

如何从ISE导入和导出证书？

简介

本文档介绍如何对身份服务引擎(ISE)进行系统证书备份。

先决条件

要求

Cisco 建议您了解以下主题：

- 身份服务引擎(ISE)的基本知识

使用的组件

本文档中的信息基于思科身份服务引擎2.7

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

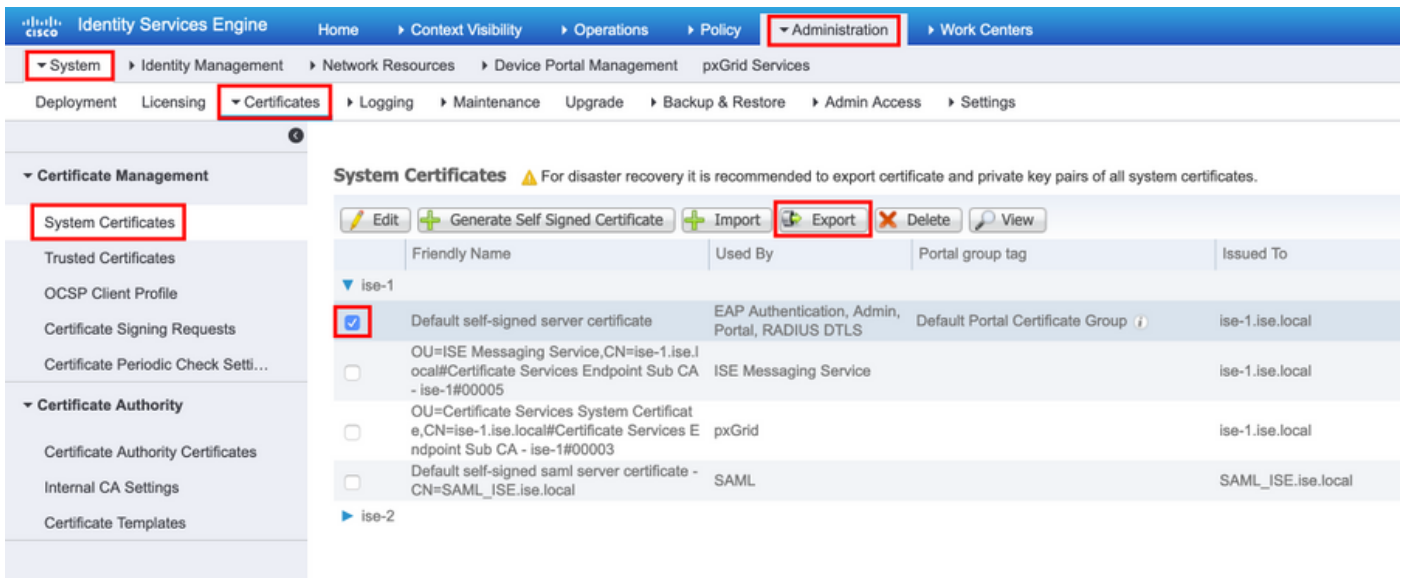
ISE使用证书用于各种用途（Web UI、Web门户、EAP、pxgrid）。ISE上存在的证书可以具有以下角色之一：

- 管理员:用于节点间通信和对管理员门户进行身份验证。
- EAP:用于EAP身份验证。
- RADIUS DTLS:用于RADIUS DTLS服务器身份验证。
- 门户：用于与所有思科ISE最终用户门户通信。
- PxGrid:用于与pxGrid控制器通信。

备份ISE节点上安装的证书非常重要。进行配置备份时，会备份配置数据和管理节点的证书。但是，对于策略服务节点(PSN)，我们必须单独备份证书。

如何获取身份服务引擎的证书备份？

导航至**管理>System >证书>证书管理>系统证书**。展开节点，选择证书，然后单击**导出**，如图所示：



选择导出证书和私钥。在长度字母数字密码中输入最少8个字符。恢复证书需要此密码。



提示：确保记住密码。

如何在身份服务引擎上导入证书？

在ISE上导入证书涉及两个步骤。

步骤1.确定证书是自签名证书还是第三方签名证书。

如果证书是自签名的，则在受信任证书下导入证书的公钥，如果证书签署了某些第三方证书，则导入根证书和证书的所有中间证书。

导航至**管理>系统>证书>证书管理>受信任证书**，单击**导入**，如此图所示。

Identity Services Engine Administration

System > Certificates > Trusted Certificates

Trusted Certificates

Import

Friendly Name	Status	Trusted For	Se
Baltimore CyberTrust Root	Enabled	Cisco Services	02
Cisco ECC Root CA 2099	Enabled	Cisco Services	03
Cisco Licensing Root CA	Enabled	Cisco Services	01
Cisco Manufacturing CA SHA2	Enabled	Infrastructure Endpoints	02
Cisco Root CA 2048	Disabled	Endpoints Infrastructure	5F
Cisco Root CA 2099	Enabled	Cisco Services	01
Cisco Root CA M1	Enabled	Cisco Services	2F

Identity Services Engine Administration

System > Certificates > 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

步骤2. 导入实际证书。

导航至管理>系统>证书>证书管理，单击导入。如果管理员角色已分配给节点上的证书服务，则会重新启动。

System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system

	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		

选择要为其导入证书的节点，浏览公钥和私钥，输入证书私钥的密码，选择所需角色，单击提交，如此图所示。

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