Preparare Cisco ISE per Client Auth EKU Sunset in Public CA Certificates

Sommario

Introduzione

Questo documento descrive l'impatto sui servizi ISE dovuto alle modifiche imminenti ai certificati TLS rilasciati dalle autorità di certificazione pubbliche con utilizzo chiavi avanzato (EKU) di autenticazione client.

Premesse

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 ISE che operano sia come server che come client in diversi scenari di connessione.

Descrizione del problema

Modifica criteri programma radice riquadro

A partire da maggio 2026, molte Autorità di certificazione pubbliche (CA) cesseranno di rilasciare certificati Transport Layer Security (TLS) che includono l'utilizzo chiavi esteso di autenticazione client (EKU). I nuovi certificati rilasciati includono in genere solo l'utilizzo chiavi avanzato per l'autenticazione del server.

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 di autenticazione server.
- 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: Marzo 2027.

Sequenza temporale risposta CA pubblica

- Ottobre 2025: Per impostazione predefinita, molte CA pubbliche (DigiCert, Sectigo, SSL) hanno iniziato a rilasciare certificati solo server.

- Maggio 2026: Molti server CA pubblici non rilasciano più certificazioni EKU di autenticazione client
- Marzo 2027: 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.

Impatto di Cisco ISE

Prodotti interessati

Tutte le versioni Cisco ISE sono interessate:

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

Nota: Sono interessate anche le versioni di Cisco ISE 2.x; tuttavia, non è prevista alcuna correzione poiché questi rilasci hanno raggiunto la fine del ciclo di vita (EOL).

Doppio ruolo di Cisco ISE

ISE opera come server e client in diversi scenari di connessione, richiedendo certificati con EKU di autenticazione server e client.

Cisco ISE come server (è necessario l'utilizzo chiavi avanzato per l'autenticazione server):

- PxGrid
- ISE Messaging Service

Cisco ISE as a Client (è necessario l'utilizzo chiavi avanzato per l'autenticazione del client):

- TC-NAC
- Syslog protetto
- LDAPS
- DTLS Radius

Casi di utilizzo specifici interessati

La tabella seguente riepiloga i servizi Cisco ISE che potrebbero essere interessati dalle prossime

modifiche dell'EKU di autenticazione client, insieme all'impatto previsto per ciascun servizio.

Servizio	Conseguenze
pxGrid	I certificati pxGrid vengono utilizzati per la comunicazione tra i nodi ISE e le integrazioni pxGrid esterne. Mentre le integrazioni pxGrid esterne richiedono solo l'utilizzo chiavi avanzato di autenticazione del server, Cisco ISE richiede attualmente certificati pxGrid importati che contengano sia l'utilizzo chiavi avanzato di autenticazione del server che l'utilizzo chiavi avanzato di autenticazione del client a causa di una restrizione dell'interfaccia utente. Di conseguenza, i certificati pxGrid emessi dalla CA pubblica vengono in genere distribuiti con entrambi gli EKU.
ISE Messaging Service (IMS)	IMS viene utilizzato per le comunicazioni back-end tra i servizi ISE interni. Cisco ISE richiede attualmente che i certificati IMS contengano sia l'EKU di autenticazione server che l'EKU di autenticazione client. I certificati rinnovati da una CA pubblica solo con EKU di autenticazione server non possono essere utilizzati per IMS, il che può causare errori nella comunicazione ISE interna.
TC-NAC	Se il certificato Admin contiene solo l'EKU di autenticazione server, l'autenticazione basata su certificato per TC-NAC potrebbe risentire dell'attivazione della modalità FIPS o della configurazione di Tenable con mTLS (introdotta nelle versioni ISE 3.4P3 e 3.5).
Syslog protetto	
LDAP	
DTLS RADIUS	

⚠ Attenzione: I clienti devono verificare il tipo di certificato utilizzato da qualsiasi client pxGrid esterno. Al momento del rinnovo, i certificati firmati dalla CA pubblica non possono più includere l'utilizzo chiavi avanzato per l'autenticazione client. Le integrazioni client pxGrid esterne devono includere l'utilizzo chiavi avanzato di autenticazione client quando si comunica con ISE, altrimenti la connessione verrà rifiutata.

Sintomi dei problemi

Dopo la distribuzione dei certificati solo EKU di autenticazione server in Cisco ISE, gli utenti osserveranno errori di importazione dei certificati nella GUI di Cisco ISE quando tenteranno di caricare certificati pxGrid o IMS (ISE Messaging Service) che non soddisfano gli attuali requisiti di utilizzo chiavi esteso (EKU) per il servizio selezionato.

Di seguito è riportato un esempio del messaggio di errore visualizzato nella GUI.

Consigli

Controlla certificati correnti (PRIMO PASSAGGIO OBBLIGATORIO)

- Preparare un inventario di tutti i certificati TLS pubblici per identificare quali certificati contengono l'utilizzo chiavi avanzato (EKU) di autenticazione client
- Utilizzo certificato documento: consente di identificare i certificati utilizzati in base alla tabella precedente e firmati con CA pubblica.
- 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

Suggerimenti per i servizi che richiedono l'utilizzo chiavi avanzato client

Nella tabella seguente vengono fornite le azioni consigliate per i servizi e le integrazioni Cisco ISE che si basano sui certificati contenenti l'utilizzo chiavi avanzato (EKU) di autenticazione client.

Servizio	Azioni consigliate
TC-NAC	• Quando si utilizza Tenable, è possibile disabilitare la convalida EKU rigorosa sul lato Tenable per mantenere la connettività.
Syslog protetto	
LDAP	
DTLS RADIUS	
Client PxGrid (CatC, FMC...ecc.)	
EAP-TLS	

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 EKU:

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 dell'amministratore di Cisco Identity Services Engine, versione 3.3
- Configurazione dei rinnovi dei certificati in ISE

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.

Opzione 3: Valutazione e migrazione a provider CA alternativi

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

Soluzione a lungo termine (aggiornamento software necessario)

I clienti devono aggiornare Cisco ISE a una versione patch che introduca una gestione aggiornata dei certificati per supportare i certificati rilasciati in base alle nuove policy CA.

I seguenti rilasci di patch risolvono questo problema pianificato per aprile 2026:

Cisco ISE versione	Versione patch
ISE 3.1	Patch 1
ISE 3.2	Patch 10
ISE 3.3	Patch 1
ISE 3.4	Patch 6

ISE 3.5	Patch 3

Comportamento dopo l'installazione delle patch

Certificato PxGrid

Dopo aver installato la release della patch:

- Il requisito corrente dell'interfaccia utente che impone sia l'utilizzo chiavi avanzato di autenticazione server che l'utilizzo chiavi avanzato di autenticazione client per i certificati pxGrid verrà rimosso.
- Cisco ISE consentirà l'importazione di certificati pxGrid contenenti solo EKU di autenticazione server, EKU di autenticazione server e client o nessuna estensione EKU.
- I certificati contenenti solo l'utilizzo chiavi avanzato di autenticazione client non verranno accettati.

Certificato ISE Messaging Service (IMS)

Per ISE 3.1, 3.2 e 3.3

Dopo l'installazione della patch non vi è alcuna modifica nel comportamento. Il servizio di messaggistica ISE continuerà a richiedere un certificato con EKU sia client che server. I clienti devono pianificare l'utilizzo di un certificato CA interno ISE alla scadenza del certificato corrente.

Per ISE 3.4 e 3.5

IMS ora supporta solo i certificati CA pubblici contenenti l'utilizzo chiavi avanzato (EKU) di autenticazione server. Tuttavia, poiché il protocollo IMS viene utilizzato solo per le comunicazioni ISE interne di Cisco, Cisco consiglia di utilizzare il certificato ISE Internal CA quando il certificato viene rinnovato.

Albero delle decisioni

INIZIO: Si utilizzano certificati CA pubblici su Cisco ISE?

Azure

├: PKI privata o autofirmato

│ └ Nessuna azione richiesta - Non influenzata dai criteri

Azure

└ SÌ: Certificati CA pubblici in uso

Azure

├. Sono utilizzati per uno dei servizi menzionati nella sezione "Casi di utilizzo specifici interessati"?

INSTALLAZIONE

¨ ├· Servizi quando ISE funge da client TLS

│ ™ Rivedere la sezione "Suggerimenti per i servizi che richiedono l'utilizzo chiavi avanzato del client".

INSTALLAZIONE

└ Servizi quando ISE funge da server TLS (PxGrid O IMS)

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

\ ├· Questo aiuterà a rendere più urgente l'applicazione di patch a Cisco ISE

PROCEDURA GUIDATA

¨ ├ ™ 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

¨ ├- Impostare l'infrastruttura della CA privata

\ ├· Rilasciare certificati EKU combinati

¨ ├ ™ - Installare la nuova CA nell'archivio attendibile ISE

│ ™] Controllo a lungo termine

INSTALLAZIONE

└ - Opzione D: Pianificazione dell'aggiornamento software

™ ├. Applicare la versione richiesta della patch ISE (disponibile da aprile 2026)

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: 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: Vedere la sezione Casi di utilizzo interessati specifici.

Domande sull'aggiornamento

Gestione certificati

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:

- 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
- Marzo 2027: Applicazione completa dei criteri Chrome

Ulteriori risorse

- ID bug Cisco: CSCws83036 - Valutazione dell'impatto dell'imposizione dell'EKU ClientAuth ad ISE

Riferimenti esterni

- Criterio programma radice riquadro

Risorse Autorità di certificazione

- Portale IdenTrust

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 ISE con connessioni mTLS. Sebbene si tratti di una modifica a livello di settore, la valutazione dell'impatto è di IMPORTANZA CRITICA ed è necessario intervenire immediatamente per evitare interruzioni del servizio.

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).