**File name:**

SecurityAppliance\_SSL\_CA.pem

SecurityApplianceSelfSignedCA.pem

**Install Certificate in Trusted Certification List of your Browser**

**Internet Explorer**

         In the Menu Bar, click **Tools > Internet Options** to display the Internet Options window.

         Switch to the **Content** tab and, under the Certificates section, click **Certificates** to display the Certificates Window.

         Switch to the **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**

         In the Menu Bar, click **Tools >** **Options** to display the Options window.

          Switch to the **Advanced**tab and then select the **Certificates** tab.

         Click **View Certificate** to display the Certificate Manager window.

         Switch to the **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**

         To the right of the Address Bar, click on **Customize and control Google Chrome** button and click **Settings**.

         Click **Show advanced settings** and scroll down to HTTPS/SSL.

         Click **Manage Certificates...**to display the Certificates window.

         Switch to the **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.

**Safari**

         Download the SSL CA Certificate as shown in step 1.

         Once downloaded, double-click the Certificate. This launches Keychain Access and displays a 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 the **Privacy & Security**tab.

         Under **HTTPS/SSL**, click **Manage Certificates…**to display the Certificates window.

         Switch to the **Trusted Root Certification Authorities**tab and click the **Import**button to start the Certificate Import Wizard.

         Import the Certificate downloaded in step 1 using this wizard.

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

**Windows**

         Open the **Microsoft Management Console** by typing "MMC" in the "Run" box.

         Open Add or Remove Snap-ins by selecting **FILE >** **ADD/REMOVE SNAP-IN...**

         Select **Certificates** from the list and click **Add**to display the 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 a Certificate Not Trusted warning.

         Click **Always Trust**to import the certificate into Login Keychain.