EAP-Verkettung mit TEAP

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie ISE und Windows-Supplicant für die EAP-Verkettung (Extensible Authentication Protocol) mit dem tunnelbasierten TEAP (Extensible Authentication Protocol) konfiguriert werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- ISE
- Konfiguration von Windows Supplicant

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ISE Version 3.0
- Windows 10, Build 2004
- Kenntnisse des Protokolls TEAP

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

TEAP ist ein tunnelbasiertes Extensible Authentication Protocol-Verfahren, das einen sicheren Tunnel erstellt und andere EAP-Verfahren unter dem Schutz dieses geschützten Tunnels ausführt.

Die TEAP-Authentifizierung erfolgt in zwei Phasen nach dem anfänglichen EAP-Identitätsanforderungs-/Antwortaustausch.

In der ersten Phase verwendet TEAP den TLS-Handshake, um einen authentifizierten Schlüsselaustausch bereitzustellen und einen geschützten Tunnel einzurichten. Sobald der Tunnel eingerichtet ist, beginnt die zweite Phase mit dem Peer, und der Server führt eine weitere Konversation durch, um die erforderlichen Authentifizierungs- und Autorisierungsrichtlinien festzulegen.

Cisco ISE 2.7 und höher unterstützt das TEAP-Protokoll. Die TLV-Objekte (Type-Length-Value) werden im Tunnel verwendet, um authentifizierungsbezogene Daten zwischen dem EAP-Peer und dem EAP-Server zu übertragen.

Microsoft hat die Unterstützung für TEAP in der Version Windows 10 2004 eingeführt, die im Mai 2020 veröffentlicht wurde.

Die EAP-Verkettung ermöglicht die Benutzer- und Geräteauthentifizierung innerhalb einer EAP/Radius-Sitzung anstelle von zwei separaten Sitzungen.

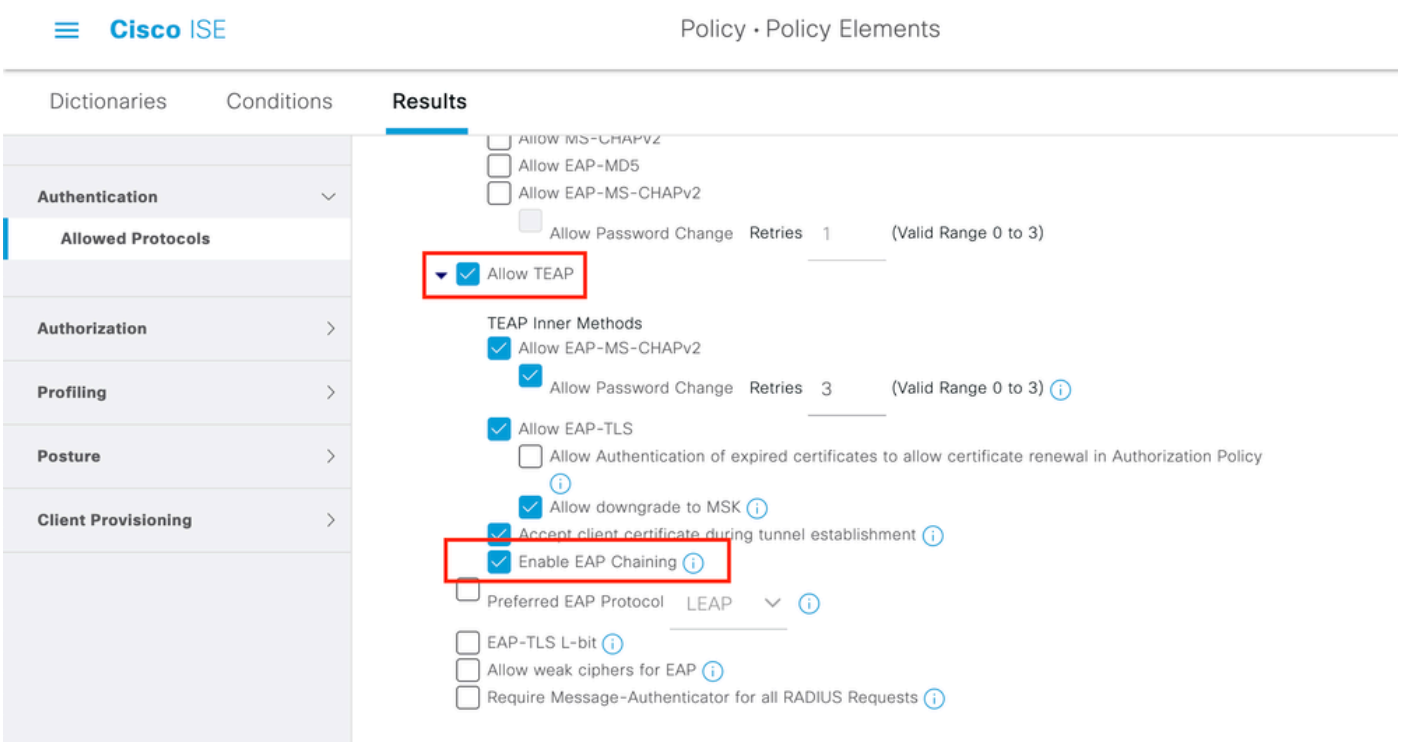
Bisher war hierzu das Cisco AnyConnect NAM-Modul erforderlich, und EAP-FAST wurde auf der Windows-Komponente verwendet, da diese von der nativen Windows-Komponente nicht unterstützt wird. Jetzt können Sie die Windows Native Supplicant verwenden, um die EAP-Verkettung mit ISE 2.7 mithilfe von TEAP durchzuführen.

Konfigurieren

Konfiguration der Cisco ISE

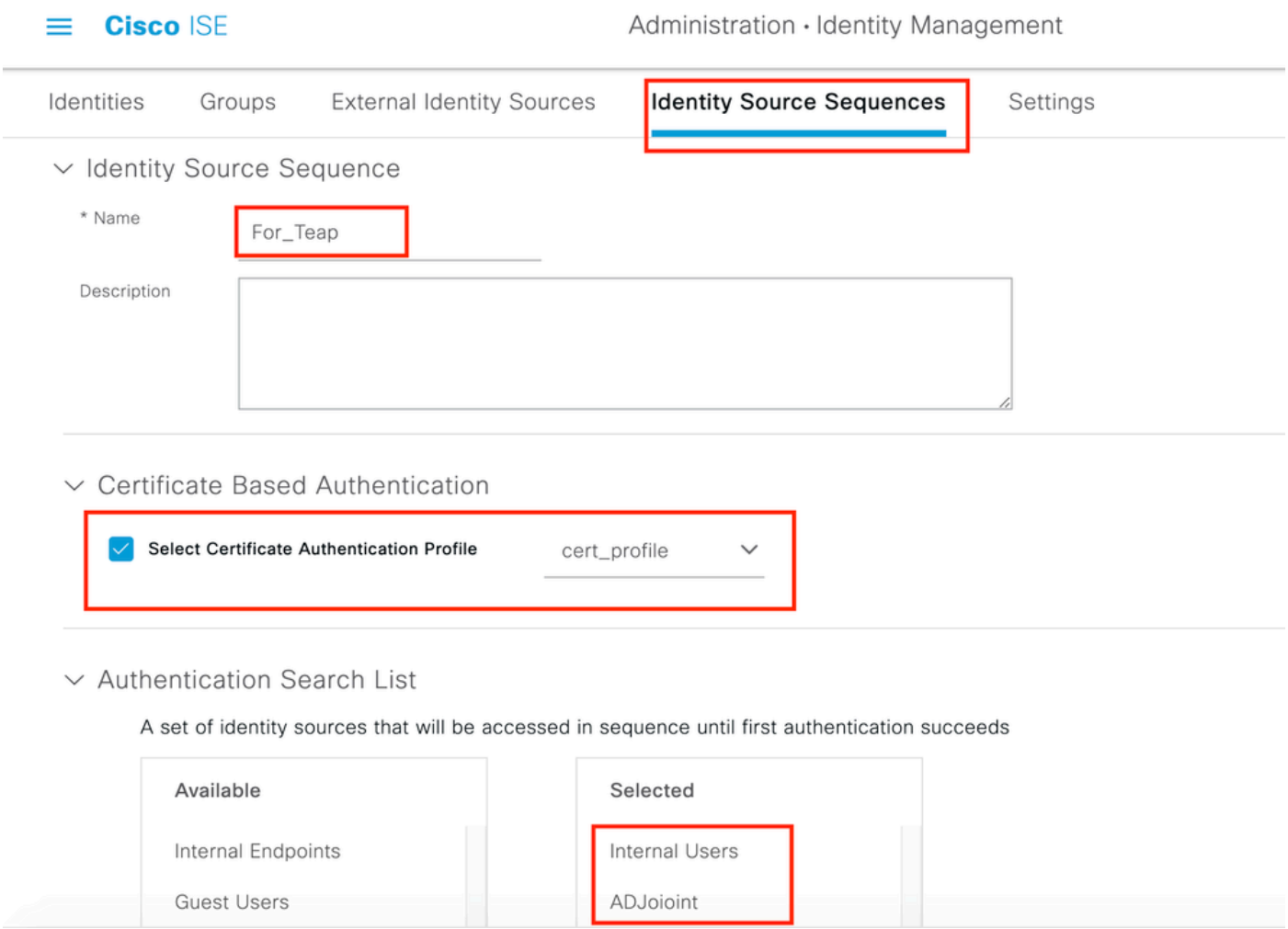
Schritt 1: Sie müssen die zulässigen Protokolle bearbeiten, um die TEAP- und EAP-Verkettung zu aktivieren.

Navigieren Sie zu **ISE > Policy > Policy Elements > Results > Authentication > Allowed Protocols > Add New** . Aktivieren Sie die Kontrollkästchen TEAP- und EAP-Verkettung.



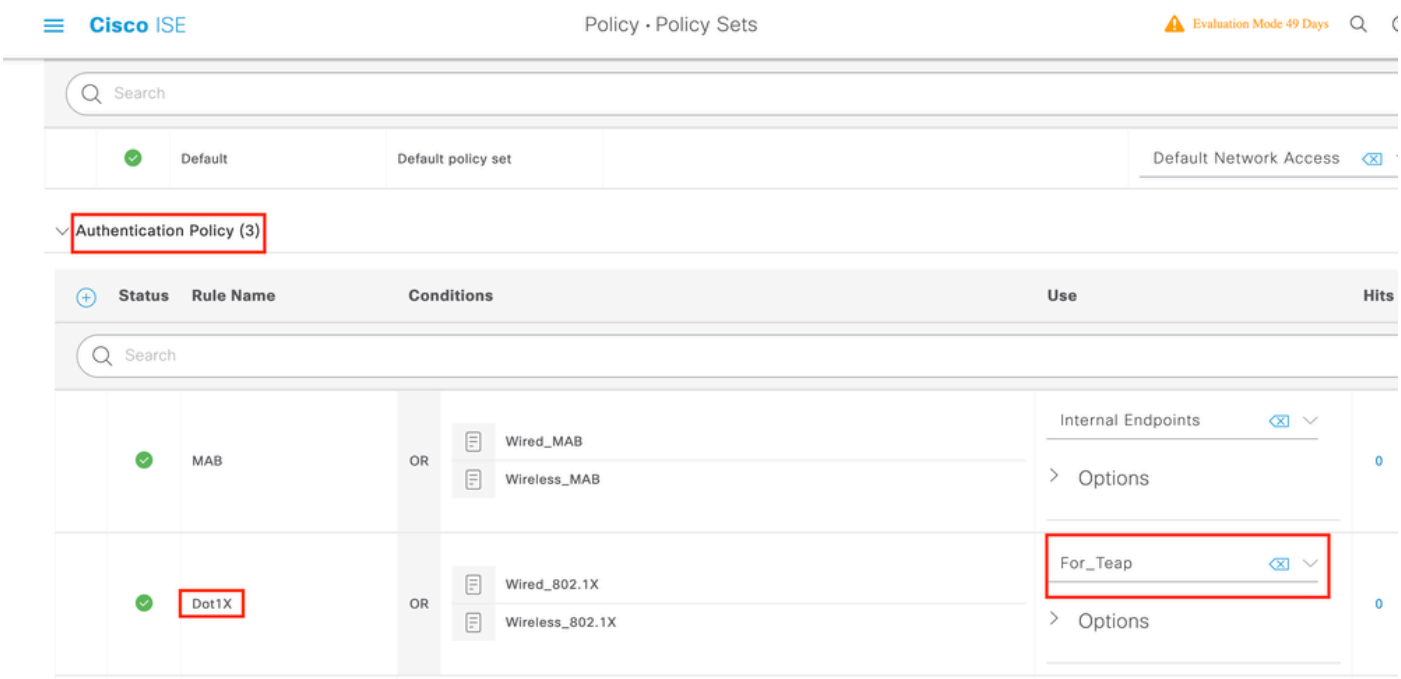
Schritt 2: Erstellen Sie ein Zertifikatprofil, und fügen Sie es der Identitätsquellensequenz hinzu.

Navigieren Sie zu **ISE > Administration > Identities > identity Source Sequence** und wählen Sie das Zertifikatprofil aus.



Schritt 3: Sie müssen diese Sequenz in der Authentifizierungsrichtlinie aufrufen.

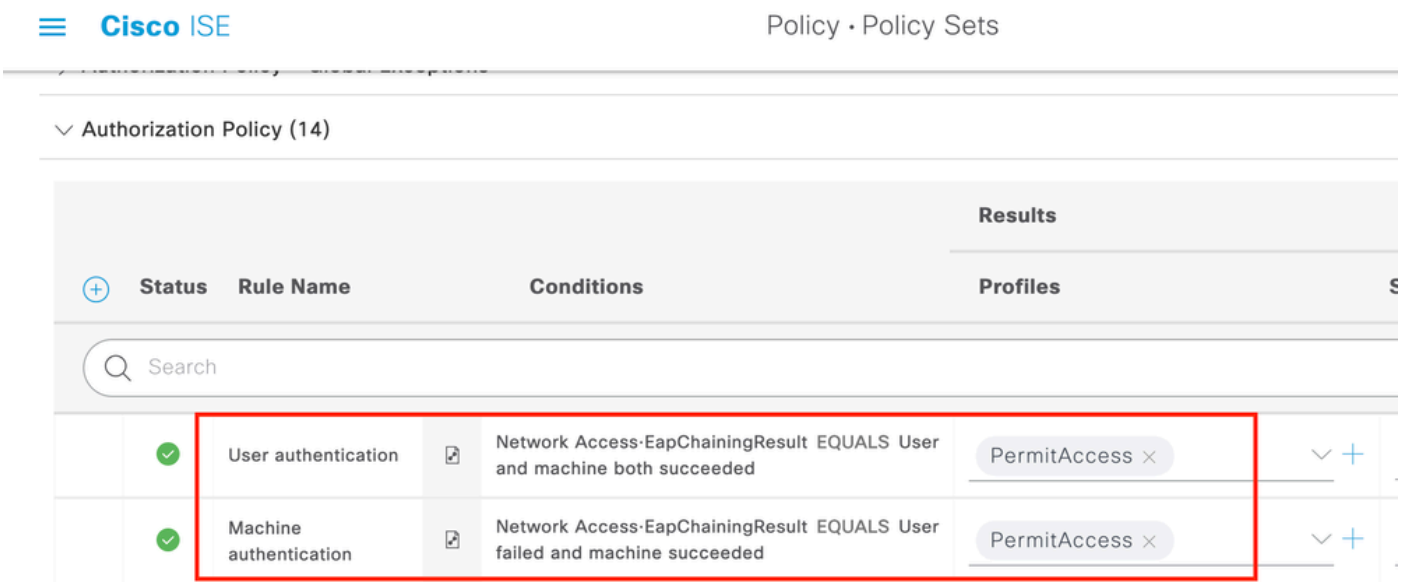
Navigieren Sie zu ISE > Policy > Policy Sets . Choose the Policy Set for Dot1x > Authentication Policy und wählen Sie die in Schritt 2 erstellte Identitätsquellensequenz aus.



Schritt 4: Nun müssen Sie die Autorisierungsrichtlinie unter dem Punkt1x-Richtliniensatz ändern.

Navigieren Sie zu **ISE > Policy > Policy Sets . Choose the Policy Set for Dot1x > Authentication Policy .**

Sie müssen zwei Regeln erstellen. Die erste Regel überprüft, ob der Computer authentifiziert ist, der Benutzer jedoch nicht. Mit der zweiten Regel wird überprüft, ob Benutzer und Computer authentifiziert sind.



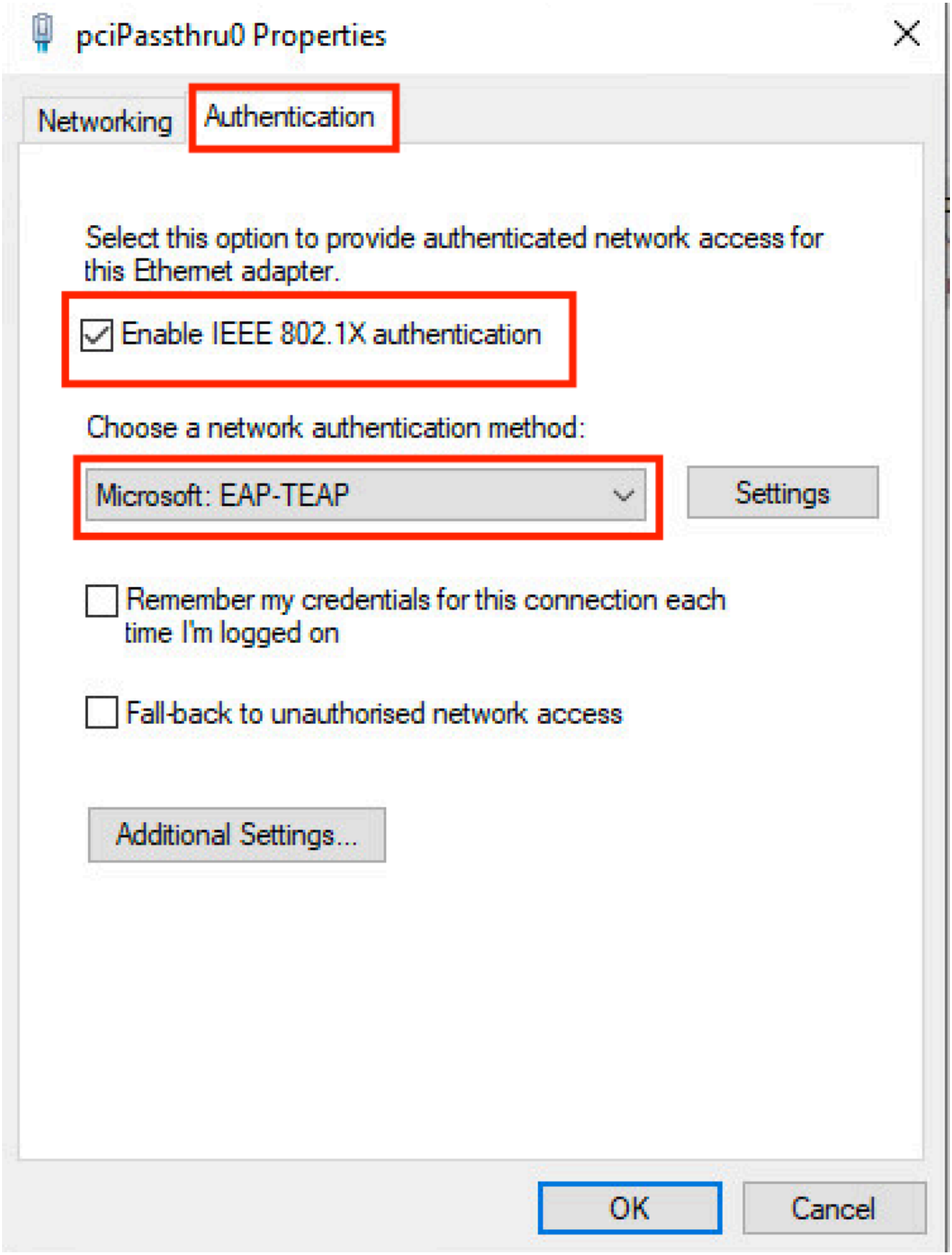
Damit ist die ISE-Serverkonfiguration abgeschlossen.

Konfiguration der nativen Windows-Komponente

Konfigurieren Sie die Einstellungen für die kabelgebundene Authentifizierung in diesem Dokument.

Navigieren Sie zu Control Panel > Network and Sharing Center > Change Adapter Settings und mit der rechten Maustaste auf **LAN Connection > Properties**. Klicken Sie auf **Authentication** aus.

Schritt 1: Klicken Sie Authentication Dropdown-Liste und wählen Microsoft EAP-TEAP.



Schritt 2: Klicken Sie auf Settings -Taste neben TEAP.

1. Beibehalten Enable Identity Privacy aktiviert mit anonymous als Identität.
2. Setzen Sie ein Häkchen neben den Stammzertifizierungsstellenservern unter Vertrauenswürdige Stammzertifizierungsstellen, die verwendet werden, um das Zertifikat für die EAP-Authentifizierung auf dem ISE PSN zu signieren.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.