安装在ISE 2.0的第三方CA证书

目录

[简介](#)
[要求](#)
[使用的组件](#)
[配置](#)
[生成证书签名请求(CSR) ：](#)
[单个服务器证书CSR示例：](#)
[通配符CSR示例：](#)
[导入新证书一系列：](#)
[验证](#)
[故障排除](#)
[请求方不在dot1x验证时委托ISE当地服务器证书。](#)
[ISE证书链是正确，但是终端拒绝艾斯的服务器证书在验证时。](#)
[参考](#)
[相关的思科支持社区讨论](#)

简介

本文在思科身份服务引擎方面描述安装第三方CA签名证书。

不管最终证书角色(EAP验证、门户、Admin和pxGrid)，进程是相同的。

要求

基本公共钥匙结构知识。

使用的组件

本文档中的信息根据以下硬件和软件版本：

- 思科身份服务引擎(ISE)版本2.0。相同的配置适用于版本1.3和1.4。

配置

生成证书签名请求(CSR) ：

要生成CSR请去Administration >证书>证书签名请求并且选择生成Certificate Signing Requests (CSR)。

- 在使用情况部分下请选择从下拉菜单将使用的角色。如果证书将使用多个角色您能选择多用途。一旦证书生成角色可以如果需要，更改。
- 选择证书将生成的节点。
- 填好信息作为需要(组织单位、组织、城市、州和国家)。

注意：在共同名称(CN)下字段ISE自动将填充节点的完全合格的域名(FQDN)。

通配符：

- 如果目标是生成通配符证书检查“请允许通配符证书”方框。
- 如果证书将使用的EAP验证“*”符号不应该在主题CN字段，因为Windows恳求者将拒绝服务器证书。

- 既使当“请验证服务器标识”在请求方禁用， SSL握手可能发生故障，当“*时”在CN字段。
  - 反而，通用的FQDN可以用于CN字段， “*.domain.com”在附属的替代方案名称(SAN) DNS名名称字段可以然后使用。

注意： 一些证书权限(CA)可能添加通配符(*)在自动证书的CN，即使它在CSR的不是存在。在此方案中，一特殊请求将需要我做防止此操作。

单个服务器证书CSR示例：

通配符CSR示例：

注意： 当您通过IP地址，访问服务器每个部署IP Address节点的可以被添加到SAN字段避免证书警告。时。

一旦CSR创建， ISE将显示一pop窗口以选项导出它。 一旦导出，应该发送此文件到签字的CA。

导入新证书一系列：

认证机关返回与全双工签署的一系列(根/中间)一起的签字的服务器证书。一旦接收，请遵从下面步骤导入证书到您的ISE服务器。

1. 导入CA和(或)半成品证书提供的所有根通过去给Administration >证书>信任证书。
2. 通过去导入服务器证书管理>>证书>>证书签名请求。
3. 选择以前创建的CSR并且点击捆绑证书。
4. 选择新证书位置，并且ISE将绑定证书对在数据库创建和存储的专用密钥。

注意：如果Admin角色为此证书选择， ISE将重新启动服务。

验证

如果admin角色选择在证书导入期间您能验证新证书通过装载在浏览器的管理员页面是到位。 浏览器应该委托新的admin证书，只要一系列正确地被构件，并且，如果证书链由浏览器委托。

对于另外的验证请选择在浏览器的锁定符号，并且在证书路径下请验证全双工一系列是存在和委托由计算机。 这不是一台直接指示器全双工一系列由服务器，但是能的浏览器的指示器正确地通过下来委托根据其本地信任存储的服务器证书。

故障排除

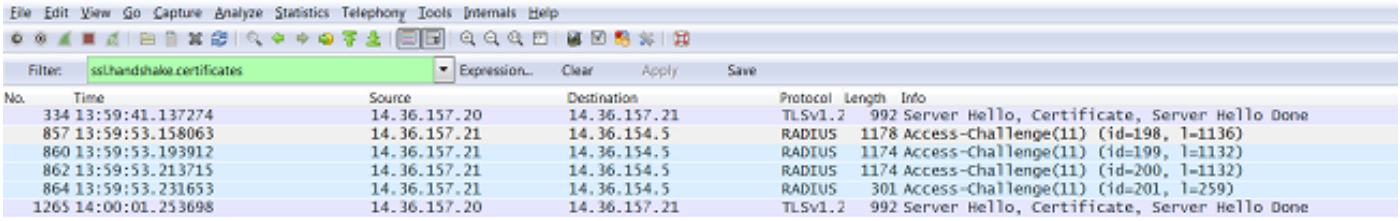
请求方不在dot1x验证时委托ISE当地服务器证书。

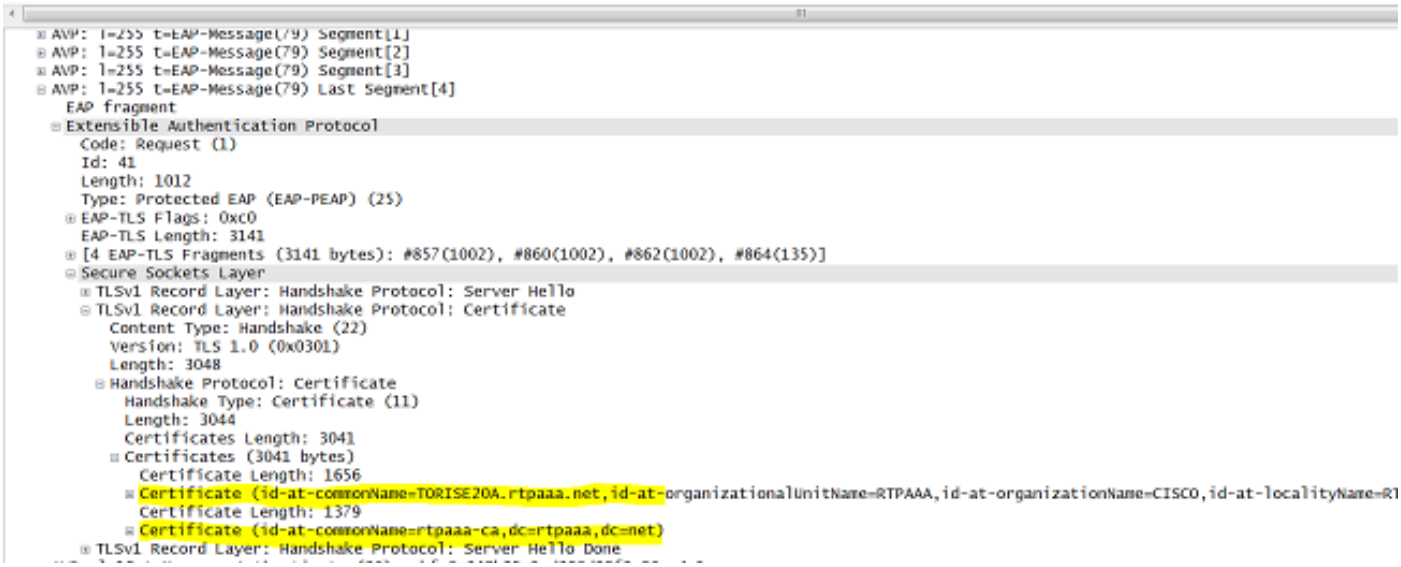
在SSL握手过程期间，验证ISE通过全双工证书链。

即当使用要求服务器证书的EAP方法(PEAP)时，并且“请验证服务器标识”选择，请求方将验证作为认证过程一部分，有在其本地信任存储的证书链使用证书。作为SSL握手过程ISE一部分将提交其证书并且其中任一根源和(或)现在半成品的证书于其一系列。 如果一系列不完整，请求方不能验证服务器标识。要验证证书链通过回到您的客户端，您可执行以下步骤：

1. 在验证时采取从ISE (Tcpdump)的一个捕获。查找在操作> Diagostic Tools>一般Tools> TCP转储下
2. 下载/打开捕获并且应用过滤器“ssl.handshake.certificates”在Wireshark并且查找访问挑战。
3. 一旦选择，请展开RADIUS协议>属性值对> EAP消息最后面几段>可扩展的认证协议>安全套接字协议层>证书>证书

捕获的证书链。

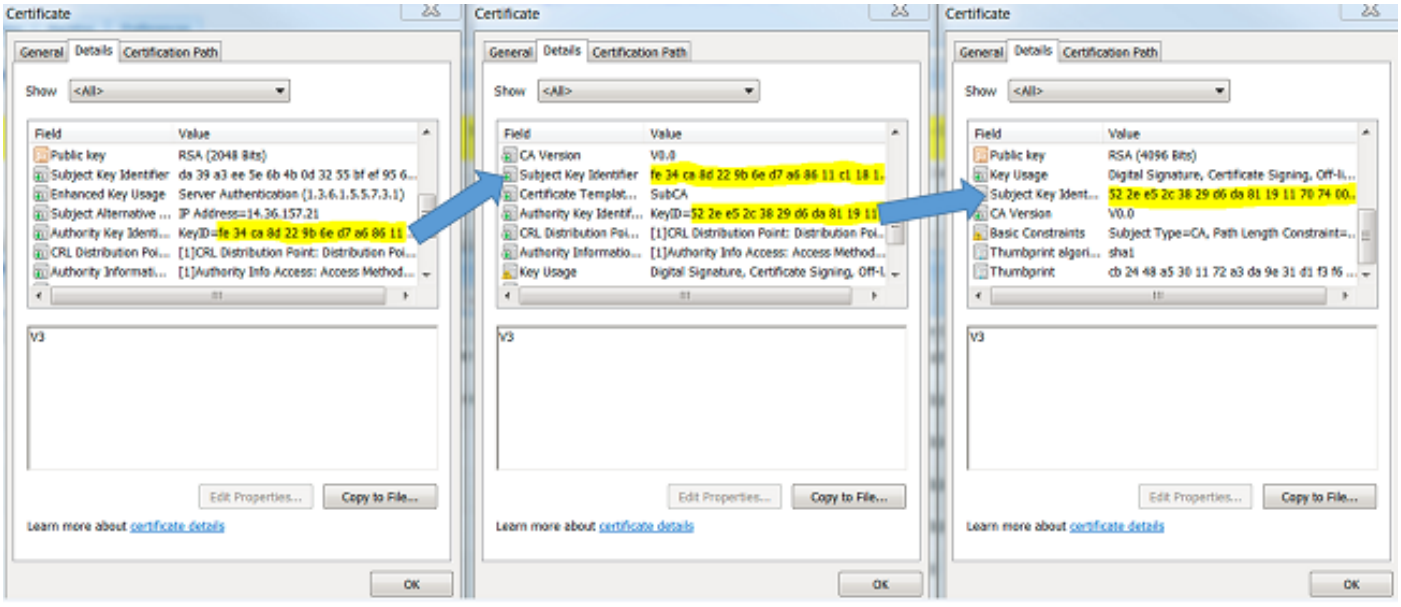




如果一系列不完成您应该去ISE Administration >证书>信任证书和验证根和(或)半成品证书存在。如果证书链顺利地通过，应该验证一系列如有效通过使用下面略述的方法。

打开每证书(服务器、中间和根)并且通过匹配附属的关键标识符验证信任一系列(滑雪)每证书到权限密钥标识符(AKI)在一系列的下证书。

证书链示例。

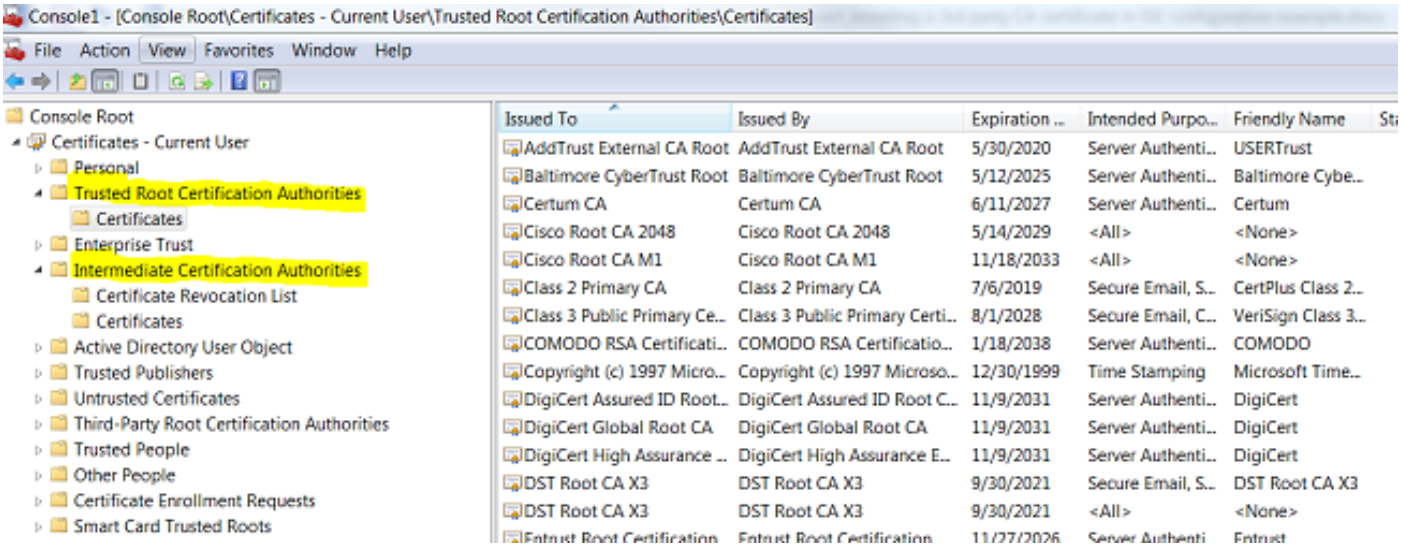


ISE证书链是正确，但是终端拒绝艾斯的服务器证书在验证时。

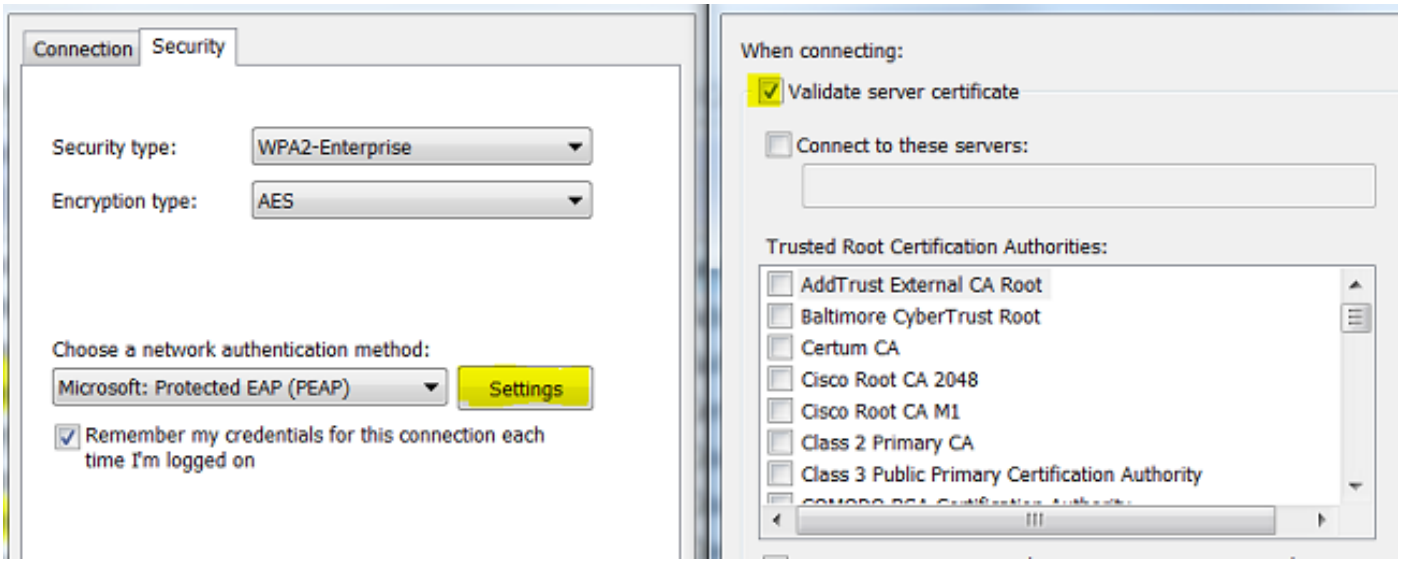
如果ISE提交其在SSL握手和请求方期间的全双工证书链仍然拒绝证书链;下一步是验证根and(or)半成品证书在客户端本地托拉斯存储。

从一Windows设备开放mmc.exe File>删除管理单元要验证此>从可用的SNAP INS列挑选证书>Add >请根据认证类型选择“我的用户帐户”或“计算机帐户”在使用中(用户或计算机)。 >好

在控制台视图下请在本地信任存储选择"Trusted Root Certification Authorities"和“半成品证书颁发机构”验证根和中间证书出现。



验证的简单的方法这是服务器标识检查问题，不选定" Validate server certificate "在请求方配置文件配置下并且再测试它。



注意：ISE当前不支持处理证书使用RSASSA-PSS作为签名算法。这包括服务器证书、根、中间或者客户端证书(即TLS、PEAP (TLS)等等)。 参考的bug CSCug22137。

参考

- 思科身份服务引擎管理员指南，版本2.0