

在ISE中匯入和匯出證書

目錄

[簡介](#)

[背景資訊](#)

[在ISE中匯出證書](#)

[在ISE中匯入證書](#)

簡介

本文說明如何匯入和匯出思科身份服務引擎(ISE)中的證書。

背景資訊

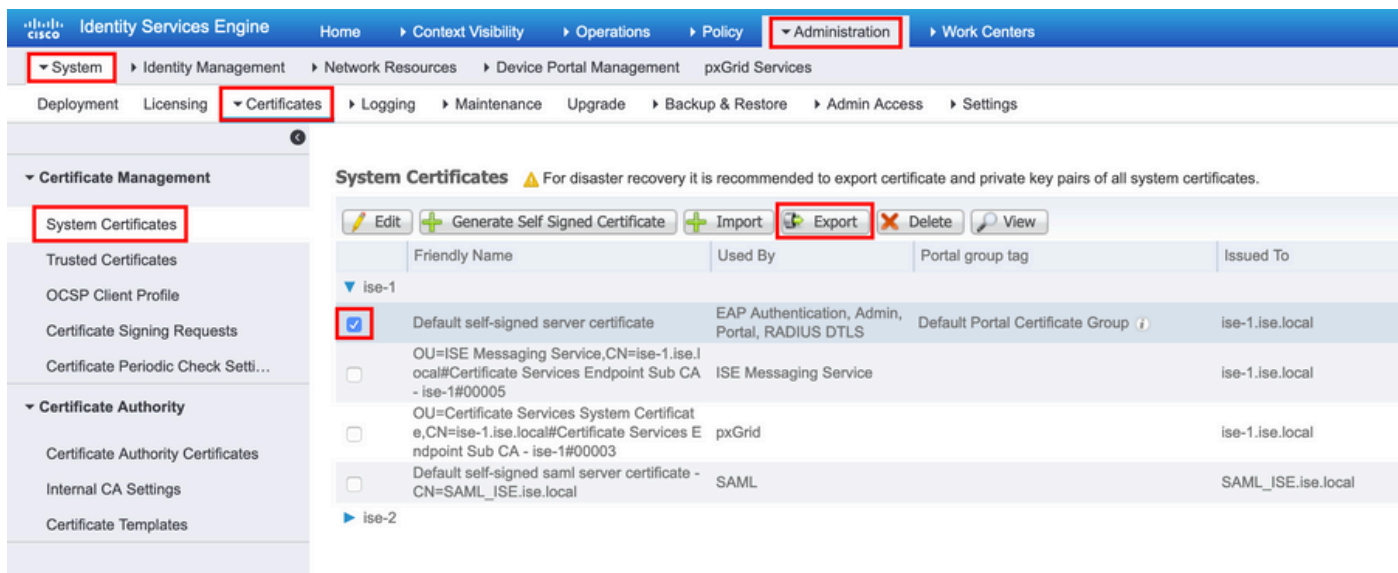
ISE將證書用於各種用途 (Web UI、Web門戶、EAP、pxgrid)。 ISE上存在的證書可以具有以下角色之一：

- 管理員：用於管理員門戶的節點間通訊和身份驗證。
- EAP：用於EAP身份驗證。
- RADIUS DTLS：用於RADIUS DTLS伺服器身份驗證。
- 門戶：在所有思科ISE終端使用者門戶之間通訊。
- PxGrid：要在pxGrid控制器之間通訊。

備份安裝在ISE節點上的證書非常重要。進行配置備份時，將進行配置資料和管理員節點證書的備份。但是，對於其他節點，證書備份是單獨進行的。

在ISE中匯出證書

導覽至Administration > System > Certificates > Certificate Management > System certificate。展開節點，選擇證書，然後按一下Export，如下圖所示：



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is Administration > System > Certificates > Certificate Management > System certificate. The 'Export' button is highlighted in red. The table below shows the list of certificates.

	Friendly Name	Used By	Portal group tag	Issued To
ise-1				
<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
ise-2				

如下圖所示，選擇**Export Certificate and Private Key**。輸入長度至少為8個字元的字母數位密碼。還原證書需要此密碼。



提示：不要忘記密碼。

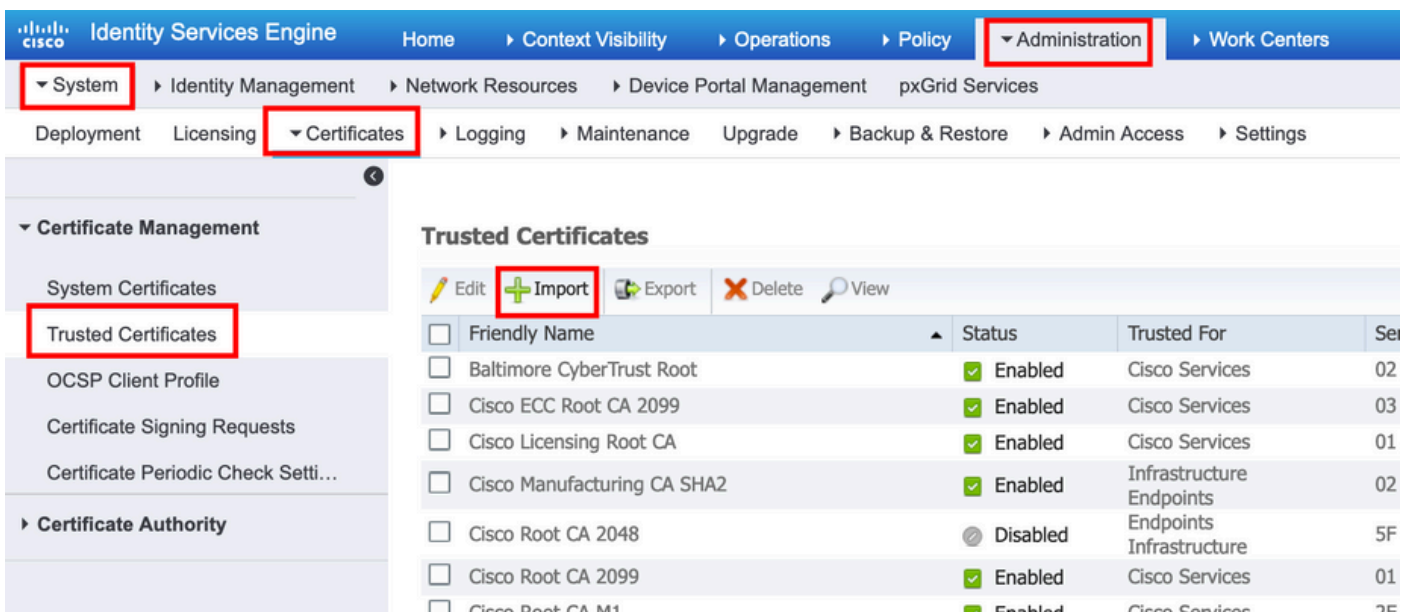
在ISE中匯入證書

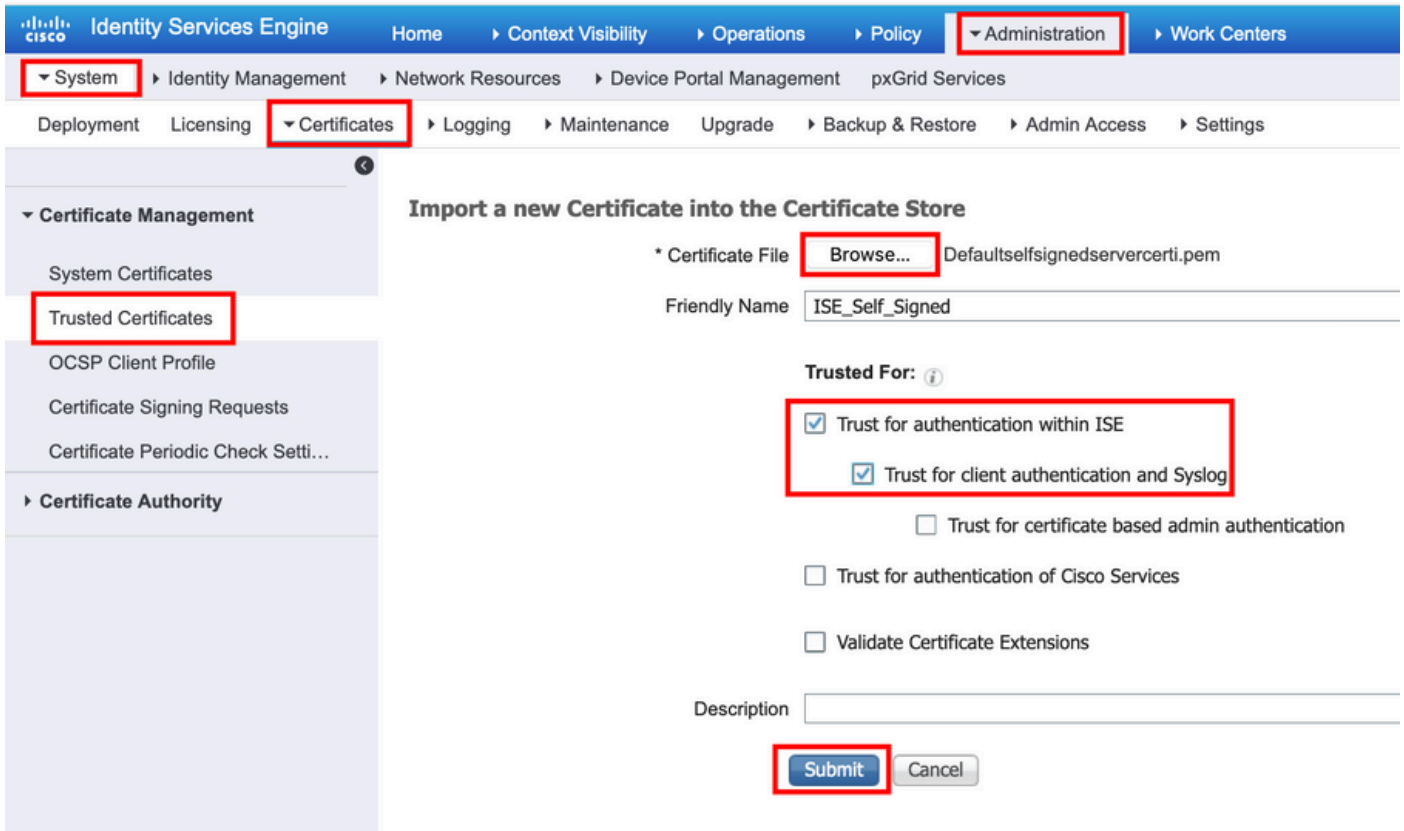
在ISE上匯入證書涉及兩個步驟。

步驟1. 確定證書是自簽名證書還是第三方簽名證書。

- 如果證書是自簽名的，則在受信任的證書下匯入證書的公鑰。
- 如果證書是由某個第三方證書頒發機構簽名的，請匯入根證書以及該證書的所有其他中間證書。

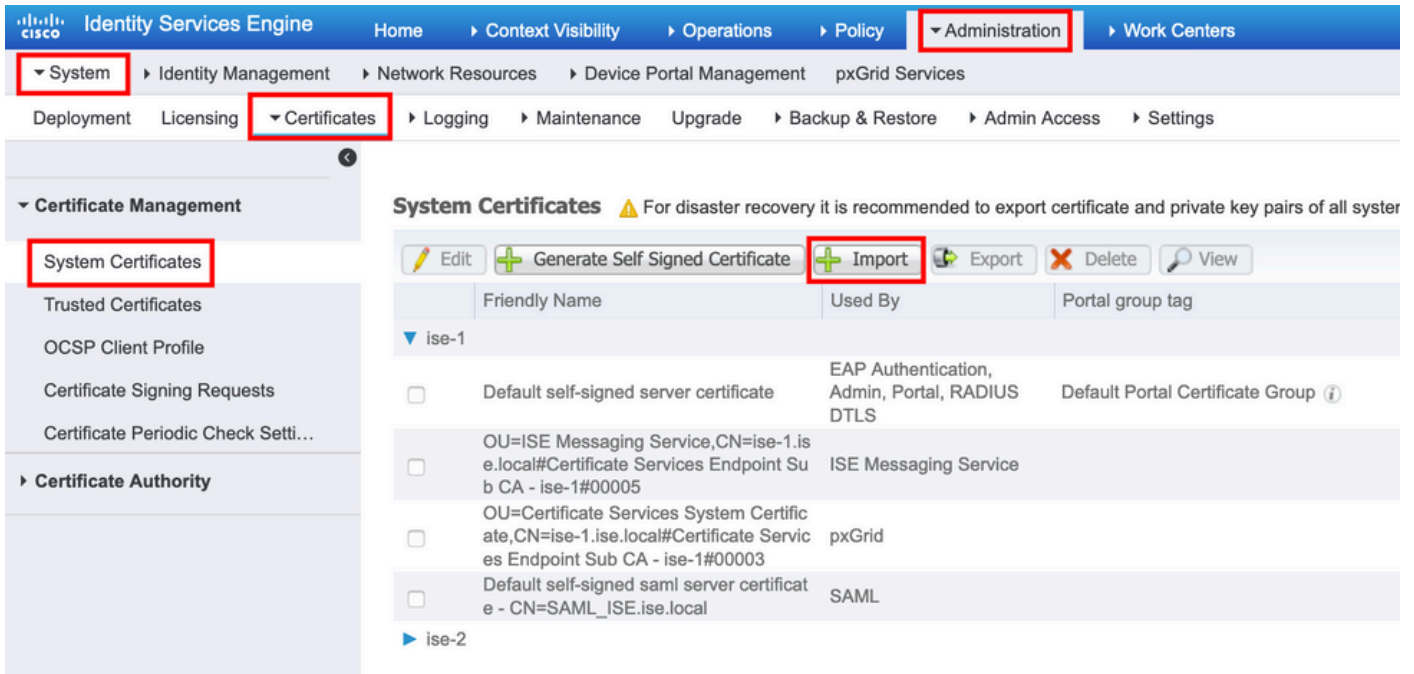
導覽至**Administration > System > Certificates > Certificate Management > Trusted Certificate**，按一下**Import**，如下圖所示。





步驟2. 匯入實際證書。

1. 如本圖所示，導覽至Administration > System > Certificates > Certificate Management，然後單擊Import。如果為證書分配了管理員角色，則節點上的服務將重新啟動。



2. 選擇要為其匯入證書的節點。

3. 瀏覽公鑰和私鑰。

4. 輸入證書私鑰的密碼，並選擇所需的角色。

5.現在按一下Submit，如下圖所示。

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。