SSL CA Certificate Installation Guide

Applicable Version: 10.00 onwards

Overview

When SSL content inspection for HTTPS traffic is enabled on Cyberoam, the web browsers prompt a warning message if the Certificate Authority (CA) for the certificate used by the Cyberoam SSL inspection is not known by the browser. For this, you need to import Cyberoam SSL Proxy certificate in the browser for decryption on SSL Inspection.

All Cyberoam appliances are shipped with a unique SSL CA Certificate which is used in HTTPS Deep Scan Inspection. This article describes how you can download Cyberoam's SSL CA Certificate and install it in your local browser and machine

Note:

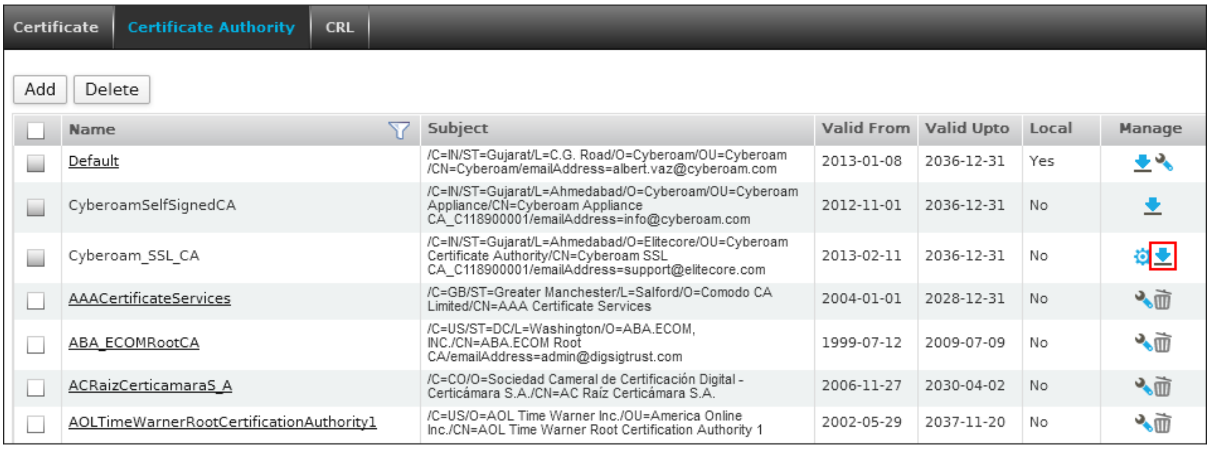
Cyberoam also provides an option to regenerate the CA Certificate when required. To know how to regenerate a CA Certificate, refer to article How To – Regenerate a Unique SSL CA Certificate.

Configuration

To download and install the Certificate in your browser and local machine, follow the steps given below.

Step 1: Download the Certificate to your local machine

Go to **System > Certificate > Certificate Authority** and click on the download icon ⬇ under **Manage** column to download the Certificate, as shown below. Save it in your local machine.



□	Name	Subject	Valid From	Valid Upto	Local	Manage
□	Default	/C=IN/ST=Gujarat/L=C.G. Road/O=Cyberoam/OU=Cyberoam /CN=Cyberoam/emailAddress=albert.vaz@cyberoam.com	2013-01-08	2036-12-31	Yes	⬇ 🔧
□	CyberoamSelfSignedCA	/C=IN/ST=Gujarat/L=Ahmedabad/O=Cyberoam/OU=Cyberoam Appliance/CN=Cyberoam Appliance CA_C118900001/emailAddress=info@cyberoam.com	2012-11-01	2036-12-31	No	⬇
□	Cyberoam_SSL_CA	/C=IN/ST=Gujarat/L=Ahmedabad/O=Elitecore/OU=Cyberoam Certificate Authority/CN=Cyberoam SSL CA_C118900001/emailAddress=support@elitecore.com	2013-02-11	2036-12-31	No	⚙ ⬇
□	AAACertificateServices	/C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate Services	2004-01-01	2028-12-31	No	🔧 🗑
□	ABA_ECOMRootCA	/C=US/ST=DC/L=Washington/O=ABA.ECOM, INC./CN=ABA.ECOM Root CA/emailAddress=admin@digsigtrust.com	1999-07-12	2009-07-09	No	🔧 🗑
□	ACRaizCerticamaraS_A	/C=CO/O=Sociedad Cameral de Certificación Digital - Certicámara S.A./CN=AC Raíz Certicámara S.A.	2006-11-27	2030-04-02	No	🔧 🗑
□	AOLTimeWarnerRootCertificationAuthority1	/C=US/O=AOL Time Warner Inc./OU=America Online Inc./CN=AOL Time Warner Root Certification Authority 1	2002-05-29	2037-11-20	No	🔧 🗑

Step 2: Install Certificate in Trusted Certification List in your Browser

Internet Explorer

- On the Menu Bar, click **Tools > Internet Options** to display the Internet Options window.
- Select **Content** tab and, under Certificates section, click **Certificates** to display Certificates Window.
- Switch to **Trusted Root Certification Authorities** tab and click the **Import** button to start Certificate Import Wizard.
- Import the Certificate downloaded in step 1 using this wizard.

Firefox

- On the Menu Bar, click **Tools > Options** to display the Options window.
- Switch to **Advanced** tab under which select **Encryption** tab.
- Click **View Certificate** to display the Certificate Manager window.
- Switch to **Authorities** tab and click **Import**.
- Select the Certificate downloaded in step 1 and click **Open**.
- In the Downloading Certificate window, select Trust this CA to identify websites and click **OK**.

Google Chrome

- On the right corner of the Address Bar, click on Chrome Tools button and click **Settings**.
- Click **Show advanced settings...** and scroll down to HTTPS/SSL.
- Click **Manage Certificates...** to display the Certificates window.
- Switch to **Trusted Root Certification Authorities** tab and click the **Import** button to start Certificate Import Wizard.
- Import the Certificate downloaded in step 1 using this wizard.

Mac Safari

- Download the SSL CA Certificate as shown in step 1.
- Once downloaded, double-click the Certificate. This launches Keychain Access and displays Certificate Not Trusted Warning.
- Click Always Trust to import the certificate into login keychain.

Opera

- Click the **Opera** button on the top left corner of the screen and click **Settings**.
- Switch to **Privacy & Security** tab.
- Under **HTTPS/SSL**, click **Manage Certificates…** to display the Certificates window.
- Switch to **Trusted Root Certification Authorities** tab and click the **Import** button to start Certificate Import Wizard.
- Import the Certificate downloaded in step 1 using this wizard.

Step 3: Install Certificate in Local Machine’s Trusted Root Authority Container

Windows

- Open the **Microsoft Management Console** by typing "MMC" in the run box.
- Add the **certificates Snap-in** by selecting **FILE → ADD/REMOVE SNAP-IN...**
- Select **Certificates** from the list and click **Add** to display Certificates Snap-in window.
- Select the **Computer Account** and click **Next**.
- Click **Finish** and close the list of snap-ins.
- Click **OK** to add the certificates snap-in, which should now be visible in the Add/Remove Snap-ins window.
- Expand the list of certificate containers, right click **Trusted Root Authorities** and choose **All Tasks > Import** to start Certificate Import Wizard.
- Import the Certificate downloaded in step 2 using this wizard.

Macintosh

- Download the SSL CA Certificate as shown in step 1.
- Once downloaded, double-click the Certificate. This launches Keychain Access and displays Certificate Not Trusted Warning.
- Click **Always Trust** to import the certificate into login keychain.

Document Version: 1.4 – 24 November, 2014