# 用Certificate Authority (CA)签名的证书配置UCCE诊断的框架门廊工具的HTTPS访问

## Contents



## Introduction

本文描述关于怎样的配置流程安装统一的联系中心企业(UCCE)诊断的框架门廊工具的CA签名的证书。

## Prerequisites

### Requirements

Cisco 建议您了解以下主题：

- Active Directory
- 域名系统(DNS)服务器
- 配置和工作为所有服务器和客户端的CA基础设施
- 诊断的框架门廊

访问诊断的框架门廊工具通过键入在浏览器的IP地址没有收到认证警告是出于范围此条款。

### Components Used

本文档中的信息基于以下软件和硬件版本：

- Cisco UCCE 11.0.1
- 微软视窗服务器2012 R2

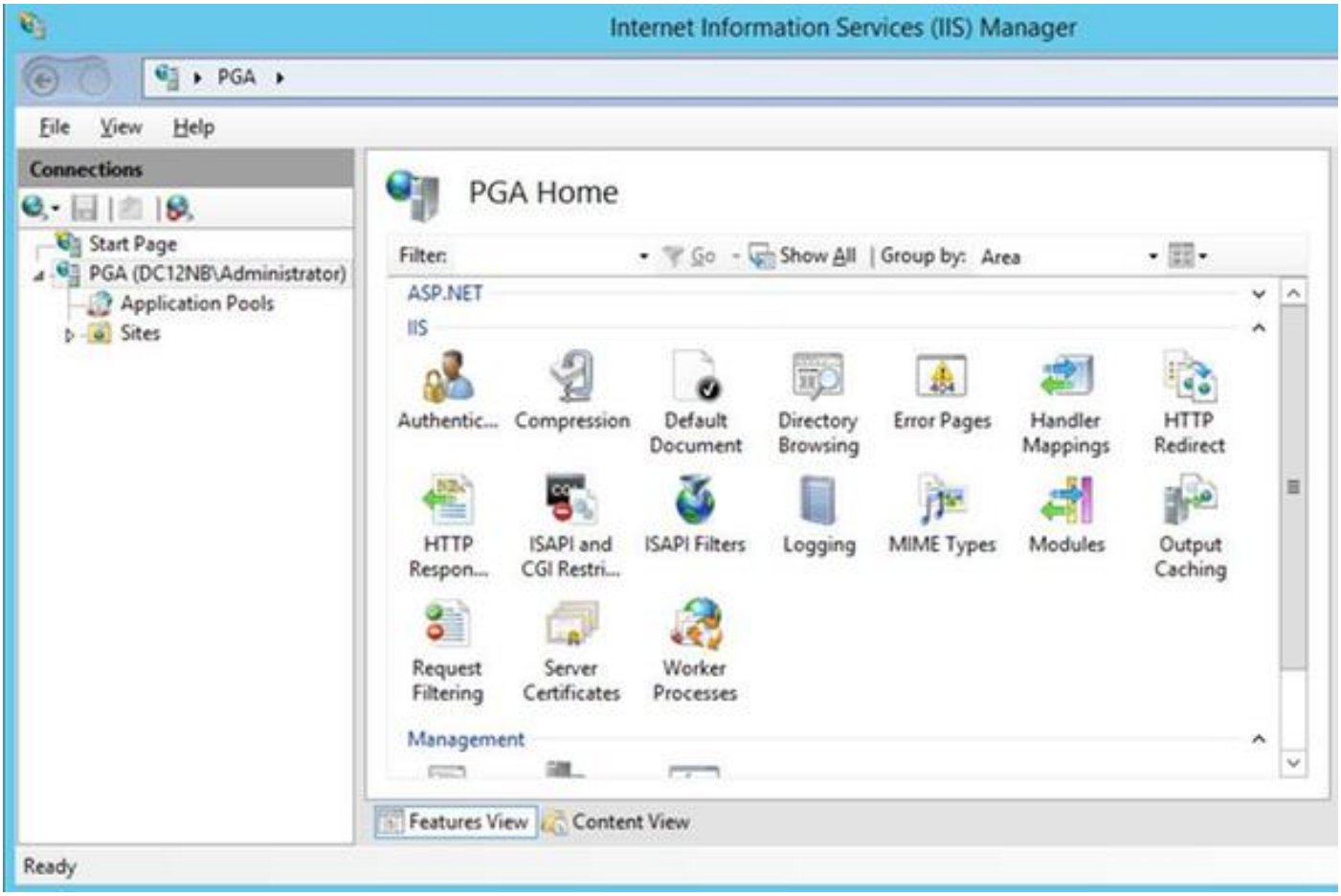
- 微软视窗服务器2012 R2认证机关
- 微软视窗7 SP1 OS

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

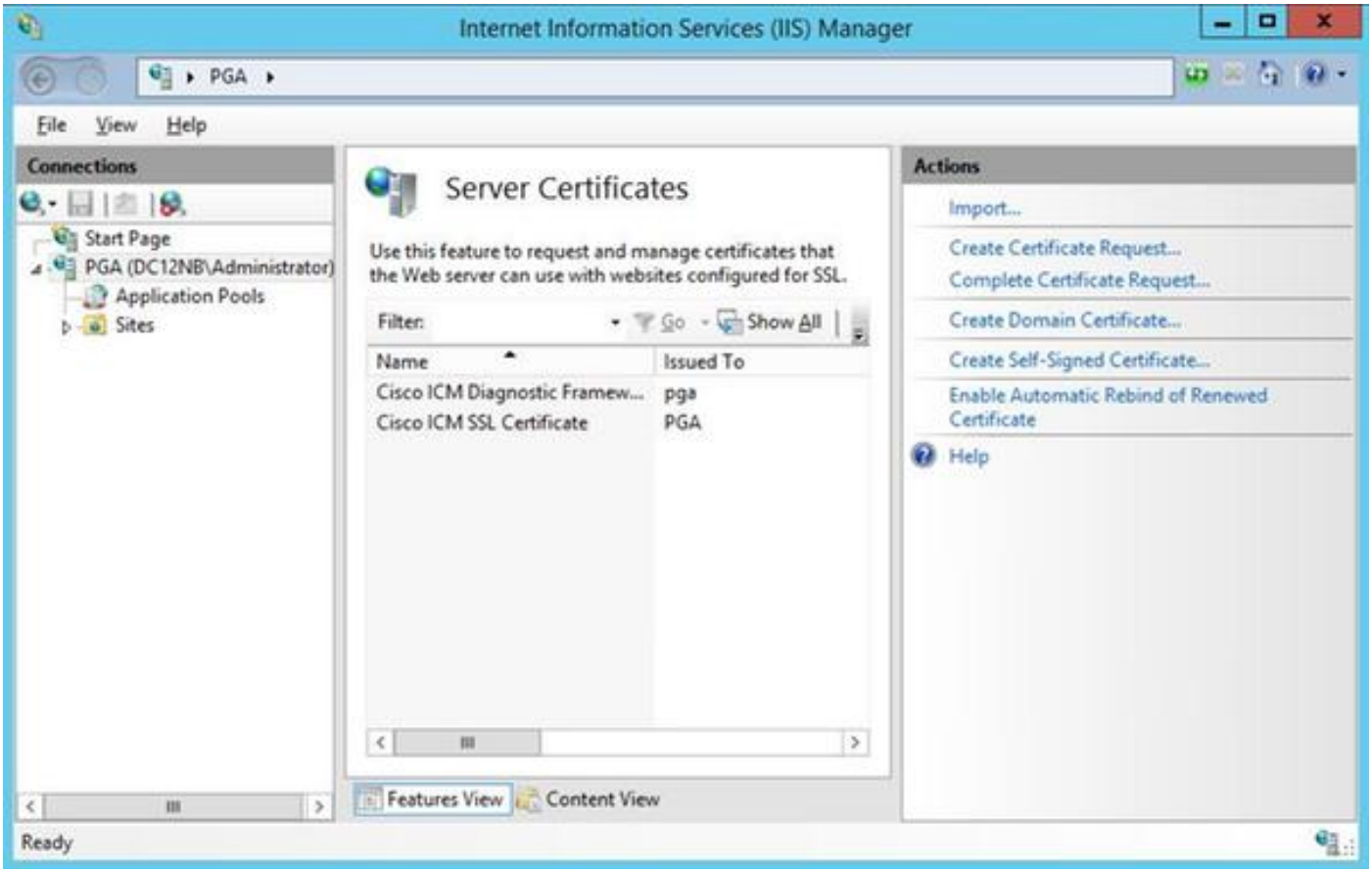
# Configure

## 生成认证签字的请求

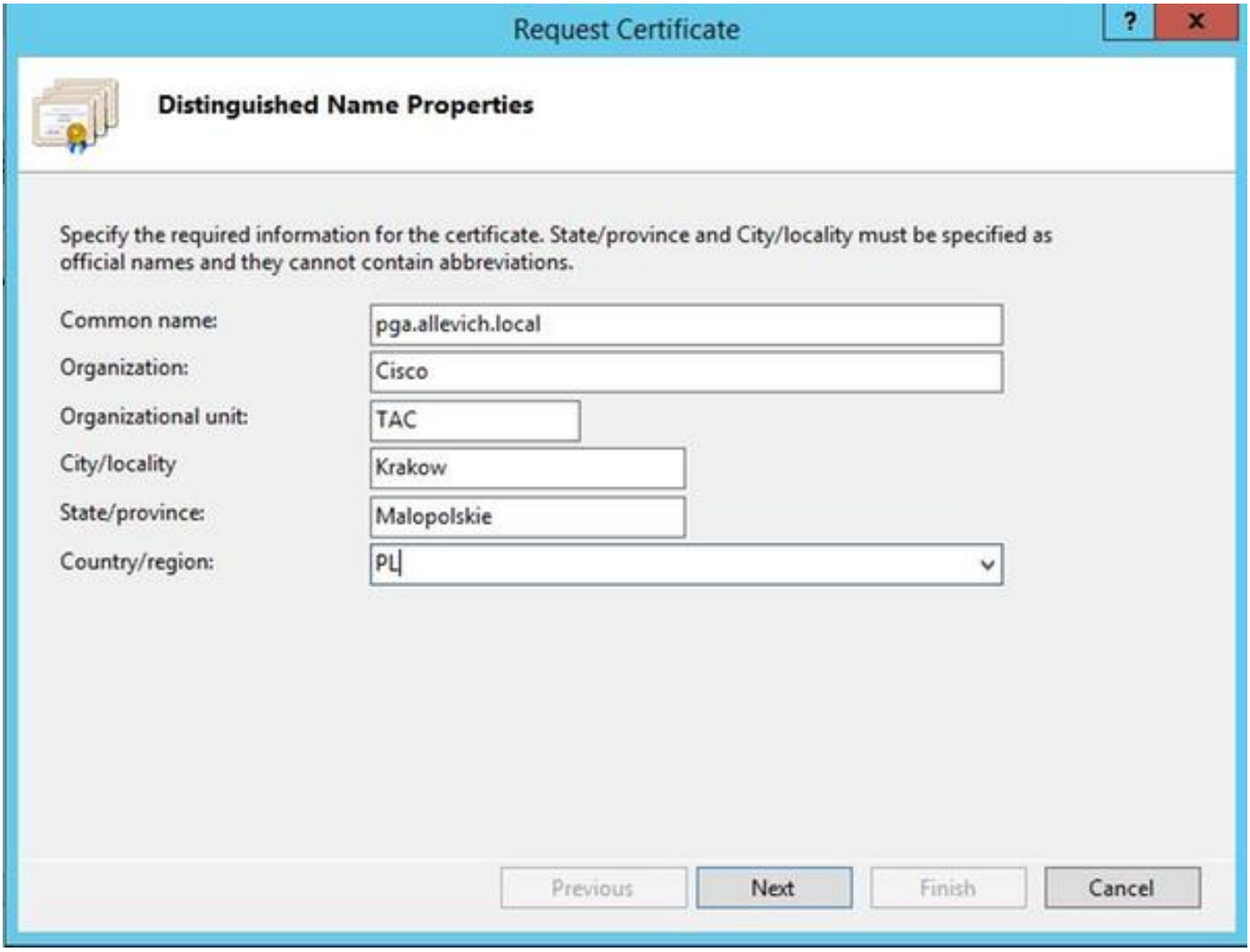
打开互联网信息服务(IIS)管理器，选择您的站点、外围网关A (PGA)在示例和**服务器证明**。




选择**创建**在动作面板的**证书请求**。



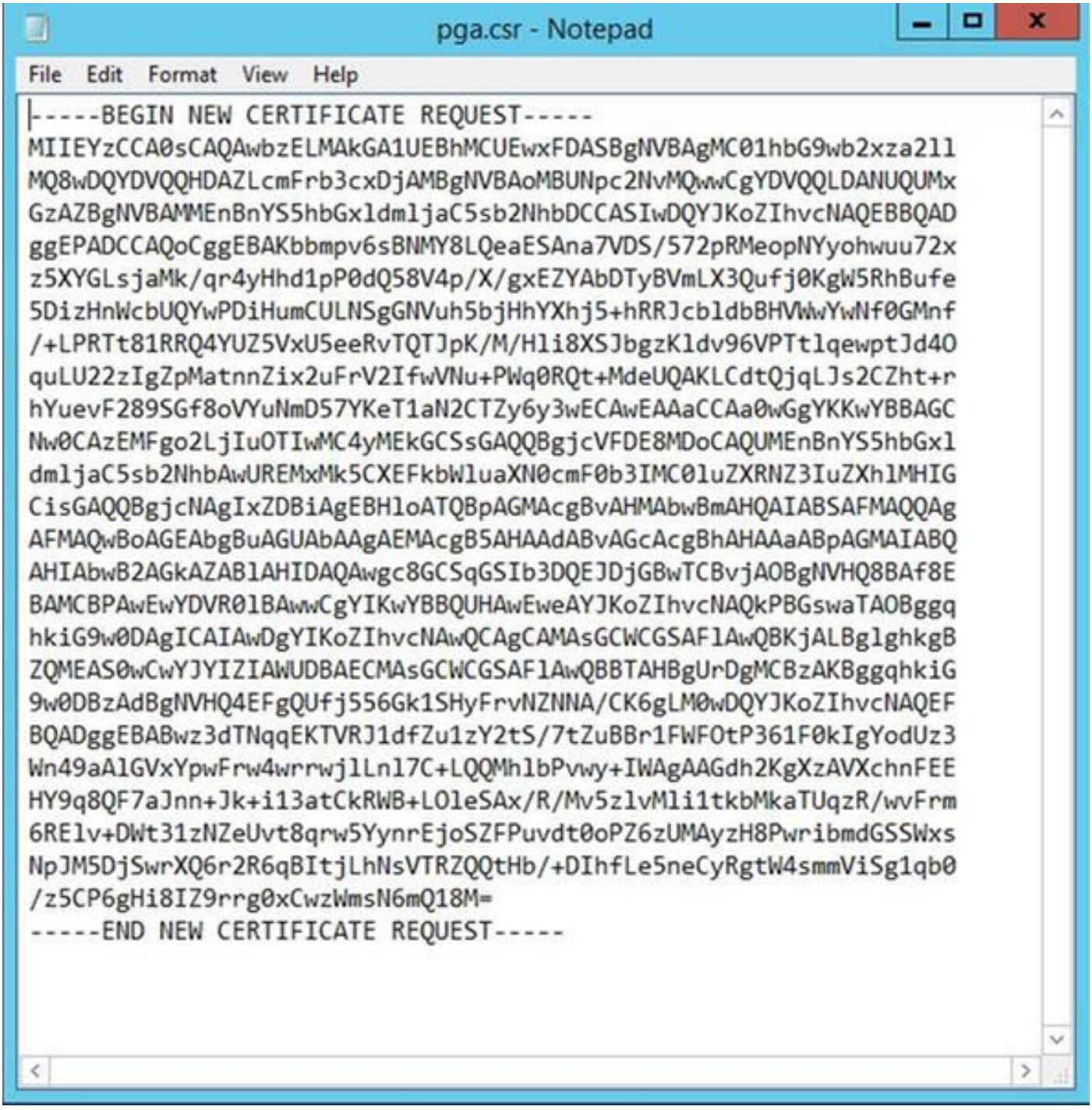

输入**共同名称(CN)**，**组织**(o)，**组织单位(OU)**，**现场**(l)，**状态**(ST)，**国家**(c)字段。普通的名字必须是相同的象您的完全合格的域名(FQDN)主机名- +域名。




留下密码服务提供商的默认设置并且指定比特长度：2048.

在哪里选择路径存储。例如在有pga.csr名字的桌面上。

打开在记事本的新建立的请求。




复制认证到与CTRL+C的缓冲区。

## 签署在认证机关的认证

**Note**:如果使用外部认证机关(类似GoDaddy)您需要与他们联系以后安排CSR文件生成。

签字对您的CA服务器证书登记页。
https:// <CA-server-address>/certsrv

Select请求**认证**，**先进的证书请求**和粘贴认证署名请求(CSR)内容对缓冲区。然后请选择**认证模板作为Web服务器**。

下载Base64编码的认证。

打开认证并且复制容量对最新使用方法的thumbprint字段。从thumbprint取消空间。

## 安装认证

### 复制认证

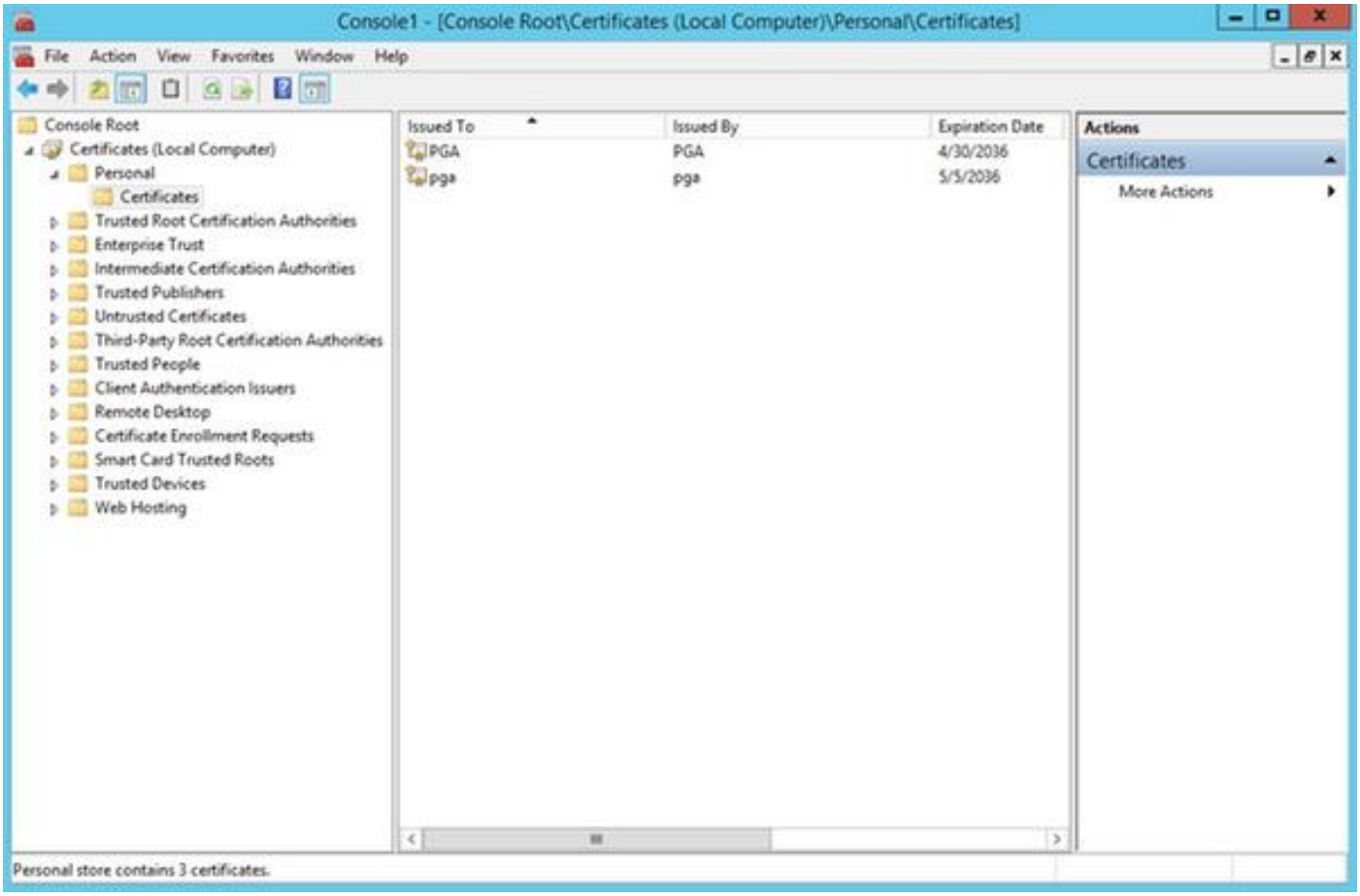
最近复制生成的证书文件到找出门廊工具的UCCE VM。

### 导入认证到本地计算机存储设备

在选择Start菜单，类型**运行**和**mmc的**同一个UCCE服务器生成微软管理控制台(MMC)控制台上。

点击 **添加/去除卡扣式，**并且在对话框请点击 **添加**。
然后请选择**证书**菜单并且添加。
在证书卡扣式对话框中，请点击**计算机帐户>本地计算机>完成**。

连接到个人证书文件夹。




在动作面中请选择**更多动作>所有任务>导入**。

点击**其次**，**访问**并且选择以前生成，并且在Next菜单请保证的认证证书存储设置对私有。在最后屏幕上请验证所选的**证书存储**和**证书文件**并且点击**完成**。

**捆绑IIS认证**

打开CMD应用程序。

连接到诊断的门廊家庭文件夹。

```
cd c:\icm\serviceability\diagnostics\bin
```

去除门廊工具的当前认证捆绑。

```
DiagFwCertMgr /task:UnbindCert
```

捆绑CA签名的证书。

**提示**：请使用某文本编辑(notepad++)取消在哈希的空间。

以被取消的空间使用以前被保存的哈希。

```
DiagFwCertMgr /task:BindCertFromStore /certhash:bc6bbe23b8b3a26d8446c252400f9264c5c30a29
```

万一认证顺利地一定您在输出中应该看到相似的线路。
“认证捆绑是有效的”
保证认证捆绑使用此命令是成功的。

```
DiagFwCertMgr /task:ValidateCertBinding
```

再次在输出中应该显示相似的消息。
“认证捆绑是有效的”

**Note**:默认情况下DiagFwCertMgr将使用端口7890。

重新启动诊断的框架服务。

```
sc stop "diagfwsvc"
sc start "diagfwsvc"
```

**提示**：服务列表，并且特别是门廊服务名称可以通过tasklist in命令CMD工具被检查。

```
tasklist /v
```

# Verify

打开诊断的框架页使用FQDN，并且不应该提示认证警告消息。

### 取消计划

万一丢失对门廓工具的访问您能重新生成自签证书和添加例外。
使用此命令，它可以执行。

```
DiagFwCertMgr /task:CreateAndBindCert
```

# Troubleshoot

请勿使用IP地址，当登录到诊断的框架门廓工具。因为FQDN必须与在Certificate CN字段，指定的值配比您仍然收到一个认证警告。

验证所有服务器与Ntp source同步。

```
w32tm /monitor
```

如果设法使用附属的代替名字(SAN)或椭圆曲线数字签名算法(EC DSA)或4096密钥长度认证-首先查出不是特定的到这些功能之一。

# 相关条款

UCCE \ PCCE -程序获得并上载Windows服务器自己-签字的或在2008个服务器的Certificate Authority (CA)认证
通过在操作系统Cisco的语音的CLI配置CA签名的证书(VOS)