

Integración de SWA con SMA

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antes de comenzar](#)

[Pasos para integrar SWA en SMA](#)

[Paso 1. Exportar el archivo de configuración desde SWA](#)

[Paso 2. Creación del Administrador de configuración](#)

[Paso 3. Configuración del Administrador de configuración](#)

[Paso 4. Agregar dispositivo web](#)

[Paso 5. Validar la integración](#)

[Corrección de errores](#)

["Los servicios centralizados están deshabilitados"](#)

["Error de autenticación para IP"](#)

["La notificación web centralizada de Cisco está desactivada en el SWA"](#)

["La lista de categorías de URL de este WSA era anterior a la lista publicada del SMA"](#)

["La clave de host parece haber cambiado"](#)

[Información Relacionada](#)

Introducción

Este documento describe el proceso de integración de Secure Web Appliance (SWA) en Security Management Appliance (SMA).

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- Acceso a la interfaz gráfica de usuario (GUI) de SWA.
- Acceso administrativo al SWA.
- Acceso administrativo al SMA.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antes de comenzar

1. Asegúrese de que el SMA y el SWA tengan licencia.
2. Compruebe la matriz de compatibilidad del SWA y el SMA, utilice este enlace: [Matriz de compatibilidad SWA-SMA-ESA](#).

 Nota: Asegúrese de que la versión que tiene pensado integrar no está desaprovionada.

Compatibility with Secure Web Appliance

Select Version

Secure Web Appliance

Secure Email and Web Manager

Search

Version Compatibility

Show Deprovisioned Releases

Export to Excel

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)	15.600
16.0.1-010 (MD)										✓	✓	✓	✓	✓		
16.0.0-195 (GD) [Deprovisioned]*													✓	✓		
15.5.4-007 (MD)										✓	✓	✓	✓	✓		
15.5.3-017 (MD)										✓	✓	✓	✓	✓		

Imagen - Versiones no suministradas

Pasos para integrar SWA en SMA

Paso 1. Exportar el archivo de configuración desde SWA	Paso 1.1. Desde la GUI, vaya a Administración del sistema y elija Archivo de configuración. Paso 1.2. Asegúrese de que la opción Descargar archivo al equipo local para verlo o guardarlo está seleccionada. Paso 1.3. Elija Cifrar contraseñas en los archivos de configuración. Paso 1.4. (Opcional) Elija un nombre para el archivo de configuración. Paso 1.5. Haga clic en Enviar.
--	--

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.

Imagen: Exportación del archivo de configuración

Paso 2.1. Desde la GUI de SMA, haga clic en la pestaña Web.

Paso 2.2. En Utilidades seleccione Administrador de configuración.

Paso 2.3. Si el Administrador de configuración no está Inicializado todavía, haga clic en el enlace Inicializar del Administrador de configuración deseado; de lo contrario, vaya al Paso 2.5.



Consejo: La versión del Administrador de configuración debe coincidir con los dos primeros segmentos de la versión SWA. Por ejemplo, si la versión de SWA es 15.5.0-710, debe utilizar Configuration Manager 15.5.

Paso 2. Creación del Administrador de configuración



Nota: Si el Administrador de configuración ya está configurado en el SMA, vaya al Paso 4.

Paso 2.4. Seleccione Use default settings y haga clic en Initialize.

Paso 2.5. Haga clic en Importar configuración para el Administrador de configuración deseado.

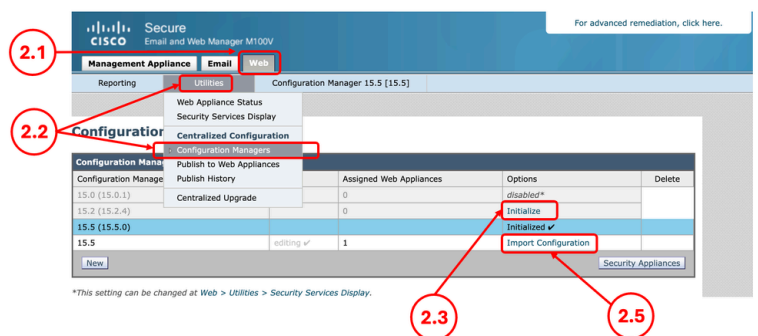


Imagen - Administrador de configuración

Paso 2.6. Desde Seleccionar Origen de Configuración elija Archivo de Configuración Web.

Paso 2.7. Seleccione el archivo de configuración que exportó en el Paso 1.



Imagen - Importar configuración

Paso 2.8. Haga clic en Importar.

Paso 2.9. Realice los cambios.

Paso 3. Configuración del Administrador de configuración

Paso 3.1. Desde la GUI de SMA, haga clic en la pestaña Web.

Paso 3.2. En Utilidades seleccione Visualización de servicios de seguridad.

Paso 3.3. Asegúrese de que las funciones deseadas están configuradas correctamente; puede activar o desactivar las funciones en Editar configuración de visualización.

Paso 3.4. Si ha realizado cambios, Enviar y Confirmar.

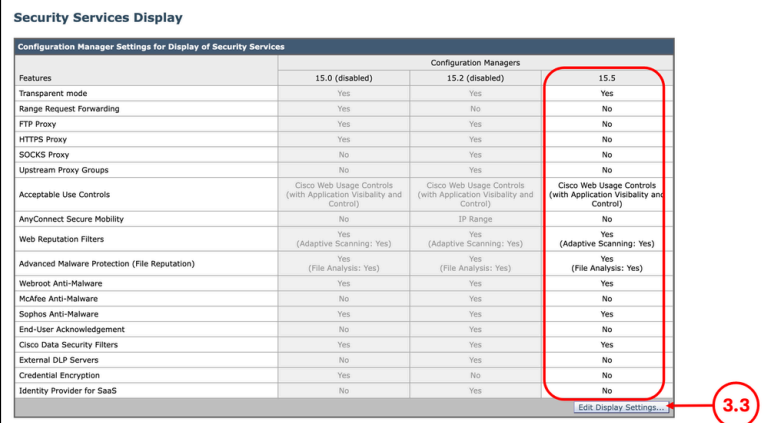


Imagen - Visualización de servicios de seguridad

Paso 4. Agregar dispositivo web

Paso 4.1. Desde la GUI de SMA, haga clic en la pestaña Dispositivo de administración.

Paso 4.2. En Servicios centralizados seleccione

Dispositivos de seguridad.

Paso 4.3. Haga clic en Agregar dispositivo web

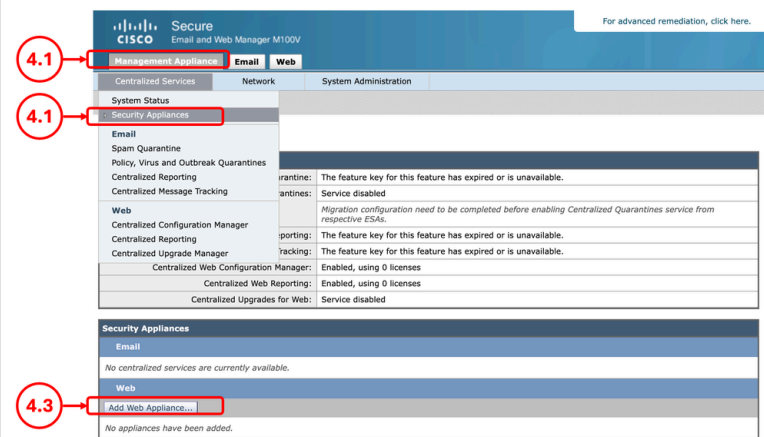


Imagen - Agregar dispositivo web

Paso 4.4. Introduzca el nombre del dispositivo y la dirección IP o el nombre de host.

Paso 4.5. Haga clic en Establecer conexión.

Paso 4.6. Introduzca el nombre de usuario y la frase de paso y haga clic en Establecer conexión.

Paso 4.7. Asignar el Administrador de configuración.

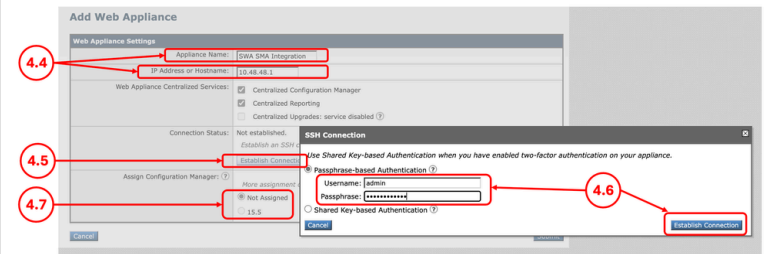


Imagen: adición del SWA

Paso 4.8. Envíe y confirme los cambios.

Paso 5. Validar la integración

Paso 5.1. Desde la GUI de SMA, haga clic en la pestaña Web.

Paso 5.2. En Utilidades, seleccione Estado del dispositivo web.

Paso 5.3. Si aparece un mensaje de advertencia Se requiere atención. Haga clic en el nombre del dispositivo para obtener más información, haga clic

en el nombre del SWA y vea los detalles.

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	User	Last Published Configuration		Security Services	
				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

Imagen - Estado del dispositivo web



Consejo: Para solucionar problemas, consulte la sección Corrección de errores de este artículo.

Corrección de errores

"Los servicios centralizados están deshabilitados"

Mientras intenta seleccionar un servicio centralizado, si la casilla de verificación está inactiva, haga clic en el signo de interrogación (?) y la guía le guiará por la ruta para habilitar ese servicio.

Add Web Appliance

Web Appliance Settings

Appliance Name:

SWA SMA Integration

IP Address or Hostname:

10.48.48.1

Web Appliance Centralized Services:

☒ Centralized Configuration Manager

☒ Centralized Reporting

☐ Centralized Upgrades: service disabled ?

Connection Status:

Not established.
Establish an SSH connection for Centralized W

Establish Connection...

Test Connection

Assign Configuration Manager: ?

More assignment options may be enabled once an SSH connection is established.
☒ Not Assigned
☐ 15.5

Upgrade Enable

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

Cancel

Submit

Imagen: los servicios centralizados están desactivados

"Error de autenticación para IP"

Mientras integra el SWA en SMA si recibe este error, asegúrese de que la dirección IP o el nombre de host y las credenciales sean correctas.

Add Web Appliance

Error — Authentication Failed for IP: 10.48.48.181.

Web Appliance Settings	
Appliance Name:	SWA SMA Integration
IP Address or Hostname:	10.48.48.181
Web Appliance Centralized Services:	☒ Centralized Configuration Manager ☒ Centralized Reporting ☐ Centralized Upgrades: service disabled ?
Connection Status:	Not established. <i>Establish an SSH connection for Centralized Web Services.</i> Establish Connection... Test Connection
Assign Configuration Manager: ?	<i>More assignment options may be enabled once an SSH connection is established.</i> ☒ Not Assigned ☐ 15.5

[Cancel](#) [Submit](#)

Imagen - Error de autenticación

"La notificación web centralizada de Cisco está desactivada en el SWA"

Si el SMA está configurado con Notificación web centralizada y asigna esa función al SWA mientras integra el SWA al SMA en el "Paso 4", debe habilitar Notificación web centralizada de Cisco:

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			

Imagen: Notificación web centralizada desactivada en el SWA

Para solucionar el problema, conéctese al SWA desde la CLI y escriba `reportingconfig` y seleccione **CENTRALIZED**, siga el asistente para habilitar la notificación centralizada y confirme los cambios.

```
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.
- 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.

[>

SWA\_CLI> commit

"La lista de categorías de URL de este WSA era anterior a la lista publicada del SMA"

Si mientras publica la configuración en SWA y recibe el mensaje de error indica que la lista de categorías de URL en SWA y SMA no es la misma, asegúrese de que ambos dispositivos puedan conectarse a Cisco Update Server y que no haya errores en "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></div> | Failure: The list of URL categories on this WSA was older than the list publishe... <a href="#">more</a> |

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

Close

Imagen: la lista de categorías de URL no coincide

Para forzar al SWA o SMA a descargar la actualización, desde la CLI, escriba updatenow.

Para ver el SMA o SMA, Logs relacionados con la actualización, desde la CLI escriba grep y elija el número asociado con updater\_logs y siga el asistente

 Consejo: para ver los registros activos, escriba "Y" en la respuesta a ¿Desea finalizar los registros? [N]>.

"La clave de host parece haber cambiado"

Si mientras está integrando el SWA en el SMA y recibe el error de que la clave de host ha sido cambiada, esto se debe a que SMA ha almacenado una clave de host diferente para la misma dirección IP en su almacén de claves.

## 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><a href="#">Establish Connection...</a> <a href="#">Test Connection</a>         |
| 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                                     |

[Cancel](#) [Submit](#)

Imagen: parece que la clave de host ha cambiado

Para corregir este error, inicie sesión en la CLI de SMA, ejecute `logconfig` e ingrese `HOSTKEYCONFIG`. Escriba `DELETE` y presione Enter. Luego, seleccione el número asociado al SWA y presione Enter hasta que el asistente termine.

Realice los cambios:

```
SMA_CLI> logconfig
```

Currently configured logs:

| Log Name           | Log Type            | Retrieval       | Interval |
|--------------------|---------------------|-----------------|----------|
| 1. aggregator_logs | Aggregator 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 BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBb...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
```

Información Relacionada

- [Guía del usuario de AsyncOS 15.2 para Cisco Secure Web Appliance](#)
- [Instalación de Secure Web Appliance en VMware ESXi](#)
- [Instalación de Secure Web Appliance en Microsoft Hyper-V](#)
- [Configuración inicial del dispositivo web seguro](#)
- [Guía de instalación de Cisco Secure Email and Web Virtual Appliance](#)
- [Configurar categorías de URL personalizadas en el dispositivo web seguro - Cisco](#)
- [Uso de las prácticas recomendadas de Secure Web Appliance](#)
- [Configuración del firewall para el dispositivo web seguro](#)
- [Configurar certificado de descifrado en dispositivo web seguro](#)
- [Solucionar problemas del servicio DNS de dispositivo web seguro](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).