Configuración del encadenamiento de EAP con TEAP

Contenido

Introducción

Este documento describe cómo configurar ISE y el suplicante de Windows para el encadenamiento de protocolo de autenticación extensible (EAP) con TEAP.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- ISE
- Configuración del solicitante de Windows

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ISE versión 3.0
- Windows 10 build 2004
- Conocimiento del protocolo Protocolo de autenticación extensible basado en túneles (TEAP)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

TEAP es un método de protocolo de autenticación extensible basado en túnel que establece un túnel seguro y ejecuta otros métodos EAP bajo la protección de ese túnel seguro.

La autenticación del GETE ocurre en dos fases después del intercambio de solicitud/respuesta de identidad EAP inicial. En la primera fase, el GETE utiliza el intercambio de señales TLS para proporcionar un intercambio de claves autenticado y establecer un túnel protegido. Una vez que se establece el túnel, la segunda fase comienza con el par y el servidor participando en una conversación adicional para establecer las políticas de autenticación y autorización requeridas.

Cisco ISE 2.7 y versiones posteriores admiten el protocolo TEAP. Los objetos tipo-longitud-valor (TLV) se utilizan dentro del túnel para transportar datos relacionados con la autenticación entre el par EAP y el servidor EAP.

Microsoft introdujo la compatibilidad con el GETE en la versión de Windows 10 2004, publicada en mayo de 2020.

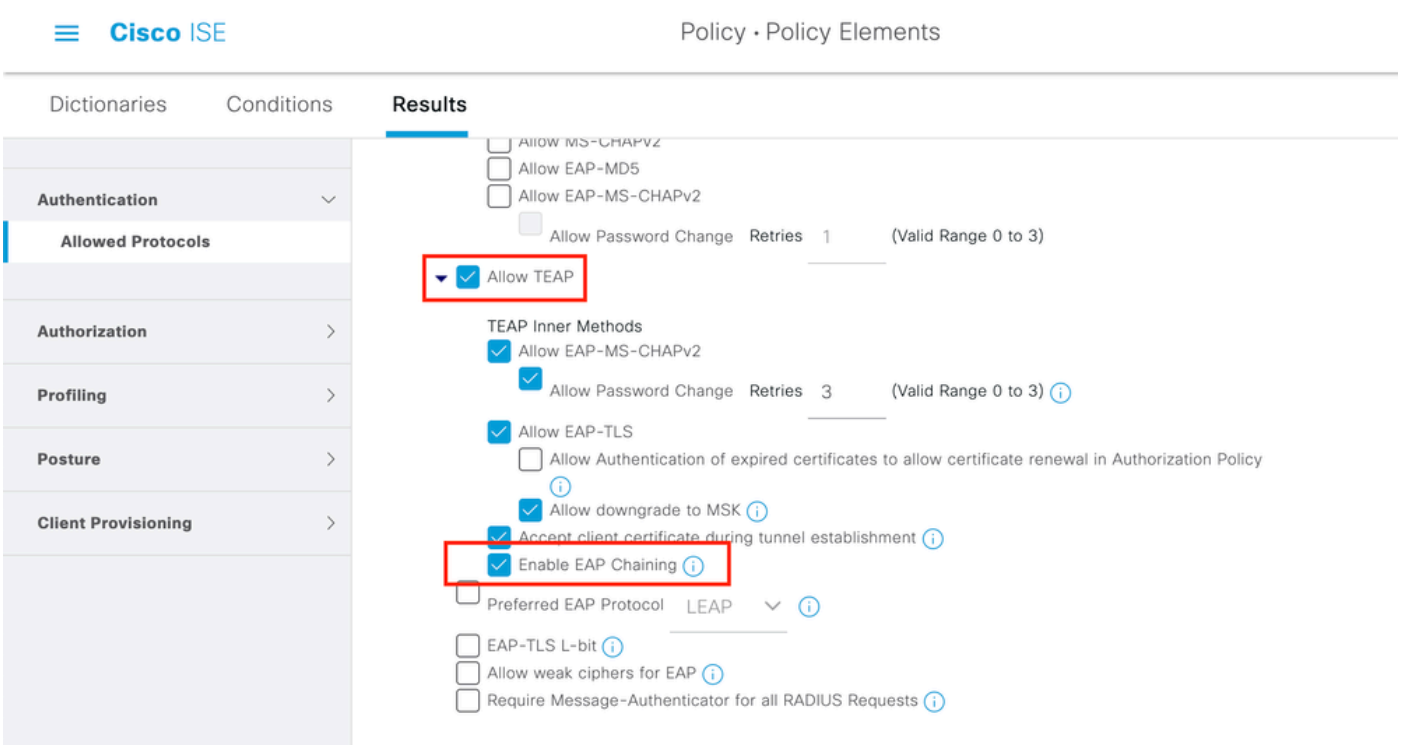
El encadenamiento de EAP permite la autenticación del usuario y la máquina dentro de una sesión EAP/Radius en lugar de dos sesiones independientes. Anteriormente, para lograr esto, necesitaba el módulo Cisco AnyConnect NAM y usar EAP-FAST en el suplicante de Windows, ya que el suplicante nativo de Windows no lo admitía. Ahora, puede utilizar el suplicante nativo de Windows para realizar el encadenamiento de EAP con ISE 2.7 con el uso de TEAP.

Configurar

Configuración de Cisco ISE

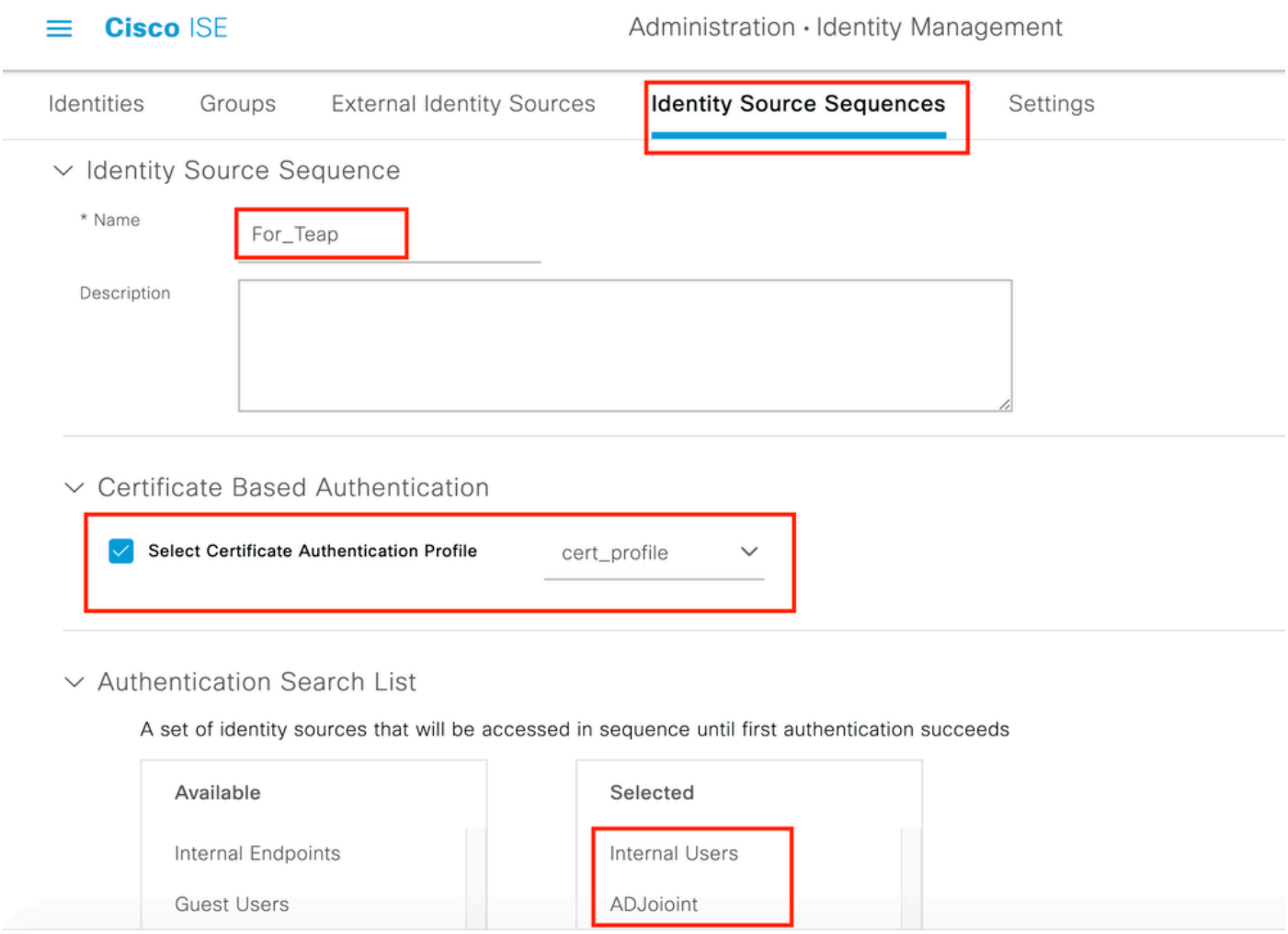
Paso 1. Debe editar los protocolos permitidos para habilitar el encadenamiento de EAP y TEAP.

Desplácese hasta ISE > Policy > Policy Elements > Results > Authentication > Allowed Protocols > Add New. Marcar las casillas de verificación de encadenamiento de EAP y TEAP.



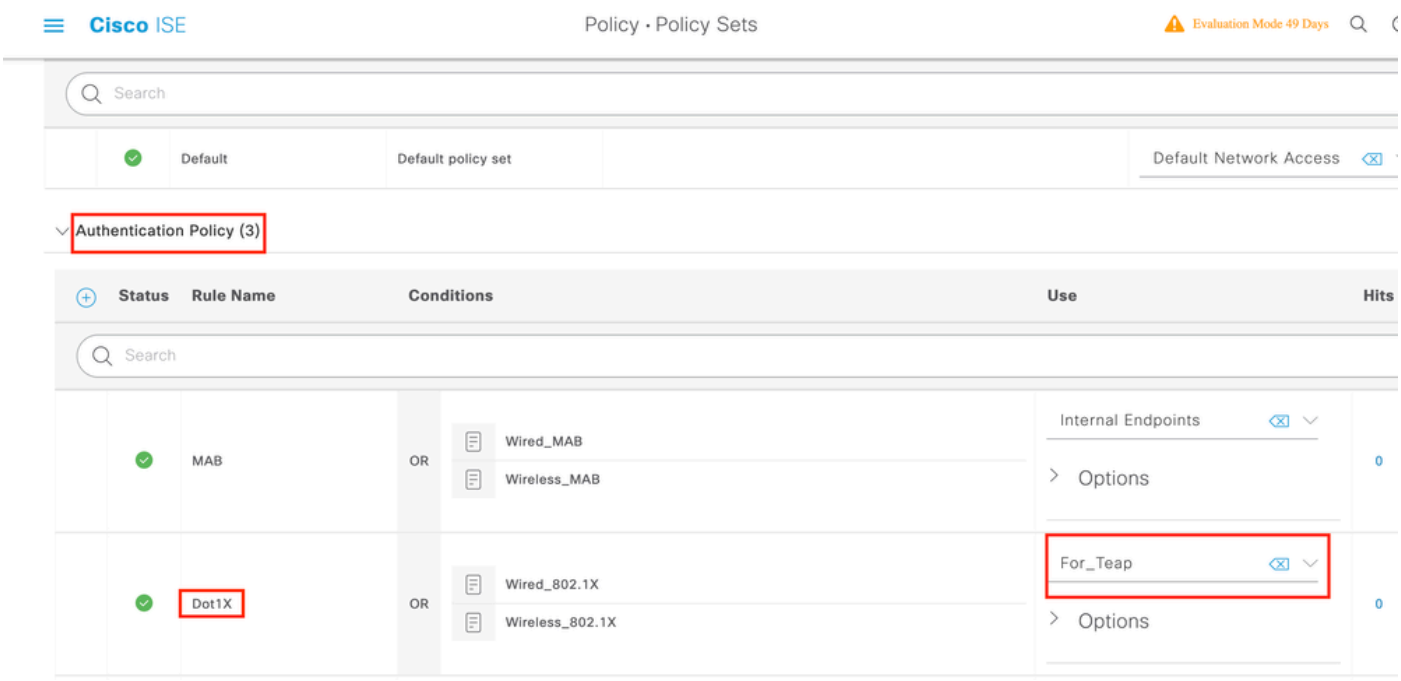
Paso 2. Cree un perfil de certificado y agréguelo a la secuencia de origen de identidad.

Desplácese hasta ISE > Administration > Identities > identity Source Sequence y elija el perfil del certificado.



Paso 3. Debe llamar a esta secuencia en la política de autenticación.

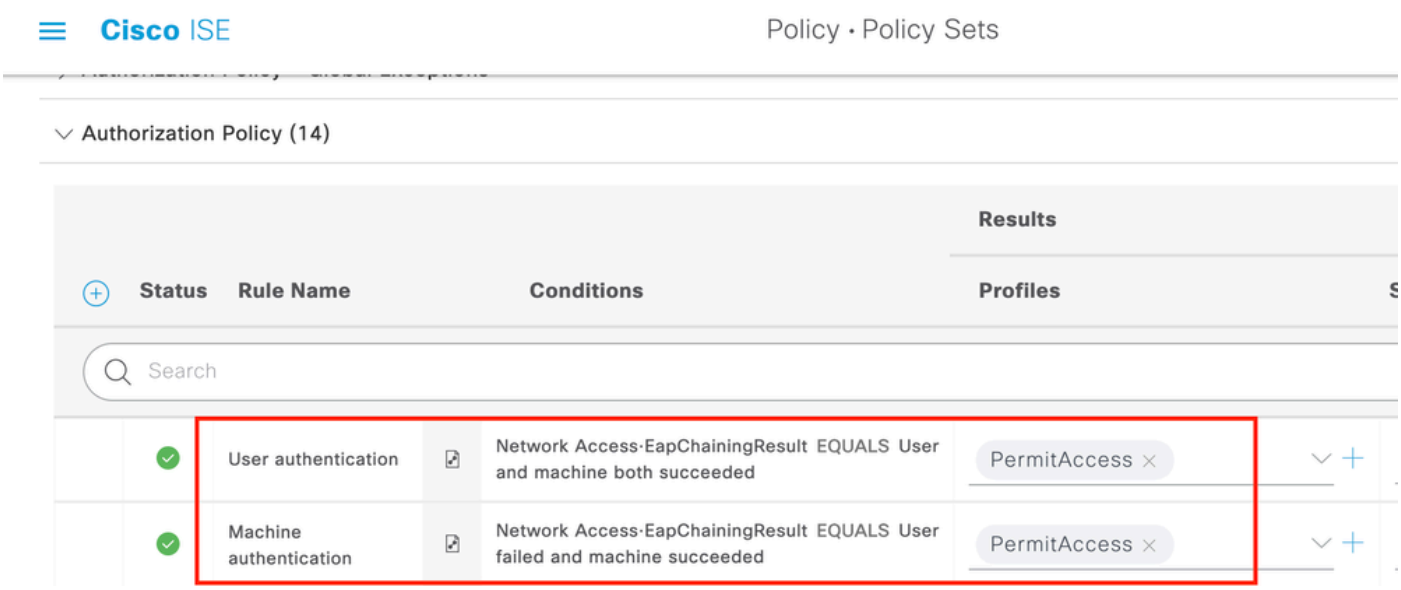
Desplácese hasta ISE > Policy > Policy Sets. Choose the Policy Set forDot1x > Authentication Policy y seleccione la secuencia de origen de identidad creada en el paso 2**.**



Paso 4. Ahora necesita modificar la política de autorización en el conjunto de políticas Dot1x.

Desplácese hasta ISE > Policy > Policy Sets. Choose the Policy Set for Dot1x > Authentication Policy.

Debe crear dos reglas. La primera regla verifica que la máquina está autenticada pero el usuario no. La segunda regla verifica que tanto el usuario como el equipo están autenticados.



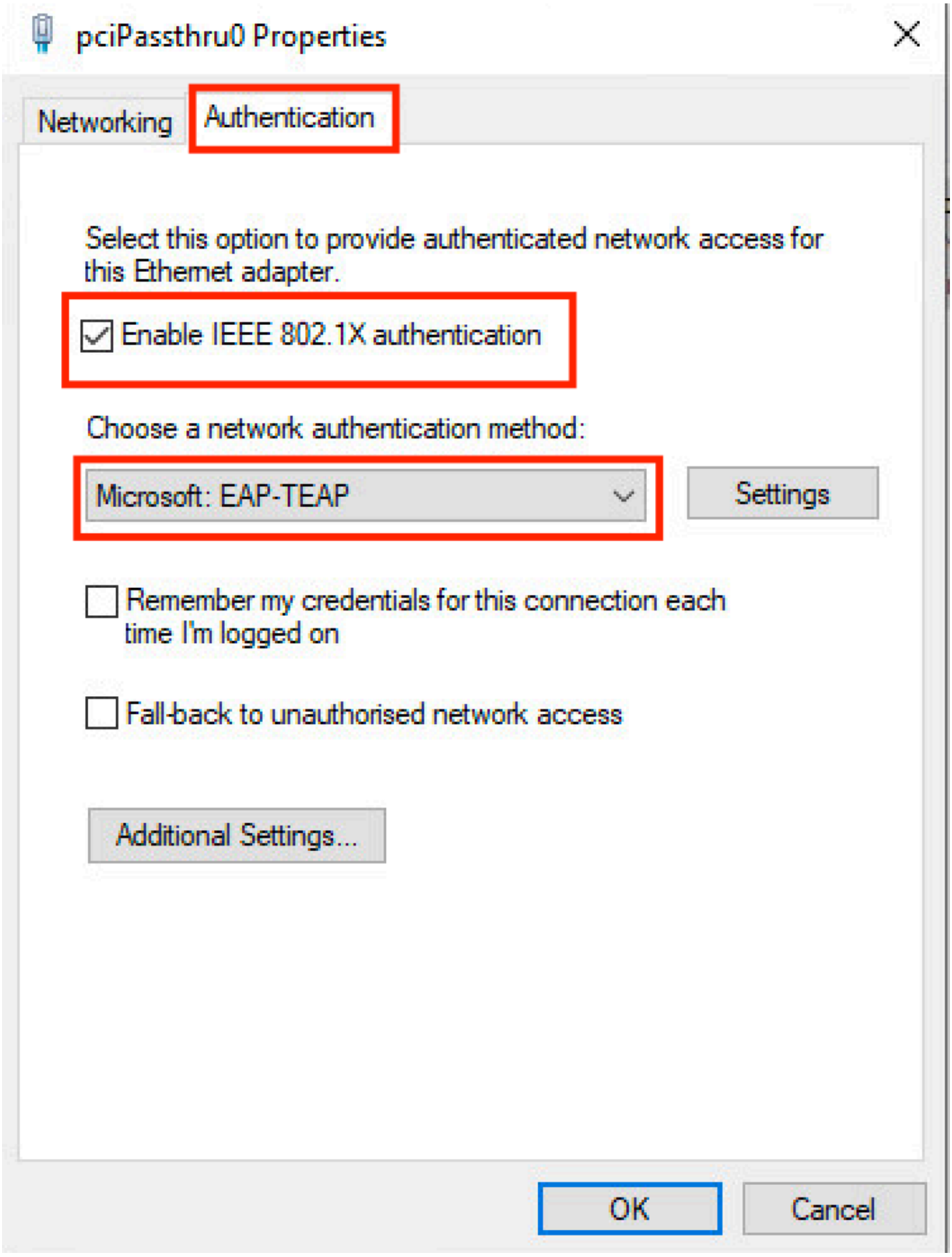
Esto completa la configuración desde el lado del servidor ISE.

Configuración del suplicante nativo de Windows

Configure la autenticación por cable en este documento.

Desplácese hasta Control Panel > Network and Sharing Center > Change Adapter Settings y haga clic con el botón derecho del ratón LAN Connection > Properties. Haga clic en la Authentication ficha.

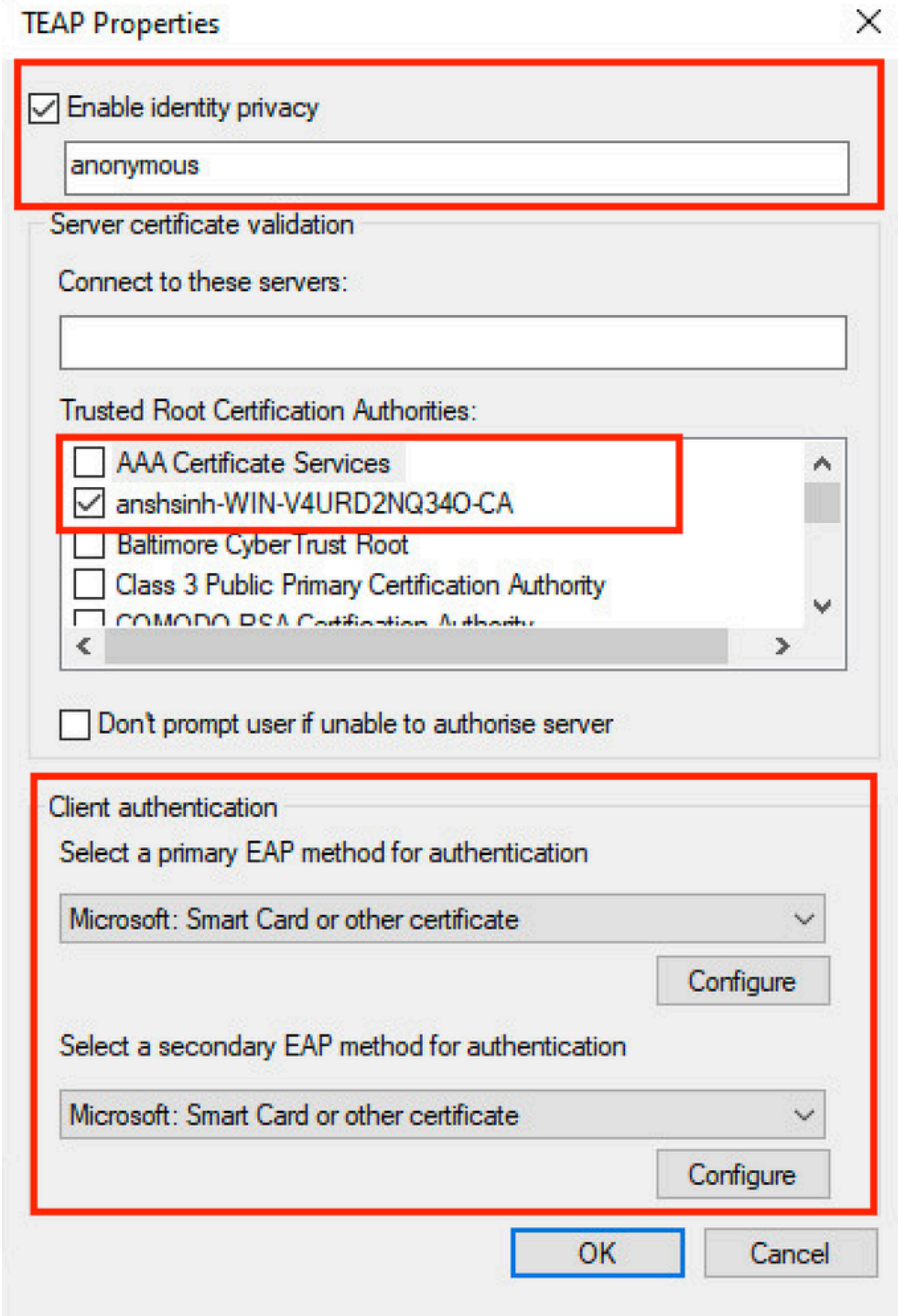
Paso 1. Haga clic en el menú Authenticationdesplegable y seleccione Microsoft EAP-TEAP.



Paso 2. Haga clic en elSettings botón situado junto al GETE.

1. Manténgase Enable Identity Privacy habilitado con anonymous como identidad.

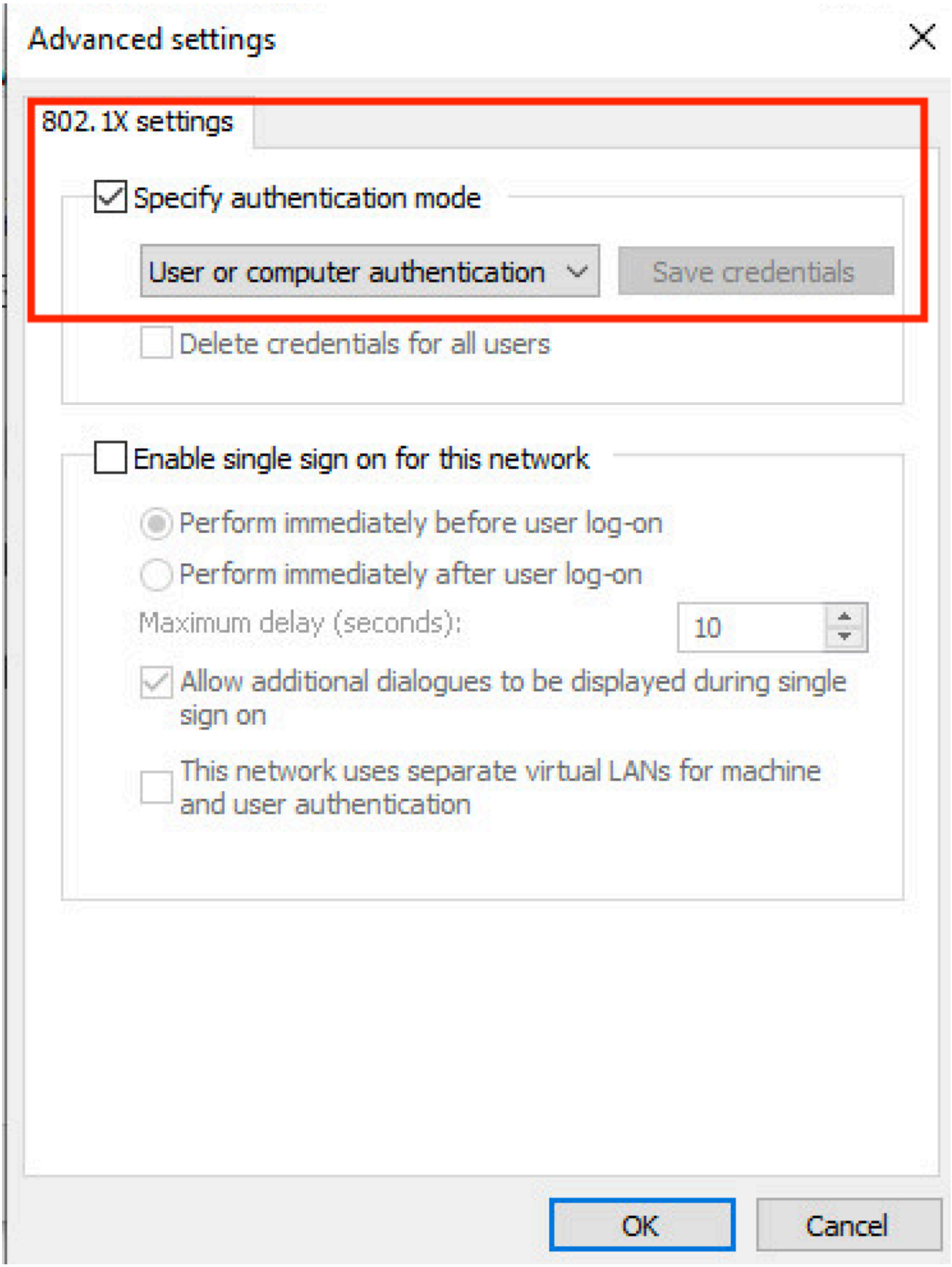
- Coloque una marca de verificación junto a los servidores de CA raíz bajo Entidades de certificación raíz de confianza que se utilizan para firmar el certificado para la autenticación EAP en ISE PSN.


TEAP Properties
Enable identity privacy
anonymous
Server certificate validation
Connect to these servers:
Trusted Root Certification Authorities:
AAA Certificate Services
anshsinh-WIN-V4URD2NQ34O-CA
Baltimore CyberTrust Root
Class 3 Public Primary Certification Authority
Don't prompt user if unable to authorise server
Client authentication
Select a primary EAP method for authentication
Microsoft: Smart Card or other certificate
Configure
Select a secondary EAP method for authentication
Microsoft: Smart Card or other certificate
Configure
OK
Cancel

1. Active Especificar modo de autenticación.

2. Establezca el menú desplegable en la configuración adecuada.

3. Elija User or computer authentication de modo que ambos estén autenticados y haga clic en OK.

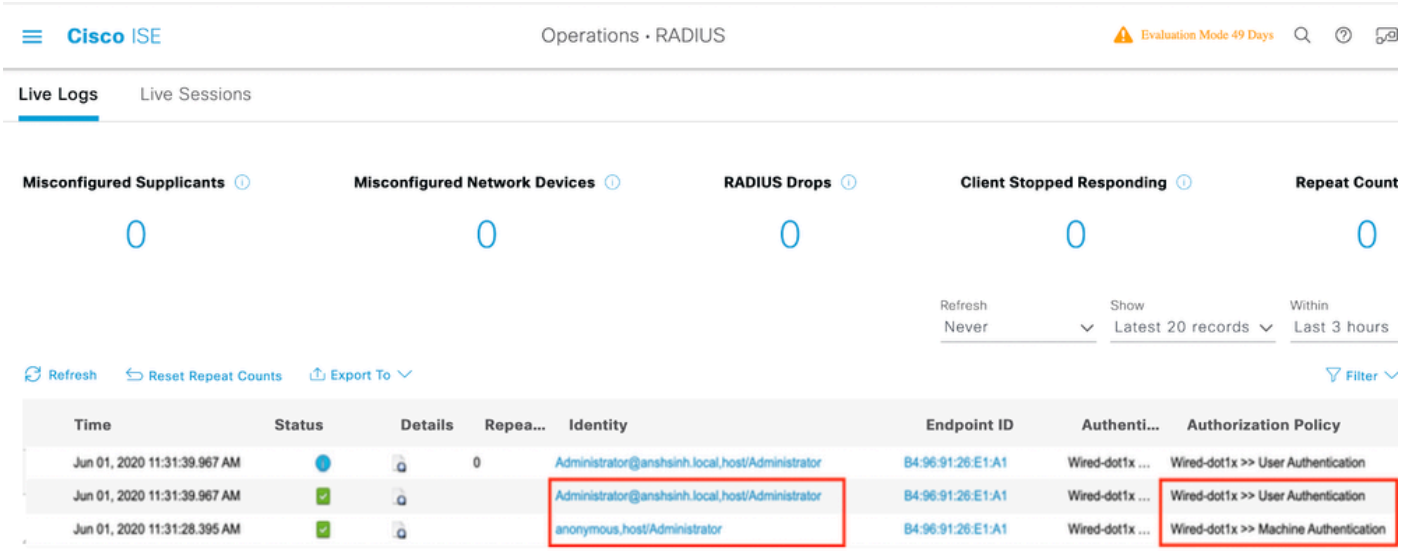


Verificación

Puede reiniciar el equipo con Windows 10 o cerrar sesión y, a continuación, iniciar sesión. Siempre que se muestre la pantalla de inicio de sesión de Windows, se activará la autenticación del equipo.

En los registros activos, verá anonymous, host/Administrator (aquí está el nombre del equipo) en el campo identity (identidad). Puede ver anonymous porque configuró suplicante para la privacidad de identidad arriba.

Cuando inicie sesión en el equipo con credenciales, puede ver en los registros en directo Administrator@example.local, host/Administrator. Este es el encadenamiento de EAP, donde la autenticación del usuario y la máquina ocurrió en una sesión de EAP.



Informe de autenticación detallado

En Detalles del registro en directo, las autenticaciones de equipo solo muestran una NACRadiusUsername entrada, pero la autenticación de usuario y equipo en cadena muestra dos entradas (una para el usuario y otra para el equipo). Además, puede ver debajo de la Authentication Details sección, que TEAP (EAP-TLS) se utilizó para el Authentication Protocol. Si utiliza MSCHAPv2 para la autenticación de equipo y usuario, se muestra el protocolo de autenticación TEAP (Microsoft: Secured password (EAP-MSCHAP v2)).

Autenticación de máquina

Authentication Details

Event	5200 Authentication succeeded
Username	anonymous,host/Administrator
Endpoint Id	B4:96:91:26:E1:A1
Calling Station Id	B4-96-91-26-E1-A1
Endpoint Profile	Intel-Device
IPv4 Address	169.254.75.41
Identity Group	Profiled
Audit Session Id	BD256A0A000000266EB5A242
Authentication Method	dot1x
Authentication Protocol	TEAP (EAP-TLS)
Service Type	Framed

Other Attributes

UseCase	Eap Chaining
NACRadiusUserName	host/Administrator
SelectedAuthenticationIdentityStores	cert_profile
AuthenticationStatus	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Machine Authentication
Serial Number	47 00 00 00 1C 84 F9 DB 39 FA 16 4F EB 00 00 00 00 00 1C
EndPointMACAddress	B4-96-91-26-E1-A1
EapChainingResult	User failed and machine succeeded

Autenticación de usuario y máquina

Authentication Details

Event	5200 Authentication succeeded
Username	Administrator@anshsinh.local,host/Administrator
Endpoint Id	B4:96:91:26:E1:A1
Calling Station Id	B4-96-91-26-E1-A1
Endpoint Profile	Intel-Device
IPv4 Address	169.254.75.41
Identity Group	Profiled
Audit Session Id	BD256A0A000000266EB5A242
Authentication Method	dot1x
Authentication Protocol	TEAP (EAP-TLS)
Service Type	Framed

Other Attributes

UseCase	Eap Chaining
NACRadiusUserName	Administrator@anshsinh.local
NACRadiusUserName	host/Administrator
SelectedAuthenticationIdentityStores	cert_profile
AuthenticationStatus	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	User Authentication
Serial Number	47 00 00 00 1C 84 F9 DB 39 FA 16 4F EB 00 00 00 00 00 1C
EndPointMACAddress	B4-96-91-26-E1-A1
EapChainingResult	User and machine both succeeded

Troubleshoot

Debe habilitar estas depuraciones en ISE:

- runtime-AAA
- nsf

- nsf-session
- Active Directory (para solucionar problemas entre ISE y AD)

En Windows, puede comprobar los registros del Visor de sucesos.

Análisis de Live Log

Autenticación de máquina

<#root>

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ... 11507 Extracted EAP-Response/Identity

12756 Prepared EAP-Request proposing TEAP with challenge

... ...

12758 Extracted EAP-Response containing TEAP challenge-response and accepting TEAP as negotiated

12800 Extracted first TLS record; TLS handshake started 12805 Extracted TLS ClientHello message 12806

11559 Client certificate was requested but not received inside the tunnel. Will continue with inner meth

... ...

11627 Starting EAP chaining 11573 Selected identity type 'User'

11564 TEAP inner method started 11521 Prepared EAP-Request/Identity for inner EAP method 11567

11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

11596 Prepared EAP-Request with another TEAP challenge 11006 Returned RADIUS Access-Challenge 11001 Re

11515 Supplicant declined inner EAP method selected by Authentication Policy but did not proposed anothe

22028 Authentication failed and the advanced options are ignored 33517 Sent TEAP Intermediate Result T

11574 Selected identity type 'Machine' 11564 TEAP inner method started

11521 Prepared EAP-Request/Identity for inner EAP method ... ... 11567 Identity type provided by clien

11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

11596 Prepared EAP-Request with another TEAP challenge ... ...

12523 Extracted EAP-Response/NAK for inner method requesting to use EAP-TLS instead

12522 Prepared EAP-Request for inner method proposing EAP-TLS with challenge 12625 Valid EAP-Key-Name

22037 Authentication Passed 12528 Inner EAP-TLS authentication succeeded

11519 Prepared EAP-Success for inner EAP method 11565 TEAP inner method finished successfully

... ... 33516 Sent TEAP Intermediate Result TLV indicating success 11596 Prepared EAP-Request with ano

11576 TEAP cryptobinding verification passed

... ...

15036 Evaluating Authorization Policy

24209 Looking up Endpoint in Internal Endpoints IDStore - anonymous,host/Administrator 24211 Found End

11597 TEAP authentication phase finished successfully 11503 Prepared EAP-Success 11002 Returned RADIUS A

Autenticación de usuario y máquina

<#root>

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ...

12756 Prepared EAP-Request proposing TEAP with challenge

... ...

12758 Extracted EAP-Response containing TEAP challenge-response and accepting TEAP as negotiated

12800 Extracted first TLS record; TLS handshake started 12805 Extracted TLS ClientHello message 12806

11620 TEAP full handshake finished successfully

11596 Prepared EAP-Request with another TEAP challenge ... ... 11595 Extracted EAP-Response containing

11627 Starting EAP chaining

11573 Selected identity type 'User' 11564 TEAP inner method started

11521 Prepared EAP-Request/Identity for inner EAP method 11596 Prepared EAP-Request with another TEAP

11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

11596 Prepared EAP-Request with another TEAP challenge ... ...

12523 Extracted EAP-Response/NAK for inner method requesting to use EAP-TLS instead

12522 Prepared EAP-Request for inner method proposing EAP-TLS with challenge ... ... 11595 Extracted E

22037 Authentication Passed

12528 Inner EAP-TLS authentication succeeded 11519 Prepared EAP-Success for inner EAP method

11565 TEAP inner method finished successfully

33516 Sent TEAP Intermediate Result TLV indicating success 11596 Prepared EAP-Request with another TEA

11576 TEAP cryptobinding verification passed 11574 Selected identity type 'Machine'

11564 TEAP inner method started ... ...

11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

11596 Prepared EAP-Request with another TEAP challenge ... ...

12523 Extracted EAP-Response/NAK for inner method requesting to use EAP-TLS instead

12522 Prepared EAP-Request for inner method proposing EAP-TLS with challenge

```
 ... ...
12524 Extracted EAP-Response containing EAP-TLS challenge-response for inner method and accepting EAP-TL

12800 Extracted first TLS record; TLS handshake started
 12545 Client requested EAP-TLS session ticket
12546 The EAP-TLS session ticket received from supplicant. Inner EAP-TLS does not support stateless sess
 12805 Extracted TLS ClientHello message 12806 Prepared TLS ServerHello message 12807 Prepared TLS Cert
22037 Authentication Passed 12528 Inner EAP-TLS authentication succeeded 11519 Prepared EAP-Success for
 11565 TEAP inner method finished successfully 33516 Sent TEAP Intermediate Result TLV indicating succe
15036 Evaluating Authorization Policy
 24209 Looking up Endpoint in Internal Endpoints IDStore - Administrator@example.local,host/Administrat
11597 TEAP authentication phase finished successfully 11503 Prepared EAP-Success 11002 Returned RADIUS A
```

Información Relacionada

- Protocolo de autenticación extensible de túnel (TEAP) versión 1
- Reanudación de sesión de seguridad de la capa de transporte (TLS) sin estado del servidor
- Comprender las implementaciones de encadenamiento y EAP-FAST en AnyConnect NAM e ISE
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).