

Integration Guide

USING DATA SECURITY MANAGER WITH APPVIEWX CLMAAS

VERSION 1.0

TABLE OF CONTENTS

1.0	INTRODUCTION	2
2.0	INTEGRATING FORTANIX HSM WITH APPVIEWX.....	2
2.1	Prerequisites.....	2
2.2	Integration Procedure	2
3.0	DOCUMENT INFORMATION	6
3.1	Document Location.....	6
3.2	Document Updates	6

1.0 INTRODUCTION

The integration between AppViewX and Fortanix helps enterprises overcome the challenges brought by managing private keys in a complex infrastructure. AppViewX acts as the automation and orchestration engine for the lifecycle management of X.509 certificates, and Fortanix Data Security Manager (DSM) ensures the security of the private keys associated with those certificates in the cloud, on-premises, or as a hybrid solution.


2.0 INTEGRATING FORTANIX HSM WITH APPVIEWX CLMaaS

2.1 PREREQUISITES

- The **avx_platform_hsm** plugin should be up and running in the AppViewX cluster. If not, follow the steps given below to enable this plugin.

2.2 INTEGRATION PROCEDURE

The following are the steps to integrate Fortanix DSM with AppViewX CMLSaaS:

1. Make sure AppViewX cloud connector is installed in your network. Communication from AppViewX to Fortanix HSM will be routed through this cloud connector.
2. Log in to the AppViewX UI using valid credentials. By default, the Dashboard is displayed.
3. From the top-right corner of the Dashboard, click .
4. From the menu displayed, select **Inventory > Device**.

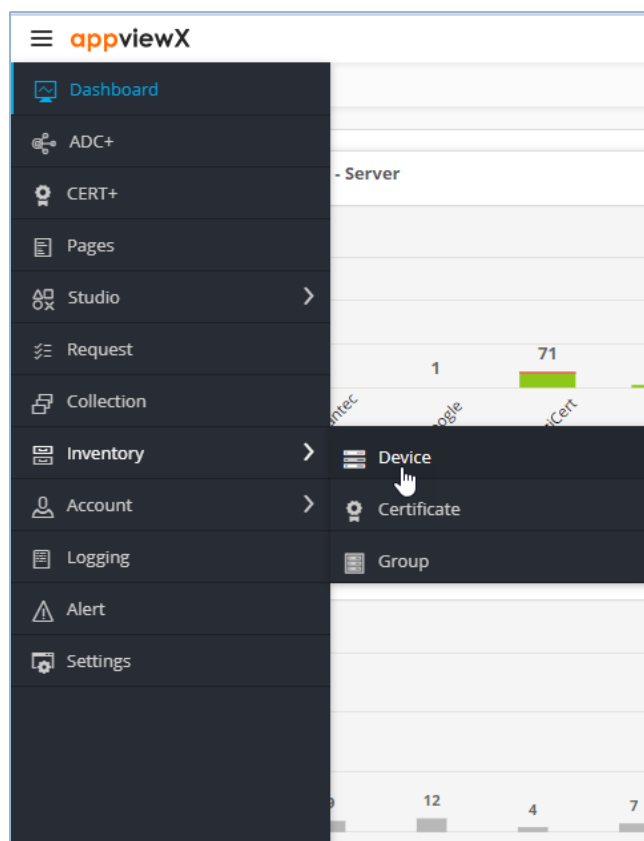


FIGURE 1: APPVIEWX DASHBOARD

The **Device :: ADC** page is displayed.

5. Under the **HSM** tab, from the navigation pane on the left, select **Fortanix**.

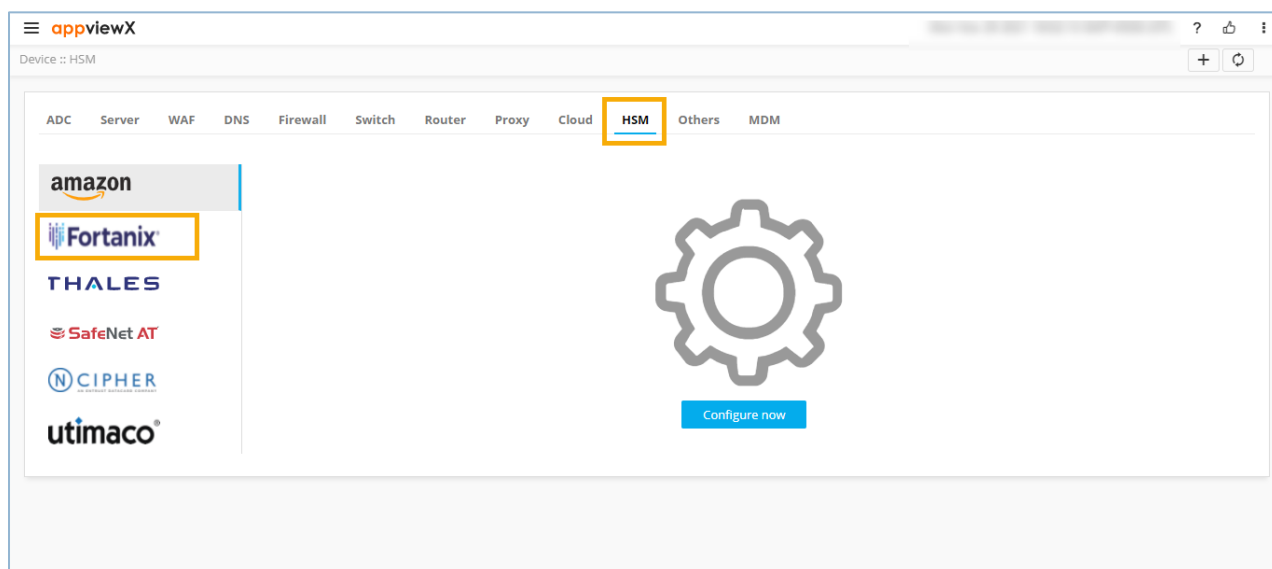


FIGURE 2: FORTANIX HSM DEVICE

6. In the **General Information** section, enter/select the following details:

- **Name***: Enter a name for this integration.
- **Description**: Enter a description for the integration.
- **Implementation type**: Select the implementation type.
- **Data center***: From the dropdown list, from the list of applicable values, select the required data center.



NOTE: The data center selected here is used to map the AppViewX Cloud Connector for this integration.

7. In the **Vendor specific details** section, enter/select the following details:

- **API Key***: Unique identification number of the slot in the HSM Luna client that will be used to communicate with the end HSM device.
- **Key handler name***: A reference name to create a Master Encryption key in HSM. This enables us to pick the right MEK for crypto operations over KEK.
- **So file location***: The SO file is used to facilitate the communication between the HSM and AppViewX.

To upload the `.so` file:

- a. Click **Browse**.
- b. Navigate to the location of the `.so` file.
- c. Select the `.so` file and click **Open**.

- **Config file location**: The Config file is used to facilitate the communication between the HSM and AppViewX.

To upload the `.conf` file:

- a. Click **Browse**.
- b. Navigate to the location of the `.conf` file.
- c. Select the `.conf` file and click **Open**.

8. Click **Save**.

9. Scroll to the end of this page to view the table that will be populated with all the details of this HSM.

If the HSM has been configured correctly, the **Status** for the HSM will be set to **Available** (after checking the encryption and decryption logic).

If the **Status** is **Not Available**:

- Check the installation path for the HSM.
- Ensure that all required permissions have been enabled.

10. If the implementation type is **CSR Generation**, to generate the CSR, follow the steps given here:

- [Server certificate](#)
- [Client certificate](#)
- [Code signing certificate](#)

3.0 DOCUMENT INFORMATION

3.1 DOCUMENT LOCATION

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

<https://support.fortanix.com/hc/en-us/articles/7251592480148-Using-Fortanix-Data-Security-Manager-With-AppViewX-CLMaaS>

3.2 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

© 2016 – 2022 Fortanix, Inc. All Rights Reserved.

Fortanix® and the Fortanix logo are registered trademarks or trade names of Fortanix, Inc.

All other trademarks are the property of their respective owners.

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.