

User Guide

FORTANIX CONFIDENTIAL COMPUTING MANAGER – CREATE, UPDATE, AND DELETE WORKFLOW GRAPHS

VERSION 4.0

TABLE OF CONTENTS

1.0	INTRODUCTION	2
2.0	DESCRIPTION OF SERVICES	2
2.1	Fortanix Confidential Computing Manager.....	2
2.2	Intel® SGX.....	2
2.3	Intel Attestation and Why it is Required	2
2.4	Navigation Buttons	3
3.0	WORKFLOW GRAPHS IN CONFIDENTIAL COMPUTING MANAGER	4
3.1	Create a Workflow	5
3.2	Edit Workflow Graphs.....	9
3.3	Clone Workflow Graphs	12
3.4	Delete Workflow Graphs.....	13
4.0	DOCUMENT INFORMATION	13
4.1	Document Location	13

1.0 INTRODUCTION

Welcome to the Fortanix Confidential Computing Manager (CCM) User Guide. This document describes how to create, update, and delete workflow graphs.

2.0 DESCRIPTION OF SERVICES

2.1 FORTANIX CONFIDENTIAL COMPUTING MANAGER

Fortanix Confidential Computing Manager provides “data-in-use” protection for your container workloads. It leverages the Intel® Software Guard Extensions (SGX) technology to run code and data in CPU-hardened “enclaves” or a “Trusted Execution Environment” (TEE). The enclave is a trusted area of memory where critical aspects of the application functionality are protected, helping keep code and data confidential and unmodified.

2.2 INTEL® SGX

Intel® SGX is an extension to the x86 architecture that allows running applications in a completely isolated secure enclave. The application is not only isolated from other applications running on the same system, but also from the Operating System and possible Hypervisor. This prevents administrators from tampering with the application once it is started. The memory of secure enclaves is also encrypted to thwart physical attacks.

The technology also supports storing persistent data securely such that it can only be read by the secure enclave. In addition, you can prove remotely that your application is running in a secure enclave using remote attestation.




2.3 INTEL ATTESTATION AND WHY IT IS REQUIRED




Since enclaves are instantiated on platforms by untrusted code, before enclaves are provisioned with application confidential information, it is essential to be able to confirm that the desired enclave was correctly instantiated on a platform protected by Intel SGX. This is done by a remote attestation process. Remote attestation consists of using Intel SGX instructions and platform software to generate a “quote” that combines the enclave digest with a digest of relevant enclave data and a platform-unique asymmetric key into a data structure that is sent to a remote server over an authenticated channel. If the remote server concludes that the enclave was instantiated as

intended and is running on a genuine Intel SGX-capable processor, it will provision the enclave as required.

2.4 NAVIGATION BUTTONS

The Navigation buttons for Fortanix Confidential Computing Manager are located on the left panel of the GUI and identify the screen functionality. The following table illustrates button functions:

MENU LIST	FUNCTIONALITY
 <p>INFRASTRUCTURE</p>	<p>Click this menu item to see:</p> <ul style="list-style-type: none"> All the Compute Nodes that are part of your cluster. You can view SGX software version, secure application’s information, and attestation status of each of these Compute Nodes on which your Fortanix Confidential Computing Manager components are running. All the Compute Clusters that you have configured in Fortanix CCM.
 <p>GROUP</p>	<p>Click this menu item to create a group, which is a collection of users and objects. A group helps users to manage identities and create third-party groups. It also helps in organizing and securing applications, datasets, workflows, and other resources that belong to the group.</p>
 <p>APPLICATIONS</p>	<p>Click this menu item to see:</p> <ul style="list-style-type: none"> All the Fortanix Confidential Computing Manager secured applications deployed on the cluster. An application is a way to let the service know which all parameters to configure for a Source Container Image to run in SGX and where to push the converted Image. All the Fortanix Confidential Computing Manager secured Docker images for the applications deployed on the cluster. All the application configurations used to customize the behavior for EDP/EnclaveOS applications.

 TASKS	Click this menu item to see all the requests that need Administrator approval. For example, node enrolment, application domain approval, application image approval, and certificate issuance.
 TOOLS	Click this menu item to access the SGX Converter tool to convert an application.
 USERS	Click this menu item to see the list of users added to Fortanix Confidential Computing Manager. The Users page also allows you to edit the properties of a user and add new users.

3.0 WORKFLOW GRAPHS IN CONFIDENTIAL COMPUTING MANAGER

Workflow graphs are maps that show how generic applications are connected to datasets and other generic applications. These are collaborative objects where multiple users can provide their own objects and approvals.

There are two types of workflows - draft and final.

- Draft workflows are unapproved/in-progress items that do not grant any permissions to applications.
- Final workflows are versioned and quorum approval protected objects. These workflows grant the applications access to datasets if they have requested and received certificates that confirm they are running in the required approved workflow.

An application running inside a final workflow is allowed to access all connected datasets, this means:

- The enclave will have access to the protected data guarded by input datasets.
- It can upload data to the protected locations defined by output datasets.

To move from a draft workflow to a final workflow, you require approvals. For approvals:

- A Fortanix CCM Account Administrator will invite other users to join the account.
- The users join the account and provide data in the form of datasets and applications/application configurations.

For example, in this guide we have the following users:

- Account Owner

- Data Owner
- Application Owner

Data Owners and Application Owners collaborate on a graph. After the graph is completed, the Administrator will submit it for approval. A workflow graph must be approved by all the users of the graph.

3.1 CREATE A WORKFLOW

Perform the following steps to create a workflow:

1. Click the **Workflows** menu item in the CCM UI left navigation bar.
2. On the Workflows page, click **+ WORKFLOW** to create a new workflow.

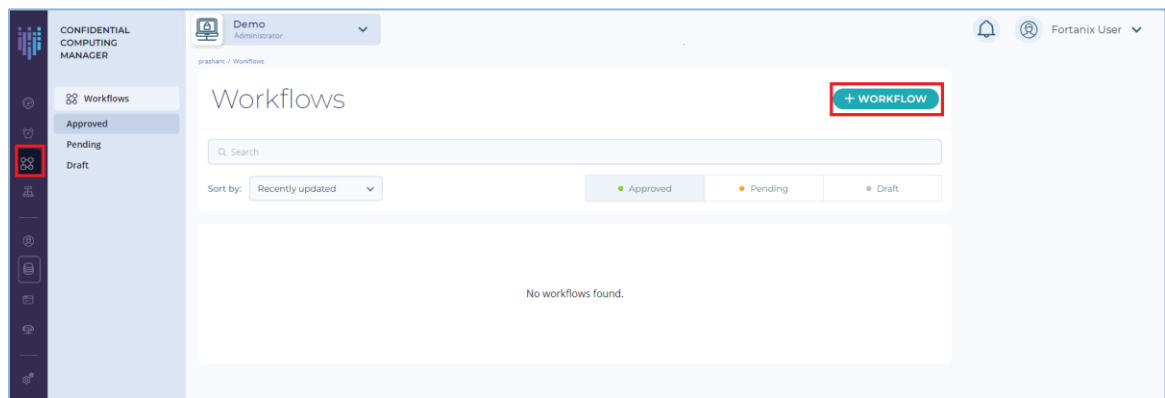


FIGURE 1: ADD WORKFLOW

3. In the **CREATE NEW WORKFLOW** dialog box, enter the workflow **Name**, assign it to a **Group**, and enter a **Description** (optional). Click **CREATE WORKFLOW** to access the workflow graph.

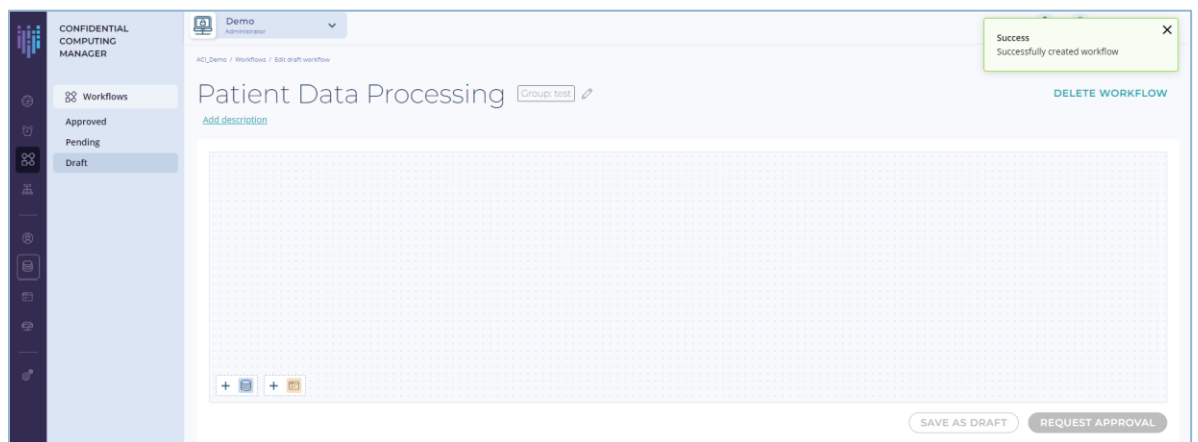


FIGURE 2: CREATE WORKFLOW

4. Add an application to the workflow graph, drag the “App icon” and drop it into the graph area. Click the **+ APPLICATION**. In the **ADD APPLICATION** dialog box, select an existing application name and image. For example, `<my-registry>/simple-python-sgx:latest`. Where, `<my-registry>` is the location of your registry.

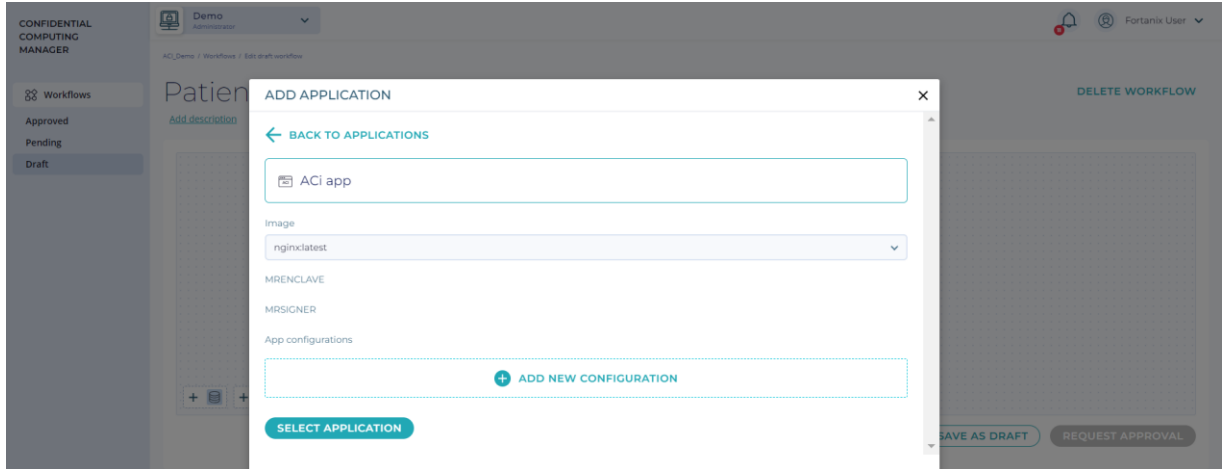


FIGURE 3: ADD APPLICATION CONFIG

5. Click the **+ ADD NEW CONFIGURATION** button add a new application configuration or select an existing one.

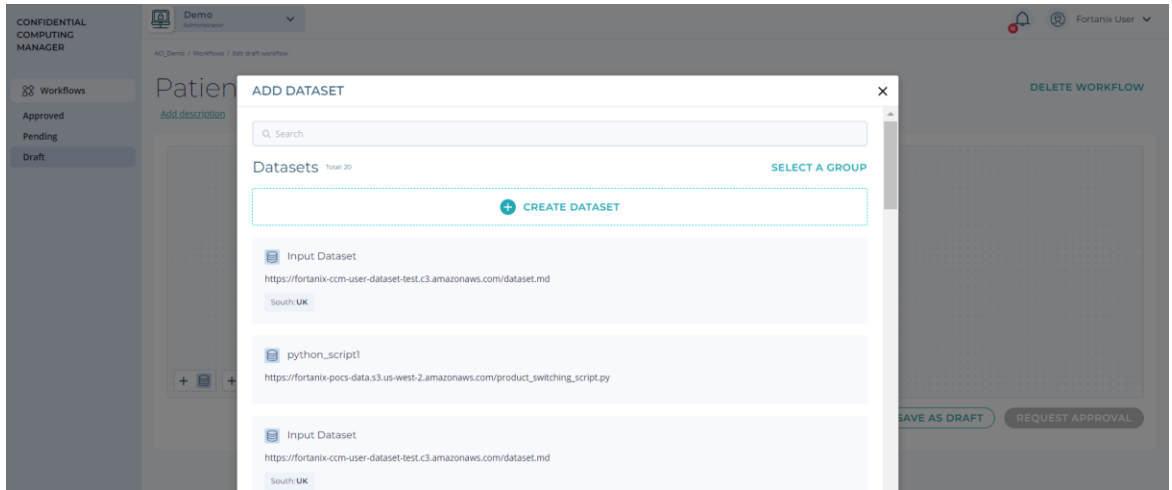


FIGURE 4: ADD APPLICATION CONFIGURATION

6. Add input and output dataset to the workflow graph by dragging the dataset icon and placing it in the graph area. Click **+DATASET**. In the **ADD DATASET** dialog box, select from an existing dataset or create a new dataset. Click **CREATE DATASET** to create the dataset.

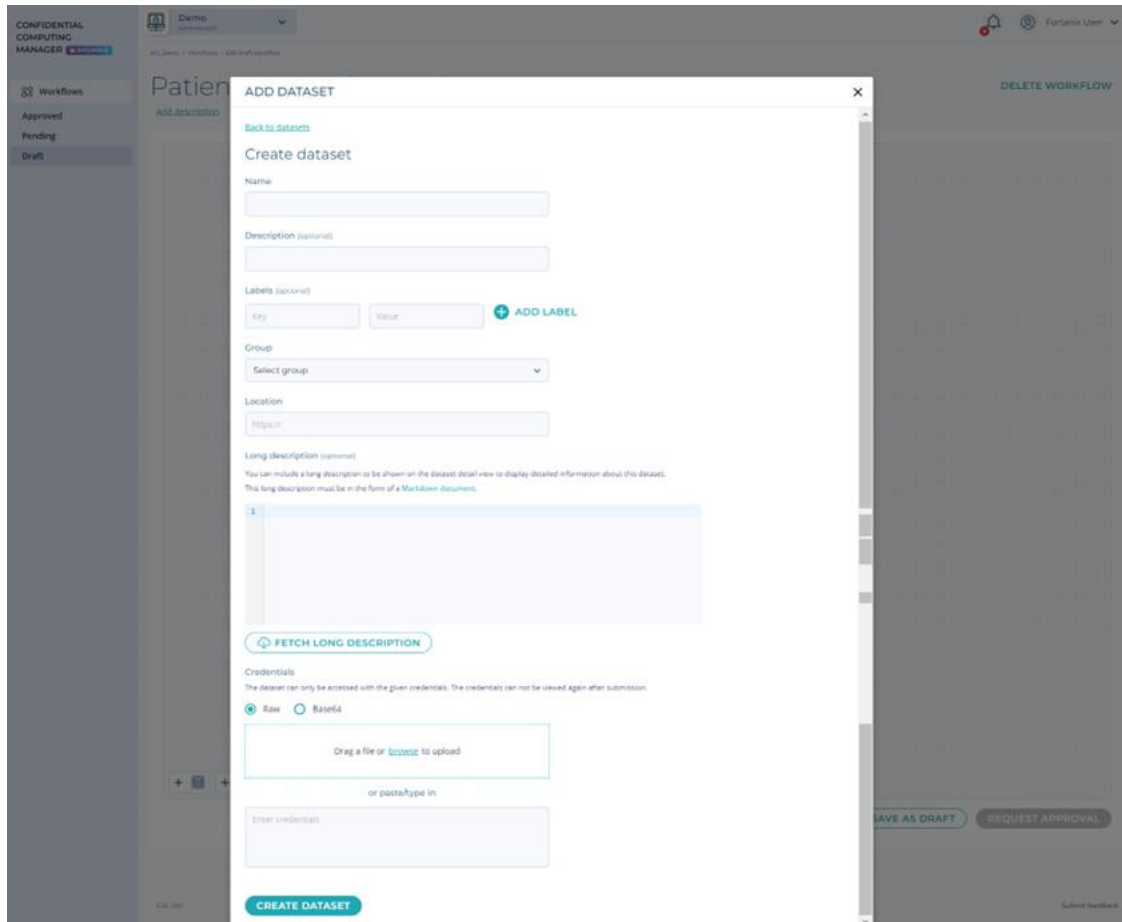


FIGURE 5: CREATE INPUT DATASET

- Establish connections between the applications and input/output datasets. To do this, connect the Input Dataset to the Application by selecting the "Input" Target Port. Repeat this process to connect the Application to the Output Dataset with the "Output" Target Port.

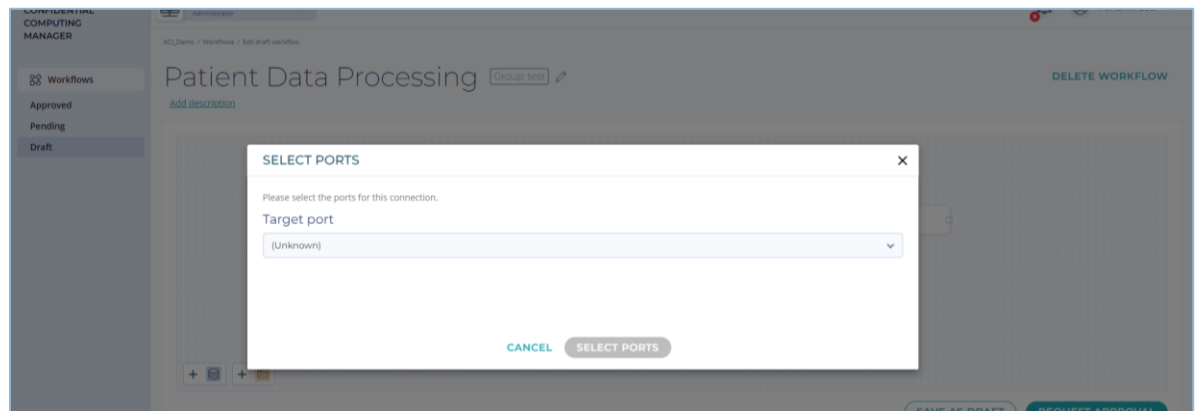


FIGURE 6: SELECT PORT FOR CONNECTION

- After the Workflow is complete, click the **REQUEST APPROVAL** button to initiate the approval process for the Workflow.

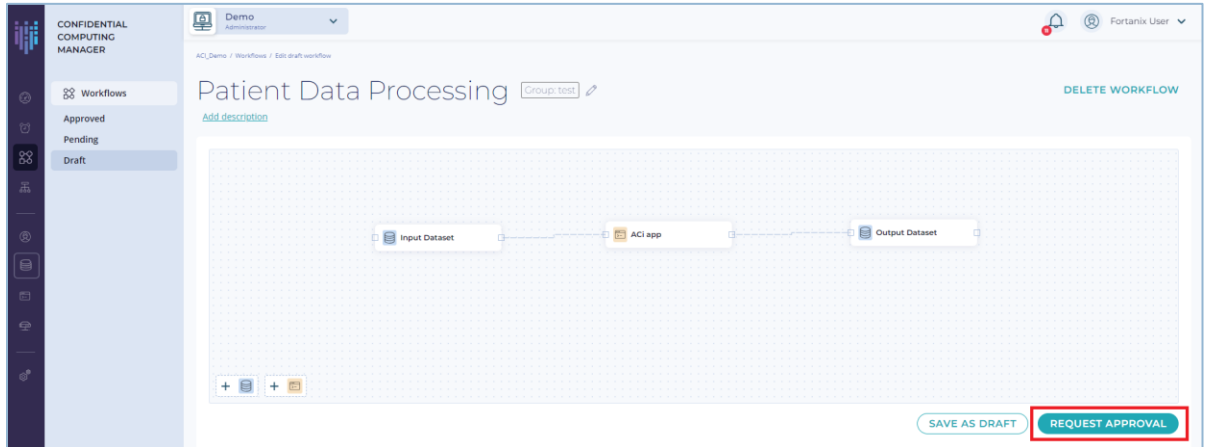


FIGURE 7: REQUEST WORKFLOW APPROVAL

WARNING: When a draft workflow is submitted for approval, it will be removed from the drafts list and editing it directly will no longer be possible once it is in a "pending" or "approved" state.

- The workflow remains in a pending state until it receives approval from all users. In the **Pending** menu item, click **SHOW APPROVAL REQUEST** to approve a Workflow.

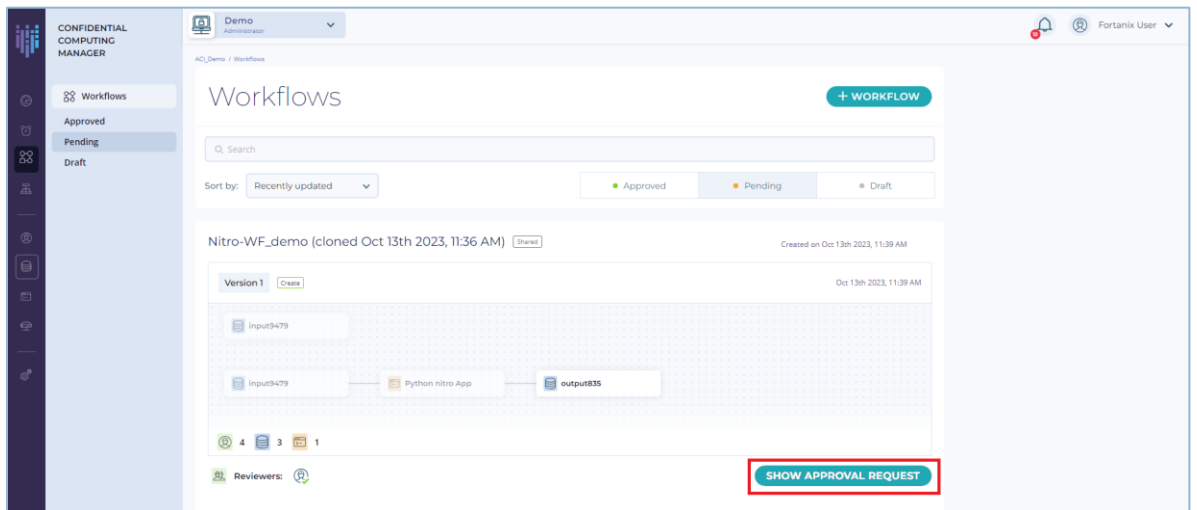


FIGURE 8: WORKFLOW IN PENDING APPROVAL STATE

- In the **APPROVAL REQUEST - CREATE WORKFLOW** dialog, you can either **APPROVE** or **DECLINE** a workflow.

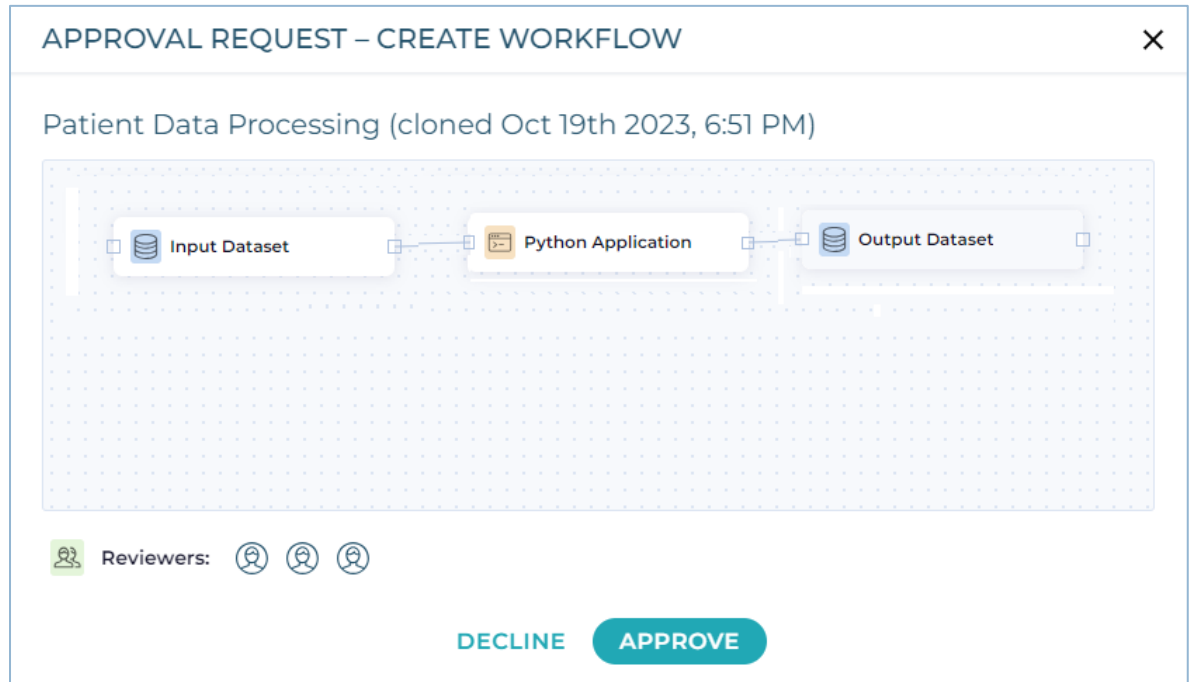


FIGURE 9: APPROVE WORKFLOW

**NOTE:**

- A user can also approve/decline a workflow from the Fortanix Confidential Computing Manager **Tasks** tab.
- Notice that the users who have approved the workflow have a green tick against their icon.

11. All the users of a workflow must approve to finalize it. If a user declines a workflow, it is rejected. When all the users approve the workflow, it is deployed.
 - a. Fortanix Confidential Computing Manager configures apps to access the Datasets.
 - b. Fortanix Confidential Computing Manager creates the Workflow Application Configs.
 - c. Fortanix Confidential Computing Manager returns the list of hashes needed to start the apps.

3.2 EDIT WORKFLOW GRAPHS

Perform the following steps to edit a workflow:

1. In the **Approved** menu item, click the overflow menu for a workflow and select **EDIT WORKFLOW** to edit the workflow. When a workflow is edited, a new version of the workflow is created for editing in "draft" state. The existing version stays unchanged. For example, if the

first version (**Version 1**) of an approved workflow “Workflow 1.0” is edited, a new version (**Version 2**) of “Workflow 1.0” is created.

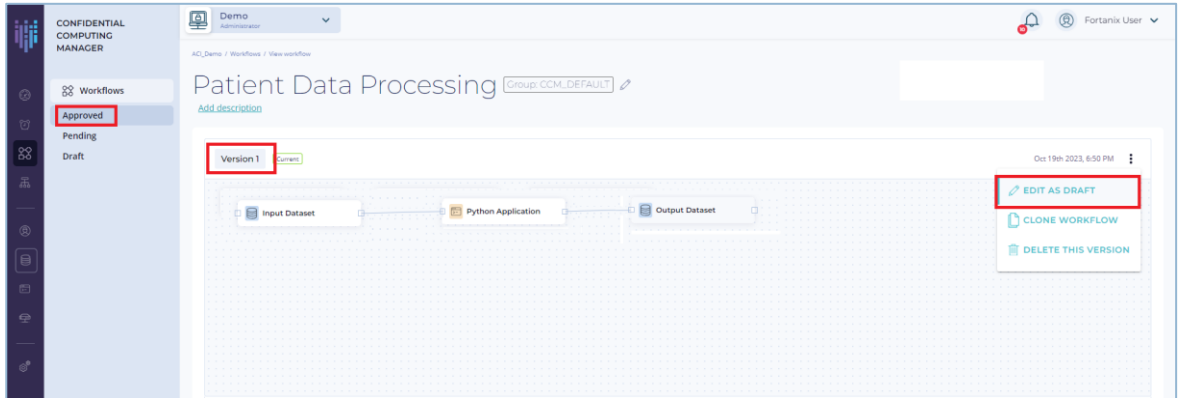


FIGURE 10: EDIT A WORKFLOW

2. Update the workflow graph with the required changes and click **REQUEST APPROVAL** to submit the workflow for approval.

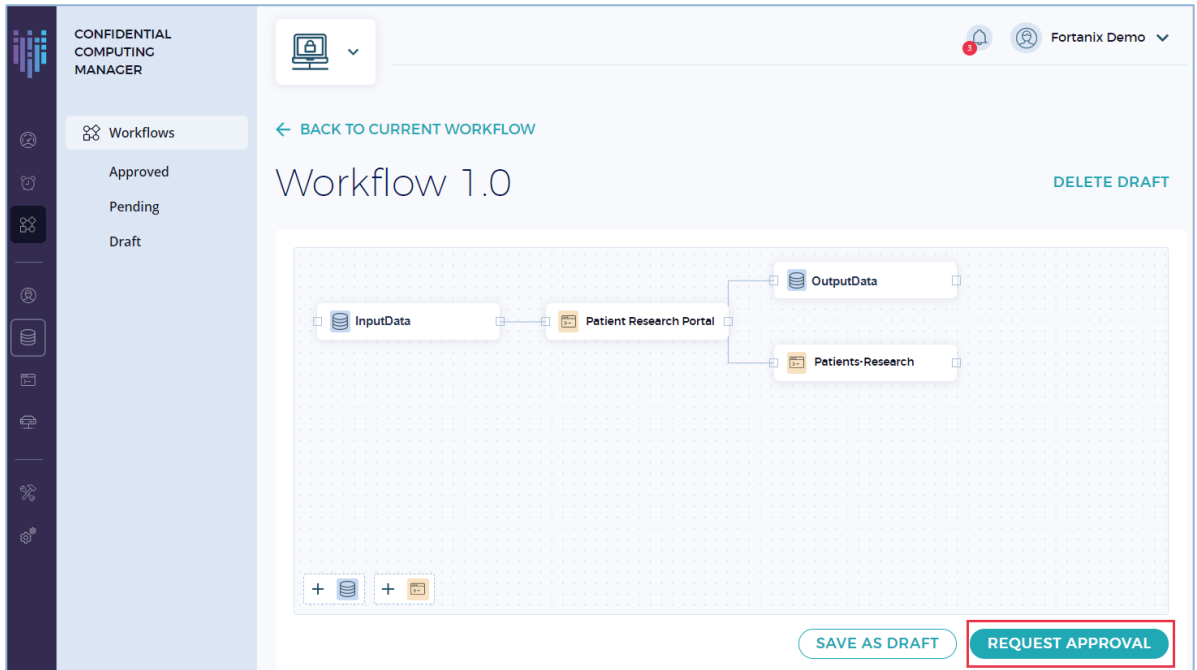


FIGURE 11: REQUEST EDITED WORKFLOW FOR APPROVAL

3. A new version (**Version 2**) of the workflow is created in “pending” state. Click **SHOW APPROVAL REQUEST** to approve the workflow.

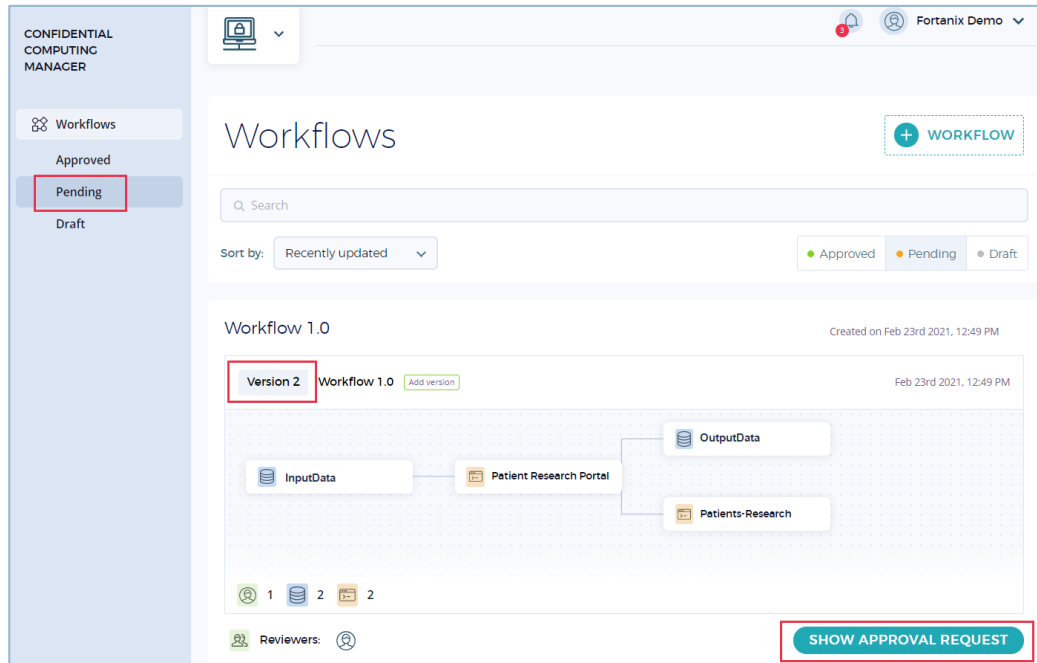


FIGURE 12: EDITED WORKFLOW IN PENDING STATE

4. Click **APPROVE** to approve the workflow.

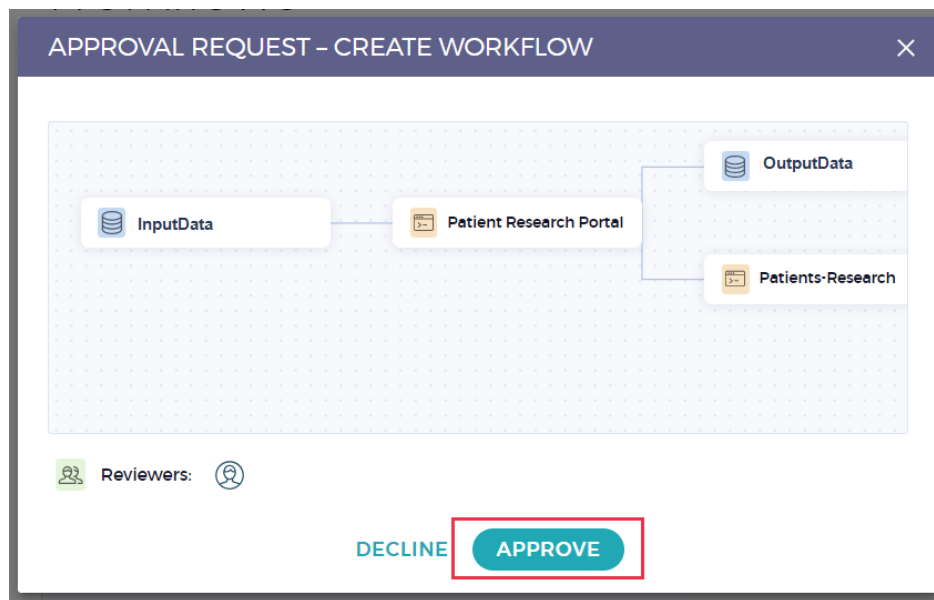


FIGURE 13: APPROVE THE WORKFLOW

5. After the workflow **Version 2** is approved, it will be linked to **Version 1**. Now, the user can either delete workflow **Version 1** or restore it.

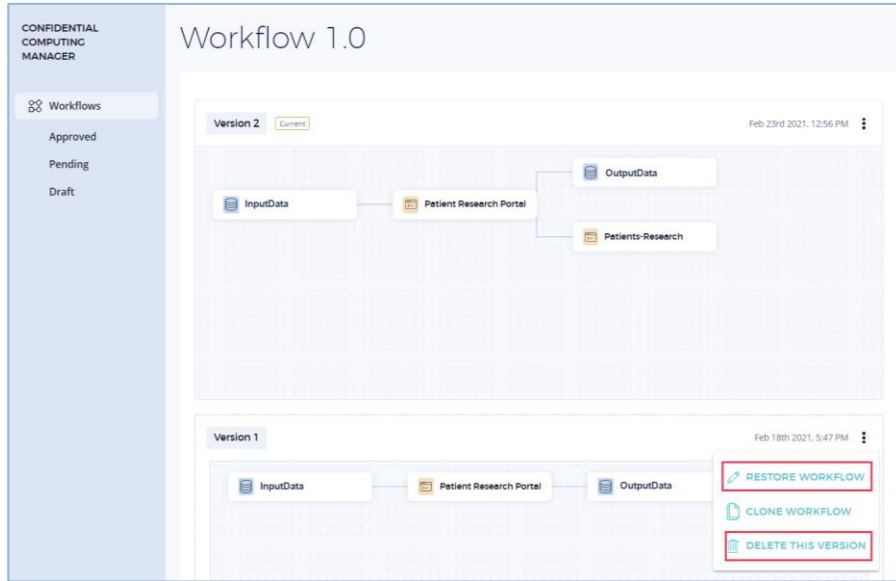



FIGURE 14: WORKFLOW VERSION 1

3.3 CLONE WORKFLOW GRAPHS

A workflow is cloned when you want to create a copy of an existing workflow instead of creating it from scratch. To create a workflow clone:

1. For an approved or draft workflow, click the overflow menu on the right and select **CLONE WORKFLOW** to copy the workflow. When a workflow is cloned, the new workflow is created with a modified name. For example, if the approved workflow “Workflow 1.0” is cloned, a new workflow “Workflow 1.0 (clone)” is created. The user can modify the workflow name using the Edit  icon next to the name.

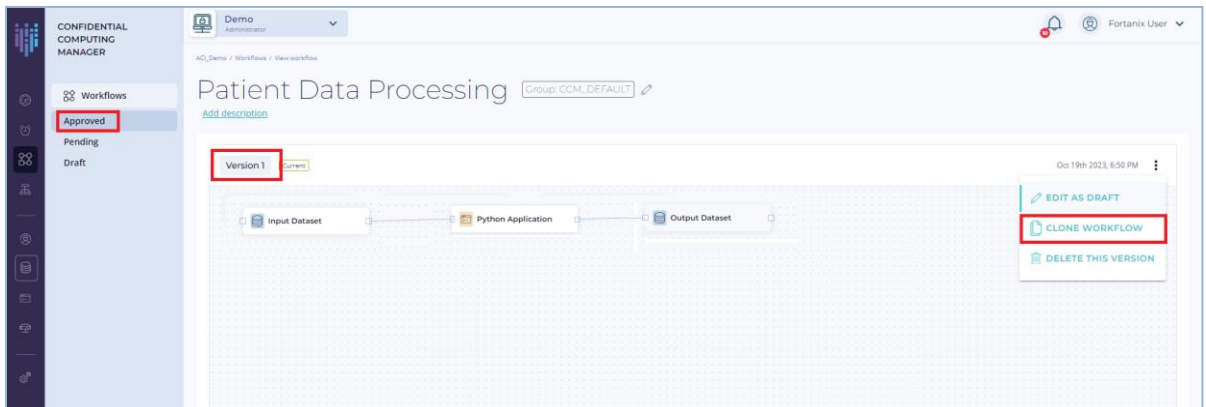


FIGURE 15: CLONE A WORKFLOW

2. Update the workflow graph with the required changes and click **REQUEST APPROVAL** to submit the workflow for approval.
3. A new workflow is created in “pending” state.

3.4 DELETE WORKFLOW GRAPHS

To delete a workflow:

1. For an approved workflow, click the overflow menu on the right and select **DELETE WORKFLOW** to delete the workflow.

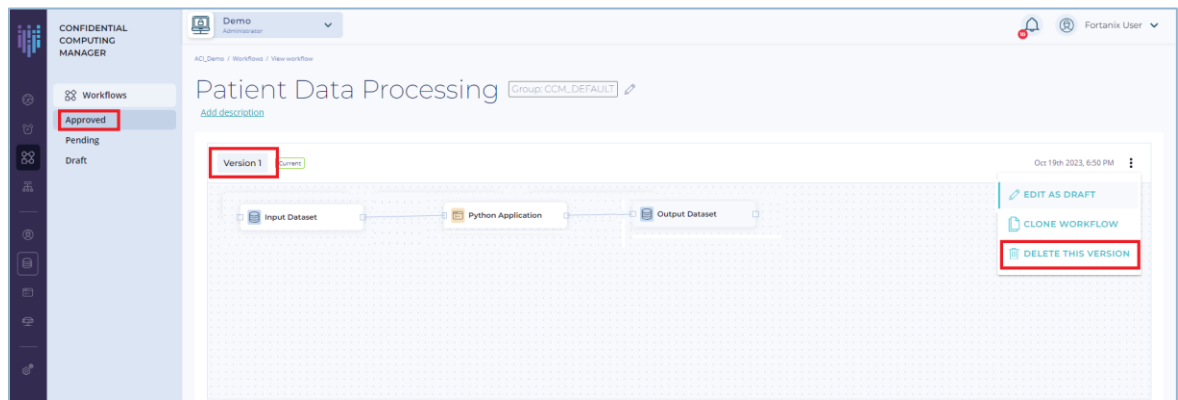


FIGURE 16: DELETE A WORKFLOW

2. In the **DELETE WORKFLOW** dialog box, click **DELETE** to confirm.
3. The workflow is deleted.

4.0 DOCUMENT INFORMATION

4.1 DOCUMENT LOCATION

The latest published version of this document is located at the URL:

<https://support.fortanix.com/hc/en-us/articles/360056935452-User-s-Guide-Create-Update-Clone-and-Delete-Workflows>

© 2016 – 2023 Fortanix, Inc. All Rights Reserved.

Fortanix® and the Fortanix logo are registered trademarks or trade names of Fortanix, Inc.

All other trademarks are the property of their respective owners.

NOTICE: This document was produced by Fortanix, Inc. (Fortanix) and contains information which is proprietary and confidential to Fortanix. The document contains information that may be protected by patents, copyrights, and/or other IP laws. If you are not the intended recipient of this material, please destroy this document and inform info@fortanix.com immediately.