Cisco ISE voorbereiden voor Client Auth EKU Sunset in openbare CA-certificaten

Inhoud

Inleiding

Dit document beschrijft de impact op ISE-services als gevolg van aankomende wijzigingen in TLS-certificaten die zijn uitgegeven door openbare certificaatautoriteiten met Client Authentication EKU.

Achtergrondinformatie

Digitale certificaten zijn elektronische referenties die worden uitgegeven door vertrouwde certificeringsinstanties (CA's) die de communicatie tussen servers en clients beveiligen door authenticatie, gegevensintegriteit en vertrouwelijkheid te waarborgen. Deze certificaten bevatten EKU-velden (Extended Key Usage) die hun doel definiëren:

- Server Authentication EKU (id-kp-serverAuth): Gebruikt wanneer een server zijn certificaat presenteert om zijn identiteit te bewijzen
- Client Authentication EKU (id-kp-clientAuth): Gebruikt in wederzijdse TLS (mTLS) verbindingen waar beide partijen elkaar authenticeren

Traditioneel kan een enkel certificaat zowel server- als clientverificatie-EKU's bevatten, waardoor het voor twee doeleinden kan worden gebruikt. Dit is vooral belangrijk voor producten zoals Cisco ISE die zowel als server als client fungeren in verschillende verbindingsscenario's.

probleemdefinitie

Wijziging van het rootprogramma van Chrome

Vanaf mei 2026 zullen veel openbare certificaatinstanties (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.

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
- Geen root-CA's voor gemengd gebruik meer voor TLS-certificaten voor openbare servers
- Tijdschema voor handhaving: maart 2027.

Openbare CA-responstijdlijn

- Oktober 2025: Veel publieke CA's (DigiCert, Sectigo, SSL) begonnen standaard met het uitgeven van alleen-servercertificaten.
- Mei 2026: veel openbare CA-servers geven geen EKU-certificeringen voor clientverificatie meer uit

- Maart 2027: Chrome Root Program Policy wordt volledig effectief

---

Opmerking: dit beleid is alleen van toepassing op certificaten die zijn uitgegeven door openbare CA's. Particuliere PKI en zelf ondertekende certificaten worden niet beïnvloed door dit beleid.

Hoe het Cisco ISE beïnvloedt

Betrokken producten

Alle Cisco ISE-releases worden beïnvloed:

- ISE 3.1
- ISE 3.2
- ISE 3.3
- ISE 3,4
- ISE 3,5

Opmerking: Cisco ISE 2.x-versies zijn ook beïnvloed; er is echter geen oplossing gepland omdat deze releases het einde van de levensduur (EOL) hebben bereikt.

Dubbele rol van Cisco ISE

ISE fungeert als zowel server als client in verschillende verbindingsscenario's, waarbij certificaten vereist zijn met zowel server- als clientverificatie-EKU's.

Cisco ISE als server (serververificatie EKU vereist):

- PxGrid
- ISE-berichtenservice

Cisco ISE als client (Client Authentication EKU vereist):

- TC-NAC
- Secure Syslog
- LDAPS
- Radius DTLS

Specifieke getroffen gebruiksgevallen

De onderstaande tabel geeft een overzicht van de Cisco ISE-services die kunnen worden beïnvloed door de komende wijzigingen in Client Authentication EKU, samen met de verwachte

impact voor elke service.

dienst	Impact
pxGrid	pxGrid-certificaten worden gebruikt voor communicatie tussen ISE-knooppunten en externe pxGrid-integraties. Terwijl voor externe pxGrid-integraties alleen Server Authentication EKU vereist is, vereist Cisco ISE momenteel dat geïmporteerde pxGrid-certificaten zowel Server Authentication EKU als Client Authentication EKU bevatten vanwege een UI-beperking. Als gevolg hiervan worden openbare CA-uitgegeven pxGrid-certificaten vaak ingezet bij beide EKU's.
ISE Messaging Service (IMS)	IMS wordt gebruikt voor backend-communicatie tussen interne ISE-diensten. Cisco ISE vereist momenteel dat IMS-certificaten zowel Server Authentication EKU als Client Authentication EKU bevatten. Certificaten die zijn verlengd door een openbare certificeringsinstantie met serververificatie EKU kunnen alleen niet worden gebruikt voor IMS, wat kan leiden tot fouten in de interne ISE-communicatie.
TC-NAC	Als het beheerderscertificaat alleen Server Authentication EKU bevat, kan certificaatgebaseerde verificatie voor TC-NAC worden beïnvloed wanneer de FIPS-modus is ingeschakeld of wanneer Tenable is geconfigureerd met mTLS (geïntroduceerd in ISE versies 3.4P3 en 3.5).
Secure Syslog	
LDAP's	
RADIUS DTLS	

⚠ Let op: klanten moeten het certificaattype controleren dat wordt gebruikt door externe pxGrid-clients. Bij verlenging mogen openbare CA-ondertekende certificaten geen Client Authentication EKU meer bevatten. Externe pxGrid-clientintegraties moeten de Client Authentication EKU bevatten bij communicatie met ISE, anders wordt de verbinding geweigerd.

Probleemsymptomen

Nadat alleen EKU-certificaten voor serververificatie in Cisco ISE zijn geïmplementeerd, zullen klanten fouten bij het importeren van certificaten in de Cisco ISE GUI observeren wanneer ze proberen pxGrid- of ISE Messaging Service (IMS)-certificaten te uploaden die niet voldoen aan de huidige EKU-vereisten (Extended Key Usage) voor de geselecteerde service.

Een voorbeeld van de foutmelding die in de GUI wordt weergegeven, wordt hieronder weergegeven.

Aanbevelingen

Controle van lopende certificaten (VERPLICHTE EERSTE STAP)

- Maak een inventarisatie van alle openbare TLS-certificaten om te bepalen welke certificaten de Client Authentication EKU bevatten
- Gebruik van documentcertificaten: identificeer welke certificaten worden gebruikt volgens de bovenstaande tabel die zijn ondertekend met Public-CA.
- CA- en root-informatie verifiëren: documenteren welke CA en root elk certificaat hebben uitgegeven
- Vervaldatums controleren: Plan verlengingen strategisch vóór beleidshandhaving

Suggesties voor services waarvoor EKU van de klant vereist is

De onderstaande tabel bevat aanbevolen acties voor Cisco ISE-services en -integraties die afhankelijk zijn van certificaten met Client Authentication EKU.

dienst	Aanbevolen acties
TC-NAC	• Wanneer Tenable wordt gebruikt, kan strikte EKU-validatie worden uitgeschakeld aan de Tenable-kant om de connectiviteit te behouden.
Secure Syslog	
LDAP's	
RADIUS DTLS	
PxGrid-clients (CatC, FMC, enz.)	
EAP-TLS	

Kortetermijnoplossingen (vóór juni 2026)

Beheerders kunnen kiezen uit een van de volgende opties:

Optie 1: Switch naar Public Root CA's die gecombineerde EKU-certificaten leveren

Sommige Public Root CA's (zoals DigiCert en IdenTrust) geven certificaten uit met gecombineerde EKU van een alternatieve root, die niet kan worden opgenomen in de Chrome-browservertrouwenswinkel.

Voorbeelden van Public Root CA's en EKU-typen:

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
DigiCert	clientAuth + serverAuth	DigiCert Assured ID Root G2	DigiCert verzekerde ID CA G2

Voorwaarden voor deze aanpak:

- Coördineer met uw CA-provider om de beschikbaarheid van dergelijke certificaten te controleren.
- Voordat u certificaten implementeert, moet u ervoor zorgen dat zowel de server die het certificaat presenteert als alle clients die het certificaat gebruiken, vertrouwen op de corresponderende basiscertificeringsinstantie.
- Informatie over basiscertificaten uitwisselen met communicatieve peers.
- Met deze aanpak wordt voorkomen dat software-upgrades onmiddellijk nodig zijn.

Referenties certificaatbeheer:

- Beheerdershandleiding voor de Cisco Identity Services-engine, release 3.3
- Certificaatvernieuwingen configureren op ISE

Optie 2: Huidige certificaten verlengen om hun geldigheid te verlengen

Certificaten die vóór mei 2026 zijn uitgegeven door Public Root CA's en die zowel server- als clientverificatie-EKU hebben, worden nog steeds gehonoreerd totdat hun termijn afloopt.

vernieuwingsstrategie

Algemene aanbevelingen zijn:

- Gecombineerde EKU-certificaten vernieuwen voordat het beleid wordt gewijzigd
- Voor de maximale geldigheid van het certificaat, plan om certificaten te vernieuwen vóór 15 maart 2026.
- Na deze datum zijn openbare CA-uitgegeven certificaten slechts 200 dagen geldig.
- Cisco raadt u ten zeerste aan om uw certificaten vóór deze datum te verlengen als u deze optie wilt volgen.
- Het beleid en de implementatiedata van openbare CA's kunnen variëren.
- Sommige publieke CA's zijn gestopt met het uitgeven van gecombineerde EKU-certificaten en kunnen er standaard geen verstrekken.
- Om een certificaat te genereren met een gecombineerde EKU, werkt u samen met uw CA-autoriteit en gebruikt u een speciaal profiel dat wordt verstrekt door openbare CA's.

Optie 3: Evalueren en migreren naar alternatieve CA-providers

Private PKI-benadering

- Evalueer de haalbaarheid van de overgang naar private PKI
- Een eigen CA instellen voor het uitgeven van afzonderlijke certificaten met gecombineerde EKU (server- en clientcertificaten met de vereiste EKU's)
- Bij het uitgeven van een privé CA-ondertekend certificaat, moet u rootcertificaatinformatie delen met de peer.
- 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 basiscertificeringsinstantie.
- Particuliere CA's zijn niet onderworpen aan het hoofdprogrammabeleid van Chrome
- Biedt langetermijncontrole over certificaatbeleid

Oplossing voor de lange termijn (software-upgrade vereist)

Klanten moeten Cisco ISE upgraden naar een patchversie die een bijgewerkte afhandeling van certificaten introduceert om certificaten te ondersteunen die zijn uitgegeven onder het nieuwe CA-beleid.

De volgende patchreleases pakken dit probleem aan, gepland voor april 2026:

Cisco ISE-versie	Patchversie
ISE 3.1	Patch 11
ISE 3.2	Patch 10
ISE 3.3	Patch 11

ISE 3,4	Patch 6
ISE 3,5	Patch 3

Gedrag na installatie van patch

PxGrid-certificaat

Na installatie van de patch release:

- De huidige UI-vereiste die zowel Server Authentication EKU als Client Authentication EKU voor pxGrid-certificaten afdwingt, wordt verwijderd.
- Cisco ISE staat de import toe van PxGrid-certificaten die alleen Server Authentication EKU's bevatten, zowel Server- als Client Authentication EKU's, of geen EKU-extensie.
- Certificaten met alleen Client Authentication EKU worden niet geaccepteerd.

ISE Messaging Service (IMS)-certificaat

Voor ISE 3.1, 3.2 en 3.3

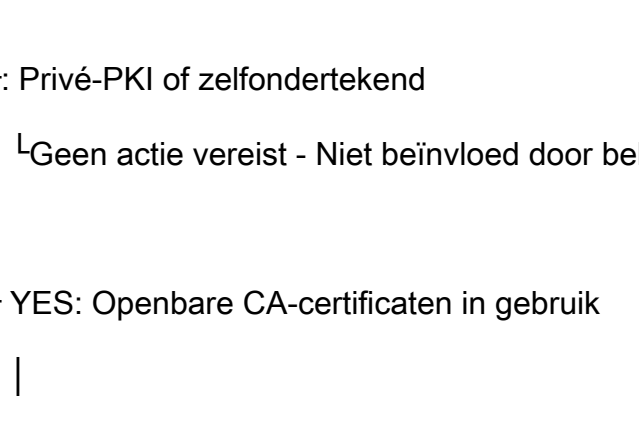
Er is geen gedragsverandering na installatie van de patch. De ISE Messaging Service blijft een certificaat nodig hebben met zowel client- als server-EKU. Klanten moeten van plan zijn om een ISE Internal CA-certificaat te gebruiken zodra het huidige certificaat verloopt.

Voor ISE 3.4 en 3.5

IMS ondersteunt nu alleen openbare CA-certificaten met serververificatie EKU. Omdat IMS echter alleen wordt gebruikt voor interne Cisco ISE-communicatie, raadt Cisco aan het ISE Internal CA-certificaat te gebruiken wanneer het certificaat wordt verlengd.

beslissingsboom

Start: Gebruikt u openbare CA-certificaten op Cisco ISE?



├Worden ze gebruikt voor een van de diensten die worden vermeld in de sectie "Specifieke getroffen gebruiksgevallen"?

│ │

│ ├ wanneer ISE optreedt als TLS-client

│ │ └"Suggesties voor services waarvoor Client EKU vereist is" sectie.

│ │

│ └ wanneer ISE optreedt als TLS-server (PxGrid OF IMS)

│ │

│ └ KIES UW AANPAK:

│ │

│ ├ Optie A: Switch naar alternatieve basiscertificeringsinstantie

│ │ ├Neem contact op met CA-provider voor gecombineerde EKU van alternatieve root

│ │ ├ Zorg ervoor dat alle peers nieuwe root vertrouwen

│ │ └Geen onmiddellijke software-upgrade nodig

│ │

│ ├ optie B: certificaten vóór de uiterste termijnen vernieuwen

│ │ ├Dit zal helpen de urgentie van het patchen van Cisco ISE los te laten

│ │ │

│ │ ├Voor maximale geldigheid: Verleng vóór 15 mrt 2026

│ │ └ Koopt tijd tot vervaldatum certificaat

│ │

│ ├ optie C: migreren naar privé-PKI

│ │ ├Een particuliere CA-infrastructuur opzetten

│ │ ├Geef gecombineerde EKU-certificaten af

│ │ ├Installeer de nieuwe CA in de ISE Trusted Store

│ │ └Langetermijncontrole

│ │

│ └ optie D: Software-upgrade plannen

│ ├Breng de vereiste ISE-patchrelease aan (beschikbaar vanaf april 2026)

Veelgestelde vragen (FAQ)

Algemene vragen

V: Moet ik me hier zorgen over maken als ik privé-PKI gebruik?

A: Nee. Dit beleid is alleen van invloed op certificaten die zijn uitgegeven door Public Root CA's. Particuliere PKI en zelf ondertekende certificaten worden niet beïnvloed.

V: Kan ik mijn bestaande certificaten blijven gebruiken?

A: Ja, bestaande certificaten met gecombineerde EKU blijven geldig totdat ze verlopen. Het probleem doet zich voor wanneer u moet vernieuwen. Ze werken voor zowel TLS- als mTLS-verbindingen tot het verstrijken.

V: Hoe weet ik of ik mTLS of standaard TLS gebruik?

A: Bekijk de sectie Specifieke getroffen gebruiksgevallen.

Upgradevragen

certificaatbeheer

Tijdlijnvragen

V: Wat gebeurt er op 15 juni 2026?

A: Chrome stopt met het vertrouwen op openbare TLS-certificaten die zowel Server- als Client Authentication EKU's bevatten. Diensten die dergelijke certificaten gebruiken, kunnen mislukken.

V: Waarom moet ik voor 15 maart 2026 vernieuwen?

A: Na 15 maart 2026 wordt de geldigheid van het certificaat teruggebracht van 398 dagen naar 200 dagen. Verlenging vóór deze datum geeft u een maximale levensduur van het certificaat.

V: Wat is de deadline voor actie?

A: Er zijn meerdere deadlines:

- 15 maart 2026: Geldigheid certificaat teruggebracht tot 200 dagen
- Mei 2026: De meeste openbare CA's stoppen volledig met de uitgifte van

gecombineerde EKU
- Maart 2027: Chrome-beleid volledig gehandhaafd

Aanvullende bronnen

- Cisco bug ID: CSCws83036- Effectbeoordeling van ClientAuth EKU-handhaving in ISE

Externe verwijzingen

- Chrome Root Program-beleid

Middelen van de certificaatautoriteit

- IdenTrust-portal

Conclusie

De onderinstelling van Client Authentication EKU in openbare CA-certificaten vertegenwoordigt een belangrijke verschuiving in het beveiligingsbeleid die van invloed is op Cisco ISE-implementaties met behulp van mTLS-verbindingen. Hoewel dit een verandering in de hele sector is, is de impactbeoordeling KRITIEK en is onmiddellijke actie vereist om onderbrekingen van de service te voorkomen.

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.