

在ISE中导入和导出证书

目录

[简介](#)

[背景信息](#)

[在ISE中导出证书](#)

[在ISE中导入证书](#)

简介

本文档介绍如何在思科身份服务引擎(ISE)中导入和导出证书。

背景信息

ISE将证书用于各种用途 (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：用于管理员门户的节点间通信和身份验证。
- EAP：用于EAP身份验证。
- RADIUS DTLS：用于RADIUS DTLS服务器身份验证。
- 门户：在所有思科ISE最终用户门户之间进行通信。
- PxGrid：要在pxGrid控制器之间通信。

备份安装在ISE节点上的证书非常重要。当您进行配置备份时，将进行配置数据和管理员节点的证书的备份。但是，对于其他节点，证书的备份是单独进行的。

在ISE中导出证书

导航到**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：

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is **Administration > System > Certificates > System Certificates**. The 'System Certificates' page displays a table of certificates with columns for 'Friendly Name', 'Used By', 'Portal group tag', and 'Issued To'. The 'Default self-signed server certificate' is selected, and the 'Export' button is highlighted.

	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

如图所示，选择**导出证书和私钥**。输入长度为字母数字的密码中至少8个字符。还原证书需要此密码。



提示：不要忘记密码。

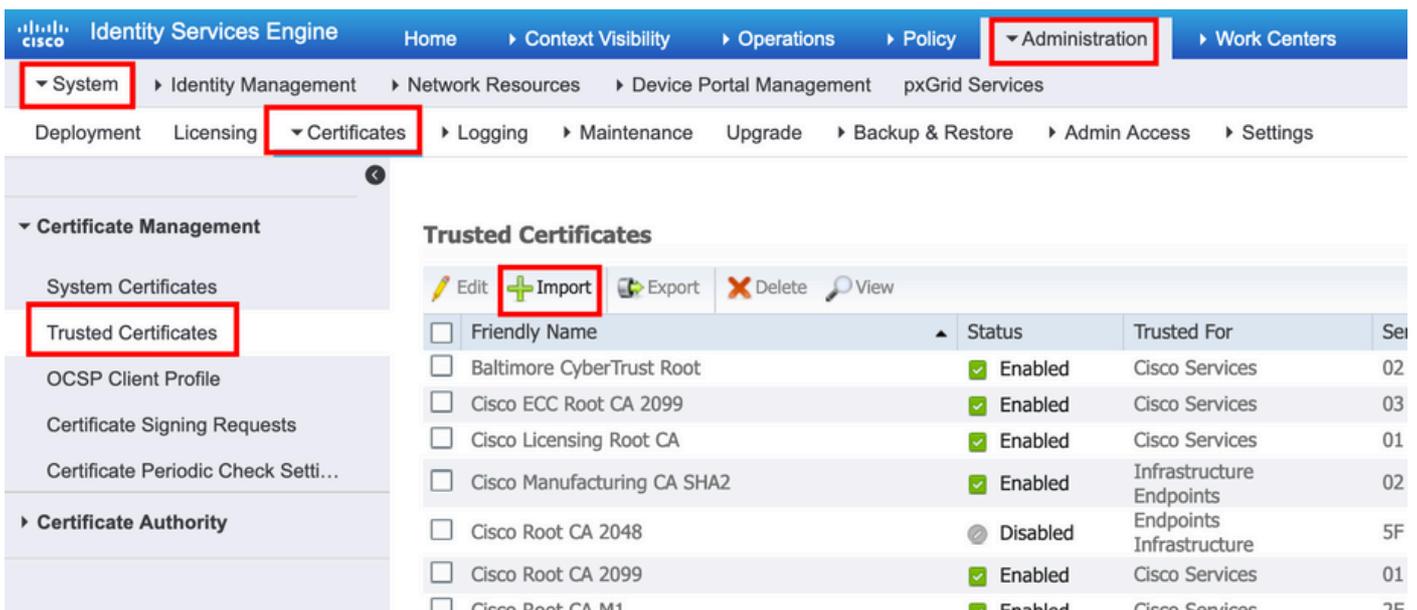
在ISE中导入证书

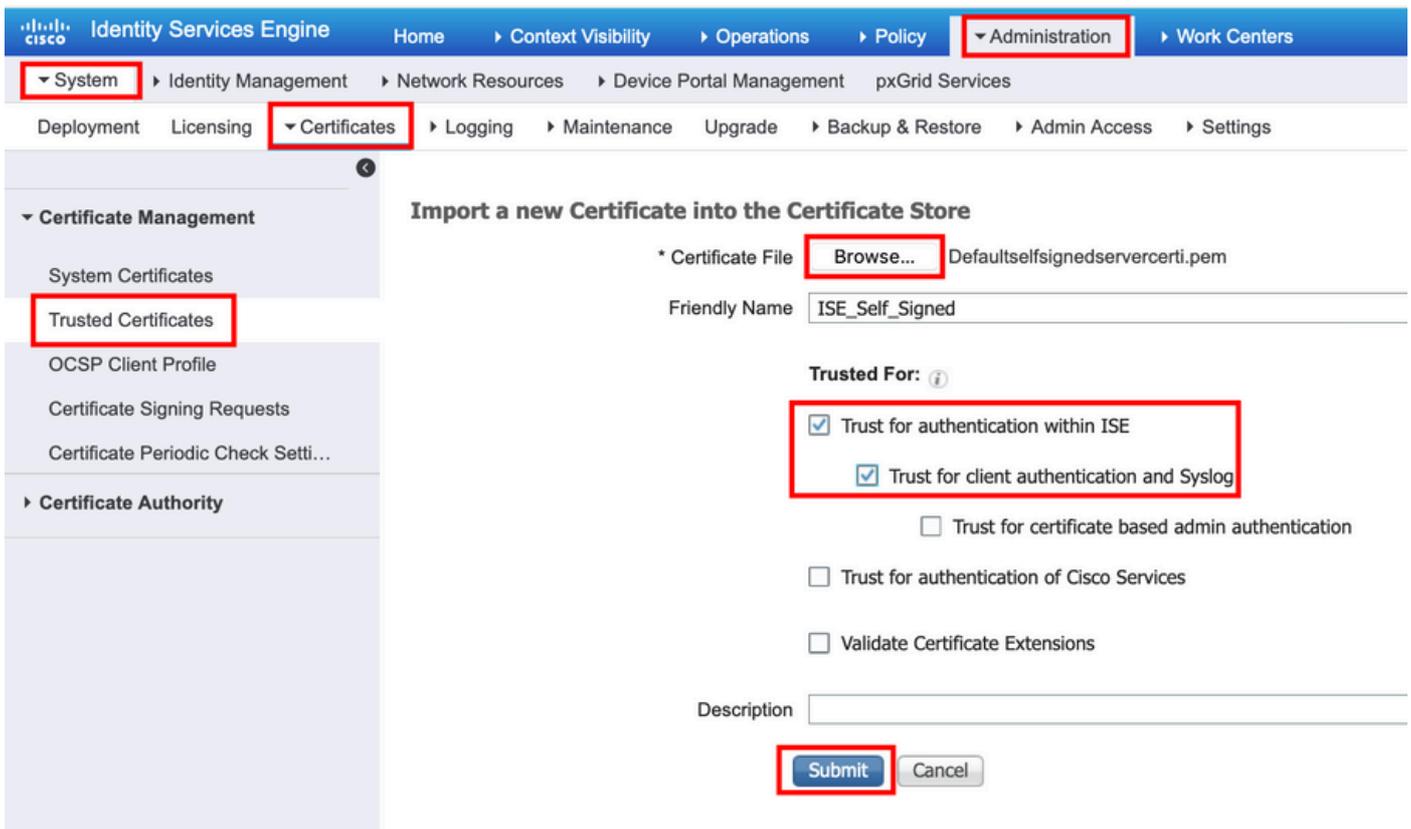
在ISE上导入证书涉及两个步骤。

步骤1:了解证书是自签名证书还是第三方签名证书。

- 如果证书是自签名证书，请在受信任证书下导入证书的公钥。
- 如果证书由某个第三方证书颁发机构签名，请导入根证书和证书的所有其他中间证书。

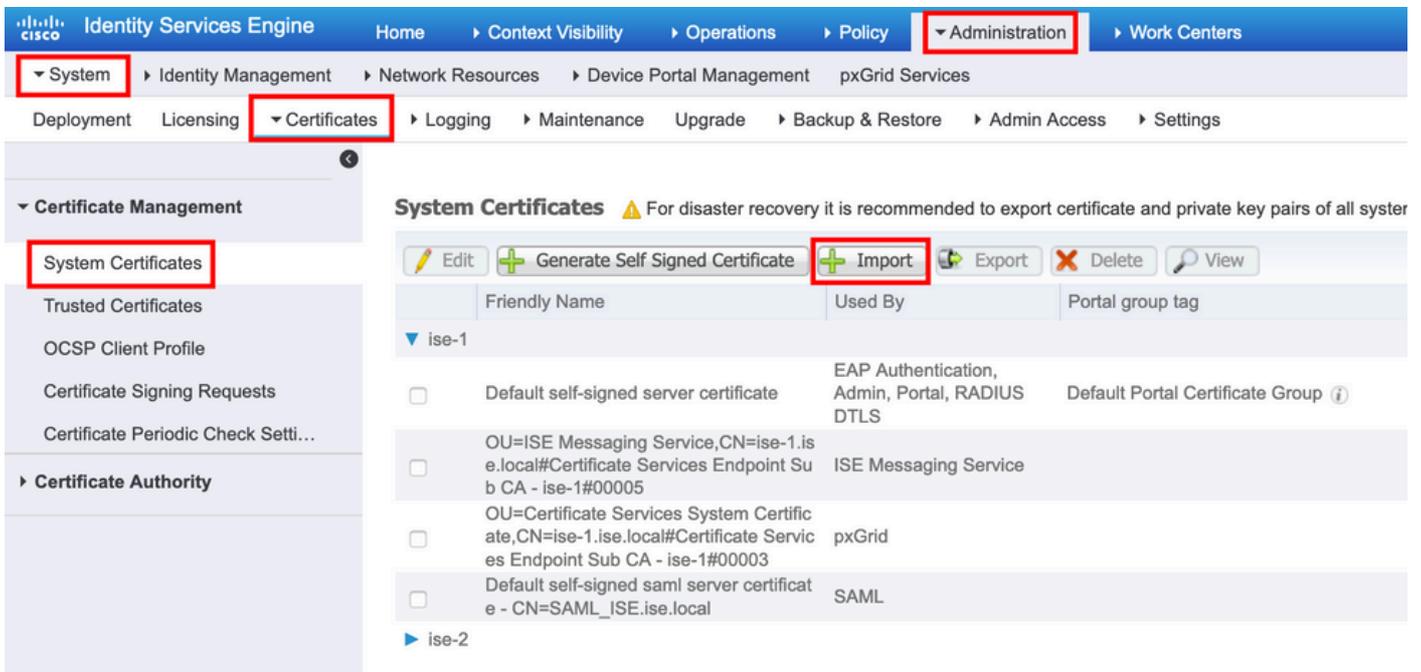
导航到**Administration > System > Certificates > Certificate Management > Trusted Certificate**，点击**Import**，如本图所示。





第二步：导入实际证书。

1.如本图所示，导航到**管理>系统>证书>证书管理**，点击**导入**。如果管理员角色已分配给证书，则节点上的服务将重新启动。



2.选择要为其导入证书的节点。

3.浏览公钥和私钥。

4.输入证书私钥的密码并选择所需的角色。

5.现在单击Submit，如图所示。

The screenshot displays the Cisco Identity Services Engine (ISE) interface for importing a server certificate. The navigation bar at the top includes 'Administration' and 'Work Centers'. The left sidebar shows 'System Certificates' under 'Certificate Management'. The main form, titled 'Import Server Certificate', contains the following elements:

- Select Node:** A dropdown menu with 'ise-1' selected.
- Certificate File:** A 'Browse...' button next to the default filename 'Defaultselfsignedservercerti.pem'.
- Private Key File:** A 'Browse...' button next to the default filename 'Defaultselfsignedservercerti.pvk'.
- Password:** A text input field containing masked characters (dots).
- Friendly Name:** A text input field with the value 'ISE_Self_Signed'.
- Allow Wildcard Certificates:** An unchecked checkbox.
- Validate Certificate Extensions:** An unchecked checkbox.
- Usage:** A section with several unchecked checkboxes:
 - 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:** Two buttons at the bottom, with 'Submit' highlighted by a red box.

Select Required Role

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。