

ISEでの証明書のインポートとエクスポート

目次

[はじめに](#)

[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](#)

はじめに

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) のために証明書を使用します。ISEに存在する証明書には、次のいずれかのロールを設定できます。

- 管理者：管理ポータルのノード間通信および認証の場合。
- EAP:EAP認証用。
- RADIUS DTLS:RADIUS DTLSサーバ認証用。
- ポータル：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ている証明書のバックアップを取ることが重要です。設定のバックアップを取ると、設定データのバックアップと管理ノードの証明書が取得されます。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。

The screenshot shows the Cisco Identity Services Engine Administration interface. The navigation path is: Administration > System > Certificates > System Certificates. The 'Export' button is highlighted with a red box. Below it, a table lists certificates. The first certificate, 'Default self-signed server certificate', is selected with a red checkmark. The table columns are: Friendly Name, Used By, Portal group tag, and Issued To.

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

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

The dialog box is titled 'Export Certificate' and shows options for exporting the 'Default self-signed server certificate'. The 'Export Certificate and Private Key' option is selected. Below the options are two input fields for passwords: '*Private Key Password' and '*Confirm Password'. A warning message states: 'Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.' The 'Export' button is highlighted with a red box.

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で証明書をインポートするには、2つの手順があります。

ステップ1：証明書が自己署名証明書かサードパーティ署名付き証明書かを確認します。

- 証明書が自己署名の場合は、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。
- 証明書が一部のサードパーティ認証局によって署名されている場合は、Import Rootと証明書のその他すべての中間証明書。

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。

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	Se
<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 **Browse...** Defaultselfsignedservercert.pem

Friendly Name ISE_Self_Signed

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

Submit Cancel

ステップ2：実際の証明書をインポートします。

1.次の図に示すように、[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、ノード上のサービスが再起動します。

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 under the 'ise-1' node:

	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. 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。

▼ 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 Defaultselfsignedservercerti.pem

* Private Key File Defaultselfsignedservercerti.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