Configure Secure Client NAM for Dot1x Using Windows and ISE 3.2

Contents

Introduction

This document describes how to configure Secure Client Network Analysis Module (NAM) on Windows.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic understanding of what is a RADIUS supplicant
- Dot1x
- PEAP
- PKI

Components Used

The information in this document is based on these software and hardware versions:

- Windows 10 Pro Version 22H2 Built 19045.3930
- ISE 3.2
- Cisco C1117 Cisco IOS® XE Software, Version 17.12.02
- Active Directory 2016

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This document describes how to configure Secure Client NAM on Windows. Pre-deploy option and Profile Editor to perform dot1x authentication are used. Also, some examples of how this is achieved are provided.

In networking, a supplicant is an entity at one end of a point-to-point LAN segment that seeks to be authenticated by an authenticator attached to the other end of that link. The IEEE 802.1X standard uses the term supplicant to refer to either hardware or software. In practice, a supplicant is a software application installed on an end-user computer. The user invokes the supplicant and submits credentials to connect the computer to a secure network. If the authentication succeeds, the authenticator typically allows the computer to connect to the network.

About Network Access Manager

Network Access Manager is client software that provides a secure Layer 2 network in accordance with its policies. It detects and selects the optimal Layer 2 access network and performs device authentication for access to both wired and wireless networks. Network Access Manager manages user and device identity and the network access protocols required for secure access. It works intelligently to prevent end users from making connections that are in violation of administrator-defined policies.

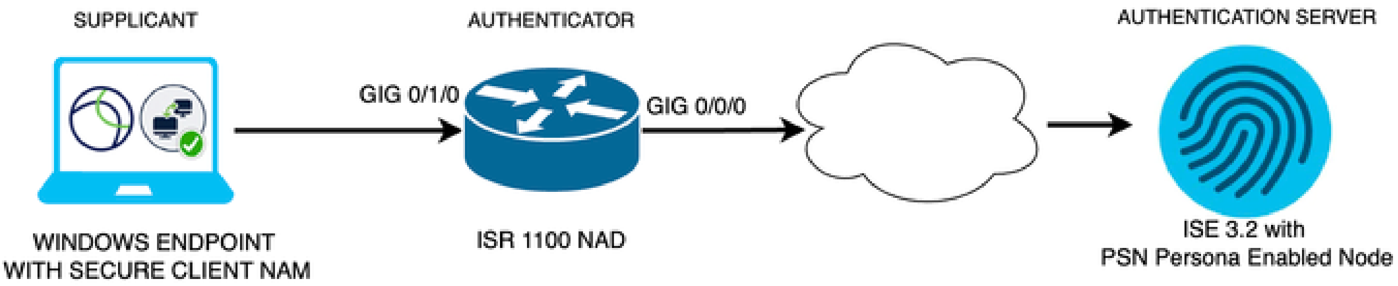
The Network Access Manager is designed to be single-homed, allowing only one network connection at a time. Also, wired connections have higher priority than wireless so if you are plugged into the network with a wired connection, the wireless adapter becomes disabled with no IP address.

Configure

Network Diagram

It is crucial to understand that for dot1x authentications 3 parts are needed; the supplicant which can do dot1x, the authenticator also known as NAS/NAD which serves as a proxy encapsulating the dot1x traffic inside RADIUS, and the authentication Server.

In this example, the supplicant is installed and configured in different ways. Later on, a scenario with the Network device config and the authentication server is shown.



Network Diagram

Configurations

1. Download and Install Secure Client NAM (Network Access Manager).
2. Download and install Secure Client NAM profile editor.
3. General default configurations
4. Scenario 1: Configure the Secure Client NAM Supplicant for PEAP (MS-CHAPv2) User Authentication.
5. Scenario 2: Configure the Secure Client NAM Supplicant for EAP-FAST simultaneously as User and Machine Authentication are configured.
6. Scenario 3 Part 1: Configure the Secure Client NAM Supplicant for EAP-TLS.
7. Scenario 3 Part 2: Configure the NAD and ISE Demonstration.

1. Download and Install Secure Client NAM (Network Access Manager)

Cisco Software Download

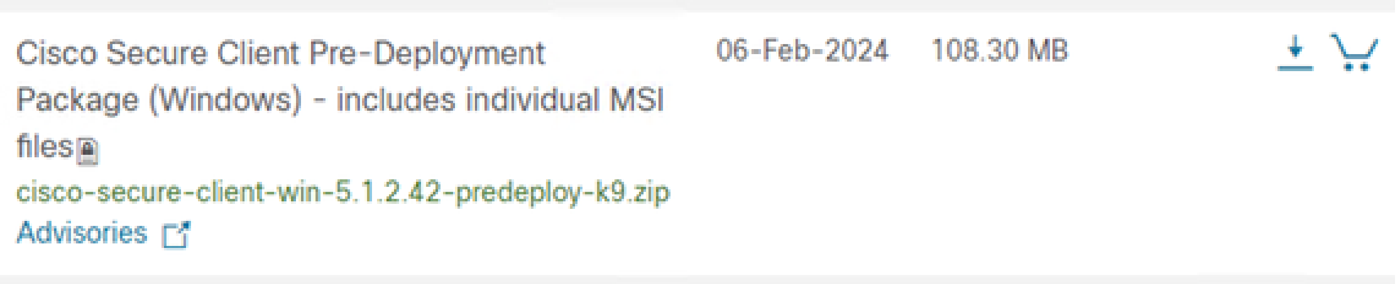
On the product name search bar type **Secure Client 5**.

Downloads Home > Security > VPN and Endpoint Security Clients > Secure Client (including AnyConnect) > Secure Client 5 > AnyConnect VPN Client Software.

In this configuration example, version 5.1.2.42 is the one used.

There are multiple ways to deploy Secure Client to Windows devices; from SCCM, from the Identity service engine, and from the VPN headend. However, in this article, the installation method used is the pre-deploy method.

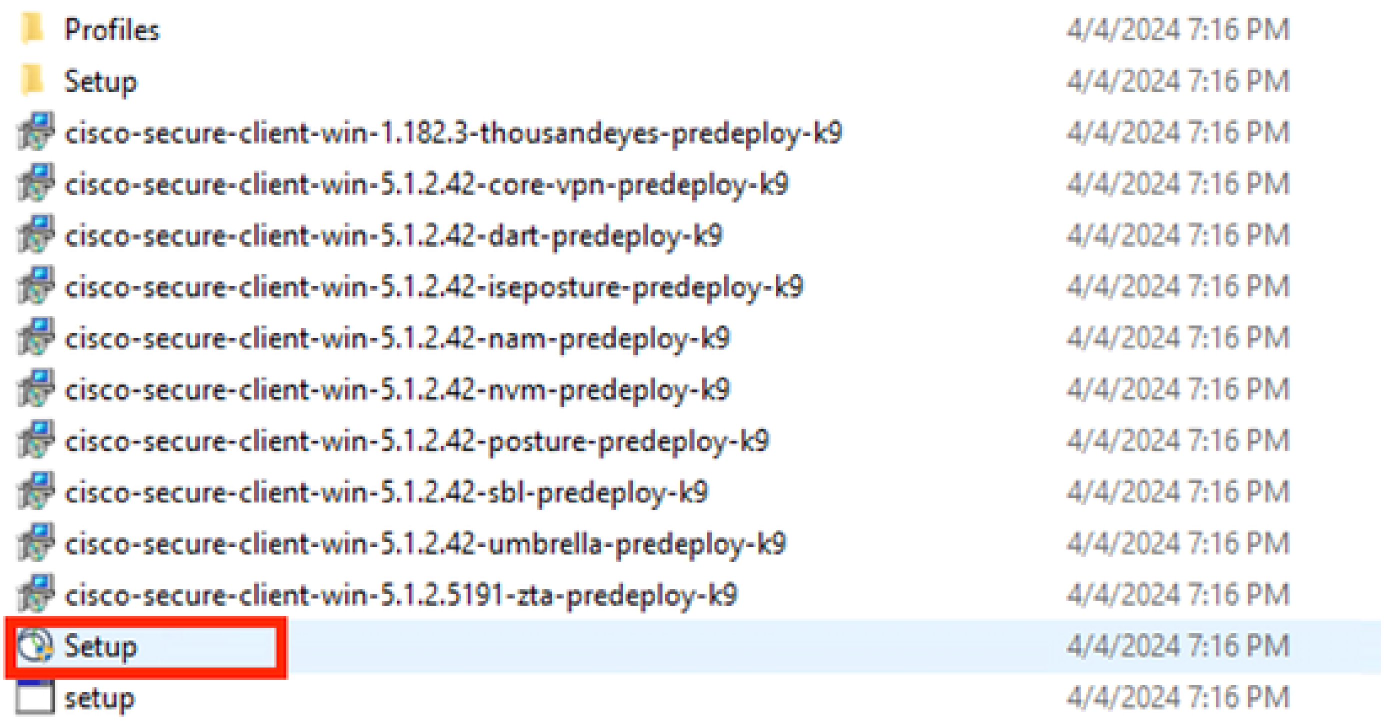
On the page, search for the file **Cisco Secure Client Headend Deployment Package (Windows)**.



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

Msi zip file

Once downloaded and extracted, click **Setup**.

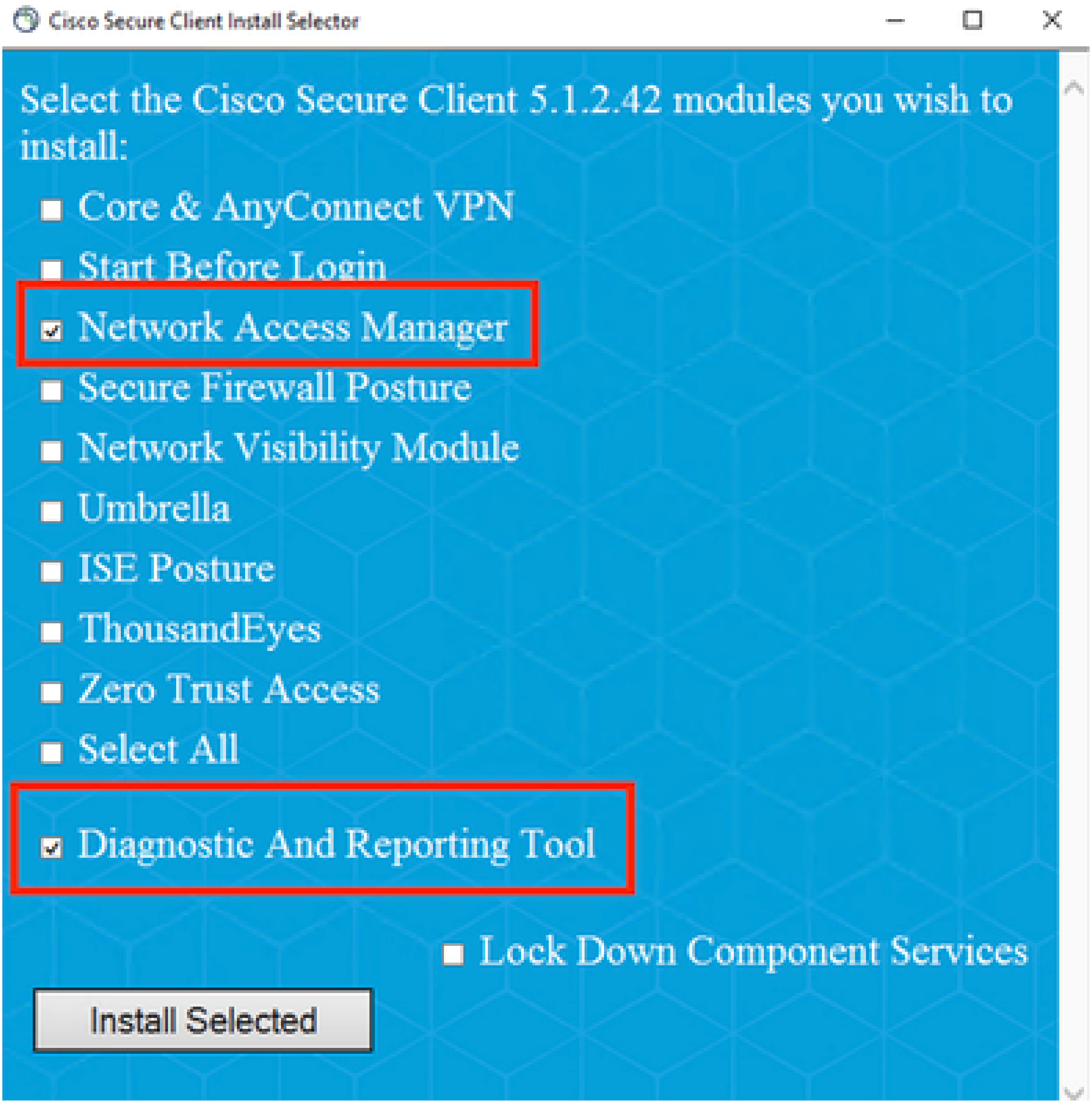


Profiles	4/4/2024 7:16 PM
Setup	4/4/2024 7:16 PM
cisco-secure-client-win-1.182.3-thousandeyes-predeploy-k9	4/4/2024 7:16 PM
cisco-secure-client-win-5.1.2.42-core-vpn-predeploy-k9	4/4/2024 7:16 PM
cisco-secure-client-win-5.1.2.42-dart-predeploy-k9	4/4/2024 7:16 PM
cisco-secure-client-win-5.1.2.42-iseposture-predeploy-k9	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

Secure Client Files

Install the **Network Access Manager** and the **Diagnostics and Reporting Tool** modules.

Warning: If you use Cisco Secure Client Wizard, the VPN module is installed automatically, and hidden in the GUI. NAM does not work if the VPN module is not installed. If you use individual MSI files or a different installation method, ensure you install the VPN module.



Cisco Secure Client Install Selector

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

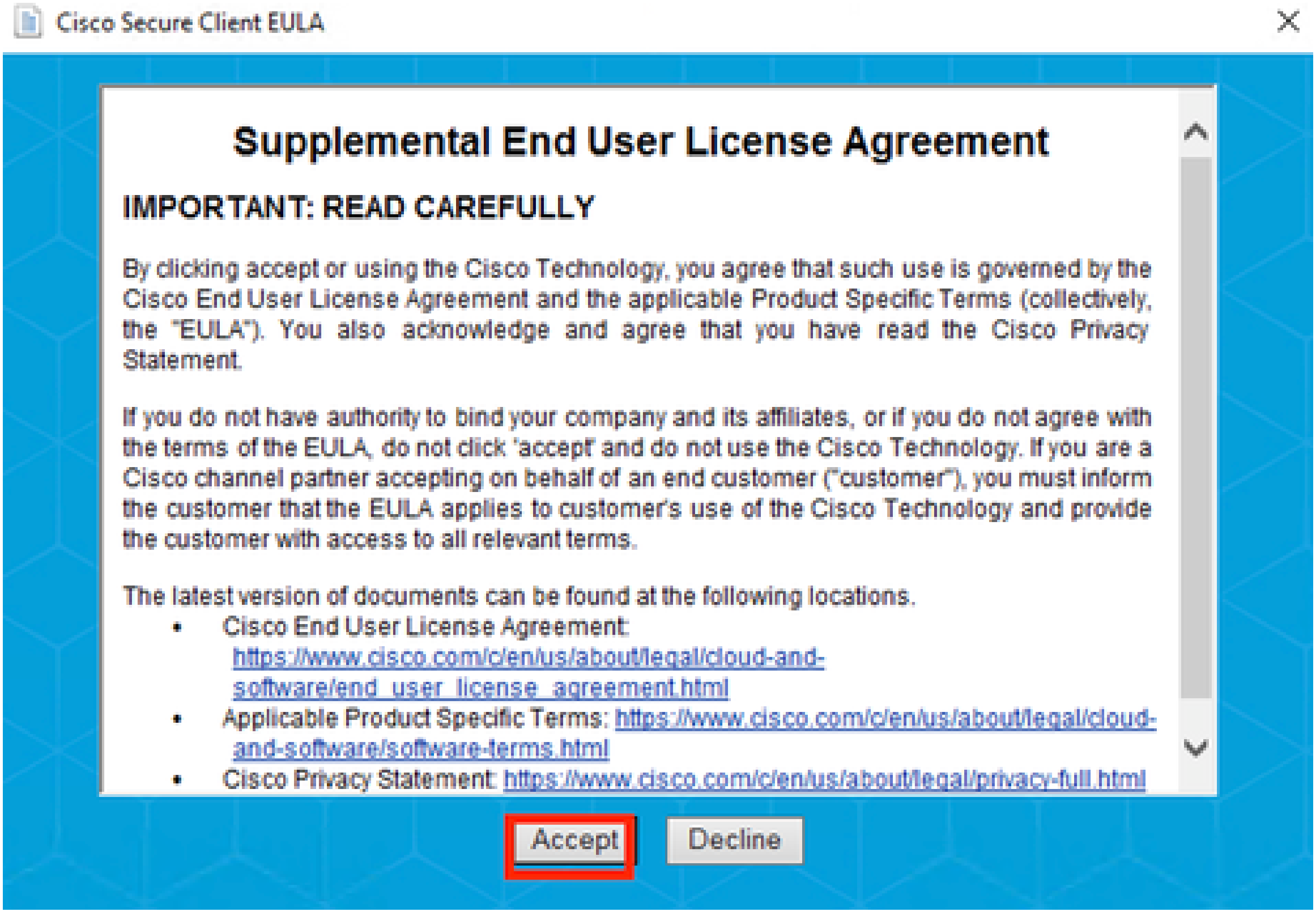
☑ Diagnostic And Reporting Tool

□ Lock Down Component Services

Install Selector

Click **Install Selected**.

Accept the EULA.



Supplemental End User License Agreement

IMPORTANT: READ CAREFULLY

By clicking accept or using the Cisco Technology, you agree that such use is governed by the Cisco End User License Agreement and the applicable Product Specific Terms (collectively, the "EULA"). You also acknowledge and agree that you have read the Cisco Privacy Statement.

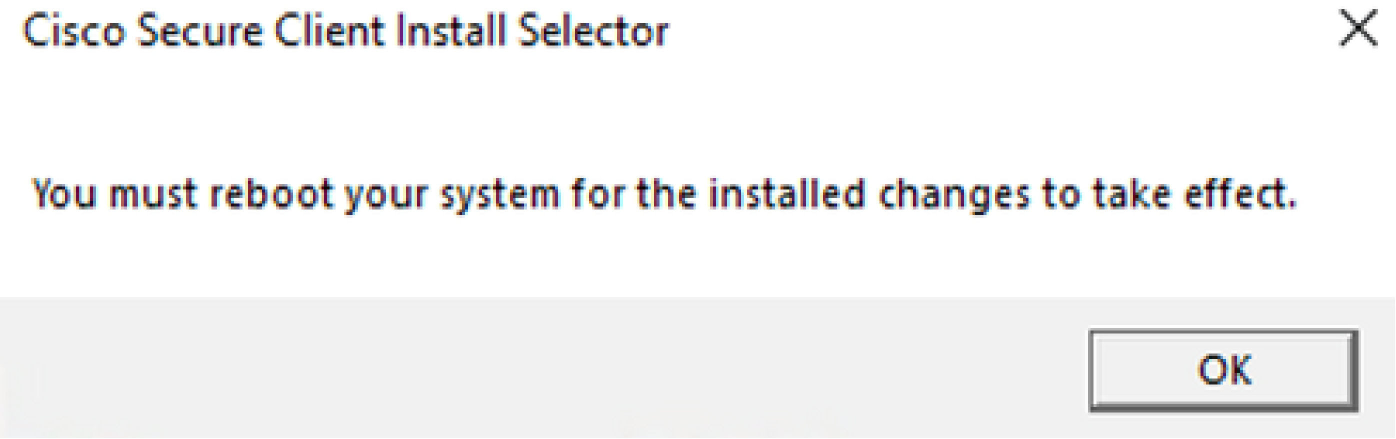
If you do not have authority to bind your company and its affiliates, or if you do not agree with the terms of the EULA, do not click 'accept' and do not use the Cisco Technology. If you are a Cisco channel partner accepting on behalf of an end customer ("customer"), you must inform the customer that the EULA applies to customer's use of the Cisco Technology and provide the customer with access to all relevant terms.

The latest version of documents can be found at the following locations.

- Cisco End User License Agreement: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/end_user_license_agreement.html
- Applicable Product Specific Terms: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html
- Cisco Privacy Statement: https://www.cisco.com/c/en/us/about/legal/privacy-full.html

EULA Window

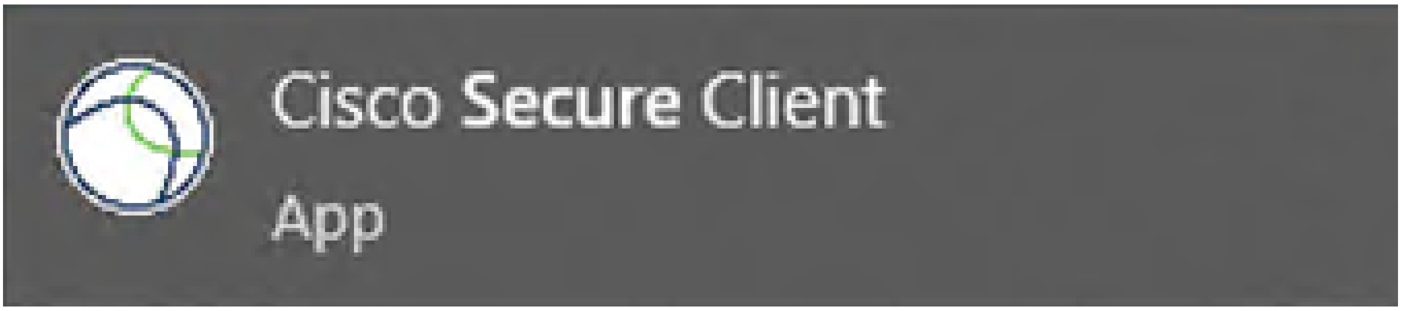
A restart is required after NAM installation.



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

Reboot Requirement Window

Once installed it can be found and opened from the Windows Search bar.



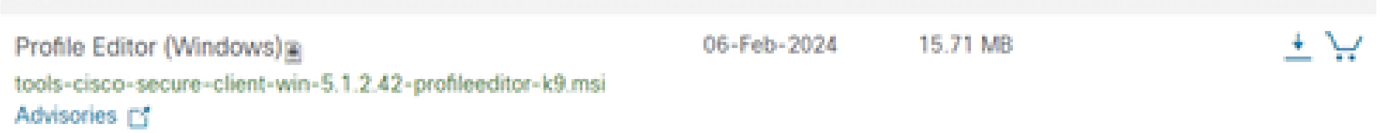
Secure Client Program

2. Download and Install Secure Client NAM Profile Editor.

Cisco Network Access Manager Profile Editor is required to configure the Dot1x preferences.

From the same page where Secure Client is downloaded, the **Profile Editor** option is found.

This example uses the option with version 5.1.2.42.



Profile Editor (Windows)
tools-cisco-secure-client-win-5.1.2.42-profileeditor-k9.msi
Advisories

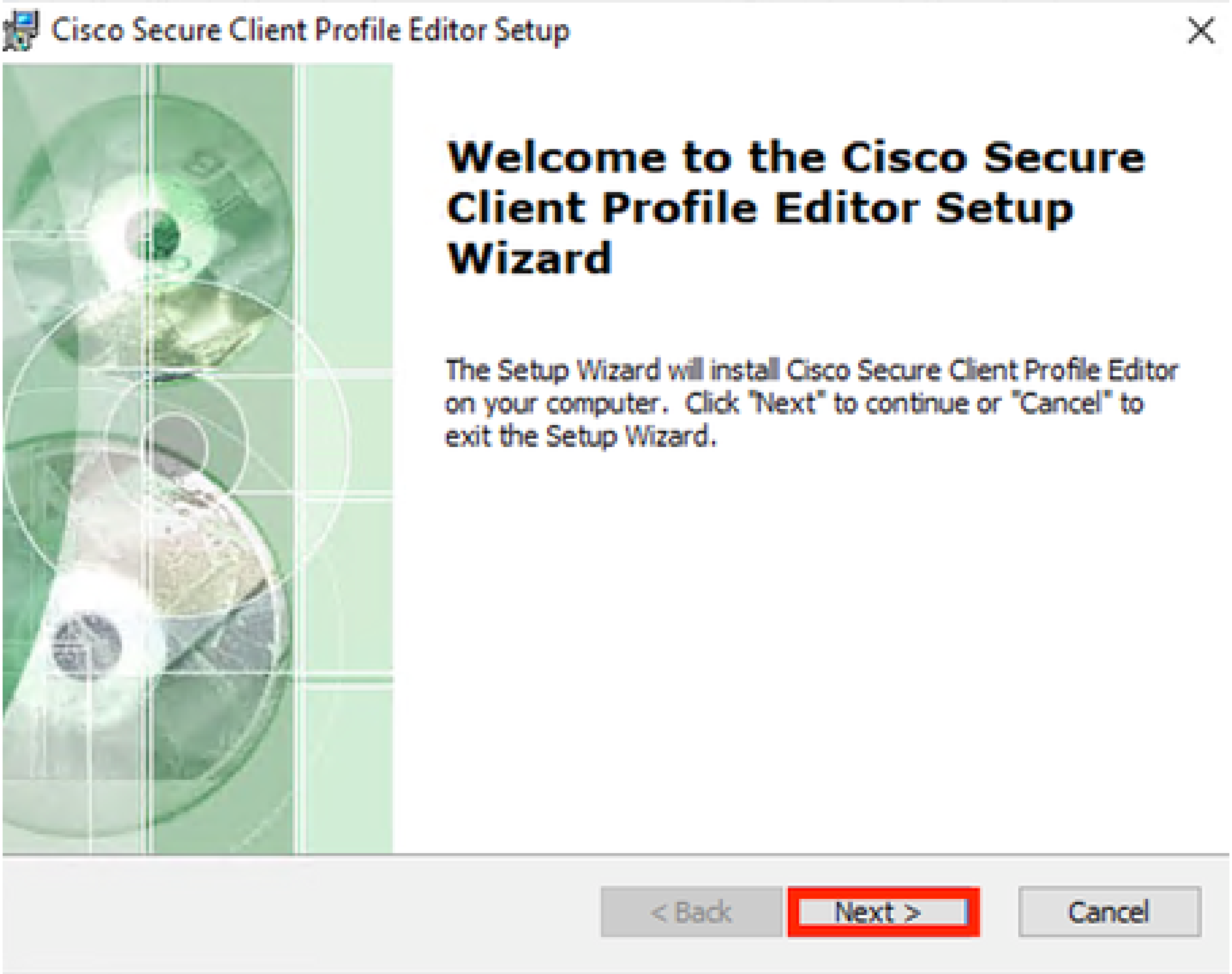
06-Feb-2024

15.71 MB

Profile Editor

Once it downloaded, proceed with the installation.

Run the msi file.



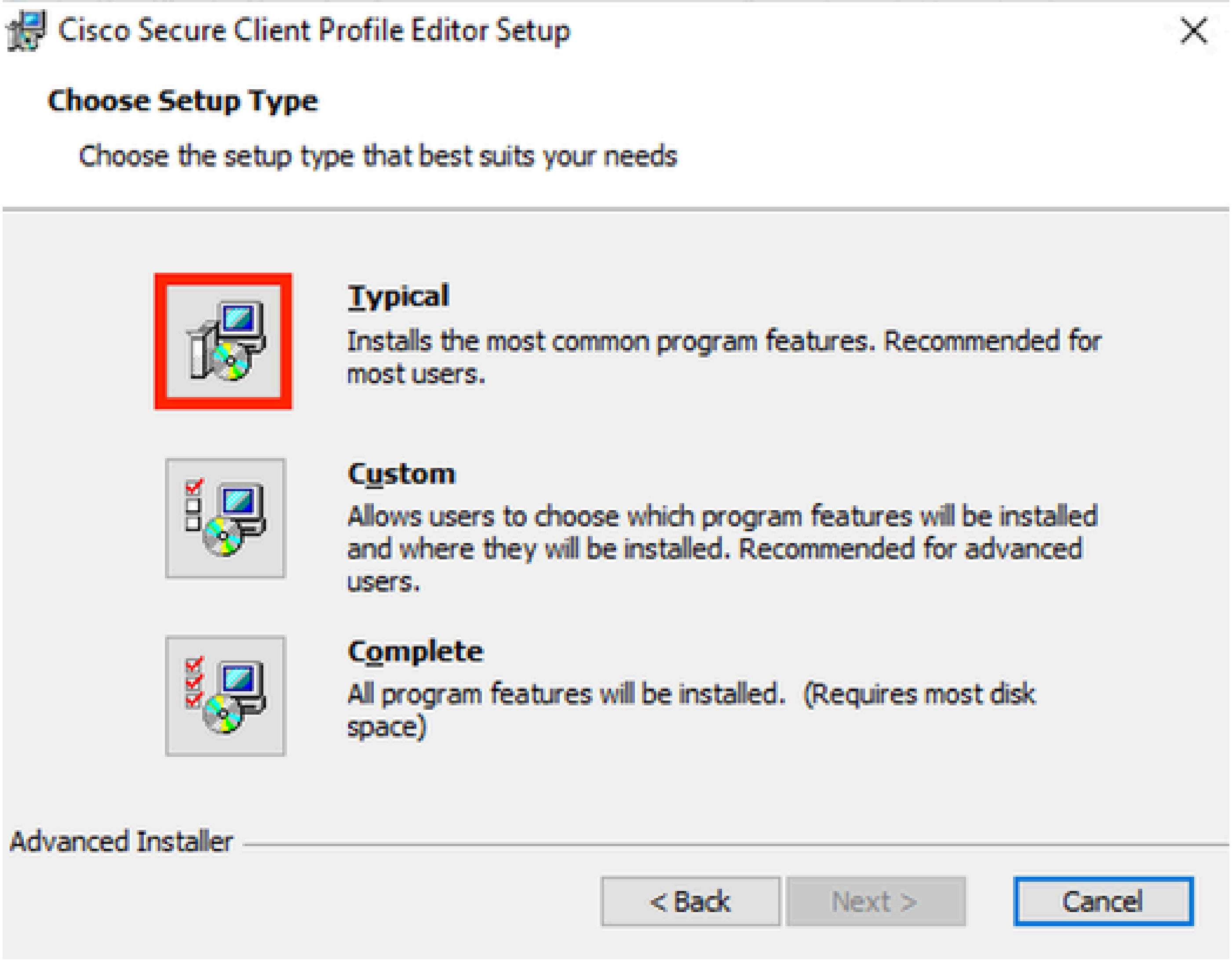
Cisco Secure Client Profile Editor Setup

Welcome to the Cisco Secure Client Profile Editor Setup Wizard

The Setup Wizard will install Cisco Secure Client Profile Editor on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

Profile Editor Setup Window

Use the **Typical** setup option.



Cisco Secure Client Profile Editor Setup

Choose Setup Type

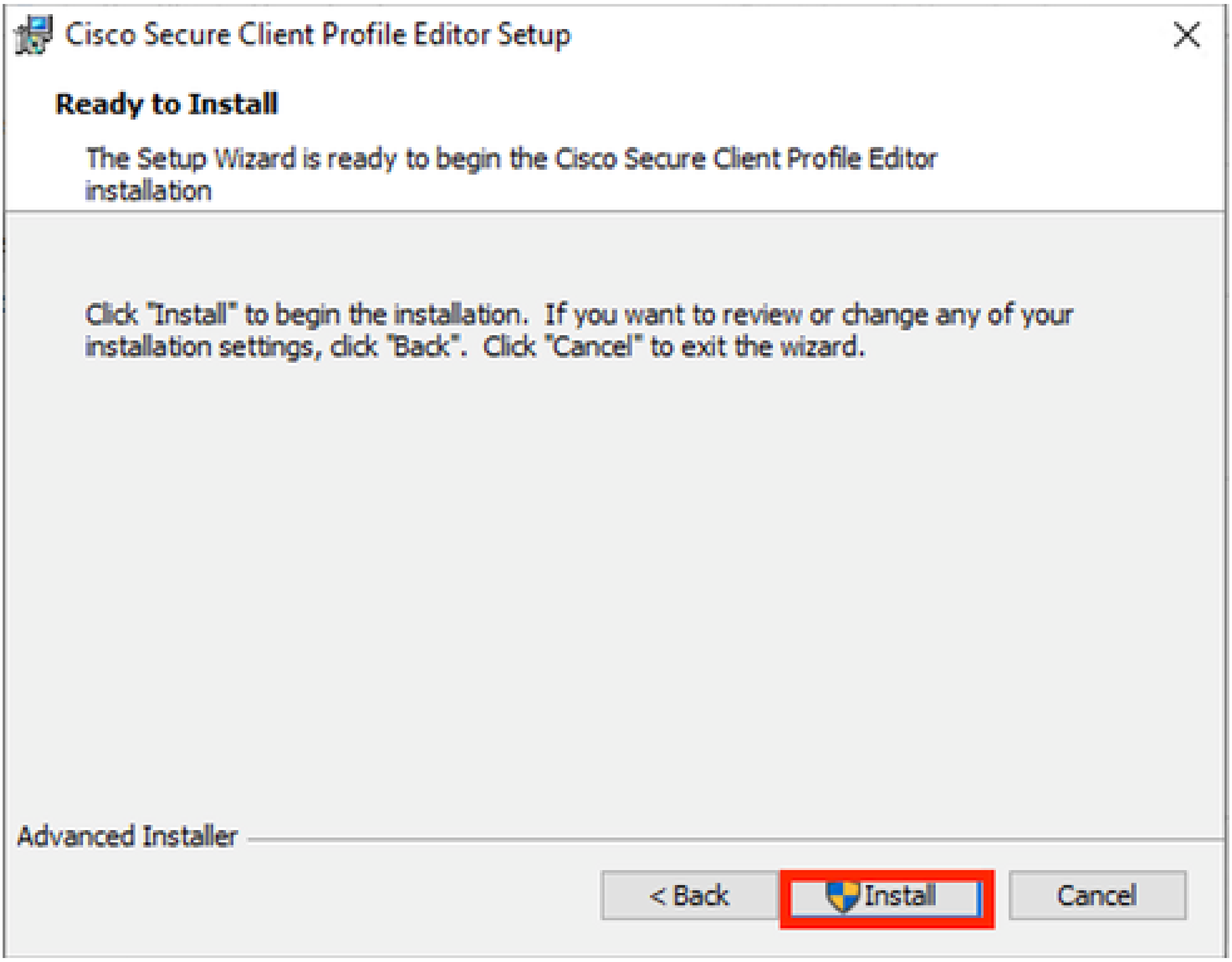
Choose the setup type that best suits your needs

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)

Profile Editor Setup



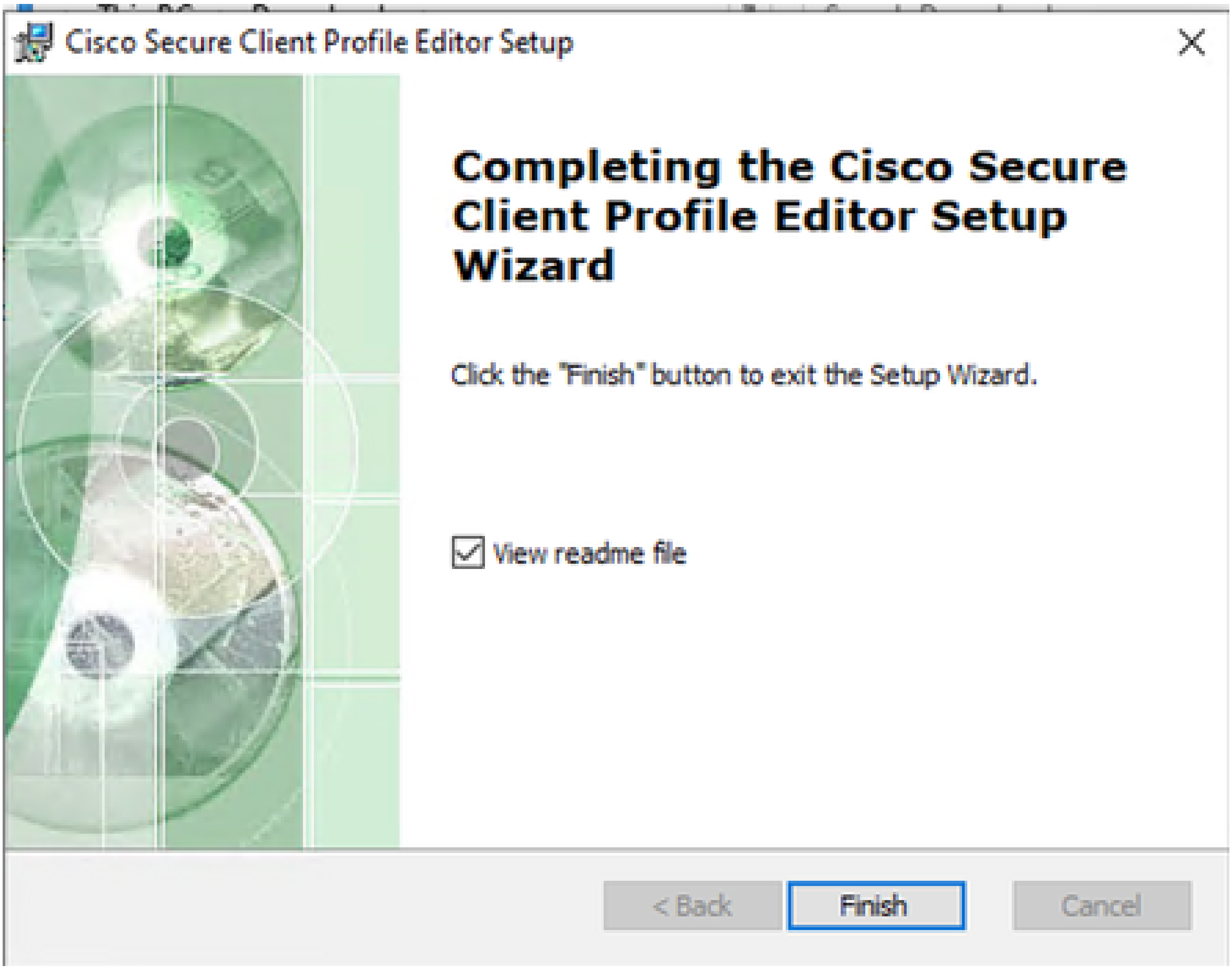
Ready to Install

The Setup Wizard is ready to begin the Cisco Secure Client Profile Editor installation

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

Installation Window

Click **Finish**.



Cisco Secure Client Profile Editor Setup

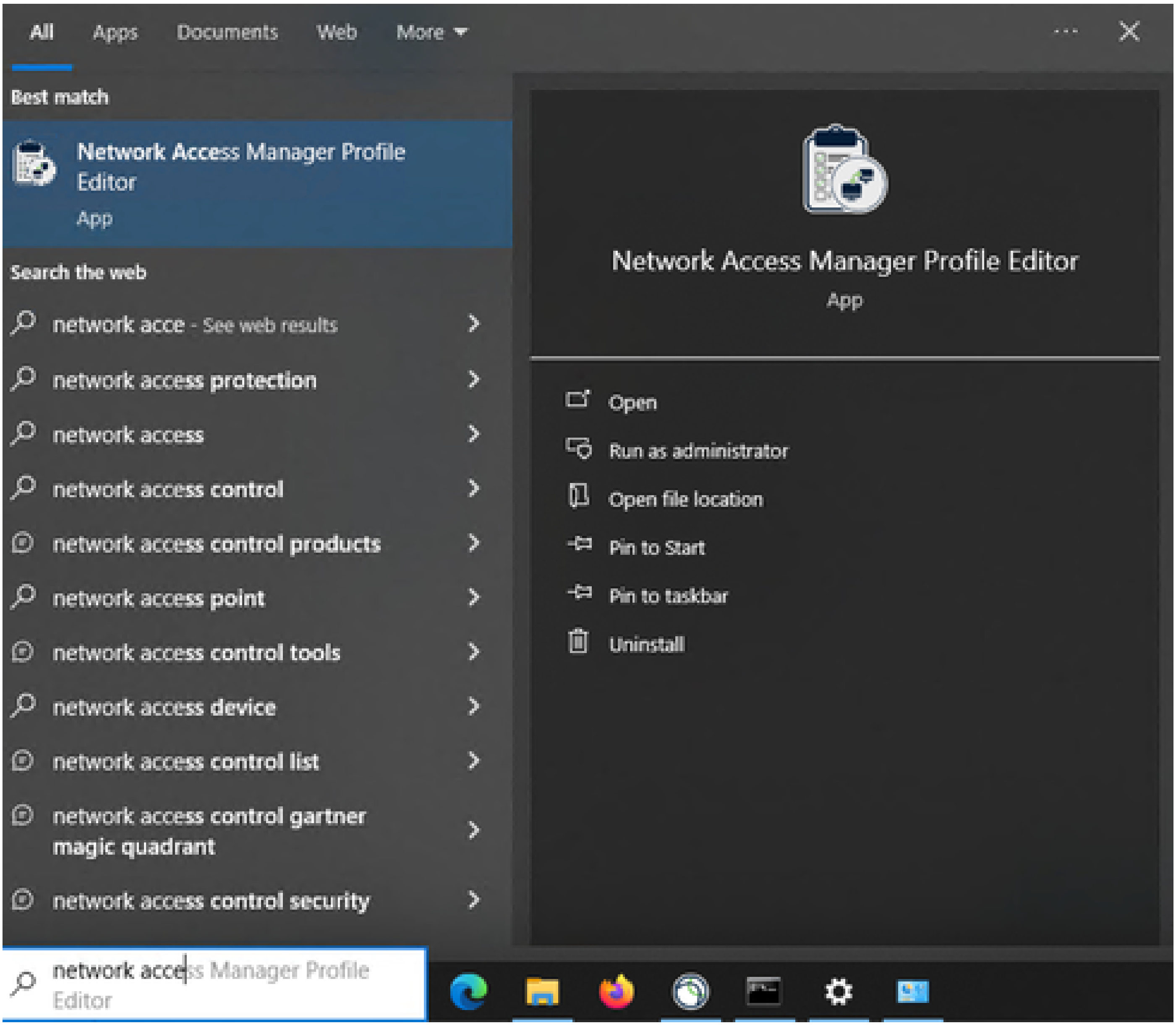
Completing the Cisco Secure Client Profile Editor Setup Wizard

Click the "Finish" button to exit the Setup Wizard.

☑ View readme file

End of Profile Editor Setup

Once installed, open **Network Access Manager Profile Editor** from the search bar.


All
Apps
Documents
Web
More
Best match
Network Access Manager Profile Editor
App
Search the web
network acce - See web results
network access protection
network access
network access control
network access control products
network access point
network access control tools
network access device
network access control list
network access control gartner magic quadrant
network access control security
network access Manager Profile Editor
Network Access Manager Profile Editor
App
Open
Run as administrator
Open file location
Pin to Start
Pin to taskbar
Uninstall

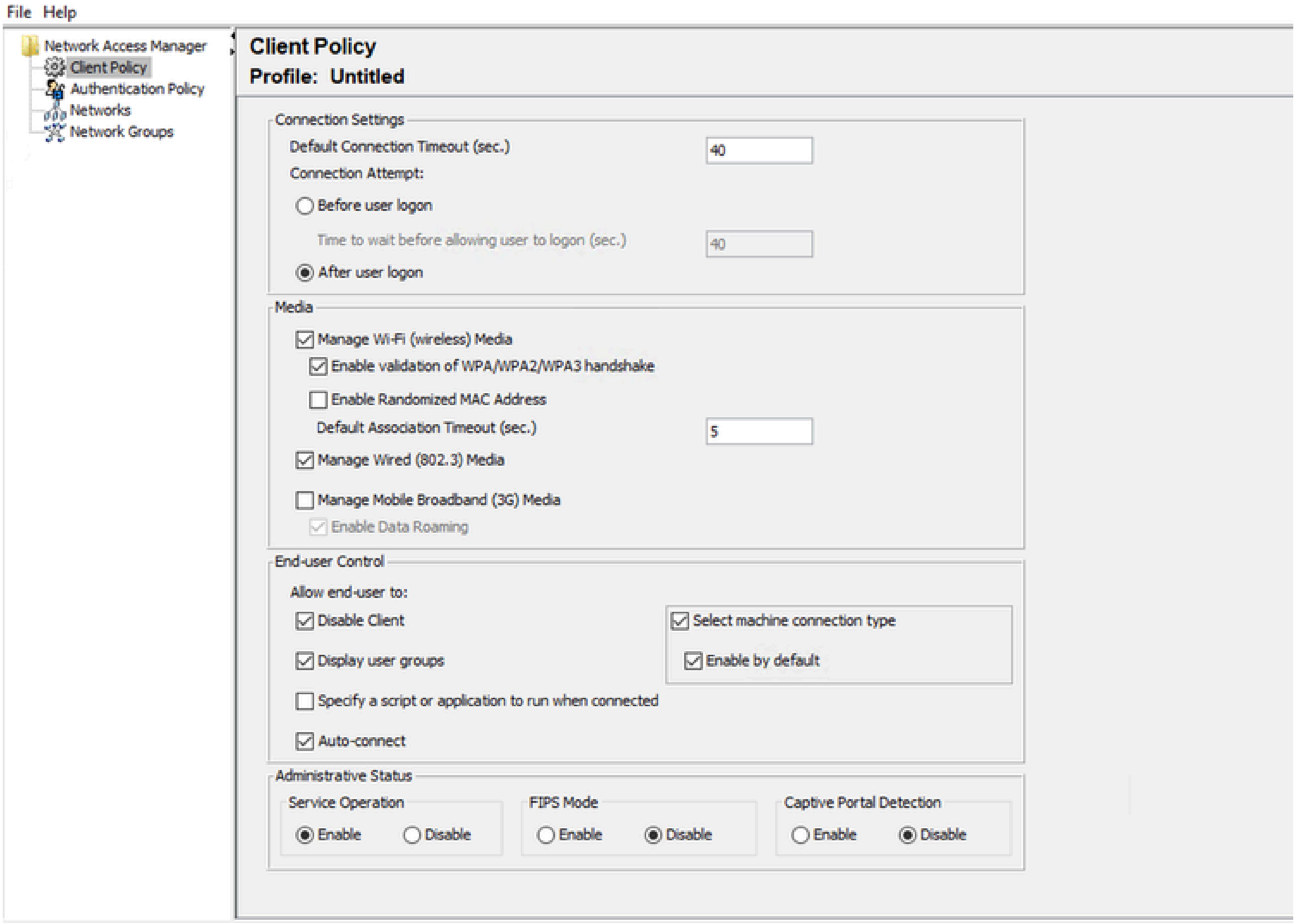
Profile Editor for NAM on Search Bar

Installation of Network Access Manager and Profile Editor is completed.

3. General Default Configurations

All the scenarios presented in this article contain configurations for:

- Client Policy
- Authentication Policy
- Network Groups



Client Policy

Profile: Untitled

Connection Settings

Default Connection Timeout (sec.) 40

Connection Attempt:

○ Before user logon

Time to wait before allowing user to logon (sec.) 40

● After user logon

Media

☑ Manage Wi-Fi (wireless) Media

☑ Enable validation of WPA/WPA2/WPA3 handshake

□ Enable Randomized MAC Address

Default Association Timeout (sec.) 5

☑ Manage Wired (802.3) Media

□ Manage Mobile Broadband (3G) Media

☑ Enable Data Roaming

End-user Control

Allow end-user to:

☑ Disable Client

☑ Display user groups

□ Specify a script or application to run when connected

☑ Auto-connect

☑ Select machine connection type

☑ Enable by default

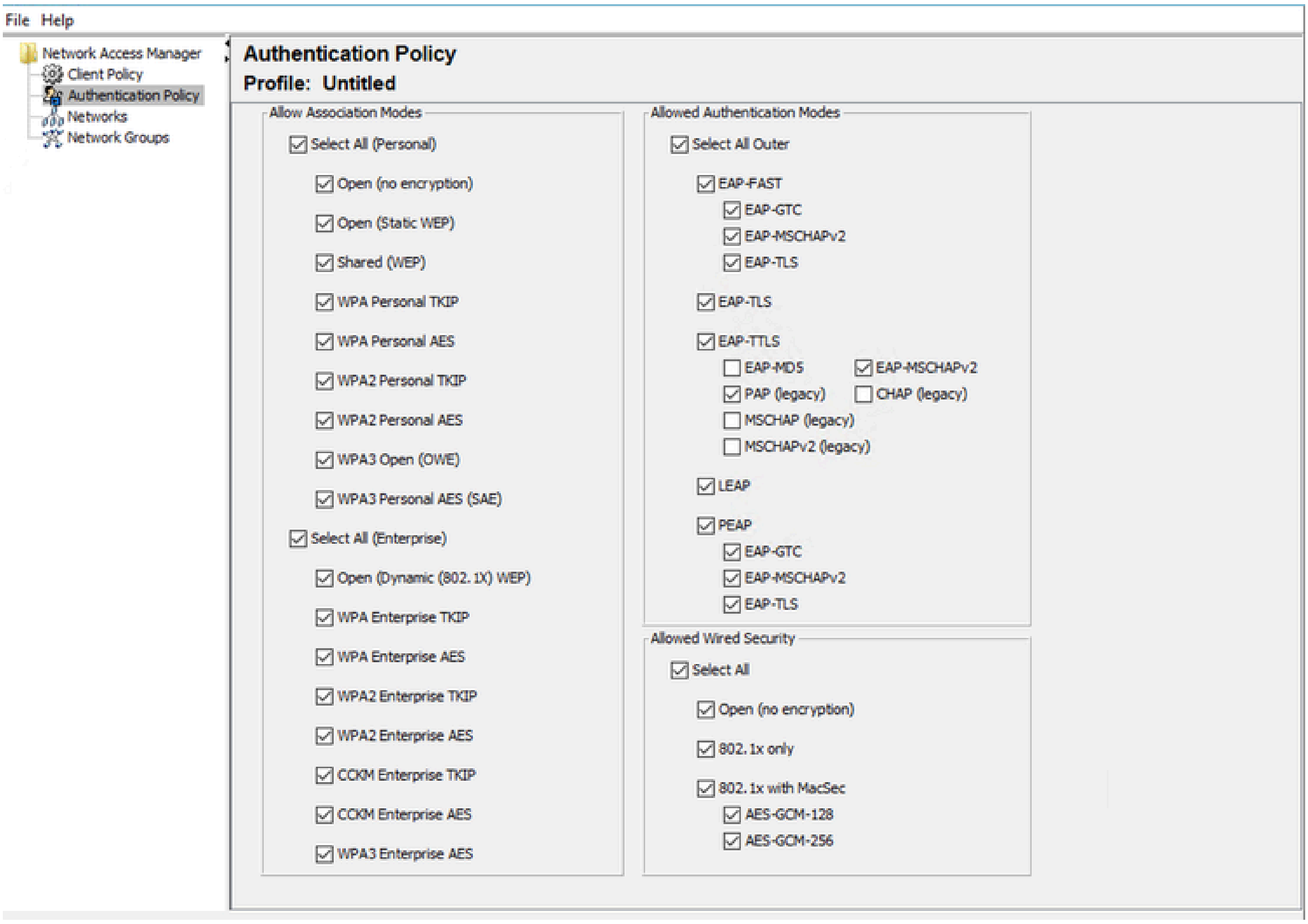
Administrative Status

Service Operation: ● Enable ○ Disable

FIPS Mode: ○ Enable ● Disable

Captive Portal Detection: ○ Enable ● Disable

NAM Profile Editor Client Policy



Authentication Policy

Profile: 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
  - ☑ CCKM Enterprise TKIP
  - ☑ CCKM Enterprise AES
  - ☑ WPA3 Enterprise AES

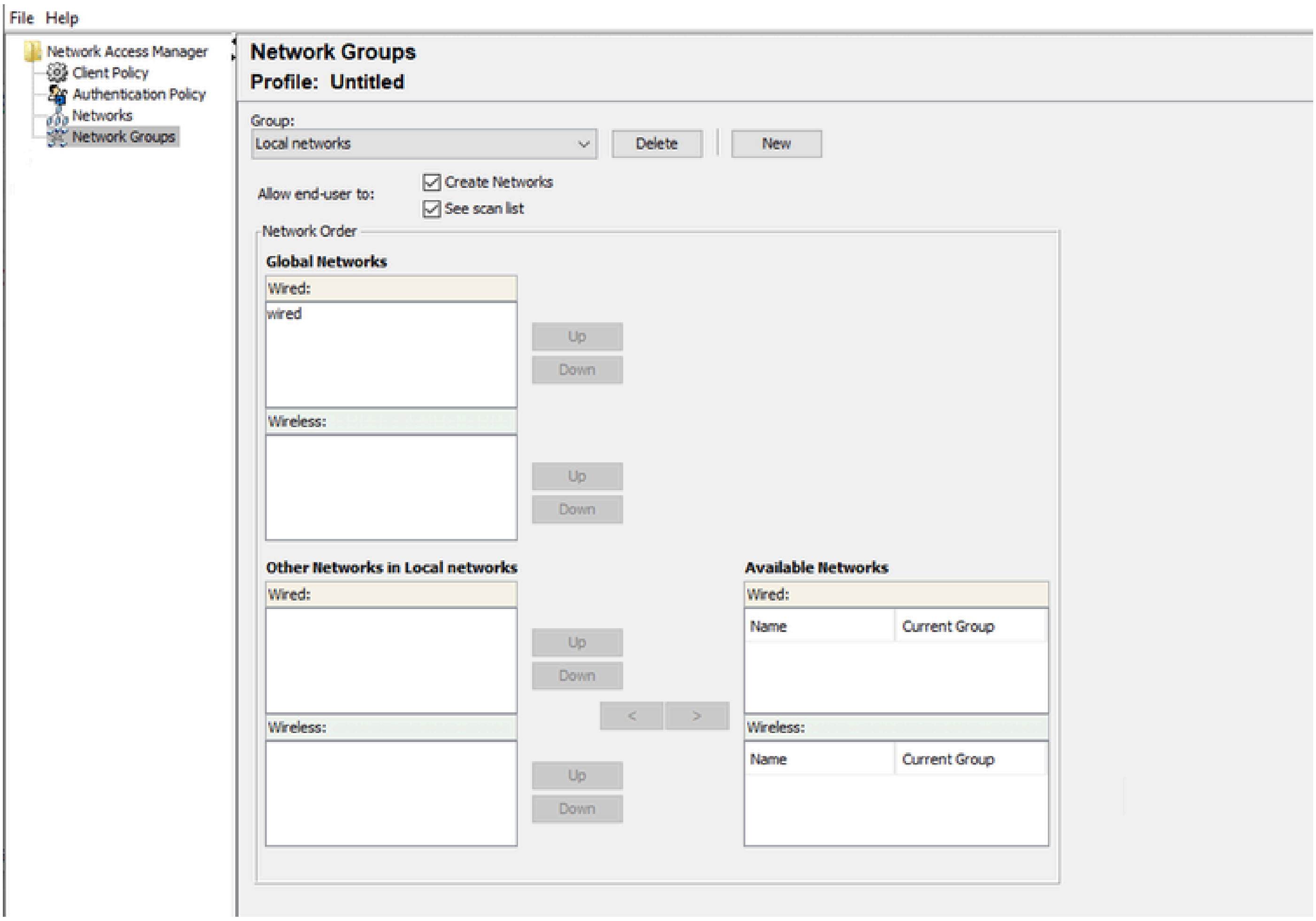
Allowed Authentication Modes

- ☑ 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

NAM Profile Editor Authentication Policy



Group: Local networks

Allow end-user to: ☑ Create Networks ☑ See scan list

Global Networks – Wired: wired

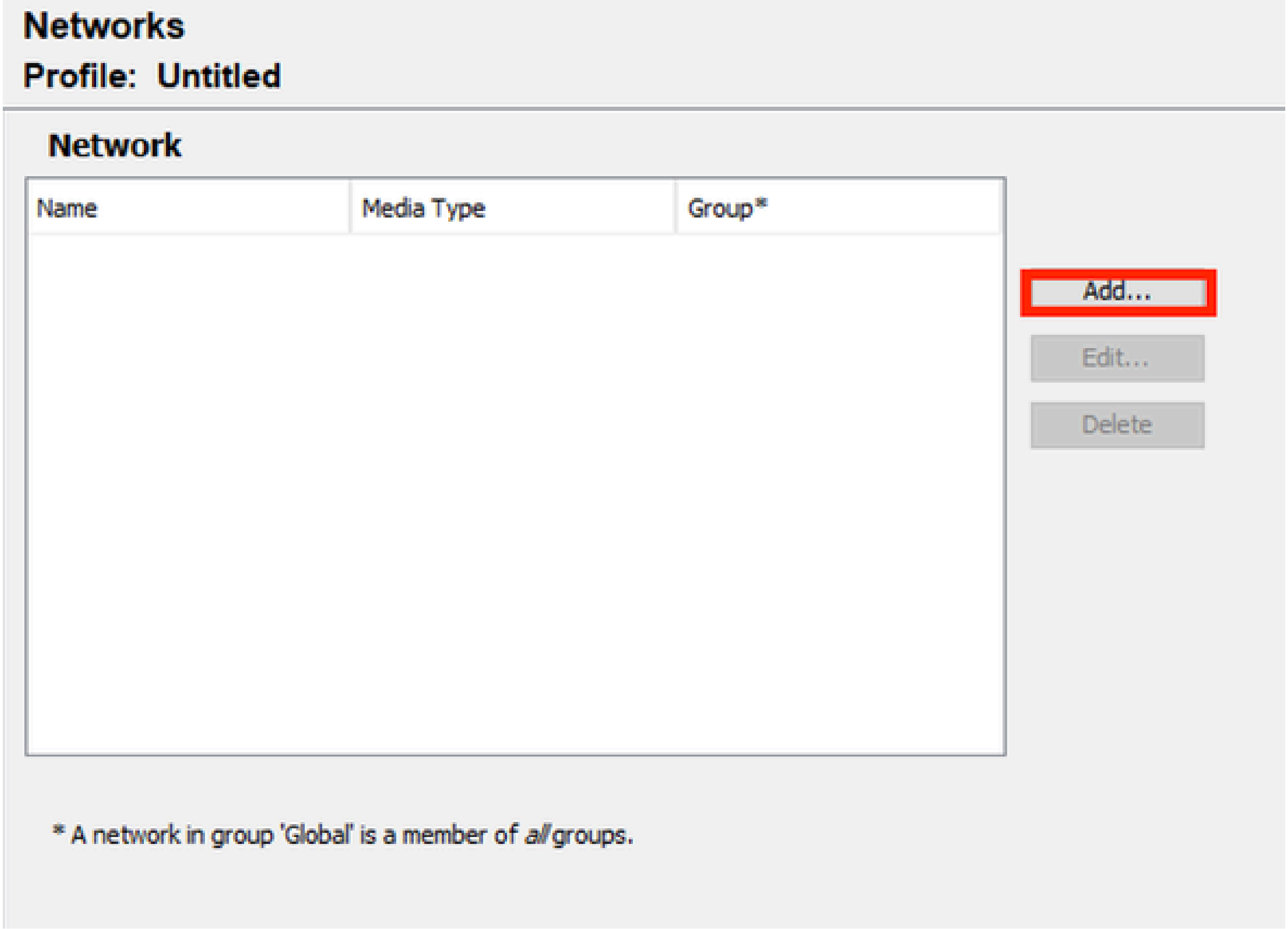
Network Groups Tab

4. Scenario 1: Configure Secure Client NAM Supplicant for PEAP (MS-CHAPv2) User Authentication

Navigate to the **Networks** section.

The default **Network** profile can be deleted.

Click **Add**.



Networks
Profile: Untitled

Network

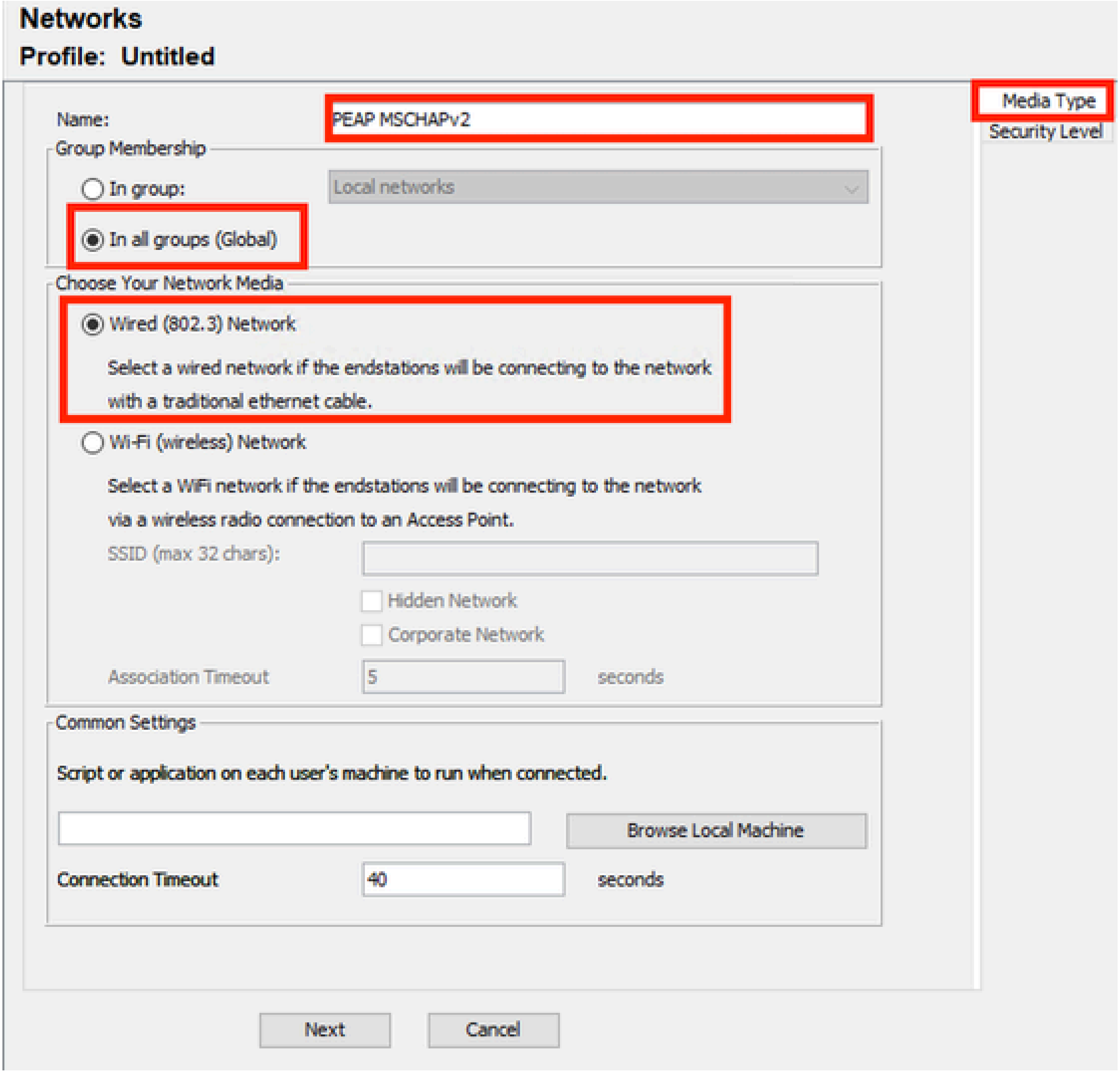
Name	Media Type	Group*

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

Network Profile Creation

Name the **Network** profile.

Select **Global** for **Group Membership**. Select **Wired Network** media.


Networks

Profile: Untitled

Name: PEAP MSCHAPv2

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 5 seconds

Common Settings

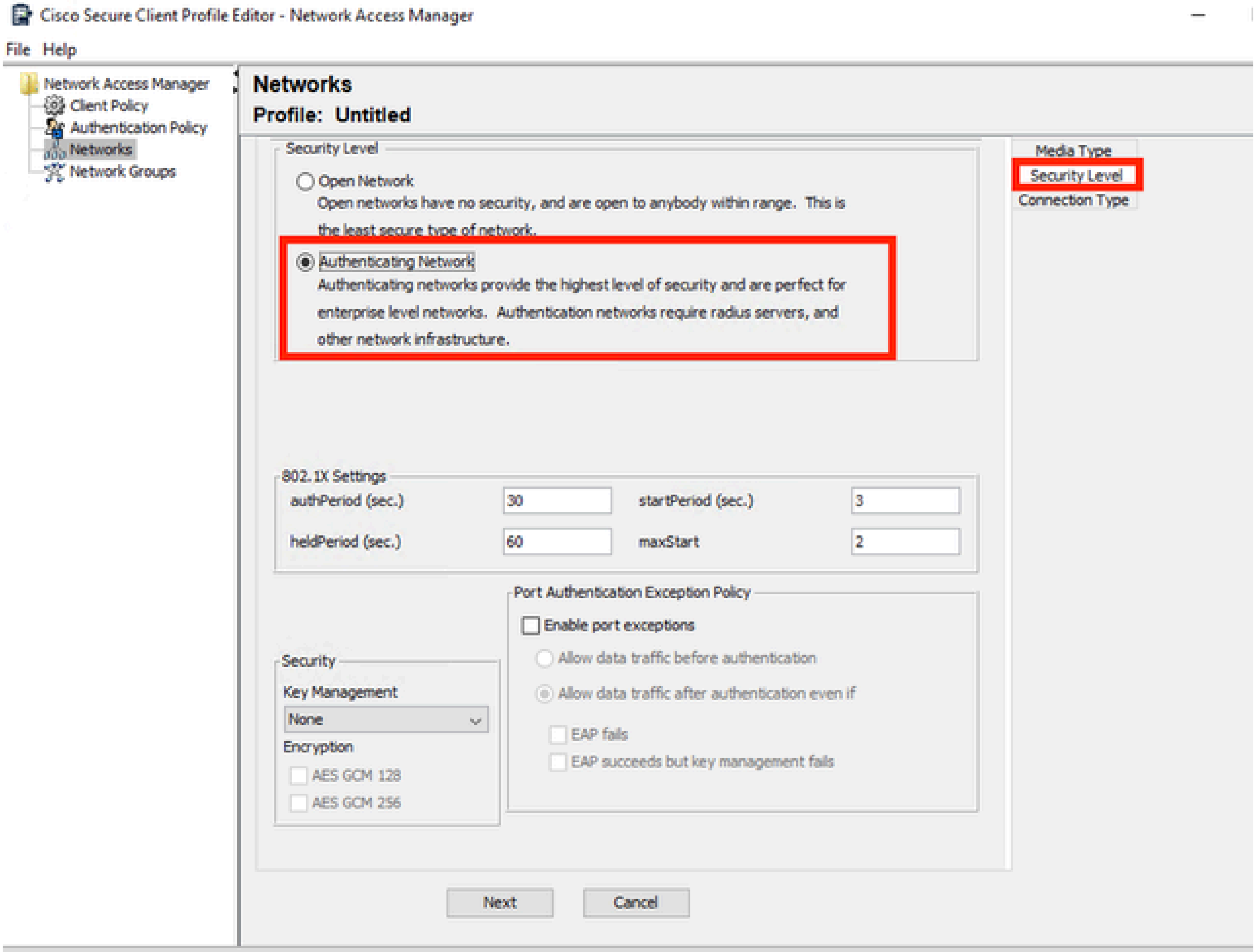
Script or application on each user's machine to run when connected.

Connection Timeout 40 seconds

Network Profile Media Type Section

Click **Next**.

Select **Authenticating Network** and use the default for the rest of the options in the **Security Level** section.



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

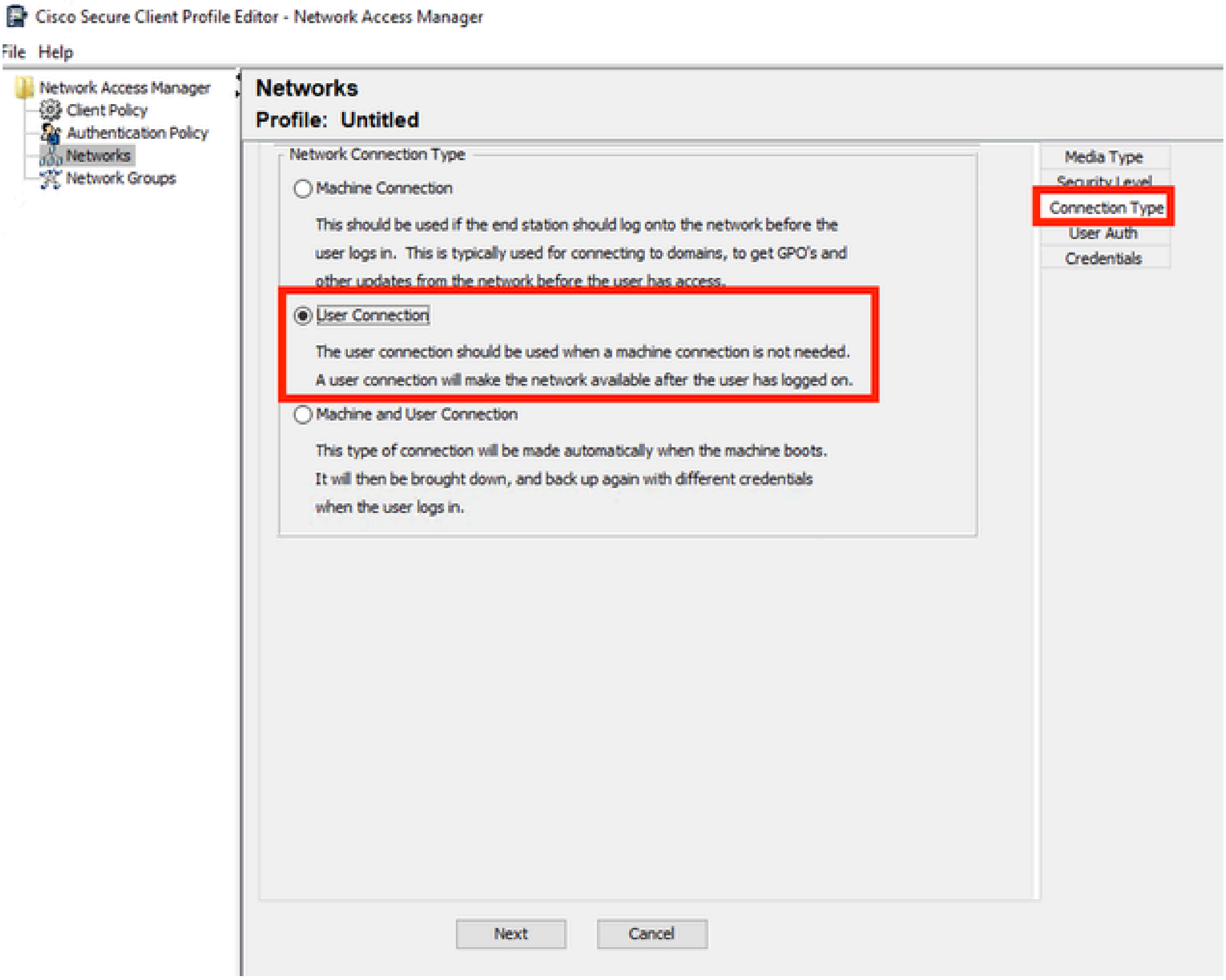
authPeriod (sec.)	30	startPeriod (sec.)	3
heldPeriod (sec.)	60	maxStart	2

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

Network Profile Security Level

Click **Next** to continue with the **Connection Type** section.



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

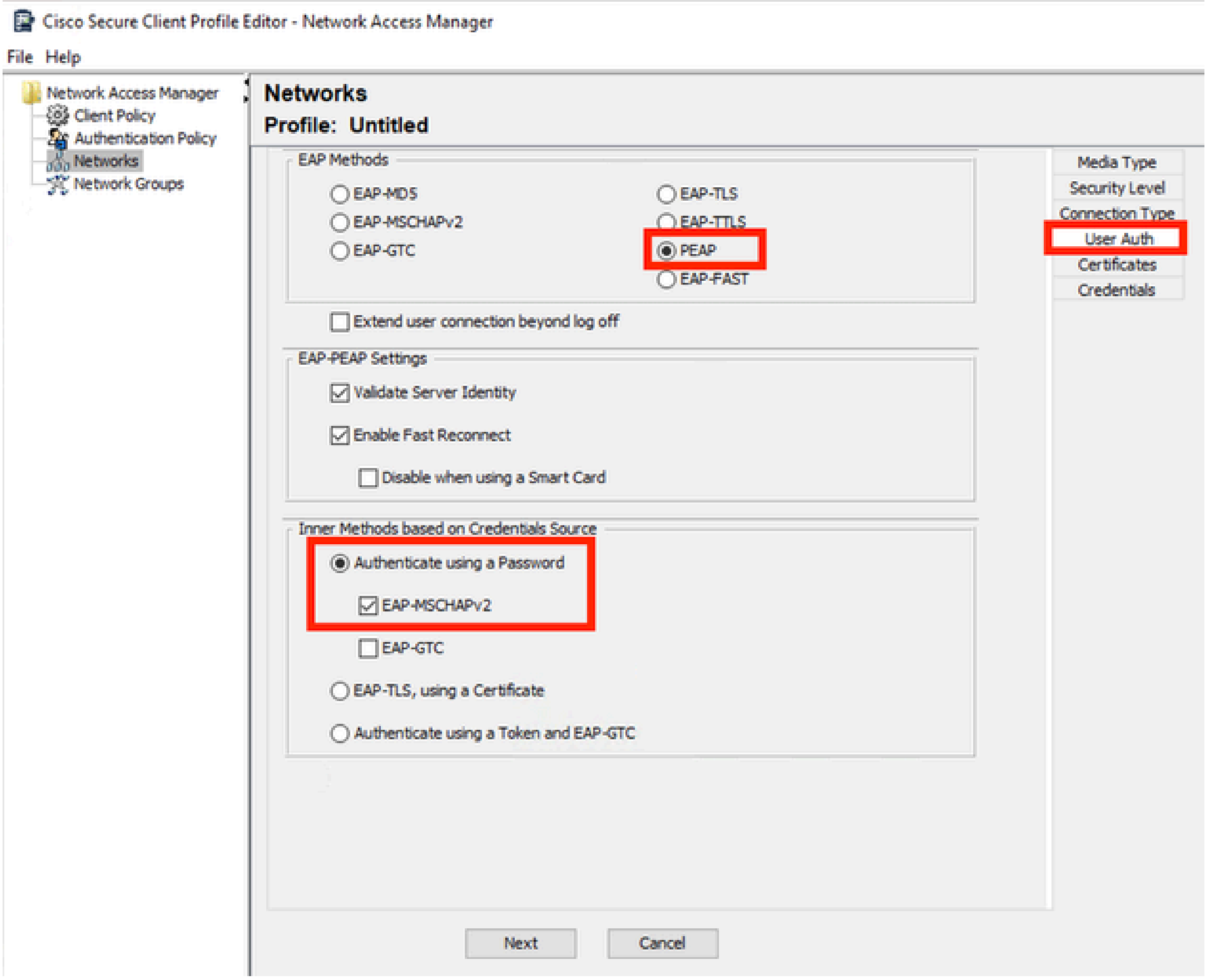
This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.

Netowork Profile Connection Type

Select the **User Connection** connection type.

Click **Next** to continue with the **User Auth** section which is now available.

Select **PEAP** as the general **EAP Method**.



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-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

Netowork Profile User Auth

Do not change the default values in the **EAP-PEAP Settings**.

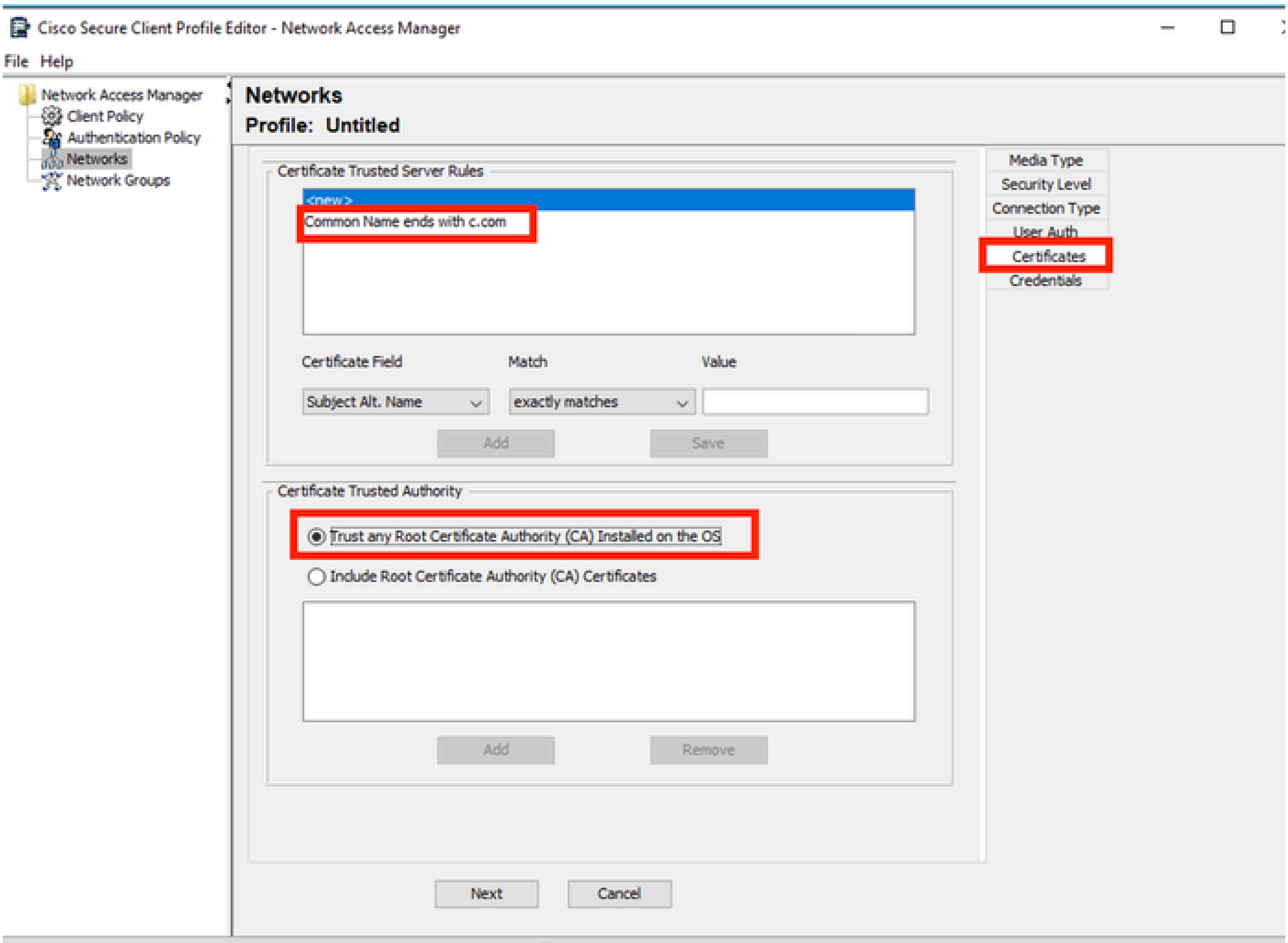
Continue with the **Inner Methods based on Credentials Source** section.

From the multiple inner methods that exist for EAP PEAP, select **Authenticate using a Password** and select **EAP-MSCHAPv2**.

Click **Next** to continue to the **Certificate** section.

Note: The **Certificate** section is displayed because the option **Validate Server Identity** in **EAP-PEAP Settings** is selected. For EAP PEAP, it does the encapsulation using the server certificate.

On the **Certificates** section, in **Certificate Trusted Server Rules** the rule **Common Name end with c.com** is used. This section of the configuration refers to the certificate that the server uses during the EAP PEAP flow. If Identity Service Engine (ISE) is used on your environment, you can use the common name of the **Policy Server Node EAP Certificate**.



Networks
Profile: Untitled

Certificate Trusted Server Rules

<new>
Common Name ends with c.com

Certificate Field: Subject Alt. Name
Match: exactly matches
Value:

Certificate Trusted Authority

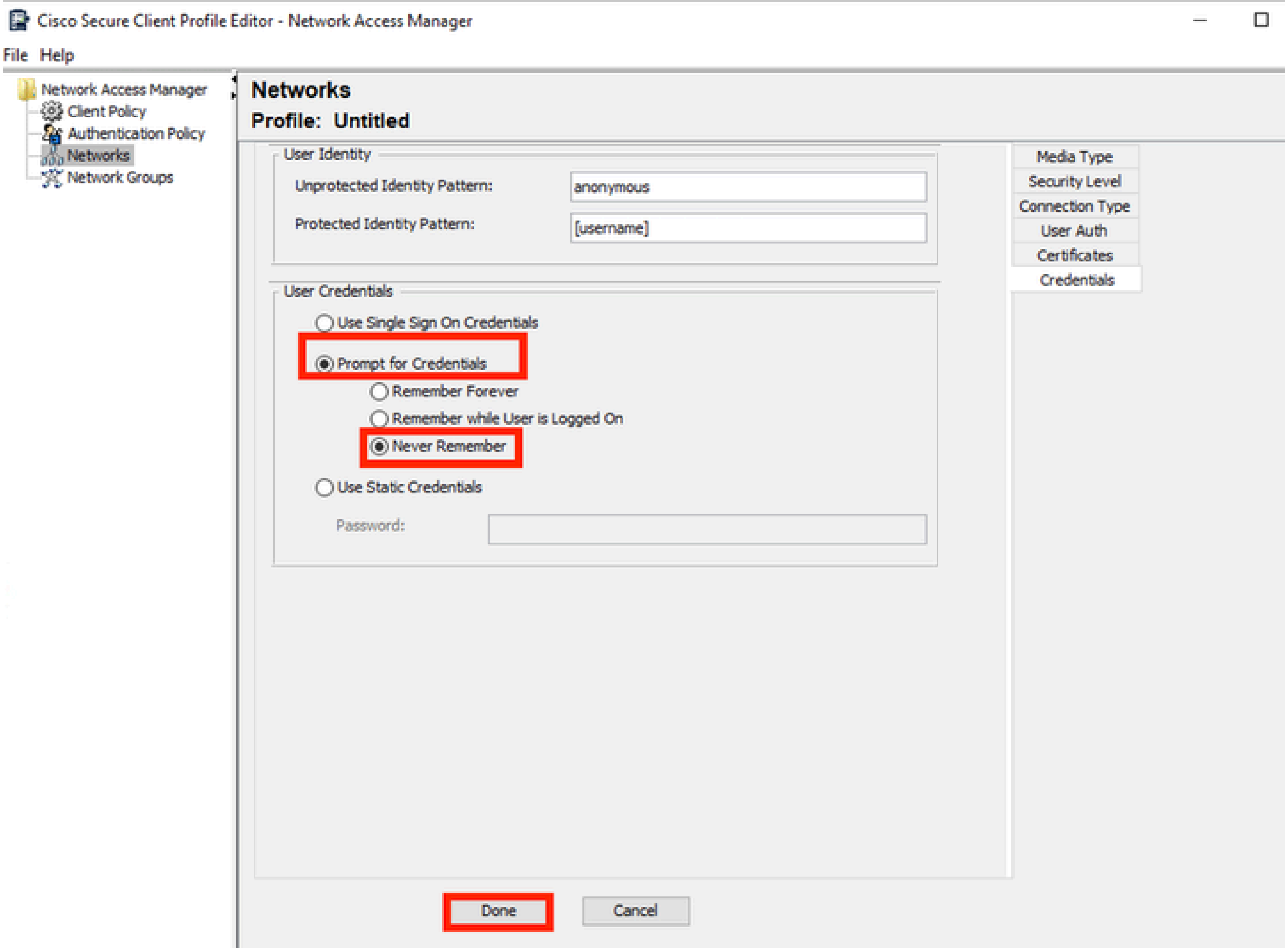
● Trust any Root Certificate Authority (CA) Installed on the OS
○ Include Root Certificate Authority (CA) Certificates

Network Profile Certificate Section

Two options can be selected in **Certificate Trusted Authority**. For this scenario instead of adding a specific CA Certificate that signed the RADIUS EAP cert, the option **Trust any Root Certificate Authority (CA) Installed on the OS** is used.

With this option the Windows device trusts any EAP cert that is signed by a cert included in Manage User Certs program Certificates — **Current User > Trusted Root Certification Authorities > Certificates**.

Click **Next**.



Networks
Profile: Untitled

User Identity

Unprotected Identity Pattern: anonymous

Protected Identity Pattern: [username]

User Credentials

○ Use Single Sign On Credentials

● Prompt for Credentials

○ Remember Forever

○ Remember while User is Logged On

● Never Remember

○ Use Static Credentials

Password:

Network Profile Credentials Section

In the **Credentials** section only the **User Credentials** section is changed.

The option **Prompt for Credentials** > **Never Remember** is selected, so in each authentication, the user making the authentication must enter their credentials.

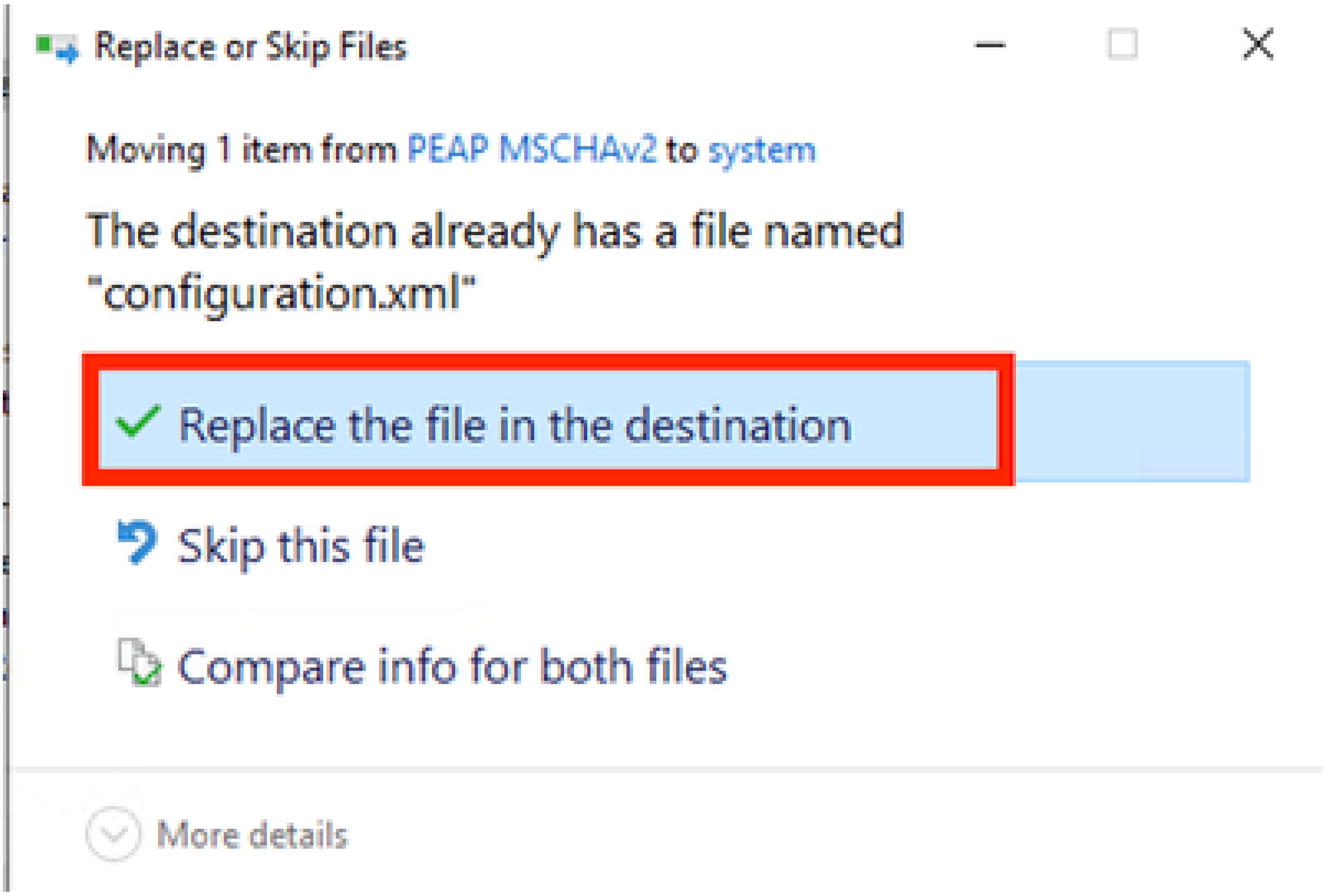
Click **Done**.

Save the Secure Client Network Access Manager profile, as **configuration.xml** with the **File** > **Save As** option.

To make Secure Client Network Access Manage use the profile that was just created, replace the configuration.xml file in the next directory with the new one:

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

Note: The file must be named configuration.xml, otherwise it does not work.



Replace or Skip Files

Moving 1 item from PEAP MSCHAv2 to system

The destination already has a file named "configuration.xml"

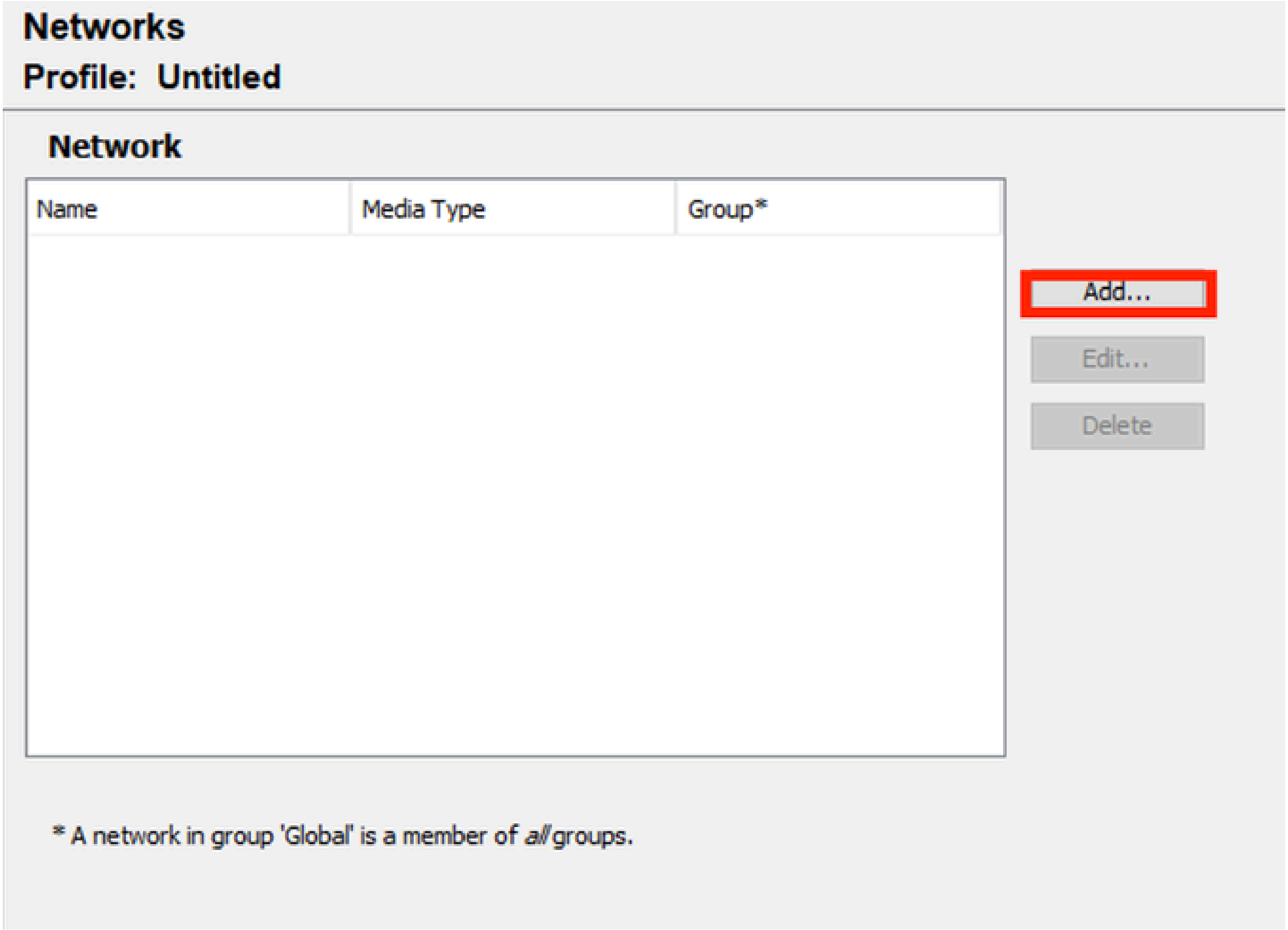
✓ Replace the file in the destination
Skip this file
Compare info for both files
More details

Replace File Section

5. Scenario 2: Configure Secure Client NAM Supplicant for EAP-FAST Simultaneous User and Machine Authentication

Open NAM Profile Editor and navigate to the **Networks** section.

Click **Add**.



Networks
Profile: Untitled

Network

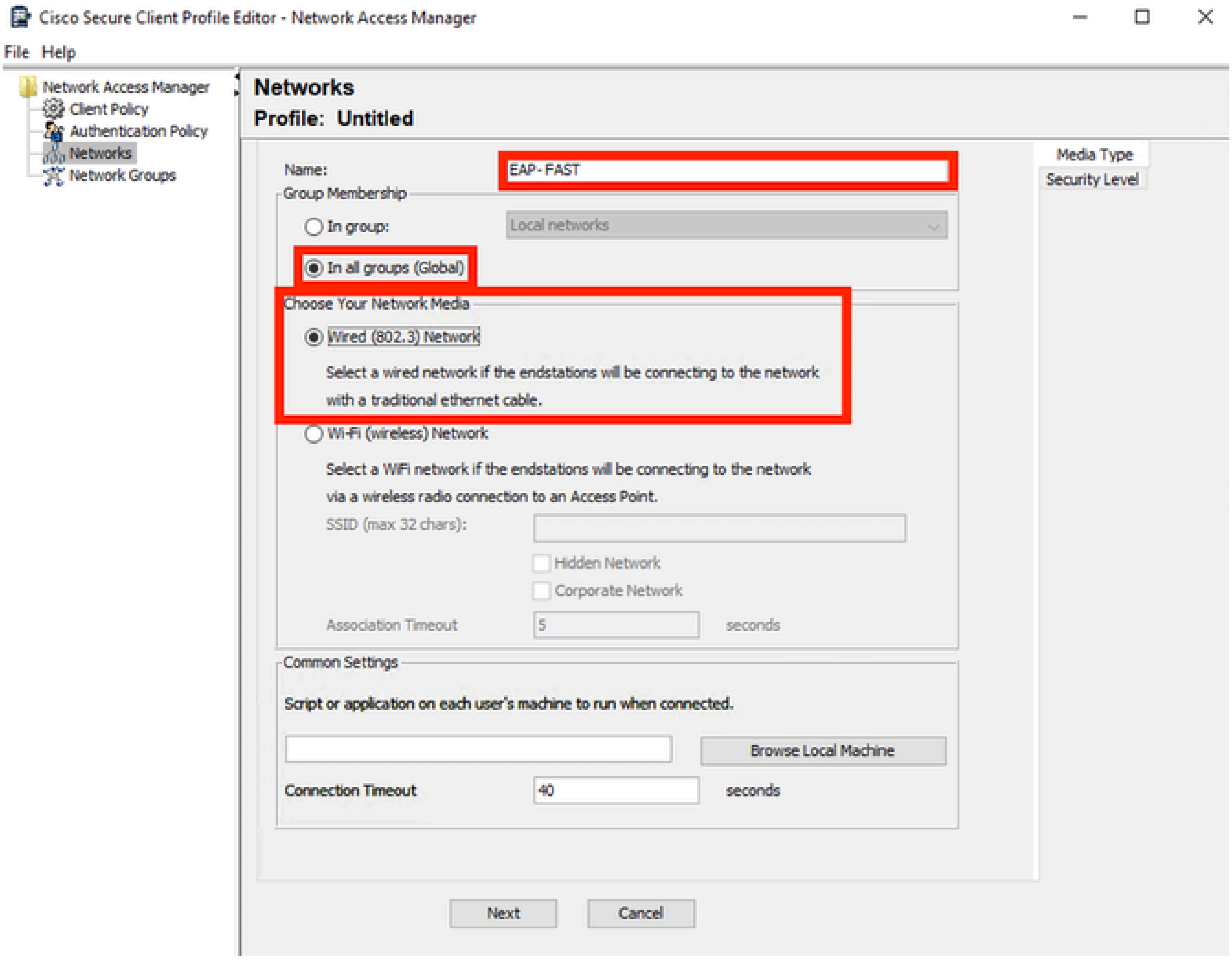
Name	Media Type	Group*

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

NAM Profile Editor Network Tab

Enter a name in the network profile.

Select **Global** for **Group Membership**. Select **WiredNetwork** Media.



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 5 seconds

Common Settings

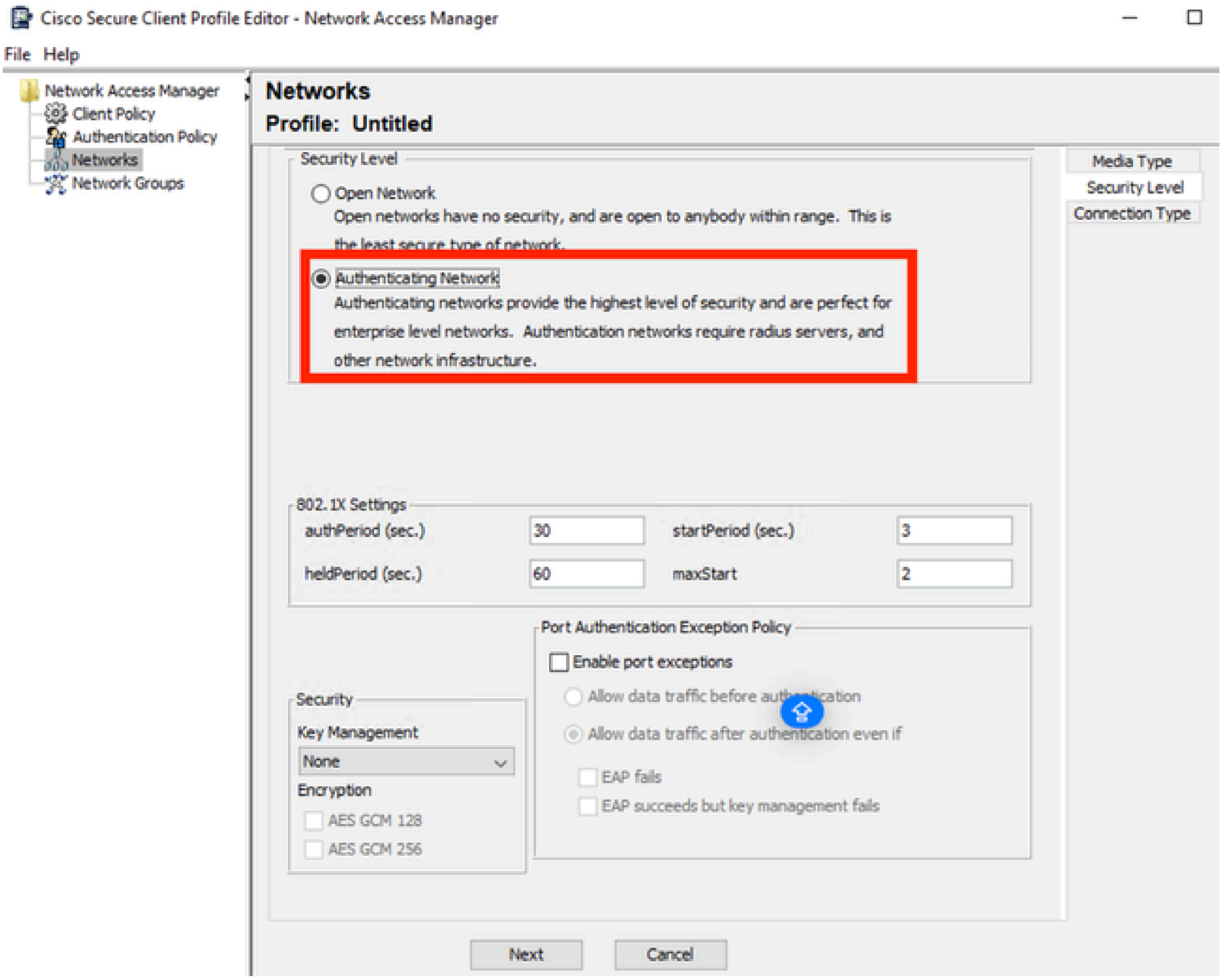
Script or application on each user's machine to run when connected.

Connection Timeout 40 seconds

Media Type Section

Click **Next**.

Select **Authenticating Network** and do not change the default values for the rest of the options in this section.



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.)	30	startPeriod (sec.)	3
heldPeriod (sec.)	60	maxStart	2

Security

Key Management: None

Encryption

□ AES GCM 128

□ AES GCM 256

Port Authentication Exception Policy

□ Enable port exceptions

○ Allow data traffic before authentication

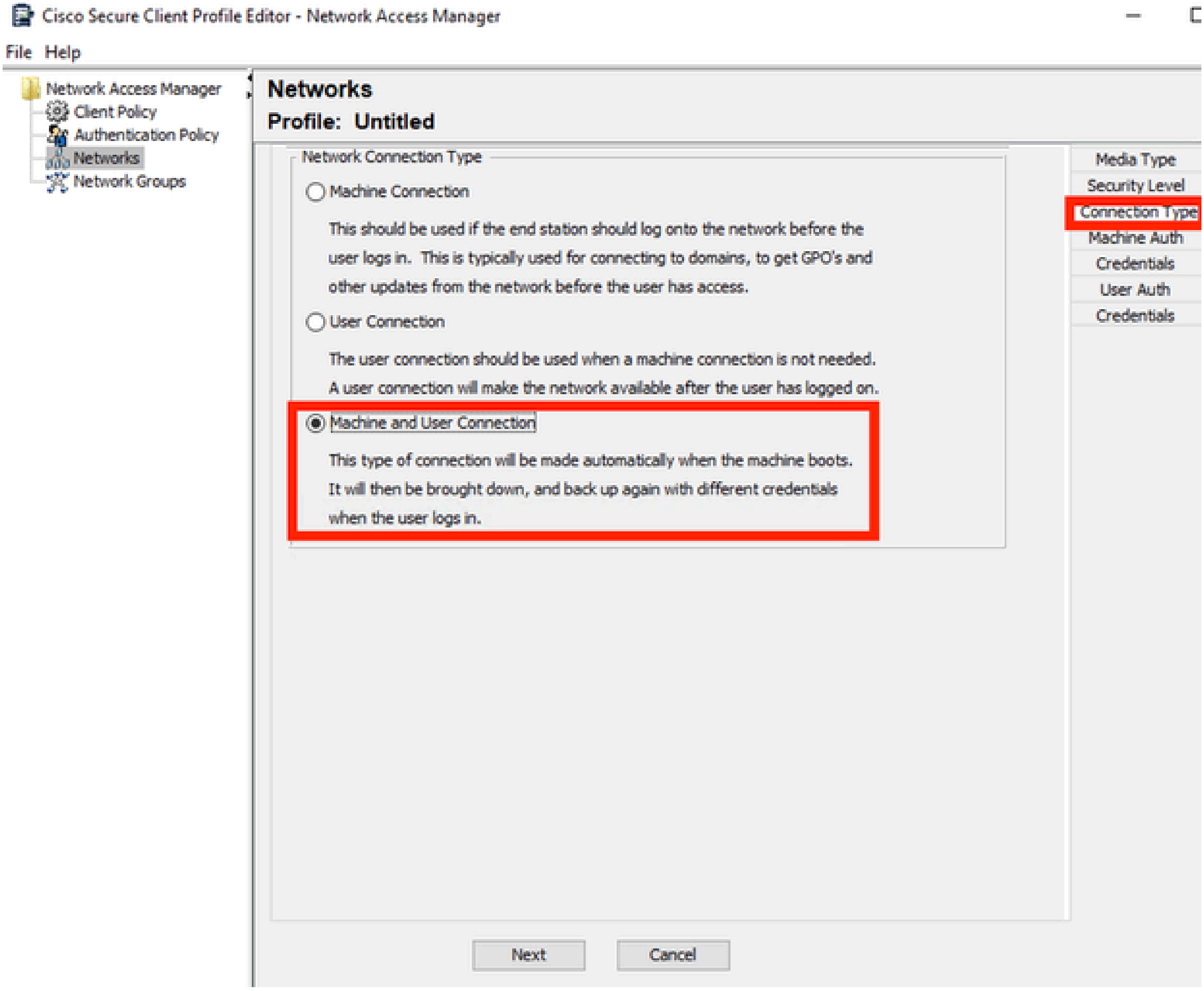
● Allow data traffic after authentication even if

□ EAP fails

□ EAP succeeds but key management fails

Security Level Profile Editor Section

Click **Next** to continue with the **Connection Type** section.



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.

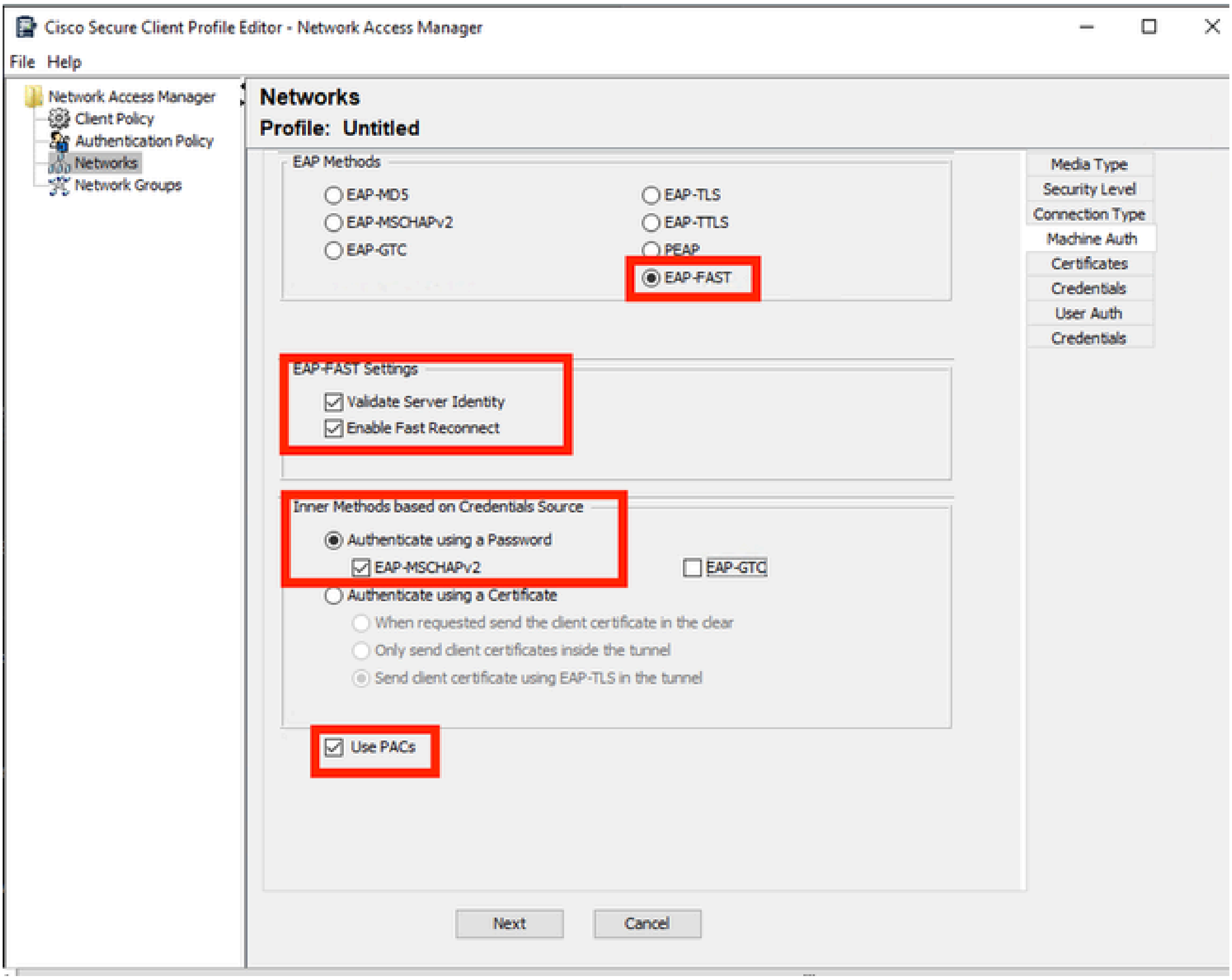
● Machine and User Connection

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.

Connection Type Section

Configure user and machine authentication simultaneously by selecting the third option.

Click **Next**.



Cisco Secure Client Profile Editor - Network Access Manager

File Help

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

Networks

Profile: Untitled

EAP Methods

○ EAP-MD5 ○ EAP-TLS

○ EAP-MSCHAPv2 ○ EAP-TTLS

○ EAP-GTC ○ PEAP

● EAP-FAST

EAP-FAST Settings

☑ Validate Server Identity

☑ Enable Fast Reconnect

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

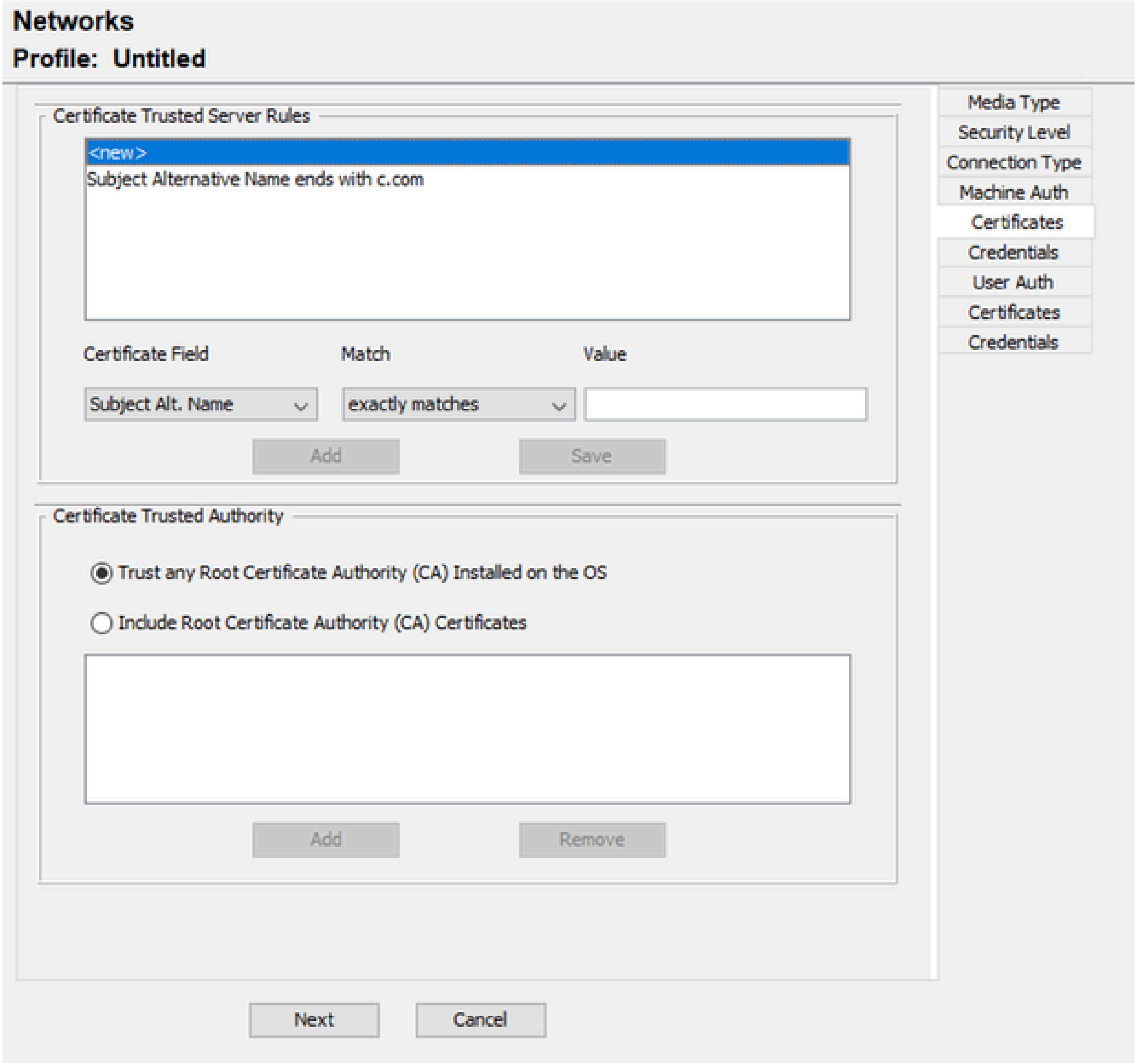
☑ Use PACs

Machine Auth Section

In the **Machine Auth** section select **EAP-FAST** as the EAP method. Do not change the **EAP FAST Settings** default values. For the **Inner methods based on Credentials Source** section select **Authenticate using a Password** and **EAP-MSCHAPv2** as the method. Then select **Use PACs** option.

Click **Next**.

On the **Certificates** section, in **Certificate Trusted Server Rules** the rule common name ends with c.com. This section refers to the certificate that the server uses during the EAP PEAP flow. If Identity Service Engine (ISE) is used on your environment the common name of the Policy Server Node EAP Certificate can be used.



Networks

Profile: Untitled

Certificate Trusted Server Rules

<new>

Subject Alternative Name ends with c.com

Certificate Field: Subject Alt. Name

Match: exactly matches

Value:

Certificate Trusted Authority

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

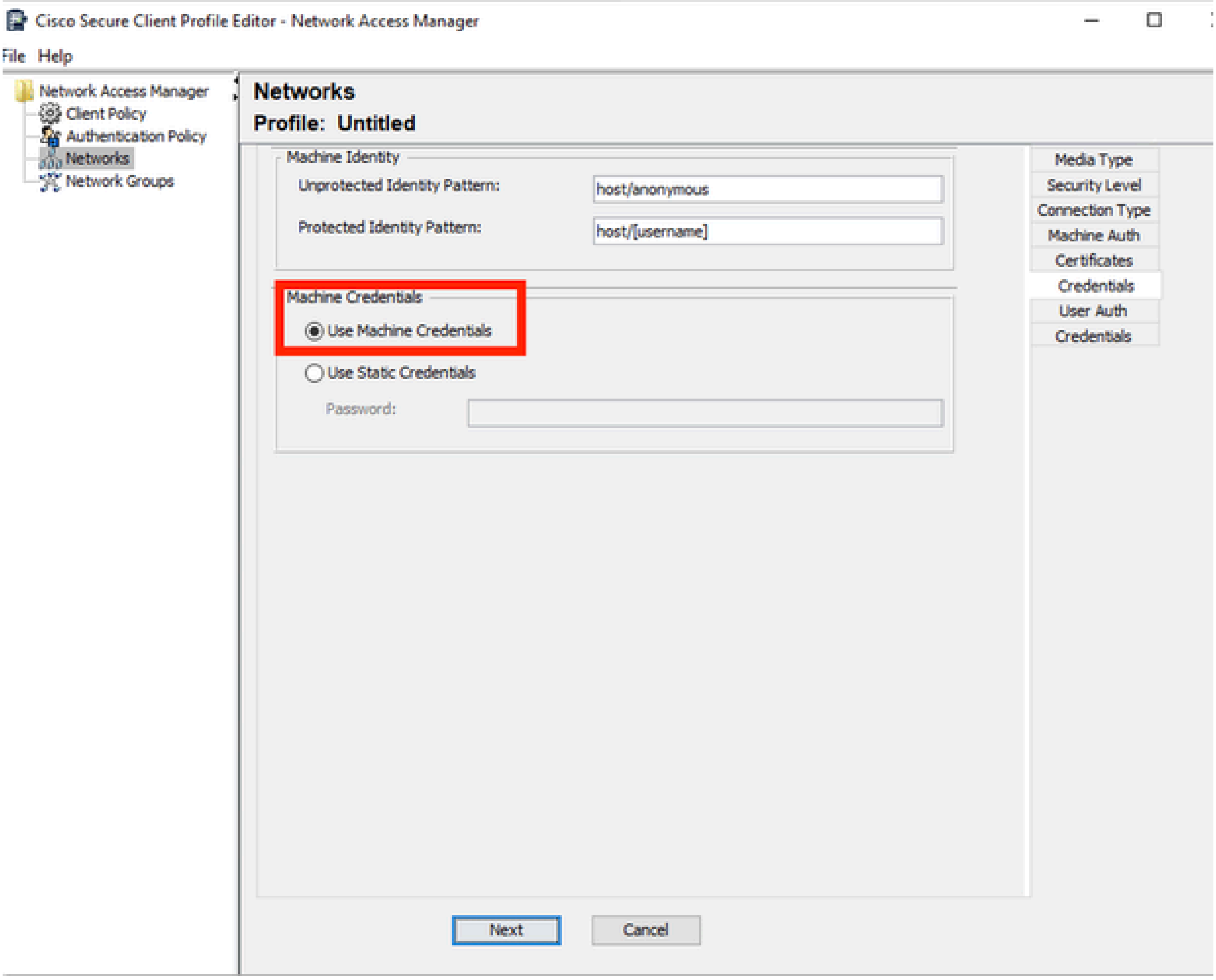
○ Include Root Certificate Authority (CA) Certificates

Machine Auth Server Certificate Trust section

Two options can be selected in **Certificate Trusted Authority**. For this scenario instead of adding a specific CA Certificate that signed the RADIUS EAP cert, use the option **Trust any Root Certificate Authority (CA) Installed on the OS**.

With this option, Windows trusts any EAP cert that is signed by a cert included in the Manage User Certs program (**Current User > Trusted Root Certification Authorities > Certificates**).

Click **Next**.



Cisco Secure Client Profile Editor - Network Access Manager

Networks

Profile: Untitled

Machine Identity

Unprotected Identity Pattern: host/anonymous

Protected Identity Pattern: host/[username]

Machine Credentials

● Use Machine Credentials

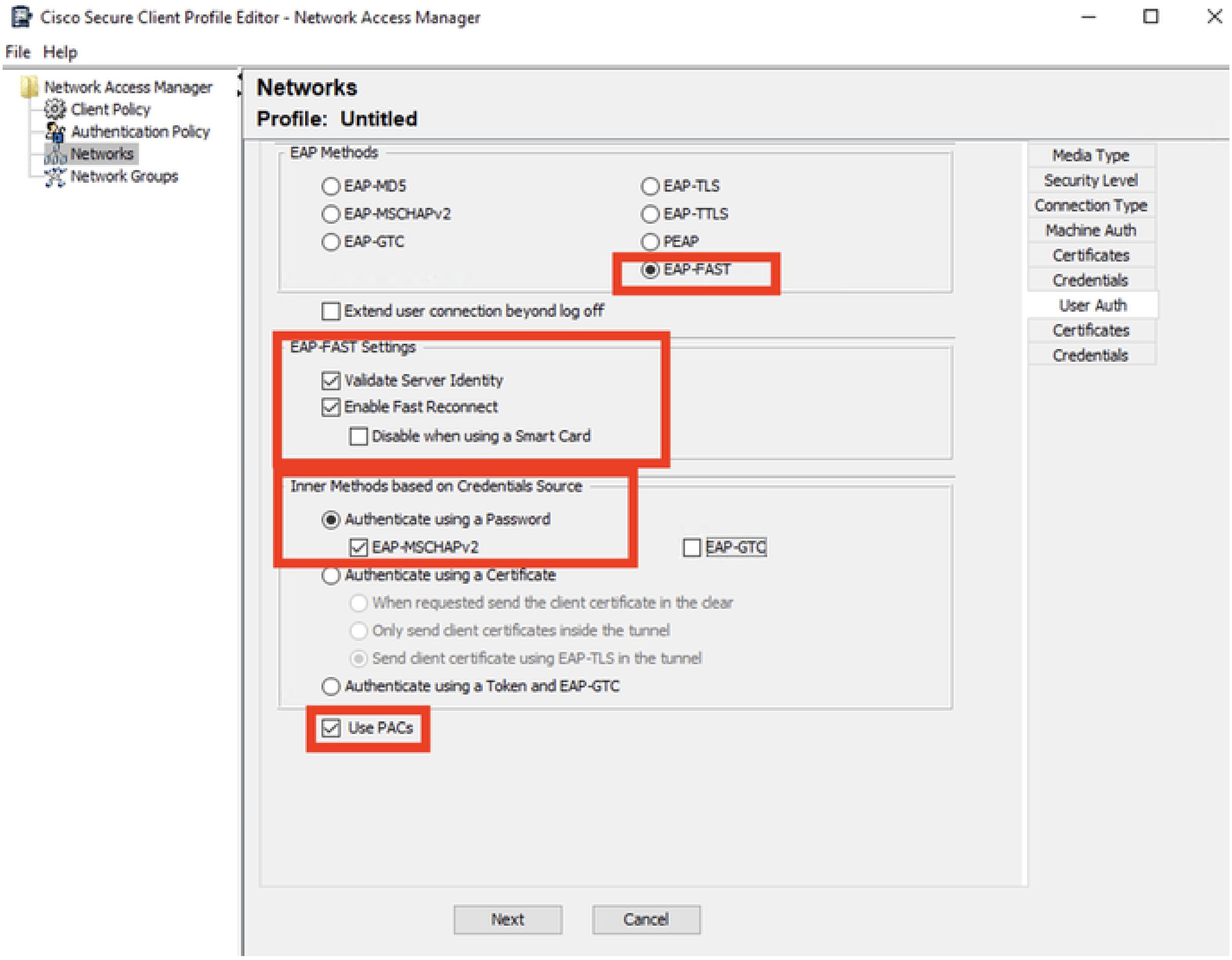
○ Use Static Credentials

Password:

Mahine Auth Credentials Section

Select **Use Machine Credentials** in the **Machine Credentials** section.

Click **Next**.



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-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

User Authentication Section

For **User Auth**, select **EAP-FAST** as the **EAP Method**.

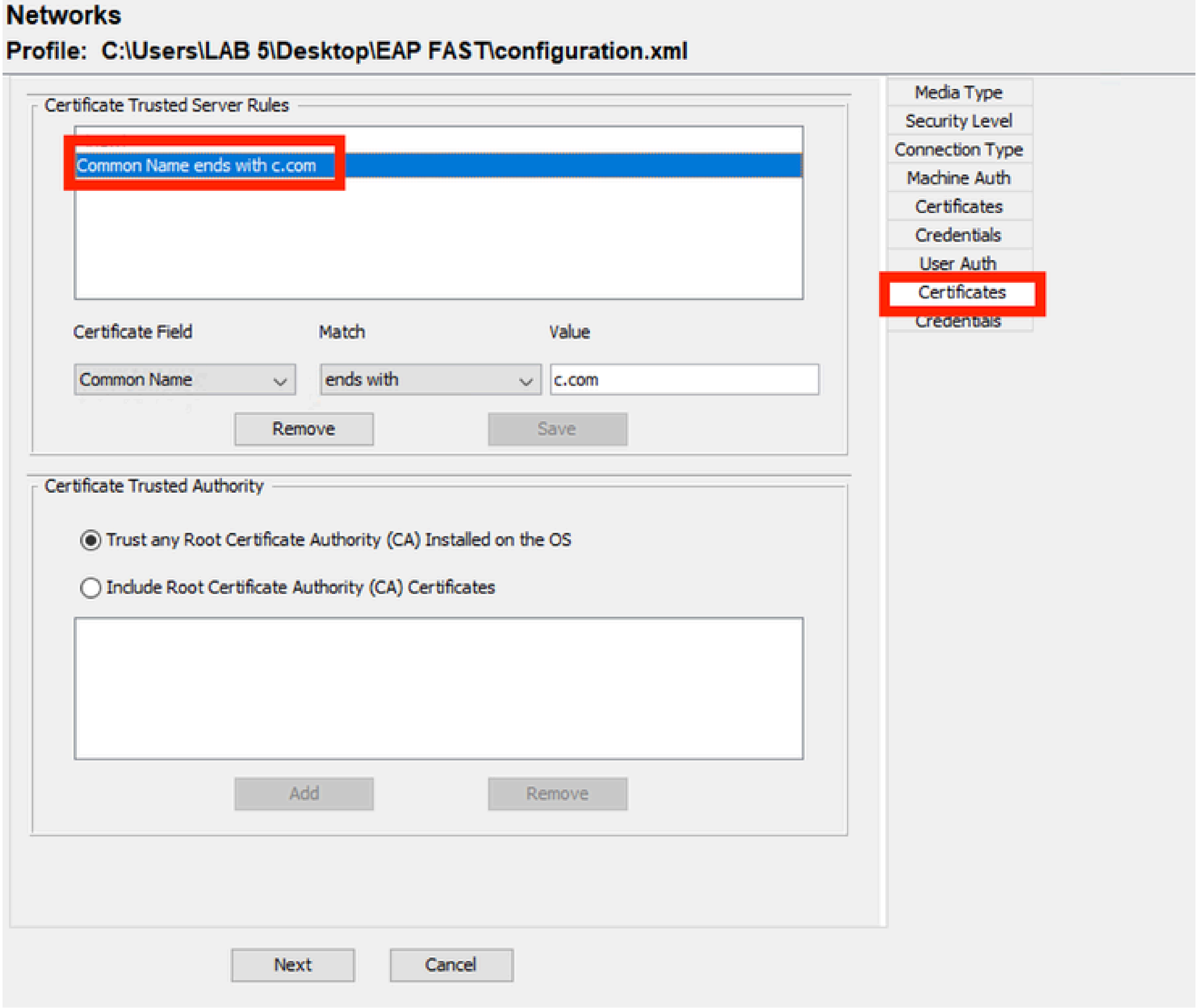
Do not change the default values in the **EAP-FAST** settings section.

For the Inner Method based on credentials source section, select **Authenticate using a Password** and **EAP-MSCHAPv2** as the method.

Select **Use PACs**.

Click **Next**.

In the **Certificates** section, in **Certificate Trusted Server Rules**, the rule is **Common Name ends with c.com**. These configurations are for the certificate that the server uses during the EAP PEAP flow. If ISE is used on your environment the common name of the Policy Server Node EAP Certificate can be used.



Certificate Trusted Server Rules

Common Name ends with c.com

Certificate Field: Common Name

Match: ends with

Value: c.com

Certificate Trusted Authority

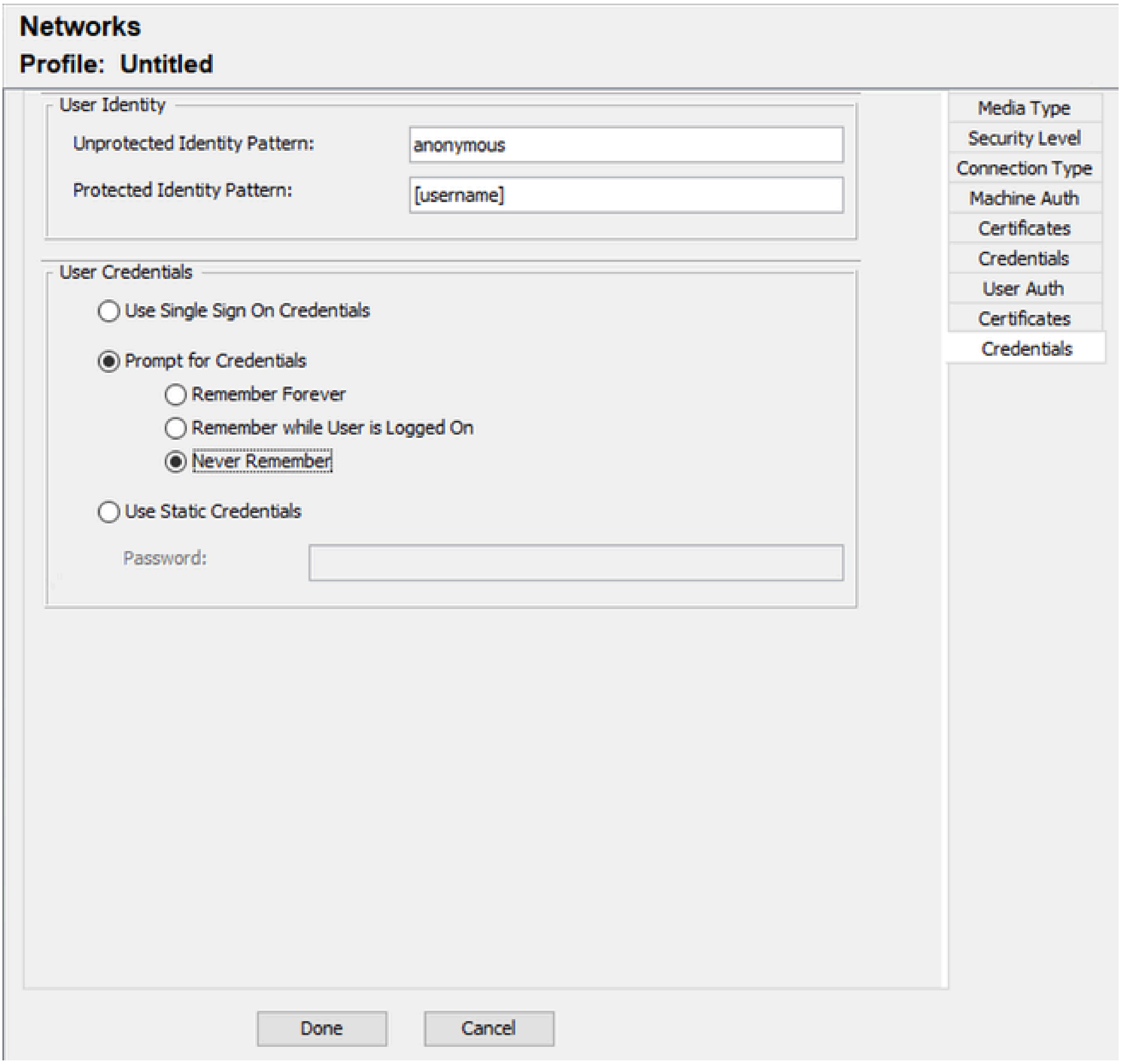
● Trust any Root Certificate Authority (CA) Installed on the OS

○ Include Root Certificate Authority (CA) Certificates

User Auth Server Certificate Trust Section

Two options can be selected in **Certificate Trusted Authority**. For this scenario instead of adding a specific CA Certificate that signed the RADIUS EAP cert, the option **Trust any Root Certificate Authority (CA) Installed on the OS** is used.

Click **Next**.



Networks

Profile: Untitled

User Identity

Unprotected Identity Pattern: anonymous

Protected Identity Pattern: [username]

User Credentials

○ Use Single Sign On Credentials

● Prompt for Credentials

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

○ Use Static Credentials

Password:

User Auth Credentials

In the Credentials section, only the **User Credentials** section is changed.

The option **Prompt for Credentials** > **Never Remember** is selected. So in each authentication, the user authenticating must enter their credentials.

Click the **Done** button.

Select **File** > **Save as** and save the **Secure Client Network Access Manager** profile as **configuration.xml**.

To make the **Secure Client Network Access Manager** use the profile that was just created, replace the configuration.xml file in the next directory with the new one:

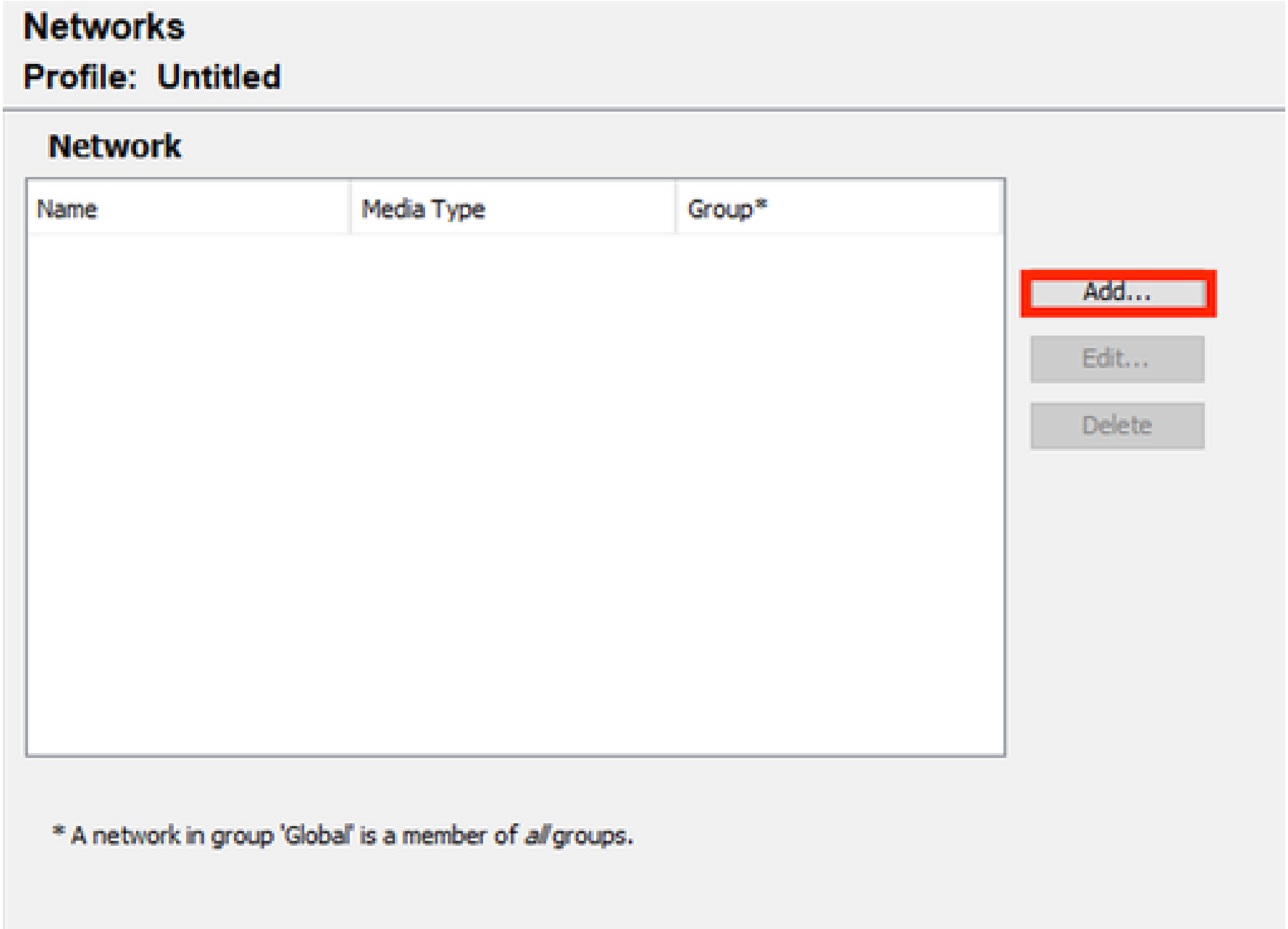
C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system

Note: The file must be named configuration.xml, otherwise it does not work.

6. Scenario 3: Configure Secure Client NAM Supplicant for EAP TLS User Certificate Authentication

Open **NAM Profile Editor** and navigate to the **Networks** section.

Click **Add**.



Networks
Profile: Untitled

Network

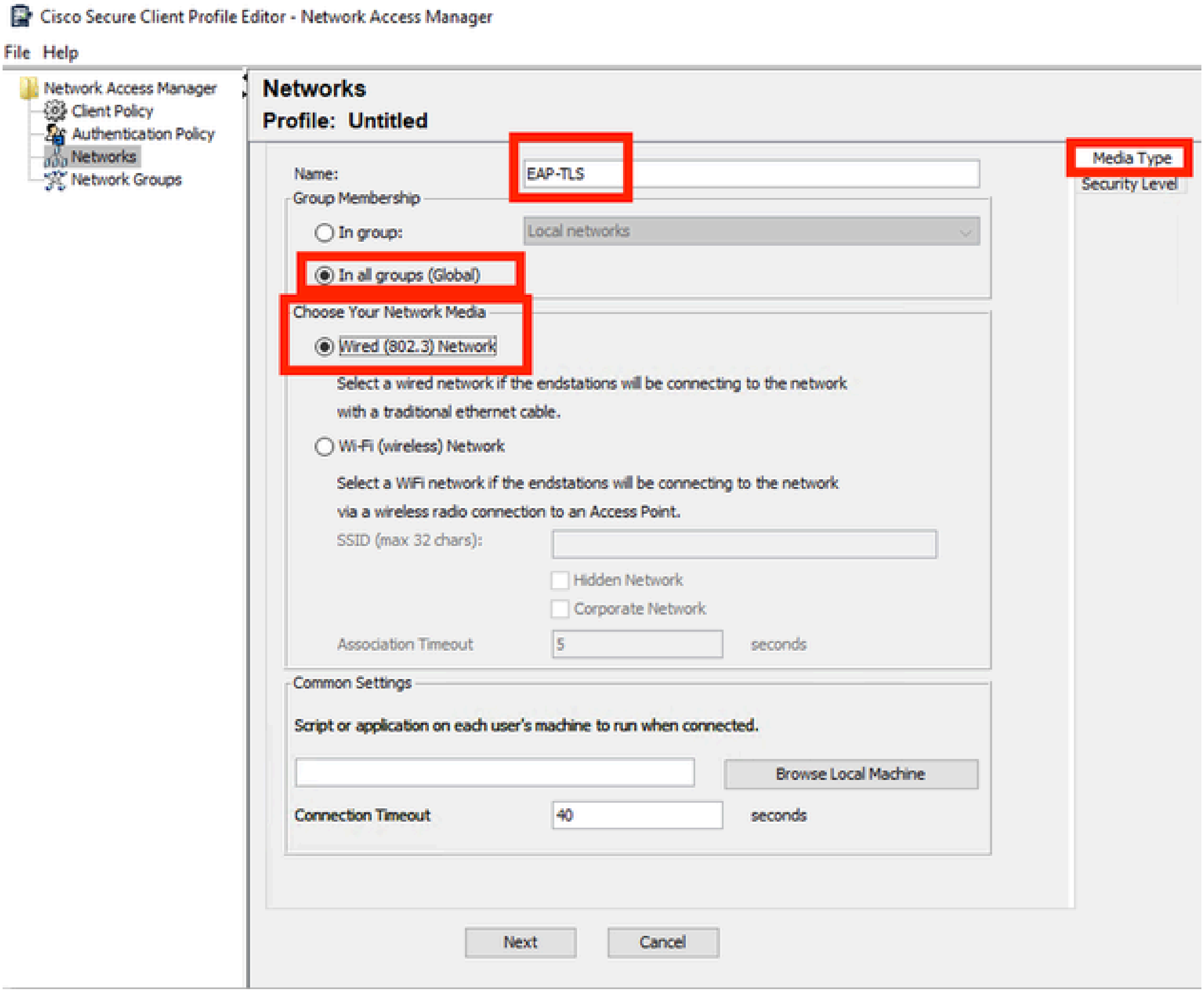
Name	Media Type	Group*

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

Network Creation Section

Name the network profile, in this case the named is with the EAP protocol used for this scenario.

Select **Global** for **Group Membership**. And **Wired Network** Media.



Networks
Profile: Untitled

Name: EAP-TLS

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 5 seconds

Common Settings

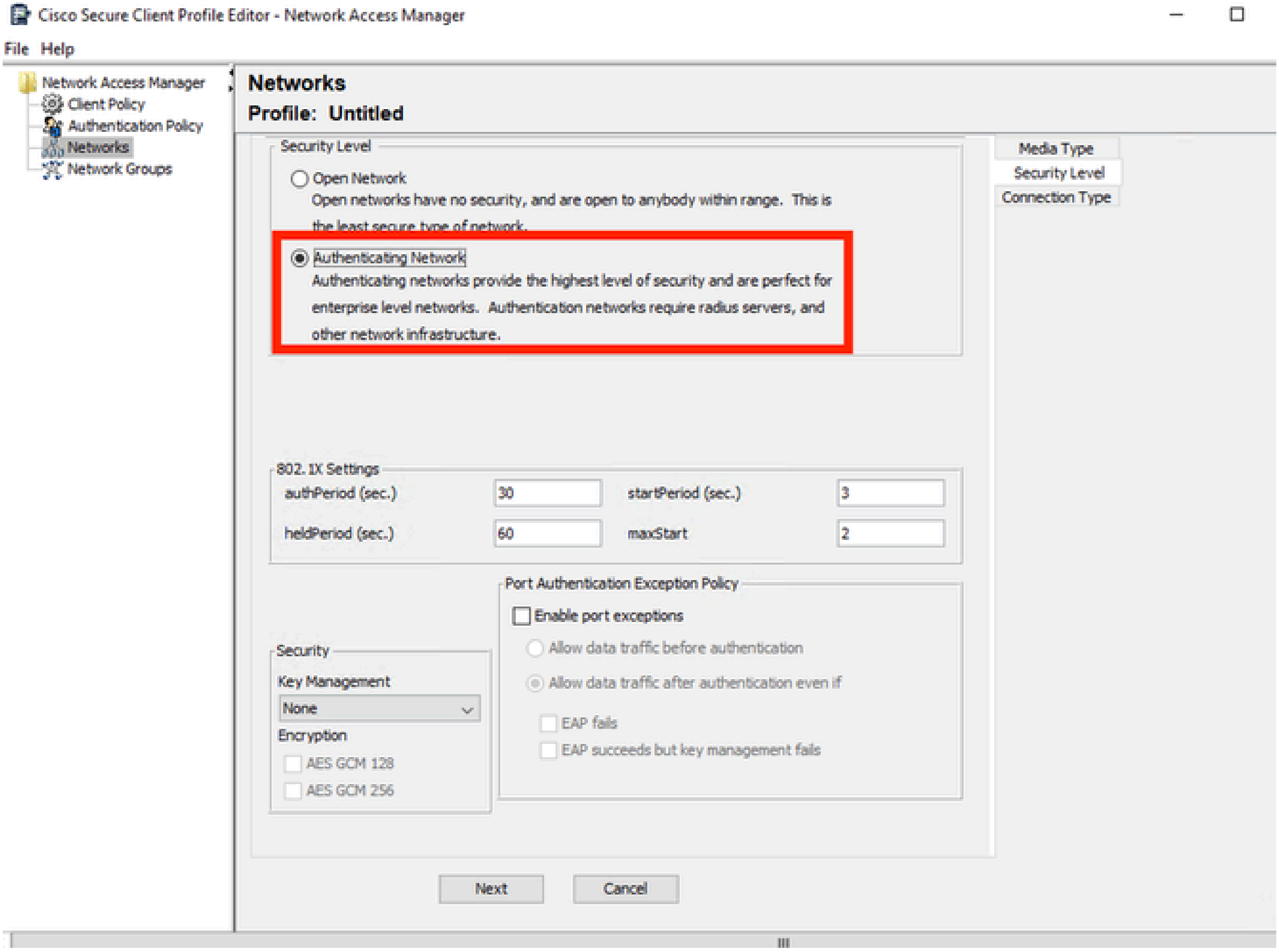
Script or application on each user's machine to run when connected.

Connection Timeout 40 seconds

Media Type Section

Click **Next**.

Select **Authenticating Network** and do not change the default values for the rest of the options in the **Security Level** section.



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.)	30	startPeriod (sec.)	3
heldPeriod (sec.)	60	maxStart	2

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

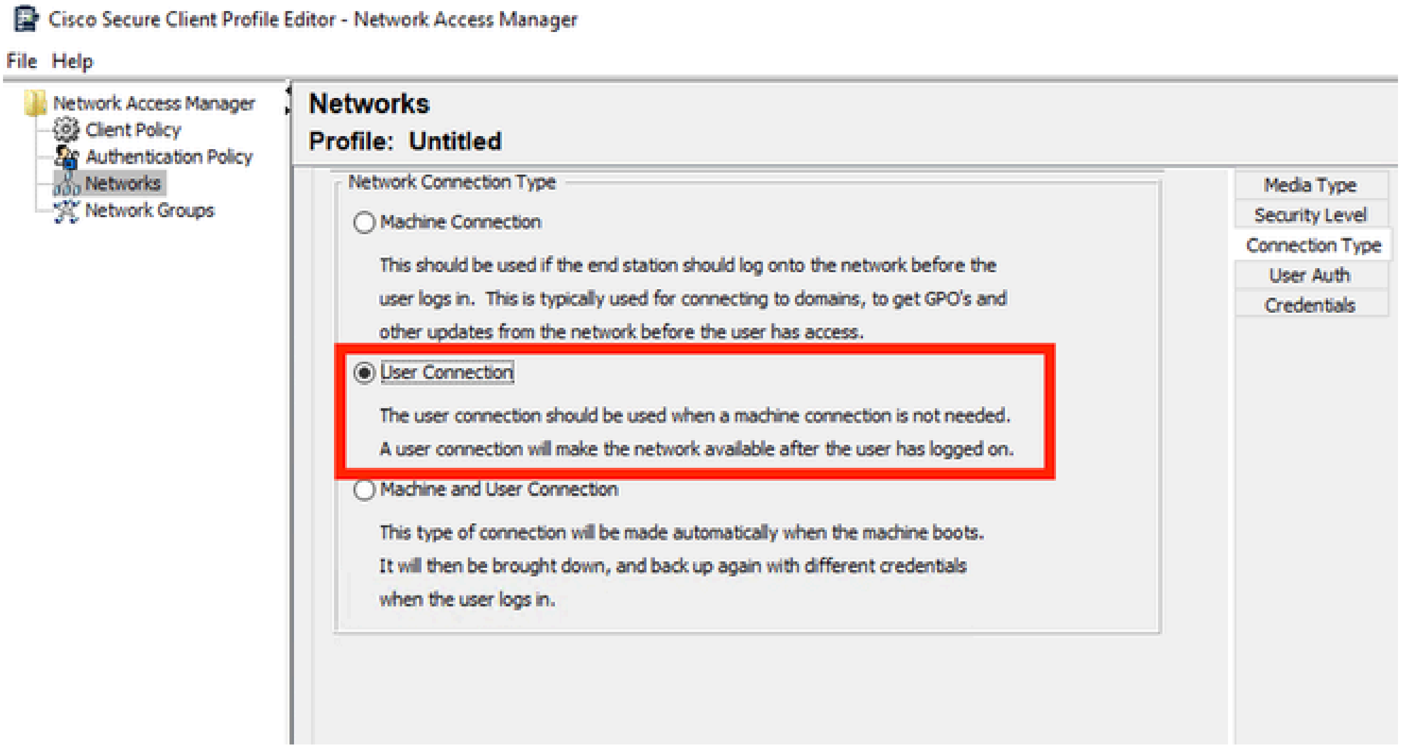
Security

Key Management: None

Encryption
□ AES GCM 128
□ AES GCM 256

Security Level

This scenario is for user authentication using a certificate. For that reason the option **User Connection** is used.



Networks

Profile: Untitled

Network Connection Type

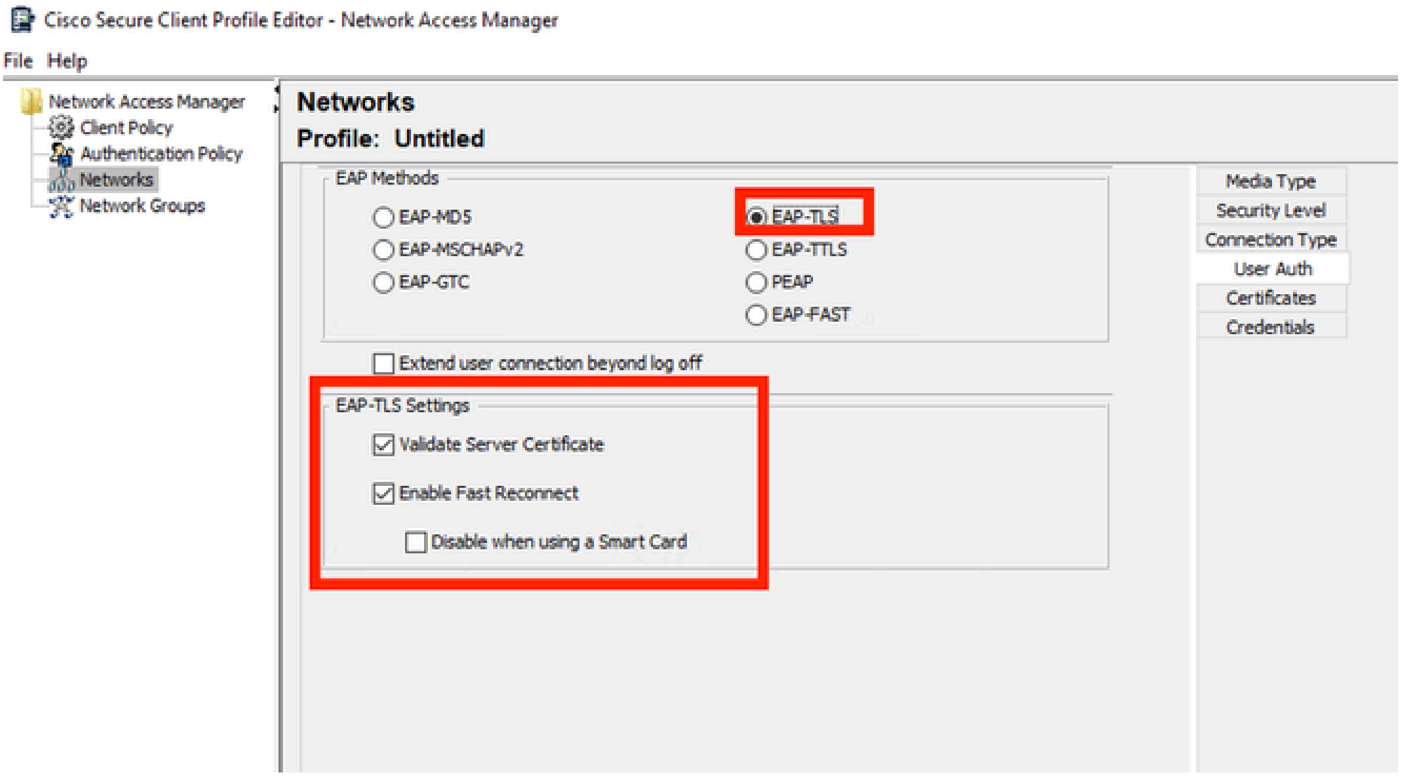
○ Machine Connection
This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.

● 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.

Conenction Type

Configure **EAP-TLS** as the EAP method. Do not change the default values in the **EAP-TLS settings** section.



EAP Methods

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

□ Extend user connection beyond log off

EAP-TLS Settings

☑ Validate Server Certificate

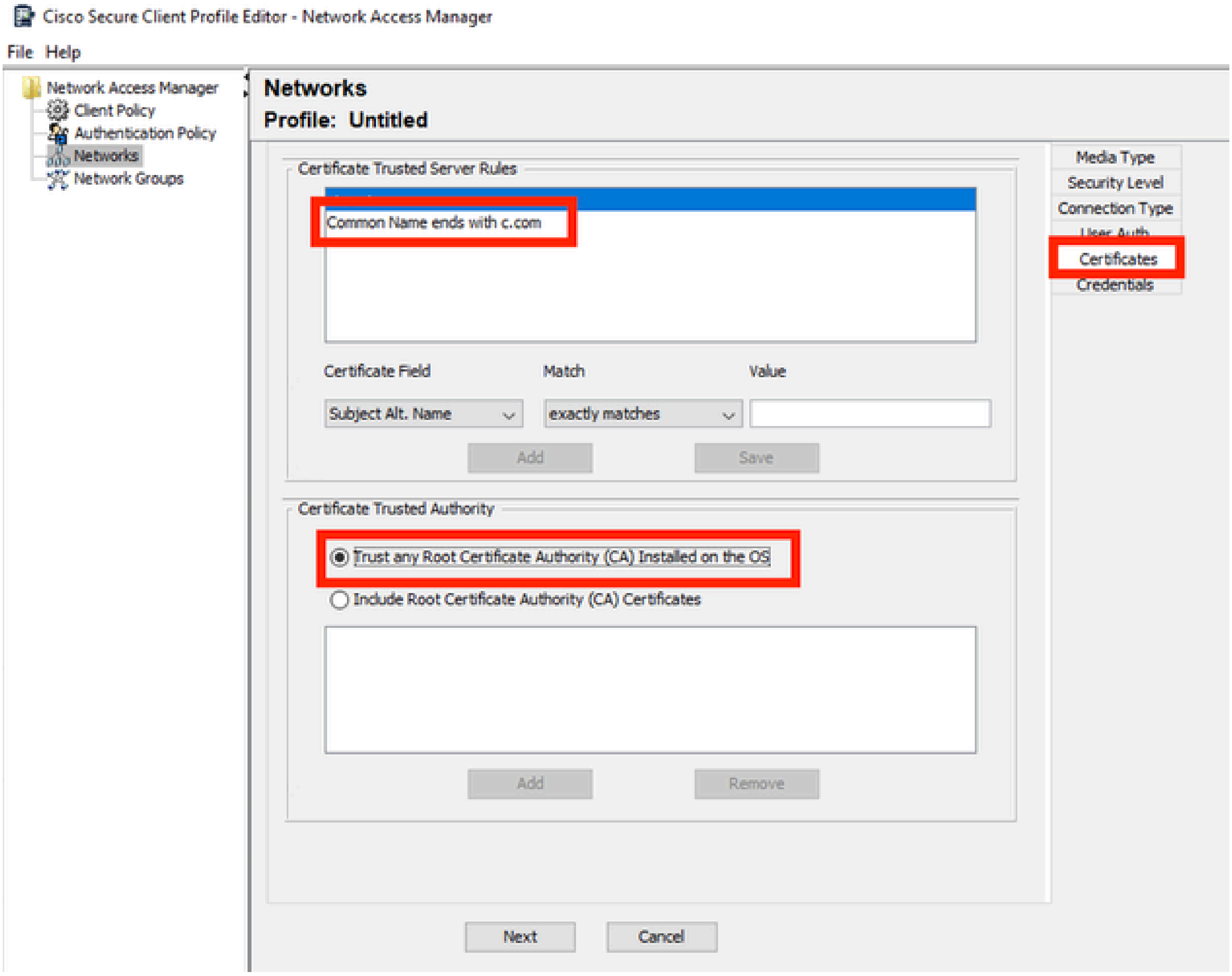
☑ Enable Fast Reconnect

□ Disable when using a Smart Card

User Auth Section

For the Certificates section, create a rule that matches the AAA **EAP-TLS** certificate. If you are using ISE, find this rule in **Administration** > **System** > **Certificates** section.

For the **Certificate Trusted Authority** section select **Trust any Root Certificate Authority (CA) installed on the OS**.



Cisco Secure Client Profile Editor - Network Access Manager

File Help

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

Networks
Profile: Untitled

Certificate Trusted Server Rules

Common Name ends with c.com

Certificate Field	Match	Value
Subject Alt. Name	exactly matches	

Certificate Trusted Authority

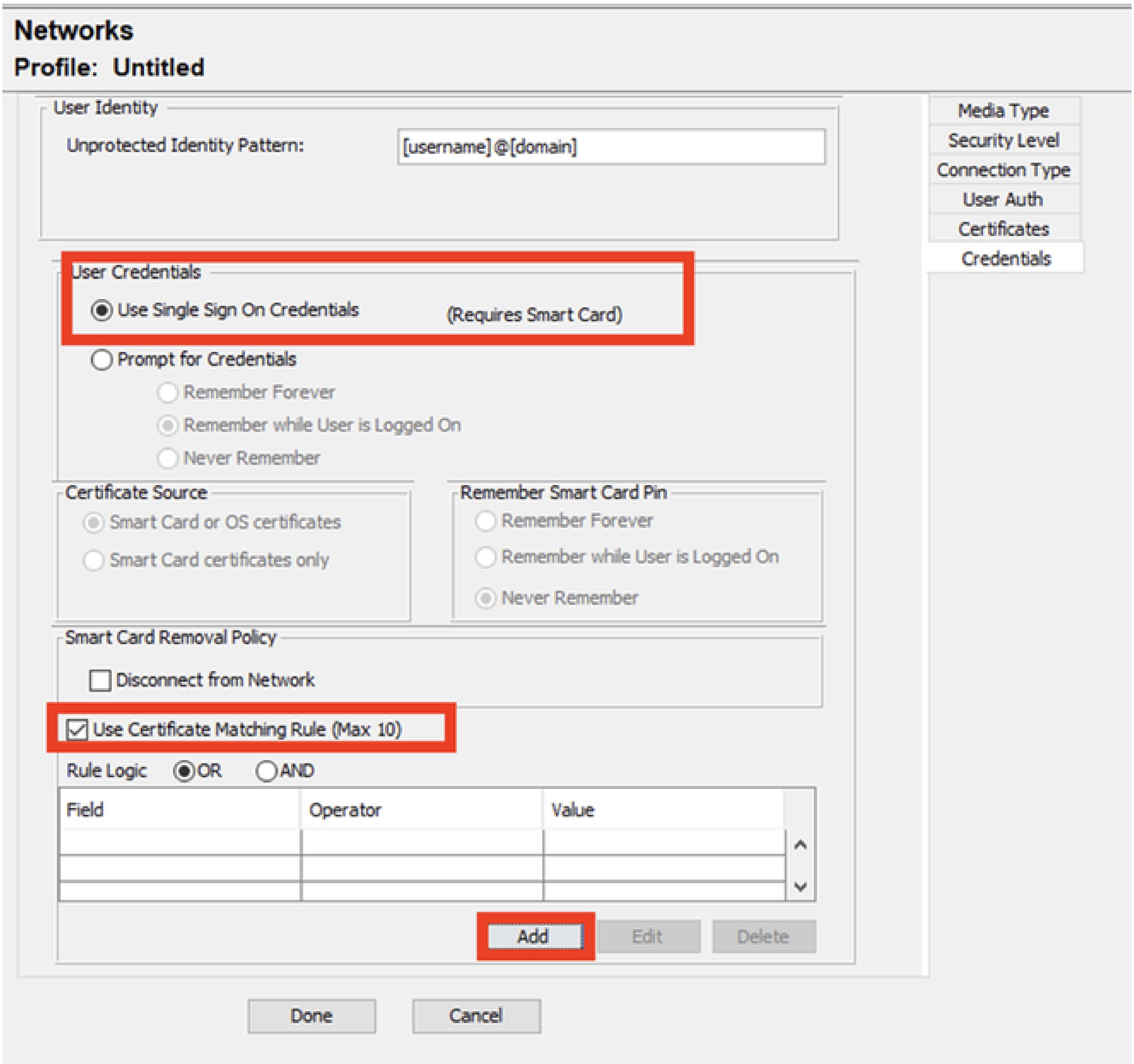
● Trust any Root Certificate Authority (CA) Installed on the OS

○ Include Root Certificate Authority (CA) Certificates

User Auth Server Certificate Trust Settings

Click **Next**.

For the **User Credentials** section, do not change the default values in the first part.



Networks

Profile: Untitled

User Identity

Unprotected Identity Pattern: [username]@[domain]

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)

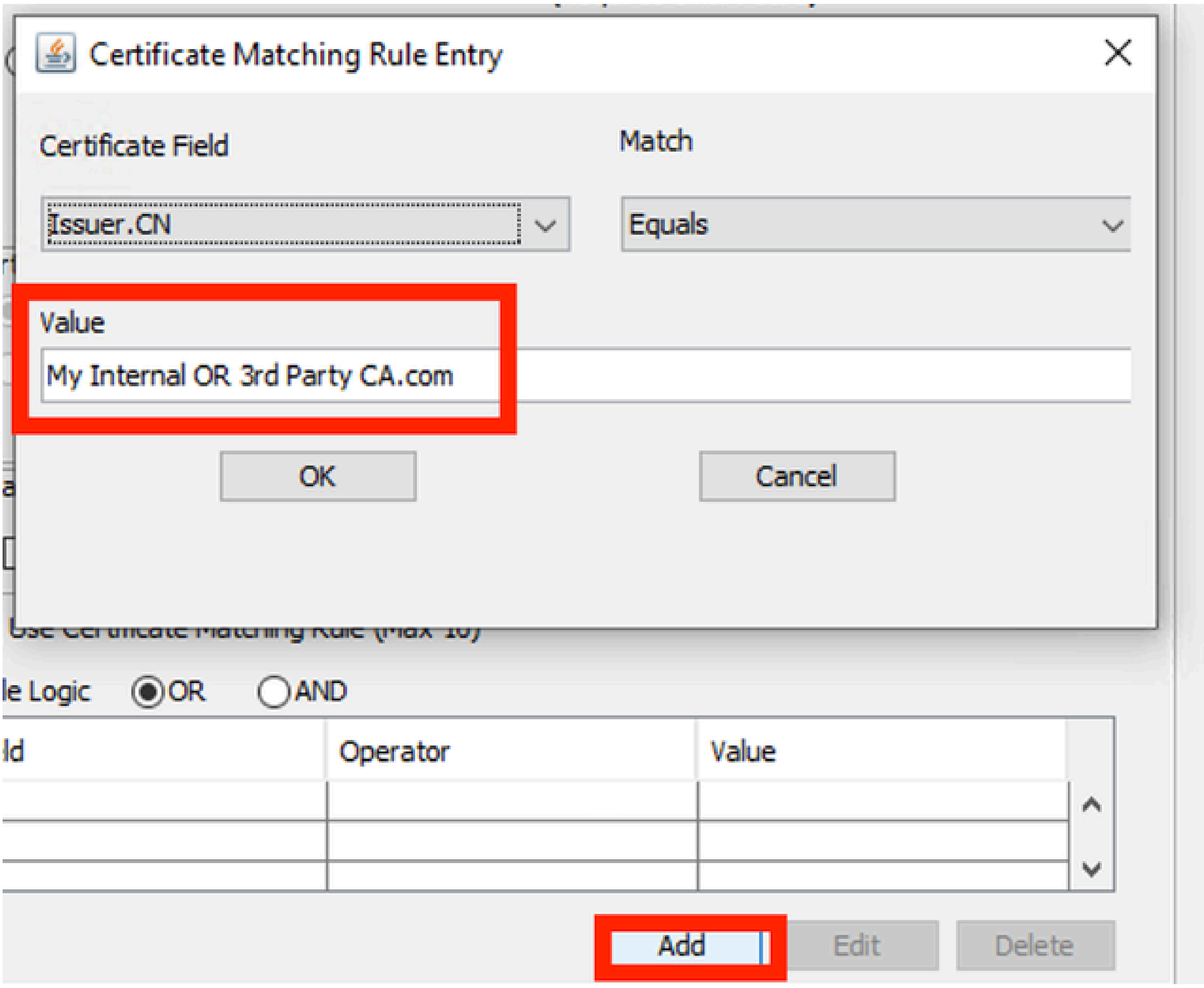
Rule Logic ● OR ○ AND

Field	Operator	Value

User Auth Credentials Section

It is important to configure a rule that matches the identity certificate that the user sends during the EAP TLS process. To do this click the checkbox next to **Use Certificate Maching Rule (Max 10)**.

Click **Add**.



Certificate Matching Rule Entry

Certificate Field: Issuer.CN

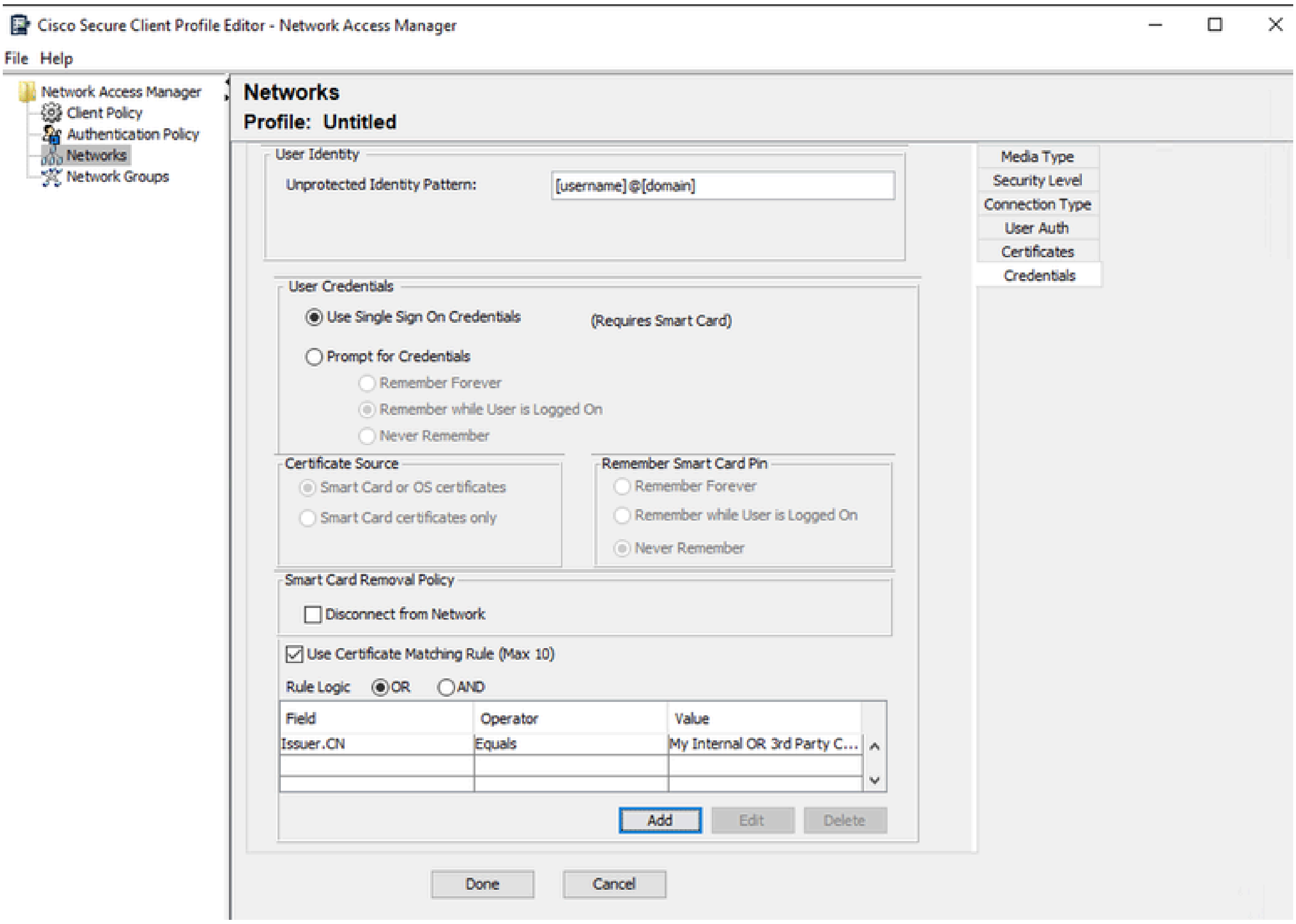
Match: Equals

Value: My Internal OR 3rd Party CA.com

le Logic ●OR ○AND

Certificate Matching Rule Window

Replace the value **My Internal OR 3rd Party CA.com** string with the CN of the user certificate.



Networks

Profile: Untitled

User Identity

Unprotected Identity Pattern: [username]@[domain]

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
Issuer.CN	Equals	My Internal OR 3rd Party C...

User Auth Certificate Credentials Section

Click **Done** to finish the configuration.

Select **File > Save as** to save the **Secure Client Network Access Manager** profile as configuration.xml.

To make the **Secure Client Network Access Manager** use the profile that was just created, replace the configuration.xml file in the next directory with the new one:

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

Note: The file must be named configuration.xml, otherwise it does not work.

7. Configure ISR 1100 and ISE to Allow Authentications Based on Scenario 1 PEAP MSCHAPv2

Configure the ISR 1100 Router.

This section covers the basic configuration that the NAD must have to make dot1x work.

Note: For multi-node ISE deployment, point to any node that has the Policy Server Node persona enabled. This can be checked by navigating to ISE in the **Administration > System > Deployment** tab.

```
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>
!
```

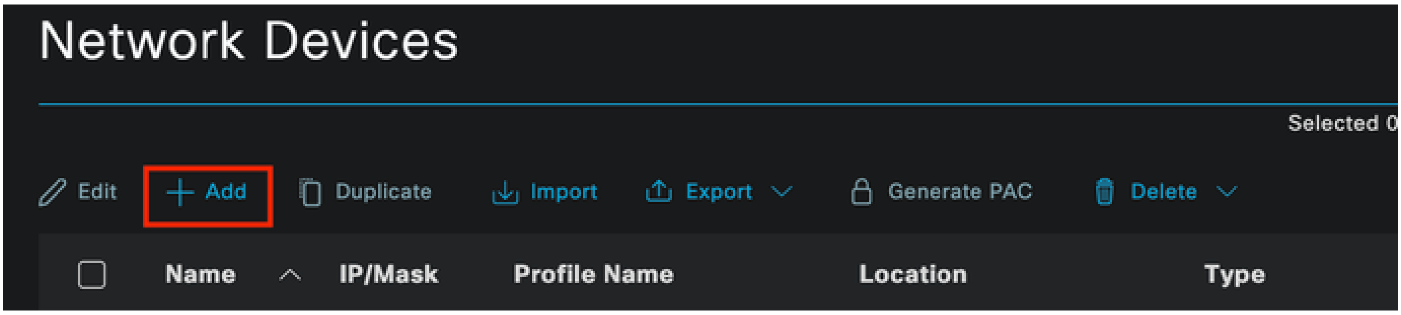
```
!
aaa group server radius ISE-CLUSTER
 server name ISE-PSN-1
!
interface GigabitEthernet0/1/0
 description "Endpoint that supports dot1x"
 switchport access vlan 15
 switchport mode access
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication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

Configure Identity Service Engine 3.2.

Configure the Network Device.

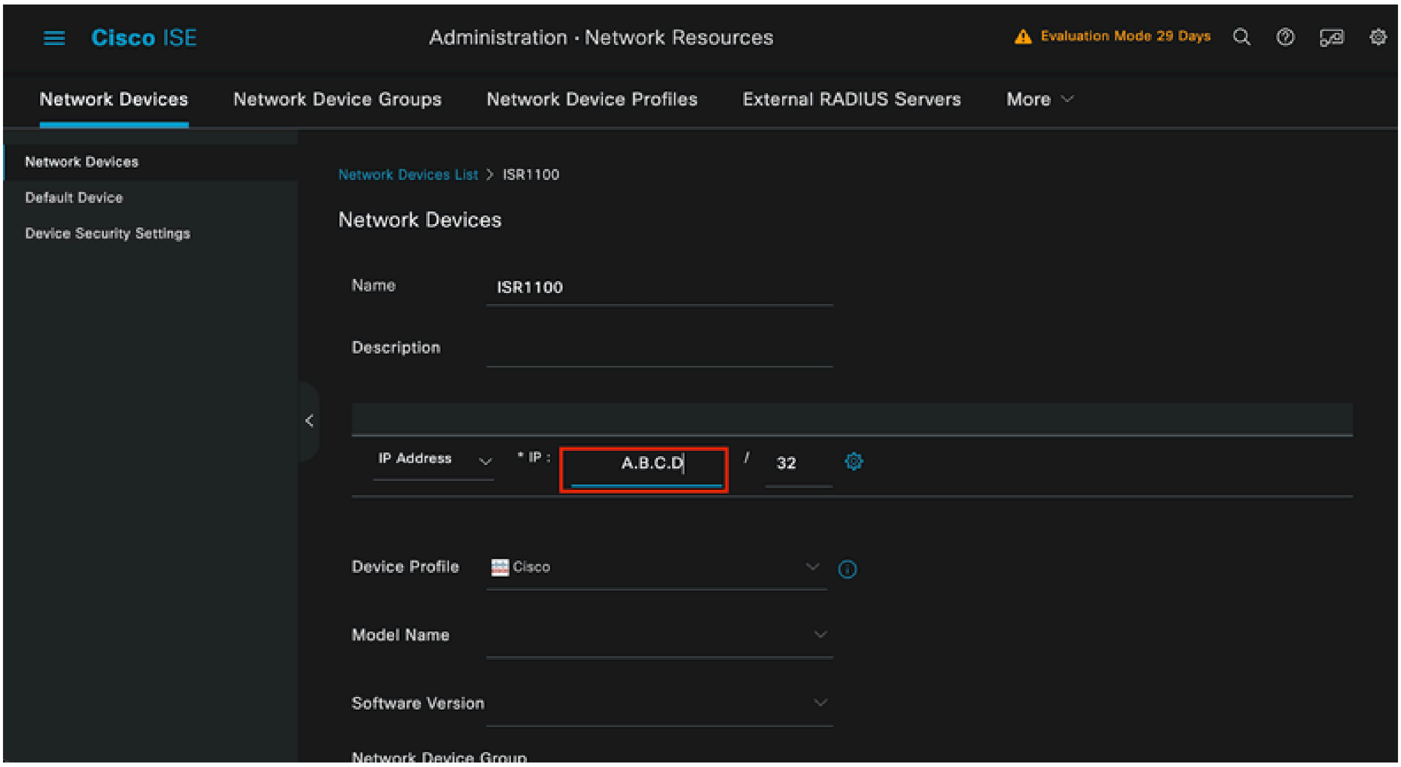
Add the ISR NAD to ISE **Administration** > **Network Resources** > **Network Devices**.

Click **Add**.



Network Device Section

Assign a name to the NAD you are creating. Add the Network Device IP.



Network Devices

Name: ISR1100

Description:

IP Address * IP : A.B.C.D / 32

Device Profile: Cisco

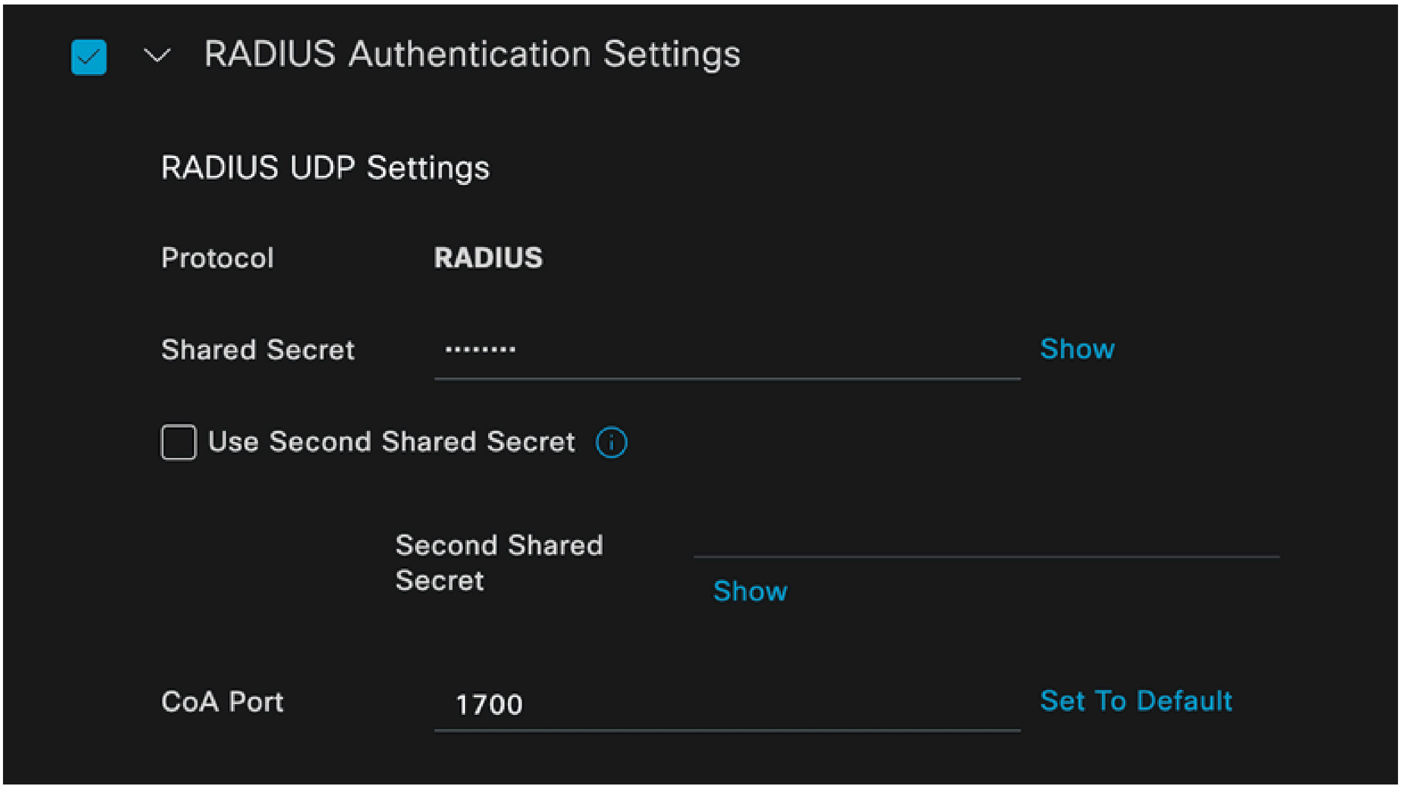
Model Name:

Software Version:

Network Device Group

Network Device Creation

At the bottom of the same page add the same **Shared Secret** that you used in your network device configuration.



☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

Shared Secret: ········· Show

□ Use Second Shared Secret

Second Shared Secret: Show

CoA Port: 1700 Set To Default

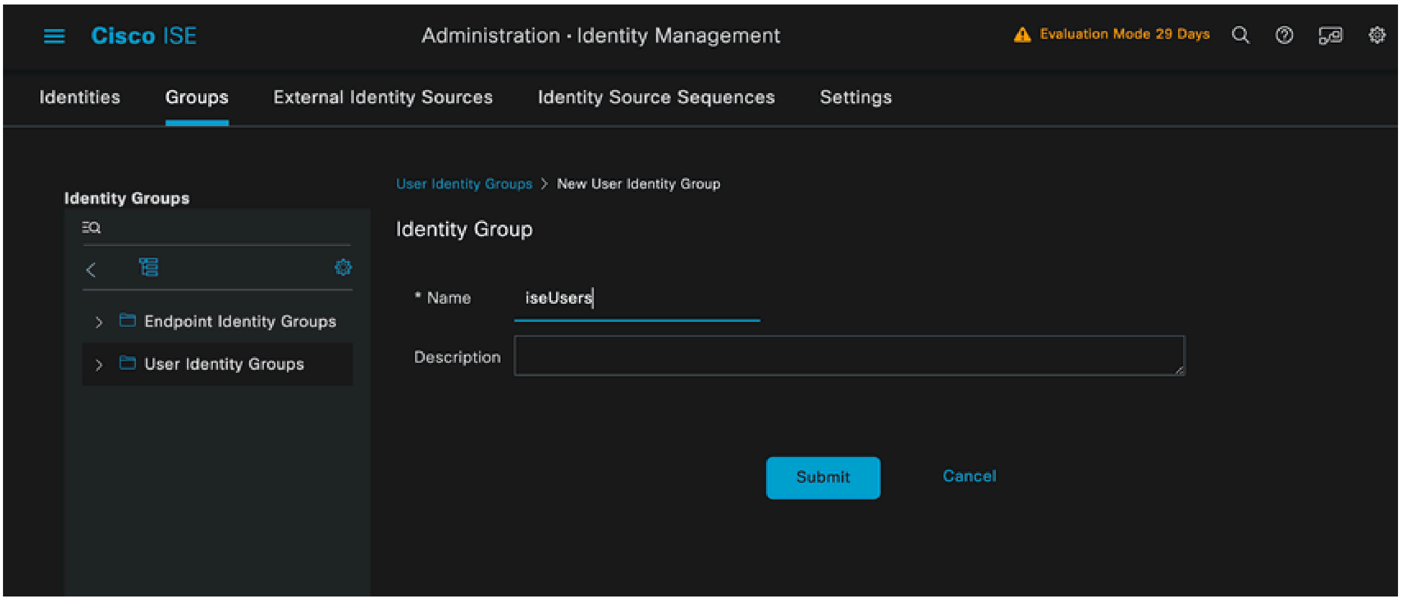
Network Device Radius Settings

Save the changes.

Configure the identity that is used to authenticate the endpoint.

ISE local authentication is used. External ISE authentication is not explained in this article.

Navigate to the **Administration** > **Identity Management** > **Groups** tab and create the group that the user is part of. The identity group created for this demonstration is **iseUsers**.



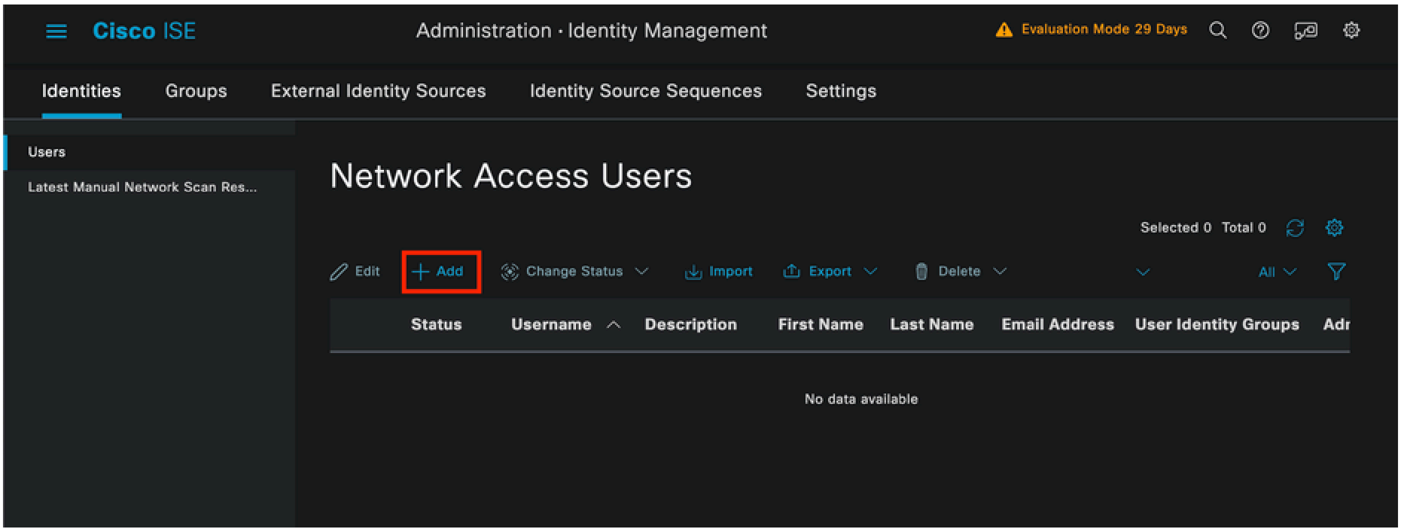
* Name iseUsers

Identity Group Creation

Click **Submit**.

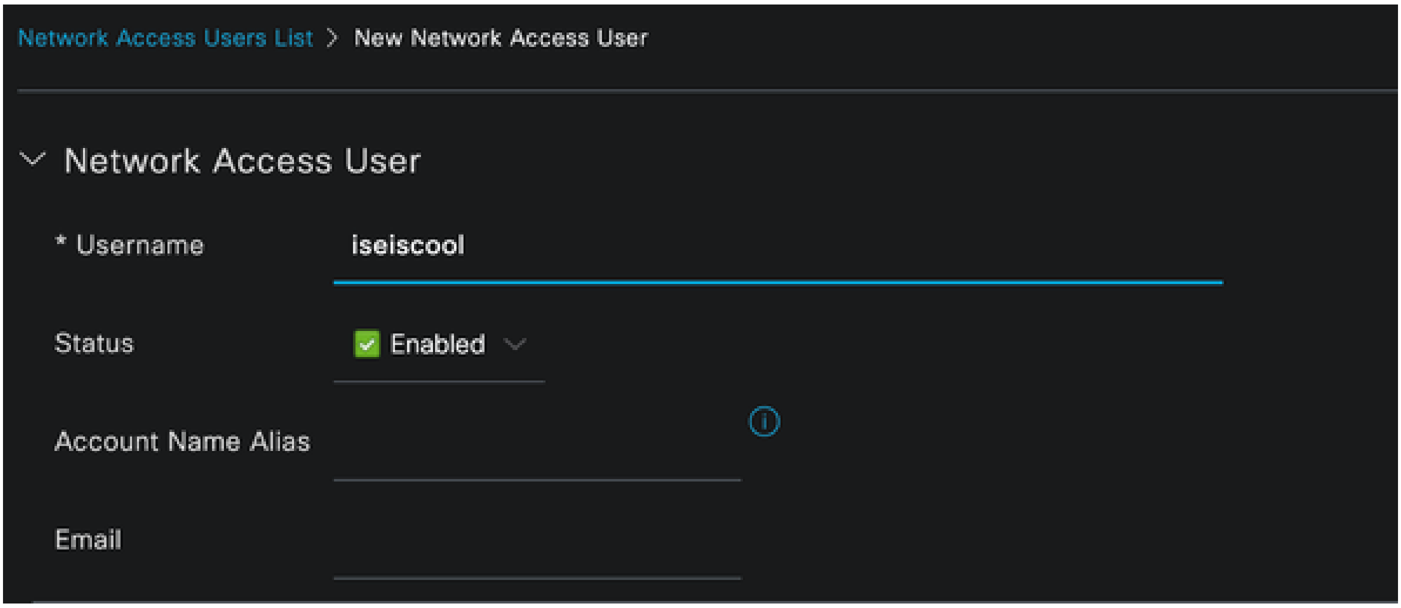
Navigate to **Admistration** > **Identity Management** > **Identity** Tab.

Click **Add**.



Network Access Users Section

As part of the mandatory fields start with the name of the user. The username **iseiscool** is used in this example.



Network Access Users List > New Network Access User

Network Access User

* Username iseiscool

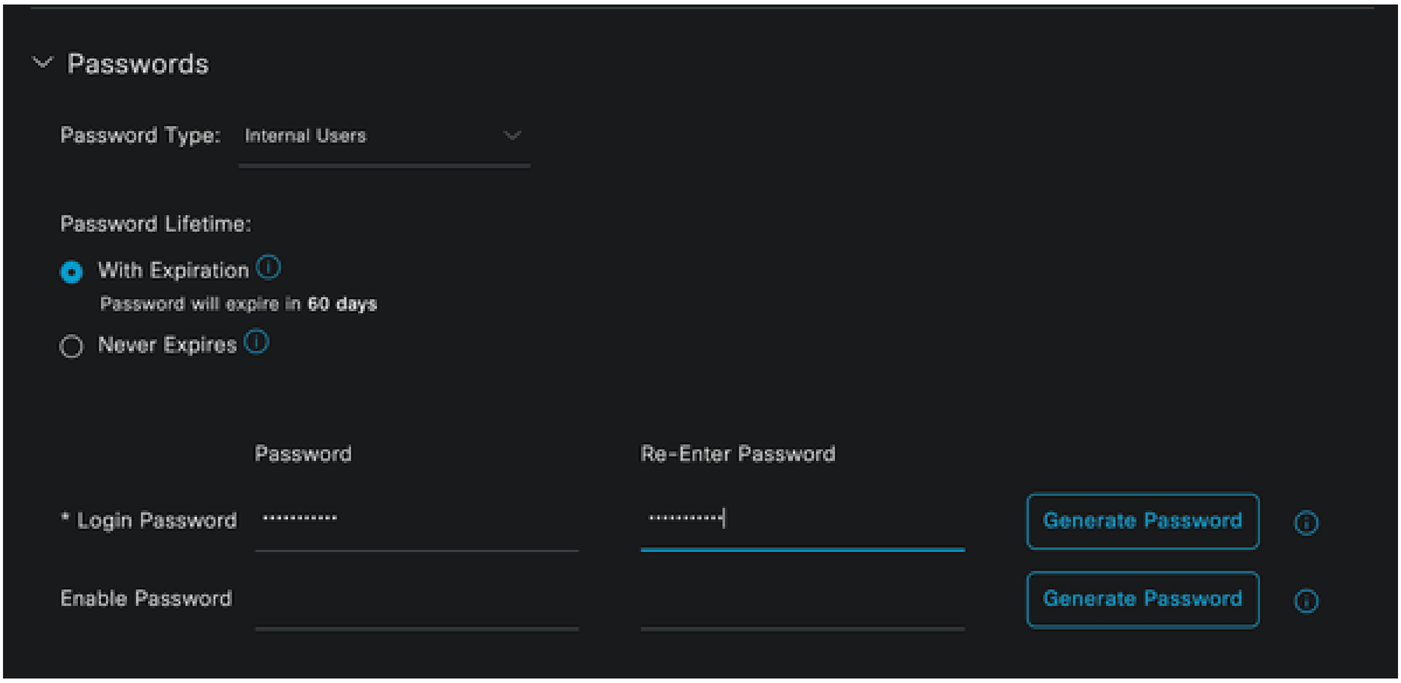
Status ☑ Enabled

Account Name Alias

Email

Network Access User Creation

Assign a password to the user. **VainillaISE97** is used.



Passwords

Password Type: Internal Users

Password Lifetime:

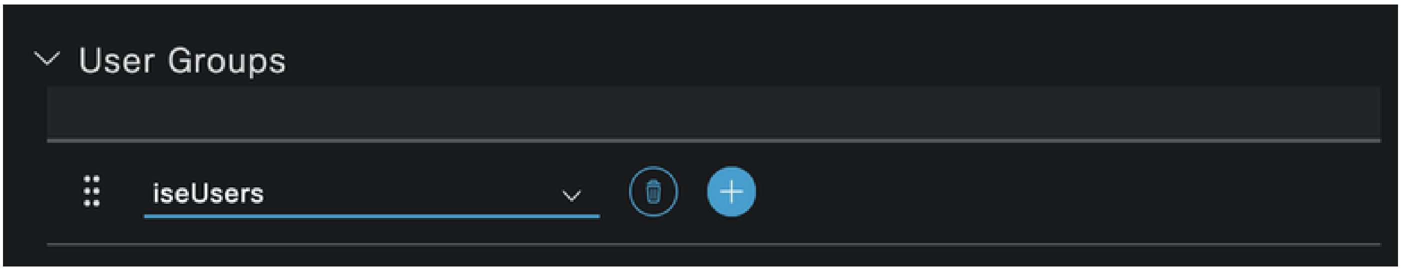
● With Expiration
Password will expire in 60 days

○ Never Expires

	Password	Re-Enter Password	
* Login Password	············	············	Generate Password
Enable Password			Generate Password

User Creation Password Section

Assign the user to the group **iseUsers**.



User Groups

iseUsers

User Group Assignation

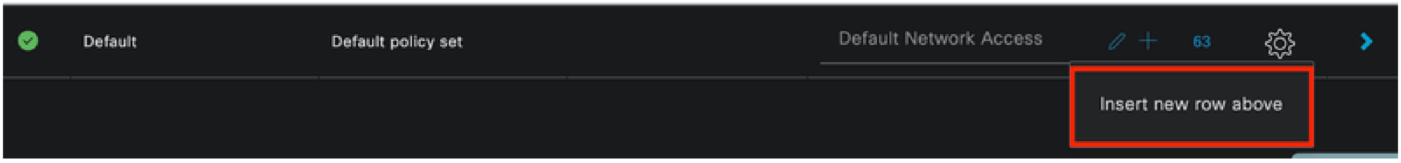
Configure the Policy set.

Navigate to the **ISE Menu > Policy > Policy Sets**.

The default Policy set can be used. However, one called Wired is created for this example.

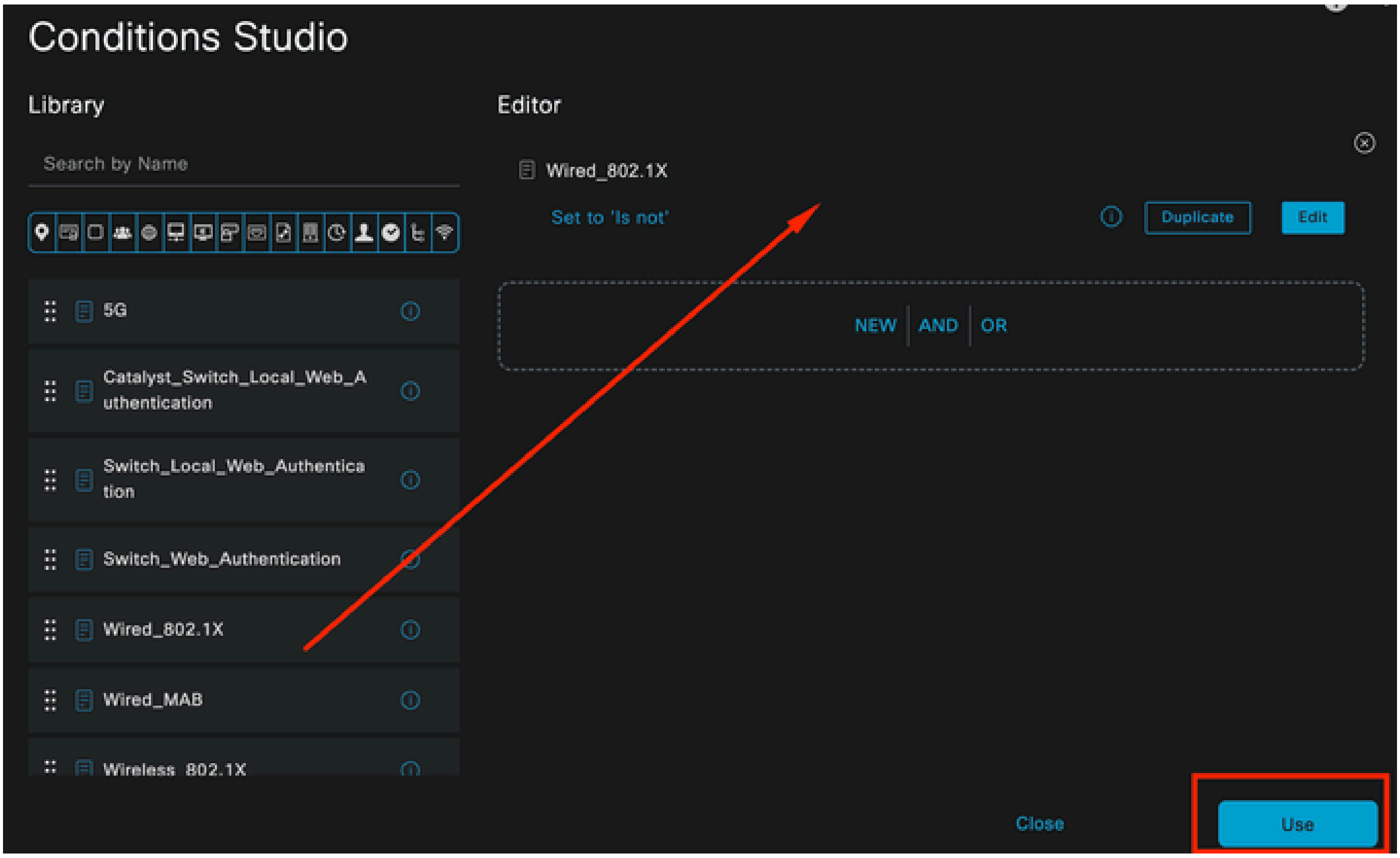
Note: Classifying and differentiating the policy sets helps when troubleshooting,

Note: If the add or plus icon is not visible, the gear icon of any policy set can clicked, and then select **Insert new row above.**



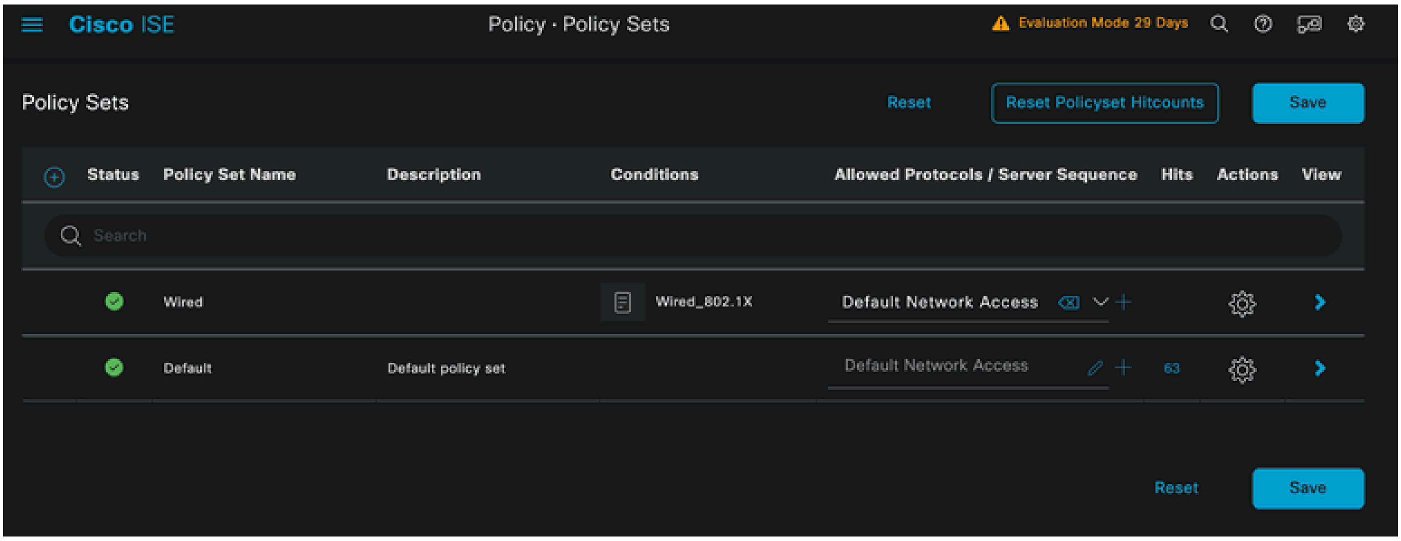
Gear Icon Options

The condition used is **Wired 8021x**. Drag it and then click **Use**.



Authentication Policy Condition Studio

Select **Default Network Access** in the **Allowed Protocols** section.



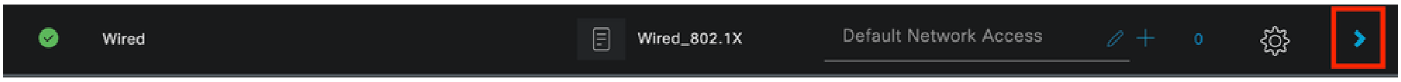
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Wired		Wired_802.1X	Default Network Access		⚙	>
✓	Default	Default policy set		Default Network Access	63	⚙	>

Policy Sets General View

Click **Save**.

2.d. Configure the Authentication and Authorization Policies.

Click the > icon.

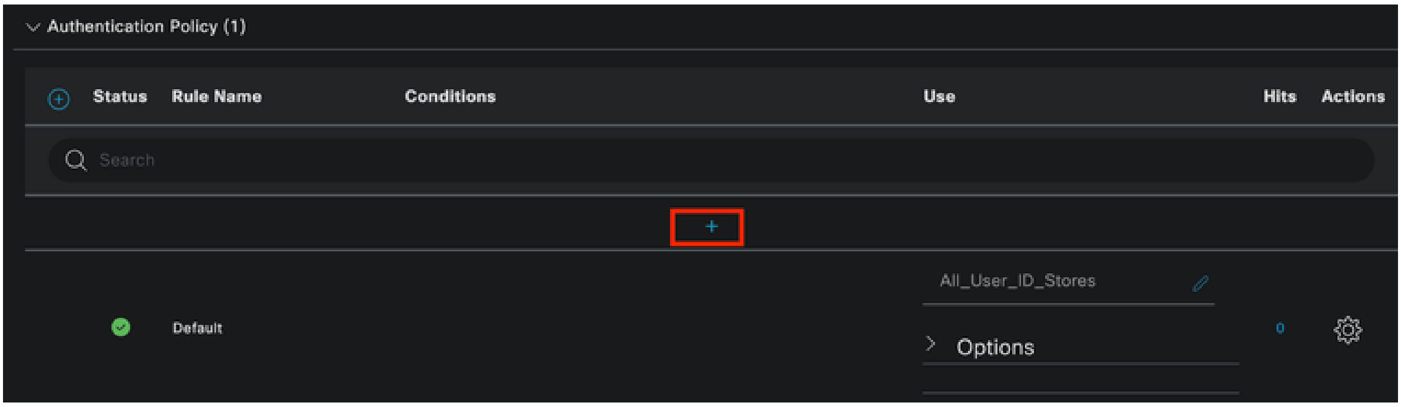


✓	Wired	Wired_802.1X	Default Network Access	0	⚙	>

Wired Policy Set

Expand the **Authentication Policy** section.

Click on the + icon.



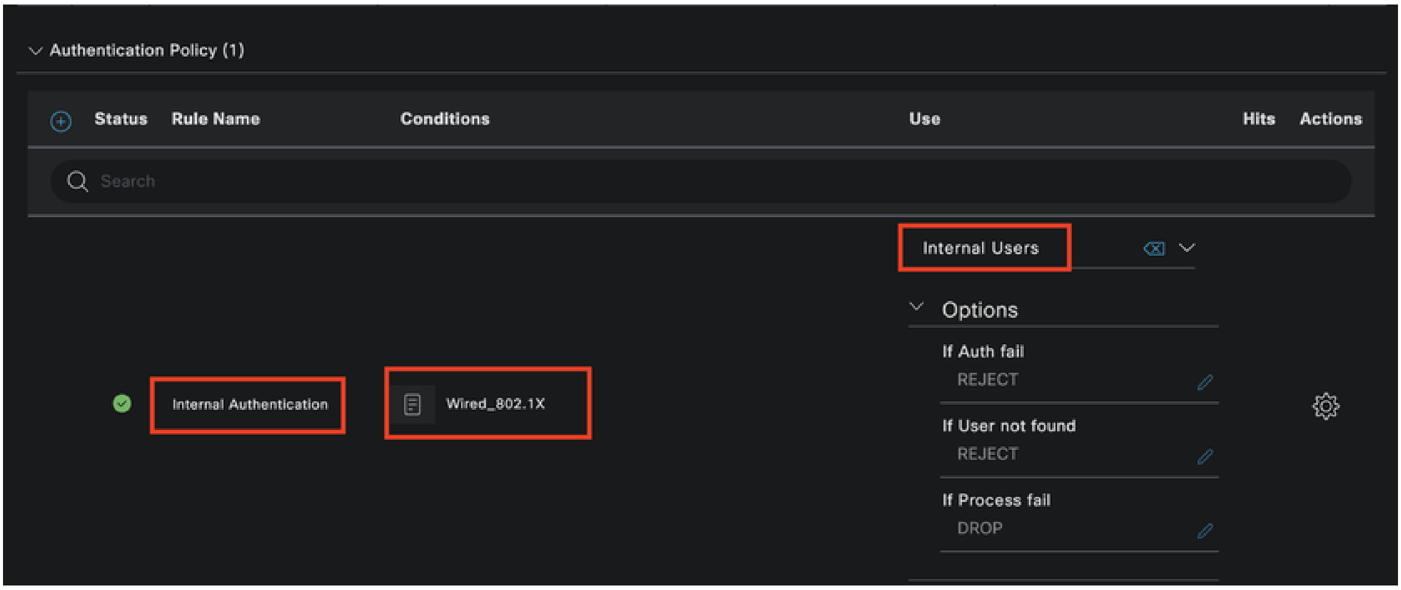
Authentication Policy

Assign a name to the **Authentication Policy**. **Internal Authentication** is used in this example.

Click the + icon on the conditions column for this new **Authentication Policy**.

The pre-configured condition **Wired Dot1x** is used.

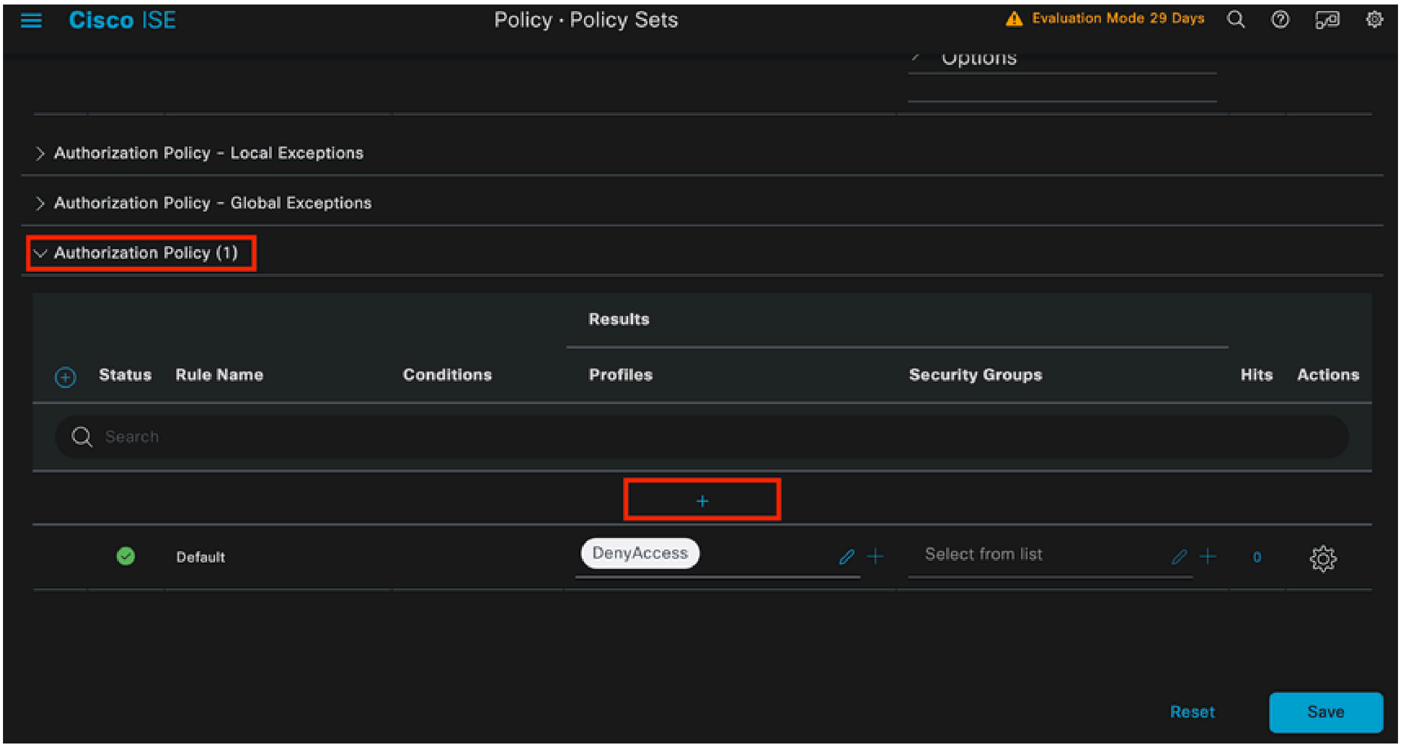
Finally, in the **Use** column select **Internal Users**.



Authentication Policy

Authorization Policy.

The **Authorization Policy** section is at the bottom of the page. Expand it and click the + icon.



Authorization Policy

Name the recently created **Authorization Policy**. In this configuration example the name **Internal ISE Users** is used.

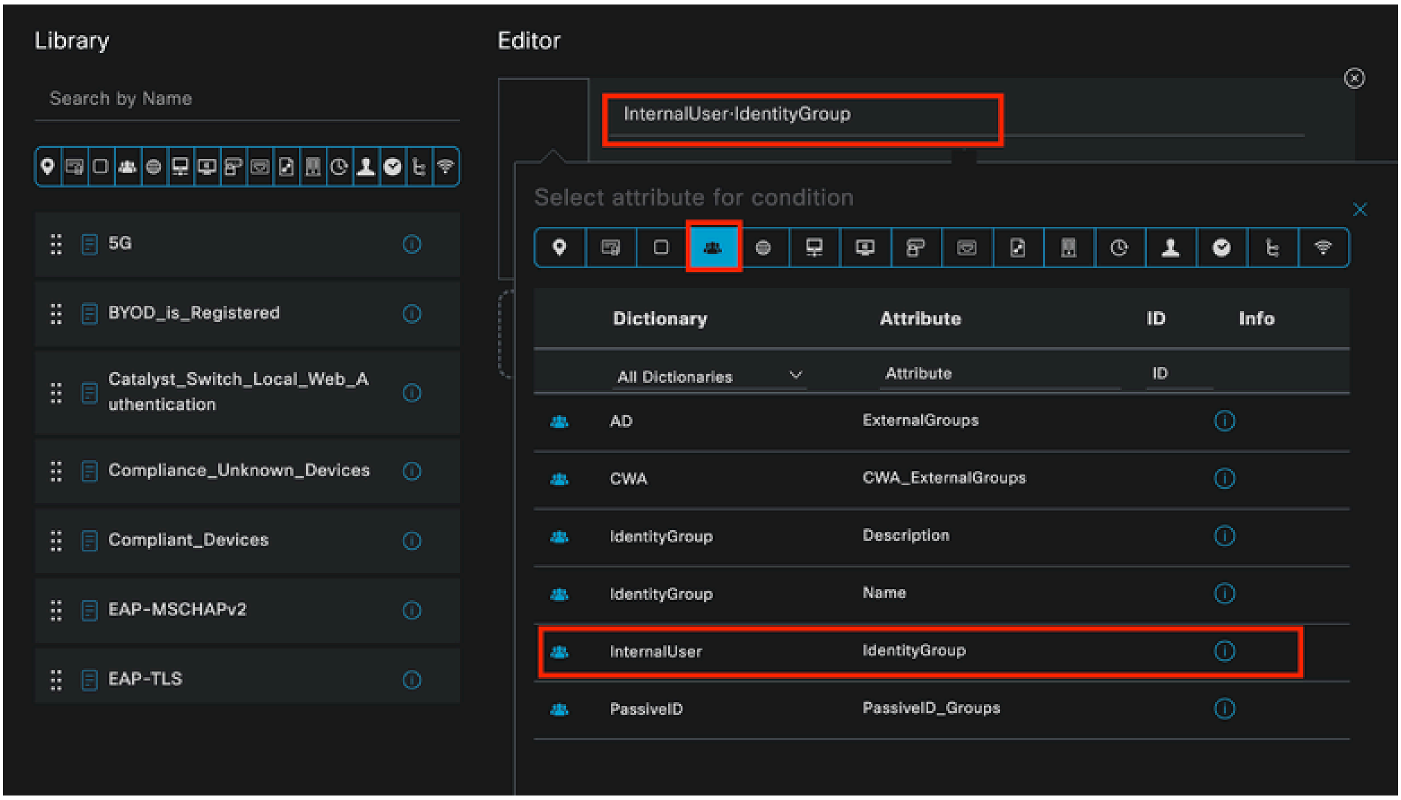
To create a condition for this **Authorization Policy**, click the **+** icon in the **Conditions** column.

The group **IseUsers** is used.

Click the **Attribute** section.

Select the **IdentityGroup** icon.

From the dictionary select the **InternalUser** dictionary that comes with the **IdentityGroup** attribute.



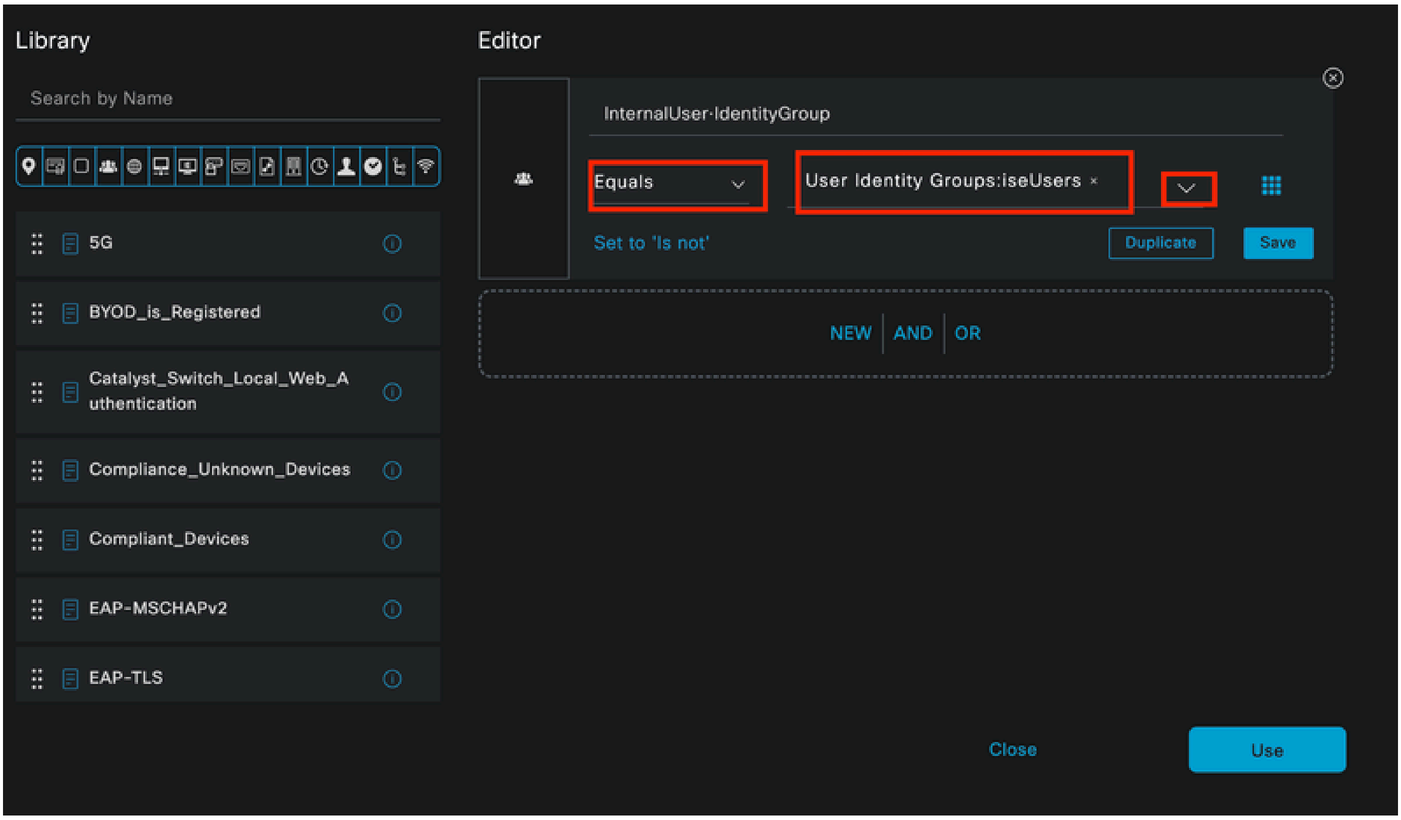
InternalUser·IdentityGroup

Dictionary	Attribute	ID	Info
AD	ExternalGroups		ⓘ
CWA	CWA_ExternalGroups		ⓘ
IdentityGroup	Description		ⓘ
IdentityGroup	Name		ⓘ
InternalUser	IdentityGroup		ⓘ
PassiveID	PassiveID_Groups		ⓘ

Condition Creation

Select the **Equals** operator.

From **User Identity Groups**, select the group **IseUsers**.



InternalUser·IdentityGroup

Equals

User Identity Groups:iseUsers ×

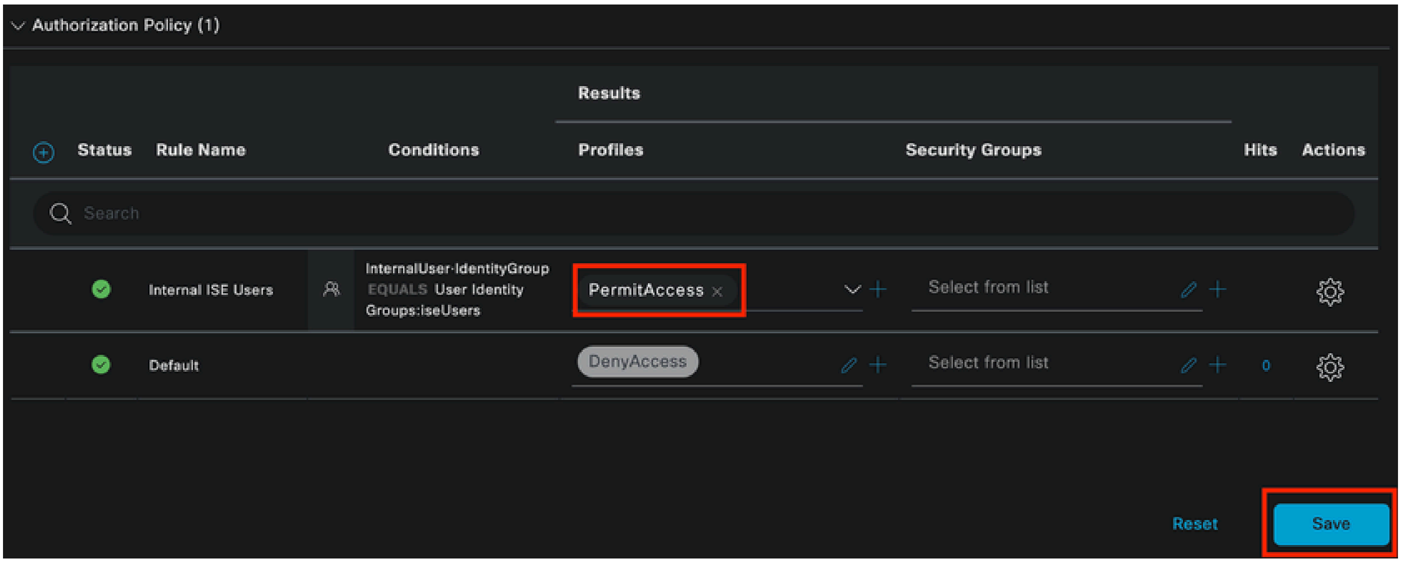
Condition Creation

Click **Use**.

Add the **Result** Authorization Profile.

The pre-configured profile **Permit Access** is used.

Note: Please notice that the Authentications coming to ISE hitting this Wired Dot1x Policy set that are not part of the Users Identity Group ISEUsers, hit the default **Authorization Policy**, which has the result **DenyAccess**.



Authorization Policy (1)

			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
●	Internal ISE Users	InternalUser·IdentityGroup EQUALS User Identity Groups:iseUsers	PermitAccess	Select from list		⚙
●	Default		DenyAccess	Select from list	0	⚙

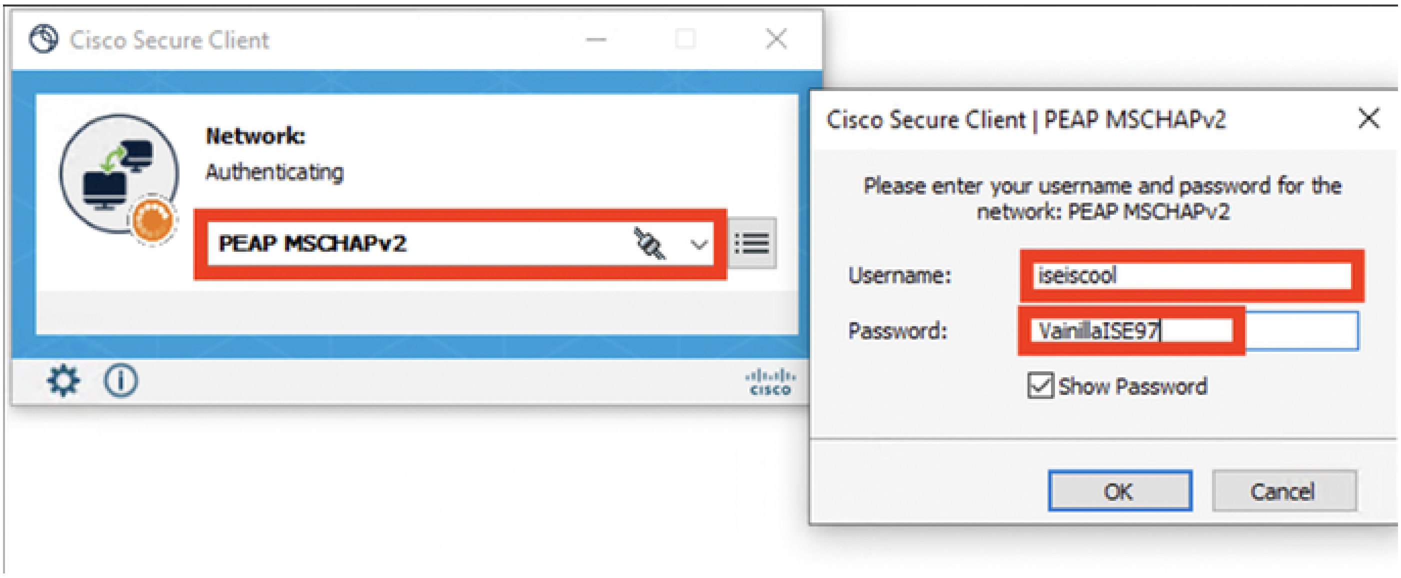
Authorization Policy

Click **Save**.

Verify

Once the configuration is finished Secure Client prompts for the credentials, and it specifies the usage of **PEAP MSCHAPv2** profile.

The credentials previously created are entered.



Cisco Secure Client

Network:
Authenticating

PEAP MSCHAPv2

Cisco Secure Client | PEAP MSCHAPv2

Please enter your username and password for the network: PEAP MSCHAPv2

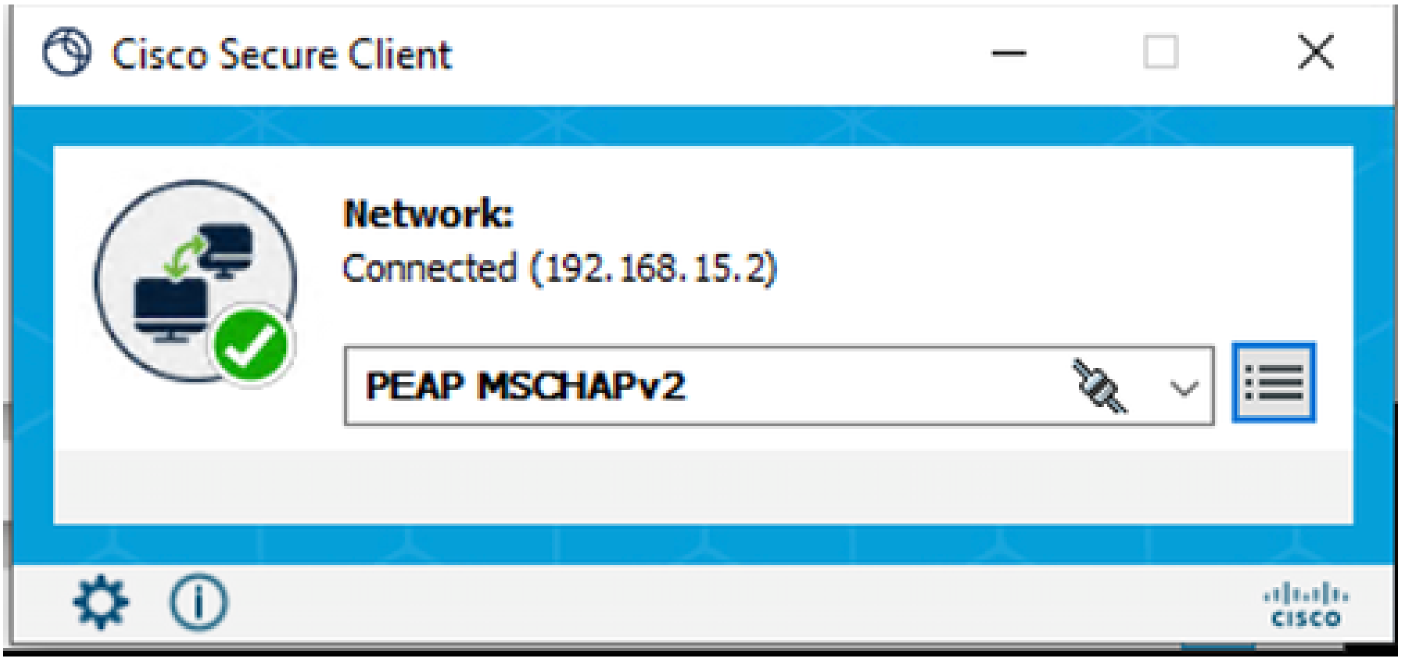
Username: iseiscool

Password: VainillaISE97

☑ Show Password

Secure Client NAM

If the endpoint authenticates correctly,. NAM displays that it is connected.

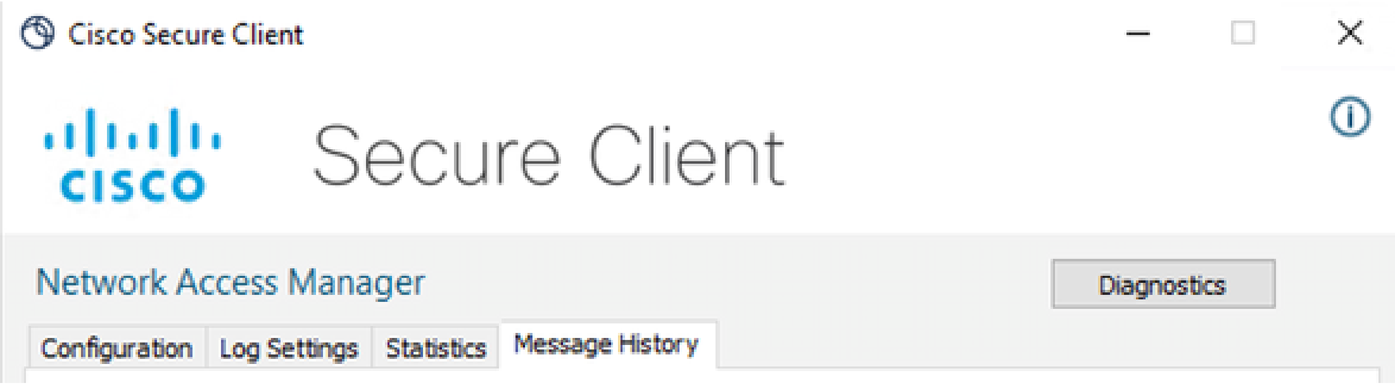


Network:
Connected (192.168.15.2)

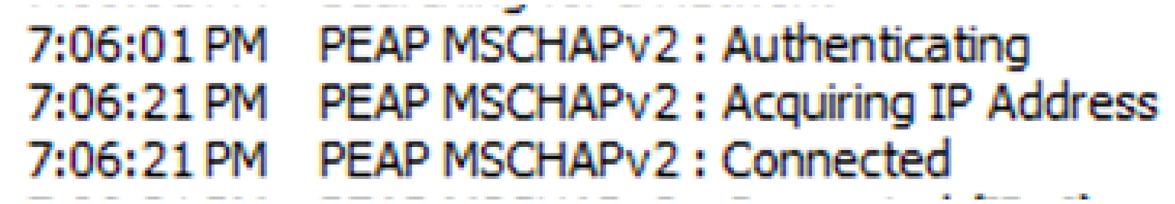
PEAP MSCHAPv2

Secure Client NAM

By clicking the information icon and navigating to the **Message History** section, the details of every step that NAM did are displayed.



Secure Client Message History



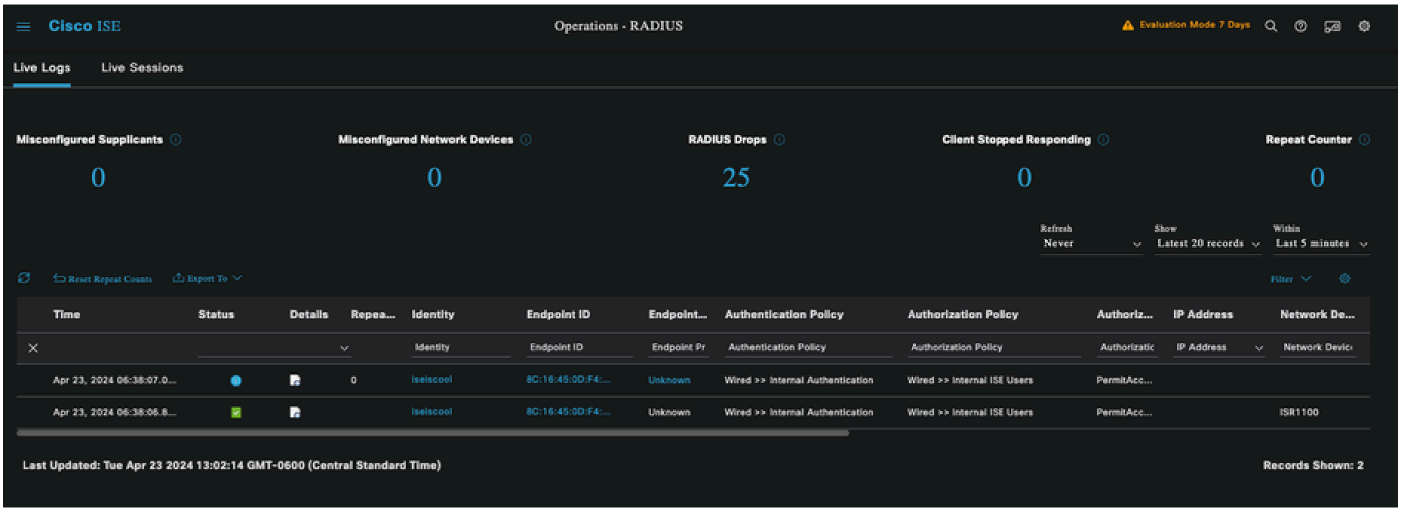
```
7:06:01 PM   PEAP MSCHAPv2 : Authenticating
7:06:21 PM   PEAP MSCHAPv2 : Acquiring IP Address
7:06:21 PM   PEAP MSCHAPv2 : Connected
```

Secure Client Message History

From ISE navigate to **Operations** > **Radius LiveLogs** to see the details of the authentication. As seen in the next image the username that was used is displayed.

Also other details like:

- Timestamp.
- Mac address.
- Policy Set used.
- Authentication Policy.
- Authorization policy.
- Other relevant information.



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	25	0	0

Refresh: Never Show: Latest 20 records Within: Last 5 minutes

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication Policy	Authorization Policy	Authoriz...	IP Address	Network De...
Apr 23, 2024 06:38:07.0...	●	🗎	0	iseiscool	8C:16:45:0D:F4:...	Unknown	Wired >> Internal Authentication	Wired >> Internal ISE Users	PermitAcc...		
Apr 23, 2024 06:38:06.8...	✓	🗎		iseiscool	8C:16:45:0D:F4:...	Unknown	Wired >> Internal Authentication	Wired >> Internal ISE Users	PermitAcc...		ISR1100

Last Updated: Tue Apr 23 2024 13:02:14 GMT-0600 (Central Standard Time)

Records Shown: 2

ISE RADIUS Live Logs

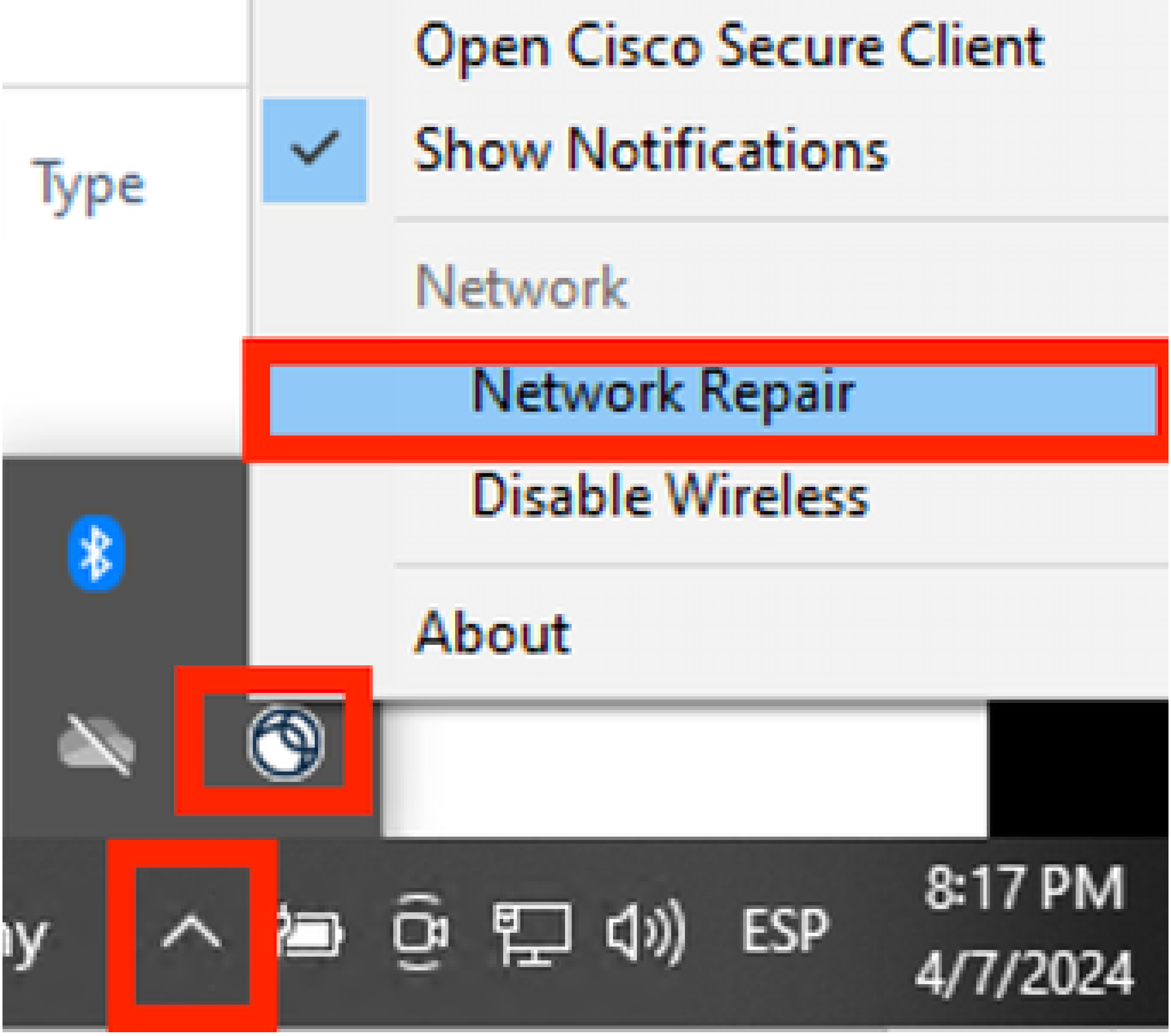
Since you can see it hits the correct policies, and the result is a successful authentication status it is conclude that the configuration is correct.

Troubleshoot

Problem: The NAM profile is not used by Secure Client.

If the new profile that was created in the profile editor is not used by NAM, use the **Network Repair** option for Secure Client.

You can find this option by navigating to the **Windows Bar > Clicking the circumflex icon > Right-Click Secure Client Icon > Click Network Repair**.

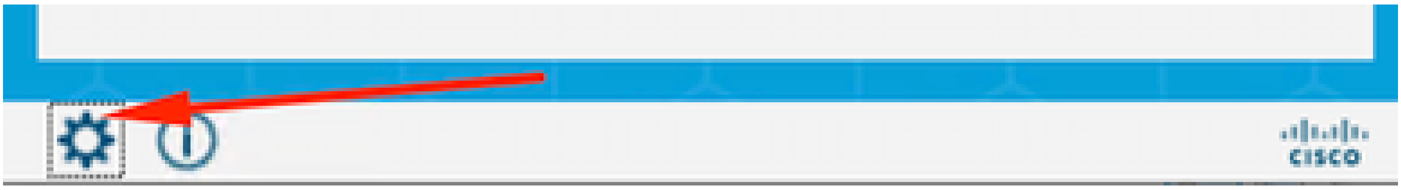


Network Repair Section

Problem 2: Logs need to be collected for further analysis.

1. Enable NAM extended logging

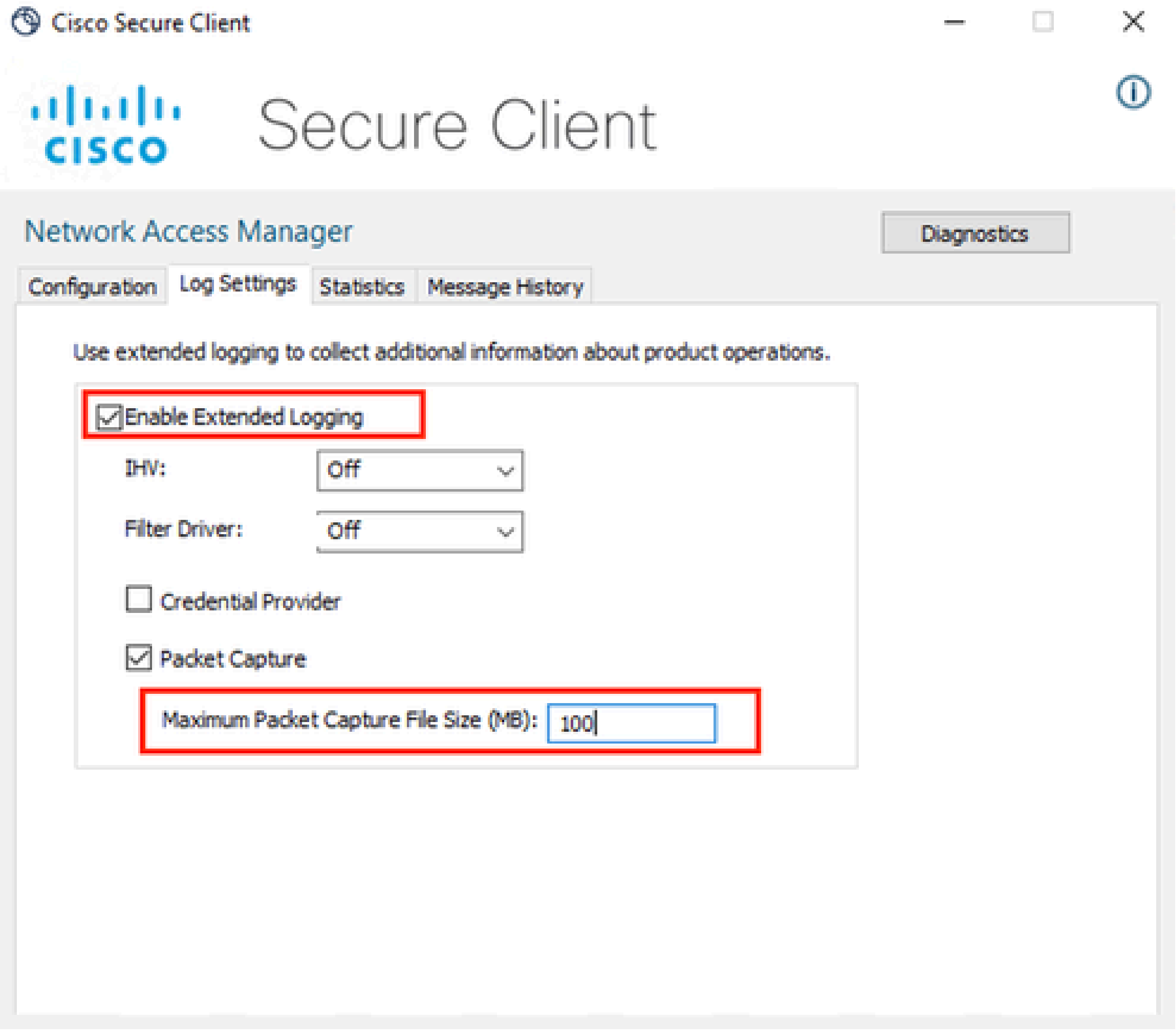
Open NAM, and click the gear icon.



NAM Interface

Navigate to the **Log Settings** tab. Check the **Enable Extended Logging** checkbox.

Set the **Packet Capture File Size** to 100 MB.



Use extended logging to collect additional information about product operations.

☑ Enable Extended Logging

IHV: Off

Filter Driver: Off

□ Credential Provider

☑ Packet Capture

Maximum Packet Capture File Size (MB): 100

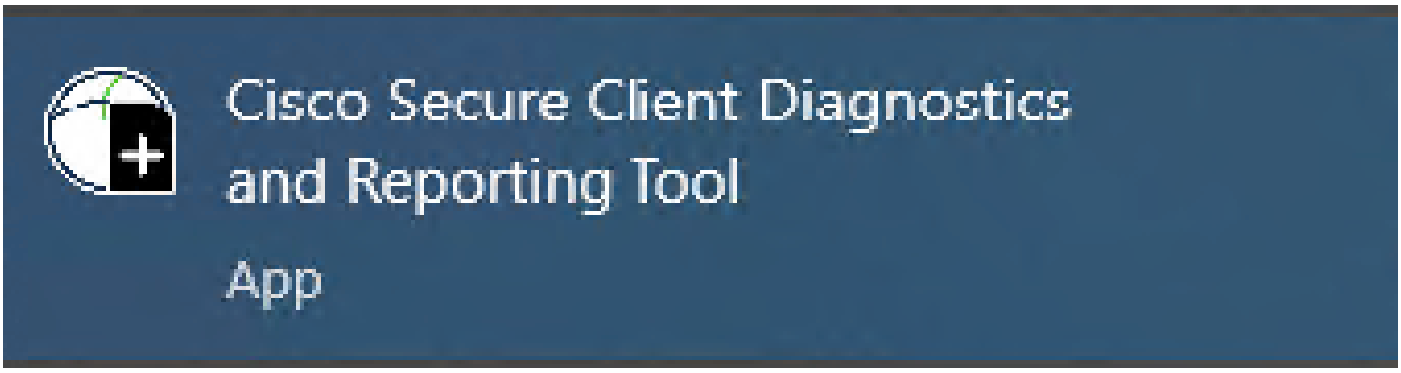
Secure Client NAM Log Settings

2. Reproduce the issue.

Once extended logging is enabled reproduce the issue multiple times to ensure the logs are generated and the traffic is captured.

3. Collect Secure Client DART bundle.

From Windows, navigate to the search bar and type, **Cisco Secure Client Diagnostics and Reporting Tool**.



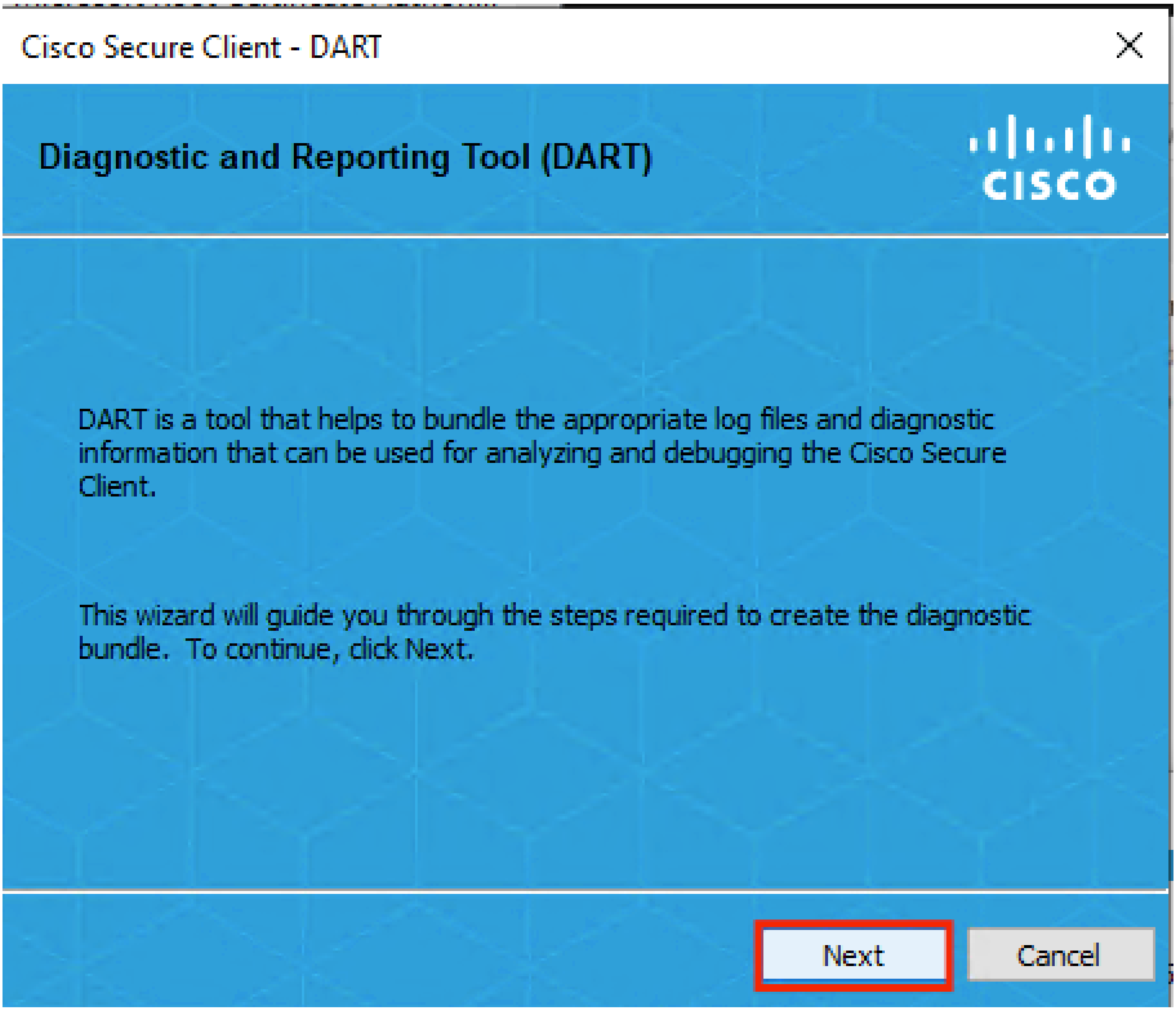
Cisco Secure Client Diagnostics and Reporting Tool

App

DART Module

During the installation process, you also installed this module. It is a tool that helps during the troubleshooting process by collecting logs and relevant dot1x session information.

Click **Next** in the first window.



Cisco Secure Client - DART

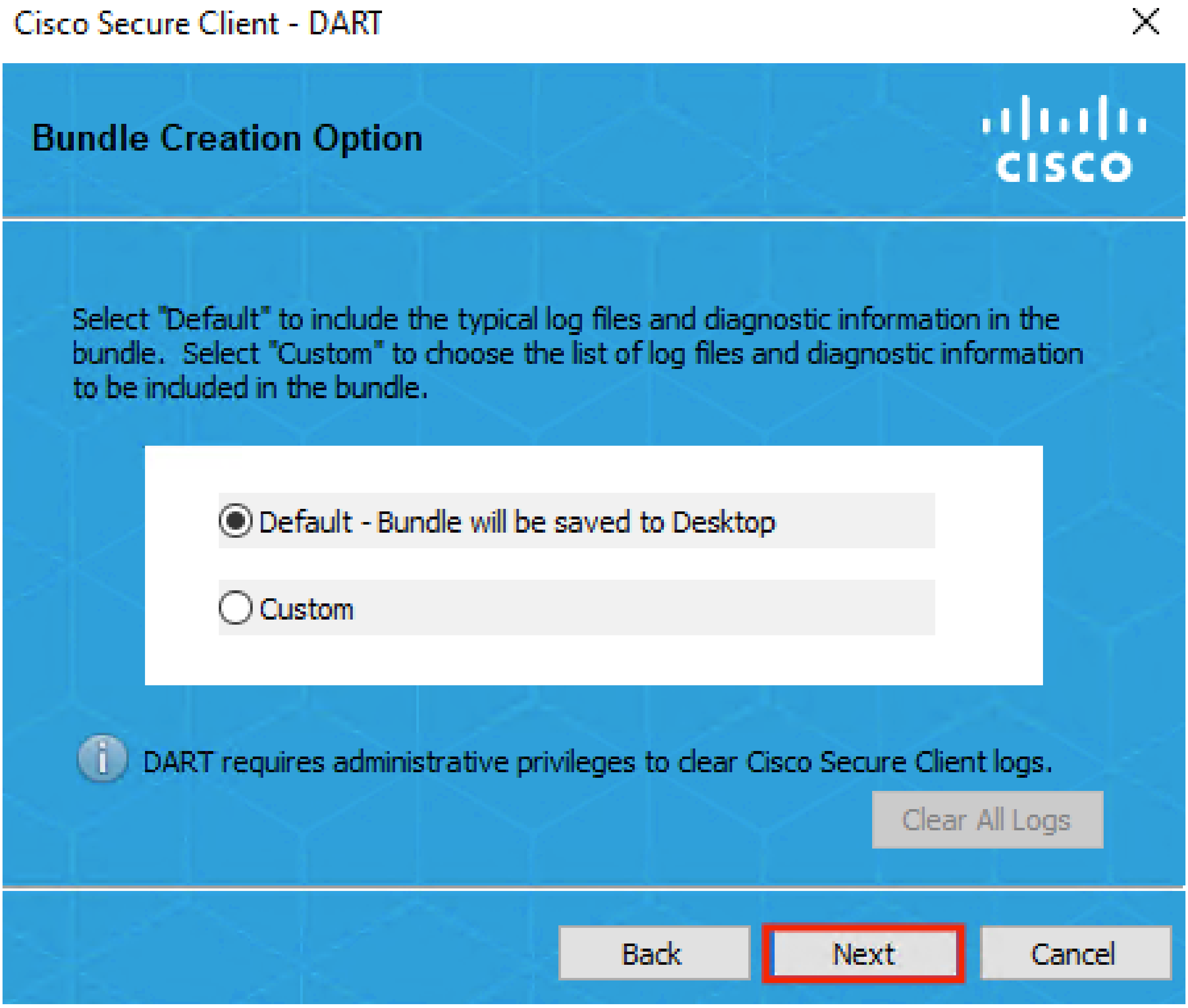
Diagnostic and Reporting Tool (DART)

DART is a tool that helps to bundle the appropriate log files and diagnostic information that can be used for analyzing and debugging the Cisco Secure Client.

This wizard will guide you through the steps required to create the diagnostic bundle. To continue, click Next.

DART Module

Once again click **Next**, so the log bundle can be saved on the 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.

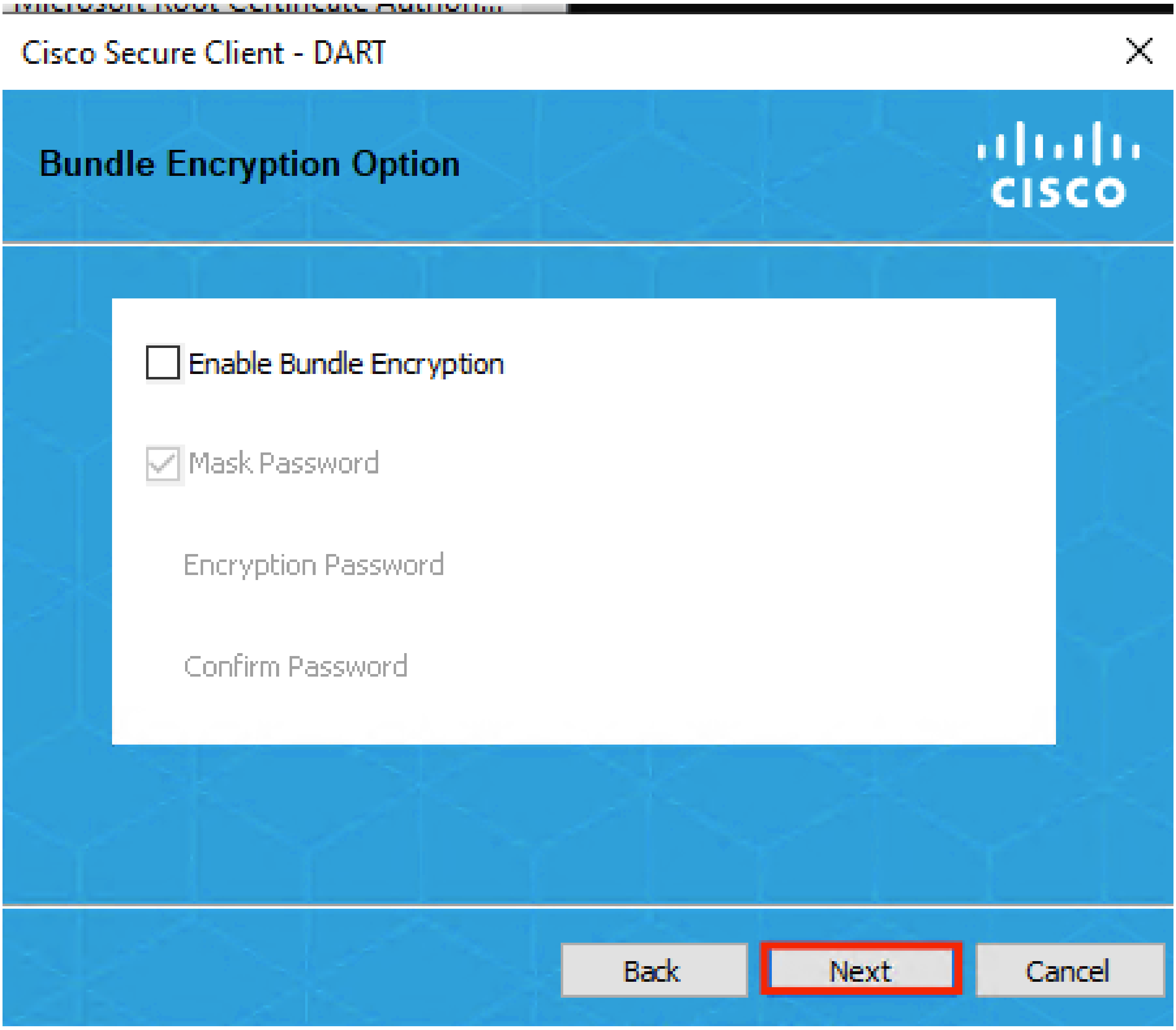
● Default - Bundle will be saved to Desktop

○ Custom

DART requires administrative privileges to clear Cisco Secure Client logs.

DART Module

If necessary check the checkbox **Enable Bundle Encryption**.



Cisco Secure Client - DART

Bundle Encryption Option

☐ Enable Bundle Encryption

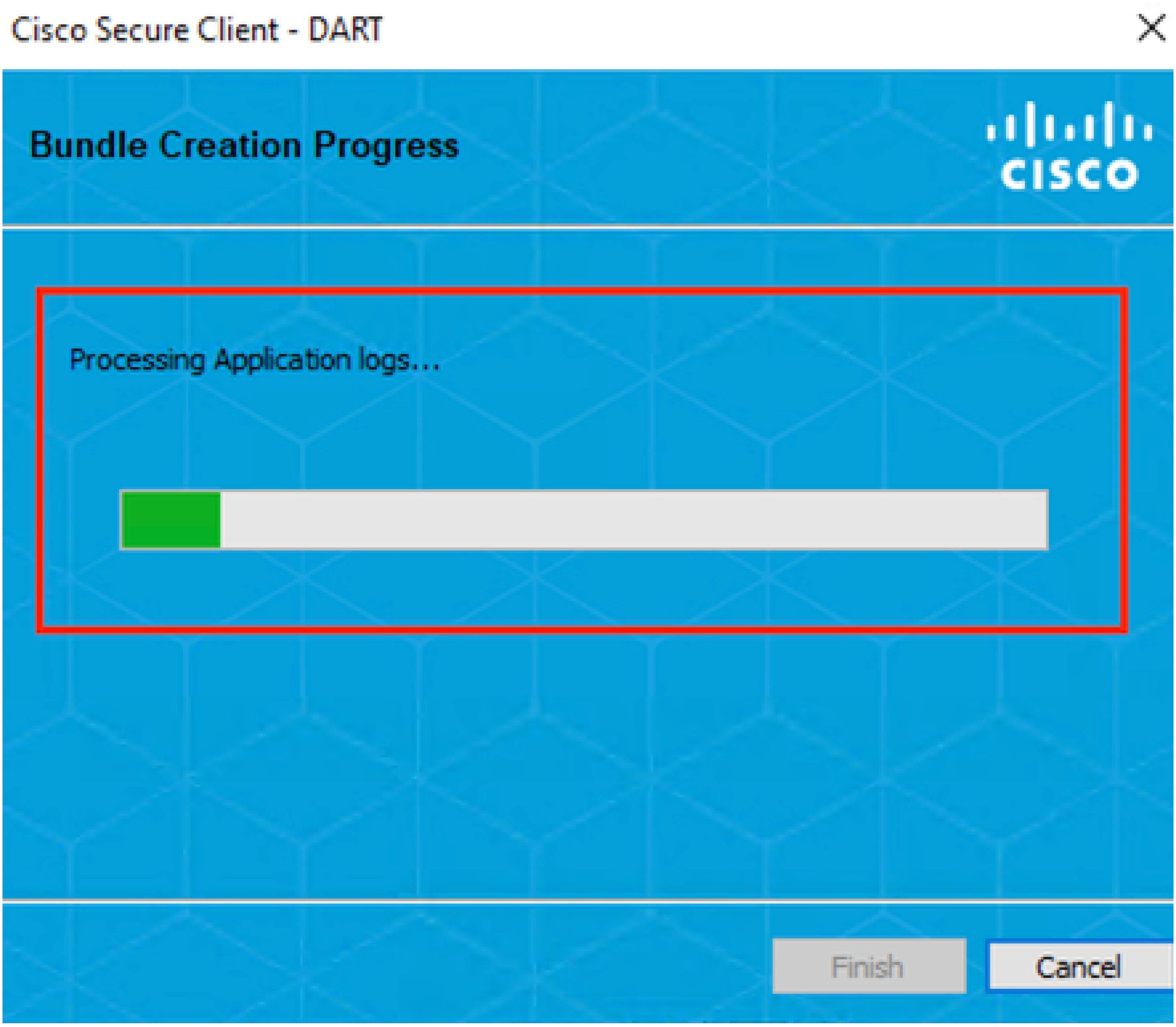
☑ Mask Password

Encryption Password

Confirm Password

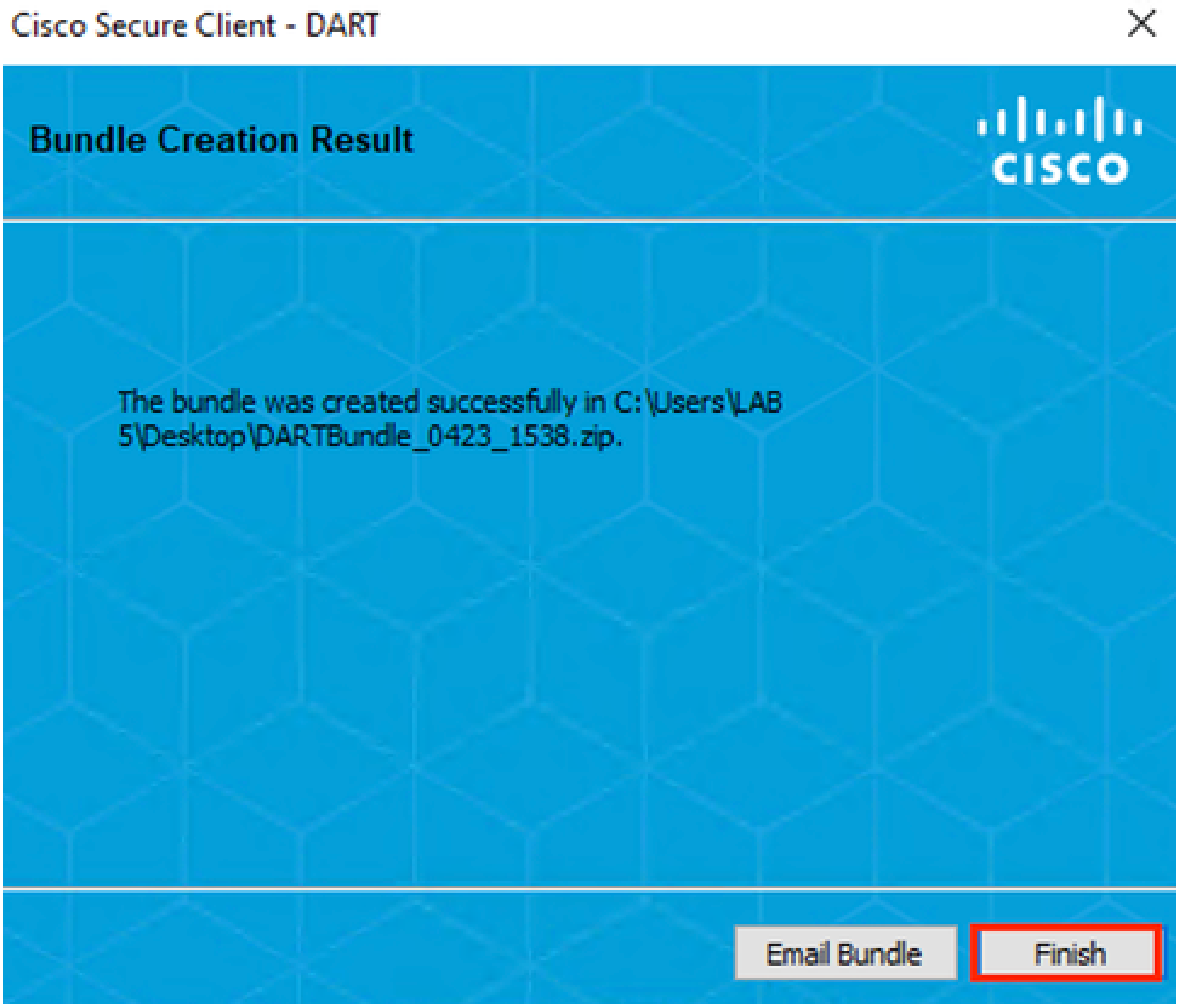
DART Module

DART log collection starts.



DART Log Collection

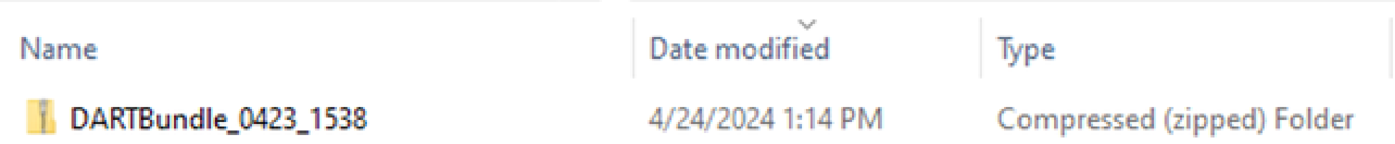
It can take 10 minutes or more until the process finishes.



The bundle was created successfully in C:\Users\LAB 5\Desktop\DARTBundle_0423_1538.zip.

DART Bundle Creation Result

The **DART** result file can be found in the desktop directory.



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

DART Result File

Related Information

- Cisco Technical Support & Downloads