

IBM z/OS Connect EE V3.0

# zOSSEC1 Quick Start



**IBM Z**  
**Wildfire Team –**  
**Washington System Center**

*Lab Version Date: February 4, 2021*

---

## Table of Contents

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

**Important:** On the desktop there is a file named *Basic Configuration CopyPaste.txt*. This file contains commands and other text that may be useful in this exercise. Locate that file and open it. 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 zCEE Customization – Basic Configuration and zCEE Customization – Basic Security

- \_\_\_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="${server.config.dir}/includes/safSecurity.xml"/>
<include location="${server.config.dir}/includes/ipic.xml"/>
<include location="${server.config.dir}/includes/keyring.xml"/>
<include location="${server.config.dir}/includes/groupAccess.xml"/>
```
- \_\_\_12. Start the angel process with MVS command **S BAQZANGL**
- \_\_\_13. Start the z/OS Connect server with MVS command **S BAQSTRT**

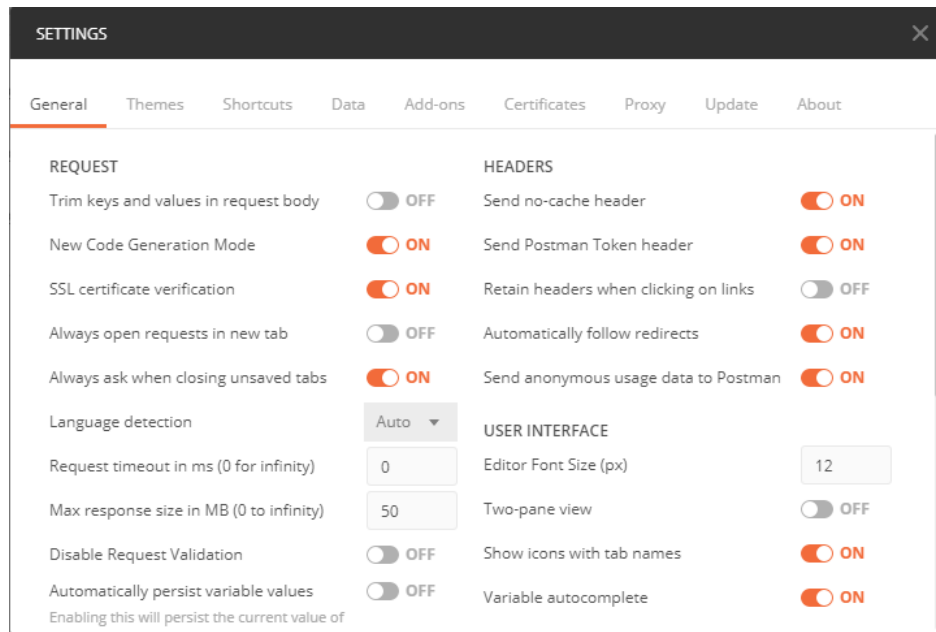
## Workstation Updates

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 *zCEE Customization Basic Security exercise* for details on how to make these certificates available to cURL, Postman and a Firefox browser.

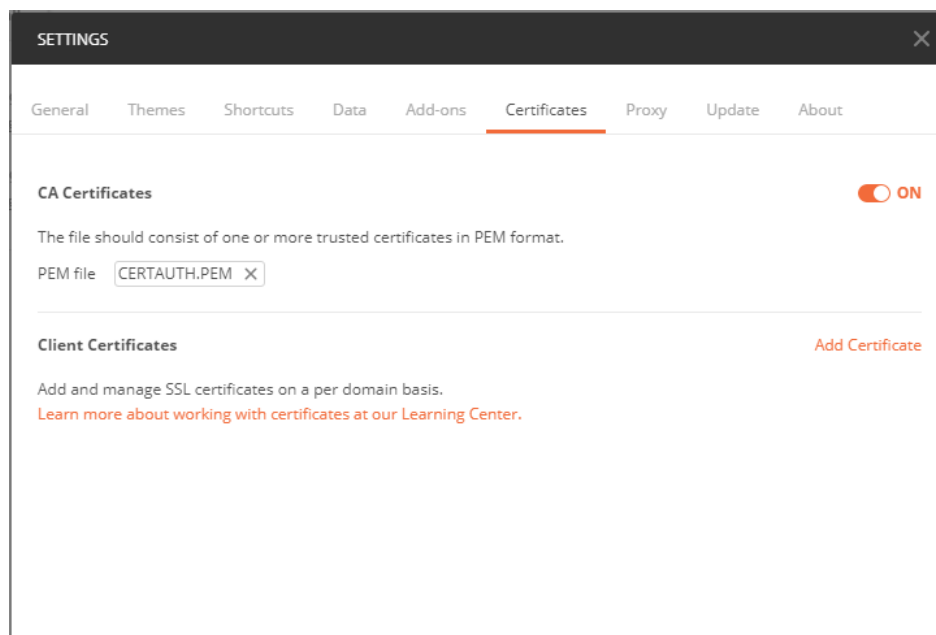
- \_\_\_ 1. On the Windows desktop, open a command prompt.
- \_\_\_ 2. Enter the command: ***cd c:\z\admin***
- \_\_\_ 3. Enter the command: ***ftp wg31.washington.ibm.com***
- \_\_\_ 4. Logon with *USER1* and the password for that ID
- \_\_\_ 5. Enter the command: ***prompt off***
- \_\_\_ 6. Enter the command: ***mget \*.pem***
- \_\_\_ 7. Enter the command: ***bin*** (this will set FTP mode to binary, or 'image')
- \_\_\_ 8. Enter the command: ***mget \*.p12***
- \_\_\_ 9. Enter the command: ***quit***

## Using mutual authentication with Postman

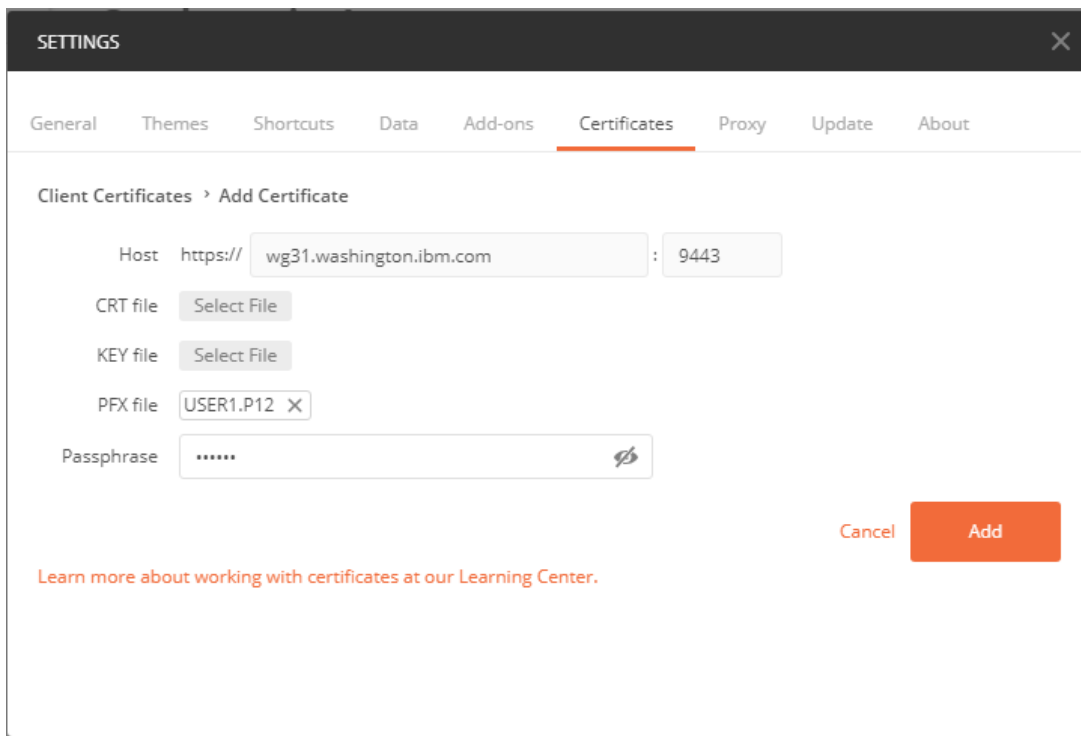
1. To test with Postman, do the following. Go into Postman and select the settings icon (the wrench on the tool bar) to open the *Settings* window.



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 'Client Certificates > Add Certificate' section contains the following fields:

- Host:** A text field containing 'https:// wg31.washington.ibm.com' followed by a colon and a port field containing '9443'.
- CRT file:** A button labeled 'Select File'.
- KEY file:** A button labeled 'Select File'.
- PFX file:** A text field containing 'USER1.P12' with a close button (X) to its right.
- Passphrase:** A text field containing six dots (password masked) and a copy icon to its right.

At the bottom right, there are two buttons: 'Cancel' and 'Add'.

Below the form, there is a link: [Learn more about working with certificates at our Learning Center.](#)