

Encadeamento EAP com TEAP

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Configuração do Cisco ISE](#)

[Configuração do Solicitante Nativo do Windows](#)

[Verificar](#)

[Relatório de Autenticação Detalhado](#)

[Autenticação da máquina](#)

[Autenticação de Usuário e Máquina](#)

[Troubleshoot](#)

[Análise de log ao vivo](#)

[Autenticação da máquina](#)

[Autenticação de Usuário e Máquina](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como configurar o ISE e o solicitante do Windows para o Encadeamento do Protocolo de Autenticação Extensível (EAP - Extensible Authentication Protocol) com o Protocolo de Autenticação Extensível baseado em Túnel (TEAP - Tunnel-based Extensible Authentication Protocol).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- ISE
- Configuração do solicitante do Windows

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco ISE versão 3.0
- Windows 10 versão 2004
- Conhecimento do protocolo 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O TEAP é um método de protocolo de autenticação extensível baseado em túnel que estabelece um túnel seguro e executa outros métodos EAP sob a proteção desse túnel seguro.

A autenticação TEAP ocorre em duas fases após a troca inicial de solicitação/resposta de identidade EAP.

Na primeira fase, o TEAP usa o handshake TLS para fornecer uma troca de chave autenticada e para estabelecer um túnel protegido. Uma vez que o túnel é estabelecido, a segunda fase começa com o peer e o servidor se envolve em conversação adicional para estabelecer as autenticações e políticas de autorização necessárias.

O Cisco ISE 2.7 e posterior suporta o protocolo TEAP. Os objetos type-length-value (TLV) são usados dentro do túnel para transportar dados relacionados à autenticação entre o peer EAP e o servidor EAP.

A Microsoft introduziu o suporte para TEAP na versão Windows 10 2004 lançado em maio de 2020.

O encadeamento EAP permite a autenticação do usuário e da máquina em uma sessão EAP/Radius em vez de duas sessões separadas.

Anteriormente, para conseguir isso, você precisava do módulo Cisco AnyConnect NAM e usar EAP-FAST no solicitante do Windows, pois o solicitante nativo do Windows não oferecia suporte a isso. Agora, você pode usar o Windows Native Supplicant para executar o encadeamento EAP com ISE 2.7 com o uso de TEAP.

Configurar

Configuração do Cisco ISE

Etapa 1. Você precisa editar os protocolos permitidos para habilitar o TEAP e o encadeamento EAP.

Navegue até **ISE > Policy > Policy Elements > Results > Authentication > Allowed Protocols > Add New** . Marque as caixas de seleção de encadeamento EAP e TEAP.

Dictionaryes Conditions **Results**

Authentication

Allowed Protocols

Authorization

Profiling

Posture

Client Provisioning

- Allow MS-CHAPV2
- Allow EAP-MD5
- Allow EAP-MS-CHAPv2
- Allow Password Change Retries 1 (Valid Range 0 to 3)
- Allow TEAP
- TEAP Inner Methods
 - Allow EAP-MS-CHAPv2
 - Allow Password Change Retries 3 (Valid Range 0 to 3) ⓘ
 - Allow EAP-TLS
 - Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy ⓘ
 - Allow downgrade to MSK ⓘ
 - Accept client certificate during tunnel establishment ⓘ
 - Enable EAP Chaining ⓘ
- Preferred EAP Protocol LEAP ⓘ
- EAP-TLS L-bit ⓘ
- Allow weak ciphers for EAP ⓘ
- Require Message-Authenticator for all RADIUS Requests ⓘ

Etapa 2. Crie um perfil de certificado e adicione-o à Sequência de Origem da Identidade.

Navegue até ISE > Administration > Identities > identity Source Sequence e escolha o perfil do certificado.

Identities Groups External Identity Sources **Identity Source Sequences** Settings

Identity Source Sequence

* Name For_Teap

Description

Certificate Based Authentication

Select Certificate Authentication Profile cert_profile

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Internal Endpoints	Internal Users
Guest Users	ADJoint

Etapa 3. Você precisa chamar esta sequência na Política de autenticação.

Navegue até ISE > Policy > Policy Sets . Choose the Policy Set for Dot1x > Authentication Policy e escolha a sequência de origem de identidade criada na Etapa 2.

Status	Rule Name	Conditions	Use	Hits
✓	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	0
✓	Dot1X	OR Wired_802.1X Wireless_802.1X	For_Teap > Options	0

Etapa 4. Agora você precisa modificar a Política de Autorização no Conjunto de Políticas Dot1x.

Navegue até ISE > Policy > Policy Sets . Choose the Policy Set for Dot1x > Authentication Policy .

Você precisa criar duas regras. A primeira regra verifica se a máquina está autenticada, mas o usuário não. A segunda regra verifica se o usuário e a máquina estão autenticados.

Status	Rule Name	Conditions	Profiles	Results
✓	User authentication	Network Access:EapChainingResult EQUALS User and machine both succeeded	PermitAccess ×	
✓	Machine authentication	Network Access:EapChainingResult EQUALS User failed and machine succeeded	PermitAccess ×	

Isso conclui a configuração no lado do servidor do ISE.

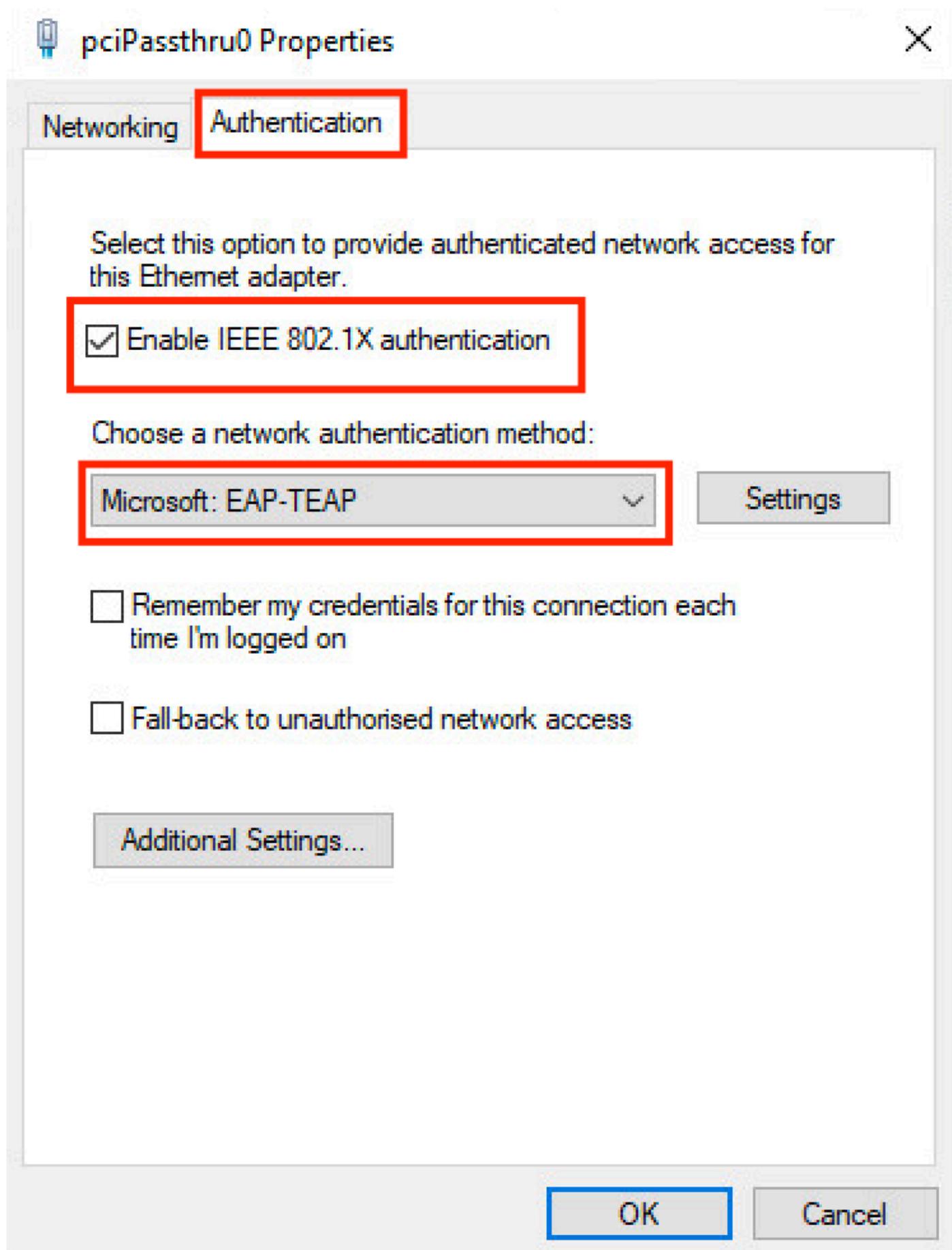
Configuração do Solicitante Nativo do Windows

Defina a configuração da autenticação com fio neste documento.

Navegue até Control Panel > Network and Sharing Center > Change Adapter Settings e clicar com o botão direito

do mouse em LAN Connection > Properties. Clique no botão Authentication guia.

Etapa 1. Clique em Authentication e escolha Microsoft EAP-TEAP.



Etapa 2. Clique no botão **Settings** ao lado de TEAP.

1. Manter **Enable Identity Privacy** habilitado com **anonymous** como a identidade.
2. Coloque uma marca de seleção ao lado do(s) servidor(es) de CA raiz em Autoridades de certificação raiz confiáveis que são usadas para assinar o certificado para autenticação EAP no PSN do ISE.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.