

# UCCE \ PCCE -步骤获得并上载Windows服务器赛弗？在2008个服务器的签字的或Certificate Authority (CA)证书

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[步骤1.生成从互联网信息服务\(IIS\)管理器的CSR](#)

[步骤2.上传CA签名证书给互联网信息服务\(IIS\)管理器](#)

[步骤3.绑定签字的CA证书到默认网站](#)

[验证](#)

[故障排除](#)

[相关的思科支持社区讨论](#)

## 简介

本文描述如何配置在Unified Contact Center企业(UCCE) Windows的自己签署的或Certificate Authority (CA)证书2008个R2服务器。

## 先决条件

### 要求

思科建议您有签字的和自签名证书进程的知识。

### 使用的组件

本文档中的信息基于以下软件版本：

- Windows 2008个R2
- UCCE 10.5(1)

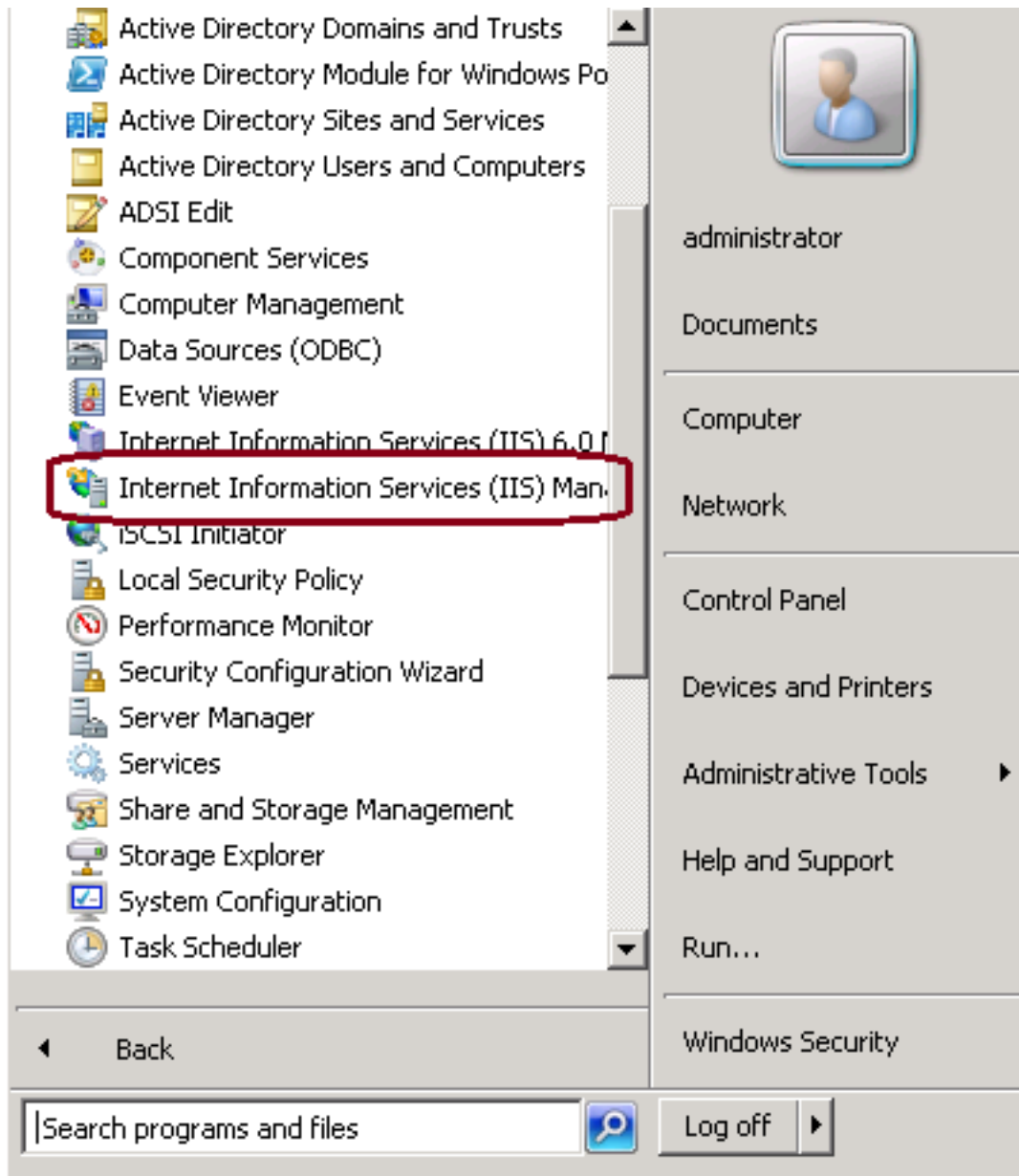
## 配置

设置HTTPS通信的证书在Windows服务器是三步的过程

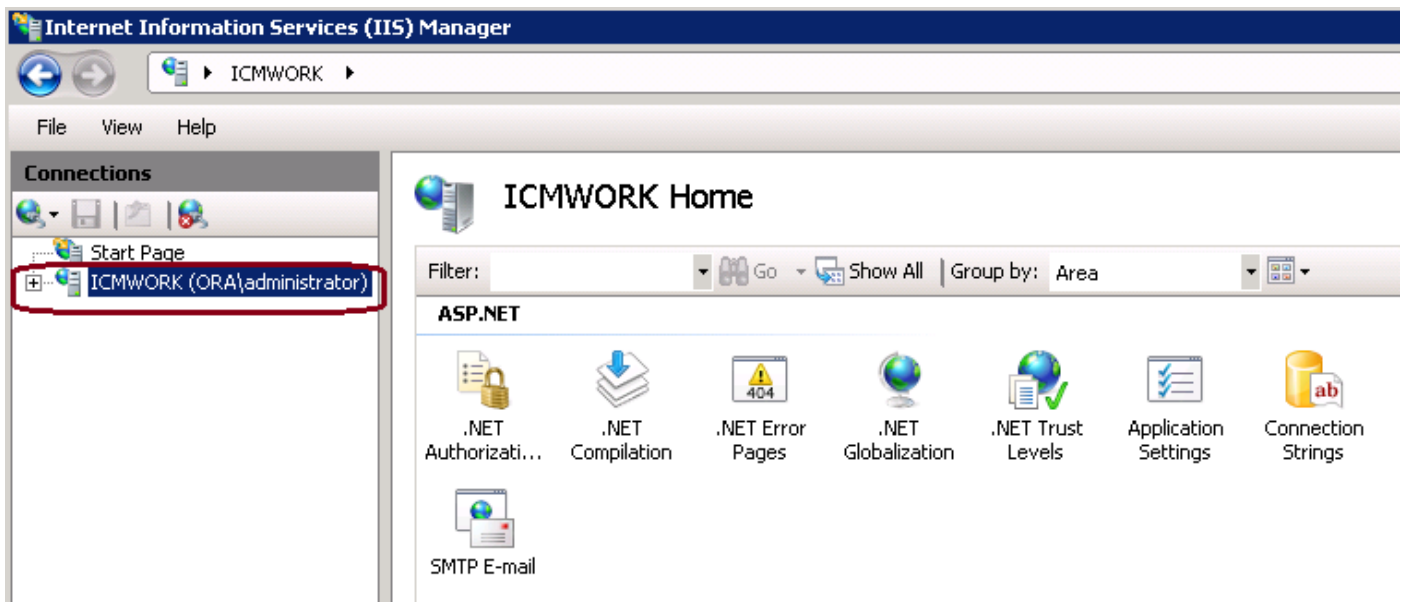
- 生成证书签名请求(CSR)从互联网信息服务(IIS)管理器
- 上传CA签名证书给互联网信息服务(IIS)管理器
- 绑定签字的CA证书到默认网站

## 步骤1.生成从互联网信息服务(IIS)管理器的CSR

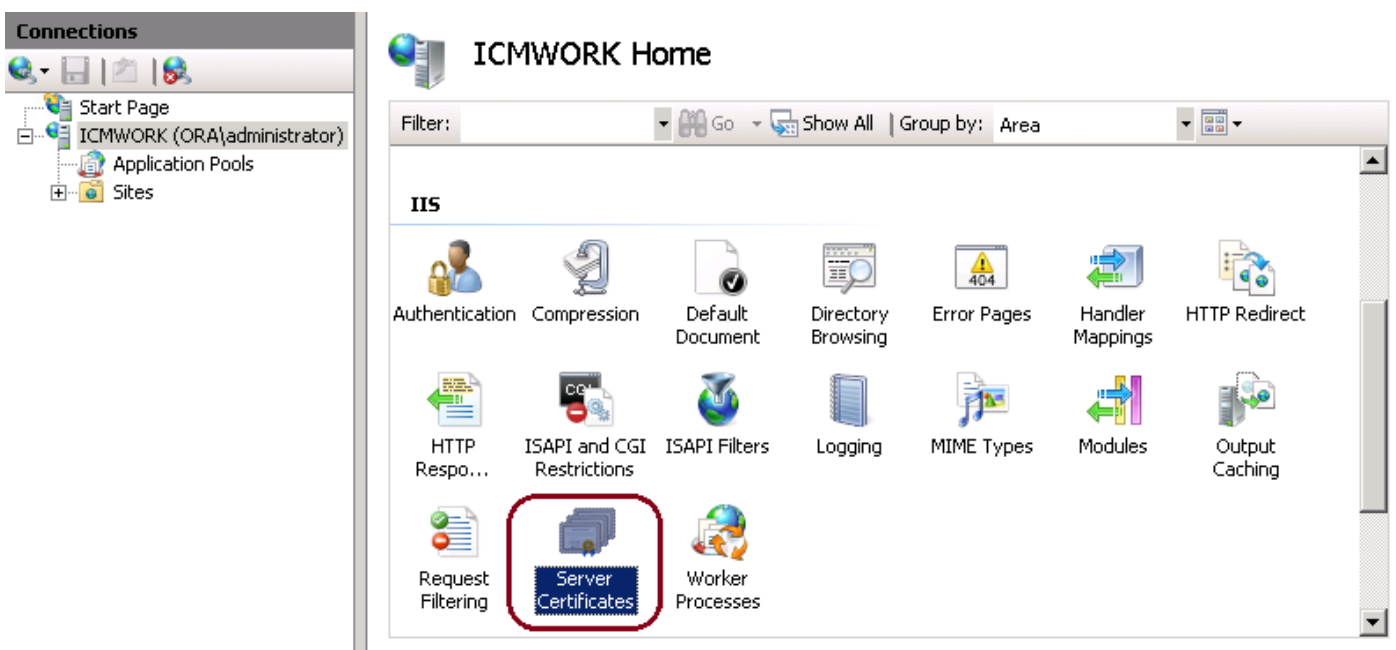
1. 登录到Windows，单击**Start > Run >所有Programs > Administrative工具> Internet信息服务(IIS)**如此镜像所显示，**管理器**。如果存在，请勿选择IIS版本6。



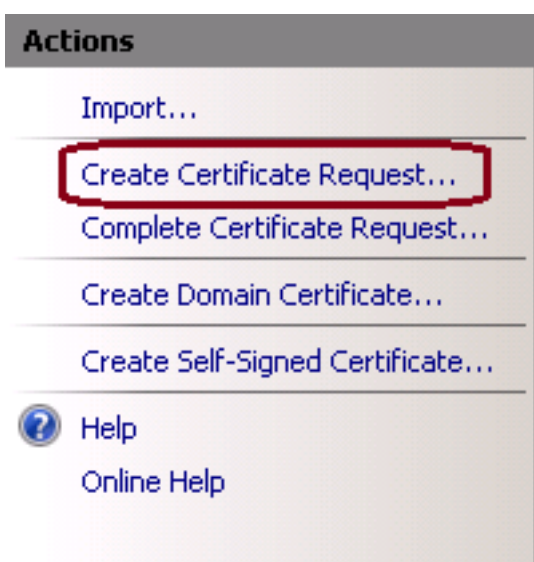
2. 如此镜像所显示，在连接窗口窗格中到左边，请选择服务器名。



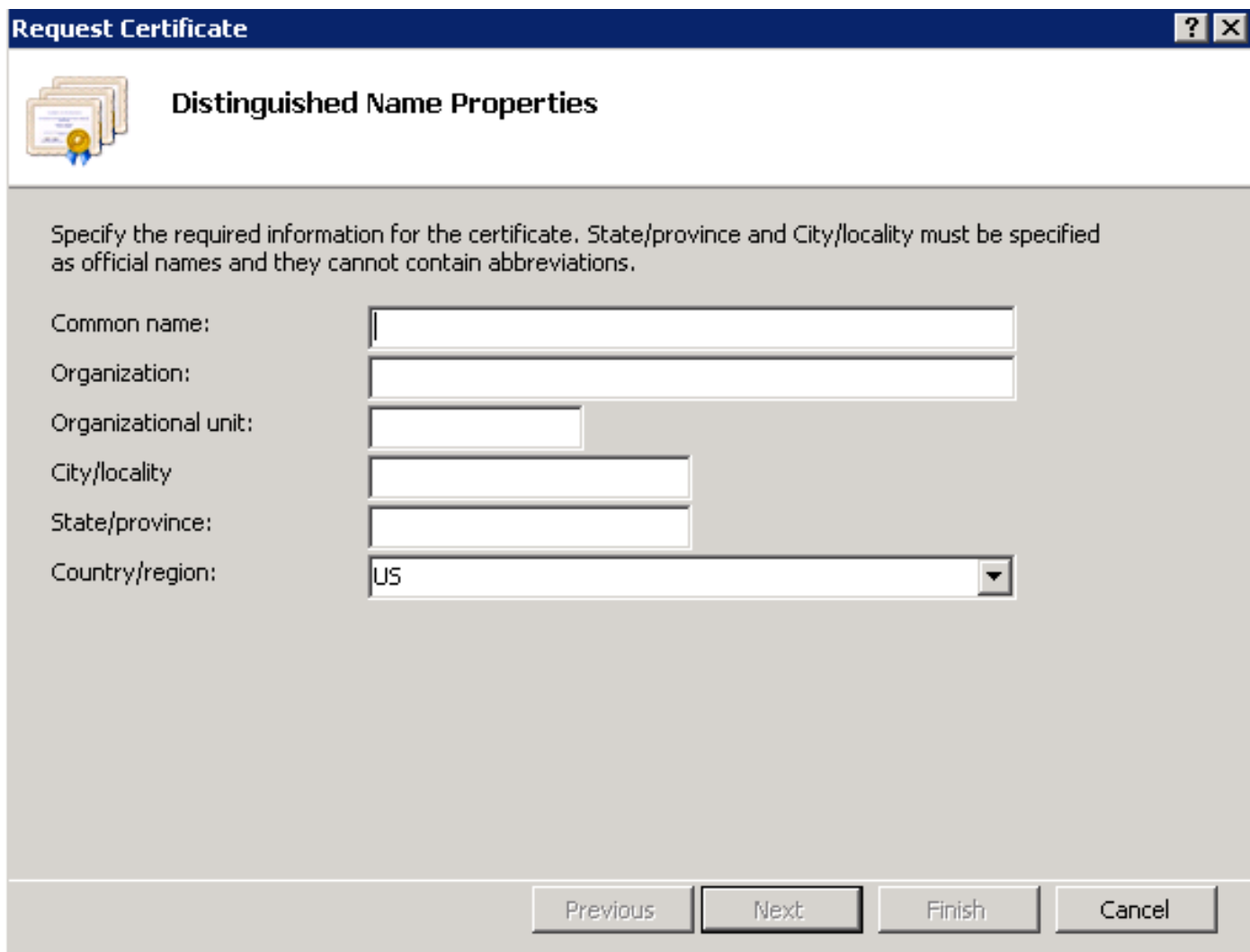
3. 在中间窗玻璃中，请选择IIS >Server证书。如此镜像所显示，双击服务器证书生成证书窗口。



4. 如此镜像所显示，在右窗格上，请点击操作>创建证书请求。

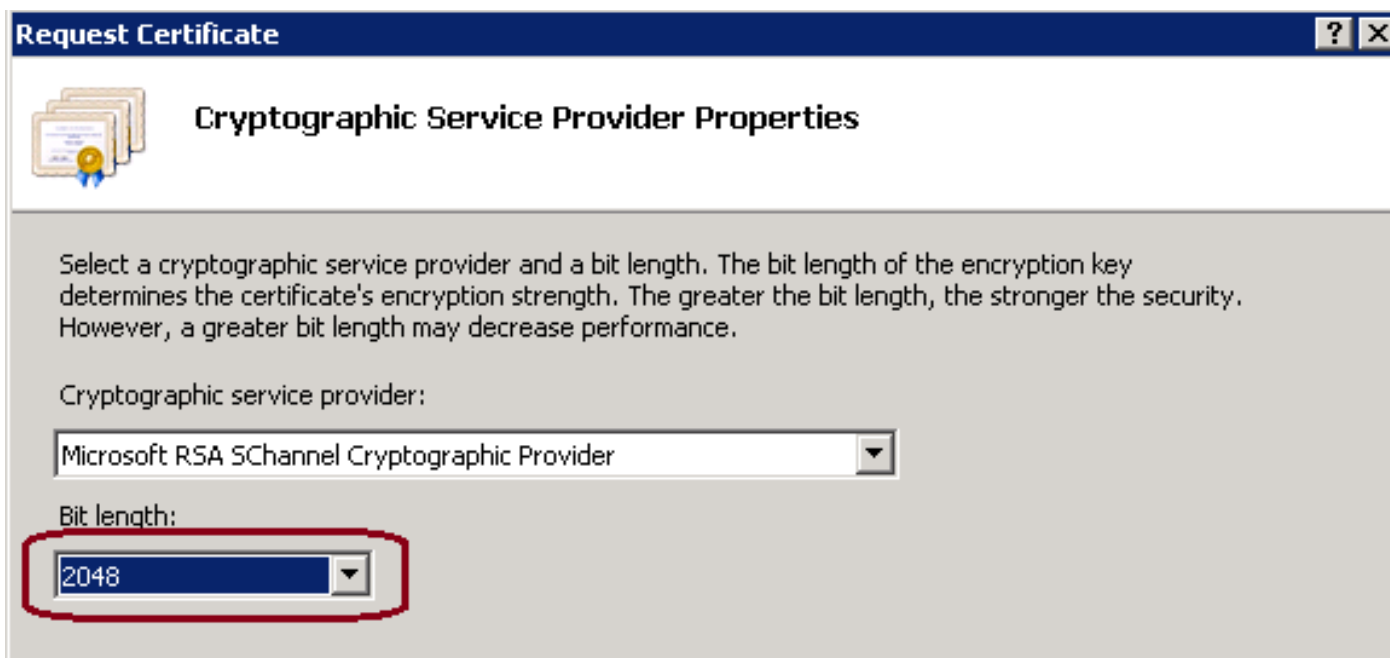


5. 如此镜像所显示，要完成证书请求，请输入在公用名称、组织、组织单位、城市/现场、州/省和国家/区域。



The screenshot shows a Windows dialog box titled "Request Certificate" with a sub-header "Distinguished Name Properties". The dialog contains a text area with instructions: "Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations." Below this are several input fields: "Common name:", "Organization:", "Organizational unit:", "City/locality", "State/province:", and "Country/region:". The "Country/region" dropdown menu is set to "US". At the bottom, there are four buttons: "Previous", "Next", "Finish", and "Cancel".

6. 在修改旁边单击密码如此镜像所显示，并且安全比特长度，推荐使用至少2048更加好的安全。



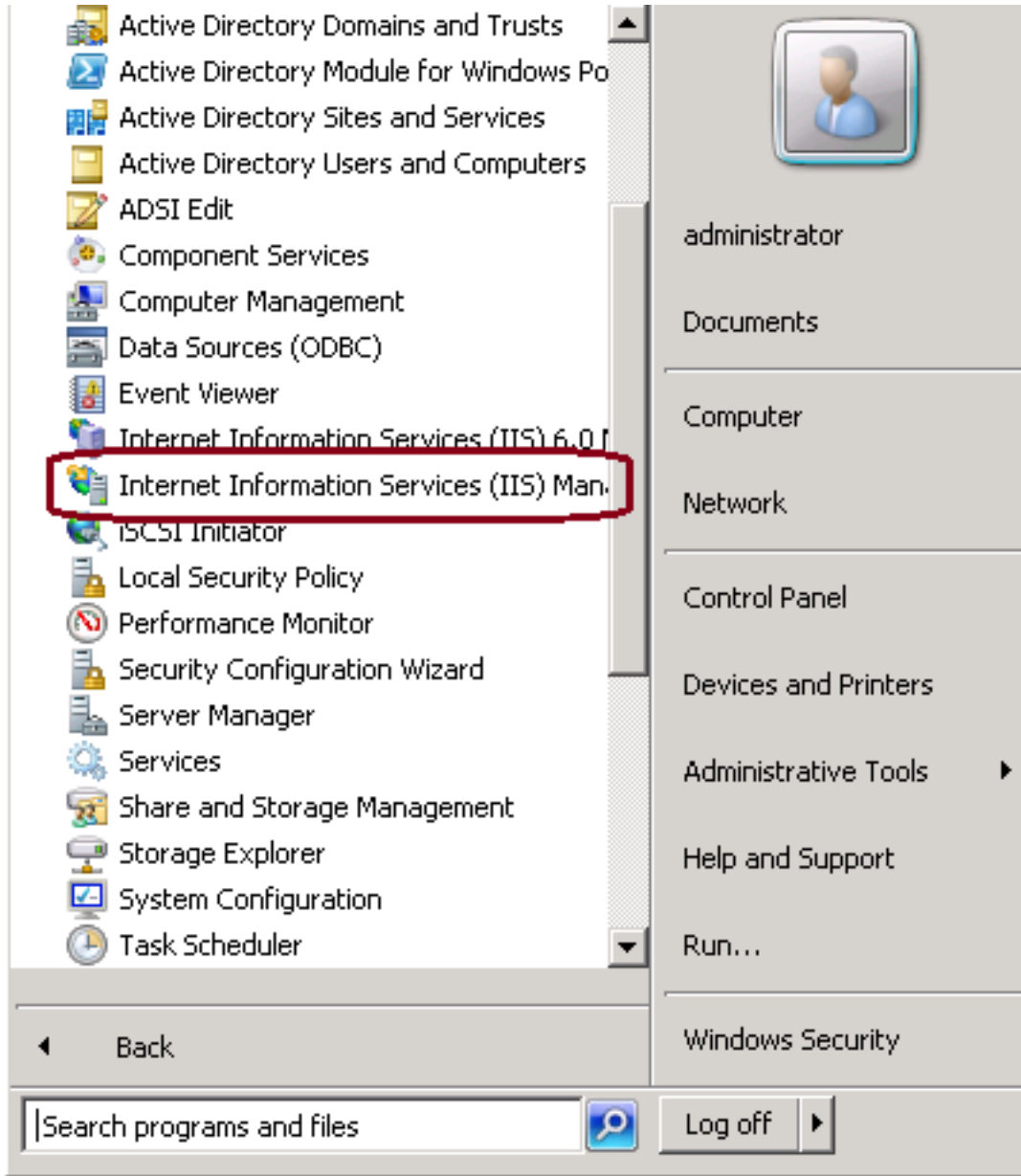
The screenshot shows a Windows dialog box titled "Request Certificate" with a sub-header "Cryptographic Service Provider Properties". The dialog contains a text area with instructions: "Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance." Below this are two dropdown menus: "Cryptographic service provider:" set to "Microsoft RSA SChannel Cryptographic Provider" and "Bit length:" set to "2048". The "Bit length" dropdown is highlighted with a red rectangle.

7. 如此镜像所显示，保存在将保存作为.TXT格式的所需位置的证书请求。

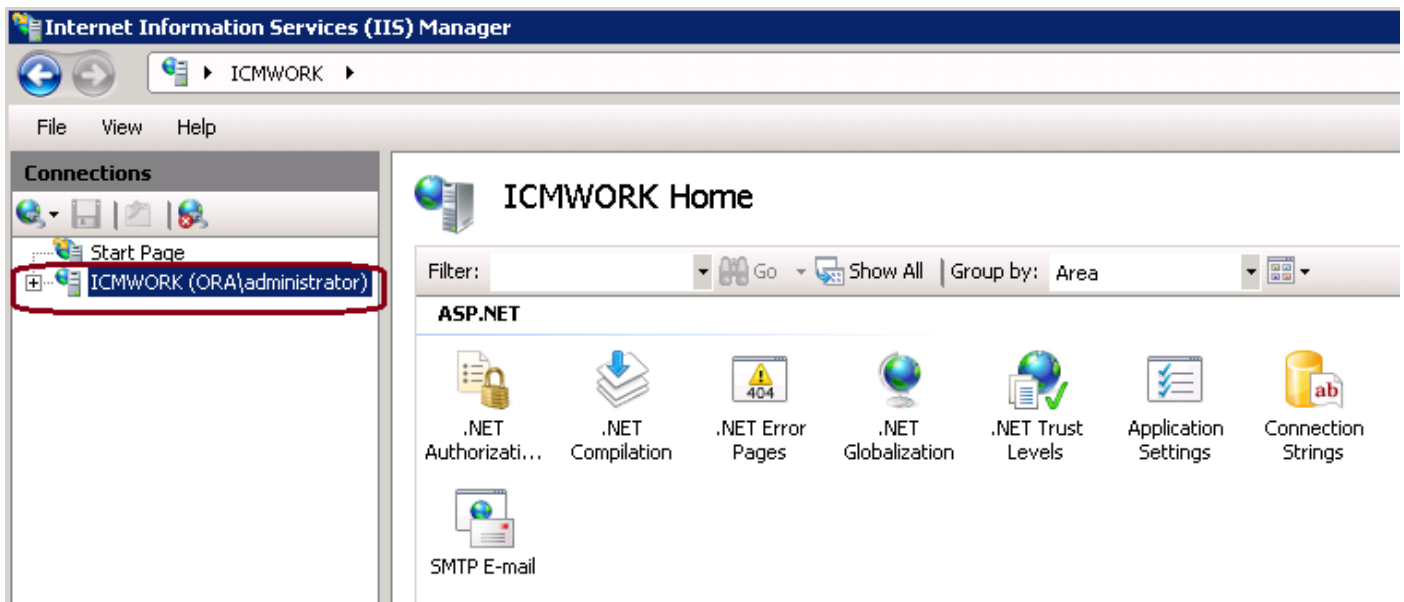
8. 提供管理内部CA或外部CA服务请求的团队将签字的此文件，如此镜像所显示。

## 步骤2.上传CA签名证书给互联网信息服务(IIS)管理器

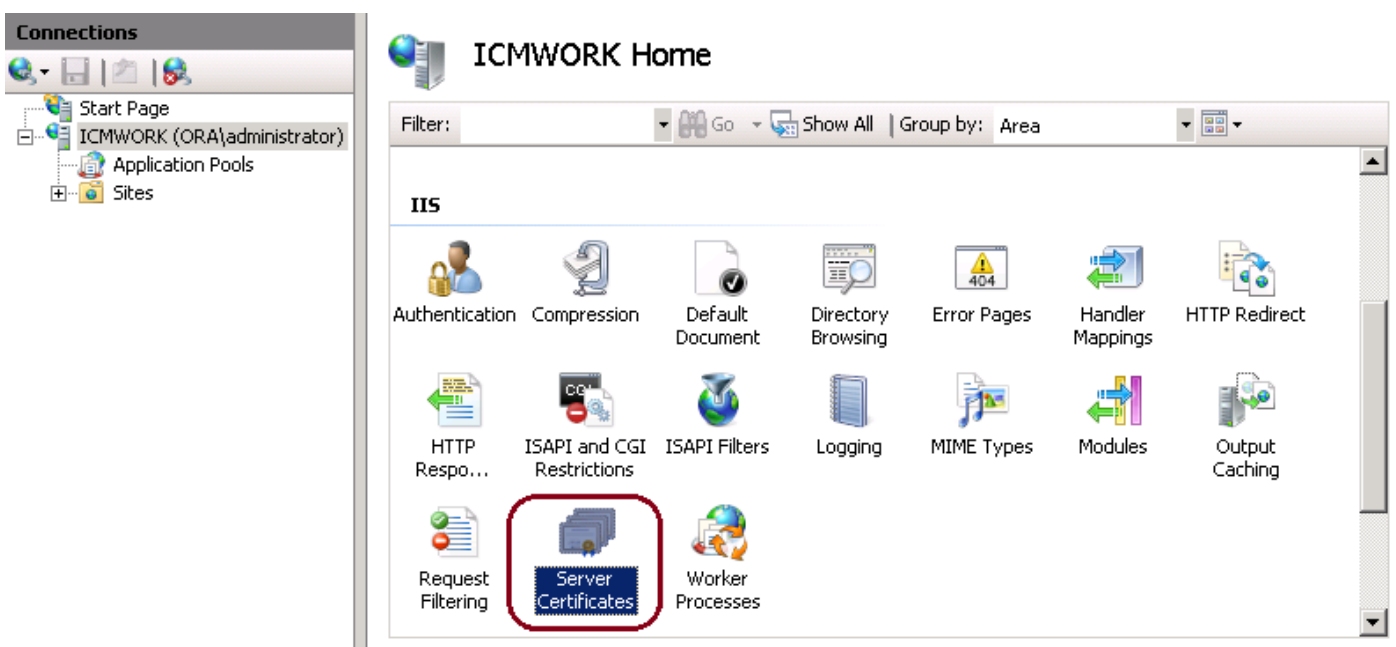
1.登录到Windows，单击Start > Run >所有Programs > Administrative工具> Internet信息服务(IIS)如此镜像所显示，管理器。如果存在，请勿选择IIS版本6。



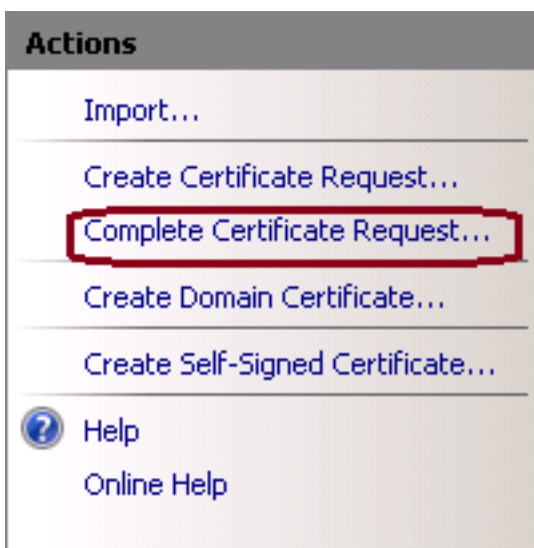
2. 如此镜像所显示，在连接窗口窗格中到左边，请选择服务器名。



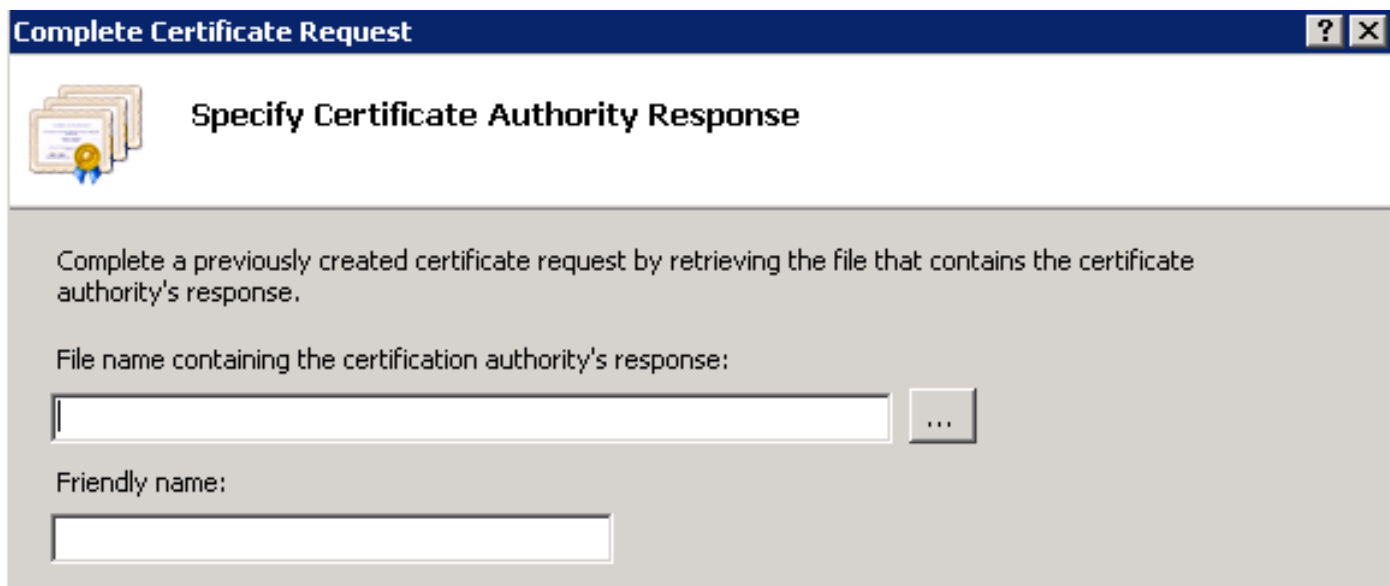
3. 在中间窗玻璃中，请选择IIS >Server证书。如此镜像所显示，双击服务器证书生成证书窗口。



4. 如此镜像所显示，在右窗格上，请点击操作>完整证书请求。



5. 在此步骤之前，请保证签名证书在.CER格式和上传到当地服务器。点击...按钮浏览.CER文件。如此镜像所显示，在友好名称里面，请使用服务器的FQDN。

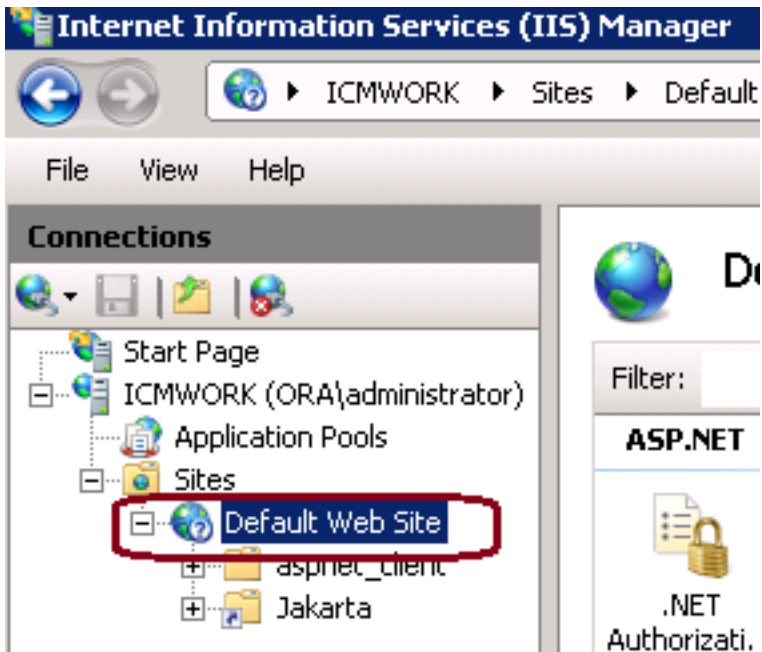


6. 点击OK键上传证书。如此镜像所显示，当完成时，请确认证书当前出现在服务器证书窗口。

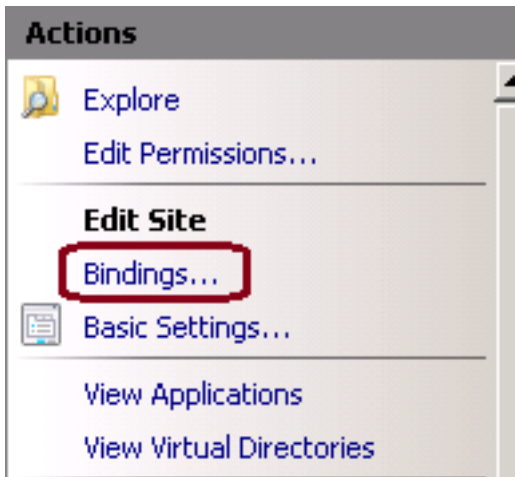


### 步骤3.绑定签字的CA证书到默认网站

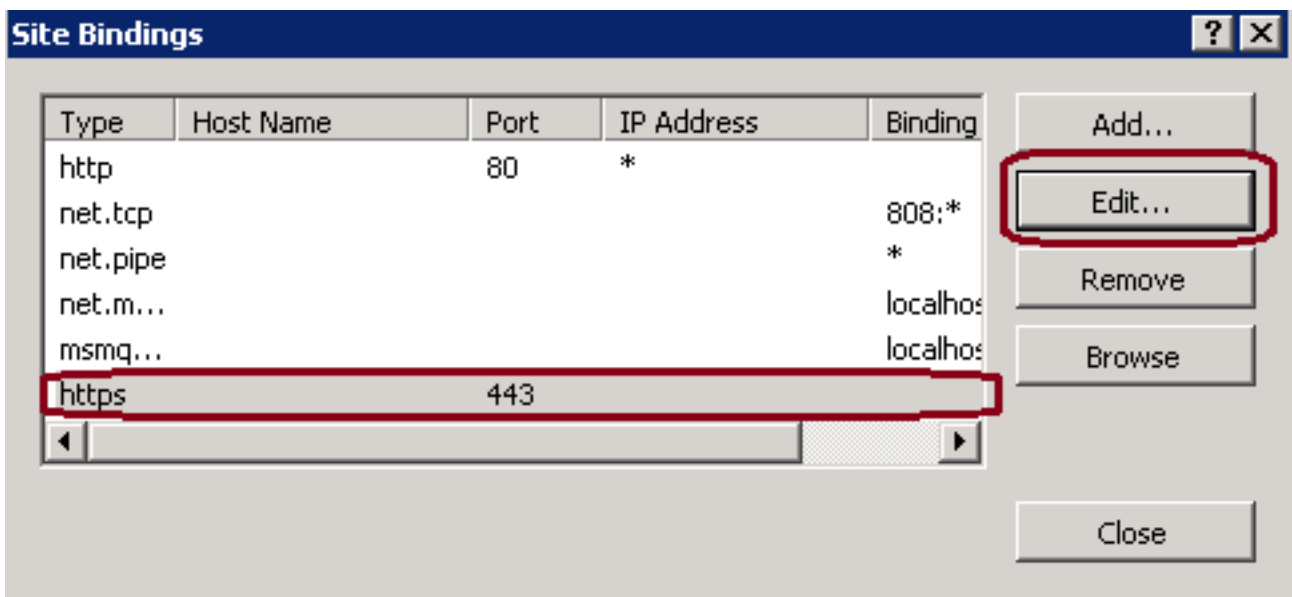
1. 如此镜像所显示，在连接窗口飞机下的IIS管理器，左手，点击<server\_name> >站点>默认网站。



2. 如此镜像所显示，在操作在右边的窗玻璃下，请点击捆绑。

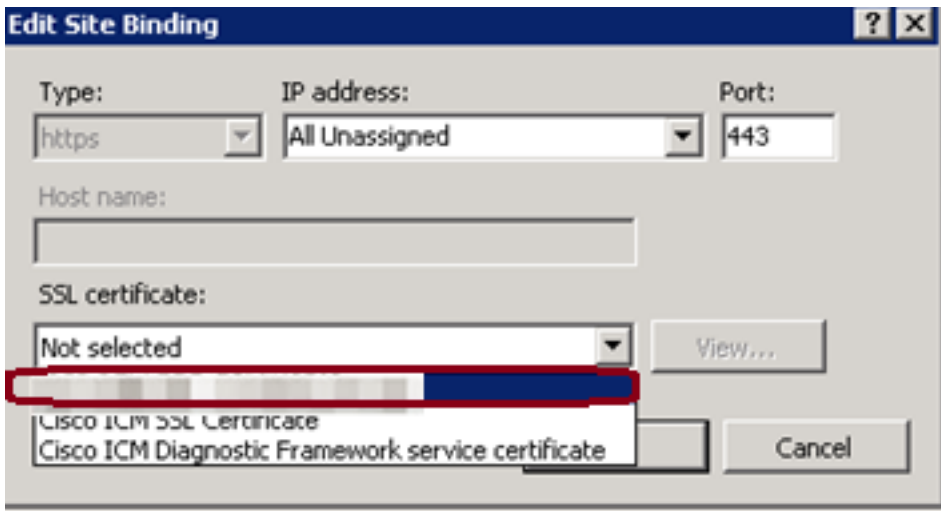


3. 在站点捆绑窗口，请点击https突出显示更多选项。如此镜像所显示，点击Edit继续。

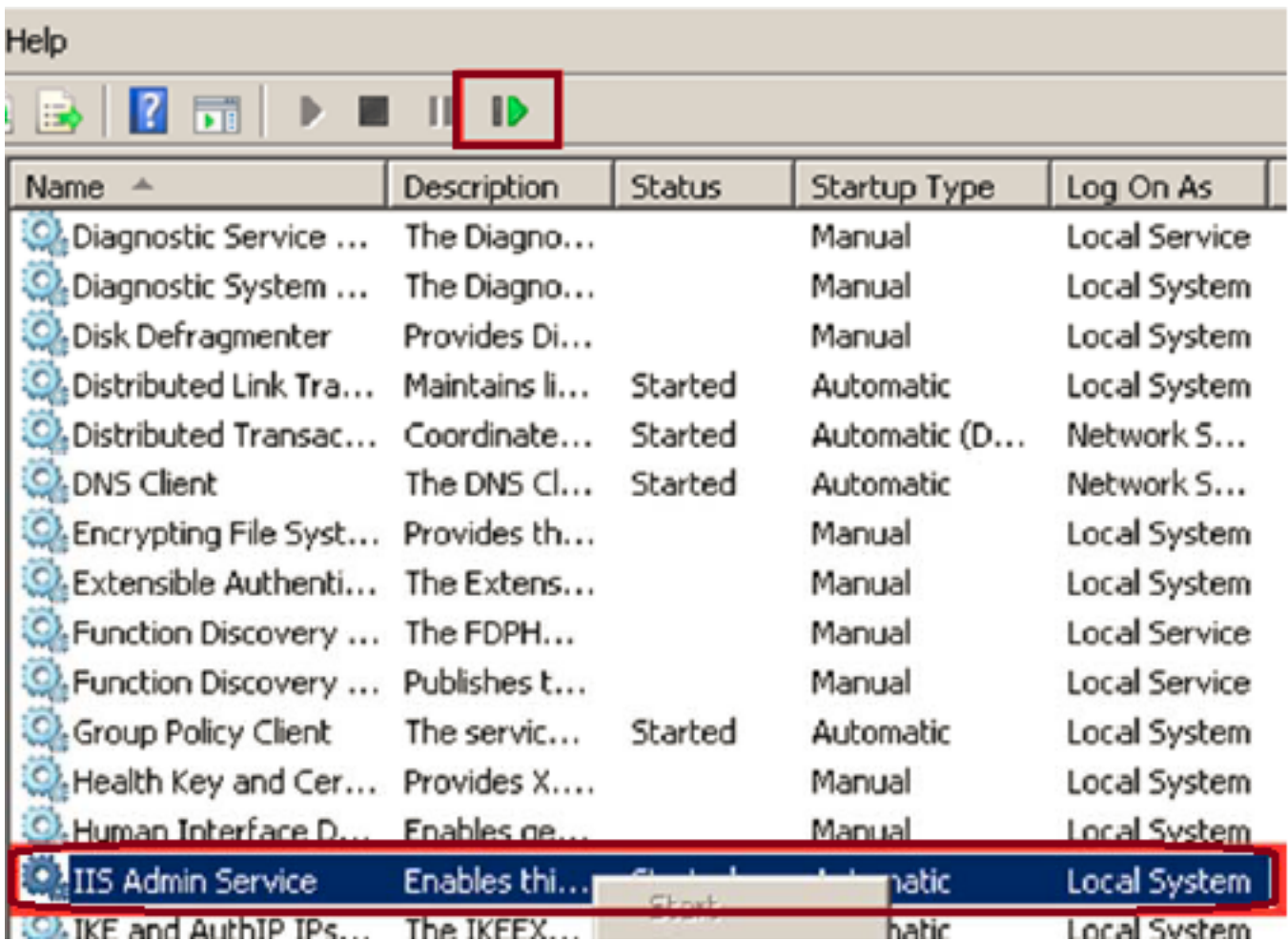


4. 在SSL验证参数下，请点击下箭头选择以前上传的签名证书。查看签名证书验证证书路径，并且值匹配当地服务器。如此镜像所显示，当完成请按OK，然后接近退出在站点捆绑窗口外面。





5. 重新启动IIS Admin服务在服务MMC管理单元下通过单击在Start > Run > services.msc。如此镜像所显示。



6. 如果成功，客户端Web浏览器不应该提示警告任何的验证错误，当输入在网站的时FQDN URL。

**注意：**如果IIS Admin服务未命中重新启动Web发布服务。

## 验证

当前没有可用于此配置的验证过程。

## 故障排除

目前没有针对此配置的故障排除信息。