

# Sterling Connect:Direct for z/OS

## Receiving a CA signed certificate

© 2016 IBM Corporation

This presentation will show you how to receive a CA signed certificate to use with Sterling Connect:Direct® for z/OS®. You will learn how to receive the CA signed certificate and import issuer certificates by using IBM GSKKYMAN, which is a component of z/OS.



## Create signed certificate files in UNIX System Services (USS)

- Highlight, copy, and paste each certificate into a separate .txt file and save them
- Transfer certificates to USS folder in text mode
- Avoid cut-and-paste instead of transfer



You must paste the contents of the signed certificate into a newly allocated text file. Copy from the beginning of the begin new certificate line to the end of the end new certificate line. Once pasted, press enter after the end of the last line and save the file.

You must then create further text files for each of the issuer certificates you receive from your certificate authority or CA. Then, you must transfer your certificates to your zSeries UNIX® System Services folder. Try to avoid the use of cut-and-paste instead of a transfer as pasting can be unreliable and introduce characters that will make the certificates unreadable.

## Start UNIX System Services (1 of 2)

- Enter 6 from the ISPF Primary Option menu

```

Menu Utilities Compilers Options Status Help
-----
ISPF Primary Option Menu
Option ==> 6
0 Settings      Terminal and user parameters      User ID : AWARN1
1 View         Display source data or listings   Time. . . : 10:39
2 Edit         Create or change source data      Terminal. : 327BA
3 Utilities    Perform utility functions         Screen. . : 1
4 Foreground   Interactive language processing   Language. : ENGLISH
5 Batch        Submit job for language processing Appl ID . : ISR
6 Command     Enter TSO or Workstation commands TSO login : TRXACNT
7 Dialog Test  Perform dialog testing           TSO prefix:
9 IBM Products IBM program development products System ID : IRVK
10 SCLM        SM Configuration Library Manager MVS acct. : 1828
11 Workplace  ISPF Object/Action Workplace     Release . : ISPF 6.3
U User Apps   General User Applications
SD SDSF       System Display And Search Facility

Enter X to Terminate using log/list defaults

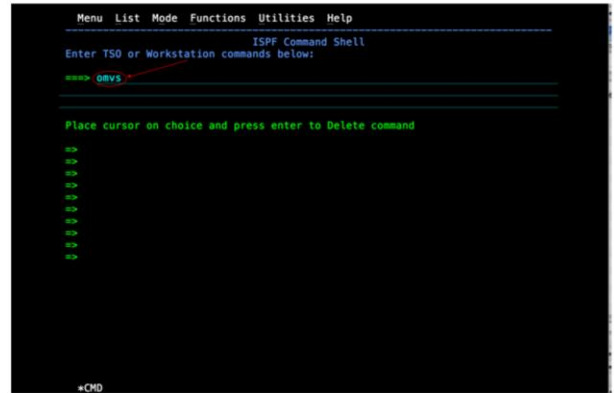
Licensed Materials - Property of IBM
5694-A01 Copyright IBM Corp. 1980, 2011.
All rights reserved.
US Government Users Restricted Rights -
Use, duplication or disclosure restricted
by GSA ADP Schedule Contract with IBM Corp.

*TSR@PRI
  
```

To receive a CA signed certificate and import issuer certificates to a z/OS key database, you need to access the GSKKYMAN application by using UNIX System Services or USS. If you are not already in OMVS or GSKKYMAN, key in 6 on the command line to enter TSO or workstation commands and press enter.

## Start UNIX System Services (2 of 2)

- Key in OMVS on the command line
- ENTER



```
Menu List Mode Functions Utilities Help
-----
ISPF Command Shell
Enter TSO or Workstation commands below:
=>>> OMVS
-----
Place cursor on choice and press enter to Delete command

=>>
=>>
=>>
=>>
=>>
=>>
=>>
=>>
=>>

*CMD
```

On the ISPF Command Shell panel, key in OMVS to access UNIX System Services. Press enter to continue.

## Start the Key Database menu

- Key in gskkyman
- ENTER

```
IBM
Licensed Material - Property of IBM
5694-ABI Copyright IBM Corp. 1993, 2011
(C) Copyright Morrice Kern systems, Inc., 1985, 1996.
(C) Copyright Software Development Group, University of Waterloo, 1989.

All Rights Reserved.

U.S. Government Users Restricted Rights -
Use, duplication or disclosure restricted by
GSA ADP Schedule Contract with IBM Corp.

IBM is a registered trademark of the IBM Corp.

$

====> gskkyman

ESC=q  1=Help      2=SubCmd  3=HlpRetrn  4=Top      5=Bottom   6=TSO
        7=BackScr   8=Scroll  9=NextSess 10=Refresh 11=PwdRetr 12=Retrieve
```

On the UNIX System Services panel, enter gskkyman to display the GSKKYMAN application menu options.

## Create a database

- Select option 2 – Open database
- ENTER

```
All Rights Reserved.
U.S. Government Users Restricted Rights -
Use, duplication or disclosure restricted by
GSA ADP Schedule Contract with IBM Corp.
IBM is a registered trademark of the IBM Corp.
$ gskkyman
Database Menu
1 - Create new database
2 - Open database
3 - Change database password
4 - Change database record length
5 - Delete database
6 - Create key parameter file
7 - Display certificate file (Binary or Base64 ASN.1 DER)
11 - Create new token
12 - Delete token
13 - Manage token
14 - Manage token from list of tokens
0 - Exit program
Enter option number:
*** 2 ***
ESC=q 1=Help 2=SubCmd 3=HlpRetrn 4=Top 5=Bottom 6=TSO INPUT
7=BackScr 8=Scroll 9=NextSess 10=Refresh 11=PwdRetr 12=Retrieve
```

From the Database Menu panel, you must select option 2 to open an existing database. Press enter to continue.

## Database name

- Key in your key database name.
- ENTER to continue.

```

U.S. Government Users Restricted Rights -
Use, duplication or disclosure restricted by
GSA AOP Schedule Contract with IBM Corp.

IBM is a registered trademark of the IBM Corp.

$ gskkyman

Database Menu

1 - Create new database
2 - Open database
3 - Change database password
4 - Change database record length
5 - Delete database
6 - Create key parameter file
7 - Display certificate file (Binary or Base64 ASN.1 DER)

11 - Create new token
12 - Delete token
13 - Manage token
14 - Manage token from list of tokens

0 - Exit program

Enter option number: 2
Enter key database name (press ENTER to return to menu):
====> cdkdb

ESC= 1=Help 2=SubCmd 3=HlpRetrn 4=Top 5=Bottom 6=TSO INPUT
      7=BackScr 8=Scroll 9=NextSess 10=Refresh 11=FwdRetr 12=Retrieve

```

You will see a request to enter a key database name. You must key in the name for your existing key database and enter to continue. You can return to the Database Menu by leaving the field blank and press enter if you want to continue later.



## Database password

- Enter the database password.
- ENTER to continue.

```
U.S. Government Users Restricted Rights -
Use, duplication or disclosure restricted by
GSA ADP Schedule Contract with IBM Corp.

IBM is a registered trademark of the IBM Corp.

$ gskkyman

Database Menu

1 - Create new database
2 - Open database
3 - Change database password
4 - Change database record length
5 - Delete database
6 - Create key parameter file
7 - Display certificate file (Binary or Base64 ASN.1 DER)

11 - Create new token
12 - Delete token
13 - Manage token
14 - Manage token from list of tokens

0 - Exit program

Enter option number: 2
Enter key database name (press ENTER to return to menu): cdkdb
Enter database password (press ENTER to return to menu):
====> *****

ESC=e 1=Help 2=SubCmd 3=HlpRetrn 4=Top 5=Bottom 6=150
7=BackScr 8=Scroll 9=NextSess 10=Refresh 11=PwdRetr 12=Retrieve

INPUT HIDDEN/INPUT
```

You will now see a request to enter a database password. Key in the database password and press enter to continue.

## Return to key management

- Go to GSKKYMAN
- Select option 2 – open database
- Enter key database name
- Enter key database password
- Select option 7 – Import a certificate

```

14 - Manage token from list of tokens
0 - Exit program

Enter option number: 2
Enter key database name (press ENTER to return to menu): cdkdb
Enter database password (press ENTER to return to menu):

Key Management Menu
Database: /u/awarn1/cdkdb
Expiration: None

1 - Manage keys and certificates
2 - Manage certificates
3 - Manage certificate requests
4 - Create new certificate request
5 - Receive requested certificate or a renewal certificate
6 - Create a self-signed certificate
7 - Import a certificate
8 - Import a certificate and a private key
9 - Show the default key
10 - Store database password
11 - Show database record length

0 - Exit program

Enter option number (press ENTER to return to previous menu):
==== 7

```

ESC=␣ 1=Help 2=SubCmd 3=HlpRetrn 4=Top 5=Bottom 6=TSO INPUT  
7=BackScr 8=Scroll 9=NextSess 10=Refresh 11=PwdRetr 12=Retrieve

You will now navigate to the key management menu in GSKKYMAN to import the issuer certificates and the newly requested certificate received from the certificate authority. Key in 7 to Import a certificate and press enter to continue.

## Import Root CA

- Enter path and file name of CA root certificate

```

0 - Exit program
Enter option number: 2
Enter key database name (press ENTER to return to menu): cdkdb
Enter database password (press ENTER to return to menu):

Key Management Menu

Database: /u/awarn1/cdkdb
Expiration: None

1 - Manage keys and certificates
2 - Manage certificates
3 - Manage certificate requests
4 - Create new certificate request
5 - Receive requested certificate or a renewal certificate
6 - Create a self-signed certificate
7 - Import a certificate
8 - Import a certificate and a private key
9 - Show the default key
10 - Store database password
11 - Show database record length

0 - Exit program

Enter option number (press ENTER to return to previous menu): 7
Enter import file name (press ENTER to return to menu):
====> cdcaroot.txt

ESC=␣ 1=Help      2=SubCmd   3=HlpRetrn  4=Top       5=Bottom   6=TSO
      7=BackScr   8=Scroll  9=NextSess 10=Refresh 11=PubRetr 12=Retrieve

```

You must start with the CA root certificate. Under Enter import file name, you will enter the name of the CA root certificate file. Press enter to continue.

## Enter CA root label (1 of 2)

- Key a label for the CA root certificate
- Enter

```

0 - Exit program
Enter option number: 2
Enter key database name (press ENTER to return to menu): cdldb
Enter database password (press ENTER to return to menu):

Key Management Menu
Database: /u/awarn1/cdldb
Expiration: None

1 - Manage keys and certificates
2 - Manage certificates
3 - Manage certificate requests
4 - Create new certificate request
5 - Receive requested certificate or a renewal certificate
6 - Create a self-signed certificate
7 - Import a certificate
8 - Import a certificate and a private key
9 - Show the default key
10 - Store database password
11 - Show database record length
0 - Exit program

Enter option number (press ENTER to return to previous menu): 7
Enter import file name (press ENTER to return to menu): cdcaroot.txt
Enter label (press ENTER to return to menu):
====> cdcaroot
INPUT
ESC=Q 1=Help 2=SubCmd 3=HlpRetrn 4=Top 5=Bottom 6=TSO
7=BackScr 8=Scroll 9=NextSess 10=Refresh 11=PwdRetr 12=Retrieve

```

You will then key in a label for your CA root certificate and press enter to continue.

## Enter CA root label (2 of 2)

- Certificate imported message displayed
- Enter

```
Enter database password (press ENTER to return to menu):
Key Management Menu
Database: /u/awarn1/cdkdb
Expiration: None
1 - Manage keys and certificates
2 - Manage certificates
3 - Manage certificate requests
4 - Create new certificate request
5 - Receive requested certificate or a renewal certificate
6 - Create a self-signed certificate
7 - Import a certificate
8 - Import a certificate and a private key
9 - Show the default key
10 - Store database password
11 - Show database record length
0 - Exit program
Enter option number (press ENTER to return to previous menu): 7
Enter import file name (press ENTER to return to menu): cdcaroot.txt
Enter label (press ENTER to return to menu): cdcaroot
Certificate imported.
Press ENTER to continue.
****
ESC=e 1=Help 2=SubCmd 3=HlpRetrn 4=Top 5=Bottom 6=T50 INPUT
7=BackScr 8=Scroll 9=NextSess 10=Refresh 11=FwdRetr 12=Retrieve
```

You will then see a message that confirms that the certificate was imported successfully. Press enter to continue.

## Import intermediate certificate

- Enter 7 – Import a certificate
- Enter the name of the intermediate certificate
- Enter the certificate label
- Enter to continue

```
Key Management Menu
Database: /u/awarn1/cdkdb
Expiration: None

1 - Manage keys and certificates
2 - Manage certificates
3 - Manage certificate requests
4 - Create new certificate request
5 - Receive requested certificate or a renewal certificate
6 - Create a self-signed certificate
7 - Import a certificate
8 - Import a certificate and a private key
9 - Show the default key
10 - Store database password
11 - Show database record length

0 - Exit program

Enter option number (press ENTER to return to previous menu): 7
Enter import file name (press ENTER to return to menu): cdcaint.txt
Enter label (press ENTER to return to menu): cdcaint

Certificate imported.

Press ENTER to continue.
====

ESC=␣ 1=Help 2=SubCmd 3=HlpRetrn 4=Top 5=Bottom 6=TS0 INPUT
7=BackScr 8=Scroll 9=NextSess 10=Refresh 11=PwdRetr 12=Retrieve
```

Once you import your CA root certificate, you will then import any other issuer certificates now. In the example, the intermediate certificate is imported.

## Receive new requested certificate

- Key in 5 - Receive requested certificate or a renewal certificate
- Enter

```

Enter import file name (press ENTER to return to menu): cdcaint.txt
Enter label (press ENTER to return to menu): cdcaint

Certificate imported.

Press ENTER to continue.

Key Management Menu

Database: /u/awarn1/cdkdb
Expiration: None

1 - Manage keys and certificates
2 - Manage certificates
3 - Manage certificate requests
4 - Create new certificate request
5 - Receive requested certificate or a renewal certificate
6 - Create a self-signed certificate
7 - Import a certificate
8 - Import a certificate and a private key
9 - Show the default key
10 - Store database password
11 - Show database record length

0 - Exit program

Enter option number (press ENTER to return to previous menu):
==== 5

ESC=q 1=Help 2=SubCmd 3=HlpRetrn 4=Top 5=Bottom 6=TSO INPUT
       7=BackScr 8=Scroll 9=NextSess 10=Refresh 11=PwdRetr 12=Retrieve

```

Once you imported the issuer certificates, you will use option 5 to receive the newly requested certificate. Key in 5 and press enter to continue.

## Certificate file name

- Key in the signed certificate file name
- Enter

```
Certificate imported.
Press ENTER to continue.

Key Management Menu
Database: /u/awarn1/cdkdb
Expiration: None

1 - Manage keys and certificates
2 - Manage certificates
3 - Manage certificate requests
4 - Create new certificate request
5 - Receive requested certificate or a renewal certificate
6 - Create a self-signed certificate
7 - Import a certificate
8 - Import a certificate and a private key
9 - Show the default key
10 - Store database password
11 - Show database record length
0 - Exit program

Enter option number (press ENTER to return to previous menu): 5
Enter certificate file name (press ENTER to return to menu):
====> signedcert.txt

ESC=e 1=Help 2=SubCmd 3=HlpRetrn 4=Top 5=Bottom 6=TSO INPUT
7=BackScr 8=Scroll 9=NextSess 10=Refresh 11=FwdRetr 12=Retrieve
```

Under Enter certificate name, you will key in the file name of the signed certificate. Press enter to continue.



## Signed certificate received

- Certificate received message is displayed
- Enter

```
Key Management Menu
Database: /u/awarn1/cdkdb
Expiration: None

1 - Manage keys and certificates
2 - Manage certificates
3 - Manage certificate requests
4 - Create new certificate request
5 - Receive requested certificate or a renewal certificate
6 - Create a self-signed certificate
7 - Import a certificate
8 - Import a certificate and a private key
9 - Show the default key
10 - Store database password
11 - Show database record length

0 - Exit program

Enter option number (press ENTER to return to previous menu): 5
Enter certificate file name (press ENTER to return to menu): signedcert.txt
Certificate received.
Press ENTER to continue.
****
ESC=q 1=Help 2=SubCmd 3=HlpRetrn 4=Top 5=Bottom 6=TS0 INPUT
7=BackScr 8=Scroll 9=NextSess 10=Refresh 11=FwdRetr 12=Retrieve
```

You will see a certificate received message to confirm that your signed certificate was received successfully. Press enter to continue.

## Exit GSKKYMAN

- Key in 0 and enter
- Key in exit and enter
- Enter

```

Enter certificate file name (press ENTER to return to menu): signedcert.txt
Certificate received.
Press ENTER to continue.

Key Management Menu
Database: /u/awarn1/cdkdb
Expiration: None

1 - Manage keys and certificates
2 - Manage certificates
3 - Manage certificate requests
4 - Create new certificate request
5 - Receive requested certificate or a renewal certificate
6 - Create a self-signed certificate
7 - Import a certificate
8 - Import a certificate and a private key
9 - Show the default key
10 - Store database password
11 - Show database record length

0 - Exit program

Enter option number (press ENTER to return to previous menu): 0
5 exit
>>>> FSUM2331 The session has ended. Press <Enter> to end OMVS.

ESC= 1=Help 2=SubCmd 3=HlpRetrn 4=Top 5=Bottom 6=TSD INPUT
      7=BackScr 8=Scroll 9=NextSess 10=Refresh 11= 12=

```

Once your certificate is received, you will now exit GSKKYMAN.

## Summary

- Import the issuer certificates
- Receive the new signed certificate
- For more information, see modules
  - “GSKKYMAN Part 1 - Creating a key database”
  - “GSKKYMAN Part 2 - Creating a self-signed certificate”
  - “GSKKYMAN Part 3 - Creating a new certificate request”

In this presentation, you learned how to receive a CA signed certificate. You can learn how to create a “certificate signing request” in module “GSKKYMAN Part 3 - create a new certificate request”. Information about how to create a self-signed certificate can be found in module “GSKKYMAN Part 2 - Creating a Self-Signed Certificate”. How to create a key database information is in module “GSKKYMAN Part 1 - Creating a Key Database”.

## Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, and z/OS are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "[Copyright and trademark information](http://www.ibm.com/legal/copytrade.shtml)" at <http://www.ibm.com/legal/copytrade.shtml>

UNIX is a registered trademark of The Open Group in the United States and other countries.

Connect.Direct is a trademark or registered trademark of IBM International Group B.V., an IBM Company.

Other company, product, or service names may be trademarks or service marks of others.

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.

© Copyright International Business Machines Corporation 2016. All rights reserved.