# Instalação, renovação e solução de problemas de certificados digitais SSL no Cisco ISE

## Introduction

Este documento contém as etapas necessárias para a instalação, renovação e soluções de certificado SSL para problemas de certificado mais comuns observados em um Identity Services Engine.  Este documento fornece as etapas recomendadas e a lista de verificação de problemas comuns a serem verificados e solucionados antes de você começar a solucionar problemas e ligar para o Suporte Técnico da Cisco.

Essas soluções vêm diretamente das solicitações de serviço que o Suporte Técnico da Cisco resolveu. Se a sua rede estiver ativa, certifique-se de que você entendeu o impacto potencial das etapas que você tomou para resolver os problemas.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- GUI do Identity Service Engine

### Componentes Utilizados

As informações neste documento são baseadas na seguinte versão de software:

- Cisco Identity Service Engine 2.7

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

Um certificado é um documento eletrônico que identifica um indivíduo, um servidor, uma empresa ou outra entidade e associa essa entidade a uma chave pública. Um certificado autoassinado é assinado por seu próprio criador. Os certificados podem ser autoassinados ou assinados digitalmente por uma autoridade de certificação externa (AC). Um certificado digital assinado por CA é considerado um padrão do setor e mais seguro.

Os certificados são usados em uma rede para fornecer acesso seguro. O Cisco ISE usa certificados para comunicação entre nós e para comunicação com servidores externos, como o servidor Syslog, o servidor de feeds e todos os portais do usuário final (portais de convidados, patrocinadores e dispositivos pessoais). Os certificados identificam um nó do Cisco ISE para um

endpoint e protegem a comunicação entre esse endpoint e o nó do Cisco ISE. Os certificados são usados para todas as comunicações HTTPS e para a comunicação EAP (Extensible Authentication Protocol).

# Configurar

Os seguintes guias explicam como importar e substituir certificados:

### Importar um certificado de sistema

https://www.cisco.com/c/en/us/td/docs/security/ise/2-7/admin_guide/workflow/html/b_basic_setup_2_7.html#ID547

### Substituir um certificado expirado

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/116977-technote-ise-cert-00.html#anc5

# Problemas comuns

## Cenário 1: não é possível substituir um certificado de portal que expira em um nó do ISE

#### Erro

Ao vincular o novo certificado do portal ao CSR, o processo de associação de certificado falha com o erro mostrado abaixo:

*Internal Error. Peça ao administrador do ISE para verificar os registros para obter mais detalhes*

Os motivos mais comuns para esse erro são:

- O novo certificado tem o mesmo nome de assunto do certificado existente

- Importar um certificado renovado que esteja usando a mesma chave privada de um certificado existente

#### Solução

1. Atribuir temporariamente o uso do portal a outro certificado no mesmo nó
2. Excluir o certificado do portal que expira
3. Instalar o novo certificado do portal e atribuir o uso do portal

Por exemplo, se você quiser atribuir temporariamente o uso do portal a um certificado existente com o uso da autenticação EAP, siga as etapas abaixo:

**Etapa 1.** Selecione e edite o certificado com o uso da Autenticação EAP, adicione a função Portal em Uso e Salvar

**Etapa 2.** Excluir o certificado do portal expirando

**Etapa 3.** Carregue o novo certificado do portal sem selecionar qualquer função (em Uso) e Enviar

**Etapa 4.** Selecione e edite o novo certificado do portal, atribua a função Portal em Uso e Salvar

## Cenário 2: Não é possível gerar dois CSR para o mesmo nó ISE com uso multiuso

### Erro

A nova criação de CSR para o mesmo nó com uso multiuso falha com o erro:
*Já existe outro certificado com o mesmo nome amigável. Os nomes amigáveis devem ser exclusivos.*

### Solução

Os nomes amigáveis de CSR são codificados para cada nó ISE, portanto, não permite criar 2 CSRs para o mesmo nó com uso multiuso. O caso de uso está em um nó específico, há um certificado assinado por CA usado para o uso de autenticação Admin e EAP e outro certificado assinado por CA usado para o uso de SAML e Portal e ambos os certificados expirarão.

In this scenario:

**Etapa 1.** Gerar o primeiro CSR com uso multiuso

**Etapa 2.** Vincule o certificado assinado pela CA ao primeiro CSR e atribua a função de autenticação Admin e EAP

**Etapa 3.** Gerar o segundo CSR com uso multiuso

**Etapa 4.** Vincule o certificado assinado pela CA ao segundo CSR e atribua SAML e função de portal

## Cenário 3: Não é possível vincular o certificado assinado pela CA para uso do portal ou não é possível atribuir a etiqueta do portal ao certificado e obter um erro

### Erro

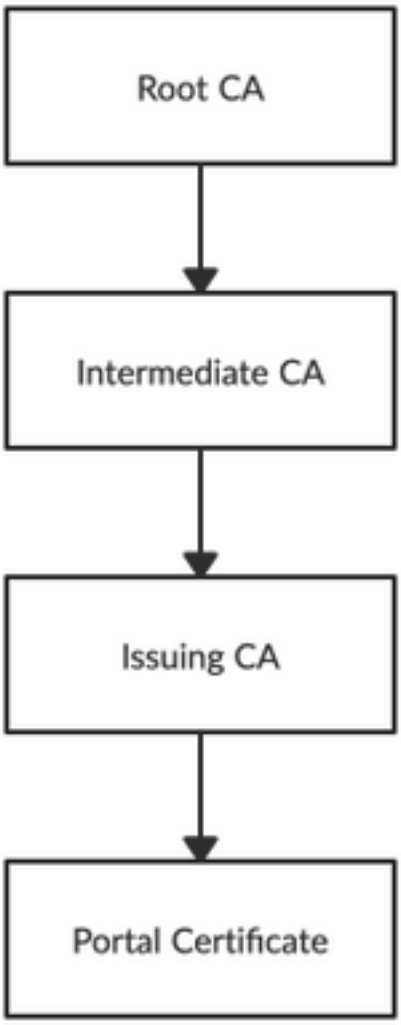
A vinculação do certificado assinado pela CA para o uso do portal gera o erro:

*Há um ou mais certificados confiáveis que fazem parte da cadeia de certificados do sistema de portal ou são selecionados com função de autenticação de administrador baseada em certificado com o mesmo nome de assunto, mas com um número de série diferente. Importação/Atualização cancelada. Para a importação/atualização bem-sucedida, você precisa desativar a função de autenticação de administrador baseada em carrinho de um certificado confiável duplicado ou alterar a função do portal do certificado do sistema que contém o certificado confiável duplicado em sua cadeia.*

### Solução

**Etapa 1.** Verifique a cadeia de certificados do certificado assinado pela AC (para uso do portal) e, no repositório de certificados confiáveis, verifique se você tem algum certificado duplicado da cadeia de certificados.
**Etapa 2.** Remova o certificado duplicado ou desmarque a caixa de seleção **Confiar na autenticação de administrador baseada em certificado** do certificado duplicado.

Por exemplo, o certificado do portal assinado pela CA tem a cadeia de certificados abaixo:




Verifique se você tem algum certificado duplicado para qualquer um dos 3 certificados CA na cadeia de certificados (pode ser um certificado expirado) e remova o certificado duplicado do repositório de Certificados Confiáveis.

## Cenário 4 : Não é possível eliminar o certificado autoassinado predefinido expirado do Arquivo de Certificados Fidedignos

### Erro

A exclusão do certificado autoassinado padrão expirado do repositório de certificados confiáveis resulta no erro:
*Não é permitido desativar ou eliminar ou confiar certificado, uma vez que está a ser referenciado em Certificados do Sistema E/OU Destino de Syslog Seguro em Destinos de Registro Remoto.*

### Solução

1. Verifique se o certificado autoassinado padrão expirado não está associado a nenhum Destino de Registro Remoto existente. Isso pode ser verificado em ***Administration > System > Logging > Remote Logging Targets > Select and Edit SecureSyslogCollector***
2. Verifique se o certificado autoassinado padrão expirado não está associado a nenhuma função específica (uso). isso pode ser verificado em ***Administração > Sistema > Certificados > Certificados do Sistema***.

Se o problema persistir, entre em contato com o TAC.

## Cenário 5 : Não é possível vincular o CA assinado com o certificado pxGrid ao CSR em um nó ISE

### Erro

Ao vincular o novo certificado pxGrid ao CSR, o processo de associação de certificado falha com erro:

***O certificado para pxGrid deve conter autenticação de cliente e servidor na extensão Extended Key Usage (EKU).***

### Solução

Certifique-se de que o certificado pxGrid assinado pela AC tem de ter a Autenticação de Servidor Web TLS (1.3.6.1.5.5.7.3.1) e a Autenticação de Cliente Web TLS (1.3.6.1.5.7.3.2) utilização de chave estendida, porque é utilizado para a autenticação de cliente e servidor (para proteger a comunicação entre o cliente e o servidor pxGrid)

Link de referência: https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_011010.html

## Cenário 6 : Não é possível excluir o certificado autoassinado padrão expirado do Repositório de certificados confiáveis devido à configuração do perfil LDAP ou do RA SCEP existente

### Erro

A exclusão do certificado autoassinado padrão expirado do repositório de certificados confiáveis resulta no erro:

Não foi possível excluir o certificado de confiança porque ele está sendo referenciado em outro lugar, possivelmente de um perfil RA SCEP ou de uma origem de identidade LDAP

* Certificado de servidor autoassinado padrão

Para excluir o(s) certificado(s), exclua o perfil RA do SCEP ou edite a origem da identidade LDAP para não usar esse certificado.

### Solução

1. Navegue até *Administration > Identity Management > External Identity Sources > LDAP > Server Name > Connection*
2. Certifique-se de que a CA raiz do servidor LDAP não está a utilizar o "certificado de servidor autoassinado predefinido"
3. Se o servidor LDAP não estiver usando o certificado necessário para uma conexão segura, navegue para *Administração > Sistema > Certificados > Autoridade de Certificação > Configurações de CA externa > Perfis de RA do SCEP*
4. Certifique-se de que qualquer um dos perfis de RA SCEP não esteja usando o certificado autoassinado padrão

## Outros recursos

### Como instalar um certificado curinga
https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_0111.html

### Gerenciar certificados do ISE
https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_0111.html

### Instalar um certificado CA de terceiros no ISE
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-software/200295-Install-a-3rd-party-CA-certificate-in-IS.html