Impatto di Cisco Secure Firewall delle modifiche all'EKU di autenticazione client CA pubblica a partire da maggio 2026 per le comunicazioni protette

Introduzione

Questo documento descrive l'impatto delle restrizioni sui criteri di rilascio dei certificati imposte dalle autorità di certificazione che sono conformi al programma Chrome Root Certificate, in particolare per quanto riguarda i prodotti Cisco Secure Firewall.

Premesse

I certificati TLS pubblicamente attendibili vengono rilasciati da CA che devono rispettare i criteri di settore che regolano il rilascio e l'utilizzo dei certificati.

La Chrome Root Program Policy, gestita da Google, definisce i requisiti che le CA devono seguire affinché i loro certificati siano considerati attendibili dal browser Google Chrome. Questi requisiti influenzano il modo in cui i certificati pubblicamente attendibili vengono rilasciati nel settore. Come parte delle pratiche di sicurezza in evoluzione, il Chrome Root Program sta introducendo linee guida più rigorose sull'uso dei certificati.

Molte CA pubbliche stanno pertanto abbandonando l'opzione di rilascio dei certificati che includono l'utilizzo chiavi avanzato di autenticazione client e stanno passando al rilascio dei certificati destinati solo all'autenticazione server. Di conseguenza, i nuovi certificati rilasciati da molte CA pubbliche devono includere solo l'utilizzo chiavi avanzato di autenticazione server.

L'utilizzo chiavi avanzato (EKU, Extended Key Usage), è un'estensione di certificato che definisce la funzione desiderata di una chiave pubblica all'interno di un certificato digitale. Stabilisce un set strutturato di applicazioni consentite, garantendo che la chiave venga utilizzata solo per operazioni di crittografia specifiche. Questa funzionalità è gestita da OID (Object Identifier), ovvero identificatori numerici univoci che categorizzano ogni utilizzo consentito, ad esempio firma codice, autenticazione server, autenticazione client o posta elettronica protetta.

Quando l'autenticazione è basata su certificato, l'entità di verifica esamina il certificato per identificare l'OID (Object

Identifier) nell'EKU. Incorporando l'estensione EKU, un'autorità di certificazione (CA) limita l'ambito del certificato a ruoli predefiniti, con ogni scopo designato mappato in modo esplicito a un OID.

Scopo degli attributi EKU

· Definizione dell'utilizzo: Gli attributi EKU chiariscono i tipi di autenticazione o crittografia che il certificato è autorizzato a eseguire.

· Miglioramento della sicurezza: Limitando i certificati a utilizzi specifici, l'utilizzo chiavi avanzato (EKU) consente di impedire l'utilizzo improprio o involontario di applicazioni (ad esempio, non è possibile utilizzare un certificato server per l'autenticazione client).

· Conformità: Assicura che i certificati vengano utilizzati in conformità con i criteri di sicurezza e gli standard di settore.

Principali utilizzi degli attributi EKU

1. Autenticazione client Web TLS

· Consente l'utilizzo di certificati per l'identificazione e l'autenticazione di utenti o dispositivi su un server.

· OID: 1.3.6.1.5.5.7.3.2

· Utilizzato in scenari VPN, TLS reciproco e accesso sicuro.

2. Autenticazione server Web TLS

· Consente l'utilizzo dei certificati da parte dei server per dimostrare la propria identità ai client.

· OID: 1.3.6.1.5.5.7.3.1

· Utilizzato in HTTPS, nei server Web SSL/TLS e negli endpoint API protetti.

3. Firma codice

· Indica che il certificato può essere utilizzato per firmare software o eseguibili.

· OID: 1.3.6.1.5.5.7.3.3

· Utilizzato nei controlli di integrità e distribuzione del software.

4. Protezione e-mail

· Consente di utilizzare i certificati per firmare e crittografare i messaggi di posta elettronica.

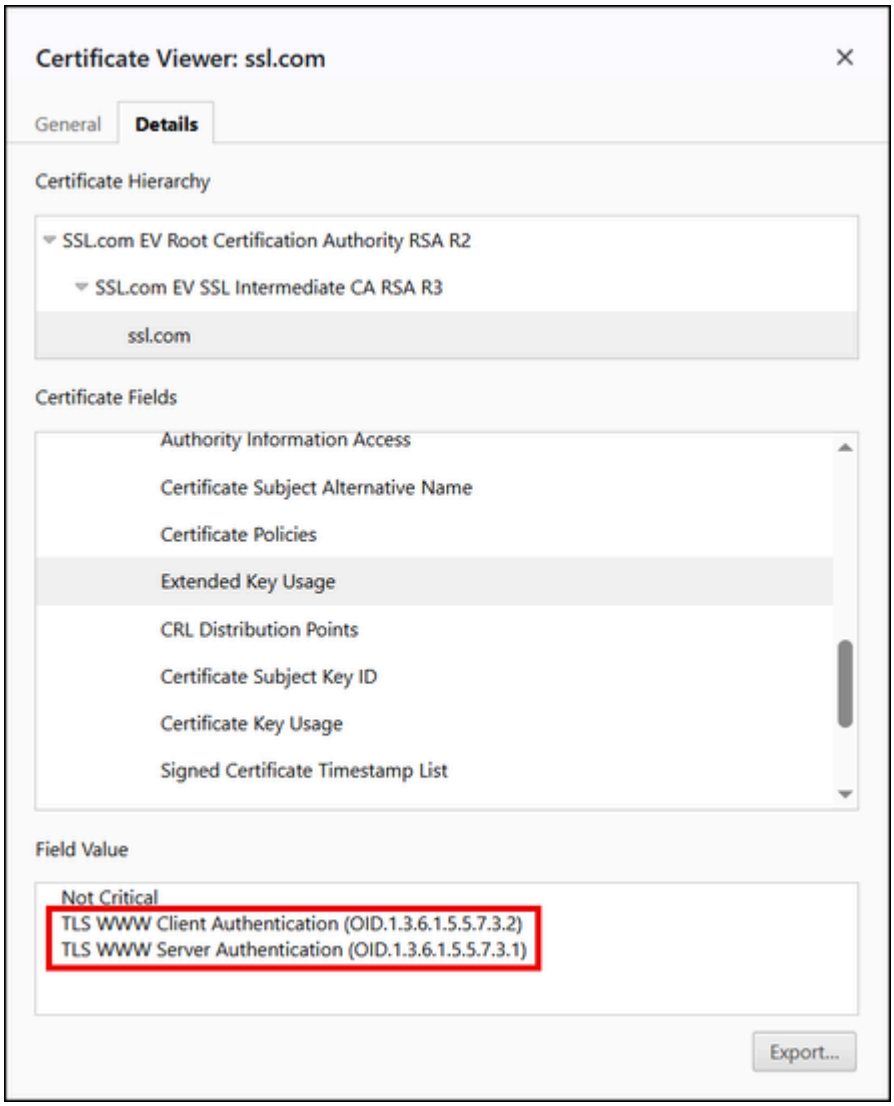
· OID: 1.3.6.1.5.5.7.3.4

· Utilizzato nella protezione e-mail S/MIME.

5. Altri scopi

· Firma dei documenti, timestamp, accesso tramite smart card e così via, ciascuno con il proprio OID.

Per stabilire una connessione protetta per HTTPS, i browser e i server devono solo utilizzare l'EKU serverAuth. Storicamente, molti certificati server TLS includevano sia l'EKU serverAuth che l'EKU clientAuth. Di seguito è riportato un esempio di tale certificato:



Perché la rimozione dell'utilizzo chiavi avanzato di autenticazione client dai certificati del server?

- Protezione e ambito: i certificati TLS pubblici devono solo autenticare i server sul Web. La rimozione offre una netta separazione tra le funzionalità server e client. L'utilizzo chiavi avanzato ClientAuth viene utilizzato per l'autenticazione di computer e utenti con Mutual TLS (mTLS) e altri scenari di autenticazione.

- Prevenzione di configurazioni errate: alcuni sistemi potrebbero considerare attendibile qualsiasi certificato di una CA pubblica per l'autenticazione client se è presente l'EKU, il che potrebbe rappresentare un rischio per la sicurezza.

- Requisiti del browser: i principali browser non richiedono o controllano l'EKU clientAuth nel certificato di un sito Web.

- Architettura PKI semplificata: separando gli utilizzi, le CA possono mantenere gerarchie di certificati distinte per i TLS del server rispetto ad altri scopi.

Ciò è particolarmente importante per prodotti come Cisco Secure Firewall Adaptive Security Appliance (ASA), Cisco Secure Firewall Threat Defense (FTD), Cisco Secure Firewall Device Manager (FDM) e Cisco Secure Firewall Management Center (FMC) che potrebbero funzionare come server o client durante l'autenticazione TLS, a seconda dello scenario di utilizzo.

Impatto sugli ambienti server

Per la maggior parte delle installazioni server, questa modifica avrà un impatto ridotto o nullo. Ecco cosa aspettarsi:

- Server Web standard (HTTPS): nessun impatto. I certificati aggiornati continueranno a funzionare normalmente.
- Certificati esistenti: tutti i certificati rilasciati prima della scadenza continueranno a funzionare fino alla scadenza.
- Scenari Mutual TLS (mTLS) e Client Cert: se si utilizza un certificato server TLS per l'autenticazione client, sarà necessario ottenere un certificato separato con l'EKU clientAuth da un'altra origine.
- Sistemi aziendali che richiedono entrambi gli EKU: alcuni sistemi legacy o aziendali prevedevano entrambi gli EKU. È necessario verificare se sono necessari aggiornamenti per conformarsi alle nuove regole.

Descrizione del problema

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

Di conseguenza, se i certificati rilasciati da una CA pubblica vengono rinnovati in base ai criteri aggiornati della CA e quindi distribuiti nei prodotti Cisco Secure Firewall, i servizi per i quali è richiesto l'utilizzo chiavi avanzato di autenticazione client non riusciranno. I servizi specifici interessati sono i seguenti:

- Quando l'ASA, FTD, FDM o FMC funge da client, ad esempio quando ci si connette a provider di identità o a server di autenticazione come ISE (pxGrid), RADIUS, LDAPS o Active Directory, l'autenticazione basata sui certificati potrebbe non riuscire se il certificato client è stato generato da una CA pubblica e non è presente l'EKU di autenticazione client. In questi scenari, se il server di autenticazione rifiuta i certificati senza l'utilizzo chiavi avanzato richiesto, potrebbero verificarsi errori di connessione.
- Cisco Secure Client (in precedenza AnyConnect) può autenticarsi sui server ASA o FTD utilizzando i certificati. Tuttavia, se il certificato client è stato generato da una CA pubblica e manca l'EKU di autenticazione client, la connessione VPN (RAVPN) ad accesso remoto avrà esito negativo.

- Quando l'FTD o l'ASA stabiliscono un tunnel VPN da sito a sito, sia per un altro FTD, ASA, router Cisco o un peer VPN di terze parti, utilizzando l'autenticazione del certificato (RSA o ECDSA), il tunnel avrà esito negativo se sul certificato di identità generato da una CA pubblica manca l'attributo EKU di autenticazione client. Ciò si verifica perché il peer VPN remoto richiede che l'utilizzo chiavi avanzato di autenticazione client sia presente nel certificato di identità.

Modifica criteri programma radice riquadro

L'implementazione dell'EKU dipende dalla CA che firma il certificato. L'utilizzo dell'utilizzo dell'utilizzo chiavi avanzato (EKU) per l'autenticazione server e l'autenticazione client è una pratica comune. Tuttavia, come parte dei criteri del programma radice Chrome, l'allineamento delle CA a questi criteri di rilascio dei certificati comporta l'interruzione della firma dei certificati TLS che includono l'utilizzo chiavi avanzato (EKU) per l'autenticazione client. I nuovi certificati rilasciati includono solo l'utilizzo chiavi avanzato di autenticazione 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 causando il contrassegno di tali certificati come "Non attendibili" da parte del browser Chrome

Linee temporali

- Settembre 2025, SSL.com emetterà certificati TLS che includono solo l'EKU ServerAuth (e non ClientAuth) per i certificati server. In altre parole, i nuovi certificati SSL/TLS per il sito Web o il server saranno esplicitamente solo per "Autenticazione server".
- Ottobre 2025: le CA che si allineano al programma (ad esempio DigiCert, Sectigo e così via) hanno iniziato a rilasciare certificati solo server per impostazione predefinita.
- Maggio 2026: le CA che si allineano al programma interrompono il rilascio dei certificati EKU di autenticazione client

- Marzo 2027: Chrome Root Program Policy diventa pienamente efficace

Impatto sui prodotti Cisco Secure Firewall

Dopo che le CA pubbliche hanno iniziato a includere solo l'utilizzo chiavi avanzato di autenticazione server nei certificati rilasciati. Questo potrebbe avere il seguente impatto sui prossimi scenari di prodotto di Cisco Secure Firewall:

- Quando l'ASA, FTD, FDM o FMC funge da client, ad esempio quando ci si connette a provider di identità o a server di autenticazione come ISE (pxGrid), RADIUS, LDAPS o Active Directory, l'autenticazione basata sui certificati potrebbe non riuscire se il certificato client è stato generato da una CA pubblica e non è presente l'EKU di autenticazione client. In questi scenari, se il server di autenticazione rifiuta i certificati senza l'utilizzo chiavi avanzato richiesto, potrebbero verificarsi errori di connessione.

- Cisco Secure Client (in precedenza AnyConnect) può autenticarsi sui server ASA o FTD utilizzando i certificati. Tuttavia, se il certificato client è stato generato da una CA pubblica e manca l'EKU di autenticazione client, la connessione VPN (RAVPN) ad accesso remoto avrà esito negativo.

- Quando l'FTD o l'ASA stabiliscono un tunnel VPN da sito a sito, sia per un altro FTD, ASA, router Cisco o un peer VPN di terze parti, utilizzando l'autenticazione del certificato (RSA o ECDSA), il tunnel avrà esito negativo se sul certificato di identità generato da una CA pubblica manca l'attributo EKU di autenticazione client. Ciò si verifica perché il peer VPN remoto richiede che l'utilizzo chiavi avanzato di autenticazione client sia presente nel certificato di identità.

Nota: se si sta integrando FMC o FDM con ISE tramite pxGrid e i certificati installati in FMC/FDM non dispongono dell'attributo EKU di autenticazione client, esaminare le soluzioni proposte in questo documento e i successivi riferimenti ISE: FN74392 e preparare Identity Services Engine for Extended Key Usage Restrictions in Certificates Issued by Public Certification Authorities.

Nota: La rimozione dell'utilizzo chiavi avanzato clientAuth dai certificati del server TLS è una modifica ai criteri a livello di settore che migliorerà la sicurezza e impedirà l'utilizzo improprio. Per la maggior parte degli utenti non vi sarà alcun impatto significativo. Tuttavia, se si utilizza l'utilizzo chiavi avanzato ClientAuth, è consigliabile adottare misure proattive per ottenere il tipo di certificato corretto per le proprie esigenze.

Prodotti interessati

Prodotto Cisco Secure Firewall	Versione del software	Scenari interessati	Correzioni
FTD	Tutte le versioni	Quando funge da client, ad esempio durante la	Opzione 1. Se si

FDM	Tutte le versioni	connessione a provider di identità o a server di autenticazione quali ISE (pxGrid), RADIUS, LDAPS o Active Directory, l'autenticazione basata su certificato potrebbe non riuscire se il certificato client è stato generato da una CA pubblica e non dispone dell'EKU di autenticazione client. In questo scenario, se il server di autenticazione rifiuta i certificati senza l'utilizzo chiavi avanzato richiesto, potrebbero verificarsi errori di connessione.	utilizza un certificato server TLS per l'autenticazione client, sarà necessario ottenere un certificato con l'EKU ClientAuth da un'altra origine. O Opzione 2. Passare alle CA radice pubbliche (Autorità di certificazione) che forniscono certificati EKU (ClientAuth e ServerAuth) combinati. NOTA: Per ulteriori informazioni, consultare la sezione Soluzioni alternative di questo documento.
CCP	Tutte le versioni		
ASA	Tutte le versioni		
Cisco Secure Client (in precedenza AnyConnect)	Tutte le versioni	Cisco Secure Client può autenticarsi sui server ASA o FTD usando i certificati. Tuttavia, se il certificato client è stato generato da una CA pubblica e manca l'EKU di autenticazione client, la connessione VPN (RAVPN) ad accesso remoto avrà esito negativo.	
FTD o ASA	Tutte le versioni	Quando l'FTD o l'ASA stabiliscono	

		un tunnel VPN da sito a sito, sia per un altro FTD, ASA, router Cisco o un peer VPN di terze parti, utilizzando l'autenticazione del certificato (RSA o ECDSA), il tunnel VPN avrà esito negativo se nel certificato di identità generato da una CA pubblica manca l'attributo EKU di autenticazione client. Ciò si verifica perché il peer VPN remoto richiede che l'utilizzo chiavi avanzato di autenticazione client sia presente nel certificato di identità.	

Nota: se si sta integrando FMC o FDM con ISE tramite pxGrid e i certificati installati in FMC/FDM non dispongono dell'attributo EKU di autenticazione client, esaminare le soluzioni proposte in questo documento e i successivi riferimenti ISE: FN74392 e preparare Identity Services Engine for Extended Key Usage Restrictions in Certificates Issued by Public Certification Authorities.

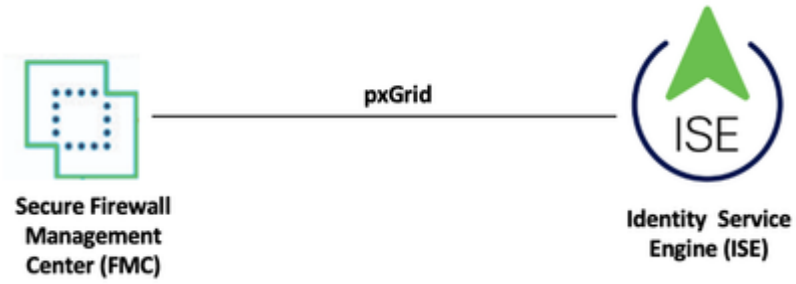
Nota: La rimozione dell'utilizzo chiavi avanzato clientAuth dai certificati del server TLS è una modifica ai criteri a livello di settore che migliorerà la sicurezza e impedirà l'utilizzo improprio. Per la maggior parte degli utenti non vi sarà alcun impatto significativo. Tuttavia, se si utilizza l'utilizzo chiavi avanzato ClientAuth, è consigliabile adottare misure proattive per ottenere il tipo di certificato corretto per le proprie esigenze.

Attenzione: Per gli ambienti di produzione, si consiglia di utilizzare i certificati con gli attributi EKU appropriati. Questa pratica garantisce sicurezza, compatibilità e conformità agli standard e alle procedure ottimali del settore. I certificati senza attributi EKU devono essere considerati solo come una soluzione temporanea e solo con una chiara comprensione dei rischi associati.

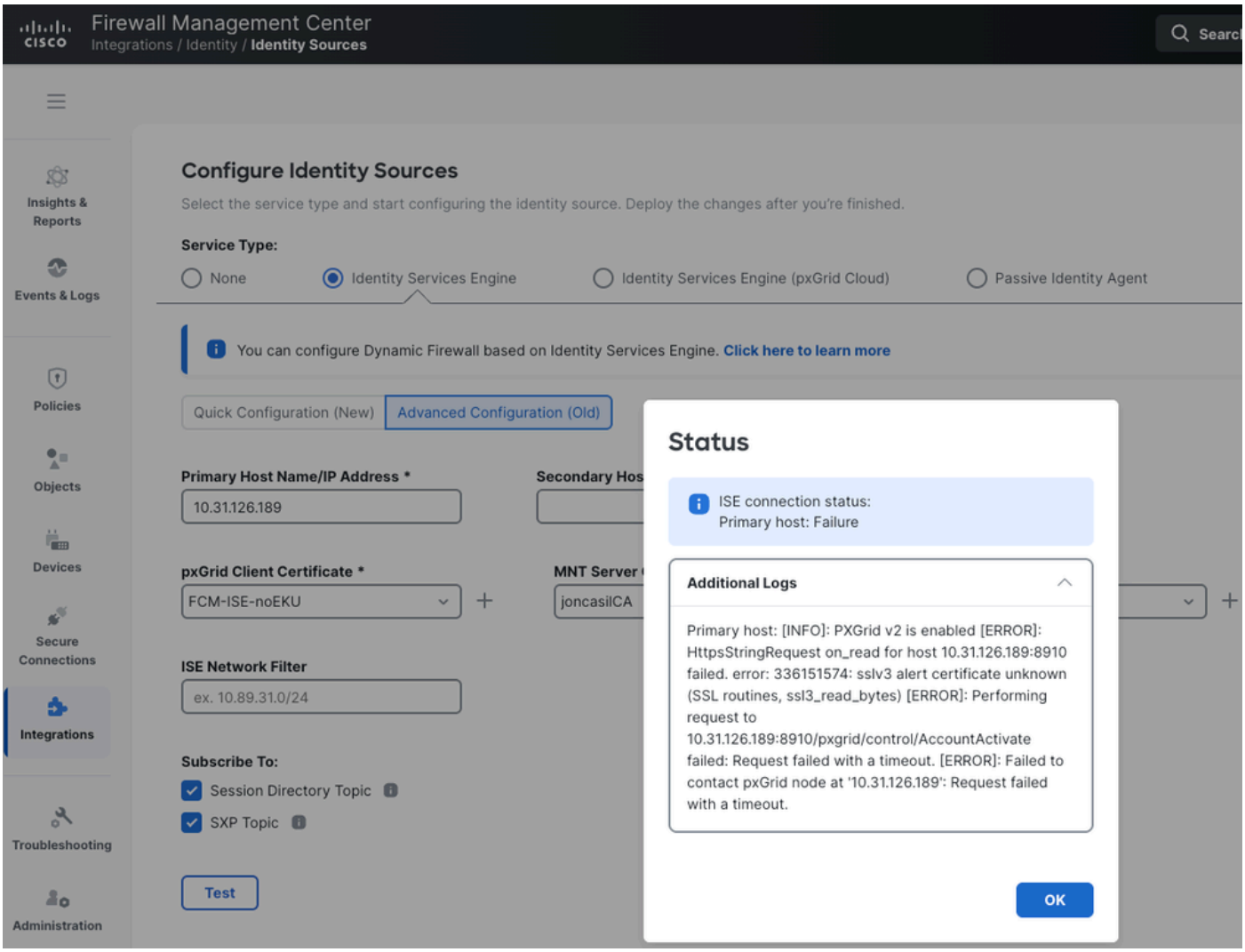
Problema 1. Problema di integrazione pxGrid tra FMC e ISE, quando il certificato FMC non dispone dell'attributo EKU di autenticazione client

In questo scenario, il certificato utilizzato dalla console centrale di gestione del sistema per l'integrazione di pxGrid con ISE non dispone dell'attributo EKU di autenticazione client. Di conseguenza, l'integrazione di pxGrid non riesce perché il server ISE si aspetta che questo attributo sia presente nel certificato presentato dal FMC.

Topologia



Errori interfaccia utente FMC: Questo è il messaggio di errore visualizzato nel CCP, quando il certificato utilizzato dal CCP non contiene l'attributo EKU di autenticazione client per l'integrazione di pxGrid con ISE.



Errori CLI FMC: Gli stessi messaggi di errore si trovano nella directory FMC /var/log/messages.

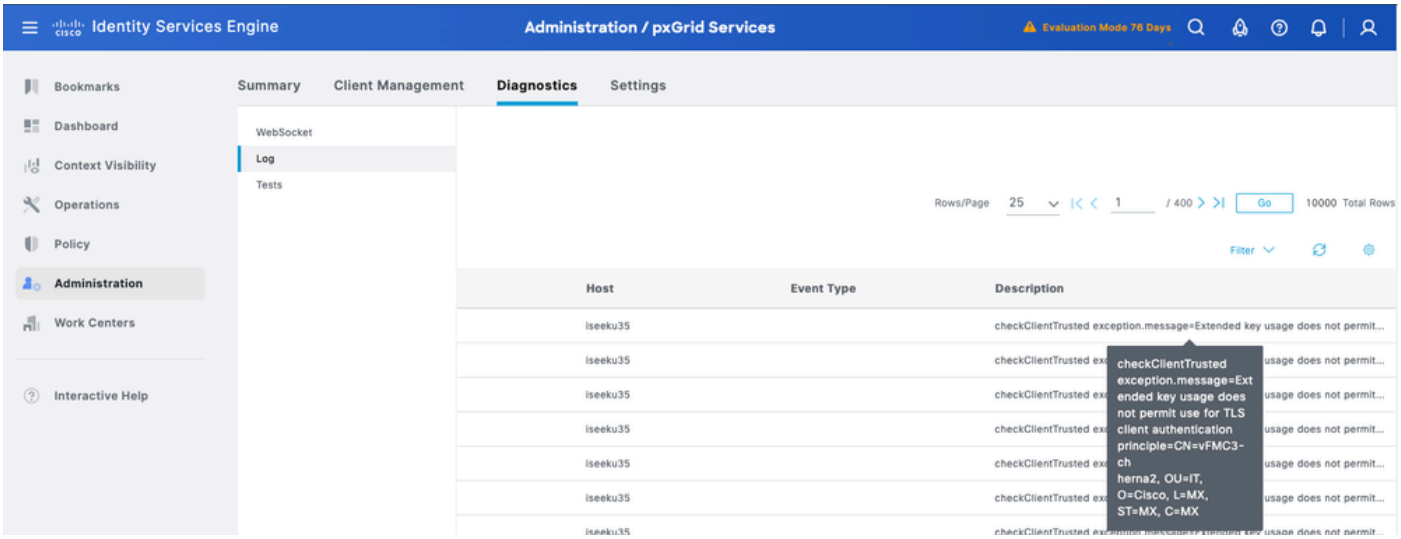
<#root>

```
HttpsStringRequest on_read for host 10.31.126.189:8910 failed. error: 336151574:

sslv3 alert certificate unknown


(SSL routines, ssl3_read_bytes)

Mar 27 23:17:17 vFMC3-chherna2 SF-IMS[8074]: [7514] ADI:HttpsEndpoint

[ERROR] Performing request to 10.31.126.189:8910/pxgrid/control/AccountActivate failed: Request failed w

Mar 27 23:17:17 vFMC3-chherna2 SF-IMS[8074]: [7514] ADI:ise_connector.PXGrid2ThreadedService
```

```
[ERROR] pxgrid2_service was not created for 10.31.126.189. Reason - Request failed with a timeout.
```

```
Mar 27 23:17:47 vFMC3-chherna2 SF-IMS[8074]: [7514] ADI:ise_connector.PXGrid2ThreadedService [I
Mar 27 23:17:47 vFMC3-chherna2 SF-IMS[8074]: [7514] ADI:ise_connector.PXGrid2ThreadedService [I
```

Errore ISE: Questo è il messaggio di errore visualizzato in ISE, "checkClientTrusted exception.message=Extended key usage does not allow use for TLS client authentication princip=CN=vFMC3-chherna2, OU=IT, O=Cisco, L=MX, ST=MX, C=MX".



Soluzione: se si sta integrando FMC o FDM con ISE tramite pxGrid e il certificato installato in FMC/FDM non dispone dell'attributo EKU di autenticazione client, rivedere i riferimenti proposti in questo documento e i successivi riferimenti ISE: FN74392 e Prepare Identity Services Engine for Extended Key Usage Restrictions in Certificates Issued by Public Certification Authorities per una corretta integrazione di pxGrid.

Nota: Il certificato client pxGrid di FMC deve includere l'attributo EKU ClientAuth oppure non deve contenere alcun attributo EKU Client o Server.

Nota: Anche se l'utilizzo di un certificato firmato dalla CA pubblica è supportato per IMS. Cisco consiglia di utilizzare il certificato CA interno ISE, in quanto questa comunicazione è valida solo per le transazioni interne.

Problema 2. Problema di integrazione FTD o ASA con un server LDAPS, quando il certificato presentato non contiene l'attributo EKU di autenticazione client

In questo scenario, l'FTD o l'ASA fungono da client per l'integrazione con un server LDAPS che utilizza l'autenticazione

del certificato. Se il certificato utilizzato dall'FTD o dall'ASA è privo dell'attributo EKU di autenticazione client, l'integrazione non riesce perché il server LDAPS richiede che questo attributo sia presente nel certificato.

Topologia

Errori server LDAPS: 'Verifica certificato TLS: Errore, scopo del certificato non supportato e 'traccia TLS: Avviso SSL3: scrittura:irreversibile:certificato non supportato'

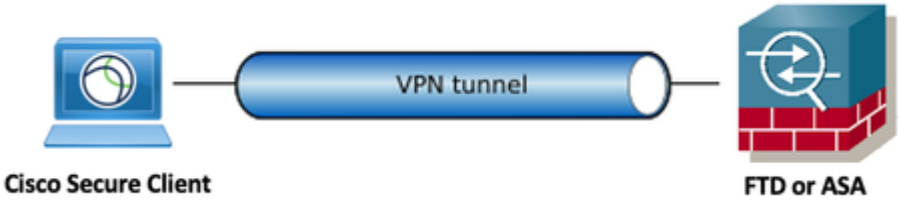
```
69ceb4f5.157b4993 0x7ff553fff700 TLS trace: SSL_accept:TLSv1.3 write server cer
tificate verify
69ceb4f5.157c01a4 0x7ff553fff700 TLS trace: SSL_accept:SSLv3/TLS write finished
69ceb4f5.157c458a 0x7ff553fff700 TLS trace: SSL_accept:TLSv1.3 early data
69ceb4f5.157c6685 0x7ff553fff700 TLS trace: SSL_accept:error in TLSv1.3 early d
ata
69ceb4f5.15b17eaa 0x7ff5522fc700 connection_get(15): got connid=1004
69ceb4f5.15b1b73f 0x7ff5522fc700 connection_read(15): checking for input on id=
1004
69ceb4f5.15b2bf05 0x7ff5522fc700 TLS trace: SSL_accept:TLSv1.3 early data
69ceb4f5.15b4c6c3 0x7ff5522fc700 TLS certificate verification: depth: 0, err: 2
6, subject: /CN=asa-server-only,69ceb4f5.15b4e8de 0x7ff5522fc700  issuer: /CN=T
est-CA
69ceb4f5.15b4f367 0x7ff5522fc700 TLS certificate verification: Error, unsupport
ed certificate purpose
69ceb4f5.15b57df8 0x7ff5522fc700 TLS trace: SSL3 alert write:fatal:unsupported
certificate
69ceb4f5.15b5b557 0x7ff5522fc700 TLS trace: SSL_accept:error in error
69ceb4f5.15b66c36 0x7ff5522fc700 TLS: can't accept: error:1417C086:SSL routines
:tls_process_client_certificate:certificate verify failed (unsupported certific
ate purpose).
69ceb4f5.15b70391 0x7ff5522fc700 connection_read(15): TLS accept failure error=
-1 id=1004, closing
69ceb4f5.15b747ae 0x7ff5522fc700 connection_close: conn=1004 sd=15
```

Soluzione: rivedere le informazioni proposte in questo documento per assicurarsi che l'FTD o l'ASA utilizzino il certificato di identità corretto, incluso l'attributo EKU di autenticazione client, per un'autenticazione basata su certificato riuscita con il server LDAPS.

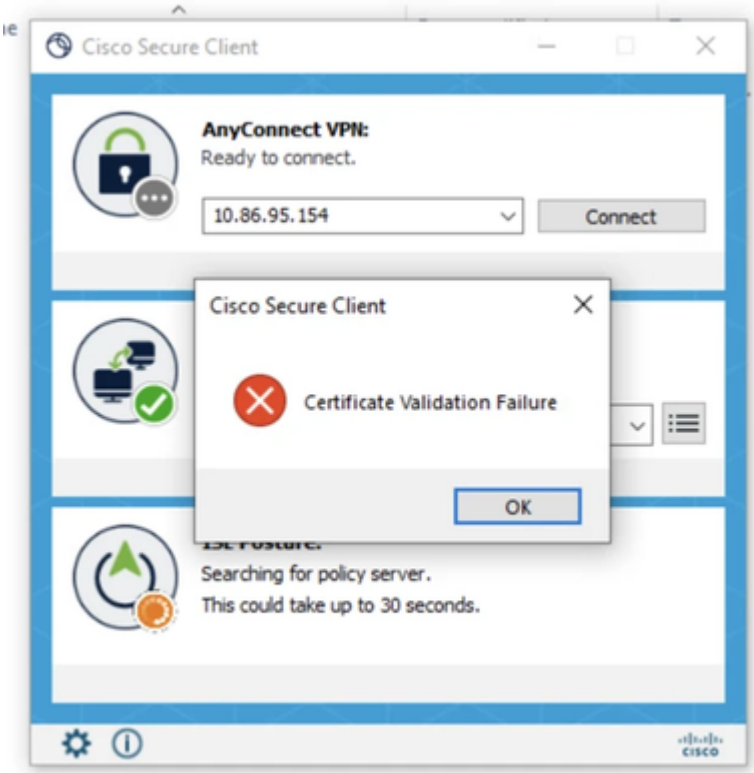
Problema 3. Cisco Secure Client (in precedenza AnyConnect) potrebbe riscontrare problemi di connessione a un FTD o a un'ASA se il certificato client non dispone dell'attributo EKU di autenticazione client

In questo scenario, Cisco Secure Client utilizza l'autenticazione dei certificati per stabilire un tunnel RAVPN per l'FTD o l'ASA. Tuttavia, se il certificato client non dispone dell'attributo EKU di autenticazione client, la sessione RAVPN avrà esito negativo perché l'ASA o l'FTD richiede che questo attributo sia presente nel certificato client.

Topologia



Errore Cisco Secure Client: 'Errore di convalida del certificato'



Errori DART di Cisco Secure Client:i seguenti log del file AnyConnectVPN.txt nel bundle DART confermano che Cisco Secure Client ha rifiutato il certificato usato per l'autenticazione basata su certificato RAVPN per FTD/ASA a causa dell'assenza dell'attributo EKU di autenticazione client (per individuare il file AnyConnectVPN.txt nel bundle DART, passare a Cisco Secure Client >

AnyConnect VPN > Log > AnyConnectVPN.txt.).

<#root>

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

Date : 04/07/2026
Time : 03:35:22
Type : Error
Source : csc_vpnapi


Description : Function: CVerifyExtKeyUsage::compareEKUs


File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\CommonCrypt\Certificates\VerifyEx
Line: 330

EKU not found in certificate: 1.3.6.1.5.5.7.3.2



*****************************************

Date : 04/07/2026
Time : 03:35:22
Type : Information
Source : csc_vpnapi


Description : Function: CCertStore::GetCertificates


File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\CommonCrypt\Certificates\CertStor
Line: 225

Ignoring client certificate because it does not contain the required EKU extension.

 Certificate details:
Store: [Omitted Output]

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

Soluzione: rivedere le informazioni proposte in questo documento per verificare che Cisco Secure Client utilizzi il certificato corretto, incluso l'attributo EKU di autenticazione client, per una corretta autenticazione basata su certificato con FTD o ASA.

Nota: Dall'errore del bundle DART sopra riportato 'EKU non trovato nel certificato: 1.3.6.1.5.5.7.3.2", questo numero "1.3.6.1.5.7.3.2" corrisponde all'OID EKU di autenticazione client.

Problema 4. I tunnel VPN da sito a sito con autenticazione basata su certificato hanno esito negativo se nel certificato di identità manca l'attributo EKU di autenticazione client

In questo scenario, che prevede l'autenticazione basata su certificato per un tunnel VPN da sito a sito IKEv2, il certificato di identità utilizzato da FTD/ASA (1) per stabilire il tunnel al peer FTD/ASA (2) non dispone dell'attributo EKU di autenticazione client. Di conseguenza, non è possibile stabilire il tunnel VPN perché il peer remoto, FTD/ASA (2), richiede che questo attributo sia presente nel certificato.

Topologia

Errori FTD o ASA CLI: sono gli errori osservati sull'FTD/ASA (2) durante l'autenticazione basata sul certificato IKEv2 quando rifiuta il certificato di identità FTD/ASA (1) privo dell'attributo EKU di autenticazione client.

<#root>

```
Apr 09 2026 15:59:50:

%ASA-3-717027: Certificate chain failed validation. Certi. Peer certificate key usage is invalid,

 subject name: CN=ASAv3.cisco.com,OU=IT,O=Cisco,C=US,unstructuredName=ASAv3.cisco.com.
Apr 09 2026 15:59:50:

%ASA-3-717027: Certificate chain failed validation. Certificate chain is either invalid or not authorize

Apr 09 2026 15:59:50: %ASA-3-751006: Local:10.3.3.6:500 Remote:10.3.3.5:500 Username:10.3.3.5

IKEv2 Certificate authentication failed.  Error: Certificate authentication failed

Apr 09 2026 15:59:50: %ASA-4-750003: Local:10.3.3.6:500 Remote:10.3.3.5:500 Username:10.3.3.5

IKEv2 Negotiation aborted due to ERROR: Auth exchange failed

Apr 09 2026 15:59:50: %ASA-4-752012: IKEv2 was unsuccessful at setting up a tunnel.  Map Tag = CMAP.  M
Apr 09 2026 15:59:50: %ASA-3-752015: Tunnel Manager has failed to establish an L2L SA.  All configured
Apr 09 2026 15:59:55: %ASA-5-752003: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2.  Map Ta
Apr 09 2026 15:59:55: %ASA-5-750001: Local:10.3.3.6:500 Remote:10.3.3.5:500 Username:Unknown IKEv2 Rece
```

Nota: Nell'esempio precedente, l'FTD/ASA (2) stava utilizzando un certificato di identità che includeva sia l'attributo EKU ClientAuth che ServerAuth.

Nota: Nell'esempio di cui sopra, l'FTD/ASA (2) può essere sostituito anche da un router o da un concentratore VPN fisico o basato su cloud di terze parti. In questo caso, lo stesso problema persiste, in quanto il peer VPN richiede che l'attributo EKU di autenticazione client sia presente nel certificato utilizzato dall'FTD o dall'ASA (1) per la riuscita dell'autenticazione basata su certificato.

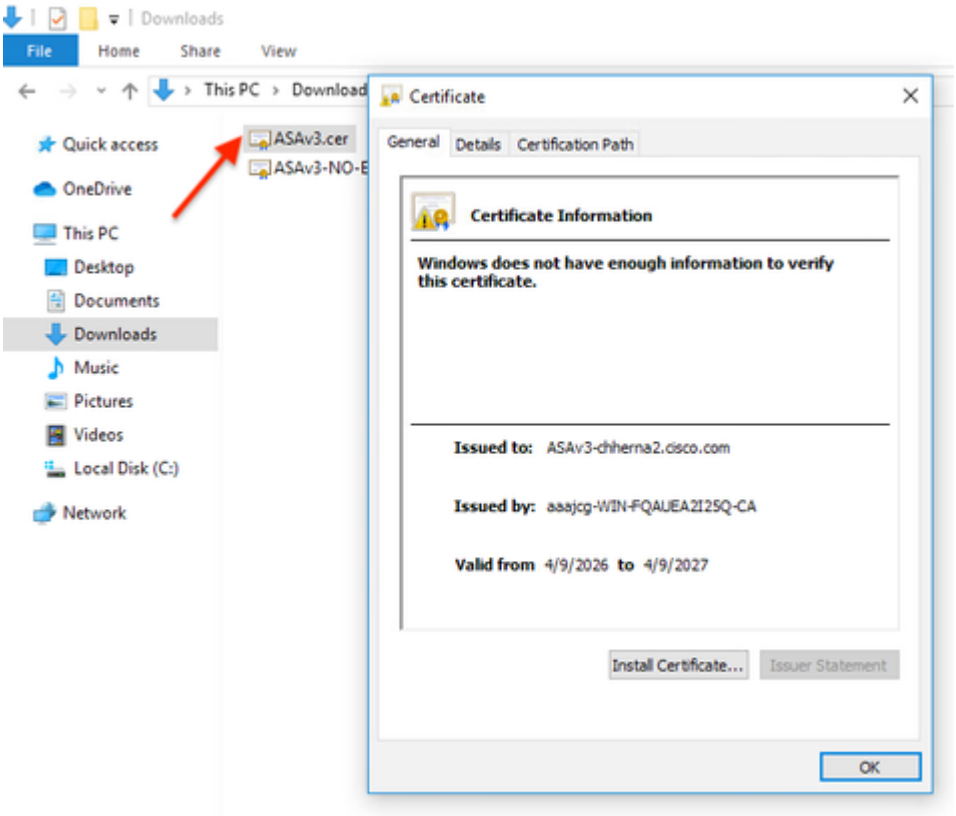
Soluzione: rivedere le informazioni proposte in questo documento per assicurarsi che FTD/ASA (1) utilizzi il certificato di identità corretto, incluso l'attributo EKU di autenticazione client, per un tunnel VPN da sito a sito con autenticazione basata su certificato.

Istruzioni per confermare se il certificato non dispone dell'attributo EKU di autenticazione client

Verificare gli attributi EKU da un certificato con estensione cer utilizzando Gestione certificati di Windows

Per verificare gli attributi EKU di un certificato con estensione cer tramite Gestione certificati di Windows, eseguire la procedura seguente:

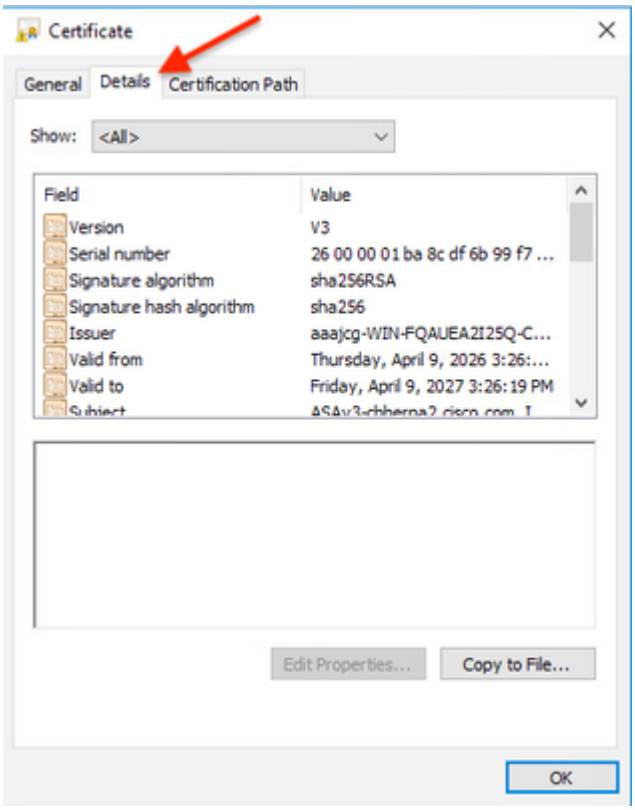
Passaggio 1. Fare doppio clic sul file con estensione cer per aprirlo in Gestione certificati di Windows.



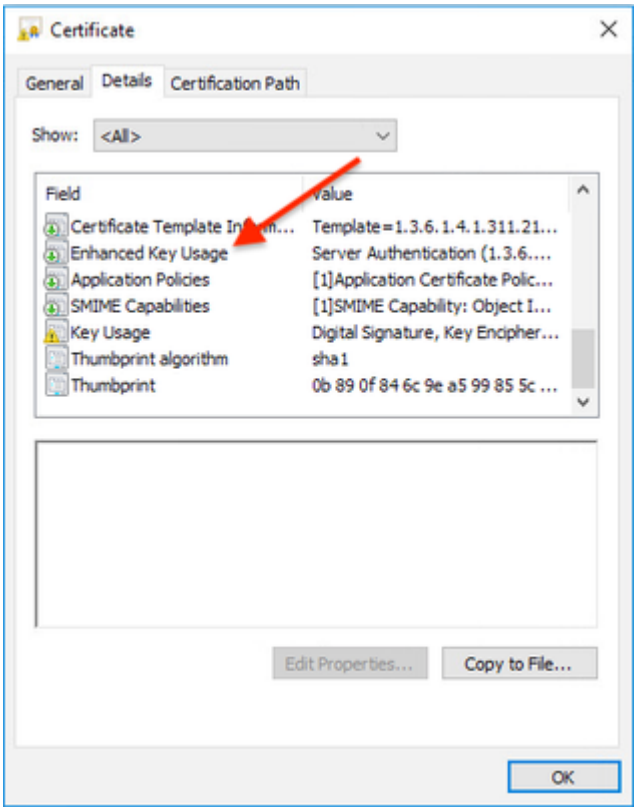
Nota: Solo i file con estensione cer verranno aperti direttamente in questo modo. se il certificato ha l'estensione pem, rinominarlo prima in cer o crt.

Passaggio 2. Gestire l'eventuale avviso di protezione. Se viene visualizzato un avviso di protezione, fare clic su Apri per continuare.

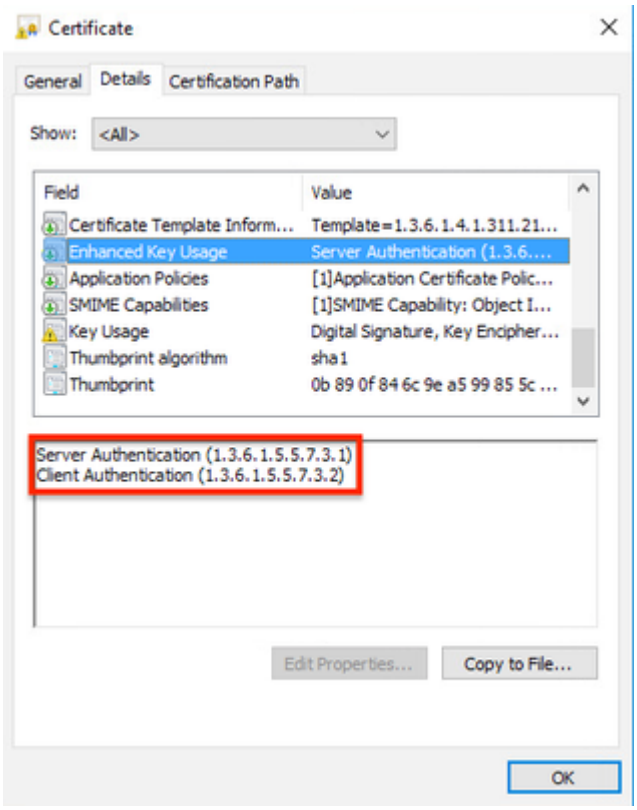
Passaggio 3. Nella finestra del certificato fare clic sulla scheda Dettagli.



Passaggio 4. Scorrere l'elenco dei campi e selezionare "Utilizzo chiave avanzato" (o Utilizzo chiave esteso).

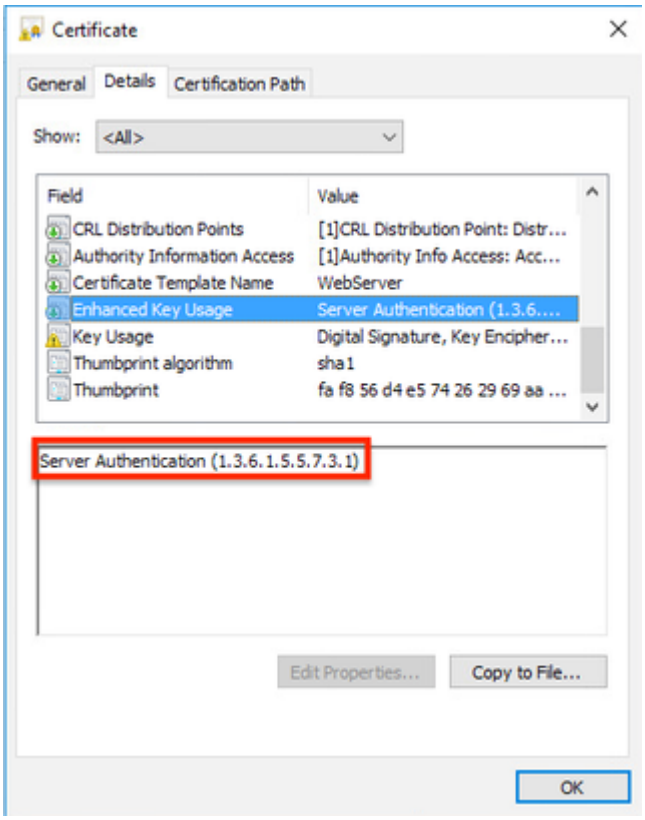


Passaggio 5. Verificare gli attributi EKU. È possibile che vengano visualizzate voci quali "Autenticazione server" e "Autenticazione client" che indicano i valori EKU presenti nel certificato.

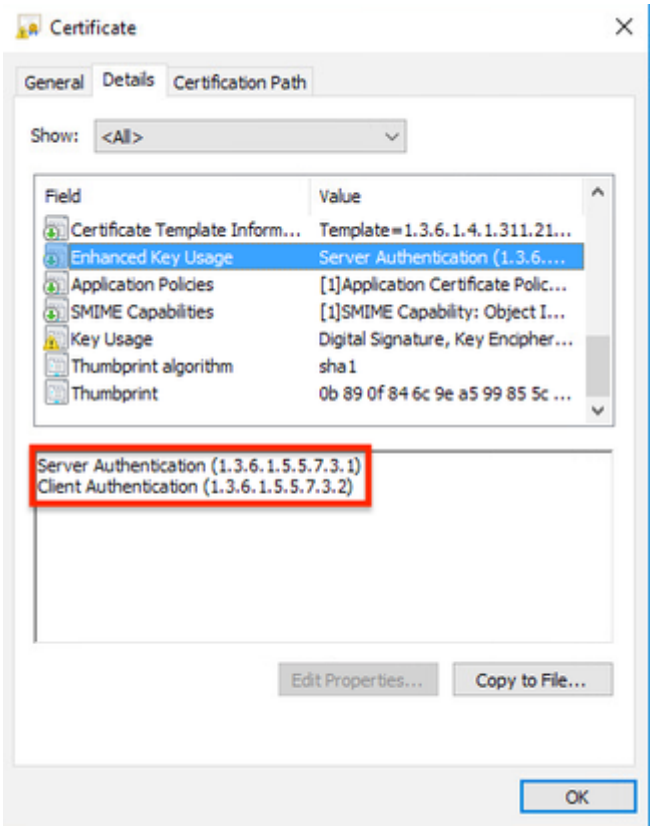


Passaggio 6. Dopo la verifica, scegliere OK per chiudere la finestra del certificato.

Esempio 1: Nel certificato con estensione cer manca l'attributo EKU di autenticazione client e viene incluso solo l'attributo EKU di autenticazione server.



Esempio 2: Questo certificato con estensione cer include gli attributi EKU di autenticazione server e client.



Verificare gli attributi EKU da un certificato PKCS#12, PEM e cer utilizzando OpenSSL

Per verificare gli attributi EKU da un certificato PKCS#12 (PKCS#12), PEM (PEM) e CER, eseguire la procedura seguente:

Passaggio 1. Individuare il certificato da controllare ed esportarlo in formato .p12 (PKCS#12), .pem (PEM) o .cer.

Per i certificati con estensione p12 (PKCS#12), utilizzare openssl per estrarre il certificato dal file con estensione p12 (PKCS#12). Il file .p12 (PKCS#12) può contenere la chiave privata, il certificato e i certificati CA.

Utilizzare il comando seguente per estrarre il certificato da un file con estensione p12 (PKCS#12) in un file con estensione pem (PEM) (senza la chiave privata o la catena di CA):

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

- fileutente.p12: Sostituire con il nome file effettivo.
- Potrebbe essere necessario immettere la password per il file .p12.
- cert.pem: Il certificato è estratto (senza la chiave privata o la catena di CA) in formato PEM.

Passaggio 2. Utilizzare i comandi openssl successivi per visualizzare i dettagli del certificato e gli attributi EKU.

a) Per i file .pem, usare il successivo comando openssl per visualizzare i dettagli del certificato e gli attributi EKU:

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

- cert.pem: Sostituire con il nome file effettivo.

b) Per i file con estensione cer, utilizzare il successivo comando openssl per visualizzare i dettagli del certificato e gli attributi EKU:

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

- file.cer: Sostituire con il nome file effettivo.

Passaggio 3. Quindi, cercare la sezione X509v3Extended Key Usage nell'output, è possibile che vengano visualizzate voci quali "Autenticazione server Web TLS" e "Autenticazione client Web TLS" che indicano i valori EKU presenti nel certificato.

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

OPPURE l'attributo EKU OIDs (Object Identifiers):

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

- OID EKU autenticazione server: 1.3.6.1.5.5.7.3.1
- OID EKU autenticazione client: 1.3.6.1.5.5.7.3.2

Esempio 1: Nel certificato PEM manca l'attributo EKU di autenticazione client e include solo l'attributo EKU di autenticazione server.

<#root>

```
MyHost$ openssl x509 -in cert.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            26:00:00:01:b7:e7:90:48:d6:f9:41:d3:54:00:01:00:00:01:b7
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=com, DC=aaajcg, CN=aaajcg-WIN-FQAUEA2I25Q-CA
        Validity
            Not Before: Mar 27 00:31:40 2026 GMT
            Not After : Mar 26 00:31:40 2028 GMT
        Subject: C=MX, ST=MX, L=MX, O=Cisco, OU=IT, CN=vFMC3-chherna2
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:cf:a8:a0:ff:dd:34:73:7d:46:86:85:05:b6:0c:
                    5e:32:8c:6f:6f:88:52:03:58:63:c6:89:d8:fc:55:
                    c5:58:ba:eb:45:88:b2:21:9e:c5:d8:67:57:39:0f:
                    91:a5:41:61:fa:94:b1:ad:9e:71:26:87:b6:30:ae:
                    a7:f6:89:b1:6d:61:ce:fa:47:7f:2a:d8:e8:4d:26:
                    4f:a7:d3:eb:5a:69:16:46:71:c7:55:cf:87:b4:10:
                    96:f2:10:6b:c0:a7:3d:3c:49:9d:ee:77:8c:b5:95:
                    9b:69:81:e0:2d:a0:6e:5c:78:73:22:5a:38:d0:74:
                    38:b2:ba:e0:ab:c5:44:eb:e1:3c:52:86:b8:2a:4e:
                    37:44:9c:34:d8:d8:6c:ae:3e:df:12:57:0e:28:52:
                    57:dc:6d:62:ea:b6:ec:19:4e:90:8f:3f:2c:23:1b:
                    e2:39:f0:ba:07:08:9a:0b:97:96:05:2e:69:fe:9a:
                    b2:b2:74:9a:ba:06:25:bc:38:1c:94:87:8e:2a:dc:
                    2f:0b:a6:31:6c:bf:11:96:2a:71:b3:87:e5:f5:cb:
                    88:f1:73:cf:88:d7:30:78:24:77:7c:b7:2c:7c:83:
                    6d:69:5b:bd:d4:21:b9:ee:19:c4:02:be:7b:44:a2:
                    55:d6:b2:95:11:46:bf:db:3e:4f:9a:8c:d4:ad:8d:
                    82:f5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                0D:8E:DA:07:6D:49:EA:51:D2:C7:EF:50:CE:CE:2B:8E:7C:DF:A6:8D
            X509v3 Authority Key Identifier:
                keyid:3A:45:60:22:F7:C8:2C:0D:D2:98:5A:BC:E0:98:D4:91:1D:67:32:22

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:ldap:///CN=aaajcg-WIN-FQAUEA2I25Q-CA,CN=WIN-FQAUEA2I25Q,CN=CDP,CN=Public%20Key%20

            Authority Information Access:
                CA Issuers - URI:ldap:///CN=aaajcg-WIN-FQAUEA2I25Q-CA,CN=AIA,CN=Public%20Key%20Services
```

```
            1.3.6.1.4.1.311.20.2:
                ...W.e.b.S.e.r.v.e.r
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
```

X509v3 Extended Key Usage:

```
        <-------- "EKU SECTION"
```

TLS Web Server Authentication

```
  <-------- "Server Authentication EKU Attribute Included"
    Signature Algorithm: sha256WithRSAEncryption
         2f:27:cd:95:7d:5c:40:fa:29:64:df:75:7d:7a:87:9b:b0:94:
         0e:6b:07:4d:d2:7e:83:da:03:08:f3:50:0d:5b:05:8c:1f:54:
         46:fe:53:f3:e2:d4:0a:ba:37:4f:cd:a4:49:04:74:79:09:23:
         d6:06:af:69:d2:7b:f5:bc:ec:fe:ce:e4:c9:07:31:d7:85:45:
         55:78:d3:42:45:f9:ce:cd:bf:43:53:b4:8e:4c:af:64:4b:a6:
         dc:47:d0:16:4e:73:62:fd:c8:5e:37:74:cb:68:48:29:7d:f9:
         41:b3:d1:46:56:24:83:23:5c:bd:b0:e3:7c:f9:8a:af:da:09:
         d0:c2:7d:4a:e6:24:0f:e6:fc:6e:0d:65:8c:96:8c:af:21:b2:
         7f:4b:bb:1c:17:33:b1:db:00:f3:12:e3:53:39:d0:e7:6a:48:
         4c:c6:4f:29:6f:74:ff:2d:a7:e5:ea:e8:89:fe:a4:2b:cd:e3:
         61:6a:9e:11:52:15:57:f2:b8:e8:fa:78:31:20:49:d9:50:f9:
         70:3f:1e:aa:9c:1a:bb:0b:59:66:1e:85:bd:76:e7:73:6f:ec:
         86:30:b0:dd:86:3c:b3:a0:7b:fb:b7:74:5d:38:88:82:3d:a3:
         2d:8c:a5:e4:db:37:eb:be:7f:62:bc:87:7c:35:17:32:fc:52:
         c5:d3:c5:8f
```

Esempio 2: Questo certificato PEM include sia gli attributi EKU di autenticazione client che quelli di autenticazione server.

<#root>

```
MyHost$ openssl x509 -in cert.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            26:00:00:01:b6:74:fc:b4:1e:99:be:7a:10:00:01:00:00:01:b6
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=com, DC=aaajcg, CN=aaajcg-WIN-FQAUEA2I25Q-CA
        Validity
            Not Before: Mar 26 23:44:58 2026 GMT
            Not After : Mar 26 23:44:58 2027 GMT
        Subject: C=MX, ST=AD, L=AD, O=Cisco, OU=IT, CN=vFMC3-chherna2
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
```

```
                    00:ab:aa:67:4e:55:19:3b:38:6c:33:2e:ba:fd:19:
                    56:e7:68:f8:f7:e9:53:95:1f:53:b4:f1:ce:94:c8:
                    ca:41:f1:52:15:eb:a5:35:9f:07:95:9f:c3:8a:5e:
                    62:d6:e1:5c:04:c5:c0:27:1c:84:ed:3d:1b:42:50:
                    91:4a:a6:86:90:e0:6e:26:7e:37:fd:17:0c:2f:bb:
                    fe:58:81:ec:3b:9d:0b:fc:dd:8c:6b:dd:ab:d3:96:
                    74:23:0d:78:d7:09:53:61:f9:b0:29:c6:7c:e2:9c:
                    2f:74:30:42:0f:45:47:cd:16:59:ed:53:62:8f:60:
                    75:f8:24:f5:1f:77:fb:89:85:4b:49:ad:93:43:04:
                    6e:4a:b3:59:fc:eb:75:70:39:67:71:60:be:b3:b7:
                    86:f7:c5:53:28:1e:bf:8f:b2:52:ec:79:d6:12:b0:
                    33:9c:6d:46:7a:9c:5d:53:a5:44:24:da:4b:36:7d:
                    c2:ec:61:d7:a0:01:c3:d2:bc:0a:df:a8:f6:0c:82:
                    48:30:fb:c6:3e:4a:48:a9:01:13:f5:4e:f2:03:24:
                    38:ee:aa:d9:60:78:30:45:ed:3b:76:16:fd:7a:d3:
                    b0:16:10:28:75:fc:41:32:e6:6d:cb:c3:96:58:77:
                    9e:11:0a:9b:33:c7:92:8d:75:1f:e5:30:29:a4:a5:
                    ba:7d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                D2:DF:62:25:17:DB:72:31:D8:D2:D0:41:CB:FB:DD:00:FF:38:BD:BB
            X509v3 Authority Key Identifier:
                keyid:3A:45:60:22:F7:C8:2C:0D:D2:98:5A:BC:E0:98:D4:91:1D:67:32:22

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:ldap:///CN=aaajcg-WIN-FQAUEA2I25Q-CA,CN=WIN-FQAUEA2I25Q,CN=CDP,CN=Public%20Key%20

            Authority Information Access:
                CA Issuers - URI:ldap:///CN=aaajcg-WIN-FQAUEA2I25Q-CA,CN=AIA,CN=Public%20Key%20Services

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            1.3.6.1.4.1.311.21.7:
                0-.%+.....7.....^..9...
...b.../ ...R...Z..d...


X509v3 Extended Key Usage:


         <-------- "EKU SECTION"


TLS Web Server Authentication, TLS Web Client Authentication


  <----- "Server & Client EKU Attributes Included"
            1.3.6.1.4.1.311.21.10:
                0.0
..+.......0
..+.......
            S/MIME Capabilities:
......0...+....0050...*.H..
..*.H..
    Signature Algorithm: sha256WithRSAEncryption
         3f:66:b1:35:7e:05:b4:69:f1:81:95:b8:18:90:f2:20:bd:8d:
         ff:03:5a:59:ca:02:ba:2d:1d:e0:8d:3f:63:e9:fe:71:3c:9a:
         11:15:5c:3b:fc:62:e4:cf:15:25:4c:74:5e:ad:3f:09:e9:3b:
         d5:08:95:7d:97:7a:ef:c1:16:6d:e0:7a:0b:21:81:46:bc:15:
```

```
c3:76:8c:fe:fb:14:94:36:92:0d:3b:4a:c9:8f:6a:bd:dc:4b:
0b:24:c3:32:35:27:e7:aa:23:95:85:e4:a9:64:71:f0:98:9e:
33:aa:6e:bd:7c:dd:dc:4b:cf:dd:0e:a7:ea:e8:aa:61:8f:67:
84:da:5b:be:8e:05:75:c8:eb:46:13:6f:14:4d:fe:4e:57:3c:
29:27:cc:0b:5b:25:87:37:24:12:79:b1:c3:78:c8:94:fe:df:
3c:77:aa:fc:f2:ee:ae:9b:ab:88:29:f9:ee:04:c2:48:5f:21:
9e:1c:25:cc:c9:c5:9c:23:8f:af:87:76:5e:46:74:ac:73:57:
01:ba:71:ae:46:e1:87:3c:94:6c:19:f7:fe:8e:66:9d:c7:1f:
b0:87:4b:65:e2:fc:d6:10:7c:44:57:56:5d:68:bb:df:f0:36:
0e:07:c5:8a:be:56:86:97:3d:a7:1c:8b:86:df:0b:51:b5:97:
cc:67:09:8e
```

Soluzioni

Gli amministratori possono scegliere una delle seguenti opzioni di soluzione.

Opzione 1. Passare a CA radice pubbliche che forniscono certificati EKU combinati

Alcune CA radice pubbliche, ad esempio DigiCert e IdenTrust, emettono certificati con tipi EKU combinati (certificati server e client) da una radice alternativa, che potrebbe non essere inclusa nell'archivio radice Chrome. Coordinarsi con il provider della CA per verificare la disponibilità di tali certificati e, prima di distribuirli, verificare che sia il server che presenta il certificato che i client che lo utilizzano considerino attendibile la CA radice corrispondente.

Questo approccio riduce la necessità di aggiornare il software del server per ridurre il sunsetting dell'EKU di autenticazione client imposto dai criteri del programma radice Chrome.

La tabella seguente, che mostra esempi di CA radice pubbliche e di tipi EKU, non è un elenco esaustivo ed è solo a scopo illustrativo.

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
AffidabilitàIden	Autenticazione client	CA radice settore pubblico IdenTrust 1	TrustID RSA ClientAuth CA 2
AffidabilitàIden	serverAuth (attendibile per il browser)	CA 1 radice commerciale IdenTrust	Server HydrantID CA O1
DigiCert	autenticazione client + autenticazione server	DigiCert Assured ID Root G2	DigiCert Assured ID CA G2
DigiCert	Autenticazione client	DigiCert Assured ID Root G2	DigiCert Assured ID Client CA G2
DigiCert	serverAuth (attendibile per il	DigiCert Global Root G2	DigiCert Global G2 TLS

Fornitore CA	Tipo EKU	CA radice	Emittente/CA secondaria
	browser)		RSA SHA256

Opzione 2. Rinnovare i certificati attuali per estenderne la validità

I certificati emessi da CA radice pubbliche prima di maggio 2026 che dispongono di EKU di autenticazione server e client continueranno a essere rispettati fino alla scadenza. Tuttavia, è consigliabile rinnovare i certificati EKU combinati prima che si verifichi il sunsetting dei criteri.

- La politica e le date di implementazione delle CA pubbliche possono variare a seconda del fornitore.
- Verificare con l'autorità di certificazione e pianificare il rinnovo del certificato di conseguenza.
- Dopo il 15 marzo 2026, i certificati emessi dalla CA pubblica sono validi solo per 200 giorni.
- Tenere presente che alcune CA pubbliche hanno smesso di rilasciare certificati EKU combinati.

Opzione 3. Eseguire la migrazione a PKI privata per rilasciare certificati EKU (server e client) combinati

Valutare la fattibilità della transizione a un'infrastruttura a chiave pubblica privata (PKI) e quindi configurare una CA privata per rilasciare certificati singoli con EKU combinati (certificati server e client con gli EKU richiesti).

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.

Opzione 4. Ottenere un certificato di attendibilità pubblica con solo l'utilizzo chiavi avanzato per l'autenticazione client

Alcune CA, ad esempio SSL.com, offrono certificati di autenticazione client dedicati. Tali certificati sono distinti dai certificati TLS e vengono in genere utilizzati per l'autenticazione Enterprise.

⚠ Attenzione: Per gli ambienti di produzione, si consiglia di utilizzare i certificati con gli attributi EKU appropriati. Questa pratica garantisce sicurezza, compatibilità e conformità agli standard e alle procedure ottimali del settore. I certificati senza attributi EKU devono essere considerati solo come una soluzione temporanea e solo con una chiara comprensione dei rischi associati.

Domande frequenti (FAQ)

Q1. Devo preoccuparmi di questo se uso una PKI privata?

R: Il criterio applicato dalle CA private è determinato da ciascuna organizzazione. Se la CA privata adotta gli stessi criteri di rilascio, ad esempio la rimozione dell'attributo EKU di autenticazione client dai certificati, sono applicabili le linee guida fornite in questo documento.

D2. È possibile continuare a utilizzare i certificati esistenti?

A: Sì, è possibile utilizzare certificati validi con EKU combinato fino alla relativa scadenza.

D3. Quali opzioni sono disponibili per l'integrazione di FMC o FDM con ISE tramite pxGrid se il certificato installato in FMC/FDM non dispone dell'attributo EKU di autenticazione client?

A: Oltre alle soluzioni proposte nel presente documento, si consiglia di controllare le seguenti referenze ISE:

- Field Notice: FN74392 - Cisco Identity Services Engine: Impatto sulle comunicazioni protette dalle modifiche all'EKU di autenticazione client CA pubbliche a partire da maggio 2026 - Soluzione fornita

- Prepara Identity Services Engine per le restrizioni estese all'utilizzo delle chiavi nei certificati rilasciati dalle autorità di certificazione pubbliche

---

Nota: Anche se l'utilizzo di un certificato firmato dalla CA pubblica è supportato per IMS. Cisco consiglia di utilizzare il certificato CA interno ISE, in quanto questa comunicazione è valida solo per le transazioni interne.

D4. Che cos'è l'utilizzo chiavi avanzato di autenticazione client e perché è incluso nel certificato?

R: L'utilizzo chiavi avanzato "Autenticazione client" indica che un certificato può essere utilizzato da un client per l'autenticazione a un server. Per impostazione predefinita, alcune CA lo includevano nei certificati TLS, ma non lo richiedevano per la normale sicurezza del sito Web.

D5. Il certificato TLS corrente riporta "Autenticazione client" nell'utilizzo esteso della chiave. Non è più valido?

R: No, resta valido. Non è necessario sostituirlo immediatamente. Al momento del rinnovo, il nuovo certificato non includerà l'EKU clientAuth.

D6. Come è possibile verificare se un certificato dispone dell'utilizzo chiavi avanzato clientAuth?

A: È possibile esaminare i dettagli del certificato utilizzando gli strumenti OpenSSL, PowerShell o GUI per verificare la presenza dell'estensione Extended Key Usage.

D7. È ancora possibile ottenere un certificato con attendibilità pubblica solo con l'utilizzo chiavi avanzato per l'autenticazione client?

A: Alcune CA, ad esempio SSL.com, offrono certificati di autenticazione client dedicati. Tali certificati sono distinti dai certificati TLS e vengono in genere utilizzati per l'autenticazione Enterprise.

D8. Ciò influisce su altri EKU o tipi di certificati (firma del codice, e-mail, ecc.)?

A: No, questa modifica è specifica dei certificati server TLS. La firma del codice e i certificati di posta elettronica hanno requisiti EKU specifici.

Q9. Dove posso vedere i requisiti ufficiali relativi a questa modifica?

A: Il Google Chrome Root Program Policy fornisce linee guida sul divieto dell'EKU clientAuth nei certificati server TLS.

Q10. È sicuro utilizzare certificati senza attributi EKU client e server nell'ambiente di produzione?

R. Per gli ambienti di produzione, è consigliabile che i clienti utilizzino i certificati con gli attributi EKU appropriati. Questa pratica garantisce sicurezza, compatibilità e conformità agli standard e alle procedure ottimali del settore. I certificati senza attributi EKU devono essere considerati solo come una soluzione temporanea e solo con una chiara comprensione dei rischi associati.

Informazioni correlate

- Per ulteriore assistenza, contattare il Cisco Technical Assistance Center (TAC). È necessario un contratto di supporto valido: Contatti del supporto Cisco internazionali.
- Supporto e download Cisco: Supporto tecnico Cisco e download

Bug correlati

- CSCwt94492 ITA: FMC deve convalidare la presenza dell'attributo EKU di autenticazione client nel certificato client utilizzato per l'integrazione pxGrid
- CSCwt94509 ITA: FMC deve visualizzare un messaggio che indica che l'attributo EKU di autenticazione client è obbligatorio nel certificato client utilizzato per l'integrazione di pxGrid
- CSCwt61767 May 2026 EKU Server-Only Change - Invia un avviso di configurazione ASA se l'EKU non è adeguato
- CSCws83036 EKU: Valutazione dell'impatto dell'applicazione dell'EKU ClientAuth in ISE

Cisco ISE References

- Field Notice: FN74392 - Cisco Identity Services Engine: Impatto sulle comunicazioni protette dalle modifiche all'EKU di autenticazione client CA pubbliche a partire da maggio 2026 - Soluzione fornita
- Prepara Identity Services Engine per le restrizioni estese all'utilizzo delle chiavi nei certificati rilasciati dalle autorità di certificazione pubbliche

Riferimenti esterni

- Criterio programma radice riquadro
- Portale IdenTrust
- SSL - Rimozione dell'utilizzo chiavi avanzato di autenticazione client dai certificati server TLS - Informazioni necessarie

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).