EAP Chaining with TEAP

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Background Information](#)
[Configure](#)
[Cisco ISE Configuration](#)
[Windows Native Supplicant Configuration](#)
[Verify](#)
[Detailed Authentication Report](#)
[Machine Authentication](#)
[User and Machine Authentication](#)
[Troubleshoot](#)
[Live Log Analysis](#)
[Machine Authentication](#)
[User and Machine Authentication](#)
[Related Information](#)

Introduction

This document describes how to configure ISE and Windows supplicant for Extensible Authentication Protocol (EAP) Chaining with Tunnel-based Extensible Authentication Protocol (TEAP).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- ISE
- Configuration of windows supplicant

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ISE version 3.0
- Windows 10 build 2004
- Knowledge of protocol TEAP

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

TEAP is a tunnel-based Extensible Authentication Protocol method that establishes a secure tunnel and executes other EAP methods under the protection of that secured tunnel.

TEAP authentication occurs in two phases after the initial EAP identity request/response exchange.

In the first phase, TEAP uses the TLS handshake to provide an authenticated key exchange and to establish a protected tunnel. Once the tunnel is established, the second phase begins with the peer and the server engages in further conversation to establish the required authentications and authorization policies.

Cisco ISE 2.7 and later supports the TEAP Protocol. The type-length-value (TLV) objects are used within the tunnel to transport authentication-related data between the EAP peer and the EAP server.

Microsoft introduced the support for TEAP in the version Windows 10 2004 released in MAY 2020.

EAP chaining allows the user and machine authentication within one EAP/Radius session instead of two separate sessions.

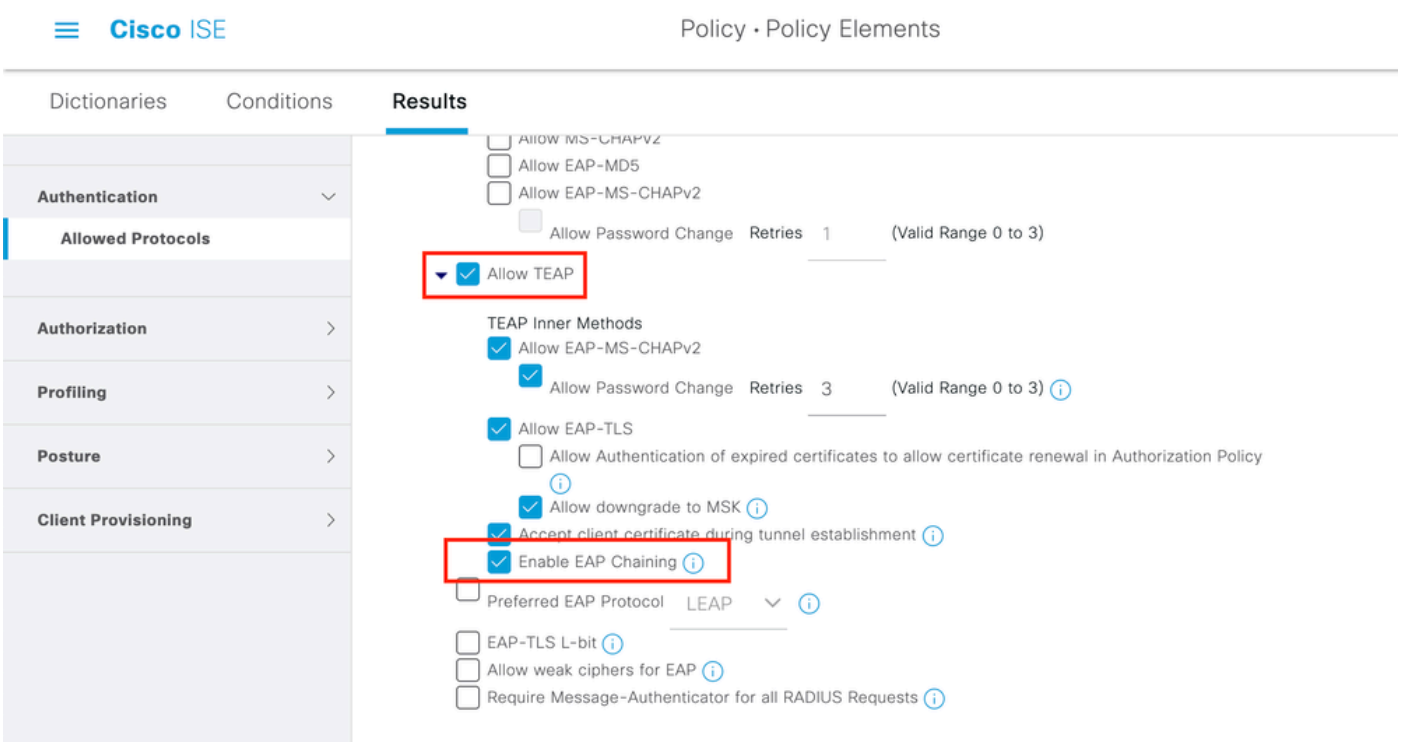
Previously, to achieve this you needed the Cisco AnyConnect NAM module and use EAP-FAST on the windows supplicant as the native Windows supplicant did not support this. Now, you can use the Windows Native Supplicant to perform EAP Chaining with ISE 2.7 with the use of TEAP.

Configure

Cisco ISE Configuration

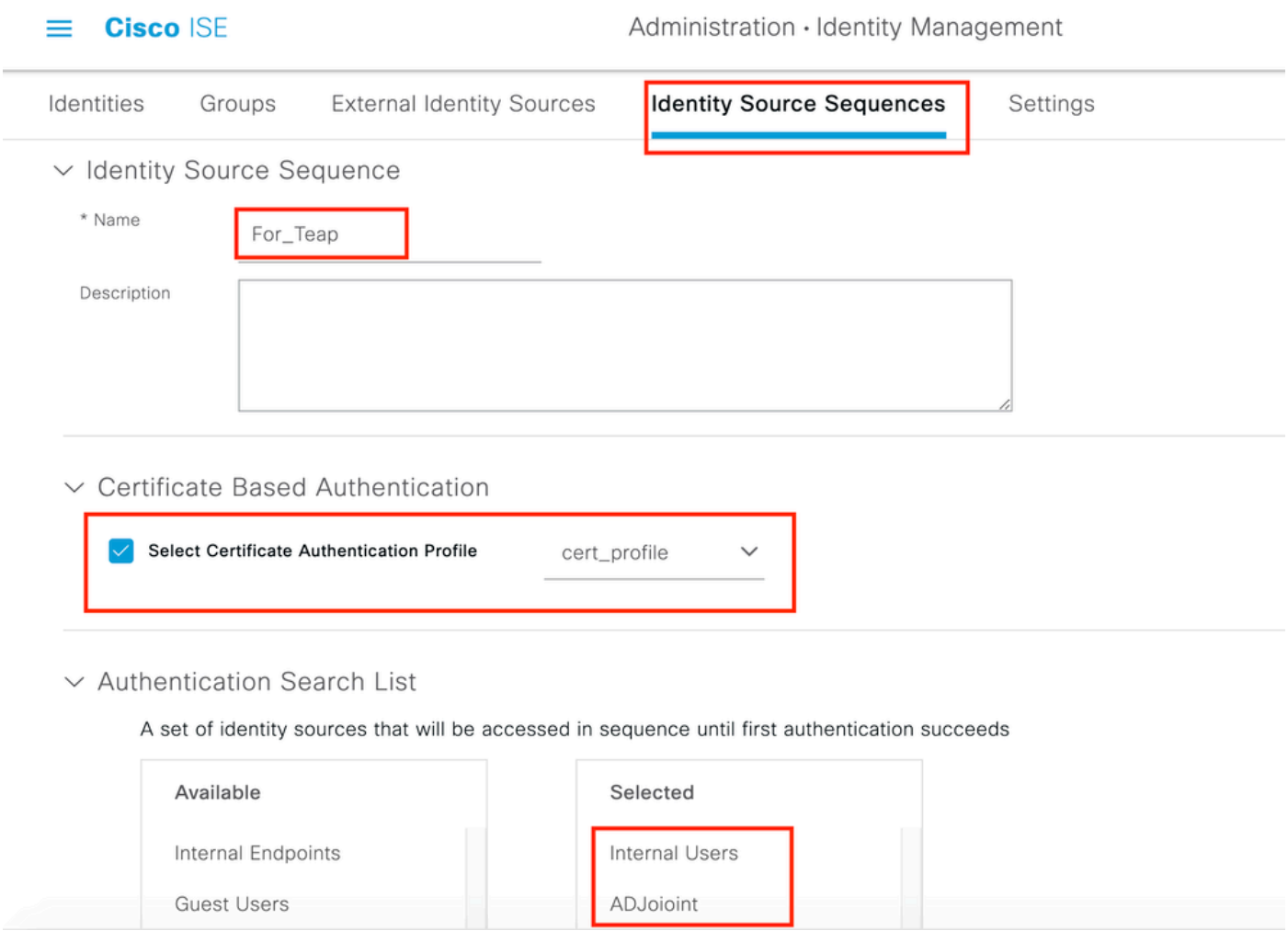
Step 1. You need to edit the Allowed Protocols to enable TEAP and EAP Chaining.

Navigate to **ISE > Policy > Policy Elements > Results > Authentication > Allowed Protocols > Add New** . Check the TEAP and EAP chaining check boxes.



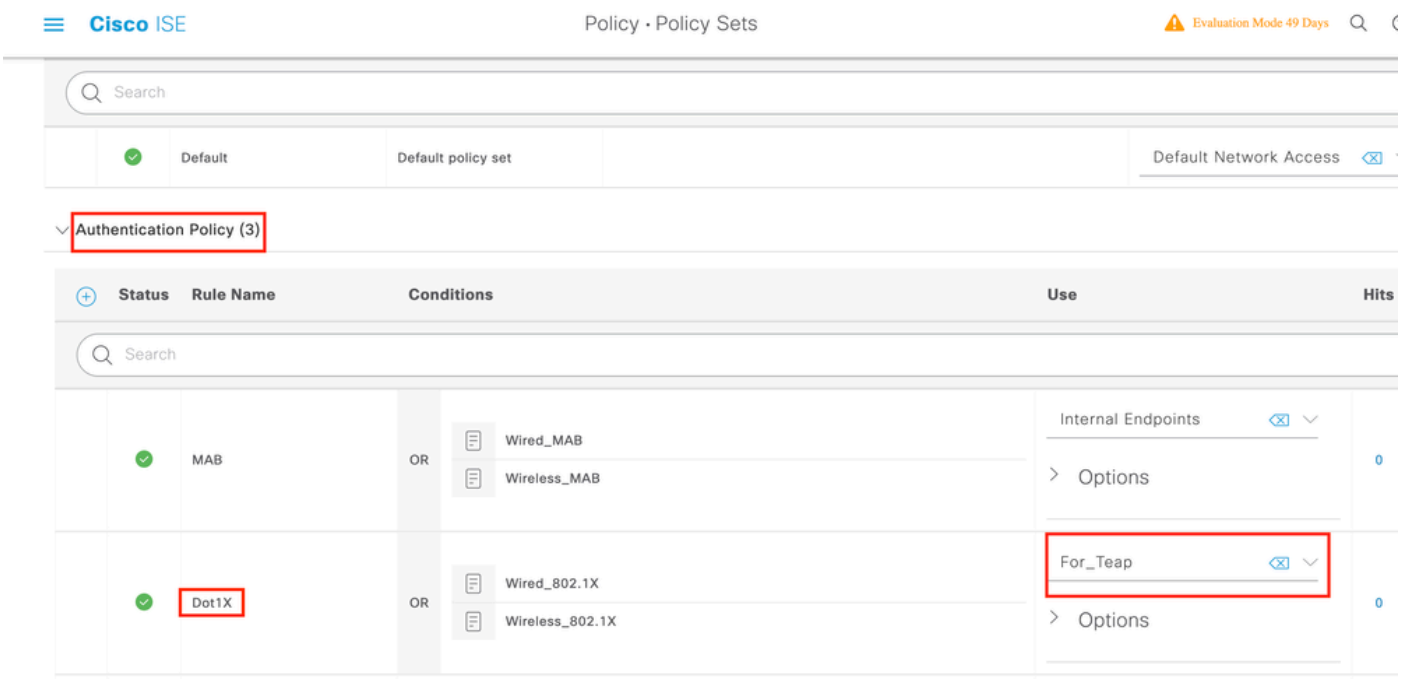
Step 2. Create a certificate profile and add it to the Identity Source Sequence.

Navigate to **ISE > Administration > Identities > identity Source Sequence** and choose the certificate Profile.



Step 3. You need to call this sequence in the Authentication Policy.

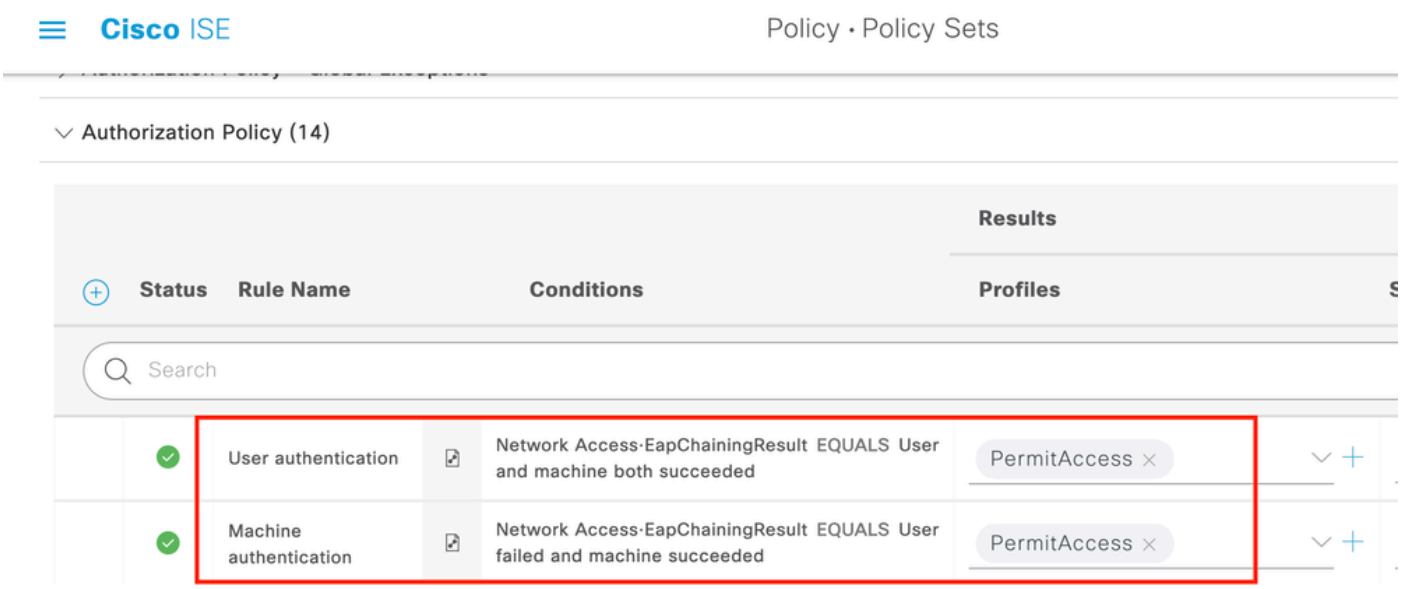
Navigate to ISE > Policy > Policy Sets . Choose the Policy Set for Dot1x > Authentication Policy and choose the Identity source sequence created in Step 2.



Step 4. Now you need to modify the Authorization Policy under the Dot1x Policy Set.

Navigate to **ISE > Policy > Policy Sets . Choose the Policy Set for Dot1x > Authentication Policy .**

You need to create two rules. The first rule checks that the machine is authenticated but the user is not. The second rule verifies that both the user and the machine are authenticated.



This completes the configuration from the ISE Server side.

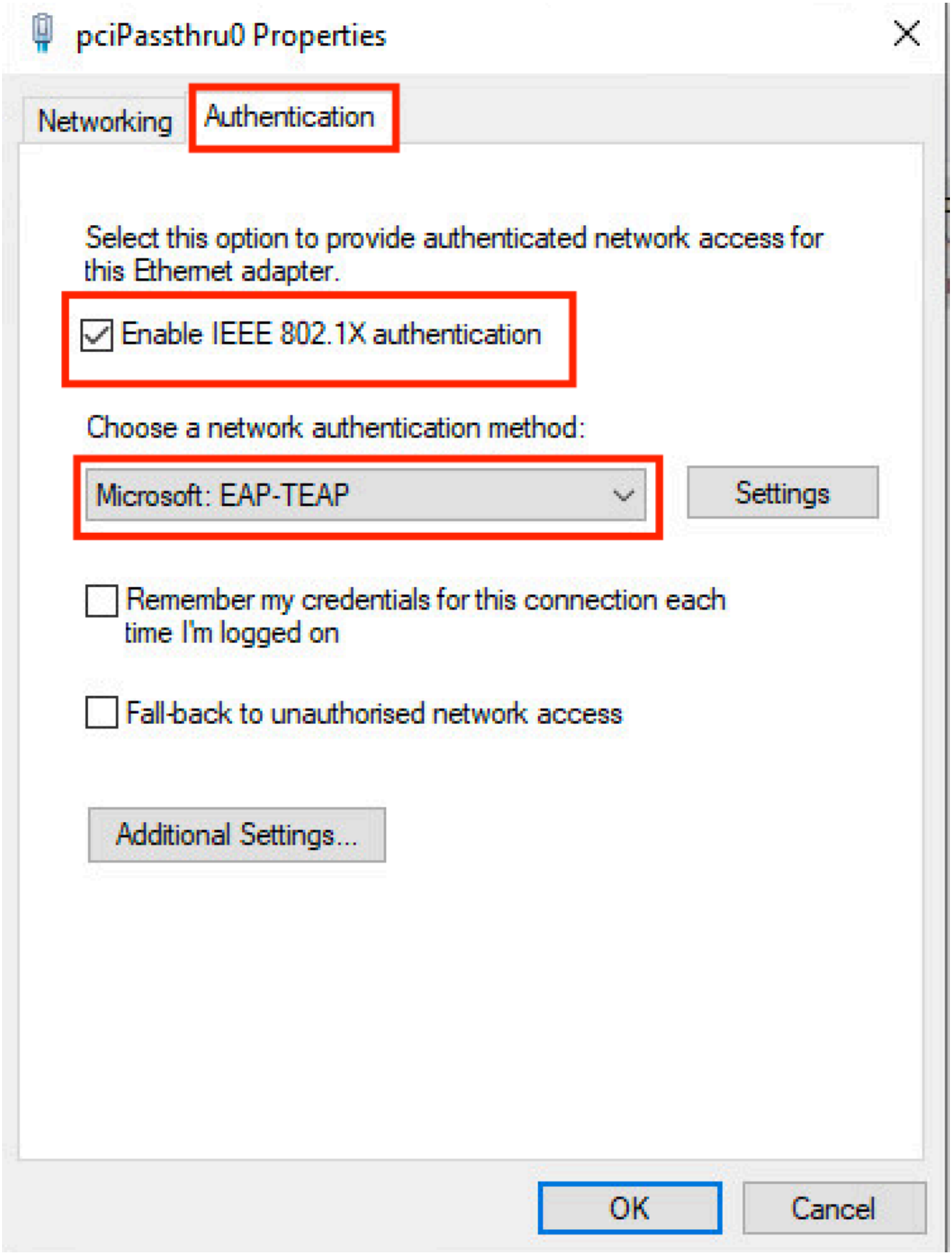
Windows Native Supplicant Configuration

Configure the wired authentication setting in this document.

Navigate to Control Panel > Network and Sharing Center > Change Adapter Settings and right-click on **LAN**

Connection > Properties. Click on the **Authentication** tab.

Step 1. Click on Authentication drop-down and choose Microsoft EAP-TEAP.



Step 2. Click the **Settings** button next to TEAP.

1. Keep Enable Identity Privacy enabled with anonymous as the identity.
2. Put a checkmark next to the root CA server(s) under Trusted Root Certification Authorities that are used to sign the certificate for EAP authentication on the ISE PSN.