Prepara Expressway per il sunset EKU di autenticazione client nei certificati CA pubblici

Sommario

Introduzione

Questo documento descrive le modifiche dei criteri del programma radice Chrome su Cisco Expressway e autenticazione client EKU tramonto nei certificati CA pubblici dopo 6/26.

Informazioni sul backgroup

I certificati digitali sono credenziali elettroniche rilasciate da Autorità di certificazione (CA) attendibili che proteggono la comunicazione tra server e client garantendo l'autenticazione, l'integrità dei dati e la riservatezza. Questi certificati contengono campi di utilizzo chiavi esteso (EKU, Extended Key Usage) che ne definiscono lo scopo:

- EKU autenticazione server (id-kp-serverAuth): Utilizzato quando un server presenta il proprio certificato per dimostrare l'identità
- EKU autenticazione client (id-kp-clientAuth): Utilizzato nelle connessioni Mutual TLS (mTLS) in cui entrambe le parti si autenticano a vicenda

In genere, un singolo certificato può contenere sia gli EKU di autenticazione server che quelli di autenticazione client, consentendone il doppio utilizzo. Ciò è particolarmente importante per prodotti come Cisco Expressway che agiscono sia come server che come client in diversi scenari di connessione.

Descrizione del problema

Modifica criteri programma radice riquadro

A partire da giugno 2026, i criteri del programma radice Chrome limitano i certificati CA (Certification Authority) radice inclusi nell'archivio radice Chrome, eliminando gradualmente le radici multiuso per allineare tutte le gerarchie di infrastrutture a chiave pubblica (PKI) per servire solo i casi di utilizzo dell'autenticazione del server TLS.

Requisiti principali dei criteri

- Le CA radice pubbliche devono dichiarare l'utilizzo chiavi avanzato (EKU) SOLO per l'autenticazione del server (id-kp-serverAuth)
- I certificati devono includere SOLO l'utilizzo chiavi avanzato per l'autenticazione del server per mantenere l'attendibilità dal browser Google Chrome
- Non è consentito includere l'utilizzo chiavi avanzato di autenticazione client in questi certificati
- Le CA radice che continuano a rilasciare certificati con l'utilizzo chiavi avanzato di autenticazione client vengono infine rimosse dall'archivio radice Chrome
- Non sono più disponibili CA radice per uso misto per certificati TLS server pubblici
- Sequenza temporale applicazione: Giugno 2026

Sequenza temporale risposta CA pubblica

- Ottobre 2025: Molte CA pubbliche (DigiCert, Sectigo, SSL) hanno iniziato a rilasciare certificati solo server per impostazione predefinita
- 11 febbraio 2026: Encrypt interrompe il rilascio di certificati con l'utilizzo chiavi avanzato di autenticazione client utilizzando il classico profilo ACME
- Maggio 2026: I server CA pubblici non rilasciano più certificazioni EKU di autenticazione client
- Giugno 2026: Chrome Root Program Policy diventa pienamente efficace

---

Nota: Questo criterio si applica solo ai certificati rilasciati da CA pubbliche. Questo criterio non influisce sulla PKI privata e sui certificati autofirmati.

Documentazione correlata di Cisco

- ID bug Cisco: CSCwr73373 - Supporto per certificati server e client separati per Expressway
- Field Notice: FN74362
- Criterio programma radice Chrome: Documentazione sui criteri del programma radice Chrome

Impatto della soluzione Expressway

Prodotti interessati

In base alla notifica sul campo FN74362, sono interessate tutte le versioni di Cisco Expressway:

Prodotto	Versioni interessate	Conseguenze
Expressway Core e Edge	X14 (tutte le versioni)	Da X14.0.0 a X14.3.7 - Tutte le versioni interessate
Expressway Core e Edge	X15 (versioni precedenti a X15.4)	Da X15.0.0 a X15.3.2 - Tutte le versioni interessate

Doppio ruolo di Expressway

I prodotti Cisco Expressway (Expressway-C ed Expressway-E) funzionano sia come server che come client in vari scenari di connessione, richiedendo certificati sia con EKU di autenticazione server che client.

Expressway E come server (richiesto EKU di autenticazione server):

- Accesso al browser HTTPS
- Connessioni trasversali UC SIP
- Connettività Webex Edge Audio/MRA

Expressway E come client (è richiesto l'utilizzo chiavi avanzato per autenticazione client):

- Comunicazioni B2B
- Connessioni MRA (Mobile and Remote Access)
- Federazione XMPP
- SIP: Connessioni Adiacenti Zona/CMS
- Interazioni con entità esterne
- Connessione a Cisco Cloud (caricamento MRA)

Casi di utilizzo specifici interessati

Il certificato pubblico firmato dalla CA con utilizzo chiavi avanzato di autenticazione client attualmente utilizzato per le connessioni mTLS in Cisco Expressway è il certificato server Expressway. Questo certificato viene utilizzato per le seguenti connessioni mTLS:

1. Chiamata SIP B2B su mTLS - Expressway E diventa client o server su connessione mTLS, a seconda del sito avviato dalla sessione
2. SIP IMP Federation over mTLS - Expressway E diventa client o server sulla connessione mTLS, a seconda del sito avviato dalla sessione
3. Zona trasversale UC - Expressway C presenta l'utilizzo chiavi avanzato di autenticazione client
4. Area trasversale con configurazione mTLS - Expressway C presenta l'utilizzo chiavi di autenticazione client
5. SIP Neighbor Zone con configurazione mTLS - Expressway diventa client o server sulla connessione mTLS, a seconda del sito avviato dalla sessione, incluse le connessioni con:

- Cisco Unified Communications Manager (Unified CM)
- Cisco Unity
- Cisco Unified Border Element (CUBE)
- Cisco Meeting Server (CMS)
- Connessione a Cisco Cloud - Caricamento MRA (Expressway avvia la connessione a Cisco Cloud e presenta l'utilizzo chiavi avanzato per l'autenticazione client)

Consigli

Controlla certificati correnti (PRIMO PASSAGGIO OBBLIGATORIO)

Avviso FN74362 per campo, prima di prendere in considerazione soluzioni alternative e opzioni:

- Preparare un inventario di tutti i certificati TLS pubblici per identificare quali certificati contengono l'utilizzo chiavi avanzato (EKU) di autenticazione client

- Eseguire un backup dell'istanza di Cisco Expressway o copiare manualmente il certificato firmato e la chiave privata
- Utilizzo certificato documento: identifica i certificati utilizzati per le connessioni mTLS
- Verificare le informazioni relative alla CA e alla radice: Documentare la CA e la radice che hanno rilasciato ciascun certificato
- Controlla date di scadenza: Pianificare i rinnovi in modo strategico prima di applicare le policy

Soluzioni a breve termine (prima di giugno 2026)

Gli amministratori possono scegliere una delle seguenti opzioni di soluzione:

Opzione 1: Passa alle CA radice pubbliche che forniscono certificati EKU combinati

Alcune CA radice pubbliche (ad esempio DigiCert e IdenTrust) emettono certificati con EKU combinato da una radice alternativa, che non può essere inclusa nell'archivio di certificati del browser Chrome.

Esempi di CA radice pubbliche e tipi di EKU (per FN74362):

Fornitore CA	Tipo EKU	CA radice	Emittente/CA secondaria
AffidabilitàIden	autenticazione client + autenticazione server	CA radice settore pubblico IdenTrust 1	Server pubblico IdenTrust CA 1
DigiCert	autenticazione client + autenticazione server	DigiCert Assured ID Root G2	DigiCert Assured ID CA G2

Prerequisiti per questo approccio:

- Coordinarsi con il proprio provider CA per verificare la disponibilità di tali certificati.
- Prima di distribuire i certificati, verificare che il server che presenta il certificato e tutti i client che lo utilizzano considerino attendibile la CA radice corrispondente.
- Scambiare le informazioni sul certificato radice con i peer di comunicazione.
- Questo approccio evita la necessità immediata di aggiornamenti del software.

Riferimenti gestione certificati:

- Guida alla creazione e all'utilizzo dei certificati Cisco Expressway (X14.0)
- Guida alla creazione e all'utilizzo dei certificati Cisco Expressway (X15.0)

Opzione 2: Rinnova i certificati correnti per estenderne la validità

I certificati rilasciati dalle CA radice pubbliche prima di maggio 2026 che dispongono di EKU di autenticazione server e client continuano a essere rispettati fino alla scadenza.

Strategia di rinnovo

Le raccomandazioni generali sono le seguenti:

- Rinnova i certificati EKU combinati prima che venga annullata l'impostazione dei criteri
- Per la validità massima dei certificati, pianificare il rinnovo dei certificati prima del 15 marzo 2026.
- Dopo questa data, i certificati rilasciati dalla CA pubblica saranno validi solo per 200 giorni.
- Cisco consiglia di rinnovare i certificati prima di questa data se si desidera continuare con questa opzione.
- Le politiche pubbliche in materia di CA e le date di implementazione possono variare.
- Alcune CA pubbliche hanno interrotto il rilascio di certificati EKU combinati e non possono fornirne uno per impostazione predefinita.
- Per generare un certificato con un EKU combinato, collaborare con l'autorità CA e utilizzare un profilo speciale fornito dalle CA pubbliche.

Considerazioni speciali su Let's Encrypt Certificates

In base a FN74362, se si utilizzano i certificati Let's Encrypt:

- Attualmente, Expressway utilizza un profilo ACME classico hardcoded che non può essere modificato dagli utenti
- Questo profilo ACME classico viene attualmente utilizzato per richiedere certificati che includono sia EKU di autenticazione server che EKU di autenticazione client
- A partire dall'11 febbraio 2026, le richieste di certificati che utilizzano questo profilo non includono più l'utilizzo chiavi avanzato di autenticazione client nei certificati generati da Crittografia
- Per ulteriori informazioni, vedere Terminare il supporto del certificato di autenticazione client TLS nel 2026 - Crittografare

Azioni per la crittografia degli utenti

- Rinnovare i certificati prima dell'11 febbraio 2026, possibilmente in prossimità di questa data per massimizzare il periodo di validità di 90 giorni.
- Disabilitare l'utilità di pianificazione automatica ACME per impedire il rinnovo automatico dei certificati dopo l'11 febbraio 2026.
- Questa azione consente di evitare che i certificati vengano inavvertitamente sovrascritti con versioni che contengono solo l'utilizzo chiavi avanzato di autenticazione server.
- Se non si esegue il rinnovo prima dell'11 febbraio 2026, contattare Cisco TAC per assistenza.

Opzione 3: Valutazione e migrazione a provider CA alternativi

Questa opzione è applicabile a: Solo Expressway C; NON applicabile a Expressway E.

Approccio PKI privato

- Valutare la fattibilità della transizione alla PKI privata
- Configurare una CA privata per il rilascio di certificati singoli con EKU combinati (certificati server e client con gli EKU richiesti)
- Quando si emette un certificato firmato da un'autorità di certificazione privata, è necessario condividere le informazioni sul certificato radice con il peer.
- Prima di emettere o distribuire un certificato, verificare che sia il server che presenta il certificato che tutti i client che lo utilizzano considerino attendibile la CA radice corrispondente.
- Le CA private non sono soggette ai criteri del programma radice Chrome
- Controllo a lungo termine dei criteri dei certificati

⚠ Attenzione: Questa opzione non è disponibile per Expressway-E, che richiede certificati CA pubblici per i servizi esterni e l'attendibilità del browser.

Soluzione a lungo termine (sono necessari aggiornamenti software)

In base alla notifica sul campo FN74362, Cisco sta implementando miglioramenti del prodotto nelle versioni fisse per risolvere completamente questo problema.

Pianificazione rilascio fisso:

Prodotto	Versione interessata	Versione fissa	Scopo della correzione	Disponibilità
Cisco Expressway	X14.x (tutte le release) X15.x (prima di X15.4)	X15,4	Soluzione intermittente: Consente il caricamento aggiuntivo di un certificato firmato solo dall'EKU di ServerAuth su Expressway E e la regolazione della verifica del certificato per il segnale SIP MRA tra Expressway E ed Expressway C	Febbraio 2026
Cisco Expressway	X14.x (tutte le release) X15.x (prima di X15.5)	X15.5	Soluzione completa: Miglioramento dell'interfaccia utente per la separazione dei certificati client e server e possibilità per gli	Maggio 2026

			amministratori di disattivare la verifica EKU	

Nota: È necessario aggiornare Cisco Expressway E ed Expressway C alla stessa versione.

Dettagli sulla soluzione Cisco Expressway X15.4 (febbraio 2026)

Scopo: soluzione intermittente per gestire i certificati solo con EKU ServerAuth e abilitare le registrazioni MRA

Miglioramenti principali:

- Rimuove le restrizioni al caricamento dei certificati
- Consente agli amministratori di caricare certificati con solo l'utilizzo chiavi avanzato di autenticazione server tramite GUI Web in Expressway E
- In precedenza, Expressway aveva rifiutato certificati solo server
- Regola la verifica del certificato per l'Autorità registrazione integrità
- Modifica la verifica dei certificati per la segnalazione SIP tra Expressway-E ed Expressway-C nelle soluzioni MRA
- Consente l'accettazione di certificati solo server da applicazioni di terze parti

Utenti autorizzati all'aggiornamento a X15.4:

- se si distribuisce un nuovo Expressway-E per Autorità registrazione integrità o se si ridistribuisce un Expressway-E esistente con certificati firmati solo dal server.
- Se si utilizzano certificati ACME (Let's Encrypt) dopo l'11 febbraio 2026.
- Distribuzioni esistenti che richiedono l'aggiornamento di certificati firmati contenenti solo l'utilizzo chiavi avanzato per l'autenticazione del server.
- problemi di autenticazione relativi ai certificati nelle connessioni mTLS

Requisiti importanti per X15.4:

- Sia Expressway-E che Expressway-C devono essere aggiornati a X15.4
- Pianificare l'aggiornamento durante la finestra di manutenzione per ridurre al minimo le interruzioni del servizio

Le limitazioni di X15.4 sono:

- Si tratta di una soluzione intermittente che risolve problemi di compatibilità immediata
- Non fornisce il supporto completo per certificati doppi
- Non include il parametro del servizio per disabilitare la verifica EKU
- Le connessioni mTLS possono non riuscire a seconda del sito avviato dalla sessione

Dettagli sulla soluzione Cisco Expressway X15.5 (maggio 2026)

Scopo: Soluzione completa per soddisfare i requisiti globali del programma Google Chrome Root

Principali miglioramenti del prodotto:

- Separazione dei certificati client e server
- Abilita il supporto per due certificati distinti sulla stessa interfaccia
- Certificati Expressway con EKU di autenticazione server e EKU di autenticazione client distinti
- Facilita le connessioni mTLS appropriate con ruoli certificati separati
- Miglioramenti UI e back-end
- Nuove interfacce di gestione dei certificati per la gestione individuale di entrambi i certificati
- Convalida dell'utilizzo chiavi avanzato di autenticazione client durante il caricamento del certificato per evitare interruzioni accidentali della connessione MTLS
- Gli amministratori possono caricare e gestire certificati server e client separatamente
- Opzioni per disabilitare il controllo dell'utilizzo chiavi avanzato di autenticazione client
- Parametro del servizio che consente agli amministratori di disabilitare il controllo dell'utilizzo chiavi per l'autenticazione client in base ai singoli requisiti aziendali
- Consente a Cisco Expressway di ignorare l'utilizzo chiavi avanzato (EKU) dal peer remoto (client) che richiede una connessione solo con certificati EKU di autenticazione server
- In assenza di un certificato EKU di autenticazione client, consente a Expressway di (ri)utilizzare il certificato solo EKU di autenticazione server come certificato client

---

Nota: In questo caso, anche il peer remoto deve supportare un modello simile di utilizzo chiavi avanzato Ignora autenticazione client

---

Albero delle decisioni

INIZIO: Si utilizzano certificati CA pubblici in Expressway?

Azure

├: PKI privata o autofirmato

│ └ Nessuna azione richiesta - Non influenzata dai criteri

Azure

└ SÌ: Certificati CA pubblici in uso

Azure

├: vengono utilizzati per le connessioni mTLS? (sezione Controllo casi di utilizzo nella sezione

Casi di utilizzo specifici interessati)

INSTALLAZIONE

\ ├- NO: Solo autenticazione server

│ ™ · Impatto minimo - Monitoraggio delle modifiche future

INSTALLAZIONE

└ - YES: connessioni mTLS con EKU autenticazione client

INSTALLAZIONE

¨ - Scegliere il proprio approccio:

INSTALLAZIONE

\ ├· Opzione A: Passa a CA radice alternativa

□ ├. Contattare il provider CA per l'EKU combinato dalla radice alternativa

\ ├- Verificare che tutti i peer siano attendibili

│ ™ Non è necessario alcun aggiornamento software immediato

INSTALLAZIONE

\ ├· Opzione B: Rinnova certificati prima delle scadenze

\ ├· Per crittografare: Rinnovo prima dell'11 febbraio 2026

Monitoraggio attività globale di Azure - Disabilita l'utilità di pianificazione ACME dopo il rinnovo

¨ ├ ™ Per la massima validità: Rinnovo prima del 15 mar 2026

│ ™]· Acquista il tempo fino alla scadenza del certificato

INSTALLAZIONE

\ ├· Opzione C: Esegui migrazione a PKI privata (solo Expressway-C)

¨ ├- Impostare l'infrastruttura della CA privata

\ ├· Rilasciare certificati EKU combinati

\ ├- Distribuire la radice a tutti i peer

│ ™] Controllo a lungo termine, NOT per Expressway-E

INSTALLAZIONE

└ - Opzione D: Pianificazione dell'aggiornamento software

\ ├- Necessità urgente? → Aggiornamento a X15.4 (Feb 2026)

¨~Soluzione completa → Aggiornamento a X15.5 (maggio 2026)

│ └ Ottenere quindi certificati server/client separati

Domande frequenti (FAQ)

Domande generali

Q: Devo preoccuparmi di questo se uso la PKI privata?

A: No. Questo criterio ha effetto solo sui certificati rilasciati da CA radice pubbliche. La PKI privata e i certificati autofirmati non sono interessati.

Q: Cosa succede se non si utilizzano le connessioni mTLS?

R: Se si utilizza solo l'autenticazione standard TLS (Server Authentication), questo criterio non influisce sull'utente. I certificati solo server continueranno a funzionare. Verificare tuttavia i casi di utilizzo confrontandoli con l'elenco nella sezione Casi di utilizzo interessati specifici, poiché alcuni casi di utilizzo utilizzano mTLS come impostazione predefinita.

Q: Le connessioni Web HTTPS standard a Expressway smetteranno di funzionare?

R: No. Le connessioni TLS standard non sono interessate. L'accesso del browser Web a Expressway continua a funzionare normalmente anche con i certificati EKU di solo server.

Q: È possibile continuare a utilizzare i certificati esistenti?

A: Sì, i certificati esistenti con utilizzo chiavi avanzato combinato rimangono validi fino alla scadenza. Il problema si verifica quando è necessario eseguire il rinnovo. Funzionano sia per le connessioni TLS che per le connessioni mTLS fino alla scadenza.

Q: Come è possibile stabilire se si sta utilizzando mTLS o TLS standard?

A: Sezione Use Casessection interessata da ReviewSpecific.

D. Cosa posso fare adesso?

R: Cisco consiglia vivamente queste azioni immediate:

- Controllare i certificati

  Identifica i certificati TLS pubblici utilizzati per mTLS

- Rinnova certificati in anticipo

  Rinnovo prima del 15 marzo 2026 per massimizzare la validità

- Controllo automazione ACME

  Disabilita rinnovi automatici che possono sostituire certificati in modo imprevisto

- Coordinarsi con la propria CA

  Alcune CA offrono profili di certificato temporanei o alternativi

Q: CUCM SU3(a) compatibile con X15.4 e X15.5

A: Sì

Q: È presente una vulnerabilità della sicurezza quando si disabilita il controllo dell'utilizzo chiavi avanzato client in Cisco Expressway E (con versione X15.5)?

R: Il certificato controlla ancora CN/SAN per verificare che l'origine della connessione sia valida, ignora solo la convalida EKU (certificato per lo scopo del ruolo del client) che è stata inclusa per impostazione predefinita finché Google non solleva problemi di sicurezza, pertanto non deve avere problemi di sicurezza rispetto a prima.

Crittografia specifica

Q: Utilizzo Let's Encrypt con ACME su Expressway. Cosa fare?

A:

1. Rinnova il certificato prima dell'11 febbraio 2026 (più vicino possibile a tale data)
2. Disabilita l'utilità di pianificazione automatica ACME subito dopo il rinnovo
3. Pianificazione dell'aggiornamento a X15.5 per una soluzione a lungo termine

Q: È possibile modificare il profilo ACME per continuare a ottenere certificati EKU combinati?

A: No. Attualmente Expressway utilizza un profilo ACME "classico" hardcoded che non può essere modificato dagli utenti. Contattare Cisco TAC per il supporto del profilo certificato ACME.

Domande sull'aggiornamento

Q: È necessario aggiornare Expressway-E ed Expressway-C?

A: Sì, assolutamente. Per un corretto funzionamento, entrambi devono essere aggiornati alla stessa versione (X15.4 o X15.5).

Q: È possibile eseguire l'aggiornamento a X15.4 o attendere X15.5?

A:

- Eseguire l'aggiornamento a X15.4 in caso di problemi urgenti o se è necessario accettare certificati solo server
- Se possibile, attendere X15.5 (maggio 2026) per la soluzione completa con supporto per doppio certificato

D: La replica del cluster viene interrotta dopo il rinnovo del certificato. Cos'è successo?

R. È molto probabile che il nuovo certificato disponga solo dell'utilizzo chiavi avanzato per l'autenticazione server, ma:

- Se la versione è precedente a X15.4 con TLS Verify = Enforcement: I peer del cluster non possono stabilire connessioni mTLS senza l'utilizzo chiavi avanzato per l'autenticazione client
- Opzioni soluzione (una):

  Imposta la modalità di verifica TLS su "Permissiva" (meno sicura)

  Ottenere certificati con EKU combinato dalla radice CA alternativa

  Eseguire l'aggiornamento a X15.4 o versione successiva, ignorando la verifica dell'utilizzo chiavi avanzato di autenticazione client per ClusterDB

Q: Dopo l'aggiornamento a X15.4, è possibile utilizzare la modalità di imposizione con certificati solo server nel cluster?

R: Sì. A partire da X15.4, Expressway ignora la verifica dell'utilizzo chiavi avanzato autenticazione client per le connessioni mTLS ClusterDB. Pertanto, è possibile impostare la verifica TLS su "Enforcement" anche se uno o più nodi cluster dispongono solo di EKU di autenticazione server.

Q: Perché non è possibile caricare il certificato tramite l'interfaccia utente grafica di Expressway Web?

R: Prima di X15.4, la GUI Web applica una convalida hardcoded che richiede certificati con EKU di autenticazione client. Se il certificato dispone solo dell'utilizzo chiavi avanzato per l'autenticazione server, sono disponibili due opzioni:

- Utilizzare SCP (Secure Copy Protocol) per caricare il certificato direttamente sul server (cartella/persistent/Certs)
- Aggiorna a X15.4 o versione successiva (solo Expressway-E), rimuovendo questa restrizione

Q: Dopo l'aggiornamento a X15.4, non è ancora possibile caricare certificati solo server in Expressway-E

R: Dopo l'aggiornamento, verificare che il comando sia abilitato

CVS certificato XCP TLS xConfiguration EnableServerEkuUpload: On

Q: È stato eseguito l'aggiornamento a X15.4. È ora possibile caricare certificati solo server sia su Expressway-E che su Expressway-C?

R: No. X15.4 rimuove solo la restrizione di caricamento per Expressway-E. Expressway-C richiede ancora certificati EKU combinati per il caricamento tramite GUI Web. Ciò è dovuto al fatto che Expressway-C agisce spesso come client TLS nelle zone di attraversamento UC e richiede l'utilizzo chiavi avanzato di autenticazione client. Assicurarsi di eseguire questo comando in

Expressway-E. Questo comando non viene eseguito su Expressway-C

CVS certificato XCP TLS xConfiguration EnableServerEkuUpload: On

Q: Non è possibile registrare la Smart License dopo il rinnovo del certificato. Perché?

A: Errore di Smart Licensing dopo il rinnovo del certificato. In genere NON è correlato all'utilizzo chiavi avanzato:

- Verificare se Expressway è in grado di raggiungere tools.cisco.com (CSSM)
- Verificare che le regole del firewall consentano l'uscita HTTPS (porta 443)
- Verifica se la configurazione del proxy è corretta (se si utilizza il proxy HTTP)
- Verificare che il certificato del server CSM sia attendibile nell'archivio di attendibilità di Expressway
- Smart Licensing non richiede clientAuth, quindi questa modifica del criterio non influisce su di esso

Specifiche MRA (Mobile and Remote Access)

Q: L'autenticazione a più livelli richiede l'utilizzo chiavi avanzato di autenticazione client su Expressway-E?

R: Dipende dalla versione di Expressway:

- Prima di X15.4: Sì, richiesta indirettamente

  Durante la segnalazione SIP MRA, Expressway-E invia il proprio certificato firmato in un messaggio SIP SERVICE a Expressway-C

  Expressway-C convalida il certificato, richiedendo sia l'autenticazione client che l'utilizzo chiavi avanzato di autenticazione server

  Senza EKU combinato, la registrazione SIP MRA non riesce

- X15.4 e versioni successive: No

  Expressway-C non convalida più l'utilizzo chiavi avanzato di autenticazione client nel messaggio SIP SERVICE

  Expressway-E richiede solo l'utilizzo chiavi avanzato di autenticazione server per l'Autorità registrazione integrità

  La zona trasversale UC funziona in modo unidirezionale (Expressway-C convalida solo il certificato del server Expressway-E)

Q: Errore delle zone adiacenti dopo il caricamento delUtilizzo chiavi avanzato di autenticazione server in Expressway x15.4

A: Se si imposta la modalità di verifica TLS su "on", è necessario che disponga di un EKU di autenticazione client. È quindi possibile disabilitare la verifica TLS nella configurazione della zona

adiacente

Q: Quali certificati sono necessari per il corretto funzionamento dell'Autorità registrazione integrità?

A: Per un'implementazione tipica dell'MRA:

Componente	Requisiti dei certificati	EKU obbligatorio	Note
Expressway-E (prima di X15.4)	AutenticazioneServer + AutenticazioneClient	Entrambi	Per la convalida SIP SERVICE da Exp-C
Expressway-E (X15.4+)	solo serverAuth	Solo server	Controllo EKU client ignorato
Expressway-C	autenticazione client + autenticazione server	Entrambi	Agisce sempre come client in UC Traversal
Zona trasversale UC	Convalida unidirezionale	Exp-E: serverAuth Exp-C: autenticazione client	Exp-C convalida il certificato del server Exp-E

Q: Il certificato MRA funziona correttamente, ma dopo il rinnovo del certificato Expressway-E con EKU solo server, la registrazione SIP non riesce. Cosa non funziona?

R: Se si esegue una versione precedente a X15.4, la segnalazione SIP MRA richiede Expressway-E per presentare gli EKU di autenticazione server e client nel messaggio SIP SERVICE. Opzioni:

- Ottenere un certificato con EKU combinato
- Passare a una radice CA alternativa che emette l'EKU combinato
- Aggiornare Expressway-E ed Expressway-C a X15.4 o versione successiva (consigliato)

Gestione certificati

Q: Come ottenere un certificato con EKU combinato da DigiCert o IdenTrust?

A: Contattare il provider CA e richiedere un certificato dalla radice alternativa che emetta ancora EKU combinato.

Q: La CA indica che è possibile fornire solo certificati di solo server. Cosa fare?

A: Sono disponibili diverse opzioni:

- Verifica radici alternative: Chiedere all'autorità di certificazione se esistono radici alternative che generano EKU combinati (come DigiCert Assured ID o IdenTrust Public Sector)
- Cambia provider CA: Cerca CA che offrono EKU combinati da radici non Chrome-trusted
- Usa PKI privata: Imposta CA interna per i certificati EKU combinati (solo distribuzioni Expressway-C)
- Aggiornamento a X15.4: Soluzione intermittente per gestire i certificati solo con l'utilizzo chiavi avanzato ServerAuth e abilitare le registrazioni MRA
- Aggiornamento a X15.5 una volta disponibile: Pianificare un'architettura con doppio certificato in cui i certificati solo server siano accettabili e una soluzione completa per soddisfare i requisiti globali del programma radice Google Chrome

Domande sulle sequenze temporali

Q: Cosa succede il 15 giugno 2026?

A: Chrome interrompe l'attendibilità dei certificati TLS pubblici contenenti sia gli EKU di autenticazione server che client. I servizi che utilizzano tali certificati possono avere esito negativo.

Q: Perché devo rinnovare prima del 15 marzo 2026?

A: Dopo il 15 marzo 2026, la validità del certificato viene ridotta da 398 a 200 giorni. Il rinnovo prima di questa data offre la durata massima del certificato.

Q: Qual è il termine per l'azione?

A: Esistono più scadenze:

- 11 febbraio 2026: Encrypt ferma EKU combinato tramite ACME classico
- 15 marzo 2026: La validità del certificato è ridotta a 200 giorni
- Maggio 2026: La maggior parte delle CA pubbliche non emettono più EKU combinati
- Giugno 2026: Applicazione completa dei criteri Chrome

Ulteriori risorse

Documentazione di Cisco

- Notifica FN74362: Impatto di Cisco Expressway sulle comunicazioni sicure a causa delle imminenti modifiche ai certificati TLS
- ID bug Cisco CSCwr73373: Supporto di certificati server e client separati per Expressway

Riferimenti esterni

- Criterio programma radice riquadro
- Crittografia: Termine del supporto del certificato di autenticazione client TLS nel 2026
- Requisiti di base del forum CA/browser

Risorse Autorità di certificazione

- Portale di supporto DigiCert
- Servizi certificati IdenTrust
- Forum della community Let's Encrypt
- Knowledge Base di Sectigo

Conclusioni

Il sunsetting dell'utilizzo chiavi avanzato (EKU) di autenticazione client nei certificati delle CA pubbliche rappresenta un cambiamento significativo nei criteri di sicurezza che influisce sulle distribuzioni Cisco Expressway che utilizzano connessioni mTLS. Sebbene si tratti di una modifica a livello di settore, la valutazione dell'impatto è CRITICA in base alla notifica sul campo FN74362, ed è necessario intervenire immediatamente per evitare interruzioni del servizio.

Soluzioni chiave

- Questo problema interessa TUTTE le versioni di Expressway (X14 e X15 prima di X15.4)
- Controlla i certificati ADESSO - Questo è il primo passaggio obbligatorio
- Sono disponibili diverse soluzioni alternative: scegliere la soluzione più adatta per l'ambiente
- Sono necessari aggiornamenti software per una soluzione a lungo termine - Pianificazione per X15.5
- È necessario aggiornare sia Expressway-E che Expressway-C contemporaneamente
- Crittografia degli utenti alla prima scadenza - 11 febbraio 2026

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).