Impacto do Cisco Secure Firewall das alterações de EKU de autenticação de cliente CA público a partir de maio de 2026 para comunicações seguras

Introdução

Este documento descreve o impacto das restrições sobre os critérios de emissão de certificados impostos pelas autoridades de certificação que cumprem com o programa Chrome Root Certificate, especificamente como eles se relacionam aos produtos Cisco Secure Firewall.

Informações de Apoio

Os certificados TLS de confiança pública são emitidos por autoridades de certificação que devem estar em conformidade com as políticas do setor que regem a emissão e o uso de certificados.

A Política do programa raiz do Chrome, operada pelo Google, define os requisitos que as CAs devem seguir para que seus certificados sejam confiáveis pelo navegador Google Chrome. Esses requisitos influenciam a forma como os certificados de confiabilidade pública são emitidos no setor. Como parte das práticas de segurança em evolução, o Chrome Root Program está introduzindo orientações mais rígidas sobre o uso de certificados.

Muitas CAs públicas estão, portanto, deixando de emitir certificados que incluem EKU de Autenticação de Cliente e estão em transição para emitir certificados destinados apenas à autenticação de servidor. Como resultado, espera-se que certificados recém-emitidos de muitas CAs públicas incluam somente EKU de Autenticação de Servidor.

O Uso Estendido de Chave (EKU), é uma extensão de certificado que define a função pretendida de uma chave pública dentro de um certificado digital. Estabelece um conjunto estruturado de aplicativos permitidos, garantindo que a chave seja usada apenas para operações criptográficas específicas. Essa funcionalidade é controlada por Identificadores de Objeto (OIDs) — identificadores numéricos exclusivos que categorizam cada uso permitido, como assinatura de código, autenticação de servidor, autenticação de cliente ou e-mail seguro.

Quando a autenticação é baseada em certificado, a entidade de verificação analisa o certificado para identificar o

Identificador de Objeto (OID) no EKU. Incorporando a extensão EKU, uma Autoridade de Certificação (CA) restringe o escopo do certificado a funções predefinidas, com cada finalidade designada mapeada explicitamente para um OID.

Finalidade dos atributos EKU

· Definir uso: Os atributos de EKU esclarecem que tipos de autenticação ou criptografia o certificado tem permissão para executar.

· Aprimorar a segurança: Restringindo certificados a usos específicos, o EKU ajuda a evitar o uso indevido ou aplicativos não intencionais (por exemplo, um certificado de servidor não pode ser usado para autenticação de cliente).

· Conformidade: Garante que os certificados sejam usados de acordo com as políticas de segurança e os padrões do setor.

Principais usos dos atributos EKU

1. Autenticação do cliente Web TLS

· Permite que os certificados sejam usados para identificar e autenticar usuários ou dispositivos em um servidor.

•OID: 1.3.6.1.5.5.7.3.2

· Usado em VPNs, TLS mútuo e cenários de login seguro.

2. Autenticação do Servidor Web TLS

· Permite que os certificados sejam usados por servidores para provar sua identidade aos clientes.

•OID: 1.3.6.1.5.5.7.3.1

· Usado em HTTPS, servidores Web SSL/TLS e endpoints de API seguros.

3. Assinatura do código

· Indica que o certificado pode ser usado para assinar software ou executáveis.

•OID: 1.3.6.1.5.5.7.3.3

· Usado na distribuição de software e verificações de integridade.

4. Proteção de e-mail

· Permite que certificados sejam usados para assinar e criptografar mensagens de e-mail.

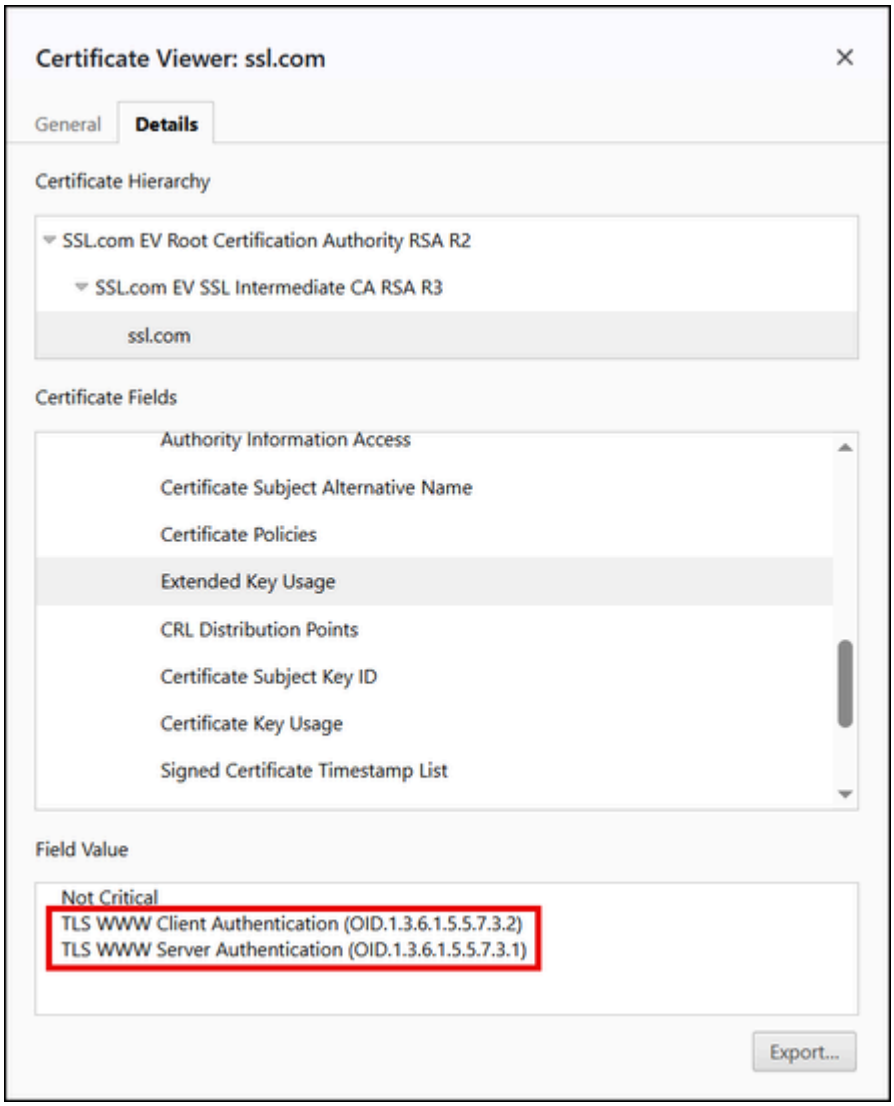
•OID: 1.3.6.1.5.5.7.3.4

· Usado na segurança de e-mail S/MIME.

5. Outros Fins

· Assinatura de documentos, carimbo de data e hora, logon por cartão inteligente etc., cada um com seus próprios OIDs.

Os navegadores e servidores precisam apenas do EKU serverAuth para estabelecer uma conexão segura para HTTPS, mas historicamente, muitos certificados de servidor TLS incluíam os EKUs serverAuth e clientAuth, abaixo está um exemplo de tal certificado:



Por que a remoção do EKU de Autenticação de Cliente de certificados de servidor?

- Segurança e escopo: certificados TLS públicos devem apenas autenticar servidores na Web. A remoção proporciona uma separação clara entre a funcionalidade do servidor e do cliente. O EKU ClientAuth é usado para autenticação de máquinas e usuários com TLS mútuo (mTLS) e outros cenários de autenticação.

- Evitar erros de configuração: alguns sistemas podem confiar em qualquer certificado de uma CA pública para autenticação de cliente se o EKU estiver presente, o que pode ser um risco à segurança.

- Requisitos do navegador: navegadores principais não exigem ou verificam o EKU clientAuth em um certificado do site.

- Arquitetura de PKI simplificada: separando os usos, as CAs podem manter hierarquias de certificado distintas para TLS de servidor versus outras finalidades.

Isso é particularmente importante para produtos como o Cisco Secure Firewall Adaptive Security Appliance (ASA), o

Cisco Secure Firewall Threat Defense (FTD), o Cisco Secure Firewall Device Manager (FDM) e o Cisco Secure Firewall Management Center (FMC) que podem atuar como servidor ou cliente durante a autenticação TLS, dependendo do caso de uso.

Impacto em ambientes de servidor

Para a grande maioria das implantações de servidor, essa alteração terá baixo impacto ou nenhum impacto. Veja o que esperar:

- Servidores Web padrão (HTTPS): sem impacto. Os certificados atualizados continuarão a funcionar normalmente.
- Certificados existentes: qualquer certificado emitido antes do corte continuará a funcionar até que expire.
- Cenários de certificação de cliente e TLS mútuo (mTLS) Se você estiver usando um certificado de servidor TLS para autenticação de cliente, precisará obter um certificado separado com o clientAuth EKU de outra origem.
- Sistemas corporativos que exigem ambos os EKUs: alguns sistemas herdados ou corporativos esperavam ambos os EKUs. Você deve verificar se são necessárias atualizações para estar em conformidade com as novas regras.

Descrição do problema

A partir de maio de 2026, muitas autoridades de certificação (CAs) públicas deixarão de emitir 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.

Como resultado, se os certificados emitidos por uma CA pública forem renovados de acordo com as políticas de CA atualizadas e, em seguida, implantados nos Produtos Cisco Secure Firewall, os serviços em que o EKU de Autenticação do Cliente for necessário falharão. Os serviços específicos afetados são os seguintes:

- Quando o ASA, o FTD, o FDM ou o FMC atuam como um cliente, por exemplo, ao se conectar a provedores de identidade ou servidores de autenticação, como ISE (pxGrid), RADIUS, LDAPS ou Ative Diretory, a autenticação baseada em certificado poderá falhar se o certificado do cliente tiver sido gerado por uma CA pública e estiver faltando o EKU de Autenticação do Cliente. Nesses cenários, se o servidor de autenticação rejeitar certificados sem o EKU necessário, poderão ocorrer falhas de conexão.
- O Cisco Secure Client (antigo AnyConnect) pode se autenticar em servidores ASA ou FTD usando certificados. No entanto, se o certificado do cliente tiver sido gerado por uma CA pública e o EKU de Autenticação do Cliente estiver ausente, a conexão de VPN de Acesso Remoto (RAVPN) falhará.

- Quando o FTD ou o ASA estabelece um túnel VPN de site a site (seja para outro FTD, ASA, roteador Cisco ou um peer VPN de terceiros) usando autenticação de certificado (RSA ou ECDSA), o túnel falhará se o certificado de identidade gerado por uma CA pública não tiver o atributo EKU de autenticação de cliente. Isso ocorre porque o par de VPN remoto exige que o EKU de Autenticação de Cliente esteja presente no certificado de identidade.

Mudança de política do programa Chrome Root

A implementação do EKU depende da assinatura do certificado pela CA. O uso de EKU de Autenticação de Servidor e Autenticação de Cliente foi uma prática comum. No entanto, como parte da Alteração de Política do Programa Raiz do Chrome, as CAs que se alinham a esses critérios de emissão de certificado estão descontinuando a assinatura de certificados TLS que incluem o Uso Estendido de Chave (EKU) da Autenticação de Cliente. Os certificados emitidos recentemente 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 nesses certificados
- As CAs raiz que continuam a emitir certificados com EKU de autenticação de cliente são removidas do Chrome Root Store, causando a sinalização de tais certificados como "Não confiável" pelo Chrome Browser

Cronogramas

- Em setembro de 2025, SSL.com emitirá certificados TLS que incluirão somente o ServerAuth EKU (e não ClientAuth) para certificados de servidor. Em outras palavras, os novos certificados SSL/TLS para o seu site ou servidor serão explicitamente apenas para "Autenticação de servidor".
- Outubro de 2025: as CAs alinhadas ao programa (por exemplo: DigiCert, Sectigo, etc.) começaram a emitir certificados somente de servidor por padrão.
- Maio de 2026: CAs alinhadas ao programa param de emitir certificados EKU de Autenticação de Cliente
- Março de 2027: A política do programa Chrome Root torna-se totalmente eficaz

Impacto nos produtos Cisco Secure Firewall

Depois que as CAs públicas começarem a incluir somente o EKU de Autenticação de Servidor nos certificados emitidos. Isso pode ter o seguinte impacto nos próximos cenários de produto do Cisco Secure Firewall:

- Quando o ASA, o FTD, o FDM ou o FMC atuam como um cliente, por exemplo, ao se conectar a provedores de identidade ou servidores de autenticação, como ISE (pxGrid), RADIUS, LDAPS ou Ative Diretory, a autenticação baseada em certificado poderá falhar se o certificado do cliente tiver sido gerado por uma CA pública e estiver faltando o EKU de Autenticação do Cliente. Nesses cenários, se o servidor de autenticação rejeitar certificados sem o EKU necessário, poderão ocorrer falhas de conexão.

- O Cisco Secure Client (antigo AnyConnect) pode se autenticar em servidores ASA ou FTD usando certificados. No entanto, se o certificado do cliente tiver sido gerado por uma CA pública e o EKU de Autenticação do Cliente estiver ausente, a conexão de VPN de Acesso Remoto (RAVPN) falhará.

- Quando o FTD ou o ASA estabelece um túnel VPN de site a site (seja para outro FTD, ASA, roteador Cisco ou um peer VPN de terceiros) usando autenticação de certificado (RSA ou ECDSA), o túnel falhará se o certificado de identidade gerado por uma CA pública não tiver o atributo EKU de autenticação de cliente. Isso ocorre porque o par de VPN remoto exige que o EKU de Autenticação de Cliente esteja presente no certificado de identidade.

Observação: se você estiver integrando o FMC ou o FDM ao ISE por meio do pxGrid e os certificados instalados no FMC/FDM não tiverem o atributo EKU de Autenticação de Cliente, revise as soluções propostas neste documento e as próximas referências do ISE: FN74392 e Prepare o Identity Services Engine para as Restrições de Uso de Chave Estendida em Certificados Emitidos por Autoridades de Certificação Públicas.

Note: A remoção da EKU clientAuth dos certificados do servidor TLS é uma alteração de política em todo o setor que aumentará a segurança e evitará o uso indevido. Para a maioria dos usuários, não haverá impacto perceptível. No entanto, se você depende do EKU ClientAuth, você deve tomar medidas proativas para obter o tipo correto de certificado para suas necessidades.

Produtos afetados

Produto Cisco Secure Firewall	Versão de software	Cenários afetados	Remediações
FTD	Todas as versões	Quando o atua como um cliente, por exemplo, ao se conectar a provedores de identidade ou servidores de autenticação, como	Opção 1. Se estiver usando um certificado de servidor TLS para autenticação de cliente, você
FDM	Todas as versões		

		ISE (pxGrid), RADIUS, LDAPS ou Ative Diretory, a autenticação baseada em certificado poderá falhar se o certificado do cliente tiver sido gerado por uma CA pública e estiver faltando o EKU de Autenticação do Cliente. Neste cenário, se o servidor de autenticação rejeitar certificados sem o EKU necessário, poderão ocorrer falhas de conexão.	precisará obter um certificado com a EKU ClientAuth de outra fonte. OU Opção2. Mude para CAs raiz públicas (Autoridades de Certificação) que fornecem certificados EKU (ClientAuth e ServerAuth) combinados. NOTE: Consulte a seção Soluções deste documento para obter opções adicionais.
CVP	Todas as versões		
ASA	Todas as versões		
Cisco Secure Client (antigo AnyConnect)	Todas as versões	O Cisco Secure Client pode se autenticar nos servidores ASA ou FTD usando certificados. No entanto, se o certificado do cliente tiver sido gerado por uma CA pública e o EKU de Autenticação do Cliente estiver ausente, a conexão de VPN de Acesso Remoto (RAVPN) falhará.	
FTD ou ASA	Todas as versões	Quando o FTD ou o ASA estabelece um túnel VPN de site a site (seja para outro FTD,	

		ASA, roteador Cisco ou um peer VPN de terceiros) usando autenticação de certificado (RSA ou ECDSA), o túnel VPN falhará se o certificado de identidade gerado por uma CA pública não tiver o atributo EKU de autenticação de cliente. Isso ocorre porque o par de VPN remoto exige que o EKU de Autenticação de Cliente esteja presente no certificado de identidade.	

Observação: se você estiver integrando o FMC ou o FDM ao ISE por meio do pxGrid e os certificados instalados no FMC/FDM não tiverem o atributo EKU de Autenticação de Cliente, revise as soluções propostas neste documento e as próximas referências do ISE: FN74392 e Prepare o Identity Services Engine para as Restrições de Uso de Chave Estendida em Certificados Emitidos por Autoridades de Certificação Públicas.

Note: A remoção da EKU clientAuth dos certificados do servidor TLS é uma alteração de política em todo o setor que aumentará a segurança e evitará o uso indevido. Para a maioria dos usuários, não haverá impacto perceptível. No entanto, se você depende do EKU ClientAuth, você deve tomar medidas proativas para obter o tipo correto de certificado para suas necessidades.

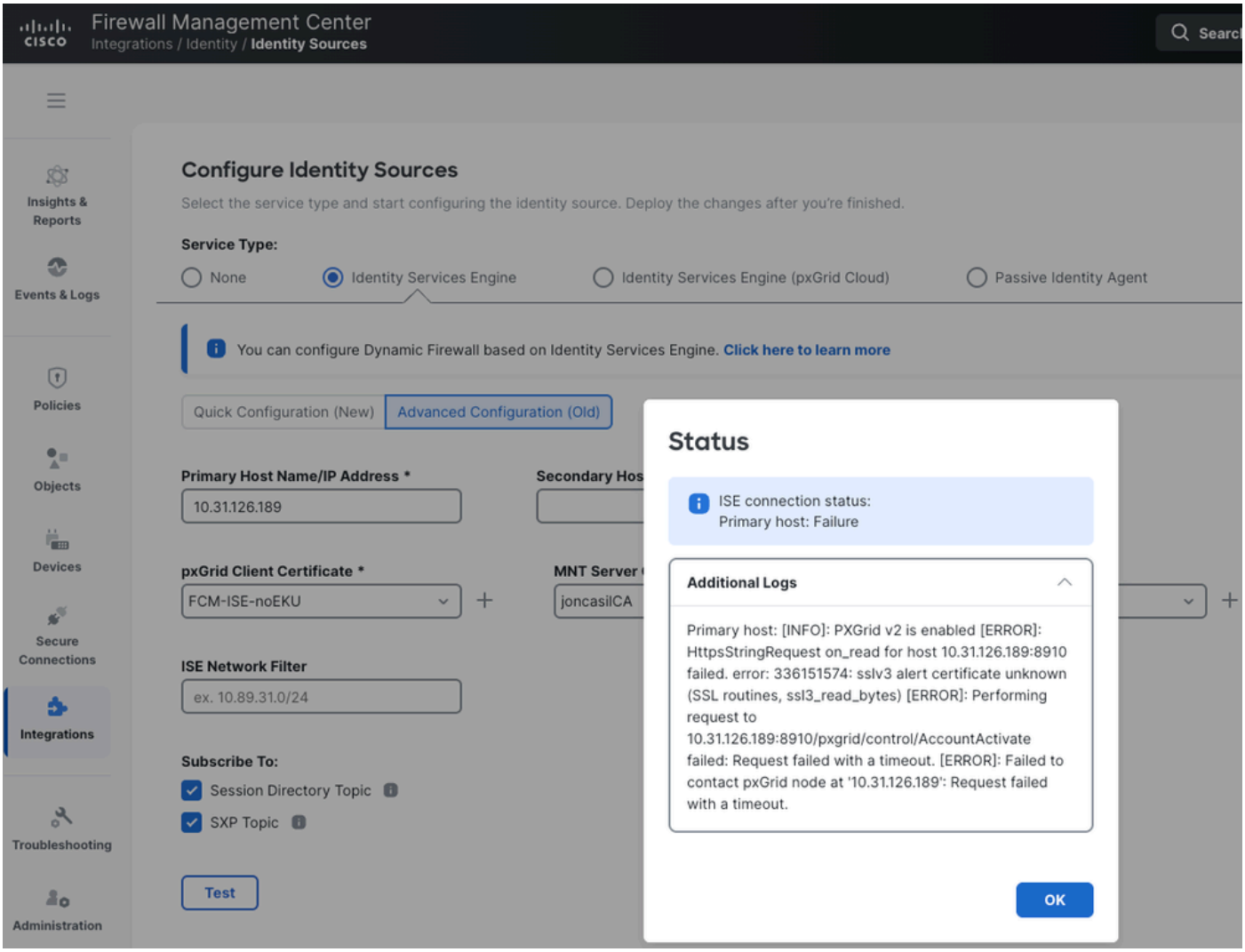
Caution: Para ambientes de produção, é altamente recomendável que os clientes usem certificados com os atributos EKU apropriados. Essa prática garante a segurança, a compatibilidade e a adesão aos padrões do setor e às práticas recomendadas. Os certificados sem atributos EKU devem ser considerados apenas como uma solução temporária e apenas com um claro entendimento dos riscos associados.

Problema 1. Problema de integração do pxGrid entre o FMC e o ISE, quando o certificado FMC não tem o atributo EKU de Autenticação do Cliente

Neste cenário, o certificado usado pelo FMC para a integração do pxGrid com o ISE não tem o atributo EKU de autenticação do cliente. Como resultado, a integração do pxGrid falha porque o servidor ISE espera que esse atributo esteja presente no certificado apresentado pelo FMC.

Topologia

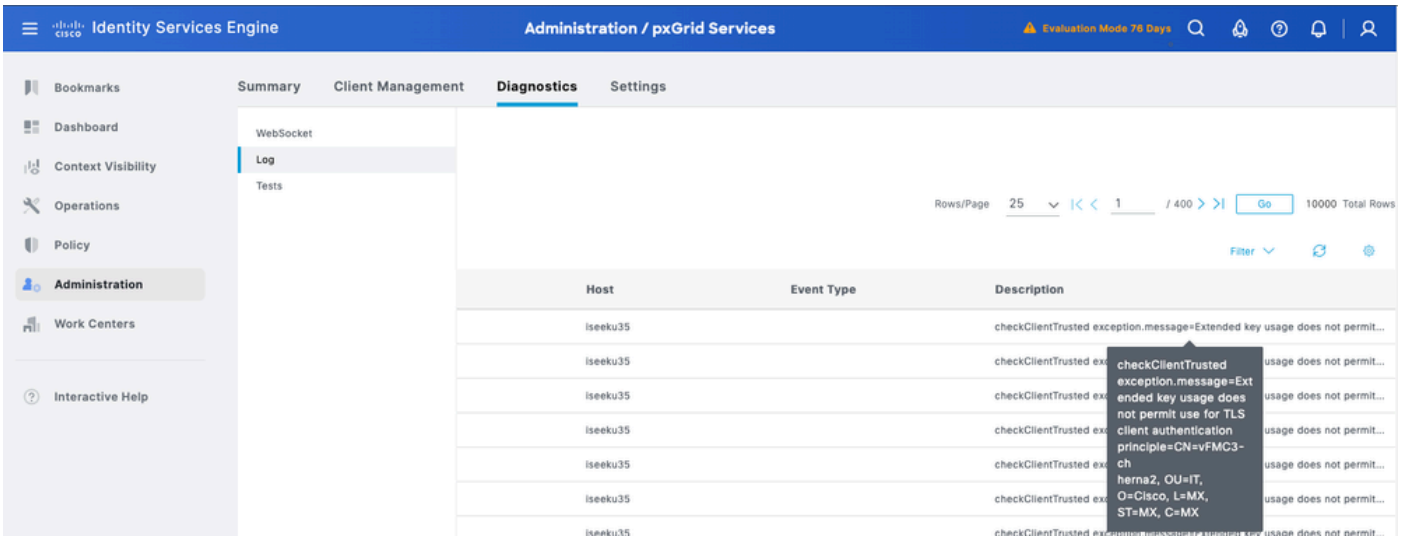
Erros de interface do usuário do FMC: Esta é a mensagem de erro exibida no FMC, quando o certificado usado pelo FMC não tem o atributo EKU de autenticação de cliente para a integração do pxGrid com o ISE.



Erros CLI do FMC: As mesmas mensagens de erro são encontradas no diretório FMC /var/log/messages.

```
<#root>

HttpsStringRequest on_read for host 10.31.126.189:8910 failed. error: 336151574:

sslv3 alert certificate unknown


(SSL routines, ssl3_read_bytes)


Mar 27 23:17:17 vFMC3-chherna2 SF-IMS[8074]: [7514] ADI:HttpsEndpoint

[ERROR] Performing request to 10.31.126.189:8910/pxgrid/control/AccountActivate failed: Request failed w


Mar 27 23:17:17 vFMC3-chherna2 SF-IMS[8074]: [7514] ADI:ise_connector.PXGrid2ThreadedService

[ERROR] pxgrid2_service was not created for 10.31.126.189. Reason - Request failed with a timeout.


Mar 27 23:17:47 vFMC3-chherna2 SF-IMS[8074]: [7514] ADI:ise_connector.PXGrid2ThreadedService [I
Mar 27 23:17:47 vFMC3-chherna2 SF-IMS[8074]: [7514] ADI:ise_connector.PXGrid2ThreadedService [I
```

Erro do ISE: Esta é a mensagem de erro exibida no ISE, "checkClientTrusted exception.message=O uso estendido de chave não permite o uso para o princípio de autenticação de cliente TLS=CN=vFMC3-chherna2, OU=IT, O=Cisco, L=MX, ST=MX, C=MX".



Solução: se você estiver integrando o FMC ou o FDM ao ISE por meio do pxGrid e o certificado instalado em seu FMC/FDM não tiver o atributo EKU de Autenticação de Cliente, revise o proposto neste documento e as próximas referências do ISE: FN74392 e Prepare o Identity Services Engine para Restrições de Uso de Chave Estendida em Certificados Emitidos por Autoridades de Certificação Públicas para obter uma integração bem-sucedida do pxGrid.

Note: O certificado de cliente do FMC pxGrid deve incluir o atributo EKU ClientAuth ou não conter nenhum atributo EKU Client ou Server.

Note: Mesmo que o IMS ofereça suporte ao uso de um certificado assinado por uma CA pública. A Cisco recomenda o uso do certificado CA interno do ISE, pois essa comunicação é somente para transações internas.

Problema 2. Problema de integração de FTD ou ASA com um servidor LDAPS, quando o certificado apresentou falta do atributo EKU de Autenticação do Cliente

Neste cenário, o FTD ou o ASA atua como um cliente para integrar com um servidor LDAPS usando a autenticação de certificado. Se o certificado usado pelo FTD ou ASA não tiver o atributo EKU de Autenticação de Cliente, a integração falhará porque o servidor LDAPS requer que esse atributo esteja presente no certificado.

Topologia

Erros do servidor LDAPS: 'Verificação de certificado TLS: Erro, propósito de certificado sem suporte' e 'Rastreamento TLS: Gravação de alerta SSL3:fatal:certificado sem suporte'

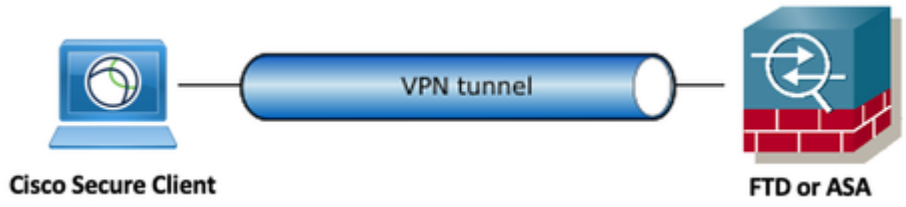
```
69ceb4f5.157b4993 0x7ff553fff700 TLS trace: SSL_accept:TLSv1.3 write server cer
tificate verify
69ceb4f5.157c01a4 0x7ff553fff700 TLS trace: SSL_accept:SSLv3/TLS write finished
69ceb4f5.157c458a 0x7ff553fff700 TLS trace: SSL_accept:TLSv1.3 early data
69ceb4f5.157c6685 0x7ff553fff700 TLS trace: SSL_accept:error in TLSv1.3 early d
ata
69ceb4f5.15b17eaa 0x7ff5522fc700 connection_get(15): got connid=1004
69ceb4f5.15b1b73f 0x7ff5522fc700 connection_read(15): checking for input on id=
1004
69ceb4f5.15b2bf05 0x7ff5522fc700 TLS trace: SSL_accept:TLSv1.3 early data
69ceb4f5.15b4c6c3 0x7ff5522fc700 TLS certificate verification: depth: 0, err: 2
6, subject: /CN=asa-server-only,69ceb4f5.15b4e8de 0x7ff5522fc700  issuer: /CN=T
est-CA
69ceb4f5.15b4f367 0x7ff5522fc700 TLS certificate verification: Error, unsupport
ed certificate purpose
69ceb4f5.15b57df8 0x7ff5522fc700 TLS trace: SSL3 alert write:fatal:unsupported
certificate
69ceb4f5.15b5b557 0x7ff5522fc700 TLS trace: SSL_accept:error in error
69ceb4f5.15b66c36 0x7ff5522fc700 TLS: can't accept: error:1417C086:SSL routines
:tls_process_client_certificate:certificate verify failed (unsupported certific
ate purpose).
69ceb4f5.15b70391 0x7ff5522fc700 connection_read(15): TLS accept failure error=
-1 id=1004, closing
69ceb4f5.15b747ae 0x7ff5522fc700 connection_close: conn=1004 sd=15
```

Solução: revise a solução proposta neste documento para garantir que o FTD ou ASA use o certificado de identidade correto, incluindo o atributo EKU de autenticação do cliente, para uma autenticação baseada em certificado bem-sucedida com o servidor LDAPS.

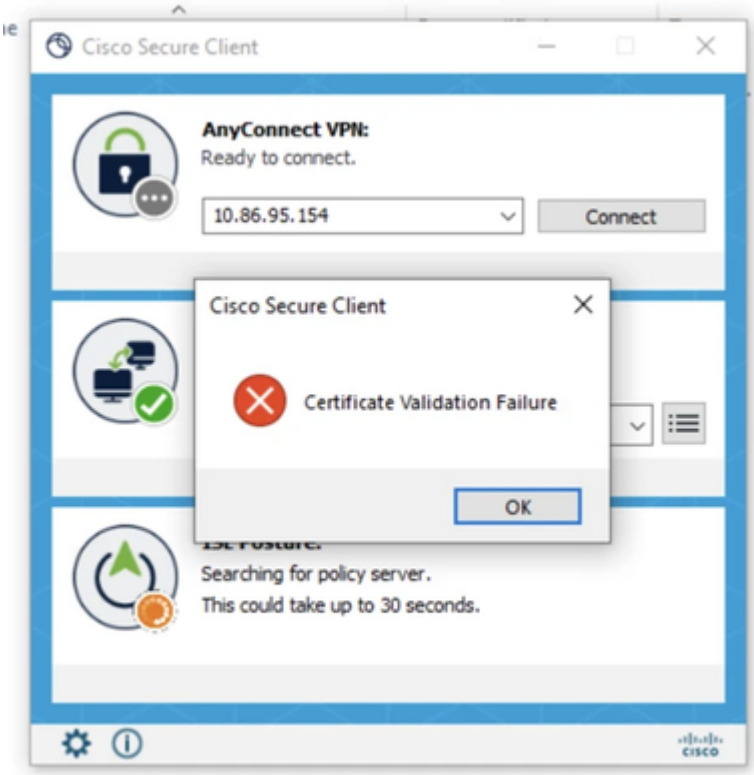
Problema 3. O Cisco Secure Client (antigo AnyConnect) poderá ter problemas de conexão com um FTD ou ASA se o certificado do cliente não tiver o atributo EKU de autenticação do cliente

Neste cenário, o Cisco Secure Client está usando a autenticação de certificado para estabelecer um túnel RAVPN para o FTD ou ASA. No entanto, se o certificado do cliente não tiver o atributo EKU de Autenticação do Cliente, a sessão de RAVPN falhará porque o ASA ou o FTD exigem que esse atributo esteja presente no certificado do cliente.

Topologia



Erro do Cisco Secure Client: 'Falha na validação do certificado'



Erros do Cisco Secure Client DART:Os seguintes logs do arquivo AnyConnectVPN.txt no pacote DART confirmam que o Cisco Secure Client rejeitou o certificado usado para a autenticação baseada em certificado RAVPN para o FTD/ASA devido à ausência do atributo EKU de autenticação do cliente (para localizar o arquivo AnyConnectVPN.txt no pacote DART, navegue até Cisco Secure Client > AnyConnect VPN > Logs > AnyConnectVPN.txt.).

<#root>

```
*******************************************

Date : 04/07/2026
Time : 03:35:22
Type : Error
Source : csc_vpnapi


Description : Function: CVerifyExtKeyUsage::compareEKUs


File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\CommonCrypt\Certificates\VerifyEx
Line: 330

EKU not found in certificate: 1.3.6.1.5.5.7.3.2



*******************************************

Date : 04/07/2026
Time : 03:35:22
```

```
Type : Information
Source : csc_vpnapi


Description : Function: CCertStore::GetCertificates


File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\CommonCrypt\Certificates\CertStor
Line: 225

Ignoring client certificate because it does not contain the required EKU extension.

 Certificate details:
Store: [Omitted Output]

*****************************************
```

Solução: revise as informações propostas neste documento para garantir que o Cisco Secure Client use o certificado correto, incluindo o atributo EKU de autenticação do cliente, para obter uma autenticação baseada em certificado bem-sucedida com o FTD ou ASA.

Note: A partir do erro de pacote DART acima 'EKU não encontrado no certificado: 1.3.6.1.5.5.7.3.2' , este número '1.3.6.1.5.5.7.3.2' corresponde ao OID de EKU de Autenticação de Cliente.

Problema 4. Túneis VPN site a site com autenticação baseada em certificado falharão se o certificado de identidade não tiver o atributo EKU de Autenticação de Cliente

Neste cenário, que envolve autenticação baseada em certificado para um túnel VPN site a site IKEv2, o certificado de identidade usado por FTD/ASA (1) para estabelecer o túnel para o par FTD/ASA (2) não tem o atributo EKU de autenticação de cliente. Como resultado, o túnel VPN não pode ser estabelecido porque o peer remoto, FTD/ASA (2), exige que esse atributo esteja presente no certificado.

Topologia

Erros de CLI de FTD ou ASA: Esses são os erros observados no FTD/ASA (2) durante a

autenticação baseada em certificado IKEv2 quando ele rejeita o certificado de identidade FTD/ASA (1) que não tem o atributo EKU de Autenticação de Cliente.

```
<#root>

Apr 09 2026 15:59:50:

%ASA-3-717027: Certificate chain failed validation. Certi. Peer certificate key usage is invalid,

 subject name: CN=ASAv3.cisco.com,OU=IT,O=Cisco,C=US,unstructuredName=ASAv3.cisco.com.
Apr 09 2026 15:59:50:

%ASA-3-717027: Certificate chain failed validation. Certificate chain is either invalid or not authorize

Apr 09 2026 15:59:50: %ASA-3-751006: Local:10.3.3.6:500 Remote:10.3.3.5:500 Username:10.3.3.5

IKEv2 Certificate authentication failed.  Error: Certificate authentication failed

Apr 09 2026 15:59:50: %ASA-4-750003: Local:10.3.3.6:500 Remote:10.3.3.5:500 Username:10.3.3.5

IKEv2 Negotiation aborted due to ERROR: Auth exchange failed

Apr 09 2026 15:59:50: %ASA-4-752012: IKEv2 was unsuccessful at setting up a tunnel.  Map Tag = CMAP.  M
Apr 09 2026 15:59:50: %ASA-3-752015: Tunnel Manager has failed to establish an L2L SA.  All configured
Apr 09 2026 15:59:55: %ASA-5-752003: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2.  Map Ta
Apr 09 2026 15:59:55: %ASA-5-750001: Local:10.3.3.6:500 Remote:10.3.3.5:500 Username:Unknown IKEv2 Rece
```

Note: No exemplo acima, o FTD/ASA (2) estava usando um certificado de identidade que incluía os atributos ClientAuth e ServerAuth EKU.

Note: No exemplo acima, o FTD/ASA (2) também pode ser substituído por um roteador ou um concentrador de VPN baseado em nuvem ou físico de terceiros. Em seguida, o mesmo problema persistirá, pois o peer de VPN requer que o atributo EKU de autenticação do cliente esteja presente no certificado usado pelo FTD/ASA (1) para autenticação baseada em certificado bem-sucedida.

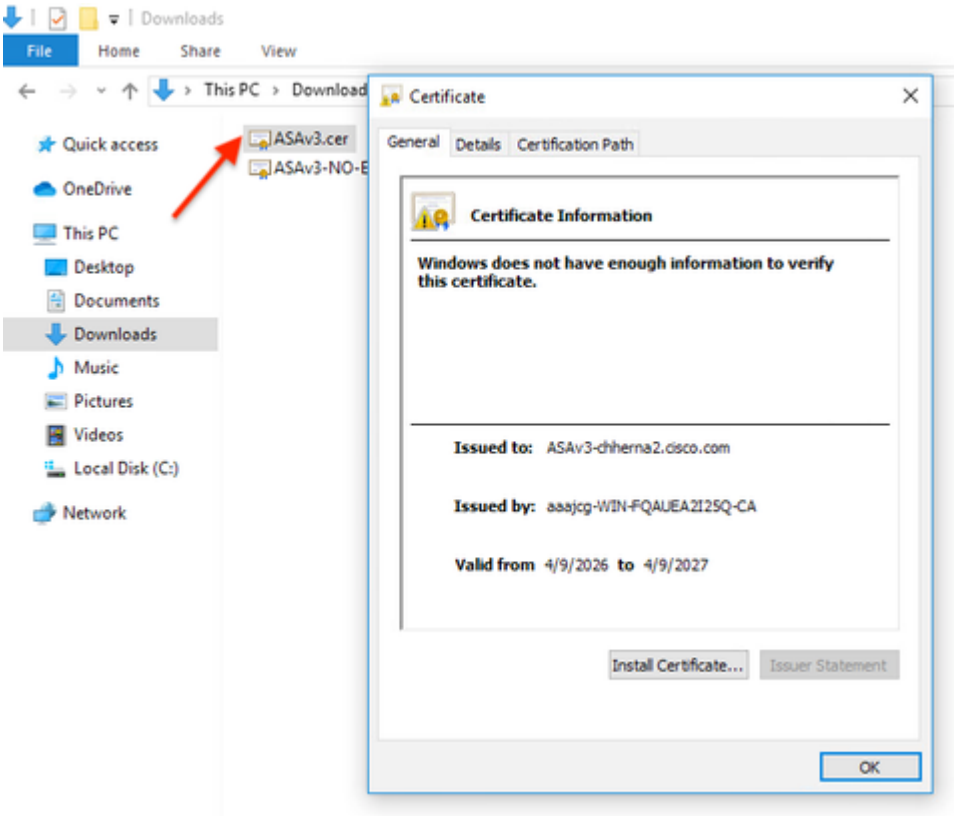
Solução: revise o proposto neste documento para garantir que o FTD/ASA (1) use o certificado de identidade correto, incluindo o atributo EKU de autenticação de cliente, para um túnel VPN site a site bem-sucedido com autenticação baseada em certificado.

Instruções para Confirmar se o seu Certificado Não Possui o Atributo EKU de Autenticação de Cliente

Verificar os Atributos EKU de um Certificado .cer usando o Gerenciador de Certificados do Windows

Siga as próximas etapas para verificar os atributos EKU de um certificado .cer usando o Gerenciador de Certificados do Windows:

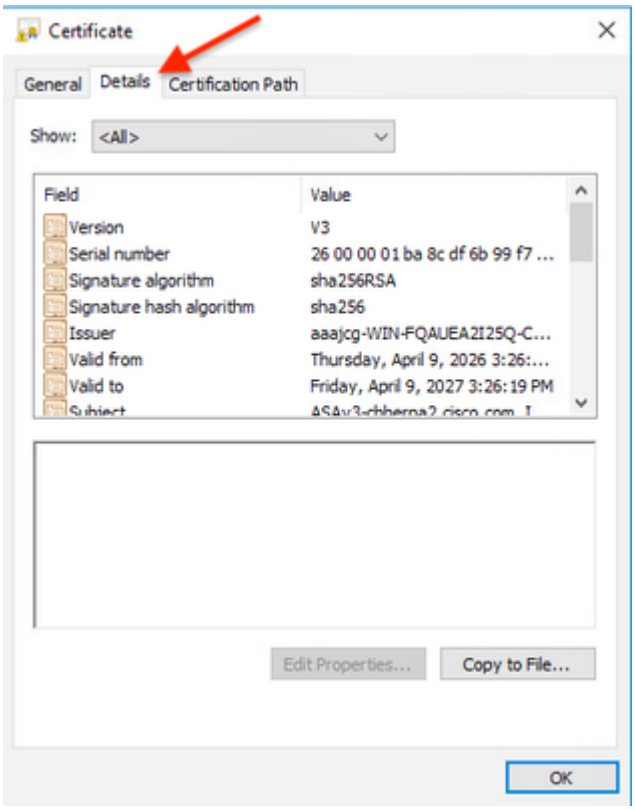
Etapa 1. Clique duas vezes no arquivo .cer para abri-lo no Gerenciador de Certificados do Windows.



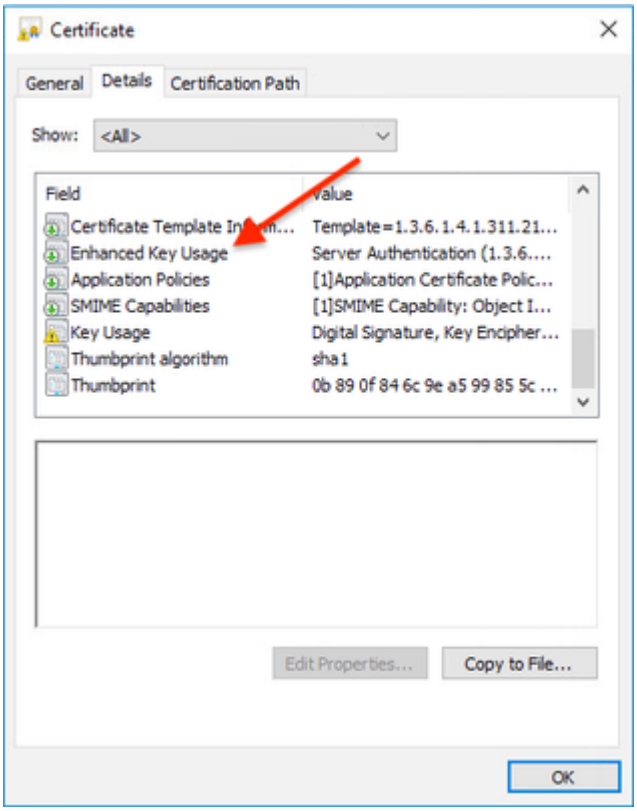
Note: Somente arquivos .cer serão abertos diretamente desta forma; se o seu certificado tiver uma extensão .pem, renomeie-o primeiro como .cer ou .crt.

Etapa 2. Manipular o aviso de segurança (se houver). Se um aviso de segurança for exibido, clique em Abrir para continuar.

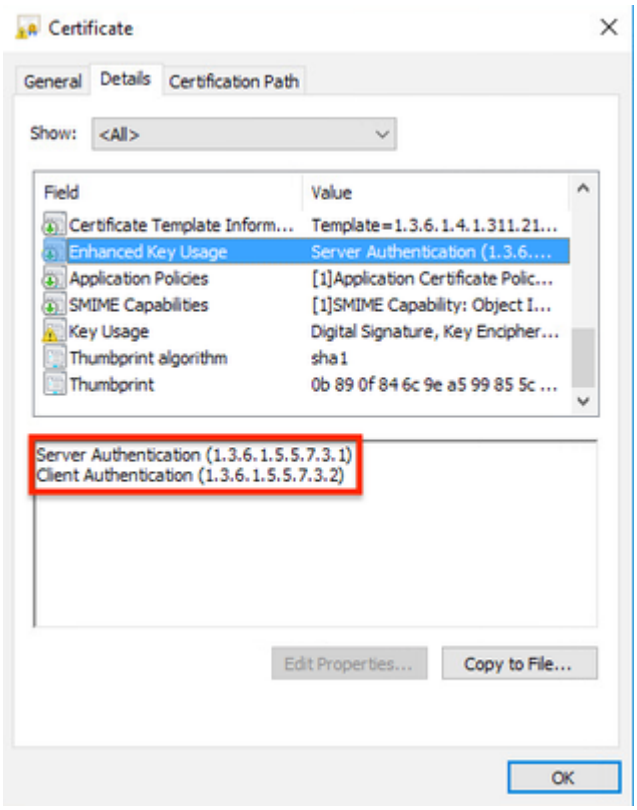
Etapa 3. Na janela do certificado, clique na guia Details (Detalhes).



Etapa 4. Percorra a lista de campos e selecione "Enhanced Key Usage" (ou Extended Key Usage).

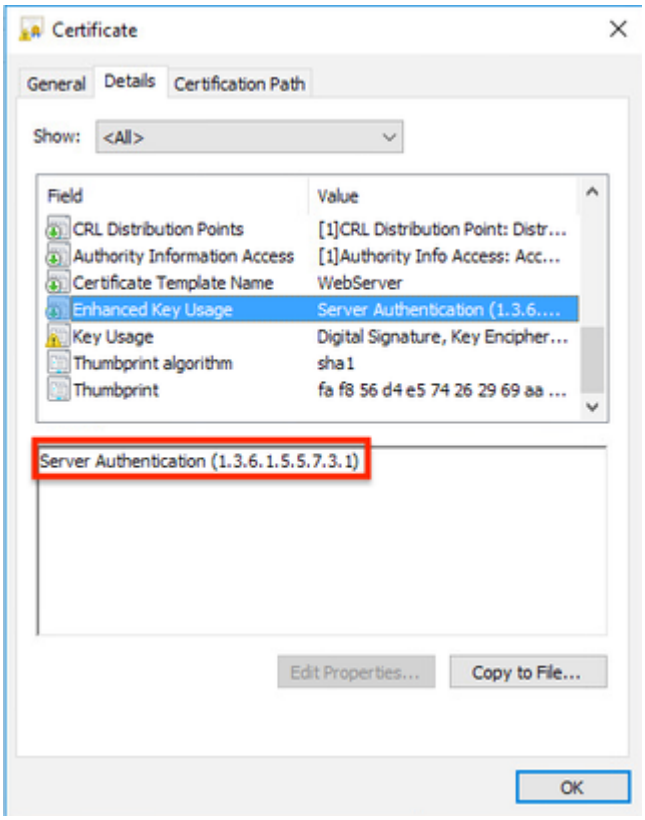


Etapa 5. Verifique os atributos de EKU; você poderá ver entradas como "Server Authentication" e "Client Authentication" indicando os valores de EKU presentes no certificado.

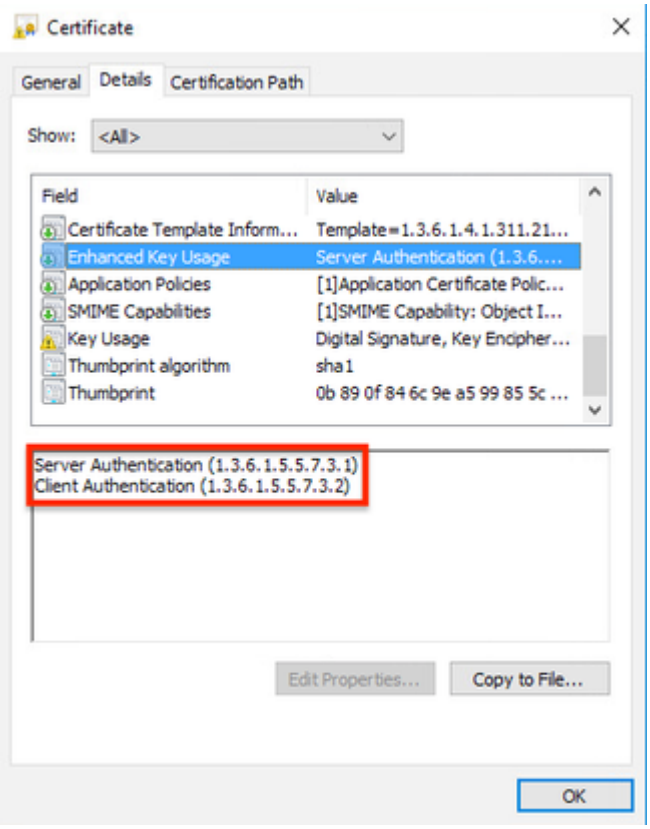


Etapa 6. Após a verificação, clique em OK para fechar a janela do certificado.

Exemplo 1: Este certificado .cer não tem o atributo EKU de Autenticação de Cliente e inclui somente o atributo EKU de Autenticação de Servidor.



Exemplo 2: Este certificado .cer inclui os atributos EKU de Autenticação de Servidor e de Cliente.



Verificar os atributos EKU de um certificado PKCS#12, PEM e .cer usando OpenSSL

Siga as próximas etapas para verificar os atributos EKU de um certificado .p12 (PKCS#12), .pem (PEM) e .cer:

Etapa 1. Localize o certificado que você precisa verificar e exporte-o no formato .p12 (PKCS#12), .pem (PEM) ou .cer.

Para certificados .p12 (PKCS#12), use openssl para extrair o certificado do arquivo .p12 (PKCS#12), o arquivo .p12 (PKCS#12) pode conter a chave privada, o certificado e os certificados de CA.

Use o seguinte comando para extrair o certificado de um arquivo .p12 (PKCS#12) em um arquivo .pem (PEM) (sem a chave privada ou cadeia de CA):

```
openssl pkcs12 -in yourfile.p12 -nokeys -clcerts -out cert.pem
```

- seuarquivo.p12: Substituir pelo nome real do arquivo.
- Talvez seja necessário digitar a senha para o arquivo .p12.
- cert.pem: O certificado foi extraído (sem a chave privada ou cadeia de CA) no formato .pem (PEM).

Etapa 2. Use os próximos comandos openssl para exibir os detalhes do certificado e os atributos EKU.

a) Para arquivos .pem, use o próximo comando openssl para exibir os detalhes do certificado e os atributos EKU:

```
openssl x509 -in cert.pem -text -noout
```

- cert.pem: Substituir pelo nome real do arquivo.

b) Para arquivos .cer, use o próximo comando openssl para exibir os detalhes do certificado e os atributos EKU:

```
openssl x509 -in yourfile.cer -text -noout
```

- seuarquivo.cer: Substituir pelo nome real do arquivo.

Etapa 3. Em seguida, procure a seção X509v3Extended Key Usage na saída, você pode ver entradas como "TLS Web Server Authentication" e "TLS Web Client Authentication" indicando os valores de EKU presentes no certificado.

```
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
```

OU o atributo EKU OIDs (Object Identifiers):

```
X509v3 Extended Key Usage:
1.3.6.1.5.5.7.3.1, 1.3.6.1.5.5.7.3.2
```

- EKU OID de autenticação de servidor: 1.3.6.1.5.5.7.3.1
- OID de EKU de Autenticação de Cliente: 1.3.6.1.5.5.7.3.2

Exemplo 1: Este certificado .pem (PEM) não tem o atributo EKU de Autenticação de Cliente e inclui somente o atributo EKU de Autenticação de Servidor.

<#root>

```
MyHost$ openssl x509 -in cert.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            26:00:00:01:b7:e7:90:48:d6:f9:41:d3:54:00:01:00:00:01:b7
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=com, DC=aaajcg, CN=aaajcg-WIN-FQAUEA2I25Q-CA
        Validity
            Not Before: Mar 27 00:31:40 2026 GMT
            Not After : Mar 26 00:31:40 2028 GMT
        Subject: C=MX, ST=MX, L=MX, O=Cisco, OU=IT, CN=vFMC3-chherna2
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:cf:a8:a0:ff:dd:34:73:7d:46:86:85:05:b6:0c:
                    5e:32:8c:6f:6f:88:52:03:58:63:c6:89:d8:fc:55:
                    c5:58:ba:eb:45:88:b2:21:9e:c5:d8:67:57:39:0f:
                    91:a5:41:61:fa:94:b1:ad:9e:71:26:87:b6:30:ae:
                    a7:f6:89:b1:6d:61:ce:fa:47:7f:2a:d8:e8:4d:26:
                    4f:a7:d3:eb:5a:69:16:46:71:c7:55:cf:87:b4:10:
                    96:f2:10:6b:c0:a7:3d:3c:49:9d:ee:77:8c:b5:95:
                    9b:69:81:e0:2d:a0:6e:5c:78:73:22:5a:38:d0:74:
                    38:b2:ba:e0:ab:c5:44:eb:e1:3c:52:86:b8:2a:4e:
                    37:44:9c:34:d8:d8:6c:ae:3e:df:12:57:0e:28:52:
                    57:dc:6d:62:ea:b6:ec:19:4e:90:8f:3f:2c:23:1b:
                    e2:39:f0:ba:07:08:9a:0b:97:96:05:2e:69:fe:9a:
                    b2:b2:74:9a:ba:06:25:bc:38:1c:94:87:8e:2a:dc:
                    2f:0b:a6:31:6c:bf:11:96:2a:71:b3:87:e5:f5:cb:
                    88:f1:73:cf:88:d7:30:78:24:77:7c:b7:2c:7c:83:
                    6d:69:5b:bd:d4:21:b9:ee:19:c4:02:be:7b:44:a2:
                    55:d6:b2:95:11:46:bf:db:3e:4f:9a:8c:d4:ad:8d:
                    82:f5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                0D:8E:DA:07:6D:49:EA:51:D2:C7:EF:50:CE:CE:2B:8E:7C:DF:A6:8D
            X509v3 Authority Key Identifier:
                keyid:3A:45:60:22:F7:C8:2C:0D:D2:98:5A:BC:E0:98:D4:91:1D:67:32:22

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:ldap:///CN=aaajcg-WIN-FQAUEA2I25Q-CA,CN=WIN-FQAUEA2I25Q,CN=CDP,CN=Public%20Key%20

            Authority Information Access:
                CA Issuers - URI:ldap:///CN=aaajcg-WIN-FQAUEA2I25Q-CA,CN=AIA,CN=Public%20Key%20Services
```

```
            1.3.6.1.4.1.311.20.2:
                ...W.e.b.S.e.r.v.e.r
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment


X509v3 Extended Key Usage:

        <-------- "EKU SECTION"


TLS Web Server Authentication


  <-------- "Server Authentication EKU Attribute Included"
    Signature Algorithm: sha256WithRSAEncryption
         2f:27:cd:95:7d:5c:40:fa:29:64:df:75:7d:7a:87:9b:b0:94:
         0e:6b:07:4d:d2:7e:83:da:03:08:f3:50:0d:5b:05:8c:1f:54:
         46:fe:53:f3:e2:d4:0a:ba:37:4f:cd:a4:49:04:74:79:09:23:
         d6:06:af:69:d2:7b:f5:bc:ec:fe:ce:e4:c9:07:31:d7:85:45:
         55:78:d3:42:45:f9:ce:cd:bf:43:53:b4:8e:4c:af:64:4b:a6:
         dc:47:d0:16:4e:73:62:fd:c8:5e:37:74:cb:68:48:29:7d:f9:
         41:b3:d1:46:56:24:83:23:5c:bd:b0:e3:7c:f9:8a:af:da:09:
         d0:c2:7d:4a:e6:24:0f:e6:fc:6e:0d:65:8c:96:8c:af:21:b2:
         7f:4b:bb:1c:17:33:b1:db:00:f3:12:e3:53:39:d0:e7:6a:48:
         4c:c6:4f:29:6f:74:ff:2d:a7:e5:ea:e8:89:fe:a4:2b:cd:e3:
         61:6a:9e:11:52:15:57:f2:b8:e8:fa:78:31:20:49:d9:50:f9:
         70:3f:1e:aa:9c:1a:bb:0b:59:66:1e:85:bd:76:e7:73:6f:ec:
         86:30:b0:dd:86:3c:b3:a0:7b:fb:b7:74:5d:38:88:82:3d:a3:
         2d:8c:a5:e4:db:37:eb:be:7f:62:bc:87:7c:35:17:32:fc:52:
         c5:d3:c5:8f
```

Exemplo 2: Esse certificado .pem (PEM) inclui os atributos EKU de autenticação de cliente e servidor.

<#root>

```
MyHost$ openssl x509 -in cert.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            26:00:00:01:b6:74:fc:b4:1e:99:be:7a:10:00:01:00:00:01:b6
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=com, DC=aaajcg, CN=aaajcg-WIN-FQAUEA2I25Q-CA
        Validity
            Not Before: Mar 26 23:44:58 2026 GMT
            Not After : Mar 26 23:44:58 2027 GMT
        Subject: C=MX, ST=AD, L=AD, O=Cisco, OU=IT, CN=vFMC3-chherna2
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
```

```
                    00:ab:aa:67:4e:55:19:3b:38:6c:33:2e:ba:fd:19:
                    56:e7:68:f8:f7:e9:53:95:1f:53:b4:f1:ce:94:c8:
                    ca:41:f1:52:15:eb:a5:35:9f:07:95:9f:c3:8a:5e:
                    62:d6:e1:5c:04:c5:c0:27:1c:84:ed:3d:1b:42:50:
                    91:4a:a6:86:90:e0:6e:26:7e:37:fd:17:0c:2f:bb:
                    fe:58:81:ec:3b:9d:0b:fc:dd:8c:6b:dd:ab:d3:96:
                    74:23:0d:78:d7:09:53:61:f9:b0:29:c6:7c:e2:9c:
                    2f:74:30:42:0f:45:47:cd:16:59:ed:53:62:8f:60:
                    75:f8:24:f5:1f:77:fb:89:85:4b:49:ad:93:43:04:
                    6e:4a:b3:59:fc:eb:75:70:39:67:71:60:be:b3:b7:
                    86:f7:c5:53:28:1e:bf:8f:b2:52:ec:79:d6:12:b0:
                    33:9c:6d:46:7a:9c:5d:53:a5:44:24:da:4b:36:7d:
                    c2:ec:61:d7:a0:01:c3:d2:bc:0a:df:a8:f6:0c:82:
                    48:30:fb:c6:3e:4a:48:a9:01:13:f5:4e:f2:03:24:
                    38:ee:aa:d9:60:78:30:45:ed:3b:76:16:fd:7a:d3:
                    b0:16:10:28:75:fc:41:32:e6:6d:cb:c3:96:58:77:
                    9e:11:0a:9b:33:c7:92:8d:75:1f:e5:30:29:a4:a5:
                    ba:7d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                D2:DF:62:25:17:DB:72:31:D8:D2:D0:41:CB:FB:DD:00:FF:38:BD:BB
            X509v3 Authority Key Identifier:
                keyid:3A:45:60:22:F7:C8:2C:0D:D2:98:5A:BC:E0:98:D4:91:1D:67:32:22

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:ldap:///CN=aaajcg-WIN-FQAUEA2I25Q-CA,CN=WIN-FQAUEA2I25Q,CN=CDP,CN=Public%20Key%20

            Authority Information Access:
                CA Issuers - URI:ldap:///CN=aaajcg-WIN-FQAUEA2I25Q-CA,CN=AIA,CN=Public%20Key%20Services

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            1.3.6.1.4.1.311.21.7:
                0-.%+.....7.....^..9...
...b.../ ...R...Z..d...


X509v3 Extended Key Usage:


         <-------- "EKU SECTION"


TLS Web Server Authentication, TLS Web Client Authentication


  <----- "Server & Client EKU Attributes Included"
            1.3.6.1.4.1.311.21.10:
                0.0
..+.......0
..+.......
            S/MIME Capabilities:
......0...+....0050...*.H..
..*.H..
    Signature Algorithm: sha256WithRSAEncryption
         3f:66:b1:35:7e:05:b4:69:f1:81:95:b8:18:90:f2:20:bd:8d:
         ff:03:5a:59:ca:02:ba:2d:1d:e0:8d:3f:63:e9:fe:71:3c:9a:
         11:15:5c:3b:fc:62:e4:cf:15:25:4c:74:5e:ad:3f:09:e9:3b:
         d5:08:95:7d:97:7a:ef:c1:16:6d:e0:7a:0b:21:81:46:bc:15:
```

```
c3:76:8c:fe:fb:14:94:36:92:0d:3b:4a:c9:8f:6a:bd:dc:4b:
0b:24:c3:32:35:27:e7:aa:23:95:85:e4:a9:64:71:f0:98:9e:
33:aa:6e:bd:7c:dd:dc:4b:cf:dd:0e:a7:ea:e8:aa:61:8f:67:
84:da:5b:be:8e:05:75:c8:eb:46:13:6f:14:4d:fe:4e:57:3c:
29:27:cc:0b:5b:25:87:37:24:12:79:b1:c3:78:c8:94:fe:df:
3c:77:aa:fc:f2:ee:ae:9b:ab:88:29:f9:ee:04:c2:48:5f:21:
9e:1c:25:cc:c9:c5:9c:23:8f:af:87:76:5e:46:74:ac:73:57:
01:ba:71:ae:46:e1:87:3c:94:6c:19:f7:fe:8e:66:9d:c7:1f:
b0:87:4b:65:e2:fc:d6:10:7c:44:57:56:5d:68:bb:df:f0:36:
0e:07:c5:8a:be:56:86:97:3d:a7:1c:8b:86:df:0b:51:b5:97:
cc:67:09:8e
```

Soluções

Os administradores podem escolher uma das seguintes opções alternativas.

Opção 1. Mudar para ACs raiz públicas que fornecem certificados EKU combinados

Algumas CAs raiz públicas, como DigiCert e IdenTrust, emitem certificados com tipos de EKU combinados (certificados de servidor e cliente) de uma raiz alternativa, que pode não ser incluída no Chrome Root Store. Coordene com o provedor de CA para verificar a disponibilidade desses certificados e, antes de implantá-los, assegure-se de que o servidor que apresenta o certificado e os clientes que o consomem confiem na CA raiz correspondente.

Essa abordagem alivia a necessidade de atualizar o software do servidor para atenuar o desligamento do EKU de Autenticação do Cliente imposto pela Política do Programa Chrome Root.

A tabela a seguir, que mostra exemplos de CAs raiz públicas e tipos de EKU, não é uma lista completa e é apenas para fins ilustrativos.

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
IdenTrustName	clientAuth	CA raiz do setor público IdenTrust 1	Autoridade de certificação TrustID RSA ClientAuth 2
IdenTrustName	serverAuth (navegador confiável)	Raiz Comercial IdenTrust CA 1	Servidor Hydrant CA O1
DigiCert	clientAuth + serverAuth	Raiz G2 do ID Assegurado do DigiCert	ID garantida do DigiCert CA G2
DigiCert	clientAuth	Raiz G2 do ID	Cliente de ID garantida DigiCert

Fornecedor de CA	Tipo de EKU	CA raiz	Emitente/Sub CA
		Assegurado do DigiCert	CA G2
DigiCert	serverAuth (navegador confiável)	Raiz Global G2 DigiCert	DigiCert Global G2 TLS RSA SHA256

Opção 2. Renovar os certificados atuais para estender sua validade

Os certificados emitidos por autoridades de certificação raiz públicas antes de maio de 2026 que tenham EKU de Autenticação de Servidor e de Cliente continuarão a ser honrados até o termo. No entanto, é melhor renovar os certificados EKU combinados antes que ocorra o desligamento da política.

- A política de CA pública e as datas de implementação podem variar de acordo com o fornecedor.
- Verifique com a CA e planeje a renovação do certificado de acordo.
- Depois de 15 de março de 2026, os certificados públicos emitidos por CA são válidos apenas por 200 dias.
- Leve em consideração que algumas CAs públicas pararam de emitir certificados EKU combinados.

Opção 3. Migrar para PKI privada para emitir certificados EKU (servidor e cliente) combinados

Avaliar a viabilidade da transição para uma infraestrutura de chave pública privada (PKI) e, em seguida, configurar uma CA privada para emitir certificados únicos com EKU combinado (certificados de servidor e cliente com os EKUs necessários).

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.

Opção 4. Obter um certificado de confiança pública somente com EKU de Autenticação de Cliente

Algumas CAs, como SSL.com, oferecem certificados de autenticação de cliente dedicados. Eles são separados de certificados TLS e geralmente usados para autenticação corporativa.

⚠ Caution: Para ambientes de produção, é altamente recomendável que os clientes usem certificados com os

---

atributos EKU apropriados. Essa prática garante a segurança, a compatibilidade e a adesão aos padrões do setor e às práticas recomendadas. Os certificados sem atributos EKU devem ser considerados apenas como uma solução temporária e apenas com um claro entendimento dos riscos associados.

Perguntas frequentes

P1. Preciso me preocupar com isso se usar uma PKI privada?

R: A política aplicada por CAs privadas é determinada por cada organização. Se sua CA privada adotar os mesmos critérios de emissão, como remover o atributo EKU de autenticação de cliente dos certificados, as diretrizes fornecidas neste documento serão aplicáveis.

P2. Posso continuar usando meus certificados existentes?

R: Sim, certificados válidos com EKU combinado podem ser usados até tempodeexpiração.

P3. Que opções estão disponíveis para integrar meu FMC ou FDM ao ISE por meio do pxGrid se o certificado instalado no FMC/FDM não tiver o atributo EKU de Autenticação de Cliente?

R: Além das soluções propostas neste documento, é altamente recomendável verificar as seguintes referências do ISE:

- Nota de campo: FN74392 - Cisco Identity Services Engine: Impacto nas comunicações seguras de alterações de EKU de autenticação de cliente de CA pública a partir de maio de 2026 - Solução alternativa fornecida
- Preparar o Identity Services Engine para Restrições de Uso Estendido de Chave em Certificados Emitidos por Autoridades de Certificação Públicas

Note: Mesmo que o IMS ofereça suporte ao uso de um certificado assinado por uma CA pública. A Cisco recomenda o uso do certificado CA interno do ISE, pois essa comunicação é somente para transações internas.

P4. O que é a EKU "Client Authentication" e por que ela estava em meu certificado?

R: A EKU "Client Authentication" indica que um certificado pode ser usado por um cliente para se autenticar em um servidor. Algumas CAs historicamente o incluíam em certificados TLS por

padrão, mas ele nunca era necessário para a segurança normal do site.

P5. Meu certificado TLS atual diz "Autenticação de Cliente" em seu Uso Estendido de Chave. Agora é inválido?

R: Não, ele continua válido. Você não precisa substituí-lo imediatamente. Quando você renova, o novo certificado simplesmente não inclui o EKU clientAuth.

P6. Como posso verificar se um certificado tem o EKU clientAuth?

R: Você pode inspecionar os detalhes do certificado usando as ferramentas OpenSSL, PowerShell ou GUI para verificar a extensão do Uso Estendido de Chave.

P7. Ainda posso obter um certificado de confiança pública somente com o EKU de Autenticação de Cliente?

R: Algumas CAs, como SSL.com, oferecem certificados de autenticação de cliente dedicados. Eles são separados de certificados TLS e geralmente usados para autenticação corporativa.

P8. Isso afeta outros EKUs ou tipos de certificado (assinatura de código, e-mail, etc.)?

R: Não, esta alteração é específica para certificados de servidor TLS. A assinatura de código e os certificados de e-mail têm seus próprios requisitos de EKU.

P9. Onde posso ver os requisitos oficiais sobre essa alteração?

R: A Google Chrome Root Program Policy fornece diretrizes sobre a proibição do EKU clientAuth em certificados de servidor TLS.

P10. É seguro usar certificados sem atributos de EKU de cliente e servidor em meu ambiente de produção?

R: Para ambientes de produção, é altamente recomendável que os clientes usem certificados com os atributos EKU apropriados. Essa prática garante a segurança, a compatibilidade e a adesão aos padrões do setor e às práticas recomendadas. Os certificados sem atributos EKU devem ser considerados apenas como uma solução temporária e apenas com um claro entendimento dos riscos associados.

Informações Relacionadas

- Para obter assistência adicional, entre em contato com o Cisco Technical Assistance Center (TAC). É necessário um contrato de suporte válido: Cisco Worldwide Support Contacts.
- Suporte e downloads da Cisco: Suporte técnico e downloads da Cisco

Bugs relacionados

- CSCwt9492 ENH: O FMC deve validar a presença do atributo EKU de Autenticação do Cliente no certificado do cliente usado para a Integração do pxGrid
- CSCwt94509 ENH: O FMC deve exibir uma mensagem indicando que o atributo EKU de autenticação do cliente é necessário no certificado do cliente usado para integração com pxGrid
- CSCwt61767 May 2026 EKU Server-Only Change - Emitir aviso de configuração ASA se EKU inadequado
- CSCws83036 EKU: Avaliação de impacto da aplicação de ClientAuth EKU no ISE

Referências do Cisco ISE

- Nota de campo: FN74392 - Cisco Identity Services Engine: Impacto nas comunicações seguras de alterações de EKU de autenticação de cliente de CA pública a partir de maio de 2026 - Solução alternativa fornecida
- Preparar o Identity Services Engine para Restrições de Uso Estendido de Chave em Certificados Emitidos por Autoridades de Certificação Públicas

Referências externas

- Política do programa Chrome Root
- Portal IdenTrust

- SSL - Remoção do EKU de autenticação de cliente dos certificados do servidor TLS - o que você precisa saber

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.