navigation tabs for 'Live Logs' and 'Live Sessions'. Below this, there are five summary cards: 'Misconfigured Supplicants' (0), 'Misconfigured Network Devices' (0), 'RADIUS Drops' (25), 'Client Stopped Responding' (0), and 'Repeat Counter' (0). Below the cards, there are controls for 'Refresh' (Never), 'Show' (Latest 20 records), and 'Within' (Last 5 minutes). A table below shows the live log entries with columns: Time, Status, Details, Repea..., Identity, Endpoint ID, Endpoint..., Authentication Policy, Authorization Policy, Authoriz..., IP Address, and Network De... The table contains two rows of data for the date Apr 23, 2024. The first row has a status of 'Success' (blue dot) and the second row has a status of 'Success' (green checkmark). At the bottom, it says 'Last Updated: Tue Apr 23 2024 13:02:14 GMT-0600 (Central Standard Time)' and 'Records Shown: 2'.

Live log ISE RADIUS

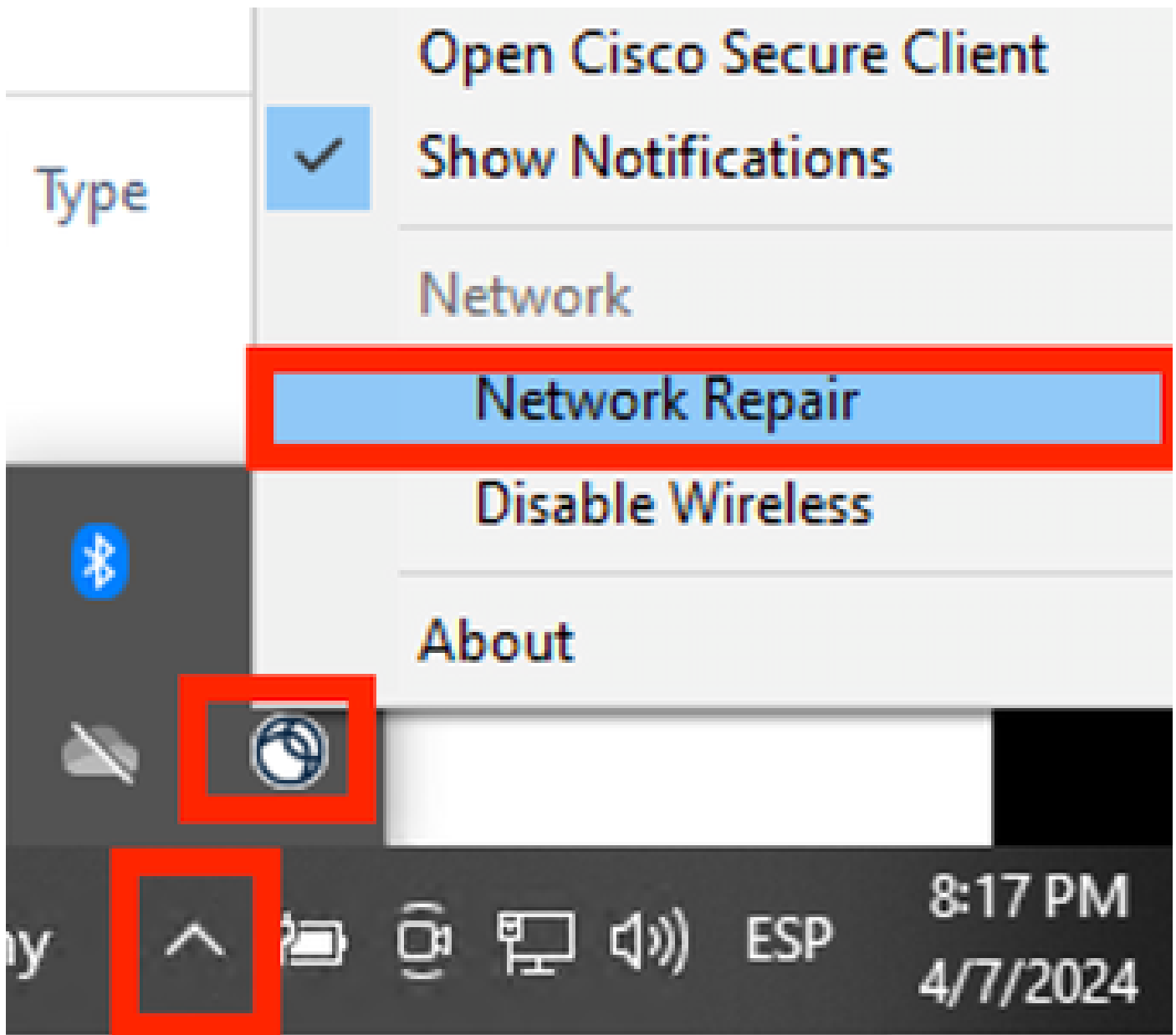
Dal momento che è possibile verificare che la configurazione rispetta i criteri corretti e che lo stato di autenticazione ha esito positivo, si può concludere che la configurazione è corretta.

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

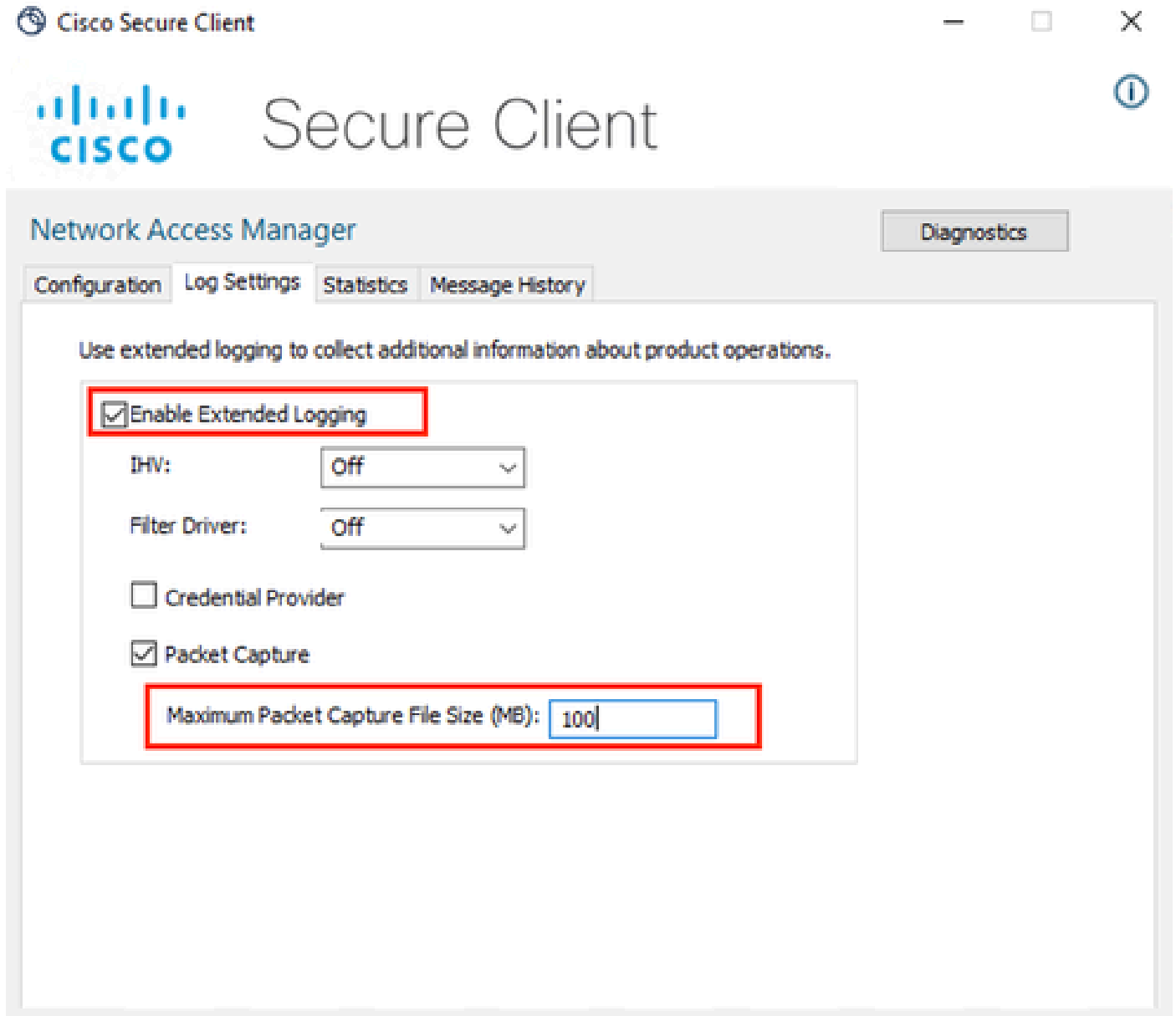
Aprirete NAM e fate clic sull'icona ingranaggio.



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.



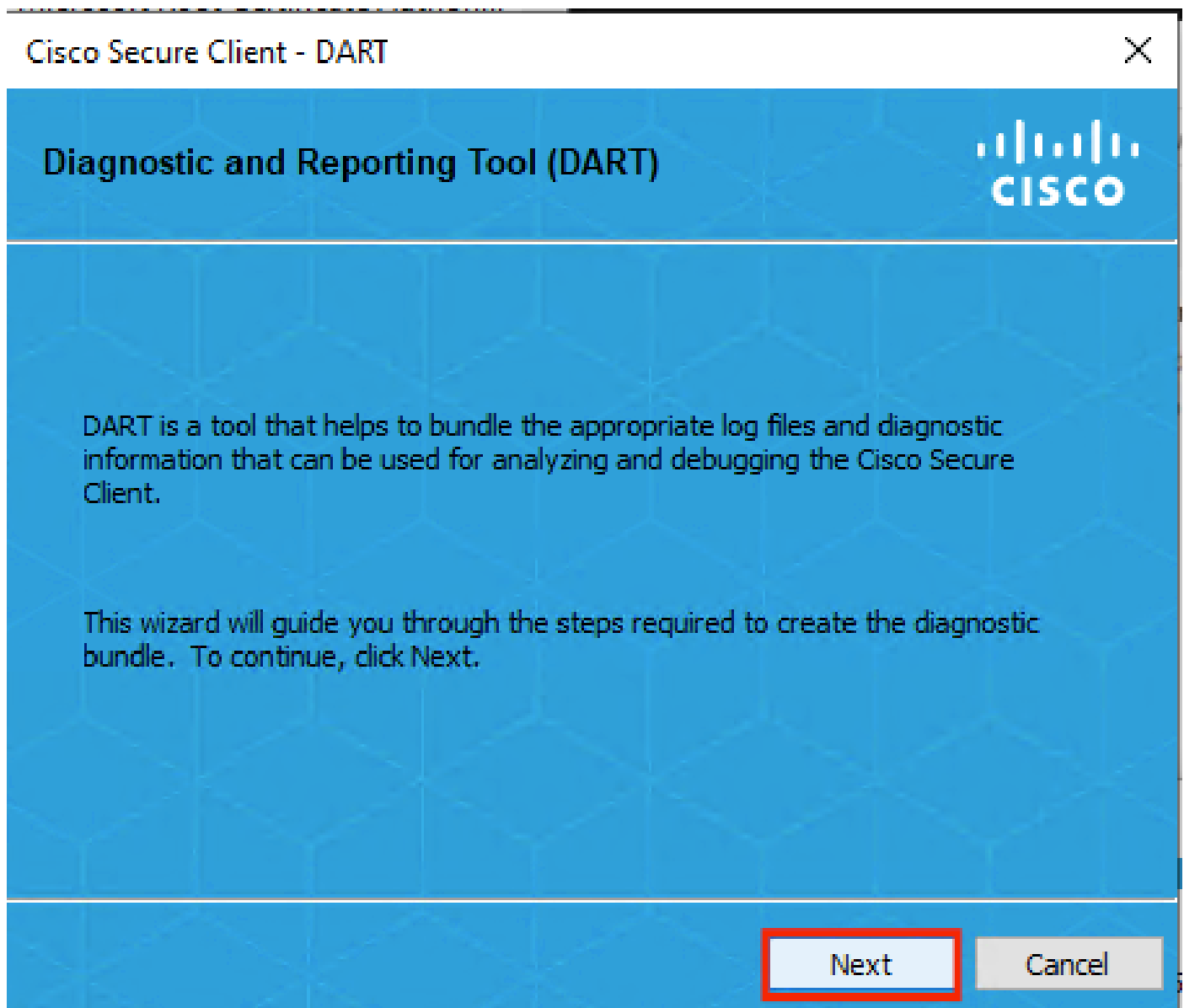
Cisco Secure Client Diagnostics and Reporting Tool

App

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.

Cisco Secure Client - DART




Bundle Creation Option 

Select "Default" to include the typical log files and diagnostic information in the bundle. Select "Custom" to choose the list of log files and diagnostic information to be included in the bundle.

Default - Bundle will be saved to Desktop

Custom

 DART requires administrative privileges to clear Cisco Secure Client logs.

[Clear All Logs](#)

[Back](#) [Next](#) [Cancel](#)

Modulo DART

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



Bundle Encryption Option



Enable Bundle Encryption

Mask Password

Encryption Password

Confirm Password

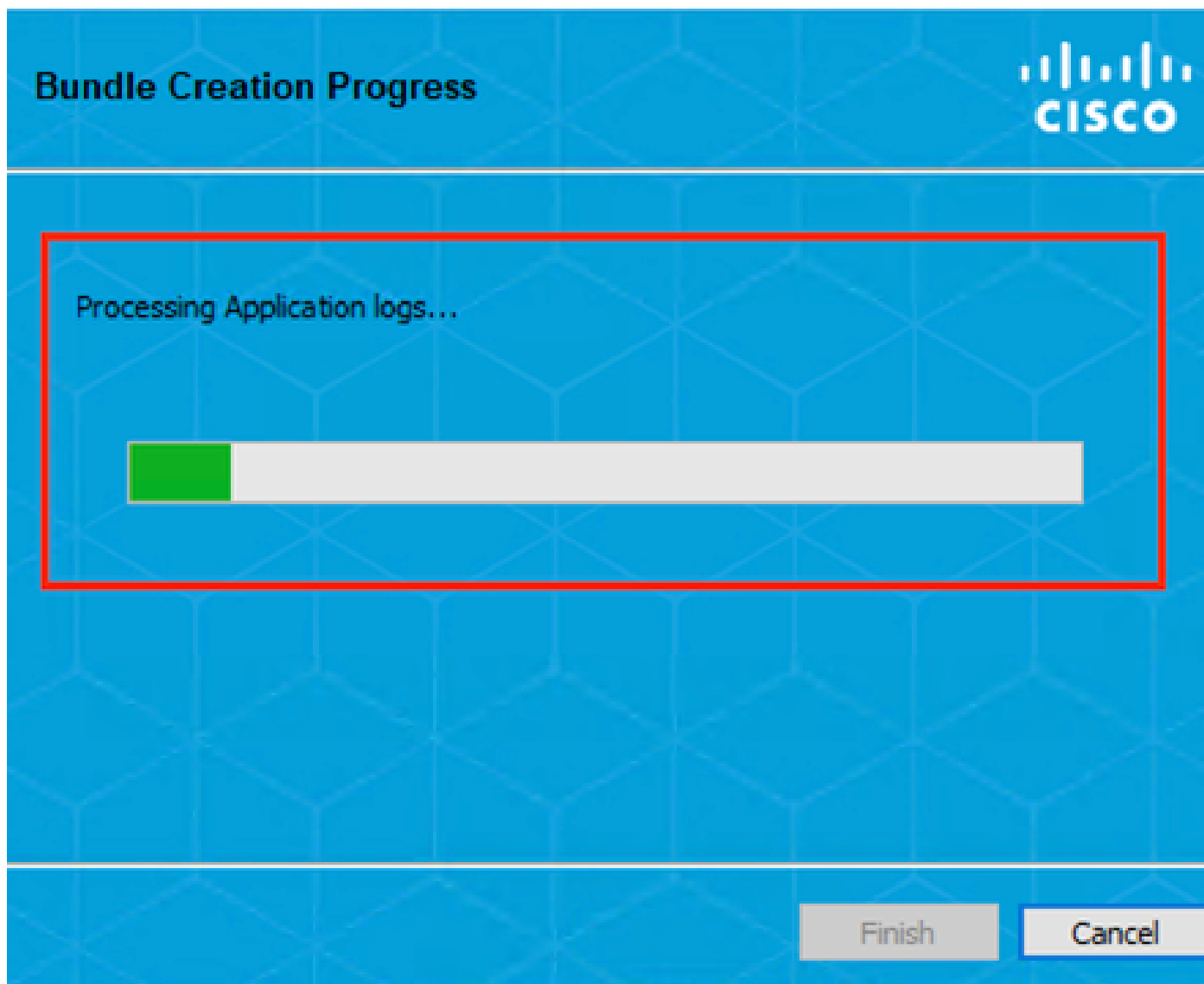
Back

Next

Cancel

Modulo DART

Verrà avviata la raccolta di log DART.



Raccolta di log DART

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

Bundle Creation Result




The bundle was created successfully in C:\Users\LAB5\Desktop\DARTBundle_0423_1538.zip.

[Email Bundle](#)[Finish](#)

Risultato creazione bundle DART

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

Name	Date modified	Type
 DARTBundle_0423_1538	4/24/2024 1:14 PM	Compressed (zipped) Folder

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).