VCS configureren met CAC en een slimme kaartlezer

Inhoud

Inleiding

Dit document beschrijft een stap-voor-stap gids voor het installeren en gebruiken van een Smart Card Reader- en Common Access Card-logbestand voor gebruik met de Cisco Video Communication Server (VCS) voor organisaties die twee-factor verificatie nodig hebben in de VCS-omgeving, zoals banken, ziekenhuizen of overheden met beveiligde faciliteiten.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Express Administrator (X14.0.2).

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Het CAC voorziet in de vereiste authenticatie zodat "systemen" weten wie toegang heeft gekregen tot hun omgeving en welk deel van de infrastructuur fysiek of elektronisch is. Binnen de overheid overheersen de regels van 'minst bevoorrechte toegang' of 'noodzaak om te weten'. Een logbestand kan door iedereen worden gebruikt, voor de authenticatie is iets nodig dat de gebruiker heeft, de CAC, ook wel bekend als de Gemeenschappelijke Toegangskaart, in 2006 is opgericht, zodat het individu niet meer meerdere apparaten hoeft te hebben, of het nu banen,

identiteitskaarten of dongles zijn, om toegang te krijgen tot zijn werk of systemen.

Wat is een slimme kaart?

Smart-kaarten zijn een belangrijk onderdeel van de PKI-infrastructuur (Public Key Infrastructure) die Microsoft gebruikt om in het Windows-platform te integreren omdat slimme kaarten alleen-software-oplossingen verbeteren, zoals clientverificatie, aanmelding en beveiligde e-mail. Smart cards zijn een convergentiepunt voor publieke basiscertificaten en bijbehorende sleutels, omdat ze:

- Aanbieden van manipulatiebestendige opslag voor de bescherming van privé-sleutels en andere vormen van persoonlijke informatie.
- Isoleer veiligheidskritische berekeningen, die authenticatie, digitale handtekeningen en belangrijke uitwisseling omvatten van andere delen van het systeem die het niet hoeven te weten.
- Overdraagbaarheid van geloofsbrieven en andere privé informatie tussen computers op het werk, thuis of op de weg mogelijk maken.

De smartcard is een integraal onderdeel van het Windows-platform geworden omdat smartcards nieuwe en wenselijke functies bieden die revolutionair zijn voor de computersector als de invoering van de muis of CD-ROM. Als u op dit moment geen interne PKI-infrastructuur hebt, moet u er zeker van zijn dat u dit eerst doet. Dit document heeft geen betrekking op de installatie van deze rol in dit specifieke artikel, maar informatie over de manier waarop deze ten uitvoer moet worden gelegd, is hier te vinden: http://technet.microsoft.com/en-us/library/hh831740.aspx.

Configureren

Dit lab gaat ervan uit dat u reeds LDAP met VCS hebt geïntegreerd en gebruikers heeft die kunnen inloggen met LDAP-referenties.

1. Lab-apparatuur
2. Installeer de slimme kaart
3. Modellen van certificeringsinstanties configureren
4. Voer het certificaat van inrolagent in
5. Inschrijven namens ...
6. Configureer de VCS voor gemeenschappelijke toegangskaart

Vereiste apparatuur:

Windows 2012R2 Domain server die deze rollen/geïnstalleerde software heeft:

- certificaatinstantie
- Actieve map
- DNS
- Windows PC met slimme kaart aangesloten
- vSEC: CMS K-Series beheersoftware voor het beheer van uw slimme kaart:

Software voor Versa Card Reader

Installeer de slimme kaart

Smart Card-lezers krijgen in het algemeen instructies over hoe u de benodigde kabels kunt aansluiten. Hier is een voorbeeld van installatie voor deze configuratie.

Een stuurprogramma voor een slimme kaart installeren

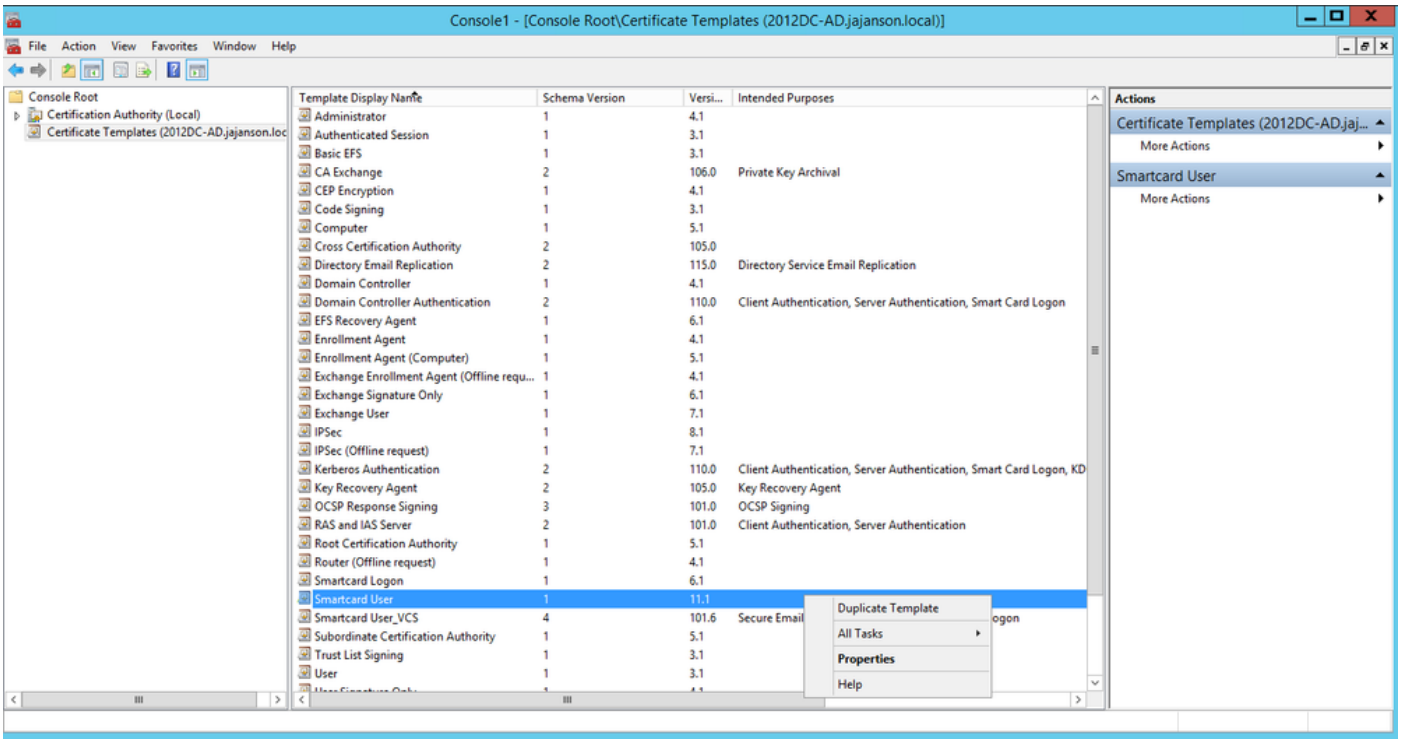
Als de slimme kaartlezer is gedetecteerd en geïnstalleerd, erkent het Welcome to Windows openingsscherm dit. Zo niet:

1. Sluit uw slimme kaart aan op de USB-poort op uw Windows-pc
2. Volg de aanwijzingen op het scherm voor het installeren van de software van het stuurprogramma. Hiervoor zijn de driver-media nodig die de fabrikant van de smartcard of het stuurprogramma in Windows wordt ontdekt. In mijn geval gebruikte ik de fabriekschauffeur van hun downloadsite. **VERTROUWT GEEN WINDOWS**.
3. Klik met de rechtermuisknop op het pictogram **Mijn computer** op uw bureaublad en klik op **Bewerken** in het submenu.

4. Vul het knooppunt **Services en toepassingen uit** en klik op **Services**.
5. Klik in het rechter venster met de rechtermuisknop op **Smart Card**. Klik op **Eigenschappen** in het submenu.
6. Selecteer in het **tabblad Algemeen de optie Automatisch** in de vervolgkeuzelijst Opstarttype. Klik op **OK**.
7. Reinig de machine als de wizard de hardware u vraagt dit te doen.

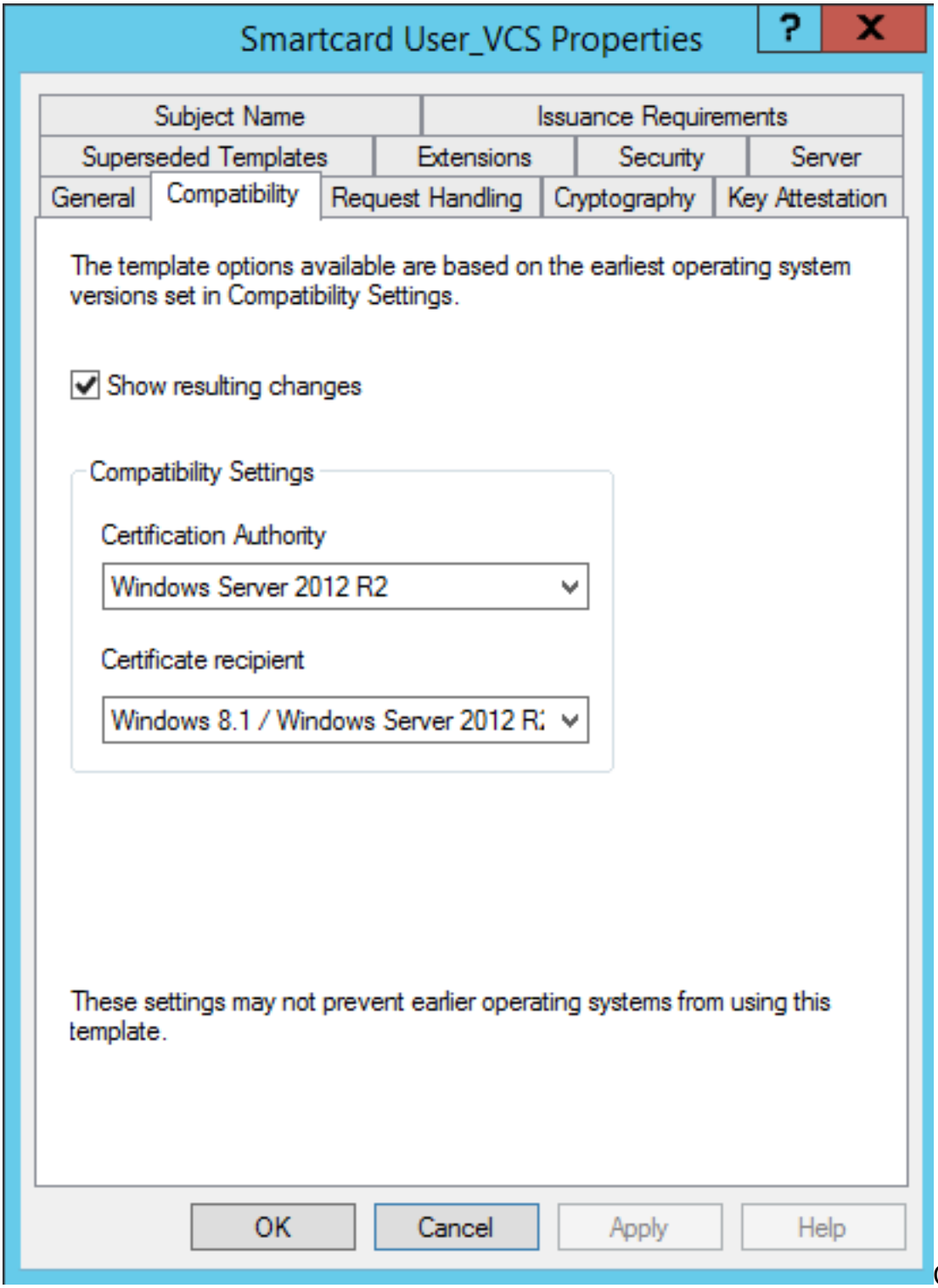
Modellen van certificeringsinstanties configureren

1. Start MGC van de certificaatinstantie.
2. Klik op of selecteer het knooppunt **certificaatsjablonen** en selecteer **Beheer**.
3. Klik met de rechtermuisknop op of selecteer de sjabloon **Smartcard-**gebruikerscertificaat en selecteer vervolgens **Dubbelklik** zoals in de afbeelding.



Domain Control-certificaatsjablonen

4. Controleer op het tabblad **Compatibiliteit** onder **certificeringsinstantie** de selectie en wijzig deze indien nodig.

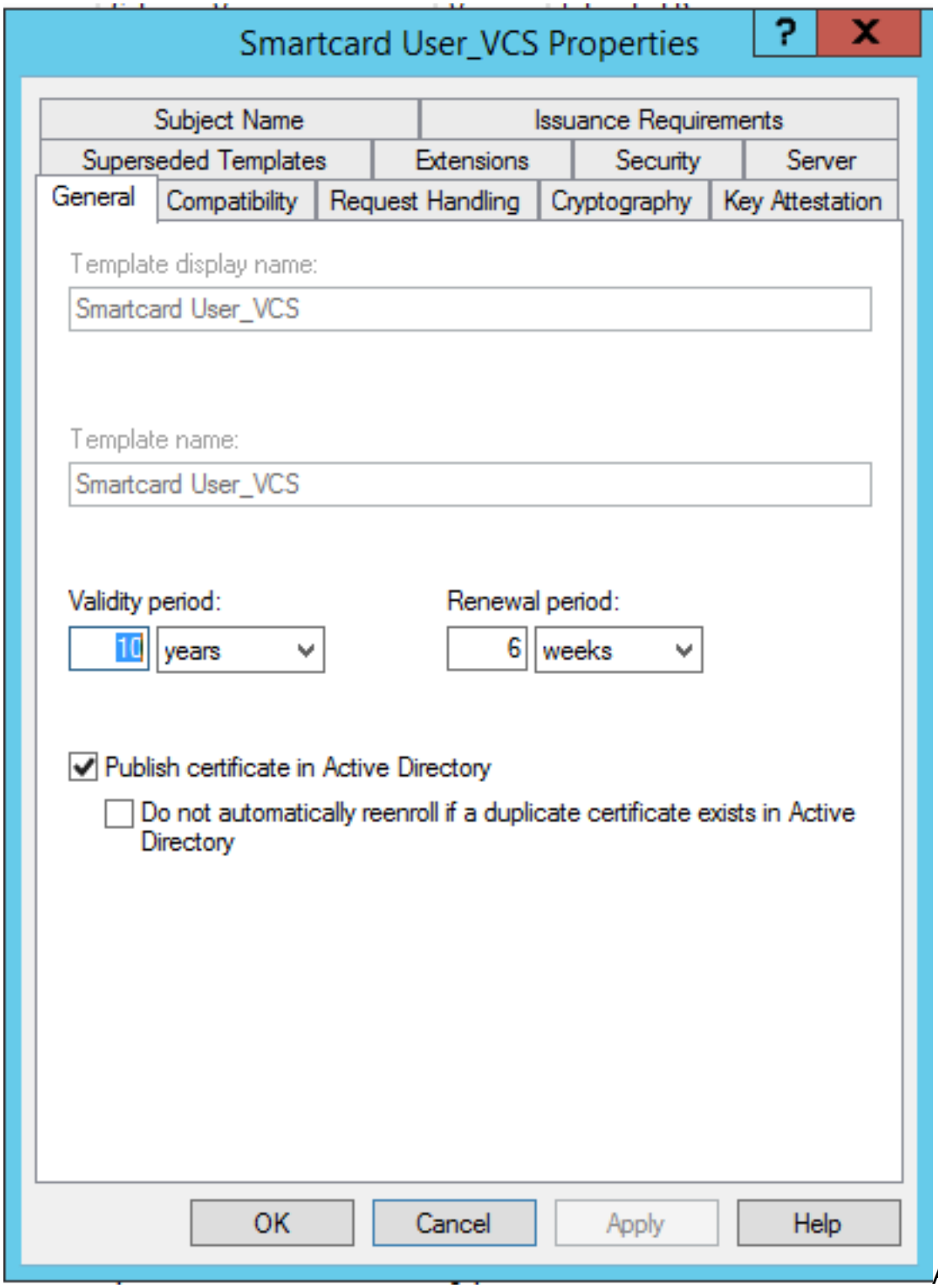


Compatibiliteitsinstellingen voor slimme kaart

5. Op het tabblad **Algemeen**:

a. Specificeer een naam, zoals **Smartcard User_VCS**.

b. Stel de geldigheidsperiode in op de gewenste waarde. Klik op **Apply** (Toepassen).

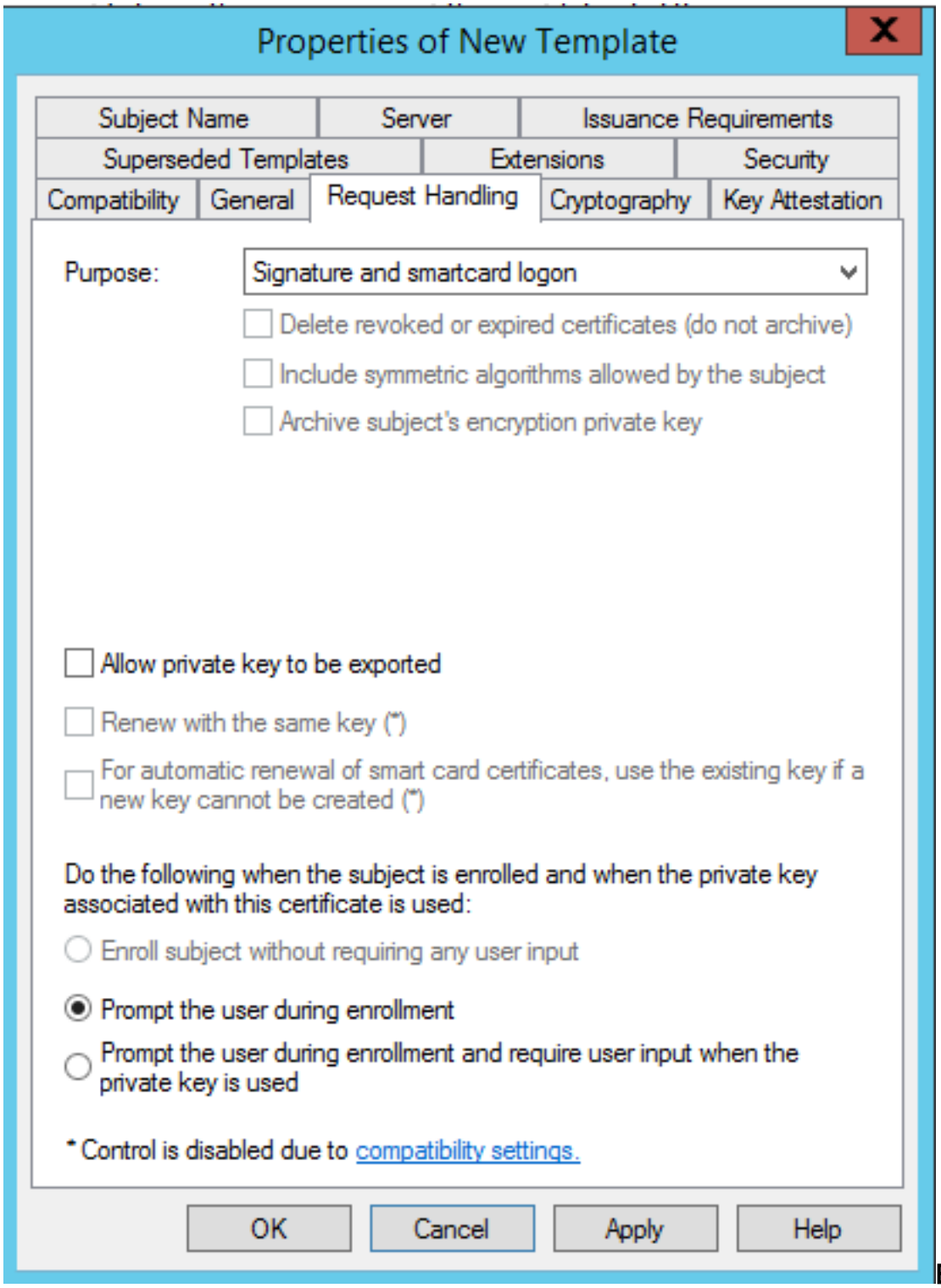


Algemene tijd slimme kaart beginnen te verlopen

6. Op het tabblad **Aanvragen**:

a. Stel het **doel in** op **Signature- en smartcard-aanmelding**.

b. Klik **tijdens de inschrijving op De gebruiker vragen.** Klik op **Apply** (Toepassen).

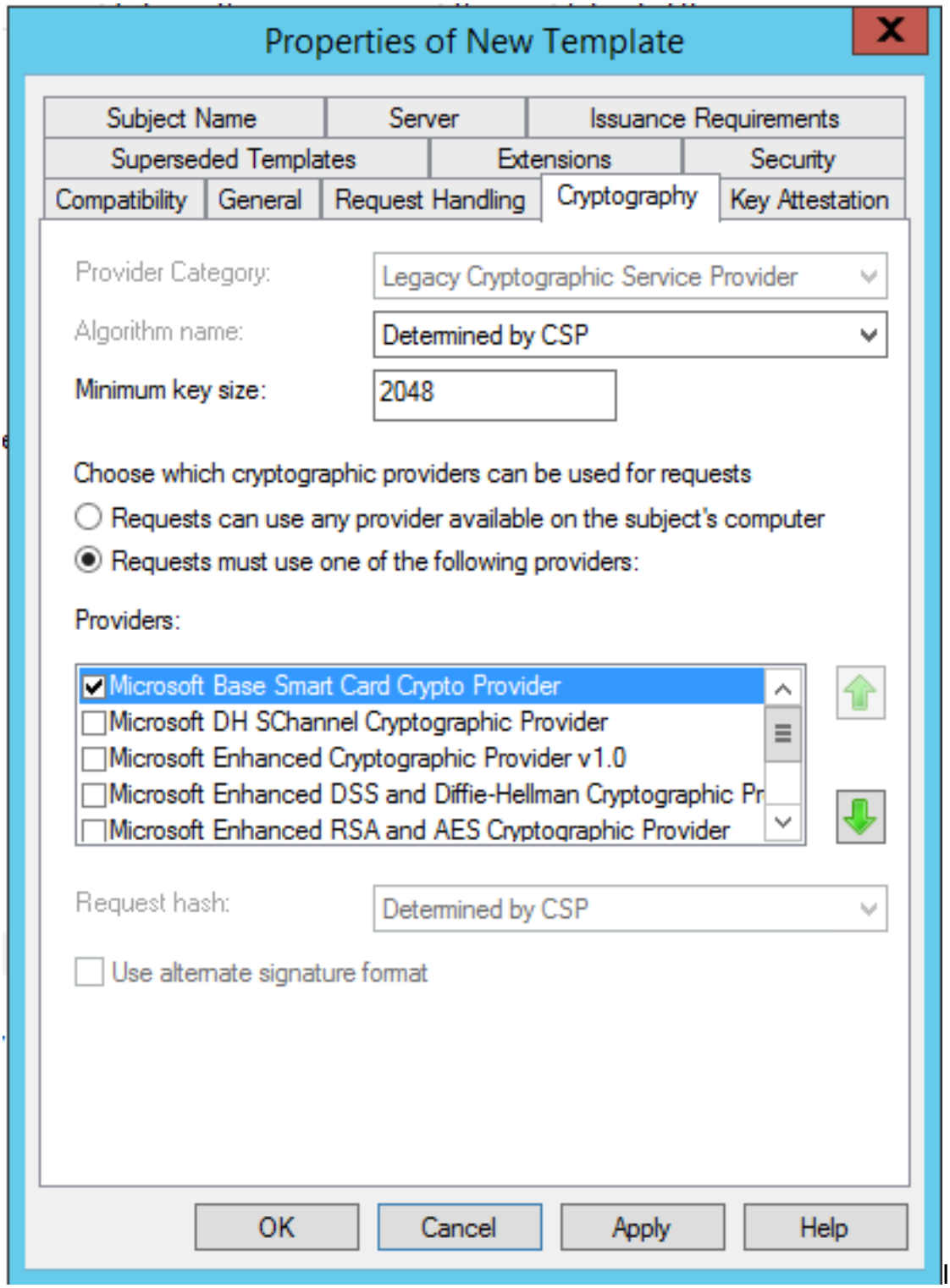


Behandeling van slimme kaartaanvraag

7. Stel in het tabblad **Cryptografie** de minimale sleutelgrootte in op 2048.

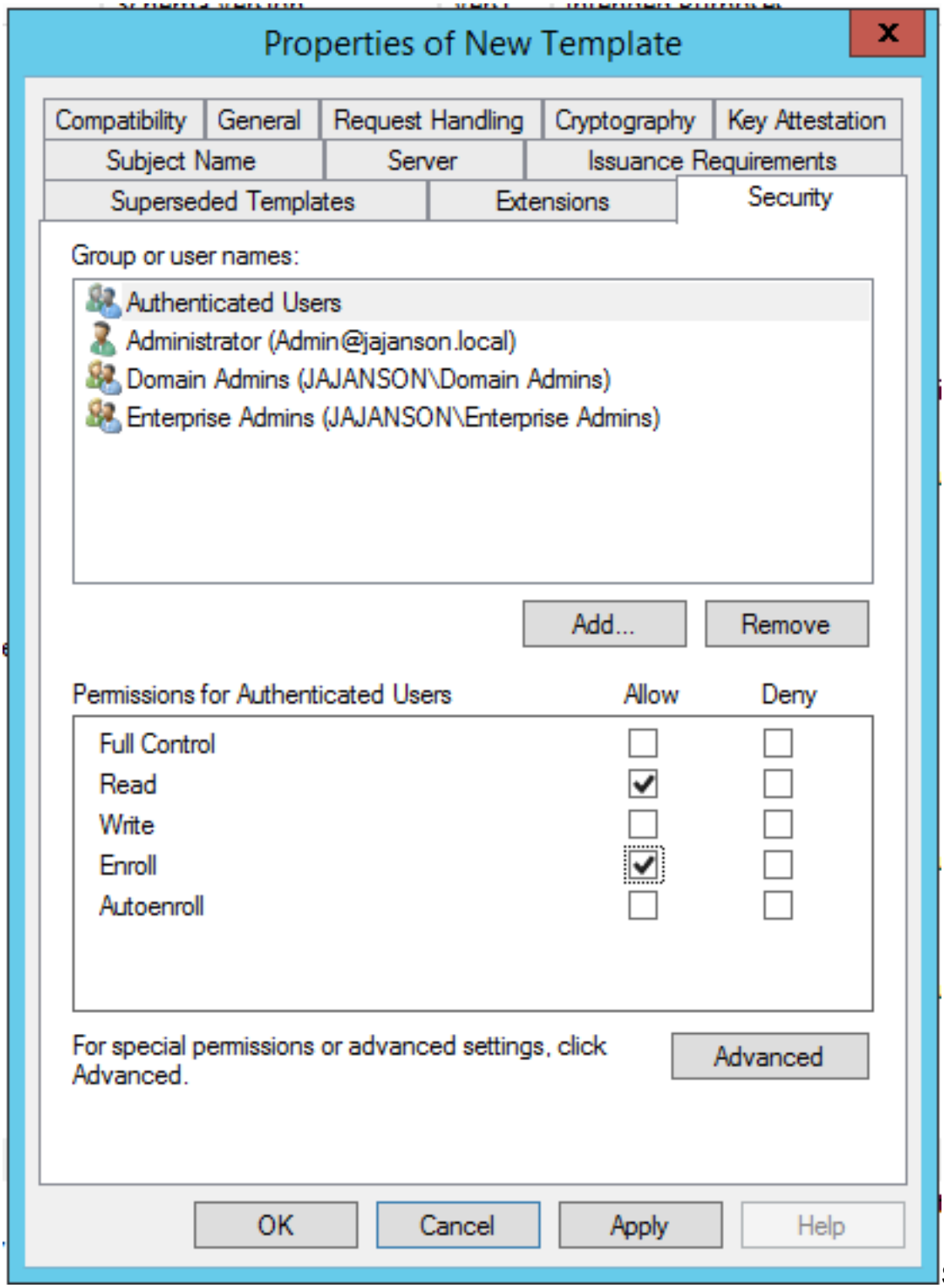
a. Klik op **Verzoeken om een van de volgende leveranciers te gebruiken**, en selecteer vervolgens **Microsoft Base Smart Card Crypto Provider**.

b. Klik op **Toepassen**.



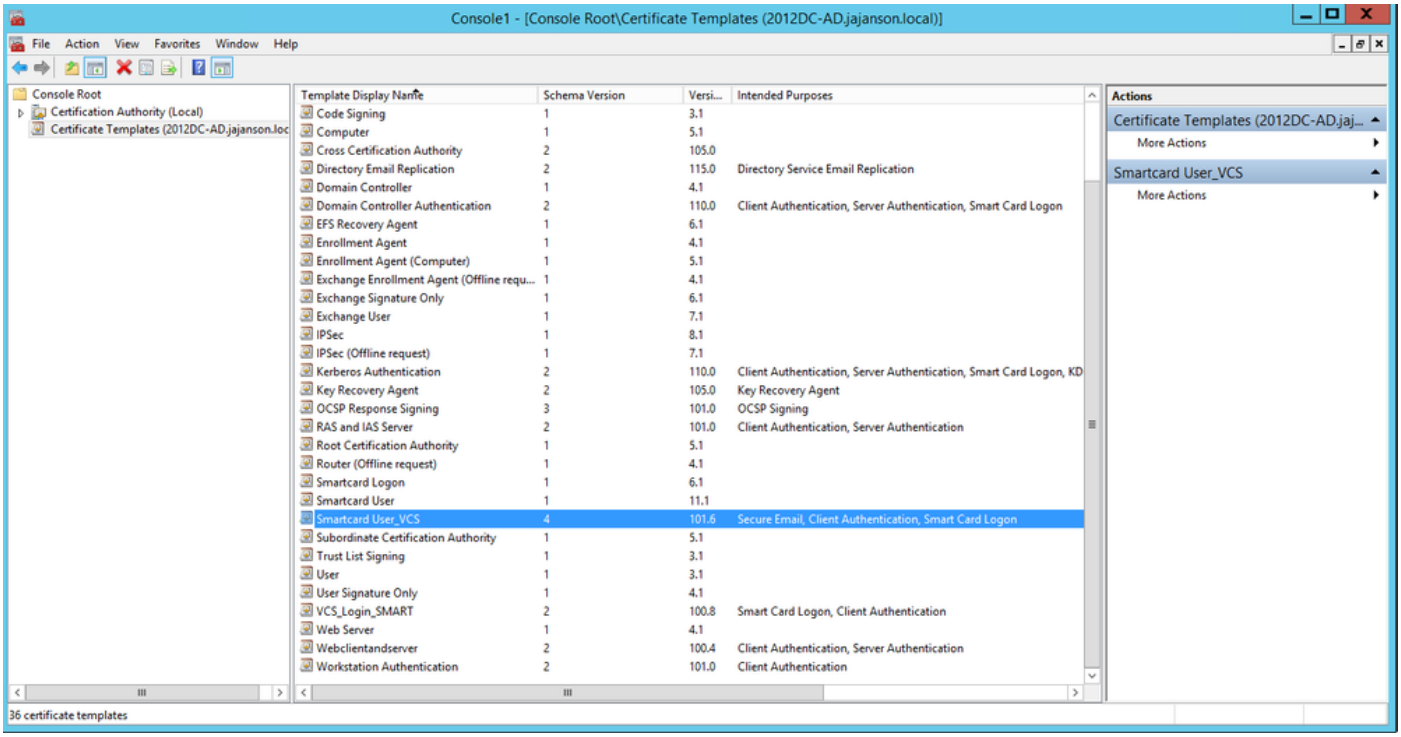
Instellingen voor certificaatversleuteling

8. Voeg in het tabblad Beveiliging de beveiligingsgroep toe waartoe u toegang tot de inschrijving wilt geven. Als u bijvoorbeeld toegang tot alle gebruikers wilt geven, selecteert u de groep Geautomatiseerde gebruikers en vervolgens selecteert u Toegang voor alle gebruikers **invoeren**.



Sjabloonbeveiliging

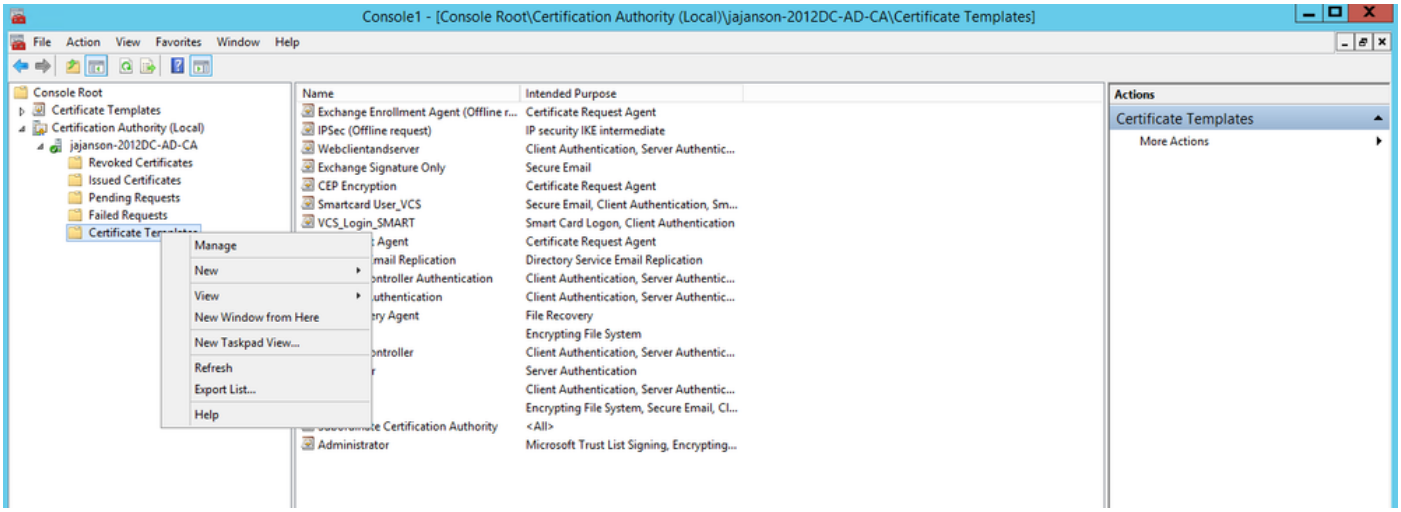
9. Klik op **OK** om de wijzigingen te voltooien en de nieuwe sjabloon te maken. Uw nieuwe sjabloon moet nu in de lijst met certificaatsjablonen verschijnen.



Sjabloon dat in een domeincontrole is weergegeven

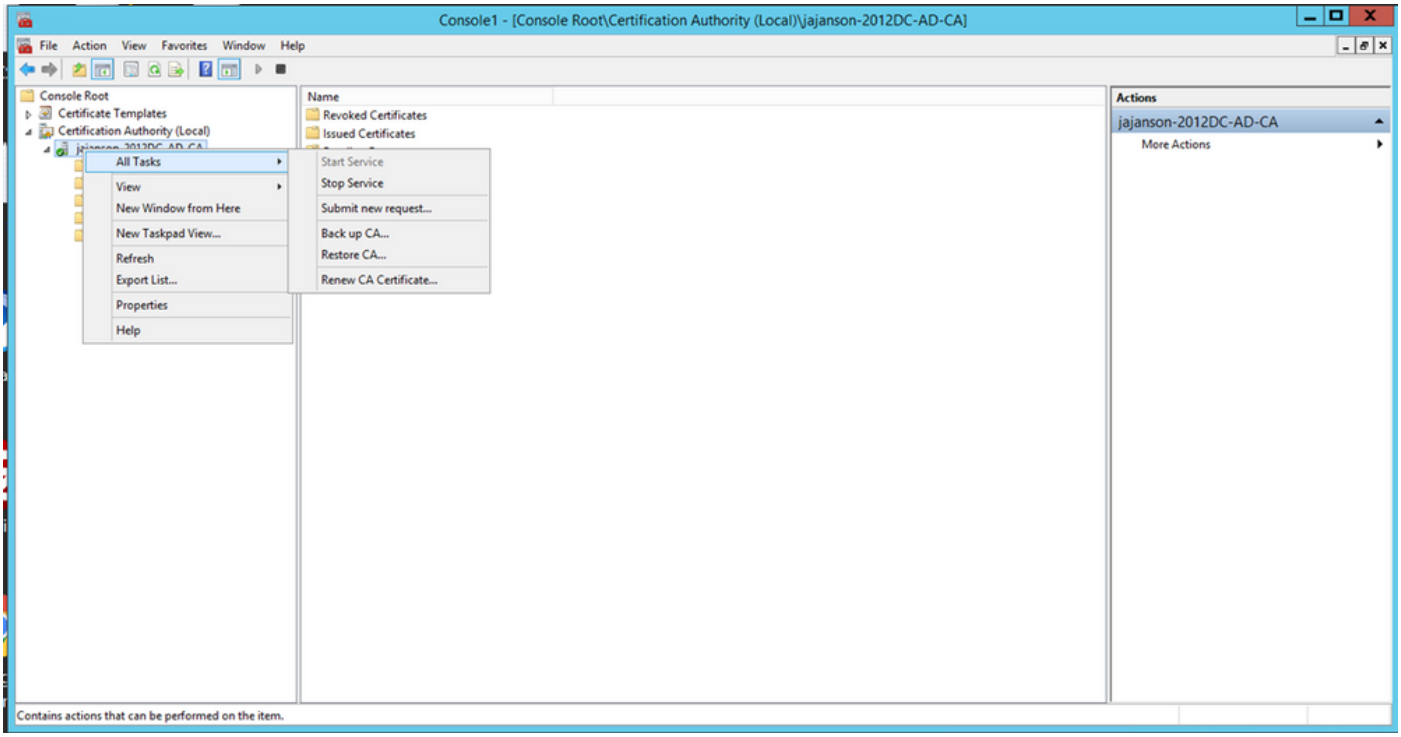
10. In het linker venster van de MMC, breid certificeringsinstantie (Lokaal) uit en breid vervolgens uw CA binnen de lijst van de certificeringsinstantie uit.

Klik met de rechtermuisknop op certificaatsjablonen, klik op **Nieuw** en klik vervolgens op **certificaatsjabloon** voor afgifte. Kies vervolgens de nieuwe Smartcard-sjabloon.



Nieuwe sjabloon uitgeven

1. Nadat de sjabloon zich heeft herhaald, klikt u in de MMC met de rechtermuisknop op of selecteert u de lijst met certificeringsinstanties. Klik vervolgens op **Alle taken** en vervolgens op **Stop Service**. Klik vervolgens met de rechtermuisknop op de naam van de CA opnieuw, klik op **Alle taken** en klik vervolgens op **Start Service**.

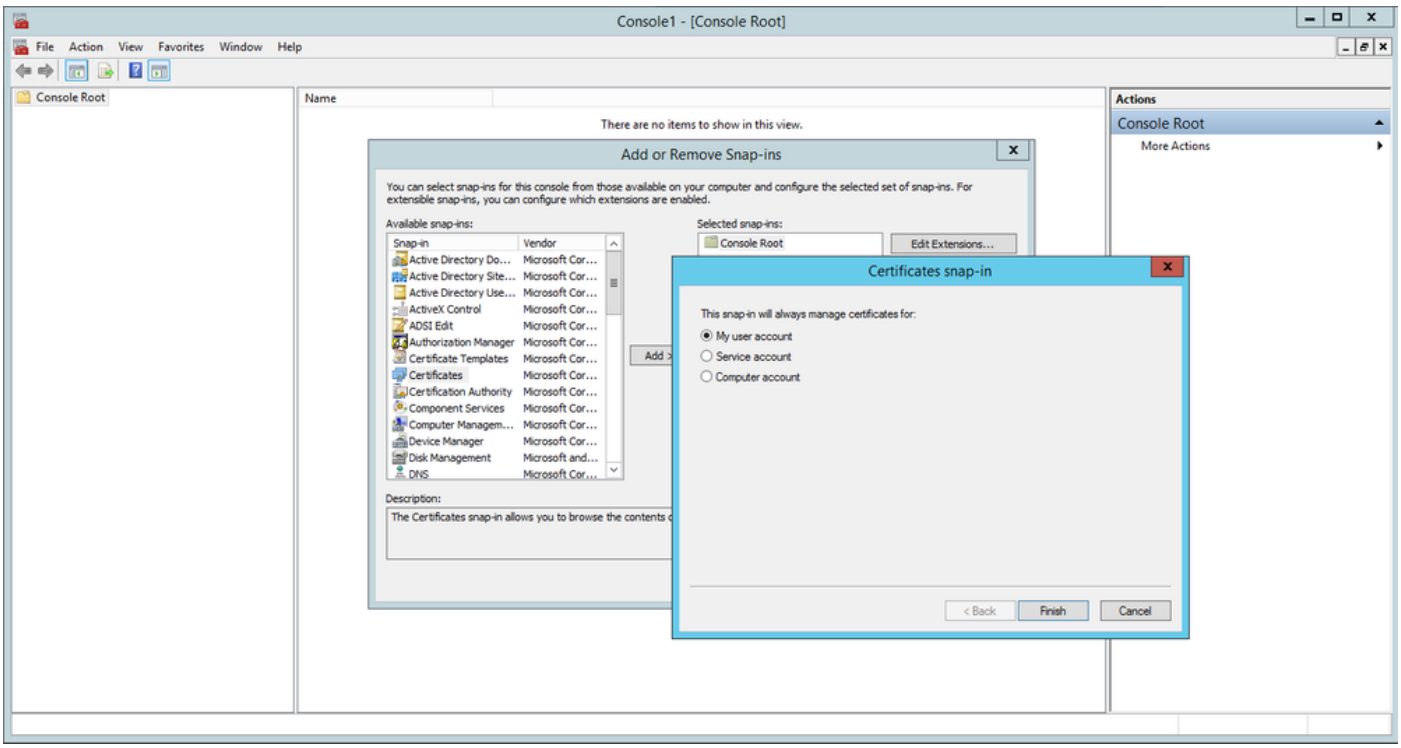


Stop dan met het starten van certificeringsdiensten

Inschrijven op certificaat van inrolagent

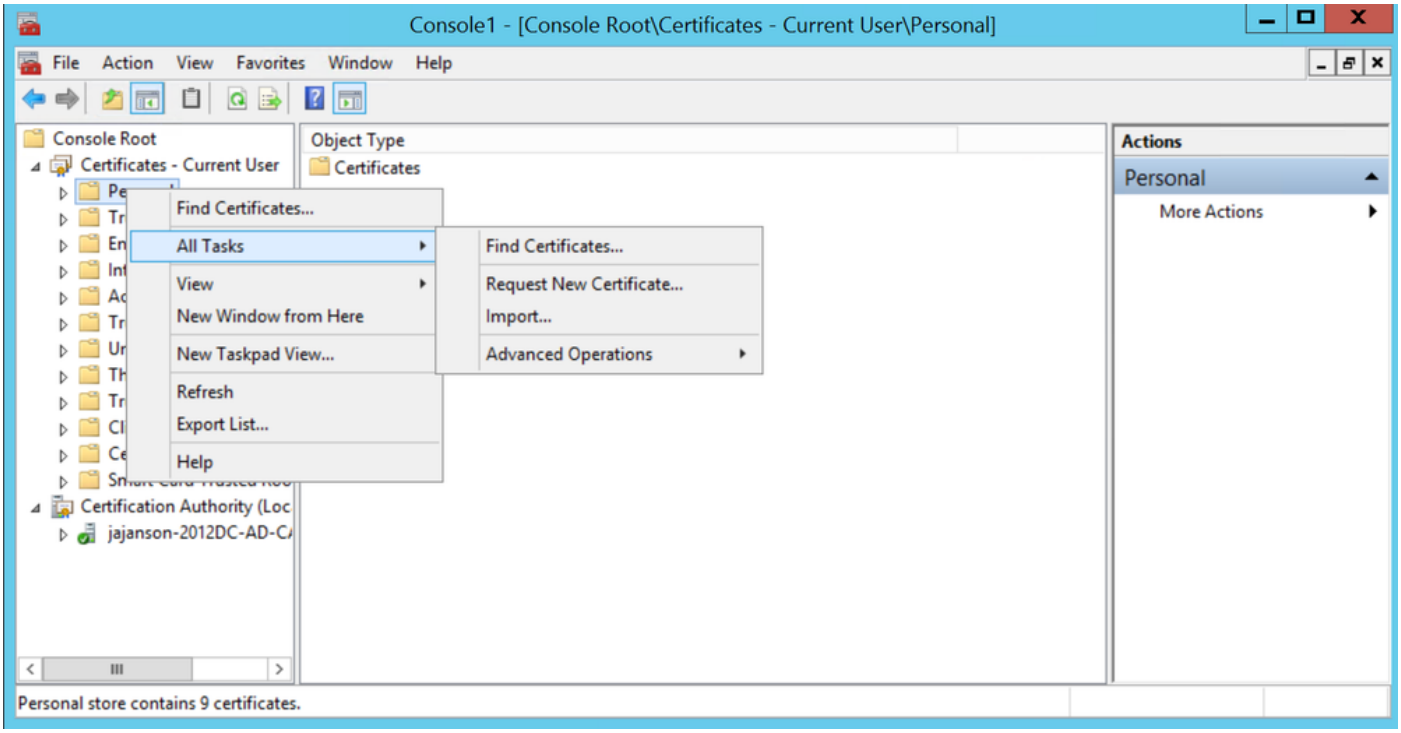
Aanbevolen wordt dit op een clientmachine te doen (IT-beheerders).

1. Start MMC om **Certificaten** te kiezen, klik op **Toevoegen** en vervolgens certificaten voor **mijn gebruikersaccount**.



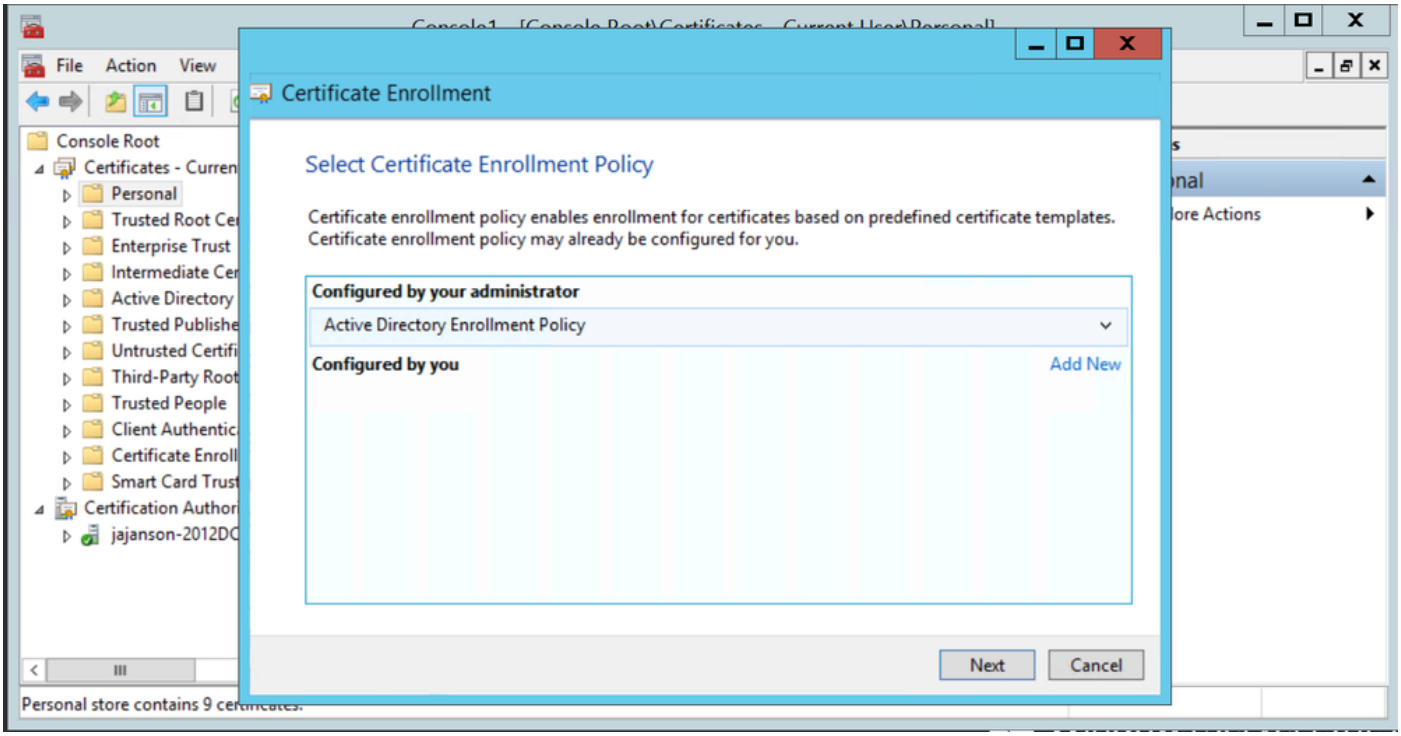
Certificaten toevoegen

2. Klik met de rechtermuisknop op of selecteer het **Persoonlijke knooppunt**, selecteer **Alle taken** en selecteer vervolgens **Nieuw certificaat aanvragen**.



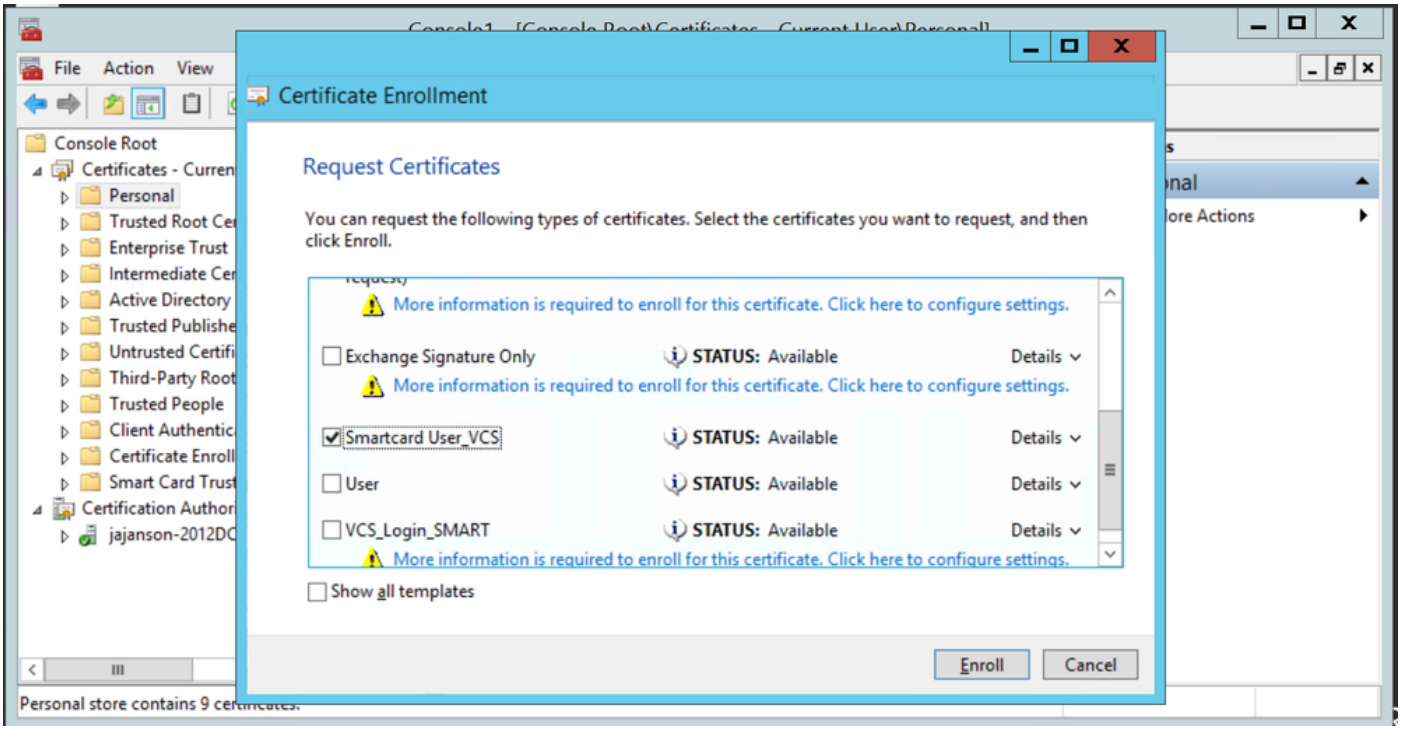
Nieuwe certificaten aanvragen

3. Klik op **Volgende** bij de wizard en selecteer vervolgens **Actief** Invoerbeleid **voor map**. Klik vervolgens nogmaals op **Volgende**.



Actieve map

4. Selecteer het **Certificaat van de Inschrijvingsagent**, in dit geval, **Smartcard User_VCS** en klik vervolgens op **Inschrijven.**

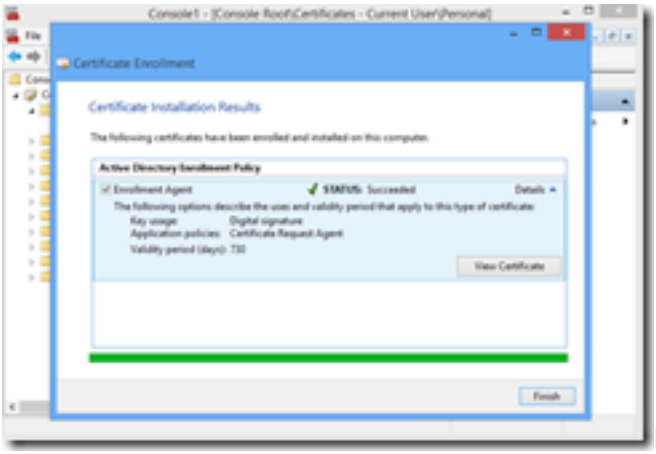


Invoercertificaat Agent

Uw IT-beheerders bureaublad is nu opgezet als een Inschrijvingsstation, waardoor u nieuwe smartcards kunt inschrijven namens andere gebruikers.

Inschrijven namens ...

Als u nu werknemers smartcards voor echtheidscontrole wilt geven, moet u deze inschrijven en het certificaat genereren dat vervolgens op de Smartcard wordt geïmporteerd.

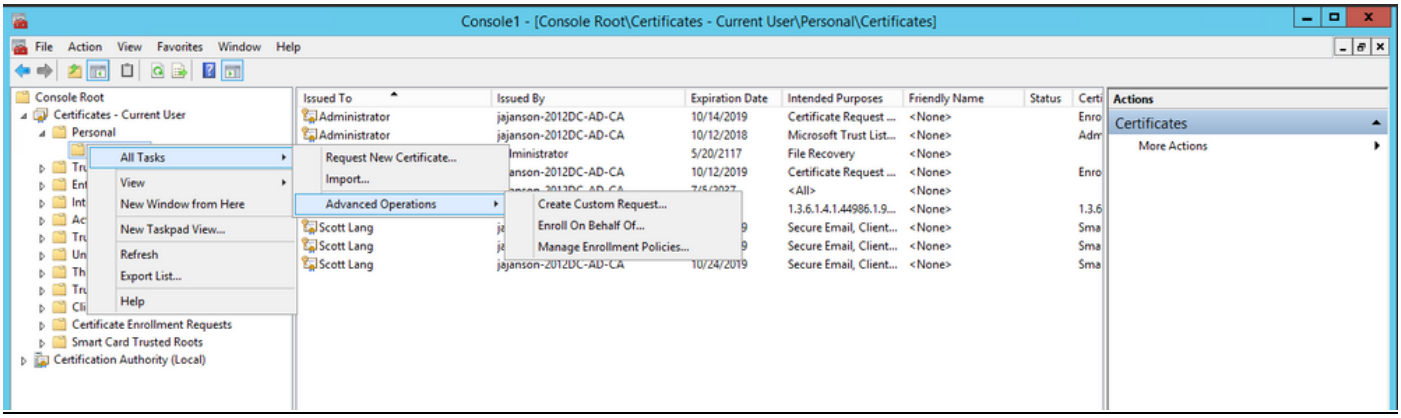


Enroll namens

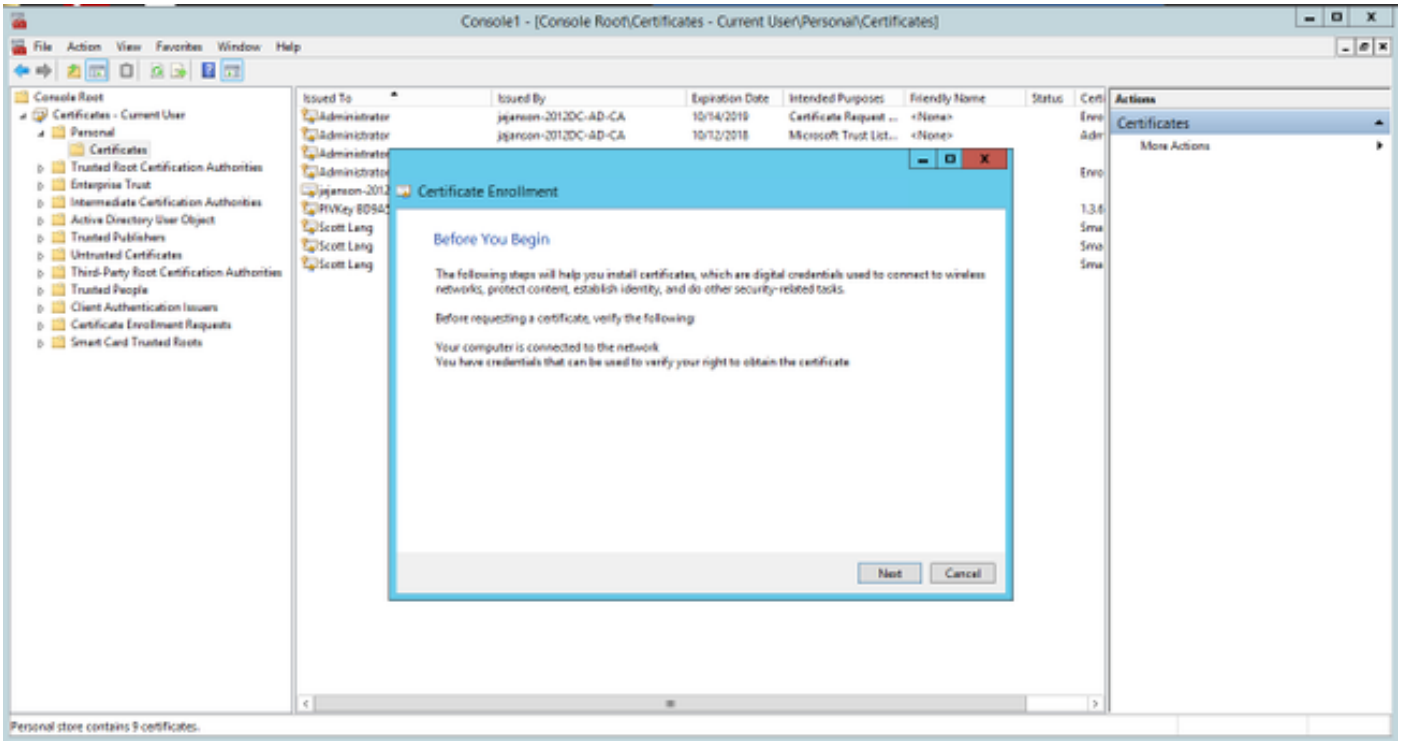
1. Start MMC en voer de **certificaatmodule** uit **en breng** de certificaten voor mijn gebruikersaccount in **gevaar**.

2. Klik met de rechtermuisknop op of selecteer **Persoonlijk > Certificaten** en selecteer **Alle taken > Geavanceerde bewerkingen** en klik **op Inschrijven namens...**

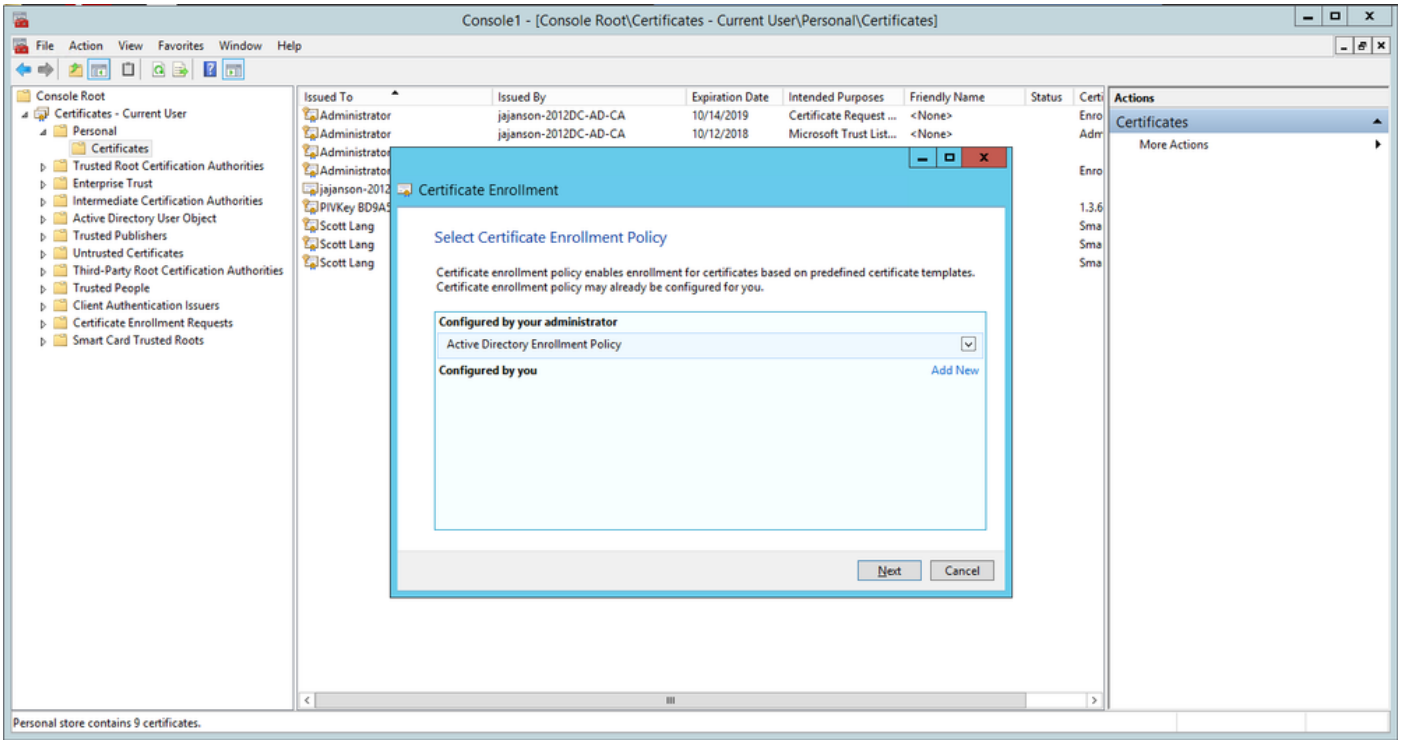
3. Klik in de wizard op **Volgende** en kies het beleid voor actieve inschrijving van de map.



Inrol voor geavanceerde

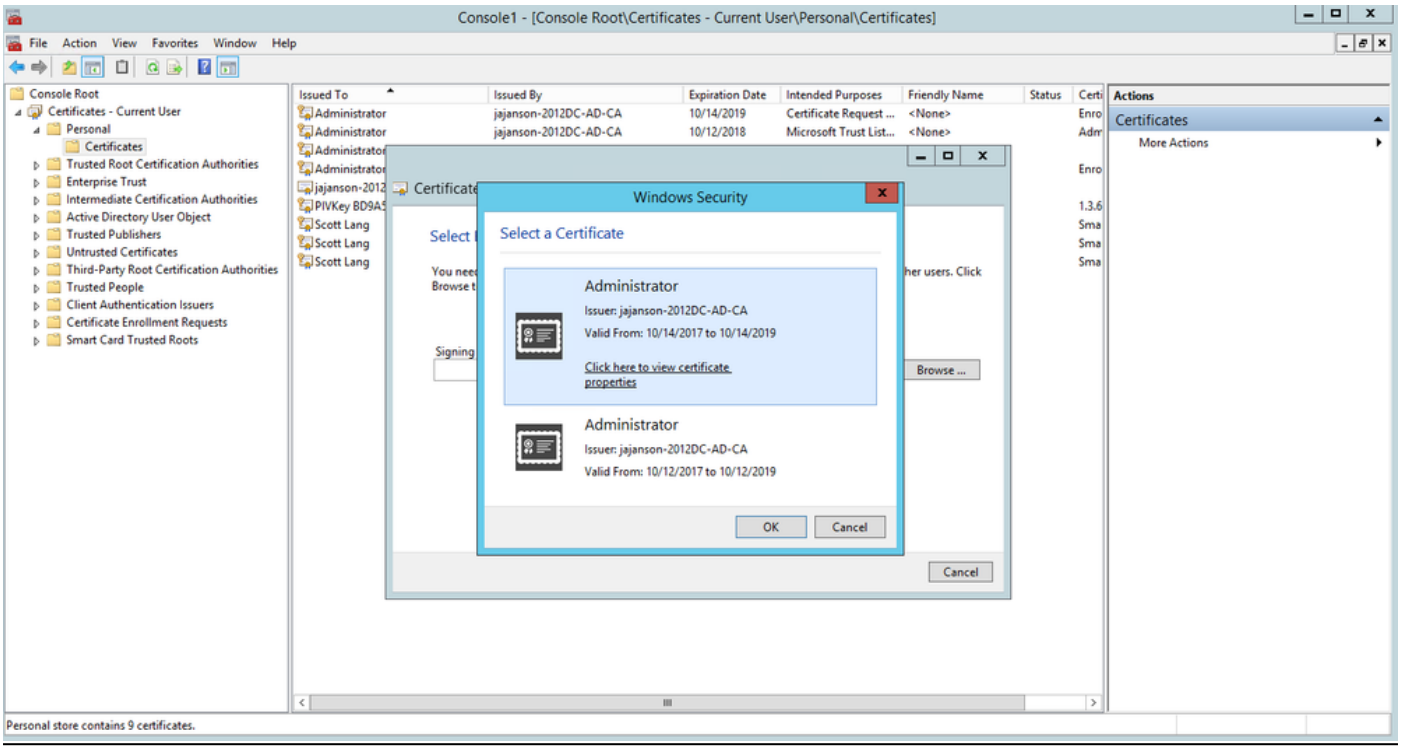


4. Selecteer certificaatinschrijvingsbeleid en klik op **Volgende**.



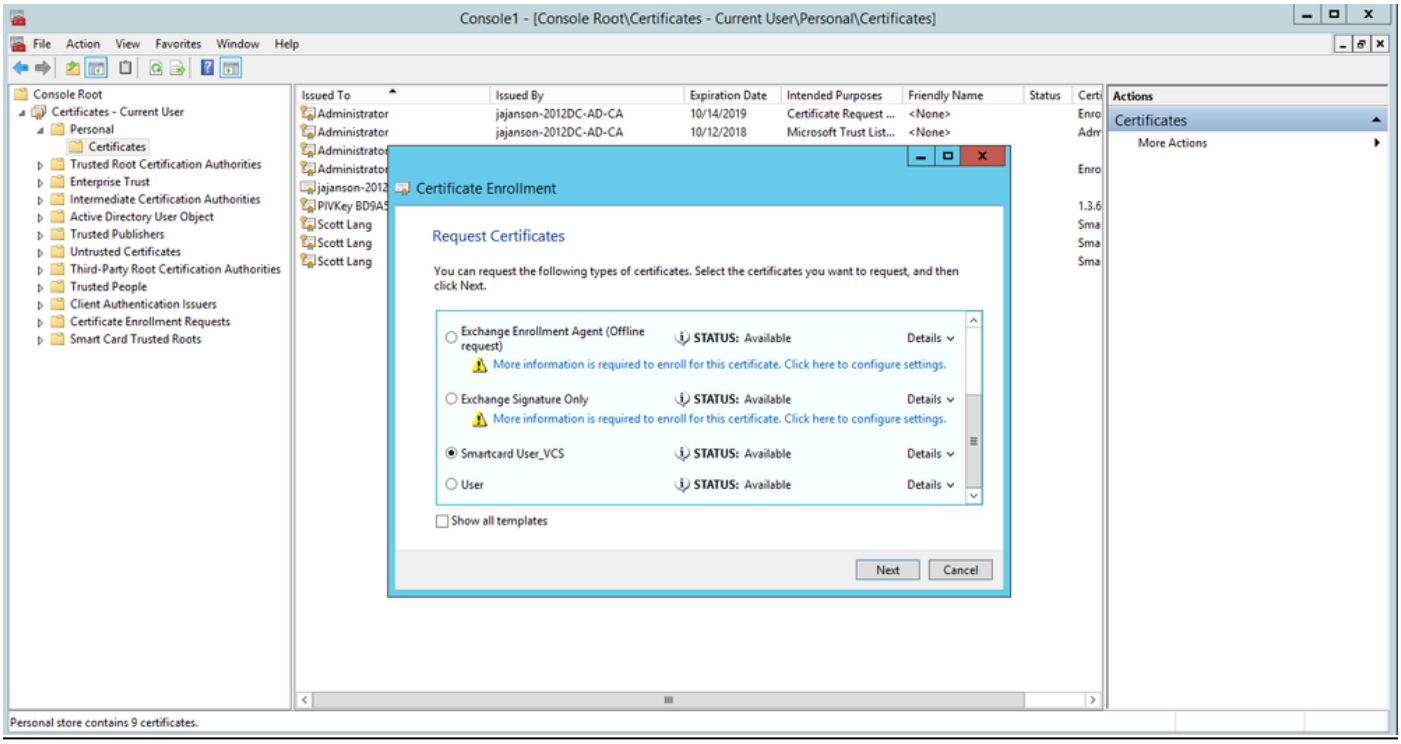
Invoerbeleid

5. U wordt nu gevraagd het **Signing-certificaat** te selecteren. Dit is het inschrijvingscertificaat dat u eerder hebt aangevraagd.



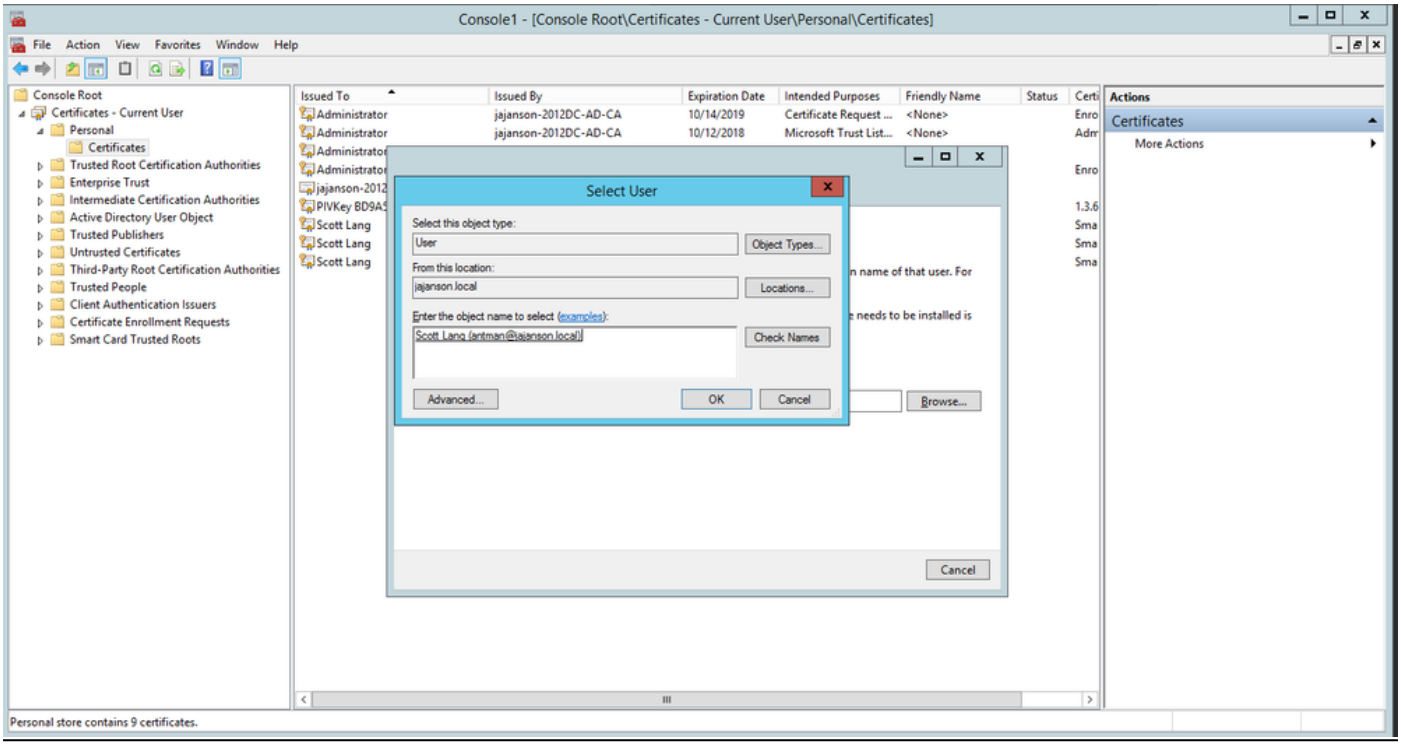
Selecteer Signaalcertificaat

6. Op het volgende scherm moet u naar het certificaat bladeren waar u om wilt vragen en in dit geval is **Smartcard User_VCS** de sjabloon die u eerder hebt gemaakt.



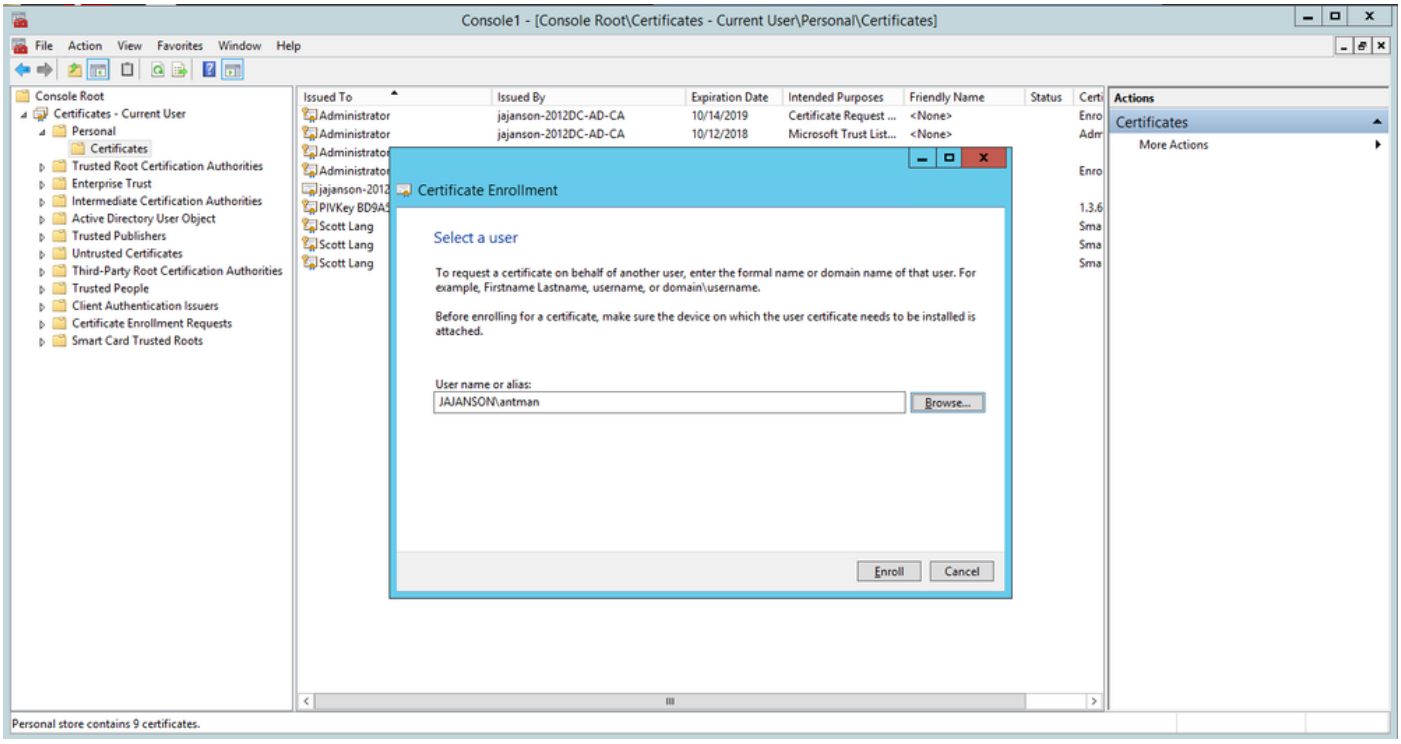
Kies de VCS slimme kaart

7. Selecteer vervolgens de gebruiker die u wilt inschrijven. Klik op **browsen** en type in de gebruikersnaam van de medewerker die u wilt inschrijven. In dit geval wordt Scott Lang 'antman@jajanson.local account' gebruikt.



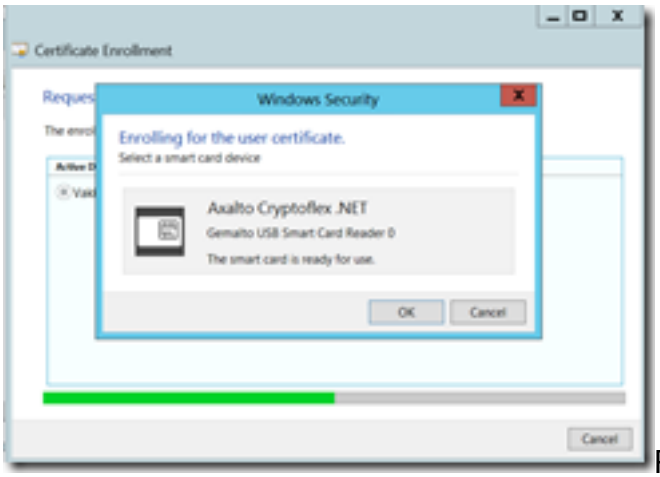
Kies de gebruiker

8. Ga verder met de inschrijving op het volgende scherm door op **Inschrijven** te klikken. Plaats nu een smartcard in de lezer.



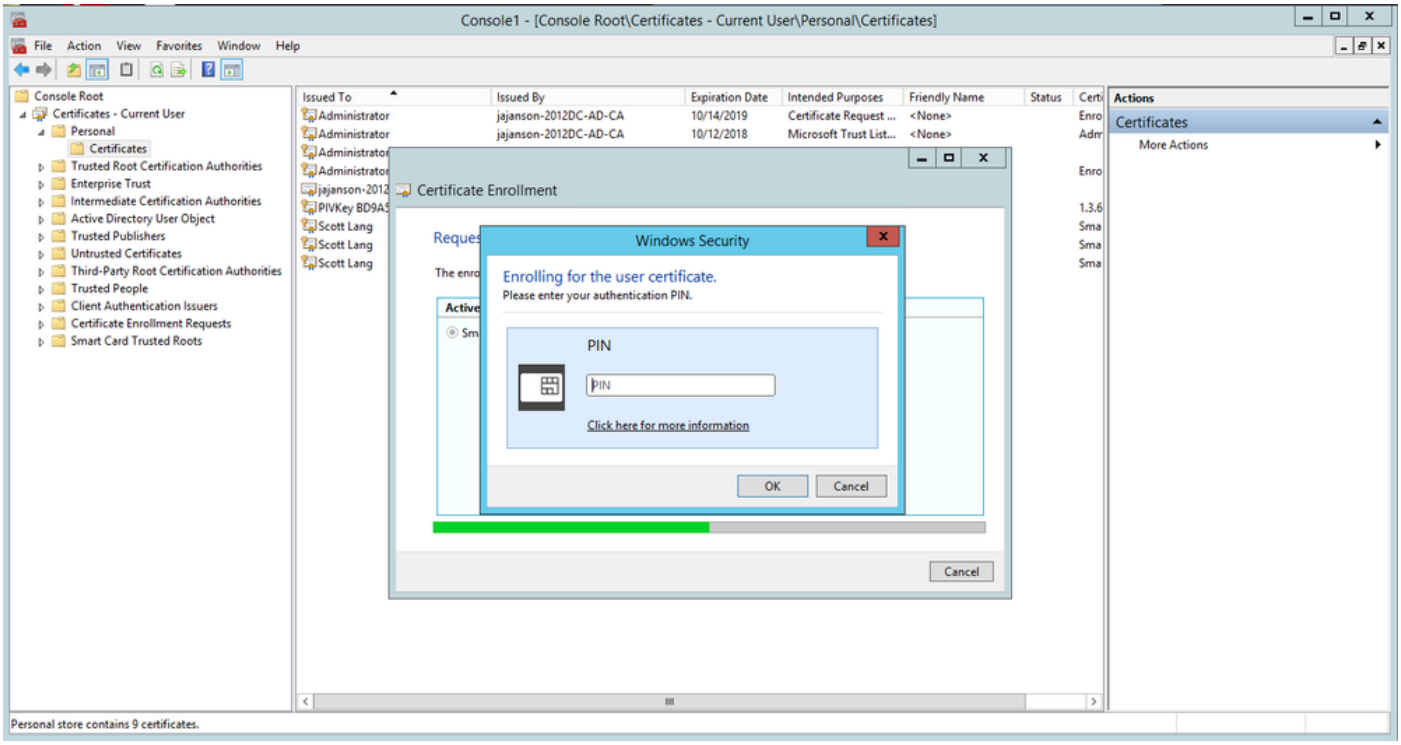
inschrijven

9. Als je je smartcard eenmaal hebt ingevoerd, is deze als volgt gedetecteerd:



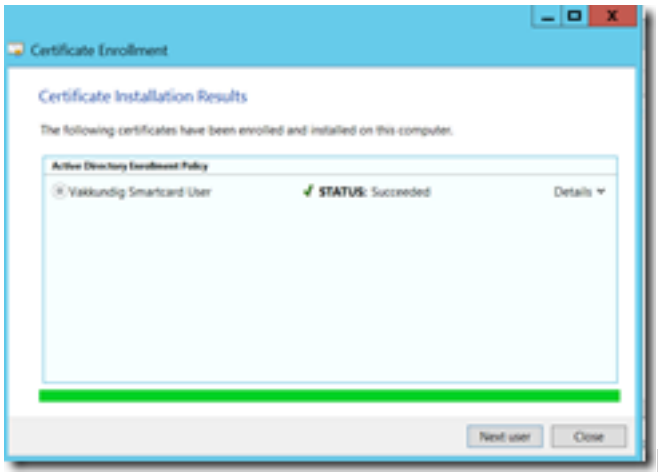
Plaats de slimme kaart

10. U wordt vervolgens gevraagd het nummer van een PIN-smartcard in te voeren (standaard pincode: 0000).



Voer de speld in

11. Ten slotte kun je, zodra je het **Succesvolle** scherm hebt gezien, deze smartcard gebruiken om in te loggen op een server met domeinnamen, zoals de VCS met alleen de kaart en een bekende pin. Het is echter niet ja, u moet de VCS nog voorbereiden om verzoeken tot echtheidscontrole door te sturen naar de Smart Card en gebruik te maken van de Gemeenschappelijke Toegangskaart om het smartcard-certificaat vrij te geven dat opgeslagen is op de smartcard voor verificatie.



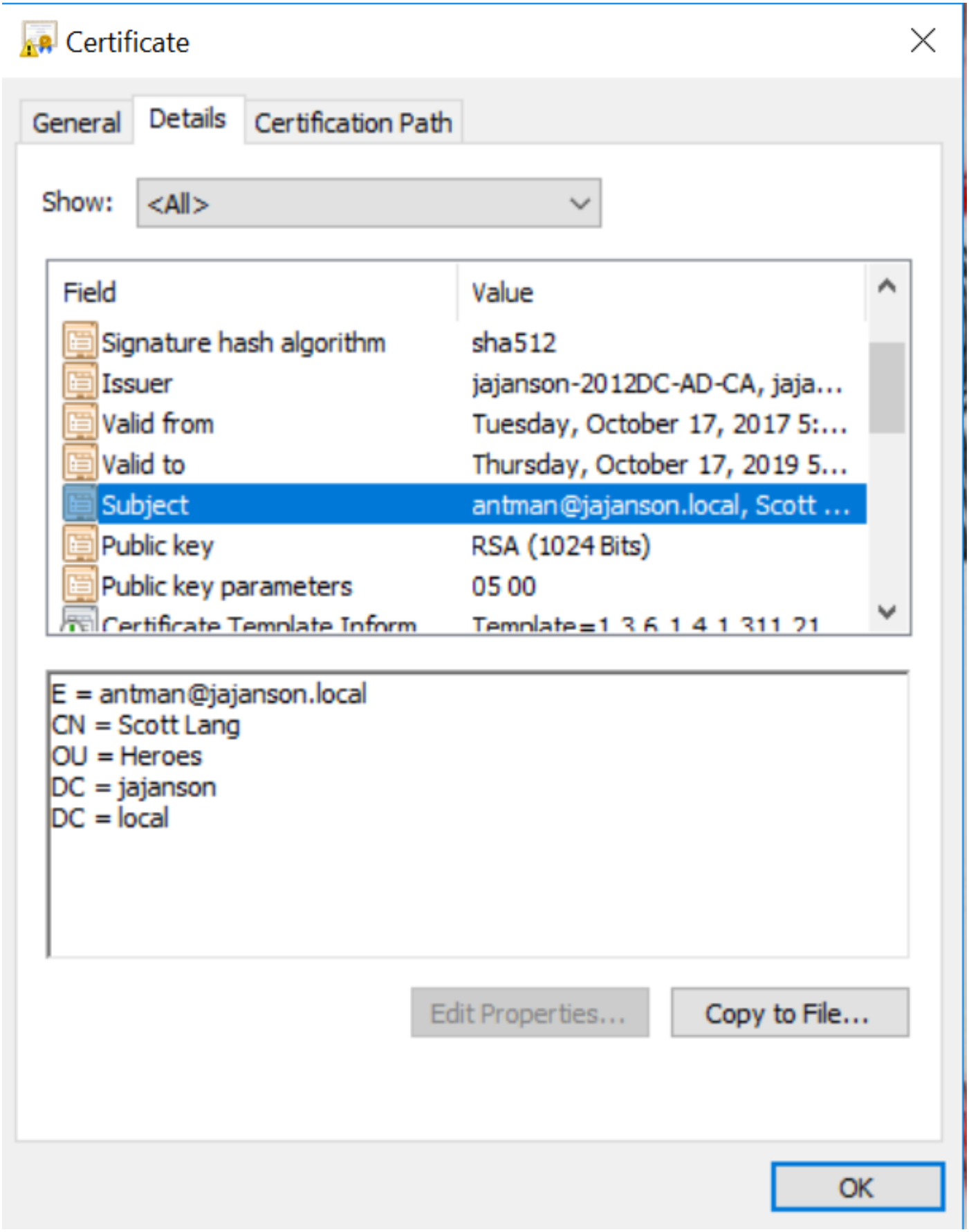
Inschrijving succesvol

Configureer de VCS voor gemeenschappelijke toegangskaart

Upload de Root CA naar de Trusted CA certificaatlijst in het VCS door te navigeren naar **Onderhoud > Security > Trusted CA-certificaat.**

2. Upload de certificaatintrekkingslijst die door de Root CA is ondertekend naar de VCS. Navigeer naar **Onderhoud > Beveiliging > CRL Management.**

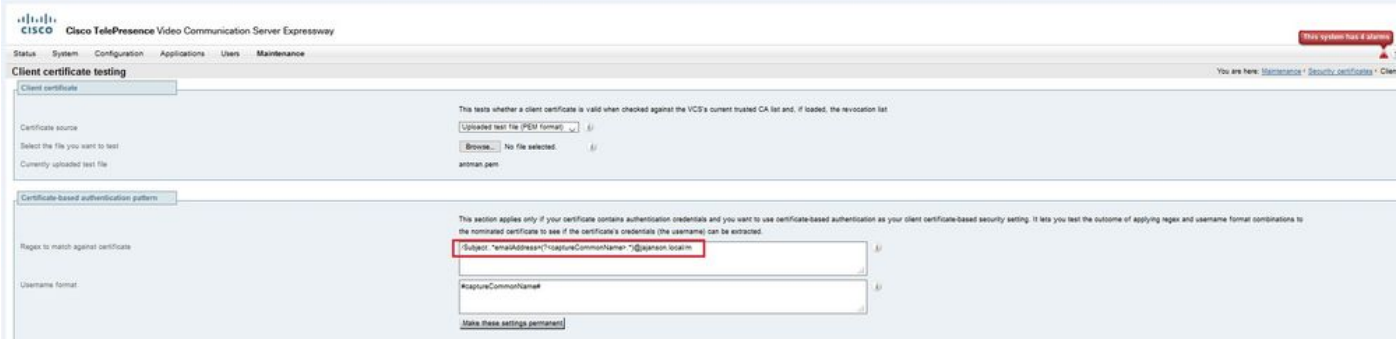
3. Test uw cliënt attest tegen uw regex dat de gebruikersnaam van het certificaat voor authenticatie aan de LDAP of lokale gebruiker trekt. De regex komt overeen met het **Onderwerp** van het certificaat. Dit kan je UPN zijn, E-mail enzovoort. In dit lab werd de e-mail om te koppelen aan het client certificaat gebruikt.



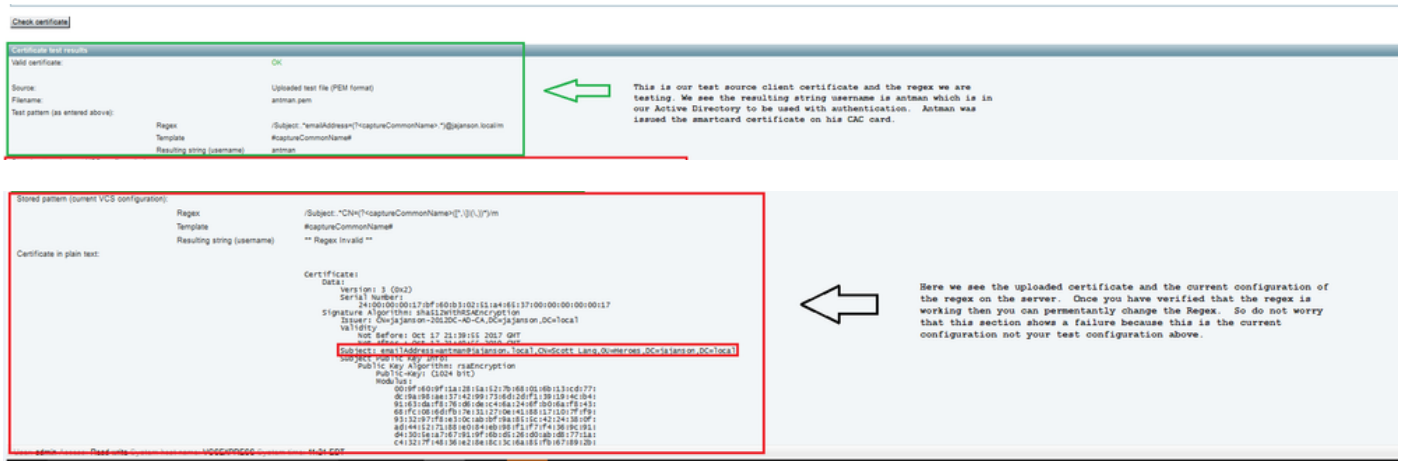
Betreft: Clientcertificaat

4. Navigeer naar **onderhoud > Beveiliging > Clientcertificatie testen**. Selecteer het te testen client certificaat in Mijn lab was het antman.pem, en uploadde het naar het testgebied. In het gedeelte **certificaatgebaseerde echtheidscontrole** onder **Regex om te vergelijken met** het **certificatieplaatje** dat u wilt testen. Wijzig het veld **Gebruikersnaam** niet.

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



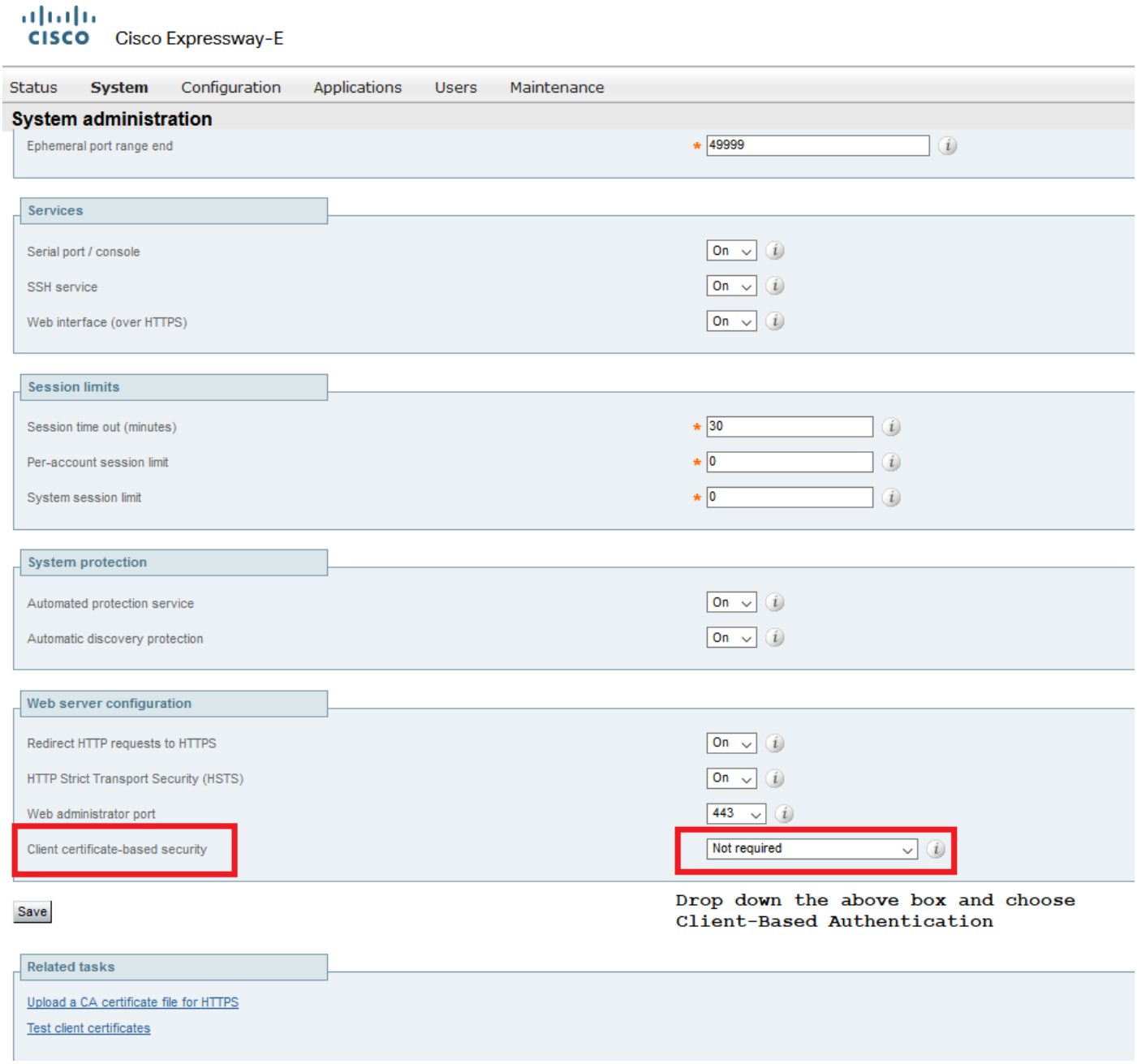
Test uw regex in VCS



Resultaten testen

5. Als de test u de gewenste resultaten oplevert, kunt u op de knop **Deze wijzigingen permanent maken**. Dit verandert uw regex voor de **op certificaat gebaseerde authenticatie configuratie** van de server. Om de verandering te verifiëren, navigeer naar die configuratie, **Onderhoud > Beveiliging > Op certificaat gebaseerde authenticatie configuratie.**

6. Verificatie op client inschakelen door naar **systeem > beheerder te** navigeren en vervolgens op het vak **Clientcertificaat** te klikken of het uitrolvak te selecteren om **clientbeveiliging = op client gebaseerde verificatie** te kiezen**.** Met deze instelling typt de gebruiker de FQDN van de VCS server in zijn browser en wordt hij gevraagd om zijn clientaccount te kiezen en de pin in te voeren die aan zijn Common Access Card is toegewezen. Het certificaat wordt dan vrijgegeven en hij krijgt de Web GUI van de VCS-server terug en hij hoeft alleen maar op de knop Administrator te klikken of de knop te selecteren. Dan wordt hij opgenomen in de server. Als de opties **Op het clientcertificaat gebaseerde beveiliging = Clientgebaseerde validatie** zijn geselecteerd, is het proces hetzelfde, met uitzondering van het geval dat de gebruiker op de knop Administrator klikt, heeft hij opnieuw het wachtwoord voor de beheerder gevraagd. Normaal gesproken is dat niet wat de organisatie met CAC probeert te bereiken.



Op client gebaseerde verificatie inschakelen

Help! Ik ben buiten!!!

Als u de Client Based Verificatie toestaat en de VCS het certificaat om welke reden dan ook afwijst, kunt u niet meer op traditionele wijze inloggen bij de web GUI. Maar maak niet bang dat er een manier is om terug in je systeem te komen. Het bijgevoegde document is te vinden op de Cisco-website en geeft informatie over hoe clientgebaseerde verificatie uit te schakelen van worteltoegang.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.