CAC 및 스마트 카드 리더로 VCS 구성

목차

소개

이 문서에서는 은행, 병원 또는 보안 시설이 있는 정부와 같은 VCS 환경에 2단계 인증을 필요로 하는 조직을 위해 Cisco VCS(Video Communication Server)와 함께 사용할 수 있도록 스마트 카드 리더와 공통 액세스 카드 로그인을 설치하고 사용하는 단계별 지침에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco Expressway 관리자(X14.0.2)을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

CAC는 필수 인증을 제공하므로 "시스템"은 환경에 대한 액세스 권한을 얻은 사람과 물리적 또는 전자 인프라를 통해 인프라의 어느 부분을 파악합니다. 정부 기밀 환경 및 기타 보안 네트워크 내에서 "최소한의 특권 액세스" 또는 "알아야 할 사항"의 규칙이 우선합니다. 로그인은 누구나 사용할 수 있으며, 인증에는 사용자가 가지고 있는 것을 필요로 하며, CAC(Common Access Card)라고도 하는 것이 2006년에 등장하여 직원이 직장 또는 시스템에 액세스하기 위해 포브, ID 카드 또는 동글처럼 여러 개의 장치를 가질 필요가 없도록 했습니다.

스마트 카드란?

스마트 카드는 클라이언트 인증, 로그온 및 보안 이메일과 같은 소프트웨어 전용 솔루션을 강화하기 때문에 Microsoft가 Windows 플랫폼에 통합하기 위해 사용하는 PKI(공개 키 인프라)의 핵심 구성 요소입니다. 스마트 카드는 다음과 같은 이유로 공개 키 인증서 및 관련 키를 통합합니다.

- 개인 키 및 기타 형태의 개인 정보 보호를 위해 변조 방지 스토리지를 제공합니다.
- 시스템 내 다른 부분으로부터 인증, 디지털 서명 및 키 교환이 포함되며 알 필요가 없는 보안 크리티컬 컴퓨팅을 격리합니다.
- 직장, 가정 또는 이동 중에 컴퓨터 간에 자격 증명 및 기타 개인 정보의 이동성을 지원합니다.

스마트 카드는 마우스나 CD-ROM을 도입하는 것과 같이 컴퓨터 업계에 혁명적이고 바람직한 새로운 기능을 제공하기 때문에 스마트 카드가 윈도우 플랫폼의 필수적인 부분이 되었다. 현재 내부 PKI 인프라가 없는 경우 먼저 이를 확인해야 합니다. 이 문서에서는 이 문서에서 이 역할의 설치에 대해 다루지 않지만, 이 역할의 구현 방법에 대한 자세한 내용은 여기에서 확인할 수 있습니다. http://technet.microsoft.com/en-us/library/hh831740.aspx

구성

이 실습에서는 LDAP를 VCS와 이미 통합했으며 LDAP 자격 증명으로 로그인할 수 있는 사용자가 있다고 가정합니다.

1. 랩 장비
2. 스마트 카드 설치
3. 인증 기관 템플릿 구성
4. 등록 에이전트 인증서 등록
5. 다음에 대한 등록...
6. 공통 액세스 카드에 대한 VCS 구성

필수 장비:

다음 역할/설치 소프트웨어가 있는 Windows 2012R2 도메인 서버:

- 인증 기관
- Active Directory
- DNS
- 스마트 카드가 연결된 Windows PC
- vSEC: 스마트 카드를 관리하는 CMS K-Series 관리 소프트웨어:

Versa Card Reader 소프트웨어

스마트 카드 설치

스마트 카드 리더는 일반적으로 필요한 케이블을 연결하는 방법에 대한 지침을 제공합니다. 다음은 이 구성에 대한 설치 예입니다.

스마트 카드 판독기 장치 드라이버 설치 방법

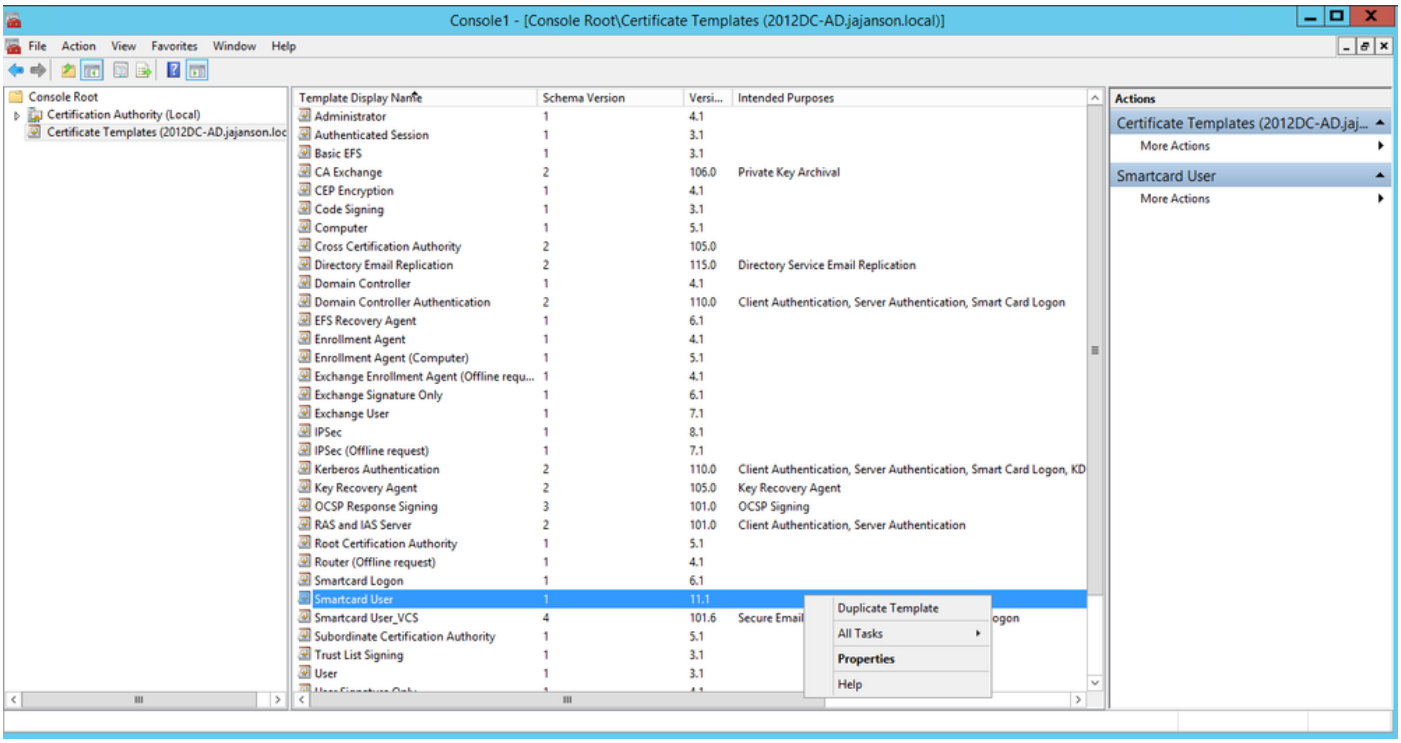
스마트 카드 판독기가 탐지되어 설치된 경우 Windows 로그온 시작 화면에서 이를 확인합니다. 그렇지 않은 경우:

1. 스마트 카드를 Windows PC의 USB 포트에 연결
2. 장치 드라이버 소프트웨어 설치에 대한 화면의 지침을 따릅니다. 이렇게 하려면 스마트 카드 또는 드라이버의 제조업체가 Windows에서 검색된 드라이버 미디어가 필요합니다. 내 경우에는 다운로드 사이트에서 제조 드라이버를 사용했습니다. **WINDOWS를 신뢰하지 마십시오**.
3. 바탕 화면에서 **내 컴퓨터** 아이콘을 마우스 오른쪽 단추로 클릭하고 하위 메뉴에서 **관리**를 클릭합니다.
4. 서비스 **및 애플리케이션** 노드를 확장하고 **서비스**를 클릭합니다.

5. 오른쪽 창에서 **스마트 카드**를 마우스 오른쪽 단추로 클릭합니다. 하위 메뉴에서 속성을 클릭합니다.
6. **General** 탭의 Startup Type 드롭다운 목록에서 **Automatic**을 선택합니다. **확인**을 **클릭합니다**.
7. 하드웨어 마법사가 지시하면 시스템을 재부팅합니다.

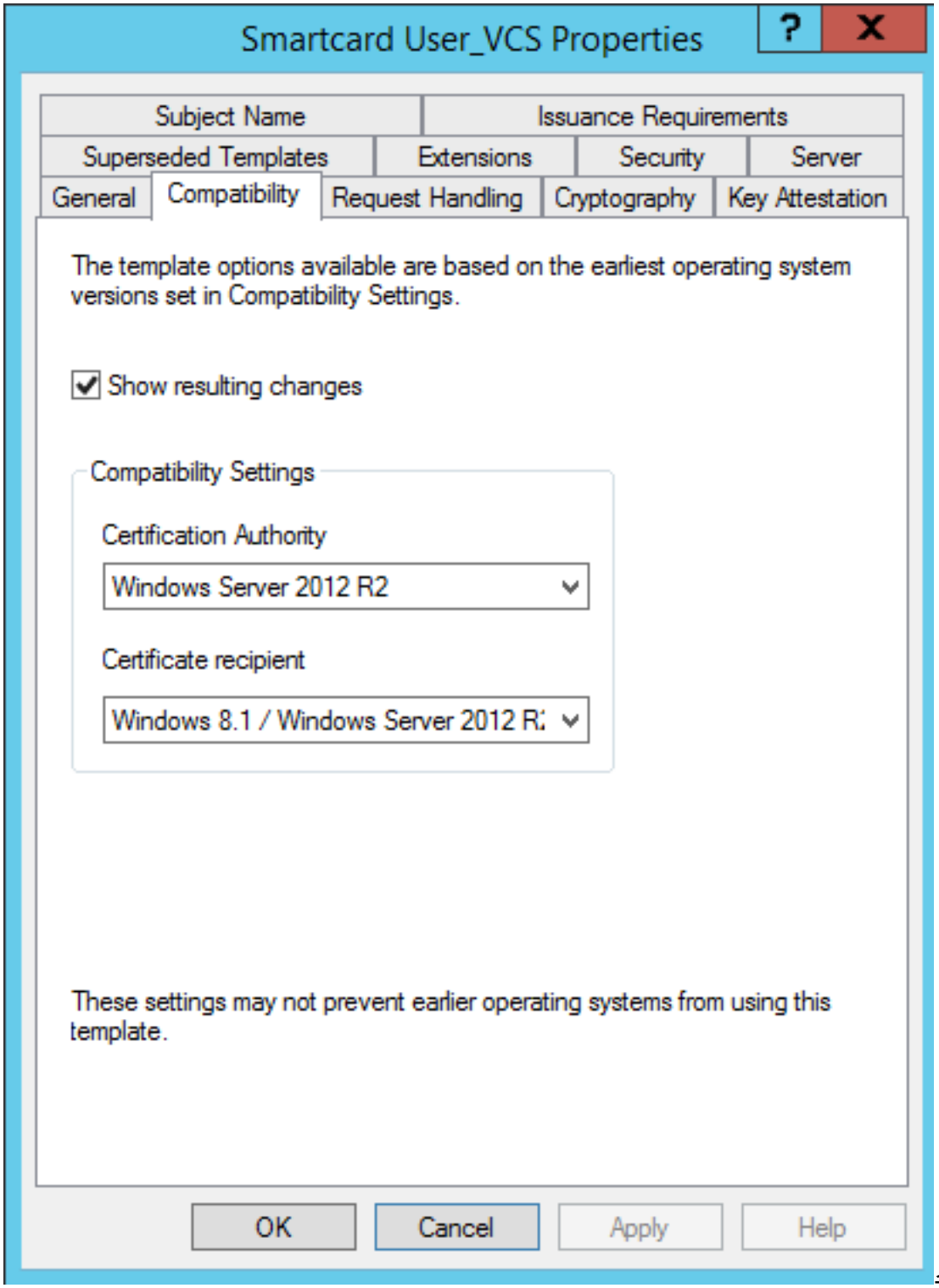
인증 기관 템플릿 구성

1. 관리 도구에서 인증 기관 MMC를 시작합니다.
2. Certificate Templates(**인증서 템플릿**) 노드를 클릭하거나 선택하고 Manage(관리)를 **선택합니다**.
3. 스마트 카드 **사용자** 인증서 템플릿을 마우스 오른쪽 단추로 클릭하거나 선택한 다음 이미지에 표시된 대로 복제를 선택합니다.



도메인 컨트롤러 인증서 템플릿

4. **호환성** 탭의 **인증 기관**에서 선택 사항을 검토하고 필요한 경우 변경합니다.

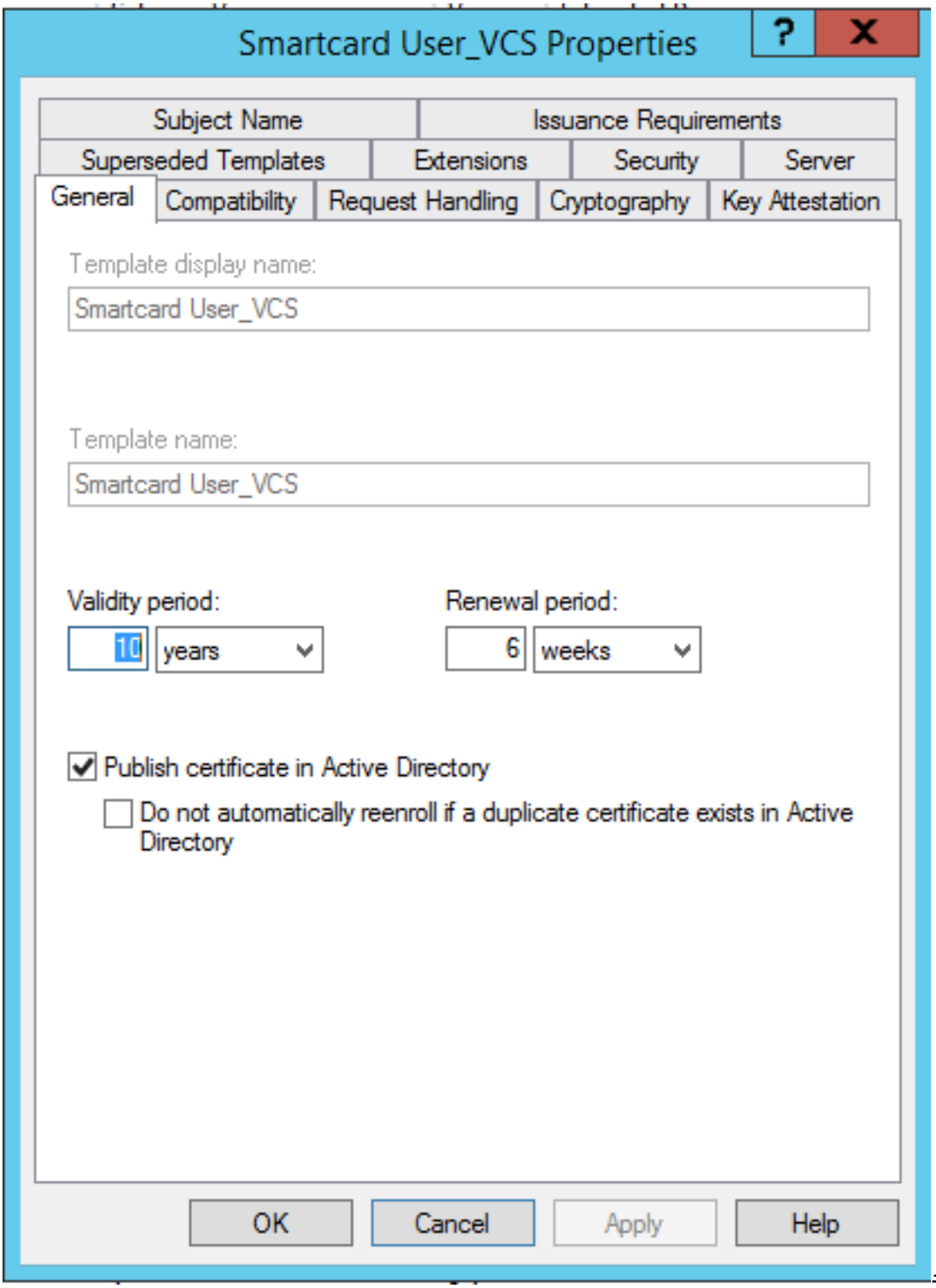


스마트 카드 호환성 설정

5. **일반** 탭

a. Smartcard **User_VCS**와 같은 이름**을 지정합니다**.

b. 유효 기간을 원하는 값으로 설정합니다. Apply를 **클릭합니다**.

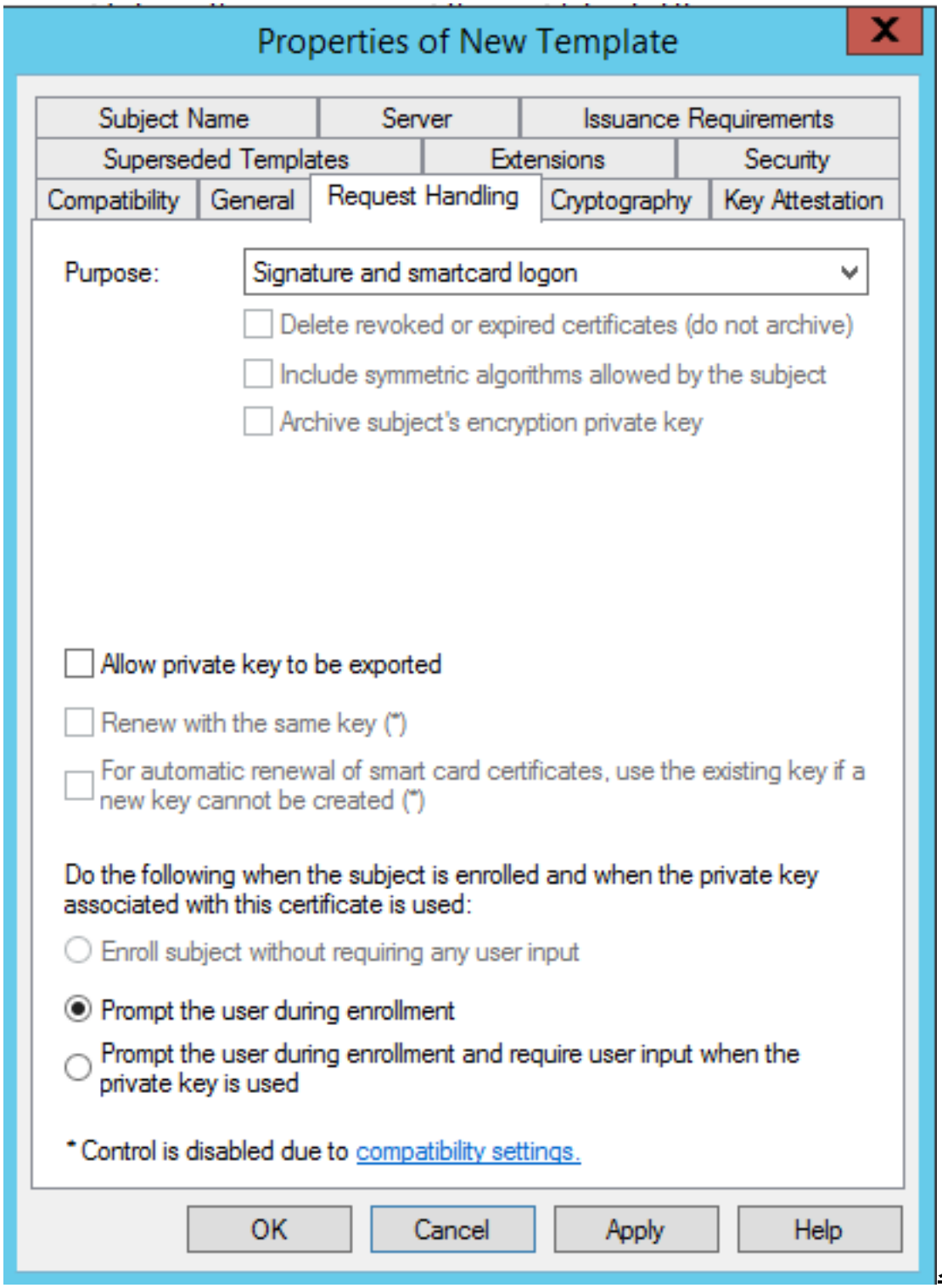


스마트 카드 일반 시간 만료

6. **요청 처리** 탭

a. Purpose를 **Signature**(서명) **및 smartcard logon(스마트 카드 로그온)으로 설정합니다**.

b. 등록 **중에 사용자에게 프롬프트를 클릭합니다.** Apply를 **클릭합니다**.

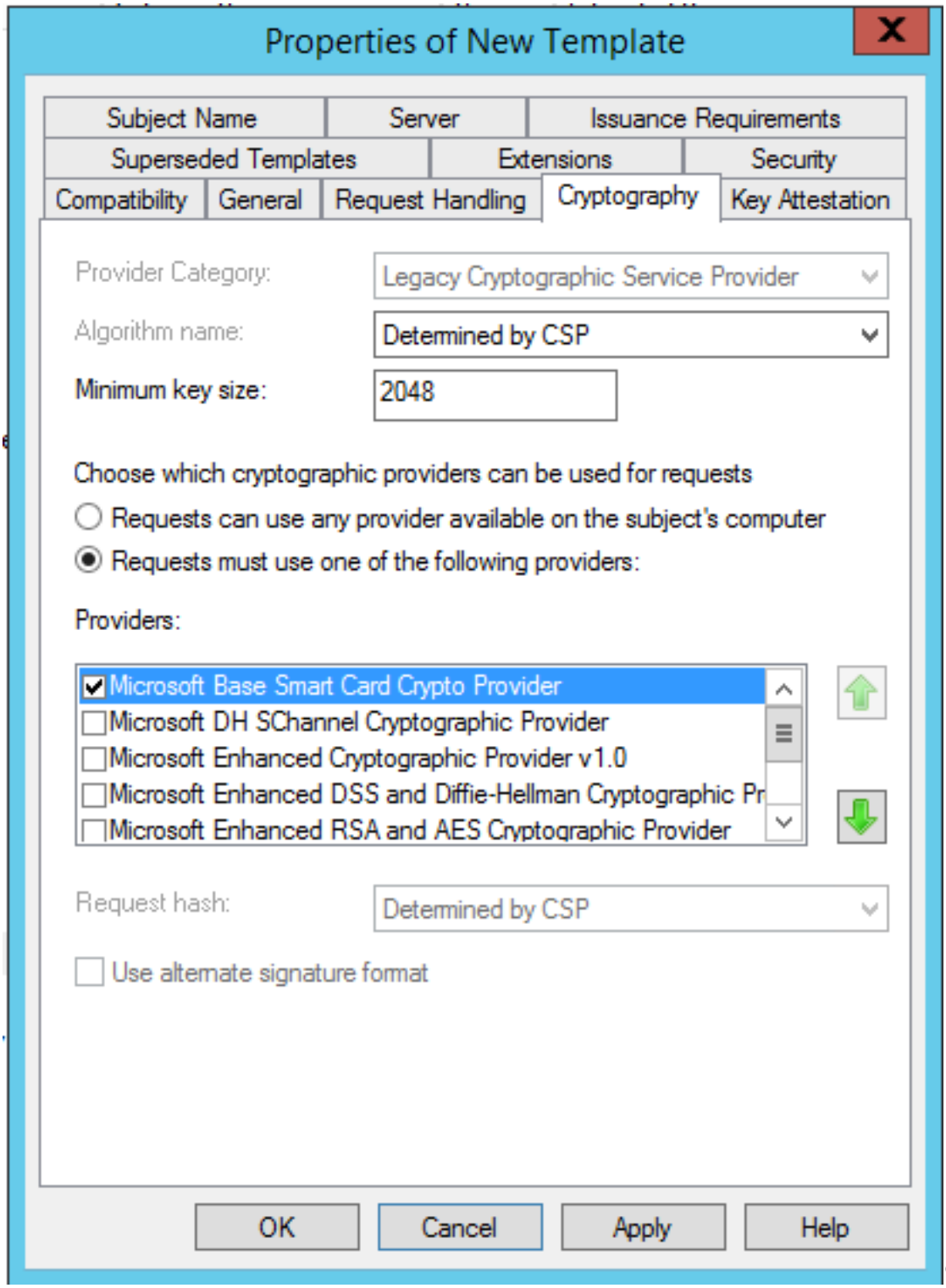


스마트 카드 요청 처리

7. **Cryptography** 탭에서 최소 키 크기를 2048로 설정합니다.

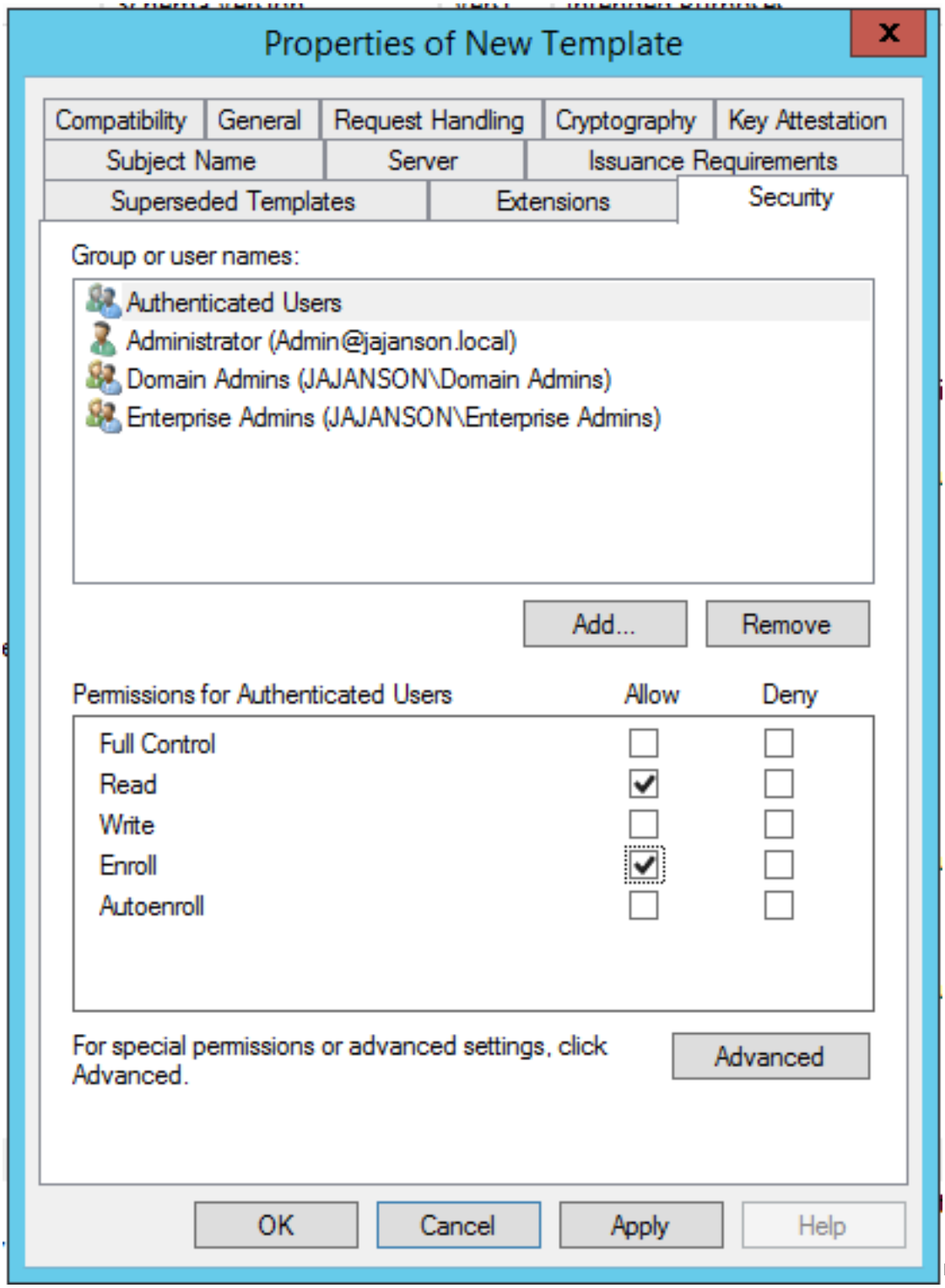
a. Requests must use **the following providers(요청에서 다음 공급자 중 하나를 사용해야 함)**를 클릭한 다음 **Microsoft Base Smart Card Crypto Provider**를 선택합니다.

b. 적용을 **클릭합니다**.



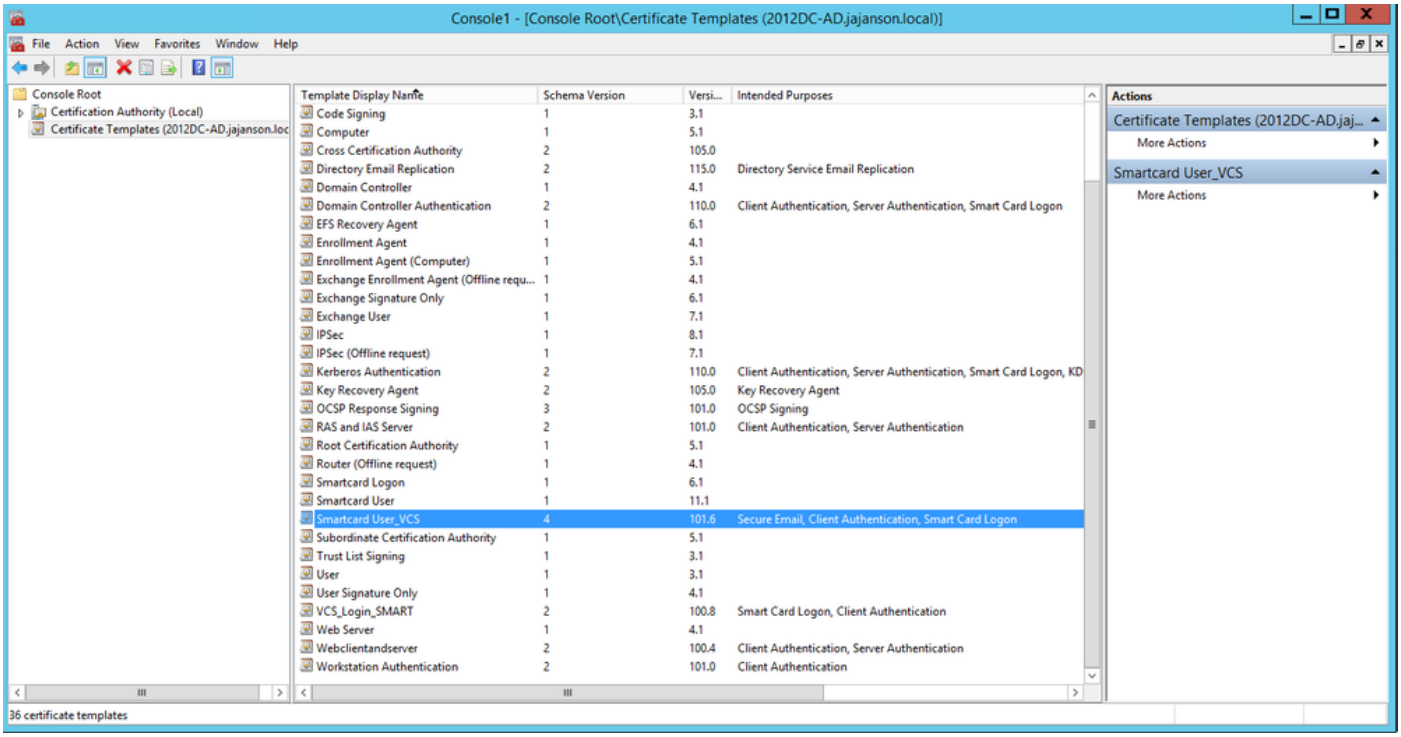
인증서 암호화 설정

8. 보안 탭에서 등록 액세스 권한을 부여할 보안 그룹을 추가합니다. 예를 들어, 모든 사용자에게 액세스 권한을 부여하려면 Authenticated users(인증된 사용자) 그룹을 선택한 다음 **Enroll** permissions(권한 등록)를 선택합니다.



템플릿 보안

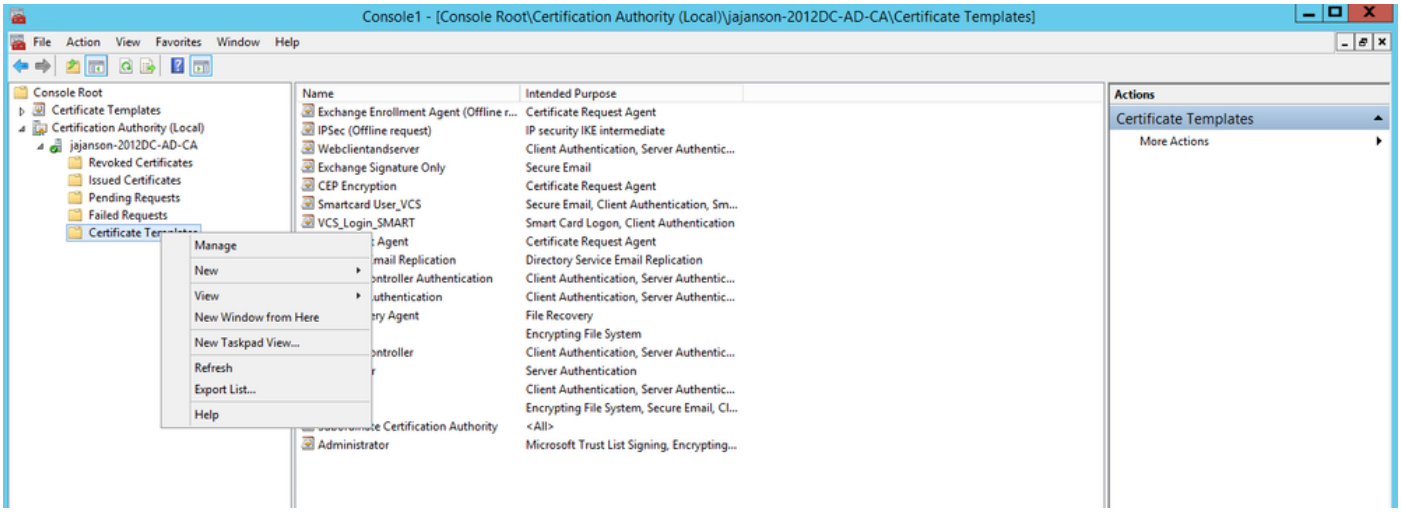
9. **확인**을 클릭하여 변경 사항을 완료하고 새 템플릿을 생성합니다. 이제 새 템플릿이 인증서 템플릿 목록에 나타나야 합니다.



도메인 제어에 표시되는 템플릿

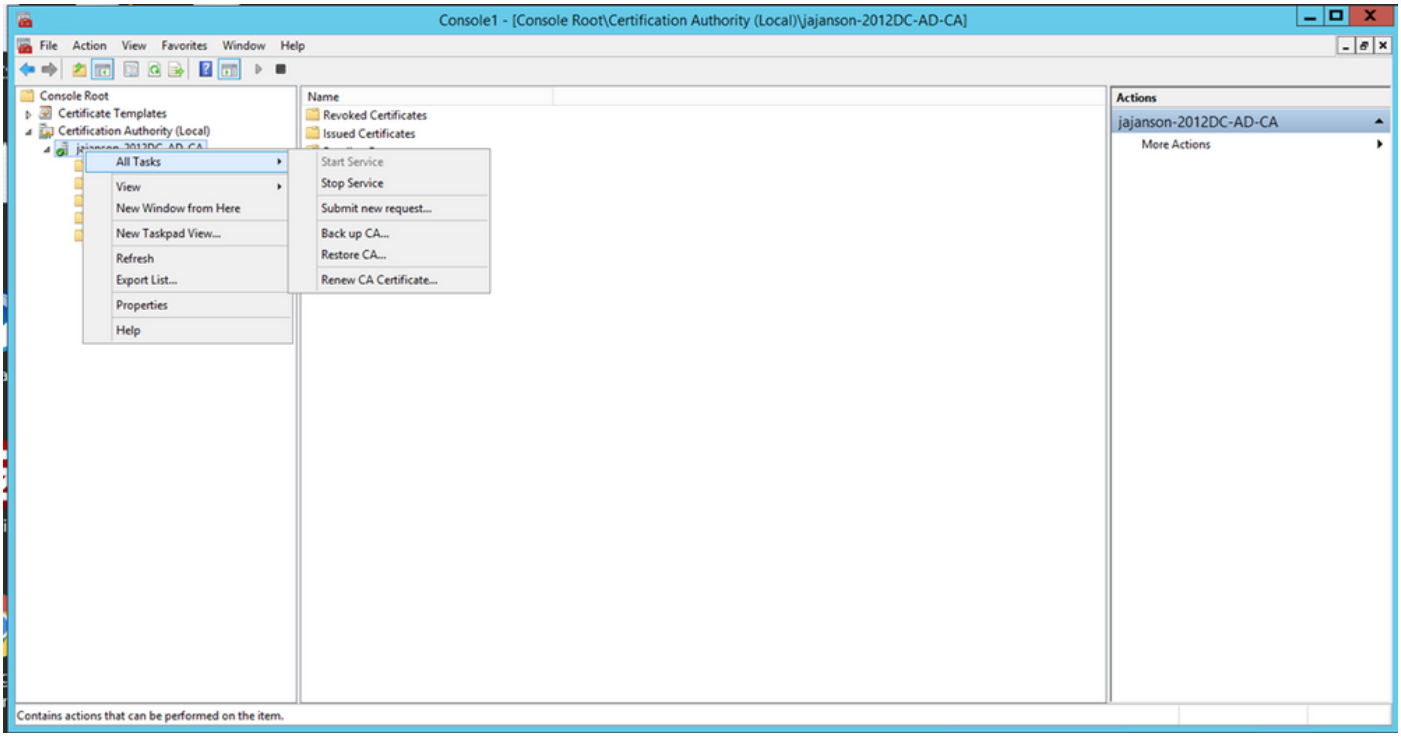
10. MMC의 왼쪽 창에서 인증 기관(로컬)을 확장한 다음 인증 기관 목록에서 CA를 확장합니다.

Certificate Templates(인증서 템플릿)를 마우스 오른쪽 버튼으로 클릭하고 **New(새로 만들기)**를 클릭한 다음 **Certificate Template to Issue(발급할 인증서 템플릿)**를 클릭합니다. 그런 다음 새로 생성된 스마트카드 템플릿을 선택합니다.



새 템플릿 문제

11. 템플릿이 복제되면 MMC에서 인증 기관 목록을 마우스 오른쪽 단추로 클릭하거나 선택한 다음 **모든 작업**을 클릭한 다음 **서비스 중지를** 클릭합니다. 그런 다음 CA의 이름을 다시 마우스 오른쪽 단추로 클릭하고 **모든 작업**을 클릭한 다음 **서비스 시작 을** 클릭합니다.

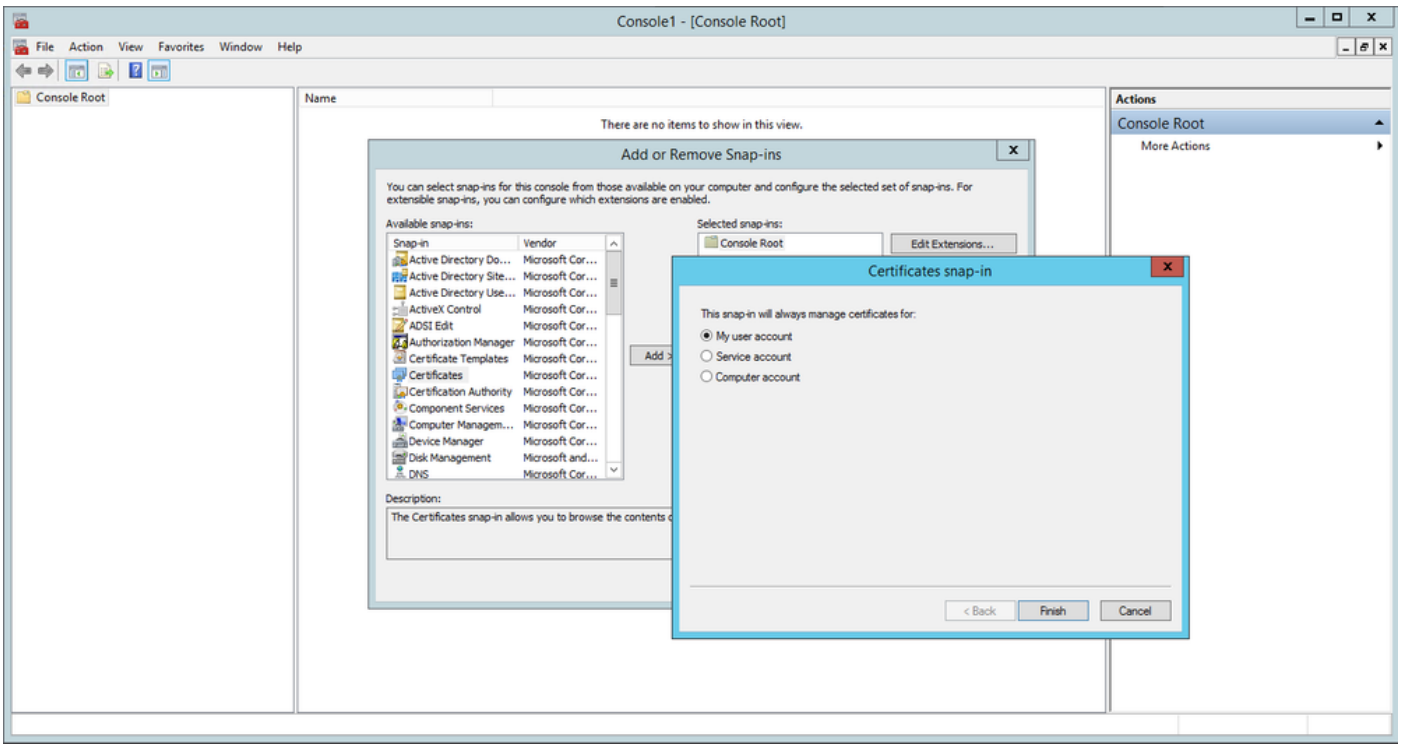


인증서 서비스 중지 후 시작

등록 에이전트 인증서에 등록

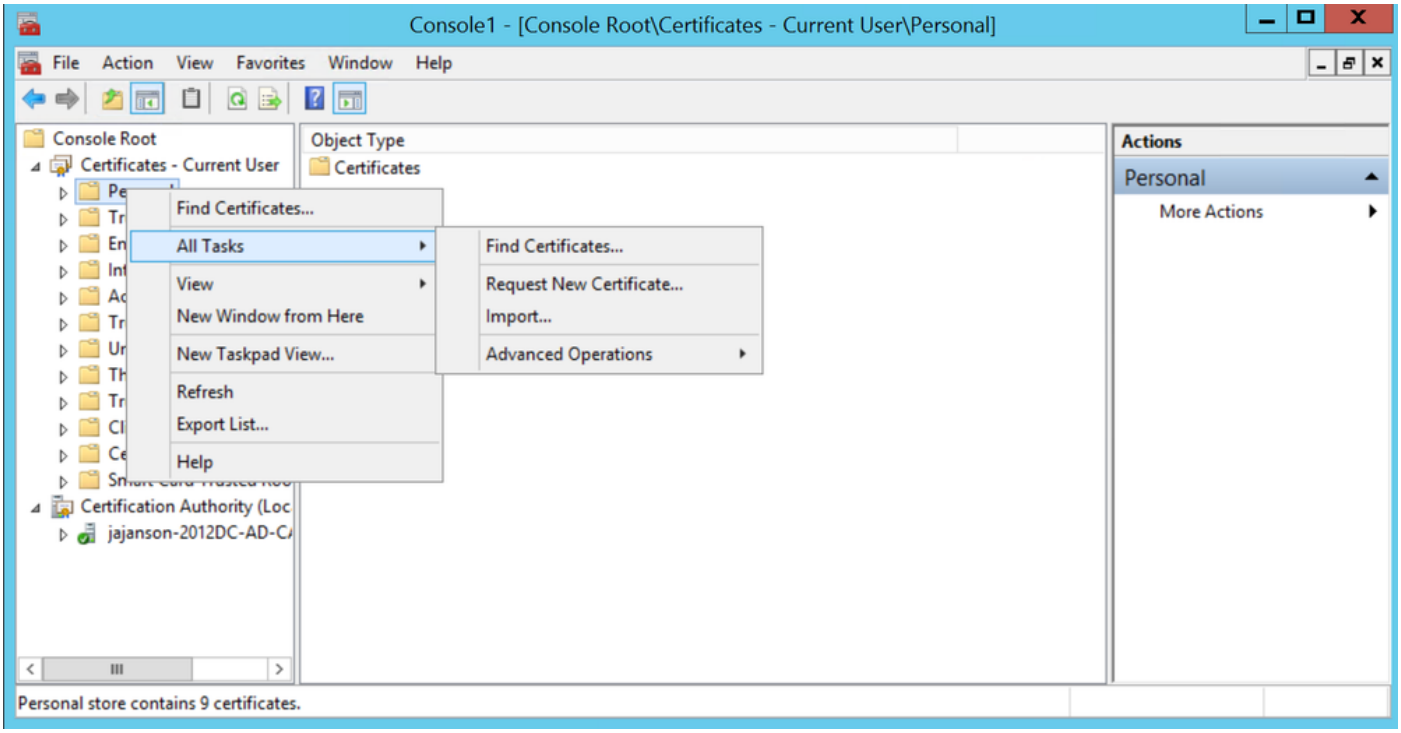
클라이언트 시스템(IT 관리자 데스크톱)에서 이 작업을 수행하는 것이 좋습니다.

1. MMC를 실행하여 **인증서**를 선택하고 **추가**를 클릭한 다음 **내 사용자 계정에 대한 인증서**를 선택합니다.



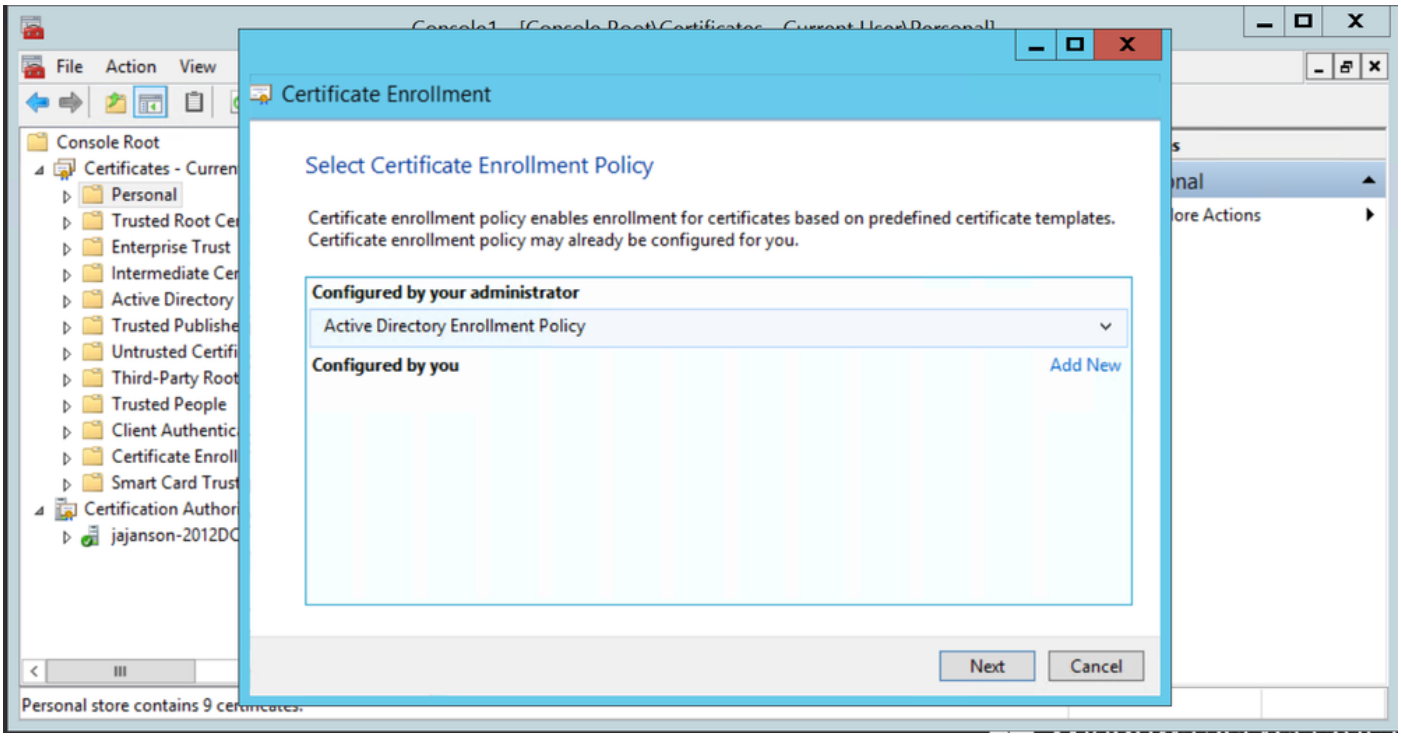
인증서 추가

2 . 마우스 오른쪽 단추를 클릭하거나 **개인 노드**를 선택하고 **모든 작업**을 선택한 다음 **새 인증서 요청**을 **선택합니다**.



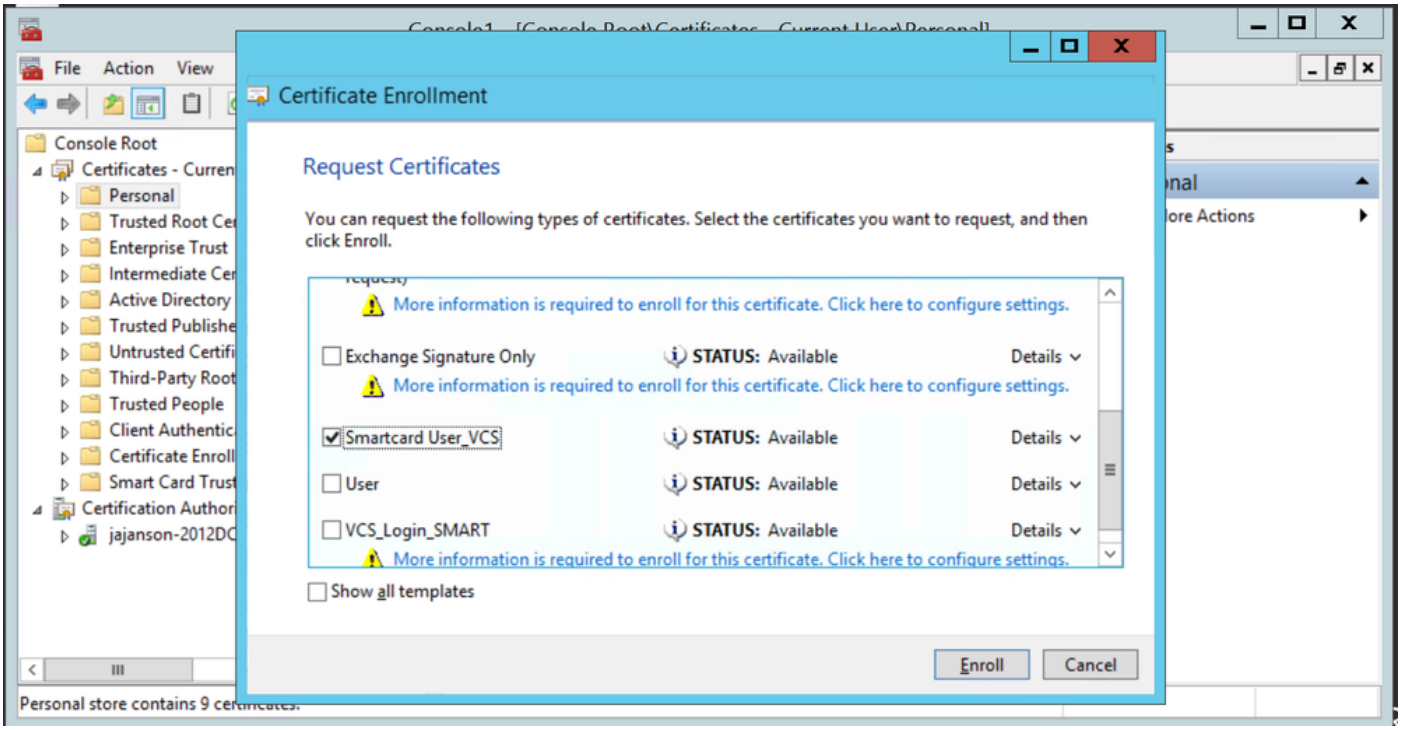
새 인증서 요청

3. 마법사에서 [다음]을 클릭한 다음 **Active Directory 등록 정책을** 선택합니다. 그런 다음 **Next(다음)를** 다시 클릭합니다.



Active Directory 등록

4. 등록 **에이전트 인증서**(이 경우 **Smartcard User_VCS)를** 선택한 다음 등록을 **클릭합니다.**

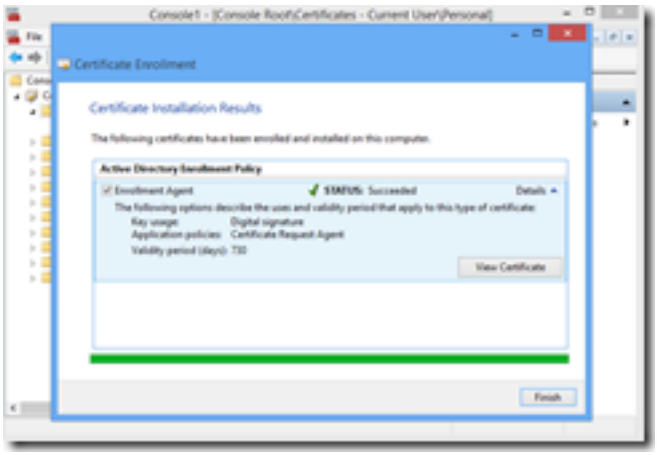


등록 인증서 에이전트

이제 IT 관리자 데스크탑이 등록 스테이션으로 설정되어 있으므로 다른 사용자를 대신하여 새 스마트 카드를 등록할 수 있습니다.

다음에 대한 등록...

이제 직원에게 인증을 위한 스마트카드를 제공하려면 이를 등록하고 인증서를 생성해야 합니다. 이 인증서는 스마트 카드로 가져옵니다.

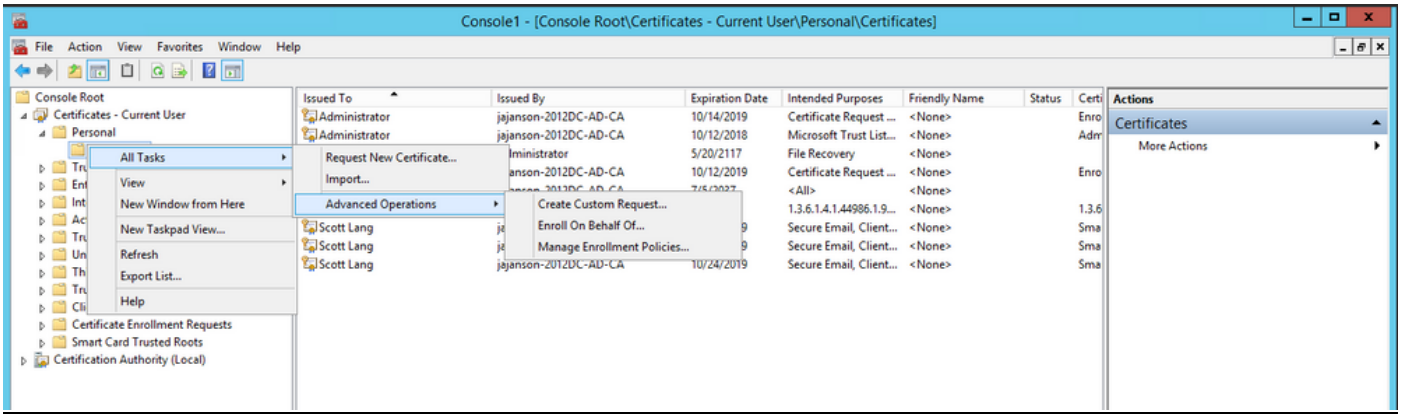


다음에 대한 등록

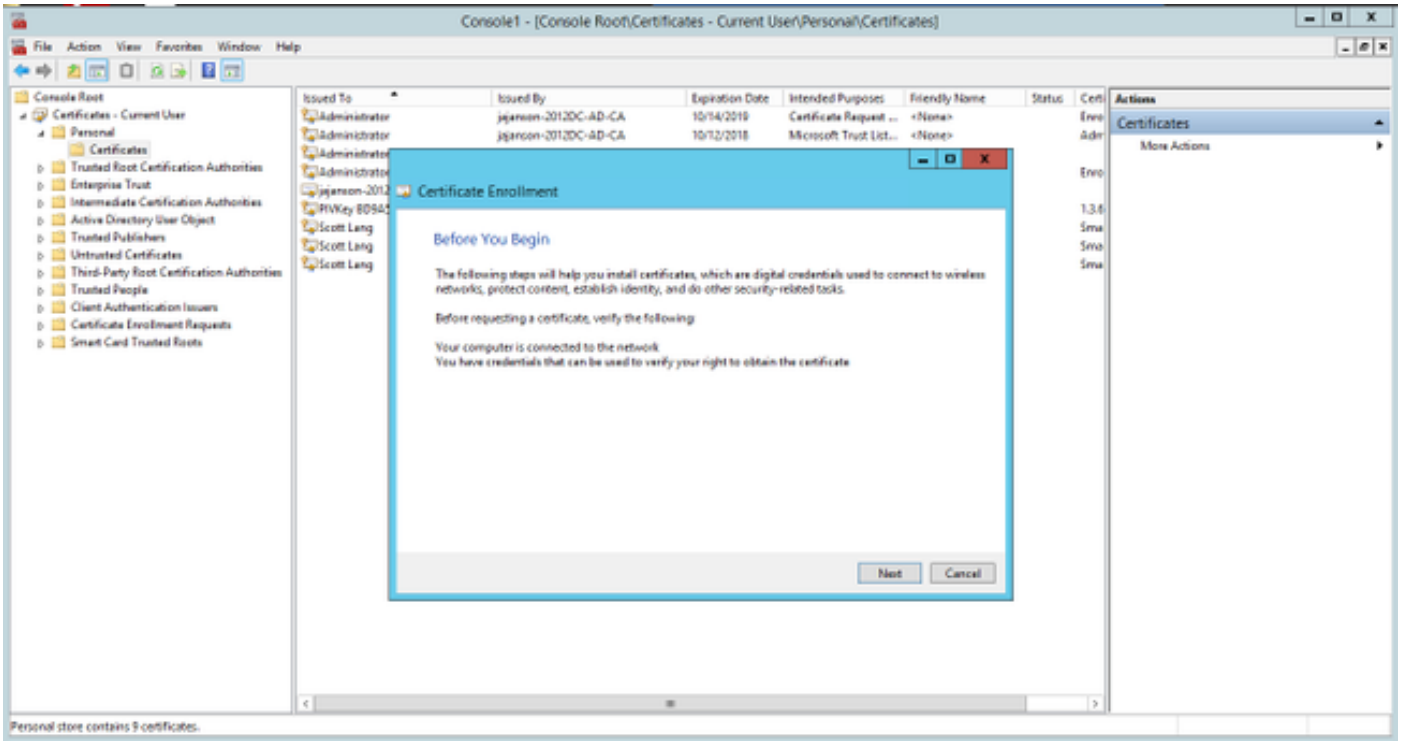
1. MMC를 시작하고 **인증서 모듈 및 관리자**를 내 사용자 계정에 대한 인증서를 가져옵니다.

2. 마우스 오른쪽 단추를 누르거나 **개인 > 인증서**를 선택하고 **모든 태스크 > 고급 작업**을 선택하고 **등록**을 **클릭합니다.**

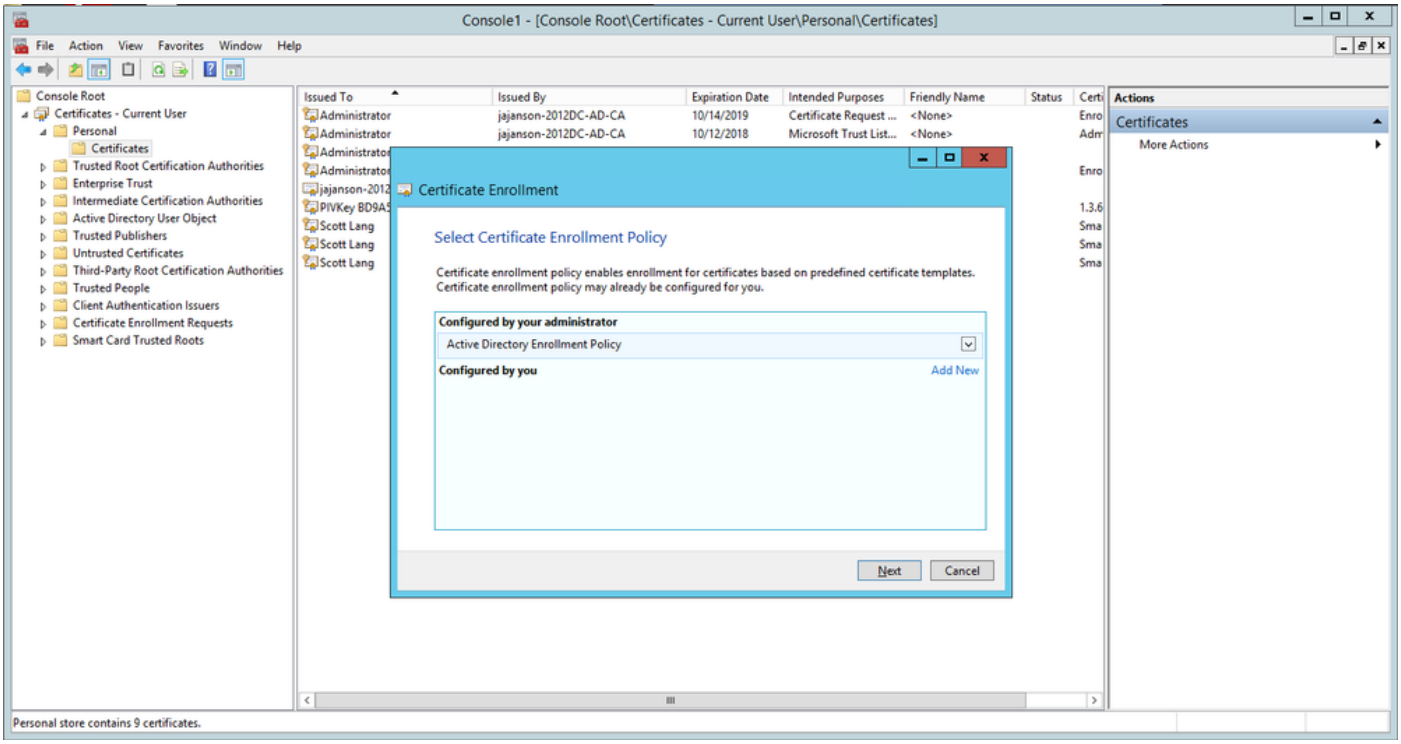
3. 마법사에서 Active Directory 등록 정책을 선택한 다음 **다음**을 클릭합니다.



고급 대신 등록

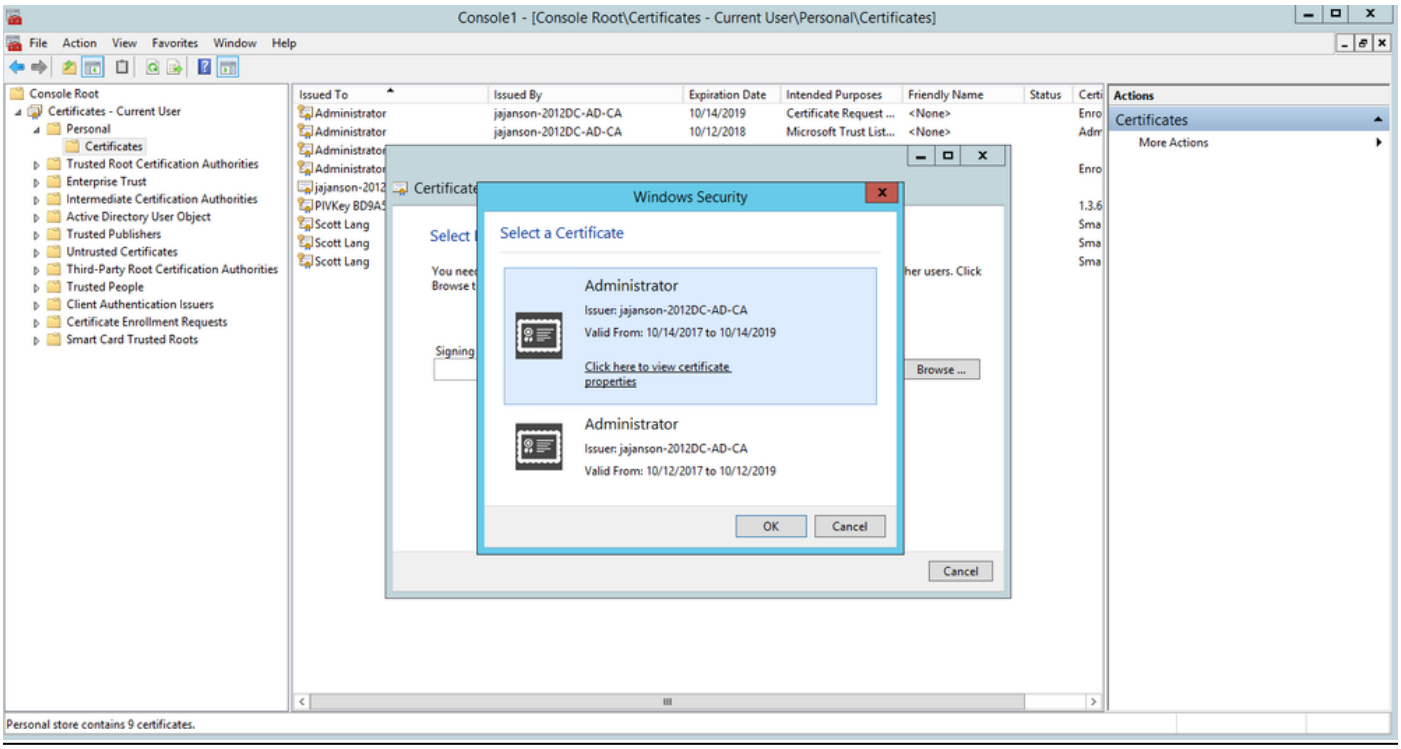


4. Certificate Enrollment Policy(인증서 등록 정책)를 선택한 다음 **Next(다음)**를 클릭합니다.



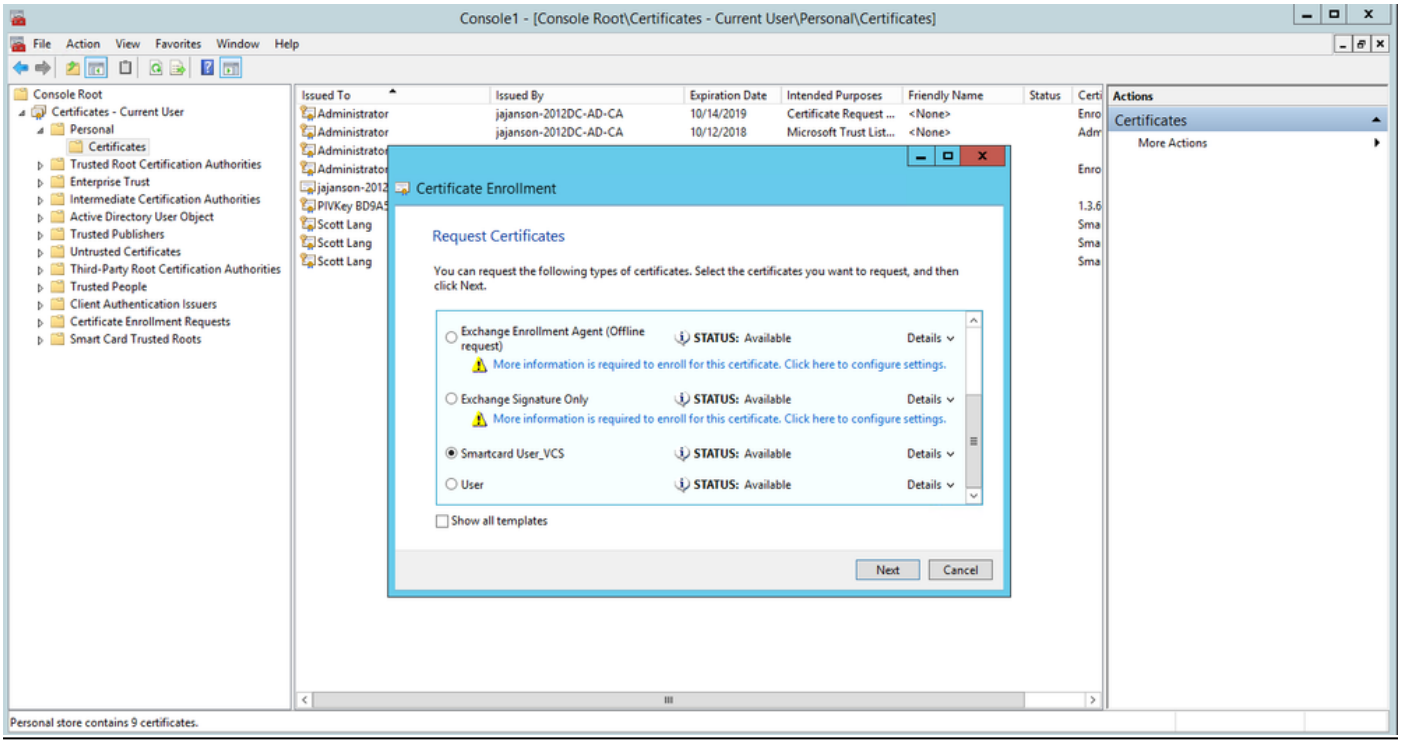
등록 정책

5. 이제 **서명 인증서**를 선택하라는 메시지가 표시됩니다. 이는 이전에 요청한 등록 인증서입니다.



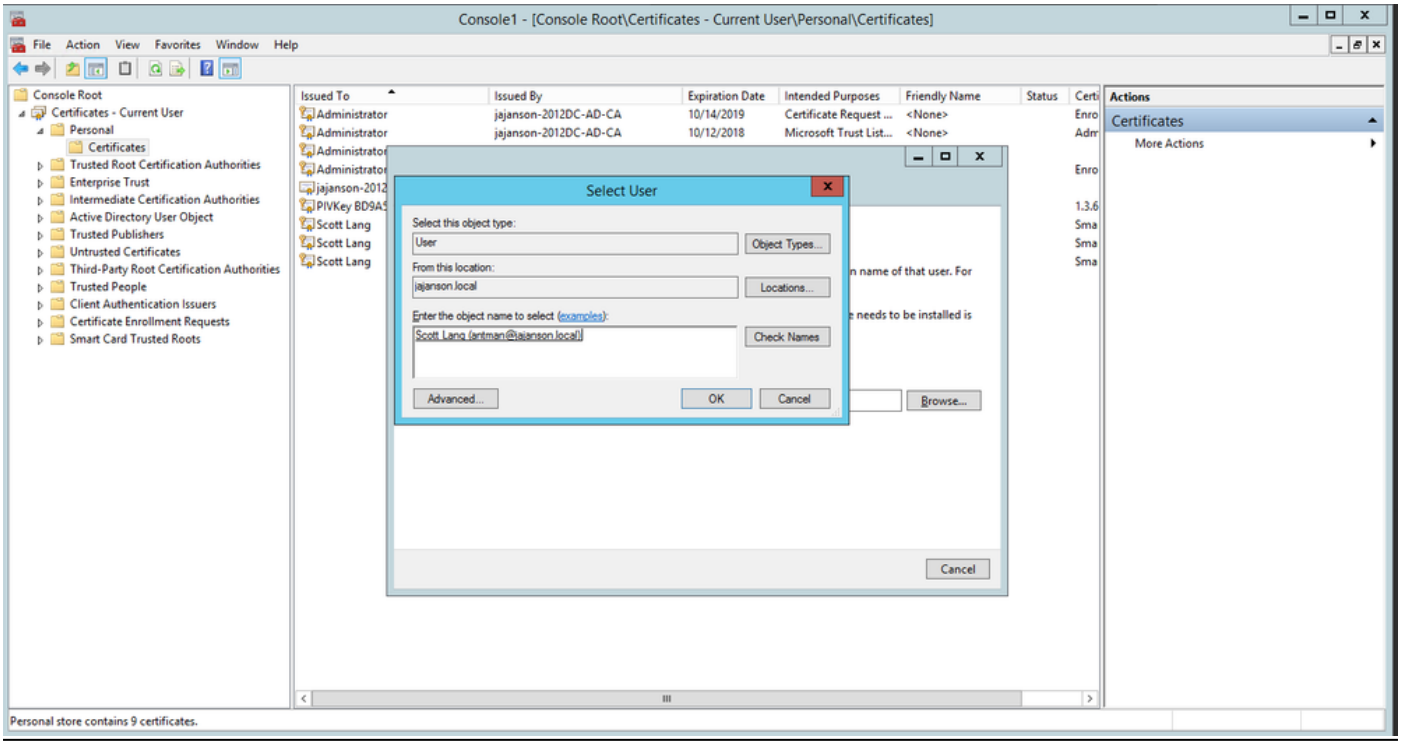
서명 인증서 선택

6. 다음 화면에서 요청하려는 인증서를 찾아보아야 하며, 이 경우에는 이전에 생성한 템플릿인 **Smartcard User_VCS**가 됩니다.



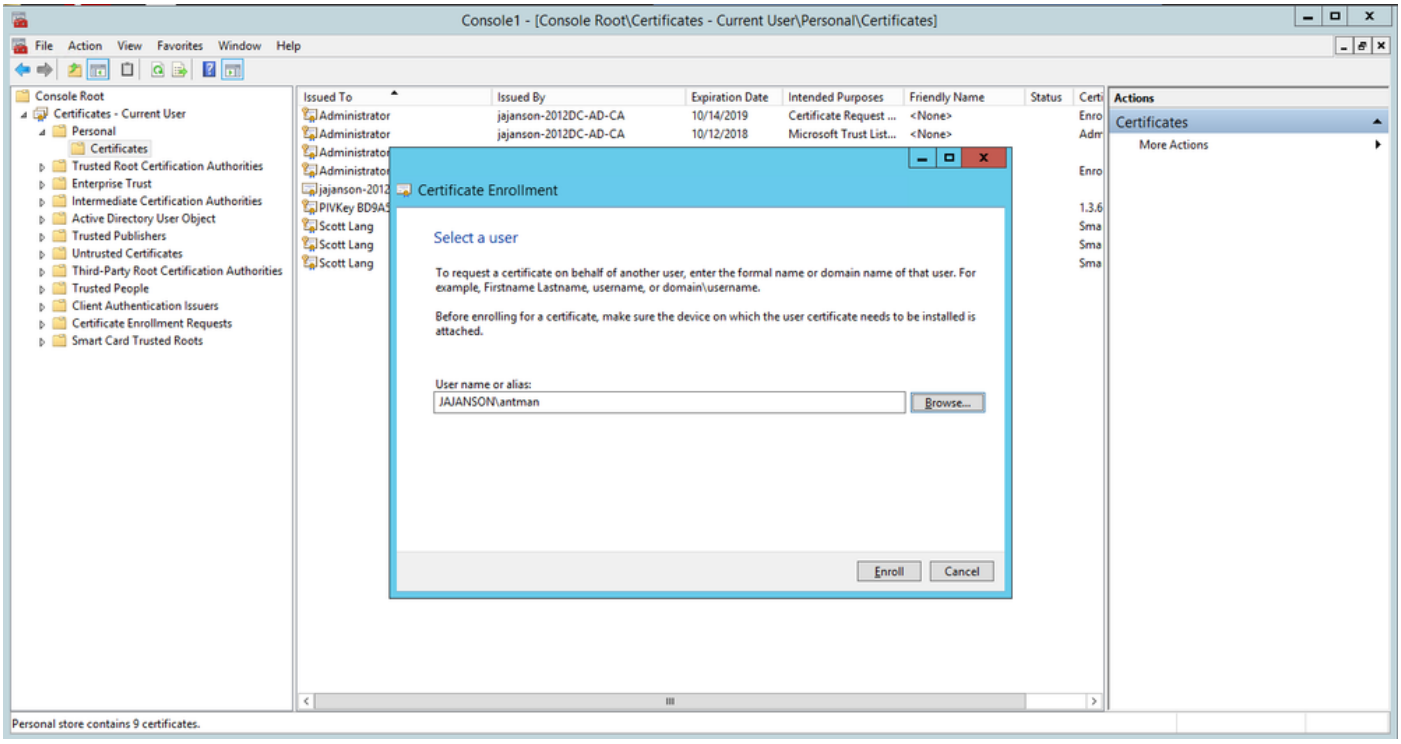
VCS 스마트 카드 선택

7. 다음으로, 등록할 사용자를 선택해야 합니다. 찾아보기를 클릭하고 등록하려는 직원의 사용자 이름을 입력합니다. 이 경우 Scott Lang 'antman@jajanson.local account'가 사용됩니다.



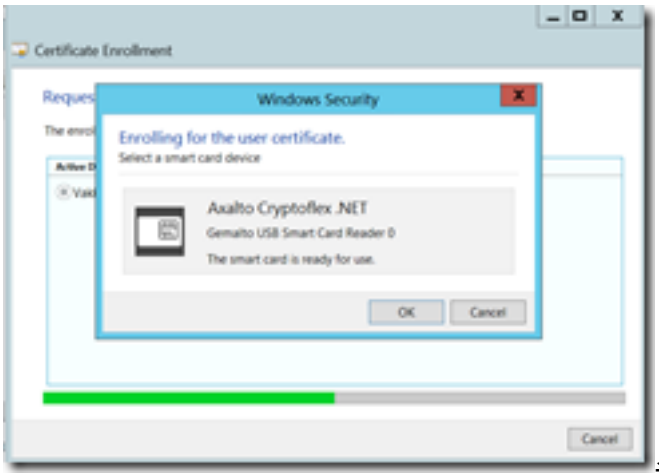
사용자 선택

8. 다음 화면에서 **등록**을 클릭하여 등록을 진행합니다. 이제 판독기에 스마트 카드를 삽입합니다.



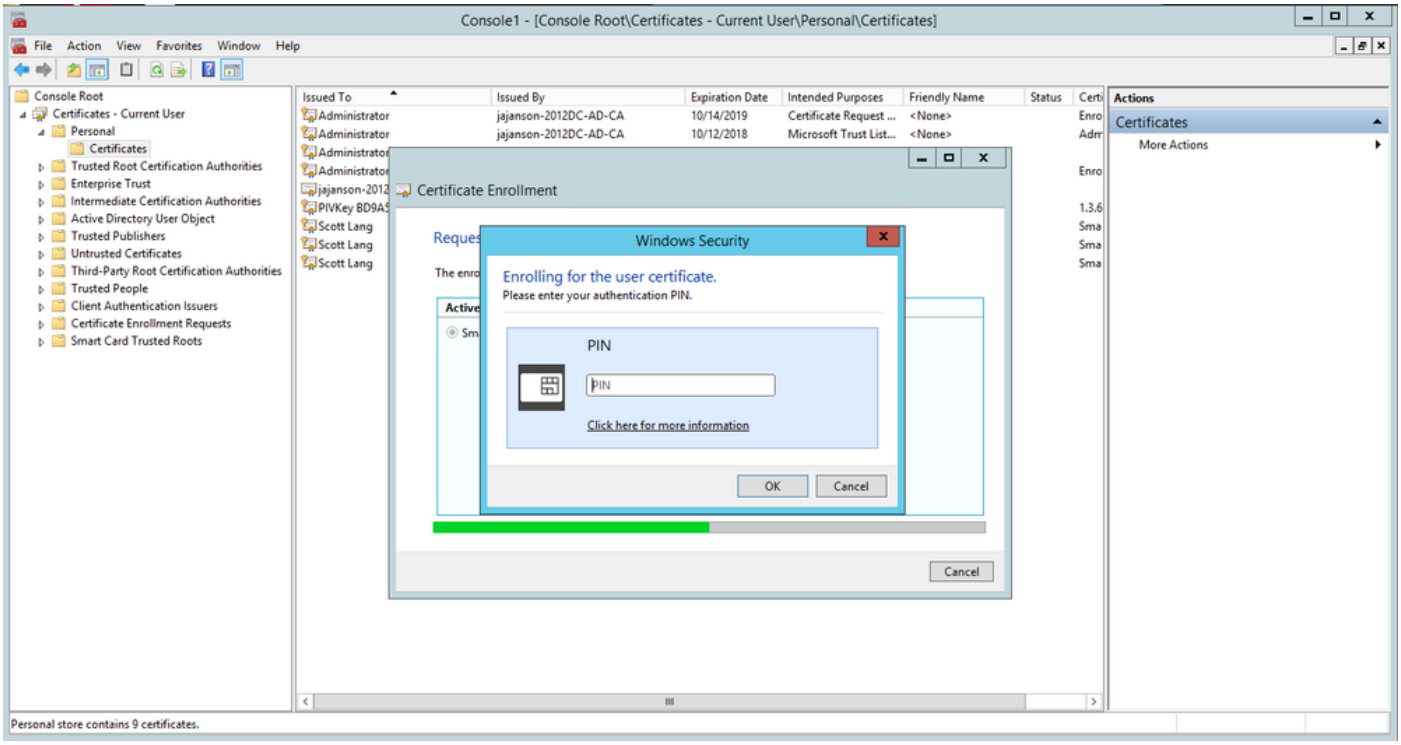
등록

9 . 스마트 카드를 삽입하면 다음과 같이 탐지됩니다.



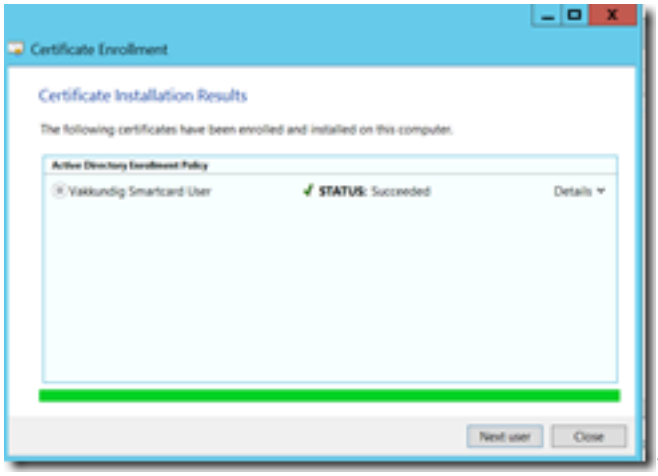
스마트 카드 삽입

10. 그런 다음 스마트 카드 PIN 번호(기본 PIN: 0000).



핀 입력

11. **Enrollment Successful(등록** 성공) 화면이 표시되면 이 스마트 카드를 사용하여 VCS(예: 카드 및 알려진 핀)와 같은 도메인 가입 서버에 로그온할 수 있습니다. 그러나 이 작업은 "예"가 아닌 경우에도 VCS를 준비하여 인증 요청을 스마트 카드로 리디렉션하고 일반 액세스 카드를 사용하여 인증을 위해 스마트 카드에 저장된 스마트 카드 인증서를 릴리스해야 합니다.



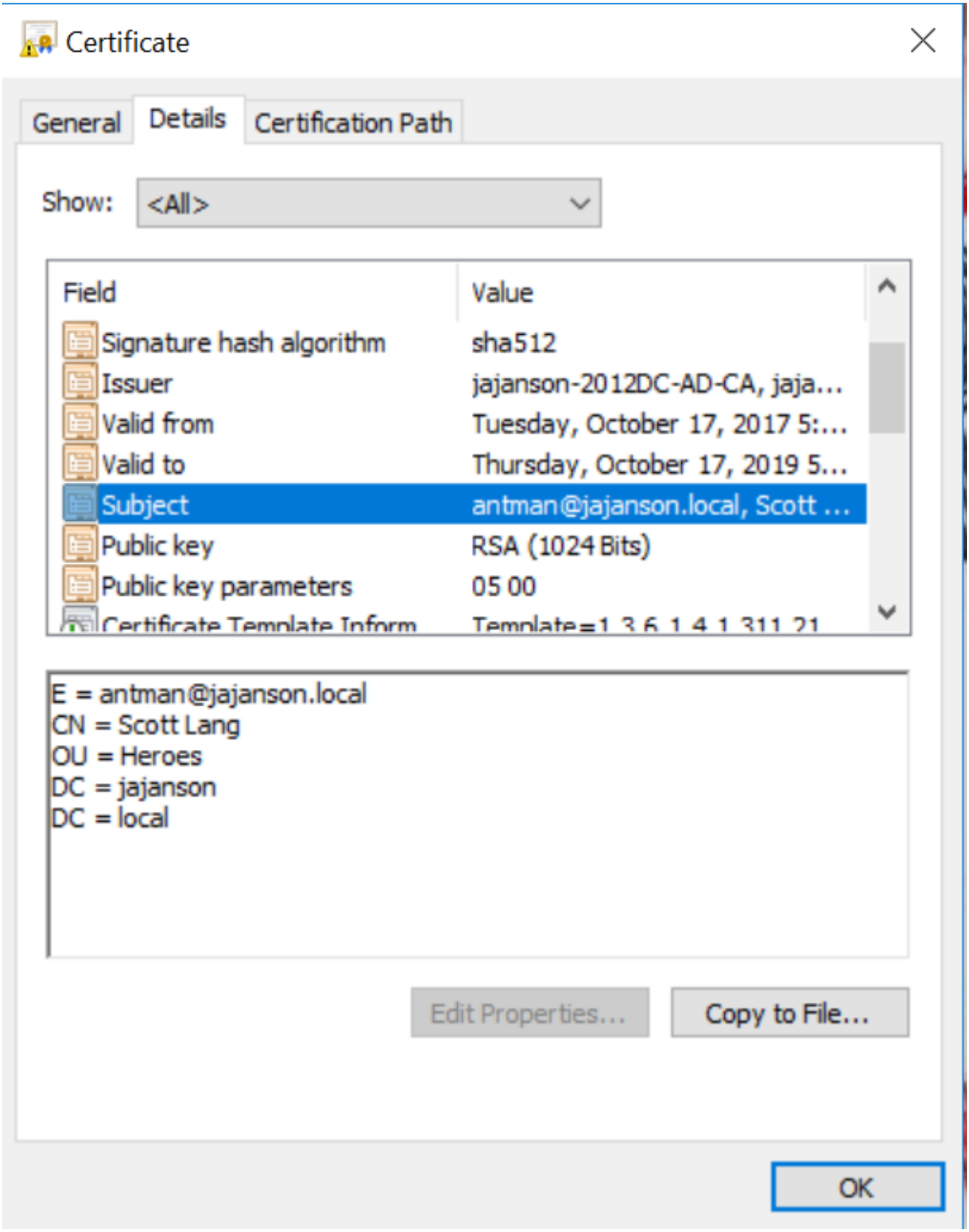
등록 성공

공통 액세스 카드에 대한 VCS 구성

Maintenance(**유지 관리**) > Security(보안) > Trusted CA Certificate(신뢰할 수 있는 CA 인증서)로 이동하여 VCS의 Trusted CA Certificate(신뢰할 수 있는 CA 인증서) 목록**에 루트 CA를 업로드합니다.**

2. 루트 CA에서 서명한 인증서 해지 목록을 VCS에 업로드합니다. Maintenance(**유지 관리) > Security(보안) > CRL Management(CRL 관리)로 이동합니다.**

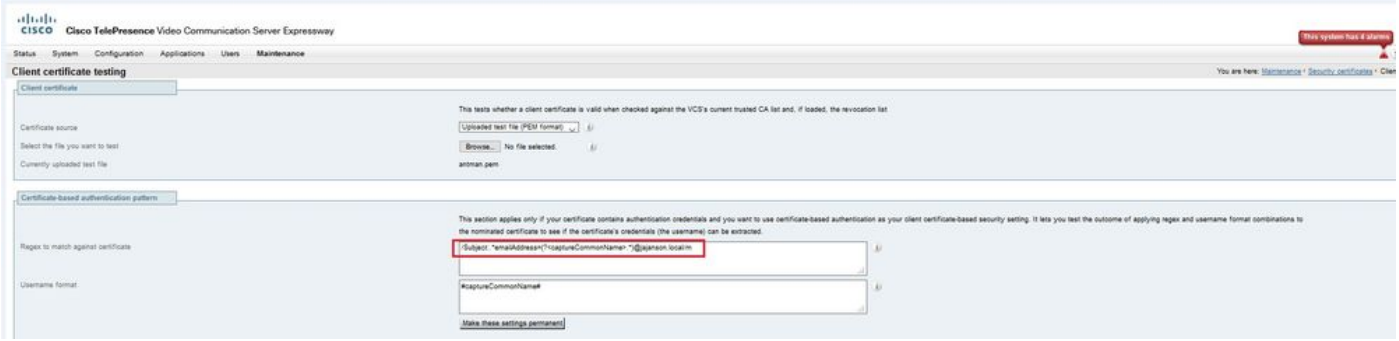
3. LDAP 또는 로컬 사용자에 대한 인증에 사용할 인증서에서 사용자 이름을 가져오는 regex에 대해 클라이언트 인증서를 테스트합니다. regex가 인증서의 **Subject**와 일치합니다. UPN, 이메일 등이 될 수 있습니다. 이 Lab에서는 클라이언트 인증서의 클라이언트 인증서와 매칭할 이메일이 사용되었습니다.


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
E = antman@jajanson.local
CN = Scott Lang
OU = Heroes
DC = jajanson
DC = local
Edit Properties...
Copy to File...
OK

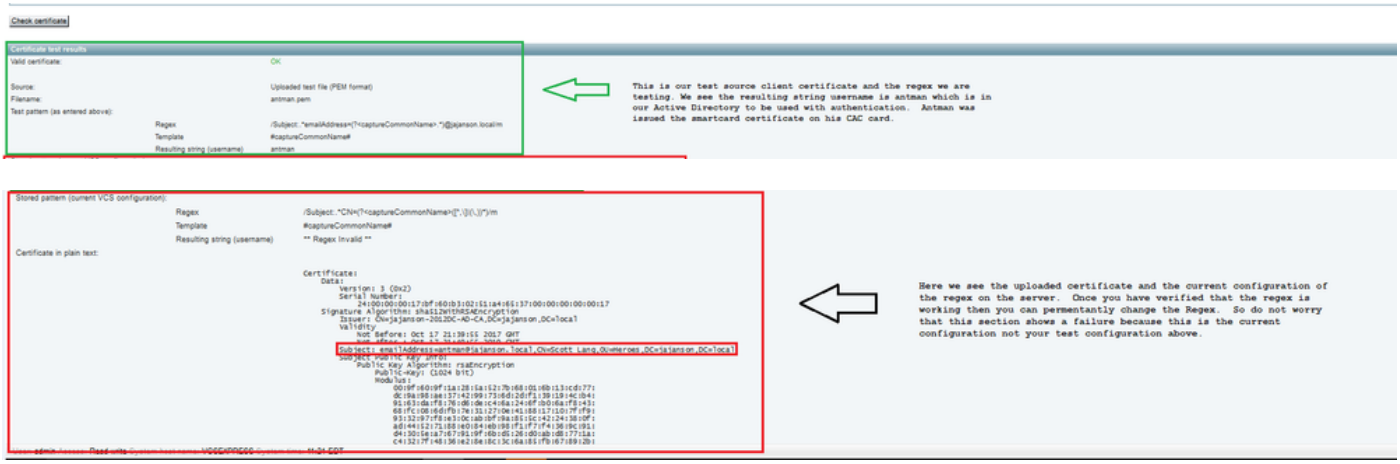
클라이언트 인증서 주체

4. Maintenance(**유지 관리) > Security(보안) > Client Certificate Testing(클라이언트 인증서 테스트)으로 이동합니다**. 테스트할 클라이언트 인증서를 선택하고 My Lab에서 antman.pem을 테스트 영역에 업로드합니다. Regex의 **Certificate-based authentication pattern(인증서 기반 인증 패턴)** 섹션**에서** 테스트할 regex를 붙여넣습니다. **Username 형식** 필드를 변경하지 마십시오.

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



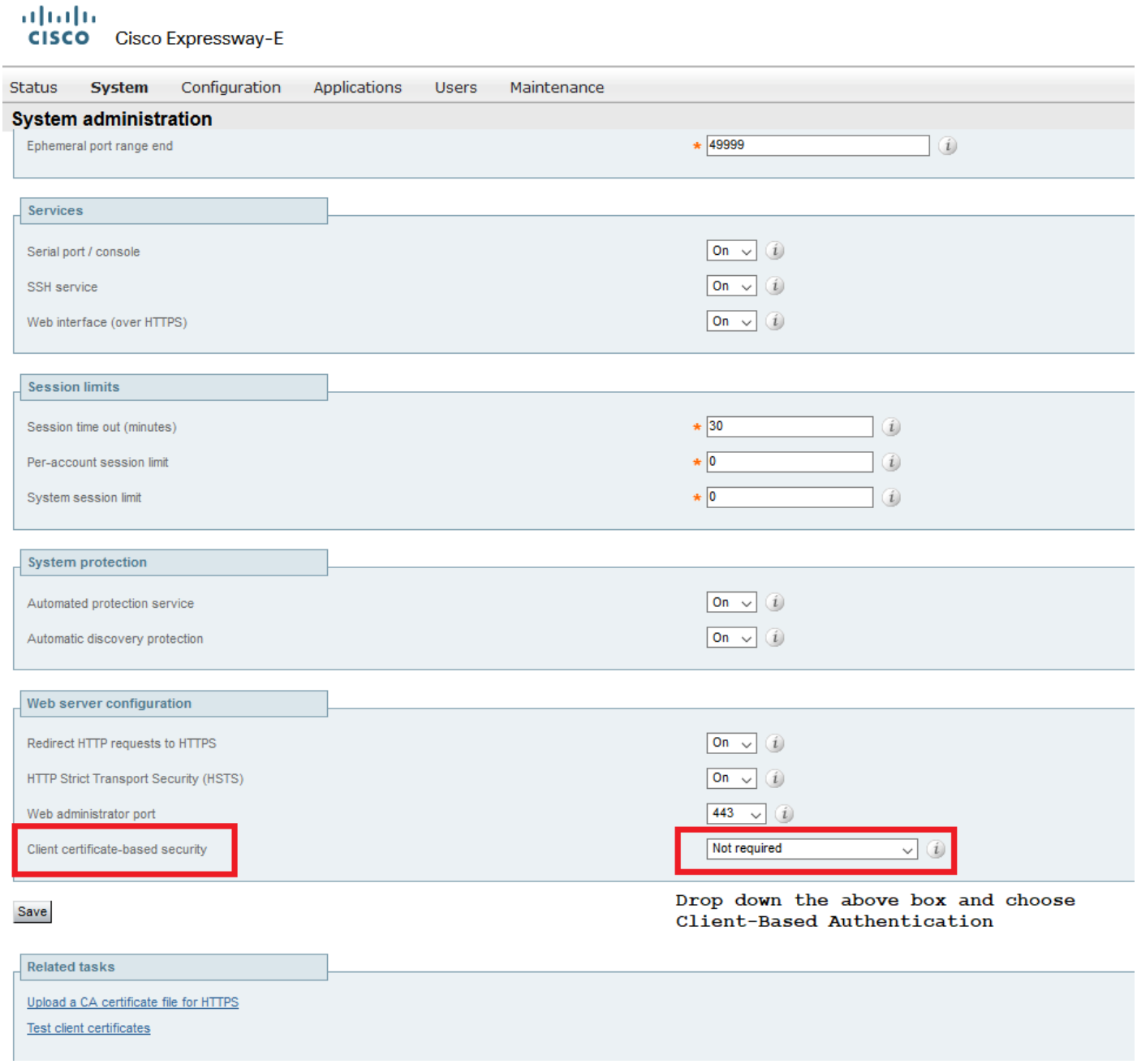
VCS에서 regex 테스트



테스트 결과

5. 테스트를 통해 원하는 결과를 얻을 수 있는 경우 **이러한 변경 사항**을 **영구적**으로 **만들기** 버튼을 클릭할 수 있습니다. 이렇게 하면 서버의 **인증서 기반 인증 컨피그레이션**에 대한 regex가 변경됩니다. 변경 사항을 확인하려면 해당 컨피그레이션, Maintenance(유지 관리) **> Security(보안) > Certificate-based authentication configuration(인증서 기반 인증 컨피그레이션)으로 이동합니다.**

6. System(**시스템**) > Administrator(관리자)로 이동하여 클라이언트 기반 인증을 활성화한 다음 드롭다운 상자를 클릭하거나 선택하여 **클라이언트 인증서 기반 보안 = Client-Based Authentication(클라이언트 기반 인증)을** 선택합니다. 이 설정을 사용하면 사용자가 브라우저에 VCS 서버의 FQDN을 입력하면 클라이언트 계정을 선택하고 자신의 일반 액세스 카드에 할당된 핀을 입력하라는 메시지가 표시됩니다. 그런 다음 인증서가 릴리스되고 VCS 서버의 웹 GUI가 반환되며, Administrator 버튼을 클릭하거나 선택하면 됩니다. 그리고 나서 그는 서버에 들어갔다. Client **certificate-based security = Client-Based Validation(클라이언트 인증서 기반 보안 = 클라이언트 기반 검증) 옵션이** 선택된 경우, 사용자가 Administrator(관리자) 버튼을 클릭할 때 프로세스가 예외와 동일하며 관리자 비밀번호를 다시 입력하라는 프롬프트가 표시됩니다. 일반적으로 후자는 조직이 CAC를 사용하여 성취하려고 하는 것이 아닙니다.



클라이언트 기반 인증 사용

도와주세요! 문이 잠겼어요!

Client Based Authentication(클라이언트 기반 인증)을 활성화하고 VCS가 어떤 이유로든 인증서를 거부하면 웹 GUI에 더 이상 기존의 방식으로 로그인할 수 없게 됩니다. 하지만 시스템을 다시 사용할 수 있는 방법이 있다고 걱정하지 마십시오. 첨부된 문서는 Cisco 웹 사이트에서 찾을 수 있으며 루트 액세스에서 클라이언트 기반 인증을 비활성화하는 방법에 대한 정보를 제공합니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.