Cisco Secure Firewall Auswirkungen der Authentifizierung des öffentlichen CA-Clients Änderungen der EKU für sichere Kommunikation ab Mai 2026

Einleitung

In diesem Dokument werden die Auswirkungen der Einschränkungen bei den Kriterien für die Zertifikatsausstellung beschrieben, die von Zertifizierungsstellen festgelegt wurden, die das Chrome Root Certificate-Programm erfüllen, insbesondere in Bezug auf die Cisco Secure Firewall-Produkte.

Hintergrundinformationen

Öffentlich vertrauenswürdige TLS-Zertifikate werden von Zertifizierungsstellen ausgestellt, die Branchenrichtlinien zur Zertifikatausstellung und -nutzung erfüllen müssen.

DieChrome Root Program Policy, betrieben von Google, definiert Anforderungen, die CAs befolgen müssen, damit ihre Zertifikate vom Google Chrome-Browser als vertrauenswürdig eingestuft werden können. Diese Anforderungen beeinflussen, wie öffentlich vertrauenswürdige Zertifikate branchenweit ausgestellt werden. Als Teil der sich entwickelnden Sicherheitsverfahren, die Chrome Root-Programm ist die Einführung strengerer Anleitung für die Verwendung von Zertifikaten.

Viele öffentliche Zertifizierungsstellen geben daher keine Zertifikate mehr aus, die die Clientauthentifizierungs-EKU enthalten, sondern gehen in Richtung, Zertifikate auszustellen, die nur für die Serverauthentifizierung bestimmt sind. Daher werden neu ausgegebene Zertifikate von vielen öffentlichen Zertifizierungsstellen nur die Serverauthentifizierungs-EKU enthalten.

Die erweiterte Schlüsselverwendung (Extended Key Usage, EKU) ist eine Zertifikaterweiterung, die die beabsichtigte Funktion eines öffentlichen Schlüssels in einem digitalen Zertifikat definiert. Es wird eine strukturierte Gruppe zulässiger Anwendungen erstellt, die sicherstellt, dass der Schlüssel nur für bestimmte kryptografische Operationen verwendet wird. Diese Funktionalität wird durch Objektkennungen (OIDs) gesteuert. Hierbei handelt es sich um eindeutige numerische Kennungen, die jede zulässige Verwendung kategorisieren, z. B. Codesignatur, Serverauthentifizierung, Clientauthentifizierung oder sichere E-Mail.

Wenn die Authentifizierung zertifikatbasiert ist, überprüft die überprüfende Entität das Zertifikat, um die Objektkennung (OID) in der EKU zu identifizieren. Durch das Einbetten der EKU-Erweiterung beschränkt eine Zertifizierungsstelle (Certificate Authority, CA) den Gültigkeitsbereich des Zertifikats auf vordefinierte Rollen, wobei jeder festgelegte Zweck explizit einer OID zugeordnet wird.

Zweck von EKU-Attributen

- Definition der Verwendung: EKU-Attribute geben an, welche Authentifizierungs- oder Verschlüsselungstypen das Zertifikat ausführen darf.

- Erhöhung der Sicherheit: Durch die Beschränkung von Zertifikaten auf bestimmte Verwendungszwecke hilft die EKU, Missbrauch oder unbeabsichtigte Anwendungen zu verhindern (z. B. kann ein Serverzertifikat nicht für die Client-Authentifizierung verwendet werden).

- Compliance: Stellt sicher, dass Zertifikate gemäß Sicherheitsrichtlinien und Branchenstandards verwendet werden.

Hauptverwendungen von EKU-Attributen

1. TLS-Web-Client-Authentifizierung

- Ermöglicht die Verwendung von Zertifikaten zur Identifizierung und Authentifizierung von Benutzern oder Geräten gegenüber einem Server.

- OID: 1.3.6.1.5.5.7.3.2

- Verwendung in VPNs, gegenseitigem TLS und Szenarien für sichere Anmeldung.

2. TLS-Webserverauthentifizierung

- Ermöglicht die Verwendung von Zertifikaten durch Server zum Nachweis ihrer Identität gegenüber Clients.

- OID: 1.3.6.1.5.5.7.3.1

- Wird in HTTPS-, SSL/TLS-Webservern und sicheren API-Endpunkten verwendet.

3. Codesignatur

- Das Zertifikat kann zum Signieren von Software oder ausführbaren Dateien verwendet werden.

- OID: 1.3.6.1.5.5.7.3.3

- Verwendung bei Softwareverteilungs- und Integritätsprüfungen.

4. E-Mail-Schutz

- Zertifikate können zum Signieren und Verschlüsseln von E-Mail-Nachrichten verwendet werden.

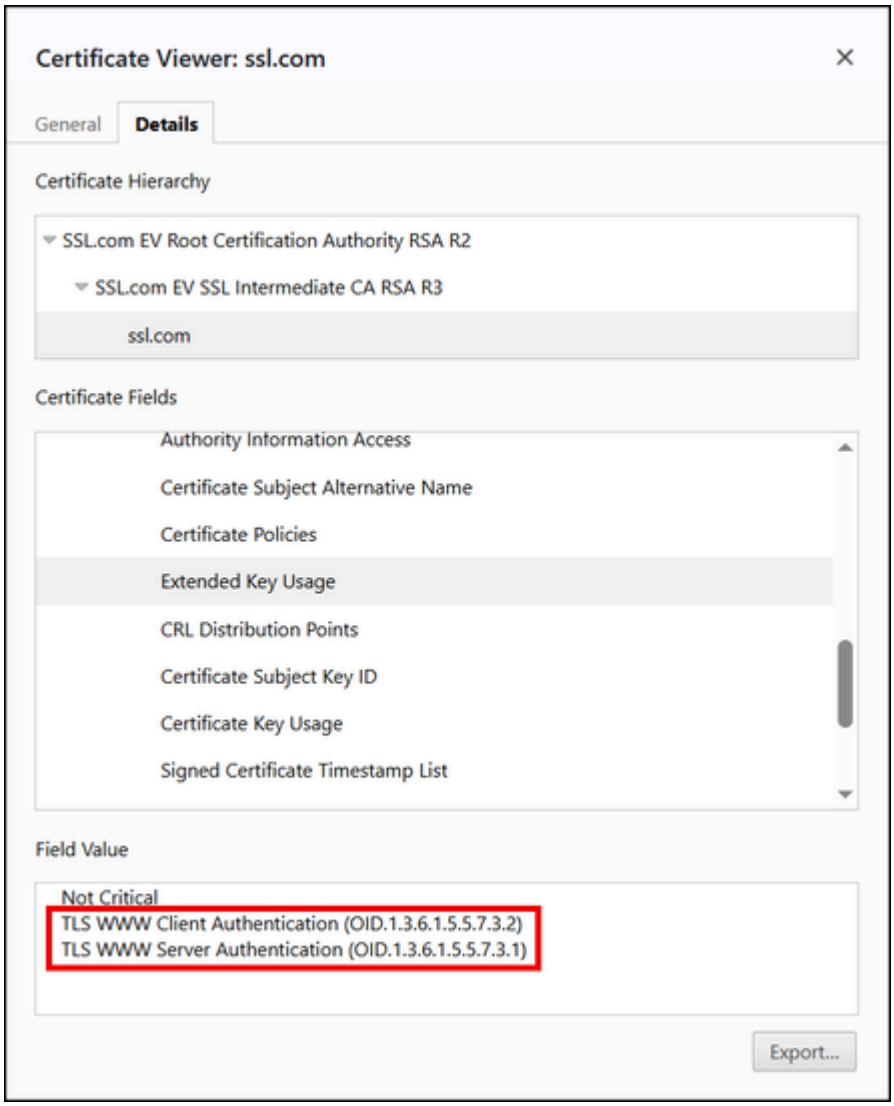
- OID: 1.3.6.1.5.5.7.3.4

- Wird in S/MIME-E-Mail-Sicherheit verwendet.

5. Sonstige Zwecke

- Dokumentensignierung, Zeitstempel, Smartcard-Anmeldung usw., jeweils mit eigenen OIDs.

Browser und Server benötigen die serverAuth EKU nur, um eine sichere Verbindung für HTTPS herzustellen. Früher enthielten viele TLS-Serverzertifikate sowohl die serverAuth- als auch die clientAuth-EKUs. Ein Beispiel für ein solches Zertifikat:



Warum wird die Client Authentication EKU aus den Serverzertifikaten entfernt?

- Sicherheit und Umfang: Öffentliche TLS-Zertifikate sollen nur Server im Web authentifizieren. Durch die Entfernung wird eine klare Trennung zwischen Server- und Client-Funktionen erreicht. Die ClientAuth EKU wird für die Authentifizierung von Maschinen und Benutzern mit Mutual TLS (mTLS) und anderen Authentifizierungsszenarien verwendet.

- Fehlkonfiguration verhindern: Einige Systeme vertrauen möglicherweise jedem Zertifikat einer öffentlichen Zertifizierungsstelle für die Clientauthentifizierung, wenn die EKU vorhanden ist. Dies kann ein Sicherheitsrisiko darstellen.

- Browser-Anforderungen: Wichtige Browser erfordern keine ClientAuth EKU im Zertifikat einer Website oder überprüfen sie nicht.

- Vereinfachte PKI-Architektur: Durch die Trennung von Verwendungen können Zertifizierungsstellen unterschiedliche Zertifikathierarchien für Server-TLS im Vergleich zu anderen Zwecken verwalten.

Dies ist besonders wichtig für Produkte wie die Cisco Secure Firewall Adaptive Security Appliance (ASA), die Cisco Secure Firewall Threat Defense (FTD), den Cisco Secure Firewall Device Manager (FDM) und das Cisco Secure Firewall Management Center (FMC), die je nach Anwendungsfall während der TLS-Authentifizierung als Server oder Client fungieren können.

Auswirkungen auf Serverumgebungen

Bei den meisten Serverbereitstellungen wird diese Änderung nur geringe oder keine Auswirkungen haben. Folgendes ist zu erwarten:

- Standard-Webserver (HTTPS): keine Auswirkungen. Die aktualisierten Zertifikate funktionieren weiterhin normal.
- Bestehende Zertifikate: Alle Zertifikate, die vor der Unterbrechung ausgestellt wurden, funktionieren so lange, bis sie ablaufen.
- Gegenseitiges TLS (mTLS) und Clientzertifikatszenarien: Wenn Sie ein TLS-Serverzertifikat für die Clientauthentifizierung verwendet haben, müssen Sie ein separates Zertifikat für die clientAuth EKU von einer anderen Quelle beziehen.
- Unternehmenssysteme, die beide EKUs erfordern: Einige Alt- oder Unternehmenssysteme haben beide EKUs erwartet. Überprüfen Sie, ob Updates erforderlich sind, um die neuen Regeln einzuhalten.

Problembeschreibung

Ab Mai 2026 stellen viele öffentliche Zertifizierungsstellen keine Transport Layer Security (TLS)-Zertifikate mehr aus, die die erweiterte Clientauthentifizierungsschlüsselverwendung (EKU) enthalten. Neu ausgestellte Zertifikate enthalten in der Regel nur die Serverauthentifizierungs-EKU.

Wenn die von einer öffentlichen Zertifizierungsstelle ausgestellten Zertifikate gemäß den aktualisierten Zertifizierungsstellenrichtlinien erneuert und dann in den Cisco Secure Firewall-Produkten bereitgestellt werden, schlagen die Dienste fehl, für die eine Clientauthentifizierungs-EKU erforderlich ist. Folgende Services sind betroffen:

- Wenn die ASA, FTD, FDM oder FMC als Client fungiert - z. B. bei der Verbindung mit Identitätsanbietern oder Authentifizierungsservern wie ISE (pxGrid), RADIUS, LDAPS oder Active Directory - kann die zertifikatbasierte Authentifizierung fehlschlagen, wenn das Clientzertifikat von einer öffentlichen Zertifizierungsstelle generiert wurde und die Clientauthentifizierungs-EKU fehlt. Wenn der Authentifizierungsserver in diesen Szenarien Zertifikate ohne die erforderliche EKU zurückweist, kann es zu Verbindungsfehlern kommen.

- Der Cisco Secure Client (ehemals AnyConnect) kann sich bei ASA- oder FTD-Servern mithilfe von Zertifikaten authentifizieren. Wenn das Clientzertifikat jedoch von einer öffentlichen Zertifizierungsstelle generiert wurde und die Clientauthentifizierungs-EKU fehlt, schlägt die RAVPN-Verbindung (Remote Access VPN) fehl.

- Wenn die FTD oder ASA einen Site-to-Site-VPN-Tunnel - sei es zu einer anderen FTD, ASA, einem Cisco Router oder einem VPN-Peer eines Drittanbieters - mit Zertifikatsauthentifizierung (RSA oder ECDSA) erstellt, schlägt der Tunnel fehl, wenn das von einer öffentlichen Zertifizierungsstelle generierte Identitätszertifikat nicht über das EKU-Attribut für die Client-Authentifizierung verfügt. Dies liegt daran, dass der Remote-VPN-Peer die Clientauthentifizierungs-EKU im Identitätszertifikat benötigt.

Änderung der Chrome-Stammprogrammrichtlinie

Die Implementierung der EKU hängt von der CA ab, die das Zertifikat signiert. Die Verwendung von EKU für die Serverauthentifizierung und die Clientauthentifizierung war eine gängige Praxis. Im Rahmen der Richtlinienänderungen des Chrome-Stammprogramms werden jedoch Zertifizierungsstellen, die auf diese Zertifikatausstellungskriterien abgestimmt sind, die Signierung von TLS-Zertifikaten mit der erweiterten Schlüsselverwendung für die Clientauthentifizierung (EKU) einstellen. Neu ausgestellte Zertifikate enthalten nur die Serverauthentifizierungs-EKU.

Wichtige Richtlinienanforderungen

- Öffentliche Stammzertifizierungsstellen müssen nur die erweiterte Schlüsselverwendung (Extended Key Usage, EKU) für die Serverauthentifizierung (id-kp-serverAuth) geltend machen

- Zertifikate müssen NUR Serverauthentifizierungs-EKU enthalten.

- Die Aufnahme von Clientauthentifizierungs-EKU in diese Zertifikate ist nicht zulässig.

- Stammzertifizierungsstellen, die weiterhin Zertifikate mit der Clientauthentifizierungs-EKU ausstellen, werden schließlich aus dem Chrome-Stammspeicher entfernt, was dazu führt, dass solche Zertifikate vom Chrome-Browser als "Nicht vertrauenswürdig" gekennzeichnet werden

Zeitplan

- Im September 2025 wird SSL.com TLS-Zertifikate ausstellen, die nur die ServerAuth EKU (und nicht ClientAuth) für Serverzertifikate enthalten. Mit anderen Worten, neue SSL/TLS-Zertifikate für Ihre Website oder Ihren Server werden explizit nur für die "Server-Authentifizierung" verwendet.

- Oktober 2025: CAs, die sich auf das Programm abstimmen (z. B. DigiCert, Sectigo usw.), haben standardmäßig

mit der Ausgabe von Zertifikaten begonnen, die nur für Server bestimmt sind.

- Mai 2026: CAs, die sich auf das Programm abstimmen, stellen keine Client Authentication EKU-Zertifikate mehr aus

- März 2027: Chrome Root-Programm-Richtlinie wird voll wirksam

Auswirkung auf Cisco Secure Firewall-Produkte

Nachdem die öffentlichen Zertifizierungsstellen begonnen haben, nur noch die Serverauthentifizierungs-EKU in die ausgestellten Zertifikate aufzunehmen. Dies könnte die folgenden Auswirkungen auf die nächsten Cisco Secure Firewall-Produktszenarien haben:

- Wenn die ASA, FTD, FDM oder FMC als Client fungiert - z. B. bei der Verbindung mit Identitätsanbietern oder Authentifizierungsservern wie ISE (pxGrid), RADIUS, LDAPS oder Active Directory - kann die zertifikatbasierte Authentifizierung fehlschlagen, wenn das Clientzertifikat von einer öffentlichen Zertifizierungsstelle generiert wurde und die Clientauthentifizierungs-EKU fehlt. Wenn der Authentifizierungsserver in diesen Szenarien Zertifikate ohne die erforderliche EKU zurückweist, kann es zu Verbindungsfehlern kommen.

- Der Cisco Secure Client (ehemals AnyConnect) kann sich bei ASA- oder FTD-Servern mithilfe von Zertifikaten authentifizieren. Wenn das Clientzertifikat jedoch von einer öffentlichen Zertifizierungsstelle generiert wurde und die Clientauthentifizierungs-EKU fehlt, schlägt die RAVPN-Verbindung (Remote Access VPN) fehl.

- Wenn die FTD oder ASA einen Site-to-Site-VPN-Tunnel - sei es zu einer anderen FTD, ASA, einem Cisco Router oder einem VPN-Peer eines Drittanbieters - mit Zertifikatsauthentifizierung (RSA oder ECDSA) erstellt, schlägt der Tunnel fehl, wenn das von einer öffentlichen Zertifizierungsstelle generierte Identitätszertifikat nicht über das EKU-Attribut für die Client-Authentifizierung verfügt. Dies liegt daran, dass der Remote-VPN-Peer die Clientauthentifizierungs-EKU im Identitätszertifikat benötigt.

Hinweis: Wenn Sie FMC oder FDM über pxGrid in die ISE integrieren und die auf Ihrem FMC/FDM installierten Zertifikate nicht über das EKU-Attribut für die Clientauthentifizierung verfügen, überprüfen Sie die in diesem Dokument und den nächsten ISE-Referenzen vorgeschlagenen Problemumgehungen: FN74392 und Vorbereiten der Identity Services Engine für erweiterte Schlüsselverwendungsbeschränkungen in von öffentlichen Zertifikaten Zertifizierungsstellen.

Anmerkung: Das Entfernen der clientAuth EKU aus TLS-Serverzertifikaten ist eine branchenweite Richtlinienänderung, die die Sicherheit erhöht und Missbrauch verhindert. Für die meisten Benutzer wird es keine spürbaren Auswirkungen geben. Wenn Sie sich jedoch auf die ClientAuth-EKU verlassen, sollten Sie proaktive Schritte unternehmen, um den richtigen Zertifikatstyp für Ihre Anforderungen zu erhalten.

Betroffene Produkte

<table>
<tr><th>Cisco Secure Firewall-Produkt</th><th>Software-Version</th><th>Betroffene Szenarien</th><th>Problembehebung</th></tr>
<tr><td>FTD</td><td>Alle Versionen</td><td rowspan="4">Wenn als Client fungiert (z. B. bei der Verbindung mit Identitätsanbietern oder Authentifizierungsservern wie ISE (pxGrid), RADIUS, LDAPS oder Active Directory), kann die zertifikatbasierte Authentifizierung fehlschlagen, wenn das Clientzertifikat von einer öffentlichen Zertifizierungsstelle generiert wurde und die Clientauthentifizierungs-EKU fehlt. In diesem Szenario kann es zu Verbindungsfehlern kommen, wenn der Authentifizierungsserver Zertifikate ohne die erforderliche EKU zurückweist.</td><td rowspan="5">Option 1. Wenn Sie ein TLS-Serverzertifikat für die Client-Authentifizierung verwenden, müssen Sie ein Zertifikat mit der ClientAuth EKU von einer anderen Quelle beziehen.

ODER

Option2. Wechseln Sie zu öffentlichen Stammzertifizierungsstellen (Zertifizierungsstellen), die kombinierte EKU-Zertifikate (ClientAuth und ServerAuth) bereitstellen.

HINWEIS: Weitere Optionen finden Sie im Abschnitt Problemumgehungen dieses Dokuments.</td></tr>
<tr><td>FDM</td><td>Alle Versionen</td></tr>
<tr><td>FMC</td><td>Alle Versionen</td></tr>
<tr><td>ASA</td><td>Alle Versionen</td></tr>
<tr><td>Cisco Secure Client (ehemals AnyConnect)</td><td>Alle Versionen</td><td>Der Cisco Secure Client kann sich mithilfe von Zertifikaten bei den ASA- oder FTD-Servern authentifizieren. Wenn das Clientzertifikat jedoch von einer öffentlichen Zertifizierungsstelle generiert wurde und die Clientauthentifizierungs-EKU fehlt, schlägt die RAVPN-Verbindung (Remote Access VPN) fehl.</td></tr>
</table>

FTD oder ASA	Alle Versionen	Wenn die FTD oder ASA einen Site-to-Site-VPN-Tunnel - sei es zu einer anderen FTD, ASA, einem Cisco Router oder einem VPN-Peer eines Drittanbieters - mit Zertifikatsauthentifizierung (RSA oder ECDSA) erstellt, schlägt der VPN-Tunnel fehl, wenn das von einer öffentlichen CA generierte Identitätszertifikat nicht über das EKU-Attribut für die Client-Authentifizierung verfügt. Dies liegt daran, dass der Remote-VPN-Peer die Clientauthentifizierungs-EKU im Identitätszertifikat benötigt.	

Hinweis: Wenn Sie FMC oder FDM über pxGrid in die ISE integrieren und die auf Ihrem FMC/FDM installierten Zertifikate nicht über das EKU-Attribut für die Clientauthentifizierung verfügen, überprüfen Sie die in diesem Dokument und den nächsten ISE-Referenzen vorgeschlagenen Problemumgehungen: FN74392 und Vorbereiten

der Identity Services Engine für erweiterte Schlüsselverwendungsbeschränkungen in von öffentlichen Zertifikaten Zertifizierungsstellen.

Anmerkung: Das Entfernen der clientAuth EKU aus TLS-Serverzertifikaten ist eine branchenweite Richtlinienänderung, die die Sicherheit erhöht und Missbrauch verhindert. Für die meisten Benutzer wird es keine spürbaren Auswirkungen geben. Wenn Sie sich jedoch auf die ClientAuth-EKU verlassen, sollten Sie proaktive Schritte unternehmen, um den richtigen Zertifikatstyp für Ihre Anforderungen zu erhalten.

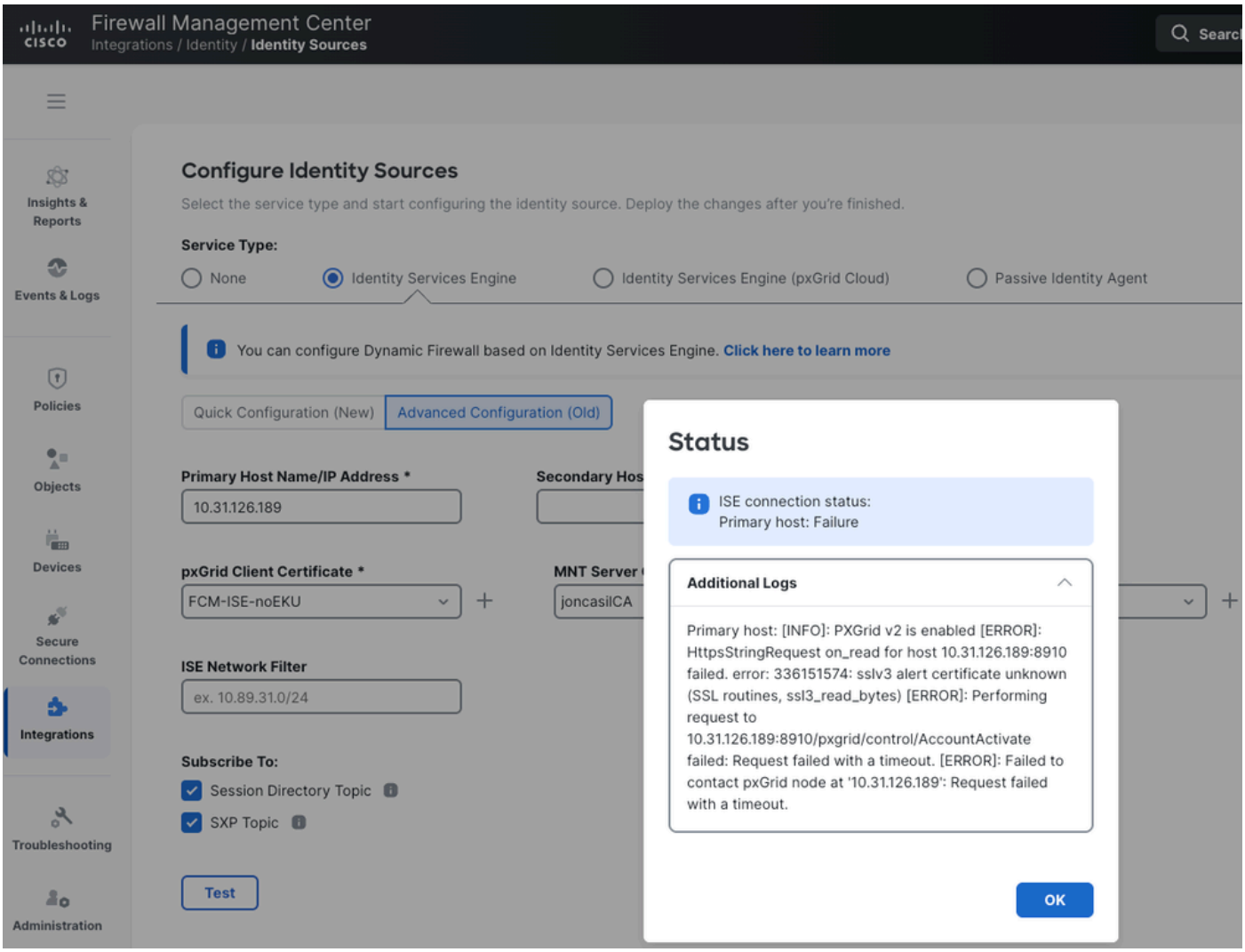
Vorsicht: Für Produktionsumgebungen wird dringend empfohlen, dass Kunden Zertifikate mit den entsprechenden EKU-Attributen verwenden. Diese Vorgehensweise gewährleistet Sicherheit, Kompatibilität und Einhaltung von Branchenstandards und Best Practices. Zertifikate ohne EKU-Attribute sollten nur als vorübergehender Workaround betrachtet werden und nur mit einem klaren Verständnis der damit verbundenen Risiken.

Problem 1. pxGrid-Integrationsproblem zwischen FMC und ISE, wenn das FMC-Zertifikat kein EKU-Attribut für die Client-Authentifizierung aufweist

In diesem Szenario fehlt dem vom FMC für die pxGrid-Integration mit der ISE verwendeten Zertifikat das EKU-Attribut für die Client-Authentifizierung. Daher schlägt die pxGrid-Integration fehl, da der ISE-Server erwartet, dass dieses Attribut im vom FMC vorgelegten Zertifikat vorhanden ist.

Topologie

FMC-UI-Fehler: Dies ist die Fehlermeldung, die im FMC angezeigt wird, wenn das vom FMC verwendete Zertifikat nicht über das EKU-Attribut für die Client-Authentifizierung für die pxGrid-Integration mit ISE verfügt.



FMC-CLI-Fehler: Dieselben Fehlermeldungen befinden sich im Verzeichnis 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

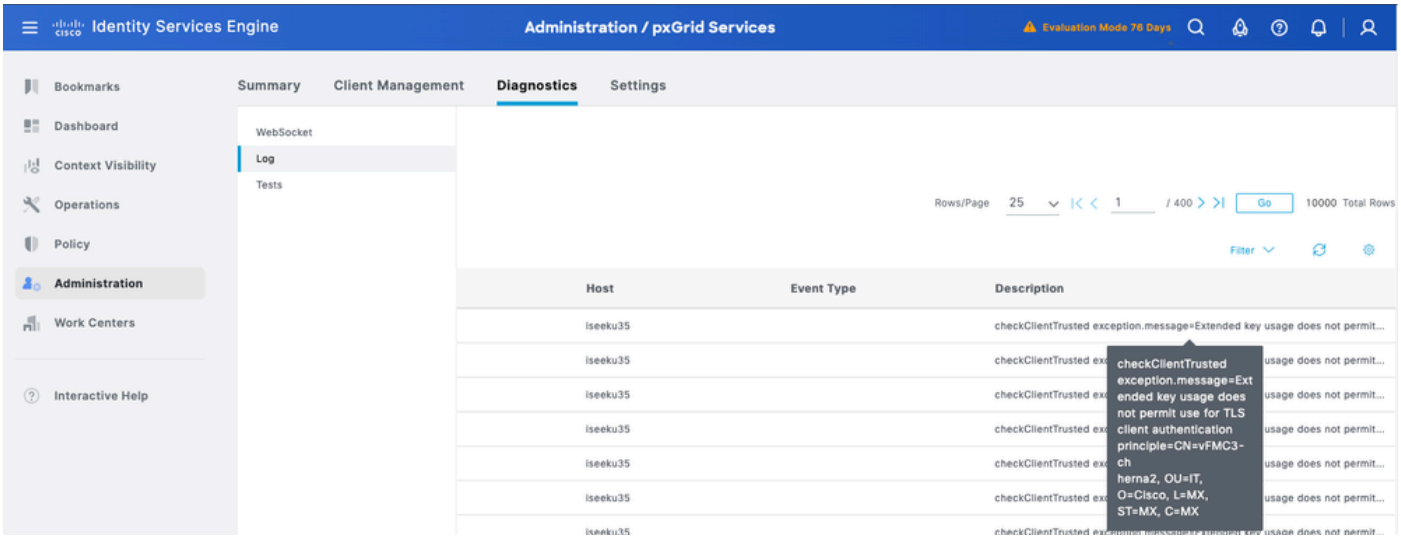
[ERROR] Performing request to 10.31.126.189:8910/pxgrid/control/AccountActivate failed: Request failed w

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-Fehler: Dies ist die in ISE angezeigte Fehlermeldung "checkClientTrusted exception.message=Extended key usage does not permit use for TLS client authentication principle=CN=vFMC3-chherna2, OU=IT, O=Cisco, L=MX, ST=MX, C=MX".



Lösung: Wenn Sie FMC oder FDM über pxGrid in die ISE integrieren und das in Ihrem FMC/FDM installierte Zertifikat nicht über das EKU-Attribut für die Clientauthentifizierung verfügt, lesen Sie den Vorschlag in diesem Dokument und in den nächsten ISE-Referenzen: FN74392 und Vorbereitung der Identity Services Engine für erweiterte Schlüssel-Nutzungsbeschränkungen in Zertifikaten, die von einer öffentlichen Zertifizierung ausgestellt wurden. Behörden für eine erfolgreiche pxGrid-Integration.

Anmerkung: Das FMC pxGrid-Clientzertifikat muss entweder das ClientAuth EKU-Attribut enthalten oder überhaupt kein Client- oder Server-EKU-Attribut enthalten.

Anmerkung: Auch wenn die Verwendung eines öffentlichen, von einer Zertifizierungsstelle signierten Zertifikats für IMS unterstützt wird. Cisco empfiehlt die Verwendung des ISE Internal CA-Zertifikats, da diese Kommunikation nur für interne Transaktionen verwendet wird.

Problem 2. FTD- oder ASA-Integrationsproblem mit einem LDAPS-Server, wenn das vorgelegte Zertifikat kein Client Authentication EKU-Attribut aufweist

In diesem Szenario fungiert die FTD oder ASA als Client für die Integration in einen LDAPS-Server mittels Zertifikatsauthentifizierung. Wenn das vom FTD oder ASA verwendete Zertifikat nicht über das EKU-Attribut für die Clientauthentifizierung verfügt, schlägt die Integration fehl, da der LDAPS-Server das Vorhandensein dieses Attributs im Zertifikat voraussetzt.

Topologie

LDAPS-Serverfehler: TLS-Zertifikatsprüfung: Fehler, nicht unterstützter Zertifikatzweck' und 'TLS-Ablaufverfolgung: SSL3-Warnung schreiben:fatal:nicht unterstütztes Zertifikat'

```
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
```

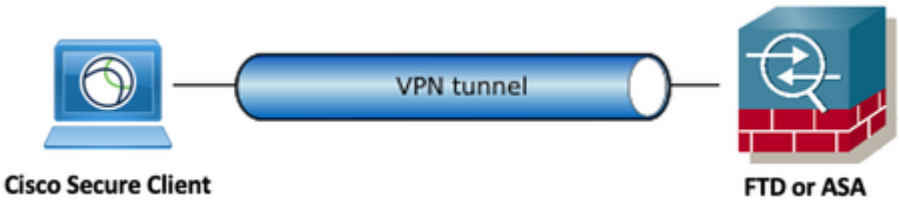
Lösung: Lesen Sie die in diesem Dokument vorgeschlagenen durch, um sicherzustellen, dass FTD oder ASA das korrekte Identitätszertifikat - einschließlich des EKU-Attributs für die Client-Authentifizierung - für eine erfolgreiche zertifikatbasierte Authentifizierung mit dem LDAPS-Server

verwendet.

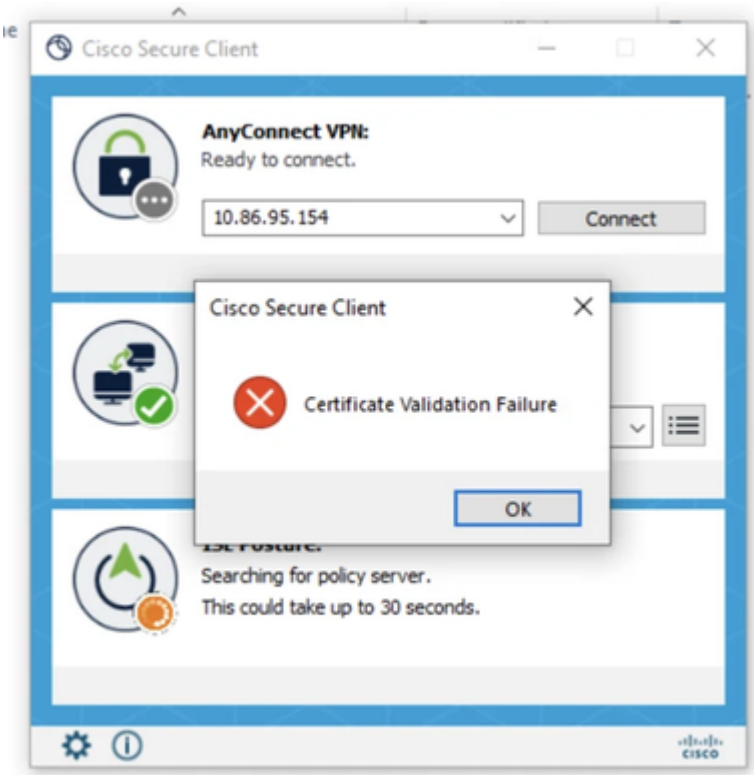
Problem 3. Beim Cisco Secure Client (ehemals AnyConnect) können Verbindungsprobleme mit einem FTD oder einer ASA auftreten, wenn das Client-Zertifikat nicht über das EKU-Attribut für die Client-Authentifizierung verfügt.

In diesem Szenario verwendet der Cisco Secure Client die Zertifikatsauthentifizierung, um einen RAVPN-Tunnel zum FTD oder zur ASA einzurichten. Wenn das Clientzertifikat jedoch nicht das EKU-Attribut für die Clientauthentifizierung enthält, schlägt die RAVPN-Sitzung fehl, da dieses Attribut von der ASA oder FTD im Clientzertifikat angegeben werden muss.

Topologie



Cisco Secure Client-Fehler: Fehler bei der Zertifikatsvalidierung



Cisco Secure Client DART-Fehler: Die folgenden Protokolle aus der Datei AnyConnectVPN.txt im DART-

Paket bestätigen, dass der Cisco Secure Client das für die RAVPN-zertifikatbasierte Authentifizierung verwendete Zertifikat an die FTD/ASA aufgrund des Fehlens des EKU-Attributs für die Client-Authentifizierung zurückgewiesen hat (Navigieren Sie im DART-Paket zur Datei AnyConnectVPN.txt, um die Datei zu finden. Secure Client > AnyConnect VPN > Protokolle > 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]

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

Lösung: Lesen Sie den Vorschlag in diesem Dokument, um sicherzustellen, dass der Cisco Secure Client das richtige Zertifikat - einschließlich des EKU-Attributs für die Client-Authentifizierung - für eine erfolgreiche zertifikatbasierte Authentifizierung mit FTD oder ASA verwendet.

Anmerkung: Aus obigem DART-Paketfehler: 'EKU nicht im Zertifikat gefunden: 1.3.6.1.5.5.7.3.2', diese Nummer "1.3.6.1.5.5.7.3.2" entspricht der Client Authentication EKU OID.

Problem 4: Fehler bei Site-to-Site-VPN-Tunneln mit zertifikatbasierter Authentifizierung, wenn das Identitätszertifikat nicht über das EKU-Attribut für die Clientauthentifizierung verfügt.

In diesem Szenario, das eine zertifikatbasierte Authentifizierung für einen IKEv2-Site-to-Site-VPN-Tunnel umfasst, fehlt dem Identitätszertifikat, das von FTD/ASA (1) zum Einrichten des Tunnels zum FTD/ASA (2)-Peer verwendet wird, das EKU-Attribut für die Client-Authentifizierung. Aus diesem Grund kann der VPN-Tunnel nicht eingerichtet werden, da der Remote-Peer, FTD/ASA (2), das Vorhandensein dieses Attributs im Zertifikat erfordert.

Topologie

FTD- oder ASA CLI-Fehler: Dies sind die Fehler, die auf der FTD/ASA (2) während der IKEv2-zertifikatbasierten Authentifizierung beobachtet wurden, wenn das FTD/ASA (1)-Identitätszertifikat zurückgewiesen wurde, für das das EKU-Attribut für die Client-Authentifizierung fehlt.

<#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
```

Anmerkung: Im obigen Beispiel verwendete FTD/ASA (2) ein Identitätszertifikat, das sowohl das ClientAuth- als auch das ServerAuth-EKU-Attribut enthielt.

Anmerkung: Im obigen Beispiel könnte FTD/ASA (2) auch durch einen Router oder einen physischen oder Cloud-basierten VPN-Konzentrator eines Drittanbieters ersetzt werden. In diesem Fall tritt das gleiche Problem weiterhin auf, da der VPN-Peer das EKU-Attribut für die Clientauthentifizierung benötigt, das in dem von FTD/ASA (1) für die erfolgreiche zertifikatbasierte Authentifizierung verwendeten Zertifikat enthalten sein muss.

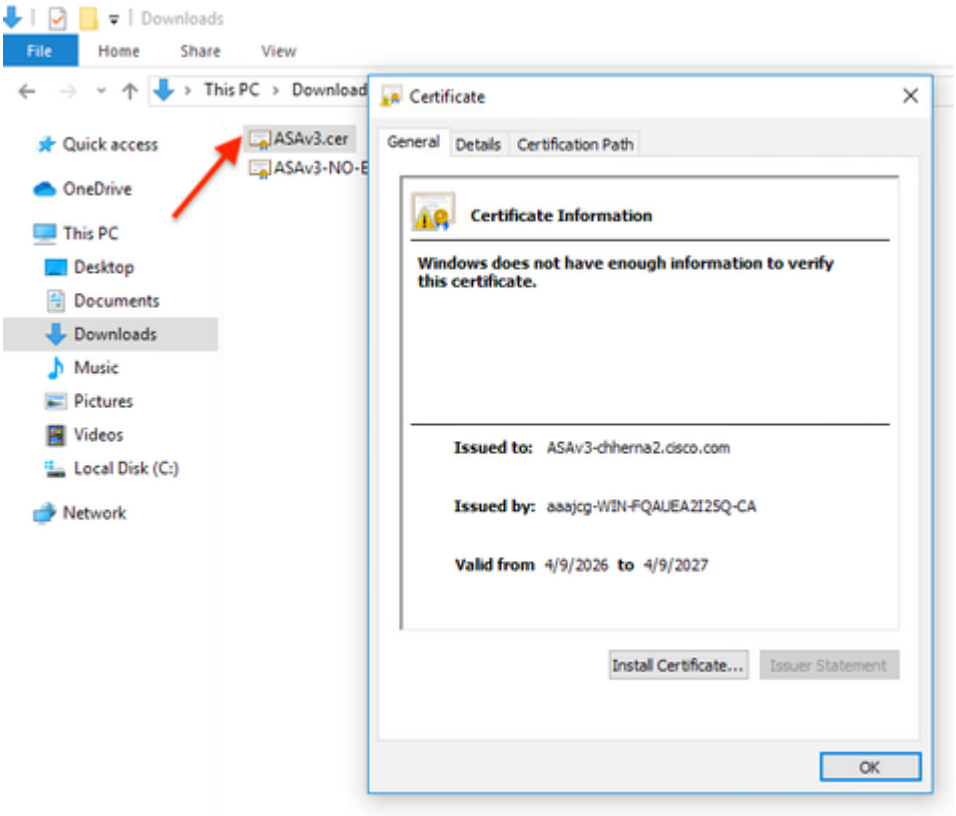
Lösung: Lesen Sie den Vorschlag in diesem Dokument, um sicherzustellen, dass FTD/ASA (1) das richtige Identitätszertifikat - einschließlich des EKU-Attributs für die Client-Authentifizierung - für einen erfolgreichen Site-to-Site-VPN-Tunnel mit zertifikatbasierter Authentifizierung verwendet.

Anweisungen zum Überprüfen, ob das EKU-Attribut für die Clientauthentifizierung des Zertifikats fehlt

Überprüfen der EKU-Attribute eines CER-Zertifikats mit dem Windows-Zertifikats-Manager

Führen Sie die folgenden Schritte aus, um die EKU-Attribute eines CER-Zertifikats mit dem Windows-Zertifikats-Manager zu überprüfen:

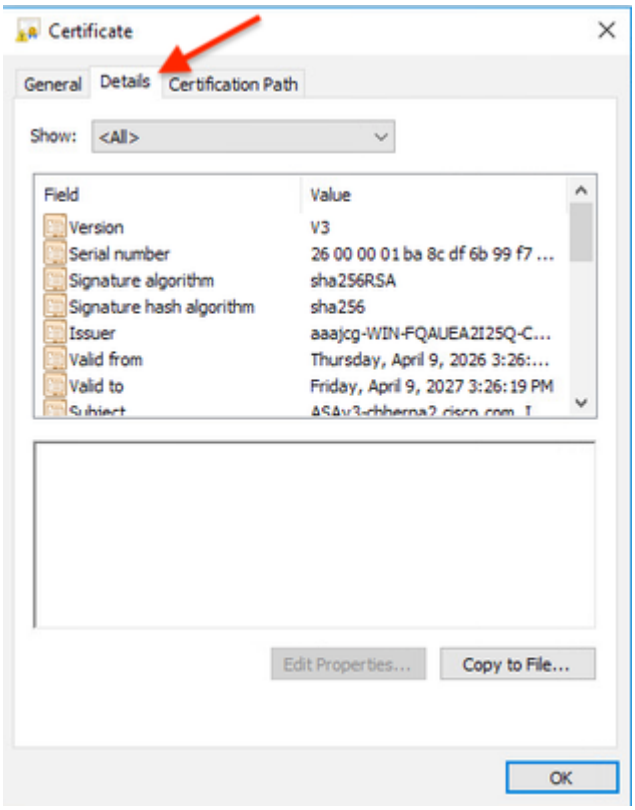
Schritt 1: Doppelklicken Sie auf die CER-Datei, um sie im Windows-Zertifikats-Manager zu öffnen.



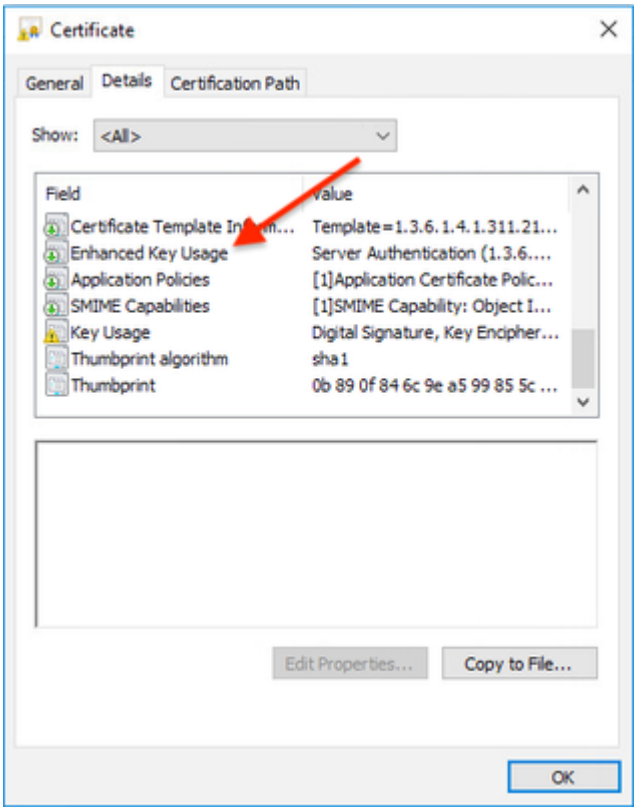
Anmerkung: Nur CER-Dateien können direkt auf diese Weise geöffnet werden. Wenn Ihr Zertifikat die Erweiterung .pem hat, benennen Sie es zuerst in .cer oder .crt um.

Schritt 2. Behandeln Sie ggf. die Sicherheitswarnung. Wenn eine Sicherheitswarnung angezeigt wird, klicken Sie auf Öffnen, um fortzufahren.

Schritt 3. Klicken Sie im Zertifikatfenster auf die Registerkarte Details.

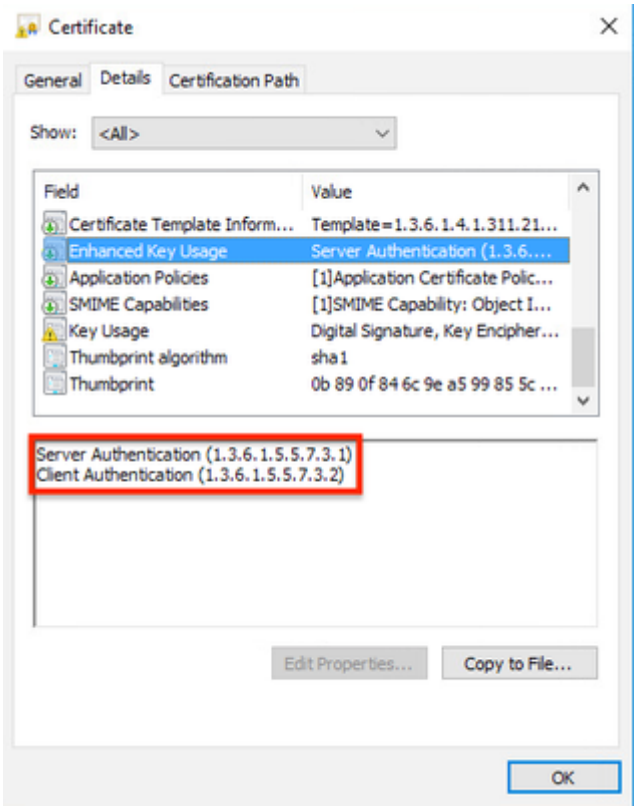


Schritt 4: Blättern Sie durch die Liste der Felder, und wählen Sie "Erweiterte Schlüsselverwendung" (oder "Erweiterte Schlüsselverwendung") aus.



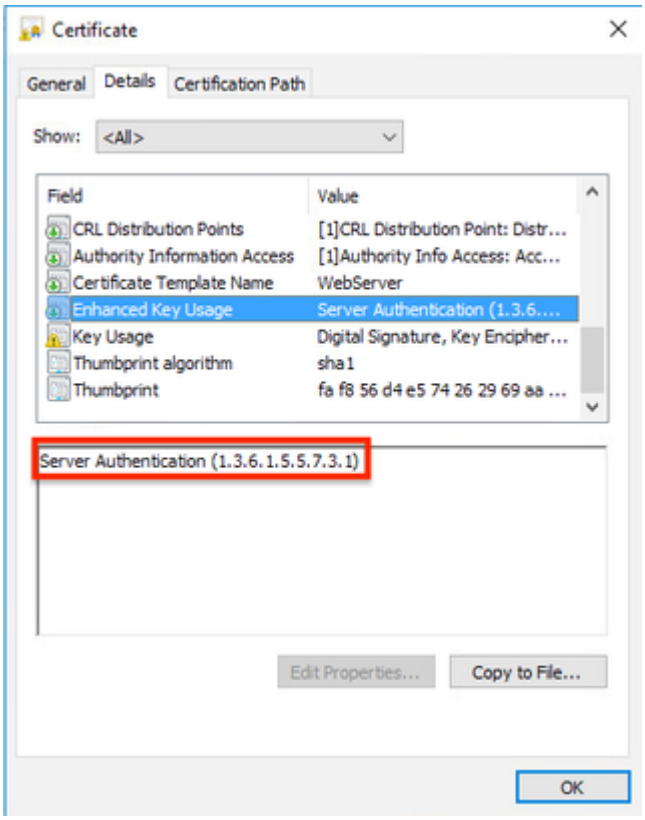
Schritt 5. Überprüfen Sie die EKU-Attribute. Möglicherweise werden Einträge wie "Server Authentication" und "Client Authentication" angezeigt, die die im Zertifikat vorhandenen EKU-

Werte angeben.

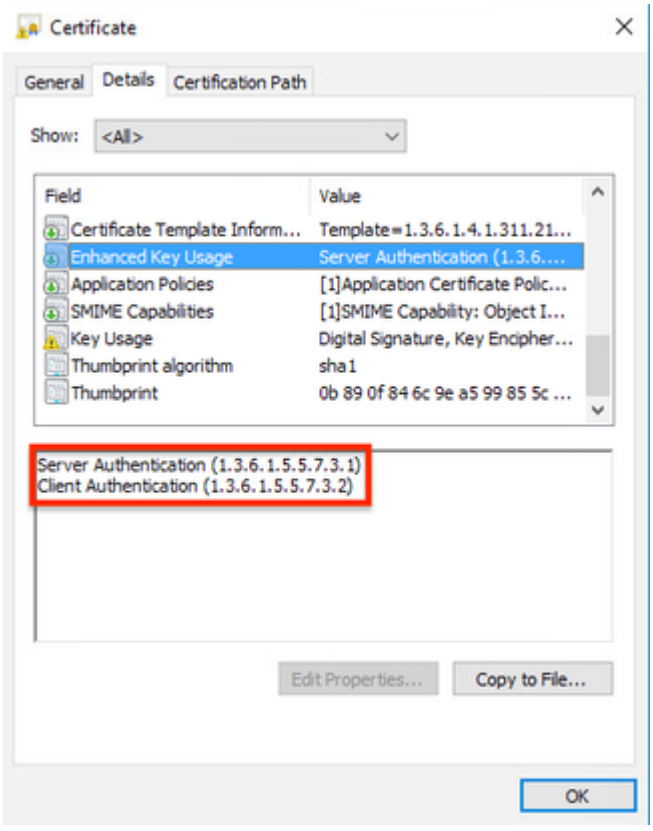


Schritt 6. Klicken Sie nach der Überprüfung auf OK, um das Zertifikatfenster zu schließen.

Beispiel 1: In diesem CER-Zertifikat fehlt das EKU-Attribut für die Clientauthentifizierung, und es enthält nur das EKU-Attribut für die Serverauthentifizierung.



Beispiel 2: Dieses CER-Zertifikat enthält sowohl das EKU-Attribut für die Server- als auch die Clientauthentifizierung.



Überprüfen der EKU-Attribute eines PKCS#12-, PEM- und CER-Zertifikats mit OpenSSL

Führen Sie die folgenden Schritte aus, um die EKU-Attribute eines .p12- (PKCS#12), .pem- (PEM) und .cer-Zertifikats zu überprüfen:

Schritt 1: Suchen Sie das zu prüfende Zertifikat, und exportieren Sie es im .p12 (PKCS#12)-, .pem (PEM)- oder .cer-Format.

Wenn Sie für .p12-Zertifikate (PKCS#12) openssl verwenden, um das Zertifikat aus der .p12-Datei (PKCS#12) zu extrahieren, kann die .p12-Datei (PKCS#12) den privaten Schlüssel, das Zertifikat und die Zertifizierungsstellenzertifikate enthalten.

Verwenden Sie den folgenden Befehl, um das Zertifikat aus einer .p12-Datei (PKCS#12) in eine .pem-Datei (PEM) zu extrahieren (ohne den privaten Schlüssel oder die CA-Kette):

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

- IhreDatei.p12: Ersetzen Sie dies durch den tatsächlichen Dateinamen.
- Möglicherweise müssen Sie das Kennwort für die .p12-Datei eingeben.
- cert.pem: Ist das Zertifikat extrahiert (ohne privaten Schlüssel oder CA-Kette) im PEM-Format (PEM)?

Schritt 2: Verwenden Sie die nächsten openssl-Befehle, um die Zertifikatdetails und die EKU-Attribute anzuzeigen.

a) Verwenden Sie für PEM-Dateien den nächsten Befehl openssl, um die Zertifikatdetails und die EKU-Attribute anzuzeigen:

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

- cert.pem: Ersetzen Sie dies durch den tatsächlichen Dateinamen.

b) Verwenden Sie für CER-Dateien den nächsten Befehl openssl, um die Zertifikatdetails und die EKU-Attribute anzuzeigen:

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

- yourfile.cer: Ersetzen Sie dies durch den tatsächlichen Dateinamen.

Schritt 3. Dann suchen Sie nach dem X509v3Extended Key Usage Abschnitt in der Ausgabe, können Sie Einträge wie "TLS Web Server Authentication" und "TLS Web Client Authentication", die die EKU-Werte im Zertifikat.

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

ODER das EKU-Attribut 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
```

- Serverauthentifizierungs-EKU-OID: 1.3.6.1.5.5.7.3.1
- Client-Authentifizierungs-EKU-OID: 1.3.6.1.5.5.7.3.2

Beispiel 1: In diesem PEM-Zertifikat fehlt das EKU-Attribut für die Clientauthentifizierung. Es enthält nur das EKU-Attribut für die Serverauthentifizierung.

<#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
```

Beispiel 2: Dieses PEM-Zertifikat (PEM-Zertifikat) enthält sowohl das EKU-Attribut für die Client- als auch die Serverauthentifizierung.

<#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
```

Problemumgehungen

Administratoren können aus einer der folgenden Workaround-Optionen wählen.

Option 1: Zu öffentlichen Stammzertifizierungsstellen wechseln, die kombinierte EKU-Zertifikate bereitstellen

Einige öffentliche Stammzertifizierungsstellen wie DigiCert und IdenTrust stellen Zertifikate mit kombinierten EKU-Typen (Server- und Clientzertifikate) von einem alternativen Stammverzeichnis

aus, das möglicherweise nicht im Chrome Root Store enthalten ist. Wenden Sie sich an den Zertifizierungsstellenanbieter, um die Verfügbarkeit solcher Zertifikate zu überprüfen, und stellen Sie vor der Bereitstellung sicher, dass sowohl der Server, der das Zertifikat präsentiert, als auch die Clients, die es nutzen, der entsprechenden Stammzertifizierungsstelle vertrauen.

Dieser Ansatz verringert die Notwendigkeit eines Upgrades der Serversoftware, um die Einstellung der Client Authentication EKU, die durch die Chrome Root Program Policy erzwungen wird, einzudämmen.

Die folgende Tabelle, die Beispiele für öffentliche Stammzertifizierungsstellen und EKU-Typen enthält, ist nicht vollständig und dient nur zur Veranschaulichung.

CA-Anbieter	EKU-Typ	Stamm-CA	Issuing/Sub-CA
IdenTrust	clientAuth + serverAuth	IdenTrust Stammzertifizierungsstelle für den öffentlichen Sektor 1	IdenTrust Public Sector Server CA 1
IdenTrust	ClientAuth	IdenTrust Stammzertifizierungsstelle für den öffentlichen Sektor 1	TrustID RSA ClientAuth CA 2
IdenTrust	serverAuth (Browser vertrauenswürdig)	IdenTrust Commercial Root CA 1	HydrantID Server CA O1
DigiCert	clientAuth + serverAuth	DigiCert Assured ID Root G2	DigiCert Assured ID CA G2
DigiCert	ClientAuth	DigiCert Assured ID Root G2	DigiCert Assured ID Client CA G2
DigiCert	serverAuth (Browser vertrauenswürdig)	DigiCert Global Root G2	DigiCert Global G2 TLS RSA SHA256

Option 2: Verlängerung der aktuellen Zertifikate zur Verlängerung ihrer Gültigkeit

Zertifikate, die von öffentlichen Stammzertifizierungsstellen vor Mai 2026 ausgestellt wurden und sowohl über eine Server- als auch eine Clientauthentifizierungs-EKU verfügen, werden bis zum Ablauf ihrer Laufzeit weiterhin anerkannt. Es ist jedoch am besten, kombinierte EKU-Zertifikate zu erneuern, bevor die Richtlinie außer Kraft gesetzt wird.

- Richtlinien für öffentliche Zertifizierungsstellen und Implementierungsdaten können je nach Anbieter variieren.
- Wenden Sie sich an die Zertifizierungsstelle, und planen Sie die Erneuerung des Zertifikats entsprechend.
- Nach dem 15. März 2026 sind von öffentlichen Zertifizierungsstellen ausgestellte Zertifikate nur noch 200 Tage gültig.
- Berücksichtigen Sie, dass einige öffentliche Zertifizierungsstellen keine kombinierten EKU-Zertifikate mehr ausstellen.

Option 3. Migration zu einer privaten PKI, um kombinierte EKU-Zertifikate (Server und Client) auszustellen

Evaluieren Sie die Machbarkeit des Übergangs zu einer Private Public Key Infrastructure (PKI), und richten Sie dann eine private Zertifizierungsstelle ein, um einzelne Zertifikate mit kombinierten EKUs (Server- und Client-Zertifikate mit den erforderlichen EKUs) auszustellen.

Bevor Sie ein Zertifikat ausstellen oder bereitstellen, stellen Sie sicher, dass sowohl der Server, der das Zertifikat präsentiert, als auch alle Clients, die es nutzen, der entsprechenden Stammzertifizierungsstelle vertrauen.

Option 4. Holen Sie sich ein öffentlich vertrauenswürdiges Zertifikat mit nur Client Authentication EKU

Einige CAs, z. B. SSL.com, bieten dedizierte Client-Authentifizierungszertifikate. Diese sind von TLS-Zertifikaten getrennt und werden in der Regel für die Enterprise-Authentifizierung verwendet.

⚠ Vorsicht: Für Produktionsumgebungen wird dringend empfohlen, dass Kunden Zertifikate mit den entsprechenden EKU-Attributen verwenden. Diese Vorgehensweise gewährleistet Sicherheit, Kompatibilität und Einhaltung von Branchenstandards und Best Practices. Zertifikate ohne EKU-Attribute sollten nur als vorübergehender Workaround betrachtet werden und nur mit einem klaren Verständnis der damit verbundenen Risiken.

Häufig gestellte Fragen

Q1. Muss ich mir darüber Gedanken machen, wenn ich eine private PKI verwende?

A: Die von privaten Zertifizierungsstellen durchgesetzte Richtlinie wird von jeder Organisation festgelegt. Wenn Ihre private Zertifizierungsstelle die gleichen Ausstellungskriterien erfüllt, z. B. das Entfernen des EKU-Attributs für die Clientauthentifizierung aus Zertifikaten, gelten die in diesem Dokument enthaltenen Richtlinien.

Q2. Kann ich meine vorhandenen Zertifikate weiterhin verwenden?

A : Ja, gültige Zertifikate mit kombinierter EKU können bis zum Ablaufdatum verwendet werden.

Q3. Welche Optionen stehen für die Integration meines FMC oder FDM mit ISE über pxGrid zur

Verfügung, wenn das auf dem FMC/FDM installierte Zertifikat nicht über das EKU-Attribut für die Client-Authentifizierung verfügt?

A : Neben den in diesem Dokument vorgeschlagenen Problemumgehungen empfehlen wir Ihnen, die folgenden ISE-Verweise zu überprüfen:

- Problemhinweis: FN74392 - Cisco Identity Services Engine: Auswirkungen auf die sichere Kommunikation durch Authentifizierung von Clients für öffentliche CA-Clients Änderungen der EKU ab Mai 2026 - Problemumgehung bereitgestellt

- Vorbereitung der Identity Services Engine auf erweiterte Schlüsselverwendungsbeschränkungen in Zertifikaten, die von öffentlichen Zertifizierungsstellen ausgestellt wurden

---

Anmerkung: Auch wenn die Verwendung eines öffentlichen, von einer Zertifizierungsstelle signierten Zertifikats für IMS unterstützt wird. Cisco empfiehlt die Verwendung des ISE Internal CA-Zertifikats, da diese Kommunikation nur für interne Transaktionen verwendet wird.

Q4. Was ist die "Client Authentication" EKU und warum war es in meinem Zertifikat?

A: Die EKU "Client Authentication" gibt an, dass ein Zertifikat von einem Client für die Authentifizierung bei einem Server verwendet werden kann. Einige CAs haben es in der Vergangenheit standardmäßig in TLS-Zertifikate aufgenommen, dies war jedoch für die normale Website-Sicherheit nie erforderlich.

Q5. Mein aktuelles TLS-Zertifikat lautet "Client Authentication" unter seiner Extended Key Usage. Ist sie jetzt ungültig?

A: Nein, es bleibt gültig. Sie müssen es nicht sofort austauschen. Bei der Verlängerung enthält das neue Zertifikat die clientAuth EKU nicht mehr.

Q6. Wie kann ich überprüfen, ob ein Zertifikat über die clientAuth EKU verfügt?

A : Sie können die Zertifikatdetails mit OpenSSL-, PowerShell- oder GUI-Tools überprüfen, um nach der Erweiterung für die erweiterte Schlüsselverwendung zu suchen.

Q7. Kann ich immer noch ein öffentlich vertrauenswürdiges Zertifikat mit nur Client Authentication EKU bekommen?

A : Einige CAs, z. B. SSL.com, bieten dedizierte Client-Authentifizierungszertifikate. Diese sind von TLS-Zertifikaten getrennt und werden in der Regel für die Enterprise-Authentifizierung verwendet.

Q8. Betrifft dies andere EKUs oder Zertifikatstypen (Codesignatur, E-Mail usw.)?

A : Nein, diese Änderung betrifft nur TLS-Serverzertifikate. Codesignatur und E-Mail-Zertifikate haben eigene EKU-Anforderungen.

Q9. Wo sehe ich die offiziellen Anforderungen zu dieser Änderung?

A : Die Google Chrome Root Program Policy enthält Richtlinien zum Verbot der clientAuth EKU in TLS-Serverzertifikaten.

Q10. Ist es sicher, Zertifikate ohne Client- und Server-EKU-Attribute in meiner Produktionsumgebung zu verwenden?

A: Für Produktionsumgebungen wird dringend empfohlen, dass Kunden Zertifikate mit den entsprechenden EKU-Attributen verwenden. Diese Vorgehensweise gewährleistet Sicherheit, Kompatibilität und Einhaltung von Branchenstandards und Best Practices. Zertifikate ohne EKU-Attribute sollten nur als vorübergehender Workaround betrachtet werden und nur mit einem klaren Verständnis der damit verbundenen Risiken.

Zugehörige Informationen

- Weitere Unterstützung erhalten Sie vom Cisco Technical Assistance Center (TAC). Ein gültiger Support-Vertrag ist erforderlich: Cisco Worldwide Support Contacts

- Cisco Support und Downloads: Technischer Support und Downloads von Cisco

Verwandte Fehler

- CSCwt94492 DEU: Das FMC muss das Vorhandensein des EKU-Attributs für die Clientauthentifizierung im Clientzertifikat für die pxGrid-Integration validieren.

- CSCwt94509 DEU: Das FMC sollte eine Meldung anzeigen, die angibt, dass das EKU-Attribut für die Clientauthentifizierung in dem für die pxGrid-Integration verwendeten

Clientzertifikat erforderlich ist.

- CSCwt61767 Mai 2026 EKU Server-Only Change - Geben Sie eine ASA-Konfigurationswarnung aus, wenn die EKU unzureichend ist.

- CSCws83036 SKU: Folgenabschätzung der ClientAuth EKU-Durchsetzung in der ISE

Referenzen zur Cisco ISE

- Problemhinweis: FN74392 - Cisco Identity Services Engine: Auswirkungen auf die sichere Kommunikation durch Authentifizierung von Clients für öffentliche CA-Clients Änderungen der EKU ab Mai 2026 - Problemumgehung bereitgestellt

- Vorbereitung der Identity Services Engine auf erweiterte Schlüsselverwendungsbeschränkungen in Zertifikaten, die von öffentlichen Zertifizierungsstellen ausgestellt wurden

Externe Referenzen

- Richtlinie für Chrome-Stammprogramm

- IdenTrust-Portal

- SSL - Entfernen der Clientauthentifizierungs-EKU aus TLS-Serverzertifikaten - Was Sie wissen müssen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.