

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). I certificati presenti sull'ISE possono avere uno dei seguenti ruoli:

- Admin: per la comunicazione tra nodi e l'autenticazione del portale Admin.
- EAP: per autenticazione EAP.
- DTLS RADIUS: per l'autenticazione del server DTLS RADIUS.
- Portal: consente di comunicare tra tutti i portali per utenti finali di Cisco ISE.
- PxGrid: per la comunicazione tra il controller pxGrid.

Creare un backup dei certificati installati sui nodi ISE. In questo modo viene salvato il backup dei dati di configurazione e viene acquisito il certificato del nodo admin. Per gli altri nodi, tuttavia, il backup dei certificati viene eseguito singolarmente.

Esportare il certificato in ISE

Passare a 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.

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.

Export Cancel

 Suggerimento: non dimenticare la password.

Importare il certificato in ISE

Per importare il certificato su ISE, è necessario eseguire due passaggi.

Passaggio 1. Determinare 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, importare il certificato radice e tutti gli altri certificati intermedi.

Selezionare Amministrazione > Sistema > Certificati > Gestione certificati > Certificato attendibile, quindi fare clic su Importa.

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

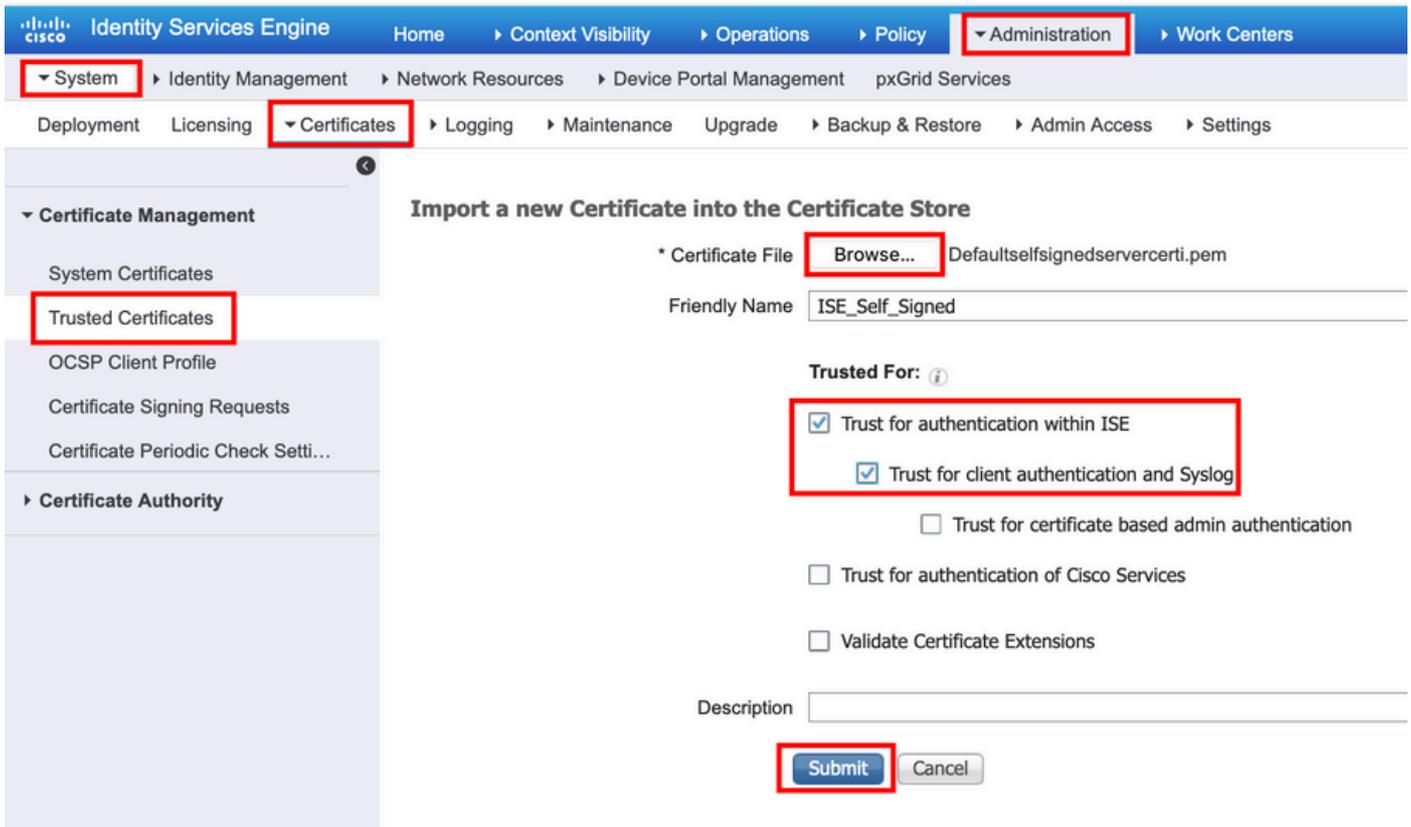
- System Certificates
- Trusted Certificates**
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Setti...

Certificate Authority

Trusted Certificates

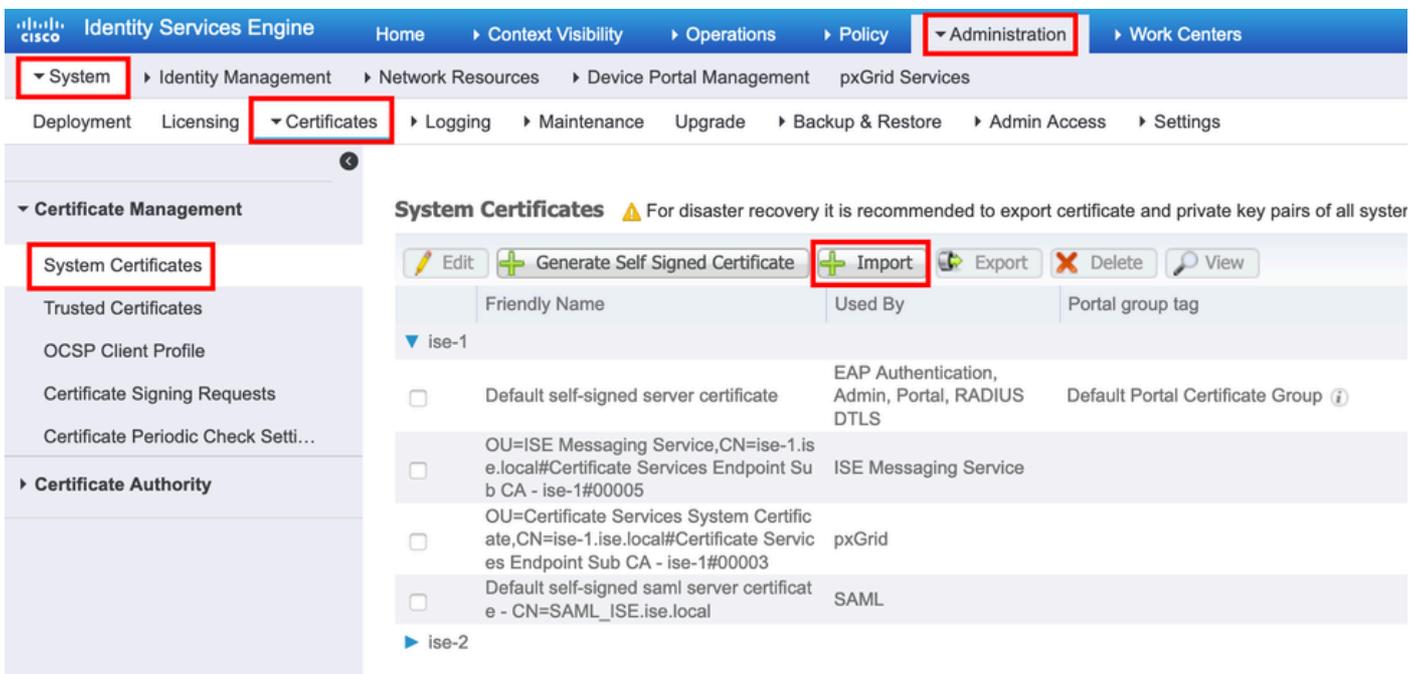
Edit **Import** Export Delete View

<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



Passaggio 2. Importa il certificato effettivo.

1. Passare ad Amministrazione > Sistema > Certificati > Gestione certificati, quindi fare clic su Importa. Se il ruolo admin è assegnato al certificato, il servizio nel nodo viene riavviato.



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 Sottometti.

The screenshot displays the Cisco Identity Services Engine (ISE) interface for importing a server certificate. The navigation path is: Administration > Certificates > System Certificates. The main form is titled "Import Server Certificate" and includes the following fields and options:

- Select Node:** A dropdown menu with "ise-1" selected.
- Certificate File:** A "Browse..." button next to the default filename "Defaultselfsignedservercert.pem".
- Private Key File:** A "Browse..." button next to the default filename "Defaultselfsignedservercert.pvk".
- Password:** A text input field containing masked characters (dots).
- Friendly Name:** A text input field with the value "ISE_Self_Signed".
- Allow Wildcard Certificates:** An unchecked checkbox.
- Validate Certificate Extensions:** An unchecked checkbox.
- Usage:** A section with several unchecked checkboxes:
 - 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

A red text overlay "Select Required Role" is positioned to the left of the "Usage" section. The "Submit" button at the bottom of the form is highlighted with a red box.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).