準備在公共CA證書中客戶端身份驗證EKU日落的思科ISE

目錄

簡介

本文檔描述了由於公共證書頒發機構使用客戶端身份驗證EKU頒發的TLS證書即將更改而對ISE服務的影響。

背景資訊

數位證書是由受信任的證書頒發機構(CA)頒發的電子憑證，通過確保身份驗證、資料完整性和機密性來保護伺服器和客戶端之間的通訊。這些證書包含定義其用途的擴展金鑰用法(EKU)欄位：

- 伺服器驗證EKU(id-kp-serverAuth):在伺服器出示證書以證明身份時使用
- 使用者端驗證EKU(id-kp-clientAuth):用於雙方TLS(mTLS)連線，其中雙方相互進行身份驗證

傳統上，單個證書可以同時包含伺服器和客戶端身份驗證EKU，使其可用於雙重用途。這對於思科ISE等在不同連線場景中同時充當伺服器和客戶端的產品尤為重要。

問題定義

Chrome根程式策略更改

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。

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)
- 證書必須僅包括伺服器身份驗證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最終會從Chrome根儲存中刪除
- 沒有更多公共伺服器TLS證書的混合使用的根CA
- 實施時間表：2027年3月。

公共CA響應時間表

- 2025年10月：許多公共CA(DigiCert、Sectigo、SSL)預設開始頒發僅伺服器證書。
- 2026年5月：許多公共CA伺服器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

附註：此策略僅適用於公共CA頒發的證書。私有PKI和自簽名證書不受此策略的影響。

It如何影響思科ISE

受影響的產品

所有Cisco ISE版本都受到影響：

- ISE 3.1
- ISE 3.2
- ISE 3.3
- ISE 3.4
- ISE 3.5

附註：思科ISE 2.x版本也受到影響；但是，未計畫任何修復，因為這些版本已到達生命期(EOL)。

思科ISE的雙重角色

在各種連線方案中，ISE同時充當伺服器和客戶端，要求證書同時具有伺服器和客戶端身份驗證EKU。

Cisco ISE作為伺服器(需要伺服器身份驗證EKU):

- Pxgrid
- ISE消息服務

作為客戶端的Cisco ISE（需要客戶端身份驗證EKU）:

- TC-NAC
- 安全系統日誌
- LDAPS
- Radius DTLS

具體受影響使用情形

下表總結了可能受即將進行的客戶端身份驗證EKU更改影響的思科ISE服務，以及每個服務的預期影響。

服務	影響
pxGrid	pxGrid證書用於ISE節點和外部pxGrid整合之間的通訊。雖然外部pxGrid整合僅需要伺服器身份驗證EKU，但由於UI限制，思科ISE當前要求匯入的pxGrid證書同時包含伺服器身份驗證EKU和客戶端身份驗證EKU。因此，公共CA頒發的pxGrid證書通常與兩個EKU一起部署。
ISE訊息服務(IMS)	IMS用於內部ISE服務之間的後端通訊。思科ISE當前需要IMS證書以同時包含伺服器身份驗證EKU和客戶端身份驗證EKU。僅具有伺服器身份驗證EKU的公共CA續訂的證書不能用於IMS，這可能會導致內部ISE通訊失敗。

TC-NAC	如果管理員證書僅包含Server Authentication EKU，則當啟用FIPS模式或使用mTLS配置Tenable（在ISE 3.4P3和3.5版中引入）時，TC-NAC的基於證書的身份驗證可能會受到影響。
安全系統日誌	
LDAP	
RADIUS DTLS	

⚠ 注意：客戶應驗證任何外部pxGrid客戶端使用的證書型別。在續訂時，公共CA簽名的證書可能不再包括客戶端身份驗證EKU。與ISE通訊時，外部pxGrid客戶端整合必須包括客戶端身份驗證EKU，否則連線將被拒絕。

問題症狀

在Cisco ISE中部署Server Authentication EKU only證書後，當客戶嘗試上傳pxGrid或ISE消息服務(IMS)證書時，將觀察思科ISE GUI中的證書匯入失敗，這些證書不符合所選服務的當前擴展金鑰使用(EKU)要求。

GUI中顯示的錯誤消息示例如下所示。

行動

稽核當前證書（強制性第一步）

- 準備所有公共TLS證書的清單，以確定哪些證書包含客戶端身份驗證EKU
- 文檔證書用法：根據上表確定使用哪些使用Public-CA簽名的證書。
- 驗證CA和根資訊：記錄哪個CA和根頒發每個證書
- 檢查到期日期：策略實施前進行戰略性的續訂計畫

需要客戶端EKU的服務建議

下表為依賴包含客戶端身份驗證EKU的證書的Cisco ISE服務和整合提供了建議操作。

服務	建議的操作
TC-NAC	• 使用Tenable時，可以在可使用端禁用嚴格EKU驗證以保持連線。

安全系統日誌	
LDAP	
RADIUS DTLS	
PxGrid客戶端 (CatC、FMC...)等等)	
EAP-TLS	

短期變通辦法（2026年6月之前）

管理員可以從以下任一解決方法選項中進行選擇：

選項 1:切換到提供組合EKU證書的公共根CA

某些公共根CA（例如DigiCert和IdenTrust）會從另一個根發出具有組合EKU的證書，該根不能包含在Chrome瀏覽器信任儲存中。

公共根CA和EKU型別的示例：

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

此方法的前提條件：

- 與您的CA提供商協調，檢查此類證書的可用性。
- 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。
- 與通訊對等方交換根證書資訊。
- 此方法避免了立即進行軟體升級的需要。

證書管理參考：

- 思科身份服務引擎管理員指南3.3版

- 在ISE上配置證書續訂

選項 2:續訂當前憑證以延長其有效性

在2026年5月之前由公共根CA頒發的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。

續訂策略

一般性建議包括：

- 在策略取消設定之前續訂組合的EKU證書
- 要獲得最高證書有效性，計畫在2026年3月15日之前續訂證書。
- 在此日期之後，公共CA頒發的證書的有效期僅為200天。
- 如果您希望使用此選項，思科強烈建議在此日期之前續訂證書。
- 公共CA策略和實施日期可能不同。
- 某些公共CA已停止發佈組合的EKU證書，並且預設情況下無法提供一個。
- 要使用組合的EKU生成證書，請與您的CA機構合作，使用公共CA提供的特殊配置檔案。

選項 3:評估並遷移至其他CA提供商

專用PKI方法

- 評估過渡到私有PKI的可行性
- 設定專用CA以使用組合的EKU（具有所需EKU的伺服器和客戶端證書）頒發單個證書
- 當頒發私有CA簽名的證書時，您需要與對等體共用根證書資訊。
- 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。
- 專用CA不受Chrome根計劃策略的約束
- 提供對證書策略的長期控制

長期解決方案（需軟體升級）

客戶應將Cisco ISE升級到引入更新證書處理的修補程式版本，以支援根據新CA策略頒發的證書。

以下修補程式版本計畫於2026年4月解決此問題：

Cisco ISE版本	修補程式版本
ISE 3.1	補丁11
ISE 3.2	補丁10
ISE 3.3	補丁11

ISE 3.4	補丁6
ISE 3.5	補丁3

安裝修補程式後的行為

PxGrid證書

安裝修補程式版本之後：

- 將刪除當前的UI要求，該要求將對pxGrid證書強制實施伺服器身份驗證EKU和客戶端身份驗證EKU。
- 思科ISE將允許匯入包含僅伺服器身份驗證EKU、伺服器身份驗證和客戶端身份驗證EKU或無EKU擴展的pxGrid證書。
- 僅包含客戶端身份驗證EKU的證書不會被接受。

ISE訊息服務(IMS)憑證

對於ISE 3.1、3.2和3.3

安裝補丁程式後行為沒有發生改變。ISE消息服務將繼續要求具有客戶端和伺服器EKU的證書。客戶應計畫在當前證書到期後使用ISE內部CA證書。

對於ISE 3.4和3.5

IMS現在僅支援包含伺服器身份驗證EKU的公共CA證書。但是，由於IMS僅用於內部思科ISE通訊，因此思科建議在證書續訂時使用ISE內部CA證書。

決策樹

開始:您是否使用思科ISE上的公共CA證書？

|

├─否：私有PKI或自簽名

| └─ 不需要操作 — 不受策略影響

|

└─是：公共CA證書正在使用

  |

  ├─它們是否用於「特定受影響使用情形」一節中提到的任何服務？

  | |

當ISE├─作TLS客戶端時使用│ Web服務

│ │ └─ 閱「需要客戶端EKU的服務建議」部分。

│ │

│ └─ Services作為TLS伺服器（PxGrid或IMS）時

│ │

│ └─選擇您的方法：

│ │

│ ├─選項A:切換到備用根CA

│ │ ├─ Contact CA provider for combined EKU from alternative root（從備選根獲取組合EKU的聯絡人CA提供商）

│ │ ├─確保所有對等體信任新根

│ │ └─ 無需立即升級軟體

│ │

│ ├─選項B:在截止時間之前續訂證書

│ │ ├─這將有助於緩解修補思科ISE的緊急狀況

│ │ │

│ │ ├─為最大有效性：在2026年3月15日之前續約

│ │ └─ 在證書到期前購買時間

│ │

│ ├─選項C:遷移到專用PKI

│ │ ├─置專用CA基礎架構

│ │ ├─ Issue combined EKU證書

│ │ ├─在ISE受信任儲存中安裝新CA

│ │ └─ 長期控制

│ │

│ └─選項D:規劃軟體升級

│ ├─應用所需的ISE補丁版本（從2026年4月開始提供）

常見問題 (FAQ)

一般問題

Q:如果使用私有PKI，是否需要擔心此問題？

A:否。此策略僅影響公共根CA頒發的證書。私有PKI和自簽名證書不受影響。

Q:是否可以繼續使用現有的證書？

A:是的，包含組合EKU的現有證書在過期之前始終有效。當您需要續訂時，會出現問題。它們同時適用於TLS和mTLS連線，直到到期。

Q:如何知道我使用的是mTLS還是標準TLS?

A:檢視特定受影響使用案例。

升級問題

憑證管理

日程表問題

Q:2026年6月15日會發生什麼？

A:Chrome停止信任同時包含伺服器和客戶端身份驗證EKU的公共TLS證書。使用此類證書的服務可能會失敗。

Q:為什麼必須在2026年3月15日前續訂？

A:2026年3月15日後，證書有效期從398天縮短至200天。在此日期之前續訂可為您提供最長證書生存期。

問：採取行動的截止日期是什麼？

A:有多個截止日期：

- 2026年3月15日：證書有效期縮短到200天
- 2026年5月：大多數公共CA完全停止發佈合併EKU
- 2027年3月：完全強制實施Chrome策略

其他資源

- 思科錯誤 ID:CSCws83036-ISE中ClientAuth EKU實施的影響評估

外部參照

- Chrome根程式策略

證書頒發機構資源

- IdenTrust入口網站

結論

公共CA證書中客戶端身份驗證EKU的設定代表重大的安全策略轉變，影響使用mTLS連線的Cisco ISE部署。雖然這是行業範圍的變更，但影響評級是關鍵的，需要立即採取措施來防止服務中斷。

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）。