使用CAC和智能卡读卡器配置VCS

目录

简介
先决条件
要求
使用的组件
背景信息
什么是智能卡？
配置
验证
故障排除

简介

本文档介绍安装和使用智能卡读卡器和通用访问卡登录以与思科视频通信服务器(VCS)配合使用的分步指南，适用于需要对VCS环境进行双因素身份验证的组织，如银行、医院或拥有安全设施的政府。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Cisco Expressway管理员(X14.0.2)。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

CAC提供所需的身份验证，以便“系统”了解谁获得了对其环境的访问权限，以及基础设施的物理或电子部分。在政府机密环境和其他安全网络中，“最不特权访问”或“需要知道”的规则占上风。任何人都可以使用登录，身份验证需要用户拥有的东西，然后CAC（也称为通用访问卡）于2006年问世，这样个人就无需拥有多个设备，无论他们是窝点、身份证还是连接器，就可以访问其工作地点或系统。

什么是智能卡？

智能卡是Microsoft用于集成到Windows平台的公钥基础设施(PKI)的关键组件，因为智能卡增强了仅软件解决方案，如客户端身份验证、登录和安全电子邮件。智能卡是公钥证书和关联密钥的融合点

，因为它们：

- 提供防篡改存储，以保护私钥和其他形式的个人信息。
- 隔离安全关键型计算，包括身份验证、数字签名和密钥交换，与系统中不需要知道的其他部分。
- 在工作、家庭或旅途中的计算机之间实现凭证和其他私有信息的可移植性。

智能卡已成为Windows平台不可或缺的一部分，因为智能卡提供了新的、可取的功能，与鼠标或CD-ROM的引入一样，对计算机行业具有革命性的意义。 如果您目前没有内部PKI基础设施，则需要确保您先执行此操作。本文档不涉及在本特定文章中安装此角色，但有关如何实施此角色的信息，请参阅：http://technet.microsoft.com/en-us/library/hh831740.aspx。

配置

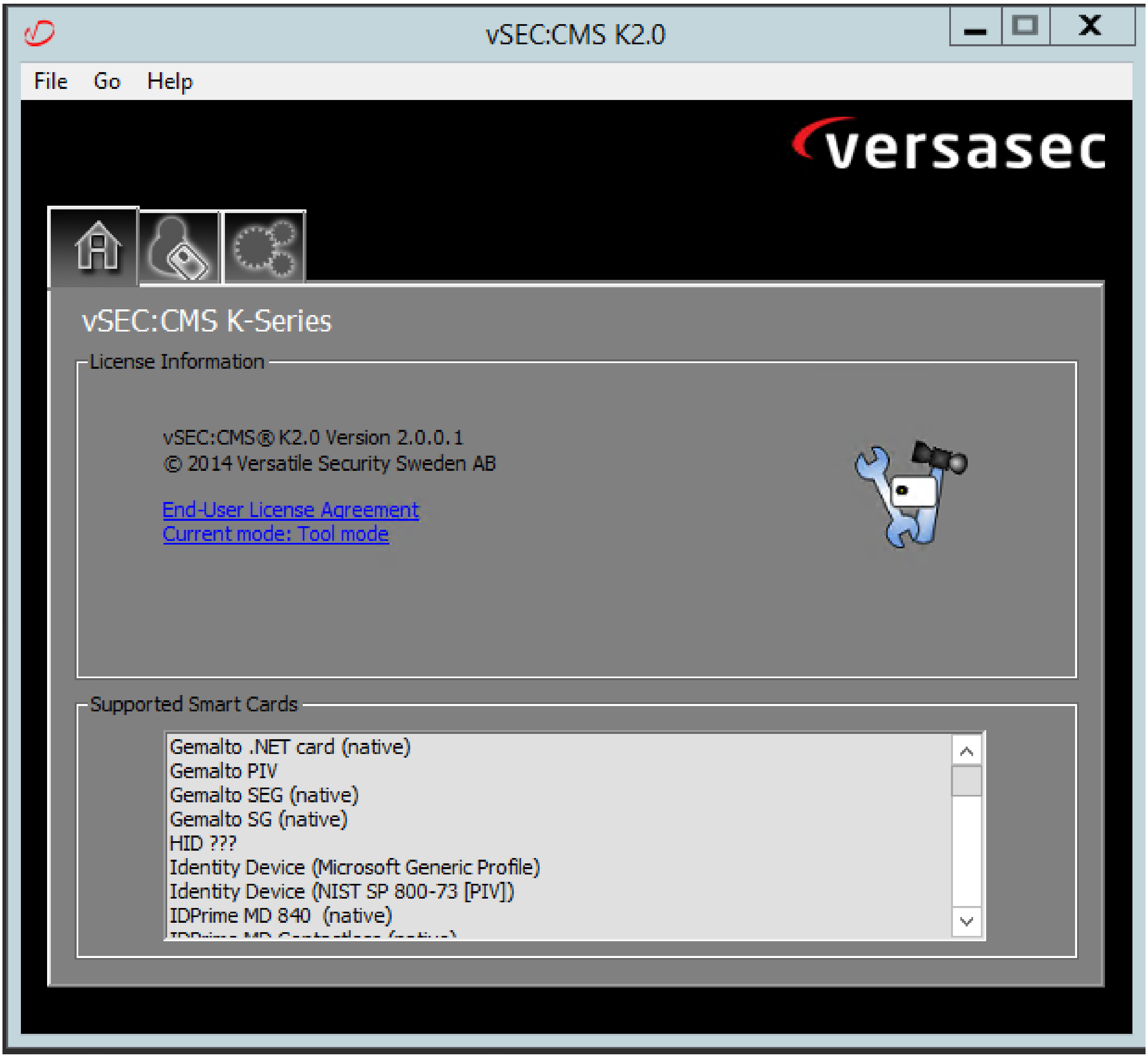
本实验假定您已将LDAP与VCS集成，并且拥有可以使用LDAP凭证登录的用户。

1. 实验设备
2. 安装智能卡
3. 配置证书颁发机构模板
4. 注册注册代理证书
5. 代表……注册
6. 配置VCS以使用通用接入卡

需要的设备:

Windows 2012R2域服务器，具有以下角色/已安装软件：

- 认证中心
- Active Directory
- DNS
- 连接了智能卡的Windows PC
- vSEC:CMS K系列管理软件，用于管理您的智能卡：



vSEC:CMS K-Series

License Information

vSEC:CMS® K2.0 Version 2.0.0.1
© 2014 Versatile Security Sweden AB

End-User License Agreement
Current mode: Tool mode

Supported Smart Cards

Gemalto .NET card (native)
Gemalto PIV
Gemalto SEG (native)
Gemalto SG (native)
HID ???
Identity Device (Microsoft Generic Profile)
Identity Device (NIST SP 800-73 [PIV])
IDPrime MD 840 (native)

Versa读卡器软件

安装智能卡

智能卡读卡器通常随附有关如何连接任何必要电缆的说明。以下是此配置的安装示例。

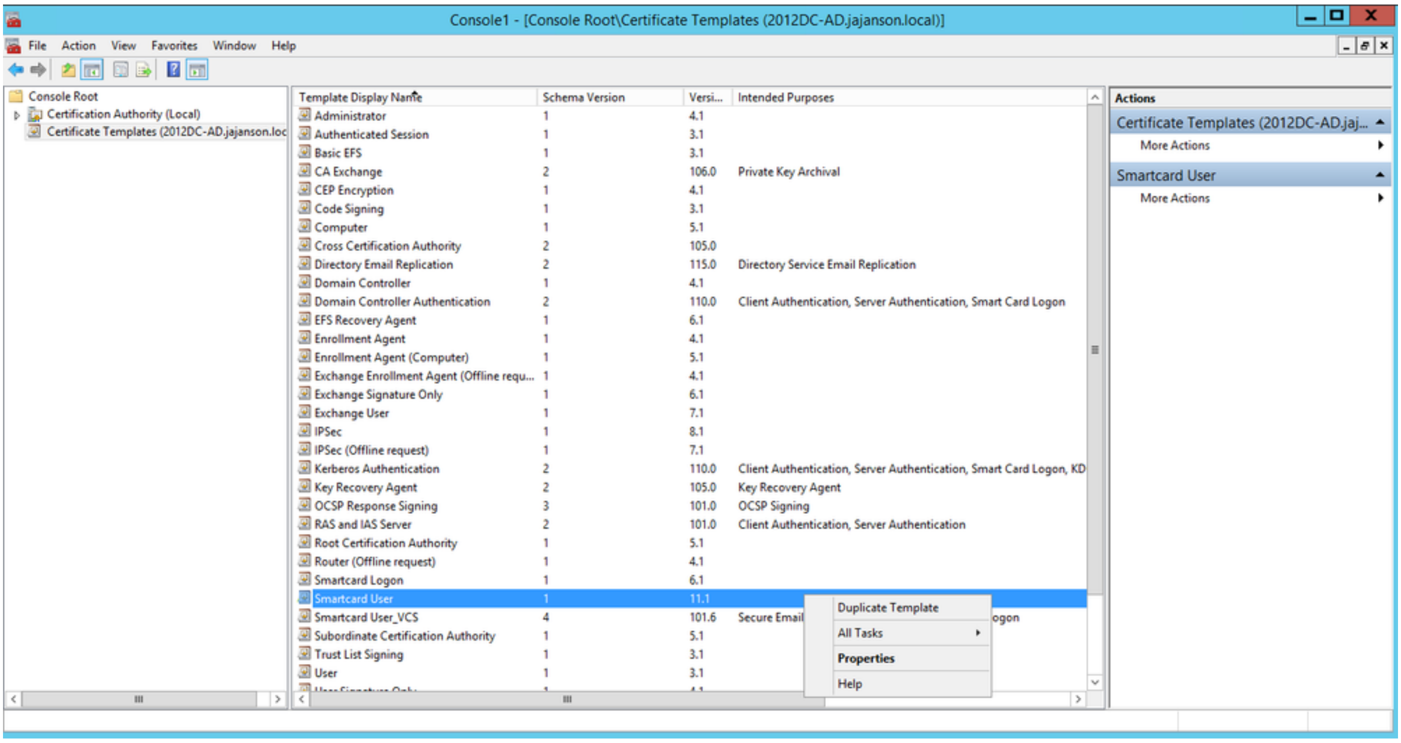
如何安装智能卡读卡器设备驱动程序

如果检测到并安装了智能卡读卡器，“欢迎使用Windows”登录屏幕会确认这一点。否则：

1. 将智能卡连接到Windows PC上的USB端口
2. 按照屏幕上的说明安装设备驱动程序软件。这需要在Windows中发现制造智能卡或驱动程序的驱动程序介质。在我的案例中，我使用了下载站点中的制造商驱动程序。**不要信任WINDOWS**。
3. 右键单击桌面上**的“My Computer(我**的电脑)”图标，然后单击子**菜单**上的“Manage（管理）”。
4. 展开“服**务和应用程**序”节点，然后单**击“服务**”。
5. 在右窗格中，右键单击**智能卡**。单击子**菜单**上的“属性”。
6. 在“常**规”**选项卡上，**在“**启动类型”下**拉列表中选择“自动”。**Click **OK**.
7. 如果硬件向导指示您重新启动计算机，请重新启动计算机。

配置证书颁发机构模板

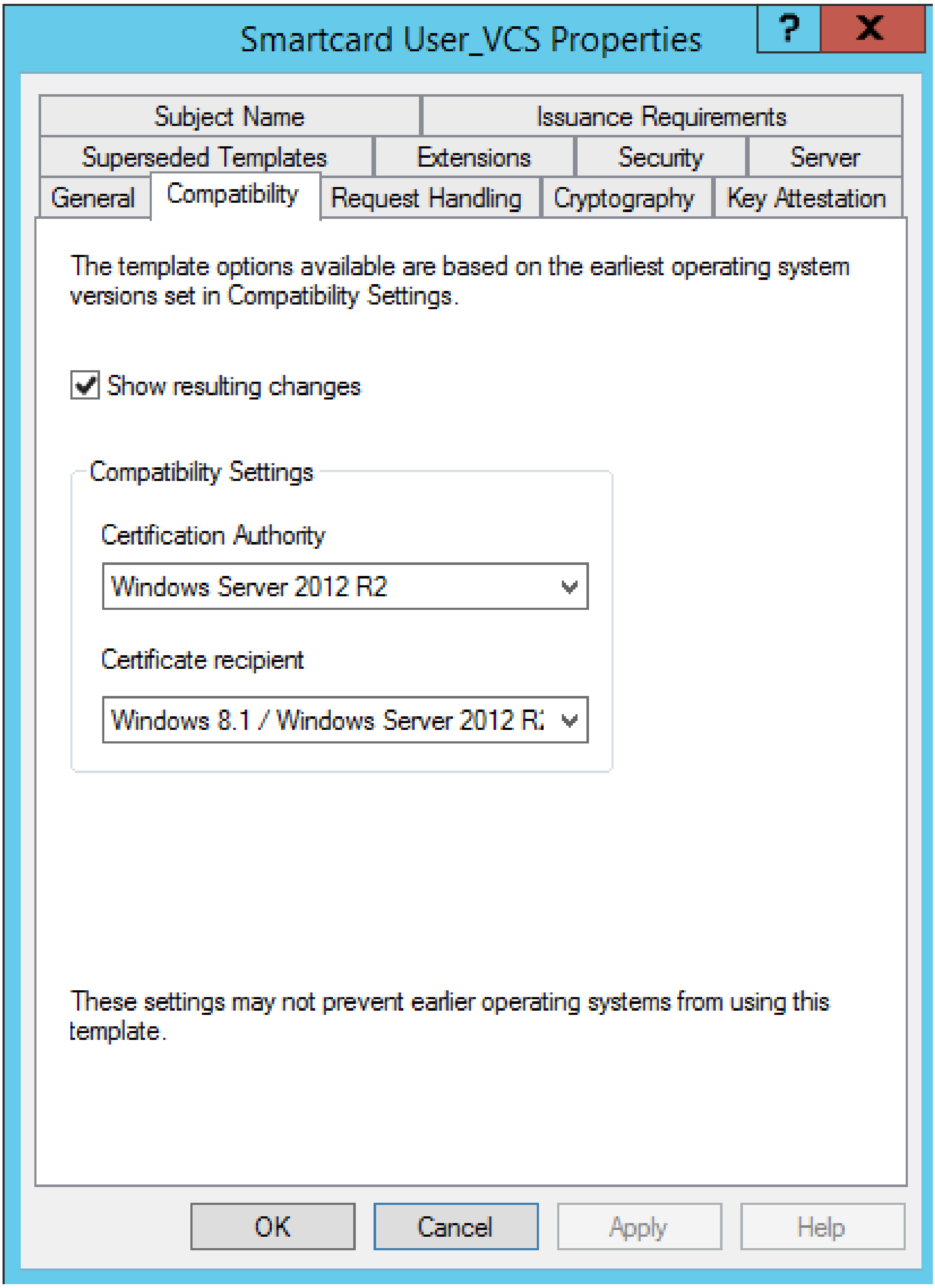
1. 从管理工具启动证书颁发机构MMC。
2. 单击或选择“证**书模板**”节点，然后**选择Manage**。
3. 右键单击或选择“Smartcard User Certificate Template**(智能卡用**户证书模板)”，然后选**择** **“**Duplicate（复制）”，如图所示。


Console1 - [Console Root\Certificate Templates (2012DC-AD.jajanson.local)]
File
Action
View
Favorites
Window
Help
Console Root
Certification Authority (Local)
Certificate Templates (2012DC-AD.jajanson.loc
Actions
Certificate Templates (2012DC-AD.jaj...
More Actions
Smartcard User
More Actions
Duplicate Template
All Tasks
Properties
Help

Template Display Name	Schema Version	Versi...	Intended Purposes
Administrator	1	4.1	
Authenticated Session	1	3.1	
Basic EFS	1	3.1	
CA Exchange	2	106.0	Private Key Archival
CEP Encryption	1	4.1	
Code Signing	1	3.1	
Computer	1	5.1	
Cross Certification Authority	2	105.0	
Directory Email Replication	2	115.0	Directory Service Email Replication
Domain Controller	1	4.1	
Domain Controller Authentication	2	110.0	Client Authentication, Server Authentication, Smart Card Logon
EFS Recovery Agent	1	6.1	
Enrollment Agent	1	4.1	
Enrollment Agent (Computer)	1	5.1	
Exchange Enrollment Agent (Offline requ...	1	4.1	
Exchange Signature Only	1	6.1	
Exchange User	1	7.1	
IPSec	1	8.1	
IPSec (Offline request)	1	7.1	
Kerberos Authentication	2	110.0	Client Authentication, Server Authentication, Smart Card Logon, KD
Key Recovery Agent	2	105.0	Key Recovery Agent
OCSP Response Signing	3	101.0	OCSP Signing
RAS and IAS Server	2	101.0	Client Authentication, Server Authentication
Root Certification Authority	1	5.1	
Router (Offline request)	1	4.1	
Smartcard Logon	1	6.1	
Smartcard User	1	11.1	
Smartcard User_VCS	4	101.6	Secure Email ogon
Subordinate Certification Authority	1	5.1	
Trust List Signing	1	3.1	
User	1	3.1	
User Signature Only	1	4.1	

域控制器证书模板

4.在“兼容性”**选项**卡的“证**书颁发机**构”下，查看选择并根据需要进行更改。



The template options available are based on the earliest operating system versions set in Compatibility Settings.

☑ Show resulting changes

Compatibility Settings

Certification Authority

Windows Server 2012 R2

Certificate recipient

Windows 8.1 / Windows Server 2012 R:

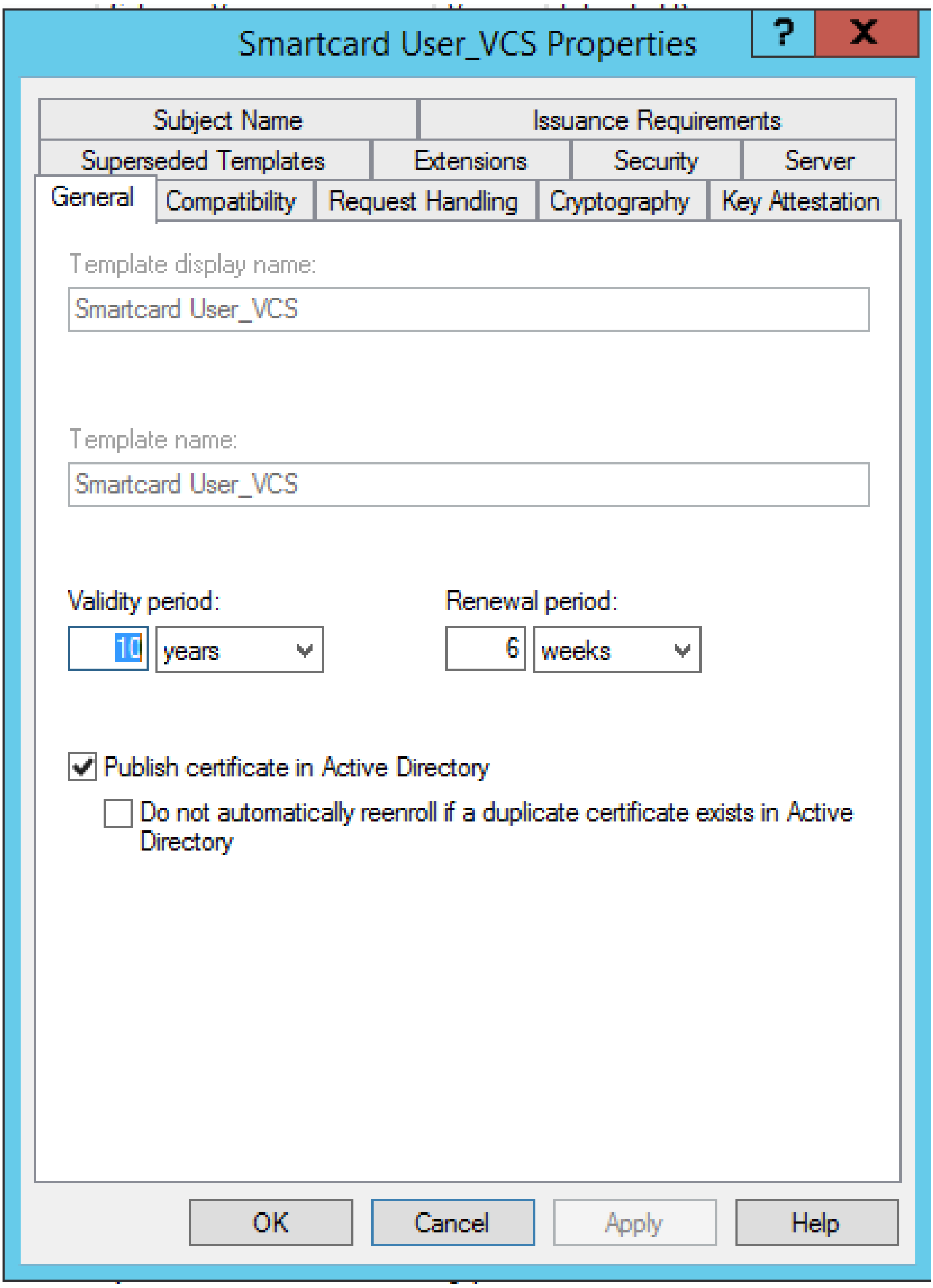
These settings may not prevent earlier operating systems from using this template.

智能卡兼容性设置

5.在“一般信息”**选项卡**上：

a.指定名称，如**Smartcard User_VCS**。

b.将有效期设置为所需值。单击 **Apply**。



Smartcard User_VCS Properties

Template display name: Smartcard User_VCS

Template name: Smartcard User_VCS

Validity period: 10 years

Renewal period: 6 weeks

☑ Publish certificate in Active Directory

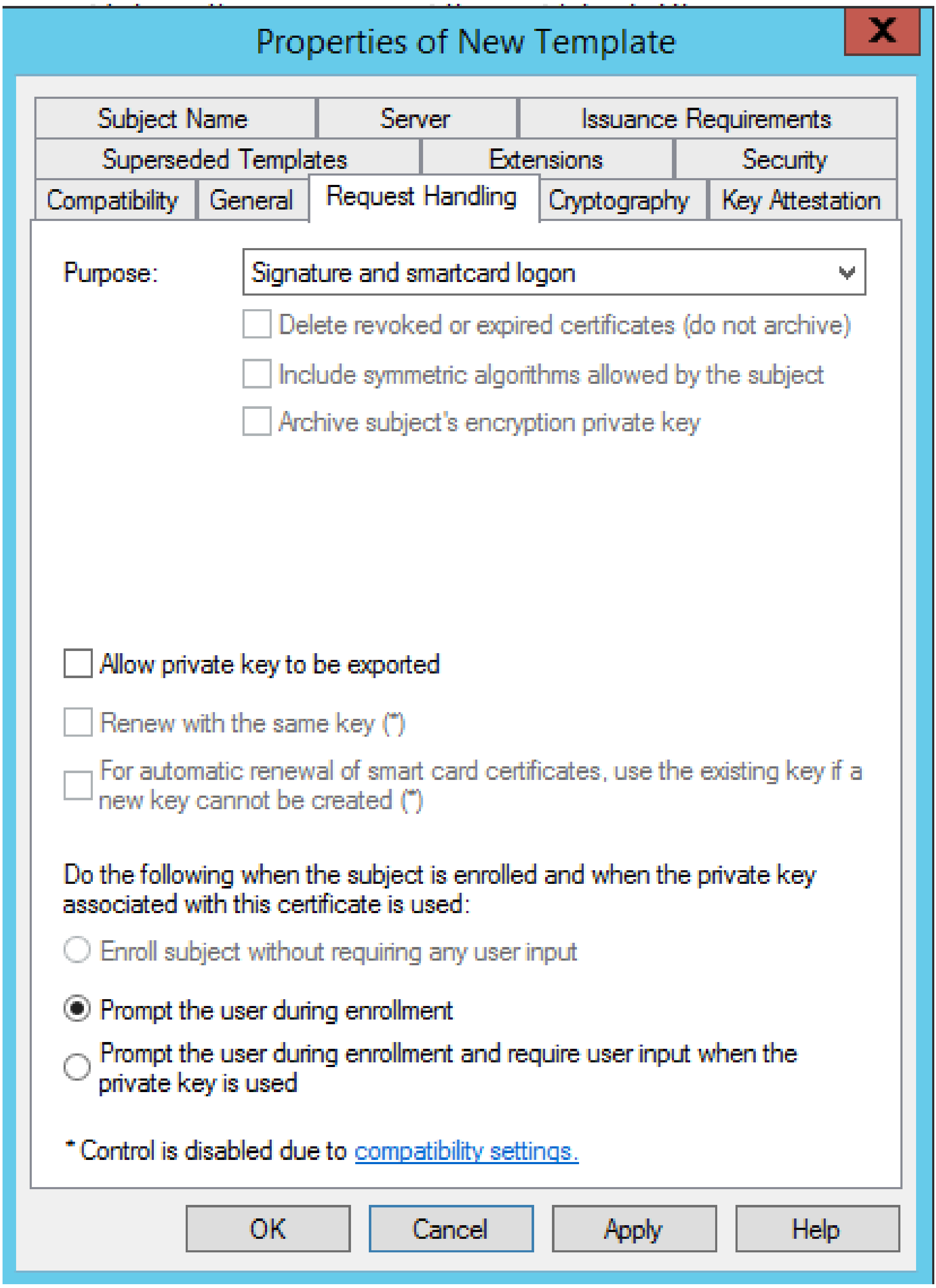
□ Do not automatically reenroll if a duplicate certificate exists in Active Directory

智能卡一般时间开始到期

6.在“请求处**理”选**项卡上：

a.设置“**Purpose to** Signature and **smartcard logon**”。

b.单击**Prompt the user during enrollment。**单击 **Apply**。



Purpose: Signature and smartcard logon

□ Delete revoked or expired certificates (do not archive)

□ Include symmetric algorithms allowed by the subject

□ Archive subject's encryption private key

□ Allow private key to be exported

□ Renew with the same key (*)

□ For automatic renewal of smart card certificates, use the existing key if a new key cannot be created (*)

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

○ Enroll subject without requiring any user input

● Prompt the user during enrollment

○ Prompt the user during enrollment and require user input when the private key is used

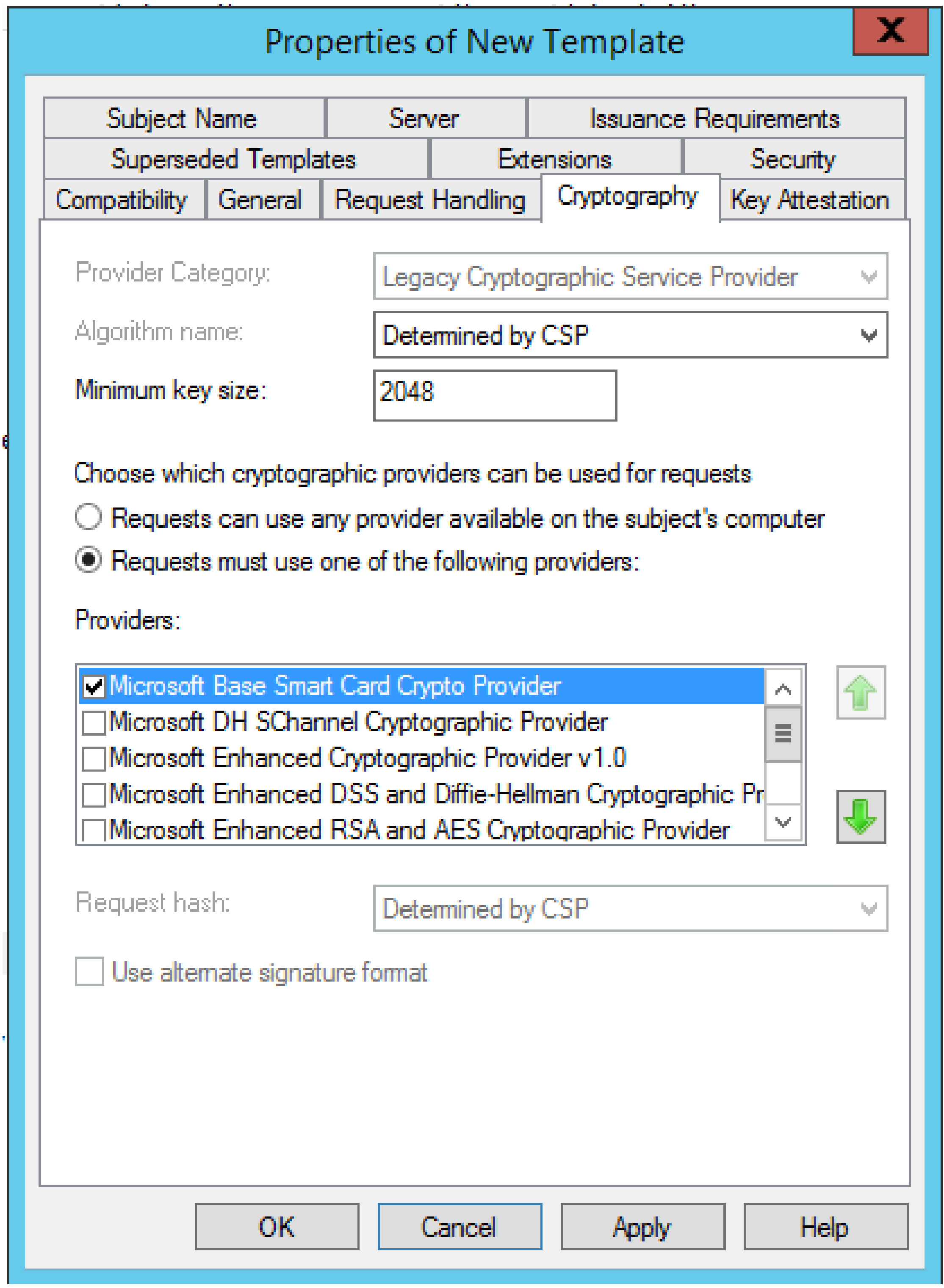
* Control is disabled due to compatibility settings.

智能卡请求处理

7.在“加密”**选项**卡上，将最小密钥大小设置为2048。

a.单击**Requests must use of the following providers，然后选**择Microsoft Base智能**卡加密提供程序**。

b.单击“应**用”**。



Properties of New Template

Provider Category: Legacy Cryptographic Service Provider

Algorithm name: Determined by CSP

Minimum key size: 2048

Choose which cryptographic providers can be used for requests

○ Requests can use any provider available on the subject's computer

● Requests must use one of the following providers:

Providers:

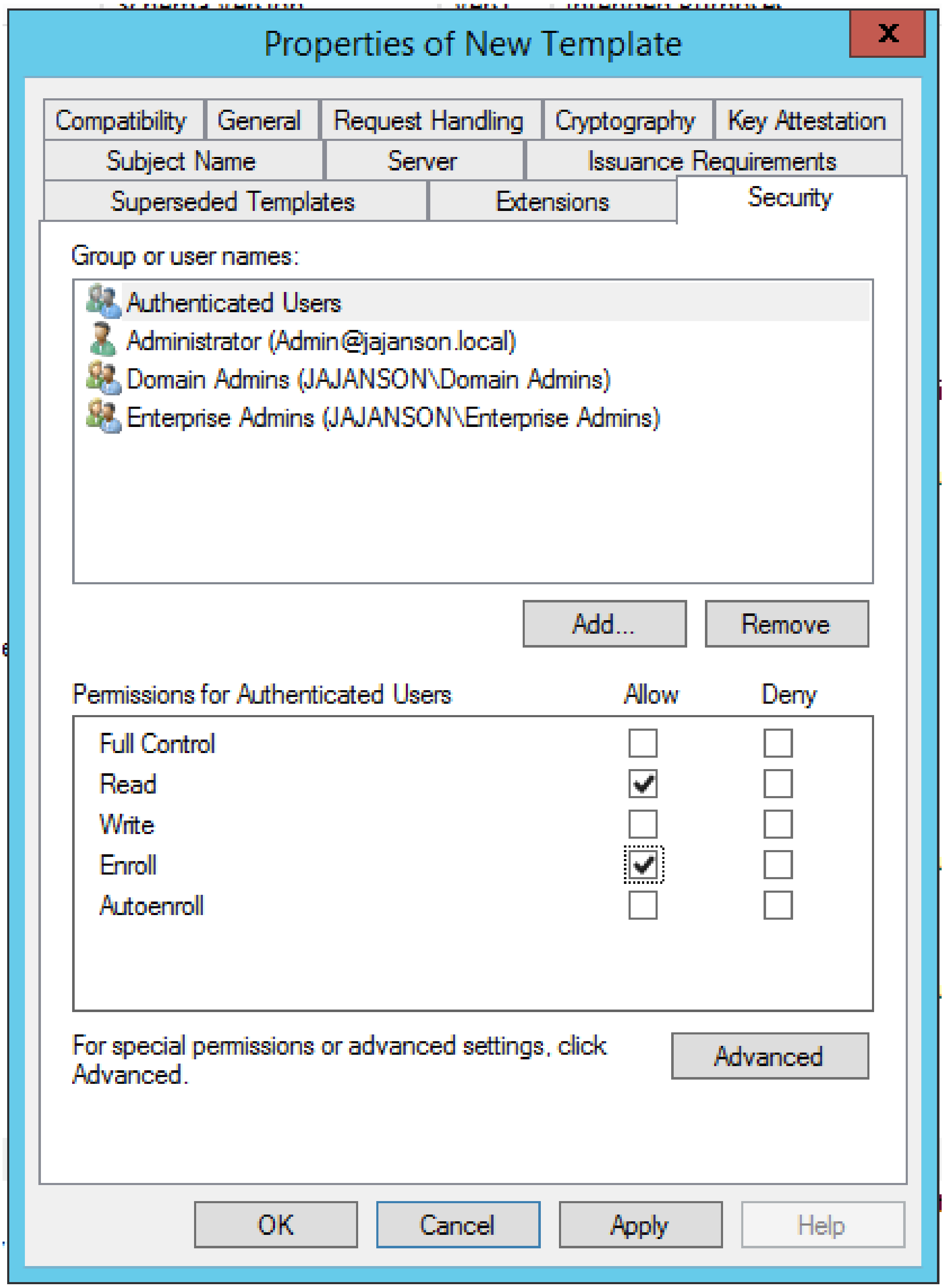
☑ Microsoft Base Smart Card Crypto Provider
□ Microsoft DH SChannel Cryptographic Provider
□ Microsoft Enhanced Cryptographic Provider v1.0
□ Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Pr
□ Microsoft Enhanced RSA and AES Cryptographic Provider

Request hash: Determined by CSP

□ Use alternate signature format

证书加密设置

8. 在Security选项卡上，添加要授予Enroll访问权限的安全组。例如，如果要授予所有用户访问权限，请选择“已验证”用户组，然后为其选择“注册权限”。



Group or user names:

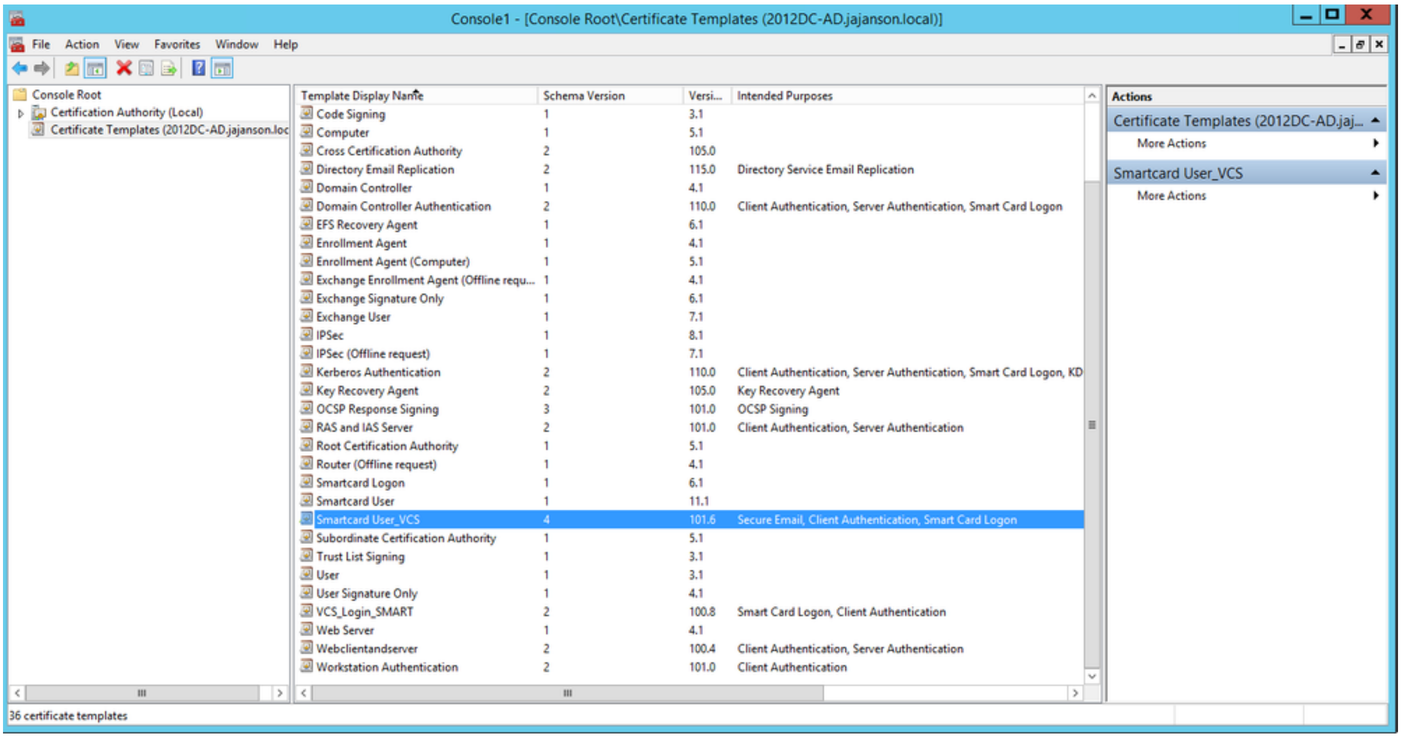
- Authenticated Users
- Administrator (Admin@jajanson.local)
- Domain Admins (JAJANSON\Domain Admins)
- Enterprise Admins (JAJANSON\Enterprise Admins)

Permissions for Authenticated Users	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□
Autoenroll	□	□

For special permissions or advanced settings, click Advanced.

模板安全

9.单击“**确定**”以完成更改并创建新模板。您的新模板现在必须显示在证书模板列表中。



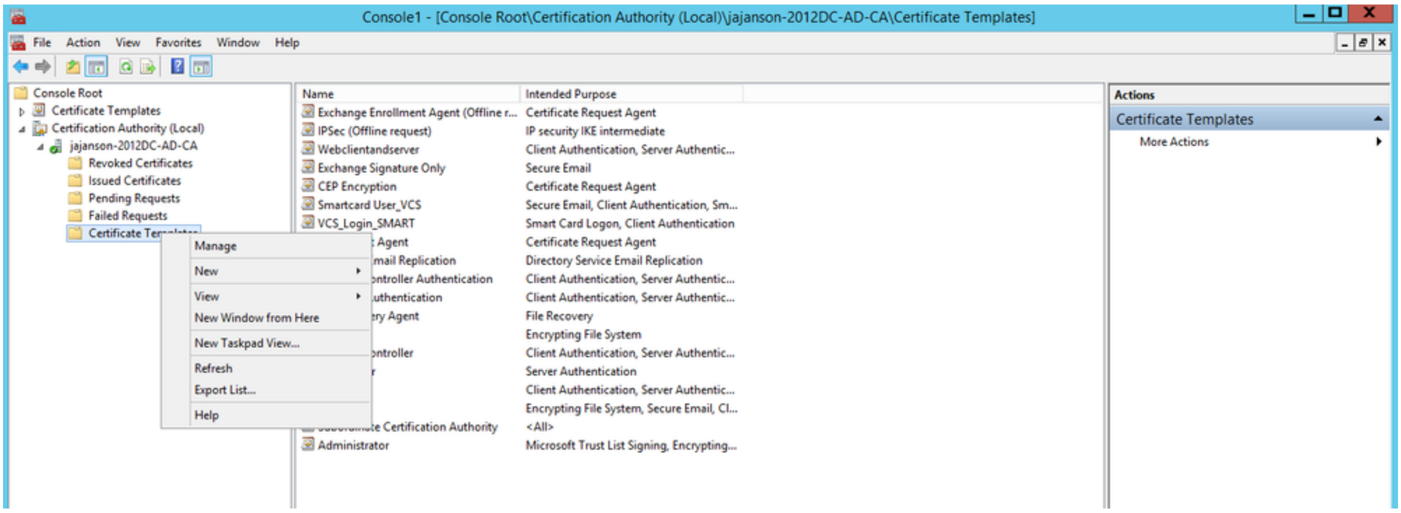
Console1 - [Console Root\Certificate Templates (2012DC-AD.jajanson.local)]
File Action View Favorites Window Help
Console Root
Certification Authority (Local)
Certificate Templates (2012DC-AD.jajanson.loc
Actions
Certificate Templates (2012DC-AD.jaj...
More Actions
Smartcard User_VCS
More Actions
36 certificate templates

Template Display Name	Schema Version	Versi...	Intended Purposes
Code Signing	1	3.1	
Computer	1	5.1	
Cross Certification Authority	2	105.0	
Directory Email Replication	2	115.0	Directory Service Email Replication
Domain Controller	1	4.1	
Domain Controller Authentication	2	110.0	Client Authentication, Server Authentication, Smart Card Logon
EFS Recovery Agent	1	6.1	
Enrollment Agent	1	4.1	
Enrollment Agent (Computer)	1	5.1	
Exchange Enrollment Agent (Offline requ...	1	4.1	
Exchange Signature Only	1	6.1	
Exchange User	1	7.1	
IPSec	1	8.1	
IPSec (Offline request)	1	7.1	
Kerberos Authentication	2	110.0	Client Authentication, Server Authentication, Smart Card Logon, KD
Key Recovery Agent	2	105.0	Key Recovery Agent
OCSP Response Signing	3	101.0	OCSP Signing
RAS and IAS Server	2	101.0	Client Authentication, Server Authentication
Root Certification Authority	1	5.1	
Router (Offline request)	1	4.1	
Smartcard Logon	1	6.1	
Smartcard User	1	11.1	
Smartcard User_VCS	4	101.6	Secure Email, Client Authentication, Smart Card Logon
Subordinate Certification Authority	1	5.1	
Trust List Signing	1	3.1	
User	1	3.1	
User Signature Only	1	4.1	
VCS_Login_SMART	2	100.8	Smart Card Logon, Client Authentication
Web Server	1	4.1	
Webclientandserver	2	100.4	Client Authentication, Server Authentication
Workstation Authentication	2	101.0	Client Authentication

在域控制中看到的模板

10. 在MMC的左窗格中，展开Certification Authority(Local)，然后在Certification Authority列表中展开CA。

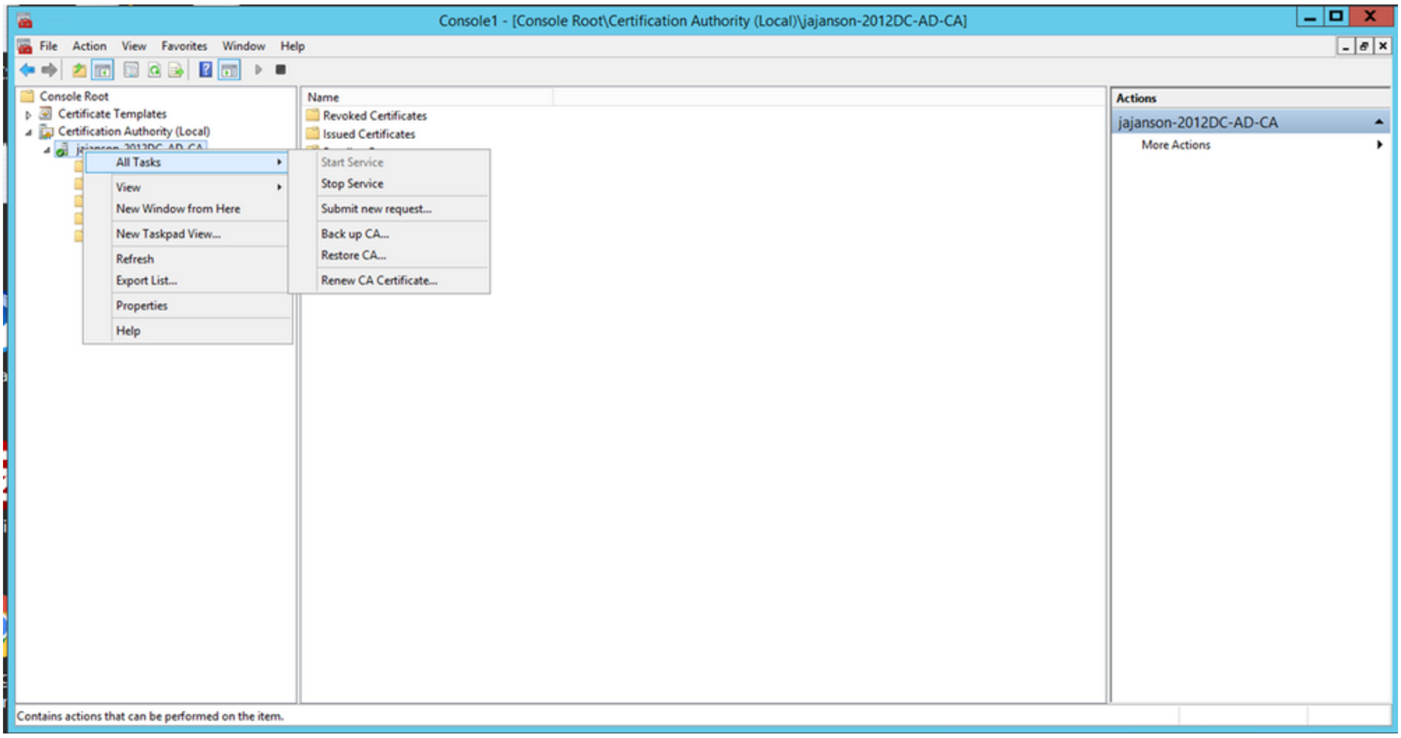
右键单击Certificate Templates，单击**New**，然后单击**Certificate Template to Issue。**然后选择新创建的智能卡模板。



Name	Intended Purpose
Exchange Enrollment Agent (Offline r...	Certificate Request Agent
IPSec (Offline request)	IP security IKE intermediate
Webclientandserver	Client Authentication, Server Authentic...
Exchange Signature Only	Secure Email
CEP Encryption	Certificate Request Agent
Smartcard User_VCS	Secure Email, Client Authentication, Sm...
VCS_Login_SMART	Smart Card Logon, Client Authentication
: Agent	Certificate Request Agent
mail Replication	Directory Service Email Replication
ontroller Authentication	Client Authentication, Server Authentic...
uthentication	Client Authentication, Server Authentic...
ry Agent	File Recovery
	Encrypting File System
ontroller	Client Authentication, Server Authentic...
r	Server Authentication
	Client Authentication, Server Authentic...
	Encrypting File System, Secure Email, Cl...
te Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting...

发布新模板

11.模板复制后，在MMC中，右键单击或选择“证书颁发机构”列表，单击“所**有任务”**，然后单击“停**止服务”**。然后，再次右键单击CA的名称，单击“All Tasks(所**有任务)”**，然后单击“**Start Service(启动服务**)”。



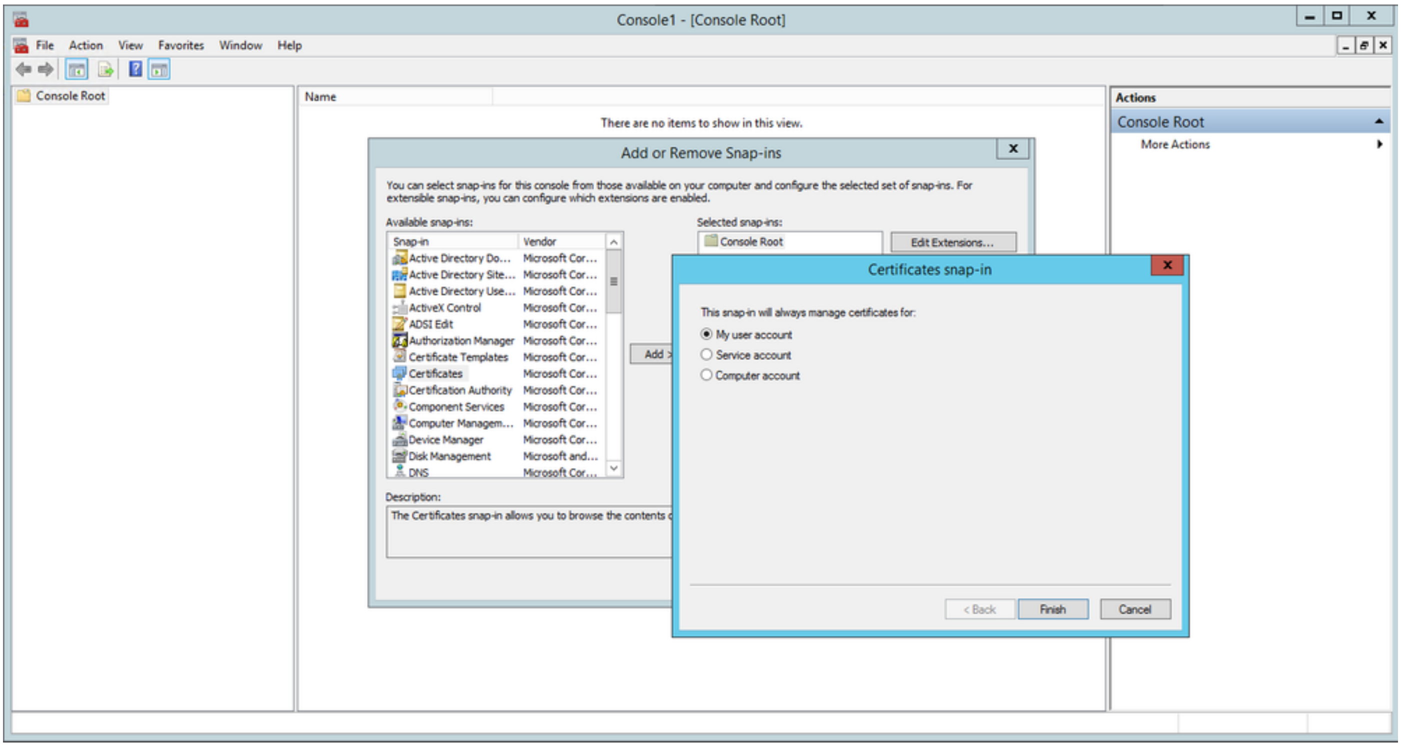
Contains actions that can be performed on the item.

停止然后启动证书服务

注册代理证书

建议您在客户端（IT管理员桌面）上执行此操作。

1. 启动MMC选择**证书**，单击添加**，**然后单击**“我的用户帐户**”。



There are no items to show in this view.

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
DNS	Microsoft Cor...

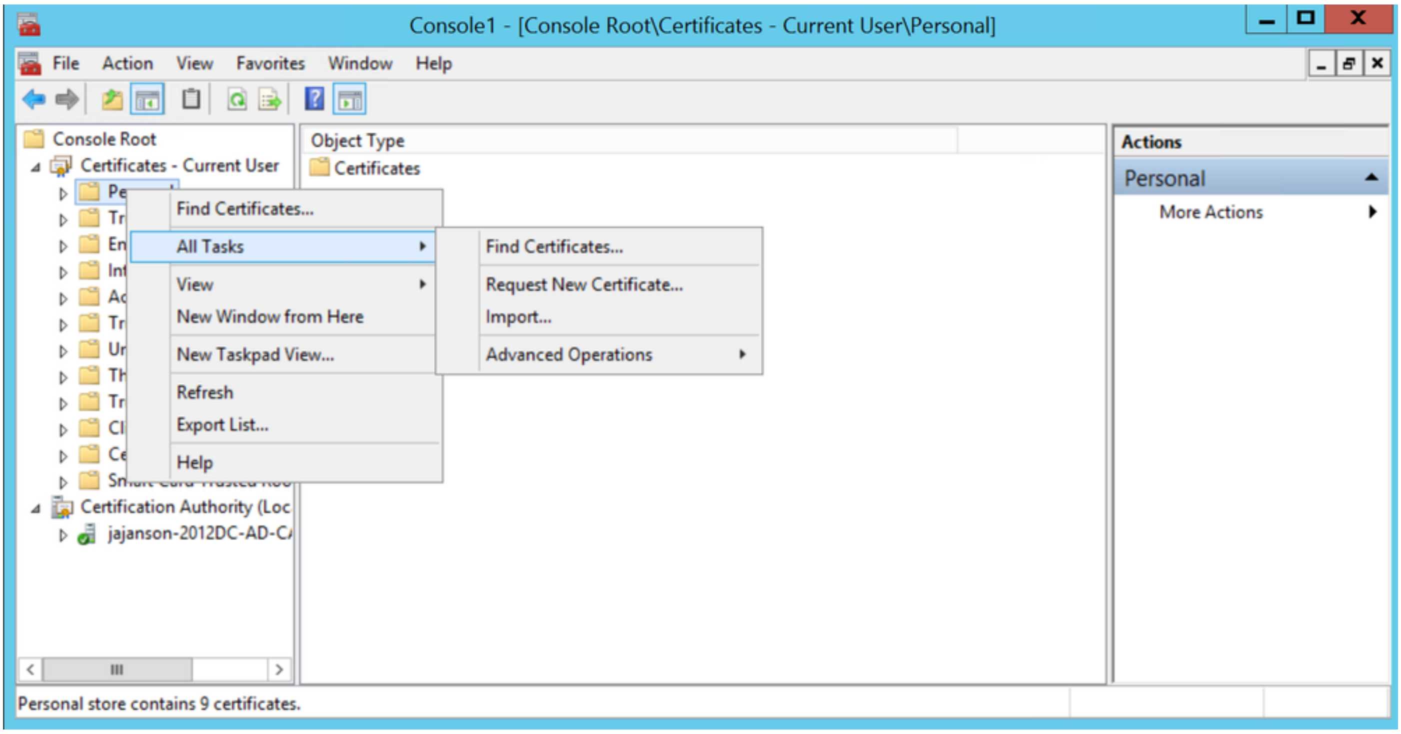
The Certificates snap-in allows you to browse the contents o

This snap-in will always manage certificates for:

● My user account
○ Service account
○ Computer account

添加证书

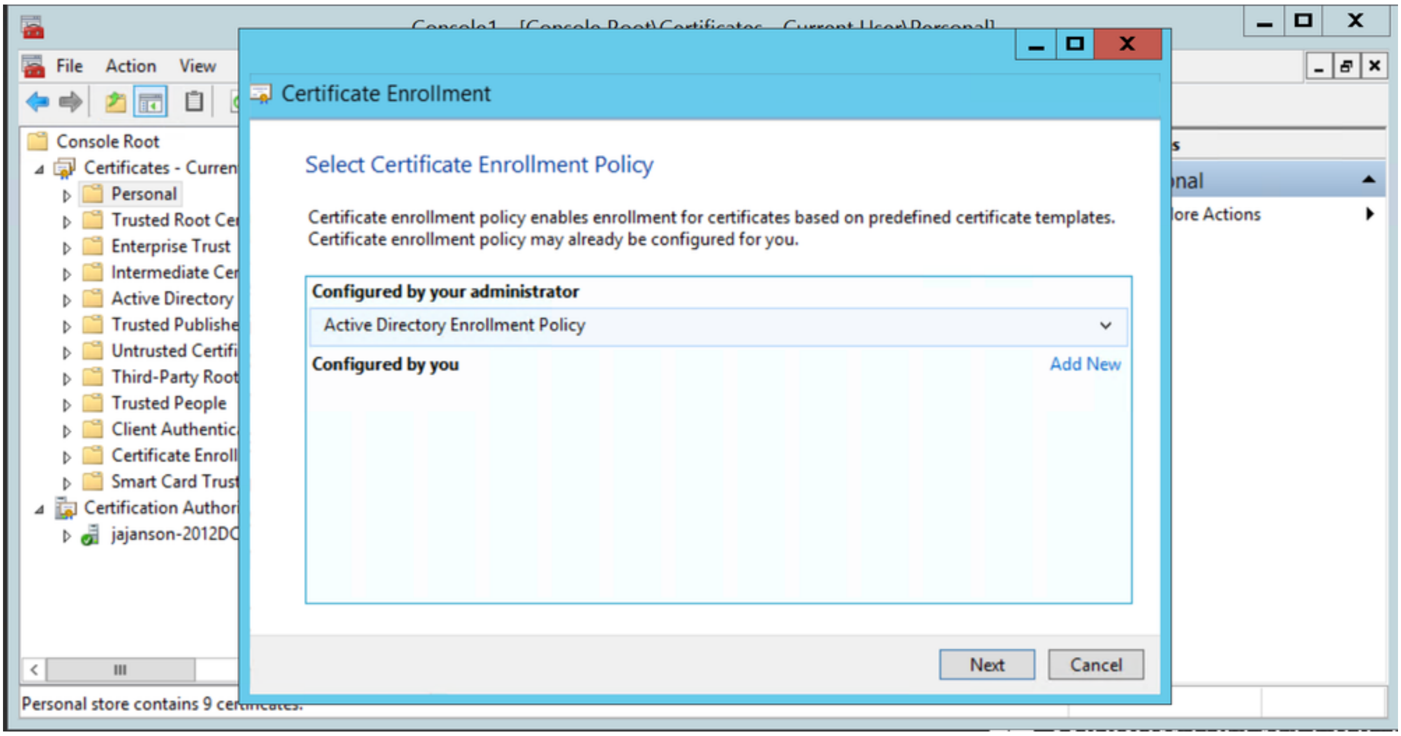
2. 右键单击或选择“个人节**点”，**选择“**所有任务”**，然后**选择“请求新证书**”。



Personal store contains 9 certificates.

请求新证书

3.在向导**上单**击“下一步”，然后选择**“Active Directory注册策略”**。然后再次单**击“下**一步”。



Certificate Enrollment

Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

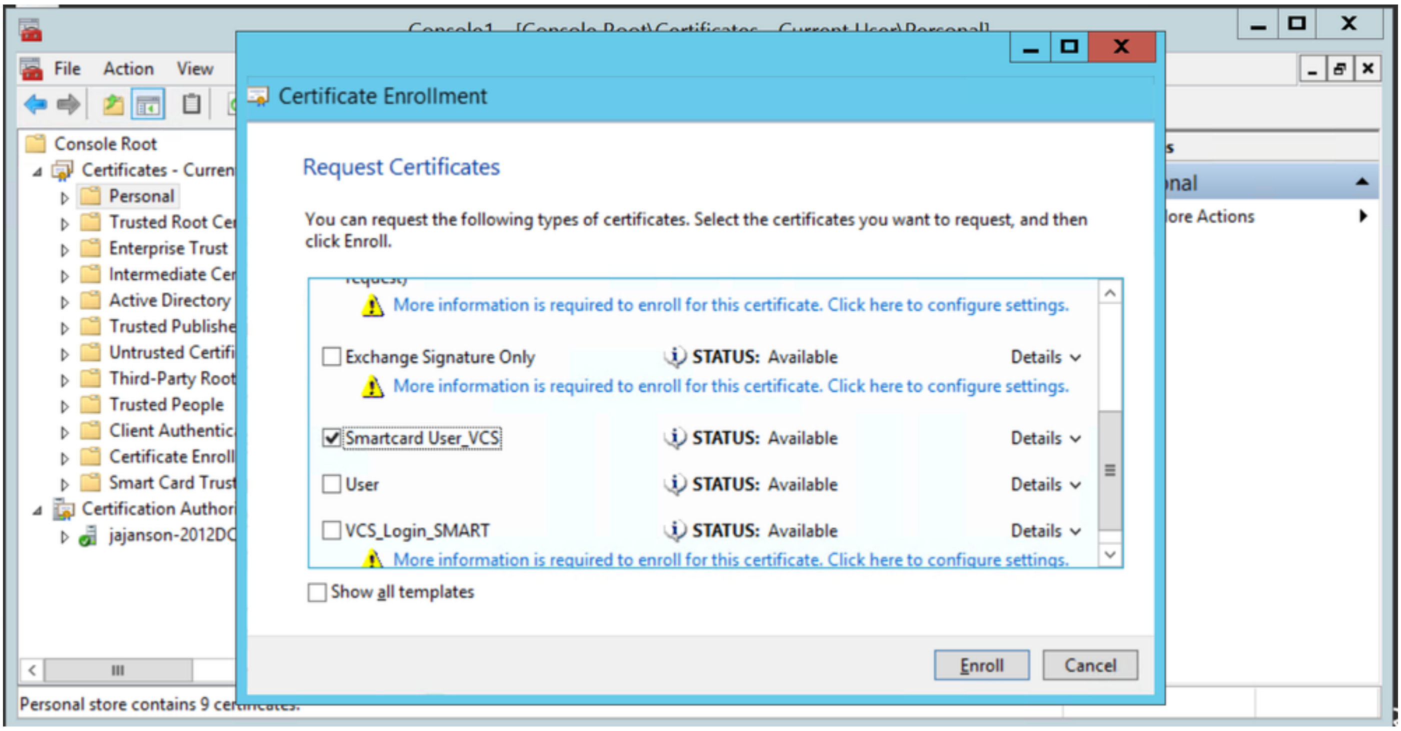
Configured by your administrator
Active Directory Enrollment Policy

Configured by you

Personal store contains 9 certificates.

Active Directory注册元素

4.选择Enrollment Agent **Certificate(注册代**理证书)，在本例**中为Smartcard User_VCS，**然后单击**Enroll。**



Certificate Enrollment

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

request)
More information is required to enroll for this certificate. Click here to configure settings.

□ Exchange Signature Only STATUS: Available Details
More information is required to enroll for this certificate. Click here to configure settings.

☑ Smartcard User_VCS STATUS: Available Details

□ User STATUS: Available Details

□ VCS_Login_SMART STATUS: Available Details
More information is required to enroll for this certificate. Click here to configure settings.

□ Show all templates

Enroll Cancel

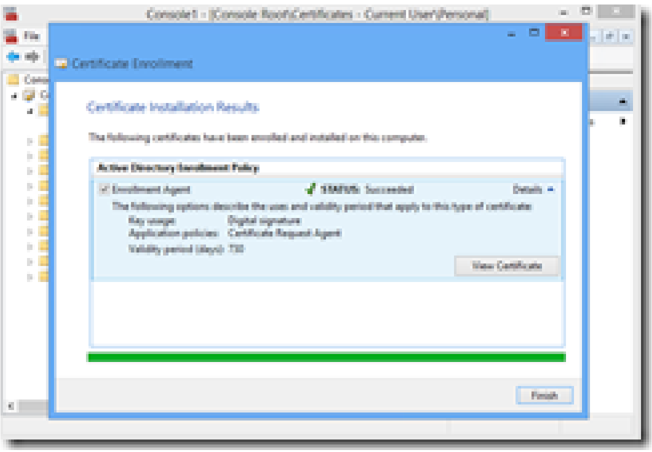
Personal store contains 9 certificates.

注册证书代理

您的IT管理员桌面现在设置为注册站，这使您能够代表其他用户注册新智能卡。

<u>代表……注册</u>

为了现在为员工提供智能卡进行身份验证，您需要注册这些智能卡并生成证书，然后将其导入智能卡。



Console1 - [Console Root\Certificates - Current User\Personal]

Certificate Enrollment

Certificate Installation Results

The following certificates have been enrolled and installed on this computer.

Active Directory Enrollment Policy

☑ Enrollment Agent ✓ STATUS: Succeeded Details

The following options describe the uses and validity period that apply to this type of certificate:
Key usage: Digital signature
Application policies: Certificate Request Agent
Validity period (days): 730

View Certificate

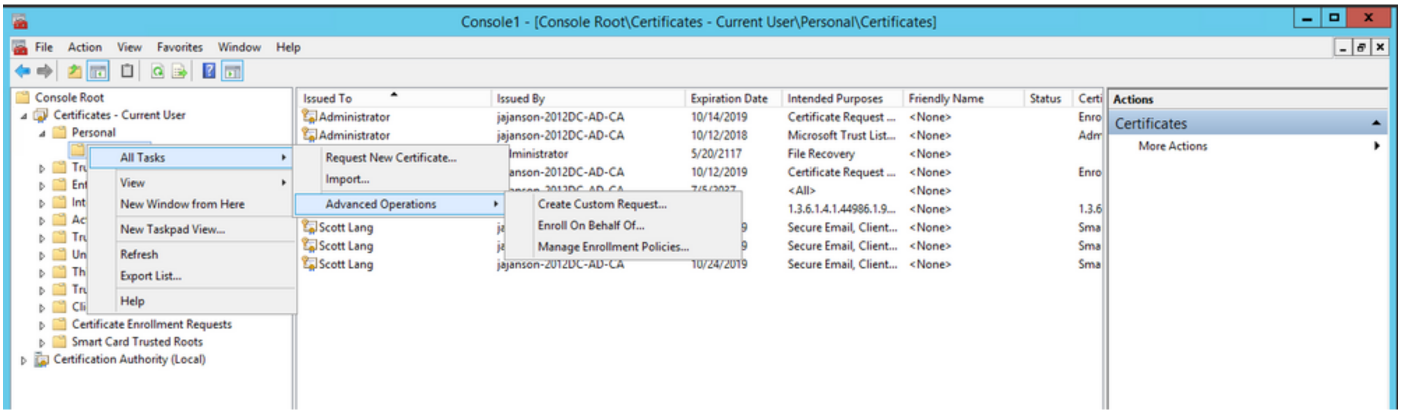
Finish

代表注册

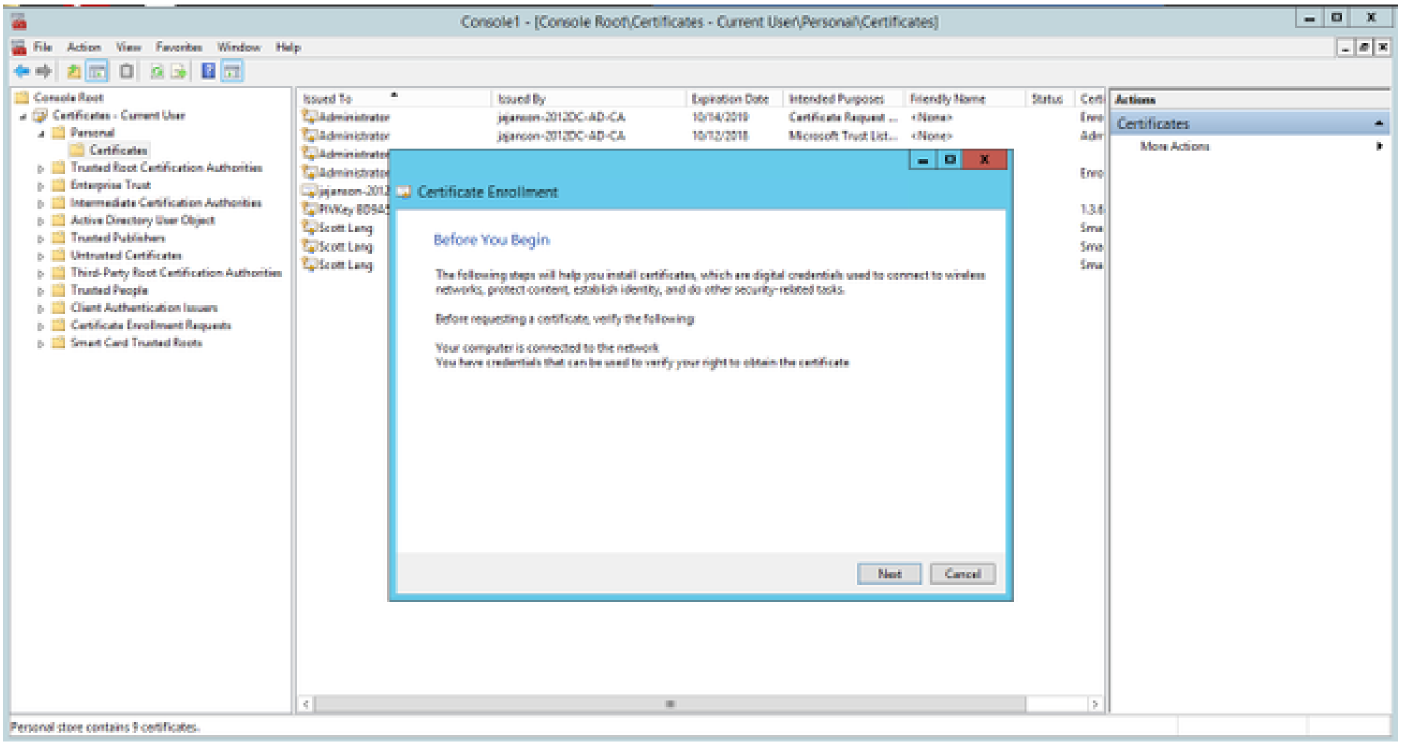
1.启动MMC并导入“**证书模块和管理**器”的“我的用户帐户”证书。

2.右键单击或选择“个人”**>“证书”**，然后选**择“所有任务”>“高级操**作”，**然后单击“代表……登记”。**

3.在向导上，选择Active Directory注册策略，然后单击“下一步”。



代表高级注册


Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File Action View Favorites Window Help
Certificate Enrollment
Next
Cancel
Actions
Certificates
More Actions
Personal store contains 9 certificates.

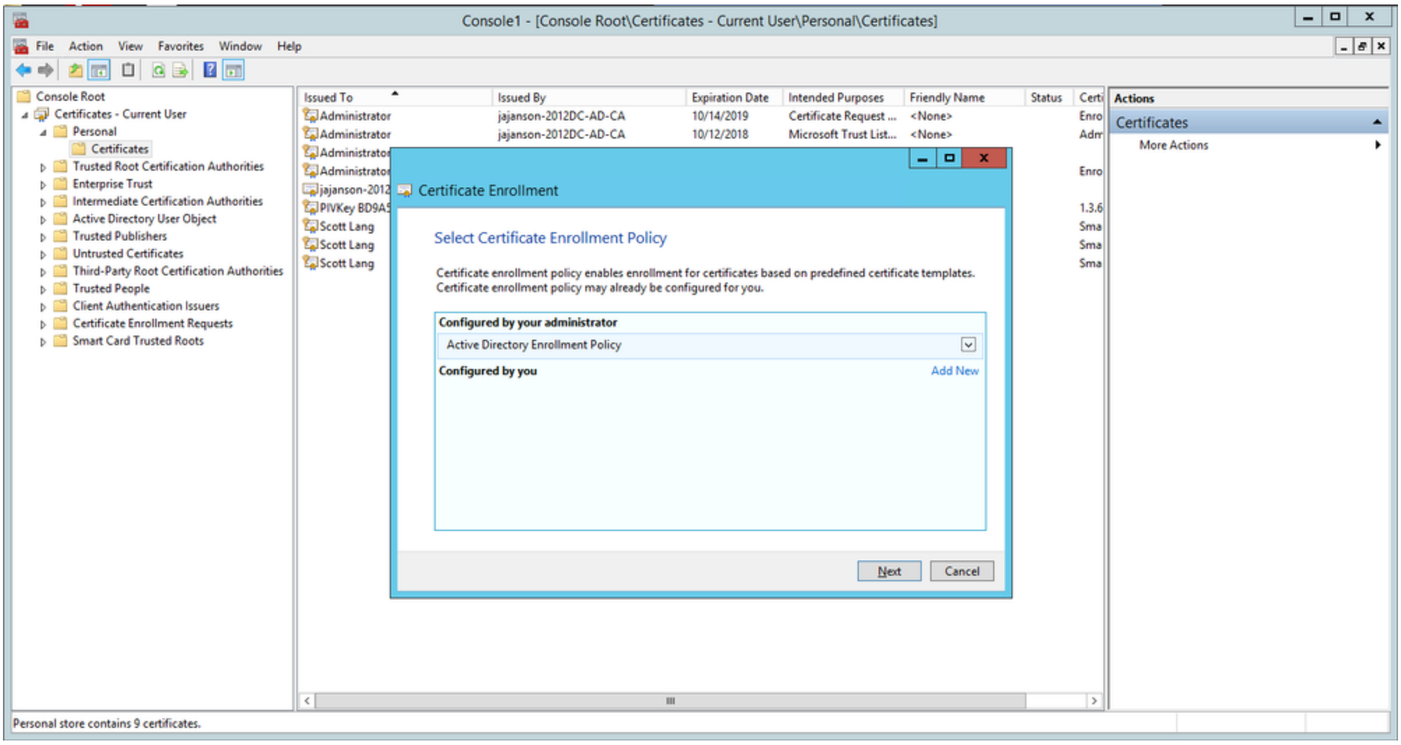
Before You Begin

The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.

Before requesting a certificate, verify the following:

Your computer is connected to the network
You have credentials that can be used to verify your right to obtain the certificate

4.选择“证书注册策略”，然后单击“下**一步”**。


Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Certificate Enrollment Requests
Smart Card Trusted Roots
Issued To
Issued By
Expiration Date
Intended Purposes
Friendly Name
Status
Actions
Certificates
More Actions
Personal store contains 9 certificates.
Certificate Enrollment
Next
Cancel

Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by your administrator

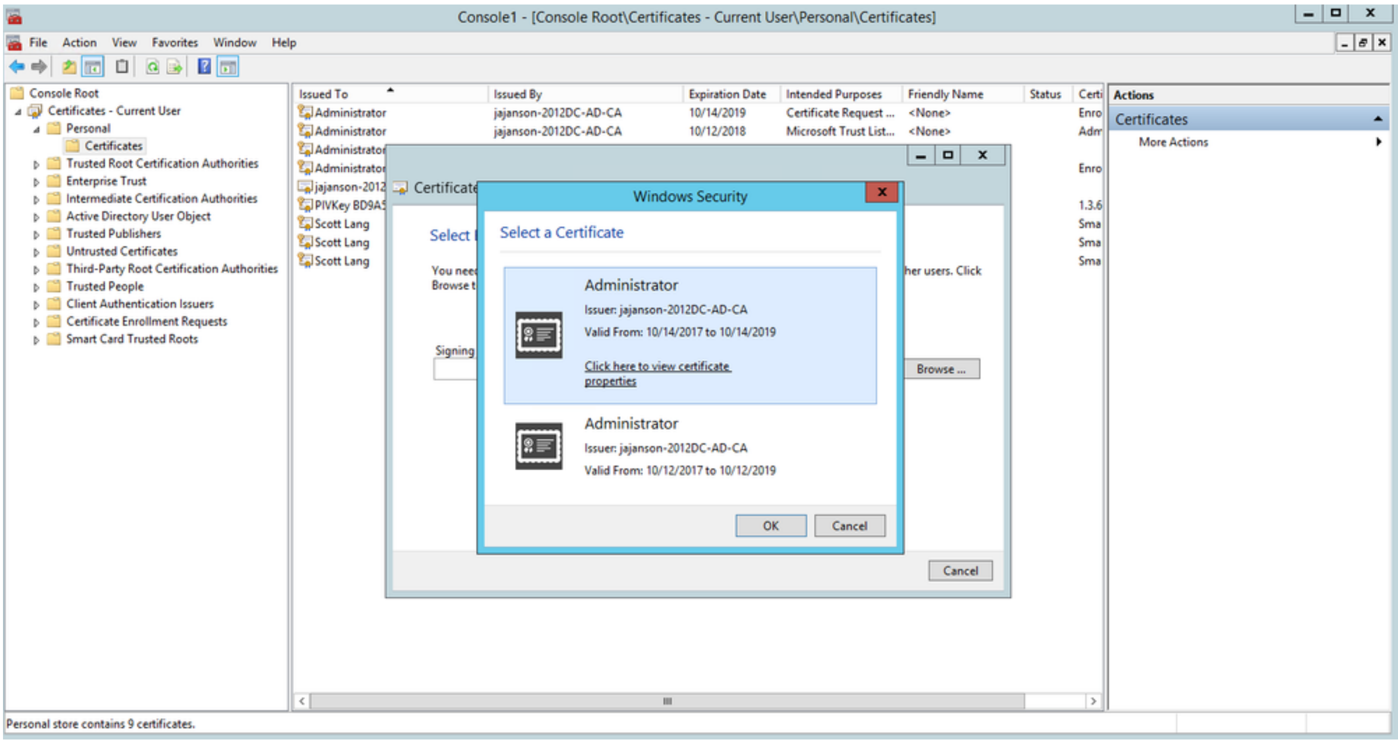
Active Directory Enrollment Policy

Configured by you

Add New

注册策略

5.现在要求您选择签**名证**书。这是您之前请求的注册证书。


Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Certificate Enrollment Requests
Smart Card Trusted Roots
Actions
Certificates
More Actions
Personal store contains 9 certificates.
Windows Security
Browse ...
OK
Cancel
Cancel

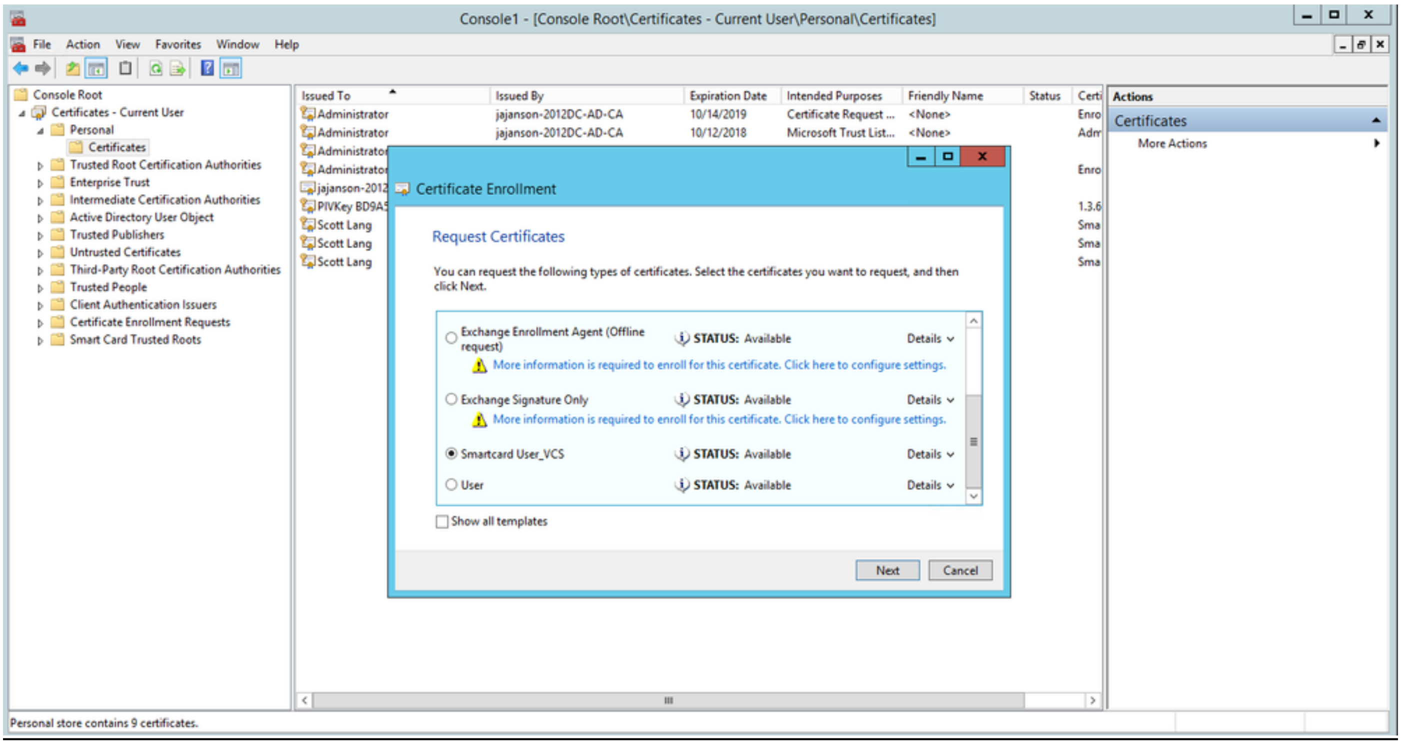
Select a Certificate

Administrator
Issuer: jajanson-2012DC-AD-CA
Valid From: 10/14/2017 to 10/14/2019
Click here to view certificate properties

Administrator
Issuer: jajanson-2012DC-AD-CA
Valid From: 10/12/2017 to 10/12/2019

选择签名证书

6.在下一个屏幕上，您需要浏览到要请求的证书，在此例中，它是您之前创建的模**板Smartcard User_VCS**。


Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Certificate Enrollment Requests
Smart Card Trusted Roots
Actions
Certificates
More Actions
Personal store contains 9 certificates.

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certi
Administrator	jajanson-2012DC-AD-CA	10/14/2019	Certificate Request ...	<None>		Enro
Administrator	jajanson-2012DC-AD-CA	10/12/2018	Microsoft Trust List...	<None>		Adm

Certificate Enrollment

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Next.

○ Exchange Enrollment Agent (Offline request) STATUS: Available Details
More information is required to enroll for this certificate. Click here to configure settings.

○ Exchange Signature Only STATUS: Available Details
More information is required to enroll for this certificate. Click here to configure settings.

● Smartcard User_VCS STATUS: Available Details

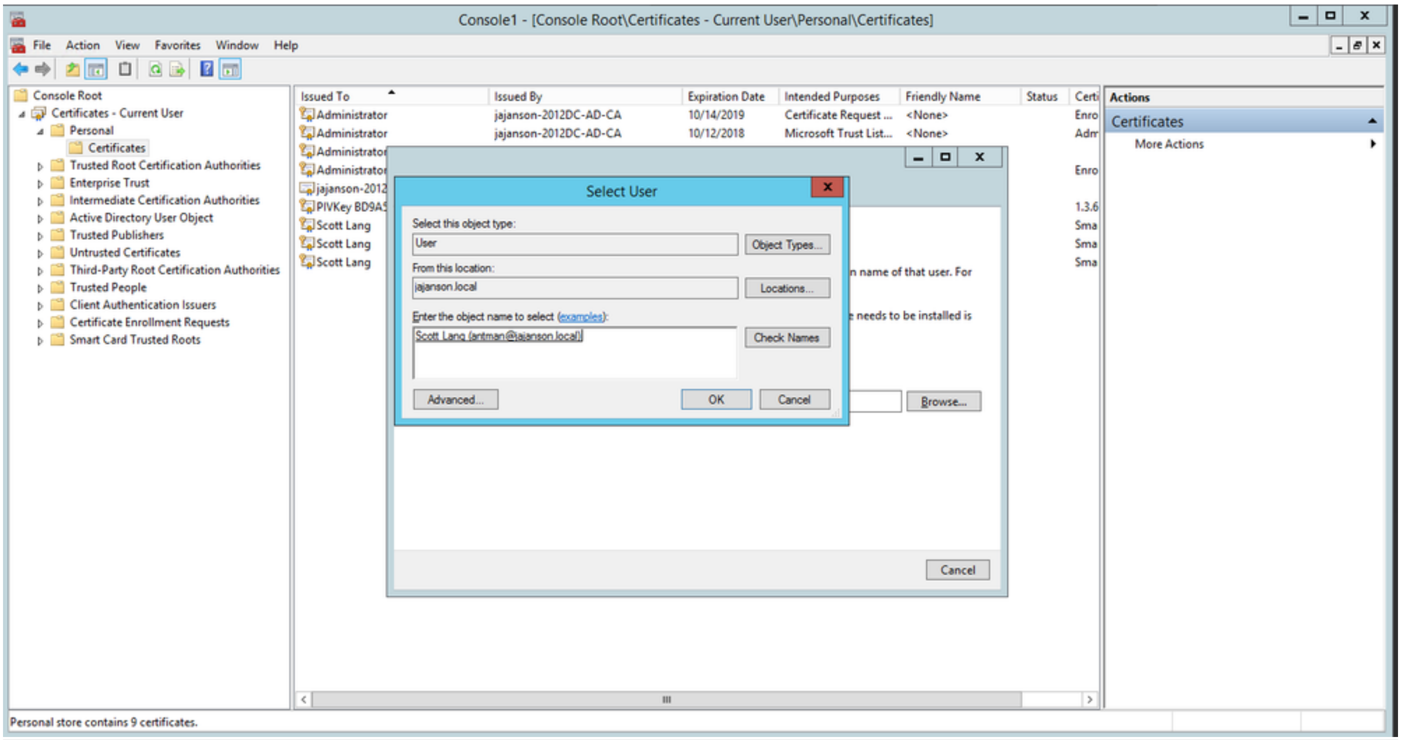
○ User STATUS: Available Details

□ Show all templates

Next Cancel

选择VCS智能卡

7.接下来，您需要选择您希望代表登记的用户。单击**browse**并键入要注册的员工的用户名。在本例中，使用Scott Lang 'antman@jajanson.local帐户'。


Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Certificate Enrollment Requests
Smart Card Trusted Roots
Actions
Certificates
More Actions
Personal store contains 9 certificates.
n name of that user. For
e needs to be installed is
Browse...
Cancel

Select User

Select this object type: User [Object Types...]

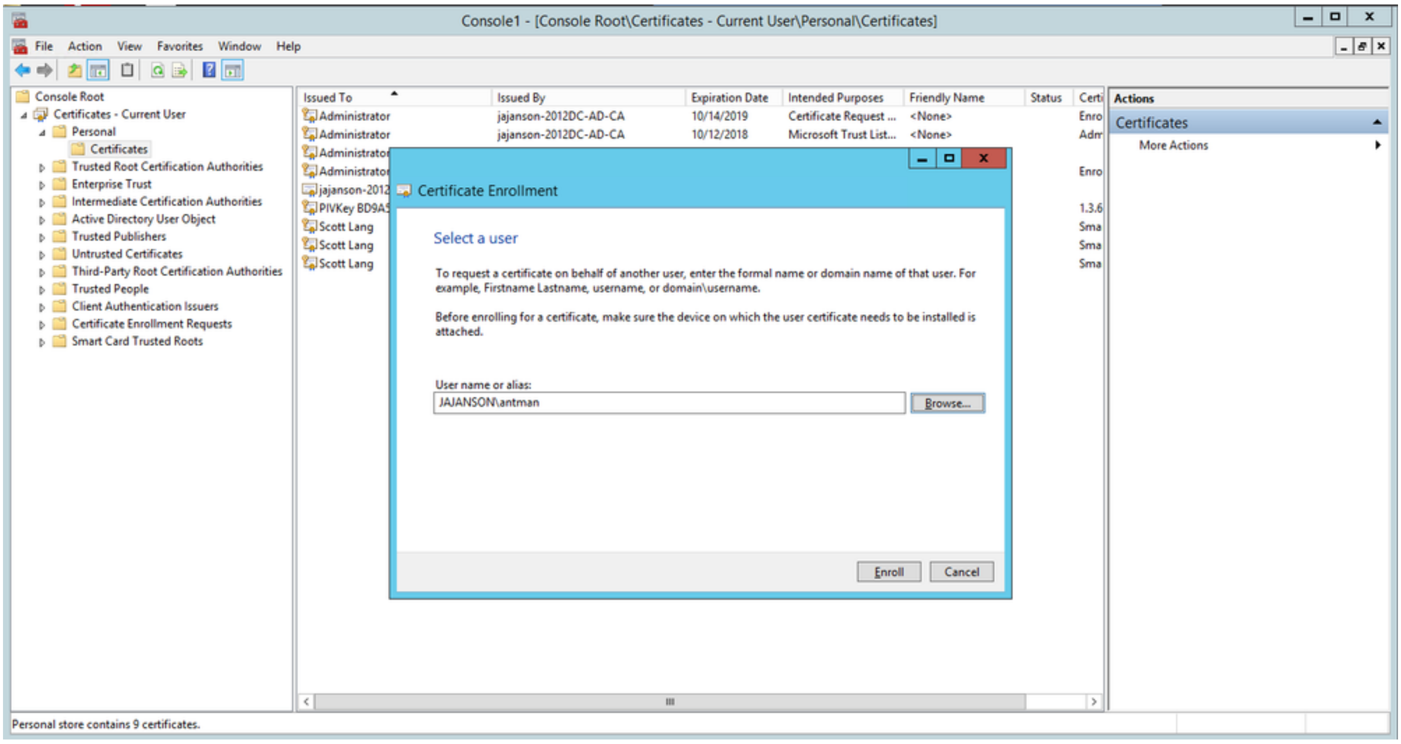
From this location: jajanson.local [Locations...]

Enter the object name to select (examples): Scott Lang (antman@jajanson.local) [Check Names]

Advanced... OK Cancel

选择用户

8. 在下一个屏幕中，单击“注册”继续注册。现在，将智能卡插入**读卡**器中。



Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

- Console Root
  - Certificates - Current User
    - Personal
      - Certificates
    - Trusted Root Certification Authorities
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Active Directory User Object
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Client Authentication Issuers
    - Certificate Enrollment Requests
    - Smart Card Trusted Roots

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certi
Administrator	jajanson-2012DC-AD-CA	10/14/2019	Certificate Request ...	<None>		Enro
Administrator	jajanson-2012DC-AD-CA	10/12/2018	Microsoft Trust List...	<None>		Adm
Administrator						
Administrator						Enro
jajanson-2012						
PIVKey BD9A5						1.3.6
Scott Lang						Sma
Scott Lang						Sma
Scott Lang						Sma

Certificate Enrollment

Select a user

To request a certificate on behalf of another user, enter the formal name or domain name of that user. For example, Firstname Lastname, username, or domain\username.

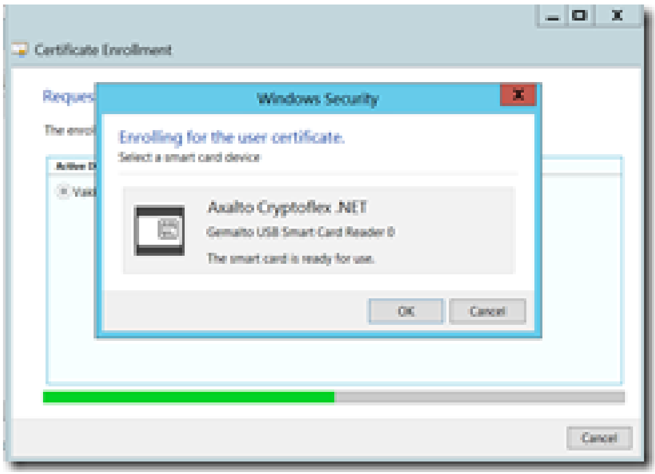
Before enrolling for a certificate, make sure the device on which the user certificate needs to be installed is attached.

User name or alias:
JAJANSON\antman

Personal store contains 9 certificates.

注册

9. 插入智能卡后，将检测到它：



Certificate Enrollment

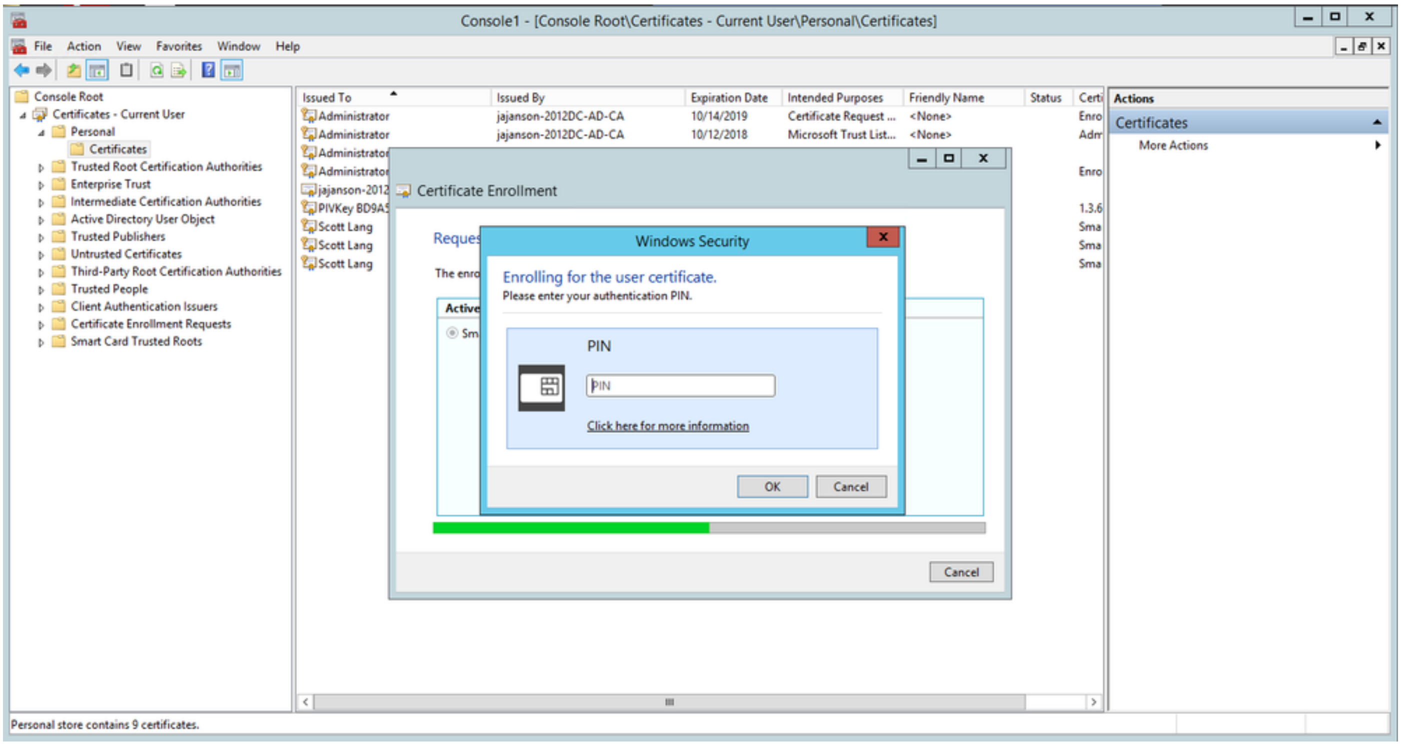
Windows Security

Enrolling for the user certificate.
Select a smart card device

Axalto Cryptoflex .NET
Gemalto USB Smart Card Reader 0
The smart card is ready for use.

插入智能卡

10. 然后要求您键入智能卡PIN码(默认PIN码：0000)。


Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

- Console Root
  - Certificates - Current User
    - Personal
      - Certificates
    - Trusted Root Certification Authorities
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Active Directory User Object
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Client Authentication Issuers
    - Certificate Enrollment Requests
    - Smart Card Trusted Roots

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certi
Administrator	jajanson-2012DC-AD-CA	10/14/2019	Certificate Request ...	<None>		Enro
Administrator	jajanson-2012DC-AD-CA	10/12/2018	Microsoft Trust List...	<None>		Adm
Administrator						
Administrator						Enro
jajanson-2012						
PIVKey BD9A5						1.3.6
Scott Lang						Sma
Scott Lang						Sma
Scott Lang						Sma

Certificate Enrollment

Windows Security

Enrolling for the user certificate.

Please enter your authentication PIN.

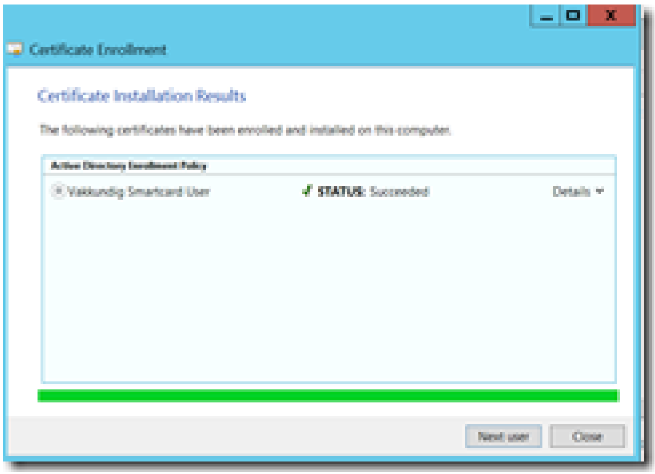
PIN: PIN

Click here for more information

Personal store contains 9 certificates.

输入引脚

11.最后，在看到**Enrollment Successful**屏幕后，您可以使用此智能卡登录到加入域的服务器，如仅带卡和已知PIN的VCS。但是，不能执行是，您仍需要准备VCS以将身份验证请求重定向到智能卡，并使用通用访问卡释放智能卡上存储的智能卡证书以进行身份验证。


Certificate Enrollment

Certificate Installation Results

The following certificates have been enrolled and installed on this computer.

Active Directory Enrollment Policy

Vakkundig Smartcard User ✓ STATUS: Succeeded

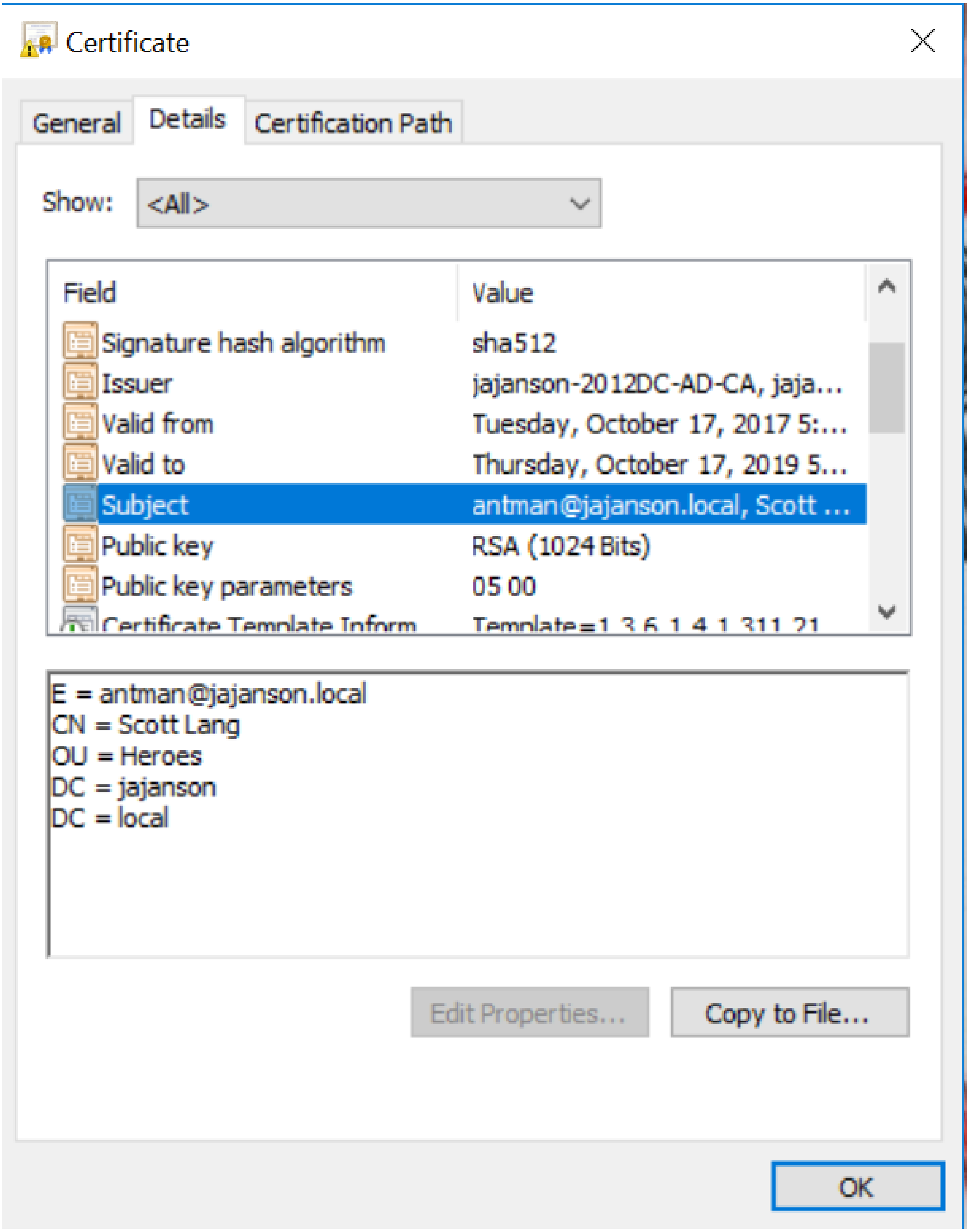
注册成功

配置VCS以使用通用接入卡

导航至Maintenance > Security > Trusted CA Certificate，将根CA上传到VCS中的Trusted CA Certificate列表。

2.将根CA签名的证书撤销列表上传到VCS。导航至**Maintenance > Security > CRL Management。**

3.根据正则表达式测试客户端证书，该正则表达式从证书中提取用户名，用于针对LDAP或本地用户进行身份验证。正则表达式将与证书的**Subject**匹配。这可以是您的UPN、电子邮件等。在本实验中，使用了与客户端证书的客户端证书匹配的电子邮件。



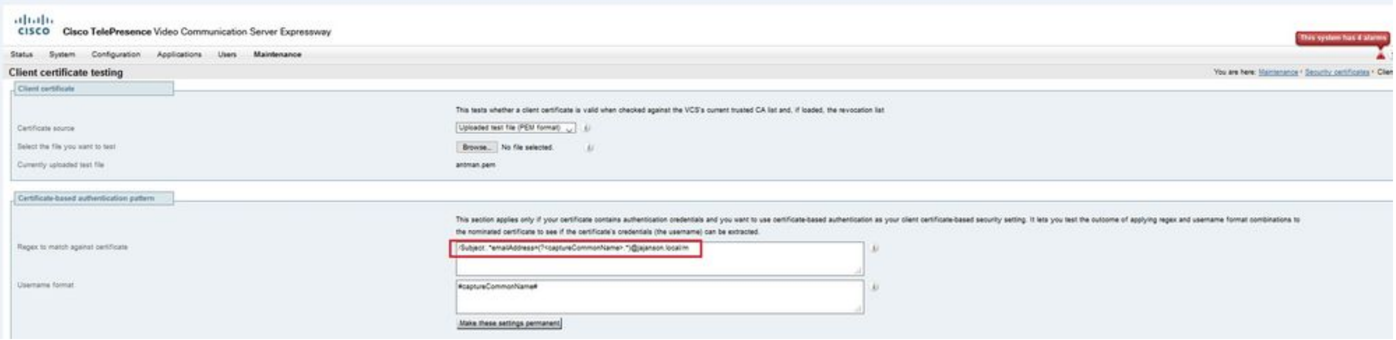
Field	Value
Signature hash algorithm	sha512
Issuer	jajanson-2012DC-AD-CA, jaja...
Valid from	Tuesday, October 17, 2017 5:...
Valid to	Thursday, October 17, 2019 5...
Subject	antman@jajanson.local, Scott ...
Public key	RSA (1024 Bits)
Public key parameters	05 00
Certificate Template Inform	Template=1.3.6.1.4.1.311.21

```
E = antman@jajanson.local
CN = Scott Lang
OU = Heroes
DC = jajanson
DC = local
```

客户端证书的使用者

4. 导航至**维护>安全>客户端证书测试**。选择要测试的客户端证书，在“我的实验”中它是antman.pem，将其上传到测试区域。在Regex下**的Certificate-based authentication pattern部分**，以**与证书进行匹配，**将regex粘贴到要测试的。请勿更改“用户名**格式”**字段。

```
My Regex:  /Subject:.*emailAddress=(?.*)@jajanson.local/m
```


Cisco TelePresence Video Communication Server Expressway
This system has 4 alarms
Status
System
Configuration
Applications
Users
Maintenance
You are here: Maintenance › Security certificates › Clien

Client certificate testing

Client certificate

This tests whether a client certificate is valid when checked against the VCS's current trusted CA list and, if loaded, the revocation list

Certificate source: Uploaded test file (PEM format)

Select the file you want to test: Browse... No file selected.

Currently uploaded test file: antman.pem

Certificate-based authentication pattern

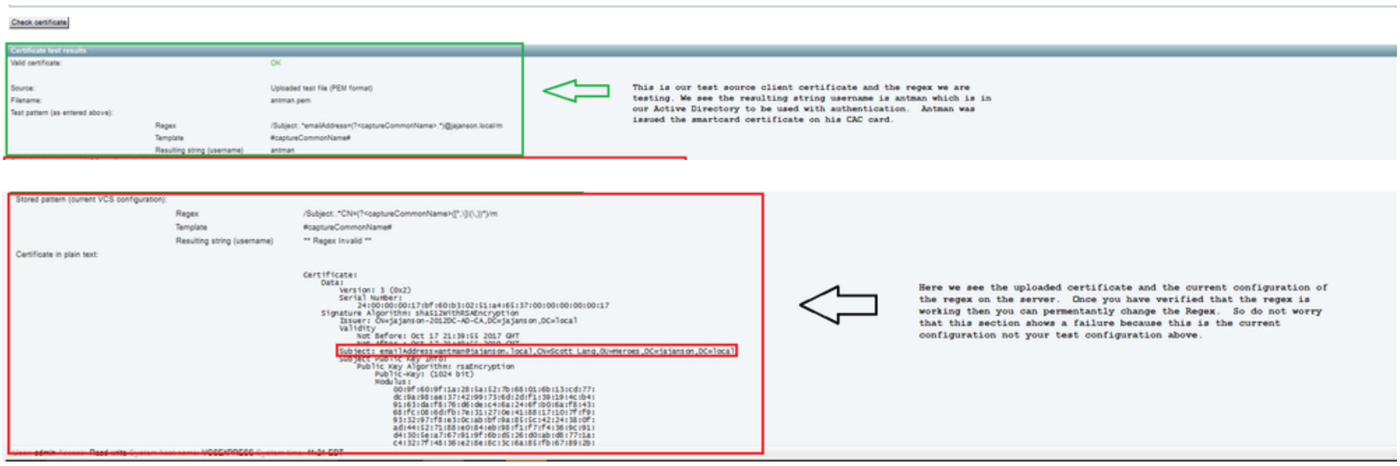
This section applies only if your certificate contains authentication credentials and you want to use certificate-based authentication as your client certificate-based security setting. It lets you test the outcome of applying regex and username format combinations to the nominated certificate to see if the certificate's credentials (the username) can be extracted.

Regex to match against certificate: /Subject:.*emailAddress=(?<captureCommonName>.*)@jajanson.local/m

Username format: #captureCommonName#

Make these settings permanent

在VCS中测试正则表达式



Valid certificate: OK

Source: Uploaded test file (PEM format)
Filename: antman.pem
Test pattern (as entered above):
Regex /Subject:.*emailAddress=(?<captureCommonName>.*)@jajanson.local/m
Template #captureCommonName#
Resulting string (username) antman

This is our test source client certificate and the regex we are testing. We see the resulting string username is antman which is in our Active Directory to be used with authentication. Antman was issued the smartcard certificate on his CAC card.

Stored pattern (current VCS configuration):
Regex /Subject:.*CN=(?<captureCommonName>([^,\]|(\,))*)/m
Template #captureCommonName#
Resulting string (username) ** Regex Invalid **
Certificate in plain text:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            24:00:00:00:17:bf:60:b3:02:51:a4:65:37:00:00:00:00:00:17
    Signature Algorithm: sha512WithRSAEncryption
        Issuer: CN=jajanson-2012DC-AD-CA,DC=jajanson,DC=local
        Validity
            Not Before: Oct 17 21:39:55 2017 GMT
            Not After : Oct 17 21:49:55 2019 GMT
        Subject: emailAddress=antman@jajanson.local,CN=Scott Lang,OU=Heroes,DC=jajanson,DC=local
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:9f:60:9f:1a:28:5a:52:7b:68:01:6b:13:cd:77:
                    dc:9a:98:ae:37:42:99:73:6d:2d:f1:39:19:4c:b4:
                    91:63:da:f8:76:d6:de:c4:6a:24:6f:b0:6a:f8:43:
                    68:fc:08:6d:fb:7e:31:27:0e:41:88:17:10:7f:f9:
                    93:32:97:f8:e3:0c:ab:bf:9a:85:5c:42:24:38:0f:
                    ad:44:52:71:88:e0:84:eb:98:f1:f7:f4:36:9c:91:
                    d4:30:5e:a7:67:91:9f:6b:d5:26:d0:ab:d8:77:1a:
                    c4:32:7f:48:36:e2:8e:8c:3c:6a:85:fb:67:89:2b:
```

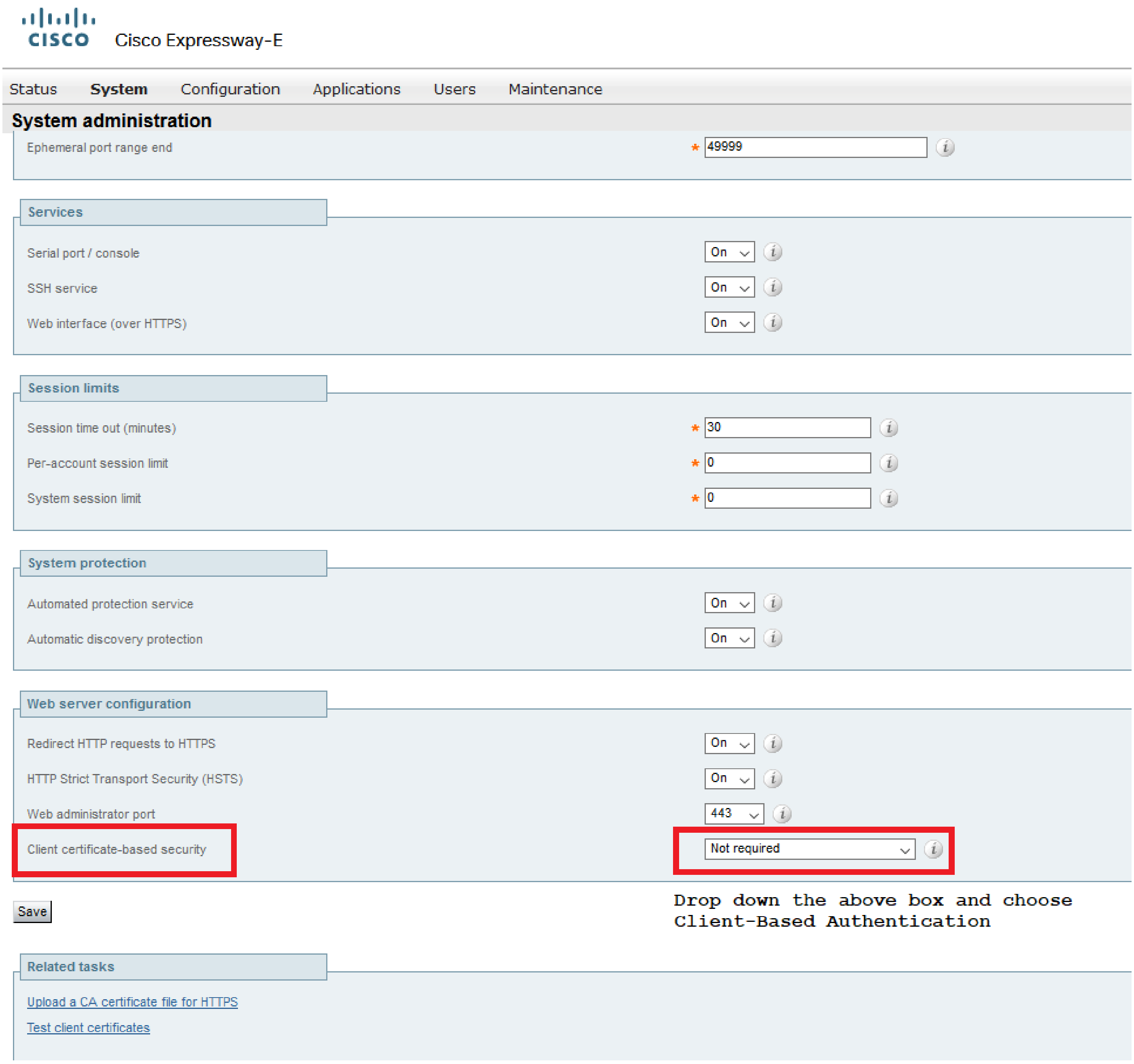
User: admin Access: Read-write System host name: VCSEXPRESS System time: 11:24 EDT

Here we see the uploaded certificate and the current configuration of the regex on the server. Once you have verified that the regex is working then you can permentantly change the Regex. So do not worry that this section shows a failure because this is the current configuration not your test configuration above.

测试结果

5.如果测试为您提供了所需的结果，则可以单击“使这些更改永久**生效”按钮**。这将更改服务器基于证**书的身份验证配置**的正则表达式。要验证更改，请导航至该配置，即**Maintenace > Security > Certificate-based authentication configuration。**

6. 通过导航到System > Administrator，然后单击或选择下拉框以选择**Client certificate-based security = Client-Based Authentication，启用基于客户端的身份验证。**使用此设置，用户在浏览器中键入VCS服务器的FQDN，系统会提示用户选择其客户端帐户并输入分配给其公共访问卡的PIN。然后，证书将被释放，并返回VCS服务器的Web GUI，他只需单击或选择Administrator按钮。然后他被允许进入服务器。如果选中**了Client certificate-based security = Client-Based Validation选项**，则进程与用户单击Administrator按钮时的例外情况相同，他再次提示输入管理员密码。通常，后者不是组织尝试通过CAC实现的目标。



System administration

Ephemeral port range end * 49999

Services

Serial port / console: On

SSH service: On

Web interface (over HTTPS): On

Session limits

Session time out (minutes) * 30

Per-account session limit * 0

System session limit * 0

System protection

Automated protection service: On

Automatic discovery protection: On

Web server configuration

Redirect HTTP requests to HTTPS: On

HTTP Strict Transport Security (HSTS): On

Web administrator port: 443

Client certificate-based security: Not required

Drop down the above box and choose Client-Based Authentication

Related tasks

Upload a CA certificate file for HTTPS

Test client certificates

启用基于客户端的身份验证

救命！我被锁了！!!

如果启用基于客户端的身份验证，而VCS出于任何原因拒绝证书，您将无法再以传统方式登录Web GUI。但是，不要担心有办法回到你的系统。附加文档可在思科网站上找到，并提供有关如何从根访问禁用基于客户端的身份验证的信息。

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。