在ISE中安装第三方CA签名的证书

目录

简介

本文档介绍如何在思科身份服务引擎(ISE)中安装由第三方证书颁发机构(CA)签名的证书。

先决条件

要求

Cisco建议您了解基本公钥基础设施。

使用的组件

本文档中的信息基于思科身份服务引擎(ISE)版本3.0。相同的配置适用于版本2.X

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。

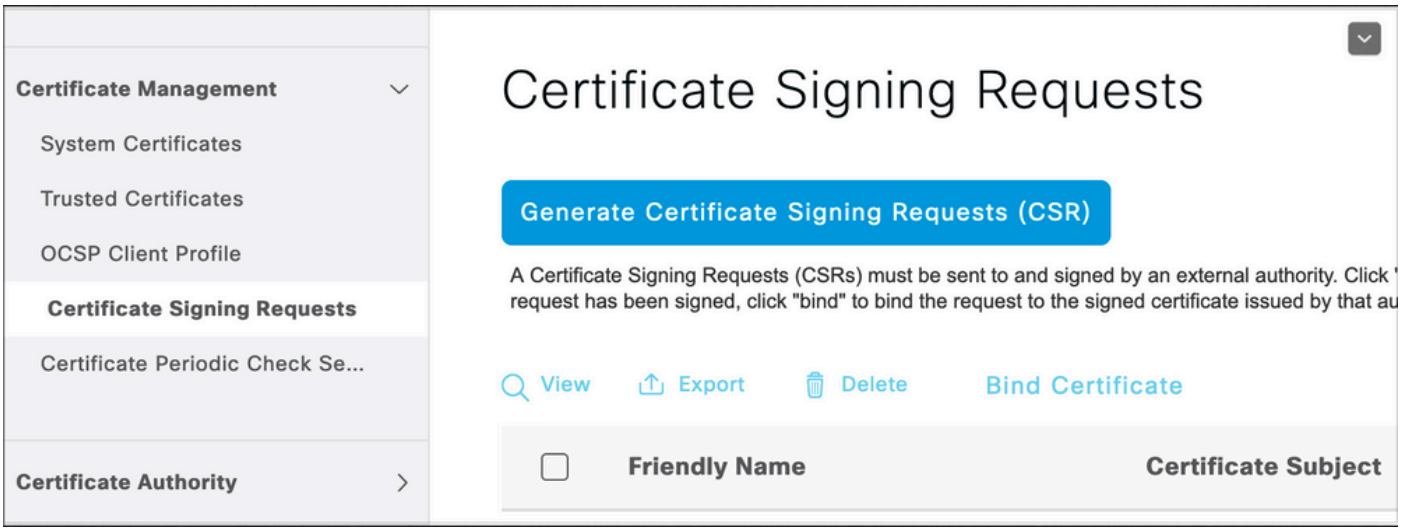
背景信息

无论最终证书角色（EAP身份验证、门户、管理员和pxGrid）如何，此过程都是相同的。

配置

步骤1:生成证书签名请求(CSR)。

要生成CSR，请导航到管理>证书>证书签名请求，然后单击生成证书签名请求(CSR)。



1. 在Usage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，则可以选择Multi-use。生成证书后，可以根据需要更改角色。

2. 选择可为其生成证书的节点。

3. 根据需要填写信息（组织单位、组织、城市、省/自治区/直辖市）。

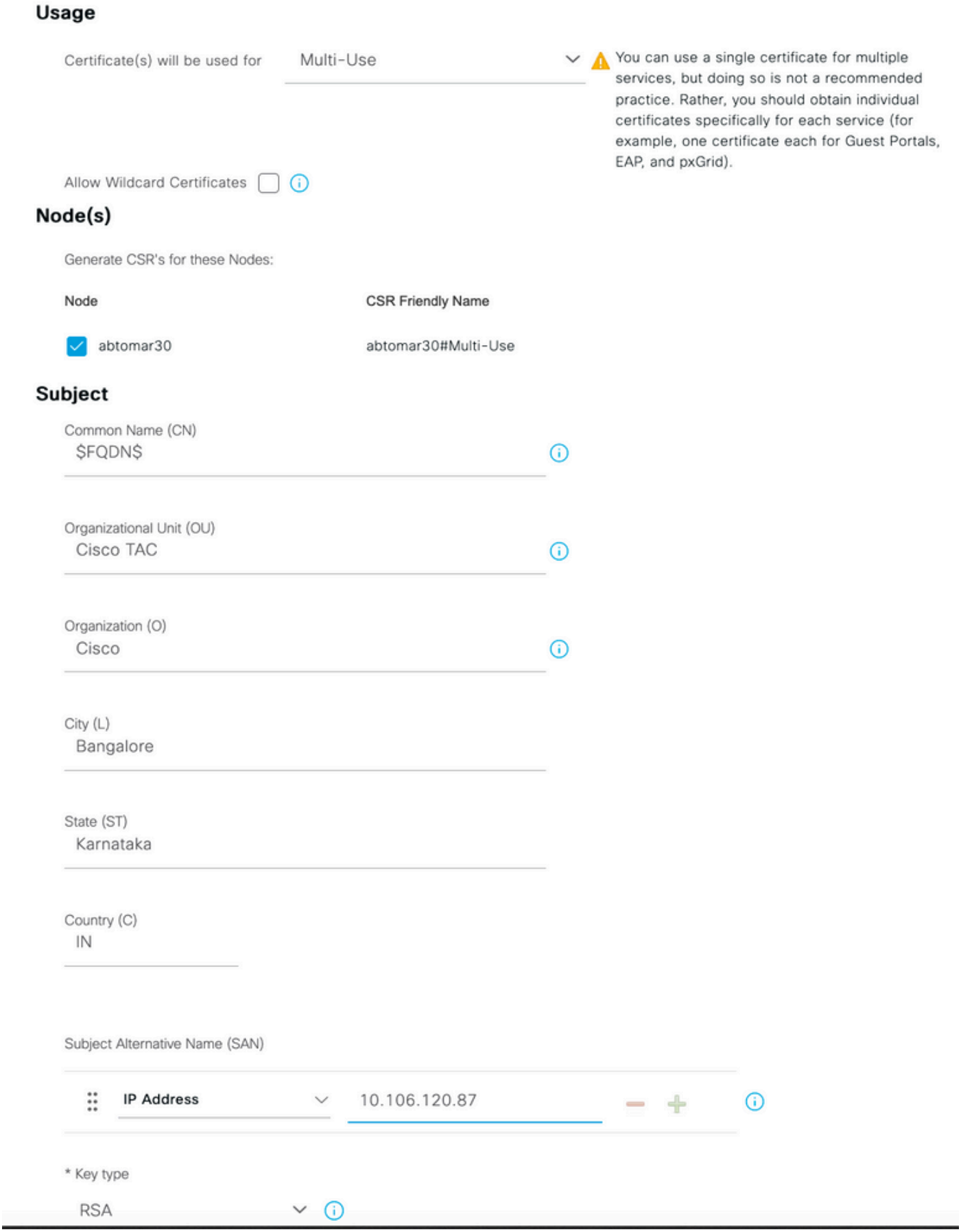
注意：在公用名(CN)字段下，ISE自动填充节点的完全限定域名(FQDN)。

通配符：

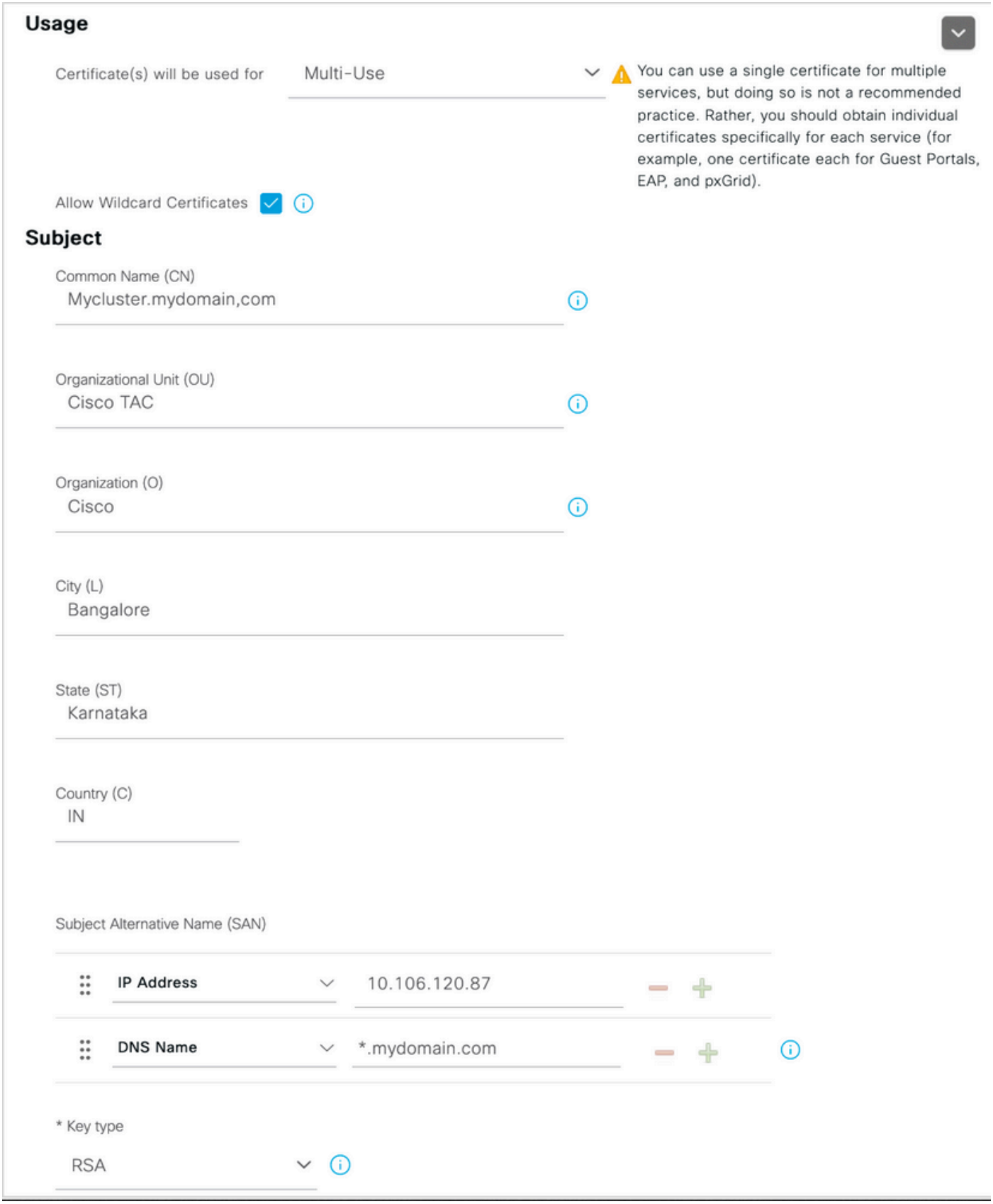
- 如果目标是生成通配符证书，请选中Allow Wildcard Certificates框。
- 如果证书用于EAP身份验证，则*符号不能位于Subject CN字段中，因为Windows请求方会拒绝服务器证书。
- 即使Supplicant客户端上禁用了Validate Server Identity，当*在CN字段中时，SSL握手也可能失败。
- 相反，可以在CN字段中使用通用FQDN，然后在*.domain.comSubject Alternative Name(SAN)DNS Name字段上使用。

注意：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。

单个服务器证书CSR示例：

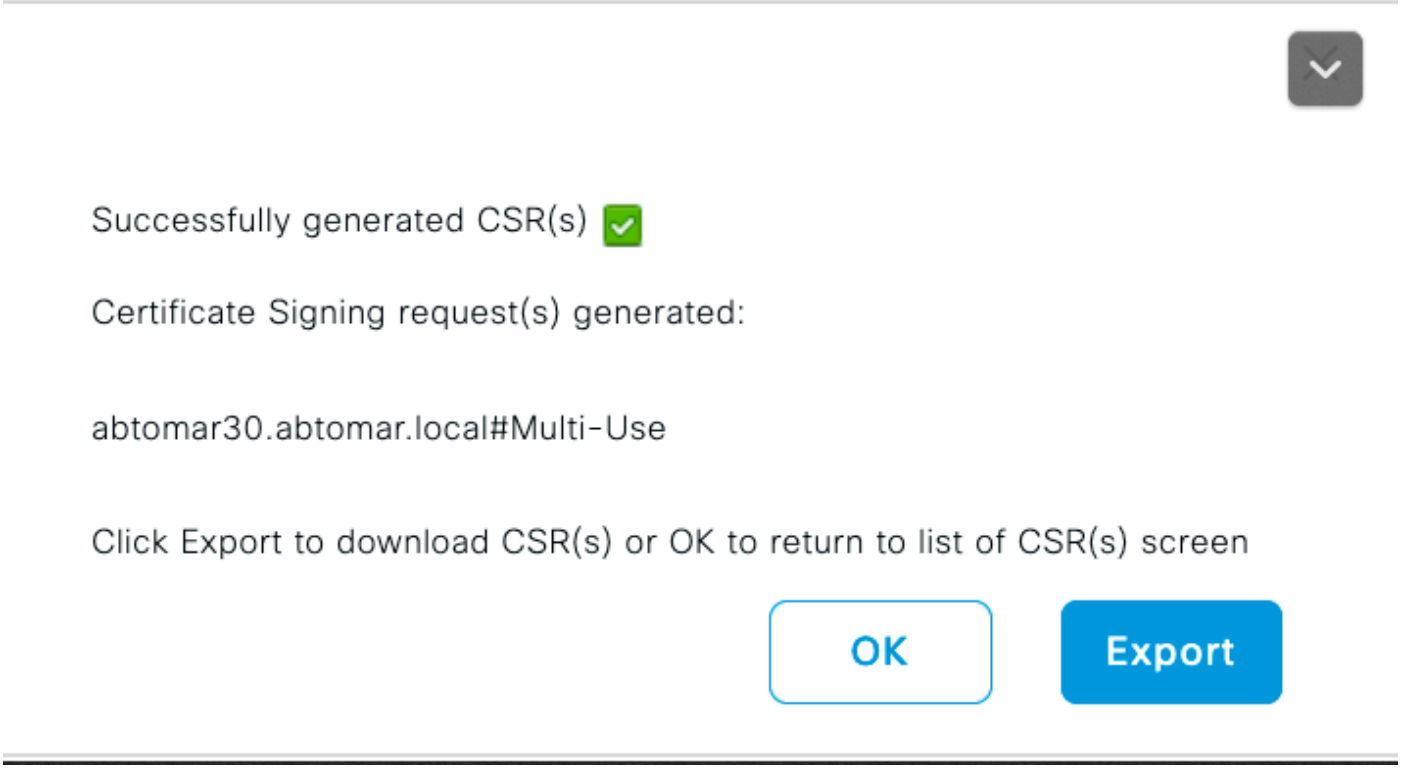

Usage
Certificate(s) will be used for
Multi-Use
You can use a single certificate for multiple services, but doing so is not a recommended practice. Rather, you should obtain individual certificates specifically for each service (for example, one certificate each for Guest Portals, EAP, and pxGrid).
Allow Wildcard Certificates
Node(s)
Generate CSR's for these Nodes:
Node
CSR Friendly Name
abtomar30
abtomar30#Multi-Use
Subject
Common Name (CN)
$FQDN$
Organizational Unit (OU)
Cisco TAC
Organization (O)
Cisco
City (L)
Bangalore
State (ST)
Karnataka
Country (C)
IN
Subject Alternative Name (SAN)
IP Address
10.106.120.87
* Key type
RSA

通配符CSR示例：



注意：每个部署节点的IP地址都可以添加到SAN字段，以避免通过IP地址访问服务器时出现证书警告。

创建CSR后，ISE将显示一个弹出窗口，其中包含导出该窗口的选项。 导出后，此文件必须发送到CA进行签名。



第二步：导入新的证书链。

证书颁发机构返回已签名的服务器证书以及完整的证书链（根/中间）。收到证书后，请执行以下步骤将证书导入到ISE服务器：

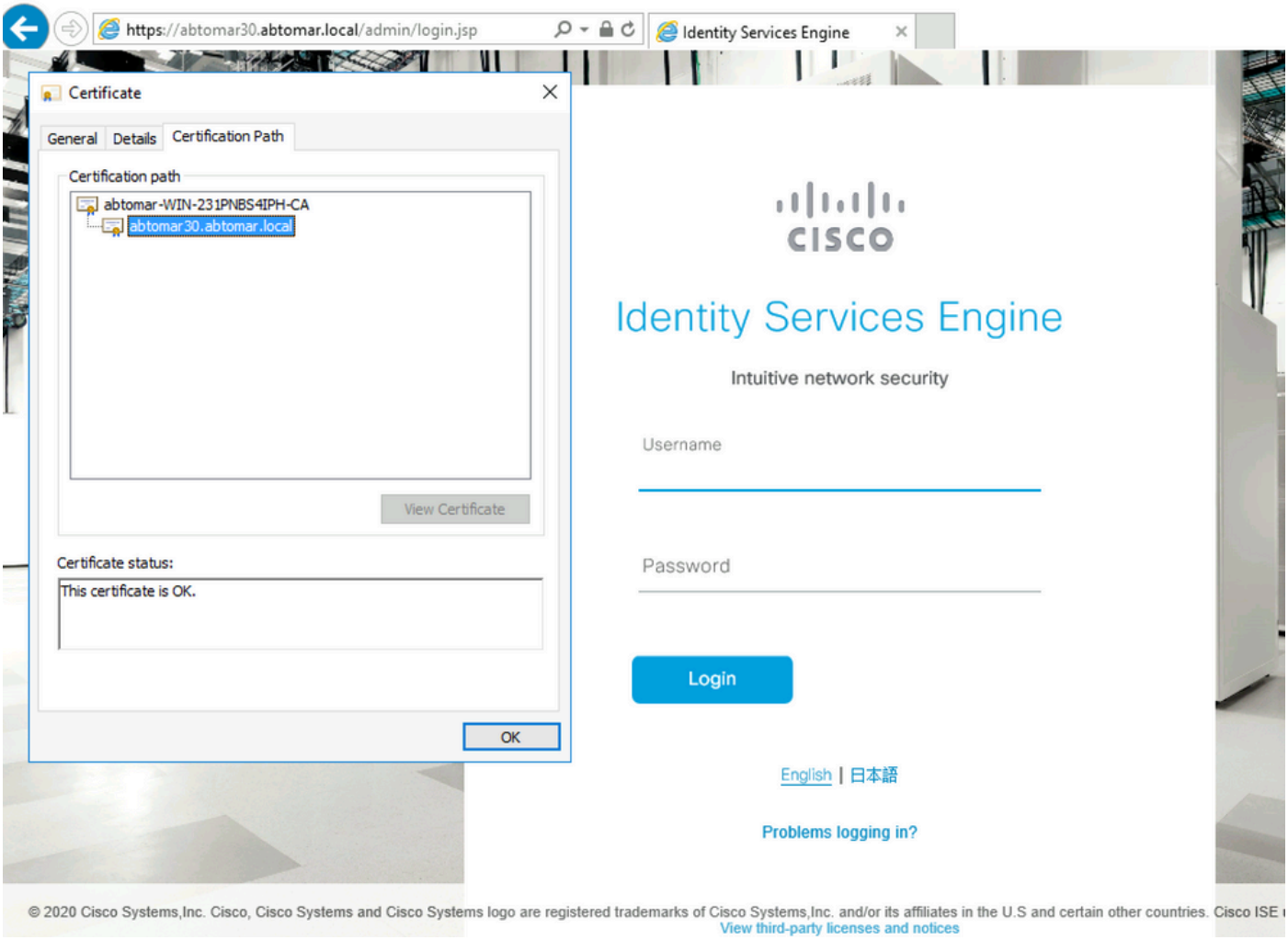
1. 要导入CA提供的任何根证书和（或）中间证书，请导航到管理>证书>受信任证书。
2. 单击Import，然后选择Root和/或Intermediate证书，并在申请提交时选择相关复选框。
3. 要导入服务器证书，请导航到管理>证书>证书签名请求。
4. 选择先前创建的CSR，然后单击Bind Certificate。
5. 选择新的证书位置，ISE将证书绑定到数据库中创建和存储的私钥。

注意：如果已为此证书选择管理员角色，则特定ISE服务器服务将重新启动。

注意：如果导入的证书适用于部署的主管理节点，并且选择了管理员角色，则所有节点上的服务会依次重新启动。这是预期结果，建议执行本练习时停机。

验证

如果在证书导入期间选择了管理员角色，则可以通过在浏览器中加载管理员页面来验证新证书是否处于适当位置。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证书。



对于其他验证，请在浏览器中选择锁定符号，并在证书路径下验证完整链是否存在，以及是否受计算机信任。这并不是服务器正确向下传递完整证书链的直接指示符，而是浏览器能够基于其本地信任存储信任服务器证书的指示符。

故障排除

在dot1x身份验证期间，请求方不信任ISE本地服务器证书

验证ISE是否在SSL握手过程中通过完整的证书链。

当使用需要服务器证书（即PEAP）的EAP方法且选择了验证服务器身份时，请求方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会提供其证书以及其链中存在的任何根证书和（或）中间证书。如果链不完整，请求方将无法验证服务器身份。要验证证书链是否传回客户端，可以执行以下步骤：

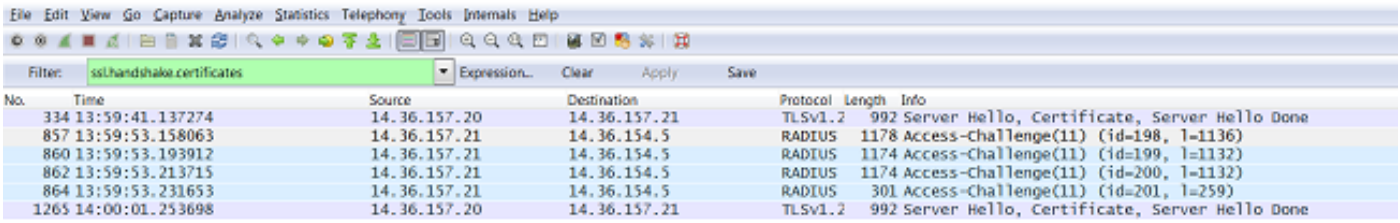
1. 要在身份验证期间从ISE(TCPDump)获取捕获，请导航到操作>诊断工具>常规工具> TCP转储。

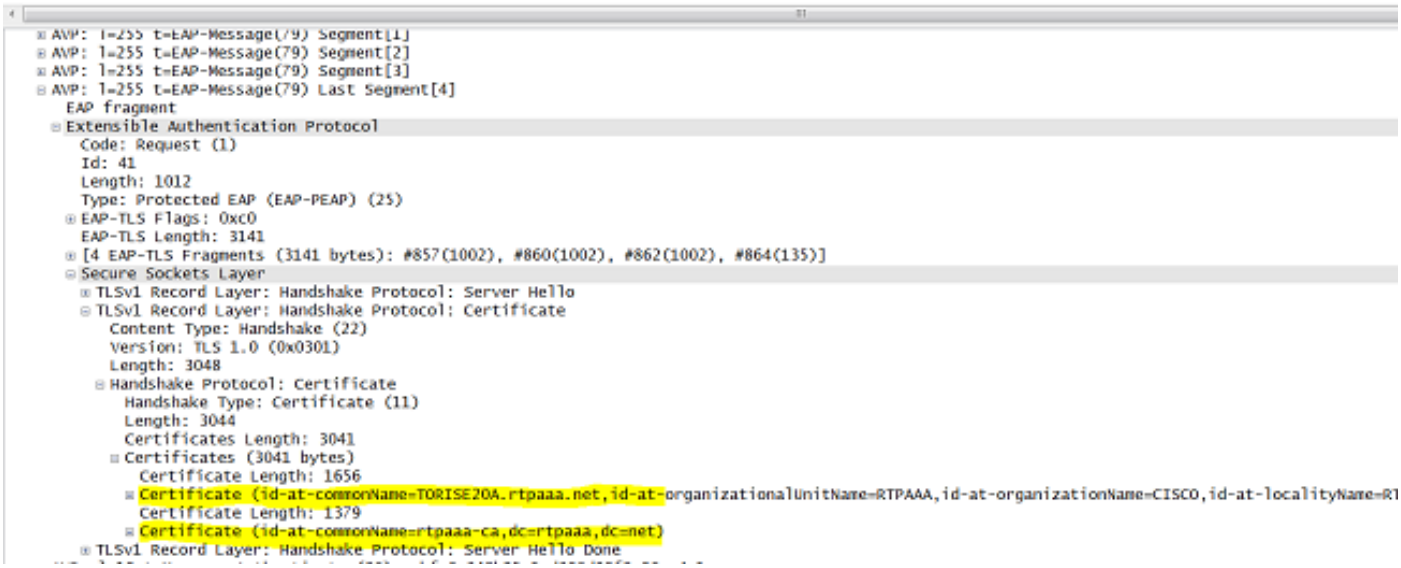
2. 下载/打开捕获并在Wireshark中应用过滤器ssl.handshake.certificates，然后查找访问质询。

3. 选中后，导航到Expand Radius Protocol > Attribute Value Pairs > EAP-Message Last

segment > Extension Authentication Protocol > Secure Sockets Layer > Certificate > Certificates。

捕获中的证书链。

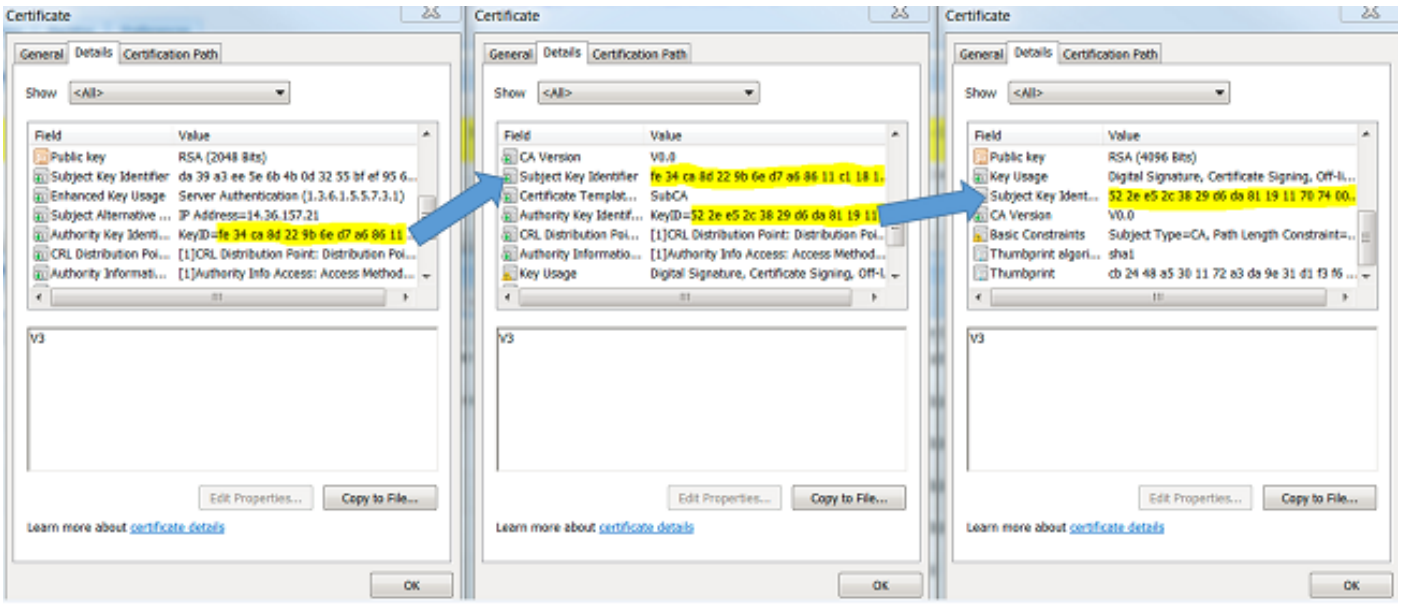




如果链不完整，请导航到ISE管理>证书>受信任证书，并验证根证书和（或）中间证书是否存在。如果证书链成功通过，则必须使用此处概述的方法来验证证书链本身是否有效。

打开每个证书（服务器、中间证书和根证书），通过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)匹配来验证信任链。

证书链示例。

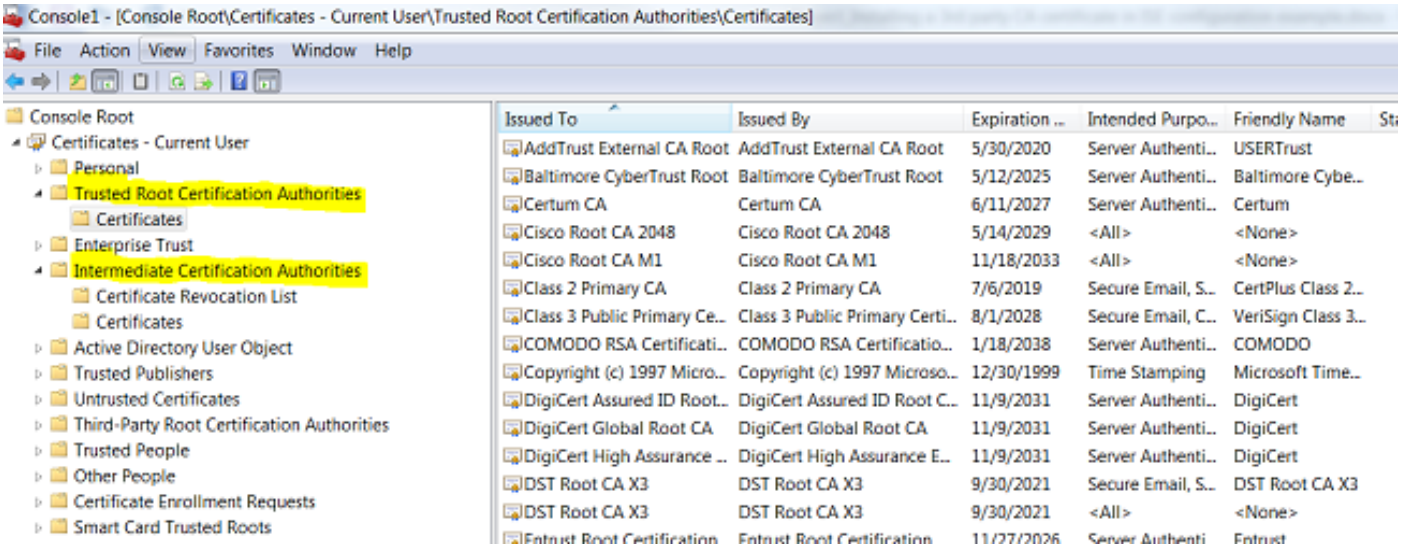


ISE证书链正确，但终端在身份验证期间拒绝ISE服务器证书

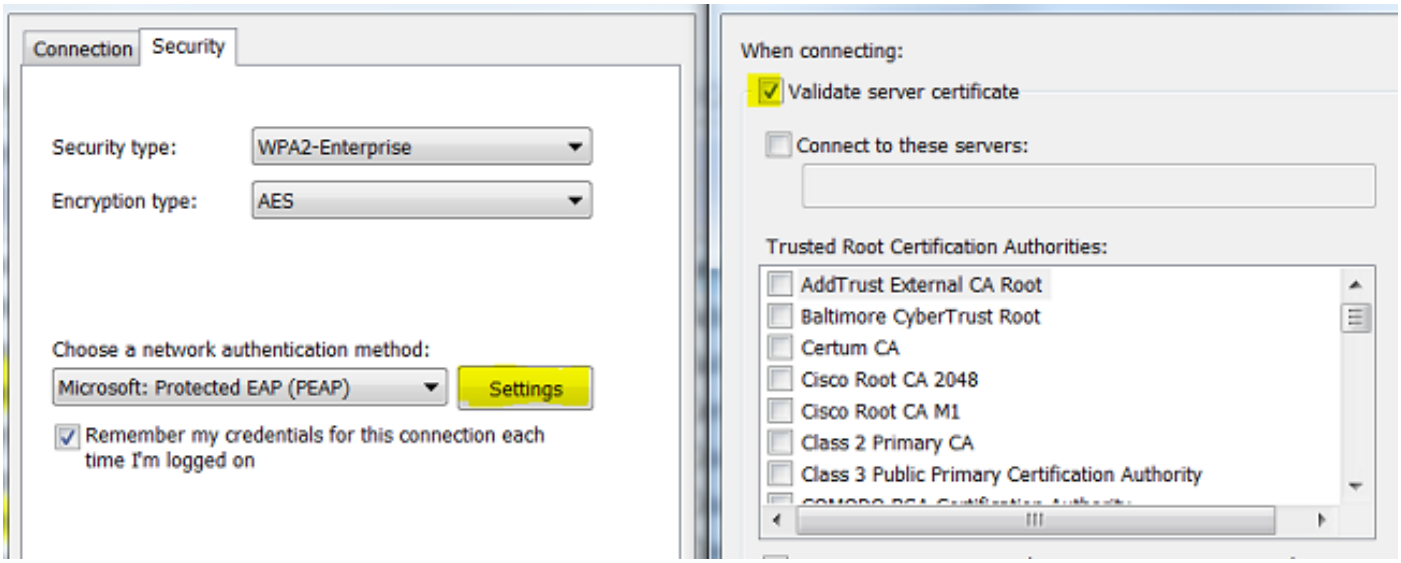
如果ISE在SSL握手期间显示其完整证书链，而请求方仍拒绝证书链；下一步是验证根证书和（或）中间证书在客户端本地信任存储中。

要从Windows设备验证这一点，请导航到mmc.exe 文件>添加 — 删除管理单元。从Available snap-ins列中选择Certificates，然后单击Add。根据使用的身份验证类型（用户或计算机）选择我的用户帐户或计算机帐户，然后单击确定。

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。



相关信息

- 思科身份服务引擎管理员指南，版本3.0
- 思科技术支持和下载

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）。