Fortanix®

User Guide

FORTANIX CONFIDENTIAL COMPUTING MANAGER –RUNNING EXAMPLE APPLICATION - SGX

VERSION 4.0

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 run an example SGX application on a compute node in Fortanix CCM.

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.
 **GROUPS**	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 EXAMPLE - RUNNING AN APPLICATION

The Fortanix Confidential Computing Manager environment is designed with the goal of protecting any application. This section describes how to run a Flask Server application on a compute node.

3.1 RUNNING A FLASK SERVER ENCLAVE OS APPLICATION – SGX PLATFORM

Prerequisites:

- A Python Web Application should be created.
- A group must be created. *See the article "User's Guide: Create a Group" for more information.*

Steps:

1. Navigate to the **APPLICATION** from the menu item in the CCM UI left navigation bar, click the **+ ADD APPLICATION** button.

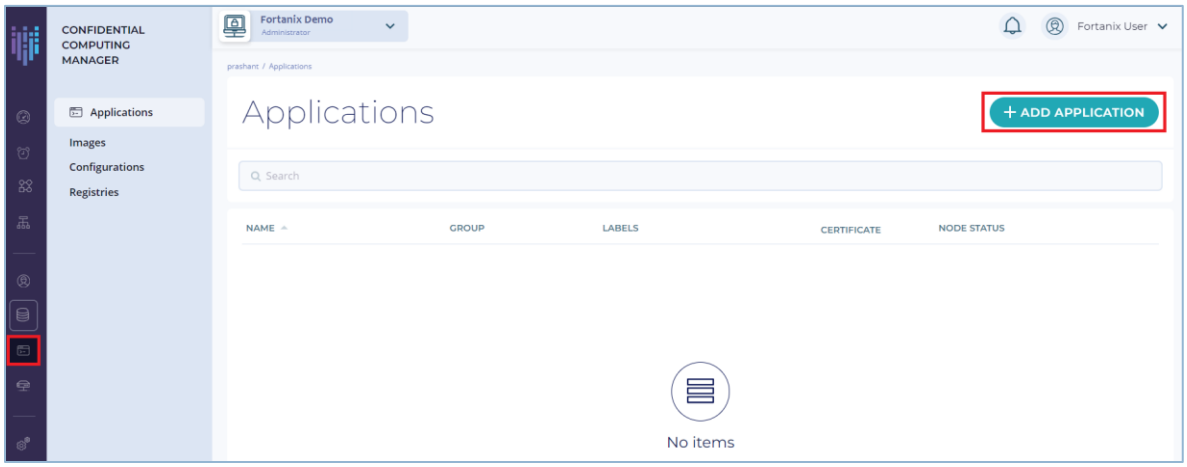


FIGURE 1: ADD APPLICATION

2. Add a Python Web Application. *See the article "User's Guide: Add and Edit an Application" for more information.*
3. Approve the domain for the Python Web Application. *See the article "User's Guide: Tasks" for more information*.
4. In the detailed view of the application, click the **+ IMAGES** button.

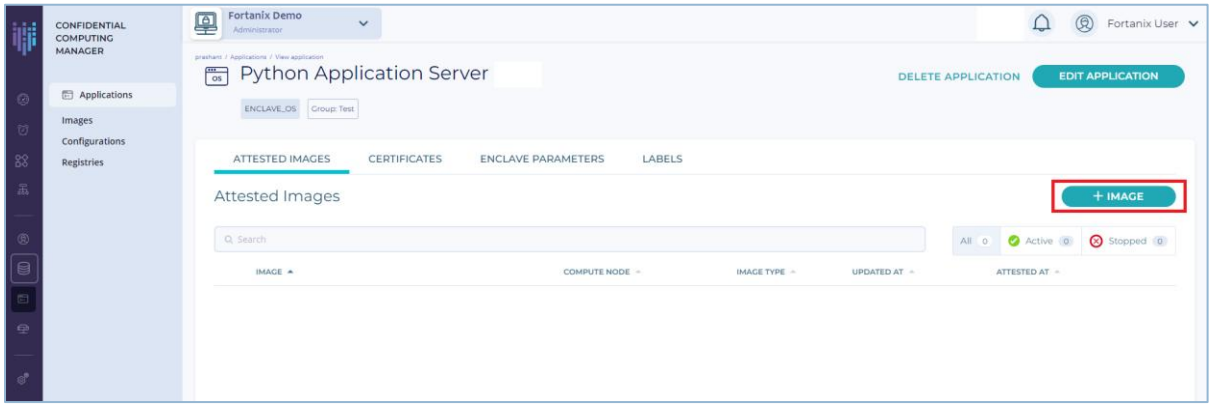


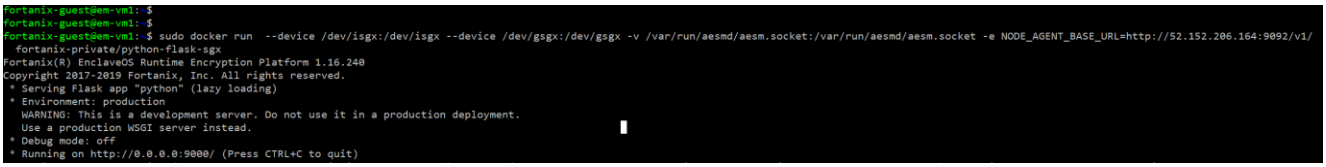
FIGURE 2: ADD IMAGE

5. Create an image of the Python Web Application by providing a proper tag. *See the article "User's Guide: Create an Image" for more information*.
6. Approve the image for the Python Web Application. *See the article "User's Guide: Tasks" for more information*.
7. For the node agent attestation type DCAP/EPID, run the application image using the following command:

```
docker run --volume /dev:/dev -v /var/run/aesmd/aesm.socket:/var/run
/aesmd/aesm.socket -e NODE_AGENT_BASE_URL=http://52.152.206.164:9092
/v1/ fortanix-private/python-flask-sgx
```

Where,

- `9092` is the port on which Node Agent listens up.
- `52.152.206.164` is the Node Agent Host IP.
- `fortanix-private/python-flask-sgx` is the converted app that can be found in the **Images** under **Image Name** column in the Images table.



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 custom port to `80` or `443`

8. To verify that the application is running, click the **APPLICATION** from the menu list in the Fortanix CCM UI and verify that there is a running application image associated with it and displayed with the application in the detailed view of the application.

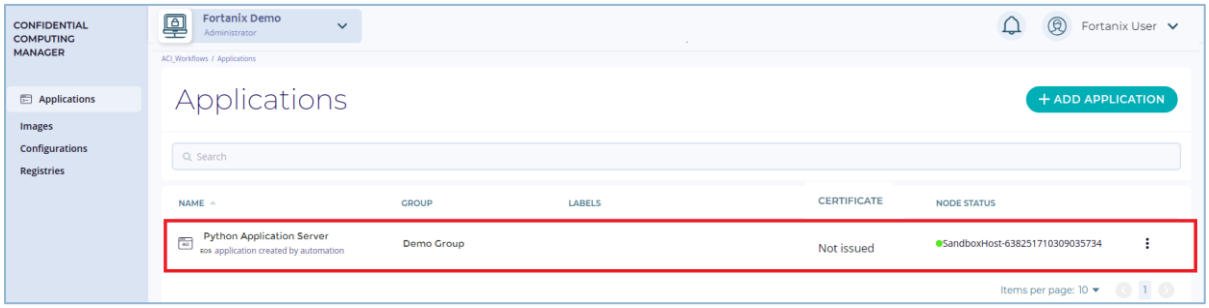


FIGURE 3: DEPLOYED APPLICATION

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/360043401152-Running-an-Example-Application-Using-SGX-Platform

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