Fortanix®

User Guide

FORTANIX CONFIDENTIAL COMPUTING MANAGER – DEPLOY WORKFLOWS - MANUAL

VERSION 4.0

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 manually.

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

MENU LIST	FUNCTIONALITY
INFRASTRUCTURE	Click this menu item 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.
GROUP	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.
APPLICATIONS	Click this menu item 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 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 DEPLOY THE WORKFLOW : MANUAL

After a workflow is approved by all the users, the Applications will have the Workflow Application Configurations provided to them. This configuration has information such as which Datasets or Apps they are connected to, any user-provided files or values to be provided within an enclave, and so on.

We provide a configuration to applications using an identifier passed as an input argument.

This identifier is a sha256sum of items that you need to secure from the configuration and workflow.

Fortanix CCM will also embed this identifier inside the certificates it issues so that it is clear what configuration is used for the KMS to allow access to credentials.

It embeds this inside a subject alternate name:

```
<identifier>.<mrenclave>.id.fortanix.cloud
```

With the identifier above, the KMS that stores the dataset credentials will authenticate and give credentials only to applications that present a proper certificate. When the application starts, CCM will keep track of which applications are allowed to access which configurations using the identifier.

To view the Application Identifier:

1. Click the application in the approved workflow graph.

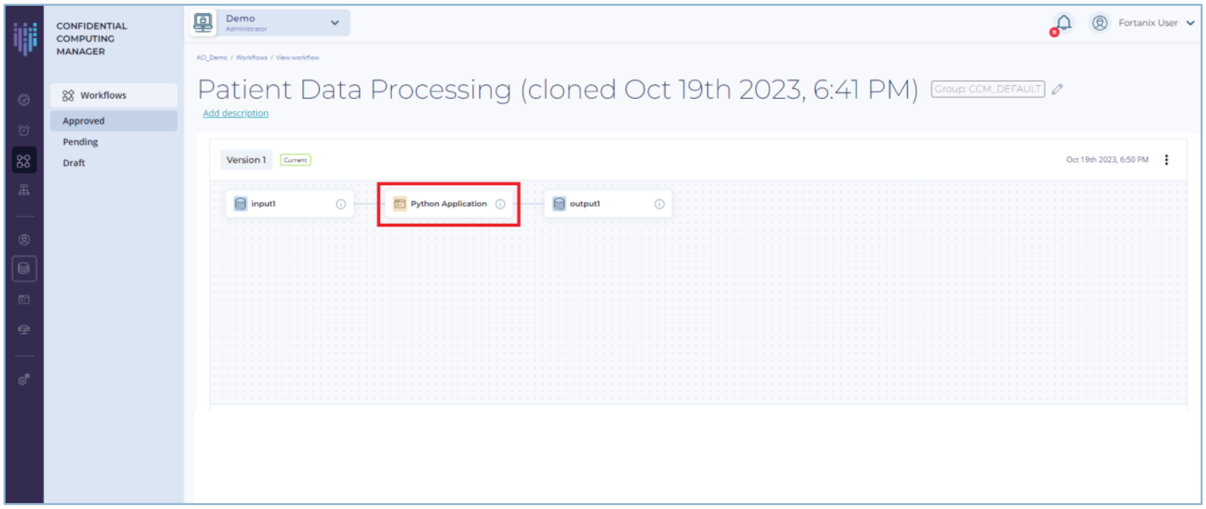
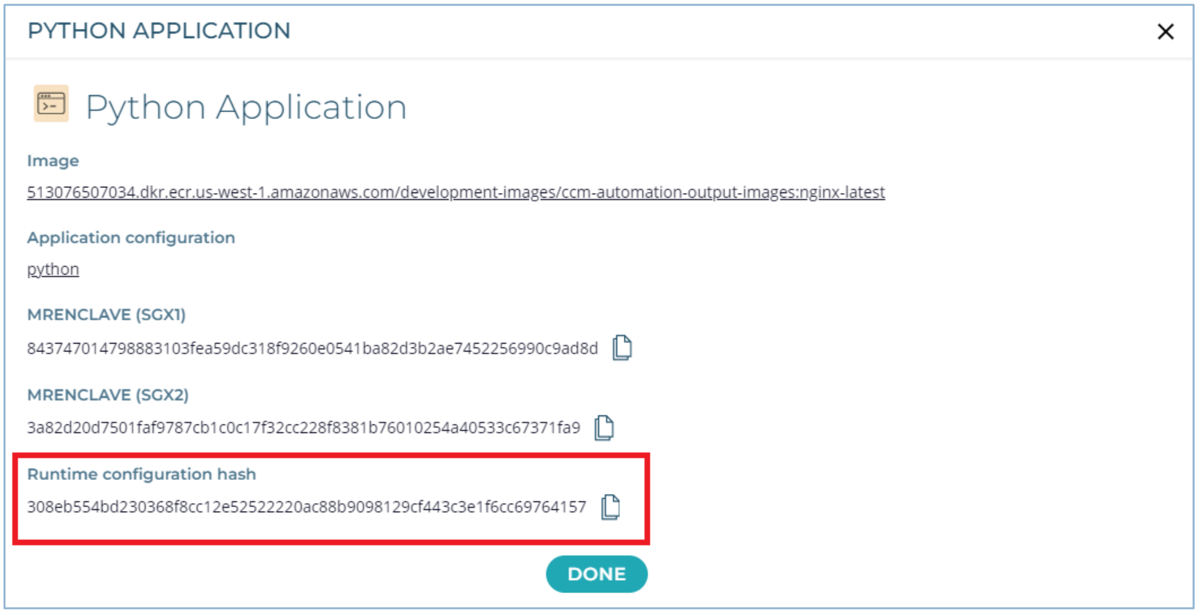


FIGURE 1: VIEW THE APP IDENTIFIER

2. In the detailed view of the workflow application, copy the value of **Runtime configuration hash**. This ID is used to run the application.



PYTHON APPLICATION

Python Application

Image

513076507034.dkr.ecr.us-west-1.amazonaws.com/development-images/ccm-automation-output-images:nginx-latest

Application configuration

python

MRENCLAVE (SGX1)

843747014798883103fea59dc318f9260e0541ba82d3b2ae7452256990c9ad8d

MRENCLAVE (SGX2)

3a82d20d7501faf9787cb1c0c17f32cc228f8381b76010254a40533c67371fa9

Runtime configuration hash

308eb554bd230368f8cc12e52522220ac88b9098129cf443c3e1f6cc69764157

FIGURE 2: COPY THE APPLICATION IDENTIFIER

3. To run the application, execute the following command depending on the type of node agent attestation:

For the node attestation type Enhanced Privacy ID (EPID)/Data Center Attestation Primitives (DCAP), use the command:

```
docker run --privileged -d -v /var/run/aesmd:/var/run/aesmd --volume
/dev:/dev -p 8085:8080 --net="host" --env NODE_AGENT_BASE_URL="http:/
/<COMPUTE_NODE_IP>:9092/v1" --env APPCONFIG_ID="de7f0cd0a293e8a9a3887
7d853dd0d94f7b67a09c48c7a520327de4ef87aa9f5" docker.io/fortanix:patie
nt-csp-v1
```

Where, `APPCONFIG_ID` is the Application identifier.

NOTE:

- Use your own inputs for Node IP, Port, and Converted Image in the above format. The information in the example above is just a sample.
- Add the following flag along with the command to get more details:
  - `-e ENCLAVEOS_LOG_LEVEL=debug` - to get debug log
  - `-p 7622:80 -p 8038:443` - to map the application's custom port to `80` or `443`.

When the App Owner starts the application with the application config identifier:

a. Applications will request an attestation certificate from the NodeAgent with the identifier as part of the report data.

b. The application requests an application certificate from NodeAgent.

c. The Fortanix Confidential Computing Manager verifies that the application is allowed to access the configuration.

d. The application requests from Fortanix Confidential Computing Manager its configuration by providing its certificate provisioned above as an authentication mechanism.

e. The Fortanix Confidential Computing Manager does certificate authentication, extracts the application identifier from the certificate, and sends back the configuration corresponding to that identifier.

f. The application verifies and applies the configuration hash.

g. The application gets the credentials from URLs in the config.

h. The application authenticates and reads/writes data from the datasets.

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/4414195329172-User-s-Guide-Enroll-a-Compute-Node-bare-metal-or-VM-SGX

https://support.fortanix.com/hc/en-us/articles/4403895262228-User-s-Guide-Deploy-the-Workflow-Manual

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

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.