在ISE中配置TLS/SSL证书

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[服务器证书](#)
[ISE证书](#)
[系统证书](#)
[受信任证书库](#)
[基本任务](#)
[生成自签名证书](#)
[续订自签名证书](#)
[安装受信任证书](#)
[安装CA签名的证书](#)
[备份证书和私钥](#)
[故障排除](#)
[检查证书有效性](#)
[删除证书](#)
[请求方不信任802.1x身份验证上的ISE服务器证书](#)
[ISE证书链正确，但终端在身份验证期间拒绝ISE服务器证书](#)
[常见问题](#)
[当ISE发出证书已经存在的警告时怎么办？](#)
[为什么浏览器会抛出警告，指出来自ISE的门户页面是由不受信任的服务器提供的？](#)
[当升级因证书无效而失败时，该怎么办？](#)
[相关信息](#)

简介

本文档介绍思科ISE中的TLS/SSL证书、ISE证书的种类和角色、如何执行常见任务和故障排除以及回答常见问题。

先决条件

要求

Cisco 建议您了解以下主题：

1. 思科身份服务引擎(ISE)
2. 用于描述不同类型ISE和AAA部署的术语。
3. RADIUS协议和AAA基础
4. SSL/TLS和x509证书
5. 公钥基础设施(PKI)基础

使用的组件

本文档中的信息基于Cisco ISE版本2.4 - 2.7软件和硬件版本。 它涵盖从2.4版到2.7版的ISE，但是，除非另有说明，它必须与其他ISE 2.x软件版本相似或相同。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

服务器证书

服务器证书用于向客户端提供服务器的身份以确保真实性，并为通信提供安全通道。这些证书可以是自签名（服务器向自身颁发证书）或由证书颁发机构（组织内部或知名供应商）颁发。

服务器证书通常颁发给服务器的主机名或FQDN（完全限定域名），也可以是通配符证书(*.domain.com影响。发布到的主机、域或子域通常在公用名(CN)或主题备用名(SAN)字段中提及。

通配符证书是使用通配符符号（用星号代替主机名）的SSL证书，因此允许在一个组织中的多个主机之间共享同一证书。例如，通配符证书Subject Name的CN或SAN值可能类似于 *.company.com 可用于保护此域的任何主机，例如 server1.com，server2.com,等等。

证书通常使用公钥加密或非对称加密。

- 公钥：公钥存在于其中一个字段的证书中，并且在设备尝试与其通信时由系统公开共享。
- 私钥：私钥是终端系统的私钥，与公钥配对。通过公钥加密的数据只能通过特定的配对私钥解密，反之亦然。

ISE证书

思科ISE依靠公钥基础设施(PKI)提供与终端、用户、管理员等的安全通信，以及多节点部署中的思科ISE节点之间的安全通信。PKI依靠x.509数字证书传输用于加密和解密消息的公钥，以及验证用户和设备提供的其他证书的真实性。思科ISE通常使用两种证书类别：

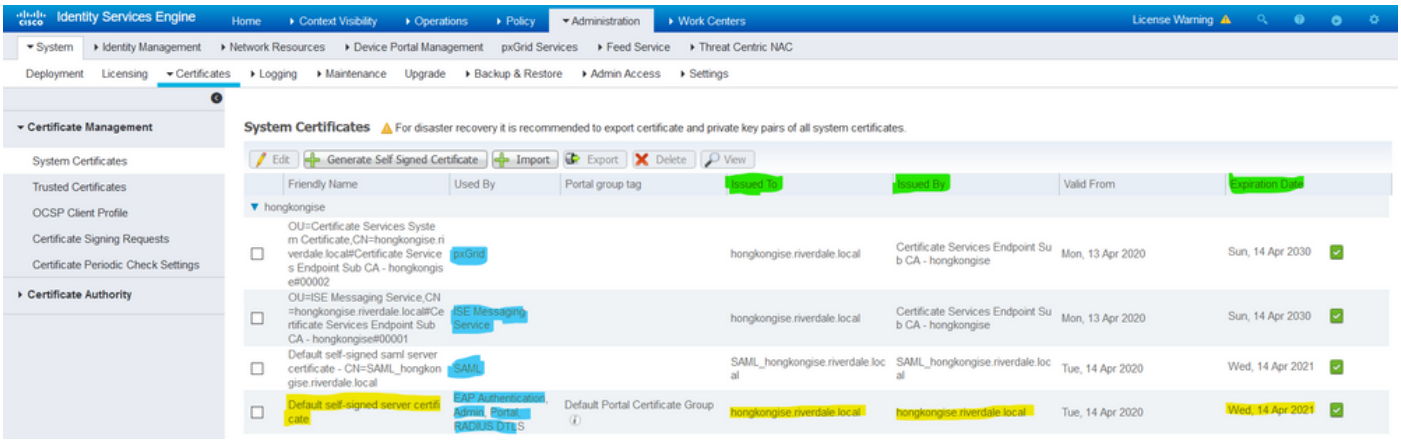
- System Certificates（系统证书）：这些是向客户端标识思科ISE节点的服务器证书。每个思科ISE节点都有自己的本地证书，每个证书与各自的私钥一起存储在节点上。
- 受信任证书存储证书(Trusted Certificates Store Certificates)：这些是用于验证提供给ISE的各种用途的证书的证书颁发机构(CA)证书。证书存储中的这些证书在主要管理节点上管理，并复制到分布式思科ISE部署中的所有其他节点。证书存储还包含由用于BYOD的ISE的内部证书颁发机构为ISE节点生成的证书。

系统证书

系统证书可用于一个或多个角色。每个角色都有不同的用途，具体解释如下：

- Admin：用于保护443上的所有通信（管理GUI）、复制，以及此处未列出的任何端口/使用情况。
- 门户：用于通过集中式Web身份验证(CWA)门户、访客、BYOD、客户端调配、本地请求方调配门户等门户保护HTTP通信。每个门户必须映射到门户组标记（默认为默认门户组标记），指示门户使用特定标记的证书。证书的“编辑”选项中的“门户组标记名称”下拉菜单允许您创建新标记或选择现有标记。
- EAP：这是一个角色，用于指定提供给客户端的证书以进行802.1x身份验证。证书几乎用于所有可能的EAP方法，例如EAP-TLS、PEAP、EAP-FAST等。对于隧道EAP方法（例如PEAP和FAST），传输层安全(TLS)用于保护凭证交换。在建立此隧道以确保安全交换之前，客户端凭证不会发送到服务器。
- RADIUS DTLS：此角色指定用于DTLS连接（UDP上的TLS连接）的证书，以加密网络接入设备(NAD)和ISE之间的RADIUS流量。NAD必须支持DTLS加密，此功能才能正常工作。
- SAML：服务器证书用于保护与SAML身份提供程序(IdP)的通信。指定用于SAML的证书不能用于任何其他服务，如管理员、EAP身份验证等。
- ISE消息传送服务：自2.6起，ISE使用ISE消息传送服务而不是旧系统日志协议来记录数据。用于加密此通信。
- PxGrid：此证书用于ISE上的PxGrid服务。

安装ISE时，它会生成 Default Self-Signed Server Certificate.默认情况下，此配置分配给EAP身份验证、管理员、门户和RADIUS DTLS。建议将这些角色移动到内部CA或已知的CA签名证书。

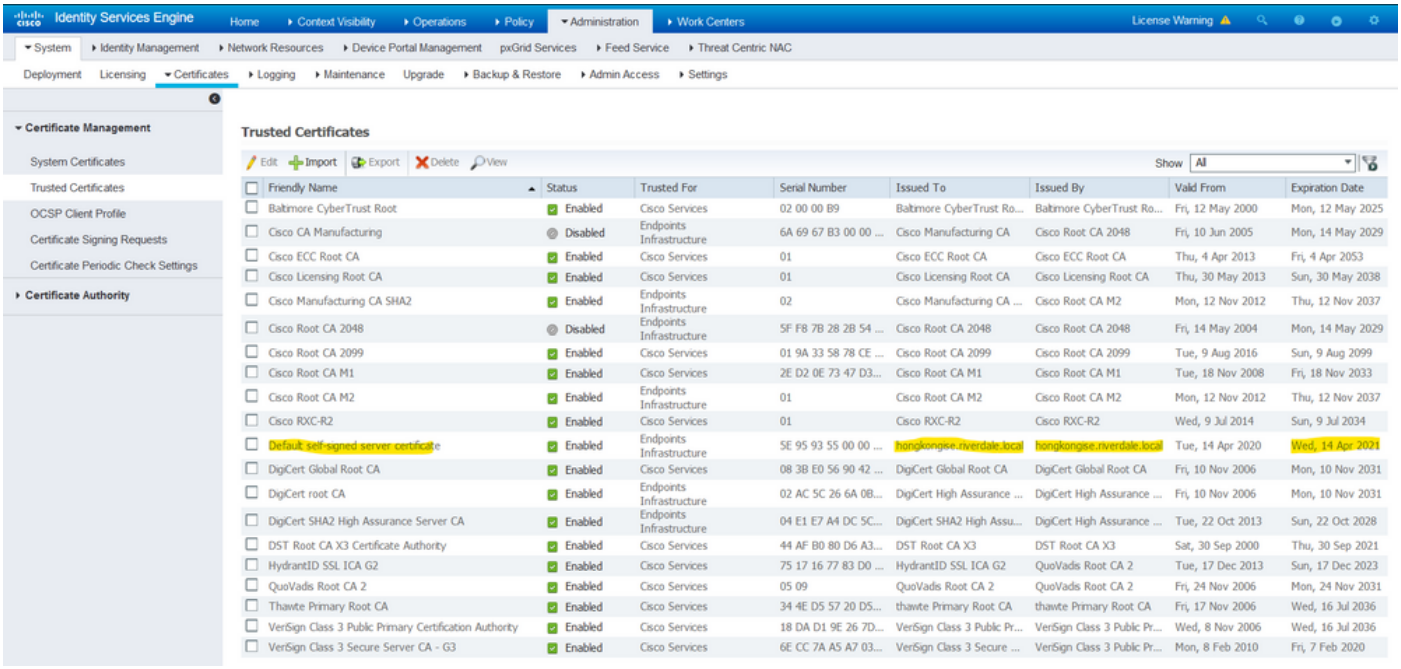


提示：最好确保ISE服务器的FQDN和IP地址都添加到ISE系统证书的SAN字段。 一般来说，为了确保思科ISE中的证书身份验证不受证书驱动的验证功能细微差异的影响，请为网络中部署的所有思科ISE节点使用小写主机名。

注:ISE证书的格式必须是隐私增强邮件(PEM)或可分辨编码规则(DER)。

受信任证书库

证书颁发机构证书必须存储在 Administration > System > Certificates > Certificate Store 他们必须拥有 Trust for client authentication 使用案例确保ISE使用这些证书验证终端、设备或其他ISE节点提供的证书。



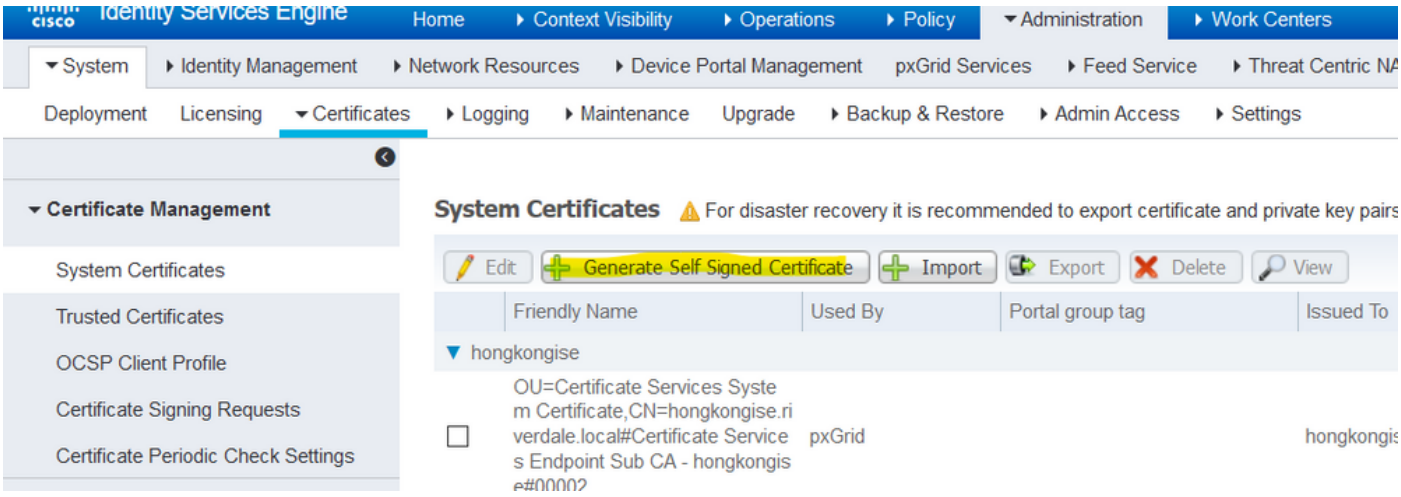
基本任务

该证书有到期日期，可以撤销证书或要求证书在某个时间进行更换。如果ISE服务器证书过期，除非使用新的有效证书替换严重问题。

> **注意**：如果用于可扩展身份验证协议(EAP)的证书过期，客户端身份验证可能会失败，因为客户端不再信任ISE证书。如果用于门户的证书过期，客户端和浏览器可能会拒绝连接到门户。如果管理员使用证书过期，风险更大，这会阻止管理员再登录ISE，并且分布式部署可能会停止运行。

生成自签名证书

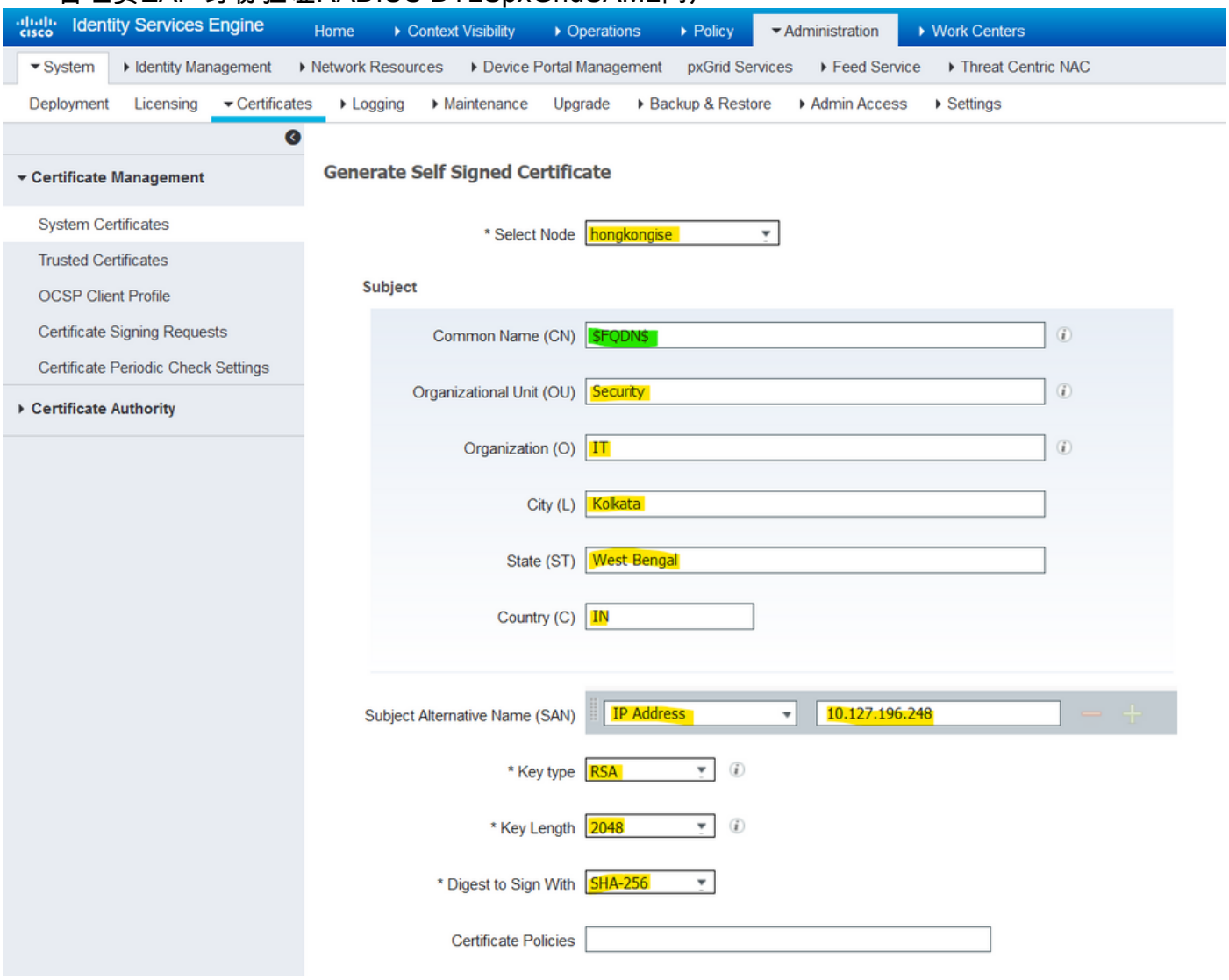
要生成新的自签名证书，请导航至 Administration > System > Certificates > System Certificates.单击 Generate Self Signed Certificate.

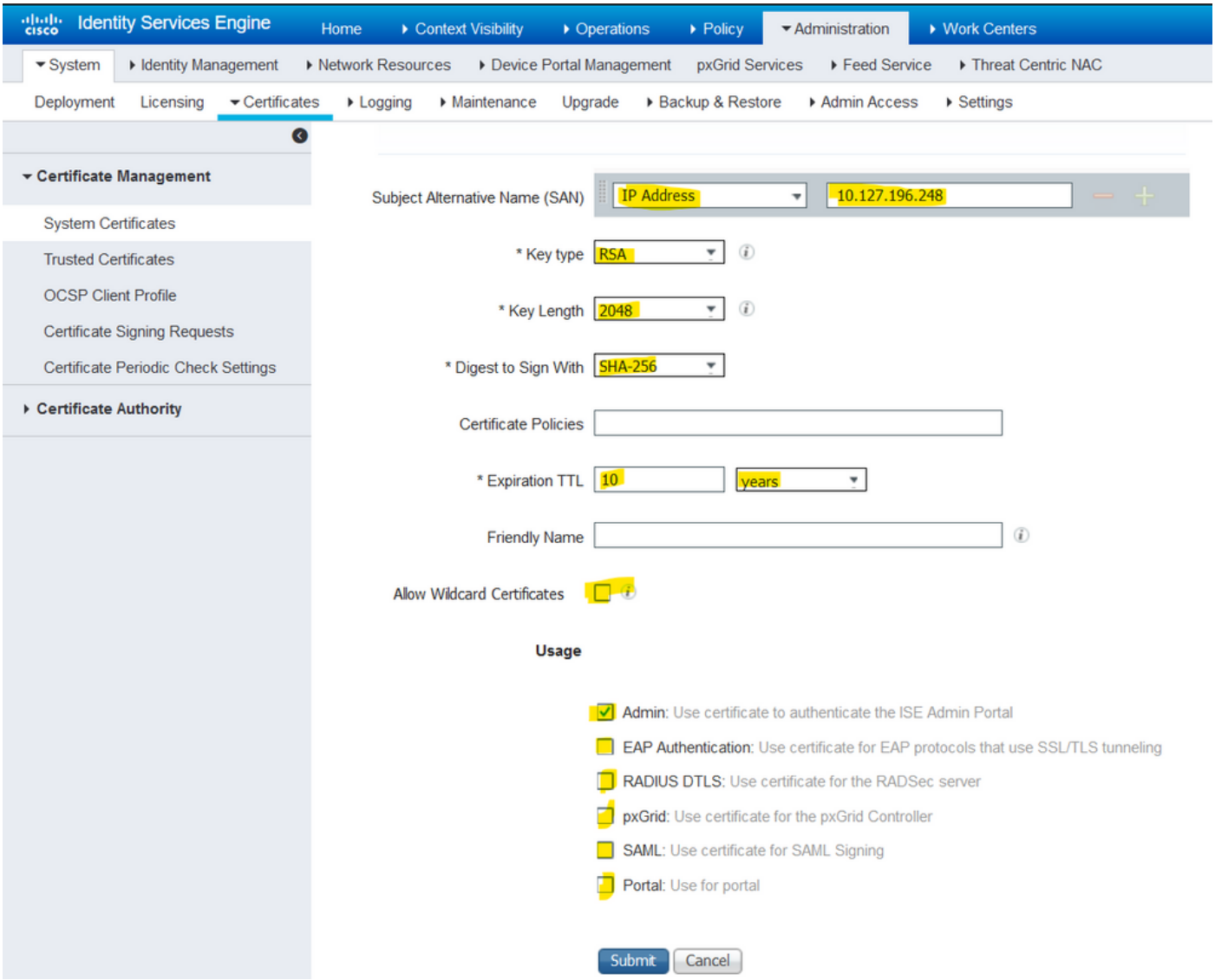


此列表介绍Generate Self Signed Certificate页面中的字段。

自签名证书设置字段名称使用指南：

- Select Node:(Required)生成系统证书所需的节点。
- CN：（如果未指定SAN则必需）默认情况下，CN是为其生成自签名证书的ISE节点的FQDN。
- 组织单位(OU)：组织单位名称，例如，工程。
- 组织(O)：组织名称，例如Cisco。
- 城市(L)：（请勿缩写）城市名称，例如San Jose。
- 州(ST)：（请勿缩写）州名，例如California。
- 国家(C)：国家/地区名称。需要两个字母的ISO国家/地区代码。例如，美国。
- SAN：与证书关联的IP地址、DNS名称或统一资源标识符(URI)。
- Key Type：指定用于创建公钥的算法：RSA或ECDSA。
- 密钥长度(Key Length)：指定公钥的位大小。这些选项可用于RSA:512 1024 2048 4096，这些选项可用于ECDSA:256 384。
- 要签名的摘要：选择以下哈希算法之一：SHA-1或SHA-256。
- Certificate Policies：输入证书必须符合的证书策略OID或OID列表。使用逗号或空格分隔OID。
- Expiration TTL：指定证书到期的天数。
- Friendly Name：输入证书的友好名称。如果未指定名称，思科ISE会自动创建格式的名称 其中 是一个唯一的5位数数字。
- 允许通配符证书(Allow Wildcard Certificates)：选中此复选框以生成自签名的通配符证书(在主题中的任何CN和/或SAN中的DNS名称中包含星号(*)的证书。例如，分配给SAN的DNS名称可以是 *.domain.com.
- 用法：选择必须使用此系统证书的服务。可用选项包括：
管理员EAP 身份验证RADIUS DTLSpxGridSAML门户





注意：对于相同的安全级别，RSA和ECDSA公钥可以具有不同的密钥长度。如果目标是获取公共CA签名证书或部署思科ISE作为符合FIPS的策略管理系统，请选择2048。

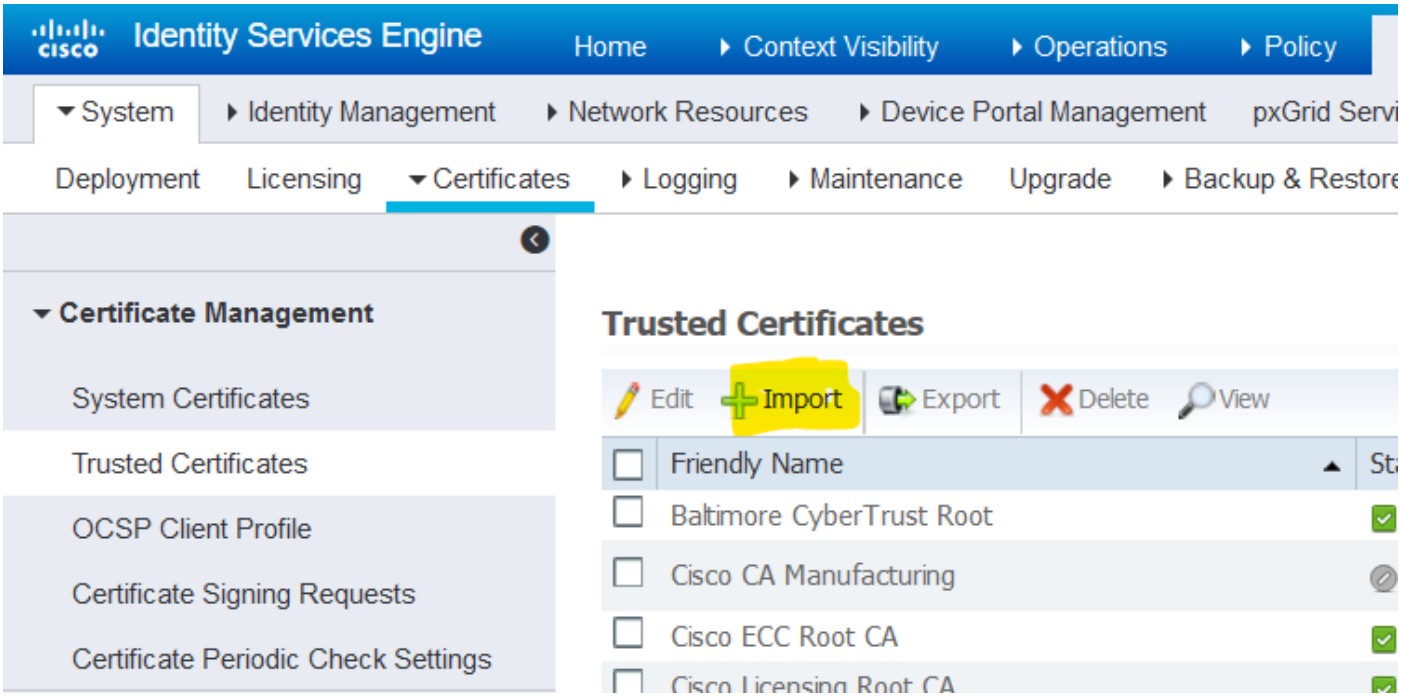
续订自签名证书

要查看存在的自签名证书，请导航至 Administration > System > Certificates > System Certificates 在ISE控制台中。如果同一ISE服务器FQDN中提到任何具有“Issued To”和“Issued By”的证书，则它是自签名证书。选择此证书，然后单击 **Edit**.
低于 **Renew Self Signed Certificate**,查看 **Renewal Period** 框，并根据需要设置Expiration TTL。最后，单击 Save.

安装受信任证书

从根CA、中间CA和/或需要受信任的主机获取Base 64编码证书。

1.登录到ISE节点并导航至 Administration > System > Certificate > Certificate Management > Trusted Certificates 并点击 Import，如图所示。

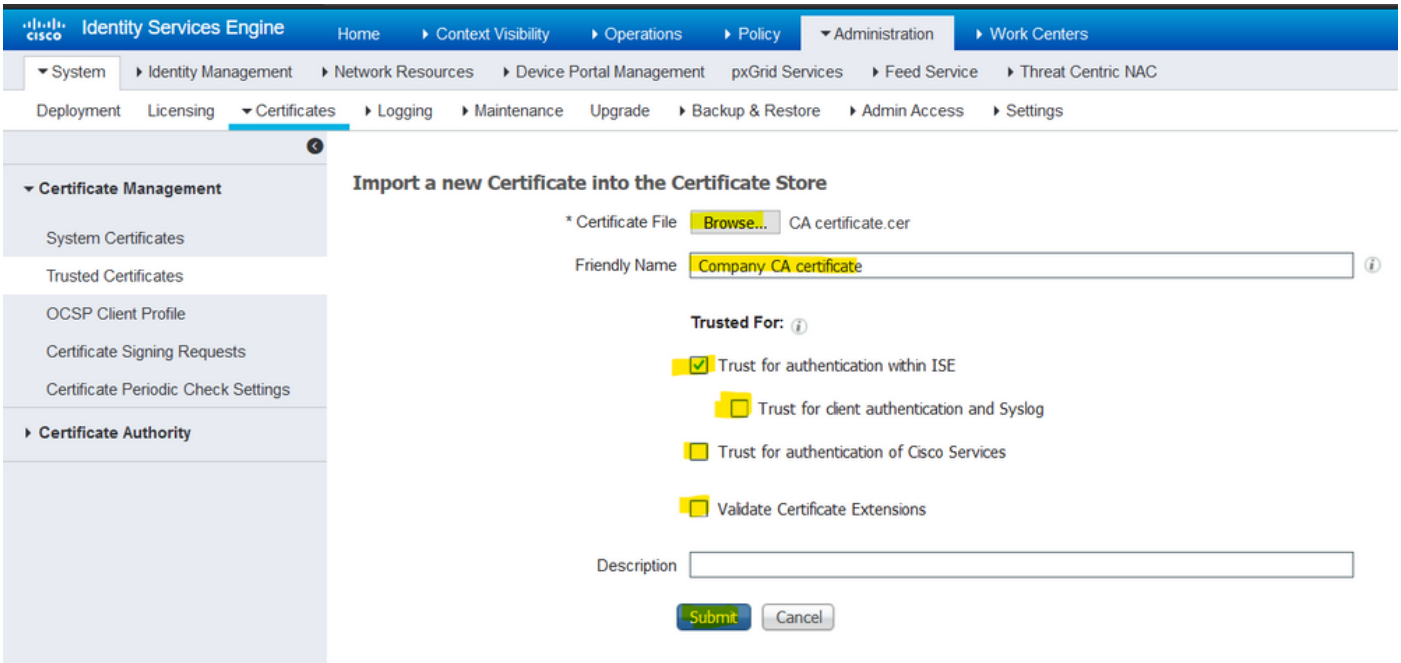


2.在下一页上，上传获得的CA证书（顺序与前面所述的相同）。为其分配一个友好名称和说明以跟踪证书。

根据使用需要，选中以下各项旁边的复选框：

- Trust for authentication within ISE — 这是当新的ISE节点将相同的受信任CA证书加载到其受信任证书库时，添加新的ISE节点。
- Trust for client authentication and Syslog — 启用此功能，以便使用证书对连接到ISE且具有EAP和/或信任安全系统日志服务器的终端进行身份验证。
- 信任思科服务的身份验证 — 仅信任外部思科服务（如源服务）才需要此功能。

3.最后，单击 Submit.现在，证书必须在受信任的存储中可见，并同步到所有辅助ISE节点（如果在部署中）。



安装CA签名的证书

一旦根和中间CA证书添加到受信任证书库，即可发出证书签名请求(CSR)，并且基于CSR签名的证书可绑定到ISE节点。

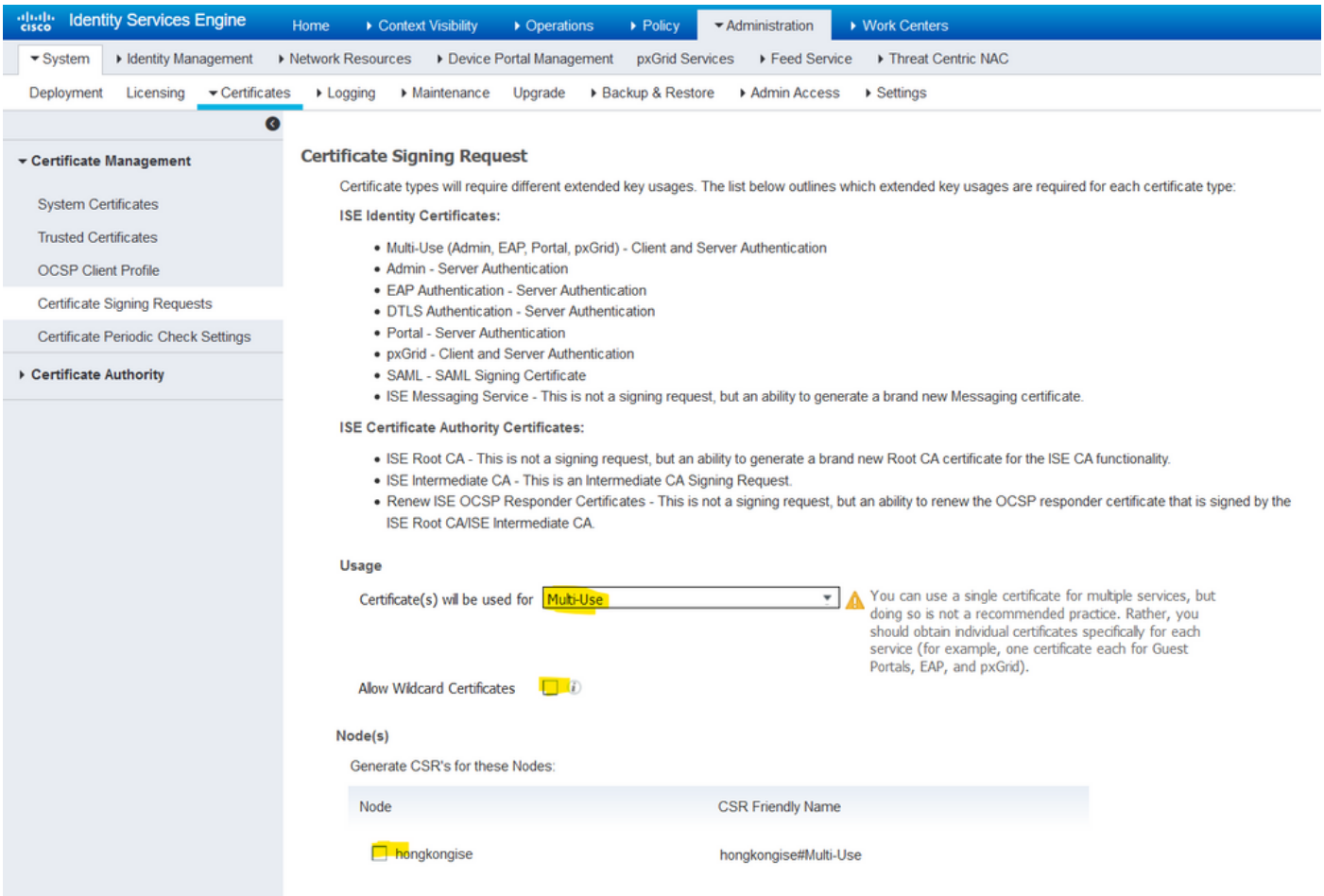
1.为此，请导航至 Administration > System > Certificates > Certificate Signing Requests 并点击 **Generate Certificate Signing Requests (CSR)** 生成CSR。

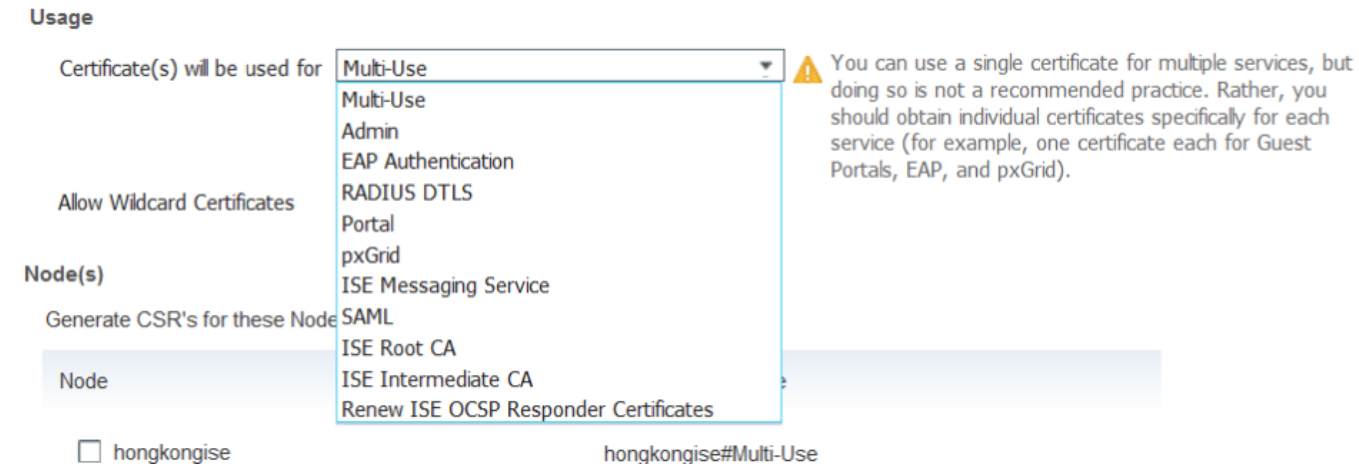
2.在出现的页面上的“用法”部分下，从下拉菜单中选择要使用的角色。

如果证书用于多个角色，请选择Multi-Use。生成证书后，可以根据需要更改角色。在大多数情况下，证书可在Used For下拉列表中设置为用于多用途；这允许证书可用于所有ISE Web门户。

3.选中ISE节点旁边的复选框，以选择为其生成证书的节点。

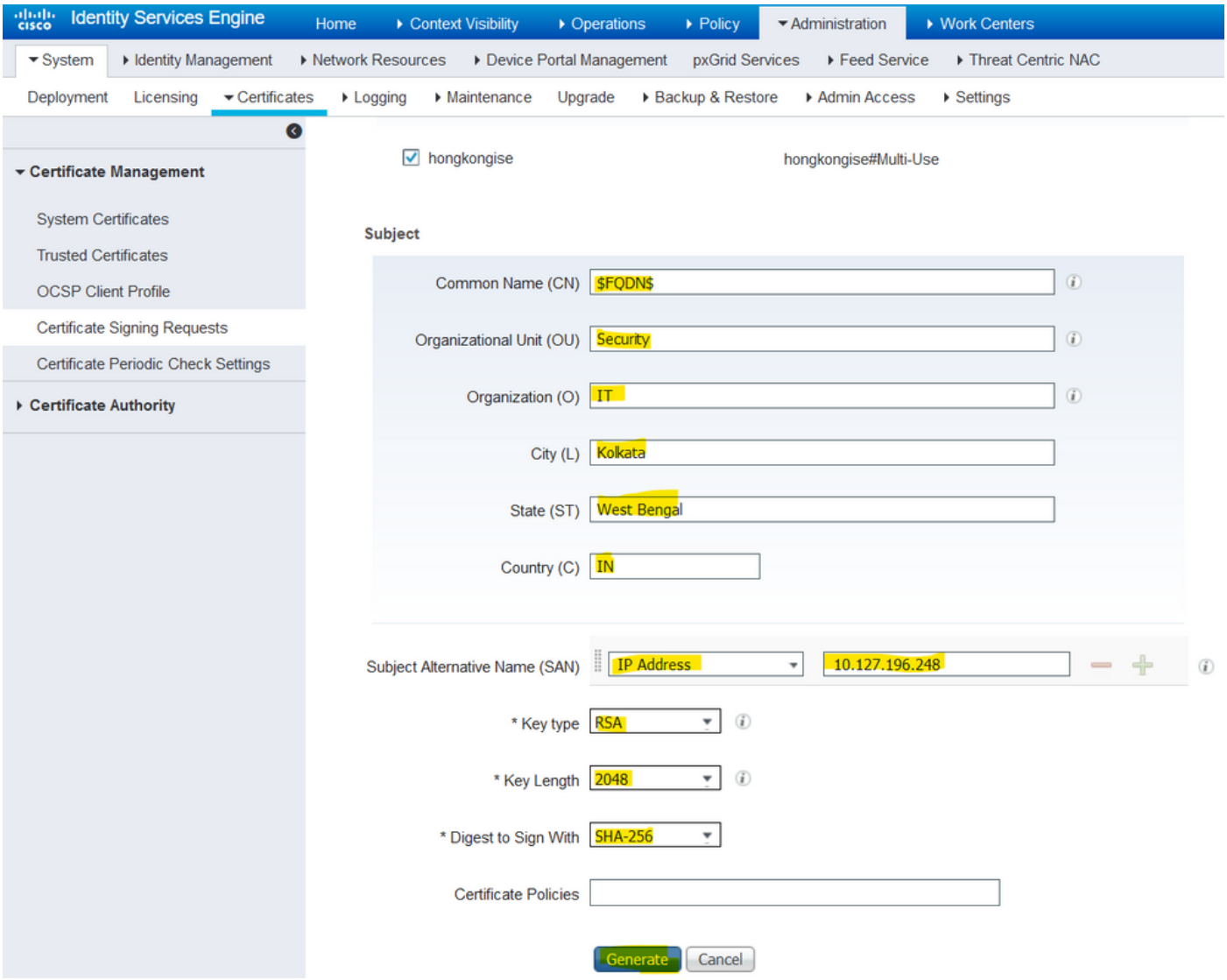
4.如果目的是安装/生成通配符证书，请查看 Allow Wildcard Certificates 包装盒.

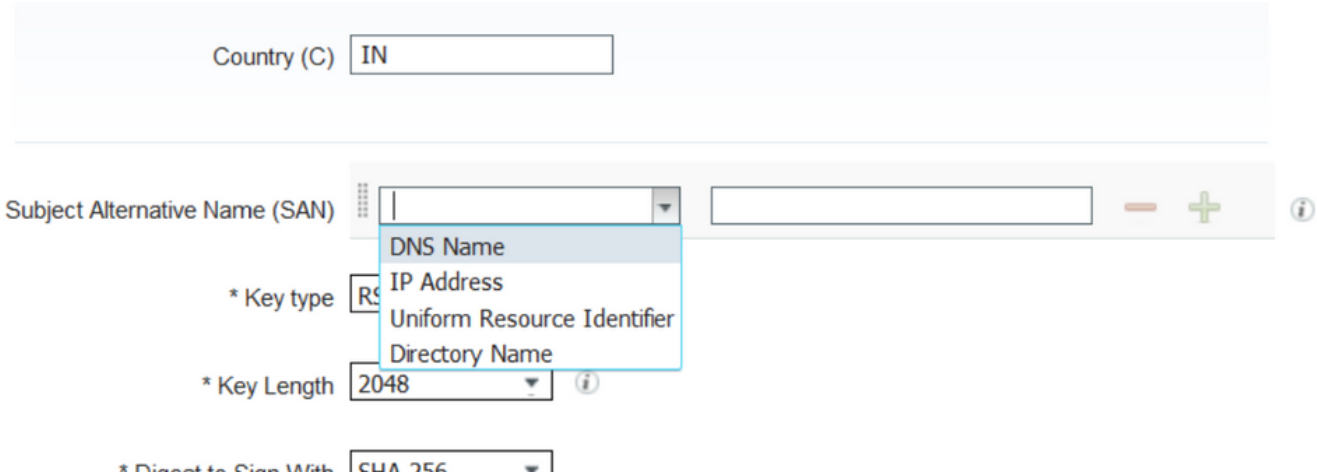




5.根据主机或组织（组织单位、组织、城市、省/自治区、国家/地区）的详细信息填写主题信息。

6.要完成此操作，请单击 Generate，然后单击 Export 在弹出窗口上。





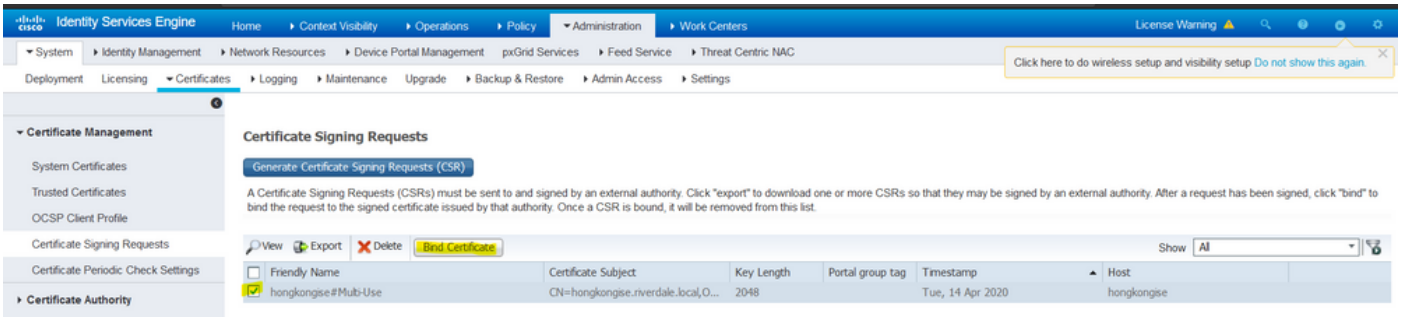
这会下载刚创建的Base-64编码的证书请求请求 — 必须将此PEM文件发送到CA进行签名，并获取生成的签名证书CER文件（Base 64编码）。

注：在CN字段下，ISE自动填充节点FQDN。

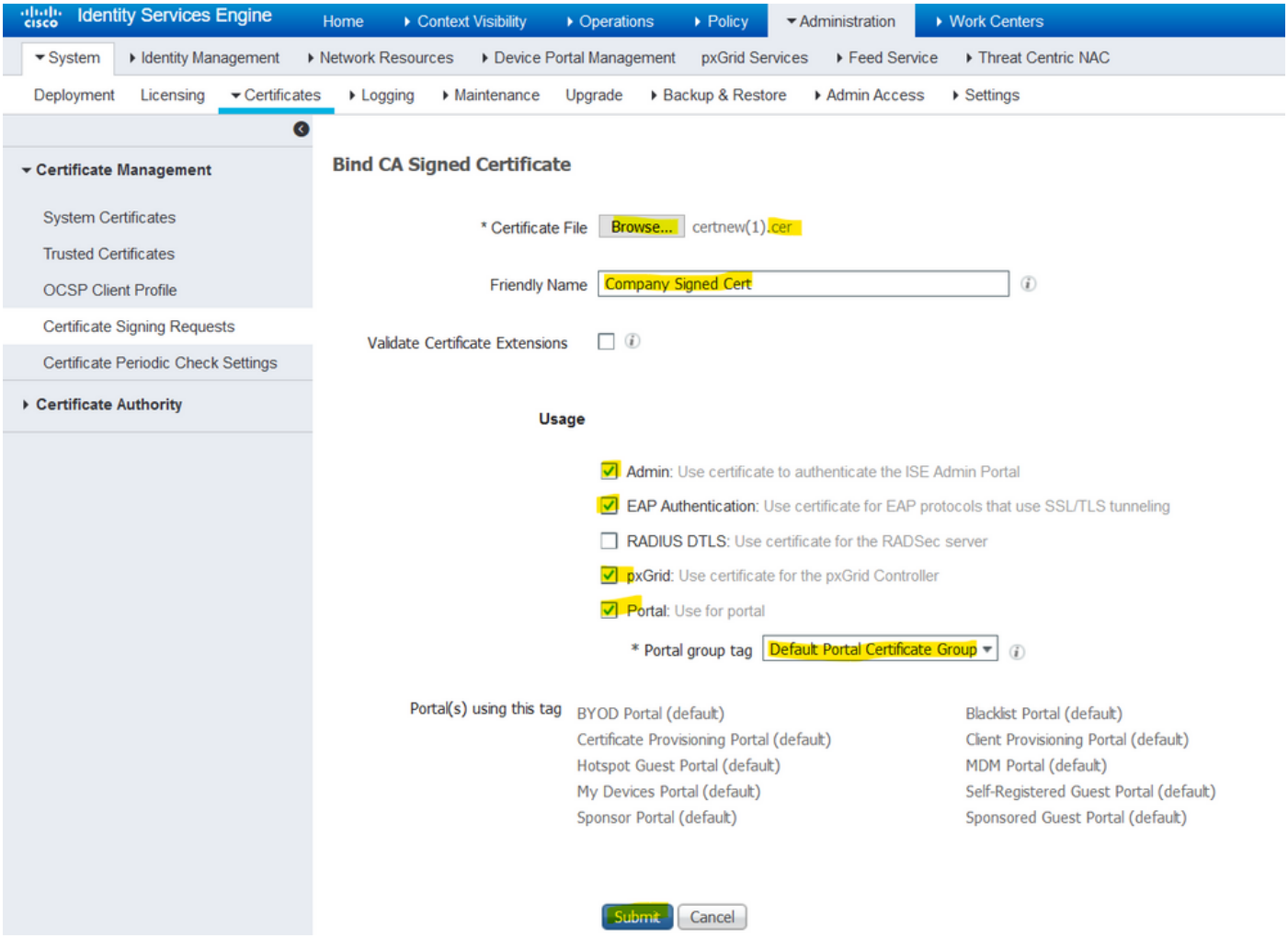
注：在ISE 1.3和1.4中，至少需要发出两个CSR才能使用pxGrid。一个专用于pxGrid，另一个专用于pxGrid的其他服务。从2.0及更高版本开始，所有这一切都集中在一个CSR上。

注：如果证书用于EAP身份验证，则"*"符号不能在Subject CN字段中，因为Windows请求方会拒绝服务器证书。即使在Supplicant客户端上禁用了Validate Server Identity，当"*"位于CN字段中时，SSL握手也可能失败。相反，可以在CN字段中使用通用FQDN，然后 *.domain.com 可用于SAN DNS名称字段。某些证书颁发机构(CA)可以在证书的CN中自动添加通配符(*)，即使该通配符不存在于CSR中。在这种情况下，需要提出特殊请求来阻止此操作。

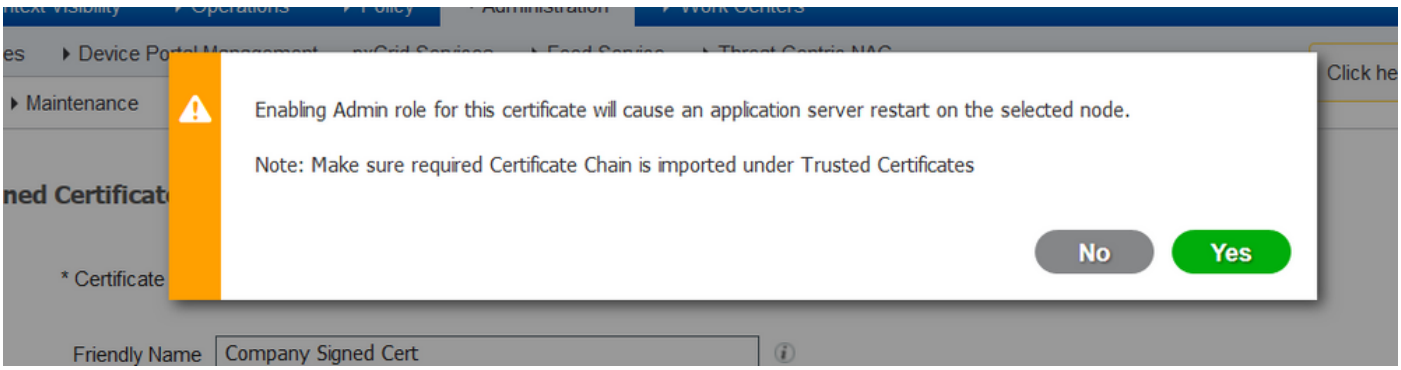
7.证书由CA签名后(如视频所示从CSR生成后，如果使用Microsoft CA，请返回到ISE GUI，然后导航到**Administration > System > Certificates > Certificate Management > Certificate Signing Request**；选中以前创建的CSR旁边的框，然后单击**Bind Certificate**按钮。

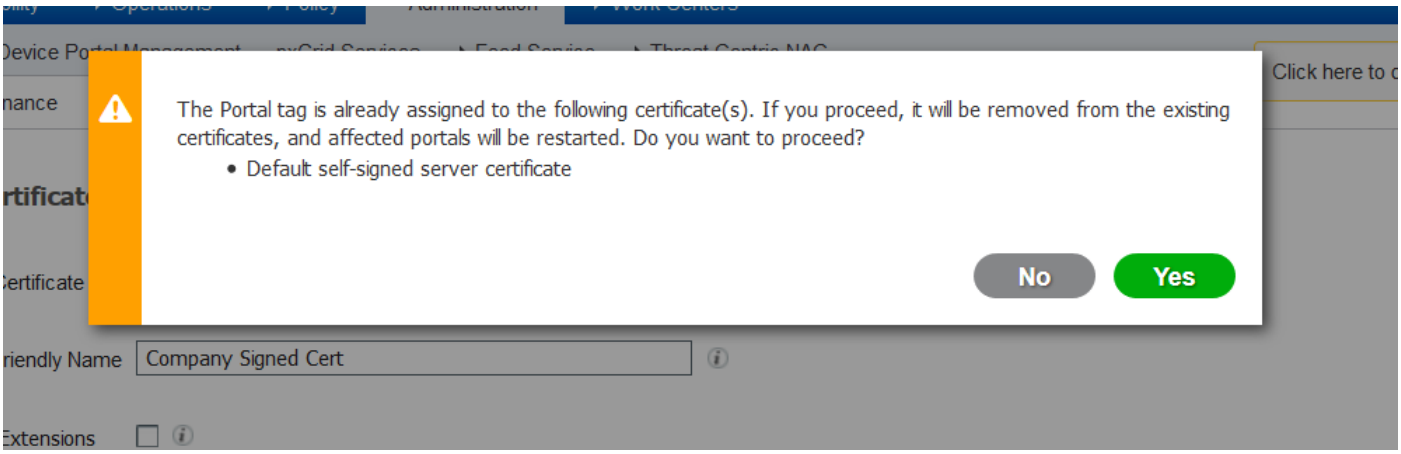


8.接下来，上传刚收到的签名证书，并为其指定友好名称ISE。然后，根据证书的需要（如管理员和EAP身份验证、门户等），继续选择使用旁的框，然后单击 Submit，如下图所示：



如果已为此证书选择管理员角色，ISE节点必须重新启动其服务。根据分配给VM的版本和资源，这需要10-15分钟。要检查应用的状态，请打开ISE命令行并发出 show application status ise 命令。





如果在证书导入时选择了管理员或门户角色，则可以在访问浏览器中的管理员或门户页面时验证新证书是否就位。在浏览器中选择锁定符号，在证书下，路径会验证整个链是否存在，以及计算机是否信任该链。只要链构建正确，并且证书链受浏览器信任，浏览器就必须信任新的管理员或门户证书。

注：要续订当前CA签名的系统证书，请生成一个新的CSR，并使用相同的选项将签名的证书绑定到该证书。由于在ISE激活之前可以安装新证书，因此计划在旧证书过期之前安装新证书。旧证书到期日期和新证书开始日期之间的这段重叠期为更新证书和计划交换提供了时间，几乎不会造成停机。新证书的开始日期应早于旧证书的到期日期。这两个日期之间的时间段即为更换窗口期。新证书进入其有效日期范围后，启用所需的协议(Admin/EAP/Portal)。请记住，如果启用Admin usage，将会重新启动服务。

提示：建议对管理员和EAP证书使用公司内部CA，对访客/发起人/热点/等门户使用公开签名的证书。原因在于，如果用户或访客进入网络并且ISE门户使用访客门户的私有签名证书，他们将会收到证书错误或者他们的浏览器可能会阻止他们从门户页面。为避免出现上述情况，请使用公共签名的门户证书来确保更好的用户体验。此外，必须将每个部署节点的IP地址添加到SAN字段，以避免通过IP地址访问服务器时出现证书警告。

备份证书和私钥

建议导出：
1.所有系统证书（来自部署中的所有节点）及其私钥（重新安装这些证书需要这些私钥）到安全位置。记录证书配置（证书用于什么服务）。

2.来自主管理节点的受信任证书库的所有证书。记录证书配置（证书用于什么服务）。

3.所有证书颁发机构证书。

为此，

1. 导航至 Administration > System > Certificates > Certificate Management > System Certificates.选择证书并单击 Export.选择 Export Certificates 和私钥单选按钮。输入私钥密码并确认密码。点击 Export.
2. 导航至 Administration > System > Certificates > Certificate Management > Trusted Certificates.选择证书并单击 Export.点击 Save File 导出证书。
3. 导航至 Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates.选择证书并单击 **Export**.选择 Export Certificates 和私钥单选按钮。输入私钥密码和确认密码。点击 Export.点击 Save File 导出证书。

故障排除

检查证书有效性

如果思科ISE受信任证书或系统证书库中的任何证书已过期，升级过程将失败。确保检查“受信任证书”(Trusted Certificates)和“系统证书”(System Certificates)窗口(Administration > System > Certificates > Certificate Management)，如有必要，请在升级前续订。

此外，在CA Certificates窗口中检查证书的Expiration Date字段的有效性(Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates)，如有必要，请在升级前续订。

删除证书

如果ISE中的证书已过期或未使用，则需要将其删除。确保在删除之前导出证书（如果适用，使用它们的私钥）。

要删除已过期的证书，请导航至 Administration > System > Certificates > Certificate Management.单击 System Certificates Store.选择过期证书，然后单击 Delete.
有关受信任证书和证书颁发机构证书存储的信息，请参阅相同内容。

请求方不信任802.1x身份验证上的ISE服务器证书

验证ISE是否为SSL握手进程发送完整证书链。

如果在客户端操作系统设置中选择了需要服务器证书（即PEAP）和验证服务器身份的EAP方法，请求方会在身份验证过程中使用其本地信任存储中的证书验证证书链。作为SSL握手过程的一部分，ISE会提供其证书以及链中存在的任何根证书和/或中间证书。如果链不完整或其信任存储中缺少此链，则请求方无法验证服务器身份。

为了验证证书链是否传递回客户端，请从ISE捕获数据包(Operations > Diagnostic Tools > General Tools > TCP Dump)或Wireshark捕获。打开捕获并应用过滤器 ssl.handshake.certificates 并查找访问质询。

选择后，导航至 Expand Radius Protocol > Attribute Value Pairs > EAP-Message Last segment > Extensible Authentication Protocol > Secure Sockets Layer > Certificate > Certificates.

如果链不完整，请导航至ISE Administration > Certificates > Trusted Certificates 并验证是否存在根证书和/或中间证书。如果证书链成功通过，则必须使用此处概述的方法验证证书链本身是否有效。

打开每个证书（服务器、中间证书和根证书），验证信任链，将每个证书的主题密钥标识符(SKI)与链中下一个证书的授权密钥标识符(AKI)匹配。

ISE证书链正确，但终端在身份验证期间拒绝ISE服务器证书

如果ISE为SSL握手提供其完整的证书链，并且请求方仍然拒绝证书链；下一步是验证根证书和/或中间证书在客户端本地信任存储中。

要从Windows设备验证这一点，请启动 mmc.exe（Microsoft管理控制台），导航至 File > Add-Remove Snap-in.从可用管理单元列中，选择 Certificates 并点击 Add.选择其中之一 My user account 或 **Computer account** 根据使用的身份验证类型（用户或计算机），然后单击 OK .

在控制台视图下，选择Trusted Root Certification Authorities和Intermediate Certification Authorities以验证本地信任存储中是否存在根证书和中间证书。

验证这是服务器身份检查问题的一种简单方法，取消选中Supplicant客户端配置文件配置下的Validate Server Certificate，然后重新测试。

常见问题

当ISE发出证书已存在的警告时怎么办？

此消息意味着ISE检测到具有完全相同OU参数的系统证书，并且尝试安装重复证书。由于不支持重复的系统证书，因此建议将任何城市/州/省的值更改为稍有不同的值，以确保新证书不同。

为什么浏览器会抛出警告，指出来自ISE的门户页面是由不受信任的服务器提供的？

当浏览器不信任服务器的身份证书时，会发生这种情况。

首先，确保浏览器上显示的门户证书符合预期，并且已在ISE上为门户配置。
其次，确保通过FQDN访问门户 — 如果使用的IP地址，请确保FQDN和IP地址都位于证书的SAN和/或CN字段中。
最后，确保客户端操作系统/浏览器软件导入/信任门户证书链（ISE门户、中间CA、根CA证书）。

> **注**:iOS、Android OS和Chrome/Firefox浏览器的某些较新版本对证书有严格的安全期望。即使满足了这些条件，如果门户和中间CA小于SHA-256，它们也可以拒绝连接。

当升级因证书无效而失败时，该怎么办？

如果思科ISE受信任证书或系统证书库中的任何证书已过期，升级过程将失败。确保检查“受信任证书”(Trusted Certificates)和“系统证书”(System Certificates)窗口(Administration > System > Certificates > Certificate Management)，如有必要，请在升级前续订。

此外，在CA Certificates窗口中检查证书的Expiration Date字段的有效性(Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates)，如有必要，请在升级前续订。

在ISE升级之前，请确保内部CA证书链有效。

导航至 Administration > System > Certificates > Certificate Authority Certificates.对于部署中的每个节点，在Friendly Name列中选择证书服务终端子CA的证书。点击 View 并检查Certificate Status（证书状态）是否为正常消息且可见。

如果任何证书链中断，请确保在Cisco ISE升级过程开始之前解决此问题。要解决此问题，请导航至 **Administration > System > Certificates > Certificate Management > Certificate Signing Requests**，并为ISE根CA选项生成一个。

相关信息

- ISE 2.7管理证书和证书存储设置
- 在ISE中实施数字证书
- 技术支持和文档 - Cisco Systems

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）。