将安全Web设备恢复为早期版本

目录

简介

本文档介绍将安全Web设备(SWA)恢复为先前版本的步骤。

先决条件

要求

建议掌握下列主题的相关知识：

- 访问SWA的图形用户界面(GUI)

- 对SWA的管理访问
- 访问思科软件许可门户或SWA许可证文件
- Active Directory具有将SWA加入域和创建DNS记录的特权用户访问权限

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

开始使用前

恢复设备具有极大的破坏性。
此数据是在过程中被销毁且必须备份的数据：
— 当前系统配置文件。
— 所有日志文件(有关详细信息，请访问：访问安全Web设备日志)
— 所有报告数据（包括已保存的计划和已存档的报告）
— 任何自定义最终用户通知页面。

警告：在恢复为早期版本之前，请确保您具有与该特定版本对应的加密配置文件。当前配置文件可能与较旧的软件版本不兼容。

准备和备份SWA

在恢复之前，请使用以下步骤从SWA收集必要的文件和配置：

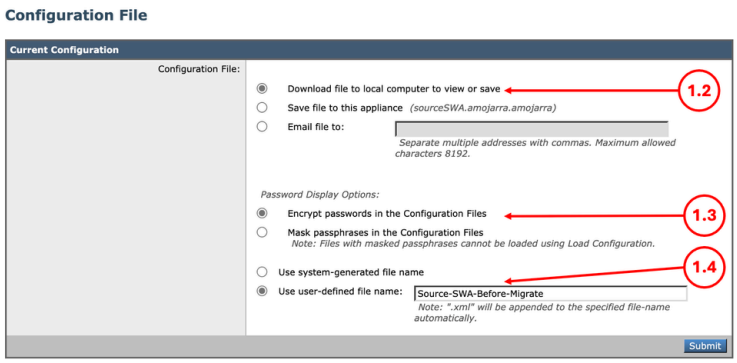
步骤1.导出配置文件	第1.1步：从GUI中，导航到System Administration并选择Configuration File。

第1.2步：确保已选择将文件下载到本地计算机以查看或保存。

步骤1.3.在配置文件中选择Encrypt password

第1.4步(可选)选择配置文件的名称。

第1.5步。单击提交。



映像 — 导出配置文件

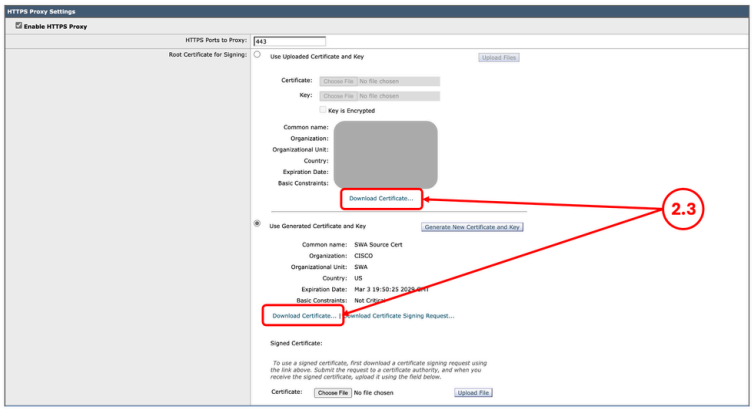
步骤2.导出解密证书

注意：如果HTTPS解密已禁用，请跳至步骤3。

第2.1步：在GUI中，导航到Security Services并点击HTTPS Proxy。

第2.2步。单击编辑设置。

第2.3步：通过点击Download Certificate...下载HTTPS解密证书 链接。



映像 — HTTPS解密证书

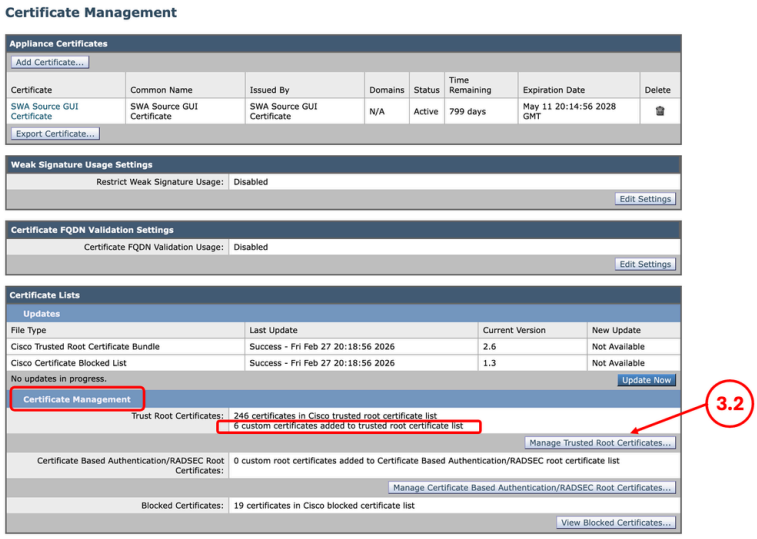
注意：在本例中，显示了两种类型的HTTPS解密证书；但是，在您的网络中，只能部署一种类型。

步骤3.导出自定义信任根证书

注意：如果SWA上没有添加自定义受信任根证书，请跳至步骤4。

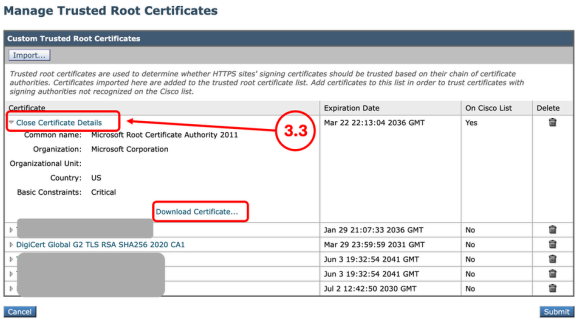
第3.1步：从GUI中，导航到Network，然后点击Certificate Management。

第3.2步：在Certificate Management部分，点击Manage Trusted Root Certificates。



映像 — 管理受信任的根证书

第3.3步：通过点击每个自定义受信任根证书(Custom Trusted Root Certificates)的名称并点击Download Certificate..



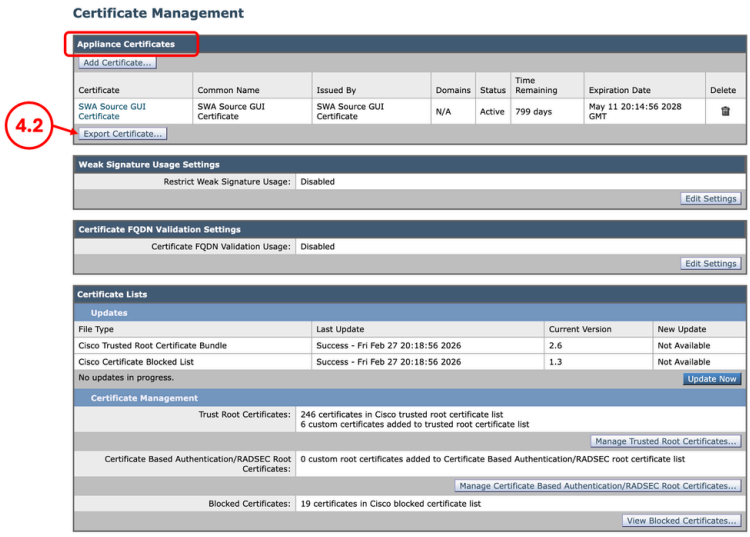
映像 — 下载受信任的根证书

步骤4.导出GUI证书

注意：如果使用的是内置GUI证书，请跳至步骤5。

第4.1步：从GUI中，导航到Network，然后点击Certificate Management。

第4.2步：在Appliance Certificates部分，点击Export Certificate。



映像 — 导出GUI证书

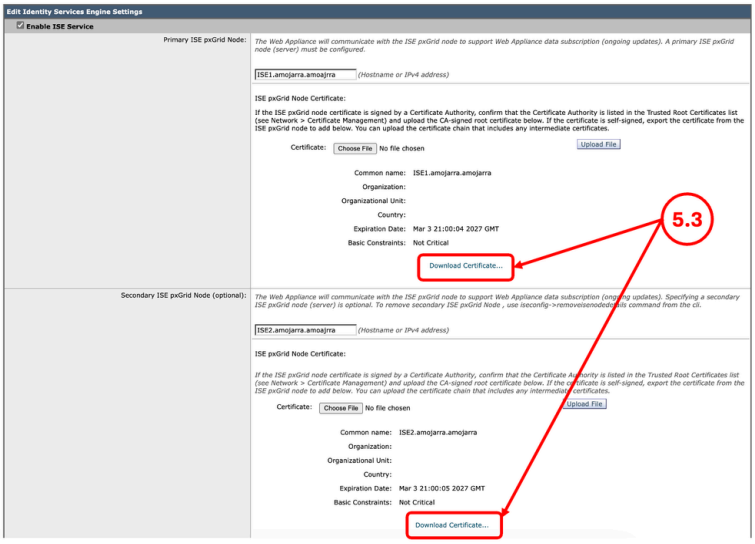
步骤5.导出ISE证书

注意：如果没有SWA、ISE集成，请跳至步骤6。

第5.1步：从GUI中，导航到网络，然后点击Identity Services Engine。

第5.2步。单击Edit Settings。

第5.3步：下载所有可用的证书。



映像 — 下载ISE证书

步骤6.许可证/功能

第6.1步：在GUI中，导航到系统管理，然后点击许可证或功能，具体取决于您使用的许可证类型。

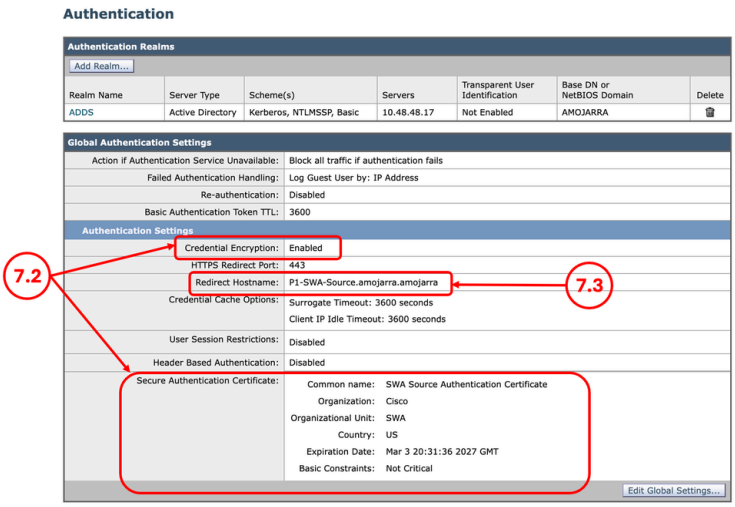
第6.2步：截取许可证/功能的截图。

步骤7.身份验证重定向证书

第7.1步：从GUI中，导航到Network，然后点击Authentication。

第7.2步：如果启用了Credential Encryption，请确保您拥有证书和密钥。

步骤7.3.截取当前配置的截图。



图像 — 身份验证证书

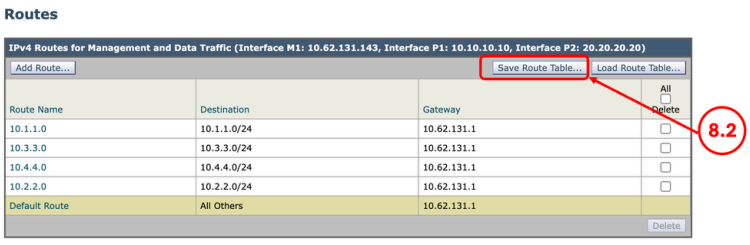
注意：无法从GUI下载身份验证证书。

步骤8.导出静态路由

注意：如果计划对目标SWA使用相同的网络配置和IP地址，请跳至步骤10。

第8.1步：在GUI中，导航到Network，然后点击Routes。

第8.2步：对于每个路由表，点击保存路由表。



图像 — 导出路由表

步骤9. DNS设置

注意：如果计划对目标SWA使用相同的网络配置和IP地址，请跳至步骤10。

第9.1步：在GUI中，导航到网络，然后点击DNS。

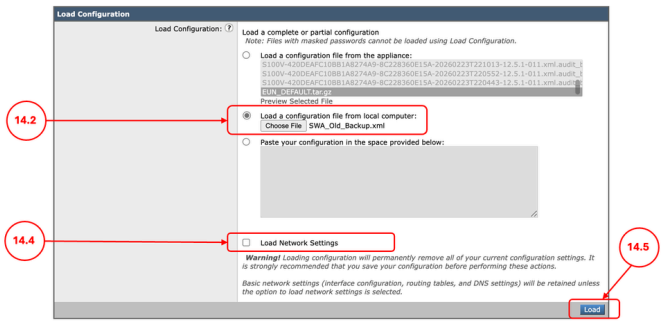
步骤9.2.截取DNS配置的截图。

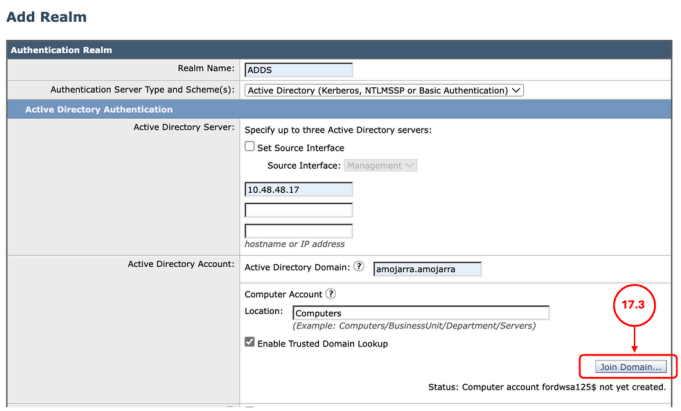
恢复SWA

步骤10.恢复SWA	步骤10.1.连接到CLI。 步骤10.2.键入revert，然后按Enter。 第10.3步。键入Y，然后按Enter键“是否要继续？”[N]> " 第10.4步。键入Y，然后按Enter键“是否确实要继续？”[N]>" 第10.5步。从列表中选择与要还原的版本相关联的Number，然后按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.

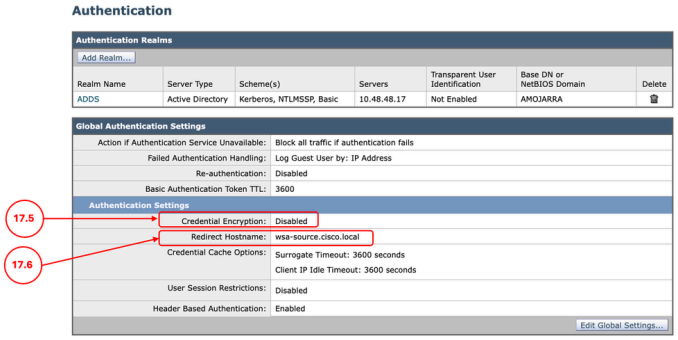
配置恢复的SWA

步骤11.许可SWA	第11.1步。有关详细信息，请访问：配置安全Web设备初始设置。
步骤12.运行系统设置向导	第12.1步。有关详细信息，请访问：配置安全Web设备初始设置。
步骤13.导入自定义受信任根证书	第13.1步：从GUI中，导航到Network，然后点击Certificate Management。

注意：如果未使用任何自定义受信任根证书，请跳至步骤14。	第13.2步：在Certificate Management部分，点击Manage Trusted Root Certificates。 步骤13.3.单击导入。 步骤13.4.上传之前在步骤3中下载的证书。 警告：当根证书和中间证书都可用时，首先上传根CA证书。提交并提交更改后，继续导入中间证书。
步骤14.导入配置文件 警告：确保导入的是与当前版本对应的配置文件，而不是在步骤1中导出的配置文件。	第14.1步：从GUI中，导航到System Administration并选择Configuration File。 步骤14.2.在Load Configuration部分，选择Load a configuration file from local computer。 第14.3步。点击选择文件，然后选择与当前版本相关的XML配置文件。 第14.4步(可选)如果恢复删除了IP地址和网络配置，请选中Load Network Settings复选框，否则不要选择此选项。 步骤14.5.单击加载。 步骤14.6.在Confirm Load Configuration弹出中点击Continue。  映像 — 加载旧配置文件 步骤14.7.提交更改。
步骤15.导入路由 注意：如果导入配置时加载网络设置，请跳	第15.1步：在GUI中，导航到Network，然后点击Routes。 步骤15.2.对于每个路由表，单击Load Route

至步骤17。	Table。 第15.3步。选择您在第8步中导出的文件。 步骤15.4.点击提交。 步骤15.5.提交更改。
步骤16.配置DNS设置 注意：如果在导入配置时加载Network Settings，请跳至步骤17。	第16.1步：在GUI中，导航到Network，然后单击DNS。 步骤16.2.单击Edit Settings。 步骤16.3.使用步骤9中的截图 第16.4步。单击提交。 步骤16.5.提交更改。
步骤17.将SWA加入/重新加入Active Directory	第17.1步：从GUI中，导航到Network，然后单击Authentication。 步骤17.2.点击身份验证领域名称的名称。 提示：如果为SWA分配了新的IP地址和主机名，请确保在Active Directory DNS服务中创建必要的DNS记录。 第17.3步：点击加入域并输入凭证：  图像 — 加入到Active Directory 第17.4步。单击提交。 步骤17.5.如果启用凭证加密，请导入安全身份验证证书。

步骤17.6.确保重定向主机名正确。



图像 — 身份验证设置

步骤17.7.提交更改。

相关信息

- 思科安全Web设备AsyncOS 15.2用户指南
- 安全Web设备初始设置
- 使用安全Web设备最佳实践
- 访问安全Web设备日志

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）。