USER GUIDE

FORTANIX ENCLAVE MANAGER SAAS

Fortanix®

TABLE OF CONTENTS

1.0 INTRODUCTION

Welcome to the Fortanix Enclave Manager User Guide. This document serves as a centralized repository for all operations related to Fortanix Enclave Manager, FAQs and supporting documents that are associated with the usage of this service. The users are provided the ability to quickly and easily navigate the Fortanix Enclave Manager interface to run containerized applications accordingly.

This document contains the information that a Fortanix Enclave Manager user needs to:

- Log in to Fortanix Enclave Manager
- Create an account
- Add an application
- Create an application image
- Whitelist the application's domain
- Whitelist the image
- Convert an application image
- Add users

DOCUMENT IDENTIFICATION INFORMATION

DOCUMENT NAME	GUIDE, USER, ENCLAVE MANAGER
DATE CREATED	14 MAY 2020
SECURITY CLASSIFICATION	For use by Fortanix internal and Fortanix Enclave 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

FORTANIX ENCLAVE MANAGER

Fortanix Enclave Manager provides ‘data-in-use’ protection for your container workloads. It leverages 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.

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.

INTEL ATTESTATION AND WHY IT IS REQUIRED

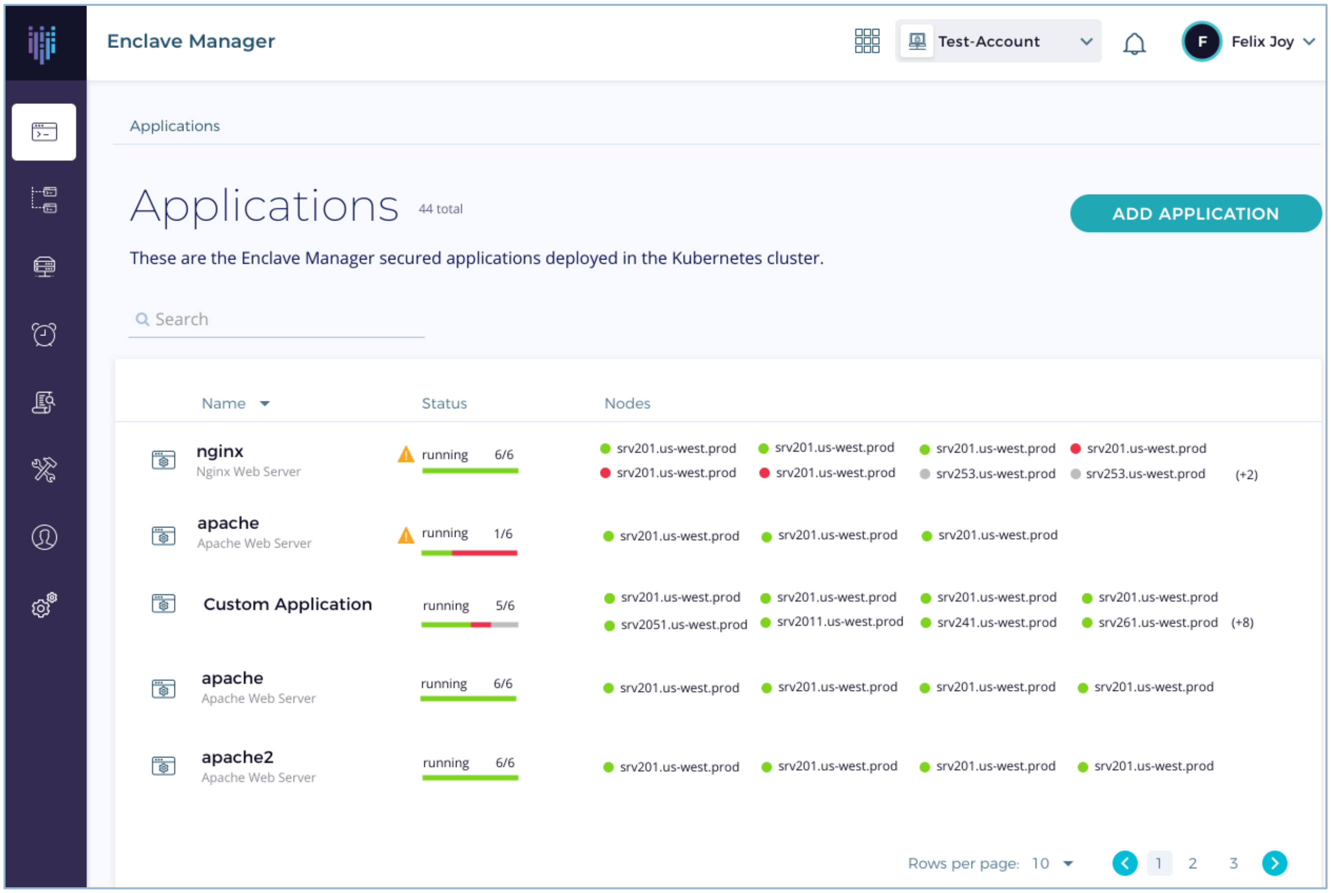
Since enclaves are instantiated on platforms by untrusted code, before enclaves are provisioned with application confidential information, it is essential to be able to confirm that the desired enclave was correctly instantiated on a platform protected by Intel SGX. This is done by a remote attestation 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.

4.0 TERMINOLOGY REFERENCES

- **ISVPRODID** – Numeric product identifier to be assigned to the enclave
- **ISVSVN** – Numeric security version to be assigned to the enclave

5.0 GRAPHICAL USER INTERFACE

The Fortanix Enclave Manager **Applications** screen shown in **Figure 1** is the main workspace which is the landing page for adding an application using the **Add application** form shown in **Figure 2**. The **Add application** page is used to add the details of an application that will be deployed in the cluster. These attributes will be used to create secure images of the application which will eventually get deployed on the cluster.

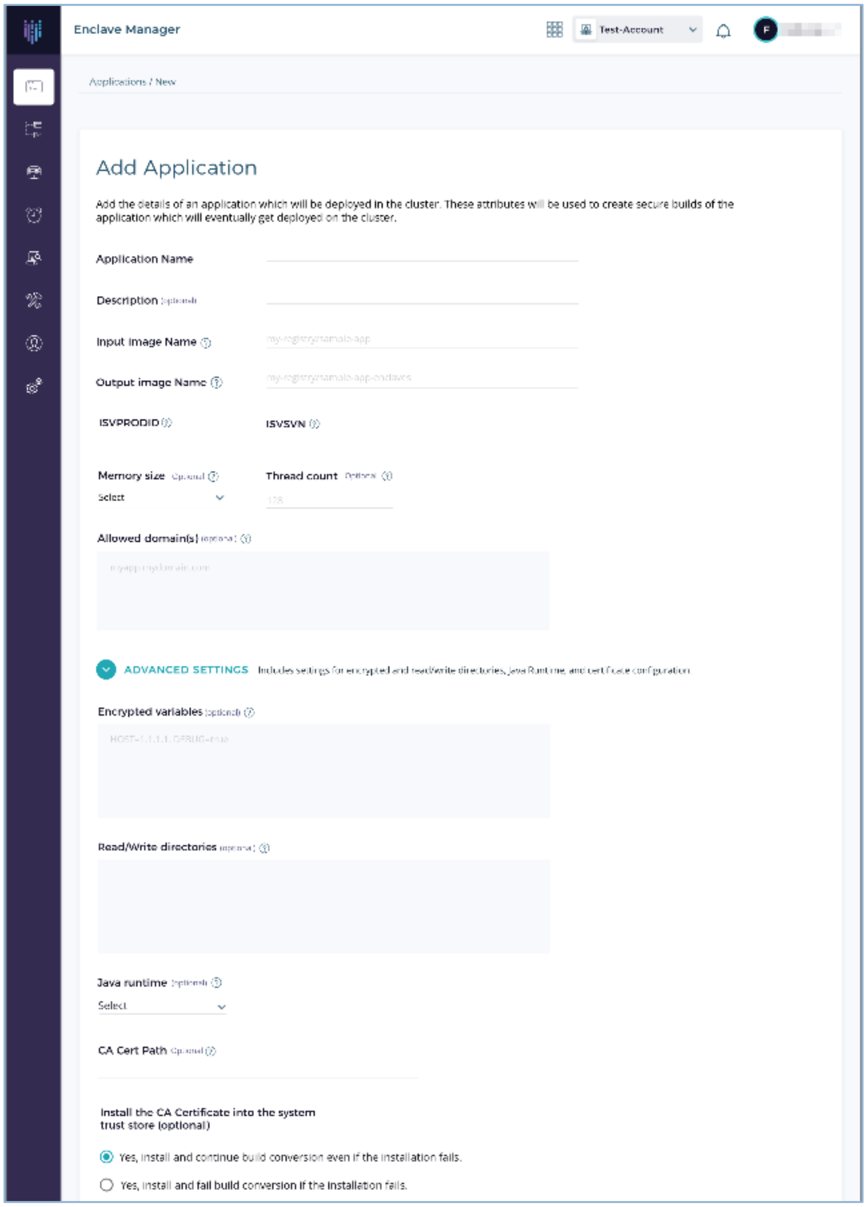


Applications 44 total

These are the Enclave Manager secured applications deployed in the Kubernetes cluster.

Name	Status	Nodes
nginx Nginx Web Server	⚠ running 6/6	● srv201.us-west.prod ● srv201.us-west.prod ● srv201.us-west.prod ● srv201.us-west.prod ● srv201.us-west.prod ● srv201.us-west.prod ● srv253.us-west.prod ● srv253.us-west.prod (+2)
apache Apache Web Server	⚠ running 1/6	● srv201.us-west.prod ● srv201.us-west.prod ● srv201.us-west.prod
Custom Application	running 5/6	● srv201.us-west.prod ● srv201.us-west.prod ● srv201.us-west.prod ● srv201.us-west.prod ● srv2051.us-west.prod ● srv2011.us-west.prod ● srv241.us-west.prod ● srv261.us-west.prod (+8)
apache Apache Web Server	running 6/6	● srv201.us-west.prod ● srv201.us-west.prod ● srv201.us-west.prod ● srv201.us-west.prod
apache2 Apache Web Server	running 6/6	● srv201.us-west.prod ● srv201.us-west.prod ● srv201.us-west.prod ● srv201.us-west.prod

FIGURE 1: APPLICATIONS PAGE



Enclave Manager

Test-Account

F [redacted]

Applications / New

Add Application

Add the details of an application which will be deployed in the cluster. These attributes will be used to create secure builds of the application which will eventually get deployed on the cluster.

Application Name

Description (optional)

Input Image Name ⓘ my-registry/sample-app

Output image Name ⓘ my-registry/sample-app-enclave

ISVPRODID ⓘ

ISVSVN ⓘ

Memory size Optional ⓘ Select

Thread count Optional ⓘ 128

Allowed domain(s) (optional) ⓘ myapp.mydomain.com

ADVANCED SETTINGS Includes settings for encrypted and read/write directories, Java Runtime, and certificate configuration

Encrypted variables (optional) ⓘ HOST=1.1.1.1, DEBUG=true

Read/Write directories (optional) ⓘ

Java runtime (optional) ⓘ Select

CA Cert Path Optional ⓘ

Install the CA Certificate into the system trust store (optional)

● Yes, install and continue build conversion even if the installation fails.

○ Yes, install and fail build conversion if the installation fails.

FIGURE 2: ADD APPLICATION PAGE

NAVIGATION BUTTONS

The Navigation buttons for Fortanix Enclave Manager are located on the left panel of the GUI and identify the screen functionality. The following table illustrates button functions:

NAVIGATION BUTTONS

BUTTON	FUNCTIONALITY
COMPUTE NODES	Click this button 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 Enclave Manager components are running.
APPLICTIONS	Click this button to see all the Fortanix Enclave 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.
IMAGES	Click this button to see all the Fortanix Enclave Manager secured Docker images for the applications deployed on the cluster.
AUDIT LOGS	Click this button to see all the important events happening across the cluster. Type of events include user logins, node enrollments, certificate issuance, and failures.
TASKS	Click this button to see all the requests that need Administrator approval. For example, node enrolment, application domain whitelist, 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 Enclave Manager. The Users page also allows you to edit the properties of a user and add new users.

6.0 WORKING IN ENCLAVE MANAGER - ADMINISTRATION

In the Fortanix Enclave Manager, you can perform administration tasks such as signing up, logging in, creating account, managing your app deployment, assign access, and handle whitelist requests. You can also view the nodes in your cluster and their attestation status, tasks, and audit logs of cluster events. To get started, sign up.

SIGN UP

Steps:

1. Open the Fortanix Enclave Manager Sign in page from the Fortanix product portal.
2. Click the **SIGN UP** button on the top-right corner of the page.

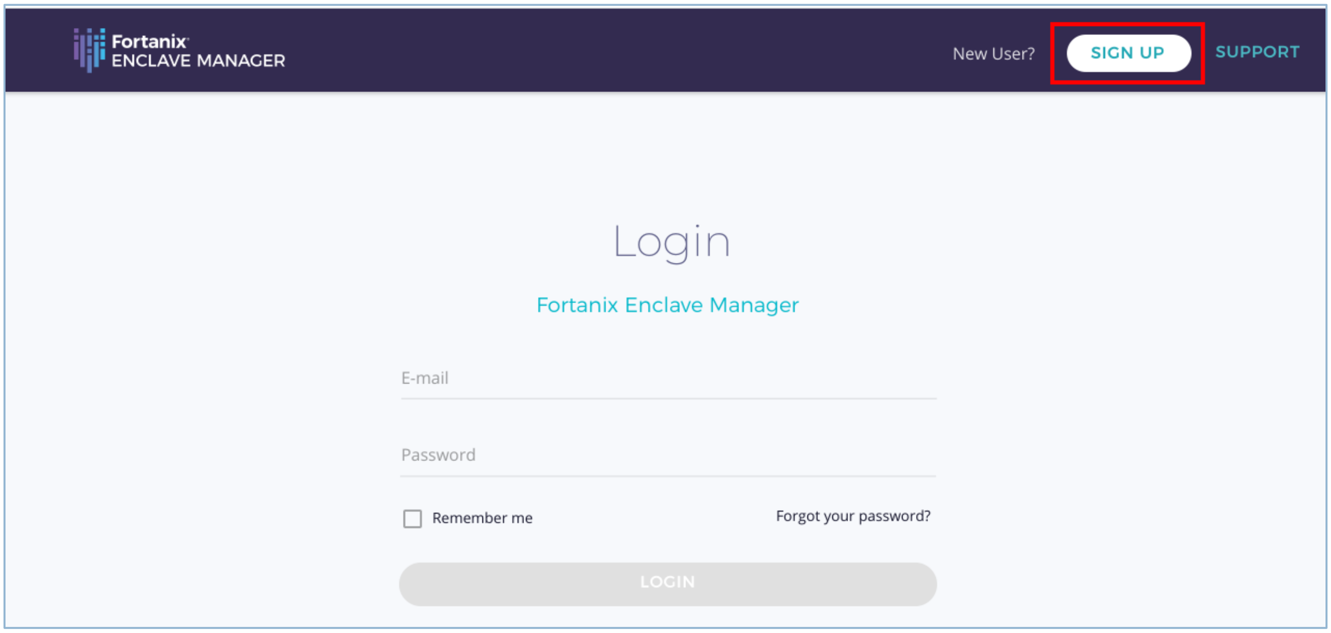


FIGURE 3: SIGN UP

3. Fill the Sign Up form and enter the necessary details such as **Email**, **First name**, **Last name**, **Create password**, **Retype password**.

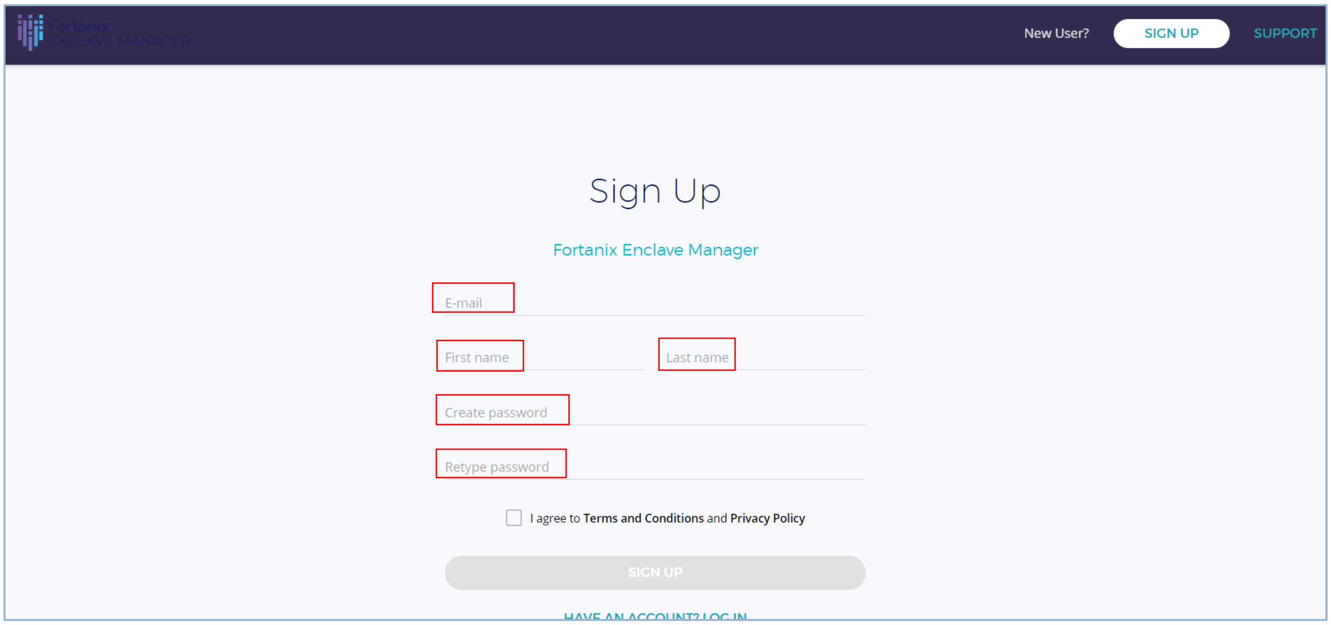
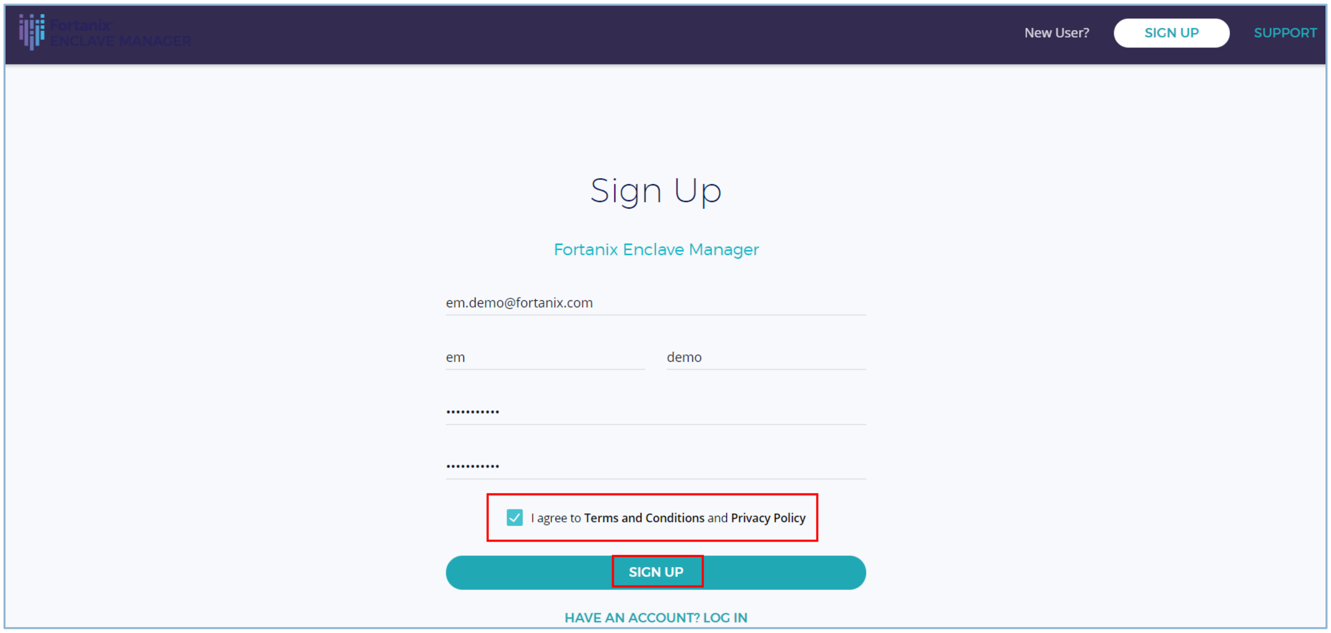


FIGURE 4: SIGN UP FORM

NOTE: The minimum password length required is 8 characters (letters, numbers, !, %,$)

4. Select the check box "**I agree to Terms and Conditions and Privacy Policy**" and click **SIGN UP**.



Sign Up

Fortanix Enclave Manager

em.demo@fortanix.com

em demo

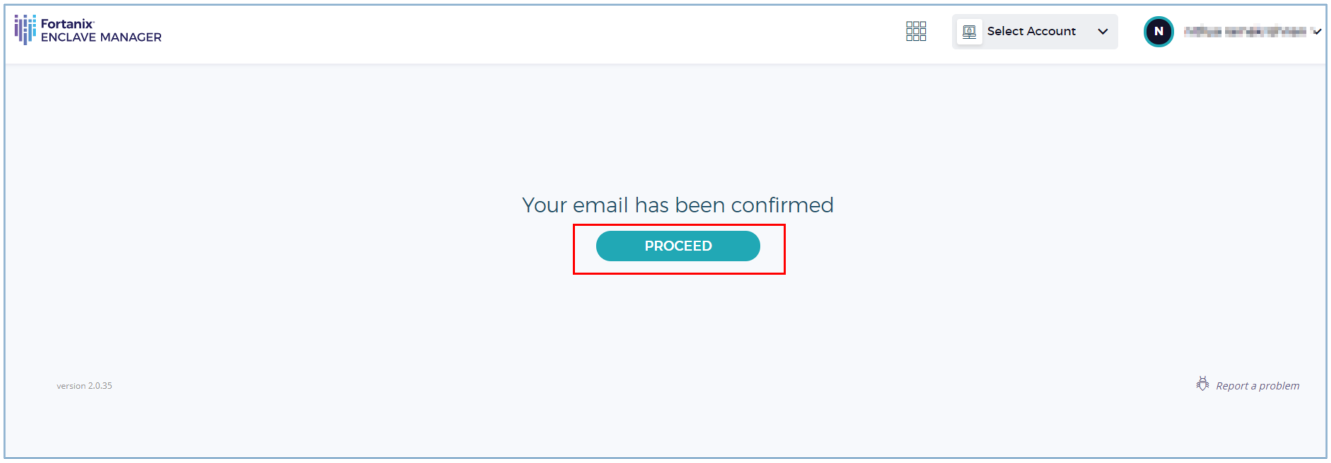
•••••••••••

•••••••••••

☑ I agree to Terms and Conditions and Privacy Policy

FIGURE 5: SIGN UP

5. Once you sign up, the administrator will receive an email to approve this request. After the administrator approves it, you will receive an email notification regarding the approval of the request.
6. You will also review an email to verify your email address. Click **CONFIRM EMAIL** in the email to verify your email. You will be redirected to the Enclave Manager UI. Click **PROCEED** in the Enclave Manager UI.



[redacted]

Your email has been confirmed

FIGURE 6: EMAIL CONFIRMED

7. After signing up, the user can log in successfully to Enclave Manager.

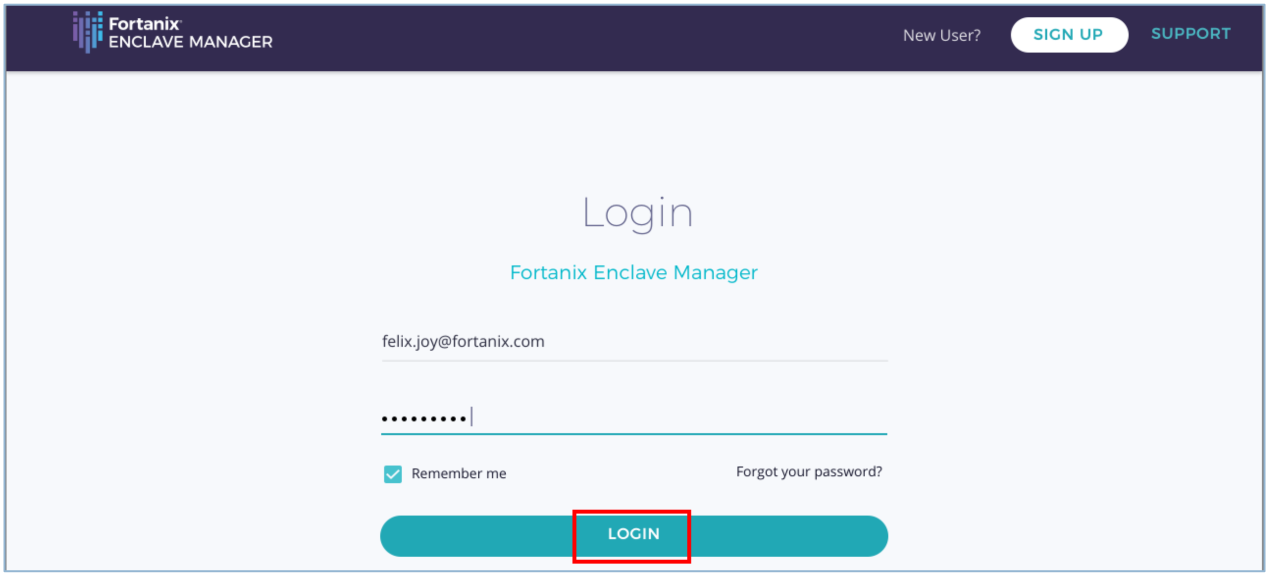
LOG IN

Prerequisites:

- Fortanix Enclave Manager account.
- A user added in Fortanix Enclave Manager with relevant permissions to access the functionality of this service.

Steps:

1. Open the Fortanix Enclave Manager Sign in page from the Fortanix product portal.
2. Enter your **E-mail** and **Password**.
3. Click **LOG IN** to log in to Fortanix Enclave Manager.



felix.joy@fortanix.com

•••••••••

☑ Remember me

FIGURE 7: LOGGING IN

4. Once you log in, create an account using the Enclave Manager Accounts page.

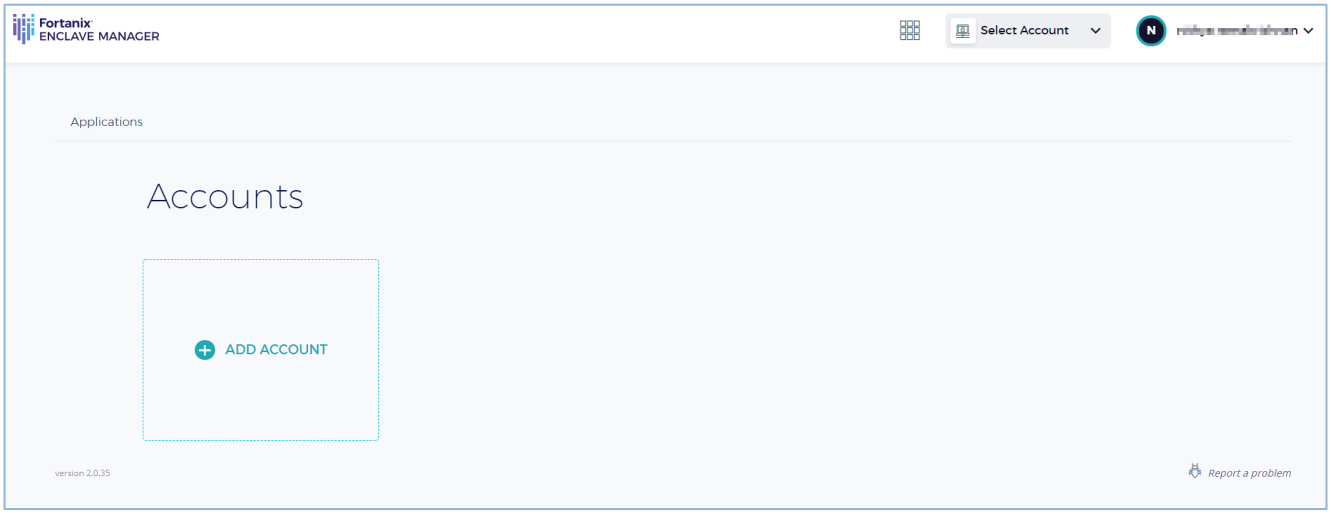


FIGURE 8: ACCOUNTS PAGE

To create an account, *refer to the "***Create Account***" section below.*

CHANGE PASSWORD

Steps:

1. In the Enclave Manager UI, click the drop-down menu associated with the user name on the top-right of the UI.
2. From the menu, click **My profile**.

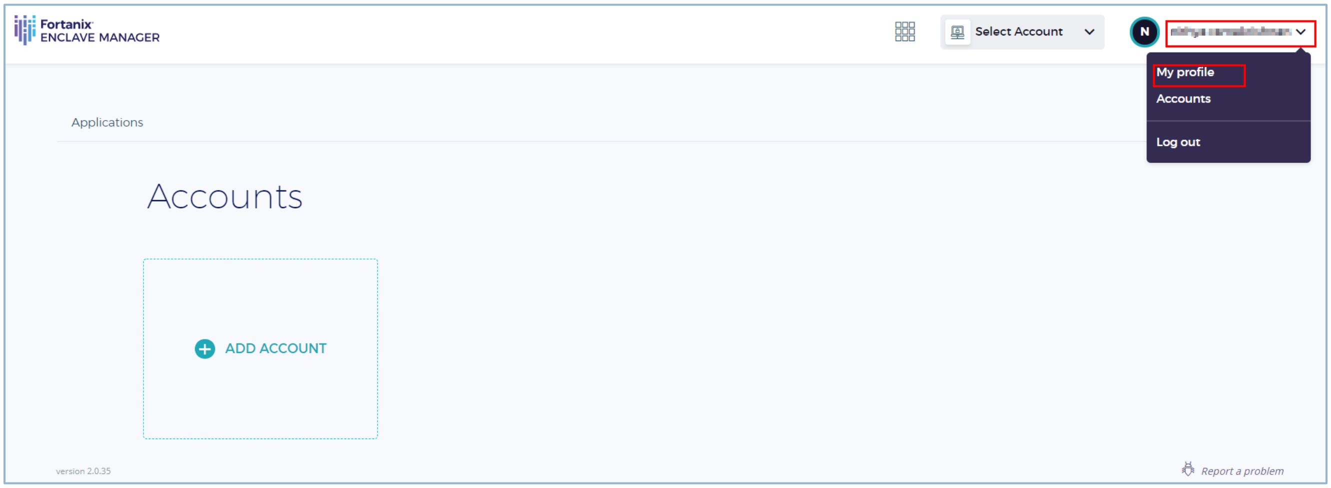
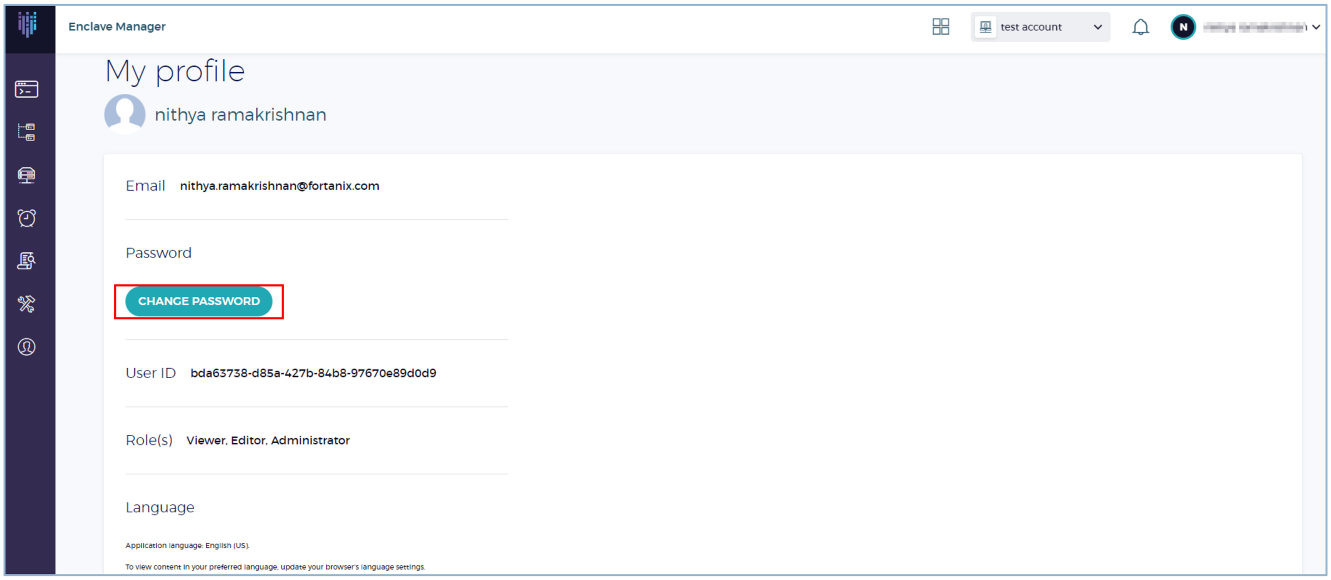


FIGURE 9: MY PROFILE

3. In the **My profile** page, click the **CHANGE PASSWORD** button.



Enclave Manager

test account

N [redacted]

My profile

nithya ramakrishnan

Email nithya.ramakrishnan@fortanix.com

Password

CHANGE PASSWORD

User ID bda63738-d85a-427b-84b8-97670e89d0d9

Role(s) Viewer, Editor, Administrator

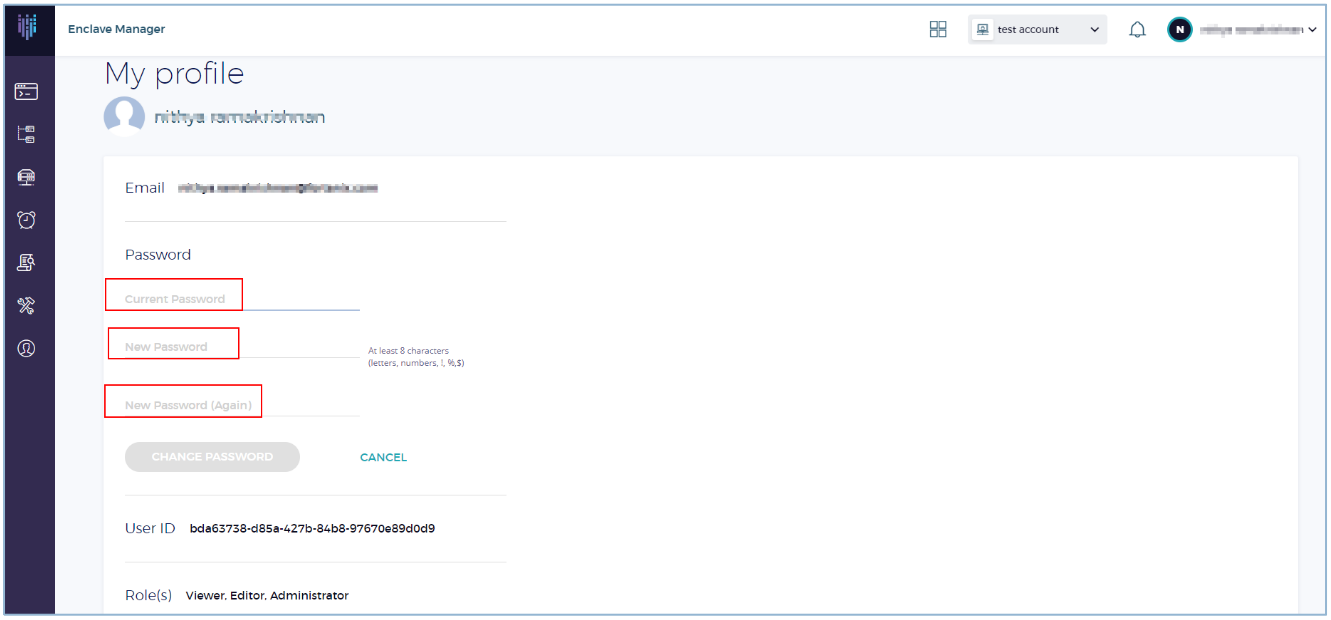
Language

Application language: English (US).

To view content in your preferred language, update your browser's language settings.

FIGURE 10: CHANGE PASSWORD

4. Enter the **Current Password** and type the **New Password** two times.



Enclave Manager

test account

N [redacted]

My profile

[redacted]

Email [redacted]

Password

Current Password

New Password

At least 8 characters (letters, numbers, !, %,$)

New Password (Again)

CHANGE PASSWORD

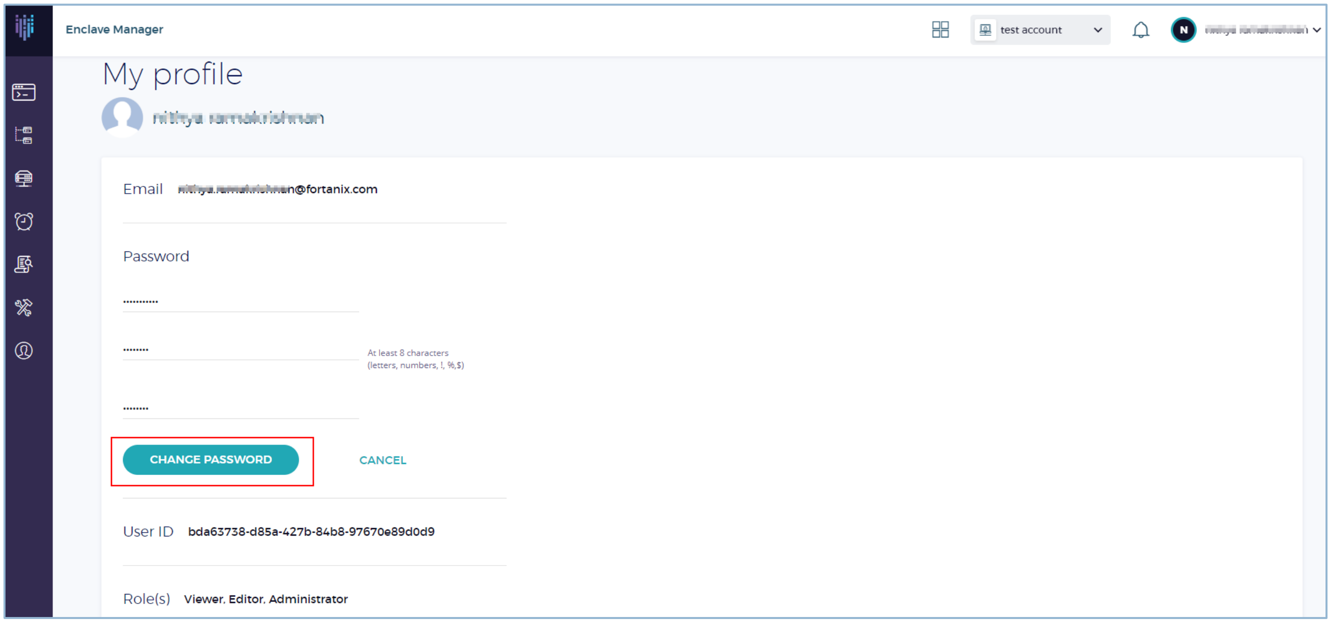
CANCEL

User ID bda63738-d85a-427b-84b8-97670e89d0d9

Role(s) Viewer, Editor, Administrator

FIGURE 11: NEW PASSWORD

5. Click **CHANGE PASSWORD** button to save changes.



Enclave Manager

test account

N [redacted]

My profile

[redacted]

Email [redacted]@fortanix.com

Password

....

.... At least 8 characters (letters, numbers, !, %, $)

....

CHANGE PASSWORD CANCEL

User ID bda63738-d85a-427b-84b8-97670e89d0d9

Role(s) Viewer, Editor, Administrator

FIGURE 12: NEW PASSWORD SAVED

CREATE AN ACCOUNT

An Enclave Manage account is the top-level container for applications, images, and nodes. An account is generally associated with an organization, rather than an individual. Different accounts are fully isolated from each other. A user can either create a new account or join an existing account. To join an account, an administrator of an account needs to invite a user using the user's email address using the **Invite User** workflow explained in the next section. So, the user needs to contact the account administrator to join an existing account. Upon accepting the invitation to join the account, the user will be added to it.

Prerequisites: You need to be an account administrator of the account.

Steps:

1. Once you sign up and log in, you will be taken to the **Accounts** page. Click **ADD ACCOUNT** to create a new account.

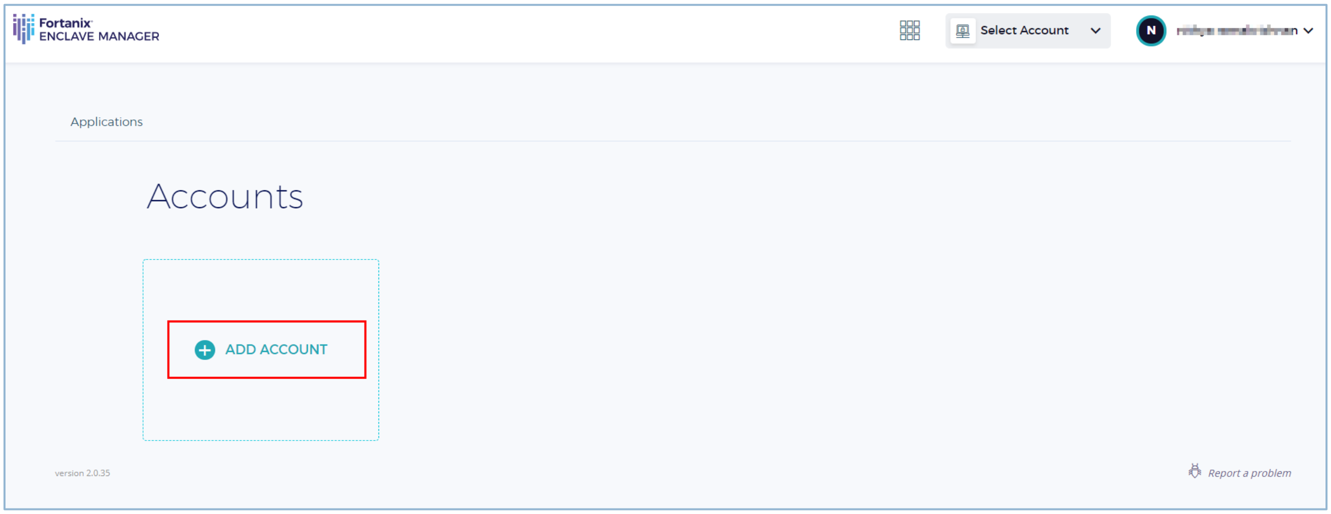
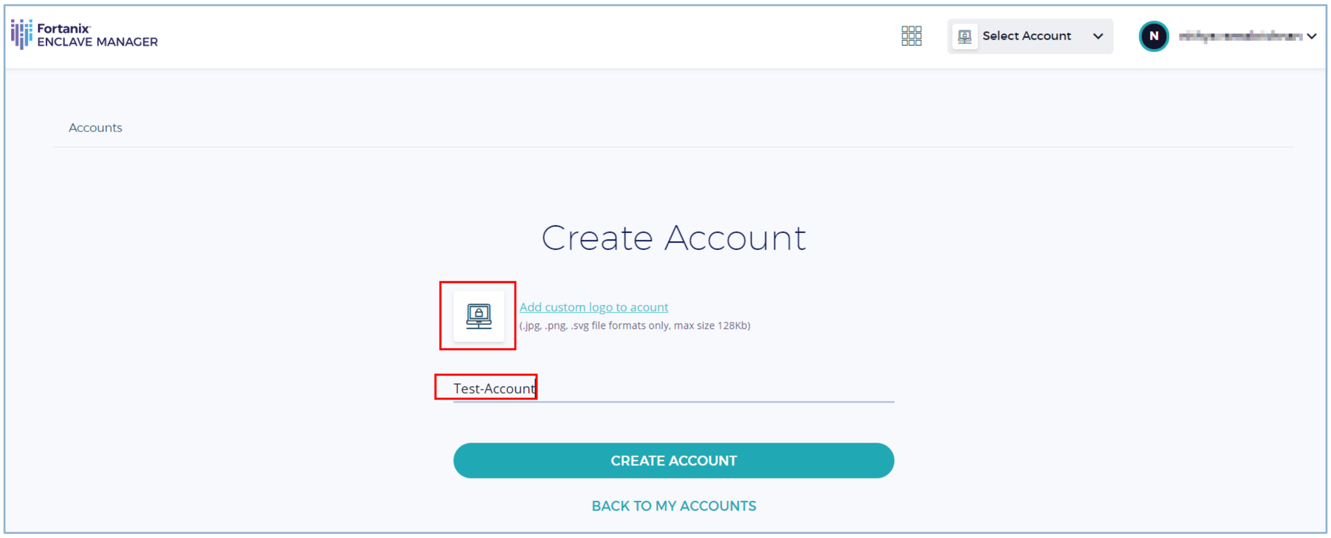


FIGURE 13: CREATE A NEW ACCOUNT

2. Enter a name for the new account and optionally add a custom logo for the account. Click **CREATE ACCOUNT** to complete the account creation.



Test-Account

FIGURE 14: CREATE ACCOUNT COMPLETE

3. The account is now successfully created.

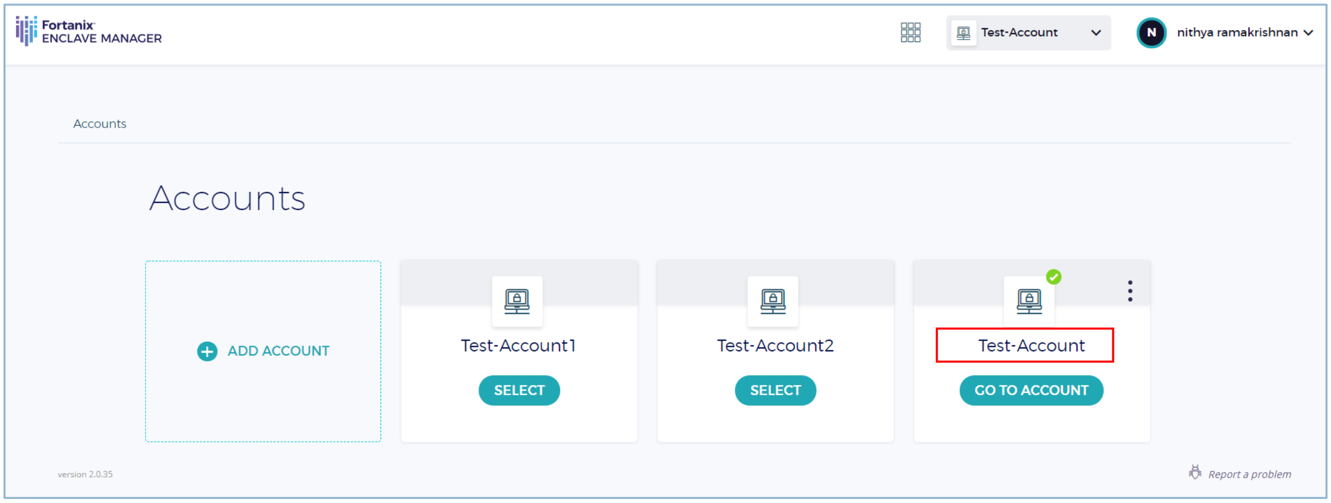


FIGURE 15: ACCOUNT CREATED SUCCESSFULLY

4. Click **SELECT** to select the newly created account. Click **GO TO ACCOUNT** to enter the account and start enrolling nodes and creating applications.

NOTE: The account name and logo can be updated using the **CUSTOMIZE ACCOUNT** option on the accounts page.

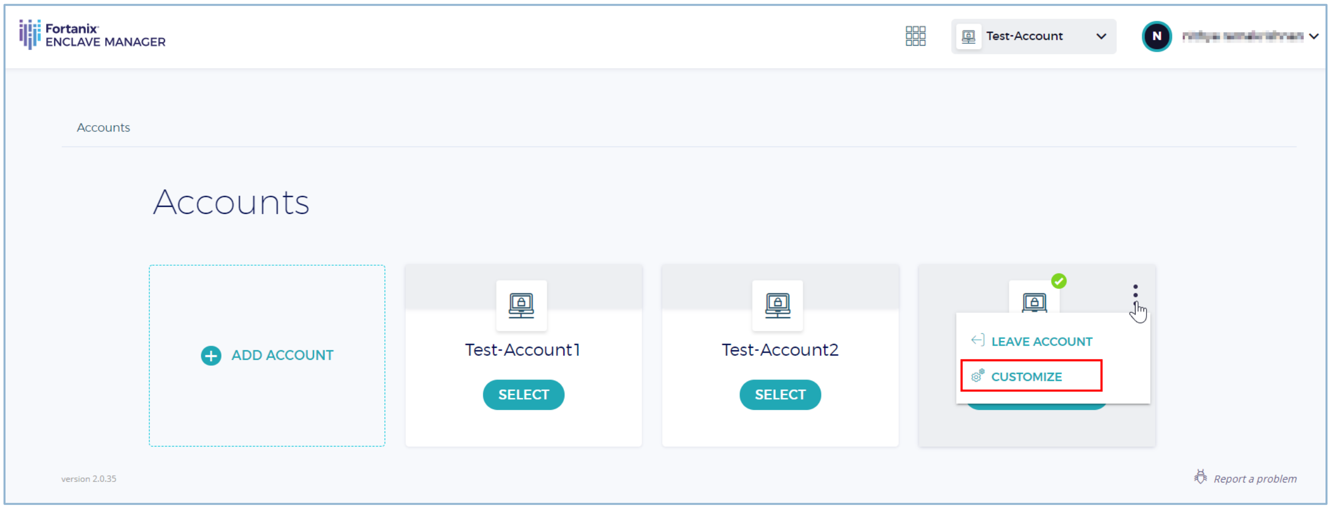


FIGURE 16: CUSTOMIZE ACCOUNT

LEAVE AN ACCOUNT

A user also has the option to leave an account.

To leave an account:

1. Click the three-dotted vertical line on the account.

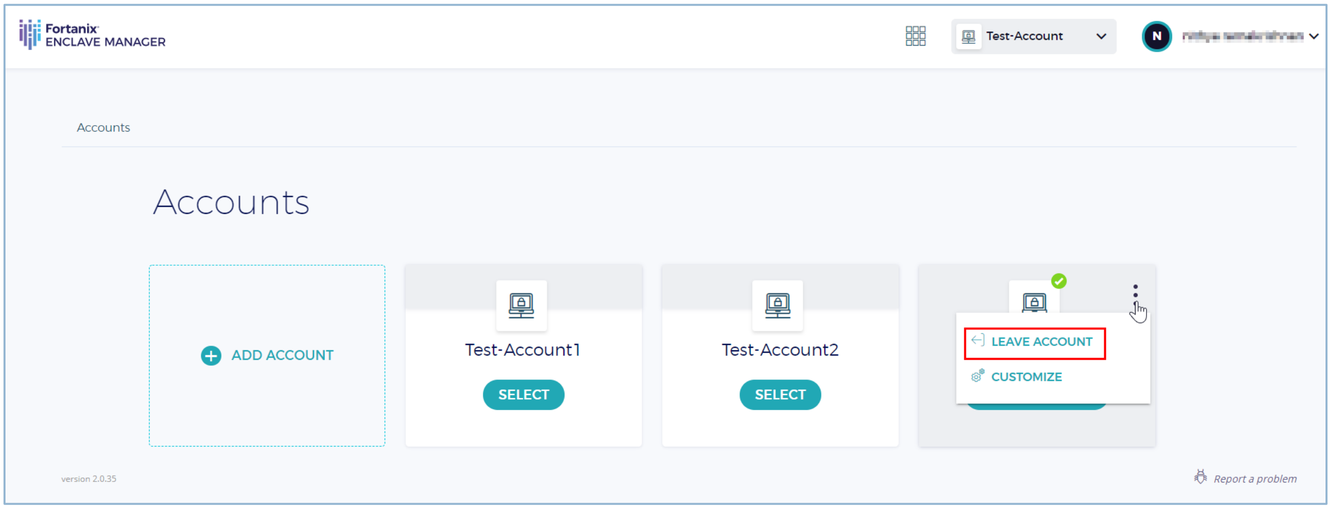


FIGURE 17: LEAVE AN ACCOUNT

2. Click **LEAVE ACCOUNT** to leave an account that you had previously joined.

NOTE:

- To leave an account, you have to be a user with editor or viewer role. If you are an administrator of an account, then to leave an account you have to ensure that there is one more user in the account with an administrator role. If you are the only admin of an account, then you can choose to delete the account instead.

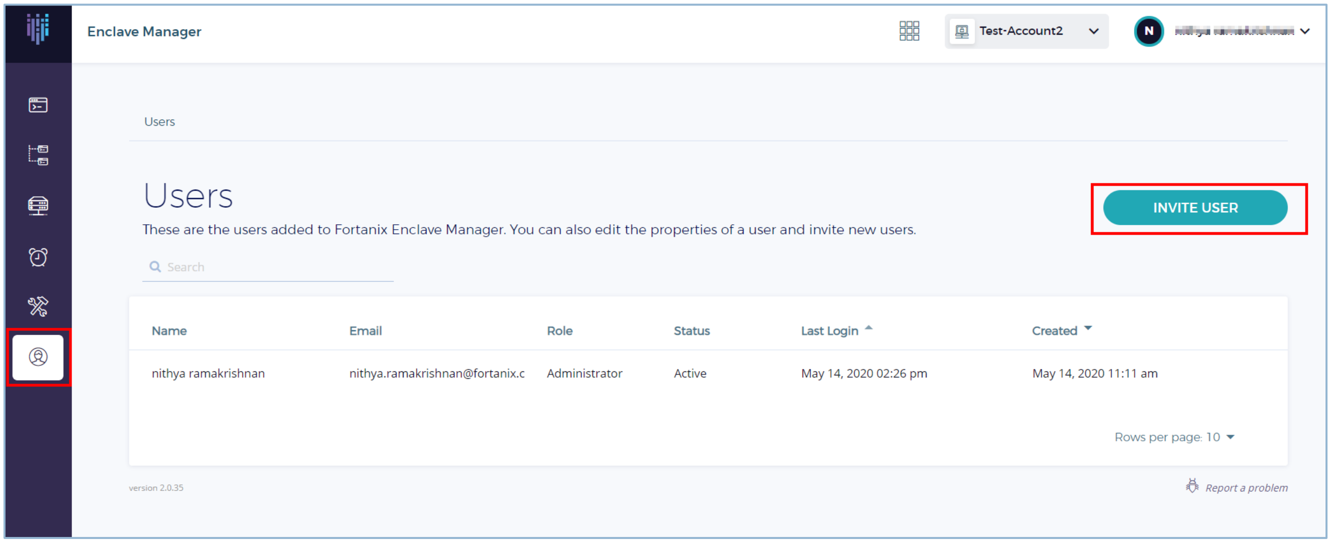
INVITE A USER

Prerequisites:

- Email id of the user is required.
- You need to be an account administrator to invite a user to an account.

Steps:

1. Open the **Users** tab in the Fortanix Enclave Manager UI to see the list of all users added to Fortanix Enclave Manager.
2. Click **INVITE USER** to add a new user to this account.



Users

These are the users added to Fortanix Enclave Manager. You can also edit the properties of a user and invite new users.

Name	Email	Role	Status	Last Login	Created
nithya ramakrishnan	nithya.ramakrishnan@fortanix.c	Administrator	Active	May 14, 2020 02:26 pm	May 14, 2020 11:11 am

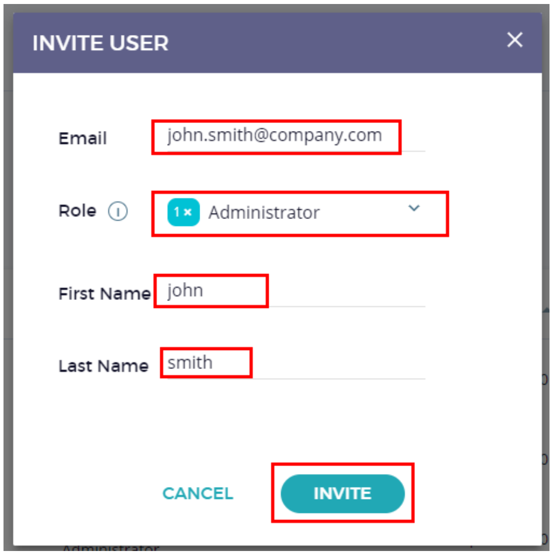
Rows per page: 10

version 2.0.35

Report a problem

FIGURE 18: USERS TAB AND INVITE USER

3. Fill all the required fields:



Email: john.smith@company.com

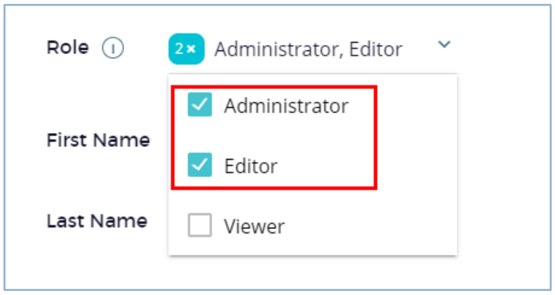
Role: 1 × Administrator

First Name: john

Last Name: smith

FIGURE 19: ADD USER FORM

- **Email** (user's email) – Email of the user, the email is case-insensitive.
- **Role** – Choose the role(s) for this user.



Role ⓘ 2 × Administrator, Editor

☑ Administrator

☑ Editor

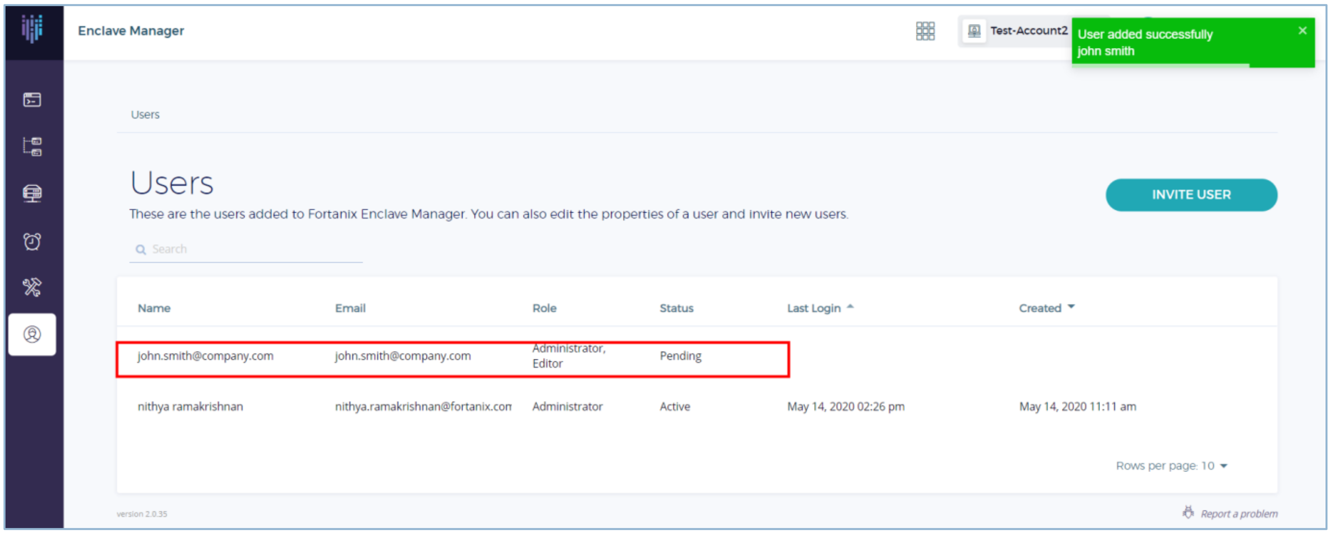
□ Viewer

FIGURE 20: CHOOSE ROLES

Optional fields:

- **First Name** – Enter the user's first name.
- **Last Name** – Enter the user's last name.

4. Click **Invite** (**Figure 19**), to invite the user. The invited user will get an email to join this account.



User added successfully
john smith

Users

These are the users added to Fortanix Enclave Manager. You can also edit the properties of a user and invite new users.

Name	Email	Role	Status	Last Login	Created
john.smith@company.com	john.smith@company.com	Administrator, Editor	Pending		
nithya ramakrishnan	nithya.ramakrishnan@fortanix.con	Administrator	Active	May 14, 2020 02:26 pm	May 14, 2020 11:11 am

Rows per page: 10

version 2.0.35

FIGURE 21: USER INVITED

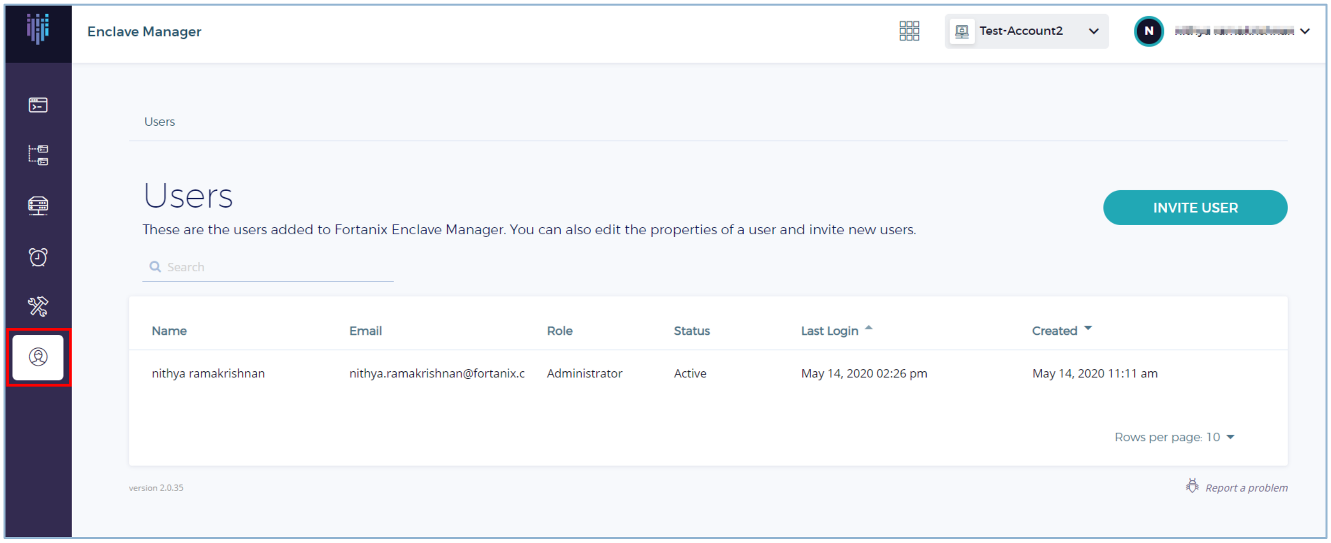
EDIT A USER

Prerequisites: An existing user.

Steps:

As an administrator of an account, you can edit another user's role. To do this:

1. Click the **Users** tab in the Fortanix Enclave Manager UI.



Users

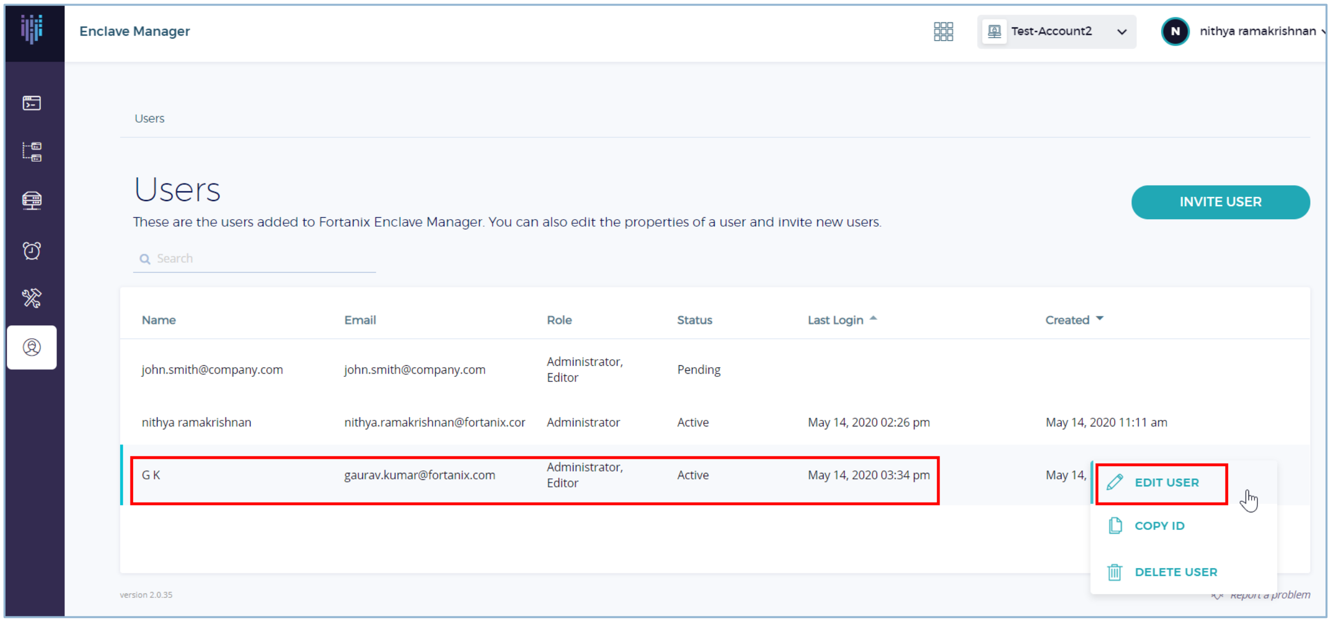
Users

These are the users added to Fortanix Enclave Manager. You can also edit the properties of a user and invite new users.

Name	Email	Role	Status	Last Login	Created
nithya ramakrishnan	nithya.ramakrishnan@fortanix.c	Administrator	Active	May 14, 2020 02:26 pm	May 14, 2020 11:11 am

FIGURE 22: USERS TAB

2. From the list of users, select a user to edit and click the three dots icon for the selected user. From this menu click **EDIT USER** to edit the user details.



Users

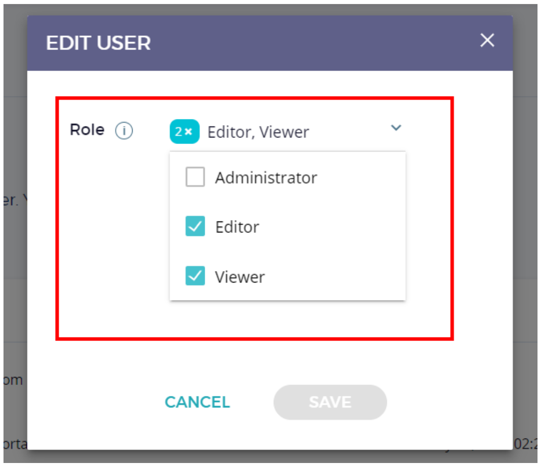
Users

These are the users added to Fortanix Enclave Manager. You can also edit the properties of a user and invite new users.

Name	Email	Role	Status	Last Login	Created
john.smith@company.com	john.smith@company.com	Administrator, Editor	Pending		
nithya ramakrishnan	nithya.ramakrishnan@fortanix.cor	Administrator	Active	May 14, 2020 02:26 pm	May 14, 2020 11:11 am
G K	gaurav.kumar@fortanix.com	Administrator, Editor	Active	May 14, 2020 03:34 pm	May 14,

FIGURE 23: SELECT USER

3. Update the user's role.



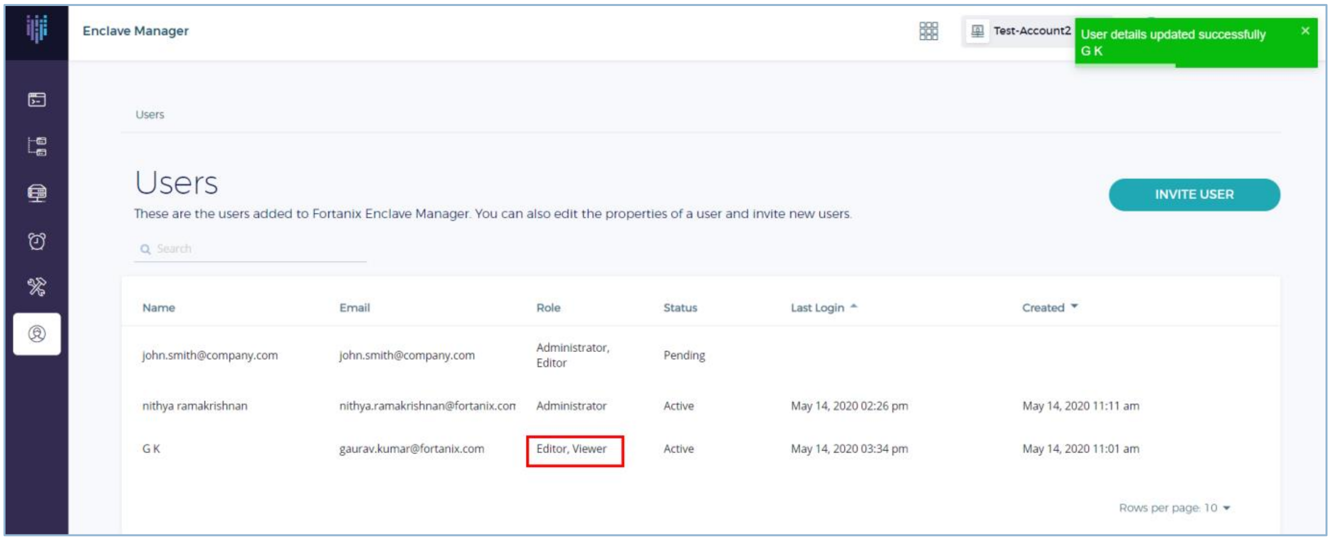
EDIT USER

Role ⓘ 2× Editor, Viewer

- ☐ Administrator
- ☑ Editor
- ☑ Viewer

FIGURE 24: EDIT USER DETAILS

4. Click **Save** to update the user details (**Figure 24**).
5. The updated user details are saved and visible now.



User details updated successfully
G K

Users

These are the users added to Fortanix Enclave Manager. You can also edit the properties of a user and invite new users.

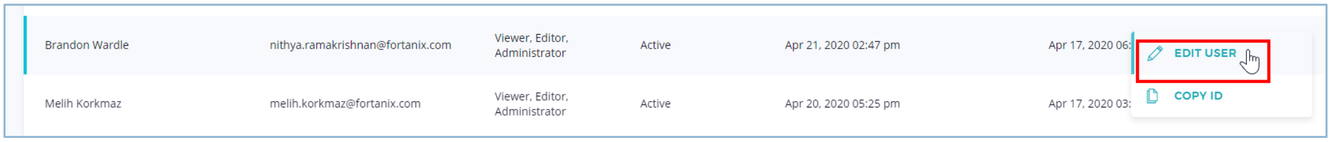
Name	Email	Role	Status	Last Login ▲	Created ▼
john.smith@company.com	john.smith@company.com	Administrator, Editor	Pending		
nithya ramakrishnan	nithya.ramakrishnan@fortanix.con	Administrator	Active	May 14, 2020 02:26 pm	May 14, 2020 11:11 am
G K	gaurav.kumar@fortanix.com	Editor, Viewer	Active	May 14, 2020 03:34 pm	May 14, 2020 11:01 am

Rows per page: 10 ▾

FIGURE 25: USER DETAILS SAVED

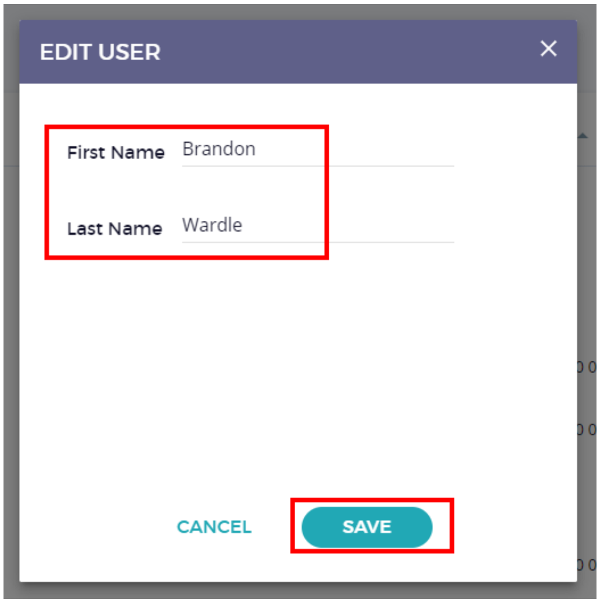
If you are an account administrator, by default you have the **Administrator**, **Editor**, and **Viewer** role. You can edit your own details like **First Name** and **Last Name** using two methods:

a. Using the **EDIT USER** option.



Brandon Wardle	nithya.ramakrishnan@fortanix.com	Viewer, Editor, Administrator	Active	Apr 21, 2020 02:47 pm	Apr 17, 2020 06:
Melih Korkmaz	melih.korkmaz@fortanix.com	Viewer, Editor, Administrator	Active	Apr 20, 2020 05:25 pm	Apr 17, 2020 03:

FIGURE 26: EDIT YOUR DETAILS



First Name Brandon

Last Name Wardle

FIGURE 27: USER FIRST AND LAST NAME

b. Using the **My profile** option.

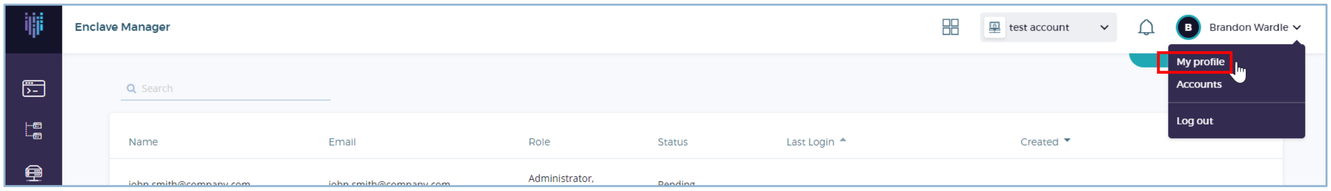


FIGURE 28: EDIT YOUR DETAILS

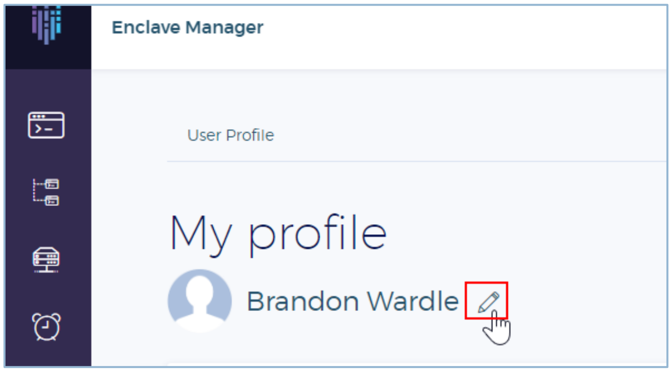
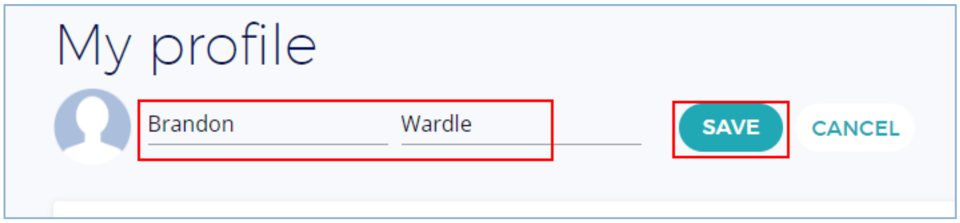


FIGURE 29: EDIT YOUR DETAILS



Brandon Wardle

FIGURE 30: EDIT FIRST AND LAST NAME

DOWNLOAD NODE AGENT

To download the node agent:

1. Click the following URL to download the Node Agent https://fortanix-fileshare.s3-us-west-1.amazonaws.com/RTE-Dev-Sandbox/Node-Agent-Installer.tar.gz
2. Extract the content of the **`Node-Agent_Installer.tar`** package and open the folder.
3. Open the **`READ_ME.txt`** file which contains the steps to enroll the compute node in Enclave Manager.

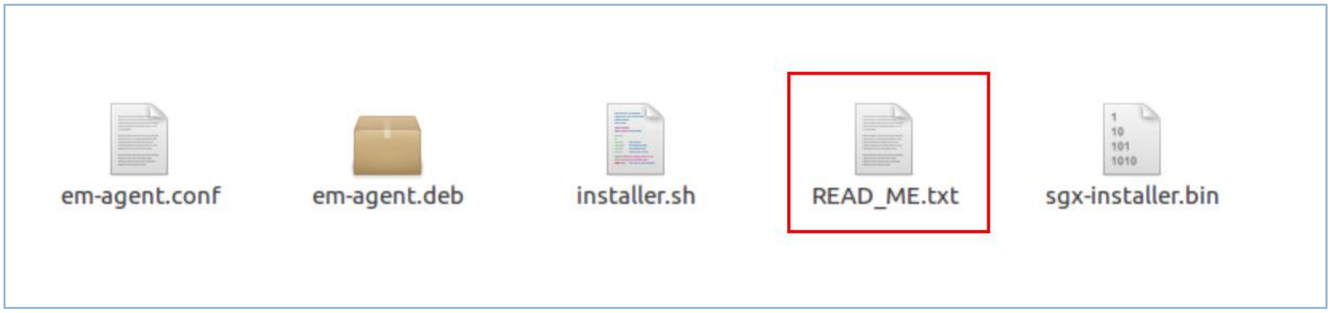


FIGURE 31: README.TXT

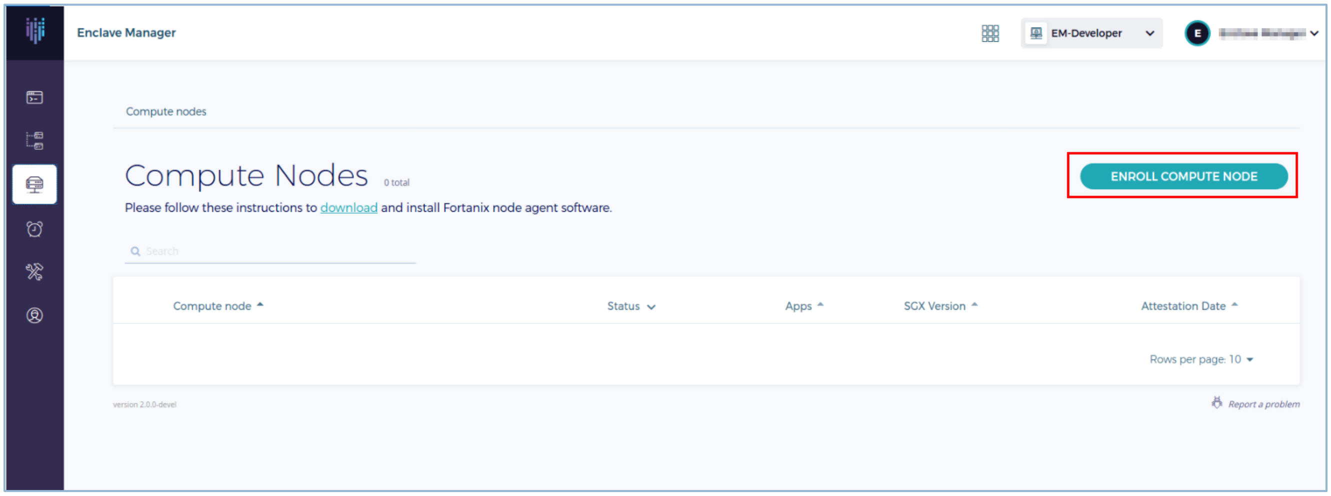
ENROLL THE COMPUTE NODE IN ENCLAVE MANAGER

The **`READ_ME.txt`** has the following steps to enroll a compute node in Enclave Manager:

1. This script assumes that you already have a DCsV2 series VM. For more information, visit https://docs.microsoft.com/en-us/azure/virtual-machines/dcv2-series
2. The Node agent listens on port 9092, so please open the port 9092 on your VM if not done already.
3. Enroll your node in Enclave Manager:
    a. Copy **`em-agent.conf`**, **`em-agent.deb`**, **`sgx-installer.bin`** and **`installer.sh`** to your VM.
    b. Run the **`installer.sh`** using the command:

```
bash installer.sh <join_token>
```

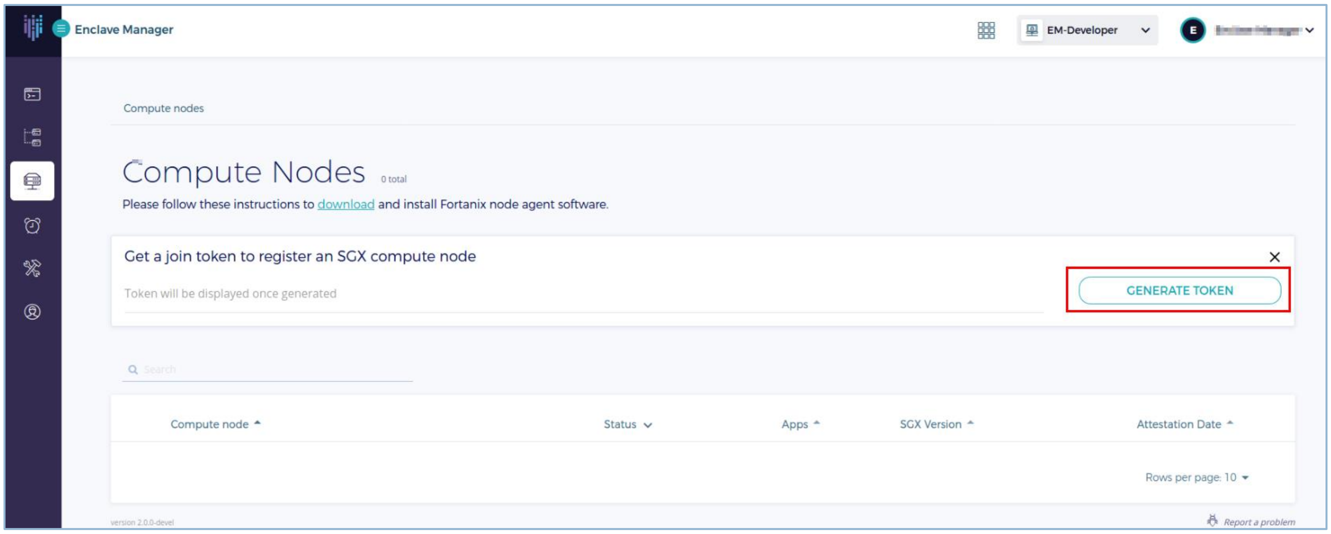
4. To generate your Join Token, please log in to https://em.fortanix.com and in the **Compute Nodes** tab, click the **ENROLL COMPUTE NODE** button.



Please follow these instructions to download and install Fortanix node agent software.

FIGURE 32: ENROLL COMPUTE NODE

5. In the following screen click the **GENERATE TOKEN** button to generate Join Token. This Join Token is used by the compute node to authenticate itself.



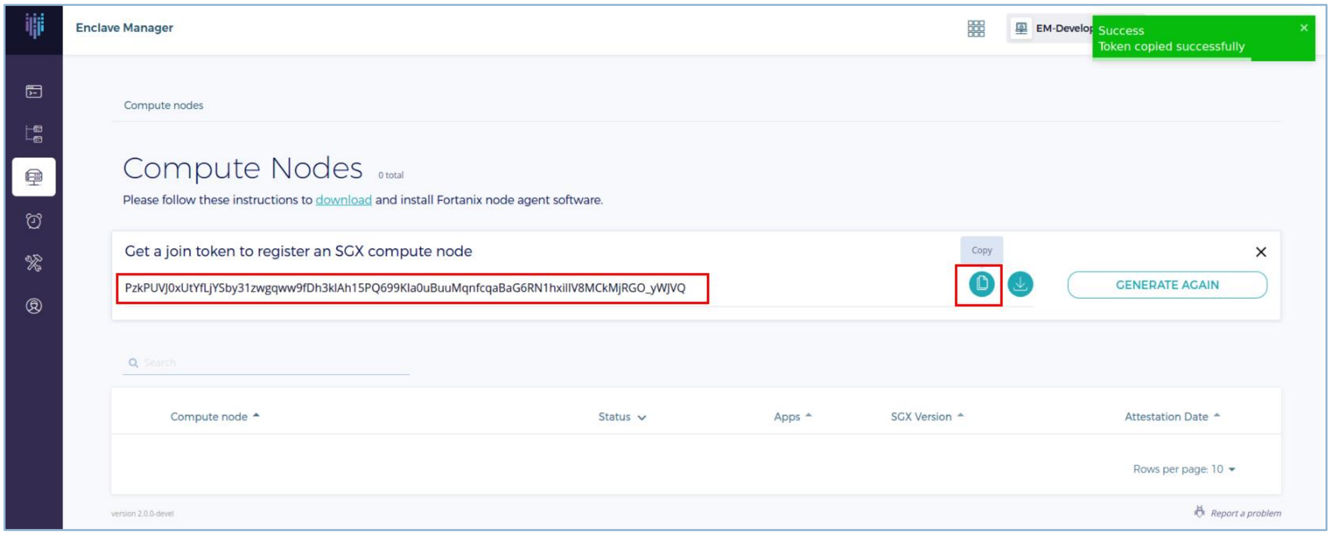
Please follow these instructions to download and install Fortanix node agent software.

Get a join token to register an SGX compute node

Token will be displayed once generated

FIGURE 33: GENERATE TOKEN

6. A Join Token will be generated in the text box for “**Get a join token to register an SGX compute node**”.
7. Click the copy icon to copy the Join Token (**Figure 34**).



Enclave Manager

EM-Develop

Success
Token copied successfully

Compute nodes

Compute Nodes 0 total

Please follow these instructions to download and install Fortanix node agent software.

Get a join token to register an SGX compute node

PzkPUVJ0xUtYfLjYSby31zwgqww9fDh3kIAh15PQ699KIa0uBuuMqnfcqaBaG6RN1hxiIlV8MCkMjRGO_yWJVQ

Compute node	Status	Apps	SGX Version	Attestation Date

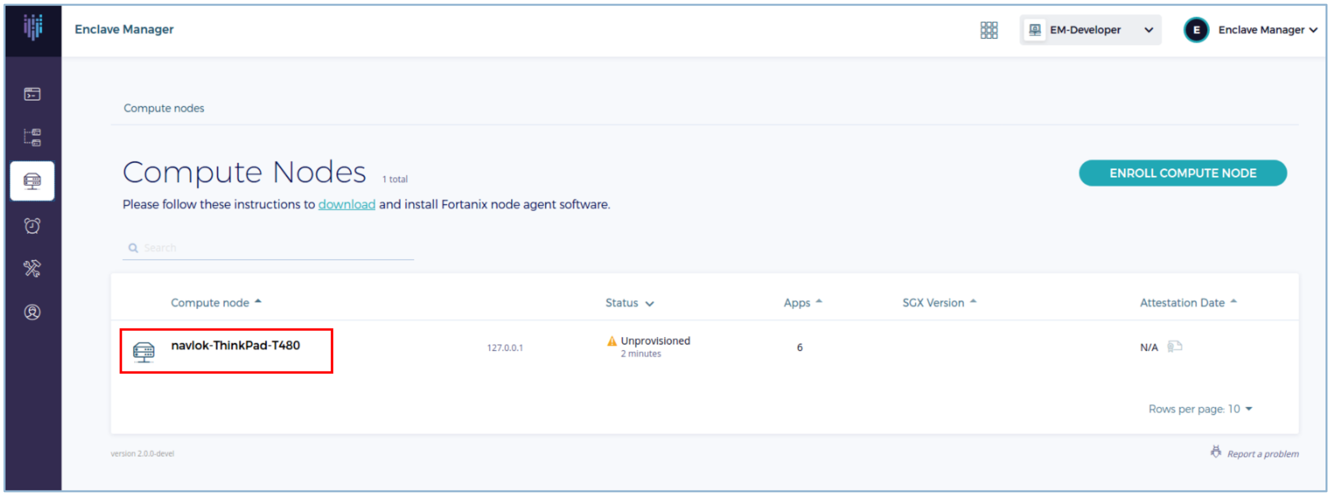
Rows per page: 10

version 2.0.0-devel

Report a problem

FIGURE 34: COPY JOIN TOKEN

8. Run the **`installer.sh`** with the Join Token that you copied. This will enroll the compute node in Enclave Manager.
9. Once the compute node is enrolled in Enclave Manager, you will see it under the **Compute Nodes** overview table.



Enclave Manager

EM-Developer

Enclave Manager

Compute nodes

Compute Nodes 1 total

Please follow these instructions to download and install Fortanix node agent software.

Compute node		Status	Apps	SGX Version	Attestation Date
navlok-ThinkPad-T480	127.0.0.1	Unprovisioned 2 minutes	6		N/A

Rows per page: 10

version 2.0.0-devel

Report a problem

FIGURE 35: ENROLLED NODE

MANAGING NODES

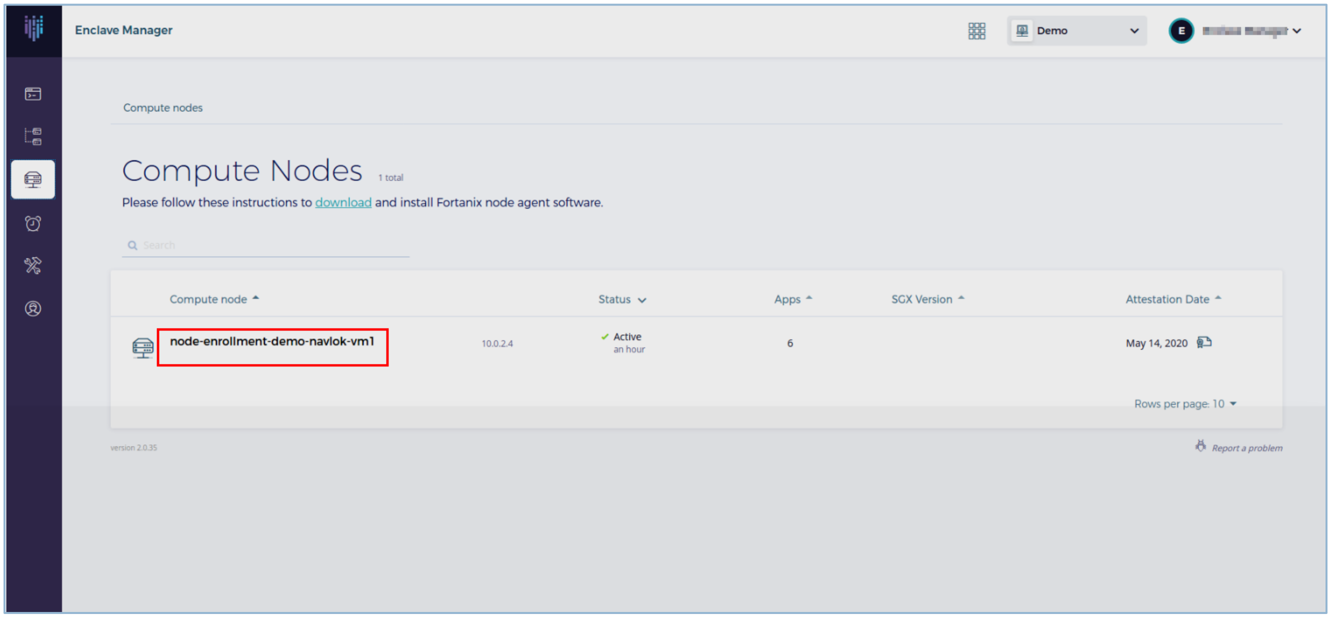
1. Sign in to the Fortanix Enclave Manager UI, and navigate to the **Compute Nodes** tab.
2. Click the IP address of the node that you want to investigate. An information screen opens.

3. On the information screen, you can choose to deactivate/delist the node or download the certificate that is used. To download the certificate, refer to the section, *Download Enclave Manager certificate*.

DOWNLOAD FORTANIX ENCLAVE MANAGER NODE ATTESTATION CERTIFICATE

To download the EM node attestation certificate:

1. Go to the **Compute Nodes** tab, and then click the compute node for which you want to download the certificate.



Compute Nodes 1 total

Please follow these instructions to download and install Fortanix node agent software.

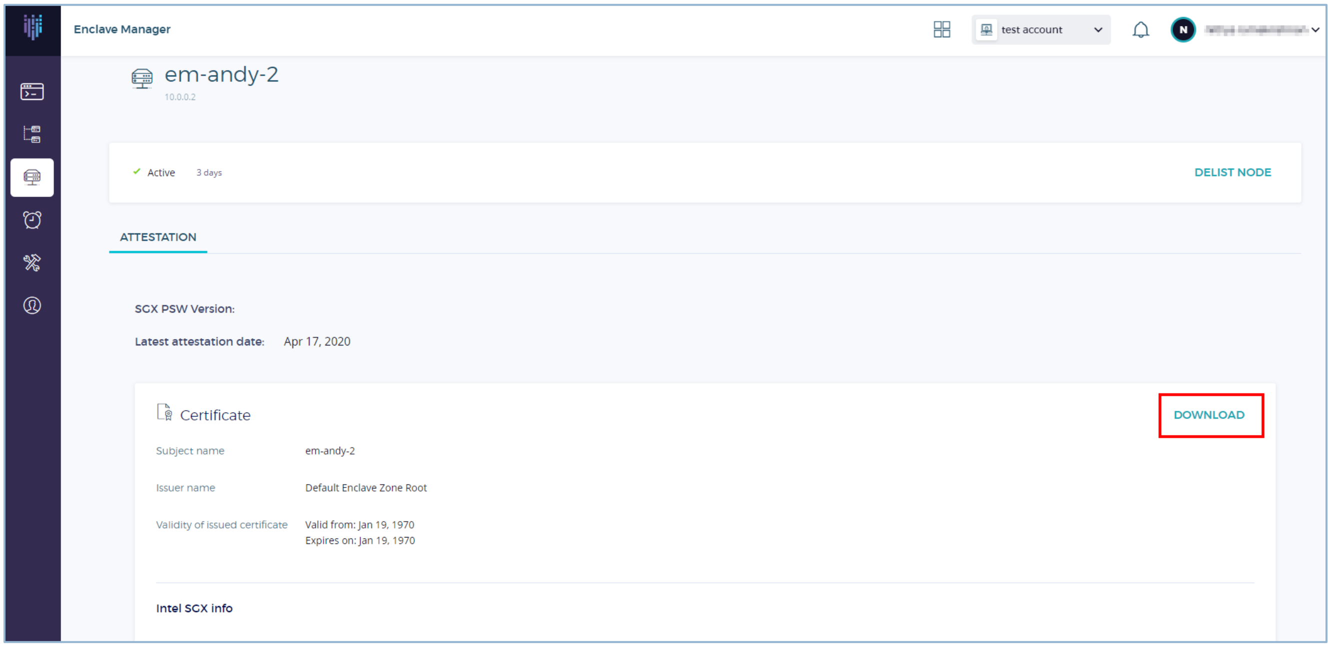
Compute node		Status	Apps	SGX Version	Attestation Date
node-enrollment-demo-navlok-vm1	10.0.2.4	✓ Active an hour	6		May 14, 2020

Rows per page: 10

version 2.0.35

FIGURE 36: SELECT NODE

2. You can download the certificate from the Compute Node detailed view using the **Download** option on the right. This certificate contains Intel SGX details such as CPUSVN (CPU Security Version Number) of the compute node, MRENCLAVE of the node agent software, and so on, as seen from the screenshot below.



em-andy-2

10.0.0.2

✓ Active 3 days

SGX PSW Version:

Latest attestation date: Apr 17, 2020

Certificate

Subject name	em-andy-2
Issuer name	Default Enclave Zone Root
Validity of issued certificate	Valid from: Jan 19, 1970 Expires on: Jan 19, 1970

FIGURE 37: DOWNLOAD CERTIFICATE

ADD AND EDIT AN APPLICATION

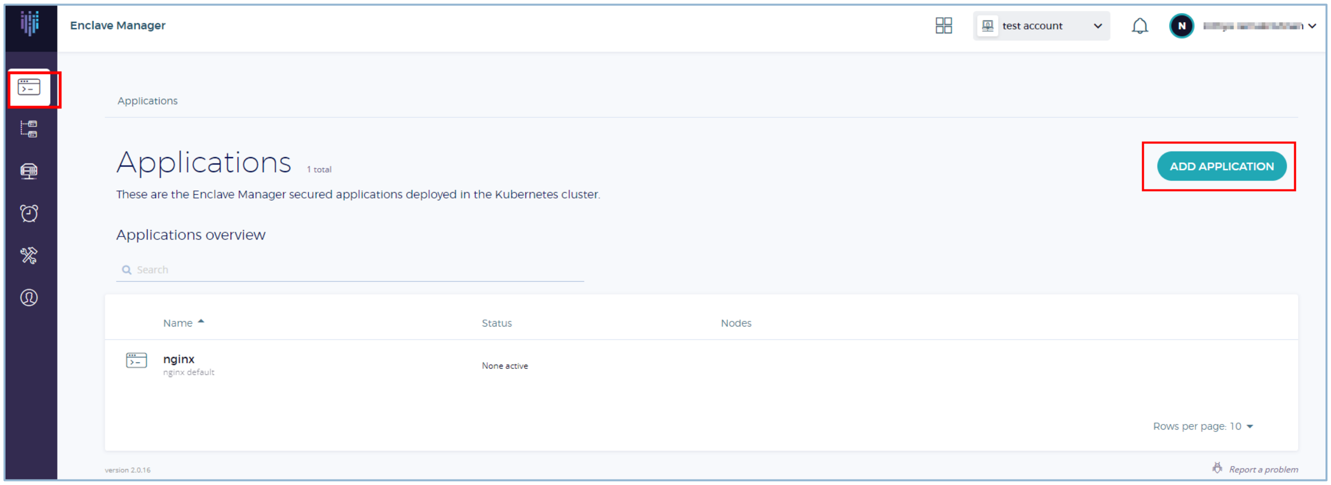
Prerequisites:

- Name of the input docker image of this application from the input registry.
- Output image location.

Steps to add an App:

You can convert, deploy, and whitelist your application all at the same time using Fortanix Enclave Manager.

1. Sign in to the Fortanix Enclave Manager, and then click the **Apps** tab.
2. Click **Add application** to add a new application.



Applications

Applications 1 total

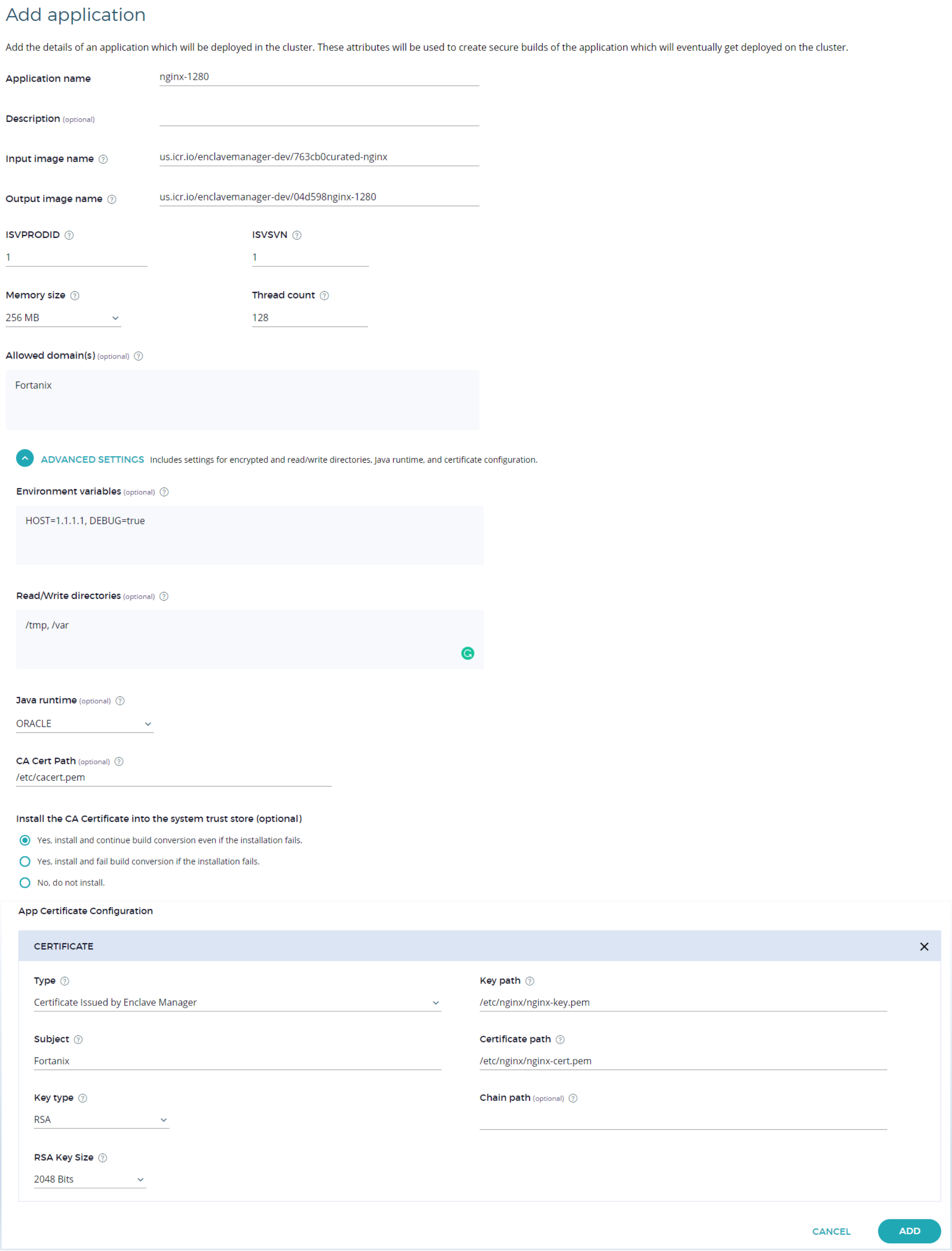
These are the Enclave Manager secured applications deployed in the Kubernetes cluster.

Applications overview

Name	Status	Nodes
nginx nginx default	None active	

FIGURE 38: ADD NEW APPLICATION

3. In the **Add application** form (**Figure 39**), fill all the required fields (**Application name**, **Input image name**, **Output image name**, **ISVPRODID**, **ISVSVN, Memory Size, Thread Count**).
    a. **Application name** is the name of the application.
    b. **ISVPRODID** is a numeric product identifier. A user must choose a unique value in the range of 0-65535 for their applications.
    c. **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.
    d. **Input image name** is your current application's current docker image.
    e. **Output image name** is where you can find the converted application.
    For more information, please see the URL https://software.intel.com/en-us/node/702979
    f. **Memory Size** – Choose the memory size from the drop-down to change the memory size of the enclave.
    g. **Thread Count** – Change the thread count to support the application.



Add application

Add the details of an application which will be deployed in the cluster. These attributes will be used to create secure builds of the application which will eventually get deployed on the cluster.

Application name: nginx-1280

Description (optional):

Input image name: us.icr.io/enclavemanager-dev/763cb0curated-nginx

Output image name: us.icr.io/enclavemanager-dev/04d598nginx-1280

ISVPRODID: 1

ISVSVN: 1

Memory size: 256 MB

Thread count: 128

Allowed domain(s) (optional): Fortanix

ADVANCED SETTINGS Includes settings for encrypted and read/write directories, Java runtime, and certificate configuration.

Environment variables (optional): HOST=1.1.1.1, DEBUG=true

Read/Write directories (optional): /tmp, /var

Java runtime (optional): ORACLE

CA Cert Path (optional): /etc/cacert.pem

Install the CA Certificate into the system trust store (optional)

● Yes, install and continue build conversion even if the installation fails.

○ Yes, install and fail build conversion if the installation fails.

○ No, do not install.

App Certificate Configuration

CERTIFICATE

Type: Certificate Issued by Enclave Manager

Key path: /etc/nginx/nginx-key.pem

Subject: Fortanix

Certificate path: /etc/nginx/nginx-cert.pem

Key type: RSA

Chain path (optional):

RSA Key Size: 2048 Bits

FIGURE 39: APPLICATION DETAILS

For the optional fields, please see the descriptions below:

- **Description** – Enter the application's description
- **Allowed domain(s)** – Enter the allowed domain(s) for the application. These are domains that appear in the TLS certificates issued by the Fortanix Enclave Manager. You can add multiple domains separated by a comma.

Edit any **Advanced settings** that you might want to change.

- **Environment variables** – Enter any environment variables that will be set at runtime. The variables need to be comma separated values.
- **Java Runtime** – Select the appropriate Java runtime values. When you select the Java Runtime option for an application, the converted docker image will run with the specified options for the chosen JVM (Java Virtual Machine).

```
OPENJDK / ORACLE -
-XX:CompressedClassSpaceSize=16m
-XX:-UsePerfData
-XX:ReservedCodeCacheSize=16m
-XX:-UseCompiler
-XX:+UseSerialGC
OPENJ9 / LIBERTY -
-Xnojit
-Xnoaot
-Xdump:none
```

- **CA Cert path** – Enter the path to store the Fortanix Enclave Manager CA certificate.

As an optional step, the user can install the CA certificate in the system trust store where all the certificates are stored. Following are the three options given:

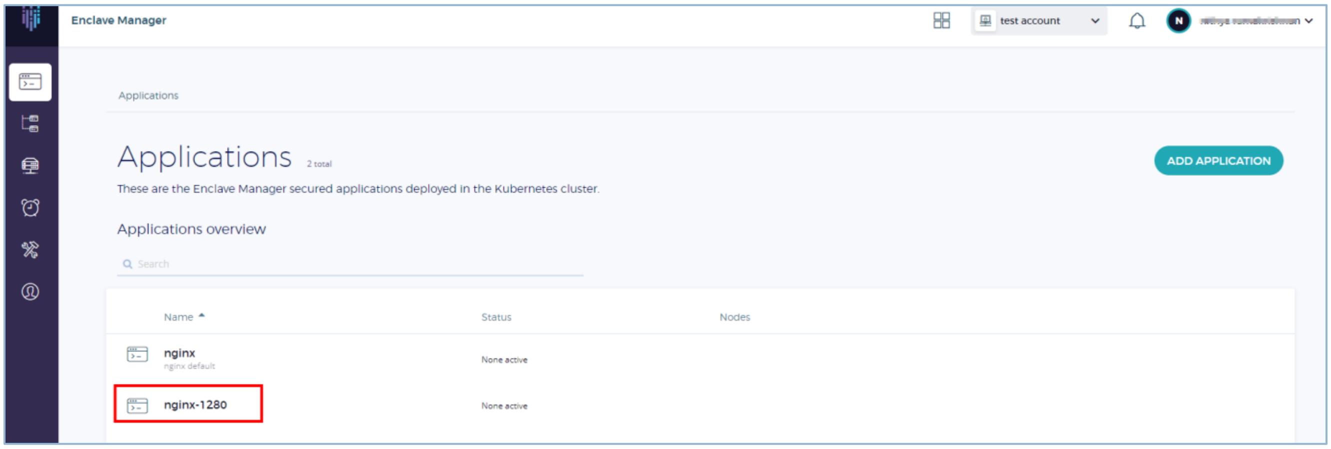
- **Yes, install and continue image conversion even if the installation fails** – select this option if you want to convert the image even after the CA Certificate installation fails.
- **Yes, install and fail image conversion if the installation fails** – select this option if you want to stop image conversion after the CA Certificate installation fails.
- **No, do not install** – select this option if you do not want to install the CA Certificate.

Add any certificate using the **App Certificate configuration** section. A converted application can request a certificate from the Fortanix Enclave Manager when your application is started. The certificates are signed by the Fortanix Enclave Manager Certificate Authority, which issues certificates only to enclaves presenting a valid attestation.

- **Key Path** – Enter the key path that will be accessible by the application.
- **Certificate Path** – Enter the certificate path that will be accessible by the application.
- **Chain Path** – Enter the chain path for the complete certificate chain. This is the path where we store the app_cert and intermediate_ca cert.
- **Subject** – Enter the subject which is same as the value in the **Allowed domain**(s) list.

NOTE: The user will be able to either add the **Certificate Path** or the **Chain Path**, not both.

4. Click **Add** to create the application (**Figure 39**). The application will now be deployed and added to your whitelist and visible in the **Apps** tab (**Figure 40**). You can approve the application domain whitelisting request in the **Tasks** tab.



Applications 2 total

These are the Enclave Manager secured applications deployed in the Kubernetes cluster.

Applications overview

Name	Status	Nodes
nginx nginx default	None active	
nginx-1280	None active	

FIGURE 40: APPLICATION CREATED

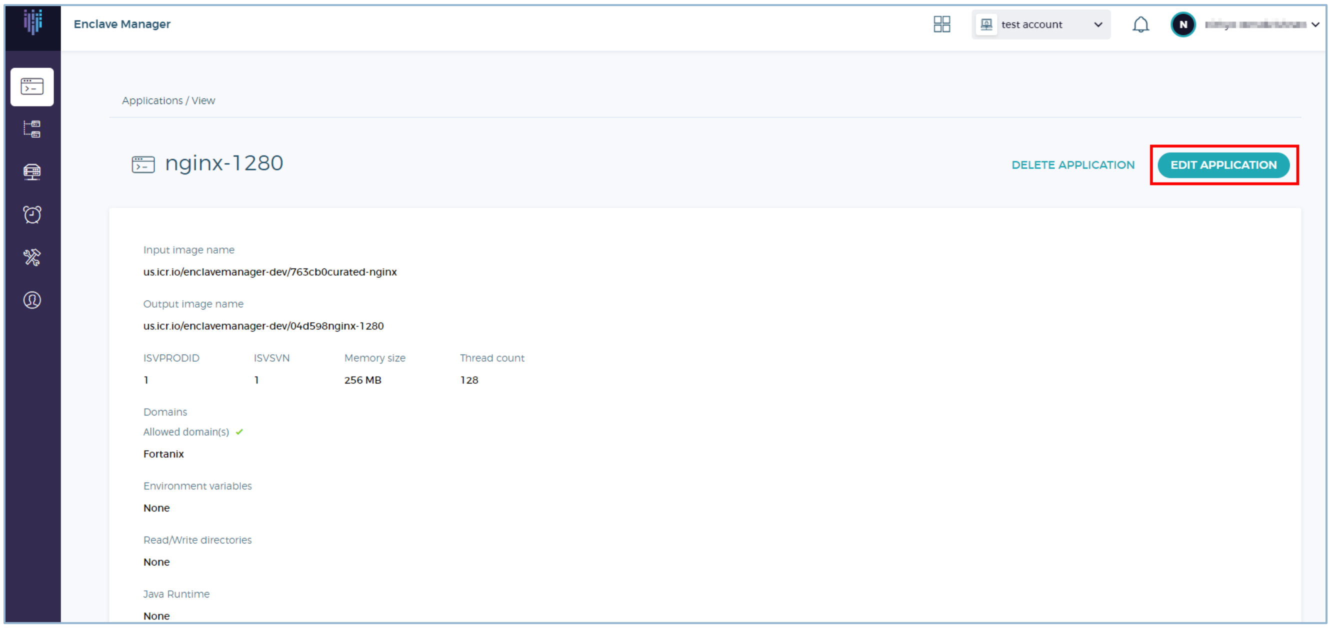
NOTE: Creating an application does not mean that an SGX Ready Image is created and pushed. An application will be converted and pushed to the specified location once an image of this application is created.

Steps to edit an App:

You can edit an application after you add it to your list.

1. Sign in to Fortanix Enclave Manager, and then navigate to the **Apps** tab.

2. Click the name of the application that you want to edit. A new screen opens where you can review and edit the configuration including certificates and deployed images.
3. Click **Edit application.**



Input image name
us.icr.io/enclavemanager-dev/763cb0curated-nginx

Output image name
us.icr.io/enclavemanager-dev/04d598nginx-1280

ISVPRODID	ISVSVN	Memory size	Thread count
1	1	256 MB	128

Domains
Allowed domain(s) ✓
Fortanix

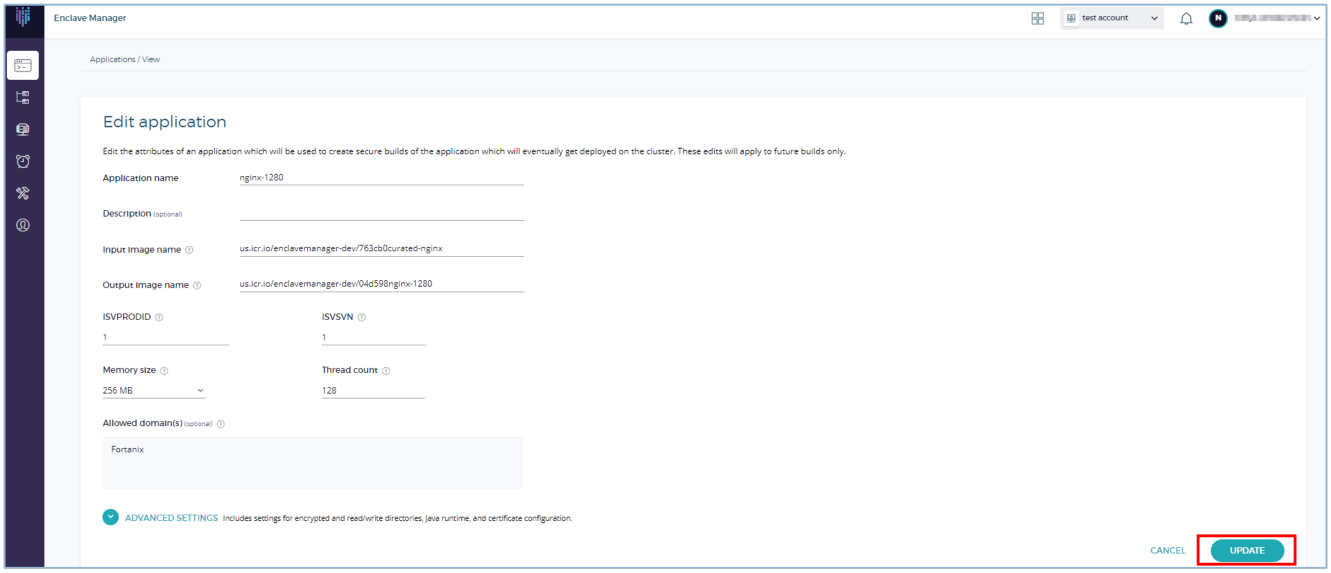
Environment variables
None

Read/Write directories
None

Java Runtime
None

FIGURE 41: EDIT APPLICATION

4. Update the configuration that you want to make. Be sure that you understand the way that changing the advanced settings affects your application before you make any change.
5. Click **UPDATE**.



Edit application

Edit the attributes of an application which will be used to create secure builds of the application which will eventually get deployed on the cluster. These edits will apply to future builds only.

Application name: nginx-1280

Description (optional):

Input image name ⓘ: us.icr.io/enclavemanager-dev/763cb0curated-nginx

Output image name ⓘ: us.icr.io/enclavemanager-dev/04d598nginx-1280

ISVPRODID ⓘ: 1

ISVSVN ⓘ: 1

Memory size ⓘ: 256 MB

Thread count ⓘ: 128

Allowed domain(s) (optional) ⓘ: Fortanix

ADVANCED SETTINGS Includes settings for encrypted and read/write directories, Java runtime, and certificate configuration.

FIGURE 42: UPDATE APPLICATION

📌 **NOTE**:

- **Application name** cannot be edited.
- **Allowed domain(s)** can only be edited if the application does not have any pending domain whitelisting task.

SETTING ENVIRONMENT VARIABLES FOR YOUR APPLICATION

Many applications can be configured by using environment variables such as a container image, a Kubernetes pod specification, or a container entrypoint script. The `{site.data.keyword.datashield_short}` conversion process transfers any environment variables that are specified by the input container image to a configuration file in the output container, where they are covered by the enclave signature. This freezes the values of the environment variables at conversion time. If variables are supplied after the conversion takes place, they are not seen by the application. Since the variables are not seen, your application is not protected from any maliciously set environment variables at runtime.

By default, the only environment variable passed to the binaries in library OSes is *`PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin`*. If the host environment variables specifies a *`HOSTNAME`* then it is also included in the list of default environment variables.

Syntax 1: `loader.env.[ENVIRON]=[VALUE]`

This syntax specifies the environment variable value that is customized for the enclaves. This syntax can be used multiple times to specify more than one environment variable.

The list of environment variables passed to the binaries in enclaves will include a merged list of default environment variables and environment variables specified with this syntax. If there are any conflicting variables, the default environment variable will be overwritten.

Syntax 2: `loader.env.allow_all_env.all = 1`

This syntax passes all the host environment variables to the binaries in the enclaves.

The list of environment variables passed to the binaries in enclaves will include a merged list of host environment variables and variables specified with syntax 1. If there are any conflicting variables, the host environment variables will be overwritten with the value specified by syntax 1. For example, if the manifest specifies `loader.env.X = Z` and the host specifies `X=Y` then the value of `X=Z`.

Syntax 3: loader.env.allow_some_env.`[ENVIRON] = 1`

This syntax specifies the environment variable that will be passed from the host environment variable to the binaries in the enclaves. This syntax can be used multiple times to specify more than one environment variable.

The list of environment variables passed to the binaries in enclaves will include a merged list of a subset of host environment variables as specified by Syntax 3 and variables specified with Syntax 1. If there are any conflicting variables, the host environment variables will be overwritten with the value specified by Syntax 1. For example, if the manifest specifies `loader.env.X = Z` and the host specifies `X=Y` then the value of `X=Z`.

Note that Syntax 2 overrides Syntax 3, so it is recommended to use one or the other of these, not both, in the manifest file.

APPROVING TASKS / DOMAIN WHITELISTING

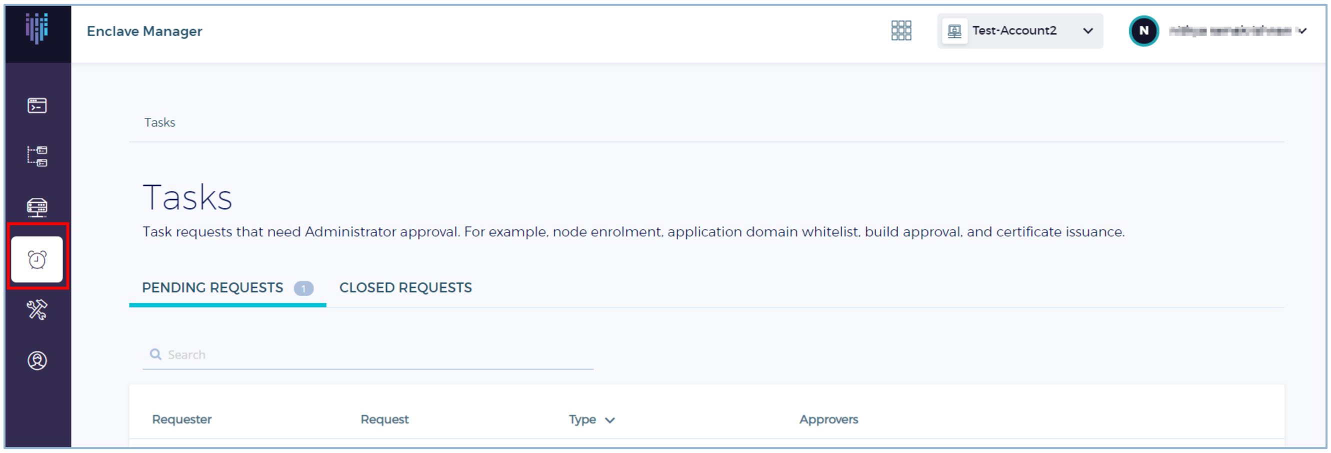
An application whose domain is whitelisted will get a TLS Certificate from Fortanix Enclave Manager. This certificate will have the domain as subject name which will allow all requests from this domain to be served by the application. If this domain is not whitelisted, the image will run but it will not be issued any TLS certificate from Fortanix Enclave Manager.

Prerequisites:

1. An application should be created with a new domain.

Steps:

1. Add an application with a domain as described in *section: Add an Application*.
2. Once the application is created successfully, click the **Tasks** tab in UI for approving a domain whitelisting task.


Enclave Manager

Test-Account2

N [redacted]

Tasks

Tasks

Task requests that need Administrator approval. For example, node enrolment, application domain whitelist, build approval, and certificate issuance.

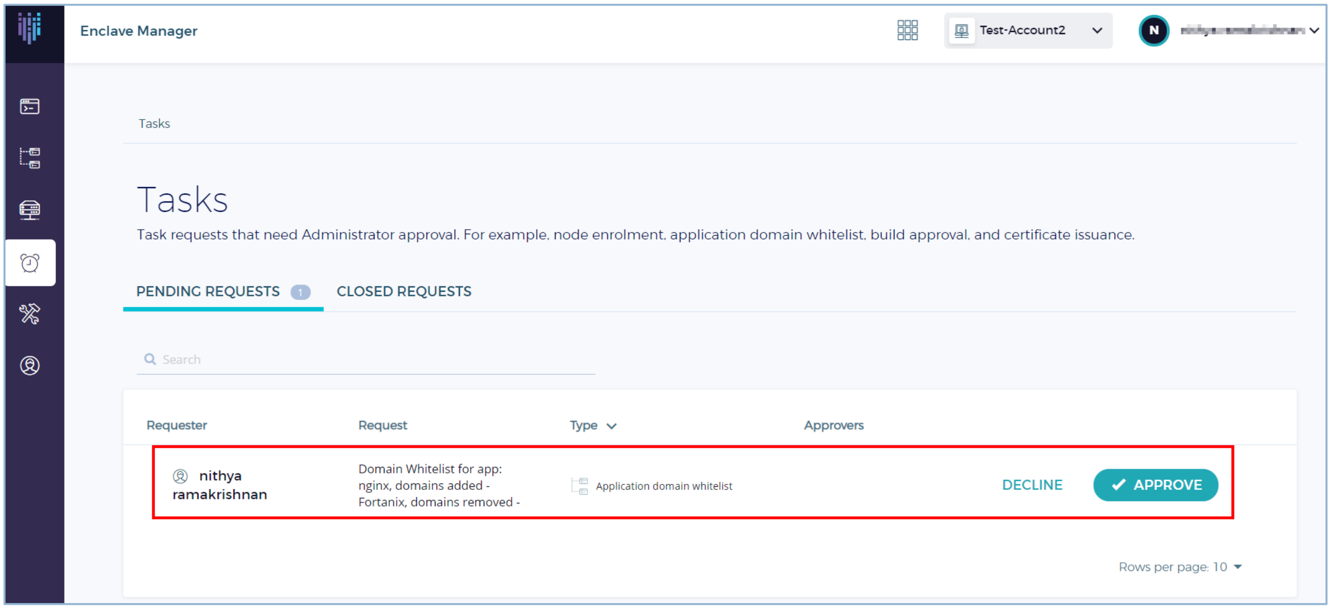
PENDING REQUESTS 1 CLOSED REQUESTS

Search

Requester	Request	Type	Approvers

FIGURE 43: TASKS TAB FOR DOMAIN WHITELISTING

3. A domain whitelist task will be created for the application. Click **Approve** to approve the task (**Figure 44**).


Enclave Manager

Test-Account2

N [redacted]

Tasks

Tasks

Task requests that need Administrator approval. For example, node enrolment, application domain whitelist, build approval, and certificate issuance.

PENDING REQUESTS 1 CLOSED REQUESTS

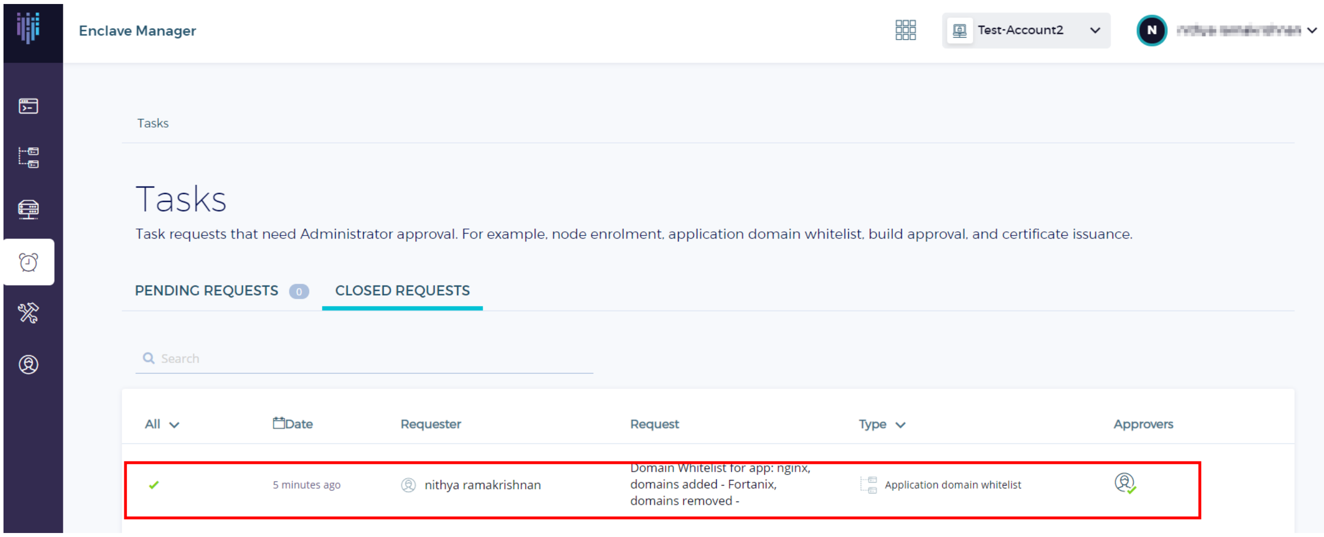
Search

Requester	Request	Type	Approvers		
nithya ramakrishnan	Domain Whitelist for app: nginx, domains added - Fortanix, domains removed -	Application domain whitelist		DECLINE	✓ APPROVE

Rows per page: 10

FIGURE 44: TASKS FOR DOMAIN WHITELISTING

4. Any user in the account with an Administrator or Editor role can approve a task.
5. Once the task is approved, you can see your closed task with summary in the **Closed requests** tab.



Tasks

Tasks

Task requests that need Administrator approval. For example, node enrolment, application domain whitelist, build approval, and certificate issuance.

All	Date	Requester	Request	Type	Approvers
✓	5 minutes ago	nithya ramakrishnan	Domain Whitelist for app: nginx, domains added - Fortanix, domains removed -	Application domain whitelist	

FIGURE 45: APPROVED TASKS

CREATING AN IMAGE YOUR APPLICATION

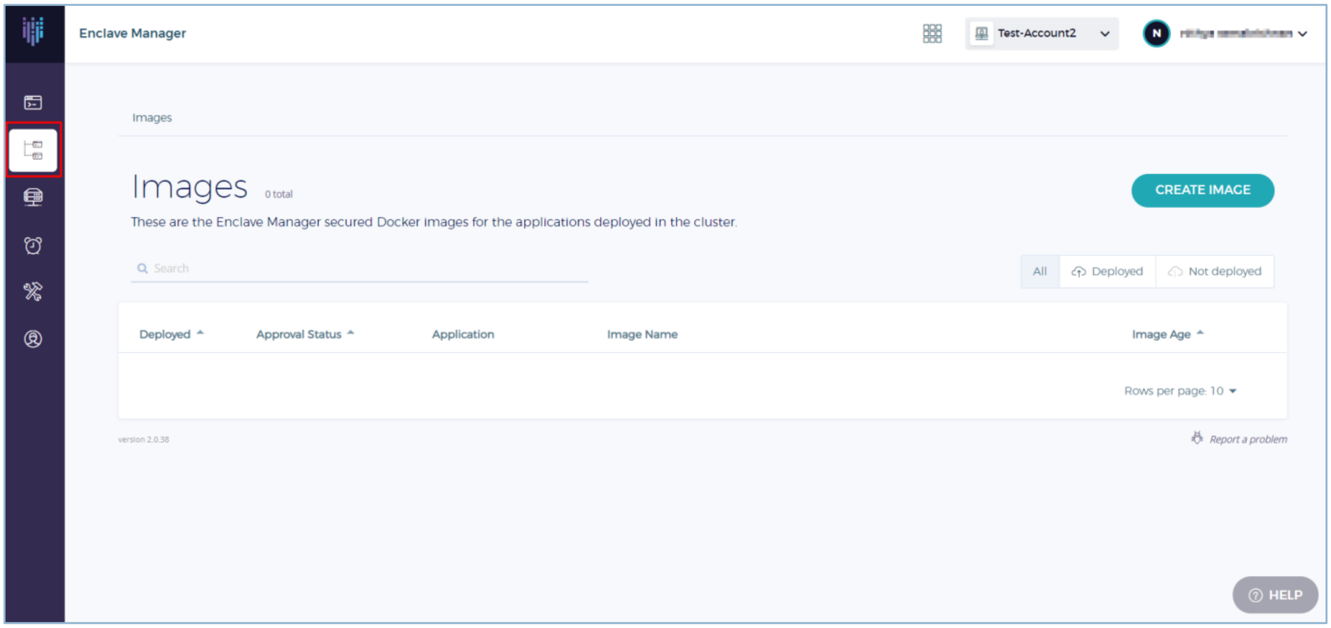
You can use the Fortanix Enclave Manager to create an image of your applications after you make changes.

Prerequisites:

- Tag of the Docker image for the application.

Steps:

1. Sign in to the Fortanix Enclave Manager, and then click the **Images** tab.

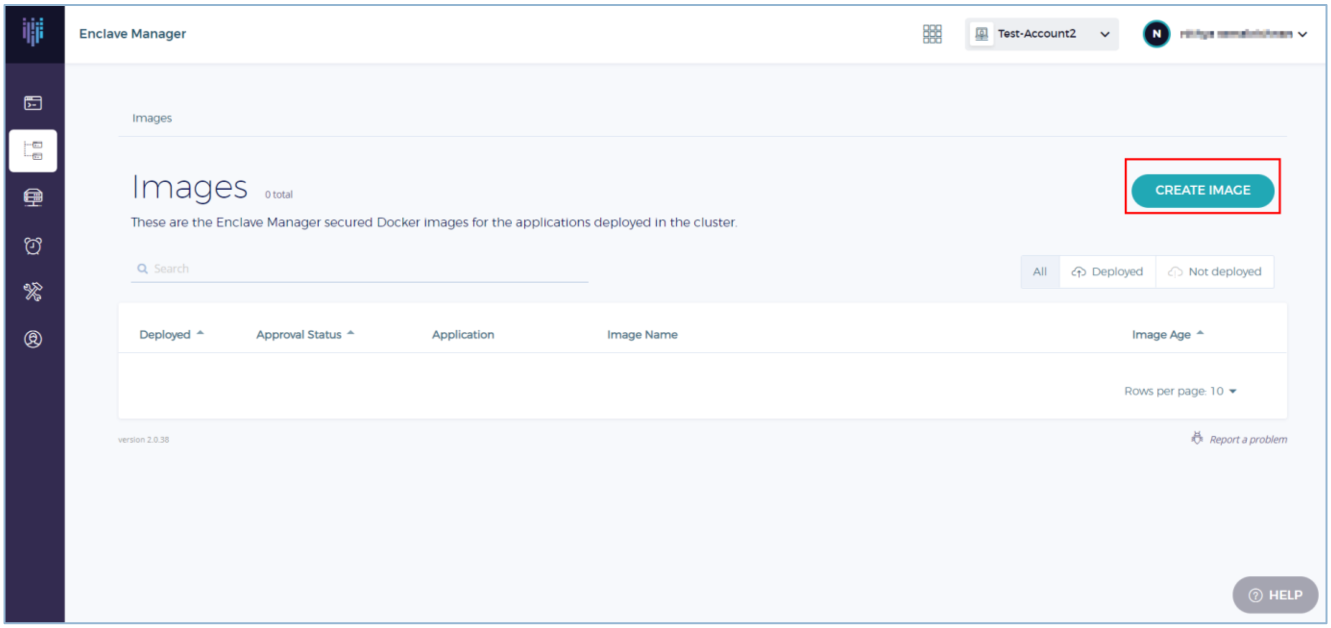


These are the Enclave Manager secured Docker images for the applications deployed in the cluster.

Deployed	Approval Status	Application	Image Name	Image Age

FIGURE 46: IMAGES TAB

2. Click **CREATE IMAGE** to create a new image for an application.

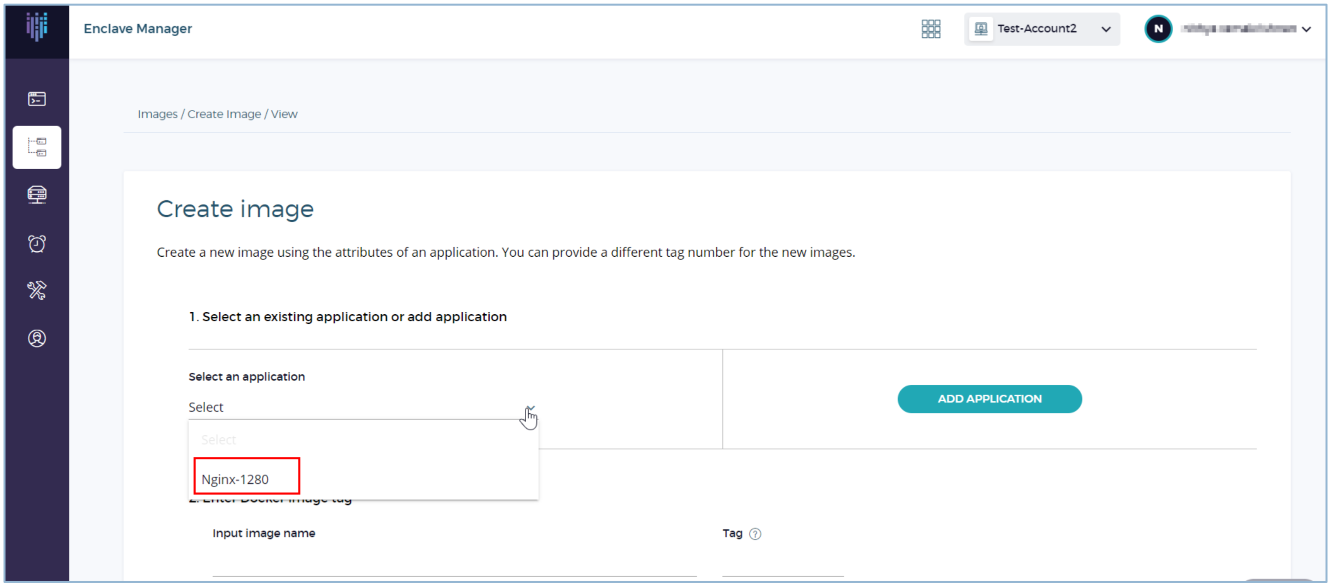


These are the Enclave Manager secured Docker images for the applications deployed in the cluster.

Deployed	Approval Status	Application	Image Name	Image Age

FIGURE 47:CREATING NEW IMAGE

3. In the **Select an application** field, select an application from the list for which a new image needs to be created.



Images / Create Image / View

Create image

Create a new image using the attributes of an application. You can provide a different tag number for the new images.

1. Select an existing application or add application

Select an application

Select

Select

Nginx-1280

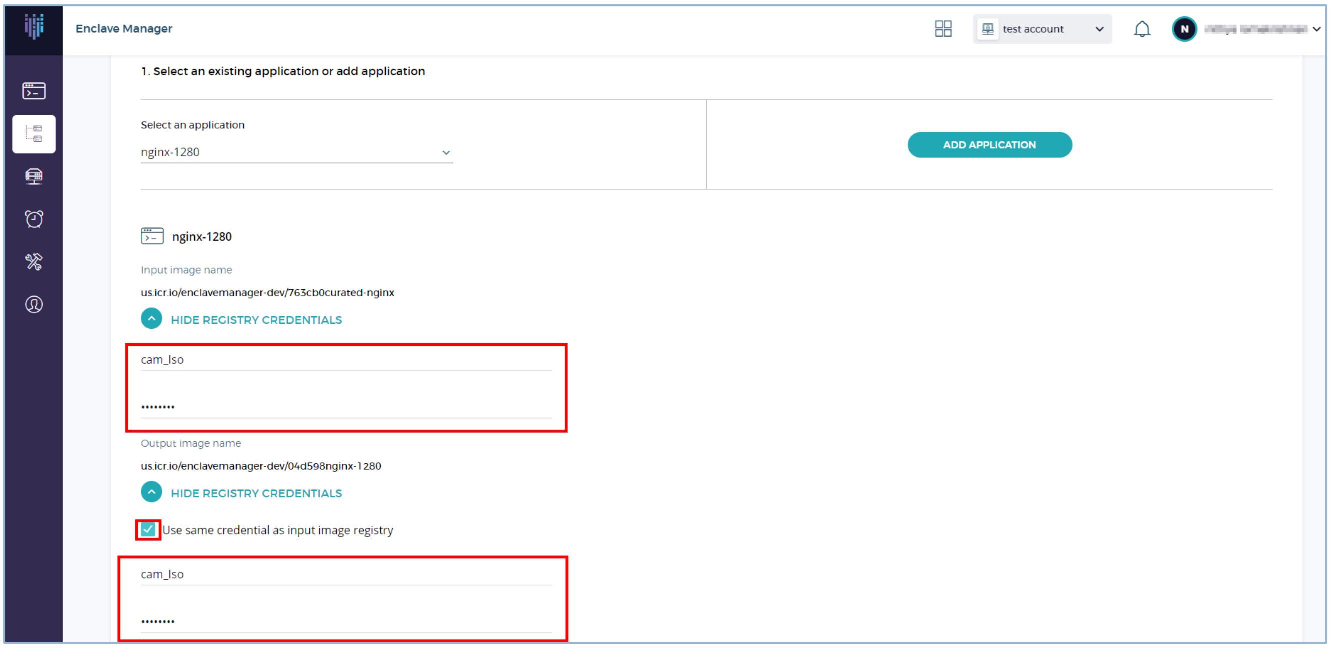
2. Enter Docker image tag

Input image name

Tag

FIGURE 48: SELECT AN APPLICATION

4. Enter the **REGISTRY CREDENTIALS** for **Input image name** and **Output image name**. The Registry Credentials are the credentials to access the private docker registry from which an image is going to be pulled or pushed. If the private docker registry is same for the input image and the output image, then select the check box **Use same credential as input image registry** in the **Output image name.**



1. Select an existing application or add application

Select an application

nginx-1280

nginx-1280

Input image name

us.icr.io/enclavemanager-dev/763cb0curated-nginx

cam_lso

••••••••

Output image name

us.icr.io/enclavemanager-dev/04d598nginx-1280

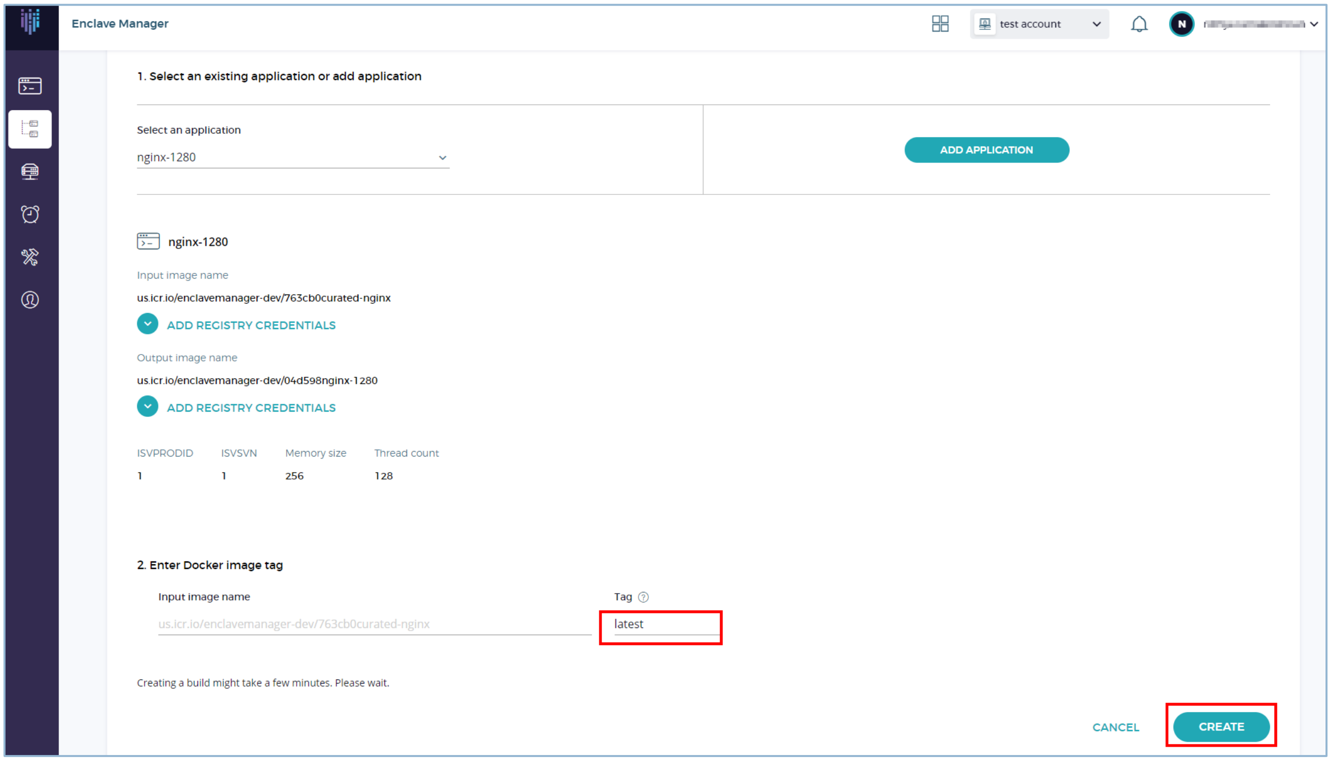
☑ Use same credential as input image registry

cam_lso

••••••••

FIGURE 49: ENTER REGISTRY CREDENTIALS

5. In the **Tag** field, enter the tag value of the Docker image (**Figure 50**).
6. Click **CREATE** to create the image (**Figure 50**).



1. Select an existing application or add application

Select an application
nginx-1280

nginx-1280

Input image name
us.icr.io/enclavemanager-dev/763cb0curated-nginx

Output image name
us.icr.io/enclavemanager-dev/04d598nginx-1280

ISVPRODID	ISVSVN	Memory size	Thread count
1	1	256	128

2. Enter Docker image tag

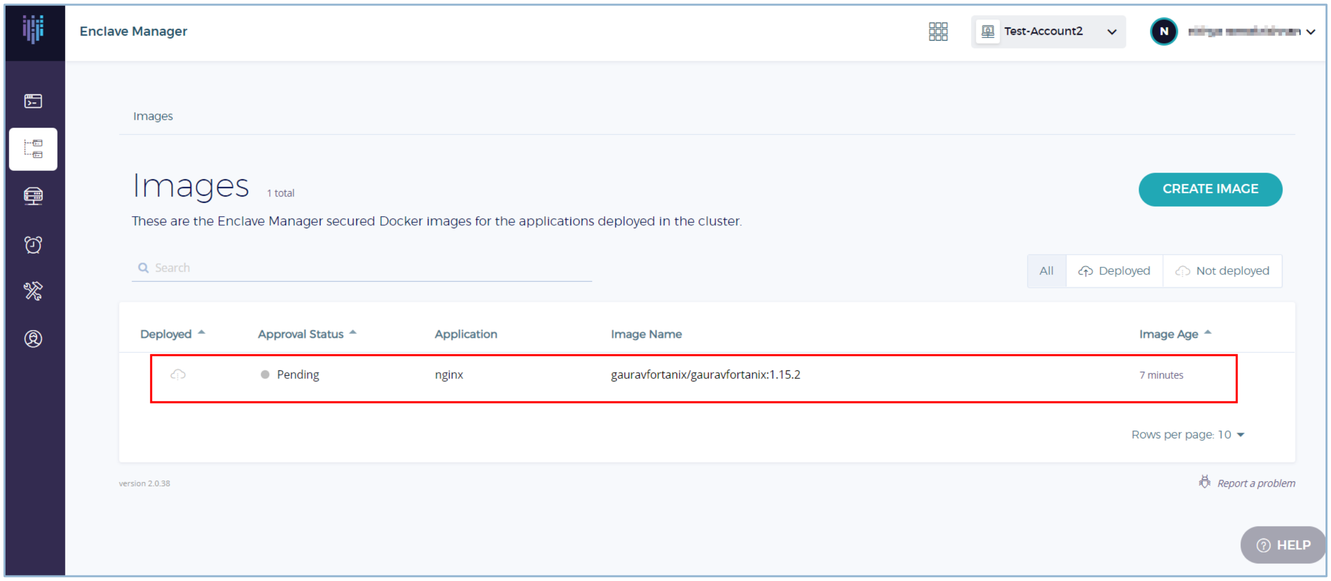
Input image name
us.icr.io/enclavemanager-dev/763cb0curated-nginx

Tag
latest

Creating a build might take a few minutes. Please wait.

FIGURE 50: DOCKER IMAGE TAG

7. An application image whitelist task is created and added which is visible in the **Images** table. You can approve the task to whitelist the image from the **Tasks** tab. Once approved, a green tick would appear in the **Approval status** column for that image.



[redacted]

Images

Images 1 total

These are the Enclave Manager secured Docker images for the applications deployed in the cluster.

Deployed	Approval Status	Application	Image Name	Image Age
	● Pending	nginx	gauravfortanix/gauravfortanix:1.15.2	7 minutes

FIGURE 51: IMAGE CREATED SUCCESSFULLY

NOTE: The Source Image tag and Output Image tag is 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.

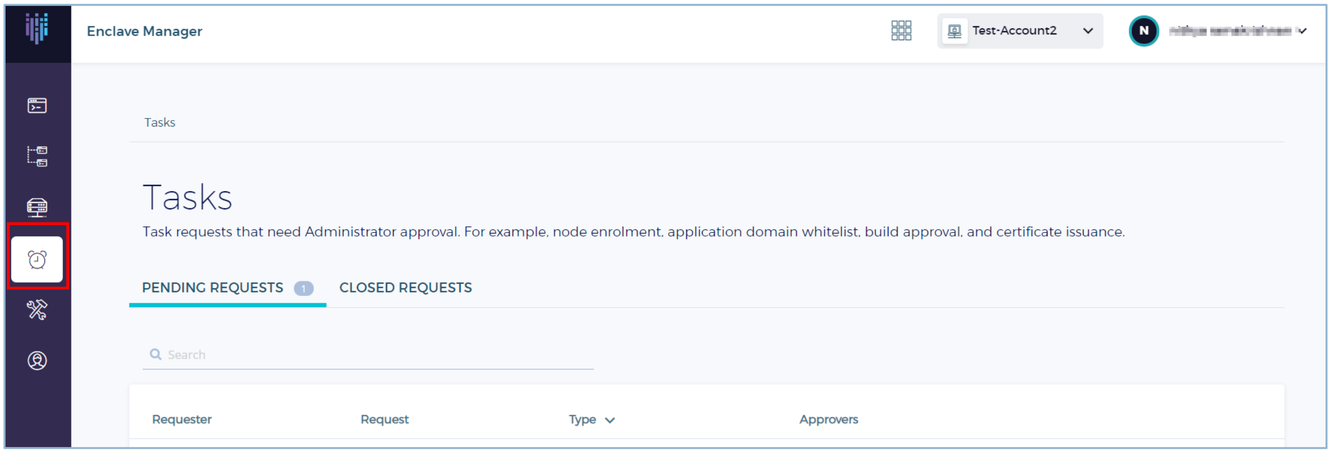
APPROVING TASKS / APPLICATION IMAGE WHITELISTING

After an image is created and when an application runs from this converted image, the application will try to contact Fortanix Enclave Manager and ask for a TLS Certificate. If the image is not whitelisted, it will run but the Fortanix Enclave Manager will deny this TLS Certificate. If the Enclave Manager denies the TLS Certificate, then the application will not run. To run applications in the enclave over certificates issued by this service, an image needs to be whitelisted. When an image is whitelisted, it is added to the list of pending requests in the **Tasks** tab of the Fortanix Enclave Manager UI. You can use the UI to approve or deny the request.

Prerequisites: An application created successfully.

Steps:

1. Create an image of an application as described in *section: Create an Image for an Application*.
2. Once the image is created successfully, click the **Tasks** tab in UI for approving the application image whitelisting task.



Enclave Manager

Test-Account2

N [redacted]

Tasks

Tasks

Task requests that need Administrator approval. For example, node enrolment, application domain whitelist, build approval, and certificate issuance.

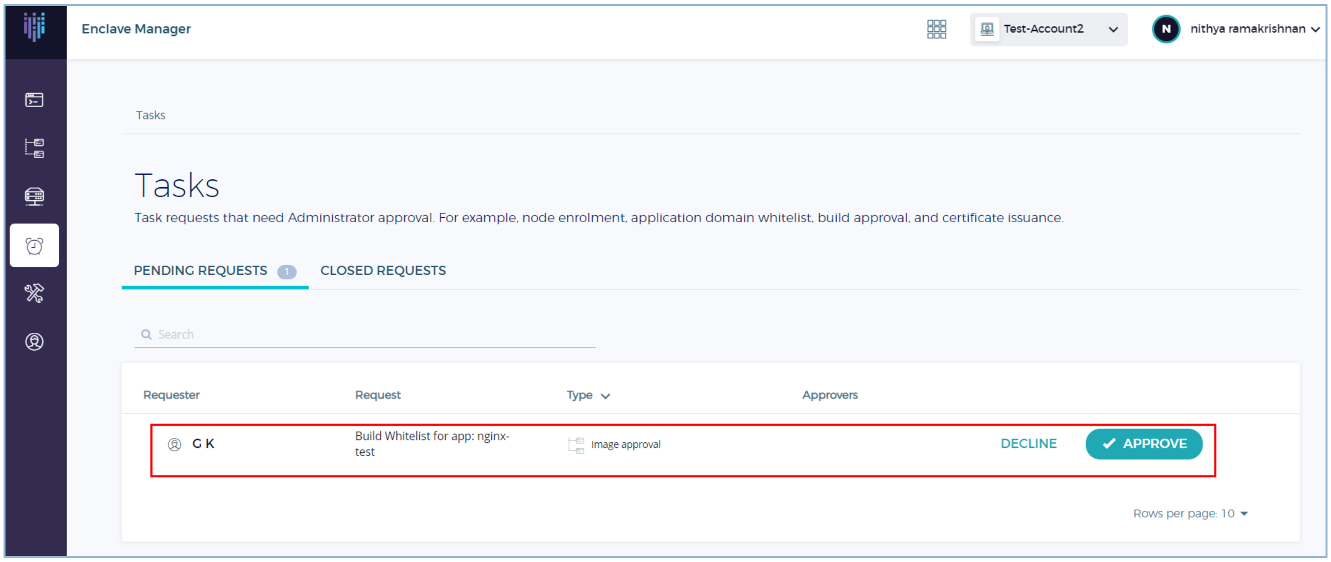
PENDING REQUESTS 1 | CLOSED REQUESTS

Search

Requester	Request	Type	Approvers

FIGURE 52: TASK TAB FOR APPLICATION IMAGE WHITELISTING

3. An application image whitelist task will be created for the application. Review the request, and then click **Approve** or **Decline**.



Enclave Manager

Test-Account2

N nithya ramakrishnan

Tasks

Tasks

Task requests that need Administrator approval. For example, node enrolment, application domain whitelist, build approval, and certificate issuance.

PENDING REQUESTS 1 | CLOSED REQUESTS

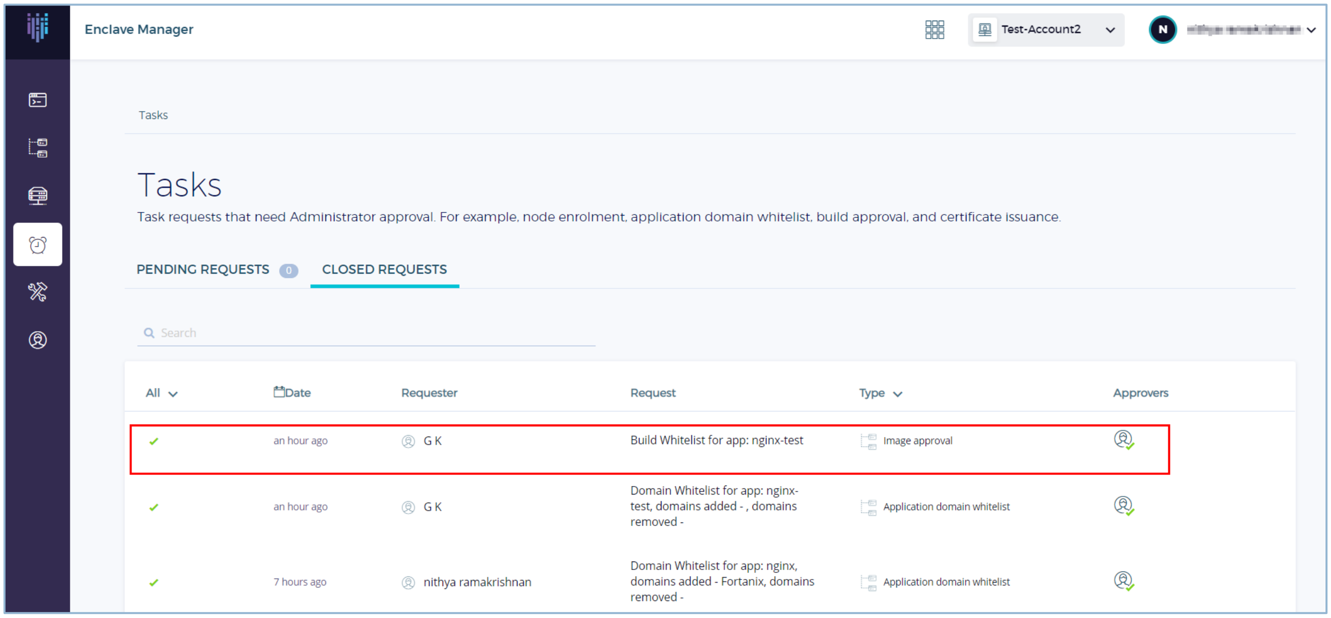
Search

Requester	Request	Type	Approvers		
G K	Build Whitelist for app: nginx-test	Image approval		DECLINE	✓ APPROVE

Rows per page: 10

FIGURE 53: TASKS FOR APPLICATION IMAGE WHITELISTING

4. Any user in the account with an Administrator or Editor role can approve an Image whitelist task.
5. Once the task is approved, click the **Close requests** tab on the same page. Your closed task will now be listed with a summary.



Tasks

Tasks

Task requests that need Administrator approval. For example, node enrolment, application domain whitelist, build approval, and certificate issuance.

All	Date	Requester	Request	Type	Approvers
✓	an hour ago	G K	Build Whitelist for app: nginx-test	Image approval	
✓	an hour ago	G K	Domain Whitelist for app: nginx-test, domains added - , domains removed -	Application domain whitelist	
✓	7 hours ago	nithya ramakrishnan	Domain Whitelist for app: nginx, domains added - Fortanix, domains removed -	Application domain whitelist	

FIGURE 54: APPROVED TASKS

7.0 WORKING IN ENCLAVE MANAGER – CONVERT YOUR APPLICATIONS

You can convert your images to run in an EnclaveOS® environment by using the Fortanix SGX Container Converter. After your images are converted, you can deploy them on your SGX capable cluster.

USING SGX CONVERTER TOOL

The SGX Container Conversion tool modifies your existing Docker containers to run in the Fortanix Enclave Manager environment. The converter pulls your existing image, converts the Application, and pushes the resulting image to the specified location. After your images are converted, you can deploy them to your SGX capable workload container.

NOTE: The conversion process does not encrypt your application. Only data that is generated at runtime – after the application is started within an SGX enclave, is protected by Fortanix Enclave Manager.

Before you begin:

Before you convert your applications, you should ensure that you fully understand the following considerations:

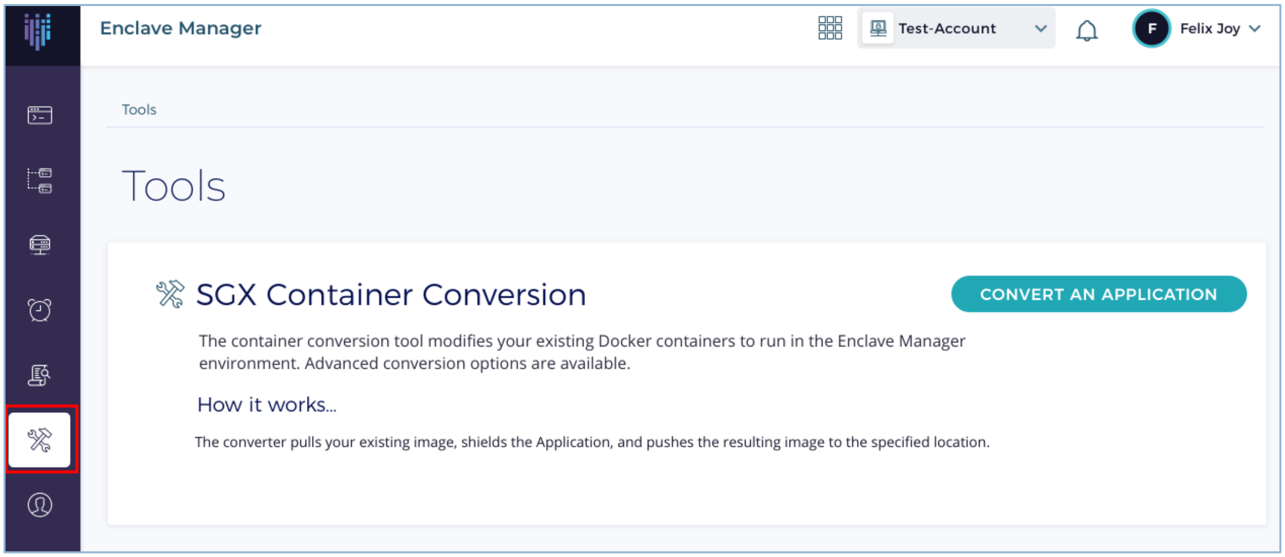
- For security reasons, secrets must be provided at runtime - not placed in the container image that you want to convert. When an app is converted and running, you can verify through attestation that the application is running in an enclave before you provide any secrets.
- Testing container environments include the following:
  - Debian 8
  - Debian 9
  - Ubuntu 16.04
  - Ubuntu 18.04
  - Java OpenJDK 8
  - Java OpenJ9 0.14

Prerequisites:

- Input image and Output image for conversion.

Steps:

1. Click the **Tools** tab in the Fortanix Enclave Manager UI.

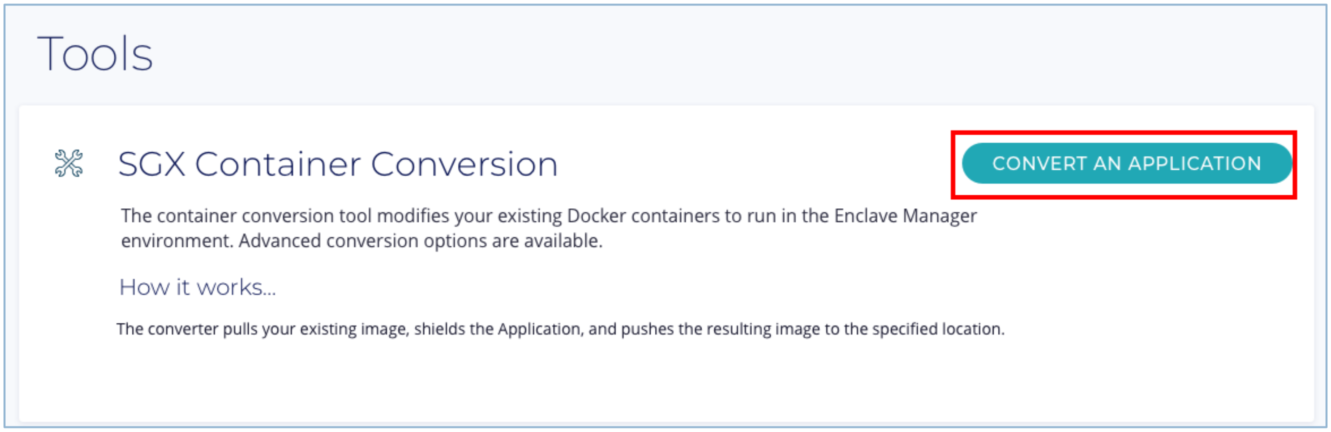


The container conversion tool modifies your existing Docker containers to run in the Enclave Manager environment. Advanced conversion options are available.

The converter pulls your existing image, shields the Application, and pushes the resulting image to the specified location.

FIGURE 55: TOOLS TAB

2. Click **CONVERT AN APPLICATION**.



Tools

SGX Container Conversion

The container conversion tool modifies your existing Docker containers to run in the Enclave Manager environment. Advanced conversion options are available.

How it works...

The converter pulls your existing image, shields the Application, and pushes the resulting image to the specified location.

FIGURE 56: CONVERT AN APPLICATION

3. In the **SGX container conversion** form, fill all the required fields:

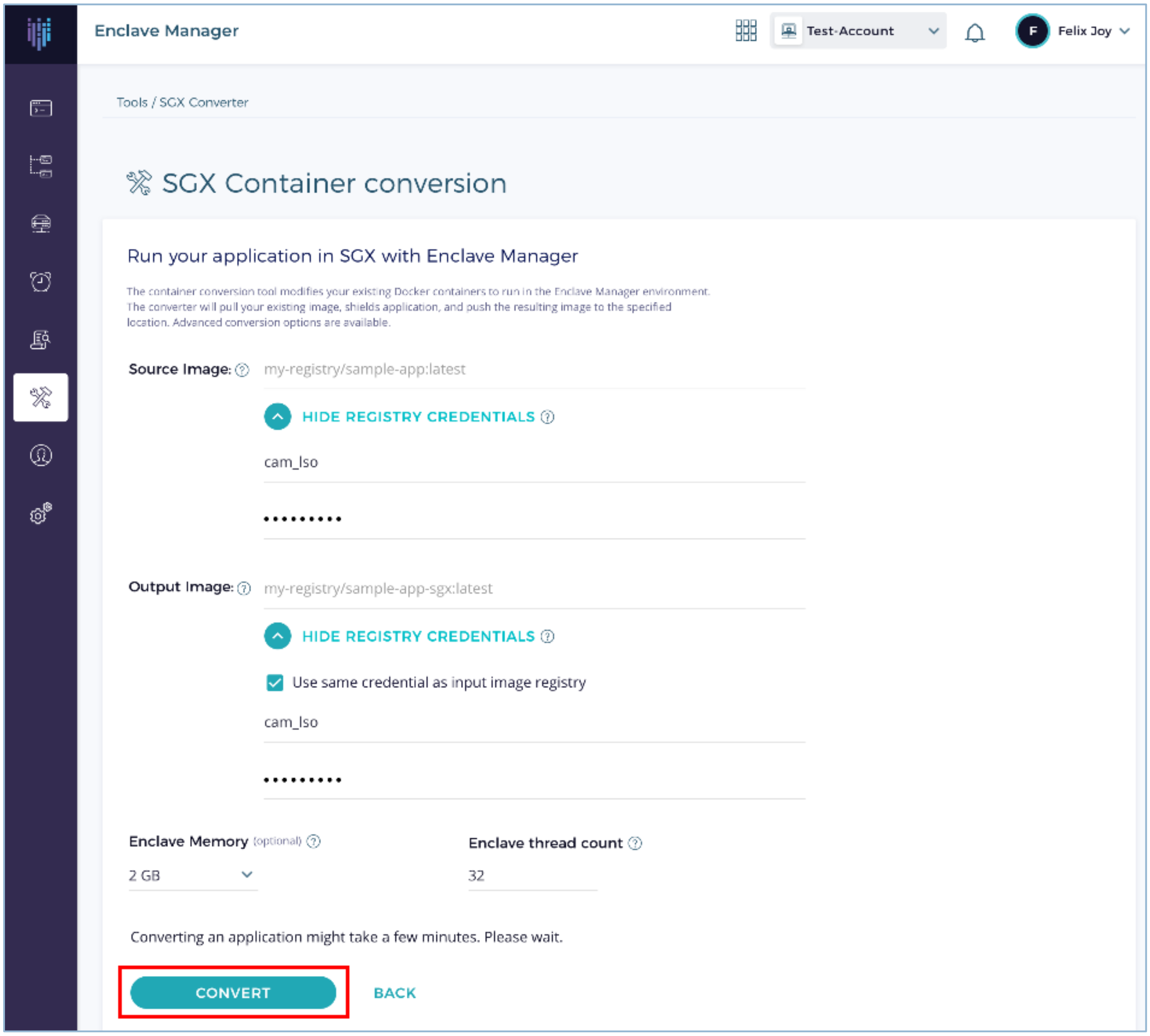
   - **Source Image**
   - **Output Image**

   Fill the optional fields:

   - **Enclave Memory**
   - **Enclave thread count**

   Enter the **REGISTRY CREDENTIALS** for **Input image name** and **Output image name**. The Registry Credentials are the credentials to access the private docker registry from which an image is going to be pulled or pushed. If the private docker registry is same for the input image and the output image, then select the check box **Use same credential as input image registry** in the **Output image name.**

4. Click **Convert** to convert the image.



SGX Container conversion

Run your application in SGX with Enclave Manager

The container conversion tool modifies your existing Docker containers to run in the Enclave Manager environment. The converter will pull your existing image, shields application, and push the resulting image to the specified location. Advanced conversion options are available.

Source Image: my-registry/sample-app:latest

HIDE REGISTRY CREDENTIALS

cam_lso

•••••••••

Output Image: my-registry/sample-app-sgx:latest

HIDE REGISTRY CREDENTIALS

☑ Use same credential as input image registry

cam_lso

•••••••••

Enclave Memory (optional): 2 GB

Enclave thread count: 32

Converting an application might take a few minutes. Please wait.

CONVERT BACK

FIGURE 57: CONVERT THE IMAGE

5. Once the image is converted, it will show up in the Output Image Path that you provided.

CONVERTING JAVA APPLICATIONS

When you convert Java-based applications, there are a few extra requirements and limitations.

When you convert Java applications using the Fortanix Enclave Manager UI, you can select `Java–Mode`. To convert Java apps by using the API, keep the following limitations and options in mind.

Limitations:

- The recommended maximum enclave size for Java apps is 4 GB. Larger enclaves might work but can experience degraded performance.
- The recommended heap size is less than the enclave size. We recommend removing any `–Xmx` option to decrease the heap size.
- The following Java libraries have been tested:
  - MySQL Java Connector
  - Crypto (`JCA`)
  - Messaging (`JMS`)
  - Hibernate (`JPA`)

Options:

To use the `Java-Mode` conversion, modify your Docker file to supply the following options. In order for the Java conversion to work, you must set all of the variables as they are defined in this section.

- Set the environment variable `MALLOC_ARENA_MAX` equal to 1.

```
MALLOC_ARENA_MAX=1
```

- If you are using the `OpenJDK JVM`, set the following options.

```
-XX:CompressedClassSpaceSize=16m
-XX:-UsePerfData
-XX:ReservedCodeCacheSize=16m
-XX:-UseCompiler
-XX:+UseSerialGC
```

- If you are using the `OpenJ9 JVM`, set the following options.

```
-Xnojit
–Xnoaot
```

8.0 EXAMPLE - RUNNING AN APPLICATION

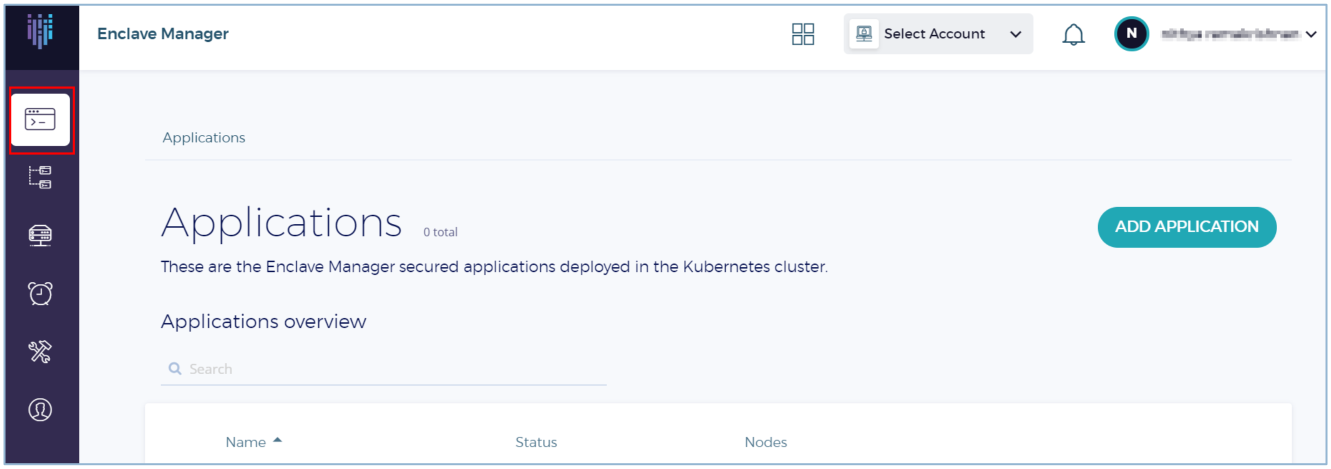
The Fortanix Enclave Manager environment is designed with the goal of protecting any application. Performance of a code executing in an Intel® SGX enclave is similar to performance of the same code.

RUNNING AN NGINX APPLICATION

Prerequisites: An NGINX application should be created.

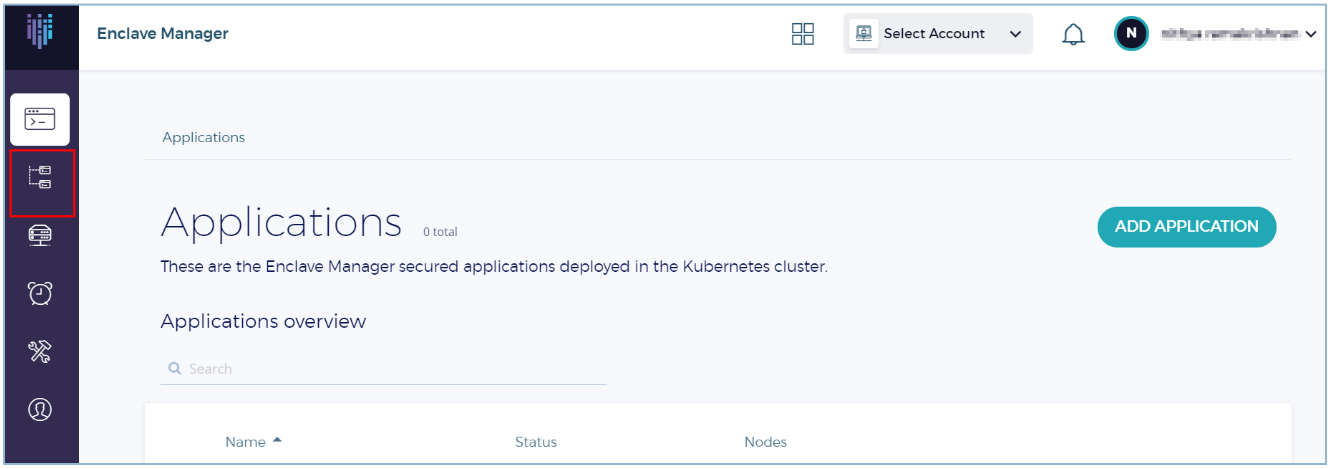
Steps:

1. Click the **Apps** tab in the Fortanix Enclave Manager UI.



These are the Enclave Manager secured applications deployed in the Kubernetes cluster.

2. Add an NGINX application. *See section "Add an Application" for more information.*
3. Whitelist the domain for the NGINX application. *See section "Domain Whitelisting" for more information.*
4. Click the **Images** tab in the Fortanix Enclave Manager UI.



These are the Enclave Manager secured applications deployed in the Kubernetes cluster.

5. Create an image of the NGINX application by providing a proper tag. *See section "Create an image for an Application" for more information*.
6. Whitelist the image for the NGINX application. *See section "Application Image Whitelisting" for more information*.
7. Create a Kubernetes pod specification similar to the below URL: https://cloud.ibm.com/docs/services/Registry?topic=RegistryImages-datashield-nginx_starter#datashield-nginx_starter
8. Run this image by using the below command:

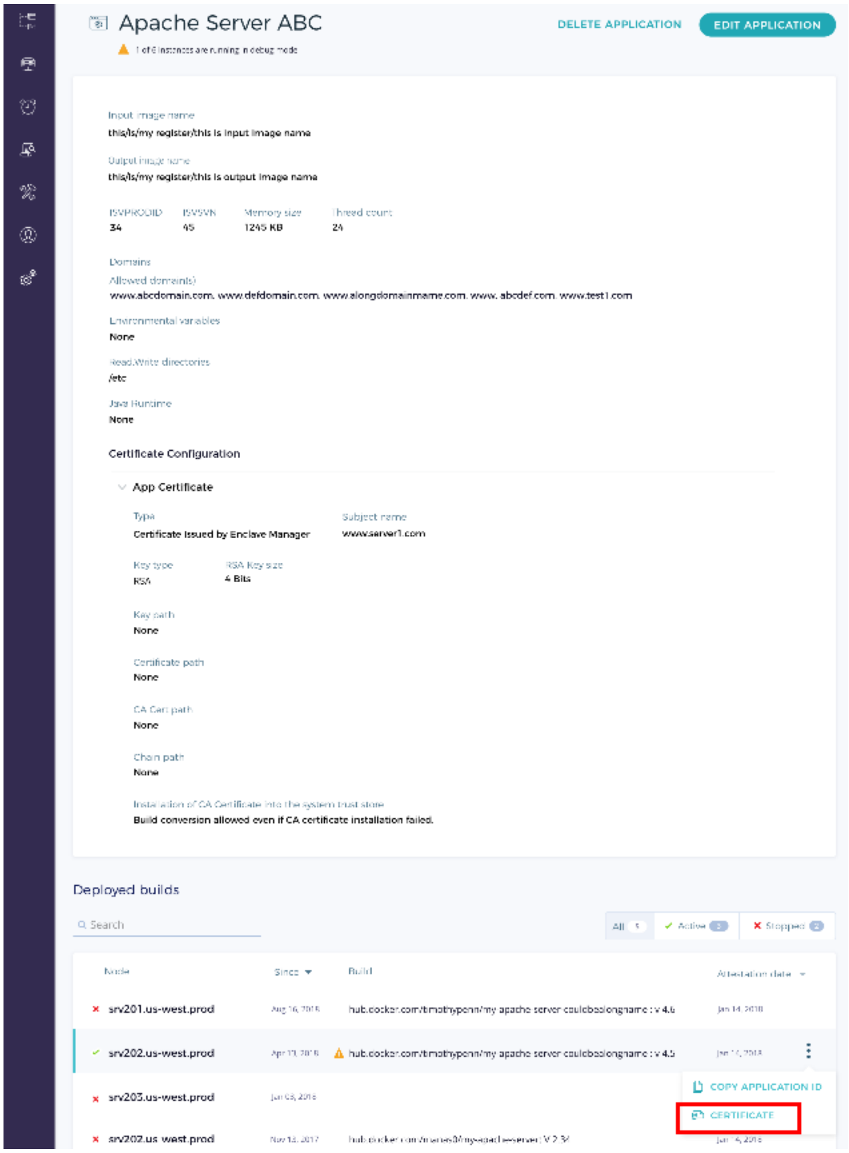
```
$ docker run -it -v /var/run/aesmd:/var/run/aesmd --device /dev/isgx
:/dev/isgx --device /dev/gsgx:/dev/gsgx   --network host -e NODE_AGE
NT_BASE_URL=http://127.0.0.1:9092/v1 <registery>/flask-hello-sgx:lat
est
```

9. Click the **Apps** tab in the Fortanix Enclave Manager UI to see the list of applications added.
10. Using the Search bar, search for the NGINX application you created.
11. Click the application and verify that there is a running image associated with it and displayed with the application in the detailed view of the application.
12. Verify that the NGINX application can serve HTML requests.

DOWNLOAD ENCLAVE MANAGER APPLICATION CERTIFICATE

To download the EM application certificate:

1. Click an application from the **Applications** table, to switch to the detailed view of an application.
2. In the application's detailed view, the nodes that are associated with the application can be seen in the table at the bottom of the page.
3. Click the three dots icon for a node and select **CERTIFICATE** to download the application certificate.



Apache Server ABC

1 of 6 instances are running in debug mode

Input image name
this/is/my register/this is input image name

Output image name
this/is/my register/this is output image name

ISVPRODID	ISVSVN	Memory size	Thread count
34	45	1245 KB	24

Domains
Allowed domain(s)
www.abcdomain.com, www.defdomain.com, www.alongdomainmame.com, www. abcdef.com, www.test1.com

Environmental variables
None

Read.Write directories
/etc

Java Runtime
None

Certificate Configuration

App Certificate

Type
Certificate Issued by Enclave Manager

Subject name
www.server1.com

Key type
RSA

RSA Key size
4 Bits

Key path
None

Certificate path
None

CA Cert path
None

Chain path
None

Installation of CA Certificate into the system trust store
Build conversion allowed even if CA certificate installation failed.

Deployed builds

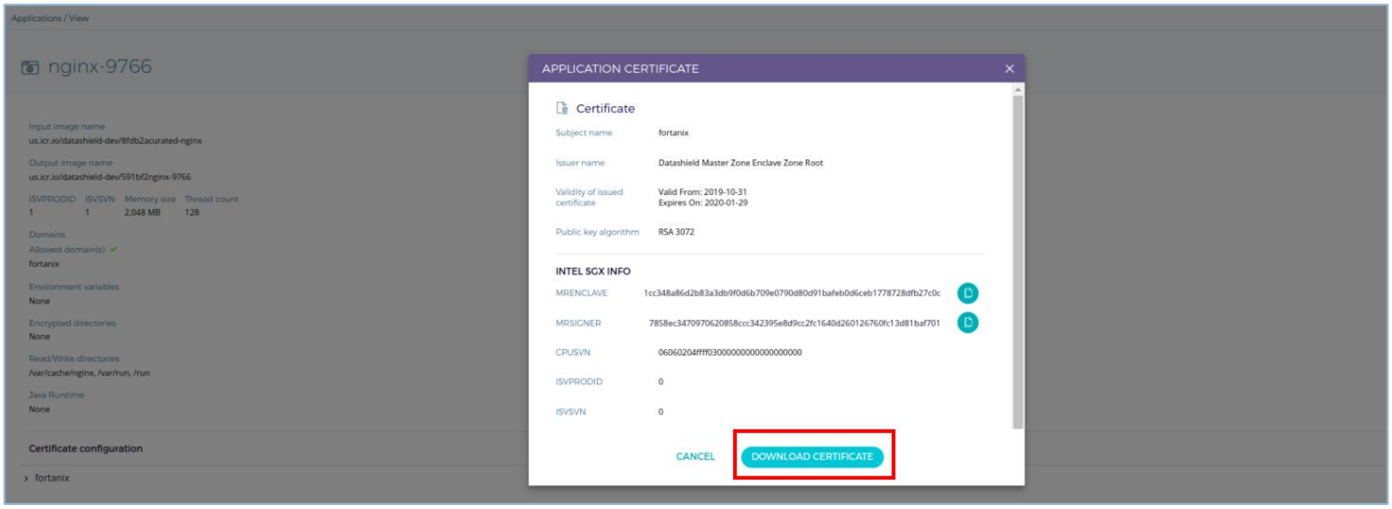
Search

All 5 | ✓ Active 3 | ✗ Stopped 2

	Node	Since	Build	Attestation date
✗	srv201.us-west.prod	Aug 16, 2018	hub.docker.com/timothypenn/my apache server couldbealongname : v 4.6	Jan 14, 2018
✓	srv202.us-west.prod	Apr 13, 2018	hub.docker.com/timothypenn/my apache server couldbealongname : v 4.5	Jan 14, 2018
✗	srv203.us-west.prod	Jan 03, 2016		
✗	srv202.us west.prod	Nov 13, 2017	hub.docker.com/[illegible]/my-apacheserver: V 2.34	Jan 14, 2018

FIGURE 58: NODES ASSOCIATED WITH AN APP

4. Click the **DOWNLOAD CERTIFICATE** button in the Application Certificate dialog to download the application certificate.



nginx-9766

Input image name
us.icr.io/datashield-dev/8fdb2acurated-nginx

Output image name
us.icr.io/datashield-dev/591bf2nginx-9766

ISVPRODID	ISVSVN	Memory size	Thread count
1	1	2,048 MB	128

Domains
Allowed domain(s) ✓
fortanix

Environment variables
None

Encrypted directories
None

Read/Write directories
/var/cache/nginx, /var/run, /run

Java Runtime
None

Certificate configuration

› fortanix

APPLICATION CERTIFICATE

Certificate

Subject name	fortanix
Issuer name	Datashield Master Zone Enclave Zone Root
Validity of issued certificate	Valid From: 2019-10-31 Expires On: 2020-01-29
Public key algorithm	RSA 3072

INTEL SGX INFO

MRENCLAVE	1cc348a86d2b83a3db9f0d6b709e0790d80d91bafeb0d6ceb1778728dfb27c0c
MRSIGNER	7858ec3470970620858ccc342395e8d9cc2fc1640d260126760fc13d81baf701
CPUSVN	06060204ffff03000000000000000000
ISVPRODID	0
ISVSVN	0

FIGURE 59: DOWNLOAD APP CERT

HOW TO KNOW IF YOUR APPLICATION IS RUNNING IN AN SGX ENCLAVE

Log in to your Fortanix Enclave Manager account and navigate to the **Apps** tab which contains information of Intel SGX remove attestation for your applications in the form of a certificate. The applications enclave can be verified any time using Intel remote attestation service (IAS) to make sure that application is running in a verified enclave. For more information on the SGX Attestation process and steps, please see the guide SGX Attestation process guide.

9.0 APPLICATION'S PERFORMANCE IN AN ENCLAVE ENVIRONMENT

The Fortanix Enclave Manager environment is designed with the goal of protecting any application. Performance of a code executing in an Intel® SGX enclave is similar to performance of the same code executed outside of enclave context. However, there are some overheads associated with enclave execution. Different applications can be more or less sensitive to these overheads and can be more or less performant in the enclave environment. This document attempts to explain some of the factors affecting enclave performance, and to set some performance expectations for applications run in the Fortanix Enclave Manager environment. This information may be useful in planning a migration or in the design of new services.

CONSIDERATIONS

Enclave Memory and Paging

Most SGX-capable processors available today have 128 MB of enclave page cache ("EPC"). The EPC holds pages that are actively available for use by an enclave. In a 128 MB EPC, 93.5 MB of memory is available for applications. The remainder of EPC holds integrity metadata. Enclaves can access larger amounts of memory through a demand-paging mechanism, but there is a performance penalty associated with paging. Applications will perform best in the Fortanix Enclave Manager environment if their working set is smaller than 90 MB. This memory limitation is a property of SGX. If more memory is available to SGX enclaves in the future, Fortanix Enclave Manager will be able to use the additional memory.

Enclave Entry/Exit Overhead

Entering or exiting an SGX enclave incurs a substantial time delay. Additionally, an entry/exit flushes certain CPU caches, which can have a performance impact due to subsequent cache misses. An enclave exit and re-entry can occur for the following reasons:

- To allow the enclave to interact with external resources (for example, sending data from the enclave over the network)
- To switch to a different thread of execution in the enclave application
- To service CPU interrupts

The Fortanix Enclave Manager environment employs various strategies to reduce the number of enclave exit/entry events, and additional optimizations will be implemented over time. However, the general issue of I/O overhead across the security boundary will remain.

GUIDANCE

The best-performing applications for the enclave environment will exhibit modest memory working set size and infrequent I/O operations relative to the amount of computation performed. In some situations, performance may be less important than security characteristics, and in these cases, it is also advisable to consider running the application in the Fortanix Enclave Manager environment.

Since every application is different, the best way to evaluate the performance of an application in the Fortanix Enclave Manager environment is through empirical measurement. However, answering the following questions may help to evaluate whether an application is a good candidate:

- What request rate (queries per second) is expected for the application? If the request rate is on the order of 1000 QPS or less, the application may be a good fit. If the request rate is 10k QPS or more, that suggests the application may be I/O limited in Fortanix Enclave Manager.
- What kind of processing does the application do for each request? Applications that perform relatively simple data processing tasks (for example, a compatibility service that rewrites requests from a stable external API format to an unstable backend API format) are unlikely to do enough computation to offset the cost of transferring data in or out of the enclave.
- What kind of internal data structures does the application use in handling the request? Applications that are already dominated by a relatively long latency (for example, a database where the request pattern is expected to go to disk most of the time) may be a good fit. Conversely, applications that make random accesses to an in-memory data structure that does not fit in EPC (for example, an in-memory key-value store) will exhibit degraded performance in the Fortanix Enclave Manager environment.

SAMPLE APPLICATIONS

Timestamp Server (Python)

This application is a custom RFC3161-compliant (mostly) timestamp server written in Python, using the Flask, ctypescrypto, and rfc3161ng packages.

Native Performance	Enclave Performance	Ratio Enclave: Native
106 QPS	74 QPS	0.70

AcmeAir Airline Booking (Java)

This is a sample Java web application, available at https://github.com/blueperf/acmeair-monolithic-java. The application uses a MongoDB database. For this benchmark, the MongoDB database was not running in an enclave.

Native Performance	Enclave Performance	Ratio Enclave: Native
89 QPS	70 QPS	0.79

CSV Processor (C)

This application reads a CSV file, parses it, and performs asymmetric encryption/decryption of data in the CSV file.

Native Runtime	Enclave Runtime	Ratio Enclave: Native
3.33236 s	3.424258 s	0.97

10.0 DOCUMENT INFORMATION

DOCUMENT LOCATION

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

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.