Preparar Expressway para Aut. de EKU de Cliente Aut. em Certificados CA Públicos

Contents

Introdução

Este documento descreve as alterações da política do programa raiz do Chrome no Cisco Expressway e o encerramento do EKU de autenticação de cliente em certificados de CA públicos após 26/6.

Informações de Backgroup

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 do 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 Expressway que atuam como servidor e cliente em diferentes cenários de conexão.

Definição do problema

Mudança de política do programa Chrome Root

A partir de junho de 2026, a Política do programa raiz do Chrome restringe os certificados de Autoridade de certificação raiz (CA) incluídos no Chrome Root Store, eliminando gradualmente as raízes multiuso para alinhar todas as hierarquias de infraestrutura de chave pública (PKI) para servir apenas casos de uso de autenticação de servidor TLS.

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 para manter a confiança do navegador Google Chrome
- 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: Junho de 2026

Cronograma de Resposta de CA Pública

- outubro de 2025: Muitas CAs públicas (DigiCert, Sectigo, SSL) começaram a emitir certificados somente de servidor por padrão
- 11 de fevereiro de 2026: Let's Encrypt pára de emitir certificados com EKU de autenticação de cliente usando o perfil ACME clássico
- Maio de 2026: Os servidores públicos de CA param de emitir certificações EKU de Autenticação de Cliente
- Junho de 2026: 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.

Documentação relacionada da Cisco

- ID de bug da Cisco: CSCwr73373- Suporte para certificado separado de servidor e cliente para Expressway
- Nota de campo: FN 74362
- Chrome Root Program Policy: Chrome Root Program Policy Documentation (Política do Chrome Root Program)

Como isso afeta a solução Expressway

Produtos afetados

Por Field Notice FN74362, todas as versões do Cisco Expressway são afetadas:

Produto	Versões afetadas	Impacto
Núcleo e borda do Expressway	X14 (Todas as versões)	X14.0.0 a X14.3.7 - Todas as versões afetadas
Núcleo e borda do Expressway	X15 (Versões anteriores a X15.4)	X15.0.0 a X15.3.2 - Todas as versões afetadas

Função dupla do Expressway

Os produtos Cisco Expressway (Expressway-C e Expressway-E) atuam como servidor e cliente em vários cenários de conexão, exigindo certificados com EKUs de autenticação de servidor e

cliente.

Expressway E como servidor (EKU de autenticação de servidor necessário):

- Acesso ao navegador HTTPS
- Conexões SIP UC Traversal
- Conectividade Webex Edge Audio/MRA

Expressway E como cliente (EKU de autenticação do cliente necessária):

- Comunicações B2B
- Conexões MRA (Mobile and Remote Access, acesso remoto e móvel)
- Federação XMPP
- Conexões CMS/zona de vizinho SIP
- Interações com entidades externas
- Conexão com a nuvem da Cisco (integração com MRA)

Casos de uso específicos afetados

O certificado assinado por CA público com EKU de autenticação de cliente atualmente usado para conexões mTLS no Cisco Expressway é o certificado de servidor Expressway. Este certificado é usado para as seguintes conexões mTLS:

1. Chamada SIP B2B sobre mTLS - O Expressway E torna-se cliente ou servidor na conexão mTLS, dependendo do site iniciado pela sessão
2. Federação SIP IMP sobre mTLS - O Expressway E torna-se cliente ou servidor na conexão mTLS, dependendo do site iniciado pela sessão
3. Zona de passagem UC - Expressway C apresenta EKU de autenticação de cliente
4. Zona transversal com configuração mTLS - Expressway C apresenta EKU de autenticação de cliente
5. Zona de vizinho SIP com configuração mTLS - O Expressway se torna cliente ou servidor na conexão mTLS, dependendo do site iniciado pela sessão, incluindo conexões com:

- Cisco Unified Communications Manager (Unified CM)
- Cisco Unity
- Cisco Unified Border Element (CUBE)
- Cisco Meeting Server (CMS)
- Conexão com a nuvem da Cisco - integração de MRA (o Expressway inicia a conexão com a nuvem da Cisco e apresenta o EKU de autenticação do cliente)

Recomendações

Auditoria de Certificados Atuais (OBRIGATÓRIO PRIMEIRO PASSO)

Por Field Notice FN74362, antes de considerar as opções de solução e solução alternativa:

- Preparar um inventário de todos os certificados TLS públicos para identificar quais

certificados contêm o EKU de Autenticação de Cliente
- Faça um backup da instância do Cisco Expressway ou copie manualmente o certificado assinado e a chave privada
- Uso do certificado do documento: identifica quais certificados são usados para conexões mTLS
- 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

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 (por FN74362):

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 de implantação de criação e uso de certificado do Cisco Expressway (X14.0)
- Guia de implantação de criação e uso de certificado do Cisco Expressway (X15.0)

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.

Considerações especiais sobre os certificados Let's Encrypt

Por FN74362, se você usar os certificados Let's Encrypt:

- Atualmente, o Expressway usa um perfil ACME clássico que é codificado e não pode ser modificado pelos usuários
- Este perfil ACME clássico é usado atualmente para solicitar certificados que incluem EKUs de Autenticação de Servidor e de Cliente
- A partir de 11 de fevereiro de 2026, as solicitações de certificado usando esse perfil não incluirão mais o EKU de autenticação de cliente em certificados gerados por Let's Encrypt
- Para obter mais informações, consulte Ending TLS Client Authentication Certificate Support in 2026 - Let's Encrypt

Itens de Ação para Criptografia de Usuários

- Renove os certificados antes de 11 de fevereiro de 2026 - idealmente o mais próximo possível desta data para maximizar o período de validade de 90 dias.
- Desative o programador automático ACME para impedir que os certificados sejam renovados automaticamente após 11 de fevereiro de 2026.
- Esta ação ajuda a evitar que certificados sejam inadvertidamente substituídos por versões que contenham apenas o EKU de Autenticação de Servidor.
- Se você não renovar antes de 11 de fevereiro de 2026, entre em contato com o TAC da

Cisco para obter suporte.

Opção 3: Avaliar e migrar para provedores de CA alternativos

Essa opção é aplicável a: Expressway C apenas; NÃO aplicável a Expressway E.

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

---

⚠ Caution: Essa opção não é viável para o Expressway-E, que requer certificados de CA públicos para serviços externos e confiança do navegador.

Solução De Longo Prazo (Atualizações De Software Necessárias)

De acordo com o aviso de campo FN74362, a Cisco está implementando aprimoramentos de produtos em versões fixas para resolver esse problema de forma abrangente.

Plano de liberação fixo:

Produto	Versão afetada	Versão fixa	Finalidade da correção	Disponibilidade
Cisco Expressway	X14.x (Todas as versões) X15.x (anterior a X15.4)	X15.4	Solução intermitente: Permite o carregamento adicional de certificado assinado somente por EKU de ServerAuth no Expressway E e ajuste de verificação de certificado para sinal SIP MRA entre Expressway E e Expressway C	Fevereiro de 2026

Cisco Expressway	X14.x (Todas as versões) X15.x (anterior a X15.5)	X15,5	Solução abrangente: Fornece aprimoramentos de interface do usuário para segregar certificados de cliente e servidor e fornece opções para administradores desabilitarem a verificação de EKU	Maio de 2026

Note: O Cisco Expressway E e o Expressway C devem ser atualizados para a mesma versão.

Detalhes da solução Cisco Expressway X15.4 (fevereiro de 2026)

Objetivo: solução intermitente para acomodar certificados somente com EKU ServerAuth e para habilitar registros MRA

Os principais aprimoramentos são:

- Remove a restrição em uploads de certificado
- Permite que os administradores carreguem certificados apenas com EKU de autenticação de servidor via GUI da Web no Expressway E
- Anteriormente, o Expressway rejeitava certificados somente de servidor
- Ajusta a verificação de certificado para MRA
- Modifica a verificação de certificado para sinalização SIP entre Expressway-E e Expressway-C em soluções MRA
- Permite a aceitação de certificados somente de servidor de aplicativos de terceiros

Quem pode atualizar para X15.4:

- se você implantar um novo ou reimplantar um Expressway-E existente para MRA com certificados assinados somente de servidor.
- Se você usar certificados ACME (Let's Encrypt) após 11 de fevereiro de 2026.
- Implantações existentes que precisam atualizar certificados assinados que contêm apenas EKU de Autenticação de Servidor.
- se você enfrentar problemas de autenticação relacionados ao certificado em conexões mTLS

Requisitos importantes para X15.4:

- O Expressway-E e o Expressway-C devem ser atualizados para X15.4
- Planejar a atualização durante a janela de manutenção para minimizar a interrupção do serviço

As limitações de X15.4 são:

- Essa é uma solução intermitente que trata de problemas imediatos de compatibilidade

- Não oferece suporte completo a certificado duplo
- Não inclui parâmetro de serviço para desabilitar verificação de EKU
- As conexões mTLS podem falhar dependendo do site iniciado pela sessão

Detalhes da solução Cisco Expressway X15.5 (maio de 2026)

Objetivo: Solução abrangente para atender aos requisitos globais do programa Google Chrome Root

Principais aprimoramentos do produto:

- Separação de certificados de cliente e servidor
- Permite o suporte para dois certificados separados na mesma interface
- Certificados Expressway com EKU de Autenticação de Servidor e EKU de Autenticação de Cliente distintas
- Facilita conexões mTLS apropriadas com funções de certificado segregadas
- Aprimoramentos de interface do usuário e back-end
- Novas interfaces de gerenciamento de certificados para gerenciamento individual de ambos os certificados
- Validação de EKU de Autenticação de Cliente durante carregamento de certificado para evitar quedas acidentais de conexão MTLS
- Os administradores podem carregar e gerenciar certificados de servidor e cliente separadamente
- Opções para Desabilitar a Verificação de EKU de Autenticação de Cliente
- Parâmetro de serviço que permite aos administradores desabilitar a verificação de EKU de Autenticação de Cliente de acordo com os requisitos corporativos individuais
- Permite que o Cisco Expressway ignore o EKU do peer remoto (cliente) que solicita uma conexão somente com certificados EKU de autenticação de servidor
- Na ausência de um certificado EKU de Autenticação de Cliente, permite que o Expressway (re)use o certificado somente EKU de Autenticação de Servidor como um certificado de Cliente

---

Note: Nesse caso, o peer remoto também tem que suportar um modelo semelhante de EKU de Ignore Client Authentication

---

Árvore de decisão

INICIAR: Você usa certificados CA públicos no Expressway?

│

├─: PKI particular ou autoassinado

│ └─ Nenhuma ação necessária - Não afetado pela política

│

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

  │

  ├─ Eles são usados para conexões mTLS? (Verifique os casos de uso na seção Casos de uso afetados específicos)

  │ │

  │ N.├─: Somente autenticação de servidor

  │ │ └─ Impacto mínimo - Monitora alterações futuras

  │ │

  │ └─ SIM: conexões mTLS com EKU de Autenticação de Cliente

  │ │

  │ └─ 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

  │ │ ├─ Se Vamos Criptografar: Renove antes de 11 de fevereiro de 2026

  │ │ │ └─ Desativar o programador ACME após a renovação

  │ │ ├─ Para validade máxima: Renove antes de 15 de março de 2026

  │ │ └─ Compra tempo até a expiração do certificado

  │ │

  │ ├─ Opção C: Migrar para PKI privada (apenas Expressway-C)

  │ │ ├─ Configurar a infraestrutura de CA privada

│ │ ├─ Emitir certificados EKU combinados

│ │ ├─ Distribuir raiz para todos os pares

│ │ └─ Controle de longo prazo, NÃO para Expressway-E

│ │

│ └─ Opção D : Planejar Atualização do Software

│ ├─ Necessidade urgente? Atualização → para X15.4 (fevereiro de 2026)

│ └─ Solução abrangente → atualização para X15.5 (maio de 2026)

│ └─ Em seguida, obtenha certificados de servidor/cliente separados

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: E se eu não usar conexões mTLS?

R: Se você usar apenas TLS padrão (autenticação de servidor), não será afetado por esta política. Seus certificados somente de servidor continuarão funcionando. No entanto, verifique seus casos de uso na lista da seção Casos de uso afetados específicos, pois alguns dos casos de uso padrão usam mTLS.

P: Minhas conexões da Web HTTPS padrão com o Expressway pararão de funcionar?

R: Não. As conexões TLS padrão não são afetadas. O acesso do navegador da Web ao Expressway continua a funcionar normalmente mesmo com certificados EKU somente de servidor.

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.

P. O que posso fazer agora?

R: A Cisco recomenda enfaticamente estas ações imediatas:

- Auditar seus certificados

  Identificar certificados TLS públicos usados para mTLS

- Renovar certificados antecipadamente

  Renove antes de 15 de março de 2026 para maximizar a validade

- Controle da automação ACME

  Desabilitar renovações automatizadas que podem substituir certificados inesperadamente

- Coordene com sua CA

  Algumas AC oferecem perfis de certificado temporários ou alternativos

P: O CUCM SU3(a) é compatível com X15.4 e X15.5

R: Yes

P: Há uma vulnerabilidade de segurança com a desabilitação da verificação de EKU do cliente no Cisco Expressway E (com a versão X15.5)

R: O certificado ainda verifica o CN/SAN para verificar se a fonte de conexão é válida, apenas ignora a validação de EKU (certificado para função de cliente), que foi incluída por padrão até que o Google manifeste preocupação com a segurança, portanto, não deve ter problema de segurança comparado a antes.

Vamos criptografar informações específicas

P: Eu uso Let's Encrypt with ACME no Expressway. O que eu posso fazer?

R:

1. Renove seu certificado antes de 11 de fevereiro de 2026 (o mais próximo possível dessa data)
2. Desativar o programador automatizado ACME imediatamente após a renovação
3. Planejam atualizar para X15.5 para uma solução de longo prazo

P: Posso modificar o perfil ACME para continuar a obter certificados EKU combinados?

R: Não. Atualmente, o Expressway usa um perfil ACME "clássico" codificado que não pode ser modificado pelos usuários. Entre em contato com o TAC da Cisco para obter suporte ao perfil do certificado ACME.

Perguntas sobre atualização

P: Preciso atualizar o Expressway-E e o Expressway-C?

R: Sim, com certeza. Ambos devem ser atualizados para a mesma versão (X15.4 ou X15.5) para uma operação adequada.

P: posso atualizar para X15.4 ou esperar por X15.5?

R:

- Atualize para o X15.4 se tiver problemas urgentes ou precisar aceitar certificados somente de servidor agora
- Se possível, aguarde X15.5 (maio de 2026) para obter a solução abrangente com suporte a certificado duplo

P: A replicação do meu cluster é interrompida após a renovação do certificado. O que aconteceu?

R: Provavelmente seu novo certificado tem apenas o EKU de Autenticação de Servidor, mas:

- Se uma versão anterior a X15.4 com Verificação TLS = Impondo: Os pares de cluster não podem estabelecer conexões mTLS sem o EKU de Autenticação de Cliente
- Opções de solução (qualquer uma):

  Definir o modo de verificação TLS como "Permissivo" (menos seguro)

  Obter certificados com EKU combinado da raiz de CA alternativa

  Atualizar para X15.4 ou posterior, ignorando a verificação de EKU de Autenticação de Cliente para ClusterDB

P: Após atualizar para X15.4, posso usar o modo de imposição com certificados somente de servidor em meu cluster?

R: Sim. Começando em X15.4, o Expressway ignora a verificação de EKU de Autenticação de Cliente para conexões mTLS ClusterDB. Portanto, a Verificação TLS pode ser definida como "Impondo" mesmo se um ou mais nós de cluster tiverem somente a EKU de Autenticação do Servidor.

P: Por que não posso carregar meu certificado através da GUI da Web do Expressway?

R: Antes de X15.4, a GUI da Web impõe uma validação codificada que exige que os certificados tenham EKU de autenticação de cliente. Se o seu certificado tiver apenas EKU de Autenticação de Servidor, você terá duas opções:

- Usar SCP (Secure Copy Protocol) para carregar o certificado diretamente no servidor (pasta /persistent/Certs)
- Atualizar para X15.4 ou posterior (apenas Expressway-E), o que remove essa restrição

P: Após a atualização para X15.4, ainda não consigo carregar certificados somente de servidor

para Expressway-E

R: Após o upgrade, certifique-se de que este comando esteja habilitado

EnableServerEkuUpload de CVS de certificado TLS XCP xConfiguration: Ligado

P: Atualizei para X15.4. Agora posso carregar certificados somente de servidor no Expressway-E e no Expressway-C?

R: Não. O X15.4 remove apenas a restrição de carregamento do Expressway-E. O Expressway-C ainda requer certificados EKU combinados para carregamento via GUI da Web. Isso ocorre porque o Expressway-C frequentemente atua como um cliente TLS em zonas de passagem de UC e requer EKU de autenticação de cliente. Certifique-se de executar esse comando no Expressway-E. Esse comando não é executado no Expressway-C

EnableServerEkuUpload de CVS de certificado TLS XCP xConfiguration: Ligado

P: Não consigo registrar a Licença inteligente após a renovação do certificado. Por quê?

R: A falha do Smart Licensing após a renovação do certificado geralmente NÃO está relacionada ao EKU:

- Verifique se o Expressway pode acessar tools.cisco.com (CSSM)
- Verificar se as regras de firewall permitem saída HTTPS (porta 443)
- Verifique se a configuração do proxy está correta (se estiver usando o proxy HTTP)
- Verifique se o certificado do servidor CSSM é confiável no repositório de confiança do Expressway
- O Smart Licensing não exige clientAuth, portanto, essa alteração de política não a afeta

Específico MRA (Mobile and Remote Access)

P: O MRA requer EKU de autenticação de cliente no Expressway-E?

R: Depende da versão do Expressway:

- Antes de X15.4: Sim, exigido indiretamente

  Durante a sinalização SIP MRA, o Expressway-E envia seu certificado assinado em uma mensagem de SERVIÇO SIP para o Expressway-C

  O Expressway-C valida o certificado, exigindo EKUs de autenticação de cliente e de autenticação de servidor

  Sem EKU combinado, o registro SIP de MRA falha

- X15.4 e posterior: No

  O Expressway-C não valida mais o EKU de autenticação do cliente na mensagem de SERVIÇO SIP

O Expressway-E só precisa de EKU de autenticação de servidor para MRA

A UC Traversal Zone opera unidirecionalmente (o Expressway-C valida apenas o certificado do servidor Expressway-E)

P: Por que minhas Zonas de Vizinhos estão falhando após o upload doEKU de Autenticação de Servidor em Expresswayx15.4

R: Se você definir o modo de verificação TLS como "on", será necessário ter um EKU de autenticação de cliente. Assim, você pode desabilitar a verificação TLS na configuração da Zona Vizinha

P: Quais certificados são necessários para que o MRA funcione corretamente?

R: Para uma implantação de MRA típica:

Componente	Requisitos do certificado	EKU Necessário	Notas
Expressway-E (antes de X15.4)	serverAuth + clientAuth	Ambos	Para validação de SERVIÇO SIP por Exp-C
Expressway-E (X15.4+)	somente serverAuth	Somente servidor	Verificação de EKU do cliente ignorada
Expressway-C	clientAuth + serverAuth	Ambos	Sempre atua como cliente no UC Traversal
Zona de passagem de UC	Validação unidirecional	Exp-E: serverAuth Exp-C: clientAuth	Exp-C valida o certificado do servidor Exp-E

P: Meu MRA estava funcionando bem, mas depois de renovar meu certificado Expressway-E com EKU somente de servidor, o registro SIP falha. O que está errado?

R: Se você estiver executando uma versão anterior a X15.4, a sinalização SIP MRA exigirá que o Expressway-E apresente EKUs de Autenticação de Servidor e de Cliente na mensagem de SERVIÇO SIP. Suas opções:

- Obter um certificado com EKU combinado
- Alternar para uma raiz de CA alternativa que emite EKU combinado
- Atualizar Expressway-E e Expressway-C para X15.4 ou posterior (recomendado)

Gerenciamento de Certificados

P: Como obtenho um certificado com EKU combinado de DigiCert ou IdenTrust?

R: Entre em contato com o provedor de CA e solicite um certificado de sua raiz alternativa que ainda emite o EKU combinado.

P: Minha autoridade de certificação diz que só podem fornecer certificados somente de servidor. O que eu posso fazer?

R: Você tem várias opções:

- Verificar raízes alternativas: Pergunte ao CA se ele tem raízes alternativas que emitem EKU combinado (como DigiCert Assured ID ou IdenTrust Public Setor)
- Provedores de autoridade de certificação do switch: Procure CAs que ofereçam EKU combinado de raízes não confiáveis do Chrome
- Usar PKI particular: Configurar CA interna para certificados EKU combinados (apenas implantações do Expressway-C)
- Atualizar para X15.4: Solução intermitente para acomodar certificados somente com EKU ServerAuth e para habilitar registros MRA
- Atualize para o X15.5 assim que estiver disponível: Planeje a arquitetura de certificado duplo onde os certificados somente de servidor são aceitáveis e a solução abrangente atende aos requisitos globais do programa raiz Google Chrome

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:

- 11 de fevereiro de 2026: Let's Encrypt pára EKU combinado via ACME clássico
- 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
- Junho de 2026: Política do Chrome totalmente aplicada

Outros recursos

Documentação da Cisco

- Nota de campo FN74362: Impacto do Cisco Expressway na comunicação segura devido às próximas alterações nos certificados TLS
- ID de bug da Cisco CSCwr73373: Suporte para certificado separado de servidor e cliente para Expressway

Referências externas

- Política do programa Chrome Root
- Vamos criptografar: Finalizando o suporte ao certificado de autenticação de cliente TLS em 2026
- Requisitos da linha de base do fórum de CA/navegador

Recursos da autoridade de certificação

- Portal de suporte DigiCert
- Serviços de Certificados IdenTrust
- Vamos criptografar o fórum da comunidade
- Base de conhecimento Sectigo

Conclusão

O desligamento do EKU de Autenticação de Cliente em certificados CA públicos representa uma mudança significativa na política de segurança que afeta as implantações do Cisco Expressway usando conexões mTLS. Embora essa seja uma mudança em todo o setor, a classificação de impacto é CRÍTICA de acordo com o aviso de campo FN74362, e é necessária uma ação imediata para evitar interrupções no serviço.

Pontos principais

- Isso afeta TODAS as versões do Expressway (X14 e X15 antes de X15.4)
- Faça a auditoria dos certificados AGORA - Esta é a primeira etapa obrigatória
- Várias soluções alternativas estão disponíveis - Escolha a melhor opção para o seu ambiente
- Atualizações de software são necessárias para soluções de longo prazo - Planeje para X15.5
- O Expressway-E e o Expressway-C devem ser atualizados juntos
- Vamos criptografar os usuários com o prazo mais curto - 11 de fevereiro de 2026

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.