EAP-TTLSによるマシン認証とユーザ認証の設定

内容

はじめに

このドキュメントでは、セキュアクライアントNAMおよびCisco ISE上でEAP-TTLS(EAP-MSCHAPv2)を使用してマシン認証とユーザ認証を設定する方法について説明します。

前提条件

要件

この導入を進める前に、次の項目に関する知識があることが推奨されます。

- Cisco Identity Services Engine（ISE）
- セキュアクライアントネットワーク解析モジュール(NAM)
- EAPプロトコル

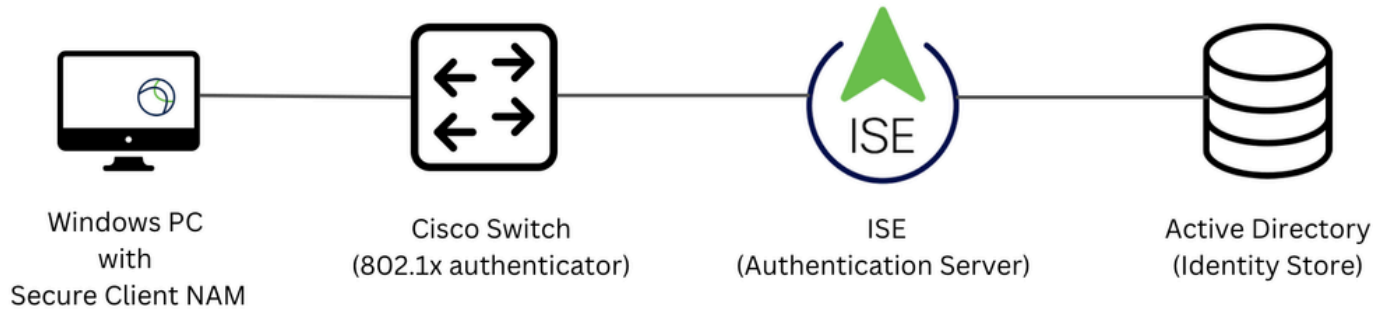
使用するコンポーネント

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。

- Identity Services Engine（ISE）バージョン 3.4
- Cisco IOS® XEソフトウェアバージョン16.12.01が稼働するC9300スイッチ
- Windows 10 Proバージョン22H2ビルド19045.3930

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。

Network Topology



Network Topology

設定

コンフィギュレーション

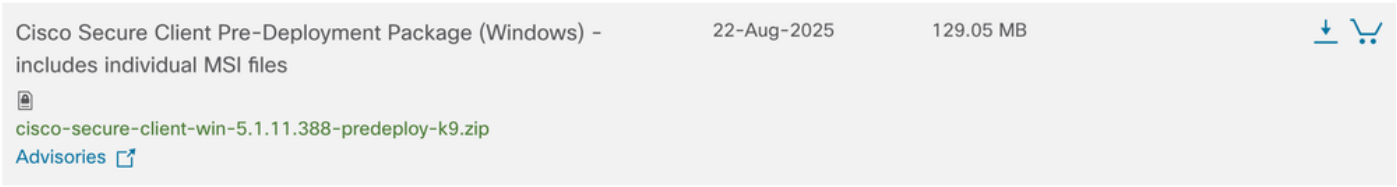
パート1:セキュアクライアントNAM(Network Access Manager)のダウンロードとインストール

ステップ 1：シスコソフトウェアダウンロードに移動します。製品検索バーに、Secure Client 5と入力します。

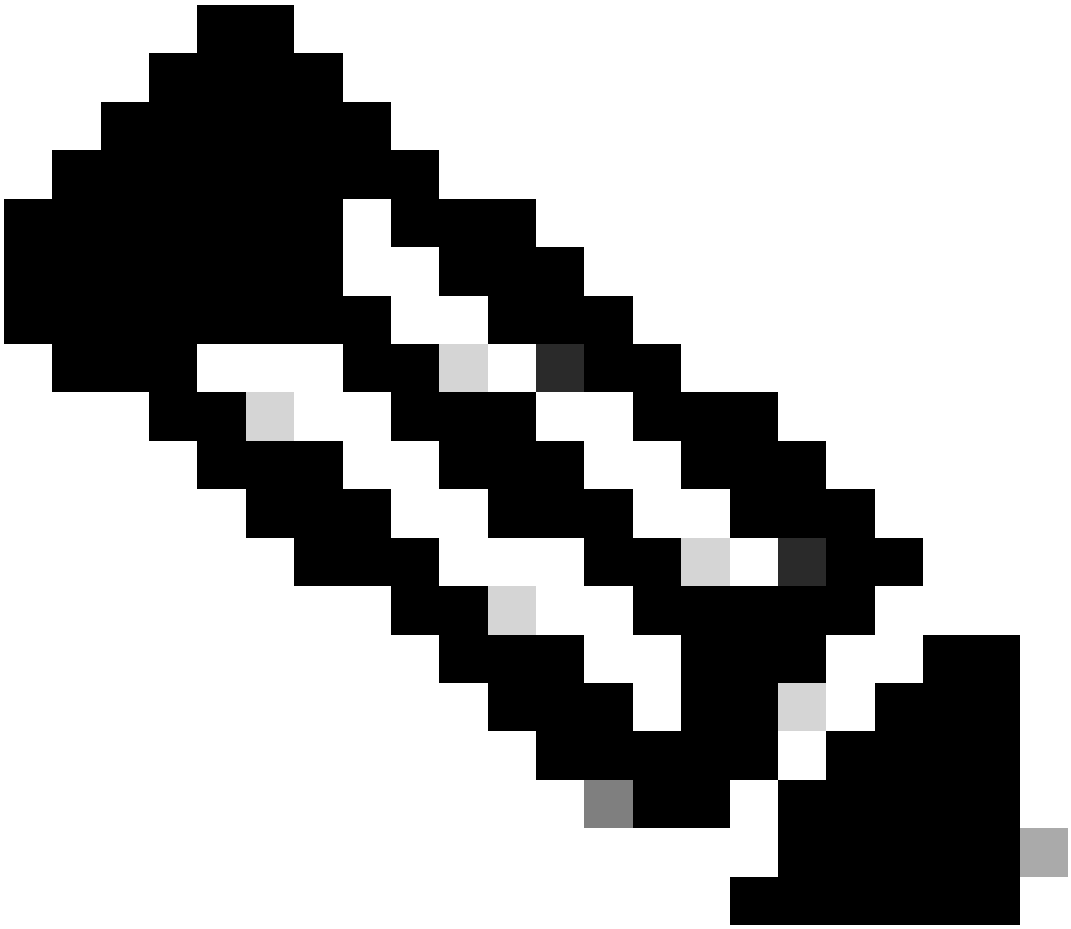
この設定例では、バージョン5.1.11.388を使用しています。インストールは、事前展開方式を使用して実行されます。

ダウンロードページで、Cisco Secure Client Pre-Deployment Package(Windows)を探してダウン

ロードします。

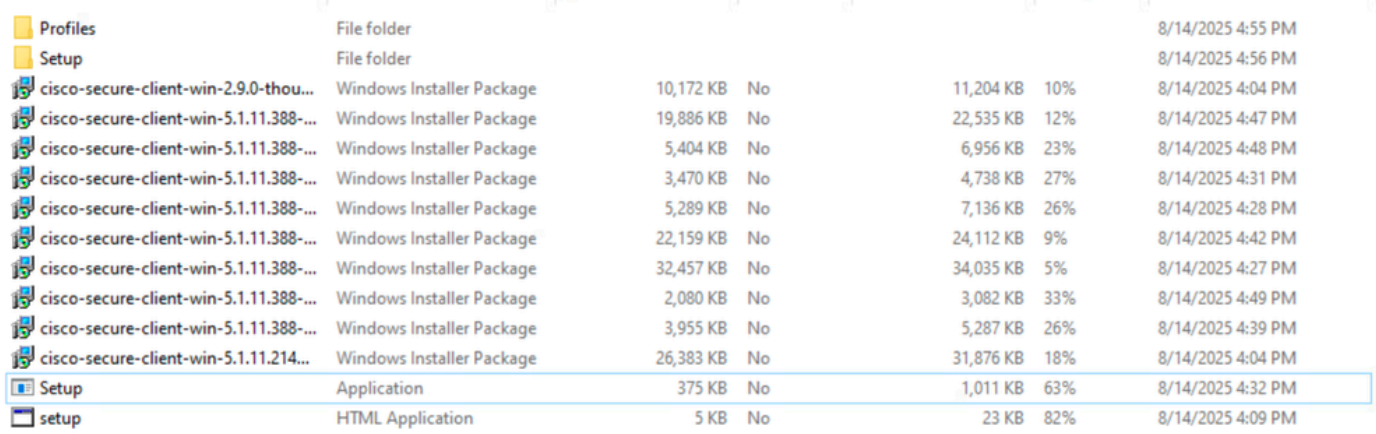


展開前のzipファイル



注:Cisco AnyConnectは廃止されたため、シスコソフトウェアダウンロードサイトでは入手できなくなりました。

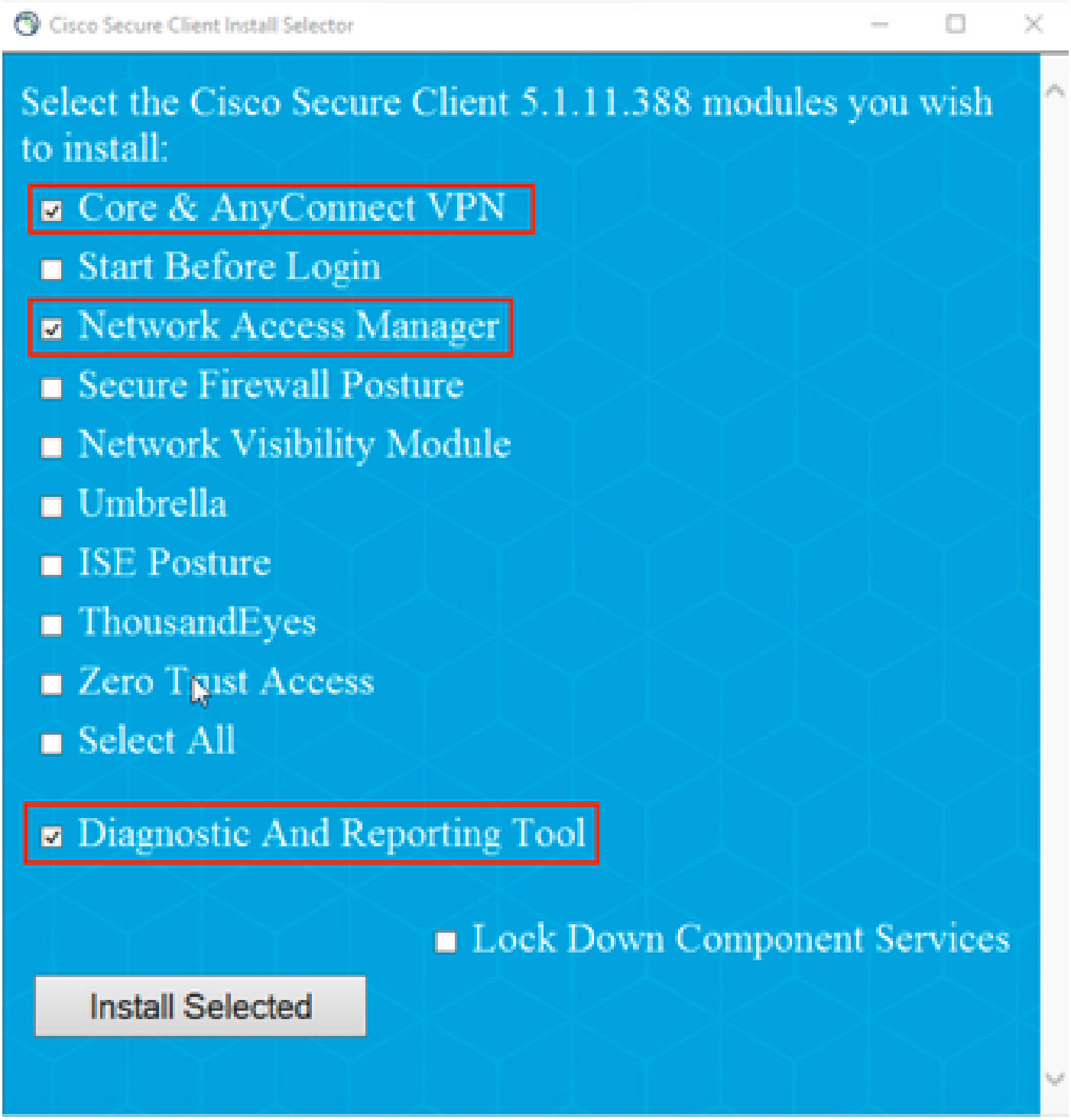
ステップ 2：ダウンロードして解凍したら、Setupをクリックします。



Profiles	File folder					8/14/2025 4:55 PM
Setup	File folder					8/14/2025 4:56 PM
cisco-secure-client-win-2.9.0-thou...	Windows Installer Package	10,172 KB	No	11,204 KB	10%	8/14/2025 4:04 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	19,886 KB	No	22,535 KB	12%	8/14/2025 4:47 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	5,404 KB	No	6,956 KB	23%	8/14/2025 4:48 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	3,470 KB	No	4,738 KB	27%	8/14/2025 4:31 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	5,289 KB	No	7,136 KB	26%	8/14/2025 4:28 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	22,159 KB	No	24,112 KB	9%	8/14/2025 4:42 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	32,457 KB	No	34,035 KB	5%	8/14/2025 4:27 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	2,080 KB	No	3,082 KB	33%	8/14/2025 4:49 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	3,955 KB	No	5,287 KB	26%	8/14/2025 4:39 PM
cisco-secure-client-win-5.1.11.214...	Windows Installer Package	26,383 KB	No	31,876 KB	18%	8/14/2025 4:04 PM
Setup	Application	375 KB	No	1,011 KB	63%	8/14/2025 4:32 PM
setup	HTML Application	5 KB	No	23 KB	82%	8/14/2025 4:09 PM

展開前のZipファイル

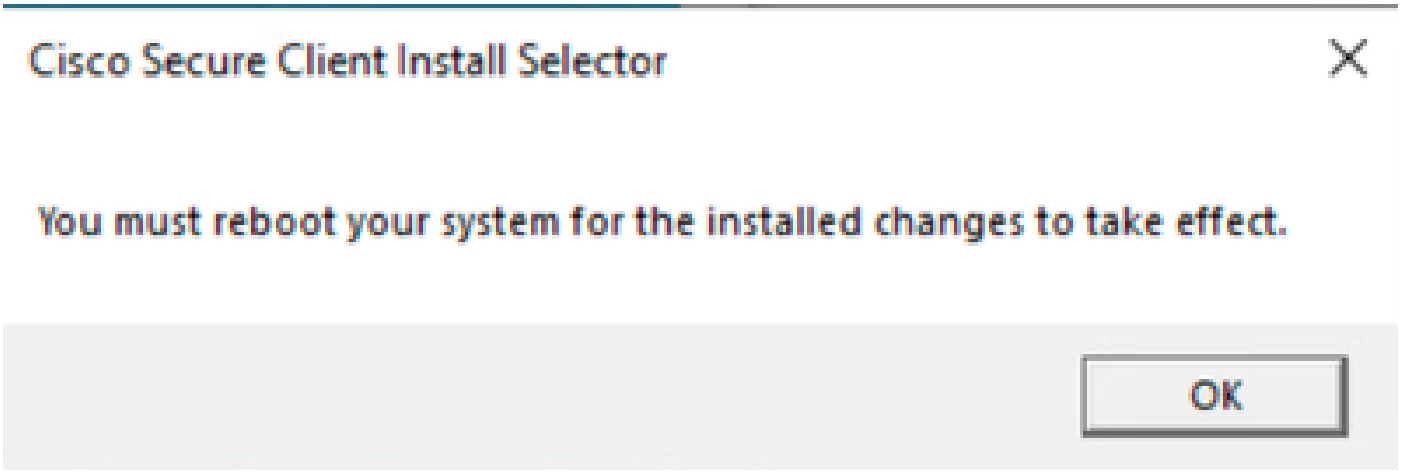
ステップ 3：Core & AnyConnect VPN、Network Access Manager、Diagnostics and Reporting ツールモジュールをインストールします。



Secure Clientインストーラ

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

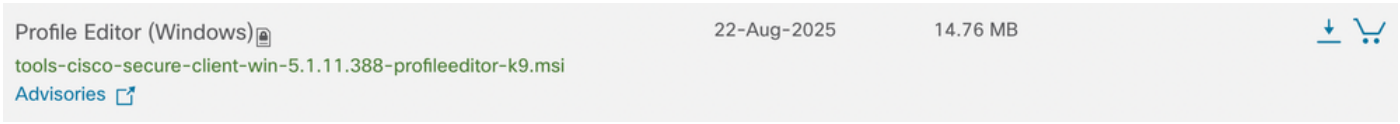
ステップ 4：インストール後に再起動が必要です。OKをクリックして、デバイスを再起動します。



再起動が必要なポップアップ

パート2：セキュアクライアントNAMプロファイルエディタのダウンロードとインストール

ステップ 1：プロファイルエディタは、セキュアクライアントと同じダウンロードページにあります。 この設定例では、バージョン5.1.11.388を使用しています。



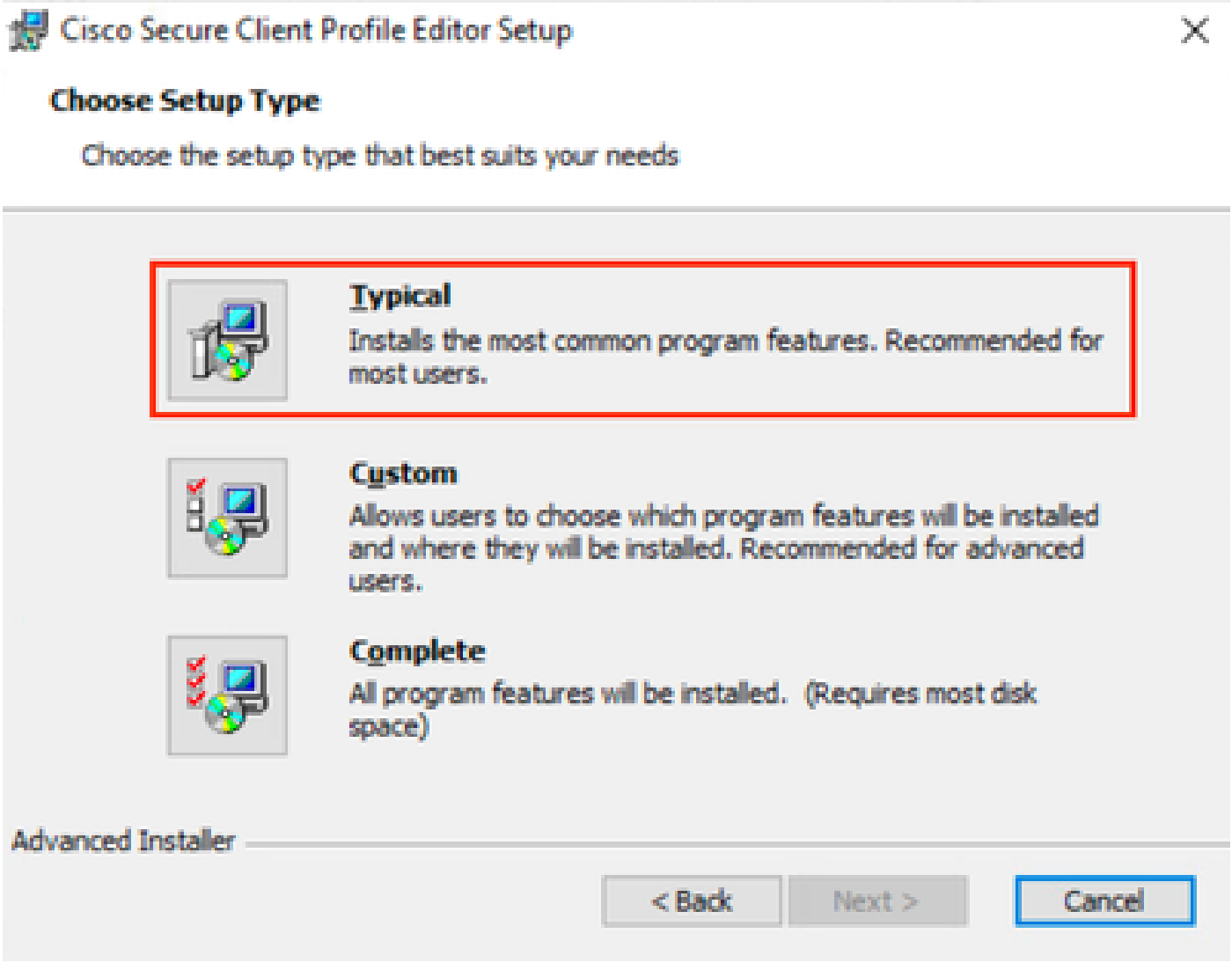
プロファイルエディタ

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。

ステップ 2：MSIファイルを実行します。

プロファイルエディタのセットアップの開始

ステップ 3：Typicalセットアップオプションを使用して、NAM Profile Editorをインストールします。

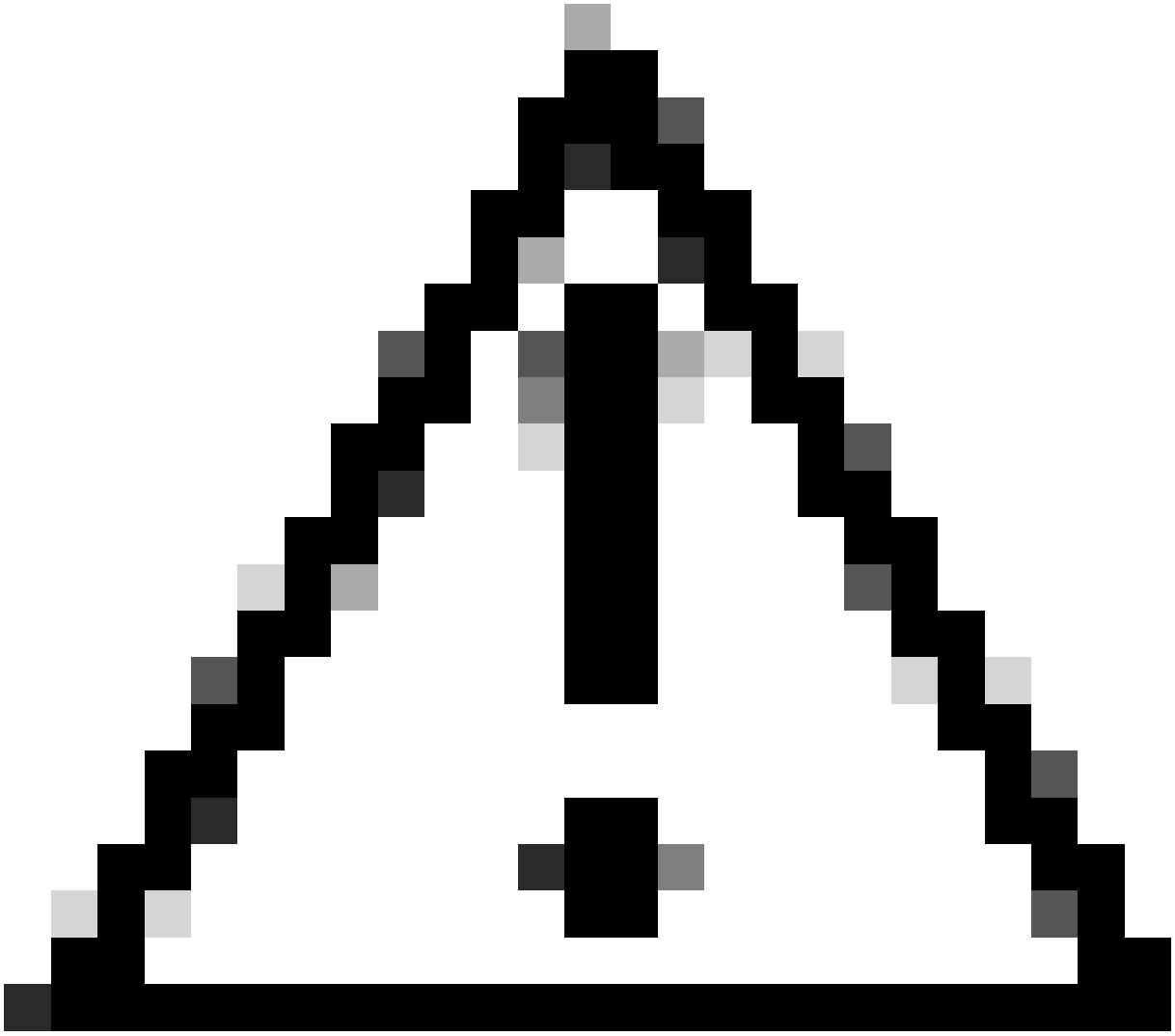


プロファイルエディタの設定

パート3:NAMによるWindowsキャッシュ資格情報へのアクセスの許可

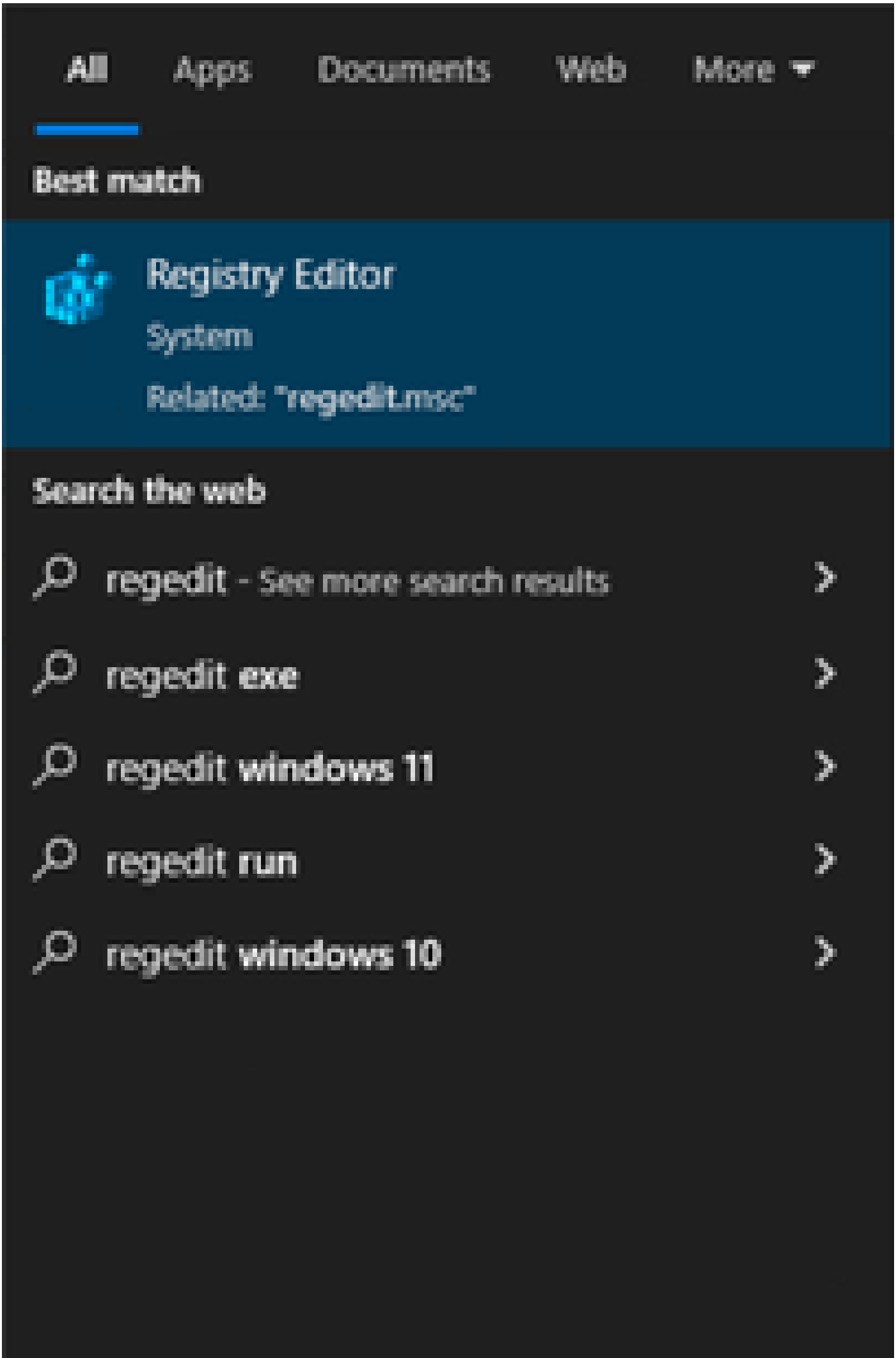
デフォルトでは、Windows 10、Windows 11、およびWindows Server 2012では、オペレーティングシステムにより、Network Access Manager(NAM)がマシン認証に必要なマシンパスワードを取得できません。その結果、レジストリ修正が適用されない限り、マシンパスワードを使用したマシン認証は機能しません。

NAMがマシンのクレデンシャルにアクセスできるようにするには、クライアントデスクトップで[Microsoft KB 2743127](#)の修正プログラムを適用します。



注意: Windowsレジストリを誤って編集すると、重大な問題が発生する可能性があります。変更を行う前に、必ずレジストリをバックアップしてください。

ステップ 1：Windowsの検索バーにregeditと入力し、Registry Editorをクリックします。

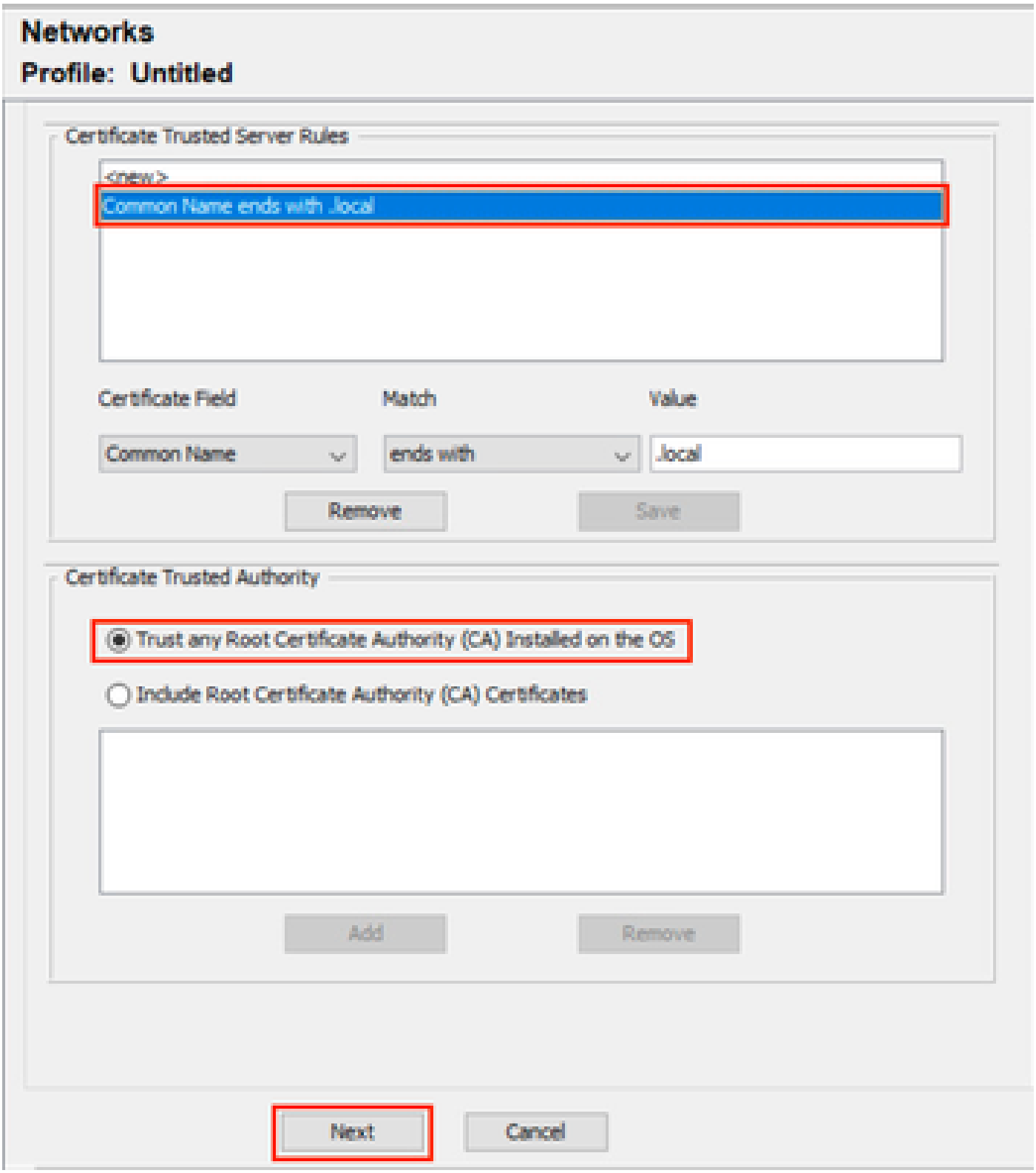

All
Apps
Documents
Web
More
Best match
Registry Editor
System
Related: "regedit.msc"
Search the web
regedit - See more search results
regedit exe
regedit windows 11
regedit run
regedit windows 10

この例では、PSNノード証明書はvarshah.varshiah.localによって発行されます。したがって、共通名は.localで終わるというルールが使用されます。このルールは、EAP-TTLSフロー中にサーバが提示する証明書を検証します。

ポリシーサービスノード(PSN)EAP認証証明書の共通名を指定することもできます。

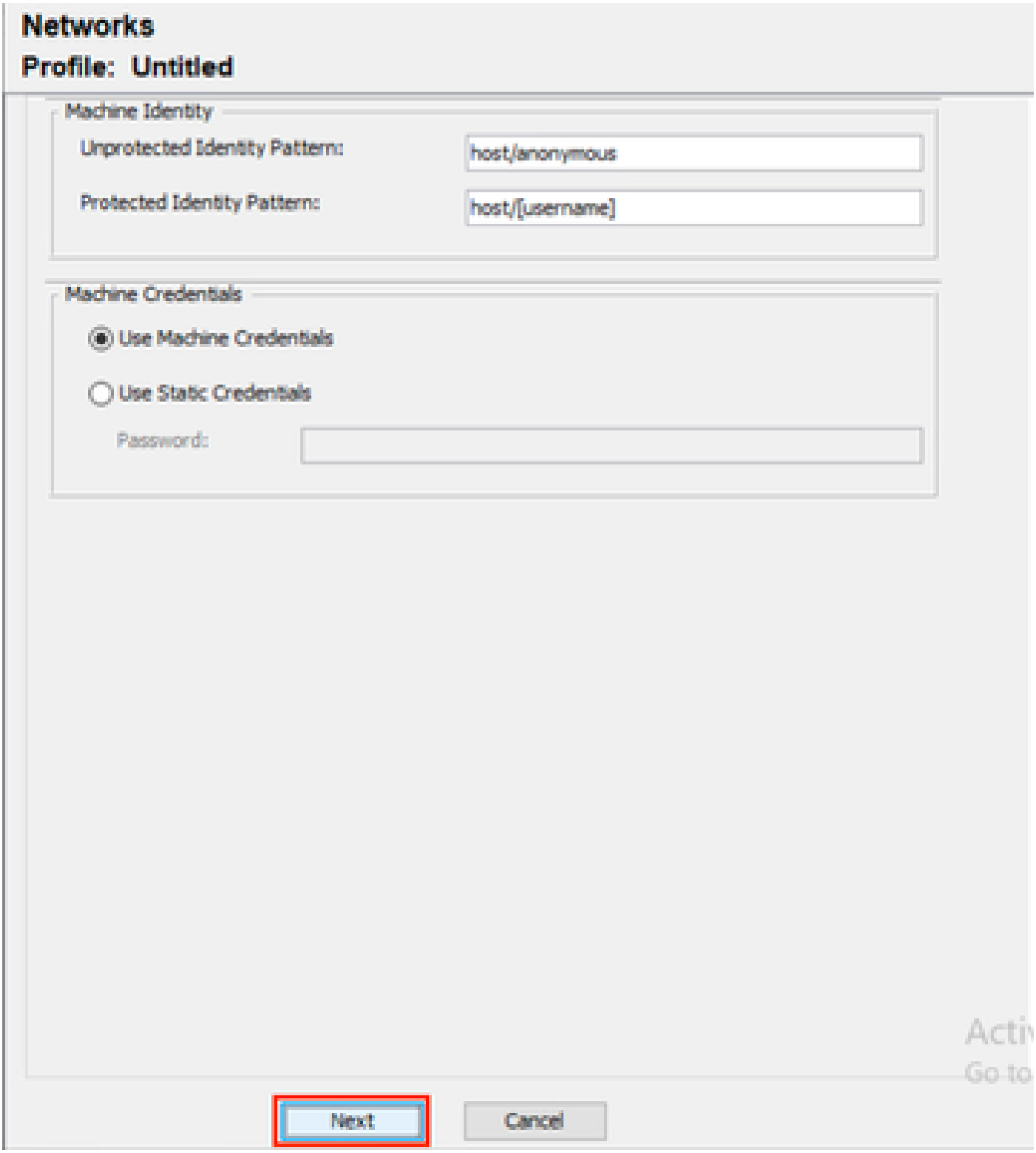
- Certificate Trusted Authorityの下に、2つのオプションがあります。
  このシナリオでは、特定のCA証明書を追加する代わりに、Trust any Root Certificate Authority (CA) installed on the OSオプションを使用します。

  このオプションを使用すると、Windowsデバイスは、（オペレーティングシステムによって管理される）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EAP証明書をすべて信頼します。
- [Next] をクリックして次に進みます。



NAMプロファイルエディタの証明書

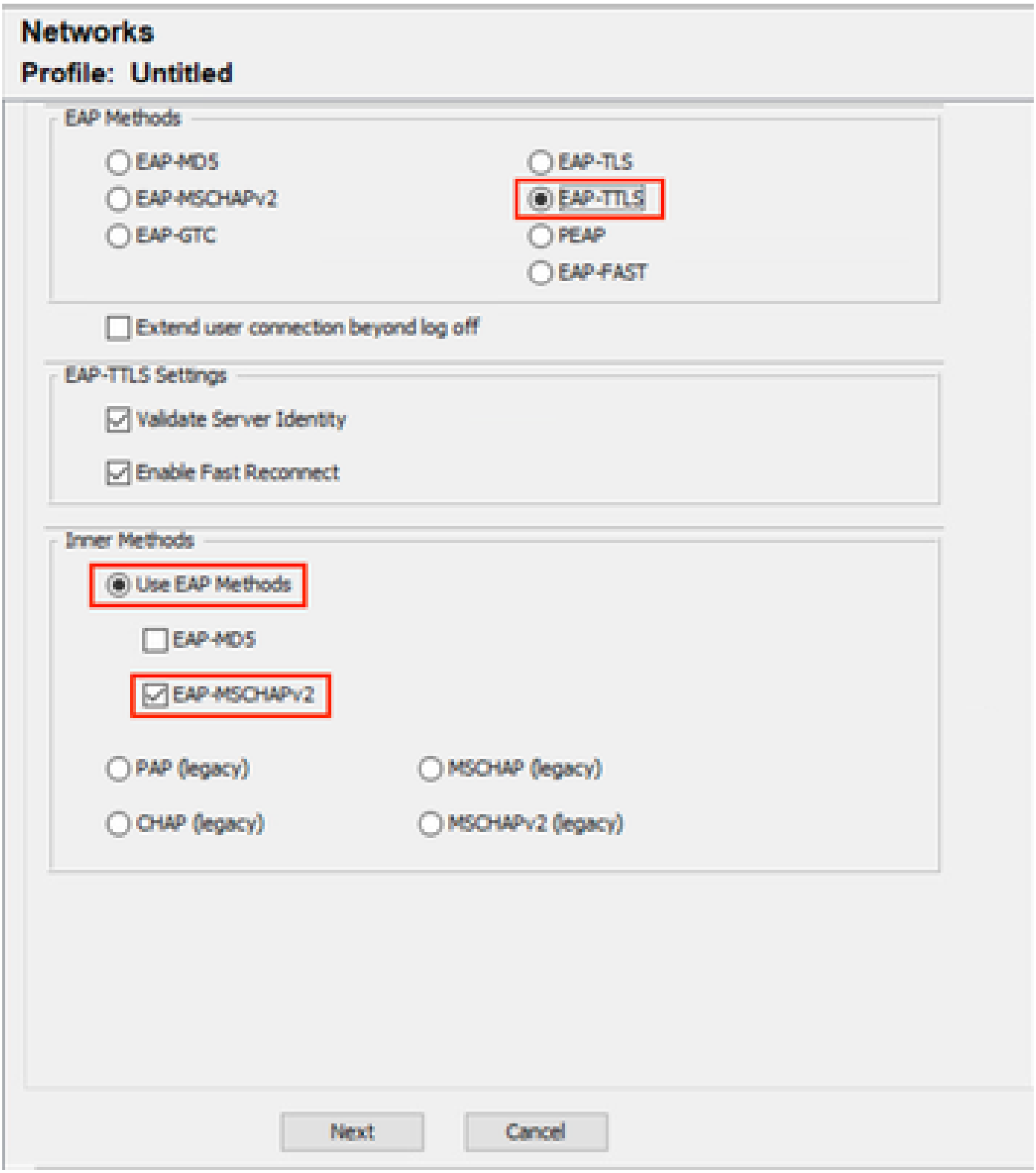
手順 6：Machine Credentialsセクションで、Use Machine Credentialsを選択し、Nextをクリックします。



NAMプロファイルエディタクレデンシャル

手順 7：User Authセクションの設定

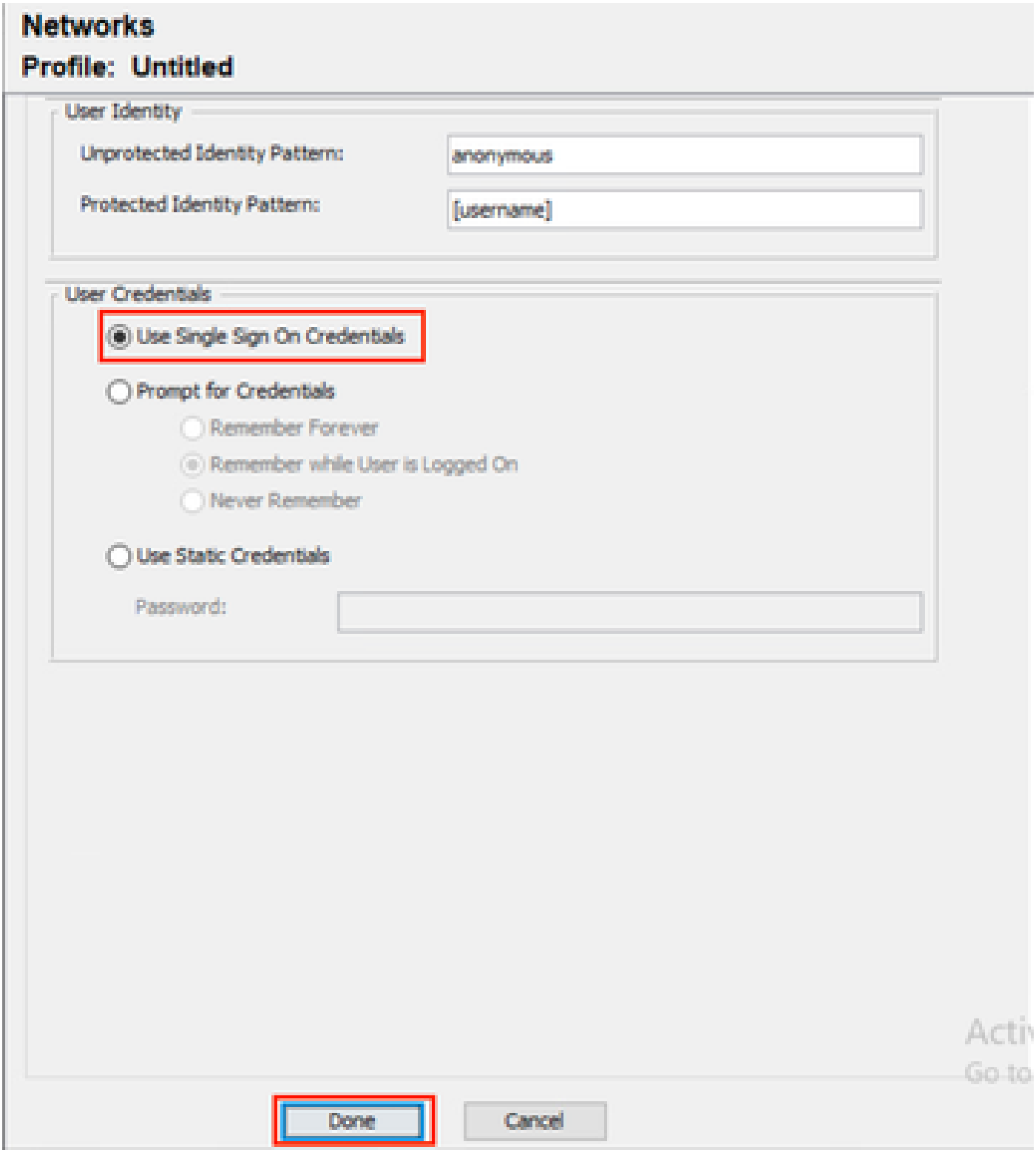
- EAP MethodsでEAP-TTLSを選択します。
- Inner Methodsの下で、Use EAP Methodsを選択し、EAP-MSCHAPv2を選択します。
- [Next] をクリックします。



NAMプロファイルエディタのユーザ認証

ステップ 8：Certificatesで、ステップ5で説明した同じ証明書検証ルールを設定します。

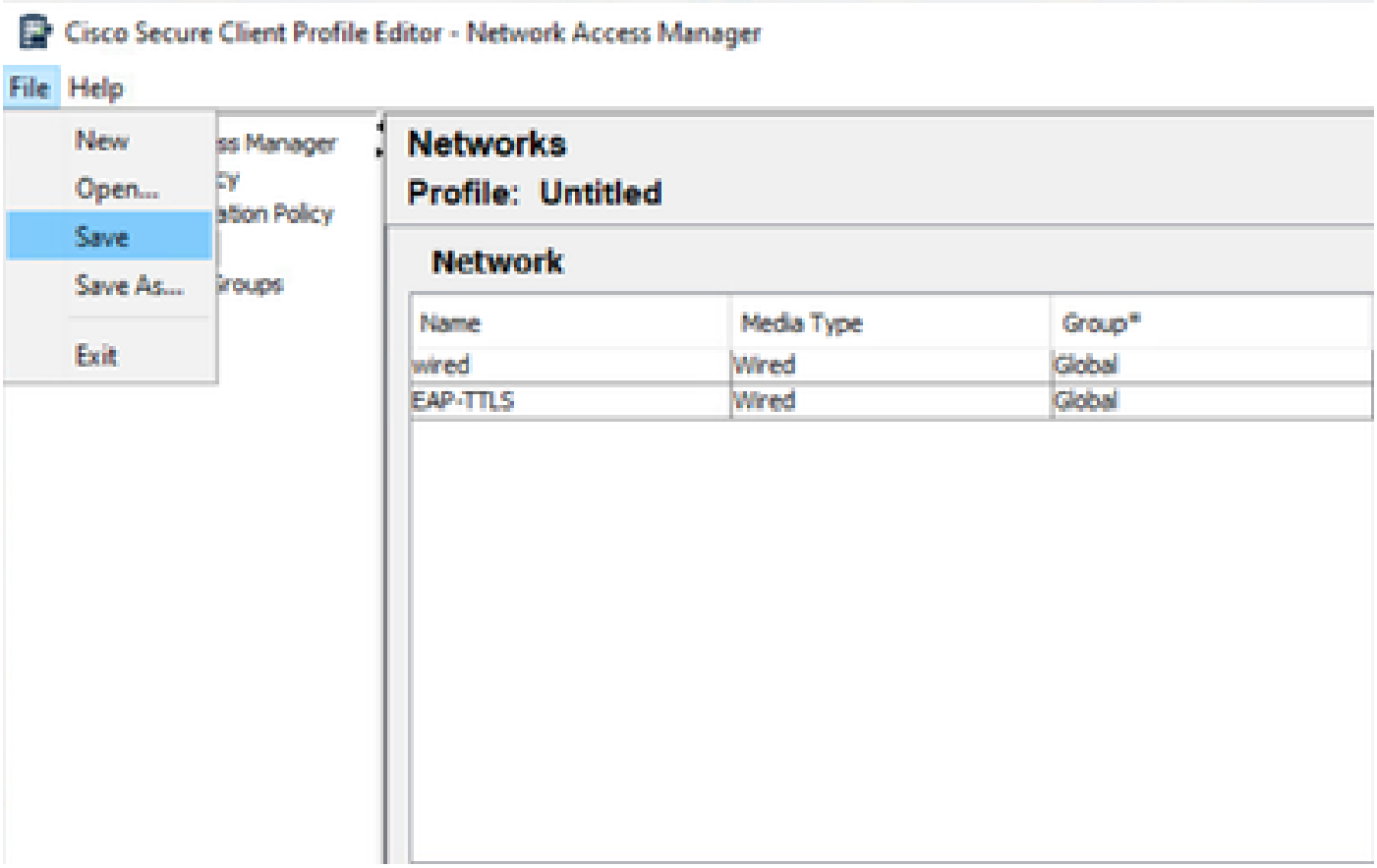
ステップ 9：User Credentialsで、Use Single Sign-On Credentialsを選択し、Doneをクリックします。



NAMプロファイルエディタのユーザクレデンシャル

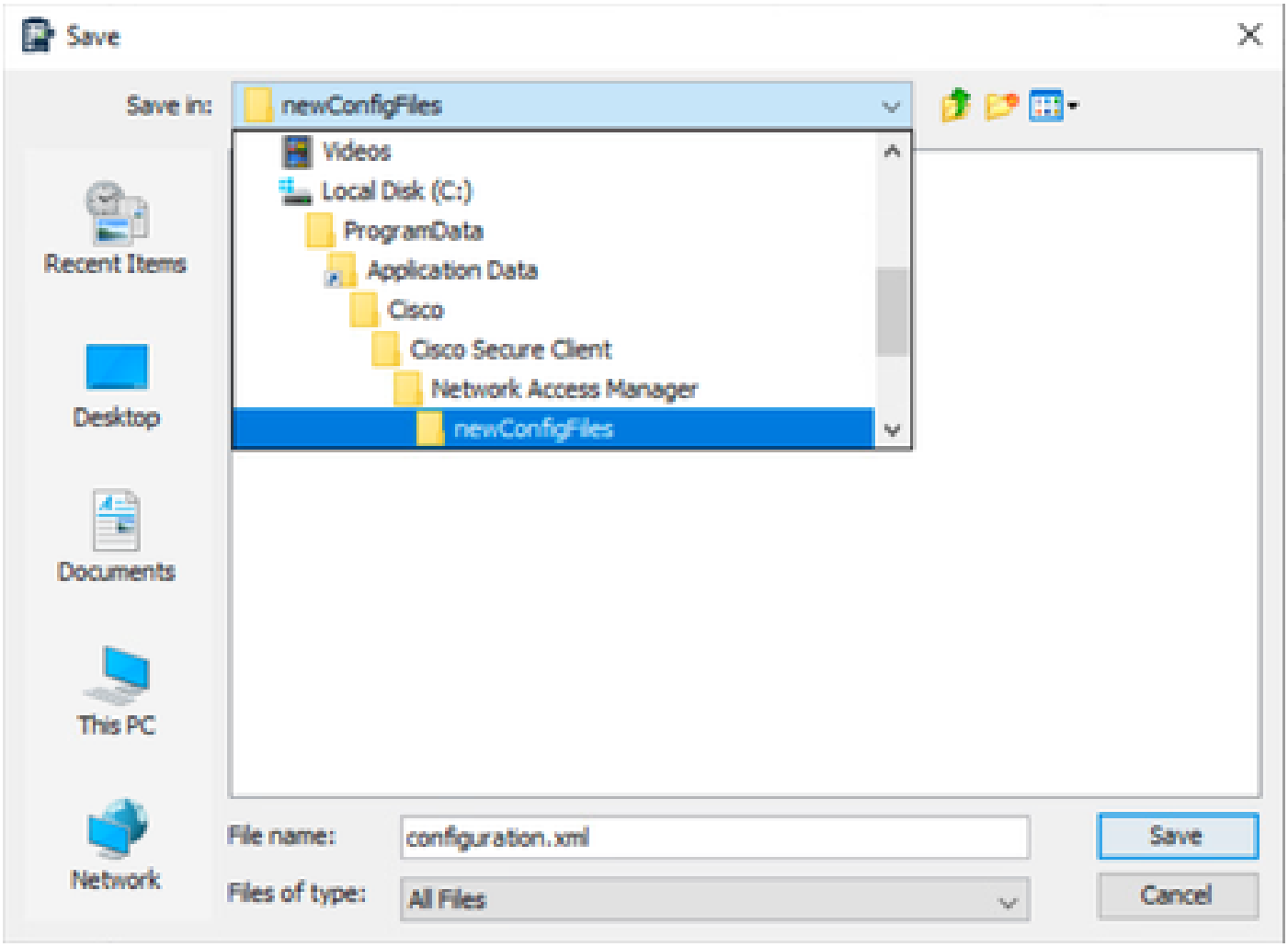
パート6：ネットワークコンフィギュレーションファイルの保存

ステップ 1：File > Saveの順にクリックします。



NAMプロファイルエディタネットワーク設定の保存

ステップ 2：ファイルをconfiguration.xmlとしてnewConfigFilesフォルダに保存します。

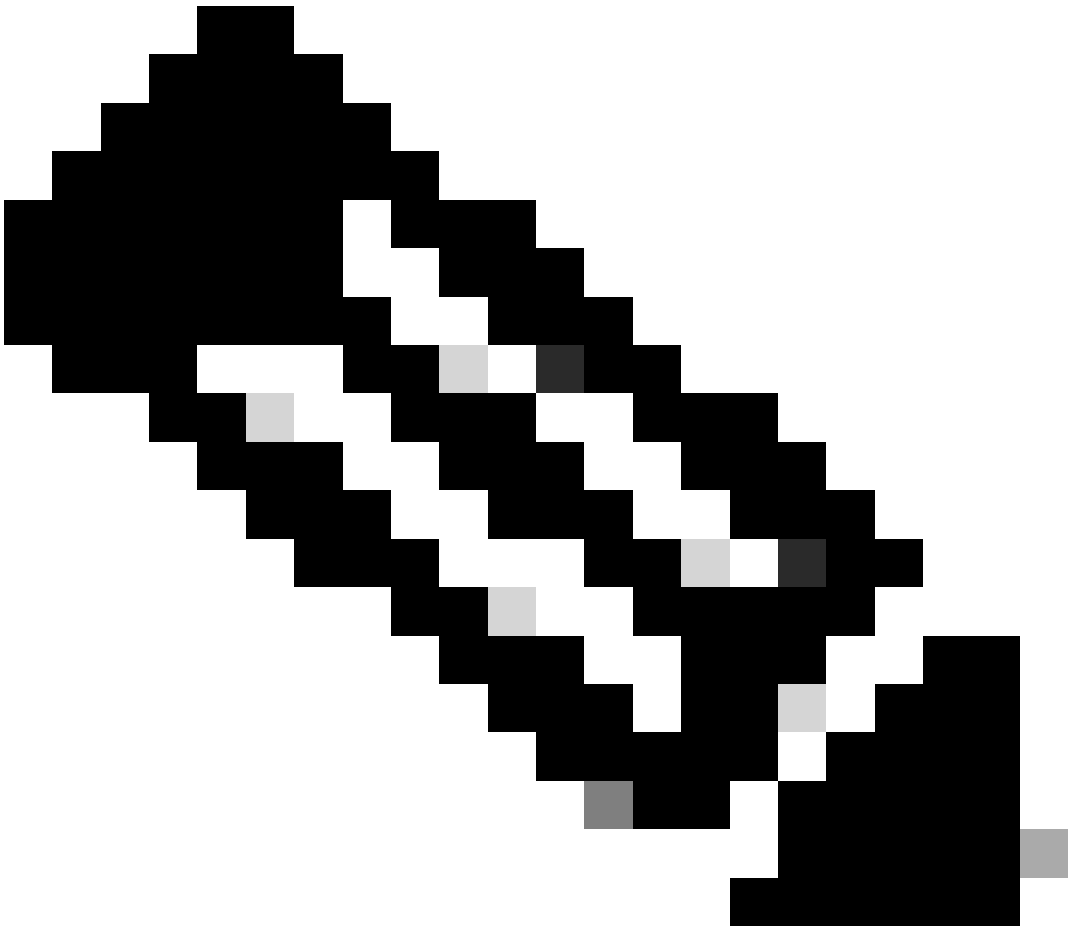


ネットワーク設定の保存

パート7：スイッチでのAAAの設定

```
C9300-1#sh run aaa
!
aaa authentication dot1x default group labgroup
aaa authorization network default group labgroup
aaa accounting dot1x default start-stop group labgroup
aaa accounting update newinfo periodic 2880
!
!
!
!
aaa server radius dynamic-author
 client 10.76.112.135 server-key cisco
!
!
radius server labserver
 address ipv4 10.76.112.135 auth-port 1812 acct-port 1813
 key cisco
!
!
aaa group server radius labgroup
 server name labserver
!
```

```
!
!
!
aaa new-model
aaa session-id common
!
!



C9300-1(config)#dot1x system-auth-control
```



注:dot1x system-auth-controlコマンドはshow running-configの出力には表示されませんが、802.1Xをグローバルに有効にする必要があります。

802.1X用のスイッチインターフェイスの設定：

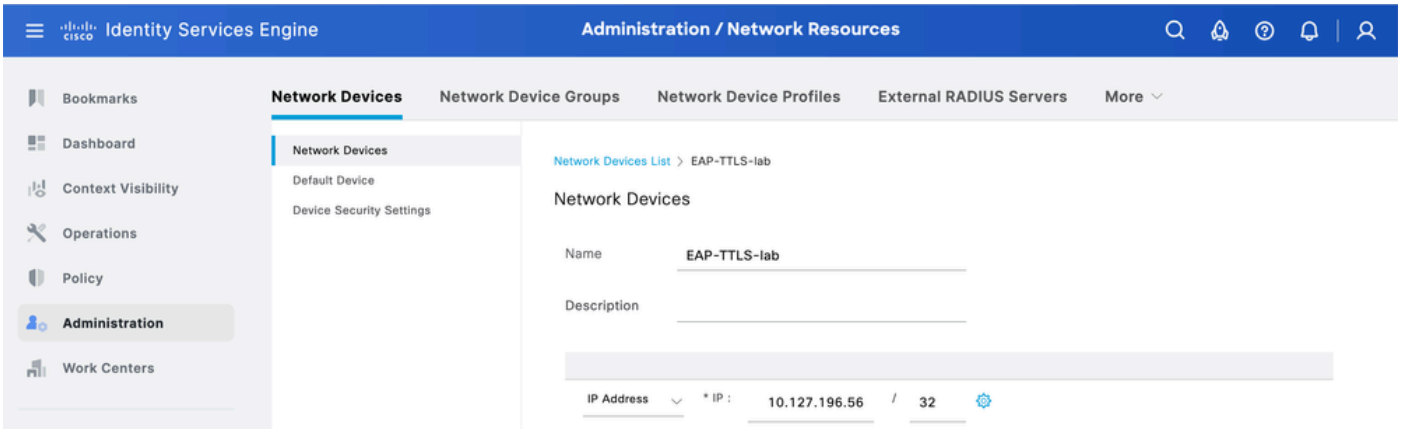
```
C9300-1(config)#do sh run int gig1/0/44
Building configuration...

Current configuration : 242 bytes
!
interface GigabitEthernet1/0/44
 switchport access vlan 96
 switchport mode access
 device-tracking
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication host-mode multi-auth
 authentication periodic

 mab
 dot1x pae authenticator
end
```

パート8:ISEの設定

ステップ 1：ISEでスイッチを設定します。

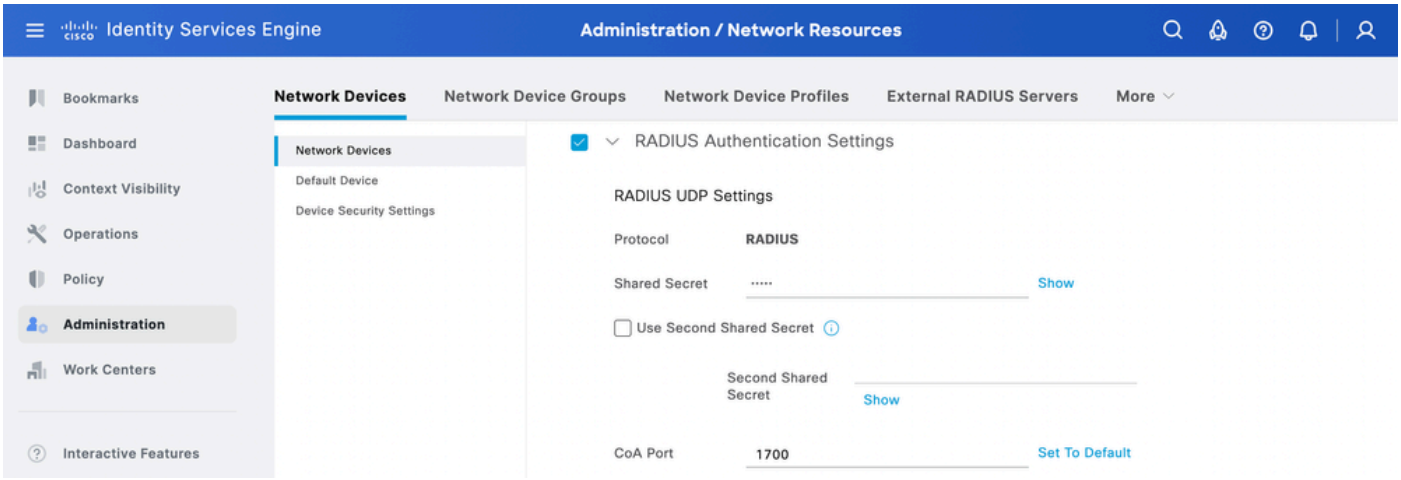
Administration > Network Resources > Network Devicesの順に移動し、Addをクリックします。

ここにスイッチ名とIPアドレスを入力します。



ネットワークデバイスISEの追加

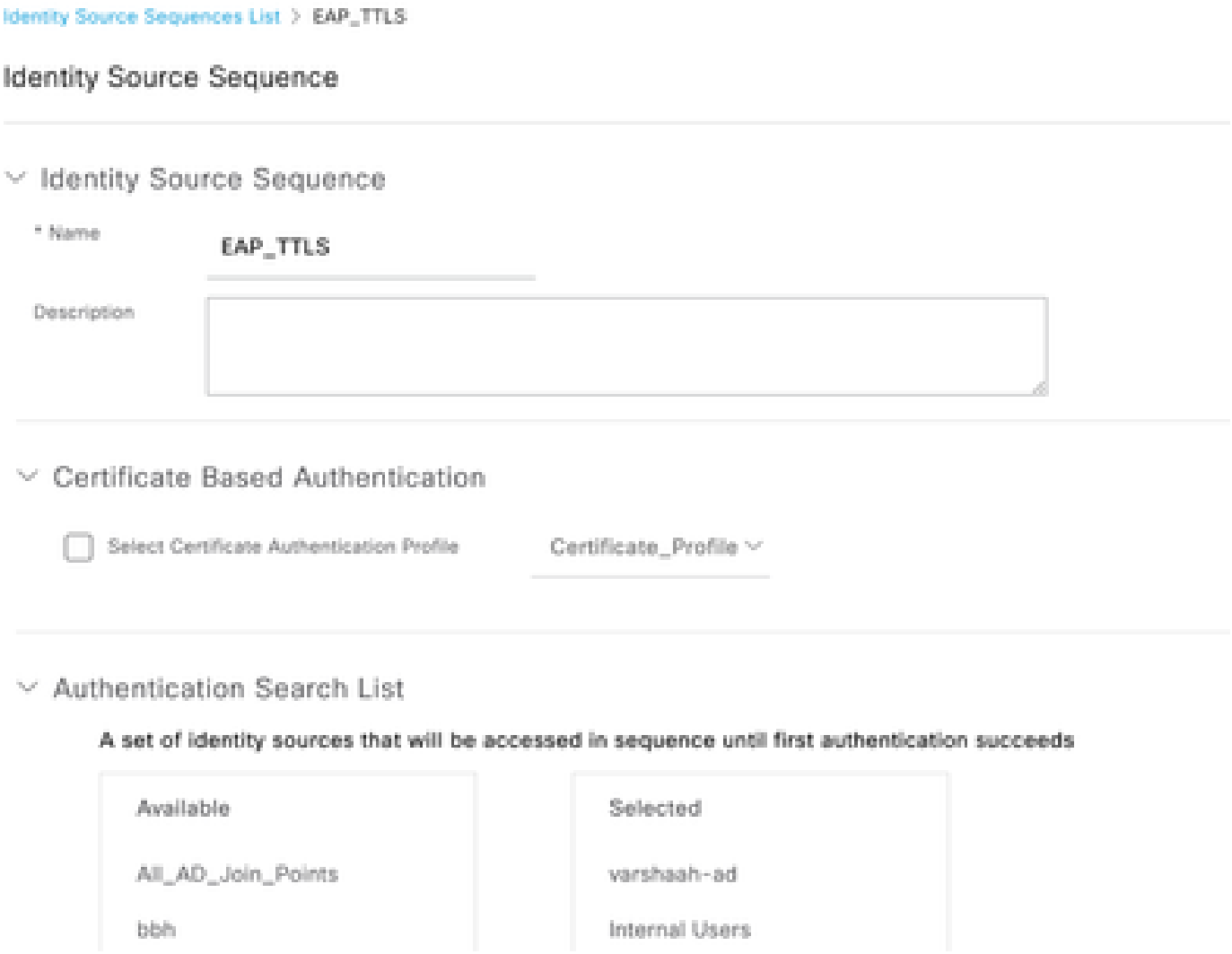
スイッチで以前に設定したRADIUS共有秘密を入力します。



RADIUS共有秘密ISE

ステップ 2：IDソースシーケンスを設定します。

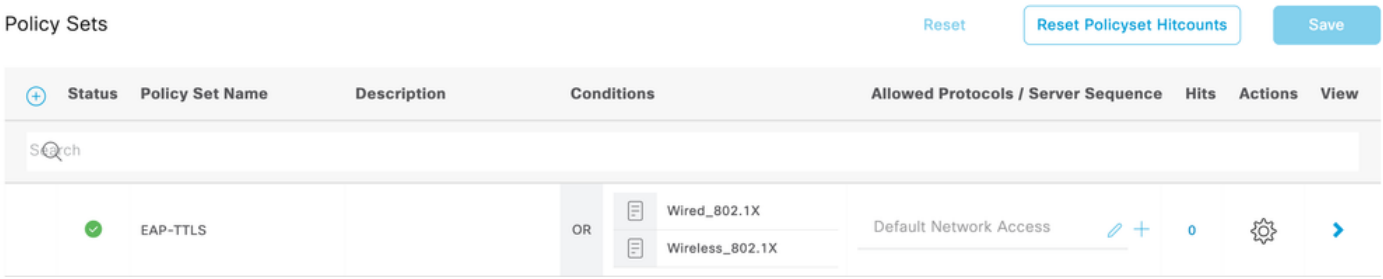
- Administration > Identity Management > Identity Source Sequencesの順に移動します。
- Addをクリックして、新しいIDソースシーケンスを作成します。
- Authentication Search Listでアイデンティティソースを設定します。



ISEアイデンティティソースシーケンス

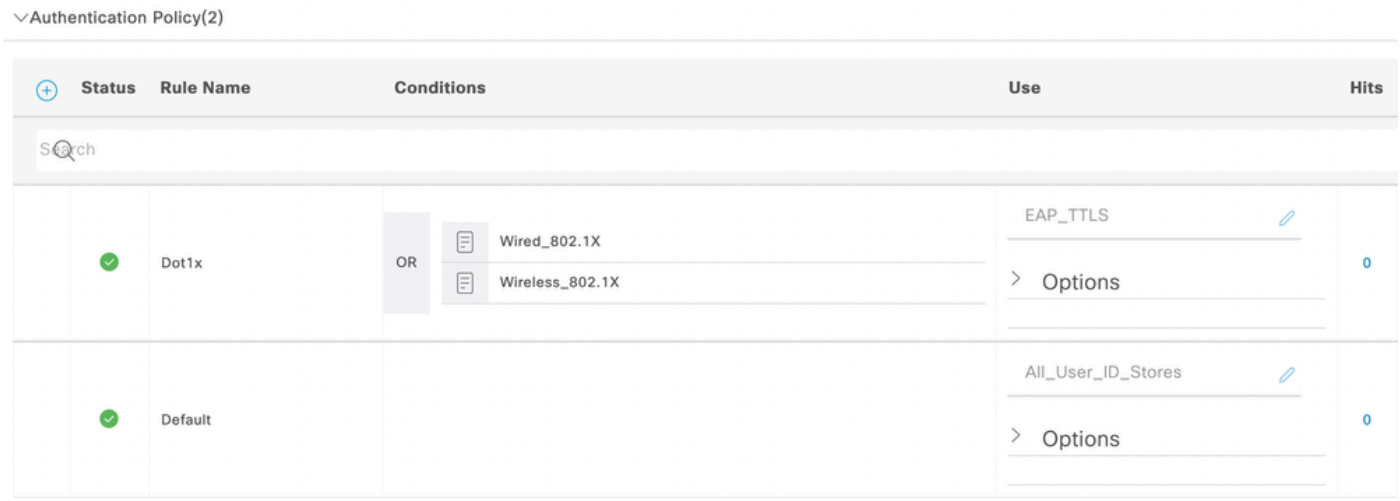
ステップ 3：ポリシーセットを設定します。

Policy > Policy Setsの順に移動し、新しいポリシーセットを作成します。条件をWired_802.1xまたはWireless_802.1xとして設定します。Allowed Protocolsで、Default Network Accessを選択します。



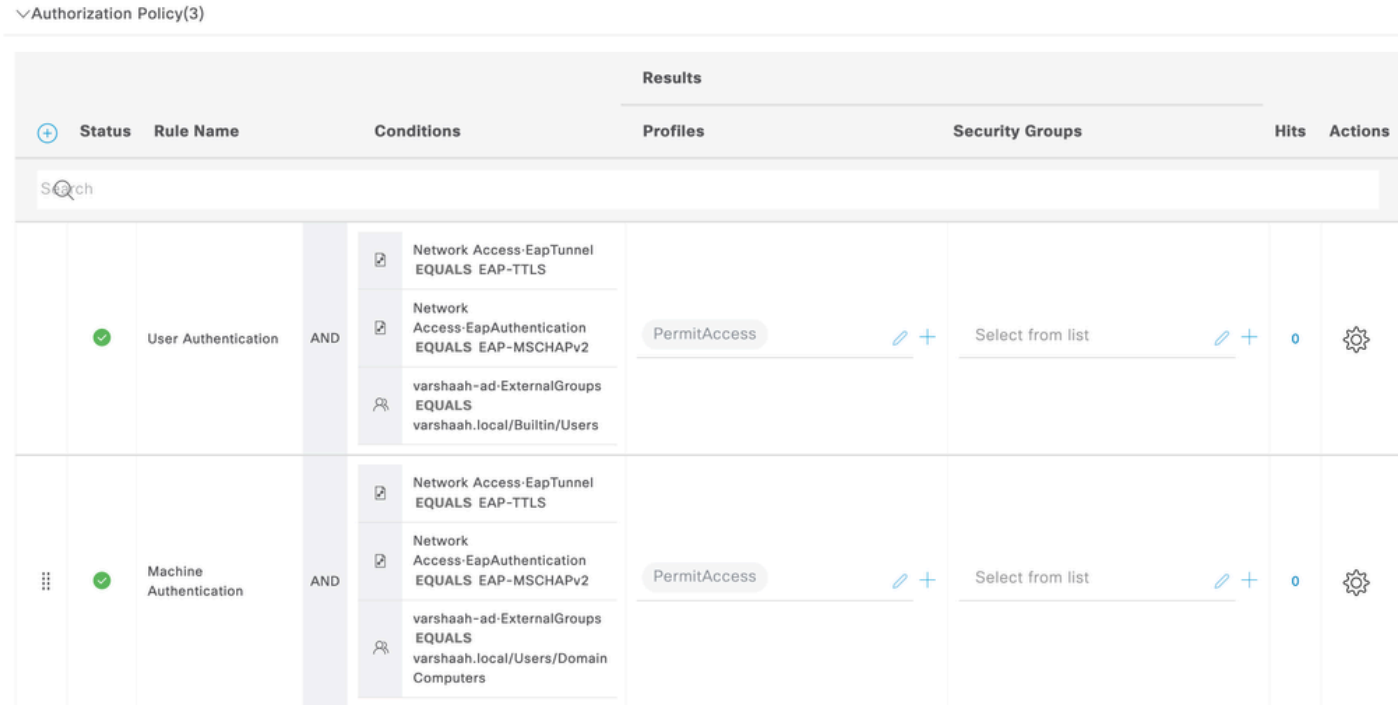
EAP-TTLSポリシーセット

dot1xの認証ポリシーを作成し、ステップ4で作成したアイデンティティソースシーケンスを選択します。



EAP-TTLS認証ポリシー

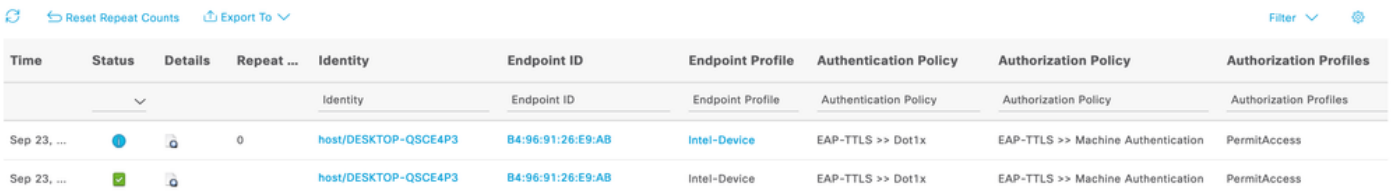
認可ポリシーの場合、3つの条件を持つルールを作成します。最初の条件では、EAP-TTLSトンネルが使用されている条件を確認します。2番目の条件は、内部EAP方式としてEAP-MSCHAPv2が使用されていることを確認します。3番目の条件は、それぞれのADグループを確認します。



Dot1x許可ポリシー

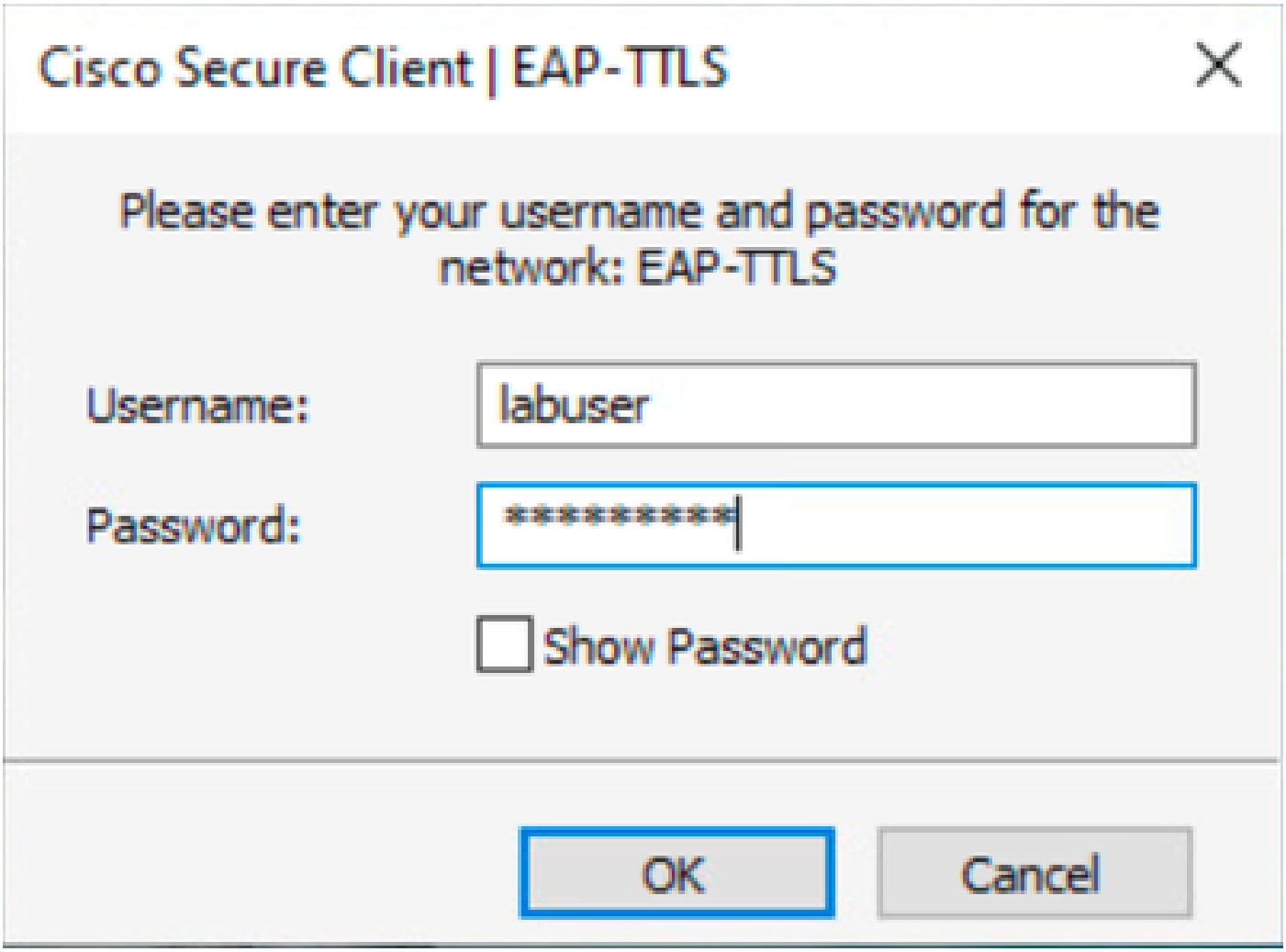
確認

Windows 10マシンを再起動するか、またはサインアウトしてからサインインします。Windowsのログイン画面が表示されるたびに、マシン認証がトリガーされます。

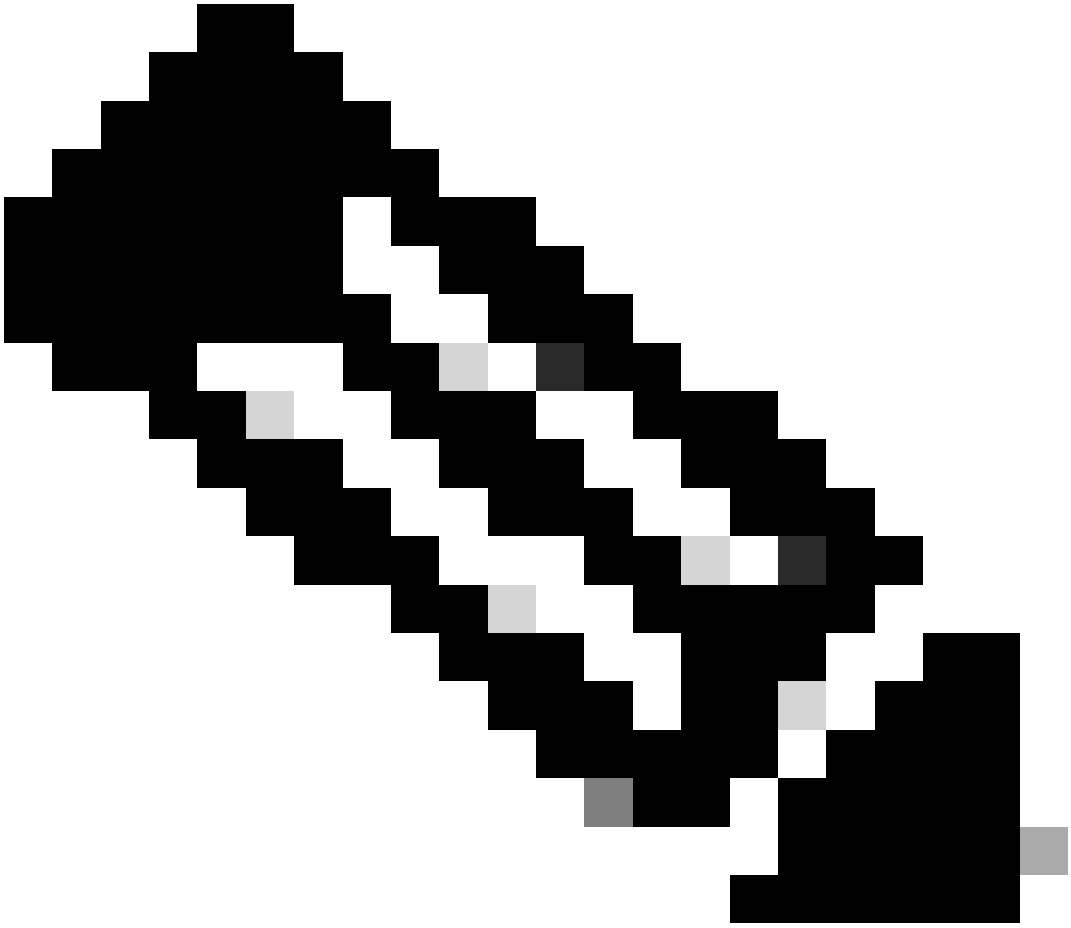


ライブログマシン認証

クレデンシャルを使用してPCにログインすると、ユーザ認証がトリガーされます。

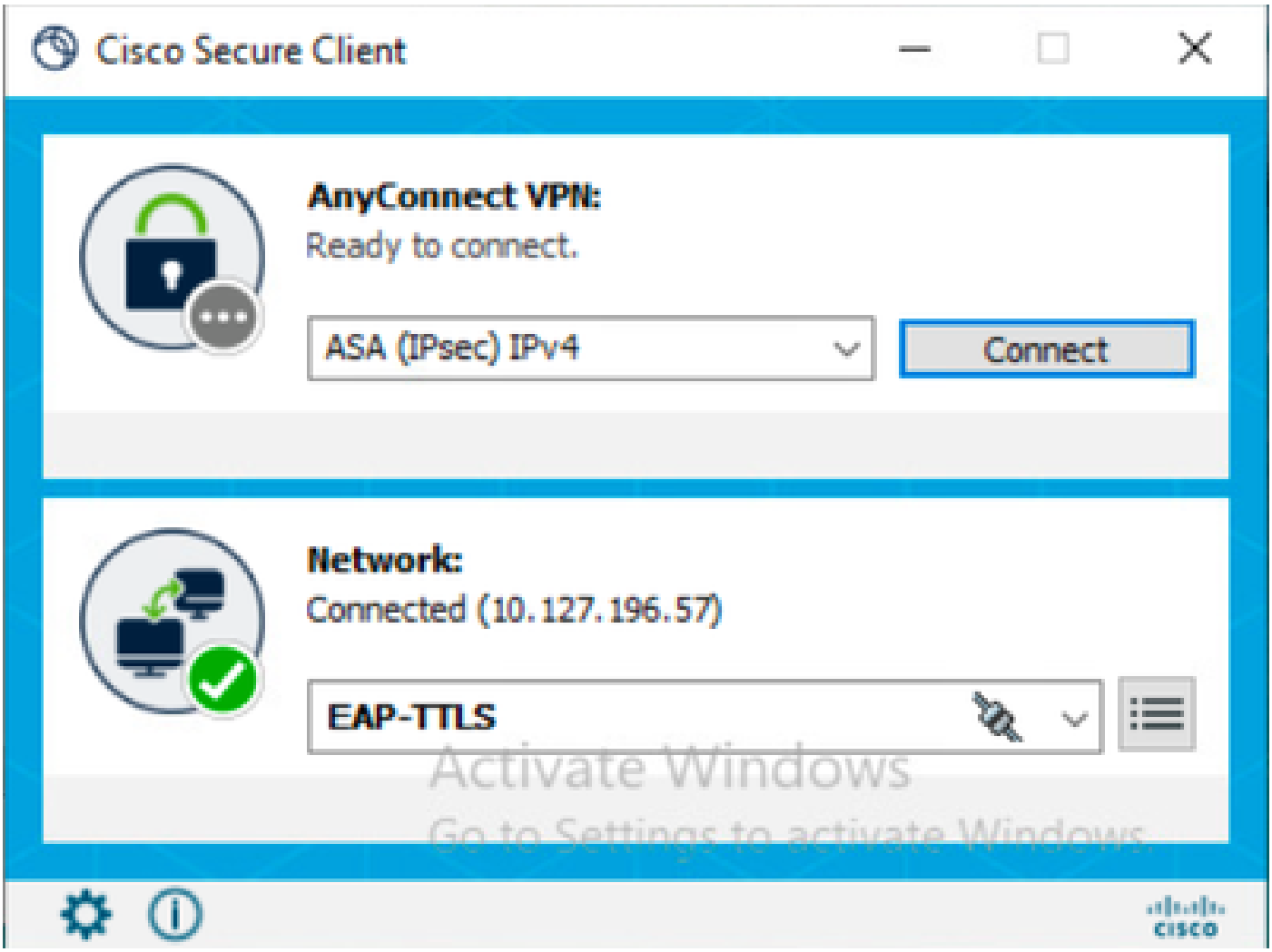


ユーザ認証クレデンシャル

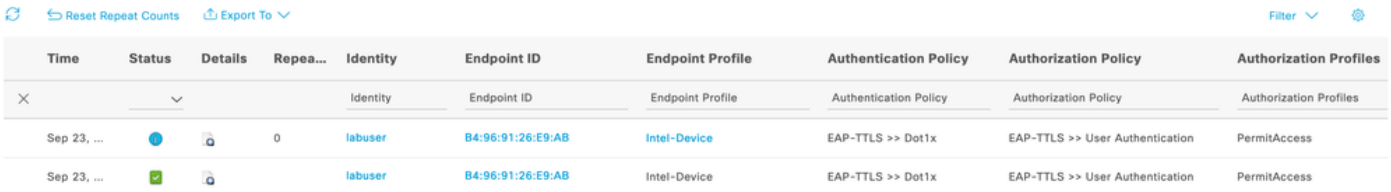


注：この例では、認証にActive Directoryユーザクレデンシャルを使用します。または、Cisco ISEで内部ユーザを作成し、そのクレデンシャルを口グインに使用できます。

クレデンシャルを入力して正常に検証すると、エンドポイントはユーザ認証でネットワークに接続されます。



接続されたEAP-TTLS



ライブログのユーザ認証

ISE RADIUSライブログの分析

このセクションでは、マシンおよびユーザ認証が成功した場合のRADIUSライブログエントリについて説明します。

マシン認証

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... .. 11507 Extracted EAP-Response/Identity 12983 Prepared EAP-Request proposing EAP-TTLS with challenge ... ... 12978 EAP-TTLS challenge-responseを含むExtracted EAP-Response and accepting EAP-TTLS as negotiated 12800 Extracted first TLS record; tls handshake started 12805 Extracted TLS ClientHello message 12806 Prepared TLS ServerHello message 12807 Prepared TLS Certificate message 12808 Prepared TLS ServerKeyExchange message 12810 Prepared TLS ServerDone message ... 12803 Extracted TLS ChangeCipherSpec message 12804 Extracted TLS Finished message 12801 12802 Prepared TLS

Finished message 12816 TLS handshake succeeded ... 11806 Prepared EAP-Request for inner method propossing EAP schap with challenge 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 Returned RADIUS Access-Challenge 11001 12971 11808 24431 24325 24343 24470 22037 12971 11810 11814 11519 12975 15036 24209 24211 15048 15048 15016 11002 Received RADIUS Access-Request ... ce4P3 ... .. RPCログオン要求が成功しました – DESKTOP-QSCE4P3$@varshaah.local Active Directoryに対するマシン認証が成功しました – varshaah-ad Exceeded ... ...

ユーザ認証

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... .. 11507 Extracted EAP-Response/Identity 12983 Prepared EAP-Request proposing EAP-TTLS with challenge ... ... 12978 EAP-TTLS challenge-responseを含むExtracted EAP-Response and accepting EAP-TTLS as negotiated 12800 Extracted first TLS record; tlsハンドシェイク12805開始されたTLS ClientHelloメッセージ12806準備されたTLS ServerHelloメッセージ12807準備されたTLS証明書メッセージ12808準備されたTLS ServerKeyExchangeメッセージ12810準備されたTLS ServerDoneメッセージ… 12812抽出されたTLS ClientKeyExchangeメッセージ12803抽出されたTLS ChangeCipherSpecメッセージ1280412801準備されたTLS1280212816準備されたメッセージ....11806 eap-Request for inner method propossing EAP-MSCHAP with challenge 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 11001 12971 11808 24430 24325 24343 24402 22037 12971 11810 11814 11519 12975 15036 24209 24211 15048 15048 15016 11002 Returned RADIUS Access-Challenge Received RADIUS Access-Request ... ad Resolving ID - labuser@varshaah.local ... RPC Logon request succeeded - labuser@varshaah.local Active Directoryに対するユーザ認証に成功 – varshaah-ad Authentication Passed ...抽出EAP-Response containing EAP-Response containing EAP-TTLS challenge-response抽出EAP-Response for inner method containing MSCHAP-response内部EAP-MSCHAP認証に成功しました準備EAP-Successful内部EAP方式認証にに成功しました内部エンドポイントでエンドポイントを検索IDStore - labuser

NAMログの分析

特に拡張ロギングを有効にした後のNAMログには大量のデータが含まれており、そのほとんどは無関係で無視できます。このセクションでは、ネットワーク接続を確立するためにNAMが実行する各ステップを示すデバッグ行を示します。ログの作業を進めるときに、問題に関連するログの部分を見つけるのに役立つキーフレーズを次に示します。

マシン認証

```
2160: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11812][comp=SAE]: 80
```

クライアントはネットワークスイッチからEAP-TTLSパケットを受信し、EAP-TTLSセッションを開始します。これは、マシン認証トンネルの開始点です。

```
2171: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11812][comp=SAE]: EA
2172: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11812][comp=SAE]: CER
2173: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11812][comp=SAE]: CER
```

クライアントはISEからServer Helloを受信し、サーバ証明書(CN=varshah.varshah.local)の検証を開始します。 証明書はクライアントの信頼ストアで見つかり、検証のために追加されます。

```
2222: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11768]: Validating th
2223: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11768]: Server certif
```

サーバ証明書が正常に検証され、TLSトンネルの確立が完了します。

```
2563: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.789 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2564: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.789 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11812][comp=SAE]: NE
2565: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.789 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
```

クライアントは、認証に成功したことを通知します。インターフェイスのブロックが解除され、内部状態のマシンがUSER_T_NOT_DISCONNECTEDに移行します。これは、このマシンがトラフィックを渡せるようになったことを示します。

```
2609: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2610: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11824][comp=SAE]: NE
2611: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2612: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11824][comp=SAE]: NE
2613: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2614: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11824][comp=SAE]: NE
2615: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
```

アダプタがauthenticatedを報告し、NAM AccessStateMachineはACCESS_AUTHENTICATEDに移行します。これにより、マシンが認証を正常に完了し、フルネットワークアクセスが可能になったことが確認されます。

ユーザ認証

```
100: DESKTOP-QSCE4P3: Sep 25 2025 14:01:26.669 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9664]: Network EAP-TT
```

NAMクライアントがEAP-TTLS接続プロセスを開始します。

```
195: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3252]: Binding adapte
198: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3252]: Network EAP-TT
```

NAMは物理アダプタをEAP-TTLSネットワークにバインドし、ACCESS_ATTACHED状態に移行して、アダプタが認証のための準備ができていることを確認します。

```
204: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3252]: Network EAP-TT
247: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3680][comp=SAE]: STAT
```

クライアントは802.1X交換を開始して、ATTACHEDからCONNECTINGに移行します。

```
291: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.388 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: 8021
```

クライアントは認証プロセスをトリガーするためにEAPOL-Startを送信します。

```
331: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.435 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: PORT
332: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.435 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: 8021
340: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.435 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: EAP
```

スイッチはIDを要求し、クライアントは外部IDで応答する準備をします。

```
402: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.685 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9580]: EAP-CB: creden
422: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.685 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: processin
460: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.685 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: credentia
```

NAMは外部IDを送信します。デフォルトでは、これはanonymousであり、交換が（マシンではなく）ユーザ認証用であることを示します。

```
488: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-6-INFO_MSG: %[tid=6088]: EAP: EAP sugges
489: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-6-INFO_MSG: %[tid=6088]: EAP: EAP reques
490: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: EAP metho
491: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: credentia
```

クライアントとサーバの両方が、外部方式としてEAP-TTLSを使用することに同意しています。

```
660: DESKTOP-QSCE4P3: Sep 25 2025 14:01:27.185 +0900: %csc_nam-7-DEBUG_MSG: %[tid=8296][comp=SAE]: EAP
661: DESKTOP-QSCE4P3: Sep 25 2025 14:01:27.185 +0900: %csc_nam-7-DEBUG_MSG: %[tid=8296][comp=SAE]: EAP
```

クライアントはClient Helloを送信し、ISE証明書を含むServer Helloを受信します。

```
706: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.967 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: 802
717: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.967 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EAP
718: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.967 +0900: %csc_nam-6-INFO_MSG: %[tid=11932][comp=SAE]: CERT
719: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-6-INFO_MSG: %[tid=11932][comp=SAE]: CERT
726: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EAP
```

サーバ証明書が提示されます。クライアントはCN varshaah.varshaah.localを検索し、一致を見つけ、証明書を検証します。X.509証明書がチェックされている間、ハンドシェイクは一時停止します。

```
729: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EAP
730: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11916][comp=SAE]: EAP
1110: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.044 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
1111: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.044 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
```

トンネルが確立されます。NAMは、内部認証のために保護されたアイデンティティとクレデンシャルを要求し、準備します。

```
1527: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.169 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11916][comp=SAE]: EA
1528: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.169 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11916][comp=SAE]: EA
1573: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.184 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EA
1574: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.184 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EA
1575: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.184 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EA
```

TLSハンドシェイクが完了します。内部認証のためにセキュアトンネルが確立されました。

```
1616: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.262 +0900: %csc_nam-6-INFO_MSG: %[tid=9664]: Protected iden
1620: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9664]: Auth[EAP-TTLS
1689: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.277 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9664]: Auth[EAP-TTLS
```

保護されたID（ユーザ名）がISEによって送信され、受け入れられます。

```
1708: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.277 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9456][comp=SAE]: EAP
1738: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.758 +0900: %csc_nam-6-INFO_MSG: %[tid=11768]: Protected pas
1741: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.200 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
```

ISEがパスワードを要求します。NAMは保護されたパスワードをTLSトンネル内で送信します。

```
1851: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
1852: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: ST
1853: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
1854: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: ST
1855: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: ST
```

ISEがパスワードを検証し、EAP-Successを送信して、NAMがAUTHENTICATEDに移行します。この時点で、ユーザ認証が完了し、クライアントはネットワークアクセスを許可されます。

トラブルシュート

Cisco ISEとスイッチの統合に関するNetwork Access Manager(NAM)の問題をトラブルシューティングする場合、Secure Client(NAM)、Cisco ISE、およびスイッチの3つのコンポーネントすべてのログを収集する必要があります。

セキュアクライアント(NAM)ログ

1. 次の手順に従って、NAM拡張ロギングを有効にします。
2. 問題を再現します。ネットワークプロファイルが適用されない場合は、Secure ClientでNetwork Repairを実行します。
3. Diagnostics and Reporting Tool(DART)を使用してDARTバンドルを収集します。

Cisco ISEログ

ISEで次のデバッグを有効にして、認証とディレクトリのやり取りをキャプチャします。

- ランタイムAAA
- nsf
- nsf-session

スイッチログ

基本的なデバッグ

```
request platform software trace rotate all
set platform software trace smd switch active R0 radius debug
set platform software trace smd switch active R0 aaa debug
set platform software trace smd switch active R0 dot1x-all debug
set platform software trace smd switch active R0 eap-all debug
debug radius all
```

高度なデバッグ（必要な場合）

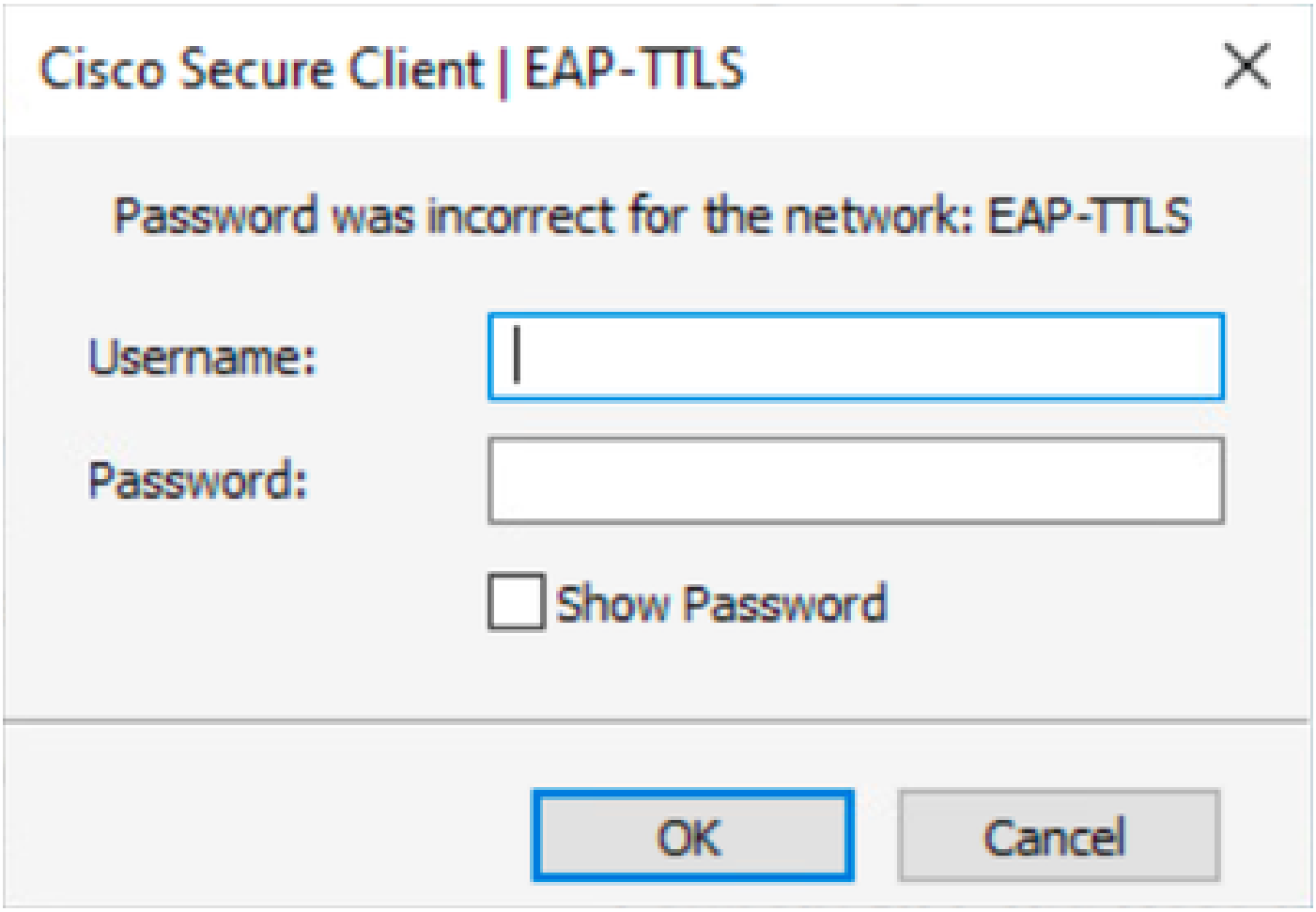
```
set platform software trace smd switch active R0 epm-all debug
set platform software trace smd switch active R0 pre-all debug
```

show コマンド

```
show version
show debugging
show running-config aaa
show authentication session interface gix/x details
show dot1x interface gix/x
show aaa servers
show platform software trace message smd switch active R0
```

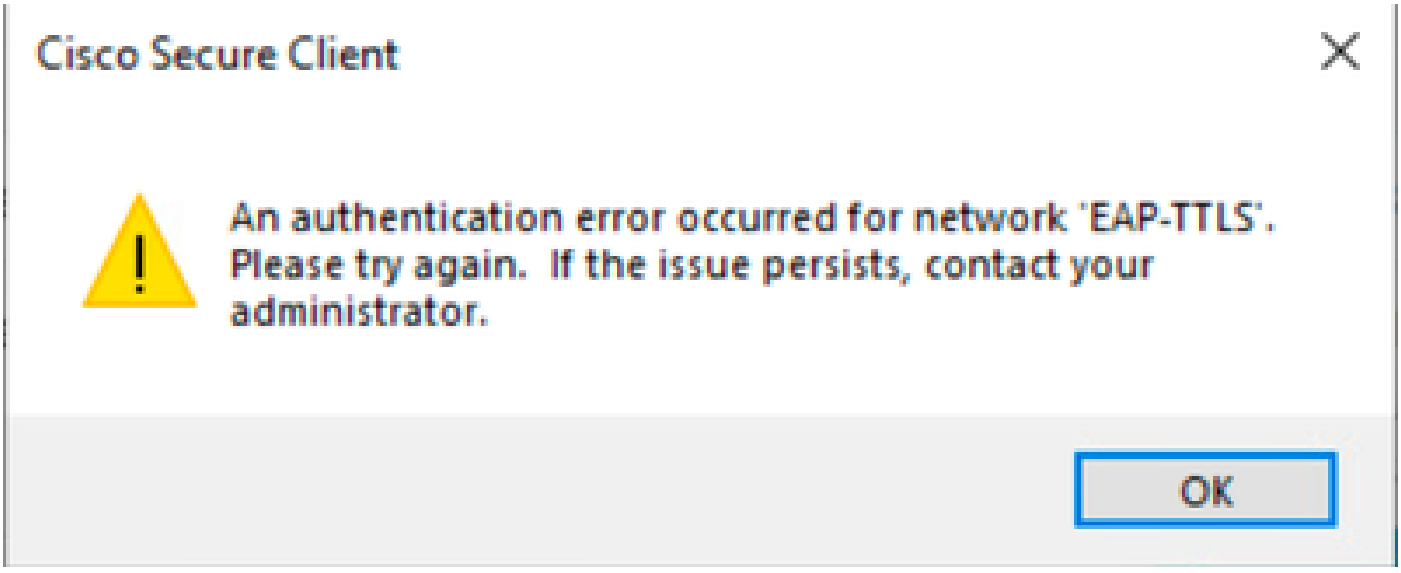
クレデンシャルが無効なため、ユーザ認証が失敗する

ユーザが誤ったクレデンシャルを入力すると、セキュアクライアントで「Password was incorrect for the network: EAP-TTLS」という一般的なメッセージが表示されます。画面上のエラーでは、問題の原因が無効なユーザ名またはパスワードであるかどうかは示されません。



不正確なパスワードエラー

認証が2回連続して失敗すると、Secure Clientに「An authentication error occurred for network 'EAP-TTLS'.」というメッセージが表示されます。 問題が解決しない場合は、管理者に問い合わせてください。



ユーザ認証の問題

原因を特定するには、NAMログを確認します。

1. パスワードが正しくない：

ユーザが誤ったパスワードを入力すると、NAMログに次の出力のようなエントリが表示されます。

```
3775: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.921 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
3776: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.921 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
3777: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.922 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
```

Cisco ISEライブログでは、対応するイベントは次のように表示されます。

Event	5400 Authentication failed
Failure Reason	24408 User authentication against Active Directory failed since user has entered the wrong password
Resolution	Check the user password credentials. If the RADIUS request is using PAP for authentication, also check the Shared Secret configured for the Network Device
Root cause	User authentication against Active Directory failed since user has entered the wrong password

パスワードの誤り

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... .. 11507 Extracted EAP-Response/Identity 10 12983 Prepared EAP-Request proposaling EAP-TTLS with challenge ... .. 12978 EAP-TTLS challenge-responseを含むEAP-Response extracted 12800 Extracted first TLS record; tls handshake started ... .. 12810 Prepared TLS ServerDone message ... .. 12812 Extracted TLS ClientKeyExchange message 12803 Extracted TLS ChangeCipherSpec message ... .. 12816 TLS handshake succeeded ... **11806 Prepared EAP-Request for inner method proposting EAP-MSCHAP with challenge** 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 11001 Returned RADIUS Access-Request . .. .. 12971 EAP-TTLS challenge-response 0を含む抽出されたEAP-Response **11808内部方式のEAP-MSCHAP challenge-responseを含み、ネゴシエートされたとおりにEAP-MSCHAPを受け入れる抽出されたEAP-Response** .. 15013 Selected Identity Source - varshaah-ad 0 24430 Authenticating user against Active Directory - varshaah-ad 0 24325 Resolving identity - labuser@varshaah.local 4 24313 24319 24323 24344 24408 11823 11815 12976 11003 0 **RPC Logon request failed - STATUS_WRONG_PASSWORD, ERROR_INVALID_PASSWORD, labuser@varshaah.local 20☆ユーザが誤ったパスワードを入力したため、Active Directoryに対するユーザ認証が失敗しました – varshah-ad 1**

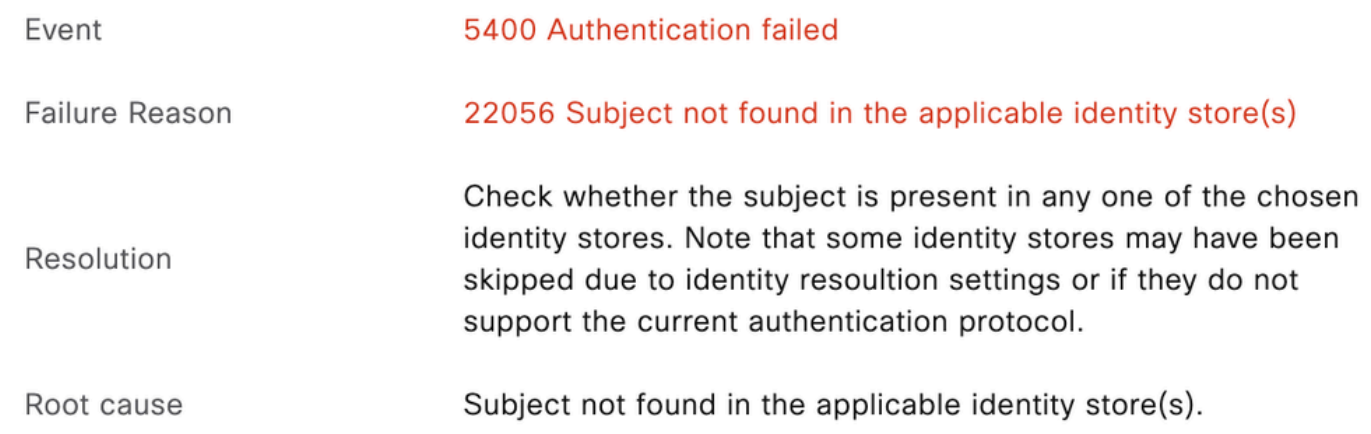
---

2. ユーザ名が正しくない：

ユーザが誤ったユーザ名を入力すると、NAMログに次のようなエントリが表示されます。

```
3788: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.923 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
3789: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.923 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300]: EAP-CB: EAP
```

Cisco ISEライブログでは、対応するイベントは次のように表示されます。



ユーザ名が正しくない

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... .. 11507 Extracted EAP-Response/Identity 12983 Prepared EAP-Request proposing EAP-TTLS with challenge ... ... 12978 EAP-TTLS challenge-responseを含むExtracted EAP-Response and accepting EAP-TTLS as negotiated 12800 Extracted first TLS record; tls handshake started ... .. 12810 Prepared TLS ServerDone message ... .. 12812 Extracted TLS ClientKeyExchange message 12803 Extracted TLS ChangeCipherSpec message ... 12816 TLS handshake succeeded ... 11806 Prepared EAP-Request for inner method proposting EAP-MSCHAP with challenge 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 11001 Returned RADIUS Access-Request .... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response 11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated ... 15013 Selected Identity Source - All_AD_Join_Points 24430 Authenticating user against Active Directory - varshah-ad 24325 Resolving identity - user@varshaah.local 24313 24352 24412 15013 24210 24216 22056 22058 22061 11823 11815 12976 11504 11003 Search for matching accounts at join - varshah.local ... Active Directoryにユーザーが見つかりません – varshah-ad ... .. .選択されたアイデンティティソース – 内部ユーザー内部ユーザーIDtoreでユーザーを検索する – user内部ユーザーIDstoreでユーザーが見つかりません...

.....

authentication failed... ... EAP-TTLS authentication failed 0 ... .

既知の障害

Bug ID	説明
Cisco Bug ID 63395	ISE 3.0は、サービスの再起動後にREST IDストアを見つけることができません

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。