Fortanix®

User Guide

FORTANIX CONFIDENTIAL COMPUTING MANAGER –AZURE ACTIVE DIRECTORY AUTHENTICATION

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 configure accounts such that they can authenticate using the Azure Active Directory (Azure AD) of an Azure tenant.

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 SETTING AZURE ACTIVE DIRECTORY AUTHENTICATION

This feature allows users to configure accounts such that they can authenticate using the Azure Active Directory (Azure AD) of an Azure tenant. For this authentication, the OpenID connect over OAuth 2.0 (OAuth) is used as the authentication protocol.

4.1 PREREQUISITE

Users will need to sign up for Fortanix CCM or must be invited to a Fortanix CCM account before they can log in to that account using Azure AD.

4.2 ENABLE AZURE AD

To add Azure AD as the OAuth identity provider:

1. Go to the **Settings**  page in Fortanix Confidential Computing Manager and click the **Authentication** tab.

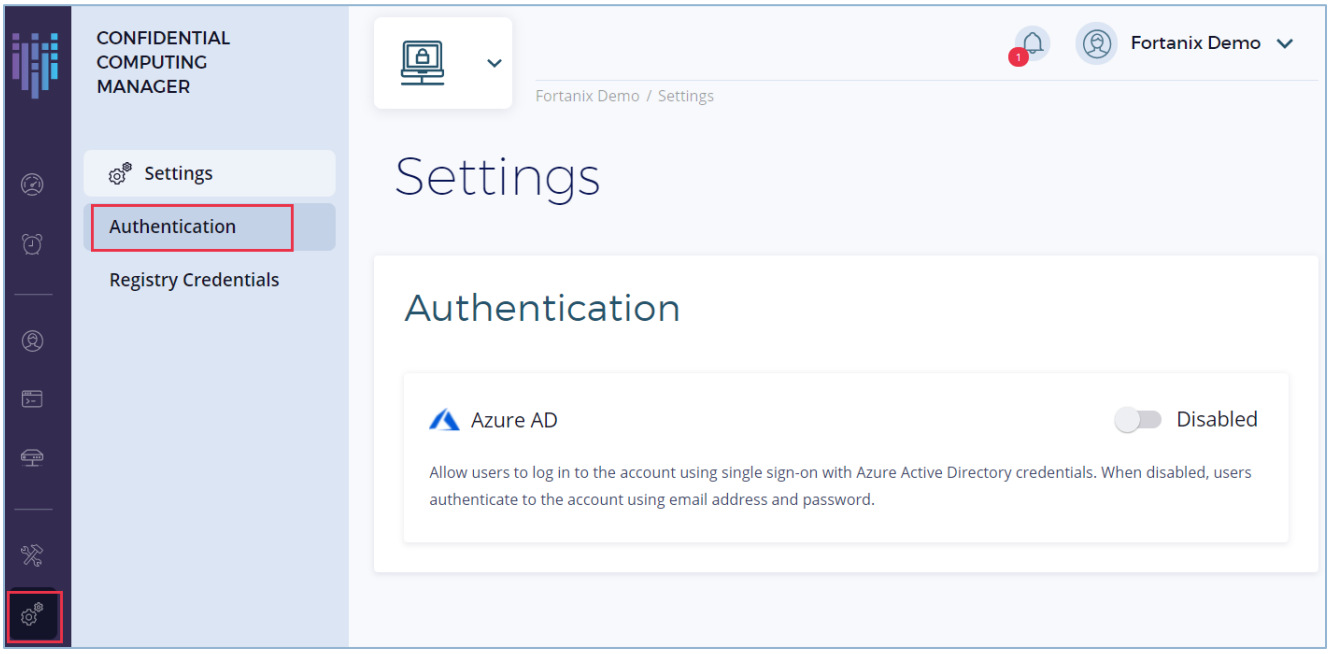

FIGURE 1: SETTINGS PAGE

2. In the Authentication page, enable the toggle for **Azure AD** to allow users to log in to the Fortanix CCM account and authenticate using single sign-on with Azure AD credentials. Click **SAVE** to save this setting.

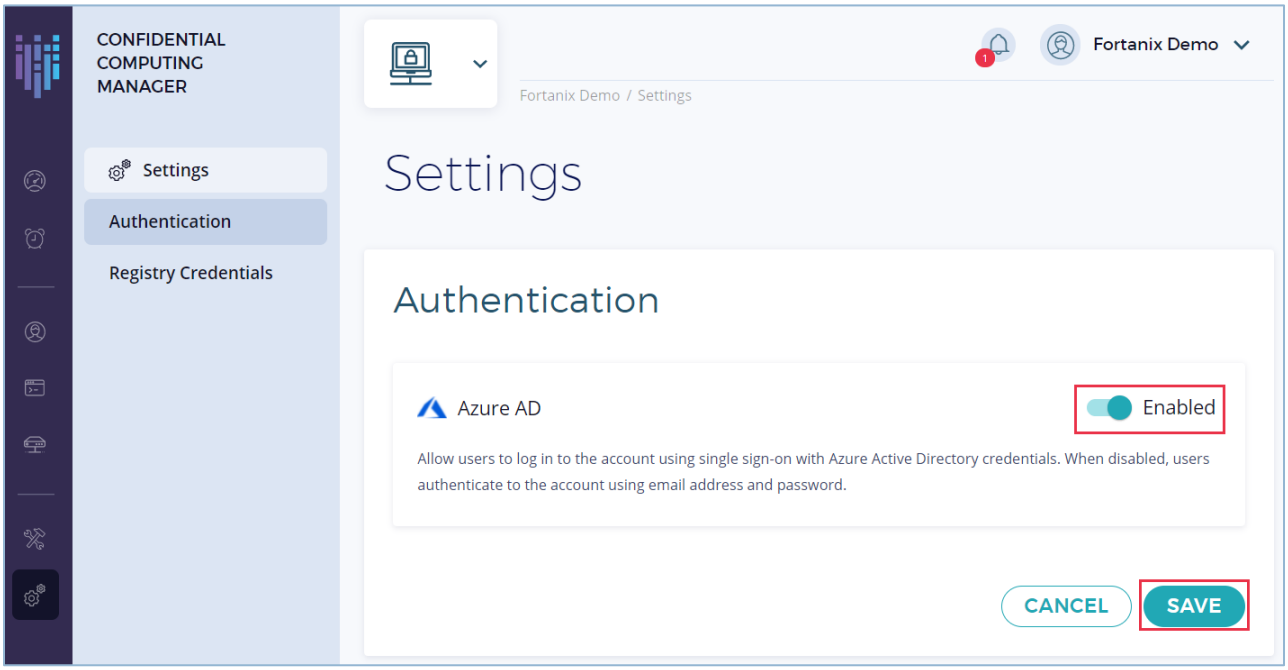

FIGURE 2: ENABLE AZURE AD

3. When the toggle is disabled, users will not be able to authenticate using Azure AD credentials. They can still authenticate to their Fortanix CCM account using the email address and password provided during user signup.
4. Now when the user logs in to Fortanix CCM in the next session, there will be two options shown on the login screen:
    a. Log in with Azure AD (with SSO)
    b. Log in with Password (Without SSO)

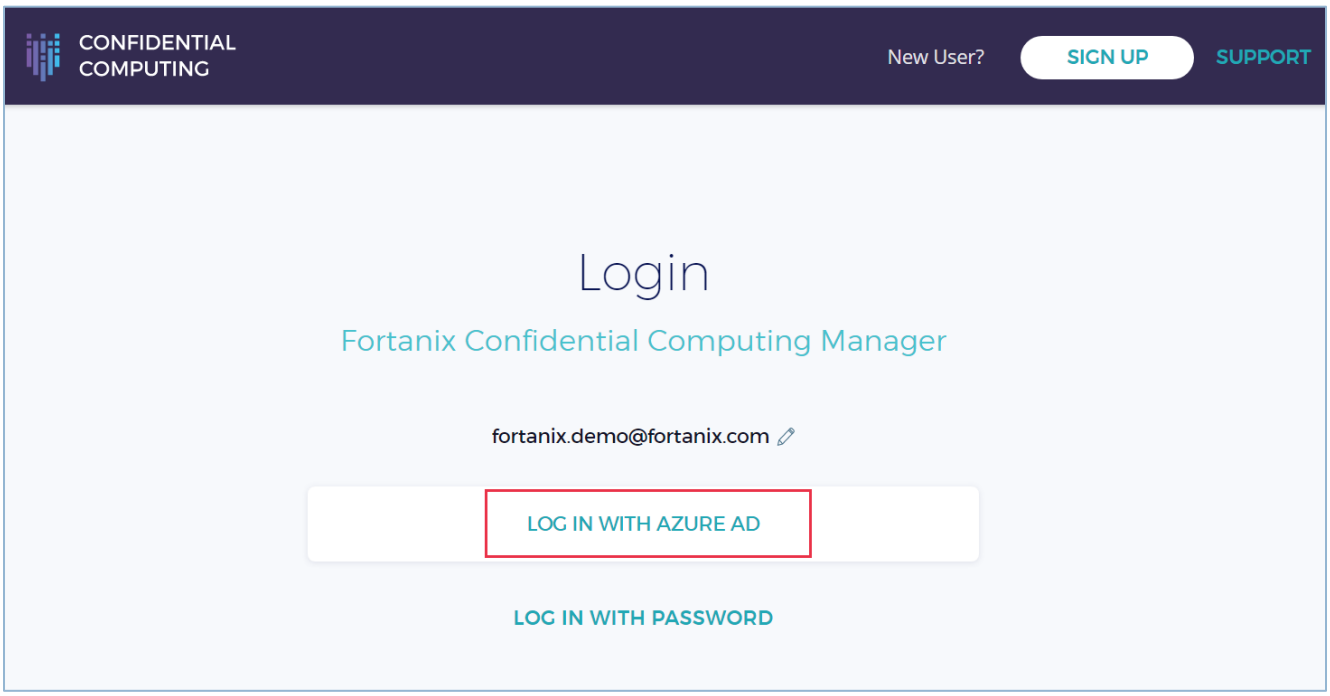

FIGURE 3: LOG IN WITH SSO

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/360059103732-User-s-Guide-Azure-Active-Directory-Authentication

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