為公共CA證書中的客戶端身份驗證EKU日落準備Expressway

目錄

簡介

本文檔介紹Cisco Expressway上的Chrome根程式策略更改，以及公共CA證書中6/26之後的Client Authentication EKU失效。

備份組資訊

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。這對於在不同連線場景中同時充當伺服器和客戶端的Cisco Expressway等產品尤為重要。

問題定義

Chrome根程式策略更改

自2026年6月起，Chrome根程式策略限制包含在Chrome根儲存中的根證書頒發機構(CA)證書，逐步停用多用途根來調整所有公共金鑰基礎結構(PKI)層次結構，以便僅使用TLS伺服器身份驗證使用案例。

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才能維護來自Google Chrome瀏覽器的信任
- 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：2026年6月

公共CA響應時間表

- 2025年10月：預設情況下，許多公共CA(DigiCert、Sectigo、SSL)開始頒發僅伺服器證書
- 2026年2月11日：讓我們加密停止使用經典ACME配置檔案使用客戶端身份驗證EKU發送證書
- 2026年5月：公共CA伺服器停止頒發客戶端身份驗證EKU證書
- 2026年6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。

相關思科檔案

- 思科錯誤 ID:CSCwr73373 — 支持Expressway的單獨伺服器和客戶端證書
- 公告:FN74362
- Chrome根程式策略：Chrome根程式策略文檔

It如何影響Expressway解決方案

受影響的產品

根據Field Notice FN74362，所有Cisco Expressway版本都會受到影響：

產品	受影響的版本	影響
Expressway核心和邊緣	X14（所有版本）	X14.0.0到X14.3.7 — 所有版本均受影響
Expressway核心和邊緣	X15（X15.4之前的版本）	X15.0.0到X15.3.2 — 所有版本均受影響

Expressway的雙重角色

Cisco Expressway產品（Expressway-C和Expressway-E）在各種連線場景中同時充當伺服器和客戶端，需要具有伺服器和客戶端身份驗證EKU的證書。

Expressway E as Server（需要伺服器身份驗證EKU）：

- HTTPS瀏覽器訪問
- SIP UC遍歷連線
- Webex邊緣音訊/MRA連線

Expressway E as Client（需要客戶端身份驗證EKU）：

- B2B通訊
- MRA（移動和遠端訪問）連線
- XMPP聯合
- SIP鄰居區域/CMS連線
- 與外部實體的互動
- 連線到思科雲（MRA自註冊）

具體受影響使用情形

Cisco Expressway中當前用於mTLS連線的具有客戶端身份驗證EKU的公共CA簽名證書是Expressway伺服器證書。此證書用於以下mTLS連線：

1. 通過mTLS進行的SIP B2B呼叫 — Expressway E成為mTLS連線的客戶端或伺服器，具體取決於會話啟動的站點
2. 基於mTLS的SIP IMP聯合 — Expressway E成為mTLS連線的客戶端或伺服器，具體取決於會話啟動的站點
3. UC遍歷區域 — Expressway C提供客戶端身份驗證EKU
4. 採用mTLS配置的遍歷區域 — Expressway C提供客戶端身份驗證EKU
5. 採用mTLS配置的SIP鄰居區域 — Expressway成為mTLS連線的客戶端或伺服器，具體取決於會話啟動的站點，包括以下連線：

- Cisco Unified Communications Manager(Unified CM)
- Cisco Unity
- 思科整合邊界元件(CUBE)
- 思科會議伺服器(CMS)
- 連線到思科雲 — MRA註入（Expressway啟動到思科雲的連線並顯示客戶端身份驗證EKU）

行動

稽核當前證書（強制性第一步）

根據現場通知FN74362，在考慮變通方法和解決方案選項之前：

- 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
- 備份Cisco Expressway例項，或手動複製已簽名的證書和私鑰
- 文檔證書用法：確定哪些證書用於mTLS連線
- 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

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型別示例(根據FN74362):

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：

- Cisco Expressway證書建立和使用部署指南(X14.0)
- Cisco Expressway證書建立和使用部署指南(X15.0)

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。

讓我們加密證書的特殊注意事項

根據FN74362，如果您使用讓我們加密證書：

- 目前，Expressway使用的經典ACME配置檔案是硬編碼的，使用者無法對其進行修改
- 此傳統ACME配置檔案當前用於請求同時包含伺服器和客戶端身份驗證EKU的證書
- 自2026年2月11日起，使用此配置檔案的證書請求不再在Let's Encrypt生成的證書中包括客戶端身份驗證EKU
- 有關詳細資訊，請參閱在2026年結束TLS客戶端身份驗證證書支援 — 讓我們加密

用於加密使用者的措施項

- 在2026年2月11日之前續訂證書 — 最好儘可能快地延長該日期，以最大限度地提高90天的有效期。
- 禁用ACME自動計畫程序，以防止證書在2026年2月11日之後自動續訂。
- 此操作有助於避免證書被僅包含伺服器身份驗證EKU的版本意外覆蓋。
- 如果您在2026年2月11日之前沒有續約，請聯絡Cisco TAC獲取支援。

選項 3:評估並遷移至其他CA提供商

此選項適用於：僅Expressway C；不適用於Expressway E。

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

⚠ 注意：此選項對Expressway-E不可行，後者要求面向外部的服務和瀏覽器信任具有公共CA證書。

長期解決方案（需軟體升級）

根據Field Notice FN74362，思科正在固定版本中實施產品增強功能，以全面解決此問題。

固定發佈計畫：

產品	受影響的版本	固定版本	修復目的	可用性
Cisco Expressway	X14.x（所有版本） X15.x（低於X15.4）	X15.4	間歇性解決方案：允許在Expressway E上額外上傳ServerAuth EKU專用簽名證書，並允許對Expressway E和Expressway C之間的MRA SIP訊號進行證書驗證調整	2026年2月
Cisco	X14.x（所有版本	X15.5	全面的解決方案：提供用於隔離客戶端和伺	2026年

Expressway	） X15.x（低於X15.5）		服器證書的UI增強功能，並為管理員提供禁用EKU檢查的選項	5月

附註：Cisco Expressway E和Expressway C必須升級到同一版本。

Cisco Expressway X15.4解決方案詳情（2026年2月）

用途:間歇性解決方案，僅使用ServerAuth EKU容納證書並啟用MRA註冊

主要增強功能包括：

- 取消證書上傳限制
- 允許管理員在Expressway E上僅使用伺服器身份驗證EKU通過Web GUI上傳證書
- 以前，Expressway拒絕僅伺服器證書
- 調整MRA的證書驗證
- 修改MRA解決方案中Expressway-E和Expressway-C之間SIP信令的證書驗證
- 允許接受來自第三方應用程式的僅伺服器證書

可以升級到X15.4的人員：

- 如果部署新的或重新部署現有的Expressway-E for MRA（僅伺服器簽名證書），
- 如果您在2026年2月11日後使用ACME（讓我們加密）證書。
- 需要升級只包含伺服器身份驗證EKU的簽名證書的現有部署。
- 如果您在mTLS連線中遇到與證書相關的身份驗證問題

X15.4的重要要求：

- Expressway-E和Expressway-C都必須升級到X15.4
- 在維護時段規劃升級，以最大限度地減少服務中斷

X15.4的限制如下：

- 這是一種間歇性解決方案，可解決直接的相容性問題
- 不提供完全雙證書支援
- 不包含用於禁用EKU檢查的服務引數
- mTLS連接可能會失敗，具體取決於會話啟動的站點

Cisco Expressway X15.5解決方案詳情（2026年5月）

目的：全面的解決方案，滿足全球Google Chrome根計畫要求

主要產品增強功能：

- 客戶端和伺服器證書的分隔
- 在同一介面上啟用對兩個獨立證書的支援

- Expressway證書包含不同的伺服器身份驗證EKU和客戶端身份驗證EKU
- 使用隔離的證書角色促進正確的mTLS連線
- 使用者介面和後端增強功能
- 用於單獨管理兩個證書的新證書管理介面
- 證書上傳期間的客戶端身份驗證EKU驗證，以避免意外的MTLS連線丟棄
- 管理員可以單獨上傳和管理伺服器和客戶端證書
- 用於禁用客戶端身份驗證EKU檢查的選項
- 允許管理員根據各個企業要求禁用客戶端身份驗證EKU檢查的服務引數
- 允許Cisco Expressway從請求僅使用伺服器身份驗證EKU證書連線的遠端對等體（客戶端）忽略EKU
- 在沒有客戶端身份驗證EKU證書的情況下，允許Expressway將伺服器身份驗證EKU專用證書用作客戶端證書

附註：在這種情況下，遠端對等體還必須支援類似的忽略客戶端身份驗證EKU模型

決策樹

開始:您是否在Expressway上使用公共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mTLS連線？（檢查特定受影響使用案例中的使用案例）部分

  │ │

  │ ├─否：僅伺服器身份驗證

  │ │ └─ 影響最小 — 監控未來的變更

  │ │

  │ └─是：使用客戶端身份驗證EKU的mTLS連線

  │ │

└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

├如果我們加密：在2026年2月11日之前續約

└後禁用ACME計畫程式

├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:遷移至專用PKI（僅限Expressway-C）

├置專用CA基礎架構

├ Issue combined EKU證書

├向所有對等點分髮根

└ 長期控制，不適用於Expressway-E

└選項D:規劃軟體升級

├急需？→升級到X15.4（2026年2月）

└全面解→方案升級到X15.5（2026年5月）

└ 然後取得獨立的伺服器/使用者端憑證

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:如果不使用mTLS連線該怎麼辦？

答：如果僅使用標準TLS（伺服器身份驗證），則不會受到此策略的影響。僅伺服器證書將繼續運行。但是，請根據特定受影響使用情形部分中的清單驗證您的使用情形，因為一些使用情形預設使用mTLS。

Q:我到Expressway的標準HTTPS Web連線是否停止工作？

答：否。標準TLS連線不受影響。即使使用僅伺服器EKU證書，對Expressway的Web瀏覽器訪問仍然可以正常運行。

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部分。

我現在能做什麼？

答：思科強烈建議立即採取以下措施：

- 稽核您的證書

  標識用於mTLS的公共TLS證書

- 提前續訂證書

  在2026年3月15日之前續訂，以最大限度地提高有效性

- 控制ACME自動化

  禁用可能會意外更換證書的自動續訂

- 與您的CA協調

  某些CA提供臨時或備用證書配置檔案

Q:CUCM SU3(a)是否與X15.4和X15.5相容

A:是

Q:在Cisco Expressway E（X15.5版本）中禁用客戶端EKU檢查是否存在安全漏洞

答：證書仍然檢查CN/SAN以驗證連線源是否有效，只繞過預設情況下包含的EKU驗證（客戶端角色用途證書），直到Google引起安全擔憂，因此不能與之前相比出現安全問題。

讓我們加密特定的

Q:我在Expressway上使用Let's Encrypt with ACME。我能做什麼？

A:

1. 在2026年2月11日之前（儘可能接近該日期）續訂您的證書
2. 續訂後立即禁用ACME自動計畫程式
3. 計畫升級到X15.5以獲得長期解決方案

Q:是否可以修改ACME配置檔案以繼續獲取組合的EKU證書？

A:否。目前，Expressway使用使用者無法修改的硬編碼「傳統」ACME配置檔案，請聯絡Cisco TAC以獲取ACME證書配置檔案支援。

升級問題

Q:我是否需要同時升級Expressway-E和Expressway-C?

A:是的，絕對的。兩者必須升級到相同版本（X15.4或X15.5）才能正常運行。

Q:我能升級到X15.4還是等待X15.5?

A:

- 如果您有緊急問題或需要立即接受純伺服器證書，請升級到X15.4
- 如有可能，請等待X15.5（2026年5月）提供支援雙證書的綜合解決方案

問：證書續訂後，我的群集複製中斷。發生了什麼事？

答：您的新證書很可能只有伺服器身份驗證EKU，但是：

- 如果X15.4之前的版本具有TLS驗證=實施：群集對等體無法在沒有客戶端身份驗證EKU的情況下建立mTLS連線
- 解決方案選項（任一）：

  將TLS驗證模式設定為「允許」（不太安全）

  從備用CA根獲取具有組合EKU的證書

  升級到X15.4或更高版本，可繞過ClusterDB的客戶端身份驗證EKU驗證

Q:升級到X15.4後，我是否可以將實施模式與群集中的僅伺服器證書一起使用？

答：是。從X15.4開始，Expressway會繞過mTLS ClusterDB連線的客戶端身份驗證EKU驗證。因此，即使一個或多個群集節點僅具有伺服器身份驗證EKU，也可以將「TLS驗證」設定為「實施」。

Q:為什麼我無法通過Expressway Web GUI上傳證書？

答：在X15.4之前，Web GUI實施硬編碼驗證，該驗證要求證書具有客戶端身份驗證EKU。如果您的憑證僅具有伺服器驗證EKU，則有兩個選項：

- 使用SCP（安全複製協定）將證書直接上傳到伺服器（/persistent/Certs資料夾）
- 升級到X15.4或更高版本（僅限Expressway-E），可取消此限制

Q:升級到X15.4後，我仍然無法將僅伺服器證書上傳到Expressway-E

A：升級後，請確保啟用此命令

xConfiguration XCP TLS證書CVS EnableServerEkuUpload:於

Q:我升級到X15.4。現在是否可在Expressway-E和Expressway-C上上傳僅伺服器證書？

答：否。X15.4僅取消了Expressway-E的上傳限制。 Expressway-C仍需要組合的EKU證書才能通過Web GUI上傳。這是因為Expressway-C經常作為UC遍歷區域中的TLS客戶端並且要求客戶端身份驗證EKU。請確保在Expressway-E上運行此命令。此命令不在Expressway-C上運行

xConfiguration XCP TLS證書CVS EnableServerEkuUpload:於

Q:在證書續訂後，我無法註冊智慧許可證。為什麼？

A:證書續訂後的智慧許可失敗通常與EKU無關：

- 檢查Expressway是否可以訪問tools.cisco.com(CSSM)
- 驗證防火牆規則是否允許HTTPS出站（埠443）
- 檢查代理配置是否正確（如果使用HTTP Proxy）
- 驗證Expressway信任儲存中是否信任CSSM伺服器證書
- 智慧許可不需要clientAuth，因此此策略更改不會影響它

特定MRA（移動和遠端訪問）

Q:Expressway-E上的MRA是否需要客戶端身份驗證EKU?

A:取決於Expressway版本：

- X15.4之前:是，間接需要

  在MRA SIP信令期間，Expressway-E將其SIP服務消息中的簽名證書傳送到Expressway-C

  Expressway-C驗證證書，要求客戶端身份驗證和伺服器身份驗證EKU

  如果沒有組合EKU，MRA SIP註冊將失敗

- X15.4及更高版本:否

  Expressway-C不再在SIP SERVICE消息中驗證客戶端身份驗證EKU

  Expressway-E僅需要用於MRA的伺服器身份驗證EKU

UC遍歷區域單向運行（Expressway-C僅驗證Expressway-E伺服器證書）

Q:為什麼我的鄰居區域在上載Expresswayx15.4上的伺服器身份驗證EKU

A:如果將TLS驗證模式設定為「開啟」，則需要具有客戶端驗證EKU。因此，可以在鄰居區域配置中禁用TLS驗證

Q:MRA正常工作需要哪些證書？

A:對於典型的MRA部署：

元件	證書要求	需要EKU	備註
Expressway-E（X15.4之前）	serverAuth + clientAuth	兩者	通過Exp-C進行SIP服務驗證
Expressway-E(X15.4+)	僅serverAuth	僅伺服器	已繞過客戶端EKU檢查
Expressway-C	clientAuth + serverAuth	兩者	在UC遍歷中始終充當客戶端
UC遍歷區域	單向驗證	Exp-E: serverAuth Exp-C:clientAuth	Exp-C驗證Exp-E伺服器證書

Q:我的MRA工作正常，但在使用僅伺服器EKU續訂Expressway-E證書後，SIP註冊失敗。什麼錯誤？

答：如果您運行的是X15.4之前的版本，則MRA SIP信令要求Expressway-E在SIP SERVICE消息中同時提供伺服器和客戶端身份驗證EKU。您的選項：

- 獲取具有組合EKU的證書
- 切換到發出組合EKU的備用CA根
- 將Expressway-E和Expressway-C升級到X15.4或更高版本（推薦）

憑證管理

Q:如何從DigiCert或IdenTrust獲取包含組合EKU的證書？

A:聯絡您的CA提供商並從其備用根目錄請求仍會發出合併EKU的證書。

Q:我的CA說他們只能提供伺服器專用證書。我能做什麼？

A:您有以下幾種選擇：

- 檢查替代根：詢問您的CA他們是否具有合併EKU問題的其他根源（如DigiCert Assured ID或IdenTrust Public Sector）
- 交換機CA提供商：從非Chrome受信任的根目錄查詢提供組合EKU的CA
- 使用專用PKI:為組合的EKU證書設定內部CA（僅限Expressway-C部署）
- 升級到X15.4:間歇性解決方案，僅使用ServerAuth EKU容納證書並啟用MRA註冊
- 可用後升級到X15.5:規劃雙證書架構，其中純伺服器證書是可接受的，並提供全面的解決方案來滿足全球Google Chrome根計畫要求

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2月11日：通過classic ACME讓Encrypt停止組合EKU
- 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
- 2026年6月：完全強制實施Chrome策略

其他資源

思科檔案

- 現場通知FN74362:由於即將對TLS證書進行更改，Cisco Expressway對安全通訊的影響
- 思科錯誤ID CSCwr73373:支援Expressway的單獨伺服器和客戶端證書

外部參照

- Chrome根程式策略
- 讓我們加密：2026年結束TLS客戶端身份驗證證書支援
- CA/瀏覽器論壇基線要求

證書頒發機構資源

- DigiCert支援入口網站
- IdenTrust證書服務

- 讓我們加密社群論壇
- Sectigo知識庫

結論

公共CA證書中的客戶端身份驗證EKU的設定表示重大的安全策略變化，影響使用mTLS連線的Cisco Expressway部署。雖然這是一個全行業範圍的變更，但根據FN74362現場通知，影響級別為「嚴重」，需要立即採取措施防止服務中斷。

要點

- 這將影響所有Expressway版本（X14和X15之前的X15.4）
- 立即稽核證書 — 這是強制性的第一步
- 提供多種解決方法 — 選擇最適合您環境的方法
- 長期解決方案需要進行軟體升級 — 為X15.5制定計畫
- 必須同時升級Expressway-E和Expressway-C
- 讓我們加密使用者的最早截止日期是2026年2月11日

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）。