Fortanix®

User Guide

FORTANIX CONFIDENTIAL COMPUTING MANAGER –DOMAIN AND IMAGE APPROVAL

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 approve an application domain and 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.

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 DOMAIN APPROVAL

An application whose domain is approved will get a TLS Certificate from Fortanix Confidential Computing 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 approved, the image will run but it will not be issued any TLS certificate from Fortanix Confidential Computing Manager.

Prerequisites:

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

Steps:

1. Add an application with a domain as described in *Add an application*.
2. After the application is created successfully, click the **Tasks** tab in UI for approving a domain approval task.

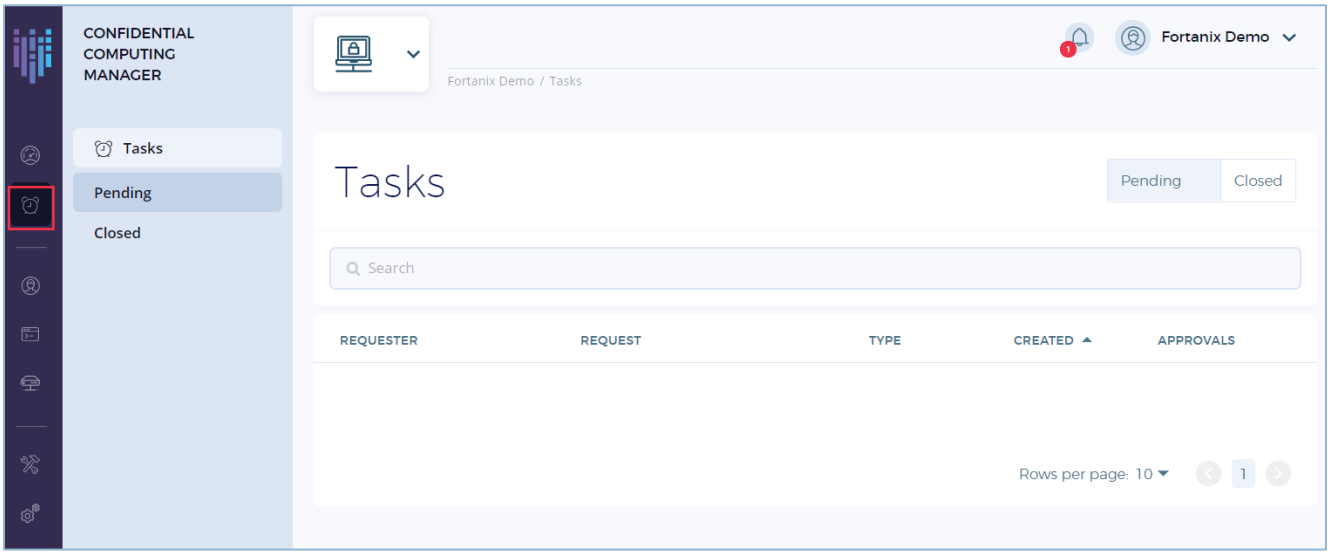

FIGURE 1: TASKS TAB FOR DOMAIN APPROVAL

3. A domain approval task will be created for the application. Click the task and click **Approve** to approve the task (**Figure 2**).

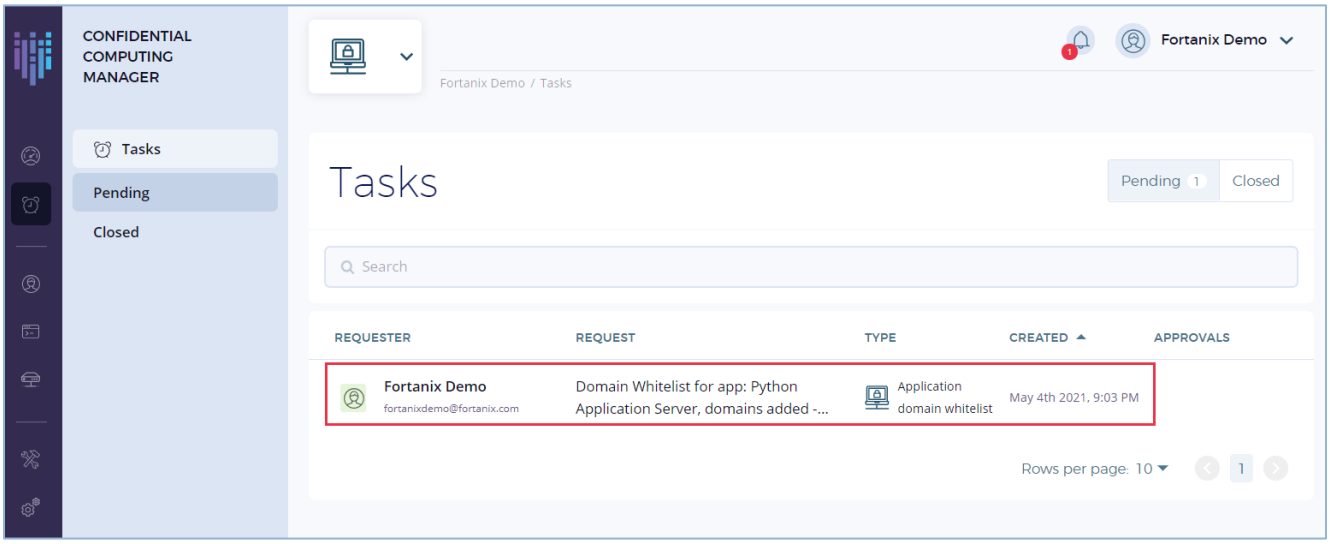

FIGURE 2: TASKS FOR ENCLAVE OS APP DOMAIN APPROVAL

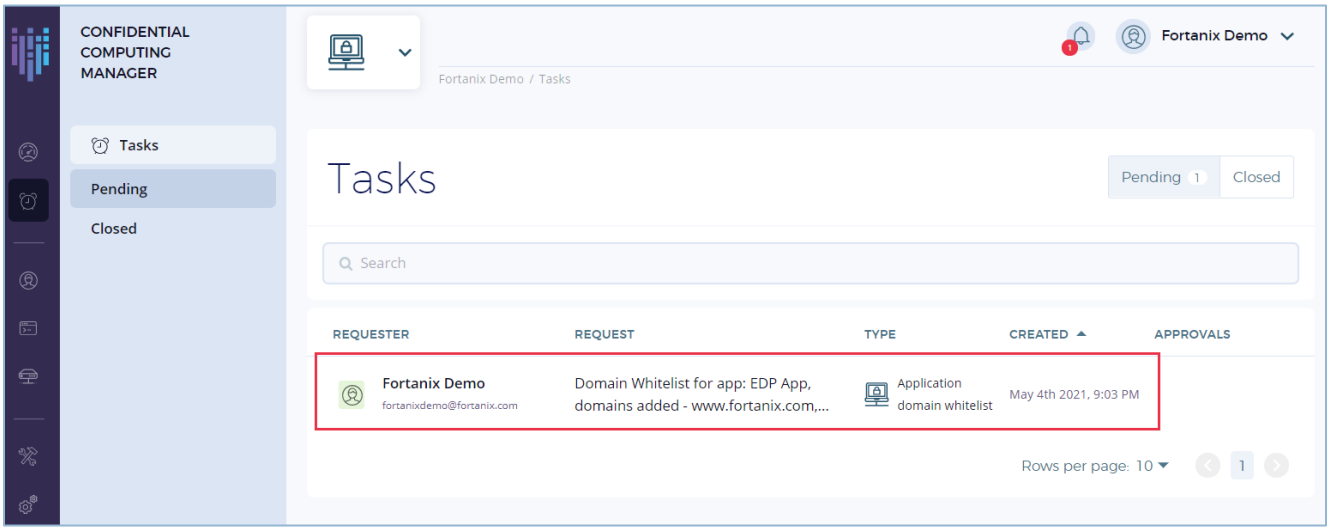

FIGURE 3: TASK FOR EDP APP DOMAIN APPROVAL

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

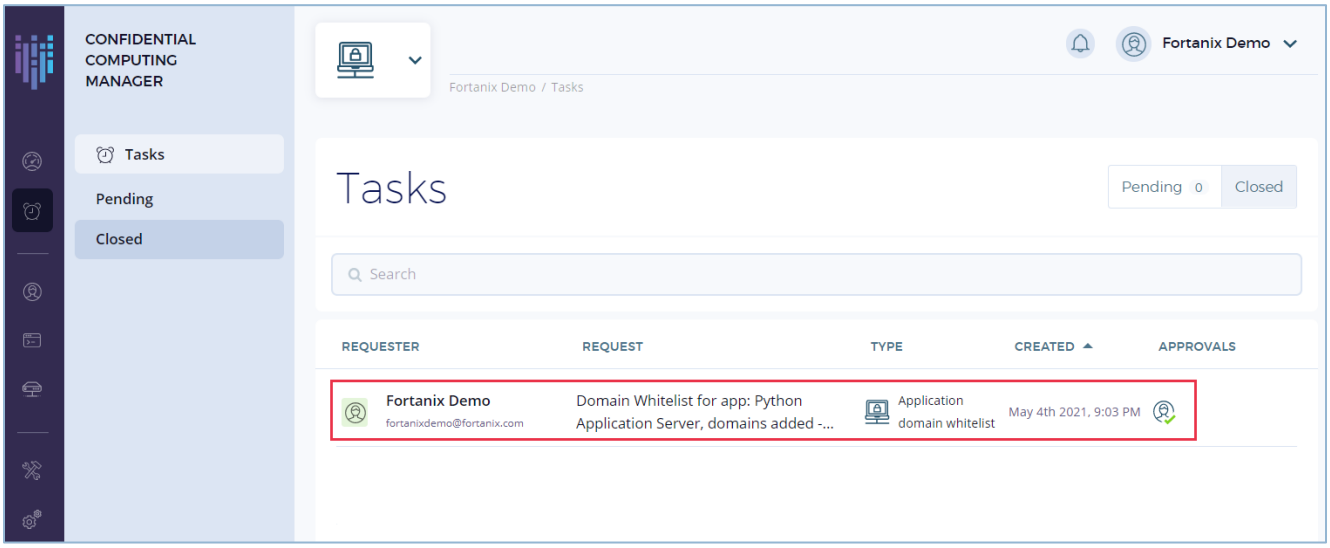

FIGURE 4: APPROVE EOS TASKS

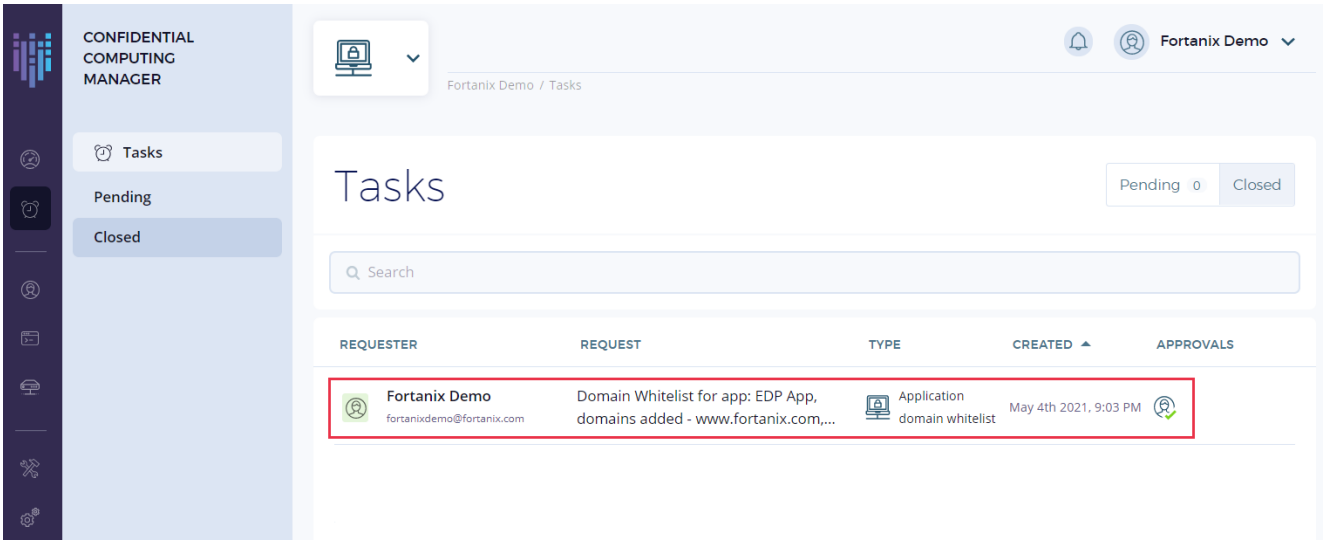

FIGURE 5: APPROVE EDP TASKS

5.0 IMAGE APPROVAL FOR ENCLAVE OS AND EDP APPLICATIONS

After an image is created and when an application runs from this converted image, the application will try to contact Fortanix Confidential Computing Manager and ask for a TLS Certificate. If the image is not approved, it will run but the Fortanix Confidential Computing Manager will deny this TLS Certificate. If the CCM 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 approved.

When an image is approved, it is added to the list of pending requests in the **Tasks** tab of the Fortanix Confidential Computing 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 *Create an Image for an Application*.
2. After the image is created successfully, click the **Tasks** tab in UI for approving the application image approval task.

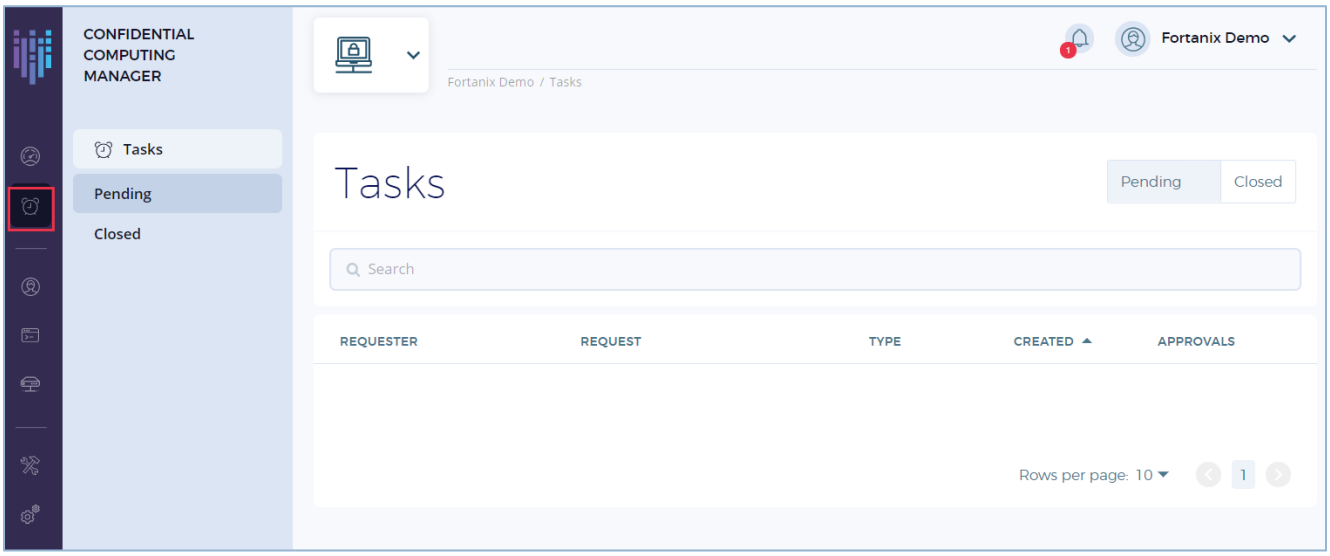

FIGURE 6: TASK TAB FOR IMAGE APPROVAL

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

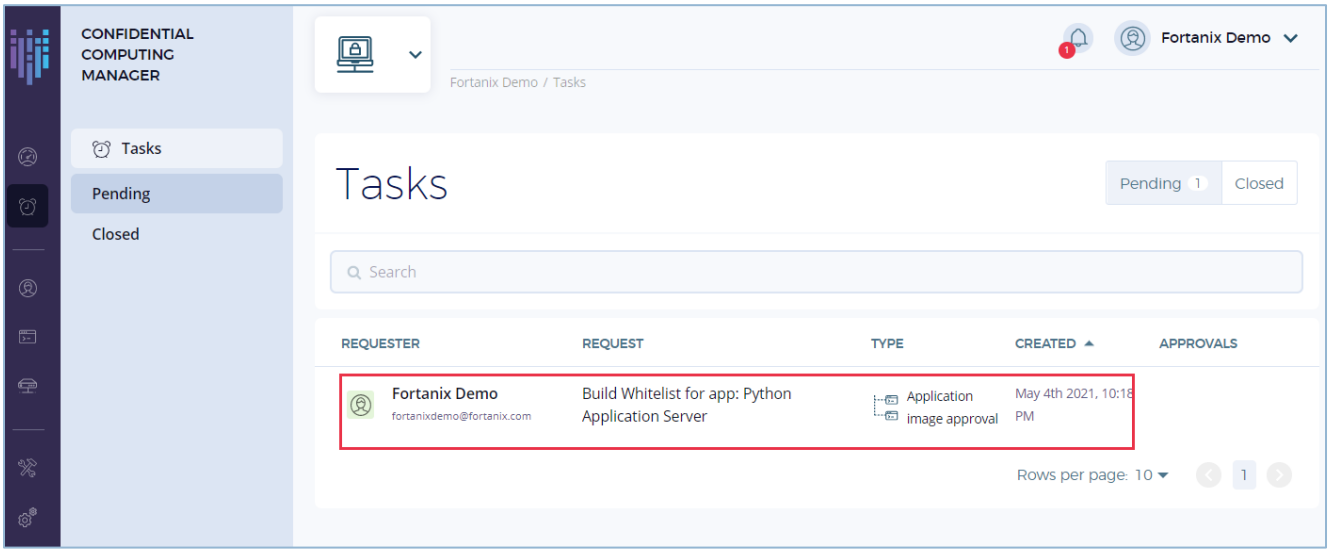

FIGURE 7: TASKS FOR ENCLAVE OS APP IMAGE APPROVAL

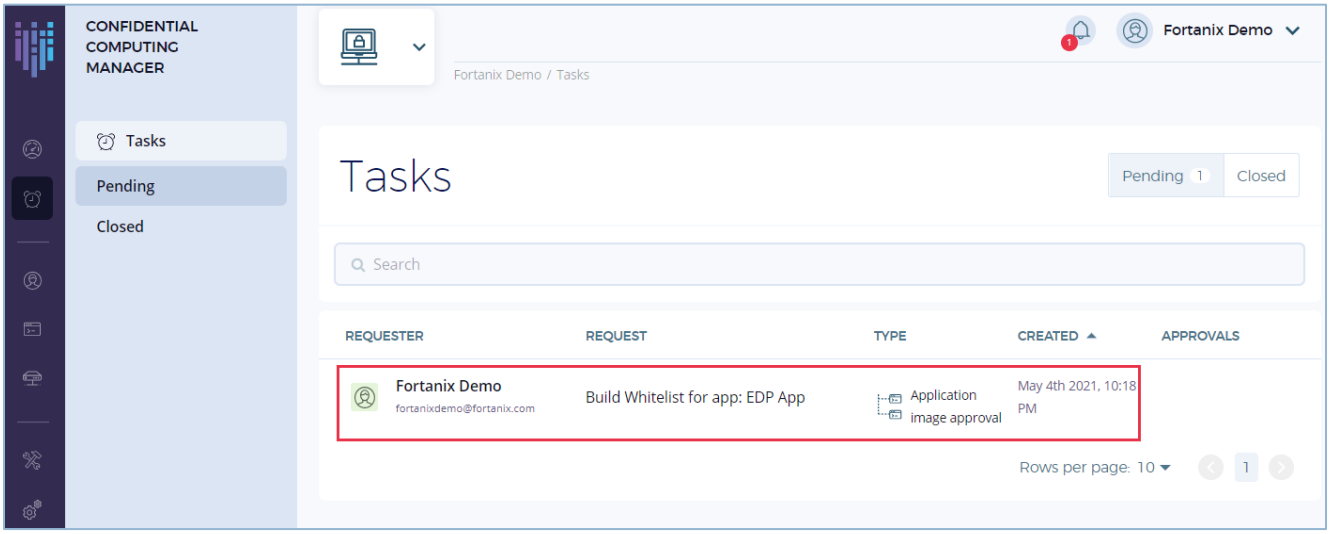

FIGURE 8: TASKS FOR EDP APP IMAGE APPROVAL

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

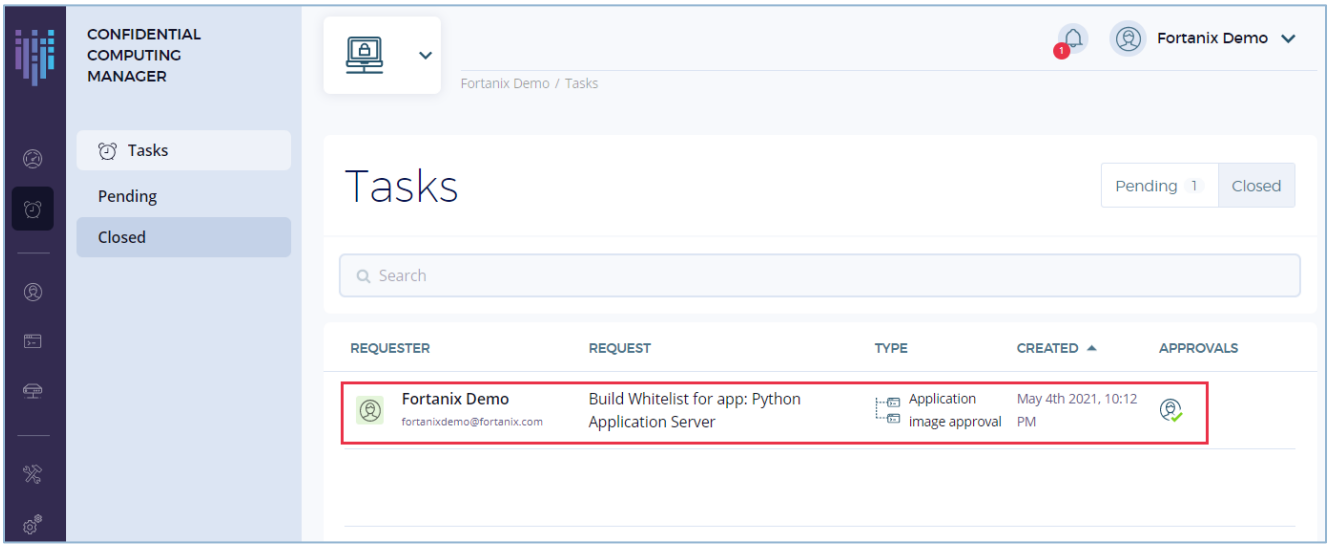

FIGURE 9: EOS IMAGE APPROVED TASKS

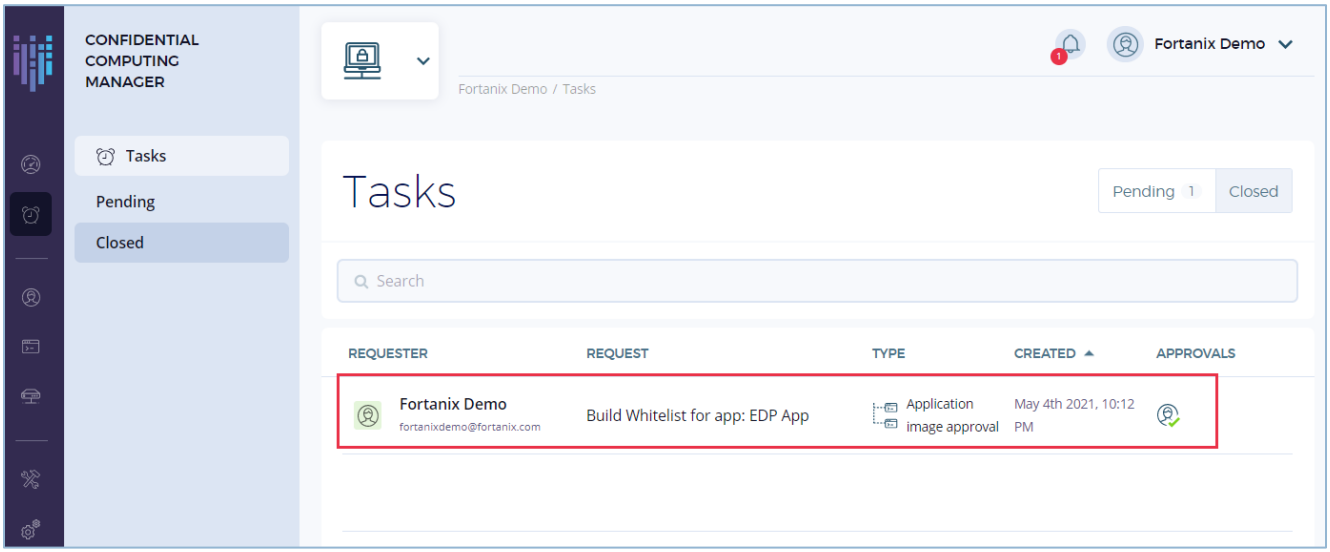

FIGURE 10: EDP IMAGE APPROVED TASKS

6.0 DOCUMENT INFORMATION

6.1 DOCUMENT LOCATION

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

https://support.fortanix.com/hc/en-us/articles/360043092812-User-s-Guide-Domain-and-Application-Image-Approval

6.2 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