

ISE 2.0 인증서 프로비저닝 포털 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[제한 사항](#)

[구성](#)

[다음을 확인합니다.](#)

[인증서 서명 요청 없이 단일 인증서 생성](#)

[인증서 서명 요청으로 단일 인증서 생성](#)

[대량 인증서 생성](#)

[문제 해결](#)

소개

이 문서에서는 ISE(Identity Services Engine) 인증서 프로비저닝 포털의 구성 및 기능에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 이러한 주제에 대한 기본적인 지식을 얻을 것을 권장합니다.

- ISE
- 인증서 및 CA(Certificate Authority) 서버.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Identity Service Engine 2.0
- Windows 7 PC

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

인증서 프로비저닝 포털은 ISE 2.0에 도입된 새로운 기능으로, 엔드 디바이스는 서버에서 ID 인증서를 등록 및 다운로드하는 데 사용할 수 있습니다. 온보딩 플로우를 통과할 수 없는 디바이스에 인

증서를 발급합니다.

예를 들어 POS(Point-of-Sale) 터미널과 같은 디바이스는 BYOD(Bring Your Own Device) 흐름을 거칠 수 없으며 인증서를 수동으로 발급해야 합니다.

Certificate Provisioning Portal(인증서 프로비저닝 포털)에서는 권한이 있는 사용자 집합이 해당 디바이스에 대한 CSR(인증서 요청)을 업로드할 수 있습니다. 키 쌍을 생성한 다음 인증서를 다운로드합니다.

ISE에서 수정된 인증서 템플릿을 생성할 수 있으며 최종 사용자는 인증서를 다운로드할 적합한 인증서 템플릿을 선택할 수 있습니다. 이러한 인증서의 경우 ISE는 CA(Certificate Authority) 서버 역할을 하며 ISE 내부 CA에서 서명한 인증서를 가져올 수 있습니다.

ISE 2.0 인증서 프로비저닝 포털은 다음 형식으로 인증서 다운로드를 지원합니다.

- PKCS12 형식(인증서 체인 포함; 인증서 체인과 키 모두에 대해 하나의 파일)
- PKCS12 형식(인증서 및 키 모두에 대해 하나의 파일)
- PEM(Privacy Enhanced Electronic Mail) 형식의 인증서(체인 포함), PKCS8 PEM 형식의 키
- PEM 형식의 인증서, PKCS8 PEM 형식의 키:

제한 사항

현재 ISE는 인증서를 서명하기 위해 CSR에서 이러한 확장만 지원합니다.

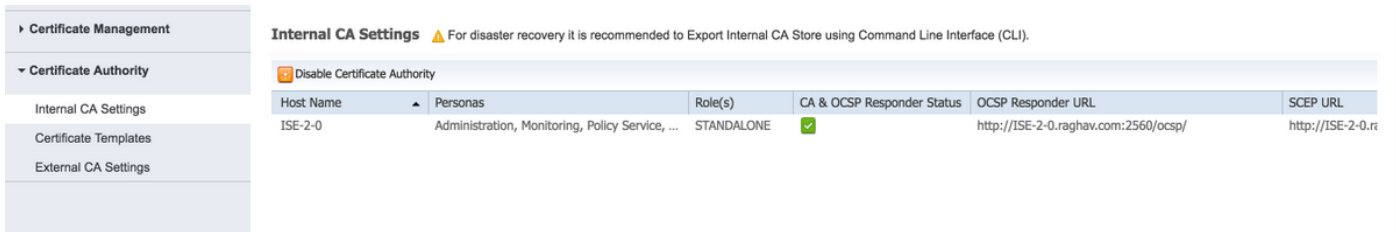
- 주체 DirectoryAttributes
- 주체 대체 이름
- 키 사용
- 주체 키 식별자
- 감사 ID
- 확장 키 사용
- CERT_TEMPLATE_OID(일반적으로 BYOD 플로우에 사용되는 템플릿을 지정하기 위해 사용자 지정 OID임)

참고: ISE 내부 CA는 BYOD와 같은 인증서를 사용하는 기능을 지원하도록 설계되었으므로 기능이 제한됩니다. ISE를 엔터프라이즈 CA로 사용하는 것은 Cisco에서 권장하지 않습니다.

구성

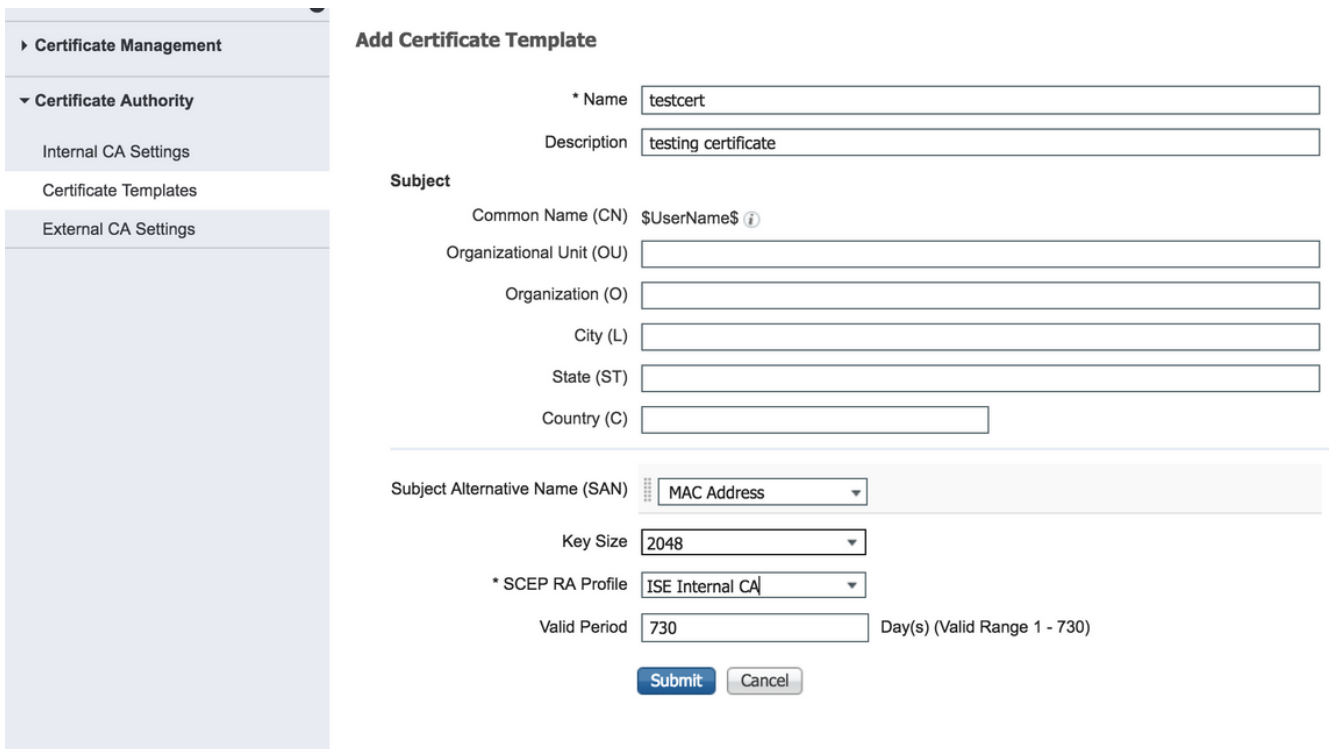
네트워크에서 인증서 프로비저닝 기능을 사용하려면 ISE 내부 CA 서비스를 활성화하고 인증서 프로비저닝 포털을 구성해야 합니다.

1단계. ISE GUI에서 **Administration(관리) > System(시스템) > Certificates(인증서) > Certificate Authority(인증 기관) > Internal CA(내부 CA)**로 이동하고 ISE 노드에서 내부 CA 설정을 활성화하려면 **Enable Certificate Authority(인증 기관 활성화)**를 클릭합니다.

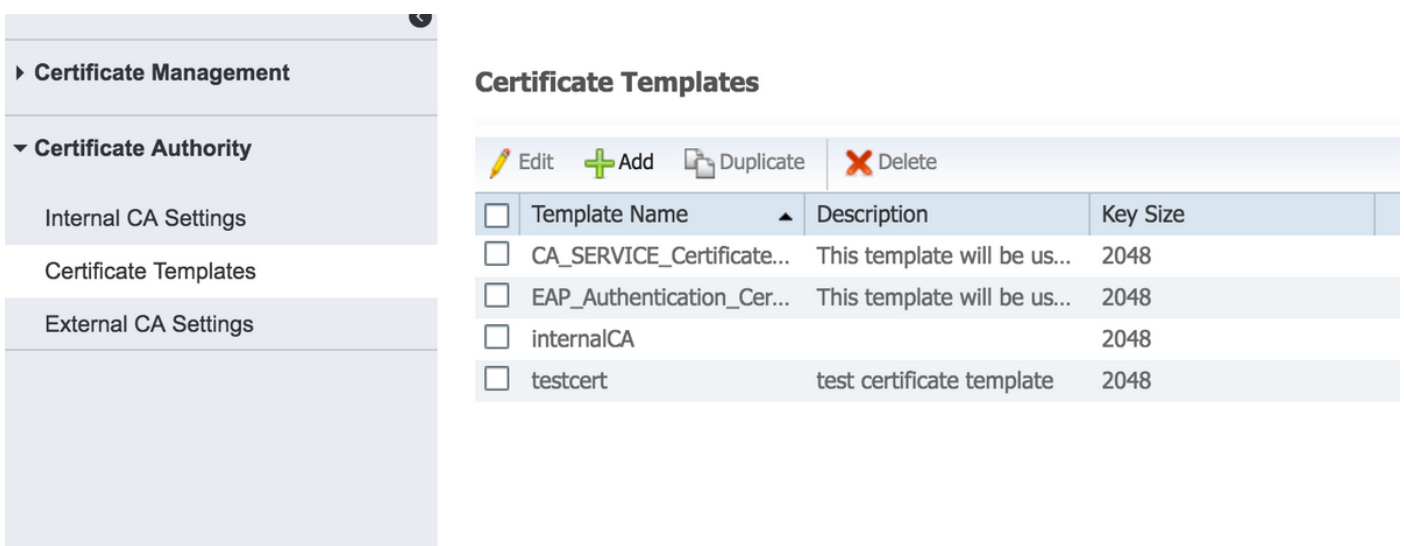


2단계. Administration(관리) > System(시스템) > Certificates(인증서) > Certificate Templates(인증서 템플릿) > Add(추가) 아래에 인증서 템플릿을 생성합니다.

요구 사항에 따라 세부 정보를 입력하고 이 이미지에 표시된 대로 Submit(제출)을 클릭합니다.



참고:이 이미지에 표시된 대로 Administration(관리) > System(시스템) > Certificates(인증서) > Certificate Templates(인증서 템플릿) 아래에 생성된 인증서 템플릿 목록을 볼 수 있습니다.



3단계. ISE 인증서 프로비저닝 포털을 구성하려면 이미지에 표시된 대로 Administration(관리) > Device Portal Management(디바이스 포털 관리) > Certificate Provisioning(인증서 프로비저닝) >

Create(생성)로 이동합니다.

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Identity Mapping

Blacklist BYOD Certificate Provisioning Client Provisioning Mobile Device Management My Devices Settings

Certificate Provisioning Portals

You can edit and customize the default Certificate Provisioning portal and create additional ones

Create Edit Duplicate Delete

Cert Portal

Certificate Provisioning Portal (default)
Default portal used by employees to request for a certificate manually

4단계. 새 인증서 포털에서 이미지에 표시된 대로 포털 설정을 확장합니다.

Portals Settings and Customization

Save Close

Portal Name: * Description: Portal test URL Language File

Cert Portal

Portal Behavior and Flow Settings
Use these settings to specify the guest experience for this portal.

Portal Page Customization
Use these settings to specify the guest experience for this portal.

Portal & Page Settings

- Portal Settings
- Login Page Settings
- Acceptable Use Policy (AUP) Page Settings
- Post-Login Banner Page Settings
- Change Password Settings
- Certificate Provisioning Portal Settings

Certificate Provisioning Flow (based on settings)

```
graph TD; LOGIN[LOGIN] --> AUP[AUP]; AUP --> PostLoginBanner[Post Login Banner]; PostLoginBanner --> [ ]
```

▼ **Portal Settings**

HTTPS port:* (8000 - 8999)

Allowed Interfaces:* Gigabit Ethernet 0
 Gigabit Ethernet 1
 Gigabit Ethernet 2
 Gigabit Ethernet 3
 Gigabit Ethernet 4
 Gigabit Ethernet 5

Certificate group tag: *
Configure certificates at:
Administration > System > Certificates > System Certificates

Authentication method: *
Configure authentication methods at:
Administration > Identity Management > Identity Source Sequences

Configure authorized groups
User account with Super admin privilege or ERS admin privilege will have access to the portal

Available	Chosen
<input type="text"/> ALL_ACCOUNTS (default) GROUP_ACCOUNTS (default) OWN_ACCOUNTS (default)	Employee

Fully qualified domain name (FQDN):

Idle timeout: 1-30 (minutes)

HTTPS 포트
 허용된 인터페이스
 인증서 그룹 태그
 인증 방법
 인증된 그룹
 FQDN(정규화된 도메인 이름)
 유효 시간 제한

HTTPS용 인증서 프로비저닝 포털에서 사용해야 하는 포트입니다.
 ISE가 이 포털을 수신 대기해야 하는 인터페이스.
 이 포털에 사용할 시스템 인증서를 나타내는 인증서 프로비저닝 포털에 사
 이 포털에 대한 로그인을 인증하는 ID 저장소 시퀀스를 선택합니다.기본적
 인증서 프로비저닝 포털에 액세스할 수 있는 사용자 집합은 특정 AD 그룹 및
 이 포털에 특정 FQDN을 지정할 수도 있습니다.http/https를 사용하여 FQDN
 이 값은 포털에 대한 유효 시간 제한을 정의합니다.

참고:ID 소스의 컨피그레이션은 Administration(관리) > Identity Management(ID 관리) > Identity Source Sequence(ID 소스 시퀀스) 아래에서 확인할 수 있습니다.

5단계. 로그인 페이지 설정을 구성합니다.

▼ **Login Page Settings**

Maximum failed login attempts before rate limiting: (1 - 999)

Time between login attempts when rate limiting: (1 - 999)

Include an AUP

Require acceptance

Require scrolling to end of AUP

6단계. AUP 페이지 설정을 구성합니다.

▼ Acceptable Use Policy (AUP) Page Settings

- Include an AUP page
- Require scrolling to end of AUP
 - On first login only
 - On every login
 - Every days (starting at first login)

7단계. 포스트 로그인 배너를 추가할 수도 있습니다.

8단계. Certificate Provisioning(인증서 프로비저닝) 포털 설정에서 허용되는 인증서 템플릿을 지정합니다.

▼ Change Password Settings

- Allow internal users to change their own passwords

▼ Certificate Provisioning Portal Settings

Certificate Templates: *

9단계. 페이지 맨 위로 스크롤한 후 **저장**을 클릭하여 변경 사항을 저장합니다.

또한 AUP 텍스트, 포스트 로그인 배너 텍스트 및 기타 메시지를 요구 사항에 따라 변경할 수 있는 **Portal page customization(포털 페이지 사용자 지정)** 탭으로 이동하여 포털을 더욱 사용자 지정할 수 있습니다.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

ISE가 인증서 프로비저닝을 위해 올바르게 구성된 경우 ISE 인증서 프로비저닝 포털에서 인증서를 요청/다운로드할 수 있습니다(다음 단계).

1단계. 브라우저를 열고 위에 구성된 인증서 프로비저닝 포털 FQDN 또는 인증서 프로비저닝 테스트 URL로 이동합니다. 다음 이미지와 같이 포털로 리디렉션됩니다.

Sign On
 Welcome to the Certificate Provisioning Portal. Sign on with the username and password supplied to you.

Username:

Password:

[Please read the terms and conditions.](#)

I agree to the terms and conditions

[Help](#)

2단계. 사용자 이름과 비밀번호로 로그인합니다.

3단계. 인증에 성공하면 AUP를 수락하고 인증서 프로비저닝 페이지로 이동합니다.

4단계. 인증서 프로비저닝 페이지는 다음 세 가지 방법으로 인증서를 다운로드하는 기능을 제공합니다.

- 단일 인증서(인증서 서명 요청 없음)
- 단일 인증서(인증서 서명 요청 포함)
- 대량 인증서

인증서 서명 요청 없이 단일 인증서 생성

- CSR 없이 단일 인증서를 생성하려면 Generate single certificate (without certificate signing request) 옵션을 선택합니다.
- CN(Common Name)을 입력합니다.

참고:지정된 CN은 요청자의 사용자 이름과 일치해야 합니다.요청자는 포털에 로그인하는 데 사용되는 사용자 이름을 참조합니다.관리자 사용자만 다른 CN에 대한 인증서를 생성할 수 있습니다.

- 인증서를 생성 중인 디바이스의 MAC 주소를 입력 합니다.
- 적절한 인증서 템플릿을 선택합니다.
- 인증서를 다운로드할 형식을 선택합니다.
- 인증서 비밀번호를 입력하고 **G**를 클릭합니다. **생성하십시오.**
- 단일 인증서가 생성되어 다운로드되었습니다.

Certificate Provisioning

I want to: *

Generate a single certificate (without a certificat..

Common Name (CN): *

test1

MAC Address: *

11:35:65:AF:EC:12

Choose Certificate Template: *

EAP_Authentication_Certificate_Template

Description:

test certificate

Certificate Download Format: *

PKCS12 format, including certificate chain (O... i

Certificate Password: *

Confirm Password: *

*****|

Generate

Reset

인증서 서명 요청으로 단일 인증서 생성

- CSR 없이 단일 인증서를 생성하려면 Generate single certificate (with certificate signing request) 옵션을 선택합니다.
- Certificate Signing Request Details(인증서 서명 요청 세부사항)의 메모장 파일에서 CSR 콘텐츠를 복사하여 붙여넣습니다.
- 인증서를 생성 중인 디바이스의 MAC 주소를 입력 합니다.
- 적절한 인증서 템플릿을 선택합니다.
- 인증서를 다운로드할 형식을 선택합니다.
- 인증서 비밀번호를 입력하고 Generate(생성)를 클릭합니다.
- 단일 인증서가 생성되어 다운로드됩니다.

Certificate Provisioning

I want to: *

Generate a single certificate (with certificate sig...

Certificate Signing Request Details: *

```
-----BEGIN CERTIFICATE REQUEST-----
MIICuCCAAIACAQAwEDEMwGA1UEAxMFdGVzdDEwggEMA0G
CSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQCFPaA5XBkMmrfUgySpKa465ecULygnjHG
NC7bPqz4+5
8vK723r23ghympvBNPw31K6qzUCmDYLOcTwp+ymbWY3rfYxQ
nde8NofbTL
CrIhcnbmn0+SD7UozaXYb1DmugD8YL9Ht0vV//WBKie6B8jZKl
WwoqAKVJ
yqJC55eBZqYBRB2xABvhlTcn1/SyHhNnIRHw6L5ABqjSToasXW
kyEIQT,8K
8DmkucOm3h46NuhnrWgRfO9H6uGrY8Vz7FvqSDsX4-na0f6P5OK
6y4YumKNzSJE
qKowamxNaGLdHcNkKa8nmfJ0wTEMMmwn7Wbn5AgMBAAAGZ
TBjBkqkqkG9wOB
CQ4xVBUUAsGA1UdDwQEAwIF4DAAdBgNVHQ4EFgQUZjmi7f5r8w
QyYb/vWYXKCY
BwkwEwYDYR0BAwwCgYIKwYBBQUHAWAwEwEQYJYIZIAWY4QqEB
BAQDAgZAMA0GCSeG
Sib3DQEBQwUAA4IBAQCeZSHBMu71Pv?H9dQHTxY5v5WCyQ7
qNzOPUymVA3h+Z
Q1t72xulTIGeEaDaYA4w4YyXDqGmEomGzLKNxH2Bdh0x5HLpXWx
7o6wR8h2k86ys
1VqZoa1mF7ALKkZWNYU9pAUeLdn9P/W0u3mfQICUPWPh8OzB
KA90V4uzV8G#f
tKDCq63/NmZ9DH0dH20y1O86dWFH18ez6k8Dtb8cdJbyXN8fmS
n2foM6CDMH
J0ypRA7w5KqJGB0HLWBAZ3ckI7ymB6QMOC5OqCDwnUSEWZ6
54/YAQ9KqHAx0+
xp2BY1uUYSEy5Hobb5RWAQrhZLsytkL6AeRiBqzo
-----END CERTIFICATE REQUEST-----
```

```
qNzOPUymVA3h+Z
Q1t72xulTIGeEaDaYA4w4YyXDqGmEomGzLKNxH2Bdh0x5HLpXWx
7o6wR8h2k86ys
1VqZoa1mF7ALKkZWNYU9pAUeLdn9P/W0u3mfQICUPWPh8OzB
KA90V4uzV8G#f
tKDCq63/NmZ9DH0dH20y1O86dWFH18ez6k8Dtb8cdJbyXN8fmS
n2foM6CDMH
J0ypRA7w5KqJGB0HLWBAZ3ckI7ymB6QMOC5OqCDwnUSEWZ6
54/YAQ9KqHAx0+
xp2BY1uUYSEy5Hobb5RWAQrhZLsytkL6AeRiBqzo
-----END CERTIFICATE REQUEST-----
```

MAC Address:

11:AF:35:23:12:EC

Choose Certificate Template: *

EAP_Authentication_Certificate_Template

Description:

test certificate

Certificate Download Format: *

PKCS12 format, including certificate chain (O...

Certificate Password: *

Confirm Password: *

Generate

Reset

CN 및 MAC 주소 필드가 포함된 CSV 파일을 업로드하는 경우 여러 MAC 주소에 대한 대량 인증서를 생성할 수 있습니다.

참고:지정된 CN은 요청자의 사용자 이름과 일치해야 합니다.요청자는 포털에 로그인하는 데 사용되는 사용자 이름을 참조합니다.관리자 사용자만 다른 CN에 대한 인증서를 생성할 수 있습니다.

- CSR 없이 단일 인증서를 생성하려면 Generate single certificate (with certificate signing request) 옵션을 선택합니다.
- 대량 요청을 위해 csv 파일을 업로드합니다.
- 적절한 인증서 템플릿을 선택합니다.
- 인증서를 다운로드할 형식을 선택합니다.
- 인증서 비밀번호를 입력하고 Generate(생성)를 클릭합니다.
- 대량 인증서 zip 파일이 생성되어 다운로드됩니다.



Certificate Provisioning

I want to: *

Generate bulk certificates

Upload CSV File: *

Choose File maclist.csv

If you don't have the CSV template, [download here](#)

Choose Certificate Template: *

EAP_Authentication_Certificate_Template

Description:

test bulk certificate

Certificate Download Format: *

PKCS12 format, including certificate chain (O... ⓘ

Certificate Password: *

.....

Confirm Password: *

.....|

Generate Reset

[Help](#)

문제 해결

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