Preparar o Cisco ISE para Aut. de EKU do Cliente em Certificados CA Públicos

Contents

Introdução

Este documento descreve o impacto sobre os serviços do ISE devido a futuras alterações em certificados TLS emitidos por autoridades de certificação públicas com EKU de autenticação de cliente.

Informações de Apoio

Os certificados digitais são credenciais eletrônicas emitidas por Autoridades de Certificação (CAs) confiáveis que protegem a comunicação entre servidores e clientes, garantindo a autenticação, a integridade dos dados e a confidencialidade. Estes certificados contêm campos de Uso Estendido de Chave (EKU) que definem sua finalidade:

- EKU de Autenticação do Servidor (id-kp-serverAuth): Usado quando um servidor apresenta seu certificado para comprovar a identidade
- EKU de Autenticação de Cliente (id-kp-clientAuth): Usado em conexões TLS mútuas (mTLS) onde ambas as partes se autenticam

Tradicionalmente, um único certificado pode conter EKUs de Autenticação de Servidor e de Cliente, permitindo que ele sirva a duas finalidades. Isso é particularmente importante para produtos como o Cisco ISE que atuam como servidor e cliente em diferentes cenários de conexão.

Definição do problema

Mudança de política do programa Chrome Root

A partir de maio de 2026, muitas Autoridades de Certificação Públicas (CAs) interromperão a emissão de certificados TLS (Transport Layer Security) que incluem o EKU (Extended Key Usage) de Autenticação de Cliente. Certificados emitidos recentemente normalmente incluem somente EKU de Autenticação de Servidor.

Principais requisitos da política

- As CAs de raiz públicas devem declarar Uso Estendido de Chave (EKU) SOMENTE para Autenticação de Servidor (id-kp-serverAuth)
- Os certificados devem incluir SOMENTE EKU de Autenticação de Servidor.
- É proibido incluir EKU de Autenticação de Cliente nestes certificados
- As CAs raiz que continuam a emitir certificados com EKU de autenticação de cliente são removidas do Chrome Root Store
- Não há mais CAs raiz de uso misto para certificados TLS de servidor público
- Cronograma de aplicação: Março de 2027.

Cronograma de Resposta de CA Pública

- outubro de 2025: Muitas CAs públicas (DigiCert, Sectigo, SSL) começaram a emitir certificados somente de servidor por padrão.
- Maio de 2026: Muitos servidores de CA públicos param de emitir certificações EKU de

Autenticação de Cliente
- Março de 2027: A política do programa Chrome Root torna-se totalmente eficaz

---

Note: Esta política se aplica somente a certificados emitidos por autoridades de certificação públicas. PKI particular e certificados autoassinados não são afetados por esta política.

Como isso afeta o Cisco ISE

Produtos afetados

Todas as versões do Cisco ISE são afetadas:

- ISE 3.1
- ISE 3.2
- ISE 3.3
- ISE 3.4
- ISE 3.5

Note: As versões do Cisco ISE 2.x também são afetadas; no entanto, não há correções planejadas, pois essas versões chegaram ao fim da vida útil (EOL).

Função dupla do Cisco ISE

O ISE atua como servidor e cliente em vários cenários de conexão, exigindo certificados com EKUs de autenticação de servidor e cliente.

Cisco ISE como um servidor (EKU de autenticação de servidor necessário):

- PxGrid
- Serviço de mensagens do ISE

Cisco ISE como um cliente (EKU de autenticação do cliente necessário):

- TC-NAC
- Syslog seguro
- LDAPS
- DTLS Radius

Casos de uso específicos afetados

A tabela abaixo resume os serviços do Cisco ISE que podem ser afetados pelas próximas

alterações de EKU de Autenticação de Cliente, juntamente com o impacto esperado para cada serviço.

Serviço	Impacto
pxGrid	Os certificados pxGrid são usados para comunicação entre nós do ISE e integrações pxGrid externas. Embora integrações pxGrid externas exijam apenas EKU de autenticação de servidor, o Cisco ISE atualmente exige certificados pxGrid importados para conter EKU de autenticação de servidor e EKU de autenticação de cliente devido a uma restrição de interface do usuário. Como resultado, os certificados pxGrid emitidos por CA pública são normalmente implantados com ambos os EKUs.
Serviço de mensagens do ISE (IMS)	O IMS é usado para comunicação de back-end entre serviços internos do ISE. O Cisco ISE atualmente requer que os certificados IMS contenham tanto o EKU de autenticação de servidor quanto o EKU de autenticação de cliente. Os certificados renovados por uma CA pública com EKU de autenticação de servidor somente não podem ser usados para IMS, o que pode resultar em falhas na comunicação interna do ISE.
TC-NAC	Se o certificado Admin contiver somente EKU de Autenticação de Servidor, a autenticação baseada em certificado para TC-NAC poderá ser afetada quando o modo FIPS estiver habilitado ou quando Tenable estiver configurado com mTLS (Introduzido nas versões 3.4P3 e 3.5 do ISE).
Syslog seguro	
LDAPs	
DTLS RADIUS	

⚠ Caution: Os clientes devem verificar o tipo de certificado usado por qualquer cliente pxGrid externo. Após a renovação, os certificados assinados por CA pública não podem mais incluir EKU de autenticação de cliente. As integrações de cliente pxGrid externo devem incluir o EKU de Autenticação de Cliente ao se comunicar com o ISE ou a conexão será rejeitada.

Sintomas do problema

Após a implantação de certificados EKU de autenticação de servidor somente no Cisco ISE, os clientes observarão falhas de importação de certificado na GUI do Cisco ISE ao tentar carregar pxGrid ou certificados do ISE Messaging Service (IMS) que não atendam aos requisitos atuais de Uso Estendido de Chave (EKU) para o serviço selecionado.

Um exemplo da mensagem de erro exibida na GUI é mostrado abaixo.

Recomendações

Auditoria de Certificados Atuais (OBRIGATÓRIO PRIMEIRO PASSO)

- Preparar um inventário de todos os certificados TLS públicos para identificar quais certificados contêm o EKU de Autenticação de Cliente
- Uso do certificado do documento: identifique quais certificados são usados conforme a tabela acima que são assinados com a CA pública.
- Verifique as informações de CA e raiz: Documentar qual CA e raiz emitiram cada certificado
- Verificar datas de vencimento: Planejar renovações estrategicamente antes da aplicação da política

Sugestões para serviços que exigem EKU do cliente

A tabela abaixo fornece ações recomendadas para serviços e integrações do Cisco ISE que dependem de certificados contendo EKU de autenticação de cliente.

Serviço	Ações recomendadas
TC-NAC	• Quando Tenable é usado, a validação de EKU estrita pode ser desabilitada no lado Tenable para manter a conectividade.
Syslog seguro	
LDAPs	
DTLS RADIUS	
Clientes PxGrid (CatC, FMC...etc.)	
EAP-TLS	

Soluções Alternativas De Curto Prazo (Antes De junho De 2026)

Os administradores podem escolher uma destas opções alternativas:

Opção 1: Alternar para CAs raiz públicas que fornecem certificados EKU combinados

Algumas CAs de raiz pública (como DigiCert e IdenTrust) emitem certificados com EKU combinado de uma raiz alternativa, que não pode ser incluída no armazenamento confiável do navegador Chrome.

Exemplos de CAs raiz públicas e tipos de EKU:

Fornecedor de CA	Tipo de EKU	CA raiz	Emitente/Sub CA
IdenTrustName	clientAuth + serverAuth	CA raiz do setor público IdenTrust 1	CA 1 do IdenTrust Public Setor Server
DigiCert	clientAuth + serverAuth	Raiz G2 do ID Assegurado do DigiCert	ID garantida do DigiCert CA G2

Pré-requisitos para esta abordagem:

- Entre em contato com o provedor de CA para verificar a disponibilidade desses certificados.
- Antes de implantar certificados, certifique-se de que o servidor que apresenta o certificado e todos os clientes que o consomem confiem na CA raiz correspondente.
- Informações de certificado raiz do Exchange com pares de comunicação.
- Essa abordagem evita a necessidade imediata de atualizações de software.

Referências de gerenciamento de certificados:

- Guia do Administrador do Cisco Identity Services Engine, Versão 3.3
- Configurar renovações de certificado no ISE

Opção 2: Renove os certificados atuais para estender sua validade

Os certificados emitidos por CAs de raiz pública antes de maio de 2026 que têm EKU de autenticação de servidor e de cliente continuam a ser honrados até o termo expirar.

Estratégia de renovação

As recomendações gerais são:

- Renovar certificados EKU combinados antes que ocorra o cancelamento da política
- Para obter a validade máxima do certificado, renove os certificados antes de 15 de março de 2026.
- Após essa data, os certificados emitidos por CA pública serão válidos somente por 200 dias.
- A Cisco recomenda que você renove seus certificados antes dessa data se desejar continuar com essa opção.
- A política de CA pública e as datas de implementação podem variar.
- Algumas CAs públicas pararam de emitir certificados EKU combinados e não podem fornecer um por padrão.
- Para gerar um certificado com um EKU combinado, trabalhe com sua autoridade de CA e use um perfil especial fornecido por CAs públicas.

Opção 3: Avaliar e migrar para provedores de CA alternativos

Abordagem de PKI privada

- Avaliar a viabilidade da transição para a PKI privada
- Configurar uma autoridade de certificação particular para emitir certificados únicos com EKU combinado (certificados de servidor e cliente com os EKUs necessários)
- Ao emitir um certificado assinado por uma CA privada, você precisa compartilhar as informações do certificado raiz com o correspondente.
- Antes de emitir ou implantar um certificado, verifique se o servidor que apresenta o certificado e todos os clientes que o consomem confiam na CA raiz correspondente.
- As autoridades de certificação privadas não estão sujeitas à política do programa raiz do Chrome
- Fornece controle de longo prazo sobre políticas de certificado

Solução de longo prazo (atualização de software necessária)

Os clientes devem atualizar o Cisco ISE para uma versão de patch que introduza o tratamento atualizado de certificados para oferecer suporte a certificados emitidos sob as novas políticas de CA.

As seguintes versões de patch resolvem esse problema planejado para abril de 2026:

Versão do Cisco ISE	Versão do patch
ISE 3.1	Correção 11
ISE 3.2	Correção 10
ISE 3.3	Correção 11

ISE 3.4	Correção 6
ISE 3.5	Correção 3

Comportamento após a instalação do patch

Certificado PxGrid

Após a instalação da versão do patch:

- O requisito atual de interface do usuário que aplica EKU de autenticação de servidor e EKU de autenticação de cliente para certificados pxGrid será removido.
- O Cisco ISE permitirá a importação de certificados pxGrid contendo somente EKU de autenticação de servidor, EKUs de autenticação de servidor e cliente ou nenhuma extensão EKU.
- Certificados contendo somente EKU de Autenticação de Cliente não serão aceitos.

Certificado do Serviço de Mensagens do ISE (IMS)

Para ISE 3.1, 3.2 e 3.3

Não há alteração no comportamento após a instalação do patch. O Serviço de Mensagens do ISE continuará a exigir um certificado com EKU de cliente e servidor. Os clientes devem planejar usar um certificado CA interno do ISE quando o certificado atual expirar.

Para ISE 3.4 e 3.5

O IMS agora oferece suporte a certificados de autoridade de certificação pública contendo somente EKU de autenticação de servidor. No entanto, como o IMS é usado somente para comunicação interna do Cisco ISE, a Cisco recomenda o uso do certificado CA interna do ISE quando o certificado é renovado.

Árvore de decisão

INICIAR: Você usa certificados CA públicos no Cisco ISE?

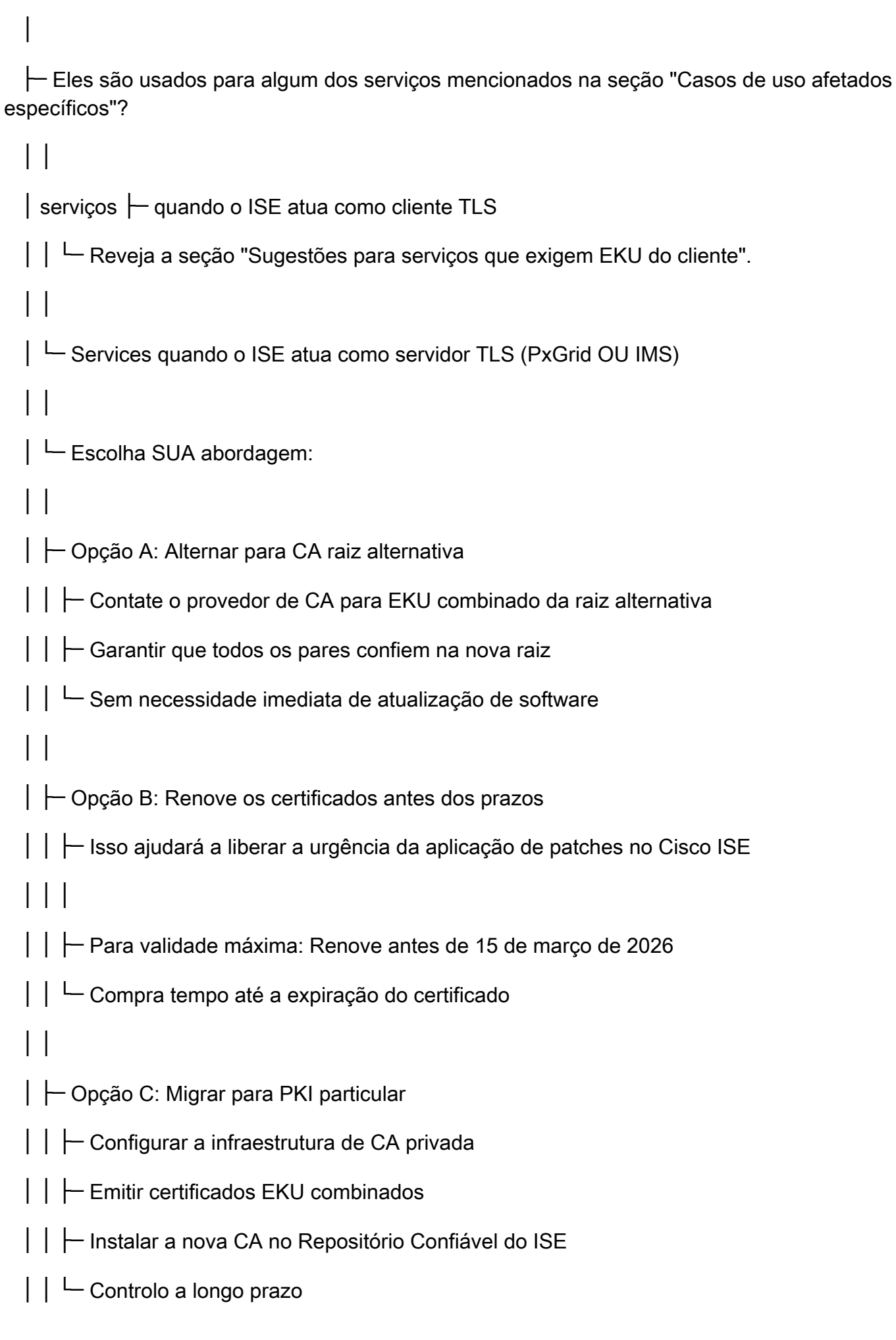
│

├─: PKI particular ou autoassinado

│ └─ Nenhuma ação necessária - Não afetado pela política

│

└─ SIM: Certificados de autoridade de certificação pública em uso


├─ Eles são usados para algum dos serviços mencionados na seção "Casos de uso afetados específicos"?
serviços ├─ quando o ISE atua como cliente TLS
└─ Reveja a seção "Sugestões para serviços que exigem EKU do cliente".
└─ Services quando o ISE atua como servidor TLS (PxGrid OU IMS)
└─ Escolha SUA abordagem:
├─ Opção A: Alternar para CA raiz alternativa
├─ Contate o provedor de CA para EKU combinado da raiz alternativa
├─ Garantir que todos os pares confiem na nova raiz
└─ Sem necessidade imediata de atualização de software
├─ Opção B: Renove os certificados antes dos prazos
├─ Isso ajudará a liberar a urgência da aplicação de patches no Cisco ISE
├─ Para validade máxima: Renove antes de 15 de março de 2026
└─ Compra tempo até a expiração do certificado
├─ Opção C: Migrar para PKI particular
├─ Configurar a infraestrutura de CA privada
├─ Emitir certificados EKU combinados
├─ Instalar a nova CA no Repositório Confiável do ISE
└─ Controlo a longo prazo

│ │

│ └─ Opção D : Planejar Atualização do Software

│ ├─ Aplique a versão de patch exigida do ISE (disponível a partir de abril de 2026)

Perguntas frequentes

Perguntas gerais

P: Preciso me preocupar com isso se eu usar PKI privado?

R: Não. Esta política afeta somente certificados emitidos por CAs de raiz pública. A PKI privada e os certificados autoassinados não são afetados.

P: Posso continuar usando meus certificados existentes?

R: Sim, os certificados existentes com EKU combinado permanecem válidos até expirarem. O problema surge quando você precisa renovar. Eles funcionam para conexões TLS e mTLS até expirarem.

P: Como sei se estou usando mTLS ou TLS padrão?

R: Reveja a seção Casos de uso afetados específicos.

Perguntas sobre atualização

Gerenciamento de Certificados

Perguntas de Cronograma

P: O que acontece em 15 de junho de 2026?

R: O Chrome para de confiar em certificados TLS públicos que contêm EKUs de autenticação de servidor e cliente. Os serviços que usam esses certificados podem falhar.

P: Por que preciso renovar antes de 15 de março de 2026?

R: Após 15 de março de 2026, a validade do certificado será reduzida de 398 dias para 200 dias. Renovar antes dessa data dá a você o tempo de vida máximo do certificado.

P: Qual é o prazo para ação?

R: Há vários prazos finais:

- 15 de março de 2026: Validade do certificado reduzida para 200 dias
- Maio de 2026: A maioria das CAs públicas pára de emitir EKU combinadas inteiramente
- Março de 2027: Política do Chrome totalmente aplicada

Outros recursos

- ID de bug da Cisco: CSCws83036 - Avaliação de impacto da aplicação de ClientAuth EKU no ISE

Referências externas

- Política do programa Chrome Root

Recursos da autoridade de certificação

- Portal IdenTrust

Conclusão

O desligamento do EKU de autenticação do cliente em certificados CA públicos representa uma mudança significativa na política de segurança que afeta as implantações do Cisco ISE usando conexões mTLS. Embora essa seja uma mudança em todo o setor, a avaliação de impacto é CRÍTICA e é necessária uma ação imediata para evitar interrupções no serviço.

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.