SSL Certificate – Citrix Gateway

Installation Guide

webnic
accelerate your business

Please select your version

Installation Instructions for Citrix Access Gateway 4.x

Installation Instructions for Citrix Access Gateway 5.0

Installation Instructions for Citrix Access Gateway 8.0

Installation Instructions for Citrix Secure Gateway on Windows

Installation Instructions for Citrix Access Gateway 4.x

Step 1. Obtain the SSL Certificate

1. The Symantec certificate will be sent by email. The certificate will be included as an attachment (Cert.cer) and it will
   be 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-----

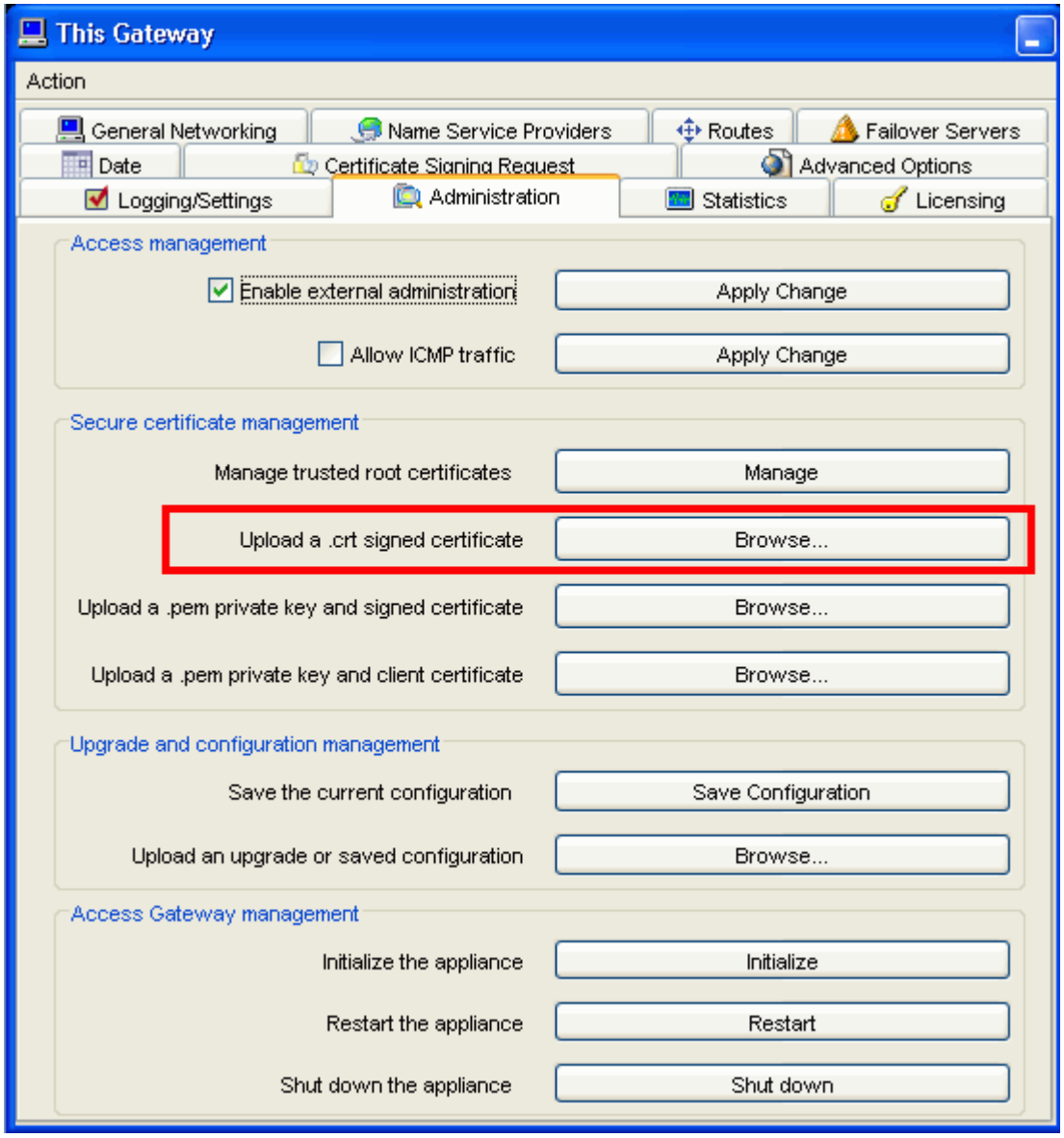
   [encoded data]

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

3. Save the file as **SSL.crt**

Step 2. Install the SSL Certificate

1. Click the **Access Gateway Cluster** tab
2. Under **Administration**, next to **Upload a .crt signed certificate** click **Browse**



3. Locate the **.crt** file that you have saved and click **Open**.
4. After the upload is complete, click on the **General Networking** tab
5. In External Public IP or FQDN, under Interface 0, type the **IP address or FQDN** for which the certificate was registered.

Step 3. Download the Root and Intermediate CA Certificate

NOTE: Ensure that the approriate **Root** and **Intermediate CA certificate** have been downloaded for your SSL Certificate type.

1. Download the Root CA certificate for your SSL product.

2. Download the Intermediate CA certificate.

   Select the appropriate Intermediate CA certificate for your SSL Certificate type.
3. Open a Notepad and paste the Intermediate CAs in the following order:

   The Intermediate CA on the top, followed by the Root CA at the bottom.

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

   [Intermediate CA]

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

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

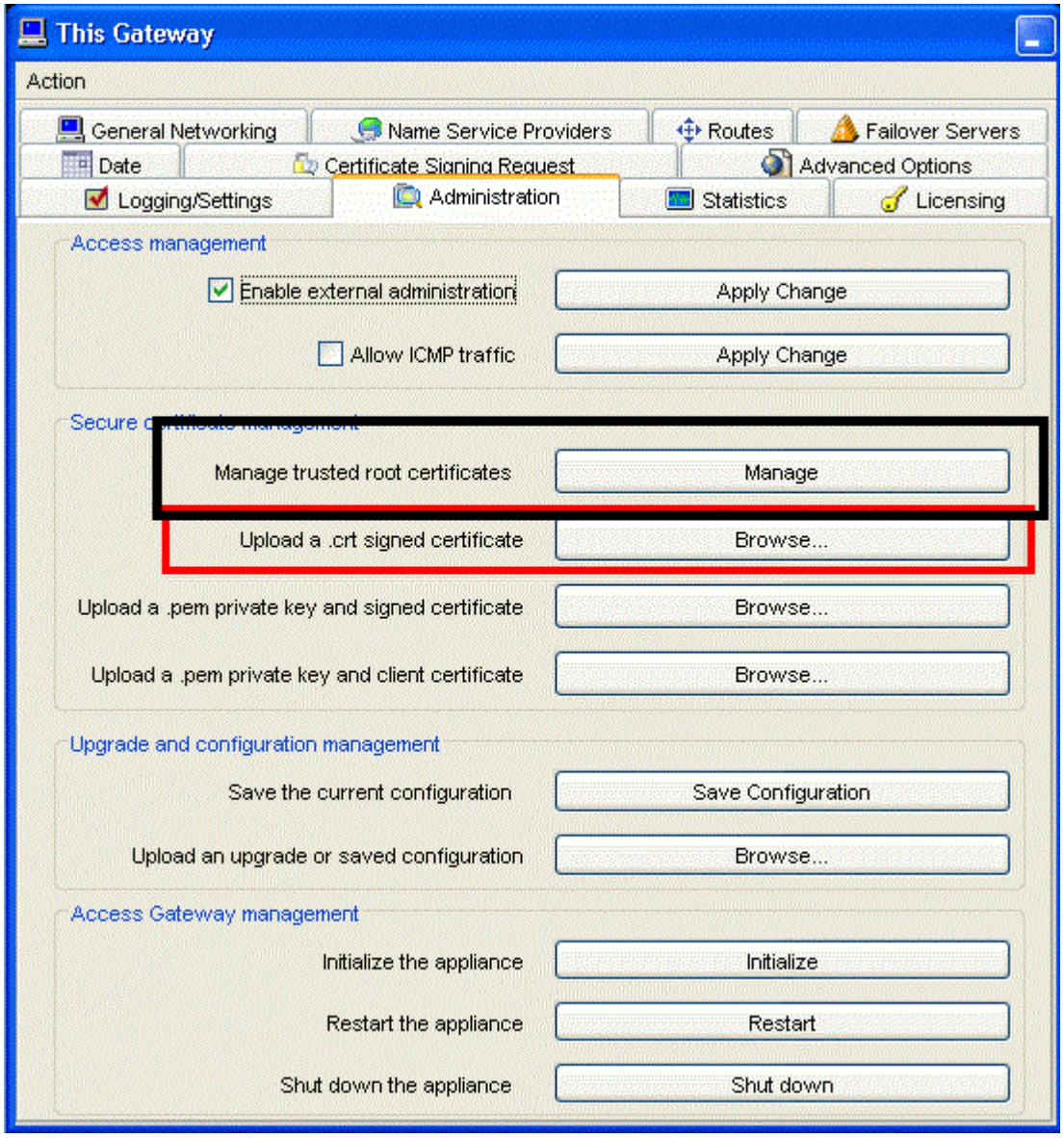
   [Root CA]

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

4. Save the file as **Intermediate.crt**

Step 4. Install the Root and the Intermediate CA certificate on Citrix Access Gateway

1. Click the **Access Gateway Cluster** tab
2. Under **Administration**, next to **Manage trusted root certificates** click **Browse**



3. Click **"Upload Trusted Root Certificate"**
4. Locate the **Intermediate.crt** file that you have saved ind **Step 3**
5. Click **Open** to complete installation.
6. Verify your installation with the Symantec SSL Certificate Checker.

Installation Instructions for Citrix Access Gateway 5.0

Step 1: Obtain and install the SSL Certificate

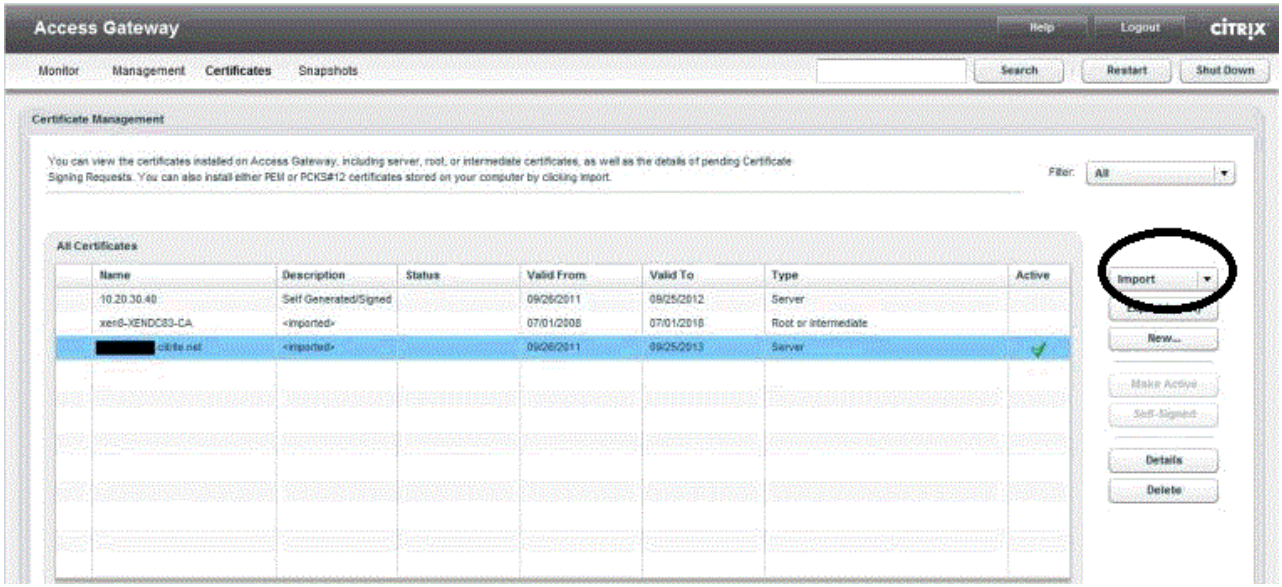
1. The Symantec certificate will be sent by email. The certificate will be included as an attachment (Cert.cer) and it will
   be also imbedded in the body of the email.
2. Copy and paste the certificate into a text file using Vi or Notepad. Do not use Microsoft Word or other word
   processing programs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

   The text file should look like:
   -----BEGIN CERTIFICATE-----

   [encoded data]

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

3. Save the file as **SSL.pem**
4. In the **Access Gateway Management Console**, click **Certificates**.



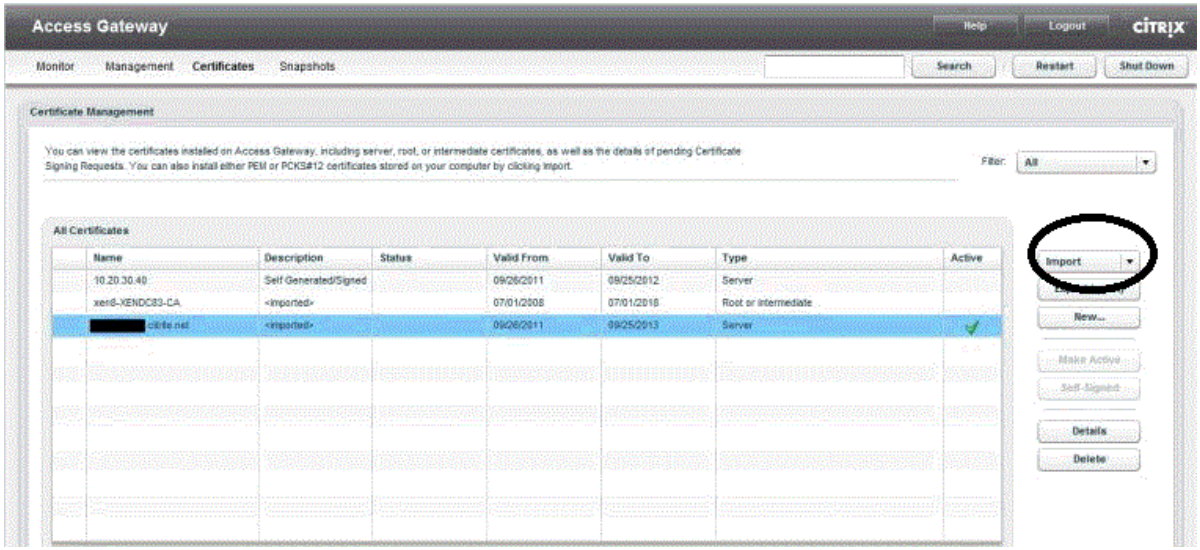
5. Click **Import** and then select **Server (.pem)**

6. In Select file to upload, navigate to the **SSL.pem** and then click Open.

Step 2: Download and install the Intermediate CA Certificate

NOTE: Ensure that the approriate **Intermediate CA certificates** have been downloaded for you SSL product type.

1. Download the Intermediate CA certificate
   Select the appropriate Intermediate CA certificate for your SSL Certificate type.
2. Save the file as **Intermediate.pem**
3. In the **Access Gateway Management Console**, click **Certificates**.

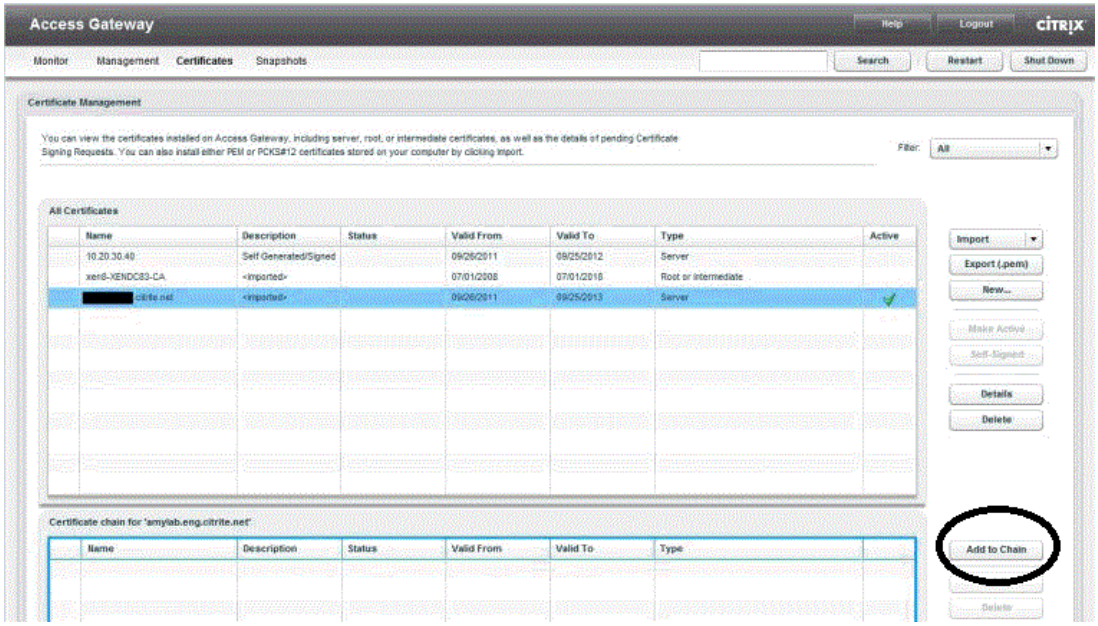


4. Click **Import** and then select **Trusted (.pem)**.
5. In **Select file to upload**, navigate to the **Intermediate.pem** file and then click **Open**.
   NOTE: When you install an intermediate certificate on Access Gateway, you do not need to specify the private key or a password.
   After the certificate is installed on the appliance, the certificate needs to be linked to the server certificate.

Step 3: Link an Intermediate CA certificate to a SSL server certificate

1. In the **Access Gateway Management Console**, click **Certificates**.

2. In the **Certificates** table, select the server certificate to which you want to link an intermediate certificate and then click **Add to Chain**.



3. In the dialog box that opens, select a certificate and then click **Add** for each certificate that you want to add to the chain.
4. When you are finished building the certificate chain, select the new certificate you wish to use, and select **Make Active**.
5. Verify your installation with the Symantec Installation Checker.

Installation Instructions for Citrix Access Gateway 8.0

Step 1. Obtain the SSL Certificate

1. The Symantec certificate will be sent by email. The certificate will be included as an attachment (Cert.cer) and it will
   be 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-----

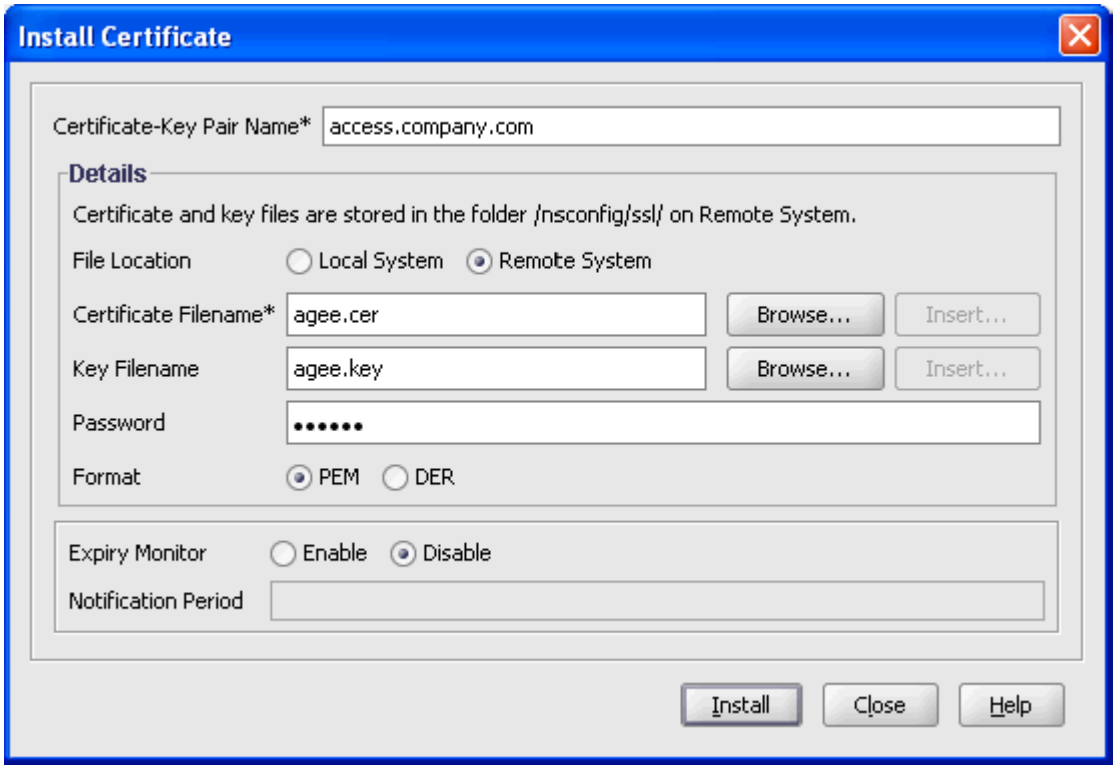
   [encoded data]

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

3. Save the file as **filename.cer**
   NOTE: It is recommended to use the **same filename** you have given to the **Private Key** when you generated the CSR for this certificate.

Step 2. Install the SSL Certificate

1. Using **WinSCP** or any other secure **FTP client**, connect to the **Access Gateway** and **log on as nsroot**.
2. Upload the agee.cer file to the **/nsconfig/ssl** directory
3. In the GUI configuration manager, go to **SSL > Certificates** and click **Add**.



4. In the **Certificate-Key Pair Name field**, type a descriptive name for this certificate entity, for example: access.company.com
5. For **File Location** select the **Remote System** radio button.
6. For **Certificate Filename**, click Browse and locate the **filename.cer** file you obtained in **Step 1**
7. For the **Key Filename** browse to the **corresponding Private Key** and enter the **PEM passphrase**
8. Keep **PEM** selected as the format.
9. Click **Install** and then Close.
10. After a few seconds, the certificate entity should appear in the background. Click Close. Your certificate can now be used.

Step 3. Download the Root and Intermediate CA Certificate

NOTE: Ensure that the approriate **Root** and **Intermediate CA certificates** have been downloaded for you SSL product type

1. Download the Root CA certificate for your SSL product.
2. Download the Intermediate CA certificate.

   Select the appropriate Intermediate CA certificate for your SSL Certificate type.

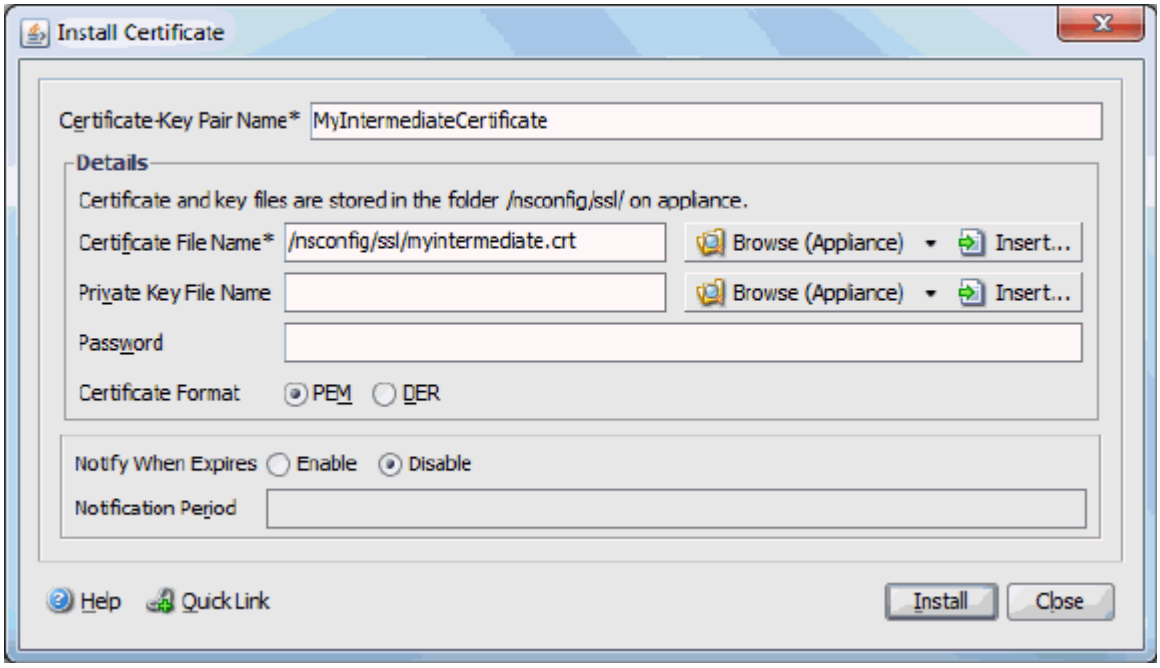
3. Open a Notepad and paste the Intermediate CA and the Root CA in the following order: The Intermediate CA certificate on the top, followed by the Root CA at the bottom.

   -----BEGIN CERTIFICATE-----
   [Intermediate CA]
   -----END CERTIFICATE-----
   -----BEGIN CERTIFICATE-----
   [Root CA]
   -----END CERTIFICATE-----

4. Ensure that any additional characters or line breaks have been added
5. Save ther file as **Intermediate.crt**

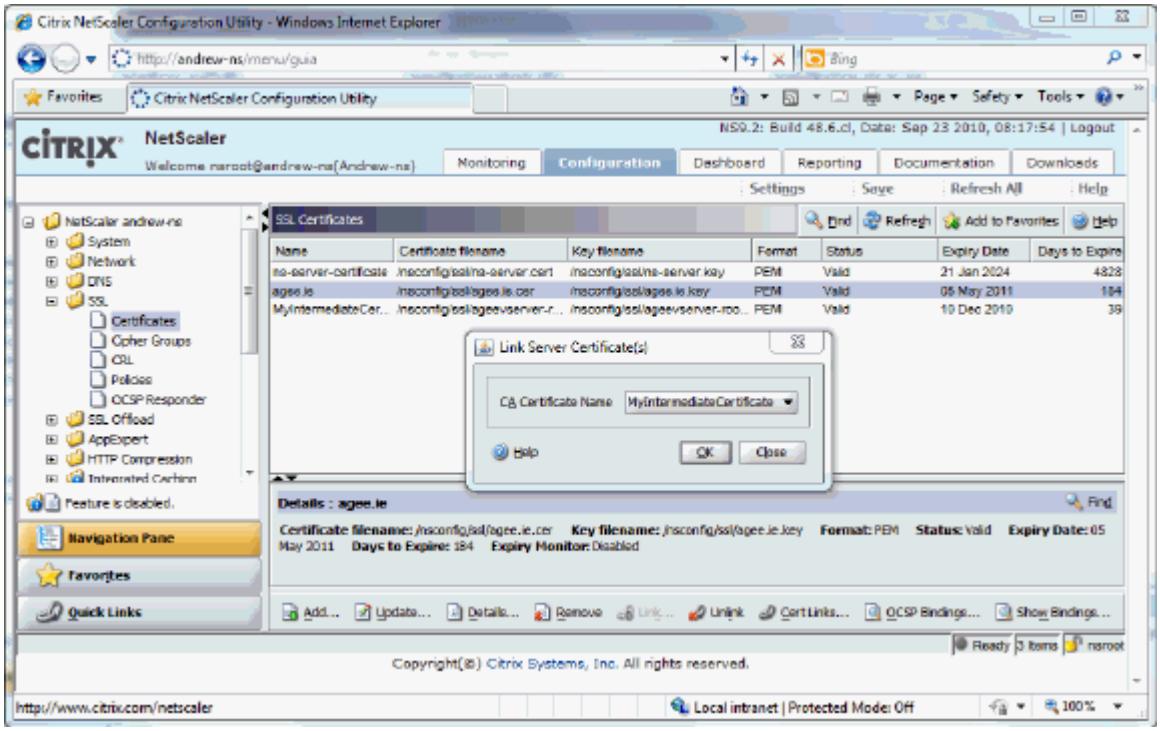
Step 4. Install the Root and the Intermediate CA certificates

1. Using WinSCP transfer the intermediate certificate to the **/nsconfig/ssl directory**
2. Log in to the **Configuration utility** of the appliance.
3. Expand the **SSL node.**
4. Click **Certificates.**
5. On the SSL Certificates page, click **Add**.
6. Specify the appropriate values in the various fields of the Install Certificate dialog box. The following screenshot displays the sample values for your reference:

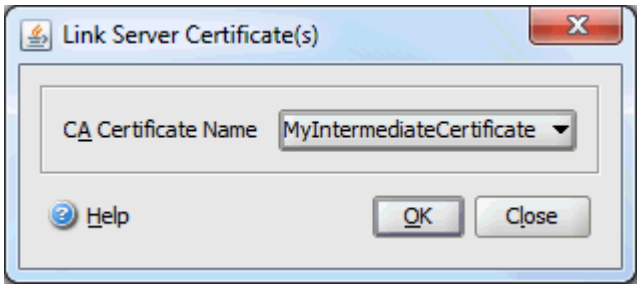


7. Click **Install.**
8. On the SSL Certificates page, select the server certificate to which you want to link the intermediate certificate.

   NOTE: Link the server certificate to the Intermediate CA certificate.
9. Click **Link.**



10. From the CA Certificate Name list, select the required intermediate certificate, as shown in the following screenshot:



11. Verify your installation with the Symantec SSL Certificate Checker.

Installation Instructions for Citrix Secure Gateway on Windows

This solution contains two Methods to install your SSL Certificate:

Method 1: Installing the certificate received via e-mail.

Method 2 (recommended) : Installing the certificate downloaded from the Symantec Trust Center account.

Method 1: Download and Install SSL certificate sent via e-mail

Step 1: Obtain the SSL certificate sent via email:

Your Symantec certificate will be **sent via email.** The certificate is imbedded in the body of the email.

Use a plain text editor such as Notepad, paste the content of the certificate and save it with extension **.txt**

NOTE: If you selected Microsoft IIS 5.0 or above during enrollment, continue with the installation here.

If you are not sure which server software was selected during the enrolment, proceed with **Step 2** bellow.

Step 2: Download and Install the Intermediate CA certificate:

To download and install the Intermediate CA certificate follow the steps from here.

Step 3: Install the SSL certificate:

To proceed with the installation steps for your SSL certificate click here.

Method 2: Download and Install SSL certificate in PKCS#7 format

Step 1: Download the SSL certificate from Symantec Trust Center account:

Download the certificate from Symantec Trust Center here.

Make sure you download the certificate in PKCS#7 format and save it with the extension **.txt** or **.p7b.**

Step 2: Install Certificate:

1. Click **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**
2. From the left menu, click the corresponding server name
3. In the Features pane (middle pane), under Security, double-click **Server Certificates**
4. From the Actions pane (right pane), select **Complete Certificate Request**
5. Provide the location of the certificate file and the **friendly name**

   NOTE: Friendly name is a reference name for quick identification of the certificate for the Administrator

   At this point the server may respond with one of the two known errors:

   CertEnroll::CX509Enrollment::p_InstallResponse:ASN1 bad tag value met. 0x8009310b (ASN: 267)

   Click here for the resolution to this message

   or

   Cannot find the certificate request associated with this certificate file.

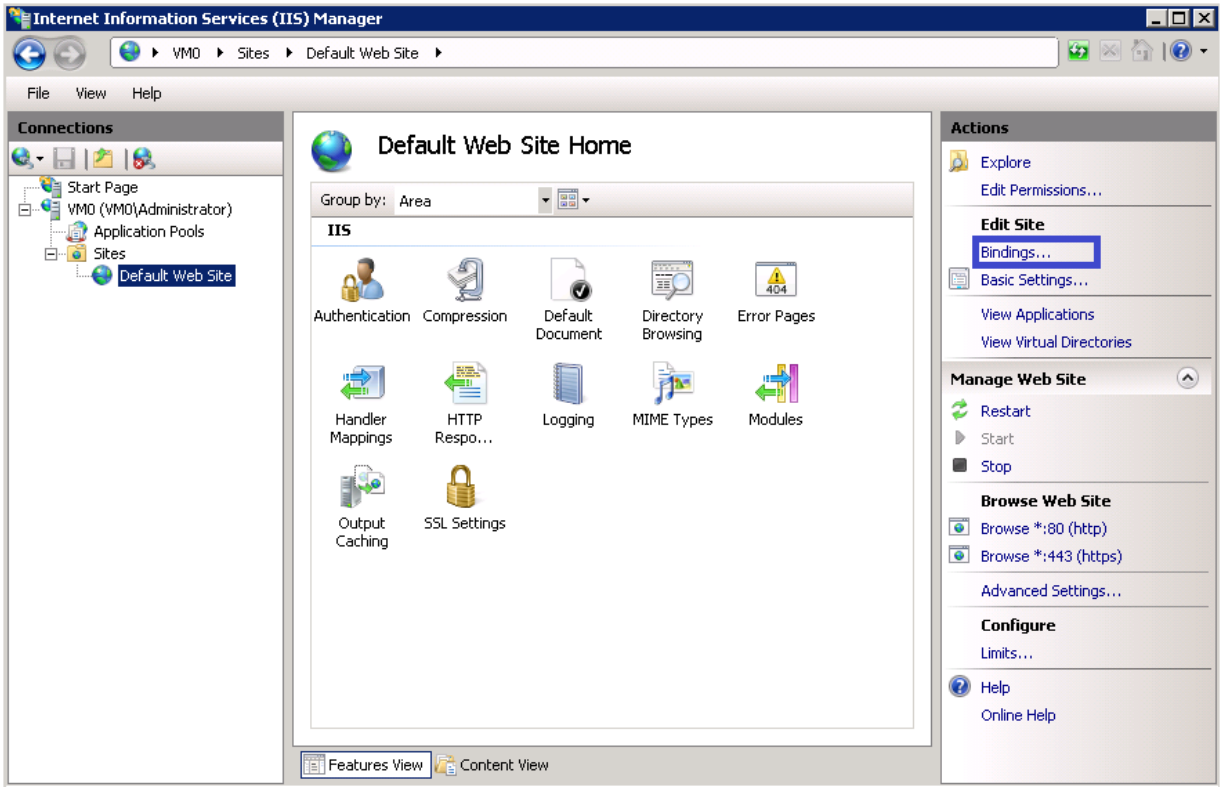
   A certificate request must be completed on the computer where it was created.

   Click here for the resolution to this message.

In IIS7, you need to install the certificate and then bind the HTTPS protocol to the site

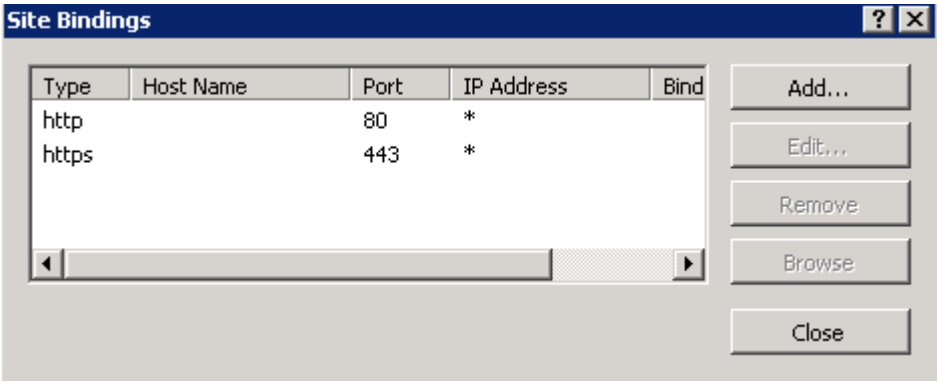
Step 3: Binding certificate to the web site:

1. Click **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**
2. Browse to your server name > Sites > Your SSL-based site
3. In the **Actions** pane, click **Bindings**.



4. In the Site Bindings window scroll down**, highlight HTTPS** and click **Remove.**

NOTE: If you wanted to secure traffic between IIS and Citrix Secure Gateway, edit the binding and change the **port to 444** or some
other non-well known TCP port. For best performance, it is only recommended to secure traffic when IIS and CSGare on different
servers



5. Click **OK**

Step 4: Configure Citrix Secure Gateway

To configure Citrix Secure Gateway, perfom the steps from here.

Step 5: Verify certificate installation:

1. Verify your installation with the Symantec Installation Checker.
2. In some cases you may need to **Stop** and **start** your Web server prior to any testing.

   NOTE: In some cases the changes may not take place after restarting IIS Services and a re-boot is needed.