Configure Decryption Certificate in Secure Web Appliance

Contents

Introduction

Prerequisites

- Requirements
- Components Used

HTTPS Decryption

Configure Decryption Certificate in SWA

- Upload a Root Certificate and Key
- Generate a Certificate and Key for the HTTPS Proxy

Import Certificate

- Import Upstream Proxy Certificate to SWA
- Import SWA Certificate to Another SWA
- Import SWA Certificate in Windows Client
- Import SWA Certificate in Mac Client
- Import SWA Certificate in Ubuntu/Debian
- Import SWA Certificate in CentOS 6
- Import SWA Certificate in CentOS 5
- Import SWA Certificate in Mozilla Firefox
- Import SWA Certificate in Google Chrome
- Import SWA Certificate in Microsoft Edge/Internet Explorer
- Import SWA Certificate in Safari
- Import SWA Certificate from Group Policy to Clients

Related Content

Introduction

This document describes the steps to configure HTTPS Encryption Certificates in Secure Web Appliances (SWA) and Proxy clients.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Administrative Access to SWA
- Access to the Graphic User Interface (GUI) of SWA

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

HTTPS Decryption

The SWA Hypertext Transfer Protocol Secure (HTTPS) decryption uses root certificates and private key files that you upload to the appliance to encrypt traffic. The root certificate and private key files that you upload to the appliance must be in PEM format.

 **Note**: DER format is not supported.

You can also upload an intermediate certificate that a root certificate authority has signed. When SWA creates a certificate that represents the server certificate, it sends the uploaded certificate along with the mimicked certificate to the client application. That way, as long as the intermediate certificate is signed by a root Certificate Authority (CA) that the client application trusts, the application trusts the mimicked server certificate.

Configure Decryption Certificate in SWA

The SWA can use an existing certificate and private key for HTTPS decryption. However, there can be confusion about the type of certificate that must be used, as not all x.509 certificates work.

There are two major types of certificates: Server Certificates and Root Certificates. All x.509 certificates contain a Basic Constraints field, which identifies the type of certificate:

- Subject Type=End Entity - Server Certificate
- Subject Type=CA - Root Certificate

Upload a Root Certificate and Key

Step 1. From the GUI, navigate to **Security Services** and choose **HTTPS Proxy**.
Step 2. Click **Edit Settings**.
Step 3. Click **Use Uploaded Certificate and Key**.
Step 4. Click **Browse the Certificate field** to navigate to the certificate file stored on the local machine.



Note: If the file you upload contains multiple certificates or keys, the Web Proxy uses the first certificate or key in the file.

Step 5. Click **Browse** in the **Key** field to navigate to the private key file.



Note: The key length must be 512, 1024, or 2048 bits.

Step 6. Select **Key is Encrypted** if the key is encrypted.
Step 7. Click **Upload Files** to transfer the certificate and key files to the Secure Web Appliance. The uploaded certificate information is displayed on the **Edit HTTPS Proxy Settings** page.
Step 8. (Optional) Click **Download Certificate** to transfer to the client applications on the network.

Step 9. Submit and **Commit** changes.

Generate a Certificate and Key for the HTTPS Proxy

Step 1. From the GUI, navigate to **Security Services** and choose **HTTPS Proxy**.
Step 2. Click **Edit Settings**.
Step 3. Choose **Use Generated Certificate and Key**.
Step 4. Click **Generate New Certificate and Key**.
Step 5. In the **Generate Certificate and Key** dialog box, enter the information to display it in the root certificate. You can enter any ASCII character except the forward slash (/) in the **Common Name** field.
Step 6. Click **Generate**.
Step 7. The generated certificate information is displayed on the **Edit HTTPS Proxy Settings** page.
Step 8. (Optional) Click **Download Certificate**, so you can transfer it to the client applications on the network.
Step 9. (Optional) Click the **Download Certificate Signing Request** link, so you can submit the Certificate Signing Request (CSR) to a CA.
Step 10. (Optional) Upload the signed certificate to the Secure Web Appliance after you receive it from the CA. You can do this at any time after you generate the certificate on the appliance.
Step 11. Submit and **Commit** changes.

Import Certificate

Import Upstream Proxy Certificate to SWA

If SWA is configured to use an upstream proxy and the upstream proxy is configured for HTTPS decryption, you must import the upstream proxy encryption certificate to SWA. You can manage the trusted certificate list and add certificates to it and functionally remove certificates from it.

Step 1. From the GUI, choose **Network** and choose **Certificate Management**.
Step 2. Click **Manage Trusted Root Certificates** on the Certificate Management page.
Step 3. To add a custom trusted root certificate with signing authority, not on the Cisco-recognized list, click **Import** and then submit the certificate file.

Step 4. Submit and **Commit** changes.

Import SWA Certificate to Another SWA

If you uploaded the HTTPS Certificate and Key in one SWA for HTTPS Proxy and the original files are accessible, you can import them to another SWA from the configuration file.

Step 1. From the GUI of both SWAs, choose **System Administration** and click **Configuration File**.

Step 2. Click **Download** file on the local computer to view or save.

Step 3. Choose **Encrypt passwords** in the Configuration Files.

Step 4. (Optional) Choose **Use a user-defined file name** and add the desired name to the Configuration File.

Step 5. Click **Submit** under the Current Configuration to download the configuration **.xml** file.

Step 6. Open downloaded files with text editors or XML editors.

Step 7. Copy these tags from SWA with the certificate, copy all data inside the tags, and replace them in the configuration file of the other 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>
```

Step 8. Save the changes in the **.xml** file of the destination SWA.

Step 9. To Import the edited **.xml** configuration file back to the destination SWA, from the GUI, choose **System Administration** and click **Configuration File**.

Step 10. In the **Load Configuration** section, click **Load a configuration file from local computer**.

Step 11. Click **Choose file** and choose the edited **.xml** configuration file.

Step 12. Click **Load** to import the new configuration file with the certificate and key.

Step 13. Commit changes if the system prompts you.

Import SWA Certificate in Windows Client

To import the SWA HTTPS Proxy certificate as trusted in client computers with the Microsoft Windows operating system, review these steps:

Step 1. Click **Start** from the taskbar and type **Manage computer certificates**.
Step 2. On the Certificates-Local Computer page, expand **Trusted Root Certification** and right-click on the **Certificates** folder.
Step 3. Click **All Tasks** and choose **Import**.
Step 4. From the Certificate Import Wizard page, click **Next**.
Step 5. To import the SWA certificate file, click **Browse** and choose the certificate you downloaded from SWA.



Tip: To download the SWA certificate, refer to **Step 8** from the section **Upload a Root Certificate and Key** or **Generating a Certificate and Key for the HTTPS Proxy**.

Step 6. Click **Place all certificates in the following** checkbox.
Step 7. Choose **Trusted Root Certification Authorities** and click **Next**.
Step 8. Click **Finish**.

Alternatively, you can run this command to import the certificate to **Trusted Root Certification Authorities**.

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

Note: You must replace **<Path to SWA Certificate/CertificateName.crt>** with your current downloaded certificate path and file name.

Import SWA Certificate in Mac Client

Step 1. Download the HTTPS Proxy certificate from SWA to the Mac OS client.
Step 2. Rename the file extension to **.crt**.
Step 3. Run this command to import the certificate as a trusted certificate:

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

Note: You must replace it with your current downloaded certificate path and file name.

Import SWA Certificate in Ubuntu/Debian

Step 1. Download the HTTPS Proxy certificate from SWA.
Step 2. Open the certificate file in the text editor and copy all contents.
Step 3. Create a new file in **/usr/local/share/ca-certificates/** with a **.crt** as extension.
Step 4. Edit the file with your desired text editor and paste copied text into the new file, and save.
Step 5. Run this command to refresh the certificates in the operating system.

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

Tip: If you have the certificate stored locally on the client, you can copy the certificate to **/usr/local/share/ca-certificates/** and run **sudo update-ca-certificates**.

Note: In some versions, you must Install the ca-certificates package with this command: **sudo apt-get install -y ca-certificates**.

Import SWA Certificate in CentOS 6

Step 1. Download the HTTPS Proxy certificate from SWA.
Step 2. Open the certificate file in the text editor and copy all the contents inside the file.

Step 3. Create a new file in **/etc/pki/ca-trust/source/anchors/** with a **.crt** extension.
Step 4. Edit the file with your desired text editor and past copied text into the new file, and save.
Step 5. Install the ca-certificates package:

```
yum install ca-certificates
```

Step 6. Run this command to refresh the certificates in the operating system:

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



Tip: If you have the certificate stored locally on the client, you can copy the certificate to **/etc/pki/ca-trust/source/anchors/** and **run update-ca-trust extract** after you Install the **ca-certificates**.

Import SWA Certificate in CentOS 5

Step 1. Download the HTTPS Proxy certificate from SWA.
Step 2. Open the certificate file in the text editor and copy all contents inside the file.
Step 3. Create a new file in the current folder with a **.crt** extension (for example, **SWA.crt**).
Step 4. Edit the **/etc/pki/tls/certs/ca-bundle.crt** with your desired text editor, paste the copied text at the end of the file, and save.



Tip: If you have the certificate stored locally on the client (in this example, the file name is **SWA.crt**), you can append the certificate with this command: **cat SWA.crt >>/etc/pki/tls/certs/ca-bundle.crt**.

Import SWA Certificate in Mozilla Firefox

Step 1. Download the HTTPS Proxy Certificate from SWA.
Step 2. Rename the file extension to **.crt**.
Step 3. Open **Firefox** and click the **Menu** (three bars in the top right corner).
Step 4. Choose **Settings** (in some versions it is **Options**).
Step 5. Click **Privacy & Security** in the left-side menu and scroll to **Certificates**.
Step 6. Click **View Certificates**.
Step 7. Click the **Authorities** tab and then **Import**.
Step 8. Choose the certificate file and click **Open**.
Step 9. Click **OK**.

Import SWA Certificate in Google Chrome

Step 1. Download the HTTPS Proxy Certificate from SWA.
Step 2. Rename the file extension to **.crt**.
Step 3. Open **Google Chrome** and click **Customize and control Google Chrome** (three dots on the top-right corner).
Step 4. Choose **Settings**.
Step 5. Click **Privacy and Security** from the left-side menu.
Step 6. Choose **Security**.
Step 7. Scroll to **Manage certificates** and click the button on the right.
Step 8. Choose the **Trusted Root Certification Authorities** tab and click **Import**.
Step 9. Choose the certificate file and click **Open**.
Step 10. Click **OK**.



Note: If you install the SWA certificate in the operating system, Google Chrome trusts that certificate and there is no need to import the certificate separately to your browser.

Import SWA Certificate in Microsoft Edge/Internet Explorer

Microsoft Edge and Internet Explorer (IE) use operating system certificates. If you install the SWA certificate in the operating system, there is no need to import the certificate separately to your browser.

Import SWA Certificate in Safari

Step 1. Download the HTTPS Proxy certificate from SWA.
Step 2. Rename the file extension to **.crt**.
Step 3. In the Launchpad, select **Keychain Access**.
Step 4. From the **File** menu, click **Add Keychain**.
Step 5. Choose the SWA certificate file and click **Add**.
Step 6. Choose **Security**.
Step 7. Scroll to **Manage certificates** and click the button on the right.
Step 8. Choose the **Trusted Root Certification Authorities** tab and click **Import**.
Step 9. Choose the certificate file and click **Open**.
Step 10. Click **OK**.

Import SWA Certificate from Group Policy to Clients

To distribute certificates to client computers by the Group Policy from Active Directory, use these steps:

Step 1. Download the HTTPS Proxy certificate from SWA.

Step 2. Rename the file extension to **.crt**.
Step 3. Copy the certificate file to your domain controller.
Step 4. On the domain controller, click **Start** and open the **Group Policy Management** snap-in.
Step 5. Find the desired Group Policy Object (GPO) or create a new GPO to contain the SWA certificate to import to the client.
Step 6. Right-click **GPO**, and click **Edit**.
Step 7. From the left-side menu, navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**.
Step 8. Right-click the **Trusted Root Certification Authorities**, and click **Import**.
Step 9. Click **Next** on the **Welcome to the Certificate Import Wizard** page.
Step 10. Choose the SWA certificate file in order to import and click **Next**.
Step 11. Click **Place all certificates in the following store**, and then click **Next**.
Step 12. Verify that the information provided is accurate, and click **Finish**.



Note: In some conditions, you must restart the client or run **gpupdate /force** to apply the changes on the Active Directory client machine.

Related Content

- User Guide for AsyncOS 14.5 for Cisco Secure Web Appliance - GD (General Deployment)
- Distribute Certificates to Client Computers by Using Group Policy | Microsoft Learn
- Technical Support & Documentation - Cisco Systems