

BYOD를 위한 ISE SCEP 지원 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[테스트된 CANDES 구축 시나리오](#)

[독립형 구축](#)

[분산 구축](#)

[중요 Microsoft 핫픽스](#)

[중요 BYOD 포트 및 프로토콜](#)

[구성](#)

[SCEP 등록 챌린지 비밀번호 요구 사항 비활성화](#)

[알려진 ISE 노드로 SCEP 등록 제한](#)

[IIS에서 URL 길이 확장](#)

[인증서 템플릿 개요](#)

[인증서 템플릿 구성](#)

[인증서 템플릿 레지스트리 구성](#)

[ISE를 SCEP 프록시로 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[일반 문제 해결 참고 사항](#)

[클라이언트측 로깅](#)

[ISE 로깅](#)

[NDES 로깅 및 문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 Cisco ISE(Identify Services Engine)에서 BYOD(Bring Your Own Device)를 위한 Microsoft NDES(Network Device Enrollment Service) 및 SCEP(Simple Certificate Enrollment Protocol)를 성공적으로 구성하는 데 사용되는 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ISE 릴리스 1.1.1 이상
- Microsoft Windows Server 2008 R2

- Microsoft Windows Server 2012 Standard
- PKI(Public Key Infrastructure) 및 인증서

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ISE 릴리스 1.1.1 이상
- KB2483564 및 KB2633200 핫픽스가 설치된 Windows Server 2008 R2 SP1
- Windows Server 2012 Standard

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

Microsoft 인증서 서비스와 관련된 정보는 Cisco BYOD를 위한 설명서로 제공됩니다. Microsoft 인증 기관, NDES(Network Device Enrollment Service) 및 SCEP 관련 서버 컨피그레이션에 대한 정확한 소스로 Microsoft TechNet을 참조하십시오.

배경 정보

Cisco ISE 지원 BYOD 구현의 이점 중 하나는 최종 사용자가 셀프 서비스 디바이스 등록을 수행할 수 있다는 점입니다. 따라서 인증 자격 증명을 배포하고 네트워크에서 디바이스를 활성화하기 위해 IT에 대한 관리 부담이 없어집니다. BYOD 솔루션의 핵심은 필수 인증서를 직원 소유 장치에 배포하려는 네트워크 신청자 프로비저닝 프로세스입니다. 이 요구 사항을 충족하기 위해 SCEP로 인증서 등록 프로세스를 자동화하기 위해 Microsoft CA(Certificate Authority)를 구성할 수 있습니다.

SCEP는 원격 액세스 클라이언트 및 라우터에 인증서 등록 및 배포를 용이하게 하기 위해 VPN(Virtual Private Network) 환경에서 수년 동안 사용되었습니다. Windows 2008 R2 서버에서 SCEP 기능을 사용하려면 NDES를 설치해야 합니다. NDES 역할을 설치하는 동안 Microsoft IIS(인터넷 정보 서비스) 웹 서버도 설치됩니다. IIS는 CA와 ISE 정책 노드 간의 HTTP 또는 HTTPS SCEP 등록 요청 및 응답을 종료하기 위해 사용됩니다.

NDES 역할은 현재 CA에 설치하거나 멤버 서버에 설치할 수 있습니다. 독립형 구축에서는 NDES 서비스가 인증 기관 서비스 및 선택적으로 인증 기관 웹 등록 서비스를 포함하는 기존 CA에 설치됩니다. 분산 구축에서는 NDES 서비스가 멤버 서버에 설치됩니다. 그런 다음 업스트림 루트 또는 하위 루트 CA와 통신하기 위해 분산 NDES 서버가 구성됩니다. 이 시나리오에서 이 문서에 설명된 레지스트리 수정 사항은 사용자 지정 템플릿을 사용하여 NDES 서버에서 이루어지며, 여기서 인증서는 업스트림 CA에 상주합니다.

테스트된 CA/NDES 구축 시나리오

이 섹션에서는 Cisco Lab에서 테스트한 CA/NDES 구축 시나리오에 대한 간략한 개요를 제공합니다. Microsoft CA, NDES 및 SCEP 관련 서버 컨피그레이션에 대한 정확한 소스로 Microsoft TechNet을 참조하십시오.

독립형 구축

ISE를 PoC(Proof of Concept) 시나리오에서 사용하는 경우 AD(Active Directory) 도메인 컨트롤러, 루트 CA 및 NDES 서버 역할을 하는 자체 포함 Windows 2008 또는 2012 시스템을 구축하는 것이 일반적입니다.



- Domain Controller
- AD
- Root CA
- NDES

분산 구축

ISE가 현재 Microsoft AD/PKI 프로덕션 환경에 통합될 경우, 여러 개별 Windows 2008 또는 2012 서버에 분산된 서비스를 보는 것이 일반적입니다. Cisco는 분산 구축에 대한 두 가지 시나리오를 테스트했습니다.

이 그림에서는 분산 구축에 대해 최초로 테스트된 시나리오를 보여 줍니다.



- Domain Controller
- AD
- Root CA



- Member Server
- Subordinate CA
- NDES

이 그림에서는 분산 구축에 대해 두 번째로 테스트된 시나리오를 보여 줍니다.



- Domain Controller
- AD
- Root CA



- Member Server
- Subordinate CA



- Member Server
- NDES

중요 Microsoft 핫픽스

BYOD에 대한 SCEP 지원을 구성하기 전에 Windows 2008 R2 NDES 서버에 다음 Microsoft 핫픽스가 설치되어 있는지 확인하십시오.

- [NDES를 사용하여 인증서를 관리하는 경우 Windows Server 2008 R2에서 SCEP 인증서에 대한 갱신 요청이 실패합니다](#) - NDES가 GetCACaps 작업을 지원하지 않기 때문에 이 문제가 발생합니다.
- [Windows Server 2008 R2에서 엔터프라이즈 CA를 다시 시작한 후 NDES는 인증서 요청을 제출하지 않습니다](#) - 이 메시지는 이벤트 뷰어에 나타납니다. "네트워크 장치 등록 서비스가 인증서 요청을 전송할 수 없습니다(0x800706ba). RPC 서버를 사용할 수 없습니다."

경고:Microsoft CA를 구성할 때 ISE가 RSSA-PSS 서명 알고리즘을 지원하지 않음을 이해하는 것이 중요합니다. 대신 sha1WithRSAEncryption 또는 sha256WithRSAEncryption을 사용하여 CA 정책을 구성하는 것이 좋습니다.

중요 BYOD 포트 및 프로토콜

다음은 중요한 BYOD 포트 및 프로토콜 목록입니다.

- TCP:8909 프로비저닝: Cisco ISE에서 마법사 설치(Windows 및 Macintosh 운영 체제(OS))
- TCP:443 프로비저닝: Google Play에서 마법사 설치(Android)
- TCP:8905 프로비저닝: 신청자 프로비저닝 프로세스
- TCP:80 또는 TCP:443 CA에 대한 SCEP 프록시(SCEP RA URL 컨피그레이션 기반)

참고:필요한 포트 및 프로토콜의 최신 목록은 ISE 1.2 [하드웨어 설치 가이드](#)를 참조하십시오.

구성

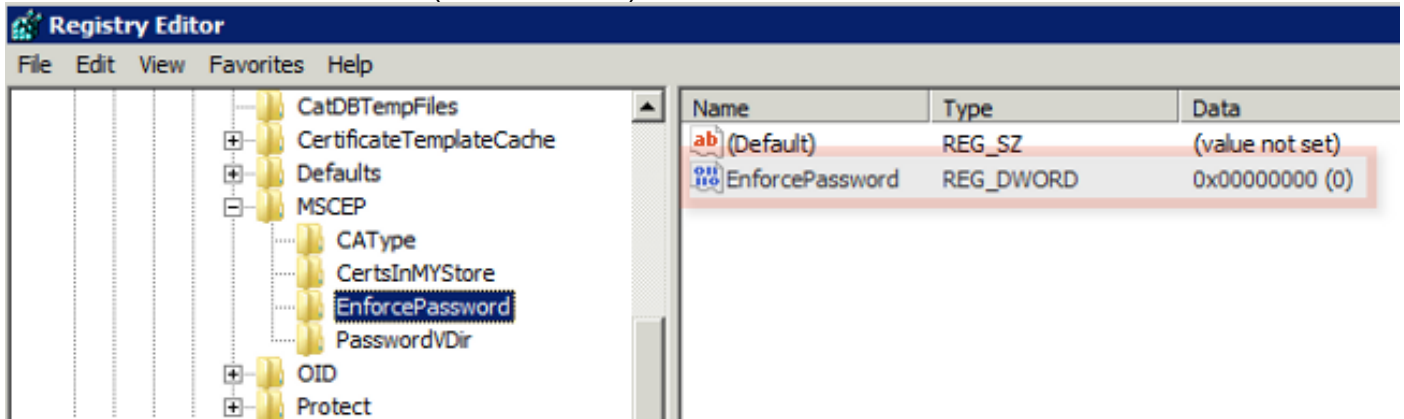
ISE에서 BYOD에 대한 NDES 및 SCEP 지원을 구성하려면 이 섹션을 사용합니다.

SCEP 등록 챌린지 비밀번호 요구 사항 비활성화

기본적으로 Microsoft SCEP(MSCEP) 구현에서는 인증서 등록 프로세스 전체에서 클라이언트와 엔드포인트를 인증하기 위해 동적 챌린지 비밀번호를 사용합니다. 이 컨피그레이션 요구 사항이 있는 경우 온디맨드 비밀번호를 생성하려면 NDES 서버에서 MSCEP 관리 웹 GUI를 찾아야 합니다. 등록 요청의 일부로 이 비밀번호를 포함해야 합니다.

BYOD 구축에서 챌린지 비밀번호 요건은 사용자 셀프 서비스 솔루션의 목적에 맞지 않습니다. 이 요구 사항을 제거하려면 NDES 서버에서 이 레지스트리 키를 수정해야 합니다.

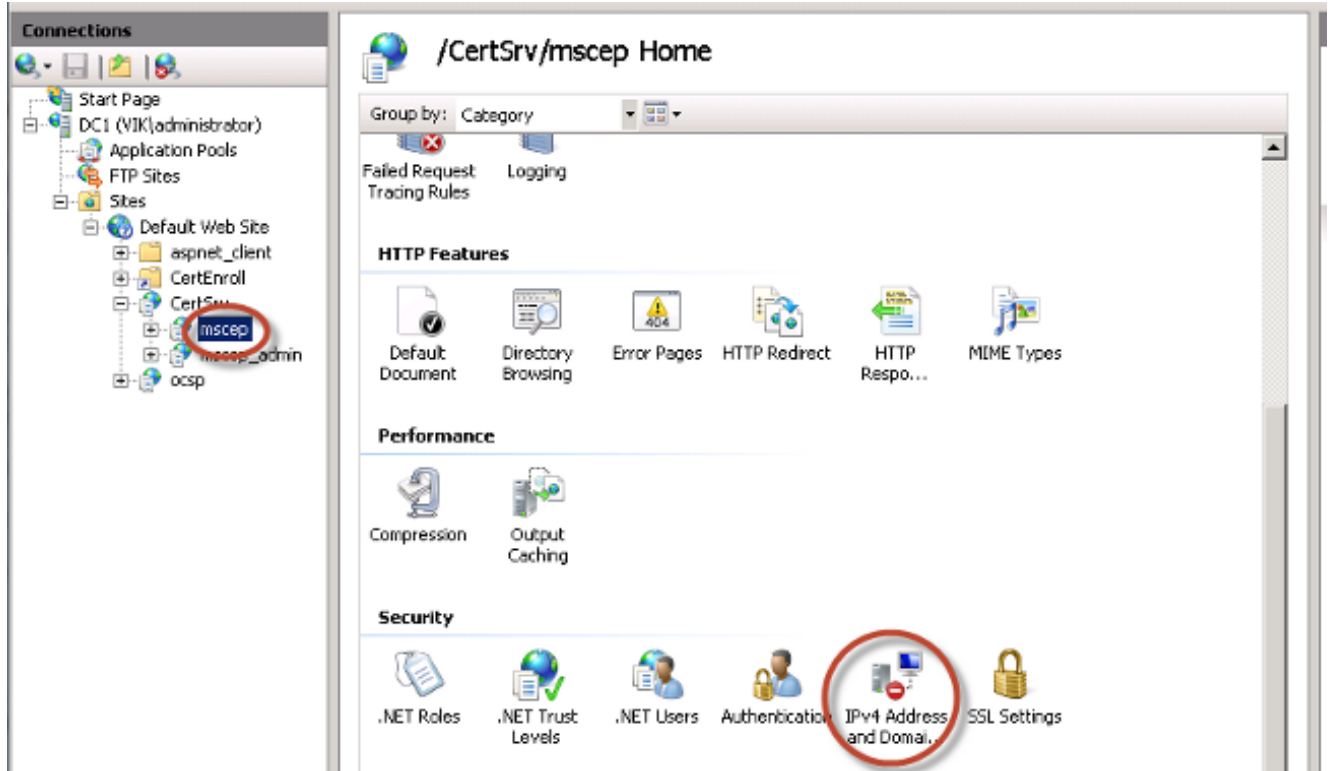
1. 시작을 클릭하고 검색 표시줄에 regedit를 입력합니다.
2. Computer(컴퓨터) > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP > EnforcePassword로 이동합니다.
3. EnforcePassword 값이 0(기본값은 1임)으로 설정되어 있는지 확인합니다.



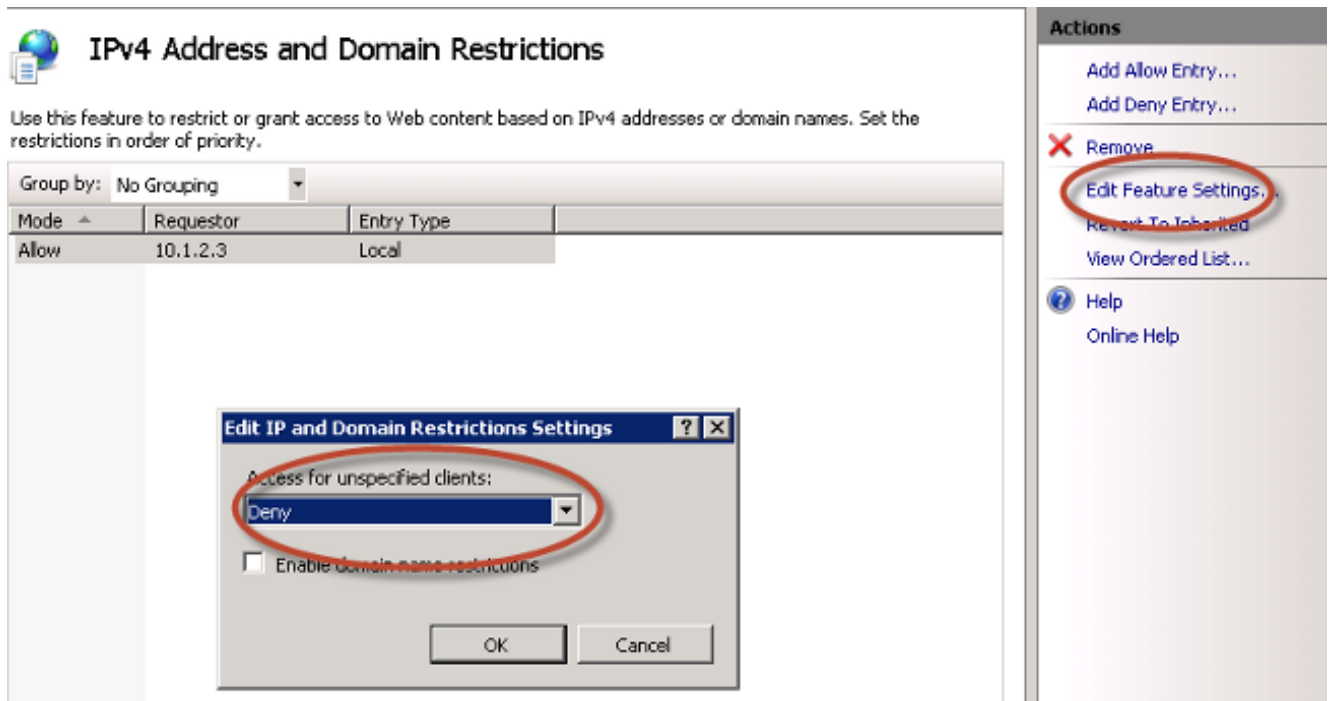
알려진 ISE 노드로 SCEP 등록 제한

일부 구축 시나리오에서는 SCEP 통신을 알려진 ISE 노드 선택 목록으로 제한하는 것이 좋습니다. 이 작업은 IIS의 IPv4 주소 및 도메인 제한 기능을 사용하여 수행할 수 있습니다.

1. IIS를 열고 /CertSrv/mscep 웹 사이트로 이동합니다.



2. Security(보안) > IPv4 Address and Domain Restrictions(IPv4 주소 및 도메인 제한)를 두 번 클릭합니다. ISE 노드 IPv4 주소 또는 도메인 이름을 기반으로 웹 콘텐츠에 대한 액세스를 허용하거나 제한하려면 Add Allow Entry(항목 추가) 및 Add Deny Entry(항목 추가) 작업을 사용합니다. 지정되지 않은 클라이언트에 대한 기본 액세스 규칙을 정의하려면 Edit Feature Settings 작업을 사용합니다.

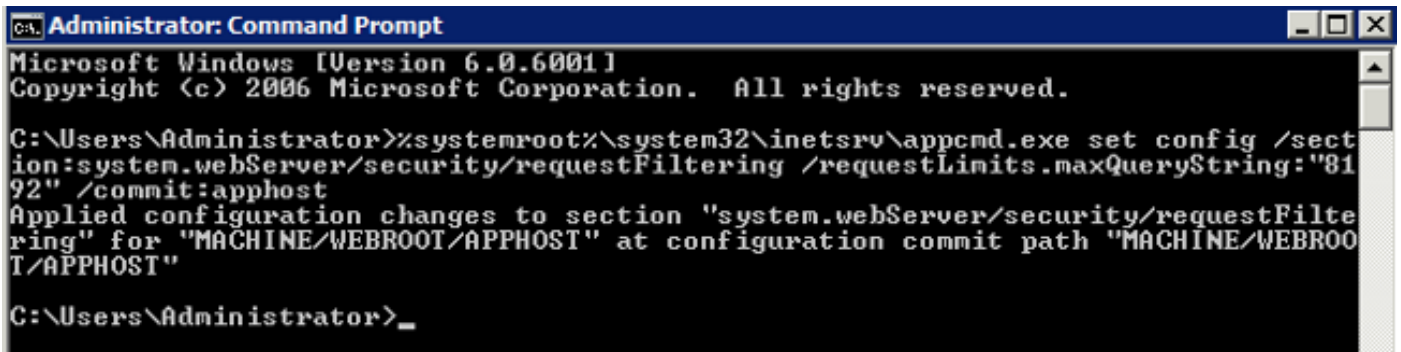


IIS에서 URL 길이 확장

ISE는 IIS 웹 서버에 너무 긴 URL을 생성할 수 있습니다. 이 문제를 방지하기 위해 기본 IIS 구성을 수정하여 더 긴 URL을 허용할 수 있습니다. NDES 서버 CLI에서 다음 명령을 입력합니다.

```
%systemroot%\system32\inetsrv\appcmd.exe set config /section:system.webServer/  
security/requestFiltering /requestLimits.maxQueryString:"8192" /commit:apphost
```

참고: 쿼리 문자열 크기는 ISE 및 엔드포인트 컨피그레이션에 따라 달라질 수 있습니다. 관리 권한이 있는 NDES 서버 CLI에서 이 명령을 입력합니다.



```
Administrator: Command Prompt  
Microsoft Windows [Version 6.0.6001]  
Copyright (c) 2006 Microsoft Corporation. All rights reserved.  
C:\Users\Administrator>%systemroot%\system32\inetsrv\appcmd.exe set config /sect  
ion:system.webServer/security/requestFiltering /requestLimits.maxQueryString:"81  
92" /commit:apphost  
Applied configuration changes to section "system.webServer/security/requestFilt  
ering" for "MACHINE/WEBROOT/APPHOST" at configuration commit path "MACHINE/WEBROO  
T/APPHOST"  
C:\Users\Administrator>_
```

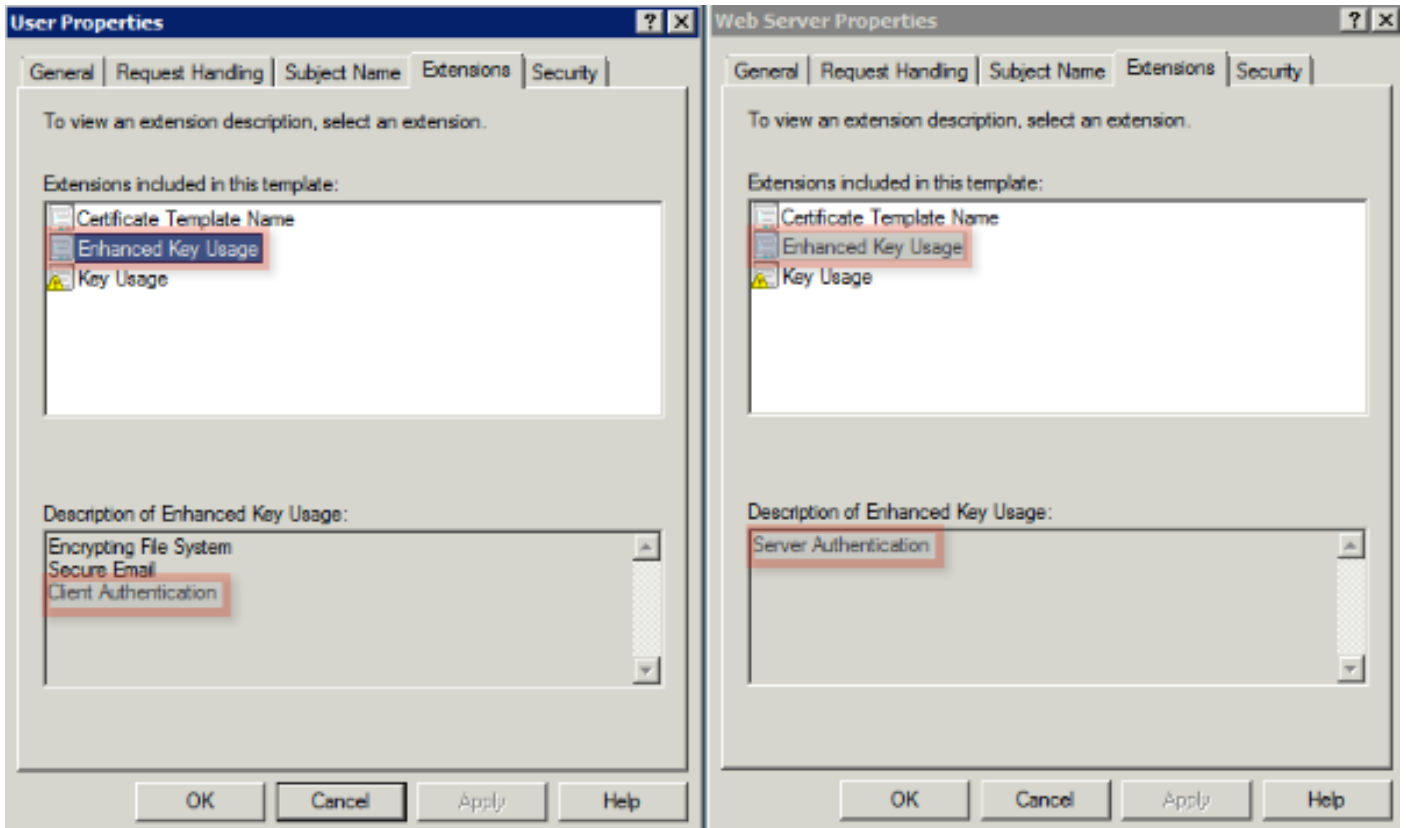
인증서 템플릿 개요

Microsoft CA의 관리자는 공통 인증서 집합에 애플리케이션 정책을 적용하기 위해 사용되는 하나 이상의 템플릿을 구성할 수 있습니다. 이러한 정책은 인증서 및 관련 키가 사용되는 기능을 식별하는 데 도움이 됩니다. 애플리케이션 정책 값은 인증서의 EKU(Extended Key Usage) 필드에 포함되어 있습니다. 인증자는 클라이언트가 제공한 인증서를 의도한 기능에 사용할 수 있도록 EKU 필드의 값을 구문 분석합니다. 더 일반적인 용도 중 일부는 서버 인증, 클라이언트 인증, IPsec VPN 및 이메일을 포함합니다. ISE의 관점에서 더 일반적으로 사용되는 EKU 값에는 서버 및/또는 클라이언트 인증이 포함됩니다.

예를 들어 보안 은행 웹 사이트를 탐색할 때 요청을 처리하는 웹 서버는 서버 인증의 애플리케이션 정책이 있는 인증서로 구성됩니다. 서버는 HTTPS 요청을 받으면 인증을 위해 서버 인증 인증서를 연결 웹 브라우저에 보냅니다. 여기서 중요한 점은 이것이 서버에서 클라이언트로의 단방향 교환이라는 것입니다. ISE와 관련된 것처럼 서버 인증 인증서에 대한 일반적인 용도는 관리 GUI 액세스입니다. ISE는 구성된 인증서를 연결된 브라우저로 전송하며 클라이언트에서 인증서를 다시 수신할 것으로 예상되지 않습니다.

EAP-TLS를 사용하는 BYOD와 같은 서비스에 대해서는 상호 인증을 사용하는 것이 좋습니다. 이 양방향 인증서 교환을 활성화하려면 ISE ID 인증서를 생성하는 데 사용되는 템플릿이 서버 인증의 최소 애플리케이션 정책을 가져야 합니다. 웹 서버 인증서 템플릿이 이 요구 사항을 충족합니다. 엔드포인트 인증서를 생성하는 인증서 템플릿은 클라이언트 인증의 최소 애플리케이션 정책을 포함해야 합니다. 사용자 인증서 템플릿은 이 요구 사항을 충족합니다. iPEP(Inline Policy Enforcement Point)와 같은 서비스에 대해 ISE를 구성하는 경우, ISE 버전 1.1.x 또는 이전 버전을 사용하는 경우 ISE 서버 ID 인증서를 생성하는 데 사용되는 템플릿은 클라이언트 및 서버 인증 특성을 모두 포함해야 합니다. 이렇게 하면 관리자 및 인라인 노드가 상호 인증할 수 있습니다. iPEP에 대한 EKU 검증이 ISE 버전 1.2에서 제거되어 이 요구 사항이 덜 관련됩니다.

기본 Microsoft CA Web Server 및 사용자 템플릿을 재사용하거나 이 문서에 설명된 프로세스를 사용하여 새 템플릿을 복제하고 생성할 수 있습니다. 이러한 인증서 요구 사항을 기반으로 CA 컨피그레이션 및 결과 ISE 및 엔드포인트 인증서를 신중하게 계획해야 프로덕션 환경에 설치할 때 원치 않는 컨피그레이션 변경을 최소화할 수 있습니다.



인증서 템플릿 구성

소개에서 설명한 것처럼 SCEP는 IPsec VPN 환경에서 널리 사용됩니다. 따라서 NDES 역할을 설치하면 SCEP용 IPsec(Offline Request) 템플릿을 사용하도록 서버가 자동으로 구성됩니다. 따라서 BYOD용 Microsoft CA를 준비하는 첫 번째 단계 중 하나는 올바른 애플리케이션 정책으로 새 템플릿을 구축하는 것입니다. 독립형 구축에서는 인증 기관 및 NDES 서비스가 동일한 서버에 결합되며 템플릿과 필요한 레지스트리 수정 사항이 동일한 서버에 포함됩니다. 분산 NDES 구축에서는 NDES 서버에서 레지스트리를 수정합니다. 그러나 실제 템플릿은 NDES 서비스 설치에 지정된 루트 또는 하위 루트 CA 서버에 정의됩니다.

인증서 템플릿을 구성하려면 다음 단계를 완료합니다.

1. CA 서버에 관리자로 로그인합니다.
2. Start(시작) > Administrative Tools(관리 툴) > Certification Authority(인증 기관)를 클릭합니다.
3. CA 서버 세부 정보를 확장하고 **Certificate Templates** 폴더를 선택합니다. 이 폴더에는 현재 활성화된 템플릿 목록이 포함되어 있습니다.
4. 인증서 템플릿을 관리하려면 **Certificate Templates** 폴더를 마우스 오른쪽 버튼으로 클릭하고 **Manage**를 선택합니다.
5. **Certificate Templates Console**에 여러 비활성 템플릿이 표시됩니다.
6. SCEP와 함께 사용할 새 템플릿을 구성하려면 이미 존재하는 템플릿(예: **User**)을 마우스 오른쪽 버튼으로 클릭하고 Duplicate Template(템플릿 복제)을 선택합니다.
7. 환경의 최소 CA OS에 따라 **Windows 2003** 또는 **Windows 2008**을 선택합니다.

8. **일반** 탭에서 ISE-BYOD 및 유효 기간과 같은 표시 이름을 추가합니다. 다른 옵션은 모두 선택하지 않습니다.
참고: 템플릿 유효 기간은 CA 루트 및 중간 인증서의 유효 기간보다 작거나 같아야 합니다.
9. **Subject Name** 탭을 클릭하고 **요청의 Supply(공급)**가 선택되었는지 확인합니다.
10. **Issuance Requirements** 탭을 클릭합니다. Cisco는 일반적인 계층적 CA 환경에서 **발급 정책**을 공백으로 두는 것이 좋습니다.
11. **Extensions(확장)** 탭, **Application Policies(애플리케이션 정책)**를 클릭한 다음 **Edit(편집)**를 클릭합니다.
12. **Add(추가)**를 클릭하고 **Client Authentication(클라이언트 인증)**이 애플리케이션 정책으로 추가되었는지 확인합니다. **확인**을 클릭합니다.
13. **보안** 탭을 클릭한 다음 **추가....NDES** 서비스 설치에 정의된 SCEP 서비스 계정이 템플릿을 완전히 제어하는지 확인한 다음 **OK(확인)**를 클릭합니다.
14. **인증 기관 GUI** 인터페이스로 돌아갑니다.
15. **Certificate Templates** 디렉토리를 마우스 오른쪽 단추로 클릭합니다. **New(새로 만들기) > Certificate Template(인증서 템플릿)**로 이동하여 **Issue(문제)**를 선택합니다.
16. 이전에 구성한 **ISE-BYOD** 템플릿을 선택하고 **OK(확인)**를 클릭합니다.

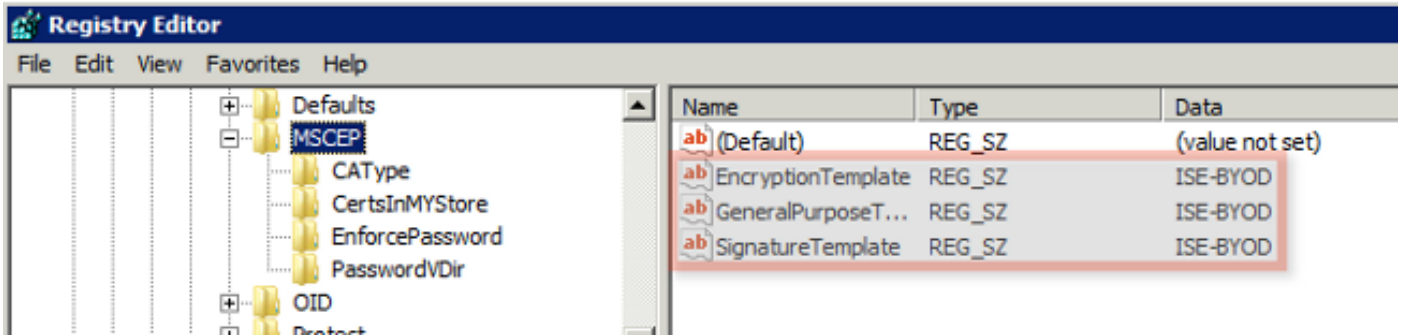
참고: 또는 certutil -SetCAtemplates + ISE-BYOD 명령을 사용하여 CLI를 통해 템플릿을 활성화할 수 있습니다.

이제 ISE-BYOD 템플릿이 활성화된 인증서 템플릿 목록에 나열됩니다.

인증서 템플릿 레지스트리 구성

인증서 템플릿 레지스트리 키를 구성하려면 다음 단계를 완료합니다.

1. NDES 서버에 연결합니다.
2. **시작**을 클릭하고 검색 표시줄에 regedit를 입력합니다.
3. **Computer(컴퓨터) > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP**로 이동합니다.
4. **EncryptionTemplate, GeneralPurposeTemplate** 및 **SignatureTemplate** 키를 **IPSec(Offline Request)**에서 이전에 생성한 ISE-BYOD 템플릿으로 변경합니다.
5. 레지스트리 설정을 적용하려면 NDES 서버를 재부팅합니다.



ISE를 SCEP 프록시로 구성

BYOD 구축에서 엔드포인트는 백엔드 NDES 서버와 직접 통신하지 않습니다. 대신 ISE 정책 노드는 SCEP 프록시로 구성되며 엔드포인트 대신 NDES 서버와 통신합니다. 엔드포인트는 ISE와 직접 통신합니다. NDES 서버의 IIS 인스턴스는 SCEP 가상 디렉터리에 대한 HTTP 및/또는 HTTPS 바인딩을 지원하도록 구성할 수 있습니다.

ISE를 SCEP 프록시로 구성하려면 다음 단계를 완료합니다.

1. 관리자 자격 증명을 사용하여 **ISE GUI**에 로그인합니다.
2. Administration(관리), Certificates(인증서), SCEP CA Profiles(SCEP CA 프로파일)를 차례로 클릭합니다.
3. Add(추가)를 클릭합니다.
4. 서버 이름과 설명을 입력합니다.
5. IP 또는 FQDN(Fully Qualified Domain Name)을 사용하여 SCEP 서버의 URL을 입력합니다 (예: <http://10.10.10.10/certsrv/mscep/>).
6. 연결 테스트를 클릭합니다. 연결에 성공하면 서버 응답 팝업 메시지가 나타납니다.
7. Save(저장)를 클릭하여 컨피그레이션을 적용합니다.
8. 확인하려면 Administration, Certificates, Certificate Store를 클릭하고 SCEP NDES 서버 RA 인증서가 ISE 노드에 자동으로 다운로드되었는지 확인합니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

컨피그레이션 문제를 해결하려면 이 섹션을 사용합니다.

일반 문제 해결 참고 사항

컨피그레이션 트러블슈팅을 위해 사용할 수 있는 중요한 참고 사항 목록은 다음과 같습니다.

- ISE, NDES 및 CA 엔드포인트 간의 경로를 따라 디버그 지점을 식별하고 캡처할 수 있도록 BYOD 네트워크 토폴로지를 논리적 경로로 세분화합니다.
- ISE 노드 및 CA가 공통 NTP(Network Time Protocol) 시간 소스를 공유하는지 확인합니다.
- 엔드포인트는 DHCP에서 학습한 NTP 및 표준 시간대 옵션을 사용하여 시간을 자동으로 설정할 수 있어야 합니다.
- 클라이언트의 DNS 서버는 ISE 노드의 FQDN을 확인할 수 있어야 합니다.
- ISE와 NDES 서버 간에 TCP 80 및/또는 TCP 443이 양방향으로 허용되는지 확인합니다.
- 클라이언트 측 로깅이 개선되어 Windows 시스템에서 테스트합니다. 선택적으로, 클라이언트 측 콘솔 로그를 모니터링하려면 Apple iDevice와 Apple iPhone Configuration Utility를 함께 사용합니다.
- CA 및 NDES 서버 애플리케이션 로그에서 등록 오류를 모니터링하고 Google 또는 TechNet을 사용하여 이러한 오류를 조사합니다.
- 테스트 단계에서 ISE, NDES 및 CA 간의 패킷 캡처를 촉진하려면 SCEP에 HTTP를 사용합니다.
- ISE PSN(Policy Service Node)에서 TCP 덤프 유틸리티를 사용하고 NDES 서버와의 트래픽을 모니터링합니다. 이 위치는 **Operations(운영) > Diagnostic Tools(진단 도구) > General Tools(일반 도구)에 있습니다.**
- CA 및 NDES 서버에 Wireshark를 설치하거나 중간 스위치에서 SPAN을 사용하여 ISE PSN에서 SCEP 트래픽을 캡처합니다.
- 클라이언트 인증서 인증을 위해 ISE 정책 노드에 적절한 CA 인증서 체인이 설치되어 있는지 확인합니다.
- 온보딩 중에 적절한 CA 인증서 체인이 클라이언트에 자동으로 설치되어 있는지 확인합니다.
- ISE 및 엔드포인트 ID 인증서를 미리 보고 올바른 ECU 특성이 있는지 확인합니다.
- ISE GUI의 라이브 인증 로그에서 인증 및 권한 부여 오류를 모니터링합니다.
참고: 서버 인증의 ECU가 있는 클라이언트 인증서와 같이 잘못된 ECU가 있는 경우 일부 신청자는 클라이언트 인증서 교환을 초기화하지 않습니다. 따라서 인증 실패가 항상 ISE 로그에 있는 것은 아닙니다.
- NDES가 분산 구축에 설치되면 서비스 설치의 CA 이름 또는 컴퓨터 이름으로 원격 루트 또는 하위 루트 CA가 지정됩니다. NDES 서버는 인증서 등록 요청을 이 대상 CA 서버로 전송합니다. 엔드포인트 인증서 등록 프로세스가 실패하면 PCAP(packet captures)에서 ISE 노드에 **404 Not Found** 오류를 반환하는 NDES 서버를 표시할 수 있습니다. 이 문제를 해결하려면 NDES 서비스를 다시 설치하고 CA 이름 대신 컴퓨터 이름 옵션을 선택합니다.

- 디바이스가 온보딩된 후 SCEP CA 체인을 변경하지 마십시오. Apple iOS와 같은 엔드포인트 OS는 이전에 설치한 BYOD 프로파일을 자동으로 업데이트하지 않습니다. 이 iOS 예에서는 온보딩을 다시 수행할 수 있도록 현재 프로필을 엔드포인트에서 삭제하고 ISE 데이터베이스에서 엔드포인트를 제거해야 합니다.
- 인터넷에 연결하고 Microsoft 루트 인증서 프로그램에서 인증서를 자동으로 업데이트하도록 Microsoft 인증서 서버를 구성할 수 있습니다. 제한된 인터넷 정책이 있는 환경에서 이 네트워크 검색 옵션을 구성할 경우 인터넷에 연결할 수 없는 CA/NDES 서버는 기본적으로 시간 초과에 15초가 걸릴 수 있습니다. 이렇게 하면 ISE와 같은 SCEP 프록시의 SCEP 요청 처리에 15초 지연이 추가될 수 있습니다. 응답이 수신되지 않은 경우 12초 후 SCEP 요청을 시간 초과하도록 ISE가 프로그래밍됩니다. 이 문제를 해결하려면 CA/NDES 서버에 대한 인터넷 액세스를 허용하거나 Microsoft CA/NDES 서버의 로컬 보안 정책에서 네트워크 검색 시간 초과 설정을 수정합니다. Microsoft 서버에서 이 컨피그레이션을 찾으려면 **Start(시작) > Administrative Tools(관리 툴) > Local Security Policy(로컬 보안 정책) > Public Key Policies(공개 키 정책) > Certificate Path Validation Settings(인증서 경로 검증 설정) > Network Retrieval(네트워크 검색)**으로 이동합니다.

클라이언트측 로깅

클라이언트 측 로깅 문제를 해결하는 데 사용되는 유용한 기술 목록은 다음과 같습니다.

- %temp%\spwProfileLog.txt 로그를 입력합니다. 명령을 사용하여 Microsoft Windows 응용 프로그램의 클라이언트측 로그를 확인합니다.
참고: WinHTTP는 Microsoft Windows 엔드포인트와 ISE 간의 연결에 사용됩니다. 오류 코드 목록은 Microsoft Windows [오류 메시지](#) 문서를 참조하십시오.
- Android 애플리케이션에 대한 클라이언트측 로그를 보려면 /sdcards/downloads/spw.log 명령을 입력합니다.
- MAC OSX의 경우 콘솔 애플리케이션을 사용하고 SPW 프로세스를 찾습니다.
- Apple iOS의 경우 [Apple Configurator 2.0](#)을 사용하여 메시지를 봅니다.

ISE 로깅

ISE 로그를 보려면 다음 단계를 완료합니다.

1. Administration(관리) > Logging(로깅) > **Debug Log Configuration(디버그 로그 컨피그레이션)**으로 이동하고 적절한 ISE 정책 노드를 선택합니다.
2. 필요에 따라 **클라이언트** 및 **프로비저닝** 로그를 디버그 또는 추적하도록 설정합니다.
3. MAC, IP, 사용자 등의 검색을 용이하게 하기 위해 문제를 재현하고 관련 시드 정보를 문서화합니다.
4. Operations(작업) > **Download Logs(로그 다운로드)**로 이동하고 적절한 ISE 노드를 선택합니다.
5. **Debug Logs(디버그 로그)** 탭에서 **ise-psc.log**라는 로그를 데스크톱에 다운로드합니다.

6. 로그 파일을 구문 분석하려면 Notepad ++와 같은 지능형 편집기를 사용합니다.

7. 문제가 격리되면 로그 수준을 기본 수준으로 되돌립니다.

NDES 로깅 및 문제 해결

자세한 내용은 [AD CS:네트워크 장치 등록 서비스](#) Windows Server [문제](#) 해결 문서

관련 정보

- [BYOD 솔루션 가이드 - 인증 기관 서버 구성](#)
- [Windows 2008 R2의 NDES 개요](#)
- [MSCEP 백서](#)
- [SSL을 지원하도록 NDES 서버 구성](#)
- [EAP-TLS와 함께 PEAP 또는 EAP-TLS를 사용하는 경우 인증서 요구 사항](#)
- [기술 지원 및 문서](#)