

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。

Identity Services Engine Administration > System > Certificates > System Certificates

System Certificates

Friendly Name	Used By	Portal group tag	Issued To
<input checked="" type="checkbox"/> Default self-signed server certificate	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group	ise-1.ise.local
<input type="checkbox"/> OU=ISE Messaging Service,CN=ise-1.ise.local#Certificate Services Endpoint Sub CA - ise-1#00005	ISE Messaging Service		ise-1.ise.local
<input type="checkbox"/> OU=Certificate Services System Certificate,CN=ise-1.ise.local#Certificate Services Endpoint Sub CA - ise-1#00003	pxGrid		ise-1.ise.local
<input type="checkbox"/> 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 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。

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.

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。

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 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

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。

The screenshot shows the Cisco Identity Services Engine Administration interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Administration' menu is expanded, showing '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'. Below this are buttons for 'Edit', 'Generate Self Signed Certificate', 'Import', 'Export', 'Delete', and 'View'. A table lists certificates under the 'ise-1' node:

	Friendly Name	Used By	Portal group tag
<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	

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 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

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。