WindowsおよびISE 3.2を使用したDot1x用のセキュアクライアント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)ユーザ認証用のセキュアなクライアントNAMサプリカントの設定
  - 5. シナリオ2:EAP-FAST同時ユーザおよびマシン認証のためのセキュアなクライアントNAMサプリカントの設定
  - 6. シナリオ3:EAP TLSユーザ証明書認証のためのセキュアなクライアントNAMサプリカントの設定
  - 7. シナリオ1 PEAP MSCHAPv2に基づいて認証を許可するためのISR 1100およびISEの設定

確認

トラブルシュート

- 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。
- 問題2：さらなる分析のためにログを収集する必要がある。
  - 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サプ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でセキュアクライアントNAM(SCA)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、サプリカントとは、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、リンクのもう一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、ハードウェアまたはソフトウェアのいずれかを指す用語としてサプリカントが使用されます。実際には、サプ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。

ユーザはサプリカントを起動し、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。

Network Access Manager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、ユーザおよびデバイスのIDと、セキュアなアクセスに必要な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はシングルホーム接続を想定して設計されており、一度に1つのネットワーク接続のみを許可します。

また、有線接続の優先順位は無線よりも高いため、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アドレスを使用せずに無効になります。

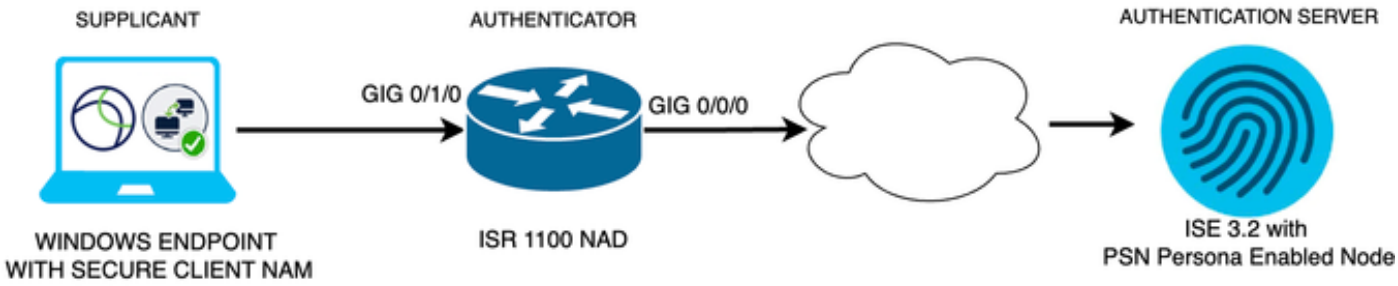
設定

ネットワーク図

dot1x認証には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。

1. dot1xを実行できるサプリカント
2. NAS/NADとも呼ばれるオーセンティケータは、RADIUS内のdot1xトラフィックをカプセル化するプロキシとして機能します。
3. と認証サーバの両方で認証を行います。

この例では、サプ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. 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)ユーザ認証用のセキュアクライアントNAMサプリカントの設定。
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サプリカントを設定します。
6. シナリオ3パート1:EAP-TLS用のセキュアクライアントNAMサプリカントの設定
7. シナリオ3パート2:NADおよび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]

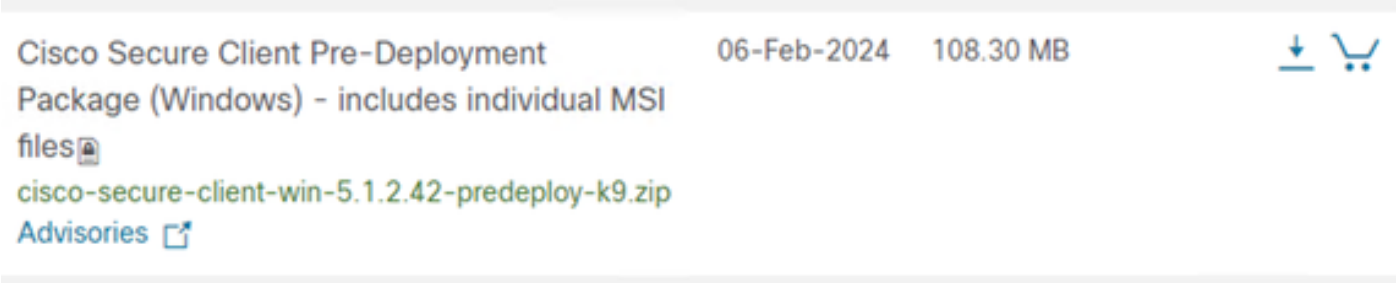
製品名の検索バーで、「Secure Client 5」と入力します。

Downloads Home > Security > VPN and Endpoint Security Clients > Secure Client (including AnyConnect) > 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。

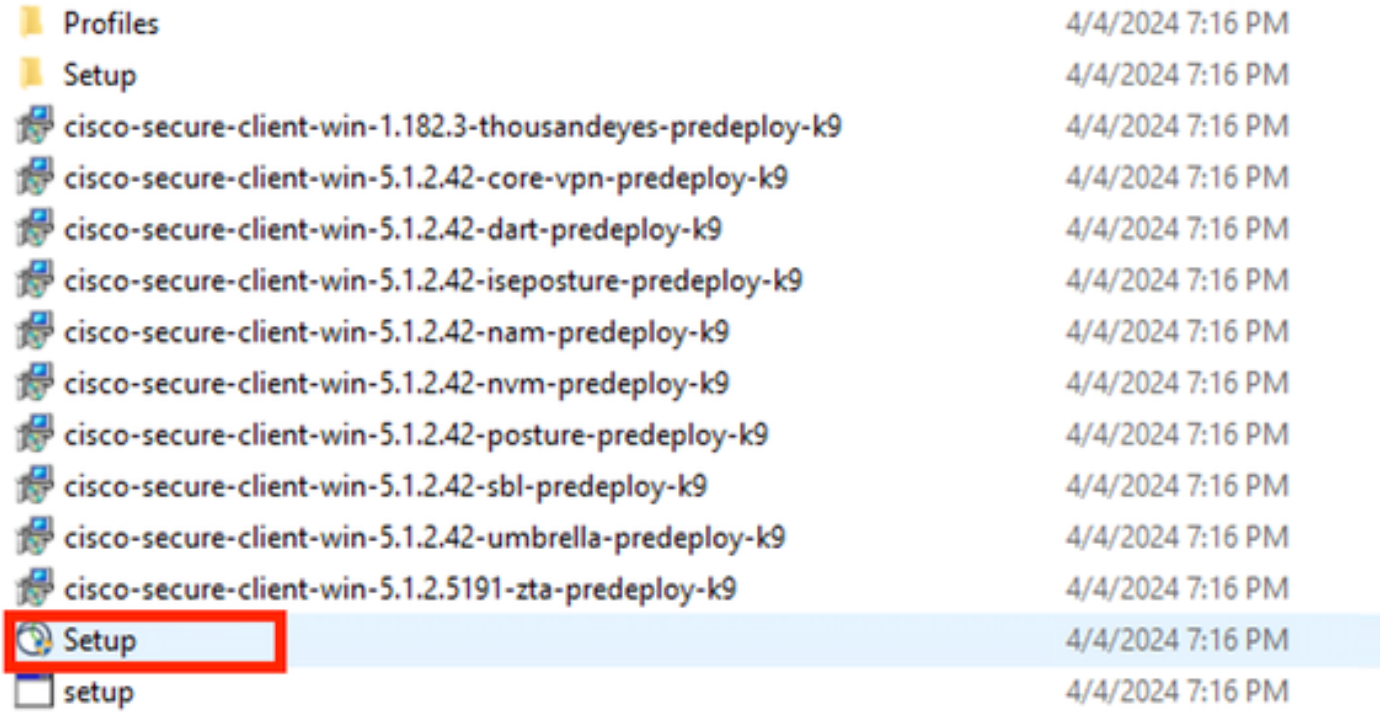
Secure ClientをWindowsデバイスに導入するには、SCCM、アイデンティティサービスエンジン、およびVPNヘッドエンドから複数の方法があります。ただし、この記事では、使用されるインストール方法は導入前の方法です。

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



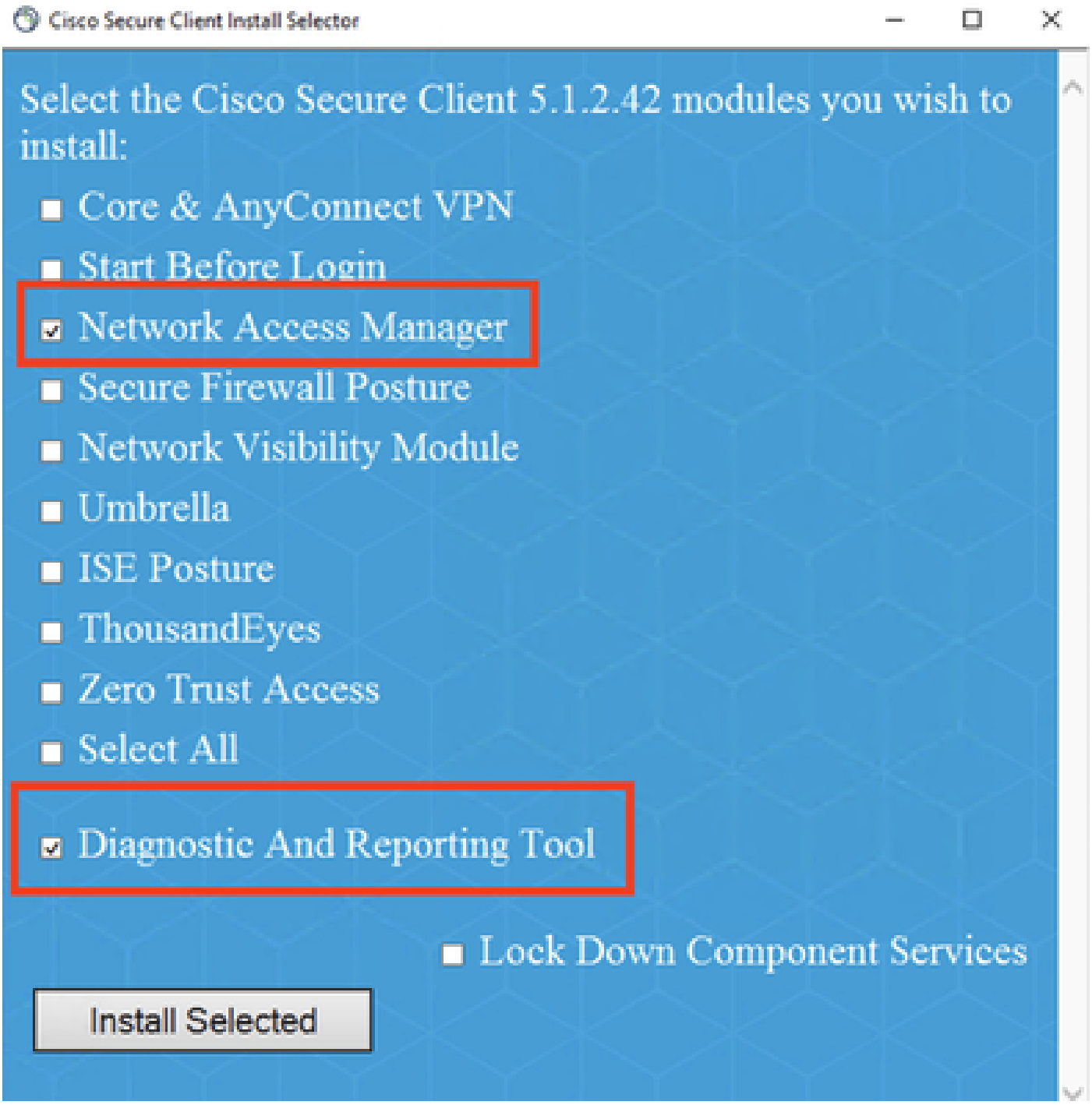
Msi zipファイル

ダウンロードして解凍したら、Setupをクリックします。



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

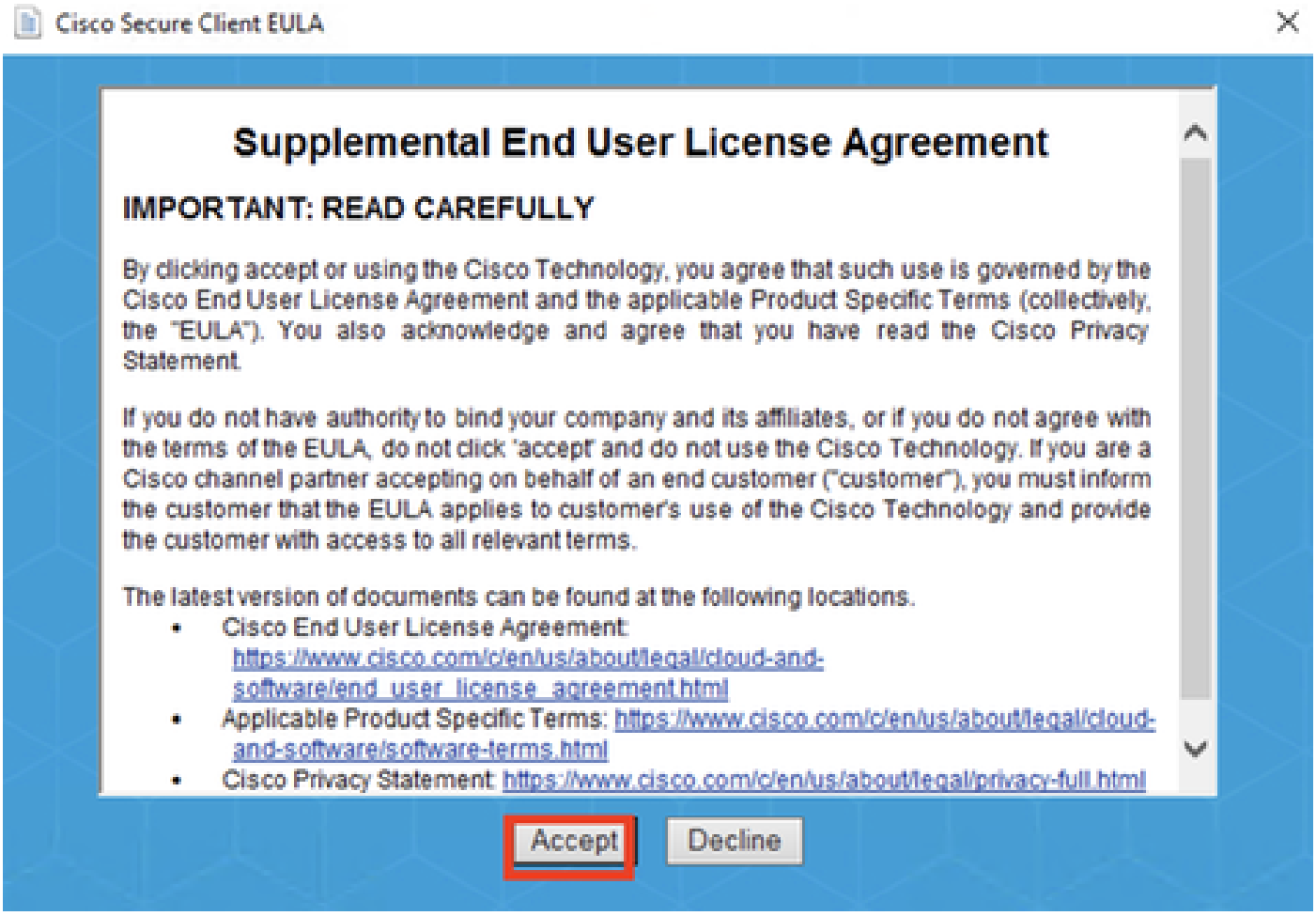
警告:Cisco Secure Client Wizardを使用する場合、VPNモジュールは自動的にインストールされ、GUIでは表示されません。VPNモジュールがインストールされていない場合、NAMは機能しません。個別のMSIファイルを使用する場合、または別のインストール方法を使用する場合は、VPNモジュールをインストールしてください。



Selectorのインストール

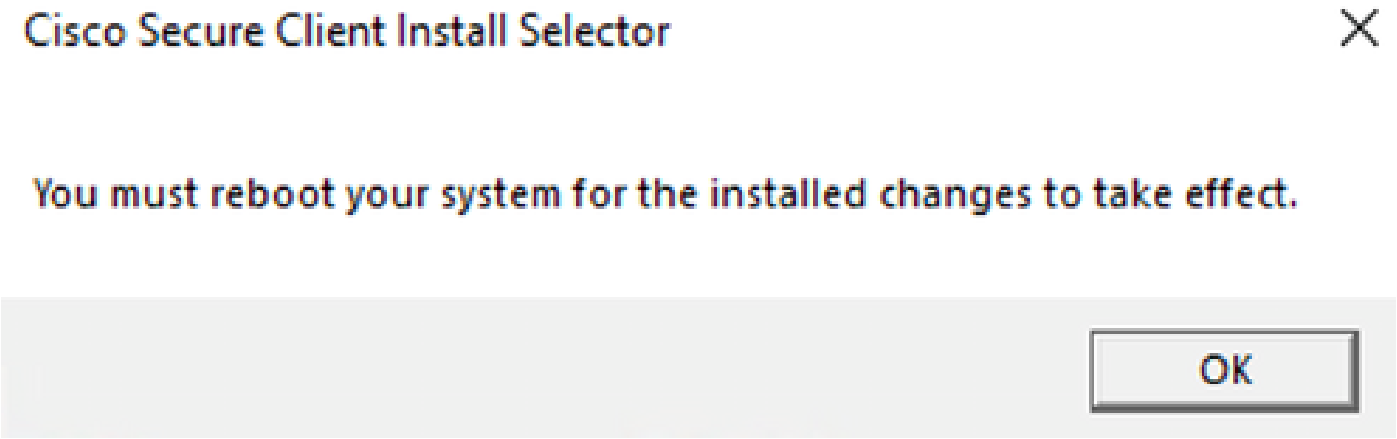
[選択項目のインストール（Install Selected）] をクリックします。

EULAに同意します。



EULAウィンドウ

NAMのインストール後に再起動が必要です。



Reboot Requirementウィンドウ

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

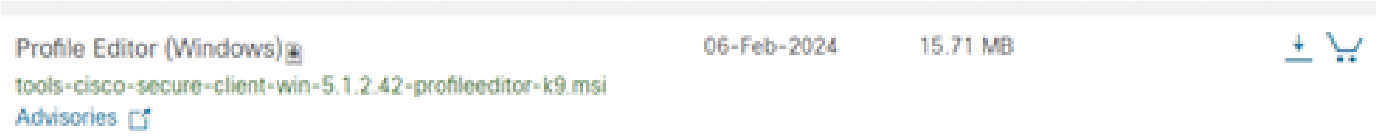
セキュアクライアントプログラム

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プリファレンスを設定するには、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。

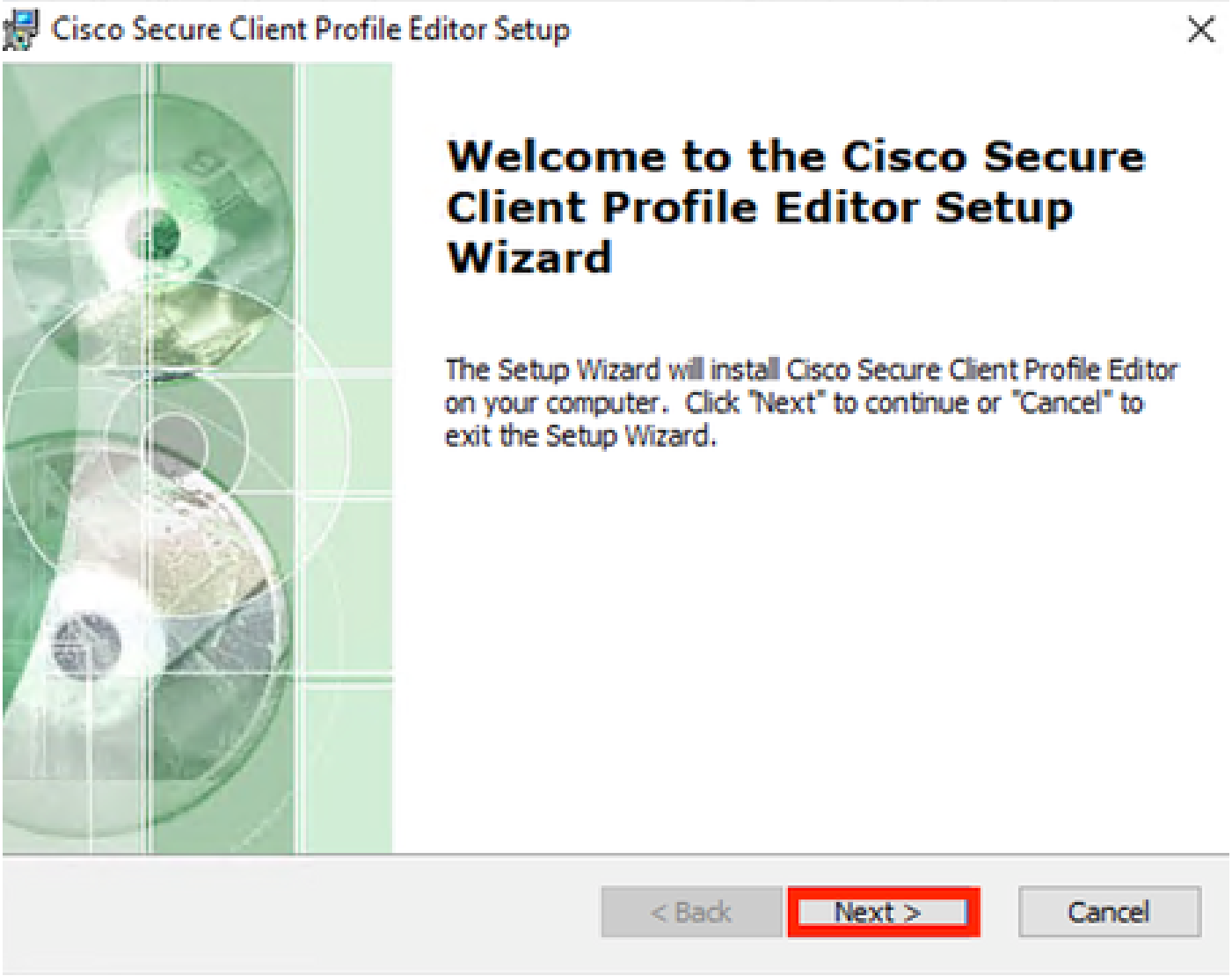
この例では、バージョン5.1.2.42のオプションを使用しています。



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。

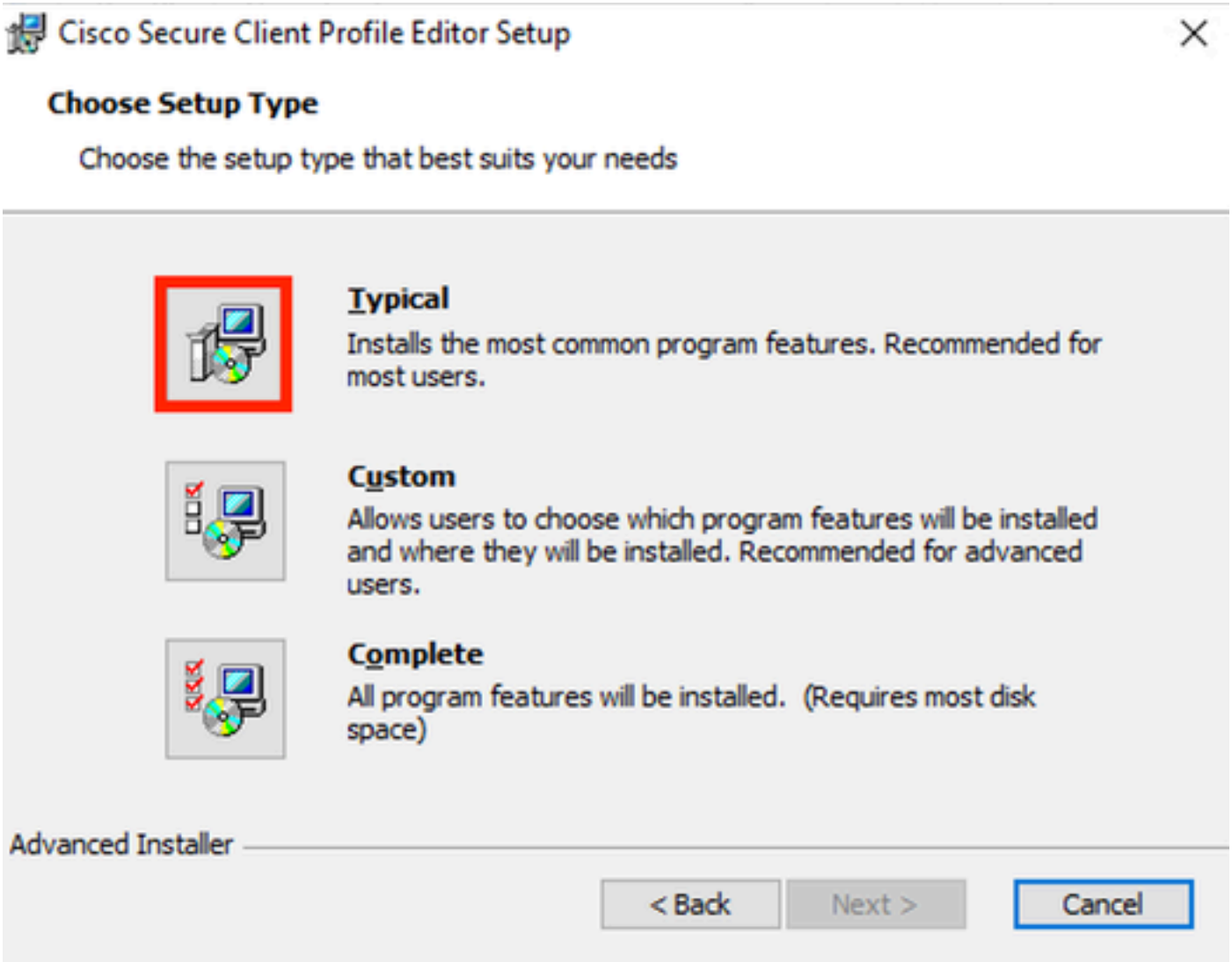
msiファイルを実行します。



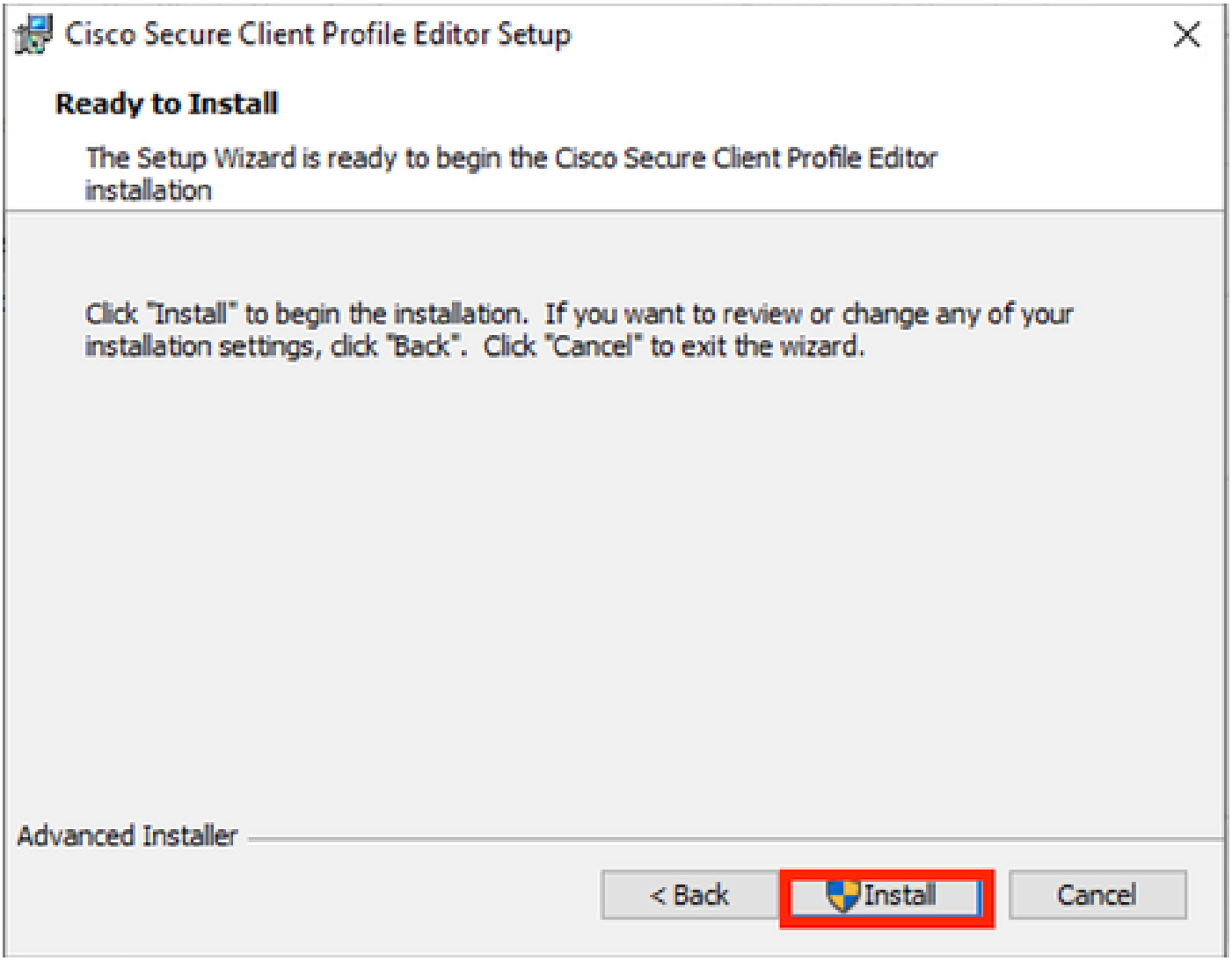
Profile Editor

*Setup*ウィンドウ

Typicalセットアップオプションを使用します。

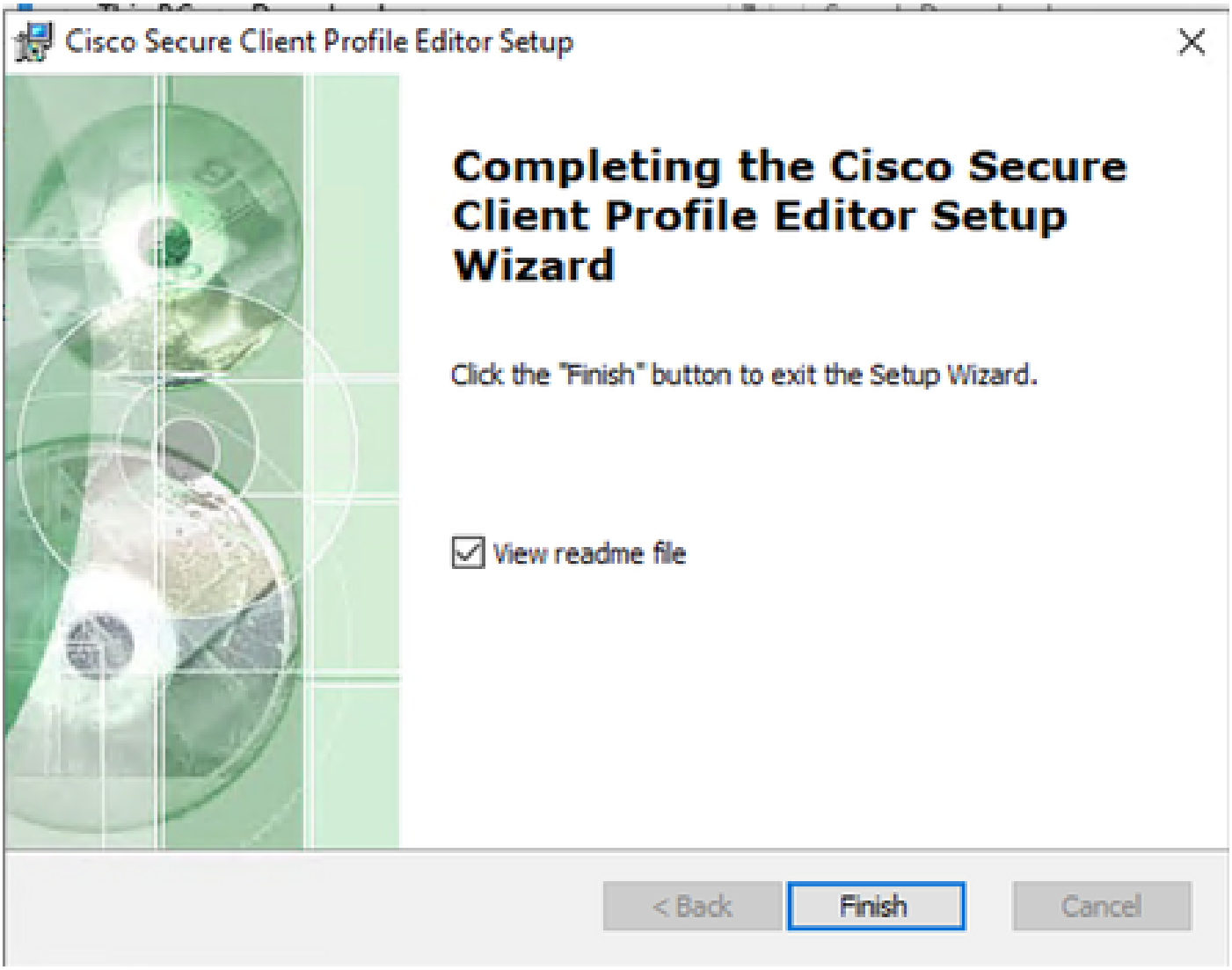


プロファイルエディタの設定



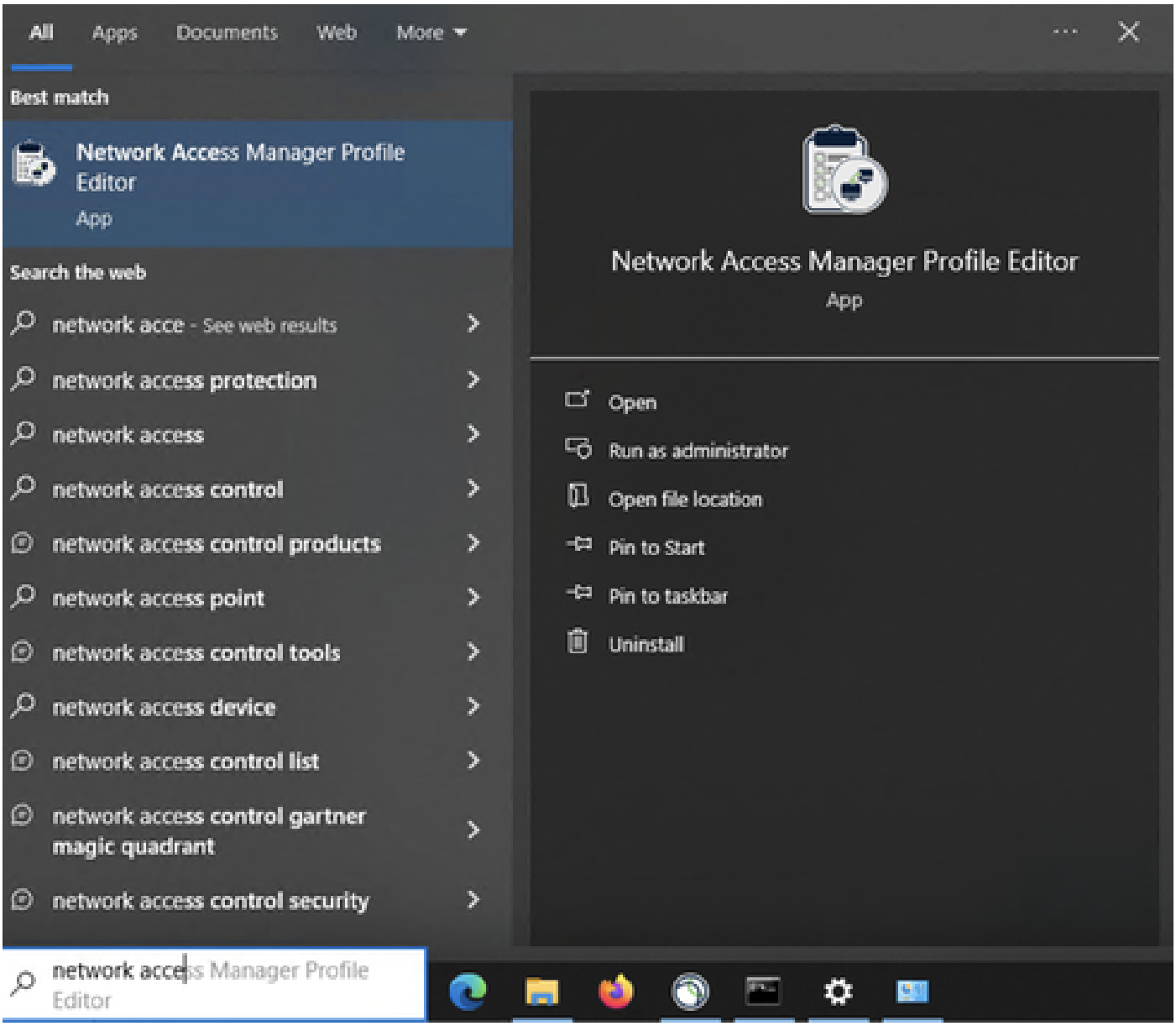
インストールウィンドウ

[Finish] をクリックします。



プロファイルエディタのセットアップの終了

インストールが完了したら、検索バーからNetwork Access Manager Profile Editorを開きます。



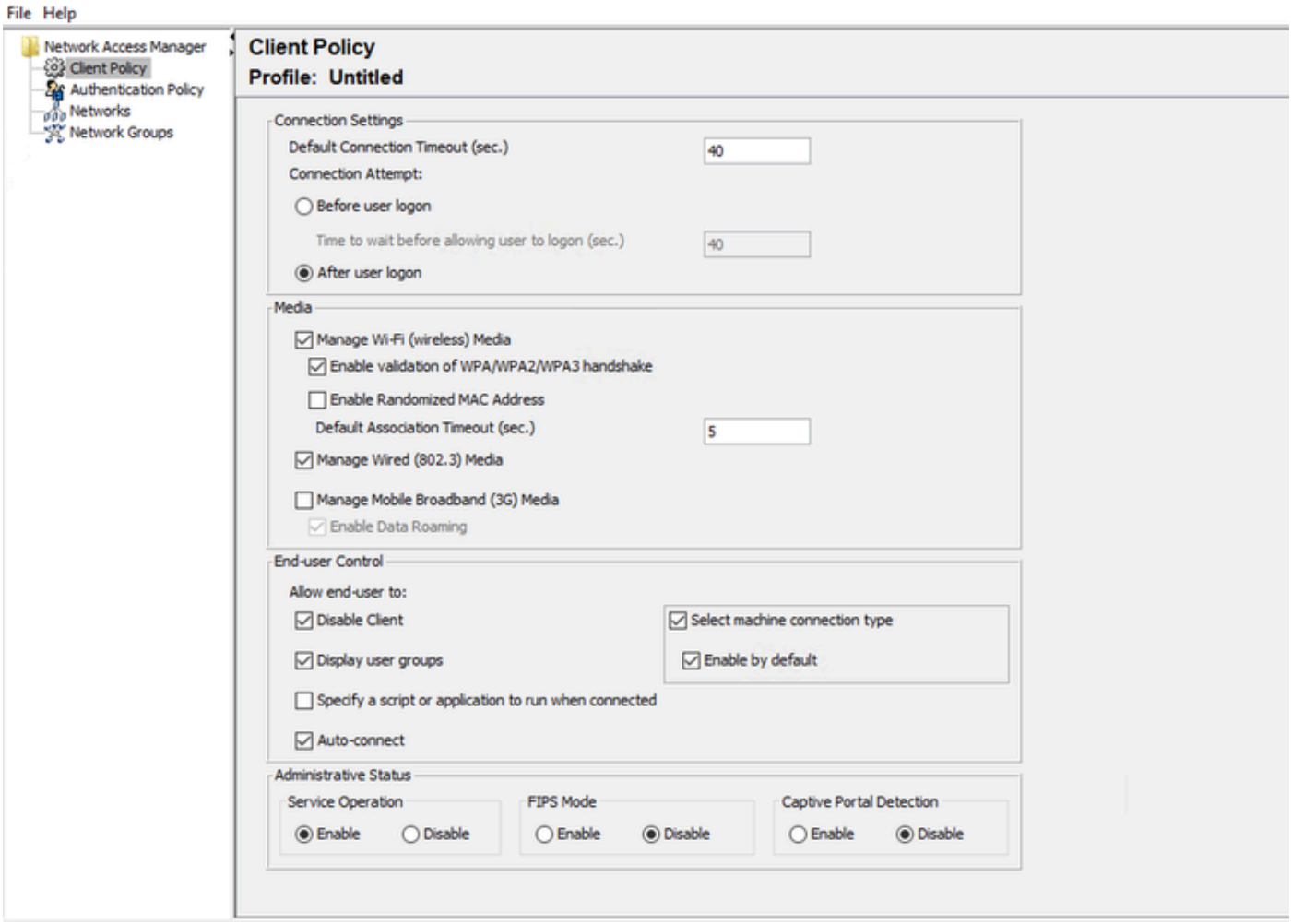
検索バーのNAMプロファイルエディタ

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。

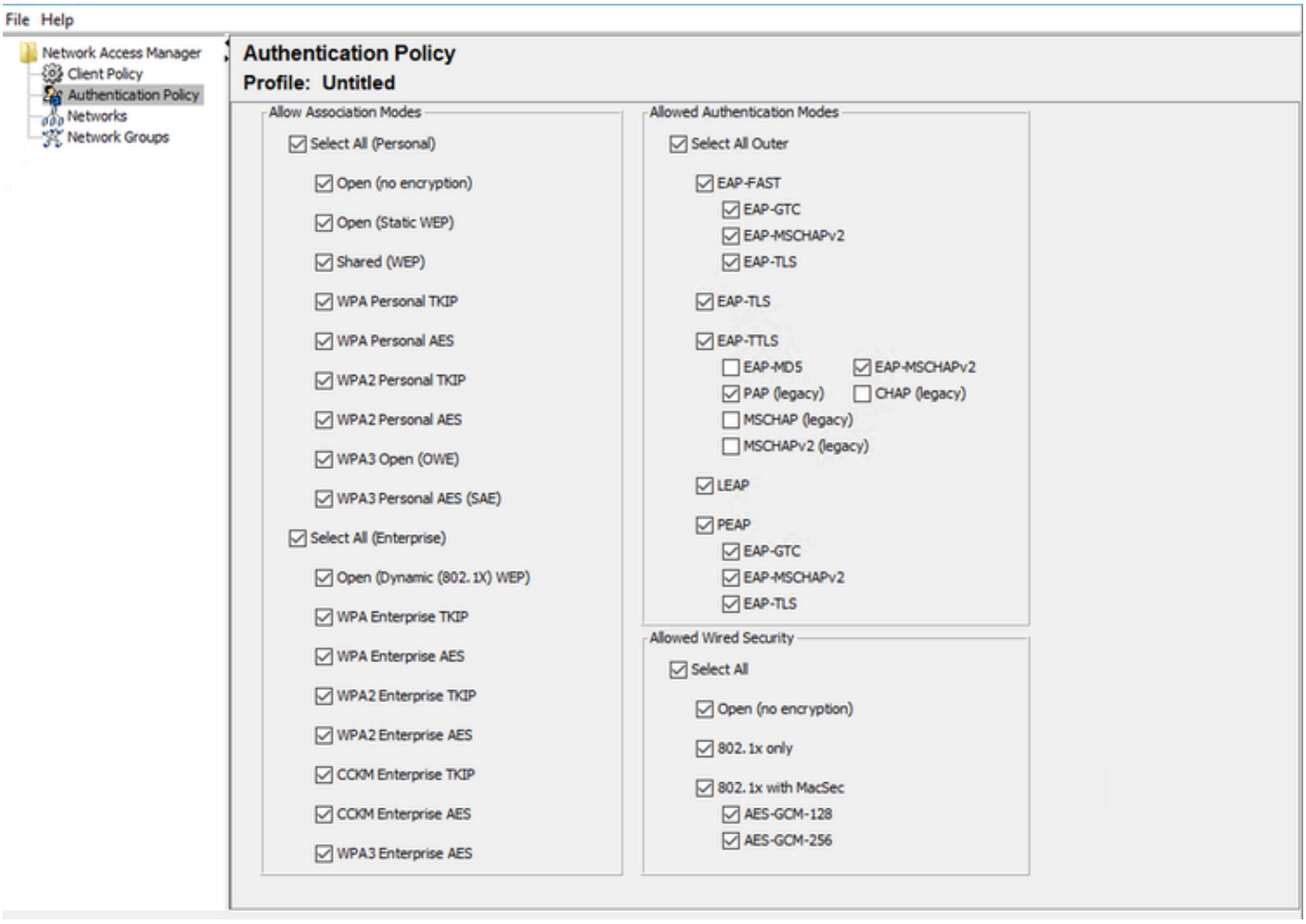
3. 一般的なデフォルト設定

この記事で説明するすべてのシナリオには、次の項目の設定が含まれています。

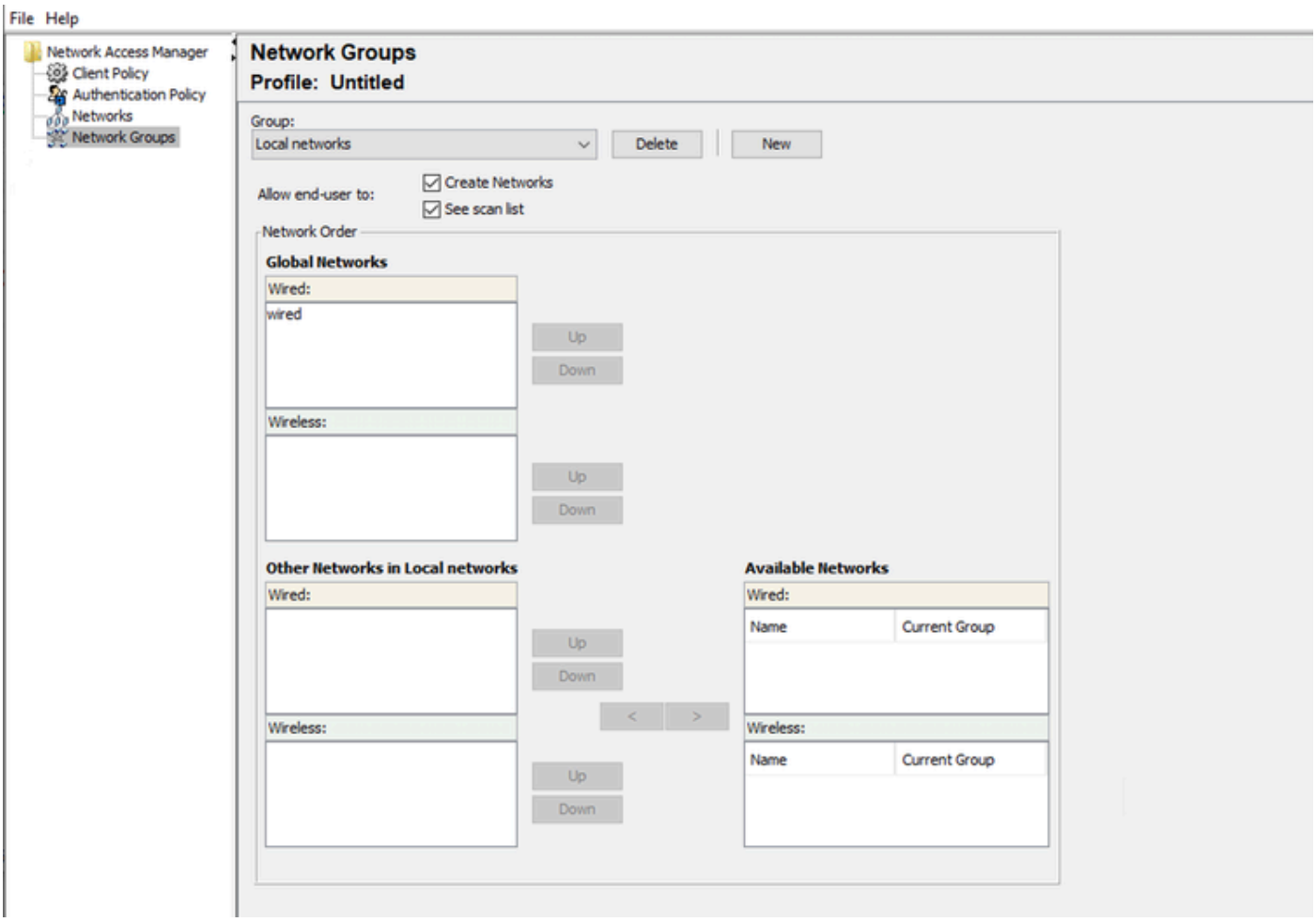
- クライアントポリシー
- 認証ポリシー
- ネットワークグループ



*NAM*プロファイルエディタクライアントポリシー



*NAM*プロファイルエディタの認証ポリシー



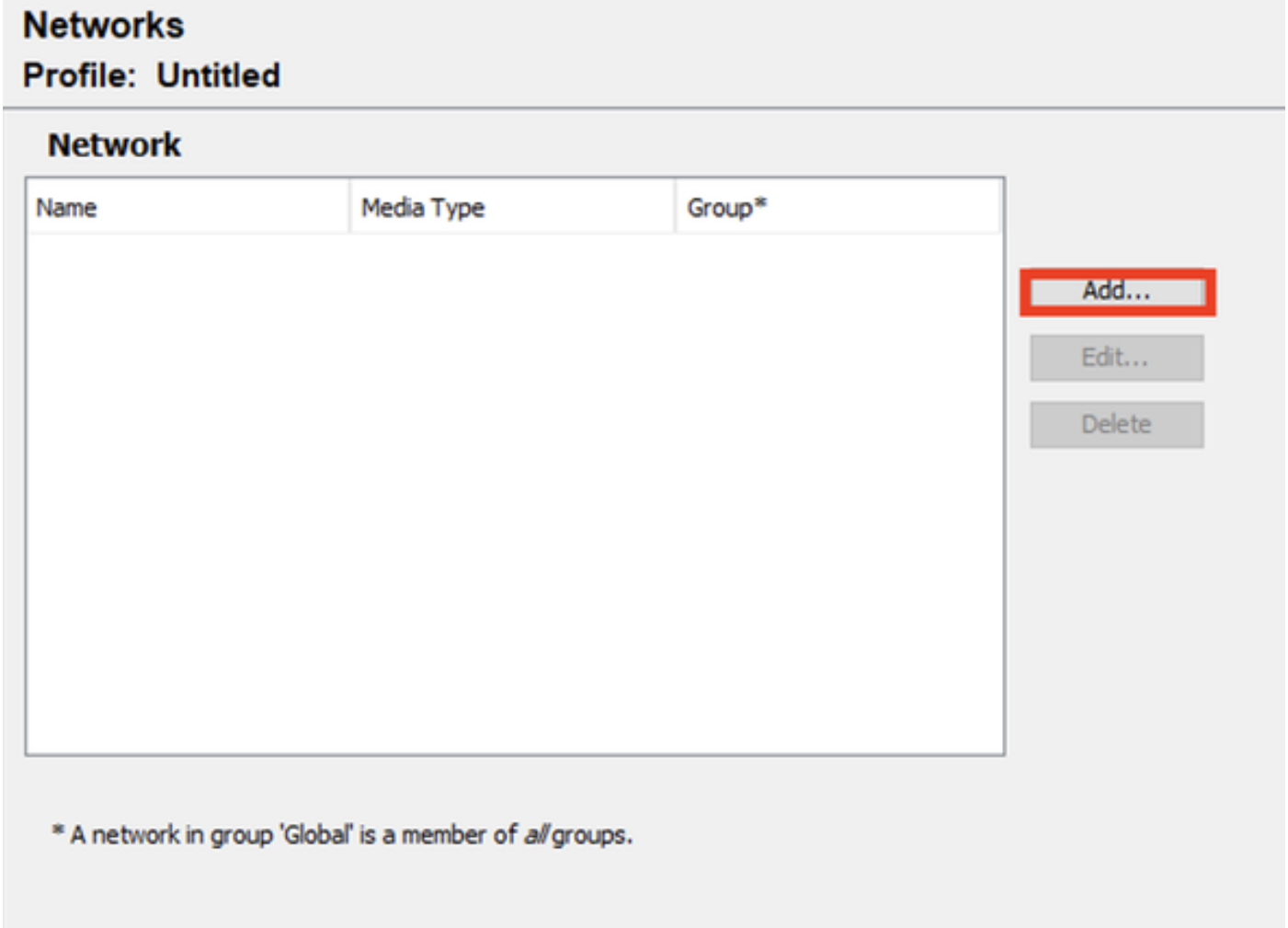
Network Groupsタブ

4. シナリオ1:PEAP(MS-CHAPv2)ユーザ認証用のセキュアなクライアントNAMサプリカントの設定

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。

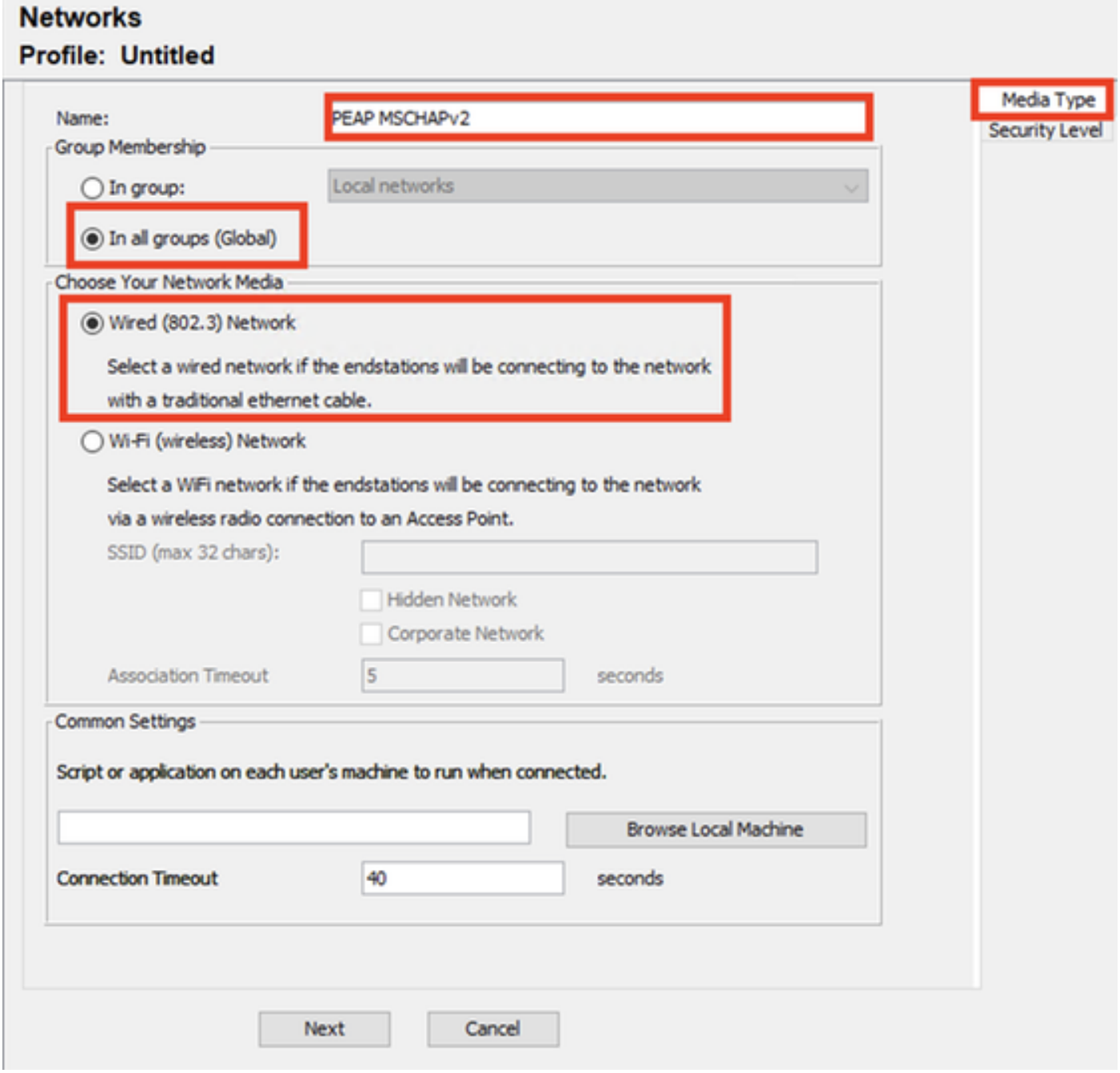
[Add] をクリックします。



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。

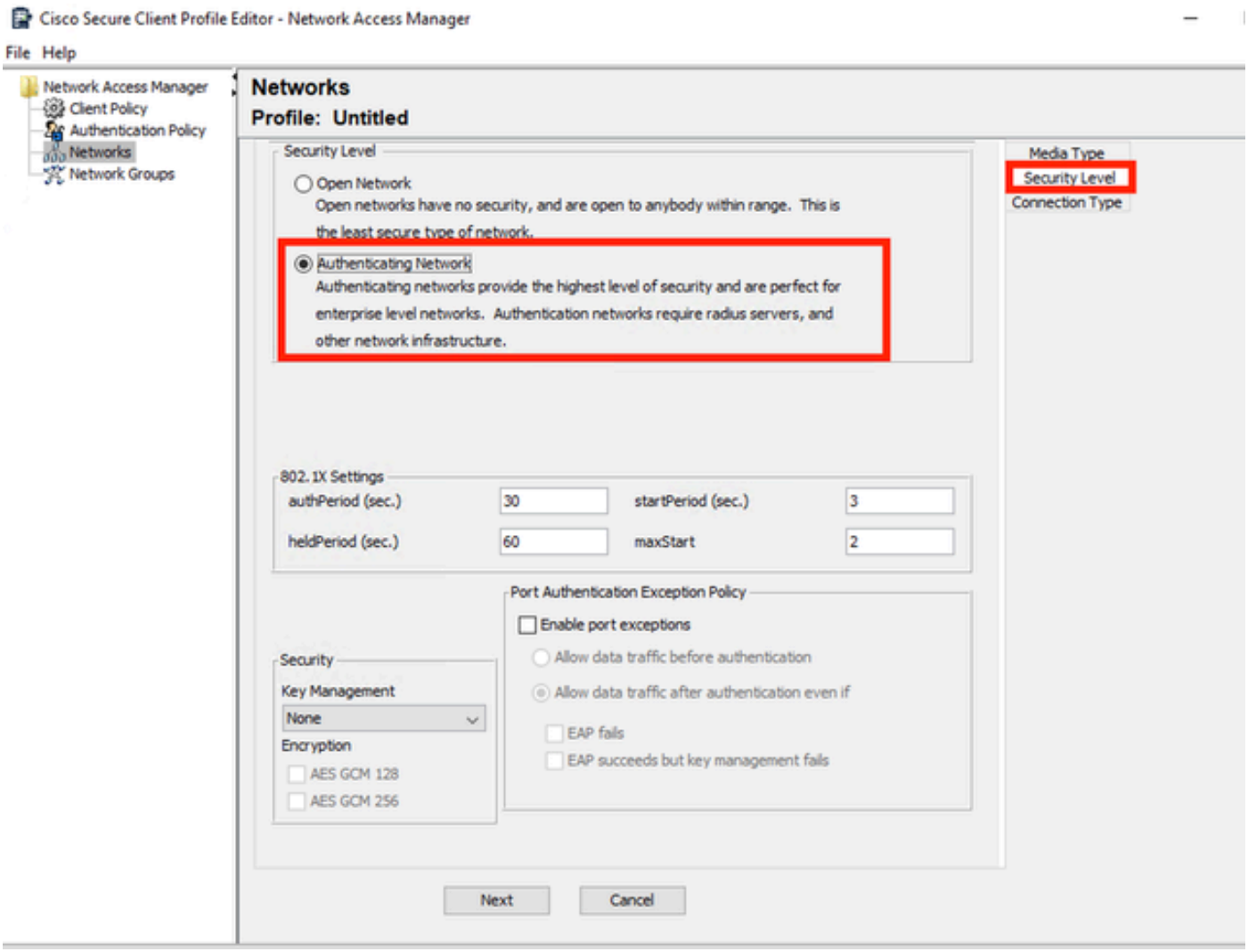
Group MembershipにGlobalを選択します。Wired Network Mediaを選択します。



Network Profile Media Typeセクション

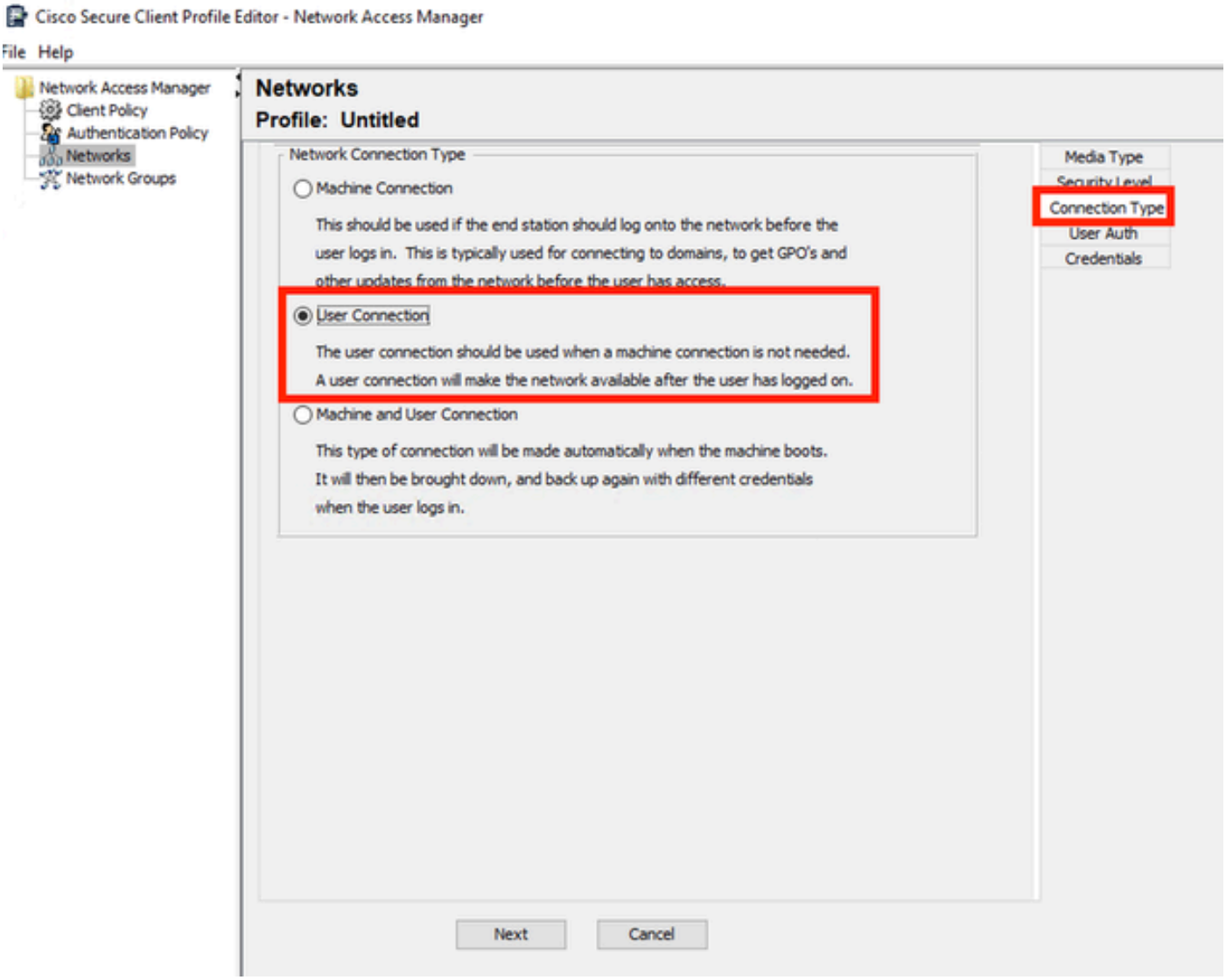
[Next] をクリックします。

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。



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。

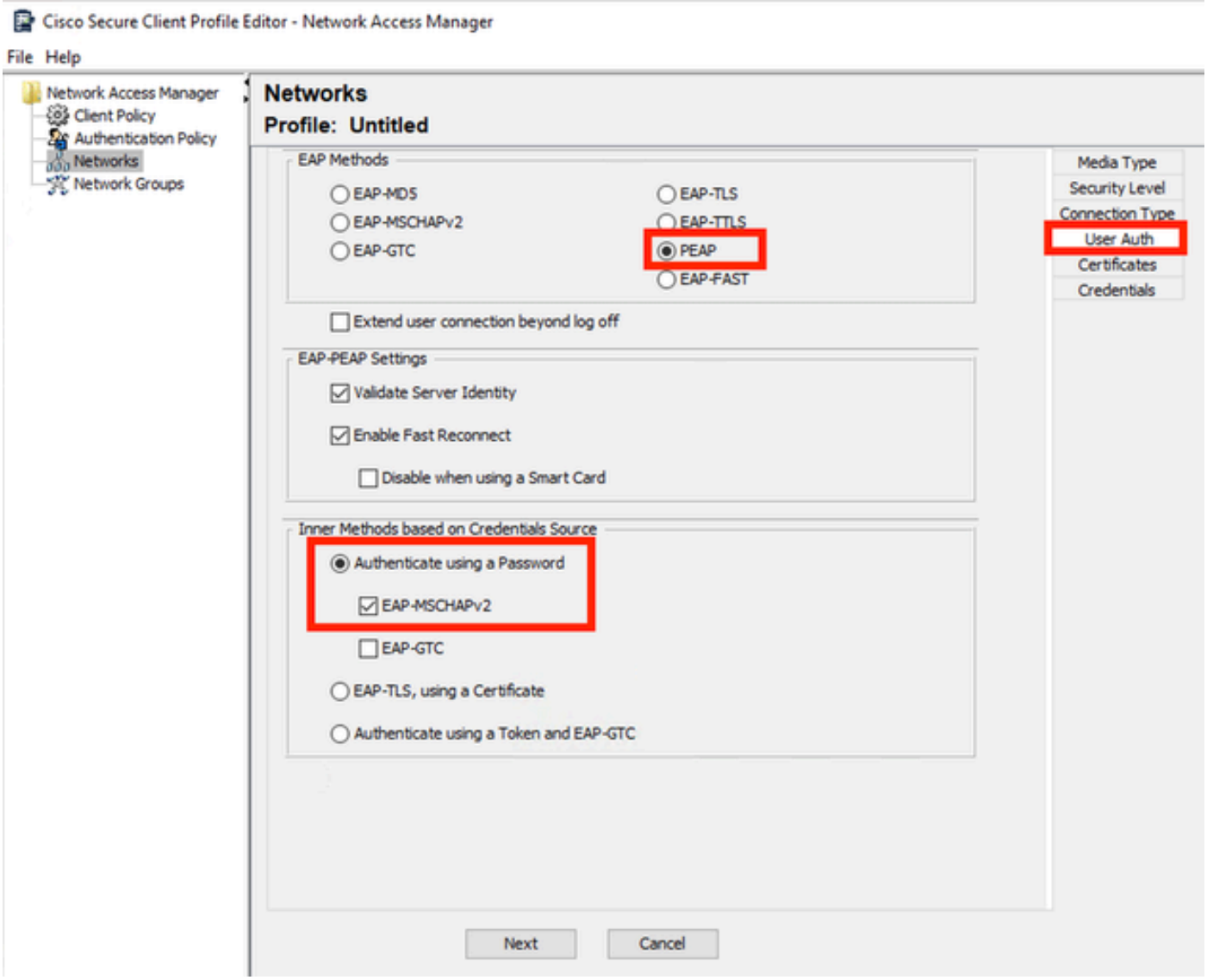


ネットワークプロファイルの接続タイプ

User Connection接続タイプを選択します。

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

一般的なEAP MethodとしてPEAPを選択します。



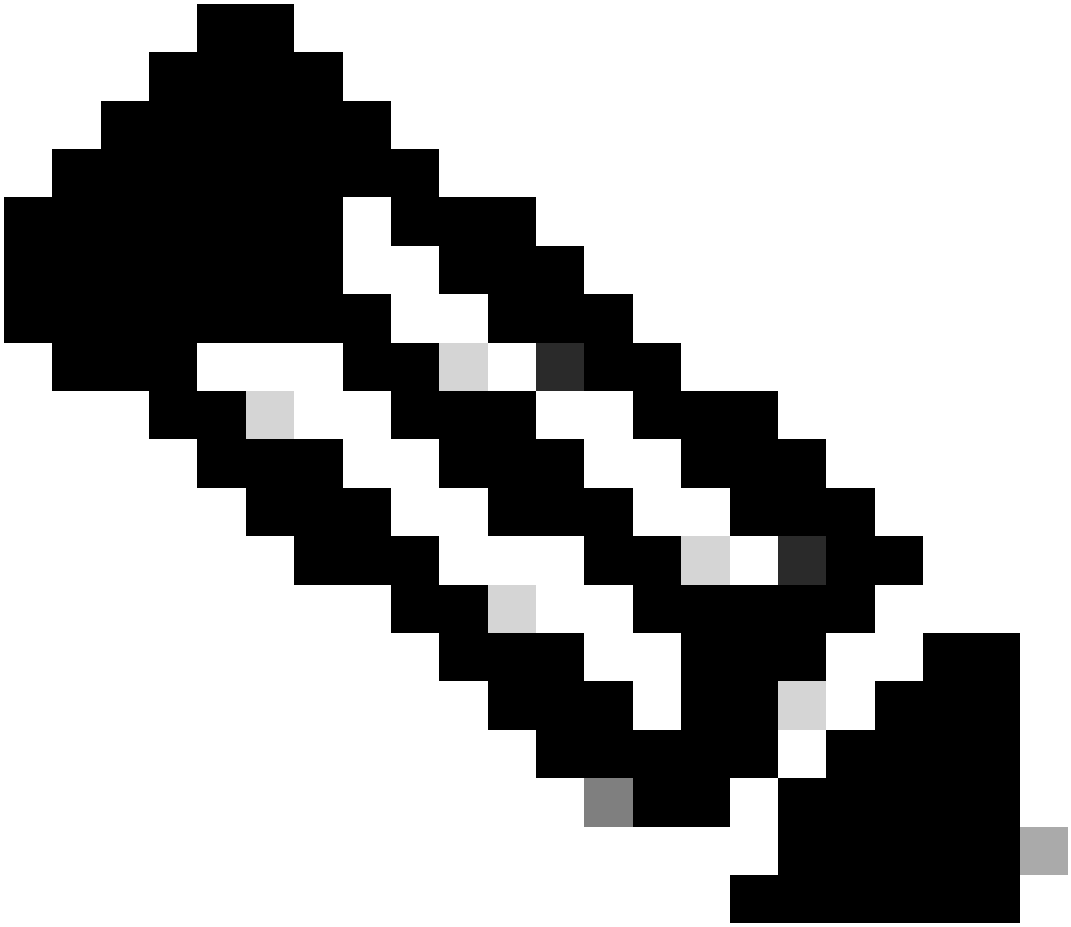
ネットワークプロファイルユーザ認証

EAP-PEAP Settingsのデフォルト値は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に対応する複数の内部方式の中から、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。

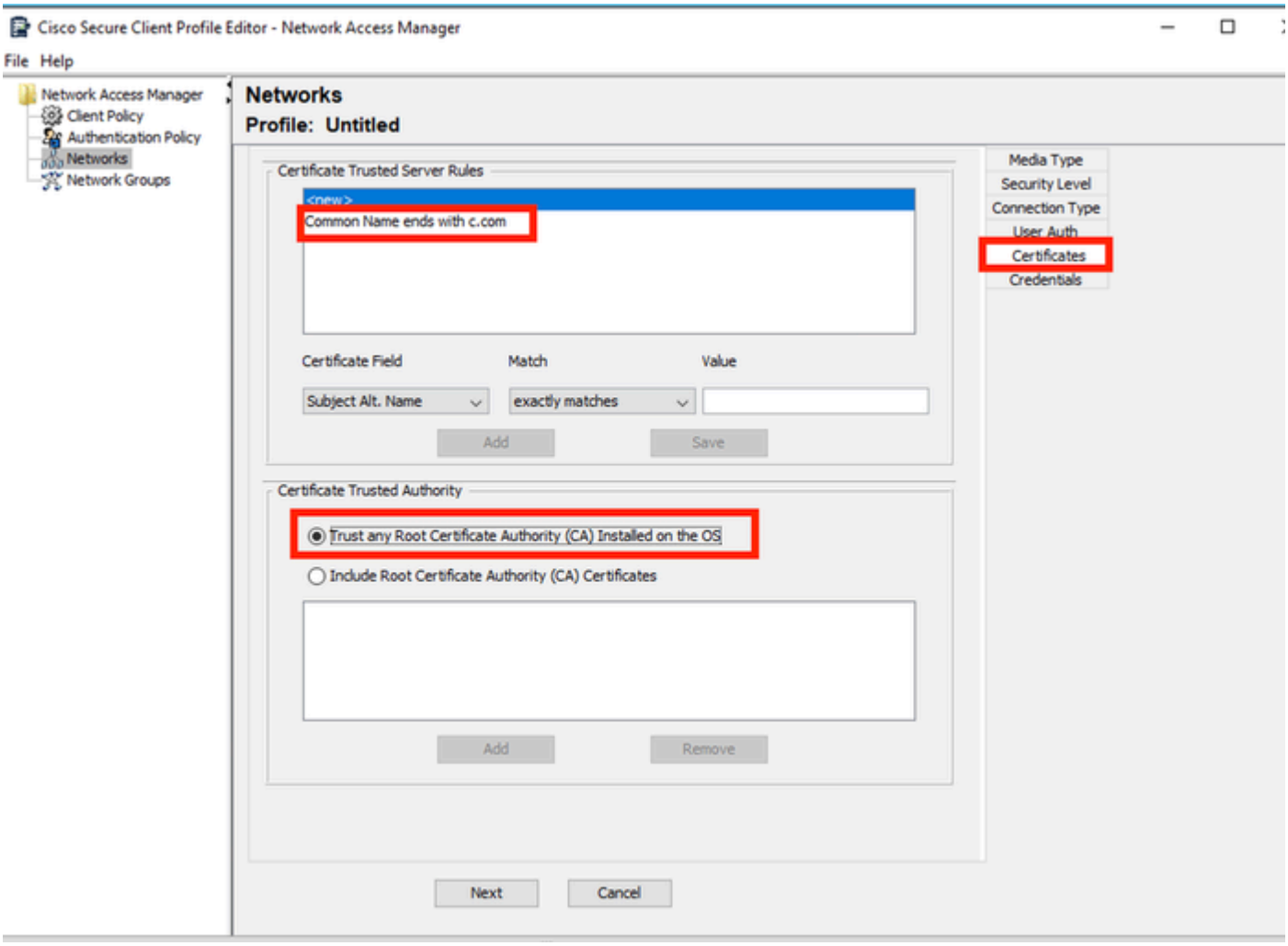


注:[Certificate] セクションは、[EAP-PEAP Settings]で[Validate Server Identity]オプションが選択されているため表示されます。EAP PEAPでは、サーバ証明書を使用してカプセル化を行います。

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。

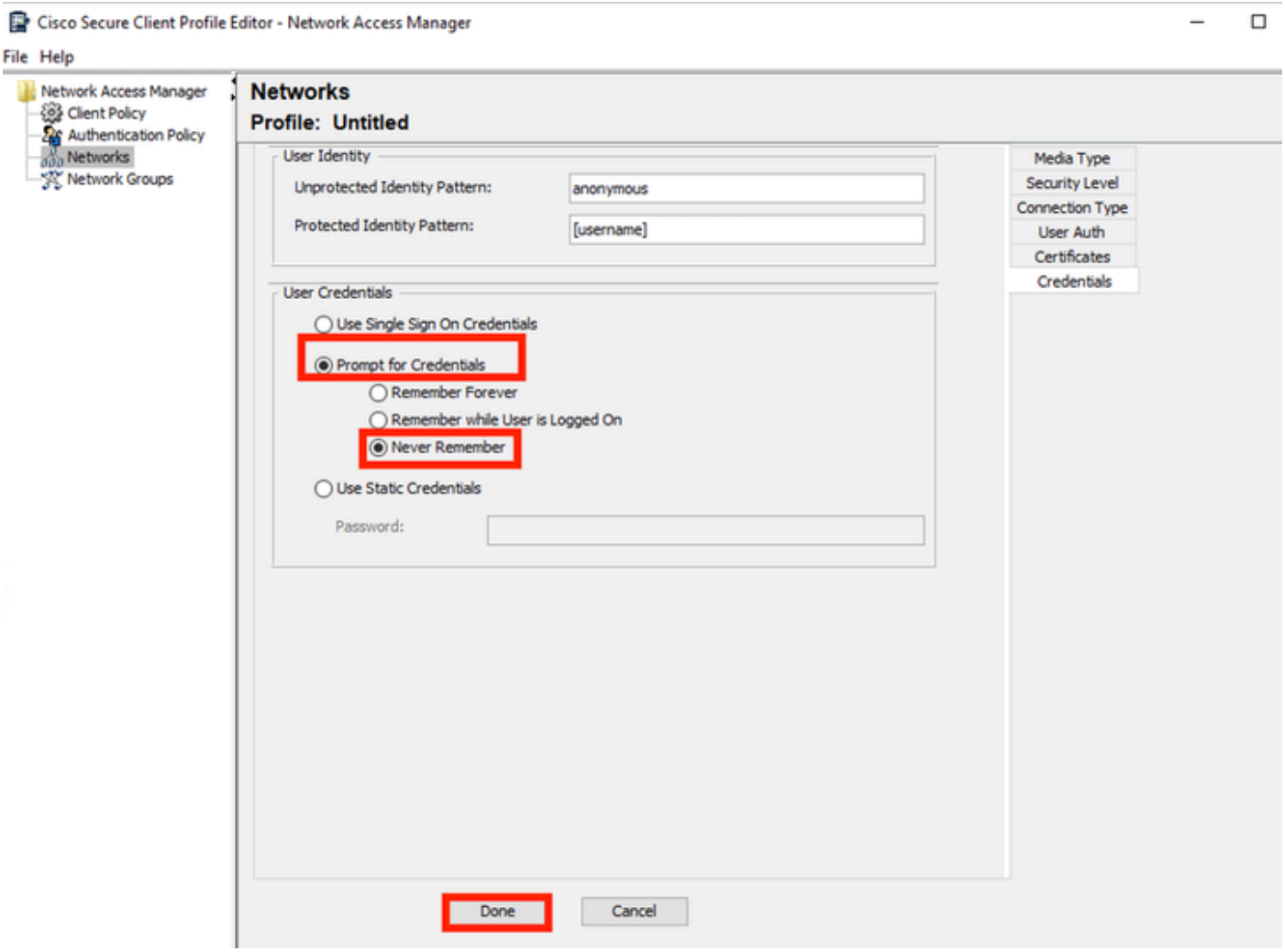


Network Profile Certificateセクション

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が使用されます。

このオプションを使用すると、Windowsデバイスは、「Manage User Certs program 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 Credentials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。

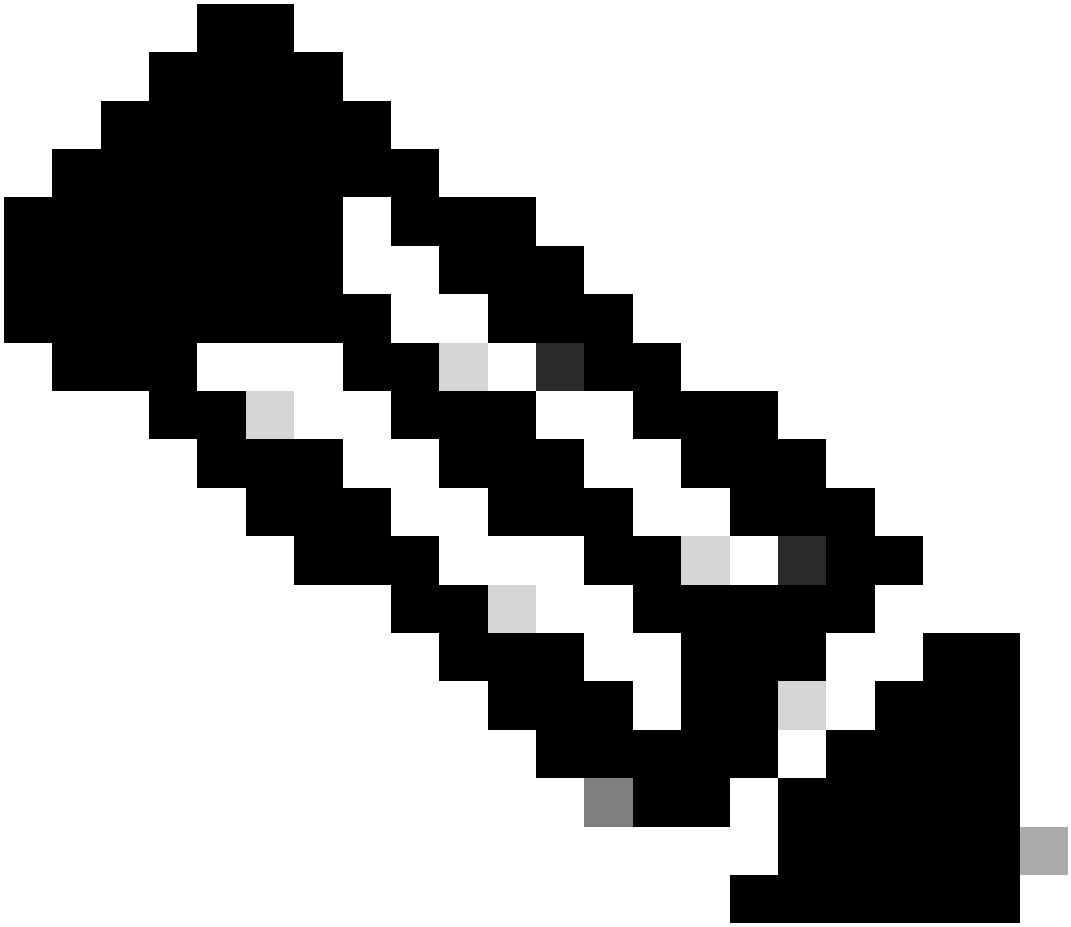
オプションPrompt for Credentials > Never Rememberが選択されているため、認証を行うユーザは認証のたびにクレデンシャルを入力する必要があります。

[Done] をクリックします。

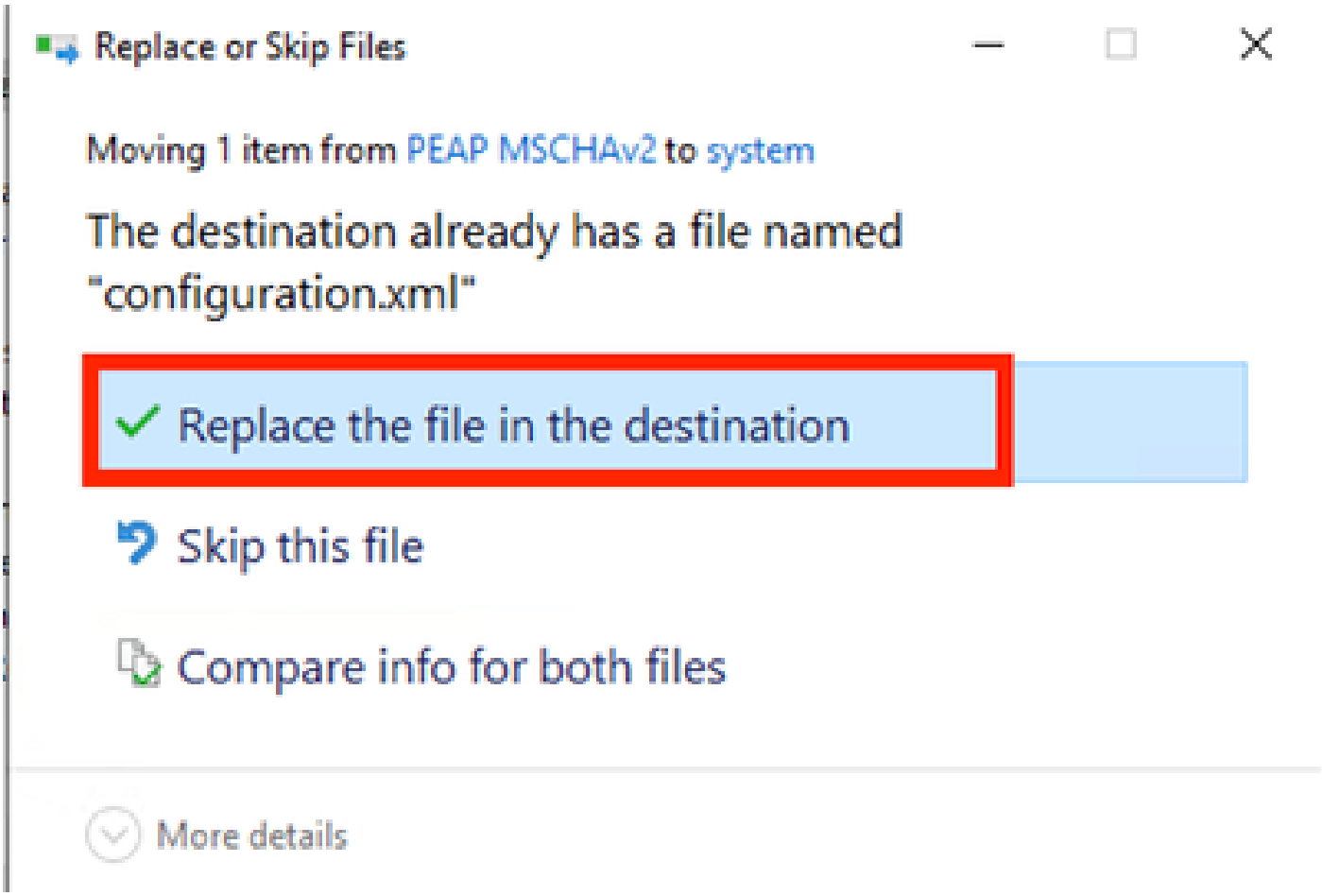
File > Save Asオプションを使用して、Secure Client Network Access Manager(SCA)プロファイルをconfiguration.xmlとして保存します。

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\ネットワークアクセスマネージャ\システム



注：このファイルは、configuration.xmlという名前にする必要があります。そうしないと機能しません。

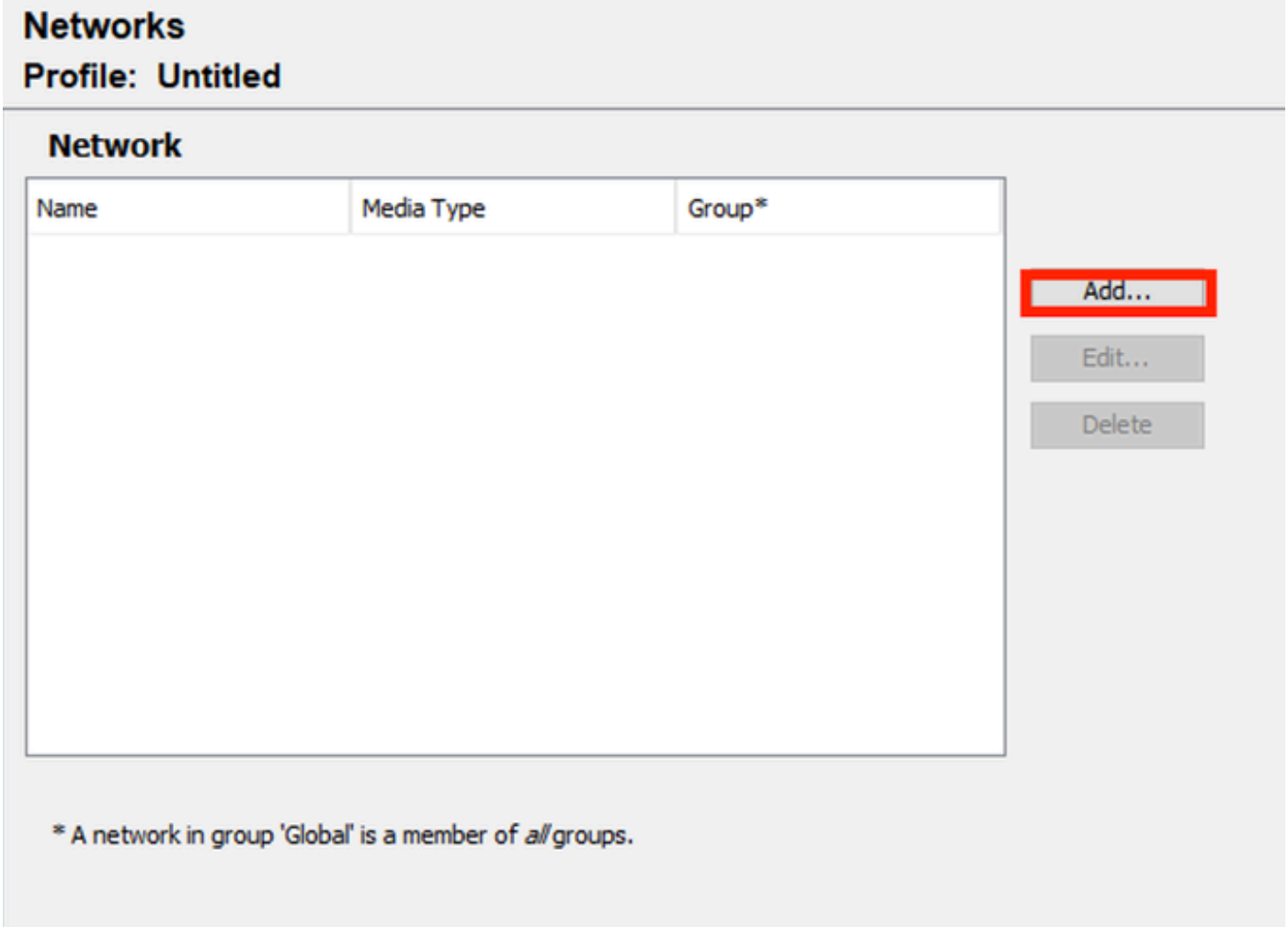


ファイルセクションの置換

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サプリカントの設定

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。

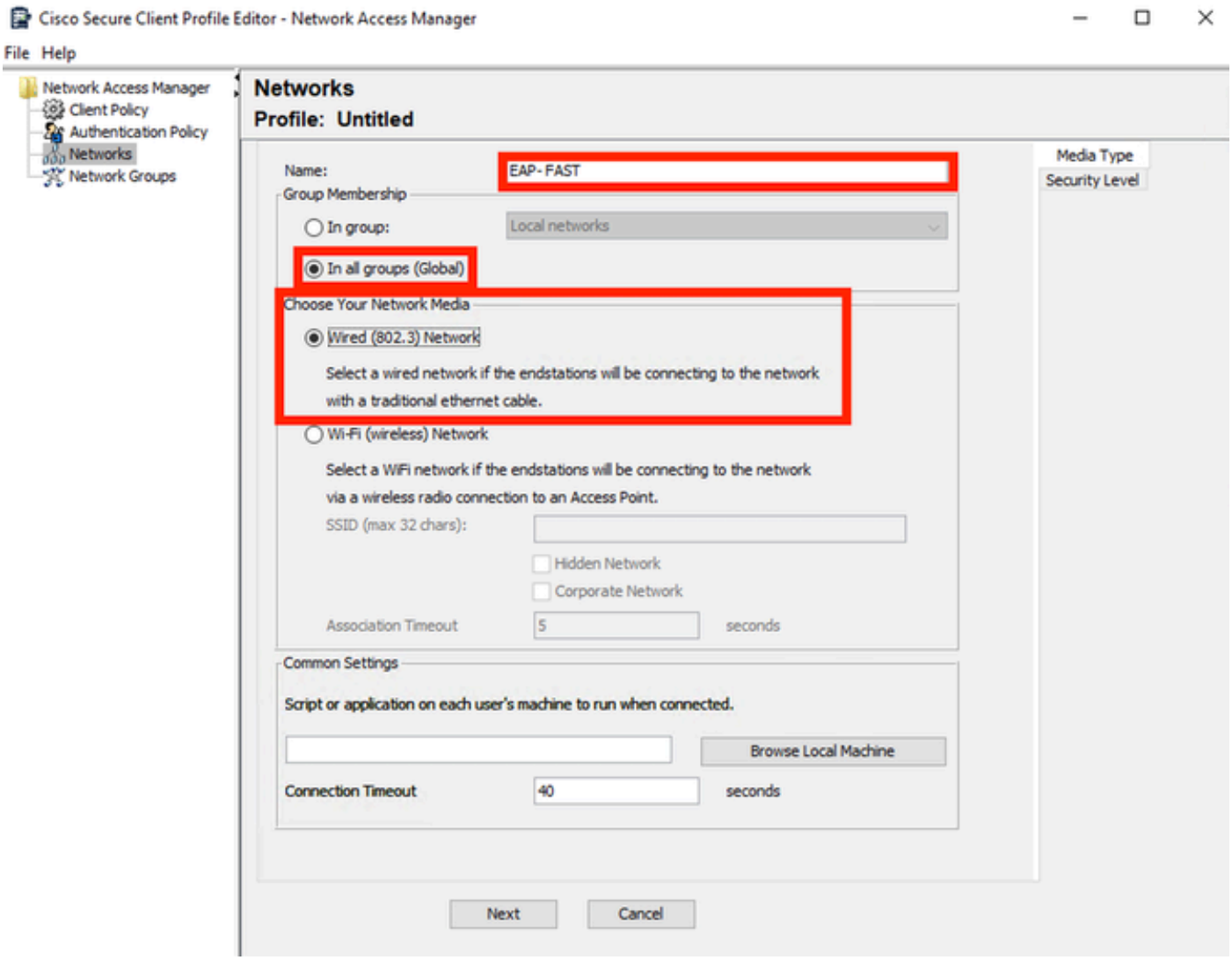
[Add] をクリックします。



NAMプロファイルエディタネットワークタブ

ネットワークプロファイルに名前を入力します。

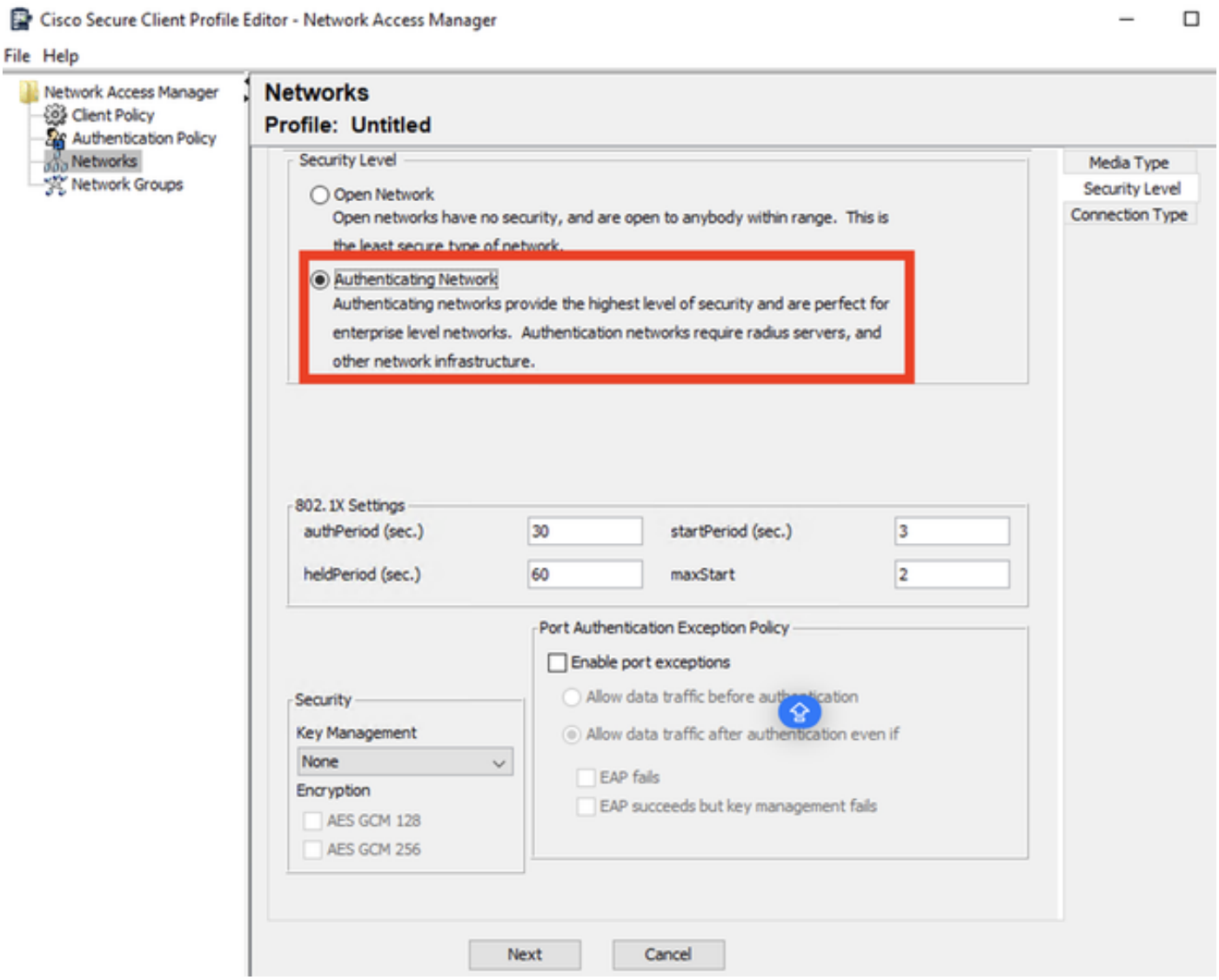
Group MembershipにGlobalを選択します。WiredNetwork Mediaを選択します。



Media Typeセクション

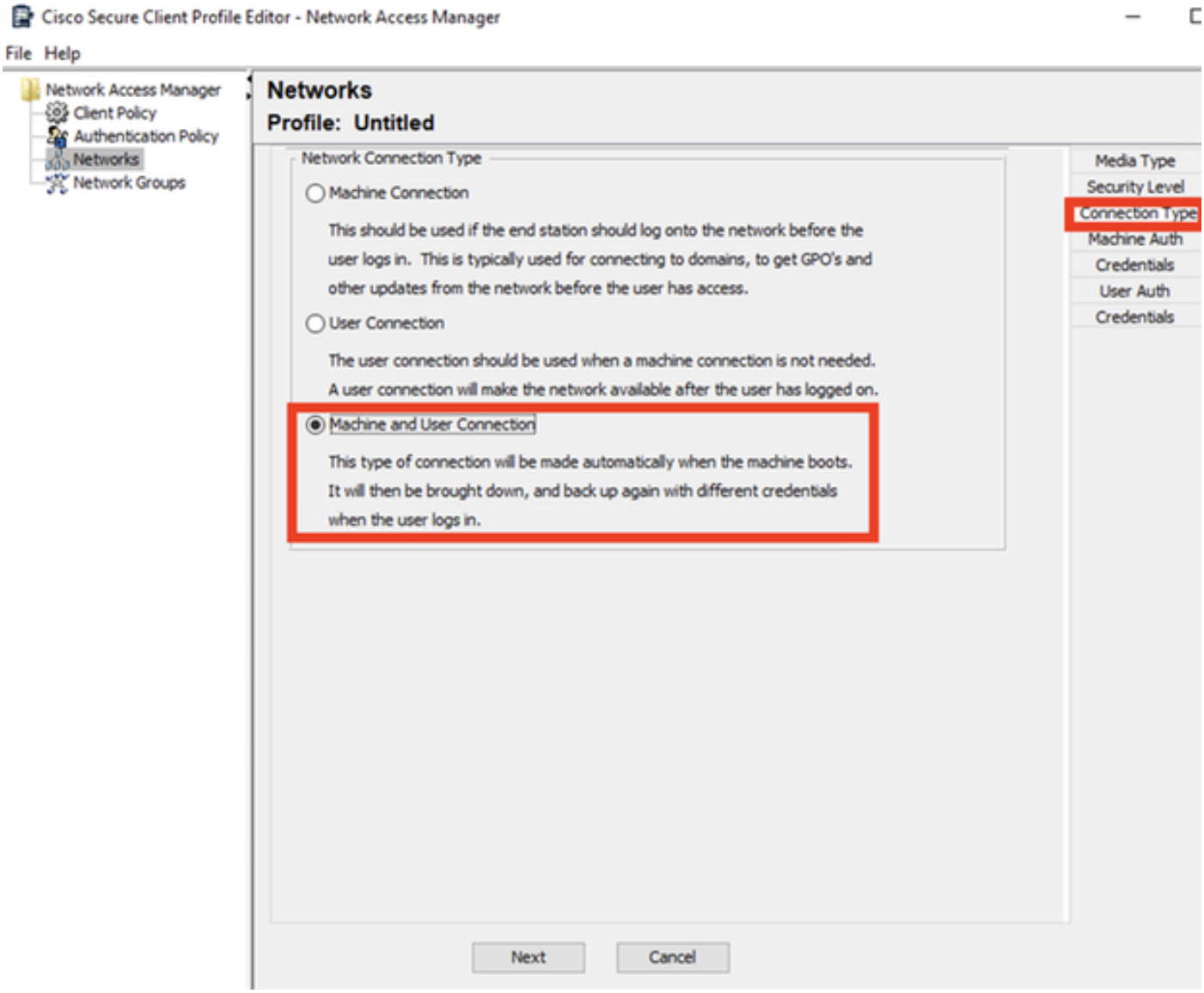
[Next] をクリックします。

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。



*Security Level Profile Editor*セクション

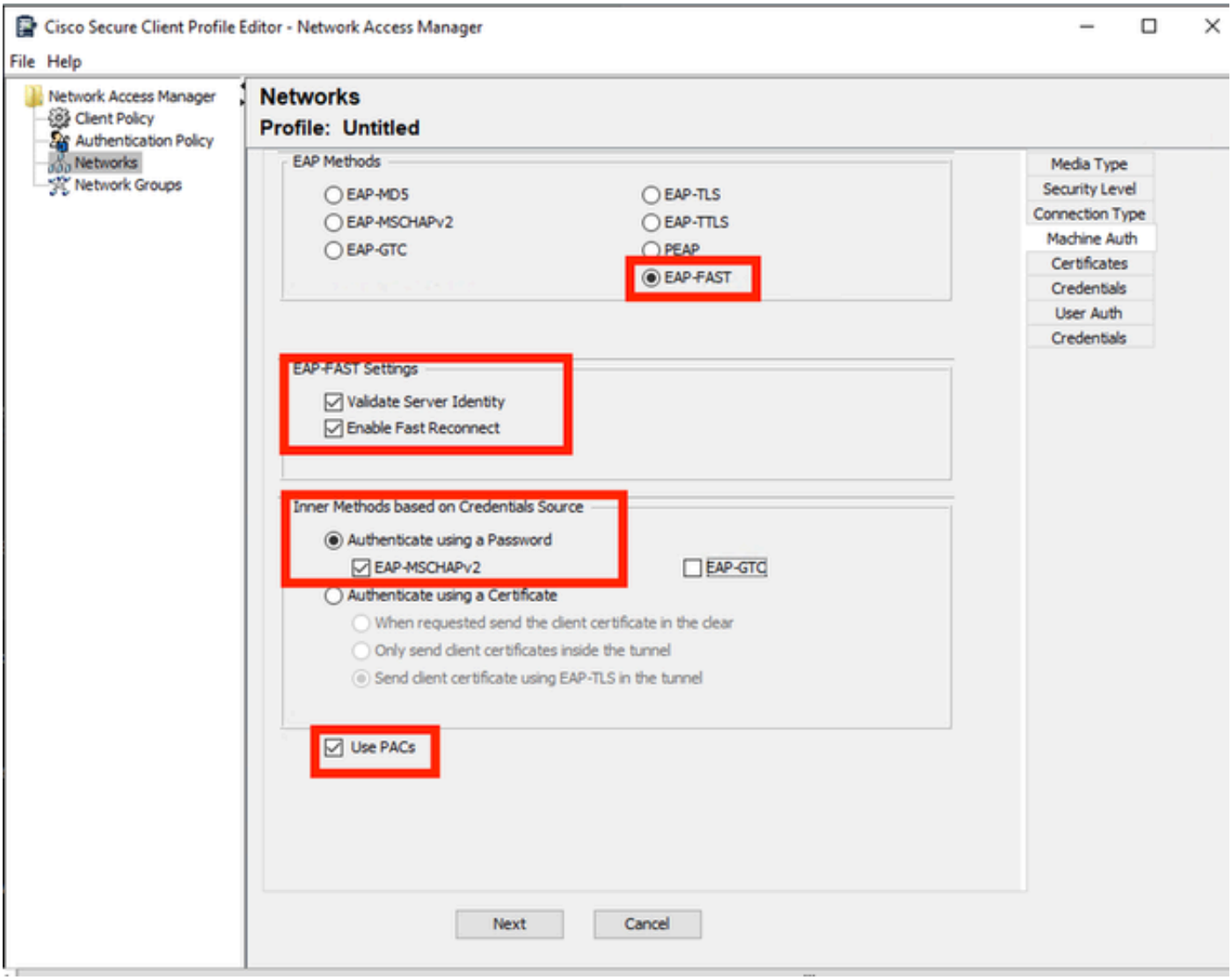
Nextをクリックして、Connection Typeセクションを続けます。



Connection Typeセクション

3番目のオプションを選択して、ユーザ認証とマシン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 Settings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。

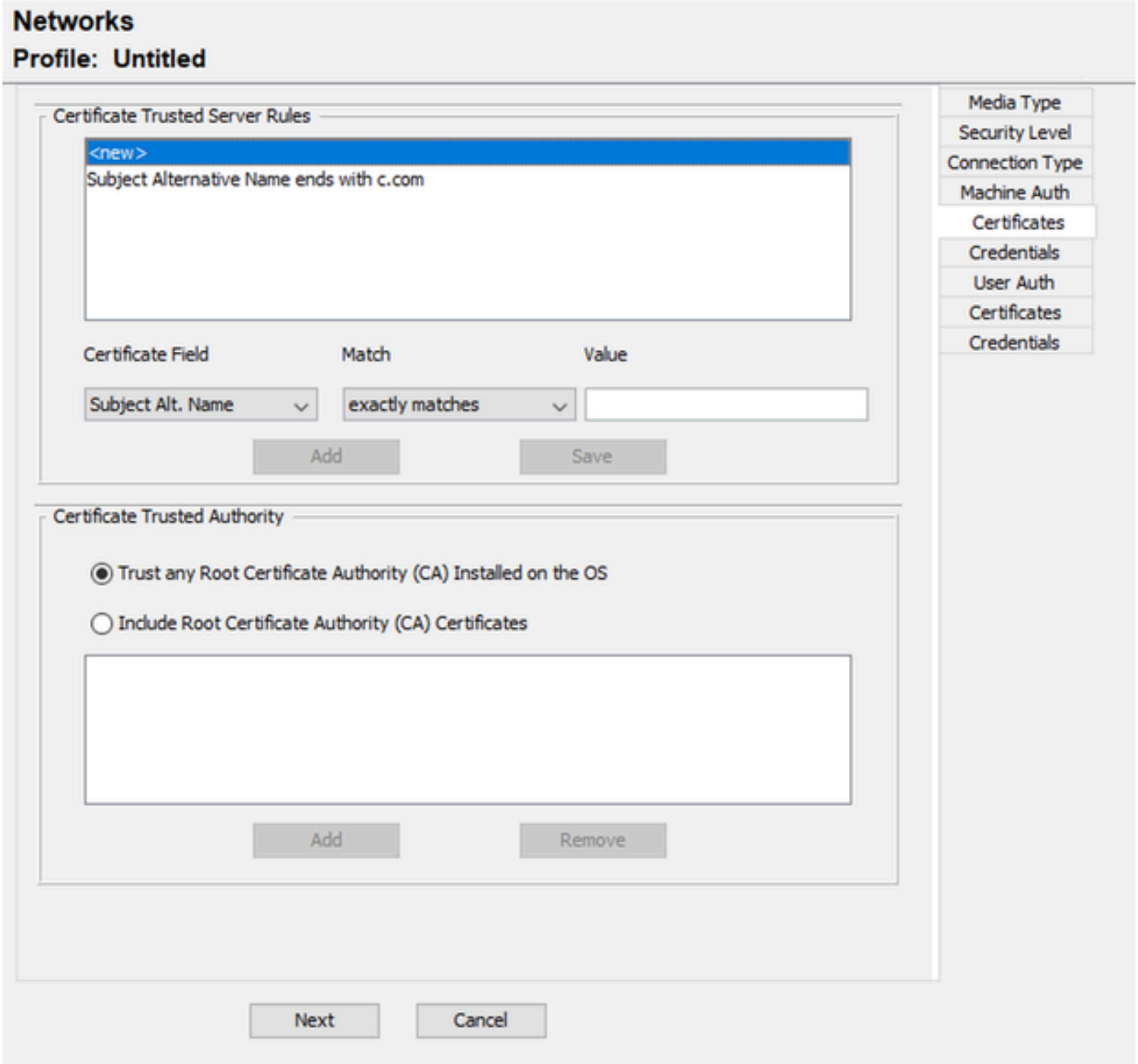
次に、Use PACsオプションを選択します。

[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。

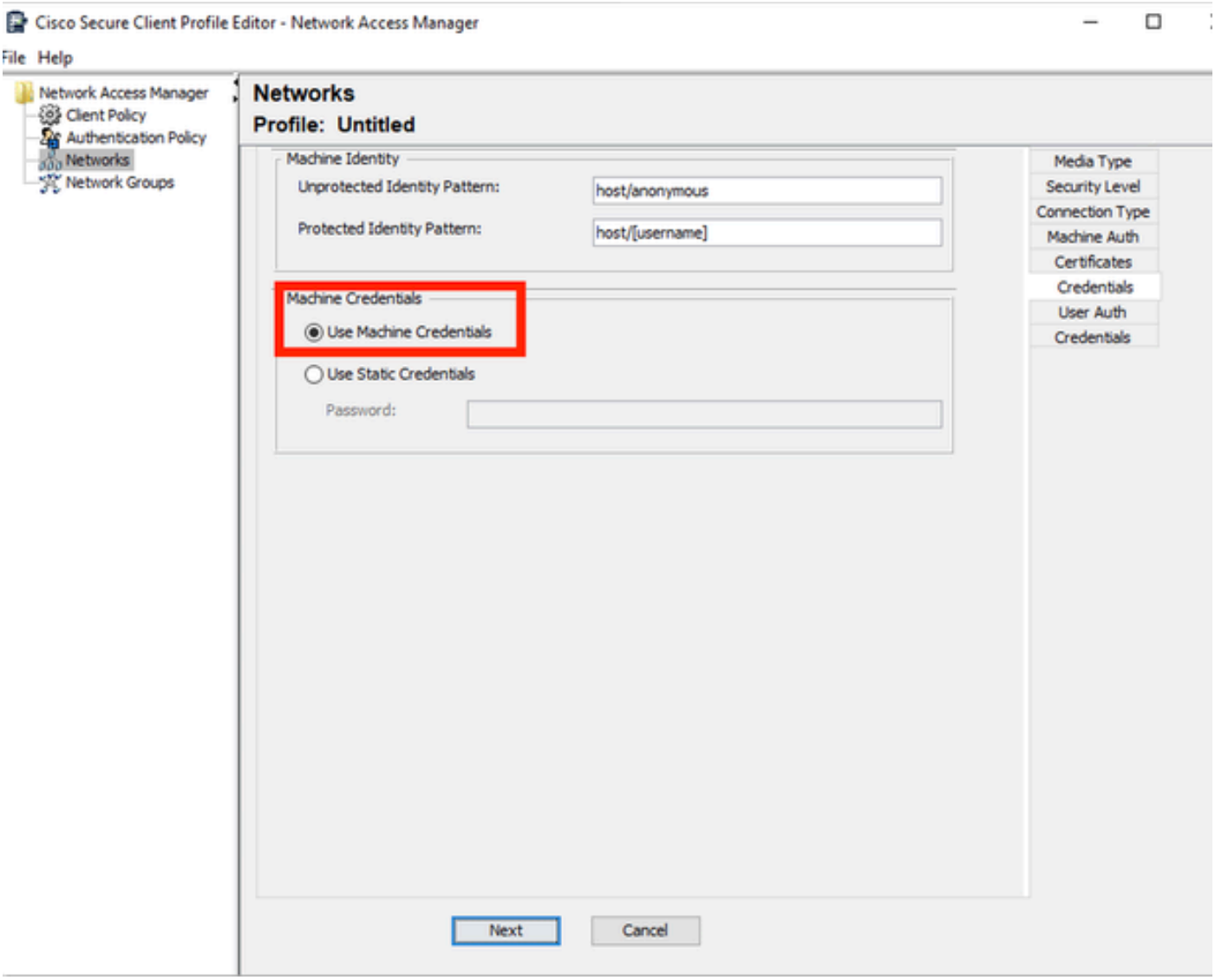


Machine Auth Server Certificate Trustセクション

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、Manage User Certsプログラムに含まれている証明書(Current User > Trusted Root Certification Authorities > Certificates)によって署名されたEAP証明書がすべて信頼されます。

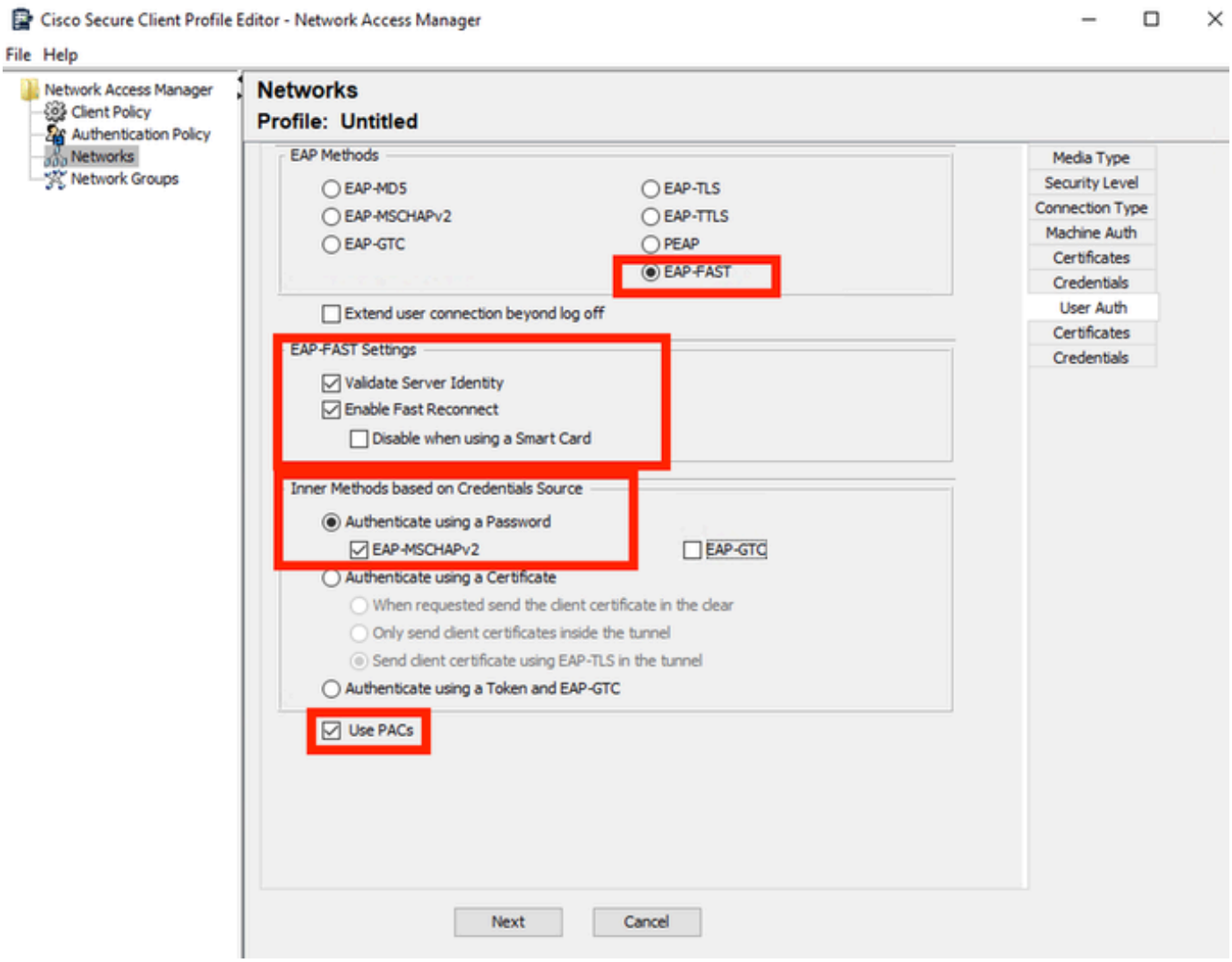
[Next] をクリックします。



Machine Auth Credentials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。



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。

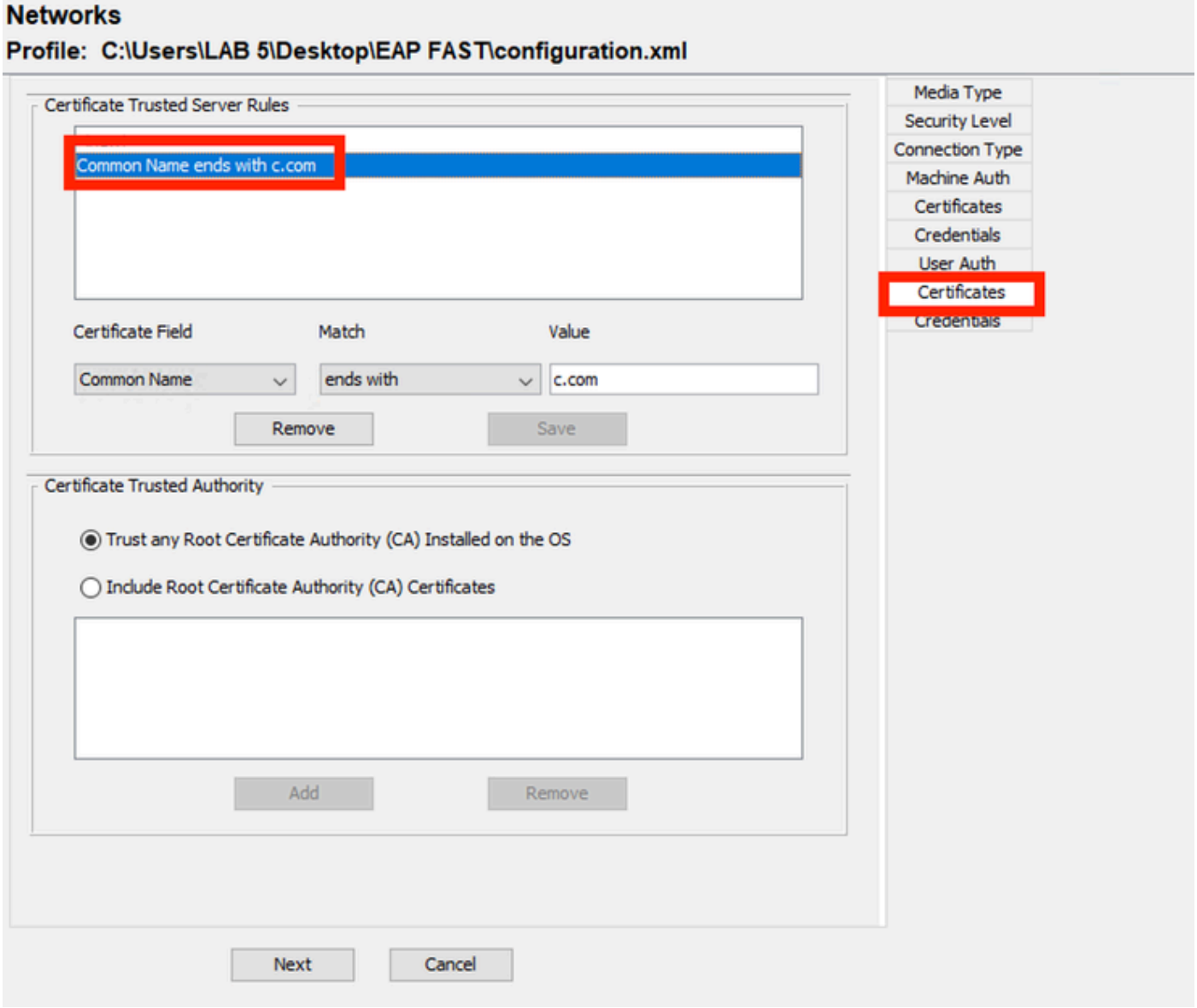
Inner Method based on credentials sourceセクションでは、方式としてAuthenticate using a PasswordおよびEAP-MSCHAPv2を選択します。

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。

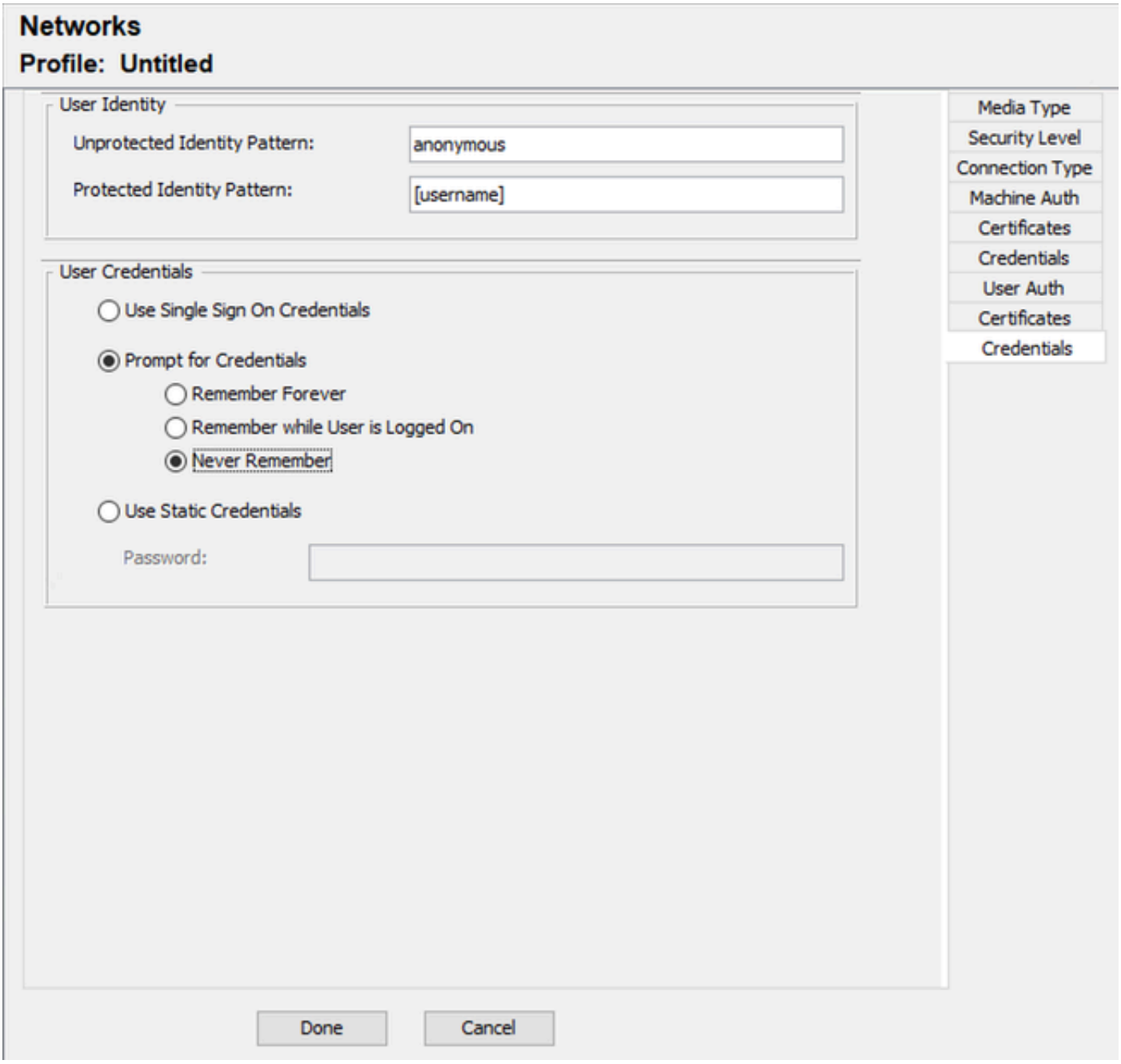
これらの設定は、EAP PEAPフロー中にサーバが使用する証明書用です。ご使用の環境でISEを使用している場合は、ポリシーサーバノードEAP証明書の共通名を使用できます。



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が使用されます。

[Next] をクリックします。



ユーザ認証クレデンシャル

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

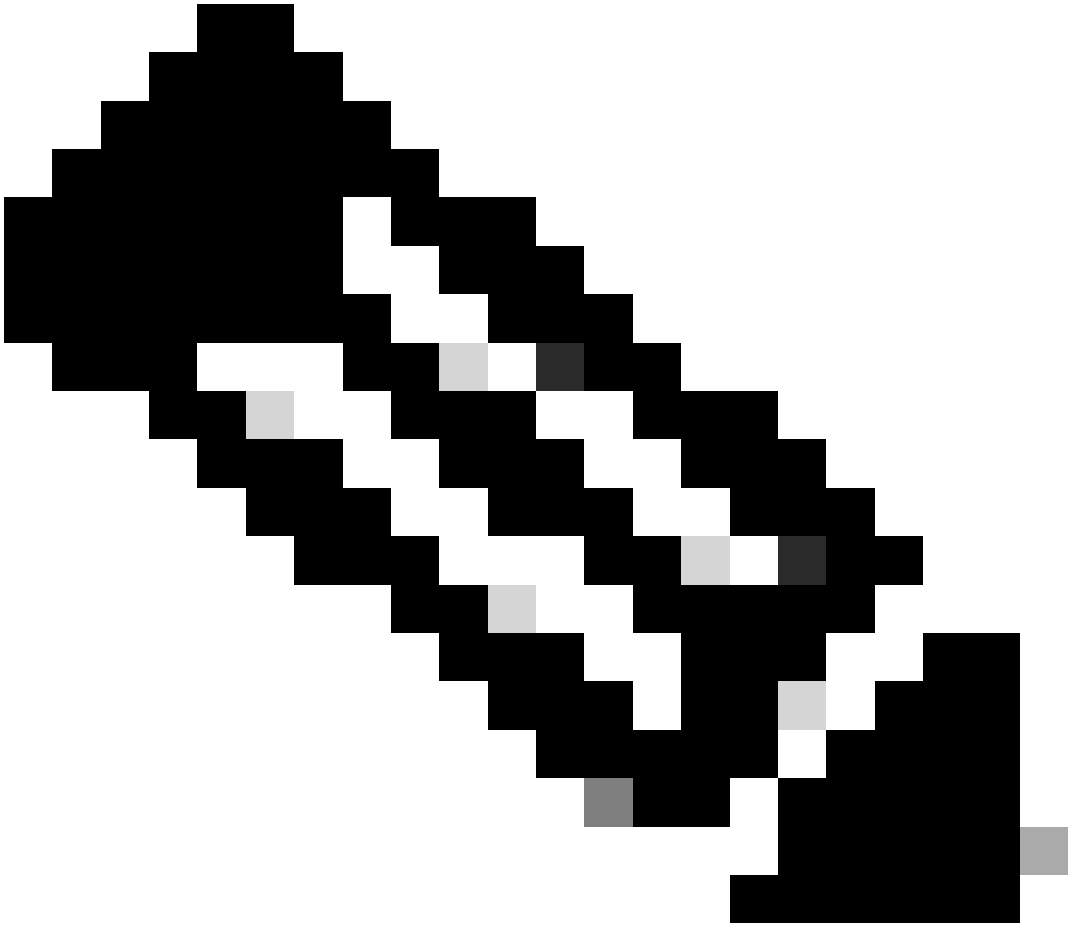
オプションPrompt for Credentials > Never Rememberが選択されています。したがって、認証のたびに、認証するユーザは自分のクレデンシャルを入力する必要があります。

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のプロファイルを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\ネットワークアクセスマネージャ\システム

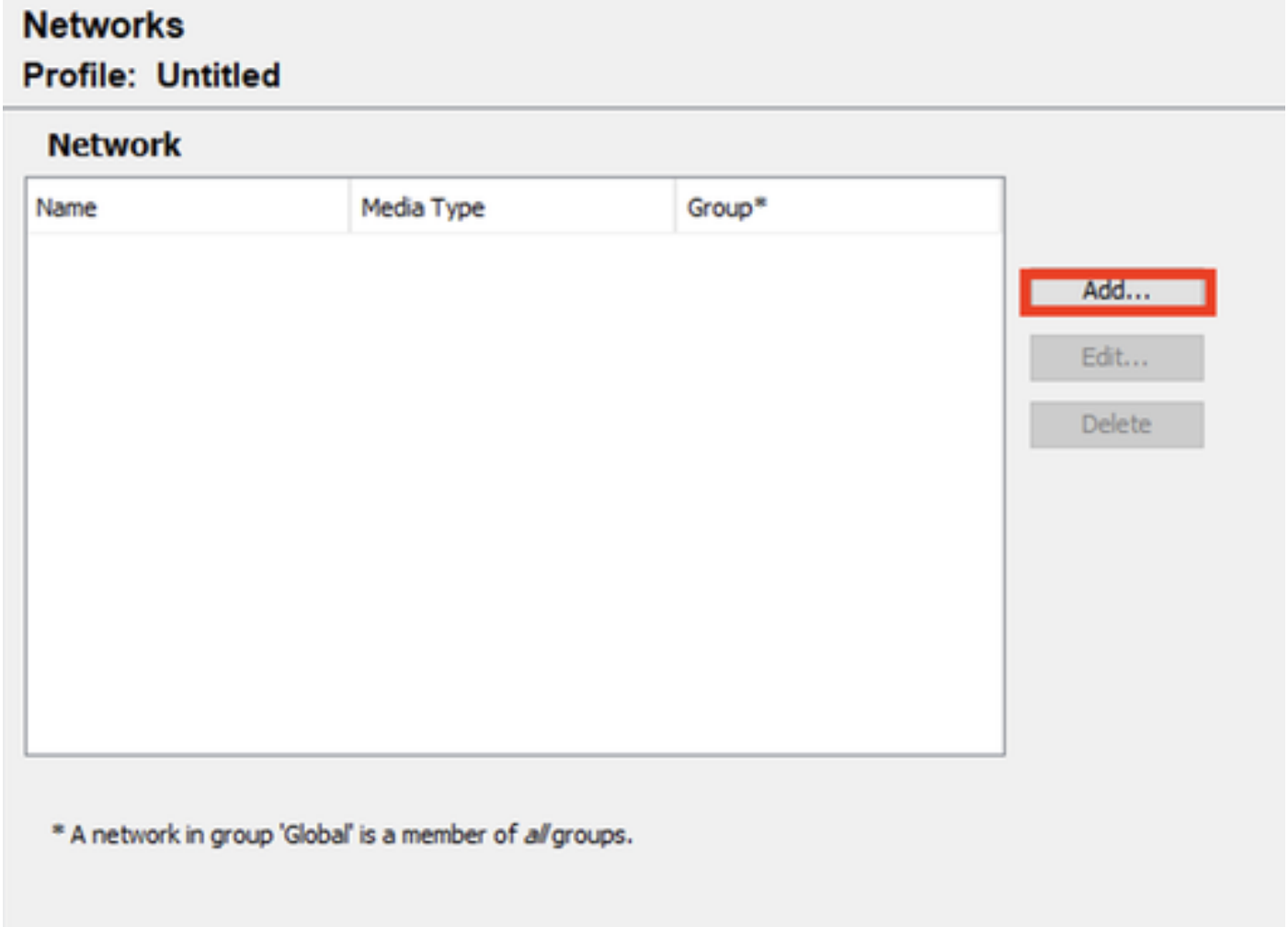


注：このファイルは、configuration.xmlという名前にする必要があります。そうしないと機能しません。

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サプリカントの設定

NAM Profile Editorを開き、Networksセクションに移動します。

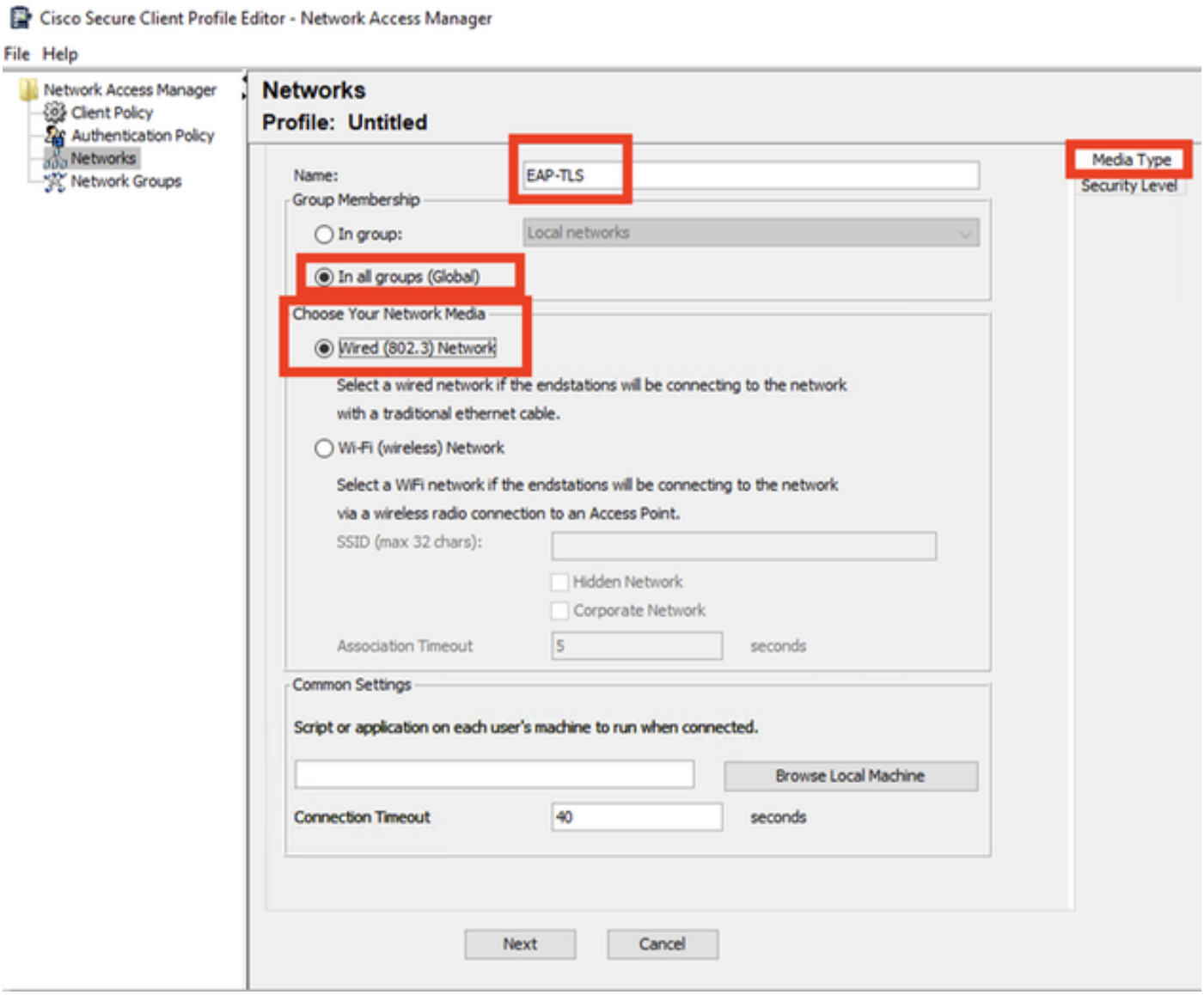
[Add] をクリックします。



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。

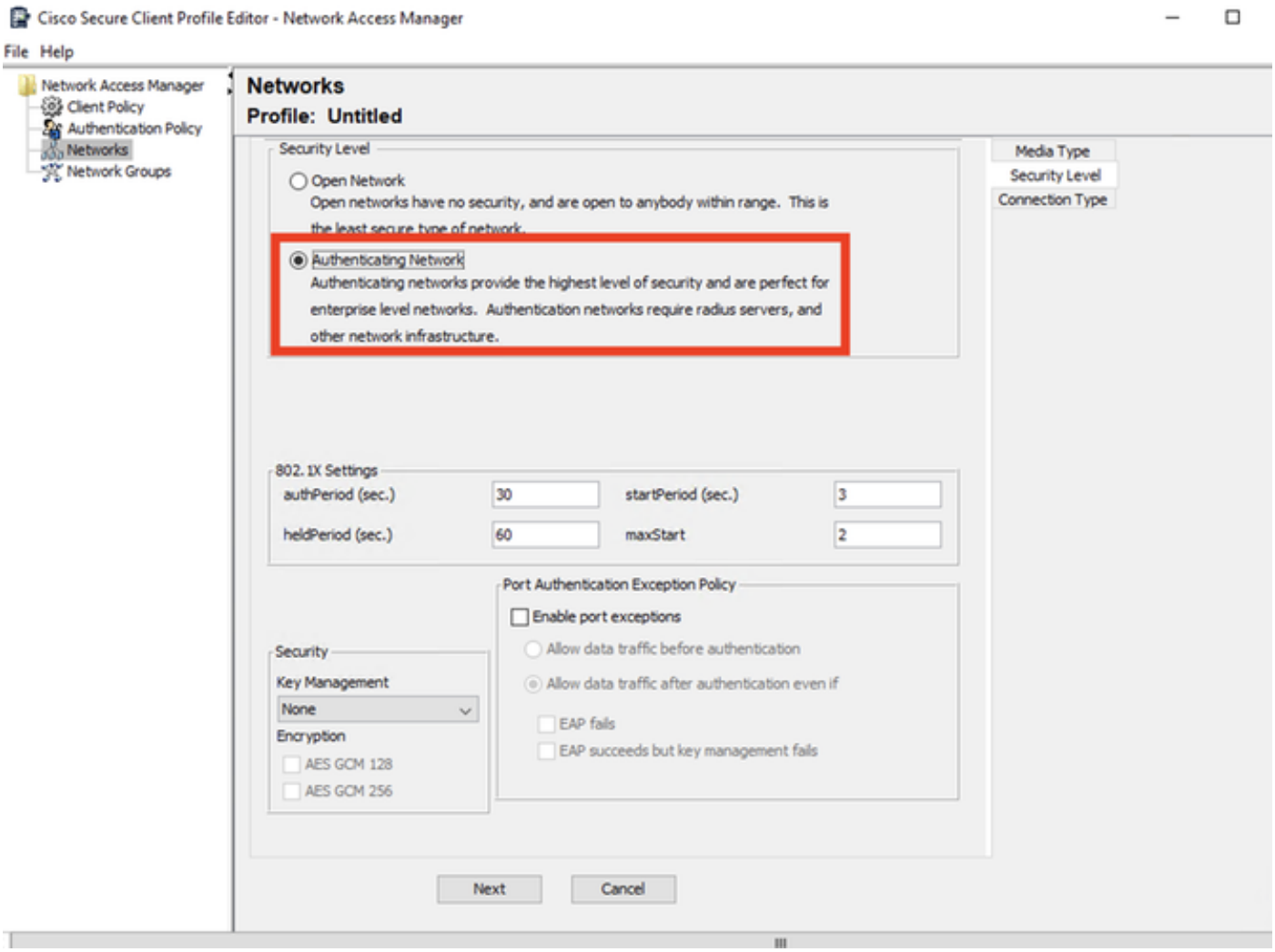
Group MembershipにGlobalを選択します。および有線ネットワークメディアです。



Media Typeセクション

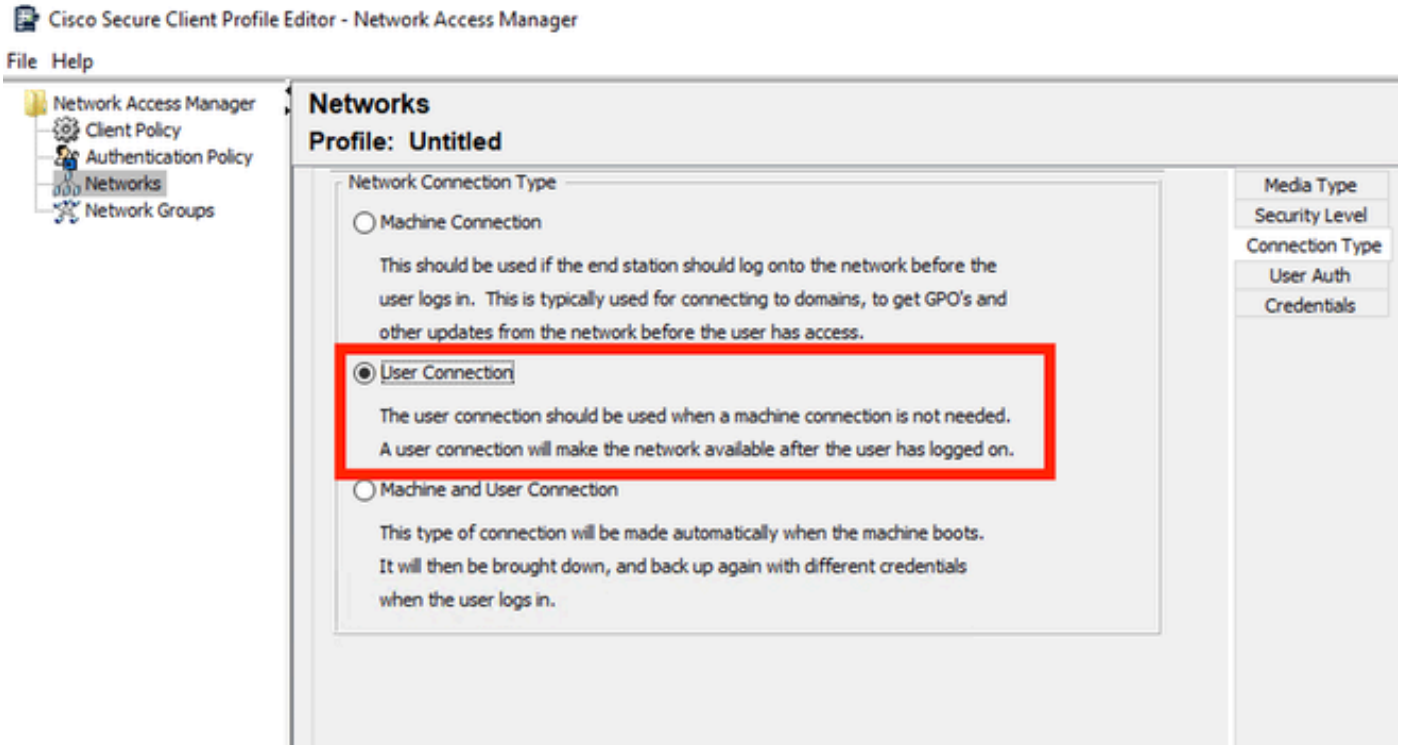
[Next] をクリックします。

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。



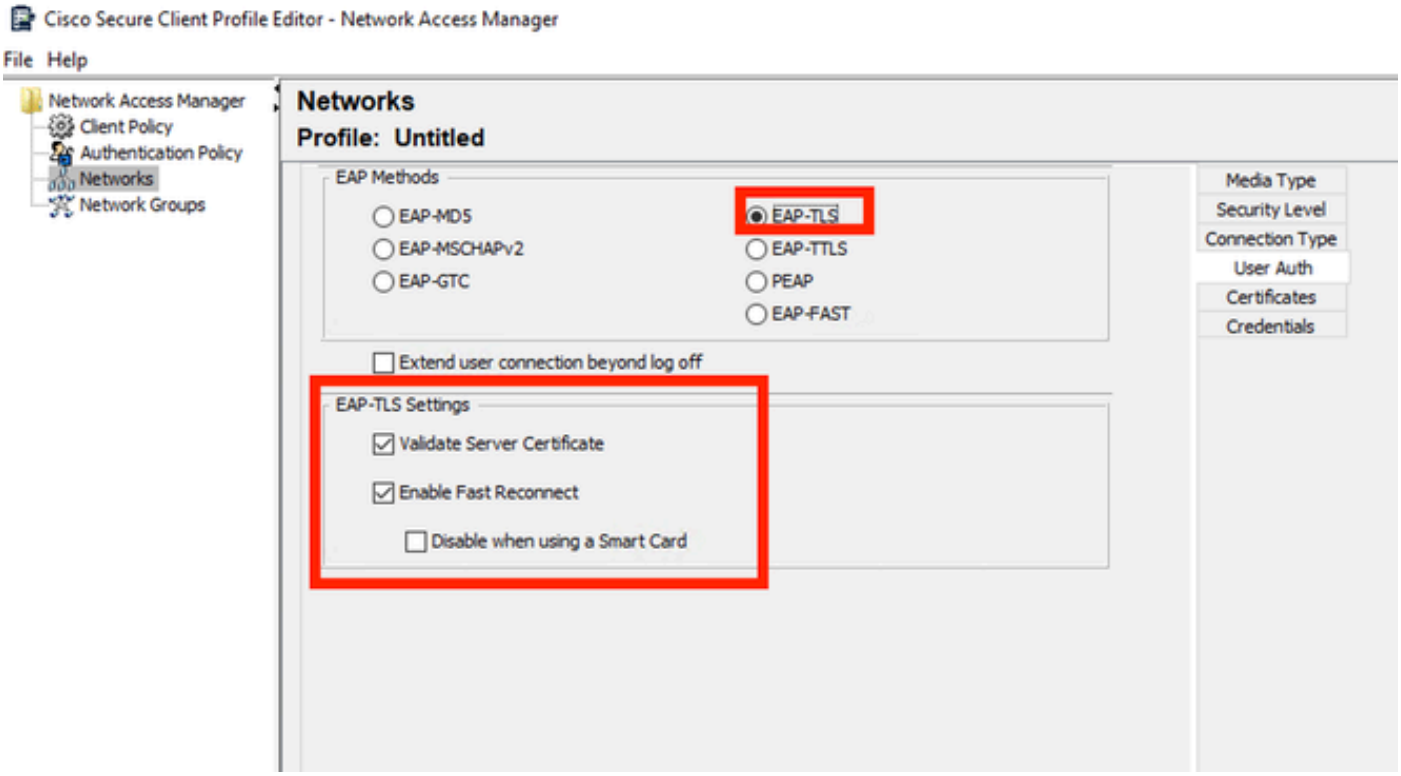
セキュリティレベル

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。そのため、オプションUser Connectionが使用されます。



接続タイプ

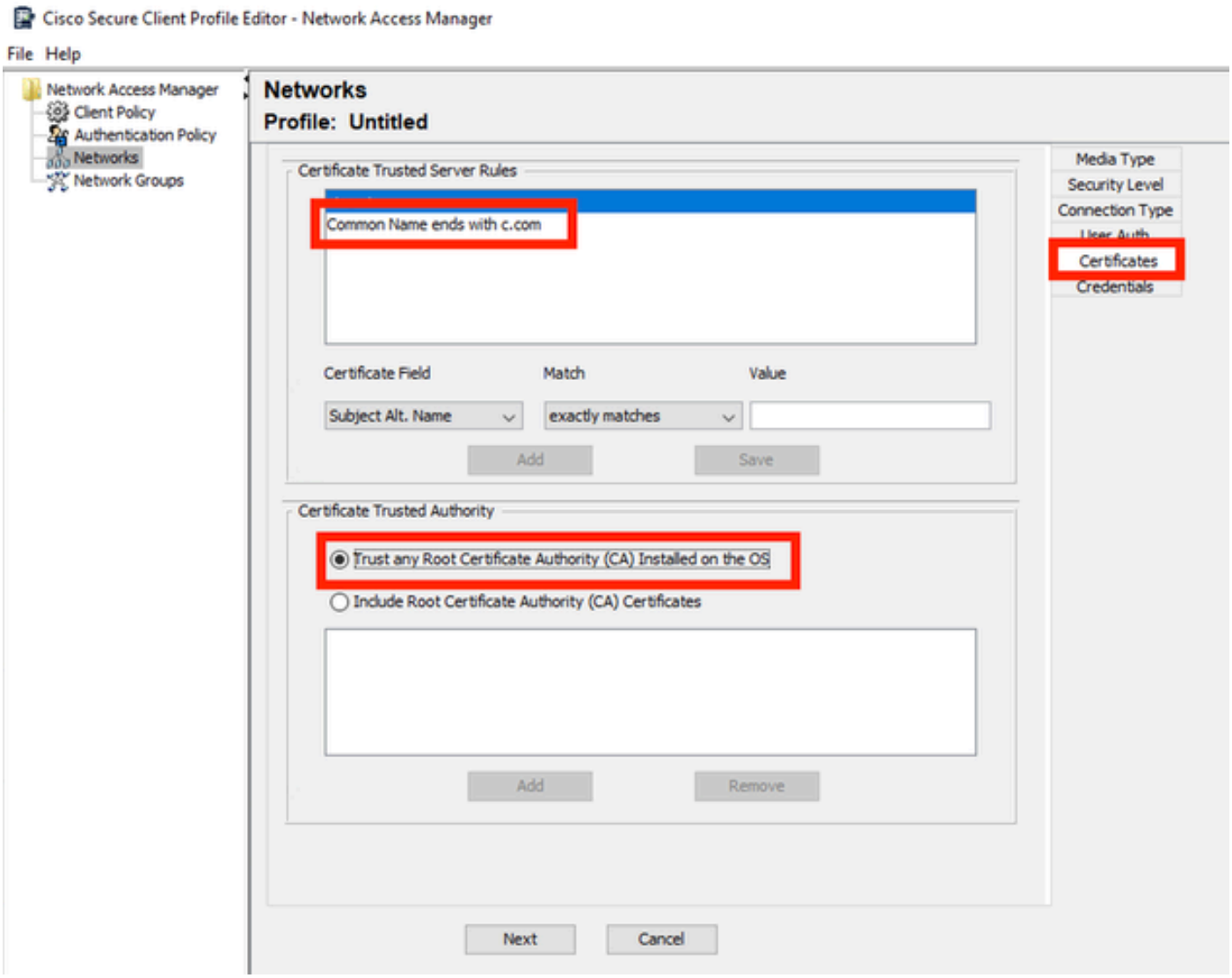
EAP方式としてEAP-TLSを設定します。EAP-TLS settingsセクションでデフォルト値を変更しないでください。



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見つけます。

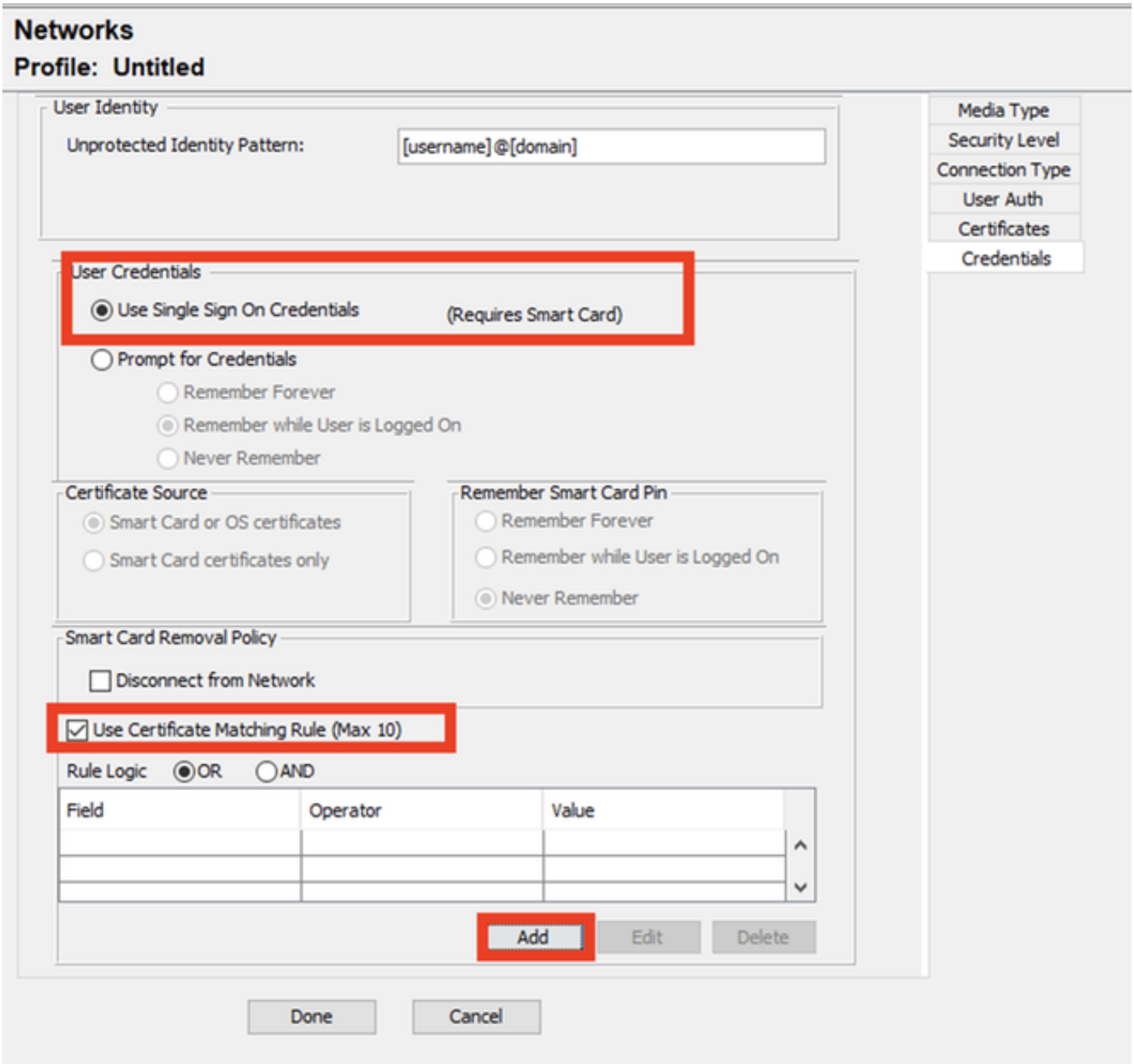
Certificate Trusted Authorityセクションで、Trust any Root Certificate Authority (CA) installed on the OSを選択します。



ユーザー認証サーバー証明書の信頼の設定

[Next] をクリックします。

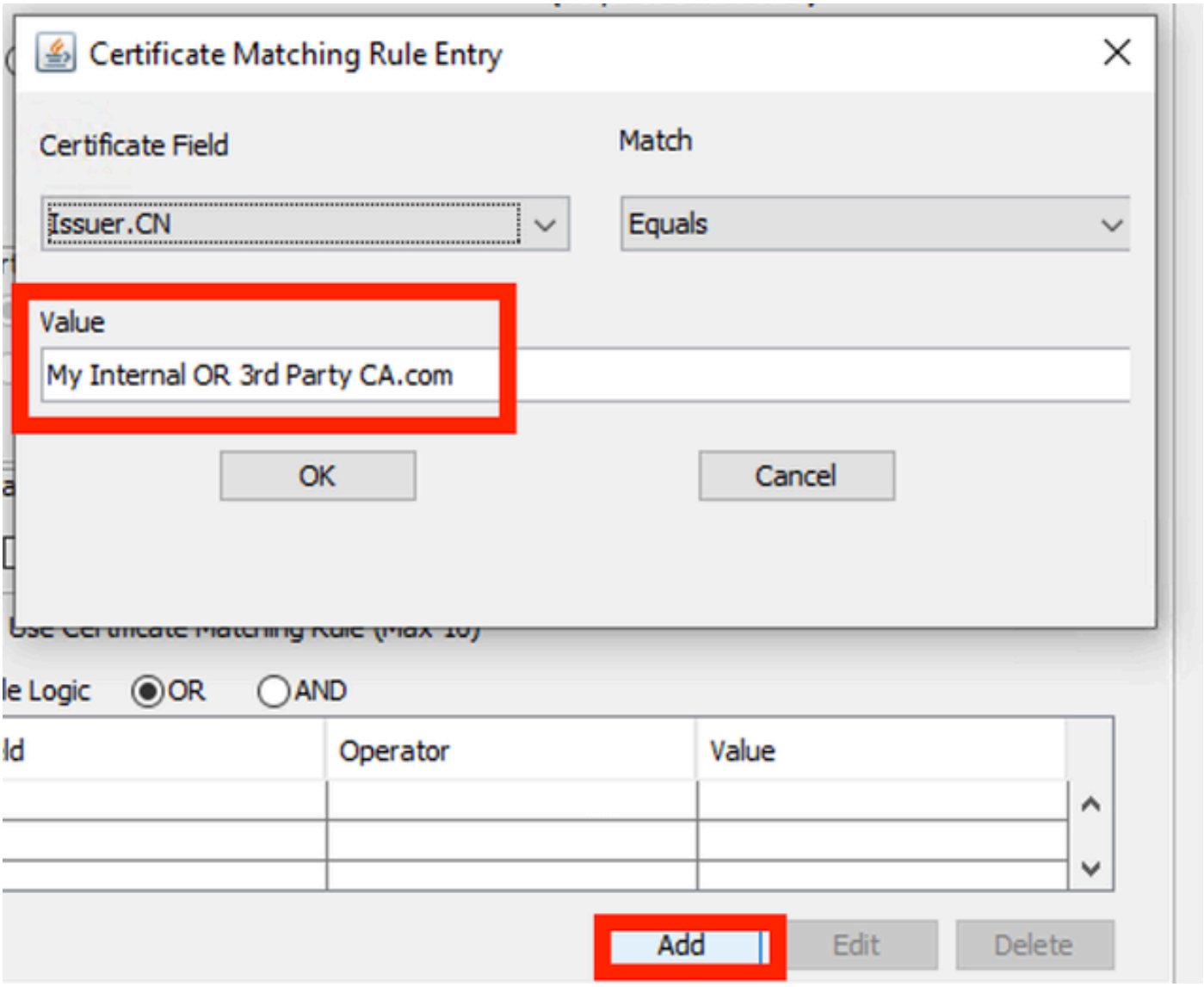
User Credentialsセクションでは、最初の部分のデフォルト値を変更しないでください。



*User Auth Credentials*セクション

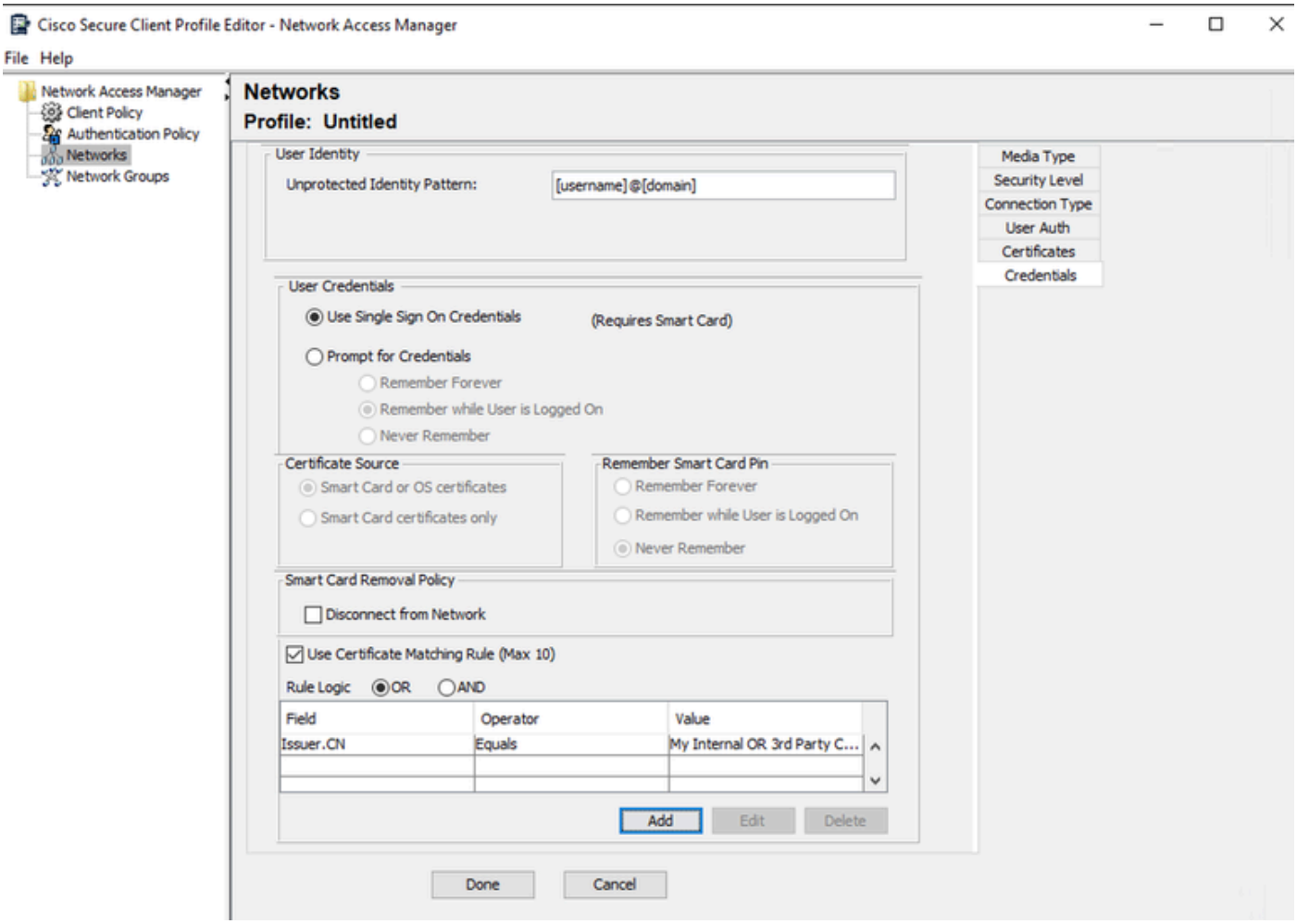
EAP TLSプロセス中にユーザが送信するID証明書と一致するルールを設定することが重要です。これを行うには、Use Certificate Maching Rule (Max 10)の横にあるチェックボックスをクリックします。

[Add] をクリックします。



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。



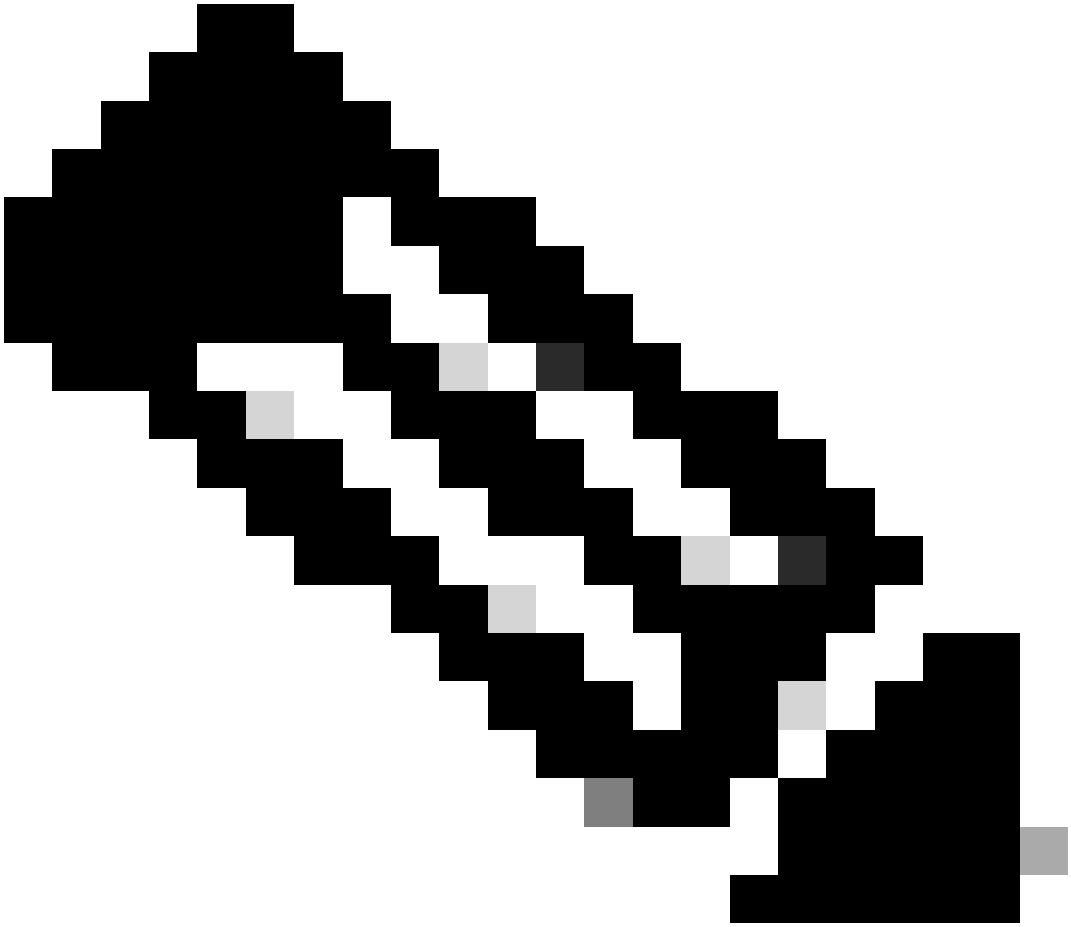
*User Auth Certificate Credentials*セクション

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\ネットワークアクセスマネージャ\システム

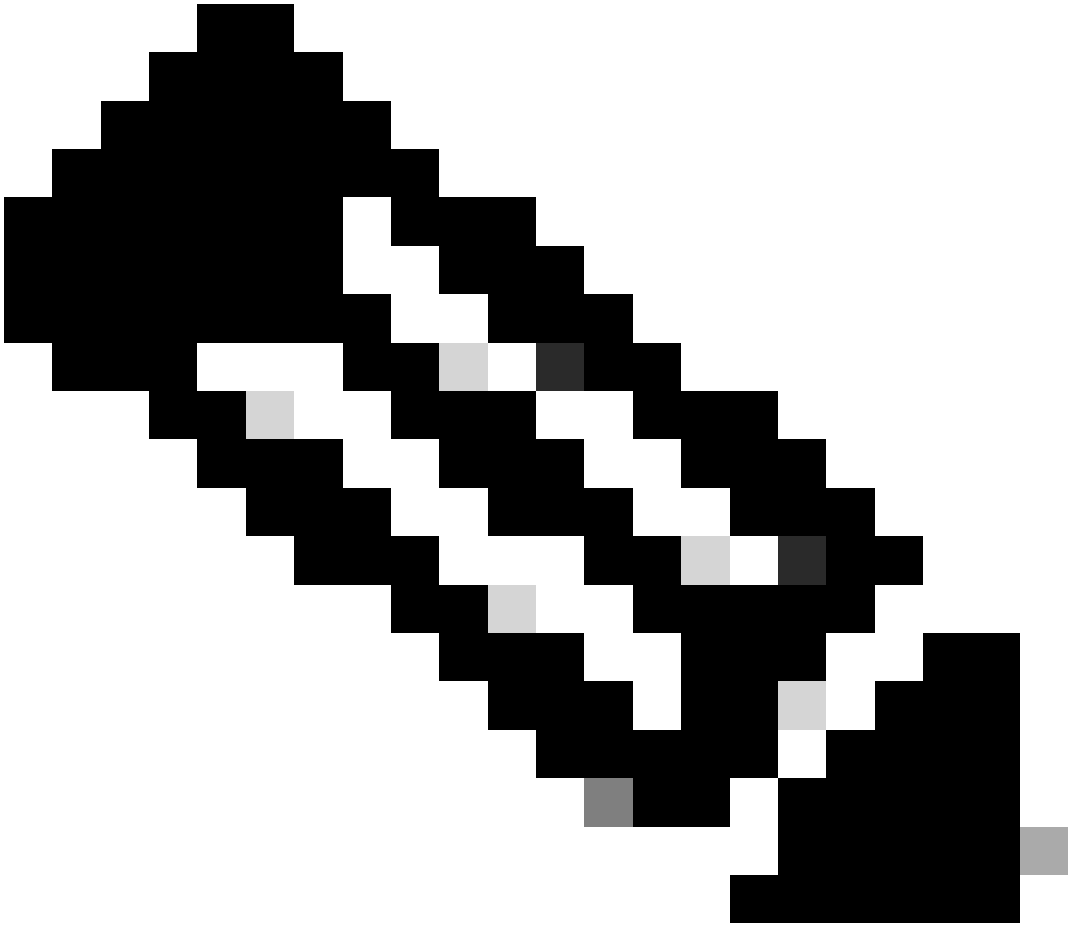


注：このファイルは、configuration.xmlという名前にする必要があります。そうしないと機能しません。

7. シナリオ1 PEAP MSCHAPv2に基づいて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、NADがdot1xを機能させるために必要な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の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>
```

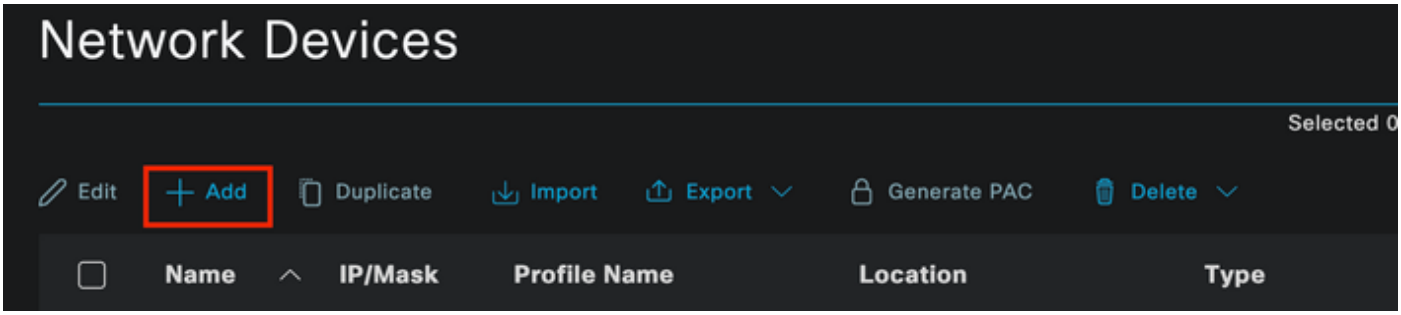
```
!
!
aaa group server radius ISE-CLUSTER
 server name ISE-PSN-1
!
interface GigabitEthernet0/1/0
 description "Endpoint that supports dot1x"
 switchport access vlan 15
 switchport mode access
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication 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。

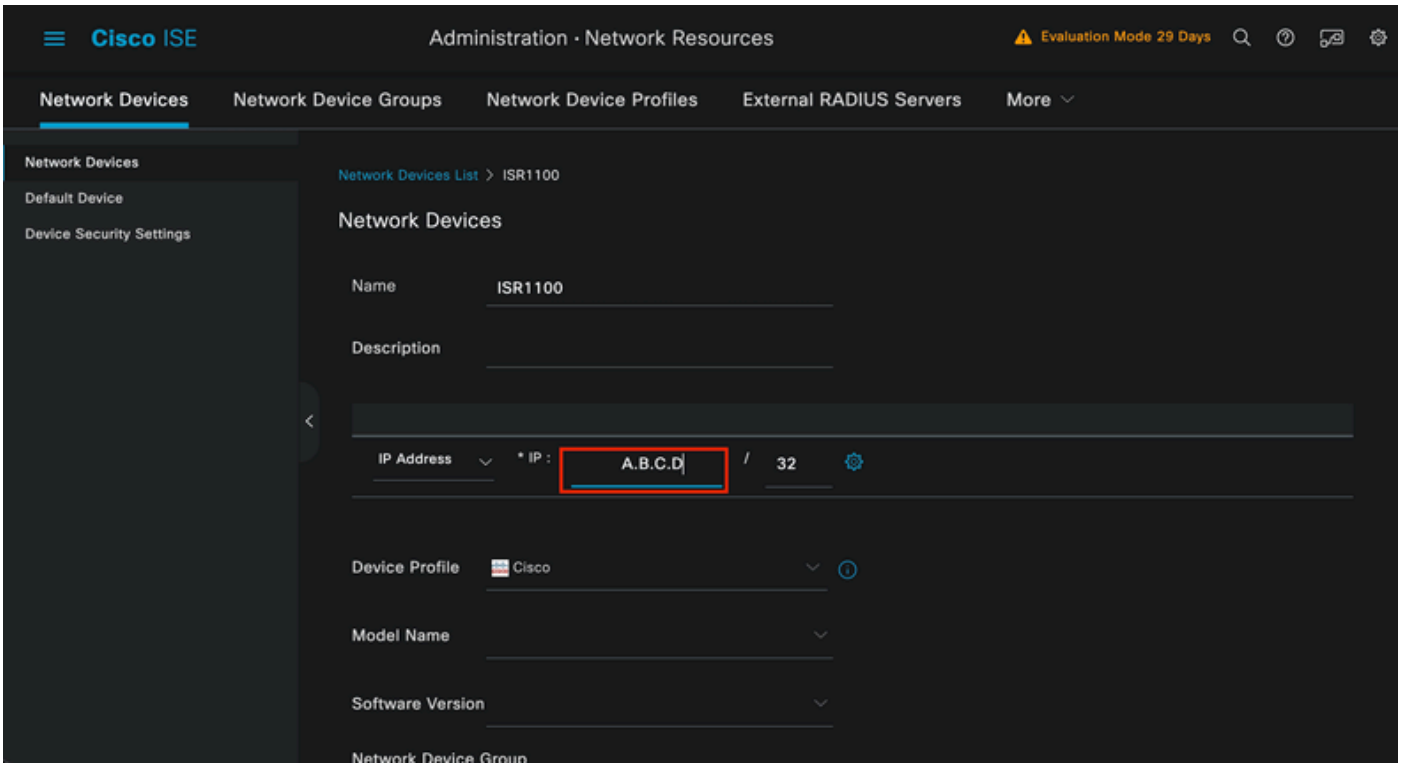
ISE Administration > Network Resources > Network DevicesにISR NADを追加します。

[Add] をクリックします。



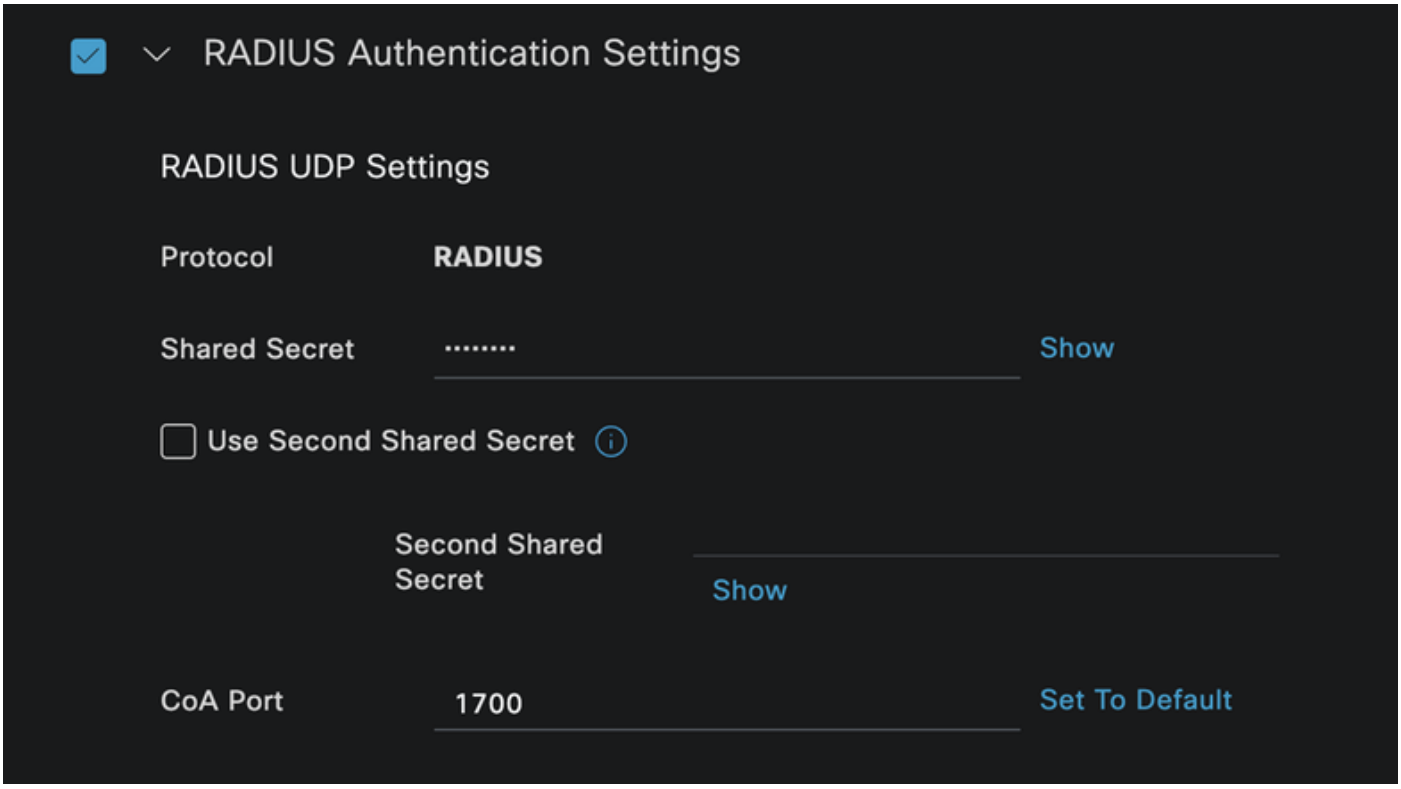
Network Deviceセクション

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の設定で使用したものと同じ共有秘密を追加します。



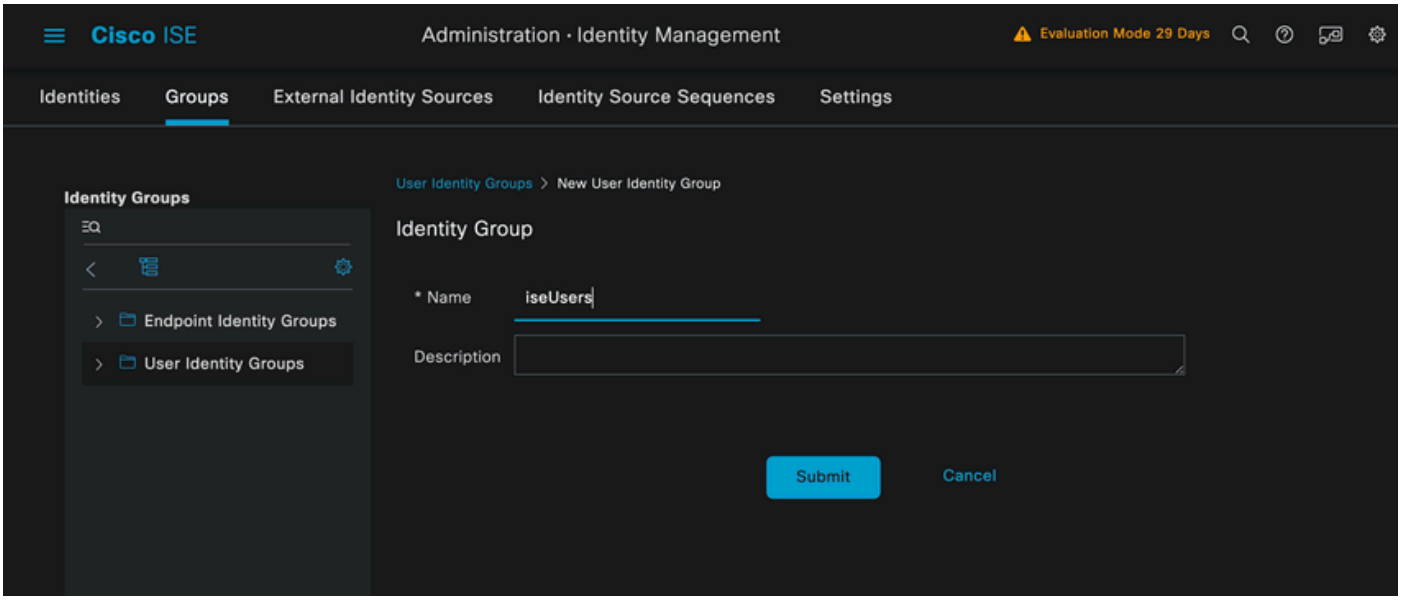
ネットワークデバイスの*Radius*設定

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。

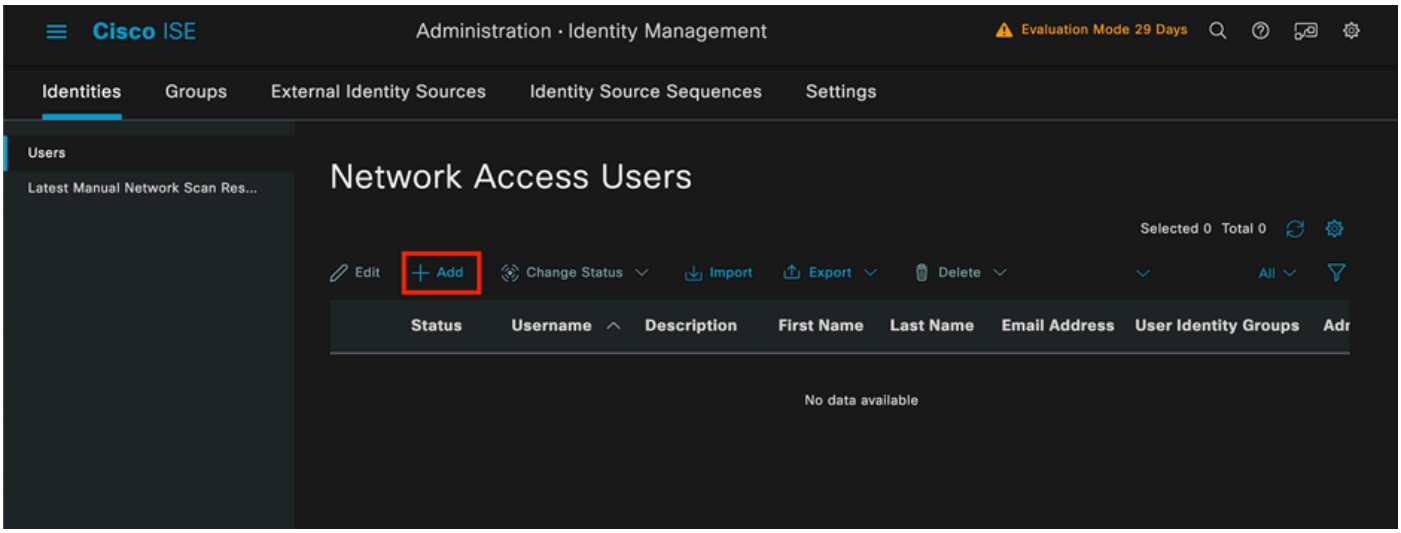


IDグループの作成

[Submit] をクリックします。

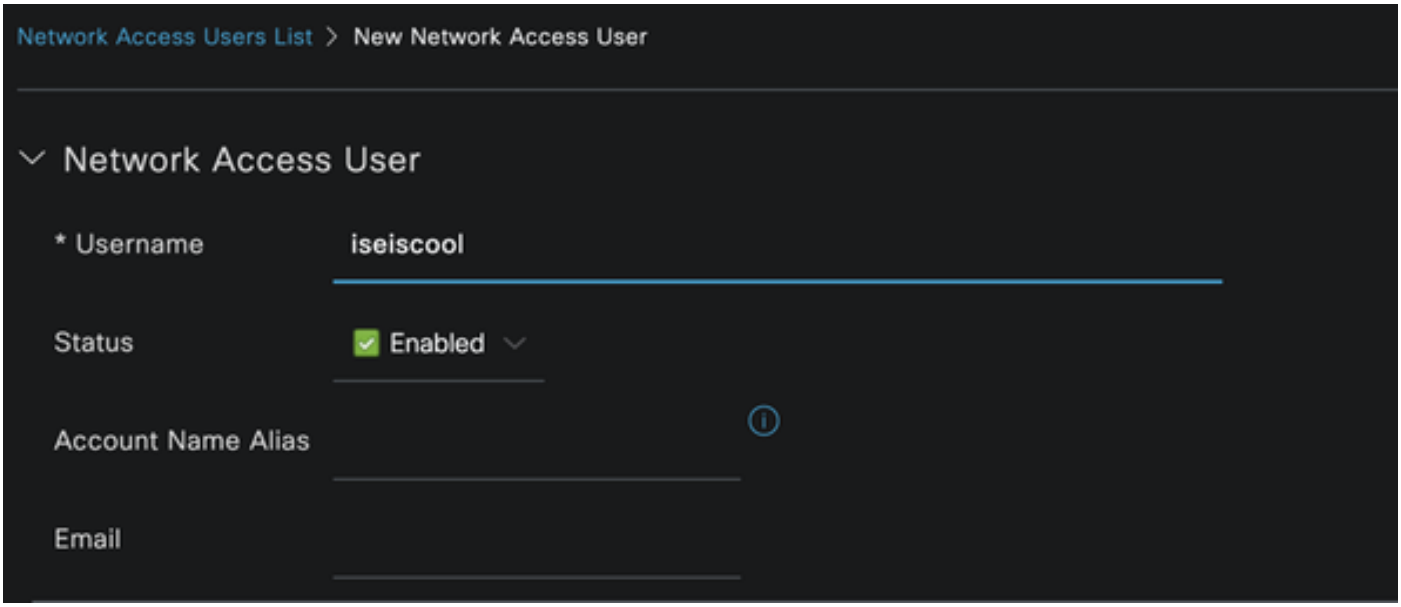
Administration > Identity Management > Identityタブの順に移動します。

[Add] をクリックします。



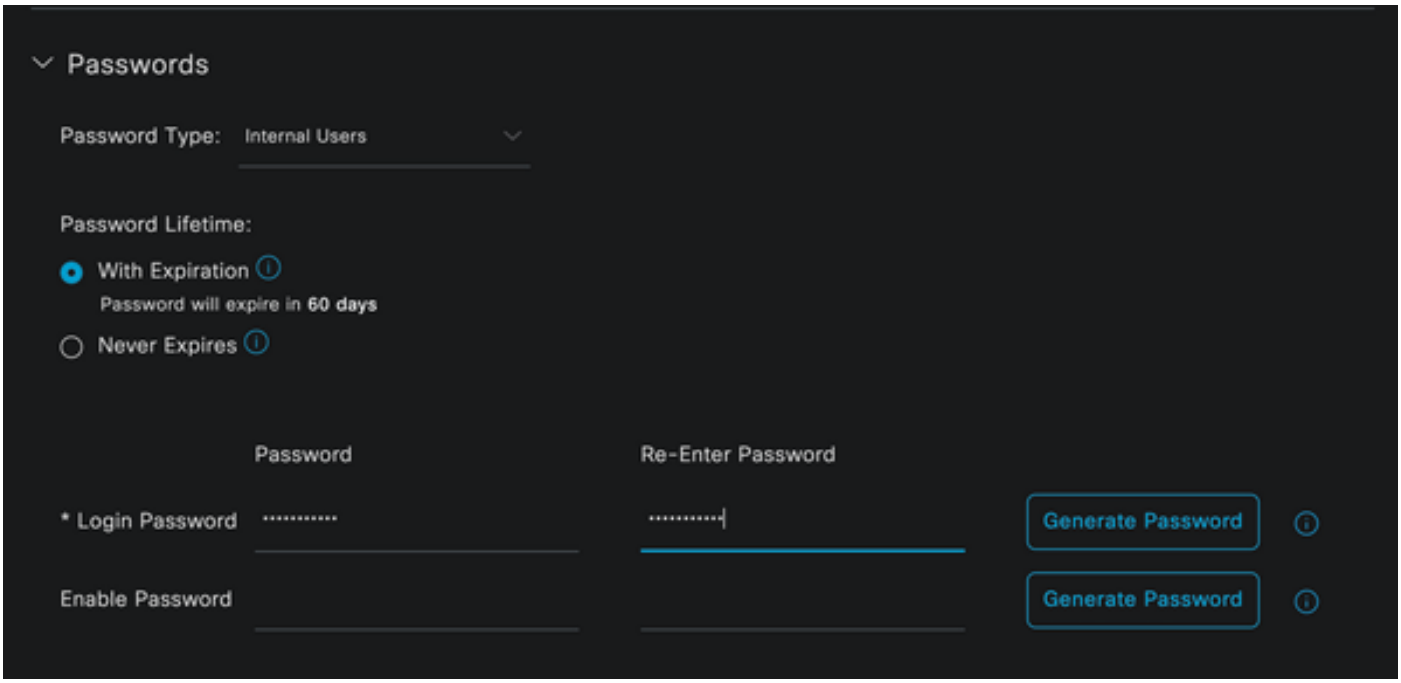
Network Access Usersセクション

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。



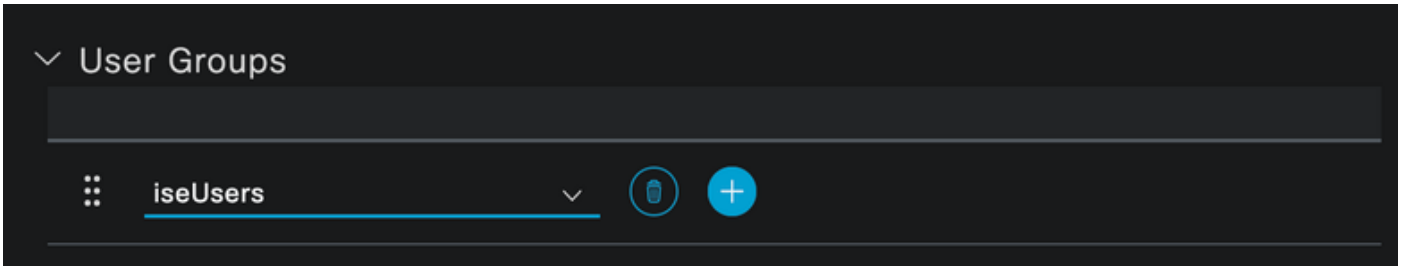
ネットワークアクセスユーザの作成

ユーザにパスワードを割り当てます。 VainitlaISE97が使用されます。



*User Creation Password*セクション

ユーザをグループiseUsersに割り当てます。

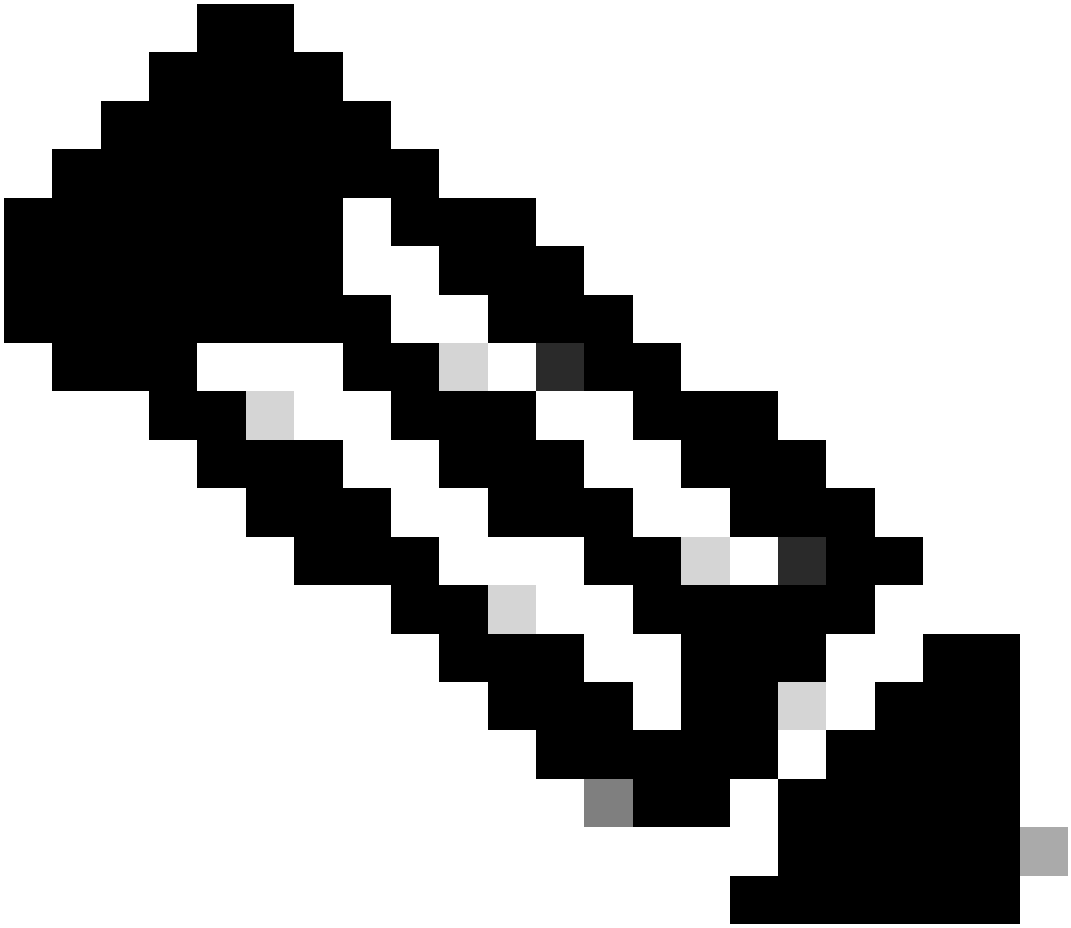


ユーザグループの割り当て

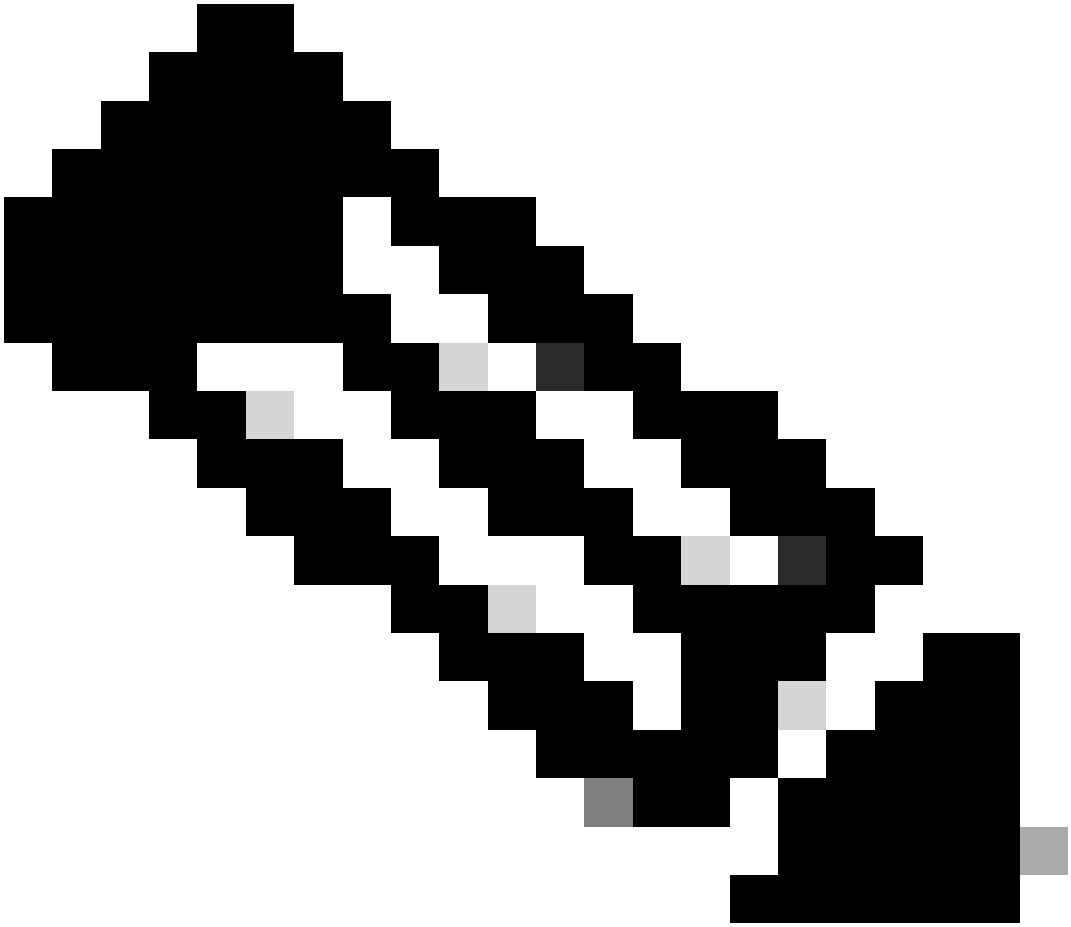
ポリシーセットの設定.

ISEメニュー>ポリシー>ポリシーセットに移動します。

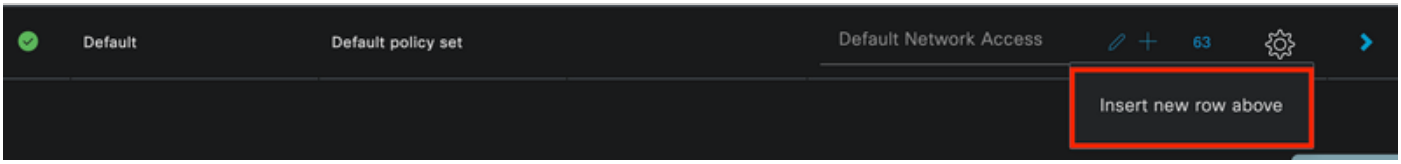
デフォルトのポリシーセットを使用できるただし、この例ではWiredという名前のAPが作成されます。



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。

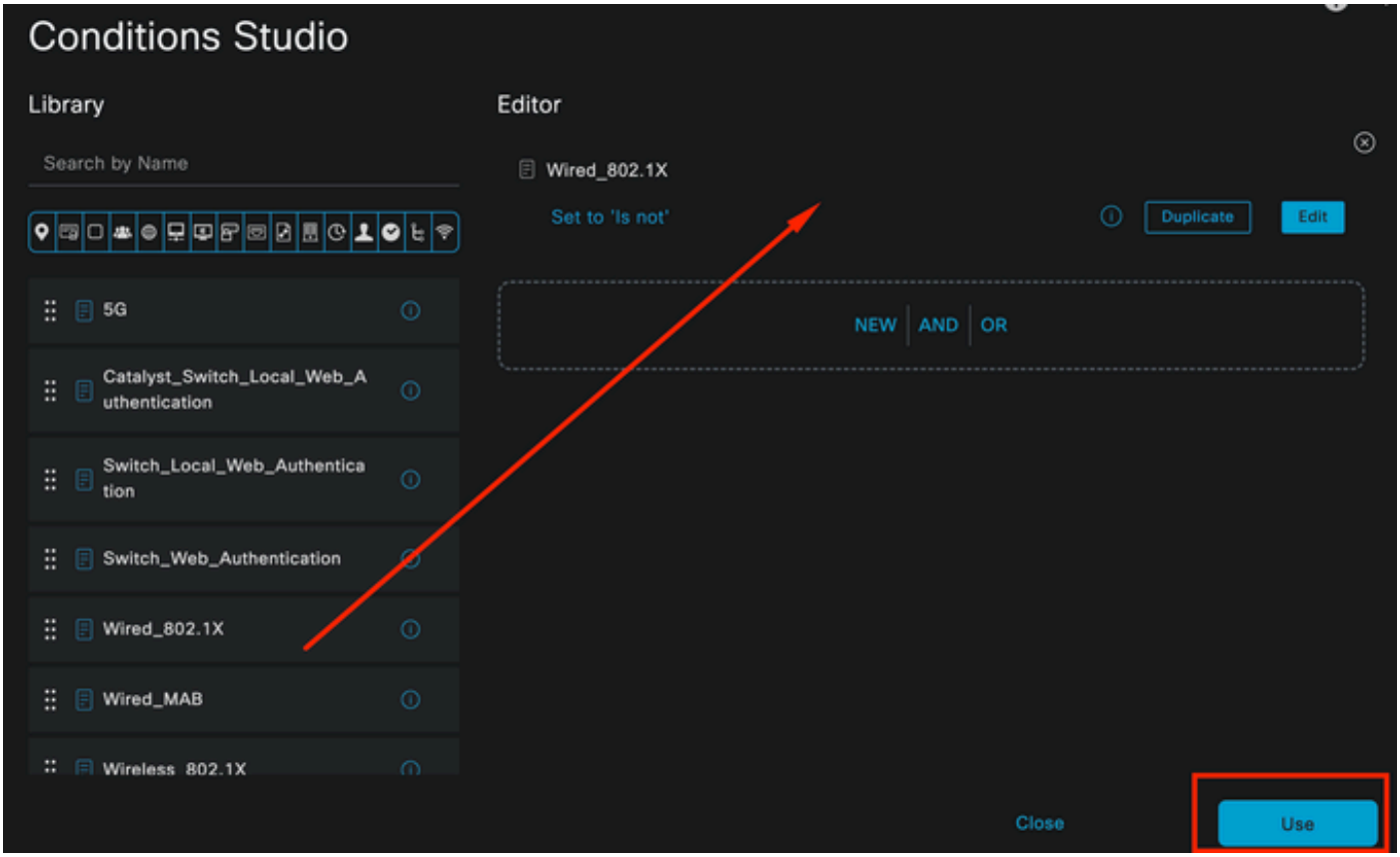


注：追加アイコンまたはプラスアイコンが表示されていない場合は、任意のポリシーセットの歯車アイコンをクリックし、[上に新しい行を挿入]を選択できます。



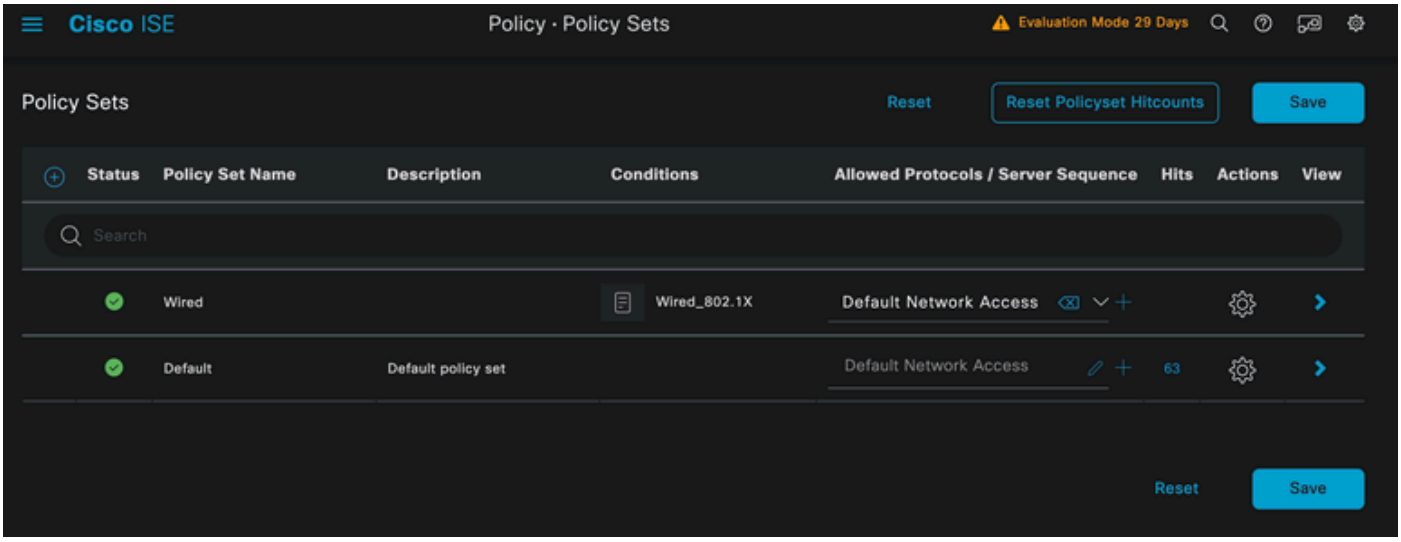
歯車アイコンのオプション

使用されている条件は有線8021xです。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。

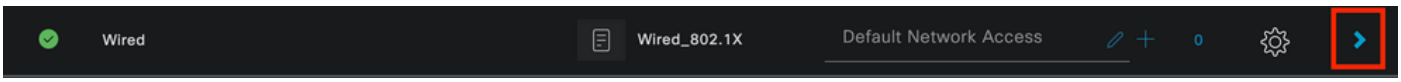


ポリシーセットの一般ビュー

[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。

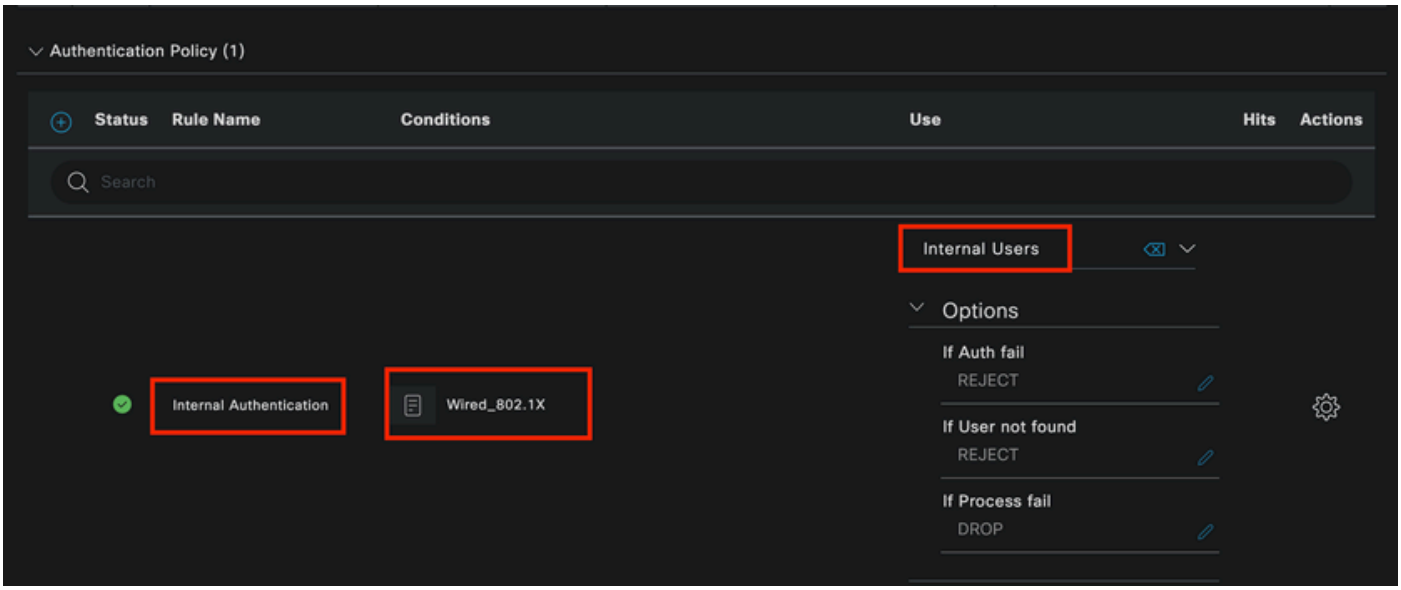
認証ポリシー

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。

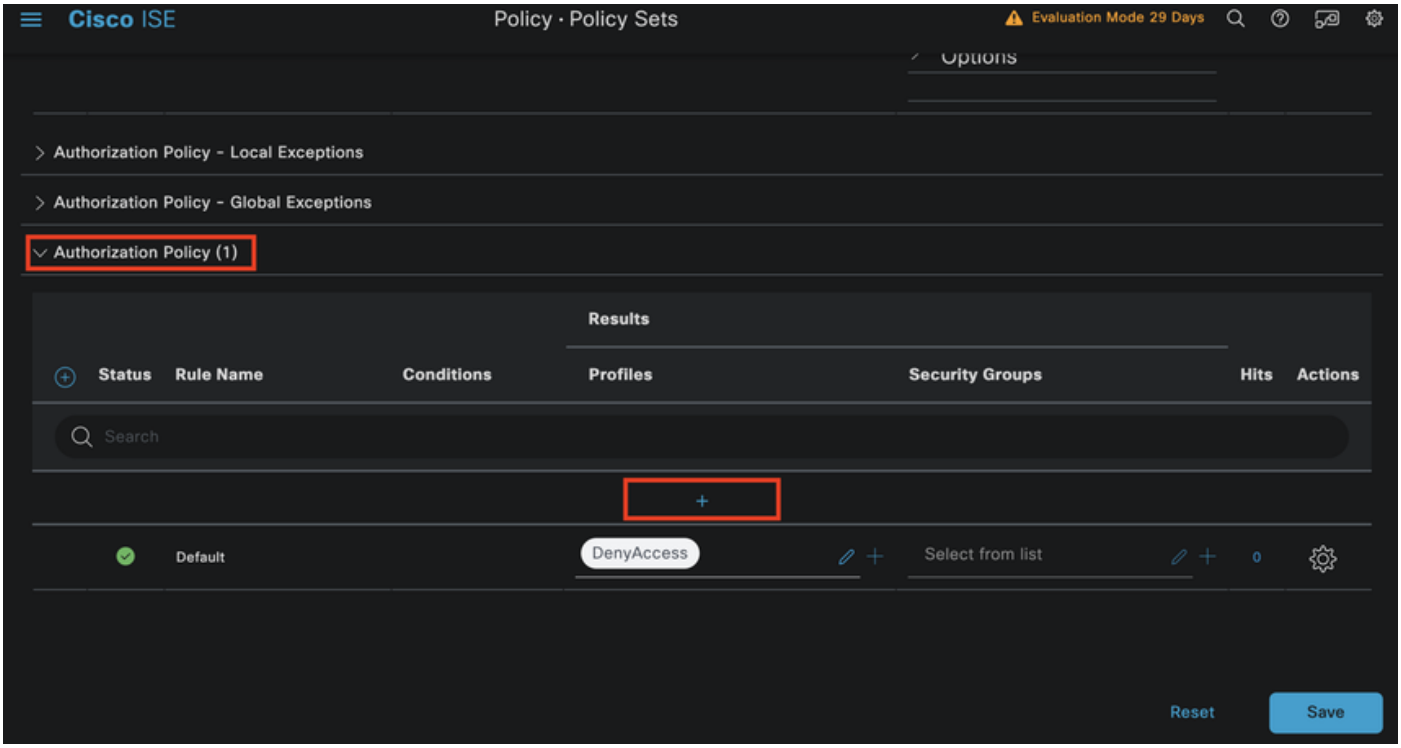
最後に、Use列でInternal Usersを選択します。



認証ポリシー

認可ポリシー.

Authorization Policyセクションはページの一番下にあります。これを展開し、+アイコンをクリックします。



認可ポリシー

最近作成した認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が使用されています。

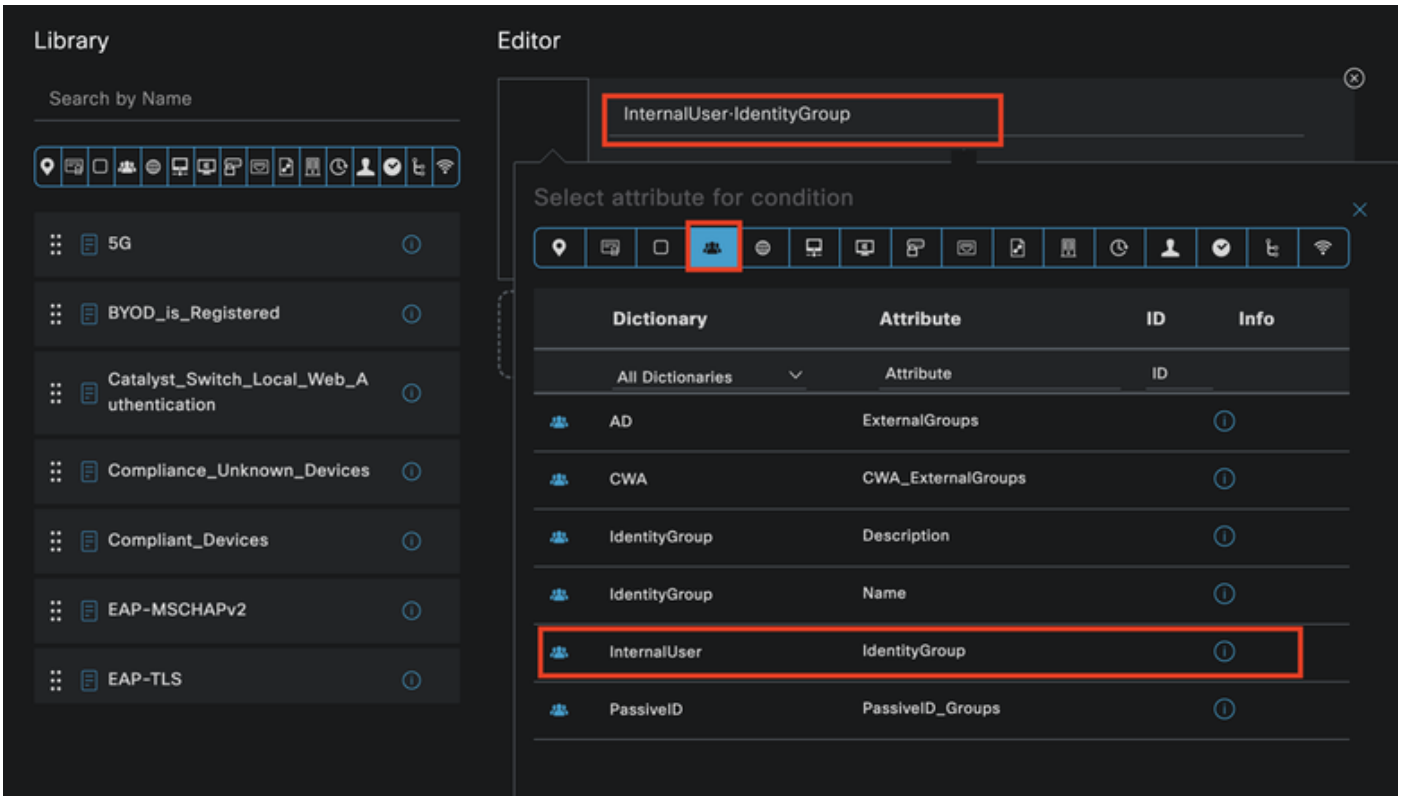
この認可ポリシーの条件を作成するには、Conditions列の+アイコンをクリックします。

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。

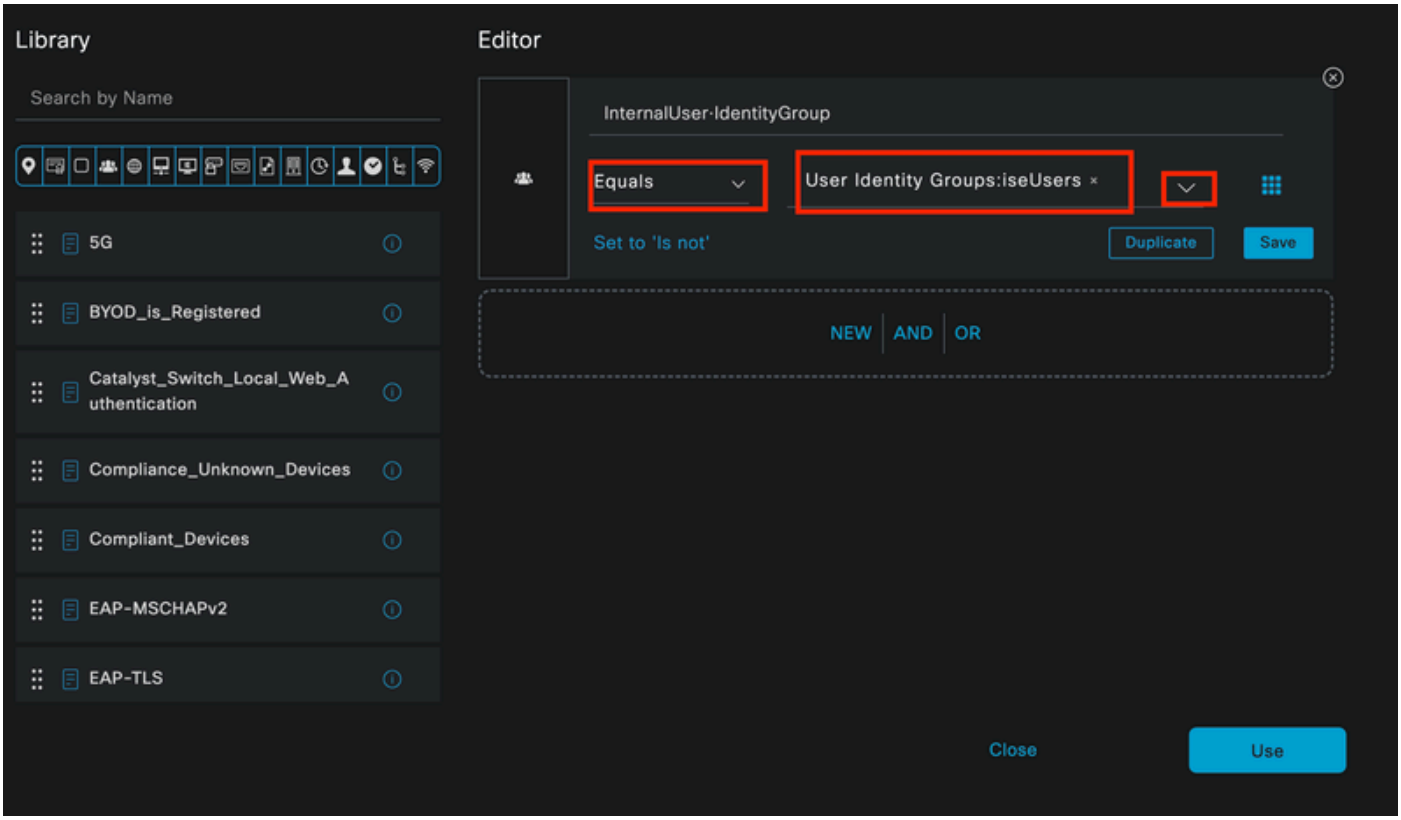
ディクショナリで、IdentityGroup属性が含まれているInternalUserディクショナリを選択します。



条件の作成

Equals演算子を選択します。

User Identity Groupsから、グループIseUsersを選択します。

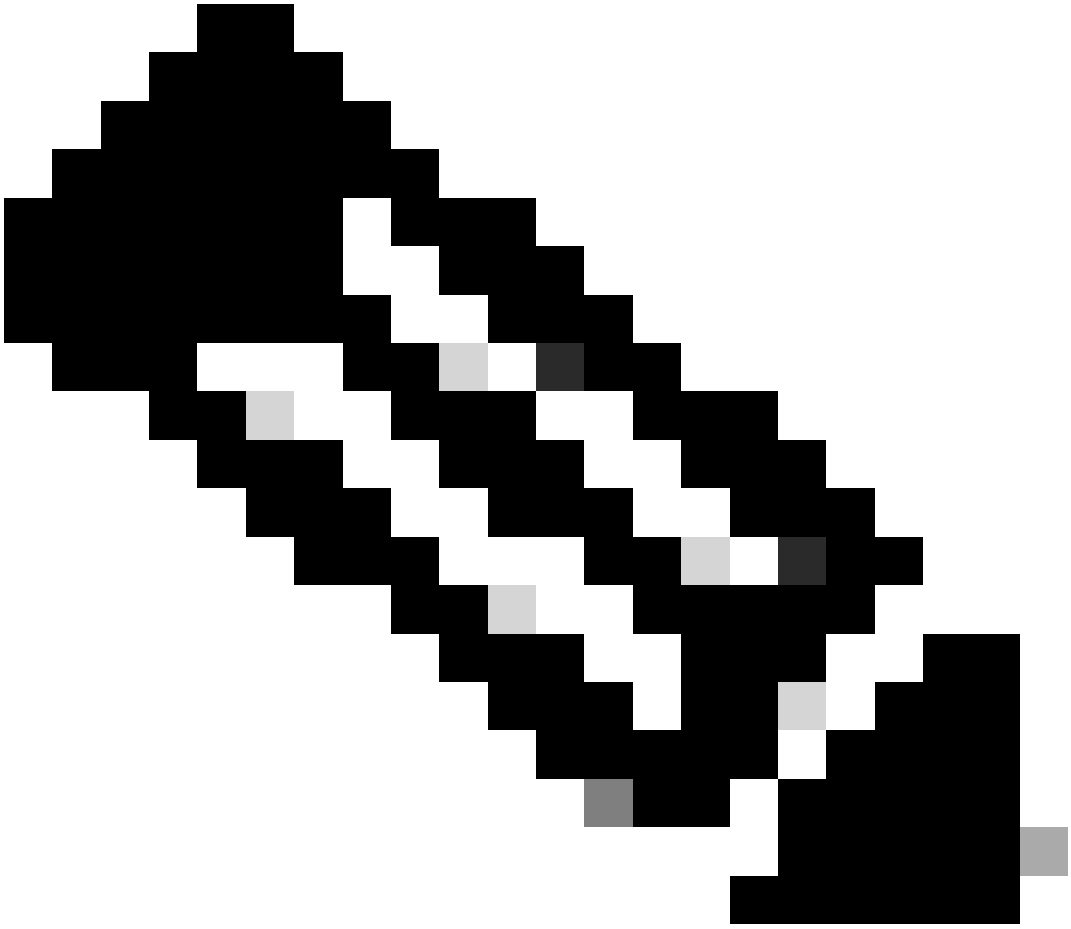


条件の作成

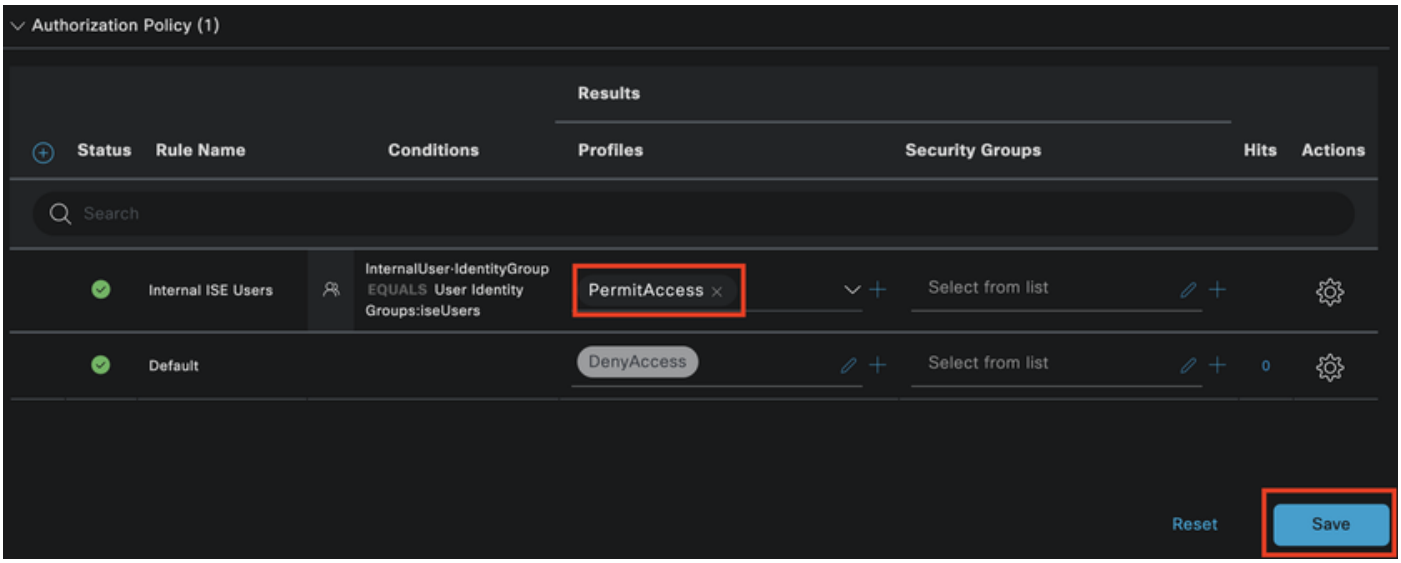
Useをクリックします。

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：ISEに到達する認証が、ユーザIDグループISEUsersに含まれていないこの有線Dot1xポリシーセットにヒットする場合、デフォルトの認可ポリシーにヒットし、結果としてDenyAccessになることに注意してください。



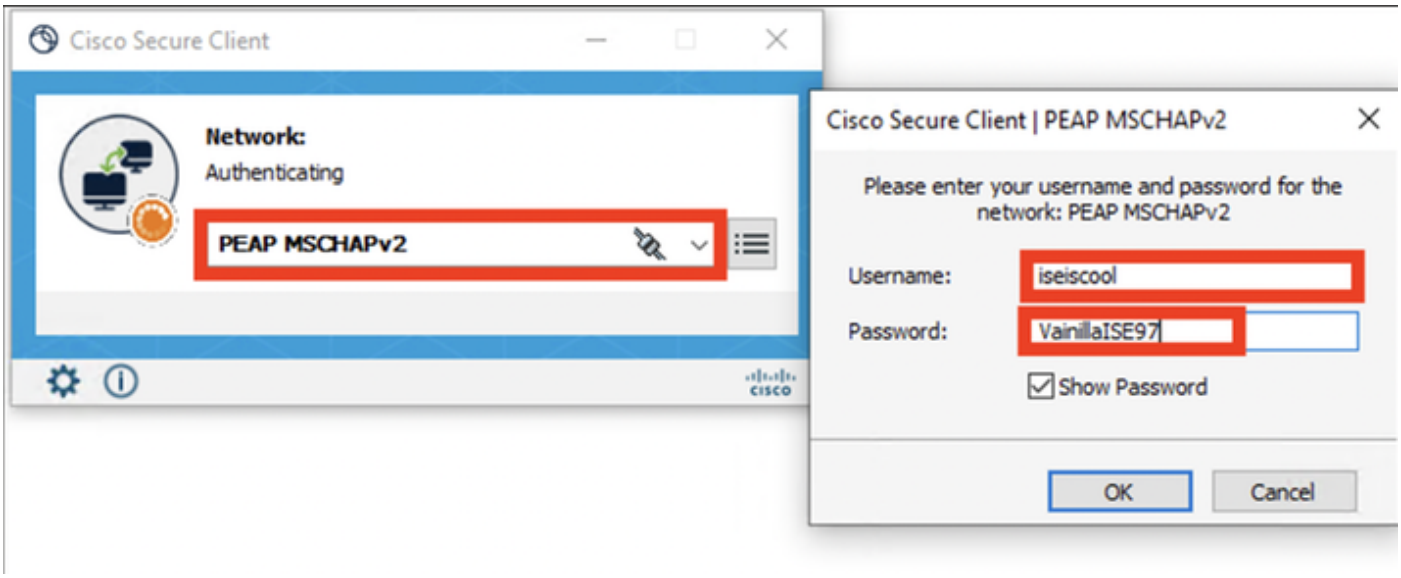
認可ポリシー

[Save] をクリックします。

確認

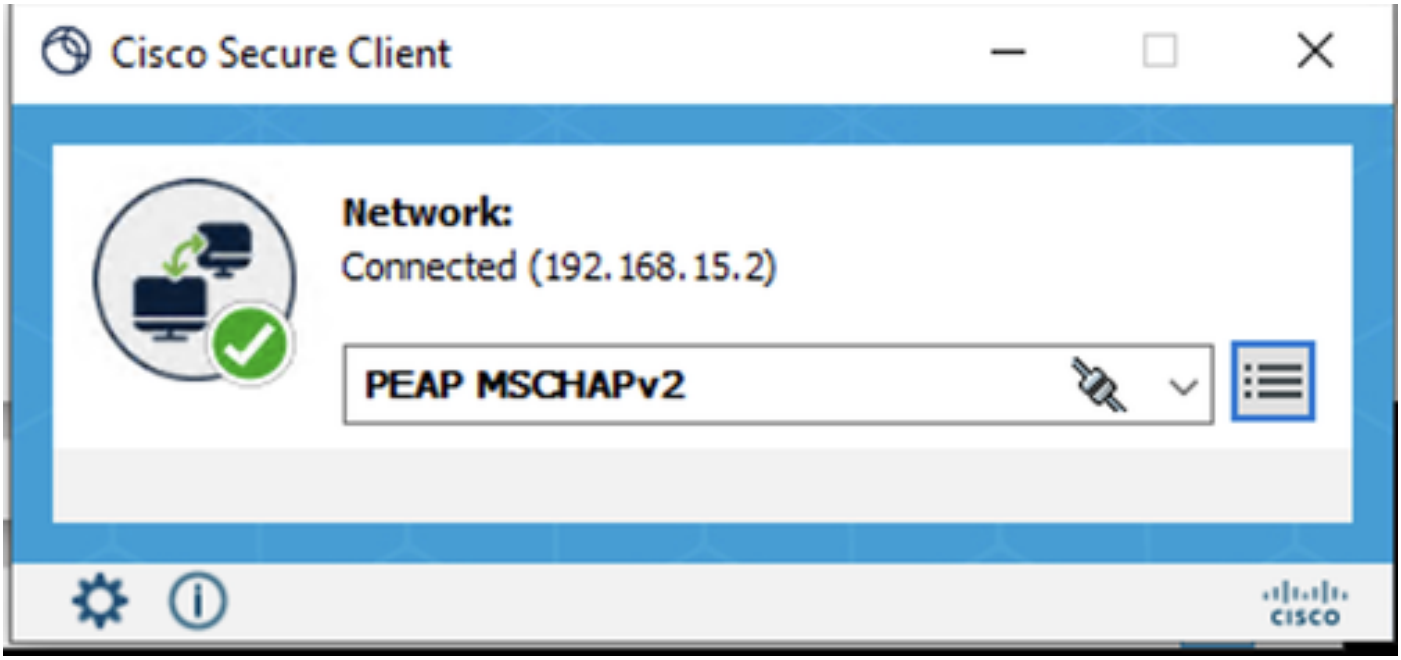
設定が終了すると、セキュアクライアントによってクレデンシャルの入力を求められ、PEAP MSCHAPv2プロファイルの使用が指定されます。

先ほど作成したクレデンシャルが入力されます。



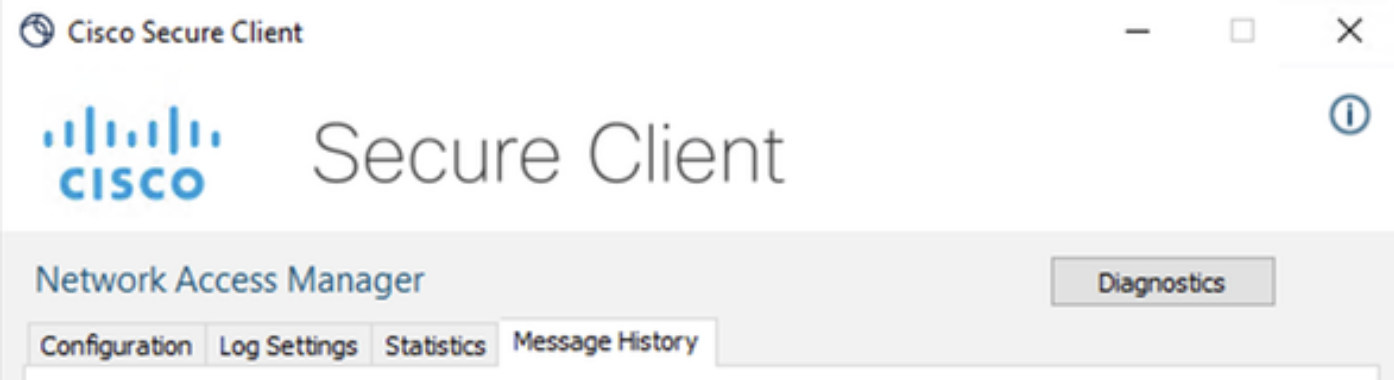
セキュアクライアント*NAM*

エンドポイントが正しく認証された場合、。 NAMは接続されていることを示します。

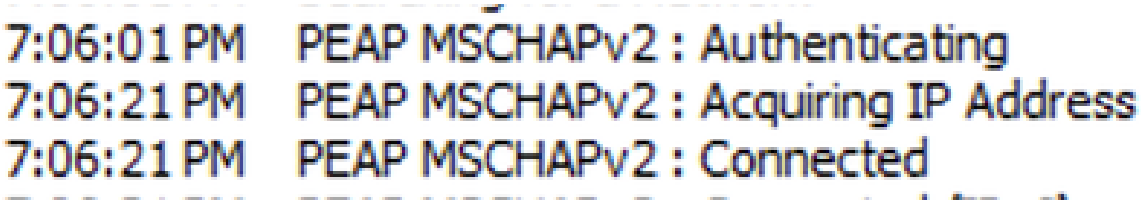


セキュアクライアントNAM

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。



セキュアクライアントメッセージ履歴



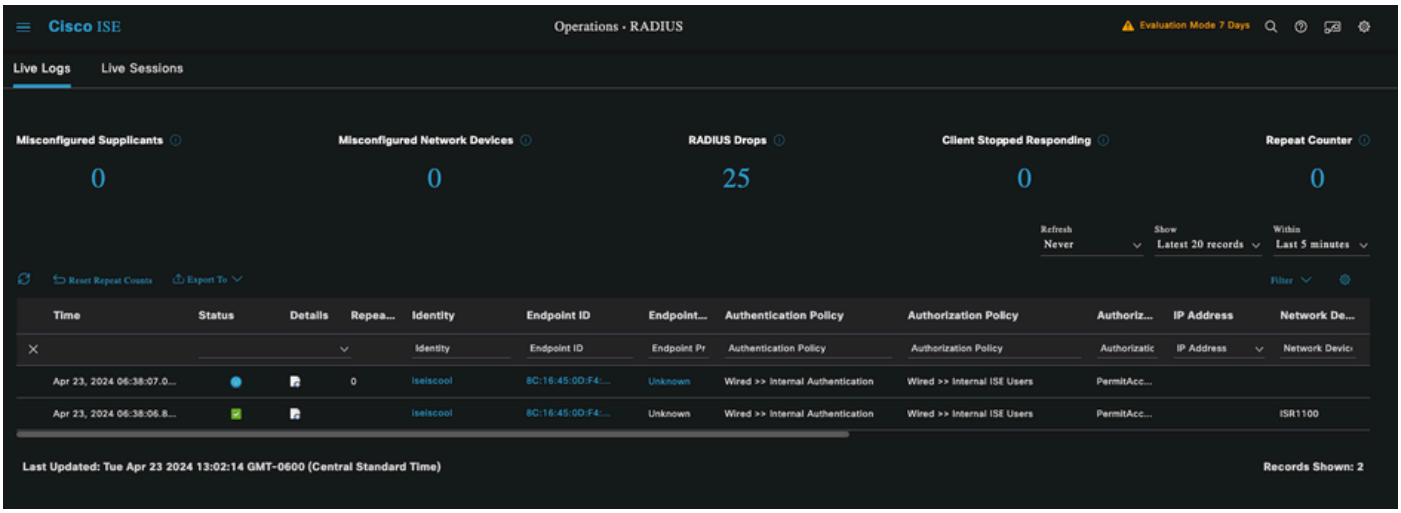
セキュアクライアントメッセージ履歴

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。

その他の詳細は次のとおりです。

- タイムスタンプ.
- MAC アドレス.
- ポリシーセットが使用されています。
- 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

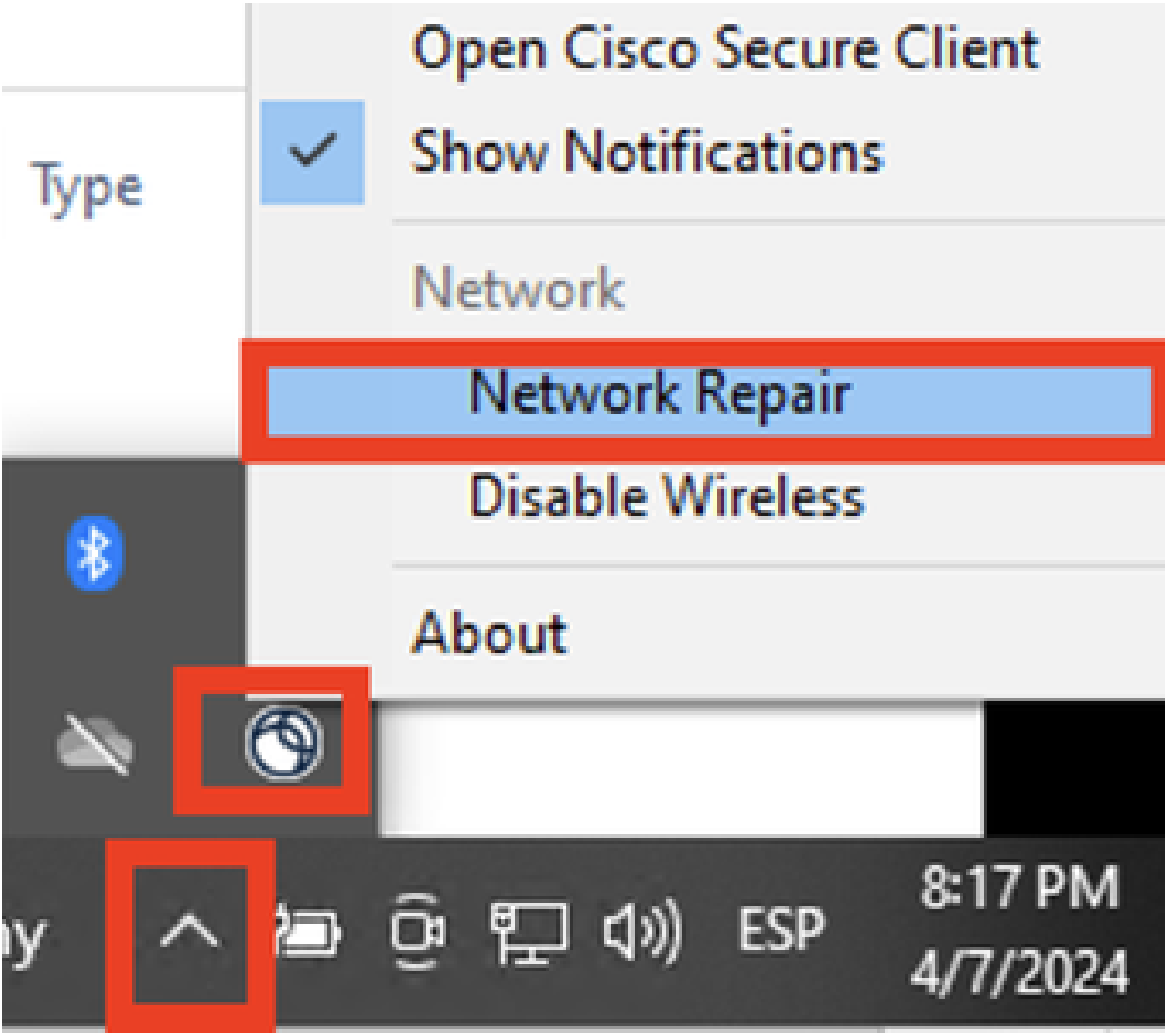
正しいポリシーにヒットすることが確認でき、その結果、認証ステータスが正常であることから、設定は正しいと結論付けられます。

トラブルシュート

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> Circumstrativeアイコンのクリック> Secure Clientアイコンの右クリック> Network Repairの順にクリック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る。

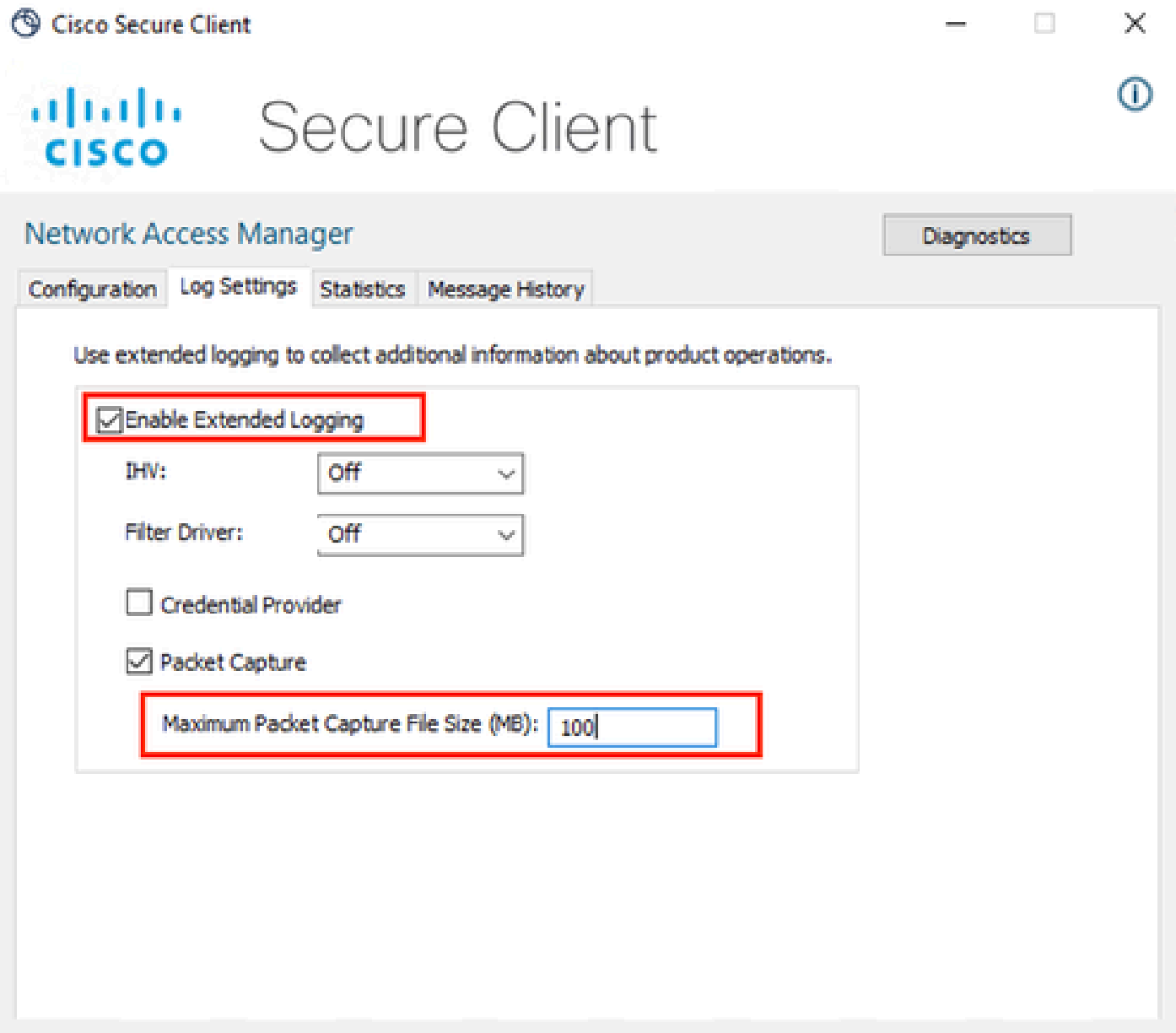
1. NAM拡張ロギングの有効化

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入れます。

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。



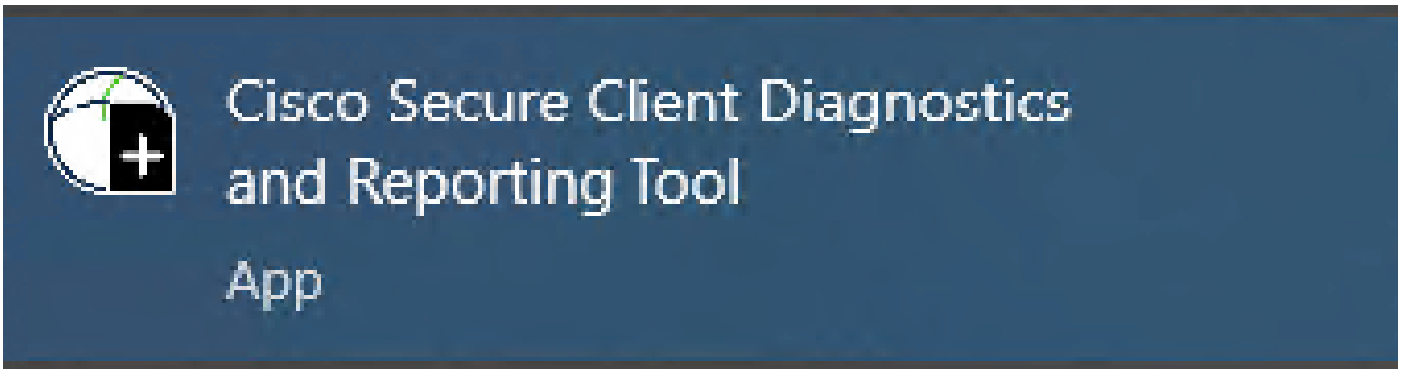
クライアントNAMログのセキュリティ設定

2. 問題を再現します。

拡張ロギングを有効にすると問題が何度も再現され、ログが生成されてトラフィックがキャプチャされていることが確認されます。

3. セキュアクライアントDARTバンドルを収集します。

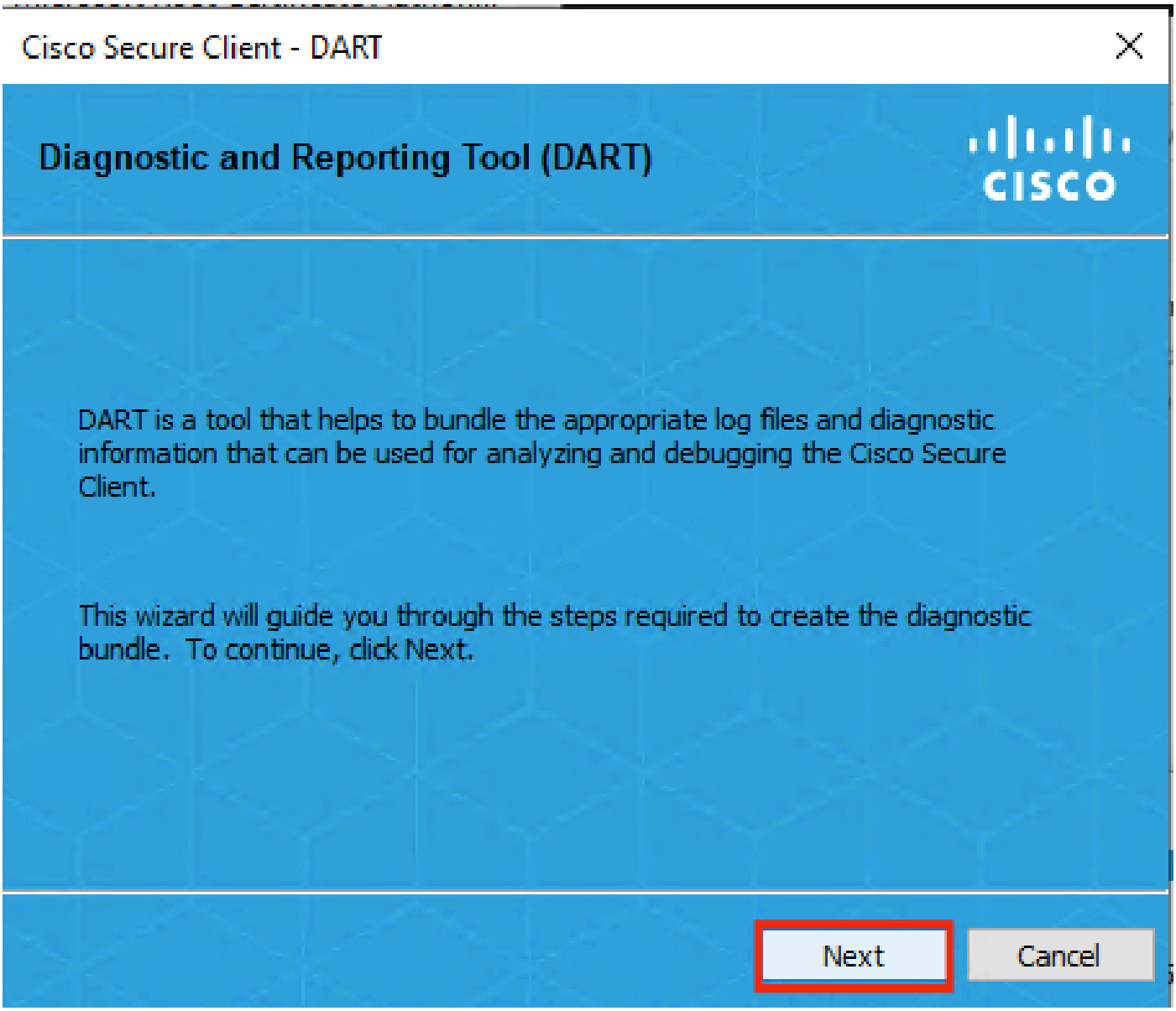
Windowsで検索バーに移動し、「Cisco Secure Client Diagnostics and Reporting Tool」と入力します。



DARTモジュール

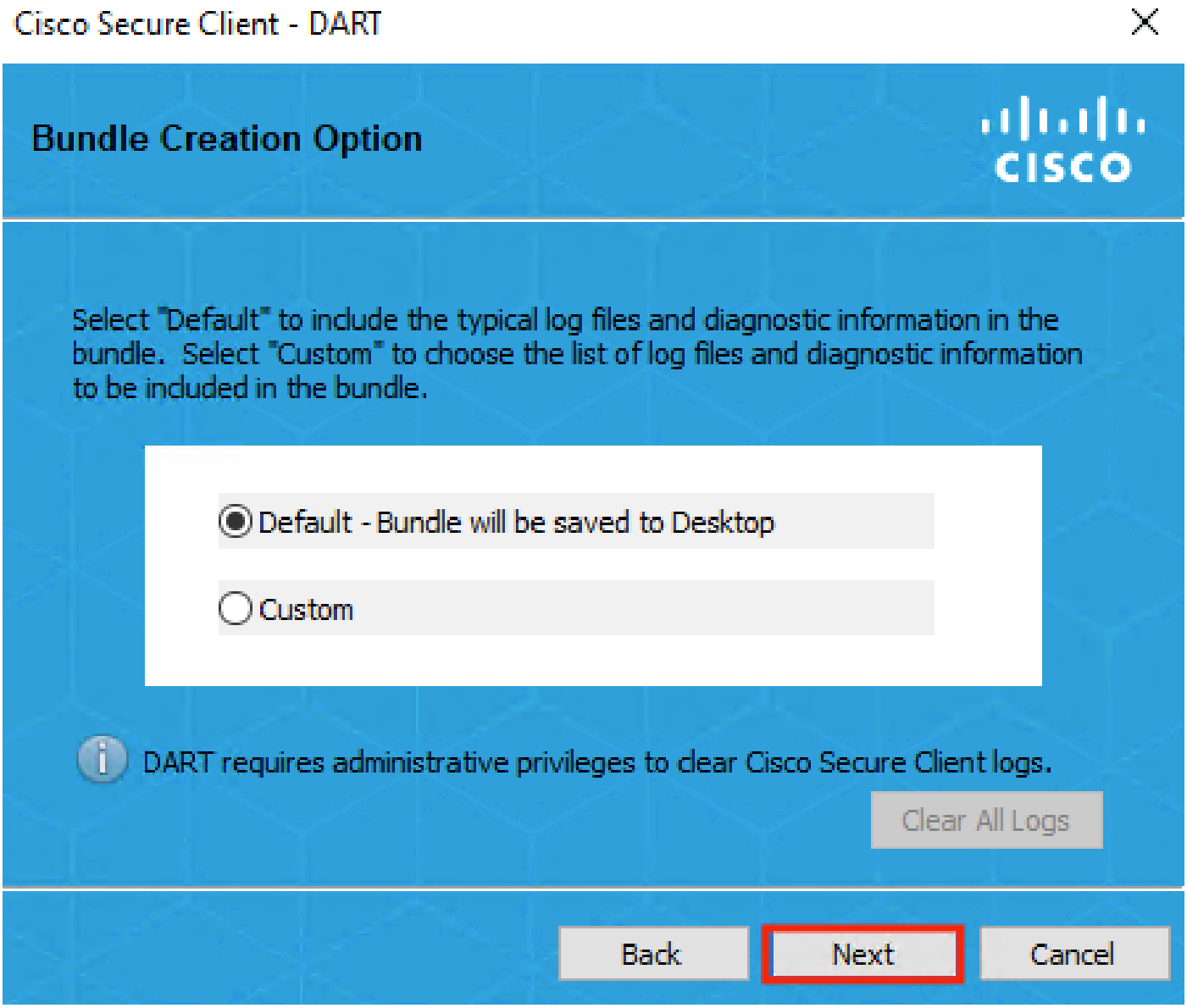
インストールプロセス中に、このモジュールもインストールしました。これは、ログと関連するdot1xセッション情報を収集することで、トラブルシューティングプロセスを支援するツールです。

最初のウィンドウでNextをクリックします。



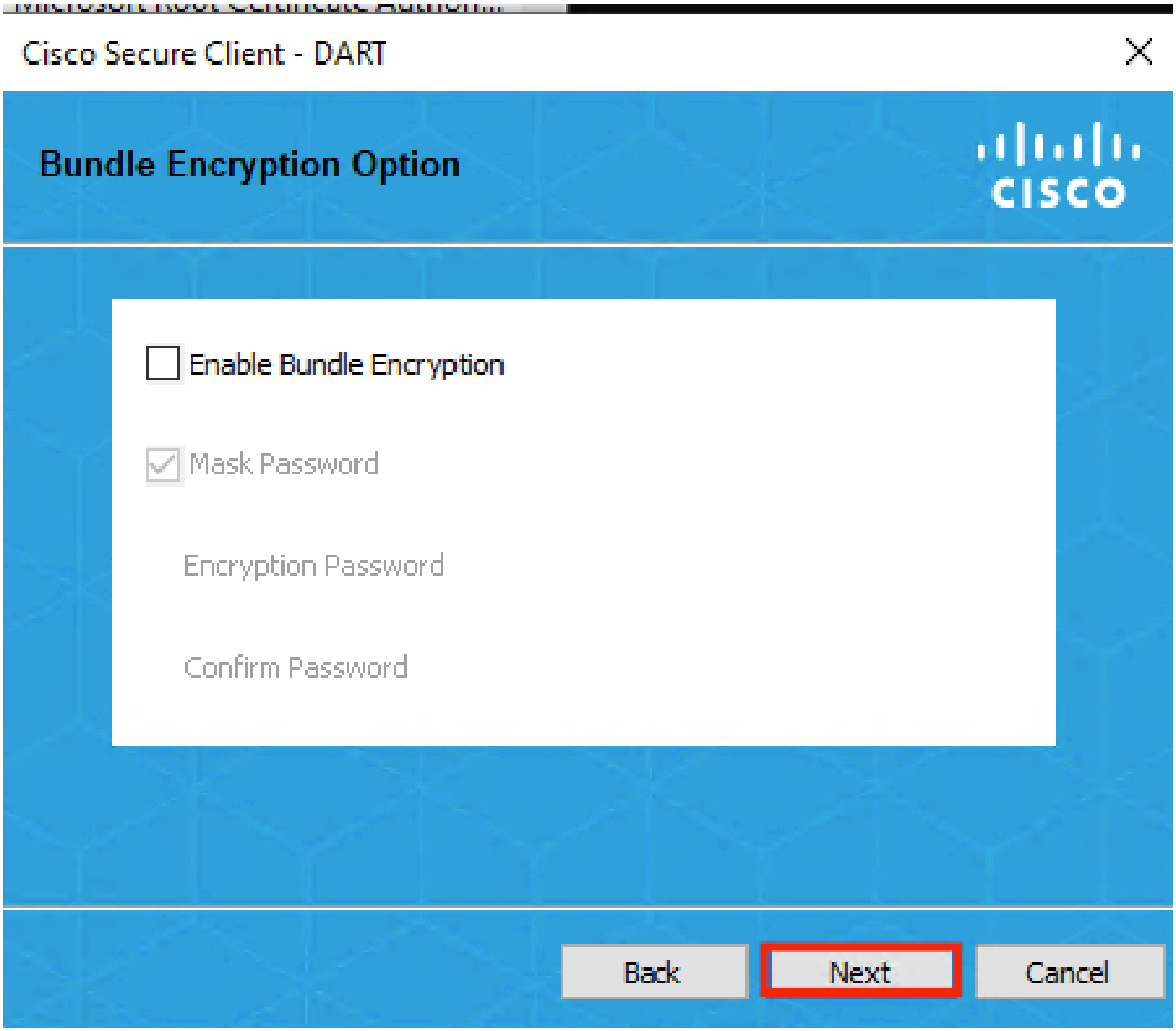
DARTモジュール

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。



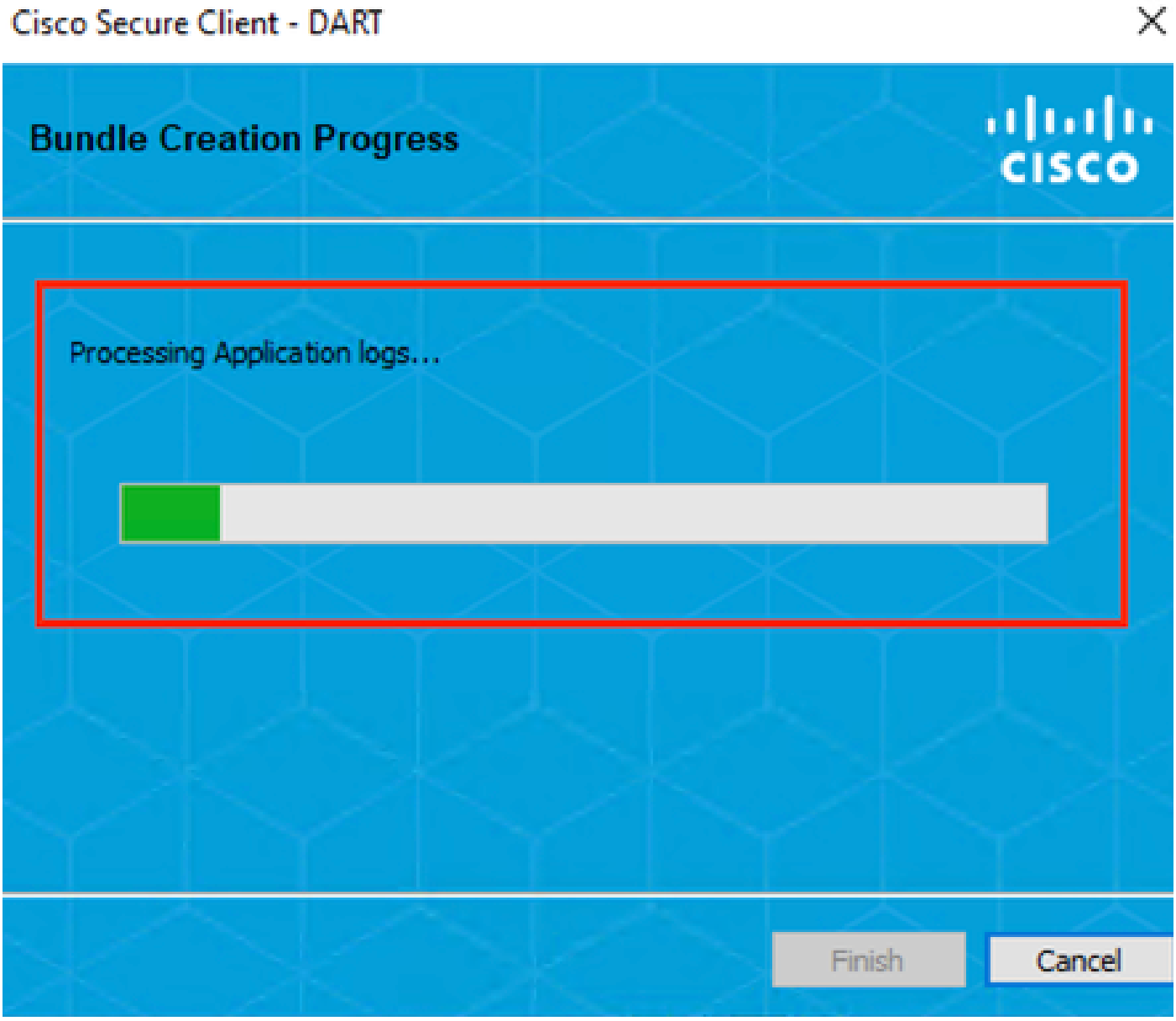
DARTモジュール

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。



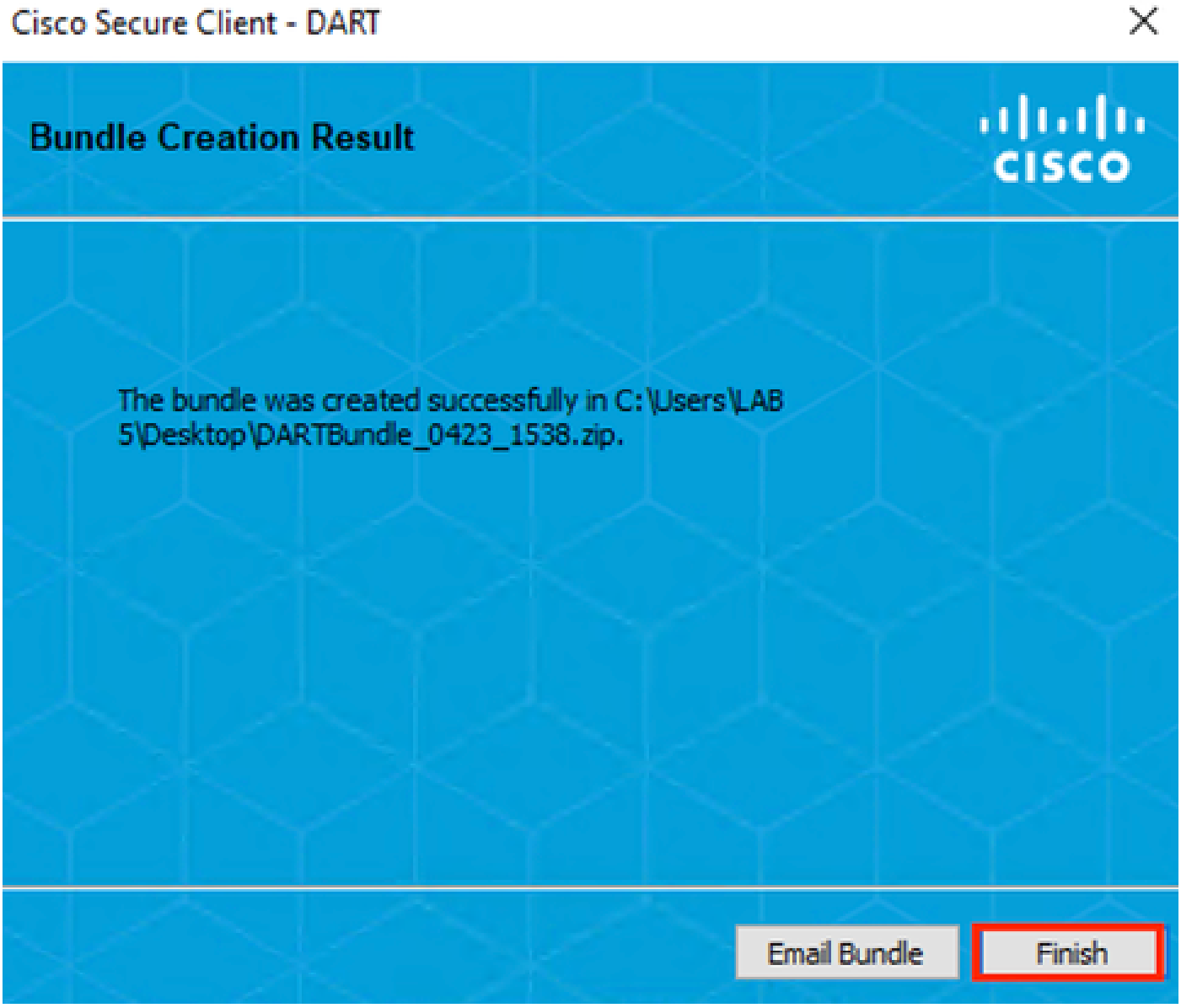
DARTモジュール

DARTログ収集が開始されます。



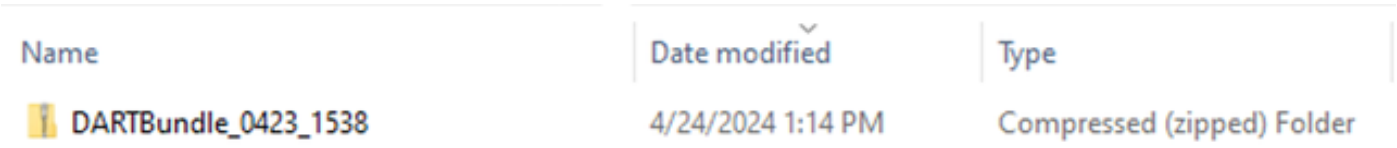
DARTログの収集

プロセスが完了するまで10分以上かかることがあります。



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。