

# Configure Secure Client NAM for Dot1x Using Windows and ISE 3.2

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Background Information](#)

### [Configure](#)

[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 Secure Client NAM Supplicant for PEAP \(MS-CHAPv2\) User Authentication](#)
- [5. Scenario 2: Configure Secure Client NAM Supplicant for EAP-FAST Simultaneous User and Machine Authentication](#)
- [6. Scenario 3: Configure Secure Client NAM Supplicant for EAP-TLS User Certificate Authentication](#)
- [7. Configure ISR 1100 and ISE to Allow Authentications Based on Scenario 1 PEAP MSCHAPv2](#)

### [Verify](#)

### [Troubleshoot](#)

[Problem: The NAM profile is not used by Secure Client.](#)

[Problem 2: Logs need to be collected for further analysis.](#)

- [1. Enable NAM extended logging](#)
- [2. Reproduce the issue.](#)
- [3. Collect Secure Client DART bundle.](#)

### [Related Information](#)

---

## 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.

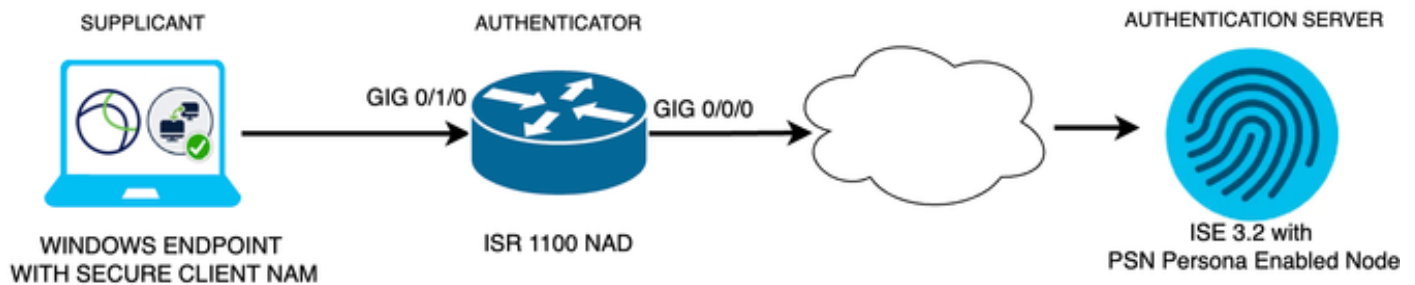
## Configure

### Network Diagram

It is crucial to understand that for dot1x authentications 3 parts are needed;

1. the supplicant which can do dot1x,
2. the authenticator also known as NAS/NAD which serves as a proxy encapsulating the dot1x traffic inside RADIUS,
3. 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   
[cisco-secure-client-win-5.1.2.42-predeploy-k9.zip](#)  
[Advisories](#) 

06-Feb-2024 108.30 MB



*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.

---

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

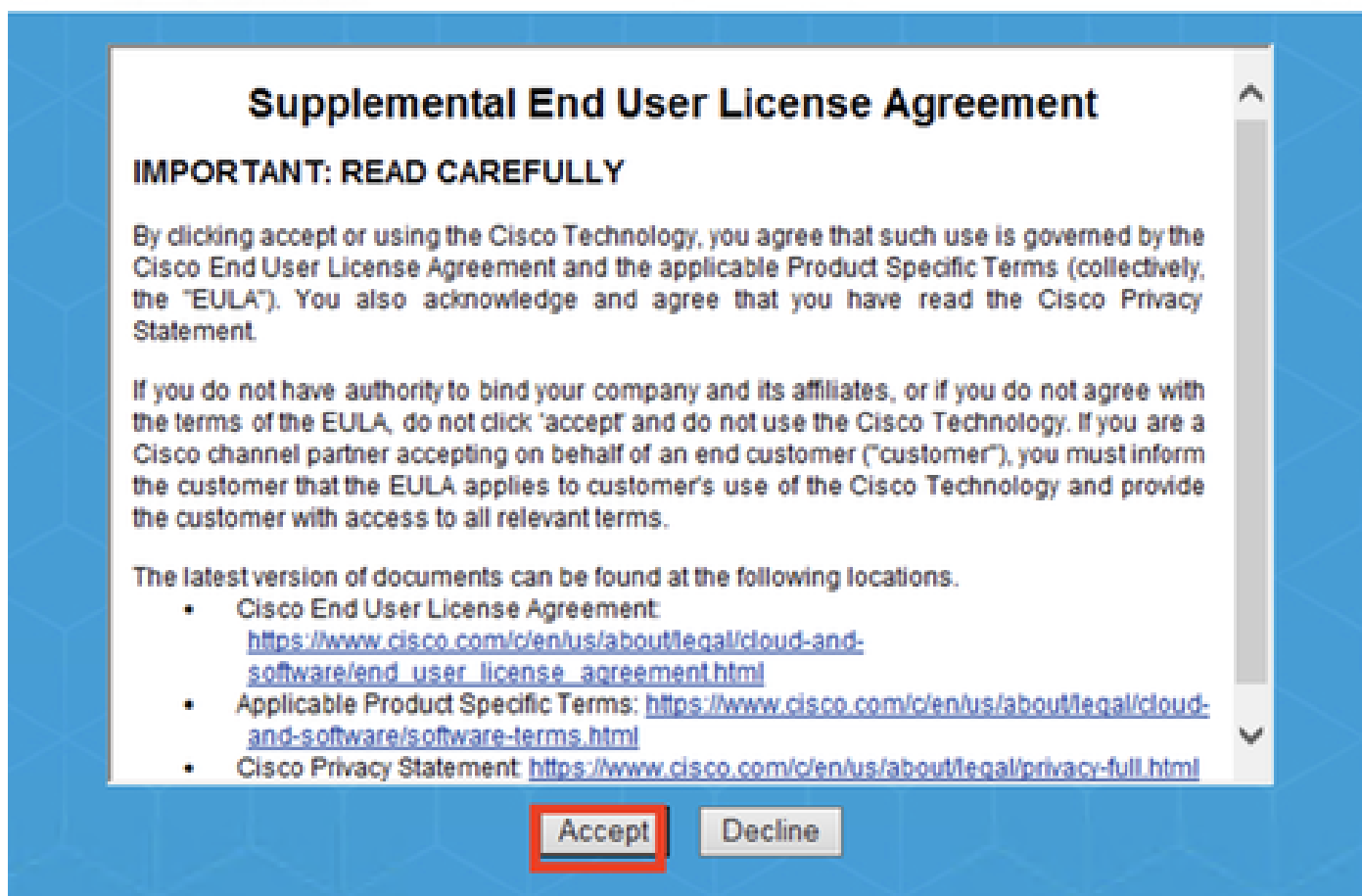
☐ Lock Down Component Services

**Install Selected**

*Install Selector*

Click **Install Selected**.

Accept the EULA.



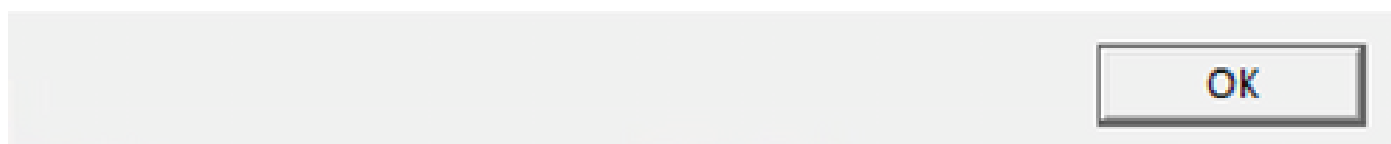
EULA Window

A restart is required after NAM installation.

## Cisco Secure Client Install Selector

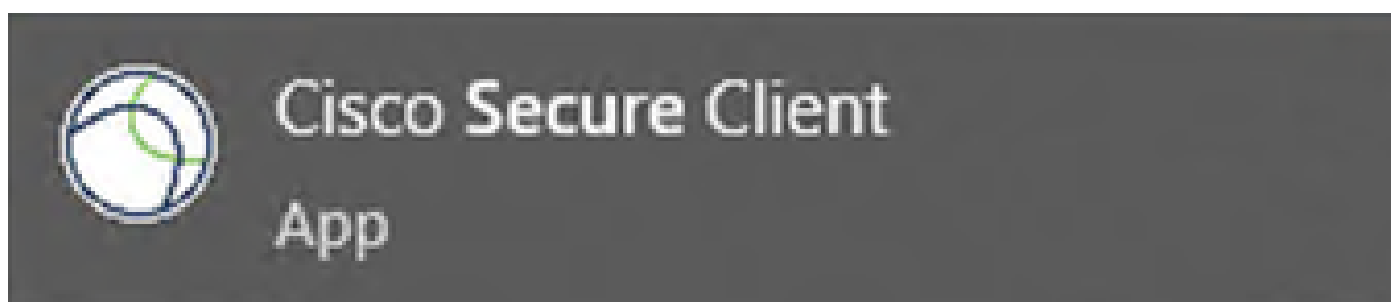


**You must reboot your system for the installed changes to take effect.**



Reboot Requirement Window

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

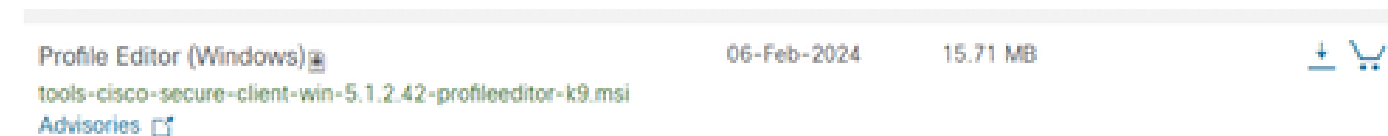


## 2. Download and Install Secure Client NAM Profile Editor.

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

Once it downloaded, proceed with the installation.

Run the msi file.



Profile Editor Setup Window

Use the **Typical** setup option.



**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**

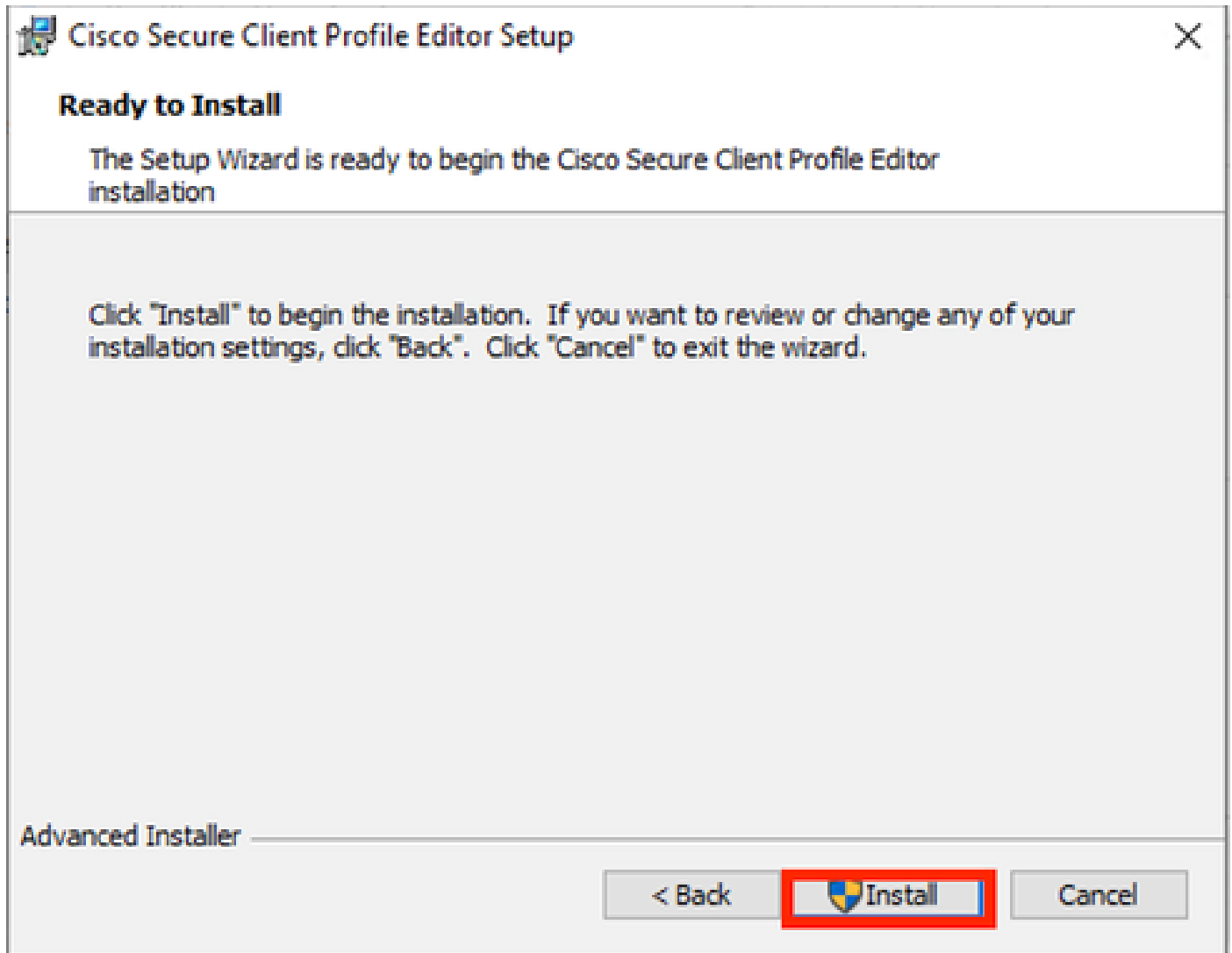
All program features will be installed. (Requires most disk space)

Advanced Installer

< Back

Next >

Cancel



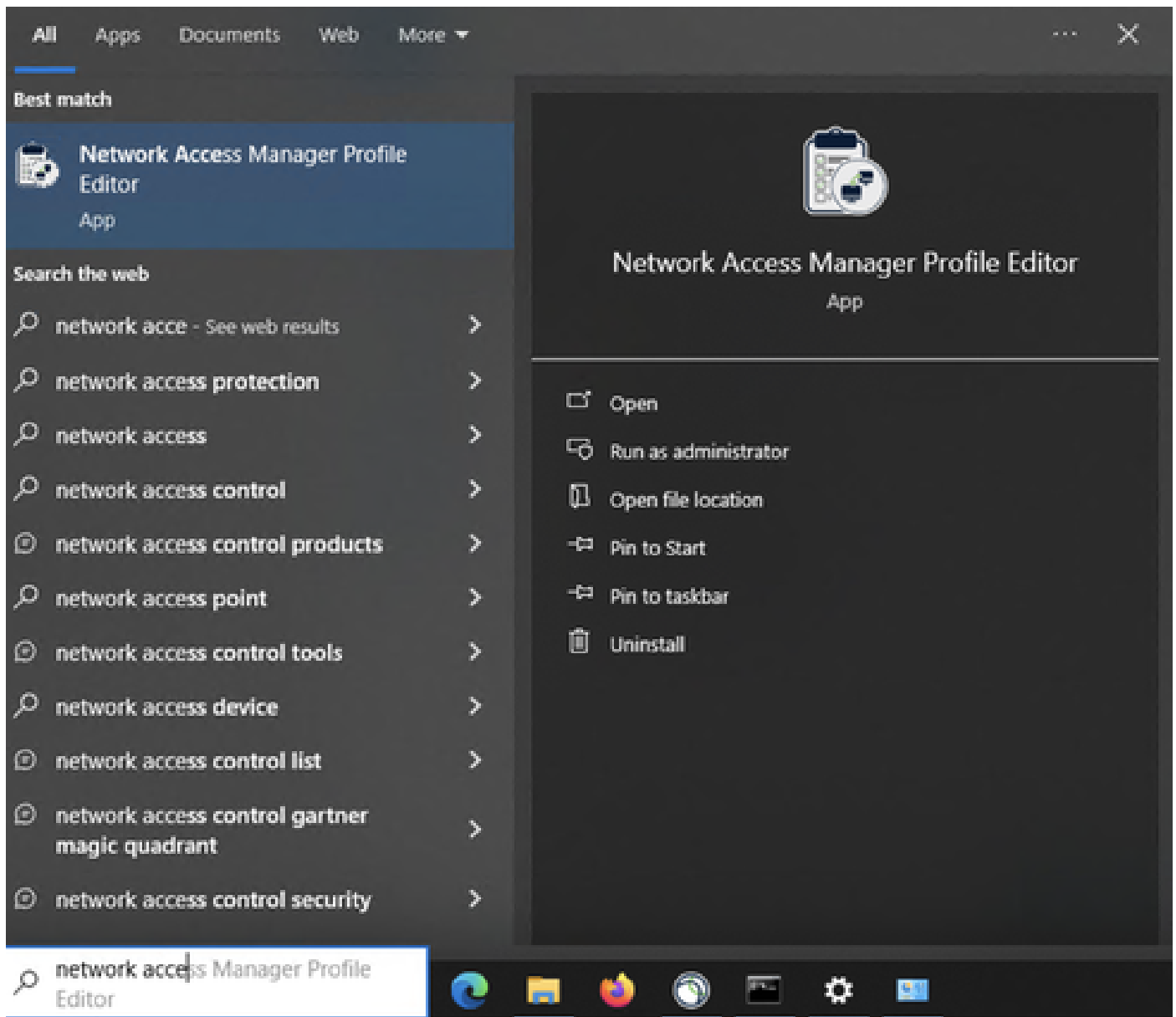
*Installation Window*

Click **Finish**.



*End of Profile Editor Setup*

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



*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

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

☒ 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

Network Access Manager

- Client Policy
- Authentication Policy**
- Networks
- Network Groups

## Authentication Policy

Profile: Untitled

Allow Association Modes

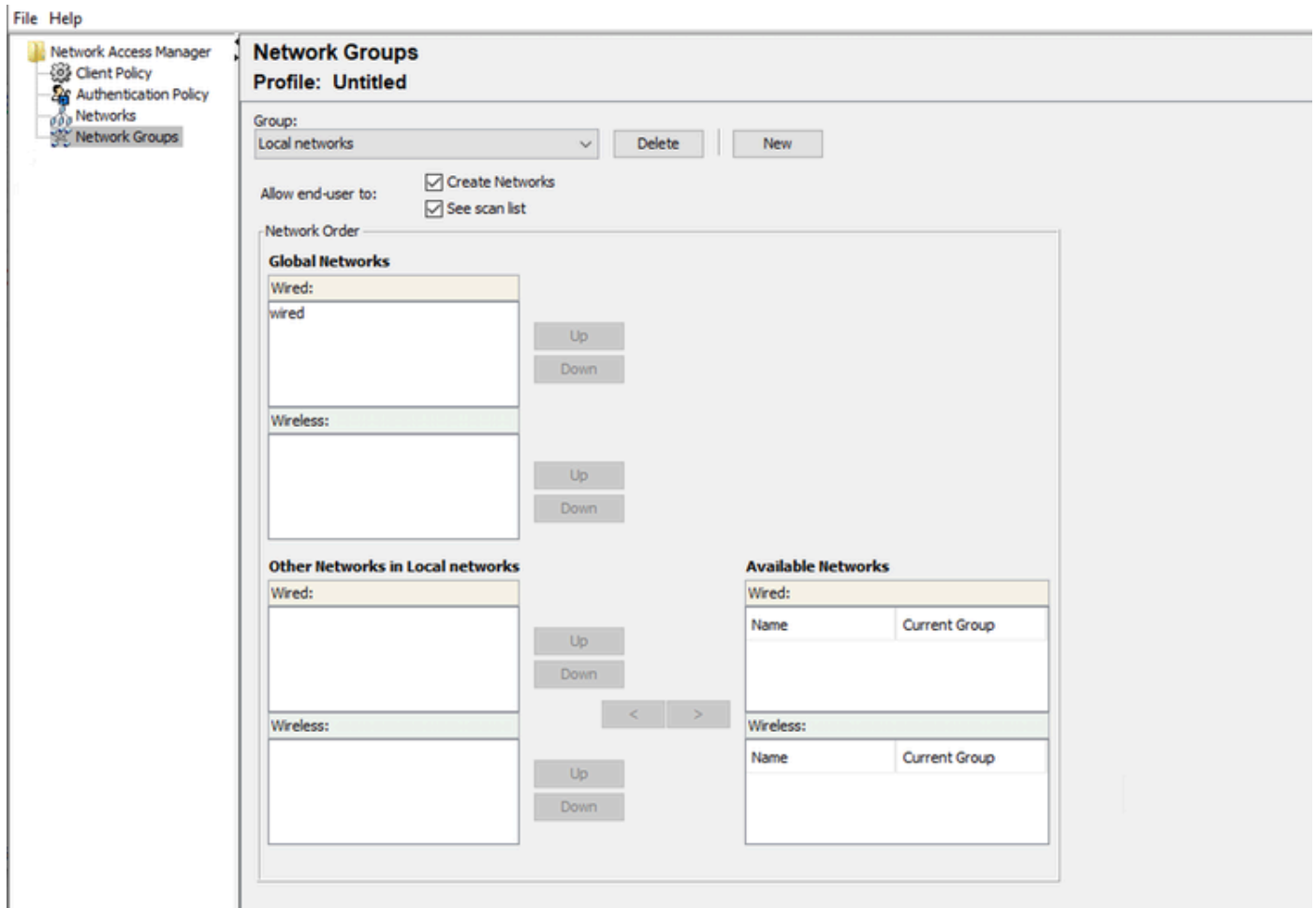
- ☒ Select All (Personal)
  - ☒ Open (no encryption)
  - ☒ Open (Static WEP)
  - ☒ Shared (WEP)
  - ☒ WPA Personal TKIP
  - ☒ WPA Personal AES
  - ☒ WPA2 Personal TKIP
  - ☒ WPA2 Personal AES
  - ☒ WPA3 Open (OWE)
  - ☒ WPA3 Personal AES (SAE)
- ☒ Select All (Enterprise)
  - ☒ Open (Dynamic (802.1X)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



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*

Add...

Edit...

Delete

\* 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: <input type="text" value="PEAP MSCHAPv2"/>		Media Type
Group Membership		Security Level
<input type="radio"/> In group: <input type="text" value="Local networks"/>		
<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"/>		

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.

**Media Type**  
**Security Level**  
Connection Type

**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

Next Cancel

Network Profile Security Level

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

The screenshot shows the 'Networks' section of the Cisco Secure Client Profile Editor. The 'Profile: Untitled' is being edited. The 'Network Connection Type' section has three options: 'Machine Connection', 'User Connection' (selected), and 'Machine and User Connection'. The 'User Connection' option is highlighted with a red box. To the right, a table lists the configuration options for the selected connection type.

Media Type
Security Level
Connection Type
User Auth
Credentials

Next Cancel

*Network 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**.

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

☐ 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

Network 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.



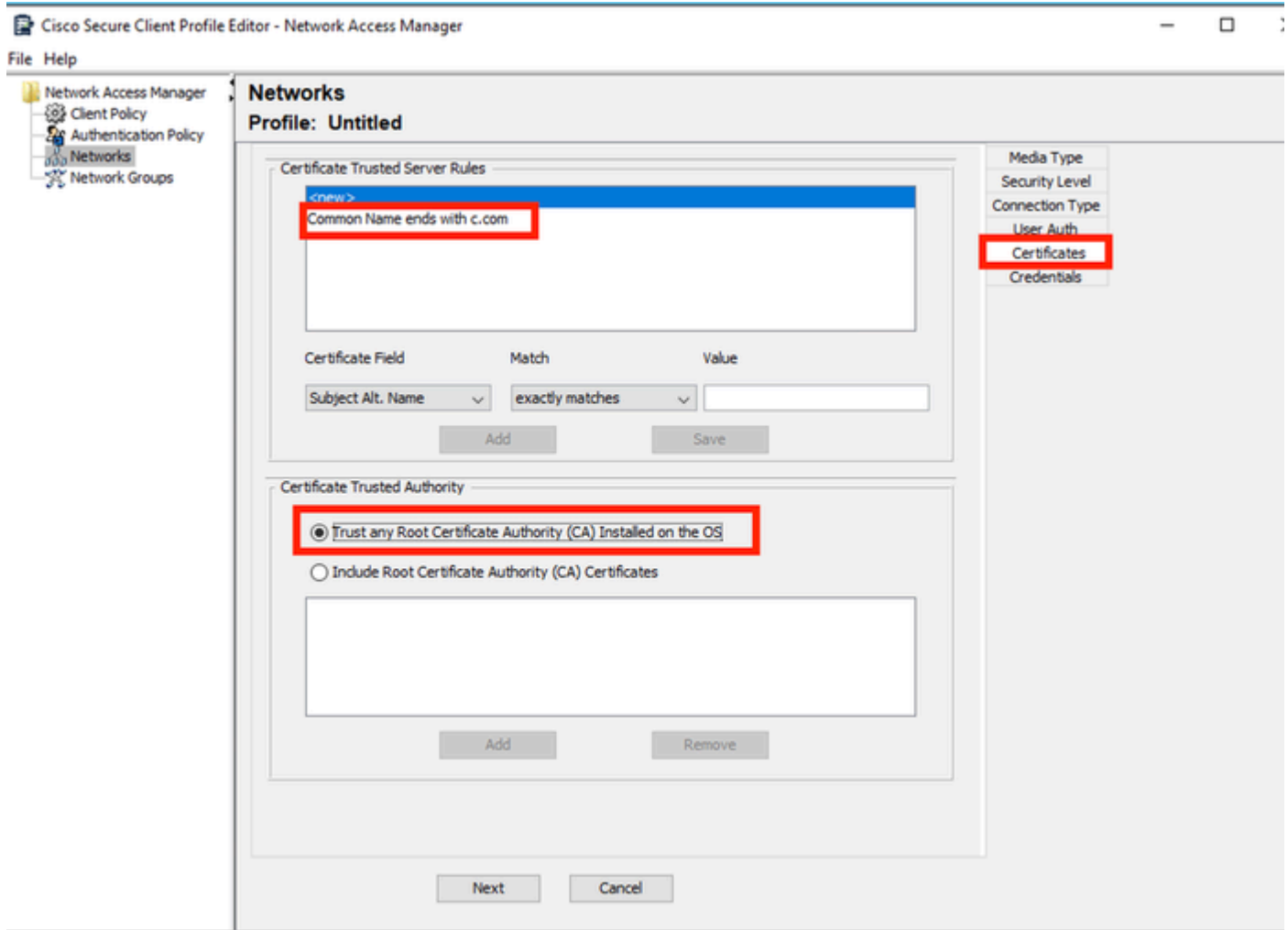
**Note:** The **Certificate** section is displayed because the option **Validate Server Identity** in **EAP-PEAP Settings** is selected. For EAP PEAP, it does the encapsulation using the server certificate.

---

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**.

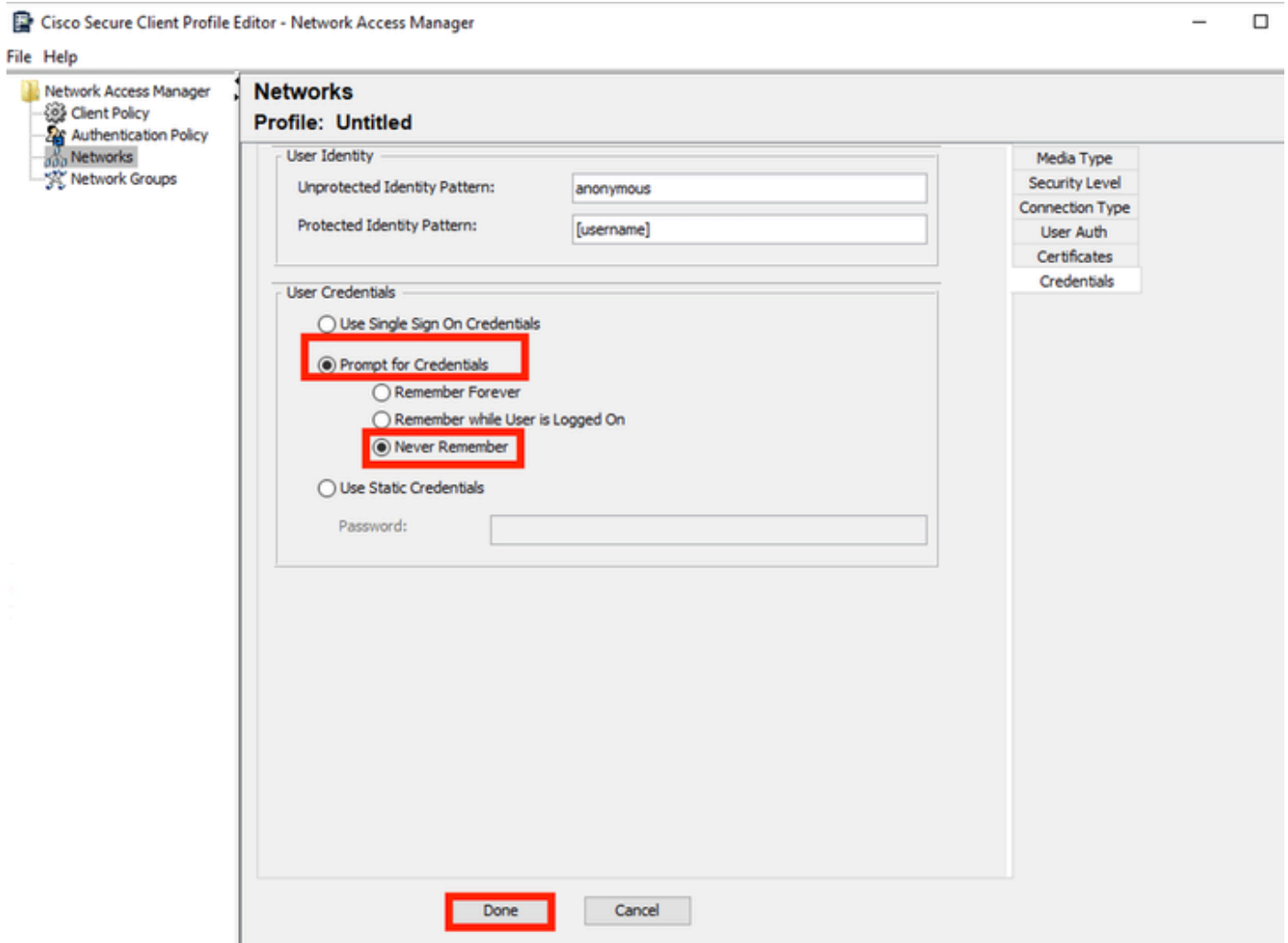


#### Network Profile Certificate Section

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**.



#### Network Profile Credentials Section

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

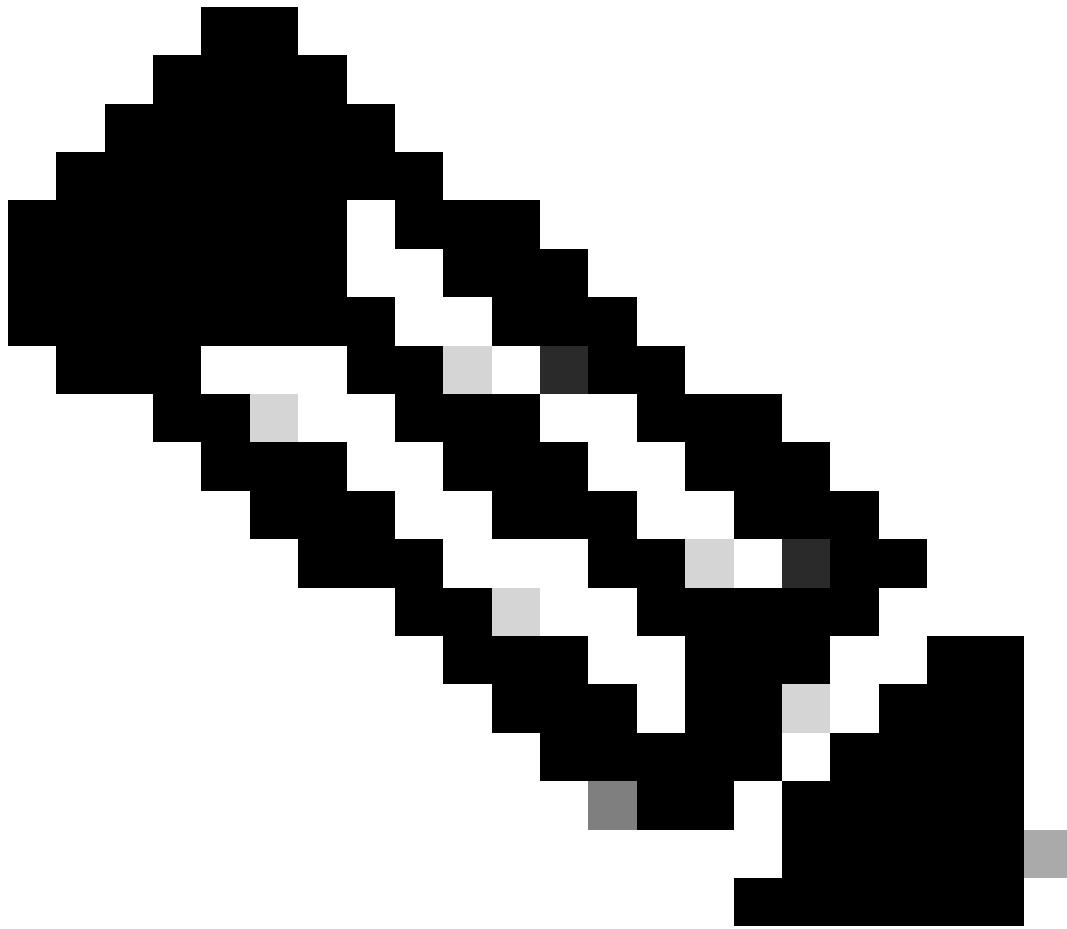
The option **Prompt for Credentials > Never Remember** is selected, so in each authentication, the user making the authentication must enter their credentials.

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 Manager use the profile that was just created, replace the configuration.xml file in the next directory with the new one:

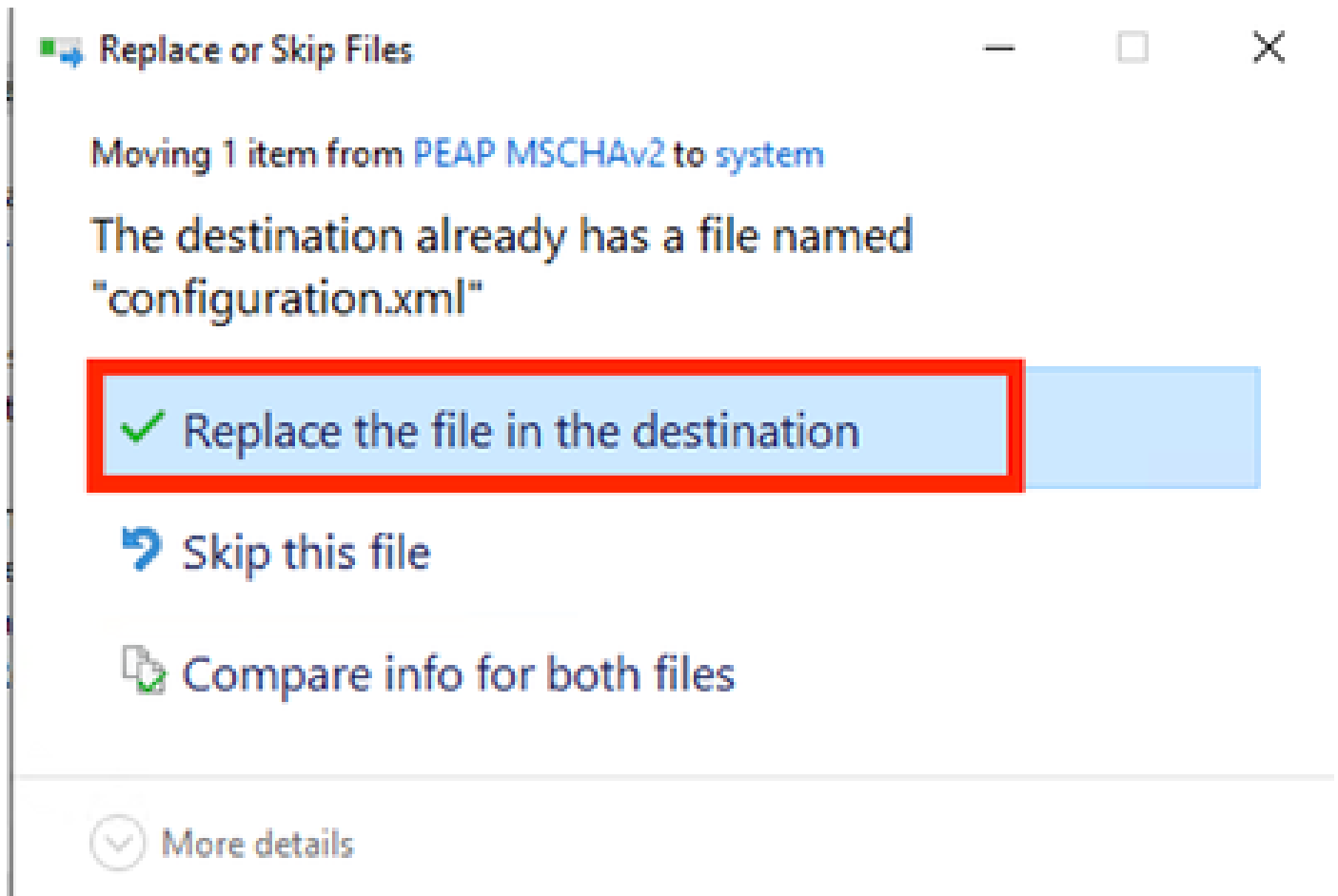
C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system



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

---





*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*

Add...

Edit...

Delete

\* 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.

Cisco Secure Client Profile Editor - Network Access Manager

File Help

Network Access Manager  
Client Policy  
Authentication Policy  
Networks  
Network Groups

## 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.

**Browse Local Machine**

Connection Timeout: 40 seconds

Media Type  
Security Level

Next Cancel

Media Type Section

Click **Next**.

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

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.)	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

**Media Type**  
Security Level  
Connection Type

**Next** **Cancel**

*Security Level Profile Editor Section*

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

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.

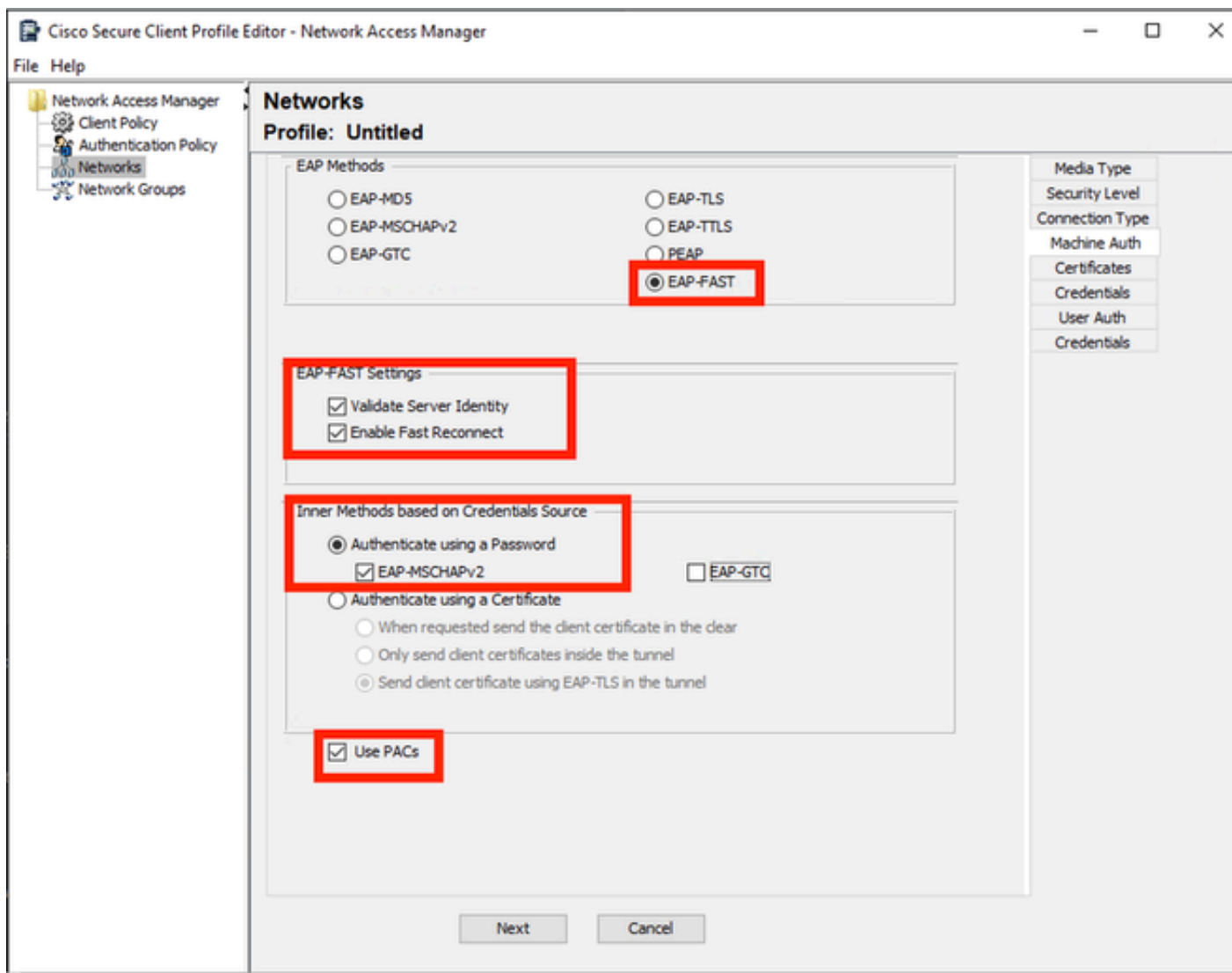
Media Type  
Security Level  
**Connection Type**  
Machine Auth  
Credentials  
User Auth  
Credentials

Next Cancel

*Connection Type Section*

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

Click **Next**.



#### 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	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

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

File Help

Network Access Manager  
Client Policy  
Authentication Policy  
Networks  
Network Groups

## Networks

Profile: Untitled

Machine Identity

Unprotected Identity Pattern:

Protected Identity Pattern:

Machine Credentials

☒ Use Machine Credentials

☐ Use Static Credentials

Password:

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

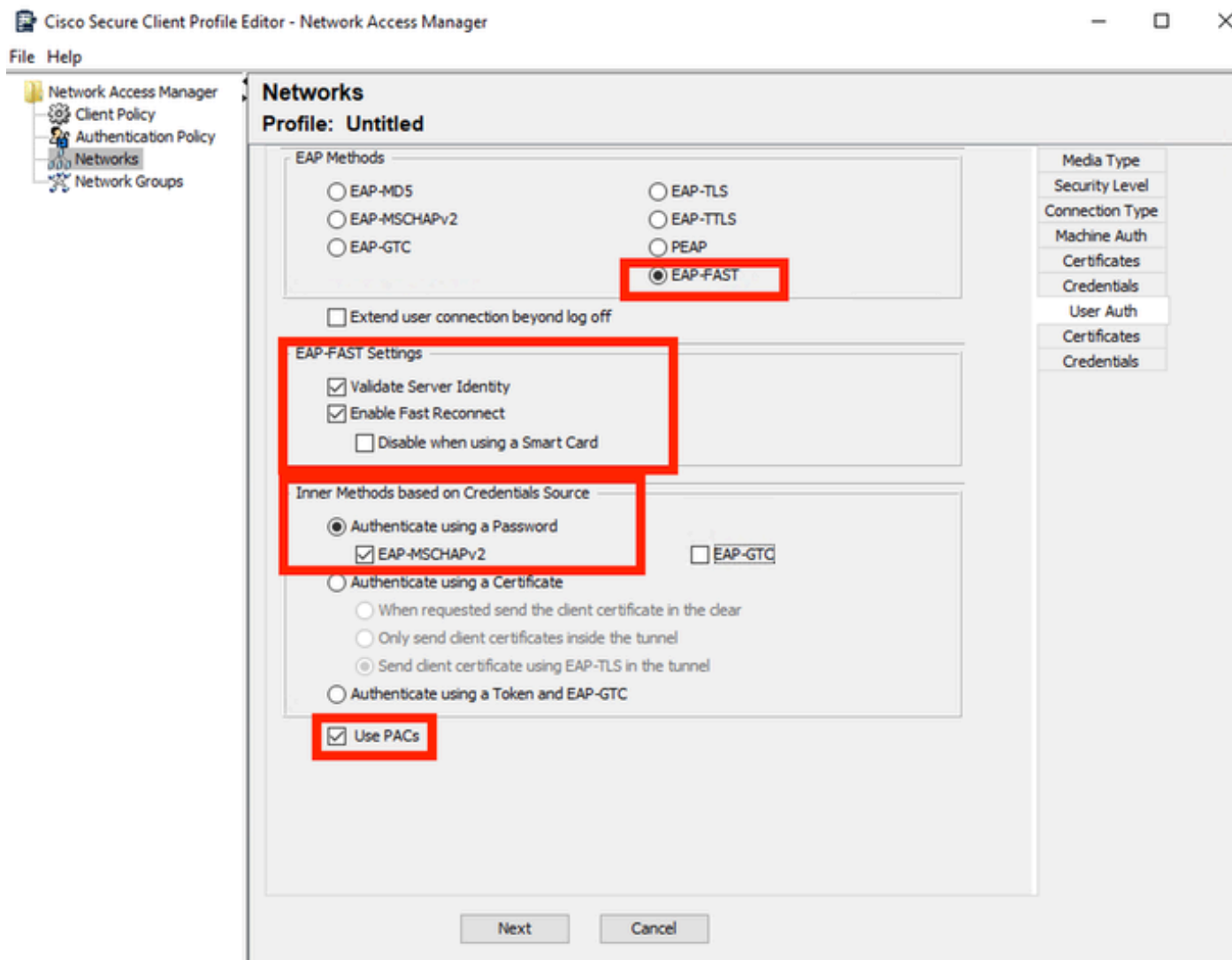
Next Cancel

*Machine Auth Credentials Section*

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

Click **Next**.





#### 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.

## Networks

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

The screenshot displays the 'User Auth Server Certificate Trust' configuration window. The window is divided into two main sections: 'Certificate Trusted Server Rules' and 'Certificate Trusted Authority'. On the right side, there is a vertical menu with several tabs: 'Media Type', 'Security Level', 'Connection Type', 'Machine Auth', 'Certificates', 'Credentials', 'User Auth', and 'Certificates' (highlighted with a red box). Below the 'Certificate Trusted Server Rules' section, there is a table with columns 'Certificate Field', 'Match', and 'Value'. The first row shows 'Common Name' in the 'Certificate Field' column, 'ends with' in the 'Match' column, and 'c.com' in the 'Value' column. Below this table are 'Remove' and 'Save' buttons. The 'Certificate Trusted Authority' section contains two radio button options: 'Trust any Root Certificate Authority (CA) Installed on the OS' (selected) and 'Include Root Certificate Authority (CA) Certificates'. Below these options is a large empty rectangular box, and at the bottom are 'Add' and 'Remove' buttons. At the very bottom of the window are 'Next' and 'Cancel' buttons.

Certificate Field	Match	Value
Common Name	ends with	c.com

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:

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
Certificates
Certificates

Done Cancel

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*
------	------------	--------

Add...

Edit...

Delete

\* 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:

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

Media Type  
Security Level

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.

Cisco Secure Client Profile Editor - Network Access Manager

File Help

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

## 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

Security Level

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

Cisco Secure Client Profile Editor - Network Access Manager

File Help

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

## 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

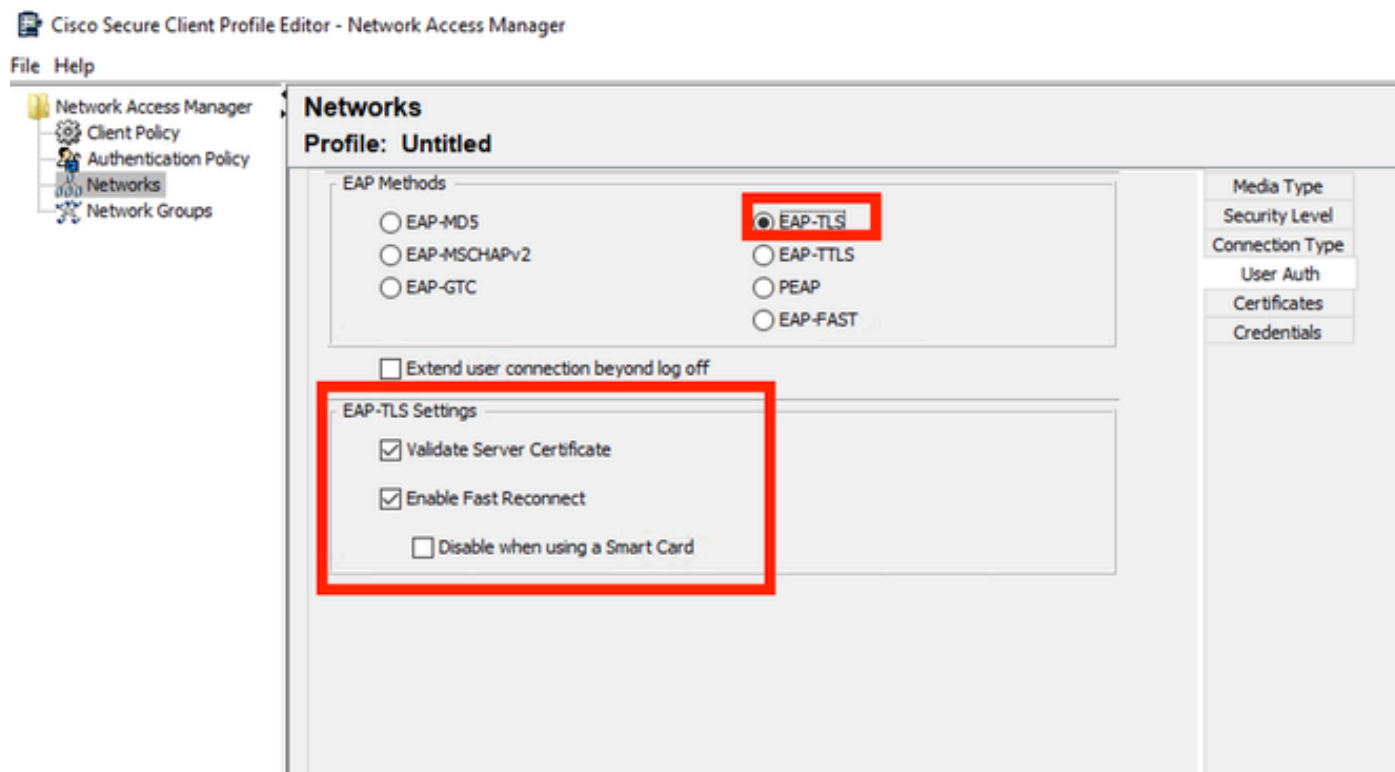
Security Level

Connection Type

User Auth

Credentials

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



**Networks**  
Profile: Untitled

Network Access Manager  
Client Policy  
Authentication Policy  
Networks  
Network Groups

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

**Certificate Trusted Server Rules**

Common Name ends with c.com

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

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

*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

Add

Edit

Delete

Done

Cancel

Media Type

Security Level

Connection Type

User Auth

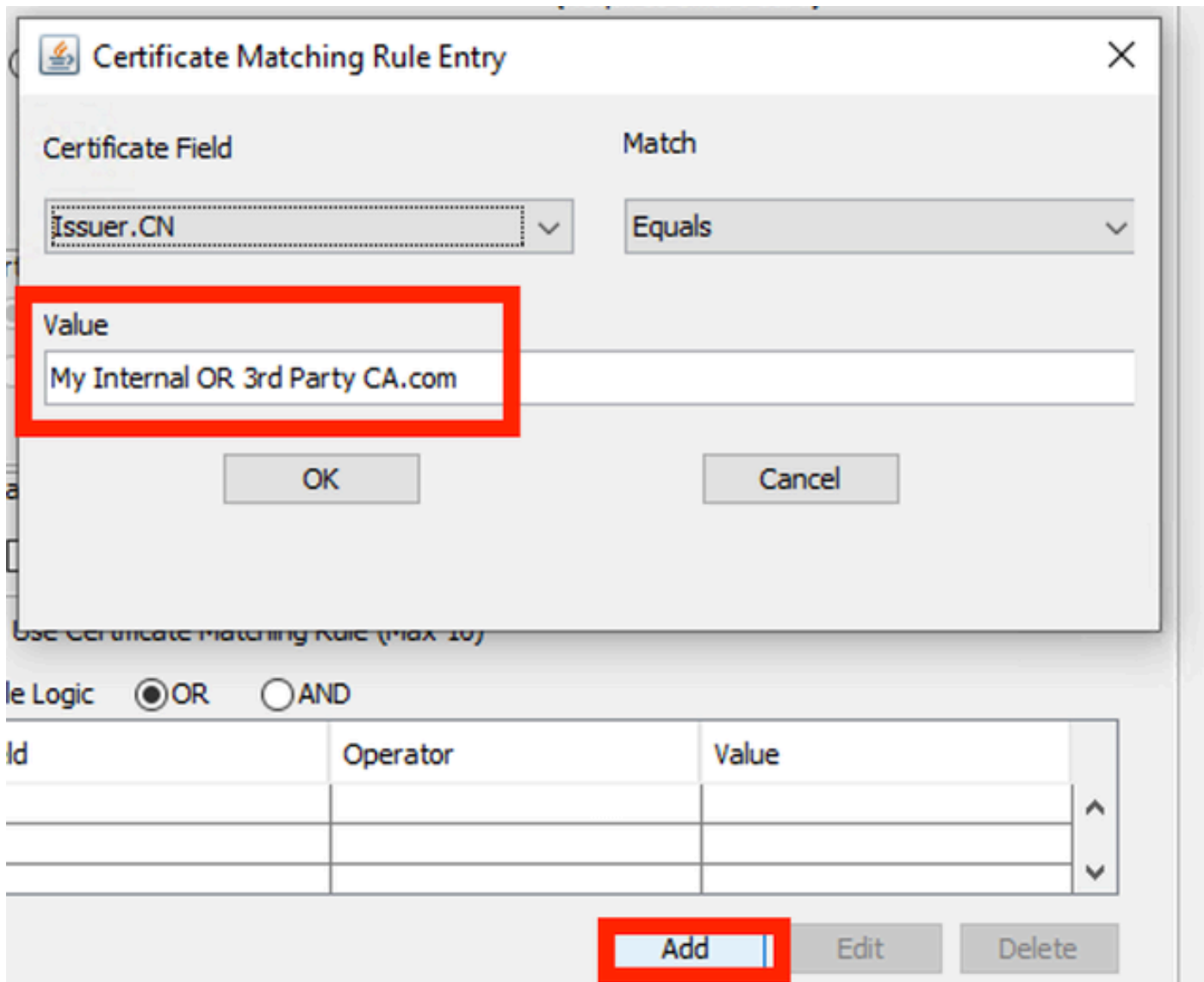
Certificates

Credentials

#### 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 Matching Rule (Max 10)**.

Click **Add**.

The image shows a 'Certificate Matching Rule Entry' dialog box. It has a title bar with a close button. Inside, there are two dropdown menus: 'Certificate Field' and 'Match'. The 'Certificate Field' dropdown is set to 'Issuer.CN'. The 'Match' dropdown is set to 'Equals'. Below these is a 'Value' label and a text input field containing the string 'My Internal OR 3rd Party CA.com'. At the bottom of the dialog are 'OK' and 'Cancel' buttons. Below the dialog, there is a section for 'Use Certificate Matching Rule (Max 10)' with radio buttons for 'OR' (selected) and 'AND'. Below this is a table with three columns: 'Id', 'Operator', and 'Value'. The table is currently empty. At the bottom right of the table are three buttons: 'Add', 'Edit', and 'Delete'. The 'Add' button is highlighted with a red box.

**Certificate Matching Rule Entry**

Certificate Field: Issuer.CN

Match: Equals

Value: My Internal OR 3rd Party CA.com

OK Cancel

Use Certificate Matching Rule (Max 10)

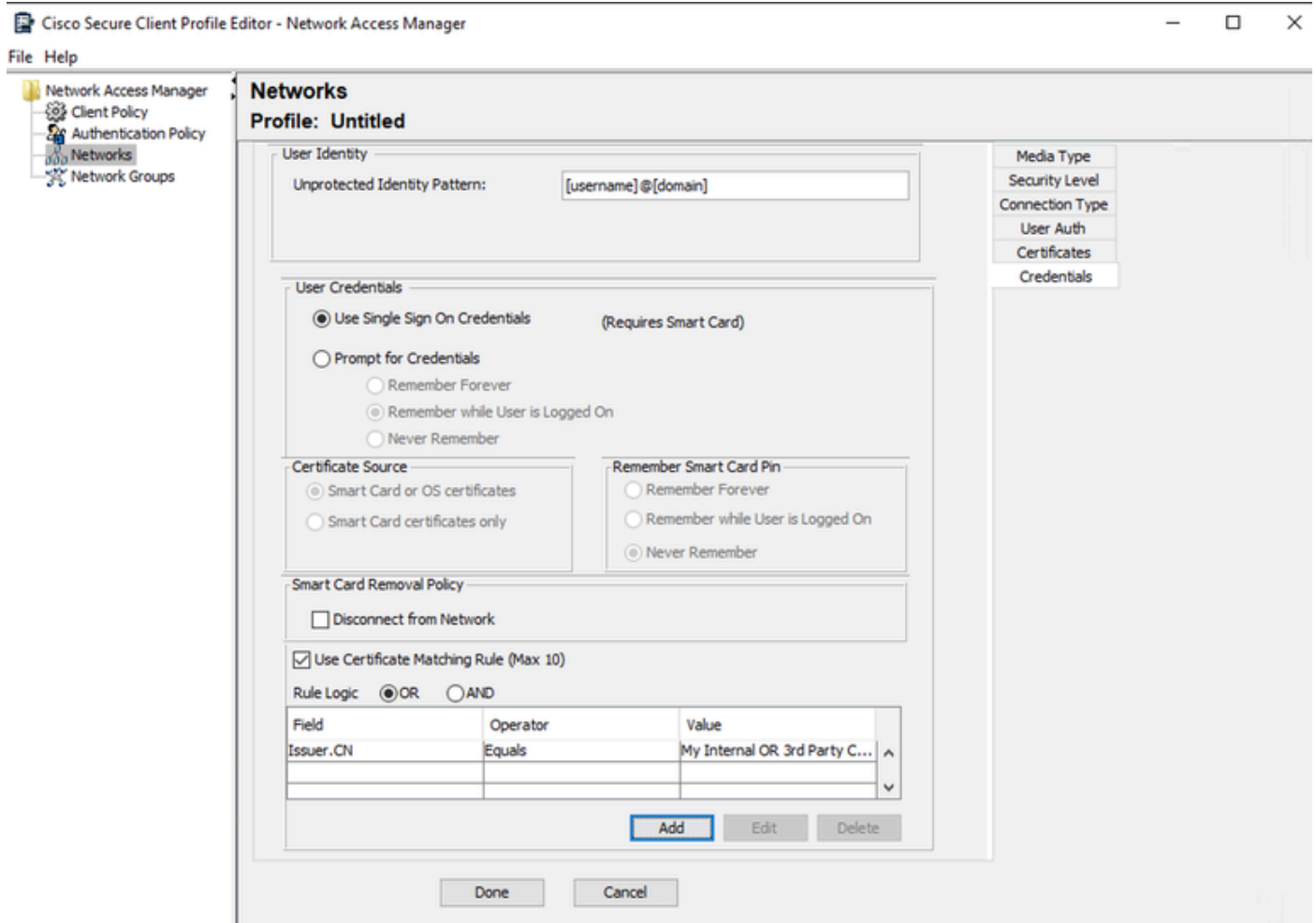
le Logic: ☒ OR ☐ AND

Id	Operator	Value

Add Edit Delete

Certificate Matching Rule Window

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



*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

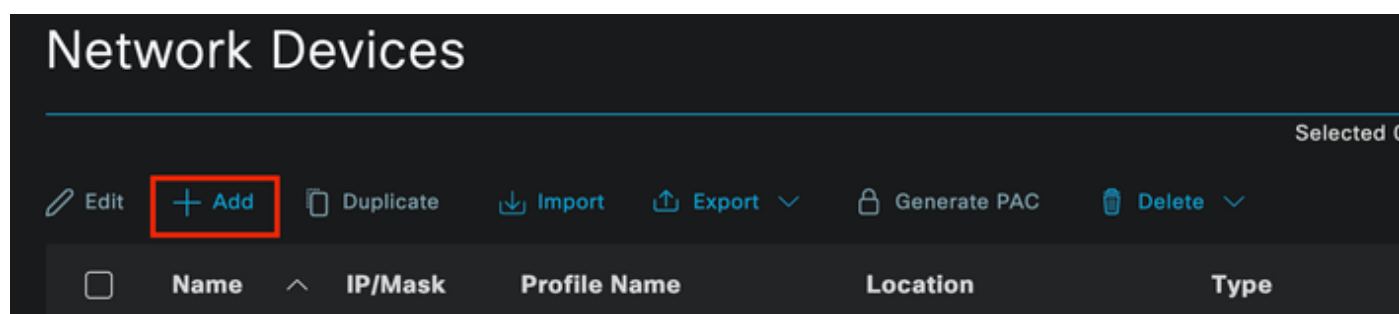
```

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.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Cisco ISE', 'Administration · Network Resources', and a status indicator 'Evaluation Mode 29 Days'. The main menu on the left lists 'Network Devices', 'Default Device', and 'Device Security Settings'. The breadcrumb trail indicates 'Network Devices List > ISR1100'. The 'Network Devices' configuration form is displayed with the following fields:

- Name:** ISR1100
- Description:** (empty)
- IP Address:** A dropdown menu is open, showing 'A.B.C.D' as the selected option. The field is highlighted with a red box.
- Device Profile:** Cisco
- Model Name:** (empty)
- Software Version:** (empty)
- Network Device Group:** (empty)

Network Device Creation

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

The screenshot shows the 'RADIUS Authentication Settings' configuration page. The 'RADIUS UDP Settings' section is expanded, showing the following configuration:

- Protocol:** RADIUS
- Shared Secret:** (masked with dots) [Show](#)
- ☐ **Use Second Shared Secret** ⓘ
- Second Shared Secret:** (empty) [Show](#)
- CoA Port:** 1700 [Set To Default](#)

Network Device Radius Settings

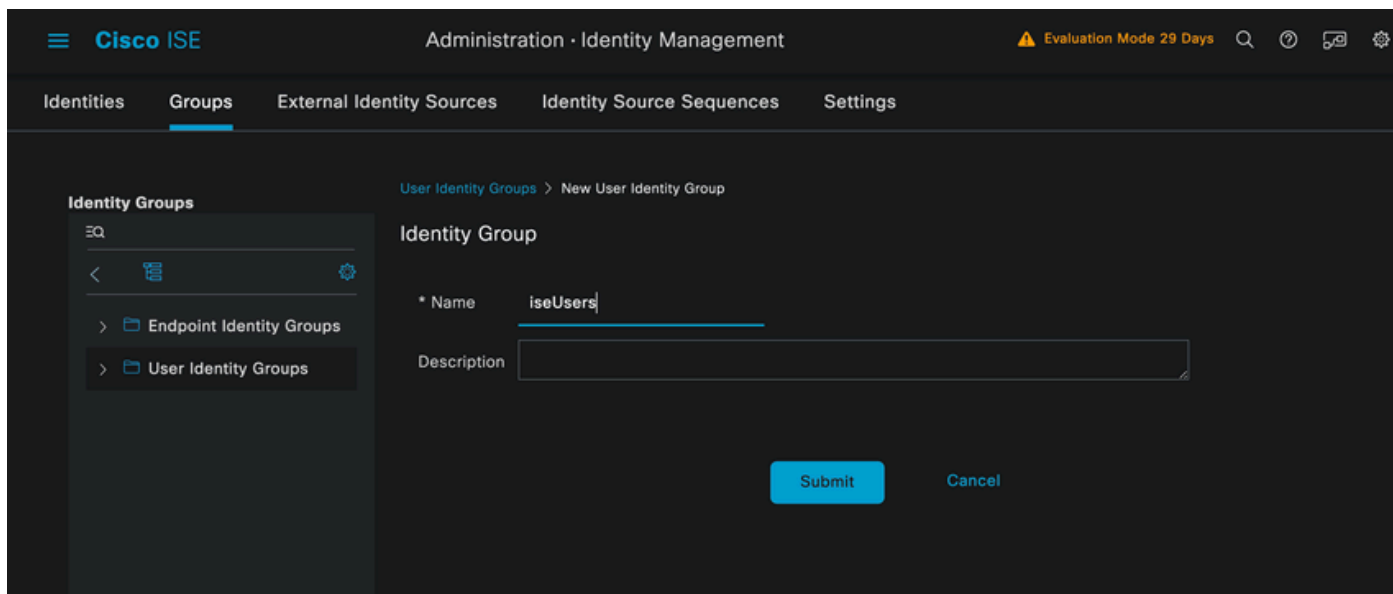
Save the changes.

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**.



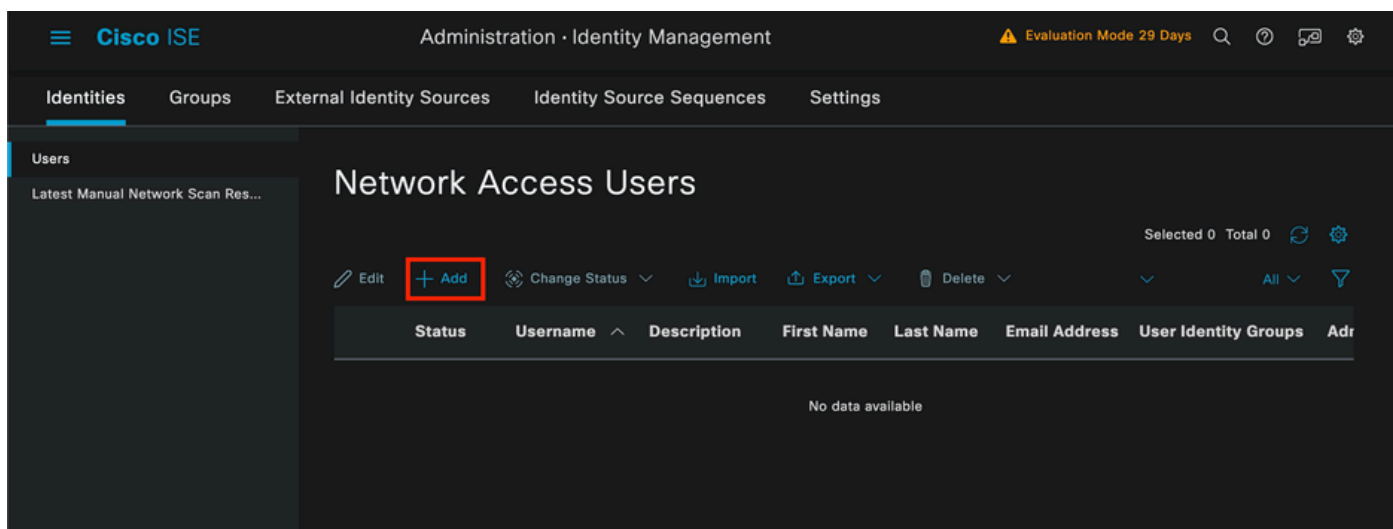
The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE', 'Administration · Identity Management', and a status indicator 'Evaluation Mode 29 Days'. The main navigation tabs are 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'Groups' tab is selected. On the left, the 'Identity Groups' sidebar shows a tree structure with 'Endpoint Identity Groups' and 'User Identity Groups'. The main content area is titled 'User Identity Groups > New User Identity Group'. It contains a form for creating a new identity group. The 'Name' field is labeled '\* Name' and contains the text 'iseUsers'. The 'Description' field is labeled 'Description' and is empty. At the bottom right of the form are two buttons: 'Submit' and 'Cancel'.

*Identity Group Creation*

Click **Submit**.

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

Click **Add**.



The screenshot shows the Cisco ISE Administration console. The top navigation bar is the same as the previous image. The main navigation tabs are 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'Identities' tab is selected. On the left, the 'Users' sidebar shows a tree structure with 'Latest Manual Network Scan Res...'. The main content area is titled 'Network Access Users'. It contains a table with columns: 'Status', 'Username', 'Description', 'First Name', 'Last Name', 'Email Address', 'User Identity Groups', and 'Ad'. Above the table, there are several action buttons: 'Edit', 'Add' (highlighted with a red box), 'Change Status', 'Import', 'Export', and 'Delete'. The 'Add' button is a blue button with a plus sign. Below the table, it says 'No data available'.

*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 User

\* Username

Status ☒ Enabled ▼

Account Name Alias  ⓘ

Email

Network Access User Creation

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

## 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](#) ⓘ

User Creation Password Section

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

## User Groups



▼



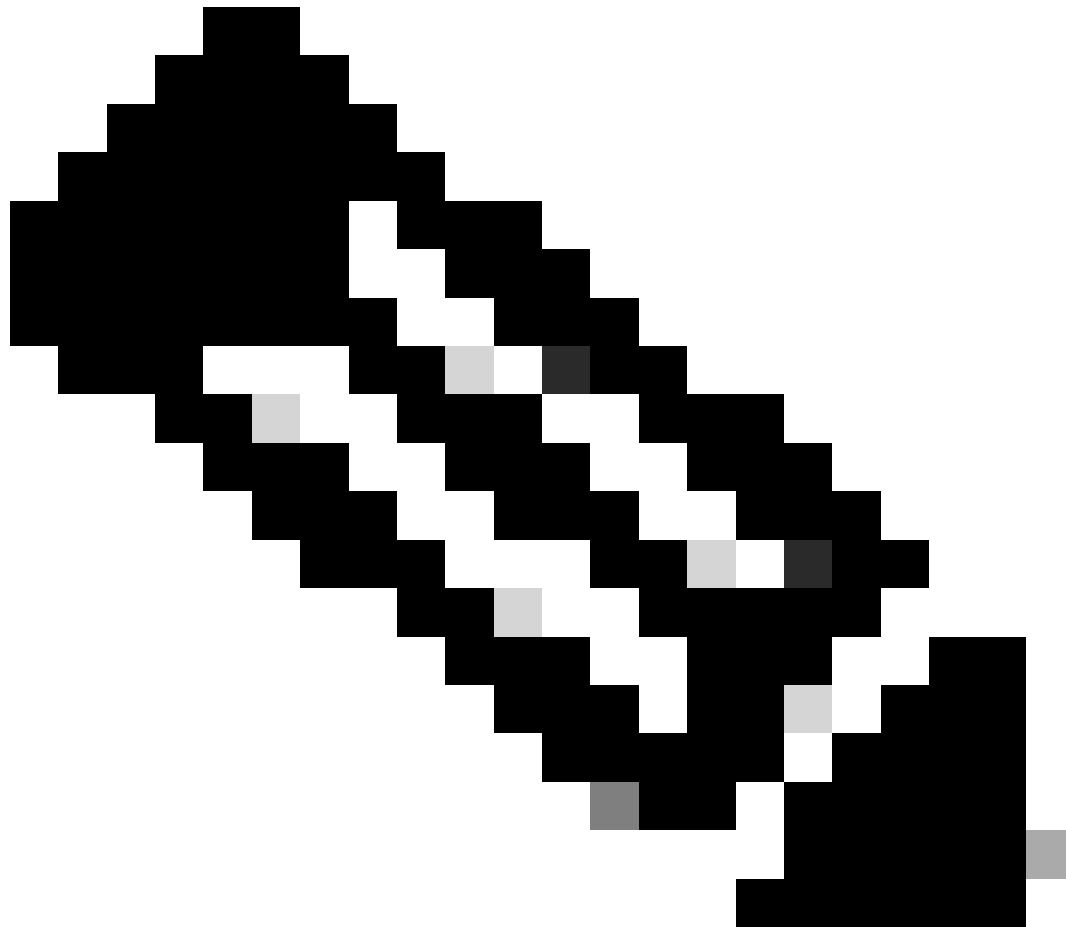
User Group Assignment

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.

---

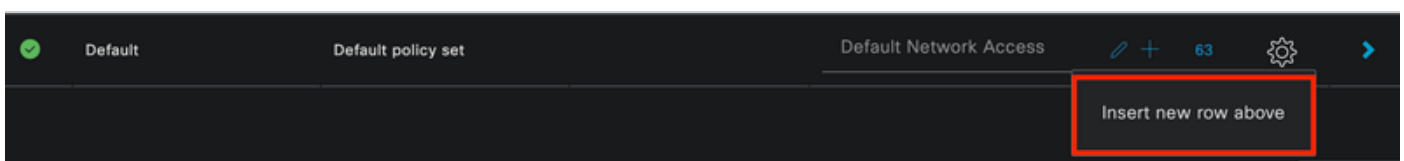


**Note:** Classifying and differentiating the policy sets helps when troubleshooting,

---

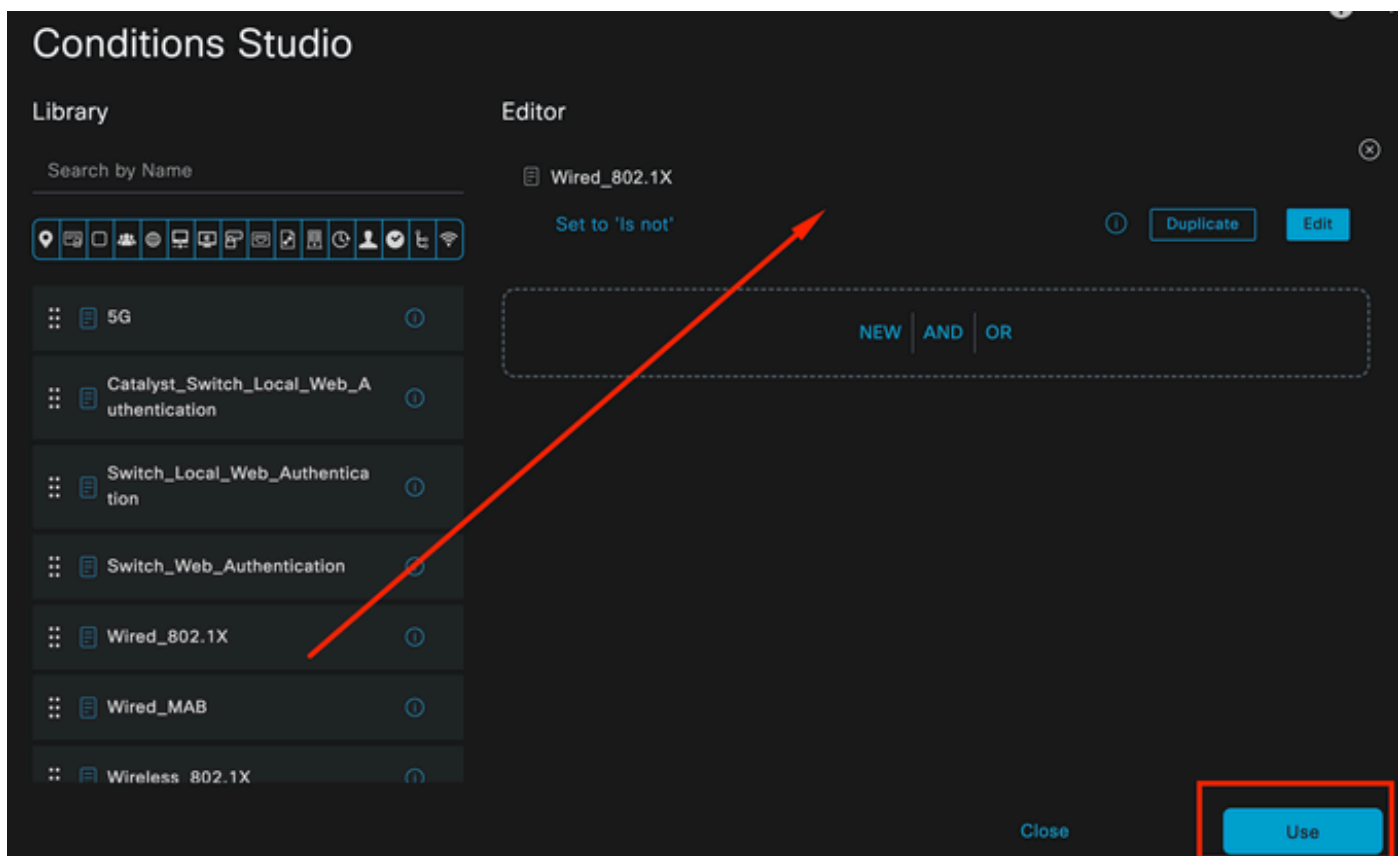


**Note:** If the add or plus icon is not visible, the gear icon of any policy set can be clicked, and then select **Insert new row above**.



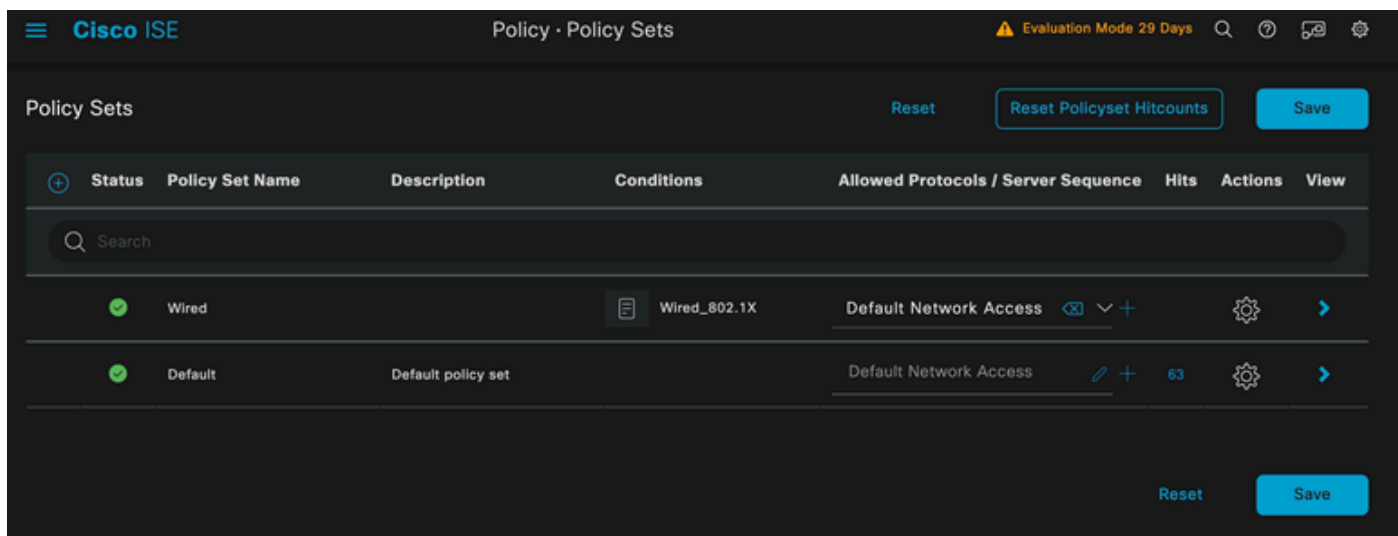
*Gear Icon Options*

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.

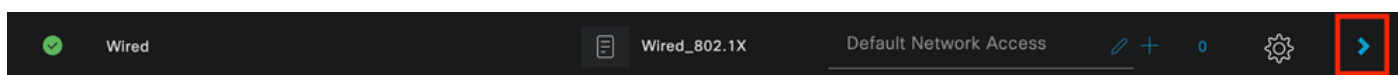


Policy Sets General View

Click **Save**.

2.d. Configure the Authentication and Authorization Policies.

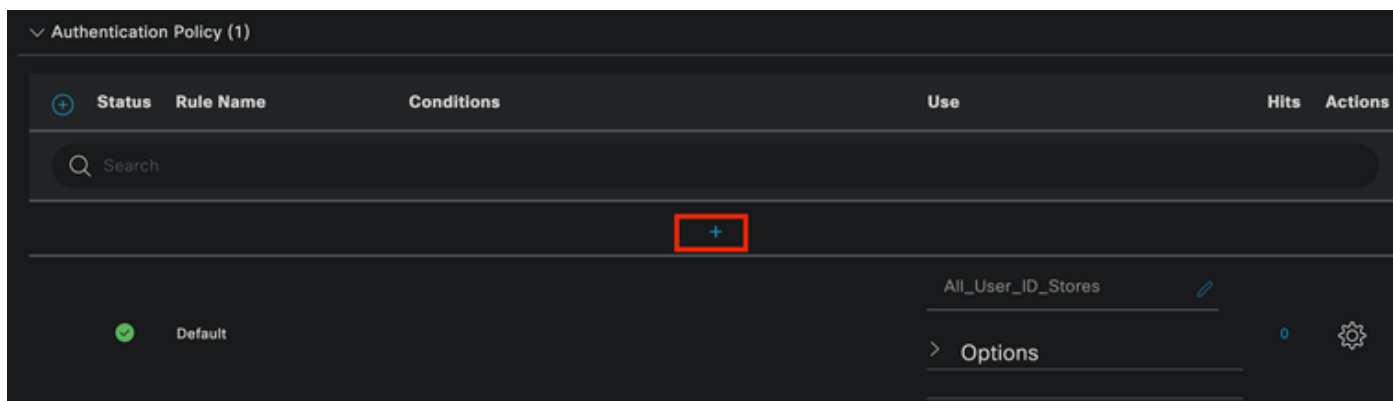
Click the > icon.



Wired Policy Set

Expand the **Authentication Policy** section.

Click on the + icon.



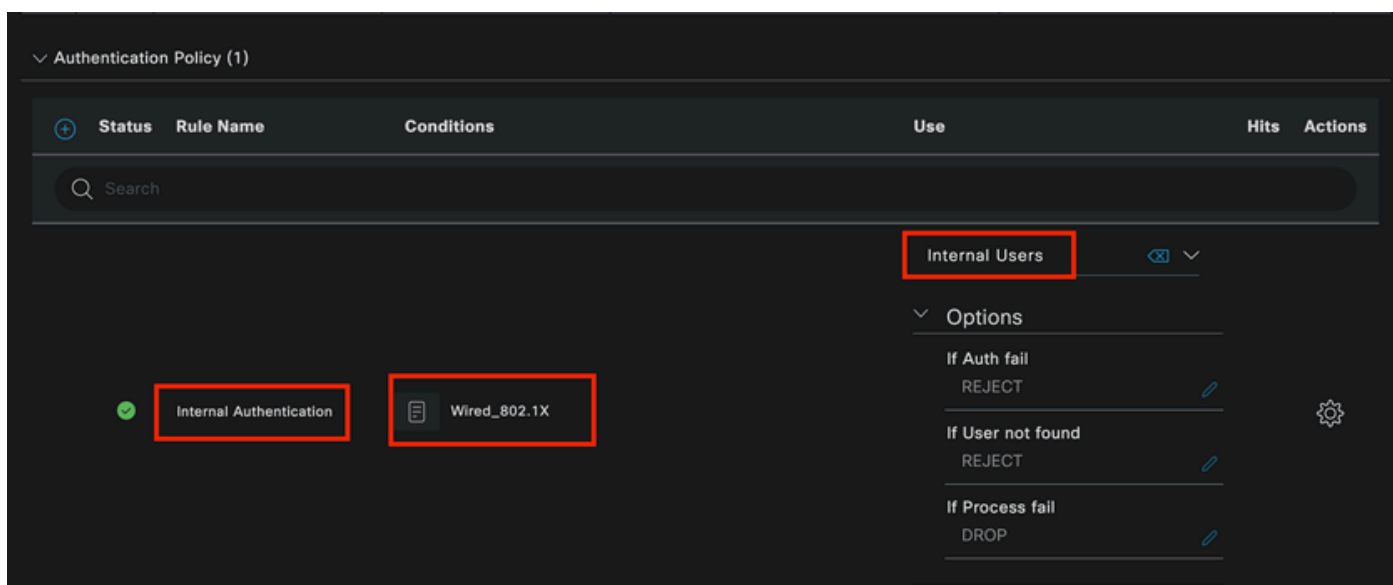
*Authentication Policy*

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.

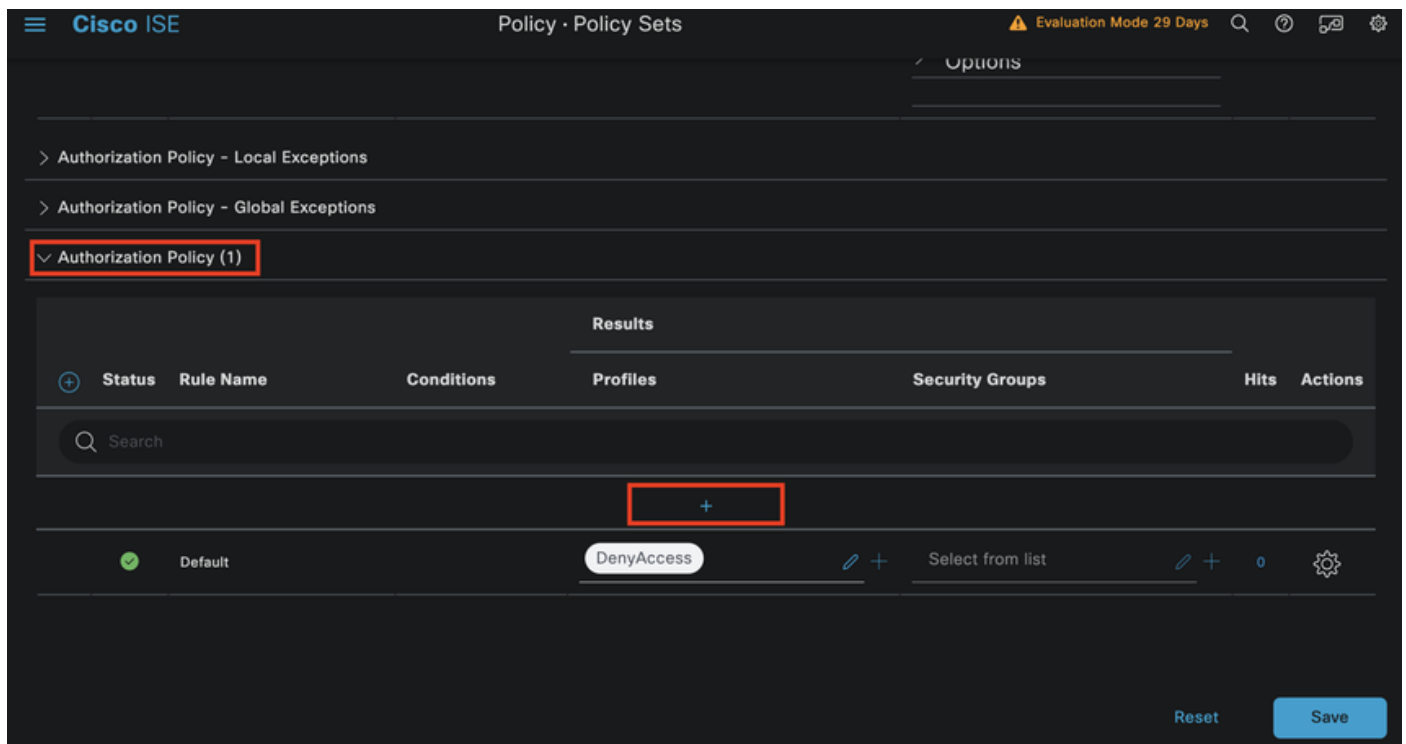
Finally, in the **Use** column select **Internal Users**.



*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.

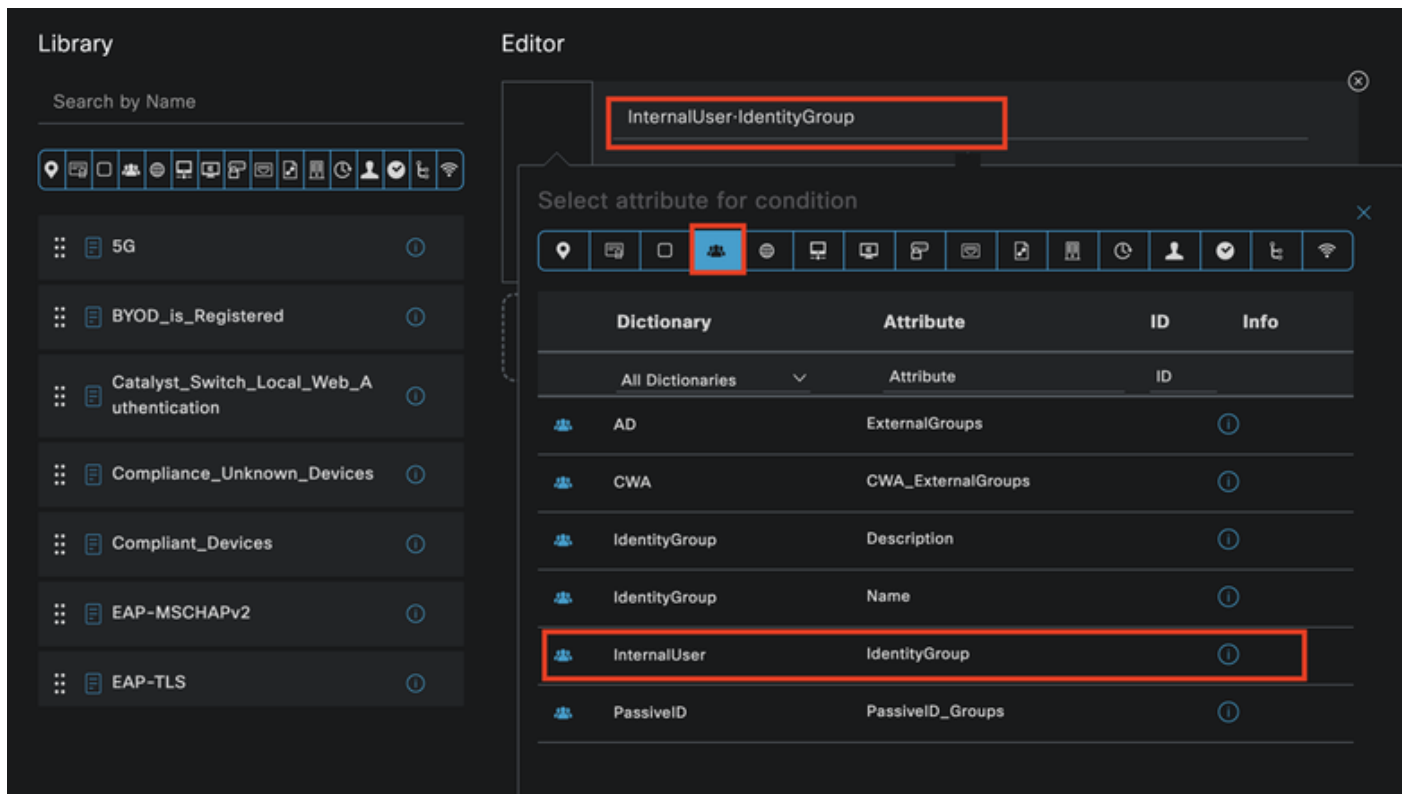
To create a condition for this **Authorization Policy**, click the + icon in the **Conditions** column.

The group **IseUsers** is used.

Click the **Attribute** section.

Select the **IdentityGroup** icon.

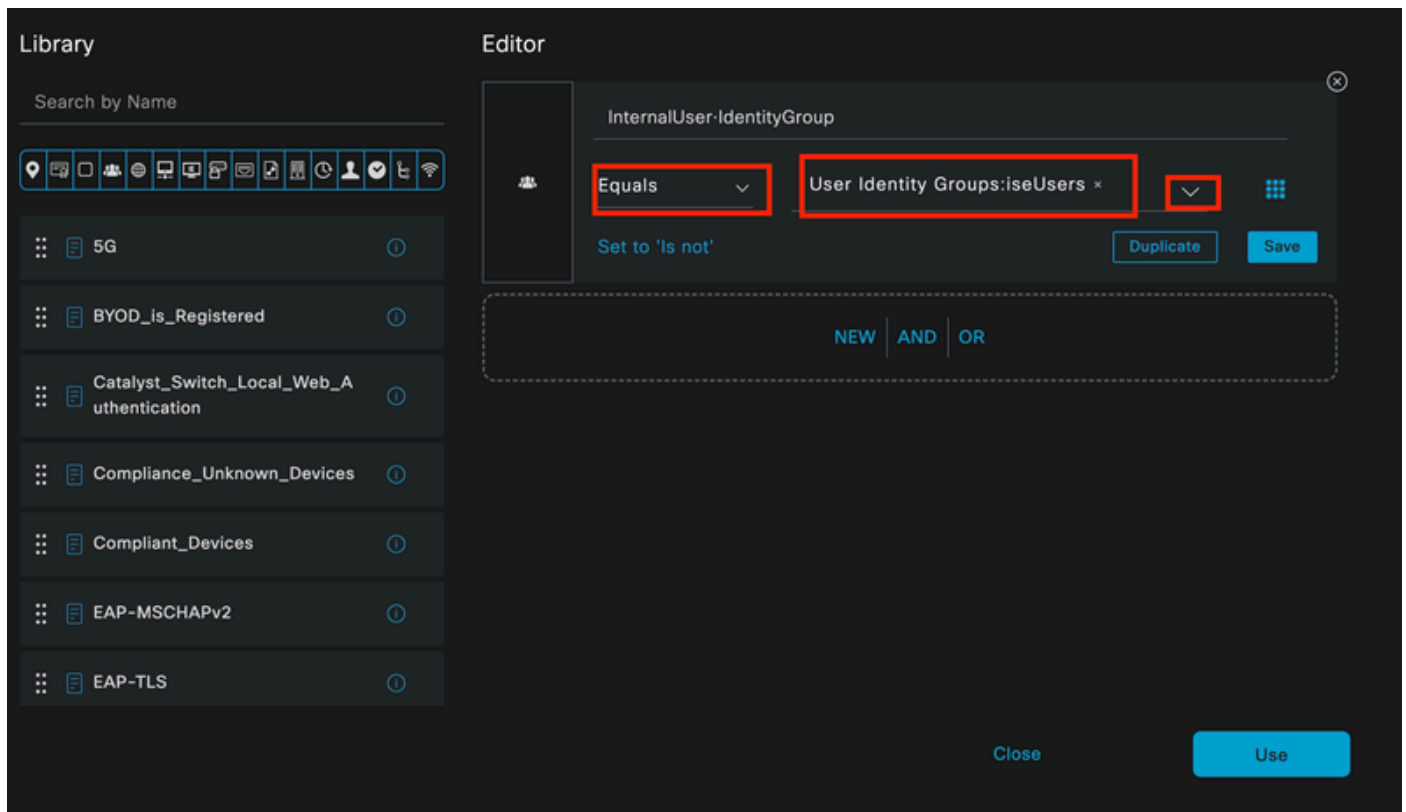
From the dictionary select the **InternalUser** dictionary that comes with the **IdentityGroup** attribute.



Condition Creation

Select the **Equals** operator.

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



Condition Creation

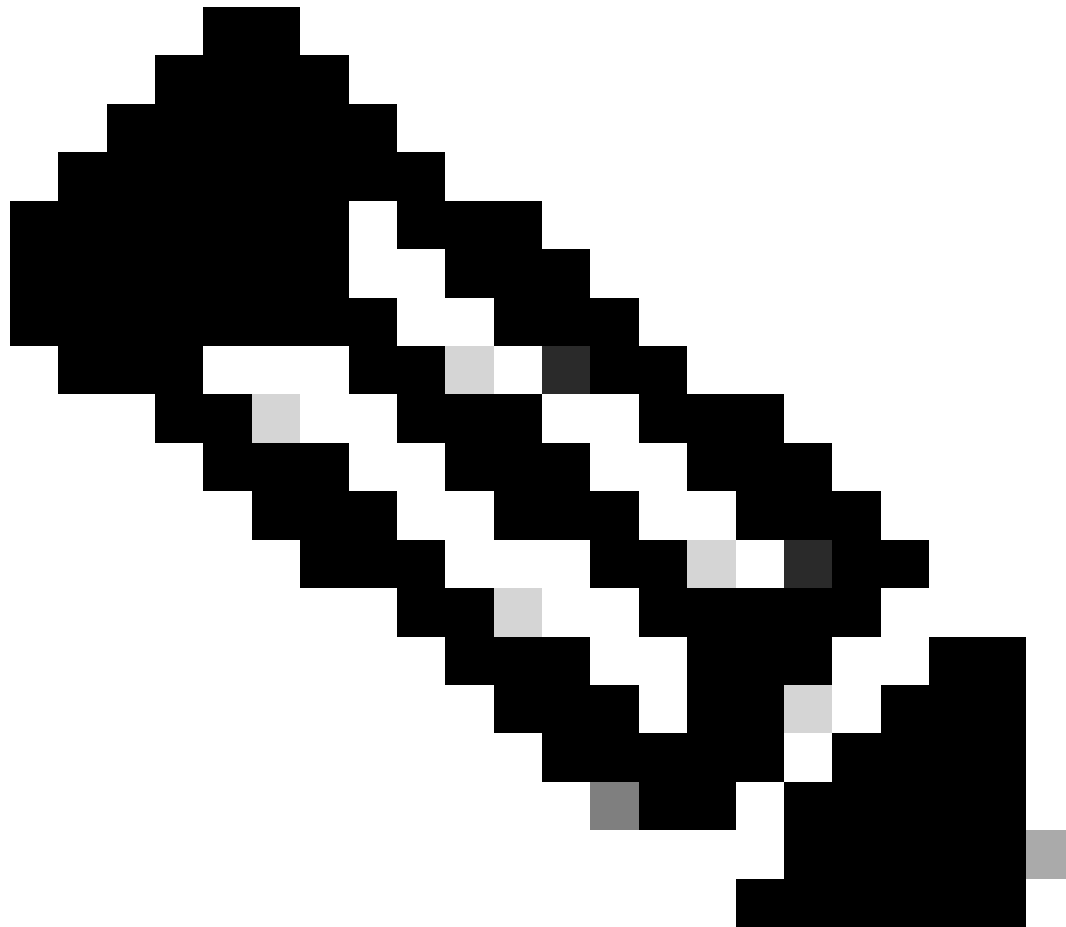
Click **Use**.



Add the **Result** Authorization Profile.

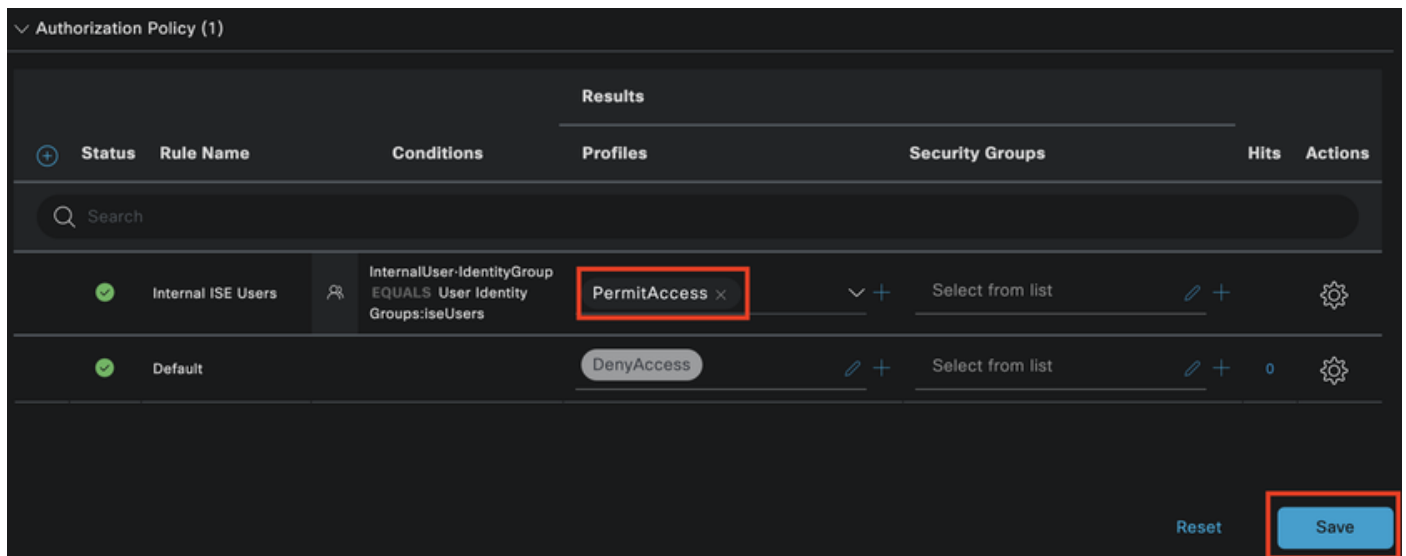
The pre-configured profile **Permit Access** is used.

---



**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**.

---



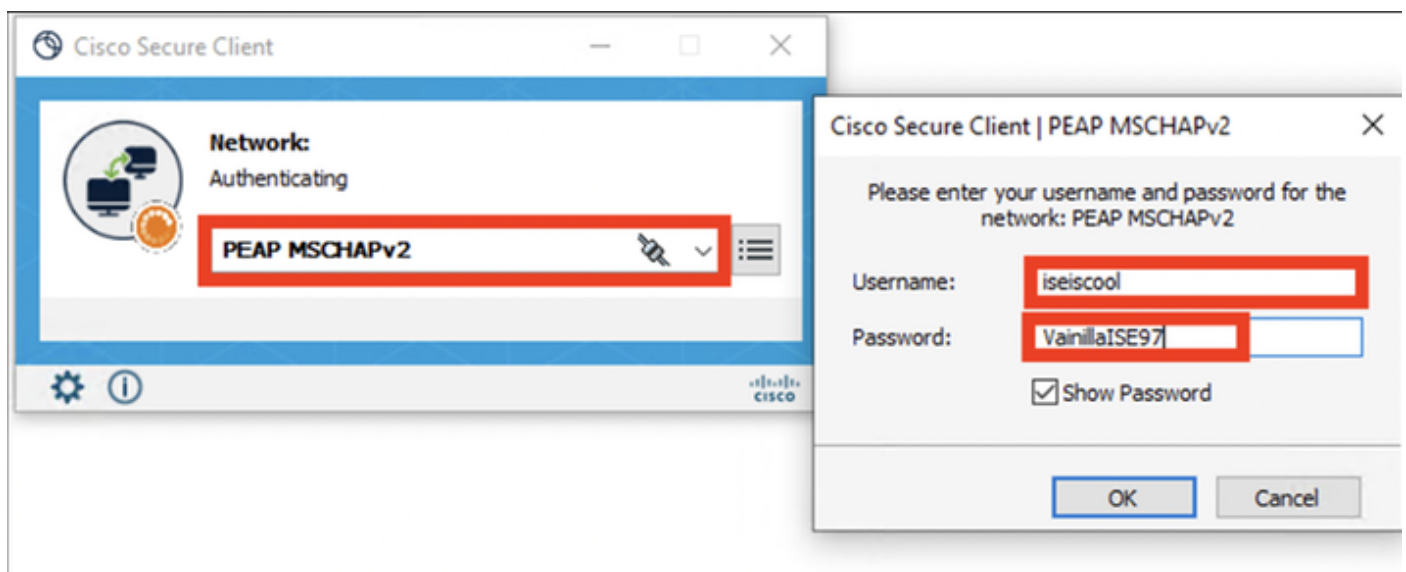
Authorization Policy

Click **Save**.

## Verify

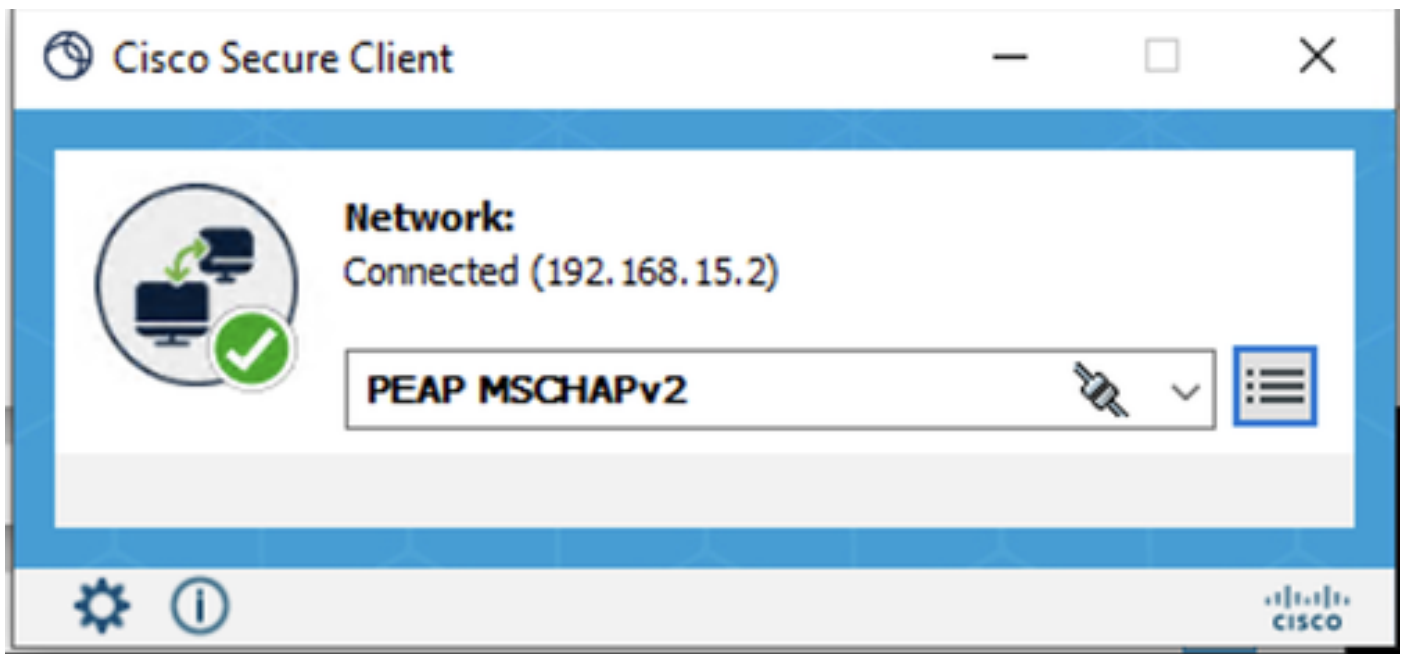
Once the configuration is finished Secure Client prompts for the credentials, and it specifies the usage of **PEAP MSCHAPv2** profile.

The credentials previously created are entered.



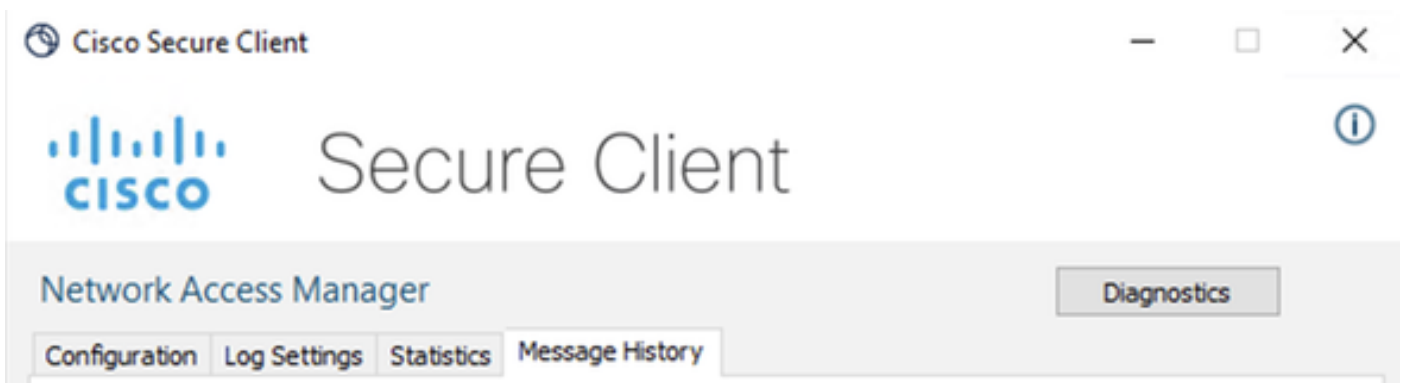
Secure Client NAM

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



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

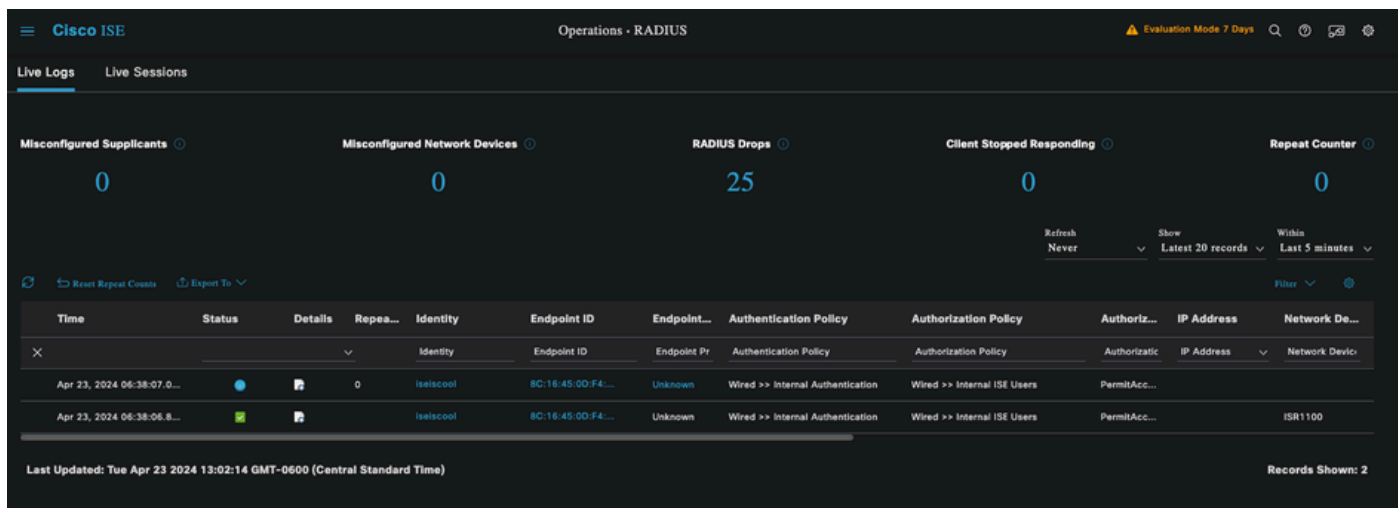
```
7:06:01 PM  PEAP MSCHAPv2 : Authenticating
7:06:21 PM  PEAP MSCHAPv2 : Acquiring IP Address
7:06:21 PM  PEAP MSCHAPv2 : Connected
```

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.



ISE RADIUS Live Logs

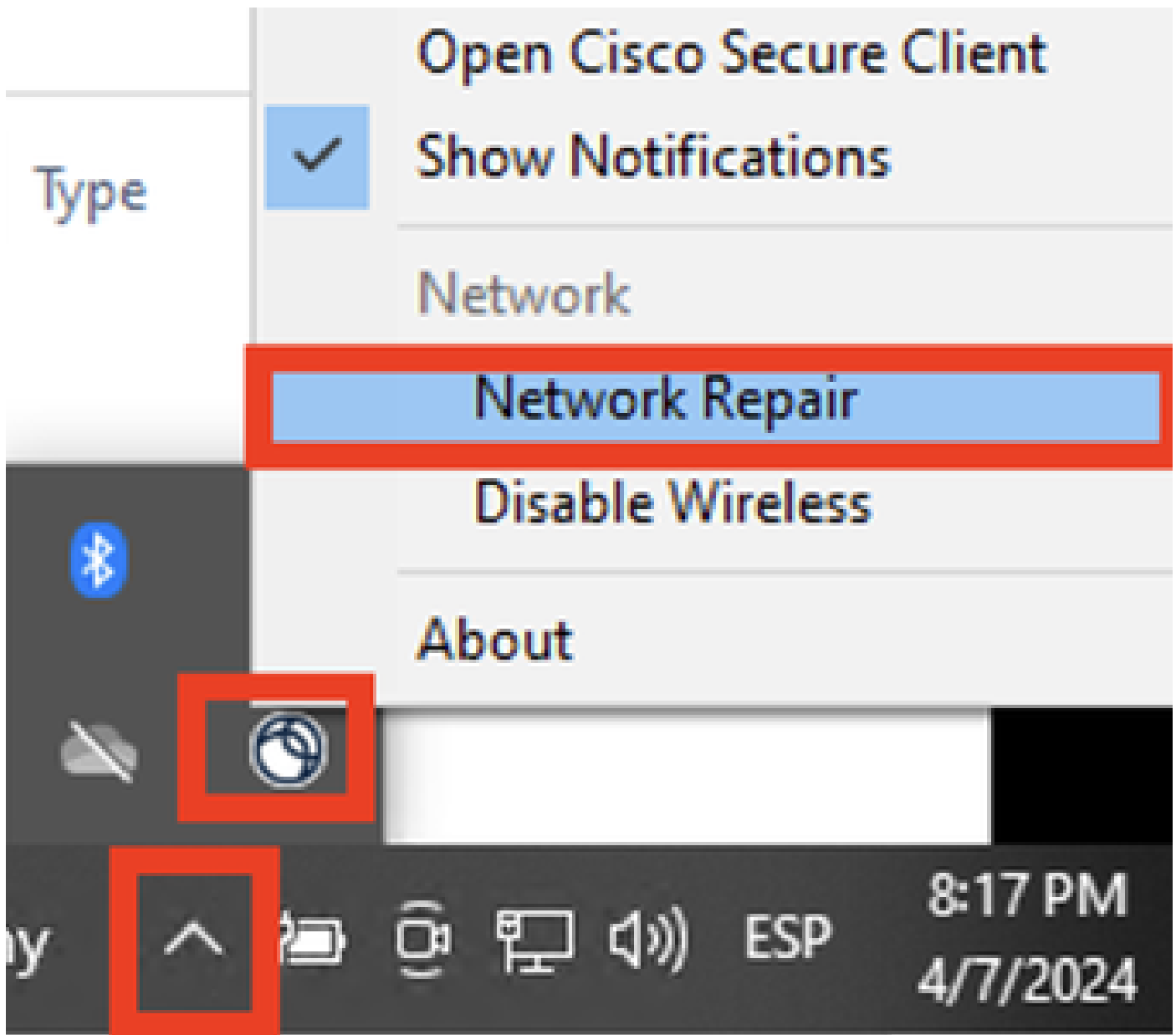
Since you can see it hits the correct policies, and the result is a successful authentication status it is conclude that the configuration is correct.

## 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**.

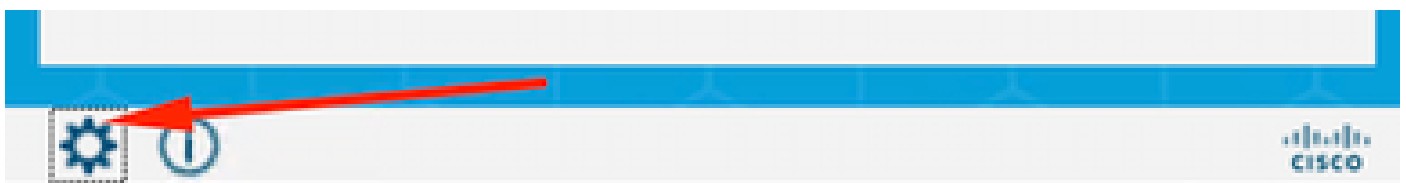


Network Repair Section

**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.



## Network Access Manager

Diagnostics

Configuration

Log Settings

Statistics

Message History

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**.



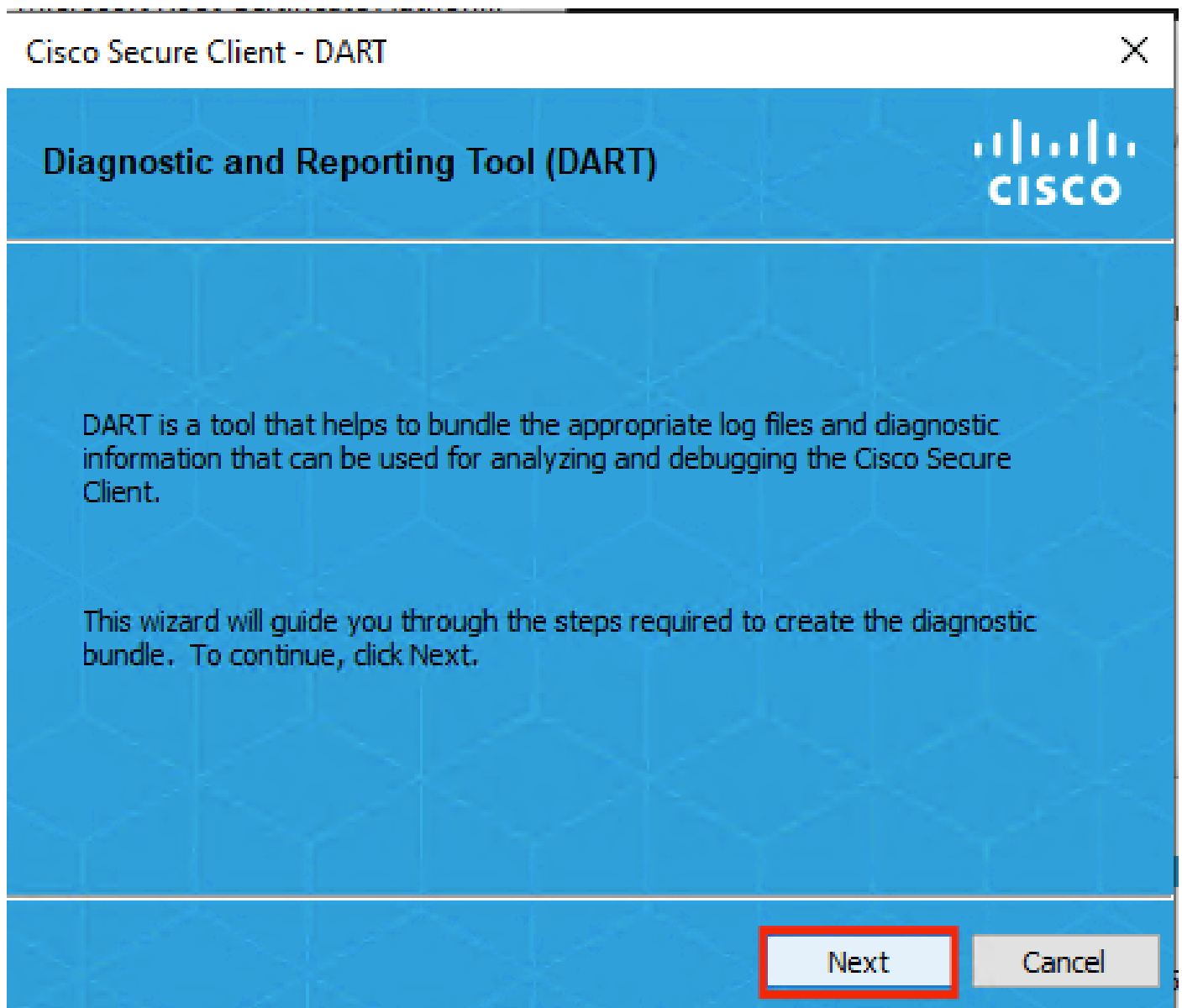
# Cisco Secure Client Diagnostics and Reporting Tool

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.



## DART Module

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

## 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

*DART Module*

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



## Bundle Encryption Option



☐ Enable Bundle Encryption

☒ Mask Password

Encryption Password

Confirm Password

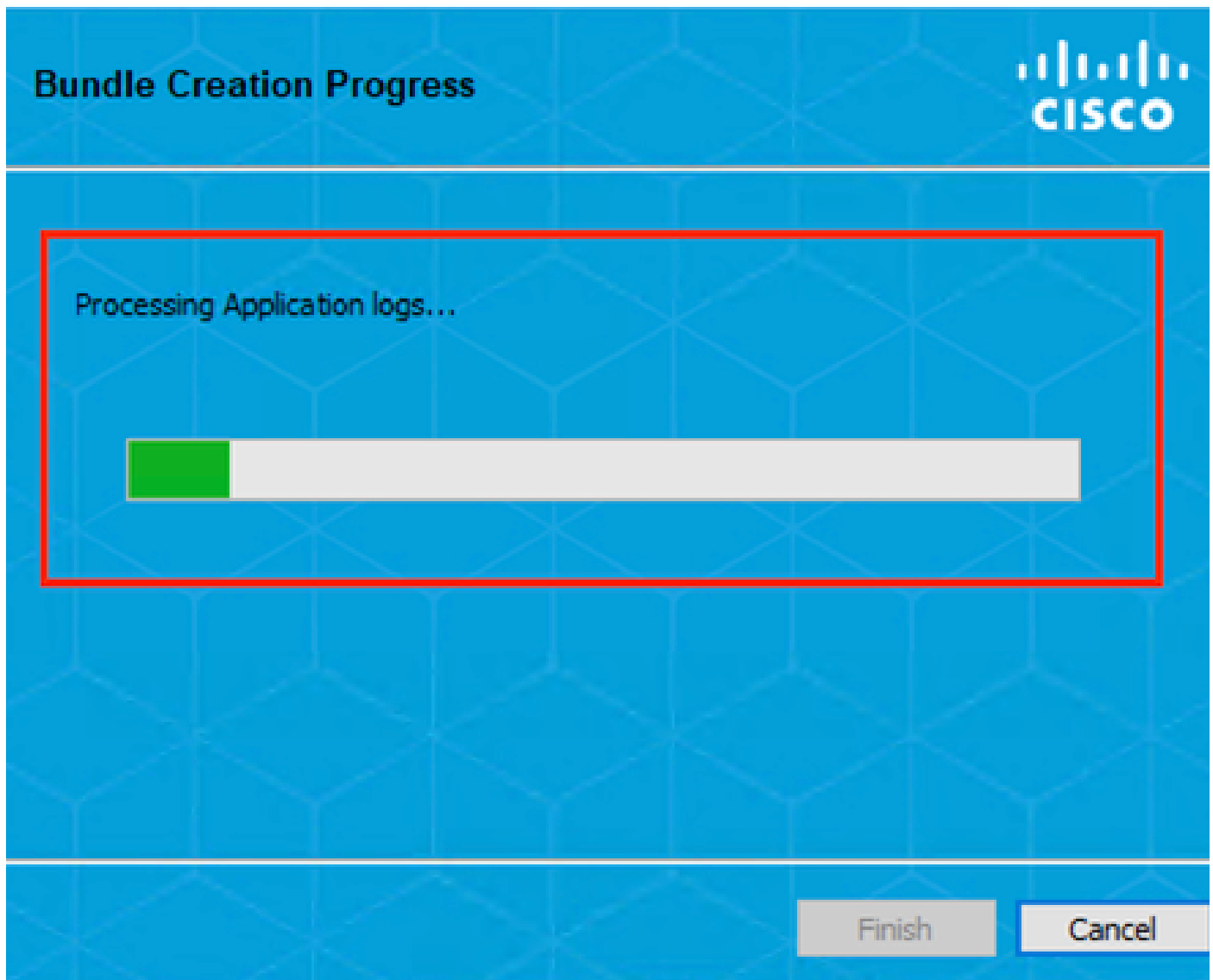
Back

Next

Cancel

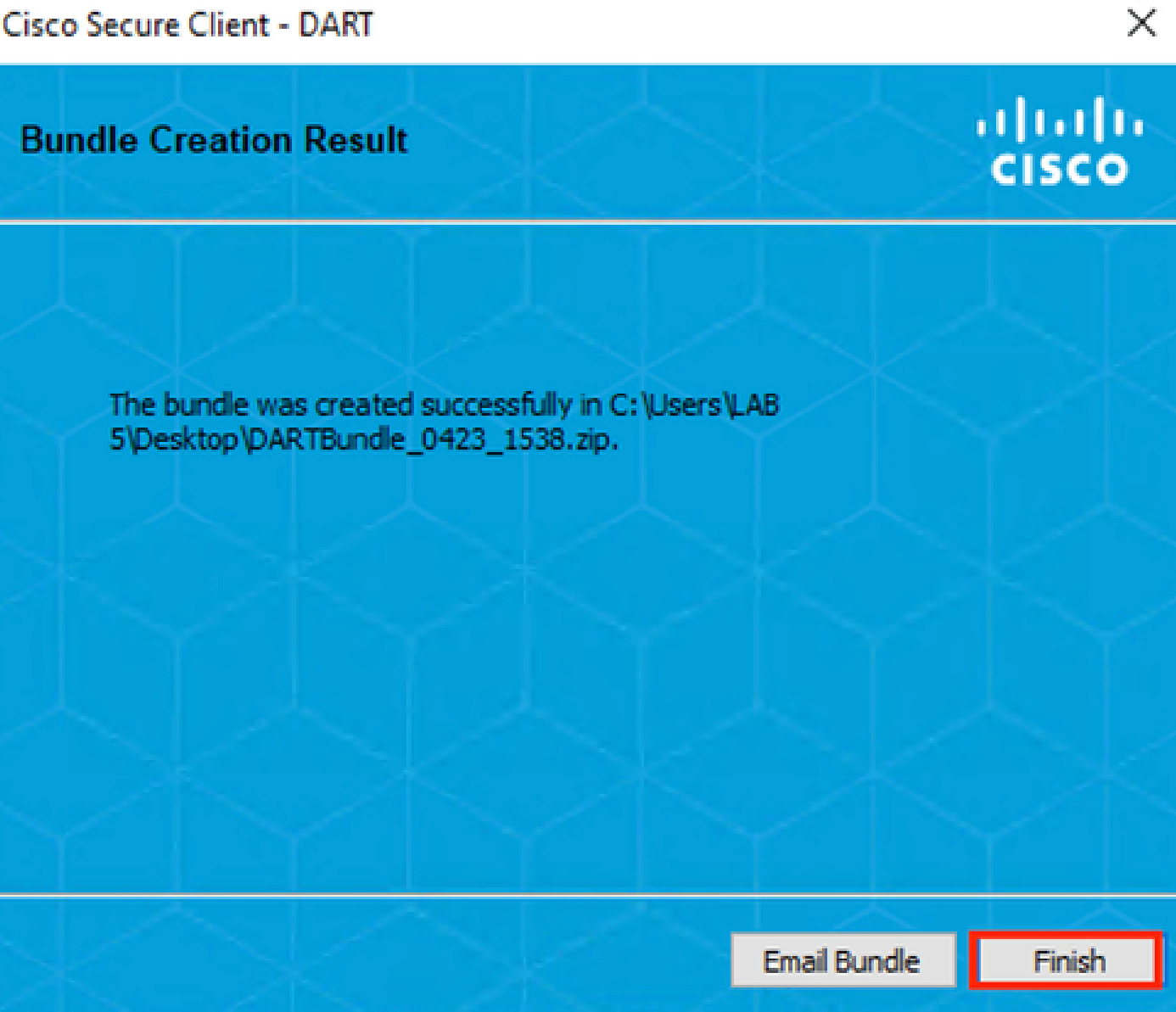
*DART Module*

**DART** log collection starts.




*DART Log Collection*

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



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](#)