

# Configurar a autenticação EAP-TLS com ISE

## Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Obter certificados de servidor e cliente](#)

[Etapa 1. Gerar uma solicitação de assinatura de certificado do ISE](#)

[Etapa 2. Importar certificados CA para o ISE](#)

[Etapa 3. Obter Certificado de Cliente para Ponto de Extremidade](#)

[Dispositivos de rede](#)

[Etapa 4. Adicionar o dispositivo de acesso à rede no ISE](#)

[Elementos de política](#)

[Etapa 5. Usar fonte de identidade externa](#)

[Etapa 6. Criar o perfil de autenticação do certificado](#)

[Passo 7. Adicionar a uma sequência de origem de identidade](#)

[Etapa 8. Definir o Serviço de Protocolos Permitidos](#)

[Etapa 9. Criar o Perfil de Autorização](#)

[Políticas de segurança](#)

[Etapa 10. Criar o conjunto de políticas](#)

[Etapa 11. Criar uma política de autenticação](#)

[Etapa 12. Criar a Política de Autorização](#)

[Verificar](#)

[Troubleshooting](#)

[Problemas Comuns e Técnicas para Troubleshooting](#)

[Informações Relacionadas](#)

## Introdução

Este documento descreve a configuração inicial para apresentar o Extensible Authentication Protocol-Transport Layer Security Authentication com o Cisco ISE.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Entendimento básico do fluxo de comunicações EAP e RADIUS.
- Conhecimento básico de autenticação RADIUS com métodos de autenticação baseados em certificado em termos de fluxo de comunicação.
- Compreensão das diferenças entre Dot1x e MAC Authentication Bypass (MAB).
- Conhecimento básico da Public Key Infrastructure (PKI).
- Familiaridade com como obter certificados assinados de uma CA (Autoridade de Certificação) e gerenciar certificados nos endpoints.
- Configuração de configurações relacionadas a Autenticação, Autorização e Contabilização (AAA -

Authentication, Authorization, and Accounting) (RADIUS) em um dispositivo de rede (com fio ou sem fio).

- Configuração do suplicante (no endpoint) para uso com RADIUS/802.1x.

## Componentes Utilizados

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

- Identity Services Engine (ISE) versão 3.x.
- CA - para emitir certificados (pode ser CA Corporativa, CA de terceiros/Pública ou usar o [Portal de Provisionamento de Certificado](#)).
- Ative Directory (fonte de identidade externa) - do Windows Server; quando [compatível com o ISE](#).
- Network Access Device (NAD) - pode ser Switch (com fio) ou [Wireless LAN Controller \(WLC\)](#) (sem fio) configurado para 802.1x/AAA.
- Endpoint - certificados emitidos para a identidade (do usuário) e a configuração do solicitante que podem ser autenticados para acesso à rede via RADIUS/802.1x: Autenticação do Usuário. É possível obter um certificado de máquina, mas ele não é usado neste exemplo.

---

**Observação:** como este guia usa o ISE versão 3.1, todas as referências de documentação são baseadas nesta versão. No entanto, a mesma configuração ou semelhante é possível e totalmente suportada em versões anteriores do Cisco ISE.

---

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

O foco principal está na configuração do ISE, que pode ser aplicada a vários cenários, como (mas não limitado a) autenticação com um telefone IP/endpoint conectado via rede com fio ou sem fio.

Para o escopo deste guia, é importante entender estas fases do fluxo de autenticação do ISE (RADIUS):

- Autenticação - identifique e valide a identidade final (máquina, usuário etc.) que solicita acesso à rede.
- Autorização - Determine quais permissões/acesso a identidade final pode ser concedida na rede.
- Contabilização - Relata e rastreia a atividade de rede da identidade final depois que o acesso à rede é alcançado.

## Configurar

### Obter certificados de servidor e cliente

#### Etapa 1. Gerar uma solicitação de assinatura de certificado do ISE

A primeira etapa é gerar uma CSR (Certificate Signing Request, Solicitação de assinatura de certificado) do ISE e enviá-la à CA (servidor) para obter o certificado assinado emitido para o ISE, como um certificado do sistema. Este certificado pode ser apresentado como um certificado de servidor pelo ISE durante a

autenticação EAP-TLS (Extensible Authentication Protocol-Transport Layer Security Authentication). Isso é executado na interface do usuário do ISE. Navegue até **Administration > System: Certificates > Certificate Management > Certificate Signing Requests**. Sob **Certificate Signing Requests**, clique em **Generate Certificate Signing Requests (CSR)** como mostrado nesta imagem.

## Certificate Signing Requests

**Generate Certificate Signing Requests (CSR)**

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external that authority. Once a CSR is bound, it will be removed from this list.

View Export Delete Bind Certificate

<input type="checkbox"/>	Friendly Name	Certificate Subject	Key Length	Portal gro...	Timestamp
No data available					

Os tipos de certificado exigem diferentes usos de chave estendida. Esta lista descreve quais usos de chave estendida são necessários para cada tipo de certificado:

### Certificados de identidade do ISE

- Multiuso (Admin, EAP, Portal, pxGrid) - Autenticação de Cliente e Servidor
- Admin - Autenticação de Servidor
- Autenticação EAP - Autenticação do servidor
- Autenticação DTLS (Datagram Transport Layer Security) - Autenticação do Servidor
- Portal - Autenticação de servidor
- pxGrid - Autenticação de cliente e servidor
- SAML (Security Assertion Markup Language) - Certificado de Autenticação SAML
- Serviço de mensagens do ISE - Gerar um certificado de assinatura ou gerar um certificado de mensagens totalmente novo

Por padrão, o Certificado do sistema do serviço de mensagens do ISE destina-se à replicação de dados em cada nó do ISE na implantação, no registro de nós e em outras comunicações entre nós, e está presente e é emitido pelo servidor da autoridade de certificação interna (CA) do ISE (interno ao ISE). Nenhuma ação precisa ser concluída com este certificado.

O certificado do sistema administrativo é usado para identificar cada nó do ISE, por exemplo, quando a API associada à interface do usuário administrativo (Gerenciamento) é usada e para algumas comunicações entre nós. Para configurar o ISE pela primeira vez, coloque o Certificado do sistema administrativo em vigor. Essa ação não está diretamente relacionada a este guia de configuração.

Para executar o IEEE 802.1x via EAP-TLS (autenticação baseada em certificado), execute uma ação para o Certificado do Sistema de Autenticação EAP, pois ele é usado como o certificado do servidor apresentado ao ponto final/cliente durante o fluxo EAP-TLS; como resultado, é protegido dentro do túnel TLS. Para começar, crie um CSR para criar o Certificado do Sistema de Autenticação EAP e forneça-o ao pessoal que gerencia os servidores de CA na sua organização (ou provedor de CA público) para assinatura. O resultado final é o Certificado assinado pela CA que se vincula ao CSR e se associa ao ISE com essas etapas.

No formulário CSR (Certificate Signing Request, Solicitação de assinatura de certificado), escolha estas opções para concluir o CSR e obter seu conteúdo:

- Uso do certificado, para este exemplo de configuração, escolha **EAP Authentication**.
- Se você planeja utilizar uma instrução curinga no certificado, **\*.example.com**, você também deve verificar o **Allow Wildcard Certificate** caixa de seleção. O melhor local é o campo de certificado SAN (Nome alternativo do assunto) para compatibilidade com qualquer uso e em vários tipos diferentes de sistemas operacionais de endpoint que podem estar presentes no ambiente.
- Se você não escolheu colocar uma instrução curinga no certificado, escolha a quais nós do ISE você deseja associar o Certificado assinado pela CA (após a assinatura).

---

**Observação:** quando você vincula o certificado assinado pela CA que contém a instrução curinga a vários nós no CSR, o certificado é distribuído para cada nó do ISE (ou para os nós selecionados) na implantação do ISE, e os serviços podem ser reiniciados. No entanto, a reinicialização dos serviços é automaticamente limitada a um nó por vez. Monitore a reinicialização dos serviços por meio do comando `show application status ise` Comando CLI do ISE.

---

Em seguida, você precisa preencher o formulário para definir o Assunto. Isso inclui os campos de certificado Nome comum (CN), Unidade organizacional (OU), Organização (O), Cidade (L), Estado (ST) e País (C). A variável `$FQDN$` é o valor que representa o nome de domínio totalmente qualificado de gerenciamento (nome de host + nome de domínio) associado a cada nó do ISE.

- O Subject Alternative Name (SAN) OS campos também devem ser preenchidos para incluir todas as informações necessárias e desejadas a serem usadas para estabelecer confiança. Como requisito, você precisa definir a Entrada DNS que aponta para o FQDN do(s) nó(s) ISE associado(s) a esse certificado, após a assinatura do certificado.
- Por fim, certifique-se de definir o tipo de chave, o comprimento da chave e o resumo apropriados para assinar com que estejam em conformidade com os recursos do(s) servidor(es) da autoridade de certificação e com as boas práticas de segurança em mente. Os valores padrão são: RSA, 4096 bits e SHA-384, respectivamente. As opções disponíveis e a compatibilidade são exibidas nesta página na IU de administração do ISE.

Este é um exemplo de um formulário CSR preenchido sem usar uma instrução curinga. Certifique-se de usar valores reais específicos do ambiente:

## Usage

Certificate(s) will be used for EAP Authentication 

Allow Wildcard Certificates  

## Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
<input checked="" type="checkbox"/> ise	ise#EAP Authentication
<input checked="" type="checkbox"/> ise2	ise2#EAP Authentication
<input checked="" type="checkbox"/> ise3	ise3#EAP Authentication

## Subject

Common Name (CN)  
\$FQDN\$ 

---

Organizational Unit (OU)  
\_\_\_\_\_ 

Organization (O)  
Example Company 

---

City (L)  
San Jose  
\_\_\_\_\_

State (ST)  
California  
\_\_\_\_\_

Country (C)  
US  
\_\_\_\_\_

#### Subject Alternative Name (SAN)

⋮	DNS Name	ise.example.com	-	+	
⋮	DNS Name	ise2.example.com	-	+	
⋮	DNS Name	ise3.example.com	-	+	ⓘ

\* Key type  
RSA ⓘ

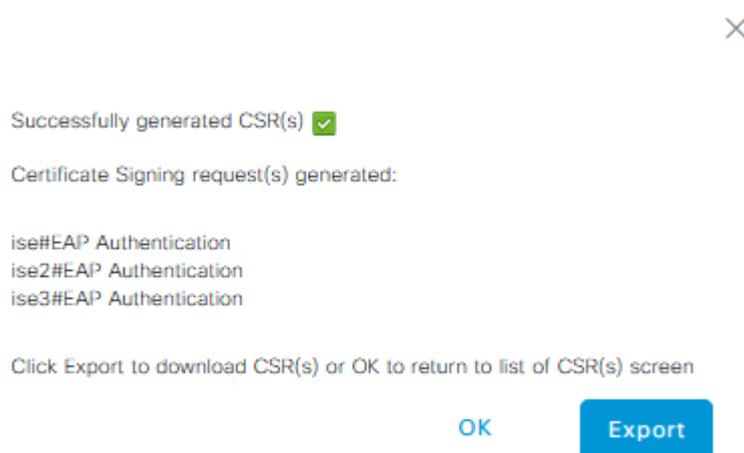
\* Key Length  
4096 ⓘ

\* Digest to Sign With  
SHA-384

Certificate Policies

#### Exemplo de CSR

Para salvar o CSR, clique em **Generate**. Clique em **Export**, localizado na parte inferior direita, para exportar o(s) arquivo(s) CSR deste prompt:



#### Exemplo de Exportação de CSR

Mais informações sobre certificados para uso com o ISE podem ser encontradas no Guia do Administrador do Cisco Identity Services Engine, Release 3.1 > Capítulo: Configuração Básica > [Gerenciamento de Certificado no Cisco ISE](#) e [Instalar um Certificado de Terceiros Assinado pela CA no ISE](#).

## Etapa 2. Importar certificados CA para o ISE

Depois que a CA retorna o certificado assinado, ela também inclui a cadeia completa de CA composta de um certificado raiz e um/vários certificados intermediários. A IU de administração do ISE força você a importar todos os certificados na cadeia de CA primeiro, antes de associar ou carregar qualquer certificado do sistema. Isso é feito para garantir que cada certificado do sistema seja associado corretamente à cadeia de CA (também conhecida como certificado confiável) no software ISE.

Estas etapas são a melhor maneira de importar os certificados de CA e o certificado do sistema para o ISE:

1. Para importar o certificado raiz para a GUI do ISE, navegue para **Administration > System: Certificates > Certificate Management**. Sob **Trusted Certificates**, clique em **Import** e marque as caixas de seleção **Trust for authentication within ISE** (Infrastructure) and **Trust for client authentication and Syslog** (Endpoints) para os usos de certificado **Trust for authentication no ISE** (Infrastructure) e **Trust for client authentication e Syslog** (Endpoints).

## Usage

Trusted For: ⓘ

- Trust for authentication within ISE
- Trust for client authentication and Syslog
- Trust for certificate based admin authentication
- Trust for authentication of Cisco Services

*Uso de Certificado para Cadeia de Autoridades de Certificação*

2. Repita a etapa anterior para cada Certificado(s) Intermediário(s) como parte da cadeia de certificados da CA.
3. Quando todos os certificados, como parte da cadeia completa de CAs, forem importados para o armazenamento de certificados confiáveis no ISE, retorne à GUI do ISE e navegue até **Administration > System: Certificates > Certificate Management: Certificate Signing Requests**. Localize a entrada de CSR em **Nome Amigável** que corresponde ao certificado assinado, clique na caixa de seleção do certificado e clique em **Bind Certificate**.

## Certificate Signing Requests

[Generate Certificate Signing Requests \(CSR\)](#)

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request that authority. Once a CSR is bound, it will be removed from this list.

View Export Delete **Bind Certificate** 2)

<input type="checkbox"/>	Friendly Name 1)	Certificate Subject	Key Length	Portal gro...	Timestamp	Host
<input checked="" type="checkbox"/>	ise#EAP Authentication	CN=ise.example.com ,O=E...	4096		Tue, 10 May 2022	ise
<input type="checkbox"/>	ise2#EAP Authentication	CN=ise2.example.com ,O=...	4096		Tue, 10 May 2022	ise2
<input type="checkbox"/>	ise3#EAP Authentication	CN=ise3.example.com ,O=...	4096		Tue, 10 May 2022	ise3

*Vincular certificado ao CSR*

**Observação:** você precisa vincular um único certificado assinado pela CA a cada CSR, um de cada vez. Repita o procedimento para todos os CSRs restantes criados para outros nós do ISE na implantação.

Na próxima página, clique em **Browse** e escolha o arquivo de certificado assinado, defina um Nome Amigável desejado e escolha o(s) Uso(s) do Certificado. Submeta para salvar as alterações.

## Bind CA Signed Certificate

\* Certificate File

EXAMPLE\_ISE.cer

Friendly Name

EAP Authentication System Certificate



e atribua ao mesmo nó para o qual o CSR foi criado. Repita o mesmo processo para outros nós e/ou outros usos de certificado.

### **Etapa 3. Obter Certificado de Cliente para Ponto de Extremidade**

É necessário navegar por um processo semelhante no endpoint para a criação de um certificado de cliente para uso com EAP-TLS. Para este exemplo, você precisa de um certificado de cliente assinado e emitido para a conta de usuário para executar a autenticação de usuário com o ISE. Um exemplo de como obter um certificado de cliente para o endpoint de um ambiente do Active Directory pode ser encontrado em: Entender e configurar EAP-TLS usando WLC e ISE > **Configurar** > [Cliente para EAP-TLS](#).

Devido aos vários tipos de endpoints e sistemas operacionais, como o processo pode ser um pouco diferente, exemplos adicionais não são fornecidos. No entanto, o processo geral é conceitualmente o mesmo. Gere um CSR que tenha todas as informações relevantes a serem incluídas no certificado e que seja assinado pela CA, seja um servidor interno no ambiente ou uma empresa pública/de terceiros que forneça esse tipo de serviço.

Além disso, os campos de certificado Nome comum (CN) e Nome alternativo do assunto (SAN) incluem a identidade a ser usada durante o fluxo de autenticação. Isso também determina como o solicitante deve ser configurado para EAP-TLS em termos de identidade: máquina e/ou autenticação de usuário, autenticação de máquina ou autenticação de usuário. Este exemplo usa somente a autenticação de usuário no restante deste documento.

## **Dispositivos de rede**

### **Etapa 4. Adicionar o dispositivo de acesso à rede no ISE**

O Network Access Device (NAD) ao qual um endpoint está conectado também é configurado no ISE para que a comunicação RADIUS/TACACS+ (Device Admin) possa ocorrer. Entre o NAD e o ISE, uma senha/segredo compartilhado é usado para fins de confiança.

Para adicionar um NAD por meio da GUI do ISE, navegue até **Administration** > **Network Resources: Network Devices** > **Network Devices** e clique em **Add**, que é mostrado nesta imagem.

Cisco ISE Administration - Network Resources

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | NAC Managers | External MDM | Location Services

Network Devices List > Switch

### Network Devices

\* Name:

Description:

---

IP Address:  /

---

\* Device Profile:

Model Name:

Software Version:

\* Network Device Group

Device Type:

IPSEC:

Location:

Exemplo de configuração de dispositivo de rede

Para uso com a Criação de perfis do ISE, você também deve configurar o SNMPv2c ou SNMPv3 (mais seguro) para permitir que o Nó de serviço de política (PSN) do ISE contate o NAD através de consultas SNMP envolvidas na autenticação do endpoint para o ISE, a fim de coletar atributos para tomar decisões precisas sobre o tipo de endpoint usado. O próximo exemplo mostra como configurar o SNMP (v2c), na mesma página do exemplo anterior:

SNMP Settings

---

\* SNMP Version:

\* SNMP RO Community:

SNMP Username

---

: a mesma ação é aplicável para adicionar grupos de segurança a uma instância LDAP. Na GUI do ISE, selecione **Administration > Identity Management: External Identity Sources > LDAP > LDAP instance name > tab: Groups > Add > Select Groups From Directory**.

---

## Etapa 6. Criar o perfil de autenticação do certificado

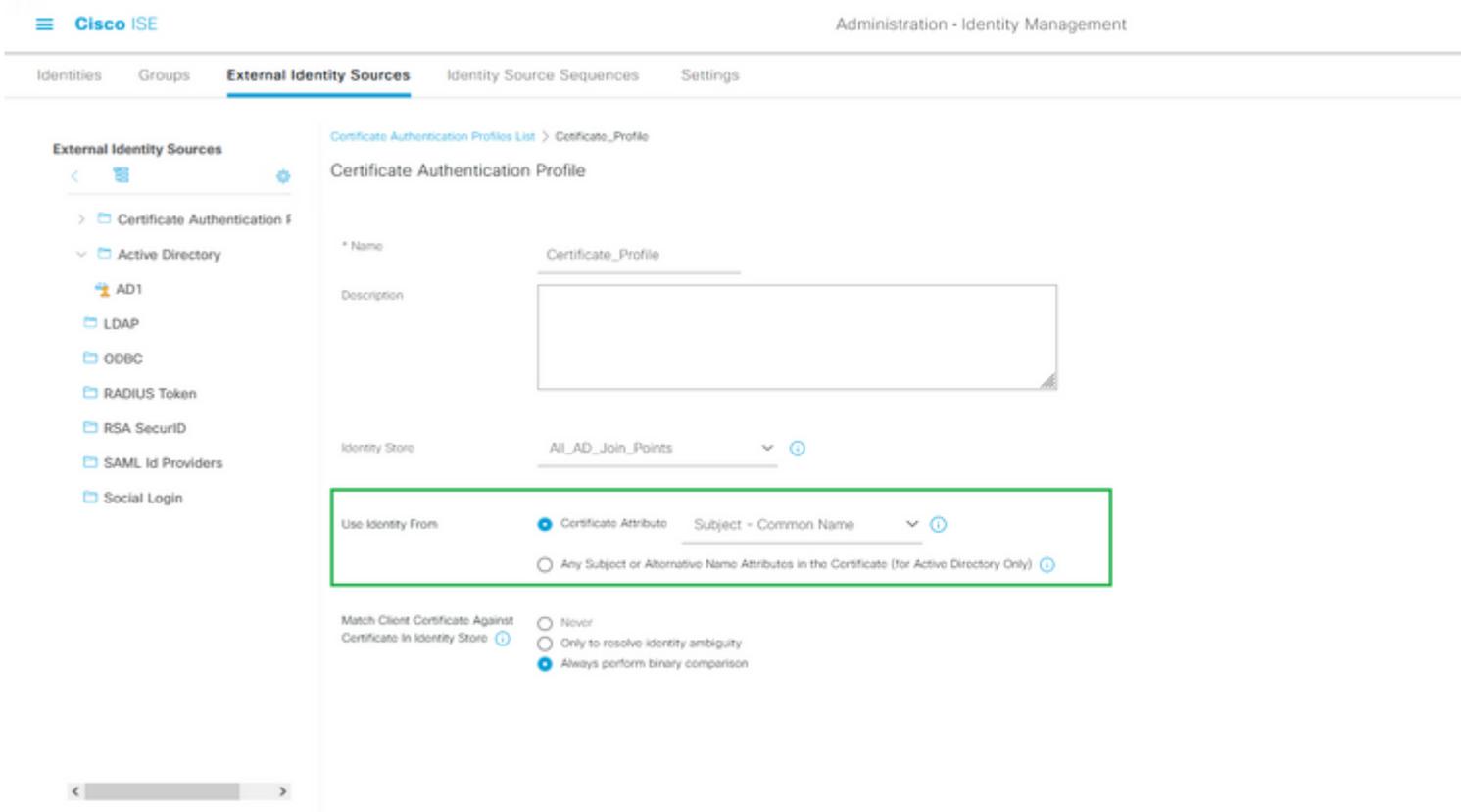
A finalidade do Perfil de autenticação de certificado é informar ao ISE qual campo de certificado a identidade (máquina ou usuário) pode ser encontrada no certificado do cliente (certificado de identidade final) apresentado ao ISE durante o EAP-TLS (também durante outros métodos de autenticação baseados em certificado). Estas configurações estão associadas à Política de Autenticação para autenticar a identidade. Na GUI do ISE, navegue até **Administration > Identity Management: External Identity Sources > Certificate Authentication Profile** e clique em **Add**.

**Usar identidade de** é usado para escolher o atributo de certificado a partir do qual um campo específico da identidade pode ser encontrado. As opções são:

- Subject - Common Name
- Subject Alternative Name
- Subject - Serial Number
- Subject
- Subject Alternative Name - Other Name
- Subject Alternative Name - EMail
- Subject Alternative Name - DNS

Se o armazenamento de identidades precisar ser apontado para o Ative Directory ou LDAP (fonte de identidade externa), um recurso chamado [Comparação Binária](#) poderá ser usado. A Comparação Binária executa uma pesquisa da identidade no Ative Directory obtida do certificado do cliente da seleção **Usar identidade de**, que ocorre durante a fase de autenticação do ISE. Sem a Comparação binária, a identidade é simplesmente obtida do certificado do cliente e não é pesquisada no Ative Directory até a fase de Autorização do ISE quando um Grupo externo do Ative Directory é usado como uma condição ou qualquer outra condição que precisaria ser executada externamente para o ISE. Para usar a Comparação binária, no **Repositório de identidades** escolha a fonte de identidade externa (Ative Directory ou LDAP) onde a conta de identidade final pode ser encontrada.

Este é um exemplo de configuração quando a identidade está localizada no campo Nome Comum (CN) do certificado do cliente, com Comparação Binária habilitada (opcional):



Perfil de autenticação de certificado

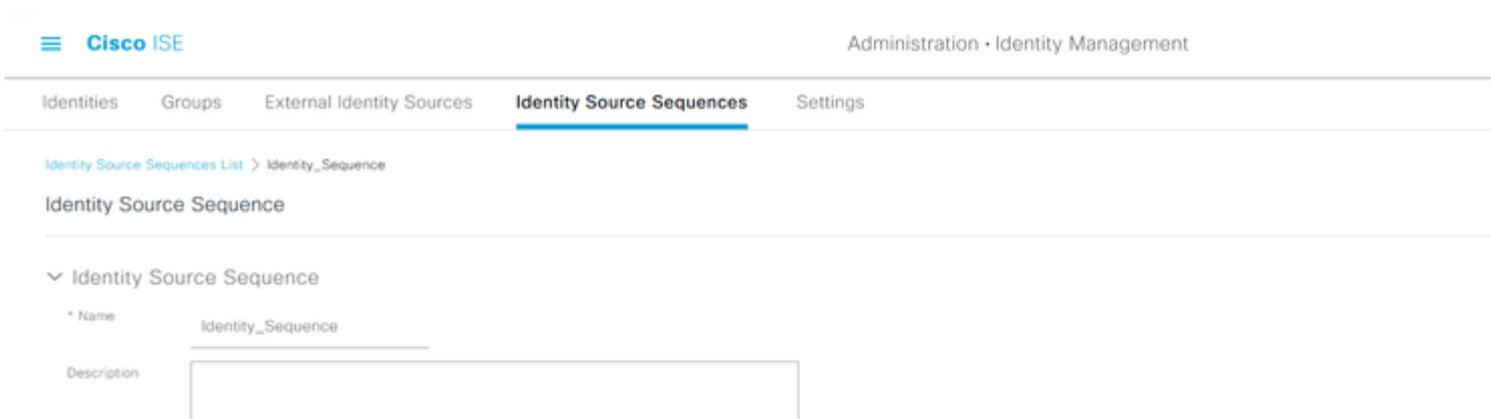
Mais informações podem ser encontradas no Guia do Administrador do Cisco Identity Services Engine, Versão 3.1 > Capítulo: Configuração básica > Cisco ISE CA Service > Configurar o Cisco ISE para usar certificados para autenticar dispositivos pessoais > [Criar um perfil de autenticação de certificado para autenticação baseada em TLS](#).

### Passo 7. Adicionar a uma sequência de origem de identidade

A sequência de origem de identidade pode ser criada na GUI do ISE. Navegue até **Administration > Identity Management**. Sob **Identity Source Sequences**, clique em **Add**.

A próxima etapa é adicionar o perfil de autenticação de certificado a uma sequência de origem de identidade, que concede a capacidade de incluir vários pontos de união do Ative Diretory ou agrupar uma combinação de fontes de identidade internas/externas, conforme desejado, que se vinculam à política de autenticação sob o Use coluna.

O exemplo mostrado aqui permite que a pesquisa seja executada primeiro no Ative Diretory e, em seguida, se o usuário não for encontrado, ele pesquisará em um servidor LDAP em seguida. Para várias origens de identidade. sempre assegure a **Treat as if the user was not found and proceed to the next store in the sequence** está marcada. Isso ocorre para que cada origem/servidor de identidade seja verificado durante a solicitação de autenticação.



---

: no mínimo, você deve habilitar o EAP-TLS já que o ISE e nosso solicitante se autenticam via EAP-TLS neste exemplo de configuração.

---

Dictionaryes Conditions **Results**

Allowed Protocols Services List > New Allowed Protocols Service

**Allowed Protocols**

Name Allowed\_Protocols

Description

▼ Allowed Protocols

Authentication Bypass

Process Host Lookup ⓘ MAB

Authentication Protocols

Allow PAP/ASCII

Allow CHAP

Allow MS-CHAPv1

Allow MS-CHAPv2

Allow EAP-MD5

Allow EAP-TLS

Allow LEAP

Allow PEAP

Allow EAP-FAST

Allow EAP-TTLS

Allow TEAP

Preferred EAP Protocol: EAP-TLS ⓘ

EAP-TLS L-bit ⓘ

Allow weak ciphers for EAP ⓘ

Require Message-Authenticator for all RADIUS Requests ⓘ

*Protocolos para permitir que o ISE use durante a solicitação de autenticação ao solicitante do ponto final*

**Observação:** o uso do Preferred EAP Protocol definido com o valor de EAP-TLS faz com que o ISE solicite o protocolo EAP-TLS como o primeiro protocolo oferecido ao solicitante IEEE 802.1x do endpoint. Essa configuração é útil se você pretende se autenticar via EAP-TLS frequentemente na maioria dos endpoints autenticados com o ISE.

## Etapa 9. Criar o Perfil de Autorização

O último elemento de política necessário para criar é o perfil de autorização, que se vincula à política de autorização e fornece o nível desejado de acesso. O Perfil de Autorização está associado à Diretiva de Autorização. Para configurá-lo a partir da GUI do ISE, navegue até **Policy > Policy Elements: Results > Authorization > Authorization Profiles** e clique em **Add**.

O perfil de autorização contém uma configuração que resulta em atributos que são passados do ISE para o NAD para uma determinada sessão RADIUS, na qual esses atributos são usados para alcançar o nível desejado de acesso à rede.

Como mostrado aqui, ele simplesmente passa RADIUS Access-Accept como o Tipo de Acesso, no entanto, itens adicionais podem ser usados na autenticação inicial. Observe os detalhes do atributo na parte inferior, que contém o resumo dos atributos que o ISE envia ao NAD quando ele corresponde a um determinado perfil de autorização.

Dictionaryes Conditions **Results**

Authorization Profiles > New Authorization Profile

Authentication >

. Elas são ativadas por padrão no ISE 3.x. Quando você instala o ISE, sempre há um conjunto de políticas definido, que é o conjunto de políticas padrão. O conjunto de políticas padrão contém regras de autenticação, autorização e política de exceção predefinidas e padrão.

Os conjuntos de políticas são configurados hierarquicamente, o que permite que o administrador do ISE agrupe políticas semelhantes, em termos de intenção, em conjuntos diferentes para uso em uma solicitação de autenticação. As políticas de personalização e agrupamento são praticamente ilimitadas. Dessa forma, um conjunto de políticas pode ser usado para autenticação de ponto final sem fio para acesso à rede, enquanto outro conjunto de políticas pode ser usado para autenticação de ponto final com fio para acesso à rede ou para qualquer outra forma exclusiva e diferenciada de gerenciar políticas.

O Cisco ISE pode avaliar os conjuntos de políticas e as políticas dentro do usa a abordagem de cima para baixo, para primeiro corresponder a um determinado conjunto de políticas quando todas as condições desse conjunto são avaliadas como Verdadeiro; no qual o ISE avalia ainda mais as políticas de autenticação e de autorização dentro do conjunto que corresponde ao conjunto de políticas, como a seguir:

1. Avaliação das Condições do Conjunto de Políticas e do Conjunto de Políticas
2. Políticas de autenticação no conjunto de políticas correspondente
3. Política de Autorização - Exceções Locais
4. Política de autorização - Exceções globais
5. Diretivas de Autorização

As exceções de política existem globalmente para todos os conjuntos de políticas ou localmente dentro de um conjunto de políticas específico. Essas Exceções de política são tratadas como parte das Políticas de autorização, já que lidam com quais permissões ou resultados são dados para acesso à rede para um determinado cenário temporário.

A próxima seção aborda como combinar os elementos de configuração e política para vincular às políticas de autenticação e autorização do ISE para autenticar um endpoint via EAP-TLS.

## **Etapa 10. Criar o conjunto de políticas**

Um conjunto de políticas é um contêiner hierárquico que consiste em uma única regra definida pelo usuário que indica o protocolo ou a sequência de servidor permitidos para acesso à rede, bem como políticas de autenticação e autorização e exceções de políticas, tudo também configurado com regras baseadas em condições definidas pelo usuário.

Para criar um conjunto de políticas a partir da GUI do ISE, navegue até **Policy > Policy Set** e clique no ícone de mais (+) no canto superior esquerdo, como mostrado nesta imagem.

## Policy Sets

Status	Policy Set Name	Description	Conditions

Adicionando um novo conjunto de políticas

O conjunto de políticas pode vincular/combina esse elemento de política configurado anteriormente e é usado para determinar qual conjunto de políticas deve ser correspondido em uma determinada solicitação de autenticação RADIUS (solicitação de acesso):

- Ligação: serviços de protocolos permitidos

Status	Policy Set Name	Description	Conditions
1) <span>+</span>	2) EAP-TLS Example		3) AND Radius-Service-Type EQUALS Framed Network Access-Protocol EQUALS RADIUS
	Default	Default policy set	

Definindo Condições do Conjunto de Políticas e Lista de Protocolos Permitidos

Este exemplo usa atributos e valores específicos que apareceriam na sessão RADIUS para aplicar o IEEE 802.1x (atributo enquadrado), mesmo que seja possivelmente redundante para reforçar novamente o protocolo RADIUS. Para obter os melhores resultados, use apenas atributos exclusivos de sessão RADIUS que sejam aplicáveis ao propósito desejado, como Grupos de dispositivos de rede ou específicos para 802.1x com fio, 802.1x sem fio ou 802.1x com fio e 802.1x sem fio.

Mais informações sobre Conjuntos de Políticas no ISE podem ser encontradas nas seções Guia do Administrador do Cisco Identity Services Engine, Release 3.1 > Chapter: Segmentation > [Policy Sets](#), [Authentication Policies](#) e [Authorization Policies](#).

## Etapa 11. Criar uma política de autenticação

Dentro do Conjunto de políticas, a Política de autenticação vincula/combina esses elementos de política previamente configurados para serem usados com condições para determinar quando uma Regra de autenticação deve ser correspondida.

- Ligação: Perfil de Autenticação de Certificado ou Sequência de Origem da Identidade.

Status	Rule Name	Conditions
1) <span>+</span>	Authentication Policy (2)	

- Contém se a autenticação foi bem-sucedida ou não.
  - Em um cenário de trabalho, o valor é: 5200 Autenticação bem-sucedida.
- Nome de usuário
    - Isso inclui a identidade final que foi extraída do certificado de cliente que foi apresentado ao ISE.
    - Em um cenário de trabalho, esse é o nome de usuário do usuário conectado ao endpoint (ou seja, employee1 na imagem anterior).
- ID do endpoint
    - Para Com fio/Sem fio, esse valor é o endereço MAC da placa de rede (NIC) do endpoint.
    - Em um cenário de trabalho, ele se torna o endereço MAC do ponto final, a menos que a conexão seja por VPN, caso em que pode ser o endereço IP do ponto final.
- Política de autenticação
    - Mostra a política de autenticação correspondente para a sessão fornecida com base em atributos de sessão que correspondem às condições da política.
    - Em um cenário de trabalho, essa é a política de autenticação esperada conforme configurada.
    - Se você vir outra política, significa que a política esperada quando comparada às condições na política não foi avaliada como verdadeira. Nesse caso, revise os atributos da sessão e verifique se cada política contém condições diferentes, porém exclusivas, para cada política.
- Política de Autorização
    - Mostra a política de autorização correspondida para a sessão fornecida com base nos atributos de sessão que correspondem às condições da política.
    - Em um cenário de trabalho, essa é a política de autorização esperada conforme configurada.
    - Se você vir outra política, significa que a política esperada, quando comparada às condições na política, não foi avaliada como verdadeira. Nesse caso, revise os atributos da sessão e certifique-se de que cada política contenha condições diferentes, porém exclusivas, para cada política.
- Resultado da Autorização
    - Com base na Política de autorização correspondente, mostra o Perfil de autorização que foi usado na sessão fornecida.
    - Em um cenário de trabalho, esse é o mesmo valor configurado na política. É bom revisar para fins de auditoria e garantir que o perfil de autorização correto foi configurado.
- **Servidor de políticas**
    - Isso inclui o nome de host do PSN (Policy Service Node, nó de serviço de política) do ISE que foi envolvido na tentativa de autenticação.
    - Em um cenário de trabalho, você vê apenas as autenticações que vão para o primeiro nó PSN como configurado no NAD (também conhecido como dispositivo de borda), a menos que o PSN não estivesse operacional ou que ocorresse failover, como devido a uma latência mais alta do que o esperado ou se ocorrer um tempo limite de autenticação.
- método de autenticação
    - Mostra o método de autenticação que foi usado na sessão fornecida. Para este exemplo, você vê o valor como **dot1x**.
    - Em um cenário de trabalho, com base nesse exemplo de configuração, você verá o valor como **dot1x**. Se você vir outro valor, isso pode significar que dot1x falhou ou não foi tentado.
- Protocolo de autenticação
    - Mostra o método de autenticação que foi usado na sessão fornecida. Para este exemplo, você vê

o valor como EAP-TLS.

- Em um cenário de trabalho, com base nesse exemplo de configuração, você sempre verá o valor como EAP-TLS. Se você vir outro valor, o suplicante e o ISE não negociaram com êxito o EAP-TLS.
- Dispositivo de rede
  - Mostra o nome do dispositivo de rede, conforme configurado no ISE, para o NAD (também conhecido como o dispositivo de borda) envolvido na tentativa de autenticação entre o ponto de extremidade e o ISE.
  - Em um cenário de trabalho, esse nome é sempre fornecido na interface do usuário do ISE: **Administration > System: Network Devices**. Com base nessa configuração, o endereço IP do NAD (também conhecido como o dispositivo de borda) é usado para determinar de qual dispositivo de rede veio a autenticação e que está incluído no atributo de sessão de endereço IPv4 do NAS.

De forma alguma essa é uma lista completa de todos os atributos de sessão possíveis a serem analisados para solução de problemas ou outras finalidades de visibilidade, já que há outros atributos úteis a serem verificados. Recomenda-se revisar todos os atributos da sessão para começar a se familiarizar com todas as informações. Você pode ver incluir o lado direito na seção Etapas, que mostra as operações ou o comportamento adotado pelo ISE.

## Problemas Comuns e Técnicas para Troubleshooting

Essa lista inclui alguns problemas comuns e conselhos para a solução de problemas, e de forma alguma deve ser uma lista completa. Em vez disso, use isso como um guia e desenvolva suas próprias técnicas para solucionar problemas quando o ISE estiver envolvido.

Problema: ocorreu uma falha de autenticação (**falha na autenticação 5400**) ou qualquer outra tentativa de autenticação malsucedida.

- Se uma falha de autenticação for encontrada, clique no ícone **details** que fornece informações sobre por que a autenticação falhou e as etapas executadas. Isso inclui o motivo da falha e a possível causa raiz.
- Como o ISE toma a decisão sobre o resultado da autenticação, ele tem as informações para entender o motivo pelo qual a tentativa de autenticação não foi bem-sucedida.

Problema: a autenticação não é concluída com êxito e o motivo da falha mostra "5440 Endpoint abandonou a sessão EAP e iniciou uma nova" ou "5411 SupPLICANT parou de responder ao ISE".

- Essa razão de falha indica que a comunicação RADIUS não foi concluída antes do tempo limite. Como o EAP está entre o endpoint e o NAD, você precisa verificar o tempo limite que é usado no NAD e garantir que ele esteja definido por pelo menos cinco segundos.
- Se cinco segundos não forem suficientes para resolver esse problema, é recomendável aumentá-lo em cinco segundos algumas vezes e testar novamente para verificar se essa técnica resolve o problema.
- Se o problema não for resolvido a partir das etapas anteriores, é recomendável garantir que a autenticação seja tratada pelo mesmo nó ISE PSN correto e que o comportamento geral não indique um comportamento anormal, como latência mais alta que o normal entre os nós NAD e ISE PSN.
- Além disso, é uma boa ideia verificar se o endpoint envia o certificado do cliente por meio da captura de pacotes. Se o ISE não receber o certificado do cliente, o endpoint (certificados do usuário) não poderá confiar no certificado de autenticação EAP do ISE. Se for considerado verdadeiro, importe a

Cadeia de Autoridades de Certificação nos armazenamentos de certificados corretos (CA raiz = CA raiz confiável | AC intermediário = AC intermediário fidedigno).

Problema: a autenticação foi bem-sucedida, mas não corresponde à política de autenticação e/ou autorização correta.

- Se você encontrar uma solicitação de autenticação bem-sucedida, mas que não corresponda às regras de Autenticação e/ou Autorização corretas, é recomendável revisar os atributos da sessão para garantir que as condições usadas sejam precisas e estejam presentes na sessão RADIUS.
- O ISE avalia essas políticas de cima para baixo (com exceção das políticas de postura). Você precisa primeiro determinar se a política que foi correspondida estava acima ou abaixo da política desejada a ser correspondida. A política de autenticação é avaliada primeiro e independentemente das políticas de autorização. Se a Política de autenticação for correspondida corretamente, ele terá 22037 Autenticação aprovada em Detalhes da autenticação na seção à direita chamada Etapas.
- Se a política desejada estiver acima da política correspondente, isso significa que a soma das condições na política desejada não foi avaliada como verdadeira. Ele revisa todos os atributos e valores na condição e na sessão para garantir que ela exista e que nenhum erro de ortografia esteja presente.
- Se a política desejada estiver abaixo da política correspondida, significa que outra política (acima) foi correspondida em vez da política desejada. Isso pode significar que os valores de condição não são específicos o suficiente, que as condições são duplicadas em outra política ou que a ordem da política não está correta. Embora a solução de problemas se torne mais difícil, é recomendável começar a analisar as políticas para determinar o motivo pelo qual a política desejada não foi correspondida. Isso ajuda a identificar as próximas ações a serem tomadas.

Problema: a identidade ou o nome de usuário usado durante a autenticação não era o valor esperado.

- Quando isso ocorre, se o ponto final envia o certificado do cliente, é mais provável que o ISE não use o campo de certificado correto no Modelo de autenticação de certificado, que é avaliado durante a Fase de autenticação.
- Revise o certificado do cliente para localizar o campo exato em que a identidade/nome de usuário desejado existe e verifique se o mesmo campo está selecionado em: **ISE UI: Administration > Identity Management: External Identity Sources > Certificate Authentication Profile > (certificate authentication profile used in the Authentication Policy).**

Problema: A autenticação não foi bem-sucedida com o motivo da falha **12514 o EAP-TLS falhou no handshake SSL/TLS devido a uma CA desconhecida na cadeia de certificados do cliente.**

- Isso poderá ocorrer se o certificado do cliente tiver um certificado na cadeia de CA que não seja Confiável na interface do usuário do ISE: **Administration > System: Certificates > Trusted Certificates.**
- Isso normalmente pode ocorrer quando o certificado do cliente (no ponto de extremidade) tem uma cadeia de CA que é diferente da cadeia de CA do certificado que é assinada ao ISE para autenticação EAP.
- Para resolução, verifique se a cadeia de certificados de CA do cliente é confiável no ISE e se a cadeia de certificados de CA do servidor de autenticação EAP do ISE é confiável no ponto de extremidade.

- Para o SO Windows e o Chrome, navegue até Start > Run MMC > Add/Remove Snap-In > Certificates > User Certificates.
- Para Firefox: importe a cadeia de CA (não o certificado de identidade final) para ser confiável para o servidor Web.

## Informações Relacionadas

- Cisco Identity Services Engine > [Guias de instalação e atualização](#)
- Cisco Identity Services Engine > [Guias de configuração](#)
- Cisco Identity Services Engine > [Informações de compatibilidade](#)
- Guia do administrador do Cisco Identity Services Engine, versão 3.1 > Capítulo: Acesso seguro > [Definição de dispositivos de rede no Cisco ISE](#)
- Guia do Administrador do Cisco Identity Services Engine, Versão 3.1 > Capítulo: Segmentação > [Conjuntos de Políticas](#)
- Guia do Administrador do Cisco Identity Services Engine, Versão 3.1 > Capítulo: Segmentação > [Políticas de autenticação](#)
- Guia do Administrador do Cisco Identity Services Engine, Versão 3.1 > Capítulo: Segmentação > [Políticas de Autorização](#)
- Cisco Identity Services Engine > Guias de configuração > [Integração do Ative Directory com o Cisco ISE 2.x](#)
- Guia do Administrador do Cisco Identity Services Engine, Versão 3.1 > Capítulo: Segmentação > Serviço de Acesso à Rede > [Acesso à Rede para Usuários](#)
- Guia do Administrador do Cisco Identity Services Engine, Versão 3.1 > Capítulo: Configuração básica > [Gerenciamento de certificados no Cisco ISE](#)
- Guia do Administrador do Cisco Identity Services Engine, Versão 3.1 > Capítulo: Configuração básica > Cisco ISE CA Service > Configurar o Cisco ISE para usar certificados para autenticar dispositivos pessoais > [Criar um perfil de autenticação de certificado para autenticação baseada em TLS](#)
- Cisco Identity Services Engine > Exemplos de Configuração e Notas Técnicas > [Configurar o Portal de Provisionamento de Certificado do ISE 2.0](#)
- Cisco Identity Services Engine > Exemplos de Configuração e Notas Técnicas > [Instalar um Certificado de Terceiros Assinado pela CA no ISE](#)
- Wireless LAN (WLAN) > Exemplos de Configuração e Notas Técnicas > [Entender e configurar o EAP-TLS usando WLC e ISE](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

## 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.