Preparación de Expressway para la extinción de EKU de autenticación de cliente en certificados de CA pública

Contenido

Introducción

Este documento describe los cambios de la política del programa root de Chrome en Cisco Expressway y la extinción de EKU de autenticación de cliente en los certificados de CA públicos después del 26/6.

Información de backgroup

Los certificados digitales son credenciales electrónicas emitidas por entidades emisoras de certificados (CA) de confianza que protegen la comunicación entre servidores y clientes garantizando la autenticación, la integridad de los datos y la confidencialidad. Estos certificados contienen campos de uso extendido de claves (EKU) que definen su propósito:

- 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

Tradicionalmente, un único certificado podía contener tanto EKU de autenticación de cliente como de servidor, lo que le permitía cumplir dos propósitos. Esto es especialmente importante para productos como Cisco Expressway que actúan como servidor y cliente en diferentes escenarios de conexión.

Definición del problema

Cambio de la política del programa raíz de Chrome

A partir de junio de 2026, la política del programa raíz de Chrome restringe los certificados de la autoridad certificadora (CA) raíz incluidos en el almacén raíz de Chrome, eliminando gradualmente las raíces multifunción para alinear todas las jerarquías de la infraestructura de clave pública (PKI) para servir solo casos de uso de autenticación de servidor TLS.

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 para mantener la confianza del navegador Google Chrome
- 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

- No más CA raíz de uso mixto para certificados TLS de servidor público
- Plazos de aplicación: Junio de 2026

Plazos de respuesta de CA pública

- Octubre de 2025: Muchas CA públicas (DigiCert, Sectigo, SSL) comenzaron a emitir certificados solo de servidor de forma predeterminada
- 11 de febrero de 2026: Let's Encrypt deja de emitir certificados con autenticación de cliente EKU mediante el perfil ACME clásico
- Mayo de 2026: Los servidores de CA pública dejan de emitir certificaciones EKU de autenticación de cliente
- Junio de 2026: La política del programa de raíz de Chrome se vuelve totalmente efectiva

---

Nota: Esta directiva sólo se aplica a los certificados emitidos por CA públicas. Esta directiva no afecta a la PKI privada ni a los certificados autofirmados.

Documentación de Cisco relacionada

- ID de falla de funcionamiento de Cisco: CSCwr73373: compatibilidad con certificado de cliente y servidor independiente para Expressway
- Aviso de problemas FN74362
- Chrome Root Program Policy: Chrome Root Program Policy Documentación

Cómo afecta a la solución Expressway

Productos afectados

Según el aviso de campo FN74362, todas las versiones de Cisco Expressway se ven afectadas:

Producto	Versiones afectadas	Impacto
Núcleo y extremo de Expressway	X14 (todas las versiones)	X14.0.0 a X14.3.7 - Todas las versiones afectadas
Núcleo y extremo de Expressway	X15 (versiones anteriores a X15.4)	X15.0.0 a X15.3.2 - Todas las versiones afectadas

Doble función de Expressway

Los productos de Cisco Expressway (Expressway-C y Expressway-E) actúan como servidor y

cliente en varios escenarios de conexión, lo que requiere certificados con EKU de autenticación de cliente y servidor.

Expressway E como servidor (se requiere autenticación de servidor EKU):

- Acceso al navegador HTTPS
- Conexiones transversales de UC SIP
- Conectividad Webex Edge Audio/MRA

Expressway E como cliente (se requiere autenticación de cliente EKU):

- Comunicaciones B2B
- Conexiones MRA (acceso móvil y remoto)
- Federación XMPP
- Conexiones CMS/zona de vecino SIP
- Interacciones con entidades externas
- Conexión a la nube de Cisco (incorporación de MRA)

Casos prácticos afectados específicos

El certificado público firmado por CA con autenticación de cliente EKU que se usa actualmente para conexiones mTLS en Cisco Expressway es el certificado de servidor de Expressway. Este certificado se utiliza para estas conexiones mTLS:

1. Llamada B2B SIP sobre mTLS: Expressway E se convierte en cliente o servidor en una conexión mTLS, según el sitio iniciado por la sesión
2. SIP IMP Federation over mTLS: Expressway E se convierte en cliente o servidor en una conexión mTLS, según el sitio iniciado por la sesión
3. Zona transversal de UC: Expressway C presenta EKU de autenticación de cliente
4. Zona transversal con configuración mTLS: Expressway C presenta EKU de autenticación de cliente
5. Zona de vecino SIP con configuración mTLS: Expressway se convierte en cliente o servidor en una conexión mTLS, en función del sitio iniciado por la sesión, incluidas las conexiones con:

- Cisco Unified Communications Manager (Unified CM)
- Cisco Unity
- Cisco Unified Border Element (CUBE)
- Cisco Meeting Server (CMS)
- Conexión a la nube de Cisco: incorporación de MRA (Expressway inicia la conexión a la nube de Cisco y presenta la autenticación de cliente EKU)

Recomendaciones

Auditar certificados actuales (PRIMER PASO OBLIGATORIO)

Según el aviso práctico FN74362, antes de considerar soluciones alternativas y opciones de

solución:

- Prepare un inventario de todos los certificados TLS públicos para identificar qué certificados contienen la EKU de autenticación de cliente
- Realice una copia de seguridad de la instancia de Cisco Expressway o copie manualmente el certificado firmado y la clave privada
- Uso de certificados de documento: identifique qué certificados se utilizan para las conexiones mTLS
- Verifique la información de CA y raíz: Documentar qué CA y raíz emitieron cada certificado
- Comprobar fechas de vencimiento: Planificar las renovaciones estratégicamente antes de la aplicación de políticas

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 raíz pública y tipos de EKU (según FN74362):

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.
- Intercambie información del certificado raíz con pares de comunicación.
- Este enfoque evita la necesidad inmediata de actualizaciones de software.

Referencias de administración de certificados:

- Guía de creación y uso de certificados de Cisco Expressway (X14.0)
- Guía de creación y uso de certificados de Cisco Expressway (X15.0)

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

Las recomendaciones generales son:

- Renueve los certificados EKU combinados antes de que se produzca la anulación de políticas
- Para obtener la validez máxima de los certificados, deberá renovarlos antes del 15 de marzo de 2026.
- Después de esta fecha, los certificados emitidos por la CA pública sólo son válidos durante 200 días.
- Cisco recomienda encarecidamente que renueve sus certificados antes de esta fecha si desea continuar con esta opción.
- La política de CA pública y las fechas de implementación pueden variar.
- Algunas CA públicas han dejado de emitir certificados EKU combinados y no pueden proporcionar uno de forma predeterminada.
- Para generar un certificado con una EKU combinada, trabaje con su autoridad de CA y utilice un perfil especial proporcionado por las CA públicas.

Consideraciones especiales para cifrar certificados

Según FN74362, si utiliza certificados de Let's Encrypt:

- Actualmente, Expressway utiliza un perfil ACME clásico que está codificado y no puede ser modificado por los usuarios
- Este perfil ACME clásico se utiliza actualmente para solicitar certificados que incluyen EKU de autenticación de cliente y servidor
- A partir del 11 de febrero de 2026, las solicitudes de certificado que utilizan este perfil ya no incluyen la EKU de autenticación de cliente en los certificados generados por Let's Encrypt
- Para obtener más información, vea Cómo finalizar el soporte del certificado de autenticación de cliente TLS en 2026 - Cifrémoslo

Elementos de acción para cifrar usuarios

- Renueve los certificados antes del 11 de febrero de 2026, lo ideal sería que se

aproximara lo más posible a esta fecha para maximizar el período de validez de 90 días.
- Desactive el programador automático ACME para evitar que los certificados se renueven automáticamente después del 11 de febrero de 2026.
- Esta acción ayuda a evitar que los certificados se sobrescriban inadvertidamente con versiones que sólo contienen la EKU de autenticación de servidor.
- Si no realiza la renovación antes del 11 de febrero de 2026, póngase en contacto con el TAC de Cisco para obtener asistencia.

Opción 3: Evaluar y migrar a proveedores de CA alternativos

Esta opción solo se aplica a Expressway C; NO se aplica a Expressway E.

Enfoque de PKI privada

- Evaluar la viabilidad de la transición a la ICP privada
- Configure una CA privada para emitir certificados únicos con EKU combinados (certificados de servidor y cliente con las EKU necesarias)
- 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 CA raíz correspondiente.
- Las CA privadas no están sujetas a la política del programa root de Chrome
- Proporciona control a largo plazo sobre las políticas de certificados

---

⚠ Precaución: Esta opción no es viable para Expressway-E, que requiere certificados de CA públicos para servicios externos y confianza del explorador.

Solución a largo plazo (actualizaciones de software necesarias)

Según el aviso de campo FN74362, Cisco está implementando mejoras de productos en versiones fijas para abordar este problema de forma exhaustiva.

Programación de lanzamiento fijo:

Producto	Versión afectada	Versión fija	Propósito de la corrección	Disponibilidad
Cisco Expressway	X14.x (todas las versiones) X15.x	X15.4	Solución intermitente: Permite la carga adicional del certificado	Febrero de 2026

	(anterior a X15.4)		firmado solo EKU de ServerAuth en Expressway E y el ajuste de verificación de certificado para la señal MRA SIP entre Expressway E y Expressway C	
Cisco Expressway	X14.x (todas las versiones) X15.x (anterior a X15.5)	X15.5	Solución completa: Proporciona mejoras en la interfaz de usuario para separar los certificados de cliente y servidor, y proporciona opciones a los administradores para deshabilitar la comprobación de EKU	Mayo de 2026

Nota: Tanto Cisco Expressway E como Expressway C deben actualizarse a la misma versión.

Detalles de la solución Cisco Expressway X15.4 (febrero de 2026)

Propósito: solución intermitente para acomodar los certificados con ServerAuth EKU solamente y para habilitar los registros MRA

Las principales mejoras son:

- Elimina la restricción de cargas de certificados
- Permite a los administradores cargar certificados solo con EKU de autenticación de servidor a través de la GUI web en Expressway E
- Anteriormente, Expressway rechazaba los certificados de solo servidor
- Ajusta la verificación de certificados para MRA
- Modifica la verificación de certificados para la señalización SIP entre Expressway-E y Expressway-C en soluciones MRA
- Permite aceptar certificados solo de servidor de aplicaciones de terceros

Quién puede actualizar a X15.4:

- si implementa o vuelve a implementar Expressway-E existente para MRA con certificados firmados solo de servidor.
- Si utiliza certificados ACME (Let's Encrypt) después del 11 de febrero de 2026.
- Implementaciones existentes que necesitan actualizar certificados firmados que sólo contienen EKU de autenticación de servidor.
- si tiene problemas de autenticación relacionados con certificados en conexiones mTLS

Requisitos importantes para X15.4:

- Tanto Expressway-E como Expressway-C deben actualizarse a X15.4
- Planificar la actualización durante el período de mantenimiento para minimizar las interrupciones del servicio

Las limitaciones de X15.4 son:

- Se trata de una solución intermitente que soluciona problemas de compatibilidad inmediatos
- No proporciona compatibilidad completa con doble certificado
- No incluye el parámetro de servicio para deshabilitar la comprobación EKU
- Las conexiones mTLS pueden fallar en función del sitio iniciado por la sesión

Detalles de la solución Cisco Expressway X15.5 (mayo de 2026)

Objetivo: Solución integral para cumplir con los requisitos globales del programa raíz de Google Chrome

Mejoras clave del producto:

- Segregación de certificados de cliente y servidor
- Habilita la compatibilidad con dos certificados independientes en la misma interfaz
- Certificados de Expressway con EKU de autenticación de servidor y EKU de autenticación de cliente diferentes
- Facilita las conexiones mTLS adecuadas con funciones de certificado separadas
- Mejoras de IU y backend
- Nuevas interfaces de administración de certificados para la administración individual de ambos certificados
- Validación de EKU de autenticación de cliente durante la carga del certificado para evitar caídas accidentales de la conexión MTLS
- Los administradores pueden cargar y administrar certificados de servidor y de cliente por separado
- Opciones para Inhabilitar la Verificación EKU de Autenticación de Cliente
- Parámetro de servicio que permite a los administradores desactivar la verificación EKU de autenticación de cliente según los requisitos individuales de la empresa
- Permite que Cisco Expressway ignore EKU del par remoto (cliente) que solicita una conexión solo con certificados EKU de autenticación de servidor
- En ausencia de un certificado EKU de autenticación de cliente, permite a Expressway (re)utilizar el certificado EKU de autenticación de servidor solo como certificado de cliente

---

Nota: En este caso, el peer remoto también tiene que soportar un modelo similar de EKU de Ignorar Autenticación de Cliente

---

Árbol de decisiones

INICIO: ¿Utiliza certificados de CA pública en Expressway?

│

├─ NO: PKI privada o autofirmado

│ └─ No se requiere ninguna acción - No se ve afectado por la política

│

└─ SÍ: Certificados de CA pública en uso

  │

  ├─ ¿Se utilizan para conexiones mTLS? (Consulte los casos prácticos en la sección Casos prácticos afectados específicos).

  │ │

  │ ├─ NO: Solo autenticación de servidor

  │ │ └─ Impacto mínimo: supervisión de cambios futuros

  │ │

  │ └─ SÍ: conexiones mTLS con EKU de autenticación de cliente

  │ │

  │ └─ Elija SU enfoque:

  │ │

  │ ├─ Opción A: Cambiar a CA raíz alternativa

  │ │ ├─ Póngase en contacto con el proveedor de la CA para obtener una EKU combinada de raíz alternativa

  │ │ ├─ Asegúrese de que todos los pares confíen en la nueva raíz

  │ │ └─ No se necesita una actualización de software inmediata

  │ │

  │ ├─ Opción B: Renovación de certificados antes de los plazos

  │ │ ├─ Si vamos a cifrar: Renovar antes del 11 de febrero de 2026

  │ │ │ └─ Deshabilitar el programador ACME después de la renovación

│ │ ├─ Para una validez máxima: Renovar antes del 15 de marzo de 2026

│ │ └─ Compra tiempo hasta la expiración del certificado

│ │

│ ├─ Opción C: Migrar a PKI privada (sólo Expressway-C)

│ │ ├─ Configuración de una infraestructura de CA privada

│ │ ├─ Emitir certificados EKU combinados

│ │ ├─ Distribuir la raíz a todos los pares

│ │ └─ Control a largo plazo, NOT para Expressway-E

│ │

│ └─ Opción D: Planificación de actualizaciones de software

│ ├─ ¿Necesidad urgente? → Actualización a X15.4 (febrero de 2026)

│ └─ Solución integral → Actualización a X15.5 (mayo de 2026)

│ └─ A continuación, obtenga certificados de servidor/cliente independientes

Preguntas frecuentes

Preguntas generales

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

R: No. Esta directiva sólo afecta a los certificados emitidos por las CA raíz públicas. La PKI privada y los certificados autofirmados no se ven afectados.

A: ¿Qué sucede si no utilizo conexiones mTLS?

R: Si sólo utiliza TLS estándar (autenticación de servidor), esta política no le afecta. Sus certificados sólo de servidor siguen funcionando. Sin embargo, verifique sus casos de uso comparándolos con la lista de la sección Casos de Uso Afectados Específicos, ya que algunos de los casos de uso utilizan mTLS de forma predeterminada.

A: ¿Dejarán de funcionar mis conexiones web HTTPS estándar a Expressway?

R: No. Las conexiones TLS estándar no se ven afectadas. El acceso del explorador web a Expressway sigue funcionando normalmente incluso con certificados EKU sólo de servidor.

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.

P. ¿Qué puedo hacer ahora mismo?

R.: Cisco recomienda encarecidamente las siguientes acciones inmediatas:

- Auditar los certificados

  Identificar certificados TLS públicos utilizados para mTLS

- Renovar los certificados antes

  Realice la renovación antes del 15 de marzo de 2026 para maximizar la validez

- Control de la automatización ACME

  Deshabilitar las renovaciones automatizadas que pueden reemplazar certificados inesperadamente

- Coordine con su CA

  Algunas CA ofrecen perfiles de certificado temporales o alternativos

A: ¿Es CUCM SU3(a) compatible con X15.4 y X15.5?

R: Yes

A: ¿Existe una vulnerabilidad de seguridad al deshabilitar la comprobación EKU del cliente en Cisco Expressway E (con la versión X15.5)?

R: El certificado sigue comprobando CN/SAN para verificar que el origen de la conexión es válido, solo omite la validación EKU (certificado para el propósito de la función de cliente) que se incluyó de forma predeterminada hasta que Google plantea problemas de seguridad, por lo tanto, no debe tener problemas de seguridad en comparación con antes.

Cifremos los datos específicos

A: Utilizo Let's Encrypt with ACME en Expressway. ¿Qué puedo hacer?

R:

1. Renueve su certificado antes del 11 de febrero de 2026 (lo más cerca posible de esa fecha)
2. Inhabilite el programador automático ACME inmediatamente después de la renovación
3. Planificar la actualización a X15.5 para una solución a largo plazo

A: ¿Puedo modificar el perfil ACME para seguir obteniendo certificados EKU combinados?

R: No. Actualmente, Expressway utiliza un perfil ACME "clásico" codificado de forma rígida que los usuarios no pueden modificar. Póngase en contacto con el TAC de Cisco para obtener asistencia para el perfil de certificado ACME.

Preguntas de actualización

A: ¿Necesito actualizar Expressway-E y Expressway-C?

R: Sí, absolutamente. Ambos deben actualizarse a la misma versión (X15.4 o X15.5) para que funcionen correctamente.

A: ¿puedo actualizar a X15.4 o esperar a X15.5?

R:

- Actualice a X15.4 si tiene problemas urgentes o necesita aceptar certificados solo de servidor ahora
- Si es posible, espere a X15.5 (mayo de 2026) para obtener la solución completa compatible con doble certificado

P: La replicación del clúster se interrumpe después de la renovación del certificado. ¿Qué ha pasado?

R: Lo más probable es que su nuevo certificado solo tenga EKU de autenticación de servidor, pero:

- Si no hay una versión anterior a X15.4 con TLS Verify = Forzando: Los pares del clúster no pueden establecer conexiones mTLS sin EKU de autenticación de cliente
- Opciones de solución (cualquiera de ellas):

  Establecer el modo de verificación de TLS en "Permisivo" (menos seguro)

  Obtener certificados con EKU combinado de raíz de CA alternativa

  Actualice a X15.4 o posterior, que omite la verificación de EKU de autenticación de cliente para ClusterDB

A: Después de actualizar a X15.4, ¿puedo utilizar el modo de aplicación con los certificados solo de servidor en mi clúster?

R: Sí. A partir de X15.4, Expressway omite la verificación EKU de autenticación de cliente para las conexiones mTLS ClusterDB. Por lo tanto, la verificación de TLS se puede establecer en "Forzosa" incluso si uno o más nodos del clúster sólo tienen EKU de autenticación de servidor.

A: ¿Por qué no puedo cargar mi certificado a través de la GUI web de Expressway?

R: Antes de X15.4, la GUI web aplica una validación codificada que requiere que los certificados tengan EKU de autenticación de cliente. Si su certificado sólo tiene EKU de autenticación de

servidor, tiene dos opciones:

- Utilice SCP (protocolo de copia segura) para cargar el certificado directamente en el servidor (carpeta /persistent/Certs)
- Actualice a X15.4 o posterior (solo Expressway-E), lo que elimina esta restricción

A: Después de actualizar a X15.4, sigo sin poder cargar certificados solo de servidor en Expressway-E

R: Una vez actualizado, asegúrese de que este comando esté habilitado

Certificado XCP TLS de xConfiguration CVS EnableServerEkuUpload: Encendido

A: Actualicé a X15.4. ¿Puedo cargar certificados solo de servidor en Expressway-E y Expressway-C?

R: No. X15.4 solo elimina la restricción de carga para Expressway-E. Expressway-C aún requiere certificados EKU combinados para la carga a través de la GUI web. Esto se debe a que Expressway-C suele actuar como cliente TLS en las zonas transversales de UC y requiere autenticación de cliente EKU. Asegúrese de ejecutar este comando en Expressway-E. Este comando no se ejecuta en Expressway-C

Certificado XCP TLS de xConfiguration CVS EnableServerEkuUpload: Encendido

A: No puedo registrar Smart License después de la renovación del certificado. ¿Por qué?

R: La falla de Smart Licensing luego de la renovación del certificado generalmente NO está relacionada con EKU:

- Compruebe si Expressway puede comunicarse con tools.cisco.com (CSSM)
- Verifique que las reglas del firewall permitan HTTPS salientes (puerto 443)
- Comprobar si la configuración del proxy es correcta (si se utiliza el proxy HTTP)
- Compruebe que el certificado de servidor CSSM es de confianza en el almacén de confianza de Expressway
- Smart Licensing no requiere clientAuth, por lo que este cambio de directiva no le afecta

Específicos de MRA (acceso móvil y remoto)

A: ¿Requiere MRA autenticación de cliente EKU en Expressway-E?

R: Depende de la versión de Expressway:

- Antes de X15.4: Sí, requerido indirectamente

  Durante la señalización SIP de MRA, Expressway-E envía su certificado firmado en un mensaje SIP SERVICE a Expressway-C

  Expressway-C valida el certificado, lo que requiere autenticación de cliente y autenticación de servidor EKU

Sin EKU combinado, el registro de MRA SIP falla

- X15.4 y posterior: No

  Expressway-C ya no valida la autenticación de cliente EKU en el mensaje SIP SERVICE

  Expressway-E solo necesita EKU de autenticación de servidor para MRA

  La zona transversal de UC funciona unidireccionalmente (Expressway-C valida únicamente el certificado de servidor de Expressway-E)

A: Por qué fallan mis zonas vecinas después de cargar elEKU de autenticación de servidor en Expresssswayx15.4

R: Si establece el modo de verificación de TLS en "on", es necesario tener una EKU de autenticación de cliente. De esta manera, puede inhabilitar la verificación de TLS en la configuración de la zona vecina

A: ¿Qué certificados son necesarios para que MRA funcione correctamente?

R: Para una implementación de MRA típica:

Componente	Requisitos del certificado	Se requiere EKU	Notas
Expressway-E (antes de X15.4)	serverAuth + clientAuth	Ambas	Para la validación del SERVICIO SIP por parte de Exp-C
Expressway-E (X15.4+)	serverAuth solamente	Solo servidor	Comprobación de EKU del cliente omitida
Expressway-C	clientAuth + serverAuth	Ambas	Siempre actúa como cliente en UC Traversal
Zona transversal de UC	Validación unidireccional	Exp-E: serverAuth Exp-C: clientAuth	Exp-C valida el certificado del servidor Exp-E

A: Mi MRA funcionaba bien, pero después de renovar mi certificado de Expressway-E con EKU solo de servidor, el registro de SIP falla. ¿Qué ocurre?

R: Si está ejecutando una versión anterior a X15.4, la señalización MRA SIP requiere que Expressway-E presente las EKU de autenticación de cliente y servidor en el mensaje SIP

SERVICE. Sus opciones:

- Obtener un certificado con EKU combinado
- Cambiar a una raíz de CA alternativa que emita EKU combinado
- Actualizar Expressway-E y Expressway-C a X15.4 o posterior (recomendado)

Administración de certificados

A: ¿Cómo obtengo un certificado con EKU combinado de DigiCert o IdenTrust?

R: Póngase en contacto con su proveedor de CA y solicite un certificado de su raíz alternativa que aún emita EKU combinado.

A: Mi CA indica que solo puede proporcionar certificados de solo servidor. ¿Qué puedo hacer?

R: Dispone de varias opciones:

- Buscar raíces alternativas: Pregunte a su CA si tiene raíces alternativas que emiten EKU combinado (como DigiCert Assured ID o IdenTrust Public Sector)
- Proveedores de CA de switch: Busque CA que ofrezcan EKU combinadas de raíces no confiables en Chrome
- Utilizar PKI privada: Configurar CA interna para certificados EKU combinados (solo implementaciones de Expressway-C)
- Actualización a X15.4: Solución intermitente para alojar certificados con ServerAuth EKU solamente y para habilitar los registros MRA
- Actualizar a X15.5 una vez disponible: Plan para la arquitectura de doble certificado donde los certificados solo de servidor son aceptables y solución integral para cumplir con los requisitos globales del programa raíz de Google Chrome

Preguntas de cronología

A: ¿Qué pasará el 15 de junio de 2026?

R: Chrome deja de confiar en los certificados TLS públicos que contienen las EKU de autenticación de cliente y servidor. Los servicios que utilizan estos certificados pueden fallar.

A: ¿Por qué tengo que renovar antes del 15 de marzo de 2026?

R: Después del 15 de marzo de 2026, la validez del certificado se reduce de 398 a 200 días. La renovación antes de esta fecha le proporciona la duración máxima del certificado.

P.: ¿Cuál es el plazo límite para actuar?

R: Existen varios plazos:

- 11 de febrero de 2026: Encriptemos las paradas combinadas de EKU a través del ACME clásico
- 15 de marzo de 2026: Validez del certificado reducida a 200 días
- Mayo de 2026: La mayoría de las CA públicas dejan de emitir EKU combinado por

completo
- Junio de 2026: Política de Chrome totalmente aplicada

Recursos adicionales

Documentación de Cisco

- Aviso práctico FN74362: Impacto de Cisco Expressway en la comunicación segura debido a los próximos cambios en los certificados TLS
- ID de bug de Cisco CSCwr73373: Compatibilidad con servidor y certificado de cliente independientes para Expressway

Referencias externas

- Política del programa raíz de Chrome
- Vamos a cifrar: Finalización del soporte del certificado de autenticación de cliente TLS en 2026
- Requisitos básicos del foro de CA/navegador

Recursos de autoridad certificadora

- Portal de soporte de DigiCert
- Servicios de certificados de IdenTrust
- Cifremos el foro de la comunidad
- Base de conocimientos de Sectigo

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 Expressway que utilizan conexiones mTLS. Aunque se trata de un cambio que afecta a todo el sector, la clasificación de impacto es CRÍTICA según el aviso FN74362, por lo que se requiere una acción inmediata para evitar interrupciones en el servicio.

Puntos clave

- Esto afecta a TODAS las versiones de Expressway (X14 y X15 antes de X15.4)
- Audite sus certificados AHORA: este es el primer paso obligatorio
- Hay disponibles varias soluciones alternativas: elija la que mejor se adapte a su entorno
- Se requieren actualizaciones de software para la solución a largo plazo: planificación para X15.5
- Tanto Expressway-E como Expressway-C se deben actualizar juntos

- Cifremos a los usuarios para que tengan la fecha límite más temprana: el 11 de febrero de 2026

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).