在ISE中匯入和匯出證書

目錄

<u>簡介</u> <u>背景資訊</u> <u>在ISE中匯出證書</u> 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:

dentity Services Engine	lome)	Context Visibility	Policy Administration	Work Centers	
System Hentity Management Network Resources Device Portal Management pxGrid Services					
Deployment Licensing ▼Certificates ► Logging ➤ Maintenance Upgrade ➤ Backup & Restore ➤ Admin Access ➤ Settings					
0					
Certificate Management System Certificates ▲ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.					
System Certificates	📝 Edit	Generate Self Signed Certificate	Import 🕃 Export 🗙	Delete View	
Trusted Certificates		Friendly Name	Used By	Portal group tag	Issued To
OCSP Client Profile	▼ ise-1				
Certificate Signing Requests		Default self-signed server certificate	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group 👔	ise-1.ise.local
Certificate Periodic Check Setti		OU=ISE Messaging Service,CN=ise-1.ise.l ocal#Certificate Services Endpoint Sub CA - ise-1#00005	ISE Messaging Service		ise-1.ise.local
Certificate Authority Certificate Authority Certificates		OU=Certificate Services System Certificat e,CN=ise-1.ise.local#Certificate Services E ndpoint Sub CA - ise-1#00003	pxGrid		ise-1.ise.local
Internal CA Settings		Default self-signed saml server certificate - CN=SAML_ISE.ise.local	SAML		SAML_ISE.ise.local
Certificate Templates	► 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。

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.			
	Export Cancel		

提示:不要忘記密碼。

在ISE中匯入證書

0

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。

dentity Services Engine	Home → Context Visibility → Opera	ations > Policy - Administra	tion Vork Centers
System Identity Management Network Resources Device Portal Management pxGrid Services			
Deployment Licensing - Certificates	► Logging ► Maintenance Upgrad	de Backup & Restore Admin	n Access
0			
✓ Certificate Management	Trusted Certificates		
System Certificates	/ Edit 🕂 Import 🚯 Export 🗙 Dele	ete 🔎 View	
Trusted Certificates	Friendly Name	▲ Status	Trusted For Ser
OCSP Client Profile	Baltimore CyberTrust Root	Enabled	Cisco Services 02
Certificate Signing Requests	Cisco ECC Root CA 2099	Enabled	Cisco Services 03
Certificate Signing Requests	Cisco Licensing Root CA	Enabled	Cisco Services 01
Certificate Periodic Check Setti	Cisco Manufacturing CA SHA2	Enabled	Infrastructure 02 Endpoints
Certificate Authority	Cisco Root CA 2048	Ø Disabled	Endpoints 5F Infrastructure
	Cisco Root CA 2099	Enabled	Cisco Services 01
	Cisco Root CA M1	Enabled	Cisco Services 2E

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
✓ System → Identity Management	Network Resources Device Portal Management pxGrid Services
Deployment Licensing - Certificate	es
0	
- Certificate Management	Import a new Certificate into the Certificate Store
System Certificates	* Certificate File Browse Defaultselfsignedservercerti.pem
Trusted Certificates	Friendly Name ISE_Self_Signed
OCSP Client Profile	Trusted For: (i)
Certificate Signing Requests	✓ Trust for authentication within ISE
Certificate Periodic Check Setti	Trust for client authentication and Syslog
Certificate Authority	Trust for certificate based admin authentication
	Trust for authentication of Cisco Services
	Validate Certificate Extensions
	Description
	Submit

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。

dentity Services Engine	lome	 Context Visibility 	 Operations 	▶ Policy	- Administration	Work Centers
▼System → Identity Management → M	Network Re	sources	Portal Management	pxGrid Ser	vices	
Deployment Licensing - Certificates	▸ Loggi	ng Maintenance	Upgrade Ba	ckup & Restor	e I Admin Ac	cess > Settings
0						
- Certificate Management	System	Certificates 🔥 F	or disaster recover	γ it is recomme	anded to export co	ertificate and private key pairs of all syster
System Certificates	📝 Edit	Generate Self	Signed Certificate	🕂 Import	Export	Colete Delete View
Trusted Certificates		Friendly Name		Used By		Portal group tag
OCSP Client Profile	▼ ise-1					
Certificate Signing Requests		Default self-signed se	erver certificate	EAP Auther Admin, Port DTLS	ntication, al, RADIUS	Default Portal Certificate Group (j)
Certificate Periodic Check Setti		OU=ISE Messaging Service,CN=ise-1.is e.local#Certificate Services Endpoint Su b CA - ise-1#00005 OU=Certificate Services System Certific ate,CN=ise-1.ise.local#Certificate Servic es Endpoint Sub CA - ise-1#00003		ISE Messaging Service		
Certificate Authority						
		Default self-signed s e - CN=SAML_ISE.is	aml server certificat se.local	SAML		
	► ise-2					

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。

uluilu Identity Services Engine Home → Context Visibility →	Operations Policy Administration Work Centers			
System Identity Management Network Resources Device Portage	al Management pxGrid Services			
Deployment Licensing Certificates Logging Maintenance U	Jpgrade Backup & Restore Admin Access Settings			
0				
Certificate Management Import Server Certificate				
System Certificates * Select Node	a ise-1			
Trusted Certificates				
OCSP Client Profile * Certificate File	Browse Defaultselfsignedservercerti.pem			
Certificate Signing Requests * Private Key File	Browse Defaultselfsignedservercerti.pvk			
Certificate Periodic Check Setti				
► Certificate Authority Password				
Friendly Name	ISE_Self_Signed			
Allow Wildcard Certificates				
Validate Certificate Extensions				
Usage	і			
	Admin: Use certificate to authenticate the ISE Admin Portal Admin: Use certificate to authenticate for EAP protocols that use SSL/TLS tuppeling			
Colort Descripted	RADIUS DTLS: Use certificate for the RADSec server			
Select Required	pxGrid: Use certificate for the pxGrid Controller			
Role	SAML: Use certificate for SAML Signing			
	Portal: Use for portal			
	Submit Cancel			

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)。