ISE SCEP 통합을 위한 HTTPS 지원 구성

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[배경 정보](#)
[구성](#)
[NDES 서버 인증서 컨피그레이션](#)
[NDES 서버 IIS 바인딩 구성](#)
[ISE 서버 컨피그레이션](#)
[다음을 확인합니다.](#)
[문제 해결](#)
[관련 정보](#)

소개

이 문서에서는 ISE(Identity Services Engine)와의 SCEP(Secure Certificate Enrollment Protocol) 통합을 위해 HTTPS(Hypertext Transfer Protocol Secure) 지원을 구성하는 데 필요한 단계를 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Microsoft의 IIS(인터넷 정보 서비스) 웹 서버에 대한 기본 지식
- ISE에서 SCEP 및 인증서 컨피그레이션 경험

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ISE 릴리스 1.1.x
- KB2483564 및 KB2633200용 핫픽스가 설치된 Windows Server 2008 R2 Enterprise

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 BYOD(Bring Your Own Device)에 대한 설명서로 제공됩니다. Microsoft 인증 기관, NDES(Network Device Enrollment Service) 및 SCEP 관련 서버 컨피그레이션에 대한 정확한 소스로 Microsoft의 TechNet을 참조하십시오.

배경 정보

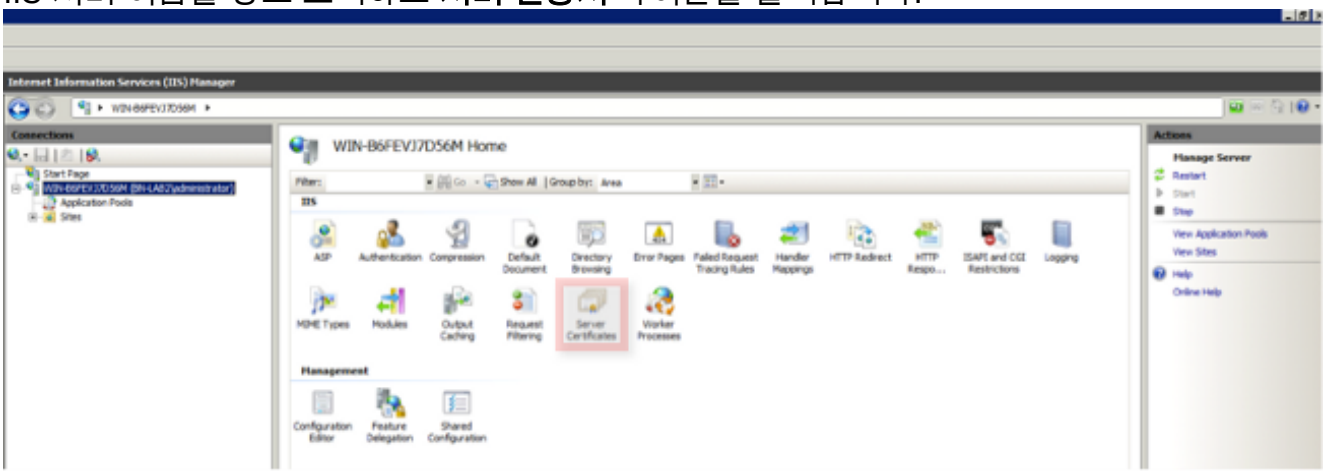
BYOD 구축에서 핵심 구성 요소 중 하나는 NDES 역할이 설치된 Microsoft 2008 R2 Enterprise 서버입니다. 이 서버는 AD(Active Directory) 포리스트의 구성원입니다. NDES를 처음 설치하는 동안 Microsoft의 IIS 웹 서버는 자동으로 설치되고 SCEP의 HTTP 종료를 지원하도록 구성됩니다. 일부 BYOD 구축에서 고객은 HTTPS를 사용하여 ISE와 NDES 간의 통신을 더 안전하게 보호할 수 있습니다. 이 절차에서는 SCEP 웹 사이트의 SSL(Secure Socket Layer) 인증서를 요청하고 설치하는 데 필요한 단계를 자세히 설명합니다.

구성

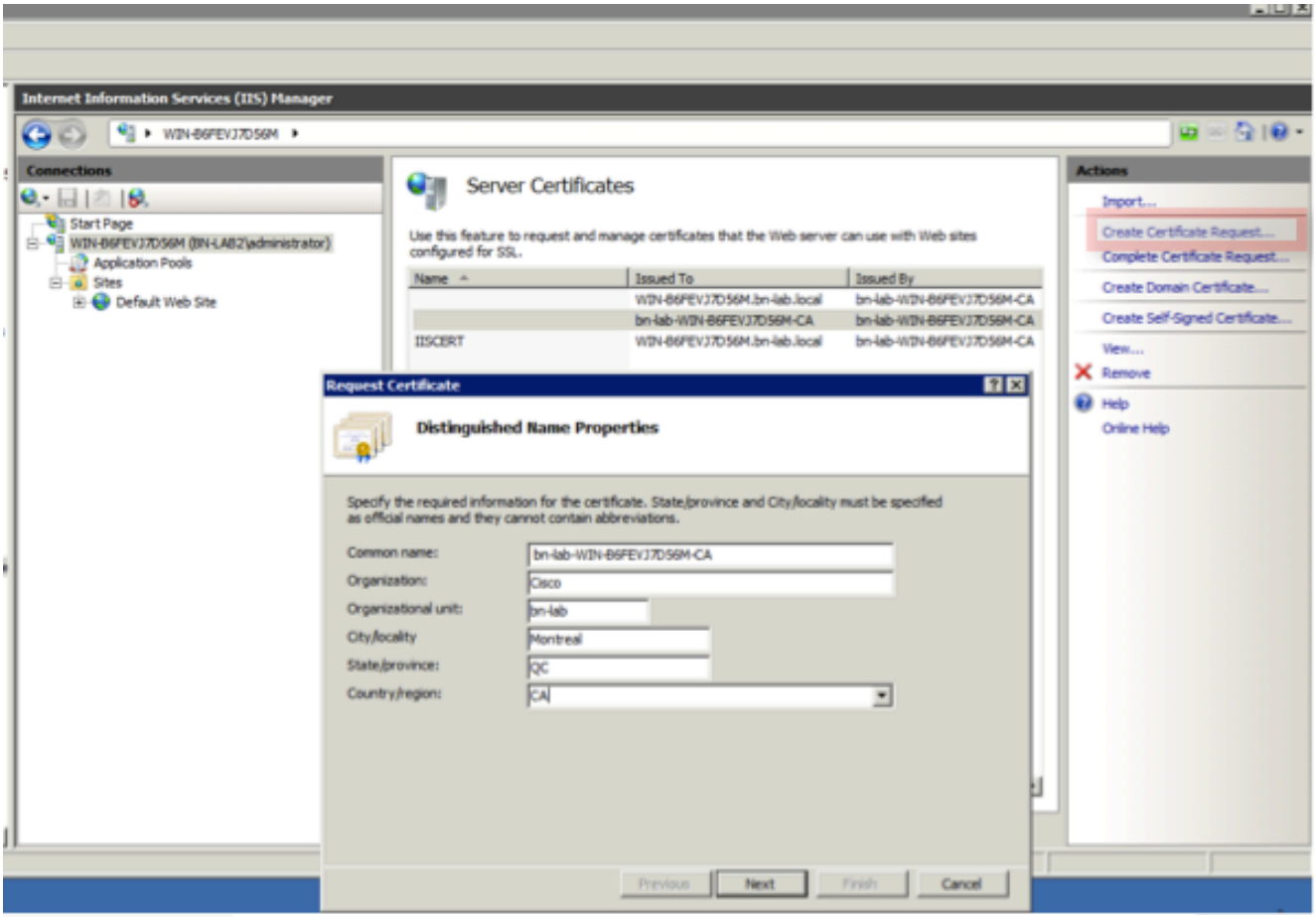
NDES 서버 인증서 컨피그레이션

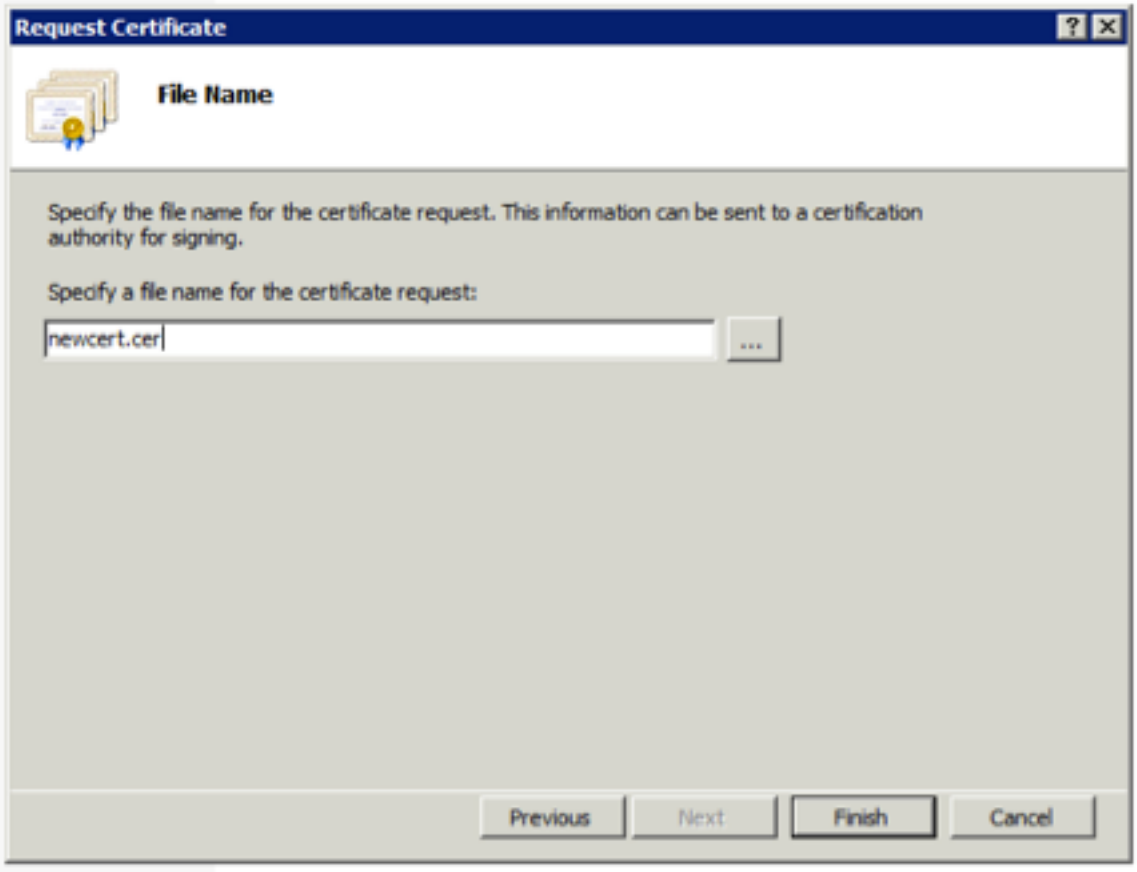
> **참고:** IIS에 대해 새 인증서를 구성해야 합니다(IIS가 Verisign과 같은 타사 PKI와 통합되거나 CA(인증 기관) 및 NDES 서버 역할이 별도의 서버로 구분되는 경우에만 필요). 설치에서 NDES 역할이 현재 Microsoft CA 서버에 있는 경우 IIS는 CA 설정 중에 생성된 서버 ID 인증서를 사용합니다. 이와 같은 독립형 컨피그레이션의 경우 이 문서의 NDES **Server IIS 바인딩 컨피그레이션** 섹션으로 직접 건너뜁니다.

1. 콘솔 또는 RDP를 통해 NDES 서버에 연결합니다.
2. **시작 -> 관리 도구 -> 인터넷 정보 서비스(IIS) 관리자를 클릭합니다**.
3. IIS 서버 이름을 강조 표시하고 **서버 인증서** 아이콘을 클릭합니다.

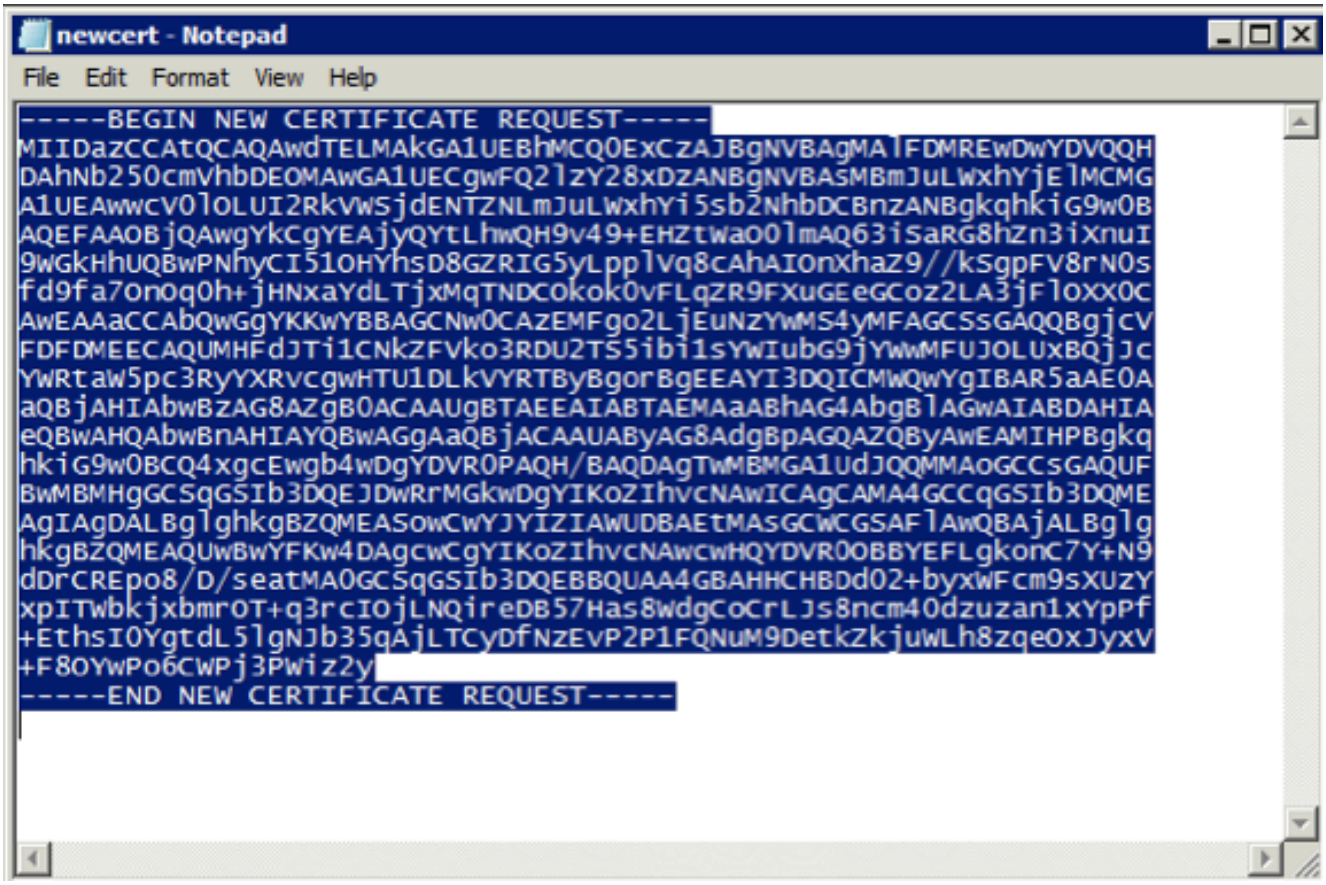


4. Create **Certificate Request(인증서 요청 생성)**를 클릭하고 필드를 완료합니다.

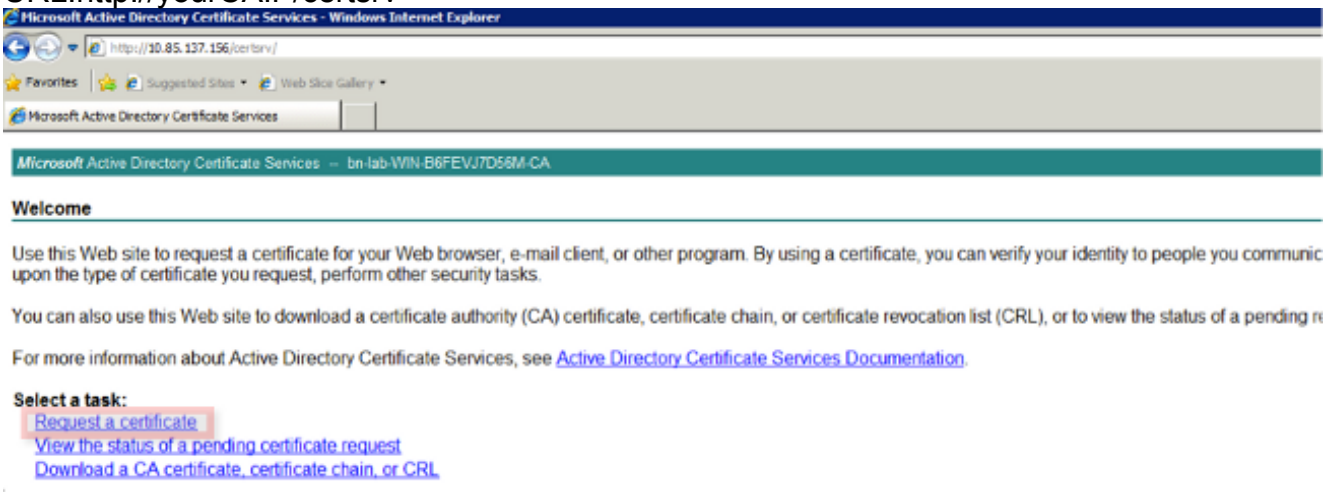




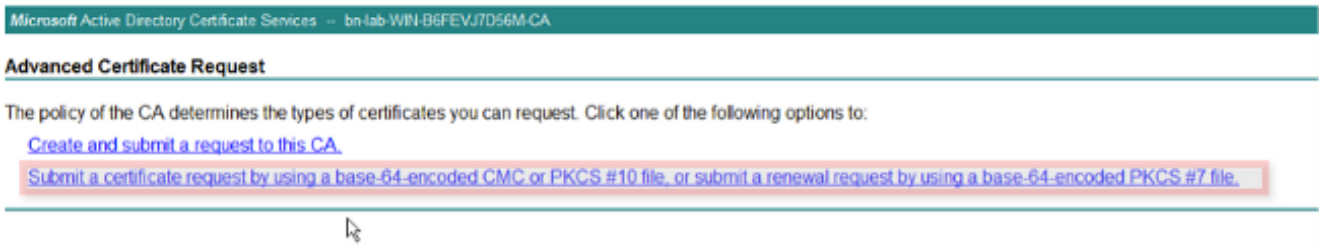
5. 텍스트 편집기로 이전 단계에서 만든 .cer 파일을 열고 클립보드로 내용을 복사합니다.



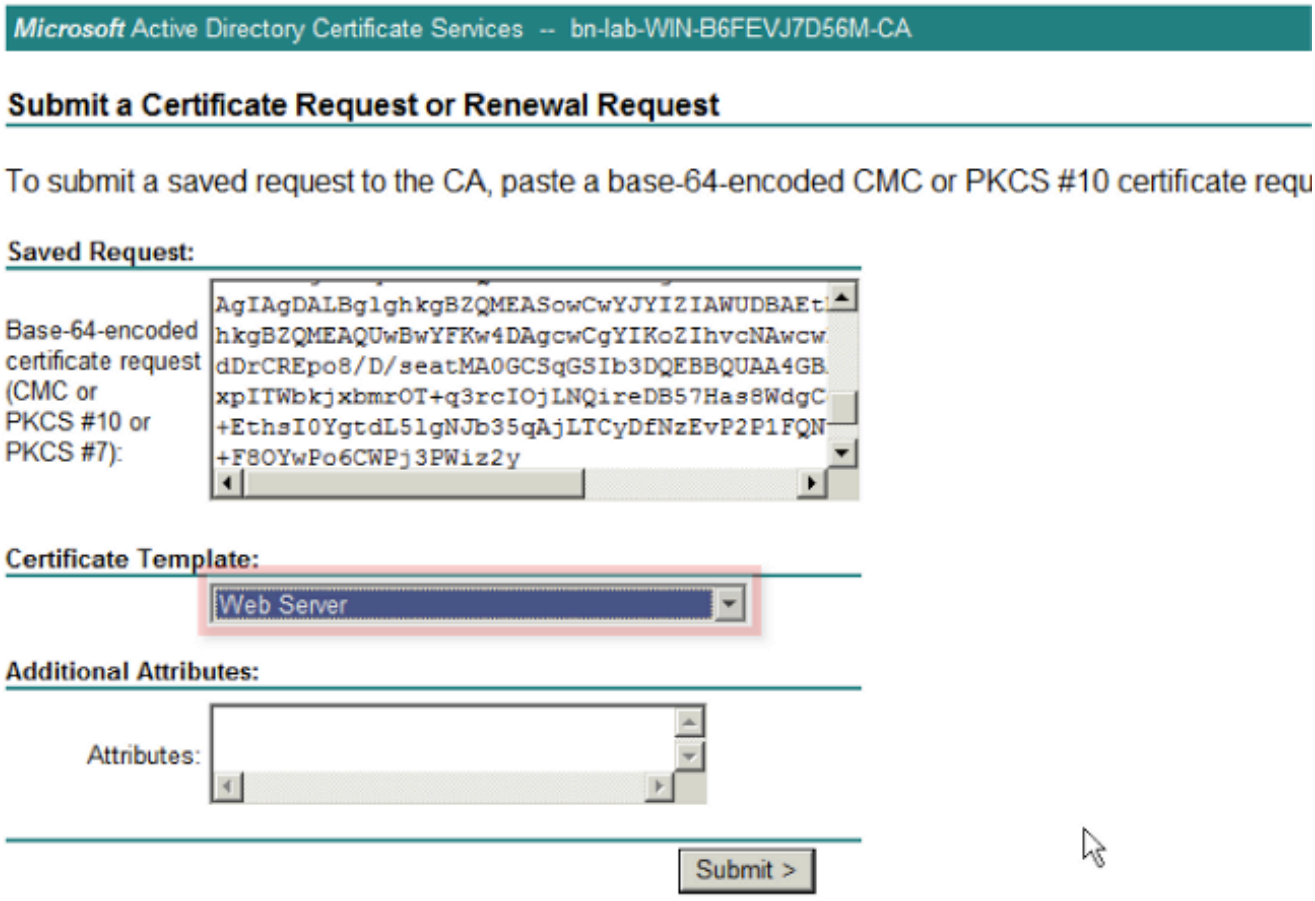
6. Microsoft CA Web Enrollment 웹 사이트에 액세스하여 **Request a Certificate**를 클릭합니다.예 URL:http://yourCAIP/certsrv



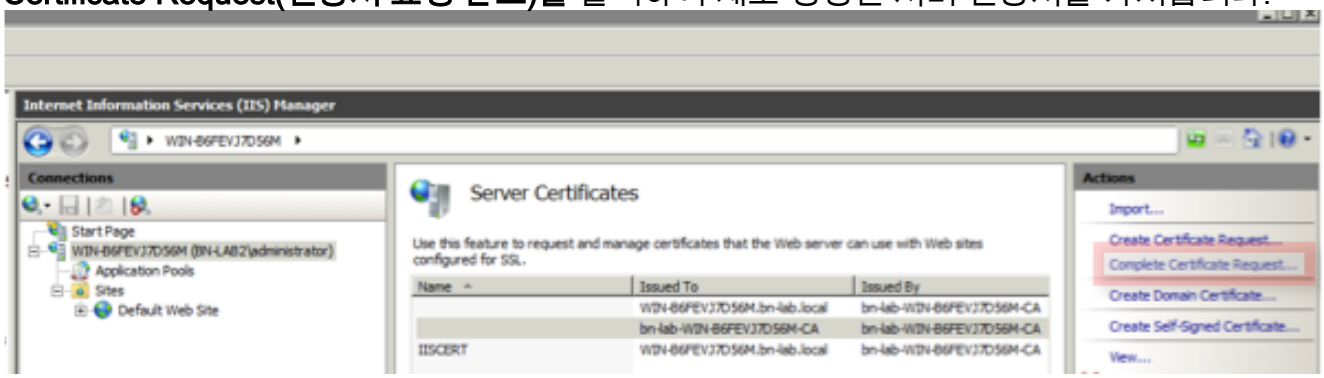
7. Submit **a certificate request by using...을** 클릭합니다..클립보드의 인증서 내용에 붙여넣고 **웹 서버** 템플릿을 선택합니다.



8. Submit(**제출**)을 클릭한 다음 인증서 파일을 데스크톱에 저장합니다.

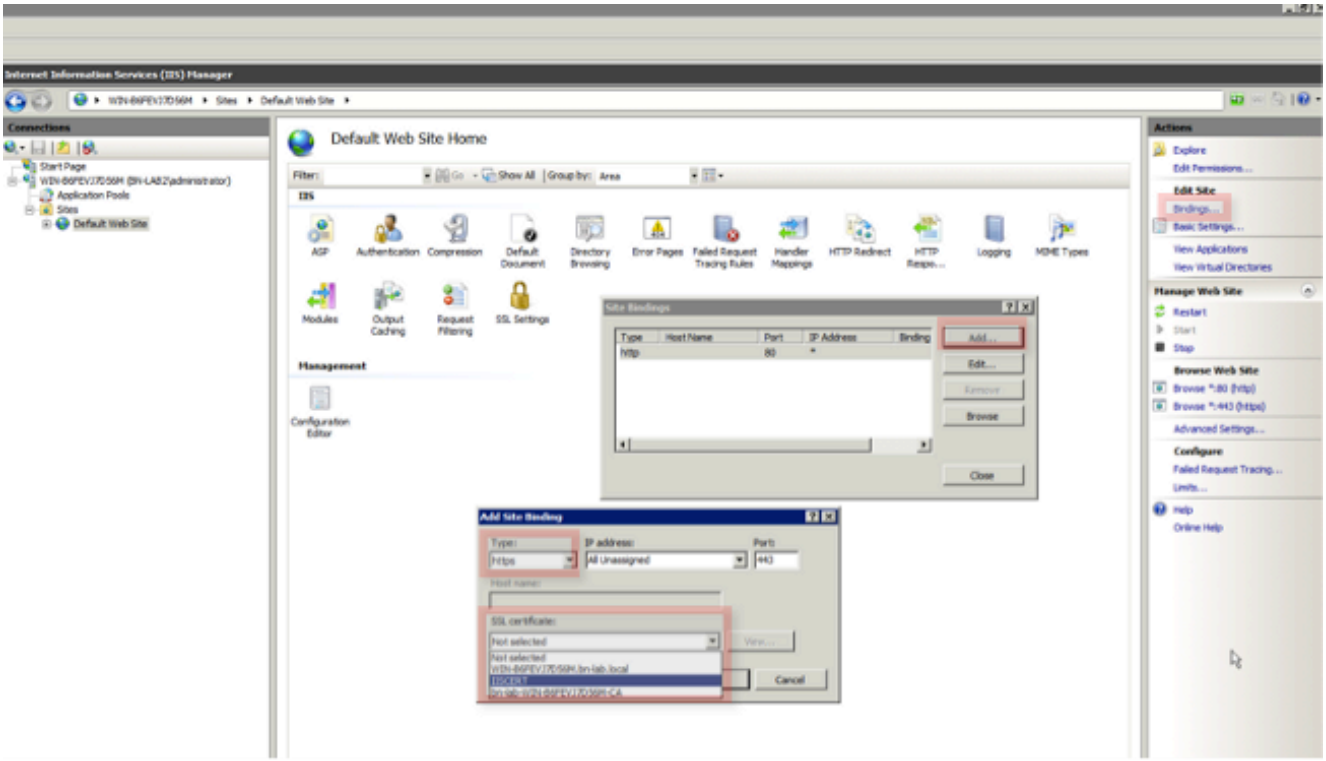


9. NDES 서버로 돌아가서 IIS 관리자 유틸리티를 엽니다.서버 이름을 클릭한 다음 **Complete Certificate Request(인증서 요청 완료)를** 클릭하여 새로 생성된 서버 인증서를 가져옵니다.



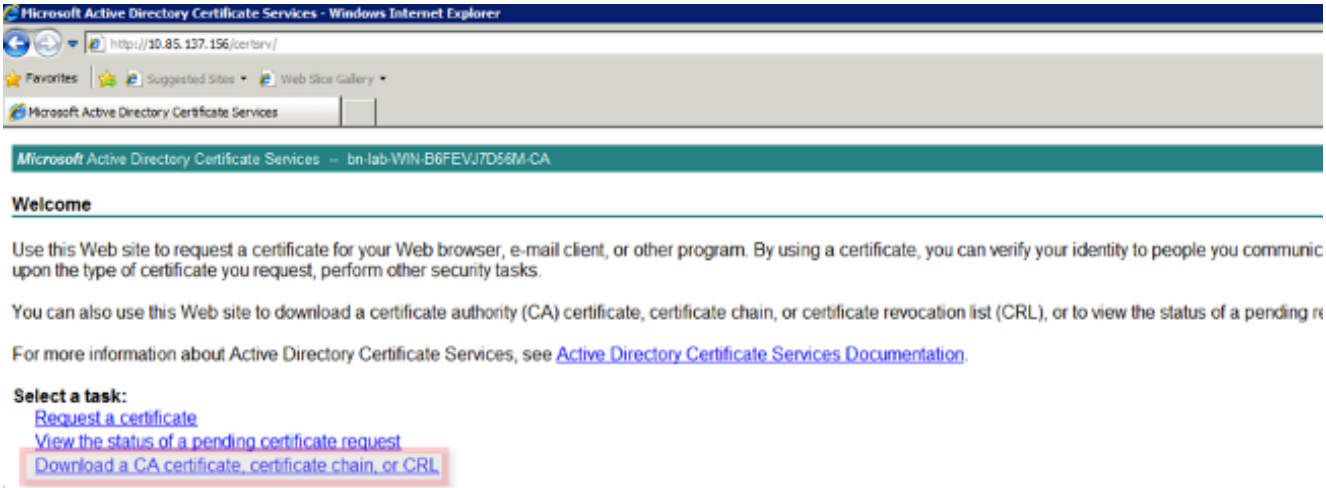
NDES 서버 IIS 바인딩 구성

1. **서버 이름**을 확장하고 **Sites**를 **확장하고** Default **Web Site를 클릭합니다**.
2. 오른쪽 상단 모서리에서 **Bindings**를 클릭합니다.
3. Add(**추가)**를 클릭하고 Type(유형)을 HTTPS로 변경하고 드롭다운 목록에서 인증서를 선택합니다.
4. **확인을 클릭합니다.**

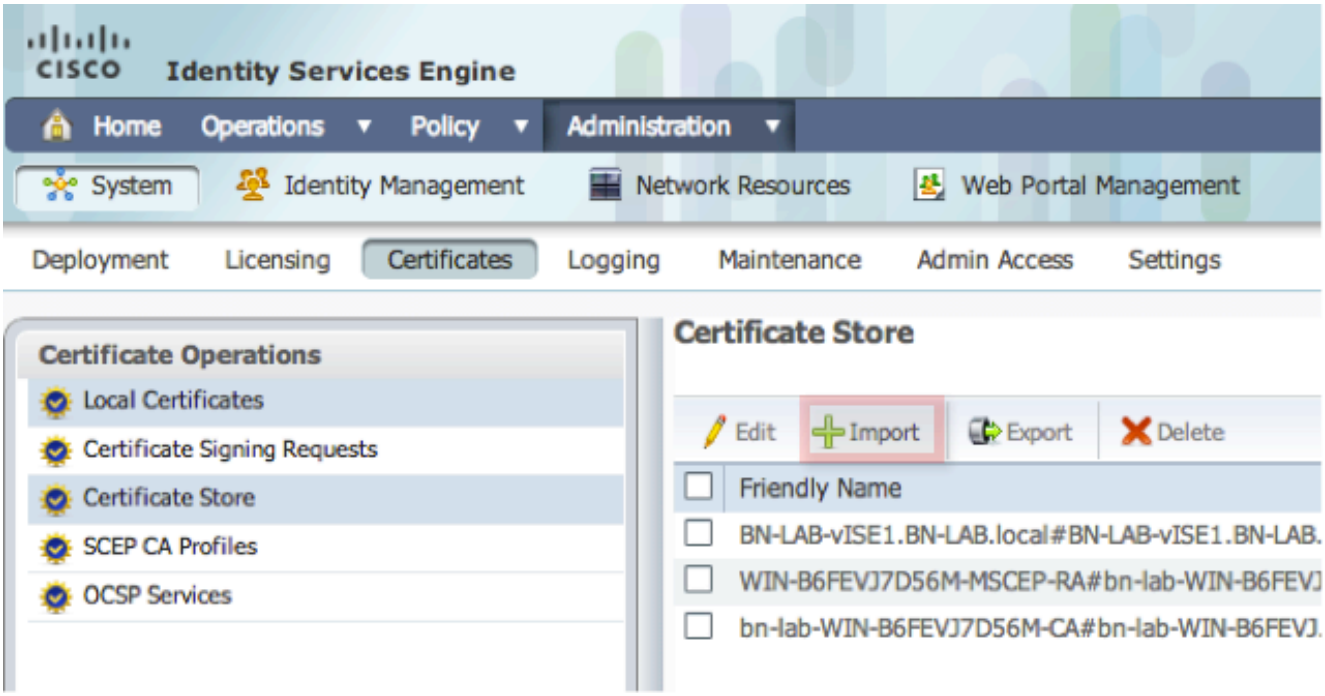


ISE 서버 컨피그레이션

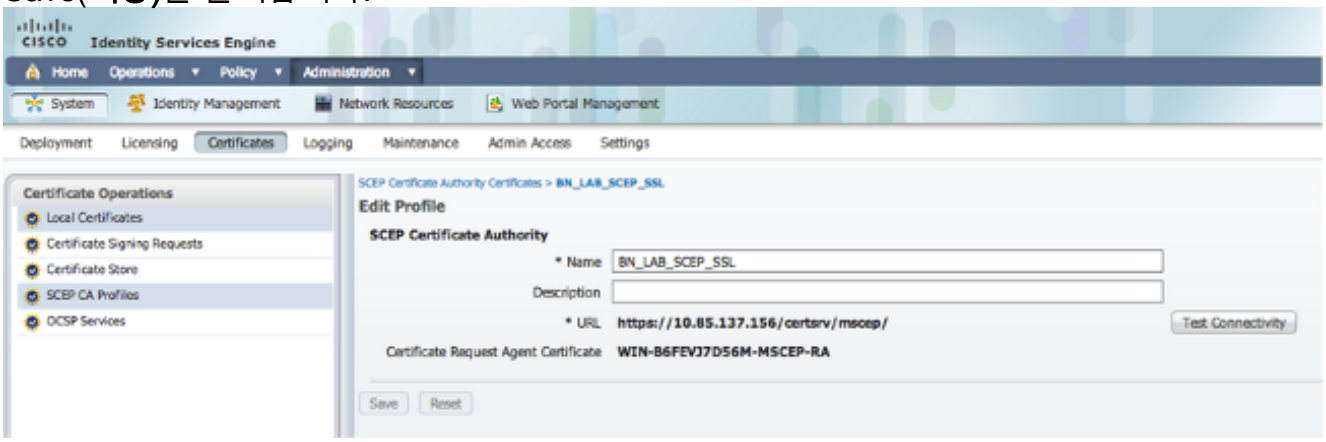
1. CA 서버의 웹 등록 인터페이스에 연결하고 CA 인증서 체인을 다운로드합니다.



2. ISE GUI에서 **Administration(관리) -> Certificates(인증서) -> Certificate Store(인증서 저장소)로 이동하고** CA 인증서 체인을 ISE 저장소로 가져옵니다.



3. Administration(관리) -> **Certificates(인증서) -> SCEP CA Profiles(SCEP CA 프로파일)로 이동하고** HTTPS에 대한 URL을 구성합니다.Test **Connectivity(연결 테스트)**를 클릭한 다음 Save(**저장)**를 클릭합니다.



다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

- Administration(관리) -> **Certificates(인증서) -> Certificate Store(인증서 저장소)로** 이동하여 CA 인증서 체인과 NDES Server Registration Authority(RA) 인증서가 있는지 확인합니다.
- Wireshark 또는 TCP Dump를 사용하여 ISE 관리 노드와 NDES 서버 간의 초기 SSL 교환을 모니터링합니다.

Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

- BYOD 네트워크 토폴로지를 논리적 경로로 분석하여 엔드포인트(ISE, NDES 및 CA) 간의 경로

를 따라 디버그 지점을 식별하고 캡처합니다.
- ISE와 NDES 서버 간에 TCP 443이 양방향으로 허용되는지 확인합니다.
- CA 및 NDES 서버 애플리케이션 로그에서 등록 오류를 모니터링하고 Google 또는 TechNet을 사용하여 이러한 오류를 조사합니다.
- ISE PSN에서 TCP 덤프 유틸리티를 사용하고 NDES 서버에서 들어오고 나가는 트래픽을 모니터링합니다.이 위치는 **Operations(운영)** > Diagnostic Tools(진단 **도구)** > General Tools(**일반 도구)에 있습니다**.
- NDES 서버에 Wireshark를 설치하거나 중간 스위치에서 SPAN을 사용하여 ISE PSN에서 SCEP 트래픽을 캡처합니다.

Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령**을** 지원합니다.**show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

참고: **debug** 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

관련 정보

- BYOD에 대한 SCEP 지원 구성
- 기술 지원 및 문서 – Cisco Systems