Fortanix®

User Guide

FORTANIX CONFIDENTIAL COMPUTING MANAGER – DEPLOY WORKFLOWS – WEB INTERFACE

VERSION 3.0

Fortanix Inc. | 3910 Freedom Circle | Suit 104 | Santa Clara, CA 95054 | United States of America | +1 (650) 943-2484
info@fortanix.com | www.fortanix.com

TABLE OF CONTENTS

1.0 INTRODUCTION

Welcome to the Fortanix Confidential Computing Manager (CCM) User Guide. This document describes how to deploy a Fortanix CCM workflow graph using the Fortanix CCM web interface.

⚠ DISCLAIMER - The Fortanix Confidential Computing Manager Workflows feature will only be enabled for Customers with an "Enterprise" license.

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:

NAVIGATION BUTTONS

TABS	FUNCTIONALITY
 **INFRASTRUCTURE**	Click this tab to see: • 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.
 **APPLICATIONS**	Click this tab to see: • 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 button 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 button to access the SGX Converter tool to convert an application.
 **USERS**	Click this button 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 DEPLOY THE WORKFLOW : WEB INTERFACE

After a workflow is approved by all the users, you can execute the application in the workflow using the workflow **RUN** button that allows users to start the application job and monitor them.

NOTE:

- Currently, the **RUN** button works only for single job deployments, that is, workflows that only contain a single application will run using the **RUN** button. In future releases of Fortanix Confidential Computing Manager, multiple jobs will be supported.
- The application execution will be performed on the Azure Kubernetes Service (AKS) runtime environment. In future releases of Fortanix Confidential Computing Manager, other runtime environments will also be supported for workflow deployment.

3.1 EXECUTE THE APPLICATION ON AZURE KUBERNETES SERVICE

3.1.1 PREREQUISITES

The following needs to be configured in Fortanix Confidential Computing Manager:

- **Compute Clusters**: A compute cluster is a set of nodes that run containerized applications. Compute clusters are used to run Fortanix Confidential Computing Manager workflows. *Refer to Section 3.1.4 for steps to configure a compute cluster in Fortanix CCM and access the cluster.*
- **Job specification**: A Kubernetes job spec is a YAML file. A skeleton is provided as input to Fortanix CCM with user parameters. This is then updated by Fortanix CCM with relevant environment variables. Please see the example for expected inputs. *Refer to Section 3.1.5 for steps to configure the Kubernetes job specification.*

3.1.2 CREATE AN AKS CLUSTER

To set up an AKS Cluster, refer to the article how to set up an AKS cluster as worker nodes in Fortanix CCM. The article shows you how to:

- Create a cluster
- Configure Fortanix Node Agent
- Use the cluster to deploy applications manually

3.1.3 OBTAIN THE KUBECTL CONFIG FILE

A `kubectl` YAML file is used to configure the compute cluster. This file stores the following:

- The client certificates, token, and cluster CA certificate. This is the only authentication mechanism for AKS. We do not yet support username/password or other authentication options.
- The server address.
- Metadata like cluster name and user name.

The following are the usual steps for Azure Kubernetes Service to obtain a `kubectl` config file. For more information refer to official documentation from Microsoft.

1. Log in on the command line.

```
az login
```

2. Get a list of all the available subscriptions.

```
az account list
```

3. Select a subscription.

```
az account set --subscription subscription-id
```

4. Get the AKS credentials.

```
az aks get-credentials --name (cluster-name) --resource-group (
cluster-resource-group)
```

The config is now available in `~/.kube/config` folder.

NOTE: The credentials can be revoked if needed using the command: "`az aks rotate-certificates`" but this will incur downtime, for more information, check Microsoft Azure Kubernetes Service documentation.

3.1.4 CONFIGURE THE AKS COMPUTE CLUSTER IN FORTANIX CCM

In order to start applications using the RUN button, you must configure the AKS credentials in Fortanix CCM.

NOTE: Only the Azure Kubernetes Service is available at the moment.

To configure the AKS cluster in Fortanix CCM:

1. Click the **Infrastructure** tab in the Fortanix CCM left panel and select the **Compute Clusters** tab.
2. In the Compute Clusters page, click **ADD COMPUTE CLUSTER** to configure a new compute cluster.

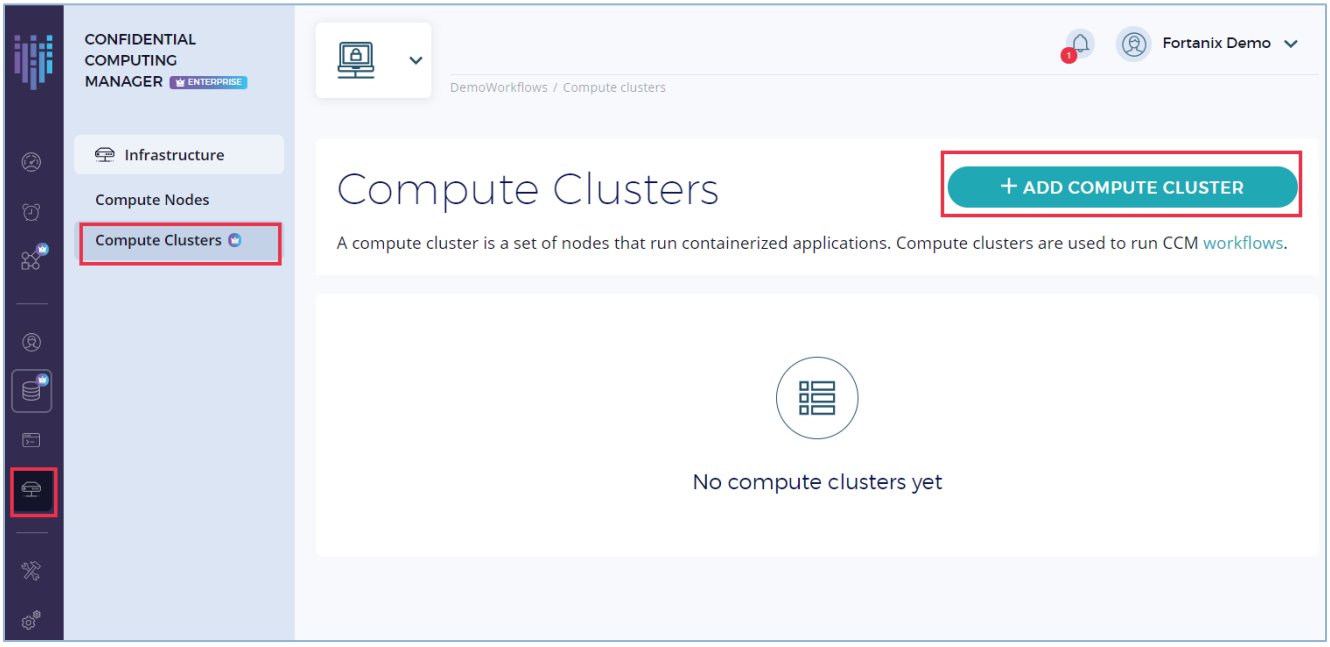

FIGURE 1: CREATE COMPUTE CLUSTER

3. In the "Add Cluster" form, enter the following details:
   - **Name**: The AKS cluster name.
   - **Type**: The runtime environment, that is, **Kubernetes**.
   - **Kubernetes Configuration**: The YAML file obtained in *Section 17.1.3* that has the AKS configuration details.

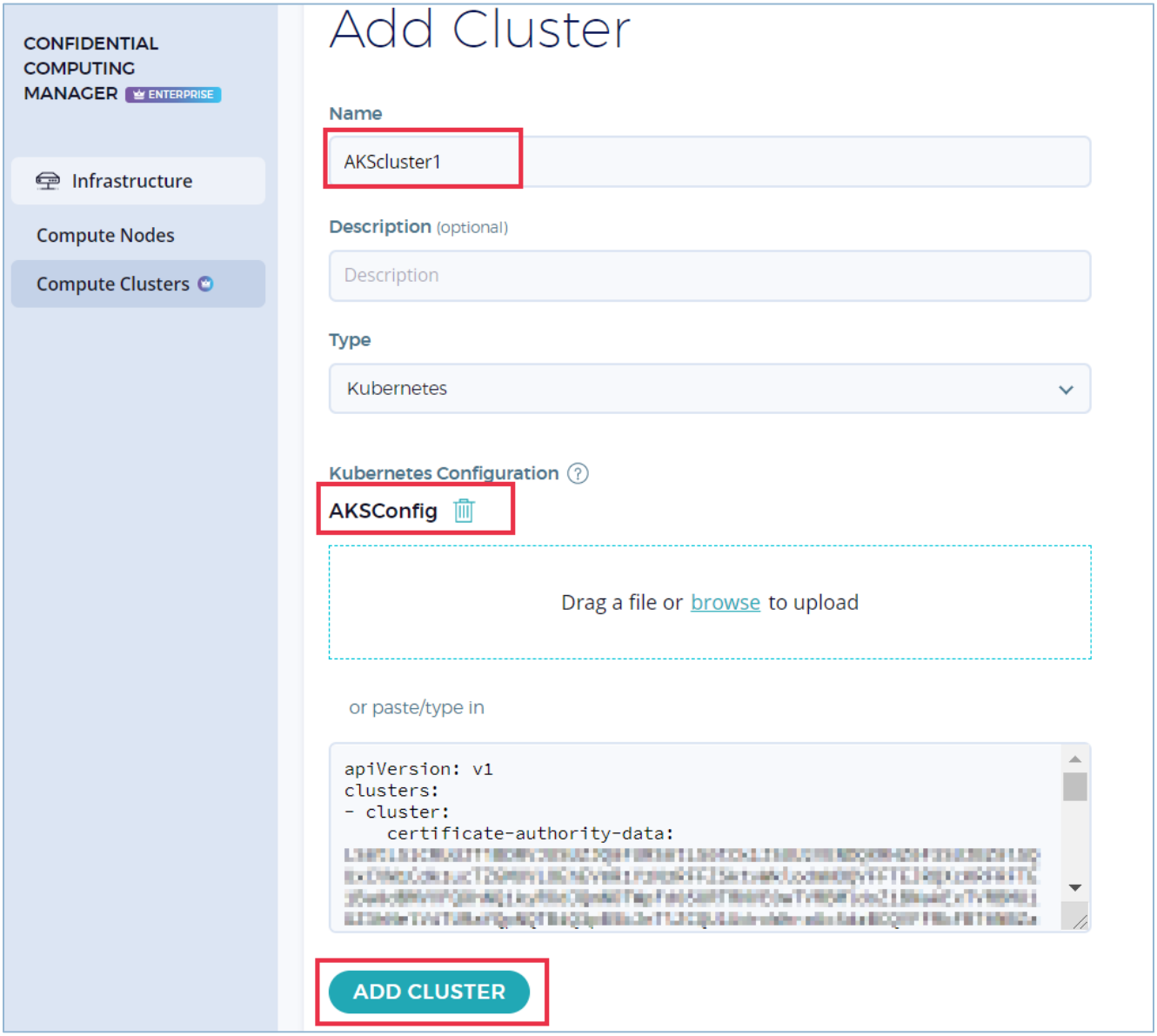

FIGURE 2: CONFIGURE THE COMPUTE CLUSTER

4. Click **ADD CLUSTER** to save the cluster configuration. The cluster is successfully configured.

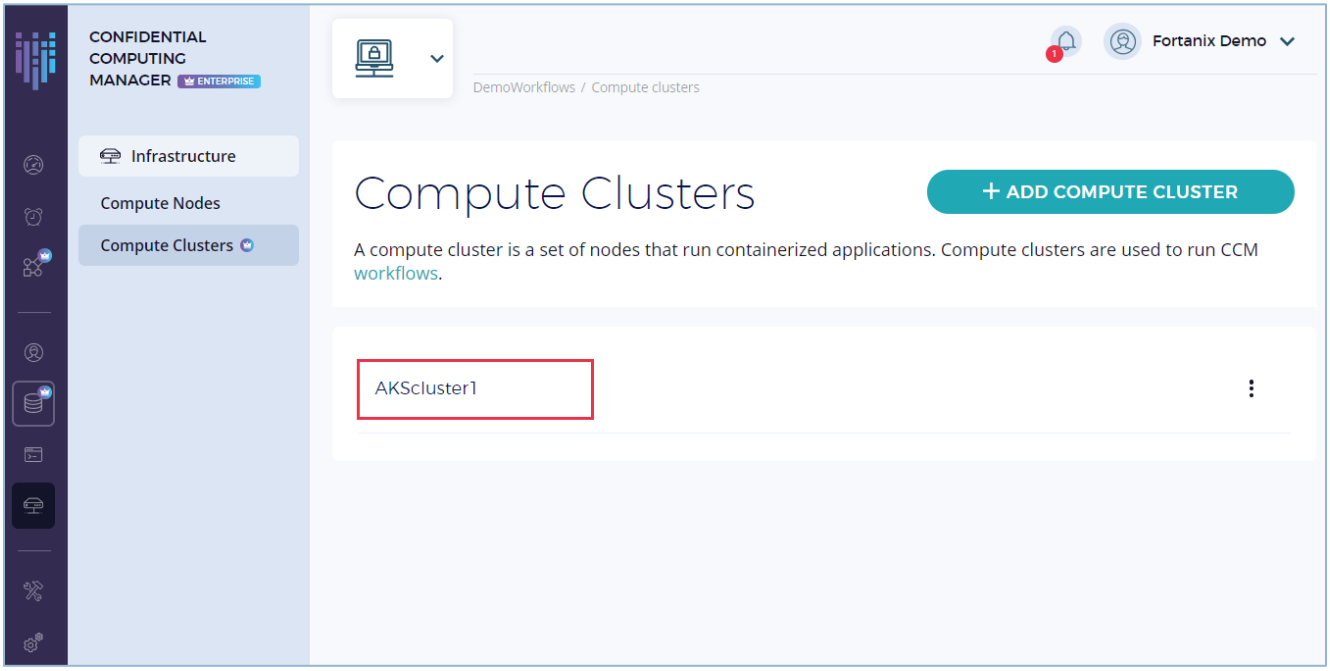

FIGURE 3: CLUSTER CONFIGURED

3.1.5 CONFIGURE WORKFLOW

To run a workflow application, you need to configure the workflow by following the steps below:

1. Click the **Workflows** tab and on the Workflows page, select the **Approved** workflows tab.
2. In the list of approved workflows, select a workflow that has a single application since Fortanix CCM 3.5 supports only single job deployments.

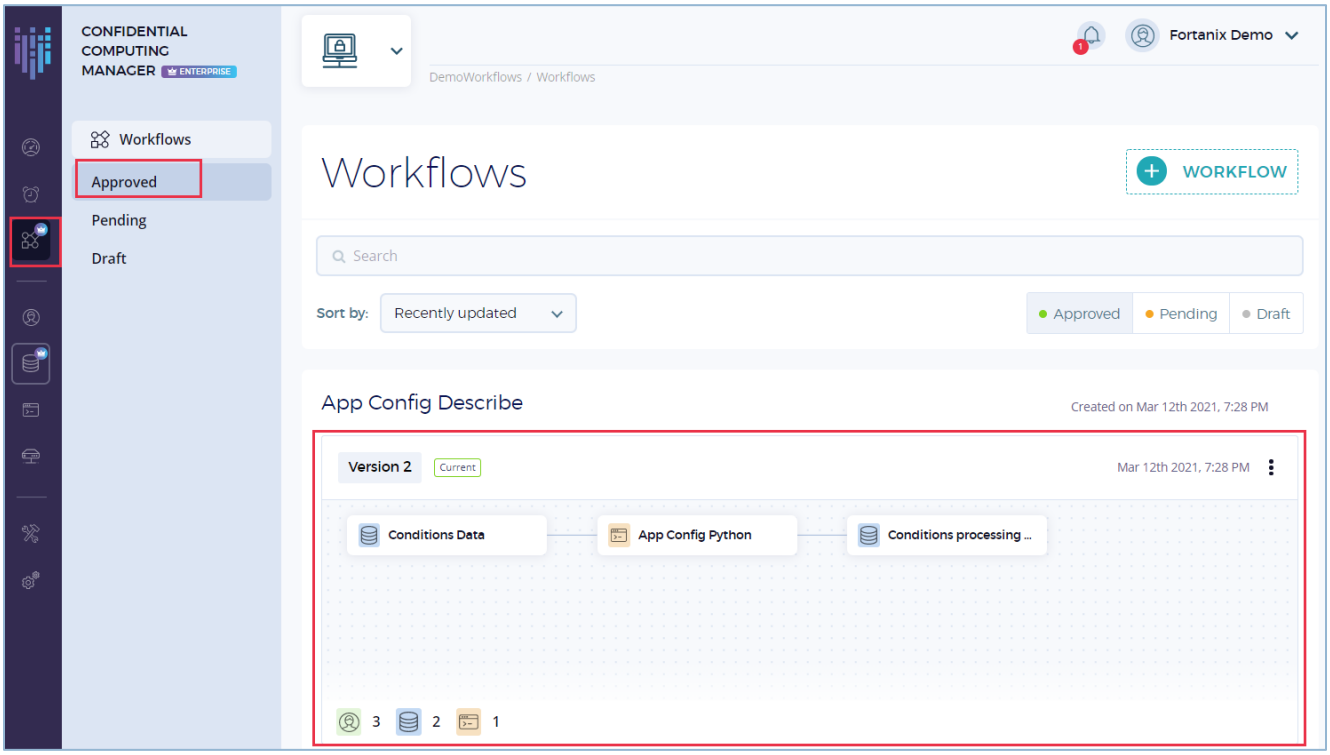

FIGURE 4: SELECT APPROVED WORKFLOW

3. In the detailed view of the selected workflow, you will notice a **RUN** button in the disabled state. The **RUN** button will be disabled if you have not configured the job specification. To enable the **RUN** button, configure the Kubernetes job specification using the Configuration icon next to the **RUN** button.

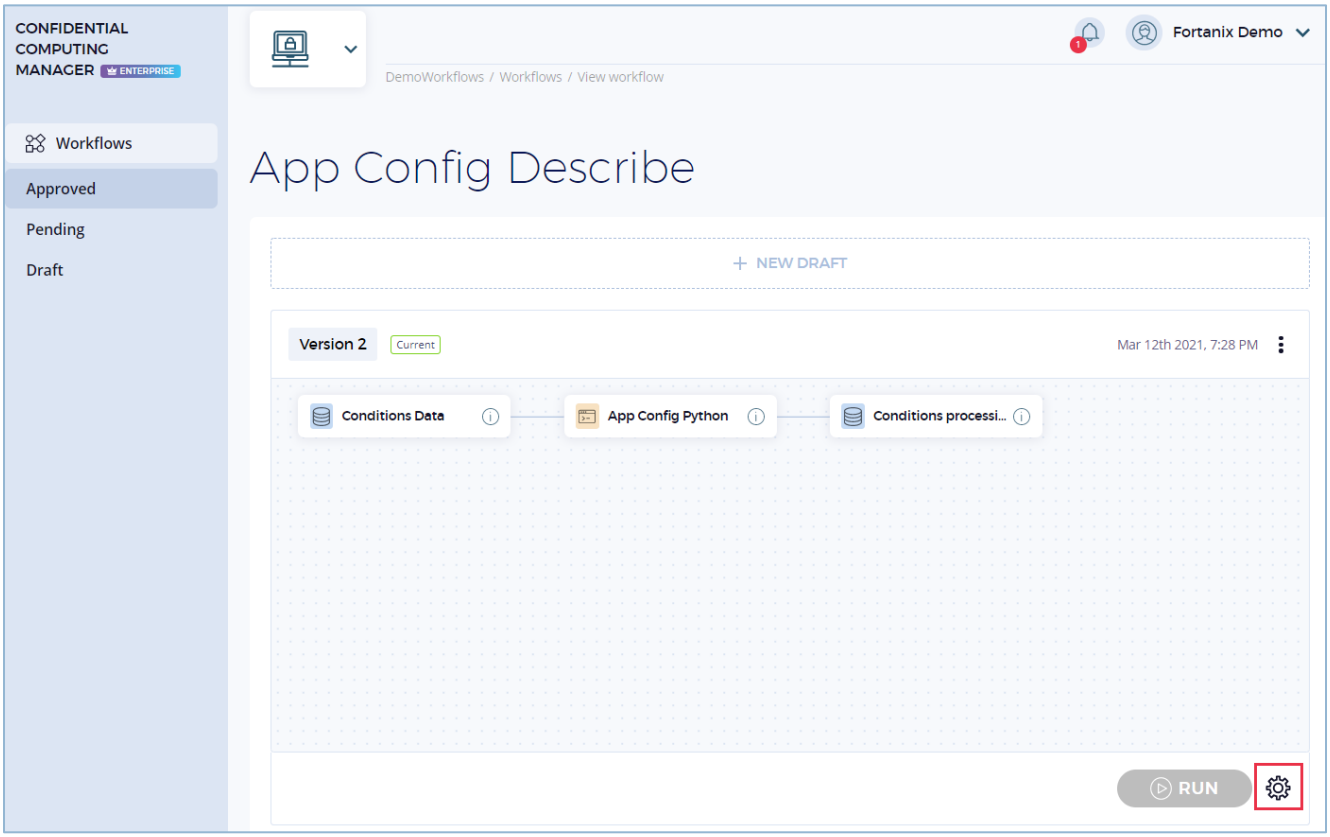

FIGURE 5: CONFIGURE JOB SPEC

4. In the RUN WORKFLOW window, enter the following details:
   - **Deployment Type**: The workflow deployment type, that is, **Kubernetes (Single Job)**. Currently, Fortanix CCM supports only a single job deployment.
   - **Namespace**: The Kubernetes namespace
   - **Cluster**: The cluster that you configured in Fortanix CCM. Currently, Fortanix CCM supports only the AKS cluster as the runtime environment for deploying the workflow.
   - **Deployment Type**: The deployment type for the application, that is, **Kubernetes**.
   - **Job Specification**: The Kubernetes job specification YAML file that is required by the cluster and the application to run the application job.

```
apiVersion: batch/v1
kind: Job
```

```
metadata:
  name: job-name
spec:
  backoffLimit: 0
  template:
    spec:
      containers:
      - name: containername
        resources:
          limits:
            kubernetes.azure.com/sgx_epc_mem_in_MiB: 1
      imagePullSecrets:
      - name: dockerhub
      restartPolicy: Never
```

 **NOTE:**

- This is a Kubernetes job spec: https://kubernetes.io/docs/concepts/workloads/controllers/job/
- Fortanix CCM will update it with relevant environment variables.
- We need to provide `imagePullSecrets` if the docker image is behind a password-protected docker repository.
- Fortanix CCM does not push any secrets stored in it, it is the user's responsibility to configure these in Kubernetes.

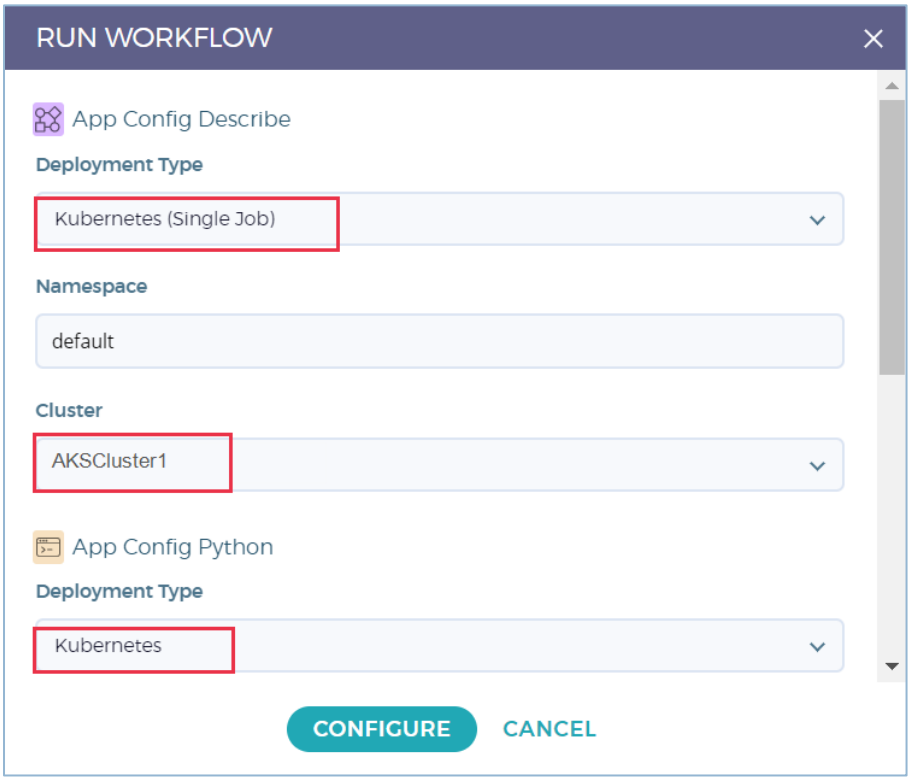

FIGURE 6: CONFIGURE JOB SPEC

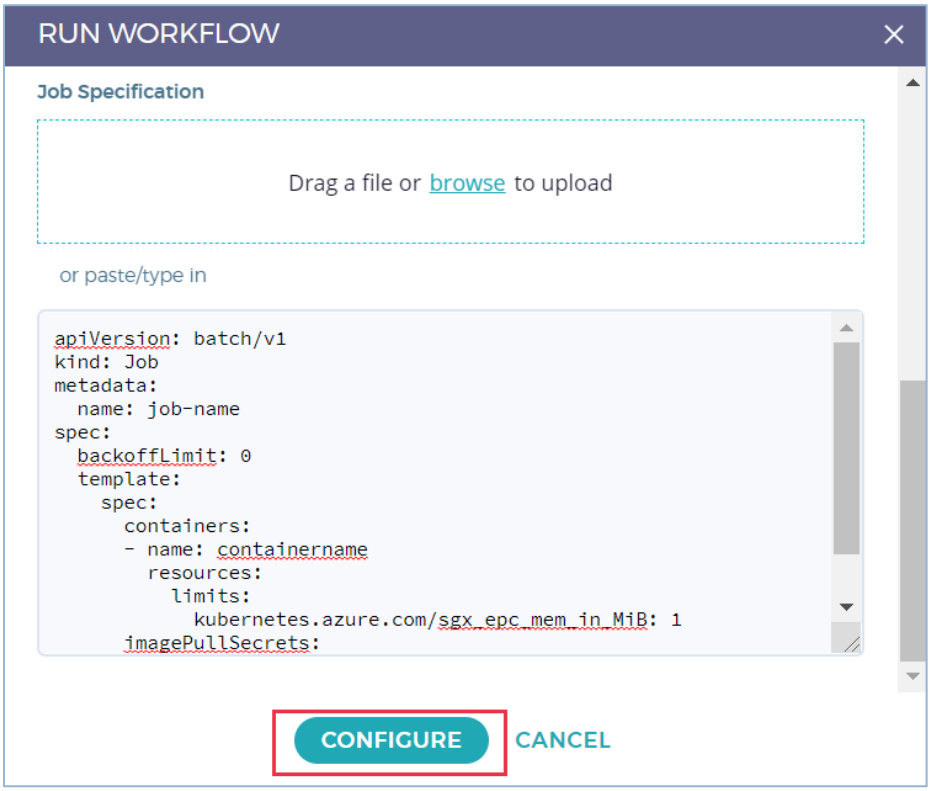

FIGURE 7: CONFIGURE JOB SPEC

5. Configure secret in Kubernetes.
   - This is a subset of: https://kubernetes.io/docs/concepts/configuration/secret/
   - For any information, please refer to the official documentation above.

   To configure the secret:
   - If you are using a docker hub, generate a token as in this example.
   - If you are using ECR - get a token using the CLI.
   - Using the docker server, for the docker hub, it is the URL used in this example.

NOTE: Tokens usually expire, so the following step needs to be refreshed.

```
kubectl delete secret dockerhub
kubectl create secret docker-registry dockerhub --docker-server=https:
//index.docker.io/v1/ --docker-username=username --docker-password=pas
sword
```

6. Click **CONFIGURE** to configure the Kubernetes job specification.
7. If the job spec is configured successfully, you will see the **RUN** button enabled.

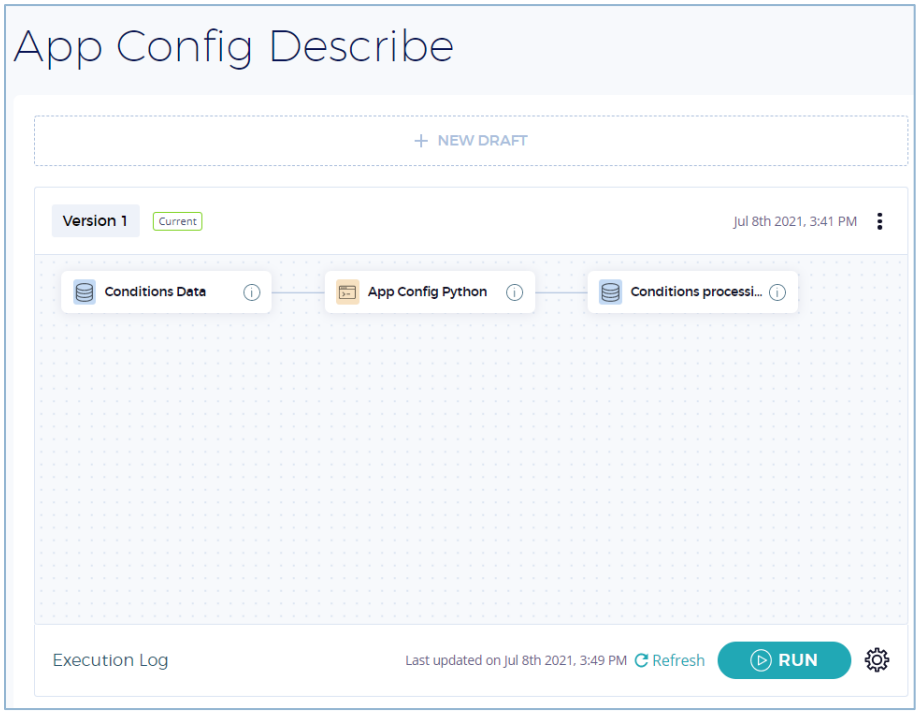

FIGURE 8: RUN ENABLED

3.2 RUN THE WORKFLOW APPLICATION

To run the Workflow application,

1. Configure the image pull secret.
2. Click the **RUN** button in the detailed view of an approved workflow that you enabled in the previous section.

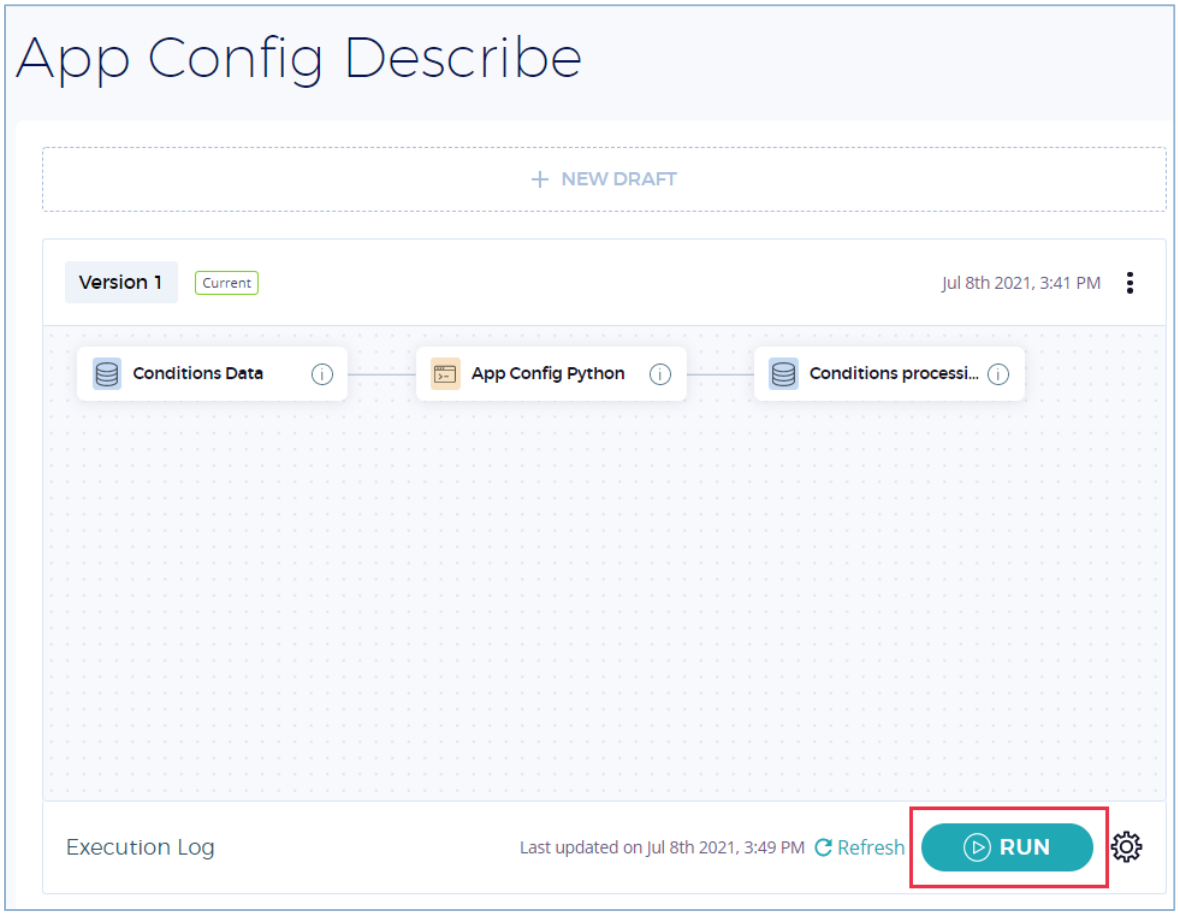

FIGURE 9: RUN THE APPLICATION

1. In the RUN WORKFLOW modal window, the **Cluster**, **Job Type**, and **Job Spec** that you configured in the previous section will be selected.
2. Click **RUN** to run the workflow.

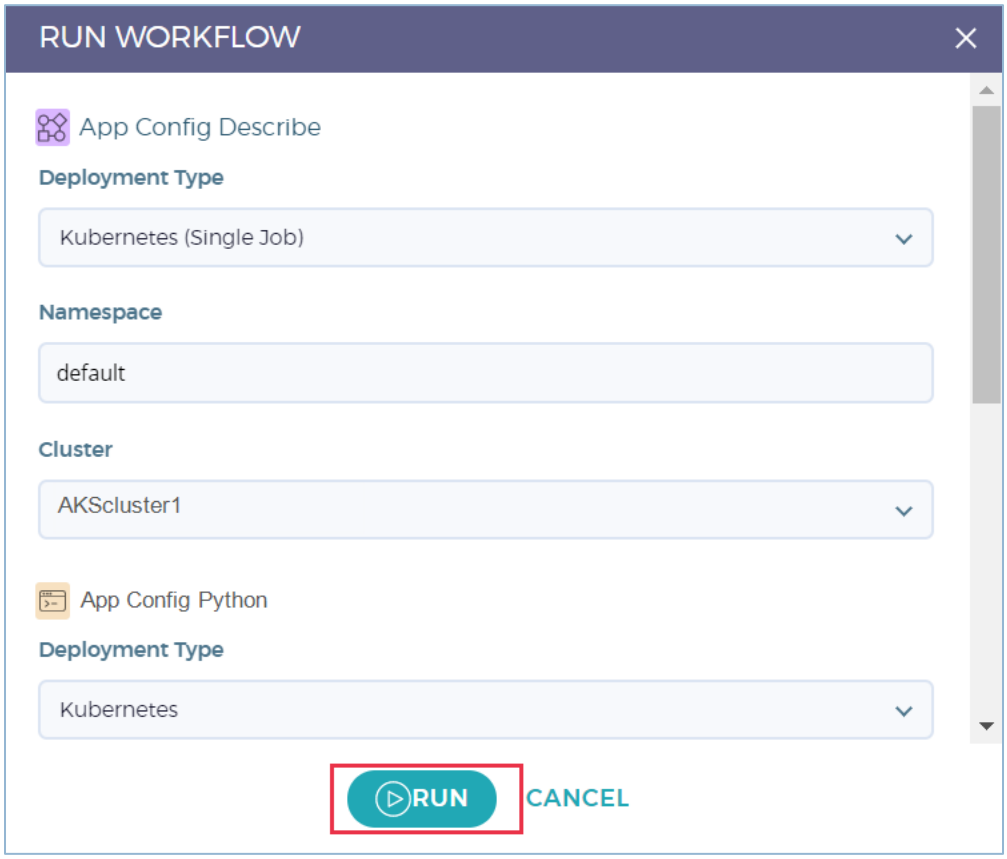

FIGURE 10: RUN WORKFLOW

3. You will notice the **Running** indication at the bottom of the workflow.

   NOTE: The workflow execution status is not updated live as it must be fetched from the cluster manually. Hence click the Refresh icon to get the latest execution status.

4. At any point, if there is a need to stop the execution, click **STOP**. This will re-enable the **RUN** button.

5. If the application is executed successfully, you will see the status of the execution under the **Execution Log**. Click the **View detail** link to view the log details.

FIGURE 11: RUNNING WORKFLOW

6. The EXECUTION LOG modal window shows the detailed logs of the run. You can also download the log using the **DOWNLOAD** link.

FIGURE 12: LOG DETAILS

NOTE: If you try to run a workflow that has more than one application, you will see the following error. The Fortanix CCM 3.5 release only supports running a workflow with a single application.

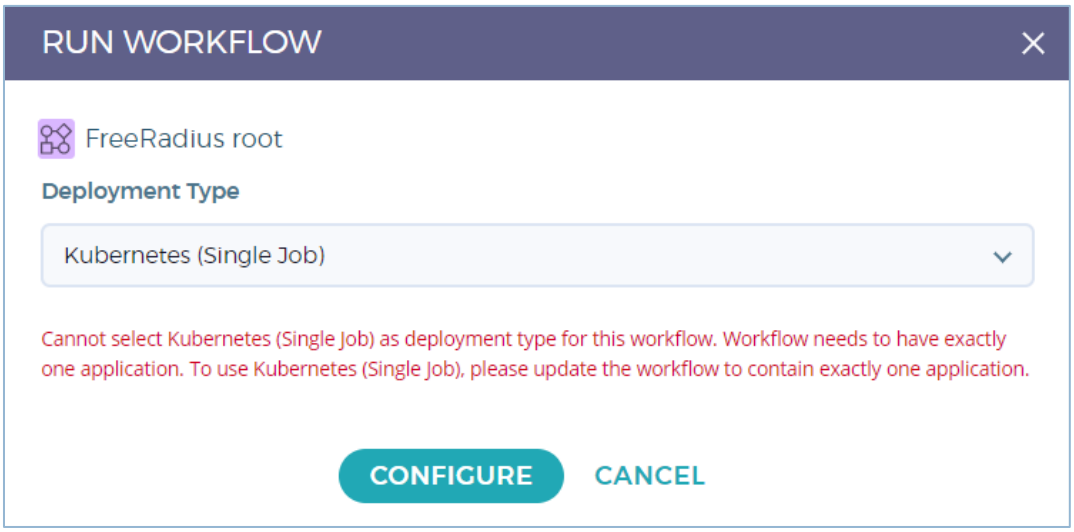

FIGURE 13: WORKFLOW EXECUTION NOT ALLOWED FOR MULTIPLE APPLICATIONS

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/4403903202836-User-s-Guide-Deploy-the-Workflow-Web-Interface

4.2 DOCUMENT UPDATES

This document will typically be updated on a periodic review and update cycle.

For any urgent document updates, please send an email to: support@fortanix.com

© 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.