ISE에서 인증서 가져오기 및 내보내기

목차

<u>소개</u> <u>배경 정보</u> <u>ISE에서 인증서 내보내기</u> <u>ISE에서 인증서 가져오기</u>

소개

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

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 관 리 노드의 컨피그레이션 데이터 및 인증서 백업이 수행됩니다.그러나 다른 노드의 경우 인증서 백 업은 개별적으로 수행됩니다.

ISE에서 인증서 내보내기

Administration(관리) > System(시스템) > Certificates(인증서) > Certificate Management(인증서 관 리) > System certificate(시스템 인증서)로 이동합니다.노드를 확장하고 인증서를 선택한 다음 이미 지에 표시된 대로 Export를 클릭합니다.

| dentity Services Engine | łome → | Context Visibility | Policy Administration | Work Centers | | |
|--|---------|--|---|------------------------------------|--------------------|--|
| System Identity Management Network Resources Device Portal Management pxGrid Services | | | | | | |
| Deployment Licensing ▼Certificates → Logging → Maintenance Upgrade → Backup & Restore → Admin Access → Settings | | | | | | |
| 0 | | | | | | |
| - Certificate Management System Certificates 🛕 For disaster recovery it is recommended to export certificate and private key pairs of all system certificates. | | | | | | |
| System Certificates | 🥖 Edit | 🕂 Generate Self Signed Certificate | Import 🕃 Export 🗙 | Delete View | | |
| Trusted Certificates | | Friendly Name | Used By | Portal group tag | Issued To | |
| OCSP Client Profile | ▼ ise-1 | | | | | |
| Certificate Signing Requests | | Default self-signed server certificate | EAP Authentication, Admin, Portal, RADIUS DTLS | Default Portal Certificate Group (| ise-1.ise.local | |
| Certificate Periodic Check Setti | | OU=ISE Messaging Service, CN=ise-1.ise.1 ocal#Certificate Services Endpoint Sub CA - ise-1#00005 | ISE Messaging Service | | ise-1.ise.local | |
| Certificate Authority Certificate Authority | 0 | OU=Certificate Services System Certificat e,CN=ise-1.ise.local#Certificate Services E advoint Sub CA ise_1#00003 | pxGrid | | ise-1.ise.local | |
| Internal CA Settings | | Default self-signed saml server certificate - CN=SAML_ISE.ise.local | SAML | | SAML_ISE.ise.local | |
| Certificate Templates | ise-2 | | | | | |

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

| Export Certificate'Default self-signed server certificate' | × |
|---|--------|
| Export Certificate Only | |
| Export Certificate and Private Key | |
| *Private Key Password | |
| *Confirm Password | |
| Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private | e key. |
| Export | ancel |

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 관 리) > Trusted Certificate(신뢰할 수 있는 인증서)로 이동하고 이 이미지에 표시된 대로 Import(가져 오기)를 클릭합니다.

| System > Identity Management > Network Resources > Device Portal Management pxGrid Services Deployment Licensing Certificates System Certificate Signing Requests Certificate Periodic Check Setti Certificate Authority Certificate Authority Certificate Management System Certificates System Cerificates System Certificates System Certificates | dentity Services Engine | Home 	► Context Visibility 	► | Operations ► Policy | - Administration | |
|---|---|---|---|---|-----------------------------|
| Deployment Licensing • Certificates • Admin Access • Settings • Certificate Management • System Certificates • Edit • Import • Export • Delete • View • Status Trusted Certificates • OCSP Client Profile Certificate Signing Requests Certificate Periodic Check Setti • Certificate Authority • Certificate Authority • Certificate Authority • Certificates • Certificate Management • Network Resources • Device Portal Management • Network Centers • System • Certificates • Logging • Maintenance • Device Portal Management • Certificate Store | ✓ System → Identity Management | Network Resources Device Porta | al Management pxGrid S | ervices | |
| Certificate Management System Certificates Cestificate Management Friendly Name Status Trusted Certificates Certificate Signing Requests Certificate Periodic Check Setti Certificate Authority Clean Red CA M1 Certificate Management Network Resources Device Portal Management System Certificates Certificate Management Network Resources Device Portal Management Network Resources System Certificate Management Network Resources Device Portal Management Network Resources Device Portal Management Network Resources Device Portal Management Network Resources System Certificate Store Certificate Management Network Resources Certificate File Browse Defaultaelfsignedservercerti.pem Friendly Name SE_Self_Signed Trust for authentication | Deployment Licensing - Certificate | es ▶ Logging ▶ Maintenance U | pgrade | tore Admin Acc | cess > Settings |
| Certificate Management System Certificates OCSP Client Profile Certificate Signing Requests Certificate Periodic Check Setti Certificate Authority Trusted Certificates Cisco Root CA 2099 Enabled Cisco Services Cisco Root CA 2099 Services Policy Administration Vork Centers Vork Centers System Identify Management Network Resources Device Portal Management pxCirificate Management System Certificate Signing Requests Certificate Periodic Check Setti Certificate Periodic Check Setti Certificate Periodic Check Setti Certificate Periodic Check Setti Certificate Periodic Check Setti< | 0 | | | | |
| System Certificates <pre> Firendly Name</pre> | ✓ Certificate Management | Trusted Certificates | | | |
| System Certificates Indext Visibility Certificate Signing Requests Certificate Signing Requests Certificate Signing Requests Certificate Periodic Check Setti Cisco ECC Root CA 2099 Enabled Cisco Services Priendly Name Status Trusted Certificate Signing Requests Certificate Periodic Check Setti Cisco ECC Root CA 2099 Enabled Cisco Services Cisco Root CA 2048 Disabled Infrastructure Endpoints Endpoints Cisco Root CA 2099 Enabled Cisco Services Enabled Cisco Services Cisco Root CA 2048 Disabled Infrastructure Endpoints Infrastructure Endpoints Cisco Root CA 2099 Enabled Cisco Services Enabled Cisco Services Cisco Root CA 2099 Enabled Cisco Services Enabled Cisco Services Cisco Root CA 2099 Enabled Cisco Services Enabled Cisco Services Vertificate Network Resources Device Portal Management vGrificates vGrificates vGrificate Signing Requests Certificate Signing Requests Certificate Signing Requests Certificate Rise Signing Requests Trust for certificate based admin authenticat | Duckers Derl'Eacher | | Delete Ottour | | |
| Trusted Certificates Friendly Name Status Trusted For Cost Client Profile Certificate Signing Requests Certificate Periodic Check Setti Certificate Periodic Check Setti Certificate Authority Cisco Root CA 2099 Enabled Cisco Services Cisco Carbon CA 2048 Disabled Trusted Carso Services Cisco Root CA 2099 Enabled Cisco Services Cisco Root CA 2048 Disabled Infrastructure Enabled Cisco Services Cisco Root CA 2099 Enabled Cisco Services Cisco Root CA 2048 Disabled Infrastructure Cisco Root CA 2099 Enabled Cisco Services Cisco Root CA 2099 Enabled Cisco Services Cisco Root CA 2099 Enabled Cisco Services Cisco Root CA 2099 Cisco Root CA 2099 Enabled Cisco Services Cisco Root CA 2099 Enabled Cisco Services Cisco Root CA 2099 Enabled Cisco Services Cisco Root CA 2099 Cisco Root CA 2099 Enabled Cisco Services Police Profilos Friendly Name | System Certificates | / Edit - Import Export | Delete View | | |
| OCSP Client Profile Gettificate Signing Requests Certificate Signing Requests Gisco ECC Root CA 2099 Enabled Gisco Services Certificate Periodic Check Setti Cisco Licensing Root CA Enabled Gisco Services Cisco Licensing Root CA 2099 Enabled Cisco Services Cisco Root CA 2048 Disabled Infrastructure Endpoints Cisco Root CA 2099 Enabled Cisco Services Cisco Root CA 2011 Prabled Cisco Services Cisco Root CA 2099 Enabled Cisco Services Cisco Root CA 4011 Enabled Cisco Services * System > Identity Management > Network Resources > Device Portal Management > Xorid Services Deployment Licensing * Certificates > Logging > Maintenance Upgrade > Backup & Restore > Admin Access > Settings * Certificate Signing Requests Certificate File Browse Defaultselfisignedservererenti.pem <t< td=""><th>Trusted Certificates</th><td>Friendly Name Raltimere OtherTruct Beet</td><td>▲ Si</td><td>tatus Tr</td><td>usted For Se</td></t<> | Trusted Certificates | Friendly Name Raltimere OtherTruct Beet | ▲ Si | tatus Tr | usted For Se |
| Certificate Signing Requests Certificate Signing Requests Cisco Licensing Root CA Enabled Cisco Services Certificate Periodic Check Setti Cisco Manufacturing CA SHA2 Enabled Infrastructure Endpoints Cisco Root CA 2048 Disabled Infrastructure Endpoints Cisco Root CA 2048 Disabled Cisco Services Cisco Root CA 2099 Enabled Cisco Services Cisco Root CA 2099 Enabled Cisco Services Cisco Root CA 2099 Enabled Cisco Services Cisco Root CA M1 Repoints Infrastructure System > Identity Management > Network Resources > Device Portal Management > Work Centers System Certificates > Logging > Maintenance Upgrade > Backup & Restore > Admin Access > Settings Trusted Certificates > Logging > Maintenance Upgrade > Backup & Restore > Admin Access > Settings Certificate Signing Requests Certificate File Browse Defaultselfsignedservercerti.pem Certificate Authority Certificate Periodic Check Setti Crust for authentication within ISE Trust for centificate based admin authentic | OCSP Client Profile | | | Enabled Ci | sco Services 02 |
| Certificate Periodic Check Setti Cisco Manufacturing CA SHA2 Enabled Infrastructure > Certificate Authority Cisco Manufacturing CA SHA2 Enabled Infrastructure Cisco Root CA 2048 Disabled Infrastructure Endbled Endbled Cisco Root CA 2048 Disabled Infrastructure Infrastructure Cisco Root CA 2099 Enabled Esco Services Cisco Root CA M1 Fnabled Occo Services * System > Identity Management > Network Resources > Device Portal Management > Work Centers * System > Identity Management > Network Resources > Device Portal Management > Work Centers * System > Identity Management > Network Resources > Device Portal Management > Work Centers * System Certificates > Logging > Maintenance Upgrade > Backup & Restore > Admin Access > Settings Trusted Certificates Certificate File Browse Defaultselfsignedservercerti.pem System Certificate Signing Requests Certificate File Browse Defaultselfsigned admin authentication and Syslog Certificate Authority | Certificate Signing Requests | | | Enabled Cit | sco Services 01 |
| Certificate Authority Cisco Root CA 2048 Disabled Endpoints <p< td=""><th>Certificate Periodic Check Setti</th><td>Cisco Manufacturing CA SHA2</td><td></td><td>Enabled In</td><td>frastructure 02</td></p<> | Certificate Periodic Check Setti | Cisco Manufacturing CA SHA2 | | Enabled In | frastructure 02 |
| □ Cisco Root CA 2099 ☑ Enabled Cisco Services □ Cisco Root CA M1 ☑ Fnabled Cisco Services □ Cisco Root CA M1 ☑ Fnabled Cisco Services □ Cisco Root CA M1 ☑ Fnabled Cisco Services □ Cisco Root CA M1 ☑ Fnabled Cisco Services □ Cisco Root CA M1 ☑ Fnabled Cisco Services □ Cisco Root CA M1 ☑ Fnabled Cisco Services □ Cisco Root CA M1 ☑ Fnabled Cisco Services □ Cisco Root CA M1 ☑ Fnabled Cisco Services □ Cisco Root CA M1 ☑ Fnabled Cisco Services □ Cisco Root CA M1 ☑ Policy ▼Administration > Work Centers □ System > Identity Management > Network Resources > Device Portal Management pxGrid Services □ Deployment Licensing ● Certificates > Logging > Maintenance Upgrade > Backup & Restore > Admin Access > Settings □ Trust Certificates > Logging > Maintenance Upgrade > Backup & Restore > Admin Access > Settings □ Cisco Services ☑ Import a new Certificate into the Certificate Store <td< td=""><th>Certificate Authority</th><td>Cisco Root CA 2048</td><td>e</td><td>Disabled Er</td><td>ndpoints frastructure 5F</td></td<> | Certificate Authority | Cisco Root CA 2048 | e | Disabled Er | ndpoints frastructure 5F |
| Cisco Root CA M1 Enabled Cisco Services Image: Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers System Identity Management Network Resources Device Portal Management pxGrid Services Deployment Licensing Certificates Logging Maintenance Upgrade Browse Defaultselfsignedservercerti.pem Certificates Logging Requests Certificate Periodic Check Setti Certificate Authority Certificate Authority Trust for authentication and Systog Trust for authentication of Cisco Services | | Cisco Root CA 2099 | | Enabled Cit | sco Services 01 |
| Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers • System Identity Management Network Resources Device Portal Management pxGrid Services Deployment Licensing • Certificates > Logging Maintenance Upgrade > Backup & Restore > Admin Access > Settings • Certificate Management System Certificates > Logging > Maintenance Upgrade > Backup & Restore > Admin Access > Settings • Certificate Management System Certificates > Certificate into the Certificate Store • Certificate File Browse Defaultselfsignedservercerti.pem System Certificates Trusted Certificates Friendly Name ISE_Self_Signed Trusted For: ① Certificate Periodic Check Setti • Certificate Authority Trust for client authentication and Syslog _ Trust for certificate based admin authentication • Certificate Authority | | Cisco Root CA M1 | | Enabled Cir | sco Services 2E |
| Validate Certificate Extensions Description | System Identity Management Deployment Licensing Certificates Certificate Management System Certificates Trusted Certificates OCSP Client Profile Certificate Signing Requests Certificate Periodic Check Setti Certificate Authority | Network Resources | tanagement pxGrid Servi rade → Backup & Restore the Certificate Store te File Browse Defa Name ISE_Self_Signed Trusted For: () Trust for authent () Trust for authent () Trust for authent () Validate Certifica ription () | ces Admin Access aultselfsignedservero ication within ISE ient authentication a st for certificate base ication of Cisco Serv te Extensions | : • Settings |

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.

| dentity Services Engine H | ome | Context Visibility Operations | Policy - Administration | on Vork Centers | |
|---|---------|--|--|---|--|
| System Identity Management Network Resources Device Portal Management pxGrid Services | | | | | |
| Deployment Licensing - Certificates | ▸ Loggi | ng Maintenance Upgrade Bac | kup & Restore + Admin | Access > Settings | |
| G | | | | | |
| ✓ Certificate Management | System | Certificates 🛕 For disaster recovery | it is recommended to export | certificate and private key pairs of all syster | |
| System Certificates | 🥖 Edit | Generate Self Signed Certificate | Import Export | 🗙 Delete 🔎 View | |
| Trusted Certificates | | Friendly Name | Used By | Portal group tag | |
| OCSP Client Profile | ▼ ise-1 | | | | |
| Certificate Signing Requests | | Default self-signed server certificate | EAP Authentication, Admin, Portal, RADIUS DTLS | Default Portal Certificate Group (i) | |
| Certificate Periodic Check Setti Certificate Authority | | OU=ISE Messaging Service, CN=ise-1.is e.local#Certificate Services Endpoint Su b CA - ise-1#00005 | ISE Messaging Service | | |
| | | OU=Certificate Services System Certific ate,CN=ise-1.ise.local#Certificate Servic es Endpoint Sub CA - ise-1#00003 | pxGrid | | |
| | | Default self-signed saml server certificat e - CN=SAML_ISE.ise.local | SAML | | |
| | ► ise-2 | | | | |

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.

| dentity Services Engine | Home | Operations Policy | - Administration | Work Centers |
|--------------------------------------|------------------------------------|-------------------------|-------------------------|--------------------------------------|
| ✓ System → Identity Management | Network Resources Device Ports | al Management pxGrid Se | ervices | |
| Deployment Licensing - Certification | tes ►Logging ► Maintenance U | Jpgrade Backup & Rest | ore Admin Acces | ss > Settings |
| 0 | | | | |
| ✓ Certificate Management | Import Server Certificate | | | |
| System Certificates | * Select Node | ise-1 | - | |
| Trusted Certificates | | | | |
| OCSP Client Profile | * Certificate File | Browse Defaultsel | fsignedservercerti.pen | 1 |
| Certificate Signing Requests | * Private Key File | Browse Defaultsel | fsignedservercerti.pvk | |
| Certificate Periodic Check Setti | | | 5 | |
| Certificate Authority | Password | ••••• | | |
| | Friendly Name | ISE Self Signed | | (i) |
| | | | | |
| | Allow Wildcard Certificates | | | |
| | Validate Certificate Extensions | | | |
| | | | | |
| | Usage | | | |
| | | | | |
| | | Admin: Use certificate | to authenticate the IS | E Admin Portal |
| | | □ EAP Authentication: U | se certificate for EAP | protocols that use SSL/TLS tunneling |
| | Select Required | RADIUS DTLS: Use ca | ertificate for the RADS | Sec server |
| | Polo | pxGrid: Use certificate | for the pxGrid Contro | ller |
| | Rule | SAML: Use certificate | for SAML Signing | |
| | | Portal: Use for portal | | |
| | | | | |
| | | Submit Cancel | | |
| | | | | |