配置ISE BYOD的SCEP支持

目录

简介

本文描述使用为了成功配置Microsoft网络设备登记服务的步骤(NDES)，并且Bring的简单认证登记协议(SCEP)您自己的设备(BYOD)在思科识别服务引擎(ISE)。

先决条件

要求

Cisco 建议您了解以下主题：

- ISE版本1.1.1或以上
- MS Windows服务器2008个R2
- MS Windows服务器2012英文虎报

- 公共密钥基础设施(PKI)和证书

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ISE版本1.1.1或以上
- 与KB2483564和KB2633200安装的ICM Hotfixes的Windows服务器2008 R2 SP1
- Windows服务器2012英文虎报

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。 如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关的信息对Microsoft证书服务特别地提供作为指南为思科BYOD。参考Microsoft TechNet作为真相明确来源Microsoft证书颁发机构、网络设备登记服务(NDES)和SCEP相关服务器配置的。

背景信息

其中一个思科ISE启用的BYOD实施的好处是最终用户的能力执行自助设备已注册。这排除对此的管理负担为了分配认证证书和启用在网络的设备。在BYOD中心解决方案是网络请求方提供的流程，寻求分配必须证书到员工拥有的设备。 为了满足此要求，微软认证授权(CA)可以配置为了自动化与SCEP的证书登记进程。

SCEP多年来用于在虚拟专用网络(VPN)环境为了实现证书登记和分配到远程访问客户端和路由器。SCEP功能的启动在Windows 2008 R2服务器的要求NDES的安装。在NDES角色期间安装，Microsoft互联网信息服务(IIS) Web服务器也安装。IIS用于为了终止HTTP或HTTPS SCEP注册请求和答复在CA和ISE策略之间节点。

NDES角色在当前CA可以安装，或者在成员服务器可以安装。在一独立部署，包括证书颁发机构服务，并且，或者，证书颁发机构Web登记服务的NDES服务在现有CA安装。在一分布式部署，NDES服务在成员服务器安装。分布式NDES服务器然后配置为了与一上行根或SUB根CA联络。 在此方案中，在本文略述的注册修改在NDES服务器被做用自定义模板，证书在上行CA驻留。

测试的CA/NDES部署方案

此部分提供在思科实验室测试了CA/NDES部署方案的简要概述。参考Microsoft TechNet作为真相明确来源Microsoft CA、NDES和SCEP相关服务器配置的。

独立部署

当ISE用于概念证明(PoC)时方案，作为激活目录(AD)域控制器、根CA和NDES服务器的是普通部署一独立性的Windows 2008年或2012计算机：

- Domain Controller
- AD
- Root CA
- NDES

分布式部署

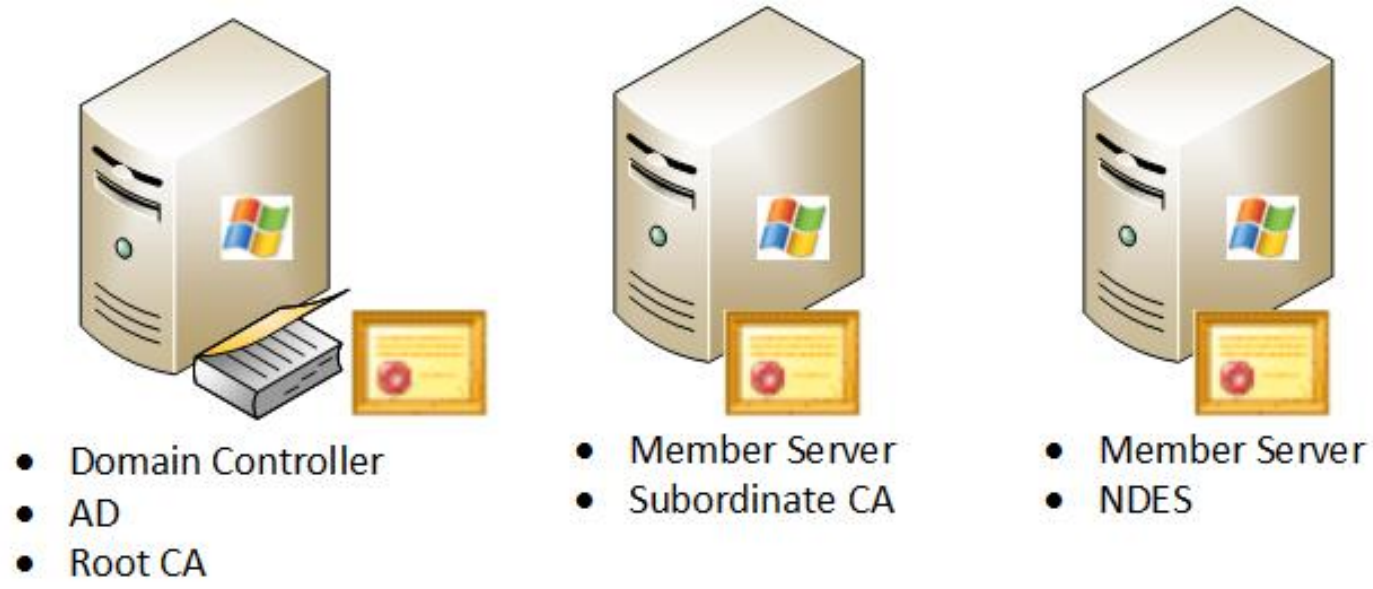
当ISE集成到一个当前Microsoft AD/PKI生产环境时，是更加普通发现在多个，明显的Windows 2008年或2012服务器间被分配的服务。思科为分布式部署测试了两个方案。

此镜像说明分布式部署的第一个测试方案：

- Domain Controller
- AD
- Root CA

- Member Server
- Subordinate CA
- NDES

此镜像说明分布式部署的第二个测试方案：



重要Microsoft ICM Hotfixes

在您配置BYOD的前SCEP支持，请保证Windows 2008 R2 NDES服务器有安装的这些Microsoft ICM Hotfixes ：

- SCEP证书的续订请求失效Windows服务器2008 R2，如果证书被管理通过使用NDES -此问题出现，因为NDES不支持**GetCACaps**操作。
- NDES不提交证书请求，在企业CA在Windows服务器2008 R2重新启动-后此消息在**事件查看器**出现：“*网络设备登记服务不能提交证书请求(0x800706ba)。RPC服务器不可用*”。

  警告：当您配置Microsoft CA时，请注意ISE不支持RSASSA-PSS签名算法。思科建议您配置CA策略，以便使用sha1WithRSAEncryption或sha256WithRSAEncryption。

重要BYOD端口&协议

这是重要BYOD端口和协议列表：

- TCP ：8909设置：从思科ISE的向导安装(Windows和麦金塔操作系统(OS))
- TCP ：443设置：从谷歌作用的向导安装(机器人)
- TCP ：8905设置：请求方提供的流程
- TCP ：80或TCP ：443 CA的SCEP代理(根据SCEP RA URL配置)

  注意：对于需要的端口和协议最新的列表，参考ISE 1.2硬件安装指南。

配置

请使用此部分为了配置BYOD的NDES和SCEP支持在ISE。

禁用SCEP登记私钥保护密码需求

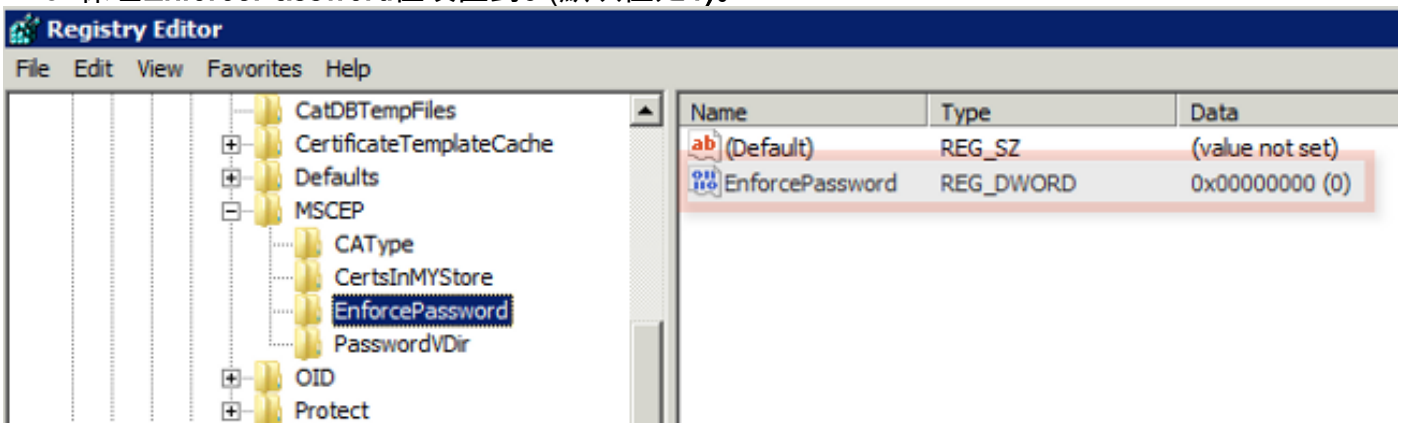
默认情况下， Microsoft SCEP (MSCEP)实施使用一动态私钥保护密码为了验证客户端和终端在证书登记进程中。使用到位此配置要求，您必须浏览到在NDES服务器的MSCEP admin Web GUI为了生成密码根据要求。作为注册请求一部分，您必须包括此密码。

在BYOD部署，私钥保护密码的需求阻挠目的对于用户自助解决方案。为了去除此需求，您必须修改在NDES服务器的此注册表项：

1. 点击**开始**并且登录**regedit**在搜索柱状图。

2. 导航对**计算机> HKEY_LOCAL_MACHINE>SOFTWARE> Microsoft >加密算法> MSCEP > EnforcePassword**。

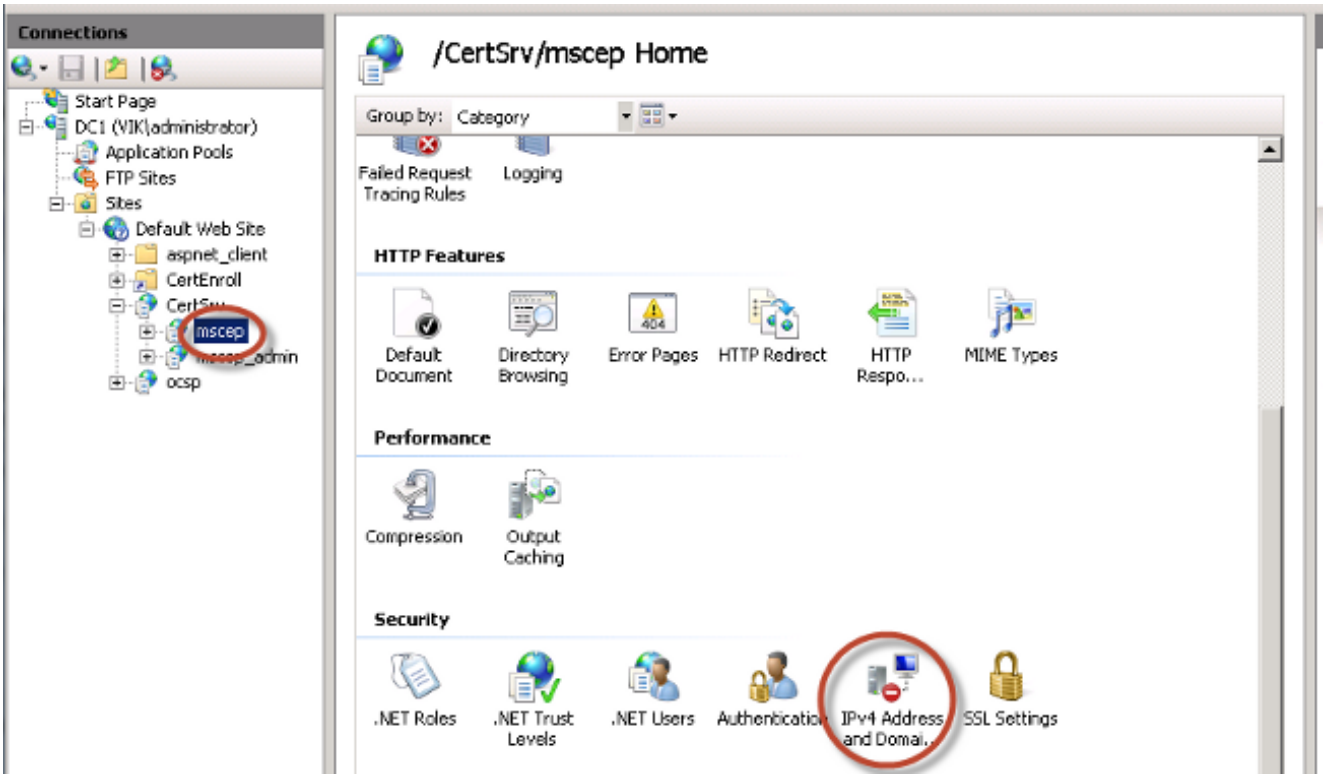
3. 保证**EnforcePassword**值设置到**0** (默认值是**1**)。



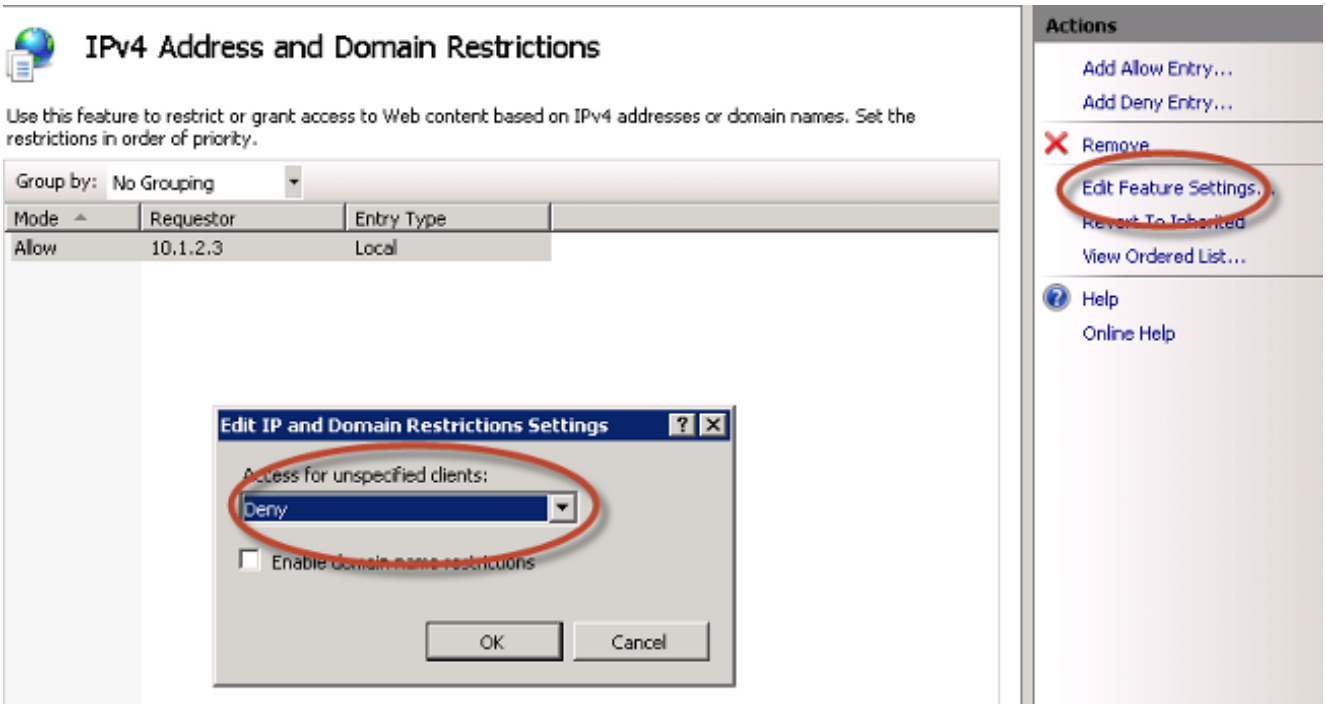
限制SCEP登记对已知ISE节点

在一些部署方案中，也许更喜欢限制SCEP通信到已知ISE节点一挑选列表。这可以用IPv4地址和域限制功能完成在IIS ：

1. 打开IIS并且导航到**/CertSrv/mscep**网站。



2. 双击**安全> IPv4地址和域限制。** 请使用**添加允许条目**并且**添加拒绝条目**操作为了允许或限制对根据ISE节点IPv4地址或域名的Web内容的访问。请使用**编辑功能设置**操作为了定义未指明的客户端的默认访问规则。

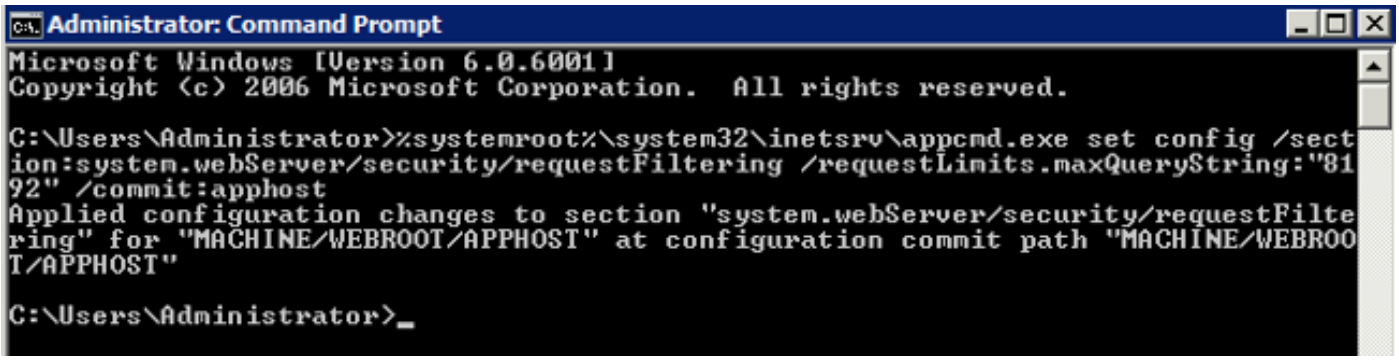


扩大在IIS的URL长度

生成为IIS Web服务器是太长的URL ISE是可能的。为了避免此问题，可以修改默认IIS配置允许更加长的URL。输入从NDES服务器CLI的此命令：

```
%systemroot%\system32\inetsrv\appcmd.exe set config /section:system.webServer/
 security/requestFiltering /requestLimits.maxQueryString:"8192" /commit:apphost
```

注意：查询串大小也许变化从属在ISE和终端配置。输入从NDES服务器CLI的此命令与管理权限。



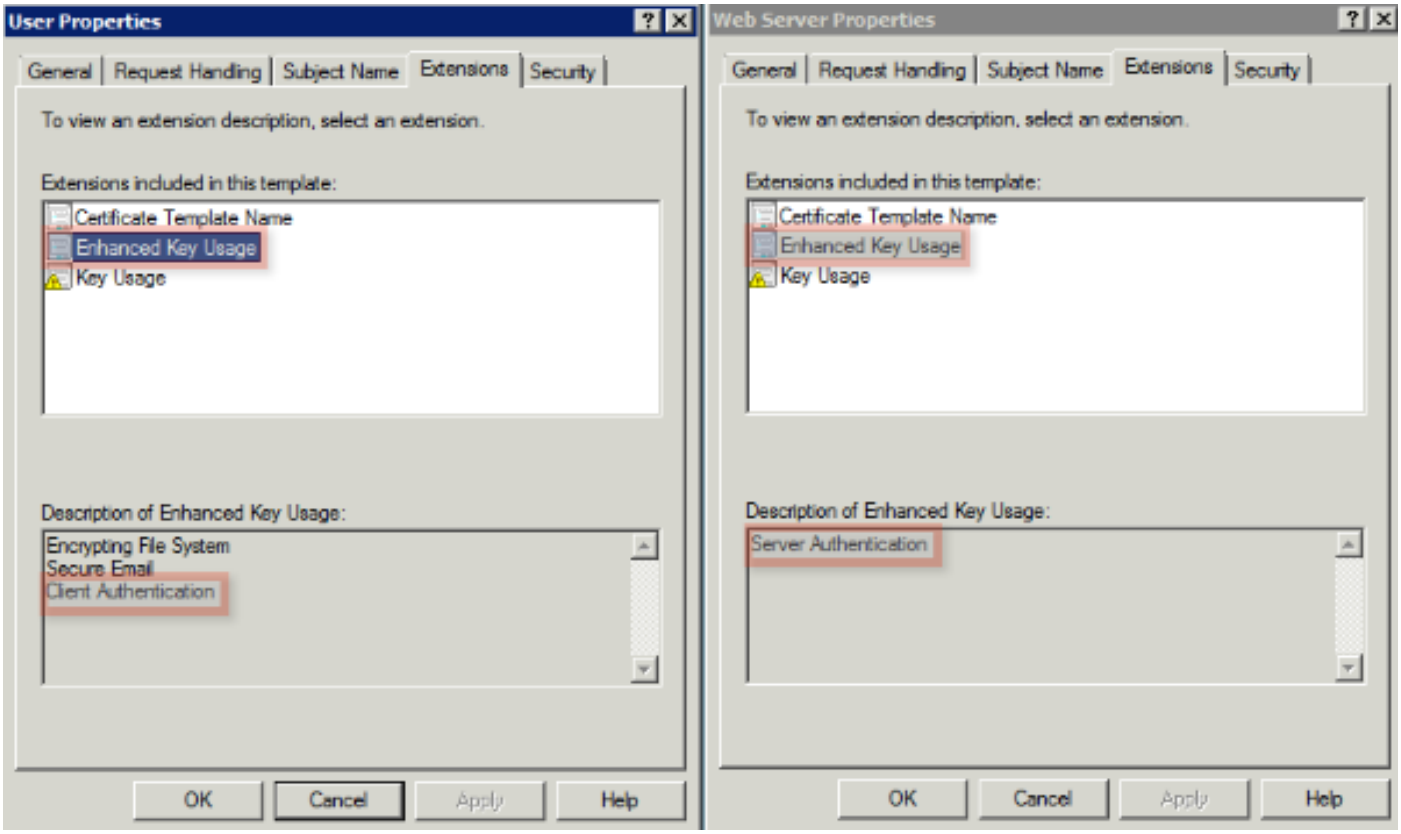
认证模板概述

Microsoft CA的管理员能配置使用为了运用应用程序策略到共同的一套证书的一个或更多模板。这些策略帮助为哪些识别证书和相关的密钥使用功能。应用程序政策价值在证书的延长的密钥用法(EKU)字段包含。验证器在EKU字段解析值为了保证客户端提交的证书可以用于打算的功能。某些更加普通的用途包括服务器验证、客户端验证、IPSec VPN和电子邮件。根据ISE，通常使用的EKU值包括服务器和客户端验证。

当您浏览到一个安全内存段网站，例如时，处理请求的Web服务器配置与有服务器验证一项应用程序策略的证书。当服务器收到HTTPS请求时，发送服务器验证证书对验证的连接的Web浏览器。此处重点是这是从服务器的单向的交换给客户端。因为它与ISE关连，一一般服务器验证证书的是admin GUI访问。ISE发送已配置的证书到已连接浏览器，并且不期望接收从客户端的一证书上一步。

当谈到服务例如使用EAP-TLS的BYOD，相互验证被偏好。为了启用此双向证书交换，用于的模板为了生成ISE身份证书必须拥有服务器验证一项最低的应用程序策略。Web服务器认证模板满足此要求。生成终端证书的认证模板必须包含客户端验证一项最低的应用程序策略。用户证书模板满足此要求。如果配置服务的ISE例如轴向政策加强点(iPEP)，用于的模板为了生成ISE服务器身份证书应该包含两个客户端和服务器验证属性，如果使用ISE版本1.1.x或以下。这允许admin和轴向节点相互互相验证。iPEP的EKU验证在ISE版本1.2删除，使此需求较不相关。

您能重新使用默认Microsoft CA Web服务器和用户模板，或者您能克隆和创建有在本文略述的进程的一个新的模板。基于这些证书需求，应该仔细计划CA配置和产生的ISE和终端证书为了最小化所有不需要的配置更改，当安装在生产环境。



认证模板配置

在介绍中注明， SCEP是用途广泛在IPSec VPN环境。结果， NDES角色的安装自动地配置服务器为SCEP使用**IPSec (脱机请求)**模板。因此，其中一在Microsoft CA的准备的第一步BYOD的是建立有正确应用程序策略的一个新的模板。在一独立部署，证书颁发机构和NDES服务在同一个服务器被排列，并且模板和需要的注册修改包含到同一个服务器。在一分布式NDES部署，注册修改在NDES服务器被做;然而，实际模板在NDES服务安装中指定的根或SUB根CA服务器定义。

完成这些步骤为了配置认证模板：

1. 登录到CA服务器作为**admin**。
2. 点击**Start > Administrative Tools >证书颁发机构**。
3. 展开CA服务器详细信息并且选择**认证模板**文件夹。此文件夹包含当前启用模板的列表。
4. 为了管理认证模板，在**认证模板**文件夹的右键单击和选择**管理**。
5. 在**认证模板中控制**，一定数量的非激活模板显示。
6. 为了配置一个新的模板为了用在SCEP上，在已经存在，例如**用户**，并且选择**重复的模板的**模板的右键单击。
7. 选择**Windows 2003年**或**Windows 2008年**，从属在最低CA OS于环境。
8. 在**常规选项卡**，请添加一显示名称，例如ISE-BYOD和有效性周期;留给所有其它选项被不选定。
   注意：模板有效性周期必须是小于或等于CA根和中间证书的有效性周期。

9. 点击**主题名称**选项卡，并且确认**在请求的供应**选择。

10. 点击**出版物需求**选项卡。思科建议您留下在一个典型的分层的CA环境的**出版物策略**空白。

11. 点击**扩展**选项卡，**应用程序策略**，然后**编辑**。

12. 单击**添加**，并且保证**客户端验证**被添加作为应用程序策略。单击 **Ok**。

13. 点击**安全选项卡**，然后**添加....**保证在NDES服务安装中定义的SCEP服务帐户有模板的完全控制，然后点击OK键。

14. 返回到**证书颁发机构GUI界面**。

15. 用鼠标右键单击在**认证模板**目录。导航对**新>发出的认证模板**。

16. 以前选择**ISE-BYOD**模板配置，并且点击OK键。

    注意：或者，您能通过与**certutil的**CLI启用模板- **SetCAtemplates +ISE-BYOD**命令。
    在已启用认证模板列表应该当前列出ISE-BYOD模板。

认证模板注册配置

完成这些步骤为了配置认证模板注册表项：

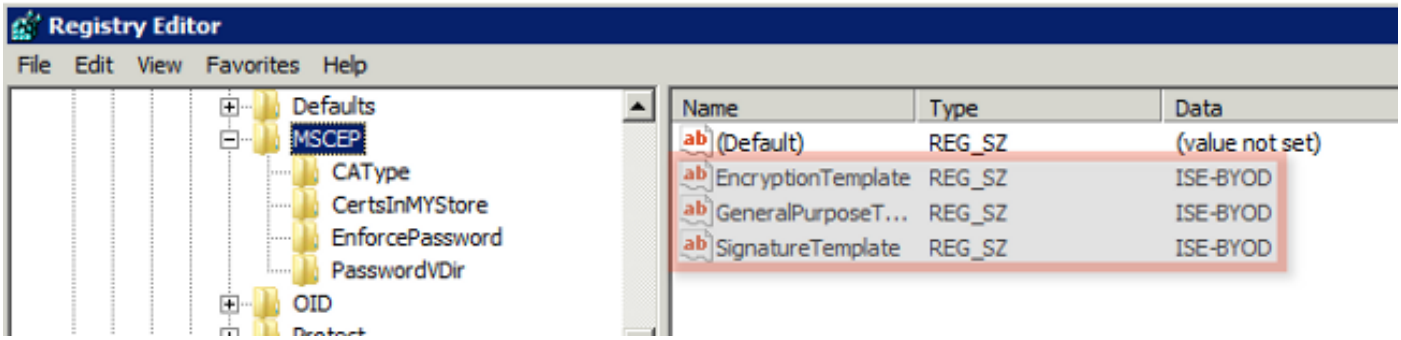
1. 连接到NDES服务器。

2. 点击**开始**并且登录**regedit**在搜索柱状图。

3. 导航对**计算机> HKEY_LOCAL_MACHINE>SOFTWARE> Microsoft >加密算法> MSCEP**。

4. 更改从**IPSec (脱机请求)的EncryptionTemplate**、**GeneralPurposeTemplate**和**SignatureTemplate**密钥到以前创建的**ISE-BYOD**模板。

5. 重新启动NDES服务器为了应用注册表设置。



配置ISE作为SCEP代理

在BYOD部署，终端不直接地与后端NDES服务器联络。反而， ISE策略节点配置作为SCEP代理并且用NDES服务器传递代表终端。终端直接地与ISE联络。在NDES服务器的IIS实例可以配置为了支持SCEP虚拟目录的HTTP和HTTPS捆绑。

完成这些步骤为了配置ISE作为SCEP代理：

1. 登录与admin凭证的**ISE GUI**。
2. 点击**管理**、**证书**然后**SCEP CA配置文件**。
3. 单击 **Add**。
4. 输入服务器名和说明。
5. 输入SCEP服务器的URL有IP或完全合格的域名(FQDN)的例如 (http://10.10.10.10/certsrv/mscep/)。
6. 点击**测验连接**。成功的连接导致一个成功的服务器响应上推消息。
7. 点击**"Save"**为了运用配置。
8. 为了验证，请点击**管理**，**证书**，**证书存储，**并且确认SCEP NDES服务器RA证书自动地下载对ISE节点。

验证

当前没有可用于此配置的验证过程。

故障排除

使用本部分可排除配置的故障。

一般请排除故障笔记

这是您能使用为了排除故障您的配置重要提示的列表：

- 为逻辑小站划分BYOD网络拓扑为了帮助识别调试和捕获沿路径的点ISE、NDES和CA终端之间。
- 保证ISE节点和CA共享一普通的网络时间协议(NTP)时间源。
- 终端应该能自动地设置他们的时刻与从DHCP和时间区域选项了解的NTP。
- 客户端的DNS服务器一定能解决ISE节点的FQDN。
- 保证TCP 80并且/或者TCP 443允许双向在ISE和NDES服务器之间。
- 测试与Windows机器由于改善的客户端记录日志。随意地，请与苹果公司IP电话配置工具一起请使用一苹果公司iDevice为了监控客户端控制台日志。
- 监控注册错误的CA和NDES服务器应用日志，并且请使用谷歌或TechNet为了研究那些错误。

- 在测试阶段期间，请使用HTTP SCEP为了实现在ISE、NDES和CA之间的数据包捕获。
- 请使用在ISE策略服务节点(PSN)的TCP转储工具，并且到/从NDES服务器监控流量。这查找在**操作>诊断工具>**General下**工具**。
- 安装在CA和NDES服务器的Wireshark或者在中间交换机的使用SPAN，为了到/从ISE PSN捕获SCEP流量。
- 保证适当的CA证书一系列在客户端证书的验证的ISE策略节点安装。
- 保证在onboarding期间，适当的CA证书一系列自动地安装在客户端上。
- 预览ISE和终端身份证书并且确认正确EKU属性存在。
- 监控实际认证登录认证和授权失败的ISE GUI。
  注意：一些恳求者不初始化客户端证书交换，如果错误的EKU存在，例如与服务器验证EKU的一个客户端证书。所以，认证失败也许总是不是存在ISE日志。
- 当NDES在一分布式部署安装，一远程根或SUB根CA将由CA名称或计算机名称选定在服务安装中。NDES服务器发送证书注册请求到此目标CA服务器。如果终端证书注册过程发生故障，数据包捕获(PCAP)也许显示NDES服务器返回**404 Not Found**错误到ISE节点。为了解决此问题，重新安装NDES服务和选择计算机名称选项而不是CA名称。
- 在设备onboarded后，请避免变更对SCEP CA一系列。终端Oss，例如苹果公司iOS，不自动地更新一以前已安装BYOD配置文件。在此iOS示例中，必须从终端和从ISE数据库删除的终端删除当前配置文件，因此onboarding可以再次表演。
- 您能配置Microsoft Certificate服务器为了连接到互联网和自动地更新从Microsoft根证明程序的证书。如果配置在环境的此网络检索选项与限制互联网策略，不能连接到互联网默认情况下的CA/NDES服务器能用15秒到超时。这能添加15第二延迟到处理SCEP请求从SCEP代理例如ISE。如果答复没有接收， ISE是被编程的为了超时SCEP请求在12秒之后。为了解决此问题，允许CA/NDES服务器的互联网访问或者修改在Microsoft CA/NDES服务器的本地安全策略的网络检索超时设置。为了找出在Microsoft服务器的此配置，请导航对**Start > Administrative Tools >本地安全策略>公共密钥策略>证书路径验证设置>网络检索**。

客户端记录日志

这是使用为了排除故障客户端记录日志问题有用的技术的列表：

- 输入**日志%temp% \ spwProfileLog.txt命令**为了查看Mircosoft Windows应用程序的客户端日志。
  注意：WinHTTP使用Microsoft Windows终端和ISE之间的连接。参考错误代码列表的Microsoft Windows错误消息条款。
- 输入**/sdcards/downloads/spw.log**命令为了查看机器人应用程序的客户端日志。
- 对于**MAC OSX**，请使用控制台应用程序，并且寻找**SPW**进程。
- 对于**苹果公司iOS**，请使用苹果公司配置器2.0为了查看消息。

ISE记录

完成这些步骤为了查看ISE日志：

1. 导航对**Administration >记录日志>调试日志配置**，并且选择适当的ISE策略节点。
2. 设置**客户端**和**供应**日志调试或跟踪，如所需求。
3. 再次产生问题并且描述相关种子信息为了实现搜索，例如MAC、IP和用户。
4. 导航对**操作>下载日志**，并且选择适当的ISE节点。
5. 在**调试日志请**选中，下载日志被命名**ise-psc.log**对桌面。
6. 请使用一台智能编辑器，例如Notepad ++为了解析日志文件。
7. 当问题隔离时，然后请返回日志级别对默认级别。

NDES记录日志和故障排除

欲知更多信息，参考AD CS ：排除故障网络设备登记服务Windows服务器条款。

相关信息

- **BYOD解决方案指南-认证机关服务器配置**
- **在Windows的NDES概述2008个R2**
- **MSCEP白皮书**
- **配置NDES服务器支持SSL**
- **证书需求，当您以EAP-TLS使用EAP-TLS或PEAP**
- **技术支持和文档**