Fortanix®

User Guide

FORTANIX CONFIDENTIAL COMPUTING MANAGER –CREATE IMAGE

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 steps to create an application image in the Fortanix Confidential Computing Manager. The users are provided the ability to quickly and easily navigate the interface to run containerized applications accordingly.

A Fortanix Confidential Computing Manager (CCM) image is a particular software release or a version of an application. Each image is associated with one enclave hash (MRENCLAVE).

When an image is first created in Fortanix CCM, it is in an unapproved state. After configurable approval actions are taken, the image is considered approved. When an image is approved, Fortanix CCM knows that enclaves with the associated hash (MRENCLAVE) are trusted instances of the corresponding application, and will issue certs with the application's domain name(s) to those enclaves.

DOCUMENT IDENTIFICATION INFORMATION

DOCUMENT NAME	GUIDE, USER, CONFIDENTIAL COMPUTING MANAGER
DATE CREATED	14 MAY 2020
SECURITY CLASSIFICATION	For use by Fortanix internal and Fortanix Confidential Computing Manager Customers ONLY.

2.0 CONTACT INFORMATION

CONTACT INFORMATION

ITEM	PRIMARY	ALTERNATE
NAME	Fortanix	
EMAIL ADDRESS	Fortanix Support Link	
CONTACT NUMBER	N/A	
TITLE	N/A	
SUPPORT HOURS	8am – 5pm Monday – Friday	

3.0 DESCRIPTION OF SERVICES

3.1 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.

3.2 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.

3.3 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.

3.4 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.

4.0 CREATING AN IMAGE OF YOUR APPLICATION

You can use the Fortanix Confidential Computing Manager to create an image of your applications after you make changes.

Prerequisites:

- For Enclave OS application - the Tag of the Docker image for the application.
- For EDP application - The `sigstruct.bin` file which is used to register the enclave with Fortanix Confidential Computing Manager.

4.1 CREATE AN IMAGE OF ENCLAVE OS APPLICATIONS

1. After you create an Enclave OS application and click **NEXT**, you will see the **Add image** page where you have to configure the image of the Enclave OS application as shown in **Figure 2** below. You can also configure an application image from the detailed view of an application (**Figure 1**) using the **+IMAGES** button.

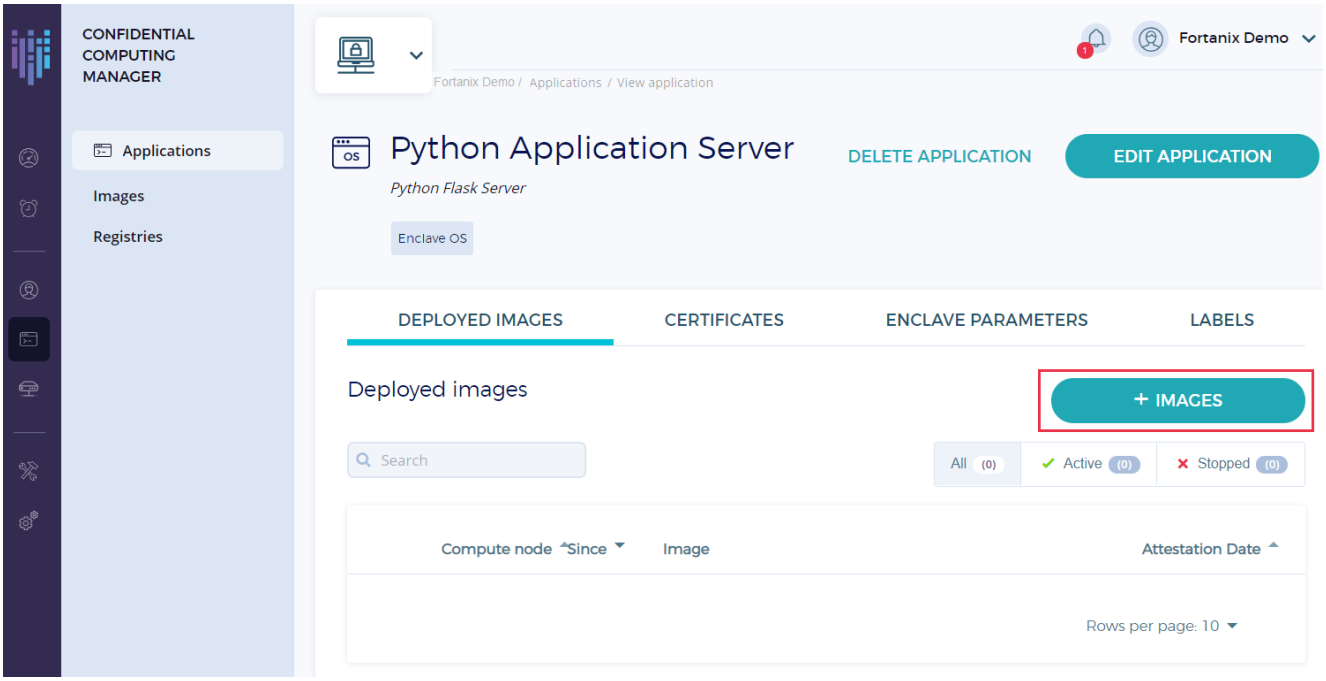

FIGURE 1: IMAGES TAB

2. In the **Add image** form, select the **Image Type** as **Intel SGX** or **AWS Nitro Enclaves** depending on the platform used.

3. Enter the **REGISTRY CREDENTIALS** for the **Output image name**. Here, the registry credentials are the credentials needed to access the private docker registry where the image will be pushed. Since the input image is stored in a public registry, there is no need to provide credentials for the input image.

    - If you have added a registry in a particular account as described in *in the article* *User's Guide: Image Registry*, then the check box **Use saved credentials** will be selected by default and the registry names for the output image will be filled automatically for the **Add Registry Credentials** fields.

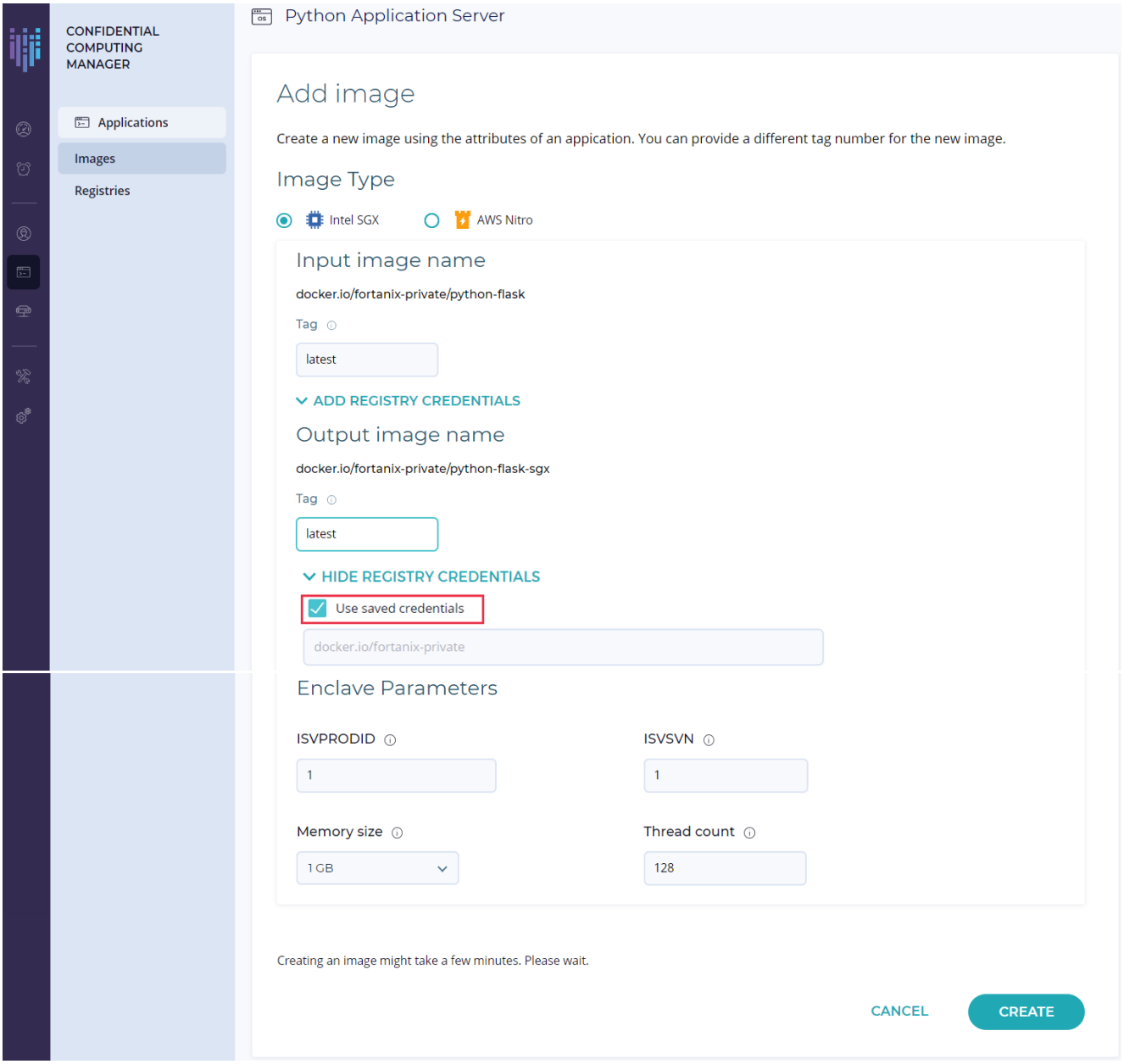

FIGURE 2: ADD SAVED REGISTRY CREDENTIALS

- If you have not saved any Registry Credentials, then manually enter the registry credentials for the **Output image name**.

4. Enter the image **Tag** which is the tag value of the Docker image.
5. If you selected the **Image Type** as **Intel SGX**, enter the following details:
    - **ISVPRODID** is a numeric product identifier. A user must choose a unique value in the range of 0-65535 for their applications.

- **ISVSVN** is a numeric security version to be assigned to the Enclave. This number should be incremented if security relevant change is made to the application.
- **Memory size** – Choose the memory size from the drop-down to change the memory size of the enclave.
- **Thread count** – Change the thread count to support the application.

If you selected the **Image Type** as **AWS Nitro**, enter the following details:

- **Memory size**
- **CPU count** - CPU count is the number of CPUs dedicated to an enclave out of all the CPUs available to the host machine.

NOTE: The Memory size and CPU count can be overridden at runtime with the following environment variables:

- `MEM_SIZE`
- `CPU_COUNT`

6. Click **CREATE** to create the image (**Figure 2**).
7. An image approval task is created and added which is visible on the **Tasks** page. You can approve the task to approve the application image. After it is approved, a green tick would appear in the **Approval status** column for that image.

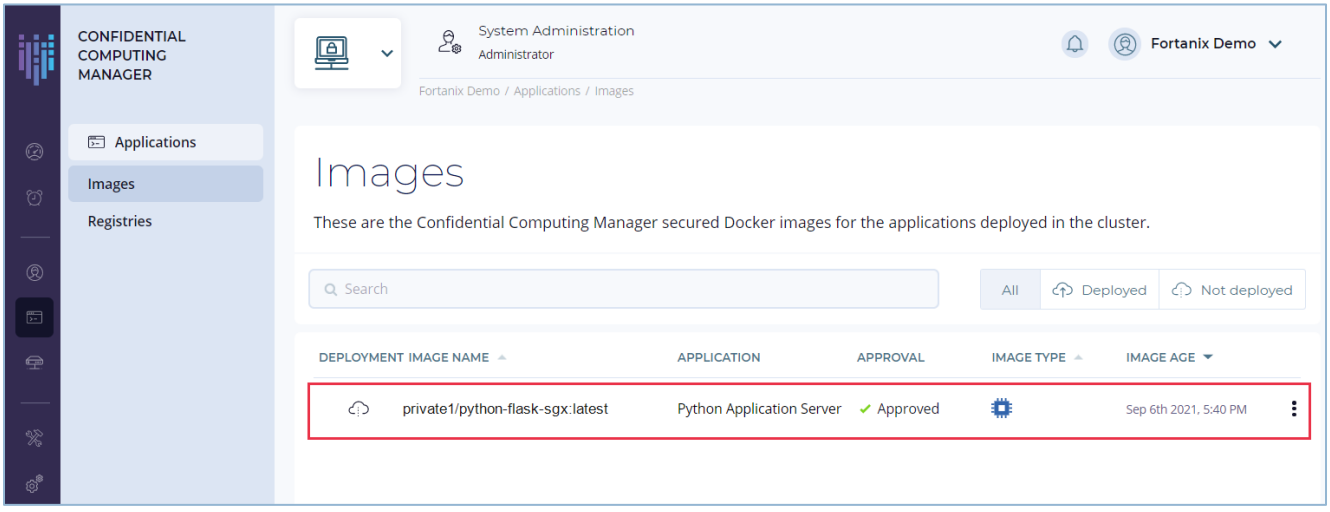

FIGURE 3: IMAGE CREATED AND APPROVED

NOTE: The Source Image tag and Output Image tag are optional fields and by default, the tag value is "latest" internally. If the user is entering a different tag value, then it can either be different values or the same. Once an image of an application is created, it will be pushed to the specified location in the **Output Image Name** of the application.

4.1.1 SGX1 AND SGX2 APPLICATION SUPPORT

When an application is converted, the converter app supports signing and running the application in both SGX1 and SGX2 hardware. After the application is converted, the application will have both SGX1 and SGX2 signatures, and the correct signature would be used depending on the hardware available.

The converted container will have two different MRENCLAVE values corresponding to SGX1 and SGX2 respectively. This allows you to run the same converted container on both SGX1 and SGX2 hardware.

On the hardware that supports dynamically adding pages to an enclave, pages for unallocated memory are not included in the initial enclave image, so the enclave can start faster. On hardware without that support, the initial enclave image includes zeroed pages for unallocated memory.

To view the MRENCLAVE values in the Fortanix CCM UI:

1. Go to the detailed view of an image, and select the **ENCLAVE** tab.
2. Notice the **MRENCLAVE (SGX1)** and **MRENCLAVE (SGX2)** fields under the **MRENCLAVE Values** section.

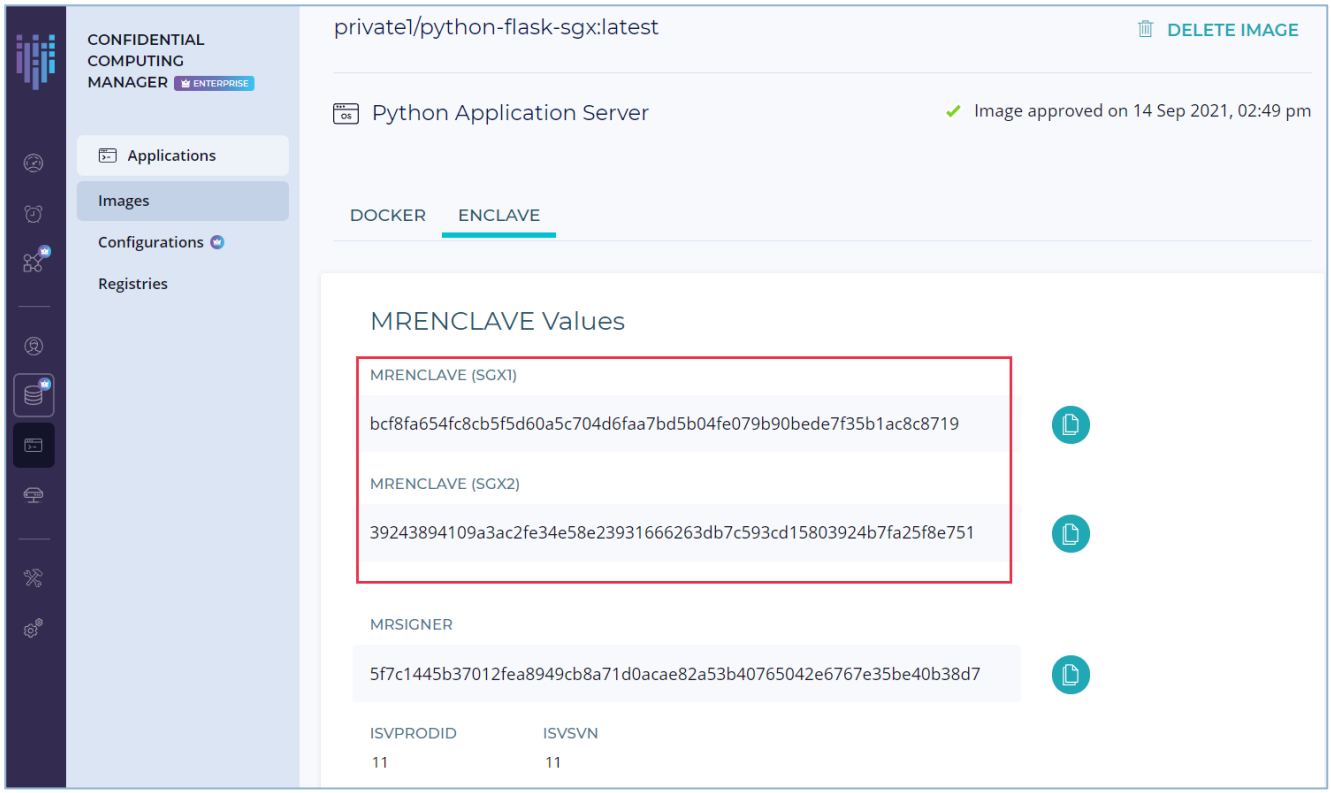

FIGURE 4: MRENCLAVE VALUES

4.2 CREATE AN IMAGE FOR EDP APPLICATIONS

1. After you create an EDP application and click **NEXT**, you will see the **Add image** page where you have to configure the image of the EDP application as shown in **Figure 5** below. You can also configure an application image from the detailed view of an application (**Figure 5**) using the **+IMAGES** button.

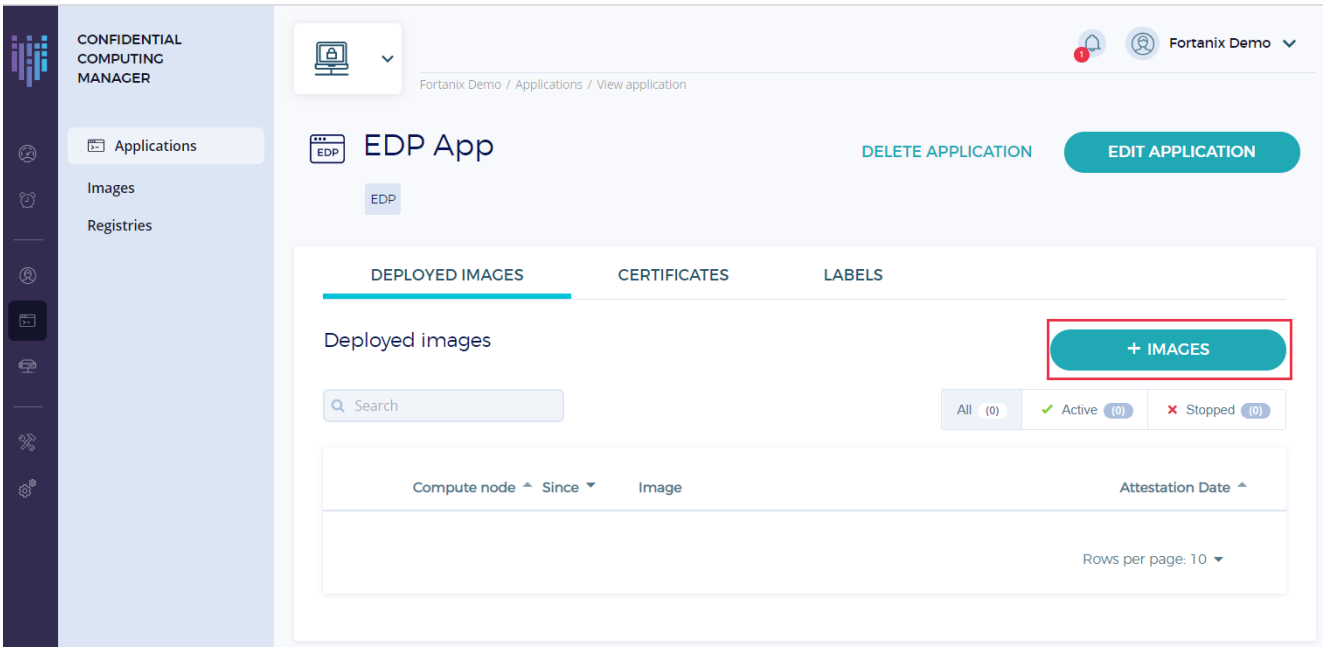

FIGURE 5: IMAGES TAB

2. In the **Add image** form, enter the **Image Version**.
3. In the **Image Type** section, select **Intel SGX** or **AWS Nitro Enclaves** as the platform.
4. If you select the Image Type as **Intel SGX**, you have to add the Sigstruct details. The SIGSTRUCT for an enclave is generated when an application is signed. It is used to register the enclave with Fortanix Confidential Computing Manager. In the **Enclave Configuration SIGSTRUCT** section, you will see three options to add SIGSTRUCT:

    a. **Upload Enclave SIGSTRUCT**: To upload an enclave `sigstruct.bin` file, click the **UPLOAD** button as shown in **Figure 6**. Here is a sample sigstruct.bin file.

    OR

    b. **Paste Base64-encoded Enclave SIGSTRUCT**: You can also paste a Base64-encoded SIGSTRUCT binary in the text box provided.

    OR

    c. **Enter Enclave SIGSTRUCT Parameters**: Enter the following parameters:

    - **MRENCLAVE**: This is the identity or hash of the enclave.
    - **MRSIGNER**: This is the identity of the signer of the enclave.

- **ISVPRODID**: This is the numeric product identifier to be assigned to the enclave. Choose a unique value in the range 0-65535 for each application.
- **ISVSVN**: This is the numeric security version to be assigned to the enclave. Increment this value when a security-relevant change is made to the application.

 **NOTE**: The **Enclave SIGSTRUCT Parameters** section is automatically filled when you either upload a **`sigstruct.bin`** file or paste a base64 encoded enclave SIGSTRUCT.

5. If you select the Image Type as **AWS Nitro Enclaves**, you have to add the Enclave Configuration JSON details which are unique enclave measurements that includes a series of Hashes and Platform. The JSON measurements for an enclave are generated when an application is signed. It is used to register the enclave with Fortanix Confidential Computing Manager. In the **Enclave Configuration JSON** section, you will see three options to add measurements:

   a. **Upload Measurement JSON**: To upload an enclave **`measurement.json`** file, click the **UPLOAD** button as shown in **Figure 7**.

   OR

   b. **Paste Measurement JSON**: You can also paste the JSON enclave measurements in the text box provided.

   OR

   c. **Enter Measurement**: Enter the following parameters:

      - **PCR0**: This is the hash of the enclave image file.
      - **PCR1**: This is the hash of the Linux kernel and bootstrap.
      - **PCR2**: This is the Hash of the user application.

       **NOTE**: The **Enter Measurement** section is automatically filled when you either upload a **`measurement.json`** file or paste the JSON enclave measurements.

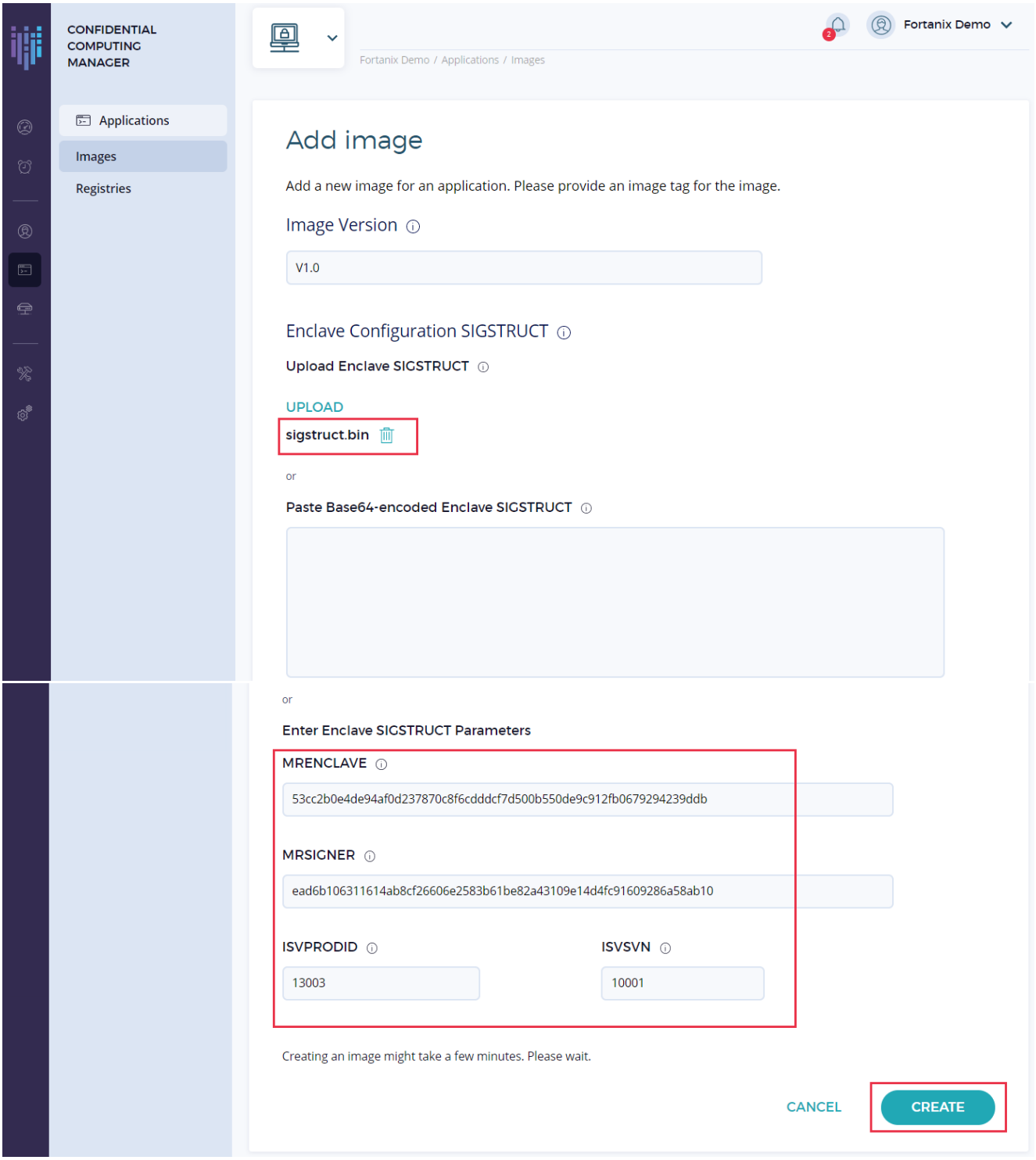

FIGURE 6: CREATE AN EDP APPLICATION IMAGE FOR INTEL SGX PLATFORM

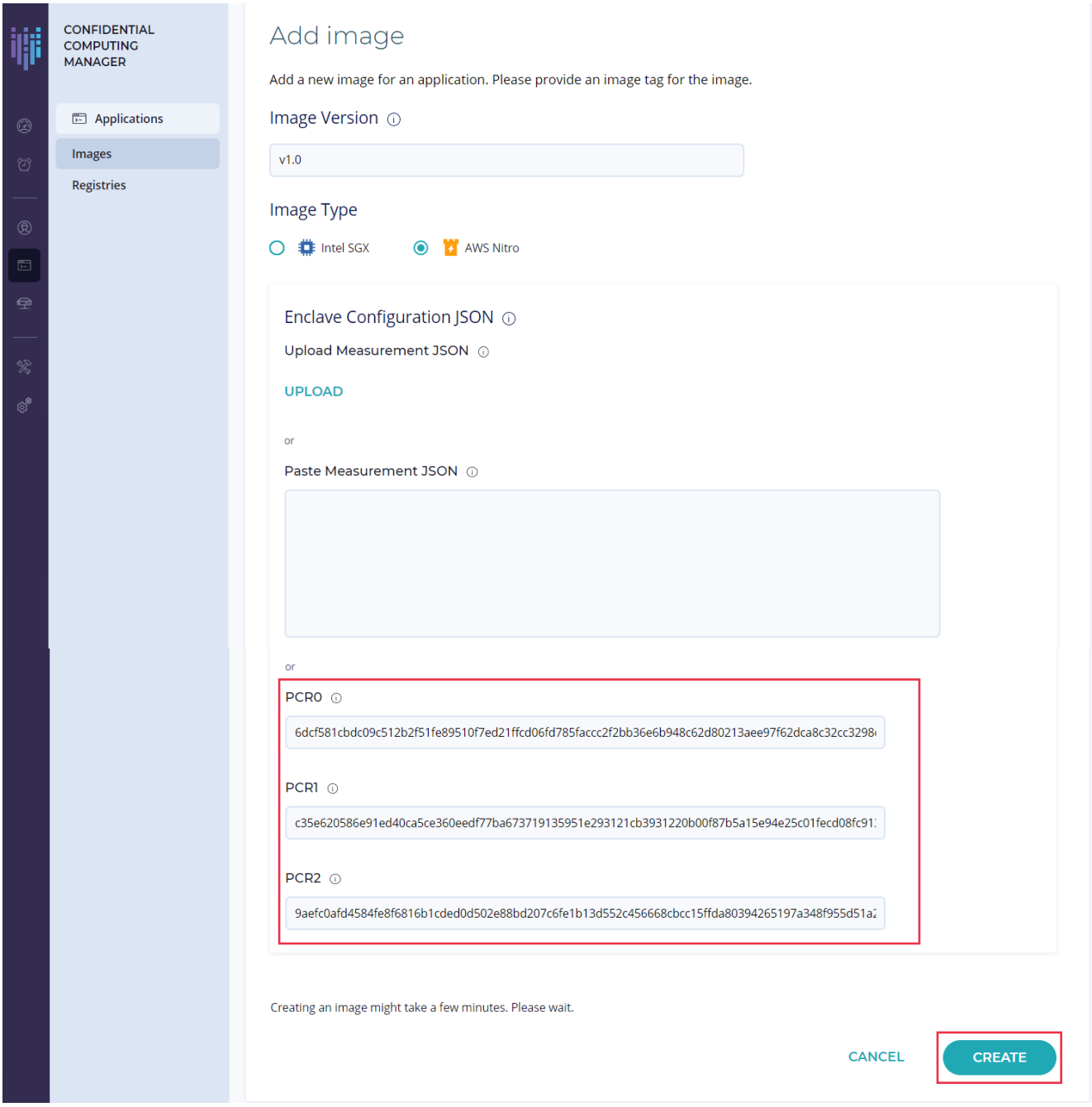

FIGURE 7: CREATE AN EDP APPLICATION FOR AWS NITRO PLATFORM

6. Click **CREATE** to create the EDP application image.
7. An image approval task is created and added which is visible on the **Tasks** page. You can approve the task to approve the image.

8. After the image is approved, a green tick would appear in the **Approval status** column for that image.

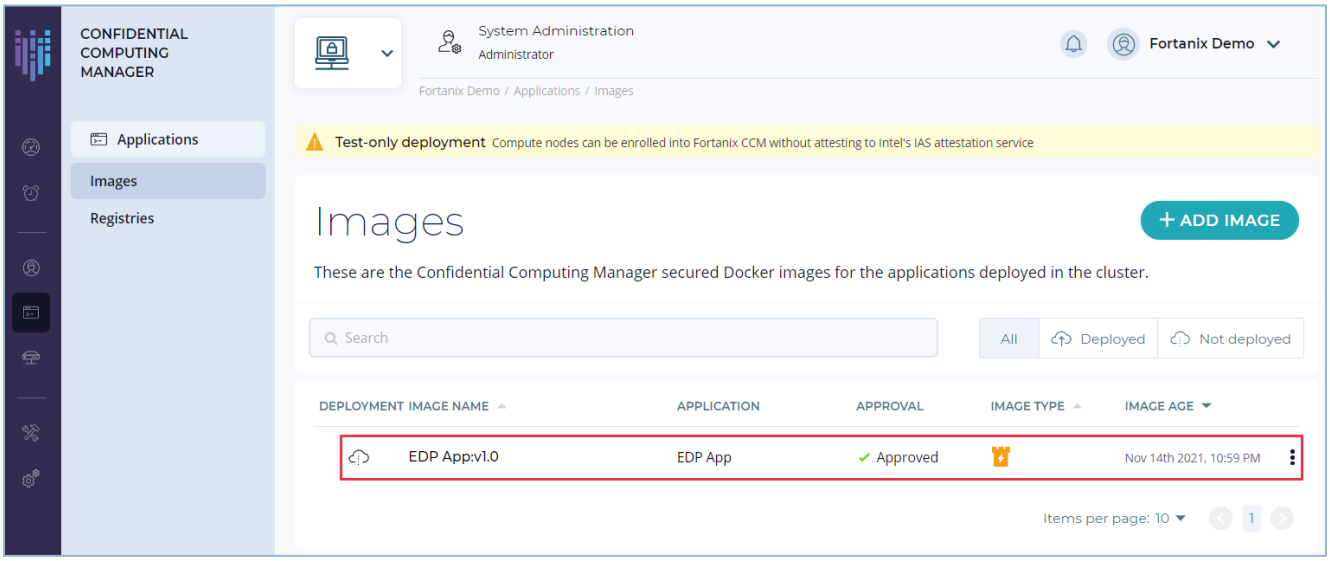

FIGURE 8: IMAGE CREATED AND APPROVED

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/360043529411-User-s-Guide-Create-an-Image

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