

Secure Web Appliance terugzetten naar vorige versie

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Voordat u begint](#)

[Vorbereiden en back-up maken van de SWA](#)

[Stap 1. Het configuratiebestand exporteren](#)

[Stap 2. Het decoderingscertificaat exporteren](#)

[Stap 3. De aangepaste basiscertificaten voor vertrouwen exporteren](#)

[Stap 4. Het GUI-certificaat exporteren](#)

[Stap 5. De ISE-certificaten exporteren](#)

[Stap 6. Licenties / functies](#)

[Stap 7. certificaat van echtheidswijziging](#)

[Stap 8. Statische routes exporteren](#)

[Stap 9. DNS-instellingen](#)

[De SWA terugdraaien](#)

[Stap 10. De SWA terugdraaien](#)

[Configuratie teruggedraaide SWA](#)

[Stap 11. Licentie voor de SWA](#)

[Stap 12. De wizard System Setup \(Systeeminstellingen\) uitvoeren](#)

[Stap 13. Aangepaste vertrouwde basiscertificaten importeren](#)

[Stap 14. Het configuratiebestand importeren](#)

[Stap 15. De routes importeren](#)

[Stap 16. De DNS-instellingen configureren](#)

[Stap 17. De SWA toevoegen aan/opnieuw toevoegen aan de Active Directory](#)

[Gerelateerde informatie](#)

Inleiding

In dit document worden de stappen beschreven voor het terugzetten van de Secure Web Appliance (SWA) naar de vorige versie.

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- Toegang tot grafische gebruikersinterface (GUI) van SWA
- Administratieve toegang tot de SWA
- Toegang tot het Cisco Software Licensing Portal of het SWA-licentiebestand
- Active Directory geeft gebruikers voorrang bij toegang tot het SWA-domein en maakt DNS-records

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.

Voordat u begint

Het terugdraaien van het apparaat is uiterst destructief.

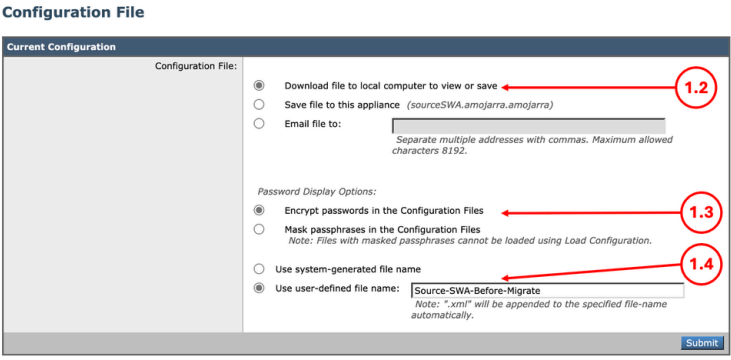

Dit zijn de gegevens die tijdens het proces worden vernietigd en waarvan een back-up moet worden gemaakt:

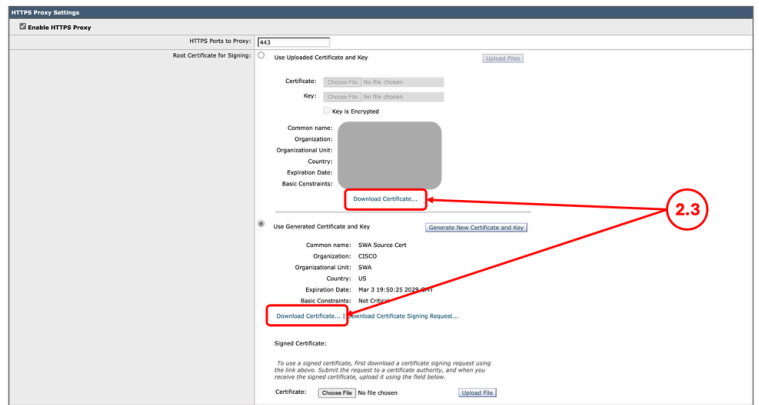
- Huidig systeemconfiguratiebestand.
- Alle logbestanden (voor meer informatie gaat u naar: [Access Secure Web Appliance Logs](#))
- Alle rapportagegegevens (inclusief opgeslagen geplande en gearchiveerde rapporten)
- Aangepaste meldingspagina's voor eindgebruikers.

 **Waarschuwing:** Voordat u terugkeert naar een eerdere versie, moet u ervoor zorgen dat u het gecodeerde configuratiebestand hebt dat overeenkomt met die specifieke versie. Het is mogelijk dat het huidige configuratiebestand niet compatibel is met oudere softwareversies.


Vorbereiden en back-up maken van de SWA

Gebruik deze stappen om de benodigde bestanden en configuratie van de SWA te verzamelen voordat u terugkeert:


<p>Stap 1. Het configuratiebestand exporteren</p>	<p>Stap 1.1. Navigeer vanuit de GUI naar Systeembeheer en kies Configuratiebestand.</p> <p>Stap 1.2. Zorg ervoor dat Bestand downloaden naar lokale computer om te bekijken of op te slaan is geselecteerd.</p> <p>Stap 1.3. Kies Wachtwoorden coderen in de configuratiebestanden</p> <p>Stap 1.4. (Optioneel) Kies een naam voor het configuratiebestand.</p> <p>Stap 1.5. Klik op Indienen.</p>  <p>Afbeelding - Het configuratiebestand exporteren</p>
<p>Stap 2. Het decoderingscertificaat exporteren</p> <hr/> <p> Opmerking: Als de HTTPS-decodering is uitgeschakeld, gaat u verder met stap 3.</p>	<p>Stap 2.1. Navigeer vanuit de GUI naar Beveiligingsservices en klik op HTTPS-proxy.</p> <p>Stap 2.2. Klik op Instellingen bewerken.</p> <p>Stap 2.3. Download het HTTPS-decoderingscertificaat door te klikken op Certificaat downloaden... link.</p>



Afbeelding - HTTPS-decoderingscertificaat

 **Opmerking:** in dit voorbeeld worden beide typen HTTPS-decoderingscertificaten geïllustreerd. In uw netwerk kunt u echter slechts één type hebben geïmplementeerd.

Stap 3. De aangepaste basiscertificaten voor vertrouwen exporteren

 **Opmerking:** Als er geen aangepast vertrouwd rootcertificaat is toegevoegd aan de SWA, gaat u verder met stap 4.

Stap 3.1. Navigeer vanuit de GUI naar Netwerk en klik op Certificaatbeheer.

Stap 3.2. Klik in het gedeelte Certificaatbeheer op Vertrouwde basiscertificaten beheren.

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

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...](#)

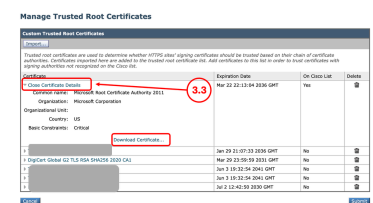
Certificate Based Authentication/RADSEC Root Certificates: 0 custom root certificates added to Certificate Based Authentication/RADSEC root certificate list [Manage Certificate Based Authentication/RADSEC Root Certificates...](#)

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

Image - Vertrouwde basiscertificaten beheren

Stap 3.3. Vouw elke aangepaste vertrouwde basiscertificaten uit door op hun naam te klikken en

op Certificaat downloaden...



Afbeelding - Vertrouwde basiscertificaten downloaden

Stap 4.1. Navigeer vanuit de GUI naar Netwerk en klik op Certificaatbeheer.

Stap 4.2. Klik in het gedeelte Toestelcertificaten op Certificaat exporteren.

Certificate Management

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	

Afbeelding - GUI-certificaat exporteren

Stap 4. Het GUI-certificaat exporteren

Opmerking: als u een ingebouwd GUI-certificaat gebruikt, gaat u naar stap 5.

Stap 5.1. Navigeer vanuit de GUI naar Netwerk en klik op Identity Services Engine.

Stap 5.2. Klik op Instellingen bewerken.

Stap 5.3. Download alle beschikbare certificaten.

Primary ISE pxGrid Node: [ISE1.amojarra.amojarra] (hostname or IP/v4 address)

ISE pxGrid Node Certificate: [Choose File] No file chosen [Upload File]

Common name: ISE1.amojarra.amojarra
Organization:
Organizational Unit:
Country:
Expiration Date: Mar 3 21:00:04 2027 GMT
Basic Constraints: Not Critical
[Download Certificate...]

Secondary ISE pxGrid Node (optional): [ISE2.amojarra.amojarra] (hostname or IP/v4 address)

ISE pxGrid Node Certificate: [Choose File] No file chosen [Upload File]

Common name: ISE2.amojarra.amojarra
Organization:
Organizational Unit:
Country:
Expiration Date: Mar 3 21:00:05 2027 GMT
Basic Constraints: Not Critical
[Download Certificate...]

Image - ISE-certificaten downloaden

Stap 5. De ISE-certificaten exporteren

Opmerking: Als er geen SWA-, ISE-integratie is, gaat u verder met stap 6.

Stap 6. Licenties / functies

Stap 6.1. Navigeer vanuit de GUI naar Systeembeheer en klik op Licenties of Functies afhankelijk van het type licentie dat u gebruikt.

Stap 6.2. Maak een screenshot van uw licenties / functies.

Stap 7. certificaat van echtheidswijziging

Stap 7.1. Navigeer vanuit de GUI naar Netwerk en klik op Verificatie.

Stap 7.2. Als de Credential Encryption is ingeschakeld, moet u het certificaat en de sleutel hebben.

Stap 7.3. Maak een screenshot van de huidige configuratie.

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: Block all traffic if authentication fails
Failed Authentication Handling: Log Guest User by: IP Address
Re-authentication: Disabled
Basic Authentication Token TTL: 3600

Authentication Settings

Credential Encryption: Enabled (7.2)
HTTPS Redirect Port: 443
Redirect Hostname: P1-SWA-Source.amojarra.amojarra (7.3)
Credential Cache Options: Surrogate Timeout: 3600 seconds
Client IP Idle Timeout: 3600 seconds
User Session Restrictions: Disabled
Header Based Authentication: Disabled

Secure Authentication Certificate:

Common name:	SWA Source Authentication Certificate
Organization:	Cisco
Organizational Unit:	SWA
Country:	US
Expiration Date:	Mar 3 20:31:36 2027 GMT
Basic Constraints:	Not Critical

[Edit Global Settings...](#)

Afbeelding - Authenticatiecertificaat



Opmerking: u kunt het verificatiecertificaat niet downloaden van de GUI.

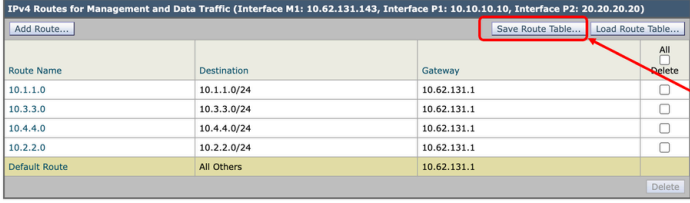
Stap 8. Statische routes exporteren




Opmerking: Als u van plan bent dezelfde netwerkconfiguratie en hetzelfde IP-adres te gebruiken voor de SWA van het doel, gaat u verder met stap 10.

Stap 8.1. Navigeer vanuit de GUI naar Netwerk en klik op Routes.

Stap 8.2. Klik voor elke routeringstabel op Routeringstabel opslaan.

	<p>Routes</p>  <p>Afbeelding - Routingstabel exporteren</p>
--	--



<p>Stap 9. DNS-instellingen</p> <p> Opmerking: Als u van plan bent dezelfde netwerkconfiguratie en hetzelfde IP-adres te gebruiken voor de SWA van het doel, gaat u verder met stap 10.</p>	<p>Stap 9.1. Navigeer vanuit de GUI naar Netwerk en klik op DNS.</p> <p>Stap 9.2. Maak een screenshot van de DNS-configuratie.</p>
--	--


De SWA terugdraaien

<p>Stap 10. De SWA terugdraaien</p>	<p>Stap 10.1. Verbinding maken met de CLI.</p> <p>Stap 10.2. Typ revert en druk op enter.</p> <p>Stap 10.3. Typ Y en druk op Enter voor "Wilt u doorgaan? [N]> "</p> <p>Stap 10.4. Typ Y en druk op Enter voor "Weet u zeker dat u wilt doorgaan? [N]>"</p> <p>Stap 10.5. Kies het nummer dat is gekoppeld aan de versie die u wilt terugzetten uit de lijst en druk op Enter.</p> <pre>SWA_CLI> revert</pre> <p>This command will revert the appliance to a previous version of AsyncOS.</p> <p>Warning: Reverting the appliance is extremely destructive. The following data will be destroyed in the process and should be backed up:</p> <ul style="list-style-type: none"> - current system configuration file - all log files - all reporting data (including saved scheduled and archived reports) - any custom end user notification pages <p>This command will try to preserve the current network settings.</p> <p>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>
--	--

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

Configuratie teruggedraaide SWA

Stap 11. Licentie voor de SWA	<p>Stap 11.1. Ga voor meer informatie naar: Beveiligde eerste configuratie van webapparatuur configureren.</p>
Stap 12. De wizard System Setup (Systeeminstellingen) uitvoeren	<p>Stap 12.1. Ga voor meer informatie naar: Beveiligde eerste configuratie van webapparatuur configureren.</p>
Stap 13. Aangepaste vertrouwde basiscertificaten importeren	<p>Stap 13.1. Navigeer vanuit de GUI naar Netwerk en klik op Certificaatbeheer.</p> <p>Stap 13.2. Klik in het gedeelte Certificaatbeheer op Vertrouwde basiscertificaten beheren.</p> <p>Stap 13.3. Klik op Import (Importeren).</p> <p>Stap 13.4. Upload de certificaten die eerder zijn gedownload in stap 3.</p>
 Opmerking: Als u geen aangepast vertrouwd basiscertificaat gebruikt, gaat u verder met stap 14.	 Let op: Wanneer zowel root- als intermediaire certificaten beschikbaar zijn, begint u met het uploaden van het root CA-certificaat. Na het indienen en vastleggen van de wijzigingen gaat u verder met het invoeren van het tussentijds certificaat.
Stap 14. Het configuratiebestand importeren	<p>Stap 14.1. Navigeer vanuit de GUI naar Systeembeheer en kies Configuratiebestand.</p>

 Let op: Zorg ervoor dat u het configuratiebestand importeert dat overeenkomt met uw huidige versie en niet met het configuratiebestand dat u hebt geëxporteerd in stap 1.

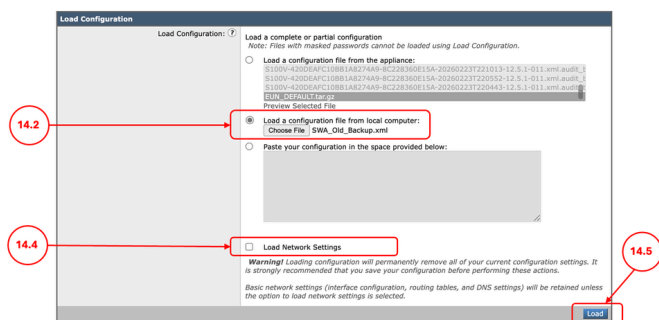
Stap 14.2. Selecteer in het gedeelte Configuratie laden de optie Een configuratiebestand laden vanaf de lokale computer.

Stap 14.3. Klik op Bestand kiezen en selecteer het XML-configuratiebestand dat betrekking heeft op de huidige versie.

Stap 14.4. (Optioneel) Als het IP-adres en de netwerkconfiguratie zijn verwijderd met de optie Retourneren, schakelt u het selectievakje Netwerkinstellingen laden in, anders selecteert u deze optie niet.

Stap 14.5. Klik op Laden.


Stap 14.6. Klik op Doorgaan in het pop-upvenster Configuratie laden bevestigen.



Afbeelding - Het oude configuratiebestand laden

Stap 14.7. Verbind de veranderingen.

Stap 15. De routes importeren

 Opmerking: Als u netwerkinstellingen laadt terwijl u de configuratie importeert, gaat u verder met stap 17.

Stap 15.1. Navigeer vanuit de GUI naar Netwerk en klik op Routes.

Stap 15.2. Klik voor elke routeringstabel op Routeringstabel laden.

Stap 15.3. Kies het bestand dat u hebt geëxporteerd in stap 8.


Stap 15.4. Klik op Indienen.

Stap 15.5. Verbind de veranderingen.

Stap 16. De DNS-instellingen

Stap 16.1. Navigeer vanuit de GUI naar Netwerk en klik op DNS.

configureren

 **Opmerking:** Als u netwerkinstellingen laadt terwijl u de configuratie importeert, gaat u verder met stap 17.

Stap 16.2. Klik op Instellingen bewerken.

Stap 16.3. Gebruik de screenshot van stap 9


Stap 16.4. Klik op Indienen.

Stap 16.5. Verbind de veranderingen.

Stap 17. De SWA toevoegen aan/opnieuw toevoegen aan de Active Directory

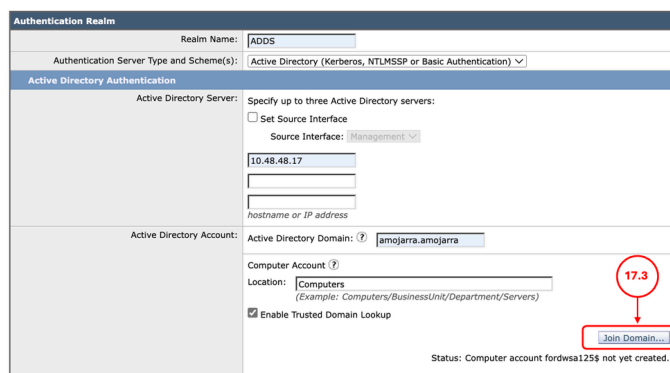
Stap 17.1. Navigeer vanuit de GUI naar Netwerk en klik op Verificatie.

Stap 17.2. Klik op de naam van de Authentication Realm Name.

 **Tip:** Als aan de SWA een nieuw IP-adres en een nieuwe hostnaam is toegewezen, moet u ervoor zorgen dat de benodigde DNS-records worden gemaakt in de Active Directory DNS-service.

Stap 17.3. Klik op Domein aanmelden en voer de referenties in:

Add Realm



Afbeelding - Deelnemen aan Active Directory

Stap 17.4. Klik op Indienen.

Stap 17.5. Als de Credential Encryption is ingeschakeld, importeert u het Secure Authentication Certificate.

Stap 17.6. Zorg ervoor dat de Redirect Hostname juist is.

Authentication

Authentication Realms						
Add Realm...						
Realm Name	Server Type	Schema(s)	Servers	Transparent User Identification	Base DN or NetBIOS Domain	Delete
ADDS	Active Directory	Kerberos, NTLMSSP, Basic	10.48.48.17	Not Enabled	AMQJARRA	

Global Authentication Settings	
Action if Authentication Service Unavailable:	Block all traffic if authentication fails
Failed Authentication Handling:	Log Guest User by: IP Address
Re-authentication:	Disabled
Basic Authentication Token TTL:	3600

Authentication Settings	
Credential Encryption:	Disabled
Redirect Hostname:	wsa-source.cisco.local
Credential Cache Options:	Surrogate Timeout: 3600 seconds Client IP Idle Timeout: 3600 seconds
User Session Restrictions:	Disabled
Header Based Authentication:	Enabled

[Edit Global Settings...](#)

Afbeelding - Authenticatie-instellingen

Stap 17.7. Verbind de veranderingen.

Gerelateerde informatie

- [Gebruikershandleiding voor AsyncOS 15.2 voor Cisco Secure Web Appliance](#)
- [Beveiligde eerste installatie van webtoestel](#)
- [Best practices voor veilige webapparaten gebruiken](#)
- [Toegang tot beveiligde logbestanden van webapparaten](#)

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.