IBM z/OS Connect

Quick Start Guide

IBM Z
Wildfire Team –
Washington System Center

Lab Version Date: June 27, 2023

Table of Contents

Important: At URL https://ibm.box.com/v/WSC-AdminSecurity there is a file named *Admin Security CopyPaste.txt*. This file contains commands and other text used in this workshop. Locate that file and open it. Download this 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.
Note: Connectivity from the remote Desktop to this site is not always available. In this case, access this URL and download the file to your local Desktop and then copy the file from the local Desktop to the remote Desktop.

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:

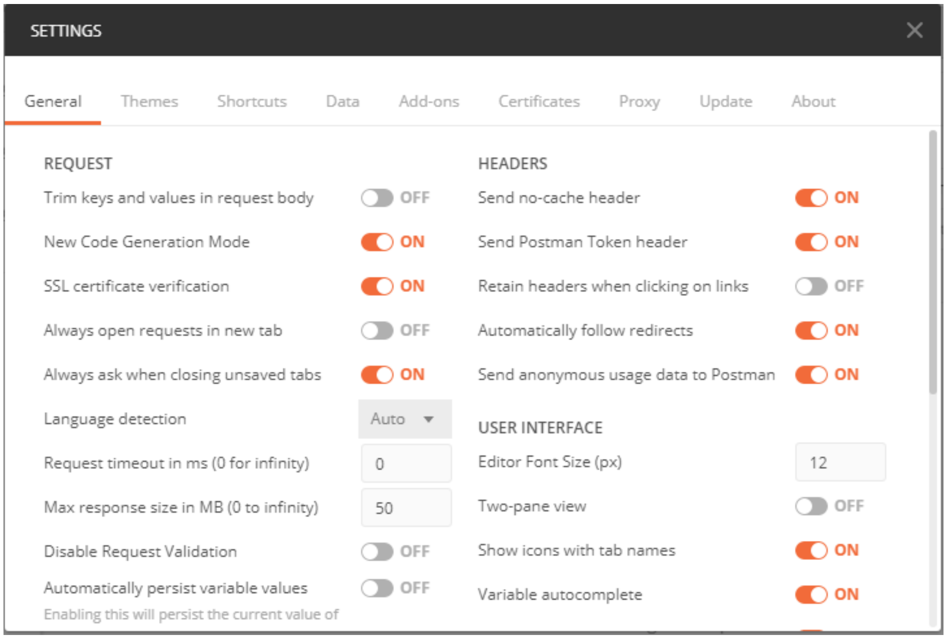
```
curl --user user1:user1 ftp:/wg31.washington.ibm.com/fred.p12 -o fred.p12
```

___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.



REQUEST

Trim keys and values in request body OFF

New Code Generation Mode ON

SSL certificate verification ON

Always open requests in new tab OFF

Always ask when closing unsaved tabs ON

Language detection Auto

Request timeout in ms (0 for infinity) 0

Max response size in MB (0 to infinity) 50

Disable Request Validation OFF

Automatically persist variable values OFF

Enabling this will persist the current value of

HEADERS

Send no-cache header ON

Send Postman Token header ON

Retain headers when clicking on links OFF

Automatically follow redirects ON

Send anonymous usage data to Postman ON

USER INTERFACE

Editor Font Size (px) 12

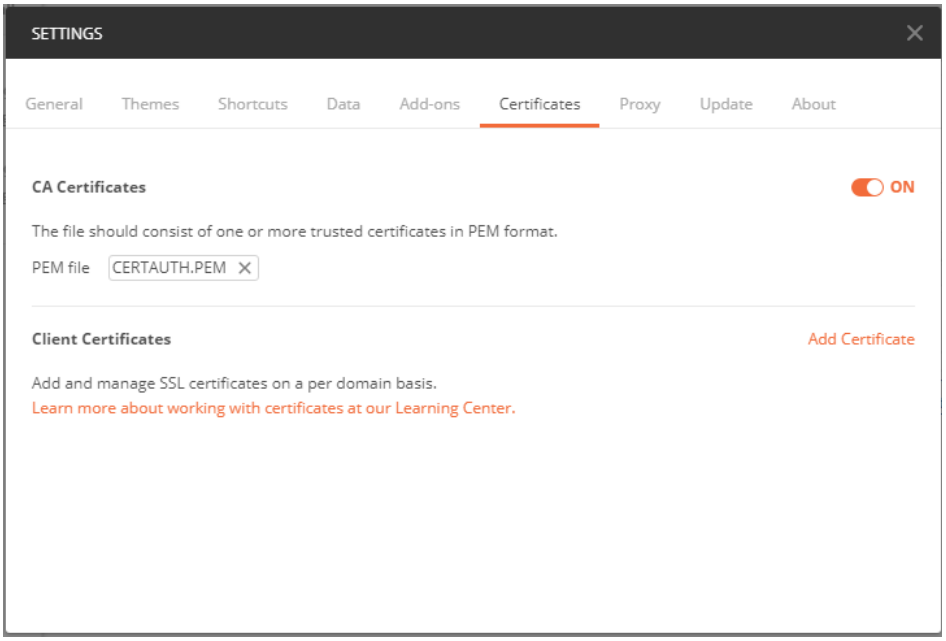
Two-pane view OFF

Show icons with tab names ON

Variable autocomplete ON

___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.



CA Certificates ON

The file should consist of one or more trusted certificates in PEM format.

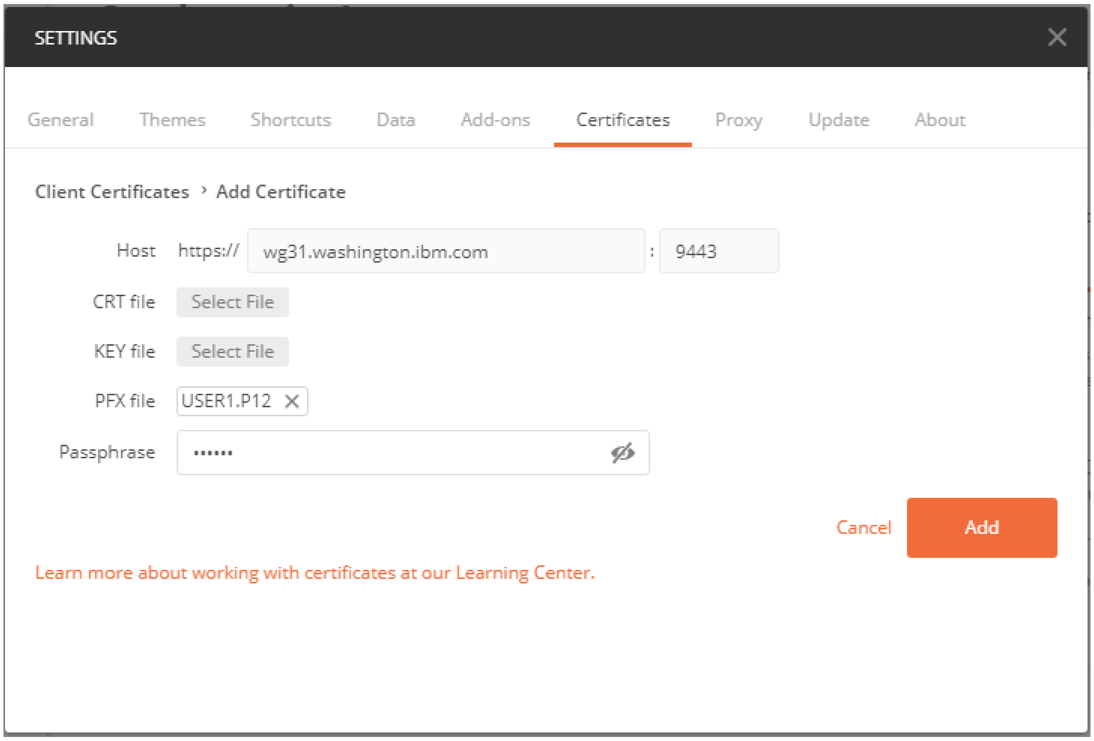
PEM file CERTAUTH.PEM

Client Certificates

Add and manage SSL certificates on a per domain basis.

Learn more about working with certificates at our Learning Center.

___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.



Client Certificates › Add Certificate

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

CRT file Select File

KEY file Select File

PFX file USER1.P12 ✕

Passphrase ••••••

Learn more about working with certificates at our Learning Center.