

Configure VCS with CAC and a Smart Card Reader

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[What is a Smart Card?](#)

[Configure](#)

[Verify](#)

[Troubleshoot](#)

Introduction

This document describes a step-by-step guide to install and use a Smart Card Reader and Common Access Card log in for use with the Cisco Video Communication Server (VCS) for organizations who require two-factor authentication to the VCS environment like banks, hospitals, or governments with secure facilities.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Expressway Administrator (X14.0.2).

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, ensure that you understand the potential impact of any command.

Background Information

The CAC provides required authentication so “systems” know who has gained access to their environment and what part of the infrastructure be it physical or electronic. Within the government classified environments, and other secure networks, the rules of “least privileged access” or “need to know” prevail. A log in could be used by anyone, authentication requires something which the user has, ergo the CAC, also known as the Common Access Card, came about in 2006 so that the individual would not need to have multiple devices, be they fobs, id cards or dongles to access their place of employment or systems.

What is a Smart Card?

Smart cards are a key component of the public key infrastructure (PKI) that Microsoft uses to integrate into the Windows platform because smart cards enhance software-only solutions, such as client authentication, logon, and secure email. Smart cards are a point of convergence for public key certificates and associated keys because they:

- Provide tamper-resistant storage for the protection of private keys and other forms of personal information.
- Isolate security-critical computations, which involves authentication, digital signatures, and key exchange from other parts of the system that don't have a need to know.
- Enable portability of credentials and other private information between computers at work, at home, or on the road.

The smart card has become an integral part of the Windows platform because smart cards provide new and desirable features as revolutionary to the computer industry as the introduction of the mouse or CD-ROM. If you do not have an Internal PKI Infrastructure at the moment then you need to ensure you do this first. This document does not cover the installation of this role in this particular article but information on how to implement this can be found here:

<http://technet.microsoft.com/en-us/library/hh831740.aspx>.

Configure

This lab assumes you have already integrated LDAP with VCS and have users that can log in with LDAP credentials.

1. [Lab Equipment](#)
2. [Install the Smart Card](#)
3. [Configure Certificate Authority Templates](#)
4. [Enroll the Enrollment Agent Certificate](#)
5. [Enroll on behalf of....](#)
6. [Configure the VCS for Common Access Card](#)

Required Equipment:

Windows 2012R2 Domain server that has these roles/installed software:

- Certificate Authority
- Active Directory
- DNS
- Windows PC with Smart Card attached
- vSEC: CMS K-Series management software to manage your Smart Card:



Versa Card Reader Software

Install the Smart Card

Smart card readers generally come with instructions on how to connect any necessary cables. Here is an example of installation for this configuration.

How to Install a Smart Card Reader Device Driver

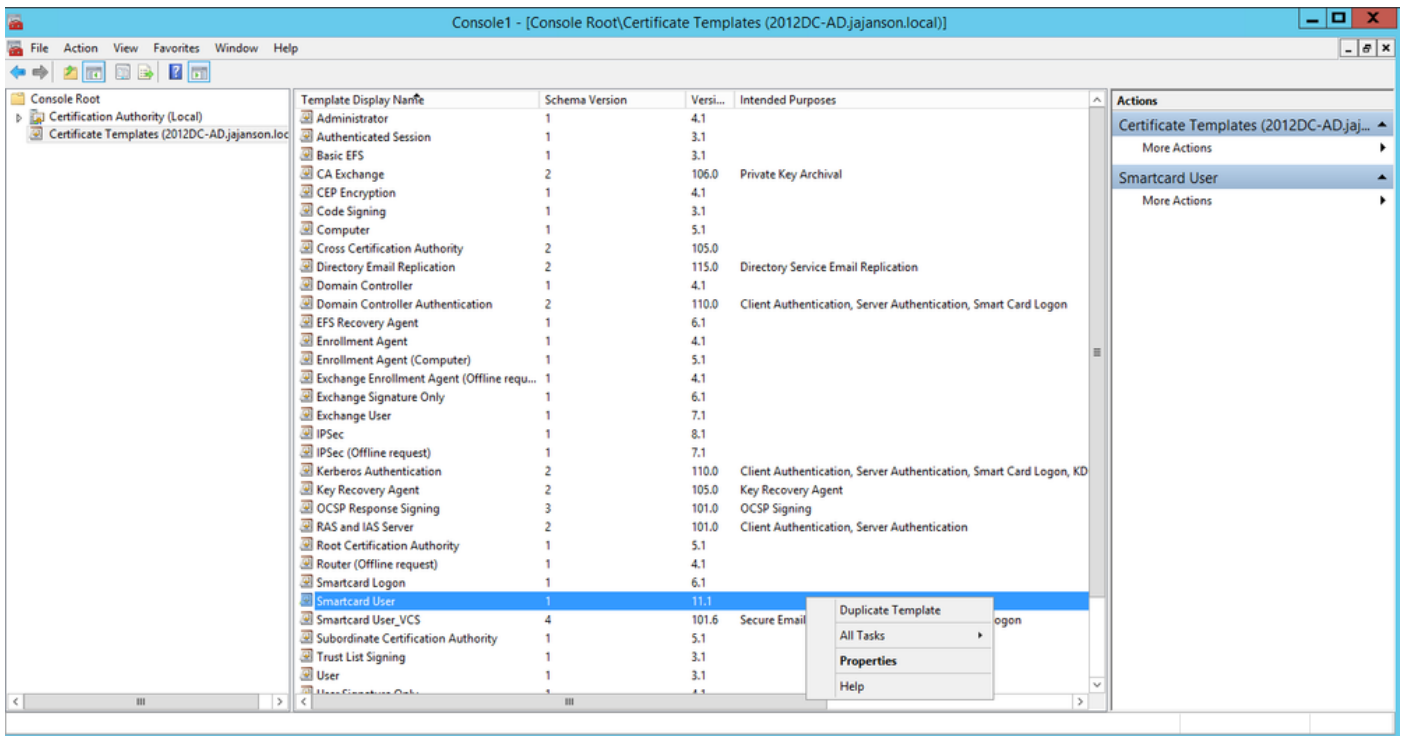
If the smart card reader has been detected and installed, the Welcome to Windows logon screen acknowledges this. If not:

1. Connect your Smart Card to the USB Port on your Windows PC
2. Follow the on-screen directions for installing the device driver software. This requires the driver media that manufacturer of the smart card or the driver is discovered in Windows. In my case I used the manufactures driver from their download site. **DON'T TRUST WINDOWS.**
3. Right-click the **My Computer** icon on your desktop and click **Manage** on the submenu.
4. Expand the **Services and Applications** node, and click **Services**.

5. In the right pane, right-click **Smart Card**. Click **Properties** on the submenu.
6. On the **General** tab, select **Automatic** in the **Startup Type** drop-down list. Click **OK**.
7. Reboot your machine if the Hardware wizard instructs you to do so.

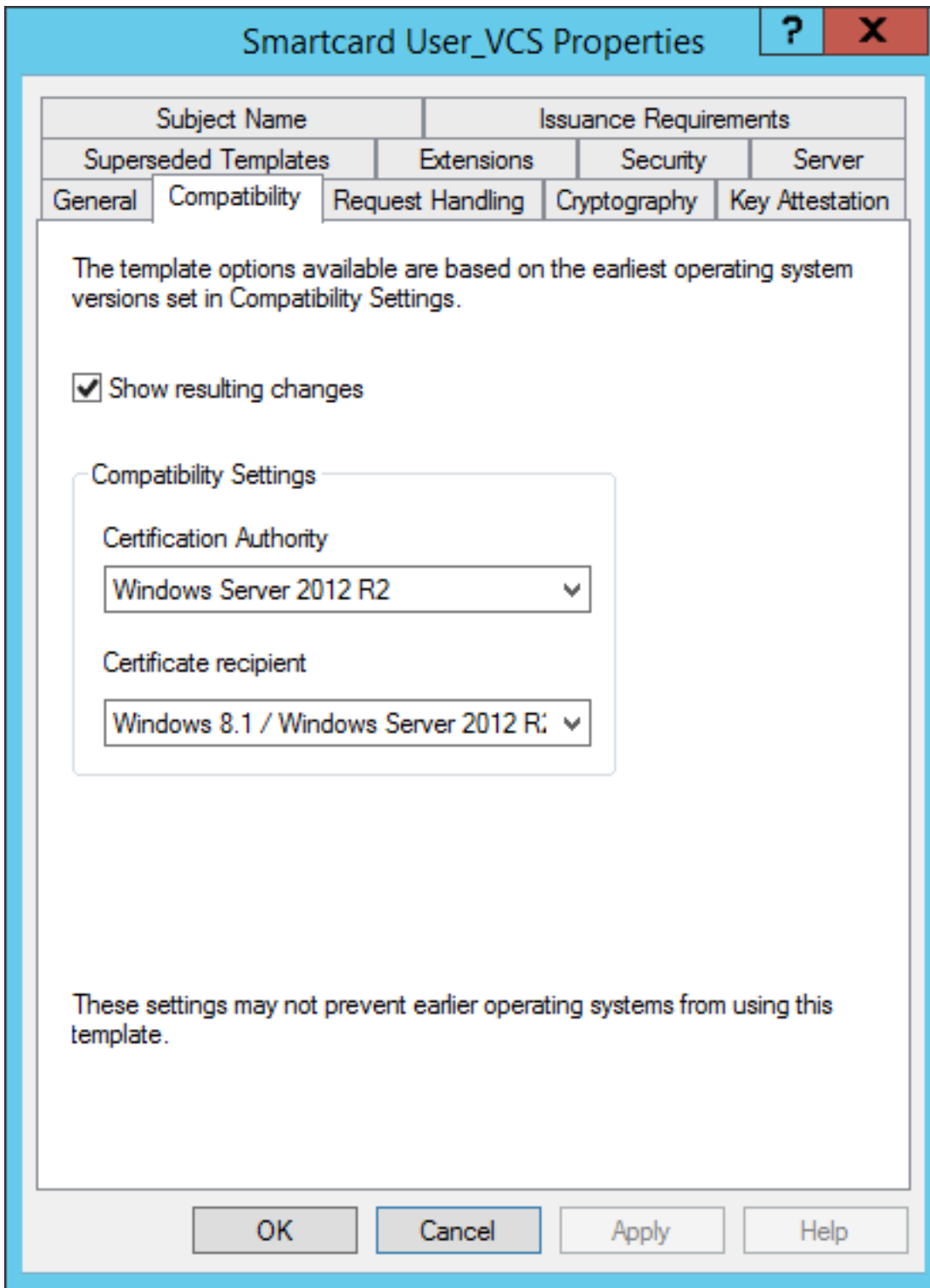
Configure Certificate Authority Templates

1. Launch Certificate Authority MMC from Administrative Tools.
2. Click or select the **Certificate Templates** node and select **Manage**.
3. Right-click or select the **Smartcard User** Certificate Template and then select **Duplicate** as shown in the image.



Domain controller Certificate Templates

4. On the **Compatibility** tab, under **Certification Authority**, review the selection and change it if needed.



Smart Card

Compatibility settings

- 5. On the **General** tab:
 - a. Specify a name, such as **Smartcard User_VCS**.
 - b. Set the validity period to the desired value. Click **Apply**.

Smartcard User_VCS Properties

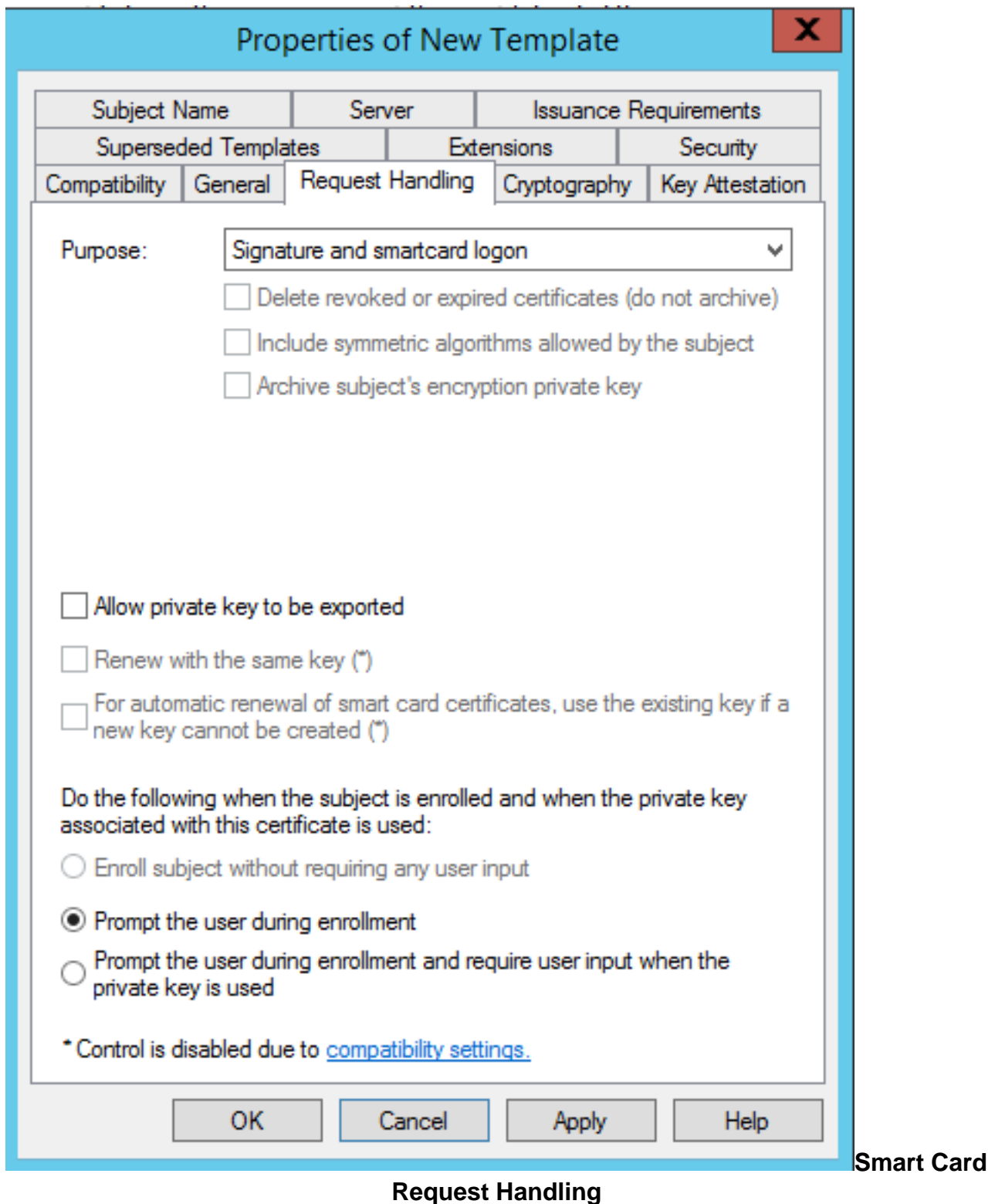
Subject Name		Issuance Requirements		
Superseded Templates		Extensions	Security	Server
General	Compatibility	Request Handling	Cryptography	Key Attestation
Template display name: <input type="text" value="Smartcard User_VCS"/>				
Template name: <input type="text" value="Smartcard User_VCS"/>				
Validity period: <input type="text" value="10"/> years		Renewal period: <input type="text" value="6"/> weeks		
<input checked="" type="checkbox"/> Publish certificate in Active Directory				
<input type="checkbox"/> Do not automatically reenroll if a duplicate certificate exists in Active Directory				

OK Cancel Apply Help

Smart Card General

Time Begin Expire

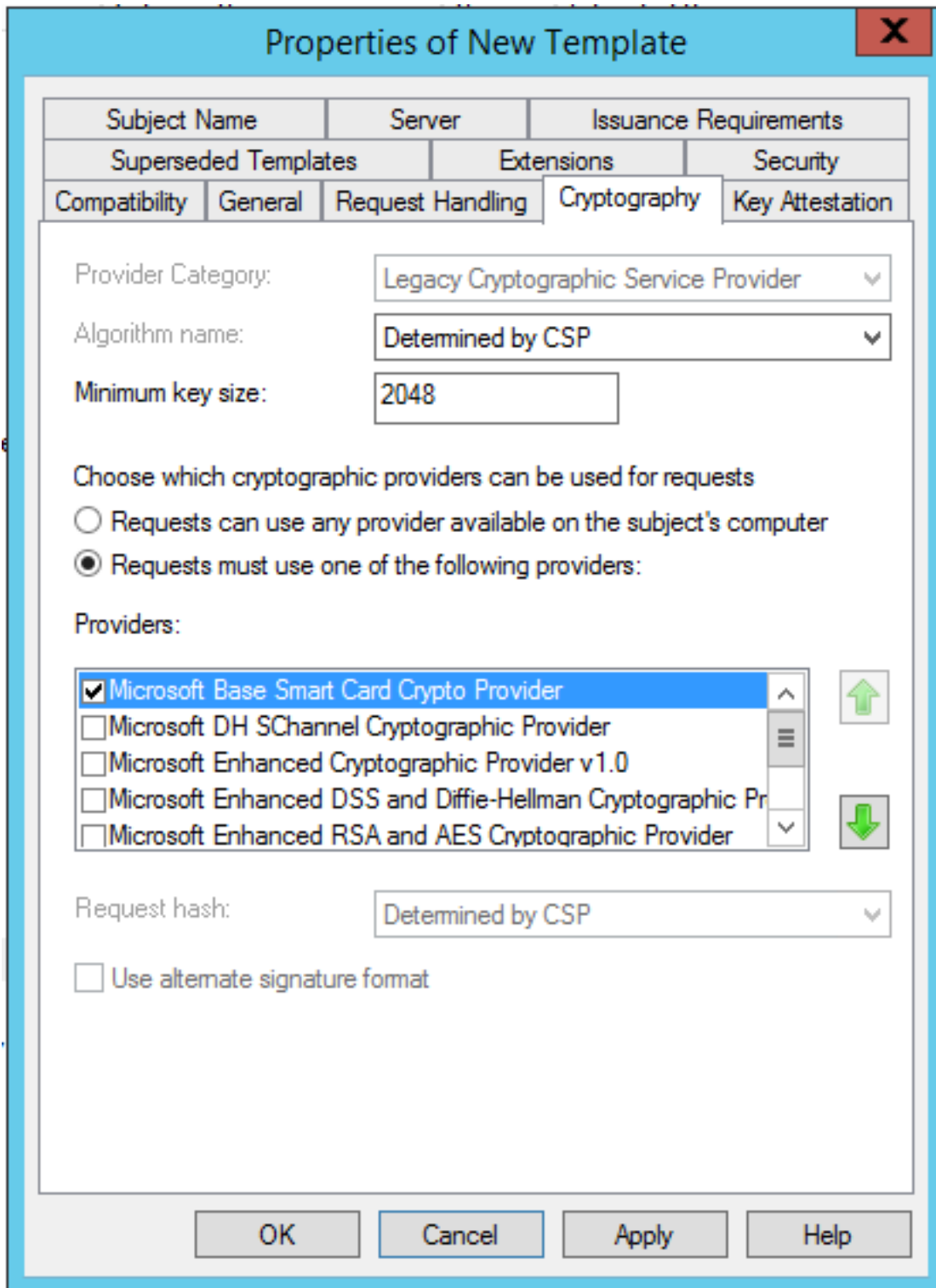
6. On the **Request Handling** tab:
 - a. Set the **Purpose** to **Signature and smartcard logon**.
 - b. Click **Prompt the user during enrollment**. Click **Apply**.



7. On the **Cryptography** tab, set the minimum key size to 2048.

a. Click **Requests must use one of the following providers**, and then select **Microsoft Base Smart Card Crypto Provider**.

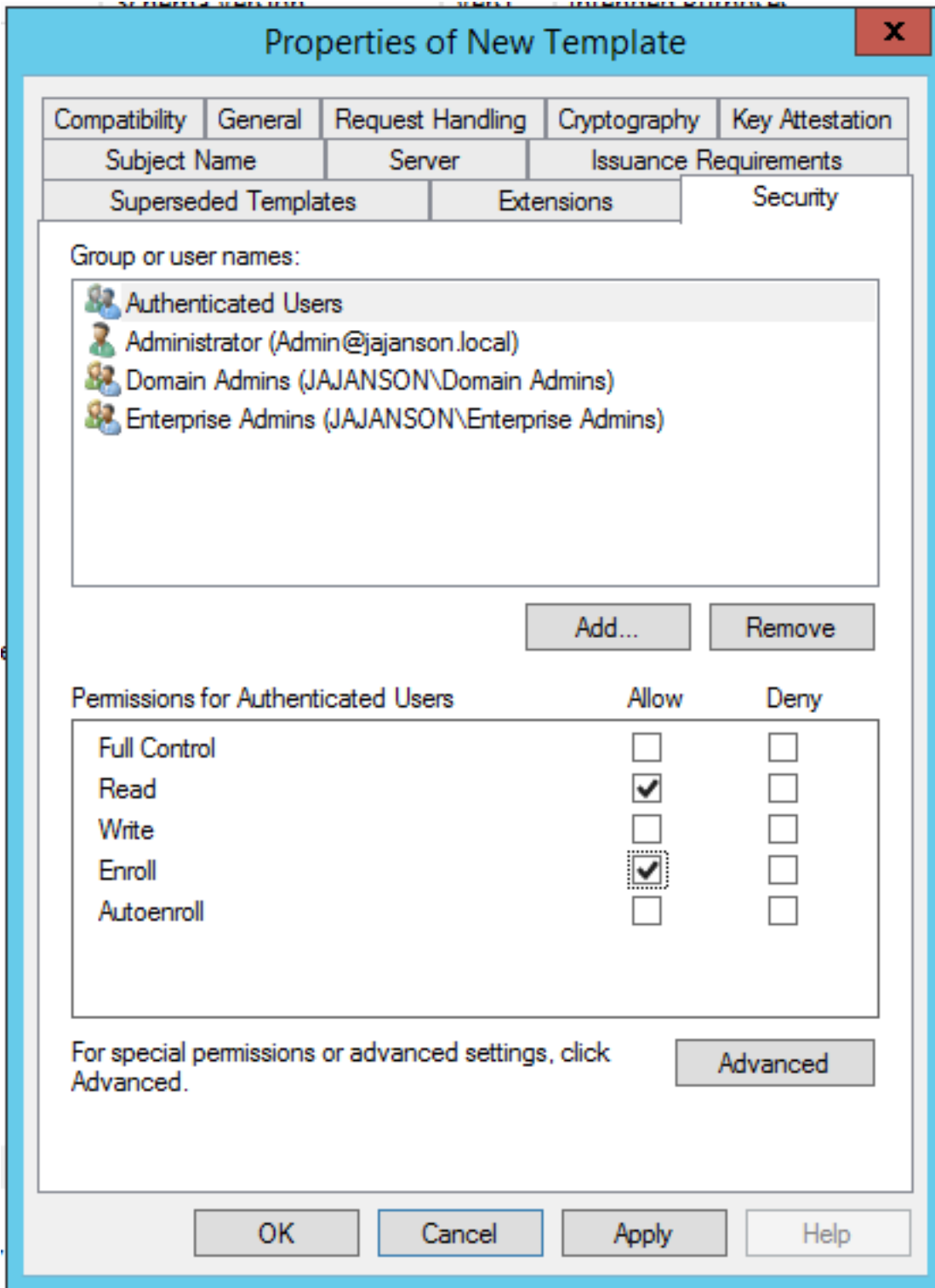
b. Click **Apply**.



Certificate Crypto

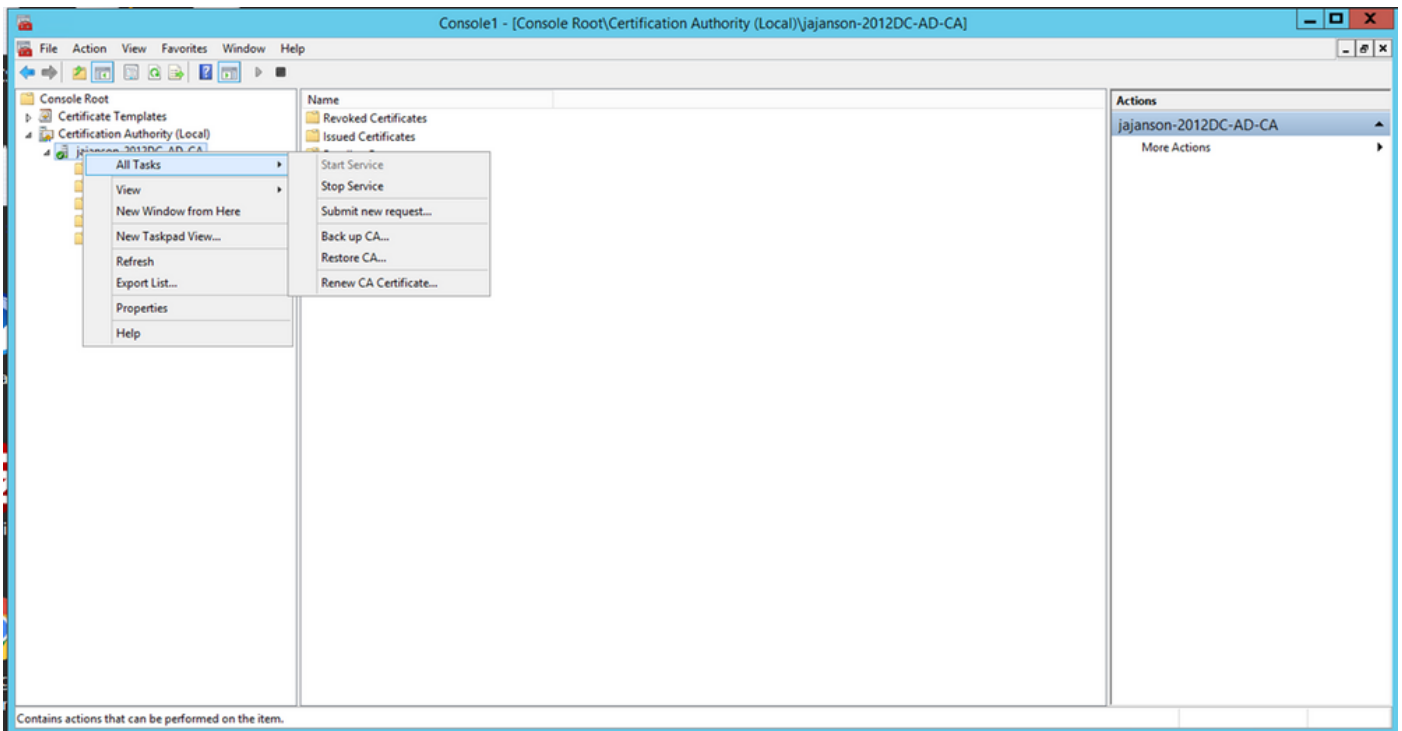
Settings

8. On the Security tab, add the security group that you want to give Enroll access to. For example, if you want to give access to all users, select the Authenticated users group, and then select **Enroll** permissions for them.



Template Security

9. Click **OK** in order to finalize your changes and create the new template. Your new template must now appear in the list of Certificate Templates.

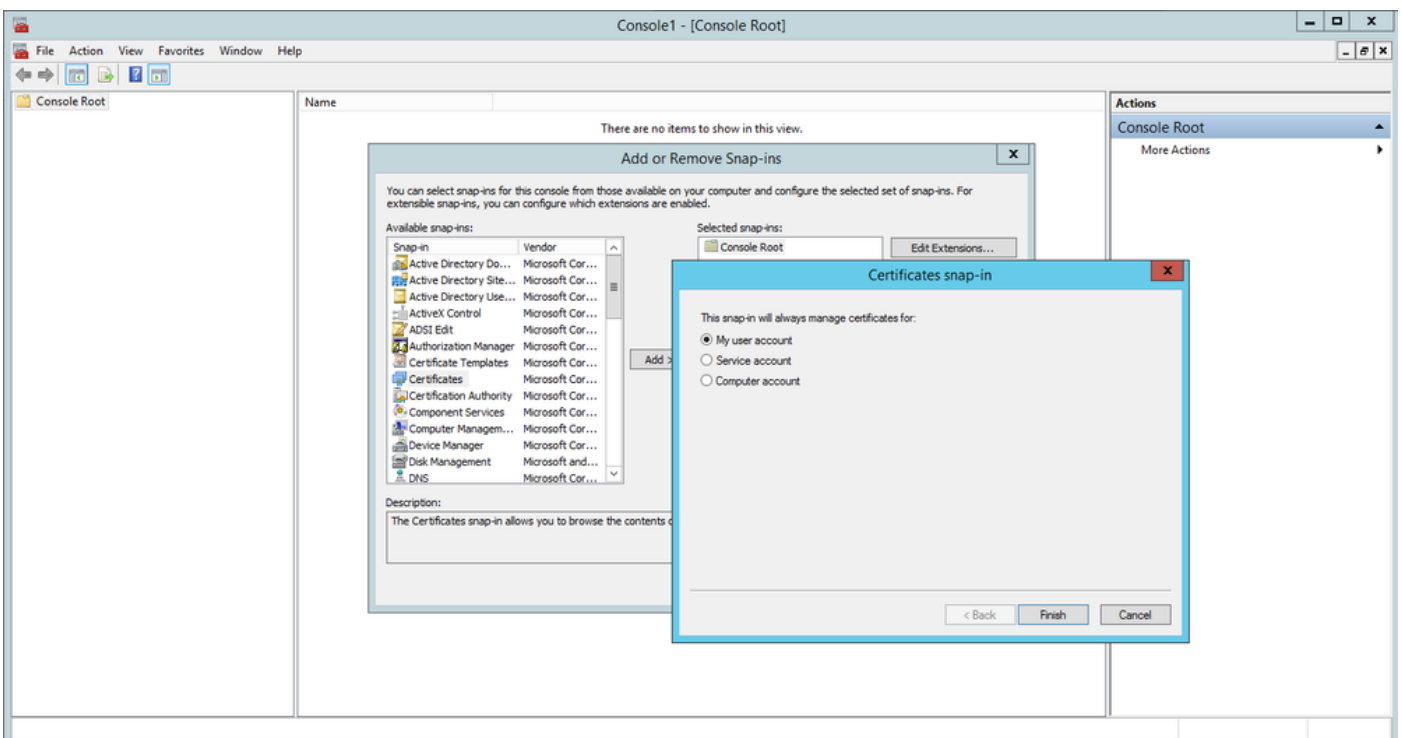


Stop then start certificate services

Enroll on the Enrollment Agent Certificate

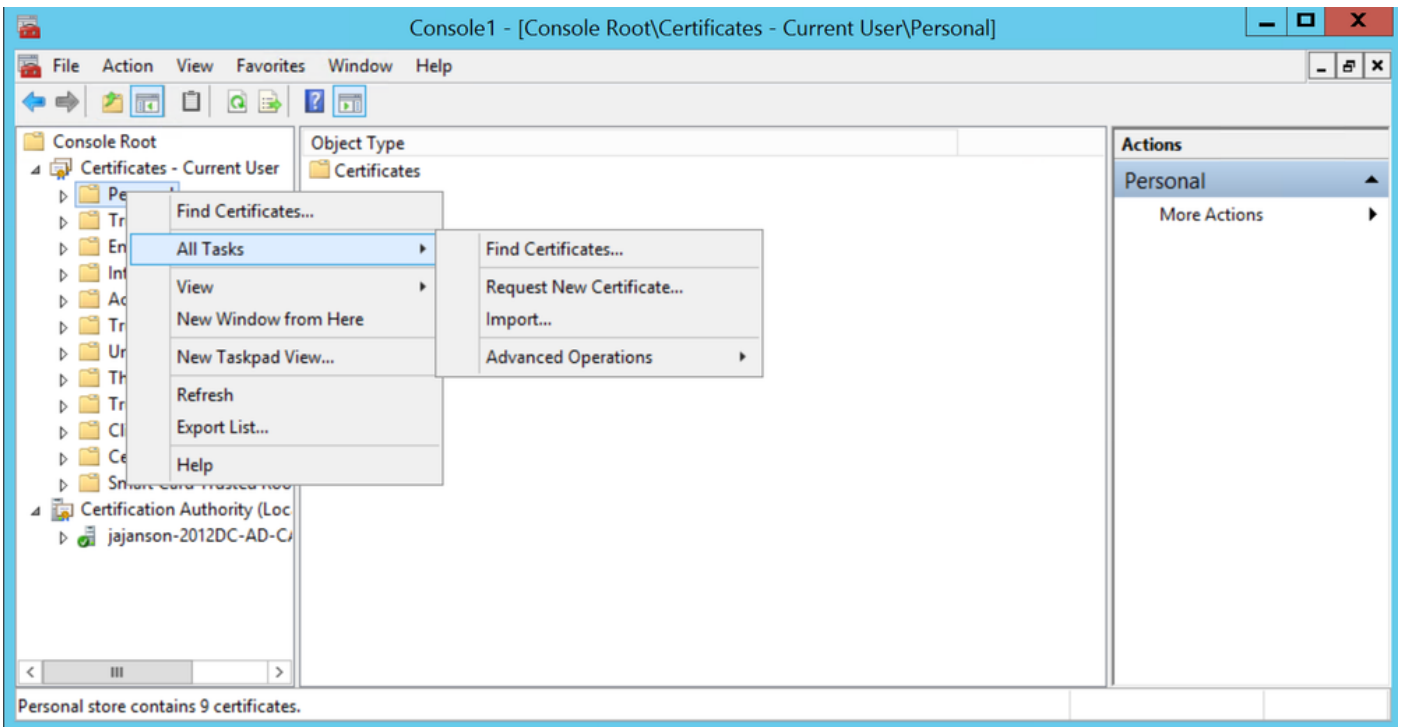
It is recommended that you do this on a Client Machine (IT Administrators Desktop).

1. Launch MMC choose **Certificates**, click **Add** then certificates for **My User Account**.



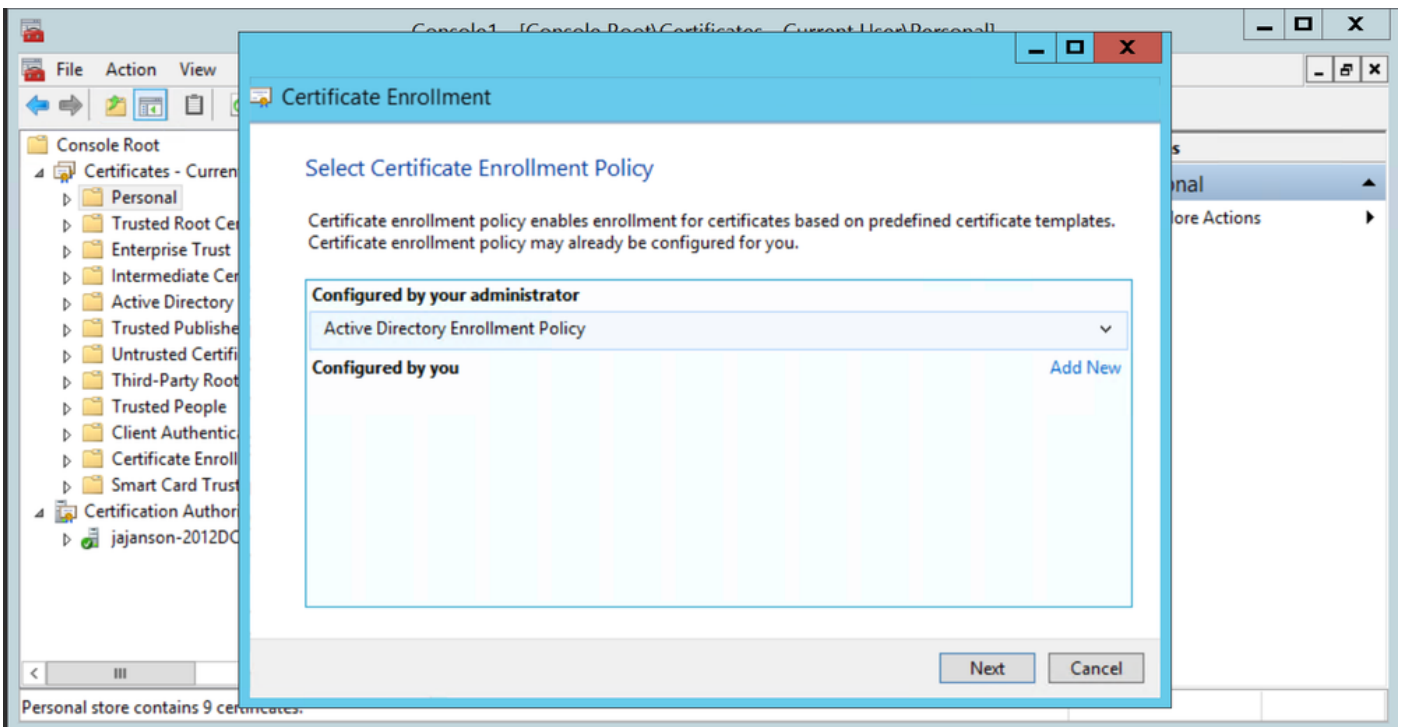
Add certificates

2. Right-click or select the **Personal Node**, select **All Tasks** and then select **Request New Certificate**.



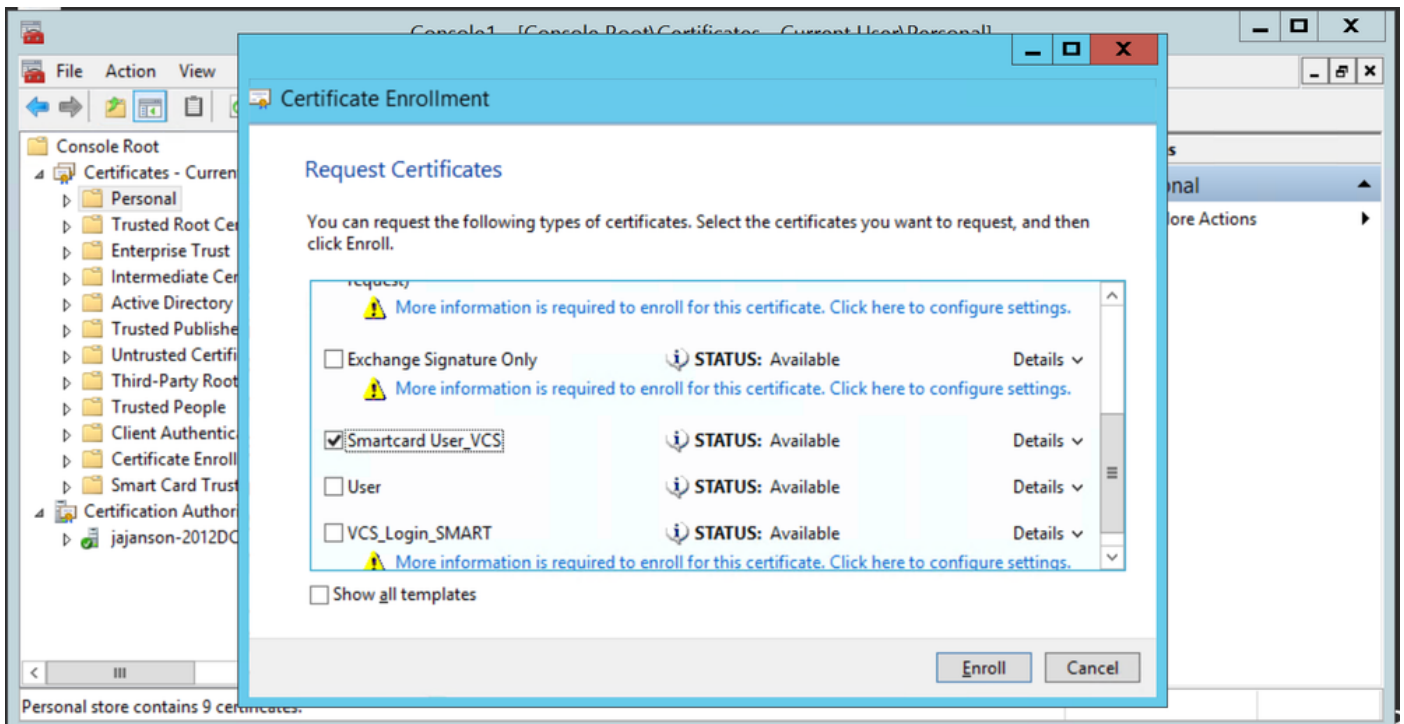
Request new certificates

3. Click **Next** on the wizard, and then select **Active Directory Enrollment Policy**. Then click **Next** again.



Active Directory Enrollement

4. Select the **Enrollment Agent Certificate**, in this case, **Smartcard User_VCS** and then click **Enroll**.

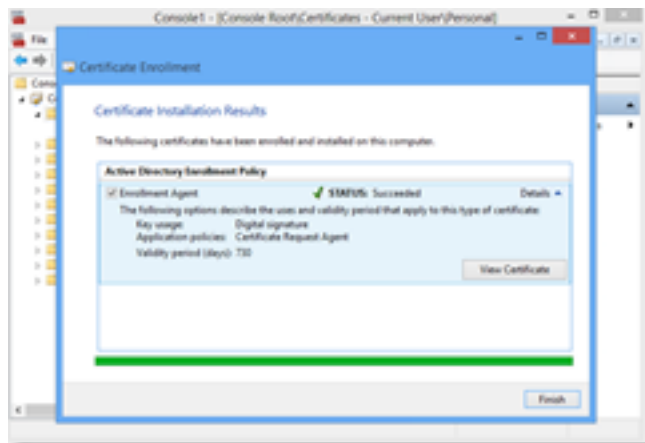


Enrollment Certificate Agent

Your IT Administrators desktop is now set up as an Enrollment Station, this enables you to enroll new smartcards on behalf of other users.

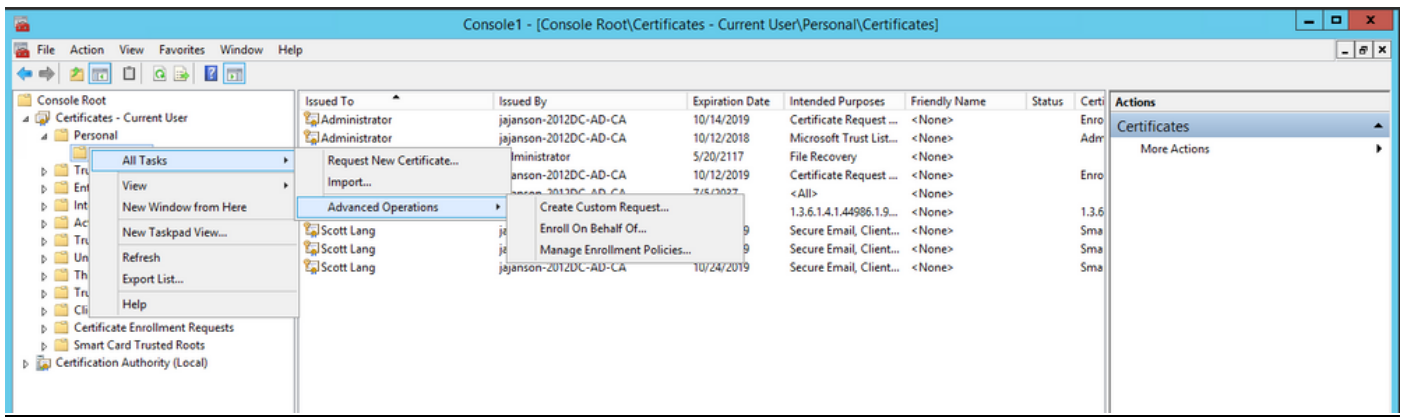
Enroll on behalf of....

In order for you to now provide employees with smartcards for authentication, you need to enroll them and generate the certificate which then is imported onto the Smartcard.

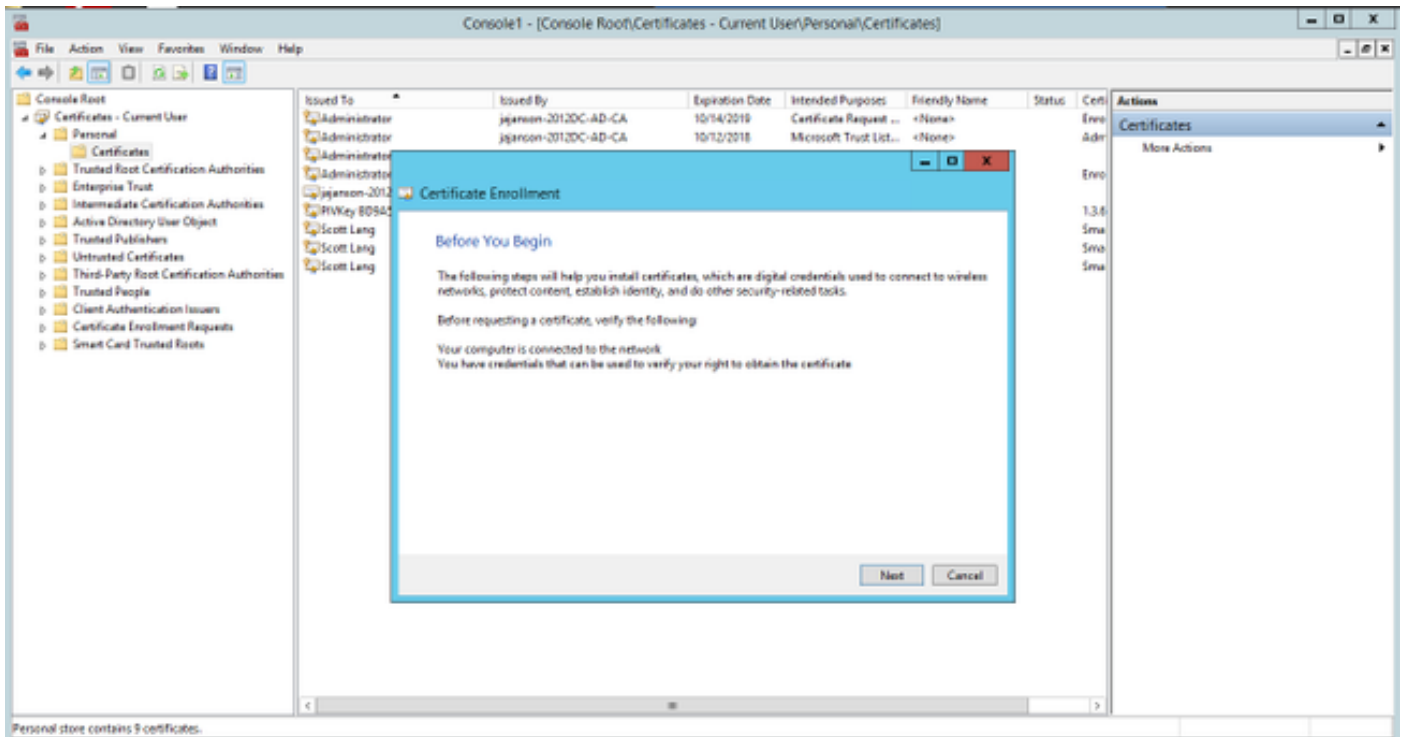


Enroll on behalf of

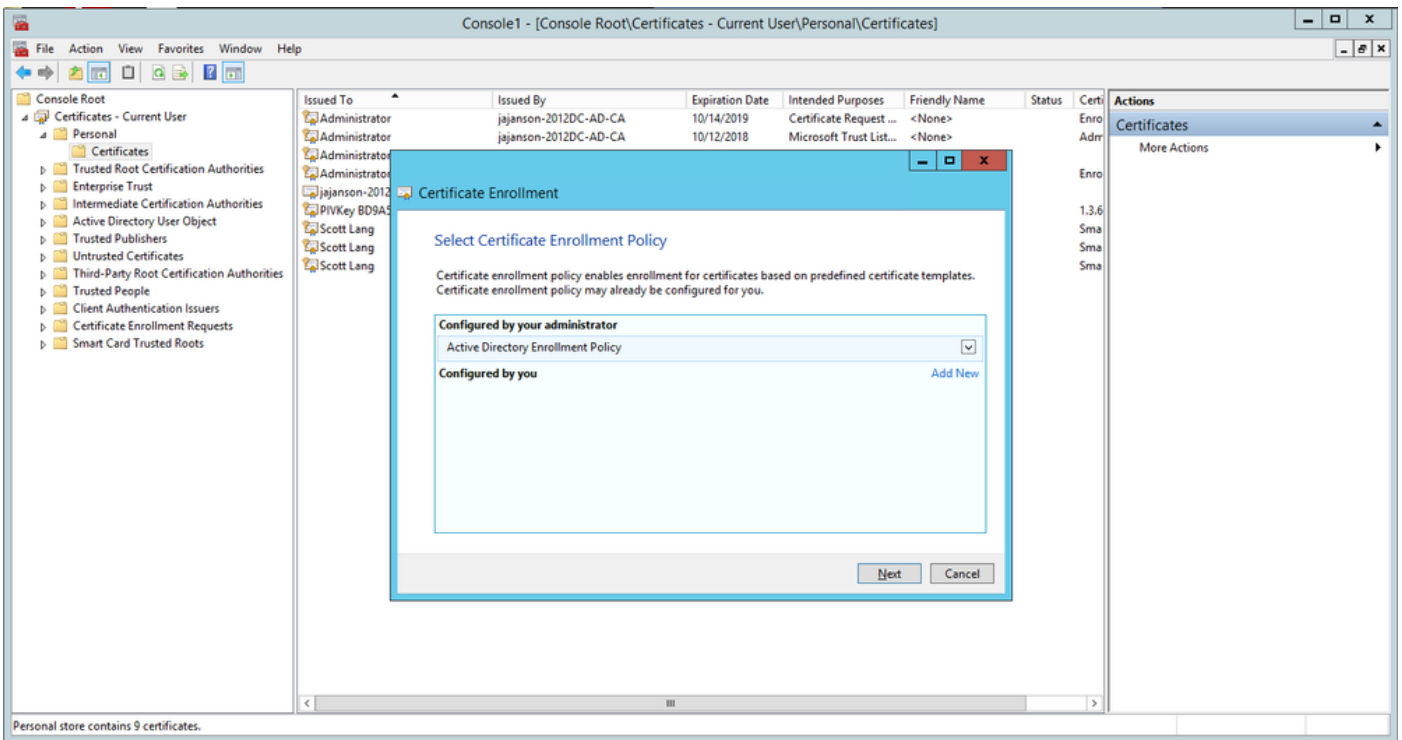
1. Launch MMC and import the **Certificates Module & Manger** the certificates for My User Account.
2. Right-click or select **Personal > Certificates** and select **All Tasks > Advanced Operations** and click **Enroll on behalf of...**
3. On the wizard, and choose the Active Directory Enrollment Policy then click **Next**.



Enroll on behalf advanced

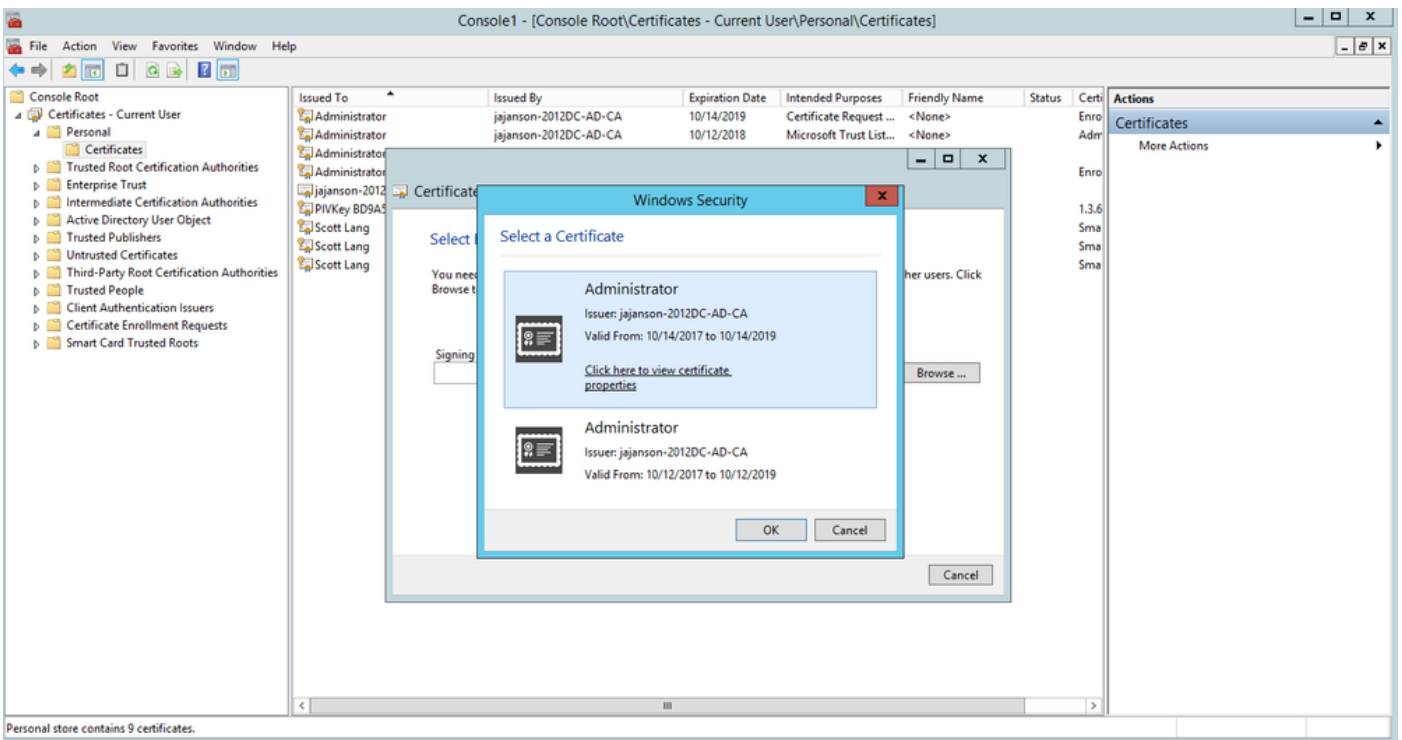


4. Select Certificate Enrollment Policy then click **Next**.



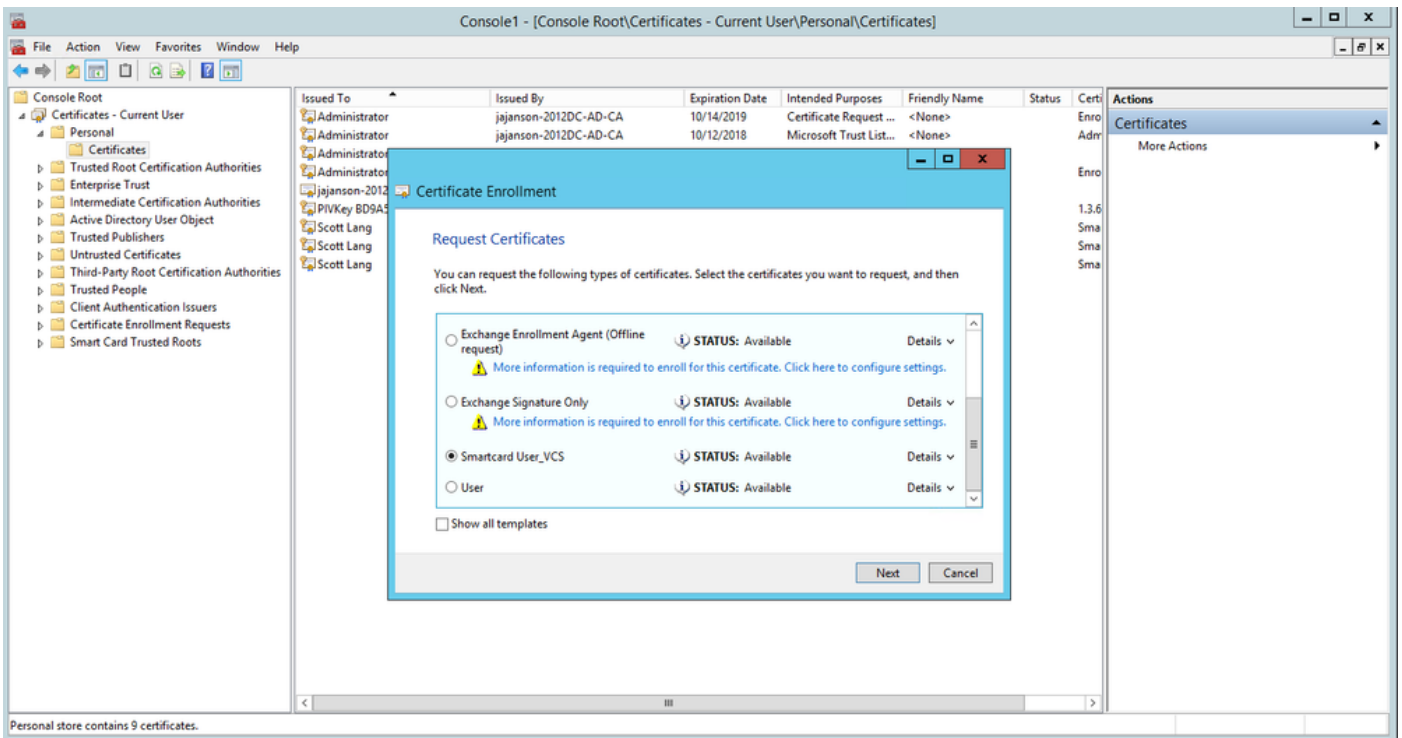
Enrollment policy

5. You are now asked to select the **Signing Certificate**. This is the enrollment certificate you requested earlier.



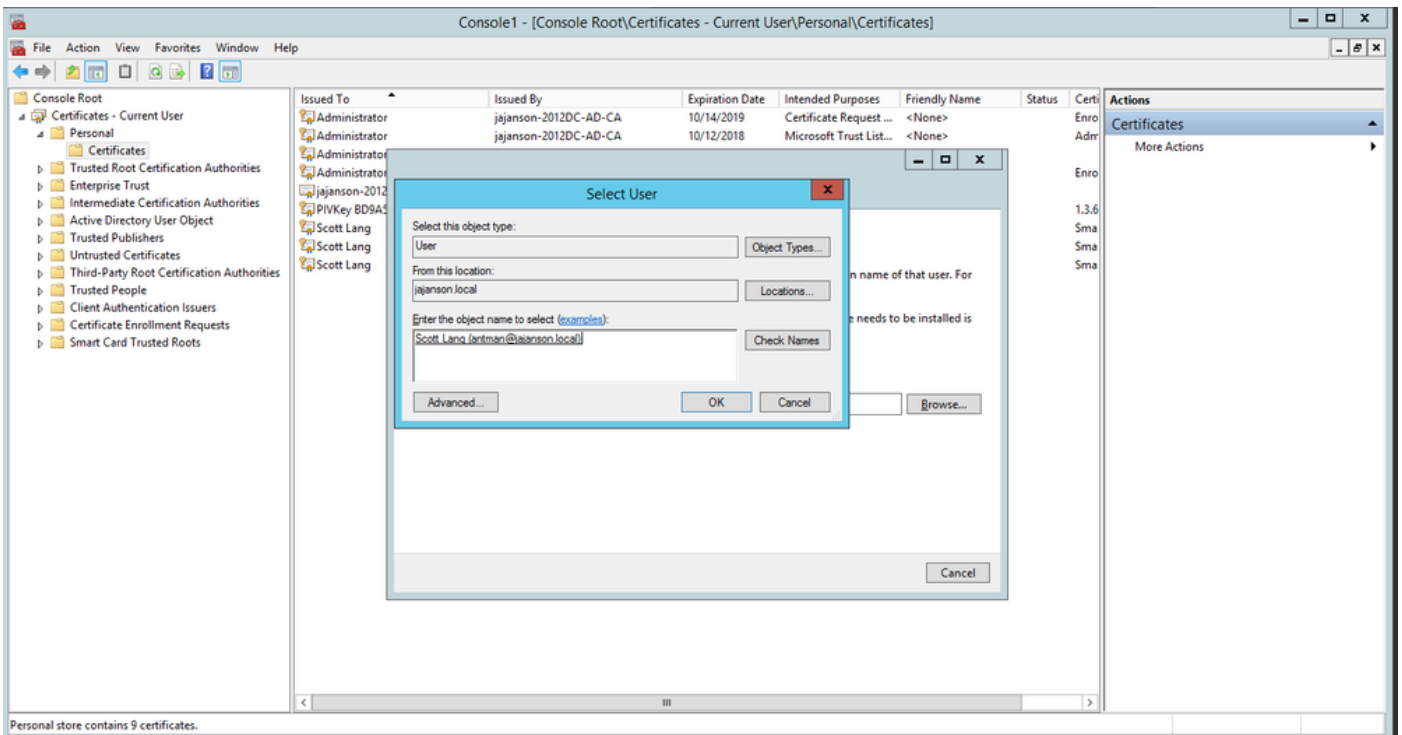
Select Signing Certificate

6. On the next screen, you need to browse to the certificate you would like to request and in this instance, it is **Smartcard User_VCS** which is the template you created earlier.



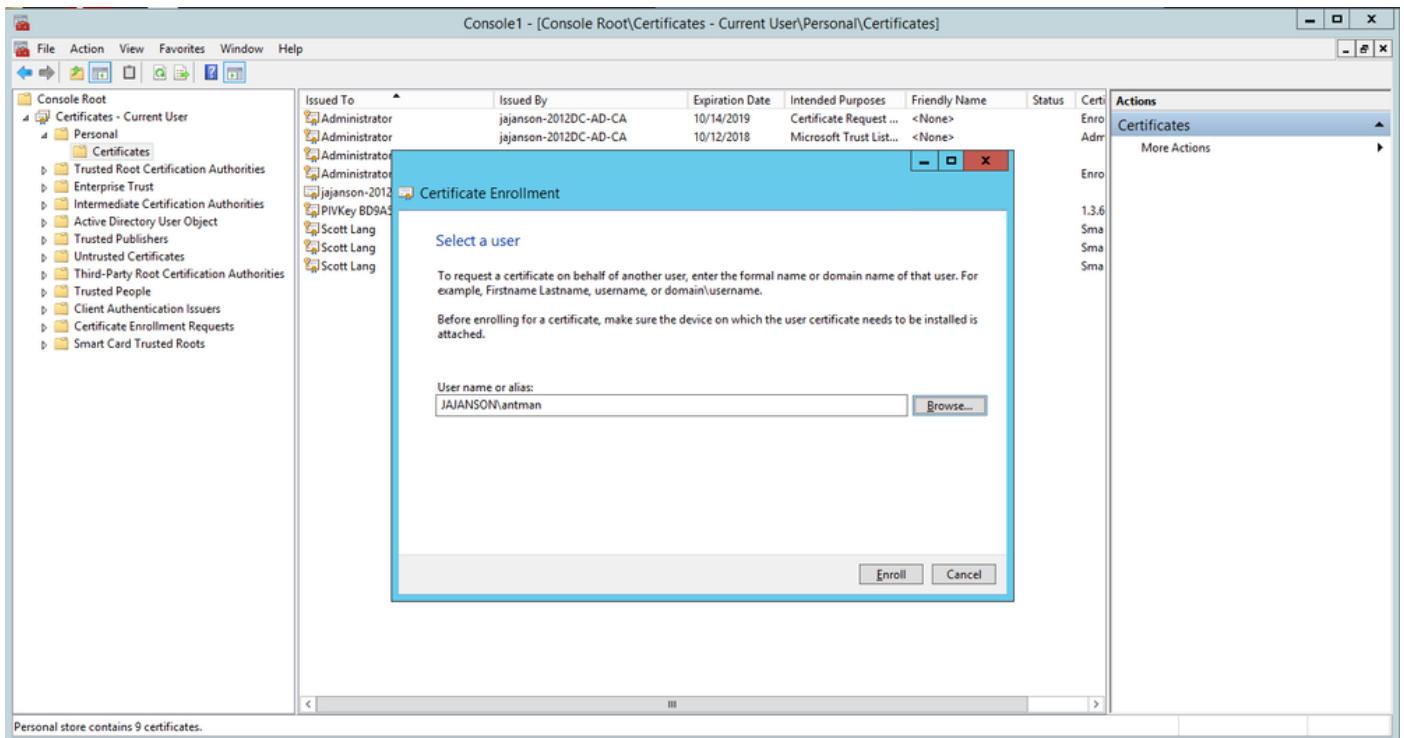
Choose the VCS Smart Card

7. Next, You need to select the user you wish to enroll on behalf of. Click **browse** and type in the username of the employee you wish to enroll. In this instance, Scott Lang 'antman@jajanson.local account' is used.



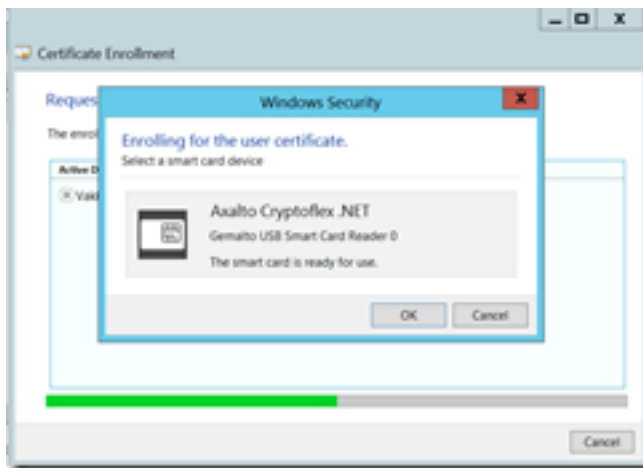
Choose the user

8. On the next screen, proceed with the enrollment by clicking on **Enroll**. Now, insert a smartcard into your reader.



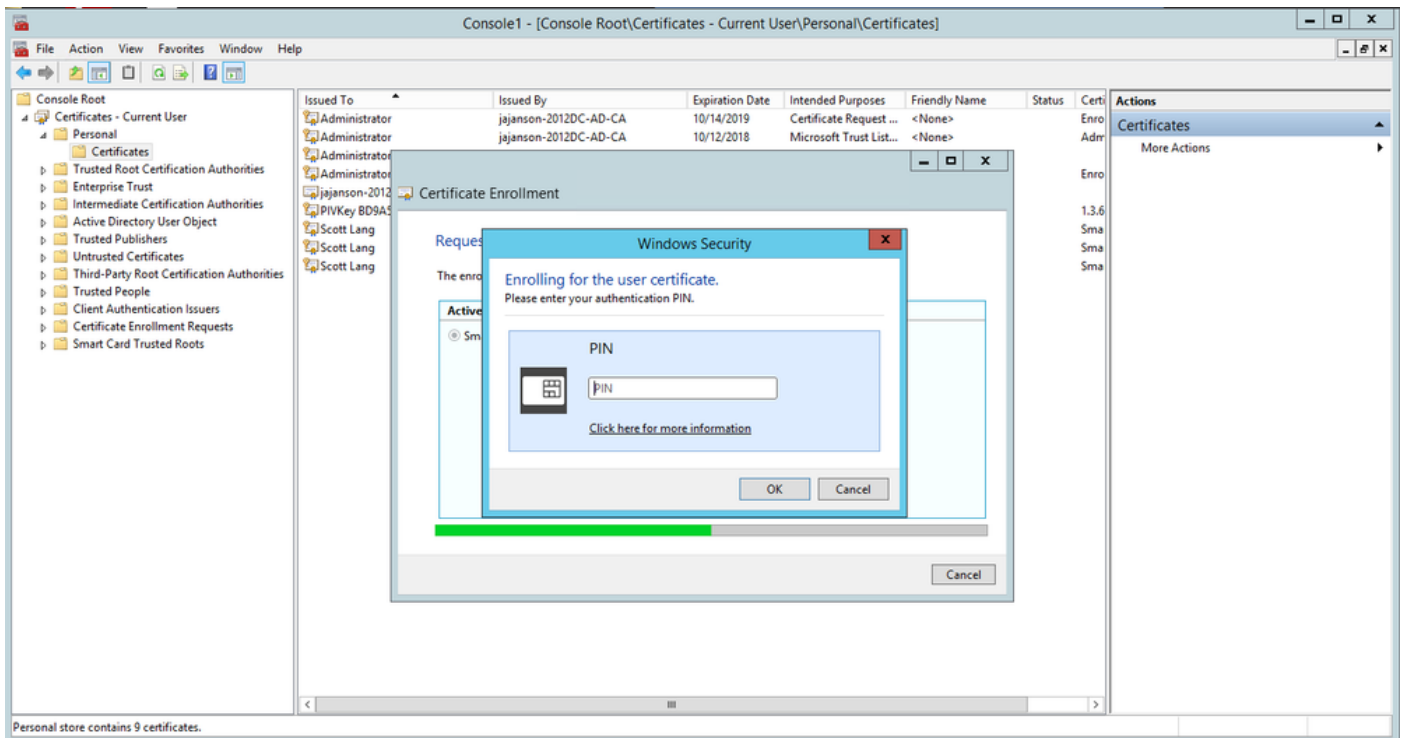
Enroll

9. Once you have inserted your smartcard, it's detected as follows:



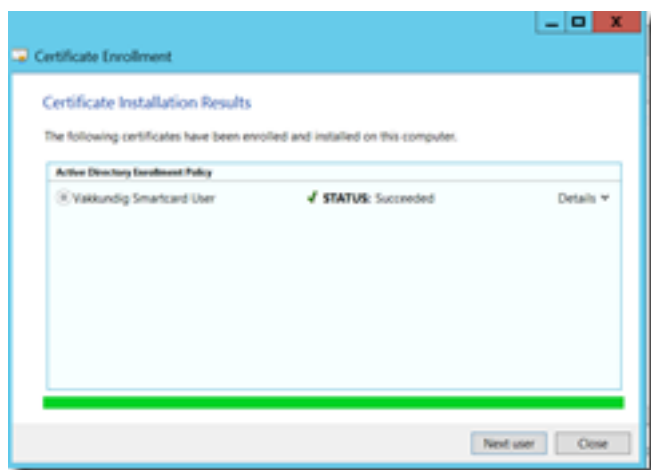
Insert the Smart Card

10. You are then asked to type in a smartcard PIN number (Default Pin: 0000).



Enter the pin

11. Finally, once you have seen the **Enrollment Successful** screen, you can then use this smartcard to log on to a domain-joined server, like the VCS with only the card and a known pin. However, it is not done yet, you still need to prepare the VCS to redirect authentication requests to the Smart Card and use Common Access Card to release the smartcard certificate stored on the smartcard for authentication.



Enrollment Successful

Configure the VCS for Common Access Card

Upload the Root CA to the Trusted CA Certificate list in the VCS by navigating to **Maintenance > Security > Trusted CA Certificate**.

2. Upload the Certificate Revocation List signed by the Root CA to the VCS. Navigate to **Maintenance > Security > CRL Management**.

3. Test your client certificate against your regex which pulls the username from the certificate to use for authentication against the LDAP or local user. The regex is going to match against the **Subject** of the certificate. This can be your UPN, Email and so on. In this lab, the email to match against the client certificate for the client certificate was used.

Certificate



General Details Certification Path

Show: <All>

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

Edit Properties...

Copy to File...

OK

Subject of Client Certificate

4. Navigate to **Maintenance > Security > Client Certificate Testing**. Select the client certificate to be tested, in My lab it was antman.pem, upload it to the test area. In the **Certificate-based authentication pattern** section under **Regex to match against certificate** paste your regex to be tested. Do not change the **Username format** field.

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

The screenshot shows the Cisco TelePresence Video Communication Server Expressway interface. The page title is "Client certificate testing". It is divided into two main sections: "Client certificate" and "Certificate-based authentication pattern".

In the "Client certificate" section, there is a "Certificate source" field with a dropdown menu set to "Uploaded test file (PEM format)". Below it is a "Browse" button with the text "No file selected" and a file name "antman.pem" is displayed.

In the "Certificate-based authentication pattern" section, there is a "Regex to match against certificates" field containing the regex: "/Subject:.*emailAddress=(?.*)@jajanson.local/m". Below it is a "Username format" field containing the text: "#captureCommonName#".

At the bottom of the "Certificate-based authentication pattern" section, there is a button labeled "Make these settings permanent".

Test your regex in VCS

Check certificate

Certificate test results	
Valid certificate:	OK
Source:	Uploaded test file (PEM format)
Filename:	antman.pem
Test pattern (as entered above):	
Regex:	/Subject: "emailAddress={?captureCommonName}*"@bjensen.localm
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:
            2410000001170f460b3102511a46513700000000000117
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=Antman,OU=CA,DC=bjensen,DC=local
        Validity
            Not Before: Oct 17 21:39:55 2017 GMT
            Not After: Oct 17 21:39:55 2017 GMT
        Subject: emailAddress={?captureCommonName}.*@Scott.Lmc.Quemeros.CC-System,DC=local
        Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
            009f4e0d0f4a12815a1517b46810246b1131d0771
            0c19a1081861374210917516d12d0f11391d91c1041
            61651d01f81761081c16d12410f10101f10101f101
            681f101081081f017a13112710e1410811711d11f1f01
            95132101f01010101010101010101010101010101
            a014411217181801041601081f1f7f413019c1951
            d0105161a1741010f10f105120100100101711a1
            c413217f14813614210419c13c10a1051f01671891201
    
```


← 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 permanently change the Regex. So do not worry that this section shows a failure because this is the current configuration not your test configuration above.

Testing Results


5. If the testing is providing you with the desired results then you can click the button **Make these changes permanent**. This changes your regex for the **Certificate-based authentication configuration** of the server. In order to verify the change, navigate to that configuration, **Maintenace > Security > Certificate-based authentication configuration**.


6. Enable client-based authentication by navigating to **System > Administrator** and then click or select drop down box to choose **Client certificate-based security = Client-Based Authentication**. With this setting, the user types the FQDN of the VCS server in his browser and he is prompted to choose his client account and enter the pin assigned to his Common Access Card. Then the certificate is released and he gets returned the Web GUI of the VCS server and all he needs to do is click or select the Administrator button. Then he is admitted into the server. If the options **Client certificate-based security = Client-Based Validation** is selected, the process is the same with the exception when the user clicks the Administrator button, he has prompted again for the admin password. Usually, the latter is not what the organization is trying to accomplish with CAC.


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 

Save

Drop down the above box and choose Client-Based Authentication

Related tasks

[Upload a CA certificate file for HTTPS](#)

[Test client certificates](#)

Enable client based authentication

Help! I am locked out!!!

If you enable the Client Based Authentication and the VCS rejects the certificate for whatever reason, you are not going to be able to log in with to the web GUI in the traditional way anymore. But, do not fret there is a way to get back into your system. The attached document can be found on the Cisco website and provides information on how to disable Client Based Authentication from root access.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.