通过CAPF在线CA配置自动证书注册和续订

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- 验证服务器时间和日期
- 更新服务器计算机名称

配置

- AD服务、用户和证书模板
  - 启用和配置Active Directory服务
  - 启用和配置证书服务
  - 为CiscoRA创建证书模板
  - 使证书模板可供颁发
  - Active Directory CiscoRA帐户创建
- IIS身份验证和SSL绑定配置
  - 启用NTLM身份验证
  - 生成Web服务器的身份证书
  - Web服务器SSL绑定
- CUCM 配置

验证

- 验证IIS证书
- 验证CUCM配置

相关链接

简介

本文档介绍通过Cisco Unified Communications Manager(CUCM)的CAPF在线功能自动注册和续订。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科统一通信管理器
- X.509 证书
- Windows 服务器
- Windows Active Directory(AD)
- Windows Internet信息服务(IIS)
- NT（新技术）LAN管理器(NTLM)身份验证

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CUCM 版本 12.5.1.10000-22
- Windows Server 2012 R2
- IP电话CP-8865/固件：SIP 12-1-1SR1-4和12-5-1SR2。

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

本文档介绍该功能的配置和相关资源，以供进一步研究之用。

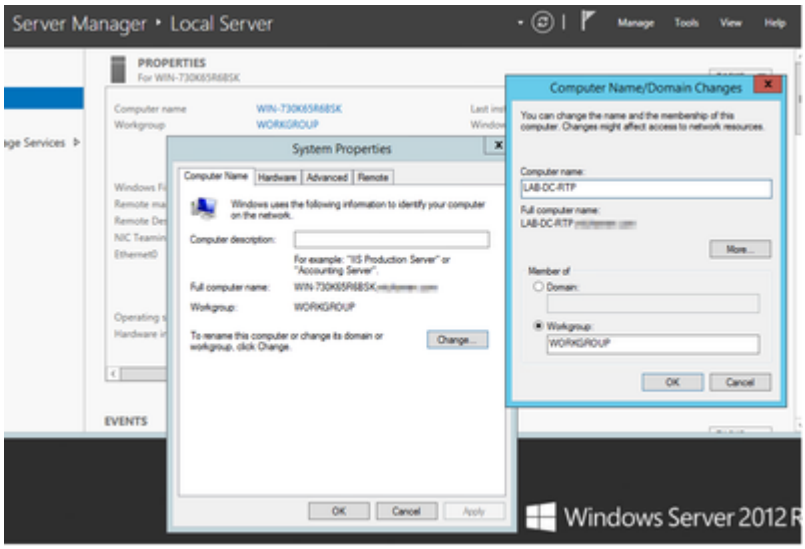
验证服务器时间和日期

确保Windows服务器配置了正确的日期、时间和时区，因为它会影响服务器根证书颁发机构(CA)证书及其颁发的证书的有效时间。

更新服务器计算机名称

默认情况下，服务器计算机名具有随机名称，例如WIN-730K65R6BSK。启用AD域服务之前需要做的第一件事是，确保在安装结束时，将服务器计算机名更新为您希望服务器主机名和根CA颁发者名称的名称；否则，在安装AD服务后，需要执行许多额外的步骤来更改此设置。

1. 导航到本地服务器，选择计算机名称以打开系统属性
2. 选择Change按钮并键入新的Computer name。



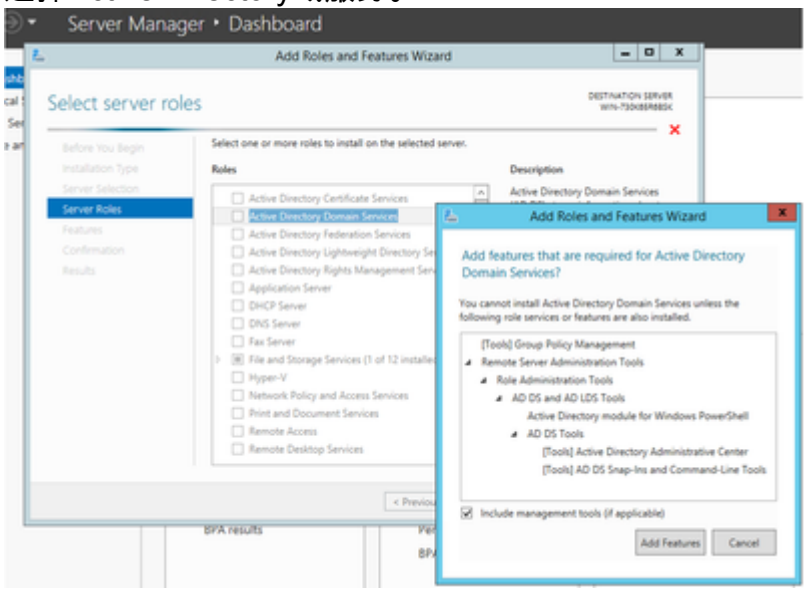
3. 重新启动服务器以应用更改。

配置

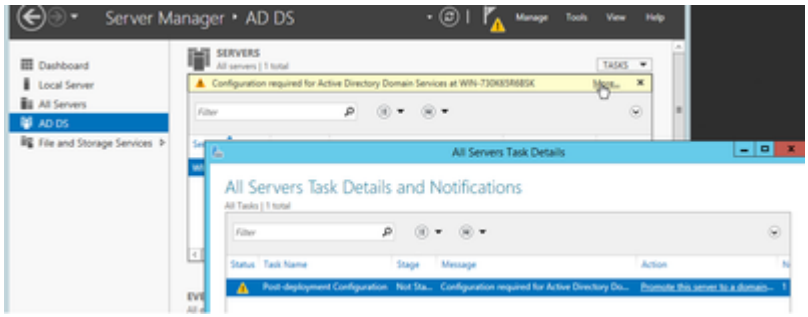
AD服务、用户和证书模板

启用和配置Active Directory服务

1. 在Server Manager中，选择Add Roles and Features，然后选择Role-based或feature-based安装。
2. 从池中选择server（池中必须只有一个服务器）。
3. 选择Active Directory域服务。

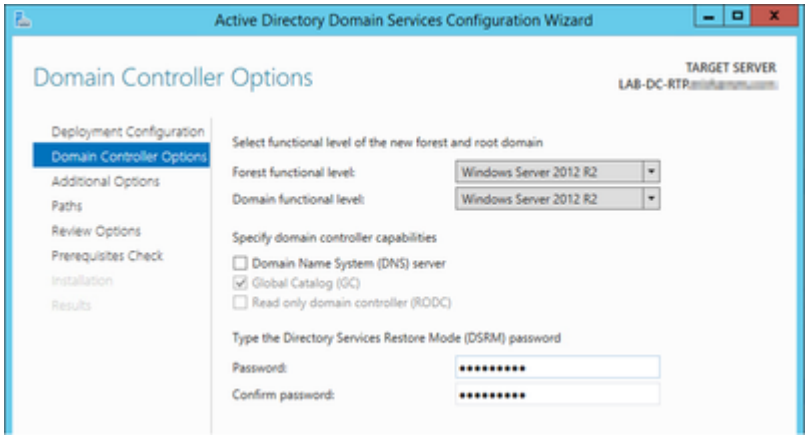


4. 继续选择Next按钮，然后选择Install。
5. 安装完成后，选择Close按钮。
6. Server Manager > AD DS下将出现一个警告选项卡，标题是Active Directory域服务所需的配置。选择more链接，然后选择available action以启动安装向导。

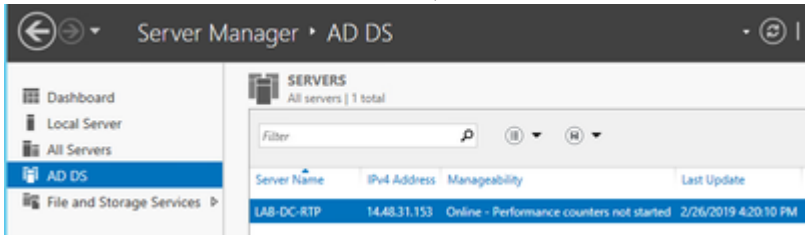


7. 完成域设置向导中的提示，使用所需的根域名添加新林，并在可用时取消选中DNS框。定义DSRM密码。



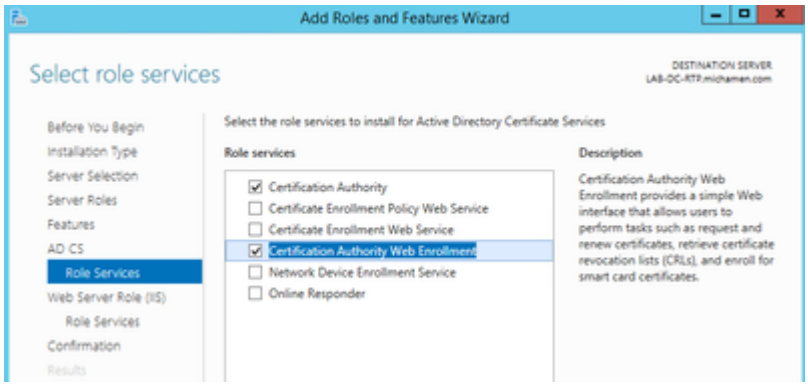


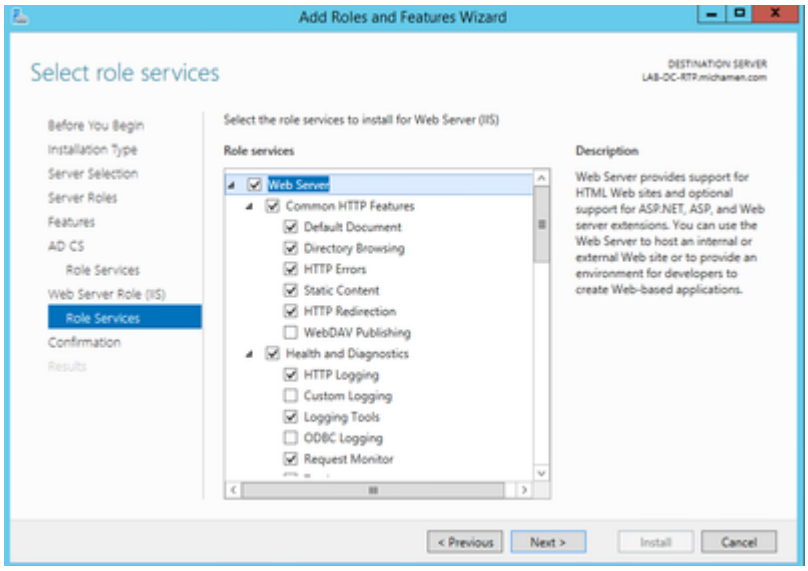
8. 指定NetBIOS域名（本实验中使用MICHAMEN1）。
9. 完成向导。然后，服务器重新启动以完成安装。
10. 下次登录时指定新域名。例如，MICHAMEN1\Administrator。



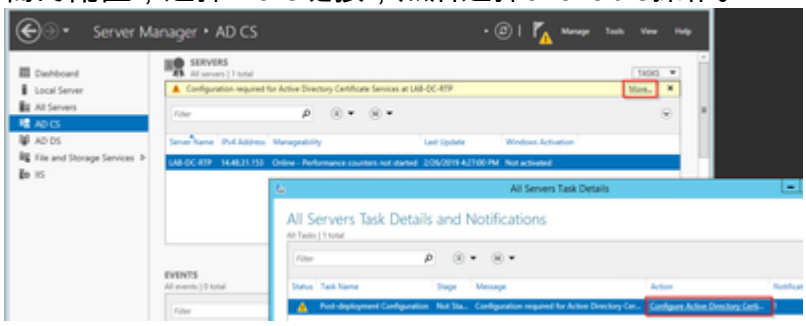
启用和配置证书服务

1. 在服务器管理器中，选择添加角色和功能。
2. 选择Active Directory Certificate Services并添加所需功能（所有可用功能均是从为此实验启用的角色服务中选择的）。
3. 对于角色服务，请检查证书颁发机构Web注册。



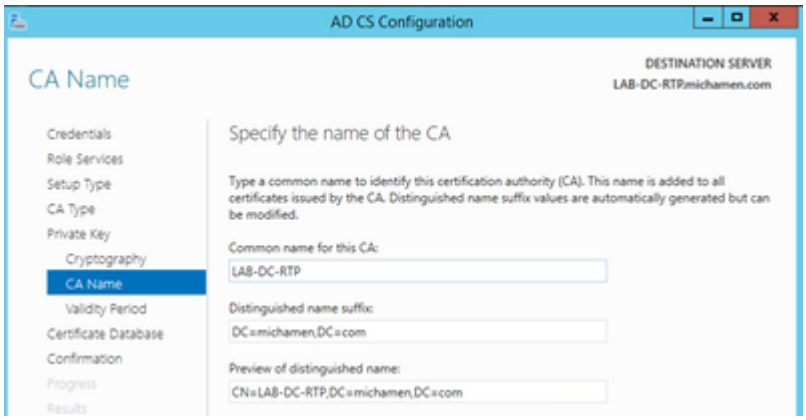


4. 在Server Manager > AD DS下必须出现一个警告选项卡，标题是Active Directory证书服务所需的配置；选择more链接，然后选择available操作。



在AD-CS安装后配置向导中完成以下步骤：

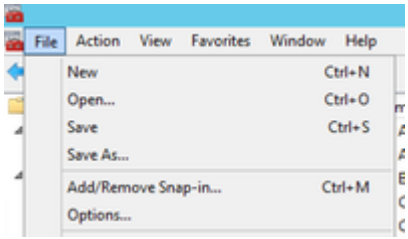
1. 选择Certification Authority和Certification Authority Web Enrollment。
2. 选择Enterprise CA及其选项：
3. 根 CA
4. 创建新私钥。
5. 使用私钥 — SHA1的默认设置。
6. 为CA设置Common Name（必须与服务器的主机名匹配）。

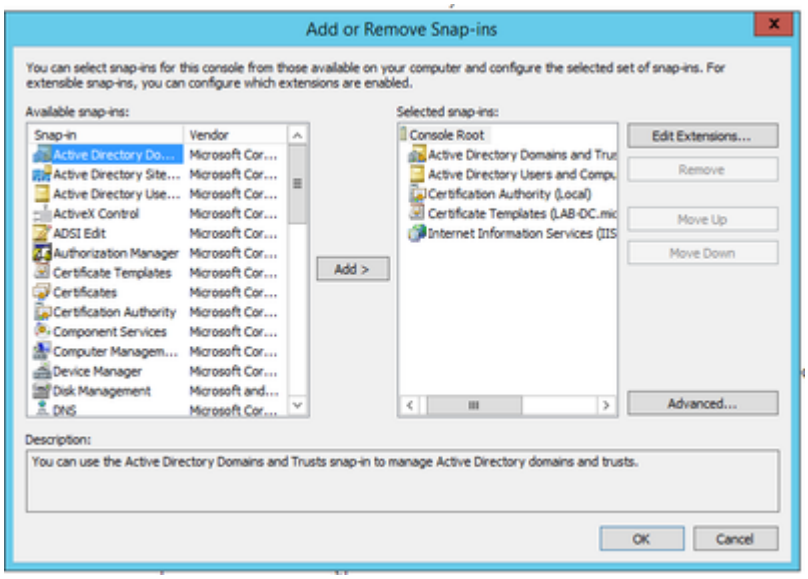


7. 将Validity设置为5年（如果需要，也可以设置更多）。
8. 通过向导的其余部分选择Next按钮。

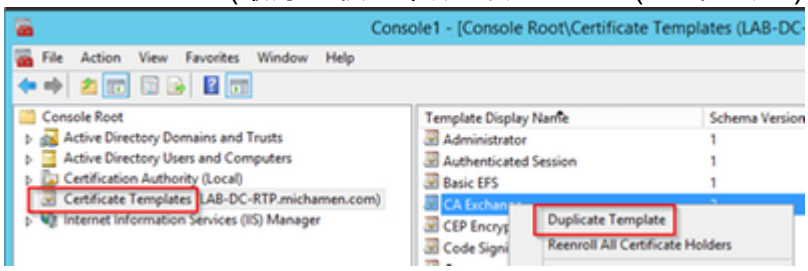
为CiscoRA创建证书模板

1. 打开MMC。选择Windows start徽标，从“运行”中键入mmc。
2. 打开MMC窗口，添加管理单元（用于配置的不同点），然后选择确定。

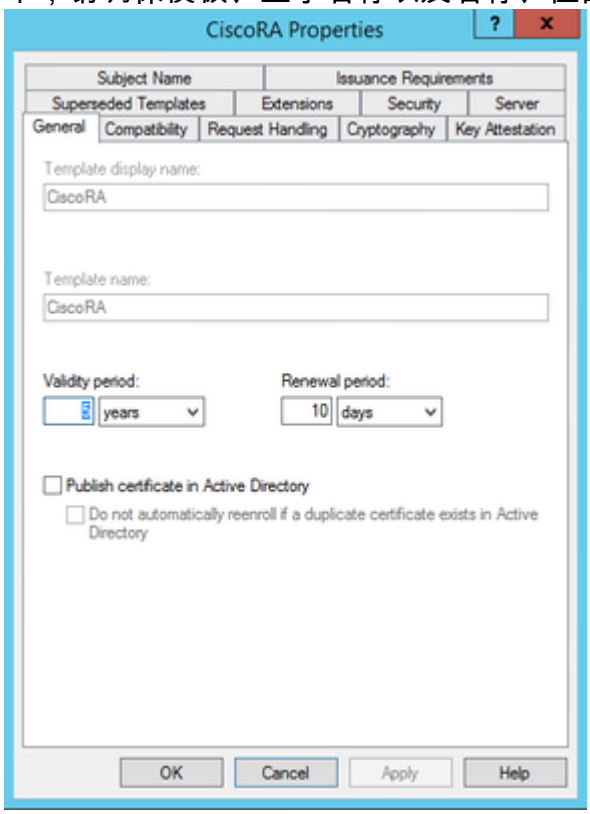




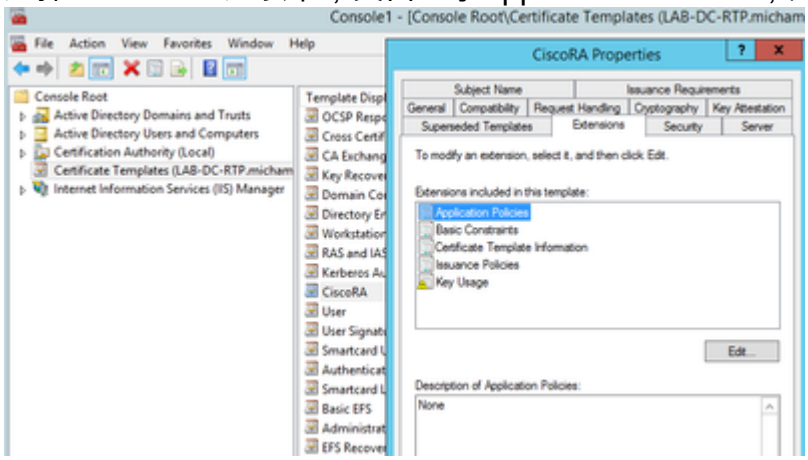
3. 选择File > Save，并将此控制台会话保存到桌面以快速重新访问。
4. 从管理单元中，选择证书模板。
5. 创建或克隆模板(最好是根证书颁发机构模板（如果可用）)，并将其命名为CiscoRA。



6. 右键单击模板并选择属性。
7. 选择General选项卡，并将有效期设置为20年（如果需要，也可以设置其他值）。 在此选项卡中，请确保模板、显示名称以及名称、值匹配。

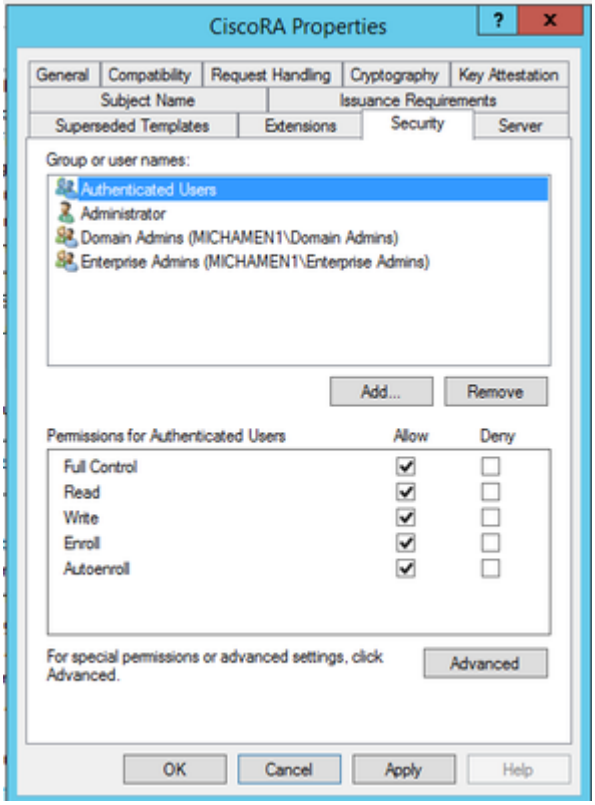


8. 选择Extensions选项卡，突出显示Application Policies，然后选择Edit。



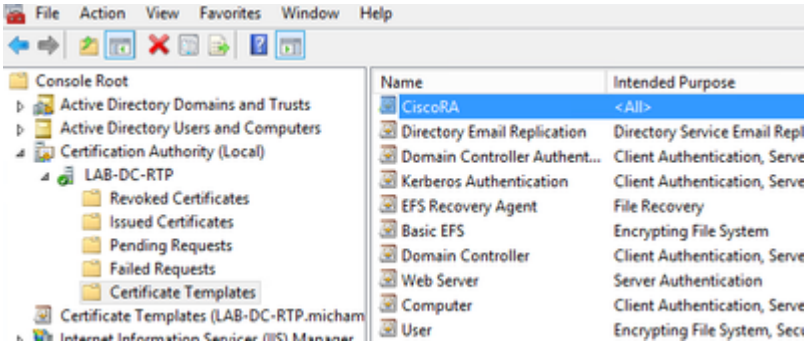
9. 删除出现的窗口中显示的所有策略。
10. 选择Subject Name选项卡，然后选择Supply in Request单选按钮。
11. 选择Security选项卡并根据您的组/用户名需要授予权限。

注意：在本示例中，为简单起见，所有用户都授予了完全权限，但这具有安全隐患。在生产环境中，只能向需要写入和注册权限的用户和组授予写入和注册权限。有关详细信息，请参阅Microsoft文档。



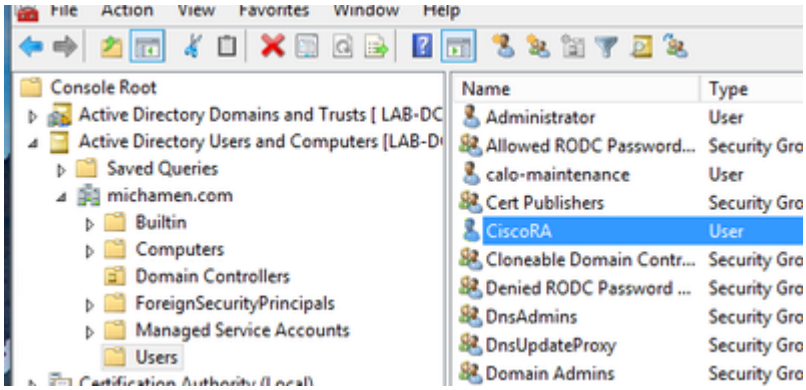
使证书模板可供颁发

1. 在MMC管理单元中，选择证书颁发机构，然后展开文件夹树以找到“证书模板”文件夹。
2. 在包含“名称”和“目标用途”的框架中的空白处单击鼠标右键。
3. 选择New和Certificate Template to Issue。
4. 选择新创建和编辑的CiscoRA模板。



Active Directory CiscoRA帐户创建

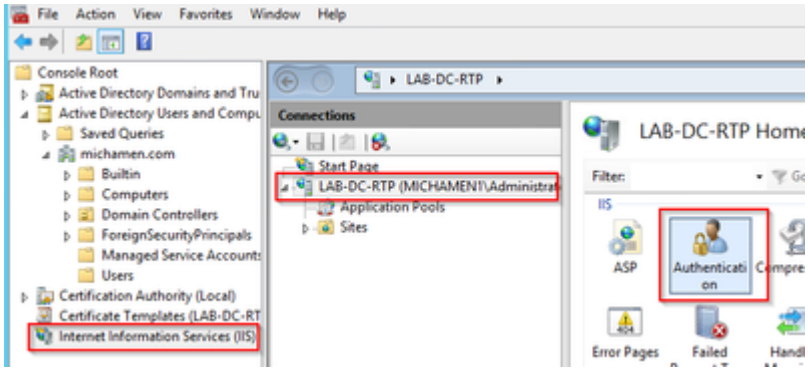
1. 导航到MMC管理单元，然后选择Active Directory用户和计算机。
2. 在最左窗格中的树中选择Users文件夹。
3. 在包含名称、类型和说明的框架中的空白处右键单击。
4. 选择New和User。
5. 使用用户名/密码创建CiscoRA帐户（本实验使用ciscora/Cisco123），并在显示时选中Password never expires复选框。



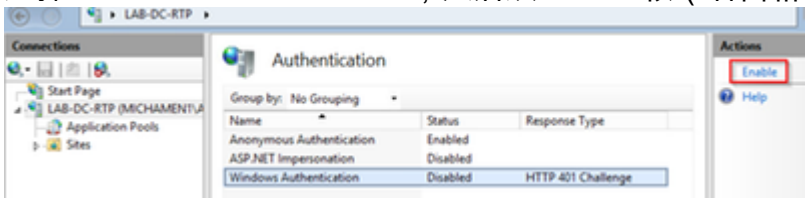
IIS身份验证和SSL绑定配置

启用NTLM身份验证

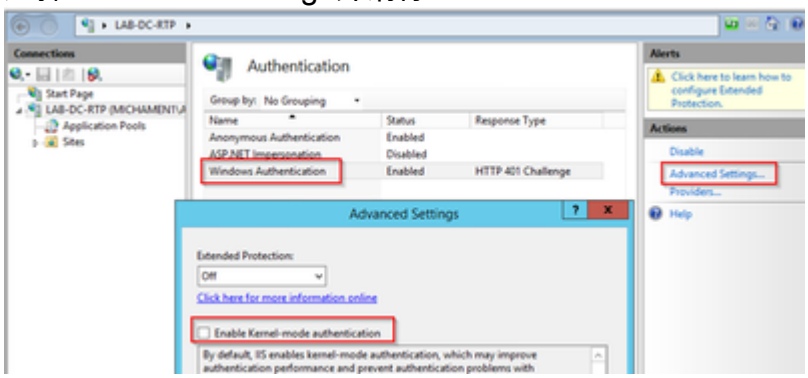
1. 导航到MMC管理单元，然后在Internet Information Services(IIS)Manager管理单元下选择服务器名称。
2. 功能列表将显示在下一帧中。双击身份验证。



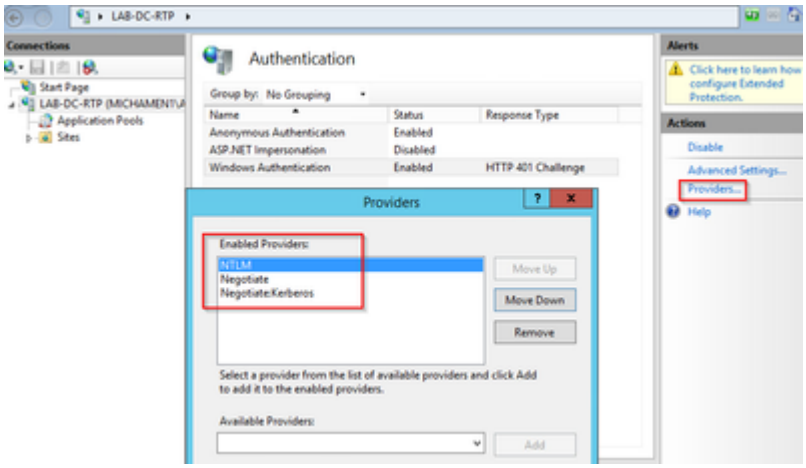
3. 选择Windows Authentication，然后从Actions帧（右窗格）中选择Enable。



4. 选择Advanced Settings并清除Enable Kernel-mode authentication复选框。



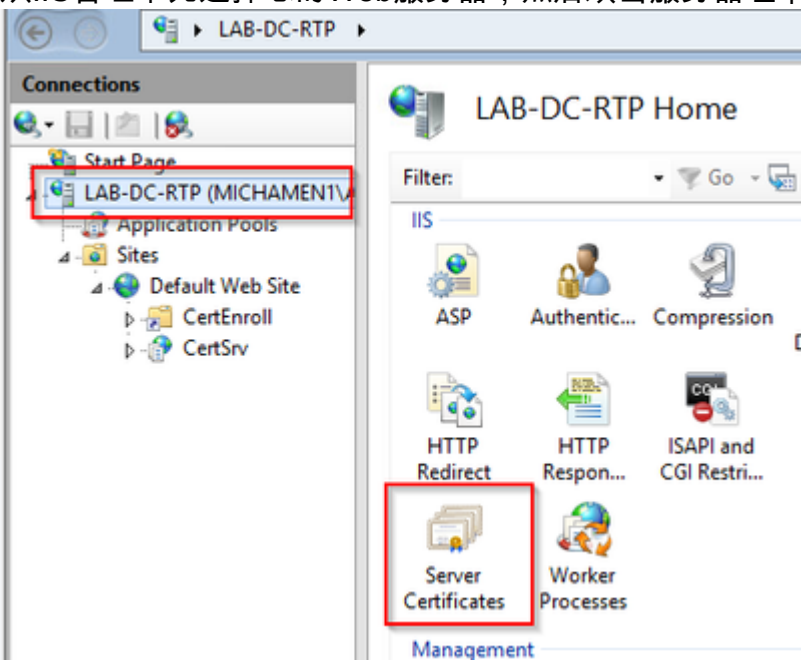
5. 选择Providers，对NTML进行排序，然后选择Negotiate。



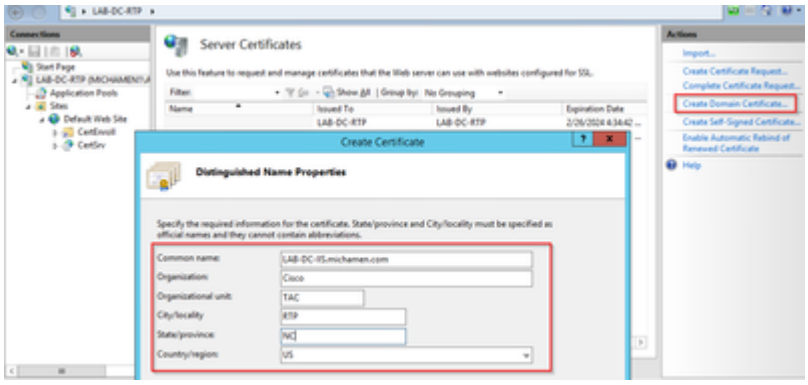
生成Web服务器的身份证书

如果尚未生成Web服务的证书和身份证书，该证书由CA签名，因为如果Web服务器证书是自签名的，CiscoRA无法连接到该证书。

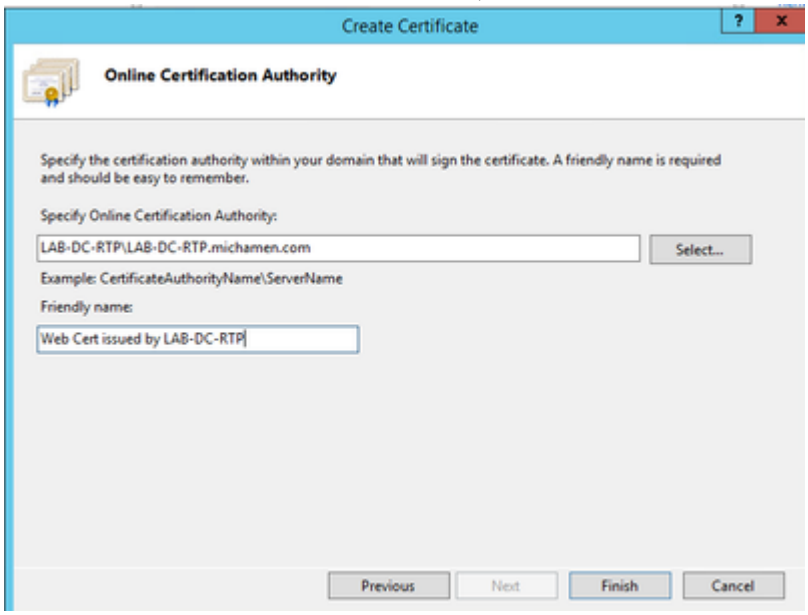
1. 从IIS管理单元选择您的Web服务器，然后双击服务器证书。



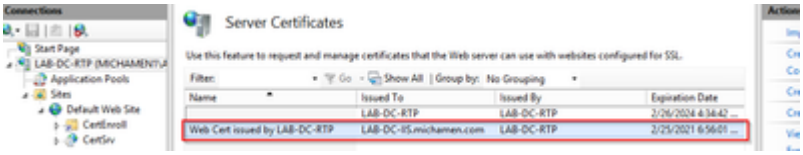
2. 默认情况下，此处列出一个证书，即自签根CA证书。从操作菜单中，选择创建域证书。在配置向导中输入值以创建新证书。确保公用名是可解析的完全限定域名(FQDN)，然后选择下一步。



3. 选择您的根CA的证书作为颁发者，然后选择完成。

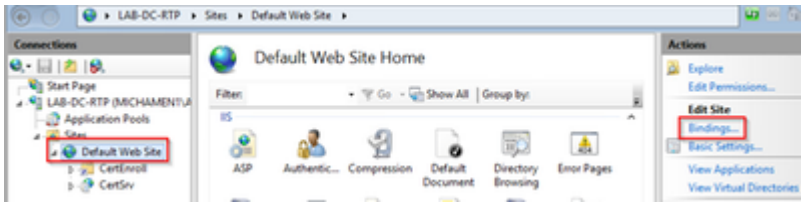


CA证书和Web服务器身份证书都会列出。

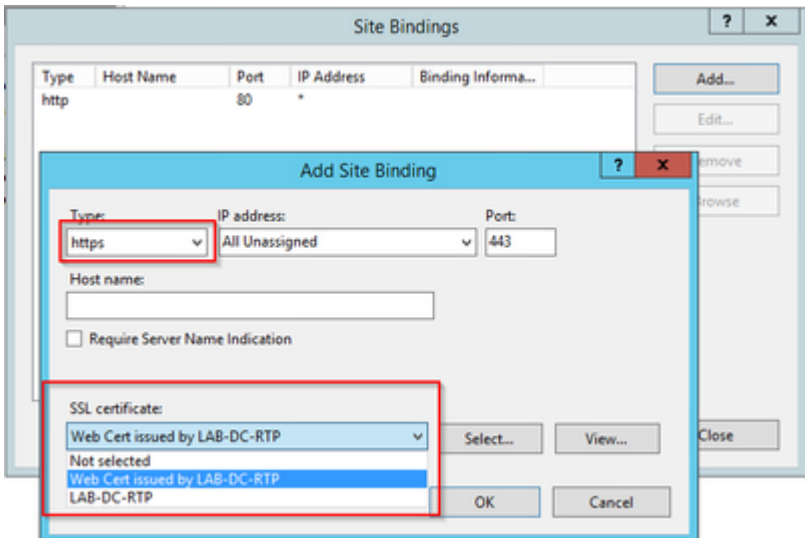


Web服务器SSL绑定

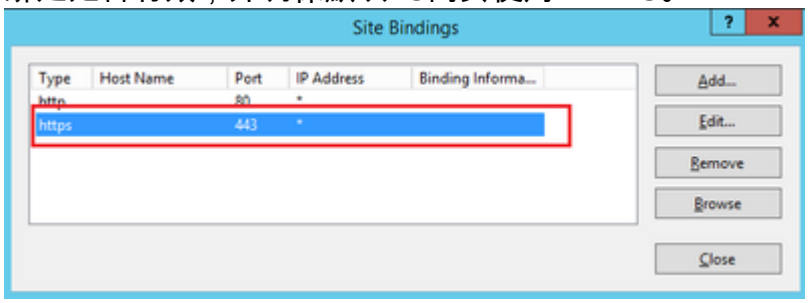
1. 在树视图中选择一个站点（您可以使用默认网站或使其更精细到特定站点），然后从操作窗格中选择绑定。此时将显示绑定编辑器，通过该编辑器可以创建、编辑和删除网站的绑定。选择Add以将新的SSL绑定添加到站点。

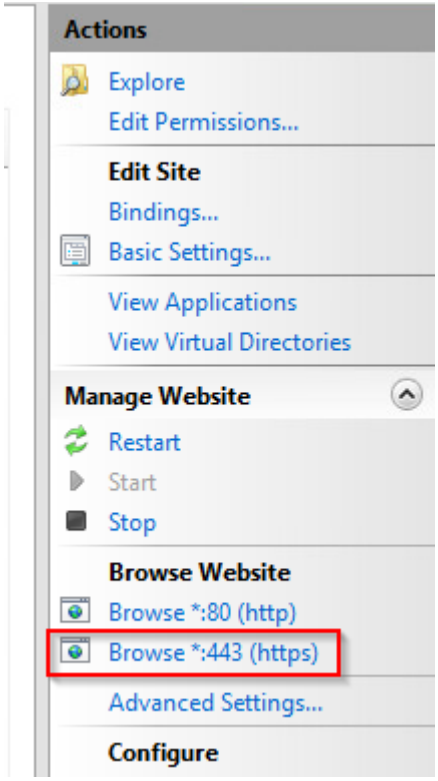


2. 新绑定的默认设置为端口80上的HTTP。对于类型，请选择https。从SSL Certificate下拉列表中选择在上一节中创建的自签名证书，然后单击OK。



3. 现在，您的站点上有新的SSL绑定，剩下的就是从菜单中选择Browse *:443(https)选项验证该绑定是否有效，并确保默认IIS网页使用HTTPS。

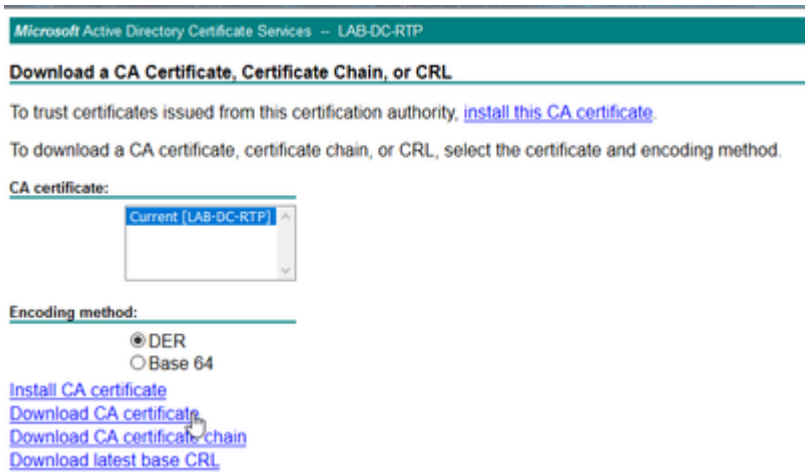




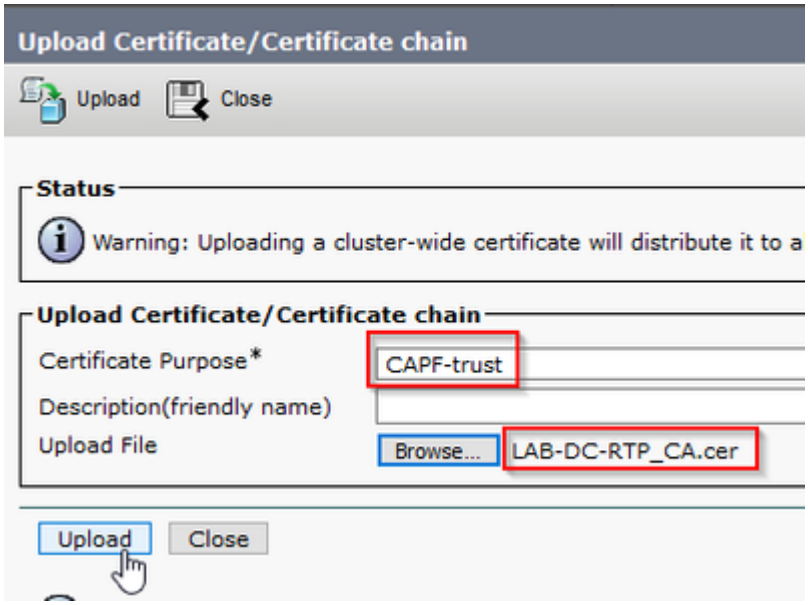
4. 请记得在配置更改后重新启动IIS服务。使用操作窗格中的重新启动选项。

CUCM 配置

1. 导航到AD CS网页(https://YOUR_SERVER_FQDN/certsrv/)并下载CA证书。

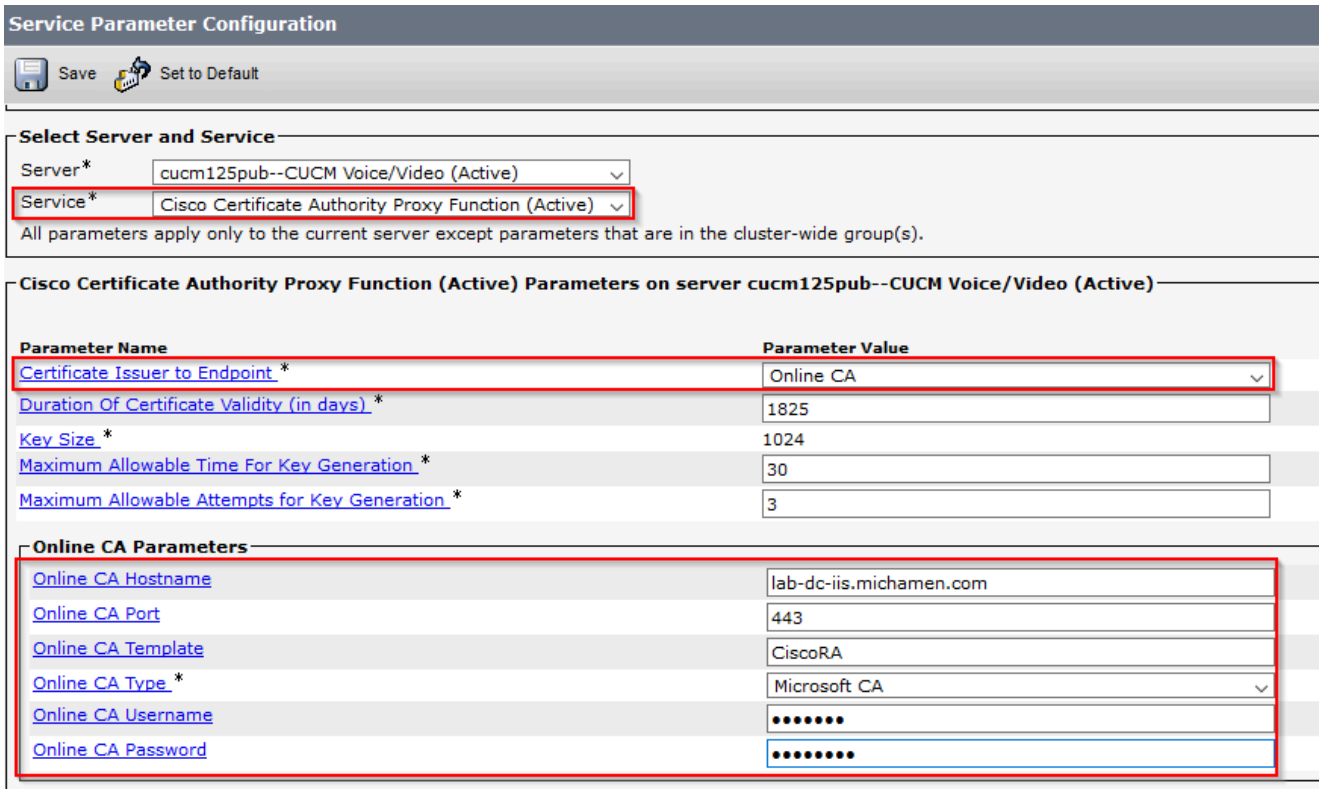


2. 从OS Administration页导航到Security > Certificate Management，然后选择Upload Certificate/Certificate chain按钮以上传目的设置为CAPF-trust的CA证书。

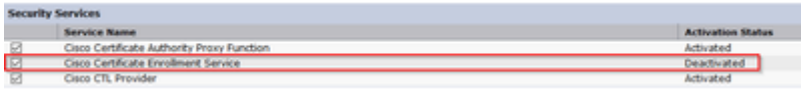


上传与CallManager-trust相同的CA证书，因为如果终端启用了安全信令加密（如果集群处于混合模式，则很可能如此），则需要该证书。

3. 导航到系统>服务参数。在server字段中选择Unified CM Publisher服务器，在Service字段中选择Cisco Certificate Authority Proxy Function。
4. 将Certificate Issuer的值设置为Endpoint to Online CA，并输入Online CA Parameters字段的值。确保使用Web服务器FQDN、之前创建的证书模板的名称(CiscoRA)、作为Microsoft CA的CA类型以及使用之前创建的CiscoRA用户帐户的凭据。



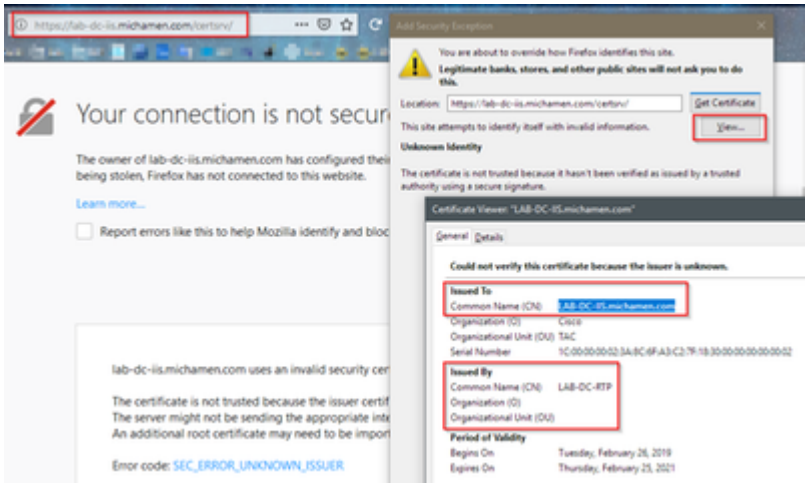
5. 弹出窗口通知您需要重新启动CAPF服务。首先，通过Cisco Unified Serviceability > Tools > Service Activation激活Cisco Certificate Enrollment Service，在server字段中选择Publisher，选中Cisco Certificate Enrollment Service复选框，然后选择Save按钮。



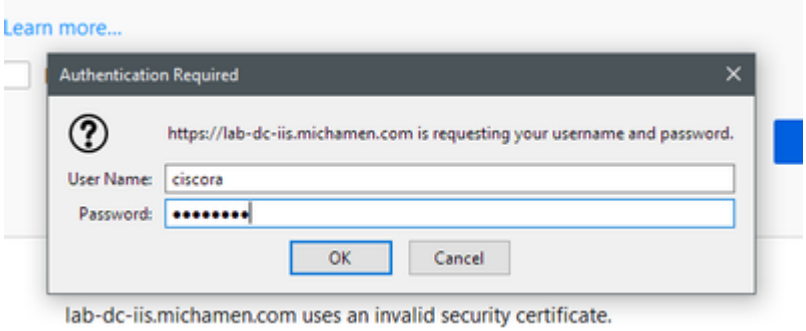
验证

验证IIS证书

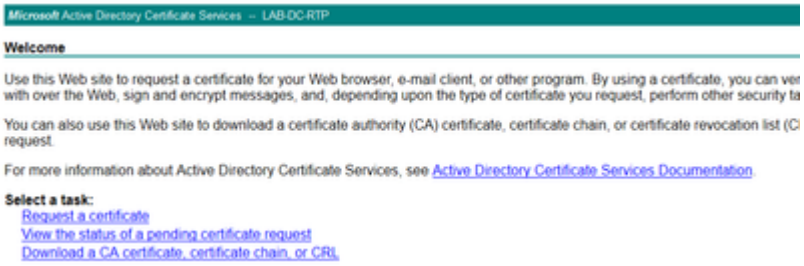
1. 从连接到服务器的PC的Web浏览器（最好与CUCM发布服务器位于同一网络）中，导航到您的服务器FQDN(https://YOUR_SERVER_FQDN/certsrv/)。
2. 显示证书不受信任警报。添加例外并检查证书。确保它与预期的FQDN匹配。



3. 接受例外后，需要authenticate;此时，您需要使用之前为CiscoRA帐户配置的凭证。



4. 身份验证后，您必须能够看到AD CS（Active Directory证书服务）欢迎页面。



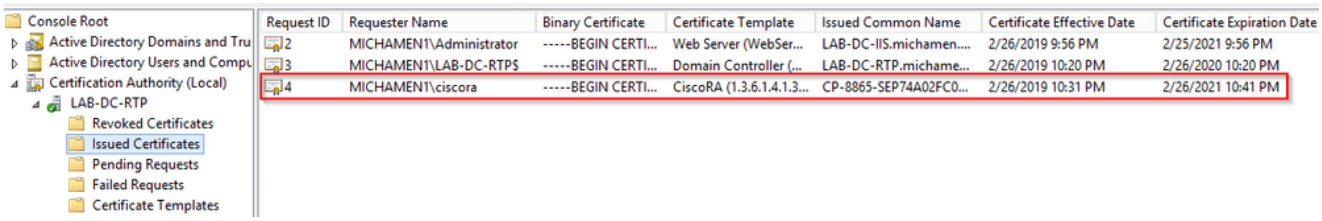
验证CUCM配置

执行以下步骤在其中一个电话上安装LSC证书。

1. 打开CallManager Administration页，依次打开Device和Phone。
2. 选择Find按钮以显示电话。
3. 选择要安装LSC的电话。
4. 向下滚动到证书颁发机构代理功能(CAPF)信息。
5. 从Certificate Operation中选择Install/Upgrade。
6. 选择Authentication Mode。（By Null String可用于测试目的。）
7. 滚动到页面顶部，为电话选择save，然后选择Apply Config。
8. 电话重新启动并注册回后，使用LSC Status过滤器确认已成功安装LSC。

并继续：

1. 从AD服务器端，打开MMC并展开证书颁发机构管理单元以选择已颁发的证书文件夹。
2. 电话条目显示在摘要视图内，包括以下详细信息：
   - 请求 ID:唯一序列号
   - 请求者名称：必须显示已配置的CiscoRA帐户的用户名。
   - 证书模板:必须显示所创建的CiscoRA模板的名称。
   - 已颁发的公用名：必须显示附加设备名称的电话型号。
   - 证书生效日期和证书到期日期



相关链接

- CAPF在线CA故障排除
- 技术支持和文档

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）。