

Server Certificate Installation steps:

To install the Server Certificate, complete the following steps:

Note: These steps are based on NSv9.1.

Step 1: Copy and paste the Server Certificate (including the BEGIN and END tags) into a text editor such as Notepad and save it on your local computer.

To install the Server Certificate, complete the following steps:



Step 2: Use a program such as WinSCP (<u>http://winscp.net</u>) to copy the Server Certificate file from the Local Computer to the NetScaler appliance. Certificate files are stored in the folder /nsconfig/ssl on the appliance.

Step 3: From the NetScaler GUI, select **NetScaler > SSL > Certificates**.



Step 4: From bottom of the NetScaler GUI, click Add.

CITRIX.	NetScaler			
Welcome nsroot@10.4.230.5(n	etscaler.entrust.com)	Mo	onitoring Configuration	
🗟 🥥 NetScaler 10.4.230.5	SSL Certificates			
 	Name	Certificate filename	Key filename	
	ns-server-certificate CA Cert - vpnlab.test ns-root netscaler netscaler-root 10.4.225.27 10.4.225.5	InsconfigIssI/ns-server.cert InsconfigIssI/ca-vpnlab.test.cer InsconfigIssI/ns-root.cert InsconfigIssI/netscaler.test.cert.cert InsconfigIssI/netscaler.test.cert-root.cert InsconfigIssI/10.4.225.27.cert InsconfigIssI/10.4.225.5.cert	/nsconfig/ssl/ns-server.key /nsconfig/ssl/ns-root.key /nsconfig/ssl/netscaler.test.ce /nsconfig/ssl/netscaler.test.ce /nsconfig/ssl/10.4.225.27.key /nsconfig/ssl/10.4.225.5.key	
🕀 🥥 SSL Offload	10.4.225.20	/nsconfig/ssl/netscaler.entrust.com.cert.txt	/nsconfig/ssl/netscaler.entrus	

Step 5: In the Install Certificate window, supply the following information:

- A Certificate-Key Pair Name.
- The Certificate File Name. Browse to the location of your Server Certificate file.
- The **Private Key File Name**. Browse to the location of the private key file that was used to create the certificate signing request.
- Select **PEM** for the **Certificate Format**.

rtificate-key Pair Nam	e* citrixns.lab.entrust.com	
)etails		
Certificate and key file	s are stored in the folder /nsconfig/ssl/ on ap	pliance.
Ierti <u>f</u> icate File Name*	/nsconfig/ssl/citrixns.lab.entrust.com.cer	🤢 Browse (Appliance) 🔹 🛃 Insert
Pri <u>v</u> ate Key File Name	/nsconfig/ssl/citrixns.lab.entrust.com.key	🧔 Browse (Appliance) 🔹 🎒 Insert
ass <u>w</u> ord		
Certificate Format		
lotify When Expires () Enable 💿 Disable	
lotification Period		



Step 6: Click **Install** to install the Server Certificate.

Step 7: Click **Close** to close the Install Certificate window.

Step 8: Find the Server Certificate just installed in the list of SSL Certificates. Right-click the certificate and select **Link.**

CITRIX.	NetScaler		
Welcome nsroot@10.4.230.5(nets)	saler.entrust.com)	_	Ma
 Gertificates Certificates Cipher Groups CRL Policies SSL Offload SSL Offload SSL Offload SSL Offload PopExpert Compression Integrated Caching Protection Features NTML Injection AAA - Application Traffic Content Switching 	Name ns-server-certificate ns-root netscaler netscaler-root 10.4.225.5 citrixns.lab.entrust.com Entrust 2048 Entrust L1C Chain Entrust 1024 Entrust L1E Chain Entrust Root Chain	Add Details Remove Remove Link Copy Pro	Certificate filename /nsconfig/ssl/ns-server.cert /nsconfig/ssl/netscaler.test.cert.cert /nsconfig/ssl/netscaler.test.cert-root.cert /nsconfig/ssl/10.4.225.5.cert /nsconfig/ssl/10.4



Step 9: Select the L1C Chain Certificate from the drop-down menu. If the L1C Chain Certificate is not in the list of available CA Certificate Names, follow the instructions for <u>L1C Chain Certificate Installation</u>.



Note: For Extended Validation (EV) certificates, link the Server Certificate to the L1E Chain Certificate instead of the L1C.

🎂 Link Server Certi	ificate(s) 🛛 🔀
C <u>A</u> Certificate Name	Entrust L1E Chain 👻
⊘ Help	OK Close

If the L1E Chain Certificate is not in the list of available CA Certificate Names, follow the instructions for <u>EV Chain</u> <u>Certificate Installation</u>.



Step 10: Click **OK** to link the certificates. You should see a dialog box confirming that the certificates were linked successfully. Click **OK**.



Step 11: Verify the certificate links by clicking **Cert Links** at the bottom of the NetScaler GUI. If the L1C Chain Certificate is not linked to the issuing CA, follow the instructions for <u>L1C Chain Certificate Installation</u>.

	Cercivanie	Issuer CA Name
	netscaler	netscaler-root
	citrixns.lab.entrust.com Entrust L1C Chain	Entrust L1C Chain Entrust 2048
Format: PEM	2) Help	Close

Step 12: The Server Certificate is ready to be bound to an SSL Virtual Server within the NetScaler. From the NetScaler GUI, select **NetScaler / Access Gateway / Virtual Servers**.



Step 13: From the **Certificates** tab, select the Server Certificate from the list of **Available** certificates. Click **Add** to add the certificate to the **Configured** list.

CITRIX:	NetScaler								NS9.1
Welcome nsroot@10.4.230.5(nets	caler.entrust.com))				Monitoring	Configuration	Dashboard	Reporting
									Settings
🖃 🥥 NetScaler 10.4.230.5	Access Gateway V	rtual Serve	rs						4
E 😡 System	Name		State	IP	Address		Port Proto	col	
ONS	Public		42.UP	10	4.225.20	40	443 55		
B OSL		🖆 Configure Access Gateway Virtual Server 🛛 🔯							×
G SSL Offload G AppExpert		Name*	Public			IP	Address 10 . 4	. 225 . 20	
E 🧧 Compression		Protocol*	SSL			- Po	rt* 443		
🗄 🍘 Integrated Caching		[Thirty.	rk VServer Range	e It		Ma	v Lisers 0		
Vite Toiseties		Davis	etata fluch	7 IX					
E Cal Load Balancing		Down	scace push						
🕀 🔞 AAA - Application Traffic		Certific	ates \ Authenticati	ion \ Bookmarks	Policies Intranet Applica	tions \ Intranet IP	s Published Applic	ations \	
🕀 🧃 Content Switching		SSL	Parameters	Ciphers					
(a) Cache Redirection		A				Confirmed			
E G Rewrite		Availa	able			Configured	 425000 	C. Transferrer of process	
G Responder		Certifi	cates			Certificates	Type	CRL Mandator	У
	ss Gateway Global Settings Virtual Servers Groups Users Policies Resources ication Firewall is disabled. tion Pane		ver-certificate rt - vpnlab.test t iler- ver-root 125.27 125.5 125.20 s.lab.entrust.com t 2048 t L1C Chain		Add >> Add as CA > < Remove Instal •	otrons.lab.entr	Send Server Ceronicate		
Feature is disabled. Navigation Pane			To bind a Certificate to Access Gateway Virtual Server, select a certificate on the left and click 'Add'. To bind a Certificate to Access Gateway Virtual Server as CA, select a certificate on the left and click 'Add as CA'. To configure SSL parameters, click 'SSL Parameters'. To configure ciphers, click 'Ciphers'.						

Step 14: Click **OK** and save the configuration.