SSL Certificate – IBM Installation Guide



Please select your version

Installation Instructions for IBM AS 400 / iSeries server

Installation Instructions for IBM HTTP Server running IKEYMAN GUI

Installation Instructions for IBM WebSphere using IKEYMAN GUI (Version 7)

Installation Instructions for IBM Websphere using the command line

Installation Instructions for IBM AS 400 / iSeries server

Step 1: Download the Symantec Intermediate CA Certificate

- 1. Download the Intermediate CA certificate from here
- 2. Select the appropriate Intermediate CA certificate for your SSL Certificate type.
- 3. Copy the Intermediate CA certificate and paste it on a Notepad.
- 4. Save the file as **intermediate.txt**

Step 2: Install the Symantec Intermediate CA Certificate

- 1. Start Digital Certificate Manager (DCM).
- 2. From navigation panel, click **Select a Certificate Store** > select ***SYSTEM**

	Digital Certificate Manager
	Select a Certificate Store
	Select the certificate store that you want to open.
and a contract of the	 Local Certificate Authority (CA)
Select a Certificate Store	SYSTEM
	 Other System Certificate Store
Expand All Collapse All	Continue Cancel

- 3. Enter in password for Certificate Store > click **Continue**
- 4. From navigation panel, select Manage Certificates
- 5. From the list, select Import Certificate > Certificate Authority (CA) > click Continue

Expand All Collapse All	^	Digital Certificate Manager
▶ <u>Fast Path</u>		Import Certificate
<u>Create Certificate</u>		Certificate store: *SYSTEM
<u>Create New Certificate Store</u>		
 Install Local CA Certificate on Your PC 	=	Select the type of certificate that you want to import.
▼ <u>Manage Certificates</u>		Server or client
 <u>Renew certificate</u> 		Certificate Authority (CA)
<u>Import certificate</u>		
Export certificate		Continue

6. On the next screen, specify the path and file name of intermediate ca certificate. This is the location and name of the intermediate ca file on the IFS of the iSeries.

Example: The file is stored in the /home directory and the intermediate ca file was called 'cert.txt' you would put in a path and file name of /home/cert.txt.



7. Click Continue

8. Create a CA certificate label. This can be any name desired as long as it is unique (should not match any labels for any other certificates).

Example: CA certificate label: Certificate Authority Name



9. Click Continue

10. A message stating the intermediate ca certificate has been imported. Click OK

Expand All Collapse All	^	Digital Certificate Manager @ IBM.
▶ <u>Fast Path</u>		Import Certificate Authority (CA) Certificate
<u>Create Certificate</u>		Message The certificate has been imported
<u>Create New Certificate Store</u>		Message The certainate has been imported.
 <u>Install Local CA Certificate on</u> <u>Your PC</u> 	Ш	Use the Manage Applications task if you want to specify that applications trust this Certificate Authority (CA).
 ✓<u>Manage Certificates</u> <u>View certificate</u> 		ОК

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

The text file should look like:

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

[encoded data]

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

3. Save the file with extansion **.txt**

Step 4: Install the SSL Certificate

- 1. Start Digital Certificate Manager (DCM).
- 2. From navigation panel, click Select a Certificate Store > select *SYSTEM
- 3. Enter in password for Certificate Store > click **Continue**
- 4. From navigation panel, select Manage Certificates
- 5. From the list, select **Import Certificate** > select **Server or Client**
- 6. Select the certificate file and complete wizard
- 7. Verify certificate installation using the <u>Symantec Installation Checker</u>.

Installation Instructions for IBM HTTP Server running IKEYMAN GUI

Step 1: Download the Symantec Intermediate CA Certificate

- 1. Download the Intermediate CA certificate.
- 2. Select the appropriate Intermediate CA certificate for your SSL Certificate type.
- 3. Copy the Intermediate CA certificate and paste it on a Notepad.
- 4. Save the file as **intermediate.cer**

Step 2: Install Symantec Intermediate CA Certificate

1. Start the key management utility (iKeyman):

On Windows: Go to the start UI and select Start Key Management Utility

On AIX, Linux or Solaris: Type ikeyman on the command line

- 2. Open the key database file that was used to create the certificate request.
- 3. Enter the password, then click **OK.**
- 4. Click on the "down arrow" to the right, to display a list of three choices.
- 5. Select Signer Certificates, then click Add.
- Click Data Type and select a data type, such as Base64-encoded ASCII data.
 NOTE: This data type must match the data type of the importing certificate.
- Enter a file name and location for intermediate.cer digital certificate or click Browse to select a file name and location.
- 8. Click OK.
- 9. Enter a label for importing certificate, for example: Intermediate CA
- 10. Click **OK**.
- 11. The Signer Certificates field displays the label of the signer certificate you added.

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.
- Copy and paste the certificate into a text file using Vi or Notepad The text file should look like:

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

[encoded data]

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

3. Save the file with extension .cer

Step 4: Install the SSL Certificate

1. Open the .kdb file using the iKeyman utility:

On Windows: Go to the start UI and select Start Key Management Utility

On AIX, Linux or Solaris: Type ikeyman on the command line

- 2. In the middle of the iKeyman GUI you will see a section called Key database content
- 3. Click on the "down arrow" to the right, to display a list of three choices
- 4. Select Personal Certificates

Key database content	
Personal Certificate Requests	▼ N
Personal Certificates	
Personal Certificate Requests	De
Signer Certificates	
	V
	Ext

5. From the **Personal Certificates** section, click **Receive**

DB-Type:	CMS key database file		
File Name:	C:\Program Files\IBM HTTP Server\ssNtest.kdb		
[Key databa	ise content	
Personal	Certificates	Receive	
		Receive the certificate you req	uested
		View/Edit	
		Import	

6. Data Type - leave the default of "Base64-encoded ASCII data"

Data type	Base64-encoded ASCII data 💌	
Certificate file name:	*.arm	Browse
Location:	C1	

- 7. Browse to the directory that contains the .cert or .arm file
- 8. Highlight the file and click **Open**.
- 9. Now click **OK** on this dialog box

Data type	Base64-encoded ASCII data 💌	
Certificate file name:	certresponse.arm	Browse
Location:	C:\Program Files\IBM HTTP Server\ssl\	

Step 5. Transfer Certificate

1. To extract an SSL certificate from a key database file and store it in a CA key ring file, start the iKeyman graphical user interface

2. Run following command:

On Windows: strmqikm

On UNIX: gsk7ikm

- 3. Choose **Open** from the **Key Database File** menu. Click **Key database type**, and select **CMS**.
- 4. Click **Browse** to navigate to the directory containing the key database files
- 5. Select the key database file to which you want to add the certificate. For example, key.kdb.
- 6. Click Open
- 7. In the Password Prompt window, type the password you set when you created the key database and then click **OK**.
- 8. Select **Signer Certificates** in the Key database content field, and then select the certificate you want to extract.
- 9. Click Extract.
- 10. Select the Data type of the certificate. For example, Base64-encoded ASCII
- 11. Click **Browse** to select the name and location of the certificate file name.
- 12. Click **OK.** The certificate is written to the file you specified.
- 13. Verify certificate installation using the Symantec Installation Checker.

Installation Instructions for IBM WebSphere using IKEYMAN GUI (Version 7)

Step 1: Download the 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 Notepad.
- 3. Save the file as **intermediate.cer**

Step 2: Install Symantec Intermediate CA Certificate

1. Start the key management utility (iKeyman):

On Windows: Go to the start UI and select Start Key Management Utility

🦉 IBM Key Managemen	t - [C:\HTTPServerTest\test.kdb]		🗖 🗗 🔀
Key Database <u>File</u> <u>C</u> reat	te <u>V</u> iew <u>H</u> elp		
🗅 🚄 🗖 😽			
		Key database information	
DB-Type: CMS		rey uatabase information	
File Name: C1HTT	PSenerTestitest krih		
Token Label:	- contra -		
		Kau databana pantant	
		ney uarabase content	
Signer Certificates			<u>A</u> dd
primary CA		_	Delete
Admin			Vie <u>w</u> /Edit
			Extract
Internet	🎯 Set Program Access and Defaults		Denulate
E mail	🐝 Windows Catalog		Populate
Outlook Express	🌯 Windows Update		Rena <u>m</u> e
~	Accessories		
Notepad	🛅 Games 🔹 🕨		
IBM Key Managemen	🛅 Startup 🕨		
	Internet Explorer		
📏 Start Admin Server	MSN Explorer		
Mozilla Eirefox (Safe	Benete Assistance		
	Windows Media Player		
Set Program Access	& Windows Messenger	Start Admin Server	
	💼 Mozilla Firefox 🔹 🕨	Start HTTP Server	
M5N Explorer	🛅 eToken 🔹 🕨	🧱 Start Key Management Utility	
	🛅 IBM WebSphere MQ 🔹 🕨	🔪 Stop Admin Server	
All Programs 🕨	💼 IBM HTTP Server ¥7.0 🛛 🔸	Stop HTTP Server	
	🔎 Log Off 🛛 🗖 Turp Off Comput	AF .	
🏭 start 🔰 😂 😫) 🎯 🦈 🗁 HTTPServerTest	🚇 Start Key Manageme 🔯 IBM Key Management	4:17 PM

On AIX, Linux or Solaris: Type ikeyman on the command line

2. Open the key database file that was used to create the certificate request.

🌉 IBM Key Mar	nagement - [C:\HTTPServerTest\test.kdb]		
Key Database <u>F</u> i	le <u>C</u> reate <u>V</u> iew <u>H</u> elp		
	3 😤 🚯 🔤		
		Key database info	formation
DB-Type:	CMS		
File Name:	C:\HTTPServerTestitest.kdb		
Token Label:			
		Key database c	content
Personal Certi	ficate Requests		▼ Ne <u>w</u>
Open			
Key databas	e type CMS 💌	Look <u>i</u> n:	THTTPServerTest
File Name:	key kdb	Browse	db Extract
Leastian	C4LITTPConvertice#		
Location.			
	<u>Q</u> K <u>C</u> ancel		
		File <u>N</u> ame:	e: test.kdb
		Files of Ty	/pe: Key database type (*.kdb)
			Open
			Open Cancer
The requested a	ction has successfully completed!		
# start	🖉 🔮 🙋 » 🎦 HTTPServerTest 🛛 🚺 Start Key Managi	eme 🌇 IBM Key Management	. 3:11 PM

3. Enter the password, then click **OK.**

BBM Key Management - [C:\HTTPServerTest\test.kdb]		💶 🗗 🔀
KeyDatabase Eile Create View Help		
Key database information		
DB-Type: CMS		
File Name: C1HTTPServerTestitestkdb		
Token Label:		
Key database content		
Personal Certificate Requests	-	Ne <u>w</u>
vincent.symantec.com		Delete
		View
Password Prompt		Extract
Password:		
<u>OK</u> <u>Reset</u> <u>Cancel</u>		
1		
The requested action has successfully completed!		
🔧 start 🖉 🖉 🥙 🖻 HTTPServerfest 🛛 🔯 Start Key Management		🔇 3:12 PM

4. Select Signer Certificates, then click Add.

🌉 IBM Key Man	agement - [C:\	HTTPServerTest\test.kdb]					
Key Database <u>F</u> il	le <u>C</u> reate <u>V</u> ie	w <u>H</u> elp					
	3 😤 🕵	<u>6.</u>					
				Key database inform	nation		
DB-Type:	CMS						
File Name:	C:\HTTPServe	rTestttest.kdb					
Token Label:							
				Key database con	tent		
Personal Certif	ficate Requests					•	Ne <u>w</u>
Personal Certif	icates						Delete
Signer Certifica	ates licato Requests						Delete
Personal Certi	icate Requests						View
							Extract
The second t	-4:						
The requested ac	ction has succe	sstully completed!	L m				
🥶 start	ා 🙂 🕑 🏈	HTTPServerTest	🛄 Start Key Manageme	IBM Key Management			3:12 PM

- 5. Click Files of Type and select All Files.
- 6. Enter a file name and location for **intermediate.cer** digital certificate or click **Browse** to select a file name and location.

🦉 IBM Key Man	agement - [C:\HTTPServerTest\test.kdb]		- - X
Key Database <u>F</u> il	le <u>C</u> reate <u>V</u> iew <u>H</u> elp		
	3 😤 🕵 🗔		
		Key database information	
DB-Type:	CMS		
File Name:	C3HTTPServerTestitest.kdb		
Token Label:			
		Kaudatahaaa aantant	
Signor Cortific	ator	🚇 Open 🛛 🔀 — 🔄	- Add
Signer Certifica	ales		<u>A</u> dd
			Delete
	_	Certreq.arm	Vie <u>w</u> /Edit
	Ope	Secondary.cer	Extract
	Eile	n test.rdb	Populate
	Loc	T test.sth	
			Rename
		File Name: primary cer	
		Files of Type:	
		Open Cancel	
l			
The requested a	ction has successfully completed!		
🛃 start	😂 🙋 🧭 🐣 🗁 HTTPServerTest 🛛 🚇	Start Key Manageme 🏨 IBM Key Management	🔇 3:16 PM

- 7. Click OK.
- 8. Enter a label for importing certificate, for example: Intermediate CA



- 7. Click OK.
- 8. The Signer Certificates field displays the label of the signer certificate you added.

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 The text file should look like:

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

[encoded data]

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

3. Save the file with extension .cer

Step 4: Install the SSL Certificate

1. Start the key management utility (iKeyman):



On Windows: Go to the start UI and select Start Key Management Utility

On AIX, Linux or Solaris: Type ikeyman on the command line

2. Choose **Open** from the **Key Database File** menu. Click **Key database type**, and select **CMS**.

Key Database Ele Create Vew Help	
Key database information	
Ney database mornation	
DB-Type: CMS	
File Name: C1HTTPServerTesttest.kdb	
Token Labet:	
Key database content	
Personal Certificate Requests	
Concerning the Open	
Key database type CMS View	
File Name: key kdb Browse	
Location: C:HTTPSenerTect	
QK Cancel	
The Menness I and July	
File game: lestration de la batti	
ries of <u>uppe</u> : <u>rey database type (-kap)</u>	
Open Cancel	
The semiconductive has encounterfully completed	
nne requesteu action nas successitairy compreteur.	3:11 PM

- 3. Click **Browse** to navigate to the directory containing the key database files.
- 4. Select the key database file to which you want to add the certificate. For example, key.kdb.
- 5. Click **Open**
- 6. In the Password Prompt window, type the password you set when you created the key database and then click **OK**.

🛄 IBM Key Management - [C:\HTTPServerTest\te	st.kdb]		- 8 🛛	
Key Database <u>F</u> ile <u>C</u> reate <u>V</u> iew <u>H</u> elp				
		Key database information		
DB-Type: CMS				
File Name: C:\HTTPServerTest\test.kdb				
Token Label:				
		Key database content		
Personal Certificate Requests		~	Ne <u>w</u>	
vincent.symantec.com			Delete	
			View	
	Dares	word Promot	Extract	
	Pass	word:		
		OK Reset Cancel		
The requested action has successfully completed!				
🛃 start 🛛 🖄 🥹 🧭 🐣 HTTPServerTest	Start Key Manageme	IBM Key Management	🔇 3:12 PM	

7. Select the **Personal Certificates** view.

🌉 IBM Key Mana	gement - [C:\HTTPServerTest\test.kdb]					
Key Database <u>F</u> ile	<u>C</u> reate <u>V</u> iew <u>H</u> elp					
	😤 🕵 🎩					
			Key database informa	ion		
DB-Type:	CMS					
File Name:	C:\HTTPServerTest\test.kdb					
Token Label:						
			Key database conte	t		
Personal Certific	ates				•	Receive
Personal Certific	ates					Delete
Personal Certific	ate Requests					
						Vie <u>w</u> /Edit
						Import
						Recre <u>a</u> te Request
						Rename
						New Self-Signed
						Extract Certificate
						P
The requested act	ion has successfully completed!	Y				
🛃 start 🔰	🖉 ڬ 🎯 🐣 🗁 HTTPServerTest	🚺 Start Key Manageme	IBM Key Management			4:38 PM

8. Click **Receive**

🦉 IBM Key Man	agement - [C:\HTTPServerTest\test.kdb]					- 2 🛛
Key Database <u>F</u> il	e <u>C</u> reate <u>V</u> iew <u>H</u> elp					
	I 😤 🕵 💶					
			Key database inform	ation		
DB-Type:	CMS					
File Name:	C:\HTTPServerTest\test.kdb					
Token Label:						
			Key database com	ent		
Personal Certif	icates				•	Receive
						Delete
						Vie <u>w</u> /Edit
		Open				Import
		File Name: cert.a	rm TPServerTesñ	<u>B</u> rowse.	·	Recreate Request
		Feenuer	OK Car	cel		Rename
						New Self Signed
						non confoightum
						Extract Certificate
The requested ac	tion has successfully completed!					
🛃 start 🚽	🚿 🔮 🞯 👋 🛅 HTTPServerTest	🚺 Start Key Manageme	🚇 IBM Key Management			🔇 4:38 PM

9. Click **Browse** to select the name and location of the certificate file name.

🚆 BM Key Management - [C:\HTTPServerTest\test.kdb]	- 2 🛛				
Key Database File _Create _View Help					
Key database information					
DB-Type: CMS					
File Name: CAHTTPServerTesttest.kdb					
Token Label:					
Key database content					
Personal Certificates	▼ Receive				
🔯 Open	Delete				
Look In: THTPServerTest	Vie <u>w</u> /Edit				
	Import				
Browse	Recreate Request				
secondary.cer	Rename				
File Name: certarm					
Files of Type: Key file type ('.cer, '.arm, '.ber, '.der, '.eml)					
Open Cancel					
	New Self-Signed				
	Extract Certificate				
The requested action has successfully completed!					
A Start A A A A A A A A A A A A A A A A A A A	4:39 PM				

10. Click OK

11. Verify certificate installation using the <u>Symantec Installation Checker</u>.

Installation Instructions for IBM Websphere using the command line

Step 1: Download the Symantec Intermediate CA Certificate

- 1. Download the Intermediate CA certificate.
- 2. Select the appropriate Intermediate CA certificate for your SSL Certificate type.
- 3. Copy the Intermediate CA certificate and paste it on a Notepad.
- 4. Save the file as **intermediate.cer**

Step 2: Install Symantec Intermediate CA Certificate

1. Run following command to add the **intermediate.cer** into the key database:

For UNIX:

gsk7cmd -cert -add -db filename -pw password -label label -file filename -format ascii

For Windows:

runmqckm -cert -add -db filename -pw password -extensionel -file filename -format ascii

- -db filename is the fully qualified file name of a CMS key database, for example: dbkey.kdb
- -pw password is the password for the CMS key database with an extansion .cms
- -label is the key label attached to the certificate, for example:
 "ibmwebspheremqqmname"
- **-file** filename is the fully qualified file name of the file containing the Intermediate CA certificate, for example intermediate.cer
- **-format** ascii is the format of the certificate. The value can be ascii for Base64encoded ASCII. The default is ascii.

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.
- Copy and paste the certificate into a text file using Vi or Notepad The text file should look like:

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

[encoded data]

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

3. Save the file with extension .cer

Step 4: Install the SSL Certificate

1. To install a certificate in iKeycmd (using UNIX command line), run following command:

For UNIX:

gsk7cmd -cert -receive -file filename -db filename -pw password -format ascii

For Windows:

runmqckm -cert -receive -file filename -db filename -pw password -format ascii

- **-file** filename is the fully qualified file name of the file containing the personal certificate.
- -db filename is the fully qualified file name of a CMS key database, for example: dbkey.kdb
- -pw password is the password for the CMS key database with an extansion .cms
- -label is the key label attached to the certificate, for example:
 "ibmwebspheremqqmname"

• **-format** ascii is the format of the certificate. The value can be ascii for Base64encoded ASCII. The default is ascii.

Steps 5: Extract SSL Certificate

1. To extract a certificate in iKeycmd, run following command:

For UNIX:

gsk7cmd -cert -extract -db filename -pw password -label label -target filename format ascii

For Windows

runmqckm -cert -extract -db filename -pw password -label label -target filename format ascii

- -db filename is the fully qualified pathname of a CMS key database.
- -pw password is the password for the CMS key database with an extansion .cms
- -label label is the label attached to the certificate.
- **-target** filename is the name of the destination file
- **-format** ascii is the format of the certificate. The value can be ascii for Base64encoded ASCII. The default is asci.
- 2. Verify certificate installation using the <u>Symantec Installation Checker</u>.