TMS WebEx SSO憑證續訂 — 思科

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>背景資訊</u> <u>在TMS上傳續訂證書的程式</u> <u>匯入證書</u> <u>匯出證書並將其上傳到TMS</u> <u>疑難排解</u> 相關資訊

簡介

本文檔介紹當TMS處於使用SSO的Webex混合配置中時,在TMS上續訂Webex SSO證書的過程。

必要條件

需求

思科建議您瞭解以下主題:

- TMS(Cisco TelePresence Management Suite)
- Webex SSO(單一登入)
- •思科協同合作會議室(CMR)混合組態

採用元件

本文中的資訊係根據以下軟體和硬體版本:

• TMS 15.0及更高版本

本檔案中的資訊是根據<u>思科協同合作會議室(CMR)混合組態設定指南(TMS 15.0 - WebEx會議中心</u> WBS30)。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

本文所介紹的情況是,通過按一下「續訂」按鈕,已通過CA Web門戶續訂了證書。本文檔中不包 括生成新CSR(證書簽名請求)的過程。 請確保您有權訪問生成原始CSR的同一Windows服務器。如果無法訪問特定Windows伺服器,則必 須根據配置指南生成新證書。

在TMS上傳續訂證書的程式

匯入證書

若要在已產生原始CSR的相同Windows伺服器上匯入續訂憑證,請執行以下步驟。

步驟1。導覽至**開始>運行> mmc**。按一下File > Add Snap-in > Local Computer(可以使用當前使 用者)。

步驟2.按一下Action > Import,然後選擇續訂的憑證。選擇Certificate Store:個人(如果需要,請選 擇其他)。

步驟3.匯入證書後,按一下右鍵證書並開啟證書。

如果根據同一伺服器的私鑰更新了證書,則證書應顯示:「您有與此憑證對應的私密金鑰」,如下例所示:

	Certificate	x		
General Details Certification Path				
	Certificate Information			
	This certificate is intended for the following purpose(s): • Ensures the identity of a remote computer			
	Issued to: TMS15.learning.com			
	Issued by: learningext-EXTDNS-CA			
Valid from 9/5/2016 to 9/5/2018 You have a private key that corresponds to this certificate.				
	Issuer Statement			
	ОК			

匯出證書並將其上傳到TMS

若要匯出續訂的憑證及其私鑰,請執行以下步驟。

步驟1.使用Windows Certificate Manager管理單元,將現有私鑰(證書對)匯出為PKCS#12文件:

📀 🌛 Certificate Export Wizard
Export Private Key You can choose to export the private key with the certificate.
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.
Do you want to export the private key with the certificate?
 Yes, export the private key
O No, do not export the private key
Next Cancel

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

- DER encoded binary X.509 (.CER)
- Base-64 encoded X.509 (.CER)
- Cryptographic Message Syntax Standard PKCS #7 Certificates (.P7B)

Include all certificates in the certification path if possible

Personal Information Exchange - PKCS #12 (.PFX)

✓ Include all certificates in the certification path if possible

Delete the private key if the export is successful

Export all extended properties

Microsoft Serialized Certificate Store (.SST)

Next Cancel

) 🍠 Certificate Export Wiza	ard
To maintain security, you mu using a password.	ust protect the private key to a security principal or by
Group or user names (rec	commended)
	Add
	Remove
Password:	
Confirm password:	
•••••	
	Next Cancel

步驟2.使用Windows證書管理器管理單元,將現有證書匯出為Base64 PEM編碼的.CER檔案。確保 副檔名為.cer或.crt,並將此檔案提供給WebEx雲服務團隊。

步驟3.登入到Cisco TMS,然後導航到**管理工具>配置> WebEx設定**。在WebEx站點窗格中,驗證 所有設定,包括SSO。

步驟4.按一下Browse並上傳PKS #12私鑰證書(.pfx),該證書是在Generating a Certificate for WebEx中生成的。使用您在生成證書時選擇的密碼和其他資訊填寫其餘的SSO配置欄位。按一下「 Save」。

如果私鑰以獨佔方式可用,則可以使用以下OpenSSL命令將.pem格式的簽名證書與私鑰合併:

openssl pkcs12 -export -inkey tms-privatekey.pem -in tms-cert.pem -out tms-cert-key.p12 -name tms-cert-key

您現在應該有一個Cisco TMS證書,其中包含要上傳到Cisco TMS的SSO配置的私鑰金鑰。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

• <u>思科合作會議室(CMR)混合配置指南(TMS 15.0 - WebEx會議中心WBS30)</u>