

# Configuración de VCS con CAC y lector de tarjetas inteligentes

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[¿Qué es una tarjeta inteligente?](#)

[Configurar](#)

[Verificación](#)

[Troubleshoot](#)

## Introducción

Este documento describe una guía paso a paso para instalar y utilizar un lector de tarjetas inteligentes y una tarjeta de acceso común para usarlas con Cisco Video Communication Server (VCS) para organizaciones que requieren autenticación de dos factores en el entorno VCS, como bancos, hospitales o gobiernos con instalaciones seguras.

## Prerequisites

### Requirements

No hay requisitos específicos para este documento.

### Componentes Utilizados

La información de este documento se basa en 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

El CAC proporciona la autenticación necesaria para que los "sistemas" sepan quién ha tenido acceso a su entorno y qué parte de la infraestructura, ya sea física o electrónica. Dentro de los entornos clasificados por el gobierno y otras redes seguras, prevalecen las reglas de "acceso menos privilegiado" o "necesidad de saber". Cualquier usuario podría utilizar un inicio de sesión, la autenticación requiere algo que el usuario tiene, además de que el CAC, también conocido como la Tarjeta de acceso común, surgió en 2006 para que el individuo no necesite tener varios dispositivos, ya sean fobs, tarjetas de identificación o dongles para acceder a su lugar de trabajo

o sistemas.

## ¿Qué es una tarjeta inteligente?

Las tarjetas inteligentes son un componente clave de la infraestructura de clave pública (PKI) que Microsoft utiliza para integrarse en la plataforma de Windows porque las tarjetas inteligentes mejoran las soluciones de software únicamente, como la autenticación de clientes, el inicio de sesión y el correo electrónico seguro. Las tarjetas inteligentes son un punto de convergencia para los certificados de clave pública y las claves asociadas porque:

- Proporcionar almacenamiento a prueba de manipulación para la protección de claves privadas y otras formas de información personal.
- Aísle los cálculos críticos para la seguridad, que implican autenticación, firmas digitales e intercambio de claves de otras partes del sistema que no necesitan saberlo.
- Habilite la portabilidad de las credenciales y otra información privada entre los ordenadores en el trabajo, en casa o de viaje.

La tarjeta inteligente se ha convertido en una parte integral de la plataforma de Windows porque las tarjetas inteligentes proporcionan características nuevas y deseables como revolucionarias para el sector informático, como la introducción del ratón o el CD-ROM. Si no dispone de una infraestructura PKI interna en este momento, debe asegurarse primero de que lo hace. Este documento no cubre la instalación de este rol en este artículo en particular, pero la información sobre cómo implementarlo puede encontrarse aquí: <http://technet.microsoft.com/en-us/library/hh831740.aspx>.

## Configurar

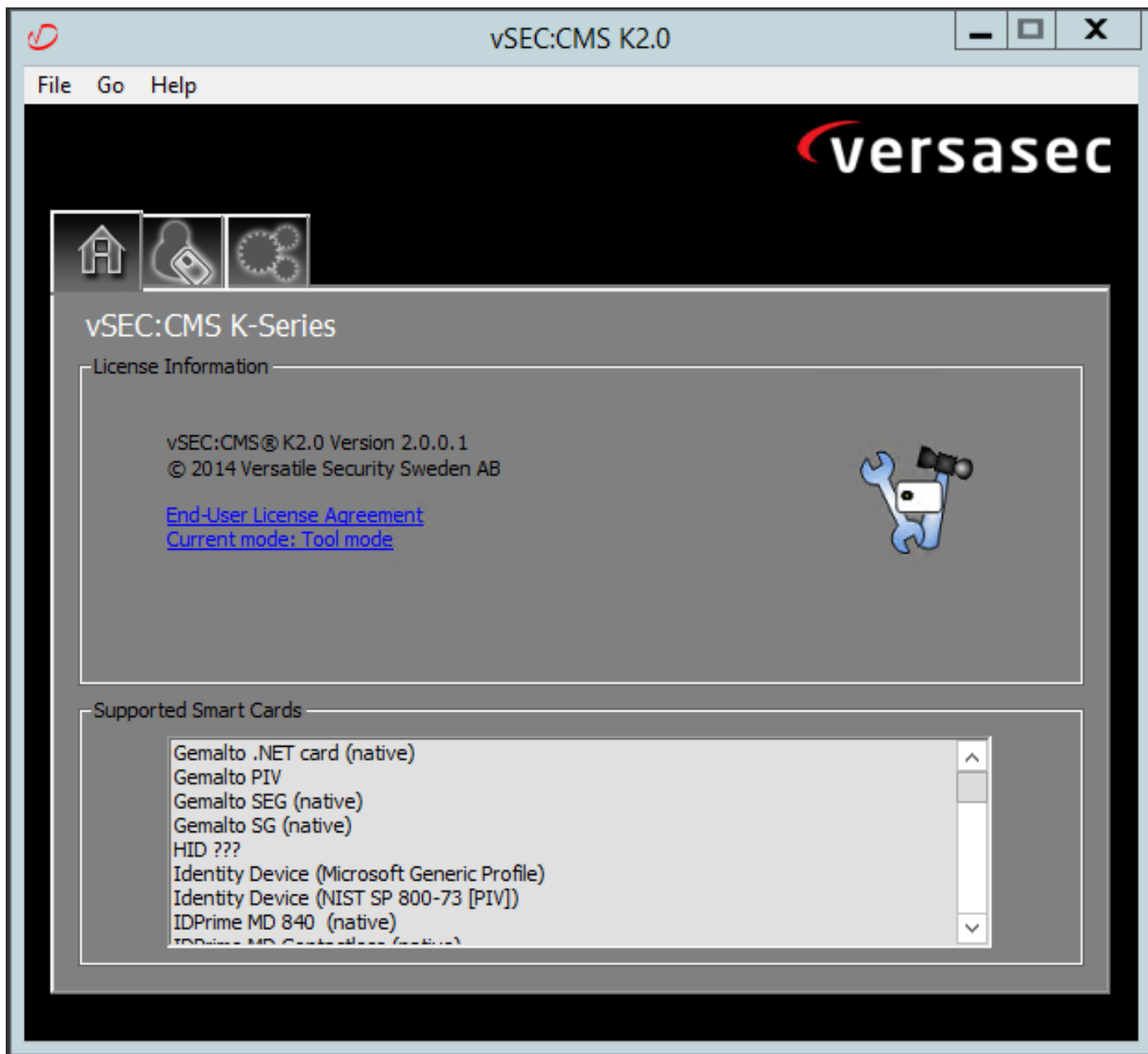
Este laboratorio asume que ya ha integrado LDAP con VCS y tiene usuarios que pueden iniciar sesión con credenciales LDAP.

1. [Equipo de laboratorio](#)
2. [Instalación de la tarjeta inteligente](#)
3. [Configurar plantillas de autoridad de certificados](#)
4. [Inscripción del Certificado del Agente de Inscripción](#)
5. [Inscríbase en nombre de...](#)
6. [Configuración de VCS para la tarjeta de acceso común](#)

Equipo requerido:

Servidor de dominio Windows 2012R2 que tiene estas funciones/software instalado:

- Autoridad de certificados
- Active Directory
- DNS
- PC Windows con tarjeta inteligente conectada
- vSEC: Software de gestión CMS serie K para gestionar su tarjeta inteligente:



Versa Card Reader Software

## Instalación de la tarjeta inteligente

Los lectores de tarjetas inteligentes generalmente incluyen instrucciones sobre cómo conectar los cables necesarios. Este es un ejemplo de instalación para esta configuración.

### Cómo instalar un controlador de dispositivo lector de tarjetas inteligentes

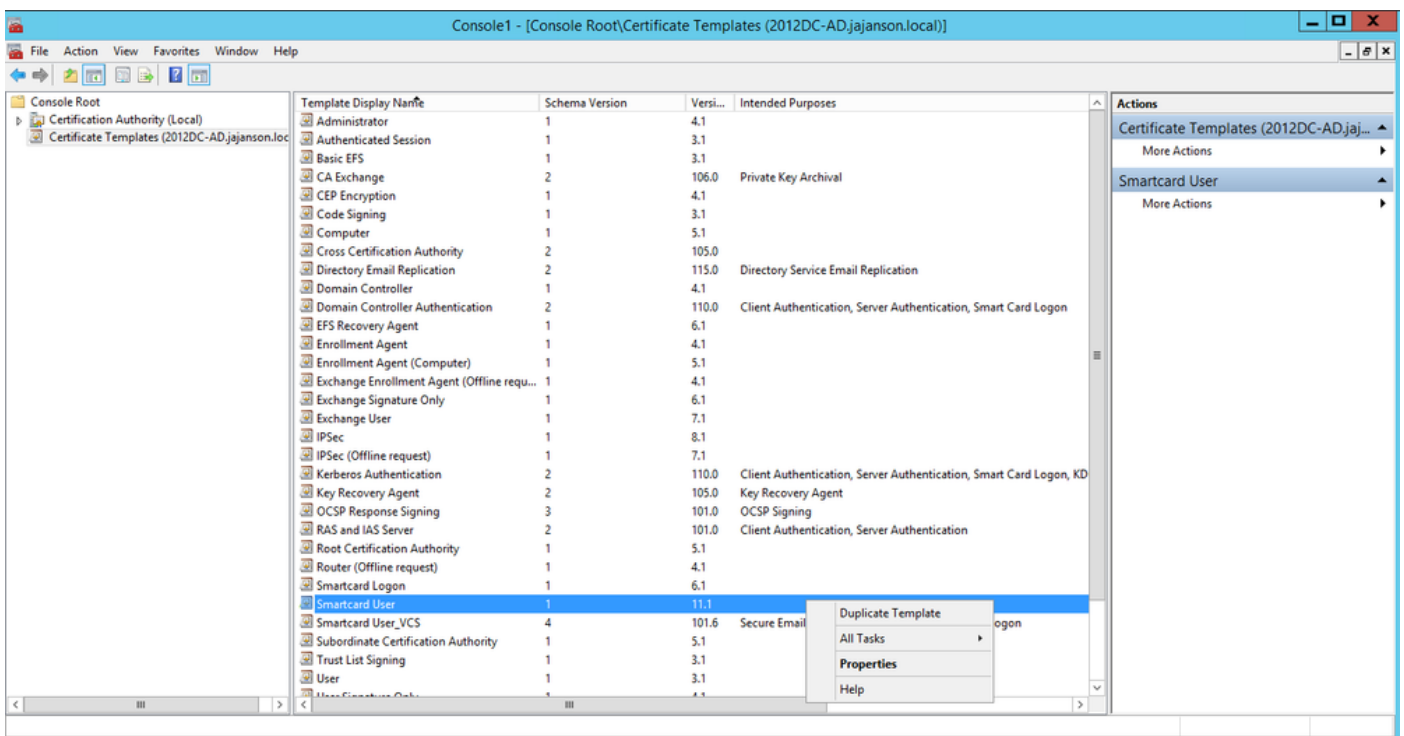
Si se ha detectado e instalado el lector de tarjetas inteligentes, la pantalla Welcome to Windows Logon (Bienvenido al inicio de sesión de Windows) lo reconoce. En caso contrario:

1. Conecte la tarjeta inteligente al puerto USB del PC con Windows
2. Siga las instrucciones que aparecen en la pantalla para instalar el software del controlador del dispositivo. Esto requiere que el medio del controlador que el fabricante de la tarjeta inteligente o el controlador se descubra en Windows. En mi caso, usé el controlador de manufacturas de su sitio de descarga. **NO CONFÍES EN WINDOWS.**
3. Haga clic con el botón derecho del ratón en el icono **Mi PC** del escritorio y haga clic en **Administrar** en el submenú.

4. Expanda el nodo **Servicios y aplicaciones** y haga clic en **Servicios**.
5. En el panel derecho, haga clic con el botón derecho del ratón en **Tarjeta inteligente**. Haga clic en **Propiedades** en el submenú.
6. En la ficha **General**, seleccione **Automático** en la lista desplegable **Tipo de inicio**. Click OK.
7. Reinicie el equipo si el asistente de hardware se lo indica.

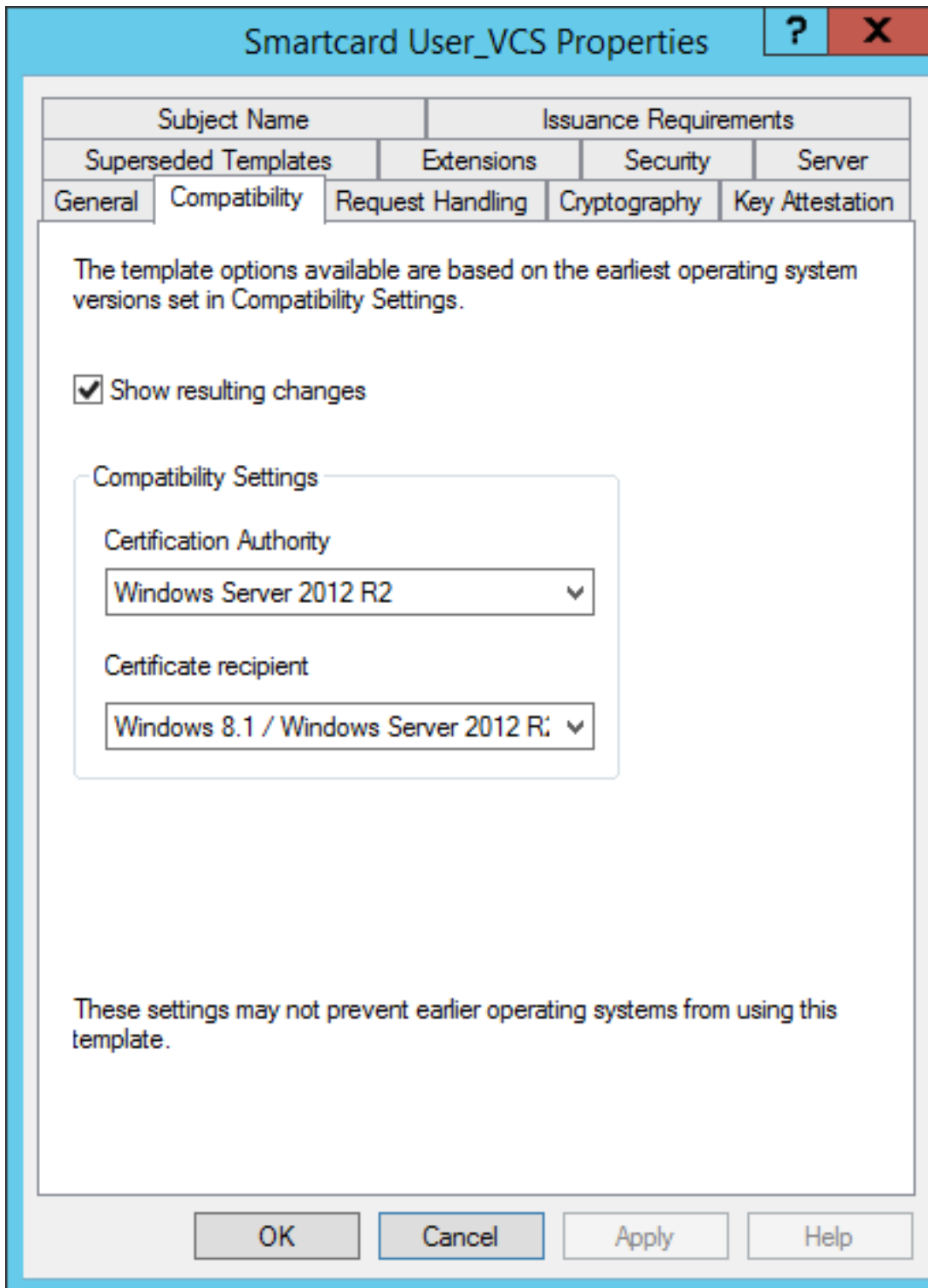
### Configurar plantillas de autoridad de certificados

1. Inicie MMC de Autoridad de Certificación desde Herramientas Administrativas.
2. Haga clic o seleccione el nodo **Plantillas de certificado** y seleccione **Administrar**.
3. Haga clic con el botón derecho del ratón o seleccione la plantilla de certificado de **usuario de Smartcard** y, a continuación, seleccione **Duplicar** como se muestra en la imagen.



### Plantillas de certificado de controlador de dominio

4. En la ficha **Compatibilidad**, en **Autoridad de certificación**, revise la selección y cámbiela si es necesario.



Configuración de

compatibilidad de tarjetas inteligentes

5. En la pestaña **General**:

a. Especifique un nombre, como **Smartcard User\_VCS**.

b. Establezca el período de validez en el valor deseado. Haga clic en Apply (Aplicar).

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

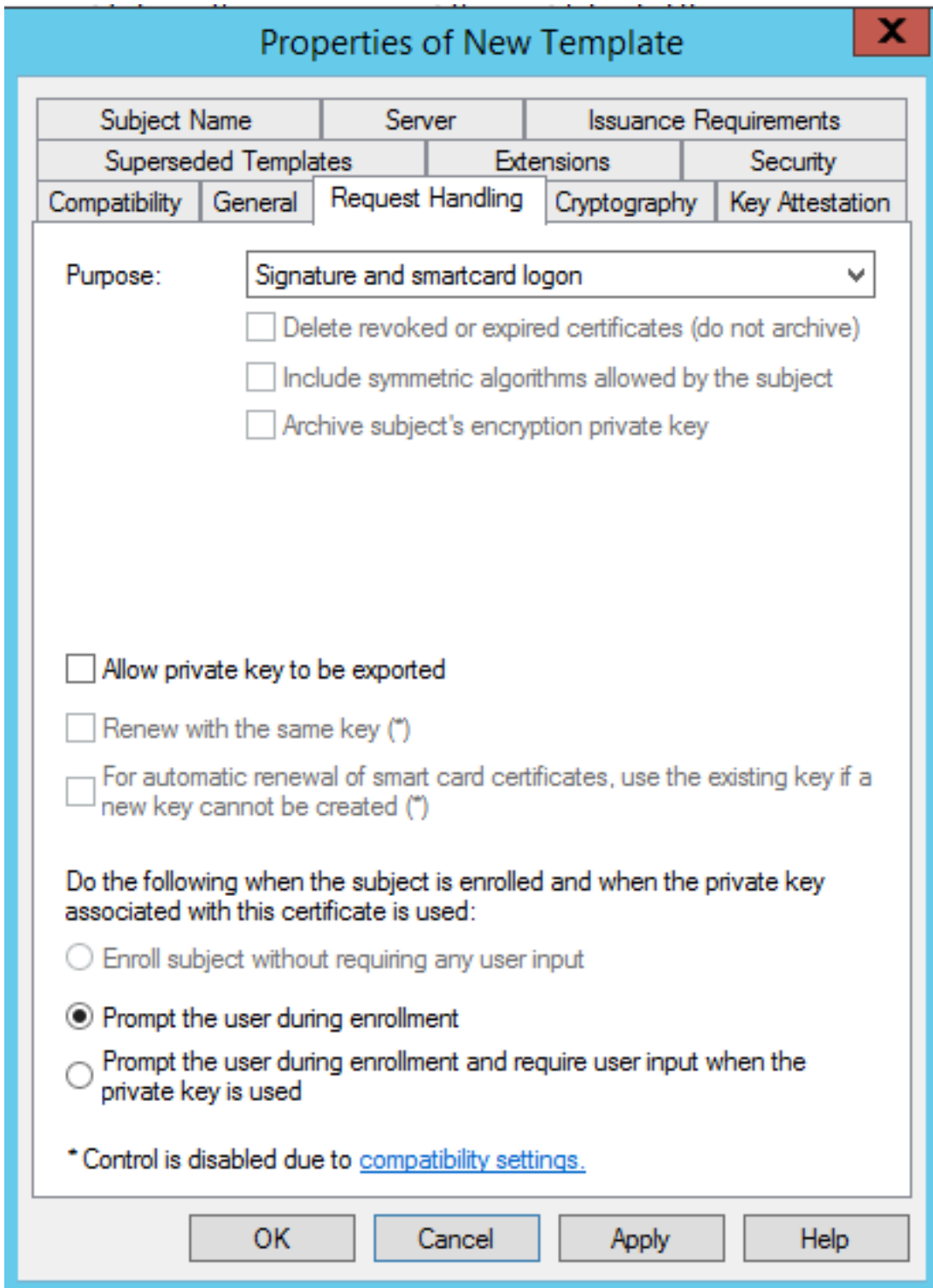
Hora de inicio de la

tarjeta inteligente

6. En la ficha **Gestión de solicitudes**:

a. Establezca el **Propósito** en **Firma e inicio de sesión con tarjeta inteligente**.

b. Haga clic en **Preguntar al usuario durante la inscripción**. Haga clic en **Apply** (Aplicar).



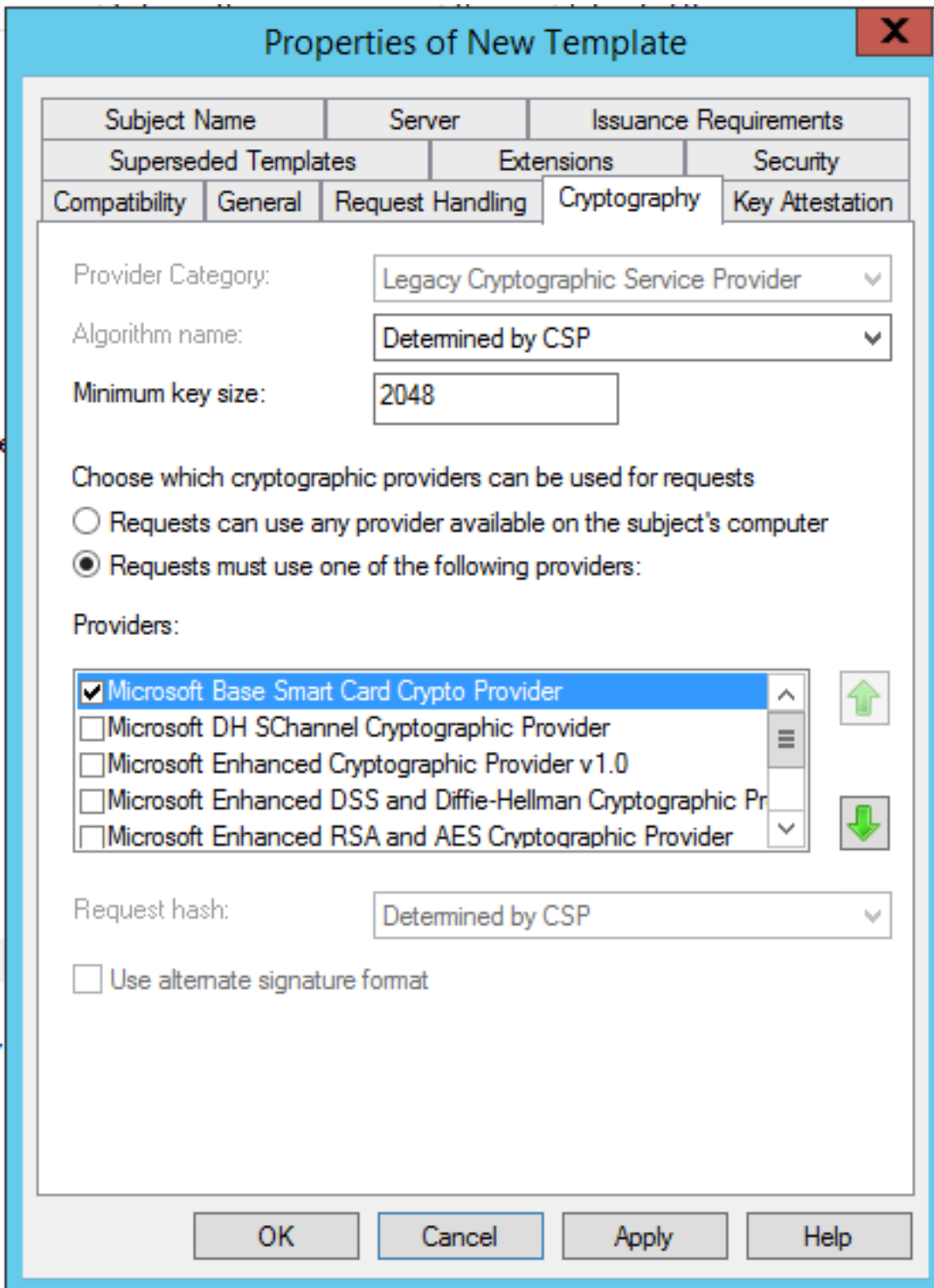
Gestión de

### solicitudes de tarjetas inteligentes

7. En la ficha **Criptografía**, establezca el tamaño mínimo de clave en 2048.

a. Haga clic en **Solicitudes debe utilizar uno de los siguientes proveedores** y, a continuación, seleccione **Proveedor criptográfico de Microsoft Base**.

b. Haga clic en **Apply** (Aplicar).

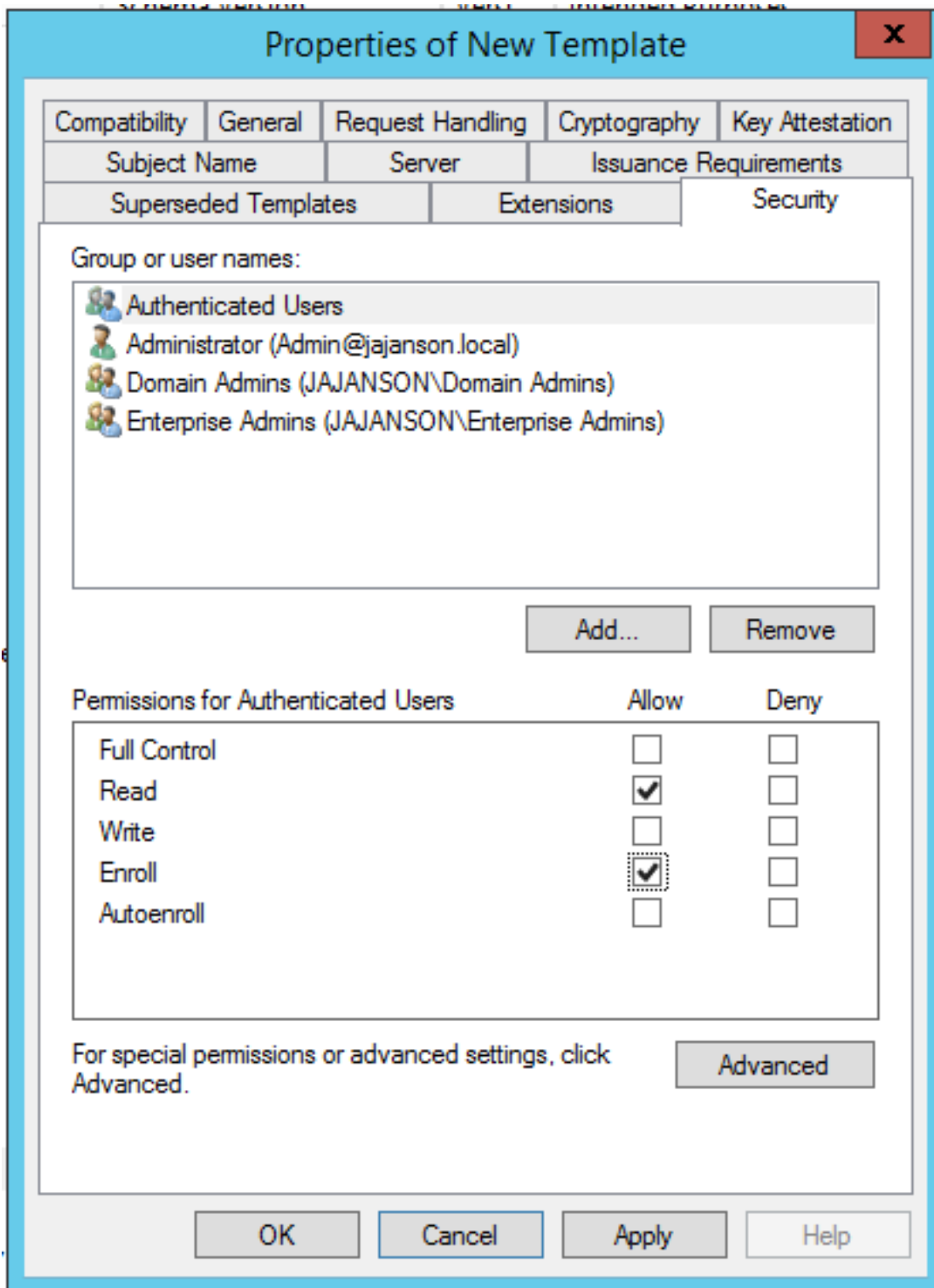


Configuración de

cifrado del certificado

8. En la ficha Seguridad, agregue el grupo de seguridad al que desea otorgar acceso al Registro. Por ejemplo, si desea otorgar acceso a todos los usuarios, seleccione el grupo Usuarios autenticados y, a continuación, seleccione **Inscribir** permisos para ellos.

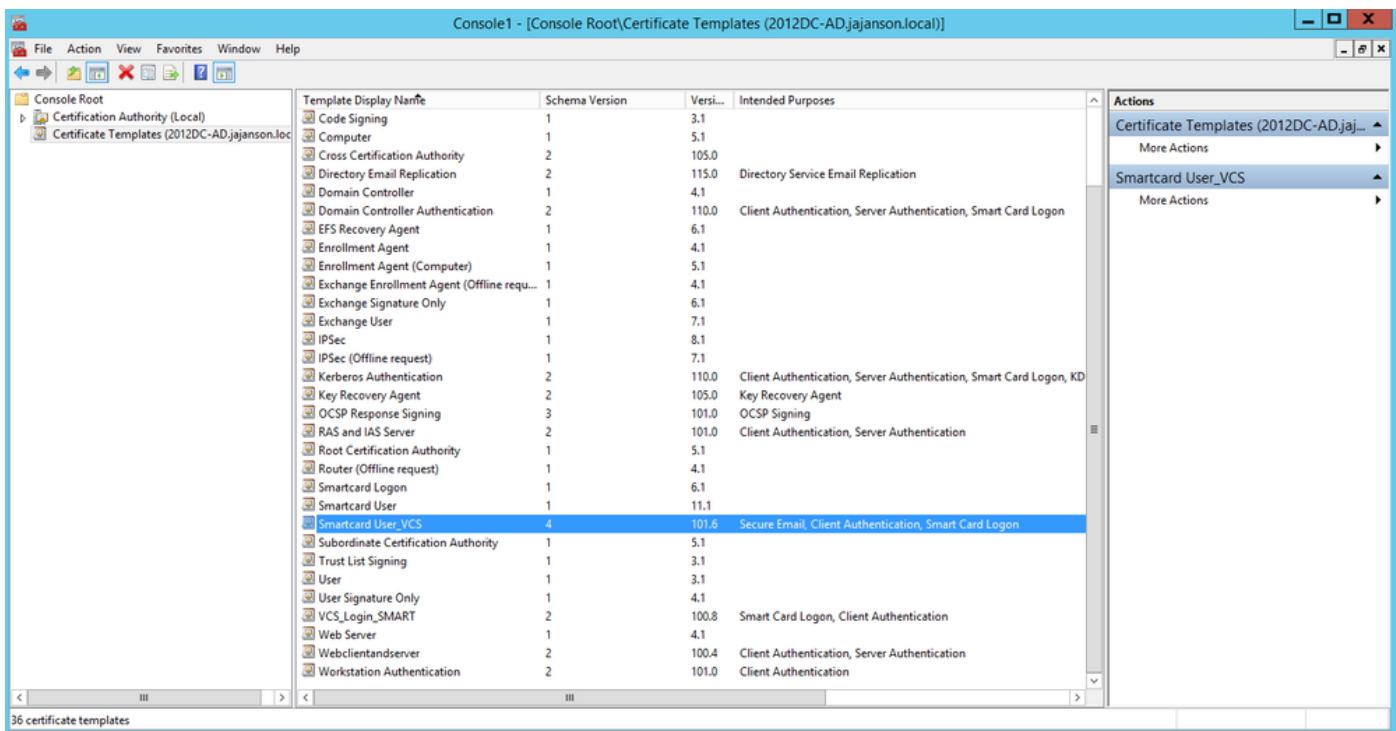




Seguridad de la

plantilla

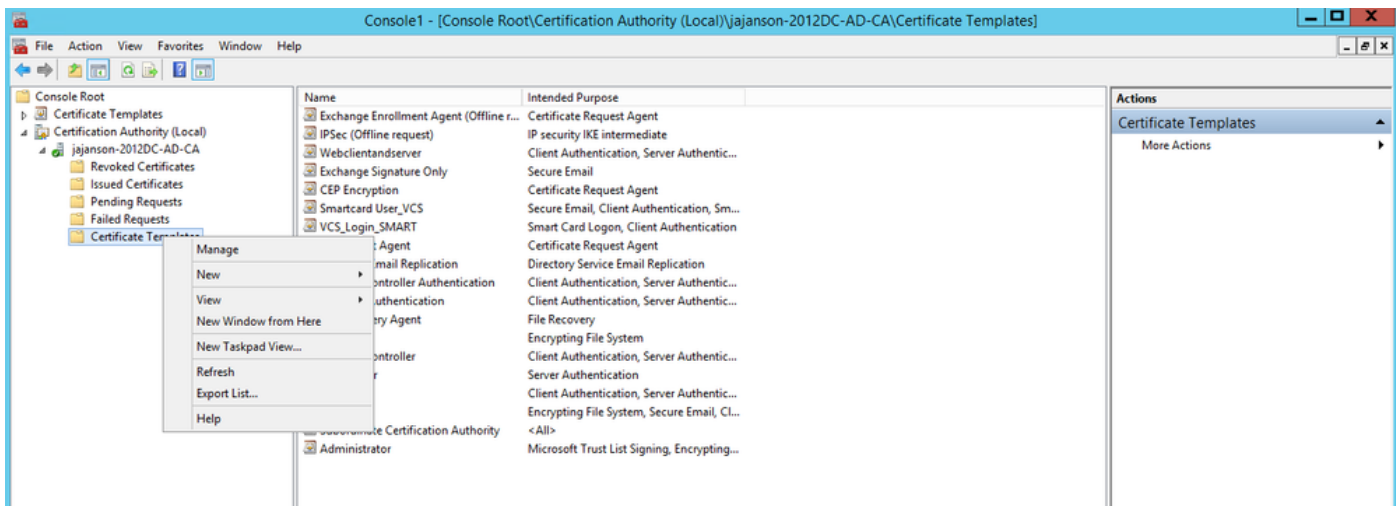
9. Haga clic en **Aceptar** para finalizar los cambios y crear la nueva plantilla. La nueva plantilla debe aparecer ahora en la lista Plantillas de certificados.



Plantilla vista en el control de dominio

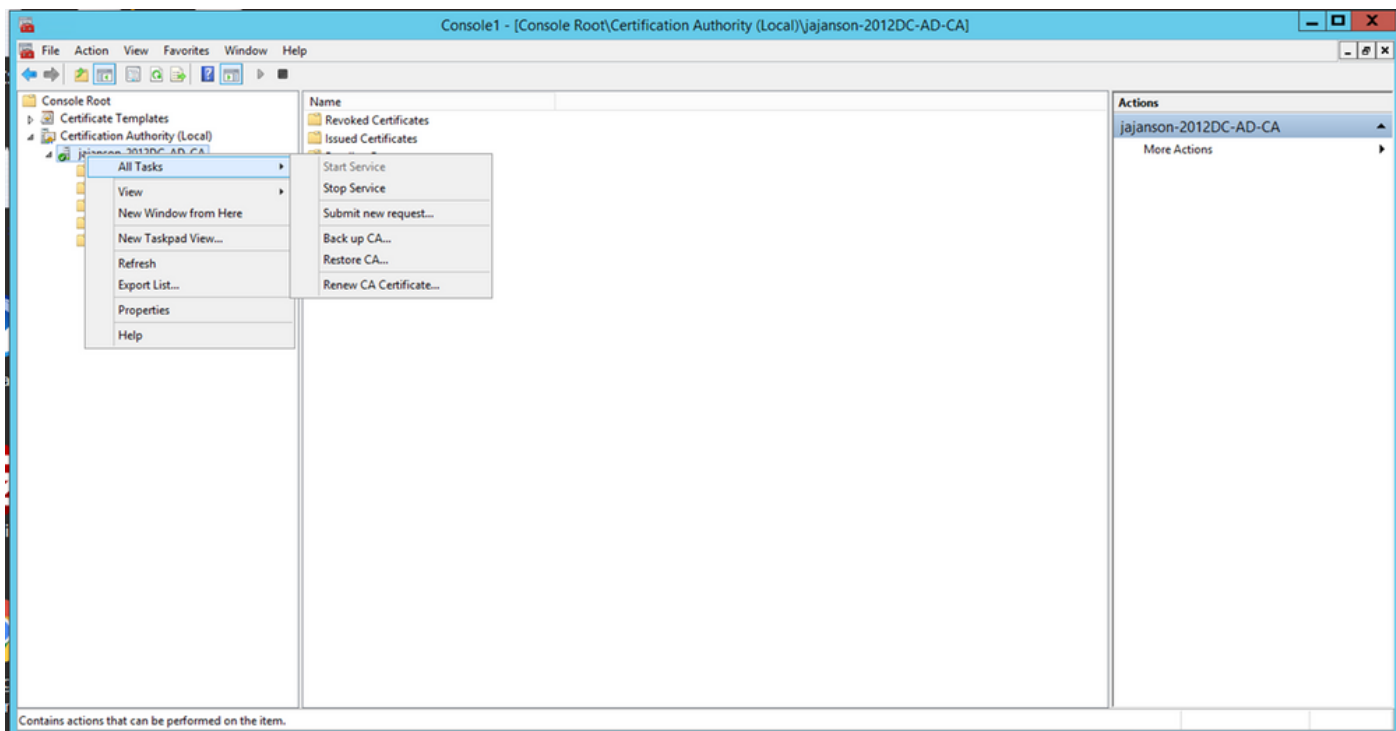
10. En el panel izquierdo de MMC, expanda Certification Authority (Local) y, a continuación, expanda su CA dentro de la lista Certification Authority (Autoridad de certificación).

Haga clic con el botón derecho del ratón en Plantillas de certificado, haga clic en **Nuevo** y, a continuación, haga clic en **Plantilla de certificado** para emitir. A continuación, elija la plantilla Smartcard recién creada.



Ejecutar nueva plantilla

11. Después de que la plantilla se replique, en el MMC, haga clic con el botón derecho del ratón o seleccione la lista Entidad de certificación, haga clic en **Todas las tareas** y, a continuación, haga clic en **Detener servicio**. A continuación, vuelva a hacer clic con el botón derecho del ratón en el nombre de la CA, haga clic en **Todas las tareas** y, a continuación, haga clic en **Iniciar servicio**.

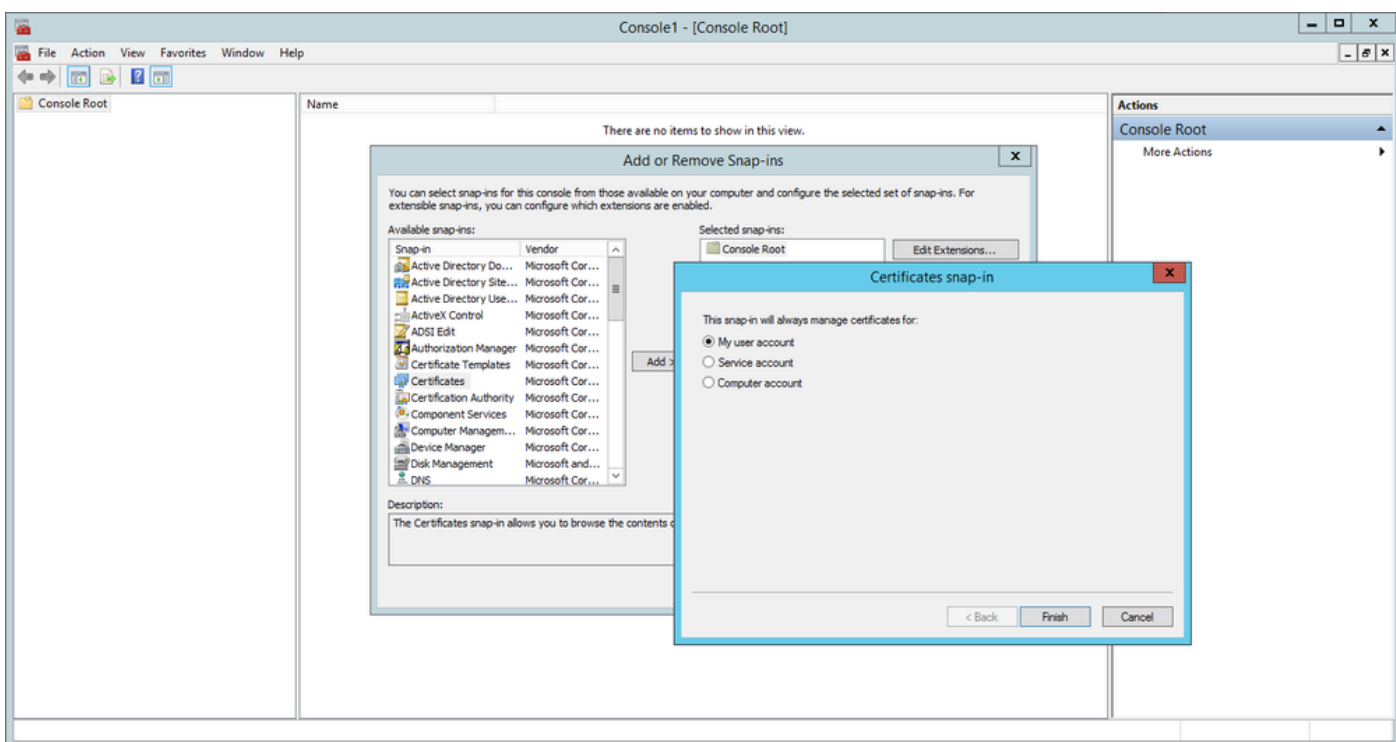


Detener luego iniciar servicios de certificados

## Inscríbese en el Certificado de agente de inscripción

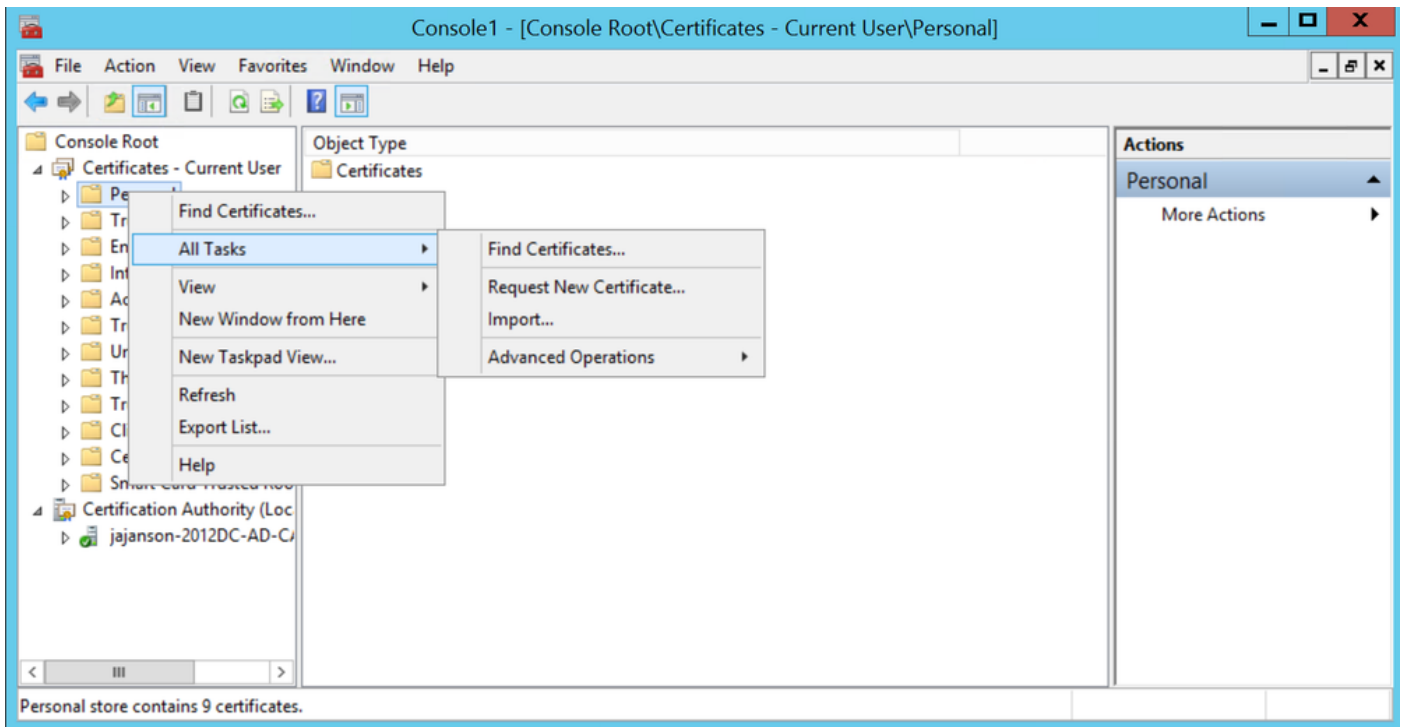
Se recomienda hacerlo en un equipo cliente (escritorio de administradores de TI).

1. Inicie MMC elija **Certificados**, haga clic en **Agregar** y luego en certificados para **Mi cuenta de usuario**.



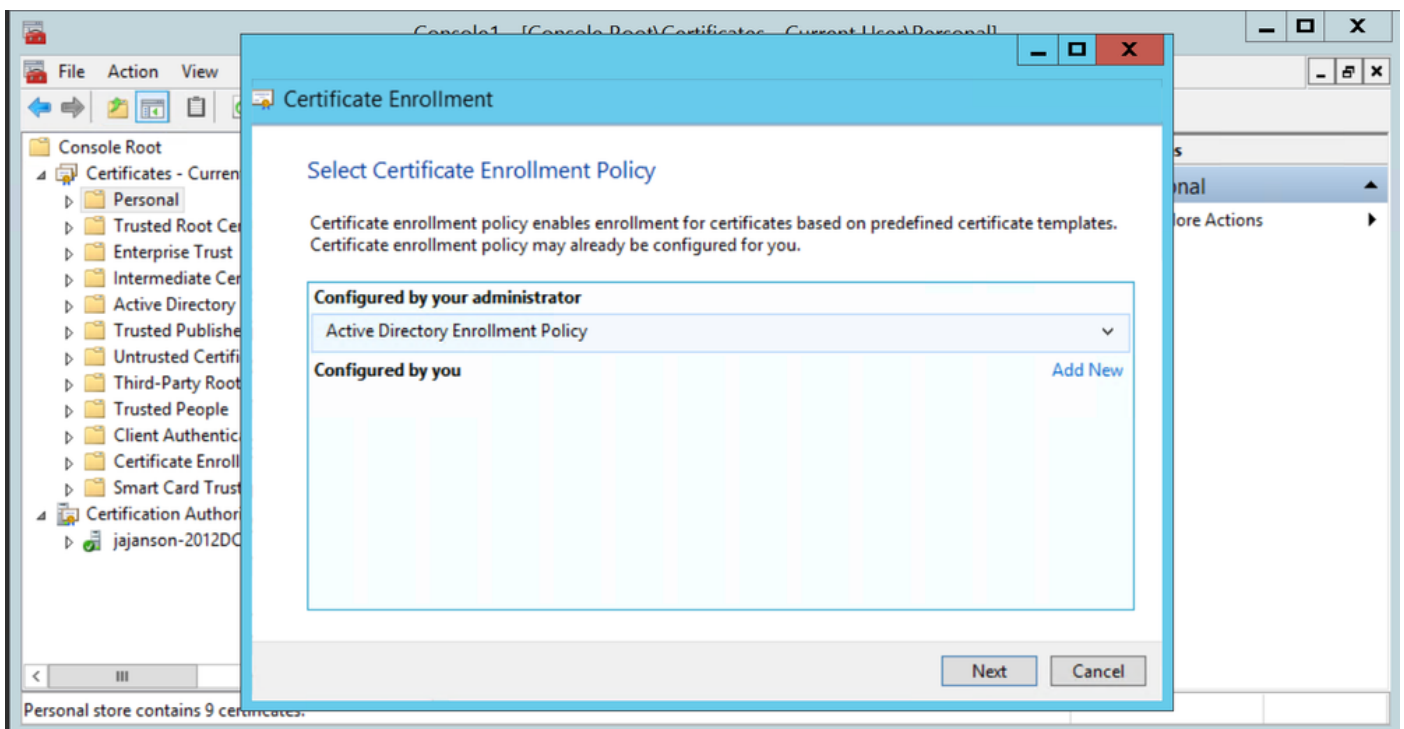
Agregar certificados

2. Haga clic con el botón derecho del ratón o seleccione el **nodo personal**, seleccione **Todas las tareas** y, a continuación, seleccione **Solicitar nuevo certificado**.



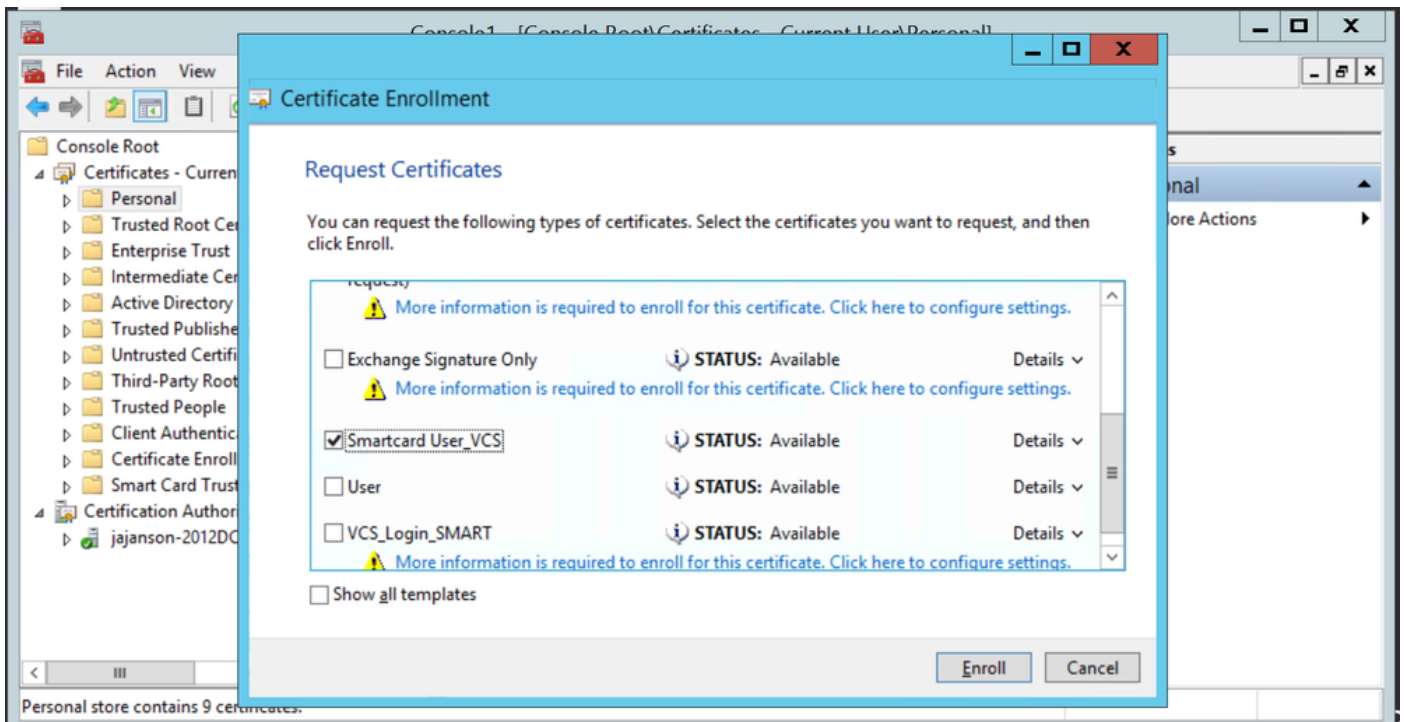
Solicitar nuevos certificados

3. Haga clic en **Next** en el asistente y, a continuación, seleccione **Directiva de inscripción de Active Directory**. A continuación, haga clic en **Siguiente** de nuevo.



Inscripción en Active Directory

4. Seleccione el **Certificado de agente de inscripción**, en este caso, **Smartcard User\_VCS** y, a continuación, haga clic en **Inscribirse**.

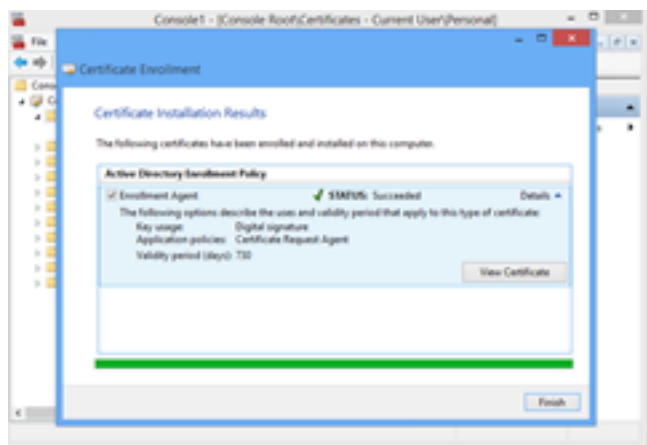


Agente de certificado de inscripción

El escritorio de los administradores de TI se ha configurado como una estación de inscripción, lo que le permite inscribir nuevas tarjetas inteligentes en nombre de otros usuarios.

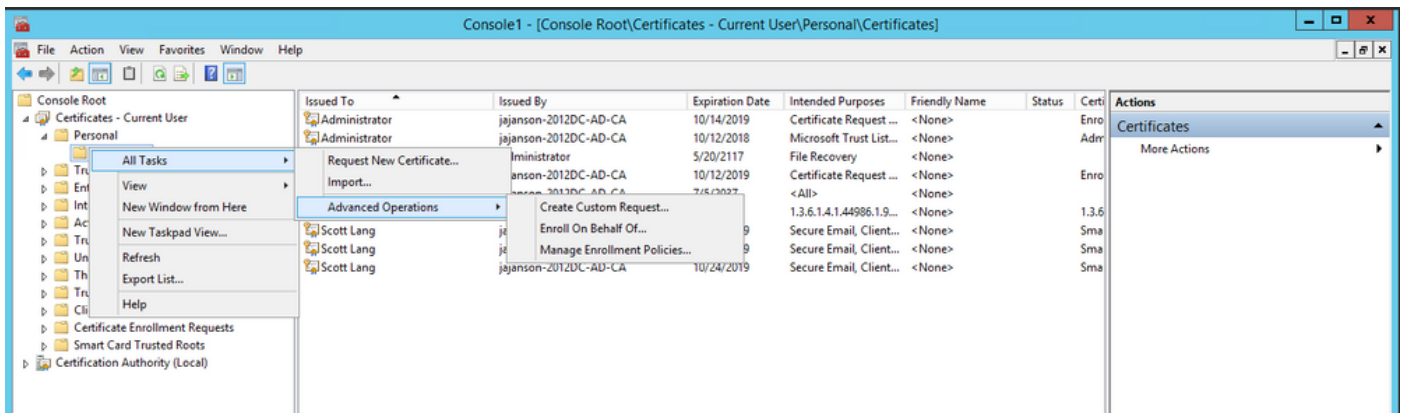
### Inscríbese en nombre de...

Para poder proporcionar a los empleados tarjetas inteligentes para la autenticación, debe inscribirlas y generar el certificado que se importa a la tarjeta inteligente.

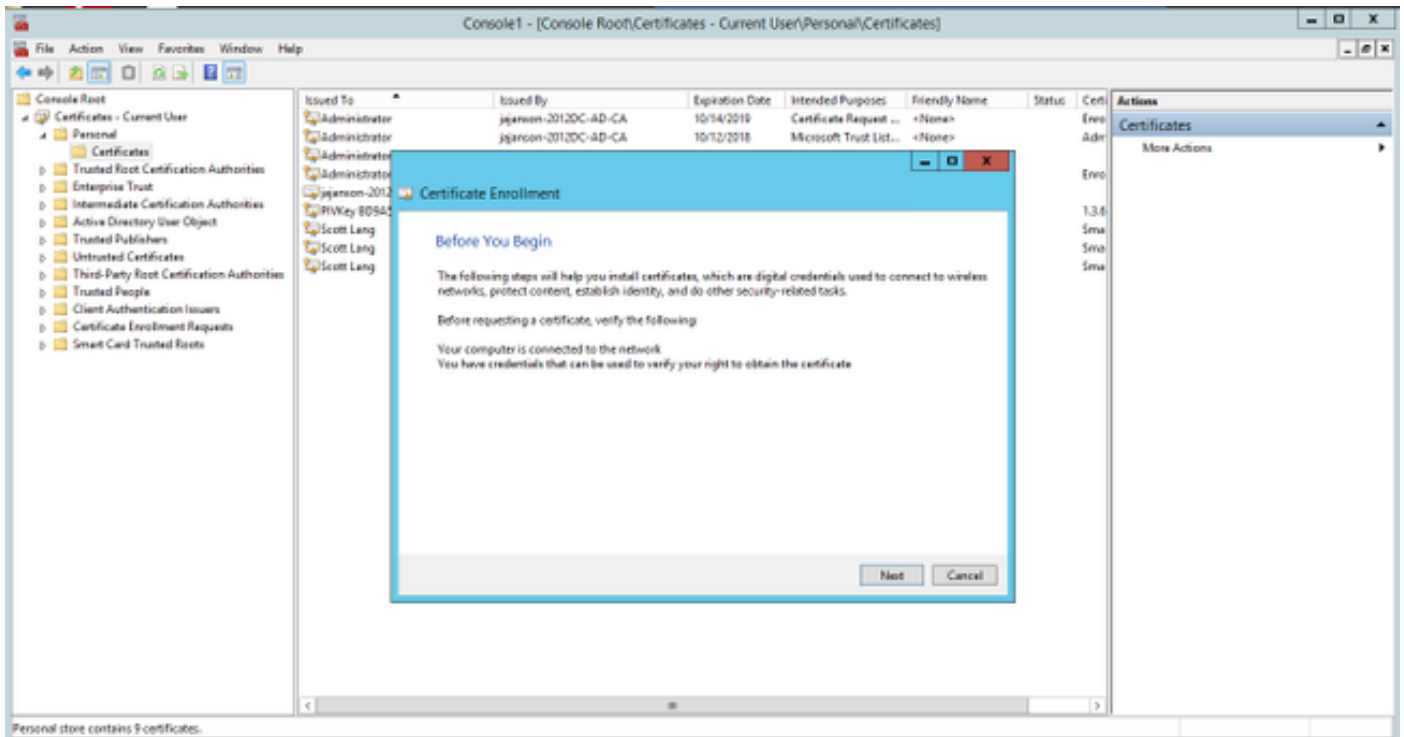


Inscríbese en nombre de

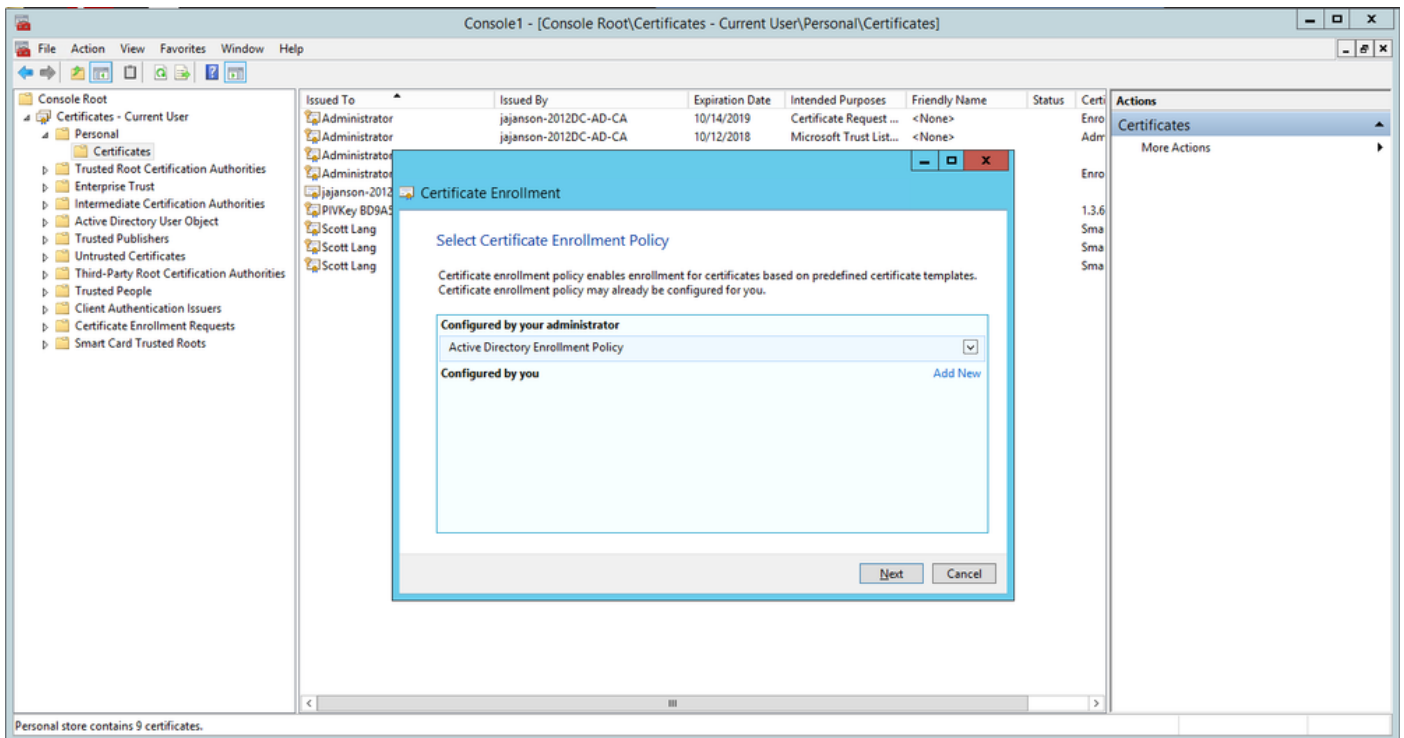
1. Inicie MMC e importe el **Módulo de certificados** y el **Administrador** de certificados para Mi cuenta de usuario.
2. Haga clic con el botón derecho del ratón o seleccione **Personal > Certificados** y seleccione **Todas las tareas > Operaciones avanzadas** y haga clic en **Inscríbese en nombre de...**
3. En el asistente, elija la Política de inscripción de Active Directory y luego haga clic en **Siguiente**.



## Inscríbese en nombre avanzado

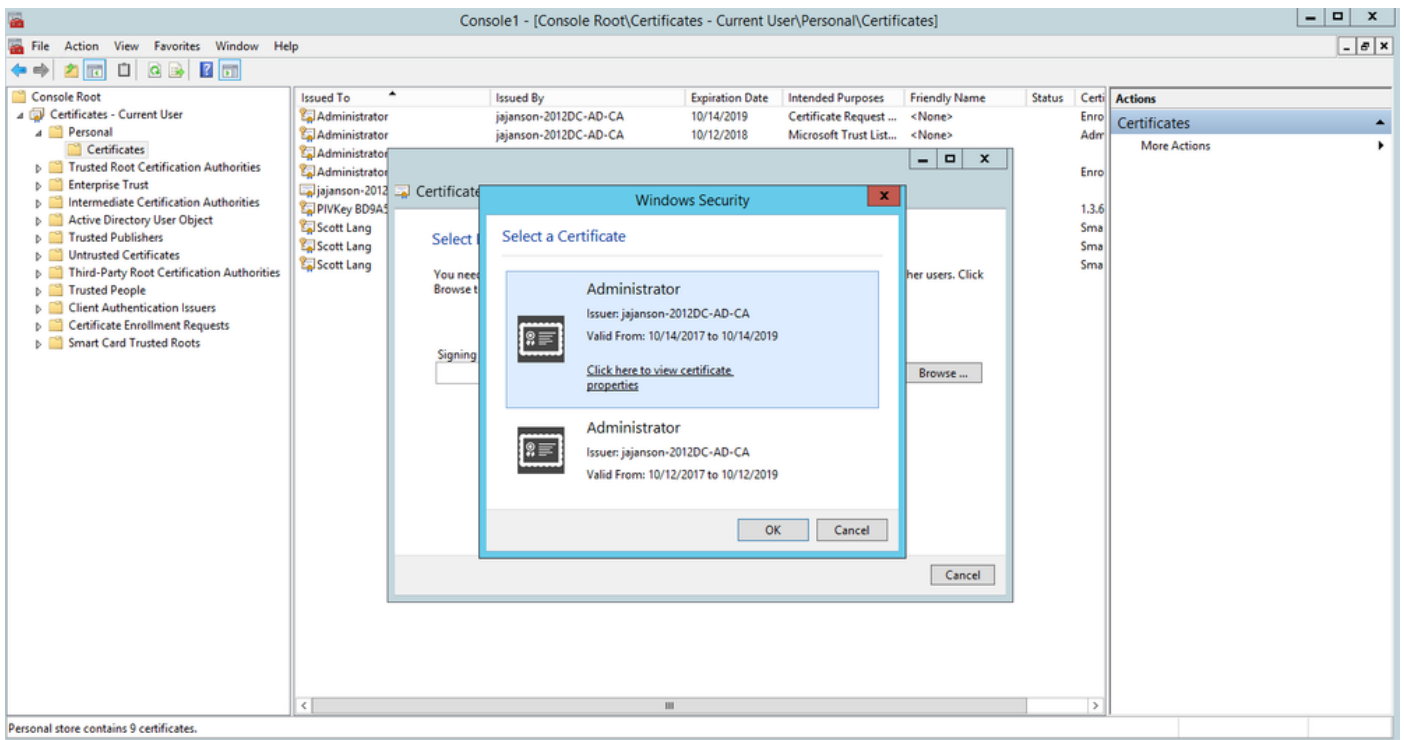


4. Seleccione Certificate Enrollment Policy y luego haga clic en **Next**.



## Política de inscripción

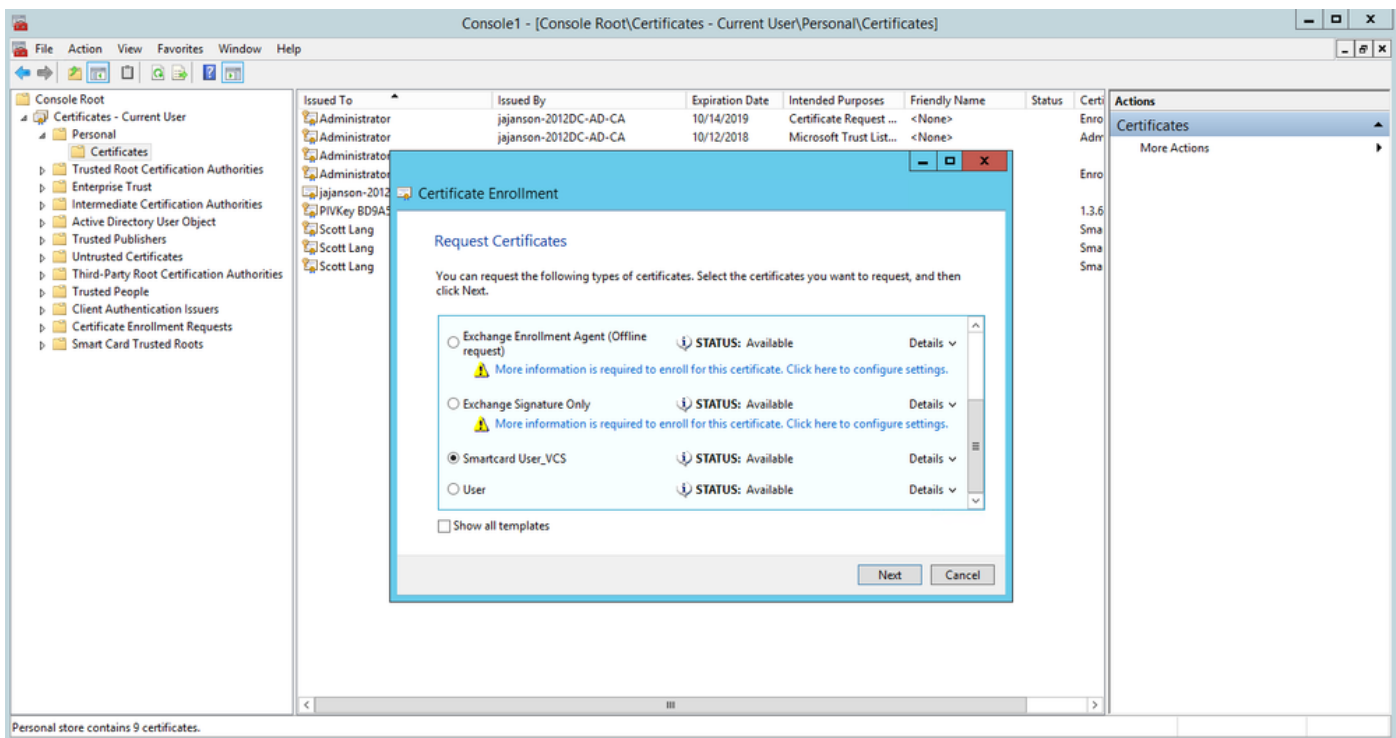
5. Ahora se le solicita que seleccione el **Certificado de firma**. Este es el certificado de inscripción que solicitó anteriormente.



## Seleccionar certificado de firma

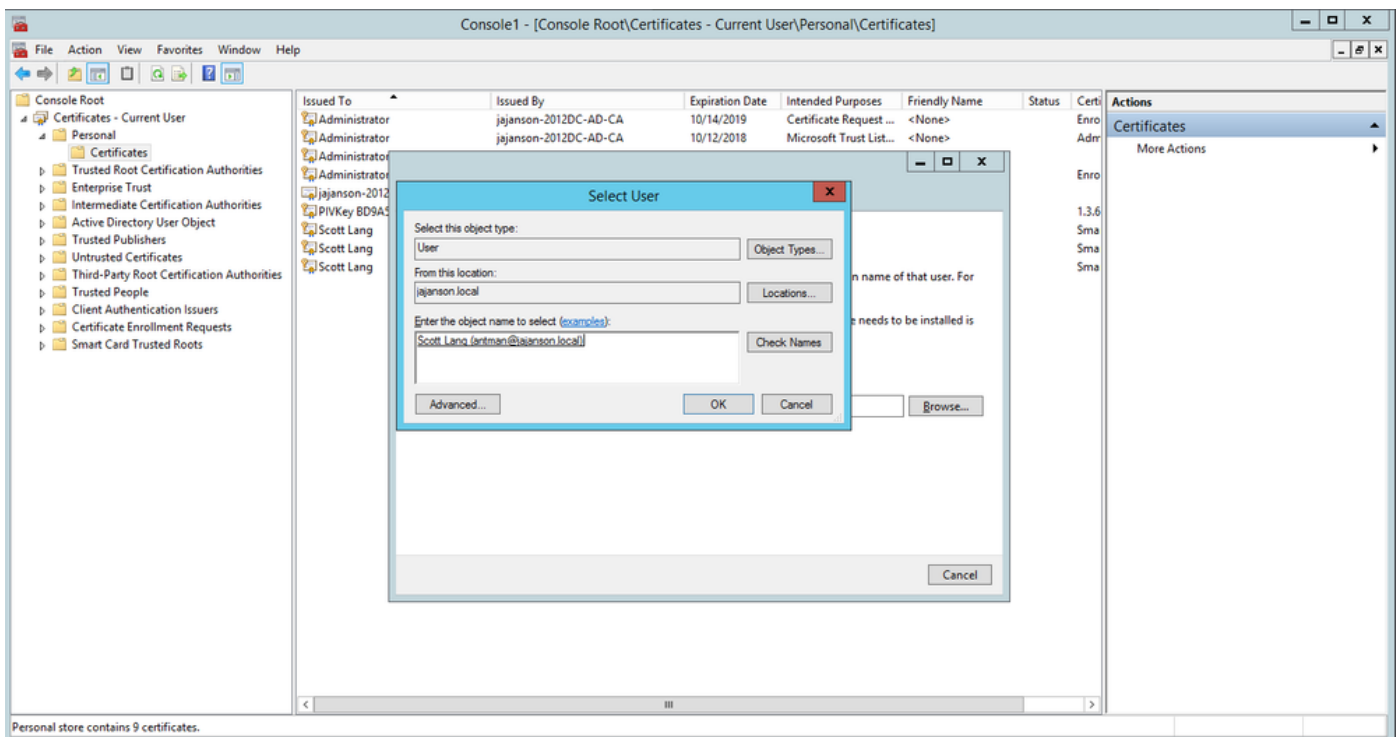
6. En la siguiente pantalla, debe buscar el certificado que desea solicitar y, en este caso, es **Smartcard User\_VCS** la plantilla que creó anteriormente.





Elija la tarjeta inteligente VCS

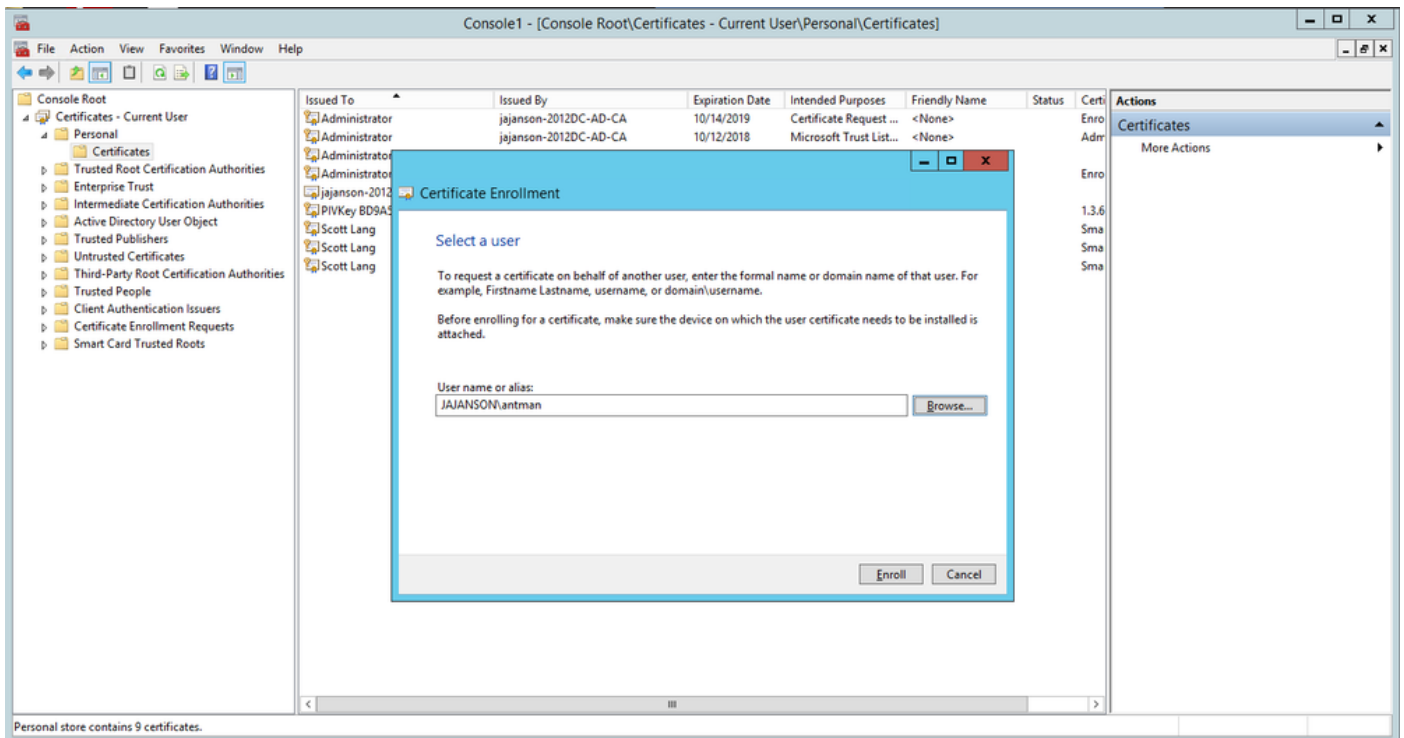
7. A continuación, debe seleccionar el usuario al que desea inscribirse en nombre de. Haga clic en **examinar** y escriba el nombre de usuario del empleado que desea inscribirse. En este caso, se utiliza la 'cuenta antman@jajanson.local' de Scott Lang.



Elija el usuario

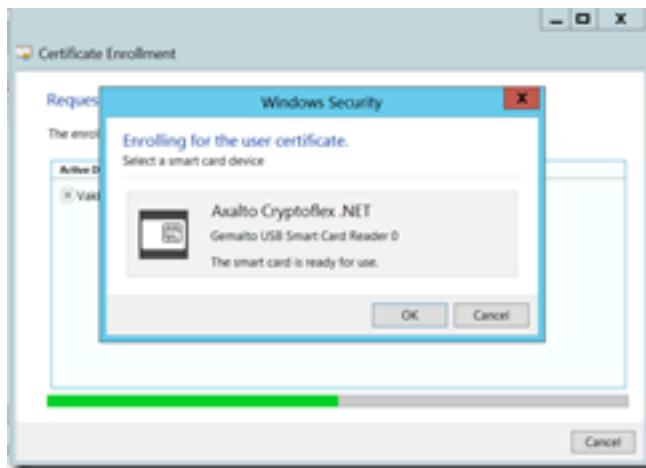
8. En la siguiente pantalla, continúe con la inscripción haciendo clic en **Inscripción**. Ahora, introduzca una tarjeta inteligente en el lector.





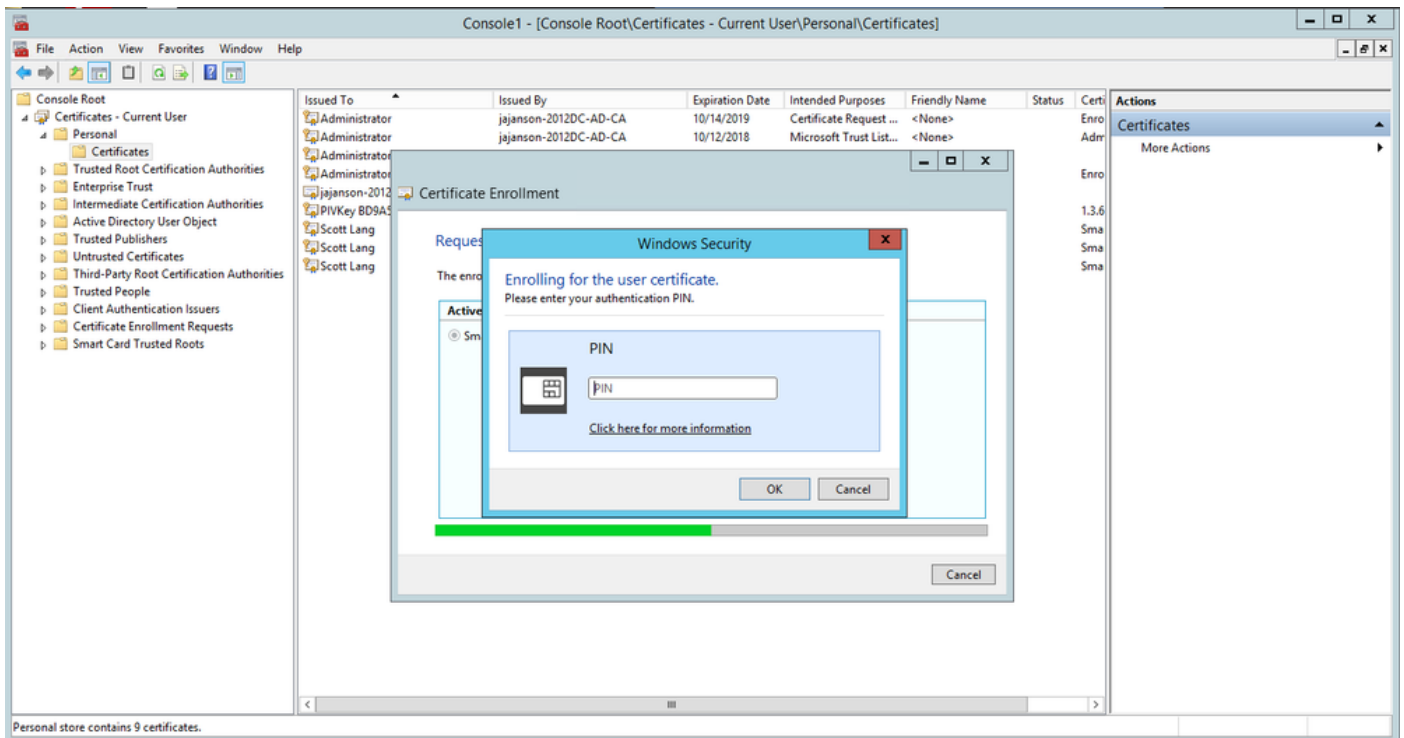
## Inscripción

9. Una vez insertada la tarjeta inteligente, se detecta de la siguiente manera:



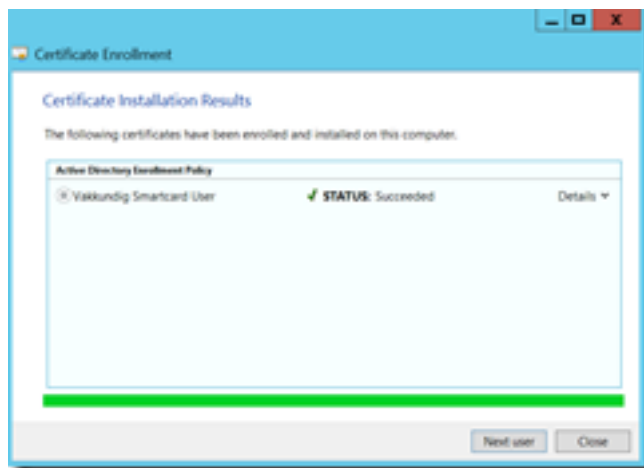
Inserte la tarjeta inteligente

10. A continuación, se le pedirá que escriba un número PIN de tarjeta inteligente (PIN predeterminado: 0000).



Introduzca el pin

11. Por último, una vez que haya visto la pantalla **Inscripción correcta**, puede utilizar esta tarjeta inteligente para iniciar sesión en un servidor unido al dominio, como el VCS con sólo la tarjeta y un pin conocido. Sin embargo, no se hace sí, todavía necesita preparar el VCS para redirigir las solicitudes de autenticación a la tarjeta inteligente y utilizar la tarjeta de acceso común para liberar el certificado de tarjeta inteligente almacenado en la tarjeta inteligente para la autenticación.



Inscripción correcta

### Configuración de VCS para la tarjeta de acceso común

Cargue la CA raíz en la lista de certificados de CA de confianza en el VCS navegando hasta **Mantenimiento > Seguridad > Certificado de CA de confianza**.

2. Cargue la Lista de Revocación de Certificados firmada por la CA raíz en el VCS. Vaya a **Mantenimiento > Seguridad > Gestión CRL**.

3. Pruebe su certificado de cliente con su regex que extrae el nombre de usuario del certificado para usar para la autenticación contra el usuario LDAP o local. El regex va a coincidir con el **Asunto** del certificado. Puede ser su UPN, correo electrónico, etc. En este laboratorio, se utilizó el correo electrónico que debe coincidir con el certificado de cliente para el certificado de cliente.

# 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

Asunto del certificado del cliente

4. Vaya a **Mantenimiento > Seguridad > Prueba de certificado de cliente**. Seleccione el certificado de cliente que se probará, en Mi laboratorio era antman.pem, cárguelo en el área de prueba. En la sección **Patrón de autenticación basada en certificados en Regex** para coincidir con el certificado pegue su regex para ser probado. No cambie el campo **Formato de nombre de usuario**.

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

The screenshot shows the Cisco TelePresence Video Communication Server Expressway configuration page. The page is titled "Client certificate testing" and contains 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, there is a "Browse" button and a "No file selected" message. The "Currently uploaded test file" field shows "antman.pem".

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

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

Pruebe su regex en 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}";@jason.local/
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:
            240000000170f460b3102511a4651370000000000017
        Signature Algorithm: sha1256sha256Encryption
        Issuer: CN=Antman,OU=DOE,OU=CA,OU=jason.local
        Validity
            Not Before: Oct 17 21:39:55 2017 GMT
            Not After: Oct 17 21:39:55 2017 GMT
        Subject: emailAddress=jason.local,CN=Scott.Lino,OU=DOE,OU=jason.local
        Subject Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
            009f-ed08ff-5a12815a1517b46810246b1131d0771
            0c19a1081841374210917516412d0f11391d94c041
            61651d01f81761081c16412418f100181f81451
            681fc1081081f817a1311271081410811711d11f1f91
            95132191f81310c10010f10a15c14213413610f1
            a8144112171881801841801981f21f71413619c1911
            d4105161816716110f1601021081001801711a1
            c413217f14813614210419c13c16a1851f816718912b1
    
```

← 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.


## Resultados de pruebas


- Si la prueba le proporciona los resultados deseados, puede hacer clic en el botón **Hacer que estos cambios sean permanentes**. Esto cambia su regex para la configuración de autenticación basada en certificados del servidor. Para verificar el cambio, navegue hasta esa configuración, **Mantenimiento > Seguridad > configuración de autenticación basada en certificados**.
- Habilite la autenticación basada en cliente navegando a **System > Administrator** y luego haga clic o seleccione el cuadro desplegable para elegir **Client certificate-based security = Client-Based Authentication**. Con esta configuración, el usuario escribe el FQDN del servidor VCS en su navegador y se le solicita que elija su cuenta cliente e introduzca el pin asignado a su tarjeta de acceso común. A continuación, se libera el certificado y se le devuelve la GUI web del servidor VCS y todo lo que necesita hacer es hacer clic o seleccionar el botón Administrador. Luego es admitido en el servidor. Si se selecciona la opción **Seguridad basada en certificados de cliente = Validación basada en cliente**, el proceso es el mismo con la excepción cuando el usuario hace clic en el botón Administrador, se le ha solicitado nuevamente la contraseña de administrador. Por lo general, esto último no es lo que la organización intenta lograr con 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](#)

Habilitar autenticación basada en cliente

¡Ayuda! ¡¡¡Estoy bloqueado!!!

Si habilita la autenticación basada en el cliente y VCS rechaza el certificado por cualquier motivo, ya no podrá iniciar sesión con la GUI web de la manera tradicional. Pero, no se preocupe, hay una forma de volver a su sistema. El documento adjunto se puede encontrar en el sitio web de Cisco y proporciona información sobre cómo inhabilitar la autenticación basada en cliente del acceso raíz.

## Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

## Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.