ISEでの証明書のインポートとエクスポート

内容

[概要](#)
[背景説明](#)
[ISEでの証明書のエクスポート](#)
[ISEでの証明書のインポート](#)

概要

このドキュメントでは、Cisco Identity Service Engine(ISE)で証明書をインポートおよびエクスポートする方法について説明します。

背景説明

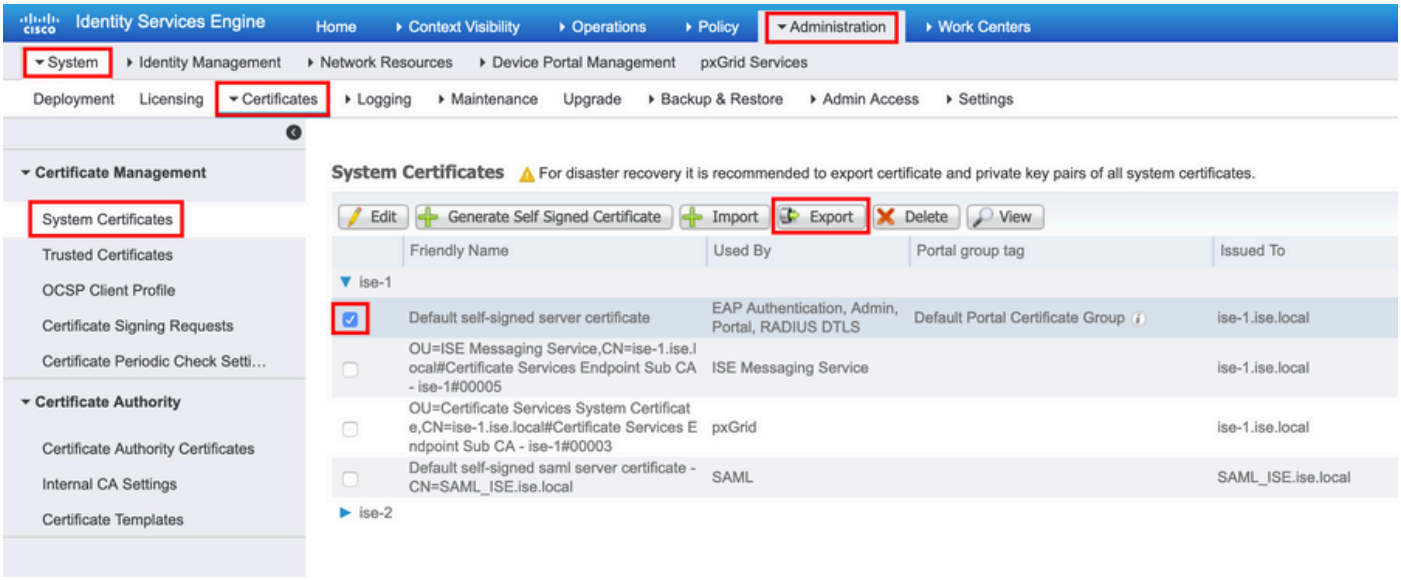
ISEは、さまざまな目的（Web UI、Webポータル、EAP、pxgrid）で証明書を使用します。
ISEに存在する証明書は、次のいずれかの役割を持つことができます。

- [Admin]：管理ポータルのノード間通信および認証に使用します。
- [EAP]:EAP認証の場合。
- [RADIUS DTLS]:RADIUS DTLSサーバ認証の場合。
- [Portal]：すべてのCisco ISEエンドユーザポータル間で通信します。
- PxGrid:pxGridコントローラ間で通信します。

ISEノードにインストールされた証明書のバックアップを作成することが重要です。設定のバックアップを作成すると、管理ノードの設定データと証明書のバックアップが作成されます。ただし、他のノードでは、証明書のバックアップは個別に行われます。

ISEでの証明書のエクスポート

[Administration] > [System] > [Certificates] > [Certificate Management] > [System certificate] に移動します。**図に示すように、ノードを展開し、証明書を選択して、[Export]** をクリックします。



次の図に示すように、[Export Certificate and Private Key] を選択します。8文字以上の英数字のパスワードを入力します。証明書を復元するには、このパスワードが必要です。

ヒント：パスワードを忘れないでください。

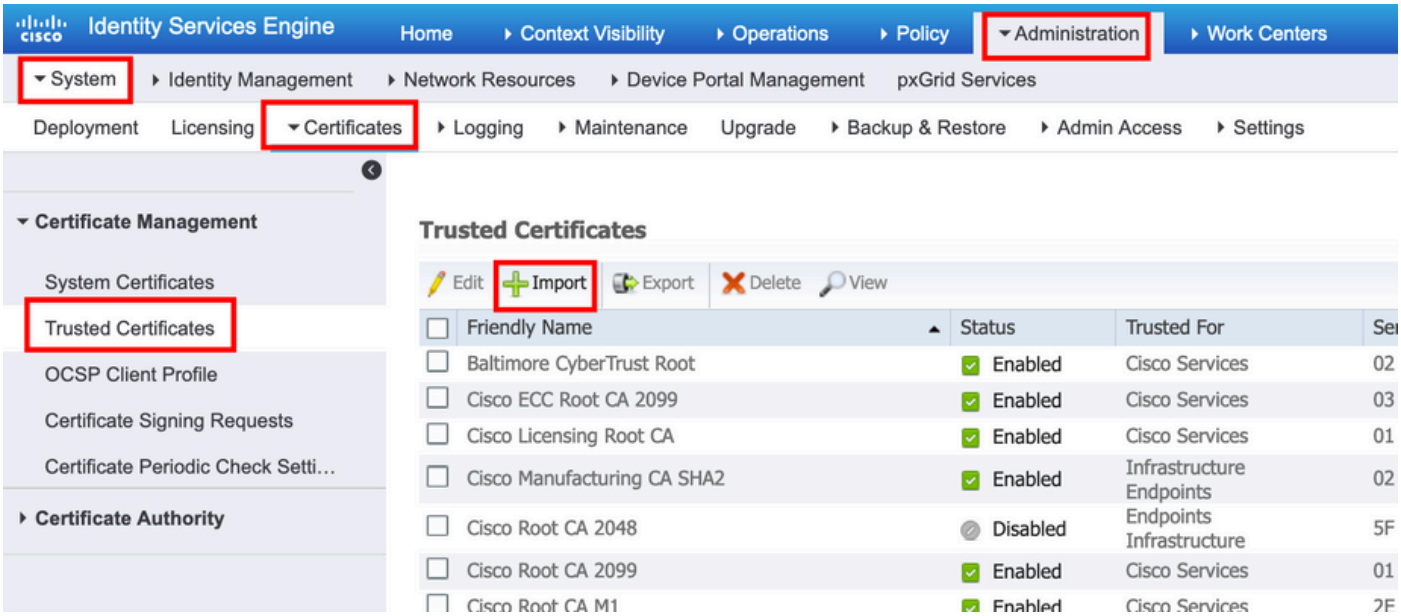
ISEでの証明書のインポート

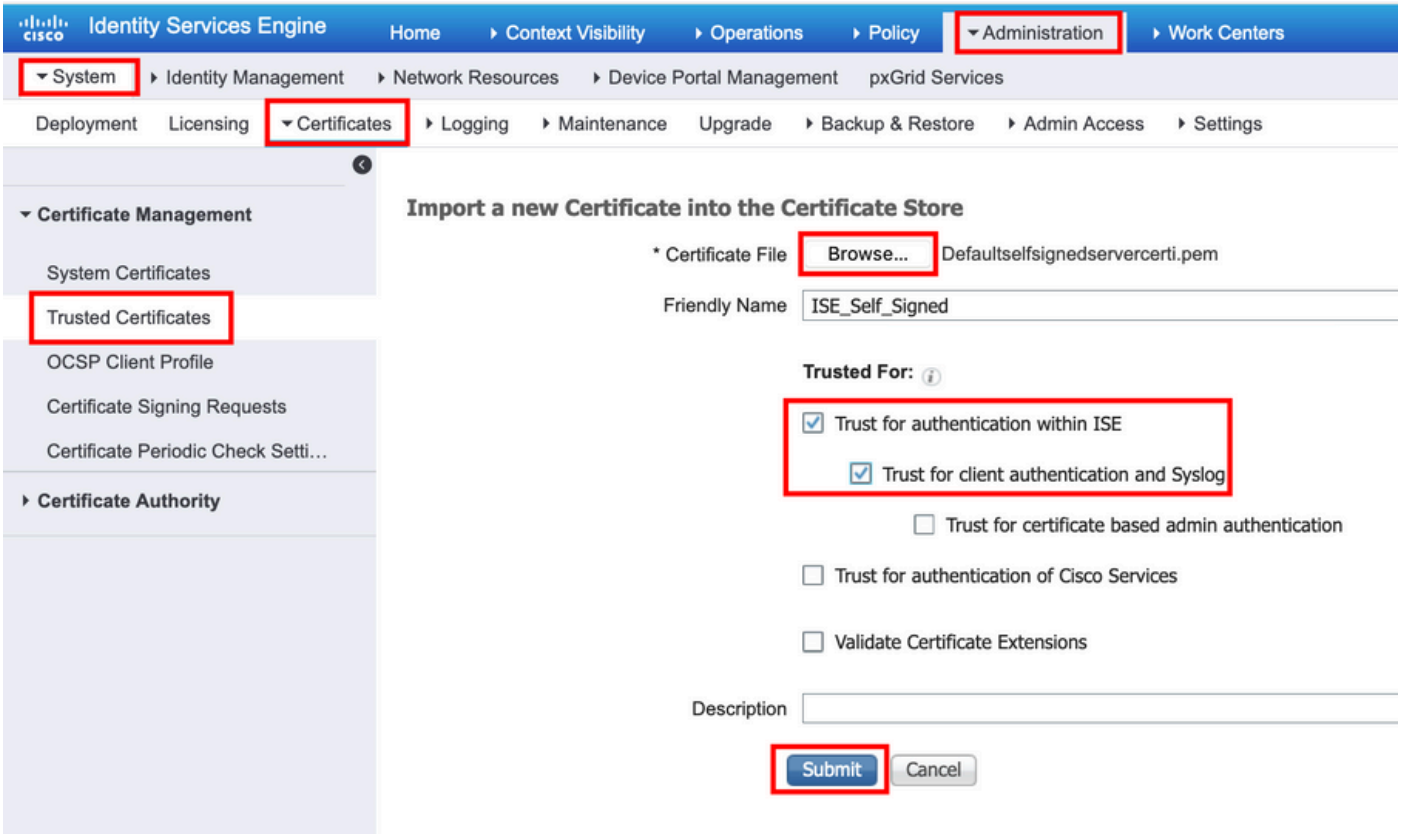
ISEに証明書をインポートするには、次の2つの手順を実行します。

ステップ 1：証明書が自己署名証明書またはサードパーティ署名付き証明書のいずれであるかを確認します。

- 証明書が自己署名されている場合は、信頼できる証明書の下に証明書の公開キーをインポートします。
- 証明書がサードパーティの認証局によって署名されている場合は、ルートおよびその証明書の他のすべての中間証明書をインポートします。

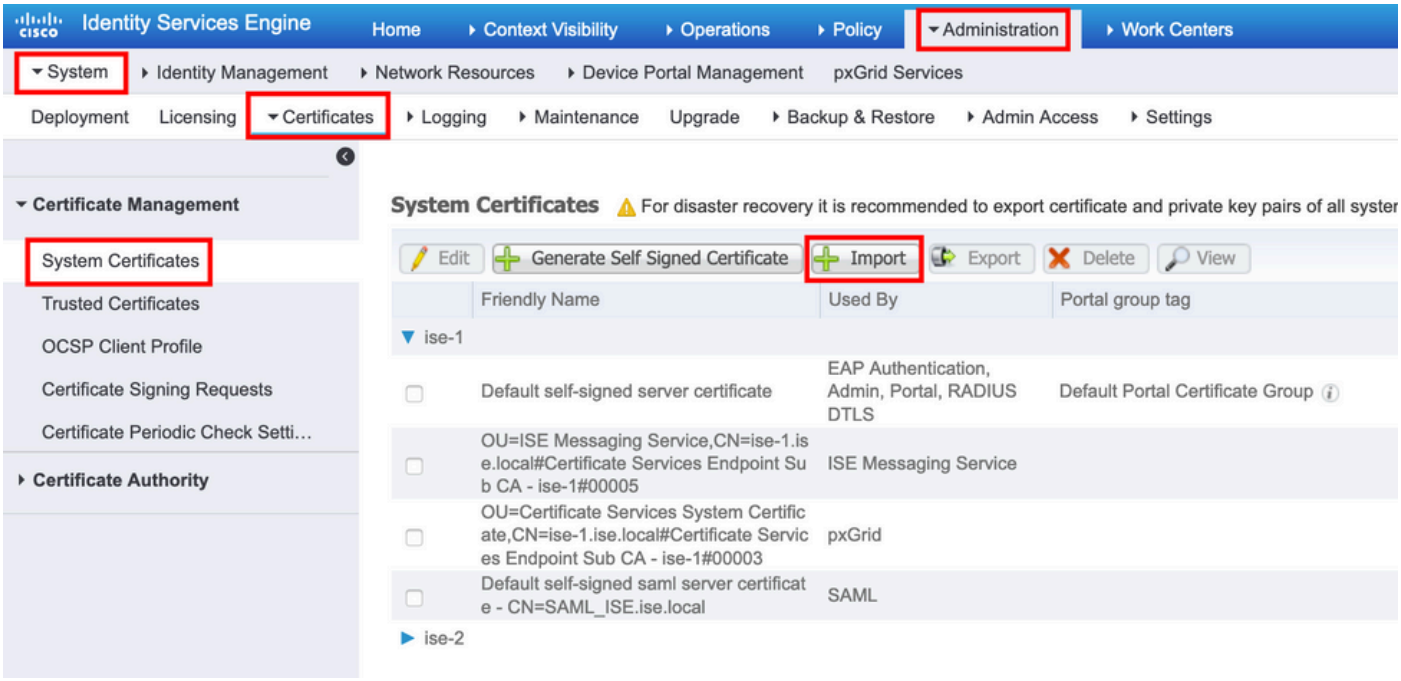
次の図に示すように、[Administration] > [System] > [Certificates] > [Certificate Management] > [Trusted Certificate] に移動し、[Import] をクリックします。





ステップ 2：実際の証明書をインポートします。

1.この図に示すように、[Administration] > [System] > [Certificates] > [Certificate Management] に移動し、[Import] をクリックします。管理者ロールが証明書に割り当てられている場合は、ノード上のサービスが再起動されます。

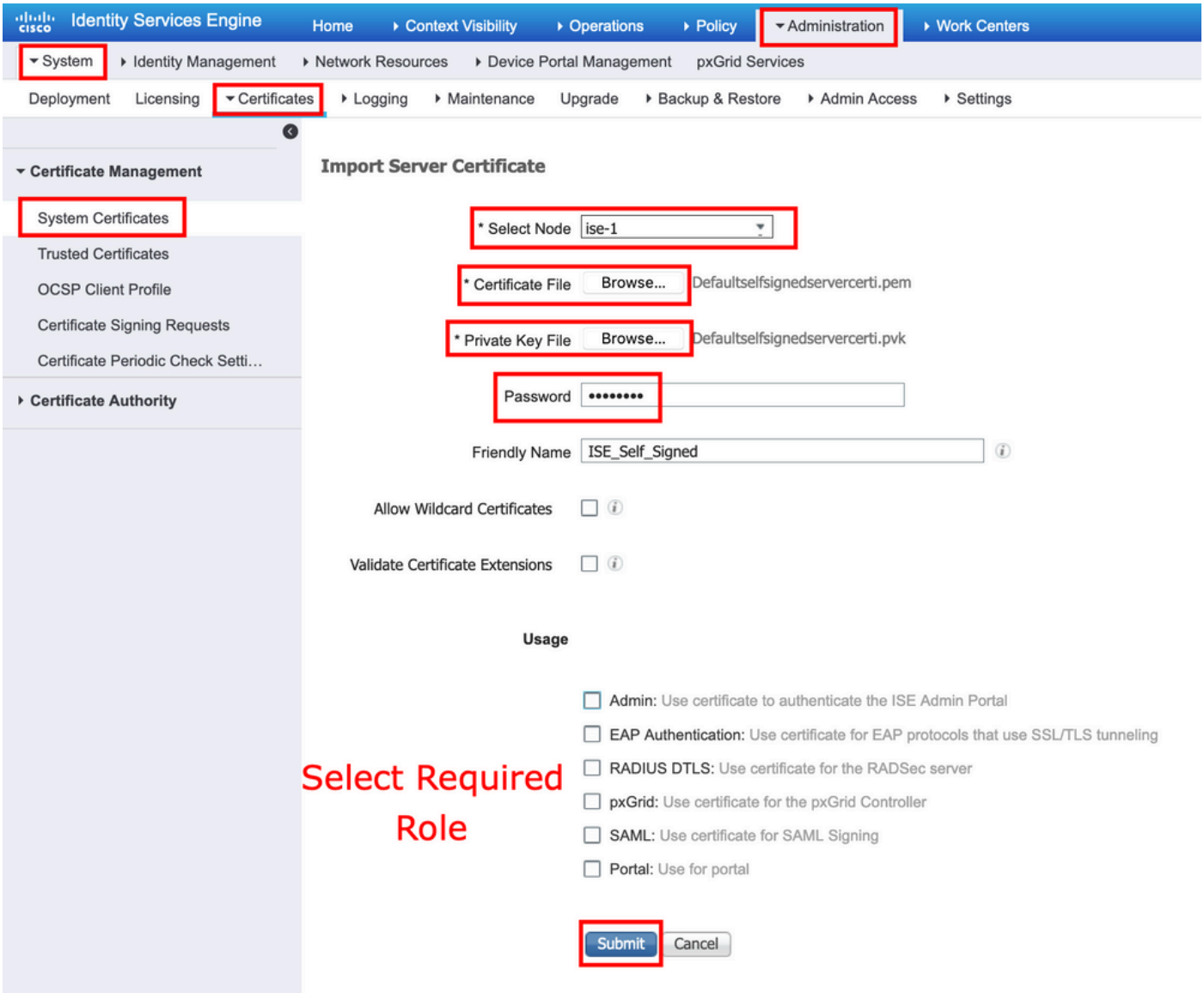


2.証明書をインポートするノードを選択します。

3.公開キーと秘密キーを参照します。

4.証明書の秘密キーのパスワードを入力し、目的のロールを選択します。

5.次の図に示すように、[Submit] をクリックします。


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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。