

# 配置ISE SCEP集成的HTTPS支持

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[NDES服务器证书配置](#)

[NDES服务器IIS绑定配置](#)

[ISE服务器配置](#)

[验证](#)

[故障排除](#)

[相关信息](#)

## 简介

本文描述要求的步骤配置Secure证书登记协议(SCEP)集成的超文本传输协议安全(HTTPS)支持用身份服务引擎(ISE)。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- Microsoft的互联网信息服务(IIS) Web服务器基础知识
- 体验在SCEP和证书的配置里在ISE

### 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.x
- 与ICM Hotfixes的Windows服务器2008 R2企业安装的[KB2483564](#)和[KB2633200](#)的

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。

对Microsoft证书服务提供相关的信息，当一个指南思科的特别地带来您自己的设备(BYOD)。参考的Microsoft的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的涉及服务器配置。

## 背景信息

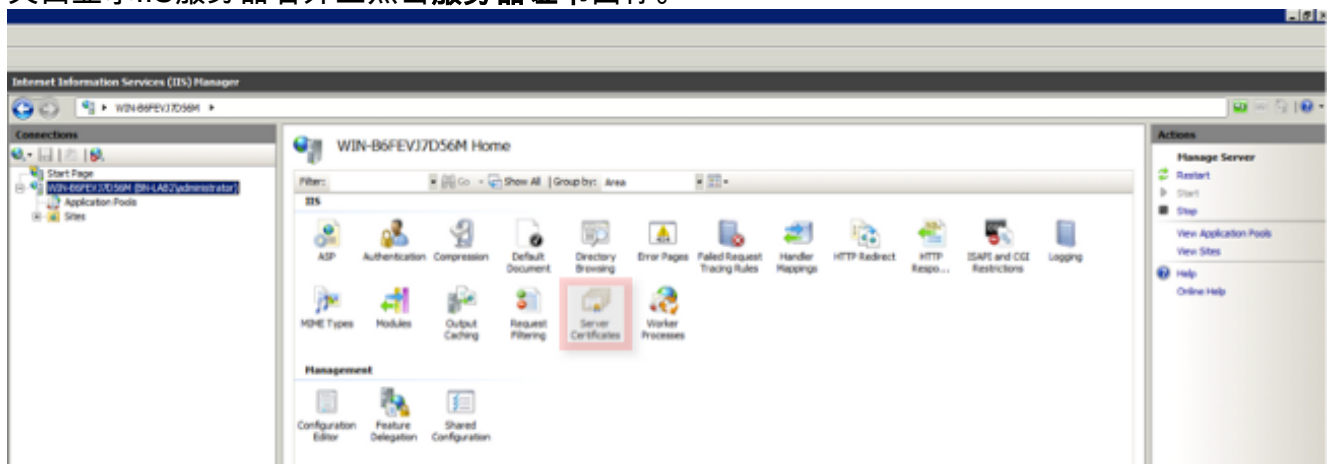
在BYOD部署，其中一核心组件是有安装的NDES角色的Microsoft 2008 R2企业服务器。此服务器是激活目录(AD)森林的成员。在NDES时初始安装，Microsoft的IIS Web服务器自动地安装并且配置支持SCEP的HTTP终端。使用HTTPS，在一些BYOD部署，客户也许要进一步巩固ISE和NDES之间的通信。此步骤选派要求的步骤请求和安装SCEP网站的一安全套接字层SSL证书。

## 配置

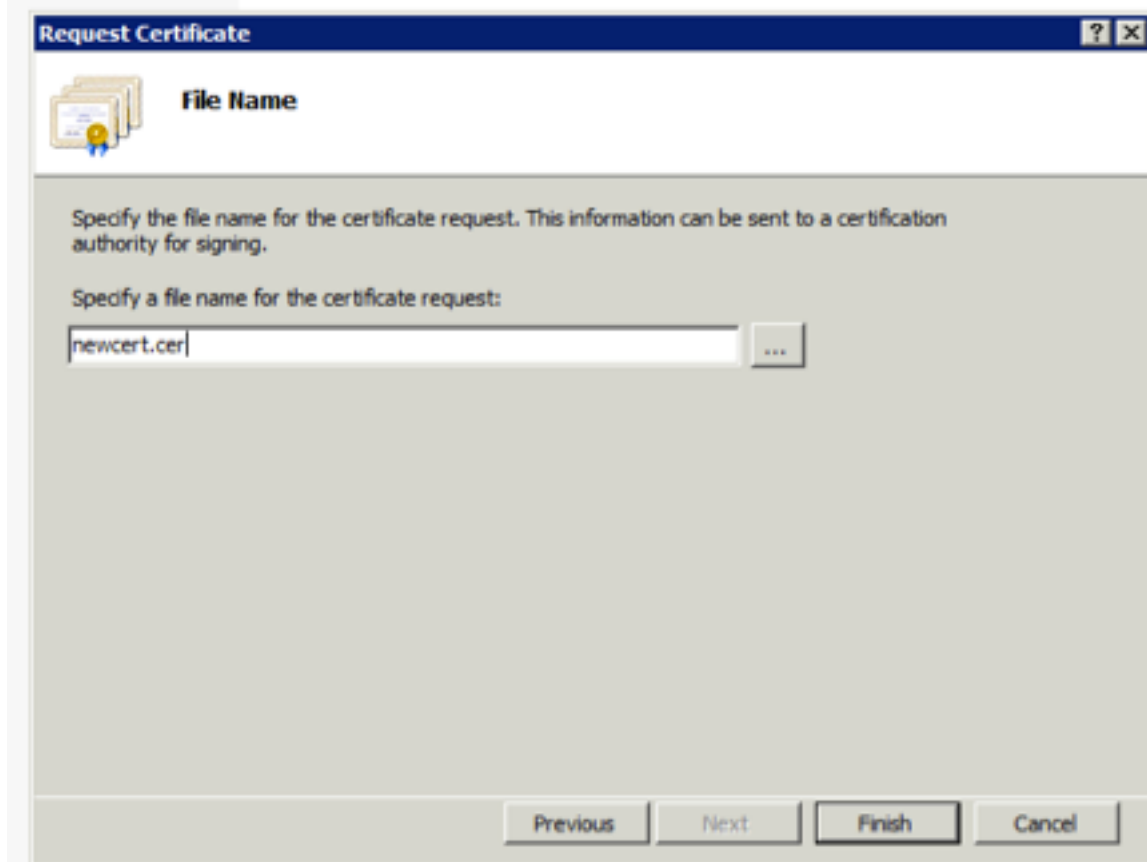
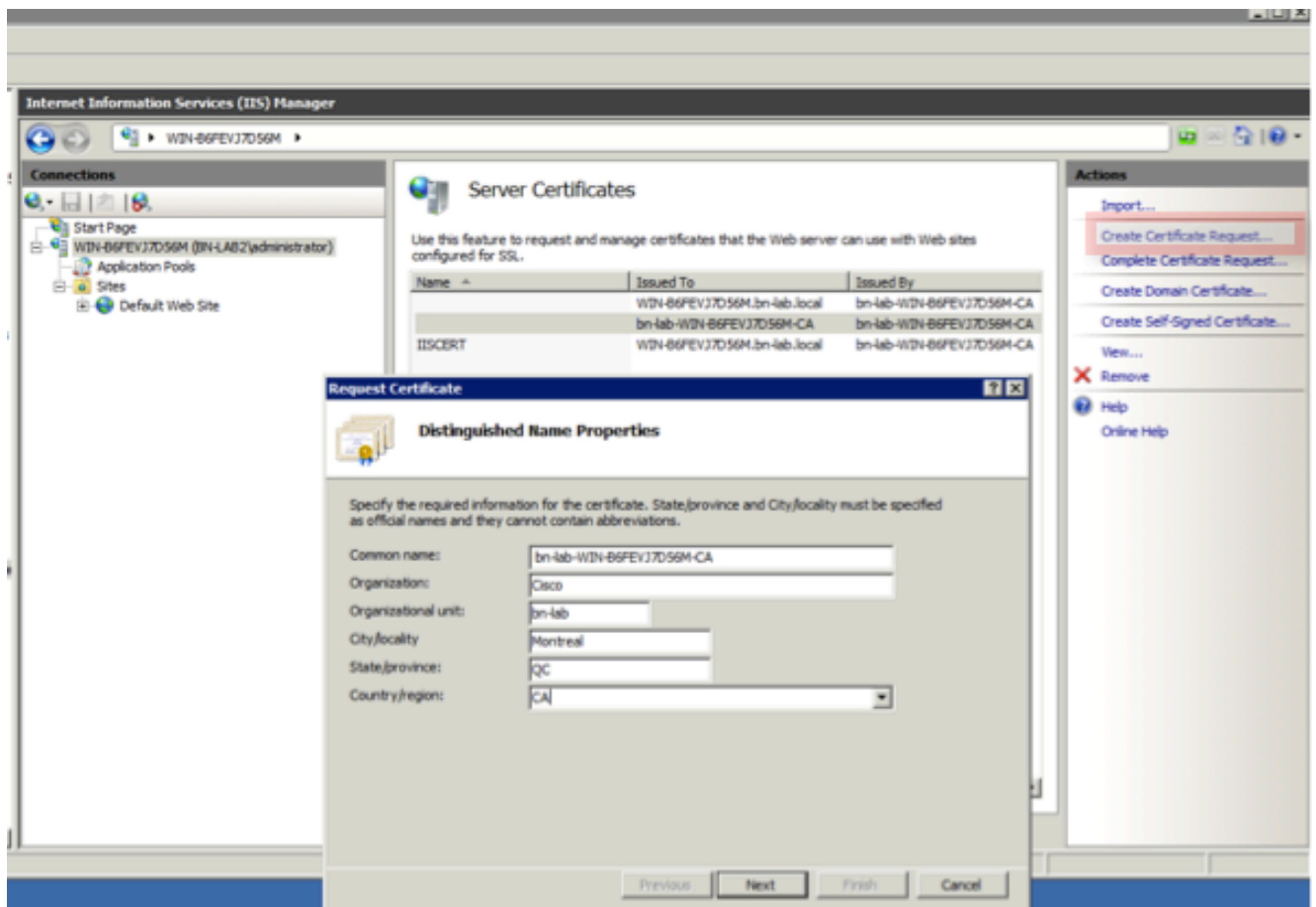
### NDES服务器证书配置

**注意：** 您必须配置IIS的一新证书(只要求，当IIS集成与第三方PKI例如Verisign时或，当认证机构(CA)和NDES服务器角色被分离在独立服务器上)时。在安装，如果NDES角色在一个当前Microsoft CA服务器，IIS使用在CA设置期间创建的服务器身份证书。对于独立配置例如此，请跳到直接地在本文的NDES服务器IIS绑定的配置部分。

1. 连接到NDES服务器通过控制台或RDP。
2. 点击**Start > Administrative Tools -> 互联网信息服务(IIS)管理器**。
3. 突出显示IIS服务器名并且点击**服务器证书**图标。



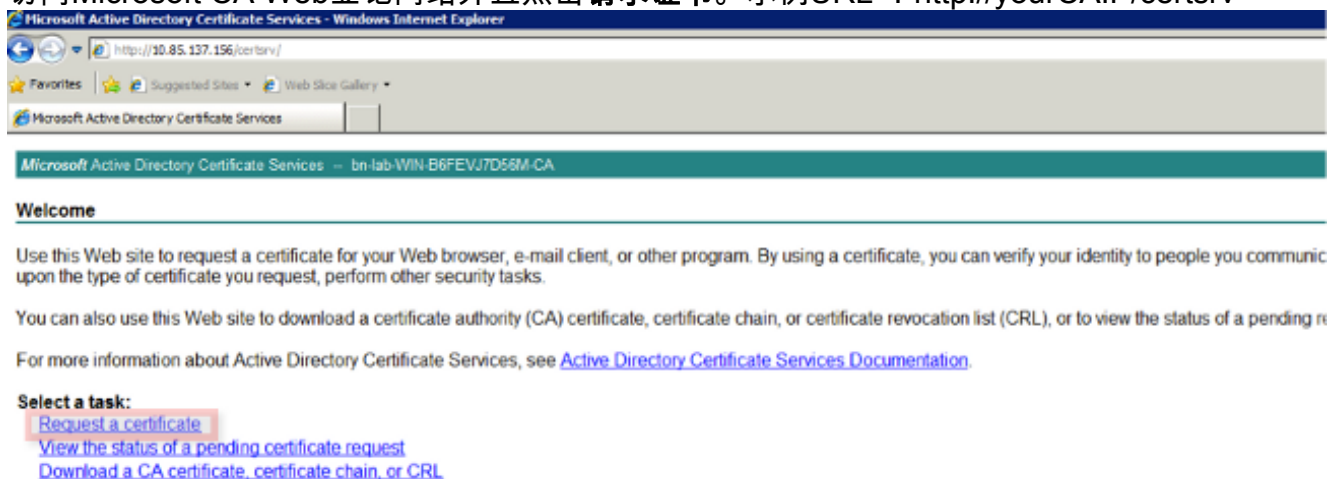
4. 点击**Create证书请求**，并且填入字段。



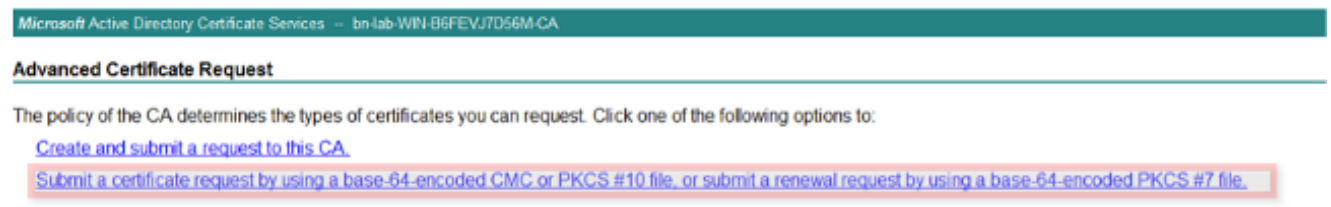
5. 打开在与文本编辑的上一步创建的.cer文件并且复制内容对剪贴板。

```
newcert - Notepad
File Edit Format View Help
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDazCCATQCAQAwTElMAkGA1UEBhMCQ0ExCzAJBgNVBAMgMA1FDMREwDwYDVQQL
DAhNb250cmVhbDEOMAwGA1UECgwFQ2lzy28xDzANBgNVBAsMBmJULWxhyjE1MCMG
A1UEAwVCV0lOLUI2RkVWsjdENTZNLmJULWxhyi5sb2NhbDCBnzANBgkqhkiG9w0B
AQEFAAOBjQAwgYkCgYEAjyQYTLhwQH9v49+EHZtwao0lmaQ63iSaRG8hzn3ixnuI
9wGkHhUQBwPNhyCI51OHYhsD8GZRIG5yLpp1Vq8cAHAIOnXhaz9//kSgpFV8rN0s
fd9fa7Onoq0h+jHNxaYdLTjxMqTNDcOkok0vFLqZR9FXuGEeGCoz2LA3jF1oXX0C
AwEAAaCCAbQwGgYKKwYBBAGCNw0CAZEMFgo2LjEuNZYwMS4yMFAGC5sGAQQBgjCV
FDFDMEECAQUMHFdJTi1CNkZFVko3RDU2TS5ibi1sYWIubG9jYwMMFUJOLUXBQjJc
YwRtaW5pc3RyYXRvcgWHTU1DLkVYRTByBgorBgEEAYI3DQICMwQwYgIBAR5aAE0A
aQBjAHIAbWZAG8AZgB0ACAAUGBTAEEAIABTAEMAaABhAG4AbgB1AGwAIABDAHIA
eQBWAHQAbwBNAHIAyQBwAGgAaQBjACAUAByAG8AdgBpAGQAZQByAwEAMIHPBgkq
hkig9w0BCQ4xgcEwgb4wDgYDVR0PAQH/BAQDAgTwMBMGA1UdJQQMMAoGCCsGAQUF
BwMBMHgGC5qGSib3DQEJDWRrMGkwDgYIKoZIhvcNAwICAgCAMA4GCCqGSIb3DQME
AgIAgDALBg1ghkgBZQMEASowCwYJYIZIAWUDBAETMASGCwCGSAF1AwQBAjALBg1g
hkGBZQMEAUwBwYFKw4DAgcwCgYIKoZIhvcNAwcwHQYDVR0OBBYEFLgkonC7Y+N9
dDrCREpo8/D/seatMA0GC5qGSib3DQEBBQUAA4GBAHHCHBDd02+byxwFcm9sXUZY
xpITwbkjbmrOT+q3rcIOjLNQireDB57Has8wdgCoCrLJs8ncm40dzuzan1xypPf
+EthSI0YgtDL5lgnJb35qAjLTCyDfNzEVP2P1FQNum9DetkzkjuwLh8zqeOxJyxv
+F80YwPo6CWPj3PwiZ2y
-----END NEW CERTIFICATE REQUEST-----
```

6. 访问Microsoft CA Web登记网站并且点击**请求证书**。示例URL : <http://yourCAIP/certsrv>



7. 单击**提交证书请求通过使用....**粘贴在从剪贴板的证书内容，并且选择**Web服务器**模板。



8. 单击**提交**然后保存证书文件到桌面。

## Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request

### Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
AgIAgDALBg1ghkgB2QMEASowCwYJYI2IAWUDBAET
hkgB2QMEAQUwBwYFKw4DAgcwCgYIKoZIhvcNAwcw
dDrCREpo8/D/seatMA0GCSqGSIs3DQEBBQUAA4GB
xpITWbkjxbmrOT+q3rcIOjLNQireDB57Has8WdgC
+EthsI0YgtL51gNjB35qAjLTCyDfNzEvP2P1FQN
+F80YwPo6CWPj3PWiz2y
```

### Certificate Template:

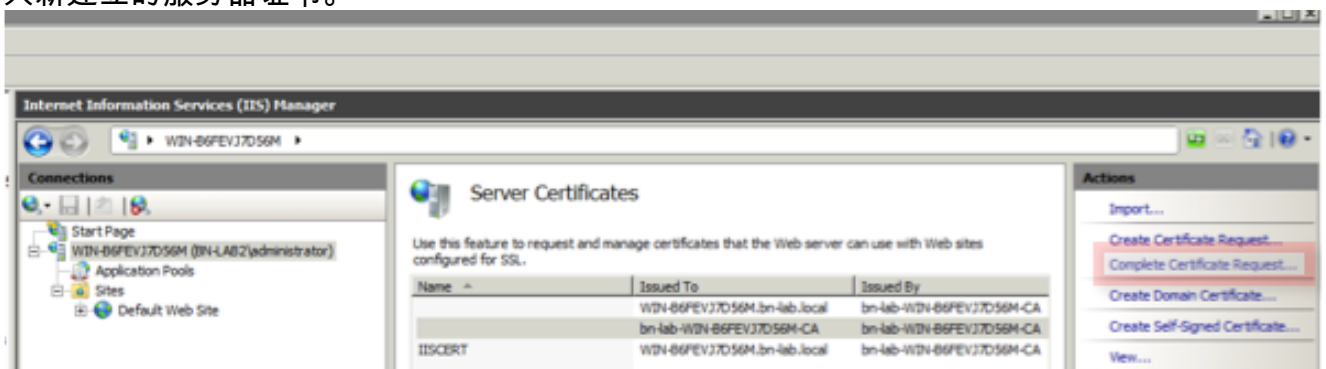
Web Server

### Additional Attributes:

Attributes:

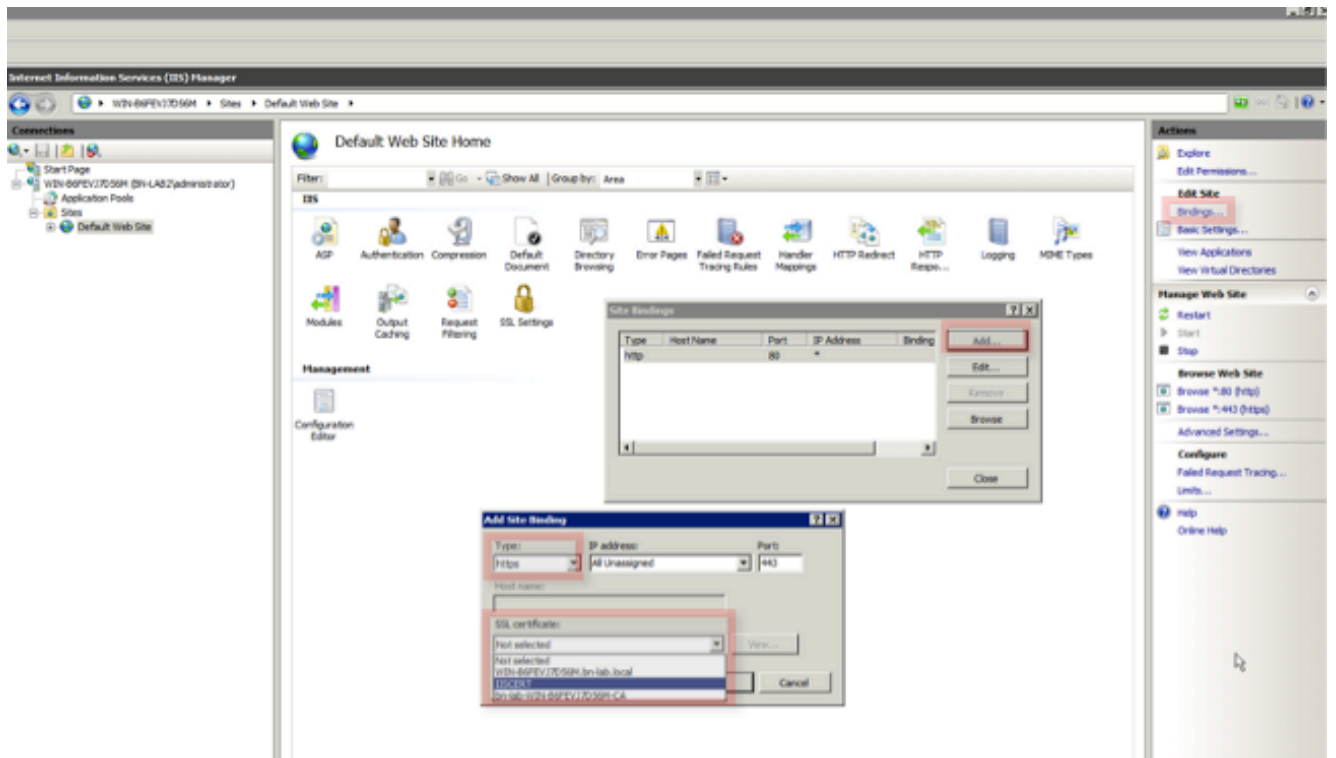
Submit >

9. 返回到NDES服务器并且打开utility IIS的管理器。点击服务器名然后单击**完整证书请求**为了导入新建立的服务器证书。



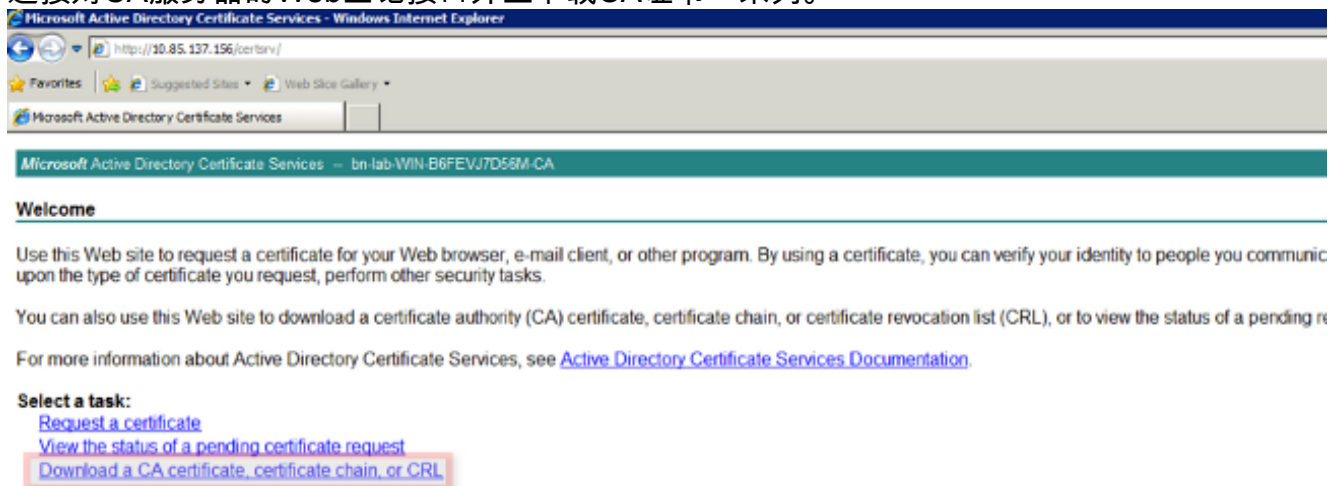
## NDES服务器IIS绑定配置

1. 展开服务器名，展开站点，点击默认网站。
2. 点击在右上角的**捆绑**。
3. 单击**添加**，更改Type到 HTTPS，并且从下拉列表选择证书。
4. 单击 **Ok**。

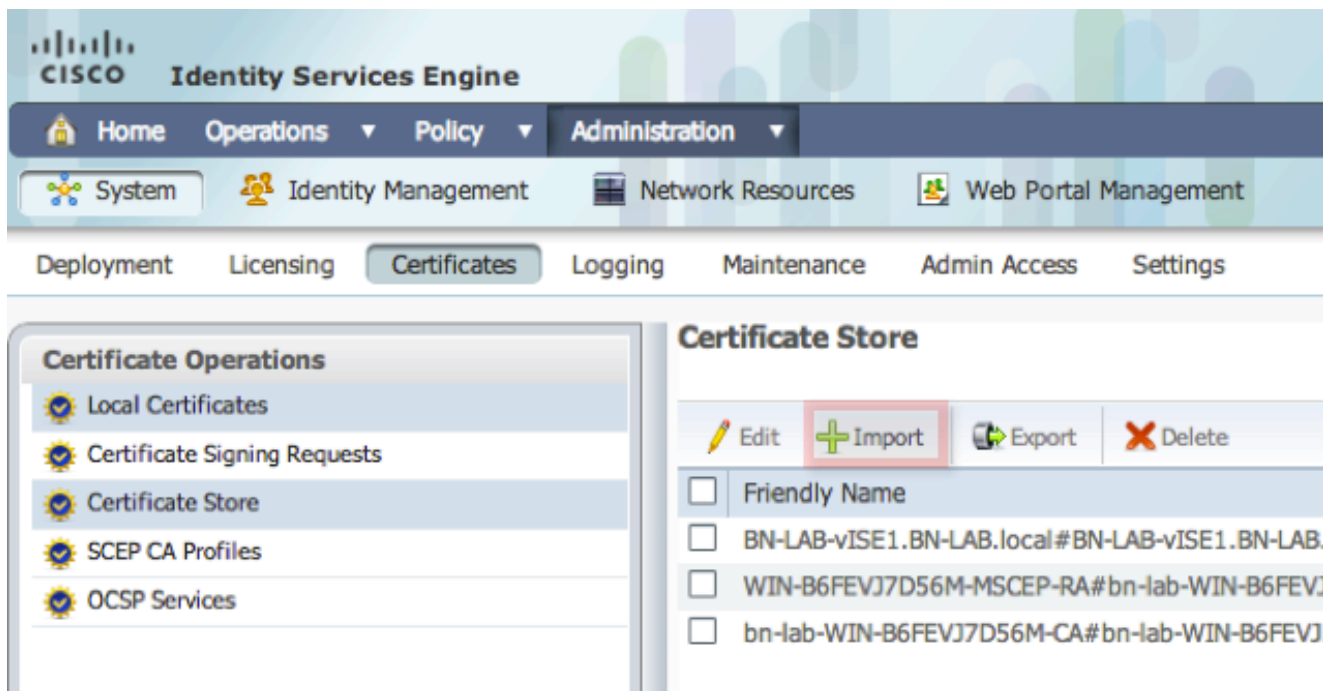


## ISE服务器配置

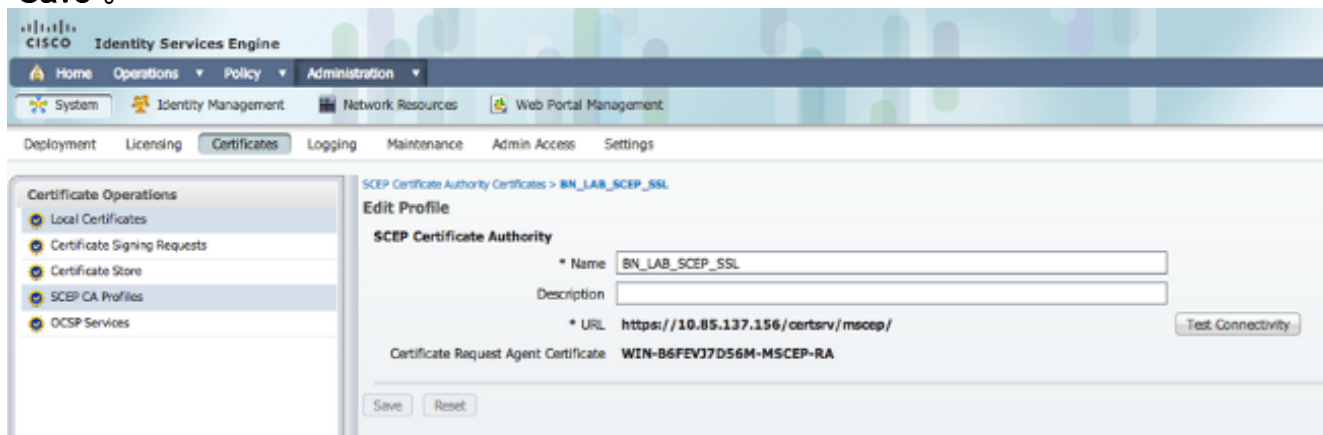
1. 连接对CA服务器的Web登记接口并且下载CA证书一系列。



2. 从ISE GUI，请导航对**管理->证书->证书存储**并且导入CA证书一系列到ISE存储。



3. 导航对**管理- >证书- > SCEP CA配置文件**并且配置HTTPS的URL。点击**测验连接**然后单击“Save”。



## 验证

使用本部分可确认配置能否正常运行。

- 导航对**管理- >证书- >证书Store**and验证CA证书一系列和NDES服务器注册机关(RA)证书存在。
- 请使用Wireshark或TCP转储监控在ISE admin节点和NDES服务器之间的初始SSL交换。

[命令输出解释程序工具](#) ( [仅限注册用户](#) ) 支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

## 故障排除

本部分提供的信息可用于对配置进行故障排除。

- 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这些终端之间- ISE、NDES和CA。
- 保证TCP 443允许双向在ISE和NDES服务器之间。
- 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研究那些错误。

- 请使用在ISE 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NDES服务器的Wireshark或在中介交换机的使用SPAN为了到/从ISE PSN捕获SCEP流量。

[命令输出解释程序工具](#) ( [仅限注册用户](#) ) 支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

**注意：** 使用 **debug** 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

## 相关信息

- [配置BYOD的SCEP支持](#)
- [技术支持和文档 - Cisco Systems](#)