准备身份服务引擎，以针对公共证书颁发机构颁发的证书中的扩展密钥使用限制。

目录

简介

背景信息

问题定义

- Chrome根计划策略更改
- 主要政策要求
- 时间表

它如何影响思科ISE

特定受影响的使用案例

问题症状

建议

- 具有潜在影响的审计证书并符合建议
- 短期应急方案（2026年6月之前）
- 选项 1：切换到提供组合EKU证书的公共根CA
- 选项 2：续订当前证书以延长其有效期
  - 续约策略
- 选项 3：评估并迁移到替代CA提供商
- 长期解决方案（需要软件升级）

安装补丁后的行为更改

- pxGrid证书
- ISE消息服务(IMS)证书

常见问题解答 (FAQ)

其它资源

- 外部引用
- 证书颁发机构资源

结论

简介

本文档介绍适用于证书颁发机构颁发的证书颁发标准的限制的影响，这些颁发标准与思科身份服务引擎(ISE)中的Chrome Root Certificate程序保持一致。

背景信息

数字证书是由证书颁发机构(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。扩展密钥使用(EKU)是定义证书公钥用途的属性。可用的EKU值有两个：

- 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

单个证书可以同时包含服务器和客户端身份验证EKU，使其可以达到双重目的。这对于像ISE这样的根据使用案例用作服务器或客户端的产品尤其重要。

问题定义

Chrome根计划策略更改

EKU的实施取决于CA对证书的签名。使用服务器身份验证和客户端身份验证EKU是一种常见做法。

但是，作为与此证书颁发条件一致的Chrome根程序策略更改CA的一部分，将停止对包括客户端身份验证扩展密钥使用(EKU)的TLS证书的签名。 新颁发的证书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最终从Chrome根存储中删除，导致Chrome浏览器将此类证书标记为“不受信任”

时间表

- 2025年10月与计划一致的CA(例如：DigiCert、Sectigo等。)默认情况下开始颁发仅服务器证书。
- 2026年5月：与程序一致的CA停止颁发客户端身份验证EKU证书
- 2027年3月：Chrome根计划策略完全生效

它如何影响思科ISE

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：上述更改会影响所有ISE版本，包括低于3.x的版本。但是，代码更改仅针对上一节中提到的版本发布。思科建议升级ISE以防止任何影响。

特定受影响的使用案例

表1汇总了即将发生的客户端身份验证EKU更改影响的服务，以及每个服务的预期影响。

服务	影响
pxGrid	ISE pxGrid服务需要通过pxGrid通道进行节点间通信。这意味着一些节点作为服务器工作，而其他节点作为客户端工作。 因此，要安装pxGrid证书，必须同时存在服务器身份验证EKU和客户端身份验证EKU。 因此，新发布的仅包含服务器身份验证EKU的公共CA证书的安装受限。 警告：ISE pxGrid服务执行证书EKU验证。外部pxGrid客户端证书必须包含客户端身份验证EKU，才能与ISE进行通信或拒绝连接。思科建议验证外部pxGrid客户端中使用的公共CA签名证书，以防止对集成产生影响，要了解更多相关信息，请查看Cisco Secure Firewall Impact of the Public CA Client Authentication EKU Changes Starts from 2026 May for Secure Communications。
ISE消息服务(IMS)	ISE消息传送服务(IMS)是一个执行严格mTLS验证的安全通道，用于节点间通信。 因此，需要同时存在Server Authentication EKU和Client Authentication EKU才能使服务正常运行。 仅在ISE 3.4和3.5上限制安装不包含两个EKU的新发布的公共CA证书。

	较低版本不会限制安装。但是，如果证书上不存在两个EKU，则服务操作将受到影响。
TC-NAC	选择TC-NAC供应商可续订安全中心时：在Administration > Threat Centric NAC > Add a new TC-NAC connector中创建VA。 在连接器准备好配置后，可以选择“基于证书的身份验证”(Certificate Based Authentication)作为TC-NAC连接器的身份验证方法，然后选择“ISE管理员证书”(ISE Admin Certificate)。在ISE PSN和VA DB之间建立TC-NAC连接，因此特定PSN的管理员证书是用作客户端证书的证书。 如果在Tenable上启用了严格mTLS，则需要客户端身份验证EKU。 缺少客户端身份验证EKU可能导致服务器拒绝ISE TC-NAC客户端证书。
LDAP、安全系统日志、用于CoA的RADIUS DTL	通过这三个服务，可以将特定证书用作TLS身份验证的“客户端证书”。 ISE不执行任何EKU验证。因此，对这些服务产生的影响完全取决于服务器端。 如果在服务器上实施证书EKU验证，则ISE使用的特定证书需要客户端身份验证EKU或TLS身份验证失败。

表 1：受影响的服务

问题症状

如果尝试仅针对具有特定EKU要求的服务安装具有服务器身份验证EKU的证书，则会生成图1中所示的错误。

pxGrid和ISE消息传送服务(IMS)是符合此类EKU要求的服务。

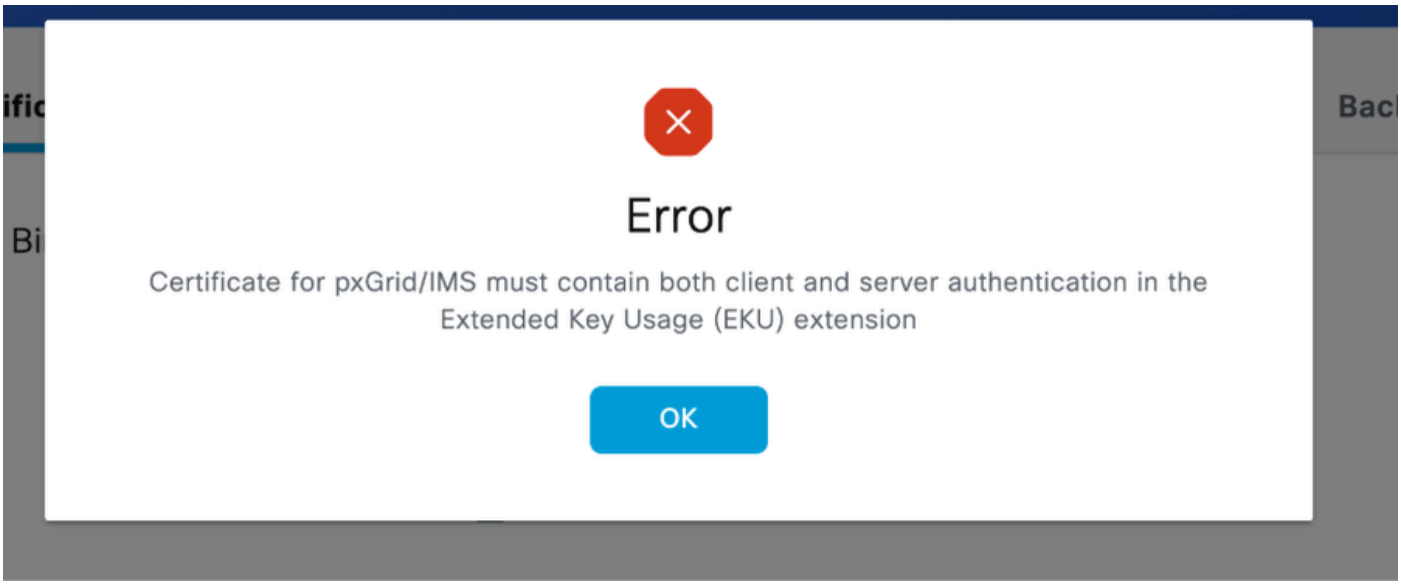


图 1:尝试安装不符合EKU要求的证书时显示的错误

建议

具有潜在影响的审计证书并符合建议

- 使用表1查找具有潜在影响的ISE服务。检查所述服务中哪些依赖于公共CA签名的证书或与Chrome根程序一致的CA。

- 记录每个证书的CA链并验证此类CA是否正在实施颁发标准更改。
- 检查到期日期：在策略实施之前进行战略性的续约。请记住，根据CA策略，可以限制客户端身份验证EKU。
- 使用表2获得受发布标准变更影响的服务的具体建议。
- ISE不显示证书上的EKU信息。如果需要验证，必须导出特定ISE证书并使用外部工具进行读取。
- 要导出ISE系统证书，请转至Administration > System > Certificates > System Certificates > Select the specific node you want export > Click in Export > Select Export Certificate Only > Click the Export按钮。

您可以使用下一个命令作为参考，检查文件名为“certnew.cer”的证书文件的信息，并使用openSSL查看Server Authentication和Client Authentication EKU。

```
mymachine% openssl x509 -noout -text -in "certnew.cer"

Certificate:

     Data:
```

```
    Version: 3 (0x2)
    Serial Number:
        XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX
Signature Algorithm: sha256WithRSAEncryption
    Issuer: DC=com, DC=mydc, CN=mycert-MYDC-DC-CA
    Validity
        Not Before: Mar 10 22:01:51 2026 GMT
        Not After : Mar 10 22:11:51 2027 GMT
    Subject: L=XX, O=XX, OU=XXX, CN=XXXX
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            RSA Public-Key: (4096 bit)
            Modulus:
               <HEX STRING>
            Exponent: XXXXX (0xXXXX)
    X509v3 extensions:
        X509v3 Key Usage:
            Digital Signature, Non Repudiation, Key Encipherment
        X509v3 Subject Key Identifier:
            XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX
        X509v3 Extended Key Usage:
            TLS Web Server Authentication, TLS Web Client Authentication
        X509v3 Subject Alternative Name:
            IP Address:x.x.x.x
        X509v3 Authority Key Identifier:
            keyid:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX
        .
        .
        .
```

服务	推荐的操作

pxGrid	如果ISE上的pxGrid证书由公共CA颁发，并且计划续订或迁移到公共CA，则我们建议进行以下操作： 1.验证证书中当前是否同时存在Server Authentication EKU和Client Authentication EKU，以及是否可以根据您的CA策略保留这两个证书 2.如果CA策略不允许存在两个EKU，则我们建议迁移证书以由ISE内部CA签名。 要进行迁移，请转到：Administration > System > Certificates > System Certificates > Select the certificate issued by the ISE internal CA of the specific node you want modify > Edit > Check the pxGrid复选框在usage section > Save。 如果ISE内部CA颁发的证书不存在，请生成一个证书。使用下一个视频作为生成证书的指导。
ISE消息证书(IMS)	如果ISE消息服务证书当前由公共CA签署，并且计划续订或迁移到公共CA，我们建议进行以下操作： 1.验证要迁移到的公共CA或用于续订的公共CA是否接受服务器身份验证和客户端身份验证EKU的使用。 2.如果公共CA不允许此操作，请迁移ISE消息传递证书以使用ISE内部CA。转至Administration > System > Certificates > Certificate Signing Request > Generate Certificate Signing Request(CSR) > select "ISE Messaging Service" in the Certificate for下拉列表>选中Regenerate ISE Messaging Service Certificate复选框>按Generate ISE Messaging Service Certificate按钮。 无需重新启动服务。 请确保从端口12001和443的角度，所有ISE节点都已启动、正在运行且可以从PAN访问，因此证书更改会正确传播到所有节点。
TC-NAC	TC-NAC服务依赖特定节点的ISE管理员证书进行mTLS身份验证。 如果证书由公共CA颁发，并且计划续订或迁移到公共CA，我们建议进行以下操作： 1.验证证书中当前是否同时存在Server Authentication EKU和Client Authentication EKU，以及是否可以根据您的CA策略保留这两个证书 2.验证是否在Tenable上启用了严格mTLS。禁用严格mTLS仅允许使用具有服务器身份验证EKU的证书。
LDAP、安全系统日志、用于CoA的RADIUS DTL	ISE不对这些服务的客户端证书执行EKU验证。如果计划续订或迁移到公共CA，请验证证书EKU是否必须在续订/迁移后更改，以及是否与服务器端的TLS策略冲突。

表 2：建议采取的行动，以避免对具体服务产生影响。

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。
- 如果未预安装CA链，则根据需要安装CA链。
- 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

一般准则：

- 在策略取消设置之前续订组合的EKU证书。
- 2026年3月15日之后，公共CA颁发的证书有效期仅为200天。
- 公共CA策略和实施日期可能不同。
- 一些公共CA已停止发布组合的EKU证书。

选项 3：评估并迁移到替代CA提供商

一般准则：

- 迁移到允许存在服务器和客户端身份验证EKU的备用CA
- 提供对证书策略的长期控制
- 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CA链

长期解决方案（需要软件升级）

客户可以将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。

接下来的补丁版本包括行为更改，以使ISE符合新的限制。计划发布日期为2026年4月：

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

安装补丁后的行为更改

⚠ 警告：此补丁在证书管理逻辑中引入行为更改。

备份ISE和IMS证书及其私钥，然后再用新证书替换它们。在安装了具有服务器身份验证

EKU的证书后卸载此补丁只会影响两个服务的TLS通信。

pxGrid证书

安装补丁版本后：

- 只允许导入包含Server Authentication EKU、Server and Client Authentication EKUs或no EKU extension的pxGrid证书。
- 仅包含客户端身份验证EKU的证书被拒绝。

ISE消息服务(IMS)证书

ISE 3.1、3.2和3.3

对于思科ISE版本3.1、3.2和3.3,IMS继续需要同时具有服务器身份验证和客户端身份验证EKU的证书。安装补丁后，将实施EKU验证，这意味着没有服务器身份验证和客户端身份验证EKU的证书将被拒绝进行安装。

当前证书过期后，客户必须计划迁移到ISE内部CA签名证书。

ISE 3.4和3.5

安装补丁后，ISE上的EKU限制会减少。使用仅包含服务器身份验证EKU（同时包含服务器和客户端身份验证EKU）或不允许使用任何EKU的CA签名证书。

仅拒绝包含客户端身份验证EKU的证书。

IMS证书用于ISE节点间通信中的服务器和客户端身份验证。



注意：即使IMS支持使用公有CA签名的证书。思科建议使用ISE内部CA证书，因为此通信仅用于内部事务。

常见问题解答 (FAQ)

如果使用私有PKI，是否需要担心此问题？

由专用CA实施的策略由每个组织定义。如果您的私有CA使用相同的发布条件，则可以使用本文档中的指南。

是否可以继续使用现有证书？

是的，在到期之前可以使用包含合并EKU的有效证书。

如何知道我使用的是mTLS还是标准TLS?

查看特定受影响使用案例部分。

其它资源

- 思科漏洞ID CSCws83036 - ISE中ClientAuth EKU实施的影响评估
- 从2026年5月开始的公共CA客户端身份验证EKU更改对思科安全防火墙的影响，用于安全通信

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。虽然这是一个行业范围的变化，但影响评级为严重，需要立即采取措施防止服务中断。

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）。