

# 为BYOD配置ISE SCEP支持

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[经过测试的CA/NDES部署方案](#)

[独立部署](#)

[分布式部署](#)

[重要的Microsoft修补程序](#)

[重要的BYOD端口和协议](#)

[配置](#)

[禁用SCEP注册质询密码要求](#)

[将SCEP注册限制为已知ISE节点](#)

[在IIS中扩展URL长度](#)

[证书模板概述](#)

[证书模板配置](#)

[证书模板注册表配置](#)

[将ISE配置为SCEP代理](#)

[验证](#)

[故障排除](#)

[一般故障排除说明](#)

[客户端日志记录](#)

[ISE日志记录](#)

[NDES日志记录和故障排除](#)

[相关信息](#)

## 简介

本文档介绍在思科身份服务引擎(ISE)上成功配置Microsoft网络设备注册服务(NDES)和简单证书注册协议(SCEP)以自带设备(BYOD)的步骤。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- ISE版本1.1.1或更高版本
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012标准版

- 公钥基础设施(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或更高版本
- 安装了KB2483564和KB2633200热修复程序的Windows Server 2008 R2 SP1
- Windows Server 2012标准版

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。

与Microsoft证书服务相关的信息作为思科BYOD的指南提供。请参阅Microsoft TechNet作为Microsoft认证机构、网络设备注册服务(NDES)和SCEP相关服务器配置的最终真相来源。

## 背景信息

支持思科ISE的BYOD实施的一个优势是最终用户能够执行自助设备注册。这样可以消除IT部门为分发身份验证凭证和启用网络设备而承担的管理负担。BYOD解决方案的核心是网络请求方调配流程，该流程旨在向员工拥有的设备分发必要的证书。为满足此要求，可以配置Microsoft证书颁发机构(CA)，以便通过SCEP自动执行证书注册流程。

SCEP在虚拟专用网络(VPN)环境中已使用多年，以便于证书注册和分发到远程访问客户端和路由器。在Windows 2008 R2服务器上启用SCEP功能需要安装NDES。在NDES角色安装期间，还安装了Microsoft Internet Information Services(IIS)Web服务器。IIS用于终止CA和ISE策略节点之间的HTTP或HTTPS SCEP注册请求和响应。

NDES角色可以安装在当前CA上，也可以安装在成员服务器上。在独立部署中，NDES服务安装在包括认证中心服务和（可选）认证中心Web注册服务的现有CA上。在分布式部署中，NDES服务安装在成员服务器上。然后配置分布式NDES服务器以与上游根或子根CA通信。在此场景中，本文中概述的注册表修改在NDES服务器上使用自定义模板进行，证书驻留在上游CA上。

## 经过测试的CA/NDES部署方案

本节简要概述在思科实验室中测试的CA/NDES部署方案。请参阅Microsoft TechNet，作为与Microsoft CA、NDES和SCEP相关的服务器配置的最终真相来源。

### 独立部署

在概念验证(PoC)场景中使用ISE时，通常部署作为Active Directory(AD)域控制器、根CA和NDES服务器的自含Windows 2008或2012计算机：



- Domain Controller
- AD
- Root CA
- NDES

### 分布式部署

当ISE集成到当前Microsoft AD/PKI生产环境时，更常见的情况是看到服务在多个不同的Windows 2008或2012服务器上分布。思科已针对分布式部署测试了两种方案。

此图显示了分布式部署的第一个测试场景：



- Domain Controller
- AD
- Root CA



- Member Server
- Subordinate CA
- NDES

此图显示了分布式部署的第二个测试场景：



- Domain Controller
- AD
- Root CA



- Member Server
- Subordinate CA



- Member Server
- NDES

## 重要的Microsoft修补程序

在为BYOD配置SCEP支持之前，请确保Windows 2008 R2 NDES服务器已安装以下Microsoft修补程序：

- [如果证书是使用NDES管理的，则Windows Server 2008 R2中SCEP证书的续订请求失败](#) — 此问题发生，因为NDES不支持GetCACaps操作。
- [在Windows Server 2008 R2中重新启动企业CA后，NDES不提交证书请求](#) — 此消息显示在事件查看器中：“网络设备注册服务无法提交证书请求(0x800706ba)。RPC服务器不可用。”

**警告：**配置Microsoft CA时，必须了解ISE不支持RSASSA-PSS签名算法。思科建议您配置CA策略，使其改用sha1WithRSAEncryption或sha256WithRSAEncryption。

## 重要的BYOD端口和协议

以下是重要的BYOD端口和协议列表：

- TCP:8909调配：从思科ISE(Windows和Macintosh操作系统(OS))进行向导安装
- TCP:443调配：从Google Play(Android)安装向导
- TCP:8905调配：请求方调配过程
- TCP:80或TCP:443 SCEP代理到CA ( 基于SCEP RA URL配置 )

**注意：**有关所需端口和协议的最新列表，请参阅《ISE 1.2硬件安[装指南](#)》。

## 配置

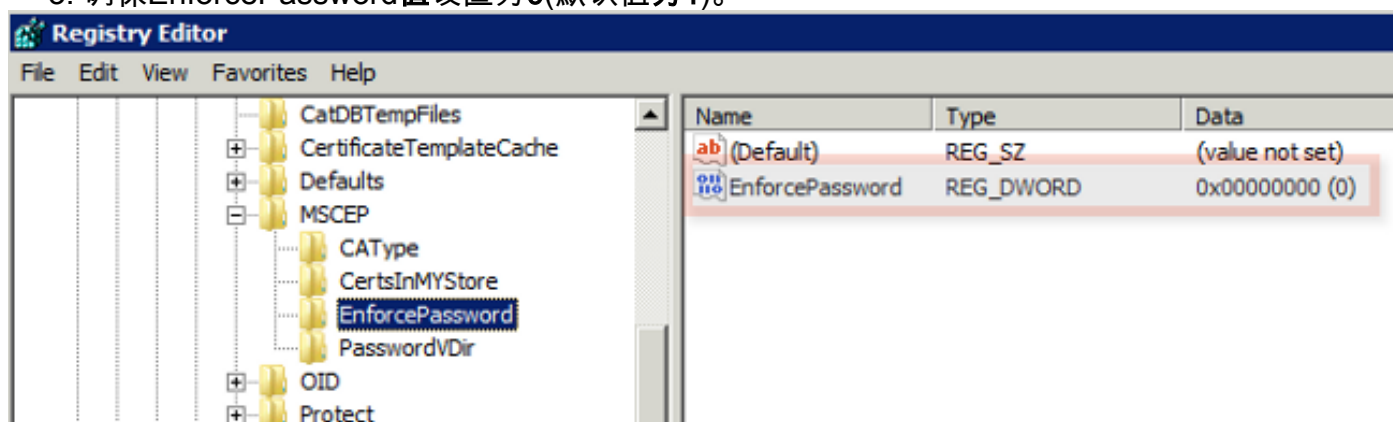
使用本部分在ISE上配置NDES和SCEP对BYOD的支持。

## 禁用SCEP注册质询密码要求

默认情况下，Microsoft SCEP(MSCEP)实施使用动态质询密码，以便在证书注册过程中对客户端和终端进行身份验证。在实施此配置要求后，您必须浏览到NDES服务器上的MSCEP管理Web GUI，才能按需生成密码。您必须在注册请求中包含此密码。

在BYOD部署中，对质询密码的要求使用户自助服务解决方案的目的落空。要删除此要求，必须在NDES服务器上修改此注册表项：

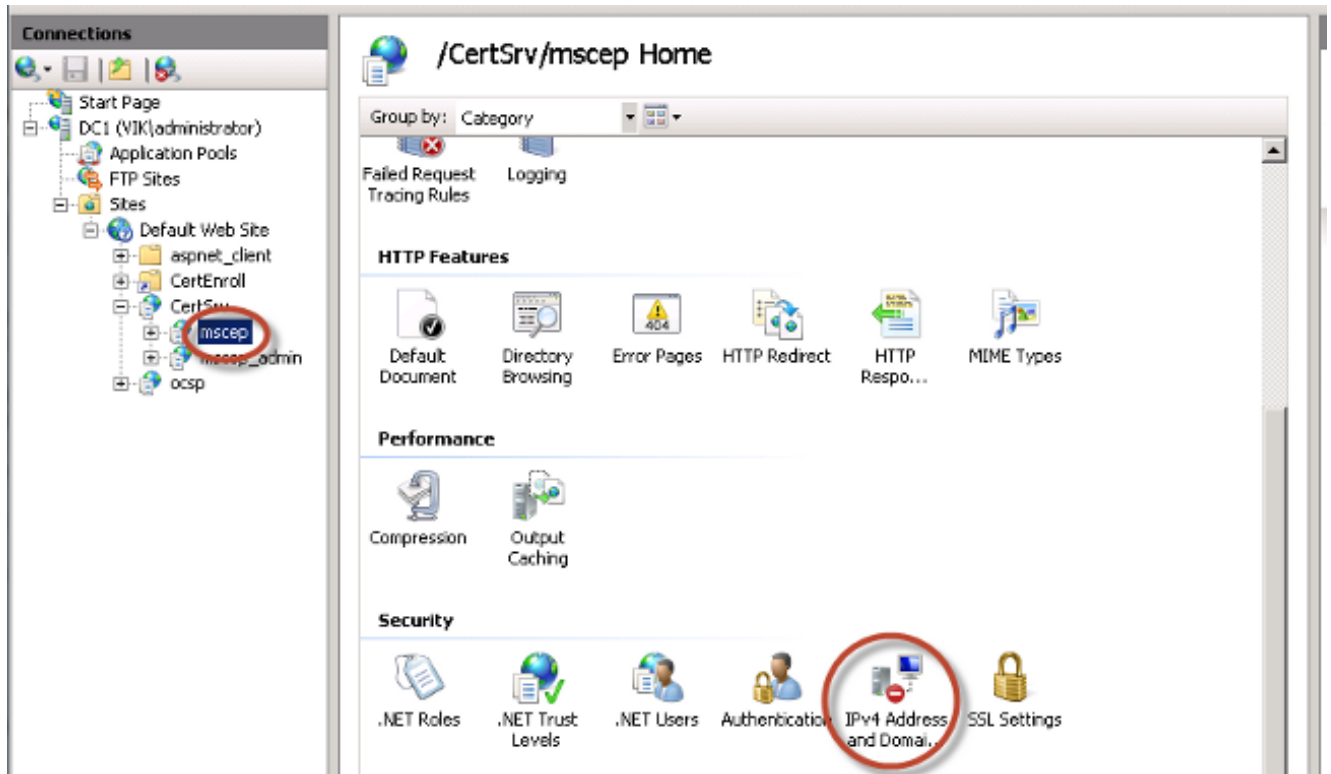
1. 单击**开始**，在**搜索**栏中输入regedit。
2. 导航至“计算机”>“HKEY\_LOCAL\_MACHINE”>“软件”>“Microsoft”>“加密”> MSCEP > EnforcePassword。
3. 确保EnforcePassword值设置为0(默认值为1)。



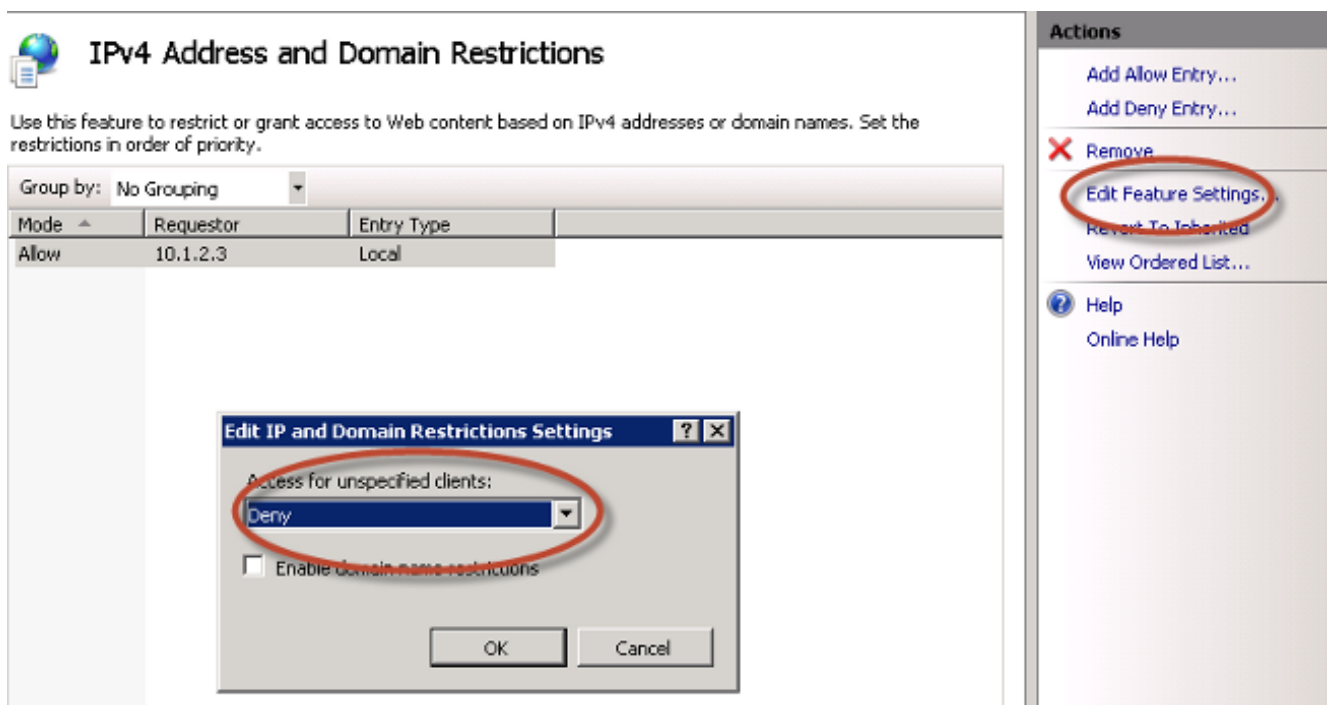
## 将SCEP注册限制为已知ISE节点

在某些部署方案中，可能首选将SCEP通信限制为选定的已知ISE节点列表。这可以通过IIS中的IPv4地址和域限制功能实现：

1. 打开IIS并导航至/CertSrv/mscep网站。



2. 双击**Security > IPv4 Address and Domain Restrictions**。使用**Add Allow Entry**和**Add Deny Entry**操作以允许或限制基于ISE节点IPv4地址或域名的Web内容访问。使用“编辑功能设置”(Edit Feature Settings)操作为未指定的客户端定义默认访问规则。

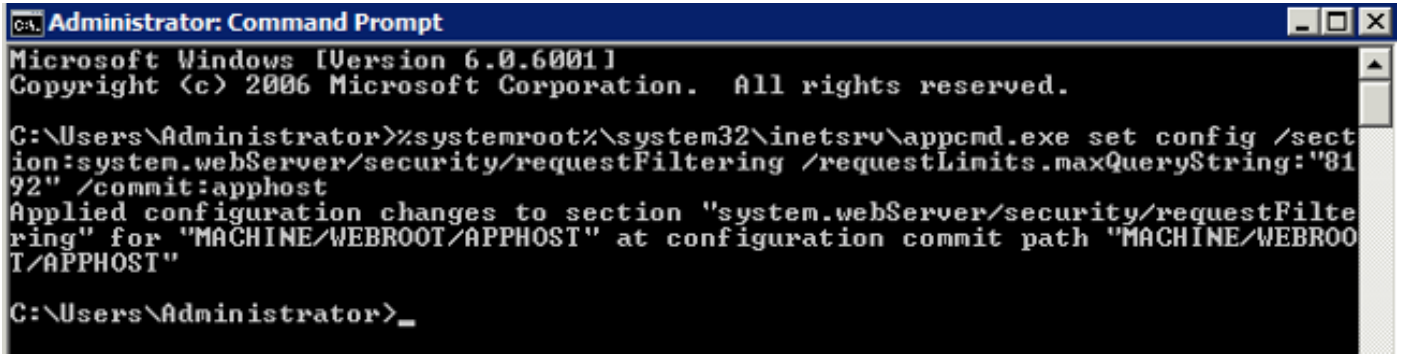


## 在IIS中扩展URL长度

ISE可能生成IIS Web服务器过长的URL。为避免此问题，可以修改默认IIS配置以允许更长的URL。从NDES服务器CLI输入以下命令：

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

**注意：**查询字符串大小可能因ISE和终端配置而异。从具有管理权限的NDES服务器CLI输入此命令。



```
Administrator: Command Prompt
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>%systemroot%\system32\inetsrv\appcmd.exe set config /section:system.webServer/security/requestFiltering /requestLimits.maxQueryString:"8192" /commit:apphost
Applied configuration changes to section "system.webServer/security/requestFiltering" for "MACHINE/WEBROOT/APPHOST" at configuration commit path "MACHINE/WEBROOT/APPHOST"

C:\Users\Administrator>_
```

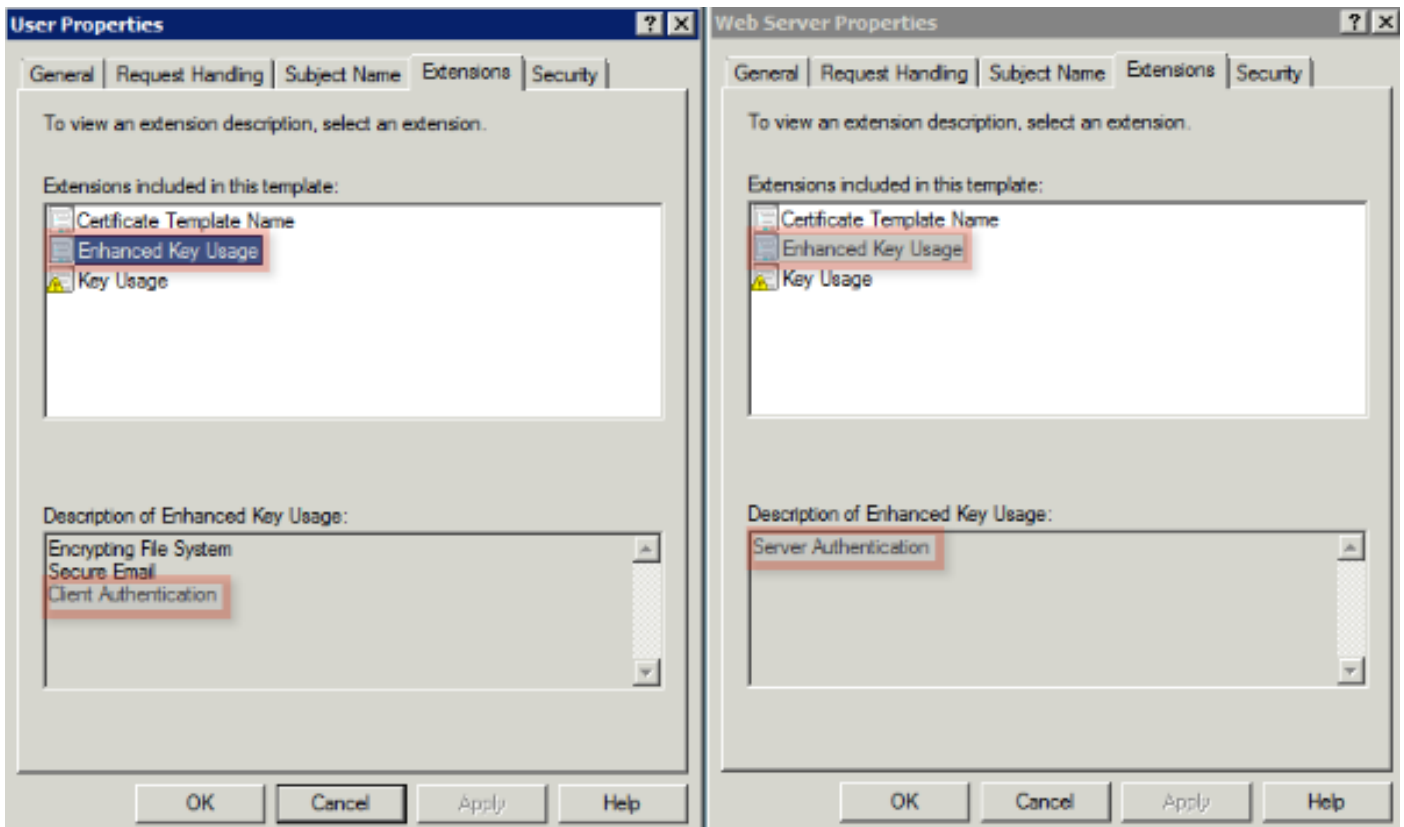
## 证书模板概述

Microsoft CA的管理人员可以配置一个或多个模板，这些模板用于将应用策略应用到一组公用证书。这些策略有助于确定证书和关联密钥的使用功能。应用策略值包含在证书的扩展密钥使用(EKU)字段中。身份验证器解析EKU字段中的值，以确保客户端提供的证书可用于预期功能。一些更常见的用途包括服务器身份验证、客户端身份验证、IPSec VPN和电子邮件。就ISE而言，更常用的EKU值包括服务器和/或客户端身份验证。

例如，当您浏览到安全银行网站时，处理请求的Web服务器配置了具有服务器身份验证应用策略的证书。当服务器收到HTTPS请求时，它会将服务器身份验证证书发送到连接的Web浏览器进行身份验证。这里的要点是这是从服务器到客户端的单向交换。与ISE相关，服务器身份验证证书的常见用途是管理GUI访问。ISE将配置的证书发送到连接的浏览器，并且不期望从客户端收到证书。

对于使用EAP-TLS的BYOD等服务，首选相互身份验证。要启用此双向证书交换，用于生成ISE身份证书的模板必须具有服务器身份验证的最低应用策略。Web服务器证书模板满足此要求。生成终端证书的证书模板必须包含客户端身份验证的最低应用策略。用户证书模板满足此要求。如果为服务(如内联策略实施点(iPEP))配置ISE，则用于生成ISE服务器身份证书的模板应包含客户端和服务端身份验证属性(如果使用ISE版本1.1.x或更低版本)。这允许管理员和内联节点相互进行身份验证。iPEP的EKU验证在ISE版本1.2中删除，这使此要求不再相关。

您可以重复使用默认的Microsoft CA Web Server和用户模板，也可以使用本文档中概述的流程克隆和创建新模板。根据这些证书要求，应仔细规划CA配置以及生成的ISE和终端证书，以便在生产环境中安装时最大限度地减少任何不需要的配置更改。



## 证书模板配置

如简介中所述，SCEP在IPSec VPN环境中广泛使用。因此，NDES角色的安装会自动将服务器配置为使用SCEP的IPSec(脱机请求)模板。因此，为BYOD准备Microsoft CA的第一步是使用正确的应用策略构建新模板。在独立部署中，证书颁发机构和NDES服务被配置在同一服务器上，并且模板和所需的注册表修改被包含在同一服务器上。在分布式NDES部署中，注册表修改在NDES服务器上进行；但是，实际模板是在NDES服务安装中指定的根或子根CA服务器上定义的。

要配置证书模板，请完成以下步骤：

1. 以管理员身份登录CA服务器。
2. 单击开始>管理工具> 证书颁发机构。
3. 展开CA服务器详细信息并选择“证书模板”文件夹。此文件夹包含当前启用的模板列表。
4. 要管理证书模板，请右键单击“证书模板”文件夹，然后选择**管理**。
5. 在**证书模板控制台**中，显示许多非活动模板。
6. 要配置新模板以与SCEP配合使用，请右键单击已存在的模板（如“用户”），然后选择“复制模板”。
7. 根据环境中的**最低CA OS,选择Windows 2003或Windows 2008**。
8. 在General(常规)选项卡上，添加显示名称，如ISE-BYOD和有效期；不选中所有其他选项。  
**注意：**模板有效期必须小于或等于CA根证书和中间证书的有效期。
9. 单击“主题名称”选项卡，确认已选中“请求中的供应”。



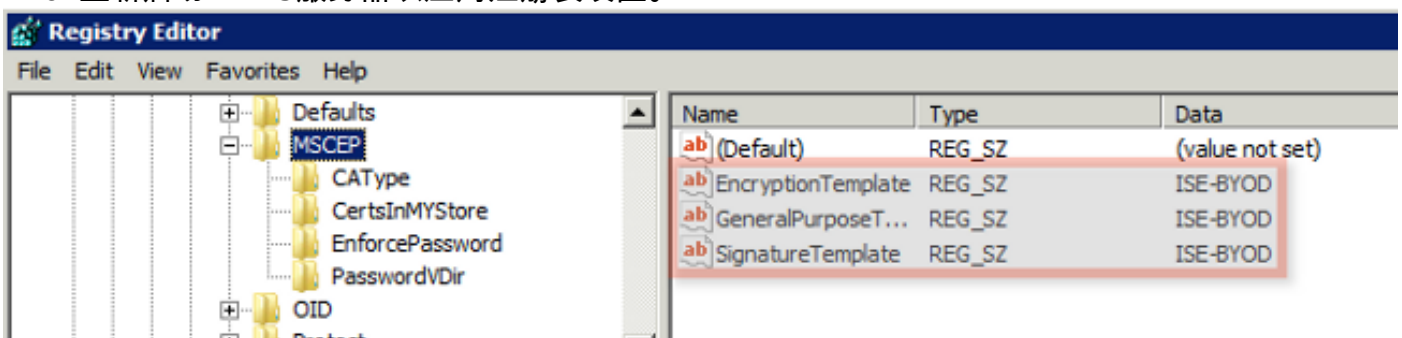
10. 单击“Issuance Requirements(发行要求)”选项卡。Cisco建议在典型的分层CA环境中将颁发策略留空。
11. 单击“Extensions(扩展)”选项卡、“Application Policies (应用策略)”，然后单击“Edit。”
12. 单击Add，并确保将Client Authentication添加为应用策略。Click OK.
13. 单击“Security(安全)”选项卡，然后单击“Add...”。确保在NDES服务安装中定义的SCEP服务帐户对模板具有完全控制权，然后单击OK。
14. 返回到证书颁发机构GUI界面。
15. 右键单击“证书模板”目录。导航到New > Certificate Template to Issue。
16. 选择之前配置的ISE-BYOD模板，然后单击OK。

**注意：**或者，您也可以通过CLI使用certutil -SetCAtemplates +ISE-BYOD命令启用模板。ISE-BYOD模板现在应列在已启用的证书模板列表中。

## 证书模板注册表配置

要配置证书模板注册表项，请完成以下步骤：

1. 连接到NDES服务器。
2. 单击开始，在搜索栏中输入regedit。
3. 导航至“计算机”>“HKEY\_LOCAL\_MACHINE”>“软件”>“Microsoft”>“加密”>“MSCEP”。
4. 将EncryptionTemplate、GeneralPuruseTemplate和SignatureTemplate密钥从IPSec (脱机请求)更改为先前创建的ISE-BYOD模板。
5. 重新启动NDES服务器以应用注册表设置。



## 将ISE配置为SCEP代理

在BYOD部署中，终端不直接与后端NDES服务器通信。相反，ISE策略节点配置为SCEP代理，并代表终端与NDES服务器通信。终端直接与ISE通信。可以配置NDES服务器上的IIS实例，以支持SCEP虚拟目录的HTTP和/或HTTPS绑定。

要将ISE配置为SCEP代理，请完成以下步骤：

1. 使用**管理员凭证**登录ISE GUI。
2. 单击**Administration**、**Certificates**和**SCEP CA Profiles**。
3. 单击 **Add**。
4. 输入服务器名称和说明。
5. 输入IP或完全限定域名(FQDN)的SCEP服务器的URL(例如 <http://10.10.10.10/certsrv/mscep/>)。
6. 单击**Test Connectivity**。连接成功会导致服务器响应弹出消息成功。
7. 单击**Save**以应用配置。
8. 要进行验证，请点击**Administration**、**Certificates**、**Certificates** 和**Certificate Store**，然后确认SCEP NDES服务器RA证书已自动下载到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。

### 一般故障排除说明

以下是可用于排除配置故障的重要注释列表：

- 将BYOD网络拓扑划分为逻辑路点，以帮助识别调试和捕获ISE、NDES和CA终端之间路径中的点。
- 确保ISE节点和CA共享一个通用网络时间协议(NTP)时间源。
- 终端应能够使用从DHCP获取的NTP和时区选项自动设置时间。
- 客户端的DNS服务器必须能够解析ISE节点的FQDN。
- 确保ISE和NDES服务器之间双向允许TCP 80和/或TCP 443。
- 由于改进了客户端日志记录，因此使用Windows计算机进行测试。或者，使用Apple iDevice和Apple iPhone配置实用程序来监控客户端控制台日志。
- 监控CA和NDES服务器应用日志中的注册错误，并使用Google或TechNet来研究这些错误。

- 在整个测试阶段，对SCEP使用HTTP，以便在ISE、NDES和CA之间捕获数据包。
- 在ISE策略服务节点(PSN)上使用TCP转储实用程序，并监控进出NDES服务器的流量。此位置位于“操作”>“诊断工具”>“常规工具”下。
- 在CA和NDES服务器上安装Wireshark，或在中间交换机上使用SPAN，以便捕获进出ISE PSN的SCEP流量。
- 确保在ISE策略节点上安装适当的CA证书链，以验证客户端证书。
- 确保在自注册期间，将相应的CA证书链自动安装到客户端。
- 预览ISE和终端身份证书并确认存在正确的EKU属性。
- 监控ISE GUI中的实时身份验证日志，以查看身份验证和授权失败。  
**注意：**如果存在错误的EKU，例如具有服务器身份验证的EKU的客户端证书，某些请求方不会初始化客户端证书交换。因此，身份验证失败可能并不总是出现在ISE日志中。
- 在分布式部署中安装NDES时，远程根或子根CA将在服务安装中由CA名称或计算机名称指定。NDES服务器向此目标CA服务器发送证书注册请求。如果终端证书注册过程失败，数据包捕获(PCAP)可能显示NDES服务器向ISE节点返回404 Not Found错误。要解决此问题，请重新安装NDES服务，并选择“计算机名”(Computer Name)选项，而不是“CA名称”(CA Name)。
- 避免在设备入网后对SCEP CA链进行更改。终端操作系统（如Apple iOS）不会自动更新之前安装的BYOD配置文件。在此iOS示例中，必须从终端删除当前配置文件，从ISE数据库删除终端，以便可以再次执行自注册。
- 您可以配置Microsoft证书服务器以连接到Internet并自动从Microsoft根证书程序更新证书。如果在具有受限互联网策略的环境中配置此网络检索选项，则无法连接到互联网的CA/NDES服务器在默认情况下可能需要15秒超时。这可以增加15秒的延迟，以处理来自SCEP代理（如ISE）的SCEP请求。ISE被编程为在12秒后超时SCEP请求（如果未收到响应）。要解决此问题，请允许CA/NDES服务器访问Internet，或修改Microsoft CA/NDES服务器的本地安全策略中的“网络检索超时”设置。要在Microsoft服务器上找到此配置，请导航至**开始>管理工具>本地安全策略>公钥策略>证书路径验证设置>网络检索**。

## 客户端日志记录

以下是用于排除客户端日志记录问题的有用技术列表：

- 输入日志%temp%\spwProfileLog.txt。命令，以查看Microsoft Windows应用的客户端日志。  
**注意：**WinHTTP用于Microsoft Windows终端和ISE之间的连接。有关错误代码的[列表](#)，请参阅Microsoft Windows错误消息文章。
- 输入/sdcards/downloads/spw.log命令以查看Android应用的客户端日志。
- 对于MAC OSX，请使用控制台应用程序并查找SPW过程。
- 对于Apple iOS，请[使用Apple Configurator 2.0](#)查看邮件。

## ISE日志记录

要查看ISE日志，请完成以下步骤：

1. 导航至Administration > Logging > Debug Log Configuration，然后选择适当的ISE策略节点。
2. 根据需要**将客户端和调配日志**设置为调试或跟踪。
3. 重现问题并记录相关种子信息，以便于搜索，例如MAC、IP和用户。
4. 导航至**操作 > 下载日志**，然后选择相应的ISE节点。
5. 在Debug Logs选项卡上，将名为ise-psc.log的日志下载到桌面。
6. 使用智能编辑器(如记事本++)来分析日志文件。
7. 隔离问题后，将日志级别返回到默认级别。

## NDES日志记录和故障排除

有关详细信息，请参阅[AD CS:排除网络设备注册服务Windows Server](#)文章的故障。

## 相关信息

- [BYOD解决方案指南 — 证书颁发机构服务器配置](#)
- [Windows 2008 R2中的NDES概述](#)
- [MSCEP白皮书](#)
- [配置NDES服务器以支持SSL](#)
- [使用EAP-TLS或PEAP与EAP-TLS时的证书要求](#)
- [技术支持和文档](#)