SSL Certificate – F5

Installation Guide

webnic
accelerate your business

Please select your version

Installation Instructions for BIG-IP F5 version 9.x and 10.x

Installation Instructions for F5 BIG-IP version 11

Installation Instructions for BIG-IP F5 version 9.x and 10.x

Step 1. Download the Intermediate CA Certificate

1. Download the Intermediate CA certificate.

   Select the appropriate Intermediate CA certificate for your SSL Certificate type.
2. Copy the Intermediate CA certificate and paste it on a Notepad.
3. Save the file as intermediate.crt.
4. Save the file to the following location: **/config/bigconfig/ssl.crt/intermediate.crt**

   NOTE: In a redundant system, the keys and certificates must be in place on both controllers before you configure the SSL Accelerator.

   You must do this manually as the configuration synchronization utilities do not perform this function.

Step 2. Install the Intermediate CA Certificate

1. Log in to the **Configuration** utility.
2. Click **Local Traffic**.
3. Click **SSL Certificates.**
4. Click **Import.**
5. Select **Certificate** from the **Import Type** menu.
6. Click the **Create New** option.
7. Type a unique name for the **Certificate Name**.
8. Click **Browse** and navigate to the file you saved as **intermediate.crt**.
9. Click **Open**.
10. Click **Import**.

Step 3. Obtain the SSL Certificate

1. The Symantec certificate will be sent by email. The certificate is included as an attachment (**Cert.cer)** and it is also imbedded in the body of the email.
2. Copy and paste the certificate into a text file using Vi or Notepad.

   Do not use Microsoft Word or other word processing programs that may add characters.

   The text file should look like:

   -----BEGIN CERTIFICATE-----

```
        [encoded data]

    -----END CERTIFICATE-----
```

3. Save the file with extension **.crt**

Step 4. Install the SSL Certificate

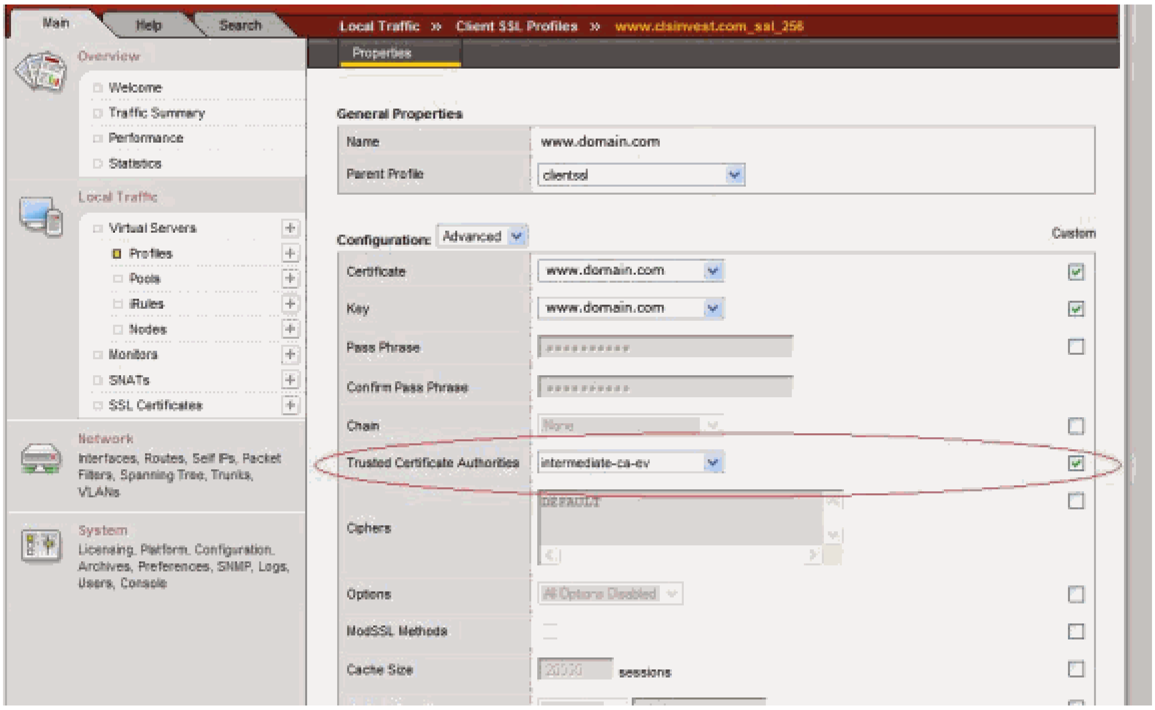
1. In the navigation pane, click **Proxies**.
2. On Proxies screen, click the **Install SSL Certificate Request** tab. The Install SSL Certificate screen opens.
3. In the **Certfile Name** box, enter the **fully qualified domain name** of the server with the file extension **.crt**. If you generated a temporary certificate when you submitted a request to Symantec,
   you can select the name of the certificate from the drop down list. This allows you to overwrite the temporary certificate with the certificate from Symantec.
4. **Paste** the text of the certificate into the **Install SSL Certificate** window.
5. Click **Write Certificate File** to install the certificate. After the certificate is installed, you can continue with the next step in creating an SSL gateway for the server.

Step 5. Establish the trust chain

NOTE: The proper Intermediate CA certificate must be set to ensure a complete chain of trust.

1. Log in to the Configuration utility.
2. Click **Local Traffic**.
3. Click **Profiles**.
4. Select **Server** from the SSL menu.
5. Select the Server SSL profile to configure.
6. Select **Advanced** from the **Configuration** menu.
7. Select the appropriate chain certificate from the **Chain** dropdown box.
8. Click **Update**.

   NOTE: Please refer to the screenshot of the F5 Big-IP interface



Local Traffic » Client SSL Profiles » www.clsinvest.com_ssl_256

General Properties

Name	www.domain.com
Parent Profile	clientssl

Configuration: Advanced

		Custom
Certificate	www.domain.com	☑
Key	www.domain.com	☑
Pass Phrase	**********	□
Confirm Pass Phrase	**********	
Chain	None	□
Trusted Certificate Authorities	intermediate-ca-ev	☑
Ciphers	DEFAULT	□
Options	All Options Disabled	□
ModSSL Methods		□
Cache Size	20000 sessions	□

9. Verify certificate installation using the Symantec Installation Checker.

Installation Instructions for F5 BIG-IP version 11

Step 1. Obtain the SSL Certificate

1. The Symantec certificate will be sent by email. The certificate is included as an attachment (**Cert.cer)** and it is
   also imbedded in the body of the email.
2. Copy and paste the certificate into a text file using Vi or Notepad.
   Do not use Microsoft Word or other word processing programs that may add characters.

   The text file should look like:

   -----BEGIN CERTIFICATE-----

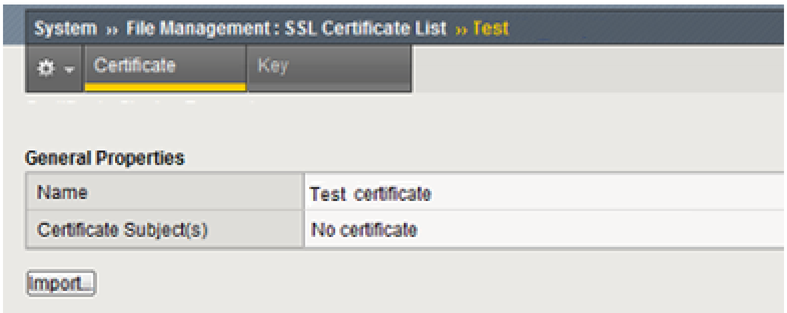
   [encoded data]

   -----END CERTIFICATE-----

3. Save the file with **.pem** extension

Step 2. Install the SSL Certificate

1. On the left Panel, click on **File Management**
2. Choose **SSL Certificate List**
3. From the list, click on the pending request (the label from when you generated the CSR)
4. Click on **Import**

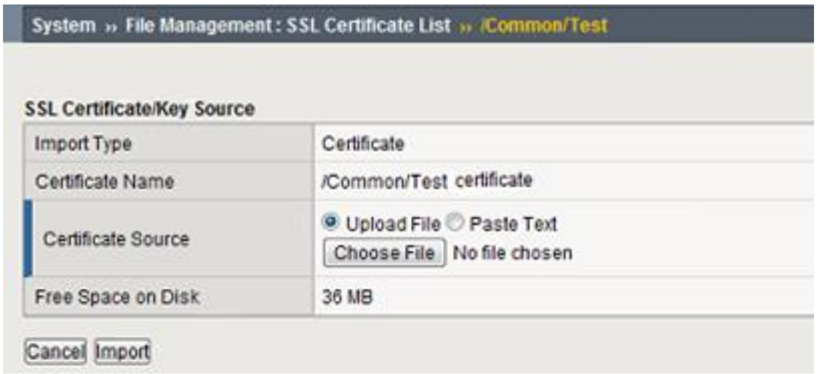


General Properties

Name	Test certificate
Certificate Subject(s)	No certificate

5. Select **Upload file**

6. Click on **Choose File**
7. Locate the **SSL certificate** file then click **OK**
8. Click on **Import**



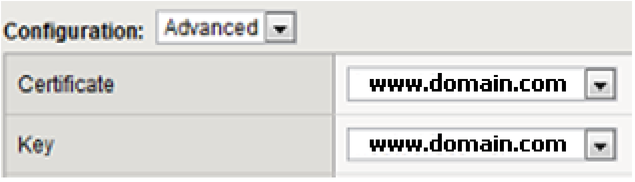
System » File Management : SSL Certificate List » /Common/Test

SSL Certificate/Key Source

Import Type	Certificate
Certificate Name	/Common/Test certificate
Certificate Source	● Upload File ○ Paste Text Choose File No file chosen
Free Space on Disk	36 MB

Step 3. Assign the SSL Certificate

1. Under **Configuration**, choose **Advanced**
2. For Certificate & Key, select from the drop down list



Configuration: Advanced

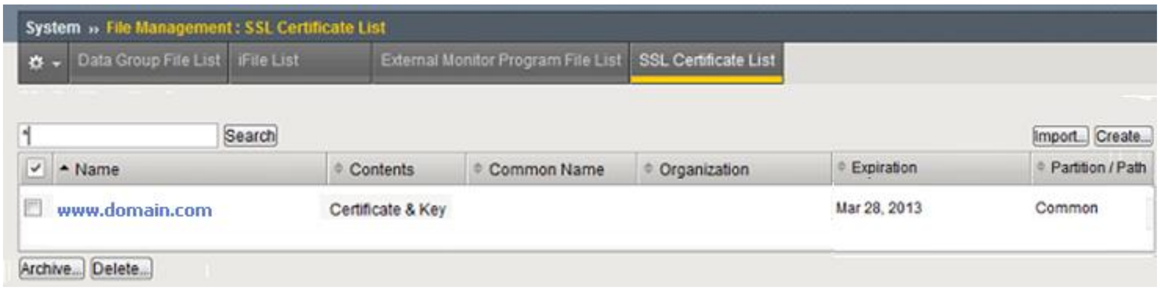
Certificate	www.domain.com
Key	www.domain.com

3. To apply the changes, scroll down to the bottom of the page and click **Submit**.

Step 4. Download Symantec Intermediate CA certificate

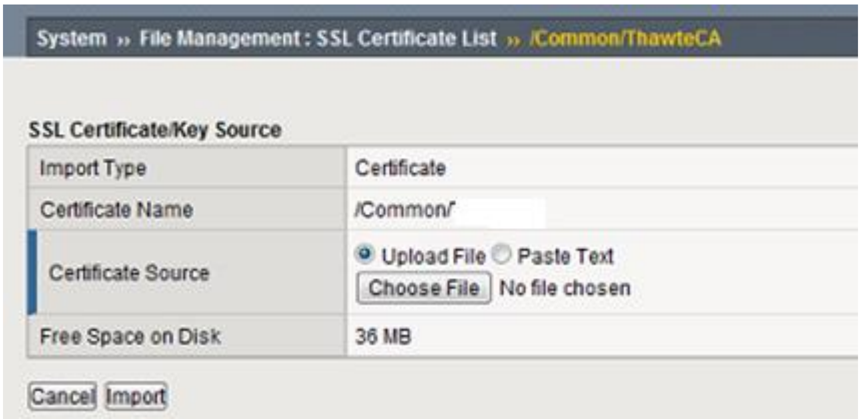
1. Download the Intermediate CA certificate.

   Select the appropriate Intermediate CA certificate for your SSL Certificate type.
2. Copy the Intermediate CA certificate and paste it on a a VI or Notepad.
3. Save the file as **Intermediate.pem**
4. On the left panel, click on **File Management**
5. Choose **SSL Certificate List**



☑	Name	Contents	Common Name	Organization	Expiration	Partition / Path
□	www.domain.com	Certificate & Key			Mar 28, 2013	Common

6. Click on **Import** (button to the right)
7. Click on **Choose File**


System » File Management : SSL Certificate List » /Common/ThawteCA
Cancel
Import

SSL Certificate/Key Source

Import Type	Certificate
Certificate Name	/Common/
Certificate Source	● Upload File ○ Paste Text Choose File No file chosen
Free Space on Disk	36 MB

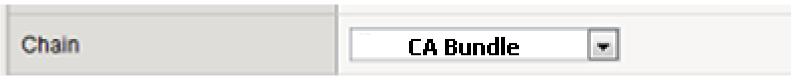
8. Locate the **Intermediate.pem** file then click **OK**
9. Click on **Import**

Step 5. Updating the SSL profile

1. On the left panel, click on **Profiles**
2. Choose **SSL**
3. Choose **Client**
4. From the list, select the SSL profile for your website

Step 6. Assigning the CA bundle

1. Under **Configuration**, choose **Advanced**
2. For **Chain**, assign the CA bundle from the drop down



Chain

CA Bundle

3. To apply the changes, scroll down to the bottom of the page and click **Submit**.
4. Verify certificate installation using the Symantec Installation Checker.