OpenSSL을 사용하여 IND 및 ISE pxGrid 통합을 위한 SAN 인증서 생성

목차

소개

이 문서에서는 IND(Industrial Network Director)와 Identity Services Engine 간의 pxGrid 통합을 위한 SAN 인증서를 생성하는 방법에 대해 설명합니다.

배경 정보

pxGrid 사용을 위해 Cisco ISE에서 인증서를 생성할 때 ISE는 FQDN 또는 IP 주소만 허용하므로 서버 짧은 호스트 이름을 ISE GUI에 입력할 수 없습니다.

호스트 이름 및 FQDN을 포함하는 인증서를 생성하려면 ISE 외부에서 인증서 요청 파일을 생성해야 합니다. OpenSSL을 사용하여 SAN(주체 대체 이름) 필드 항목이 있는 CSR(Certificate Signing Request)을 생성할 수 있습니다.

이 문서에는 IND 서버와 ISE 서버 간의 pxGrid 통신을 활성화하는 포괄적인 단계가 포함되어 있지 않습니다. 이러한 단계는 pxGrid가 구성되고 서버 호스트 이름이 필요한 것으로 확인된 후에 사용할 수 있습니다. ISE 프로파일러 로그 파일에서 이 오류가 발견되면 통신에 호스트 이름 인증서가 필요합니다.

```
Unable to get sync statusjava.security.cert.CertificateException: No subject alternative DNS name matcht
```

pxGrid 통신을 사용하는 IND의 초기 구축 단계는 https://www.cisco.com/c/dam/en/us/td/docs/switches/ind/install/IND_PxGrid_Registration_Guide_Final.pdf 서 확인할 수 있습니다.

필요한 애플리케이션

- Cisco IND(Industrial Network Director)
- Cisco ISE(Identity Services Engine)
- OpenSSL
  - MacOS뿐만 아니라 대부분의 최신 Linux 버전에서는 OpenSSL 패키지가 기본적으로 설치됩니다. 명령을 사용할 수 없는 경우 운영 체제의 패키지 관리 애플리케이션을 사용하여 OpenSSL을 설치하십시오.
  - Windows용 OpenSSL에 대한 자세한 내용은

https://wiki.openssl.org/index.php/Binaries을 참조하십시오.

추가 정보

이 문서에서는 다음 세부 정보를 사용합니다.

- IND 서버 호스트 이름: rch-mas-ind
- FQDN: rch-mas-ind.cisco.com
- OpenSSL 구성: rch-mas-ind.req
- 인증서 요청 파일 이름: rch-mas-ind.csr
- 개인 키 파일 이름: rch-mas-ind.pem
- 인증서 파일 이름: rch-mas-ind.cer

프로세스 단계

인증서 CSR 생성

1. OpenSSL이 설치된 시스템에서 SAN 정보를 포함하여 OpenSSL 옵션에 대한 요청 텍스트 파일을 생성합니다.
   - 대부분의 "_default" 필드는 선택 사항이며, #2단계에서 OpenSSL 명령을 실행하는 동안 답변을 입력할 수 있습니다.
   - SAN 세부 정보(DNS.1, DNS.2)가 필요하며 DNS 짧은 호스트 이름 및 서버의 FQDN을 모두 포함해야 합니다. DNS.3, DNS.4 등을 사용하여 필요한 경우 DNS 이름을 더 추가할 수 있습니다.
   - 요청 파일 텍스트 파일 예:

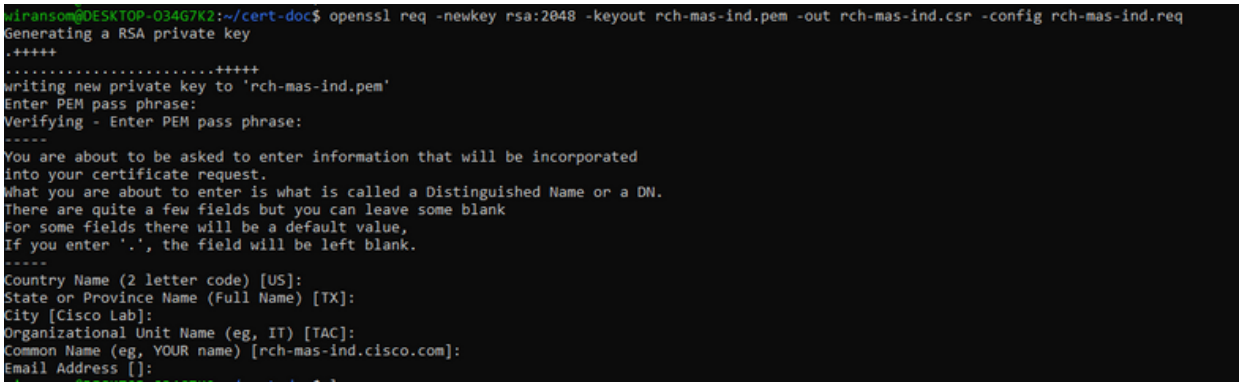
```
[요청]
distinguished_name = 이름
req_extensions = v3_req

[이름]
countryName = 국가 이름(2자 코드)
countryName_default = 미국
stateOrProvinceName = 시/도 이름(전체 이름)
stateOrProvinceName_default = TX
localityName = 시
localityName_default = Cisco 랩
organizationalUnitName = 조직 구성 단위 이름(예: IT)
organizationalUnitName_default = TAC
commonName = Common Name(예: 사용자 이름)
commonName_max = 64
commonName_default = rch-mas-ind.cisco.com
emailAddress = 이메일 주소
emailAddress_max = 40
```

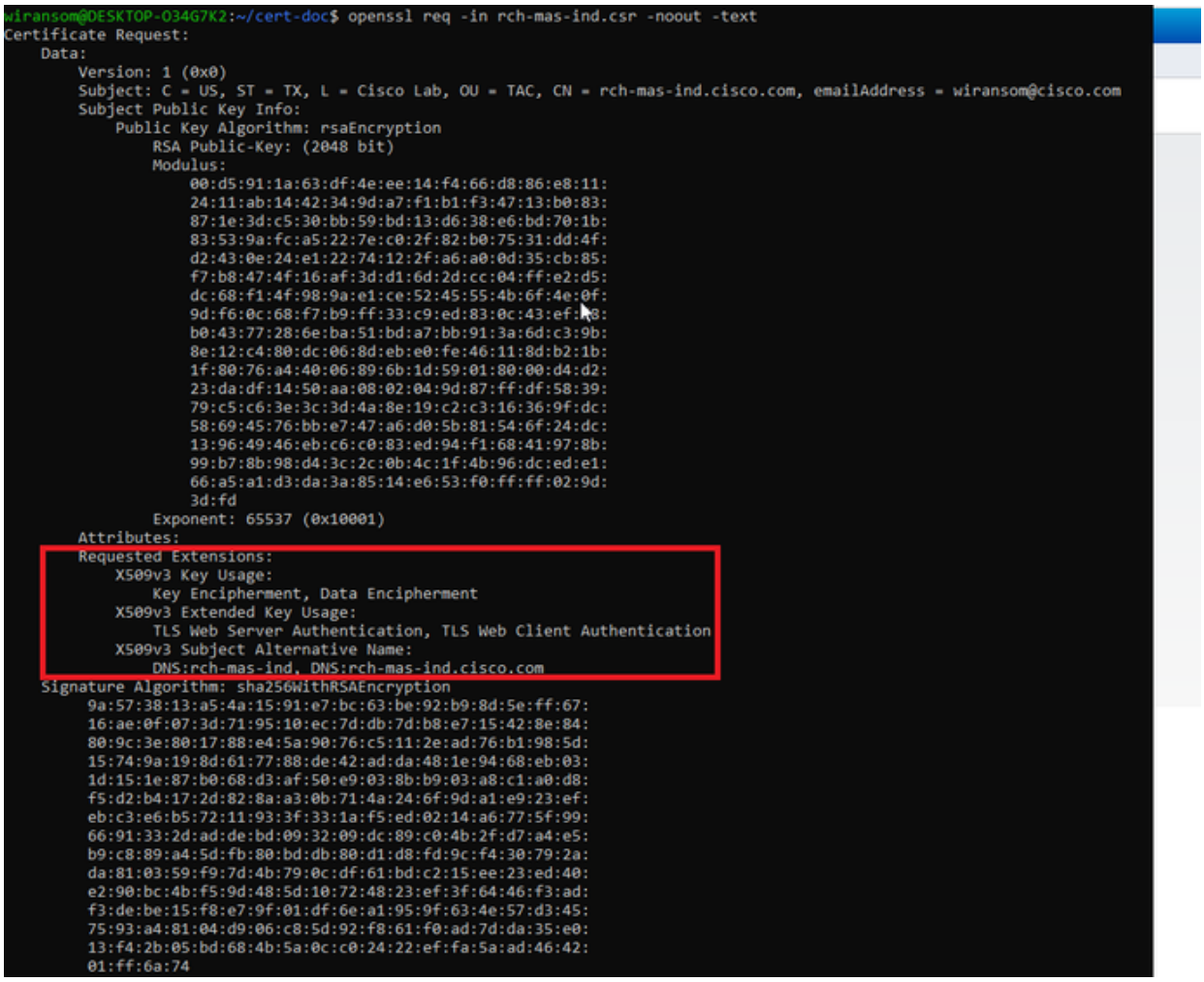
```
[v3_req]
keyUsage = keyEncipherment, 데이터 암호화
확장 키 사용 = serverAuth, clientAuth
subjectAltName = @alt_names

[alt_names]
DNS.1 = rch-mas-ind
DNS.2 = rch-mas-ind.cisco.com
```

2. OpenSSL을 사용하여 SAN 필드에 DNS 짧은 호스트 이름으로 CSR을 생성합니다. CSR 파일 외에 개인 키 파일을 생성합니다.
   - 명령을 사용합니다:
     openssl req -newkey rsa:2048 -keyout <서버>.pem -out <서버>.csr -config <서버>.req
   - 프롬프트가 표시되면 선택한 비밀번호를 입력합니다. 이 비밀번호는 이후 단계에서 사용되므로 반드시 기억해야 합니다.
   - 프롬프트가 표시되면 유효한 이메일 주소를 입력하거나 필드를 비워 두고 <ENTER>를 누릅니다.



3. 필요한 경우 CSR 파일 정보를 확인합니다. SAN 인증서의 경우 이 스크린샷에서 강조 표시된 대로 "x509v3 Subject Alternative Name"을 확인합니다.
   - 명령줄:
     openssl req -in <server>.csr -noout -text



4. 텍스트 편집기에서 CSR 파일을 엽니다. 보안상의 이유로, 샘플 스크린샷은 불완전하고 편집되었습니다. 실제로 생성된 CSR 파일에는 더 많은 행이 포함되어 있습니다.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDMDCCAhgCAQAwfzELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAlRYMRIwEAYDVQQH
DAlDaXNjbyBMYWIxDDAKBgNVBAsMA1RBQzEeMBwGA1UEAwwVcmNoLW1hcy1pbmQu
Y2lzY28uY29tMSEwHwYJKoZIhvcNAQkBFhJ3aXJhbnNvbUBjaXNjby5jb20wggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDVkRpj307uFPRm2IboESQRqxRC
NJ2n8bHzRxOwg4cePcUwu1m9E9Y45r1wG4NTmvylIn7AL4KwdTHdT9JDDiThInQS
L6agDTXLhfe4R08Wrz3RbS3MBP/i1dxo8U+YmuHOUkVVS29OD532DGj3uf8zye2D
0iPa3xRQqggCBJ2H/99YOXnFxj48PUqOGcLDFjaf3FhpRXa750em0FuBVG8k3BOW
AAGgbDBqBgkqhkiG9w0BCQ4xXTBbMAsGA1UdDwQEAwIEMDAdBgNVHSUEFjAUBggr
BgEFBQcDAQYIKwYBBQUHAwIwLQYDVR0RBCYwJIILcmNoLW1hcy1pbmSCFXJjaC1t
YXMtaW5kLmNpc2NvLmNvbTANBgkqhkiG9w0BAQsFAAOCAQEAmlc4E6VKFZHnvGO+
krmNXv9nFq4PBz1xlRDsfdt9uOcVQo6EgJw+gBeI5FqQdsURLq12sZhdFXSaGY1h
d4jeQq3aSB6UaOsDHRUeh7Bo069Q6QOLuQOowaDY9dK0Fy2CiqMLcUokb52h6SPv
Af9qdA==
-----END CERTIFICATE REQUEST-----
```

5. 개인 키 파일(<server>.pem)을 이후 단계에서 사용한 대로 PC에 복사합니다.

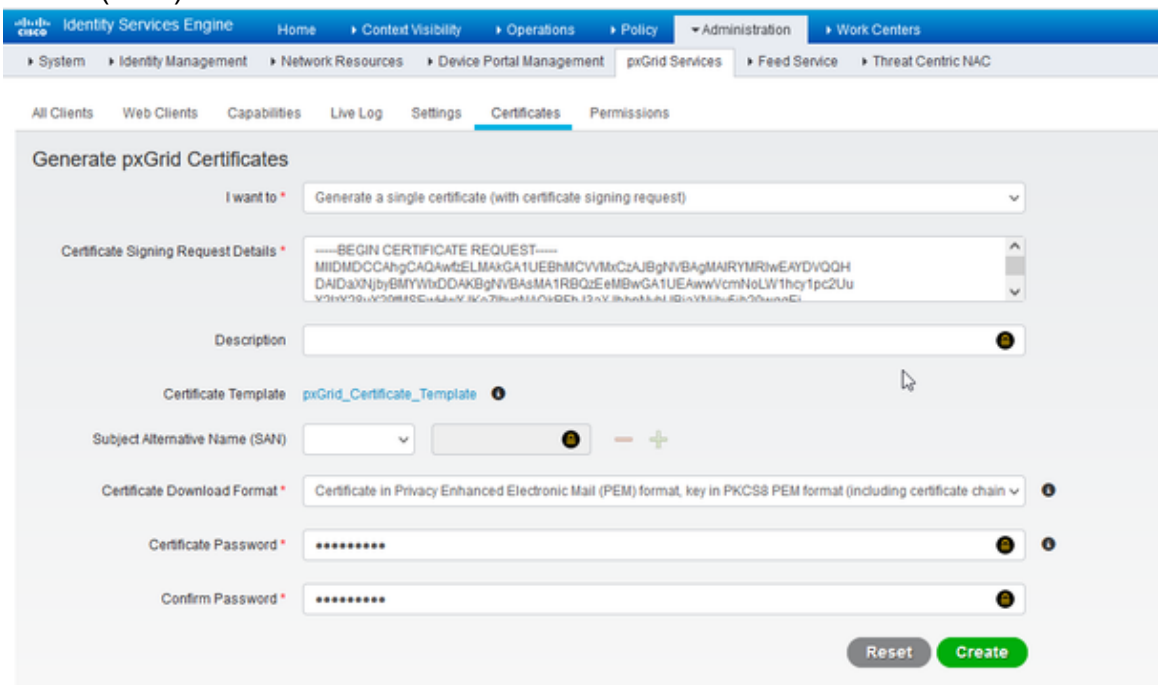
Cisco ISE를 사용하여 생성된 CSR 파일 정보를 사용하여 인증서를 생성합니다

ISE GUI에서 다음을 수행합니다.

1. 기존 pxGrid 클라이언트를 제거합니다.

- Administration(관리) > pxGrid Services(pxGrid 서비스) > All Clients(모든 클라이언트)로 이동합니다.
- 기존 클라이언트 호스트 이름을 찾아 선택합니다(나열된 경우).
- 선택한 경우 삭제 버튼을 클릭하고 "선택한 항목 삭제"를 선택합니다. 필요에 따라 확인합니다.

2. 새 인증서를 만듭니다.
   - pxGrid 서비스 페이지에서 Certificates(인증서) 탭을 클릭합니다.
   - 다음 옵션을 선택합니다.
     - "원하는 기능":
       - "단일 인증서 생성(인증서 서명 요청 포함)"
     - "CSR(Certificate Signing Request) 세부 정보:
       - 텍스트 편집기에서 CSR 세부사항을 복사/붙여넣습니다. BEGIN 및 END 행을 포함해야 합니다.
     - "Certificate Download Format(인증서 다운로드 형식)"
       - "PEM(Privacy Enhanced Electronic Mail) 형식의 인증서, PKCS8 PEM 형식의 키"
     - 인증서 비밀번호를 입력하고 확인합니다.
     - Create(생성) 버튼을 클릭합니다.

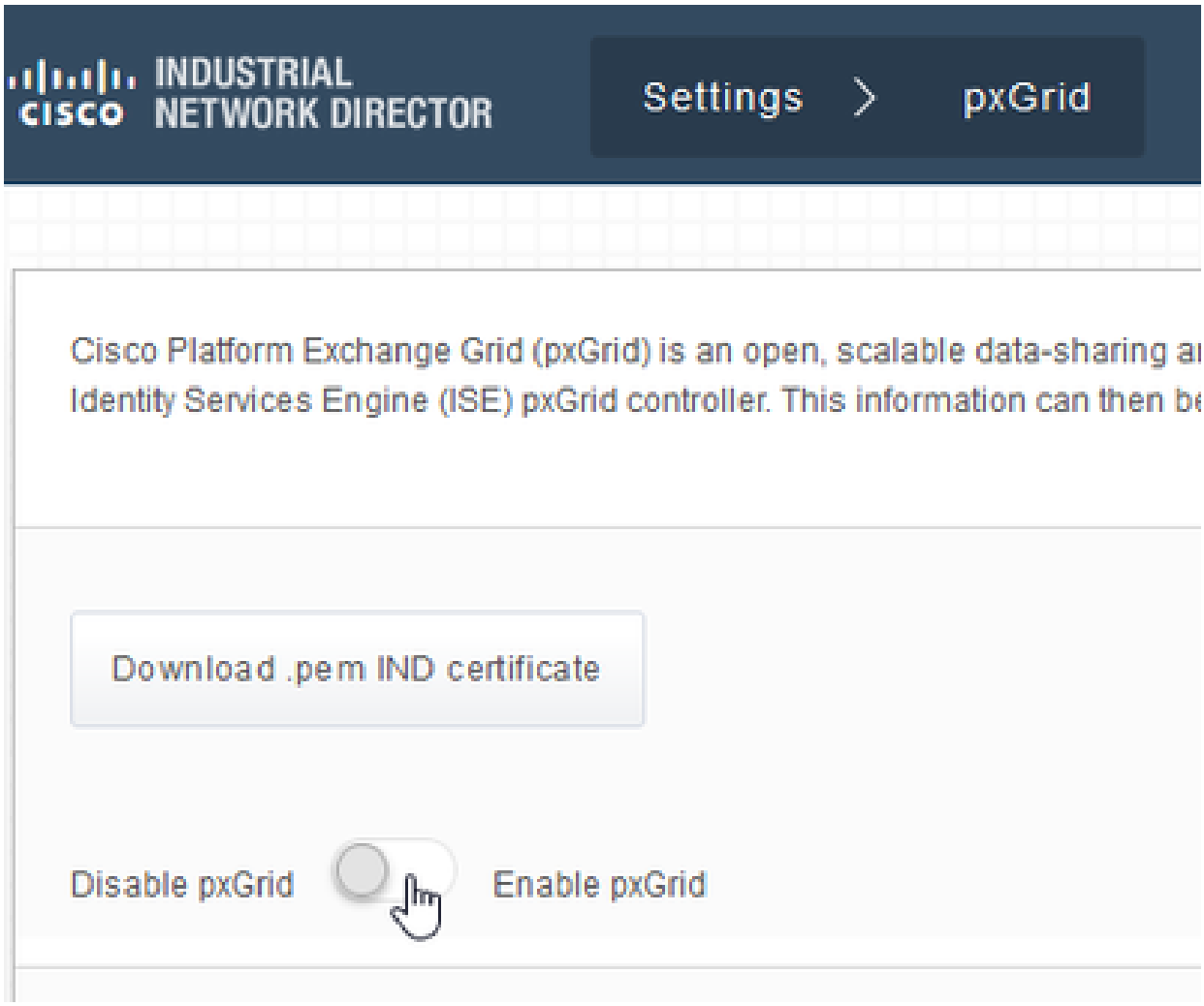


     - 이렇게 하면 인증서 파일 및 인증서 체인에 대한 추가 파일이 포함된 ZIP 파일이 생성 및 다운로드됩니다. ZIP을 열고 인증서를 추출합니다.
       - 파일 이름은 일반적으로 <IND server fqdn>.cer입니다.
       - 일부 ISE 버전에서 파일 이름은 <IND fqdn>_<IND short name>.cer입니다

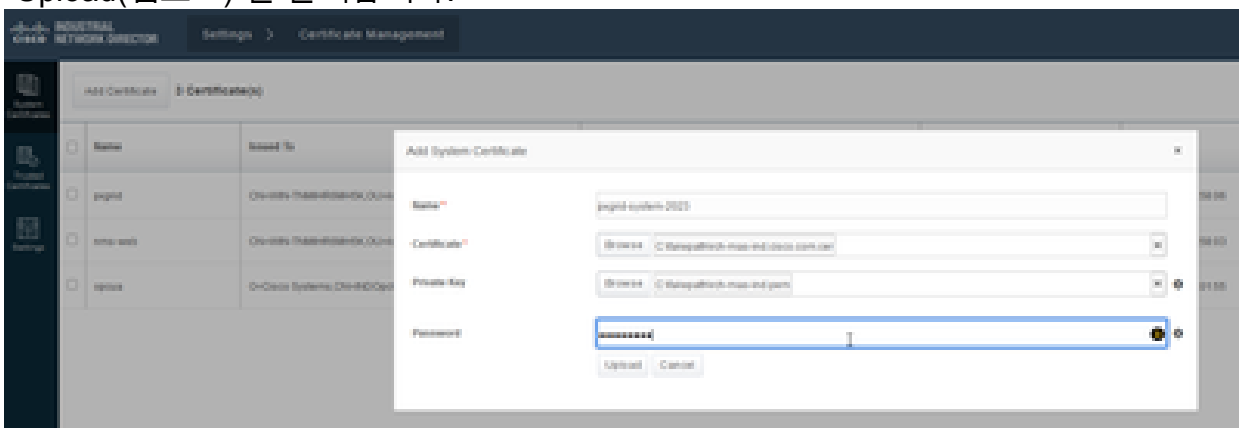
새 인증서를 IND 서버로 가져오고 pxGrid 사용을 위해 활성화합니다

IND GUI 내에서

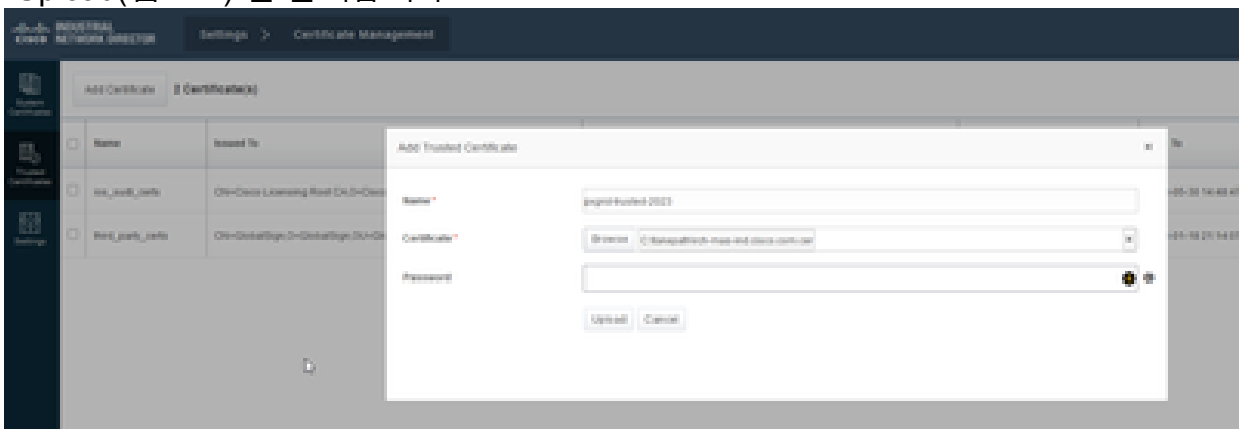
1. 새 인증서를 가져오고 활성 인증서로 설정할 수 있도록 pxGrid 서비스를 비활성화합니다.
   - Settings(설정) > pxGrid로 이동합니다.
   - pxGrid를 비활성화하려면 클릭합니다.



2. 새 인증서를 시스템 인증서로 가져옵니다.
   - Settings(설정) > Certificate Management(인증서 관리)로 이동합니다.
   - "System Certificates(시스템 인증서)"를 클릭합니다.
   - "Add Certificate(인증서 추가)"를 클릭합니다.
   - 인증서 이름을 입력합니다.
   - "Certificate(인증서)" 왼쪽에 있는 "Browse(찾아보기)"를 클릭하고 새 인증서 파일을 찾습니다.
   - "Certificate(인증서)" 왼쪽에 있는 "Browse(찾아보기)"를 클릭하고 CSR을 생성할 때 저장된 개인 키를 찾습니다.
   - OpenSSL을 사용하여 개인 키 및 CSR을 생성할 때 이전에 사용한 비밀번호를 입력합니다.
   - "Upload(업로드)"를 클릭합니다.



3. 새 인증서를 신뢰할 수 있는 인증서로 가져옵니다.
    - Settings(설정) > Certificate Management(인증서 관리)로 이동하고 "Trusted Certificates(신뢰할 수 있는 인증서)"를 클릭합니다.
    - "Add Certificate(인증서 추가)"를 클릭합니다.
    - 인증서 이름을 입력합니다. 이 이름은 시스템 인증서에서 사용되는 이름과 달라야 합니다.
    - "Certificate(인증서)" 왼쪽에 있는 "Browse(찾아보기)"를 클릭하고 새 인증서 파일을 찾습니다.
    - 비밀번호 필드는 비워둘 수 있습니다.
    - "Upload(업로드)"를 클릭합니다.

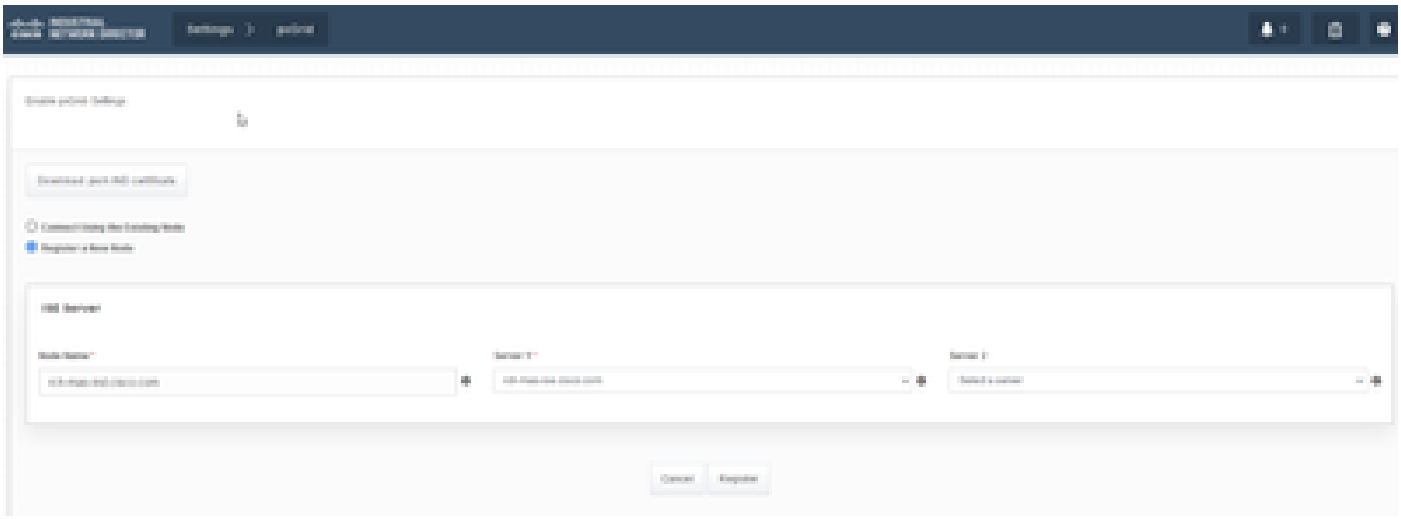


4. 새 인증서를 사용하도록 pxGrid를 설정합니다.
    - Settings(설정) > Certificate Management(인증서 관리)로 이동하여 "Settings(설정)"를 클릭합니다.
    - 아직 수행하지 않은 경우 "pxGrid" 아래에서 "CA Certificate"를 선택합니다.
    - 인증서 가져오기 중에 생성된 시스템 인증서 이름을 선택합니다.
    - 저장을 클릭합니다.

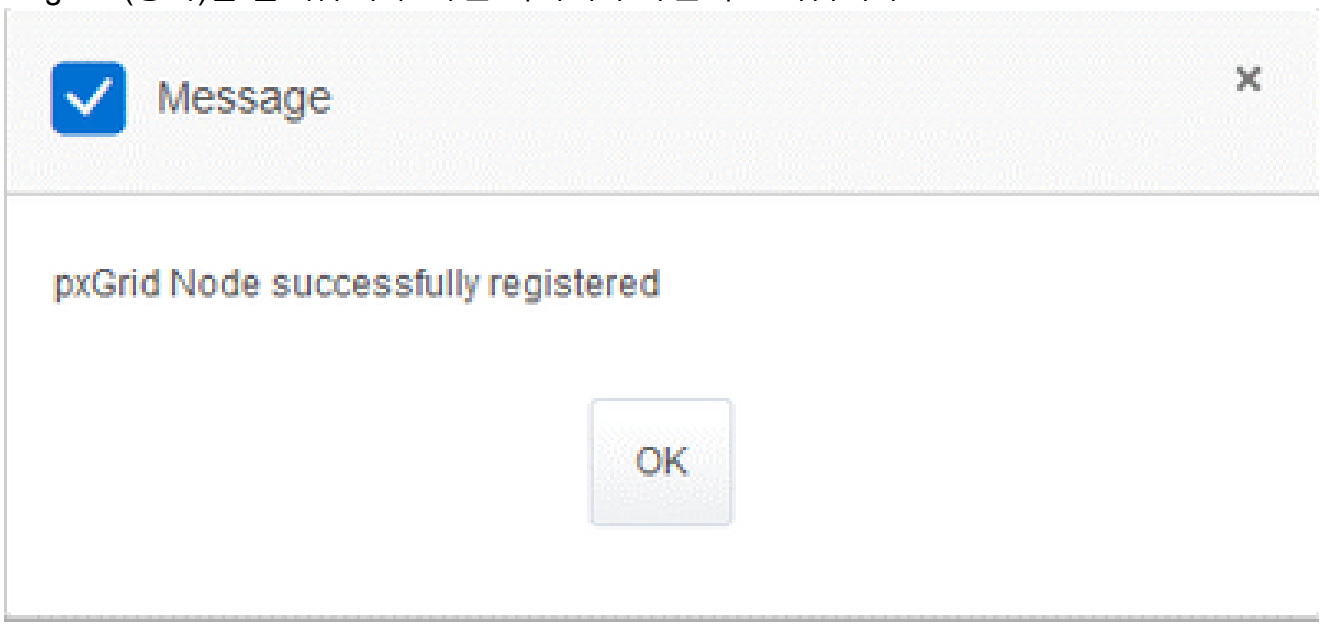
pxGrid를 활성화하고 ISE 서버에 등록

IND GUI 내에서

1. Settings(설정) > pxGrid로 이동합니다.
2. 슬라이더를 클릭하여 pxGrid를 활성화합니다.
3. 이 IND 서버에서 ISE에 pxGrid를 처음 등록하는 경우가 아니면 "기존 노드를 사용하여 연결"을 선택합니다. IND 노드 및 ISE 서버 정보가 자동으로 채워집니다.
4. 필요한 경우 새 IND 서버를 등록하여 pxGrid를 사용하려면 "Register a New Node(새 노드 등록)"를 선택합니다. IND 노드 이름을 입력하고 필요에 따라 ISE 서버를 선택합니다.
    - ISE 서버가 Server 1(서버 1) 또는 Server 2(서버 2)의 드롭다운 옵션 내에 나열되지 않은 경우 Settings(설정) > Policy Server(정책 서버)를 사용하여 새 pxGrid 서버로 추가할 수 있습니다



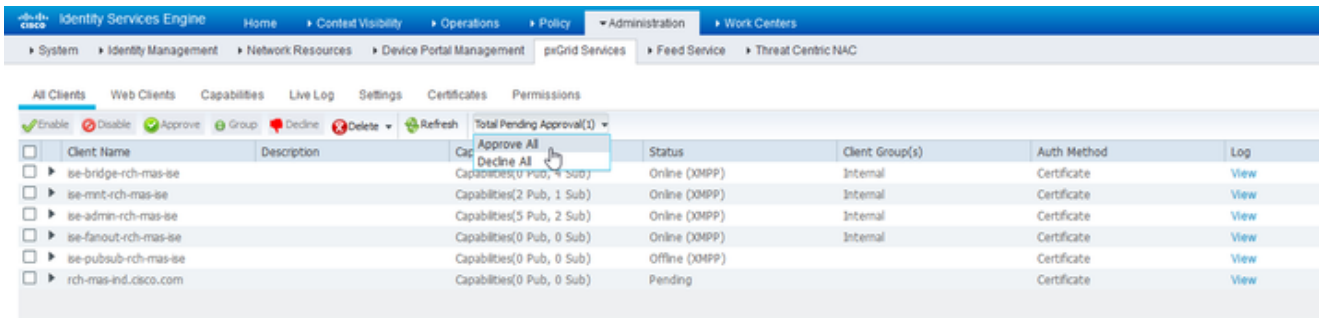
5. Register(등록)를 클릭합니다. 확인 메시지가 화면에 표시됩니다.



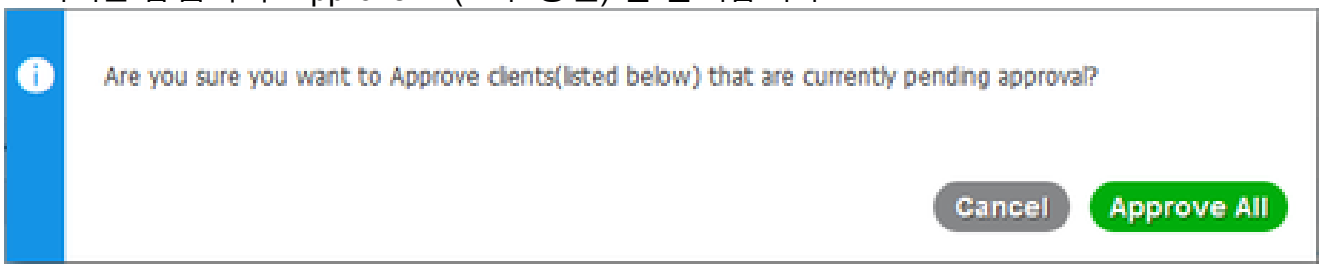
ISE 서버에서 등록 요청 승인

ISE GUI에서 다음을 수행합니다.

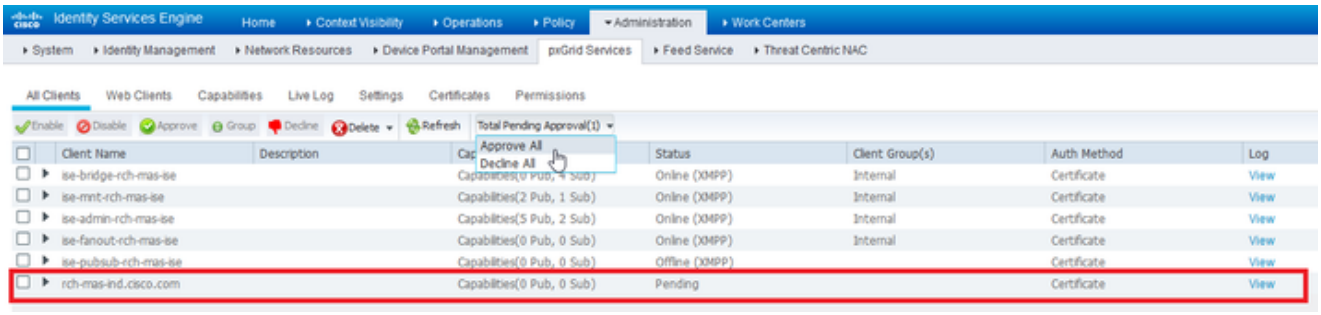
1. Administration(관리) > pxGrid Services(pxGrid 서비스) > All Clients(모든 클라이언트)로 이동합니다. Request Pending Approval(승인 보류 중 요청)은 "Total Pending Approval(1)(총 승인 보류 중(1))"으로 표시됩니다.
2. "Total Pending Approval(1)(총 승인 보류 중(1))"을 클릭하고 "Approve All(모두 승인)"을 선택합니다.



3. 표시되는 팝업에서 "Approve All(모두 승인)"을 클릭합니다.



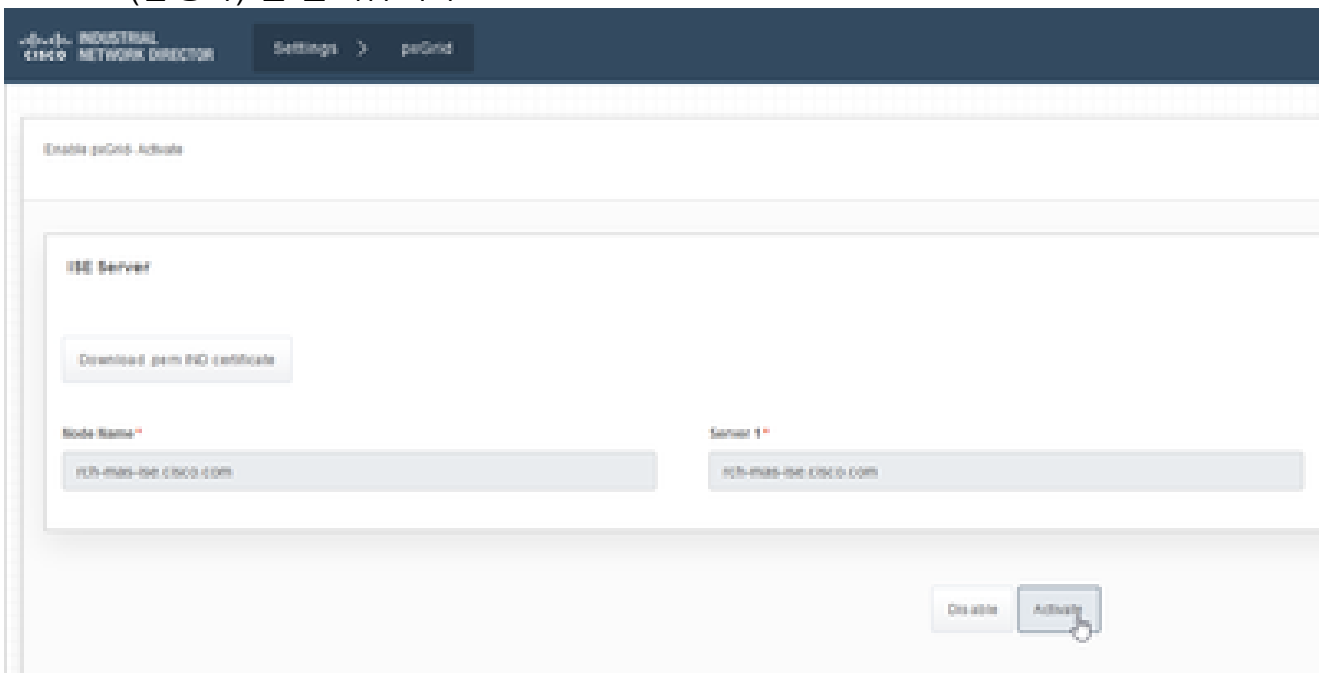
4. IND 서버는 여기에 표시된 대로 클라이언트로 표시됩니다.



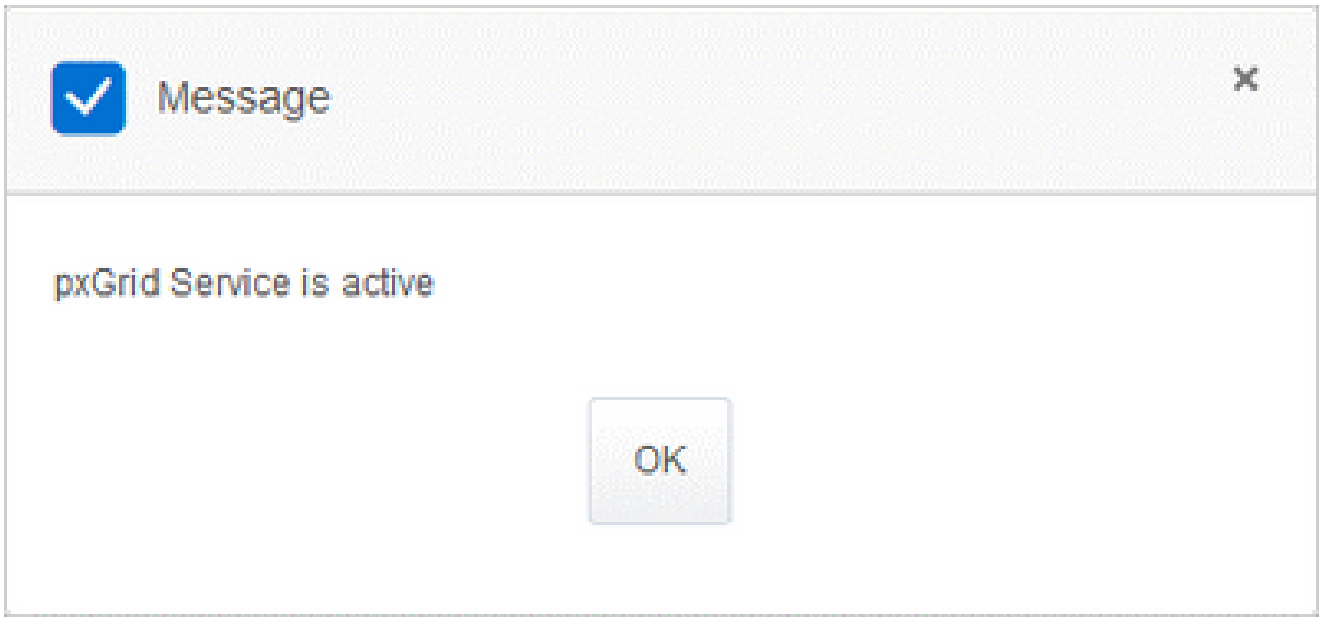
IND 서버에서 pxGrid 서비스 활성화

IND GUI 내에서

1. Settings(설정) > pxGrid로 이동합니다.
2. "Activate(활성화)"를 클릭합니다.



3. 확인 메시지가 화면에 표시됩니다.


Message
pxGrid Service is active
OK

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.