Cisco Secure Firewall Impact of the Public CA Client Authentication EKU Wijzigingen vanaf mei 2026 voor beveiligde communicatie

Inleiding

Dit document beschrijft de impact van de beperkingen op de criteria voor de afgifte van certificaten die zijn opgelegd door certificaatautoriteiten die voldoen aan het Chrome Root Certificate-programma, met name omdat ze betrekking hebben op de Cisco Secure Firewall-producten.

Achtergrondinformatie

Publiek vertrouwde TLS-certificaten worden uitgegeven door CA's die moeten voldoen aan het industriebeleid dat de uitgifte en het gebruik van certificaten regelt.

Het Chrome Root Program Policy, beheerd door Google, definieert de vereisten waaraan CA's moeten voldoen om hun certificaten te laten vertrouwen door de Google Chrome-browser. Deze vereisten hebben invloed op de manier waarop publiek betrouwbare certificaten worden uitgegeven in de hele branche. Als onderdeel van de zich ontwikkelende beveiligingspraktijken introduceert het Chrome Root Program strengere richtlijnen voor het gebruik van certificaten.

Veel publieke CA's zijn daarom bezig met het afgeven van certificaten die Client Authentication EKU bevatten en gaan over op het uitgeven van certificaten die alleen bedoeld zijn voor serververificatie. Als gevolg hiervan wordt verwacht dat nieuw uitgegeven certificaten van veel openbare CA's alleen Server Authentication EKU bevatten.

De Extended Key Usage (EKU), is een certificaatuitbreiding die de beoogde functie van een publieke sleutel binnen een digitaal certificaat definieert. Het stelt een gestructureerde set van toegestane toepassingen vast, zodat de sleutel alleen wordt gebruikt voor specifieke cryptografische bewerkingen. Deze functionaliteit wordt beheerd door Object Identifiers (OID's) - unieke numerieke identificatoren die elk toegestaan gebruik categoriseren, zoals codeondertekening, serververificatie, clientverificatie of beveiligde e-mail.

Wanneer verificatie op basis van certificaten plaatsvindt, controleert de controlerende entiteit de cert om de Object Identifier (OID) binnen de EKU te identificeren. Door de EKU-extensie in te sluiten, beperkt een certificeringsinstantie (CA) de reikwijdte van het certificaat tot vooraf gedefinieerde rollen, waarbij elk aangewezen doel expliciet is toegewezen

aan een OID.

Doel van EKU-attributen

· Gebruik definiëren: EKU-kenmerken verduidelijken welke soorten verificatie of codering het certificaat mag uitvoeren.

· Verbeterde beveiliging: door certificaten te beperken tot specifieke toepassingen, helpt EKU misbruik of onbedoelde toepassingen te voorkomen (een servercertificaat kan bijvoorbeeld niet worden gebruikt voor clientverificatie).

· Compliance: zorgt ervoor dat certificaten worden gebruikt in overeenstemming met het beveiligingsbeleid en industriestandaarden.

Belangrijkste toepassingen van EKU Attributen

1. TLS Web Client-verificatie

· Certificaten kunnen worden gebruikt voor het identificeren en verifiëren van gebruikers of apparaten op een server.

· OID: 1.3.6.1.5.5.7.3.2

· Gebruikt in VPN's, wederzijdse TLS en veilige aanmeldingsscenario's.

2. TLS-webserververificatie

· Vergunningcertificaten die door servers worden gebruikt om hun identiteit aan klanten te bewijzen.

· OID: 1.3.6.1.5.5.7.3.1

· Gebruikt in HTTPS, SSL/TLS webservers en beveiligde API-eindpunten.

3. Ondertekening van de code

· Geeft aan dat het certificaat kan worden gebruikt om software of uitvoerbare bestanden te ondertekenen.

· OID: 1.3.6.1.5.5.7.3.3

· Gebruikt bij softwaredistributie en integriteitscontroles.

4. E-mailbeveiliging

· Hiermee kunnen certificaten worden gebruikt voor het ondertekenen en coderen van e-mailberichten.

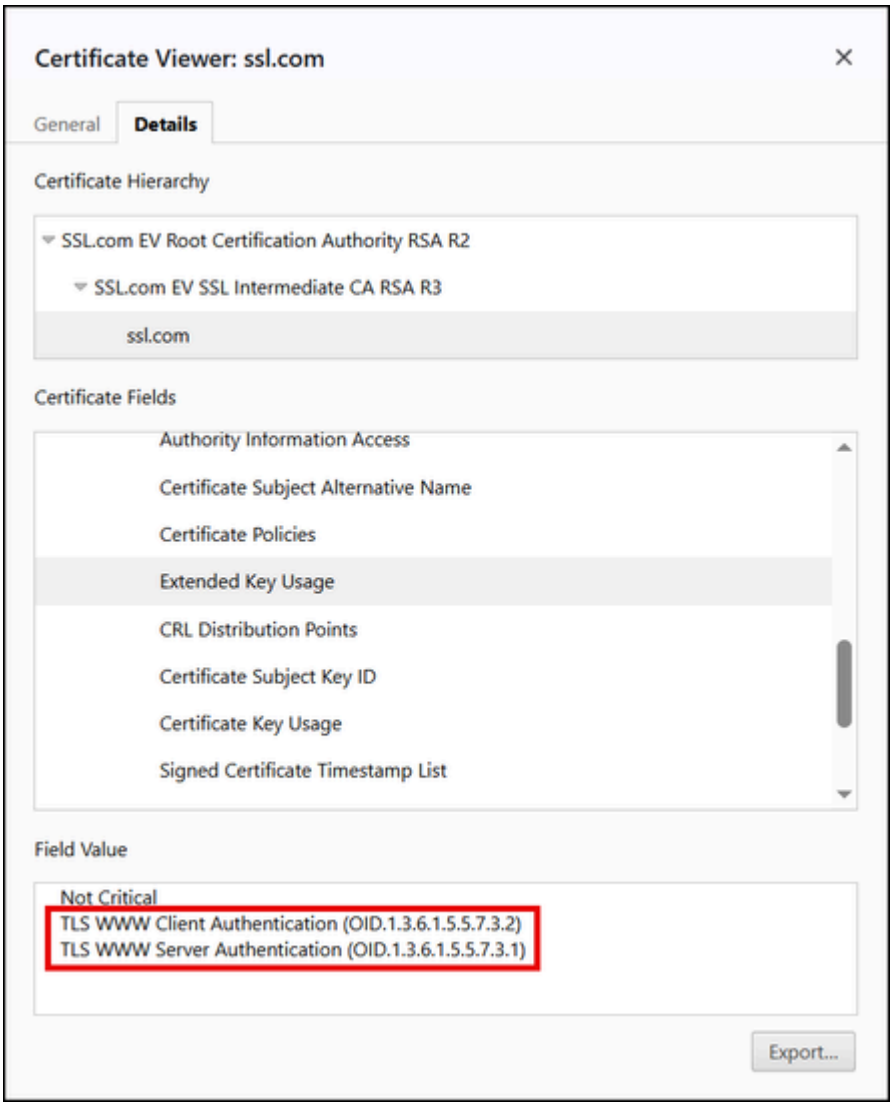
· OID: 1.3.6.1.5.5.7.3.4

· Gebruikt in S/MIME e-mailbeveiliging.

5. ANDERE DOELEINDEN

· Ondertekening van documenten, tijdstempeling, aanmelding bij smartcard, enz., elk met hun eigen OID's.

Browsers en servers hebben alleen de serverAuth EKU nodig om een beveiligde verbinding voor HTTPS tot stand te brengen, maar historisch gezien bevatten veel TLS-servercertificaten zowel de serverAuth als clientAuth EKU's, hieronder is een voorbeeld van een dergelijk certificaat:



Waarom de verwijdering van de Client Authentication EKU van server certs?

- Beveiliging en reikwijdte: openbare TLS-certificaten worden alleen verondersteld om servers op het web te verifiëren. De verwijdering zorgt voor een duidelijke scheiding tussen server- en clientfunctionaliteit. De ClientAuth EKU wordt gebruikt voor authenticatie van machines en gebruikers met Mutual TLS (mTLS) en andere authenticatiescenario's.

- Misconfiguratie voorkomen: Sommige systemen vertrouwen mogelijk elk certificaat van een openbare CA voor clientverificatie als de EKU aanwezig is, wat een beveiligingsrisico kan vormen.

- Browservereisten: grote browsers vereisen of controleren de clientAuth EKU niet in het certificaat van een website.

- Vereenvoudigde PKI-architectuur: door gebruik van elkaar te scheiden, kunnen CA's afzonderlijke certificathiërarchieën voor TLS-servers en andere doeleinden handhaven.

Dit is met name belangrijk voor producten zoals de Cisco Secure Firewall Adaptive Security Appliance (ASA), de Cisco Secure Firewall Threat Defense (FTD), de Cisco Secure Firewall Device Manager (FDM) en het Cisco Secure Firewall Management Center (FMC) die kunnen fungeren als server of client tijdens de TLS-verificatie, afhankelijk van het gebruiksscenario.

Impact op serveromgevingen

Voor de overgrote meerderheid van de serverimplementaties zal deze wijziging weinig of geen impact hebben. Dit is wat je kunt verwachten:

- Standaard webservers (HTTPS): geen impact. De bijgewerkte certificaten blijven normaal functioneren.

- Bestaande certificaten: elk certificaat dat is afgegeven voordat de afsnijding is verlopen, blijft functioneren totdat het is verlopen.

- Mutual TLS (mTLS) en Client Cert Scenarios: Als u een TLS-servercertificaat gebruikt voor clientverificatie, moet u een afzonderlijk certificaat verkrijgen met de clientAuth EKU van een andere bron.

- Bedrijfssystemen waarvoor beide EKU's nodig zijn: sommige bestaande of bedrijfssystemen verwachtten beide EKU's. Controleer of er updates nodig zijn om aan de nieuwe regels te voldoen.

Probleembeschrijving

Vanaf mei 2026 zullen veel openbare certificaatautoriteiten (CA's) stoppen met het uitgeven van TLS-certificaten (Transport Layer Security) die de EKU (Client Authentication Extended Key Usage) bevatten. Nieuw uitgegeven certificaten bevatten doorgaans alleen serververificatie-EKU.

Als certificaten die zijn uitgegeven door een openbare certificeringsinstantie worden verlengd onder het bijgewerkte CA-beleid en vervolgens worden geïmplementeerd in de Cisco Secure Firewall Products, zullen services waarvoor Client Authentication EKU is vereist, mislukken. De specifieke diensten die worden beïnvloed zijn de volgende:

- Wanneer de ASA, FTD, FDM of FMC als client optreedt, bijvoorbeeld wanneer verbinding wordt gemaakt met identiteitsproviders of verificatieservers zoals ISE (pxGrid), RADIUS, LDAPS of Active Directory, kan op certificaten gebaseerde verificatie mislukken als het clientcertificaat is gegenereerd door een openbare CA en de Client Authentication EKU ontbreekt. In deze scenario's kunnen verbindingsfouten optreden als de verificatieserver certificaten afwijst zonder de vereiste EKU.

- De Cisco Secure Client (voorheen AnyConnect) kan met behulp van certificaten worden geverifieerd op ASA- of FTD-servers. Als het clientcertificaat echter is gegenereerd door een openbare CA en de Client Authentication EKU ontbreekt, mislukt de verbinding met Remote Access VPN (RAVPN).

- Wanneer de FTD of ASA een site-to-site VPN-tunnel tot stand brengt - of het nu gaat om een andere FTD, ASA, Cisco-router of een VPN-peer van een derde partij - met behulp van certificaatverificatie (RSA of ECDSA), zal de tunnel mislukken als het identiteitscertificaat dat is gegenereerd door een openbare CA het EKU-kenmerk voor clientverificatie mist. Dit gebeurt omdat de externe VPN-peer vereist dat de Client Authentication EKU aanwezig is in het identiteitscertificaat.

Wijziging van het rootprogramma van Chrome

De tenuitvoerlegging van de EKU hangt af van de ondertekening van het certificaat door de bevoegde autoriteit. Het gebruik van zowel Server Authentication als Client Authentication EKU was een gangbare praktijk. Als onderdeel van het Chrome Root Program Policy Change stoppen CA's die zich afstemmen op deze criteria voor de afgifte van certificaten echter met het ondertekenen van TLS-certificaten die de EKU (Client Authentication Extended Key Usage) bevatten. Nieuw uitgegeven certificaten bevatten alleen serververificatie EKU.

Belangrijkste beleidsvereisten

- Public Root CA's moeten EKU (Extended Key Usage) ALLEEN voor serververificatie (id-kp-serverAuth) bevestigen

- Certificaten moeten ALLEEN serververificatie EKU bevatten.

- Het opnemen van Client Authentication EKU in deze certificaten is verboden

- Root-CA's die certificaten blijven uitgeven met Client Authentication EKU worden uiteindelijk verwijderd uit de Chrome Root Store, waardoor dergelijke certificaten als 'Niet vertrouwd' door de Chrome-browser worden gemarkeerd

tijdlijnen

- In september 2025 zal SSL.com TLS-certificaten uitgeven die alleen de ServerAuth EKU bevatten (en niet ClientAuth) voor servercertificaten. Met andere woorden, nieuwe SSL/TLS-certificaten voor uw website of server zijn alleen expliciet bedoeld voor "serververificatie".

- Oktober 2025: CA's die zich afstemden op het programma (bijv. DigiCert, Sectigo, enzovoort) begonnen standaard certificaten voor alleen servers uit te geven.

- Mei 2026: CA's die zich afstemmen op het programma, geven geen EKU-certificaten voor clientverificatie meer uit

- Maart 2027: Chrome Root Program Policy wordt volledig effectief

Gevolgen voor Cisco Secure Firewall-producten

Nadat de openbare CA's zijn gestart met het opnemen van alleen de EKU voor serververificatie in de uitgegeven certificaten. Dit kan de volgende impact hebben op de volgende Cisco Secure Firewall-productscenario's:

- Wanneer de ASA, FTD, FDM of FMC als client optreedt, bijvoorbeeld wanneer verbinding wordt gemaakt met identiteitsproviders of verificatieservers zoals ISE (pxGrid), RADIUS, LDAPS of Active Directory, kan op certificaten gebaseerde verificatie mislukken als het clientcertificaat is gegenereerd door een openbare CA en de Client Authentication EKU ontbreekt. In deze scenario's kunnen verbindingsfouten optreden als de verificatieserver certificaten afwijst zonder de vereiste EKU.

- De Cisco Secure Client (voorheen AnyConnect) kan met behulp van certificaten worden geverifieerd op ASA- of FTD-servers. Als het clientcertificaat echter is gegenereerd door een openbare CA en de Client Authentication EKU ontbreekt, mislukt de verbinding met Remote Access VPN (RAVPN).

- Wanneer de FTD of ASA een site-to-site VPN-tunnel tot stand brengt - of het nu gaat om een andere FTD, ASA,

Cisco-router of een VPN-peer van een derde partij - met behulp van certificaatverificatie (RSA of ECDSA), zal de tunnel mislukken als het identiteitscertificaat dat is gegenereerd door een openbare CA het EKU-kenmerk voor clientverificatie mist. Dit gebeurt omdat de externe VPN-peer vereist dat de Client Authentication EKU aanwezig is in het identiteitscertificaat.

Opmerking: Als u FMC of FDM integreert met ISE via pxGrid en de certificaten die op uw FMC/FDM zijn geïnstalleerd, het EKU-kenmerk voor clientverificatie missen, bekijkt u de tijdelijke oplossingen die in dit document worden voorgesteld en de volgende ISE-referenties: FN74392 en Prepare Identity Services Engine for Extended Key Usage Restrictions in Certificates Issued by Public Certification Authorities.

Opmerking: Het verwijderen van de clientAuth EKU van TLS-servercertificaten is een beleidswijziging in de hele branche die de beveiliging verbetert en misbruik voorkomt. Voor de meeste gebruikers zal er geen merkbare impact zijn. Als u echter vertrouwt op de ClientAuth EKU, moet u proactieve stappen ondernemen om het juiste type certificaat voor uw behoeften te verkrijgen.

Betrokken producten

Cisco Secure Firewall-product	Softwareversie	Geïmpacteerde scenario's	sanering
FTD	Alle versies	Wanneer een client als client fungeert, bijvoorbeeld wanneer verbinding wordt gemaakt met identiteitsproviders of verificatieservers zoals ISE (pxGrid), RADIUS, LDAPS of Active Directory, kan op certificaten gebaseerde verificatie mislukken als het clientcertificaat is gegenereerd door een openbare CA en de Client Authentication EKU ontbreekt. In dit scenario kunnen verbindingsfouten optreden als de verificatieserver certificaten afwijst	Optie 1. Als u een TLS-servercertificaat gebruikt voor clientverificatie, moet u een certificaat verkrijgen bij de ClientAuth EKU van een andere bron. OF Optie 2. Switch naar publieke root-CA's (Certificate Authorities) die gecombineerde EKU-certificaten (ClientAuth en ServerAuth) leveren.
FDM	Alle versies		
FMC	Alle versies		
ASA	Alle versies		

		zonder de vereiste EKU.	OPMERKING: Raadpleeg het gedeelte Oplossingen van dit document voor aanvullende opties.
Cisco Secure Client (voorheen AnyConnect)	Alle versies	De Cisco Secure Client kan met behulp van certificaten worden geverifieerd op de ASA- of FTD-servers. Als het clientcertificaat echter is gegenereerd door een openbare CA en de Client Authentication EKU ontbreekt, mislukt de Remote Access VPN (RAVPN)-verbinding.	
FTD of ASA	Alle versies	Wanneer de FTD of ASA een site-to-site VPN-tunnel tot stand brengt - of dit nu naar een andere FTD, ASA, Cisco-router of een VPN-peer van een derde partij gaat - met behulp van certificaatverificatie (RSA of ECDSA), zal de VPN-tunnel mislukken als het identiteitscertificaat dat door een openbare CA is gegenereerd, het EKU-kenmerk voor clientverificatie mist. Dit gebeurt omdat de externe VPN-peer vereist dat de Client Authentication EKU aanwezig is in het identiteitscertificaat.	

Opmerking: Als u FMC of FDM integreert met ISE via pxGrid en de certificaten die op uw FMC/FDM zijn geïnstalleerd, het EKU-kenmerk voor clientverificatie missen, bekijkt u de tijdelijke oplossingen die in dit document worden voorgesteld en de volgende ISE-referenties: FN74392 en Prepare Identity Services Engine for Extended Key Usage Restrictions in Certificates Issued by Public Certification Authorities.

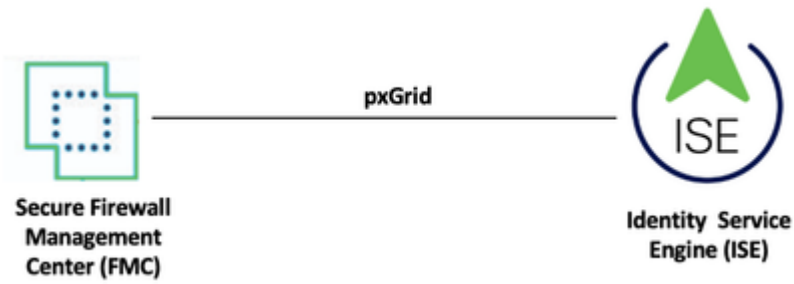
Opmerking: Het verwijderen van de clientAuth EKU van TLS-servercertificaten is een beleidswijziging in de hele branche die de beveiliging verbetert en misbruik voorkomt. Voor de meeste gebruikers zal er geen merkbare impact zijn. Als u echter vertrouwt op de ClientAuth EKU, moet u proactieve stappen ondernemen om het juiste type certificaat voor uw behoeften te verkrijgen.

Let op: Voor productieomgevingen wordt het sterk aanbevolen dat klanten certificaten gebruiken met de juiste EKU-kenmerken. Deze praktijk zorgt voor veiligheid, compatibiliteit en naleving van industriestandaarden en best practices. Certificaten zonder EKU-kenmerken mogen alleen worden beschouwd als een tijdelijke tijdelijke oplossing en alleen met een duidelijk inzicht in de bijbehorende risico's.

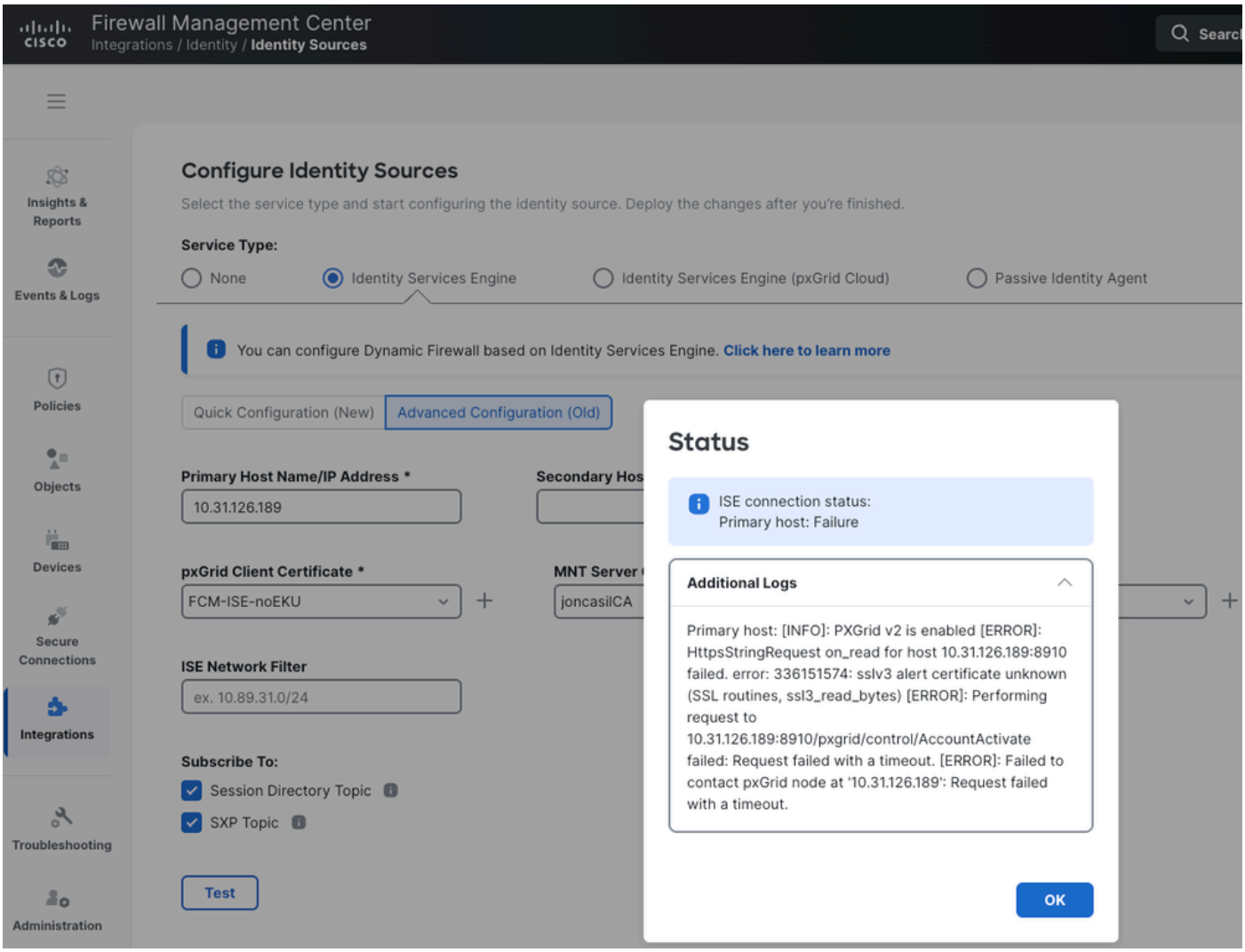
Probleem 1. pxGrid-integratieprobleem tussen FMC en ISE, wanneer het FMC-certificaat het EKU-kenmerk voor clientverificatie mist

In dit scenario mist het certificaat dat door de FMC wordt gebruikt voor de integratie van pxGrid met ISE het EKU-kenmerk voor clientverificatie. Als gevolg hiervan mislukt de pxGrid-integratie omdat de ISE-server verwacht dat dit kenmerk aanwezig is in het certificaat dat door de FMC wordt gepresenteerd.

Topologie



FMC UI-fouten: Dit is de foutmelding die wordt weergegeven in de FMC wanneer het certificaat dat door de FMC wordt gebruikt, het EKU-kenmerk voor clientverificatie mist voor de integratie van pxGrid met ISE.



FMC CLI-fouten: Dezelfde foutmeldingen zijn te vinden in de map FMC /var/log/messages.

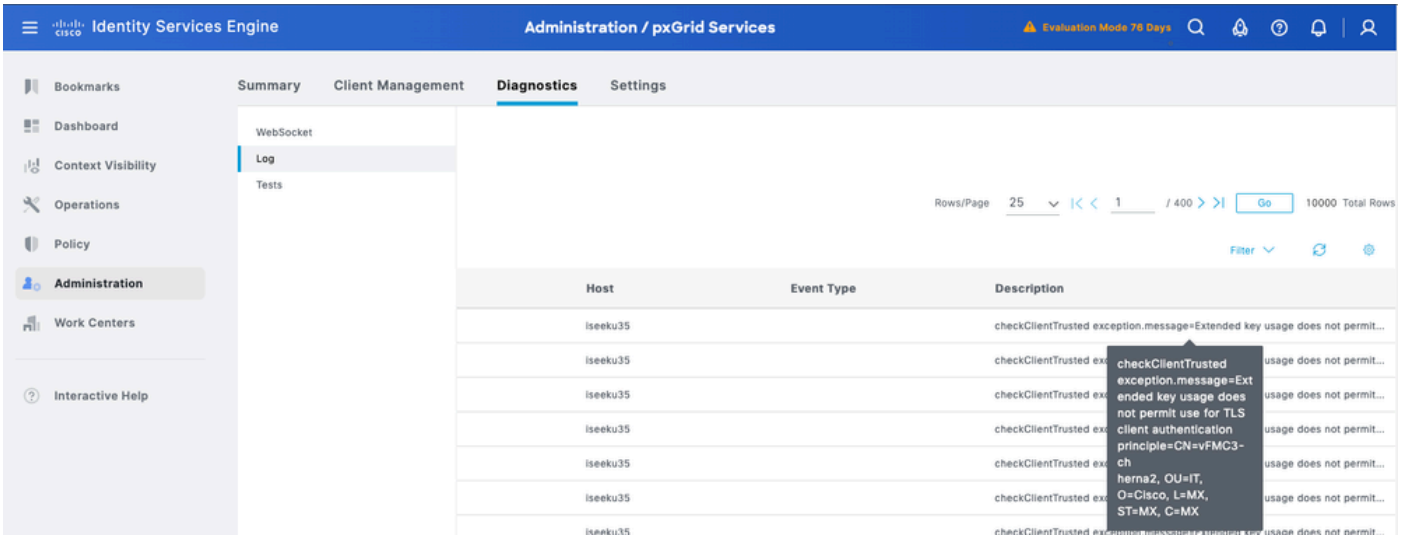
<#root>

```
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
```

ISE-fout: dit is de foutmelding die wordt weergegeven in ISE, "checkClientTrusted exception.message=Extended key use does not allow use for TLS client authentication principle=CN=vFMC3-chherna2, OU=IT, O=Cisco, L=MX, ST=MX, C=MX".



Oplossing: Als u FMC of FDM integreert met ISE via pxGrid en het certificaat dat in uw FMC/FDM is geïnstalleerd, het EKU-kenmerk voor clientverificatie mist, bekijkt u de voorgestelde opties in dit document en de volgende ISE-referenties: FN74392 en bereidt de engine voor identiteitsservices voor uitgebreide belangrijke gebruiksbeperkingen voor in certificaten uitgegeven door openbare certificeringsinstanties voor een succesvolle pxGrid-integratie.

Opmerking: het FMC pxGrid-clientcertificaat moet het ClientAuth EKU-kenmerk bevatten of helemaal geen Client- of Server EKU-kenmerken bevatten.

Opmerking: Hoewel het gebruik van een door een openbare certificeringsinstantie ondertekend certificaat wordt ondersteund voor IMS. Cisco raadt aan het ISE Internal CA-certificaat te gebruiken, omdat deze communicatie alleen voor interne transacties is.

Probleem 2. FTD- of ASA-integratieprobleem met een LDAPS-server, wanneer het gepresenteerde certificaat het EKU-kenmerk voor clientverificatie mist

In dit scenario fungeert de FTD of ASA als een client om te integreren met een LDAPS-server met behulp van certificaatverificatie. Als het certificaat dat door de FTD of ASA wordt gebruikt, het EKU-kenmerk voor clientverificatie mist, mislukt de integratie omdat de LDAPS-server vereist dat dit kenmerk in het certificaat aanwezig is.

Topologie

LDAPS-serverfouten: 'TLS-certificaatverificatie: fout, niet-ondersteund certificaatdoel' en 'TLS-trace: SSL3-waarschuwing schrijven: fataal: niet-ondersteund certificaat'

```
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
```

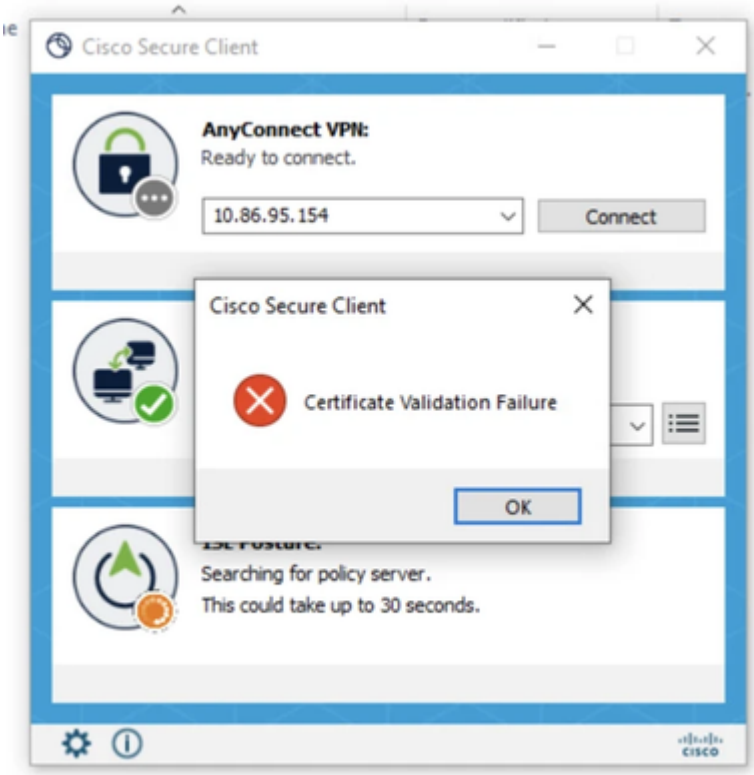
Oplossing: bekijk de in dit document voorgestelde gegevens om ervoor te zorgen dat de FTD of ASA het juiste identiteitscertificaat gebruikt, inclusief het EKU-kenmerk voor clientverificatie, voor een succesvolle op certificaten gebaseerde verificatie met de LDAPS-server.

Probleem 3. Cisco Secure Client (voorheen AnyConnect) kan verbindingsproblemen ondervinden met een FTD of ASA als het clientcertificaat het EKU-kenmerk voor clientverificatie mist

In dit scenario gebruikt de Cisco Secure Client certificaatverificatie om een RAVPN-tunnel naar de FTD of ASA tot stand te brengen. Als het clientcertificaat echter het EKU-kenmerk voor clientverificatie mist, zal de RAVPN-sessie mislukken omdat de ASA of FTD vereist dat dit kenmerk aanwezig is in het clientcertificaat.

Topologie

Cisco Secure Client-fout: 'Fout bij certificaatvalidatie'



Cisco Secure Client DART-fouten: De volgende logs uit het bestand AnyConnectVPN.txt in de DART-bundel bevestigen dat de Cisco Secure Client het certificaat dat wordt gebruikt voor de RAVPN-certificaatgebaseerde verificatie heeft afgewezen voor de FTD/ASA vanwege de afwezigheid van het attribuut Client Authentication EKU (om het bestand AnyConnectVPN.txt in de DART-bundel te

vinden, gaat u naar Cisco Secure Client > AnyConnect VPN > Logs > 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]

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

Oplossing: controleer de opties die in dit document worden voorgesteld om ervoor te zorgen dat de Cisco Secure Client het juiste certificaat gebruikt, inclusief het EKU-kenmerk voor clientverificatie, voor een succesvolle op certificaten gebaseerde verificatie met de FTD of ASA.

Opmerking: Van de bovenstaande DART-bundelfout 'EKU niet gevonden in certificaat: 1.3.6.1.5.5.7.3.2', komt dit nummer '1.3.6.1.5.5.7.3.2' overeen met de Client Authentication EKU OID.

Probleem 4. Site-to-site VPN-tunnels met op certificaten gebaseerde verificatie mislukken als het identiteitscertificaat het EKU-kenmerk voor clientverificatie mist

In dit scenario, dat een op certificaten gebaseerde authenticatie voor een IKEv2 site-to-site VPN-tunnel omvat, ontbreekt het identiteitscertificaat dat door FTD/ASA (1) wordt gebruikt om de tunnel naar de FTD/ASA (2)-peer tot stand te brengen, het EKU-kenmerk voor clientverificatie. Als gevolg hiervan kan de VPN-tunnel niet worden ingesteld omdat de externe peer, FTD / ASA (2), vereist dat dit kenmerk aanwezig is in het certificaat.

Topologie

FTD- of ASA-CLI-fouten: Dit zijn de fouten die zijn waargenomen op de FTD/ASA (2) tijdens de IKEv2-certificaatgebaseerde authenticatie wanneer deze het FTD/ASA (1)-identiteitscertificaat afwijst dat het EKU-kenmerk voor clientverificatie mist.

<#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
```

Opmerking: In het bovenstaande voorbeeld gebruikte de FTD/ASA (2) een identiteitscertificaat dat zowel de ClientAuth- als ServerAuth EKU-kenmerken bevatte.

Opmerking: In het bovenstaande voorbeeld kan de FTD/ASA (2) ook worden vervangen door een router of een fysieke of cloud-gebaseerde VPN-concentrator van derden. Vervolgens zal hetzelfde probleem blijven bestaan, omdat de VPN-peer vereist dat het EKU-attribuut voor clientverificatie aanwezig is in het certificaat dat door de FTD / ASA (1) wordt gebruikt voor succesvolle op certificaten gebaseerde verificatie.

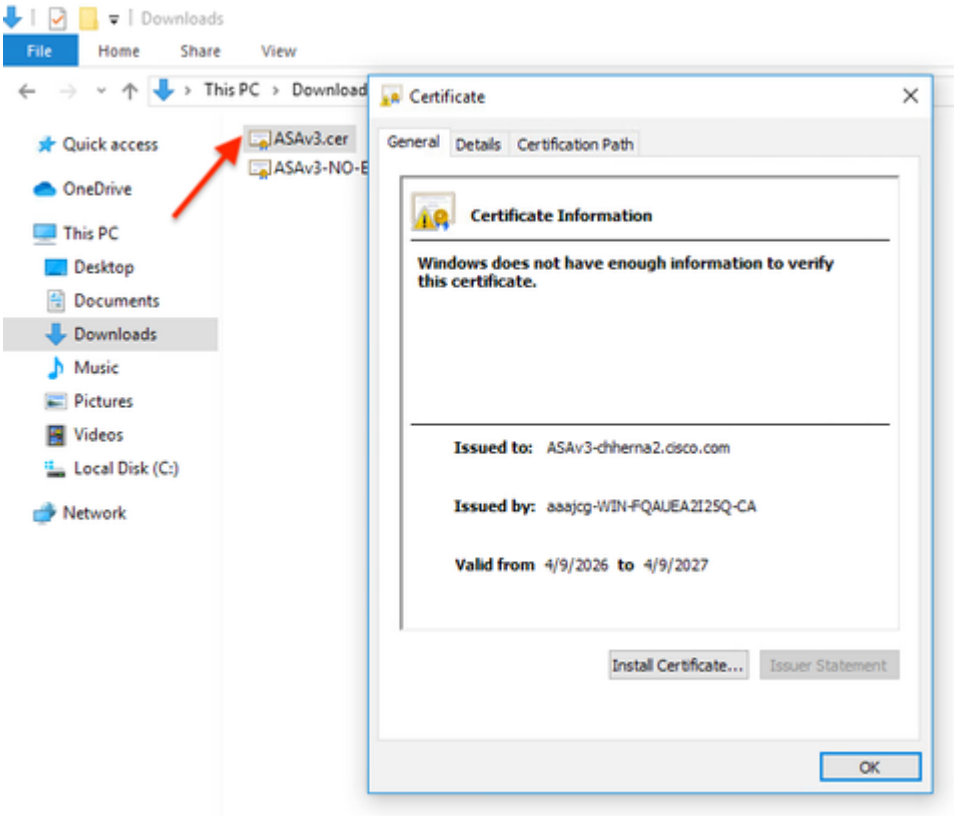
Oplossing: bekijk de in dit document voorgestelde gegevens om ervoor te zorgen dat FTD/ASA (1) het juiste identiteitscertificaat gebruikt, inclusief het EKU-kenmerk voor clientverificatie, voor een succesvolle site-to-site VPN-tunnel met op certificaten gebaseerde verificatie.

Instructies om te bevestigen of uw certificaat het EKU-kenmerk voor clientverificatie mist

Verifieer de EKU-kenmerken van een .cer-certificaat met behulp van Windows Certificate Manager

Volg de volgende stappen om de EKU-kenmerken van een .cer-certificaat te verifiëren met behulp van Windows Certificate Manager:

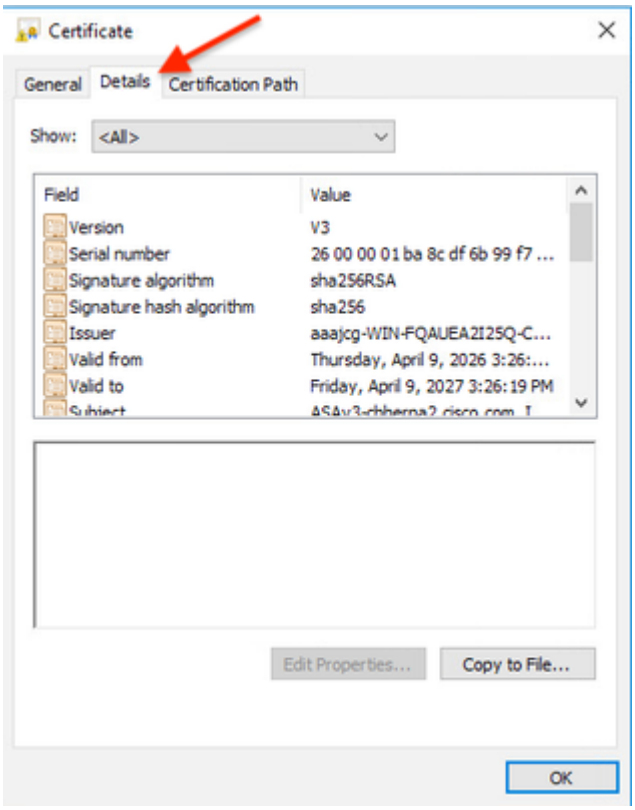
Stap 1. Dubbelklik op het .cer-bestand om het te openen in Windows Certificate Manager.



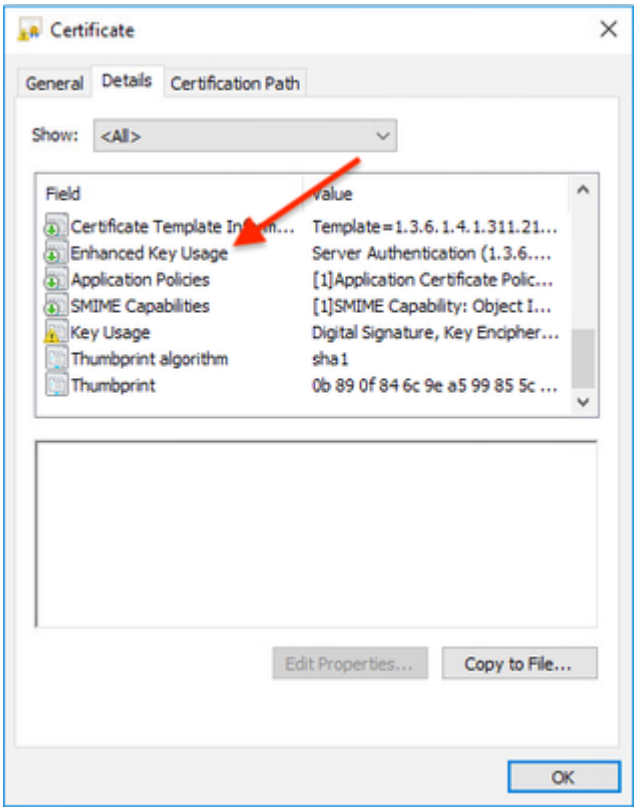
Opmerking: Alleen .cer-bestanden worden direct op deze manier geopend; als uw certificaat een .pem-extensie heeft, wijzigt u de naam eerst in .cer of .crt.

Stap 2. Veiligheidswaarschuwing afhandelen (indien aanwezig). Klik op Openen om door te gaan als er een beveiligingswaarschuwing verschijnt.

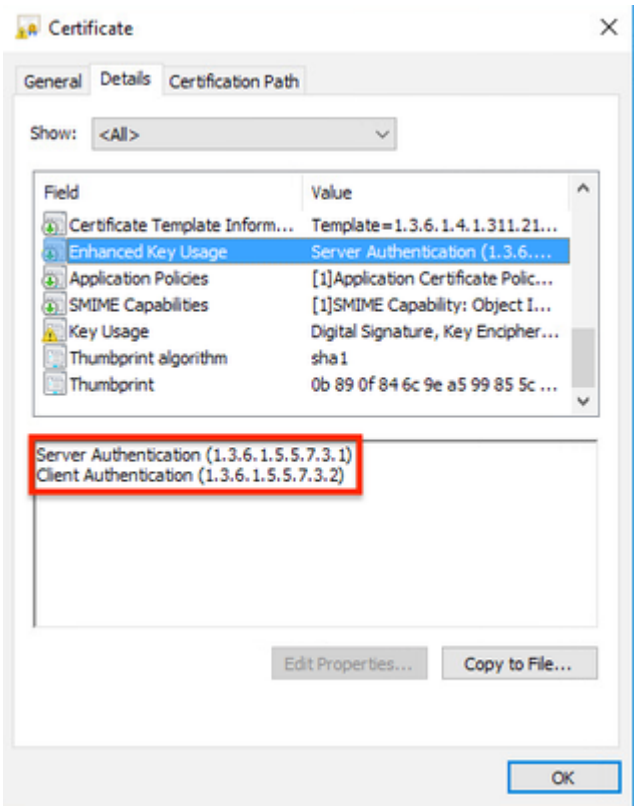
Stap 3. Klik in het certificaatvenster op het tabblad Details.



Stap 4. Blader door de lijst met velden en selecteer "Enhanced Key Usage" (of Extended Key Usage).

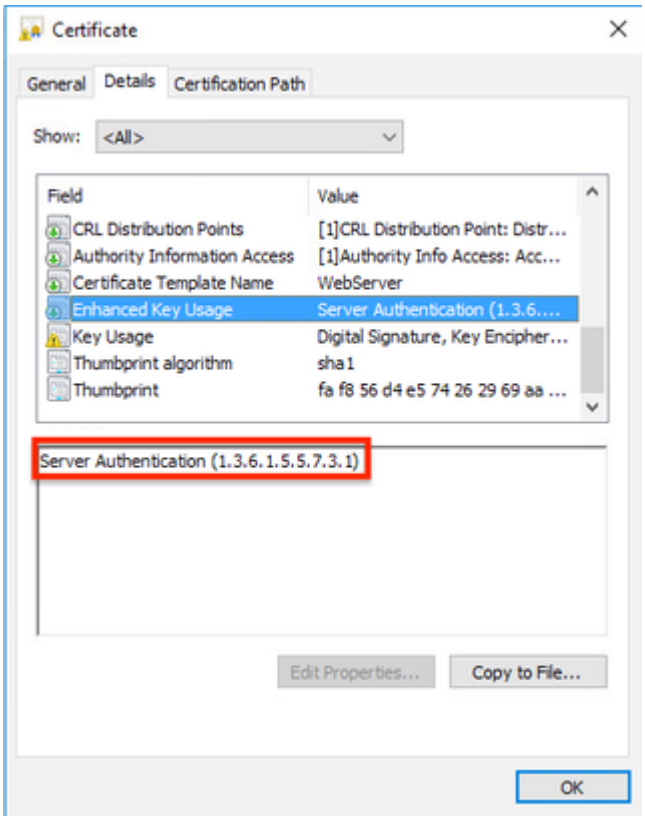


Stap 5. Als u de EKU-kenmerken verifieert, ziet u mogelijk vermeldingen zoals "Serververificatie" en "Clientverificatie" die de EKU-waarden in het certificaat aangeven.

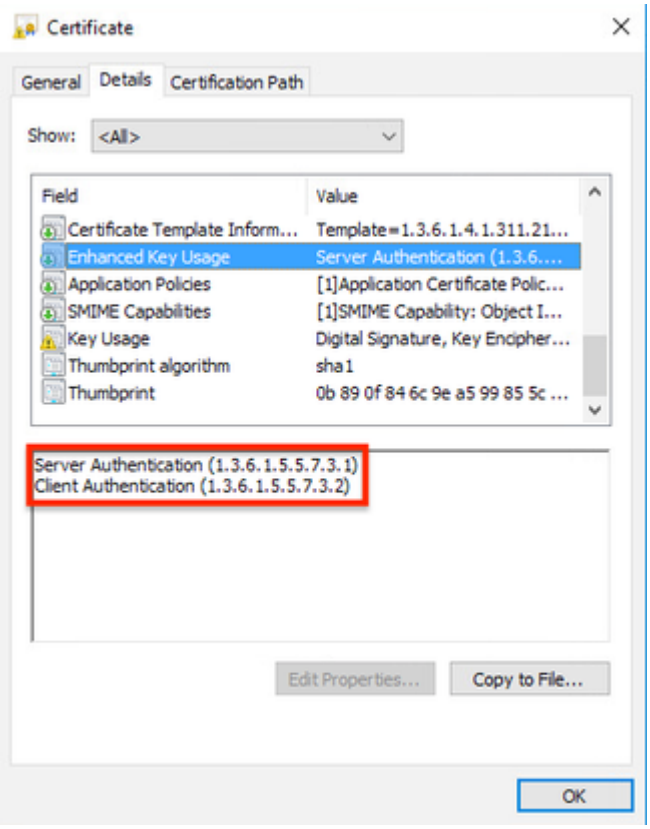


Stap 6. Klik na verificatie op OK om het certificaatvenster te sluiten.

Voorbeeld 1: Dit .cer-certificaat mist het EKU-kenmerk voor clientverificatie en bevat alleen het EKU-kenmerk voor serververificatie.



Voorbeeld 2: Dit .cer-certificaat bevat zowel de EKU-kenmerken voor server- als clientverificatie.



Verifieer de EKU-kenmerken van een PKCS#12-, PEM- en .cer-certificaat met OpenSSL

Volg de volgende stappen om de EKU-kenmerken te verifiëren van een .p12 (PKCS#12), .pem (PEM) en .cer-certificaat:

Stap 1. Zoek het certificaat dat u moet controleren en exporteer het in .p12 (PKCS # 12), .pem (PEM) of .cer-indeling.

Voor .p12 (PKCS#12) certificaten, gebruik openssl om het certificaat uit het .p12 (PKCS#12) bestand te halen, het .p12 (PKCS#12) bestand kan de private key, certificaat en CA certificaten bevatten.

Gebruik de volgende opdracht om het certificaat uit een .p12 (PKCS#12) -bestand te extraheren naar een .pem (PEM) -bestand (zonder de privésleutel of CA-keten):

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

- your file.p12: Vervang uw huidige bestandsnaam.
- Mogelijk moet u het wachtwoord voor het .p12-bestand invoeren.
- cert.pem: Wordt het certificaat geëxtraheerd (zonder de private sleutel of CA-keten) in .pem (PEM) formaat.

Stap 2. Gebruik de volgende openssl-opdrachten om de certificaatdetails en EKU-kenmerken weer te geven.

a) Gebruik voor .pem-bestanden de volgende opdracht openssl om de certificaatdetails en EKU-kenmerken weer te geven:

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

- cert.pem: Vervang door uw werkelijke bestandsnaam.

b) Gebruik voor .cer-bestanden de volgende opdracht openssl om de certificaatdetails en EKU-kenmerken weer te geven:

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

- your file.cer: Vervang door uw werkelijke bestandsnaam.

Stap 3. Zoek vervolgens naar de sectie X509v3Extended Key Usage in de uitvoer, mogelijk ziet u vermeldingen zoals "TLS Web Server Authentication" en "TLS Web Client Authentication" die de EKU-waarden aangeven die in het certificaat aanwezig zijn.

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

OF het EKU-kenmerk OID's (Object Identifiers):

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

- Serververificatie EKU OID: 1.3.6.1.5.5.7.3.1
- Client Authentication EKU OID: 1.3.6.1.5.5.7.3.2

Voorbeeld 1: Dit .pem (PEM)-certificaat mist het EKU-kenmerk voor clientverificatie en bevat alleen het EKU-kenmerk voor serververificatie.

<#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
```

Voorbeeld 2: Dit .pem-certificaat (PEM) bevat zowel de EKU-attributen voor client- als serververificatie.

<#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
```

tijdelijke oplossingen

Beheerders kunnen kiezen uit een van de volgende opties.

Optie 1. Switch aan publieke root-CA's die gecombineerde EKU-certificaten leveren

Sommige publieke root-CA's, zoals DigiCert en IdenTrust, geven certificaten uit met gecombineerde EKU-typen (server- en clientcertificaten) van een alternatieve root, die mogelijk niet zijn opgenomen in de Chrome Root Store. Coördineren met de CA-provider om de beschikbaarheid van dergelijke certificaten te controleren en ervoor te zorgen dat zowel de server die het certificaat presenteert als de clients die het gebruiken, vertrouwen op de corresponderende root-CA voordat ze worden geïmplementeerd.

Deze aanpak maakt het minder nodig om serversoftware te upgraden om het onderbreken van Client Authentication EKU te beperken, zoals wordt afgedwongen door het Chrome Root Program Policy.

De volgende tabel, die voorbeelden van public root CA's en EKU-typen toont, is geen uitputtende lijst en dient alleen ter illustratie.

CA-leverancier	EKU-type	Root CA	Uitgevende instantie/subinstantie
IdenTrust	clientAuth + serverAuth	IDenTrust-basisoplossing voor de publieke sector CA 1	IDenTrust Public Sector Server CA 1
IdenTrust	clientAuth	IDenTrust-basisoplossing voor de publieke sector CA 1	TrustID RSA ClientAuth CA 2
IdenTrust	serverAuth (vertrouwde browser)	IdenTrust Commercial Root CA 1	HydrantID Server CA O1
DigiCert	clientAuth + serverAuth	DigiCert Assured ID Root G2	DigiCert verzekerde ID CA G2

CA-leverancier	EKU-type	Root CA	Uitgevende instantie/subinstantie
DigiCert	clientAuth	DigiCert Assured ID Root G2	DigiCert Assured ID Client CA G2
DigiCert	serverAuth (vertrouwde browser)	DigiCert Global Root G2	DigiCert Global G2 TLS RSA SHA256

Optie 2. Huidige certificaten verlengen om hun geldigheid te verlengen

Certificaten die vóór mei 2026 zijn uitgegeven door publieke root-CA's en die zowel server- als clientverificatie-EKU hebben, blijven worden gehonoreerd totdat hun termijn afloopt. Het is echter het beste om gecombineerde EKU-certificaten te vernieuwen voordat het beleid vervalt.

- Openbaar CA-beleid en implementatiedata kunnen per leverancier verschillen.
- Neem contact op met de certificeringsinstantie en plan de verlenging van het certificaat dienovereenkomstig.
- Na 15 maart 2026 zijn openbare CA-uitgegeven certificaten slechts 200 dagen geldig.
- Houd er rekening mee dat sommige openbare CA's zijn gestopt met het uitgeven van gecombineerde EKU-certificaten.

Optie 3. Migreren naar private PKI om gecombineerde EKU-certificaten (server en client) uit te geven

Evalueer de haalbaarheid van de overstap naar een Private Public Key Infrastructure (PKI) en stel vervolgens een private CA in om enkelvoudige certificaten uit te geven met gecombineerde EKU (server- en clientcertificaten met de vereiste EKU's).

Voordat u een certificaat afgeeft of implementeert, moet u ervoor zorgen dat zowel de server die het certificaat presenteert als alle clients die het certificaat gebruiken, vertrouwen op de corresponderende root-CA.

Optie 4. Krijg een openbaar vertrouwd certificaat met alleen Client Authentication EKU

Sommige CA's, zoals SSL.com, bieden speciale clientverificatiecertificaten. Deze staan los van TLS-certificaten en worden doorgaans gebruikt voor bedrijfsverificatie.

⚠ Let op: Voor productieomgevingen wordt het sterk aanbevolen dat klanten certificaten gebruiken met de juiste

⚠ EKU-kenmerken. Deze praktijk zorgt voor veiligheid, compatibiliteit en naleving van industriestandaarden en best practices. Certificaten zonder EKU-kenmerken mogen alleen worden beschouwd als een tijdelijke tijdelijke oplossing en alleen met een duidelijk inzicht in de bijbehorende risico's.

Veelgestelde vragen (FAQ)

V1. Moet ik me hier zorgen over maken als ik een privé-PKI gebruik?

A: Het beleid dat wordt afgedwongen door particuliere CA's wordt bepaald door elke organisatie. Als uw particuliere certificeringsinstantie dezelfde uitgiftecriteria hanteert, zoals het verwijderen van het EKU-kenmerk voor clientverificatie van certificaten, zijn de richtlijnen in dit document van toepassing.

V2. Kan ik mijn bestaande certificaten blijven gebruiken?

A: Ja, geldige certificaten met gecombineerde EKU kunnen worden gebruikt tot de vervaltijd.

V3. Welke opties zijn beschikbaar voor de integratie van mijn FMC of FDM met ISE via pxGrid als het certificaat dat op de FMC/FDM is geïnstalleerd, het EKU-kenmerk voor clientverificatie mist?

A: Naast de oplossingen die in dit document worden voorgesteld, raden we u ten zeerste aan de volgende ISE-referenties te controleren:

- Kennisgeving ter plaatse: FN74392 - Cisco Identity Services Engine: impact op beveiligde communicatie van openbare CA-clientverificatie EKU-wijzigingen vanaf mei 2026 - Aangeboden oplossing
- De Identity Services Engine voorbereiden op uitgebreide beperkingen voor sleutelgebruik in certificaten die zijn uitgegeven door openbare certificeringsinstanties

✎ Opmerking: Hoewel het gebruik van een door een openbare certificeringsinstantie ondertekend certificaat wordt ondersteund voor IMS. Cisco raadt aan het ISE Internal CA-certificaat te gebruiken, omdat deze communicatie alleen voor interne transacties is.

V4. Wat is de "Client Authentication" EKU en waarom stond het in mijn certificaat?

A: De "Client Authentication" EKU geeft aan dat een certificaat kan worden gebruikt door een

client om te authenticeren naar een server. Sommige CA's namen het in het verleden standaard op in TLS-certificaten, maar het was nooit vereist voor normale websitebeveiliging.

V5. Mijn huidige TLS-certificaat zegt "Client Authentication" onder zijn Extended Key Usage. Is het nu ongeldig?

A: Nee, het blijft geldig. Je hoeft het niet onmiddellijk te vervangen. Wanneer u verlengt, bevat het nieuwe certificaat eenvoudigweg niet de clientAuth EKU.

V6. Hoe kan ik controleren of een certificaat de clientAuth EKU heeft?

A: U kunt de certificaatgegevens inspecteren met behulp van OpenSSL-, PowerShell- of GUI-tools om te controleren op de extensie Extended Key Usage.

V7. Kan ik nog steeds een openbaar vertrouwd certificaat krijgen met alleen Client Authentication EKU?

A: Sommige CA's, zoals SSL.com, bieden speciale clientverificatiecertificaten. Deze staan los van TLS-certificaten en worden doorgaans gebruikt voor bedrijfsverificatie.

V8. Heeft dit invloed op andere EKU's of certificaattypen (codeondertekening, e-mail, enz.)?

A: Nee, deze wijziging is specifiek voor TLS-servercertificaten. Codeondertekening en e-mailcertificaten hebben hun eigen EKU-vereisten.

V9. Waar kan ik de officiële vereisten over deze wijziging zien?

A: Het Google Chrome Root Program Policy bevat richtlijnen voor het verbieden van de clientAuth EKU in TLS-servercertificaten.

V10. Is het veilig om certificaten te gebruiken zonder Client en Server EKU attributen in mijn productieomgeving?

A: Voor productieomgevingen wordt het sterk aanbevolen dat klanten certificaten gebruiken met de juiste EKU-kenmerken. Deze praktijk zorgt voor veiligheid, compatibiliteit en naleving van industriestandaarden en best practices. Certificaten zonder EKU-kenmerken mogen alleen worden beschouwd als een tijdelijke tijdelijke oplossing en alleen met een duidelijk inzicht in de bijbehorende risico's.

Gerelateerde informatie

- Neem voor meer hulp contact op met het Cisco Technical Assistance Centre (TAC). Een geldig supportcontract is vereist: Cisco Worldwide Support Contacts.
- Cisco Support & Downloads: Cisco Technical Support & Downloads

Gerelateerde bugs

- CSCwt94492 ENH: FMC moet aanwezigheid van EKU-attribuut voor clientverificatie valideren in het clientcertificaat dat wordt gebruikt voor integratie van pxGrid
- CSCwt94509 ENH: FMC moet een bericht weergeven dat het EKU-kenmerk voor clientverificatie vereist is in het clientcertificaat dat wordt gebruikt voor pxGrid-integratie
- CSCwt61767 mei 2026 Wijziging alleen EKU-server - Probleem met een configuratiewaarschuwing als EKU niet voldoet
- CSCws83036 EKU: Effectbeoordeling van ClientAuth EKU-handhaving in ISE

Cisco ISE-referenties

- Kennisgeving ter plaatse: FN74392 - Cisco Identity Services Engine: impact op beveiligde communicatie van openbare CA-clientverificatie EKU-wijzigingen vanaf mei 2026 - Aangeboden oplossing
- De Identity Services Engine voorbereiden op uitgebreide beperkingen voor sleutelgebruik in certificaten die zijn uitgegeven door openbare certificeringsinstanties

Externe verwijzingen

- Chrome Root Program-beleid
- IdenTrust-portal

- SSL - Verwijdering van de Client Authentication EKU van TLS Server Certificates - Wat u moet weten

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.