

Importieren und Exportieren von Zertifikaten in ISE

Inhalt

[Einführung](#)

[Hintergrundinformationen](#)

[Zertifikat in ISE exportieren](#)

[Zertifikat in ISE importieren](#)

Einführung

In diesem Dokument wird beschrieben, wie Zertifikate in die Cisco Identity Service Engine (ISE) importiert und exportiert werden.

Hintergrundinformationen

Die ISE verwendet Zertifikate für verschiedene Zwecke (Webbenutzeroberfläche, Web-Portale, EAP, pxgrid). Das auf der ISE vorhandene Zertifikat kann eine der folgenden Rollen haben:

- Administrator: Für die Kommunikation zwischen Knoten und Authentifizierung des Admin-Portals.
- EAP: Für die EAP-Authentifizierung.
- RADIUS-DTLS: Für die RADIUS DTLS-Serverauthentifizierung.
- Portal: Um zwischen allen Cisco ISE-Endbenutzerportalen zu kommunizieren.
- PxGrid: Um zwischen dem pxGrid-Controller zu kommunizieren.

Es ist wichtig, eine Sicherung der Zertifikate durchzuführen, die auf ISE-Knoten installiert sind. Wenn Sie die Konfigurationssicherung durchführen, werden die Konfigurationsdaten und das Zertifikat des Admin-Knotens gesichert. Bei anderen Knoten wird die Sicherung von Zertifikaten jedoch einzeln durchgeführt.

Zertifikat in ISE exportieren

Navigieren Sie zu **Administration > System > Certificates > Certificate Management > System certificate**. Erweitern Sie den Knoten, wählen Sie das Zertifikat aus, und klicken Sie auf **Exportieren**, wie im Bild gezeigt:

Identity Services Engine Administration > System > Certificates > System Certificates

System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

Buttons: Edit, Generate Self Signed Certificate, Import, Export, Delete, View

	Friendly Name	Used By	Portal group tag	Issued To
▼	ise-1			
<input checked="" type="checkbox"/>	Default self-signed server certificate	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group	ise-1.ise.local
<input type="checkbox"/>	OU=ISE Messaging Service,CN=ise-1.ise.local#Certificate Services Endpoint Sub CA - ise-1#00005	ISE Messaging Service		ise-1.ise.local
<input type="checkbox"/>	OU=Certificate Services System Certificate,CN=ise-1.ise.local#Certificate Services Endpoint Sub CA - ise-1#00003	pxGrid		ise-1.ise.local
<input type="checkbox"/>	Default self-signed saml server certificate - CN=SAML_ISE.ise.local	SAML		SAML_ISE.ise.local
▶	ise-2			

Wählen Sie, wie in diesem Bild gezeigt, das **Zertifikat exportieren und den privaten Schlüssel aus**. Geben Sie ein alphanumerisches Kennwort mit mindestens 8 Zeichen Länge ein. Dieses Kennwort ist erforderlich, um das Zertifikat wiederherzustellen.

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 key.

Tipp: Vergessen Sie nicht das Kennwort.

Zertifikat in ISE importieren

Es gibt zwei Schritte, um das Zertifikat auf der ISE zu importieren.

Schritt 1: Finden Sie heraus, ob es sich bei dem Zertifikat um ein selbstsigniertes oder ein von einem Drittanbieter unterzeichnetes Zertifikat handelt.

- Wenn das Zertifikat selbst signiert ist, importieren Sie den öffentlichen Schlüssel des Zertifikats unter vertrauenswürdigen Zertifikaten.
- Wenn das Zertifikat von einer Zertifizierungsstelle eines Drittanbieters signiert wird, müssen "Import Root" und alle anderen Zwischenzertifikate des Zertifikats importiert werden.

Navigieren Sie zu **Administration > System > Certificates > Certificate Management > Trusted Certificate**, und klicken Sie auf **Importieren**, wie in diesem Bild gezeigt.

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
- Trusted Certificates**
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Setti...

Certificate Authority

Trusted Certificates

Edit Import Export Delete View

<input type="checkbox"/>	Friendly Name	Status	Trusted For	Sei
<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 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
- Trusted Certificates**
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Setti...

Certificate Authority

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

Schritt 2: Importieren Sie das eigentliche Zertifikat.

1. Navigieren Sie, wie in diesem Bild gezeigt, zu **Administration > System > Certificates > Certificate Management (Verwaltung > Zertifikate > Zertifikatsverwaltung)**, und klicken Sie auf **Import (Importieren)**. Wenn dem Zertifikat die Rolle admin zugewiesen ist, wird der Dienst auf dem Knoten neu gestartet.

The screenshot shows the Cisco Identity Services Engine Administration interface. The navigation menu includes 'Administration' and 'System' > 'Certificates'. The main content area is titled 'System Certificates' and contains a table of certificates. The 'Import' button is highlighted in red.

	Friendly Name	Used By	Portal group tag
▼ ise-1			
<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	
▶ ise-2			

2. Wählen Sie den Knoten aus, für den Sie das Zertifikat importieren möchten.

3. Durchsuchen Sie die öffentlichen und privaten Schlüssel.

4. Geben Sie das Kennwort für den privaten Schlüssel des Zertifikats ein, und wählen Sie die gewünschte Rolle aus.

5. Klicken Sie nun auf **Senden**, wie in diesem Bild gezeigt.

▼ 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