User Guide

FORTANIX CONFIDENTIAL COMPUTING MANAGER –THIRD-PARTY GROUPS

VERSION 3.0

TABLE OF CONTENTS

1.0 INTRODUCTION

Welcome to the Fortanix Confidential Computing Manager (CCM) User Guide. This document describes groups and third-party groups in CCM.

A Fortanix CCM group is a collection of users and objects.

In Fortanix CCM, users can own resources such as workflows, datasets, and applications through their individual accounts, but these assets are inaccessible to users from other accounts. The third-party support enables users from other Fortanix CCM accounts to own these assets by group and collaborate with different users within a shared group.

⚠ DISCLAIMER - The Fortanix CCM Workflows, and Datasets 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.

3.0 GROUP

In the Fortanix CCM's organizational hierarchy, a group is a collection of users and objects and helps users to manage identities, create third-party groups as described in *Section 4.0: Third-Party group*, and help in organizing and securing applications, datasets, and workflows that belong to the group. A group is used to control access and usage of objects in a workflow. A group is an entity under a Fortanix CCM account. A user of an account who is an account administrator can create a group. The user who creates a group automatically gets assigned the role of group administrator. The group administrator can add more users to the group in the role of administrators or auditors.

NOTE:

- For existing Fortanix CCM accounts, after the CCM 3.35 release, a group will automatically be created for all the resources, such as applications, datasets, workflows, and so on, and set as default.
- For a new Fortanix CCM account, you must create a group manually.
- From the group list page, you can check all the associated datasets and workflows.
- You can create new datasets and workflows from the group details page.
- After a dataset, workflow, application, and application configuration are created, the `group_id` value cannot be changed.
- You can assign a `group_id` to datasets, workflows, and application configurations from their respective creation forms.
- For users in a group, you can assign the following two permissions:
    - Group administrator
    - Group auditor.

    For more information about the group roles and how to add them, refer to User's Guide: Create Groups.

4.0 THIRD-PARTY GROUP

A Fortanix CCM third-party group is an entity that is created when two groups from different accounts wish to collaborate. During collaboration, they can share the objects of each other's groups.

NOTE:

- A Fortanix CCM group can act as a source group and create third-party shared groups with other groups with which it wants to collaborate. When such third-party groups are created, the source group, along with other recipient groups (there can be more than one), can enter into a collaboration. This collaboration manifests itself in the form of a workflow.
- The creation of third-party group sharing between groups under the same Fortanix CCM account is not allowed.
- A third-party group can be in one of the following states, depending on the role (source or recipient):
    - Pending, Accepted, Rejected, or Revoked.
- After the recipient group accepts the third-party group, collaboration can begin between the respective source and the recipient groups.
- In the workflow, the source group user can allocate a placeholder to the recipient groups with whom it has a third-party sharing agreement. The recipient group user can only fill the placeholder node allocated for itself in the shared workflow. The user cannot add or delete any of the nodes in the workflow. The placeholder nodes enable the groups to bring in their respective resources (apps, datasets, and so on) for collaborating in the workflow.
- The recipient group users can only contribute datasets to a workflow, they cannot add or update an application to the workflow.
- After a workflow with placeholder nodes is filled with the objects from the required groups and is ready to go, each of the recipient groups should approve it, and the source group cannot approve the request until all recipient groups approve it. After the shared workflow is approved by all participant groups, the shared workflow will be an approved workflow.
- When a workflow is created and if any one of the participants has revoked the third-party group sharing with the source group, then the workflow will not progress.

4.1 SOURCE GROUP

A Fortanix CCM source group is the group that initiates the collaboration or sharing of assets with another group of a different Fortanix CCM account.

4.2 RECIPIENT GROUP

A Fortanix CCM recipient group is the group that receives a request from another Fortanix CCM group to participate in a collaboration or sharing of assets.

4.3 GROUP PARTICIPATION TOKEN

For a Fortanix CCM source group to request a Fortanix CCM recipient group for collaboration, it must prove itself to be an authenticated group. If this authentication is not present, a recipient group can receive multiple spam requests for group sharing from various source groups. To avoid this spamming of requests, the recipient group's administrator creates a 'group participation token', that can be used to identify itself. Only valid source group administrators are given such a group participation token. When the source group requests a recipient group for collaboration, the recipient group provides the group participation token to identify itself. The recipient group verifies the participation token in the request and authenticates the source group.

NOTE:

- The creation and sharing of a Group Participation Token between the source and the recipient group is a prerequisite for third-party groups.
- For the source group to collaborate with any recipient group, it must know the Group Participation Token of the recipient group. The recipient group user with administrator rights can generate the Group Participation token from the recipient group’s details page and share it with the source group. If the recipient group already has a generated Group Participation Token, it can share it with the source group.
- The methods in which the Group Participation Token can be shared by the recipient group with the source group are not covered in this guide and are at the discretion of the users.
- A recipient group can generate as many group participation tokens, as it requires. There is no one-to-one relationship between a source group and the Group Participation Token.

- A Group Participation Token can also be revoked by the recipient group administrator. Revoking of a Group Participation Token does not affect the existing third-party group relation between the recipient group and the source group with which the recipient group shared the Group Participation Token.

4.4 PLACEHOLDER NODE

It is a node in the Fortanix CCM workflow graph. This node can be filled with various Fortanix CCM resources, like applications, datasets, and so on.

5.0 DOCUMENT INFORMATION

5.1 DOCUMENT LOCATION

The latest published version of this document is located at the URL:

https://support.fortanix.com/hc/en-us/articles/20196282848788-User-s-Guide-Third-Party-Groups

5.2 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.