CACおよびスマートカードリーダーを使用したVCSの設定

内容

概要

このドキュメントでは、Cisco Video Communication Server(VCS)で使用するSmart Card ReaderおよびCommon Access Card(CCC)ログインをインストールして使用する手順を説明します。これは、銀行、病院、または政府機関などのVCS環境に2要素認証を必要とするとする組織です。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco Expressway Administrator(X14.0.2)に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

CACは必要な認証を提供するため、「システム」は環境にアクセスできるユーザと、インフラストラクチャのどの部分が物理的または電子的であるかを認識します。政府が分類した環境、およびその他のセキュアなネットワークでは、「最小特権アクセス」または「知る必要がある」というルールが優先されます。ログインは誰でも利用できます認証にはCACが持っているものを必要としますCACは2006年に登場しました個人が複数のデバイスを持つ必要はありません例えばfobs, id card, donglesです

スマートカードとは

スマートカードは、クライアント認証、ログオン、および安全な電子メールなどのソフトウェアのみのソリューションを強化するため、MicrosoftがWindowsプラットフォームに統合するために使用する公開キーインフラストラクチャ(PKI)の主要コンポーネントです。スマートカードは、公開キー証明書と関連キーを統合するポイントです。その理由は次のとおりです。

- 秘密鍵およびその他の個人情報を保護するための改ざん防止ストレージを提供します。
- セキュリティクリティカルな計算を切り分けます。この計算には、認証、デジタル署名、およびシステムの他の部分からのキー交換が含まれます。これらの情報を知る必要はありません。
- 職場、自宅、または外出先のコンピュータ間で、クレデンシャルやその他のプライベート情報のポータビリティを有効にします。

スマートカードは、マウスやCD-ROMの導入と同様に、コンピュータ業界に画期的な新しい望ましい機能を提供するため、Windowsプラットフォームの不可欠な要素となっています。 現時点で内部PKIインフラストラクチャがない場合は、最初にこれを行う必要があります。このドキュメントでは、この記事でこのロールをインストールする方法については説明しませんが、この機能の実装方法については、次のリンクを参照してください。http://technet.microsoft.com/en-us/library/hh831740.aspx にアクセスしてください。

設定

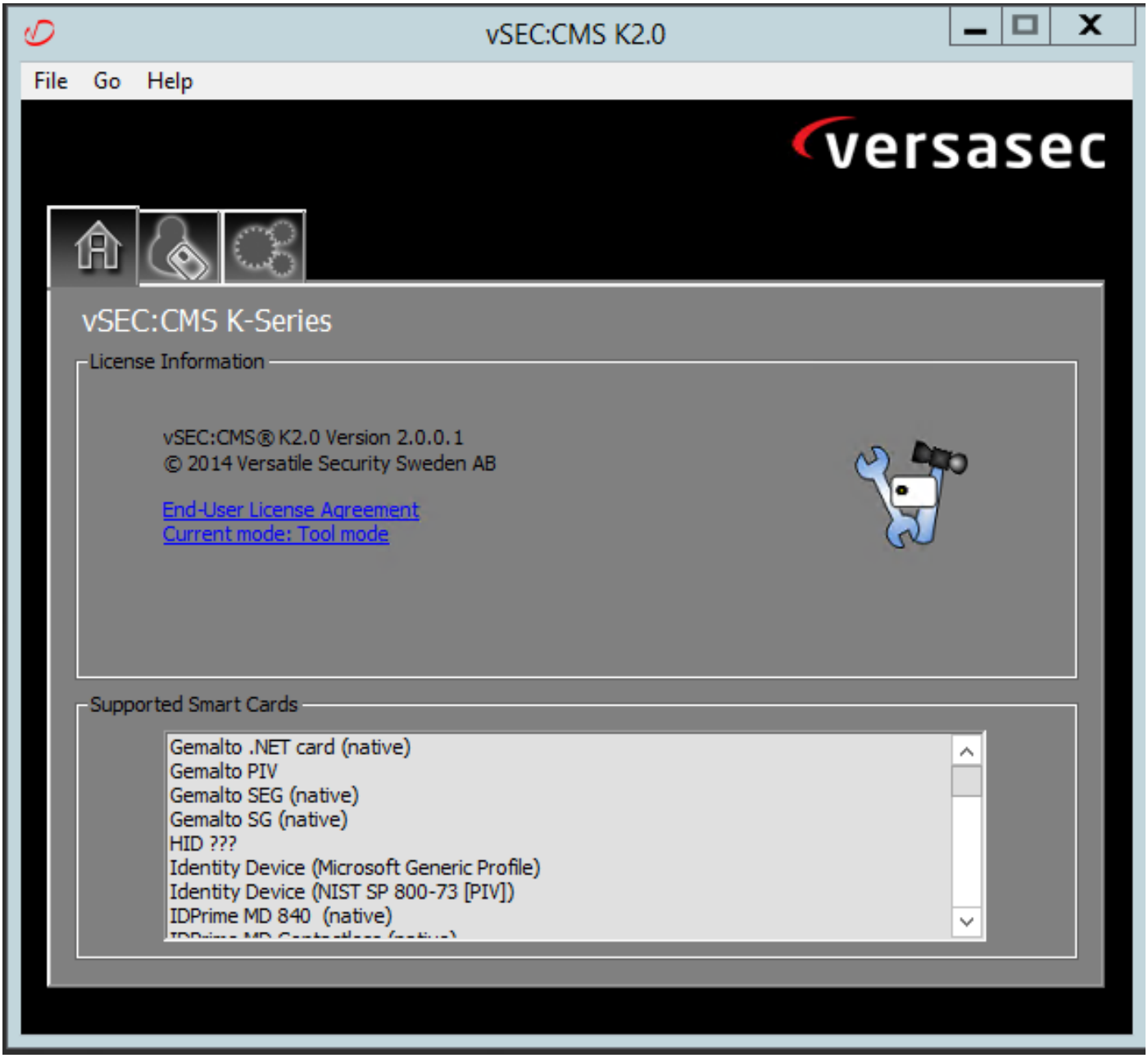
この実習では、LDAPとVCSがすでに統合されており、LDAPクレデンシャルでログインできるユーザがいることを前提としています。

1. ラボ機器
2. スマートカードの取り付け
3. 認証局テンプレートの設定
4. 登録エージェント証明書の登録
5. の代理で登録....
6. 共通アクセスカード用のVCSの設定

必要な機器：

次の役割またはインストールされたソフトウェアを持つWindows 2012R2ドメインサーバ：

- 認証局
- Active Directory
- DNS
- スマートカードが接続されたWindows PC
- vSEC:スマートカードを管理するためのCMS Kシリーズ管理ソフトウェア：



Versa Card Readerソフトウェア

スマートカードの取り付け

通常、スマートカードリーダーには、必要なケーブルの接続方法に関する指示が記載されています。この設定のインストール例を次に示します。

スマートカードリーダーデバイスドライバのインストール方法

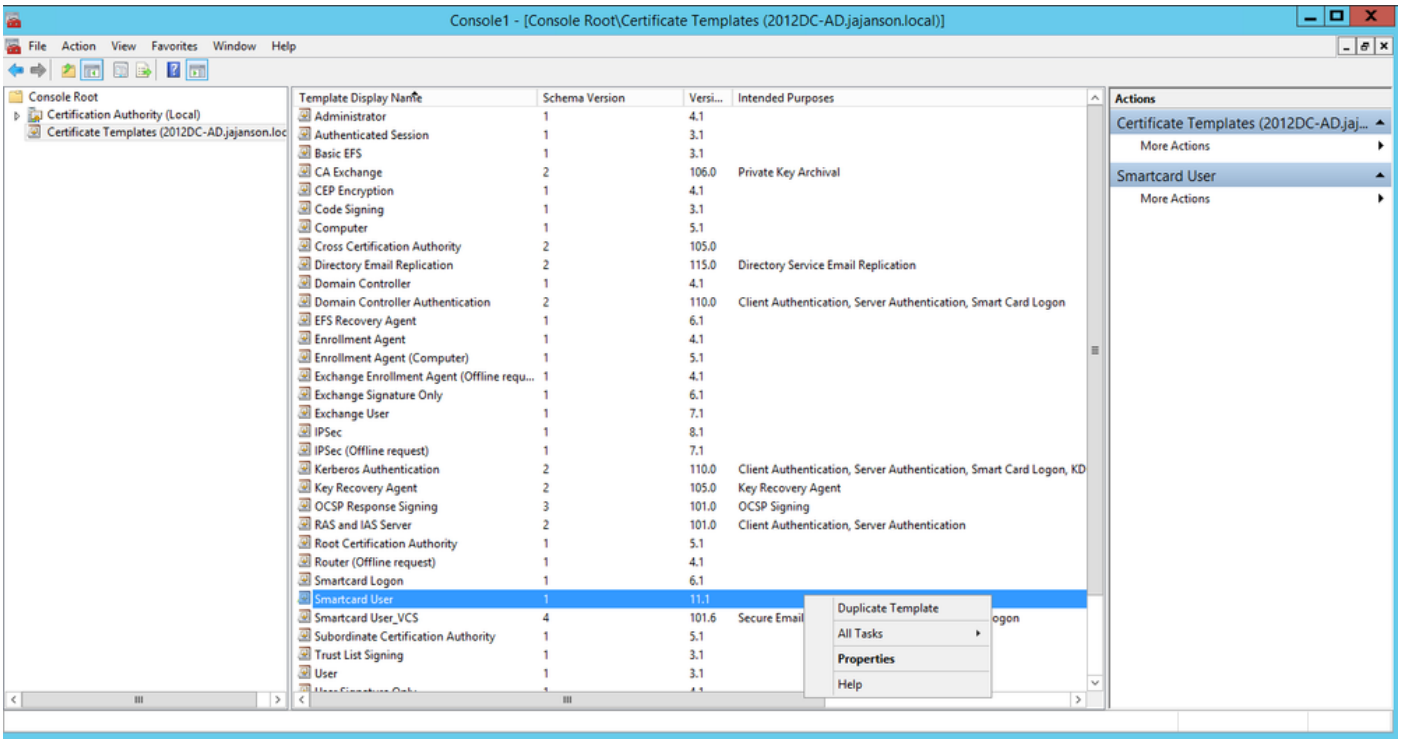
スマートカード読み取り装置が検出され、インストールされている場合は、[Windowsログオンへようこそ]画面で確認できます。そうでない場合：

1. スマートカードをWindows PCのUSBポートに接続します
2. 画面の指示に従って、デバイスドライバソフトウェアをインストールします。これには、スマートカードまたはドライバの製造元がWindowsで検出されているドライバメディアが必要です。私の場合、私は彼らのダウンロードサイトからメーカーのドライバを使用しました。**WINDOWSを信頼しないでください。**
3. デスクトップの[マイコンピュータ]アイコンを右クリックし、サブメニューの[管理]をクリックします。

4. 「サービスとアプリケーション」ノードを展開し、「サービス」をクリックします。
5. 右側のペインで、[スマートカード]を右クリックします。サブメニューの「プロパティ」をクリックします。
6. [全般]タブで、[スタートアップタイプ]ドロップダウンリストの[自動]を選択します。[OK] をクリックします。
7. ハードウェアウィザードで指示された場合は、マシンを再起動します。

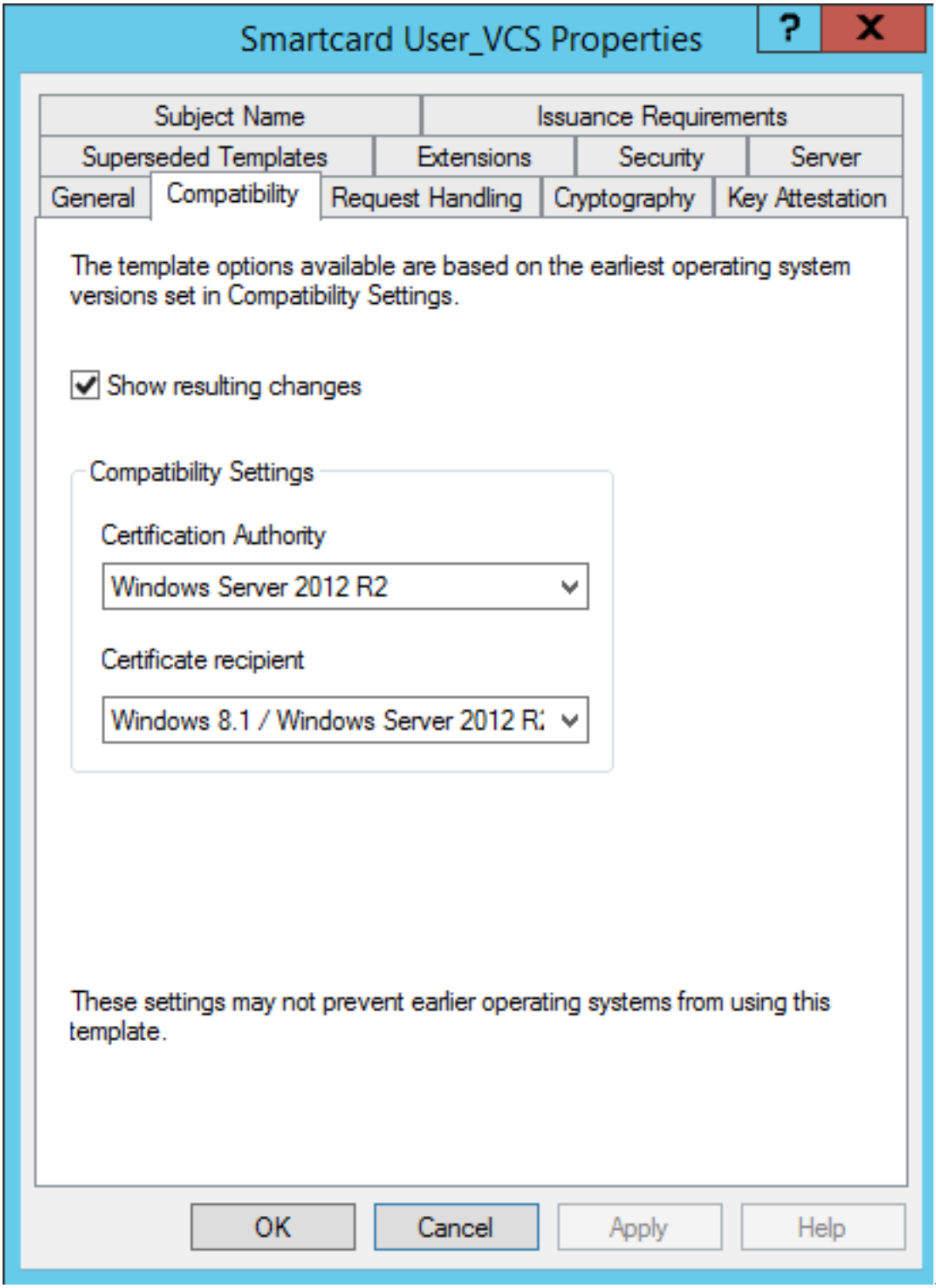
認証局テンプレートの設定

1. [管理ツール(Administrative Tools)]から認証局(CA)MMCを起動します。
2. [証明書テンプレート]ノードをクリックまたは選択し、[管理]を選択します。
3. 右クリックするか、[Smartcard User Certificate Template]を選択し、図のように[Duplicate]を選択します。



ドメインコントローラ証明書テンプレート

4. [Compatibility]タブの[Certification Authority]で、選択を確認して、必要に応じて変更します。

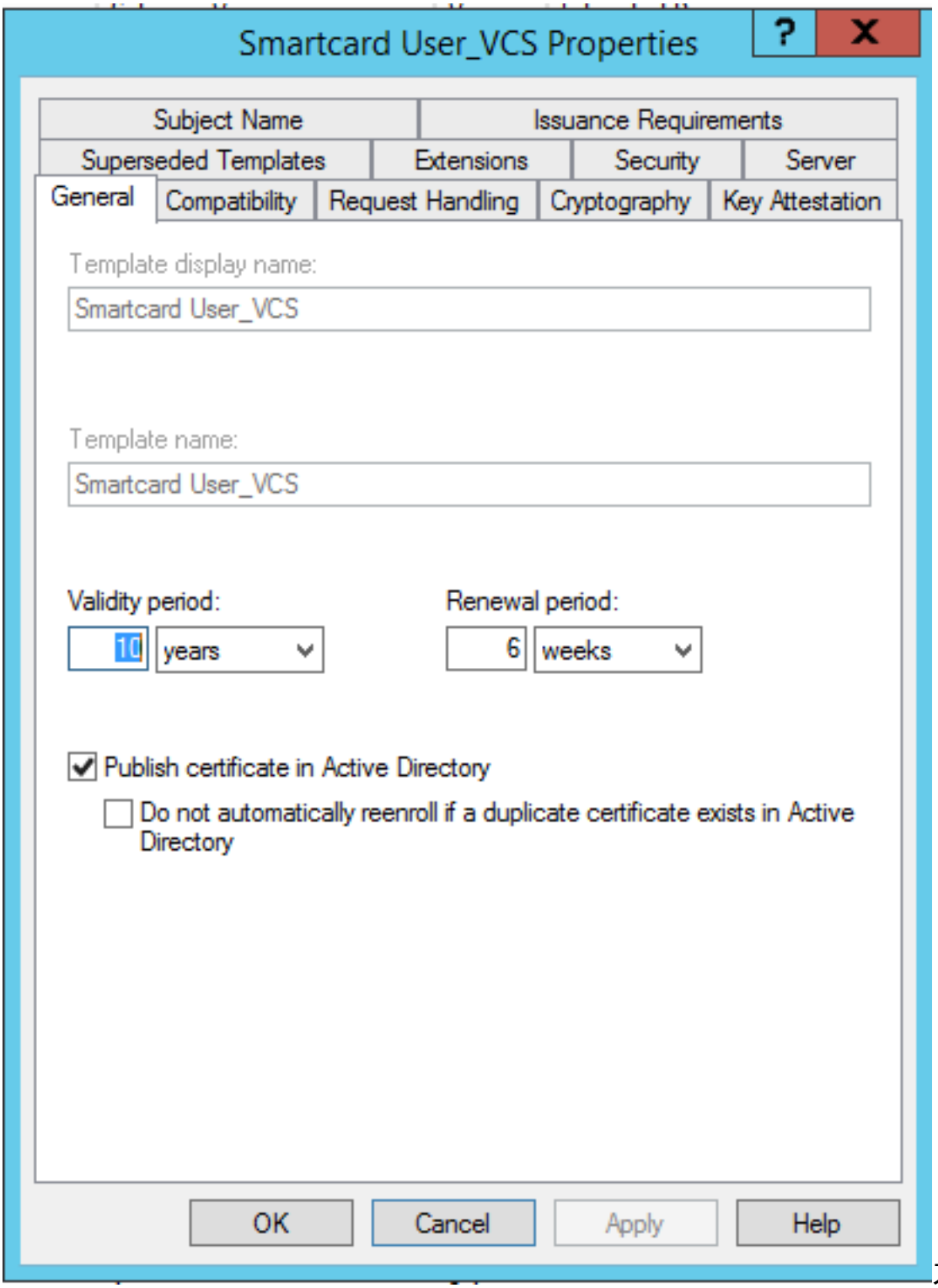


スマートカード互換性の設定

5. [General]タブで次の操作を行います。

a.名前を指定します(Smartcard User_VCSなど)。

b.有効期間を目的の値に設定します。[Apply] をクリックします。



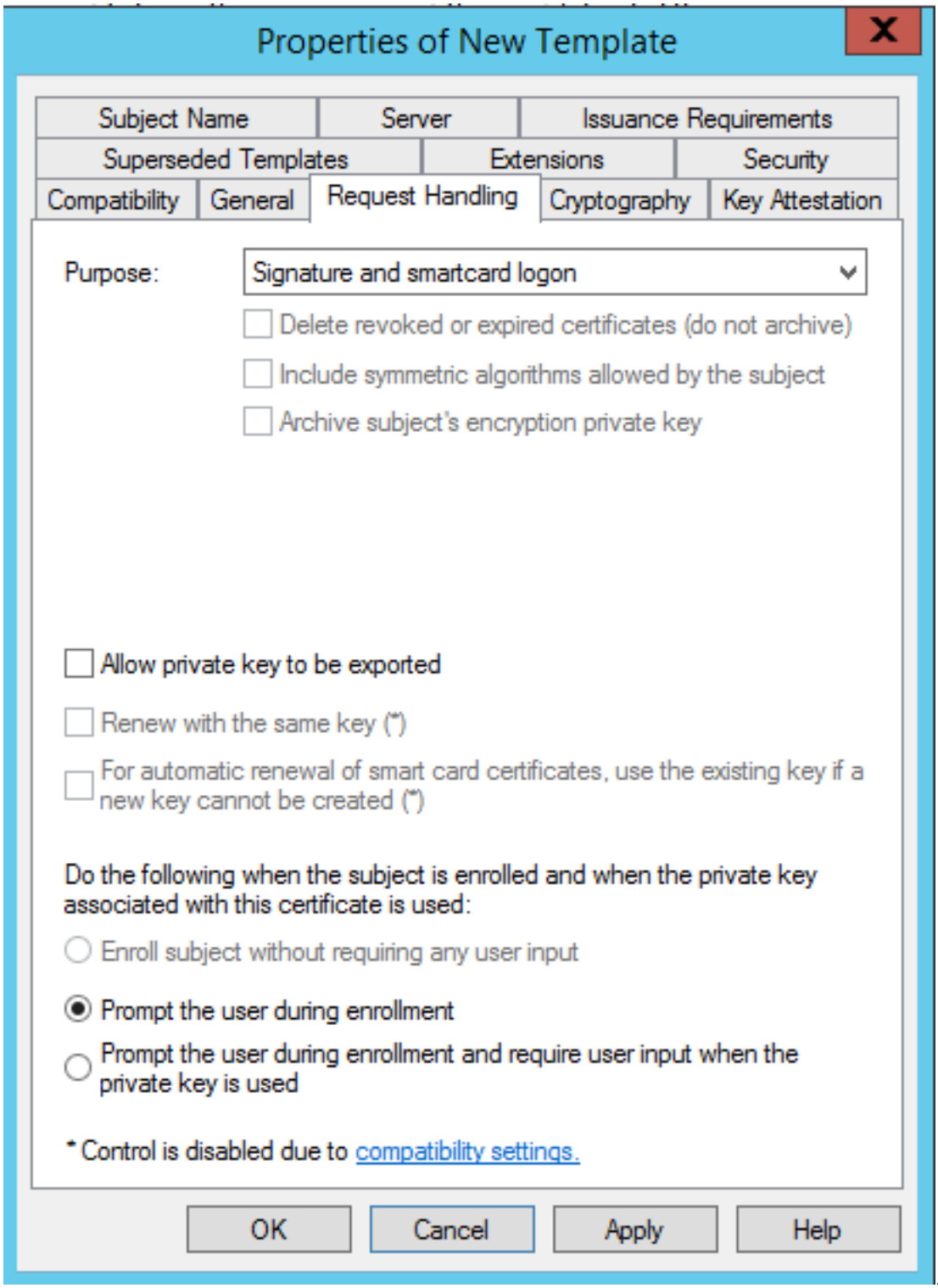
スマートカードー般

開始時間の有効期限

6. 「要求の処理」**タブでは、次を行います。**

a.[Purpose]を**[Signature]および[smartcard logon]に設定します。**

b.[登録時に**ユーザーにプロンプトを表示]をクリックします。**[Apply] をクリックします。

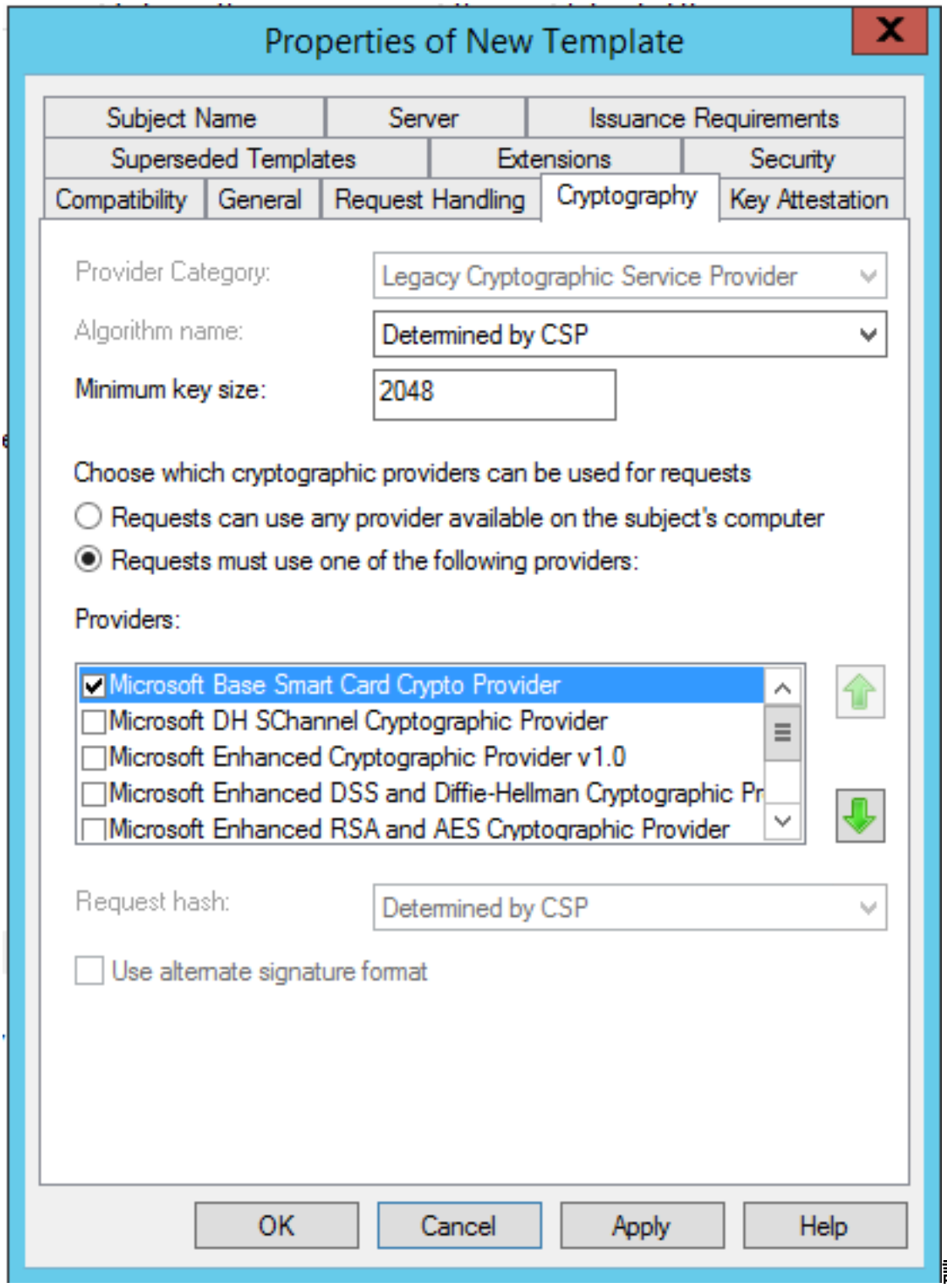


スマートカード要求の処理

7. [暗号化]タブで、最小キーサイズを2048に設定します。

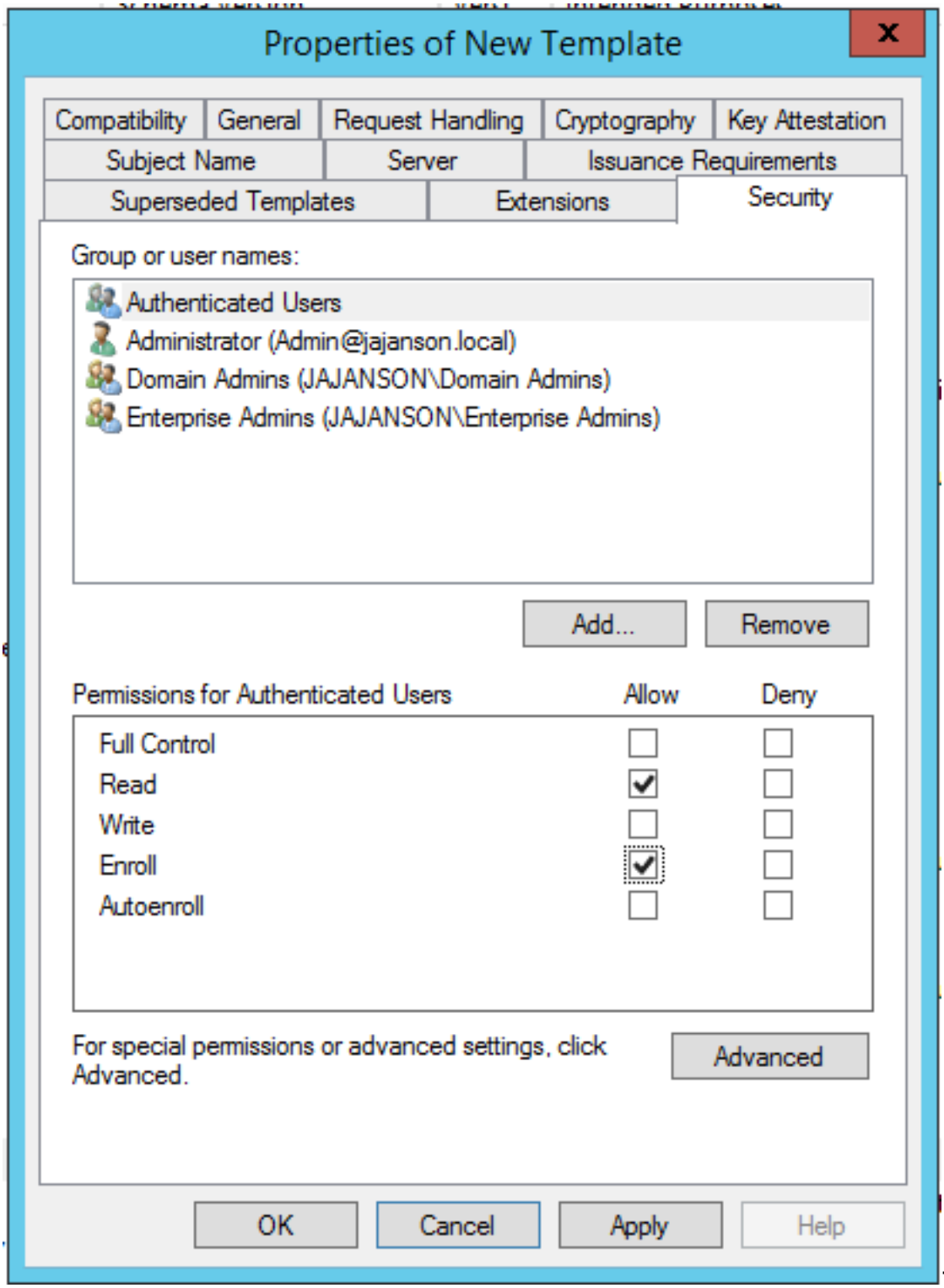
a.[Requests must use **one the following providers]をクリックし、[Microsoft Base Smart Card Crypto Provider]を選択します。**

b. 「適用」をクリックします。



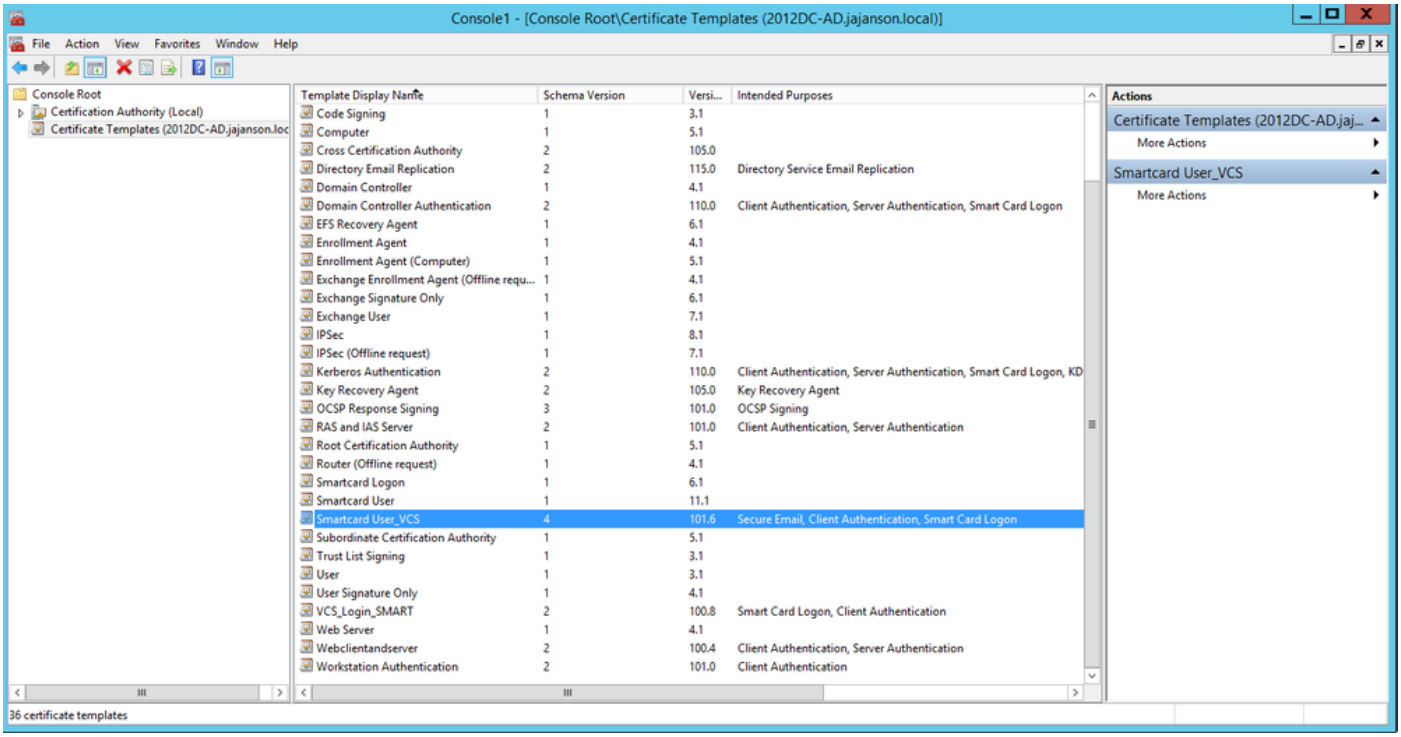
証明書暗号化設定

8. [セキュリティ]タブで、登録アクセス権を付与するセキュリティグループを追加します。たとえば、すべてのユーザーにアクセス権を付与する場合は、[認証済みユーザー]グループを選択し、そのグループに対して[登録]権限を選択します。



テンプレートセキュリティ

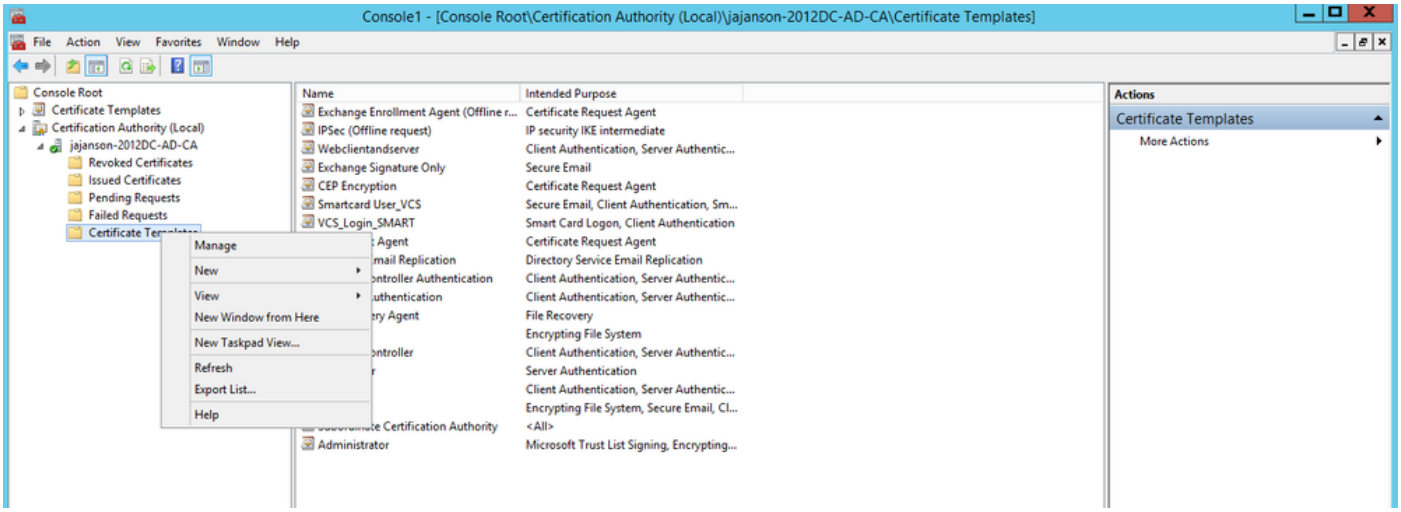
9. [OK]をクリックして、変更を確定し、新しいテンプレートを作成します。新しいテンプレートが[証明書テンプレート(Certificate Templates)]のリストに表示されます。



ドメイン制御で表示されるテンプレート

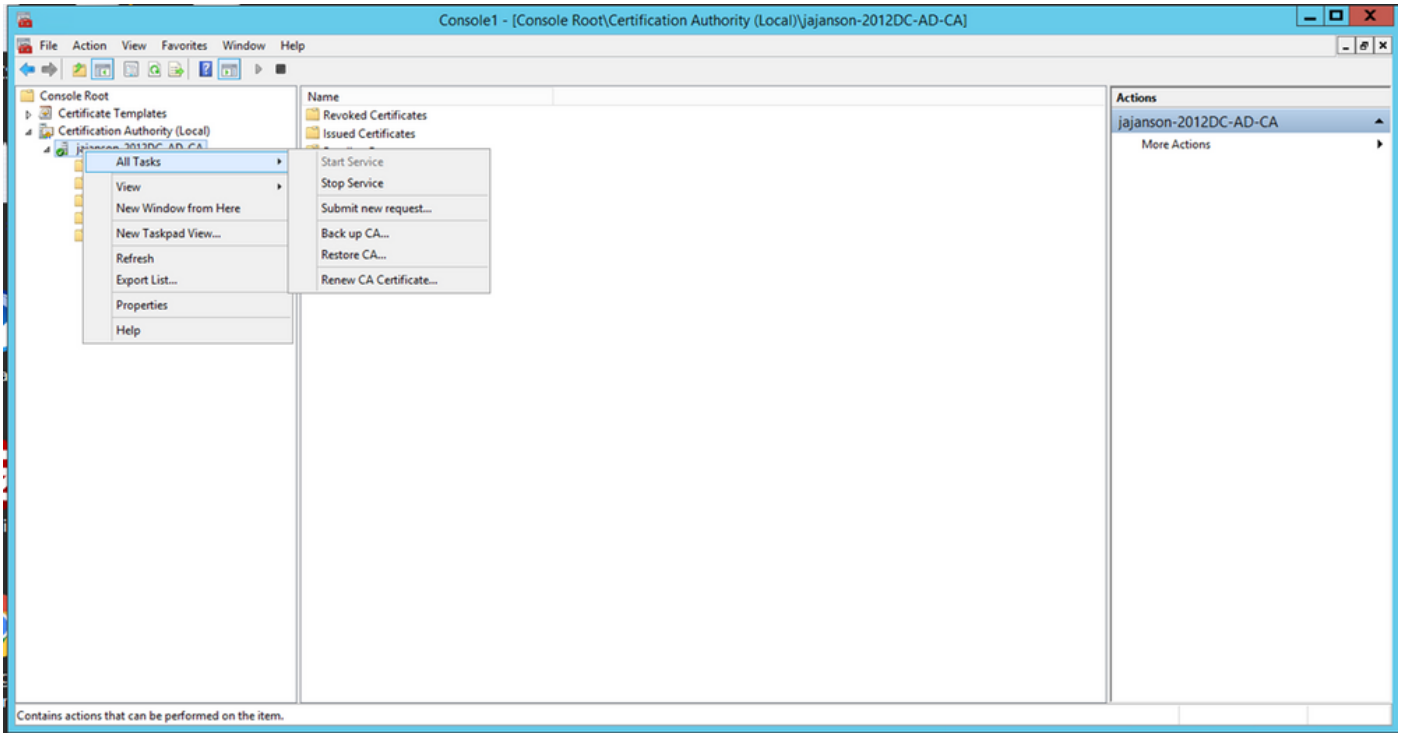
10. MMCの左側のペインで、[Certification Authority (Local)]を展開し、[Certification Authority]リスト内のCAを展開します。

[Certificate Templates]を右クリックし、[New]をクリックし、[Certificate Template to Issue]をクリックします。次に、新しく作成したスマートカードテンプレートを選択します。



新しいテンプレートの発行

11.テンプレートが複製された後、MMCで[証明機関]の一覧を右クリックまたは選択し、[すべてのタスク]をクリックして、[サービスの停止]をクリックします。次に、CAの名前を再度右クリックし、[すべてのタスク]をクリックし、[サービスの開始]をクリックします。

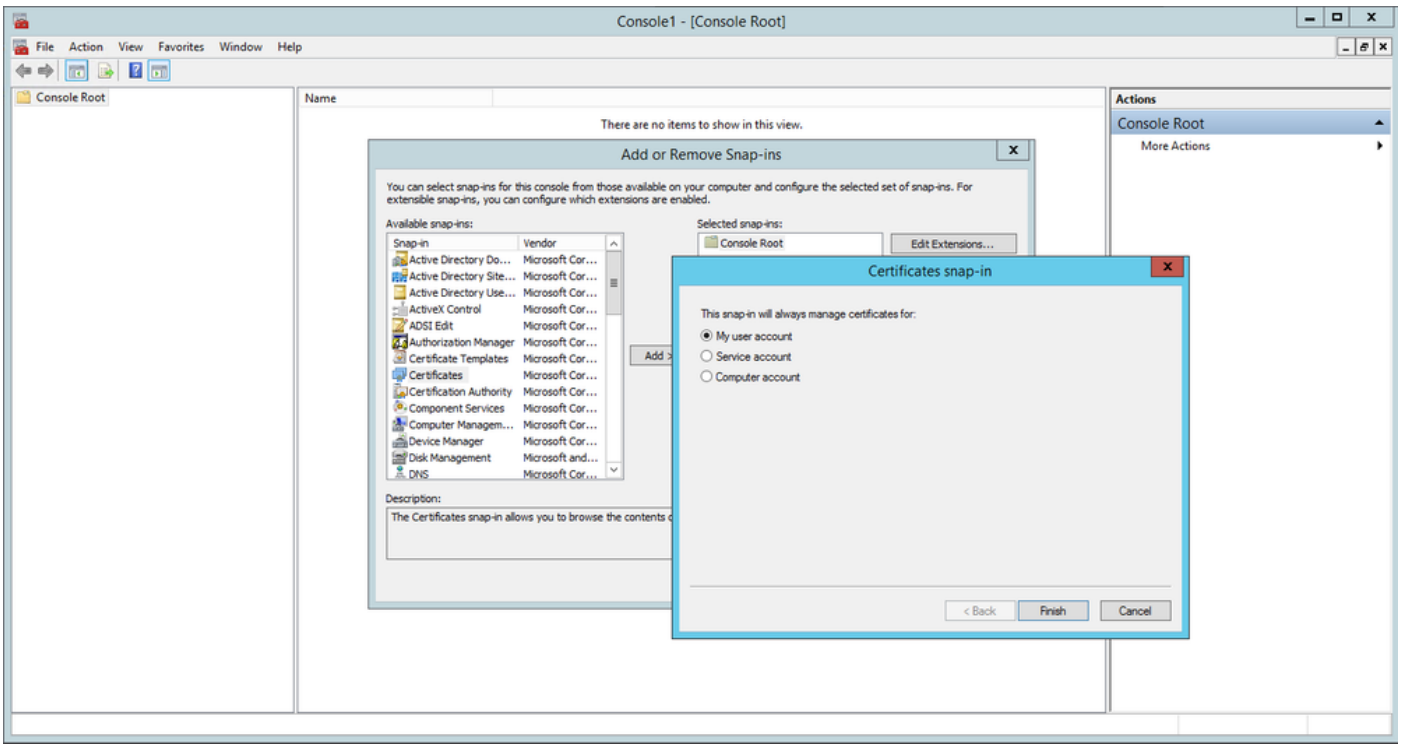


証明書サービスを停止してから開始する

登録エージェント証明書への登録

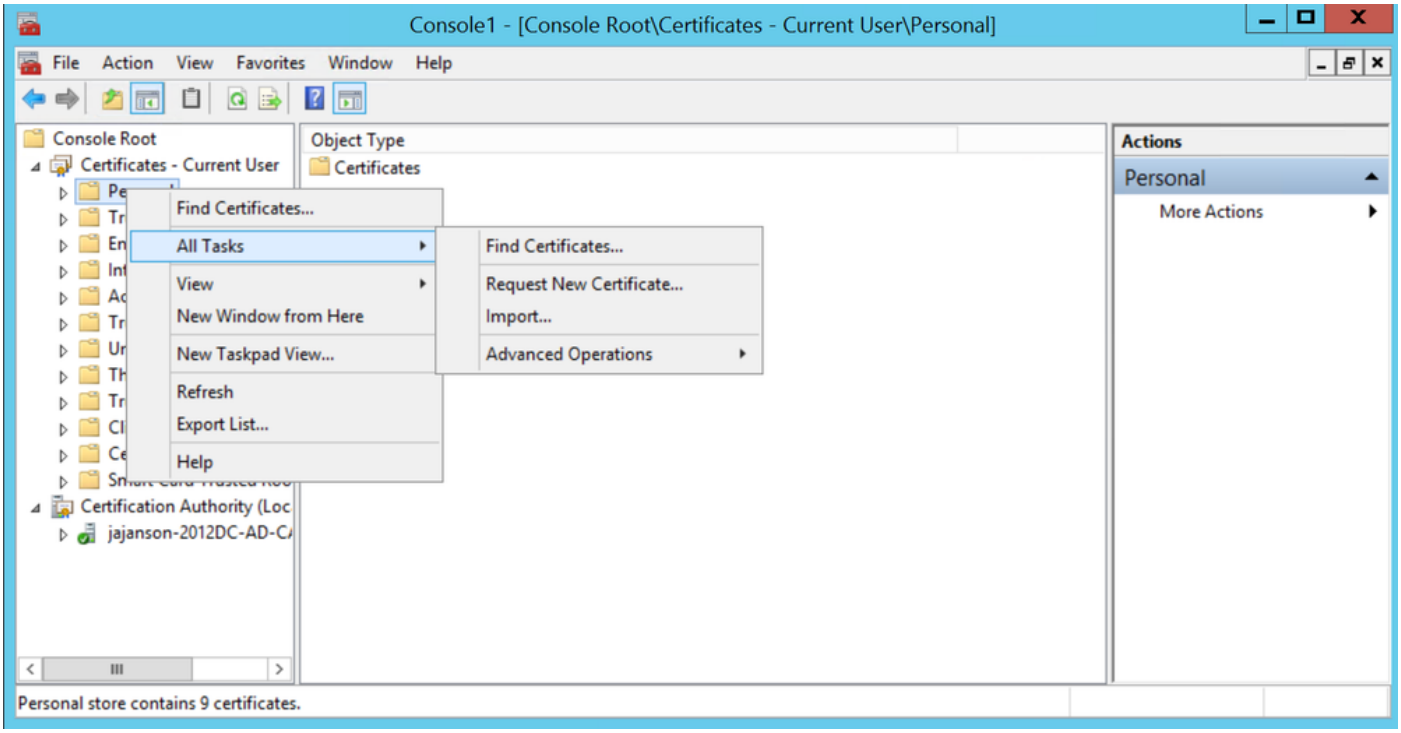
これは、クライアントマシン(IT Administrators Desktop)で行うことをお勧めします。

1. MMCを起動し、[証明書]を選択し、[追加]をクリックして、[マイユーザアカウント]の証明書をクリックします。



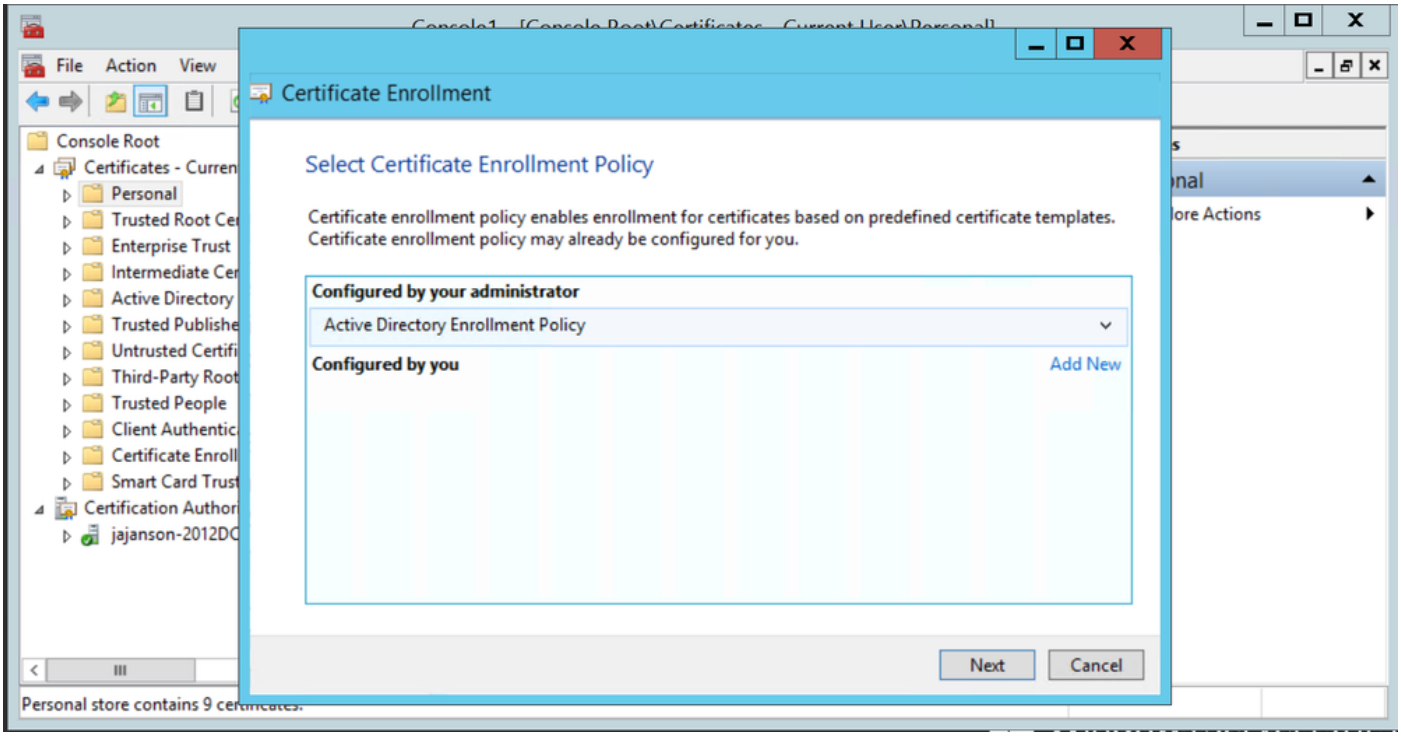
証明書の追加

2. 右クリックするか、[個人ノード]を選択し、[すべてのタスク]を選択し、[新規証明書の要求]を選択します。



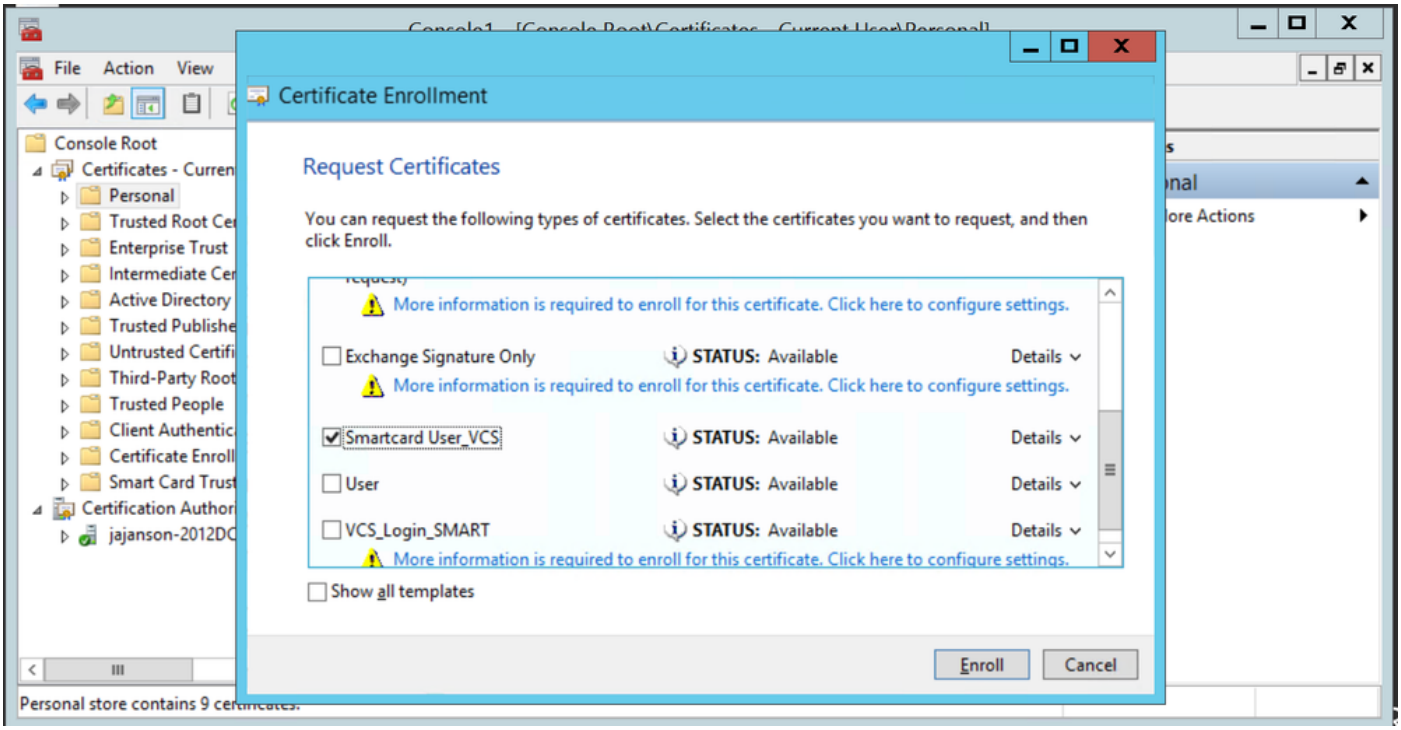
新しい証明書の要求

3.ウィザードの[次へ]をクリックし、[Active Directory Enrollment Policy]を選択します。次に、もう一度[次]をクリックします。



Active Directory登録

4. [Enrollment Agent Certificate]を選択し、この場合は[Smartcard User_VCS]を選択し、[Enroll]をクリックします。

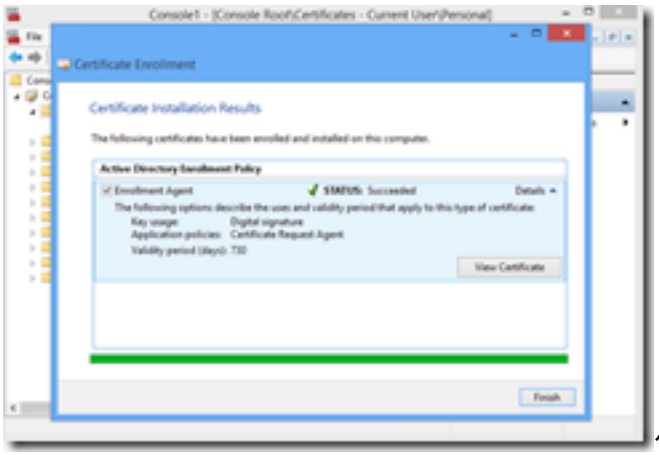


登録証明書エージェント

IT管理者のデスクトップが登録ステーションとして設定されました。これにより、他のユーザに代わって新しいスマートカードを登録できます。

の代理で登録....

認証のために従業員にスマートカードを提供するには、従業員を登録して証明書を生成する必要があります。証明書はスマートカードにインポートされます。

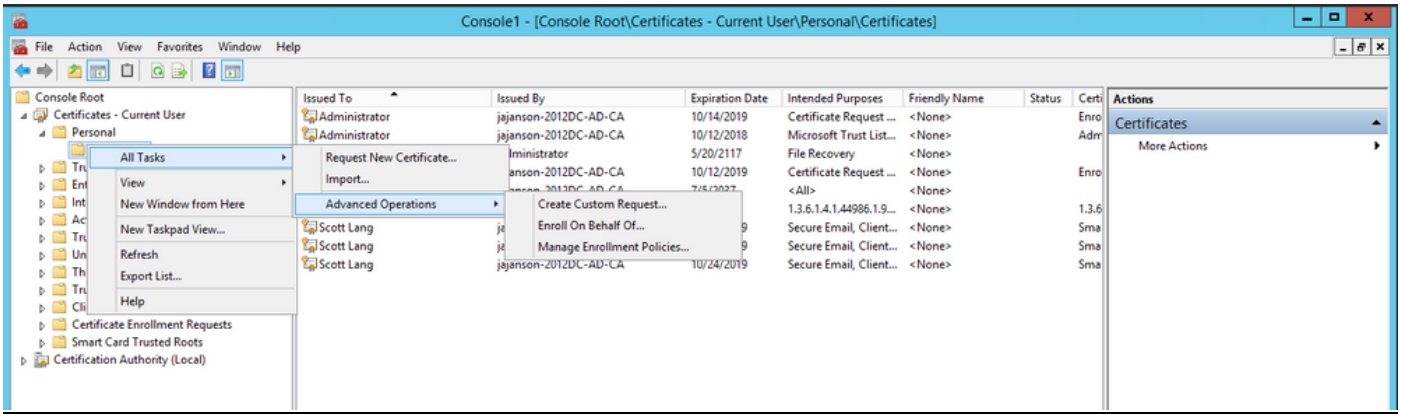


代理で登録

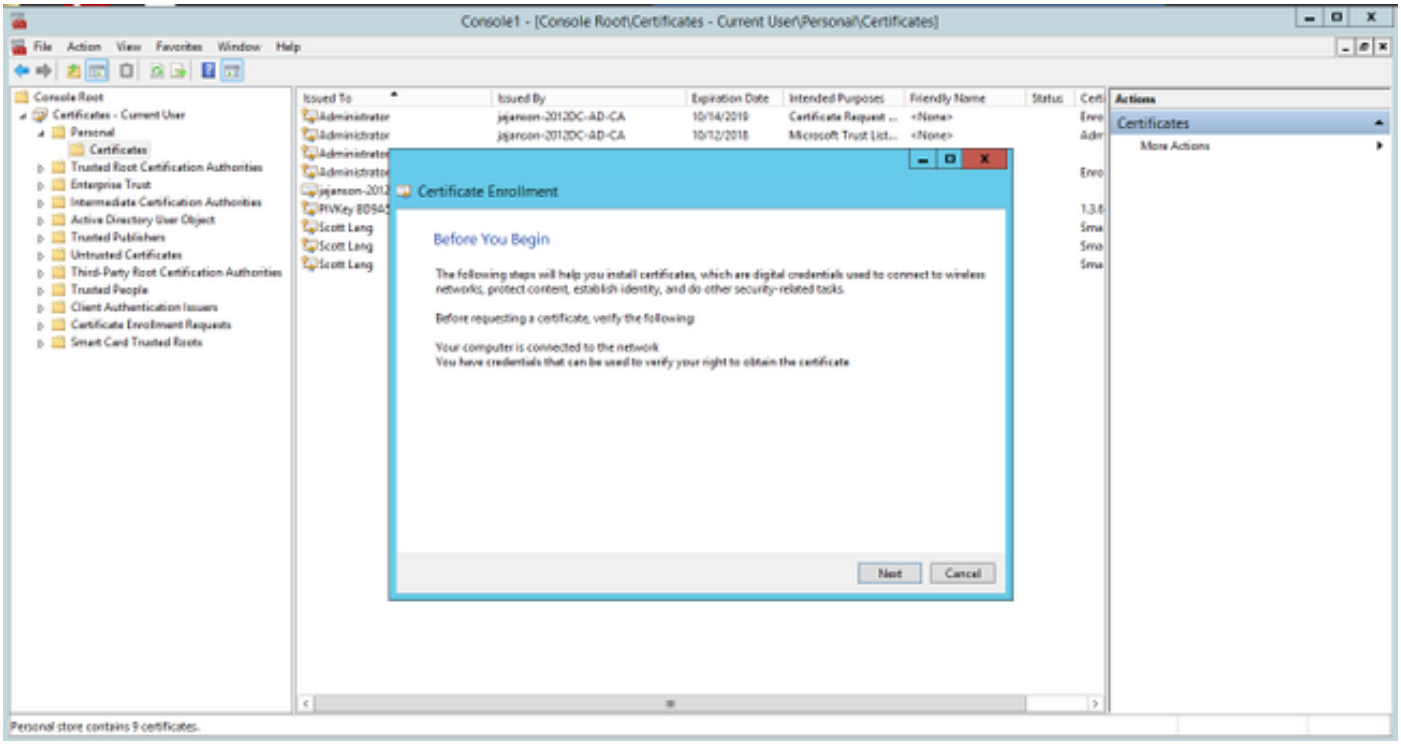
1. MMCを起動し、**Certificates Module & Managerをインポートし、マイユーザアカウントの証明書をインポートします。**

2.右クリックするか、「個人」>「証明書」を選択して、「すべてのタスク」>**「詳細操作」を選択し、「代理で登録」をクリックします。**

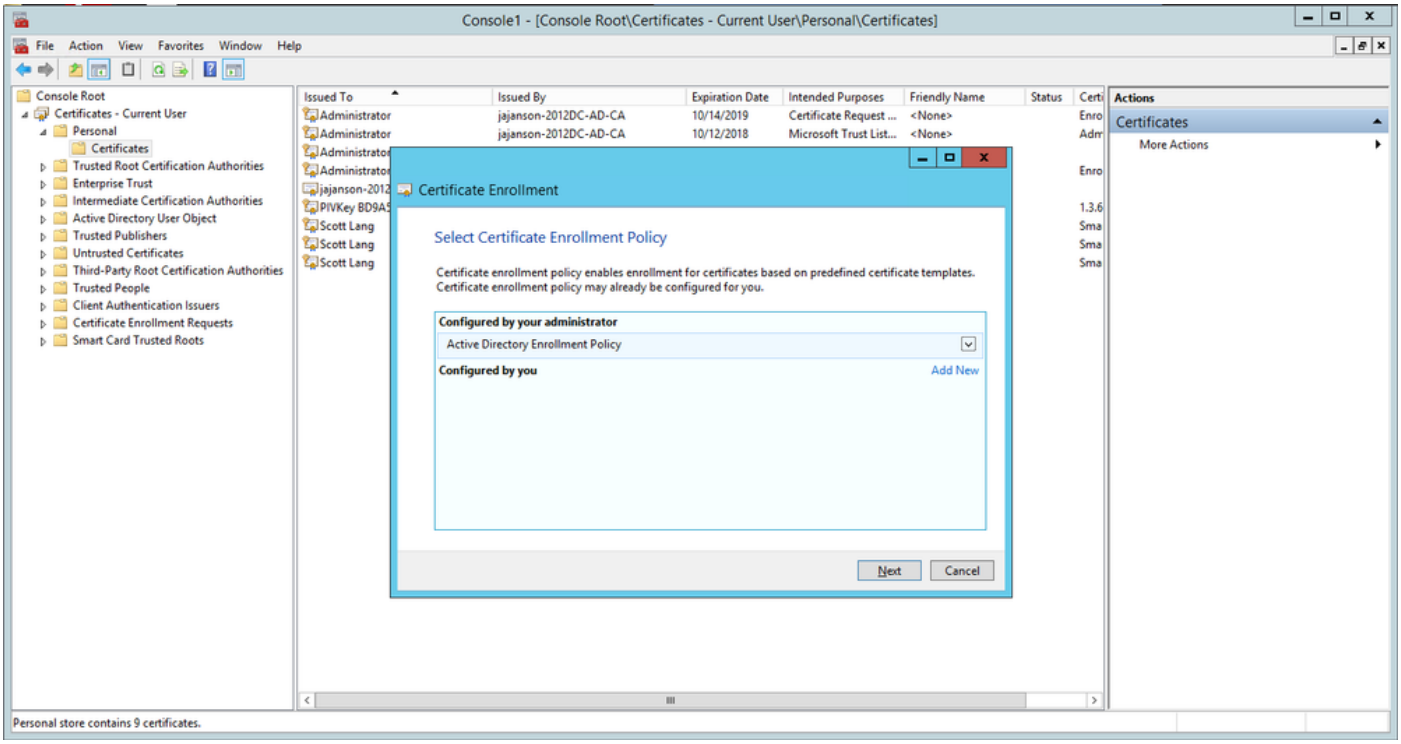
3.ウィザードで、[Active Directory Enrollment Policy]を選択し、[Next]をクリックします。



代理登録の詳細設定

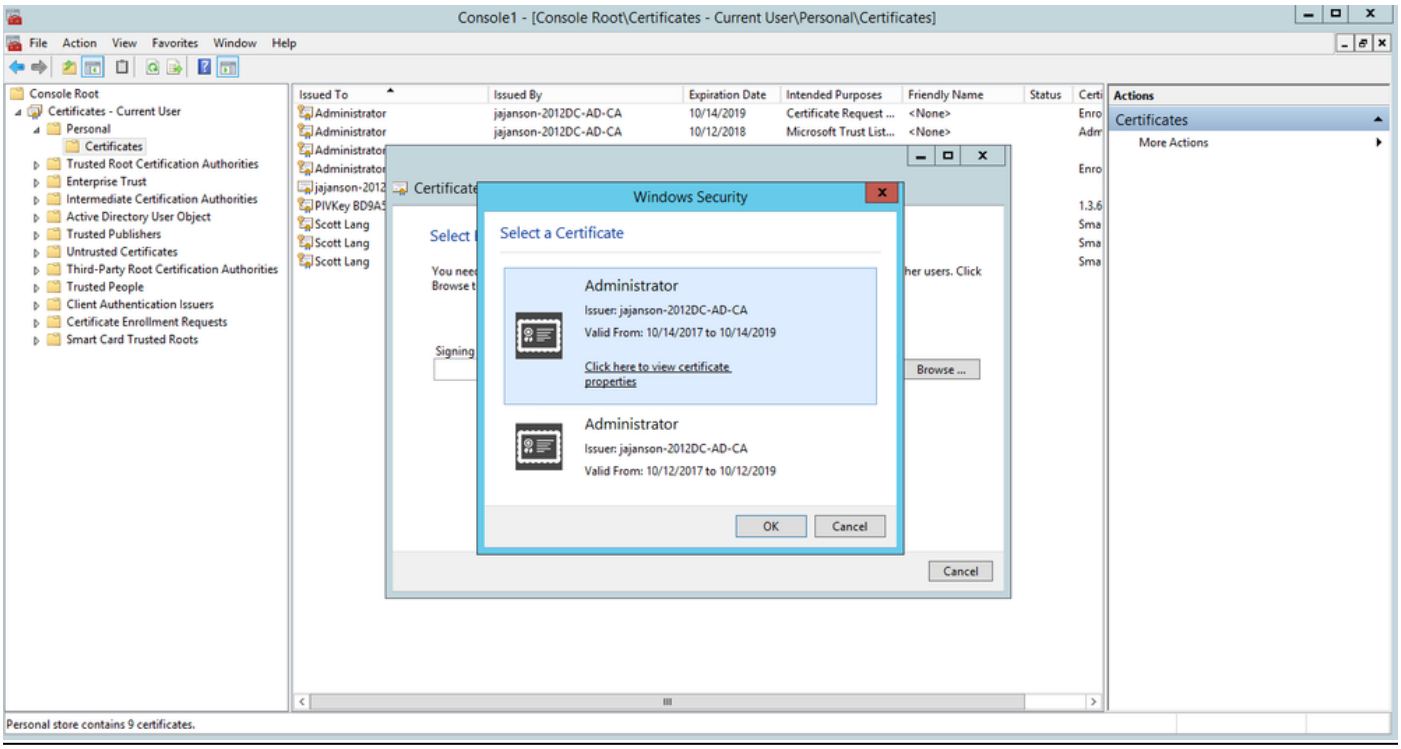


4. [Certificate Enrollment Policy]を選択し、**[Next]をクリックします。**



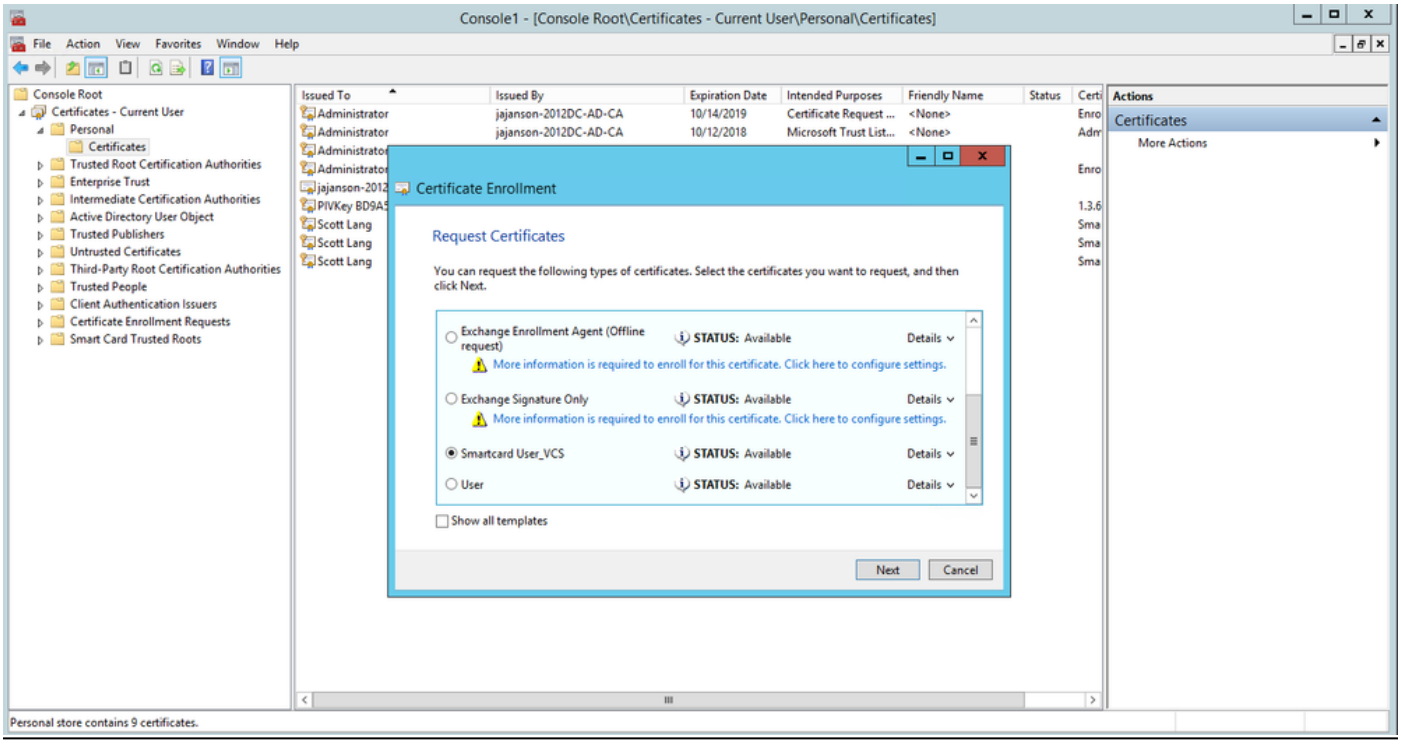
登録ポリシー

5.署名証明書の選択を求められました。これは、以前に要求した登録証明書です。



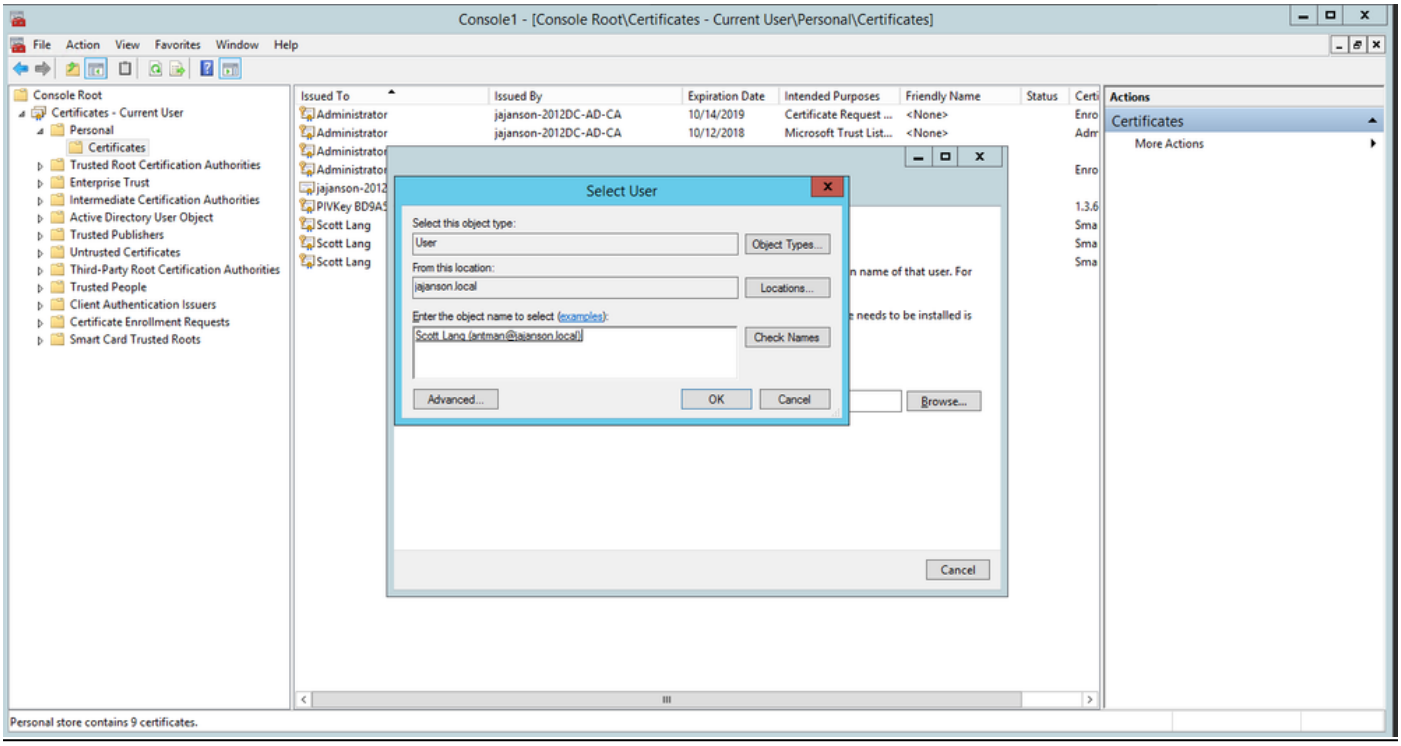
署名証明書の選択

6.次の画面で、要求する証明書を参照する必要があります。この例では、以前に作成したテンプレートであるSmartcard User_VCSです。



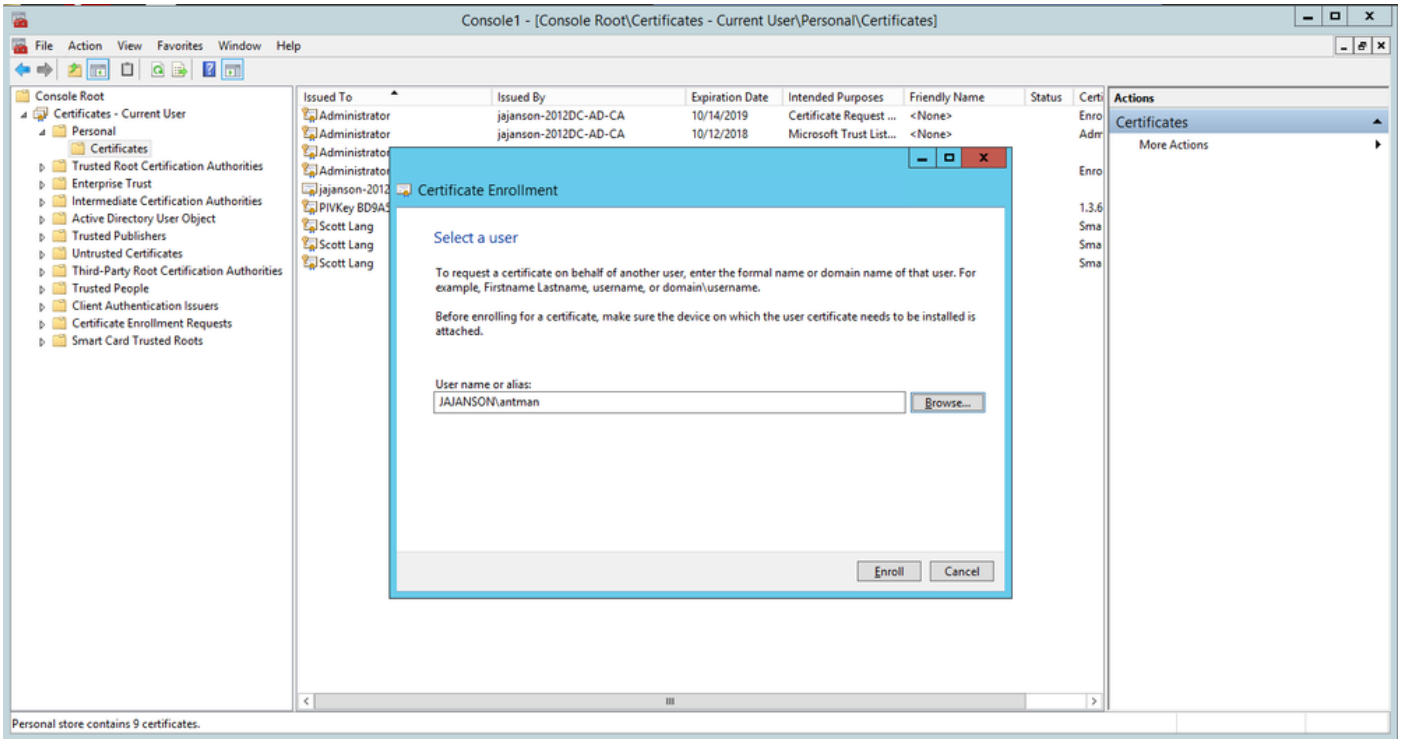
VCSスマートカードの選択

7.次に、に代わって登録するユーザを選択する必要があります。[参照]**をクリック**し、登録する従業員のユーザ名を入力します。この例では、Scott Lang 'antman@jajanson.local account'が使用されます。



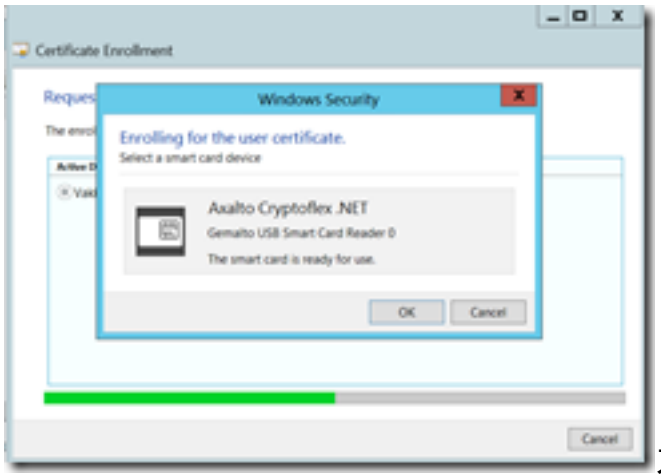
ユーザの選択

8. 次の画面で、[登録]をクリックして登録を続行します。今すぐに、スマートカードをリーダーに挿入します。



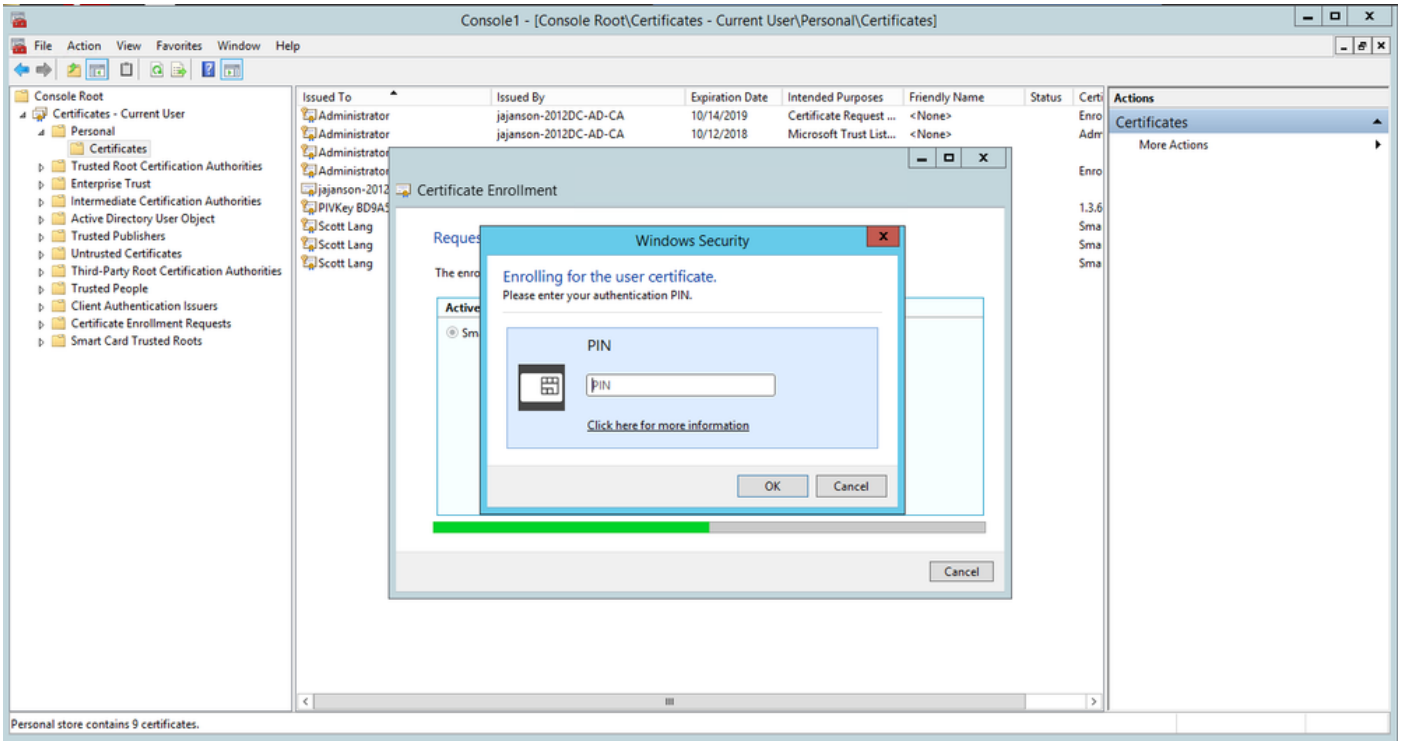
登録

9. スマートカードを挿入すると、次のように検出されます。



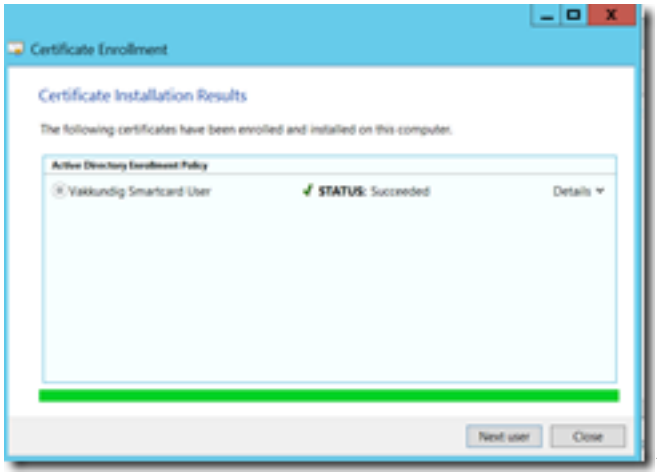
スマートカードの挿入

10. 次に、スマートカードの暗証番号（デフォルトの暗証番号）を入力するように求められます。：0000）。



ピンを入力します

11. [Enrollment Successful]画面が表示されたら、このスマートカードを使用して、ドメインに参加しているサーバ（カードと既知のPINのみを持つVCSなど）にログオンできます。ただし、VCSを準備して認証要求をスマートカードにリダイレクトし、共通アクセスカードを使用してスマートカードに保存されているスマートカード証明書を認証のために解放する必要があります。



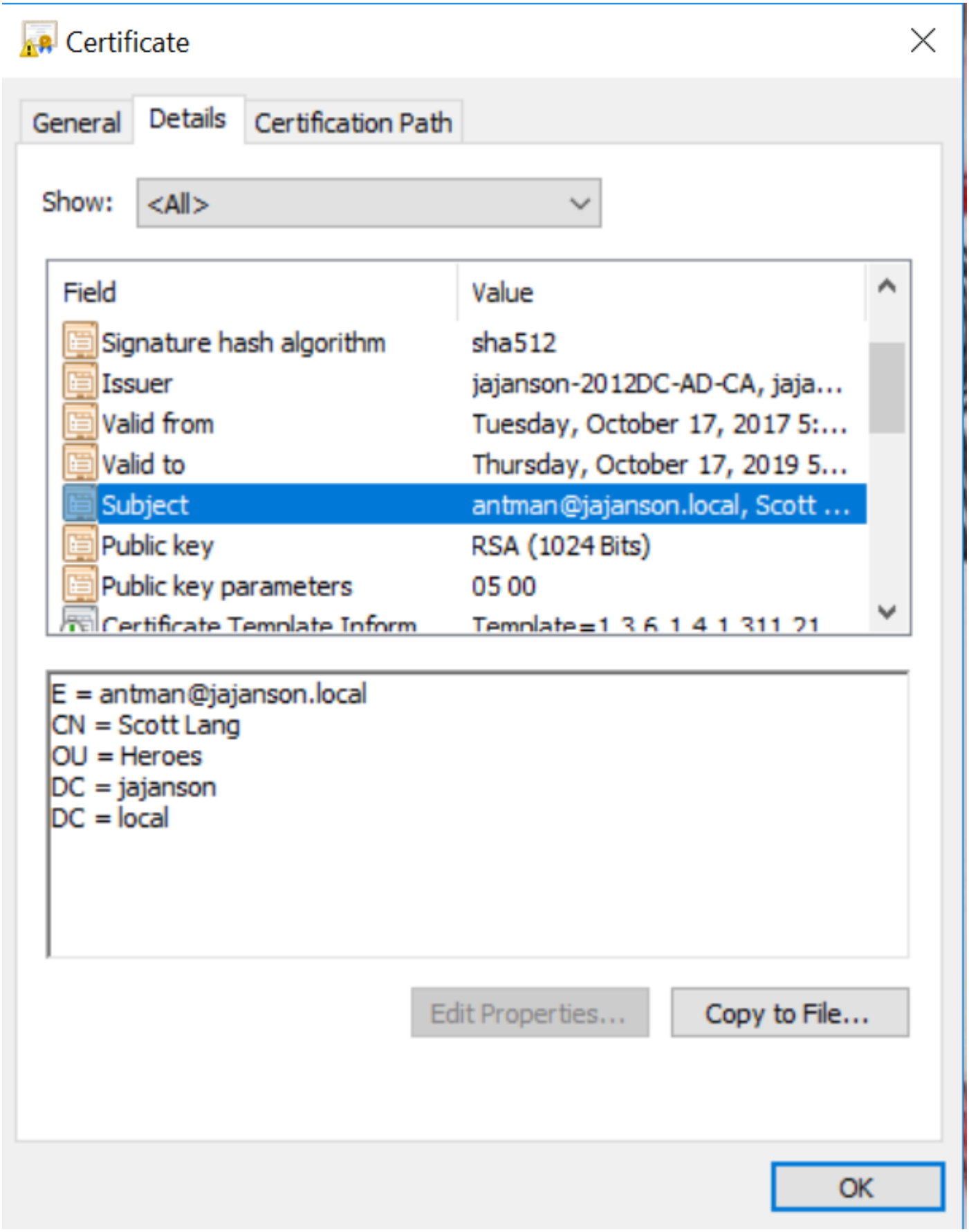
登録に成功しました

共通アクセスカード用のVCSの設定

[Maintenance] > [Security] > [Trusted CA Certificate]の順に移動して、ルートCAをVCSの[Trusted CA Certificate]リストにアップロードします。

2.ルートCAによって署名された証明書失効リスト(CRL)をVCSにアップロードします。[Maintenance] > [Security] > [CRL Management]に移動します。

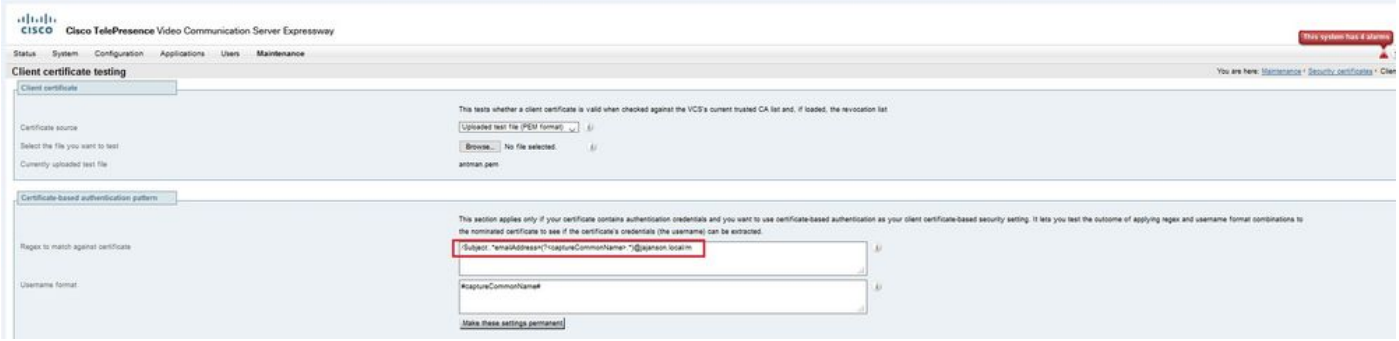
3. LDAPまたはローカルユーザに対する認証に使用するユーザ名を証明書から取得する正規表現に対してクライアント証明書をテストします。正規表現が証明書の件名と照合されます。これは、UPN、電子メールなどになります。この実習では、クライアント証明書のクライアント証明書と照合する電子メールを使用しました。



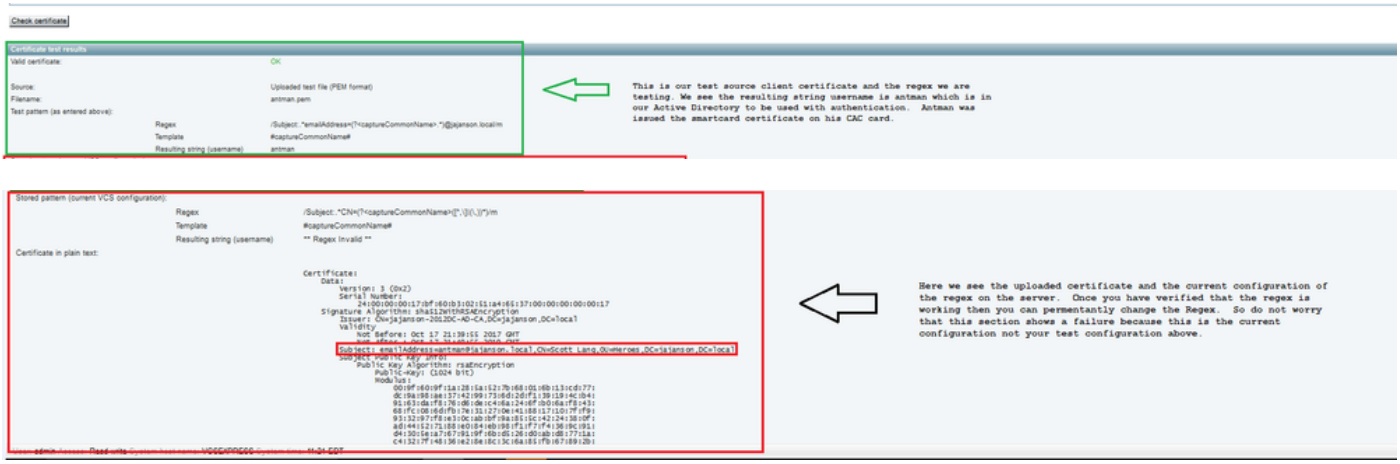
クライアント証明書の件名

4. [**Maintenance**] > [**Security**] > [**Client Certificate Testing**]**に移動します**。テスト対象のクライアント証明書を選択し、[My lab it was antman.pem]でテストエリアにアップロードします。[証明書ベースの**認証パターン**]**セクション**の[証明書**と照合する正規表現**]**で、テスト**対象の正規表現を貼り付けます。[ユーザー名の形式]フィールド**は変更しないで**ください。

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



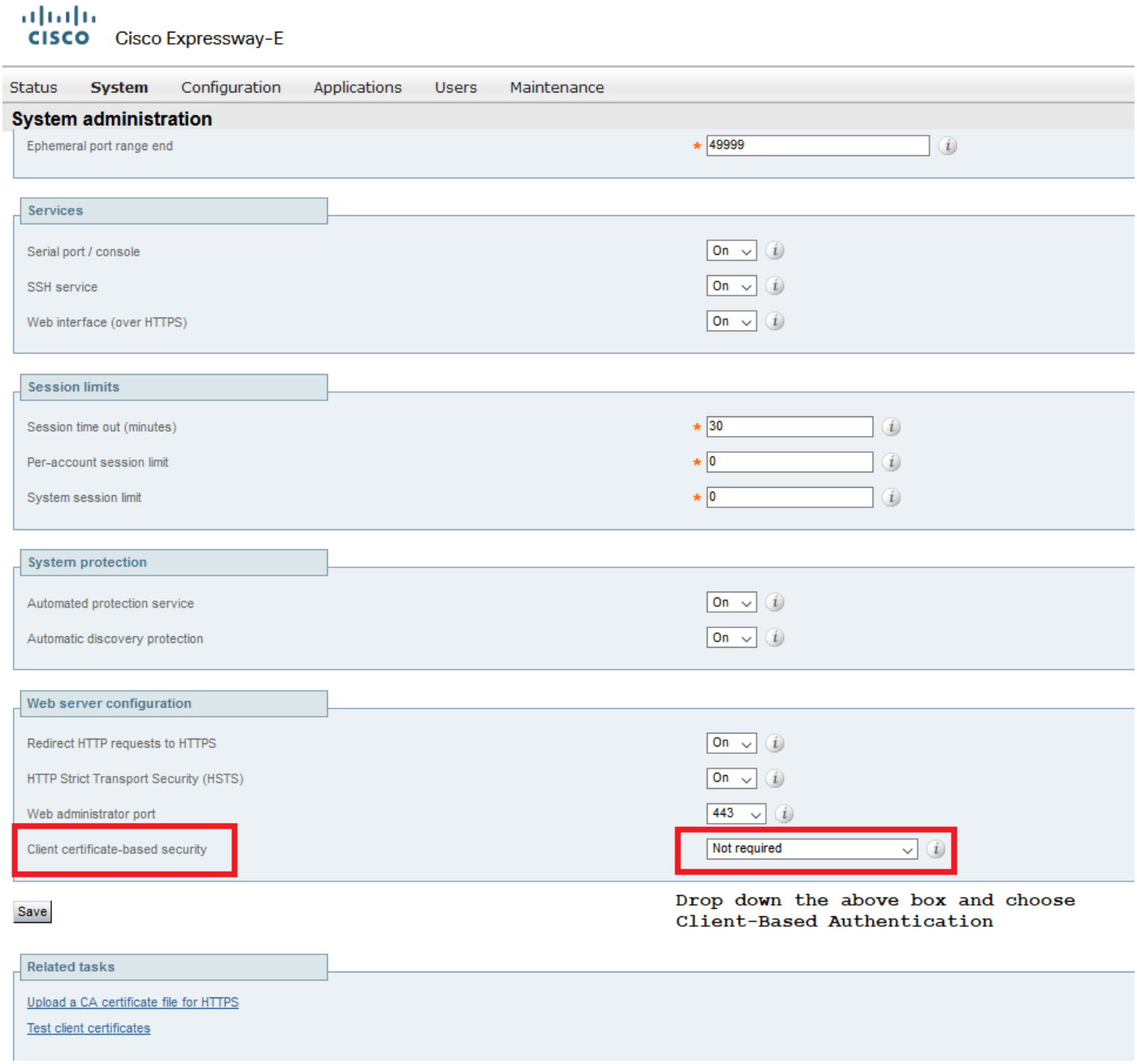
VCSでの正規表現のテスト



テスト結果

5.テストで目的の結果が得られる場合は、[Make these changes permanent]ボタンをクリックし**てください。**これにより、サーバの証明書ベースの**認証設定の正規表現が**変更されます。変更を確認するには、[Maintenace] > [Security] > [Certificate-based authentication configuration]**の設定に移動します。**

6. [System] > [Administrator]の順に移動し、ドロップダウンボックスをクリックまたは選択して**Client certificate-based security = Client-Based Authenticationを選択し、クライアントベース認証を有効にします。**この設定を使用すると、ユーザはブラウザでVCSサーバのFQDNを入力し、クライアントアカウントを選択して共通アクセスカードに割り当てられたPINを入力するよう求められます。その後、証明書がリリースされ、VCSサーバのWeb GUIが返されます。必要なのは、[Administrator]ボタンをクリックするか選択するだけです。その後、彼はサーバに入ります。オプションClient certificate-based security = Client-Based Validation**を選択した場**合、ユーザが[Administrator]ボタンをクリックした場合を除き、管理者パスワードの入力を再度求めるメッセージが表示されます。通常、後者は組織がCACを使用して達成しようとしているわけではありません。



クライアントベースの認証を有効にする

このサイトについて!ロックアウト!!!

クライアントベース認証を有効にして、VCSが何らかの理由で証明書を拒否すると、従来の方法でWeb GUIにログインできなくなります。しかし、システムに戻る方法があることを心配しないでください。添付のドキュメントはシスコのWebサイトにあり、クライアントベース認証をルートアクセスから無効にする方法について説明しています。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。