# Decryptiecertificaat configureren in beveiligd webtoestel

## Inhoud


Inleiding

Voorwaarden

- Vereisten
- Gebruikte componenten

HTTPS-decodering

Decryptiecertificaat configureren in SWA

- Upload een basiscertificaat en sleutel
- Een certificaat en sleutel voor de HTTPS-proxy genereren

invoercertificaat

- Upstream Proxy Certificate importeren naar SWA
- SWA-certificaat importeren naar een andere SWA
- SWA-certificaat importeren in Windows-client
- SWA-certificaat importeren in Mac-client
- SWA-certificaat importeren in Ubuntu/Debian
- SWA-certificaat importeren in CentOS 6
- SWA-certificaat importeren in CentOS 5
- SWA-certificaat importeren in Mozilla Firefox
- SWA-certificaat importeren in Google Chrome
- SWA-certificaat importeren in Microsoft Edge/Internet Explorer
- SWA-certificaat importeren in Safari
- SWA-certificaat importeren van groepsbeleid naar klanten

Gerelateerde inhoud


## Inleiding

In dit document worden de stappen beschreven voor het configureren van HTTPS-coderingscertificaten in Secure Web Appliances (SWA)- en Proxy-clients.

---

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Administratieve toegang tot SWA
- Toegang tot de grafische gebruikersinterface (GUI) 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.

---

## HTTPS-decodering

De SWA Hypertext Transfer Protocol Secure (HTTPS) decryptie maakt gebruik van root certificaten en private key bestanden die u uploadt naar het toestel om het verkeer te versleutelen. Het basiscertificaat en de privésleutelbestanden die u naar het toestel uploadt, moeten in PEM-indeling zijn.

---

Opmerking: DER-indeling wordt niet ondersteund.

---

U kunt ook een tussenliggend certificaat uploaden dat door een basiscertificeringsinstantie is ondertekend. Wanneer SWA een certificaat maakt dat het servercertificaat vertegenwoordigt, verzendt het het geüploade certificaat samen met het nagebootste certificaat naar de clienttoepassing. Op die manier vertrouwt de toepassing het nagemaakte servercertificaat, zolang het tussenliggende certificaat is ondertekend door een basiscertificeringsinstantie (CA) die de clienttoepassing vertrouwt.

---

## Decryptiecertificaat configureren in SWA

De SWA kan een bestaand certificaat en private key gebruiken voor HTTPS-decryptie. Er kan echter verwarring ontstaan over het type certificaat dat moet worden gebruikt, omdat niet alle x.509-certificaten werken.

Er zijn twee belangrijke soorten certificaten: servercertificaten en basiscertificaten. Alle x.509-certificaten bevatten een veld Basisbeperkingen, waarin het type certificaat wordt aangegeven:

- Onderwerptype=Eindentiteit - Servercertificaat
- Onderwerp Type=CA - Root Certificate

---

## Upload een basiscertificaat en sleutel

Stap 1. Navigeer vanuit de GUI naar Security Services en kies HTTPS Proxy.
Stap 2. Klik op Instellingen bewerken.
Stap 3. Klik op Geüpload certificaat en sleutel gebruiken.
Stap 4. Klik op Bladeren in het veld Certificaat om naar het certificaatbestand op het lokale systeem te navigeren.

---



Opmerking: als het bestand dat u uploadt meerdere certificaten of sleutels bevat, gebruikt de webproxy het eerste certificaat of de eerste sleutel in het bestand.

---

Stap 5. Klik op Bladeren in het veld Toets om naar het bestand met de privésleutel te navigeren.

---



Opmerking: de sleutellengte moet 512, 1024 of 2048 bits zijn.

---

Stap 6. Selecteer Sleutel is versleuteld als de sleutel versleuteld is.
Stap 7. Klik op Bestanden uploaden om het certificaat en de belangrijkste bestanden naar het beveiligde webtoestel over te brengen. De geüploade certificaatgegevens worden weergegeven op de pagina HTTPS-proxyinstellingen bewerken.
Stap 8. (Optioneel) Klik op Certificaat downloaden om de clienttoepassingen op het netwerk over te zetten.

Stap 9. Wijzigingen verzenden en vastleggen.

---

## Een certificaat en sleutel voor de HTTPS-proxy genereren

Stap 1. Navigeer vanuit de GUI naar Security Services en kies HTTPS Proxy.
Stap 2. Klik op Instellingen bewerken.
Stap 3. Kies Gegenereerd certificaat en sleutel gebruiken.
Stap 4. Klik op Nieuw certificaat en nieuwe sleutel genereren.
Stap 5. Voer in het dialoogvenster Certificaat en sleutel genereren de informatie in die in het basiscertificaat moet worden weergegeven. U kunt elk ASCII-teken invoeren, behalve de voorwaartse slash (/) in het veld Algemene naam.
Stap 6. Klik op Genereren.
Stap 7. De gegenereerde certificaatgegevens worden weergegeven op de pagina HTTPS-proxyinstellingen bewerken.
Stap 8. (Optioneel) Klik op Certificaat downloaden, zodat u het kunt overbrengen naar de clienttoepassingen op het netwerk.
Stap 9. (Optioneel) Klik op de link Certificaatondertekeningsaanvraag downloaden, zodat u het Certificaatondertekeningsverzoek (CSR) kunt indienen bij een CA.
Stap 10. (Optioneel) Upload het ondertekende certificaat naar het Secure Web Appliance nadat u het van de CA hebt ontvangen. U kunt dit op elk moment doen nadat u het certificaat op het apparaat hebt gegenereerd.
Stap 11. Wijzigingen verzenden en vastleggen.

---

# invoercertificaat

## Upstream Proxy Certificate importeren naar SWA

Als SWA is geconfigureerd om een upstream-proxy te gebruiken en de upstream-proxy is geconfigureerd voor HTTPS-decodering, moet u het upstream-proxycoderingscertificaat importeren naar SWA. U kunt de lijst met vertrouwde certificaten beheren en er certificaten aan toevoegen en er certificaten functioneel uit verwijderen.

Stap 1. Kies in de GUI Netwerk en kies Certificaatbeheer.
Stap 2. Klik op de pagina Certificaatbeheer op Vertrouwde basiscertificaten beheren.
Stap 3. Als u een aangepast vertrouwd basiscertificaat met ondertekeningsbevoegdheid wilt toevoegen, niet in de lijst met Cisco-herkenningen, klikt u op Importeren en dient u het certificaatbestand in.

Stap 4. Wijzigingen verzenden en vastleggen.

---

## SWA-certificaat importeren naar een andere SWA

Als u het HTTPS-certificaat en de sleutel in één SWA voor HTTPS-proxy hebt geüpload en de

oorspronkelijke bestanden toegankelijk zijn, kunt u deze vanuit het configuratiebestand importeren naar een andere SWA.

Stap 1. Kies in de GUI van beide SWA's Systeembeheer en klik op Configuratiebestand.

Stap 2. Klik op Bestand downloaden op de lokale computer om het bestand te bekijken of op te slaan.

Stap 3. Kies Wachtwoorden versleutelen in de configuratiebestanden.

Stap 4. (Optioneel) Kies Een door de gebruiker gedefinieerde bestandsnaam gebruiken en voeg de gewenste naam toe aan het configuratiebestand.

Stap 5. Klik op Indienen onder de huidige configuratie om het bestand configuratie.xml te downloaden.

Stap 6. Open gedownloade bestanden met teksteditors of XML-editors.

Stap 7. Kopieer deze tags van SWA met het certificaat, kopieer alle gegevens in de tags en vervang ze in het configuratiebestand van de andere SWA:

```
<prox_config_signing_cert_name>....</prox_config_signing_cert_name>
<prox_config_uploaded_cert_name>....</prox_config_uploaded_cert_name>
<prox_config_uploaded_cert>....</prox_config_uploaded_key>
<prox_config_uploaded_key>....</prox_config_uploaded_key>
```

---

Stap 8. Sla de wijzigingen op in het .xml-bestand van de SWA van bestemming.

Stap 9. Als u het bewerkte .xml-configuratiebestand wilt importeren naar de SWA van de bestemming, kiest u Systeembeheer en klikt u op Configuratiebestand.

Stap 10. Klik in het gedeelte Configuratie laden op Configuratiebestand laden vanaf lokale computer.

Stap 11. Klik op Bestand kiezen en kies het bewerkte .xml configuratiebestand.

Stap 12. Klik op Laden om het nieuwe configuratiebestand te importeren met het certificaat en de sleutel.

Stap 13. Wijzig wijzigingen als het systeem u daarom vraagt.

---

## SWA-certificaat importeren in Windows-client

Ga als volgt te werk om het SWA HTTPS-proxycertificaat te importeren als vertrouwd in clientcomputers met het Microsoft Windows-besturingssysteem:

Stap 1. Klik op Start op de taakbalk en typ Computercertificaten beheren.
Stap 2. Vouw op de pagina Certificaten-lokale computer de Trusted Root Certification (Vertrouwde basiscertificering) uit en klik met de rechtermuisknop op de map Certificaten.
Stap 3. Klik op Alle taken en kies Importeren.
Stap 4. Klik op de pagina Wizard Certificaat importeren op Volgende.
Stap 5. Als u het SWA-certificaatbestand wilt importeren, klikt u op Bladeren en kiest u het certificaat dat u van SWA hebt gedownload.

---



Tip: Als u het SWA-certificaat wilt downloaden, raadpleegt u Stap 8 in het gedeelte Een basiscertificaat en -sleutel uploaden of Een certificaat en sleutel voor de HTTPS-proxy genereren.

---

Stap 6. Klik op Alle certificaten plaatsen in het volgende selectievakje.
Stap 7. Kies Trusted Root Certification Authorities en klik op Volgende.
Stap 8. Klik op Finish (Voltooien).

U kunt deze opdracht ook uitvoeren om het certificaat te importeren naar Trusted Root Certification Authorities.

```
certutil -addstore -f "ROOT" <Path to SWA Certificate/CertificateName.crt>
```

---



Opmerking: U moet <Pad naar SWA Certificate/CertificateName.crt> vervangen door uw huidige gedownloade certificaatpad en bestandsnaam.

---

## SWA-certificaat importeren in Mac-client

Stap 1. Download het HTTPS-proxycertificaat van SWA naar de Mac OS-client.
Stap 2. Wijzig de bestandsextensie in .crt.

Stap 3. Voer deze opdracht uit om het certificaat te importeren als een vertrouwd certificaat:

```
sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain <Path to SWA Certi
```



Opmerking: u moet het vervangen door uw huidige gedownloade certificaatpad en bestandsnaam.

## SWA-certificaat importeren in Ubuntu/Debian

Stap 1. Download het HTTPS Proxy certificaat van SWA.
Stap 2. Open het certificaatbestand in de teksteditor en kopieer alle inhoud.
Stap 3. Maak een nieuw bestand in /usr/local/share/ca-certificates/ met een .crt als extensie.
Stap 4. Bewerk het bestand met de gewenste teksteditor en plak gekopieerde tekst in het nieuwe bestand en sla op.
Stap 5. Voer deze opdracht uit om de certificaten in het besturingssysteem te vernieuwen.

```
sudo update-ca-certificates
```



Tip: Als u het certificaat lokaal op de client hebt opgeslagen, kunt u het certificaat kopiëren naar /usr/local/share/ca-certificaten/ en sudo update-ca-certificaten uitvoeren.



Opmerking: In sommige versies moet u het ca-certificatenpakket installeren met deze opdracht: sudo apt-get install -y ca-certificaten.

## SWA-certificaat importeren in CentOS 6

Stap 1. Download het HTTPS Proxy certificaat van SWA.
Stap 2. Open het certificaatbestand in de teksteditor en kopieer alle inhoud in het bestand.
Stap 3. Maak een nieuw bestand in /etc/pki/ca-trust/source/anchors/ met een .crt extensie.
Stap 4. Bewerk het bestand met de gewenste teksteditor en gekopieerde tekst uit het verleden in het nieuwe bestand en sla het op.
Stap 5. Installeer het ca-certificatenpakket:

```
yum install ca-certificates
```

---

Stap 6. Voer deze opdracht uit om de certificaten in het besturingssysteem te vernieuwen:

```
update-ca-trust extract
```

---



Tip: Als u het certificaat lokaal op de client hebt opgeslagen, kunt u het certificaat kopiëren naar /etc/pki/ca-trust/source/anchors/ en update-ca-trust-extract uitvoeren nadat u de ca-certificaten hebt geïnstalleerd.

---

## SWA-certificaat importeren in CentOS 5

Stap 1. Download het HTTPS Proxy certificaat van SWA.
Stap 2. Open het certificaatbestand in de teksteditor en kopieer alle inhoud in het bestand.
Stap 3. Maak een nieuw bestand in de huidige map met een .crt extensie (bijvoorbeeld SWA.crt).
Stap 4. Bewerk de /etc/pki/tls/certs/ca-bundle.crt met de gewenste teksteditor, plak de gekopieerde tekst aan het einde van het bestand en sla op.

---



Tip: Als u het certificaat lokaal op de client hebt opgeslagen (in dit voorbeeld is de bestandsnaam SWA.crt), kunt u het certificaat toevoegen met deze opdracht: cat SWA.crt >>/etc/pki/tls/certs/ca-bundle.crt.

---

## SWA-certificaat importeren in Mozilla Firefox

Stap 1. Download het HTTPS Proxy Certificate van SWA.
Stap 2. Wijzig de bestandsextensie in .crt.
Stap 3. Open Firefox en klik op het menu (drie balken rechtsboven).
Stap 4. Kies Instellingen (in sommige versies zijn het Opties).
Stap 5. Klik in het linkermenu op Privacy en beveiliging en blader naar Certificaten.
Stap 6. Klik op Certificaten weergeven.
Stap 7. Klik op het tabblad Autoriteiten en vervolgens op Importeren.
Stap 8. Kies het certificaatbestand en klik op Openen.
Stap 9. Klik op OK.

---

## SWA-certificaat importeren in Google Chrome

Stap 1. Download het HTTPS Proxy Certificate van SWA.
Stap 2. Wijzig de bestandsextensie in .crt.
Stap 3. Open Google Chrome en klik op Google Chrome aanpassen en besturen (drie stippen in de rechterbovenhoek).
Stap 4. Kies Instellingen.
Stap 5. Klik op Privacy en beveiliging in het menu aan de linkerkant.
Stap 6. Kies Beveiliging.
Stap 7. Blader naar Certificaten beheren en klik op de knop rechts.
Stap 8. Kies het tabblad Vertrouwde basiscertificeringsinstanties en klik op Importeren.
Stap 9. Kies het certificaatbestand en klik op Openen.
Stap 10. Klik op OK.

---



Opmerking: Als u het SWA-certificaat in het besturingssysteem installeert, vertrouwt Google Chrome dat certificaat en hoeft u het certificaat niet afzonderlijk in uw browser te importeren.

---

## SWA-certificaat importeren in Microsoft Edge/Internet Explorer

Microsoft Edge en Internet Explorer (IE) gebruiken besturingssysteemcertificaten. Als u het SWA-certificaat in het besturingssysteem installeert, hoeft u het certificaat niet afzonderlijk in uw browser te importeren.

---

## SWA-certificaat importeren in Safari

Stap 1. Download het HTTPS Proxy certificaat van SWA.
Stap 2. Wijzig de bestandsextensie in .crt.
Stap 3. Selecteer in het Launchpad Keychain Access.
Stap 4. Klik in het menu Bestand op Sleutelhanger toevoegen.
Stap 5. Kies het SWA-certificaatbestand en klik op Toevoegen.
Stap 6. Kies Beveiliging.
Stap 7. Blader naar Certificaten beheren en klik op de knop rechts.
Stap 8. Kies het tabblad Vertrouwde basiscertificeringsinstanties en klik op Importeren.
Stap 9. Kies het certificaatbestand en klik op Openen.
Stap 10. Klik op OK.

---

### SWA-certificaat importeren van groepsbeleid naar klanten

Ga als volgt te werk om certificaten te distribueren naar clientcomputers volgens het groepsbeleid vanuit Active Directory:

Stap 1. Download het HTTPS Proxy certificaat van SWA.
Stap 2. Wijzig de bestandsextensie in .crt.
Stap 3. Kopieer het certificaatbestand naar de domeincontroller.
Stap 4. Klik op de domeincontroller op Start en open de module Groepsbeleidsbeheer.
Stap 5. Zoek het gewenste Group Policy Object (GPO) of maak een nieuwe GPO om het SWA-certificaat te bevatten dat moet worden geïmporteerd naar de client.
Stap 6. Klik met de rechtermuisknop op GPO en klik op Bewerken.
Stap 7. Ga in het menu aan de linkerkant naar Computerconfiguratie > Beleid > Windows-instellingen > Beveiligingsinstellingen > Beleid voor openbare sleutels.
Stap 8. Klik met de rechtermuisknop op de vertrouwde basiscertificeringsinstanties en klik op Importeren.
Stap 9. Klik op Volgende op de pagina Welkom bij de wizard Certificaat importeren.
Stap 10. Kies het SWA-certificaatbestand om te importeren en klik op Volgende.
Stap 11. Klik op Alle certificaten plaatsen in de volgende winkel en klik vervolgens op Volgende.
Stap 12. Controleer of de verstrekte informatie juist is en klik op Voltooien.

---

Opmerking: In sommige omstandigheden moet u de client opnieuw opstarten of gupdate /force uitvoeren om de wijzigingen op het Active Directory-clientsysteem toe te passen.

---

## Gerelateerde inhoud

- Gebruikershandleiding voor AsyncOS 14.5 voor Cisco Secure Web Appliance - GD (General Deployment)
- Certificaten naar clientcomputers distribueren met behulp van groepsbeleid | Microsoft Learn
- Technische ondersteuning en documentatie – Cisco Systems

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.