SSL Certificate – Citrix Gateway Installation Guide



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

- 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.
- 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

📙 This Gateway			
Action			
📃 📃 General Networking 🔰 🌀 Name Service Pro	viders 🛛 🕂 Routes 🛛 🙆 Failover Servers 🗍		
Date 🖾 Certificate Signing Requi	est 🔬 🔊 Advanced Options		
Logging/Settings 📃 🦳 Administratio	n 📃 Statistics 🦪 Licensing		
Access management			
Enable external administration	Apply Change		
Allow ICMP traffic	Apply Change		
Secure certificate management			
Manage trusted root certificates	Manage		
Upload a .crt signed certificate	Browse		
Upload a .pem private key and signed certificate	Browse		
Upload a .pem private key and client certificate	Browse		
Upgrade and configuration management			
Save the current configuration	Save Configuration		
Upload an upgrade or saved configuration	Browse		
Access Gateway management			
Initialize the appliance	Initialize		
Restart the appliance	Restart		
Shut down the appliance	Shut down		

- 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. <u>Download the Intermediate CA certificate</u>.

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

 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----[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

📙 This Gateway					
Action					
📃 General Networking 🔰 🦪 Name Service F	Providers	+ Routes	👌 Failover Servers		
🔲 Date 🖧 Certificate Signing Reg	uest	<u> </u>	Advanced Options		
🗹 Logging/Settings 📃 🔍 Administra	tion	📰 Statistics	of Licensing		
Access management					
Enable external administration		Apply Ch	ange		
Allow ICMP traffic		Apply Ch	ange		
-Secure contilicate management					
Manage trusted root certificates		Manage			
Upload a .crt signed certificate		Browse			
Upload a .pem private key and signed certificate		Browse	a		
Upload a .pem private key and client certificate		Browse	ə		
Upgrade and configuration management					
Save the current configuration		Save Config	uration		
Upload an upgrade or saved configuration		Browse	e		
Access Gateway management					
Initialize the appliance		Initializ	e		
Restart the appliance		Resta	rt		
Shut down the appliance		Shut do	wn		

- 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 <u>Symantec SSL Certificate Checker</u>.

Installation Instructions for Citrix Access Gateway 5.0

Step 1: Obtain and install the SSL Certificate

- 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.
- 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.

ccess	s Gateway						Help	Logout CIT
onitor	Management Certificates	Snapshots					Search	Restart Shut Do
tricate	Management		al secolaria					
You can	view the certificates installed on Acco	iss Galeway, including si	rver, root, or intermediate	certificates, as well as t	the details of pending Cert	ficale		
Signing R	lequests. You can also install either Pf	EM or PCKS#12 certificate	s stored on your compute	r by clicking import.			Føer.	All
All Cer	rtificates							\frown
	Name	Description	Status	Valid From	Valid To	Туре	Active	Import ·
副級	10.20.30.40	Self Generated/Signed		09/26/2011	09/25/2012	Server	(後期)限(Constant State
	xer8-XENDC83-CA	<imported></imported>		07/01/2008	07/01/2018	Root or intermediate	su-merico d	Rent Contractor
1935	citte net	<inported-< td=""><td>- Henry Andreas</td><td>09/26/2011</td><td>09/25/2013</td><td>Server</td><td>4</td><td></td></inported-<>	- Henry Andreas	09/26/2011	09/25/2013	Server	4	
							5 A 1	Stan Maker Active
3387							R DEGENING	det dimit
					STATISTICS AND		51 00705078	With Reading
100 California 100 California 100 California					However		economic e	Details
							n www.	Delete
1.00							C S PARA STATUL	
8							18	
1.553							C. Prantationante BA	

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.

- 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.

nitor	Management Certificates	Snapshots					Search	Restart Shut f
toficate	Management							
					an a			
iou can Signing P	view the certificates installed on Acce Requests. You can also install either PE	ss Gateway, including se M or PCKS#12 certificate	rver, root, or intermediate stored on your compute	r certificates, as well as r by clicking import.	the details of pending Cert	ificale	Filler.	AR
								\sim
ALC .	Name	Description	Status	Valid From	Valid To	Type	Active	
	10 20 30 40	Self Generated/Signed		09/26/2011	09/25/2012	Server		amport
	xer8-XENDC83-CA	<imported></imported>		07/01/2008	07/01/2018	Root or intermediate		(Chinesesser)
THE ST	citte net	<inportativ< td=""><td></td><td>09/26/2011</td><td>09/25/2013</td><td>Server</td><td>4</td><td>New</td></inportativ<>		09/26/2011	09/25/2013	Server	4	New
	and the second sec						1 A 1	See Make Activities
							9889995 (Aug. Asimilar
							amana	
							denue a la competitione de la co	Details
102) 102)							ANTERNA A	Delete
							A REAL PROPERTY AND	
							1469436650	

- 4. Click **Import** and then select **Trusted** (.pem).
- 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**.

tificate	e Management							
du car	n view the certificates installed on Ac Requests. You can also install either	cess Galeway, including s PEM or PCKS#12 certificate	erver, root, or interm s stored on your co	rediate certificates, as well reduter by clicking import.	as the details of pending	Certificate	Filter.	AB
ABC	ertificates							
	Name	Description	Statue	Valid From	Valid To	Туре	Active	Import
	10.20.30.40	Self Generated/Signed		09/26/2011	09/25/2012	Server		Export (.pem)
	xer8-XENDC83-CA	<imported></imported>		07/01/2008	07/01/2018	Root or intermediate	n la constant de la c	Street New Lorented
0.555	cittensi	 suboting. 		09626/2011	09/25/2013	Server	4	
							uit manani di	Make Active
							5X, 16363484457 17	Self-Signert
							5 CIN9776	
								Details
								Delete
-				Í.			and the second second	
Certil	ficate chain for 'amylab.eng.citrite	e.net'	0.000	Constant Pro-			No.	\frown
0.000						1		E

- 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 <u>Symantec Installation Checker</u>.

Installation Instructions for Citrix Access Gateway 8.0

Step 1. Obtain the SSL Certificate

- 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.
- 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.

etails	e* _access.company.com		
Certificate and key file	es are stored in the folder /ns	config/ssl/ on Remote System.	
file Location	🔵 Local System 🛛 💿 Remot	e System	
Certificate Filename*	agee.cer	Browse	Insert
(ey Filename	agee.key	Browse	Insert
Password	•••••		
Format	PEM O DER		
xpiry Monitor) Enable 💿 Disable		
lotification Period			

- 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**
- 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.
- 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. <u>Download the Root CA certificate for your SSL product</u>.
- 2. <u>Download the Intermediate CA certificate</u>.

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.
- Specify the appropriate values in the various fields of the Install Certificate dialog box. The following screenshot displays the sample values for your reference:

install Certificate		
Certificate-Key Pair Name	* MyIntermediateCertificate	
Details		
Certificate and key file	s are stored in the folder /nsconfig/ssl/ o	on appliance.
Certi <u>f</u> icate File Name*	/nsconfig/ssl/myintermediate.crt	👰 Browse (Appliance) 🔹 🛃 Insert
Pri <u>v</u> ate Key File Name		🥥 Browse (Appliance) 🔹 න Insert
Pass <u>w</u> ord		
Certificate Format		
Notify When Expires) Enable () Disable	
Notification Period		
) Help 🔏 Quick Link		InstallClose

- 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:

4	Link Server Certifica	ate(s)
	C <u>A</u> Certificate Name	MyIntermediateCertificate 💌
	@ <u>H</u> elp	QK Close

11. Verify your installation with the <u>Symantec SSL Certificate Checker</u>.

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. <u>Method 2 (recommended)</u>: 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 <u>here</u>.

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 <u>click here</u>.

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
- 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 <u>here</u> 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

e Bindiı	ngs			?
Туре	Host Name	Port	IP Address Bind	Add
http		80	*	
https		443	*	Edit
				Remove
•			Þ	Browse
				Close

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 <u>Symantec Installation Checker</u>.
- 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.