

# Revert Secure Web Appliance to Previous Version

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Before You Begin](#)

### [Preparing and Backing Up the SWA](#)

[Step 1. Export the Configuration File](#)

[Step 2. Export the Decryption Certificate](#)

[Step 3. Export the Custom Trust Root Certificates](#)

[Step 4. Export the GUI Certificate](#)

[Step 5. Export the ISE Certificates](#)

[Step 6. Licences / Features](#)

[Step 7. Authentication Redirection Certificate](#)

[Step 8. Export Static Routes](#)

[Step 9. DNS Settings](#)

### [Revert the SWA](#)

[Step 10. Reverting the SWA](#)

### [Configuration Reverted SWA](#)

[Step 11. License the SWA](#)

[Step 12. Run the System Setup Wizard](#)

[Step 13. Import Custom Trusted Root Certificates](#)

[Step 14. Import the Configuration File](#)

[Step 15. Import the Routes](#)

[Step 16. Configure the DNS Settings](#)

[Step 17. Join/Rejoin the SWA to the Active Directory](#)

### [Related Information](#)

---

## 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.

This is 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:

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

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

**Step 1.5.** Click **Submit**.

#### Configuration File

Current Configuration

Configuration File:

Download file to local computer to view or save **1.2**

Save file to this appliance: (sourceSWA.amojarra.amojarra)

Email file to:   
Separate multiple addresses with commas. Maximum allowed characters 8192.

Password Display Options:

Encrypt passwords in the Configuration Files **1.3**

Mask passphrases in the Configuration Files  
Note: Files with masked passphrases cannot be loaded using Load Configuration.

Use system-generated file name

Use user-defined file name:  **1.4**  
Note: ".xml" will be appended to the specified file-name automatically.

Image - Exporting the configuration File

**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.

HTTPS Proxy Settings

Enable HTTPS Proxy

HTTPS Proxy to Proxy: [413]

Root Certificate for Signing:

Certificate:

Key:

Key is Encrypted

Common name:

Organization:

Organizational Unit:

Country:

Expiration Date:

Basic Constraints:

Use Generated Certificate and Key

Common name: SWA Source Cert

Organization: CISCO

Organizational Unit: SWA

Country: US

Expiration Date: Mar 2 19:50:23 2025 GMT

Basic Constraints: Not Critical

**2.3**

Signed Certificate:

To use a signed certificate, first download a certificate signing request using the link above. Submit the request to a certificate authority, and when you receive the signed certificate, upload it using the field below.

Certificate:

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 2. Export the Decryption Certificate

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

## 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**.

### Certificate Management

**Appliance Certificates**

Certificate	Common Name	Issued By	Domains	Status	Time Remaining	Expiration Date	Delete
SWA Source GUI Certificate	SWA Source GUI Certificate	SWA Source GUI Certificate	N/A	Active	799 days	May 11 20:14:56 2028 GMT	

**Weak Signature Usage Settings**

Restrict Weak Signature Usage: Disabled [Edit Settings](#)

**Certificate FQDN Validation Settings**

Certificate FQDN Validation Usage: Disabled [Edit Settings](#)

**Certificate Lists**

**Updates**

File Type	Last Update	Current Version	New Update
Cisco Trusted Root Certificate Bundle	Success - Fri Feb 27 20:18:56 2026	2.6	Not Available
Cisco Certificate Blocked List	Success - Fri Feb 27 20:18:56 2026	1.3	Not Available

No updates in progress. [Update Now](#)

**Certificate Management**

Trust Root Certificates: 246 certificates in Cisco trusted root certificate list  
[6 custom certificates added to trusted root certificate list](#) [Manage Trusted Root Certificates...](#)

Certificate Based Authentication/RADSEC Root Certificates: 0 custom root certificates added to Certificate Based Authentication/RADSEC root certificate list  
[Manage Certificate Based Authentication/RADSEC Root Certificates...](#)

Blocked Certificates: 19 certificates in Cisco blocked certificate list  
[View Blocked Certificates...](#)

Image - Manage Trusted Root Certificates

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

Image - Download 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.**

**Certificate Management**

**Appliance Certificates**

Certificate	Common Name	Issued By	Domains	Status	Time Remaining	Expiration Date	Delete
SWA Source GUI Certificate	SWA Source GUI Certificate	SWA Source GUI Certificate	N/A	Active	799 days	May 11 20:14:56 2028 GMT	

[Export Certificate...](#)

**Weak Signature Usage Settings**

Restrict Weak Signature Usage: Disabled [Edit Settings](#)

**Certificate FQDN Validation Settings**

Certificate FQDN Validation Usage: Disabled [Edit Settings](#)

**Certificate Lists**

**Updates**

File Type	Last Update	Current Version	New Update
Cisco Trusted Root Certificate Bundle	Success - Fri Feb 27 20:18:56 2026	2.6	Not Available
Cisco Certificate Blocked List	Success - Fri Feb 27 20:18:56 2026	1.3	Not Available

No updates in progress. [Update Now](#)

**Certificate Management**

Trust Root Certificates: 246 certificates in Cisco trusted root certificate list  
[6 custom certificates added to trusted root certificate list](#) [Manage Trusted Root Certificates...](#)

Certificate Based Authentication/RADSEC Root Certificates: 0 custom root certificates added to Certificate Based Authentication/RADSEC root certificate list  
[Manage Certificate Based Authentication/RADSEC Root Certificates...](#)

Blocked Certificates: 19 certificates in Cisco blocked certificate list  
[View Blocked Certificates...](#)

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.

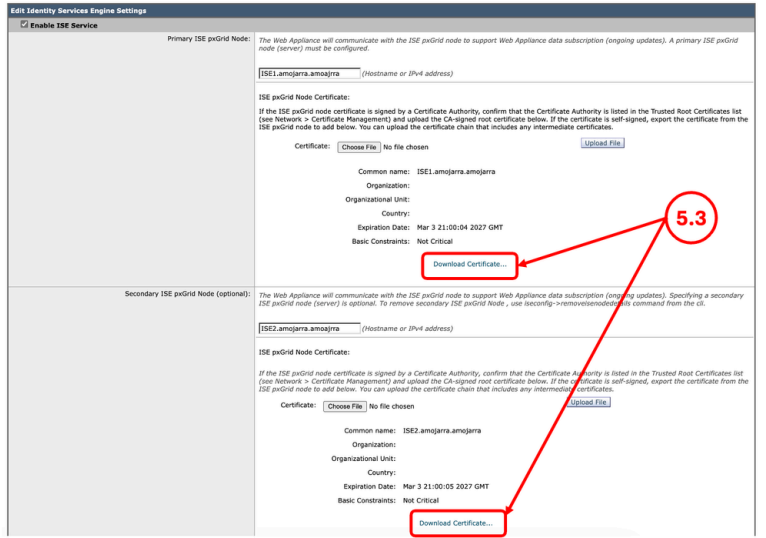


Image - Download ISE Certificates

## 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.

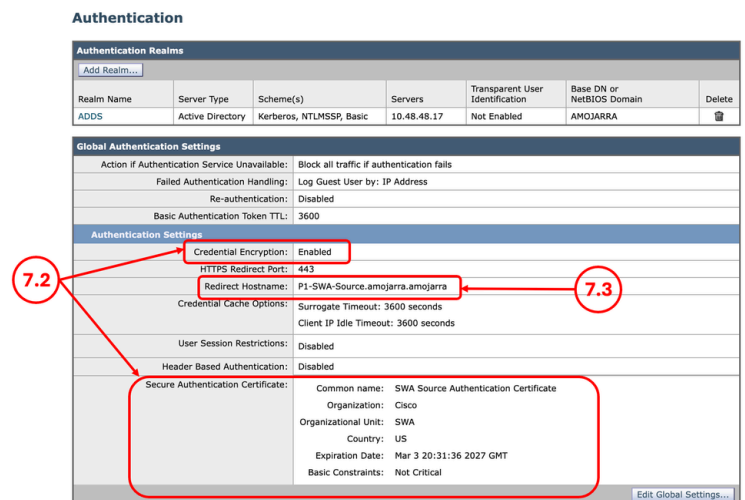



Image - Authentication Certificate



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

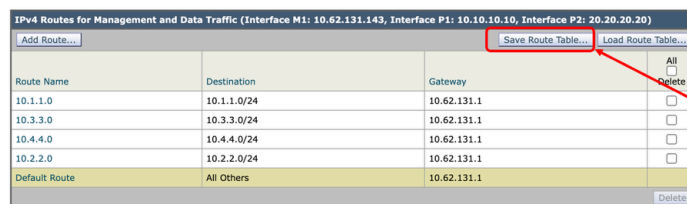
## Step 8. Export Static Routes

 **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**.


### Routes



Route Name	Destination	Gateway	All	Delete
10.1.1.0	10.1.1.0/24	10.62.131.1	<input type="checkbox"/>	<input type="checkbox"/>
10.3.3.0	10.3.3.0/24	10.62.131.1	<input type="checkbox"/>	<input type="checkbox"/>
10.4.4.0	10.4.4.0/24	10.62.131.1	<input type="checkbox"/>	<input type="checkbox"/>
10.2.2.0	10.2.2.0/24	10.62.131.1	<input type="checkbox"/>	<input type="checkbox"/>
Default Route	All Others	10.62.131.1		<input type="checkbox"/>

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.

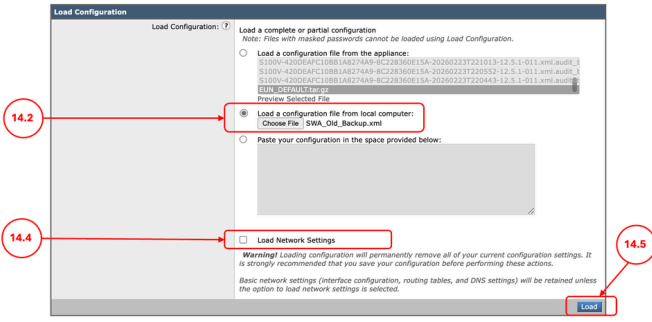



Reverting the device will cause a reboot to take place.

After rebooting, the appliance reinitializes itself and reboots again to the desired version, with the earlier system configuration.

	<p>Do you want to continue? [N]&gt; Y          Are you sure you want to continue? [N]&gt; Y</p> <p>Available versions          =====</p> <p>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.</p>
--	--

## Configuration Reverted SWA

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

	<p><b>Step 14.5.</b> Click <b>Load</b>.</p> <p><b>Step 14.6.</b> Click <b>Continue</b> in the <b>Confirm Load Configuration</b> pop up.</p>  <p><i>Image - Load the Old Configuration File</i></p> <p><b>Step 14.7.</b> <b>Commit</b> the changes.</p>
<p><b>Step 15. Import the Routes</b></p> <p> <b>Note:</b> If you <b>Load Network Settings</b> while importing the configuration, skip to <b>Step 17</b>.</p>	<p><b>Step 15.1.</b> From the GUI, Navigate to <b>Network</b> and click <b>Routes</b>.</p> <p><b>Step 15.2.</b> For each routing table, click <b>Load Route Table</b>.</p> <p><b>Step 15.3.</b> Choose the file you exported on <b>Step 8</b>.</p> <p><b>Step 15.4.</b> Click <b>Submit</b>.</p> <p><b>Step 15.5.</b> <b>Commit</b> the changes.</p>
<p><b>Step 16. Configure the DNS Settings</b></p> <p> <b>Note:</b> If you <b>Load Network Settings</b> while importing the configuration, skip to <b>Step 17</b>.</p>	<p><b>Step 16.1.</b> From the GUI, Navigate to <b>Network</b> and click <b>DNS</b>.</p> <p><b>Step 16.2.</b> Click <b>Edit Settings</b>.</p> <p><b>Step 16.3.</b> Use the screenshot from <b>Step 9</b></p> <p><b>Step 16.4.</b> Click <b>Submit</b>.</p> <p><b>Step 16.5.</b> <b>Commit</b> the changes.</p>
<p><b>Step 17. Join/Rejoin the SWA to the Active Directory</b></p>	<p><b>Step 17.1.</b> From the GUI, Navigate to <b>Network</b> and click <b>Authentication</b>.</p> <p><b>Step 17.2.</b> Click the name of the Authentication Realm Name.</p> <p> <b>Tip:</b> If the SWA is assigned a new IP address and host-name, ensure that the necessary DNS records are created in the Active Directory</p>

 DNS service.

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

**Add Realm**

**Authentication Realm**

Realm Name:

Authentication Server Type and Scheme(s):

**Active Directory Authentication**

Active Directory Server: Specify up to three Active Directory servers:

Set Source Interface

Source Interface:

hostname or IP address

Active Directory Account: Active Directory Domain:

Computer Account

Location:

(Example: Computers/BusinessUnit/Department/Servers)

Enable Trusted Domain Lookup

Status: Computer account for dwsa125\$ not yet created.

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.

**Authentication**

**Authentication Realms**

Realm Name	Server Type	Scheme(s)	Servers	Transparent User Identification	Base DN or NetBIOS Domain	Delete
ADDS	Active Directory	Kerberos, NTLMSSP, Basic	10.48.48.17	Not Enabled	AMOJARRA	

**Global Authentication Settings**

Action if Authentication Service Unavailable:

Failed Authentication Handling:

Re-authentication:

Basic Authentication Token TTL:

**Authentication Settings**

Credential Encryption: Disabled

Redirect Hostname:

Credential Cache Options:

User Session Restrictions:

Header Based Authentication:

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](#)