

Configurer VCS avec CAC et un lecteur de carte à puce

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Qu'est-ce qu'une carte à puce ?](#)

[Configuration](#)

[Vérification](#)

[Dépannage](#)

Introduction

Ce document décrit un guide détaillé pour installer et utiliser un lecteur de carte à puce et une carte d'accès commune pour une utilisation avec le serveur de communication vidéo Cisco (VCS) pour les entreprises qui ont besoin d'une authentification à deux facteurs pour l'environnement VCS, comme les banques, les hôpitaux ou les gouvernements disposant d'installations sécurisées.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations de ce document sont basées sur 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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Le CAC fournit l'authentification requise afin que " systèmes " savoir qui a obtenu l'accès à leur environnement et quelle partie de l'infrastructure, qu'elle soit physique ou électronique. Dans les environnements classifiés du gouvernement et dans d'autres réseaux sécurisés, les règles d'accès " moins privilégiés " ou " doivent savoir " prévaloir. Une connexion peut être utilisée par n'importe qui, l'authentification nécessite quelque chose que l'utilisateur a, par exemple, le CAC, également connu sous le nom de Common Access Card, est né en 2006, de sorte que l'individu

n'aurait pas besoin d'avoir plusieurs appareils, qu'il s'agisse de postes, de cartes d'identité ou de dongles pour accéder à son lieu de travail ou à ses systèmes.

Qu'est-ce qu'une carte à puce ?

Les cartes à puce sont un composant clé de l'infrastructure à clé publique (PKI) que Microsoft utilise pour s'intégrer à la plate-forme Windows, car les cartes à puce améliorent les solutions logicielles uniquement, telles que l'authentification des clients, la connexion et la messagerie sécurisée. Les cartes à puce constituent un point de convergence pour les certificats de clé publique et les clés associées car elles :

- Fournir un stockage résistant aux altérations pour la protection des clés privées et d'autres formes d'informations personnelles.
- Isoler les calculs stratégiques en matière de sécurité, qui impliquent l'authentification, les signatures numériques et l'échange de clés à partir d'autres parties du système qui n'ont pas besoin de savoir.
- Permettre la portabilité des informations d'identification et autres informations privées entre les ordinateurs au travail, à la maison ou en déplacement.

La carte à puce fait désormais partie intégrante de la plate-forme Windows, car les cartes à puce offrent de nouvelles fonctionnalités souhaitables, révolutionnaires pour l'industrie informatique comme l'introduction de la souris ou du CD-ROM. Si vous n'avez pas d'infrastructure d'ICP interne pour le moment, vous devez d'abord vous assurer de le faire. Ce document ne couvre pas l'installation de ce rôle dans cet article particulier, mais des informations sur la façon de le mettre en oeuvre peuvent être trouvées ici : <http://technet.microsoft.com/en-us/library/hh831740.aspx>.

Configuration

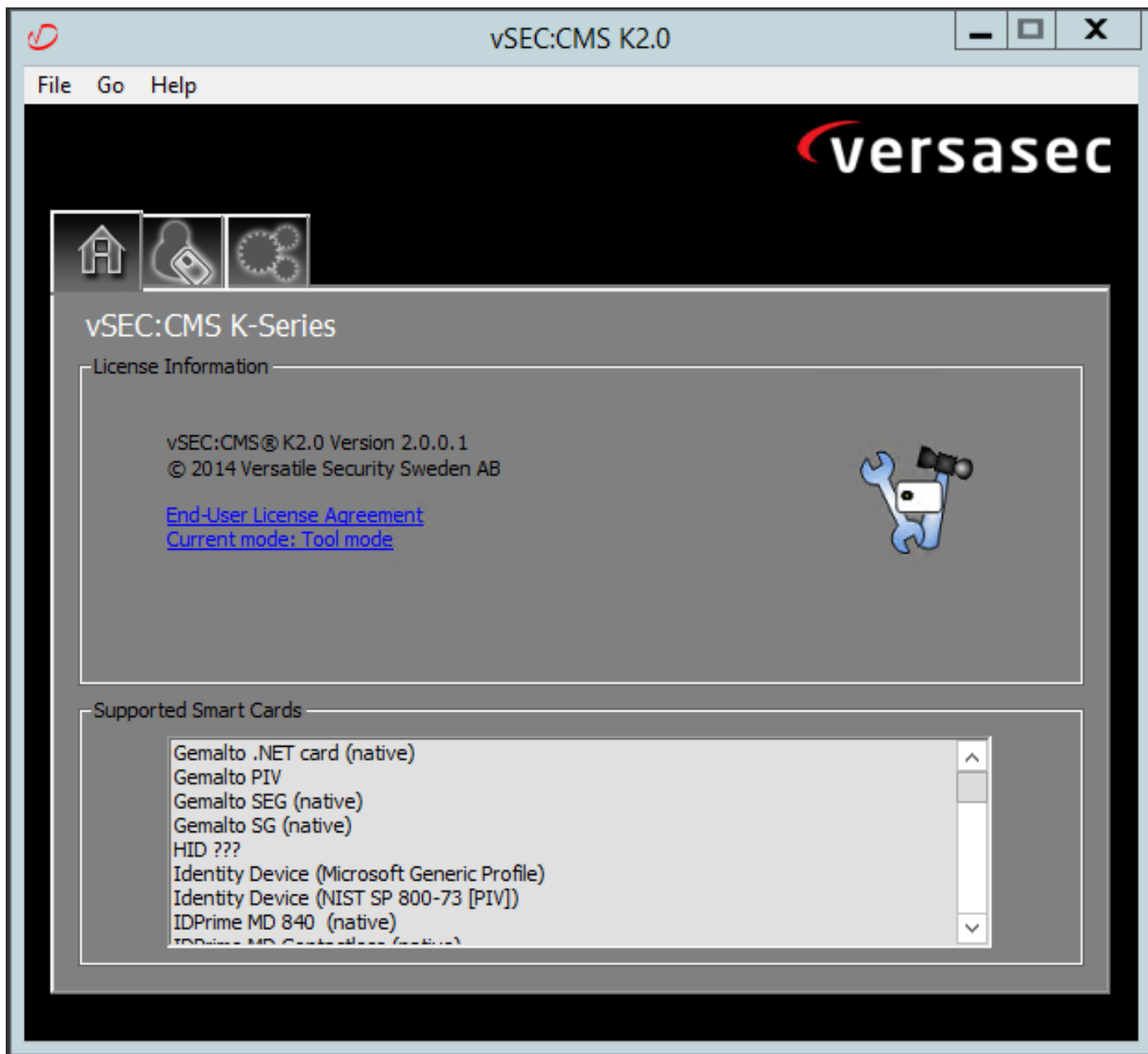
Ce TP suppose que vous avez déjà intégré LDAP à VCS et que vous avez des utilisateurs capables de se connecter avec des informations d'identification LDAP.

1. [Équipement de laboratoire](#)
2. [Installer la carte à puce](#)
3. [Configurer les modèles d'autorité de certification](#)
4. [Inscrire le certificat d'agent d'inscription](#)
5. [S'inscrire au nom de...](#)
6. [Configuration de VCS pour la carte d'accès commune](#)

Équipement requis :

Serveur de domaine Windows 2012R2 doté des rôles et du logiciel installé suivants :

- Autorité de certification
- Active Directory
- DNS
- PC Windows avec carte à puce connectée
- vSEC : Logiciel de gestion CMS série K pour gérer votre carte à puce :



Logiciel Versa Card Reader

Installer la carte à puce

Les lecteurs de cartes à puce contiennent généralement des instructions sur la façon de connecter les câbles nécessaires. Voici un exemple d'installation pour cette configuration.

Installation d'un pilote de périphérique de lecteur de carte à puce

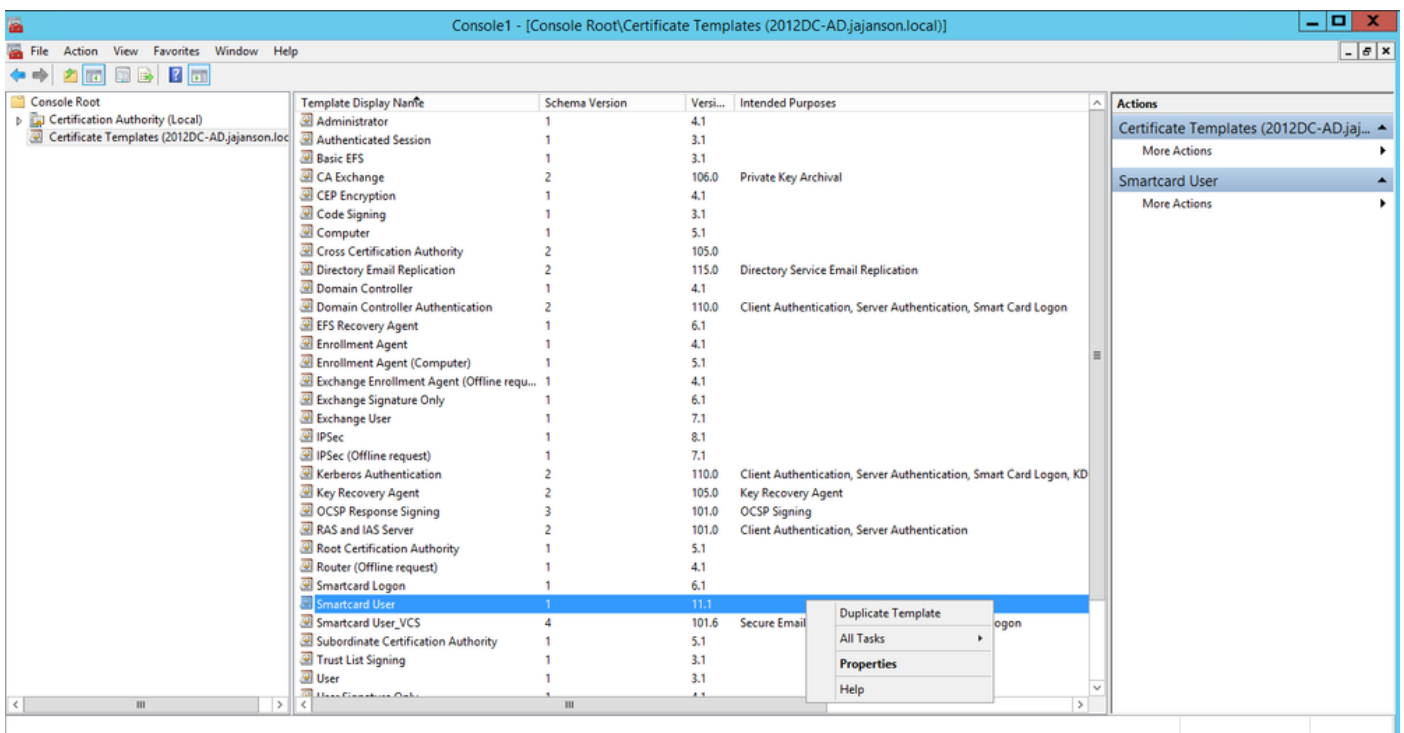
Si le lecteur de carte à puce a été détecté et installé, l'écran d'ouverture de session Welcome to Windows le reconnaît. Dans le cas contraire :

1. Connectez votre carte à puce au port USB de votre ordinateur Windows
2. Suivez les instructions à l'écran pour installer le pilote de périphérique. Cela nécessite le support du pilote que le fabricant de la carte à puce ou le pilote est détecté dans Windows. Dans mon cas, j'ai utilisé le pilote de fabrication à partir de leur site de téléchargement. **NE FAITES PAS CONFIANCE AUX FENÊTRES.**
3. Cliquez avec le bouton droit de la souris sur l'icône **Poste de travail** de votre bureau et cliquez sur **Gérer** dans le sous-menu.

4. Développez le noeud **Services et applications**, puis cliquez sur **Services**.
5. Dans le volet droit, cliquez avec le bouton droit de la souris sur **Carte à puce**. Cliquez sur **Propriétés** dans le sous-menu.
6. Dans l'onglet **Général**, sélectionnez **Automatique** dans la liste déroulante **Type de démarrage**. Cliquez OK.
7. Redémarrez votre machine si l'assistant Matériel vous le demande.

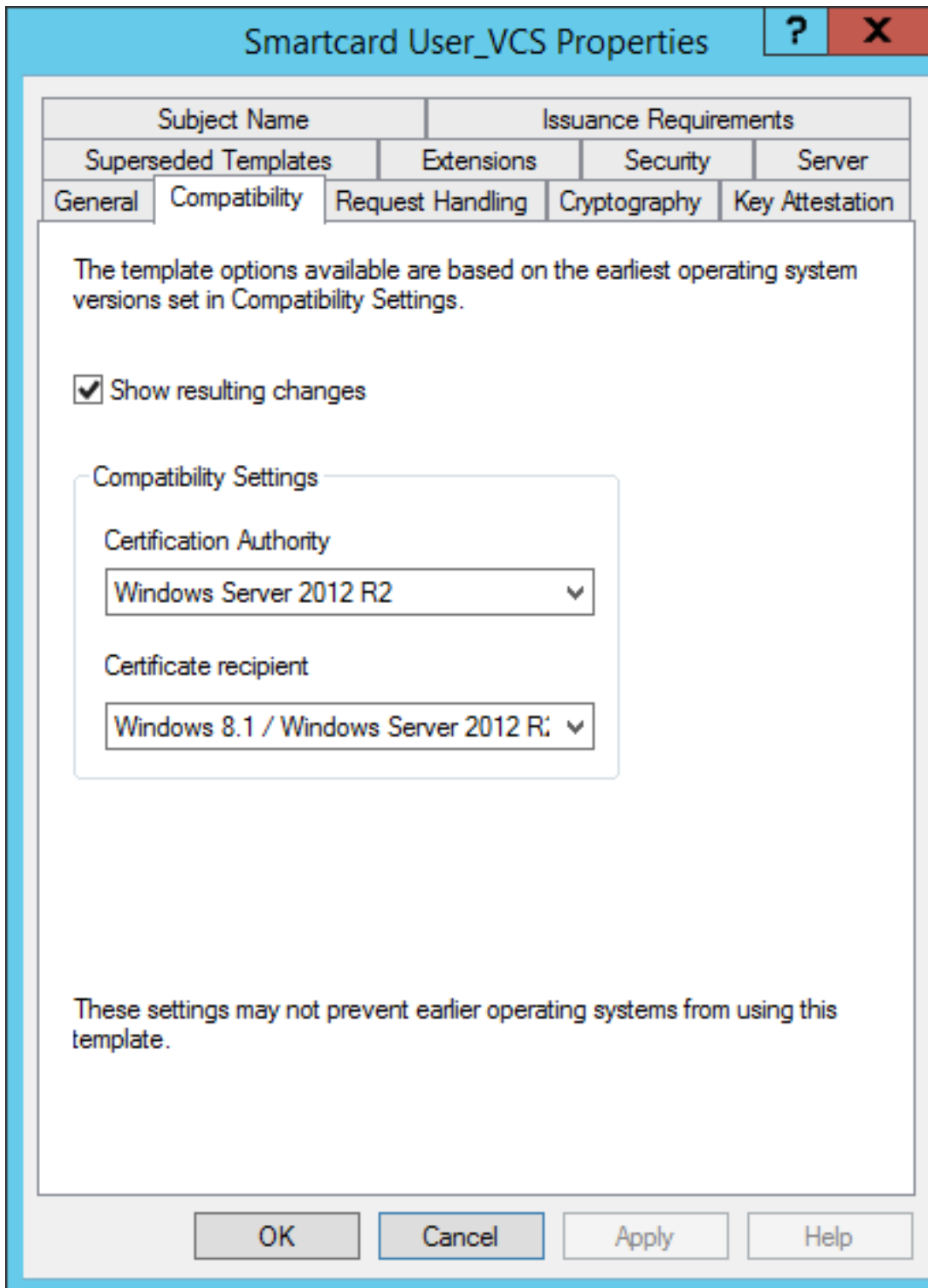
Configurer les modèles d'autorité de certification

1. Lancez l'autorité de certification MMC à partir des outils d'administration.
2. Cliquez ou sélectionnez le noeud **Modèles de certificats** et sélectionnez **Gérer**.
3. Cliquez avec le bouton droit de la souris ou sélectionnez le modèle de certificat **utilisateur Smartcard**, puis sélectionnez **Dupliquer** comme indiqué dans l'image.



Modèles de certificats de contrôleur de domaine

4. Dans l'onglet **Compatibility**, sous **Certification Authority**, passez en revue la sélection et modifiez-la si nécessaire.



Paramètres de

compatibilité des cartes à puce

5. Dans l'onglet **Général** :

a. Spécifiez un nom, tel que **Smartcard User_VCS**.

b. Définissez la période de validité sur la valeur souhaitée. Cliquez sur Apply.

Smartcard User_VCS Properties

Subject Name		Issuance Requirements	
Superseded Templates		Extensions	Security
Server			
General	Compatibility	Request Handling	Cryptography
Key Attestation			

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

OK Cancel Apply Help

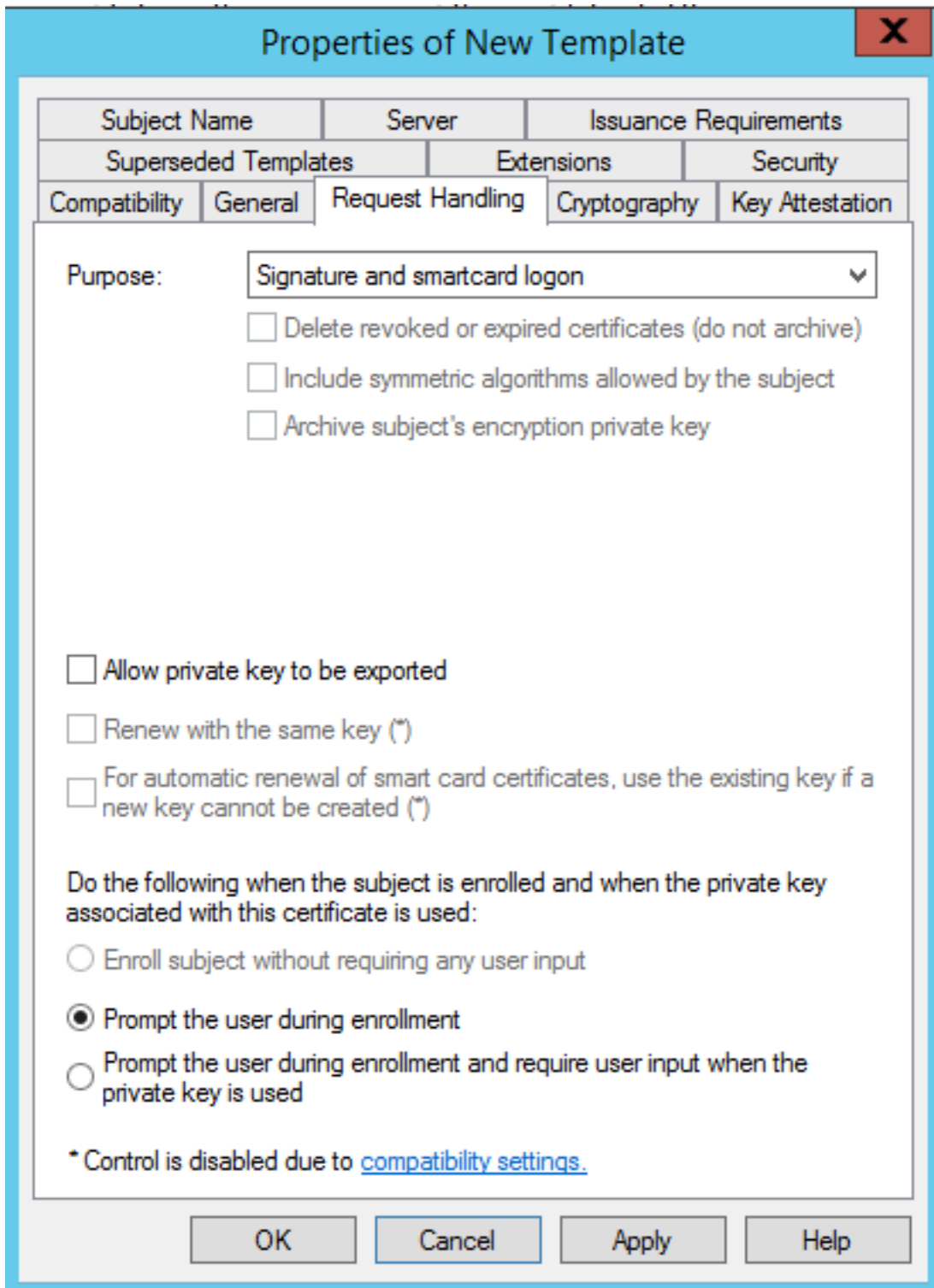
Expiration de l'heure

de début générale de la carte à puce

6. Dans l'onglet **Gestion des demandes** :

a. Définissez la fonction sur **Signature et connexion par carte à puce**.

b. Cliquez sur **Demander à l'utilisateur lors de l'inscription**. Cliquez sur Apply.



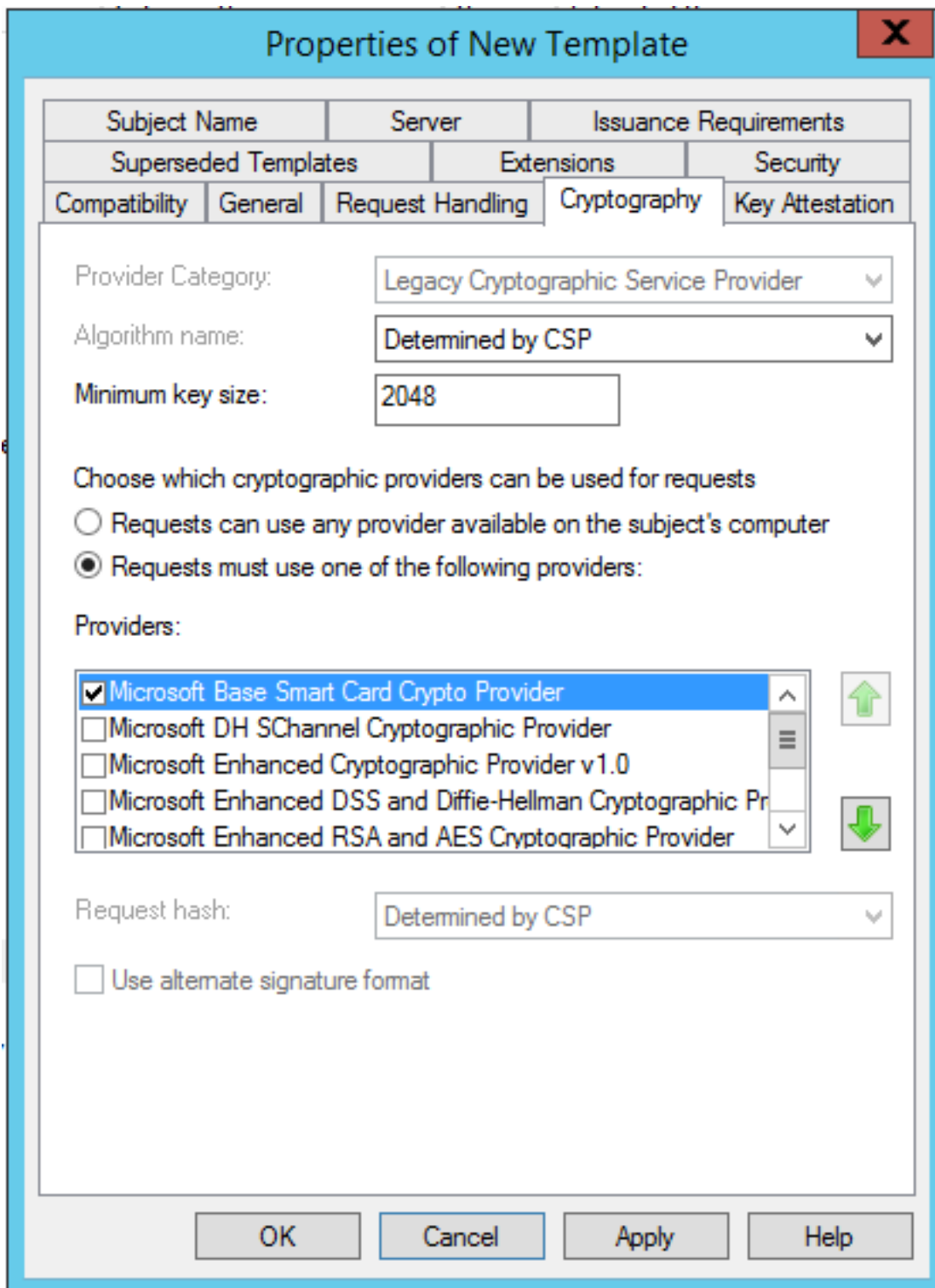
Gestion des

demandes de carte à puce

7. Dans l'onglet **Cryptographie**, définissez la taille de clé minimale sur 2048.

a. Cliquez sur **Demandes doivent utiliser l'un des fournisseurs suivants**, puis sélectionnez **Fournisseur de chiffrement de carte à puce Microsoft Base**.

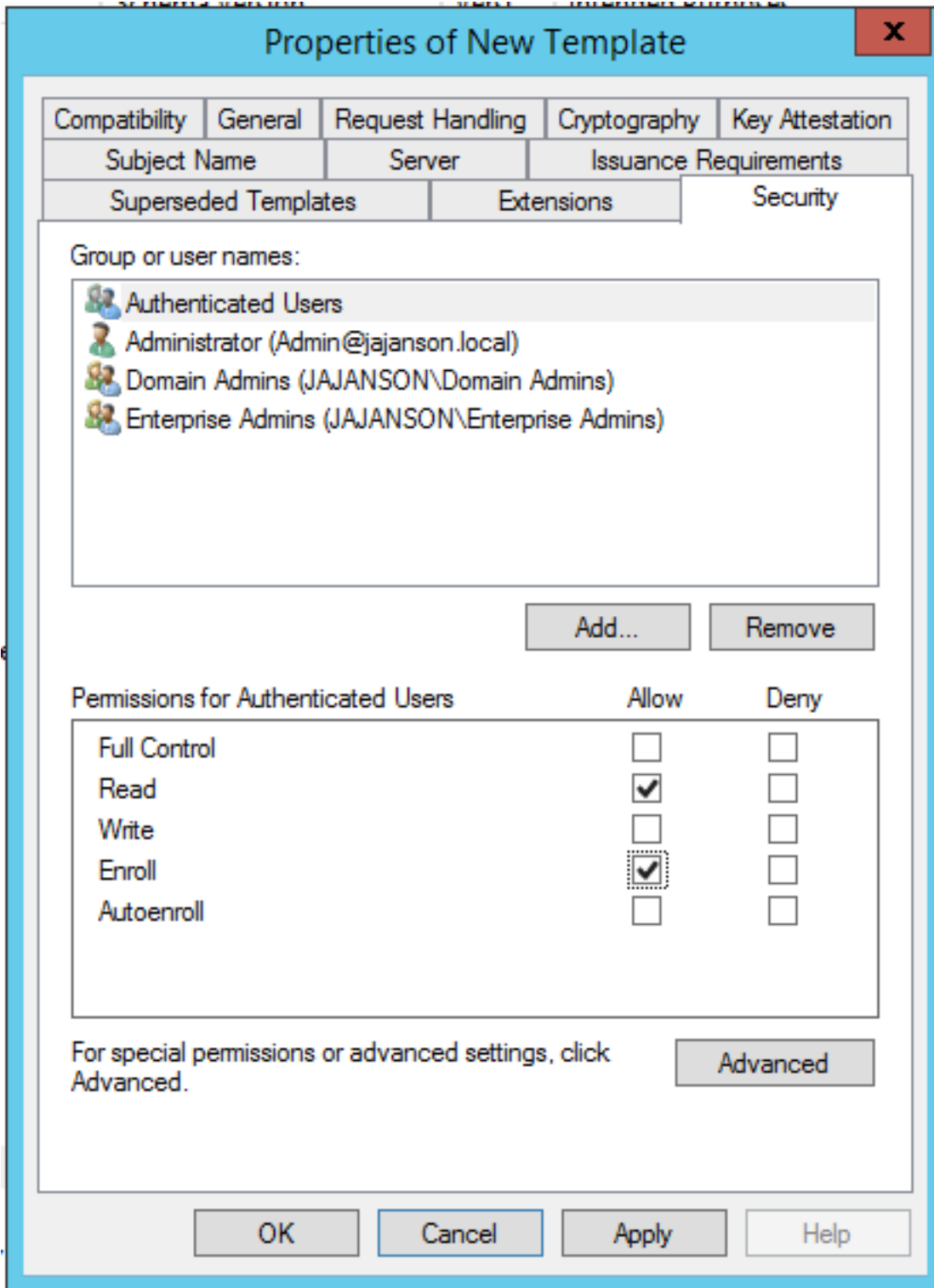
b. Cliquez sur **Apply**.



Paramètres de

chiffrement du certificat

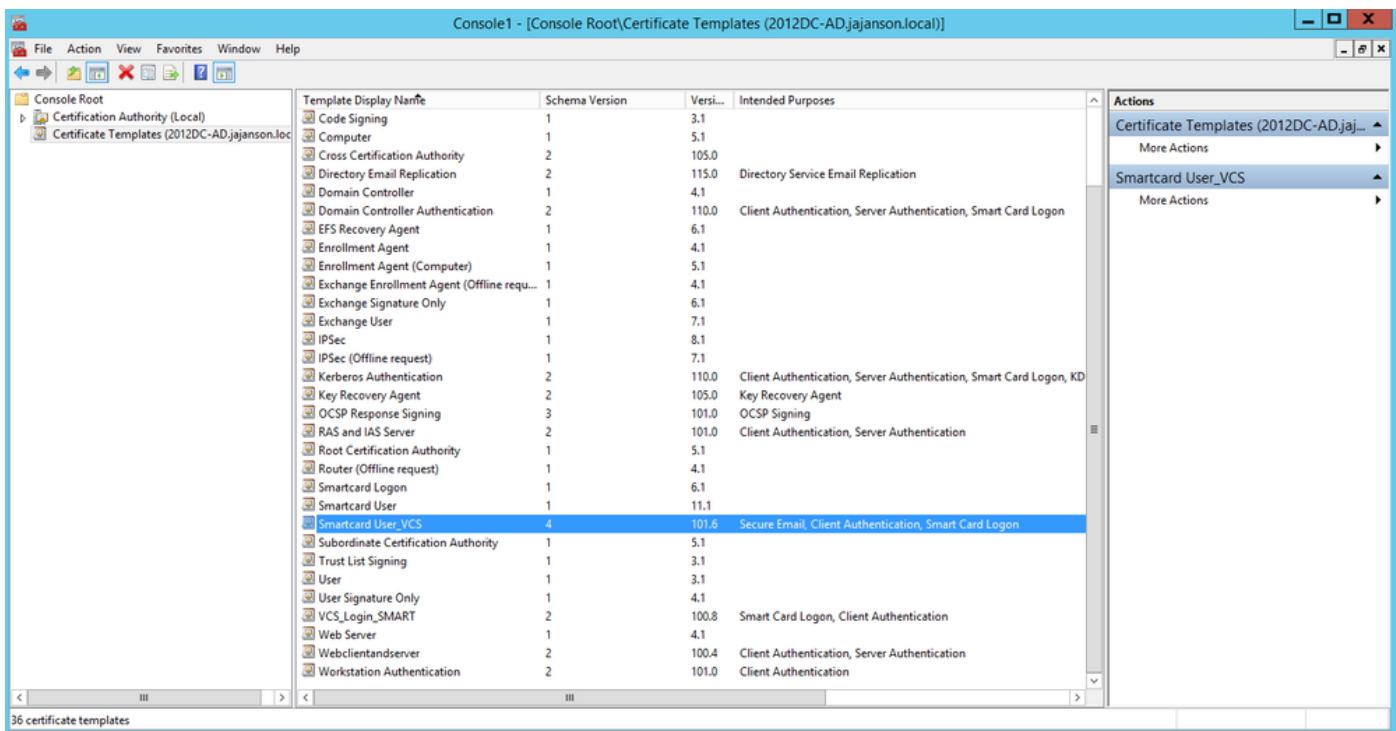
8. Dans l'onglet Sécurité, ajoutez le groupe de sécurité auquel vous souhaitez donner accès à l'option Inscription. Par exemple, si vous voulez donner accès à tous les utilisateurs, sélectionnez le groupe Utilisateurs authentifiés, puis sélectionnez Autorisations **d'inscription** pour eux.



Sécurité des

modèles

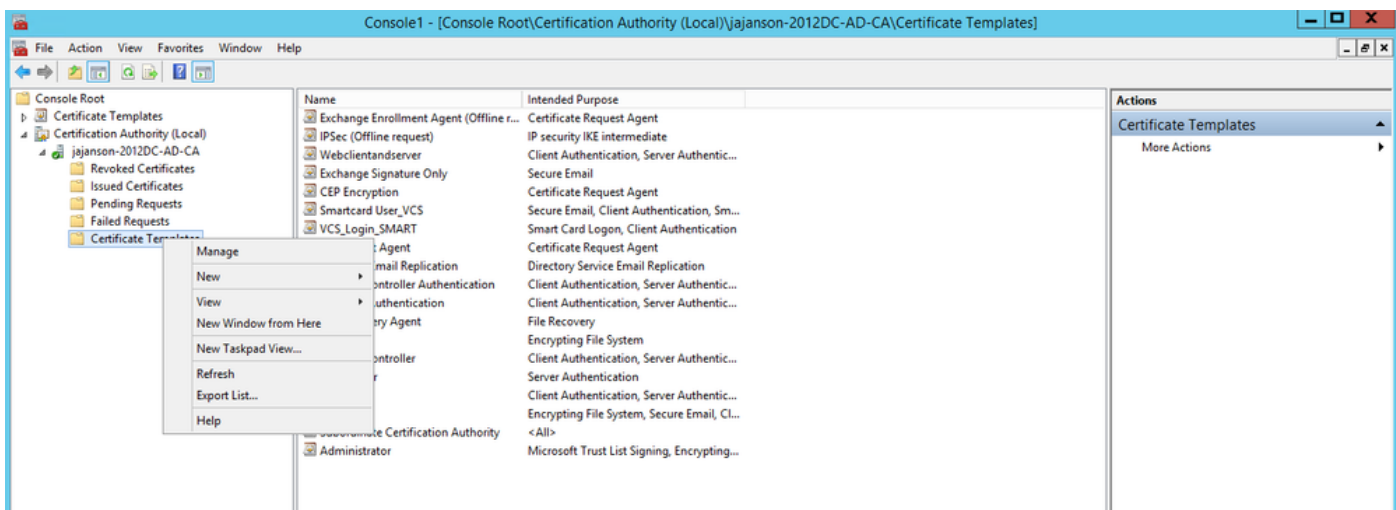
9. Cliquez sur **OK** afin de finaliser vos modifications et de créer le nouveau modèle. Votre nouveau modèle doit maintenant apparaître dans la liste des modèles de certificat.



Modèle vu dans le contrôle de domaine

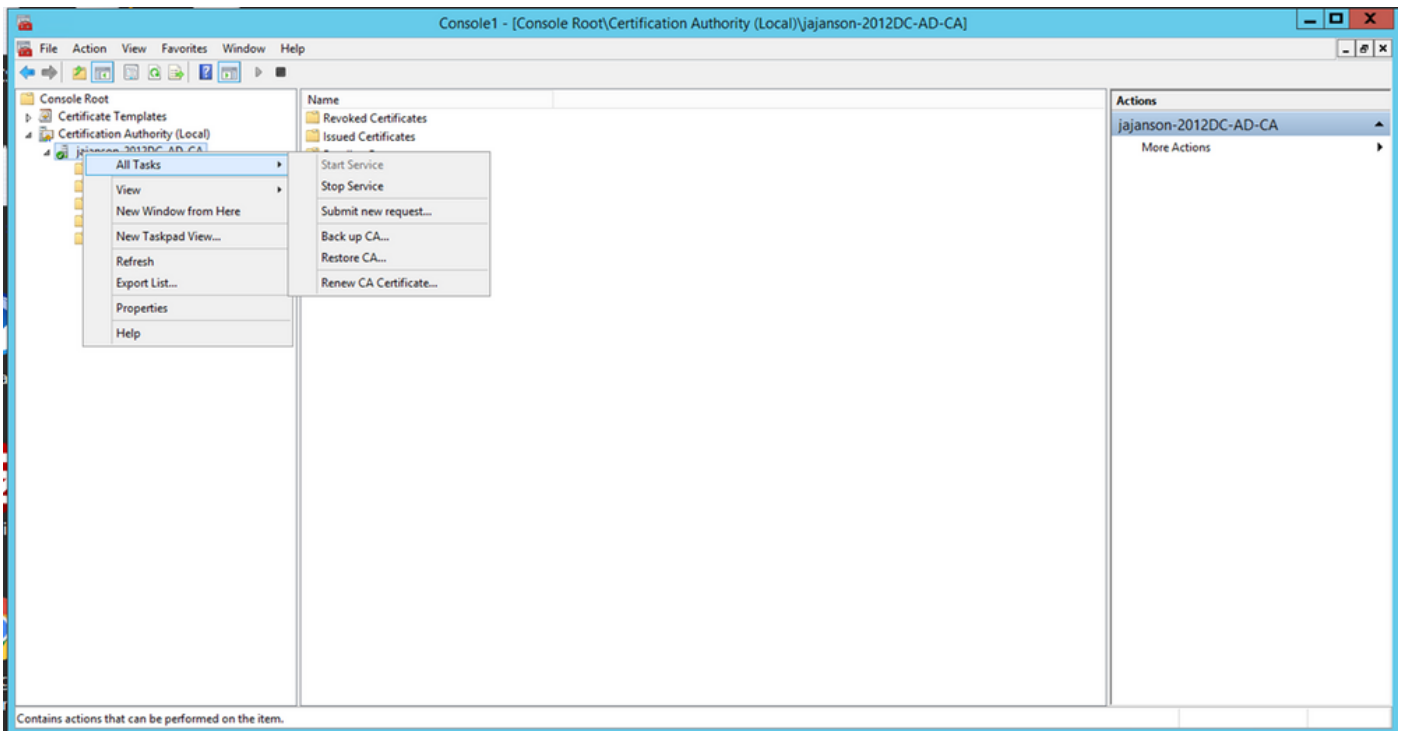
10. Dans le volet gauche du MMC, développez Autorité de certification (locale), puis développez votre Autorité de certification dans la liste Autorité de certification.

Cliquez avec le bouton droit sur Modèles de certificats, cliquez sur **Nouveau**, puis sur **Modèle de certificat** pour émettre. Choisissez ensuite le nouveau modèle de carte à puce.



Émettre un nouveau modèle

11. Une fois le modèle répliqué, dans MMC, cliquez avec le bouton droit de la souris ou sélectionnez la liste Autorité de certification, cliquez sur **Toutes les tâches**, puis cliquez sur **Arrêter le service**. Ensuite, cliquez à nouveau avec le bouton droit sur le nom de l'Autorité de certification, cliquez sur **Toutes les tâches**, puis sur **Démarrer le service**.

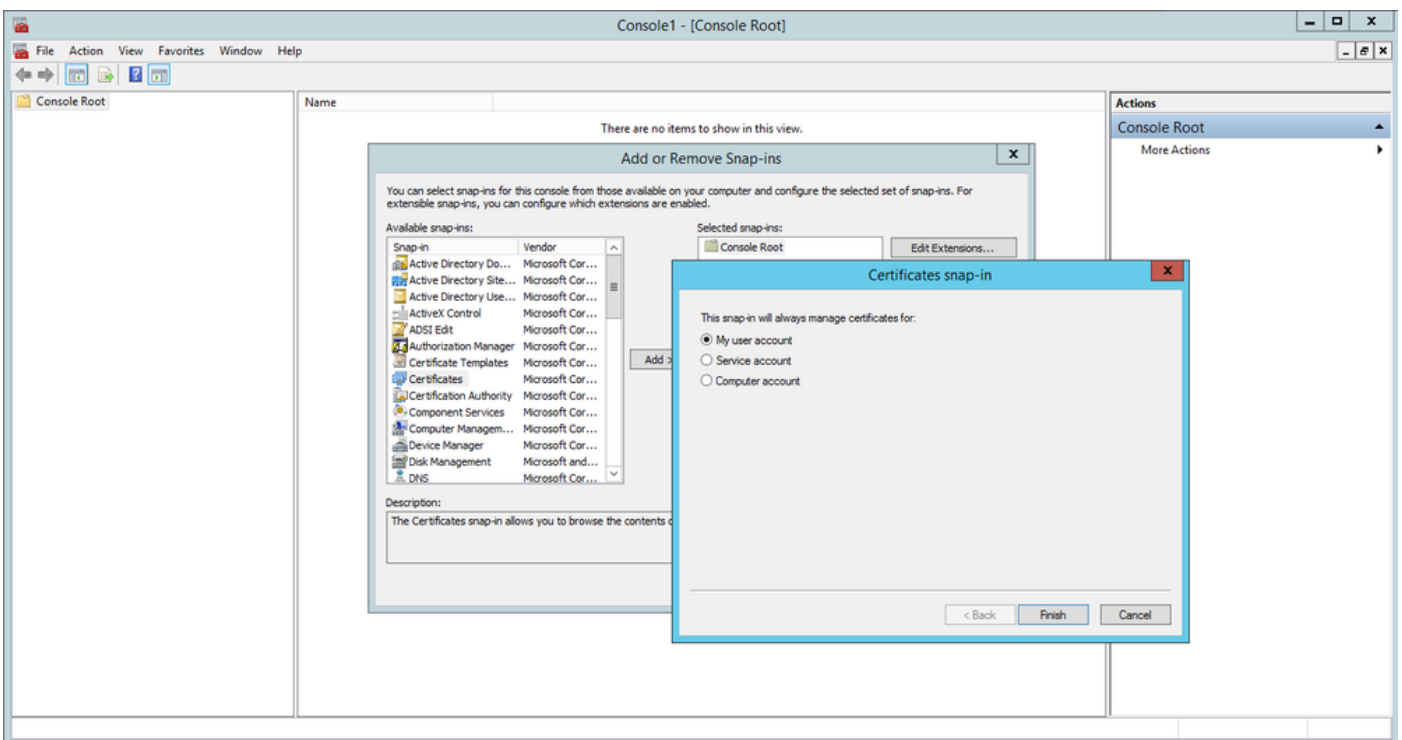


Arrêter puis démarrer les services de certificats

S'inscrire au certificat d'agent d'inscription

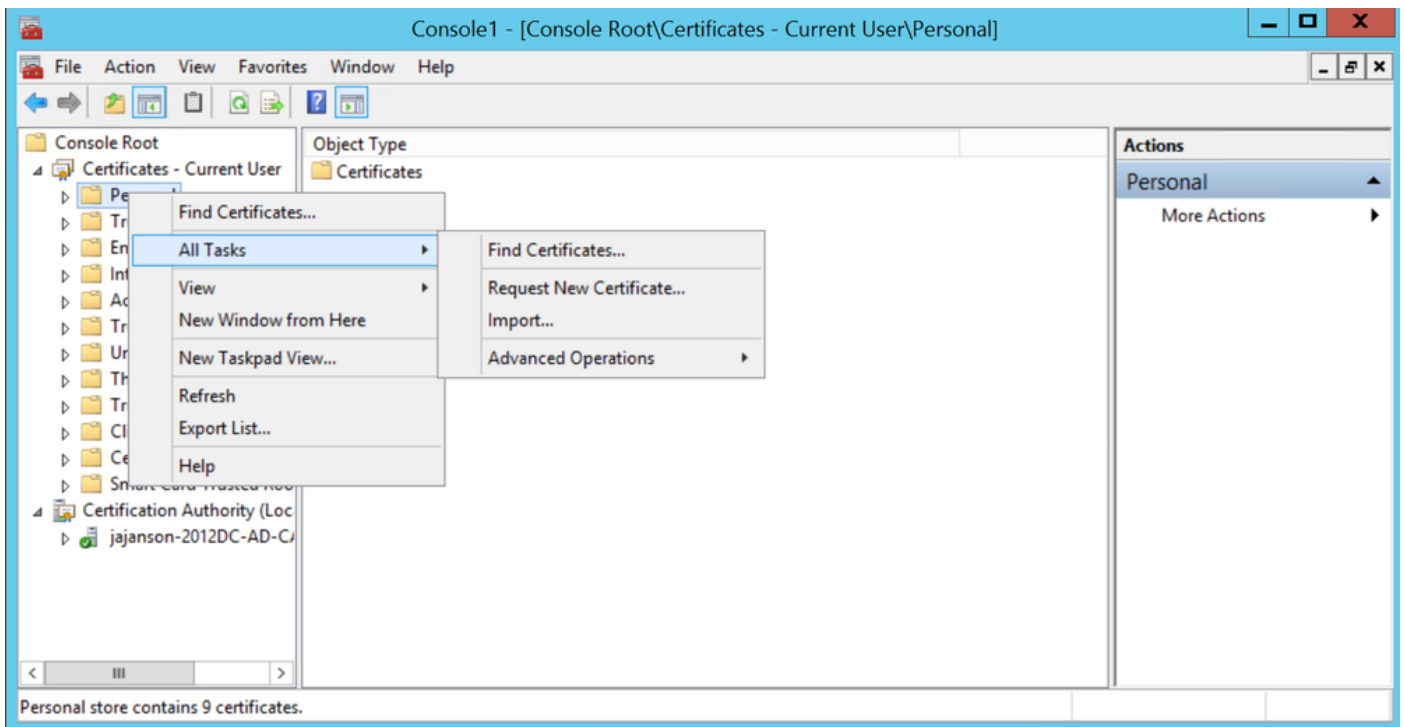
Il est recommandé d'effectuer cette opération sur un ordinateur client (bureau des administrateurs informatiques).

1. Lancer MMC choisissez **Certificates**, cliquez sur **Ajouter** puis certificats pour **Mon compte d'utilisateur**.



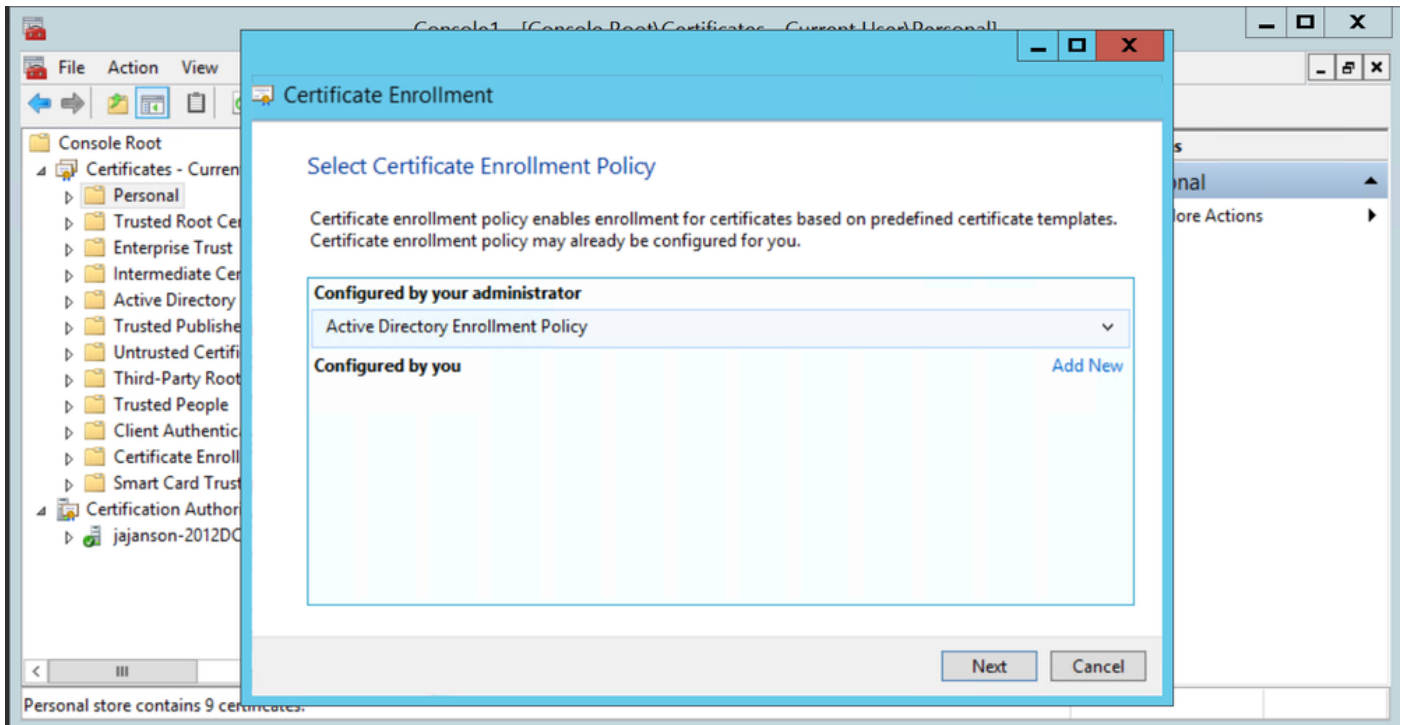
Ajouter des certificats

2. Cliquez avec le bouton droit de la souris ou sélectionnez le **noeud personnel**, sélectionnez **Toutes les tâches**, puis sélectionnez **Demander un nouveau certificat**.



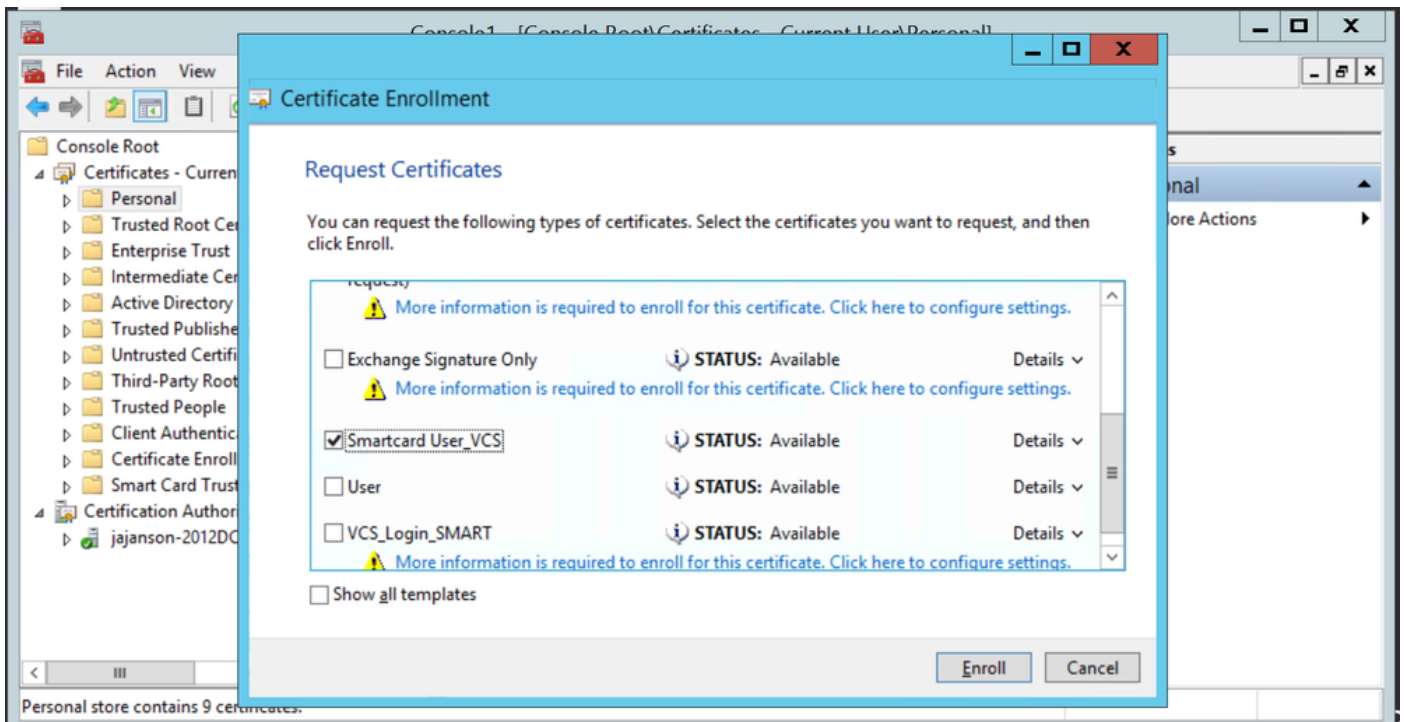
Demander de nouveaux certificats

3. Cliquez sur **Suivant** dans l'Assistant, puis sélectionnez **Stratégie d'inscription Active Directory**. Cliquez ensuite de nouveau sur **Suivant**.



Inscription à Active Directory

4. Sélectionnez le **certificat d'agent d'inscription**, dans ce cas, **Smartcard User_VCS** puis cliquez sur **S'inscrire**.

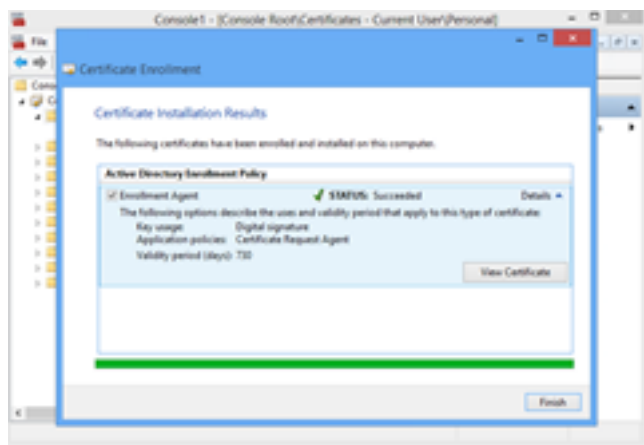


Agent de certificat d'inscription

Votre bureau Administrateurs IT est maintenant configuré en tant que poste d'inscription, ce qui vous permet d'inscrire de nouvelles cartes à puce au nom d'autres utilisateurs.

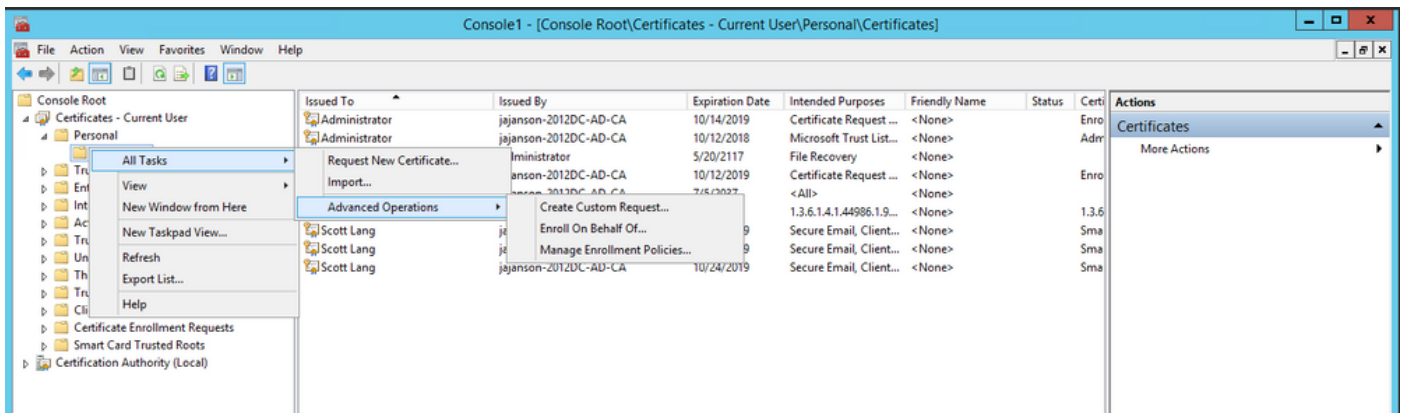
S'inscrire au nom de...

Pour que vous puissiez maintenant fournir aux employés des cartes à puce pour l'authentification, vous devez les inscrire et générer le certificat qui est ensuite importé sur la carte à puce.

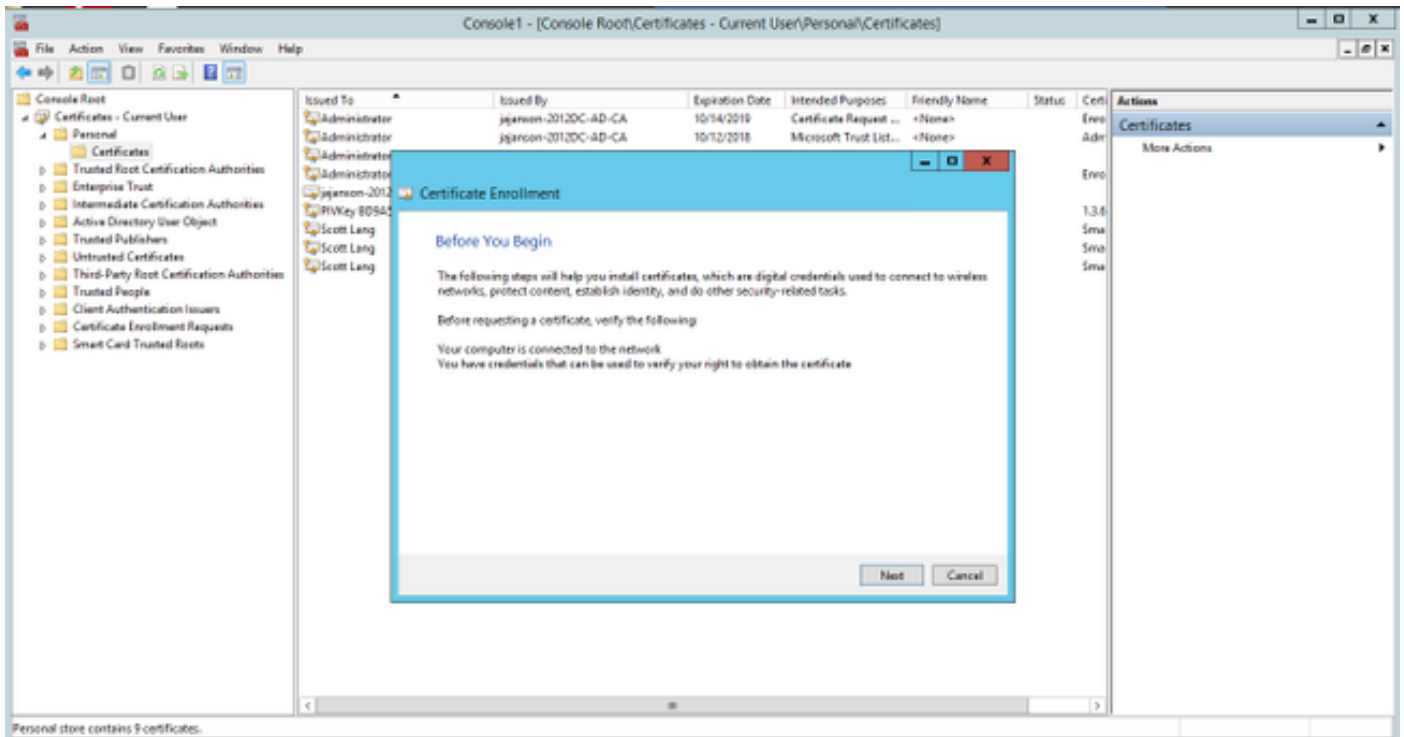


S'inscrire au nom de

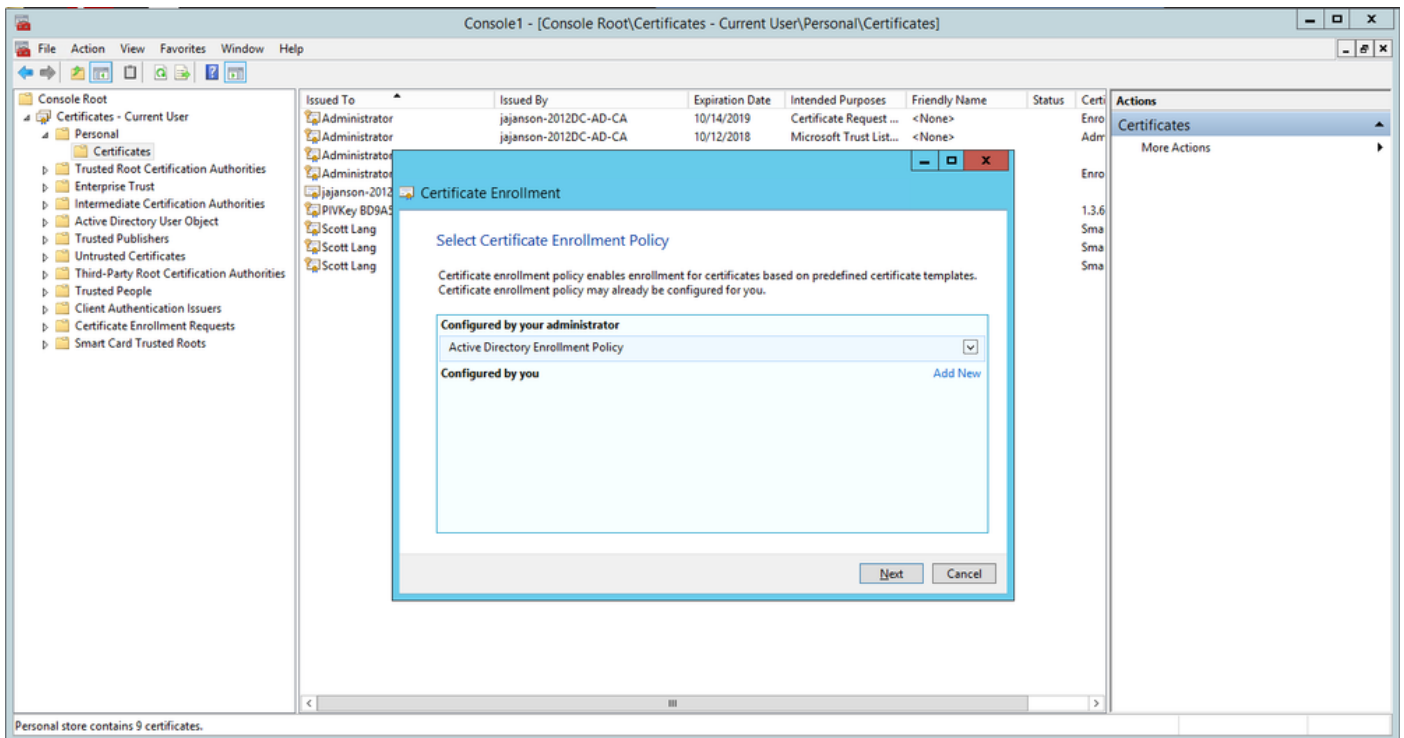
1. Lancez MMC et importez le **module Certificats et gérez** les certificats de mon compte d'utilisateur.
2. Cliquez avec le bouton droit de la souris ou sélectionnez **Personnel > Certificats** et sélectionnez **Toutes les tâches > Opérations avancées** et cliquez sur **S'inscrire au nom de...**
3. Dans l'Assistant, sélectionnez la stratégie d'inscription Active Directory, puis cliquez sur **Suivant**.



S'inscrire au nom avancé

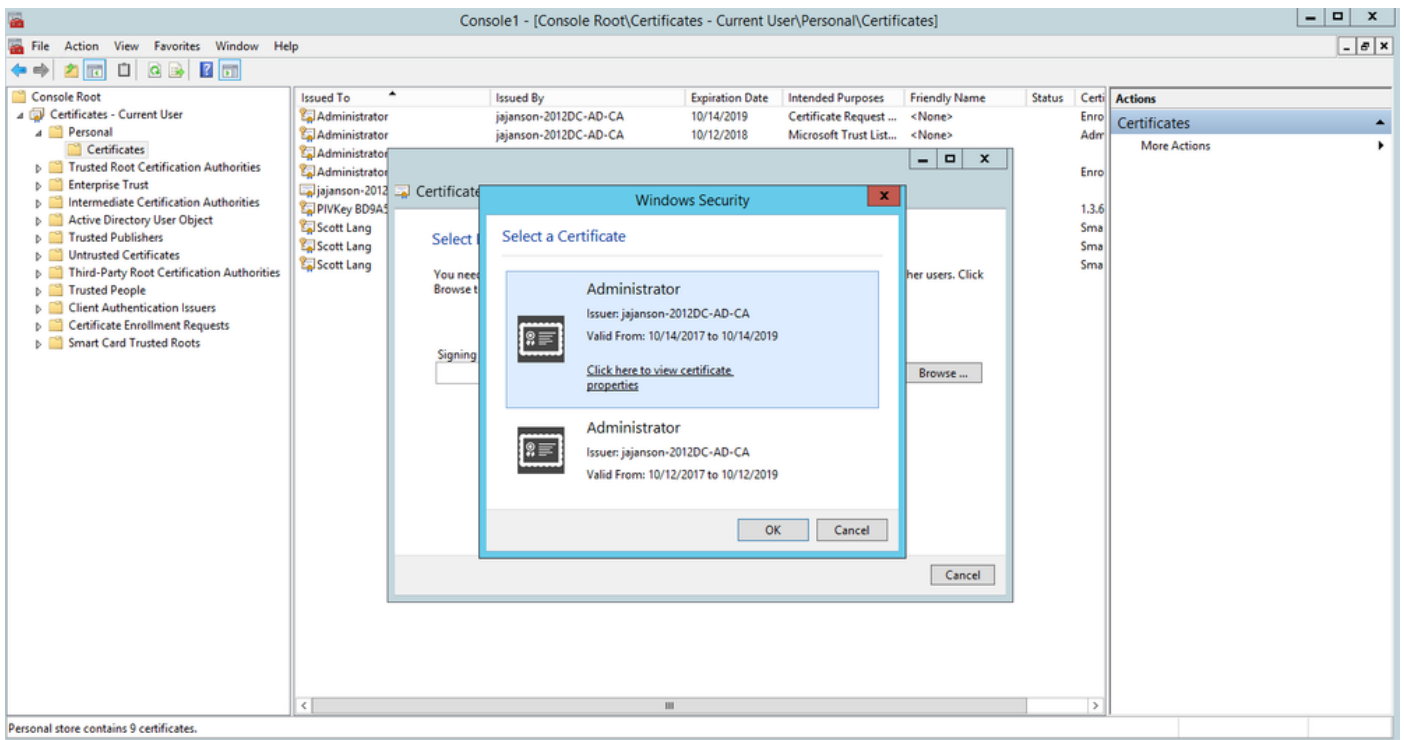


4. Sélectionnez Stratégie d'inscription de certificat, puis cliquez sur **Suivant**.



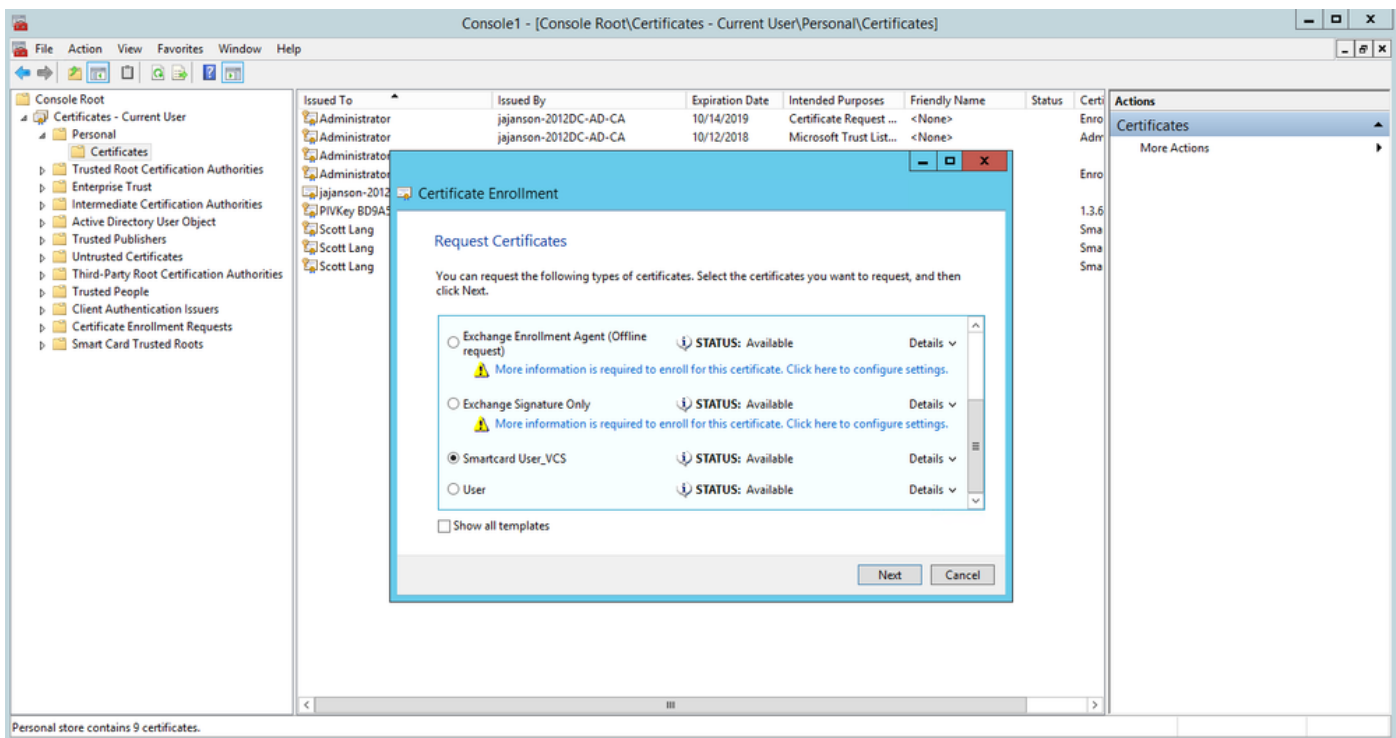
Stratégie d'inscription

5. Vous êtes maintenant invité à sélectionner le **certificat de signature**. Il s'agit du certificat d'inscription que vous avez demandé précédemment.



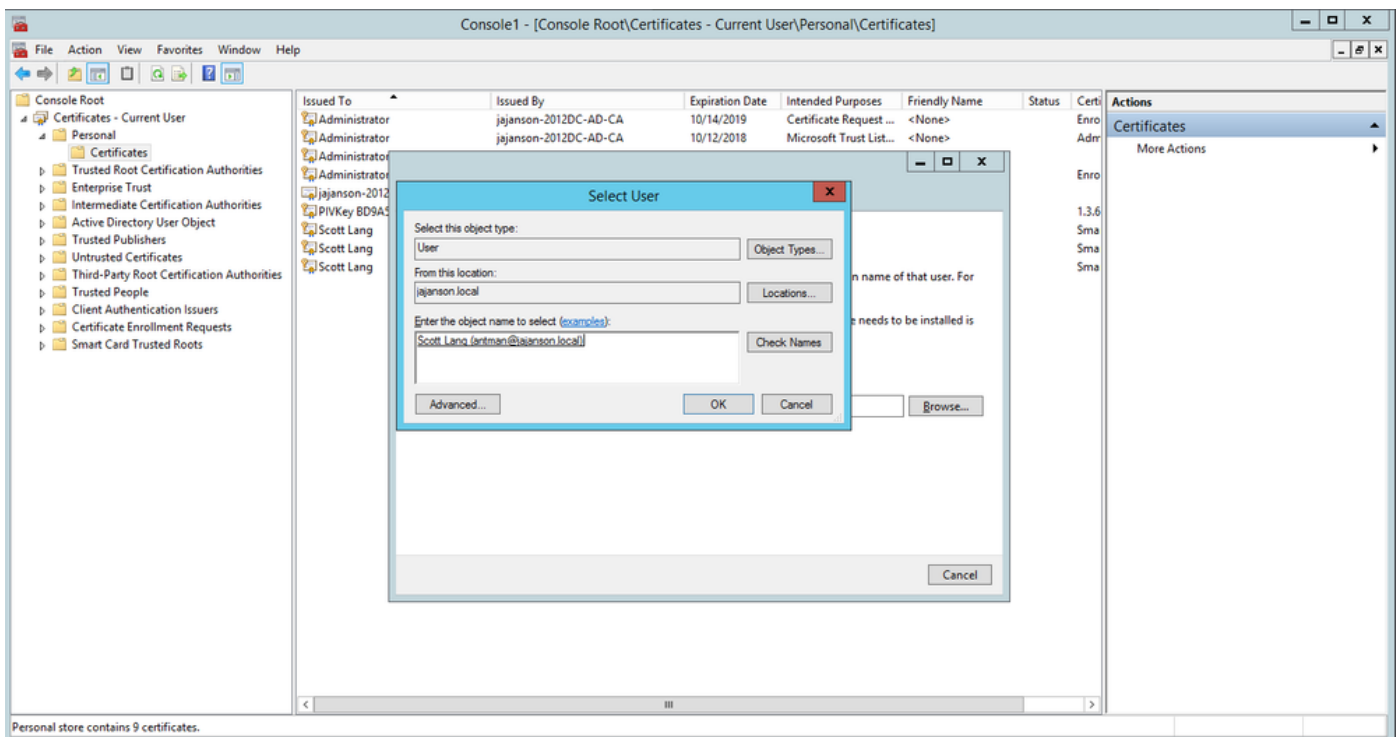
Sélectionner un certificat de signature

6. Dans l'écran suivant, vous devez accéder au certificat que vous souhaitez demander et dans ce cas, c'est **Smartcard User_VCS** qui est le modèle que vous avez créé précédemment.



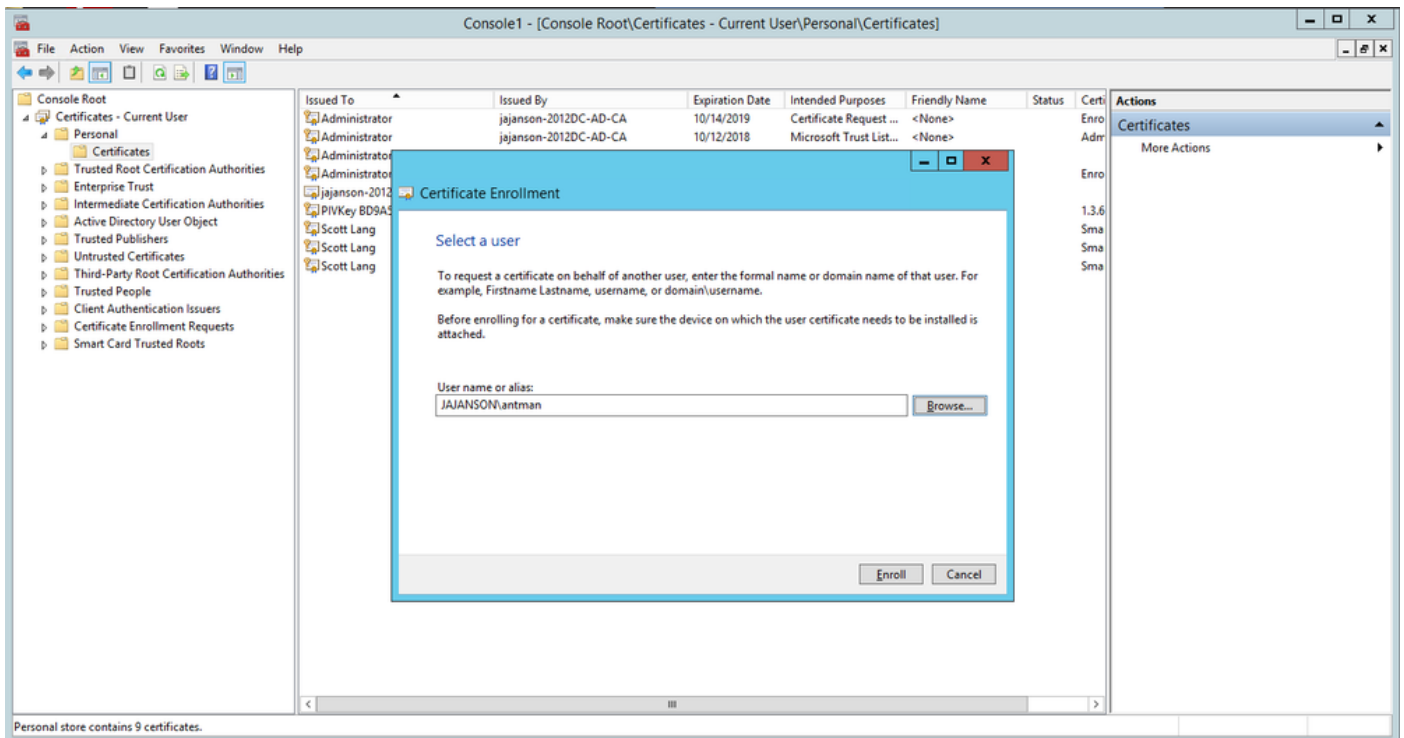
Choisir la carte à puce VCS

7. Ensuite, vous devez sélectionner l'utilisateur auquel vous souhaitez vous inscrire pour le compte de. Cliquez sur **Parcourir** et saisissez le nom d'utilisateur de l'employé que vous souhaitez inscrire. Dans ce cas, Scott Lang 'antman@jajanson.local account' est utilisé.



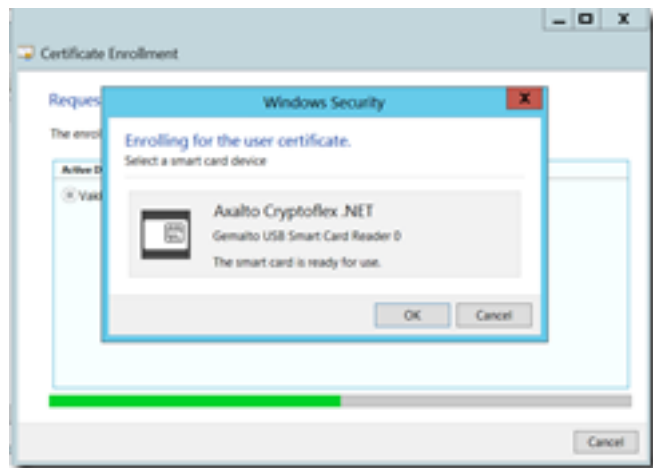
Choisir l'utilisateur

8. Dans l'écran suivant, poursuivez l'inscription en cliquant sur **Inscription**. Maintenant, insérez une carte à puce dans votre lecteur.



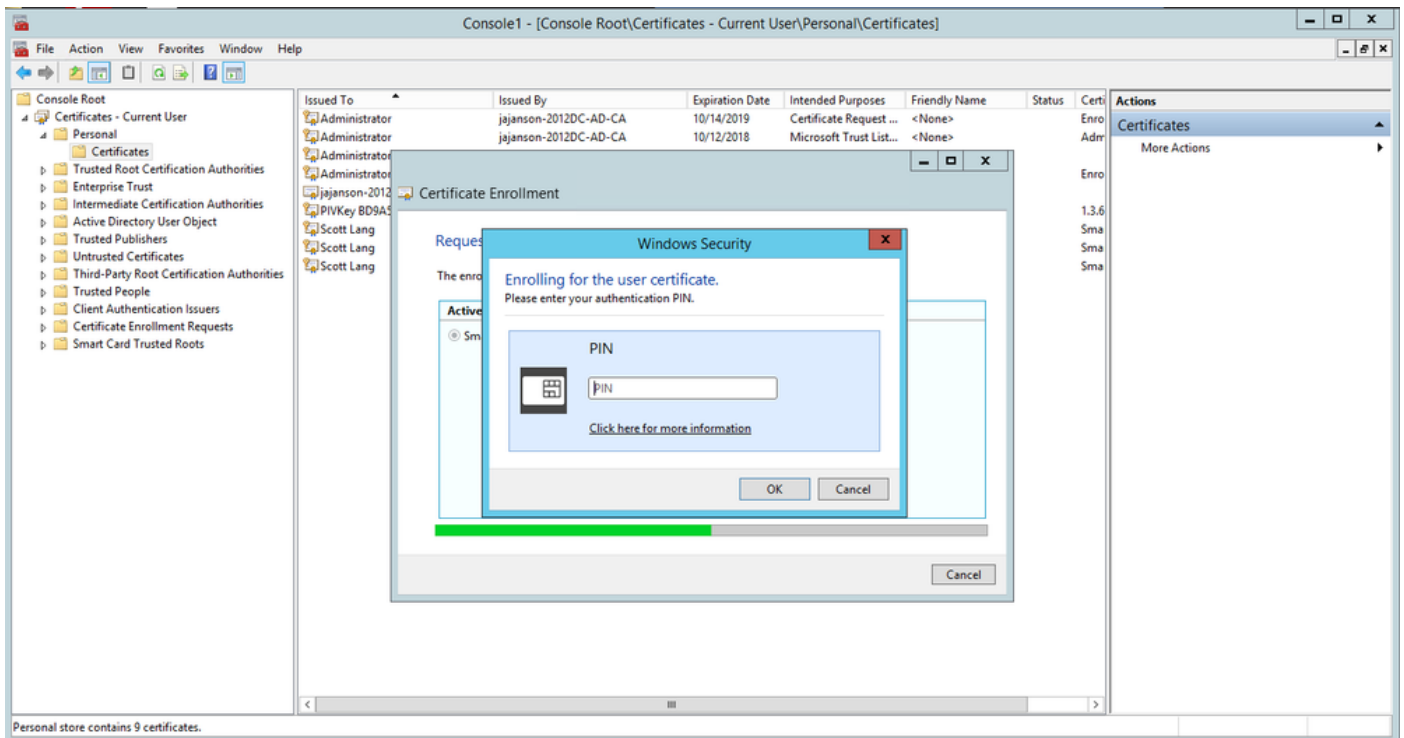
Inscire

9. Une fois que vous avez inséré votre carte à puce, elle est détectée comme suit :



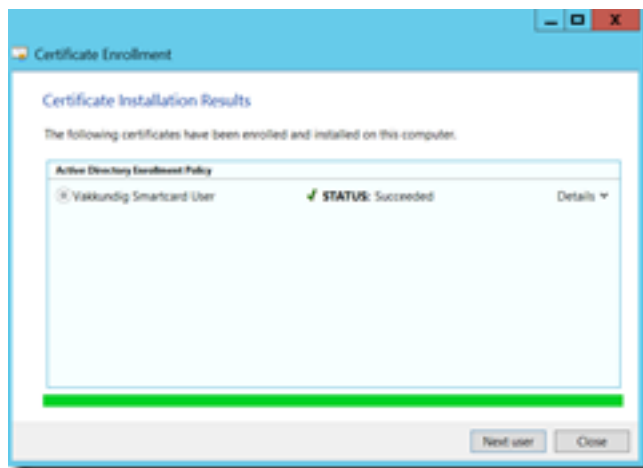
Insérer la carte à puce

10. Il vous est ensuite demandé de saisir un code PIN de carte à puce (code PIN par défaut : 0000).



Entrez la broche

11. Enfin, une fois que vous avez vu l'écran **Inscription réussie**, vous pouvez utiliser cette carte à puce pour vous connecter à un serveur joint au domaine, comme le serveur VCS avec seulement la carte et une broche connue. Cependant, il n'est pas fait oui, vous devez toujours préparer le VCS pour rediriger les demandes d'authentification vers la carte à puce et utiliser la carte d'accès commune pour libérer le certificat de carte à puce stocké sur la carte à puce pour l'authentification.



Inscription réussie

Configuration de VCS pour la carte d'accès commune

Téléchargez l'autorité de certification racine dans la liste des certificats de l'autorité de certification de confiance dans le VCS en accédant à **Maintenance > Security > Trusted CA Certificate**.

2. Téléchargez la liste de révocation de certificats signée par l'autorité de certification racine dans le VCS. Accédez à **Maintenance > Security > CRL Management**.

3. Testez votre certificat client par rapport à votre regex qui extrait le nom d'utilisateur du certificat à utiliser pour l'authentification contre l'utilisateur LDAP ou local. Le regex va correspondre avec l'**Objet** du certificat. Il peut s'agir de votre UPN, de votre e-mail, etc. Au cours de ces travaux pratiques, l'e-mail à comparer au certificat client pour le certificat client a été utilisé.

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

Objet du certificat client

4. Accédez à **Maintenance > Security > Client Certificate Testing**. Sélectionnez le certificat client à tester, dans Mon laboratoire c'était antman.pem, téléchargez-le dans la zone de test. Dans la section **Modèle d'authentification basé sur les certificats** sous **Regex pour correspondre au certificat** collez votre regex à tester. Ne modifiez pas le champ **Format du nom d'utilisateur**.

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 the 'Certificate source' section, 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.

Testez votre regex dans 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}*"@bjpenson.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:
            240000000170f460b3102511a4651370000000000017
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=Antman,OU=DOE,OU=CA,OU=BJPenson,DC=local
        Validity
            Not Before: Oct 17 21:39:55 2017 GMT
            Not After: Oct 17 21:39:55 2017 GMT
        Subject: emailAddress=antman@bjpenson.local,CN=Scott Lmc,OU=DOE,OU=BJPenson,DC=local
        Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
            009f46d09f5a12815a1517b46810246b1131d0771
            0c19a1081041374210917516d12d0f11391d91c041
            616510d1f81761081c16d12410f4010a1f51451
            681fc1081081f017a13112710a1410811711d11f1f01
            9112101f016110c10d10f10a115c14210413610f1
            a014a1121718810d1041601081f21f71413610c10c1
            0410510a181671610f10f10512010d10b10b1711a1
            c413217714813614210410c13c10a1051f01671891201
    -----END CERTIFICATE-----

```


← 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.

Résultats des tests


5. Si le test vous fournit les résultats souhaités, vous pouvez cliquer sur le bouton **Rendez ces modifications permanentes**. Cela modifie votre rég pour la **configuration de l'authentification basée sur les certificats** du serveur. Afin de vérifier la modification, accédez à cette configuration, **Maintenance > Security > Certificate-based authentication configuration**.


6. Activez l'authentification basée sur le client en naviguant vers **System > Administrator** puis cliquez sur ou sélectionnez une zone déroulante pour sélectionner **Client certificate-based security = Client-Based Authentication**. Avec ce paramètre, l'utilisateur tape le nom de domaine complet du serveur VCS dans son navigateur et il est invité à choisir son compte client et à saisir la broche attribuée à sa carte d'accès commune. Le certificat est ensuite libéré et il est renvoyé à l'interface utilisateur graphique Web du serveur VCS et tout ce qu'il doit faire est de cliquer ou sélectionner le bouton **Administrateur**. Puis il est admis dans le serveur. Si les options **Sécurité basée sur le certificat du client = Validation basée sur le client** sont sélectionnées, le processus est le même, sauf lorsque l'utilisateur clique sur le bouton **Administrateur**, il a demandé à nouveau le mot de passe administrateur. Habituellement, ce dernier n'est pas ce que l'organisation essaie d'accomplir avec CVC.


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](#)

Activer l'authentification basée sur le client

Aide ! Je suis enfermé !!!

Si vous activez l'authentification basée sur le client et que le VCS rejette le certificat pour une raison quelconque, vous ne pourrez plus vous connecter à l'interface utilisateur graphique Web de manière traditionnelle. Mais ne vous inquiétez pas, il y a un moyen de revenir dans votre système. Le document ci-joint se trouve sur le site Web de Cisco et fournit des informations sur la façon de désactiver l'authentification basée sur le client à partir de l'accès racine.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.