TEAPとのEAPチェーン

内容

概要

このドキュメントでは、Tunnel-based Extensible Authentication Protocol(TEAP)を使用したExtensible Authentication Protocol(EAP)チェーン用にISEおよびWindowsサプリカント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。

- ISE
- Windowsサプリカントの設定

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。

- Cisco ISE バージョン 3.0
- Windows 10ビルド2004
- プロトコルTEAPの知識

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、初期（デフォルト）設定の状態から起動しています。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

TEAPはトンネルベースのExtensible Authentication Protocol(EAP)方式で、セキュアなトンネルを確立し、そのセキュアなトンネルの保護のもとで他のEAP方式を実行します。

TEAP認証は、最初のEAP ID要求/応答の交換の後、2つのフェーズで行われます。

最初のフェーズでは、TEAPはTLSハンドシェイクを使用して、認証されたキー交換を提供し、保護されたトンネルを確立します。トンネルが確立されると、2番目のフェーズはピアから開始され、サーバは必要な認証と認可ポリシーを確立するために会話を続けます。

Cisco ISE 2.7以降では、TEAPプロトコルがサポートされています。 type-length-value(TLV)オブジェクトは、EAPピアとEAPサーバ間で認証関連のデータを転送するためにトンネル内で使用されます。

Microsoftは、2020年5月にリリースされたWindows 10 2004バージョンでTEAPのサポートを導入しました。

EAPチェーンを使用すると、2つの個別のセッションではなく、1つのEAP/Radiusセッション内でユーザ認証とマシン認証を実行できます。

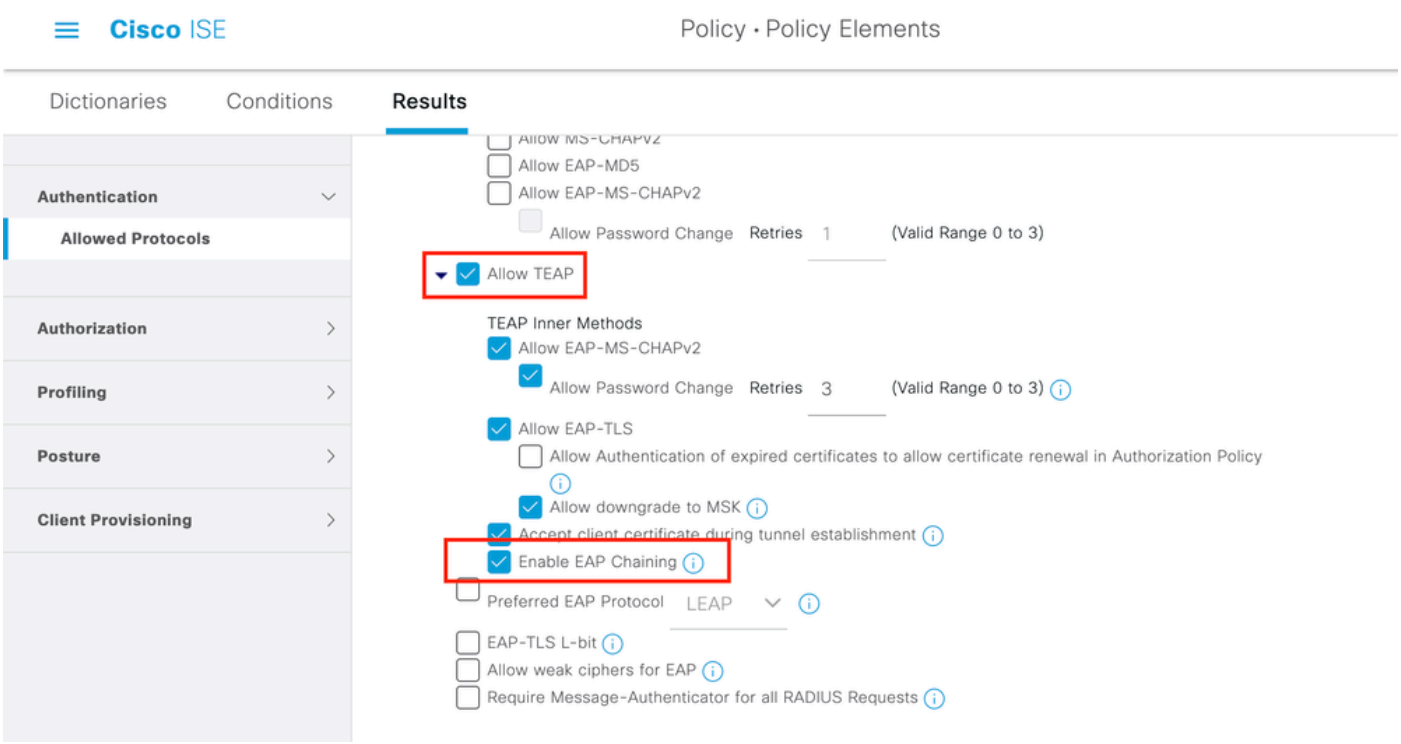
以前は、これを実現するには、Cisco AnyConnect NAMモジュールが必要でした。ネイティブWindowsサプリカントではEAP-FASTをサポートしていなかったため、WindowsサプリカントでEAP-FASTを使用する必要がありました。これで、Windowsネイティブサプリカントを使用して、TEAPを使用したISE 2.7とのEAPチェーンを実行できます。

設定

Cisco ISE の設定

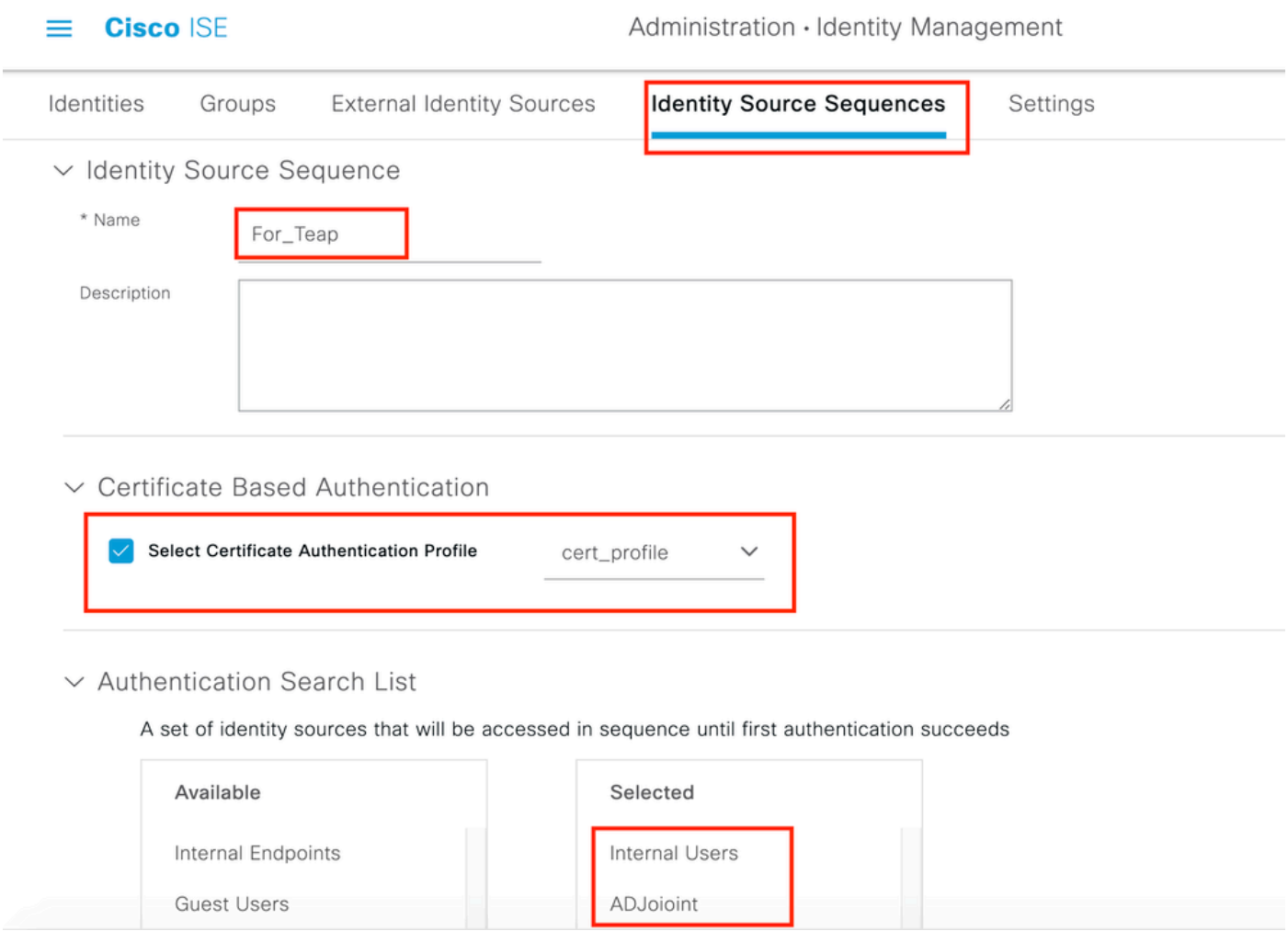
ステップ 1：TEAPおよびEAPチェーンを有効にするには、[Allowed Protocols]を編集する必要があります。

移動先 ISE > Policy > Policy Elements > Results > Authentication > Allowed Protocols > Add New .[TEAP]および[EAP chaining]チェックボックスをオンにします。



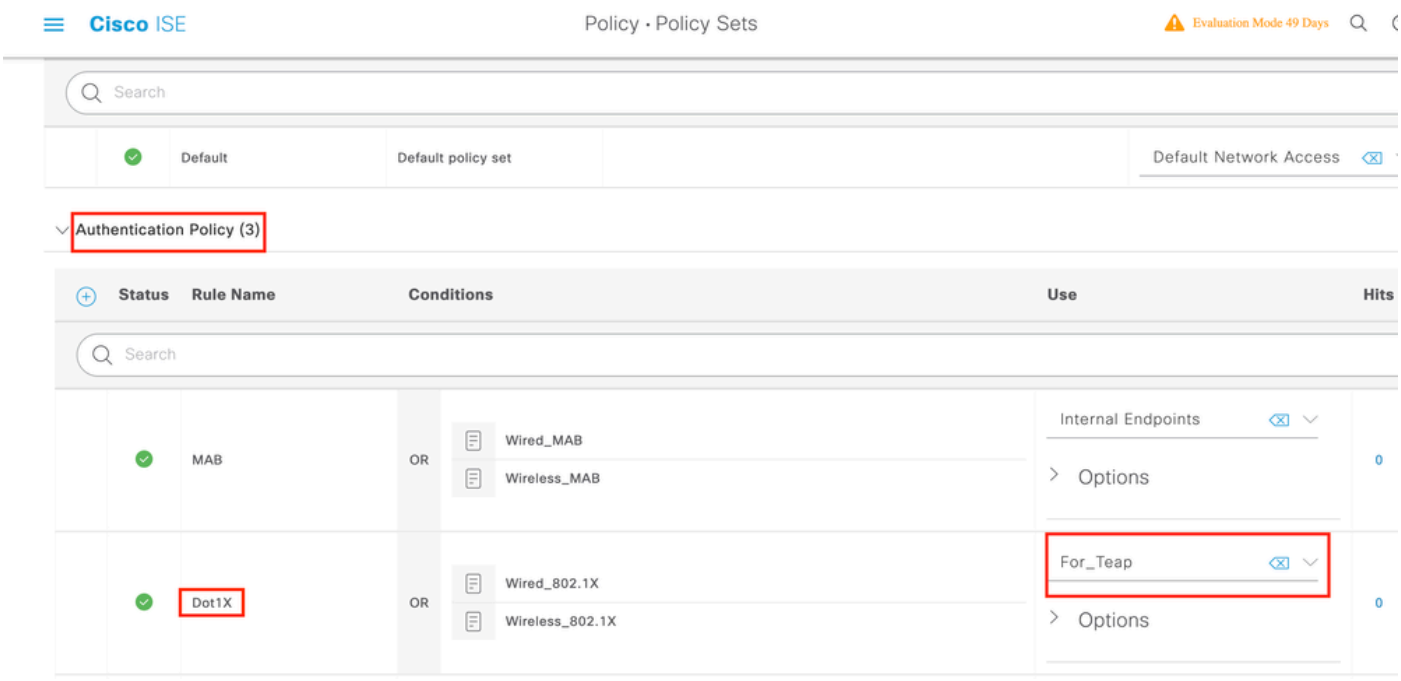
ステップ 2：証明書プロファイルを作成し、アイデンティティソースシーケンスに追加します。

移動先 **ISE > Administration > Identities > identity Source Sequence** 証明書プロファイルを選択します。



ステップ 3：認証ポリシーでこのシーケンスを呼び出す必要があります。

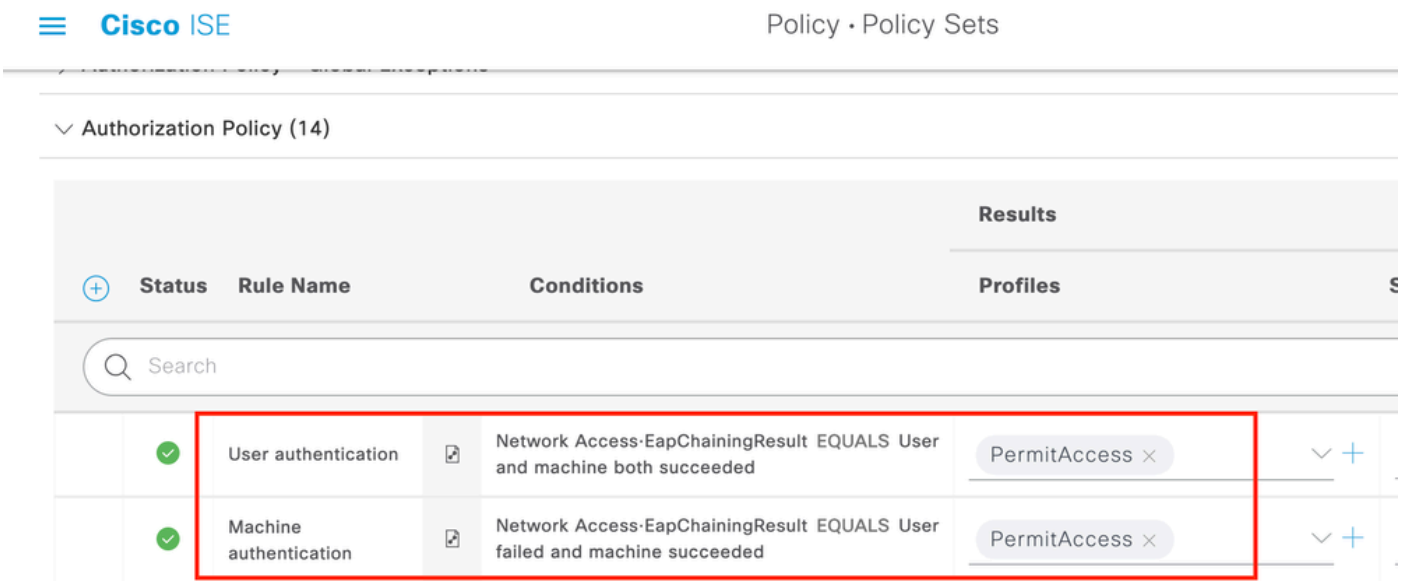
移動先 ISE > Policy > Policy Sets . Choose the Policy Set for Dot1x > Authentication Policy ステップ2で作成したアイデンティティソースシーケンスを選択します。



ステップ 4：次に、Dot1xポリシーセットの下の認可ポリシーを変更する必要があります。

移動先 ISE > Policy > Policy Sets . Choose the Policy Set for Dot1x > Authentication Policy .

2つのルールを作成する必要があります。最初のルールでは、マシンは認証されているが、ユーザは認証されていないことを確認します。2番目のルールは、ユーザとマシンの両方が認証されていることを確認します。



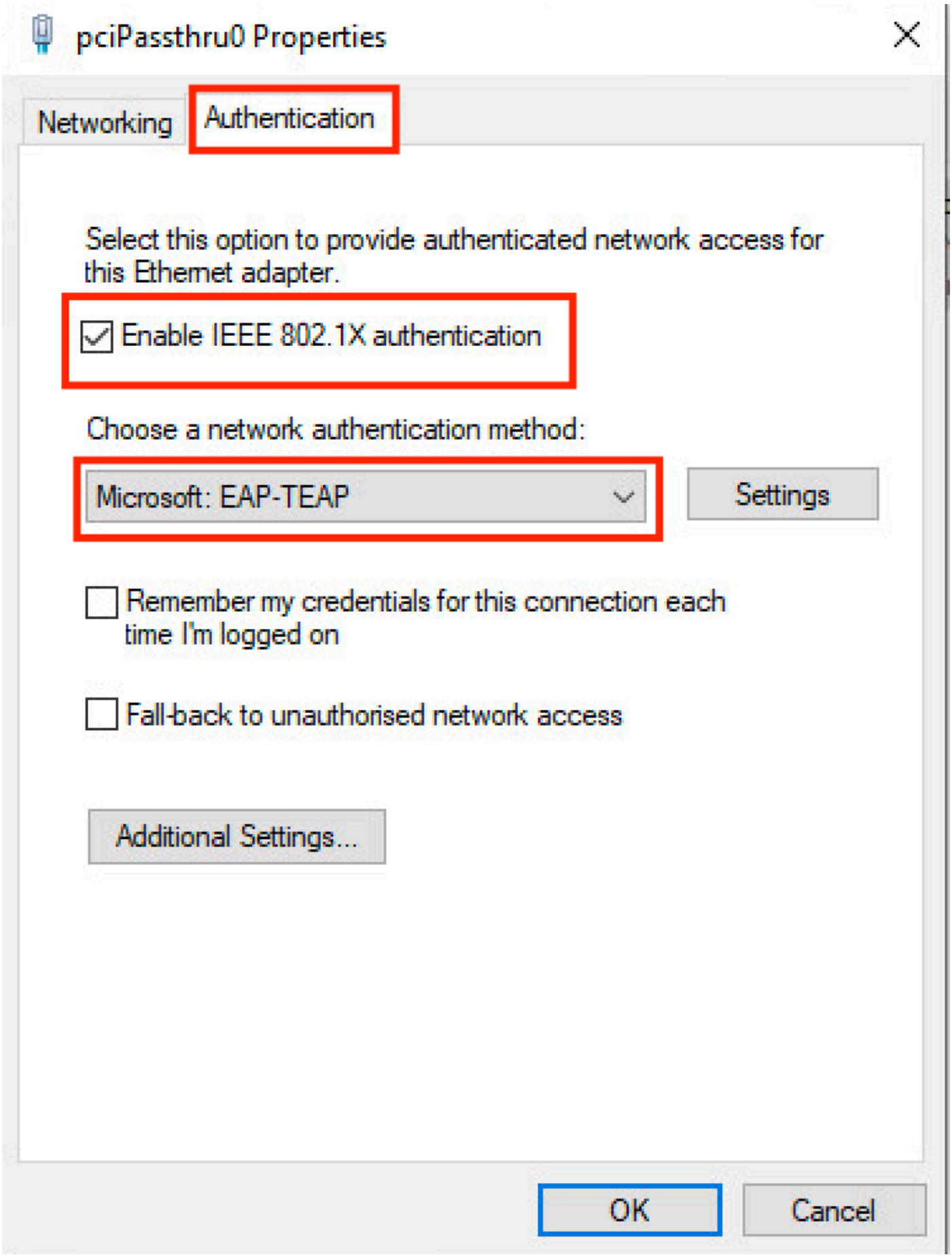
これで、ISEサーバ側からの設定が完了します。

Windowsネイティブサプリカントの設定

このドキュメントで有線認証設定を行います。

移動先 Control Panel > Network and Sharing Center > Change Adapter Settings 右クリックして **LAN Connection > Properties.**をクリックします。 **Authentication** tab.

ステップ 1：クリック Authentication ドロップダウンから、 Microsoft EAP-TEAP.



ステップ 2： ポリシーの横の [レポート（Report）] Settings ボタンをクリックします。

1. 保持 Enable Identity Privacy 有効： anonymous をIDとして使用します。
2. [Trusted Root Certification Authorities]の下で、ルートCAサーバの横にチェックマークを付けます。このサーバは、ISE PSN上でEAP認証用の証明書に署名するために使用されます。

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。