

# z/OS 3.1 IBM Education Assistant

Solution Name: Run Workflow Signed Steps as Different User

Solution Element(s): z/OSMF Workflows

July 2023



# Agenda

---

- Trademarks
- Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Upgrade & Coexistence Considerations
- Installation & Configuration
- Summary
- Appendix

# Trademarks

---

- See url <http://www.ibm.com/legal/copytrade.shtml> for a list of trademarks.
- Additional Trademarks:
  - None.

# Objectives

---

- This initiative allows clients to get their own workflow step signed so that their steps could be automatically executed under their credential during workflow automation and also ensure that their steps can not be changed since they sign the step.

# Overview

---

- Who (Audience)
  - z/OSMF Workflows users
- What (Solution)
  - Workflow editor and workflow engine provide signing workflow function to allow the users to sign and execute runAsUser step automatically in general workflow instance.
- Wow (Benefit / Value, Need Addressed)
  - Workflow users can get their runAsUser workflow step signed so that the steps could be automatically executed under their credential during workflow automation and ensure that the steps cannot be changed since being signed.

# Terminology

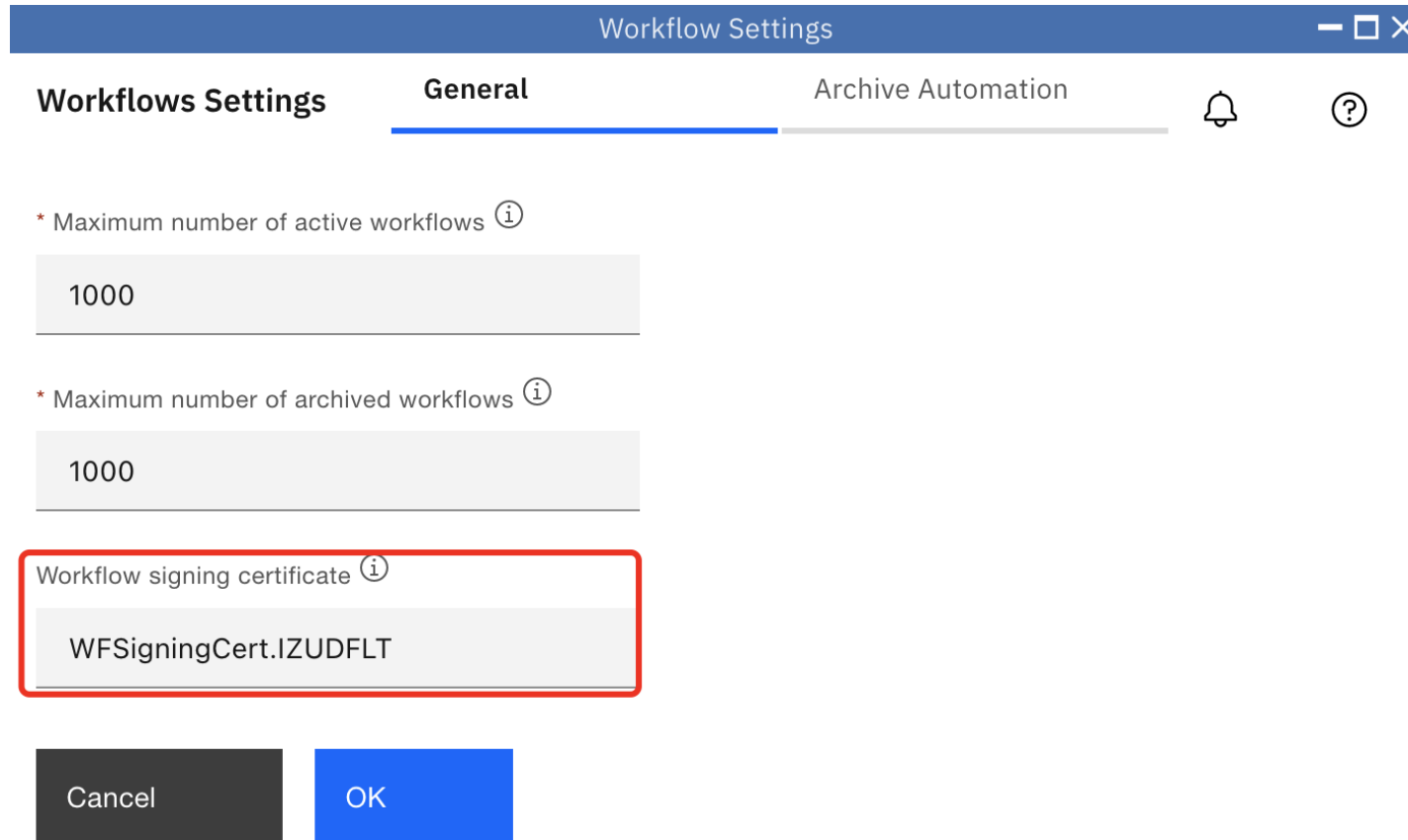
---

- The step signer
  - The signer of workflow step should have the access to read the SAF resource `<SAF-prefix> .ZOSMF.WORKFLOW.SIGNER` in the ZMFAPLA class.
  - The step signer can sign any runAsUser steps in Workflow Editor task.
- The runAsUser ID
  - The runAsUser ID should be the z/OSMF user ID with permission to read the SAF resource `<SAF-prefix> .ZOSMF.WORKFLOW.RUNASUSER` in the ZMFAPLA class.
  - The signed workflow step with runAsUser ID specified can be performed under the runAsUser ID in automation mode.
- Workflow signing certificate

A new certificate which is used for signing and validating.
- Fully signed step
  - Step has runAsUser ID and one or more signers, all signers have signed this step correctly.
- Fully signed workflow definition file
  - All runAsUser steps are fully signed steps.

# Usage & Invocation

- 1. Set "Workflow signing certificate"



Workflow Settings

Workflows Settings General Archive Automation

\* Maximum number of active workflows ⓘ

1000

\* Maximum number of archived workflows ⓘ

1000

Workflow signing certificate ⓘ

WFSigningCert.IZUDFLT

Cancel OK

Workflow signing certificate:

Label of the certificate that is used to sign the workflow steps.

Before using workflow signing function, you must create a workflow signing certificate and connect it to z/OSMF server key ring. Then put the signing workflow keyLabel in Workflow Settings page.

Refer to the new chapter “Configuring the z/OSMF workflow signing certificate ” in “IBM z/OS Management Facility Configuration Guide” for details.

# Usage & Invocation

- 2. Specify runAsUser ID and step signers in Workflow Editor

## Workflow Editor

### Step Security

On this tab, you can modify the authorizations for the selected step. You can indicate whether a step must be performed under a specific user ID. Or, whether approvals or signatures from other users are required before the step can be performed.

Run this step as user ID:

☐ User ID contains variable substitution (Only applies to Cloud Provisioning & Management or z/OS Management Services Catalog workflow definitions.)

#### Signers Table

Not applicable to Cloud Provisioning & Management or z/OS Management Services Catalog workflow definitions.

Actions

Search

Signer/Group ID

Signature Status

Actions supported:

- Add Signer
- Modify Signer
- Remove Signer
- Sign Step
- Unsign Step

## Implementation details

- Only automated step with runAsUser ID can be signed
- More than one signer(user id or group id) can be specified
- If the step is not fully signed, the definition file cannot create a new workflow
- Signer and runAsUser ID cannot be substituted in the signed step
- The signature with version is generated based on the step content, workflow content and signer, and will be saved in the definition file.

```
<step name="RunAsUserStepWithSigner" optional="false">
  <title>RunAsUser Step With Signer</title>
  <description>This is an example of an automated RunAsUser step.</description>
  <runAsUser substitution="false">ZOSMFT1</runAsUser>
  <stepSignature>
    <sign>
      <signer>IBMUSER</signer>
      <signature version="1.0">o0CHBTvdDafv+n0LCJdkIhs6driR0up2Beryig4mzV+H
    </sign>
    <sign>
      <signer>ZOSMFAD</signer>
      <signature version="1.0">gl8g204rYtvsYiM0Kp3JSeaTAusdwtMWnexpGAGMsVNxv
    </sign>
  </stepSignature>
</step>
```



# Usage & Invocation

---


- 3. Signer related actions

Add signer, see the detail description in next Page.



A screenshot of a dialog box titled "Add Signer". It features a text input field with the placeholder text "Signer user/group ID (if more than one, separate with spaces):". Below the input field are three buttons: "OK", "Cancel", and "Help".

Modify signer, see the detail description in next Page.



A screenshot of a dialog box titled "Modify Signer". It features a text input field with the placeholder text "Signer user/group ID (if more than one, separate with spaces):". The input field contains the text "ibmuser". Below the input field are three buttons: "OK", "Cancel", and "Help".

# Usage & Invocation

---

- 3. Signer related actions (cont.)

Action	Description
<b>Modify</b>	To modify an signer user ID, select one user ID in the table, and select Modify from the table actions menu. When you do so, a window is displayed for you to change the signer user ID. To complete the change, click OK. Otherwise, click Cancel to discard your changes.
<b>Remove</b>	To remove a user ID from the table, select one or more user IDs in the table and select Remove from the table actions menu. You are prompted to confirm your selection. To complete the change, click OK. Otherwise, click Cancel to discard your changes.
<b><u>Unsign</u></b>	To remove signature from the table, select one or more signers in the table and select Unsign from the table actions menu.
<b>Add</b>	To add signers, select Add in the actions menu of the table. When you do so, a window is displayed for you to enter the user IDs of one or more signers. To enter multiple user IDs, separate each entry with a blank. To complete the change, click OK. Otherwise, click Cancel to discard your changes.  Note: There are a maximum of twelve signer records in Signer Table.
<b>Sign</b>	To sign the step, it means that you agrees to perform the step under the runAsUser identity. Select Sign from the table actions menu, your signer records can be signed at the same time.  If you click sign, it will be signed again, even if you have signed before.

# Usage & Invocation

- 4. Add new column called “Signature Status” which indicates the signature status of steps

## Workflow Editor

Workflow Definition: /tmp/workflow\_sample\_parallel\_runAsUser\_stepsWithSignerAndSignature.xml

Workflow Editor				
Workflow Definition: /tmp/workflow_sample_parallel_runAsUser_stepsWithSignerAndSignature.xml				
A workflow is composed of one or more units of work called steps. A workflow definition file must contain at least one step; each step can contain substeps. On this tab, you can launch actions to view or modify the steps in the selected workflow definition.				
Actions   Create Step				
Search				
Step No.	Name	Title	Signature Status	
1	rootStep	Root Step		
2	attrConditionStep	Step Attribute Conditional Step	N/A	
3	AutomatedStep	Automated Step	Incomplete	
4	RunAsUserStepWithSigner	RunAsUser Step With Signer	Completed	

The signature status of a runAsUser step.

There are three signature status for a runAsUser step:

**Complete:** The step has signers and all signers have signed and all the signatures are valid.


**Incomplete:** The step has signers and part of signers have signed. Some signatures are invalid. Or all the signers haven't signed.

**N/A:** Other types steps.

# Usage & Invocation

- 5. Create a workflow instance with the workflow definition file contains signer

## Create Workflow

 The definition file is not valid to create the workflow. The definition contains a step signer, but not all runAsUser steps are fully signed. The runAsUser steps that are not fully signed are: "AutomatedStep" . IZUWF0439E

\* Location (system) of definition and variable input files:

SVPLEX6.P01 (P01\_001) - Local

\* Workflow definition file: ?

/tmp/workflow\_sample\_parallel\_runAsUser\_stepsWithSignerAndSignature.xml

Workflow variable input file: ?

Select or type

< Back

Next >

Finish

Cancel

Help

When create a workflow instance with the workflow definition file contains signer, you should confirm all the runAsUser steps are automated step, they must have valid runAsUser ID and all the runAsUser steps have been fully signed.

Otherwise, it will throw the exceptions *IZUWF0438E*, *IZUWF0439E* or *IZUWF0440E* when create workflow instance .

# Usage & Invocation

- 5. Create a workflow instance with the workflow definition file contains signer (cont.)

[Workflows](#) ▶ Test runAsUser steps workflow

## Test runAsUser steps workflow

▶ Workflow Details						
Workflow Steps						
Actions ▾						
↔ No filter applied						
<input type="checkbox"/>	State Filter	No. Filter	Title Filter	CalledWorkflow Filter	Automated Filter	Use RunAsUser ID Filter
<input type="checkbox"/>	In Progress	1	Root Step			
<input type="checkbox"/>	Not Ready	2	Step Attribute Conditional Step		Yes	
<input type="checkbox"/>	Ready	3	Automated Step		Yes	debug63
<input type="checkbox"/>	Ready	4	RunAsUser Step With Signer		Yes	debug62

New column called "Use RunAsUserID" is provided.

After create a workflow instance with fully signed workflow definition file, these signed steps will be run under this specific user identity (shown in the column "Use RunAsUserID") during automation.

# Interactions & Dependencies

---

- Software Dependencies
  - None
- Hardware Dependencies
  - None
- Exploiters
  - z/OSMF Workflow users

# Upgrade & Coexistence Considerations

---

- If the z/OSMF workflow signing certificate is changed, please refer to the chapter “Configuring the z/OSMF workflow signing certificate ” in IBM z/OS Management Facility Configuration Guide to take actions accordingly.

# Installation & Configuration

---

- The new function needs additional configuration:

## 1. Add two new profiles

Resource class	Resource name	Who needs access?	Type of access required	Why
ZMFAPLA	<SAF-prefix>.ZOSMF.WORKFLOW.RUNASUSER	IZUUSER	READ	Allow the user to be defined as the runAsUser ID in the workflow instance that does not originate from z/OS Management Services Catalog or Cloud Provisioning and Management.
ZMFAPLA	<SAF-prefix>.ZOSMF.WORKFLOW.SIGNER	IZUADMIN	READ	Allow the user to be granted the runAsUser step signer role.

## 2. Configuring the z/OSMF workflow signing certificate

Refer to the new chapter "Configuring the z/OSMF workflow signing certificate" in "IBM z/OS Management Facility Configuration Guide" for details.



# Summary

---

- The following z/OS V3R1 z/OSMF Workflow Initiative has been explained:
  - Run Workflow Signed Steps as Different User

# Appendix

---

- Book updates
  - IBM z/OS Management Facility Programming Guide
  - IBM z/OS Management Facility Configuration Guide
  - IBM z/OS Management Facility Online Help