Prepare Identity Services Engine para las restricciones de uso de claves extendidas en certificados emitidos por entidades de certificación públicas.

Contenido

Introducción

Este documento describe el impacto de las restricciones aplicadasa los criterios de expedición de los certificados expedidos porentidades emisoras de certificados que se adaptan al programa Chrome Root Certificate de Cisco Identity Services Engine (ISE).

Antecedentes

Los certificados digitales son credenciales electrónicas emitidas por entidades de certificación (CA) que protegen la comunicación entre servidores y clientes garantizando la autenticación, la integridad de los datos y la confidencialidad.
El campo Uso extendido de claves (EKU) son atributos que definen el propósito de la clave pública del certificado

Dos de los valores EKU disponibles son:

- Autenticación del servidor EKU (id-kp-serverAuth): Se utiliza cuando un servidor presenta su certificado para probar la identidad
- Autenticación de cliente EKU (id-kp-clientAuth): Se utiliza en conexiones TLS mutuas (mTLS) en las que ambas partes se autentican mutuamente

Un único certificado podría contener tanto EKU de autenticación de cliente como de servidor, lo que le permitiría cumplir dos propósitos. Esto es especialmente importante para productos como ISE que actúan como servidor o cliente en función del caso práctico.

Definición del problema

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 del Servidor y la Autenticación del Cliente EKU era una práctica común.

Sin embargo, como parte de la Chrome Root Program Change Public CAs 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 clientes (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 autenticación de servidor EKU.
- La inclusión de la autenticación de cliente EKU 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"
- No más CA raíz de uso mixto para certificados TLS de servidor público
- Plazos de aplicación: Marzo de 2027.

Plazos

- 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

Cómo afecta a Cisco ISE

Productos afectados

Todas las versiones de Cisco ISE se ven afectadas:

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

Nota: El cambio mencionado afecta a todas las versiones de ISE, incluidas las versiones anteriores a 3.x. Sin embargo, los cambios de código sólo se liberan para las versiones mencionadas en la sección anterior. Cisco recomienda actualizar ISE para evitar cualquier impacto.

Casos prácticos afectados específicos

La Tabla 1 resume los servicios afectados por los próximos cambios en la EKU de autenticación de cliente, junto con el impacto esperado para cada servicio.

Servicio	Impacto
pxGrid	El servicio pxGrid de ISE requiere comunicación entre nodos a través del canal pxGrid. Esto significa que algunos nodos funcionarán como servidores y otros como clientes. Por lo tanto, la presencia de la EKU de autenticación de servidor y la EKU de autenticación de cliente son necesarias para la instalación del certificado pxGrid.

	Como resultado, la instalación de los certificados de CA pública recién emitidos que contienen solamente la EKU de autenticación de servidor está restringida. ⚠ Precaución: El servicio pxGrid de ISE realiza la validación de EKU del certificado. Los certificados de cliente pxGrid externos deben incluir la EKU de autenticación de cliente al comunicarse con ISE o se rechaza la conexión. Cisco recomienda la verificación de los certificados públicos firmados por CA utilizados en clientes pxGrid externos para evitar el impacto en la integración.
Servicio de mensajería ISE (IMS)	ISE Messaging Services (IMS) es un canal seguro utilizado para la comunicación entre nodos. Por lo tanto, la presencia de EKU de autenticación de servidor y de EKU de autenticación de cliente es necesaria para la instalación del certificado IMS. Como resultado, se restringe la instalación de los certificados de CA pública recién emitidos que no contienen ambas EKU.
TC-NAC	Al seleccionar el proveedor de TC-NAC Tenable Security Center: VA en Administration > Threat Centric NAC > Add se crea un nuevo conector TC-NAC. Una vez que el conector esté listo para configurarse, es posible seleccionar la "Autenticación basada en certificados" como método de autenticación para el conector TC-NAC y, a continuación, seleccionar el "Certificado de administración de ISE". La conexión TC-NAC se establece entre ISE PSN y VA DB, por lo que el certificado de administración del PSN específico es el que se utiliza como certificado de cliente Si mTLS estricto está habilitado en Tenable, se requiere la autenticación de cliente EKU. La falta de esto causa interrupciones en la conexión TLS.
LDAP, registro del sistema seguro, DTL RADIUS para CoA	Estos tres servicios ofrecen la posibilidad de utilizar certificados específicos como "certificados de cliente" para la autenticación TLS. ISE no realiza ninguna validación de EKU. Por lo tanto, el impacto en estos servicios depende completamente del lado del servidor. si la validación de EKU del certificado se exige en el servidor, el certificado específico utilizado por ISE requiere la EKU de autenticación de cliente o la autenticación TLS falla.

Tabla 1: Servicios afectados

Indicios de problema

Al intentar instalar un certificado con EKU de autenticación de servidor sólo para servicios con requisitos de EKU específicos, se genera el error que se muestra en la imagen 1.

pxGrid e ISE Messaging Service (IMS) son servicios con tales requisitos EKU.

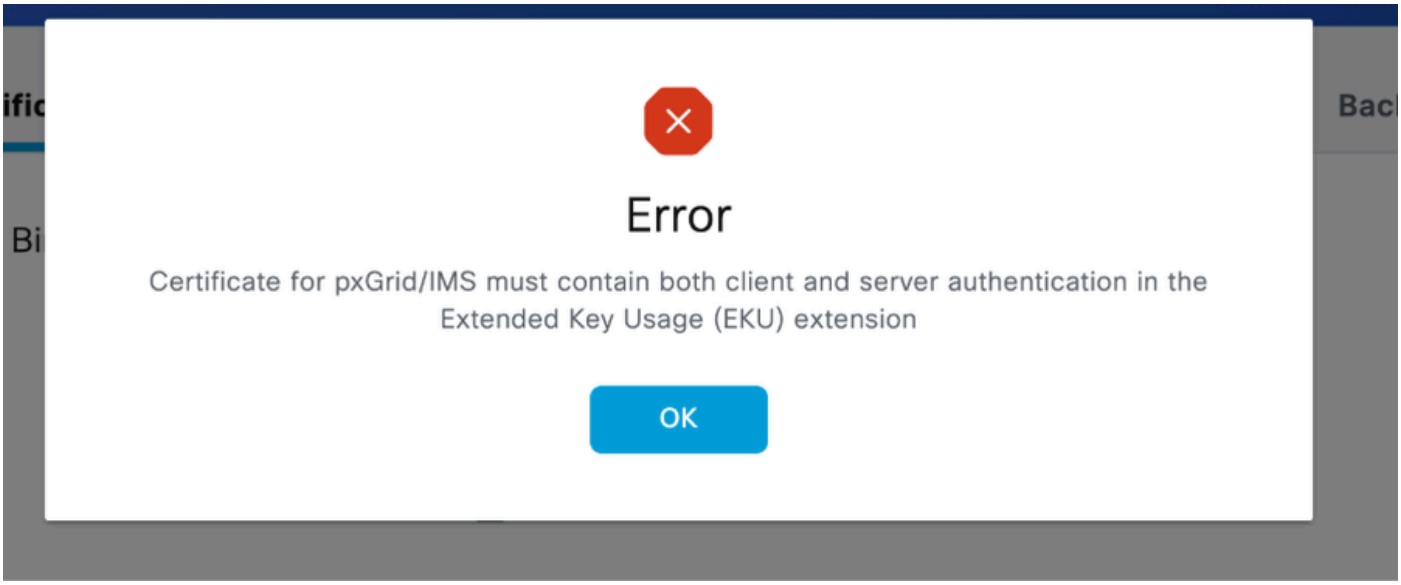

Imagen 1: Error al intentar instalar un certificado que no cumple los requisitos de EKU

Recomendaciones

Audite los certificados con impacto potencial y siga las recomendaciones

- Utilice la tabla 1 para encontrar los servicios de ISE que podrían tener un impacto. Compruebe cuáles de los servicios mencionados dependen de certificados públicos firmados por CA.
- Documentar la cadena de CA para cada certificado y validar si dicha CA está implementando los cambios en los criterios de emisión.
- Comprobar fechas de vencimiento: Planifique las renovaciones estratégicamente antes de la aplicación de políticas. Tenga en cuenta que la autenticación de cliente EKU se puede restringir según la política de la CA.
- Utilice la tabla 2 para obtener recomendaciones específicas para los servicios afectados por el cambio en los criterios de emisión

Servicio	Acciones recomendadas

pxGrid	Si el certificado pxGrid en ISE lo emite una CA pública y se planea una renovación o migración a una CA pública, recomendamos lo siguiente: 1.- Verifique si actualmente tanto Server Authentication EKU como Client Authentication EKU están presentes en el certificado y si es posible mantener ambos dependiendo de su política de CA 2.- Si la política de la CA no permite la presencia de ambas EKU, se recomienda migrar el certificado para que lo firme la CA interna de ISE. Para realizar la migración, vaya a: Administración > Sistema > Certificados > Certificados del sistema > Seleccione el certificado emitido por la CA interna de ISE del nodo específico que desea modificar > Editar > Active la casilla pxGrid en la sección de uso > Haga clic en Guardar. Si no existe un certificado emitido por la CA interna de ISE, deberá generar uno. Utilice el siguiente vídeo como guía para generar el certificado.
Certificado de mensajería ISE (IMS)	Si el certificado del servicio de mensajería de ISE está firmado actualmente por una CA pública y está prevista una renovación o migración a una CA pública, le recomendamos lo siguiente: 1.- Verifique si la CA pública a la que está migrando o que está utilizando para la renovación acepta el uso de las EKU de autenticación de servidor y de cliente. 2.- Si la CA pública no lo permite, migre el certificado de mensajería de ISE para usar la CA interna de ISE. Para ello, vaya a Administration > System > Certificates > Certificate Signing Request > Generate Certificate Signing Request (CSR) > Select "ISE Messaging Service" in the "Certificate(s) will be used for" desplegable > Check the box "Regenerate ISE Messaging Service Certificate > Press the button "Generate ISE Messaging Service Certificate" en la esquina derecha de la pantalla No es necesario reiniciar el servicio. Asegúrese de que todos los nodos ISE estén en funcionamiento y sean accesibles desde la perspectiva PAN en los puertos 12001 y 443, de modo que el cambio de certificado se propague correctamente a todos los nodos.
TC-NAC	El servicio TC-NAC se basa en el certificado de administración de ISE del nodo específico para la autenticación mTLS. Si el certificado lo emite una CA pública y está prevista una renovación o migración a una CA pública, le recomendamos lo siguiente: 1.- Verifique si actualmente tanto Server Authentication EKU como Client

	Authentication EKU están presentes en el certificado y si es posible mantener ambos dependiendo de su política de CA 2.- Verificar si mTLS estricto está habilitado en Tenable. La inhabilitación de mTLS estricto permite el uso de un certificado sólo con EKU de autenticación de servidor.
LDAP, registro del sistema seguro, DTL RADIUS para CoA	ISE no realiza la validación EKU para los certificados de cliente de estos servicios. Si se planea una renovación o una migración a una CA pública, se recomienda validar si el certificado EKU se cambiará después de la renovación o migración y si esto entra en conflicto con la política TLS en el lado del servidor.

Tabla 2: Acciones recomendadas para evitar el impacto en los servicios específicos.

Soluciones temporales (antes de junio de 2026)

Los administradores pueden elegir una de estas opciones de solución alternativa:

Opción 1: Cambiar a CA raíz pública que proporcionan certificados EKU combinados

Algunas CA raíz públicas (como DigiCert e IdenTrust) emiten certificados con EKU combinada desde una raíz alternativa, que no se puede incluir en el almacén de confianza del explorador de Chrome.

Ejemplos de CA de raíz pública y tipos de EKU:

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
DigiCert	clientAuth + serverAuth	DigiCert Assured ID Root G2	ID garantizada de DigiCert CA G2

Prerrequisitos de este enfoque:

- Coordine con su proveedor de CA para comprobar la disponibilidad de dichos certificados.
- Antes de implementar certificados, asegúrese de que tanto el servidor que presenta el certificado como todos los clientes que lo consumen confían en la CA raíz

correspondiente.
- Si la cadena de la CA no está preinstalada, instale la cadena de la CA donde sea necesario.
- Este enfoque evita la necesidad inmediata de actualizaciones de software.

Referencias de administración de certificados:

- Guía del administrador de Cisco Identity Services Engine, versión 3.3
- Configuración de renovaciones de certificados en ISE

Opción 2: Renueve los certificados actuales para ampliar su validez

Los certificados emitidos por las CA raíz públicas antes de mayo de 2026 que tienen EKU de autenticación de cliente y de servidor continúan cumpliéndose hasta que caduque su plazo.

Estrategia de renovación

Pautas generales:

- Renueve los certificados EKU combinados antes de que se produzca la anulación de políticas
- Después del 15 de marzo de 2026, los certificados emitidos por CA pública solo son válidos durante 200 días.
- La política de CA pública y las fechas de implementación pueden variar.
- Algunas CA públicas han dejado de emitir certificados EKU combinados.

Opción 3: Evaluar y migrar a proveedores de CA alternativos

Pautas generales:

- Migrar a una CA alternativa que permita la presencia de EKU de autenticación de cliente y servidor
- Proporciona control a largo plazo sobre las políticas de certificados
- Al emitir un certificado firmado por una CA privada, debe compartir la información del certificado raíz con el par.
- 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 cadena de CA correspondiente

Solución a largo plazo (actualización de software necesaria)

Los clientes pueden actualizar ISE a una versión de revisión que introduzca una gestión de certificados actualizada para admitir certificados emitidos bajo las nuevas políticas de CA.

Las próximas versiones de parches incluyen cambios de comportamiento para alinear ISE con las nuevas restricciones. La fecha de lanzamiento prevista es abril de 2026:

Versión de Cisco ISE	Versión del parche
ISE 3.1	Parche 11
ISE 3.2	Parche 10
ISE 3.3	Parche 11
ISE 3.4	Parche 6
ISE 3.5	Parche 3

Comportamiento después de la instalación del parche

⚠ Precaución: Este parche introduce cambios de comportamiento en la lógica de administración de certificados. Realice una copia de seguridad del certificado pxGrid de ISE y del certificado IMS antes de instalar el parche. Un posible escenario de interrupción es la instalación del parche, la instalación de los certificados sólo con EKU de autenticación de servidor y la reversión del parche. En esta situación, el sistema ignora los certificados que afectan a las funciones específicas.

Certificado PxGrid

Después de instalar la versión de revisión:

- La importación de certificados pxGrid que contienen solamente EKU de autenticación de servidor, tanto EKU de autenticación de servidor como de cliente, o ninguna extensión EKU está permitida.
- Los certificados que contienen solamente EKU de autenticación de cliente se rechazan.

Certificado del servicio de mensajería ISE (IMS)

ISE 3.1, 3.2 y 3.3

No se ha introducido ningún cambio de comportamiento después de instalar el parche. El servicio de mensajería de ISE requiere un certificado con EKU de cliente y servidor. Los clientes deben planificar la migración a un certificado firmado por una CA interna de ISE una vez que caduque el certificado actual.

ISE 3.4 y 3.5

Después de la instalación de la revisión, se permite el uso de un certificado firmado por una CA pública que contiene EKU de autenticación de servidor solamente.

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.

Preguntas frecuentes

Preguntas generales

A: ¿Tengo que preocuparme por esto si uso una PKI privada?

R.: La política aplicada por las CA privadas la define cada organización. Si su CA privada sigue los mismos criterios de emisión, se pueden utilizar las directrices de este documento.

A: ¿Puedo seguir utilizando mis certificados existentes?

R: Sí, los certificados existentes con EKU combinado siguen siendo válidos hasta que caducan. El problema surge cuando necesita renovar. Funcionan para las conexiones TLS y mTLS hasta que caducan.

A: ¿Cómo puedo saber si estoy utilizando mTLS o TLS estándar?

R: Sección Revisar Casos Prácticos Afectados Específicos.

Recursos adicionales

- Id. de error de Cisco CSCws83036- Evaluación del impacto de la aplicación ClientAuth EKU en ISE

Referencias externas

- Política del programa raíz de Chrome

Recursos de autoridad certificadora

- Portal de IdenTrust

Conclusión

La anulación de la autenticación de cliente EKU en los certificados de CA públicos representa un cambio significativo en la política de seguridad que afecta a las implementaciones de Cisco ISE que utilizan conexiones mTLS. Aunque se trata de un cambio que afecta a todo el sector, el índice

de impacto es CRÍTICO y se requiere una acción inmediata para evitar interrupciones en el servicio.

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).