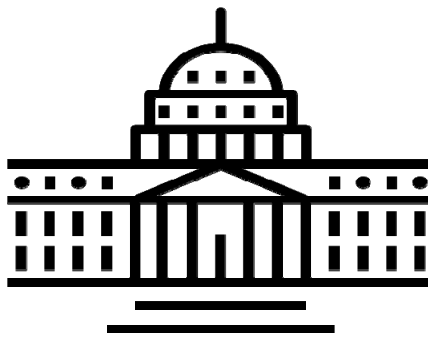


IBM z/OS Connect

Quick Start Guide



Lab Version Date: August 8, 2023

Table of Contents

General Exercise Information and Guidelines	3
z/OS Updates.....	4
Workstation Updates	5
<i>Using mutual authentication with Postman</i>	6

Important: There is a folder on the Windows desktop named *CopyPaste Files*. This folder contains file with the commands and other text used in this workshop. Locate the file identified in the *General Exercise Information and Guidelines* section of this exercise and copy it to the desktop. Open the file and use the copy-and-paste function (**Ctrl-C** and **Ctrl-V**) to enter commands or text. It will save time and help avoid typo errors. As a reminder text that appears in this file will be highlighted in yellow.

General Exercise Information and Guidelines

- ✓ This exercise compresses the steps performed in exercises *Customization – Basic Configuration (1 of 2)* and *Customization Basic Security (2 of 2)*. The explanations for the steps performed in this exercise can be found in the original exercises.
- ✓ This exercise provides a shortcut so someone could go directly to the more complex subsystem exercises.
- ✓ For information regarding the use of the Personal Communication 3270 emulator, see the *Personal Communications Tips* PDF in the exercise folder.

z/OS Updates

Use these instructions to bypass the steps performed by the *IBM z/OS Connect Customization – Basic Configuration (1 of 2)* and *IBM z/OS Connect Customization – Basic Security (2 of 2)*.

- ___ 1. Edit data set **USER1.ZCEE30.CNTL**.
- ___ 2. Submit member **ZCEEGRPS** and wait for the job to complete.
- ___ 3. Submit member **ZCEERSTC** and wait for the job to complete
- ___ 4. Submit member **ZCEERACF** and wait for the job to complete.
- ___ 5. Submit member **ZCEERSVR** and wait for the job to complete
- ___ 6. Submit member **ZCEETLSS** and wait for the job to complete
- ___ 7. Submit member **ZCEETLSX** and wait for the job to complete
- ___ 8. Submit member **MYSERVER** and wait for the job to complete.
- ___ 9. Submit member **ZCEELN** and wait for the job to complete.
- ___ 10. Copy the contents of **USER1.PROCLIB** to **SYS1.PROCLIB**.
- ___ 11. Edit **server.xml** in `/var/zcee/myServer` and add the following includes after the `<server >` XML tag.

```
<include location="${shared.config.dir}/safSecurity.xml"/>
<include location="${shared.config.dir}/ipic.xml"/>
<include location="${shared.config.dir}/keyringMutual.xml"/>
<include location="${shared.config.dir}/groupAccess.xml"/>
```
- ___ 12. Start the angel process with MVS command **S BAQZANGL**
- ___ 13. Start the z/OS Connect server with MVS command **S BAQSTRT**

Workstation Updates

The previous instructions created and export user digital certificates. The exported certificates need to be moved to the workstation for use in Postman and cURL commands. See section *Enabling mutual authentication using TLS* in the *IBM z/OS Customization - Basic Security (2 of 2)* exercise for details on how to make these certificates available to cURL, Postman, and a Firefox browser.

___ 1. On the Windows desktop, open a command prompt.

___ 2. Enter the command: ***cd c:\z\admin***

___ 3. Enter the command below to download the public Liberty CA certificate:

curl --user user1:user1 ftp://wg31.washington.ibm.com/CERTAUTH.PEM --use-ascii -o certauth.pem

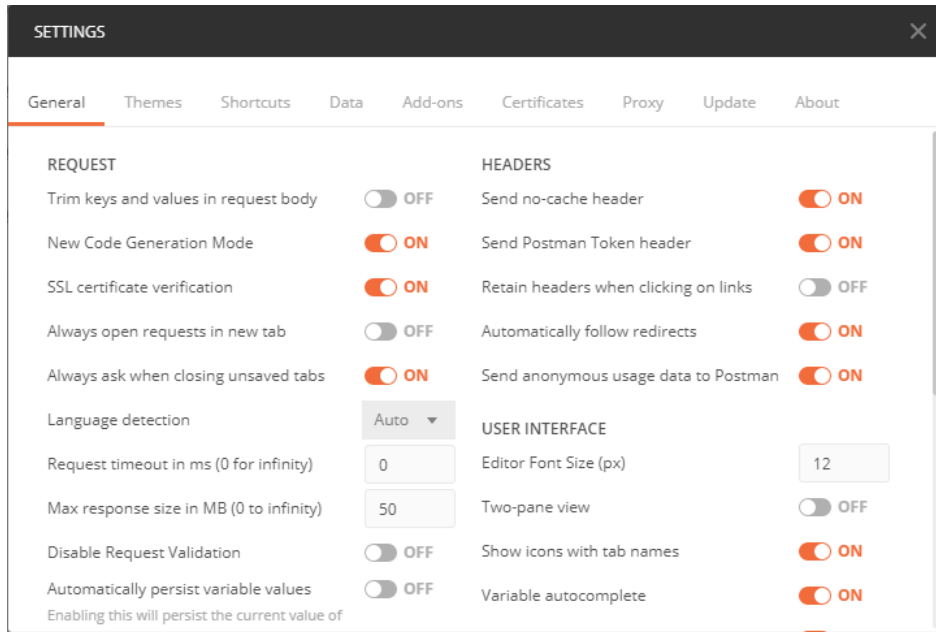
___ 4. Enter the command below to download FRED's personal certificate:

___ 5. Enter the command below to download USER1's personal certificate:

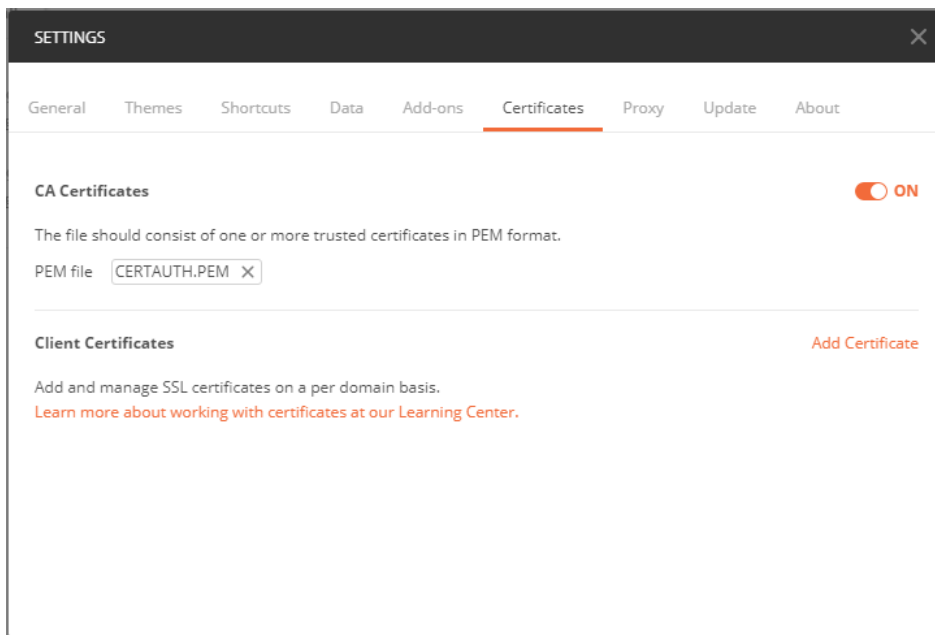
curl --user user1:user1 ftp://wg31.washington.ibm.com/user1.p12 -o user1.p12

Using mutual authentication with Postman

1. To test with Postman, do the following. Go into Postman and select the settings icon (the wrench on the tool bar) to open the *Settings* window.



2. In the *General* tab, turn SSL certificate verification on (see above).
3. Go to the *Certificates* tab and turn on the **On** radio button. Use the *Select File* button to add the CA certificate to be *CERTAUTH.PEM* file downloaded earlier.



4. Click the *Add Certificate* and enter ***wg31.washington.ibm.com*** and port ***9443*** for the *Host* as shown below. Use the Select File button beside PFX file to select file *USER1.P12* downloaded earlier. Note the password of “secret” is entered as the value in the *Passphrase* field.

The screenshot shows the 'SETTINGS' window with the 'Certificates' tab selected. The 'Add Certificate' section is active. The 'Host' field is set to 'https:// wg31.washington.ibm.com' and the port is '9443'. The 'CRT file' and 'KEY file' fields have 'Select File' buttons. The 'PFX file' field is set to 'USER1.P12' with a close button. The 'Passphrase' field is masked with dots. There are 'Cancel' and 'Add' buttons at the bottom right. A link to the Learning Center is at the bottom left.

SETTINGS

General Themes Shortcuts Data Add-ons Certificates Proxy Update About

Client Certificates > Add Certificate

Host https:// wg31.washington.ibm.com : 9443

CRT file Select File

KEY file Select File

PFX file USER1.P12 X

Passphrase

Cancel Add

[Learn more about working with certificates at our Learning Center.](#)