Fortanix®

User Guide

FORTANIX CONFIDENTIAL COMPUTING MANAGER – APPLICATION AND COMPUTE NODE POLICY ENFORCEMENT

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 the Fortanix CCM application and compute node policy.

Users can control which applications are allowed to run on which nodes, primarily through the use of application and node labels in the form of "Key:Value" pairs. This is enforced by having the Fortanix Confidential Computing Manager (CCM) only issue application certificates for nodes that satisfy the Fortanix CCM Application and Compute Node Policy.

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 POLICY

When labels are added for an application, we are adding requirements to the application and these labels become the "required" labels. When the same labels are added to the compute nodes, we are adding labels that can be provided by the compute node on which the application will run once the compute node is enrolled in Fortanix CCM. The attached labels of an application and compute node will be compared when Fortanix CCM issues a certificate to an application and if all the required application labels match with the provided compute node labels then a certificate for the application on the compute node will be issued. In the case of a label mismatch, no such certificate will be issued. This can be seen in the logs of the application.

Hence, for an application to be allowed to run on a compute node, the set of provided compute node labels must be a superset of the set of required application labels.

Currently, the policy is enforced only when we issue certificates. So, if the policy changes after a certificate was issued, that certificate will not be revoked, it will remain valid until it expires.

3.1 RULES TO BE SATISFIED

In order for Fortanix CCM to issue a certificate for an application image to run on a compute node, the following rules must be satisfied.

- **Basic security rules:**
  - The compute node has been attested to be an SGX-capable node running Node Agent.
  - An instance of the application image has been attested to be running on the compute node.
- **Manual approvals:**
  - The image has been approved by a manager.
  - The requested domain for the certificate (that is, its subject common name) has been approved by a manager.
  - The compute node is still active (that is, it has not been deactivated).
- **Label-based rules:**

- For each key-value label associated with the application, the compute node must have the *same key* with the *same value*.

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/360045793612-Application-and-Compute-Node-Policy-Enforcement

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