Setup Guide
Revision C

Importing Certificates for SSL

Importing Web Protection certificates

Importing Web Protection certificates into the user's browser certificate store allows the browser to recognize the SSL Scanning proxy each time the user accesses SSL Scanning. This recognition eliminates the need for users to accept certificates for individual hosts.

The certificate(s) are included in the .zip file (WebProtection_SaaS_Certificate_Bundle.zip) that contained these instructions and that you downloaded from the **Policy** | **SSL** page. Extract the contents of the zip file to a location of your choice.

Certificates are user-specific. If multiple users share a computer, certificates need to be manually imported for each user that uses a given machine.

For support information, visit http://support.mcafeesaas.com

Import certificates using Internet Explorer and Chrome

You can use a Microsoft Internet Explorer web browser to manually import a Web Protection certificate.

Task

1 From the **Tools** menu (in Internet Explorer) or from the Control Panel, select **Internet Options**.

2 Click **Content** .

3 Click **Certificates**.

4 Click **Import**.

5 On the **Certificate Import Wizard** welcome page, click **Next**.

6 Click **Browse** and navigate to where you stored **WebProtectionRootAuthority.crt** certificate file.

7 Click **Open**.

8 Click **Next**.

9 Select **Place all certificates in the following store**, and click **Browse**.

10 Select **Trusted Root Certification Authorities**, and click **OK**.

11 Click **Next**.

12 Click **Finish** .

13 If a Security Warning dialog box appears, click **Yes**.

The message **The import was successful** appears.

14 Click **OK**.

15 Click **Import**.

16 On the **Certificate Import Wizard** welcome page, click **Next**.

17 Click **Browse** and navigate to where you stored **WebProtectionIntermediateServer.crt** certificate file.

18 Click **Open**.

19 Click **Next**.

20 Select **Place all certificates in the following store**, and click **Browse**.

21 Select **Intermediate Certification Authorities**, and click **OK**.

22 Click **Next**.

23 Click **Finish** .

24 If a Security Warning dialog box appears, click **Yes**.

The message **The import was successful** appears.

25 Click **OK**.

26 Close all open windows.

Import certificates using Firefox

You can use a Firefox web browser to manually import a Web Protection certificate.

Task

1 From the **Tools** menu, select **Options**.

2 Click **Advanced**.

3 Click **Certificates**.

4 Click **View Certificates**.

5 Click **Authorities**.

6 Click **Import**.

7 Navigate to where you stored the **WebProtectionRootAuthority.crt** certificate file.

8 Select the certificate file and click **Open**.

9 Select **Trust this CA to identify websites**.

10 Click **OK**.

11 Click **Servers**.

12 Click **Import**.

13 Navigate to where you stored the **WebProtectionIntermediateServer.crt** certificate file.

14 Scroll down in the list of certificates to find **McAfee Web SaaS Root Certification Authority**, and click **wps.mcafeesaas.com**.

15 Click **Edit Trust**.

16 Select **Trust this CA to identify websites**.

17 Click **OK**.

18 Click **OK** to close all open Firefox windows

Managed Certificate Imports

You can install the Web Protection certificate via Active Directory Group Policy Objects (GPO) or login scripts.

Windows Server 2003

The functionality to import the certificates using group policy is available in Windows Server 2008 but not in Windows Server 2003. For Windows 2003 domains, you must use a script to push out the certificates.

Before you begin

Use the System account to import the certificates.

Task

1 To install the root CA, enter **certutil -addstore root WebProtectionRootAuthority.crt**.

2 To install the intermediate CA, enter **certutil -addstore ca WebProtectionIntermediateServer.crt**.

The **.crt** certificate files must be in the same folder as the script or the full path to the certificate must be included before the filename in the script. In addition, the server will have to be rebooted for the import to take effect.

Windows Server 2008 and above

On a Window Server 2008, you can import certificates through the Group Policy Objects of Active Directory.

Task

1 Open **Group Policy Management Console**.

2 Find an existing GPO or create a new GPO to contain the certificate settings. Ensure that the GPO is associated with the domain, site, or organizational unit whose users you want affected by the policy.

3 Right-click the GPO, and then select **Edit**.

The **Group Policy Management Editor** opens, and displays the current contents of the policy object.

4 In the navigation pane, open **Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Trusted Root Certification Authorities**.

5 Click the **Action** menu, and select **Import**.

The **Certificate Import Wizard** appears.

6 Click **Browse** and locate the **WebProtectionRootAuthority.crt** file.

7 Click **Next**.

8 Click **Finish**.

9 In the navigation pane, select **Intermediate Certification Authorities**.

10 Click the **Action** menu, and select **Import**.

The **Certificate Import Wizard** appears.

11 Click **Browse** and locate the **WebProtectionIntermediateServer.crt** file.

12 Click **Next**.

13 Click **Finish**.