Revert Secure Web Appliance to Previous Version

Contents

Introduction

This document describes the steps to revert the Secure Web Appliance (SWA) to previous version.

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- Access ToGraphic User Interface (GUI)of SWA

- Administrative Access to the SWA
- Access to Cisco Software Licensing Portal or the SWA license file
- Active Directory privileged user access to join the SWA to domain and create DNS records

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Before You Begin

Reverting the appliance is extremely destructive.
Thia iis the data that is destroyed in the process and must be backed up:
- Current system configuration file.
- All log files (For more information visit: Access Secure Web Appliance Logs)
- All reporting data (including saved scheduled and archived reports)
- Any custom end user notification pages.

Warning: Before reverting to an earlier version, please ensure you have the encrypted configuration file corresponding to that specific version. It is possible that the current configuration file is not compatible with older software versions.

Preparing and Backing Up the SWA

Use these steps to collect the necessary files and configuration from the SWA before reverting:

Step 1. Export the Configuration File	**Step 1.1.** From the GUI, Navigate to **System Administration** and choose **Configuration File**. **Step 1.2.** Make sure **Download file to local computer to view or save** is selected. **Step 1.3.** Choose **Encrypt passwords in the Configuration Files**

Step 1.4. (Optional) Choose a name for the configuration file.

Step 1.5. Click **Submit**.

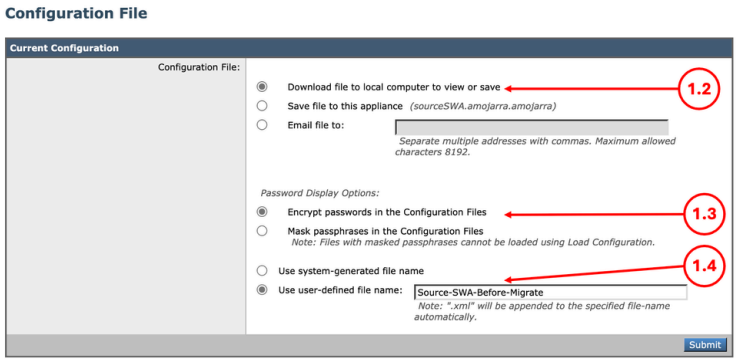


Image - Exporting the configuration File

Step 2. Export the Decryption Certificate

Note: If the HTTPS Decryption is disabled, skip to **Step 3**.

Step 2.1. From the GUI, Navigate to **Security Services** and click **HTTPS Proxy**.

Step 2.2. Click **Edit Settings**.

Step 2.3. Download the HTTPS Decryption Certificate, by clicking **Download Certificate...** link.

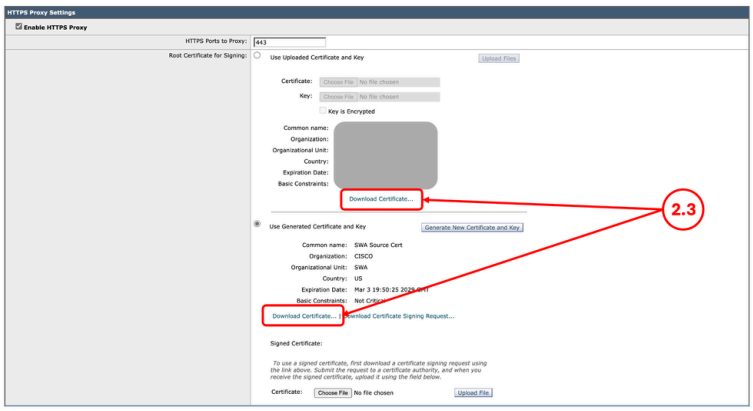


Image - HTTPS Decryption Certificate

Note: In this example, both types of HTTPS Decryption certificates are illustrated; however, in your network, you can have only one type deployed.

Step 3. Export the Custom Trust Root Certificates

Note: If there no custom trusted root certificate added on the SWA skip to **Step 4**.

Step 3.1. From the GUI, navigate to **Network** and click **Certificate Management**.

Step 3.2. In the **Certificate Management** section, click **Manage Trusted Root Certificates**.

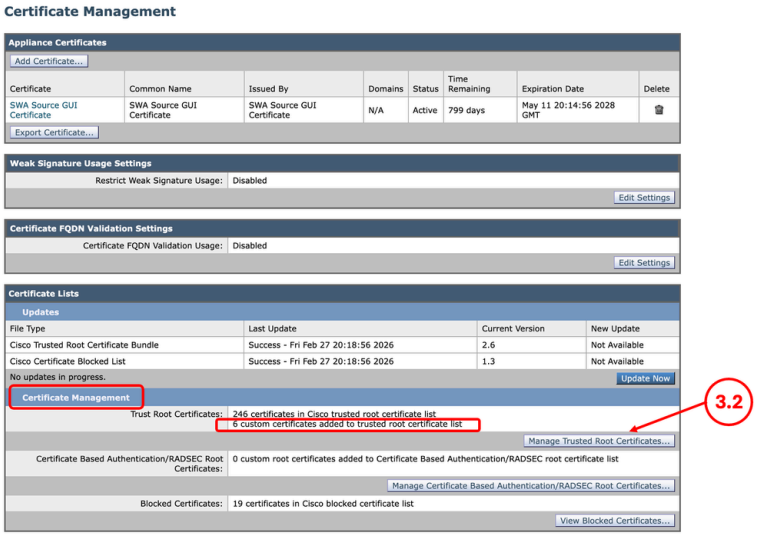


Image - Manage Trusted Root Certificates

Step 3.3. Expand each **Custom Trusted Root Certificates** by clicking their name and click **Download Certificate...**

Image - Downlaod Trusted root Certificates

Step 4. Export the GUI Certificate

Note: If you are using built-in GUI certificate, skip to **Step 5**.

Step 4.1. From the GUI, Navigate to **Network** and click **Certificate Management**.

Step 4.2. In the **Appliance Certificates** section, click **Export Certificate**.

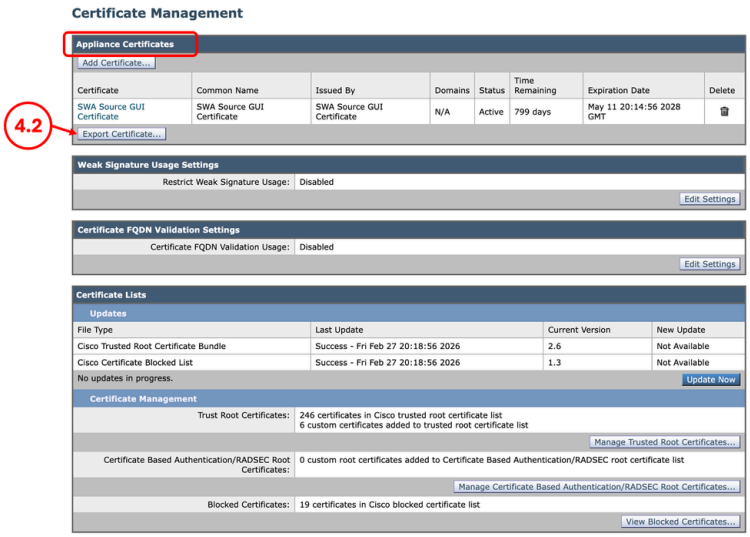


Image - Export GUI Certificate

Step 5. Export the ISE Certificates

Note: If there are no SWA, ISE integration, skip to **Step 6**.

Step 5.1. From the GUI, Navigate to **Network** and click **Identity Services Engine**.

Step 5.2. Click **Edit Settings**.

Step 5.3. Download all available certificates.

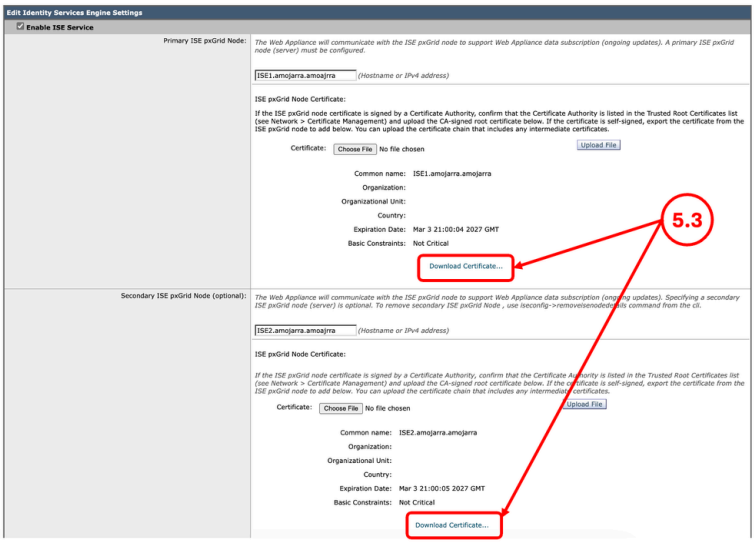


Image - Download ISE Certificates

Step 6. Licences / Features

Step 6.1. From the GUI, Navigate to **System Administration** and click **Licenses** or **Features** depends on the type of the license you are using.

Step 6.2. Take a screenshot of your Licenses / Features.

Step 7. Authentication Redirection Certificate

Step 7.1. From the GUI, Navigate to **Network** and click **Authentication**.

Step 7.2. If the **Credential Encryption** is enabled, Make sure you have the Certificate and the Key.

Step 7.3. Take a screenshot of the current configuration.

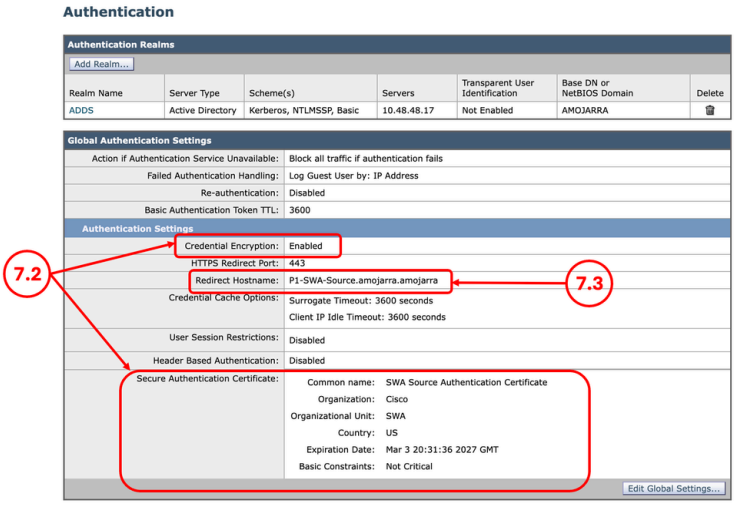
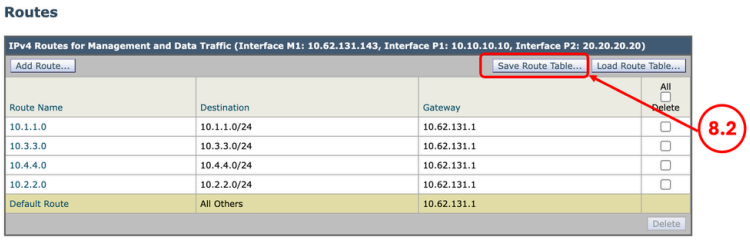


Image - Authentication Certificate

Note: You cannot download the Authentication certificate from the GUI.

Step 8. Export Static Routes **Note**: If you are planning to use the same Network configuration and IP address for the target SWA, skip to **Step 10**.	**Step 8.1.** From the GUI, Navigate to **Network** and click **Routes**. **Step 8.2.** For each routing table, click **Save Route Table**.  *Image - Exporting Routing Table*
Step 9. DNS Settings **Note**: If you are planning to use the same Network configuration and IP address for the target SWA, skip to **Step 10**.	**Step 9.1.** From the GUI, Navigate to **Network** and click **DNS**. **Step 9.2.** Take a screenshot of the DNS configuration.

Revert the SWA

Step 10. Reverting the SWA	**Step 10.1.** Connect to the CLI.
	
	Step 10.2. Type **revert** and press enter.
	
	Step 10.3. Type **Y** and press Enter for "**Do you want to continue? [N]**> "
	
	Step 10.4. Type **Y** and press Enter for "**Are you sure you want to continue? [N]**>"
	
	Step 10.5. Choose the Number associated with the version you want to revert back from the list and press 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.

Configuration Reverted SWA

Step 11. License the SWA	**Step 11.1.** For more information visit: Configure Secure Web Appliance Initial Setup.
Step 12. Run the System Setup Wizard	**Step 12.1.** For more information visit: Configure Secure Web Appliance Initial Setup.
Step 13. Import Custom Trusted Root Certificates **Note**: If you are not using any Custom Trusted Root Certificate, skip to **Step 14**.	**Step 13.1.** From the GUI, Navigate to **Network** and click **Certificate Management**. **Step 13.2.** In the **Certificate Management** section, click **Manage Trusted Root Certificates**. **Step 13.3.** Click **Import**. **Step 13.4.** Upload the certificates that previously was downloaded in **Step 3**. **Caution**: When both root and intermediate certificates are available, begin by uploading the root CA certificate. After submitting and committing the changes, proceed to import the intermediate certificate.
Step 14. Import the Configuration File **Caution**: Make sure you are importing the configuration file corresponding to your current version and **not** the configuration file you exported on **Step 1**.	**Step 14.1.** From the GUI, Navigate to **System Administration** and choose **Configuration File**. **Step 14.2.** In the **Load Configuration** section, Select **Load a configuration file from local computer**. **Step 14.3.** Click **Choose File** and select the XML configuration file related to the current version. **Step 14.4.** (Optional) If the revert removed the IP address and network configuration ,Select the check box **Load Network Settings**, else do not select this option.

Step 14.5. Click **Load**.

Step 14.6. Click **Continue** in the **Confirm Load Configuration** pop up.

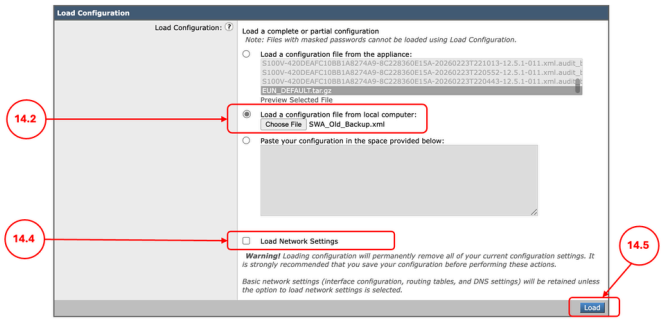


Image - Load the Old Configuration File

Step 14.7. Commit the changes.

Step 15. Import the Routes

Note: If you **Load Network Settings** while importing the configuration, skip to **Step 17**.

Step 15.1. From the GUI, Navigate to **Network** and click **Routes**.

Step 15.2. For each routing table, click **Load Route Table**.

Step 15.3. Choose the file you exported on **Step 8**.

Step 15.4. Click **Submit**.

Step 15.5. Commit the changes.

Step 16. Configure the DNS Settings

Note: If you **Load Network Settings** while importing the configuration, skip to **Step 17**.

Step 16.1. From the GUI, Navigate to **Network** and click **DNS**.

Step 16.2. Click **Edit Settings**.

Step 16.3. Use the screenshot from **Step 9**

Step 16.4. Click **Submit**.

Step 16.5. Commit the changes.

Step 17. Join/Rejoin the SWA to the Active Directory

Step 17.1. From the GUI, Navigate to **Network** and click **Authentication**.

Step 17.2. Click the name of the Authentication **Realm Name**.

Tip: If the SWA is assigned a new IP address and host-name, ensure that the necessary DNS records are created in the Active Directory

DNS service.

Step 17.3. Click **Join Domain** and enter the credentials:

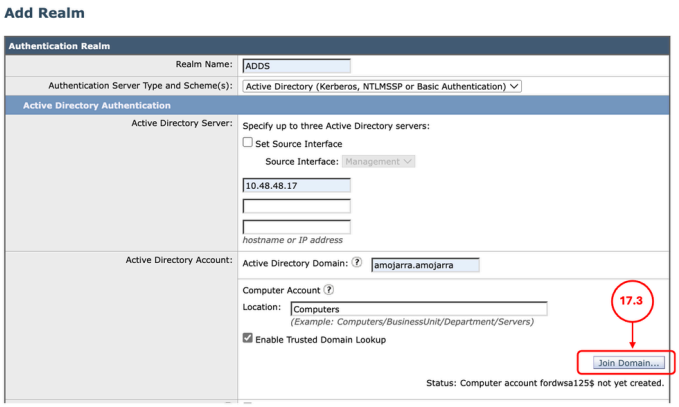


Image - Join to Active Directory

Step 17.4. Click **Submit**.

Step 17.5. If the **Credential Encryption** is enabled, Import the **Secure Authentication Certificate**.

Step 17.6. Make sure the **Redirect Hostname** is correct.

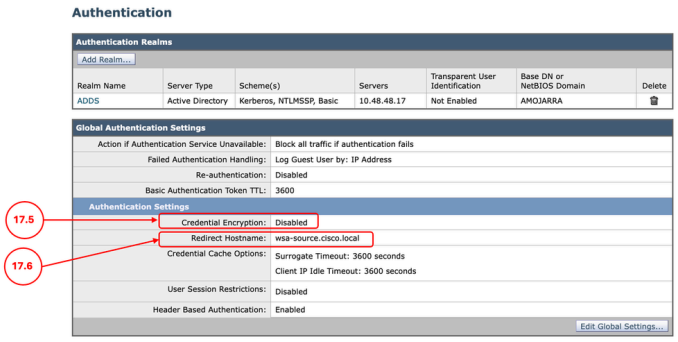


Image - Authentication Settings

Step 17.7. Commit the changes.

Related Information

- User Guide for AsyncOS 15.2 for Cisco Secure Web Appliance
- Secure Web Appliance Initial Setup

- Use Secure Web Appliance Best Practices
- Access Secure Web Appliance Logs