

Configuración de la copia de seguridad en el dispositivo web seguro

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Generar copia de seguridad desde GUI](#)

[Copia de seguridad automática en una ubicación remota](#)

[Generar copia de seguridad desde CLI](#)

[Importación del archivo de configuración a SWA](#)

[Información Relacionada](#)

Introducción

Este documento describe el proceso de copia de seguridad y restauración de la configuración en Secure Web Appliance (SWA).

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- Acceso a la interfaz gráfica de usuario (GUI) de SWA.
- Acceso a la interfaz de línea de comandos (CLI) de SWA.

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.

Generar copia de seguridad desde GUI

Paso 1. Desde la GUI, vaya a Administración del sistema y elija Archivo de configuración.

Paso 2. Asegúrese de que la opción Descargar archivo al equipo local para verlo o guardarlo está seleccionada.

Paso 3. Elija Cifrar contraseñas en los archivos de configuración

Paso 4. (Opcional) Elija un nombre para el archivo de configuración.

Paso 5. Haga clic en Enviar.

Configuration File

Current Configuration

Configuration File:

2 → ☒ Download file to local computer to view or save

☐ Save file to this appliance (*wsa-source.cisco.local*)

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

Password Display Options:

3 → ☒ Encrypt passwords in the Configuration Files

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

4 → ☒ Use system-generated file name

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

Submit

Imagen - Exportar la configuración

⚠ Precaución: Si genera la copia de seguridad con una máscara de contraseña, no podrá importar el archivo a SWA.

Copia de seguridad automática en una ubicación remota

Puede configurar SWA para guardar una copia de la configuración actual en otra ubicación, mientras confirma los nuevos cambios.

Paso 1. Desde la GUI, vaya a Administración del sistema y elija Archivo de configuración.

Paso 2. En la sección Copia de seguridad de la configuración, active la casilla de verificación para habilitar la copia de seguridad de la configuración.

Paso 3. Para poder importar el archivo de configuración a SWA, seleccione Yes en Include Passphrase in Configuration File?

Paso 4. Dependiendo de su diseño, puede seleccionar File Transfer Protocol (FTP) o Secure Copy (SCP) como protocolo deseado para guardar el archivo de configuración.

Paso 5. Haga clic en Enviar y confirme los cambios.

The screenshot shows the 'Configuration Backup' web interface. It has a dark blue header with the title 'Configuration Backup'. The main content area is white with a light blue sidebar on the left. The sidebar contains a large grey rectangular area. Four red circles with numbers 2, 3, and 4 are on the left, with red arrows pointing to specific fields in the form. Callout 2 points to the 'Enable Config Backup:' checkbox, which is checked and labeled 'Enable'. Callout 3 points to the 'Retrieval Method:' radio buttons, where 'FTP on Remote Server' is selected. Callout 4 points to the input fields for 'FTP Host:', 'Directory:', 'Username:', and 'Passphrase:'. The 'FTP Host:' field contains '10.48.48.192', 'Directory:' contains 'SWA1_Backup', 'Username:' contains 'administrator', and 'Passphrase:' contains a series of dots. Below these, there are fields for 'SCP Host:', 'SCP Port:', 'Directory:', and 'Username:'. The 'SCP Port:' field contains '22'. At the bottom right, there is a 'Submit' button. Below the SCP fields, there is a section for 'Enable Host Key Checking' with two radio buttons: 'Automatically Scan' (selected) and 'Enter Manually'.

Imagen - Copia de seguridad de configuración automática

Generar copia de seguridad desde CLI

Puede generar una copia de seguridad de la configuración desde la CLI, que almacena el archivo exportado localmente en el SWA.

Paso 1. Inicie sesión en la CLI.

Paso 2. Ejecute saveconfig.

Paso 3. Escriba 2 para seleccionar las contraseñas cifradas.

Paso 4. (Opcional) Escriba N si desea utilizar un nombre de archivo definido por el usuario para el archivo exportado, o escriba Y para ¿Desea que el sistema genere un nombre para el archivo de configuración? [Y]>.

```
SWA_CLI> saveconfig
```

Choose the password option:

1. Mask passwords (Files with masked passwords cannot be loaded using loadconfig command)
 2. Encrypt passwords
- ```
[1]> 2
```

Do you want the system to generate a name for the configuration file? [Y]>

The file S1000V-4444444444444444-AAAAAAAAAAAAA-BBBBBBBBBBBB.xml has been saved in the configuration di



Consejo: El archivo de configuración generado se almacena en el directorio de configuración del equipo, al que se puede acceder a través de FTP.

## Importación del archivo de configuración a SWA

Paso 1. Desde la GUI, vaya a Administración del sistema y elija Archivo de configuración.

Paso 2. En la sección Cargar configuración, seleccione Cargar un archivo de configuración desde el equipo local.

Paso 3. Haga clic en Choose File y seleccione el archivo de configuración XML.

Paso 4. (Opcional) Si desea importar la configuración de red, active la casilla de verificación Cargar configuración de red.

Paso 5. Haga clic en Cargar.

Paso 6. Haga clic en Continuar en la ventana emergente Confirmar configuración de carga.

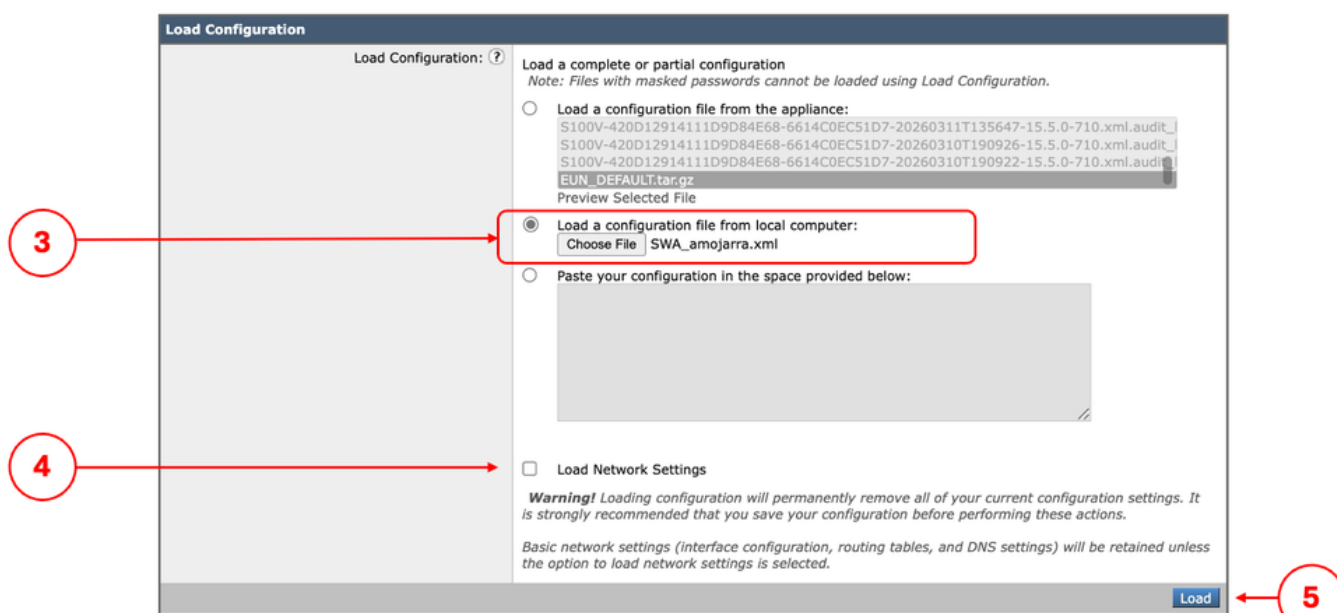


Imagen - Importar configuración

## Información Relacionada

- [Guía del usuario de AsyncOS 15.2 para Cisco Secure Web Appliance](#)
- [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](#)

#### 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).