# Importazione ed esportazione di certificati in ISE

## Sommario



## Introduzione

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

## Premesse

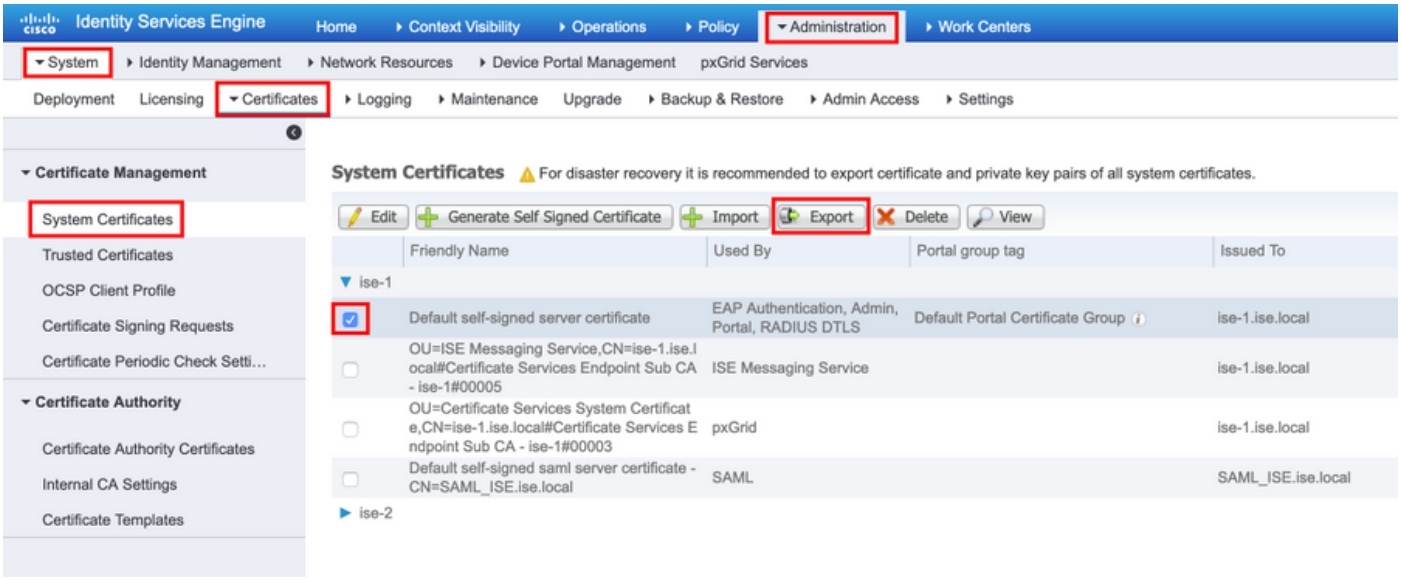
ISE utilizza i certificati per vari scopi (interfaccia utente Web, portali Web, EAP, pxgrid). Il certificato presente sull'ISE può avere uno dei seguenti ruoli:

- 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.

Èimportante 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.

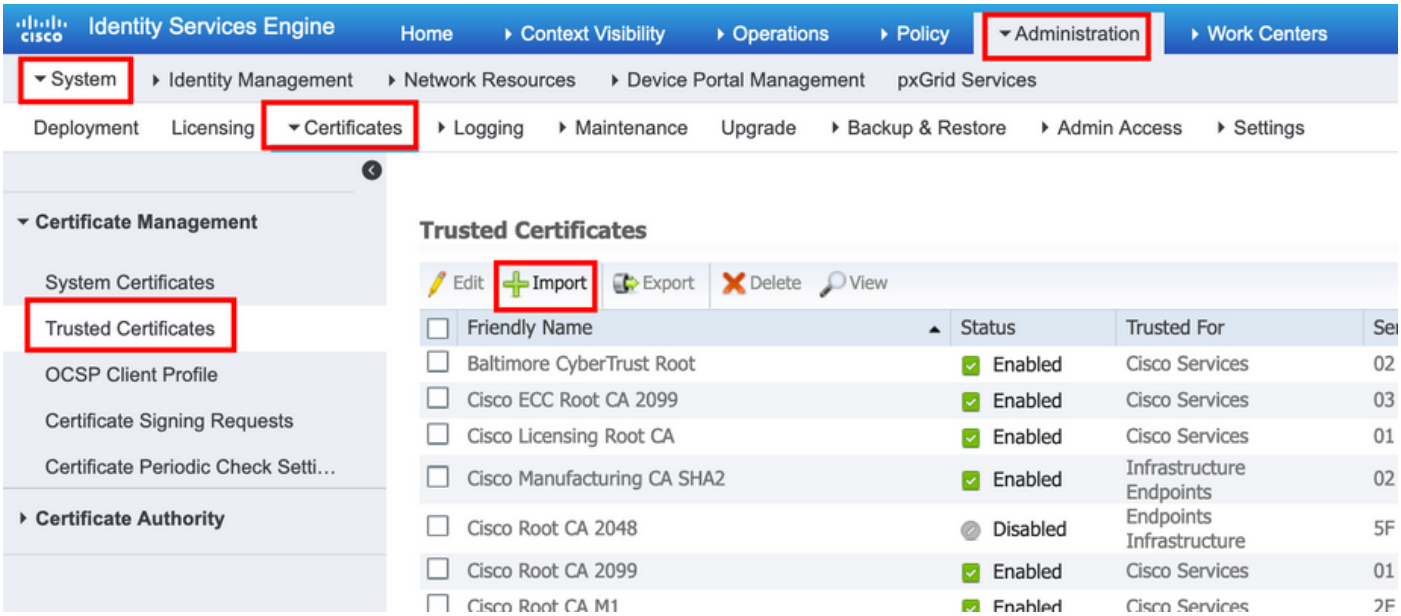
# Importare il certificato in ISE

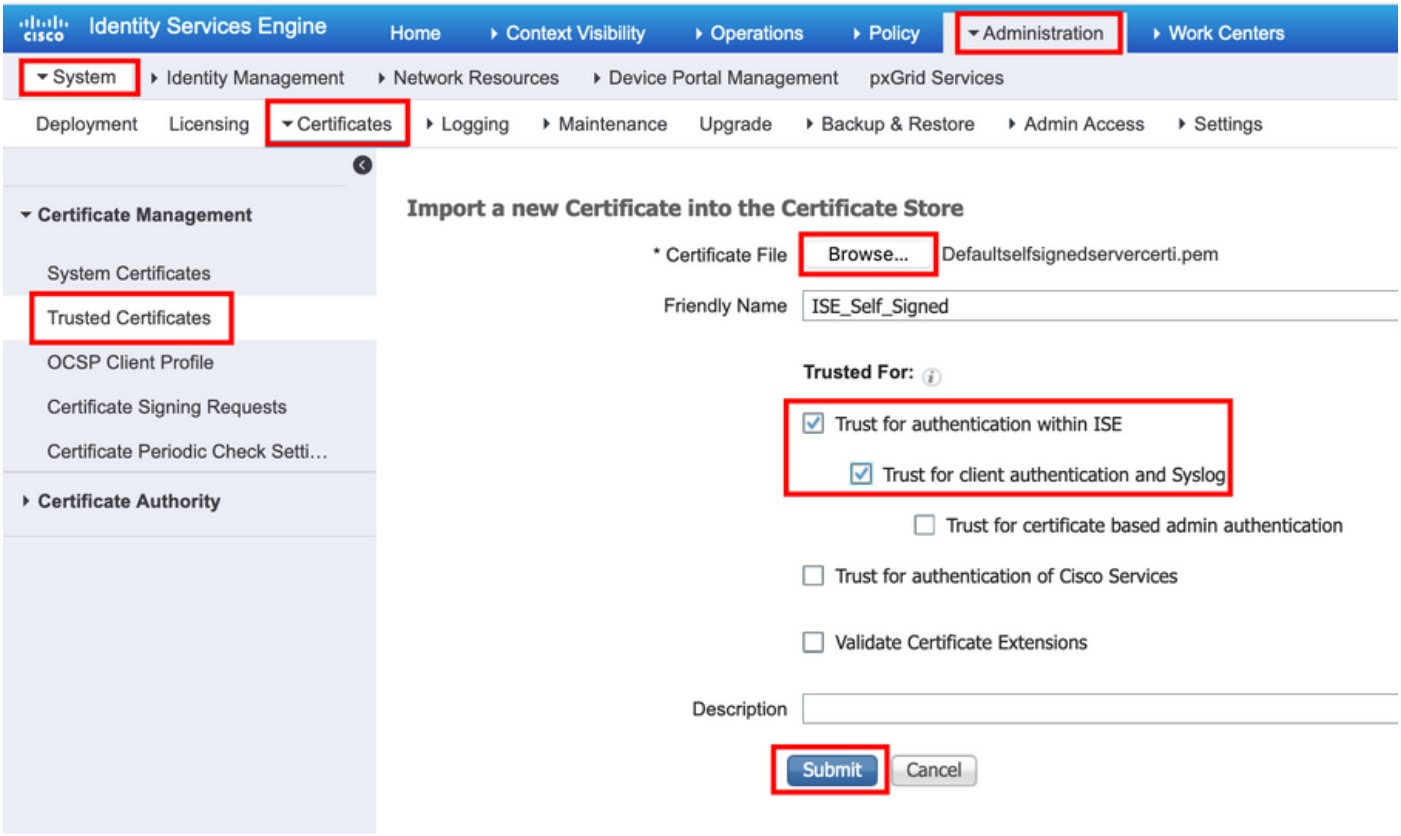
L'importazione del certificato su ISE richiede due passaggi.

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.

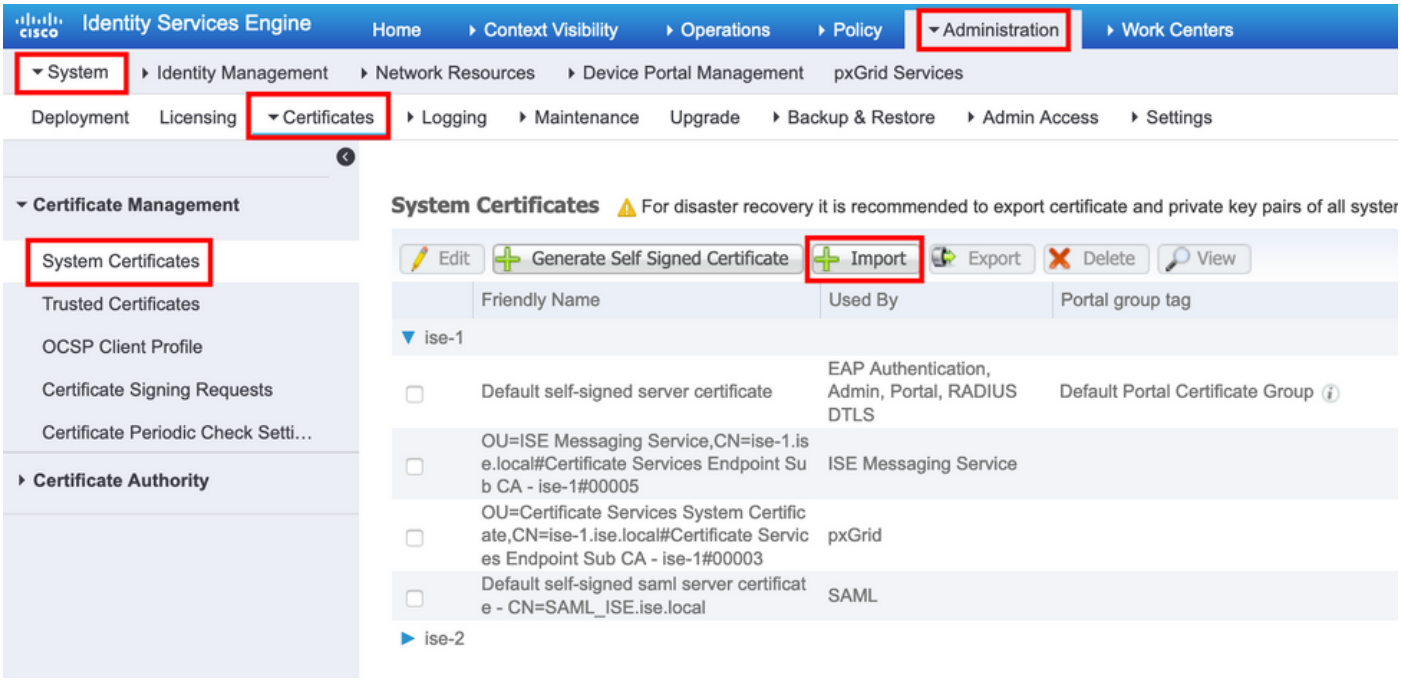
Selezionare **Amministrazione > Sistema > Certificati > Gestione certificati > Certificato attendibile,** quindi fare clic su **Importa**, come mostrato nell'immagine.




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.

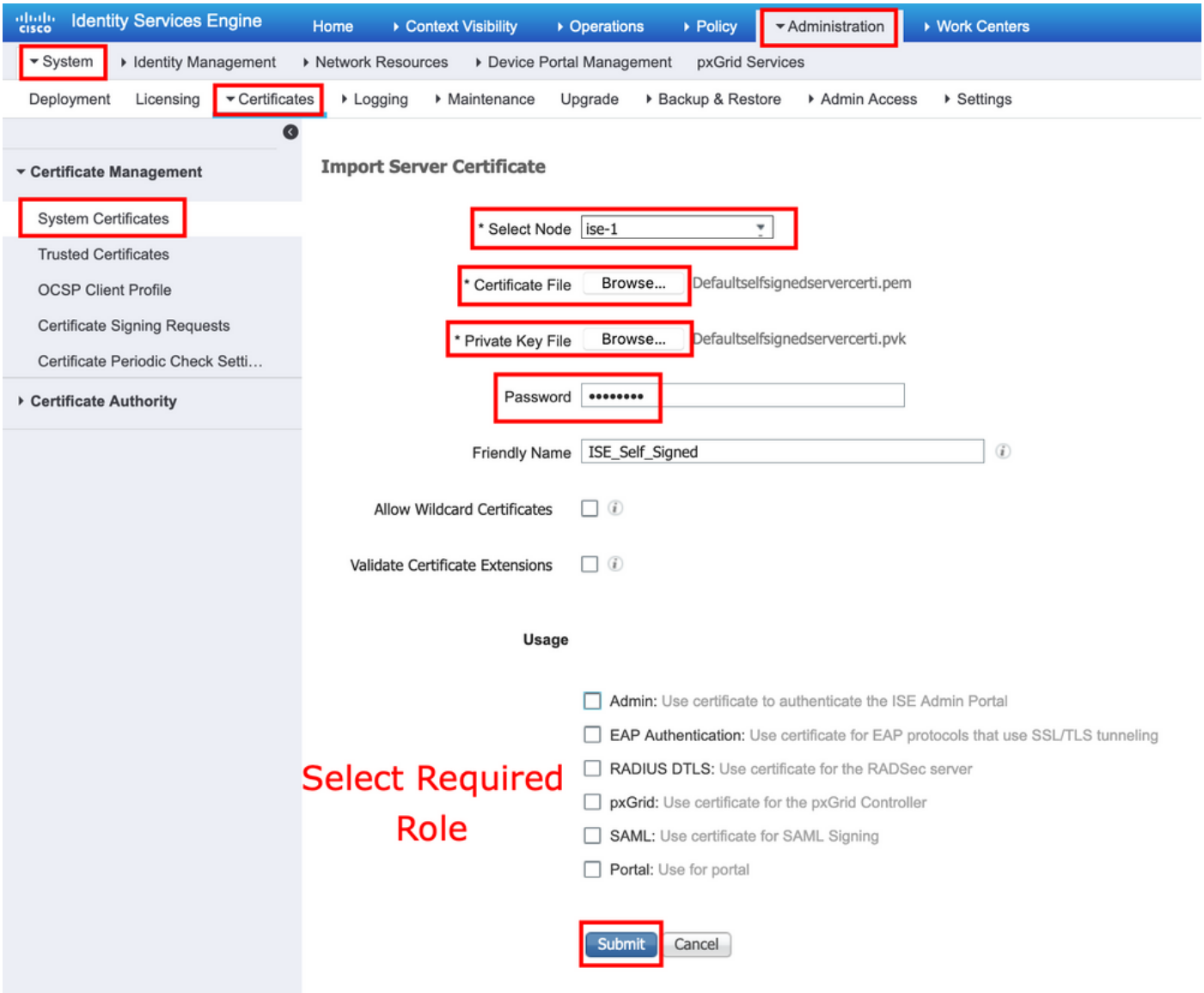



2. Selezionare il nodo per il quale si desidera importare il certificato.

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.


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 Server Certificate
* Select Node
ise-1
* Certificate File
Browse...
Defaultselfsignedservercerti.pem
* Private Key File
Browse...
Defaultselfsignedservercerti.pvk
Password
Friendly Name
ISE_Self_Signed
Allow Wildcard Certificates
Validate Certificate Extensions
Usage
Select Required Role
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
Submit
Cancel