Impacto de Cisco Secure Firewall en los cambios de EKU de autenticación de clientes de CA pública a partir de mayo de 2026 para comunicaciones seguras

Introducción

Este documento describe el impacto de las restricciones en los criterios de emisión de certificados impuestas por las autoridades de certificados que cumplen con el programa Chrome Root Certificate, específicamente en lo que se relacionan con los productos Cisco Secure Firewall.

Antecedentes

Los certificados TLS de confianza pública son emitidos por CA que deben cumplir con las políticas del sector que rigen la emisión y el uso de certificados.

LaChrome Root Program Policy, operado por Google, define los requisitos que las CA deben seguir para que sus certificados sean confiados por el navegador de Google Chrome. Estos requisitos influyen en el modo en que se emiten los certificados de confianza pública en el sector. Como parte de la evolución de las prácticas de seguridad, el programa de raíz de Chrome está introduciendo directrices más estrictas en torno al uso de certificados.

Por lo tanto, muchas CA públicas están dejando de emitir certificados que incluyen EKU de autenticación de cliente y están realizando la transición hacia la emisión de certificados destinados únicamente a la autenticación del servidor. Como resultado, se espera que los certificados recién emitidos de muchas CA públicas incluyan sólo EKU de autenticación de servidor.

El uso extendido de claves (EKU), es una extensión de certificado que define la función deseada de una clave pública dentro de un certificado digital. Establece un conjunto estructurado de aplicaciones permitidas, lo que garantiza que la clave sólo se utilice para operaciones criptográficas específicas. Esta funcionalidad se rige por los identificadores de objeto (OID): identificadores numéricos únicos que clasifican cada uso permitido, como la firma de código, la autenticación del servidor, la autenticación del cliente o el correo electrónico seguro.

Cuando la autenticación se basa en certificados, la entidad verificadora revisa el certificado para identificar el

identificador de objeto (OID) dentro de la EKU. Al incrustar la extensión EKU, una autoridad certificadora (CA) restringe el ámbito del certificado a funciones predefinidas, con cada finalidad designada asignada explícitamente a un OID.

Finalidad de los atributos EKU

· Defina el uso: Los atributos EKU aclaran qué tipos de autenticación o cifrado puede realizar el certificado.

· Mejore la seguridad: Al restringir los certificados a usos específicos, EKU ayuda a evitar el uso indebido o las aplicaciones no deseadas (por ejemplo, no se puede utilizar un certificado de servidor para la autenticación de clientes).

· Cumplimiento: Garantiza que los certificados se utilizan de acuerdo con las políticas de seguridad y los estándares del sector.

Usos principales de los atributos EKU

1. Autenticación de cliente web TLS

· Permite utilizar certificados para identificar y autenticar usuarios o dispositivos en un servidor.

· OID: 1.3.6.1.5.5.7.3.2

· Se utiliza en VPN, TLS mutuo y escenarios de inicio de sesión seguro.

2. Autenticación del servidor web TLS

· Permite que los servidores utilicen los certificados para demostrar su identidad a los clientes.

· OID: 1.3.6.1.5.5.7.3.1

· Se utiliza en servidores web HTTPS, SSL/TLS y terminales API seguros.

3. Firma de código

· Indica que el certificado se puede utilizar para firmar software o ejecutables.

· OID: 1.3.6.1.5.5.7.3.3

· Se utiliza en la distribución de software y comprobaciones de integridad.

4. Protección del correo electrónico

· Permite utilizar certificados para firmar y cifrar mensajes de correo electrónico.

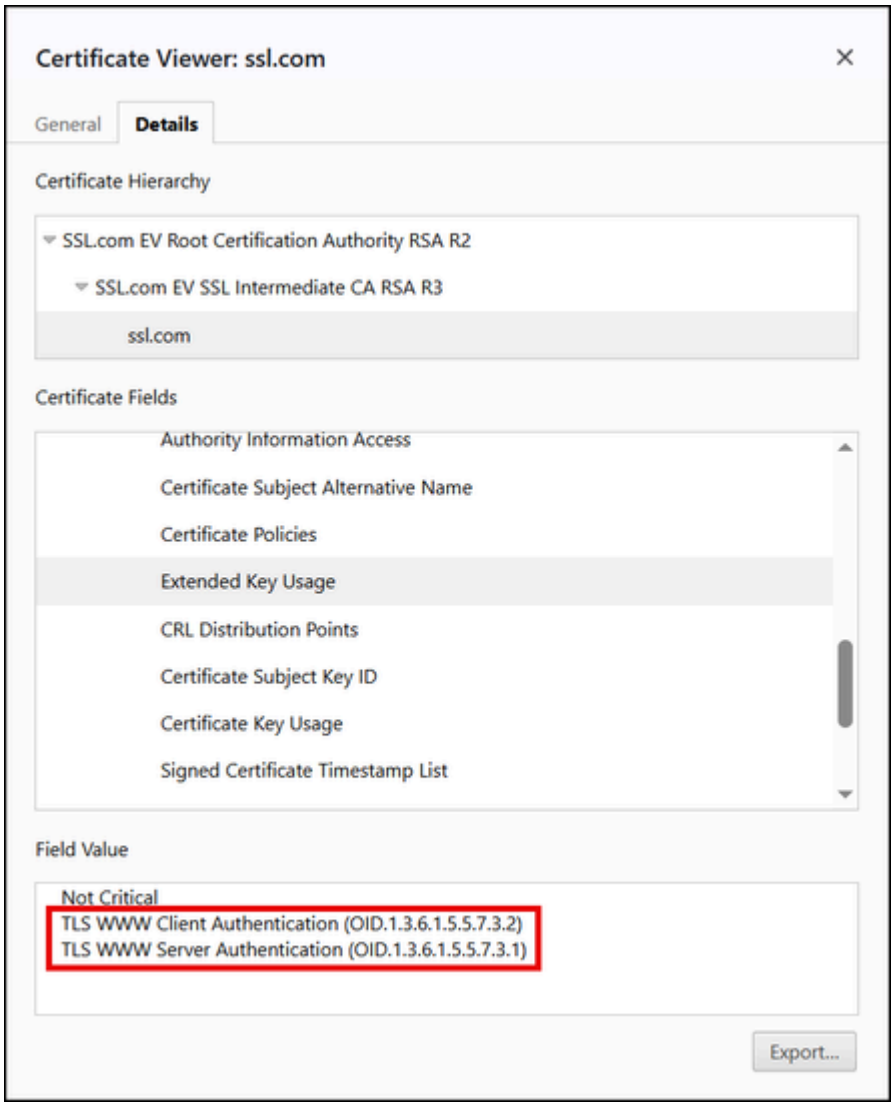
· OID: 1.3.6.1.5.5.7.3.4

· Se utiliza en la seguridad de correo electrónico S/MIME.

5. Otros fines

· Firma de documentos, marca de tiempo, inicio de sesión con tarjeta inteligente, etc., cada uno con sus propios OID.

Los exploradores y servidores sólo necesitan el serverAuth EKU para establecer una conexión segura para HTTPS, pero históricamente, muchos certificados de servidor TLS incluían tanto el serverAuth como el clientAuth, a continuación se muestra un ejemplo de dicho certificado:



¿Por qué la eliminación de la autenticación de cliente EKU de los certificados del servidor?

- Seguridad y alcance: los certificados TLS públicos solo deben autenticar servidores en la Web. La eliminación proporciona una separación clara entre la funcionalidad del servidor y la del cliente. ClientAuth EKU se utiliza para la autenticación de máquinas y usuarios con TLS mutuo (mTLS) y otros escenarios de autenticación.

- Evitar errores de configuración: algunos sistemas pueden confiar en cualquier certificado de una CA pública para la autenticación de cliente si está presente la EKU, lo que podría suponer un riesgo para la seguridad.

- Requisitos del navegador: Los navegadores principales no requieren o verifican la EKU de autenticación del cliente en el certificado de un sitio web.

- Arquitectura PKI simplificada: al separar los usos, las CA pueden mantener jerarquías de certificados distintas para TLS de servidor frente a otros fines.

Esto es especialmente importante para productos como Cisco Secure Firewall Adaptive Security Appliance (ASA), Cisco

Secure Firewall Threat Defense (FTD), Cisco Secure Firewall Device Manager (FDM) y Cisco Secure Firewall Management Center (FMC) que podrían actuar como servidor o cliente durante la autenticación de TLS, en función del caso práctico.

Impacto en entornos de servidores

Para la gran mayoría de las implementaciones de servidores, este cambio será de bajo impacto o no tendrá impacto. Esto es lo que cabe esperar:

- Servidores web estándar (HTTPS): sin impacto. Los certificados actualizados seguirán funcionando con normalidad.
- Certificados existentes: cualquier certificado emitido antes del corte seguirá funcionando hasta que caduque.
- Escenarios de certificados de cliente y TLS mutuo (mTLS): si estaba utilizando un certificado de servidor TLS para la autenticación de cliente, necesitará obtener un certificado independiente con la EKU de autenticación de cliente de otro origen.
- Sistemas empresariales que requieren ambas EKU: algunos sistemas empresariales o heredados esperaban ambas EKU. Debe comprobar si las actualizaciones son necesarias para cumplir con las nuevas reglas.

Descripción de problemas

A partir de mayo de 2026, muchas autoridades de certificación públicas (CA) dejarán de emitir certificados de seguridad de la capa de transporte (TLS) que incluyen el uso extendido de claves de autenticación de clientes (EKU). Los certificados recién emitidos normalmente sólo incluirán EKU de autenticación de servidor.

Como resultado, si los certificados emitidos por una CA pública se renuevan conforme a las políticas de CA actualizadas y luego se implementan en los productos Cisco Secure Firewall, los servicios donde se requiere autenticación de cliente EKU fallarán. Los servicios específicos afectados son los siguientes:

- Cuando ASA, FTD, FDM o FMC actúa como cliente (por ejemplo, al conectarse a proveedores de identidad o servidores de autenticación como ISE (pxGrid), RADIUS, LDAPS o Active Directory), la autenticación basada en certificados puede fallar si el certificado de cliente fue generado por una CA pública y falta la EKU de autenticación de cliente. En estos escenarios, si el servidor de autenticación rechaza los certificados sin la EKU requerida, pueden ocurrir fallas de conexión.
- Cisco Secure Client (anteriormente AnyConnect) puede autenticarse en los servidores ASA o FTD mediante

certificados. Sin embargo, si el certificado de cliente fue generado por una CA pública y falta la EKU de autenticación de cliente, la conexión VPN de acceso remoto (RAVPN) fallará.

- Cuando el FTD o el ASA establecen un túnel VPN de sitio a sitio (ya sea a otro FTD, ASA, router de Cisco o un par VPN de terceros) mediante autenticación de certificado (RSA o ECDSA), el túnel fallará si el certificado de identidad generado por una CA pública no tiene el atributo EKU de autenticación de cliente. Esto ocurre porque el par VPN remoto requiere que la EKU de autenticación de cliente esté presente en el certificado de identidad.

Cambio de la política del programa raíz de Chrome

La implementación de la EKU depende de que la CA firme el certificado. El uso de la autenticación de servidor y la autenticación de cliente EKU era una práctica común. Sin embargo, como parte de la modificación de la directiva del programa raíz de Chrome, las CA que se alinean con estos criterios de emisión de certificados están interrumpiendo la firma de certificados TLS que incluyen el uso extendido de claves de autenticación de cliente (EKU). Los certificados recién emitidos sólo incluyen EKU de autenticación de servidor.

Requisitos de política clave

- Las CA raíz públicas deben afirmar el uso de clave ampliada (EKU) SOLO para la autenticación de servidor (id-kp-serverAuth)

- Los certificados deben incluir SOLO EKU de autenticación de servidor.

- La inclusión de EKU de autenticación de cliente en estos certificados está prohibida

- Las CA raíz que continúan emitiendo certificados con autenticación de cliente EKU se eliminan finalmente del almacén raíz de Chrome, lo que provoca que el explorador de Chrome marque los certificados como "no fiables"

Plazos

- En septiembre de 2025, SSL.com emitirá certificados TLS que solo incluyan la ServerAuth EKU (y no ClientAuth) para los certificados de servidor. En otras palabras, los nuevos certificados SSL/TLS para su sitio web o servidor serán explícitamente para "Autenticación de servidor" solamente.

- Octubre de 2025: las CA que se alinean con el programa (por ejemplo, DigiCert, Sectigo, etc.) comenzaron a emitir certificados solo de servidor de forma predeterminada.

- Mayo de 2026: las CA que se alinean con el programa dejan de emitir certificados EKU de autenticación de cliente

- Marzo de 2027: La política del programa de raíz de Chrome se vuelve totalmente efectiva

Impacto en los productos Cisco Secure Firewall

Después de que las CA públicas comiencen a incluir solamente la EKU de autenticación de servidor en los certificados emitidos. Esto podría tener el siguiente impacto en los próximos escenarios de productos de Cisco Secure Firewall:

- Cuando ASA, FTD, FDM o FMC actúa como cliente (por ejemplo, al conectarse a proveedores de identidad o servidores de autenticación como ISE (pxGrid), RADIUS, LDAPS o Active Directory), la autenticación basada en certificados puede fallar si el certificado de cliente fue generado por una CA pública y falta la EKU de autenticación de cliente. En estos escenarios, si el servidor de autenticación rechaza los certificados sin la EKU requerida, pueden ocurrir fallas de conexión.

- Cisco Secure Client (anteriormente AnyConnect) puede autenticarse en los servidores ASA o FTD mediante certificados. Sin embargo, si el certificado de cliente fue generado por una CA pública y falta la EKU de autenticación de cliente, la conexión VPN de acceso remoto (RAVPN) fallará.

- Cuando el FTD o el ASA establecen un túnel VPN de sitio a sitio (ya sea a otro FTD, ASA, router de Cisco o un par VPN de terceros) mediante autenticación de certificado (RSA o ECDSA), el túnel fallará si el certificado de identidad generado por una CA pública no tiene el atributo EKU de autenticación de cliente. Esto ocurre porque el par VPN remoto requiere que la EKU de autenticación de cliente esté presente en el certificado de identidad.

Nota: si está integrando FMC o FDM con ISE a través de pxGrid y los certificados instalados en FMC/FDM carecen del atributo EKU de autenticación de cliente, revise las soluciones alternativas propuestas en este documento y las siguientes referencias a ISE: FN74392 y Prepare Identity Services Engine para las restricciones de uso de clave ampliada en los certificados emitidos por entidades de certificación públicas.

Nota: La eliminación de la EKU clientAuth de los certificados de servidor TLS es un cambio de política en todo el sector que mejorará la seguridad y evitará el mal uso. Para la mayoría de los usuarios, no habrá un impacto notable. Sin embargo, si confía en la EKU ClientAuth, debe tomar medidas proactivas para obtener el tipo correcto de certificado para sus necesidades.

Productos afectados

Producto Cisco Secure Firewall	Versión del software	Escenarios afectados	Remediaciones

FTD	Todas las versiones	Cuando actúa como cliente (por ejemplo, al conectarse a proveedores de identidad o servidores de autenticación como ISE (pxGrid), RADIUS, LDAPS o Active Directory), la autenticación basada en certificados puede fallar si el certificado de cliente fue generado por una CA pública y falta la EKU de autenticación de cliente. En esta situación, si el servidor de autenticación rechaza certificados sin la EKU necesaria, pueden producirse errores de conexión.	Opción 1. Si está utilizando un certificado de servidor TLS para la autenticación de cliente, necesitará obtener un certificado con la EKU ClientAuth de otra fuente. O Opción 2. Cambie a CA raíz pública (autoridades de certificación) que proporcionen certificados EKU combinados (ClientAuth y ServerAuth). NOTE: Consulte la sección Soluciones temporales de este documento para ver opciones adicionales.
FDM	Todas las versiones		
FMC	Todas las versiones		
ASA	Todas las versiones		
Cisco Secure Client (anteriormente AnyConnect)	Todas las versiones	Cisco Secure Client puede autenticarse en los servidores ASA o FTD mediante certificados. Sin embargo, si el certificado de cliente fue generado por una CA pública y falta la EKU de autenticación de cliente, la conexión VPN de acceso remoto (RAVPN)	

		fallará.	
FTD o ASA	Todas las versiones	Cuando el FTD o el ASA establecen un túnel VPN de sitio a sitio (ya sea a otro FTD, ASA, router de Cisco o un par VPN de terceros) mediante autenticación de certificado (RSA o ECDSA), el túnel VPN fallará si el certificado de identidad generado por una CA pública no tiene el atributo EKU de autenticación de cliente. Esto ocurre porque el par VPN remoto requiere que la EKU de autenticación de cliente esté presente en el certificado de identidad.	

Nota: si está integrando FMC o FDM con ISE a través de pxGrid y los certificados instalados en FMC/FDM carecen del atributo EKU de autenticación de cliente, revise las soluciones alternativas propuestas en este documento y las siguientes referencias a ISE: FN74392 y Prepare Identity Services Engine para las restricciones de uso de clave ampliada en los certificados emitidos por entidades de certificación públicas.

Nota: La eliminación de la EKU clientAuth de los certificados de servidor TLS es un cambio de política en todo el sector que mejorará la seguridad y evitará el mal uso. Para la mayoría de los usuarios, no habrá un impacto notable. Sin embargo, si confía en la EKU ClientAuth, debe tomar medidas proactivas para obtener el tipo correcto de certificado para sus necesidades.

Precaución: Para entornos de producción, se recomienda encarecidamente que los clientes utilicen certificados con los atributos EKU adecuados. Esta práctica garantiza la seguridad, la compatibilidad y el cumplimiento de los estándares y las prácticas recomendadas del sector. Los certificados sin atributos EKU solo deben considerarse

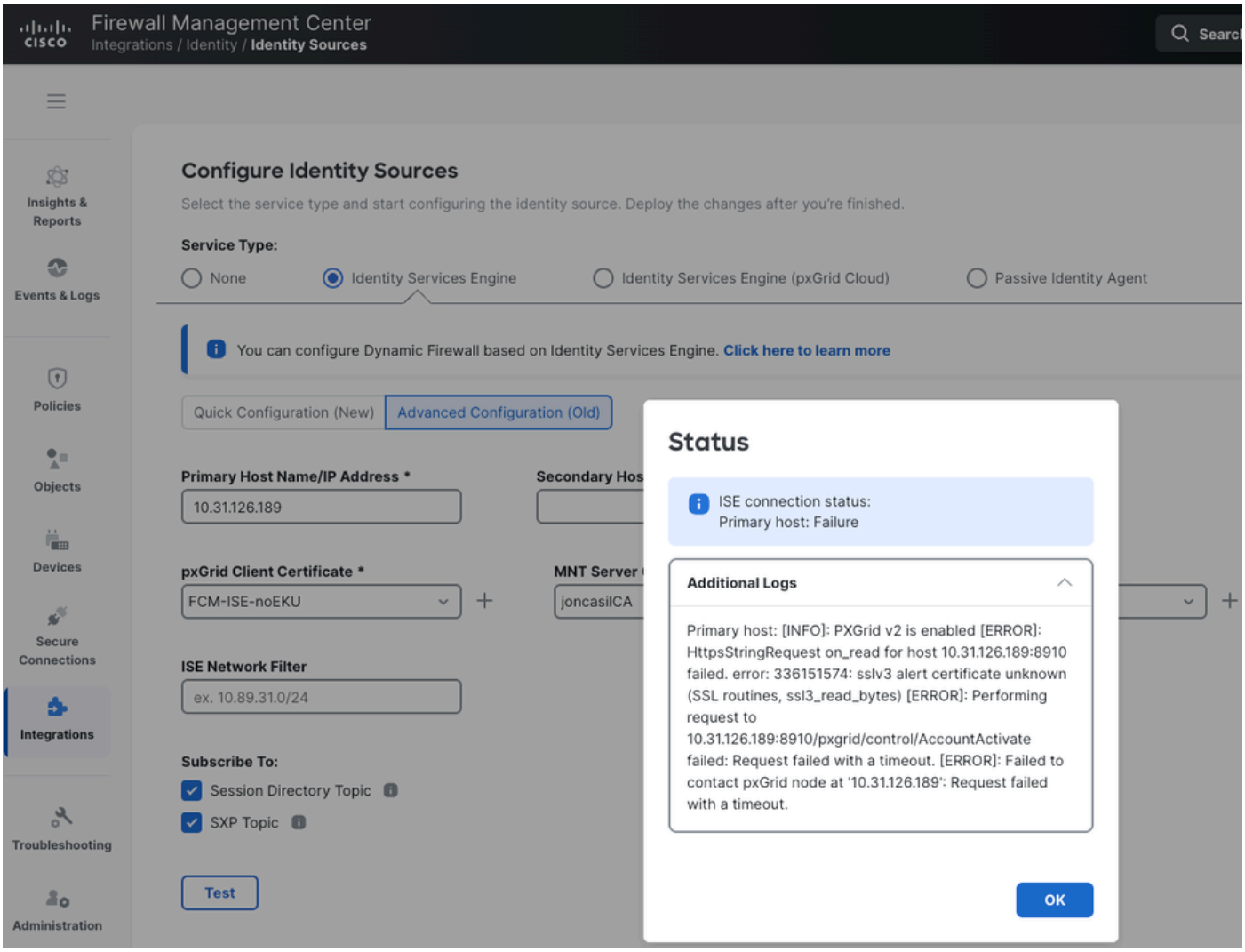
⚠ como una solución temporal y solo con una comprensión clara de los riesgos asociados.

Problema 1. Problema de integración de pxGrid entre FMC e ISE, cuando el certificado FMC carece del atributo EKU de autenticación de cliente

En esta situación, el certificado utilizado por el FMC para la integración de pxGrid con ISE carece del atributo EKU de autenticación de cliente. Como resultado, la integración de pxGrid falla porque el servidor ISE espera que este atributo esté presente en el certificado presentado por el FMC.

Topología

Errores de IU de FMC: Este es el mensaje de error que aparece en el FMC, cuando el certificado utilizado por el FMC carece del atributo EKU de autenticación de cliente para la integración de pxGrid con ISE.



Errores de CLI de FMC: Los mismos mensajes de error se encuentran en el directorio FMC /var/log/messages.

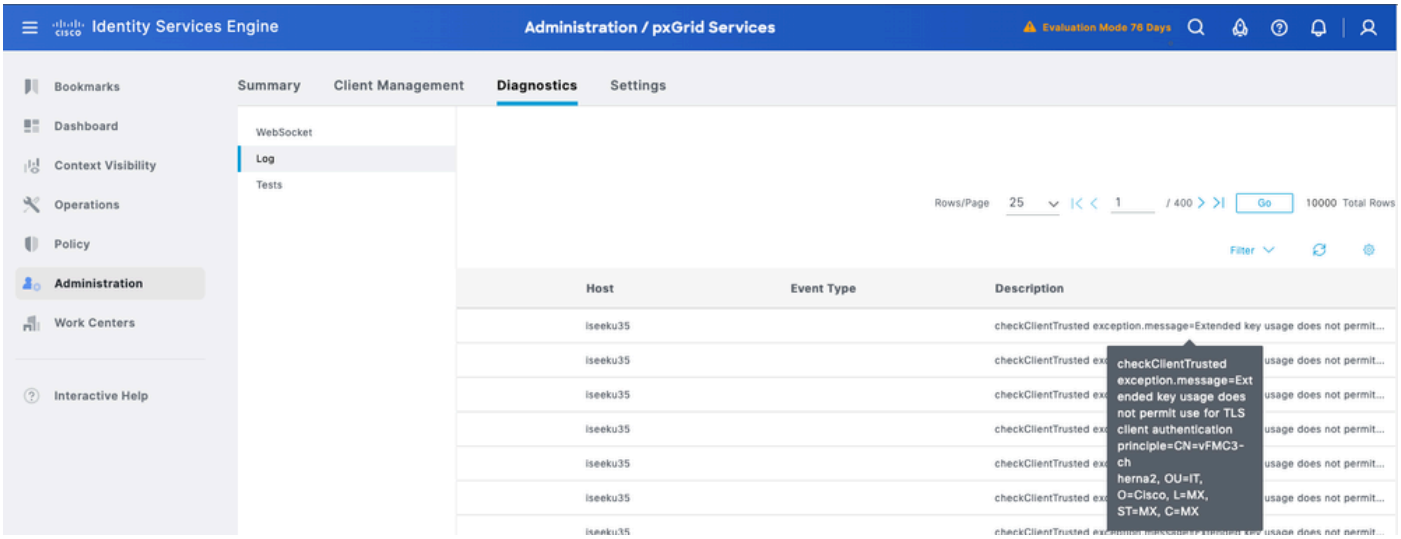
<#root>

```
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
```

Error de ISE: Este es el mensaje de error que se muestra en ISE: "checkClientTrusted exception.message=El uso de clave ampliada no permite el uso para el principio de autenticación de cliente TLS=CN=vFMC3-cadena2, OU=TI, O=Cisco, L=MX, ST=MX, C=MX".



Solución: si está integrando FMC o FDM con ISE a través de pxGrid y el certificado instalado en FMC/FDM carece del atributo EKU de autenticación de cliente, revise la información propuesta en este documento y las siguientes referencias de ISE: FN74392 y Prepare Identity Services Engine para las restricciones de uso de clave ampliada en los certificados emitidos por autoridades de certificación públicas para lograr una integración correcta de pxGrid.

Nota: El certificado de cliente pxGrid de FMC debe incluir el atributo EKU ClientAuth o no contener ningún atributo EKU Client o Server.

Nota: Aunque IMS admite el uso de un certificado firmado por una CA pública. Cisco recomienda utilizar el certificado de CA interna de ISE, ya que esta comunicación es solo para transacciones internas.

Problema 2. Problema de integración de FTD o ASA con un servidor LDAPS, cuando el certificado presentado carece del atributo EKU de autenticación de cliente

En esta situación, el FTD o ASA actúa como cliente para integrarse con un servidor LDAPS mediante la autenticación de

certificados. Si el certificado utilizado por el FTD o ASA carece del atributo EKU de autenticación de cliente, la integración falla porque el servidor LDAPS requiere que este atributo esté presente en el certificado.

Topología

Errores del servidor LDAPS: 'Verificación de certificado TLS: Error, propósito de certificado no admitido' y 'Seguimiento de TLS: SSL3 alert write:fatal:unsupported certificate'

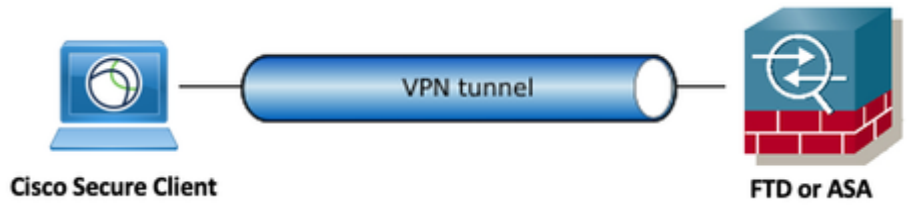
```
69ceb4f5.157b4993 0x7ff553fff700 TLS trace: SSL_accept:TLSv1.3 write server cer
tificate verify
69ceb4f5.157c01a4 0x7ff553fff700 TLS trace: SSL_accept:SSLv3/TLS write finished
69ceb4f5.157c458a 0x7ff553fff700 TLS trace: SSL_accept:TLSv1.3 early data
69ceb4f5.157c6685 0x7ff553fff700 TLS trace: SSL_accept:error 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
```

Solución: Revise los parámetros propuestos en este documento para asegurarse de que el FTD o el ASA utilicen el certificado de identidad correcto (incluido el atributo EKU de autenticación de cliente) para una autenticación correcta basada en certificados con el servidor LDAPS.

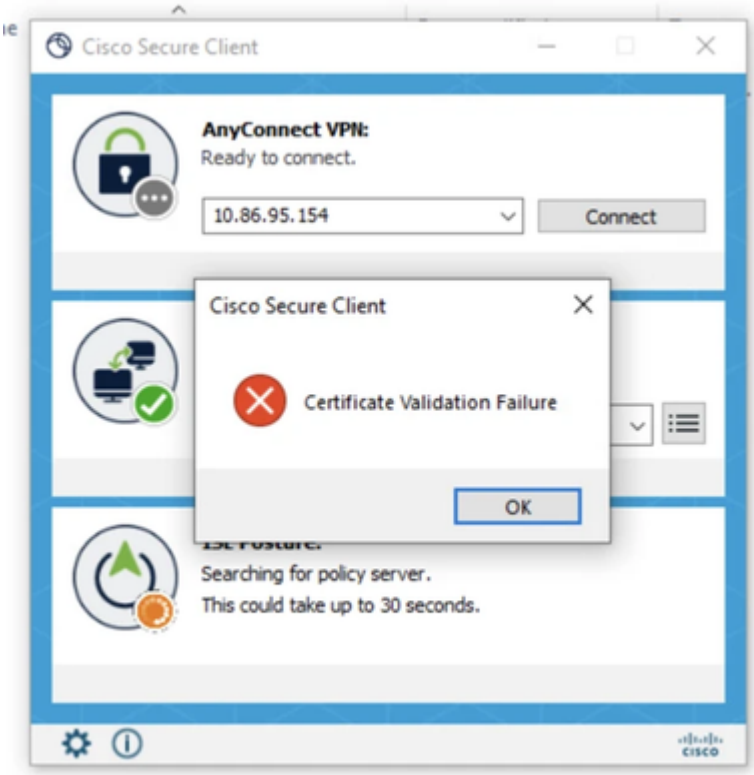
Problema 3. Es posible que Cisco Secure Client (anteriormente AnyConnect) experimente problemas de conexión con un FTD o ASA si el certificado del cliente carece del atributo EKU de autenticación de cliente

En esta situación, Cisco Secure Client utiliza la autenticación de certificados para establecer un túnel RAVPN al FTD o ASA. Sin embargo, si el certificado de cliente carece del atributo EKU de autenticación de cliente, la sesión RAVPN fallará porque el ASA o FTD requiere que este atributo esté presente en el certificado de cliente.

Topología



Error de Cisco Secure Client: 'Error de validación del certificado'



Errores DART de Cisco Secure Client:Los siguientes registros del archivo AnyConnectVPN.txt del paquete DART confirman que Cisco Secure Client rechazó el certificado utilizado para la autenticación basada en certificados RAVPN en el FTD/ASA debido a la ausencia del atributo EKU de autenticación de cliente (para localizar el archivo AnyConnectVPN.txt en el paquete

DART, vaya a Cisco Secure Client > AnyConnect VPN > Registros > 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]

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

Solución: revise la información propuesta en este documento para asegurarse de que Cisco Secure Client utiliza el certificado correcto (incluido el atributo EKU de autenticación de cliente) para una autenticación correcta basada en certificados con el FTD o el ASA.

Nota: Del error de paquete DART anterior 'EKU no encontrado en el certificado: 1.3.6.1.5.5.7.3.2' , este número '1.3.6.1.5.5.7.3.2' corresponde al OID EKU de autenticación de cliente.

Problema 4. Los túneles VPN de sitio a sitio con autenticación basada en certificados fallan si al certificado de identidad le falta el atributo EKU de autenticación de cliente

En esta situación, que implica la autenticación basada en certificados para un túnel VPN de sitio a sitio IKEv2, el certificado de identidad utilizado por FTD/ASA (1) para establecer el túnel al par FTD/ASA (2) carece del atributo EKU de autenticación de cliente. Como resultado, no se puede establecer el túnel VPN porque el par remoto, FTD/ASA (2), requiere que este atributo esté presente en el certificado.

Topología

Errores CLI de FTD o ASA: estos son los errores observados en FTD/ASA (2) durante la autenticación basada en certificados IKEv2 cuando rechaza el certificado de identidad FTD/ASA (1) que carece del atributo EKU de autenticación 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
```

Nota: En el ejemplo anterior, el FTD/ASA (2) estaba utilizando un certificado de identidad que incluía los atributos EKU ClientAuth y ServerAuth.

Nota: En el ejemplo anterior, el FTD/ASA (2) también podría sustituirse por un router o un concentrador VPN físico o basado en la nube de terceros. Entonces, el mismo problema persistirá, ya que el par VPN requiere que el atributo EKU de autenticación de cliente esté presente en el certificado utilizado por el FTD/ASA (1) para una autenticación exitosa basada en certificados.

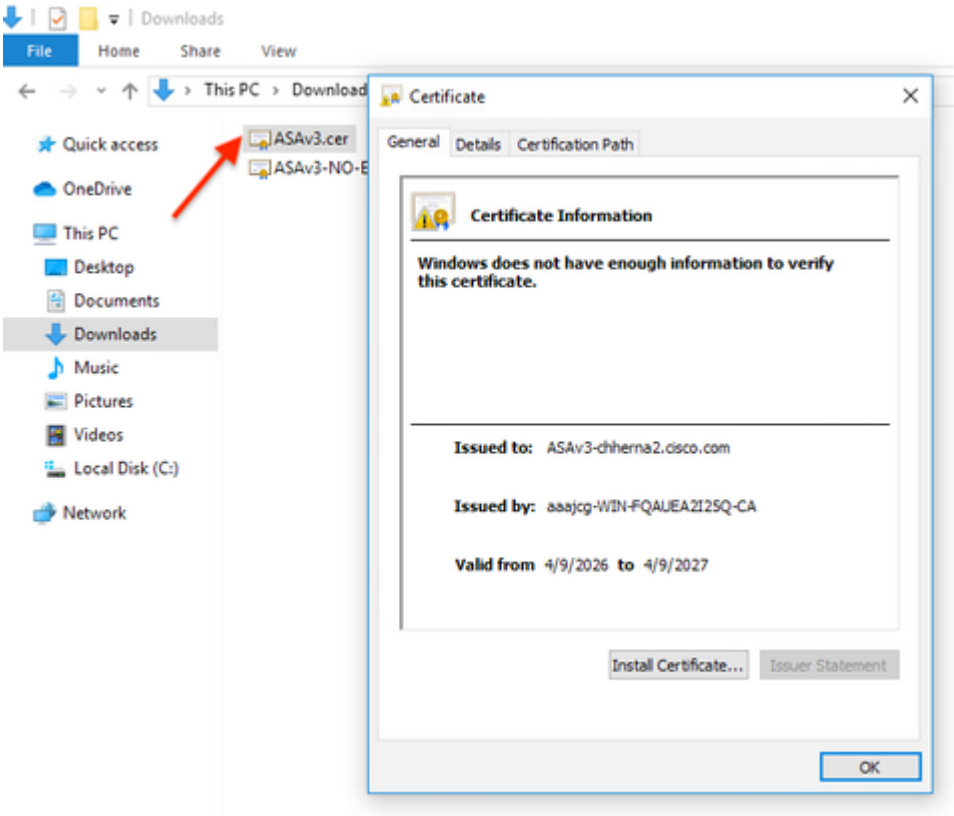
Solución: revise la información propuesta en este documento para asegurarse de que FTD/ASA (1) utiliza el certificado de identidad correcto (incluido el atributo EKU de autenticación de cliente) para un túnel VPN de sitio a sitio correcto con autenticación basada en certificados.

Instrucciones para confirmar si su certificado carece del atributo EKU de autenticación de cliente

Verifique los atributos EKU de un certificado .cer mediante el Administrador de certificados de Windows

Siga los siguientes pasos para verificar los atributos EKU de un certificado .cer mediante el Administrador de certificados de Windows:

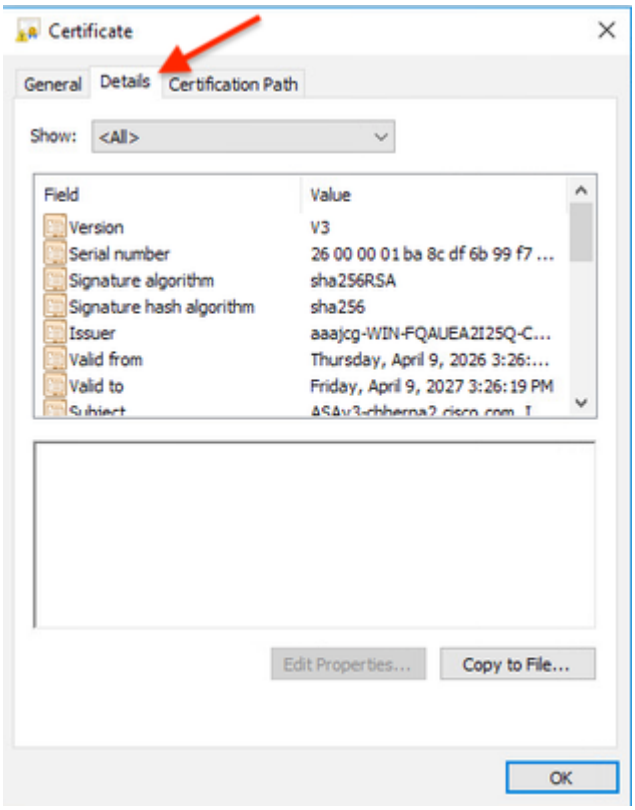
Paso 1. Haga doble clic en el archivo .cer para abrirlo en el Administrador de certificados de Windows.



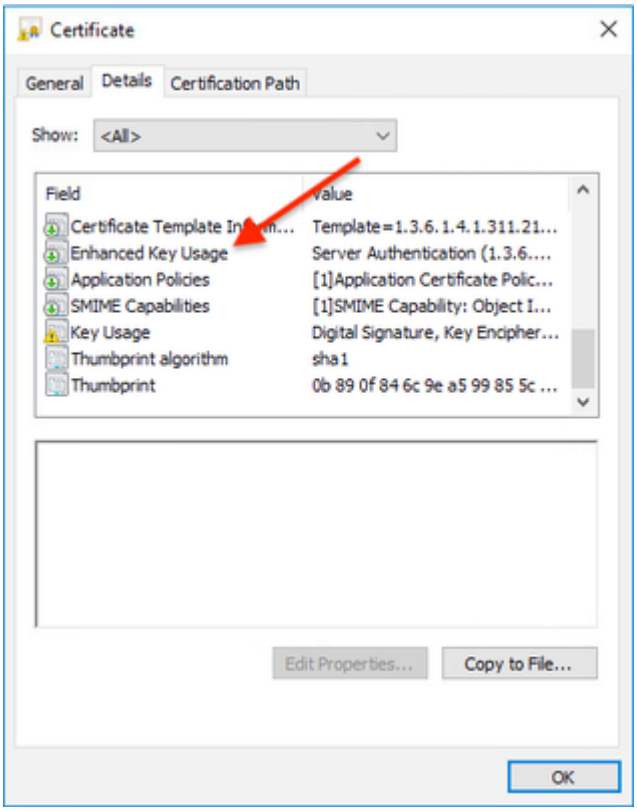
Nota: Sólo los archivos .cer se abrirán directamente de esta manera; si el certificado tiene la extensión .pem, cámbiele el nombre a .cer o a .crt en primer lugar.

Paso 2. Gestionar advertencia de seguridad (si la hay). Si aparece un mensaje de advertencia de seguridad, haga clic en Abrir para continuar.

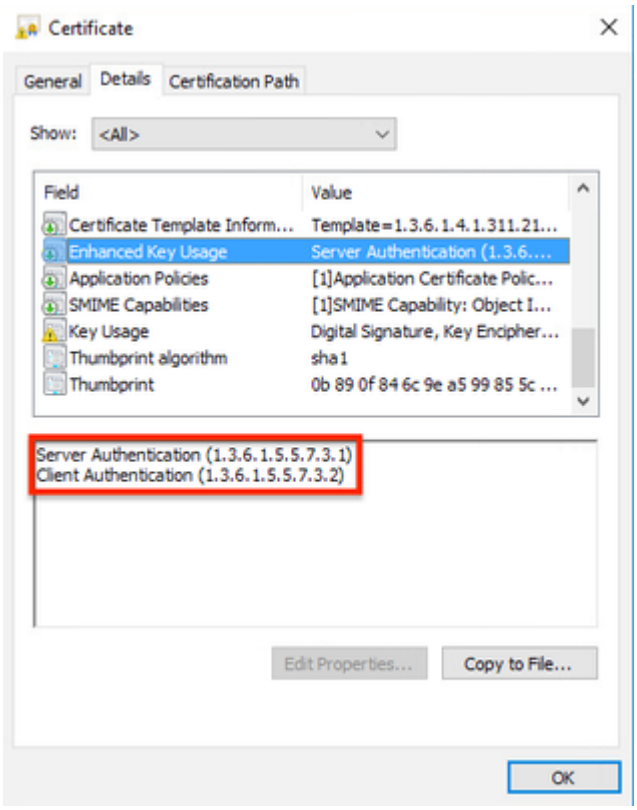
Paso 3. En la ventana de certificado, haga clic en la pestaña Detalles.



Paso 4. Desplácese por la lista de campos y seleccione "Enhanced Key Usage" (Uso mejorado de claves).

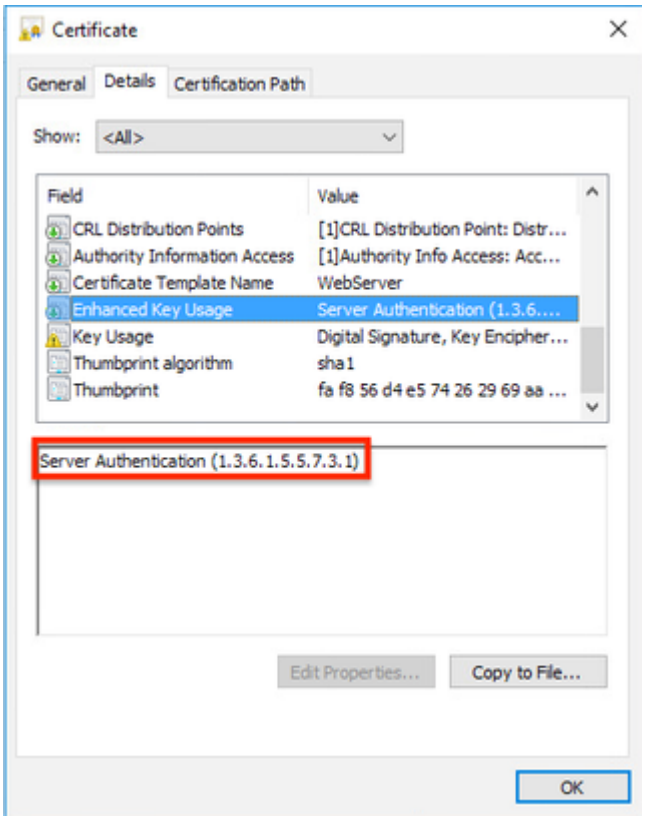


Paso 5. Verifique los Atributos EKU, es posible que vea entradas como "Autenticación del servidor" y "Autenticación del cliente" que indican los valores EKU presentes en el certificado.

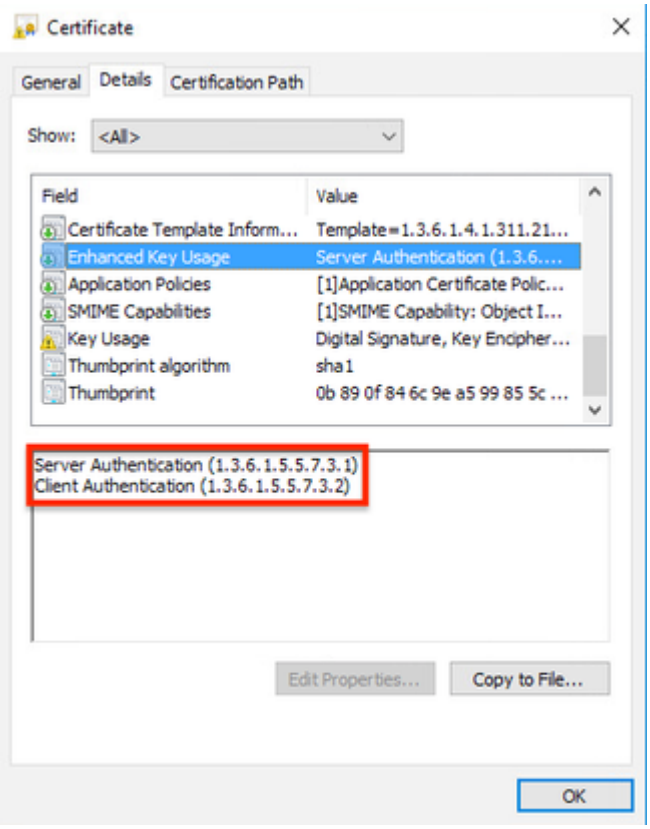


Paso 6. Después de la verificación, haga clic en Aceptar para cerrar la ventana del certificado.

Ejemplo 1: A este certificado .cer le falta el atributo EKU de autenticación de cliente e incluye sólo el atributo EKU de autenticación de servidor.



Ejemplo 2: Este certificado .cer incluye los atributos EKU de autenticación de cliente y servidor.



Verifique los Atributos EKU desde un Certificado PKCS#12, PEM y .cer usando OpenSSL

Siga los siguientes pasos para verificar los atributos EKU desde un certificado .p12 (PKCS#12), .pem (PEM) y .cer:

Paso 1. Localice el certificado que necesita comprobar y expórtelo en formato .p12 (PKCS#12), .pem (PEM) o .cer.

Para los certificados .p12 (PKCS#12), utilice openssl para extraer el certificado del archivo .p12 (PKCS#12); el archivo .p12 (PKCS#12) puede contener la clave privada, el certificado y los certificados de CA.

Utilice el siguiente comando para extraer el certificado de un archivo .p12 (PKCS#12) a un archivo .pem (PEM) (sin la clave privada o la cadena de CA):

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

- suarchivo.p12: Reemplazar por el nombre real del archivo.
- Es posible que tenga que introducir la contraseña del archivo .p12.
- cert.pem: ¿Se extrae el certificado (sin la clave privada o la cadena de CA) en formato .pem (PEM)?

Paso 2. Utilice los siguientes comandos openssl para mostrar los detalles del certificado y los atributos EKU.

a) Para los archivos .pem, utilice el siguiente comando openssl para mostrar los detalles del certificado y los atributos EKU:

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

- cert.pem: Reemplazar por el nombre real del archivo.

b) Para los archivos .cer, utilice el siguiente comando openssl para mostrar los detalles del certificado y los atributos EKU:

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

- suarchivo.cer: Reemplazar por el nombre real del archivo.

Paso 3. Luego, busque la sección X509v3Extended Key Usage en el resultado, es posible que vea entradas como "TLS Web Server Authentication" y "TLS Web Client Authentication" que indican los valores EKU presentes en el certificado.

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

O los OID de atributo EKU (identificadores de objeto):

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

- Autenticación del servidor EKU OID: 1.3.6.1.5.5.7.3.1
- Autenticación de cliente EKU OID: 1.3.6.1.5.5.7.3.2

Ejemplo 1: A este certificado .pem (PEM) le falta el atributo EKU de autenticación de cliente e incluye sólo el atributo EKU de autenticación 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
```

Ejemplo 2: Este certificado .pem (PEM) incluye los atributos EKU de autenticación de cliente y 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
```

Soluciones alternativas

Los administradores pueden elegir una de las siguientes opciones de solución alternativa.

Opción 1. Cambiar a CA raíz pública que proporcionen certificados EKU combinados

Algunas CA raíz públicas, como DigiCert e IdenTrust, emiten certificados con tipos EKU combinados (certificados de servidor y cliente) desde una raíz alternativa, que puede no estar incluida en el almacén raíz de Chrome. Coordine con el proveedor de la CA para comprobar la disponibilidad de dichos certificados y, antes de implementarlos, asegúrese de que tanto el servidor que presenta el certificado como los clientes que lo consumen confían en la CA raíz correspondiente.

Este enfoque alivia la necesidad de actualizar el software del servidor para mitigar la anulación de la autenticación de cliente EKU aplicada por la política del programa raíz de Chrome.

La siguiente tabla, que muestra ejemplos de CA raíz pública y tipos EKU, no es una lista exhaustiva y tiene fines ilustrativos solamente.

Proveedor de CA	Tipo de EKU	CA raíz	Emisión/CA secundaria
IdenTrust	clientAuth + serverAuth	IdenTrust Public Sector Root CA 1	Servidor del sector público IdenTrust CA 1
IdenTrust	clientAuth	IdenTrust Public Sector Root CA 1	TrustID RSA ClientAuth CA 2
IdenTrust	serverAuth (navegador de confianza)	IdenTrust Commercial Root CA 1	Servidor HydrantID CA O1
DigiCert	clientAuth + serverAuth	DigiCert Assured ID Root G2	ID garantizada de DigiCert CA G2
DigiCert	clientAuth	DigiCert Assured ID	Cliente de identificación

Proveedor de CA	Tipo de EKU	CA raíz	Emisión/CA secundaria
		Root G2	garantizada DigiCert CA G2
DigiCert	serverAuth (navegador de confianza)	Raíz global DigiCert G2	DigiCert Global G2 TLS RSA SHA256

Opción 2. Renovar los certificados actuales para ampliar su validez

Los certificados emitidos por entidades emisoras de certificados raíz públicas antes de mayo de 2026 que tengan autenticación EKU de cliente y servidor seguirán aceptándose hasta que expire su plazo. Sin embargo, es mejor renovar los certificados EKU combinados antes de que se produzca la anulación de la directiva.

- La política de CA pública y las fechas de implementación pueden variar según el proveedor.
- Consulte a la CA y planifique la renovación del certificado según corresponda.
- Después del 15 de marzo de 2026, los certificados públicos emitidos por CA solo son válidos durante 200 días.
- Tenga en cuenta que algunas CA públicas han dejado de emitir certificados EKU combinados.

Opción 3. Migrar a PKI privada para emitir certificados EKU (servidor y cliente) combinados

Evaluar la viabilidad de la transición a una infraestructura de clave pública privada (PKI) y, a continuación, configurar una CA privada para emitir certificados únicos con EKU (certificados de servidor y cliente con las EKU necesarias) combinadas.

Antes de emitir o implementar un certificado, asegúrese de que tanto el servidor que presenta el certificado como todos los clientes que lo consumen confían en la CA raíz correspondiente.

Opción 4. Obtener un certificado de confianza pública con solo autenticación de cliente EKU

Algunas CA, como SSL.com, ofrecen certificados de autenticación de cliente dedicados. Estos son independientes de los certificados TLS y normalmente se utilizan para la autenticación empresarial.

⚠ Precaución: Para entornos de producción, se recomienda encarecidamente que los clientes utilicen certificados con los atributos EKU adecuados. Esta práctica garantiza la seguridad, la compatibilidad y el cumplimiento de los

---

⚠ estándares y las prácticas recomendadas del sector. Los certificados sin atributos EKU solo deben considerarse como una solución temporal y solo con una comprensión clara de los riesgos asociados.

Preguntas frecuentes

P1. ¿Tengo que preocuparme por esto si uso una PKI privada?

R: La política aplicada por las CA privadas la determina cada organización. Si su CA privada adopta los mismos criterios de emisión, como eliminar el atributo EKU de autenticación de cliente de los certificados, se aplicarán las directrices proporcionadas en este documento.

P2. ¿Puedo seguir utilizando mis certificados existentes?

R: Sí, se pueden utilizar certificados válidos con EKU combinado hasta el tiempode caducidad.

P3. ¿Qué opciones hay disponibles para integrar mi FMC o FDM con ISE a través de pxGrid si el certificado instalado en el FMC/FDM carece del atributo EKU de autenticación de cliente?

R: Además de las soluciones alternativas propuestas en este documento, le recomendamos que consulte las siguientes referencias de ISE:

- Aviso de problemas FN74392 - Cisco Identity Services Engine: Impacto en las comunicaciones seguras de la autenticación de clientes de CA pública Cambios en EKU a partir de mayo de 2026: solución alternativa proporcionada
- Preparación de Identity Services Engine para las restricciones de uso de claves ampliadas en certificados emitidos por entidades de certificación públicas

✎ Nota: Aunque IMS admite el uso de un certificado firmado por una CA pública. Cisco recomienda utilizar el certificado de CA interna de ISE, ya que esta comunicación es solo para transacciones internas.

P4. ¿Qué es la EKU de "Autenticación del Cliente" y por qué estaba en mi certificado?

R: La EKU "Client Authentication" (Autenticación del cliente) indica que un cliente puede utilizar un certificado para autenticarse en un servidor. Algunas CA lo incluían históricamente en los certificados TLS de forma predeterminada, pero nunca se requería para la seguridad normal del

sitio web.

P5. Mi certificado TLS actual indica "Autenticación de cliente" en Uso de clave ampliada. ¿Ahora no es válido?

R: No, sigue siendo válido. No es necesario que la sustituya de inmediato. Al renovar, el nuevo certificado simplemente no incluirá el clienteAuth EKU.

P6. ¿Cómo puedo verificar si un certificado tiene el clienteAuth EKU?

R: Puede inspeccionar los detalles del certificado mediante herramientas OpenSSL, PowerShell o GUI para comprobar la extensión Extended Key Usage.

P7. ¿Puedo obtener un certificado de confianza pública solo con EKU de autenticación de cliente?

R: Algunas CA, como SSL.com, ofrecen certificados de autenticación de cliente dedicados. Estos son independientes de los certificados TLS y normalmente se utilizan para la autenticación empresarial.

P8. ¿Afecta esto a otros tipos de EKU o certificados (firma de código, correo electrónico, etc.)?

R: No, este cambio es específico de los certificados de servidor TLS. La firma de código y los certificados de correo electrónico tienen sus propios requisitos EKU.

P9. ¿Dónde puedo ver los requisitos oficiales sobre este cambio?

R: La política del programa raíz de Google Chrome proporciona directrices sobre la prohibición de la EKU clientAuth en los certificados de servidor TLS.

P10. ¿Es seguro utilizar certificados sin atributos EKU de cliente y servidor en mi entorno de producción?

R.: En entornos de producción, se recomienda encarecidamente que los clientes utilicen certificados con los atributos EKU adecuados. Esta práctica garantiza la seguridad, la compatibilidad y el cumplimiento de los estándares y las prácticas recomendadas del sector. Los certificados sin atributos EKU solo deben considerarse como una solución temporal y solo con una comprensión clara de los riesgos asociados.

Información Relacionada

- Para obtener asistencia adicional, póngase en contacto con el centro de asistencia técnica Cisco Technical Assistance Center (TAC). Se necesita un contrato de asistencia válido: Contactos de asistencia globales de Cisco.

- Soporte y descargas de Cisco: Soporte técnico y descargas de Cisco

Errores relacionados

- CSCwt9492 ENH: FMC debe validar la presencia del atributo EKU de autenticación de cliente en el certificado de cliente utilizado para la integración de pxGrid

- CSCwt94509 ENH: FMC debe mostrar un mensaje que indique que el atributo EKU de autenticación de cliente es necesario en el certificado de cliente utilizado para la integración de pxGrid

- CSCwt61767 Mayo de 2026 Cambio de EKU solo de servidor - Emita una advertencia de configuración de ASA si EKU inadecuada

- CSCws83036 EKU: Evaluación del impacto de la aplicación de ClientAuth EKU en ISE

Referencias de Cisco ISE

- Aviso de problemas FN74392 - Cisco Identity Services Engine: Impacto en las comunicaciones seguras de la autenticación de clientes de CA pública Cambios en EKU a partir de mayo de 2026: solución alternativa proporcionada

- Preparación de Identity Services Engine para las restricciones de uso de claves ampliadas en certificados emitidos por entidades de certificación públicas

Referencias externas

- Política del programa raíz de Chrome

- Portal de IdenTrust

- SSL: eliminación de la EKU de autenticación de cliente de los certificados de servidor TLS: qué necesita saber

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).