EAP Chaining met TEAP

Inhoud

Inleiding

In dit document wordt beschreven hoe u ISE en Windows plug-in kunt configureren voor EAP-koppeling (Extensible Verification Protocol) met behulp van Tunnel-gebaseerde Extensible Verification Protocol (TEAP).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ISE
- Configuratie van Windows-applicator

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ISE versie 3.0
- Windows 10 build 2004
- Kennis van protocol TEAP

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

TEAP is een tunnelgebaseerde Extensible Verification Protocol-methode die een beveiligde tunnel tot stand brengt en andere EAP-methoden uitvoert onder de bescherming van die beveiligde tunnel.

De TEAP-verificatie vindt in twee fasen plaats na de eerste EAP-identiteitsaanvraag/reactieuitwisseling.

In de eerste fase gebruikt TEAP de TLS handshake om een geauthenticeerde sleuteluitwisseling te bieden en een beschermde tunnel tot stand te brengen. Wanneer de tunnel eenmaal tot stand is gebracht, begint de tweede fase met de peer en voert de server verdere gesprekken om het vereiste authenticatie- en autorisatiebeleid vast te stellen.

Cisco ISE 2.7 en hoger ondersteunt het TEAP-protocol. De TLV-objecten (type-length-value) worden binnen de tunnel gebruikt om verificatiegerelateerde gegevens te transporteren tussen de EAP-peer en de EAP-server.

Microsoft introduceerde de ondersteuning voor TEAP in de versie Windows 10 2004 die in mei 2020 werd uitgebracht.

EAP-koppeling maakt verificatie van gebruiker en machine mogelijk binnen één EAP/Radius-sessie in plaats van twee afzonderlijke sessies.

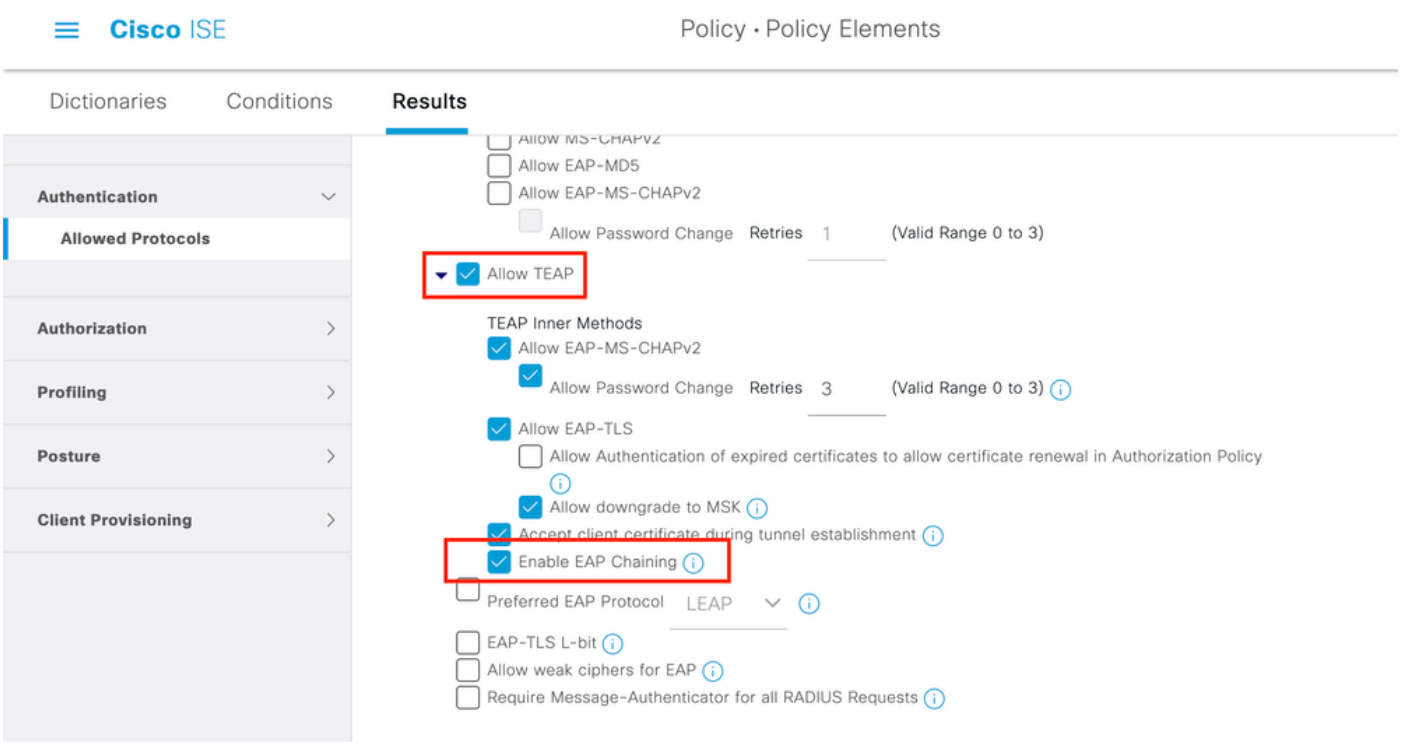
Eerder had u hiervoor de Cisco AnyConnect NAM-module nodig en gebruikte u EAP-FAST op de Windows-applicatie omdat de native Windows-applicatie dit niet ondersteunde. Nu kunt u de Windows Native Supplicant gebruiken om EAP Chaining uit te voeren met ISE 2.7 met het gebruik van TEAP.

Configureren

Cisco ISE-configuratie

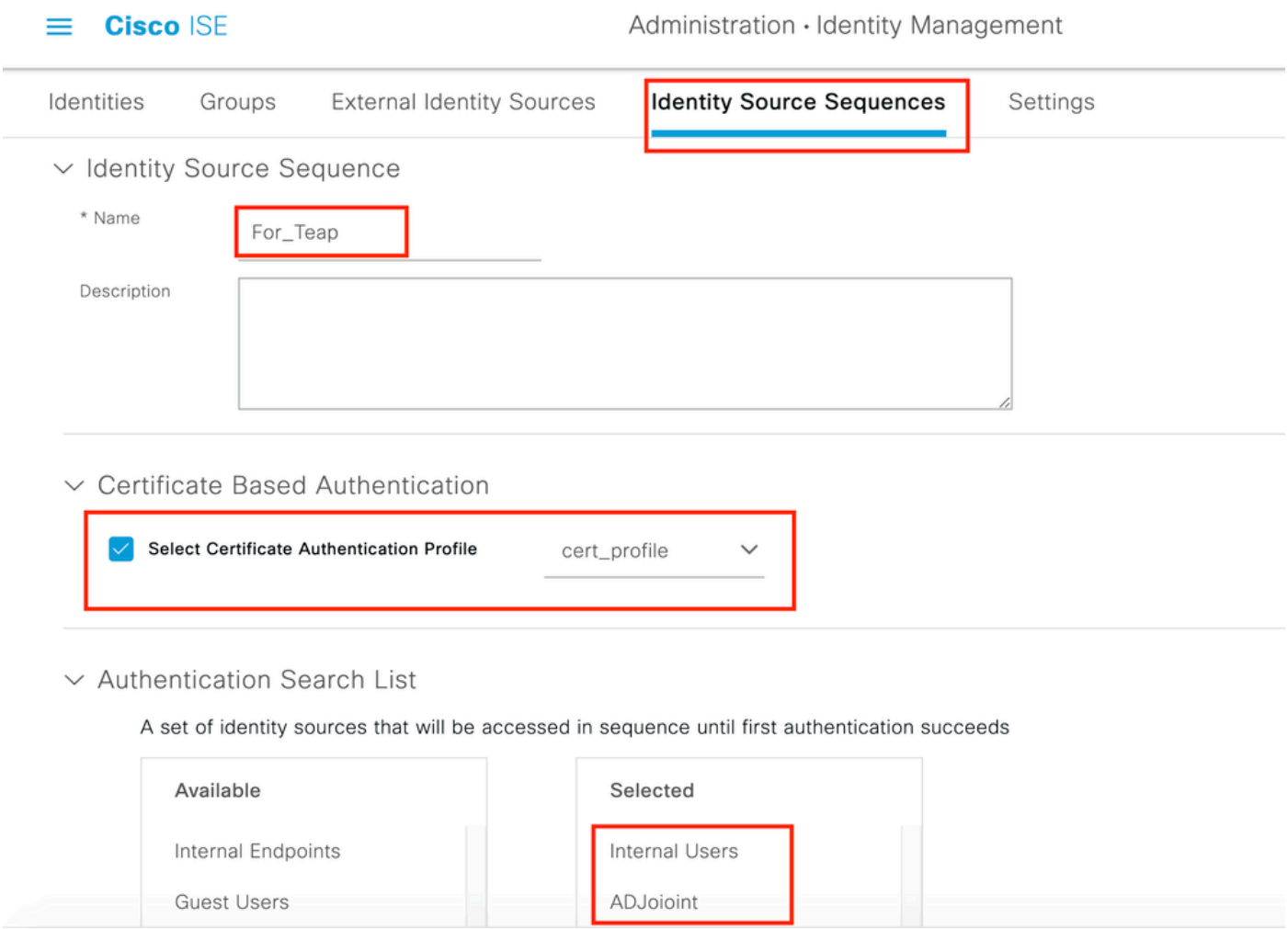
Stap 1. U moet de Toegestane protocollen bewerken om TEAP en EAP Chaining in te schakelen.

Naar navigeren **ISE > Policy > Policy Elements > Results > Authentication > Allowed Protocols > Add New** . Schakel de selectievakjes TEAP en EAP-koppeling in.



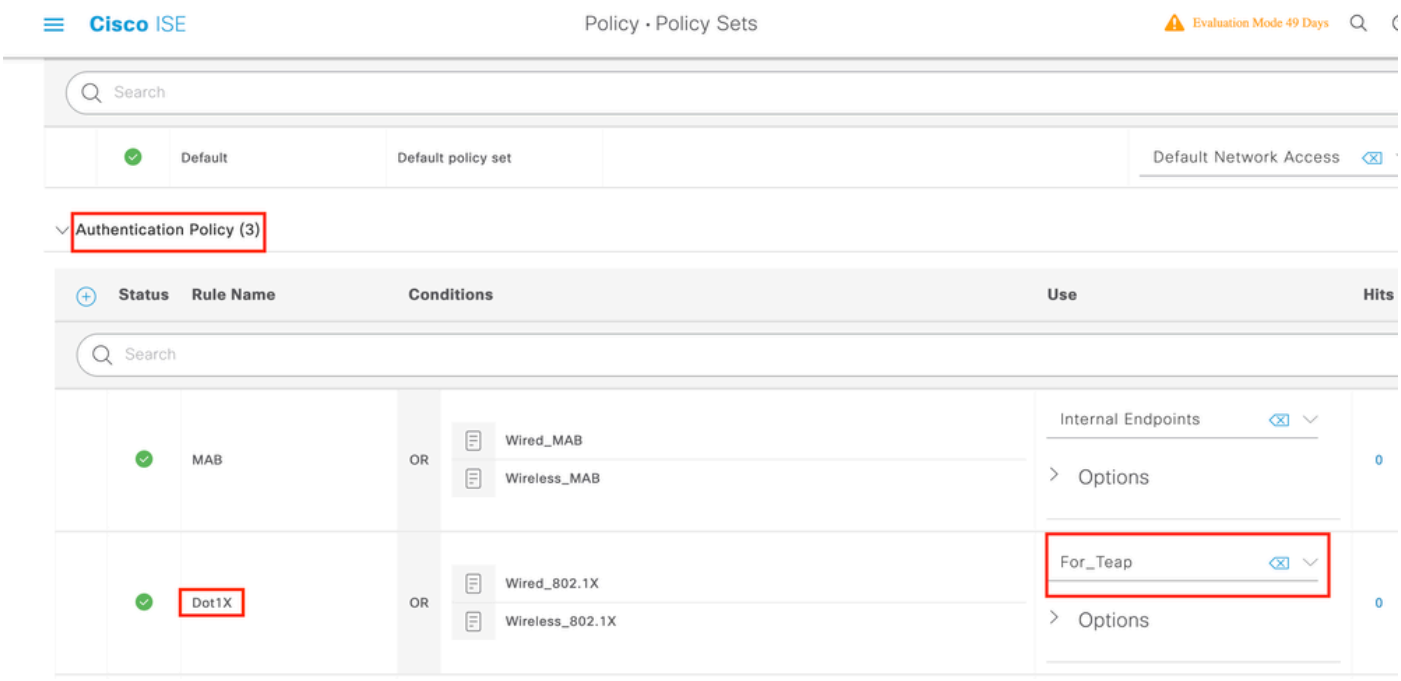
Stap 2. Maak een certificaatprofiel en voeg het toe aan de Identity Source Sequence.

Naar navigeren **ISE > Administration > Identities > identity Source Sequence** en kies het certificaatprofiel.



Stap 3. U moet deze volgorde aanroepen in het verificatiebeleid.

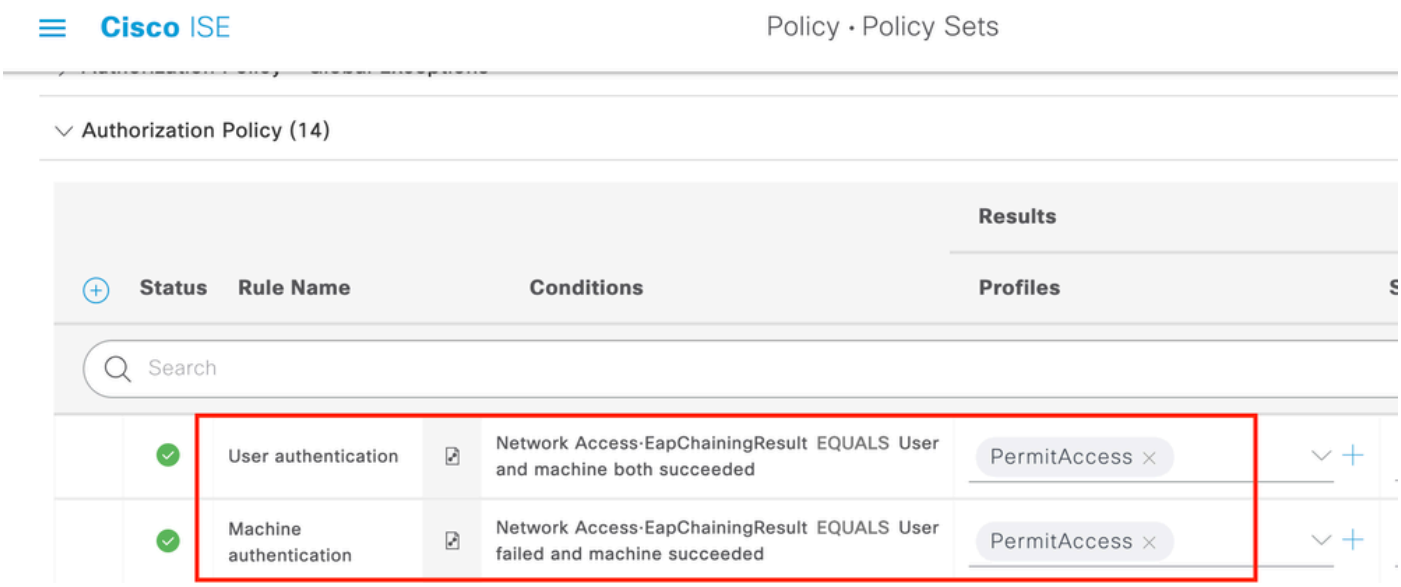
Naar navigeren ISE > Policy > Policy Sets . Choose the Policy Set for Dot1x > Authentication Policy en kies de volgorde van de identiteitsbron die in Stap 2 is gemaakt.



Stap 4. U moet nu het autorisatiebeleid wijzigen onder de Dot1x Policy Set.

Naar navigeren **ISE > Policy > Policy Sets . Choose the Policy Set for Dot1x > Authentication Policy .**

Je moet twee regels maken. De eerste regel controleert of de machine geauthenticeerd is maar de gebruiker niet. De tweede regel verifieert dat zowel de gebruiker als de machine zijn geverifieerd.



Hiermee is de configuratie aan de kant van de ISE-server voltooid.

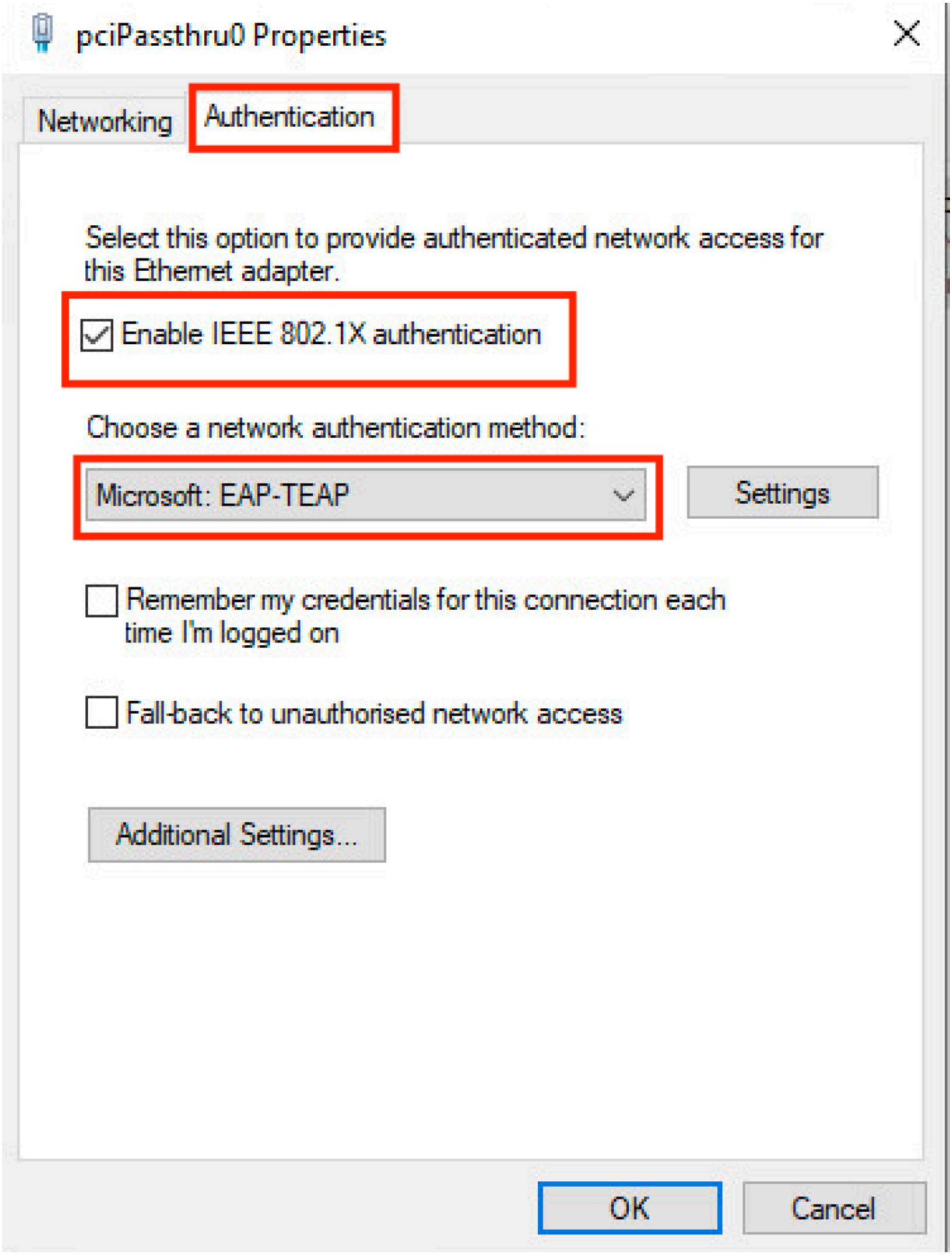
Configuratie van Windows-native applicatie

Configureer de instelling voor bekabelde verificatie in dit document.

Naar navigeren Control Panel > Network and Sharing Center > Change Adapter Settings en klik met de

rechtermuisknop op **LAN Connection > Properties**. Klik op de **Authentication** tabblad.

Stap 1. Klik op Authentication vervolgkeuzelijst en kies Microsoft EAP-TEAP.



Stap 2. Klik op de **Settings** knop naast TEAP.

1. behouden Enable Identity Privacy ingeschakeld met anonymous als identiteit.
2. Schakel een selectieteken in naast de CA-basisserver(s) onder Trusted Root-certificeringsinstanties die worden gebruikt om het certificaat voor EAP-verificatie te ondertekenen op de ISE-netwerkmodule.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.