

Importazione ed esportazione di certificati in ISE

Sommario

[Introduzione](#)

[Premesse](#)

[Esportare il certificato in ISE](#)

[Importare il certificato in ISE](#)

Introduzione

In questo documento viene descritto come importare ed esportare i certificati in Cisco Identity Service Engine (ISE).

Premesse

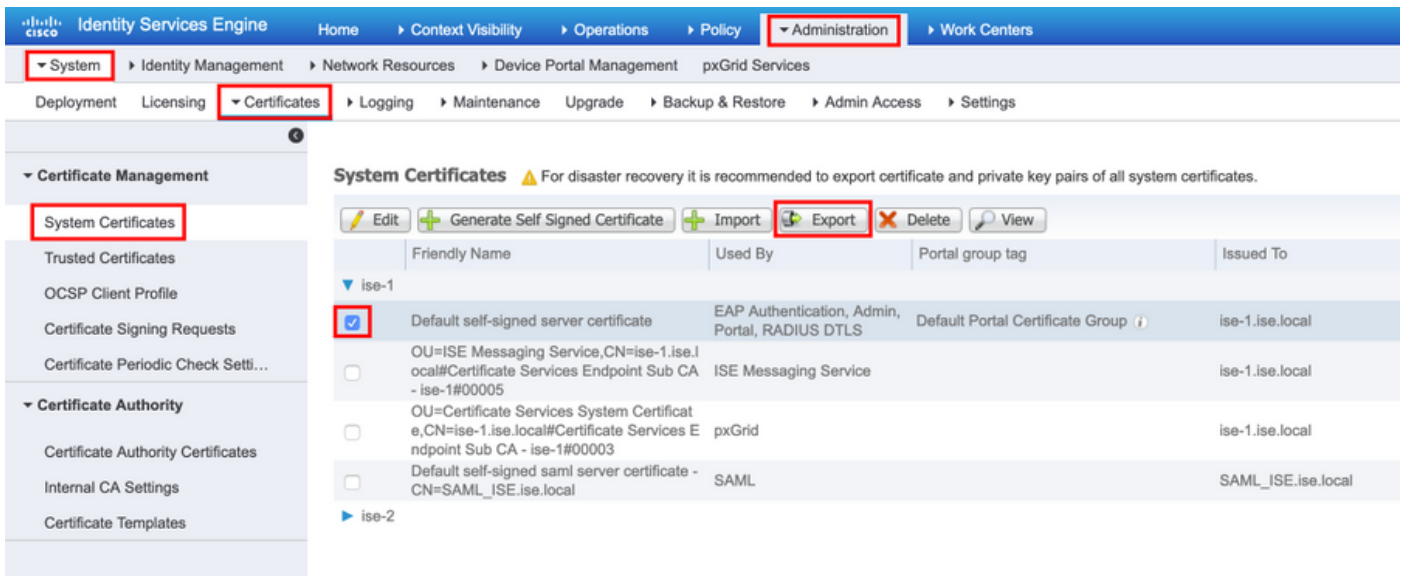
ISE utilizza i certificati per vari scopi (interfaccia utente Web, portali Web, EAP, pxgrid). Il certificato presente sull'ISE può avere uno dei seguenti ruoli:

- Amministratore: Per la comunicazione tra nodi e l'autenticazione del portale di amministrazione.
- EAP: Per l'autenticazione EAP.
- DTL RADIUS: Per l'autenticazione del server DTLS RADIUS.
- Portale: Per comunicare tra tutti i portali degli utenti finali di Cisco ISE.
- PxGrid Per comunicare tra il controller pxGrid.

È importante eseguire un backup dei certificati installati sui nodi ISE. Quando si esegue il backup della configurazione, viene eseguito il backup dei dati di configurazione e del certificato del nodo admin. Per gli altri nodi, tuttavia, il backup dei certificati viene eseguito singolarmente.

Esportare il certificato in ISE

Selezionare **Amministrazione > Sistema > Certificati > Gestione certificati > Certificato di sistema**. Espandere il nodo, selezionare il certificato e fare clic su **Esporta**, come mostrato nell'immagine:



Come illustrato in questa immagine, selezionare **Esporta certificato e chiave privata**. Immettere una password alfanumerica lunga almeno 8 caratteri. Questa password è necessaria per ripristinare il certificato.



Suggerimento: Non dimenticare la password.

Importare il certificato in ISE

L'importazione del certificato su ISE richiede due passaggi.

Passaggio 1. Verificare se il certificato è autofirmato o firmato da terze parti.

- Se il certificato è autofirmato, importare la chiave pubblica del certificato in certificati attendibili.
- Se il certificato è firmato da un'autorità di certificazione di terze parti, Importa radice e tutti gli altri certificati intermedi del certificato.

Selezionare **Amministrazione > Sistema > Certificati > Gestione certificati > Certificato attendibile**, quindi fare clic su **Importa**, come mostrato nell'immagine.

Identity Services Engine Administration

System > Certificates

Trusted Certificates

Friendly Name	Status	Trusted For	Se
Baltimore CyberTrust Root	Enabled	Cisco Services	02
Cisco ECC Root CA 2099	Enabled	Cisco Services	03
Cisco Licensing Root CA	Enabled	Cisco Services	01
Cisco Manufacturing CA SHA2	Enabled	Infrastructure Endpoints	02
Cisco Root CA 2048	Disabled	Endpoints Infrastructure	5F
Cisco Root CA 2099	Enabled	Cisco Services	01
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

Passaggio 2. Importare il certificato effettivo.

1. Come mostrato in questa immagine, passare ad **Amministrazione > Sistema > Certificati > Gestione certificati**, fare clic su **Importa**. Se il ruolo admin è assegnato al certificato, il servizio nel nodo viene riavviato.

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 with columns for 'Friendly Name', 'Used By', and 'Portal group tag'. The table is grouped by 'ise-1' and 'ise-2'.

	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. Selezionare il nodo per il quale si desidera importare il certificato.

3. Sfogliare le chiavi pubbliche e private.

4. Immettere la password per la chiave privata del certificato e selezionare il ruolo desiderato.

5. Fare clic su **Submit** (Invia), come mostrato nell'immagine.

- ▼ 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