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

目录

简介

背景信息

- EKU属性的用途
- EKU属性的主要用途
- 为什么从服务器证书中删除客户端身份验证EKU?
- 对服务器环境的影响

问题说明

- Chrome根计划策略更改
- 主要政策要求
- 时间表

对思科安全防火墙产品的影响

- 受影响的产品
- 问题1. pxGrid在FMC和ISE之间的集成问题，当FMC证书缺少客户端身份验证EKU属性时
- 问题2. LDAPS服务器的FTD或ASA集成问题，当提供的证书缺少Client Authentication EKU属性
- 问题3.如果客户端证书缺少客户端身份验证EKU属性，思科安全客户端（以前称为AnyConnect）可能会遇到到FTD或ASA的连接问题
- 问题4.如果身份证书缺少Client Authentication EKU属性，则使用基于证书的身份验证的站点到站点VPN隧道失败

用于确认证书是否缺少客户端身份验证EKU属性的说明

- 使用Windows证书管理器验证.cer证书中的EKU属性
  - 示例 1：此.cer证书缺少客户端身份验证EKU属性，并且仅包括服务器身份验证EKU属性。
  - 示例 2：此.cer证书包括服务器和客户端身份验证EKU属性。
- 使用OpenSSL验证来自aPKCS#12、PEM和.cer证书的EKU属性
  - 示例 1：此.pem(PEM)证书缺少Client Authentication EKU属性，并且仅包括Server Authentication EKU属性。
  - 示例 2：此.pem(PEM)证书包括客户端和服务器身份验证EKU属性。

解决方法

- 选项1.切换到提供组合EKU证书的公用根CA
- 选项2.更新当前证书以延长其有效期
- 选项3.迁移到私有PKI以颁发组合EKU（服务器和客户端）证书
- 选项4.仅使用客户端身份验证EKU获取公共受信任证书

常见问题解答 (FAQ)

相关信息

- 相关 Bug
- 思科ISE参考
- 外部引用

简介

本文档介绍符合Chrome根证书计划的证书颁发机构对证书颁发标准施加的限制的影响，尤其是这些限制与Cisco安全防火墙产品相关的影响。

背景信息

公共受信任的TLS证书由CA颁发，这些证书必须遵守管理证书颁发和使用情况的行业策略。

由Google操作的Chrome根程序策略定义了CA必须遵循的要求，其证书才能被Google Chrome浏览器信任。这些要求会影响整个行业中发布受公共信任证书的方式。作为不断发展的安全实践的一部分，Chrome根计划正在引入更严格的证书使用指南。

因此，许多公共CA不再发行包含客户端身份验证EKU的证书，而是改为发行仅用于服务器身份验证的证书。因此，预计许多公共CA的新签发的证书仅包含服务器身份验证EKU。

Extended Key Usage(EKU)是定义数字证书中公钥的预期功能的证书扩展。它建立一组结构化的允许应用程序，确保密钥仅用于特定的加密操作。此功能由对象标识符(OID)管理，对象标识符是对每个允许的使用进行分类的唯一数字标识符，如代码签名、服务器身份验证、客户端身份验证或安全电子邮件。

当身份验证基于证书时，验证实体将审核证书以识别EKU中的对象标识符(OID)。通过嵌入EKU扩展，证书颁发机构(CA)将证书范围限制为预定义角色，其中每个指定用途都显式映射到OID。

EKU属性的用途

·定义用法：EKU属性明确允许证书执行哪些类型的身份验证或加密。

·增强安全性：通过将证书限制为特定用途，EKU有助于防止滥用或意外应用（例如，服务器证书不能用于客户端身份验证）。

·合规性：确保证书的使用符合安全策略和行业标准。

EKU属性的主要用途

1. TLS Web客户端身份验证

·允许使用证书对服务器或设备进行标识和身份验证。

•OID:1.3.6.1.5.5.7.3.2

·用于VPN、双向TLS和安全登录场景。

2. TLS Web服务器身份验证

·允许服务器使用证书向客户端证明其身份。

•OID:1.3.6.1.5.5.7.3.1

·用于HTTPS、SSL/TLS Web服务器和安全API终端。

3.代码签名

· 表示证书可用于签署软件或可执行文件。

•OID:1.3.6.1.5.5.7.3.3

·用于软件分发和完整性检查。

4.电子邮件保护

·允许证书用于签名和加密电子邮件。

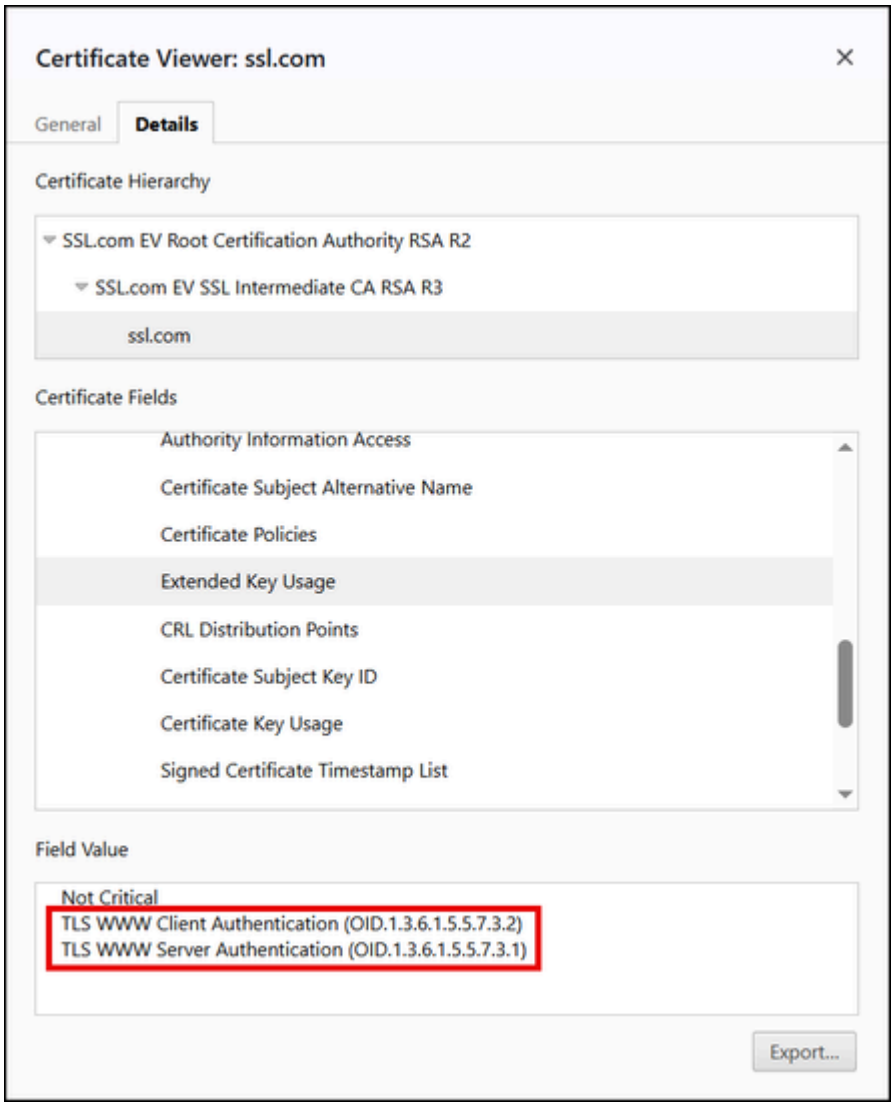
•OID:1.3.6.1.5.5.7.3.4

·用于S/MIME邮件安全中。

5.其他目的

·文档签名、时间戳、智能卡登录等，每个都有自己的OID。

浏览器和服务器只需要serverAuth　　EKU来建立HTTPS的安全连接，但过去，许多TLS服务器证书同时包含serverAuth和clientAuth EKU，下面是此类证书的示例：



为什么从服务器证书中删除客户端身份验证EKU?

- 安全和范围：公共TLS证书只用于对网络上的服务器进行身份验证。删除操作可明确区分服务器和客户端功能。ClientAuth EKU用于使用相互TLS(mTLS)和其他身份验证方案的计算机和用户的身份验证。
- 防止配置错误：如果EKU存在，某些系统可能信任来自公共CA的任何证书进行客户端身份验证，这可能带来安全风险。
- 浏览器要求：主要浏览器不要求或检查网站证书中的clientAuth EKU。
- 简化的PKI架构：通过将用法分开，CA可以维护服务器TLS与其他用途不同的证书层次结构。

这对于思科安全防火墙自适应安全设备(ASA)、思科安全防火墙威胁防御(FTD)、思科安全防火墙设备管理器(FDM)和思科安全防火墙管理中心(FMC)等产品尤为重要，这些产品在TLS身份验证期间可以充当服务器或客户端，具体取决于使用案例。

对服务器环境的影响

对于绝大多数服务器部署，此更改将是低影响或无影响的。以下是预期结果：

- 标准Web服务器(HTTPS):无影响。更新后的证书将继续正常运行。
- 现有证书：在截止时间之前签发的任何证书将继续运行，直到其过期。
- 双向TLS(mTLS)和客户端证书方案：如果您使用TLS服务器证书进行客户端身份验证，则需要从其他源获取带clientAuth EKU的单独证书。
- 同时需要两个EKU的企业系统：一些传统系统或企业系统需要两个EKU。您应验证是否需要更新以遵守新规则。

问题说明

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。

因此，如果由公共CA颁发的证书根据更新的CA策略进行续订，然后部署到Cisco安全防火墙产品中，需要客户端身份验证EKU的服务将失败。受到影响的特定服务如下：

- 当ASA、FTD、FDM或FMC充当客户端时(例如，当连接到身份提供程序或身份验证服务器(例如ISE(pxGrid)、RADIUS、LDAPS或Active Directory)时)，如果客户端证书由公共CA生成且缺少客户端身份验证EKU，基于证书的身份验证可能会失败。在这些情况下，如果身份验证服务器拒绝证书而不使用所需的EKU，则可能会发生连接故障。
- 思科安全客户端（以前称为AnyConnect）可以使用证书对ASA或FTD服务器进行身份验证。但是，如果客户端证书由公共CA生成并且缺少客户端身份验证EKU，则远程接入VPN(RAVPN)连接将失败。
- 当FTD或ASA使用证书身份验证（RSA或ECDSA）建立站点到站点VPN隧道（无论是连接到其他FTD、ASA、思科路由器还是第三方VPN对等体）时，如果公共CA生成的身份证书缺少“客户端身份验证EKU”属性，则隧道将失败。发生这种情况是因为远程VPN对等体要求身份证书中存在Client Authentication EKU。

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

发标准一致的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)
- 证书必须仅包括Server Authentication 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9月,SSL.com将颁发仅包含服务器证书的ServerAuth EKU(而不是ClientAuth)的TLS证书。换句话说，您的网站或服务器的新SSL/TLS证书将明确仅用于“服务器身份验证”。
- 2025年10月：与该计划一致的CA（例如：DigiCert、Sectigo等）开始默认颁发仅服务器证书。
- 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

对思科安全防火墙产品的影响

公共CA开始在颁发的证书中仅包含服务器身份验证EKU后。这可能会对下一个思科安全防火墙产品方案产生以下影响：

- 当ASA、FTD、FDM或FMC充当客户端时(例如，当连接到身份提供程序或身份验证服务器(例如ISE(pxGrid)、RADIUS、LDAPS或Active Directory)时)，如果客户端证书由公共CA生成且缺少客户端身份验证EKU，基于证书的身份验证可能会失败。在这些情况下，如果身份验证服务器拒绝证书而不使用所需的EKU，则可能会发生连接故障。
- 思科安全客户端（以前称为AnyConnect）可以使用证书对ASA或FTD服务器进行身份验证。但是，如果客户端证书

由公共CA生成并且缺少客户端身份验证EKU，则远程接入VPN(RAVPN)连接将失败。

- 当FTD或ASA使用证书身份验证（RSA或ECDSA）建立站点到站点VPN隧道（无论是连接到其他FTD、ASA、思科路由器还是第三方VPN对等体）时，如果公共CA生成的身份证书缺少“客户端身份验证EKU”属性，则隧道将失败。发生这种情况是因为远程VPN对等体要求身份证书中存在Client Authentication EKU。

注意：如果您通过pxGrid将FMC或FDM与ISE集成，并且FMC/FDM上安装的证书缺少“客户端身份验证EKU”属性，则查看本文档中提议的解决方法以及下一个ISE参考：FN74392和准备身份服务引擎，以便在公共证书颁发机构颁发的证书中扩展密钥使用限制。

注意：从TLS服务器证书中删除clientAuth EKU是一项行业范围的策略更改，将增强安全性并防止误用。对于大多数用户而言，不会产生明显的影响。但是，如果您依靠ClientAuth EKU，您应该采取主动措施，根据自己的需要获取正确的证书类型。

受影响的产品

思科安全防火墙产品	软件版本	受影响的情景	补救
FTD	全部版本	当作为客户端时(例如，当连接到身份提供程序或身份验证服务器(例如ISE(pxGrid)、RADIUS、LDAPS或Active Directory)时)，如果客户端证书由公共CA生成并且缺少客户端身份验证EKU，基于证书的身份验证可能会失败。在这种情况下，如果身份验证服务器拒绝证书而不使用所需的EKU，则可能会发生连接故障。	选项1.如果使用TLS服务器证书进行客户端身份验证，则需要从其他源获取具有ClientAuth EKU的证书。 或者 Option2.切换到提供组合EKU（ClientAuth和ServerAuth）证书的公共根CA（证书颁发机构）。 NOTE:有关其他选项，请参阅本文档的解决方法部分。
FDM	全部版本		
FMC	全部版本		
ASA	全部版本		

思科安全客户端（以前称为AnyConnect）	全部版本	思科安全客户端可以使用证书向ASA或FTD服务器进行身份验证。但是，如果客户端证书由公共CA生成并且缺少客户端身份验证EKU，则远程接入VPN(RAVPN)连接将失败。	
FTD或ASA	全部版本	当FTD或ASA使用证书身份验证（RSA或ECDSA）建立站点到站点VPN隧道（无论是连接到另一个FTD、ASA、思科路由器还是第三方VPN对等体）时，如果公共CA生成的身份证书缺少“客户端身份验证EKU”属性，则VPN隧道将失败。发生这种情况是因为远程VPN对等体要求身份证书中存在Client Authentication EKU。	

注意：如果您通过pxGrid将FMC或FDM与ISE集成，并且FMC/FDM上安装的证书缺少“客户端身份验证EKU”属性，则查看本文档中提议的解决方法以及下一个ISE参考：FN74392和准备身份服务引擎，以便在公共证书颁发机构颁发的证书中扩展密钥使用限制。

注意：从TLS服务器证书中删除clientAuth EKU是一项行业范围的策略更改，将增强安全性并防止误用。对于大多数用户而言，不会产生明显的影响。但是，如果您依靠ClientAuth EKU，您应该采取主动措施，根据自己的需要获取

正确的证书类型。

警告：对于生产环境，强烈建议客户使用具有相应EKU属性的证书。此做法可确保安全性、兼容性，以及符合行业标准和最佳实践。不具有EKU属性的证书应仅视为临时解决方法，并且仅在明确了解相关风险的情况下才使用。

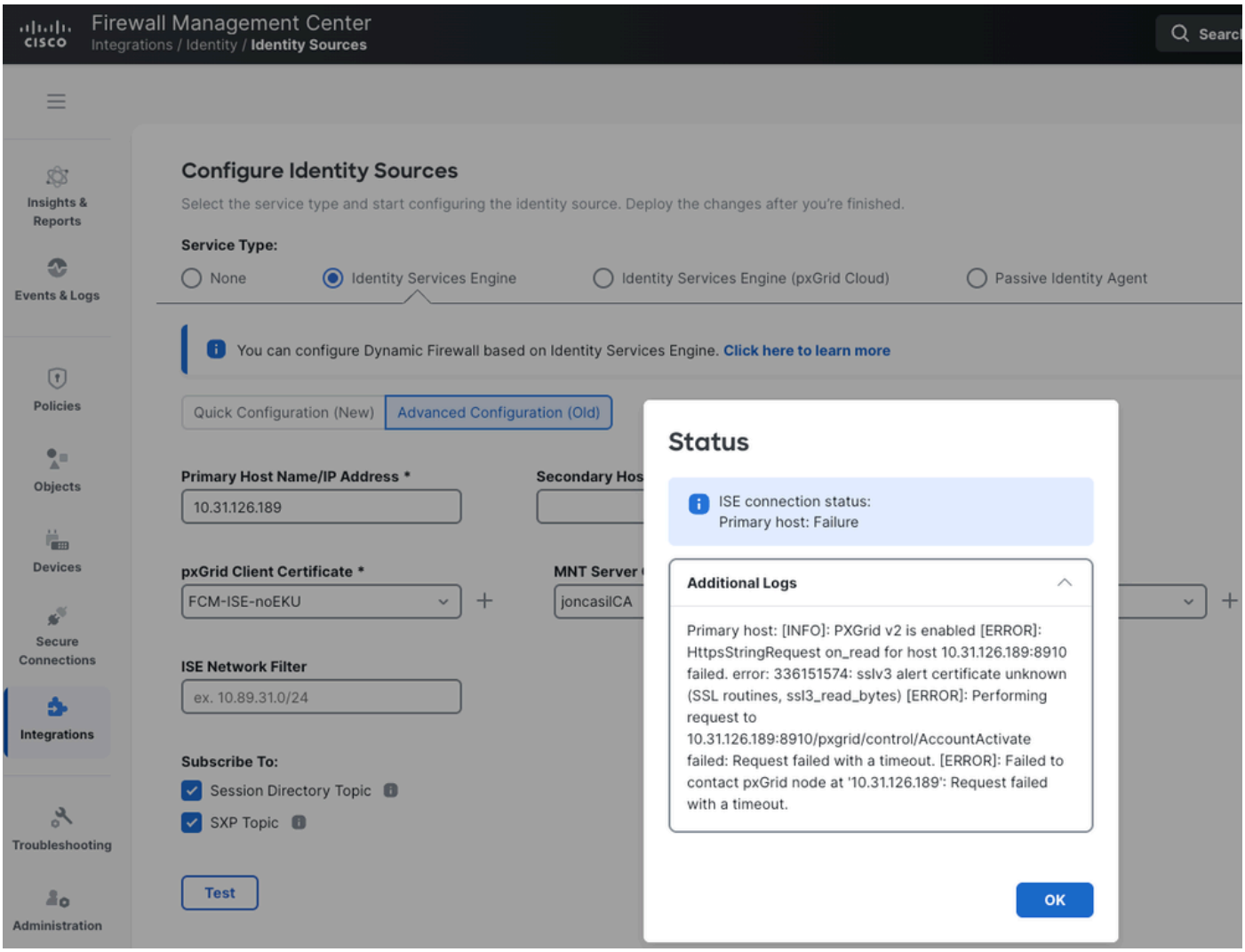
问题1. pxGrid在FMC和ISE之间的集成问题，当FMC证书缺少客户端身份验证EKU属性时

在此场景中，FMC用于pxGrid与ISE集成的证书缺少Client Authentication EKU属性。因此，pxGrid集成失败，因为ISE服务器希望此属性出现在FMC提供的证书中。

拓扑



FMC UI错误：这是FMC中显示的错误消息，当FMC使用的证书缺少pxGrid与ISE集成的客户端身份验证EKU属性时。



FMC CLI错误：在FMC /var/log/messages目录中发现了相同的错误消息。

```
<#root>
HttpsStringRequest on_read for host 10.31.126.189:8910 failed. error: 336151574:

sslv3 alert certificate unknown


(SSL routines, ssl3_read_bytes)

Mar 27 23:17:17 vFMC3-chherna2 SF-IMS[8074]: [7514] ADI:HttpsEndpoint

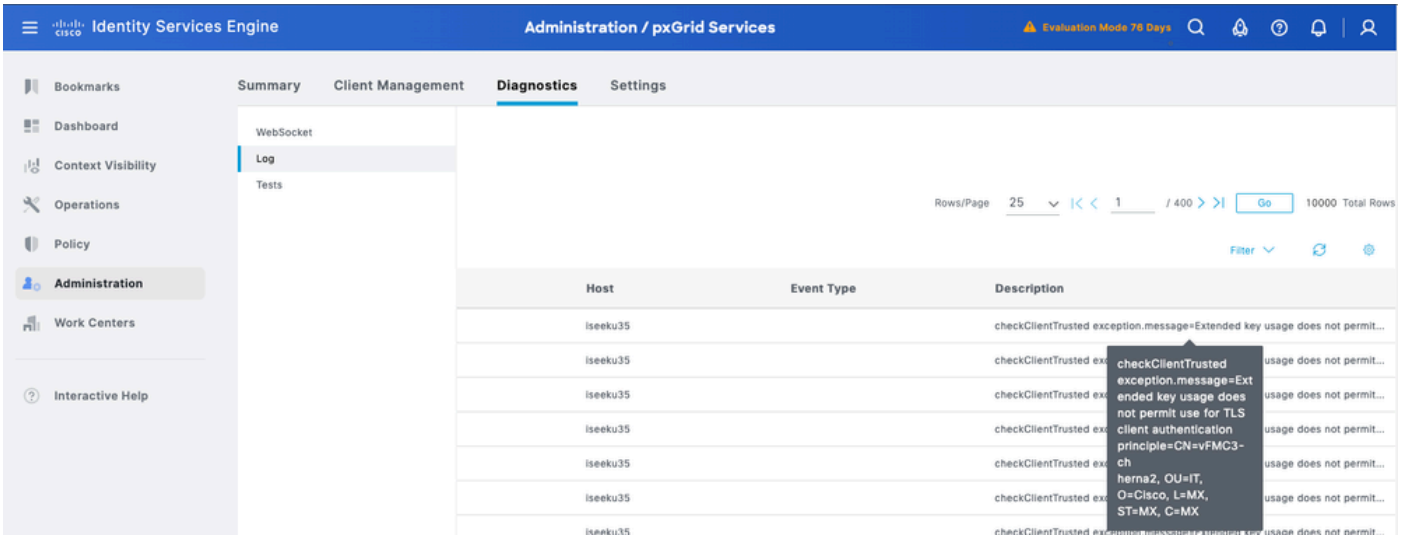
[ERROR] Performing request to 10.31.126.189:8910/pxgrid/control/AccountActivate failed: Request failed w

Mar 27 23:17:17 vFMC3-chherna2 SF-IMS[8074]: [7514] ADI:ise_connector.PXGrid2ThreadedService
```

```
[ERROR] pxgrid2_service was not created for 10.31.126.189. Reason - Request failed with a timeout.
```

```
Mar 27 23:17:47 vFMC3-chherna2 SF-IMS[8074]: [7514] ADI:ise_connector.PXGrid2ThreadedService [I
Mar 27 23:17:47 vFMC3-chherna2 SF-IMS[8074]: [7514] ADI:ise_connector.PXGrid2ThreadedService [I
```

ISE错误：这是ISE中显示的错误消息“checkClientTrusted exception.message=Extended key usage does not permit use for TLS client authentication principle=CN=vFMC3-chherna2, OU=IT， O=Cisco， L=MX， ST=MX， C=MX”。



解决方案：如果您通过pxGrid将FMC或FDM与ISE集成，并且FMC/FDM中安装的证书缺少Client Authentication EKU属性，则查看本文档中建议的和下一个ISE参考：FN74392和Prepare Identity Services Engine for Extended Key Usage Restrictions in Certificates Issued for a successful pxGrid集成。

注意：FMC pxGrid客户端证书必须包含ClientAuth EKU属性或根本不包含客户端或服务器EKU属性。

注意：即使IMS支持使用公共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。

问题2. LDAPS服务器的FTD或ASA集成问题，当提供的证书缺少Client Authentication EKU属性

在此场景中，FTD或ASA充当客户端，使用证书身份验证与LDAPS服务器集成。如果FTD或ASA使用的证书缺少Client Authentication EKU属性，则集成失败，因为LDAPS服务器要求证书中存在此属性。

拓扑



LDAP服务器错误：'TLS证书验证：错误，不支持的证书用途和“TLS跟踪：SSL3警报写入：致命：不支持的证书'

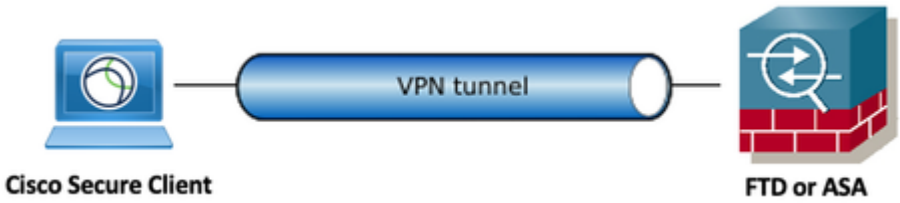
```
69ceb4f5.157b4993 0x7ff553fff700 TLS trace: SSL_accept:TLSv1.3 write server cer
tificate verify
69ceb4f5.157c01a4 0x7ff553fff700 TLS trace: SSL_accept:SSLv3/TLS write finished
69ceb4f5.157c458a 0x7ff553fff700 TLS trace: SSL_accept:TLSv1.3 early data
69ceb4f5.157c6685 0x7ff553fff700 TLS trace: SSL_accept:error in TLSv1.3 early d
ata
69ceb4f5.15b17eaa 0x7ff5522fc700 connection_get(15): got connid=1004
69ceb4f5.15b1b73f 0x7ff5522fc700 connection_read(15): checking for input on id=
1004
69ceb4f5.15b2bf05 0x7ff5522fc700 TLS trace: SSL_accept:TLSv1.3 early data
69ceb4f5.15b4c6c3 0x7ff5522fc700 TLS certificate verification: depth: 0, err: 2
6, subject: /CN=asa-server-only,69ceb4f5.15b4e8de 0x7ff5522fc700  issuer: /CN=T
est-CA
69ceb4f5.15b4f367 0x7ff5522fc700 TLS certificate verification: Error, unsupport
ed certificate purpose
69ceb4f5.15b57df8 0x7ff5522fc700 TLS trace: SSL3 alert write:fatal:unsupported
certificate
69ceb4f5.15b5b557 0x7ff5522fc700 TLS trace: SSL_accept:error in error
69ceb4f5.15b66c36 0x7ff5522fc700 TLS: can't accept: error:1417C086:SSL routines
:tls_process_client_certificate:certificate verify failed (unsupported certific
ate purpose).
69ceb4f5.15b70391 0x7ff5522fc700 connection_read(15): TLS accept failure error=
-1 id=1004, closing
69ceb4f5.15b747ae 0x7ff5522fc700 connection_close: conn=1004 sd=15
```

解决方案：查看本文档中建议的内容，确保FTD或ASA使用正确的身份证书（包括客户端身份验证EKU属性）成功通过LDAPS服务器进行基于证书的身份验证。

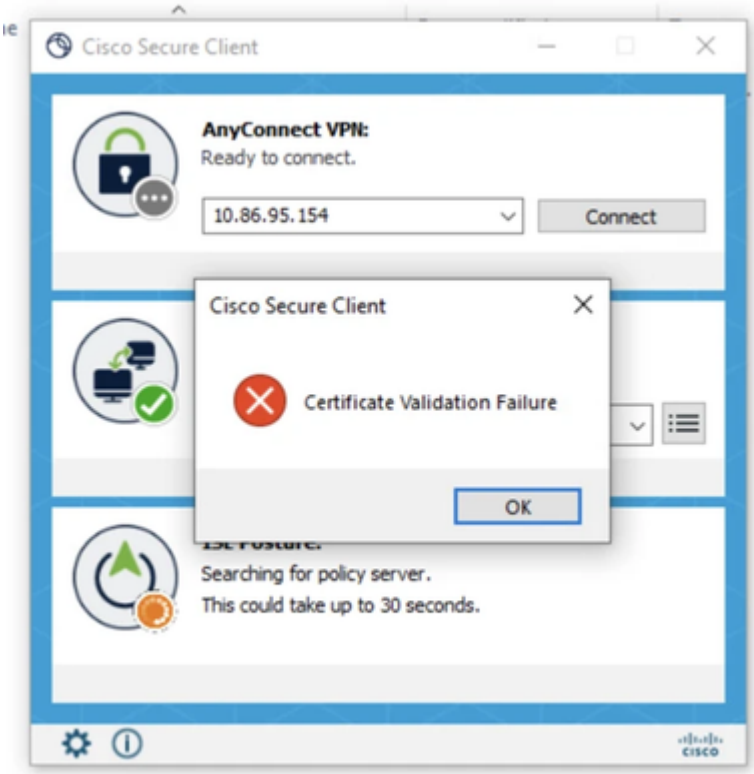
问题3.如果客户端证书缺少客户端身份验证EKU属性，Cisco安全客户端（以前称为AnyConnect）可能会遇到到FTD或ASA的连接问题

在此场景中，思科安全客户端使用证书身份验证建立到FTD或ASA的RAVPN隧道。但是，如果客户端证书缺少Client Authentication EKU属性，则RAVPN会话将失败，因为ASA或FTD要求在客户端证书中显示此属性。

拓扑



Cisco安全客户端错误：“证书验证失败”



Cisco安全客户端DART错误：DART捆绑包中AnyConnectVPN.txt文件的以下日志确认Cisco安全客户端因缺少客户端身份验证EKU属性而拒绝了FTD/ASA的RAVPN基于证书身份验证使用的证书(要在DART捆绑包中找到AnyConnectVPN.txt文件，请导航到Cisco安全客户端> AnyConnect VPN >日志> AnyConnectVPN.txt.)。

<#root>

```
****************************************

Date : 04/07/2026
Time : 03:35:22
Type : Error
Source : csc_vpnapi


Description : Function: CVerifyExtKeyUsage::compareEKUs
```

```
File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\CommonCrypt\Certificates\VerifyEx
Line: 330

EKU not found in certificate: 1.3.6.1.5.5.7.3.2



****************************************

Date : 04/07/2026
Time : 03:35:22
Type : Information
Source : csc_vpnapi



Description : Function: CCertStore::GetCertificates


File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\CommonCrypt\Certificates\CertStor
Line: 225

Ignoring client certificate because it does not contain the required EKU extension.

 Certificate details:
Store: [Omitted Output]

****************************************
```

解决方案：查看本文档中建议的，确保Cisco安全客户端使用正确的证书（包括Client Authentication EKU属性）成功通过FTD或ASA进行基于证书的身份验证。

注意：从上述DART捆绑错误“EKU not found in certificate:1.3.6.1.5.5.7.3.2”，此数字“1.3.6.1.5.5.7.3.2”对应于客户端身份验证EKU OID。

问题4.如果身份证书缺少“客户端身份验证EKU”属性，则使用基于证书的身份验证的站点到站点VPN隧道失败

在此方案中，涉及IKEv2站点到站点VPN隧道的基于证书的身份验证，FTD/ASA(1)用来建立到FTD/ASA(2)对等体的隧道的身份证书缺少Client Authentication EKU属性。因此，无法建立VPN隧道，因为远程对等体FTD/ASA(2)要求在证书中存在此属性。

拓扑



FTD或ASA CLI错误：以下是FTD/ASA(2)在基于IKEv2证书的身份验证期间观察到的错误，即拒绝缺少客户端身份验证EKU属性的FTD/ASA(1)身份证书。

<#root>

```
Apr 09 2026 15:59:50:

%ASA-3-717027: Certificate chain failed validation. Certi. Peer certificate key usage is invalid,

 subject name: CN=ASAv3.cisco.com,OU=IT,O=Cisco,C=US,unstructuredName=ASAv3.cisco.com.
Apr 09 2026 15:59:50:

%ASA-3-717027: Certificate chain failed validation. Certificate chain is either invalid or not authorize

Apr 09 2026 15:59:50: %ASA-3-751006: Local:10.3.3.6:500 Remote:10.3.3.5:500 Username:10.3.3.5

IKEv2 Certificate authentication failed. Error: Certificate authentication failed

Apr 09 2026 15:59:50: %ASA-4-750003: Local:10.3.3.6:500 Remote:10.3.3.5:500 Username:10.3.3.5

IKEv2 Negotiation aborted due to ERROR: Auth exchange failed

Apr 09 2026 15:59:50: %ASA-4-752012: IKEv2 was unsuccessful at setting up a tunnel.  Map Tag = CMAP.  M
Apr 09 2026 15:59:50: %ASA-3-752015: Tunnel Manager has failed to establish an L2L SA.  All configured
Apr 09 2026 15:59:55: %ASA-5-752003: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2.  Map Ta
Apr 09 2026 15:59:55: %ASA-5-750001: Local:10.3.3.6:500 Remote:10.3.3.5:500 Username:Unknown IKEv2 Rece
```

注意：在上面的示例中，FTD/ASA(2)使用包含ClientAuth和ServerAuth EKU属性的身份证书。

注意：在上述示例中，FTD/ASA(2)也可由路由器或第三方物理或基于云的VPN集中器替代。然后，同样的问题将持续存在，因为VPN对等体要求在FTD/ASA(1)使用的证书中存在Client Authentication EKU属性，以便成功进行基于证书的身份验证。

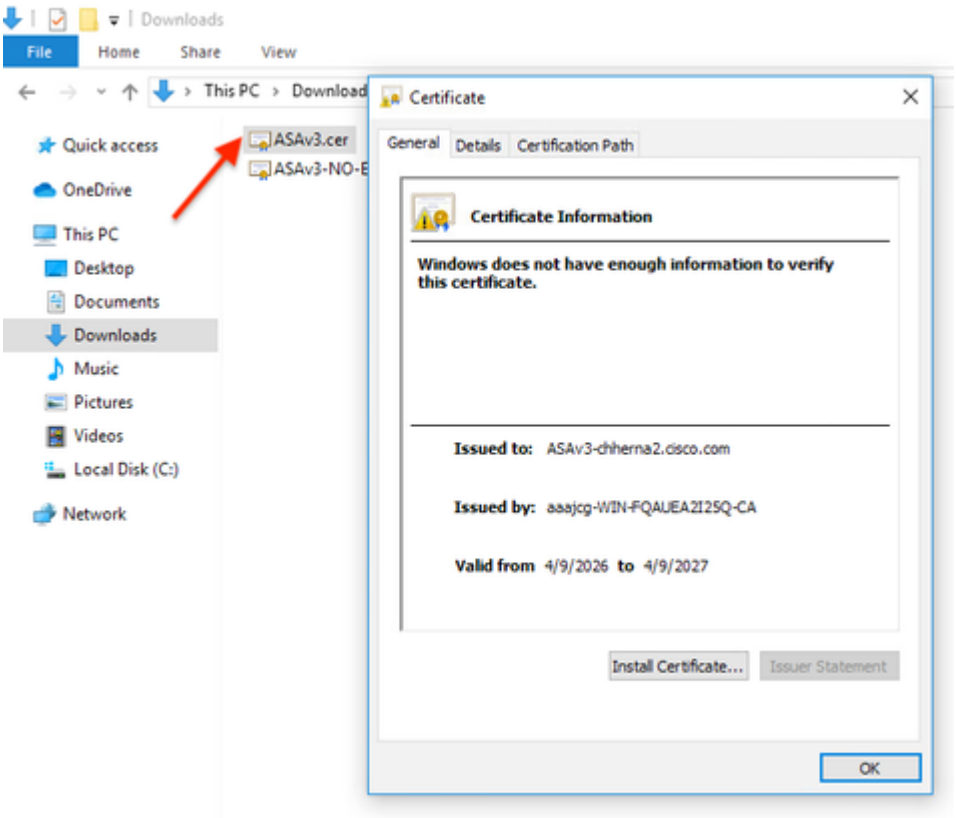
解决方案：查看本文档中建议的，确保FTD/ASA(1)使用正确的身份证书（包括客户端身份验证EKU属性）成功实现基于证书身份验证的站点到站点VPN隧道。

用于确认证书是否缺少客户端身份验证EKU属性的说明

使用Windows证书管理器验证.cer证书中的EKU属性

按照以下步骤使用Windows证书管理器验证.cer证书中的EKU属性：

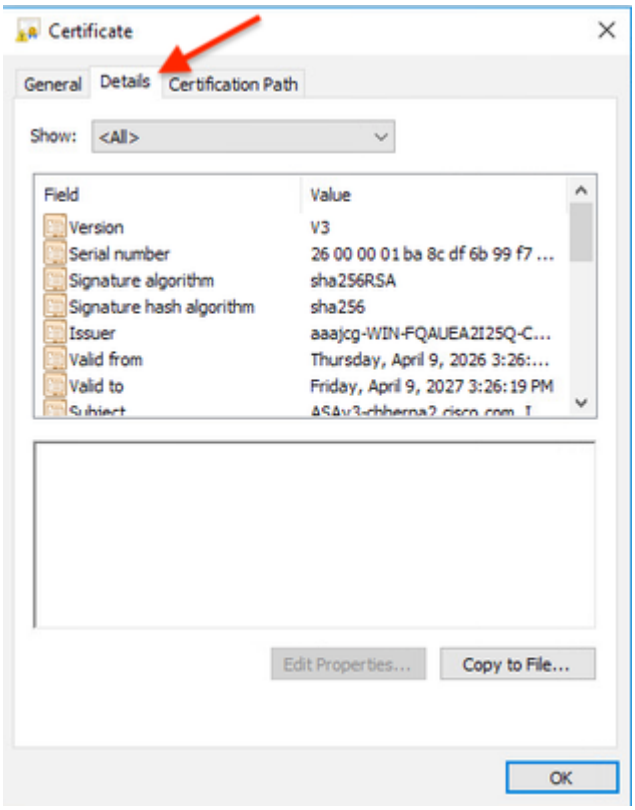
步骤1.双击.cer文件，在Windows证书管理器中将其打开。



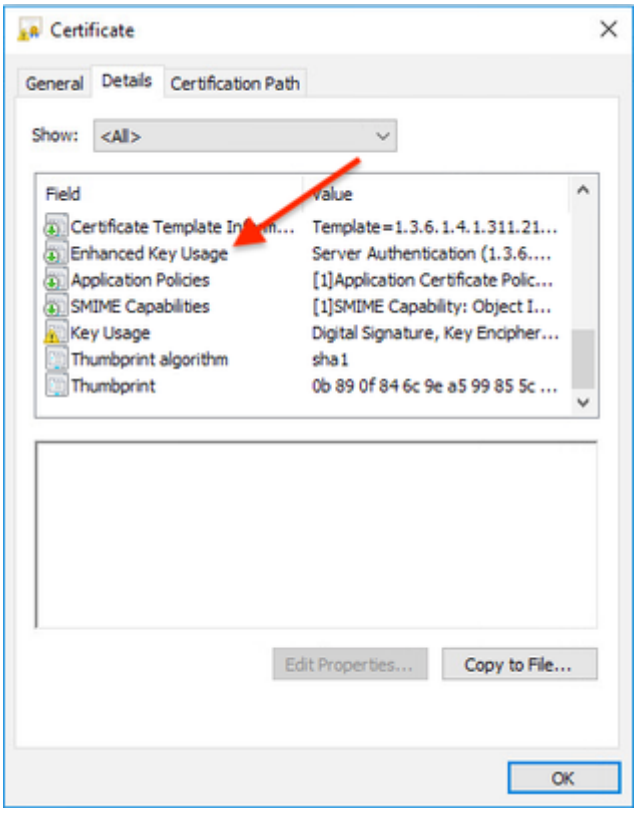
注意：只有.cer文件会以这种方式直接打开；如果您的证书具有.pem扩展名，请先将其重命名为.cer或.crt。

步骤2.处理安全警告（如果有），如果出现安全警告提示，请点击打开以继续。

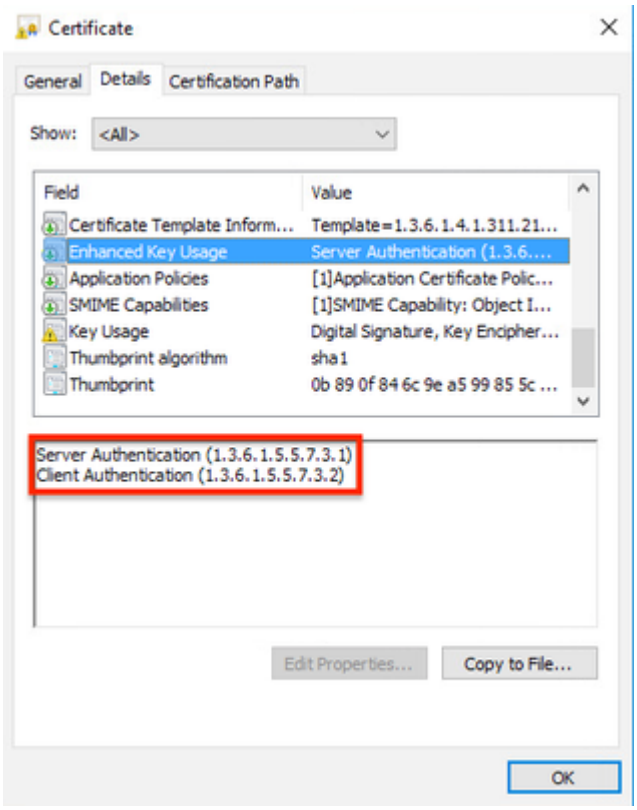
步骤3.在证书窗口中，点击Details选项卡。



步骤4.滚动浏览字段列表并选择“Enhanced Key Usage”（或Extended Key Usage）。

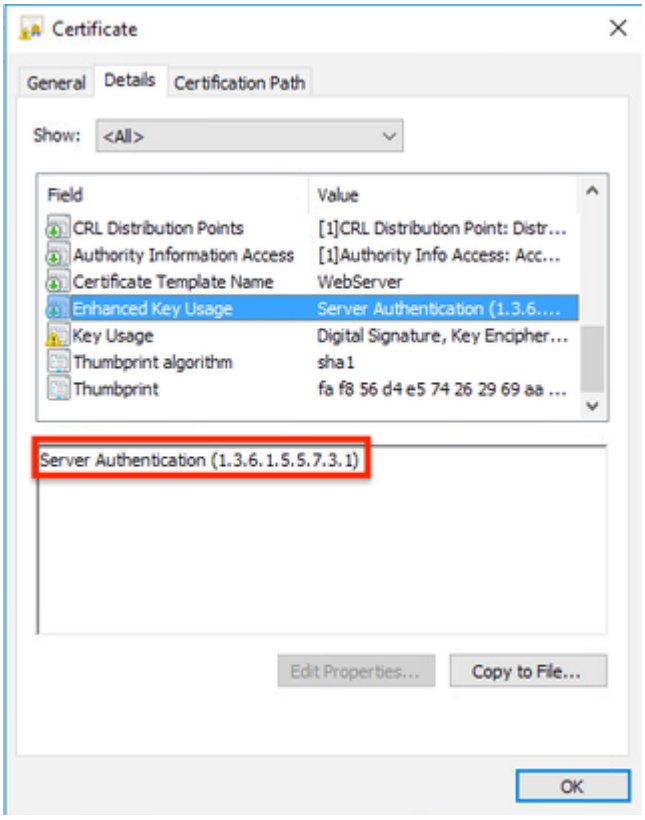


第5步：验证EKU属性，您可能会看到诸如“服务器身份验证”和“客户端身份验证”等条目，这些条目指示证书中存在的EKU值。

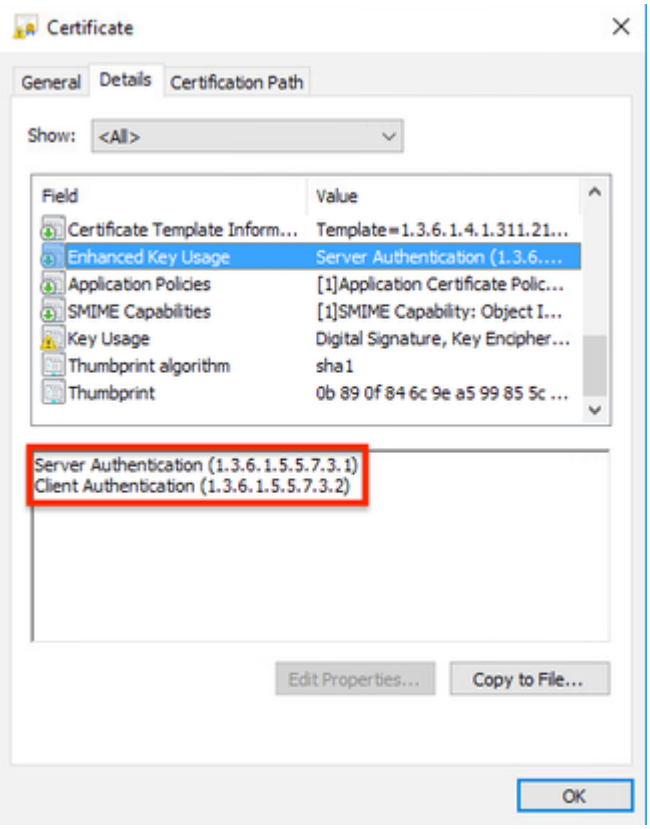


步骤6.验证后，点击OK关闭证书窗口。

示例 1：此.cer证书缺少客户端身份验证EKU属性，并且仅包括服务器身份验证EKU属性。



示例 2：此.cer证书包括服务器和客户端身份验证EKU属性。



使用OpenSSL验证来自PKCS#12、PEM和.cer证书的EKU属性

按照以下步骤验证来自.p12(PKCS#12)、.pem(PEM)和.cer证书的EKU属性：

步骤1.找到需要检查的证书，然后以.p12(PKCS#12)、.pem(PEM)或.cer格式将其导出。

对于.p12(PKCS#12)证书，请使用openssl从.p12(PKCS#12)文件中提取证书，.p12(PKCS#12)文件可能包含私钥、证书和CA证书。

使用以下命令将证书从.p12(PKCS#12)文件提取到.pem(PEM)文件（没有私钥或CA链）：

```
openssl pkcs12 -in yourfile.p12 -nokeys -clcerts -out cert.pem
```

- yourfile.p12:替换为实际的文件名。
- 您可能需要输入.p12文件的密码。
- cert.pem:是以.pem(PEM)格式提取的证书（不含私钥或CA链）。

步骤2.使用下一个openssl命令显示证书详细信息和EKU属性。

a)对于.pem文件，使用next openssl命令显示证书详细信息和EKU属性：

```
openssl x509 -in cert.pem -text -noout
```

- cert.pem:替换为实际的文件名。

b)对于.cer文件，使用next openssl命令显示证书详细信息和EKU属性：

```
openssl x509 -in yourfile.cer -text -noout
```

- yourfile.cer:替换为实际的文件名。

步骤3.然后，在输出中查找X509v3Extended Key Usage部分，您可能会看到类似于“TLS Web Server Authentication”和“TLS Web Client Authentication”的条目，这些条目指示证书中存在的EKU值。

```
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
```

或EKU属性OID（对象标识符）：

```
X509v3 Extended Key Usage:
1.3.6.1.5.5.7.3.1, 1.3.6.1.5.5.7.3.2
```

- 服务器身份验证EKU OID:1.3.6.1.5.5.7.3.1
- 客户端身份验证EKU OID:1.3.6.1.5.5.7.3.2

示例 1：此.pem(PEM)证书缺少Client Authentication EKU属性，并且仅包括Server Authentication EKU属性。

<#root>

```
MyHost$ openssl x509 -in cert.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            26:00:00:01:b7:e7:90:48:d6:f9:41:d3:54:00:01:00:00:01:b7
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=com, DC=aaajcg, CN=aaajcg-WIN-FQAUEA2I25Q-CA
        Validity
            Not Before: Mar 27 00:31:40 2026 GMT
            Not After : Mar 26 00:31:40 2028 GMT
        Subject: C=MX, ST=MX, L=MX, O=Cisco, OU=IT, CN=vFMC3-chherna2
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:cf:a8:a0:ff:dd:34:73:7d:46:86:85:05:b6:0c:
                    5e:32:8c:6f:6f:88:52:03:58:63:c6:89:d8:fc:55:
                    c5:58:ba:eb:45:88:b2:21:9e:c5:d8:67:57:39:0f:
                    91:a5:41:61:fa:94:b1:ad:9e:71:26:87:b6:30:ae:
                    a7:f6:89:b1:6d:61:ce:fa:47:7f:2a:d8:e8:4d:26:
                    4f:a7:d3:eb:5a:69:16:46:71:c7:55:cf:87:b4:10:
                    96:f2:10:6b:c0:a7:3d:3c:49:9d:ee:77:8c:b5:95:
                    9b:69:81:e0:2d:a0:6e:5c:78:73:22:5a:38:d0:74:
                    38:b2:ba:e0:ab:c5:44:eb:e1:3c:52:86:b8:2a:4e:
                    37:44:9c:34:d8:d8:6c:ae:3e:df:12:57:0e:28:52:
                    57:dc:6d:62:ea:b6:ec:19:4e:90:8f:3f:2c:23:1b:
                    e2:39:f0:ba:07:08:9a:0b:97:96:05:2e:69:fe:9a:
                    b2:b2:74:9a:ba:06:25:bc:38:1c:94:87:8e:2a:dc:
                    2f:0b:a6:31:6c:bf:11:96:2a:71:b3:87:e5:f5:cb:
                    88:f1:73:cf:88:d7:30:78:24:77:7c:b7:2c:7c:83:
                    6d:69:5b:bd:d4:21:b9:ee:19:c4:02:be:7b:44:a2:
                    55:d6:b2:95:11:46:bf:db:3e:4f:9a:8c:d4:ad:8d:
                    82:f5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                0D:8E:DA:07:6D:49:EA:51:D2:C7:EF:50:CE:CE:2B:8E:7C:DF:A6:8D
            X509v3 Authority Key Identifier:
                keyid:3A:45:60:22:F7:C8:2C:0D:D2:98:5A:BC:E0:98:D4:91:1D:67:32:22

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:ldap:///CN=aaajcg-WIN-FQAUEA2I25Q-CA,CN=WIN-FQAUEA2I25Q,CN=CDP,CN=Public%20Key%20

            Authority Information Access:
                CA Issuers - URI:ldap:///CN=aaajcg-WIN-FQAUEA2I25Q-CA,CN=AIA,CN=Public%20Key%20Services

            1.3.6.1.4.1.311.20.2:
                ...W.e.b.S.e.r.v.e.r
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment


X509v3 Extended Key Usage:

        <-------- "EKU SECTION"
```

TLS Web Server Authentication

```
  <-------- "Server Authentication EKU Attribute Included"
    Signature Algorithm: sha256WithRSAEncryption
         2f:27:cd:95:7d:5c:40:fa:29:64:df:75:7d:7a:87:9b:b0:94:
         0e:6b:07:4d:d2:7e:83:da:03:08:f3:50:0d:5b:05:8c:1f:54:
         46:fe:53:f3:e2:d4:0a:ba:37:4f:cd:a4:49:04:74:79:09:23:
         d6:06:af:69:d2:7b:f5:bc:ec:fe:ce:e4:c9:07:31:d7:85:45:
         55:78:d3:42:45:f9:ce:cd:bf:43:53:b4:8e:4c:af:64:4b:a6:
         dc:47:d0:16:4e:73:62:fd:c8:5e:37:74:cb:68:48:29:7d:f9:
         41:b3:d1:46:56:24:83:23:5c:bd:b0:e3:7c:f9:8a:af:da:09:
         d0:c2:7d:4a:e6:24:0f:e6:fc:6e:0d:65:8c:96:8c:af:21:b2:
         7f:4b:bb:1c:17:33:b1:db:00:f3:12:e3:53:39:d0:e7:6a:48:
         4c:c6:4f:29:6f:74:ff:2d:a7:e5:ea:e8:89:fe:a4:2b:cd:e3:
         61:6a:9e:11:52:15:57:f2:b8:e8:fa:78:31:20:49:d9:50:f9:
         70:3f:1e:aa:9c:1a:bb:0b:59:66:1e:85:bd:76:e7:73:6f:ec:
         86:30:b0:dd:86:3c:b3:a0:7b:fb:b7:74:5d:38:88:82:3d:a3:
         2d:8c:a5:e4:db:37:eb:be:7f:62:bc:87:7c:35:17:32:fc:52:
         c5:d3:c5:8f
```

示例 2：此.pem(PEM)证书包括客户端和服务器身份验证EKU属性。

<#root>

```
MyHost$ openssl x509 -in cert.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            26:00:00:01:b6:74:fc:b4:1e:99:be:7a:10:00:01:00:00:01:b6
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=com, DC=aaajcg, CN=aaajcg-WIN-FQAUEA2I25Q-CA
        Validity
            Not Before: Mar 26 23:44:58 2026 GMT
            Not After : Mar 26 23:44:58 2027 GMT
        Subject: C=MX, ST=AD, L=AD, O=Cisco, OU=IT, CN=vFMC3-chherna2
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:ab:aa:67:4e:55:19:3b:38:6c:33:2e:ba:fd:19:
                    56:e7:68:f8:f7:e9:53:95:1f:53:b4:f1:ce:94:c8:
                    ca:41:f1:52:15:eb:a5:35:9f:07:95:9f:c3:8a:5e:
                    62:d6:e1:5c:04:c5:c0:27:1c:84:ed:3d:1b:42:50:
                    91:4a:a6:86:90:e0:6e:26:7e:37:fd:17:0c:2f:bb:
                    fe:58:81:ec:3b:9d:0b:fc:dd:8c:6b:dd:ab:d3:96:
                    74:23:0d:78:d7:09:53:61:f9:b0:29:c6:7c:e2:9c:
                    2f:74:30:42:0f:45:47:cd:16:59:ed:53:62:8f:60:
                    75:f8:24:f5:1f:77:fb:89:85:4b:49:ad:93:43:04:
                    6e:4a:b3:59:fc:eb:75:70:39:67:71:60:be:b3:b7:
                    86:f7:c5:53:28:1e:bf:8f:b2:52:ec:79:d6:12:b0:
                    33:9c:6d:46:7a:9c:5d:53:a5:44:24:da:4b:36:7d:
                    c2:ec:61:d7:a0:01:c3:d2:bc:0a:df:a8:f6:0c:82:
                    48:30:fb:c6:3e:4a:48:a9:01:13:f5:4e:f2:03:24:
                    38:ee:aa:d9:60:78:30:45:ed:3b:76:16:fd:7a:d3:
```

```
                    b0:16:10:28:75:fc:41:32:e6:6d:cb:c3:96:58:77:
                    9e:11:0a:9b:33:c7:92:8d:75:1f:e5:30:29:a4:a5:
                    ba:7d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                D2:DF:62:25:17:DB:72:31:D8:D2:D0:41:CB:FB:DD:00:FF:38:BD:BB
            X509v3 Authority Key Identifier:
                keyid:3A:45:60:22:F7:C8:2C:0D:D2:98:5A:BC:E0:98:D4:91:1D:67:32:22

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:ldap:///CN=aaajcg-WIN-FQAUEA2I25Q-CA,CN=WIN-FQAUEA2I25Q,CN=CDP,CN=Public%20Key%20

            Authority Information Access:
                CA Issuers - URI:ldap:///CN=aaajcg-WIN-FQAUEA2I25Q-CA,CN=AIA,CN=Public%20Key%20Services

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            1.3.6.1.4.1.311.21.7:
                0-.%+.....7.....^..9...
...b.../ ...R...Z..d...


X509v3 Extended Key Usage:

          <-------- "EKU SECTION"


TLS Web Server Authentication, TLS Web Client Authentication


  <----- "Server & Client EKU Attributes Included"
            1.3.6.1.4.1.311.21.10:
                0.0
..+.......0
..+.......
            S/MIME Capabilities:
......0...+....0050...*.H..
..*.H..
    Signature Algorithm: sha256WithRSAEncryption
         3f:66:b1:35:7e:05:b4:69:f1:81:95:b8:18:90:f2:20:bd:8d:
         ff:03:5a:59:ca:02:ba:2d:1d:e0:8d:3f:63:e9:fe:71:3c:9a:
         11:15:5c:3b:fc:62:e4:cf:15:25:4c:74:5e:ad:3f:09:e9:3b:
         d5:08:95:7d:97:7a:ef:c1:16:6d:e0:7a:0b:21:81:46:bc:15:
         c3:76:8c:fe:fb:14:94:36:92:0d:3b:4a:c9:8f:6a:bd:dc:4b:
         0b:24:c3:32:35:27:e7:aa:23:95:85:e4:a9:64:71:f0:98:9e:
         33:aa:6e:bd:7c:dd:dc:4b:cf:dd:0e:a7:ea:e8:aa:61:8f:67:
         84:da:5b:be:8e:05:75:c8:eb:46:13:6f:14:4d:fe:4e:57:3c:
         29:27:cc:0b:5b:25:87:37:24:12:79:b1:c3:78:c8:94:fe:df:
         3c:77:aa:fc:f2:ee:ae:9b:ab:88:29:f9:ee:04:c2:48:5f:21:
         9e:1c:25:cc:c9:c5:9c:23:8f:af:87:76:5e:46:74:ac:73:57:
         01:ba:71:ae:46:e1:87:3c:94:6c:19:f7:fe:8e:66:9d:c7:1f:
         b0:87:4b:65:e2:fc:d6:10:7c:44:57:56:5d:68:bb:df:f0:36:
         0e:07:c5:8a:be:56:86:97:3d:a7:1c:8b:86:df:0b:51:b5:97:
         cc:67:09:8e
```

解决方法

管理员可以从以下解决方法选项中选择一种。

选项1.切换到提供组合EKU证书的公用根CA

某些公共根CA（如DigiCert和IdenTrust）会从备用根颁发包含组合EKU类型（服务器和客户端证书）的证书，这些类型可能不包含在Chrome根存储中。与CA提供商协调检查此类证书的可用性，并在部署证书之前，确保提供证书的服务器和使用该证书的客户端都信任相应的根CA。

此方法无需升级服务器软件来缓解由Chrome根程序策略实施的客户端身份验证EKU的取消设置。

下表显示了公共根CA和EKU类型的示例，该表不是详尽的列表，仅供说明之用。

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
IdenTrust	clientAuth	IdenTrust公共部门根CA 1	TrustID RSA ClientAuth CA 2
IdenTrust	serverAuth（浏览器受信任）	IdenTrust商业根CA 1	HydrantID服务器CA O1
DigiCert	clientAuth + serverAuth	DigiCert保证ID根G2	DigiCert保证ID CA G2
DigiCert	clientAuth	DigiCert保证ID根G2	DigiCert Assured ID Client CA G2
DigiCert	serverAuth（浏览器受信任）	DigiCert全局根G2	DigiCert Global G2 TLS RSA SHA256

选项2.更新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的证书将继续保留，直到其期限到期。但是，最好在策略取消设置之前续订合并EKU证书。

- 公共CA策略和实施日期可能因供应商而异。
- 请与CA联系并相应地规划证书续订。
- 2026年3月15日之后，CA颁发的公共证书有效期仅为200天。
- 考虑到某些公共CA已停止发布合并EKU证书。

选项3.迁移到私有PKI以颁发组合EKU（服务器和客户端）证书

评估过渡到专用公钥基础设施(PKI)的可行性，然后设置专用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。

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。

选项4.仅使用客户端身份验证EKU获取公共受信任证书

某些CA(如SSL.com)提供专用客户端身份验证证书。这些证书与TLS证书分开，通常用于企业身份验证。

⚠ 警告：对于生产环境，强烈建议客户使用具有相应EKU属性的证书。此做法可确保安全性、兼容性，以及符合行业标准和最佳实践。不具有EKU属性的证书应仅视为临时解决方法，并且仅在明确了解相关风险的情况下才使用。

常见问题解答 (FAQ)

问题1：如果使用私有PKI，是否需要担心此问题？

回答：由专用CA实施的策略由每个组织决定。如果您的专用CA采用相同的颁发条件（例如从证书中删除客户端身份验证EKU属性），则本文档中提供的准则适用。

问题2：我是否可继续使用现有证书？

A：是，在到期时间之前，可以使用包含组合EKU的有效证书。

问题3：如果安装在FMC/FDM上的证书没有“客户端身份验证EKU”属性，可以使用哪些选项通过pxGrid将我的FMC或FDM与ISE集成？

A：除了本文档中建议的解决方法，我们强烈建议您检查以下ISE参考：

- Field Notice：FN74392 — 思科身份服务引擎：从2026年5月开始的公共CA客户端身份验证EKU更改对安全通信的影响 — 提供的解决方法
- 准备身份服务引擎，以在公共证书颁发机构颁发的证书中扩展密钥使用限制

✎ 注意：即使IMS支持使用公共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。

问题4. “客户端身份验证” EKU是什么？为什么它出现在我的证书中？

A：“客户端身份验证” EKU表示客户端可以使用证书向服务器进行身份验证。历史上，有些CA默认将其包含在TLS证书中，但一般网站安全并不需要它。

问题5：我当前的TLS证书在其扩展密钥使用下显示“客户端身份验证”。现在是否无效？

答：否，它仍然有效。你不需要立即替换它续订时，新证书不会包括clientAuth EKU。

问题6.如何检查证书是否具有clientAuth EKU?

A：您可以使用OpenSSL、PowerShell或GUI工具检查证书详细信息，以检查扩展密钥使用情况扩展。

问题7.我是否仍然可以获取仅具有客户端身份验证EKU的公共信任证书？

A：某些CA(如SSL.com)提供专用客户端身份验证证书。这些证书与TLS证书分开，通常用于企业身份验证。

问题8.这是否会影响其他EKU或证书类型（代码签名、电子邮件等）？

A：否，此更改特定于TLS服务器证书。代码签名和电子邮件证书有它们自己的EKU要求。

问题9.我可以在何处了解关于此更改的官方要求？

A：Google Chrome Root Program Policy提供了在TLS服务器证书中禁止clientAuth EKU的准则。

问题10：在我的生产环境中不使用客户端和服务器EKU属性的证书是否安全？

答：对于生产环境，强烈建议客户使用具有适当EKU属性的证书。此做法可确保安全性、兼容性，以及符合行业标准和最佳实践。不具有EKU属性的证书应仅视为临时解决方法，并且仅在明确了解相关风险的情况下才使用。

相关信息

- 如需获取其他帮助，请联系思科技术支持中心 (TAC)。联系时需要提供有效的支持合同：思科全球支持联系信息
- 思科支持和下载:思科技术支持和下载

相关 Bug

- CSCwt94492 ENH:FMC应验证用于pxGrid集成的客户端证书中是否存在客户端身份验证EKU属性
- CSCwt94509加强版：FMC应显示一条消息，指示用于pxGrid集成的客户端证书中需要Client Authentication EKU属性
- CSCwt61767 2026年5月仅适用于EKU服务器的更改 — 如果EKU不足，请发出ASA配置警告
- CSCws83036 EKU:ISE中ClientAuth EKU实施的影响评估

思科ISE参考

- Field Notice：FN74392 — 思科身份服务引擎：从2026年5月开始的公共CA客户端身份验证EKU更改对安全通信的影响 — 提供的解决方法
- 准备身份服务引擎，以在公共证书颁发机构颁发的证书中扩展密钥使用限制

外部引用

- Chrome根计划策略
- IdenTrust门户
- SSL — 从TLS服务器证书中删除客户端身份验证EKU — 您需要了解的信息

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）。