

Configure o VCS com CAC e um leitor de Smart Card

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[O que é um Smart Card?](#)

[Configurar](#)

[Verificar](#)

[Troubleshoot](#)

Introduction

Este documento descreve um guia passo a passo para instalar e usar um leitor de Smart Card e um cartão de acesso comum para uso com o Cisco Video Communication Server (VCS) para organizações que exigem autenticação de dois fatores para o ambiente VCS, como bancos, hospitais ou governos com instalações seguras.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O CAC fornece a autenticação necessária para que os "sistemas" saibam quem ganhou acesso ao seu ambiente e que parte da infraestrutura é física ou eletrônica. Nos ambientes classificados pelo governo e em outras redes seguras, prevalecem as regras do "acesso menos privilegiado" ou da "necessidade de saber". Um login pode ser usado por qualquer pessoa, a autenticação requer algo que o usuário tem, depois de remover o CAC, também conhecido como Cartão de Acesso Comum, lançado em 2006 para que o indivíduo não precise ter vários dispositivos, sejam eles fobs, cartões de identificação ou dongles para acessar seu local de trabalho ou sistemas.

O que é um Smart Card?

Os cartões inteligentes são um componente chave da infraestrutura de chave pública (PKI) que a Microsoft usa para integrar à plataforma Windows porque os cartões inteligentes aprimoram soluções somente de software, como autenticação de cliente, login e e-mail seguro. Os cartões inteligentes são um ponto de convergência para certificados de chave pública e chaves associadas porque:

- Fornece armazenamento resistente a adulterações para proteção de chaves privadas e outras formas de informações pessoais.
- Isole as computações críticas de segurança, que envolvem autenticação, assinaturas digitais e troca de chaves de outras partes do sistema que não precisam saber.
- Habilitar a portabilidade de credenciais e outras informações privadas entre computadores no trabalho, em casa ou em trânsito.

O cartão inteligente tornou-se parte integrante da plataforma Windows porque os cartões inteligentes fornecem recursos novos e desejáveis, tão revolucionários para a indústria de computadores como a introdução do mouse ou CD-ROM. Se você não tem uma infraestrutura interna de PKI no momento, é preciso garantir que faça isso primeiro. Este documento não aborda a instalação desta função neste artigo específico, mas informações sobre como implementá-la podem ser encontradas aqui: <http://technet.microsoft.com/en-us/library/hh831740.aspx>.

Configurar

Este laboratório pressupõe que você já tenha um LDAP integrado com VCS e que tenha usuários que possam fazer login com credenciais LDAP.

1. [Equipamento de laboratório](#)
2. [Instale o Smart Card](#)
3. [Configurar modelos de autoridade de certificado](#)
4. [Inscreva o certificado do agente de inscrição](#)
5. [Inscrever-se em nome de...](#)
6. [Configure o VCS para a placa de acesso comum](#)

Equipamento necessário:

Servidor de Domínio do Windows 2012R2 que tem estas funções/software instalado:

- Autoridade de certificação
- Ative Directory
- DNS
- PC Windows com Smart Card conectado
- vSEC: Software de gerenciamento CMS K-Series para gerenciar seu Smart Card:



Software Versa Card Reader

Instale o Smart Card

Os leitores de Smart Card geralmente recebem instruções sobre como conectar os cabos necessários. Aqui está um exemplo de instalação para esta configuração.

Como instalar um driver de dispositivo do leitor de Smart Card

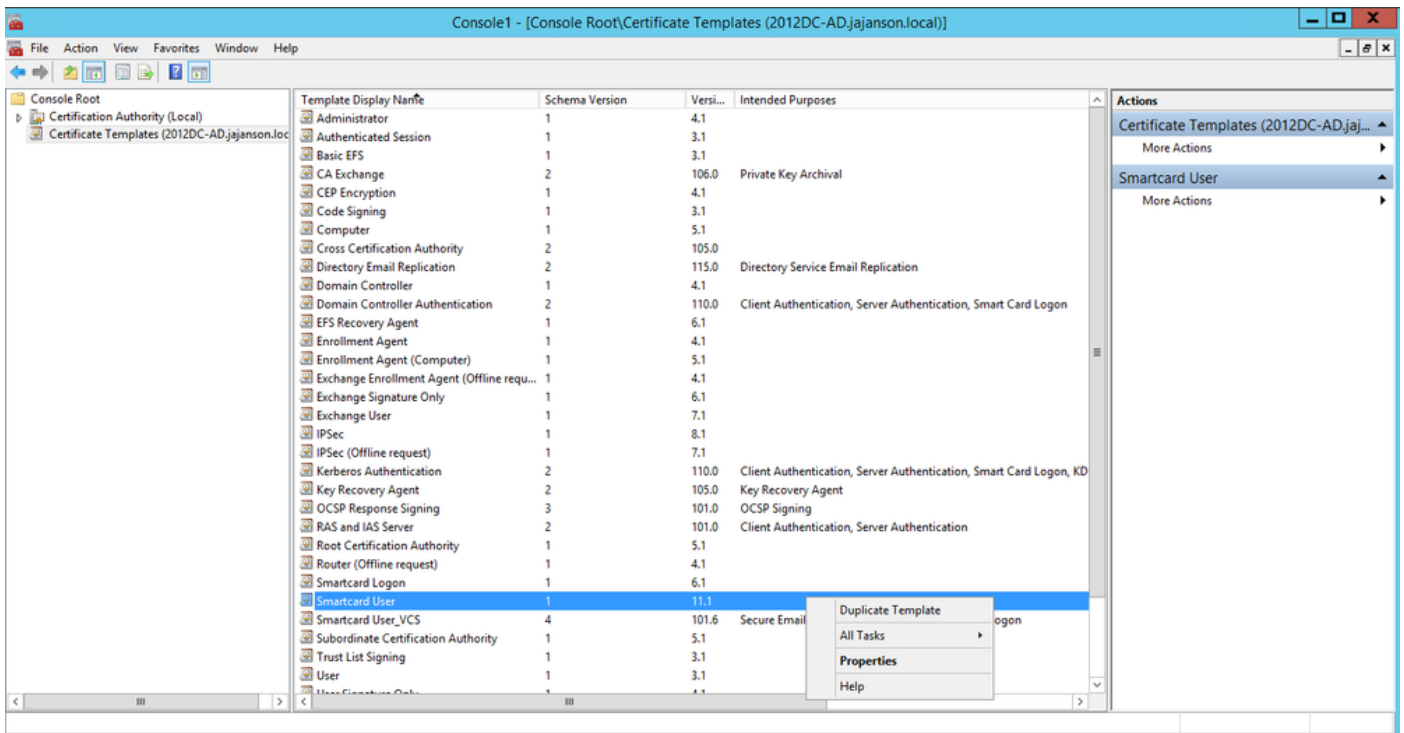
Se o leitor de cartão inteligente tiver sido detectado e instalado, a tela Bem-vindo ao login do Windows confirmará isso. Caso contrário:

1. Conecte seu Smart Card à porta USB no PC Windows
2. Siga as instruções na tela para instalar o software do driver do dispositivo. Isso exige a mídia do driver que o fabricante do smart card ou do driver foi descoberto no Windows. No meu caso, usei o driver de fabricação do site de download. **NÃO CONFIE EM JANELAS.**
3. Clique com o botão direito do mouse no ícone **Meu computador** na área de trabalho e clique em **Gerenciar** no submenu.
4. Expanda o nó **Serviços e aplicativos** e clique em **Serviços**.

5. No painel direito, clique com o botão direito do mouse em **Smart Card**. Clique em **Propriedades** no submenu.
6. Na guia **Geral**, selecione **Automático** na lista suspensa **Tipo de inicialização**. Click **OK**.
7. Reinicie a máquina se o Assistente de hardware instruir você a fazê-lo.

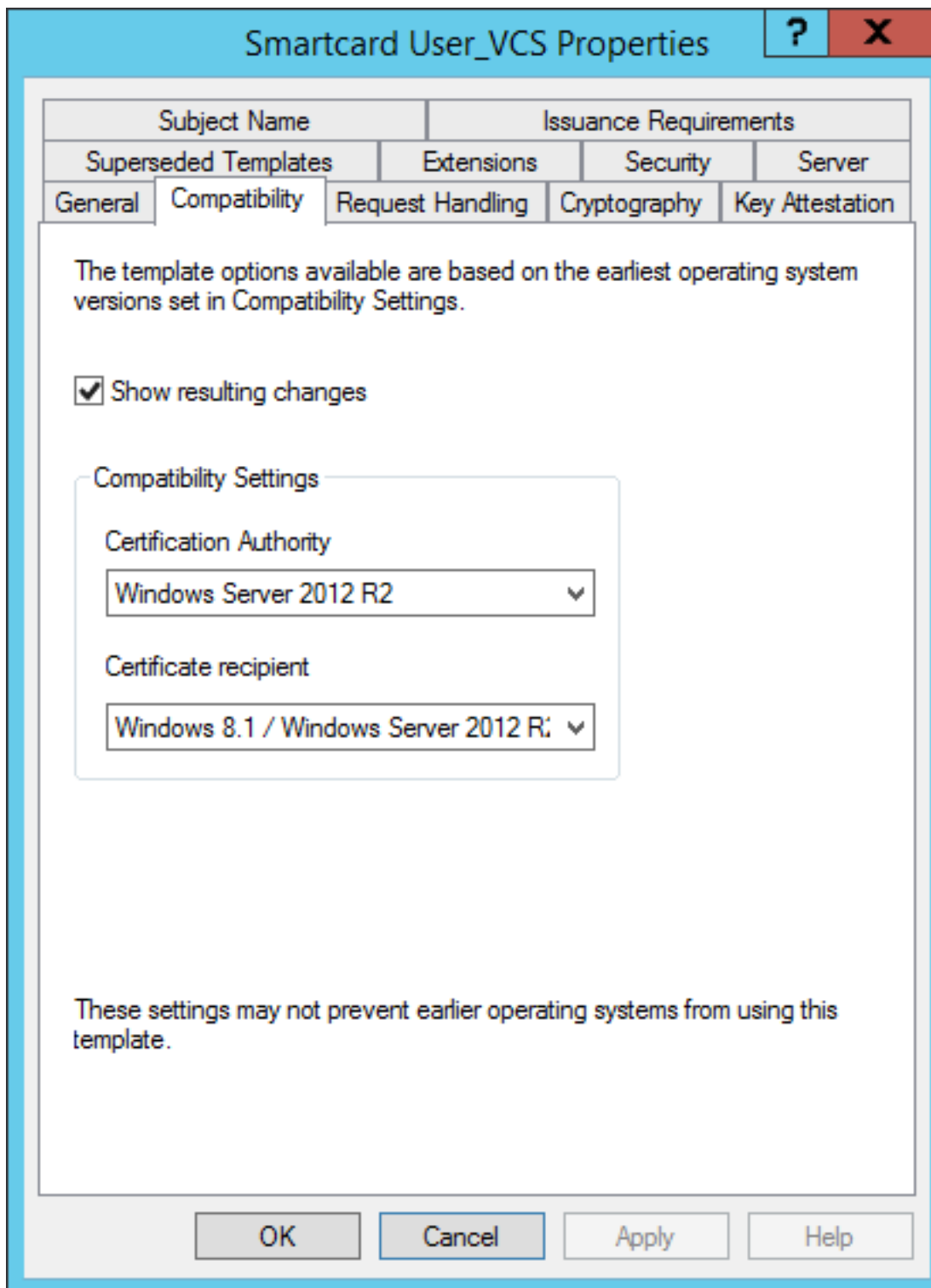
Configurar modelos de autoridade de certificado

1. Inicie a Autoridade de Certificação MMC a partir de Ferramentas Administrativas.
2. Clique ou selecione o nó **Modelos de certificado** e selecione **Gerenciar**.
3. Clique com o botão direito do mouse ou selecione **Smartcard User Certificate Template** e selecione **Duplicate** conforme mostrado na imagem.



Modelos de certificado do controlador de domínio

4. Na guia **Compatibilidade**, em **Autoridade de certificação**, revise a seleção e altere-a, se necessário.



Configurações de

compatibilidade de Smart Card

5. Na guia **Geral**:

a. Especifique um nome, como **Smartcard User_VCS**.

b. Defina o período de validade para o valor desejado. Clique em **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

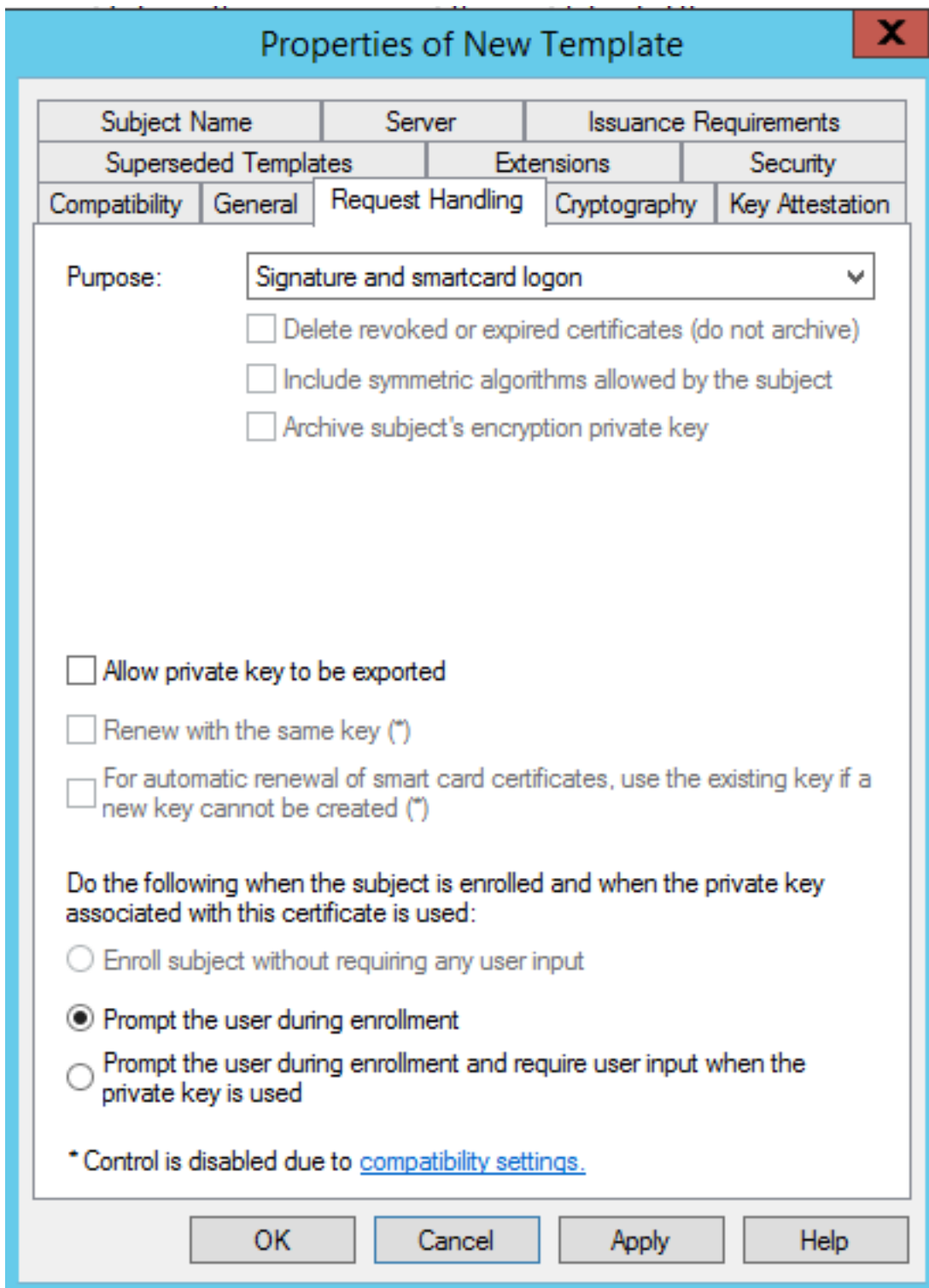
Tempo geral do

cartão inteligente vencimento

6. Na guia **Solicitar tratamento**:

a. Defina a **Finalidade** como **Login de assinatura e cartão inteligente**.

b. Clique em **Solicitar ao usuário durante a inscrição**. Clique em **Apply**.



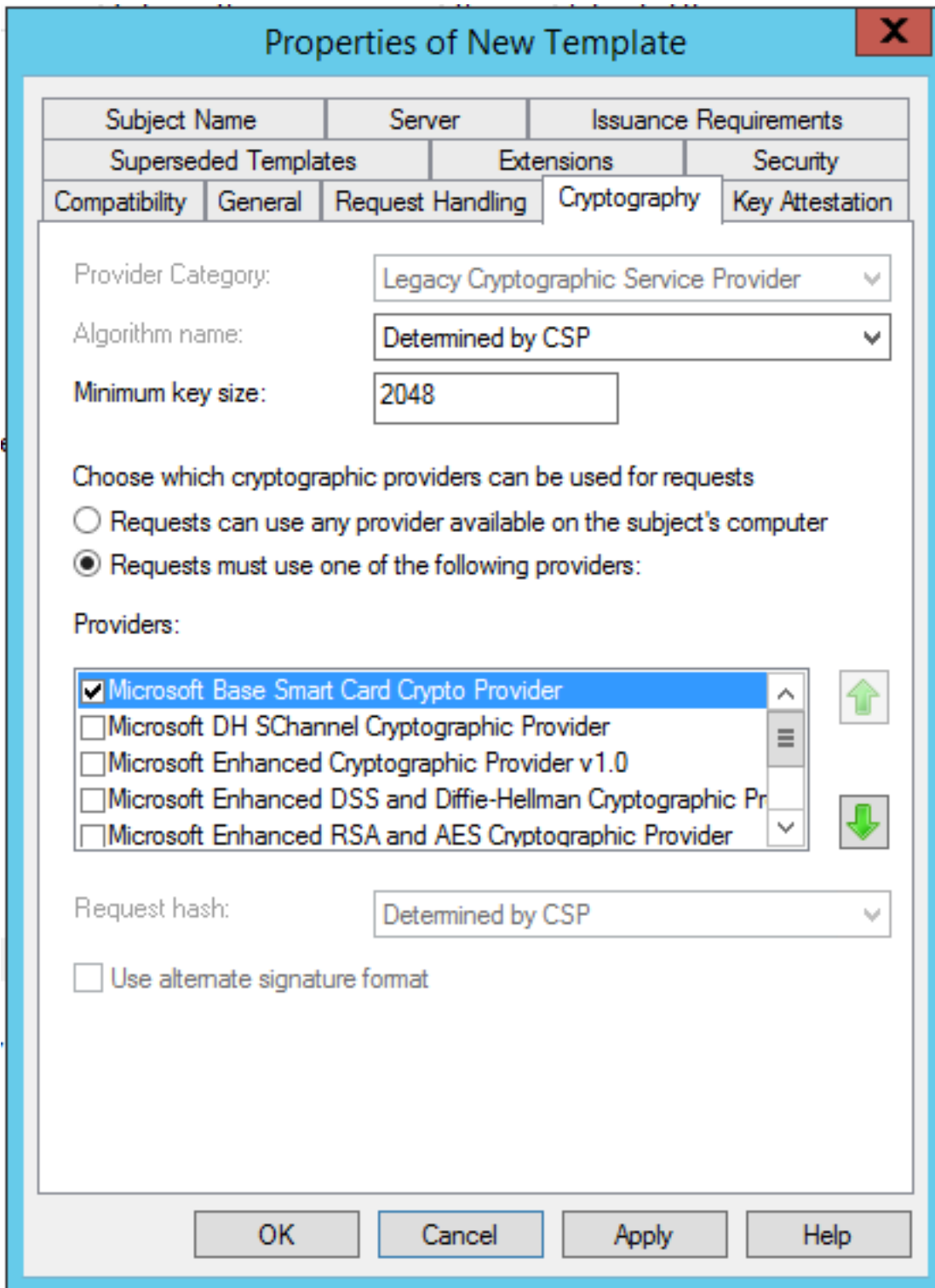
Tratamento de

Solicitações de Cartão Inteligente

7. Na guia **Cryptography**, defina o tamanho mínimo da chave como 2048.

a. Clique em **Requests must use a um dos seguintes provedores** e selecione **Microsoft Base Smart Card Crypto Provider**.

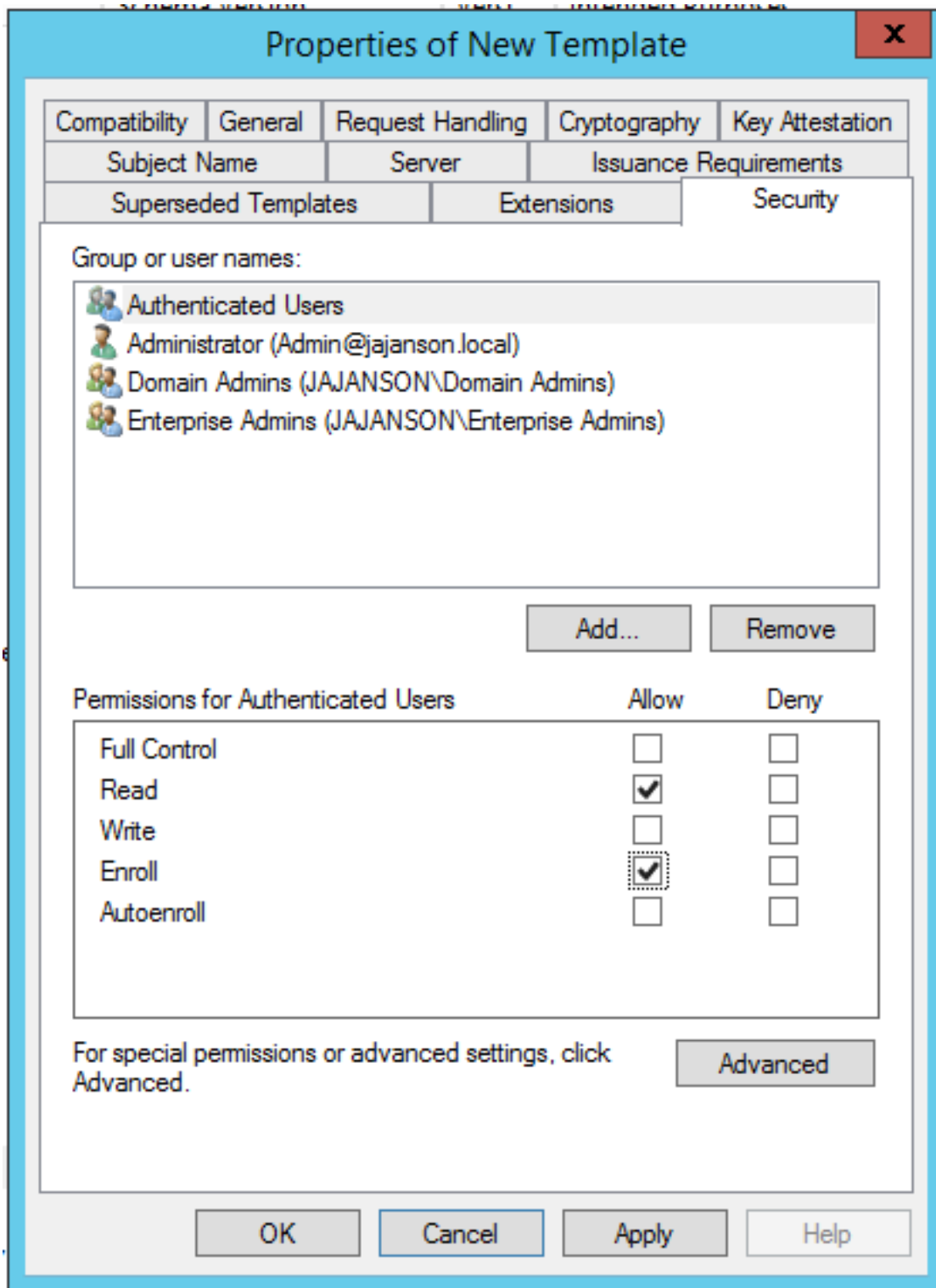
b. Clique em **Apply**.



Configurações de

criptografia de certificado

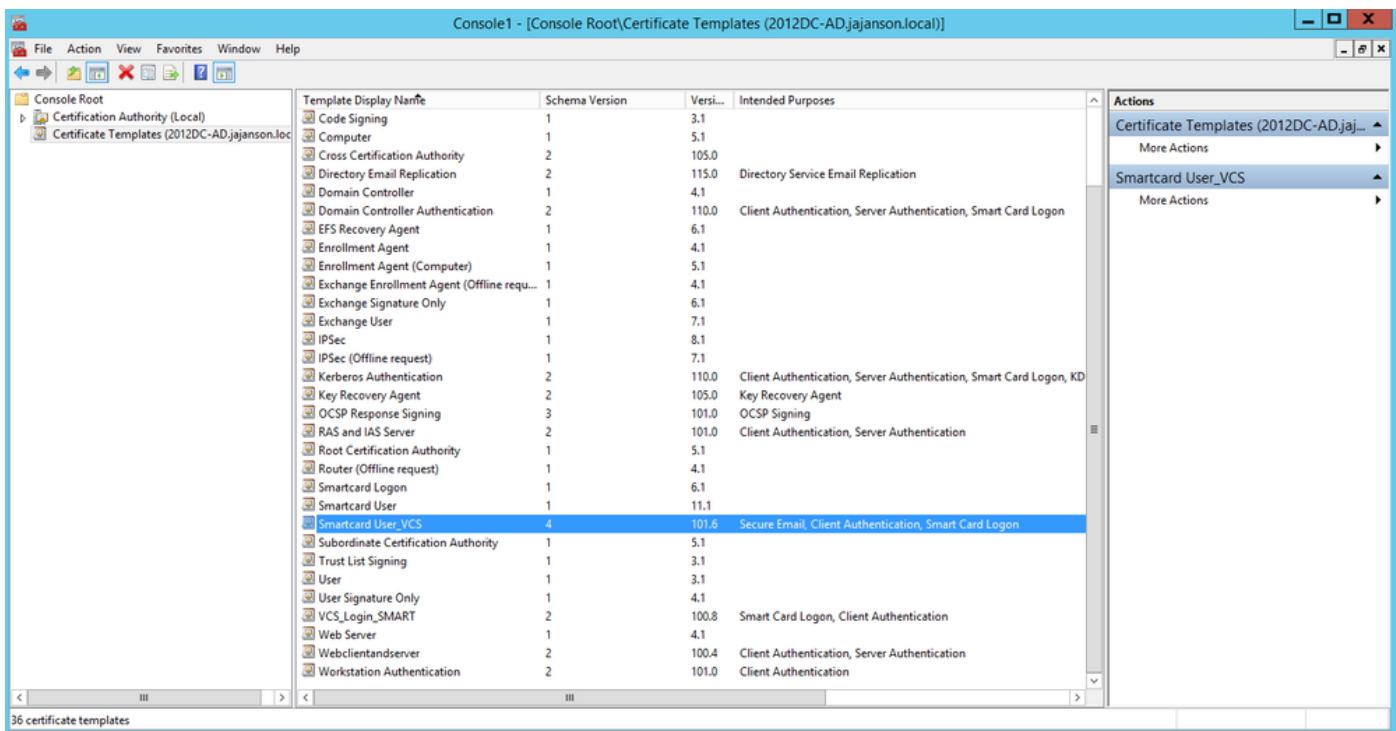
8. Na guia Segurança, adicione o grupo de segurança ao qual deseja conceder acesso de Inscrição. Por exemplo, se quiser conceder acesso a todos os usuários, selecione o grupo de usuários autenticados e selecione **Inscrever** permissões para eles.



Segurança de

modelo

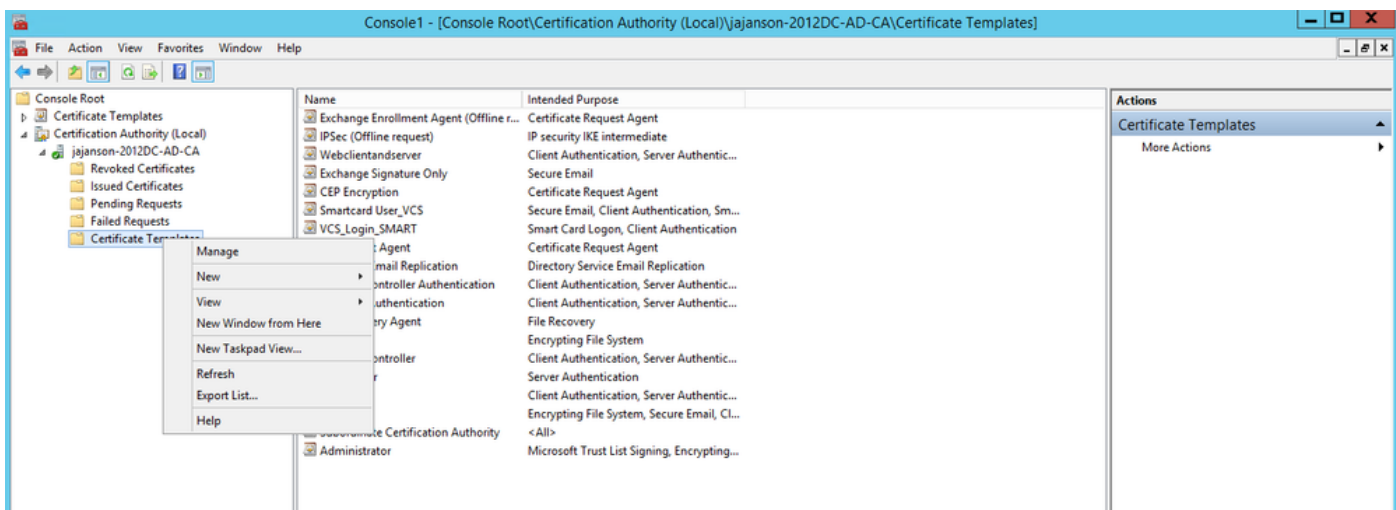
9. Clique em **OK** para finalizar suas alterações e criar o novo modelo. O novo modelo deve aparecer agora na lista de Modelos de certificado.



Modelo visto no controle de domínio

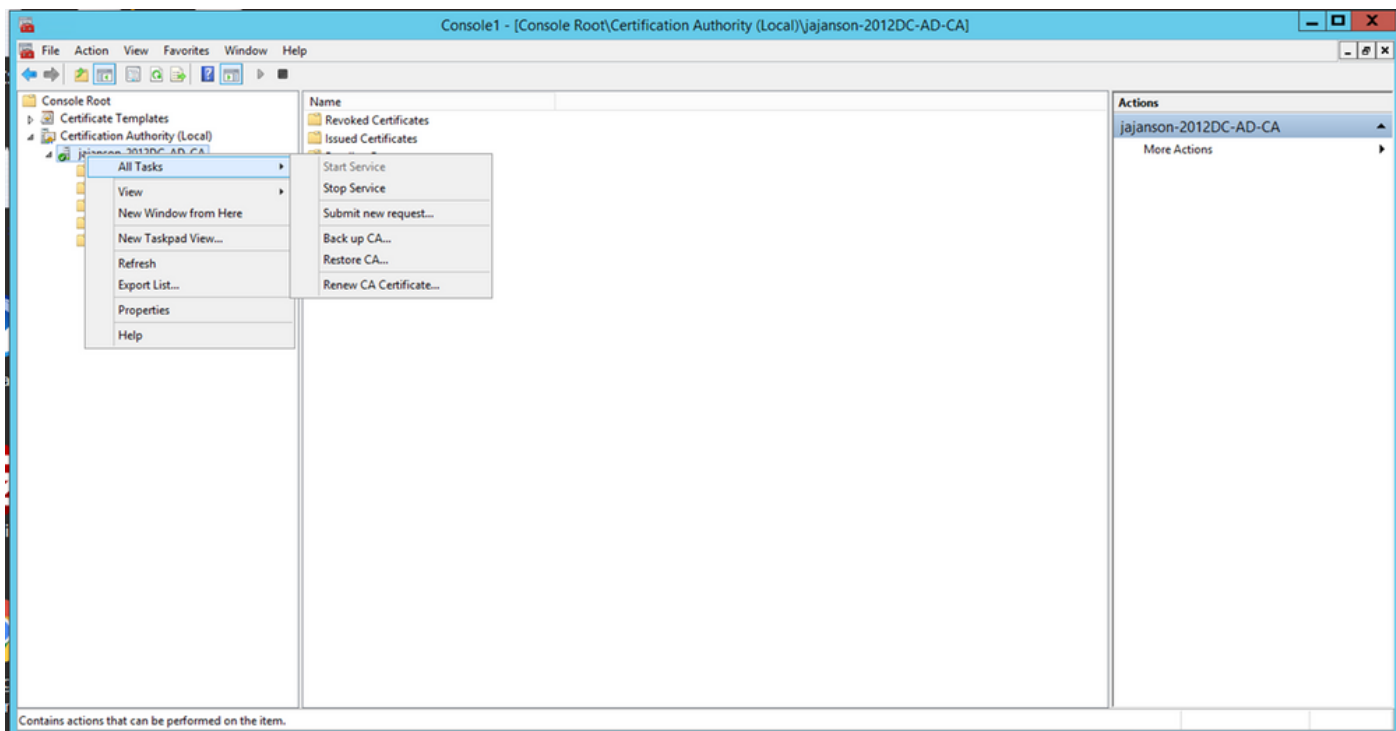
10. No painel esquerdo do MMC, expanda Certification Authority (Local) e expanda sua CA na lista da Certification Authority.

Clique com o botão direito do mouse em Modelos de certificado, clique em **Novo** e em **Modelo de certificado** para problemas. Em seguida, escolha o modelo de Smartcard recém-criado.



Emitir novo modelo

11. Depois que o modelo for replicado, no MMC, clique com o botão direito do mouse ou selecione a lista Autoridade de certificação, clique em **Todas as tarefas** e, em seguida, clique em **Parar serviço**. Em seguida, clique com o botão direito do mouse no nome da AC novamente, clique em **Todas as tarefas** e, em seguida, clique em **Iniciar serviço**.

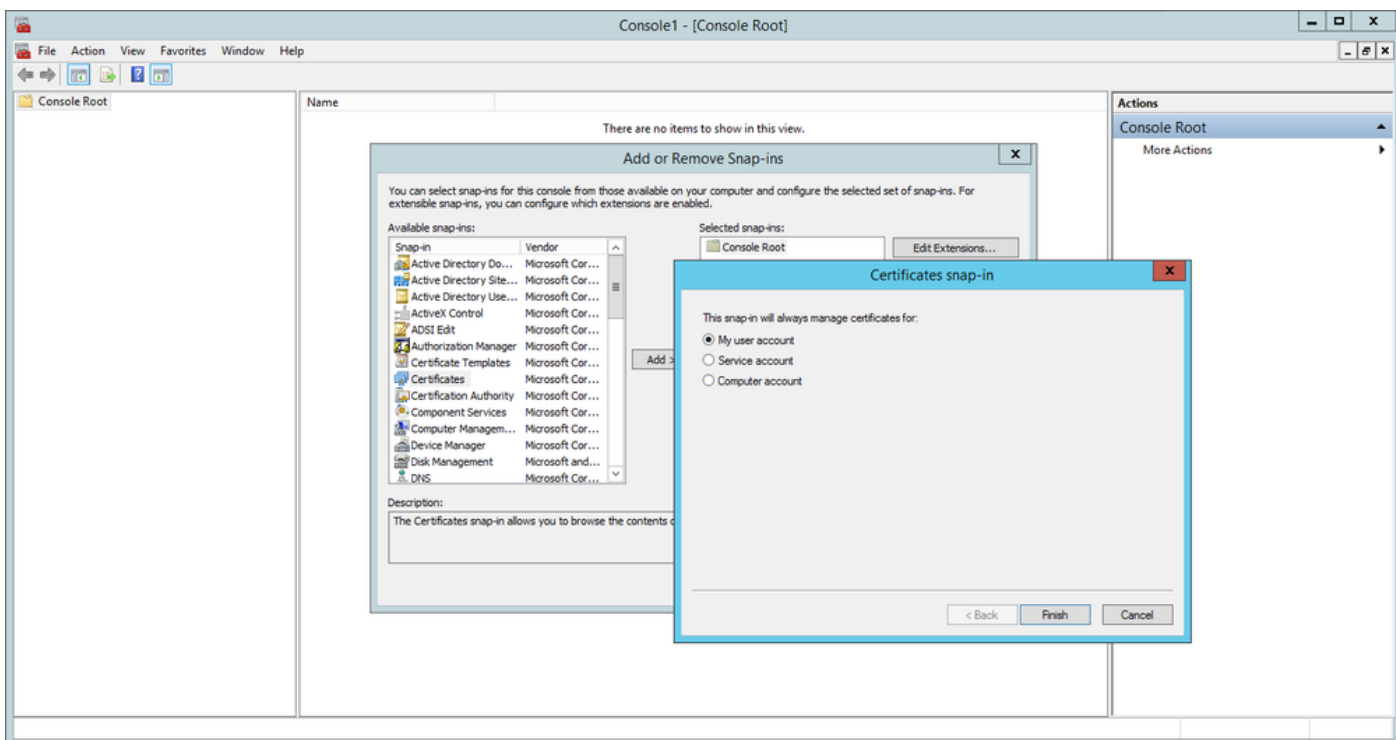


Parar e iniciar serviços de certificado

Inscreeva-se no certificado do agente de inscrição

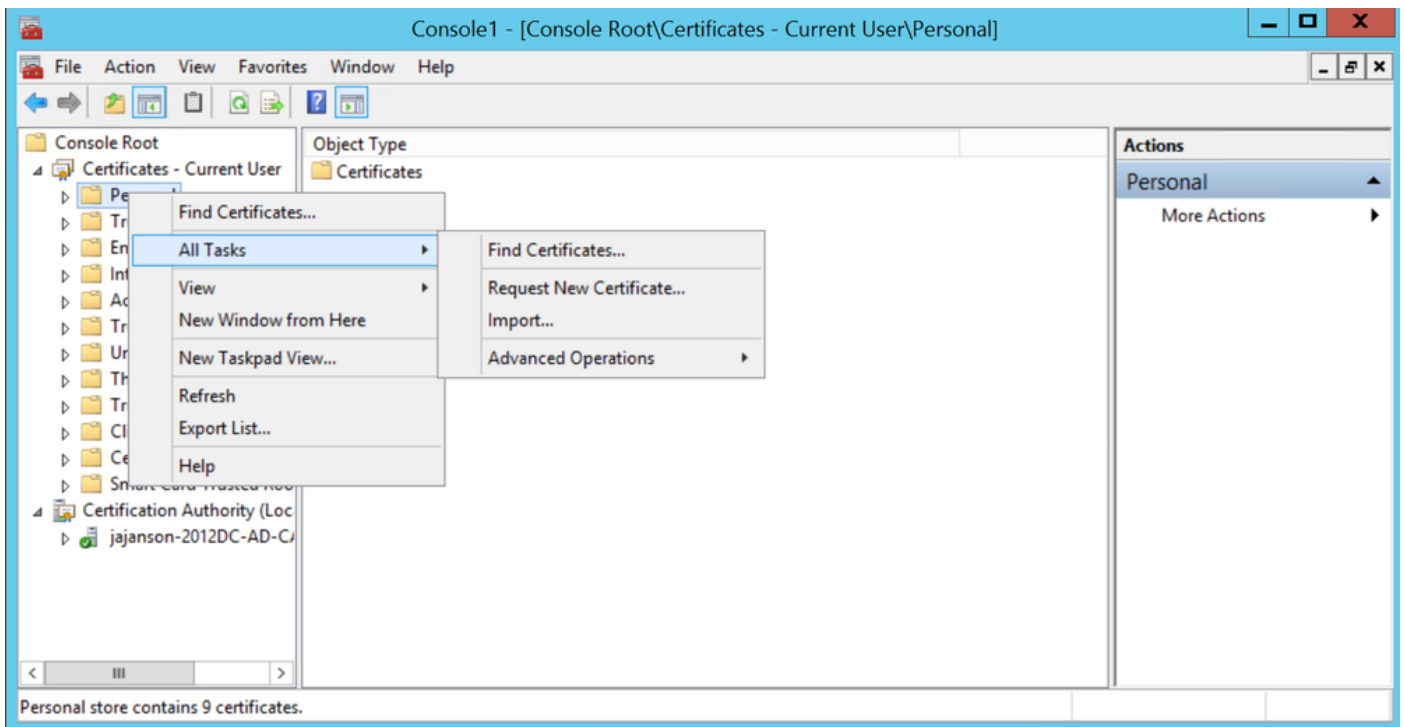
É recomendável que você faça isso em uma máquina cliente (área de trabalho dos administradores de TI).

1. Inicie o MMC escolha **Certificados**, clique em **Adicionar** e depois em **Certificados** para a **Minha Conta de Usuário**.



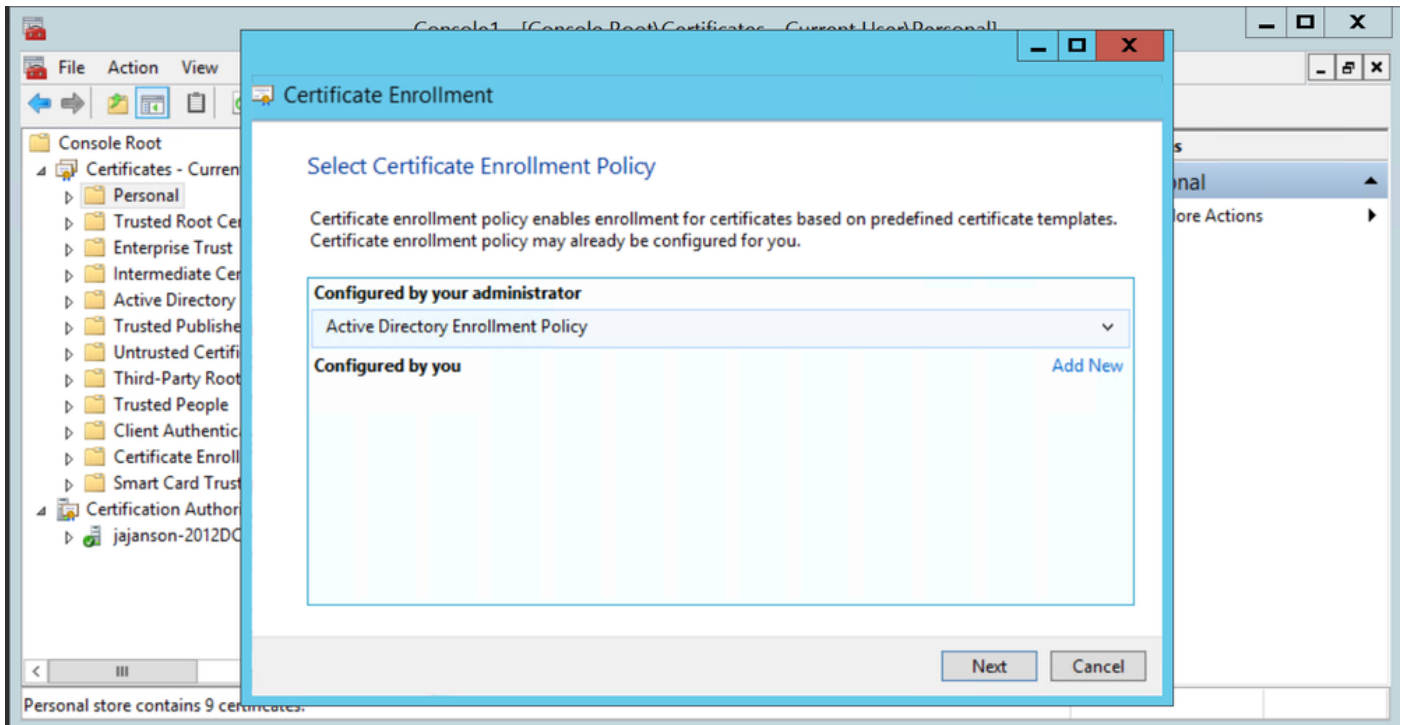
Adicionar certificados

2. Clique com o botão direito do mouse ou selecione o **Nó pessoal**, selecione **Todas as tarefas** e selecione **Solicitar novo certificado**.



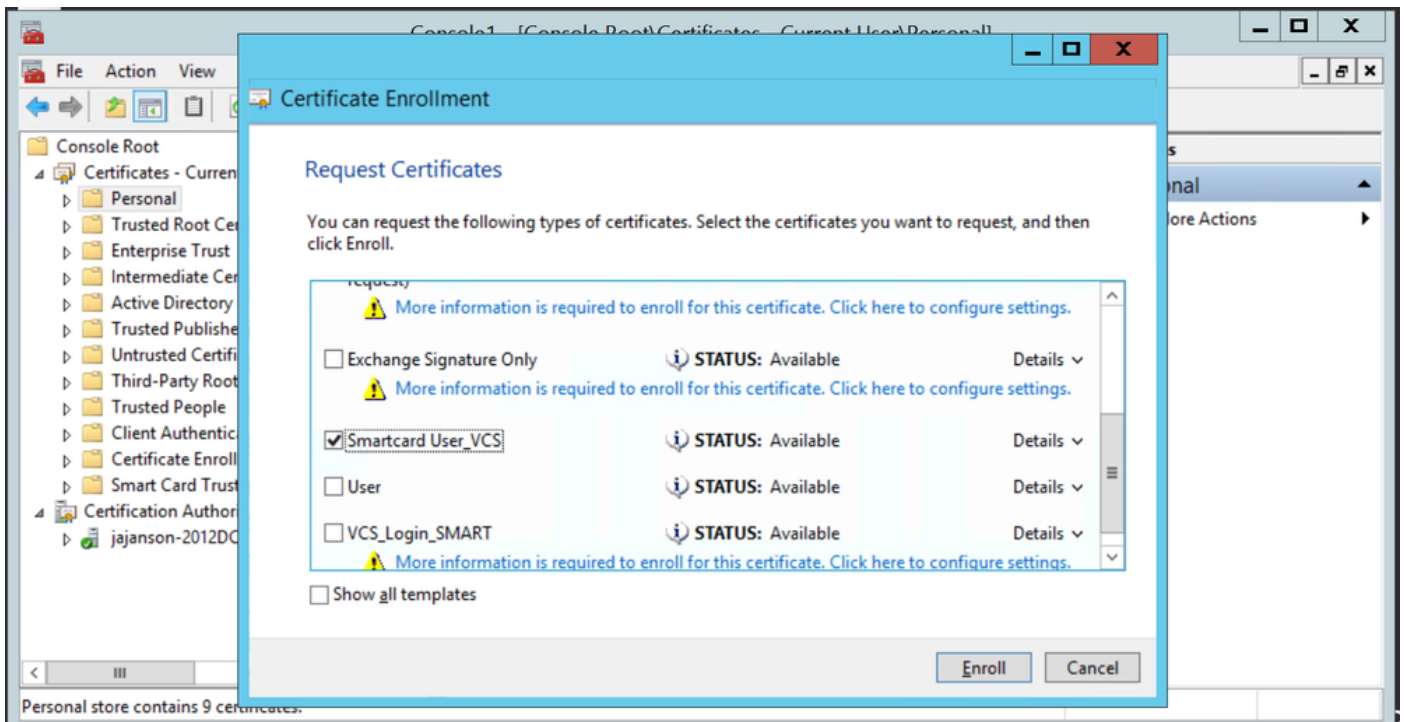
Solicitar novos certificados

3. Clique em **Next** no assistente e selecione **Active Directory Enrollment Policy**. Em seguida, clique em **Avançar** novamente.



Inscrição no Active Directory

4. Selecione o **Certificado do agente de inscrição**, nesse caso, **Smartcard User_VCS** e clique em **Inscriver-se**.

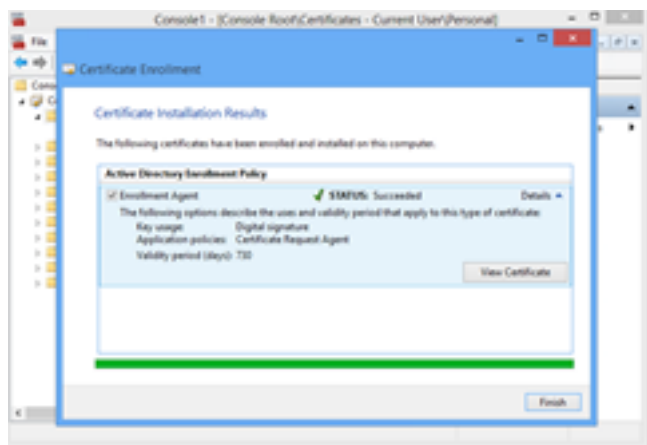


Agente de certificado de inscrição

A área de trabalho dos Administradores de TI agora está configurada como uma Estação de Inscrição, permitindo que você inscreva novos smartcards em nome de outros usuários.

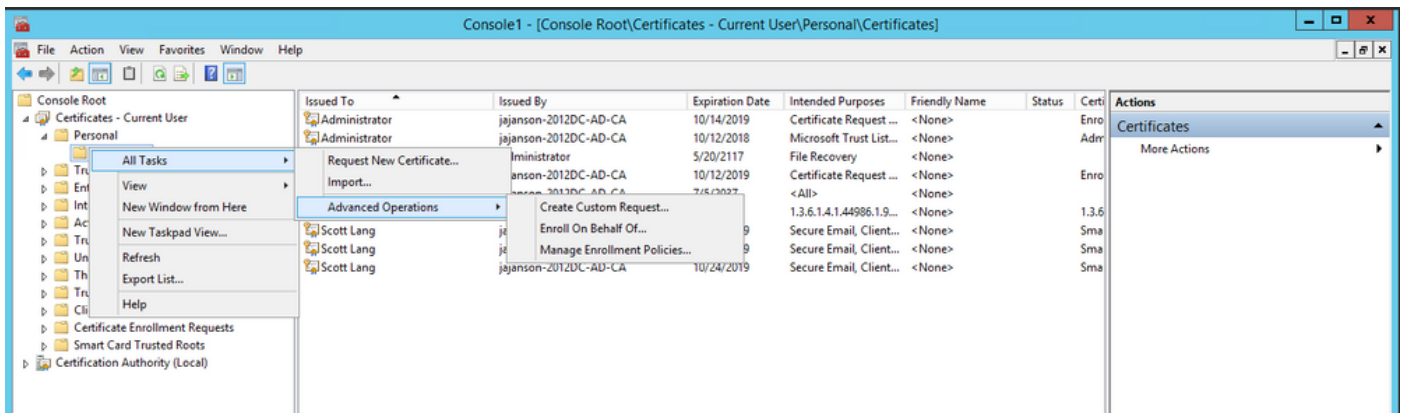
Inscriver-se em nome de...

Para que agora você forneça aos funcionários smartcards para autenticação, você precisa inscrevê-los e gerar o certificado que é importado para o Smartcard.

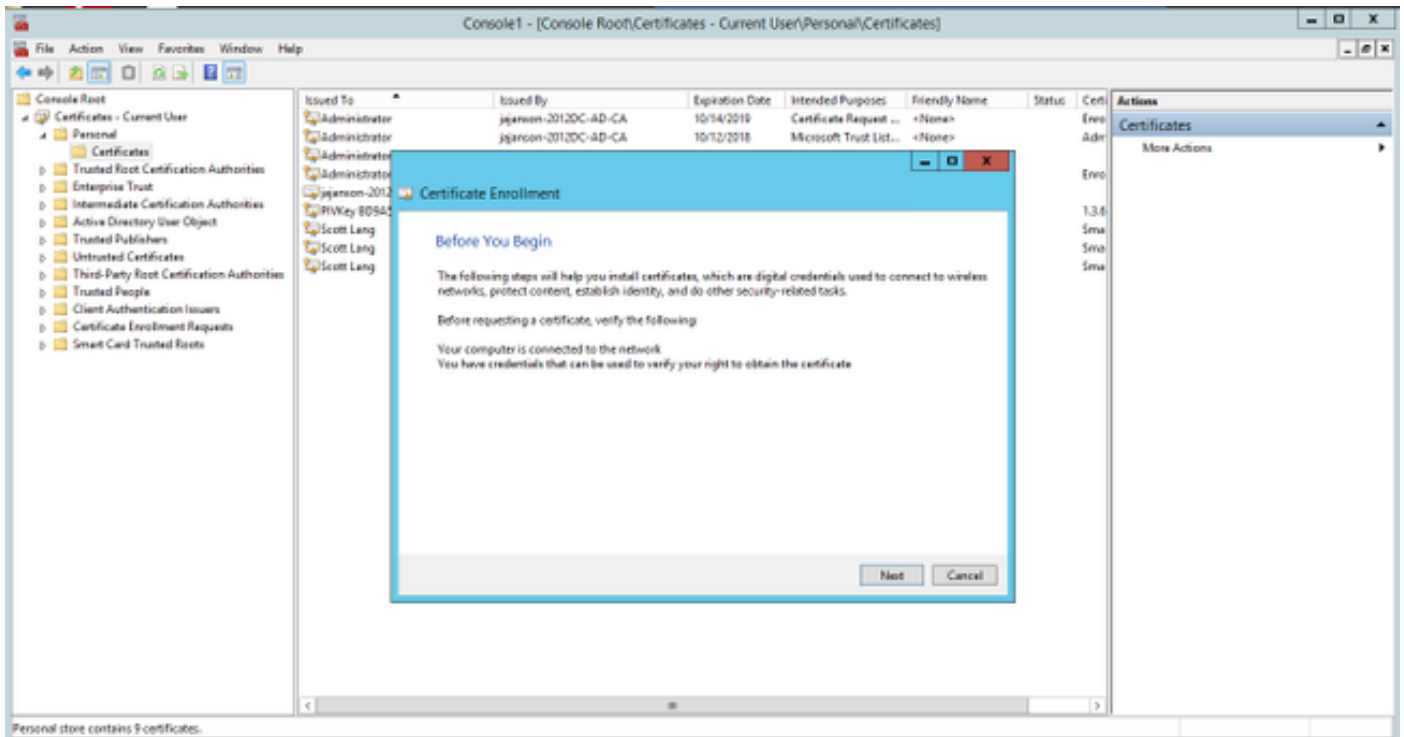


Inscriver-se em nome de

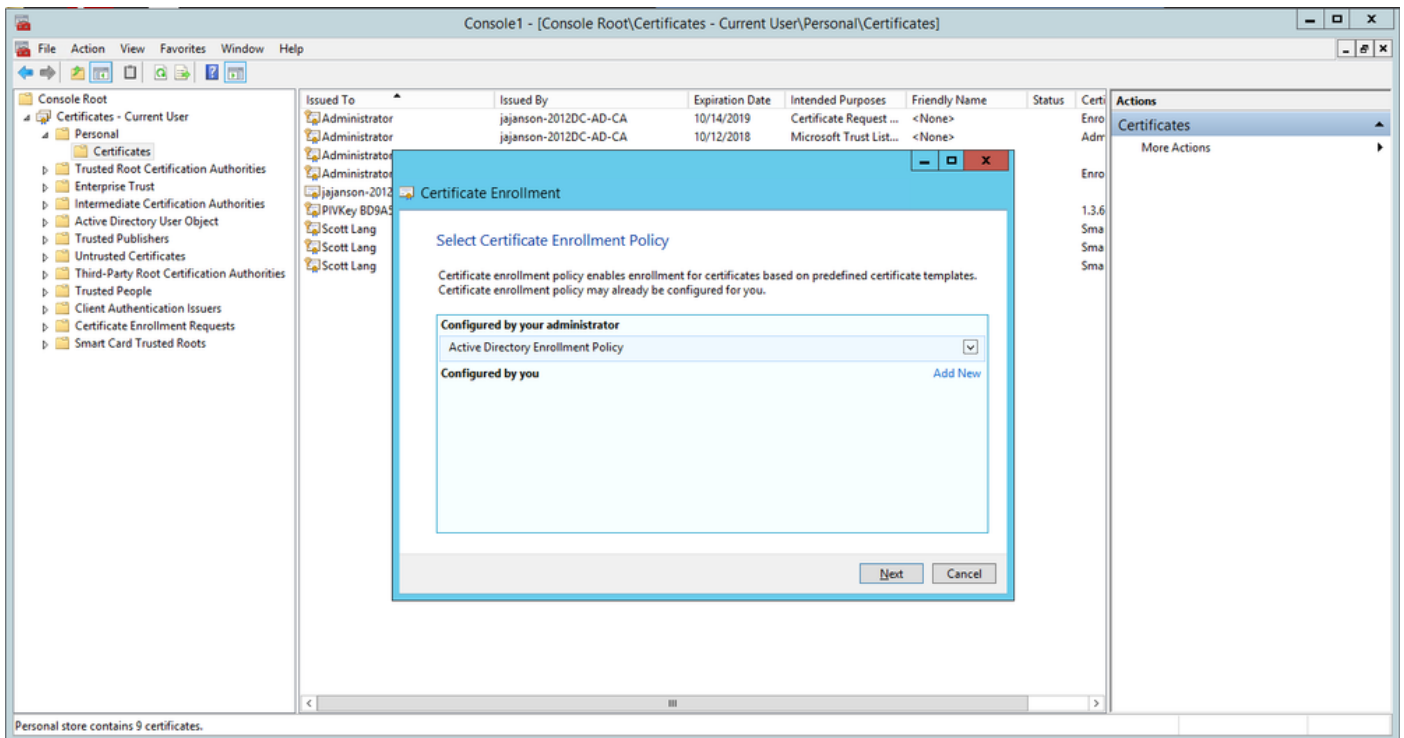
1. Inicie o MMC e importe o **Módulo e o Gerente de Certificados** para a Minha Conta de Usuário.
2. Clique com o botão direito do mouse ou selecione **Pessoal > Certificados** e selecione **Todas as Tarefas > Operações Avançadas** e clique em **Inscriver-se em nome de...**
3. No assistente, escolha a Política de Registro do Ative Directory e clique em **Avançar**.



Inscreeva-se em nome de

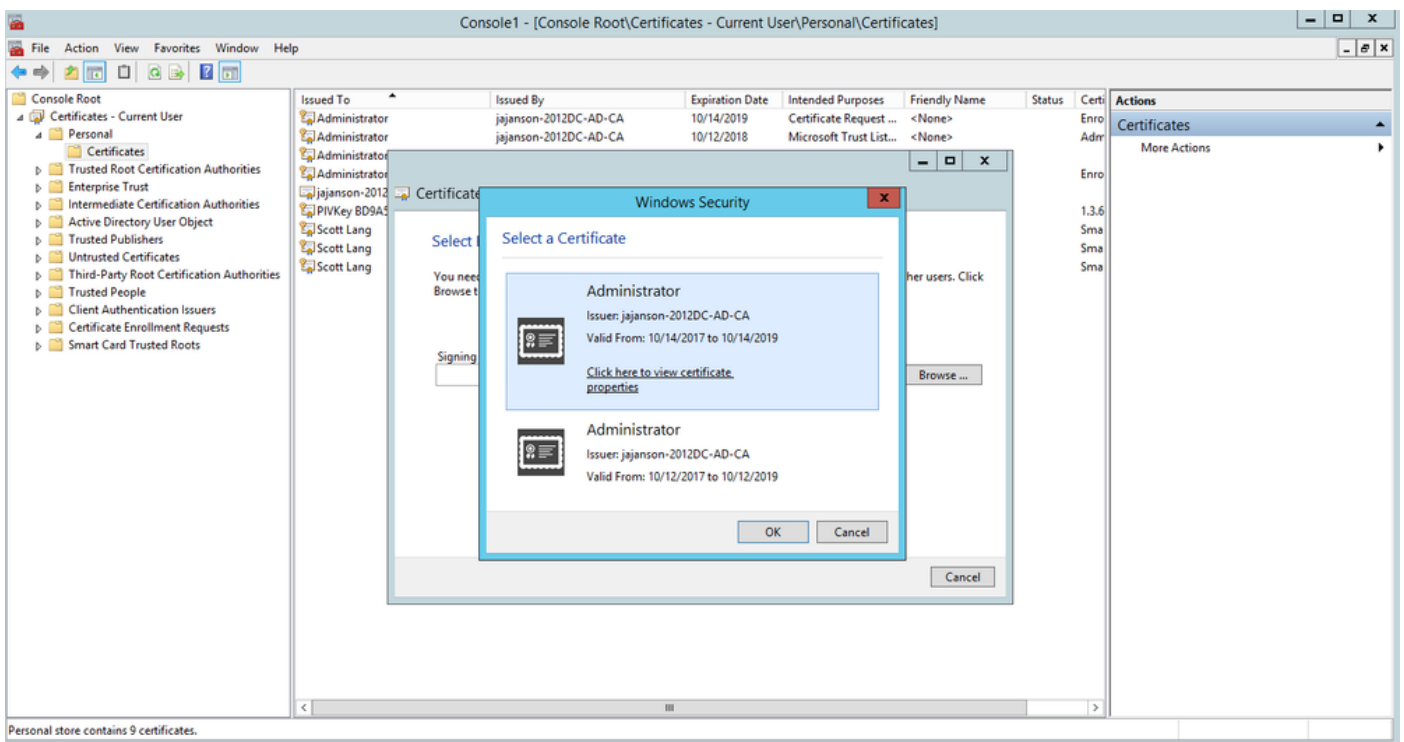


4. Seleccione Política de registro de certificado e clique em **Avançar**.



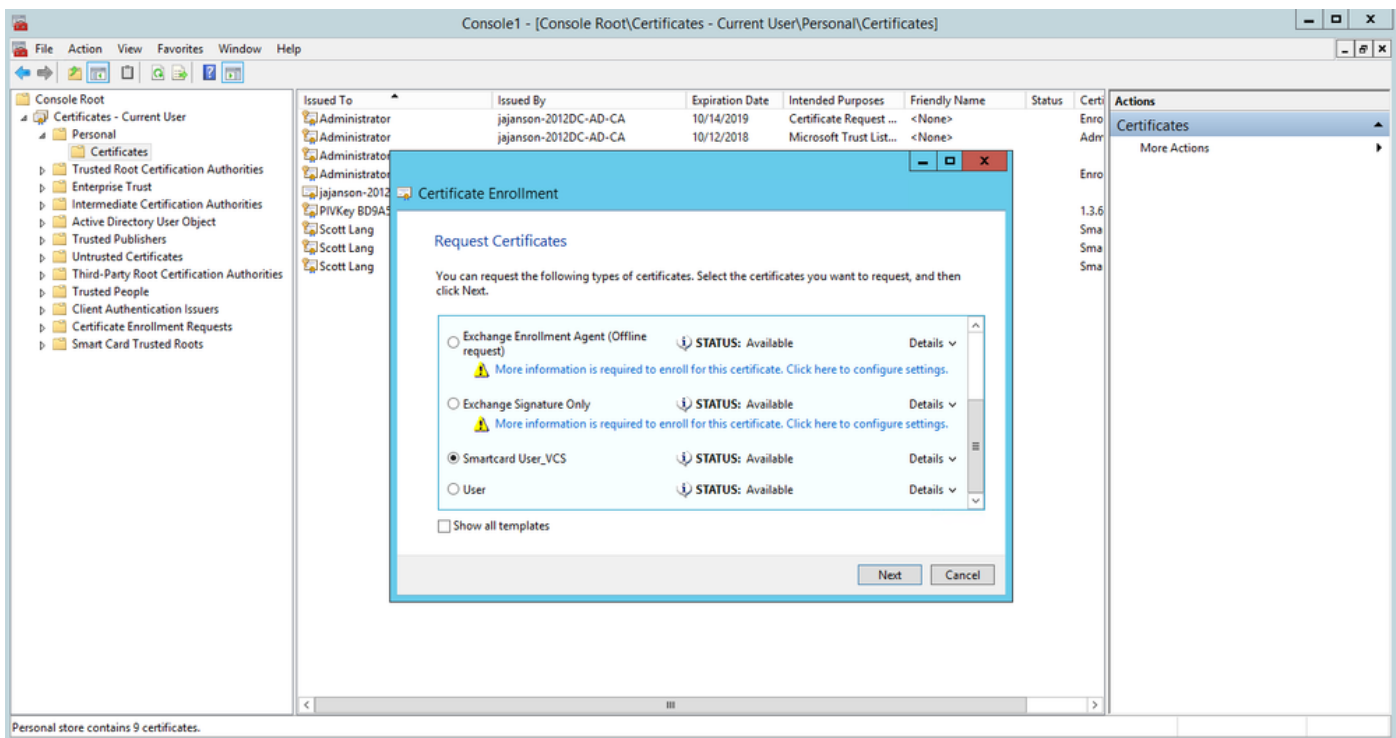
Política de inscrição

5. Agora, é solicitado que você selecione o **certificado de assinatura**. Este é o certificado de inscrição solicitado anteriormente.



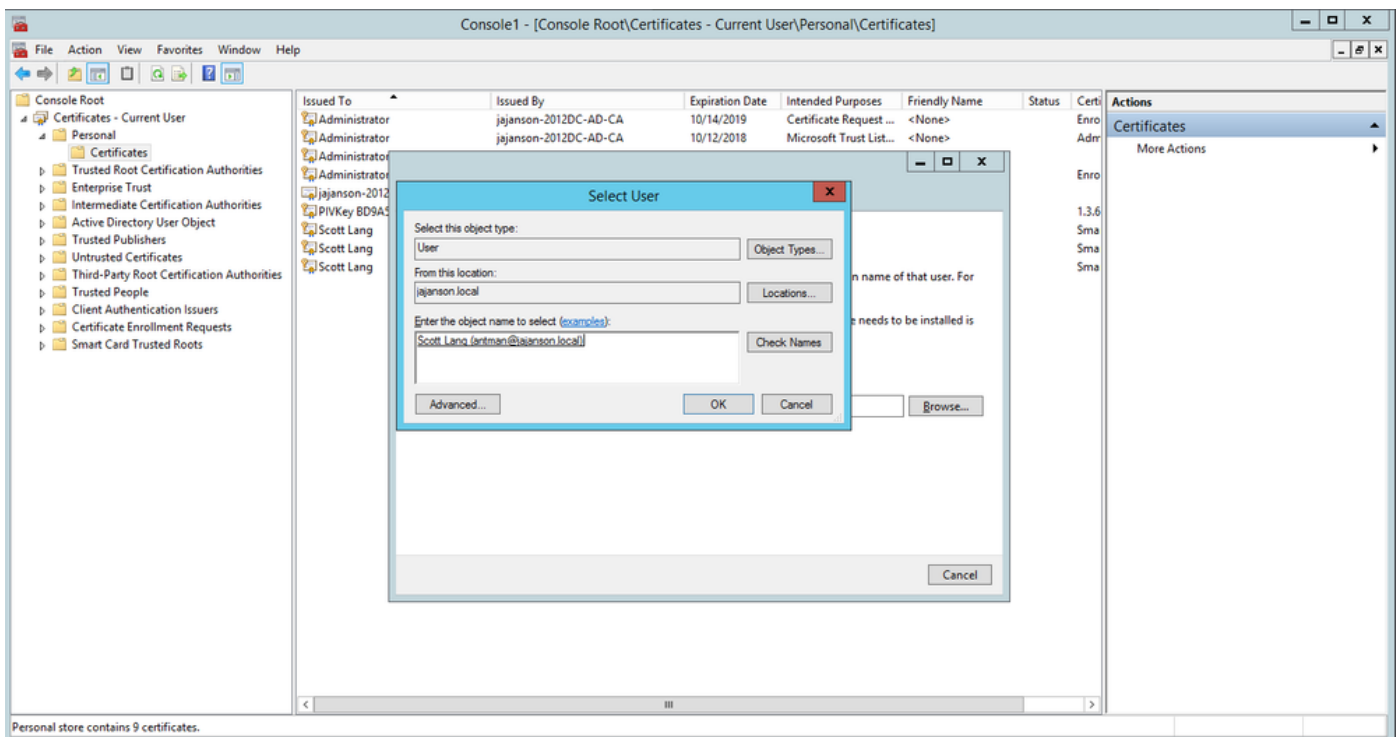
Selecionar certificado de assinatura

6. Na próxima tela, você precisa navegar até o certificado que gostaria de solicitar e, nesta instância, é o **Smartcard User_VCS** que é o modelo criado anteriormente.



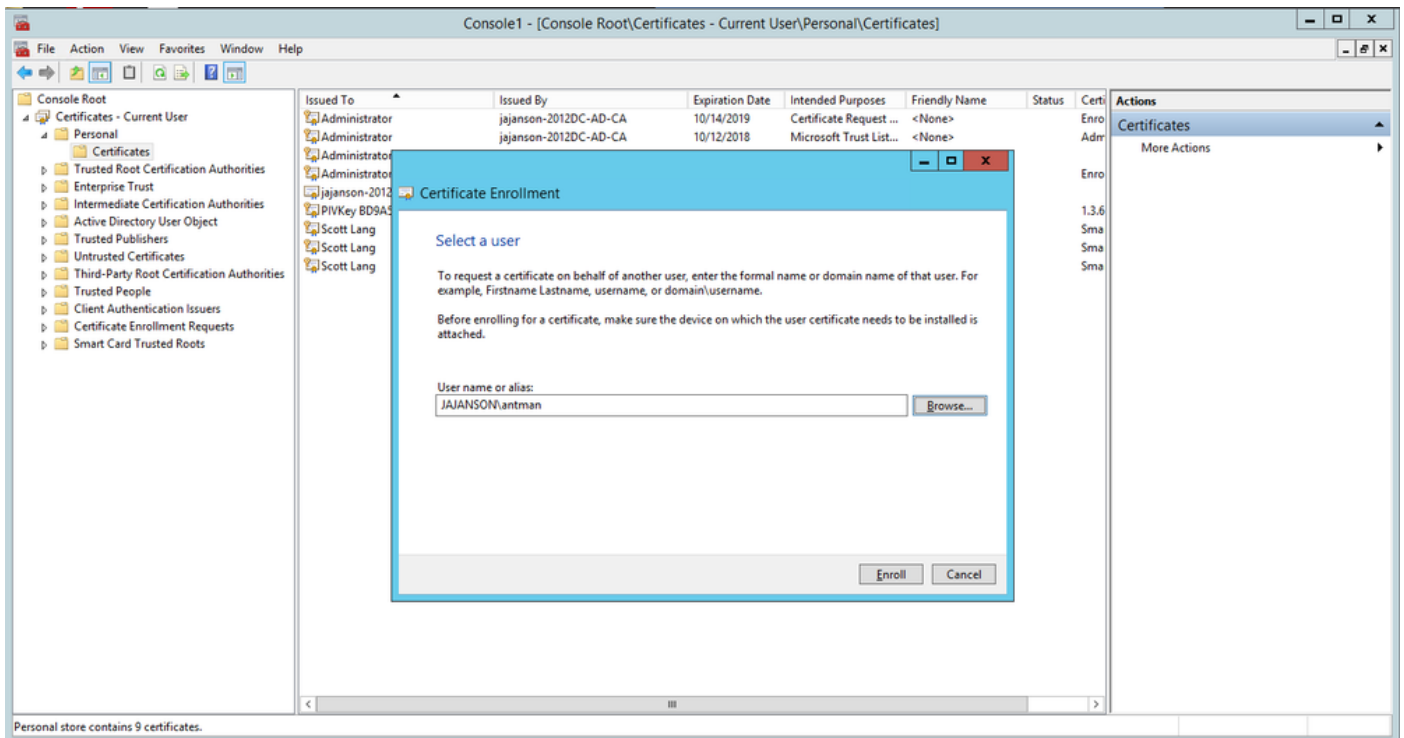
Escolha o cartão inteligente VCS

7. Em seguida, selecione o usuário que deseja inscrever em nome do. Clique em **Procurar** e digite o nome de usuário do funcionário que deseja inscrever. Neste caso, é usada a 'conta antman@jajanson.local' de Scott Lang.



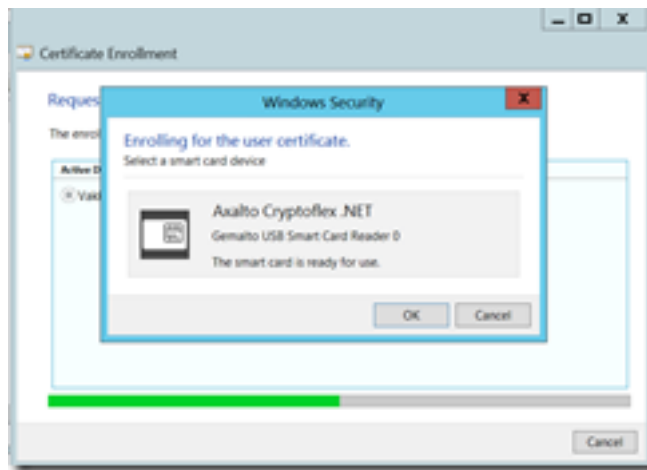
Escolha o usuário

8. Na próxima tela, continue com a inscrição clicando em **Inscriver-se**. Agora, insira um smartcard em seu leitor.



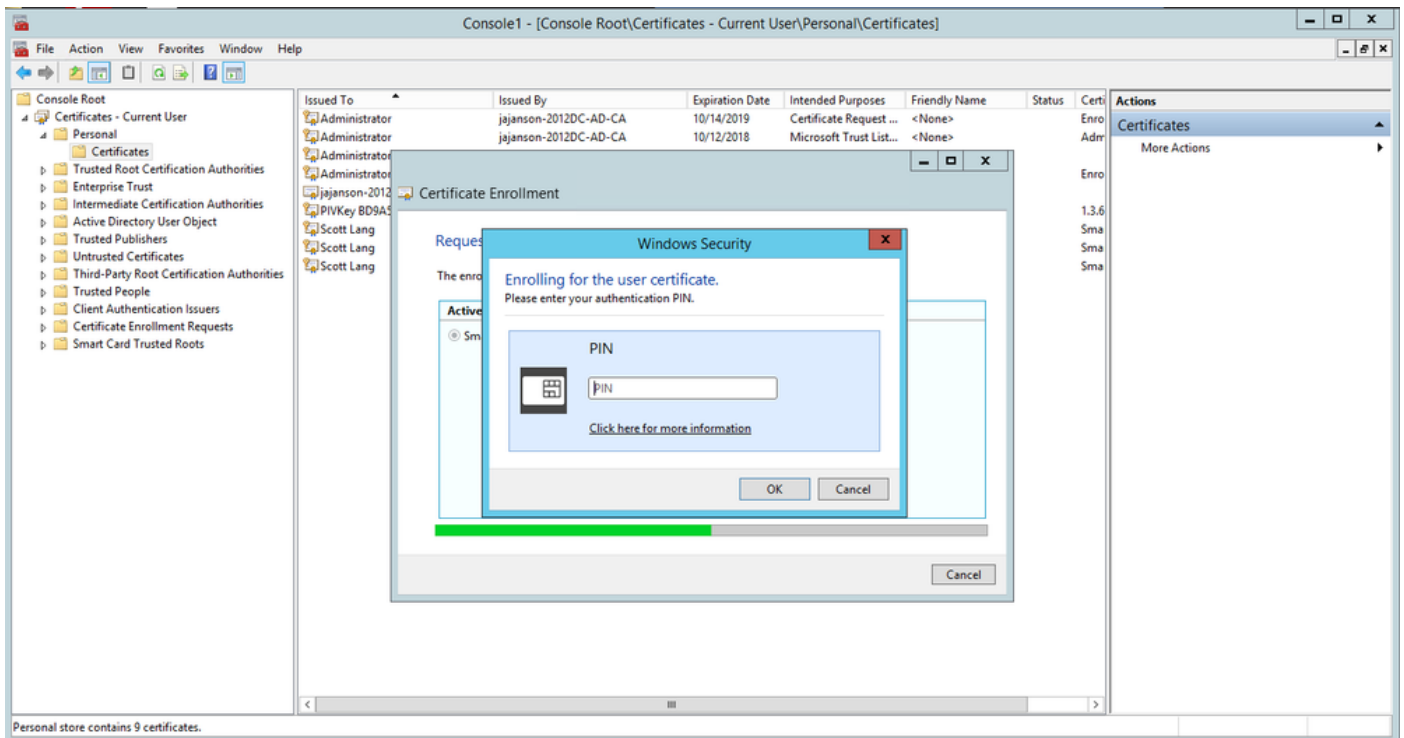
Inscrever-se

9. Depois de inserir seu smartcard, ele é detectado da seguinte forma:



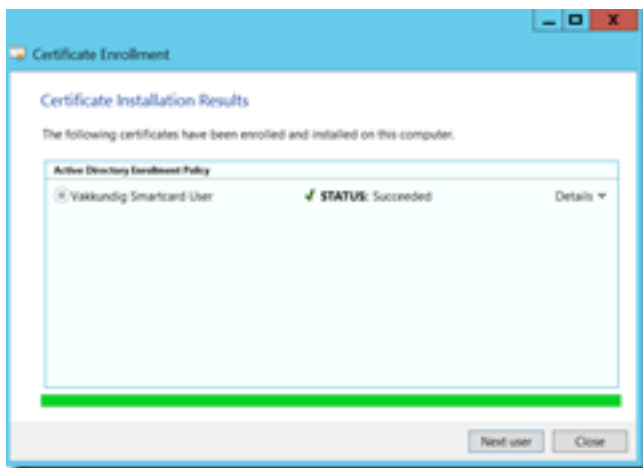
Insira o Smart Card

10. Em seguida, é solicitado que você digite um número PIN do cartão inteligente (Pino padrão: 0000).



Insira o pino

11. Por fim, depois de ver a tela **Enrollment Successful**, você poderá usar esse smartcard para fazer login em um servidor associado a domínio, como o VCS com apenas a placa e um pin conhecido. No entanto, não é feito sim, você ainda precisa preparar o VCS para redirecionar as solicitações de autenticação para o Smart Card e usar o Common Access Card para liberar o certificado de smartcard armazenado no smartcard para autenticação.



Inscrição bem-sucedida

Configure o VCS para a placa de acesso comum

Carregue a CA raiz na lista de certificados CA confiáveis no VCS navegando para **Manutenção > Segurança > Certificado CA confiável**.

2. Carregue a lista de revogação de certificado assinada pela CA raiz no VCS. Navegue até **Manutenção > Segurança > Gerenciamento de CRL**.

3. Teste seu certificado de cliente em relação ao seu regex, que extrai o nome de usuário do certificado para usar para autenticação em relação ao LDAP ou usuário local. O regex vai corresponder ao **assunto** do certificado. Pode ser o seu UPN, e-mail e assim por diante. Neste laboratório, o e-mail para correspondência com o certificado do cliente para o certificado do cliente foi usado.

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

Assunto do certificado do cliente

4. Navegue até **Manutenção > Segurança > Teste de certificado do cliente**. Selecione o certificado do cliente a ser testado, em Meu laboratório foi antman.pem, carregue-o na área de teste. Na seção **Padrão de autenticação baseado em certificado em Regex para corresponder ao certificado** cole seu regex para ser testado. Não altere o campo **Formato do nome de usuário**.

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

The screenshot shows the Cisco TelePresence Video Communication Server Expressway interface. The main heading is 'Client certificate testing'. Under 'Certificate source', there is a dropdown menu for 'Certificate source' and a 'Browse...' button. Below that, it says 'Currently uploaded test file: antman.pem'. The 'Certificate-based authentication pattern' section has a 'Regex to match against certificates' field containing the regex: /Subject:.*emailAddress=(? .*)@jajanson.local/m. Below this is a 'Username format' field containing: #captureCommonName#. There is a 'Make these settings permanent' button at the bottom of this section.

Teste seu regex no 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}";@bjackson.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:
            2400000001170f460b3102511a46513700000000000117
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=Antman,OU=DOE,OU=CA,OU=BJackson,DC=local
        Validity
            Not Before: Oct 17 21:39:55 2017 GMT
            Not After: Oct 17 21:39:55 2017 GMT
        Subject: emailAddress={captureCommonName};@bjackson.local
        Subject Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
            009f46d09f5a12815a1517b46810246b1131cd0771
            0c19a1081841374210917516d12d0f11391d91c041
            61651db1f81761081c16d12410f0010a1f51451
            681fc1081081f817a13112710e1410811711d11f1f91
            9512191f26131c10c10010f10a115c14210410e10f1
            a81441121718810d10410d1081f21f71f410610c1011
            041105161a1761210f10510210810010b1001711a1
            c413217f14813614210410c13c10a1051f816718912b1
    
```


← 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 do teste


5. Se o teste fornecer os resultados desejados, clique no botão **Torne essas alterações permanentes**. Isso altera seu regex para a **configuração de autenticação baseada em certificado** do servidor. Para verificar a alteração, navegue até essa configuração, **Manutenção > Segurança > configuração de autenticação baseada em certificado**.


6. Ative a autenticação baseada em cliente navegando para **Sistema > Administrador** e clique ou selecione a caixa suspensa para escolher **Segurança baseada em certificado do cliente = Autenticação baseada em cliente**. Com essa configuração, o usuário digita o FQDN do servidor VCS em seu navegador e é solicitado que ele escolha sua conta de cliente e insira o pino atribuído a sua Placa de Acesso Comum. Em seguida, o certificado é liberado e ele retorna a GUI da Web do servidor VCS e tudo o que precisa fazer é clicar ou selecionar o botão Administrador. Então ele é admitido no servidor. Se as opções **Segurança baseada em certificado do cliente = Validação baseada em cliente** estiverem selecionadas, o processo será o mesmo, com exceção quando o usuário clicar no botão Administrador, ele terá solicitado novamente a senha do administrador. Normalmente, o último não é o que a organização está tentando realizar com o 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](#)

Ativar autenticação baseada em cliente

Socorro! Estou trancado para fora!!

Se você habilitar a autenticação baseada em cliente e o VCS rejeitar o certificado por qualquer motivo, você não poderá mais fazer login com a GUI da Web da maneira tradicional. Mas, não se preocupe, há uma maneira de voltar ao seu sistema. O documento anexo pode ser encontrado no site da Cisco e fornece informações sobre como desativar a autenticação baseada em cliente do acesso raiz.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta

configuração.