Fortanix®

User Guide

FORTANIX CONFIDENTIAL COMPUTING MANAGER - CREATE APPLICATION CONFIGURATION

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 create an application configuration to customize the behaviour for EDP/EnclaveOS applications.

⚠ DISCLAIMER - The Fortanix CCM Application Configuration feature will only be enabled for Customers with an "Enterprise" license.

An application configuration is an object used to customize the behavior for EDP/EnclaveOS applications.

- For EnclaveOS applications, use this to insert files on the disk in a specific path.
- For EDP applications, use this to provide a key/value map to the applications.

The Application Configuration also provides information regarding connections to datasets or other applications when they are part of a workflow.

For example: You can have an Nginx Enclave OS image and use application config to provide a custom `nginx.conf` to it.

1.1 WORKFLOW APPLICATION CONFIGURATION

Application configuration objects can be assigned to apps in draft workflows. These draft workflows are sent for approval and finalized once all users approve the Workflow.

Fortanix CCM then generates a secondary/derived object called Workflow Application Configuration. This contains the original object plus information on Workflow connections needed by enclaves to access the data.

For more details about workflows, refer to User's Guide: Workflows.

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 CREATE AN APPLICATION CONFIGURATION

To create an application configuration, you need to have a pre-existing application and an image of the application.

1. Click the **Applications** icon in the CCM left panel and from the left menu select **Configurations**.
2. Click **ADD CONFIGURATION** to add a new configuration.

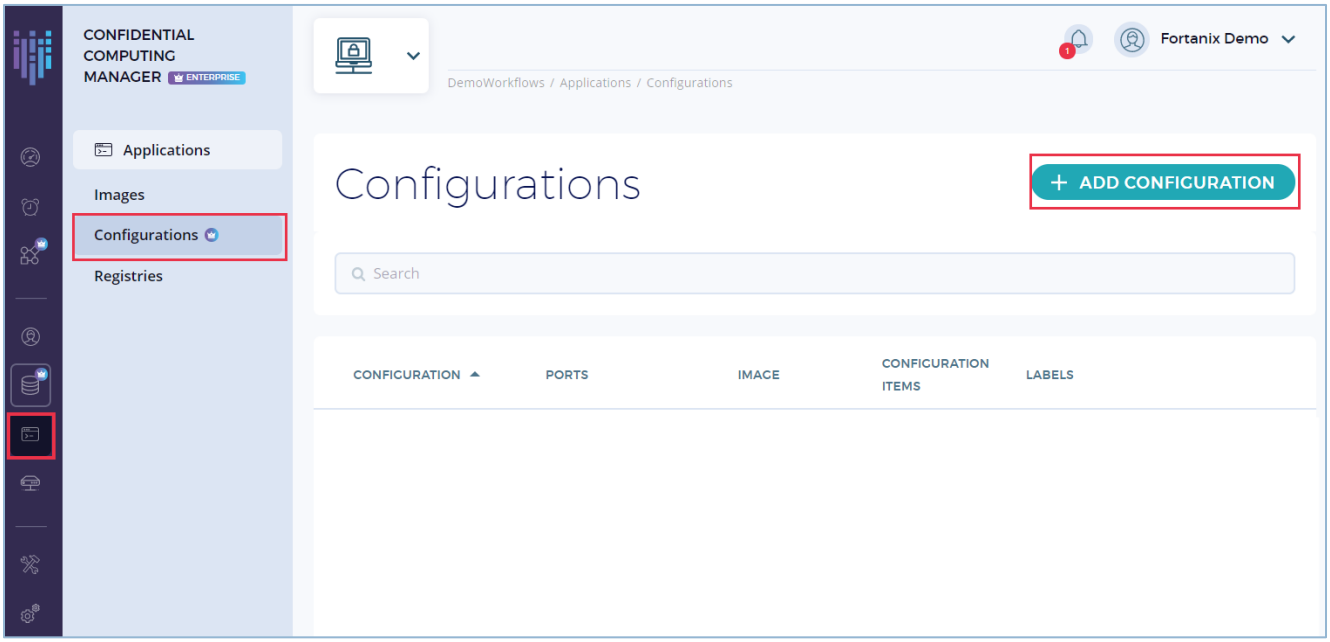


FIGURE 1: ADD APPLICATION CONFIGURATION

3. In the ADD APPLICATION CONFIGURATION window, fill the following:
   - **Image** - select the application images for which you want to create a configuration.
   - **Name** and **Description** – Enter a name and description of the configuration.
   - **Ports** – Enter the connections to be used in the workflow. These are not network ports, they are string-based tags that will be used to identify connections. You can add multiple ports depending on how the connection should work. For example: "**input**", "**output**", "**heartbeat**", and so on.
   - **Labels** (optional) – attach one or more key-value labels to the configuration.
   - **Configuration items** – These are key-value pairs used for configuring the app.

- For EnclaveOS applications, the **Key** is the path of the file that contains the **Value** for configuring an app.

   **NOTE**

  We only allow files in the path `/opt/fortanix/enclave-os/app-config/rw` for EOS applications.

- For EDP applications, set a **Key** and **Value** to configure the app.

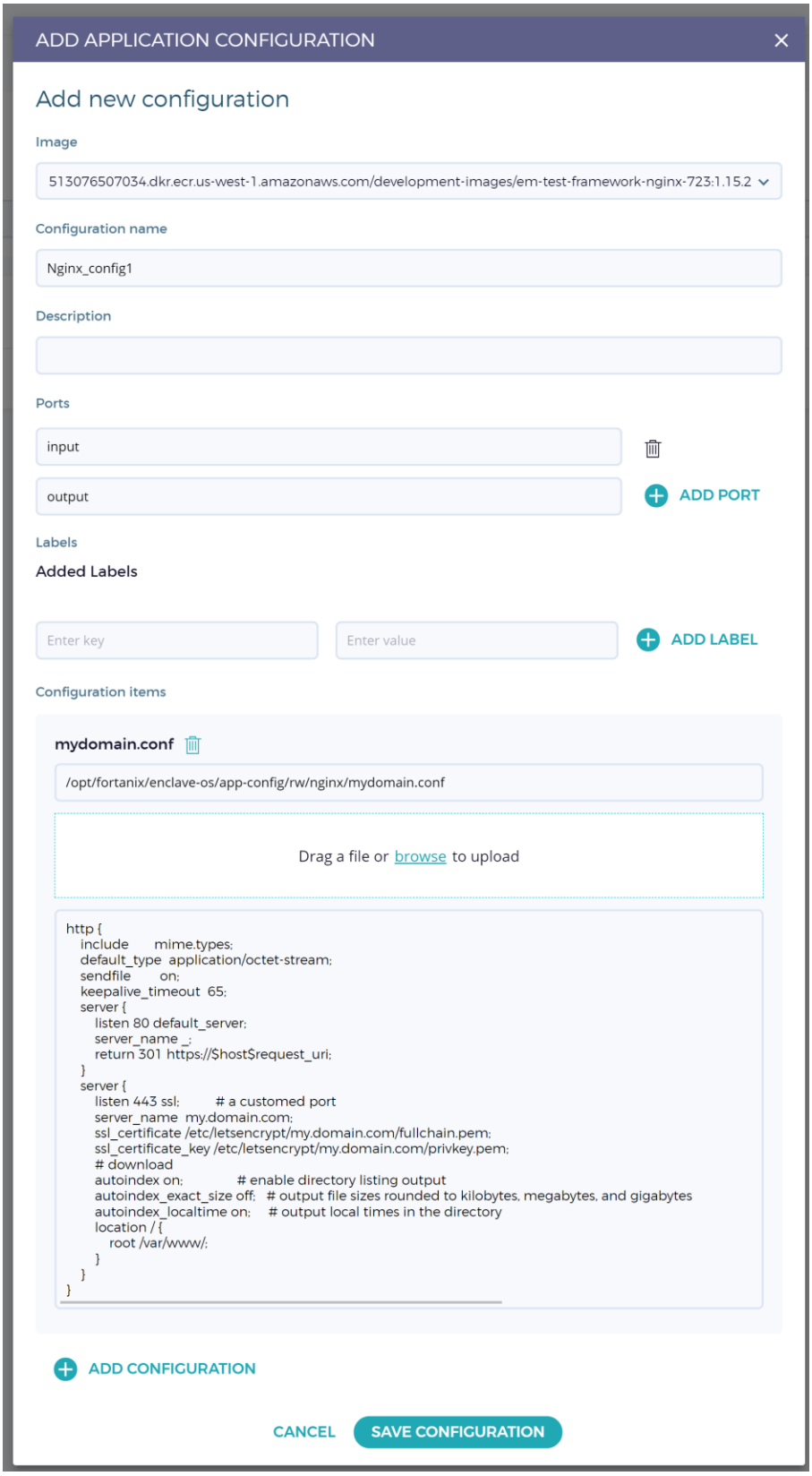
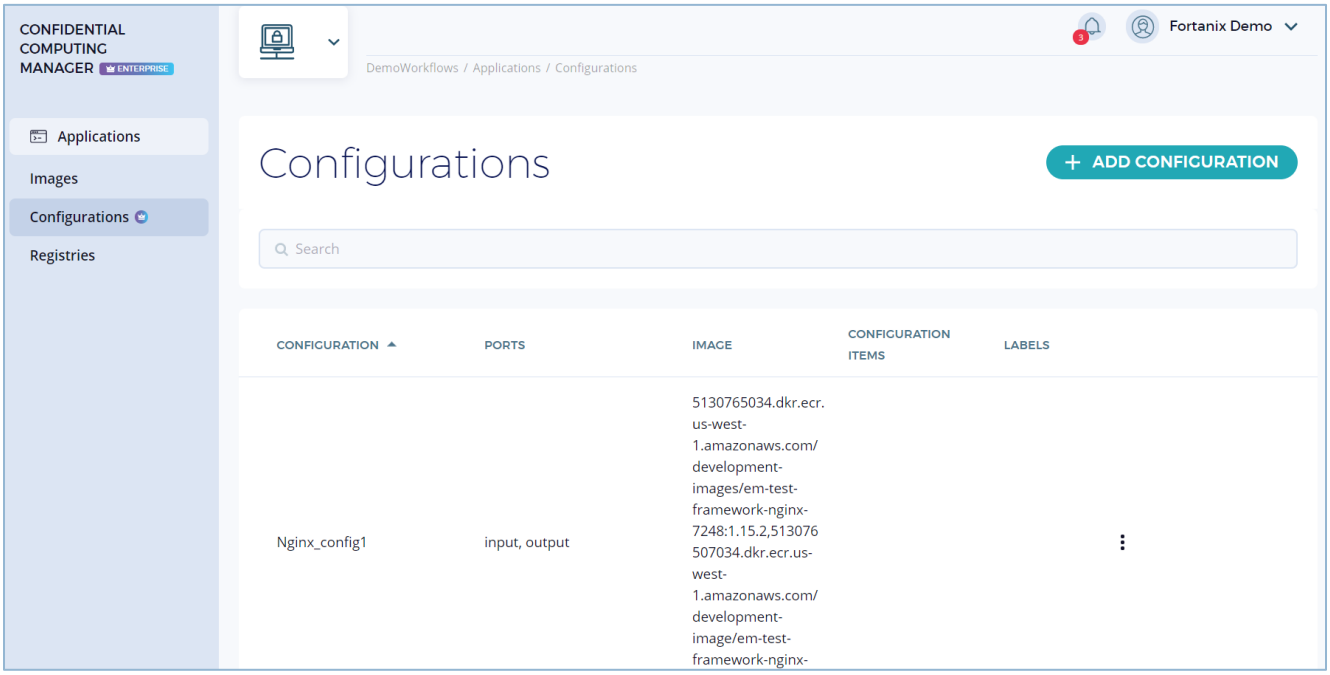


FIGURE 2: ADD APP CONFIGURATION

4. Click **SAVE CONFIGURATION** to save the configuration.



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/360057401111-User-s-Guide-Create-Application-Configuration

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