

# WindowsおよびISE 3.2を使用したDot1x用のセキュアなクライアントNAMの設定

## 内容

---

### [はじめに](#)

### [前提条件](#)

#### [要件](#)

#### [使用するコンポーネント](#)

### [背景説明](#)

### [設定](#)

#### [ネットワーク図](#)

#### [コンフィギュレーション](#)

- [1. セキュアクライアントNAM\(Network Access Manager\)のダウンロードとインストール](#)
- [2. セキュアクライアントNAMプロファイルエディタをダウンロードしてインストールします](#)
- [3. 一般的なデフォルト設定](#)
- [4. シナリオ1:PEAP\(MS-CHAPv2\)ユーザ認証のためのセキュアクライアントNAMサブリカントの設定](#)
- [5. シナリオ2:EAP-FAST同時ユーザ認証とマシン認証のためのセキュアクライアントNAMサブリカントの設定](#)
- [6. シナリオ3:EAP-TLSユーザ証明書認証のためのセキュアクライアントNAMサブリカントの設定](#)
- [7. シナリオ1 PEAP MSCHAPv2に基づく認証を許可するためのISR 1100およびISEの設定](#)

### [確認](#)

### [トラブルシューティング](#)

[問題1:セキュアクライアントでNAMプロファイルが使用されていません。](#)

[問題2:さらなる分析のためにログを収集する必要があります。](#)

- [1. NAM拡張ロギングの有効化](#)
- [2. 問題を再現します。](#)
- [3. セキュアクライアントDARTバンドルを収集します。](#)

### [関連情報](#)

---

## はじめに

このドキュメントでは、Windowsでセキュアクライアントネットワーク解析モジュール(NAM)を設定する方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- RADIUSサブリカントとは何かについての基本的な知識
- Dot1x
- PEAP
- PKI

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Windows 10 Proバージョン22H2ビルド19045.3930
- ISE 3.2
- Cisco C1117 Cisco IOS® XEソフトウェア、バージョン17.12.02
- Active Directory 2016

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

このドキュメントでは、WindowsでセキュアなクライアントNAMを設定する方法について説明します。事前展開オプションと、dot1x認証を実行するプロファイルエディタが使用されます。また、これを実現する方法の例をいくつか示します。

ネットワーキングにおいて、サブリカントとは、ポイントツーポイントLANセグメントの一方の端にあるエンティティで、そのリンクの他方の端に接続されたオーセンティケータによる認証を求めるものです。IEEE 802.1X標準では、「サブリカント」という用語はハードウェアまたはソフトウェアを指します。実際には、サブリカントはエンドユーザコンピュータにインストールされるソフトウェアアプリケーションです。ユーザはサブリカントを呼び出し、クレデンシャルを送信して、コンピュータをセキュアネットワークに接続します。認証に成功すると、通常、オーセンティケータはコンピュータがネットワークに接続することを許可します。

### ネットワークアクセスマネージャについて

Network Access Managerは、ポリシーに従ってセキュアなレイヤ2ネットワークを提供するクライアントソフトウェアです。最適なレイヤ2アクセスネットワークを検出して選択し、有線ネットワークとワイヤレスネットワークの両方にアクセスするためのデバイス認証を実行します。

Network Access Managerは、セキュアなアクセスに必要なユーザとデバイスのIDおよびネットワークアクセスプロトコルを管理します。インテリジェントに機能し、管理者が定義したポリシーに違反する接続をエンドユーザが行わないようにします。

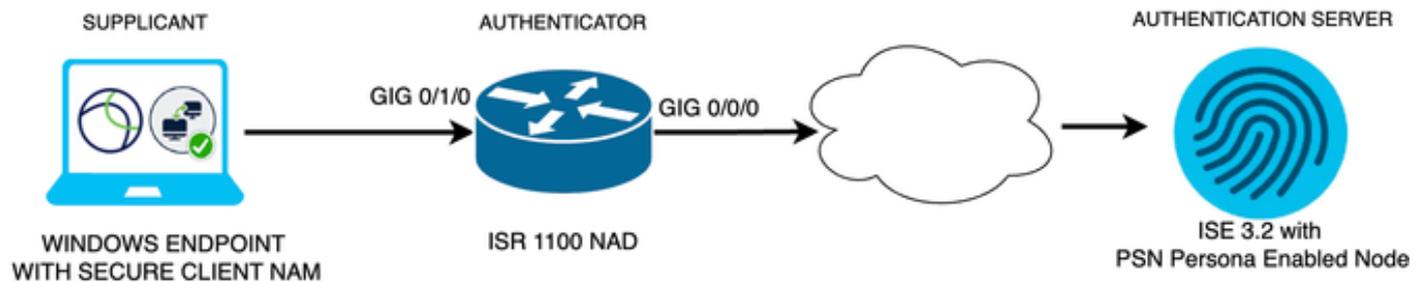
Network Access Managerはシングルホーム設計になっており、一度に1つのネットワーク接続だけを許可します。また、有線接続は無線よりも優先順位が高いため、有線接続を使用してネットワークに接続している場合、ワイヤレスアダプタはIPアドレスなしで無効になります。

## 設定

## ネットワーク図

dot1x認証では、dot1xを実行できるサブリカント、RADIUS内でdot1xトラフィックをカプセル化するプロキシとして機能するNAS/NADとも呼ばれるオーセンティケータ、および認証サーバの3つの部分が必要であることを理解することが重要です。

この例では、サブリカントはさまざまな方法でインストールおよび設定されます。後で、ネットワークデバイスの設定と認証サーバのシナリオを示します。



ネットワーク図

## コンフィギュレーション

1. セキュアクライアントNAM(Network Access Manager)をダウンロードしてインストールします。
2. Secure Client NAMプロファイルエディタをダウンロードしてインストールします。
3. 一般的なデフォルト設定
4. シナリオ1:PEAP(MS-CHAPv2)ユーザ認証用のセキュアクライアントNAMサブリカントの設定。
5. シナリオ2 : ユーザ認証とマシン認証の設定と同時に、EAP-FAST用のセキュアなクライアントNAMサブリカントを設定します。
6. シナリオ3パート1:EAP-TLS用のセキュアなクライアントNAMサブリカントの設定
7. シナリオ3パート2:NADとISEのデモンストレーションを設定します。

1. セキュアクライアントNAM(Network Access Manager)のダウンロードとインストール

### [Cisco Software のダウンロード](#)

製品名の検索バーで、「Secure Client 5」と入力します。

Downloads Home > Security > VPN and Endpoint Security Clients > Secure Client ( AnyConnectを含む ) > Secure Client 5 > AnyConnect VPN Client Softwareの順に選択します。

この設定例では、バージョン5.1.2.42が使用されています。

Secure ClientをWindowsデバイスに導入する方法は、SCCM、アイデンティティサービスエンジン、およびVPNヘッドエンドから複数あります。ただし、この記事で使用するインストール方法は、導入前の方法です。

ページで、Cisco Secure Client Headend Deployment Package(Windows)ファイルを検索します。

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ファイル

ダウンロードして解凍したら、Setupをクリックします。

 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
 <b>Setup</b>	4/4/2024 7:16 PM
 setup	4/4/2024 7:16 PM

クライアント・ファイルの保護

Network Access ManagerとDiagnostics and Reporting Toolモジュールをインストールします。



警告: Cisco Secure Client Wizardを使用する場合、VPNモジュールは自動的にインストールされ、GUIでは表示されません。VPNモジュールがインストールされていない場合、NAMは機能しません。個々のMSIファイルを使用する場合、または別のインストール方法を使用する場合は、VPNモジュールをインストールしてください。

---

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

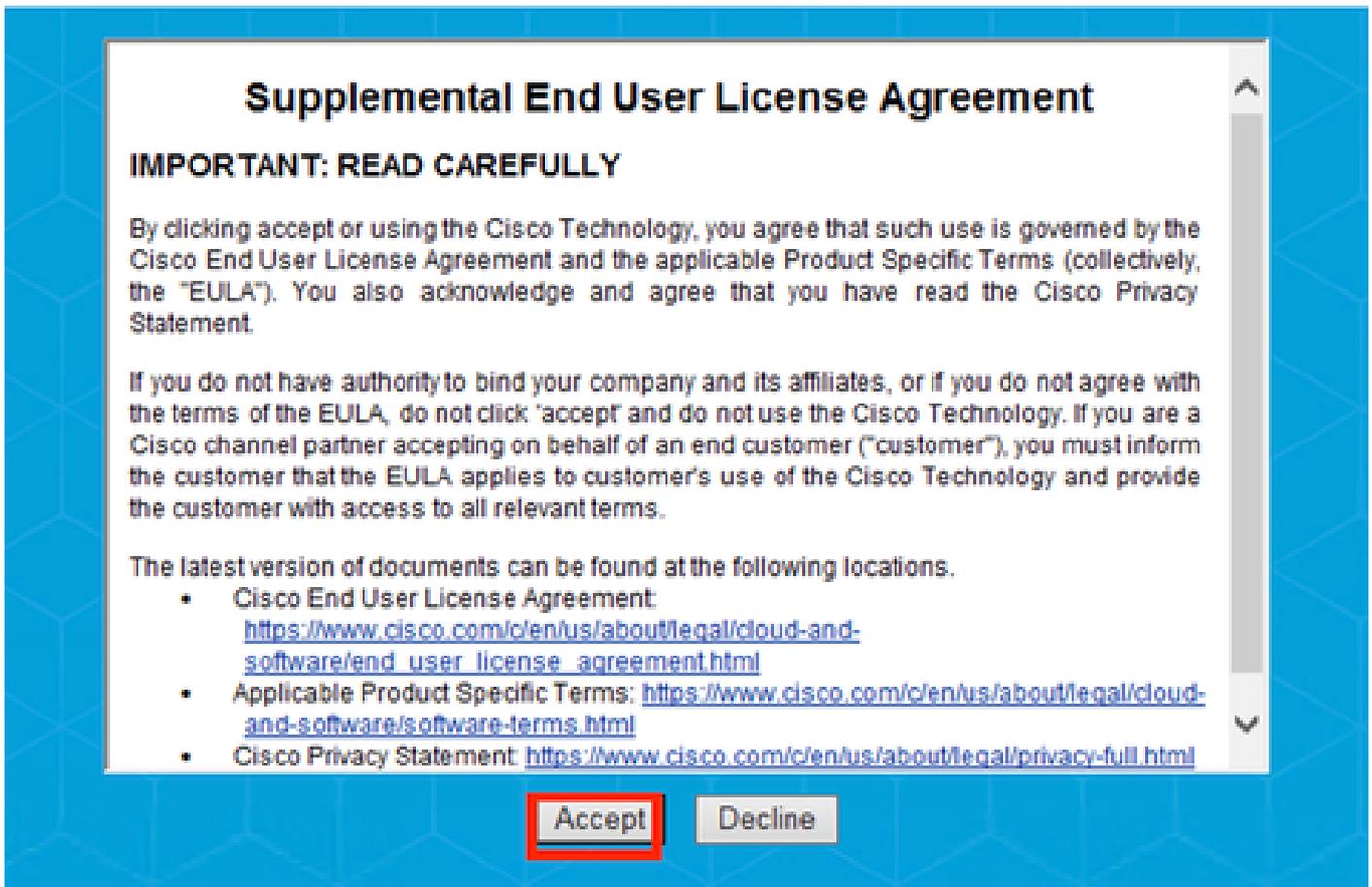
- Core & AnyConnect VPN
- Start Before Login
- Network Access Manager
- Secure Firewall Posture
- Network Visibility Module
- Umbrella
- ISE Posture
- ThousandEyes
- Zero Trust Access
- Select All
- Diagnostic And Reporting Tool
- Lock Down Component Services

Install Selected

インストールセレクタ

[選択項目のインストール ( Install Selected ) ] をクリックします。

EULAに同意します。



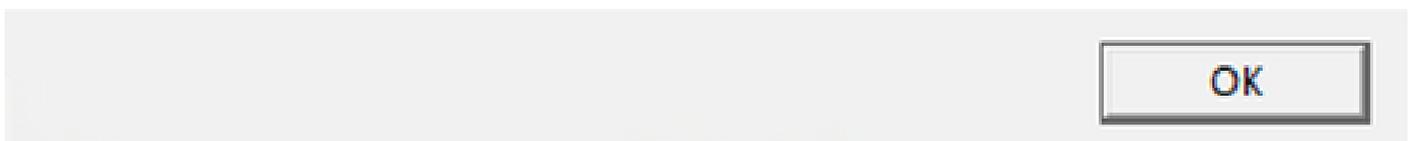
EULAウインドウ

NAMのインストール後に再起動が必要です。

## Cisco Secure Client Install Selector

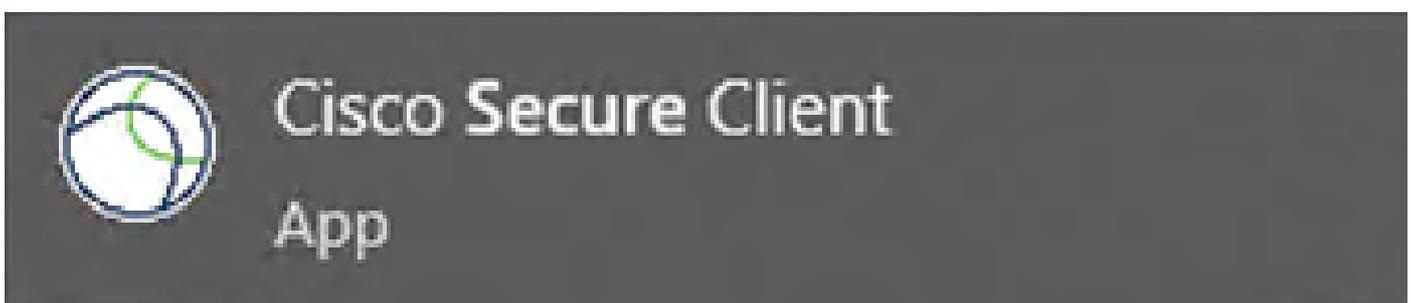


**You must reboot your system for the installed changes to take effect.**



リブート要件ウインドウ

インストールが完了すると、Windowsの検索バーからファイルを検索して開くことができます。



2. セキュアクライアントNAMプロファイルエディタをダウンロードしてインストールする。

Dot1xの設定には、Cisco Network Access Manager Profile Editorが必要です。

セキュアクライアントをダウンロードした同じページに、Profile Editorオプションがあります。

この例では、バージョン5.1.2.42のオプションを使用しています。

Profile Editor (Windows) 

06-Feb-2024

15.71 MB



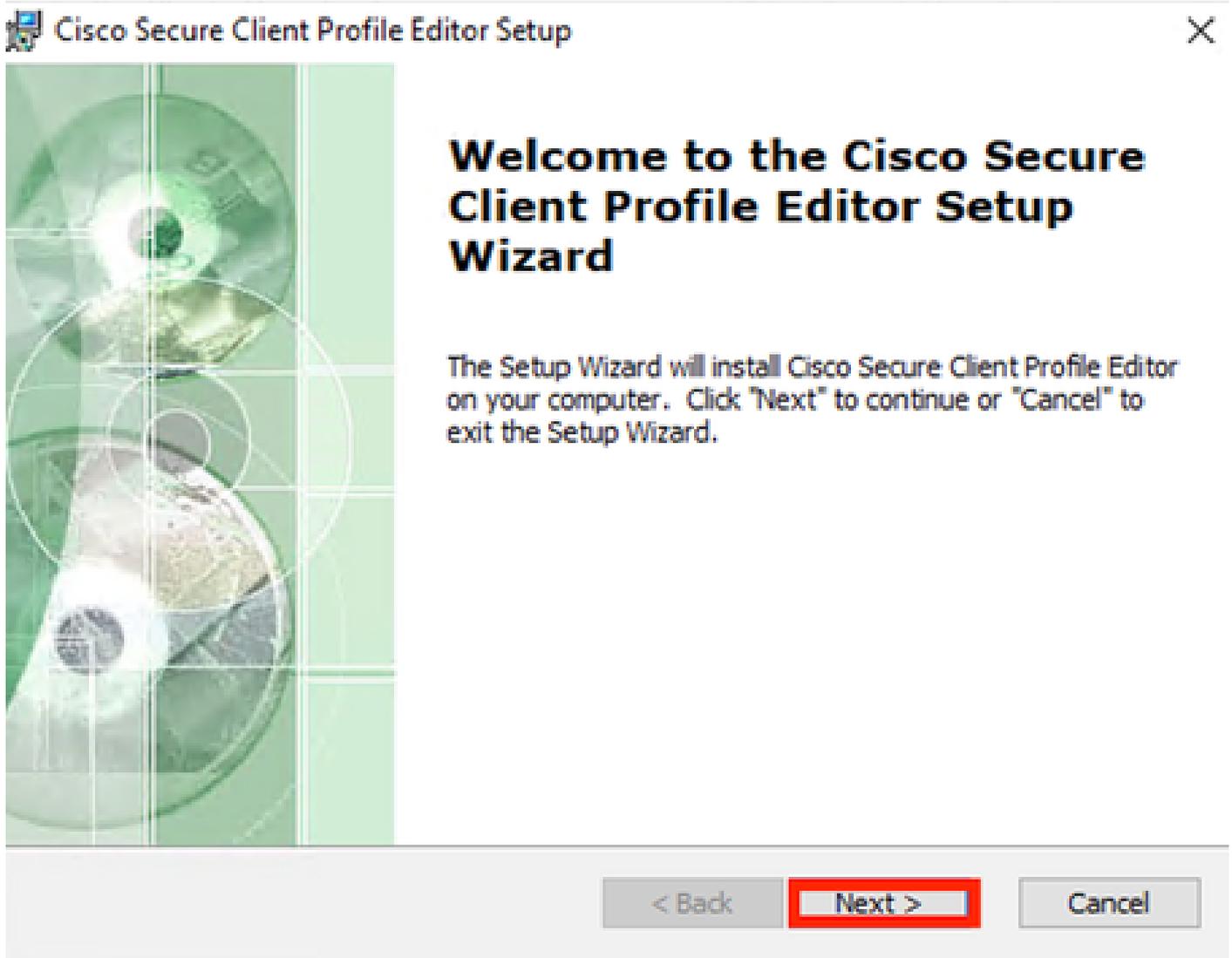
tools-cisco-secure-client-win-5.1.2.42-profileeditor-k9.msi

Advisories 

プロファイルエディタ

ダウンロードが完了したら、インストールに進みます。

msiファイルを実行します。



プロファイルエディタの設定ウィンドウ

Typicalセットアップオプションを使用します。

Cisco Secure Client Profile Editor Setup

### Choose Setup Type

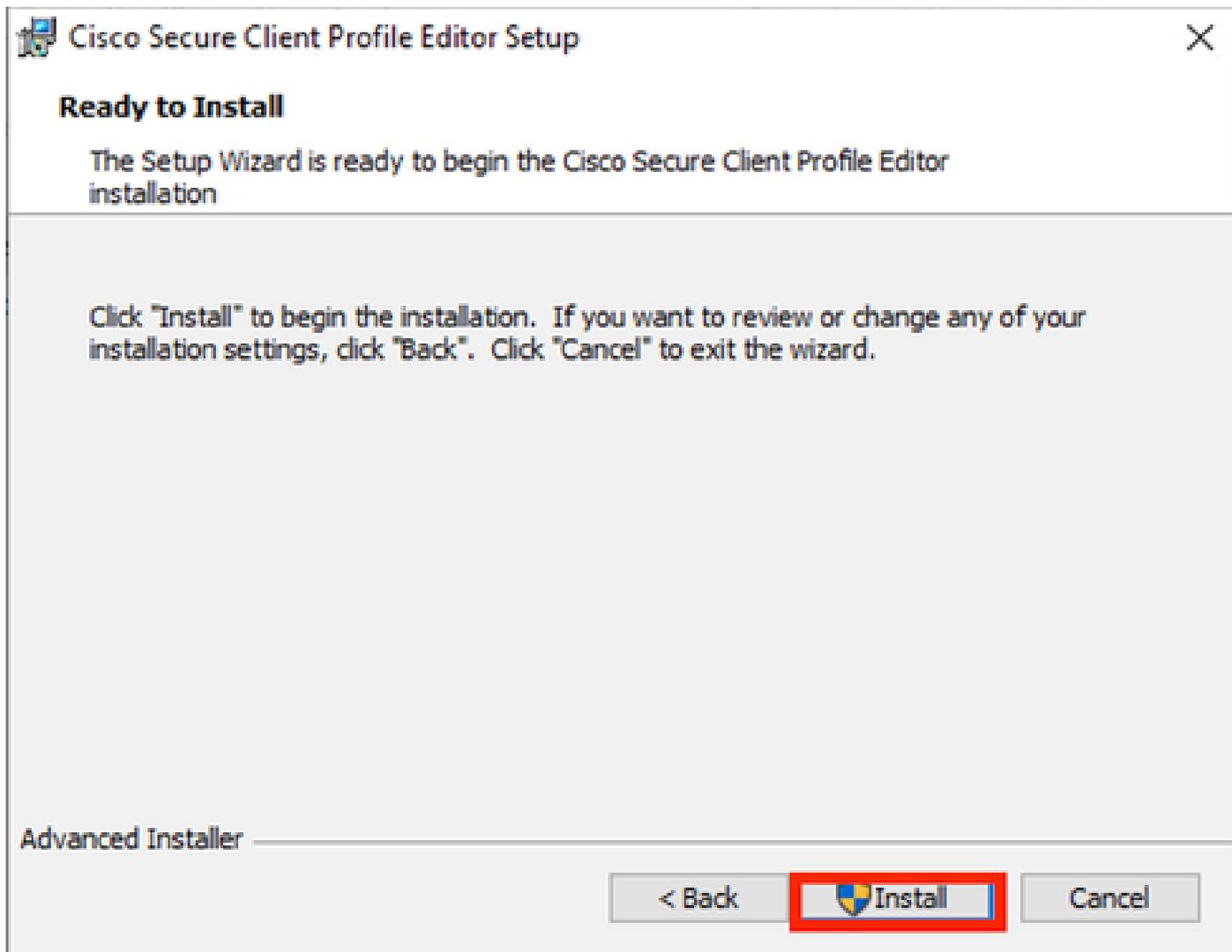
Choose the setup type that best suits your needs

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

Advanced Installer

< Back    Next >    Cancel

プロファイルエディタの設定



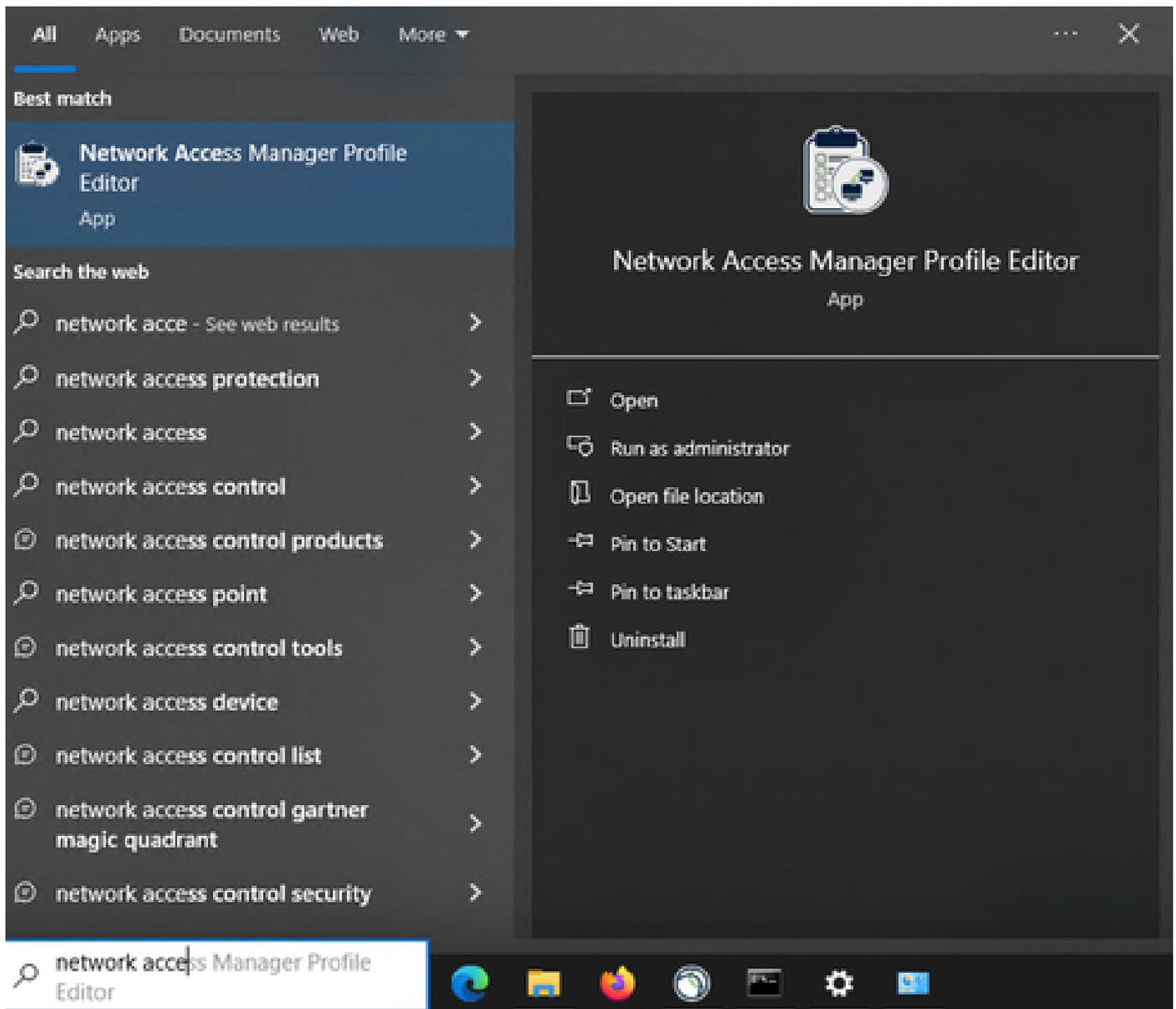
インストールウィンドウ

[Finish] をクリックします。



プロフィールエディタの設定の終了

インストールが完了したら、検索バーからNetwork Access Managerプロフィールエディタを開きます。



検索バーのNAMプロファイルエディタ

Network Access Managerとプロファイルエディタのインストールが完了しました。

### 3. 一般的なデフォルト設定

この記事で説明するすべてのシナリオには、次の設定が含まれています。

- クライアントポリシー
- 認証ポリシー
- ネットワークグループ

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

NAMプロファイルエディタクライアントポリシー

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

### Authentication Policy

Profile: Untitled

#### Allow Association Modes

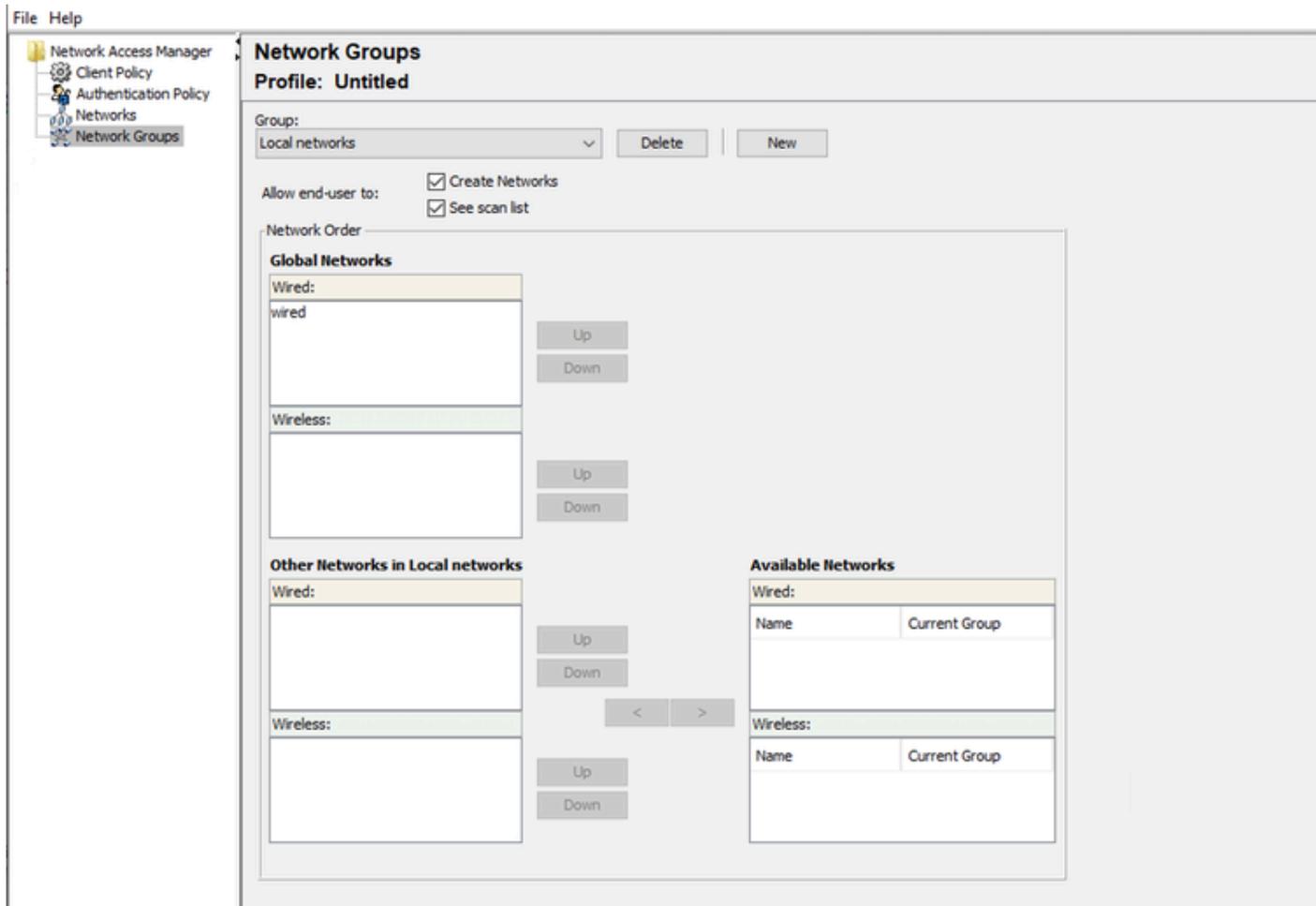
- Select All (Personal)
  - Open (no encryption)
  - Open (Static WEP)
  - Shared (WEP)
  - WPA Personal TKIP
  - WPA Personal AES
  - WPA2 Personal TKIP
  - WPA2 Personal AES
  - WPA3 Open (OWE)
  - WPA3 Personal AES (SAE)
- Select All (Enterprise)
  - Open (Dynamic (802.1X) WEP)
  - WPA Enterprise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

#### 4. シナリオ1:PEAP(MS-CHAPv2)ユーザ認証のためのセキュアなクライアントNAMサブリカントの設定

Networksセクションに移動します。

デフォルトのNetworkプロファイルは削除できます。

[Add] をクリックします。

## Networks

Profile: Untitled

### Network

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

Add...

Edit...

Delete

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

ネットワークプロファイルの作成

Networkプロファイルに名前を付けます。

Group MembershipにGlobalを選択します。Wired Network Mediaを選択します。

## Networks

Profile: Untitled

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

Network Profile Media Typeセクション

[Next] をクリックします。

Authenticating Networkを選択し、Security Levelセクションのその他のオプションにはデフォルトを使用します。

**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

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

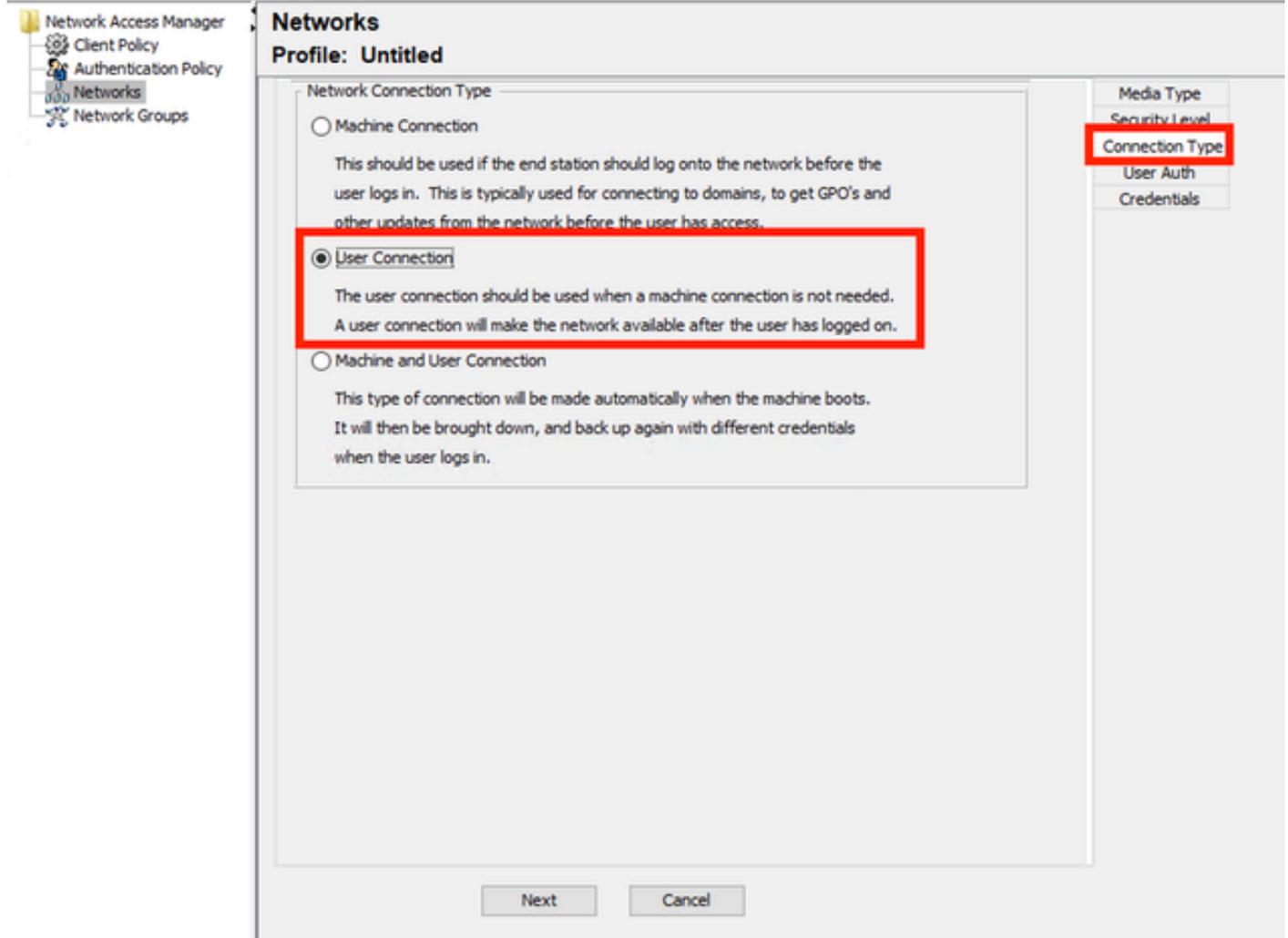
AES GCM 128

AES GCM 256

Next Cancel

ネットワークプロファイルのセキュリティレベル

Nextをクリックして、Connection Typeセクションを続けます。



ネットワークプロファイル接続タイプ

User Connection接続タイプを選択します。

Nextをクリックして、利用可能になったUser Authセクションを続けます。

一般的なEAP MethodとしてPEAPを選択します。

**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

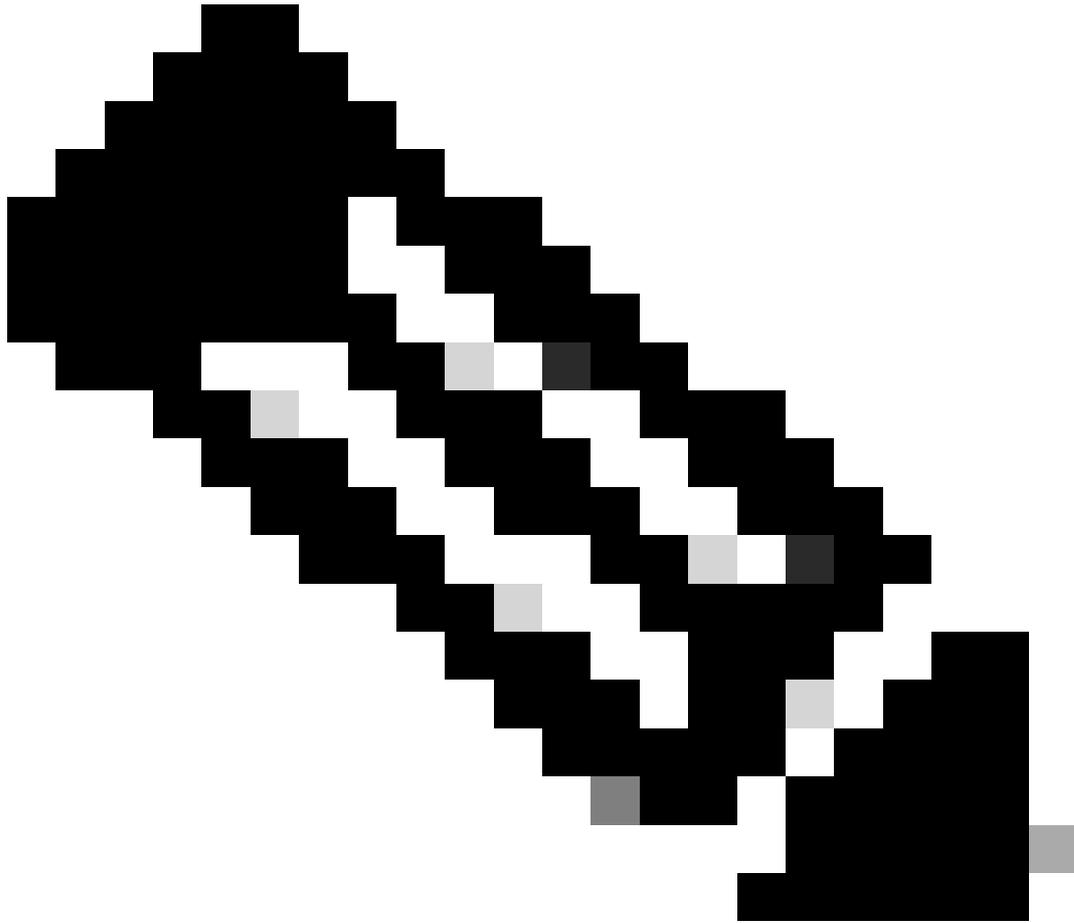
ネットワークプロファイルユーザ認証

EAP-PEAP Settingsでデフォルト値を変更しないでください。

「クレデンシャルソースに基づく内部メソッド」セクションに進みます。

EAP PEAPに対して存在する複数の内部方式から、Authenticate using a Passwordを選択し、EAP-MSCHAPv2を選択します。

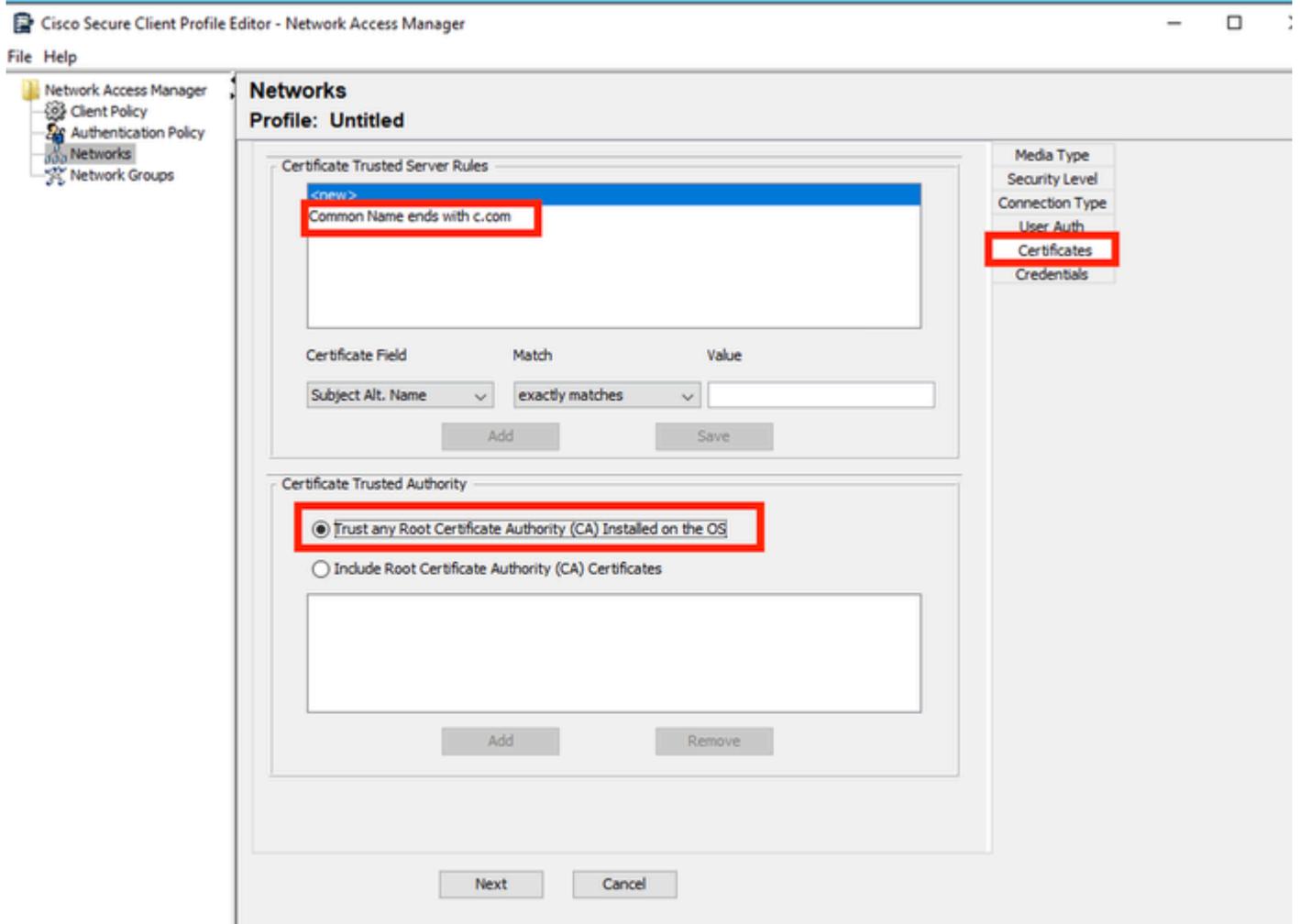
Nextをクリックして、Certificateセクションに進みます。



注：[Certificate]セクションが表示されるのは、[EAP-PEAP Settings]で[Validate Server Identity]オプションが選択されているためです。EAP PEAPでは、サーバ証明書を使用してカプセル化を行います。

---

CertificatesセクションのCertificate Trusted Server Rulesで、Common Name end with c.com ルールが使用されます。設定のこのセクションでは、EAP PEAPフロー中にサーバが使用する証明書について説明します。ご使用の環境でIdentity Service Engine(ISE)を使用している場合は、ポリシーサーバノードEAP証明書の共通名を使用できます。

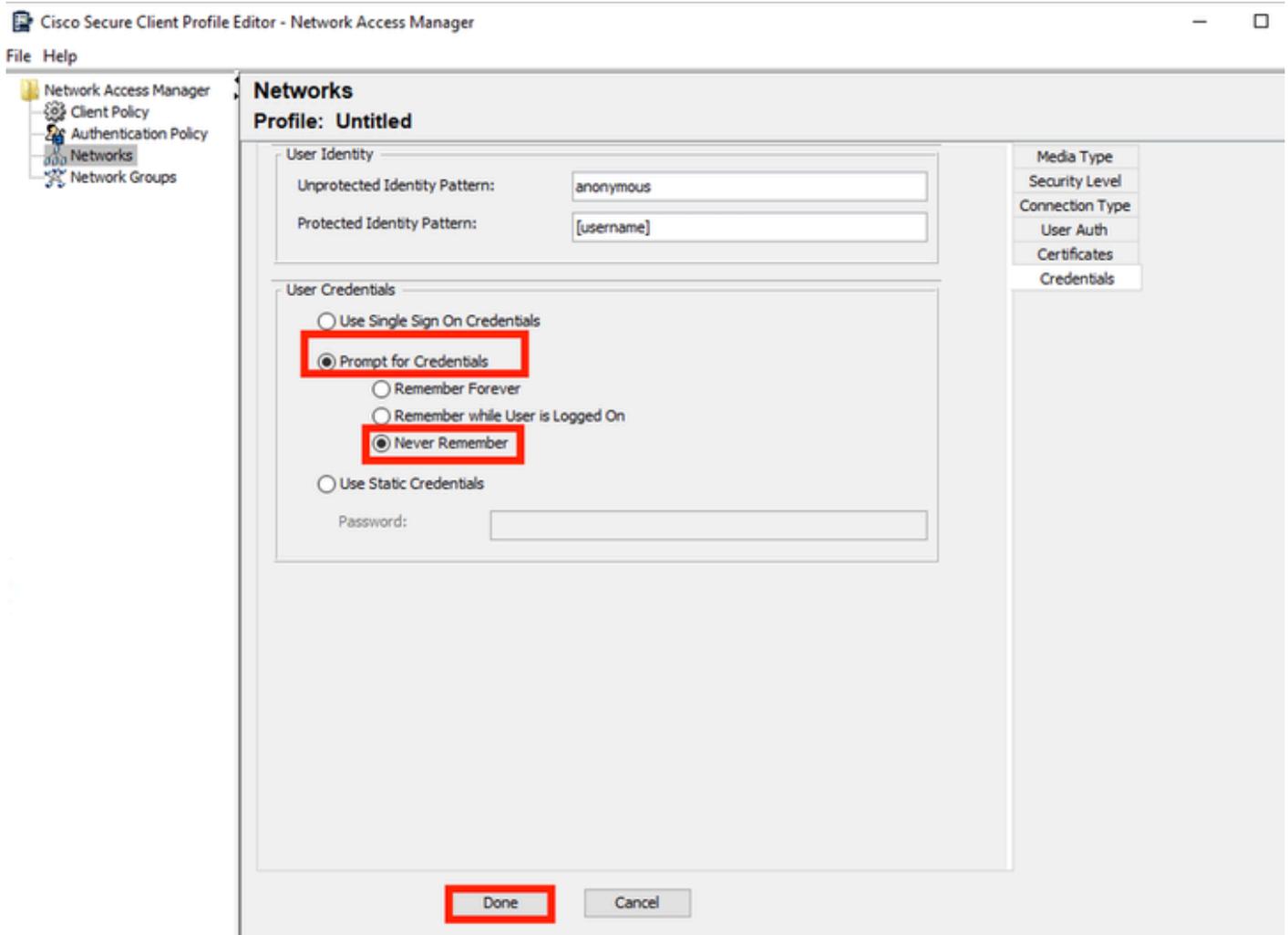


#### Network Profile Certificateセクション

Certificate Trusted Authorityでは、2つのオプションを選択できます。このシナリオでは、RADIUS EAP証明書に署名した特定のCA証明書を追加する代わりに、オプションTrust any Root Certificate Authority (CA) Installed on the OSを使用します。

このオプションを使用すると、Windowsデバイスは、Manage User CertsプログラムのCertificates — Current User > Trusted Root Certification Authorities > Certificatesに含まれている証明書によって署名されたすべてのEAP証明書を信頼します。

[Next] をクリックします。



Network Profile Credentialセクション

Credentialsセクションでは、User Credentialsセクションのみが変更されます。

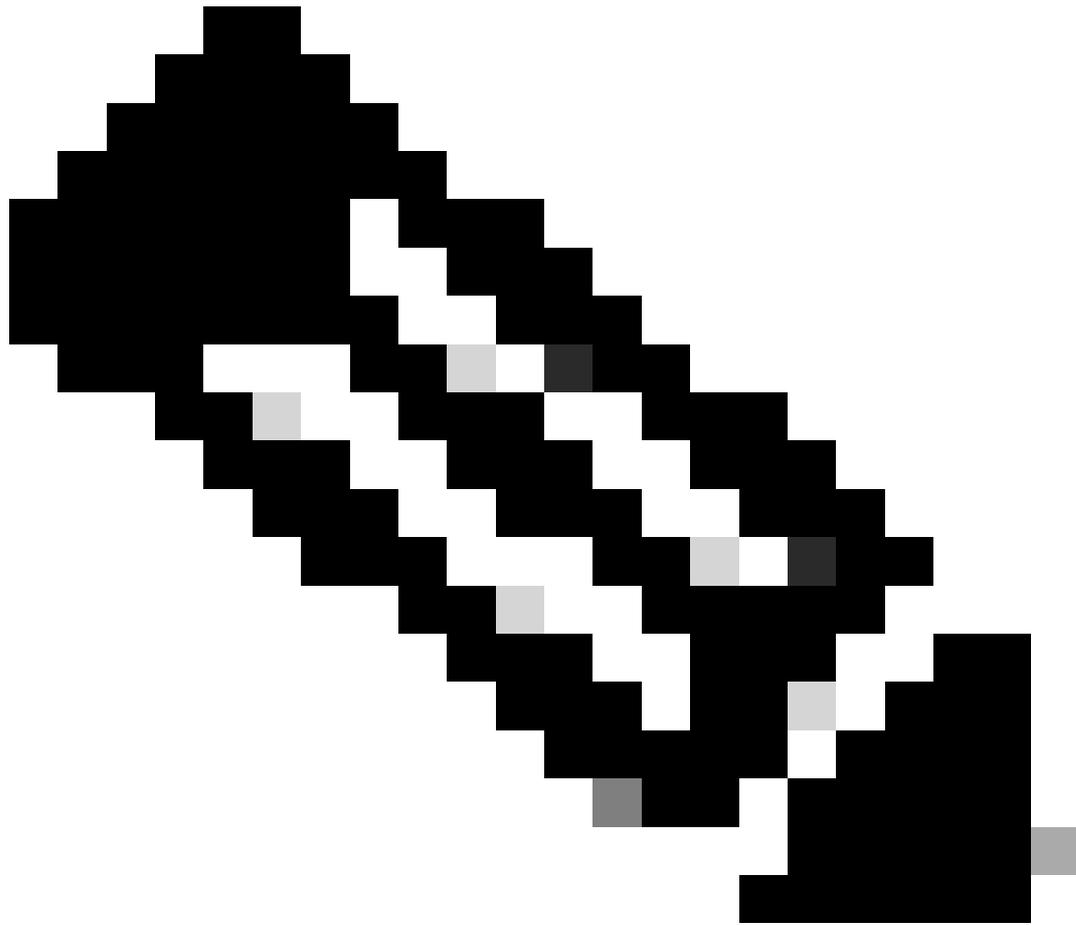
Prompt for Credentials > Never Rememberオプションが選択されているため、認証を行うユーザは認証ごとにクレデンシャルを入力する必要があります。

[Done] をクリックします。

File > Save Asオプションを使用して、Secure Client Network Access Manager(SCA)プロファイルをconfiguration.xmlとして保存します。

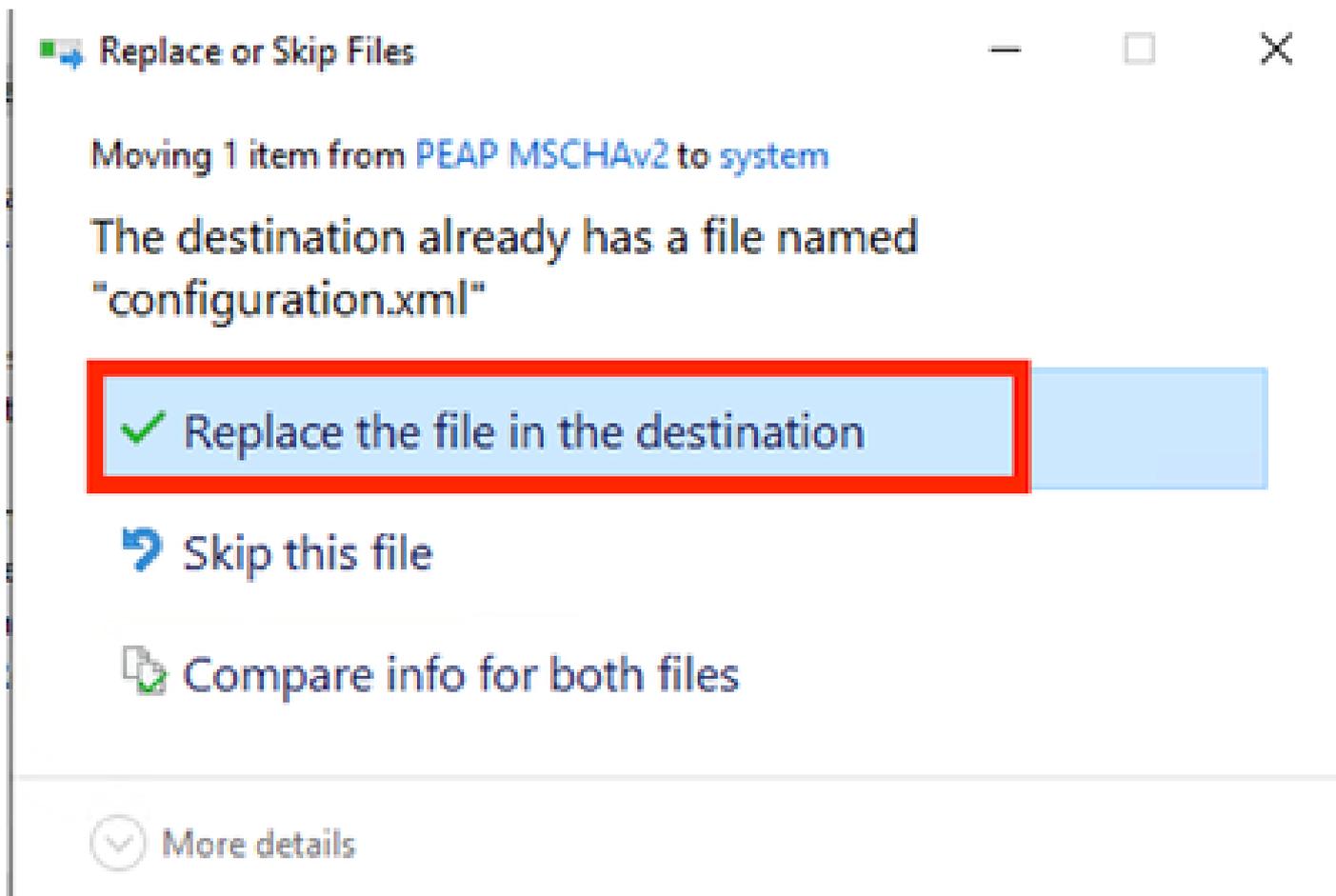
作成したばかりのプロファイルをセキュアクライアントネットワークアクセスマネージャで使用するには、次のディレクトリにあるconfiguration.xmlファイルを新しいファイルで置き換えます。

C:\ProgramData\Cisco\Ciscoセキュアクライアント\Network Access Manager\system



注：ファイルはconfiguration.xmlという名前である必要があります。そうでない場合は機能しません。

---



ファイルセクションの置換

## 5. シナリオ2:EAP-FASTユーザとマシンの同時認証のためのセキュアなクライアントNAMサブリンクの設定

NAMプロファイルエディタを開き、Networksセクションに移動します。

[Add] をクリックします。

## Networks

Profile: Untitled

### Network

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

Add...

Edit...

Delete

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

NAMプロフィールエディタネットワークタブ

ネットワークプロフィールに名前を入力します。

Group MembershipにGlobalを選択します。WiredNetwork Mediaを選択します。

File Help

**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セクション

[Next] をクリックします。

Authenticating Networkを選択し、このセクションの残りのオプションではデフォルト値を変更しないでください。

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セクション

Nextをクリックして、Connection Typeセクションを続けます。

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.

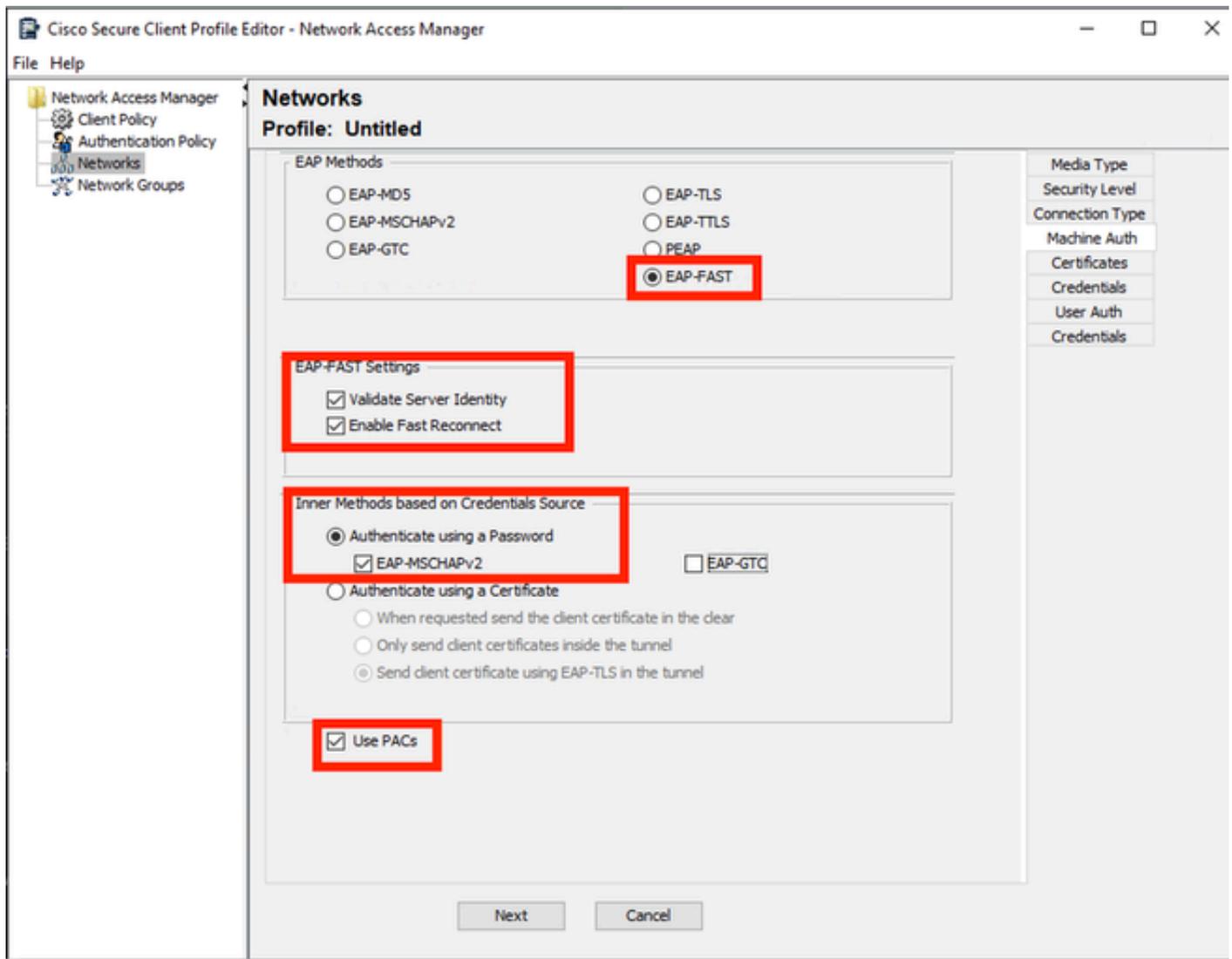
Media Type  
Security Level  
**Connection Type**  
Machine Auth  
Credentials  
User Auth  
Credentials

Next Cancel

Connection Typeセクション

3番目のオプションを選択して、ユーザとマシンの認証を同時に設定します。

[Next] をクリックします。



#### Machine Authセクション

Machine Authセクションで、EAP方式としてEAP-FASTを選択します。EAP FAST設定のデフォルト値は変更しないでください。Inner methods based on Credentials Sourceセクションで、方式としてAuthenticate using a PasswordとEAP-MSCHAPv2を選択します。次にUse PACsオプションを選択します。

[Next] をクリックします。

CertificatesセクションのCertificate Trusted Server Rulesで、ルールの共通名はc.comで終わっています。このセクションでは、EAP PEAPフロー中にサーバが使用する証明書について説明します。ご使用の環境でIdentity Service Engine(ISE)を使用している場合は、ポリシーサーバノードEAP証明書の共通名を使用できます。

## Networks

Profile: Untitled

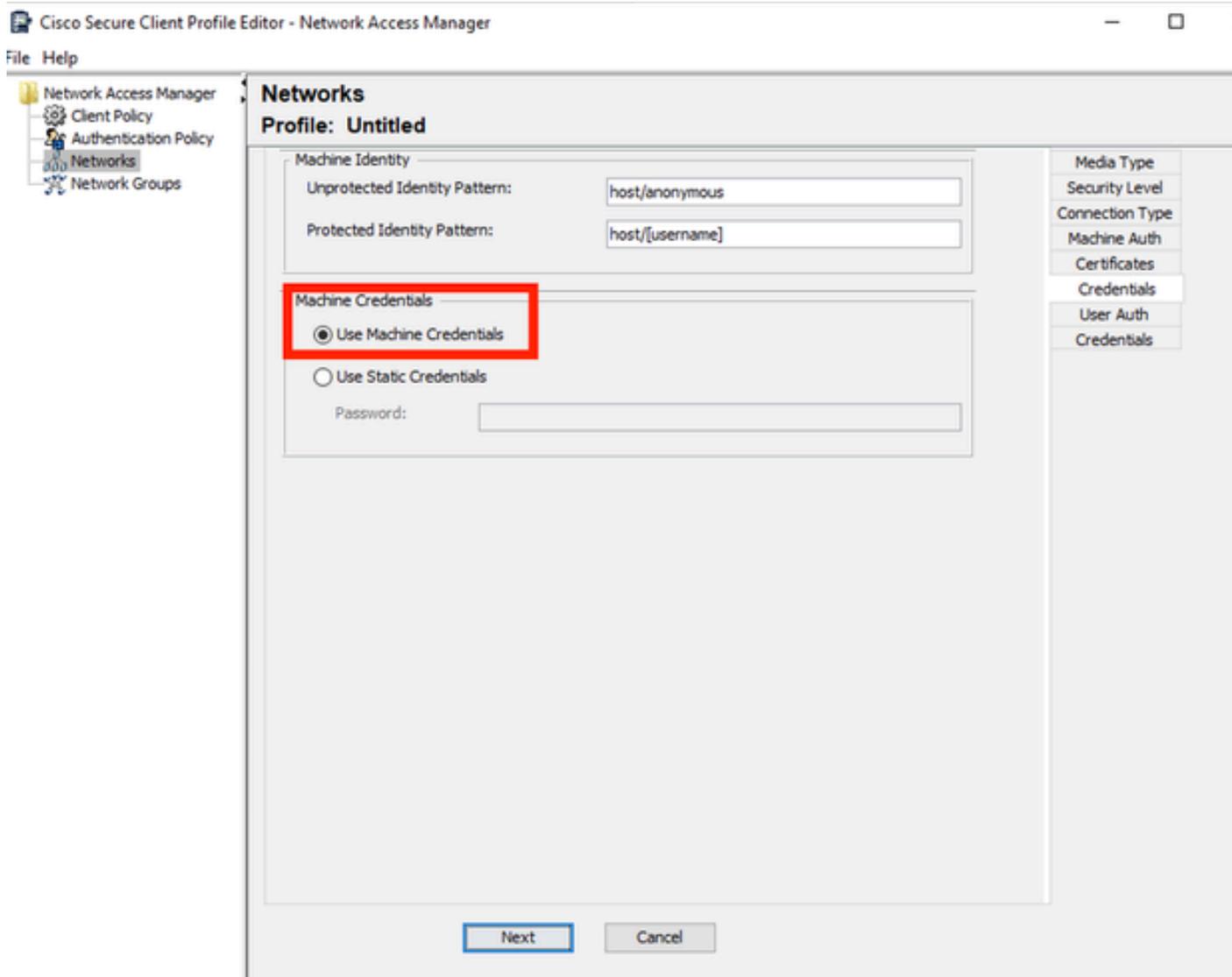
The screenshot shows the 'Certificate Trusted Server Rules' section with a list containing '<new>' and 'Subject Alternative Name ends with c.com'. Below the list are fields for 'Certificate Field' (Subject Alt. Name), 'Match' (exactly matches), and 'Value'. There are 'Add' and 'Save' buttons. The 'Certificate Trusted Authority' section has two radio button options: 'Trust any Root Certificate Authority (CA) Installed on the OS' (selected) and 'Include Root Certificate Authority (CA) Certificates'. Below these are 'Add' and 'Remove' buttons. At the bottom of the wizard are 'Next' and 'Cancel' buttons. On the right side, a vertical menu lists: Media Type, Security Level, Connection Type, Machine Auth, Certificates (highlighted), Credentials, User Auth, Certificates, and Credentials.

Machine Auth Server Certificate Trustセクション

Certificate Trusted Authorityでは、2つのオプションを選択できます。このシナリオでは、RADIUS EAP証明書に署名した特定のCA証明書を追加する代わりに、オプションTrust any Root Certificate Authority (CA) Installed on the OSを使用します。

このオプションを使用すると、ユーザ証明書の管理プログラム(Current User > Trusted Root Certification Authorities > Certificates)に含まれている証明書によって署名されたすべてのEAP証明書がWindowsによって信頼されます。

[Next] をクリックします。



マシン認証クレデンシャルセクション

Machine CredentialsセクションでUse Machine Credentialsを選択します。

[Next] をクリックします。

File Help

**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

Next Cancel

User Authenticationセクション

User Authでは、EAP MethodとしてEAP-FASTを選択します。

EAP-FAST設定セクションでデフォルト値を変更しないでください。

Inner Method based on credentials sourceセクションでは、方式としてAuthenticate using a PasswordとEAP-MSCHAPv2を選択します。

Use PACsを選択します。

[Next] をクリックします。

CertificatesセクションのCertificate Trusted Server Rulesで、このルールはCommon Name ends with c.comです。次の設定は、EAP PEAPフロー中にサーバが使用する証明書用です。ご使用の環境でISEを使用している場合は、ポリシーサーバノードEAP証明書の共通名を使用できます。

## Networks

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

The screenshot shows the 'Networks' configuration window for a profile named 'C:\Users\LAB 5\Desktop\EAP FAST\configuration.xml'. The window is divided into several sections:

- Certificate Trusted Server Rules:** A list box contains one rule: 'Common Name ends with c.com', which is highlighted in blue and has a red box around it. Below the list box is a table with columns 'Certificate Field', 'Match', and 'Value'. The table contains one row: 'Common Name' (with a dropdown arrow), 'ends with' (with a dropdown arrow), and 'c.com'. Below the table are 'Remove' and 'Save' buttons.
- Certificate Trusted Authority:** Two radio button options are present: 'Trust any Root Certificate Authority (CA) Installed on the OS' (which is selected) and 'Include Root Certificate Authority (CA) Certificates'. Below these options is an empty list box and 'Add' and 'Remove' buttons.
- Navigation:** 'Next' and 'Cancel' buttons are located at the bottom of the window.
- Right-Hand Side:** A vertical list of tabs includes 'Media Type', 'Security Level', 'Connection Type', 'Machine Auth', 'Certificates', 'Credentials', 'User Auth', and 'Certificates' (which is highlighted with a red box). 'Credentials' is also visible below the highlighted 'Certificates' tab.

User Auth Server Certificate Trustセクション

Certificate Trusted Authorityでは、2つのオプションを選択できます。このシナリオでは、RADIUS EAP証明書に署名した特定のCA証明書を追加する代わりに、オプションTrust any Root Certificate Authority (CA) Installed on the OSを使用します。

[Next] をクリックします。

## Networks

### Profile: Untitled

User Identity

Unprotected Identity Pattern:

Protected Identity Pattern:

User Credentials

Use Single Sign On Credentials

Prompt for Credentials

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

Use Static Credentials

Password:

Media Type

Security Level

Connection Type

Machine Auth

Certificates

Credentials

User Auth

Certificates

Credentials

Done Cancel

ユーザ認証クレデンシャル

Credentialsセクションでは、User Credentialsセクションだけが変更されます。

オプションPrompt for Credentials > Never Rememberが選択されています。したがって、認証のたびに、認証するユーザは自分のクレデンシャルを入力する必要があります。

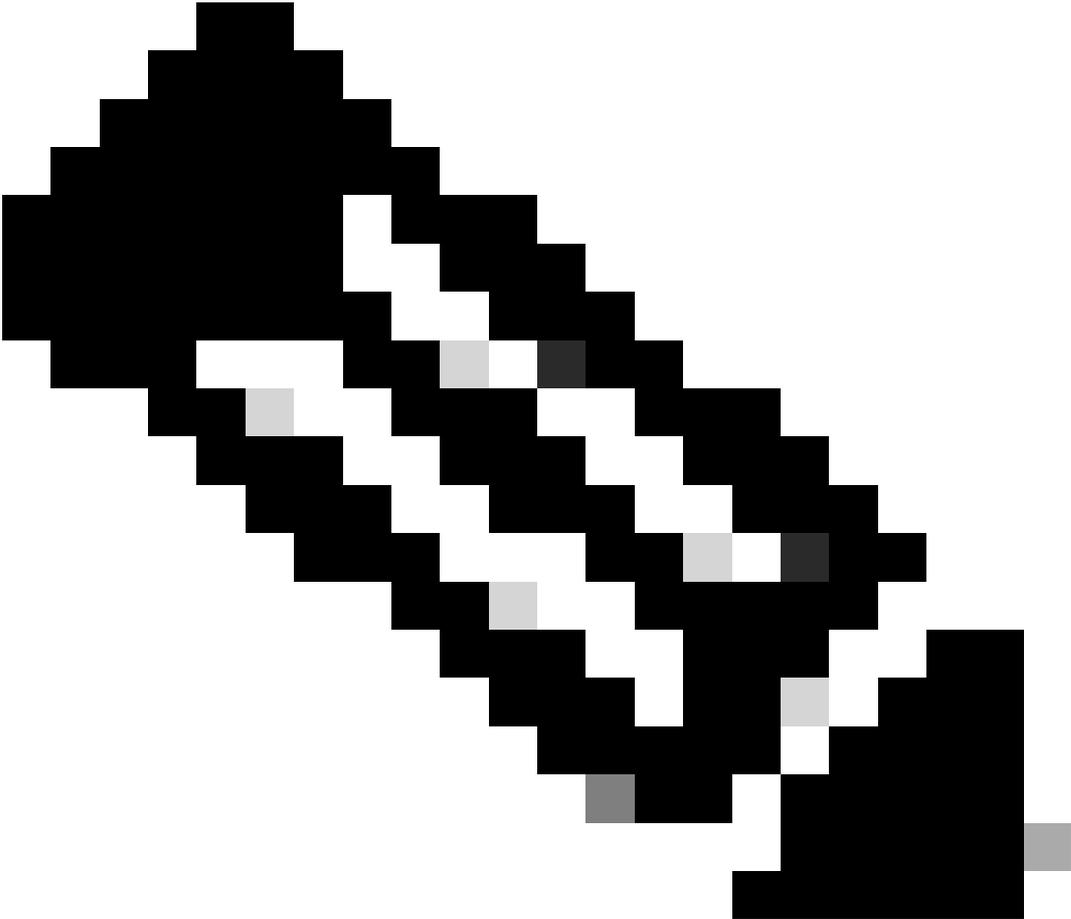
Doneボタンをクリックします。

File > Save asの順に選択し、Secure Client Network Access Manager(SCA)プロファイルをconfiguration.xmlとして保存します。

作成したばかりのプロファイルをSecure Client Network Access Managerで使用するには、次のディレクトリにあるconfiguration.xmlファイルを新しいファイルで置き換えます。

C:\ProgramData\Cisco\Ciscoセキュアクライアント\Network Access Manager\system

---



注：ファイルはconfiguration.xmlという名前である必要があります。そうでない場合は機能しません。

---

## 6. シナリオ3:EAP TLSユーザ証明書認証のためのセキュアなクライアントNAMサブリカントの設定

NAMプロファイルエディタを開き、Networksセクションに移動します。

[Add] をクリックします。

## Networks

Profile: Untitled

### Network

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

Add...

Edit...

Delete

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

Network Creationセクション

ネットワークプロファイルに名前を付けます。この例では、名前付きはこのシナリオで使用されるEAPプロトコルと一致します。

Group MembershipにGlobalを選択します。有線ネットワークメディアです

**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セクション

[Next] をクリックします。

Authenticating Networkを選択し、Security Levelセクションの残りのオプションではデフォルト値を変更しないでください。

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

セキュリティレベル

このシナリオは、証明書を使用したユーザ認証を対象としています。このため、オプションUser Connectionが使用されます。

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

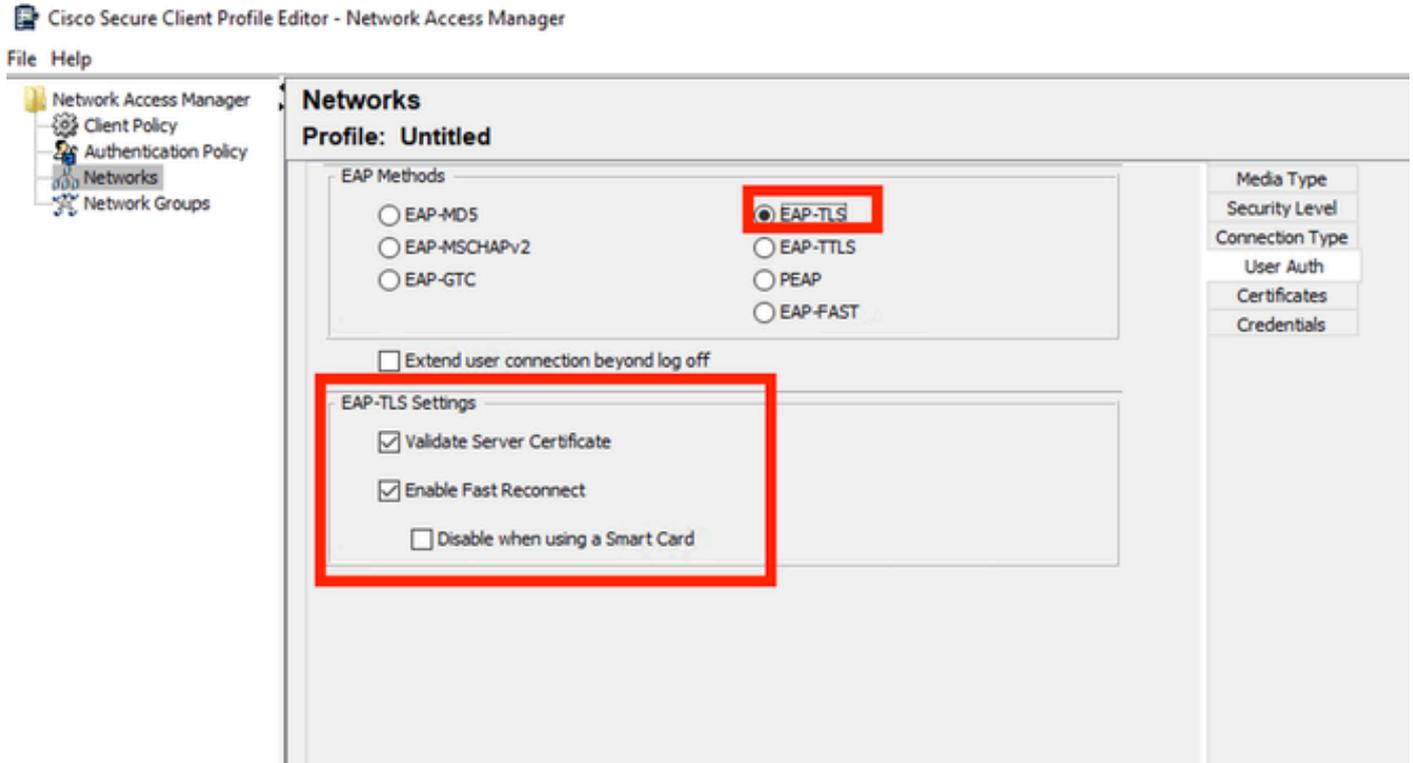
Connection Type

User Auth

Credentials

接続タイプ

EAP方式としてEAP-TLSを設定します。EAP-TLS設定セクションでデフォルト値を変更しないでください。



User Authセクション

Certificatesセクションで、AAA EAP-TLS証明書と一致するルールを作成します。ISEを使用している場合は、Administration > System > Certificatesセクションでこのルールを確認します。

Certificate Trusted Authorityセクションで、Trust any Root Certificate Authority (CA) installed on the OSを選択します。

The screenshot shows the 'Networks' section of the Cisco Secure Client Profile Editor. The main window is titled 'Profile: Untitled'. On the left, a navigation pane shows 'Network Access Manager', 'Client Policy', 'Authentication Policy', 'Networks', and 'Network Groups'. The 'Networks' section is active, displaying two main configuration areas:

- Certificate Trusted Server Rules:** A list box contains one rule: 'Common Name ends with c.com'. Below this is a table for defining rules:

Certificate Field	Match	Value
Subject Alt. Name	exactly matches	

Buttons for 'Add' and 'Save' are located below the table.

- Certificate Trusted Authority:** Two radio buttons are present: 'Trust any Root Certificate Authority (CA) Installed on the OS' (which is selected) and 'Include Root Certificate Authority (CA) Certificates'. Below these is an empty list box with 'Add' and 'Remove' buttons.

At the bottom of the main window are 'Next' and 'Cancel' buttons. On the right side, a vertical menu contains 'Media Type', 'Security Level', 'Connection Type', 'User Auth', 'Certificates', and 'Credentials'. The 'Certificates' option is highlighted with a red box.

ユーザ認証サーバ証明書の信頼設定

[Next] をクリックします。

User Credentialsセクションでは、最初の部分のデフォルト値を変更しないでください。

## Networks

### Profile: Untitled

User Identity

Unprotected Identity Pattern:

User Credentials

Use Single Sign On Credentials (Requires Smart Card)

Prompt for Credentials

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

Certificate Source

Smart Card or OS certificates

Smart Card certificates only

Remember Smart Card Pin

Remember Forever

Remember while User is Logged On

Never Remember

Smart Card Removal Policy

Disconnect from Network

Use Certificate Matching Rule (Max 10)

Rule Logic  OR  AND

Field	Operator	Value

Media Type

Security Level

Connection Type

User Auth

Certificates

Credentials

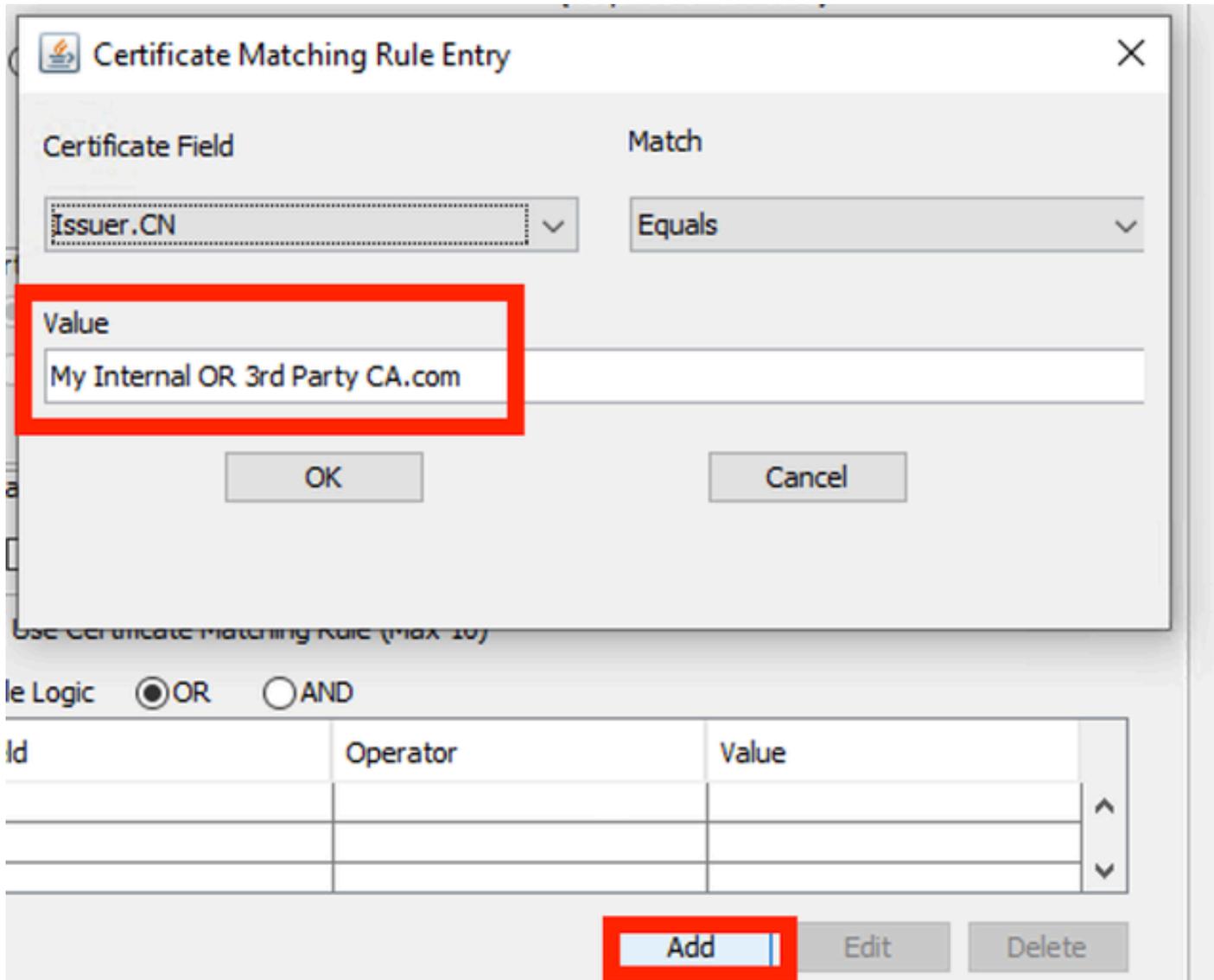
Done

Cancel

User Auth Credentialsセクション

EAP TLSプロセス中にユーザが送信するID証明書と一致するルールを設定することが重要です。これを行うには、Use Certificate Maching Rule (Max 10)の横にあるチェックボックスをクリックします。

[Add] をクリックします。

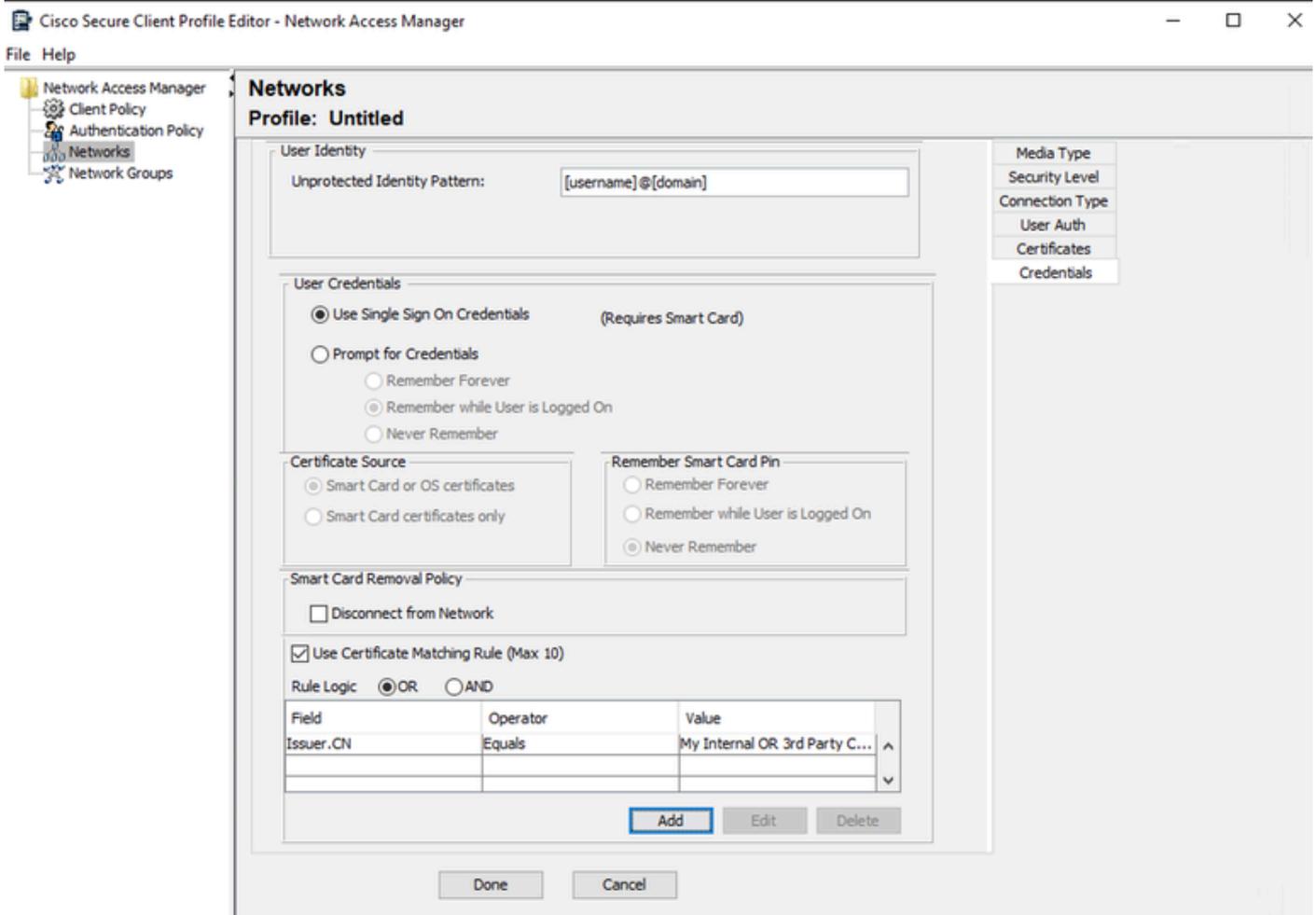


The image shows a 'Certificate Matching Rule Entry' dialog box. It has two dropdown menus: 'Certificate Field' set to 'Issuer.CN' and 'Match' set to 'Equals'. Below these is a 'Value' text box containing 'My Internal OR 3rd Party CA.com'. At the bottom of the dialog are 'OK' and 'Cancel' buttons. Below the dialog, there is a section for 'Rule Logic' with radio buttons for 'OR' (selected) and 'AND'. Below that is a table with columns 'Id', 'Operator', and 'Value'. At the bottom right of the table area are 'Add', 'Edit', and 'Delete' buttons.

Id	Operator	Value

Certificate Matching Ruleウィンドウ

My Internal OR 3rd Party CA.comという文字列を、ユーザ証明書のCNに置き換えます。



User Auth Certificate Credentialsセクション

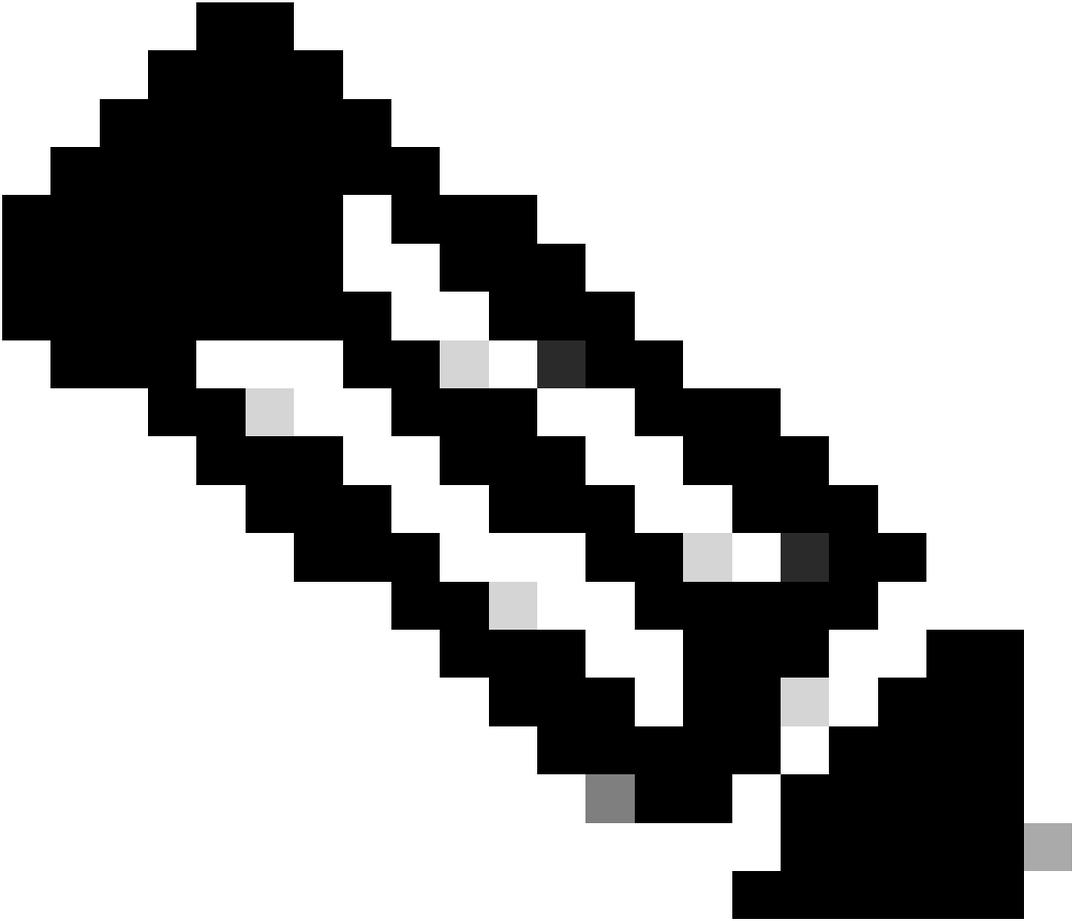
Doneをクリックして、設定を終了します。

File > Save asの順に選択して、Secure Client Network Access Managerプロファイルを configuration.xmlとして保存します。

作成したばかりのプロファイルをSecure Client Network Access Managerで使用するには、次のディレクトリにあるconfiguration.xmlファイルを新しいファイルで置き換えます。

C:\ProgramData\Cisco\Ciscoセキュアクライアント\Network Access Manager\system

---



注：ファイルはconfiguration.xmlという名前である必要があります。そうでない場合は機能しません。

---

## 7. シナリオ1 PEAP MSCHAPv2に基づく認証を許可するためのISR 1100およびISEの設定

ISR 1100ルータを設定します。

このセクションでは、dot1xを機能させるためにNADが必要とする基本設定について説明します。

---

注：マルチノードISE導入の場合は、ポリシーサーバノード(PSN)ペルソナが有効になっている任意のノードをポイントします。これを確認するには、Administration > System > DeploymentタブでISEに移動します。

---

```
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>
```

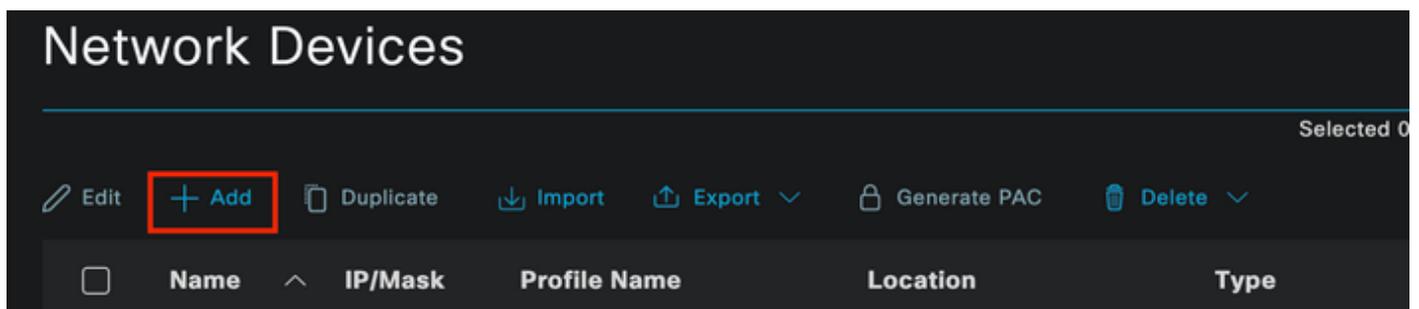
```
!  
!  
aaa group server radius ISE-CLUSTER  
  server name ISE-PSN-1  
!  
interface GigabitEthernet0/1/0  
  description "Endpoint that supports dot1x"  
  switchport access vlan 15  
  switchport mode access  
  authentication host-mode multi-auth  
  authentication order dot1x mab  
  authentication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

Identity Service Engine 3.2を設定します。

ネットワークデバイスを設定します。

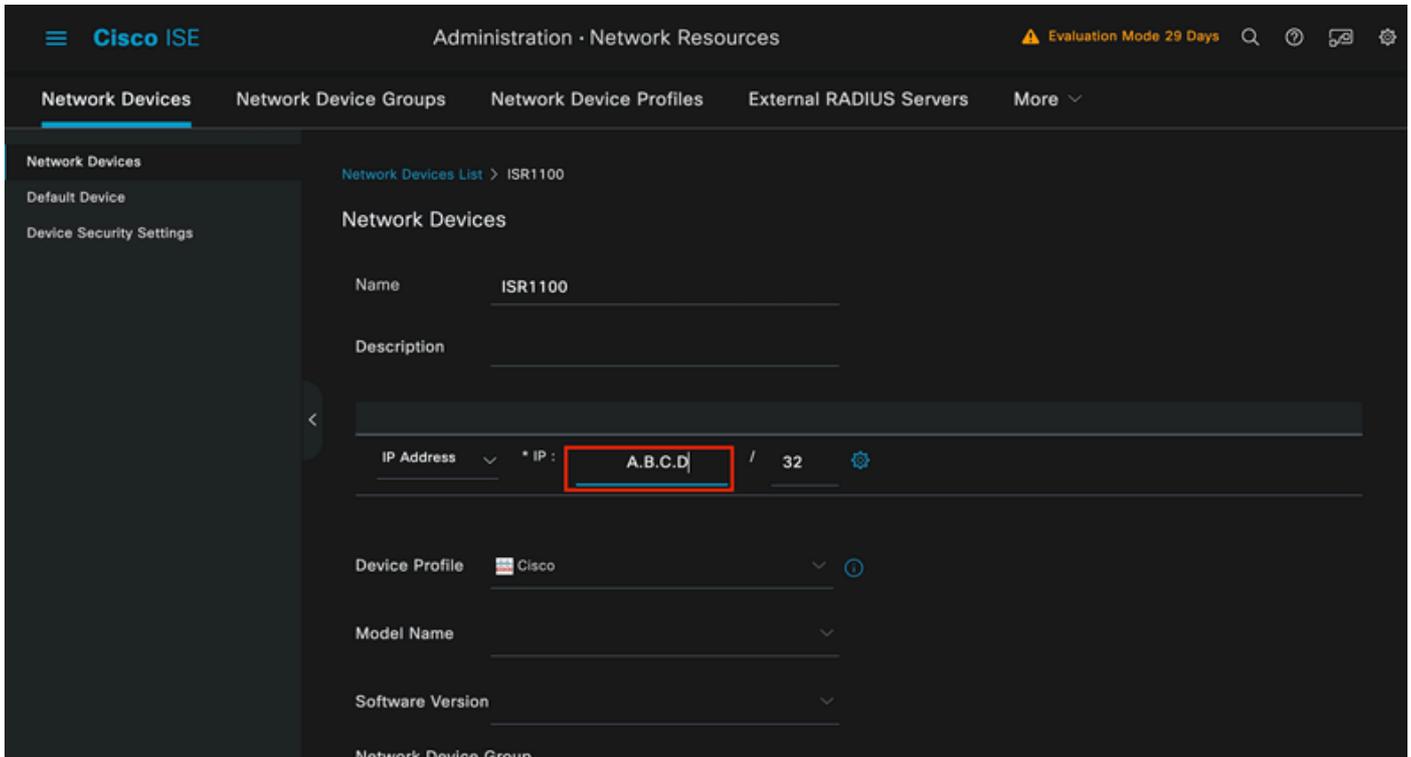
ISE Administration > Network Resources > Network DevicesにISR NADを追加します。

[Add] をクリックします。



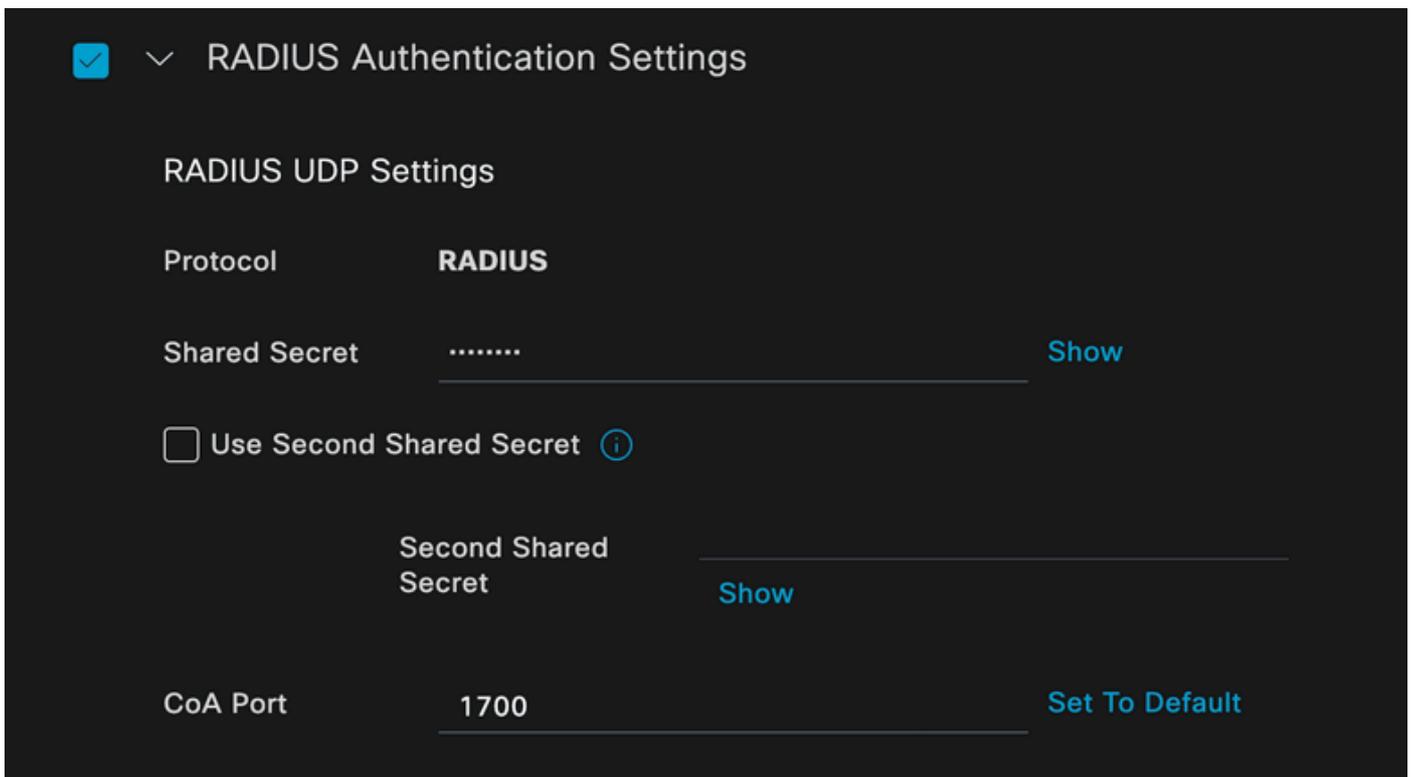
Network Deviceセクション

作成するNADに名前を割り当てます。ネットワークデバイスのIPを追加します。



ネットワークデバイスの作成

同じページの下部に、ネットワークデバイス設定で使用したものと同一共有秘密を追加します。



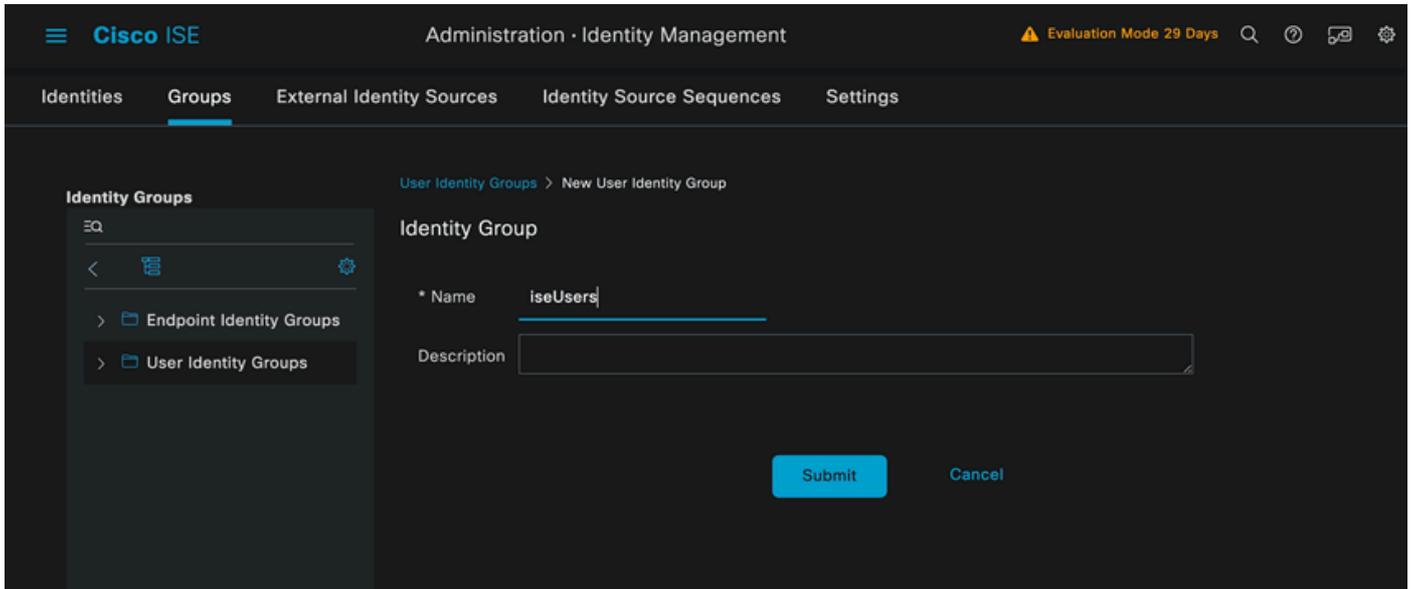
ネットワークデバイスのRadius設定

変更を保存します。

エンドポイントの認証に使用されるIDを設定します。

ISEローカル認証が使用されます。外部ISE認証については、この記事では説明しません。

Administration > Identity Management > Groupsタブに移動し、ユーザが属するグループを作成します。このデモンストレーション用に作成したIDグループはiseUsersです。

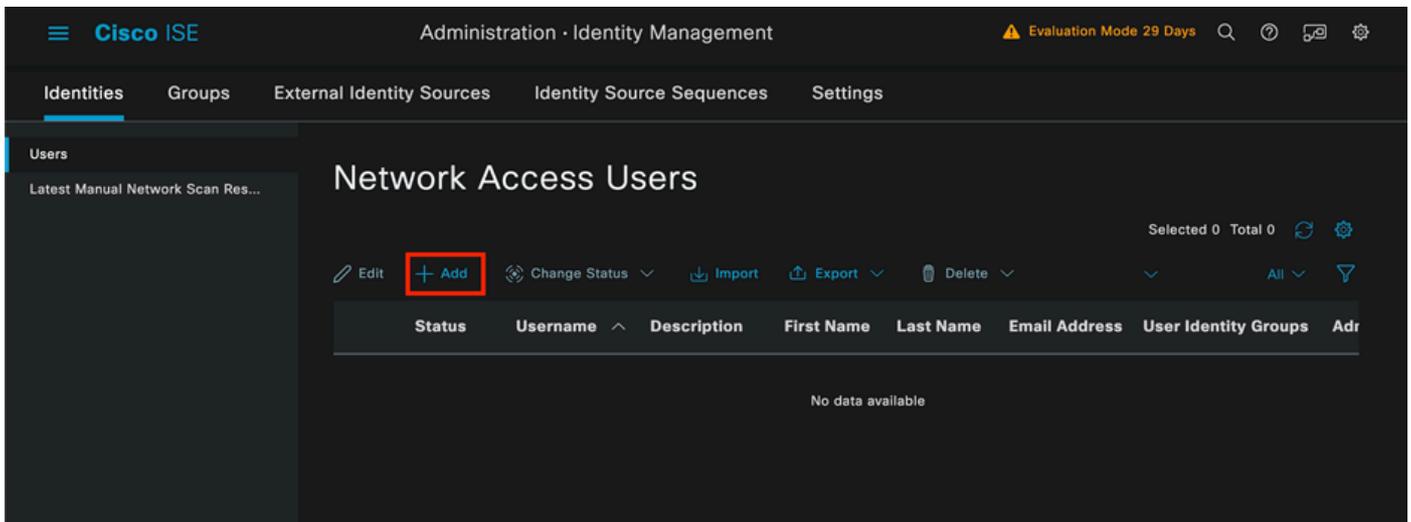


IDグループの作成

[Submit] をクリックします。

Administration > Identity Management > Identityタブに移動します。

[Add] をクリックします。



Network Access Usersセクション

必須フィールドの一部として、ユーザの名前で始まります。この例では、ユーザ名iseiscoolを使用しています。

### Network Access User

\* Username

Status  Enabled ▼

Account Name Alias  ⓘ

Email

ネットワークアクセスユーザの作成

ユーザにパスワードを割り当てます。VainillaISE97が使用されます。

### 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セクション

ユーザをグループiseUsersに割り当てます。

### User Groups



iseUsers



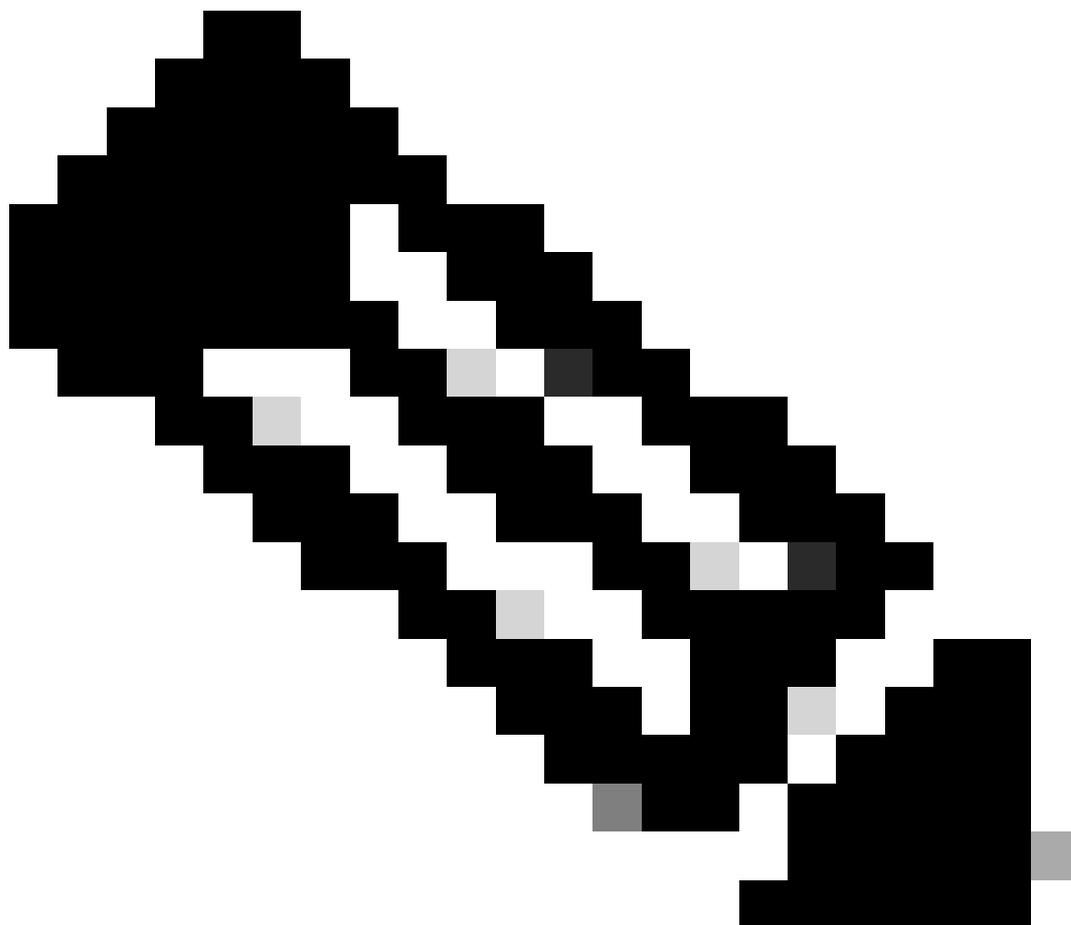
ユーザグループの割り当て

ポリシーセットを設定します。

ISEメニュー>ポリシー>ポリシーセットに移動します。

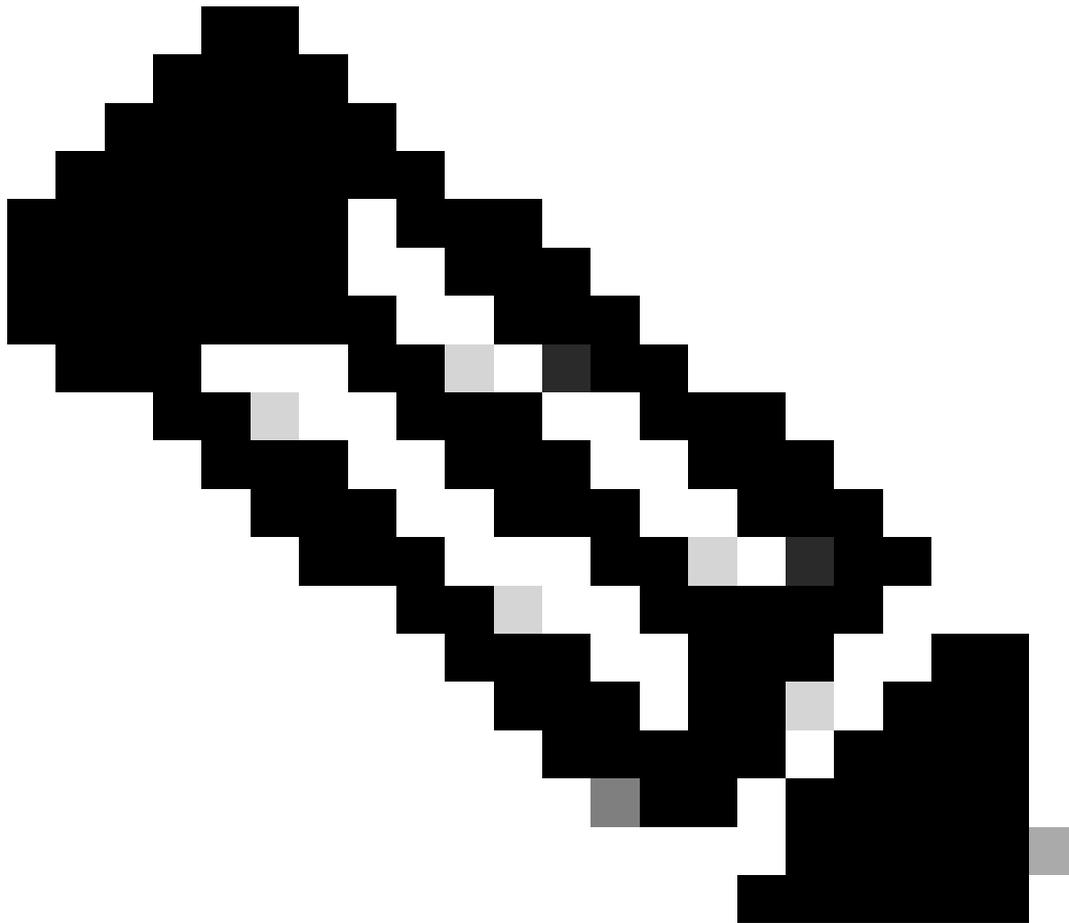
デフォルトのポリシーセットを使用できます。ただし、この例では「Wired」という名前のAPが作成されます。

---

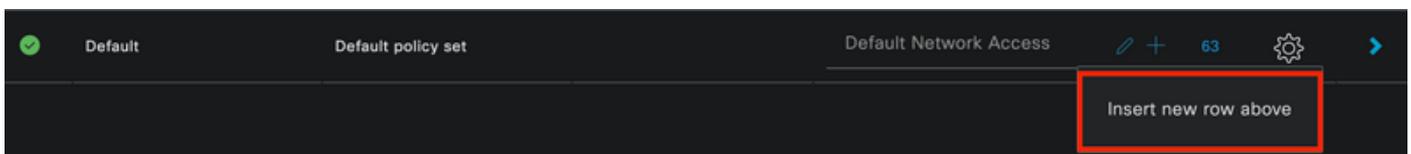


注：ポリシーセットの分類と区別は、トラブルシューティングに役立ちます。

---

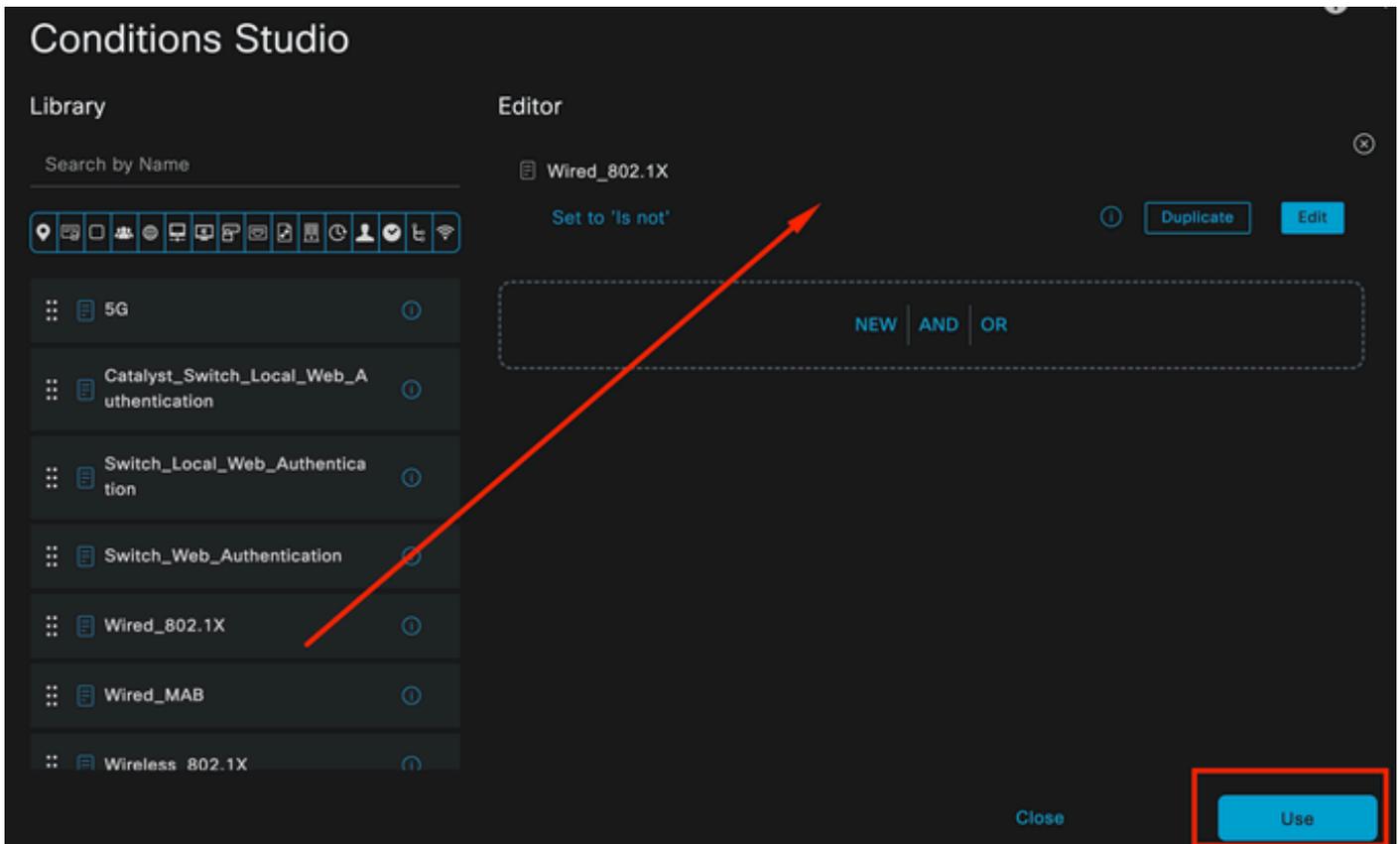


注：追加アイコンまたはプラスアイコンが表示されていない場合は、任意のポリシーセットの歯車アイコンをクリックし、[上に新しい行を挿入]を選択できます。



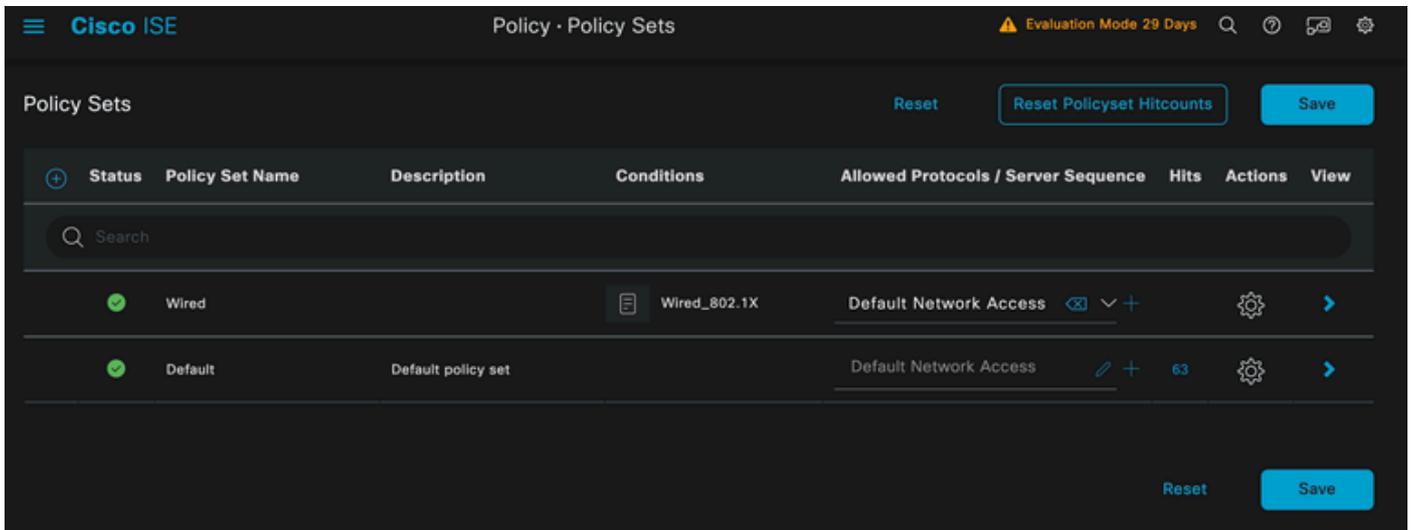
歯車アイコンのオプション

使用されている条件は有線8021xです。これをドラッグして、Useをクリックします。



認証ポリシー条件スタジオ

Allowed ProtocolsセクションでDefault Network Accessを選択します。



ポリシーセットの概要

[Save] をクリックします。

2.d.認証ポリシーと認可ポリシーを設定します。

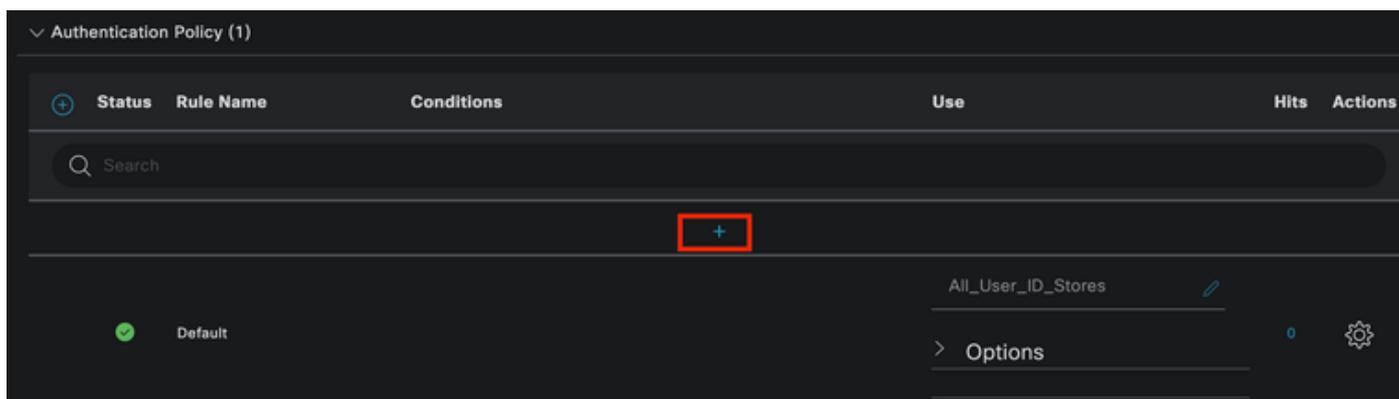
>アイコンをクリックします。



有線ポリシーセット

Authentication Policyセクションを展開します。

+アイコンをクリックします。



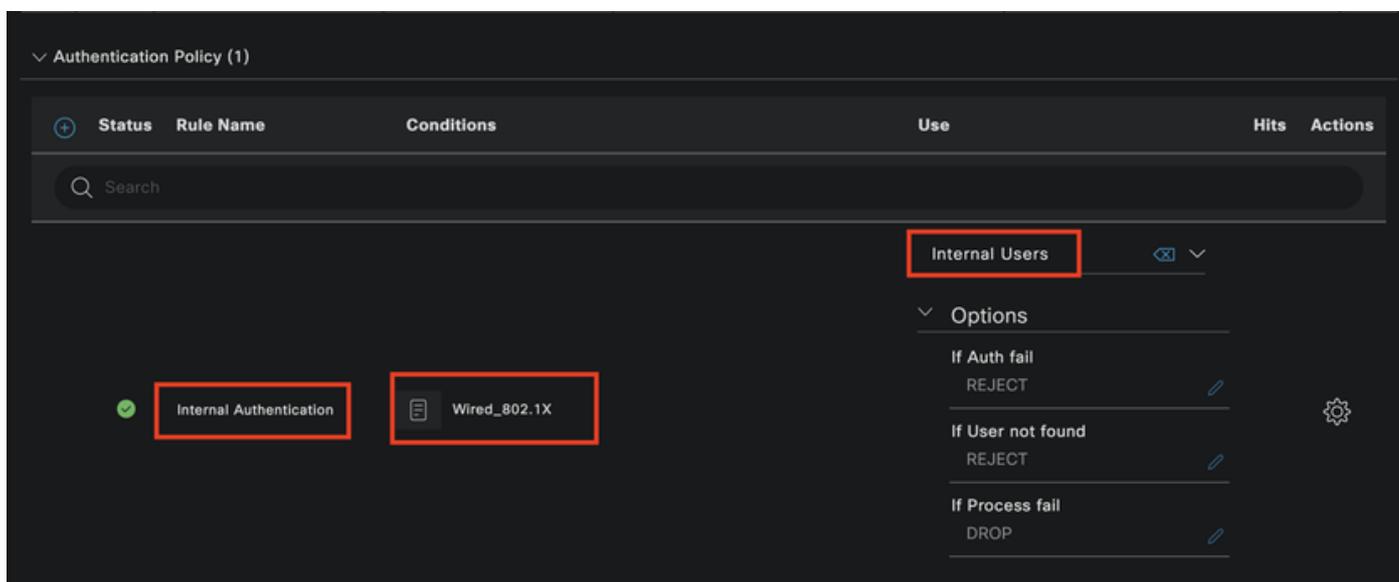
認証ポリシー

認証ポリシーに名前を割り当てます。この例では、「Internal Authentication」を使用しています。

この新しい認証ポリシーの条件列で+アイコンをクリックします。

事前に設定された条件Wired Dot1xが使用されます。

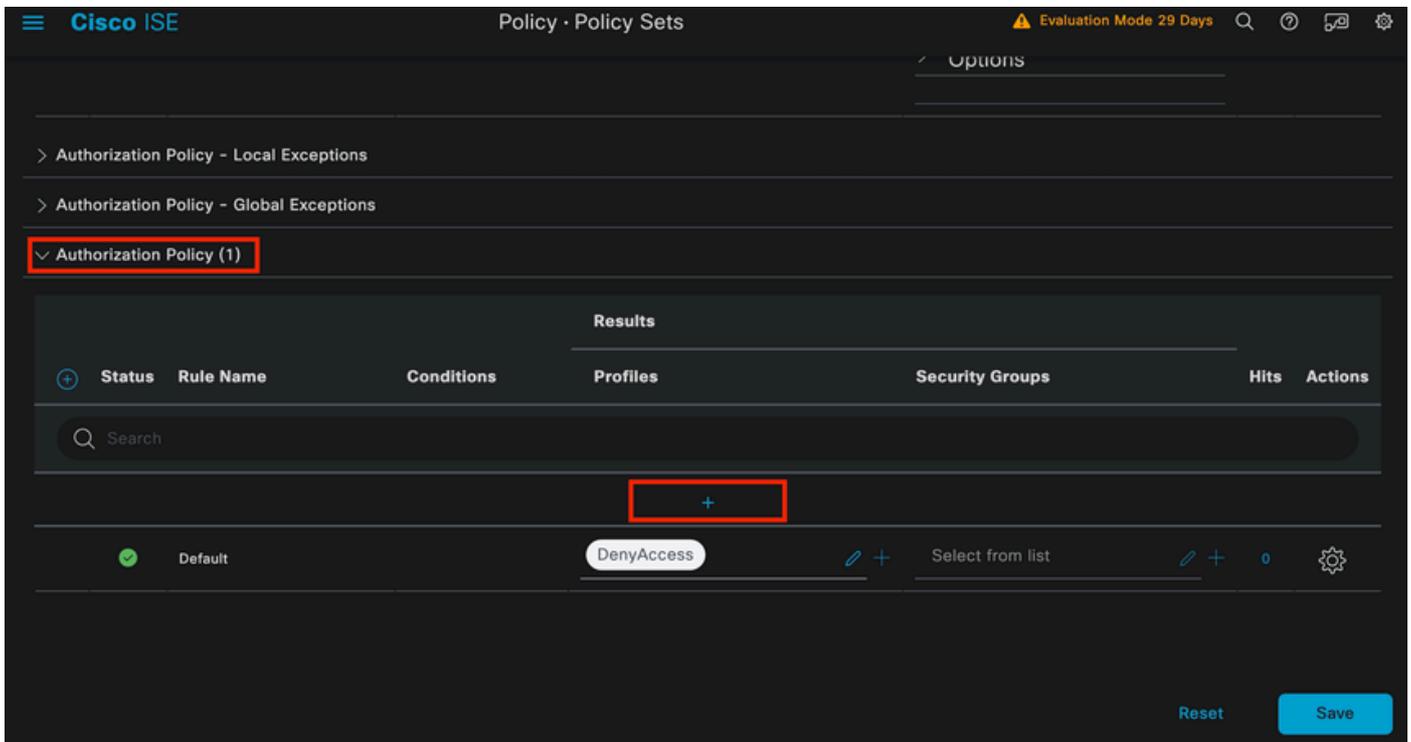
最後に、Use列でInternal Usersを選択します。



認証ポリシー

認可ポリシー

Authorization Policyセクションは、ページの下部にあります。これを展開して、+アイコンをクリックします。



#### 認可ポリシー

最近作成した許可ポリシーに名前を付けます。この設定例では、名前Internal ISE Usersを使用します。

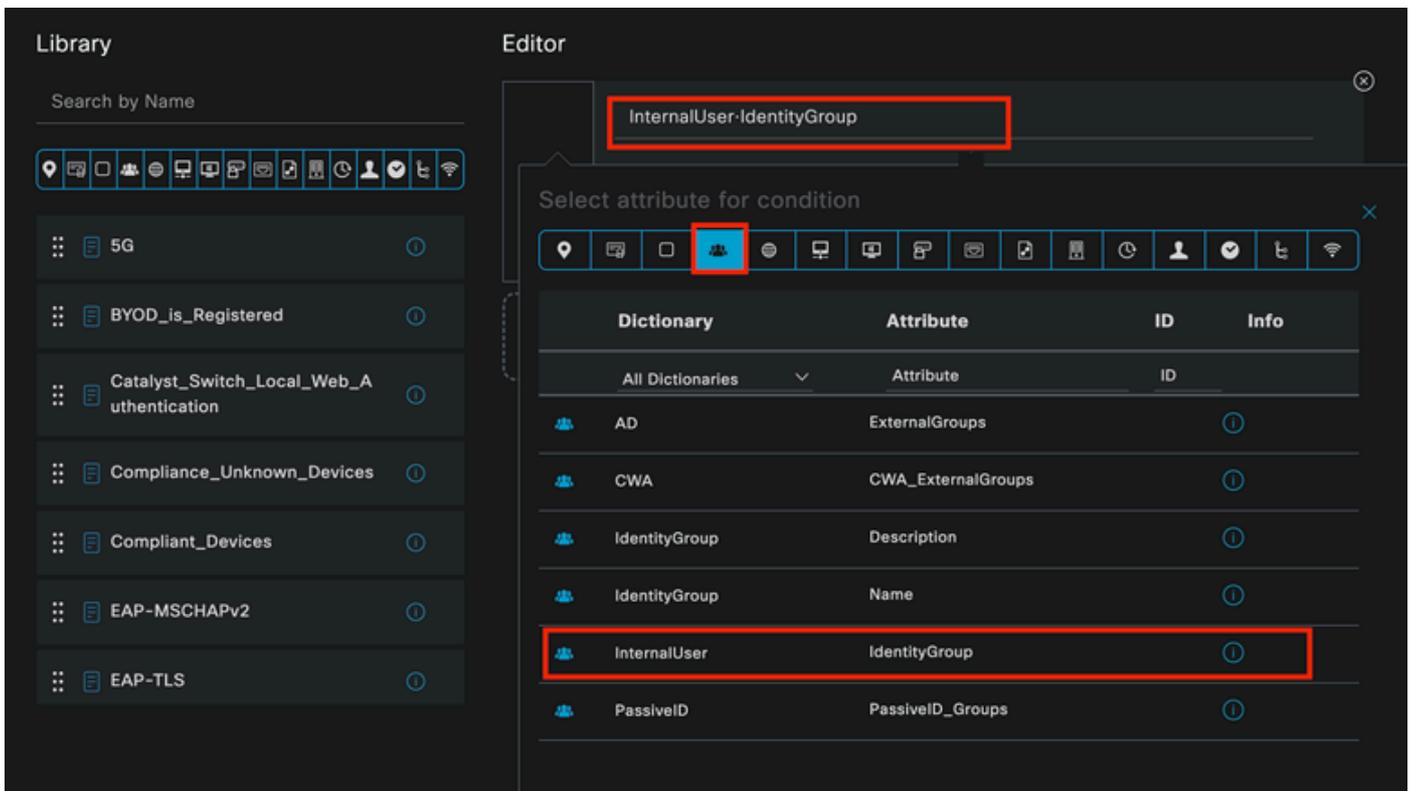
この許可ポリシーの条件を作成するには、Conditions列の+アイコンをクリックします。

グループIseUsersが使用されます。

Attributeセクションをクリックします。

IdentityGroupアイコンを選択します。

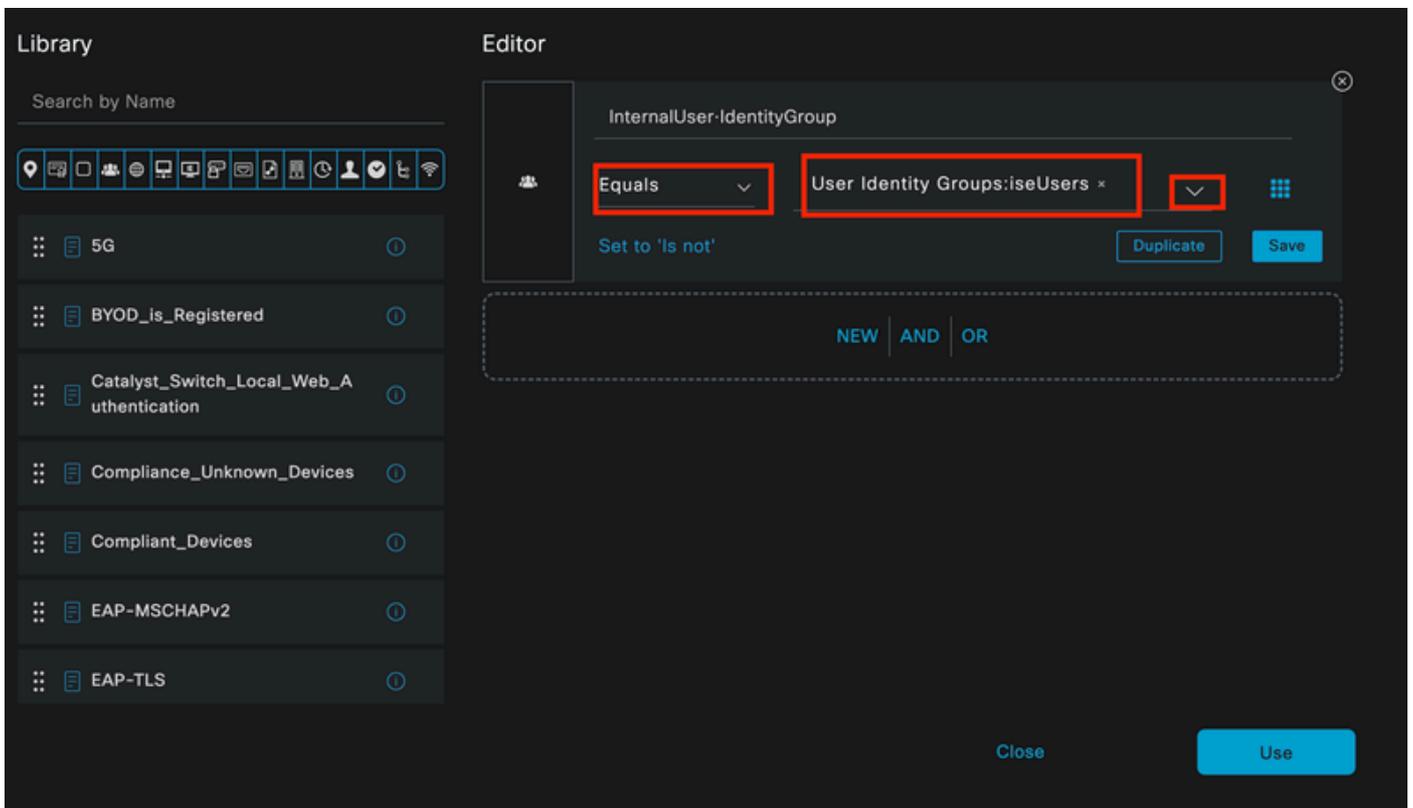
ディクショナリから、IdentityGroup属性に付属するInternalUserディクショナリを選択します。



条件の作成

Equals演算子を選択します。

User Identity Groupsで、グループiseUsersを選択します。



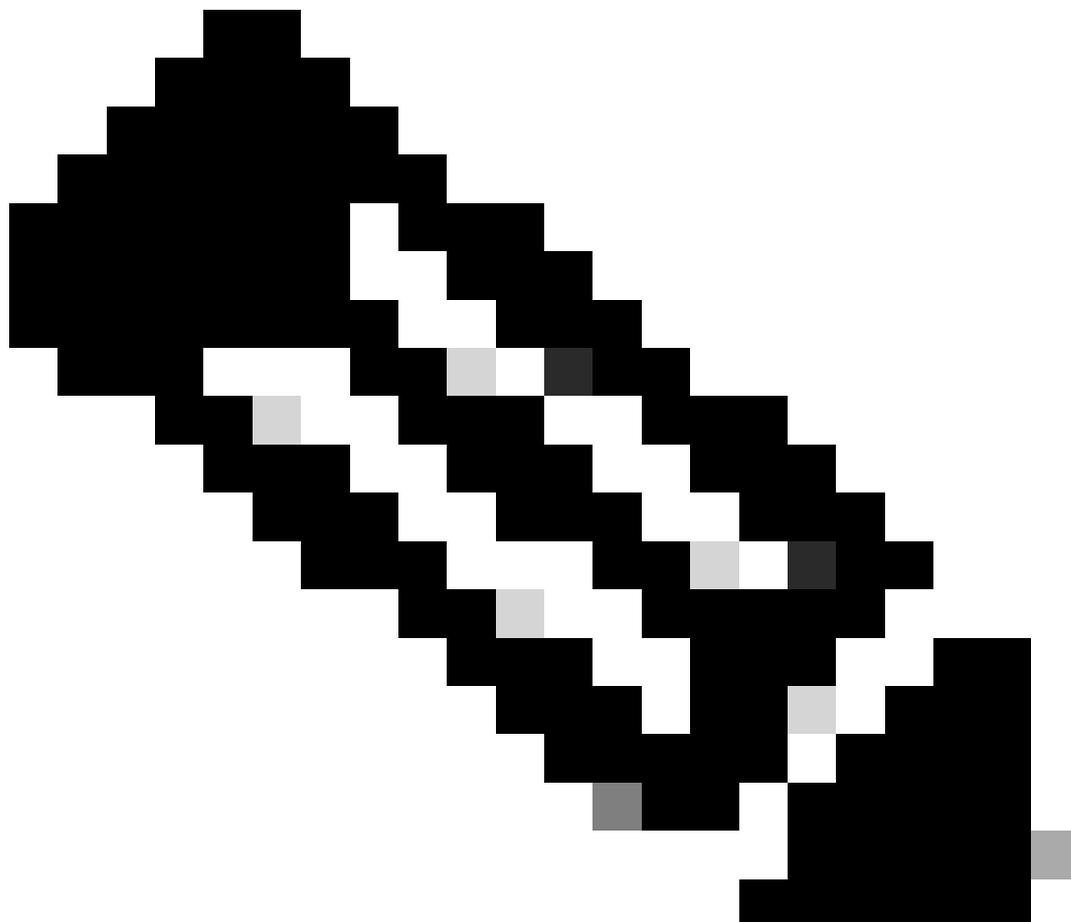
条件の作成

Useをクリックします。

Result認可プロファイルを追加します。

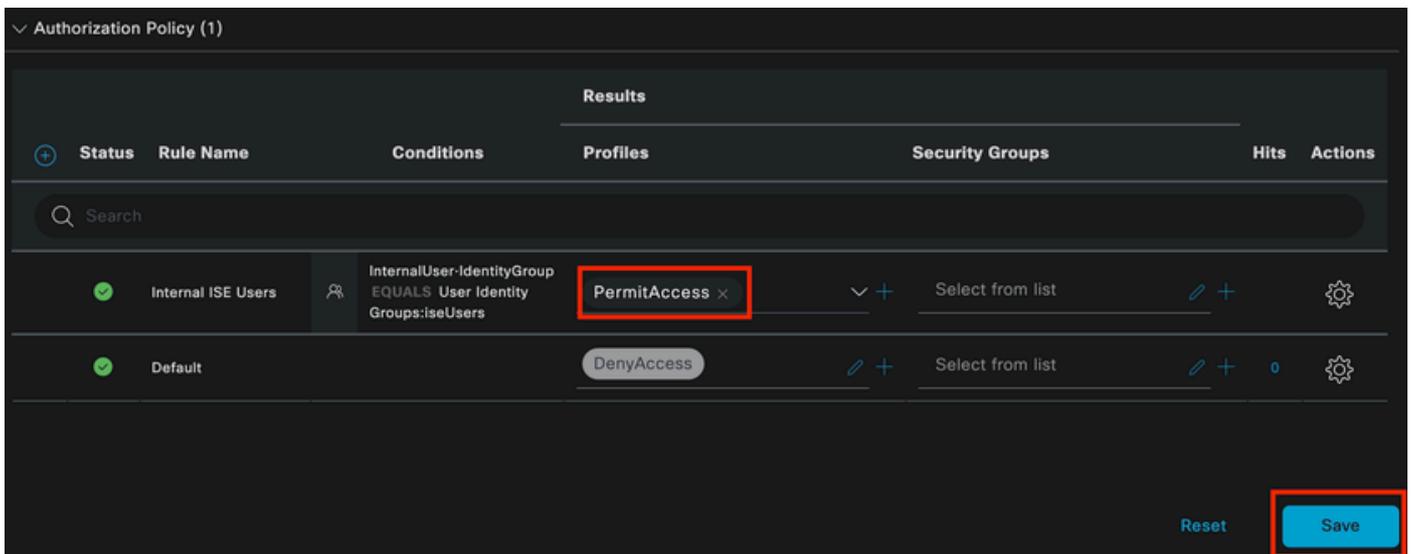
事前に設定されたプロファイルPermit Accessが使用されます。

---



注：この有線Dot1xポリシーセットに一致する、ユーザIDグループISEUsersに属さないISEへの認証は、デフォルトの認可ポリシーに一致し、結果はDenyAccessになることに注意してください。

---



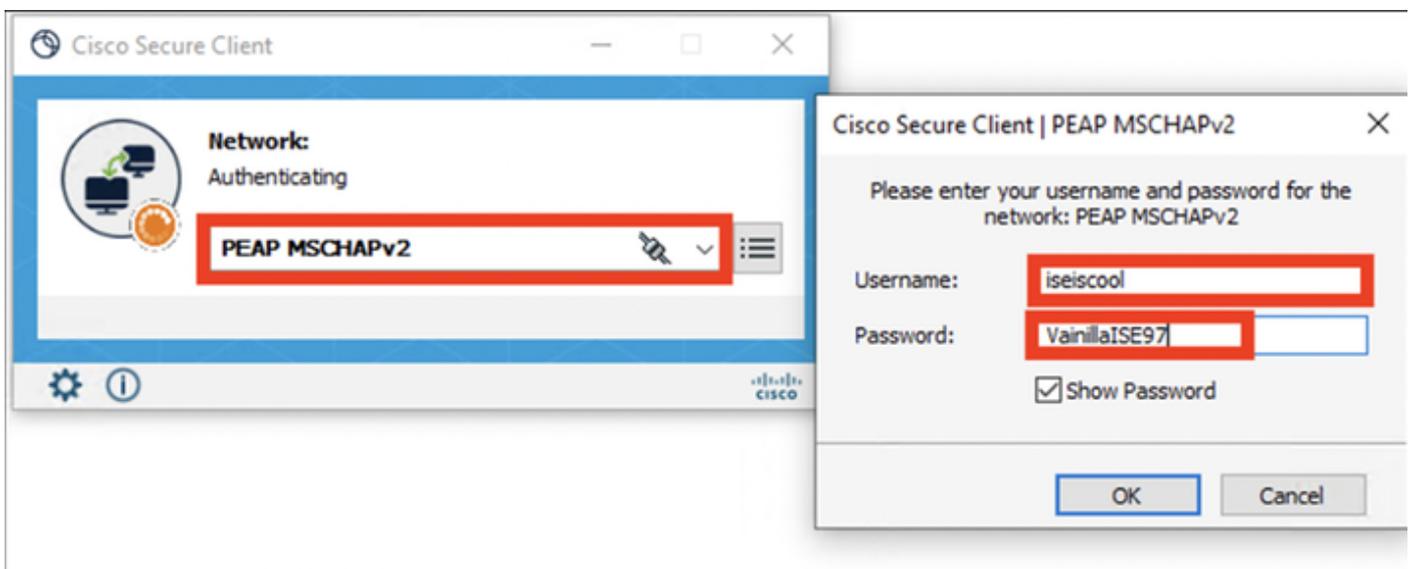
認可ポリシー

[Save] をクリックします。

## 確認

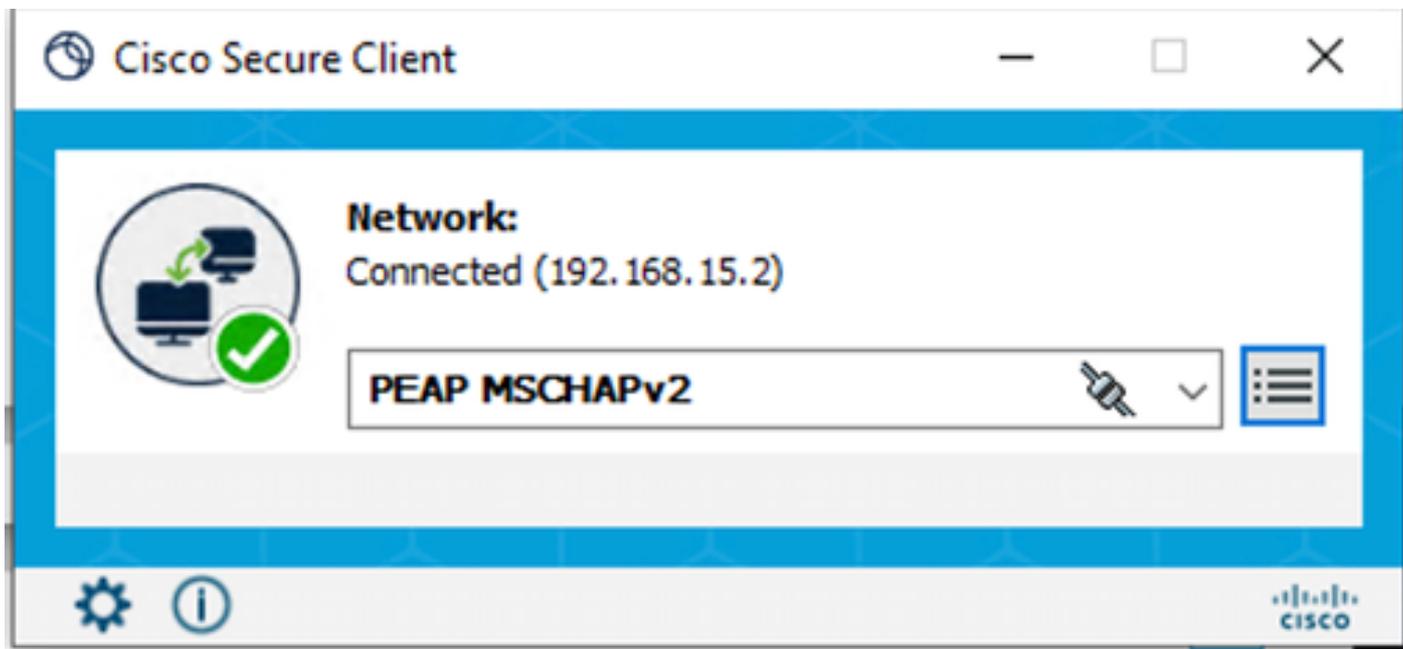
設定が完了すると、Secure Clientによってクレデンシャルの入力を求めるプロンプトが表示され、PEAP MSCHAPv2プロファイルの使用が指定されます。

以前に作成したクレデンシャルが入力されます。



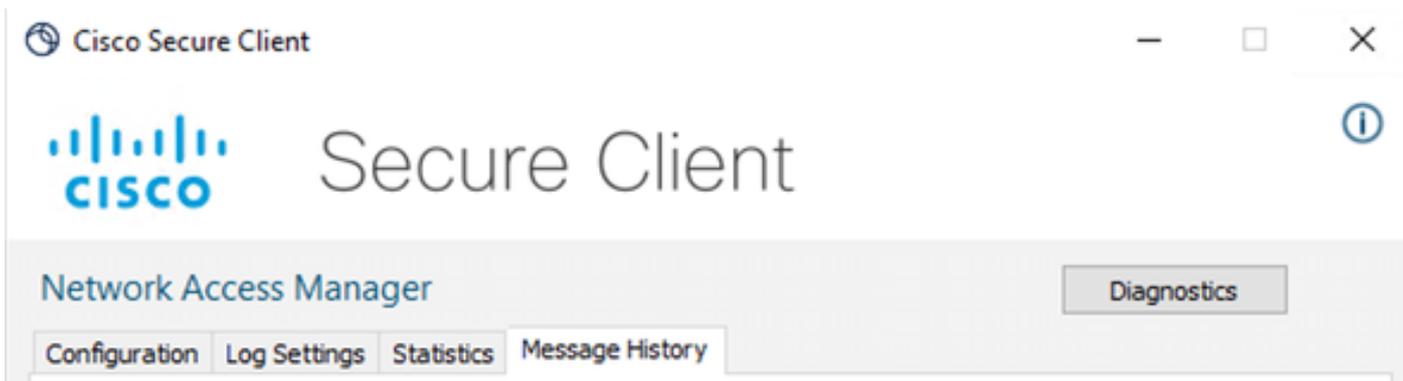
セキュアクライアントNAM

エンドポイントの認証が正しく行われているかどうかを確認します。NAMが接続されていることを表示します。



セキュアクライアントNAM

情報アイコンをクリックし、メッセージ履歴セクションに移動すると、NAMが実行したすべての手順の詳細が表示されます。



クライアントのメッセージ履歴の保護

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

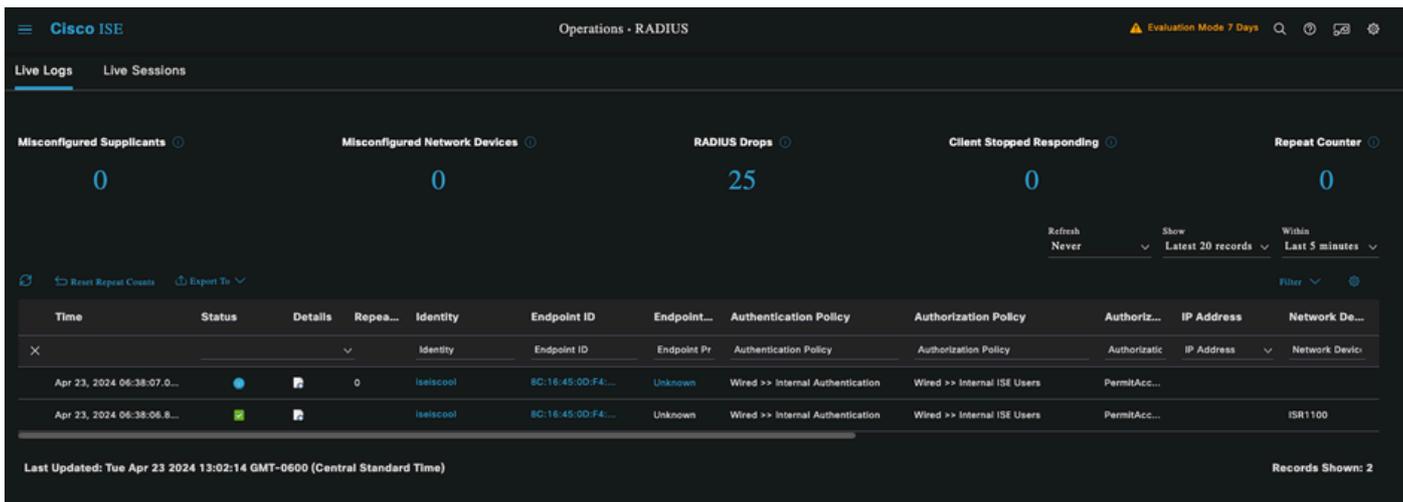
クライアントのメッセージ履歴の保護

ISEから、Operations > Radius LiveLogsの順に移動して、認証の詳細を確認します。次の図に示すように、使用されたユーザ名が表示されます。

また、次のような詳細情報もあります。

- タイムスタンプ.
- MAC アドレス.
- ポリシーセットが使用されました。
- 認証ポリシー。

- 認可ポリシー.
- その他関連情報



ISE RADIUSライブログ

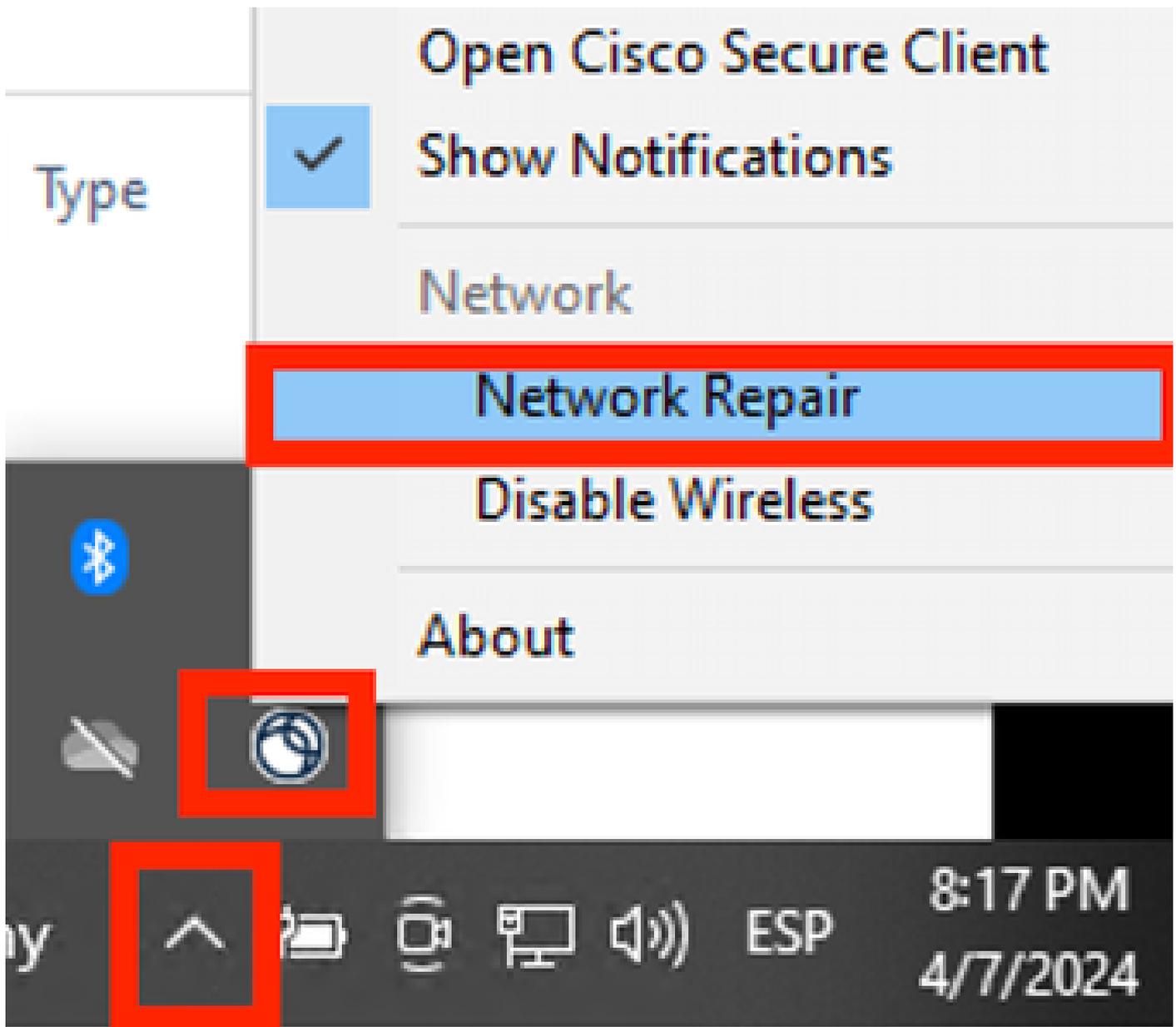
正しいポリシーにヒットすることが確認でき、結果として認証ステータスの成功となるので、設定は正しいと結論付けられます。

## トラブルシューティング

**問題：**セキュアクライアントでNAMプロファイルが使用されていません。

プロファイルエディタで作成した新しいプロファイルがNAMで使用されていない場合は、Secure ClientのNetwork Repairオプションを使用します。

このオプションは、Windowsバー> Circumflexアイコンのクリック> Secure Clientアイコンの右クリック> Network Repairの順に選択すると表示されます。



Network Repairセクション

問題2：さらなる分析のためにログを収集する必要があります。

### 1. NAM拡張ロギングの有効化

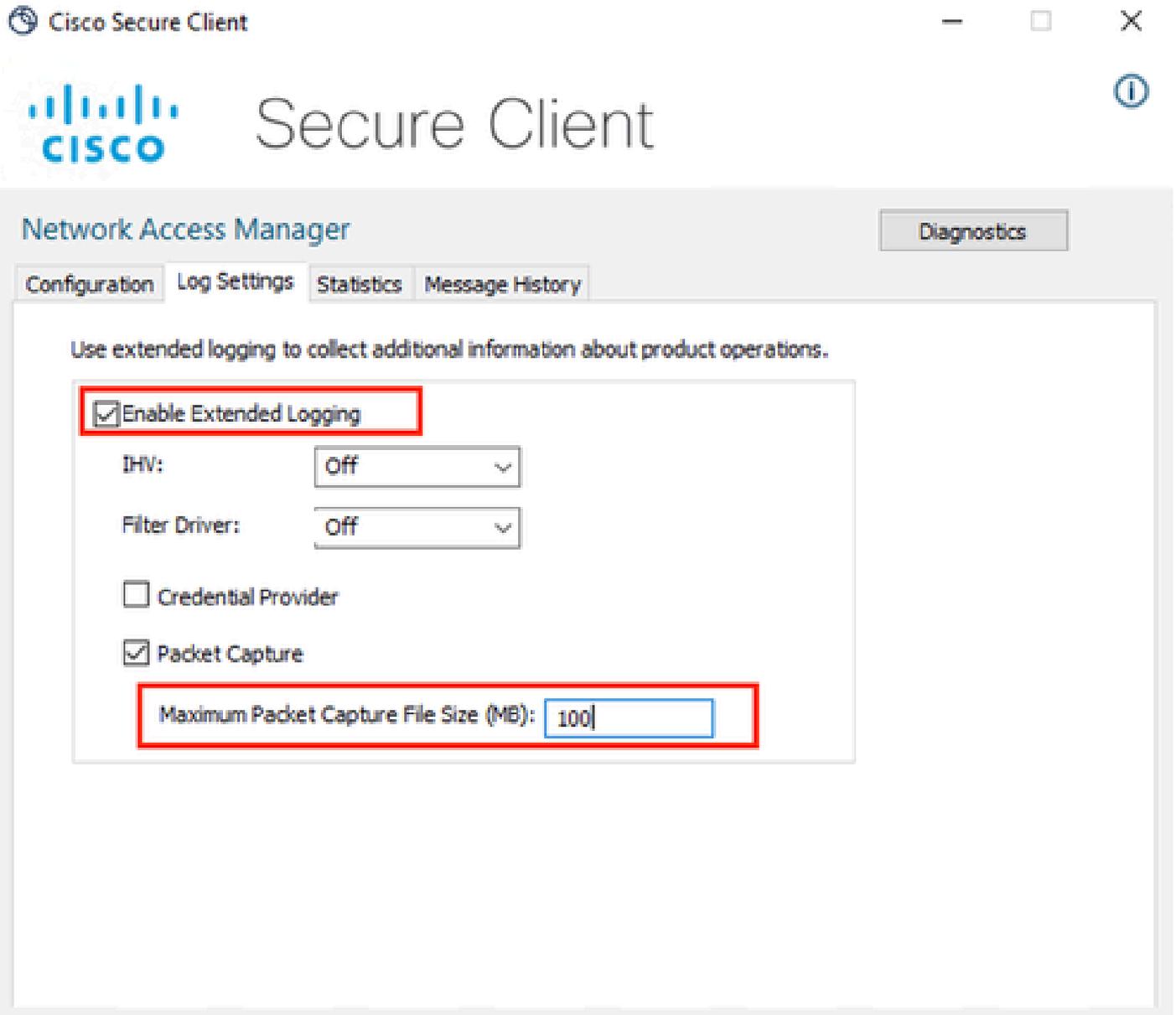
NAMを開き、歯車アイコンをクリックします。



NAMインターフェイス

Log Settingsタブに移動します。Enable Extended Loggingチェックボックスにチェックマークを付けます。

パケットキャプチャファイルサイズを100 MBに設定します。



クライアントNAMログのセキュリティ設定

2. 問題を再現します。

拡張ロギングを有効にすると、ログが生成されてトラフィックがキャプチャされたことを確認するために、問題が複数回再現されます。

3. セキュアクライアントDARTバンドルを収集します。

Windowsから検索バーに移動し、Cisco Secure Client Diagnostics and Reporting Toolと入力します。



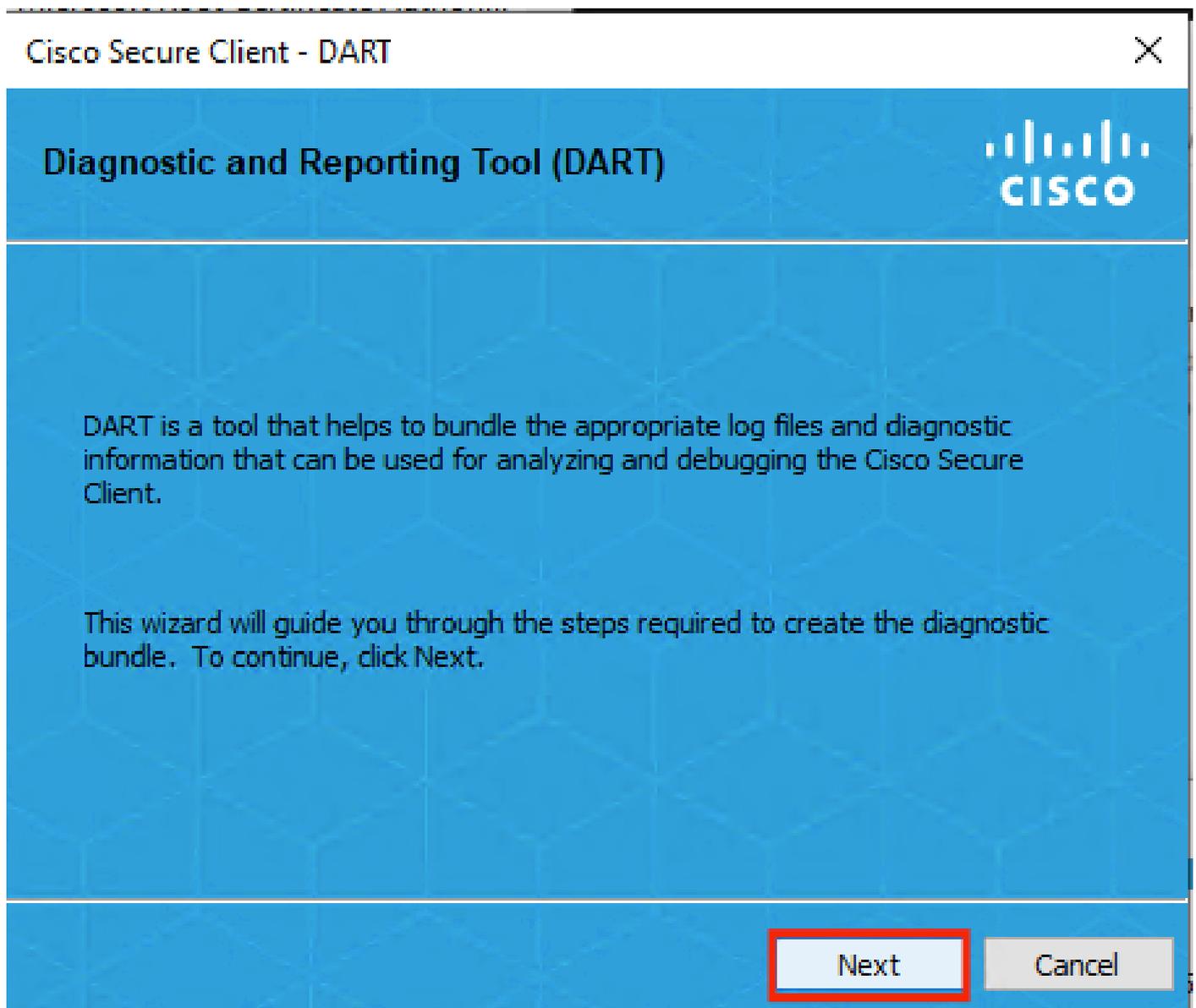
# Cisco Secure Client Diagnostics and Reporting Tool

App

DARTモジュール

インストールプロセス中に、このモジュールもインストールしました。これは、ログと関連する dot1xセッション情報を収集することで、トラブルシューティングプロセスを支援するツールです。

最初のウィンドウでNextをクリックします。



DARTモジュール

再度Nextをクリックして、ログバンドルをデスクトップに保存できるようにします。

Cisco Secure Client - DART



## Bundle Creation Option



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

Default - Bundle will be saved to Desktop

Custom

 DART requires administrative privileges to clear Cisco Secure Client logs.

[Clear All Logs](#)

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

DARTモジュール

必要に応じて、Enable Bundle Encryptionチェックボックスにチェックマークを付けます。

## Bundle Encryption Option



Enable Bundle Encryption

Mask Password

Encryption Password

Confirm Password

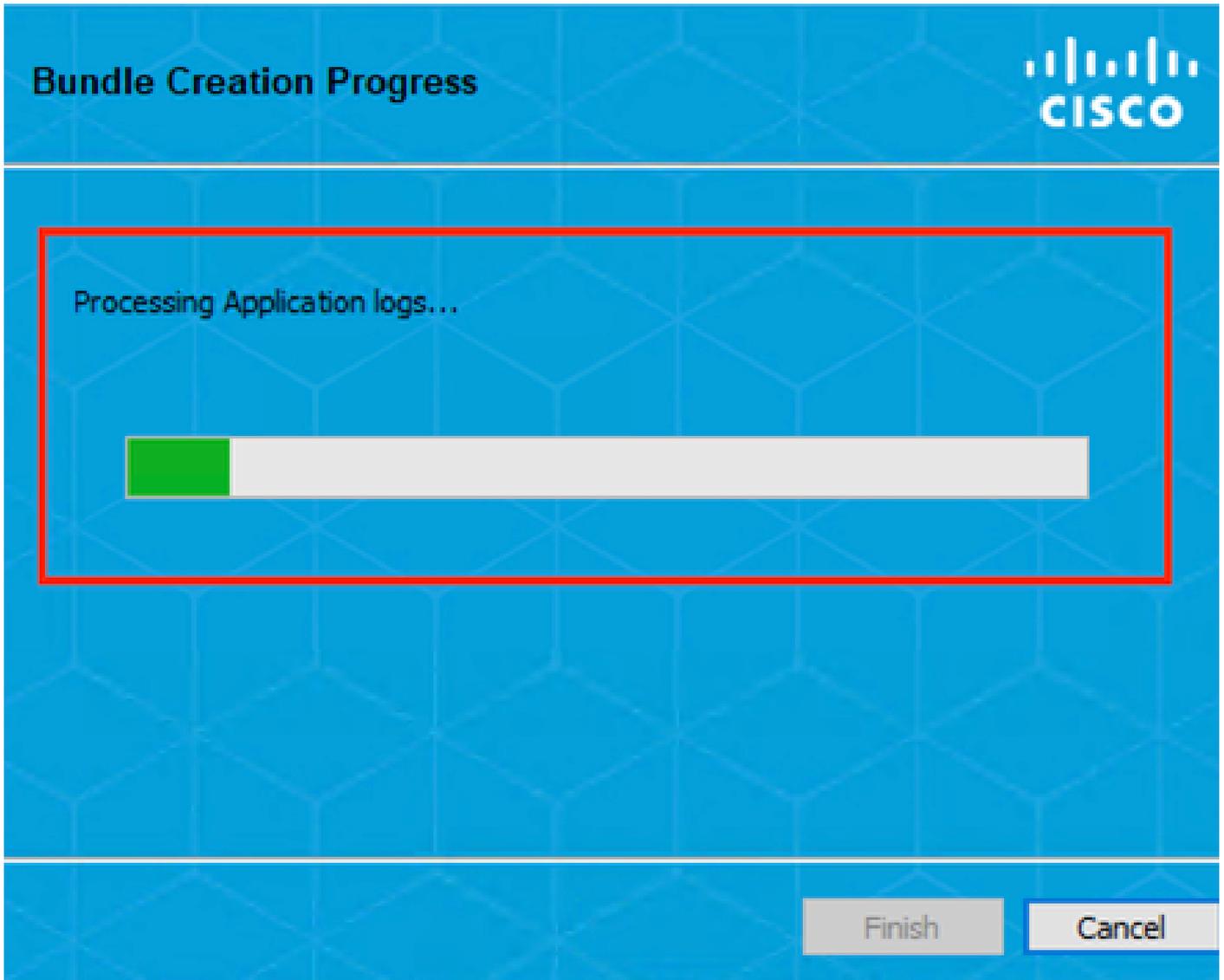
Back

Next

Cancel

DARTモジュール

DARTログ収集が開始されます。



DARTログの収集

プロセスが完了するまで10分以上かかる場合があります。

## Bundle Creation Result



The bundle was created successfully in C:\Users\LAB5\Desktop\DARTBundle\_0423\_1538.zip.

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

DARTバンドルの作成結果

DART結果ファイルは、デスクトップディレクトリにあります。

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

DART結果ファイル

## 関連情報

- [シスコのテクニカルサポートとダウンロード](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。