將Secure Web Appliance還原為先前版本

目錄

簡介

本文檔介紹將Secure Web Appliance(SWA)恢復為先前版本的步驟。

必要條件

需求

思科建議瞭解以下主題：

- 訪問SWA的圖形使用者介面(GUI)

- 對SWA的管理訪問
- 訪問思科軟體許可門戶或SWA許可證檔案
- Active Directory具有將SWA加入域和建立DNS記錄的特權使用者訪問許可權

採用元件

本文件所述內容不限於特定軟體和硬體版本。

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。

開始之前

恢復裝置具有極大的破壞性。
Thia是在過程中銷毀的資料，必須備份：
— 當前系統配置檔案。
— 所有日誌檔案(有關詳細資訊，請訪問：訪問Secure Web裝置日誌)
— 所有報告資料（包括已儲存的計畫和已存檔的報告）
— 任何自定義終端使用者通知頁面。

警告：在還原到早期版本之前，請確保您具有與該特定版本對應的加密配置檔案。當前配置檔案可能與較舊的軟體版本不相容。

準備和備份SWA

在恢復之前，請使用以下步驟從SWA收集必要的檔案和配置：

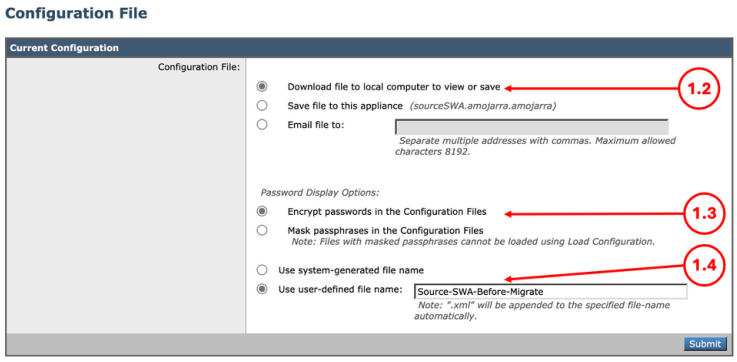
步驟1.匯出配置檔案	步驟1.1.從GUI導航到System Administration並選擇Configuration File。

步驟1.2.確保選中「Download file to local computer to view or save（將檔案下載到本地電腦檢視或儲存）」。

步驟1.3.在組態檔中選擇Encrypt passwords

步驟1.4.（可選）選擇配置檔案的名稱。

步驟1.5.按一下Submit。



映像 — 匯出配置檔案

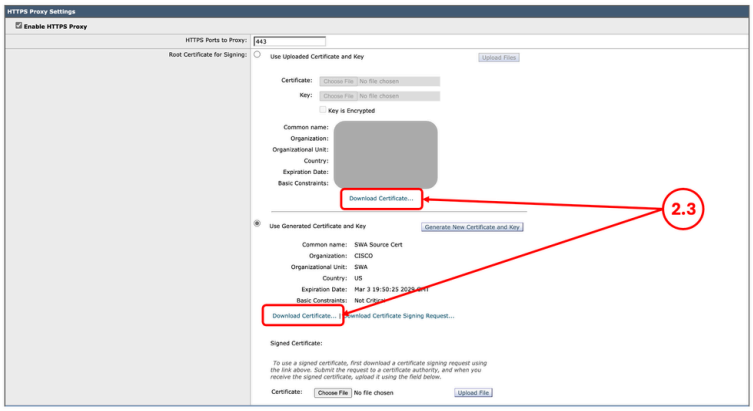
步驟2.匯出解密證書

附註：如果已停用HTTPS解密，請跳至步驟3。

步驟2.1.在GUI中，導覽至Security Services，然後按一下HTTPS Proxy。

步驟2.2.按一下Edit Settings。

步驟2.3.通過按一下Download Certificate...下載HTTPS解密證書 連結。



映像 — HTTPS解密證書

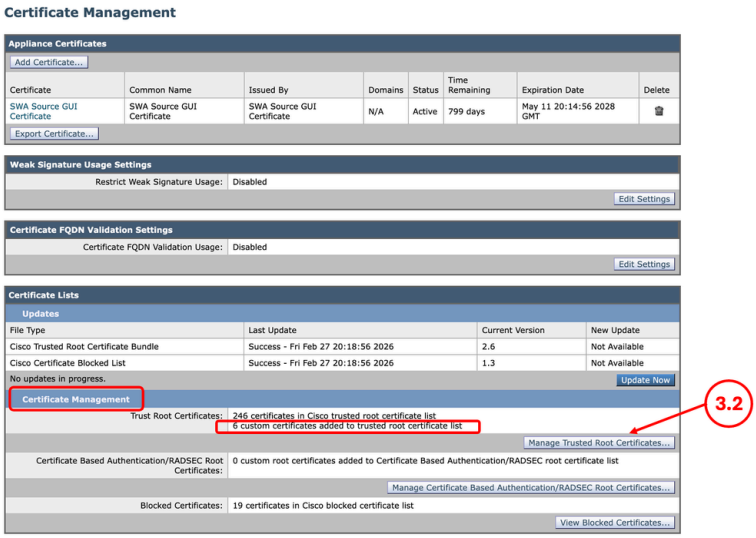
附註：在此範例中，說明兩種型別的HTTPS解密憑證；但是，在您的網路中，只能部署一種型別。

步驟3.匯出自定義信任根證書

附註：如果在SWA上沒有新增自定義受信任的根證書，請跳至步驟4。

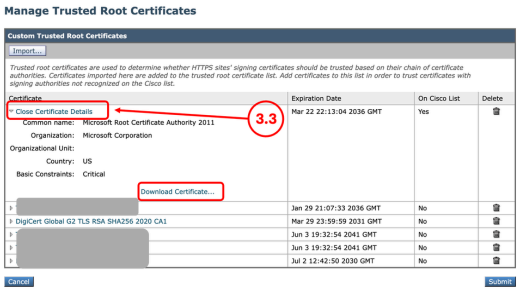
步驟3.1.在GUI中，導覽至Network，然後按一下Certificate Management。

步驟3.2.在Certificate Management部分，點選Manage Trusted Root Certificates。



映像 — 管理受信任的根證書

步驟3.3.按一下每個自定義受信任的根證書，然後按一下下載證書……



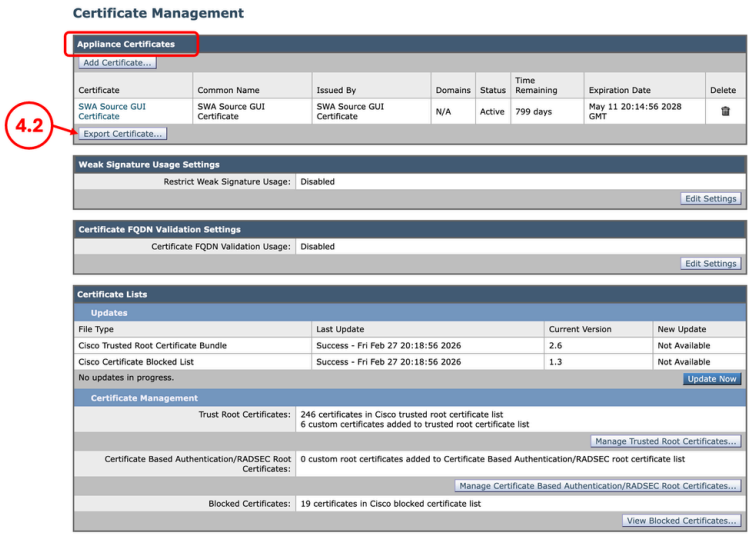
映像 — 下載受信任的根證書

步驟4.匯出GUI證書

附註：如果使用的是內建GUI證書，請跳至步驟5。

步驟4.1.在GUI中導覽至Network，然後按一下Certificate Management。

步驟4.2.在Appliance Certificates部分，點選Export Certificate。

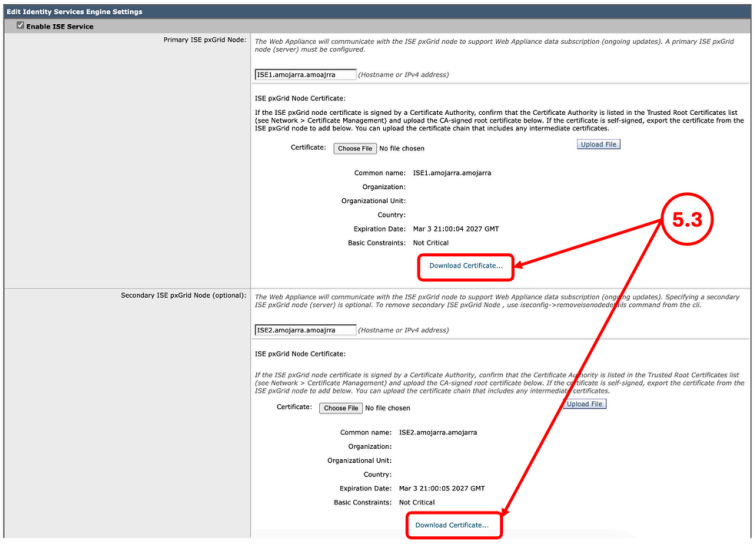
<table>
<tr>
<td></td>
<td> 

映像 — 匯出GUI證書</td>
</tr>
<tr>
<td>步驟5.匯出ISE證書

附註：如果沒有SWA、ISE整合，請跳至步驟6。</td>
<td>步驟5.1.在GUI中，導覽至Network，然後按一下Identity Services Engine。

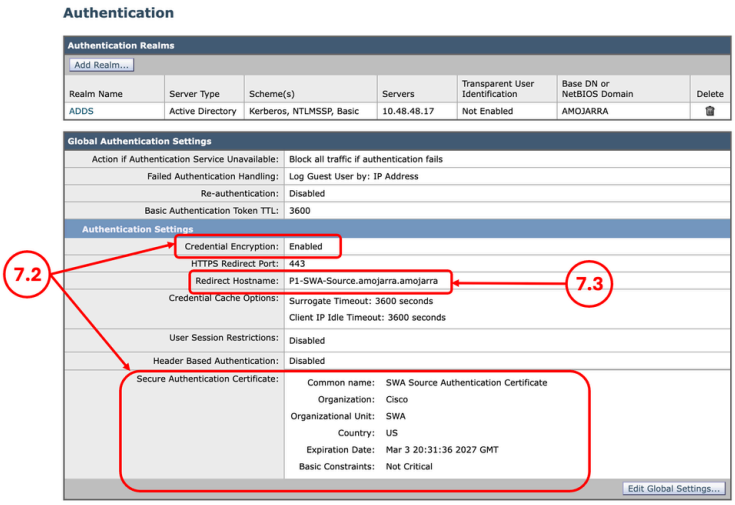
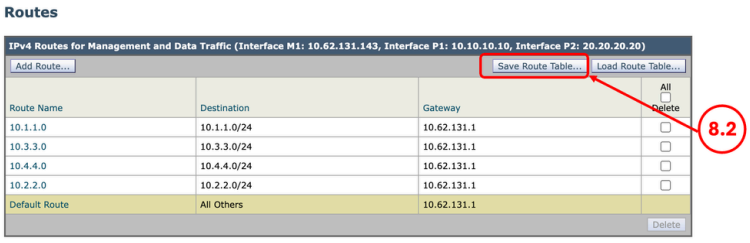
步驟5.2.按一下「Edit Settings」。

步驟5.3.下載所有可用的證書。

映像 — 下載ISE證書</td>
</tr>
<tr>
<td>步驟6.許可證/功能</td>
<td>步驟6.1.在GUI中，導覽至System Administration，然後按一下Licenses或Features，具體取決於您使用的許可證型別。

步驟6.2.擷取許可證/功能的截圖。</td>
</tr>
</table>

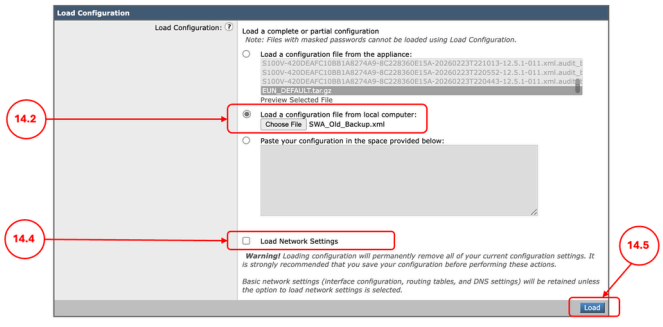
步驟7.驗證重新導向憑證	步驟7.1.在GUI中，導覽至Network，然後按一下Authentication。 步驟7.2.如果Credential Encryption已啟用，請確保您擁有憑證和金鑰。 步驟7.3.獲取當前配置的截圖。  映像 — 身份驗證證書 附註：無法從GUI下載身份驗證證書。
步驟8.匯出靜態路由 附註：如果計畫對目標SWA使用相同的網路配置和IP地址，請跳至步驟10。	步驟8.1.在GUI中導覽至Network，然後按一下Routes。 步驟8.2.對於每個路由表，按一下Save Route Table。  影象 — 匯出路由表
步驟9. DNS設定 附註：如果計畫對目標SWA使用相同的網路配置和IP地址，請跳至步驟10。	步驟9.1.在GUI中，導覽至Network，然後按一下DNS。 步驟9.2.擷取DNS配置的截圖。

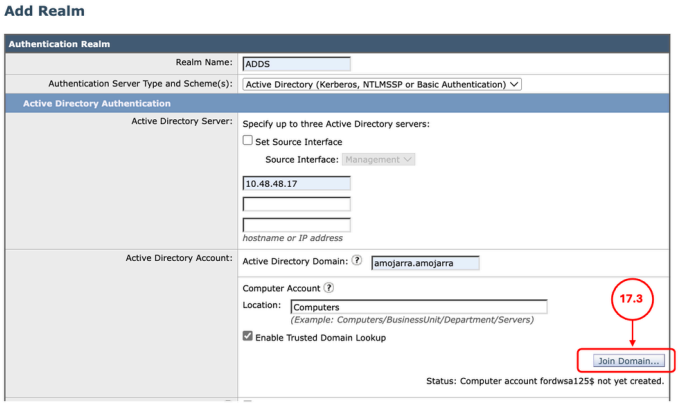
恢復SWA

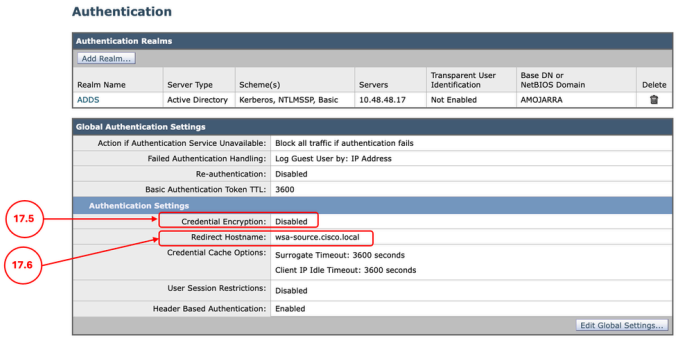
步驟10.恢復SWA	步驟10.1.連線到CLI。 步驟10.2.鍵入revert並按Enter鍵。 步驟10.3.鍵入Y，然後按Enter鍵「是否要繼續？」[N]> " 步驟10.4。鍵入Y，然後按Enter鍵「是否確實要繼續？」[N]>" 步驟10.5.從清單中選擇與要還原的版本相關聯的數字，然後按Enter。 SWA_CLI> revert This command will revert the appliance to a previous version of AsyncOS. Warning: Reverting the appliance is extremely destructive. The following data will be destroyed in the process and should be backed up: - current system configuration file - all log files - all reporting data (including saved scheduled and archived reports) - any custom end user notification pages This command will try to preserve the current network settings. Reverting the device will cause a reboot to take place. After rebooting, the appliance reinitializes itself and reboots again to the desired version, with the earlier system configuration. Do you want to continue? [N]> Y Are you sure you want to continue? [N]> Y Available versions ========== 1. 12.5.1-011 Please select an AsyncOS version: 1 You have selected "12.5.1-011". The system will now reboot to perform the revert operation.

配置已恢復SWA

步驟11.許可SWA	步驟11.1。有關詳細資訊，請訪問：配置安全Web裝置初始設定。
步驟12.運行系統設定嚮導	步驟12.1。有關詳細資訊，請訪問：配置安全Web裝置初始設定。

步驟13.匯入自定義受信任的根證書 附註：如果未使用任何自定義受信任的根證書，請跳至步驟14。	步驟13.1。在GUI中，導覽至Network，然後按一下Certificate Management。 步驟13.2.在Certificate Management部分，點選Manage Trusted Root Certificates。 步驟13.3.單擊Import。 步驟13.4.上傳先前在步驟3中下載的憑證。 注意：如果根證書和中間證書都可用，則首先上傳根CA證書。提交並提交更改後，繼續匯入中間證書。
步驟14.匯入配置檔案 注意：確保正在匯入與當前版本對應的配置檔案，而不是在步驟1中匯出的配置檔案。	步驟14.1.在GUI中，導覽至System Administration，然後選擇Configuration File。 步驟14.2.在Load Configuration部分，選擇Load a configuration file from local computer。 步驟14.3.單擊Choose File，然後選擇與當前版本相關的XML配置檔案。 步驟14.4。(可選)如果恢復刪除了IP地址和網路配置，請選中Load Network Settings覈取方塊，否則不選擇此選項。 步驟14.5。單擊Load。 步驟14.6.在Confirm Load Configuration快出視窗中單擊Continue。  映像 — 載入舊配置檔案 步驟14.7.提交更改。
步驟15.匯入路由	步驟15.1.在GUI中，導覽至Network，然後按一

注意：如果在導入配置時載入網路設定，請跳至步驟17。	下Routes。 步驟15.2.按一下每個路由表的載入路由表。 步驟15.3.選擇您在第8步中匯出的檔案。 步驟15.4.按一下Submit。 步驟15.5.提交更改。
步驟16.配置DNS設定 附註：如果在匯入配置時載入Network Settings，請跳至步驟17。	步驟16.1.在GUI中導覽至Network，然後按一下DNS。 步驟16.2。單擊Edit Settings。 步驟16.3.使用步驟9中的截圖 步驟16.4.單擊提交。 步驟16.5.提交更改。
步驟17.將SWA加入/重新加入Active Directory	步驟17.1.在GUI中導覽至Network ，然後按一下Authentication。 步驟17.2。按一下身份驗證領域名稱的名稱。 提示：如果為SWA分配了新的IP地址和主機名，請確保在Active Directory DNS服務中建立必要的DNS記錄。 步驟17.3.單擊Join Domain並輸入憑據：  影象 — 加入Active Directory 步驟17.4.單擊提交。 步驟17.5.如果啟用憑證加密，請匯入安全驗證憑

	證。 步驟17.6.確保重定向主機名正確。  影象 — 身份驗證設定 步驟17.7.提交更改。

相關資訊

- Cisco Secure Web Appliance AsyncOS 15.2使用手冊
- 安全Web裝置初始設定
- 使用安全Web裝置最佳做法
- 訪問安全Web裝置日誌

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）。