

# Integrate SWA with SMA

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Before you Begin](#)

### [Steps to Integrate SWA to SMA](#)

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

[Step 2. Create the Configuration Manager](#)

[Step 3. Configuration Manager Settings](#)

[Step 4. Add Web Appliance](#)

[Step 5. Validate the Integration](#)

### [Fixing Errors](#)

["The CentralizedServices is Disabled"](#)

["Authentication Failed for IP"](#)

["Cisco Centralized Web Reporting is disabled in the SWA"](#)

["The list of URL categories on this WSA was older than the list published from the SMA"](#)

["The host key appears to have changed"](#)

### [Related Information](#)

---

## Introduction

This document describes the process of integrating the Secure Web Appliance (SWA) to Security Management Appliance (SMA).

## Prerequisites

### Requirements

Cisco recommends knowledge of these topics:

- Access ToGraphic User Interface (GUI)of SWA.
- Administrative Access to the SWA.
- Administrative Access to the SMA.

### 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

1. Make sure the SMA and SWA are both licensed.
2. Check the compatibility matrix of the SWA and SMA, use this link: [SWA-SMA-ESA Compatibility Matrix](#).

 **Note:** Make sure the version you are planning to integrate is not deprovisioned.

## Compatibility with Secure Web Appliance

Select Version  Secure Web Appliance  Secure Email and Web Manager

Version Compatibility  Show Deprovisioned Releases

Secure Email and Web Manager	Secure Web Appliance														
	15.5.1-002 (MD)	15.5.0-710 (GD)	15.5.0-574 (GD)	15.5.0-566 (LD)	15.2.5-013 (MD)	15.2.4-022 (MD)	15.2.3-505 (HP)	15.2.3-007 (MD)	15.2.2-009 (MD)	15.2.2-009 (MD)	15.2.1-011 (MD)	15.2.0-164 (GD)	15.0.1-004 (MD)	15.0.0-612 (HP)	15.0.0-604 (MD)
16.0.1-010 (MD)									✓	✓	✓	✓	✓		
16.0.0-195 (GD) [Deprovisioned]*												✓	✓		
15.5.4-007 (MD)									✓	✓	✓	✓	✓		
15.5.3-017 (MD)									✓	✓	✓	✓	✓		

Image - Deprovisioned Releases

## Steps to Integrate SWA to SMA

<p><b>Step 1. Export the Configuration File from SWA</b></p>	<p><b>Step 1.1.</b> From the GUI, Navigate to <b>System Administration</b> and choose <b>Configuration File</b>.</p> <p><b>Step 1.2.</b> Make sure <b>Download file to local computer to view or save</b> is selected.</p> <p><b>Step 1.3.</b> Choose <b>Encrypt passwords in the Configuration Files</b>.</p> <p><b>Step 1.4.</b> (Optional) Choose a name for the configuration file.</p> <p><b>Step 1.5.</b> Click <b>Submit</b>.</p>
--	--

## Configuration File

Configuration File:

Download file to local computer to view or save

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

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:   
Note: ".xml" will be appended to the specified file-name automatically.

Image - Exporting the configuration File

**Step 2.1.** From the SMA GUI Click on the **Web** tab.

**Step 2.2.** From **Utilities** select **Configuration Manager**.

**Step 2.3.** If the Configuration manger is not **Initialized** yet, click on the **Initialize** link for the desired Configuration Manager, else skip to **Step 2.5**.

 **Tip:** The Configuration Manager version must align with the first two segments of your SWA version. For example, if your SWA version is 15.5.0-710, you must use Configuration Manager 15.5.

**Step 2.4.** Select **Use default settings** and click **Initialize**.

**Step 2.5.** Click **Import Configuration** for the desired Configuration Manager.

## Step 2. Create the Configuration Manager

 **Note:** If the Configuration Manager is already in configured in the SMA, skip to **Step 4**.

2.1 Management Appliance Email Web

2.2 Configuration Managers

2.3 15.5 (15.5.0)

2.5 Import Configuration

Configuration Manager	Assigned Web Appliances	Options	Delete
15.0 (15.0.1)	0	disabled*	
15.2 (15.2.4)	0	Initialize	
15.5 (15.5.0)	1	Initialize ✓	

\*This setting can be changed at Web > Utilities > Security Services Display.

Image - Configuration Manager

**Step 2.6.** From the **Select Configuration Source** choose **Web Configuration File**.

**Step 2.7.** Select the configuration file you exported on **Step 1**.



Image - Import Configuration

**Step 2.8. Click Import.**

**Step 2.9. Commit the changes.**

### Step 3. Configuration Manager Settings

**Step 3.1.** From the SMA GUI Click on the **Web** tab.

**Step 3.2.** From **Utilities** select **Security Services Display**.

**Step 3.3.** Make sure the desired features are configured correctly, you can enable or disable the features from **Edit Display Settings**.

**Step 3.4.** If you made any changes, **Submit** and **Commit**.

#### Security Services Display

Configuration Manager Settings for Display of Security Services	Configuration Managers		
	15.0 (disabled)	15.2 (disabled)	15.5
Features	Yes	Yes	Yes
Transparent mode	Yes	No	No
Range Request Forwarding	Yes	Yes	No
FTP Proxy	Yes	Yes	No
HTTPS Proxy	No	Yes	No
SOCKS Proxy	No	Yes	No
Upstream Proxy Groups	No	Yes	No
Acceptable Use Controls	Cisco Web Usage Controls (with Application Visibility and Control)	Cisco Web Usage Controls (with Application Visibility and Control)	Cisco Web Usage Controls (with Application Visibility and Control)
AnyConnect Secure Mobility	No	IP Range	No
Web Reputation Filters	Yes (Adaptive Scanning: Yes)	Yes (Adaptive Scanning: Yes)	Yes (Adaptive Scanning: Yes)
Advanced Malware Protection (File Reputation)	Yes (File Analysis: Yes)	Yes (File Analysis: Yes)	Yes (File Analysis: Yes)
Webroot Anti-Malware	Yes	Yes	Yes
McAfee Anti-Malware	No	Yes	No
Sophos Anti-Malware	Yes	Yes	Yes
End-User Acknowledgement	No	Yes	No
Cisco Data Security Filters	Yes	Yes	Yes
External DLP Servers	No	Yes	No
Credential Encryption	Yes	No	No
Identity Provider for SaaS	No	Yes	No

Image - Security Services Display

### Step 4. Add Web Appliance

**Step 4.1.** From the SMA GUI Click on the **Management Appliance** tab.

**Step 4.2.** From **Centralized Services** select **Security Appliances**.

**Step 4.3.** Click **Add Web Appliance**

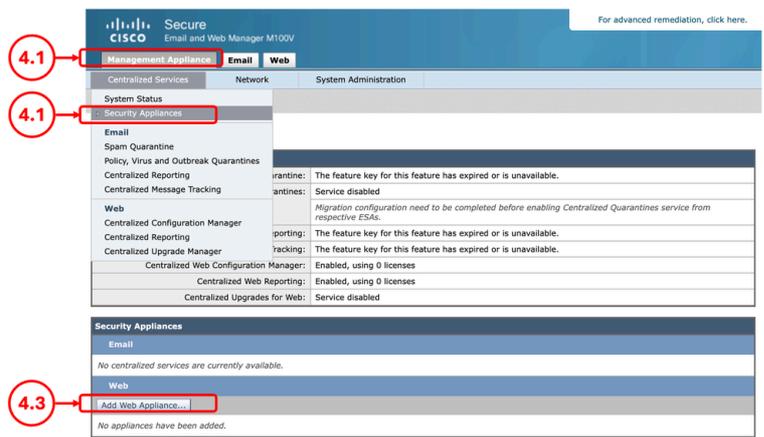


Image - Add Web Appliance

**Step 4.4.** Enter the **Appliance Name** and the **IP address** or **Hostname**.

**Step 4.5.** Click **Establish Connection**.

**Step 4.6.** Enter the **Username** and **Passphrase** and click **Establish Connection**.

**Step 4.7.** Assign the **Configuration Manager**.

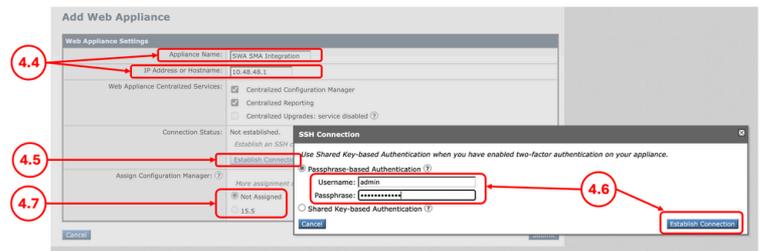


Image - Adding the SWA

**Step 4.8.** **Submit** and **Commit** the changes.

## Step 5. Validate the Integration

**Step 5.1.** From the SMA GUI, Click on the **Web** tab.

**Step 5.2.** From **Utilities**, select **Web Appliance Status**.

**Step 5.3.** If you are seeing a Warning message **Attention Required**. Click on the appliance name for details, click the name of the SWA and view the details.

### Web Appliance Status

⚠ Attention Required. Click on the appliance name for details.

Total Web Appliances: 1

Web Appliances								
Appliance Name	IP Address or Hostname	AsyncoS Version	Last Published Configuration			Security Services		
			User	Job Name	Configuration	Enabled	Disabled	
⚠ SWA SMA Integration	10.48.48.181	15.5.0-710	admin	admin.10_Mar_2026.09:37	15.5	12	11	

Image - Web Appliance Status



**Tip:** For troubleshooting view the **Fixing Errors** section in this article.

## Fixing Errors

### "The Centralized Services is Disabled"

While you try to select a Centralized services, if the check box is inactive, click on the question mark (?) and the guide navigates you through the path to enable that service.

#### Add Web Appliance

Web Appliance Settings	
Appliance Name:	<input type="text" value="SWA SMA Integration"/>
IP Address or Hostname:	<input type="text" value="10.48.48.1"/>
Web Appliance Centralized Services:	<input checked="" type="checkbox"/> Centralized Configuration Manager <input checked="" type="checkbox"/> Centralized Reporting <input type="checkbox"/> Centralized Upgrades: service disabled ?
Connection Status:	Not established. <i>Establish an SSH connection for Centralized W</i> <input type="button" value="Establish Connection..."/> <input type="button" value="Test Connection"/>
Assign Configuration Manager: ?	<i>More assignment options may be enabled once an SSH connection is established.</i> <input checked="" type="radio"/> Not Assigned <input type="radio"/> 15.5

**Upgrade Enable**   
To enable the services navigate to centralized services -> centralized upgrade Manager .

Image - The Centralized Services is Disabled

### "Authentication Failed for IP"

While you are integrating the SWA to SMA if you receive this error, make sure the IP address or hostname and the credentials are correct.

## Add Web Appliance

Error — Authentication Failed for IP: 10.48.48.181.

Web Appliance Settings	
Appliance Name:	<input type="text" value="SWA SMA Integration"/>
IP Address or Hostname:	<input type="text" value="10.48.48.181"/>
Web Appliance Centralized Services:	<input checked="" type="checkbox"/> Centralized Configuration Manager <input checked="" type="checkbox"/> Centralized Reporting <input type="checkbox"/> Centralized Upgrades: service disabled <span>?</span>
Connection Status:	Not established. <i>Establish an SSH connection for Centralized Web Services.</i> <input type="button" value="Establish Connection..."/> <input type="button" value="Test Connection"/>
Assign Configuration Manager: <span>?</span>	<i>More assignment options may be enabled once an SSH connection is established.</i> <input checked="" type="radio"/> Not Assigned <input type="radio"/> 15.5

Image - Authentication Failed

### "Cisco Centralized Web Reporting is disabled in the SWA"

If the SMA is configured with the Centralized Web Reporting and you assign that feature to the SWA while integrating the SWA to SMA in "Step 4", you need to enable **Cisco Centralized Web Reporting**:

Security Services						
 One or more of the services on the Web Appliance does not match the corresponding <i>Security Service Display</i> setting on the Management Appliance.						
Description	Services		Feature Keys			
	Web Appliance Service	Is Service Displayed on Management Appliance?	Status	Time Remaining	Expiration Date	
Cisco Web Proxy & DVS(TM) Engine	Enabled	Yes	Active	Perpetual	N/A	
Cisco L4 Traffic Monitor	Enabled	N/A	Active	Perpetual	N/A	
Proxy Mode	Transparent	Yes (Bypass Proxy)				
Range Request Forwarding	Disabled	No				
FTP Proxy	Disabled	No				
Cisco HTTPS Proxy	Disabled	No	Active	Perpetual	N/A	
SOCKS Proxy	Disabled	No				
Upstream Proxy Groups	Configured	No (Routing Policies)				
AnyConnect Secure Mobility	Disabled	No	Active	Perpetual	N/A	
Cisco URL Filtering	N/A	N/A	N/A	N/A	N/A	
Cisco Web Usage Controls	Enabled	Yes	Active	Perpetual	N/A	
Application Visibility and Control	Enabled	Yes				
Application Discovery and Control	Disabled	No				
Cisco Centralized Web Reporting	Disabled	Yes				
Cisco Web Reputation Filters	Enabled	Yes	Active	Perpetual	N/A	
Adaptive Scanning	Enabled	Yes				
Advanced Malware Protection (File Reputation)	Enabled	Yes	Active	Perpetual	N/A	
File Analysis	Enabled	Yes	Active	Perpetual	N/A	
Webroot Anti-Malware	Enabled	Yes	Active	Perpetual	N/A	
McAfee Anti-Malware	N/A	No	N/A	N/A	N/A	
Sophos Anti-Malware	Enabled	Yes	Active	Perpetual	N/A	
End-User Acknowledgement	Disabled	No				
Cisco Data Security Filters	Enabled	Yes				
External DLP Servers	Not Configured	No				
Credential Encryption	Disabled	No				
Identity Provider for SaaS	Not Configured	No				

Image - Centralized Web Reporting is Disabled in the SWA

To fix the issue, connect to the SWA from CLI and type **reportingconfig** and select **CENTRALIZED**, follow the wizard to enable the Centralized Reporting and **commit** the changes.

```
SWA_CLI> reportingconfig
```

Choose the operation you want to perform:

- COUNTERS - Limit counters recorded by the reporting system.
  - WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries.
  - AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings Calculation.
  - WEBEVENTBUCKETING - Enable or Disable web transaction event bucketing.
  - CTROBSERVABLE - Enable or Disable CTR observable based indexing.
  - CENTRALIZED - Enable/Disable Centralized Reporting for this Secure Web Appliance.
- ```
[ ]> CENTRALIZED
```

```
Reporting service status: Local Reporting enabled. (Show usernames in reports.)
```

```
Do you want to enable Centralized Reporting for this appliance? [N]> Y
```

```
Do you want to anonymize usernames in reports? [N]> N
```

```
Reporting service status: Centralized Reporting enabled. (Show usernames in reports.)
```

Choose the operation you want to perform:

- COUNTERS - Limit counters recorded by the reporting system.
- WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries.
- AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings Calculation.
- WEVENTBUCKETING - Enable or Disable web transaction event bucketing.
- CTROBSERVABLE - Enable or Disable CTR observable based indexing.
- CENTRALIZED - Enable/Disable Centralized Reporting for this Secure Web Appliance.

[ ]>

SWA\_CLI> commit

## "The list of URL categories on this WSA was older than the list published from the SMA"

If while you are publishing the configuration to SWA and receiving the Error indicates that the URL category list in SWA and SMA are not the same, make sure both devices are able to connect to Cisco Update Server and there are no Errors in the "**updater\_logs**":

### Publish in Progress: admin.10\_Mar\_2026.13:19

**Warning** — Configuration Publish job admin.10\_Mar\_2026.13:19 has completed. The configuration was not successfully published to at least one of the destination web appliances.

| Job admin.10_Mar_2026.13:19 Started at 10 Mar 2026 13:19 (GMT) |                                                                       |                                                                                                           |
|----------------------------------------------------------------|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| Web Appliances                                                 | Progress                                                              | Status                                                                                                    |
| SWA SMA Integration                                            | <div style="width: 100%; height: 10px; background-color: red;"></div> | Failure: The list of URL categories on this WSA was older than the list published... <a href="#">more</a> |

Final status of this job will be reported on the [Publish History](#) page.

Close

*Image - The list of URL categories are not matching*

To force the SWA or SMA to download the update, from the CLI, type **updatenow**.

To view the SMA or SMA, Logs related to update, from the CLI type **grep** and choose the number associated with **updater\_logs** and follow the wizard

 **Tip:** to view the live logs, type "Y" in the answer to **Do you want to tail the logs? [N]>**.

## "The host key appears to have changed"

If while you are integrating the SWA to the SMA and receiving the Error that the host key has been changed, this is due to the reason that SMA has stored a different host Key for the same IP address in its key store.

## Edit Web Appliance: Source SWA

**Error** — The host key for 10.48.48.181 appears to have changed.

- It is possible that someone is trying to hijack the encrypted connection to the remote host. Please use the `logconfig->hostkeyconfig` command to verify (and possibly update) the SSH host key for 10.48.48.181.

| Web Appliance Settings              |                                                                                                                                                                                                                               |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Appliance Name:                     | Source SWA                                                                                                                                                                                                                    |
| IP Address or Hostname:             | 10.48.48.181                                                                                                                                                                                                                  |
| Web Appliance Centralized Services: | <input checked="" type="checkbox"/> Centralized Configuration Manager<br><input checked="" type="checkbox"/> Centralized Reporting<br><input type="checkbox"/> Centralized Upgrades: service disabled (?)                     |
| Connection Status:                  | File transfer credentials have been established.<br><i>Establish an SSH connection for Centralized Web Services.</i><br><input type="button" value="Establish Connection..."/> <input type="button" value="Test Connection"/> |
| Assign Configuration Manager: (?)   | <i>More assignment options may be enabled once an SSH connection is established.</i><br><input checked="" type="radio"/> Not Assigned<br><input type="radio"/> 15.5                                                           |

Image -The host key appears to have changed

To fix this Error, log in to CLI of SMA, run **logconfig** and Enter **HOSTKEYCONFIG**. Type **DELETE** and press **Enter**. Then, select the number associated to the SWA and press enter until the wizard is finished.

**Commit** the changes:

```
SMA_CLI> logconfig
```

Currently configured logs:

| Log Name            | Log Type            | Retrieval       | Interval |
|---------------------|---------------------|-----------------|----------|
| 1. aggregatord_logs | Aggregatord Logs    | Manual Download | None     |
| 2. authentication   | Authentication Logs | Manual Download | None     |
| ...                 |                     |                 |          |

Choose the operation you want to perform:

- NEW - Create a new log.
  - EDIT - Modify a log subscription.
  - DELETE - Remove a log subscription.
  - DELETELOGFILE - Delete log files
  - SETUP - General settings.
  - LOGHEADERS - Configure headers to log.
  - HOSTKEYCONFIG - Configure SSH host keys.
- ```
[> HOSTKEYCONFIG
```

Currently installed host keys:

1. 10.48.48.182 ssh-rsa AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...ZhW4gEXWE=
2. 10.48.48.181 ssh-rsa BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBb...4p74b9Q9k=

Choose the operation you want to perform:

- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.

```
- SCAN - Automatically download a host key.  
- PRINT - Display a key.  
- HOST - Display system host keys.  
- FINGERPRINT - Display system host key fingerprints.  
- USER - Display system user keys.  
- REGENERATESCPKEYS - Regenerate SSH Keys for SCP Log Subscription Retrieval.  
[> DELETE
```

Enter the number of the key you wish to delete.

```
[> 2
```

Currently installed host keys:

```
1. 10.62.131.143 ssh-rsa AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...ZhW4gEXWE=
```

```
...
```

```
SMA_CLI> commit
```

## Related Information

- [User Guide for AsyncOS 15.2 for Cisco Secure Web Appliance](#)
- [Install Secure Web Appliance on Vmware ESXi](#)
- [Install Secure Web Appliance on Microsoft Hyper-V](#)
- [Secure Web Appliance Initial Setup](#)
- [Cisco Secure Email and Web Virtual Appliance Installation Guide](#)
- [Configure Custom URL Categories in Secure Web Appliance - Cisco](#)
- [Use Secure Web Appliance Best Practices](#)
- [Configure Firewall for Secure Web Appliance](#)
- [Configure Decryption Certificate in Secure Web Appliance](#)
- [Troubleshoot Secure Web Appliance DNS Service](#)