Concatenamento EAP con TEAP

Sommario

Introduzione

In questo documento viene descritto come configurare ISE e Windows supplicant per il concatenamento EAP (Extensible Authentication Protocol) con TEAP (Tunnel-Based Extensible Authentication Protocol).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- ISE
- Configurazione del supplicant di Windows

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ISE versione 3.0
- Windows 10 build 2004
- Conoscenza del protocollo TEAP

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

TEAP è un metodo EAP (Extensible Authentication Protocol) basato su tunnel che stabilisce un tunnel sicuro ed esegue altri metodi EAP sotto la protezione di tale tunnel protetto.

L'autenticazione TEAP si verifica in due fasi dopo lo scambio iniziale di richiesta/risposta di identità EAP.

Nella prima fase, TEAP utilizza l'handshake TLS per fornire uno scambio di chiavi autenticato e per stabilire un tunnel protetto. Una volta stabilito il tunnel, la seconda fase inizia con il peer e il server avvia un'ulteriore conversazione per stabilire le autenticazioni e i criteri di autorizzazione necessari.

Cisco ISE 2.7 e versioni successive supportano il protocollo TEAP. Gli oggetti TLV (Type-Length-Value) vengono utilizzati all'interno del tunnel per trasportare i dati relativi all'autenticazione tra il peer EAP e il server EAP.

Microsoft ha introdotto il supporto per TEAP nella versione Windows 10 2004 rilasciata a MAGGIO 2020.

Il concatenamento EAP consente l'autenticazione dell'utente e del computer all'interno di una sessione EAP/Radius anziché in due sessioni separate.

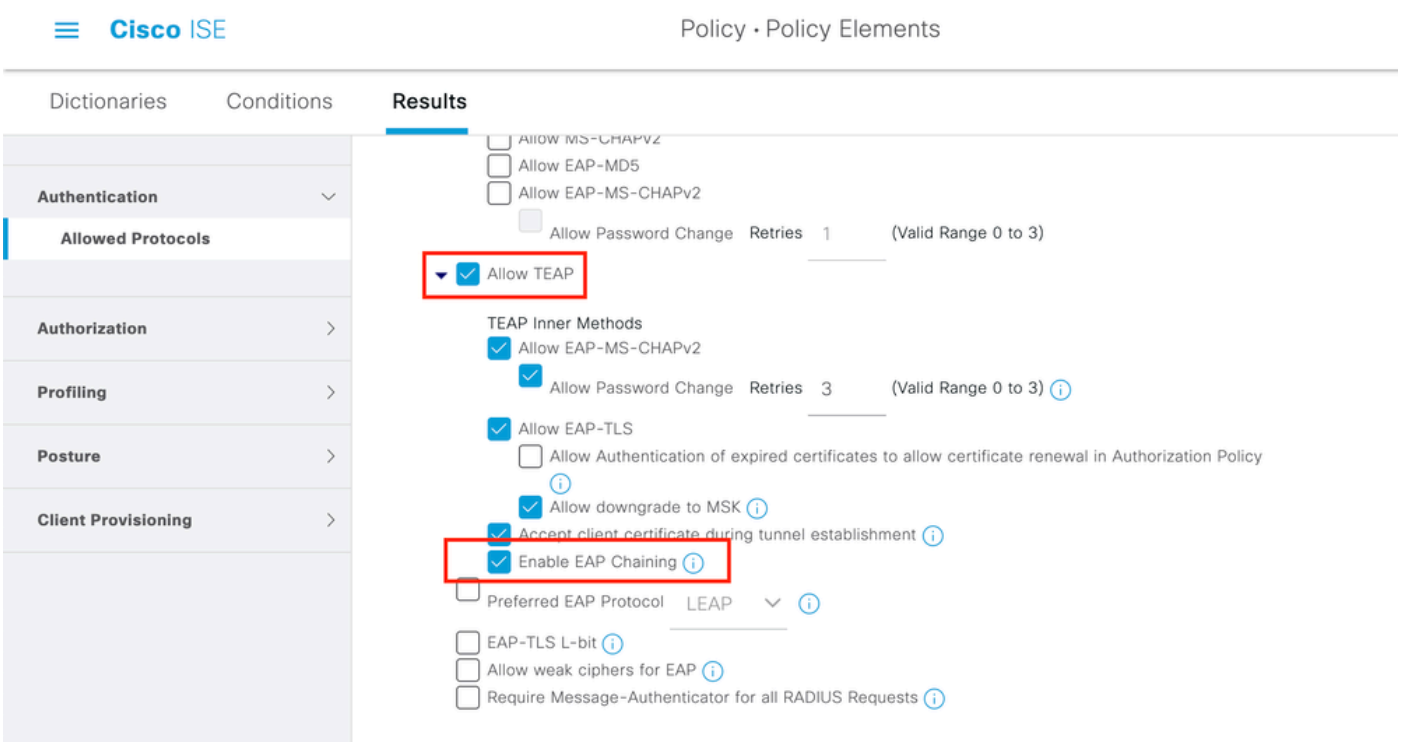
In precedenza, per ottenere questo risultato, era necessario usare il modulo Cisco AnyConnect NAM e usare EAP-FAST sui sistemi Windows supplicant, in quanto il sistema Windows supplicant nativo non lo supportava. È ora possibile utilizzare Windows Native Supplicant per eseguire il concatenamento EAP con ISE 2.7 utilizzando TEAP.

Configurazione

Cisco ISE Configuration

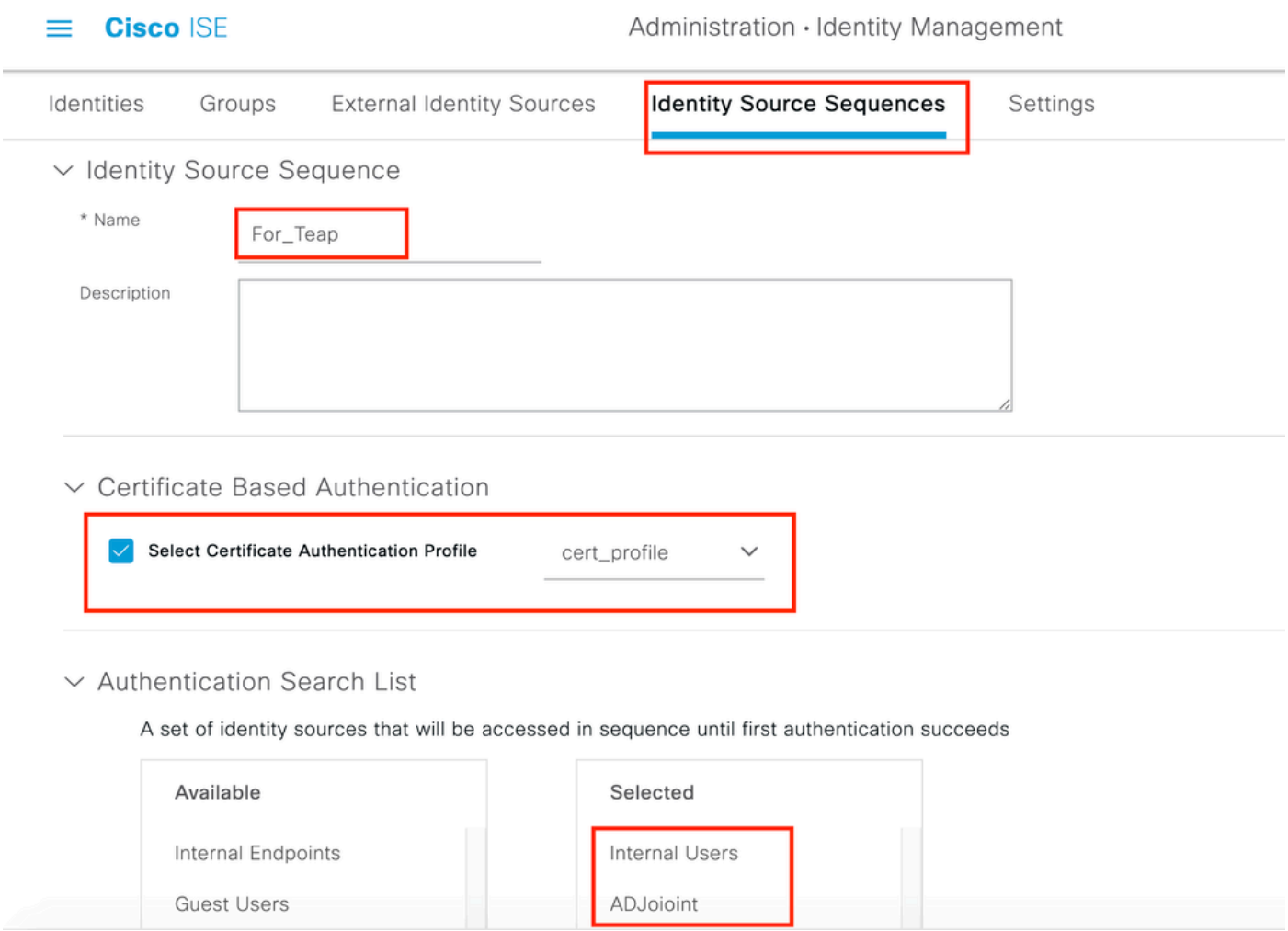
Passaggio 1. È necessario modificare i Protocolli consentiti per abilitare il concatenamento TEAP ed EAP.

Passa a **ISE > Policy > Policy Elements > Results > Authentication > Allowed Protocols > Add New** . Selezionare le caselle di controllo TEAP ed EAP chaining.



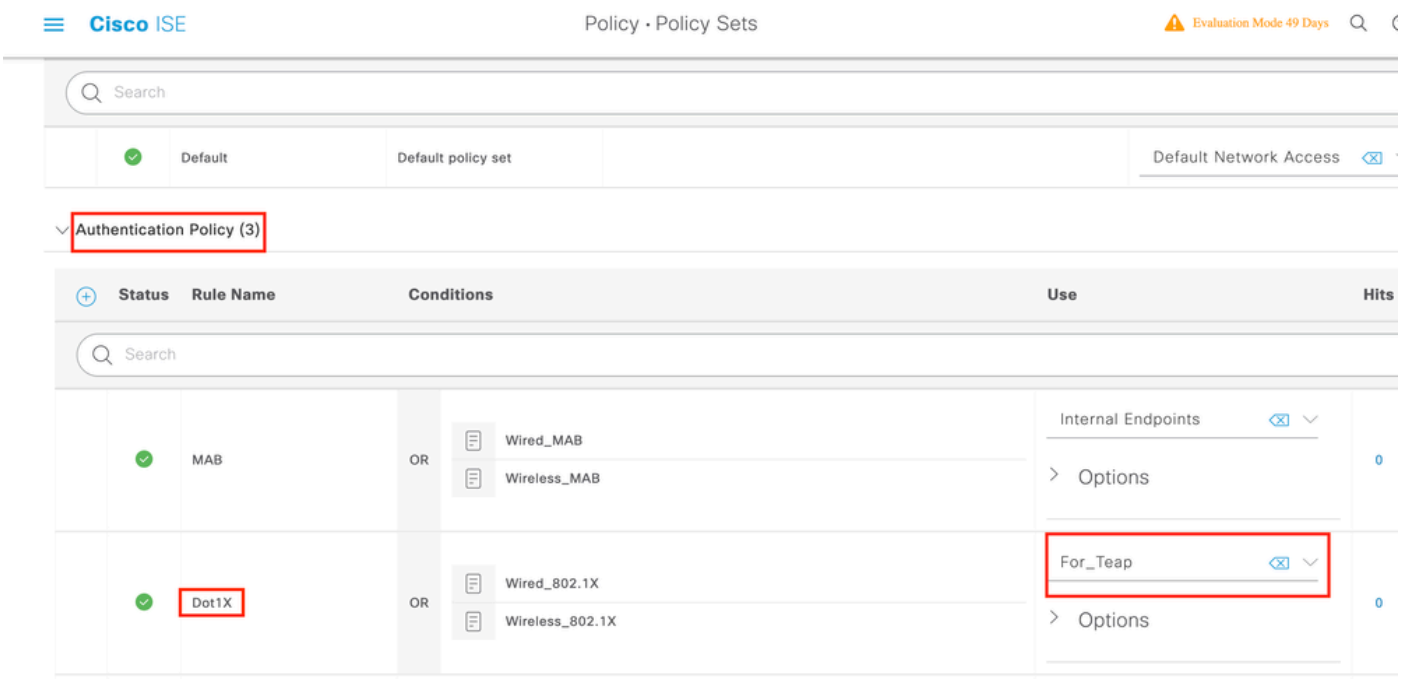
Passaggio 2. Creare un profilo di certificato e aggiungerlo alla sequenza Origine identità.

Passa a **ISE > Administration > Identities > identity Source Sequence** e scegliere il profilo del certificato.



Passaggio 3. È necessario chiamare questa sequenza nei criteri di autenticazione.

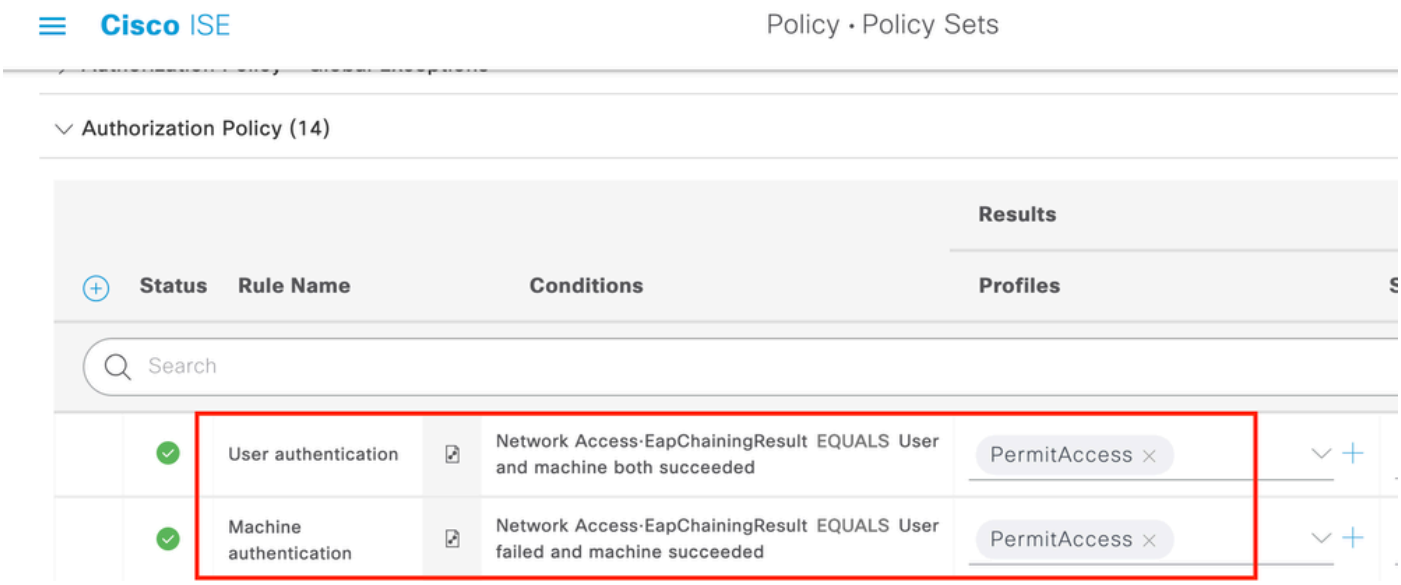
Passa a ISE > Policy > Policy Sets . Choose the Policy Set for Dot1x > Authentication Policy e scegliere la sequenza di origine Identità creata al passo 2.



Passaggio 4. A questo punto è necessario modificare i criteri di autorizzazione nel set di criteri Dot1x.

Passa a **ISE > Policy > Policy Sets . Choose the Policy Set for Dot1x > Authentication Policy** .

Ènecessario creare due regole. La prima regola verifica che il computer sia autenticato, ma l'utente non lo è. La seconda regola verifica che l'utente e il computer siano autenticati.



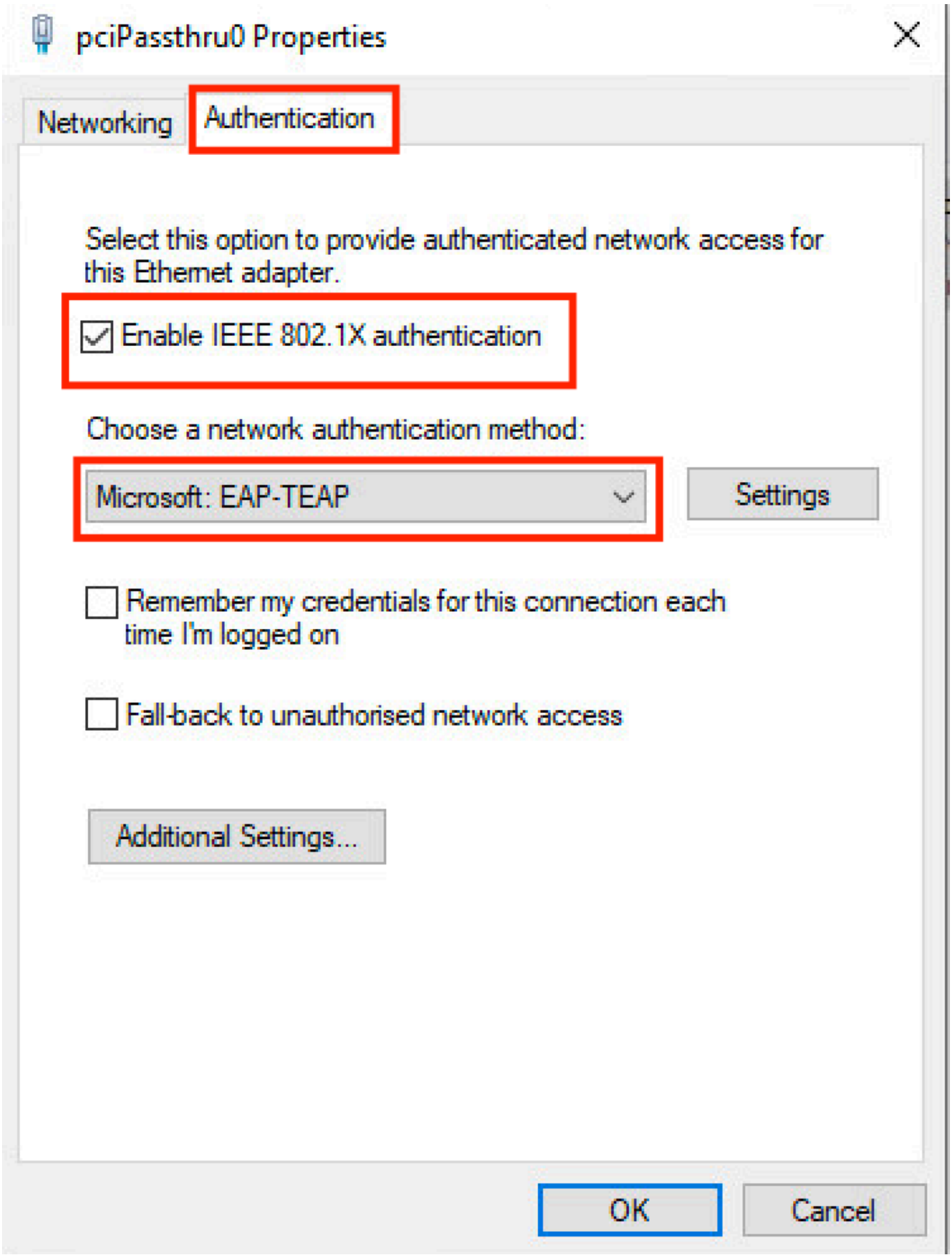
La configurazione è completata dal lato server ISE.

Configurazione supplicant nativo di Windows

Configurare l'impostazione di autenticazione della rete cablata in questo documento.

Passa a Control Panel > Network and Sharing Center > Change Adapter Settings e fare clic con il pulsante destro del mouse su **LAN Connection > Properties**. Fare clic sul pulsante **Authentication** scheda.

Passaggio 1. Fare clic su Authentication e scegliere Microsoft EAP-TEAP.



Passaggio 2. Fare clic sul pulsante **Settings** accanto a TEAP.

1. Mantieni Enable Identity Privacy abilitato con anonymous come identità.
2. Selezionare i server CA radice sotto Autorità di certificazione radice attendibili utilizzati per firmare il certificato per l'autenticazione EAP sul numero di serie del servizio (PSN) ISE.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).