准备公共CA证书中的客户端身份验证EKU日落的Expressway

目录

简介

本文档介绍Cisco Expressway上的Chrome根计划策略更改和客户端身份验证EKU在6/26之后的公共CA证书中的失效。

备份组信息

数字证书是由受信任的证书颁发机构(CA)颁发的电子凭证，通过确保身份验证、数据完整性和机密性来保护服务器和客户端之间的通信。这些证书包含定义其用途的扩展密钥使用(EKU)字段：

- 服务器身份验证EKU(id-kp-serverAuth):服务器提供证书以证明身份时使用
- 客户端身份验证EKU(id-kp-clientAuth):用于双向TLS(mTLS)连接，其中双方相互进行身份验证

传统上，单个证书可以同时包含服务器和客户端身份验证EKU，使其具有双重用途。这对于在不同连接场景中同时充当服务器和客户端的产品（例如Cisco Expressway）尤为重要。

问题定义

Chrome根计划策略更改

自2026年6月起，Chrome根程序策略限制包含在Chrome根存储中的根证书颁发机构(CA)证书，逐步取消多用途根以调整所有公共密钥基础结构(PKI)层次结构以仅服务TLS服务器身份验证使用案例。

主要政策要求

- 公共根CA必须声明仅用于服务器身份验证的扩展密钥使用(EKU)(id-kp-serverAuth)
- 证书必须仅包含服务器身份验证EKU才能从Google Chrome浏览器保持信任
- 禁止在这些证书中包含客户端身份验证EKU
- 继续使用客户端身份验证EKU颁发证书的根CA最终会从Chrome根存储中删除
- 公共服务器TLS证书没有更多混合使用的根CA
- 实施时间表：2026年6月

公共CA响应时间表

- 2025年10月默认情况下，许多公共CA(DigiCert、Sectigo、SSL)开始发布纯服务器证书
- 2026年2月11日：让我们加密停止使用传统ACME配置文件使用客户端身份验证EKU发送证书
- 2026年5月：公共CA服务器停止颁发客户端身份验证EKU认证
- 2026年6月：Chrome根计划策略完全生效

注意：此策略仅适用于公共CA颁发的证书。私有PKI和自签名证书不受此策略的影响。

相关思科文档

- Cisco Bug ID:CSCwr73373 -支持Expressway的单独服务器和客户端证书
- Field Notice：FN74362
- Chrome根计划策略：Chrome根计划策略文档

It如何影响Expressway解决方案

受影响的产品

根据Field Notice FN74362，所有Cisco Expressway版本都会受到影响：

产品	受影响的版本	影响
Expressway核心和边缘	X14（所有版本）	X14.0.0到X14.3.7 — 所有受影响的版本
Expressway核心和边缘	X15（X15.4之前的版本）	X15.0.0到X15.3.2 — 所有受影响的版本

Expressway的双重角色

Cisco Expressway产品（Expressway-C和Expressway-E）在各种连接场景中同时充当服务器和客户端，需要具有服务器和客户端身份验证EKU的证书。

Expressway E作为服务器（需要服务器身份验证EKU）：

- HTTPS浏览器访问
- SIP UC遍历连接
- Webex Edge音频/MRA连接

Expressway E作为客户端（需要客户端身份验证EKU）：

- B2B通信
- MRA（移动和远程访问）连接
- XMPP联合
- SIP邻居区域/CMS连接
- 与外部实体的互动
- 连接到思科云（MRA自注册）

特定受影响的使用案例

Cisco Expressway中当前用于mTLS连接的具有客户端身份验证EKU的公共CA签名证书是

Expressway服务器证书。此证书用于以下mTLS连接：

1. 基于mTLS的SIP B2B呼叫 — Expressway E成为mTLS连接的客户端或服务器，具体取决于会话启动的站点
2. 基于mTLS的SIP IMP联合 — Expressway E成为mTLS连接的客户端或服务器，具体取决于会话启动的站点
3. UC遍历区域 — Expressway C提供客户端身份验证EKU
4. 使用mTLS配置的遍历区域 — Expressway C提供客户端身份验证EKU
5. 使用mTLS配置的SIP邻居区域 — Expressway将成为mTLS连接的客户端或服务器，具体取决于会话启动的站点，包括以下连接：

- 思科统一通信管理器(Unified CM)
- Cisco Unity
- 思科统一边界元素(CUBE)
- 思科会议服务器(CMS)
- 连接到思科云 — MRA注册（Expressway启动到思科云的连接并显示客户端身份验证EKU）

建议

审核当前证书（强制第一步）

根据现场通知FN74362，在考虑解决方法和解决方案选项之前：

- 准备所有公共TLS证书的清单，以确定哪些证书包含客户端身份验证EKU
- 备份Cisco Expressway实例或手动复制签名证书和私钥
- 文档证书用法：确定哪些证书用于mTLS连接
- 验证CA和根信息：记录颁发每个证书的CA和根证书
- 检查到期日期：在策略实施之前进行战略性的续约

短期应急方案（2026年6月之前）

管理员可以从以下解决方法选项中选择一项：

选项 1：切换到提供组合EKU证书的公共根CA

某些公共根CA（例如DigiCert和IdenTrust）使用来自备用根的组合EKU颁发证书，该证书不能包含在Chrome浏览器信任库中。

公共根CA和EKU类型示例(根据FN74362):

CA供应商	EKU类型	根 CA	签发/子CA
IdenTrust	clientAuth + serverAuth	IdenTrust公共部门根CA 1	IdenTrust公共部门服务器CA 1

DigiCert	clientAuth + serverAuth	DigiCert保证ID根G2	DigiCert保证ID CA G2

此方法的必备条件：

- 与您的CA提供商协调，检查此类证书的可用性。
- 部署证书之前，请确保提供证书的服务器和使用证书的所有客户端都信任相应的根CA。
- 与通信对等体交换根证书信息。
- 此方法可避免立即进行软件升级。

证书管理参考：

- Cisco Expressway证书创建和使用部署指南(X14.0)
- Cisco Expressway证书创建和使用部署指南(X15.0)

选项 2：续订当前证书以延长其有效期

在2026年5月之前由公共根CA颁发的同时具有服务器和客户端身份验证EKU的证书将继续有效，直到其期限到期。

续约策略

一般建议如下：

- 在策略取消设置之前续订组合的EKU证书
- 要获得最高证书有效期，计划在2026年3月15日之前更新证书。
- 在此日期之后，公有CA颁发的证书的有效期仅为200天。
- 如果您希望使用此选项，思科强烈建议在此日期之前更新证书。
- 公共CA策略和实施日期可能不同。
- 某些公共CA已停止发布组合的EKU证书，并且默认情况下无法提供这些证书。
- 要生成包含组合EKU的证书，请与您的CA机构合作并使用由公共CA提供的特殊配置文件。

加密证书的特殊注意事项

根据FN74362，如果您使用让我们加密证书：

- 目前，Expressway使用的传统ACME配置文件是硬编码的，用户无法修改
- 此传统ACME配置文件当前用于请求同时包含服务器和客户端身份验证EKU的证书
- 从2026年2月11日起，使用此配置文件的证书请求不再在Let's Encrypt生成的证书中包含客户端身份验证EKU
- 有关详细信息，请参阅在2026年结束TLS客户端身份验证证书支持 — 让我们加密

加密用户的措施项

- 在2026年2月11日前续签证书 — 最好尽可能接近该日期，以便最大限度地延长90天的有

效期。
- 禁用ACME自动调度程序，以防止证书在2026年2月11日之后自动续订。
- 此操作有助于避免证书被仅包含服务器身份验证EKU的版本无意覆盖。
- 如果您在2026年2月11日之前没有续约，请联系Cisco TAC寻求支持。

选项 3：评估并迁移到替代CA提供商

此选项仅适用于：Expressway C；不适用于Expressway E。

私有PKI方法

- 评估过渡到私有PKI的可行性
- 设置专用CA以使用组合的EKU（具有所需EKU的服务器和客户端证书）颁发单个证书
- 当颁发私有CA签名的证书时，您需要与对等体共享根证书信息。
- 在颁发或部署证书之前，请确保提供证书的服务器和使用证书的所有客户端都信任相应的根CA。
- 专用CA不受Chrome根计划策略的约束
- 提供对证书策略的长期控制

⚠ 警告：此选项对Expressway-E不可行，后者需要面向外部的服务和浏览器信任的公共CA证书。

长期解决方案（需要软件升级）

根据Field Notice FN74362，思科正在固定版本中实施产品增强功能，以全面解决此问题。

固定发布计划：

产品	受影响的版本	固定版本	修复目的	可用性
思科Expressway	X14.x（所有版本） X15.x（早于X15.4）	X15.4	间歇性解决方案：允许在Expressway E上额外上传ServerAuth EKU专用签名证书，并为Expressway E和Expressway C之间的MRA SIP信号调整证书验证	2026年2月
思科Expressway	X14.x（所有版本） X15.x（早于X15.5）	X15.5	完善的解决方案:提供用于隔离客户端和服务器证书的UI增强功能，并为管理员提供禁用EKU检查的选项	2026年5月

注意：Cisco Expressway E和Expressway C必须升级到同一版本。

Cisco Expressway X15.4解决方案详情（2026年2月）

用途:间歇性解决方案，仅使用ServerAuth EKU容纳证书并启用MRA注册

主要增强功能包括：

- 取消证书上传限制
- 允许管理员在Expressway E上通过Web GUI仅使用服务器身份验证EKU上传证书
- 以前，Expressway拒绝纯服务器证书
- 调整MRA的证书验证
- 修改MRA解决方案中Expressway-E和Expressway-C之间SIP信令的证书验证
- 允许接受来自第三方应用的纯服务器证书

可以升级到X15.4的人员：

- 如果部署新的或重新部署现有Expressway-E for MRA，且仅使用服务器签名证书。
- 如果您在2026年2月11日后使用ACME（让我们加密）证书。
- 需要升级仅包含服务器身份验证EKU的签名证书的现有部署。
- 如果在mTLS连接中遇到证书相关的身份验证问题

X15.4的重要要求：

- Expressway-E和Expressway-C都必须升级到X15.4
- 在维护时段规划升级，以最大限度地减少服务中断

X15.4的限制包括：

- 这是一个间歇性解决方案，可解决直接的兼容性问题
- 不提供完全双证书支持
- 不包括用于禁用EKU检查的服务参数
- mTLS连接可能会失败，具体取决于会话启动的站点

Cisco Expressway X15.5解决方案详情（2026年5月）

目的：提供满足全球Google Chrome根计划要求的综合解决方案

主要产品增强功能：

- 客户端证书和服务器证书的分离
- 在同一接口上启用对两个独立证书的支持
- Expressway证书包含不同的服务器身份验证EKU和客户端身份验证EKU
- 通过分离证书角色促进适当的mTLS连接
- UI和后端增强
- 新证书管理接口，用于单独管理两个证书

- 证书上传期间的客户端身份验证EKU验证，以避免意外的MTLS连接丢弃
- 管理员可以单独上传和管理服务器和客户端证书
- 禁用客户端身份验证EKU检查的选项
- 允许管理员根据各个企业要求禁用客户端身份验证EKU检查的服务参数
- 允许Cisco Expressway忽略来自请求仅使用服务器身份验证EKU证书进行连接的远程对等体（客户端）的EKU
- 在没有客户端身份验证EKU证书的情况下，允许Expressway将服务器身份验证EKU专用证书用作客户端证书

注意：在这种情况下，远程对等体还必须支持类似的忽略客户端身份验证EKU模型

决策树

开始：您是否在Expressway上使用公共CA证书？

│

├─否：私有PKI或自签名

│ └─ 无需操作 — 不受策略影响

│

└─是：正在使用的公共CA证书

  │

  ├─它们是否用于mTLS连接？（选中“特定受影响的使用案例”部分中的使用案例）

  │ │

  │ ├─否：仅服务器身份验证

  │ │ └─ 影响最小 — 监控未来的变更

  │ │

  │ └─是：使用客户端身份验证EKU的mTLS连接

  │ │

  │ └─选择您的方法：

  │ │

```
├─选项A:切换到备用根CA
│ ├─联系CA提供商获取来自备用根的合并EKU
│ ├─确保所有对等体信任新根
│ └─ 无需立即升级软件
│
├─选项B:在截止时间之前更新证书
│ ├─如果我们加密：在2026年2月11日之前续订
│ │ └─续订后禁用ACME计划程序
│ ├─对于最大有效性：在2026年3月15日之前续订
│ └─证书到期前购买时间
│
├─选项C:迁移到专用PKI（仅限Expressway-C）
│ ├─设置专用CA基础设施
│ ├─ Issue combined EKU证书
│ ├─向所有对等体分发根
│ └─ 长期控制，不适用于Expressway-E
│
└─选项D:规划软件升级
  ├─急需？→升级到X15.4（2026年2月）
  └─全面解决→案升级到X15.5（2026年5月）
  └─ 获取单独的服务器/客户端证书
```

常见问题解答 (FAQ)

一般问题

问:如果使用私有PKI，是否需要担心此问题？

A：否。此策略仅影响公共根CA颁发的证书。私有PKI和自签名证书不受影响。

问:如果不使用mTLS连接怎么办？

答：如果仅使用标准TLS（服务器身份验证），则不受此策略的影响。仅服务器证书将继续运行。但是，请根据特定受影响使用案例(Specific Affected Use Cases)部分中的列表验证您的使用案例，因为某些使用案例默认使用mTLS。

问:我到Expressway的标准HTTPS Web连接是否会停止工作？

答：没有。标准TLS连接不受影响。即使使用仅服务器EKU证书，对Expressway的Web浏览器访问仍然可以正常工作。

问:是否可以继续使用现有证书？

A：是的，包含合并EKU的现有证书在到期之前始终有效。当您需要续订时，会出现问题。它们适用于TLS和mTLS连接，直到到期。

问:如何知道我使用的是mTLS还是标准TLS?

A：查看特定受影响使用案例部分。

我现在能做什么？

答：思科强烈建议立即采取以下措施：

- 审核证书

  标识用于mTLS的公共TLS证书

- 提前更新证书

  在2026年3月15日之前续订，以最大限度提高有效性

- 控制ACME自动化

  禁用可能会意外替换证书的自动续订

- 与您的CA协调

  某些CA提供临时或备用证书配置文件

问:CUCM SU3(a)是否与X15.4和X15.5兼容

A：Yes

问:在Cisco Expressway E（X15.5版本）中禁用客户端EKU检查是否存在安全漏洞

答：证书仍检查CN/SAN以验证连接源是否有效，仅绕过默认情况下包含的EKU验证（客户端角色用途证书），直到Google提出安全问题，因此与之前相比不得存在安全问题。

让我们加密特定的

问:我在Expressway上使用Let's Encrypt with ACME。我该怎么办？

A：

1. 在2026年2月11日之前（尽可能接近该日期）更新您的证书
2. 续订后立即禁用ACME自动计划程序
3. 计划升级到X15.5以获得长期解决方案

问:是否可以修改ACME配置文件以继续获取组合的EKU证书？

A：否。目前，Expressway使用用户无法修改的硬编码“传统”ACME配置文件，请联系Cisco TAC以获取ACME证书配置文件支持。

升级问题

问:是否需要同时升级Expressway-E和Expressway-C?

A：是的，绝对的。两者必须升级到同一版本（X15.4或X15.5）才能正常运行。

问:是否可以升级到X15.4或等待X15.5?

A：

- 如果您有紧急问题或需要立即接受纯服务器证书，请升级到X15.4
- 如有可能，请等待X15.5（2026年5月）提供支持双证书的综合解决方案

问：我的群集复制在证书续订后中断。发生了什么？

答：您的新证书很可能只有服务器身份验证EKU，但是：

- 如果X15.4之前的版本具有TLS验证=实施：集群对等体无法在没有客户端身份验证EKU的情况下建立mTLS连接
- 解决方案选项（任一）：

  将TLS验证模式设置为“允许”(Permissive)（不太安全）

  从备用CA根获取具有组合EKU的证书

  升级到X15.4或更高版本，可绕过ClusterDB的客户端身份验证EKU验证

问:升级到X15.4后，我是否可以在集群中对纯服务器证书使用实施模式？

答：是。从X15.4开始，Expressway将绕过对mTLS ClusterDB连接的客户端身份验证EKU验证。因此，即使一个或多个群集节点仅具有服务器身份验证EKU，也可以将TLS验证设置为“实施”。

问:为什么我不能通过Expressway Web GUI上传证书？

答：在X15.4之前,Web GUI实施硬编码验证，该验证要求证书具有客户端身份验证EKU。如果您的证书只有服务器身份验证EKU，则有两个选项：

- 使用SCP（安全复制协议）将证书直接上传到服务器（/persistent/Certs文件夹）

- 升级到X15.4或更高版本（仅限Expressway-E），可取消此限制

问:升级到X15.4后，我仍然无法将仅服务器证书上传到Expressway-E

A：升级后，请确保启用此命令

xConfiguration XCP TLS Certificate CVS EnableServerEkuUpload:开启

问:我升级到X15.4。现在是否可以在Expressway-E和Expressway-C上上传仅服务器证书？

答：不。X15.4仅删除Expressway-E的上传限制。Expressway-C仍需要组合的EKU证书才能通过Web GUI上传。这是因为Expressway-C经常用作UC遍历区域中的TLS客户端，并且需要客户端身份验证EKU。请确保在Expressway-E上运行此命令。此命令不在Expressway-C上运行

xConfiguration XCP TLS Certificate CVS EnableServerEkuUpload:开启

问:我在证书续订后无法注册智能许可证。为什么？

A：证书续订后的智能许可故障通常与EKU无关：

- 检查Expressway是否可以访问tools.cisco.com(CSSM)
- 验证防火墙规则允许HTTPS出站（端口443）
- 检查代理配置是否正确（如果使用HTTP代理）
- 验证CSSM服务器证书在Expressway信任存储中是否受信任
- 智能许可不需要clientAuth，因此此策略更改不会影响它

特定MRA（移动和远程访问）

问:Expressway-E上的MRA是否需要客户端身份验证EKU?

答：取决于Expressway版本：

- 在X15.4之前:是，间接需要

  在MRA SIP信令期间，Expressway E将其签名证书以SIP SERVICE消息发送到Expressway C

  Expressway-C验证证书，同时需要客户端身份验证和服务器身份验证EKU

  没有合并EKU，MRA SIP注册失败

- X15.4及更高版本:无

  Expressway-C不再在SIP SERVICE消息中验证客户端身份验证EKU

  Expressway-E仅需要用于MRA的服务器身份验证EKU

  UC遍历区域单向运行（Expressway-C仅验证Expressway-E服务器证书）

问:为什么我的邻居区域在上传后发生故障Expresswayx15.4上的服务器身份验证EKU

A：如果将TLS验证模式设置为“打开”，则需要客户端身份验证EKU。因此，您可以在邻居区域配置中禁用TLS验证

问:MRA正常工作需要哪些证书？

A：对于典型的MRA部署：

组件	证书要求	需要EKU	备注
Expressway-E（X15.4之前）	serverAuth + clientAuth	两者	通过Exp-C进行SIP服务验证
Expressway-E(X15.4+)	serverAuth only	仅服务器	已绕过客户端EKU检查
Expressway-C	clientAuth + serverAuth	两者	在UC遍历中始终充当客户端
UC穿越区域	单向验证	Exp-E:serverAuth Exp-C:clientAuth	Exp-C验证Exp-E服务器证书

问:我的MRA工作正常，但在使用仅服务器EKU续订Expressway-E证书后，SIP注册失败。什么错误？

答：如果您运行的是X15.4之前的版本，则MRA SIP信令要求Expressway-E在SIP SERVICE消息中显示服务器和客户端身份验证EKU。您的选项：

- 获取具有组合EKU的证书
- 切换到发出合并EKU的备用CA根
- 将Expressway-E和Expressway-C都升级到X15.4或更高版本（推荐）

证书管理

问:如何从DigiCert或IdenTrust获取包含合并EKU的证书？

A：联系您的CA提供商并向其备用根证书申请仍然颁发合并EKU的证书。

问:我的CA说他们只能提供服务器专用证书。我该怎么办？

A：您有多种选择：

- 检查替代根：询问您的CA是否具有合并EKU问题的其他根源（如DigiCert Assured ID或IdenTrust Public Sector）
- 交换机CA提供商：从非Chrome受信任的根目录查找提供合并EKU的CA

- 使用专用PKI:为合并EKU证书设置内部CA（仅限Expressway-C部署）
- 升级到X15.4:间歇性解决方案，仅使用ServerAuth EKU容纳证书并启用MRA注册
- 可用后升级到X15.5:规划双证书架构，其中纯服务器证书是可接受的，并提供全面的解决方案来满足全球Google Chrome根计划要求

日程表问题

问:2026年6月15日会发生什么？

A：Chrome停止信任同时包含服务器和客户端身份验证EKU的公共TLS证书。使用此类证书的服务可能会失败。

问:为什么必须在2026年3月15日前续订？

A：2026年3月15日之后，证书有效期从398天减少到200天。在此日期之前续订可为您提供最长的证书有效期。

问：请问采取行动的最后期限是多久？

A：有多个截止日期：

- 2026年2月11日：让我们加密停止通过传统ACME合并EKU
- 2026年3月15日：证书有效期缩短至200天
- 2026年5月：大多数公共CA完全停止发布合并EKU
- 2026年6月：完全实施Chrome策略

其它资源

思科文档

- 售后通知FN74362:由于即将对TLS证书进行更改，Cisco Expressway对安全通信的影响
- Cisco Bug ID CSCwr73373:支持Expressway的独立服务器和客户端证书

外部引用

- Chrome根计划策略
- 让我们加密：2026年结束TLS客户端身份验证证书支持
- CA/浏览器论坛基线要求

证书颁发机构资源

- DigiCert支持门户
- IdenTrust证书服务
- 让我们加密社区论坛
- Sectigo知识库

结论

公共CA证书中的客户端身份验证EKU的取消设置代表重大的安全策略转变，会影响Cisco Expressway使用mTLS连接的部署。虽然这是一个行业范围的变更，但根据Field Notice FN74362，影响评级为“CRITICAL”，且需要立即采取措施来防止服务中断。

要点

- 这会影响所有Expressway版本（X14和X15之前的X15.4）
- 立即审核证书 — 这是强制性的第一步
- 提供多种解决方案 — 选择最适合您的环境
- 长期解决方案需要进行软件升级 — 为X15.5制定计划
- Expressway-E和Expressway-C必须一起升级
- 让我们加密用户的最早期限为2026年2月11日

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。