

# ISE에서 인증서 가져오기 및 내보내기

## 목차

[소개](#)

[배경 정보](#)

[ISE에서 인증서 내보내기](#)

[ISE에서 인증서 가져오기](#)

## 소개

이 문서에서는 Cisco ISE(Identity Service Engine)에서 인증서를 가져오고 내보내는 방법에 대해 설명합니다.

## 배경 정보

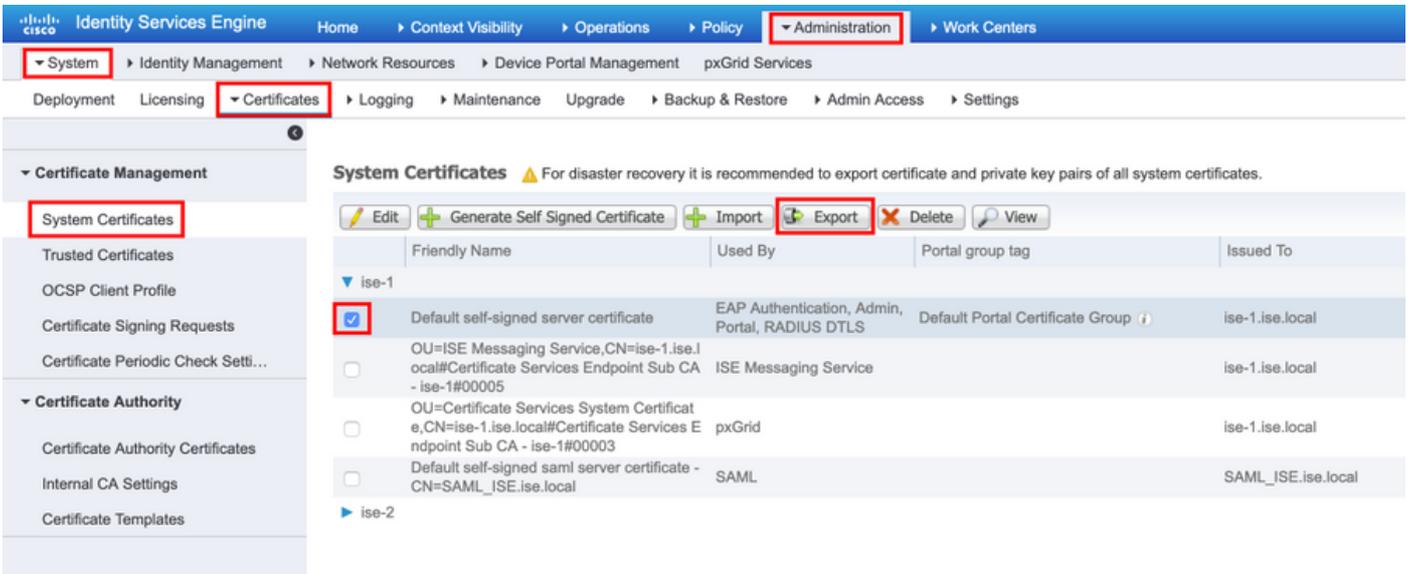
ISE는 다양한 용도(웹 UI, 웹 포털, EAP, pxgrid)에 인증서를 사용합니다. ISE에 있는 인증서는 다음 역할 중 하나를 가질 수 있습니다.

- 관리자:관리 포털의 노드 간 통신 및 인증
- EAP:EAP 인증을 위한 것입니다.
- RADIUS DTLS:RADIUS DTLS 서버 인증의 경우
- 포털:모든 Cisco ISE 최종 사용자 포털 간에 통신하기 위해.
- pxGrid:pxGrid 컨트롤러 간에 통신하기 위한 것입니다.

ISE 노드에 설치된 인증서의 백업을 수행하는 것이 중요합니다.컨피그레이션 백업을 수행할 때 관리 노드의 컨피그레이션 데이터 및 인증서 백업이 수행됩니다.그러나 다른 노드의 경우 인증서 백업은 개별적으로 수행됩니다.

## ISE에서 인증서 내보내기

Administration(관리) > System(시스템) > Certificates(인증서) > Certificate Management(인증서 관리) > System certificate(시스템 인증서)로 이동합니다.노드를 확장하고 인증서를 선택한 다음 이미지에 표시된 대로 **Export**를 클릭합니다.



이 이미지에 표시된 대로 Export Certificate and Private Key(인증서 및 개인 키 내보내기)를 선택합니다. 최소 8자의 영숫자 암호를 입력합니다. 인증서를 복원하려면 이 암호가 필요합니다.



팁:비밀번호를 잊지 마십시오.

## ISE에서 인증서 가져오기

ISE에서 인증서를 가져오는 두 단계가 있습니다.

1단계. 인증서가 자체 서명 또는 서드파티 서명 인증서인지 확인합니다.

- 인증서가 자체 서명된 경우 신뢰할 수 있는 인증서 아래 인증서의 공개 키를 가져옵니다.
- 인증서가 일부 서드파티 인증 기관에서 서명된 경우 루트 및 인증서의 다른 모든 중간 인증서를 가져옵니다.

Administration(관리) > System(시스템) > Certificates(인증서) > Certificate Management(인증서 관리) > Trusted Certificate(신뢰할 수 있는 인증서)로 이동하고 이 이미지에 표시된 대로 Import(가져오기)를 클릭합니다.

Identity Services Engine Administration

System > Certificates > Trusted Certificates

Trusted Certificates

Edit
  Import
  Export
  Delete
  View

<input type="checkbox"/> Friendly Name	Status	Trusted For	Se
<input type="checkbox"/> Baltimore CyberTrust Root	✓ Enabled	Cisco Services	02
<input type="checkbox"/> Cisco ECC Root CA 2099	✓ Enabled	Cisco Services	03
<input type="checkbox"/> Cisco Licensing Root CA	✓ Enabled	Cisco Services	01
<input type="checkbox"/> Cisco Manufacturing CA SHA2	✓ Enabled	Infrastructure Endpoints	02
<input type="checkbox"/> Cisco Root CA 2048	⊖ Disabled	Endpoints Infrastructure	5F
<input type="checkbox"/> Cisco Root CA 2099	✓ Enabled	Cisco Services	01
<input type="checkbox"/> Cisco Root CA M1	✓ Enabled	Cisco Services	2F

Identity Services Engine Administration

System > Certificates > Import a new Certificate into the Certificate Store

\* Certificate File  Defaultselfsignedservercert.pem

Friendly Name

Trusted For: ⓘ

Trust for authentication within ISE  
 Trust for client authentication and Syslog  
 Trust for certificate based admin authentication  
 Trust for authentication of Cisco Services  
 Validate Certificate Extensions

Description

2단계. 실제 인증서를 가져옵니다.

1. 이 이미지에 표시된 대로 Administration(관리) > System(시스템) > Certificates(인증서) > Certificate Management(인증서 관리)로 이동하여 Import(가져오기)를 클릭합니다.관리자 역할이 인증서에 할당된 경우 노드의 서비스가 다시 시작됩니다.

The screenshot shows the Cisco Identity Services Engine Administration interface. The navigation menu includes 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', and 'pxGrid Services'. Under 'System', 'Certificates' is selected. The left sidebar shows 'Certificate Management' with 'System Certificates' highlighted. The main content area is titled 'System Certificates' and includes a warning: 'For disaster recovery it is recommended to export certificate and private key pairs of all system certificates'. Below this are buttons for 'Edit', 'Generate Self Signed Certificate', 'Import', 'Export', 'Delete', and 'View'. The 'Import' button is highlighted with a red box. A table lists certificates for the 'ise-1' node:

	Friendly Name	Used By	Portal group tag
<input type="checkbox"/>	Default self-signed server certificate	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group ⓘ
<input type="checkbox"/>	OU=ISE Messaging Service,CN=ise-1.ise.local#Certificate Services Endpoint Sub CA - ise-1#00005	ISE Messaging Service	
<input type="checkbox"/>	OU=Certificate Services System Certificate,CN=ise-1.ise.local#Certificate Services Endpoint Sub CA - ise-1#00003	pxGrid	
<input type="checkbox"/>	Default self-signed saml server certificate - CN=SAML_ISE.ise.local	SAML	

2. 인증서를 가져올 노드를 선택합니다.

3. 공개 및 개인 키를 찾습니다.

4. 인증서의 개인 키에 대한 비밀번호를 입력하고 원하는 역할을 선택합니다.

5. 이제 이 이미지에 표시된 대로 Submit(제출)을 클릭합니다.

- ▼ Certificate Management
  - System Certificates
  - Trusted Certificates
  - OCSP Client Profile
  - Certificate Signing Requests
  - Certificate Periodic Check Setti...
- ▶ Certificate Authority

### Import Server Certificate

\* Select Node

\* Certificate File  Defaultselfsignedservercert.pem

\* Private Key File  Defaultselfsignedservercert.pvk

Password

Friendly Name  ⓘ

Allow Wildcard Certificates  ⓘ

Validate Certificate Extensions  ⓘ

#### Usage

- Admin: Use certificate to authenticate the ISE Admin Portal
- EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
- RADIUS DTLS: Use certificate for the RADSec server
- pxGrid: Use certificate for the pxGrid Controller
- SAML: Use certificate for SAML Signing
- Portal: Use for portal

Select Required Role