准备在公共CA证书中客户端身份验证EKU日落的思科ISE

目录

简介

本文档介绍对由具有客户端身份验证EKU的公共证书颁发机构颁发的TLS证书即将进行的更改对ISE服务的影响。

背景信息

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 ISE）尤为重要。

问题定义

Chrome根计划策略更改

从2026年5月开始，许多公共证书颁发机构(CA)将停止颁发包含客户端身份验证扩展密钥使用(EKU)的传输层安全(TLS)证书。 新颁发的证书通常仅包括服务器身份验证EKU。

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。
- 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：2027年3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5月：许多公共CA服务器停止颁发客户端身份验证EKU认证
- 2027年3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。

It如何影响Cisco ISE

受影响的产品

所有思科ISE版本都会受到影响：

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

注意：Cisco ISE 2.x版本也受到影响；但是，由于这些版本已经达到寿命终止(EOL)，因此未计划进行修复。

Cisco ISE的双重角色

ISE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。

Cisco ISE作为服务器(需要服务器身份验证EKU):

- PxGrid
- ISE消息服务

Cisco ISE作为客户端(需要客户端身份验证EKU):

- TC-NAC
- 安全系统日志
- LDAPS
- Radius DTLS

特定受影响的使用案例

下表汇总了受即将进行的客户端身份验证EKU更改影响的思科ISE服务，以及每个服务的预期影响。

服务	影响
pxGrid	pxGrid证书用于ISE节点和外部pxGrid集成之间的通信。虽然外部pxGrid集成只需要服务器身份验证EKU，但由于UI限制，思科ISE当前要求导入的pxGrid证书同时包含服务器身份验证EKU和客户端身份验证EKU。因此，公共CA颁发的pxGrid证书通常与两个EKU一起部署。
ISE消息服务(IMS)	IMS用于内部ISE服务之间的后端通信。思科ISE当前需要IMS证书以同时包含服务器身份验证EKU和客户端身份验证EKU。仅具有服务器身份验证EKU的公共CA续订的证书不能用于IMS，这可能导致内部ISE通信失败。

TC-NAC	如果Admin证书仅包含Server Authentication EKU，则在启用FIPS模式或使用mTLS配置时（在ISE版本3.4P3和3.5中引入），TC-NAC的基于证书的身份验证可能会受到影响。
安全系统日志	
LDAP	
RADIUS DTLS	

⚠ 警告：客户应验证任何外部pxGrid客户端使用的证书类型。续订后，公共CA签名的证书可能不再包含客户端身份验证EKU。外部pxGrid客户端集成必须包括客户端身份验证EKU，才能与ISE通信，否则连接将被拒绝。

问题症状

在思科ISE中部署仅服务器身份验证EKU证书后，当客户尝试上传pxGrid或ISE消息服务(IMS)证书时，将观察思科ISE GUI中的证书导入失败，这些证书不符合所选服务的当前扩展密钥使用(EKU)要求。

GUI中显示的错误消息示例如下所示。

建议

审核当前证书（强制第一步）

- 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
- 文档证书用法：根据上表，确定使用哪些使用Public-CA签名的证书。
- 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

需要客户端EKU的服务建议

下表为依赖于包含客户端身份验证EKU的证书的Cisco ISE服务和集成提供建议操作。

服务	推荐的操作
TC-NAC	• 当使用Tenable时，可以在Tenable端禁用严格EKU验证以保持连接。

安全系统日志	
LDAP	
RADIUS DTLS	
PxGrid客户端 (CatC、FMC...)等)	
EAP-TLS	

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类型的示例：

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：

- 思科身份服务引擎管理员指南，版本3.3
- 在ISE上配置证书续订

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。

选项 3：评估并迁移到替代CA提供商

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

长期解决方案（需要软件升级）

客户应将Cisco ISE升级到引入更新证书处理的补丁版本，以支持根据新的CA策略颁发的证书。

以下修补程序版本将解决计划于2026年4月发布的此问题：

思科ISE版本	补丁版本
ISE 3.1	补丁11
ISE 3.2	补丁10
ISE 3.3	补丁11
ISE 3.4	补丁6

ISE 3.5	补丁3

安装补丁后的行为

PxGrid证书

安装补丁版本后：

- 将删除pxGrid证书的当前的UI要求，该要求同时实施服务器身份验证EKU和客户端身份验证EKU。
- 思科ISE将允许导入仅包含服务器身份验证EKU、服务器身份验证和客户端身份验证EKU或无EKU扩展的pxGrid证书。
- 仅包含客户端身份验证EKU的证书不会被接受。

ISE消息服务(IMS)证书

对于ISE 3.1、3.2和3.3

安装补丁后行为没有变化。ISE消息服务将继续需要客户端和服务器EKU的证书。客户应计划在当前证书过期后使用ISE内部CA证书。

对于ISE 3.4和3.5

IMS现在仅支持包含服务器身份验证EKU的公共CA证书。但是，由于IMS仅用于内部Cisco ISE通信，因此Cisco建议在证书续订时使用ISE内部CA证书。

决策树

开始：您是否在思科ISE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“特定受影响使用案例”一节中提到的任何服务？

  │ │

  │ ISE├─作TLS客户端时启用服务

│ │ └─查看“需要客户端EKU的服务建议”部分。

│ │

│ └─充当TLS服务器（PxGrid或IMS）时的思科服务

│ │

│ └─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

│ │ ├─这将有助于缓解修补思科ISE的紧迫性

│ │ │

│ │ ├─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

│ │ ├─设置专用CA基础设施

│ │ ├─ Issue combined EKU证书

│ │ ├─在ISE受信任存储中安装新CA

│ │ └─ 长期控制

│ │

└─选项D:规划软件升级

├─应用所需的ISE补丁版本（从2026年4月开始提供）

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: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：复习特定受影响使用案例部分。

升级问题

证书管理

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
- 2027年3月：完全实施Chrome策略

其它资源

- Cisco Bug ID:CSCws83036 - ISE中客户端身份验证EKU实施的影响评估

外部引用

- Chrome根计划策略

证书颁发机构资源

- IdenTrust门户

结论

公共CA证书中客户端身份验证EKU的取消设置表示显着的安全策略转变，这会影响使用mTLS连接的思科ISE部署。虽然这是行业范围的变更，但影响评级非常关键，需要立即采取措施来防止服务中断。

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）。