

Configuratie tussen twee SWA's migreren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Voordat u begint](#)

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

[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 doel-SWA vorbereiden](#)

[Stap 10. De virtuele SWA installeren](#)

[Stap 11. Eerste SWA-configuratie](#)

[Stap 12. Het configuratiebestand reinigen](#)

[Het configuratiebestand importeren naar doel-SWA](#)

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

[Stap 14. Het configuratiebestand importeren](#)

[Stap 15. Het beheerderswachtwoord wijzigen](#)

[Stap 16. plegen](#)

[Stap 17. Importeren van routes](#)

[Stap 18. De DNS-instellingen configureren](#)

[Stap 19. De SWA toevoegen aan/opnieuw toevoegen aan de Active Directory](#)

[Stap 20. Opnieuw lid worden van SMA](#)

[Fouten herstellen](#)

[Fout bij parseren van element port_name](#)

[Fout bij parseren van element ise_service](#)

[Failover werkt niet op nieuwe virtuele SWA](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft het proces van het terugzetten van de configuratie van een Secure Web Appliance (SWA) naar een andere.

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- Toegang tot grafische gebruikersinterface (GUI) van SWA
- Administratieve toegang tot de SWA
- Administratieve toegang tot het Security Management Appliance (SMA)
- 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

In dit artikel beschrijven we de stappen voor migratie van de SWA-bron naar de SWA-doelomgeving. Deze tabel bevat de specificaties voor elk systeem.

	Bron SWA	Doel-SWA
Model	S396	S100v
Versie	15.5.0-710	15.5.0-710
Licentie	Slimme licentie	Slimme licentie
Active Directory	verenigd	verenigd
Geïntegreerd met Identity Services Engine (ISE)	Ja	Ja

Aantal netwerkinterfacekaarten (NIC)	5	5
HTTPS-decodering	Ingeschakeld met zelfondertekend certificaat	Ingeschakeld met zelfondertekend certificaat
transparante omleiding	WCCP	WCCP
Beheerd door SMA	Ja	Ja
Externe logboekserver	SCP-push	SCP-push
Hoge beschikbaarheid	Ingeschakeld	Ingeschakeld

 **Opmerking:** zorg er altijd voor dat bij de installatie van een nieuwe virtuele SWA alle netwerkinterfaces die door Cisco worden aanbevolen, aanwezig zijn en zijn geconfigureerd op de virtuele machine (VM). De interfaces kunnen losgekoppeld blijven, maar ze moeten beschikbaar zijn binnen de VM.

Er zijn twee mogelijke scenario's bij het migreren van de SWA van het ene apparaat naar het andere:

[Scenario-1] De bestaande SWA vervangen: de oorspronkelijke SWA wordt buiten bedrijf gesteld en het IP-adres van de doelSWA is hetzelfde als de bron SWA.

[Scenario-2] Een nieuwe SWA toevoegen: de oorspronkelijke SWA blijft in gebruik terwijl de nieuwe SWA is geconfigureerd.

Vorbereiden en back-up maken van de SWA-broncode

Gebruik deze stappen om de benodigde bestanden en configuratie te verzamelen van de SWA-bron:

Stap 1. Het configuratiebestand exporteren	Stap 1.1. Navigeer vanuit de GUI naar Systeembeheer en kies Configuratiebestand. Stap 1.2. Zorg ervoor dat Bestand downloaden naar lokale computer om te bekijken of op te slaan is geselecteerd. Stap 1.3. Kies Wachtwoorden coderen in de configuratiebestanden
--	--

Stap 1.4. (Optioneel) Kies een naam voor het configuratiebestand.

Stap 1.5. Klik op Indienen.

Configuration File

Configuration File

Current Configuration

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.

Submit

Afbeelding - Het configuratiebestand exporteren

Stap 2.1. Navigeer vanuit de GUI naar Beveiligingsservices en klik op HTTPS-proxy.

Stap 2.2. Klik op Instellingen bewerken.

Stap 2.3. Download het HTTPS-decoderingscertificaat door te klikken op Certificaat downloaden... link.

HTTPS Proxy Settings

☒ Enable HTTPS Proxy

HTTPS Ports to Proxy:

Root Certificate for Signing: ☐ Use Uploaded Certificate and Key ☐ Use Generated Certificate and Key

Uploaded Certificate and Key:

Certificate: No file chosen

Key: No file chosen

Key is Encrypted

Common name:

Organization:

Organizational Unit:

Country:

Expiration Date:

Basic Constraints:

Use Generated Certificate and Key:

Common name:

Organization:

Organizational Unit:

Country:

Expiration Date:

Basic Constraints:

Signed Certificate:

To use a signed certificate, first download a certificate signing request using the link above. Submit the request to a certificate authority, and when you receive the signed certificate, upload it using the field below.

Certificate: No file chosen

Afbeelding - HTTPS-decoderingscertificaat

Stap 2. Het decoderingscertificaat exporteren

 Opmerking: Als de HTTPS-decodering is uitgeschakeld, gaat u verder met stap 3.

 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

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

exporteren

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

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

Certificate FQDN Validation 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.

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...

3.2

Image - Vertrouwde basiscertificaten beheren

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

Manage Trusted Root Certificates

Cisco Trusted Root Certificates

Trusted root certificates are used to determine whether HTTP(S) client signing certificates should be trusted based on their chain of certificate authorities. Certificates associated here are added to the trusted root certificate list. All certificates in this list enable for root certificates only. Signing certificates are not added here and are not used for client signing.

Certificate	Expiration Date	On Close List	Delete
Open Certificate Details Common Name: Microsoft Root Certificate Authority 2011 Organization: Microsoft Corporation Country: US Basic Constraints: Critical Download Certificate	Mar 22 22:23:04 2036 GMT	Yes	
1	Jan 29 21:07:33 2036 GMT	No	
2	Mar 22 22:23:04 2036 GMT	No	
3	Jan 29 21:07:33 2036 GMT	No	
4	Jan 29 21:07:33 2036 GMT	No	
5	Jan 29 21:07:33 2036 GMT	No	

3.3

op Certificaat downloaden...

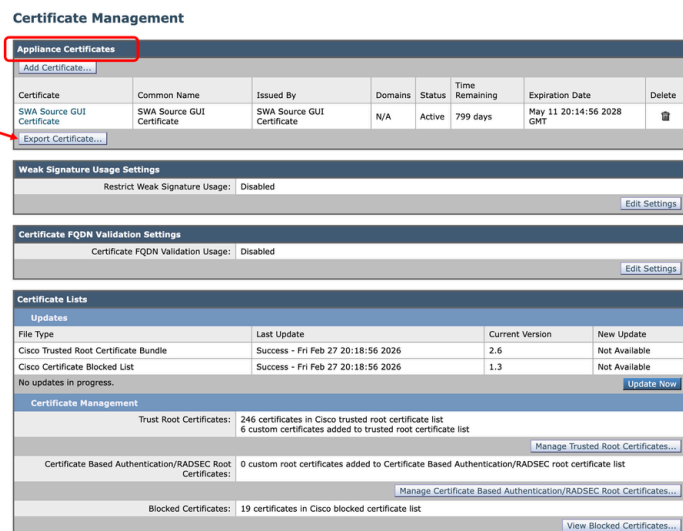
Afbeelding - Vertrouwde basiscertificaten downloaden

Stap 4. Het GUI-certificaat exporteren

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

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

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



Afbeelding - GUI-certificaat exporteren

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.

Stap 5. De ISE-certificaten exporteren

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

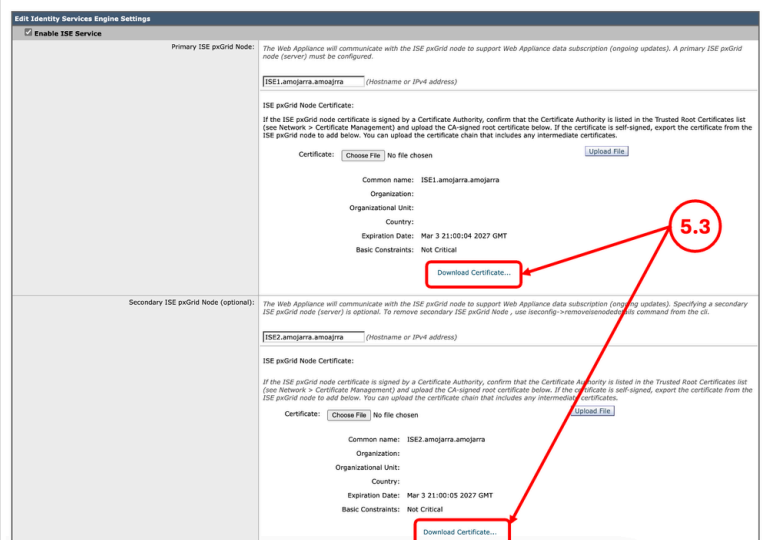


Image - ISE-certificaten downloaden

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.

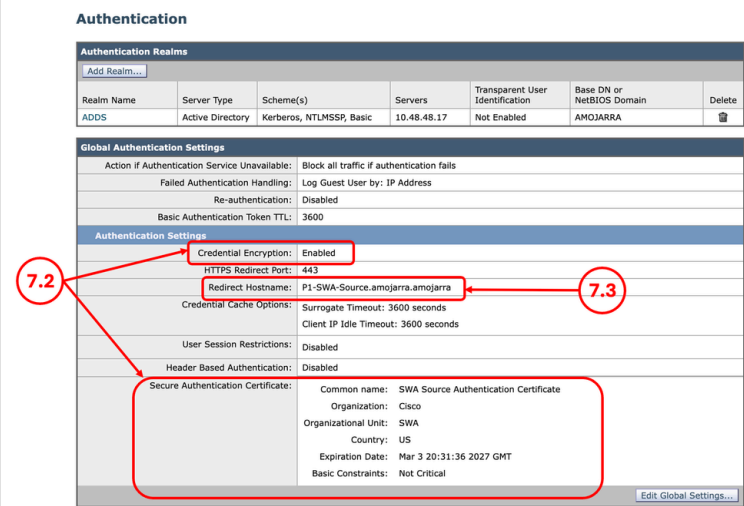
Stap 6.2. Maak een screenshot van uw licenties / functies.

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.



Afbeelding - Authenticatiecertificaat

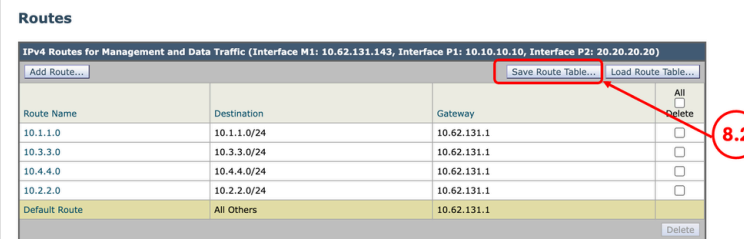
 Opmerking: u kunt het verificatiecertificaat niet downloaden van de GUI.

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 routingstabel op Routingstabel opslaan.



Afbeelding - Routingstabel exporteren

Stap 9. DNS-instellingen

Stap 9.1. Navigeer vanuit de GUI naar Netwerk en klik op DNS.

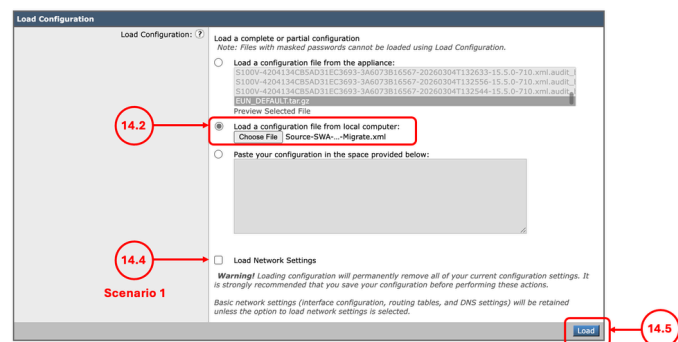
 Opmerking: Als u van plan bent dezelfde netwerkconfiguratie en hetzelfde IP-adres te gebruiken voor de SWA van het doel, gaat u verder met stap 10.	Stap 9.2. Maak een screenshot van de DNS-configuratie.
---	--

De doel-SWA voorbereiden

Stap 10. De virtuele SWA installeren	Stap 10.1. Gebruik deze handleidingen om de virtuele SWA te installeren: • Secure Web Appliance installeren op VMware ESXi • Secure Web Appliance installeren op Microsoft Hyper-V
 Opmerking: als de doel-SWA fysiek is, kunt u overslaan naar stap 11.	Stap 10.2. Zorg ervoor dat de nieuwe SWA de aanbevolen netwerktoegang heeft: • Firewall configureren voor Secure Web Appliance
Stap 11. Eerste SWA-configuratie	Stap 11.1. Het IP-adres configureren. Stap 11.2. Configureer de standaardgateway. Stap 11.3. De DNS-server configureren. Stap 11.4. Geef het apparaat een licentie. Stap 11.5. Schakel de functies in. Stap 11.6. Voer de wizard Systeeminstellingen uit. U kunt de gedetailleerde stappen in dit artikel vinden: Eerste installatie van Secure Web Appliance
Stap 12. Het configuratiebestand reinigen	Stap 12.1. Bekijk de sectie Fouten herstellen in dit artikel om de ISE-certificaatconfiguratie uit het XML-back-upbestand te verwijderen.
 Opmerking: Als u ISE niet integreert met de SWA, kunt u overslaan naar stap 13.	

Het configuratiebestand importeren naar doel-SWA

Stap 13. Aangepaste vertrouwde basiscertificaten importeren	Stap 13.1. Navigeer vanuit de GUI naar Netwerk en klik op Certificaatbeheer. Stap 13.2. Klik in het gedeelte Certificaatbeheer op Vertrouwde basiscertificaten beheren. Stap 13.3. Klik op Import (Importeren). Stap 13.4. Upload de certificaten die eerder zijn gedownload in stap 3.
 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	

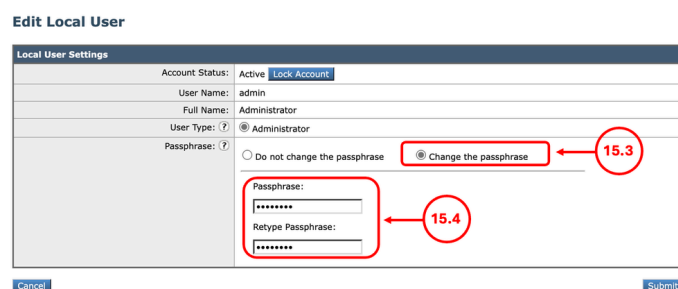


Afbeelding - De configuratie importeren

Stap 15. Het beheerderswachtwoord wijzigen

 Opmerking: als u het SWA-beheerderswachtwoord voor de bron hebt, gaat u naar stap 16.

- 15.1. Navigeer vanuit de GUI naar Systeembeheer en kies Gebruikers.
- 15.2. Klik op de Admin gebruikersnaam.
- 15.3. Selecteer Wachtwoordgroep wijzigen.
- 15.4. Voer het wachtwoord in.
- 15.5. klik op Indienen.



Afbeelding - Admin-wachtwoord wijzigen

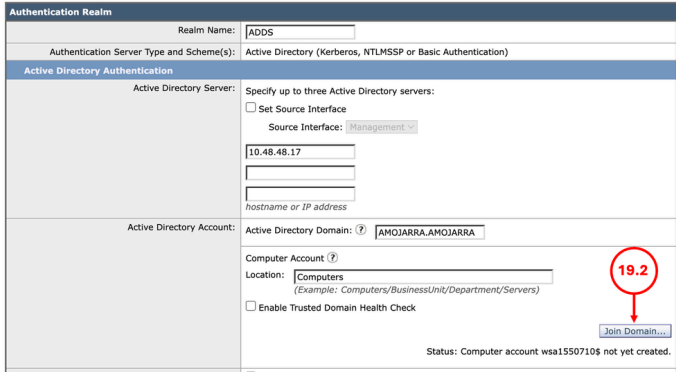
Stap 16. plegen

- Stap 16.1. Nu kunt u de wijzigingen vastleggen.

Stap 17. Importeren van routes

 Opmerking: Als u netwerkinstellingen laadt terwijl u de configuratie importeert, gaat u verder met stap 19.

- Stap 17.1. Navigeer vanuit de GUI naar Netwerk en klik op Routes.
- Stap 17.2. Klik voor elke routingstabel op Routingstabel laden.
- Stap 17.3. Kies het bestand dat u hebt geëxporteerd in stap 8.
- Stap 17.4. Klik op Indienen.
- Stap 17.5. Verbind de veranderingen.

Stap 18. De DNS-instellingen configureren  Opmerking: Als u netwerkinstellingen laadt terwijl u de configuratie importeert, gaat u verder met stap 19.	Stap 18.1. Navigeer vanuit de GUI naar Netwerk en klik op DNS. Stap 18.2. Klik op Instellingen bewerken. Stap 18.3. Gebruik de screenshot van stap 9 Stap 18.4. Klik op Indienen. Stap 18.5. Verbind de veranderingen.
Stap 19. De SWA toevoegen aan/opnieuw toevoegen aan de Active Directory	Stap 19.1. Navigeer vanuit de GUI naar Netwerk en klik op Verificatie. Stap 19.2. klik op de naam van de domeinnaam voor verificatie.  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 19.2. Klik op Domein aanmelden en voer de referenties in: Edit Realm  Afbeelding - Deelnemen aan Active Directory-domein Stap 19.3. Klik op Indienen. Stap 19.4. Zorg ervoor dat de Redirect Hostname juist is. Stap 19.5. Als de Credential Encryption is ingeschakeld, controleert u of het Secure Authentication Certificate juist is.

Authentication

Authentication Realms						
Add Realm...						
Realm Name	Server Type	Scheme(s)	Servers	Transparent User Identification	Base DN or NetBIOS Domain	Delete
ADOS	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
HTTPS Redirect Port:	443
Redirect Hostname:	P1-SWA-Source.amojarra.amojarra
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 - Authenticatie-instellingen

Stap 19.6. Verbind de veranderingen.



Opmerking: Als u de bestaande SWA (Scenario-2) niet hebt vervangen en de gemigreerde SWA geen nieuw IP-adres heeft, voegt u de SWA als een nieuw apparaat toe aan SMA en slaat u stap 20 over.

Stap 20. Opnieuw lid worden van SMA



Opmerking: Als de SWA niet door SMA wordt beheerd, slaat u deze stap over.

Stap 20.1. Maak verbinding met de CLI van de SMA.

Stap 20.2. voer logconfig uit.

Stap 20.3. Voer HOSTKEYCONFIG in.

Stap 20.4. Typ DELETE en druk op Enter.

Stap 20.5. Typ het nummer dat is gekoppeld aan de SWA die onlangs is gemigreerd en druk op Enter totdat de wizard is voltooid.

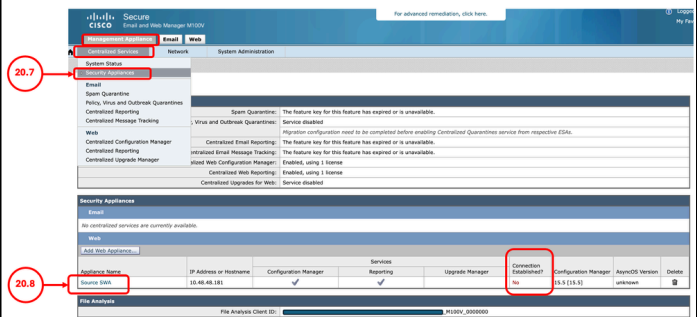
Stap 20.6. Typ commit en druk op Enter om de wijzigingen op te slaan.

Stap 20.7. Navigeer vanuit de SMA GUI naar Management Appliance. Selecteer Gecentraliseerde services en klik op Beveiligingstoestellen.

Stap 20.8. klik op de naam van de SWA die onlangs is gemigreerd.



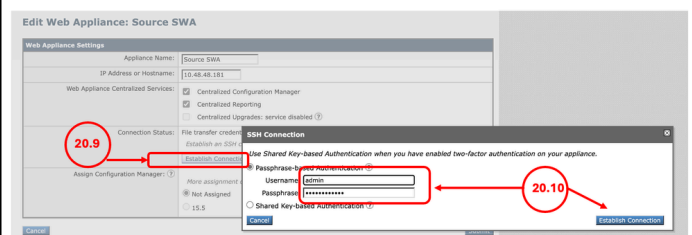
Tip: u kunt zien dat de kolom Verbinding tot stand is ingesteld op Nee.



Afbeelding - Toestelstatus SMA-beveiliging

Stap 20.9. klik op Verbinding tot stand brengen.

Stap 20.10. Voer de gebruikersnaam en wachtwoordgroep in en klik op Verbinding maken.



Afbeelding - Verbinding tot stand brengen met de SWA

Stap 20.11. Wijs de configuratiebeheerder toe.

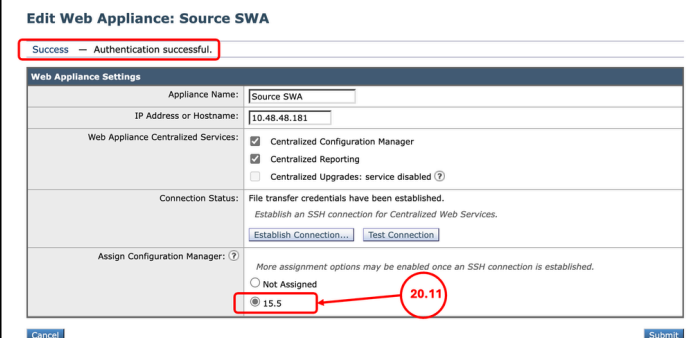


Image - Configuratiebeheer toewijzen

Stap 20.12. Verzenden en vastleggen van de wijzigingen.

Stap 20.13. (Optioneel) u kunt testen door de configuratie naar de SWA te publiceren.



Tip: De SMA bewaart alle rapportage- en trackinggegevens van de vorige SWA.

Fouten herstellen

Fout bij parseren van element port_name

De naam van de netwerkpoort moet een van de volgende zijn: ['Beheer', 'P1', 'P2', 'T1', 'T2']:

Configuration File

Error — Configuration File was not loaded. Parse Error on element "port_name" line number 85 column 18 with value "M2": The network port name must be one of ['Management', 'P1', 'P2', 'T1', 'T2'] (with optional "_v6" suffix), or start with "VLAN" or "Loopback".

Afbeelding - Naamgevingsfout netwerkinterface

Error — Configuration File was not loaded. Parse Error on element "port_name" line number 85 column 18 with value "M2": The network port name must be one of ['Management', 'P1', 'P2', 'T1', 'T2'] (with optional "_v6" suffix), or start with "VLAN" or "Loopback".

Deze fout treedt op wanneer u van fysiek SWA naar virtueel migreert. de virtuele SWA heeft slechts 5 NIC's en de M2-interface is ongeldig. Als u de fout wilt herstellen, bewerkt u het XML-configuratiebestand in een teksteditor en verwijdt u de volgende regels:

M2

M2

M2

autoselect

aa:bb:cc:00:00:00

Fout bij parseren van element ise_service

Configuration File

Error — Configuration File was not loaded. Parse Error on element "ise_service" line number 548 column 17:
b4Y4mw.crt.pem ISE certificate not present in /data/db/isecerts/.

Afbeelding - ISE-certificaatfout

Error - Configuration File was not loaded. Parse Error on element "ise_service" line number 548 column 17:

Aangezien de ISE-certificaten niet zijn opgenomen in de SWA-exportconfiguratie en rechtstreeks op het apparaat worden geüpload, moet u de certificaatconfiguratie uit het XML-bestand verwijderen en na succesvolle import ISE handmatig configureren. om dit probleem op te lossen, bewerkt u het XML-configuratiebestand in de teksteditor en zoekt u in de fout naar de

certificaatnaam (in dit voorbeeld zoekt u naar AA11AA) en verwijdt u deze uit het configuratiebestand:

Before:

AA11AA

BB22BB

After:

Naast de naam van het certificaat moet u ook de naam van het clientcertificaat van het webtoestel verwijderen.

In dit voorbeeld is het Web Appliance Client Certificate een zelf ondertekend certificaat:

Before:

1

xAcK6T

After:

Failover werkt niet op nieuwe virtuele SWA

Als de High Availability (Failover) niet werkt op de virtuele SWA van het doel, moet u ervoor zorgen dat de hypervisor correct is geconfigureerd. Ga voor meer informatie naar: [Zorg voor de juiste functionaliteit van de virtuele WSA HA-groep in een VMware-omgeving](#)

Gerelateerde informatie

- [Gebruikershandleiding voor AsyncOS 15.2 voor Cisco Secure Web Appliance](#)
- [Secure Web Appliance installeren op VMware ESXi](#)
- [Secure Web Appliance installeren op Microsoft Hyper-V](#)
- [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](#)
- [Firewall configureren voor Secure Web Appliance](#)
- [Decryptiecertificaat configureren in Secure Web Appliance](#)
- [Problemen oplossen met de DNS-service van een beveiligd webapparaat](#)
- [Zorgen voor de juiste functionaliteit van de virtuele WSA HA-groep in een VMware-omgeving](#)

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.