自2026年5月開始用於安全通訊的Cisco安全防火牆對公共CA客戶端身份驗證EKU更改的影響

簡介

本檔案介紹遵守Chrome Root Certificate計畫的憑證授權單位施加的憑證頒發標準限制的影響，尤其是與思科安全防火牆產品相關的限制。

背景資訊

公共信任的TLS證書由CA頒發，這些證書必須符合管理證書頒發和使用情況的行業策略。

由Google運作的Chrome根程式原則定義了CA必須遵循的要求，其憑證才能被Google Chrome瀏覽器信任。這些要求會影響在行業中頒發受公共信任證書的方式。作為不斷發展的安全實踐的一部分，Chrome根計畫正在引入關於證書使用的更嚴格指導。

因此，許多公共CA不再頒發包含客戶端身份驗證EKU的證書，而是改為頒發僅用於伺服器身份驗證的證書。因此，許多公共CA新頒發的證書預期將僅包含伺服器身份驗證EKU。

延伸金鑰使用(EKU)是定義數位憑證中公用金鑰的預期功能的憑證擴充模組。它建立一組允許的應用程式，確保該金鑰僅用於特定的加密操作。此功能由對象識別符號(OID)管理，對象識別符號是對每個允許的用途進行分類的唯一數字識別符號，如代碼簽名、伺服器身份驗證、客戶端身份驗證或安全電子郵件。

當身份驗證基於證書時，驗證實體檢查證書以標識EKU中的對象識別符號(OID)。通過嵌入EKU擴展，證書頒發機構(CA)將證書範圍限製為預定義角色，每個指定用途都顯式對映到OID。

EKU屬性的用途

·定義用法：EKU屬性說明允許證書執行的身份驗證或加密型別。

·增強安全性：通過將證書限製為特定用途，EKU有助於防止濫用或意外應用（例如，伺服器證書不能用於客戶端身份驗證）。

·法規遵從性：確保證書的使用符合安全策略和行業標準。

EKU屬性的主要用途

1. TLS Web客戶端驗證

· 允許使用證書對伺服器或裝置進行標識和身份驗證。

· OID:1.3.6.1.5.5.7.3.2

·用於VPN、雙向TLS和安全登入方案。

2. TLS Web服務器驗證

·允許伺服器使用證書向客戶端證明其身份。

· OID:1.3.6.1.5.5.7.3.1

·用於HTTPS、SSL/TLS Web伺服器和安全API終端。

3.代碼簽名

· 表示證書可用於對軟體或執行檔進行簽名。

· OID:1.3.6.1.5.5.7.3.3

·用於軟體分發和完整性檢查。

4.電子郵件保護

· 啟用證書用於對電子郵件進行簽名和加密。

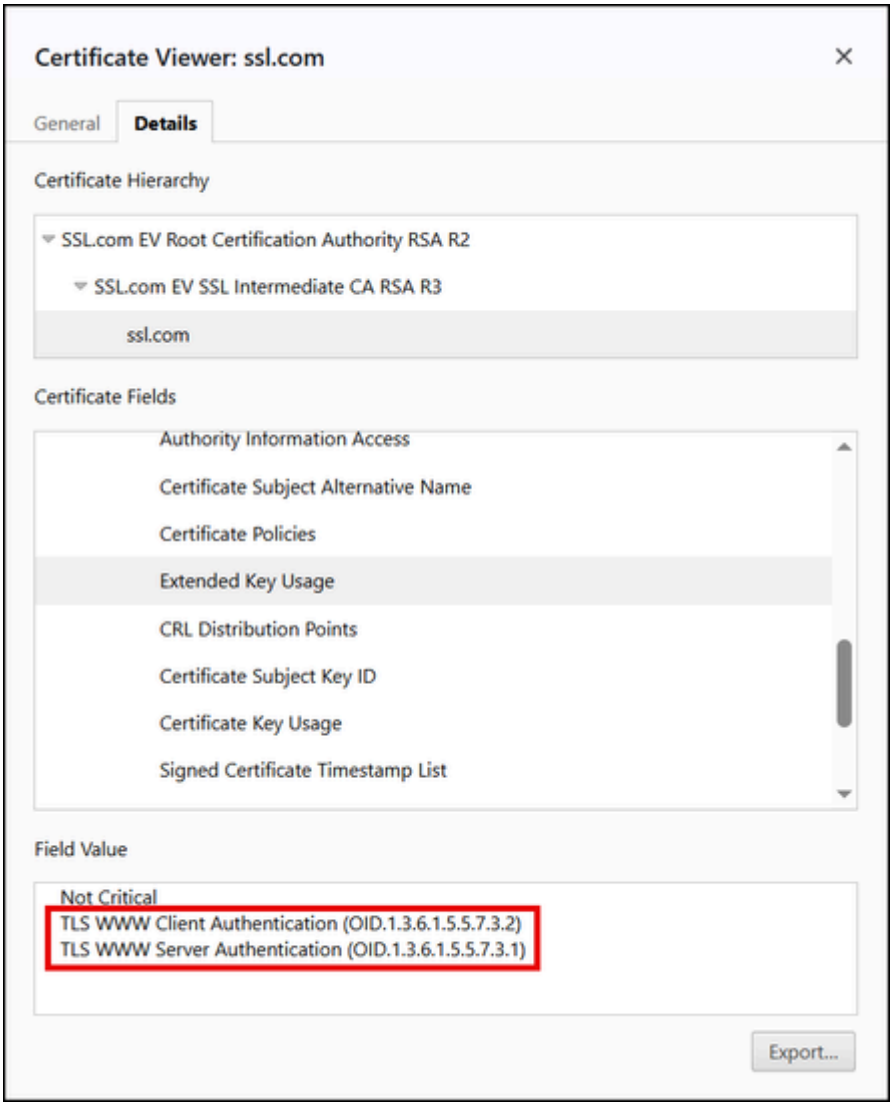
· OID:1.3.6.1.5.5.7.3.4

· 用於S/MIME郵件安全。

5.其他目的

·文檔簽名、時間戳、智慧卡登入等，每個都有自己的OID。

瀏覽器和伺服器僅需使用serverAuth EKU來建立HTTPS的安全連線，但過去，許多TLS伺服器憑證同時包含serverAuth和clientAuthEKU，以下是此類憑證的範例：



為什麼從伺服器證書中刪除客戶端身份驗證EKU?

- 安全性和範圍：公共TLS證書僅用於對Web上的服務器進行驗證。刪除操作可將伺服器和客戶端功能明確分開。ClientAuth EKU用於使用相互TLS(mTLS)和其他身份驗證方案的電腦和使用者身份驗證。
- 防止配置錯誤：如果EKU存在，則某些系統可能信任來自公共CA的任何證書進行客戶端身份驗證，這可能帶來安全風險。
- 瀏覽器要求：主要瀏覽器不要求或檢查網站證書中的clientAuth EKU。
- 簡化的PKI架構：通過分離使用，CA可以維護伺服器TLS與其他用途不同的證書層次結構。

這對於思科安全防火牆自適應安全裝置(ASA)、思科安全防火牆威脅防禦(FTD)、思科安全防火牆裝置管理器(FDM)和思科安全防火牆管理中心(FMC)等產品尤為重要，這些產品在TLS身份驗證期間可能充當伺服器或客戶端，具體取決於使用案例。

對伺服器環境的影響

對於絕大多數伺服器部署而言，此更改將是低影響或無影響的。下面是預期結果：

- 標準Web伺服器(HTTPS):無影響。更新的證書將繼續正常工作。
- 現有證書：在中斷之前發布的任何證書將繼續運行，直到其過期為止。
- 相互TLS(mTLS)和客戶端證書方案：如果您正在使用TLS伺服器證書進行客戶端驗證，則需要從另一個源獲取具有clientAuth EKU的單獨證書。
- 同時需要兩個EKU的企業系統：一些傳統系統或企業系統需要兩個EKU。您應驗證是否需要更新以遵守新規則。

問題描述

從2026年5月開始，許多公共證書頒發機構(CA)將停止頒發包含客戶端身份驗證擴展金鑰使用(EKU)的傳輸層安全(TLS)證書。 新頒發的證書通常僅包括伺服器身份驗證EKU。

因此，如果根據更新的CA策略更新由公共CA頒發的證書，然後將其部署到Cisco安全防火牆產品中，則要求客戶端身份驗證EKU的服務將失敗。受到影響的特定服務如下：

- 當ASA、FTD、FDM或FMC充當客戶端時(例如，當連線到身份提供程式或身份驗證伺服器(例如ISE(pxGrid)、RADIUS、LDAPS或Active Directory)時)，如果客戶端證書由公共CA生成並且缺少客戶端身份驗證EKU，基於證書的身份驗證可能會失敗。在這些情況下，如果身份驗證伺服器拒絕證書而沒有所需的EKU，則可能會發生連線故障。
- Cisco Secure Client（以前稱為AnyConnect）可以使用證書向ASA或FTD伺服器進行身份驗證。但是，如果客戶端證書由公共CA生成並且缺少客戶端身份驗證EKU，則遠端訪問VPN(RAVPN)連線將失敗。
- 當FTD或ASA使用證書身份驗證（RSA或ECDSA）建立站點到站點VPN隧道（無論是到其他FTD、ASA、思科路由器還是第三方VPN對等體）時，如果公共CA生成的身份證書缺少客戶端身份驗證EKU屬性，則隧道將失敗。之所以會出現這種情況，是因為遠端VPN對等體要求身份證書中存在客戶端身份驗證EKU。

Chrome根程式策略更改

EKU的實施取決於CA對證書的簽名。伺服器身份驗證和客戶端身份驗證EKU的使用是常見做法。但是，作為與此證書頒發條件一致的Chrome根程式策略更改CA的一部分，將停止對包括客戶端身份驗證擴展金鑰用法(EKU)的TLS證書的簽名。新頒發的證書僅包含伺服器身份驗證EKU。

主要政策要求

- 公共根CA必須宣告僅用於伺服器身份驗證的擴展金鑰使用(EKU)(id-kp-serverAuth)
- 證書必須僅包含伺服器身份驗證EKU。
- 禁止在這些證書中包括客戶端身份驗證EKU
- 繼續使用客戶端身份驗證EKU頒發證書的根CA最終從Chrome根儲存中刪除，導致Chrome瀏覽器將此類證書標籤為「不可信」

時間表

- 2025年9月,SSL.com將頒發僅包含伺服器證書的ServerAuth EKU(而不是ClientAuth)的TLS證書。換句話說，您的網站或伺服器的新SSL/TLS證書將明確僅用於「伺服器身份驗證」。
- 2025年10月：與該計劃一致的CA（例如：DigiCert、Sectigo等）開始預設頒發僅伺服器證書。
- 2026年5月：與程式對齊的CA停止頒發客戶端身份驗證EKU證書
- 2027年3月：Chrome根計劃策略完全生效

對思科安全防火牆產品的影響

公共CA開始在頒發的證書中僅包含伺服器身份驗證EKU之後。這可能會對下一個思科安全防火牆產品方案產生以下影響：

- 當ASA、FTD、FDM或FMC充當客戶端時(例如，當連線到身份提供程式或身份驗證伺服器(例如ISE(pxGrid)、RADIUS、LDAPS或Active Directory)時)，如果客戶端證書由公共CA生成並且缺少客戶端身份驗證EKU，基於證書的身份驗證可能會失敗。在這些情況下，如果身份驗證伺服器拒絕證書而沒有所需的EKU，則可能會發生連線故障

。

- Cisco Secure Client（以前稱為AnyConnect）可以使用證書向ASA或FTD伺服器進行身份驗證。但是，如果客戶端證書由公共CA生成並且缺少客戶端身份驗證EKU，則遠端訪問VPN(RAVPN)連線將失敗。

- 當FTD或ASA使用證書身份驗證（RSA或ECDSA）建立站點到站點VPN隧道（無論是到其他FTD、ASA、思科路由器還是第三方VPN對等體）時，如果公共CA生成的身份證書缺少客戶端身份驗證EKU屬性，則隧道將失敗。之所以會出現這種情況，是因為遠端VPN對等體要求身份證書中存在客戶端身份驗證EKU。

註意：如果通過pxGrid將FMC或FDM與ISE整合，並且在FMC/FDM上安裝的證書缺少「客戶端身份驗證EKU」屬性，則檢視本文檔中建議的解決方法以及下一個ISE引用：FN74392和準備身份服務引擎，以針對公共證書頒發機構頒發的證書中的擴展金鑰使用限制。

附註：從TLS伺服器證書中刪除clientAuth EKU是一項行業範圍的策略更改，將增強安全性並防止誤用。對大多數使用者來說，不會產生明顯的影響。但是，如果您依靠ClientAuth EKU，您應該採取主動措施，以便根據自己的需求獲取正確的證書型別。

受影響的產品

思科安全防火牆產品	軟體版本	受影響的方案	補救
FTD	所有版本	當作為客戶端時(例如，當連線到身份提供程式或身份驗證伺服器(如ISE(pxGrid)、RADIUS、LDAPS或Active Directory)時)，如果客戶端證書由公共CA生成並且缺少客戶端身份驗證EKU，基於證書的身份驗證可能會失敗。在這種情況下，如果身份驗證伺服器拒絕證書而沒有所需的EKU，則可能會發生連線故障。	選項1。如果您使用TLS伺服器證書進行客戶端身份驗證，則需要從另一個源獲取具有ClientAuth EKU的證書。 或 選項2.切換到提供組合EKU（ClientAuth和ServerAuth）證書的公共根CA（證書頒發機構）。 附註：如需其他選項，請參閱本檔案的解決方法一節。
FDM	所有版本		
FMC	所有版本		
ASA	所有版本		

Cisco Secure Client（前身為AnyConnect）	所有版本	思科安全客戶端可以使用證書向ASA或FTD伺服器進行身份驗證。但是，如果客戶端證書由公共CA生成並且缺少客戶端身份驗證EKU，則遠端訪問VPN(RAVPN)連線將失敗。	
FTD或ASA	所有版本	當FTD或ASA使用證書身份驗證（RSA或ECDSA）建立站點到站點VPN隧道（無論是到另一個FTD、ASA、思科路由器還是第三方VPN對等體）時，如果公共CA生成的身份證書缺少客戶端身份驗證EKU屬性，則VPN隧道將失敗。之所以會出現這種情況，是因為遠端VPN對等體要求身份證書中存在客戶端身份驗證EKU。	

註意：如果通過pxGrid將FMC或FDM與ISE整合，並且在FMC/FDM上安裝的證書缺少「客戶端身份驗證EKU」屬性，則檢視本文檔中建議的解決方法以及下一個ISE引用：FN74392和準備身份服務引擎，以針對公共證書頒發機構頒發的證書中的擴展金鑰使用限制。

附註：從TLS伺服器證書中刪除clientAuth EKU是一項行業範圍的策略更改，將增強安全性並防止誤用。對大多數使用者來說，不會產生明顯的影響。但是，如果您依靠ClientAuth　EKU，您應該採取主動措施，以便根據自己的需求獲取正確的證書型別。

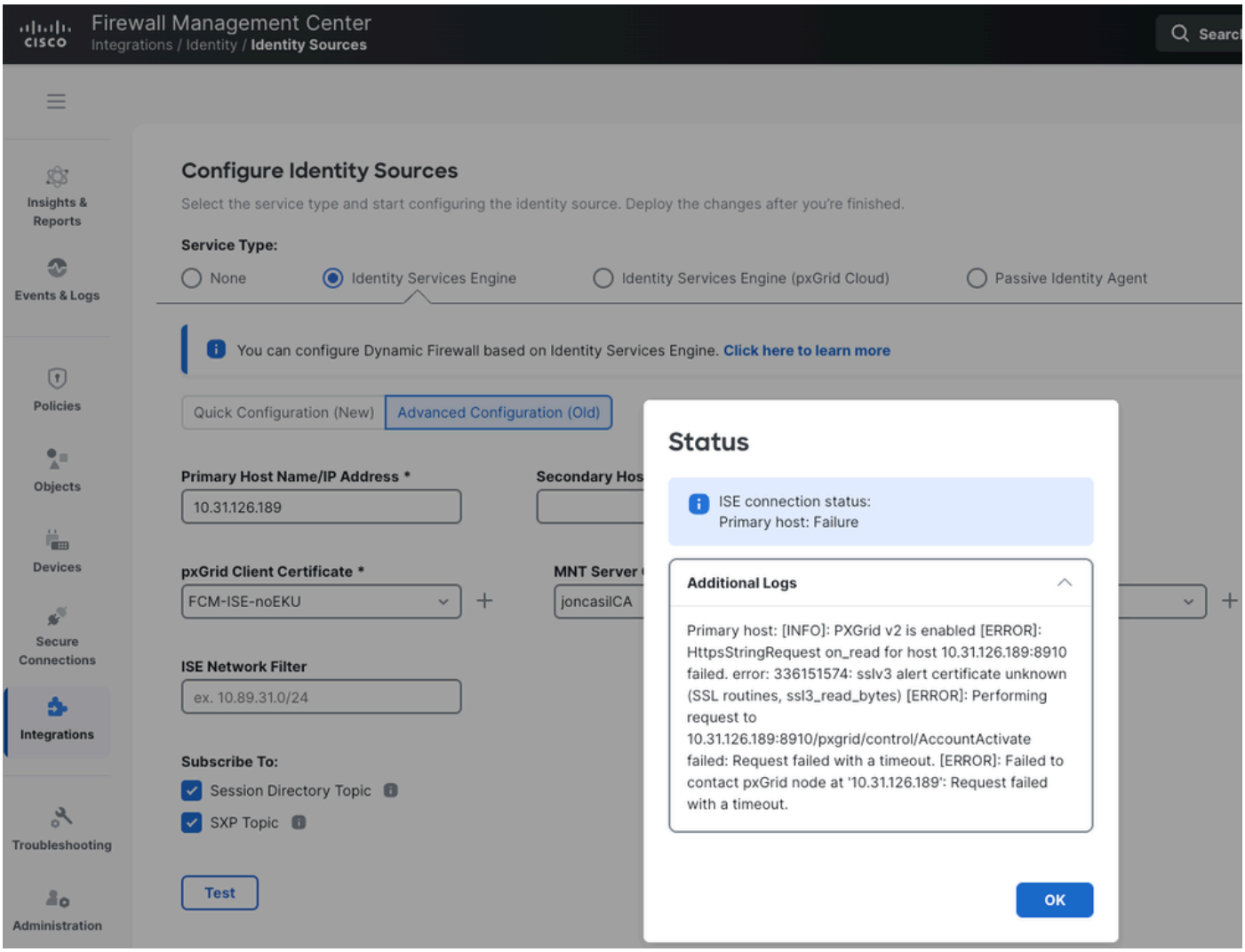
注意：對於生產環境，強烈建議客戶使用具有適當EKU屬性的證書。這一做法確保了安全性、相容性，並符合行業標準和最佳實踐。不具EKU屬性的證書僅應視為臨時解決辦法，並且必須明確瞭解相關的風險。

問題1. pxGrid在FMC和ISE之間的整合問題，當FMC證書缺少客戶端身份驗證EKU屬性時

在此方案中，FMC用於與ISE整合pxGrid的證書缺少客戶端身份驗證EKU屬性。因此，pxGrid整合失敗，因為ISE伺服器希望此屬性出現在FMC提供的證書中。

拓撲

FMC UI錯誤：當FMC使用的證書缺少pxGrid與ISE整合的客戶端身份驗證EKU屬性時，將顯示在FMC中的錯誤消息。



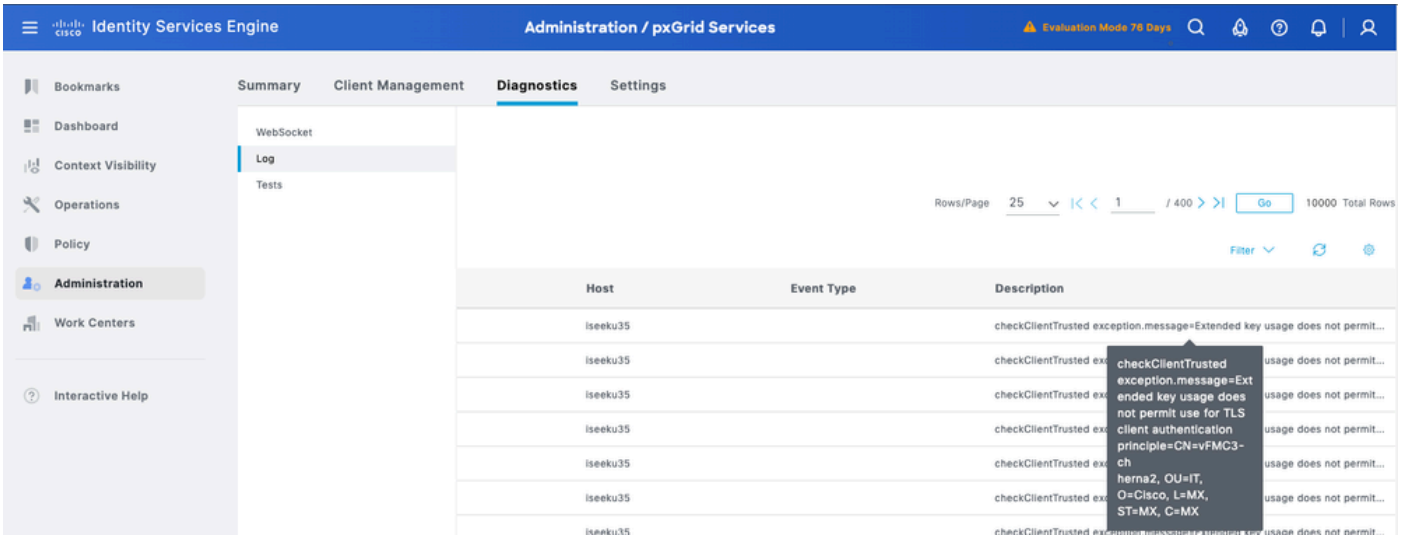
FMC CLI錯誤：在FMC /var/log/messages目錄中發現了相同的錯誤消息。

```
<#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錯誤：這是ISE中顯示的錯誤消息「checkClientTrusted exception.message=Extended key usage not permit use for TLS client authentication principle=CN=vFMC3-chherna2, OU=IT， O=Cisco， L=MX， ST=MX， C=MX」。



解決方案：如果通過pxGrid將FMC或FDM與ISE整合，並且在FMC/FDM中安裝的證書缺少「客戶端身份驗證EKU」屬性，則檢視本文檔中建議的內容以及下一個ISE參考：FN74392和準備身份服務引擎，瞭解公共證書頒發機構頒發的證書中的擴展金鑰使用限制，以便成功整合pxGrid。

附註：FMC pxGrid客戶端證書必須包含ClientAuth EKU屬性或完全不包含客戶端或伺服器EKU屬性。

附註：即使IMS支援使用公有CA簽名的證書。思科建議使用ISE內部CA證書，因為此通訊僅用於內部事務。

問題2. LDAPS伺服器的FTD或ASA整合問題，當提供的證書缺少「客戶端身份驗證」EKU屬性時

在此案例中，FTD或ASA充當客戶端，使用證書身份驗證與LDAPS伺服器整合。如果FTD或ASA使用的證書缺少Client Authentication EKU屬性，則整合將失敗，因為LDAPS伺服器要求證書中存在此屬性。

拓撲

LDAPS伺服器錯誤：'TLS證書驗證：錯誤，不支援的證書用途」和「TLS跟蹤：SSL3警報寫入：致命：不支援的證書'

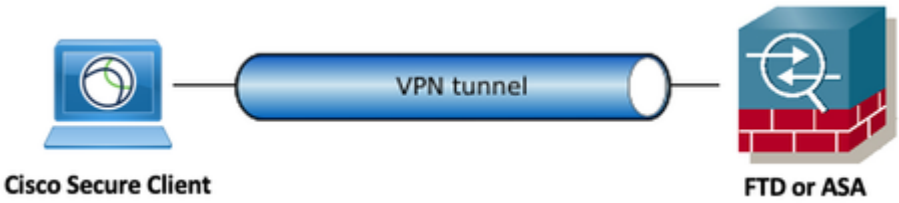
```
69ceb4f5.157b4993 0x7ff553fff700 TLS trace: SSL_accept:TLSv1.3 write server cer
tificate verify
69ceb4f5.157c01a4 0x7ff553fff700 TLS trace: SSL_accept:SSLv3/TLS write finished
69ceb4f5.157c458a 0x7ff553fff700 TLS trace: SSL_accept:TLSv1.3 early data
69ceb4f5.157c6685 0x7ff553fff700 TLS trace: SSL_accept:error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

解決方案：檢視本文檔中建議的項目，確保FTD或ASA使用正確的身份證書（包括Client Authentication EKU屬性）成功通過LDAPS伺服器進行基於證書的身份驗證。

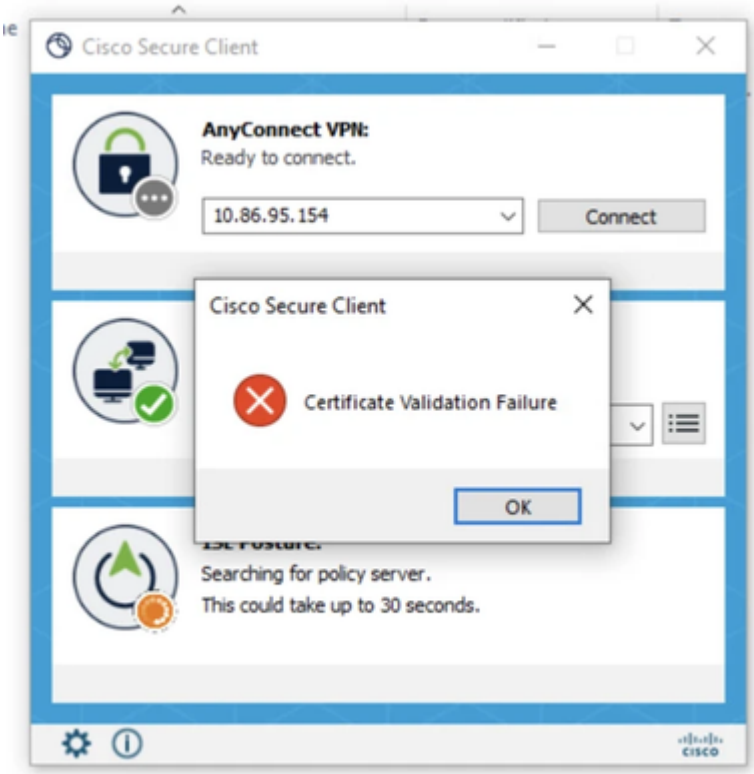
問題3.如果客戶端證書缺少客戶端身份驗證EKU屬性，Cisco安全客戶端（以前稱為AnyConnect）可能會遇到與FTD或ASA的連線問題

在此案例中，思科安全使用者端使用憑證驗證來建立到FTD或ASA的RAVPN通道。但是，如果客戶端證書缺少Client Authentication EKU屬性，則RAVPN會話將失敗，因為ASA或FTD要求客戶端證書中存在此屬性。

拓撲



Cisco Secure Client錯誤： '證書驗證失敗'



Cisco安全客戶端DART錯誤：DART捆綁包中AnyConnectVPN.txt檔案的以下日誌確認，由於沒有「客戶端身份驗證EKU」屬性，Cisco安全客戶端已拒絕用於FTD/ASA基於證書身份驗證的證書(要在DART捆綁包中找到AnyConnectVPN.txt檔案，請導航至Cisco安全客戶端> AnyConnect VPN >日誌> 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]

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

解決方案：檢視本文檔中建議的，確保Cisco Secure Client使用正確的證書（包括Client Authentication EKU屬性）成功通過FTD或ASA進行基於證書的身份驗證。

附註：從上面的DART捆綁包錯誤「證書中找不到EKU:1.3.6.1.5.5.7.3.2」，此編號「1.3.6.1.5.5.7.3.2」對應客戶端身份驗證EKU OID。

問題4.如果身份證書缺少「客戶端身份驗證」EKU屬性，則使用基於證書的身份驗證的站點到站點VPN隧道將失敗

在此案例中，涉及IKEv2站點到站點VPN隧道的基於證書的身份驗證，FTD/ASA(1)用來建立到FTD/ASA(2)對等體的隧道的身份證書缺少Client Authentication EKU屬性。因此，無法建立VPN通道，因為遠端對等點FTD/ASA(2)要求憑證中必須存在此屬性。

拓撲

FTD或ASA CLI錯誤：FTD/ASA(2)拒絕缺少客戶端身份驗證EKU屬性的FTD/ASA(1)身份證書時，在基於IKEv2證書的身份驗證過程中觀察到這些錯誤。

<#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
```

附註：在上方範例中，FTD/ASA(2)使用的身分憑證包括ClientAuth和ServerAuth EKU屬性。

附註：在上方示例中，FTD/ASA(2)也可由路由器或第三方物理或基於雲的VPN集中器替換。然後，相同的問題會持續存在，因為VPN對等點要求在FTD/ASA(1)使用的證書中存在「客戶端身份驗證」EKU屬性，以便成功進行基於證書的身份驗證。

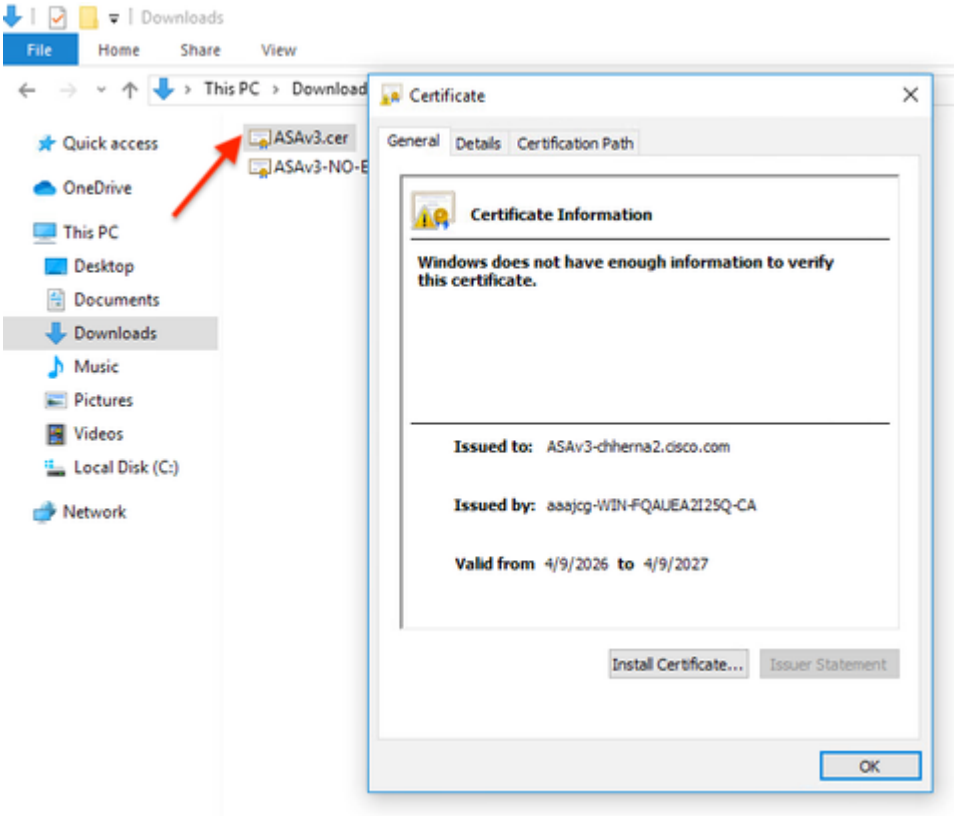
解決方案：檢視本文檔中建議的，確保FTD/ASA(1)使用正確的身份證書（包括Client Authentication EKU屬性），通過基於證書的身份驗證成功實現站點到站點VPN隧道。

用於確認您的證書是否缺少客戶端身份驗證EKU屬性的說明

使用Windows證書管理器驗證.cer證書中的EKU屬性

按照以下步驟使用Windows證書管理器驗證.cer證書中的EKU屬性：

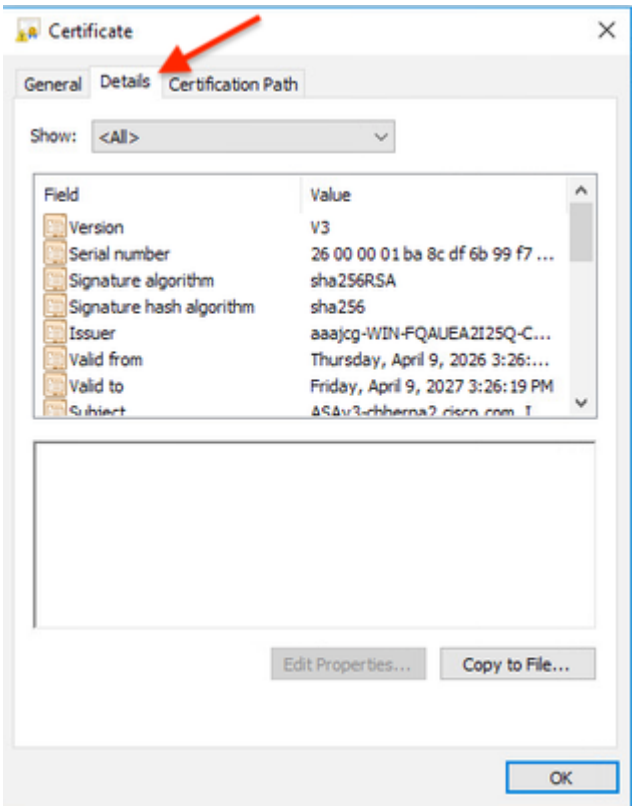
步驟1.按兩下.cer檔案，在Windows證書管理器中開啟該檔案。



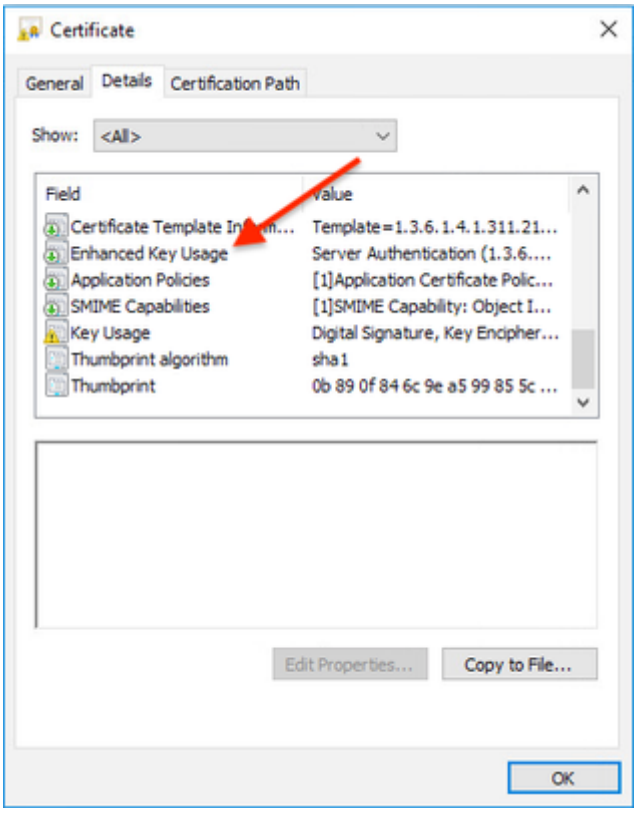
附註：只有.cer檔案會以這種方式直接開啟；如果您的憑證具有.pem擴充模組，請先將其重新命名為.cer或.crt。

步驟2.處理安全警告（如果有），如果出現安全警告提示，請按一下「開啟」繼續。

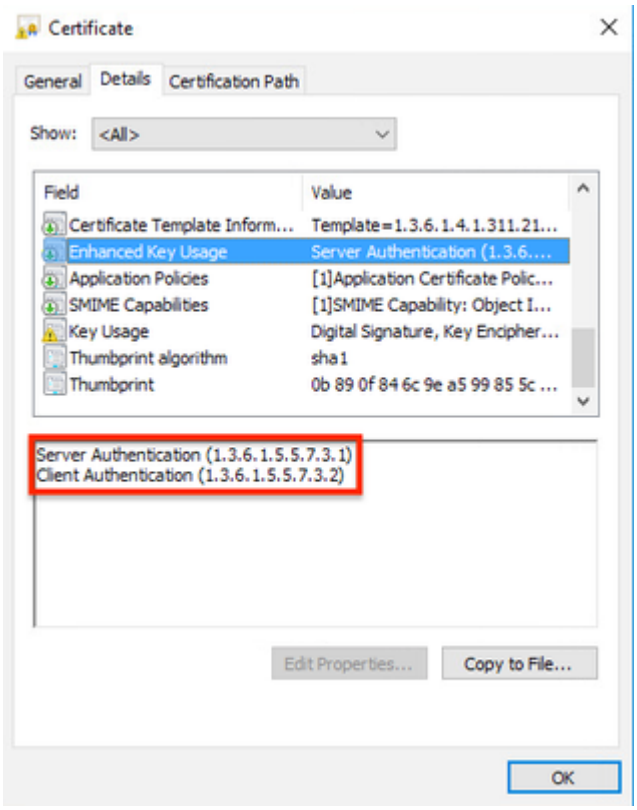
步驟3.在憑證視窗中，按一下Details索引標籤。



步驟4.滾動瀏覽欄位清單並選擇「Enhanced Key Usage」（或Extended Key Usage）。

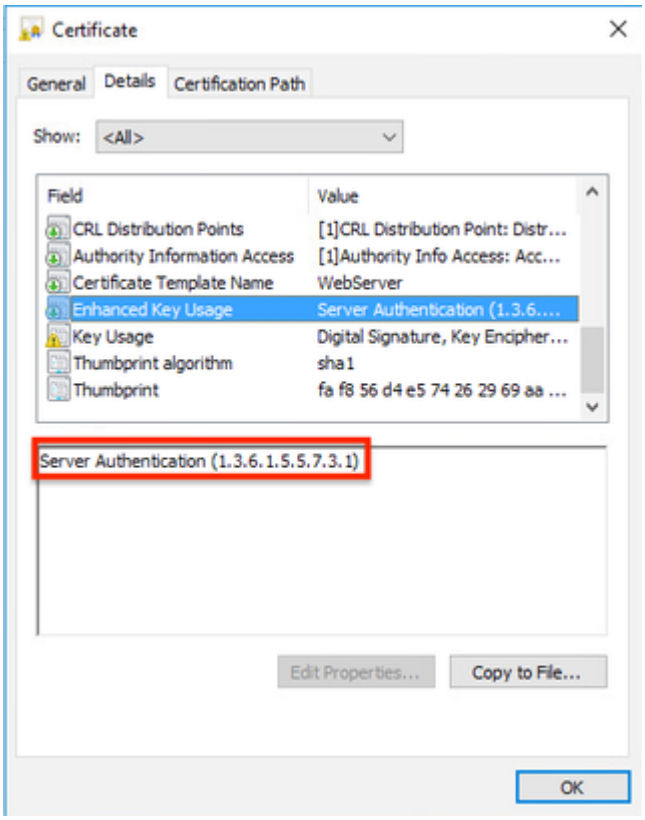


步驟5.驗證EKU屬性，您可能會看到諸如「伺服器身份驗證」和「客戶端身份驗證」之類的條目，這些條目指示證書中存在的EKU值。

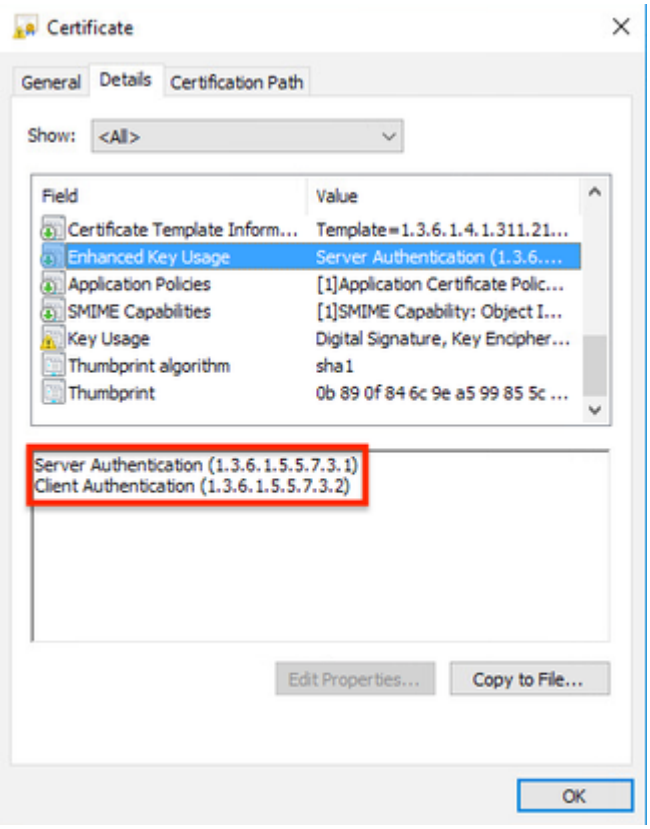


步驟6.驗證後，按一下OK以關閉憑證視窗。

範例 1：此.cer證書缺少「客戶端身份驗證」EKU屬性，並且僅包含「伺服器身份驗證」EKU屬性。



範例 2：此.cer證書包括伺服器和客戶端身份驗證EKU屬性。



使用OpenSSL驗證PKCS#12、PEM和.cer證書的EKU屬性

按照以下步驟驗證.p12(PKCS#12)、.pem(PEM)和.cer證書中的EKU屬性：

步驟1.找到需要檢查的證書，並以.p12(PKCS#12)、.pem(PEM)或.cer格式將其匯出。

對於.p12(PKCS#12)證書，請使用openssl從.p12(PKCS#12)檔案中提取證書，.p12(PKCS#12)檔案可能包含私鑰、證書和CA證書。

使用以下命令將憑證從.p12(PKCS#12)檔案提取到.pem(PEM)檔案（不含私鑰或CA鏈結）：

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

- yourfile.p12:替換為實際的檔名。
- 您可能需要輸入.p12檔案的密碼。
- cert.pem:是以.pem(PEM)格式提取的憑證（不含私鑰或CA鏈結）。

步驟2.使用下一個openssl命令顯示憑證詳細資訊和EKU屬性。

a)對於.pem檔案，請使用next openssl命令顯示證書詳細資訊和EKU屬性：

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

- cert.pem:替換為實際的檔名。

b)對於.cer檔案，使用next openssl命令顯示證書詳細資訊和EKU屬性：

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

- yourfile.cer:替換為實際的檔名。

步驟3。然後，在輸出中查詢「X509v3Extended Key Usage」部分，您可能會看到諸如「TLS Web Server Authentication」和「TLS Web Client Authentication」之類的條目，這些條目指示證書中存在的EKU值。

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

或EKU屬性OID（對象識別符號）：

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

- 伺服器身份驗證EKU OID:1.3.6.1.5.5.7.3.1
- 客戶端身份驗證EKU OID:1.3.6.1.5.5.7.3.2

範例 1：此.pem(PEM)證書缺少「客戶端身份驗證」EKU屬性，並且僅包含「伺服器身份驗證」EKU屬性。

<#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
```

範例 2：此.pem(PEM)證書包括客戶端和伺服器身份驗證EKU屬性。

<#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
```

因應措施

管理員可以從以下任一解決方法選項中選擇。

選項1.切換到提供組合EKU證書的公用根CA

某些公共根CA（例如DigiCert和IdenTrust）會從另一個根頒發具有組合EKU型別（伺服器和客戶端證書）的證書，這些型別可能不包含在Chrome根儲存中。與CA提供商協調檢查此類證書的可用性，並在部署證書之前，確保提供證書的伺服器和使用該證書的客戶端都信任相應的根CA。

此方法無需升級伺服器軟體來緩解由Chrome根程式策略實施的客戶端身份驗證EKU的取消設定。

下表顯示了公共根CA和EKU型別的示例，該表不是詳盡的清單，僅供參考。

CA供應商	EKU型別	根CA	簽發/子CA
IdenTrust	clientAuth + serverAuth	IdenTrust公共部門根CA 1	IdenTrust Public Sector Server CA 1
IdenTrust	clientAuth	IdenTrust公共部門根CA 1	TrustID RSA ClientAuth CA 2
IdenTrust	serverAuth（瀏覽器受信任）	IdenTrust商業根CA 1	HydrantID伺服器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（瀏覽器受信任）	DigiCert全域性根G2	DigiCert Global G2 TLS RSA SHA256

選項2.續訂當前證書以延長其有效性

在2026年5月之前由公共根CA頒發、同時具有伺服器和客戶端身份驗證EKU的證書將繼續保留，直到其期限到期。但是，最好在策略失效設定發生之前續訂組合的EKU證書。

- 公共CA策略和實施日期可能因供應商而異。
- 請諮詢CA並相應地計畫證書續訂。
- 2026年3月15日後，CA頒發的公共證書有效期僅為200天。
- 考慮到一些公共CA已停止發佈合併EKU證書。

選項3.遷移到專用PKI以頒發組合的EKU（伺服器和客戶端）證書

評估過渡到私有公共金鑰基礎設施(PKI)的可行性，然後設定一個私有CA以使用組合的EKU（具有必要EKU的伺服器和客戶端證書）頒發單個證書。

在頒發或部署證書之前，請確保呈現證書的伺服器和使用證書的所有客戶端都信任相應的根CA。

選項4.僅使用客戶端身份驗證EKU獲取公共信任證書

某些CA(如SSL.com)提供專用的客戶端身份驗證證書。這些證書與TLS證書分開，通常用於企業身份驗證。

⚠ 注意：對於生產環境，強烈建議客戶使用具有適當EKU屬性的證書。這一做法確保了安全性、相容性，並符合行業標準和最佳實踐。不具EKU屬性的證書僅應視為臨時解決辦法，並且必須明確瞭解相關的風險。

常見問題 (FAQ)

問1：如果使用私有PKI，是否需要擔心此問題？

答：由專用CA實施的策略由每個組織決定。如果您的私人CA採用相同的頒發標準（例如從證書中刪除客戶端身份驗證EKU屬性），則本文檔中提供的准則適用。

問題2：是否可以繼續使用現有的證書？

A:是，在到期時間之前，可以使用結合EKU的有效證書。

問題3.如果FMC/FDM上安裝的證書沒有「客戶端身份驗證EKU」屬性，可以使用哪些選項通過pxGrid將我的FMC或FDM與ISE整合？

A:除了本文檔中建議的解決方法，我們強烈建議您檢查以下ISE參考：

- 公告：FN74392 - Cisco Identity Services Engine:從2026年5月開始的公共CA客戶端身份驗證EKU更改對安全通訊的影響 — 提供解決方法
- 準備身份服務引擎，使其適用於公共證書頒發機構頒發的證書中的擴展金鑰使用限制

附註：即使IMS支援使用公有CA簽名的證書。思科建議使用ISE內部CA證書，因為此通訊僅用於內部事務。

問題4. 「客戶端身份驗證」EKU是什麼？為什麼它出現在我的證書中？

A：「Client Authentication」 EKU表示客戶端可以使用證書對伺服器進行身份驗證。歷史上，有些CA會預設將其包含在TLS證書中，但正常網站安全從來不需要它。

問題5：我當前的TLS證書在其擴展金鑰用法下顯示「客戶端身份驗證」。現在是否無效？

答：否，仍然有效。你不需要立即替換它續訂時，新憑證不會包括clientAuth EKU。

問題6.如何檢查證書是否具有clientAuth EKU?

A:您可以使用OpenSSL、PowerShell或GUI工具檢查憑證詳細資訊，以檢查是否有延伸金鑰使用擴充。

問題7.我是否仍可以僅使用客戶端身份驗證EKU獲得公共信任證書？

A:某些CA(如SSL.com)提供專用的客戶端身份驗證證書。這些證書與TLS證書分開，通常用於企業身份驗證。

問題8.這是否會影響其他EKU或證書型別（代碼簽名、電子郵件等）？

A:否，此更改特定於TLS服務器證書。代碼簽名和電子郵件證書有它們自己的EKU要求。

問9.在哪裡可以看到有關此變更的官方要求？

A:Google Chrome根程式策略提供了在TLS伺服器證書中禁止clientAuth EKU的准則。

問題10：在我的生產環境中不使用客戶端和伺服器EKU屬性的證書是否安全？

答：對於生產環境，強烈建議客戶使用具有適當EKU屬性的證書。這一做法確保了安全性、相容性，並符合行業標準和最佳實踐。不具EKU屬性的證書僅應視為臨時解決辦法，並且必須明確瞭解相關的風險。

相關資訊

- 如需其他協助，請聯絡思科技術協助中心(TAC)。需要有效的支援合約：Cisco全球支援聯絡人。
- 思科支援與下載:思科技術支援與下載

相關錯誤

- CSCwt94492 ENH:FMC應驗證用於pxGrid整合的客戶端證書中是否存在客戶端身份驗證EKU屬性
- CSCwt94509加強版：FMC應顯示一條消息，指示用於pxGrid整合的客戶端證書中需要Client Authentication EKU屬性
- CSCwt61767 2026年5月EKU僅伺服器更改 — 如果EKU不夠，請發出ASA配置警告
- CSCws83036 EKU:ISE中ClientAuth EKU實施的影響評估

思科ISE參考

- 公告：FN74392 - Cisco Identity Services Engine:從2026年5月開始的公共CA客戶端身份驗證EKU更改對安全通訊的影響 — 提供解決方法
- 準備身份服務引擎，使其適用於公共證書頒發機構頒發的證書中的擴展金鑰使用限制

外部參照

- Chrome根程式策略
- IdenTrust入口網站
- SSL — 從TLS伺服器證書中刪除客戶端身份驗證EKU — 您需要瞭解的資訊

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。