

Back-up configureren in Secure Web Appliance

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Back-up genereren vanuit GUI](#)

[Automatische back-up op een externe locatie](#)

[Back-up genereren vanuit CLI](#)

[Het configuratiebestand importeren in SWA](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe u een back-up maakt van de configuratie en deze terugzet in Secure Web Appliance (SWA).

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- Toegang tot grafische gebruikersinterface (GUI) van SWA.
- Toegang tot de Command Line Interface (CLI) van SWA.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Back-up genereren vanuit GUI

Stap 1. Navigeer vanuit de GUI naar Systeembeheer en kies Configuratiebestand.

Stap 2. Zorg ervoor dat Bestand downloaden naar lokale computer om te bekijken of op te slaan is geselecteerd.

Stap 3. Kies Wachtwoorden coderen in de configuratiebestanden

Stap 4. (Optioneel) Kies een naam voor het configuratiebestand.

Stap 5. Klik op Indienen.

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.

3

4

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.

Submit

Afbeelding - De configuratie exporteren

⚠ Let op: als u de back-up genereert met een maskerwachtwoord, kunt u het bestand niet importeren in SWA.

Automatische back-up op een externe locatie

U kunt SWA configureren om een kopie van de huidige configuratie op een andere locatie op te slaan terwijl u de nieuwe wijzigingen doorvoert.

Stap 1. Navigeer vanuit de GUI naar Systeembeheer en kies Configuratiebestand.

Stap 2. Schakel in het gedeelte Configuration Backup het selectievakje in om Config Backup in te schakelen.

Stap 3. Als u het configuratiebestand wilt importeren in SWA, selecteert u Ja in Wachtwoordgroep opnemen in configuratiebestand?

Stap 4. Afhankelijk van uw ontwerp kunt u het configuratiebestand opslaan met File Transfer Protocol (FTP) of Secure Copy (SCP).

Stap 5. Klik op Indienen en verbind de wijzigingen.

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 gray sidebar on the left. The sidebar contains a large gray rectangle. Four red circles with numbers 2, 3, and 4 are on the left, with red arrows pointing to specific settings in the main area:

- Circle 2 points to the 'Enable Config Backup:' checkbox, which is checked and labeled 'Enable'.
- Circle 3 points to the 'Retrieval Method:' radio button, which is selected and labeled 'FTP on Remote Server'.
- Circle 4 points to the 'SCP on Remote Server' radio button, which is not selected.

The main area contains the following settings:

- 'Include Passphrase in Configuration File?': Radio buttons for 'No' and 'Yes' (selected).
- 'Retrieval Method:': Radio buttons for 'FTP on Remote Server' (selected) and 'SCP on Remote Server'.
- Under 'FTP on Remote Server':
 - 'FTP Host:': Text input field with '10.48.48.192'.
 - 'Directory:': Text input field with 'SWA1_Backup'.
 - 'Username:': Text input field with 'administrator'.
 - 'Passphrase:': Text input field with masked characters '.....'.
- Under 'SCP on Remote Server':
 - 'SCP Host:': Text input field.
 - 'SCP Port:': Text input field with '22'.
 - 'Directory:': Text input field.
 - 'Username:': Text input field.
- 'Enable Host Key Checking':
 - Checkbox: Not checked.
 - 'Automatically Scan': Radio button (selected).
 - 'Enter Manually': Radio button.

A 'Submit' button is located at the bottom right of the form.

Image - Automatische back-up van configuratie

Back-up genereren vanuit CLI

U kunt een back-up van de configuratie maken vanuit de CLI, waarin het geëxporteerde bestand lokaal wordt opgeslagen op de SWA.

Stap 1. Log in bij de CLI.

Stap 2. Voer saveconfig uit.

Stap 3. Typ 2 om de wachtwoorden te versleutelen.

Stap 4. (Optioneel) Type N als u een door de gebruiker gedefinieerde bestandsnaam voor het geëxporteerde bestand wilt gebruiken, typt u Y voor Wilt u dat het systeem een naam genereert voor het configuratiebestand? [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-BBBBBBBBBBBBBB.xml has been saved in the configuration di

---

 Tip: Het gegenereerde configuratiebestand wordt opgeslagen in de configuratiemap op het

---

 systeem, die toegankelijk is via FTP.

## Het configuratiebestand importeren in SWA

Stap 1. Navigeer vanuit de GUI naar Systeembeheer en kies Configuratiebestand.

Stap 2. Selecteer in het gedeelte Configuratie laden de optie Een configuratiebestand laden vanaf de lokale computer.

Stap 3. Klik op Bestand kiezen en selecteer het XML-configuratiebestand.

Stap 4. (Optioneel) Als u de netwerkconfiguratie wilt importeren, schakelt u het selectievakje Netwerkinstellingen laden in.

Stap 5. Klik op Laden.

Stap 6. Klik op Doorgaan in het pop-upvenster Configuratie laden bevestigen.

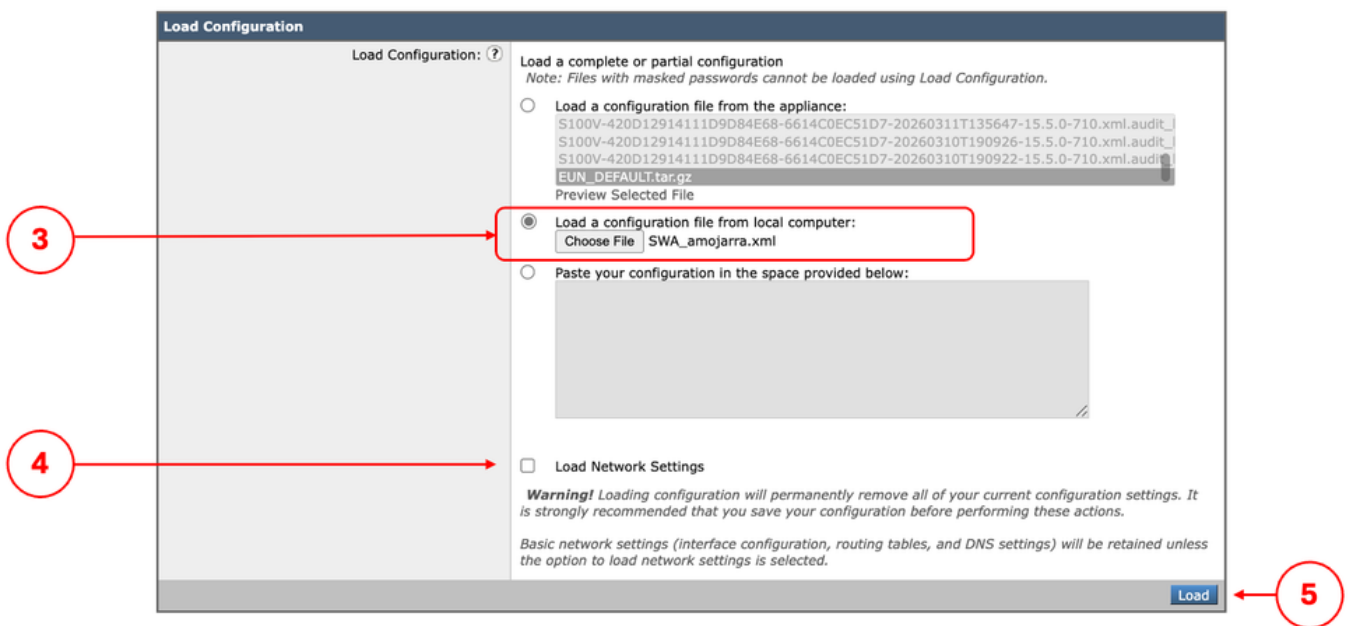


Image - Configuratie importeren

## Gerelateerde informatie

- [Gebruikershandleiding voor AsyncOS 15.2 voor Cisco Secure Web Appliance](#)
- [Beveiligde eerste installatie van webtoestel](#)
- [Installatiehandleiding voor Cisco Secure Email and Web Virtual Appliance](#)
- [Aangepaste URL-categorieën configureren in Secure Web Appliance - Cisco](#)
- [Best practices voor veilige webapparaten gebruiken](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.