# Impact du pare-feu sécurisé Cisco sur l'authentification du client AC public Modifications de l'UKE à partir de mai 2026 pour les communications sécurisées

## Table des matières


Introduction

Informations générales

- Objectif des attributs EKU
- Principales utilisations des attributs EKU
- Pourquoi la suppression de l'EKU d'authentification client des certificats de serveur ?
- Impact sur les environnements de serveurs

Description du problème

- Modification de la politique du programme racine Chrome
- Principales exigences de stratégie
- Échéances

Impact sur les produits Cisco Secure Firewall

- Produits concernés
- Problème 1. Problème d'intégration pxGrid entre FMC et ISE, lorsque le certificat FMC n'a pas l'attribut Client Authentication EKU
- Problème 2. Problème d'intégration FTD ou ASA avec un serveur LDAPS, lorsque le certificat présenté ne présente pas l'attribut Client Authentication EKU
- Problème 3.Le client sécurisé Cisco (anciennement AnyConnect) peut rencontrer des problèmes de connexion à un FTD ou à un ASA si le certificat client ne possède pas l'attribut Client Authentication EKU
- Problème 4.Les tunnels VPN site à site avec authentification basée sur certificat échouent si le certificat d'identité ne comporte pas l'attribut EKU d'authentification du client

Instructions pour confirmer si votre certificat ne possède pas l'attribut EKU d'authentification du client

- Vérifier les attributs EKU d'un certificat .cer à l'aide du Gestionnaire de certificats Windows
  - Exemple 1 : Ce certificat .cer ne contient pas l'attribut EKU d'authentification client et inclut uniquement l'attribut EKU d'authentification serveur.
  - Exemple 2 : Ce certificat .cer inclut les attributs EKU d'authentification du serveur et du client.
- Vérifiez les attributs EKU à partir d'un certificat PKCS#12, PEM et .cer à l'aide d'OpenSSL
  - Exemple 1 : Ce certificat .pem (PEM) ne contient pas l'attribut EKU d'authentification client et inclut uniquement l'attribut EKU d'authentification serveur.
  - Exemple 2 : Ce certificat .pem (PEM) inclut les attributs EKU d'authentification client et serveur.

Solution De Contournement

- Option 1. Passer à des autorités de certification racine publiques qui fournissent des certificats EKU combinés
- Option 2. Renouveler les certificats actuels pour prolonger leur validité
- Option 3. Migrer vers une ICP privée pour émettre des certificats EKU (serveur et client) combinés

Option 4. Obtenir un certificat de confiance publique avec seulement l'EKU d'authentification du client

Foire aux questions (FAQ)

Informations connexes

Bogues associés

Références Cisco ISE

Références externes

# Introduction

Ce document décrit l'impact des restrictions sur les critères d'émission de certificat imposés par les autorités de certification qui se conforment au programme Chrome Root Certificate, en particulier en ce qui concerne les produits Cisco Secure Firewall.

# Informations générales

Les certificats TLS de confiance publique sont émis par des autorités de certification qui doivent se conformer aux politiques du secteur qui régissent l'émission et l'utilisation des certificats.

La politique du programme racine Chrome, gérée par Google, définit les exigences que les autorités de certification doivent respecter pour que leurs certificats soient approuvés par le navigateur Google Chrome. Ces exigences influencent la manière dont les certificats de confiance publique sont émis dans l'ensemble du secteur. Dans le cadre de l'évolution des pratiques de sécurité, le programme racine Chrome introduit des conseils plus stricts sur l'utilisation des certificats.

De nombreuses autorités de certification publiques s'éloignent donc de l'émission de certificats qui incluent l'EKU d'authentification du client et passent à l'émission de certificats destinés uniquement à l'authentification du serveur. Par conséquent, les certificats nouvellement émis par de nombreuses autorités de certification publiques devraient inclure uniquement l'EKU d'authentification du serveur.

L'utilisation de clé étendue (EKU), est une extension de certificat qui définit la fonction prévue d'une clé publique dans un certificat numérique. Il établit un ensemble structuré d'applications autorisées, en s'assurant que la clé est utilisée uniquement pour des opérations cryptographiques spécifiques. Cette fonctionnalité est régie par des identificateurs d'objet (OID)—des identificateurs numériques uniques qui catégorisent chaque utilisation autorisée, tels que la signature de code, l'authentification du serveur, l'authentification du client ou la messagerie électronique sécurisée.

Lorsque l'authentification est basée sur un certificat, l'entité de vérification examine le certificat pour identifier l'identificateur d'objet (OID) dans l'EKU. En incorporant l'extension EKU, une autorité de certification (CA) limite l'étendue

du certificat à des rôles prédéfinis, chaque fonction désignée étant explicitement mappée à un OID.

Objectif des attributs EKU

· Définir l'utilisation : Les attributs EKU précisent les types d'authentification ou de cryptage que le certificat est autorisé à effectuer.

· Améliorer la sécurité : En restreignant les certificats à des utilisations spécifiques, l'UER permet d'empêcher une utilisation abusive ou une application non intentionnelle (par exemple, un certificat de serveur ne peut pas être utilisé pour l'authentification du client).

· Conformité : Garantit que les certificats sont utilisés conformément aux politiques de sécurité et aux normes du secteur.

Principales utilisations des attributs EKU

1. Authentification du client Web TLS

· Permet d’utiliser des certificats pour identifier et authentifier des utilisateurs ou des périphériques sur un serveur.

•OID: 1.3.6.1.5.5.7.3.2

· Utilisé dans les VPN, les TLS mutuels et les scénarios de connexion sécurisée.

2. Authentification du serveur Web TLS

· Permet aux serveurs d’utiliser des certificats pour prouver leur identité aux clients.

•OID: 1.3.6.1.5.5.7.3.1

· Utilisé dans les serveurs Web HTTPS, SSL/TLS et les terminaux API sécurisés.

3. Signature du code

· Indique que le certificat peut être utilisé pour signer des logiciels ou des exécutables.

•OID: 1.3.6.1.5.5.7.3.3

· Utilisé pour la distribution de logiciels et les contrôles d'intégrité.

4. Protection de la messagerie

· Permet l'utilisation de certificats pour la signature et le chiffrement des e-mails.

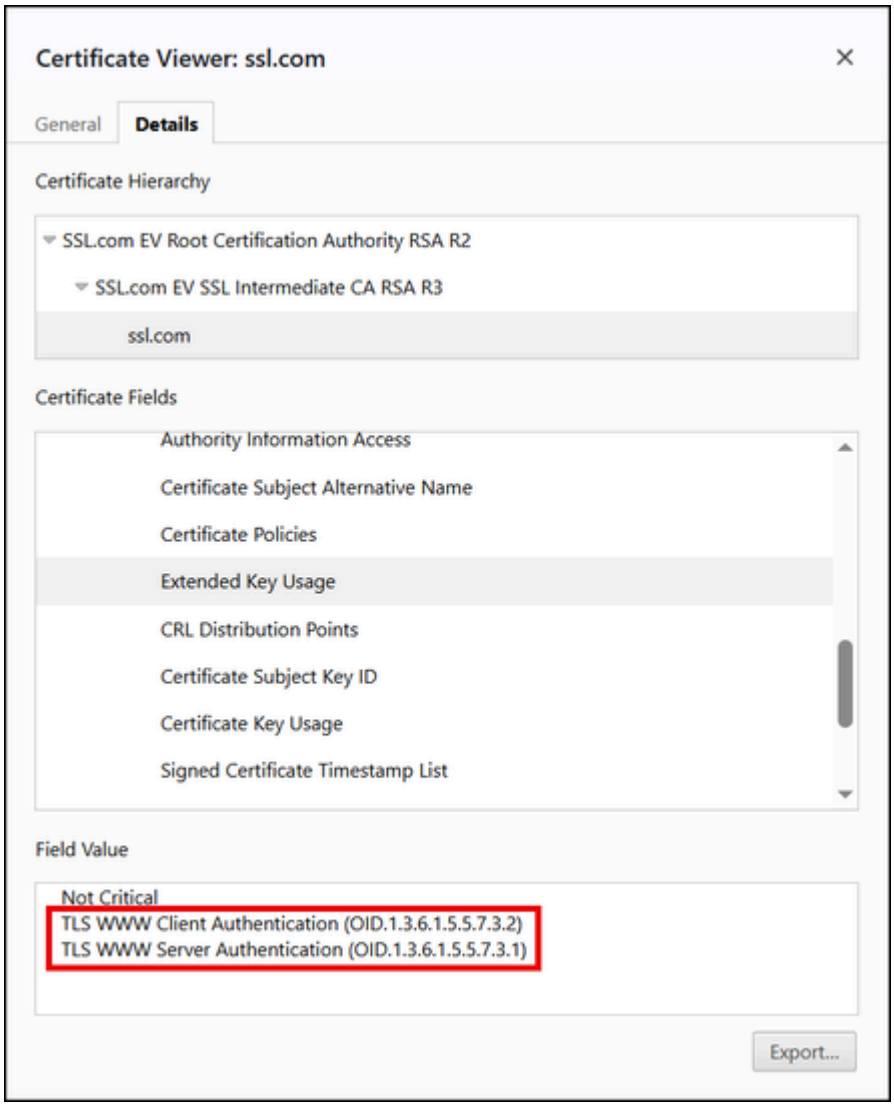
•OID: 1.3.6.1.5.5.7.3.4

· Utilisé dans la sécurité de la messagerie S/MIME.

5. Autres finalités

· Signature de documents, horodatage, connexion par carte à puce, etc., chacun avec son propre OID.

Les navigateurs et les serveurs n'ont besoin que de l'EKU serverAuth pour établir une connexion sécurisée pour HTTPS, mais historiquement, de nombreux certificats de serveur TLS incluaient à la fois les EKU serverAuth et clientAuth, voici un exemple d'un tel certificat :




Pourquoi la suppression de l'EKU d'authentification client des certificats de serveur ?

- Sécurité et portée : les certificats TLS publics ne sont censés authentifier que les serveurs sur le Web. La suppression permet une séparation claire entre la fonctionnalité serveur et la fonctionnalité client. L'EKU ClientAuth est utilisée pour l'authentification des machines et des utilisateurs avec le protocole Mutual TLS (mTLS) et d'autres scénarios d'authentification.

- Prévention des erreurs de configuration : certains systèmes peuvent faire confiance à tout certificat d'une autorité de certification publique pour l'authentification du client si l'unité EKU est présente, ce qui peut représenter un risque pour la sécurité.

- Configuration requise pour le navigateur : les principaux navigateurs ne requièrent pas ou ne vérifient pas l'EKU d'authentification client dans le certificat d'un site Web.

- Architecture PKI simplifiée : en séparant les utilisations, les autorités de certification peuvent gérer des hiérarchies de certificats distinctes pour le serveur TLS et d’autres fonctions.

Cela est particulièrement important pour les produits tels que Cisco Secure Firewall Adaptive Security Appliance (ASA), Cisco Secure Firewall Threat Defense (FTD), Cisco Secure Firewall Device Manager (FDM) et Cisco Secure Firewall Management Center (FMC) qui peuvent agir en tant que serveur ou client lors de l'authentification TLS, selon le cas d'utilisation.

Impact sur les environnements de serveurs

Pour la grande majorité des déploiements de serveurs, cette modification aura un impact faible ou aucun impact. Voici à quoi s'attendre :

- Serveurs Web standard (HTTPS) : aucun impact. Les certificats mis à jour continueront à fonctionner normalement.
- Certificats existants : tout certificat émis avant la coupure continuera à fonctionner jusqu'à son expiration.
- Scénarios de certification mutuelle TLS (mTLS) et client : si vous utilisiez un certificat de serveur TLS pour l'authentification client, vous devrez obtenir un certificat distinct avec l'EKU d'authentification client à partir d'une autre source.
- Systèmes d'entreprise nécessitant les deux unités EKU : certains systèmes existants ou d'entreprise attendaient les deux unités EKU. Vous devez vérifier si des mises à jour sont nécessaires pour respecter les nouvelles règles.

# Description du problème

À partir de mai 2026, de nombreuses autorités de certification publiques cesseront d’émettre des certificats TLS (Transport Layer Security) incluant l’utilisation de la clé étendue d’authentification du client (EKU). Les certificats nouvellement émis incluent généralement l'EKU d'authentification du serveur uniquement.

Par conséquent, si les certificats émis par une autorité de certification publique sont renouvelés en vertu des stratégies d'autorité de certification mises à jour, puis déployés dans les produits Cisco Secure Firewall, les services pour lesquels l'EKU d'authentification client est requise échoueront. Les services spécifiques concernés sont les suivants :

- Lorsque l'ASA, le FTD, le FDM ou le FMC agit en tant que client (par exemple, lors de la connexion à des fournisseurs d'identité ou à des serveurs d'authentification tels que ISE (pxGrid), RADIUS, LDAPS ou Active Directory), l'authentification basée sur les certificats peut échouer si le certificat client a été généré par une autorité de certification publique et qu'il manque l'EKU d'authentification client. Dans ces scénarios, si le serveur d'authentification rejette les certificats sans l'EKU requise, des échecs de connexion peuvent se produire.

- Le client sécurisé Cisco (anciennement AnyConnect) peut s'authentifier auprès des serveurs ASA ou FTD à l'aide de certificats. Toutefois, si le certificat client a été généré par une autorité de certification publique et qu'il manque l'EKU d'authentification client, la connexion RAVPN (Remote Access VPN) échouera.

- Lorsque le FTD ou l'ASA établit un tunnel VPN site à site (qu'il soit vers un autre FTD, ASA, routeur Cisco ou homologue VPN tiers) à l'aide de l'authentification de certificat (RSA ou ECDSA), le tunnel échoue si l'attribut Client Authentication EKU est manquant dans le certificat d'identité généré par une autorité de certification publique. Cela se produit parce que l'homologue VPN distant nécessite que l'EKU d'authentification du client soit présent dans le certificat d'identité.

Modification de la politique du programme racine Chrome

La mise en oeuvre de l'UER dépend de la signature du certificat par l'AC. L'utilisation de l'authentification serveur et de l'authentification client EKU était une pratique courante. Cependant, dans le cadre de la modification de la stratégie du programme racine Chrome, les autorités de certification qui s'alignent sur ces critères d'émission de certificat cessent de signer les certificats TLS qui incluent l'utilisation de la clé étendue d'authentification client (EKU). Les certificats récemment émis incluent uniquement l'EKU d'authentification serveur.

Principales exigences de stratégie

- Les autorités de certification racine publiques doivent affirmer l'utilisation de clé étendue (EKU) UNIQUEMENT pour l'authentification du serveur (id-kp-serverAuth)

- Les certificats doivent inclure UNIQUEMENT l'EKU d'authentification serveur.

- Il est interdit d'inclure Client Authentication EKU dans ces certificats

- Les autorités de certification racine qui continuent à émettre des certificats avec l'EKU d'authentification client sont finalement retirées du magasin racine Chrome provoquant le marquage de tels certificats comme "non approuvés" par le navigateur Chrome

Échéances

- Septembre 2025, SSL.com émettra des certificats TLS qui incluent uniquement l'EKU ServerAuth (et non ClientAuth) pour les certificats de serveur. En d'autres termes, les nouveaux certificats SSL/TLS pour votre site Web ou votre serveur seront explicitement réservés à l'« authentification serveur ».

- Octobre 2025 : les autorités de certification s'alignant sur le programme (par exemple : DigiCert, Sectigo, etc.) ont

commencé à émettre des certificats de serveur uniquement par défaut.

- Mai 2026 : les autorités de certification s'alignant sur le programme cessent d'émettre des certificats EKU d'authentification client

- Mars 2027 : La politique du programme racine de Chrome devient pleinement efficace

## Impact sur les produits Cisco Secure Firewall

Une fois que les autorités de certification publiques ont commencé à inclure uniquement l'EKU d'authentification du serveur dans les certificats émis. Cela pourrait avoir l'impact suivant sur les scénarios de produits Cisco Secure Firewall suivants :

- Lorsque l'ASA, le FTD, le FDM ou le FMC agit en tant que client (par exemple, lors de la connexion à des fournisseurs d'identité ou à des serveurs d'authentification tels que ISE (pxGrid), RADIUS, LDAPS ou Active Directory), l'authentification basée sur les certificats peut échouer si le certificat client a été généré par une autorité de certification publique et qu'il manque l'EKU d'authentification client. Dans ces scénarios, si le serveur d'authentification rejette les certificats sans l'EKU requise, des échecs de connexion peuvent se produire.

- Le client sécurisé Cisco (anciennement AnyConnect) peut s'authentifier auprès des serveurs ASA ou FTD à l'aide de certificats. Toutefois, si le certificat client a été généré par une autorité de certification publique et qu'il manque l'EKU d'authentification client, la connexion RAVPN (Remote Access VPN) échouera.

- Lorsque le FTD ou l'ASA établit un tunnel VPN site à site (qu'il soit vers un autre FTD, ASA, routeur Cisco ou homologue VPN tiers) à l'aide de l'authentification de certificat (RSA ou ECDSA), le tunnel échoue si l'attribut Client Authentication EKU est manquant dans le certificat d'identité généré par une autorité de certification publique. Cela se produit parce que l'homologue VPN distant nécessite que l'EKU d'authentification du client soit présent dans le certificat d'identité.

---

Remarque : si vous intégrez FMC ou FDM avec ISE via pxGrid et que les certificats installés sur votre FMC/FDM n'ont pas l'attribut EKU d'authentification client, examinez les solutions de contournement proposées dans ce document et les références ISE suivantes : FN74392 et Prepare Identity Services Engine for Extended Key Usage Restrictions in Certificates Issued by Public Certification Authorities.

---

Remarque : La suppression de l'EKU d'authentification du client des certificats du serveur TLS est une modification de stratégie à l'échelle du secteur qui améliorera la sécurité et empêchera toute utilisation abusive. Pour la plupart des utilisateurs, il n'y aura pas d'impact notable. Cependant, si vous vous fiez à l'EKU ClientAuth, vous devez prendre des mesures proactives pour obtenir le type de certificat approprié à vos besoins.

---

Produits concernés

<table>
<tr><th>Produit Cisco Secure Firewall</th><th>Version du logiciel</th><th>Scénarios impactés</th><th>Corrections</th></tr>
<tr><td>FTD</td><td>Toutes les versions</td><td rowspan="4">Lorsqu'agit en tant que client (par exemple, lors de la connexion à des fournisseurs d'identité ou à des serveurs d'authentification tels que ISE (pxGrid), RADIUS, LDAPS ou Active Directory), l'authentification basée sur certificat peut échouer si le certificat client a été généré par une autorité de certification publique et qu'il manque l'EKU d'authentification client. Dans ce scénario, si le serveur d'authentification rejette les certificats sans l'EKU requise, des échecs de connexion peuvent se produire.</td><td rowspan="5">Option 1. Si vous utilisez un certificat de serveur TLS pour l'authentification client, vous devrez obtenir un certificat avec l'EKU ClientAuth d'une autre source.<br><br>OU<br><br>Option2. Basculer vers des autorités de certification racines publiques (autorités de certification) qui fournissent des certificats EKU (ClientAuth et ServerAuth) combinés.<br><br>NOTE: Pour plus d'options, reportez-vous à la section Solutions de contournement de ce document.</td></tr>
<tr><td>FDM</td><td>Toutes les versions</td></tr>
<tr><td>FMC</td><td>Toutes les versions</td></tr>
<tr><td>ASA</td><td>Toutes les versions</td></tr>
<tr><td>Cisco Secure Client (anciennement AnyConnect)</td><td>Toutes les versions</td><td>Le client sécurisé Cisco peut s'authentifier auprès des serveurs ASA ou FTD à l'aide de certificats. Toutefois, si le certificat client a été généré par une</td></tr>
</table>

| | | | |
|---|---|---|---|
| | | autorité de certification publique et qu'il manque l'EKU d'authentification client, la connexion au VPN d'accès à distance (RAVPN) échouera. | |
| FTD ou ASA | Toutes les versions | Lorsque le FTD ou l'ASA établit un tunnel VPN site à site (qu'il soit vers un autre FTD, ASA, routeur Cisco ou homologue VPN tiers) à l'aide de l'authentification de certificat (RSA ou ECDSA), le tunnel VPN échoue si l'attribut Client Authentication EKU est manquant dans le certificat d'identité généré par une autorité de certification publique. Cela se produit parce que l'homologue VPN distant nécessite que l'EKU d'authentification du client soit présent dans le certificat d'identité. | |

Remarque : si vous intégrez FMC ou FDM avec ISE via pxGrid et que les certificats installés sur votre FMC/FDM n'ont pas l'attribut EKU d'authentification client, examinez les solutions de contournement proposées dans ce document et les références ISE suivantes : FN74392 et Prepare Identity Services Engine for Extended Key Usage Restrictions in Certificates Issued by Public Certification Authorities.

Remarque : La suppression de l'EKU d'authentification du client des certificats du serveur TLS est une

modification de stratégie à l'échelle du secteur qui améliorera la sécurité et empêchera toute utilisation abusive. Pour la plupart des utilisateurs, il n'y aura pas d'impact notable. Cependant, si vous vous fiez à l'EKU ClientAuth, vous devez prendre des mesures proactives pour obtenir le type de certificat approprié à vos besoins.

Mise en garde : Pour les environnements de production, il est fortement recommandé aux clients d'utiliser des certificats avec les attributs EKU appropriés. Cette pratique garantit la sécurité, la compatibilité et le respect des normes du secteur et des meilleures pratiques. Les certificats sans attributs UER ne doivent être considérés que comme une solution de contournement temporaire et uniquement avec une compréhension claire des risques associés.

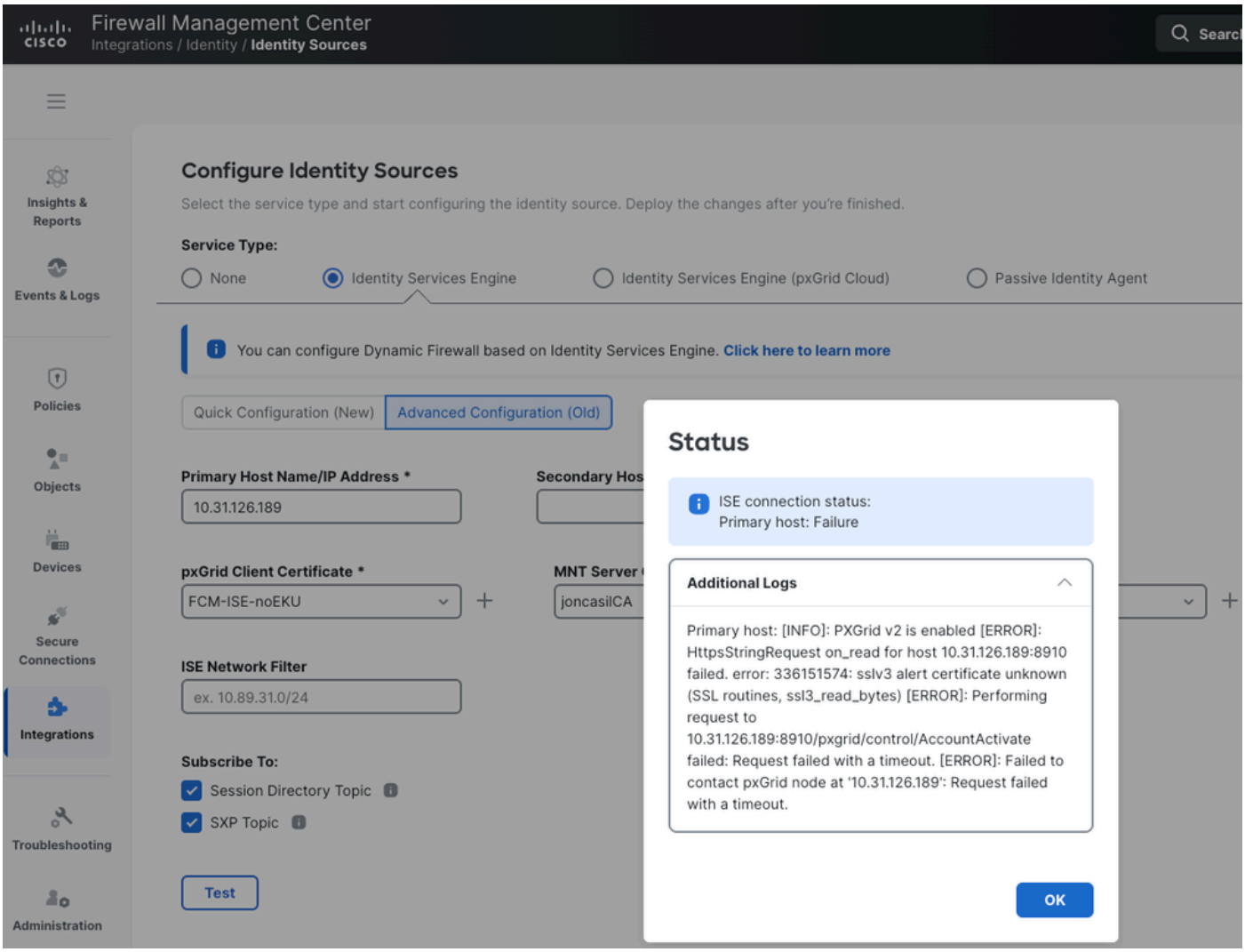
Problème 1. Problème d'intégration pxGrid entre FMC et ISE, lorsque le certificat FMC n'a pas l'attribut Client Authentication EKU

Dans ce scénario, le certificat utilisé par le FMC pour l'intégration de pxGrid avec ISE n'a pas l'attribut EKU d'authentification du client. Par conséquent, l'intégration de pxGrid échoue car le serveur ISE s'attend à ce que cet attribut soit présent dans le certificat présenté par le FMC.

Topologie




Erreurs FMC UI : Il s'agit du message d'erreur affiché dans le FMC, lorsque le certificat utilisé par le FMC ne contient pas l'attribut Client Authentication EKU pour l'intégration de pxGrid avec ISE.




Erreurs CLI FMC : Les mêmes messages d'erreur se trouvent dans le répertoire 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

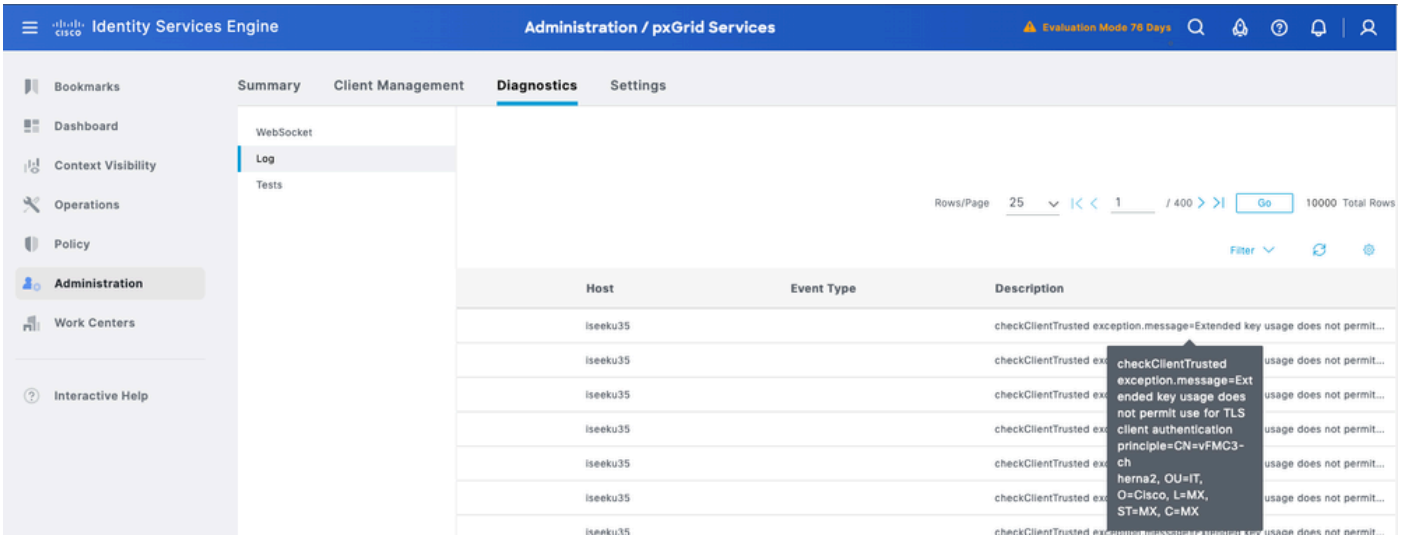
[ERROR] Performing request to 10.31.126.189:8910/pxgrid/control/AccountActivate failed: Request failed w

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
```

Erreur ISE : Il s'agit du message d'erreur affiché dans ISE, "checkClientTrusted exception.message=Extended key usage does not permit use for TLS client authentication rule=CN=vFMC3-cherna2, OU=IT, O=Cisco, L=MX, ST=MX, C=MX".




Solution : si vous intégrez FMC ou FDM avec ISE via pxGrid et que le certificat installé dans votre FMC/FDM ne possède pas l'attribut EKU d'authentification du client, passez en revue la proposition contenue dans ce document et les références ISE suivantes : FN74392 et Prepare Identity Services Engine for Extended Key Usage Restrictions in Certificates Issued by Public Certification Authorities for a successful pxGrid integration.

---

Remarque : Le certificat client FMC pxGrid doit inclure l'attribut EKU ClientAuth ou ne contenir aucun attribut EKU Client ou Server.

---

Remarque : Même si l'utilisation d'un certificat signé par une autorité de certification publique est prise en charge pour IMS. Cisco recommande d'utiliser le certificat d'autorité de certification interne ISE, car cette communication ne concerne que les transactions internes.

---

Problème 2. Problème d'intégration FTD ou ASA avec un serveur LDAPS, lorsque le certificat présenté ne présente pas l'attribut Client Authentication EKU

Dans ce scénario, le FTD ou l'ASA agit en tant que client pour s'intégrer à un serveur LDAPS à l'aide de l'authentification

par certificat. Si le certificat utilisé par le FTD ou l'ASA n'a pas l'attribut EKU d'authentification client, l'intégration échoue car le serveur LDAPS exige que cet attribut soit présent dans le certificat.

Topologie




Erreurs du serveur LDAP : 'Vérification du certificat TLS : Erreur, fonction de certificat non prise en charge' et 'Trace TLS : SSL3 alert write:fatal:unsupported certificate'

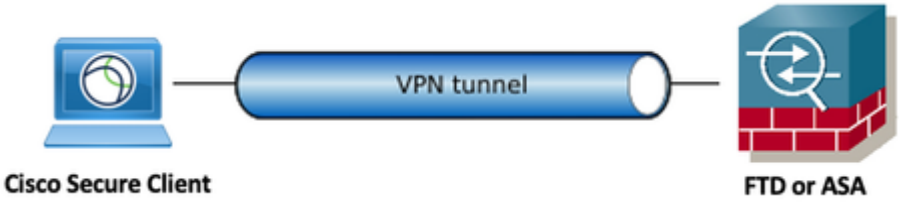
```
69ceb4f5.157b4993 0x7ff553fff700 TLS trace: SSL_accept:TLSv1.3 write server cer
tificate verify
69ceb4f5.157c01a4 0x7ff553fff700 TLS trace: SSL_accept:SSLv3/TLS write finished
69ceb4f5.157c458a 0x7ff553fff700 TLS trace: SSL_accept:TLSv1.3 early data
69ceb4f5.157c6685 0x7ff553fff700 TLS trace: SSL_accept:error 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
```

Solution : Examinez la proposition dans ce document pour vous assurer que le FTD ou l'ASA utilise le certificat d'identité correct, y compris l'attribut EKU d'authentification client, pour une authentification basée sur certificat réussie avec le serveur LDAPS.

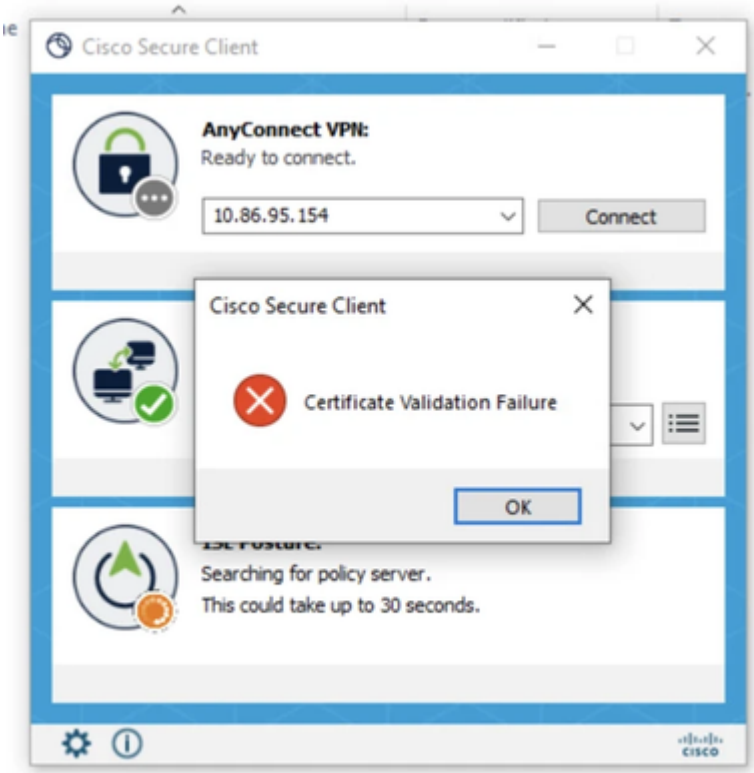
Problème 3. Cisco Secure Client (anciennement AnyConnect) peut rencontrer des problèmes de connexion à un FTD ou à un ASA si le certificat client ne possède pas l'attribut Client Authentication EKU

Dans ce scénario, le client sécurisé Cisco utilise l'authentification de certificat pour établir un tunnel RAVPN vers le FTD ou l'ASA. Cependant, si le certificat client ne possède pas l'attribut Client Authentication EKU, la session RAVPN échouera car l'ASA ou le FTD exige que cet attribut soit présent dans le certificat client.

Topologie




Erreur du client sécurisé Cisco : 'Échec de la validation du certificat'




Erreurs DART du client sécurisé Cisco : Les journaux suivants du fichier AnyConnectVPN.txt dans le bundle DART confirment que le client sécurisé Cisco a rejeté le certificat utilisé pour l'authentification basée sur certificat RAVPN vers le FTD/ASA en raison de l'absence de l'attribut EKU d'authentification du client (afin de localiser le fichier AnyConnectVPN.txt dans le bundle

DART, accédez à 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]

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

Solution : Examinez les propositions présentées dans ce document pour vous assurer que le client sécurisé Cisco utilise le certificat correct, y compris l'attribut Client Authentication EKU, pour une authentification basée sur certificat réussie avec le FTD ou l'ASA.

---

Remarque : À partir de l'erreur de bundle DART ci-dessus 'EKU introuvable dans le certificat : 1.3.6.1.5.5.7.3.2' , ce numéro '1.3.6.1.5.5.7.3.2' correspond à l'OID de l'unité EKU d'authentification du client.

---

Problème 4. Les tunnels VPN site à site avec authentification basée sur certificat échouent si le certificat d'identité ne comporte pas l'attribut EKU d'authentification client

Dans ce scénario, qui implique une authentification basée sur un certificat pour un tunnel VPN site à site IKEv2, le certificat d'identité utilisé par FTD/ASA (1) pour établir le tunnel vers l'homologue FTD/ASA (2) ne possède pas l'attribut Client Authentication EKU. Par conséquent, le tunnel VPN ne peut pas être établi parce que l'homologue distant, FTD/ASA (2), exige que cet attribut soit présent dans le certificat.

Topologie




Erreurs FTD ou ASA CLI : il s'agit des erreurs observées sur le FTD/ASA (2) pendant l'authentification basée sur le certificat IKEv2 lorsqu'il rejette le certificat d'identité FTD/ASA (1) qui ne possède pas l'attribut EKU d'authentification 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
```

Remarque : Dans l'exemple ci-dessus, le FTD/ASA (2) utilisait un certificat d'identité qui incluait à la fois les attributs ClientAuth et ServerAuth EKU.

Remarque : Dans l'exemple ci-dessus, le FTD/ASA (2) peut également être remplacé par un routeur ou un concentrateur VPN tiers physique ou basé sur le cloud. Ensuite, le même problème persistera, car l'homologue VPN exige que l'attribut Client Authentication EKU soit présent dans le certificat utilisé par le FTD/ASA (1) pour une authentification basée sur certificat réussie.

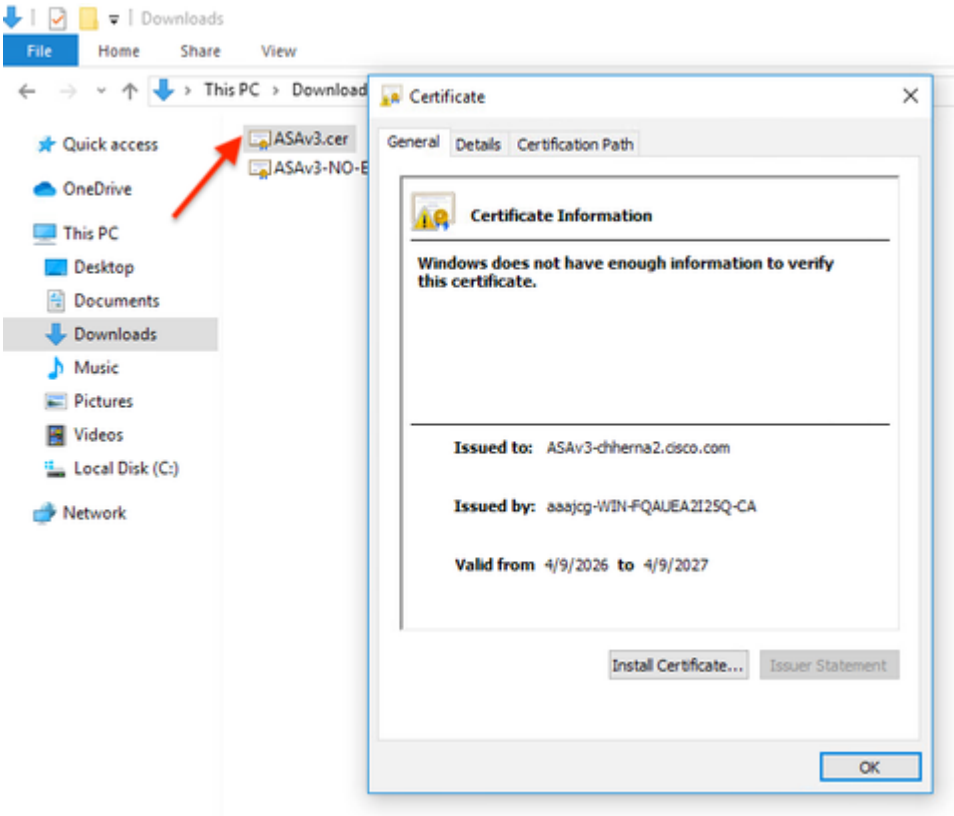
Solution : Examinez les propositions présentées dans ce document pour vous assurer que FTD/ASA (1) utilise le certificat d'identité correct, y compris l'attribut EKU d'authentification client, pour un tunnel VPN site à site réussi avec authentification basée sur certificat.

# Instructions pour confirmer si votre certificat ne possède pas l'attribut EKU d'authentification du client

## Vérifier les attributs EKU d'un certificat .cer à l'aide du Gestionnaire de certificats Windows

Suivez les étapes suivantes pour vérifier les attributs EKU d'un certificat .cer à l'aide du Gestionnaire de certificats Windows :

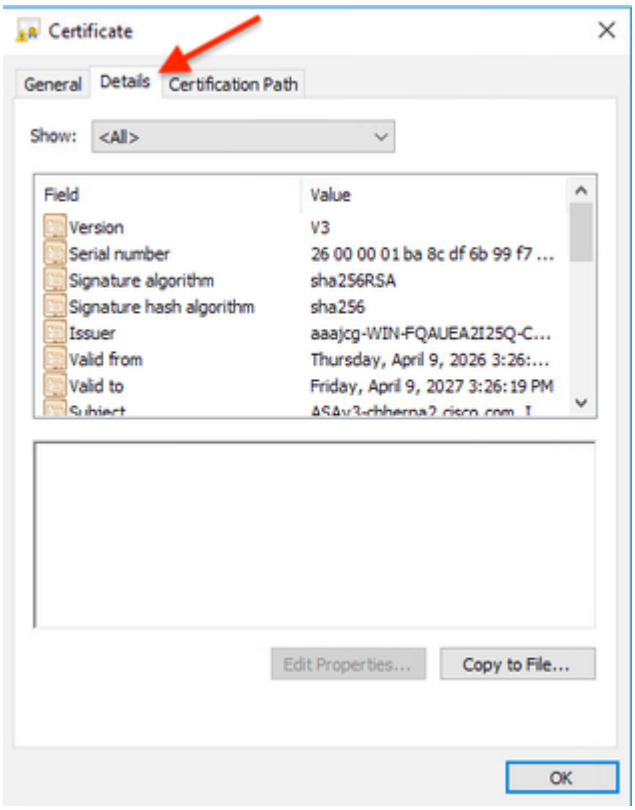
Étape 1. Double-cliquez sur le fichier .cer pour l'ouvrir dans le Gestionnaire de certificats Windows.



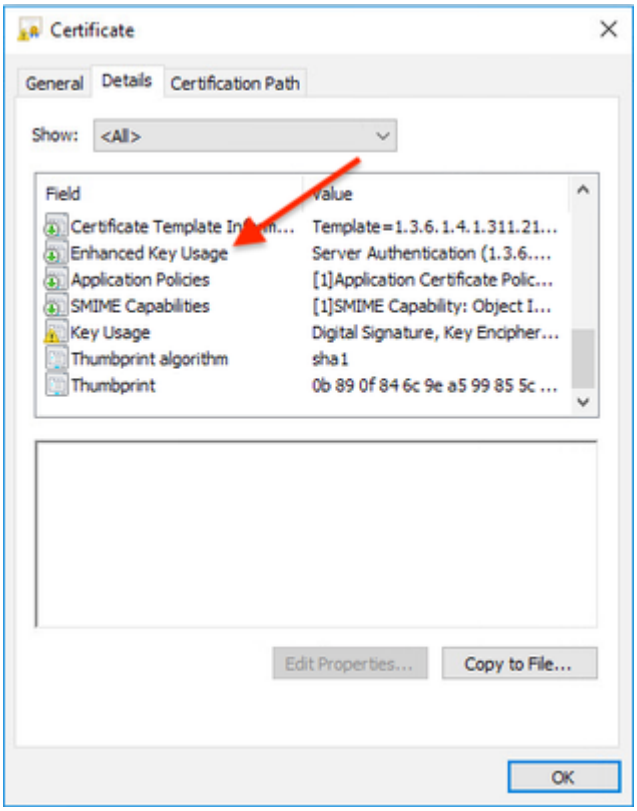

Remarque : Seuls les fichiers .cer s'ouvrent directement de cette façon ; si votre certificat a une extension .pem, renommez-le d'abord en .cer ou .crt.

Étape 2. Gestion des avertissements de sécurité (le cas échéant) : si une invite d'avertissement de sécurité s'affiche, cliquez sur Ouvrir pour continuer.

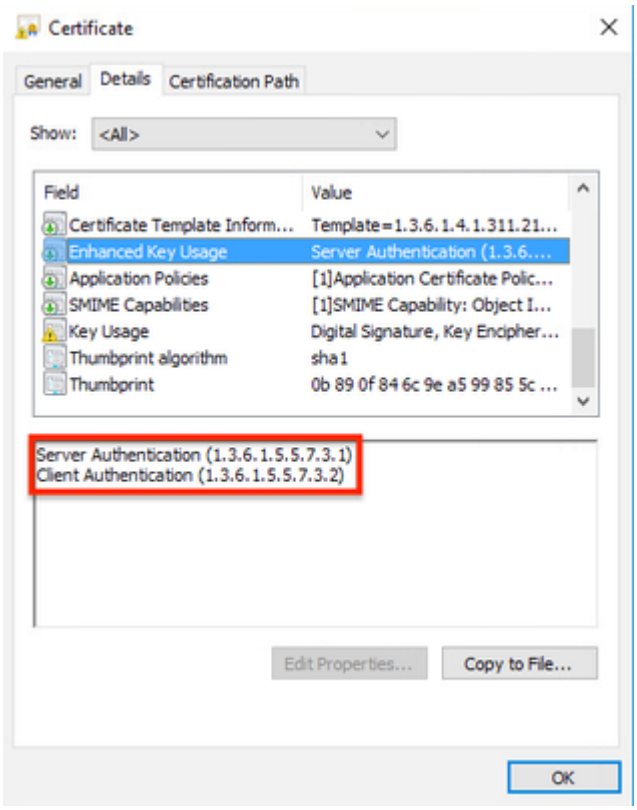
Étape 3. Dans la fenêtre du certificat, cliquez sur l’onglet Détails.




Étape 4. Faites défiler la liste des champs et sélectionnez « Enhanced Key Usage » (ou Extended Key Usage).

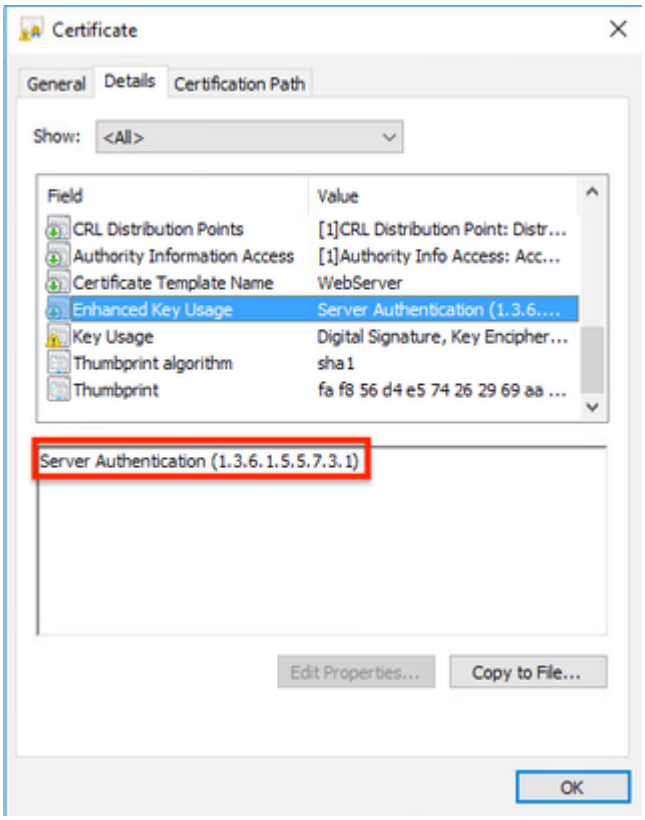



Étape 5. Vérifiez les attributs EKU, vous pouvez voir des entrées comme "Authentification serveur" et "Authentification client" indiquant les valeurs EKU présentes dans le certificat.

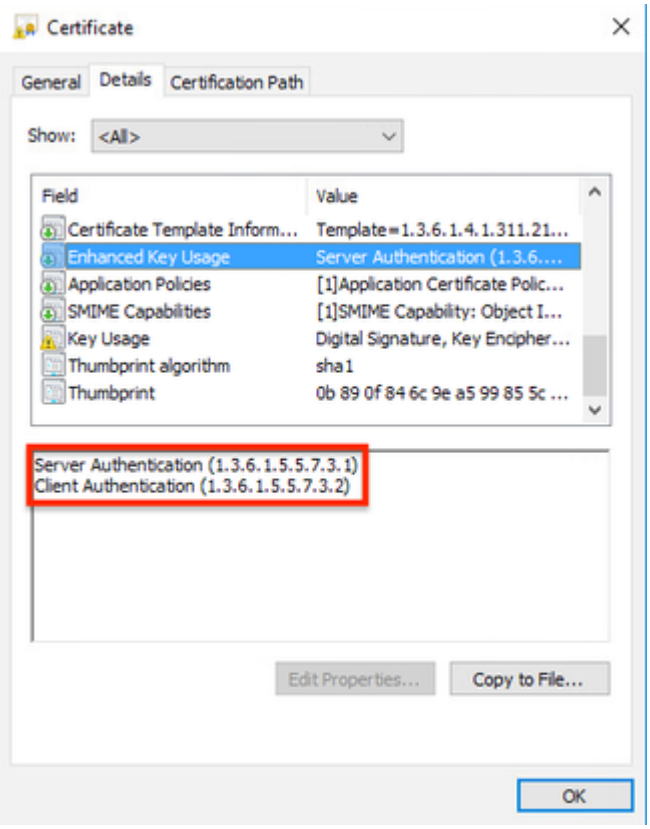



Étape 6. Après la vérification, cliquez sur OK pour fermer la fenêtre du certificat.

Exemple 1 : Ce certificat .cer ne contient pas l'attribut EKU d'authentification client et inclut uniquement l'attribut EKU d'authentification serveur.



Exemple 2 : Ce certificat .cer inclut les attributs EKU d'authentification du serveur et du client.




## Vérification des attributs EKU à partir d'un certificat PKCS#12, PEM et .cer à l'aide d'OpenSSL

Suivez les étapes suivantes pour vérifier les attributs EKU d'un certificat .p12 (PKCS#12), .pem (PEM) et .cer :

Étape 1 : localisez le certificat à vérifier et exportez-le au format .p12 (PKCS#12), .pem (PEM) ou .cer.

Pour les certificats .p12 (PKCS#12), utilisez openssl pour extraire le certificat du fichier .p12 (PKCS#12), le fichier .p12 (PKCS#12) peut contenir la clé privée, le certificat et les certificats d'autorité de certification.

Utilisez la commande suivante pour extraire le certificat d'un fichier .p12 (PKCS#12) dans un fichier .pem (PEM) (sans la clé privée ni la chaîne CA) :

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

- votrefichier.p12 : Remplacez par votre nom de fichier réel.
- Vous devrez peut-être entrer le mot de passe du fichier .p12.
- cert.pem : Le certificat est-il extrait (sans la clé privée ou la chaîne CA) au format .pem (PEM) ?

Étape 2. Utilisez les commandes openssl suivantes pour afficher les détails du certificat et les attributs EKU.

a) Pour les fichiers .pem, utilisez la commande next openssl pour afficher les détails du certificat et les attributs EKU :

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

- cert.pem : Remplacez par votre nom de fichier réel.

b) Pour les fichiers .cer, utilisez la commande next openssl pour afficher les détails du certificat et les attributs EKU :

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

- votrefichier.cer : Remplacez par votre nom de fichier réel.

Étape 3. Ensuite, recherchez la section Extended Key Usage de X509v3 dans le résultat, vous pouvez voir des entrées comme "Authentification du serveur Web TLS" et "Authentification du client Web TLS" indiquant les valeurs EKU présentes dans le certificat.

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

OU l'attribut 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 d'EKU d'authentification du serveur : 1.3.6.1.5.5.7.3.1
- OID de l'UER d'authentification du client : 1.3.6.1.5.5.7.3.2

Exemple 1 : Ce certificat .pem (PEM) ne contient pas l'attribut EKU d'authentification client et inclut uniquement l'attribut EKU d'authentification serveur.

<#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
```

Exemple 2 : Ce certificat .pem (PEM) inclut les attributs EKU d'authentification client et serveur.

<#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
```

# Solution De Contournement

Les administrateurs peuvent choisir l'une des solutions de contournement suivantes.

## Option 1. Passer à des autorités de certification racine publiques qui fournissent des certificats EKU combinés

Certaines autorités de certification racines publiques, telles que DigiCert et IdenTrust, émettent des certificats avec des types EKU combinés (certificats serveur et clients) à partir d'une racine alternative, qui peut ne pas être incluse dans le magasin racine Chrome. Collaborer avec le fournisseur d’autorité de certification pour vérifier la disponibilité de ces certificats et, avant de les déployer, s’assurer que le serveur qui présente le certificat et les clients qui l’utilisent font confiance à l’autorité de certification racine correspondante.

Cette approche évite d'avoir à mettre à niveau le logiciel du serveur pour atténuer la temporisation de l'EKU d'authentification du client imposée par la politique du programme racine de Chrome.

Le tableau suivant, qui présente des exemples d'AC racine publiques et de types d'UER, n'est pas une liste exhaustive et n'est fourni qu'à titre d'exemple.

| Fournisseur CA | Type EKU | Autorité de certification racine | Émission/sous-AC |
|---|---|---|---|
| FiducieIden | clientAuth + serverAuth | IdenTrust Public Sector Root CA 1 | IdenTrust Public Sector Server CA 1 |
| FiducieIden | clientAuth | IdenTrust Public Sector Root CA 1 | TrustID RSA ClientAuth CA 2 |
| FiducieIden | serverAuth (navigateur approuvé) | IdenTrust - Racine commerciale CA 1 | Serveur HydrantID CA O1 |
| DigiCert | clientAuth + serverAuth | ID garanti DigiCert - Racine G2 | ID certifié DigiCert CA G2 |
| DigiCert | clientAuth | ID garanti DigiCert - | Client d'ID certifié DigiCert |

| Fournisseur CA | Type EKU | Autorité de certification racine | Émission/sous-AC |
|---|---|---|---|
| | | Racine G2 | CA G2 |
| DigiCert | serverAuth (navigateur approuvé) | Racine globale DigiCert G2 | DigiCert Global G2 TLS RSA SHA256 |

## Option 2. Renouveler les certificats actuels pour prolonger leur validité

Les certificats qui sont émis par des autorités de certification racines publiques avant mai 2026 et qui ont à la fois une clé d'authentification serveur et client continueront à être honorés jusqu'à l'expiration de leur durée. Cependant, il est préférable de renouveler les certificats EKU combinés avant que la temporisation de la stratégie ne se produise.

- Les dates de mise en oeuvre et de stratégie des autorités de certification publiques peuvent varier selon le fournisseur.
- Vérifiez auprès de l'autorité de certification et planifiez le renouvellement du certificat en conséquence.
- Après le 15 mars 2026, les certificats émis par une autorité de certification publique ne sont valides que pendant 200 jours.
- Tenez compte du fait que certaines autorités de certification publiques ont cessé de délivrer des certificats UER combinés.

## Option 3. Migrer vers une ICP privée pour émettre des certificats EKU (serveur et client) combinés

Évaluer la faisabilité de la transition vers une infrastructure à clé publique privée (PKI), puis configurer une autorité de certification privée pour émettre des certificats uniques avec des EKU combinés (certificats serveur et client avec les EKU requis).

Avant d’émettre ou de déployer un certificat, assurez-vous que le serveur qui présente le certificat et tous les clients qui l’utilisent font confiance à l’autorité de certification racine correspondante.

## Option 4. Obtenir un certificat de confiance publique avec seulement l'EKU d'authentification du client

Certaines autorités de certification, comme SSL.com, offrent des certificats d’authentification client dédiés. Ces certificats sont distincts des certificats TLS et généralement utilisés pour l’authentification d’entreprise.

⚠ Mise en garde : Pour les environnements de production, il est fortement recommandé aux clients d'utiliser des certificats avec les attributs EKU appropriés. Cette pratique garantit la sécurité, la compatibilité et le respect des normes du secteur et des meilleures pratiques. Les certificats sans attributs UER ne doivent être considérés que comme une solution de contournement temporaire et uniquement avec une compréhension claire des risques associés.

## Foire aux questions (FAQ)

Q1. Dois-je m'inquiéter de cela si j'utilise une ICP privée ?

R : La stratégie appliquée par les autorités de certification privées est déterminée par chaque organisation. Si votre autorité de certification privée adopte les mêmes critères d'émission, comme la suppression de l'attribut EKU d'authentification client des certificats, les directives fournies dans ce document s'appliquent.

Q2. Puis-je continuer à utiliser mes certificats existants ?

A : Oui, les certificats valides avec EKU combiné peuvent être utilisés jusqu'à l'expiration.

Q3. Quelles sont les options disponibles pour intégrer mon FMC ou FDM avec ISE via pxGrid si le certificat installé sur le FMC/FDM n'a pas l'attribut Client Authentication EKU ?

A : Outre les solutions de contournement proposées dans ce document, nous vous recommandons vivement de vérifier les références ISE suivantes :

- Avis de champ : FN74392 - Cisco Identity Services Engine : Impact sur les communications sécurisées à partir de l'authentification du client AC public EKU Modifications à partir de mai 2026 - Solution fournie

- Préparer Identity Services Engine pour les restrictions étendues d'utilisation des clés dans les certificats émis par les autorités de certification publiques

✎ Remarque : Même si l'utilisation d'un certificat signé par une autorité de certification publique est prise en charge pour IMS. Cisco recommande d'utiliser le certificat d'autorité de certification interne ISE, car cette communication ne concerne que les transactions internes.

Q4. Qu'est-ce que l'UKE « Authentification client » et pourquoi était-elle dans mon certificat ?

R : L'UER « Authentification client » indique qu'un certificat peut être utilisé par un client pour s'authentifier auprès d'un serveur. Certaines autorités de certification l'ont inclus dans les certificats TLS par défaut, mais il n'a jamais été nécessaire pour la sécurité normale des sites Web.

Q5. Mon certificat TLS actuel indique « Authentification client » sous son utilisation de clé étendue. Est-elle maintenant invalide ?

R : Non, il reste valide. Vous n'avez pas besoin de le remplacer immédiatement. Lorsque vous renouvelez, le nouveau certificat n'inclut tout simplement pas l'EKU d'authentification du client.

Q6. Comment puis-je vérifier si un certificat a l'EKU Auth du client ?

A : Vous pouvez vérifier les détails du certificat à l'aide des outils OpenSSL, PowerShell ou de l'interface utilisateur graphique pour vérifier l'extension Extended Key Usage.

Q7. Puis-je quand même obtenir un certificat de confiance publique avec seulement l'EKU d'authentification du client ?

A : Certaines autorités de certification, comme SSL.com, offrent des certificats d’authentification client dédiés. Ces certificats sont distincts des certificats TLS et généralement utilisés pour l’authentification d’entreprise.

Q8. Cela affecte-t-il d'autres unités clés ou types de certificats (signature de code, e-mail, etc.) ?

A : Non, cette modification est spécifique aux certificats de serveur TLS. Les certificats de signature de code et d'e-mail ont leurs propres exigences EKU.

Q9. Où puis-je consulter les exigences officielles relatives à ce changement ?

A : La politique du programme racine de Google Chrome fournit des directives sur l'interdiction de l'EKU d'authentification du client dans les certificats du serveur TLS.

Q10. Est-il sûr d’utiliser des certificats sans attributs EKU client et serveur dans mon environnement de production ?

R : Pour les environnements de production, il est fortement recommandé aux clients d'utiliser des certificats avec les attributs EKU appropriés. Cette pratique garantit la sécurité, la compatibilité et le respect des normes du secteur et des meilleures pratiques. Les certificats sans attributs UER

ne doivent être considérés que comme une solution de contournement temporaire et uniquement avec une compréhension claire des risques associés.

## Informations connexes

- Pour obtenir de l'aide supplémentaire, contactez le centre d'assistance technique de Cisco. Un contrat d'assistance valide est requis : Cisco Worldwide Support Contacts.
- Assistance et téléchargements Cisco : Assistance technique de Cisco et téléchargements

### Bogues associés

- CSCwt94492 ENH : FMC doit valider la présence de l'attribut EKU d'authentification client dans le certificat client utilisé pour l'intégration pxGrid
- CSCwt94509 ENH : FMC doit afficher un message indiquant que l'attribut Client Authentication EKU est requis dans le certificat client utilisé pour l'intégration pxGrid
- CSCwt61767 May 2026 EKU Server-Only Change - Émettez un avertissement de configuration ASA si EKU inadéquat
- CSCws83036 EKU : Évaluation de l'impact de l'application ClientAuth EKU dans ISE

### Références Cisco ISE

- Avis de champ : FN74392 - Cisco Identity Services Engine : Impact sur les communications sécurisées à partir de l'authentification du client AC public EKU Modifications à partir de mai 2026 - Solution fournie
- Préparer Identity Services Engine pour les restrictions étendues d'utilisation des clés dans les certificats émis par les autorités de certification publiques

### Références externes

- Politique du programme racine Chrome

- Portail IdenTrust

- SSL - Suppression de l'EKU d'authentification client des certificats de serveur TLS - Ce que vous devez savoir

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.