Fortanix®

Integration Guide

USING DATA SECURITY MANAGER WITH RSA SECURE ID ACCESS

VERSION 1.0

Fortanix, Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052| United States of America | +1 (650) 943-2484 |
info@fortanix.com | www.fortanix.com

TABLE OF CONTENTS

1.0 INTRODUCTION

This article describes how to integrate **Fortanix Data Security Manager (DSM)** with **RSA SecurID Access** using SAML **Relying Party** and **SSO Agent** configuration. It also contains the information that a user requires to:

- Configure RSA Cloud Authentication Service
- Configure Fortanix Data Security Manager

Relying party integrations use SAML 2.0 to integrate RSA SecurID Access as a SAML Identity Provider (IdP) to Fortanix DSM SAML Service Provider (SP).

SSO Agent integrations use SAML 2.0 technology to direct users' web browsers to Cloud Authentication Service for authentication. SSO Agents also provide Single Sign-On to other applications using the RSA Application Portal.

When integrated, the Fortanix DSM end users must authenticate with RSA SecurID Access to sign in.

2.0 ARCHITECTURE DIAGRAM

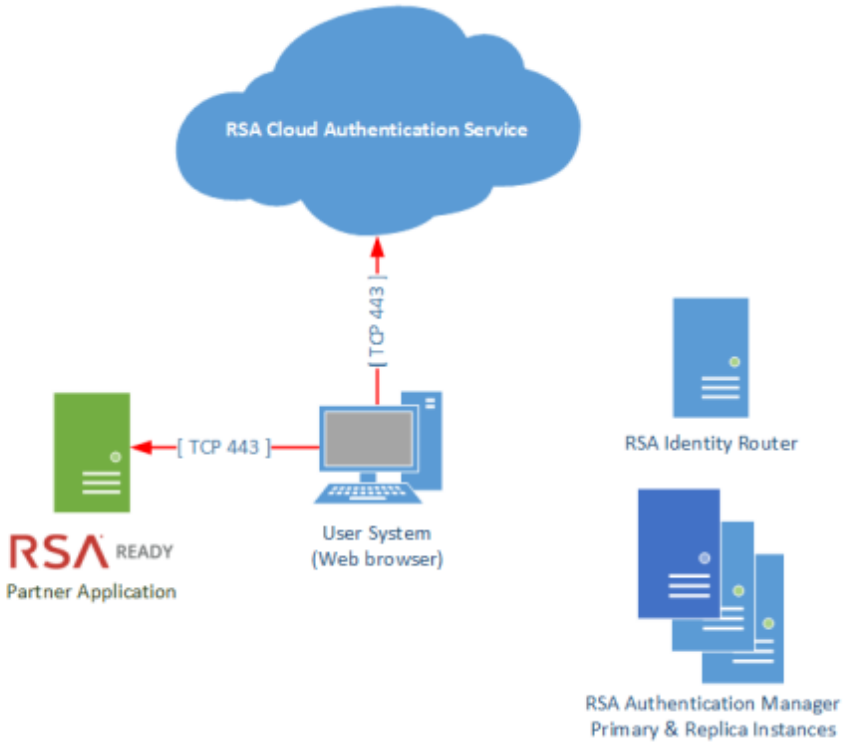

FIGURE 1: ARCHITECTURE DIAGRAM FOR FORTANIX DSM WITH RELYING PARTY INTEGRATION

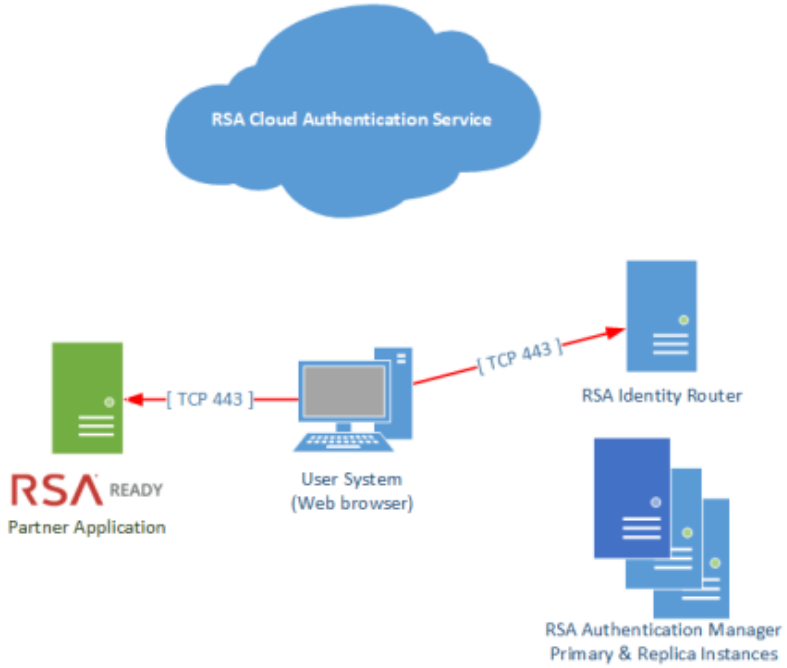

FIGURE 2: ARCHITECTURE DIAGRAM FOR FORTANIX DSM WITH SSO AGENT INTEGRATION

3.0 CONFIGURE RSA CLOUD AUTHENTICATION SERVICE - RELYING PARTY

Perform the following steps to configure RSA Cloud Authentication Service as a relying party SAML IdP to Fortanix DSM.

3.1 PROCEDURE

1. Sign in to the RSA Cloud Administration Console and browse to **Authentication Clients** > **Relying Parties** and click **Add a Relying Party**.

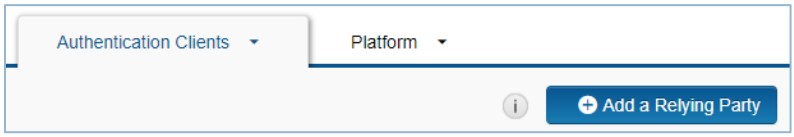

FIGURE 3: ADD RELYING PARTY

2. From the Relying Party Catalog, click **+Add** for **Service Provider** SAML.

FIGURE 4: ADD SERVICE PROVIDER SAML

3. In the **Basic Information** section, enter a name and click **Next Step**.

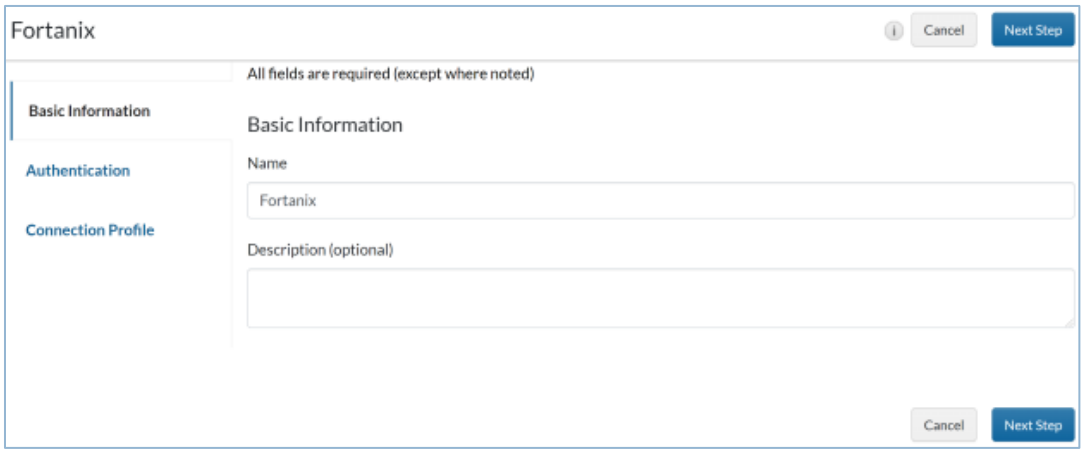

FIGURE 5: ENTER BASIC INFORMATION

4. In the **Authentication** section, do the following:
   a. Under **Authentication Details**, select **SecurID Access manages all authentication**.
   b. Select the appropriate primary and additional authentication methods.

c. Click **Next Step**.

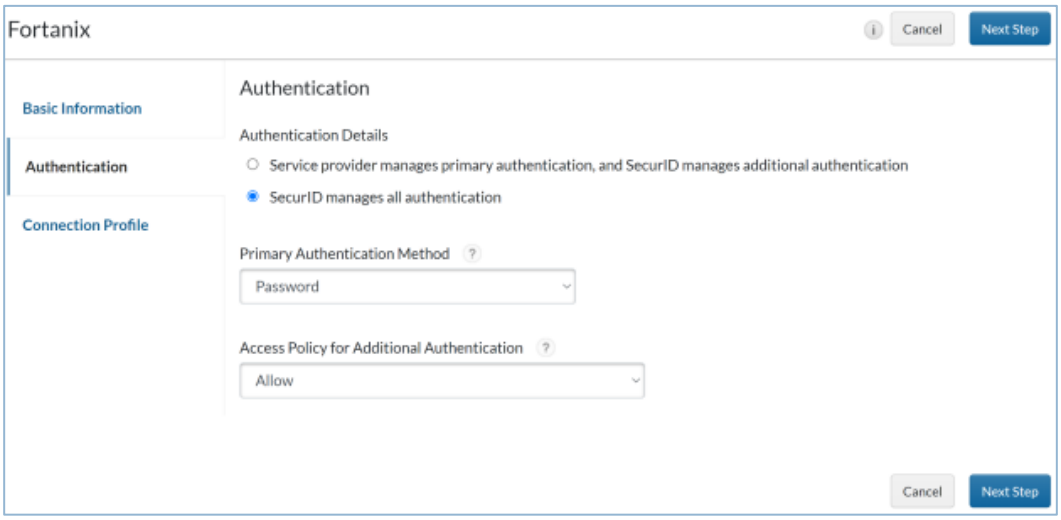

FIGURE 6: AUTHENTICATION DETAILS

5. On the next page, under **Service Provider Metadata** enter the following values:
   a. **Assertion Consumer Service (ACS) URL**: Enter the URL: https:// <fortanix_dsm_url>/saml.
   b. **Service Provider Entity ID** - Enter the URL:
      https://<fortanix_dsm_url>/saml/metadata.xml.

FIGURE 7: SERVICE PROVIDER METADATA

6. Select **Default Service Provider Entity ID** in **Audience for SAML Response** section.

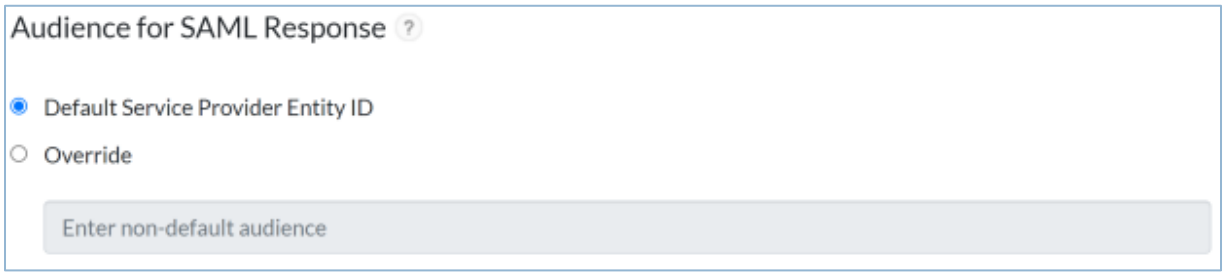

FIGURE 8: AUDIENCE FOR SAML RESPONSE

7. In the **Message Protection** section, under **SAML Response Protection**, select **IdP signs entire SAML response**.

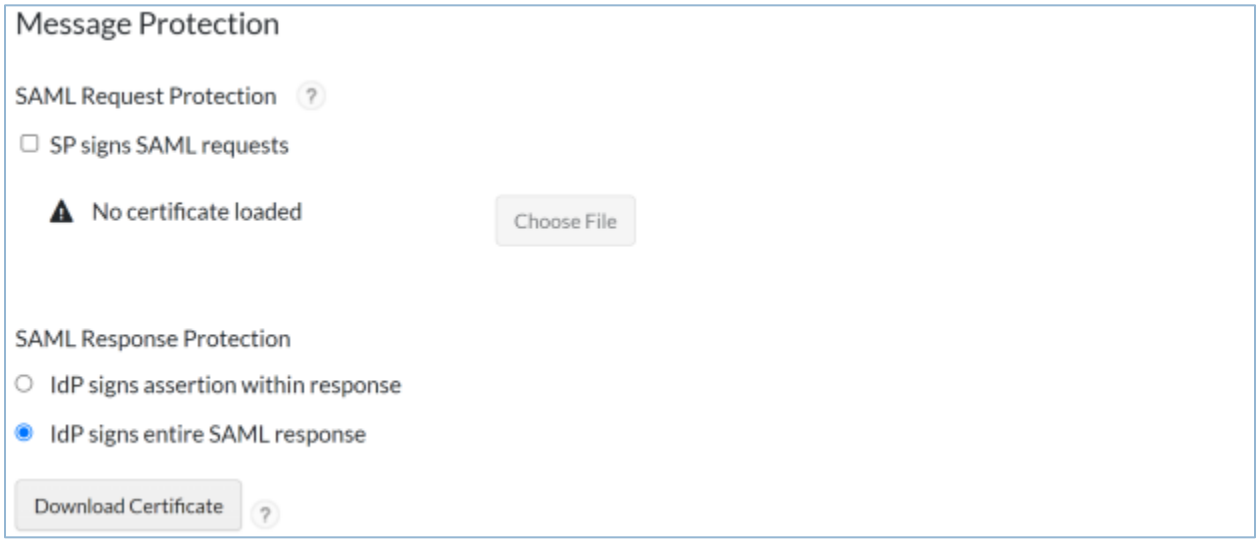

FIGURE 9: MESSAGE PROTECTION

8. Click **Show Advanced Configuration**.

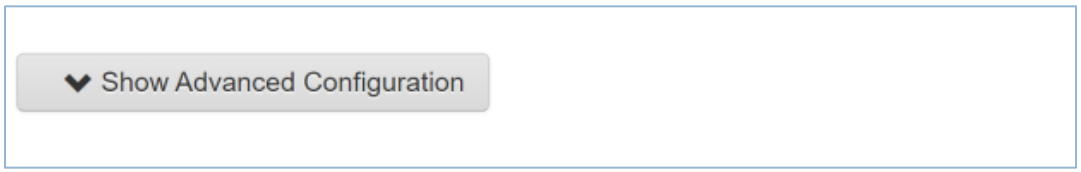

FIGURE 10: ADVANCED CONFIGURATION

9. Under the **User Identity** section, select the following:
   a. **Identifier Type**: Select Auto Detect.
   b. **Property**: Select Auto Detect.

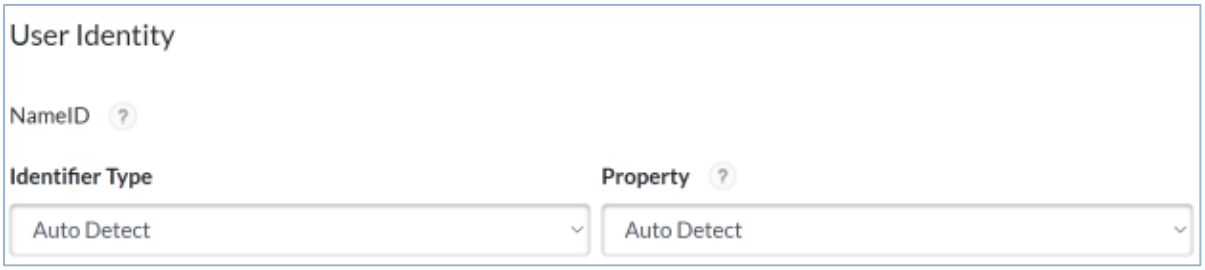

FIGURE 11: USER IDENTITY DETAILS

10. Click **Save and Finish**.
11. Click **Publish Changes** in the top left corner of the page and wait for the operation to complete.

FIGURE 12: PUBLISH CHANGES

12. On the **My Relying Parties** page, do the following:
    a. Select **Metadata** from the **Edit** drop-down list to view and download an XML file containing your RSA SecurID Access IdP's metadata.
    b. Click **Download Metadata File** in the View or Download Identity Provider Metadata page to download the file. A file named `IdpMetadata.xml` should be downloaded.

FIGURE 13: MY RELYING PARTIES

4.0 CONFIGURE RSA CLOUD AUTHENTICATION SERVICE – SSO AGENT

Perform the following steps to configure RSA Cloud Authentication Service as an SSO Agent SAML IdP to Fortanix DSM.

4.1 PROCEDURE

1. Sign in to the RSA Cloud Administration Console and browse to **Applications** > **Application Catalog**.
2. Click **Create From Template** and select **SAML Direct**.

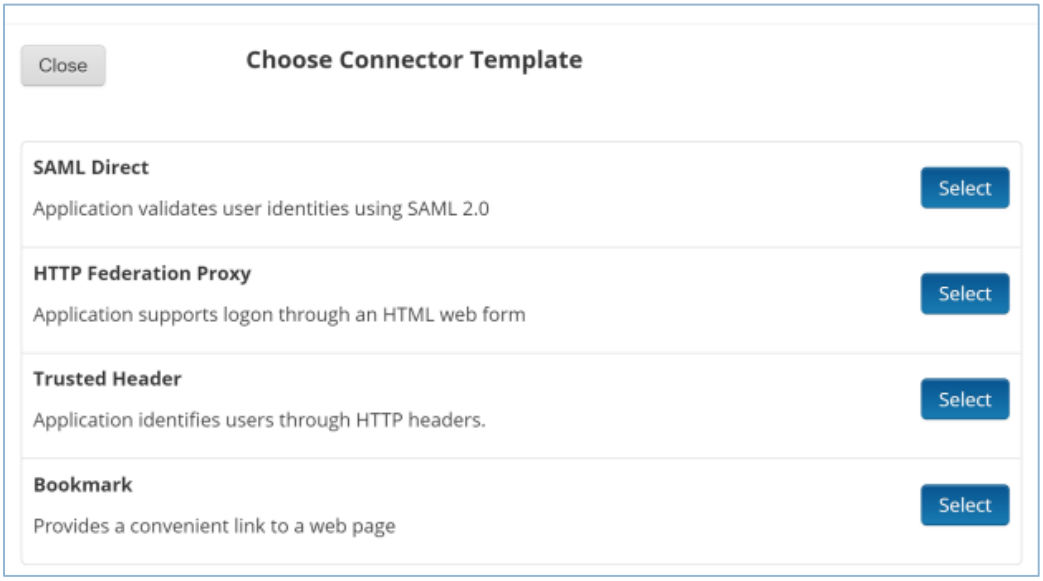

FIGURE 14: CHOOSE SAML DIRECT CONNECTOR TEMPLATE

3. On the **Basic Information** page, specify the application name and click **Next Step**.

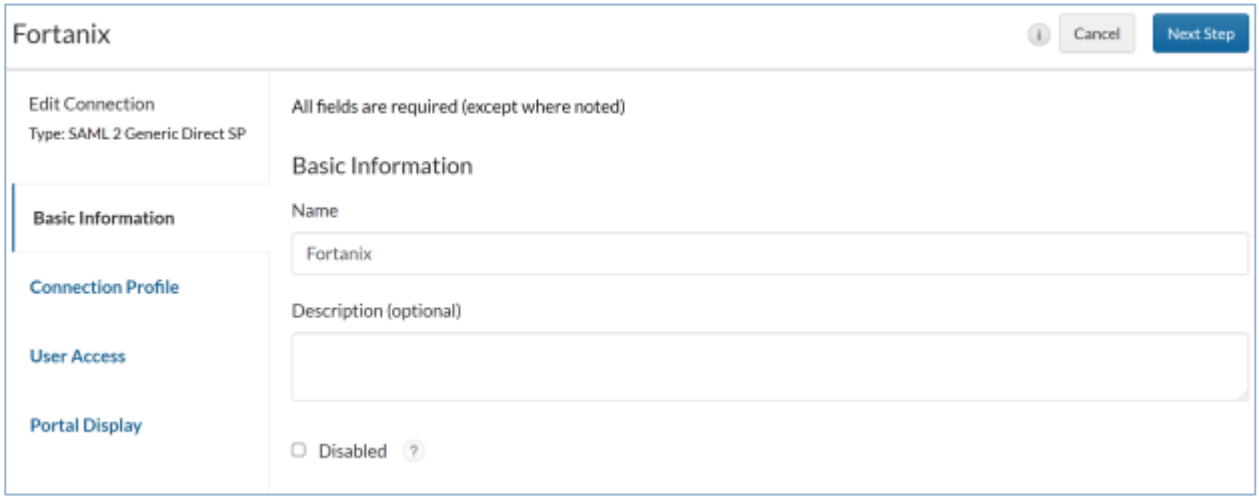

FIGURE 15: ENTER BASIC INFORMATION

4. In the **Initiate SAML Workflow** section:
   a. **Connection URL**: In the **Connection URL** field, enter the URL: https:// <fortanix_dsm_url>.
   b. Select the **SP-initiated** radio button.

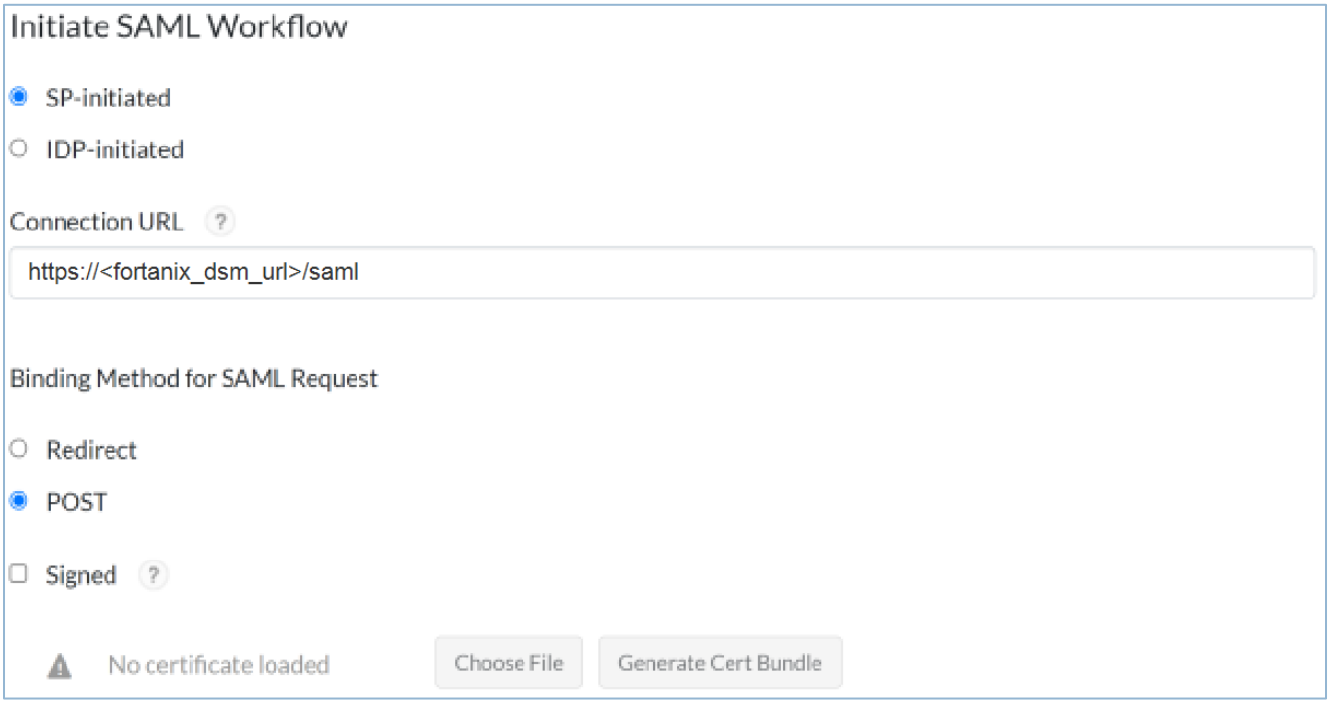

FIGURE 16: INITIATE XAML WORKFLOW

5. In the **SAML Identity Provider (Issuer)** section:
   a. **Identity Provider URL**: This will be automatically generated.
   b. **Issuer Entity ID**: This will be automatically generated.
   c. Click **Generate Cert Bundle** to generate and download a zip file containing the private key and certificate. Unzip the downloaded file to extract the certificate and private key.
   d. For the **Private Key Loaded** field, click **Choose File** and upload the RSA SecurID Access private key.
   e. For the **Certificate Loaded** field, click **Choose File** and upload the RSA SecurID Access public certificate.

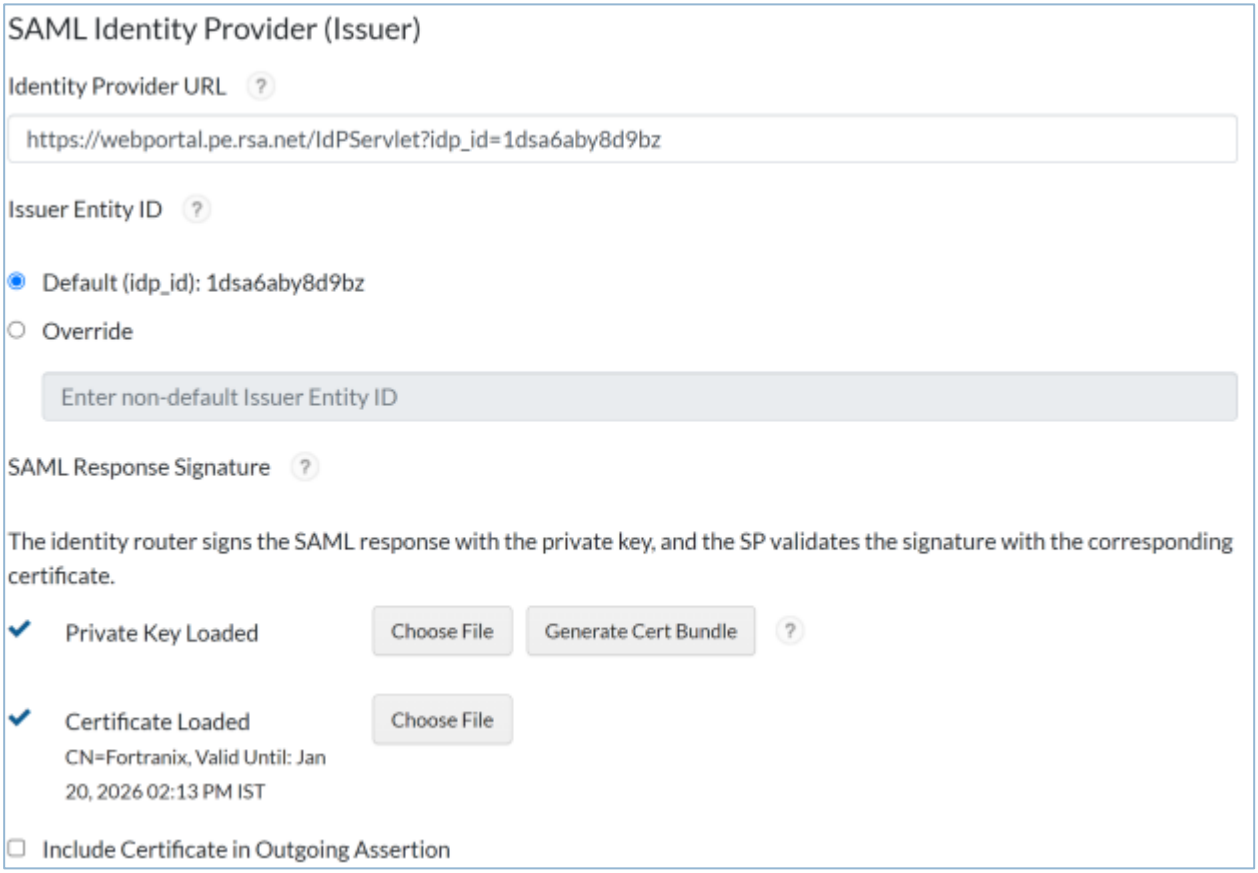

FIGURE 17: SAML IDP

6. Under the **Service Provider** section:
    a. **Assertion Consumer Service (ACS) URL**: In the **Assertion Consumer Service (ACS) URL** field enter the URL: https://<fortanix_dsm_url>/saml.
    b. **Audience (Service Provider Entity ID)**: In the **Audience** field enter the URL: https://<fortanix_dsm_url>/saml/metadata.xml.

FIGURE 18: SERVICE PROVIDER DETAILS

7. Under **User Identity** section, select **Email Address** from the **Identifier Type** drop down list, select the name of your user **Identity Source** and select the **property** value as **mail**.

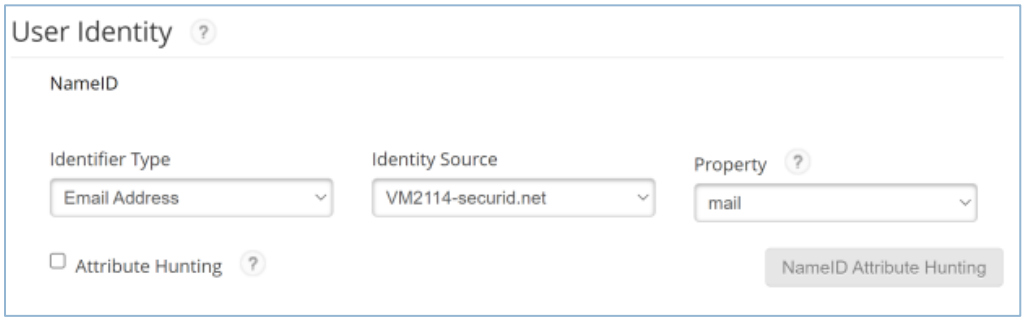

FIGURE 19: USER IDENTITY

8. Scroll to the bottom of the page and click **Next Step**.
9. On the **User Access page**, select the access policy the identity router will use to determine which users can access the Fortanix service provider. Click **Next Step**.

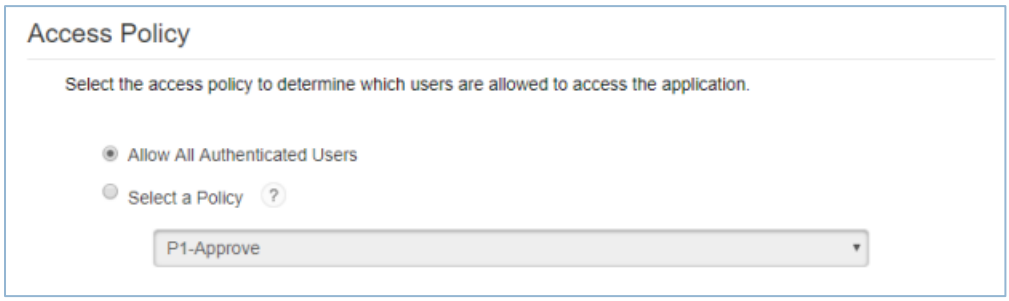

FIGURE 20: ACCESS POLICY

10. On the **Portal Display** page, configure the portal display and other settings. Click **Save and Finish**.
11. Click **Publish Changes** in the top left corner of the page and wait for the operation to complete.

FIGURE 21: PUBLISH CHANGES

12. Navigate to **Applications** > **My Applications** and locate Fortanix in the list and from the **Edit** option, select **Export Metadata**.

5.0 CONFIGURATION ON FORTANIX DATA SECURITY MANAGER

Perform the following steps to integrate Fortanix Data Security Manager with RSA SecurID Access as a Relying Party SAML Service Provider or as a SAML SSO Agent.

5.1 PROCEDURE

1. Log in to the Fortanix DSM portal (https://<fortanix_dsm_url>).
2. In the Fortanix DSM left panel, click the **Settings** tab, and then in the **AUTHENTICATION** tab, select **SINGLE SIGN-ON**.

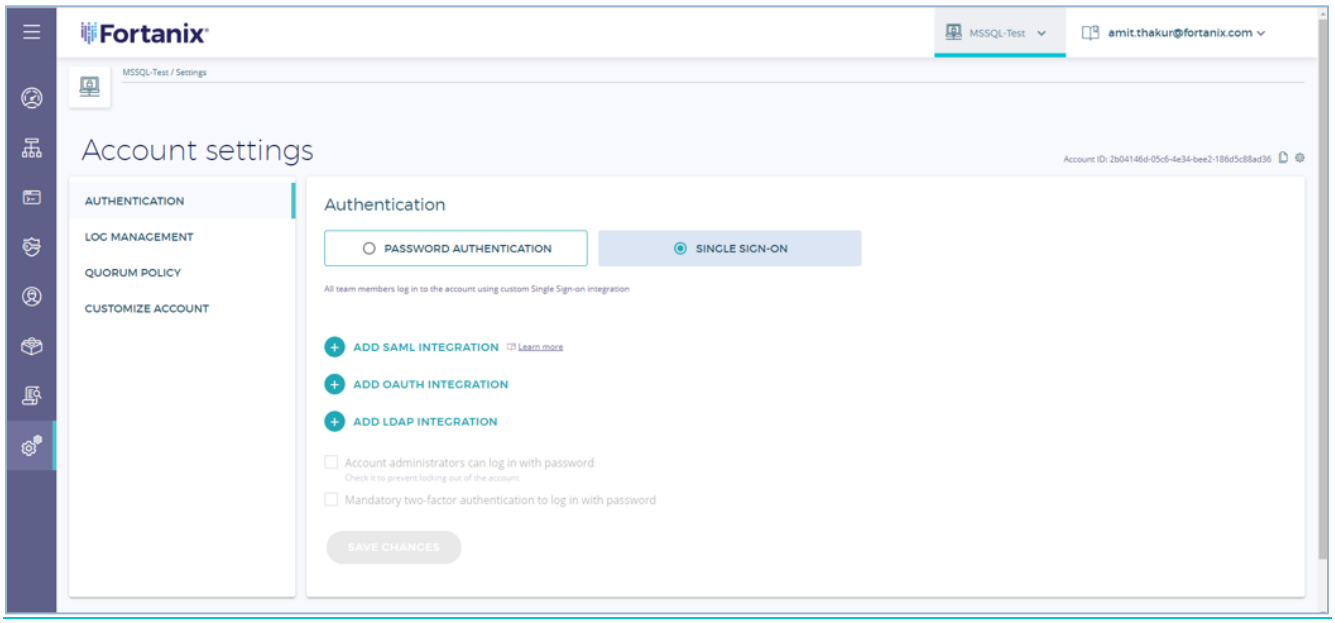

FIGURE 22: SELECT SINGLE SIGN ON

3. Add the SAML integration and upload the SAML file downloaded from *Step 12* of **Configure RSA Cloud Authentication Service – Relying Party** or **Configure RSA Cloud Authentication Service – SSO Agent**.

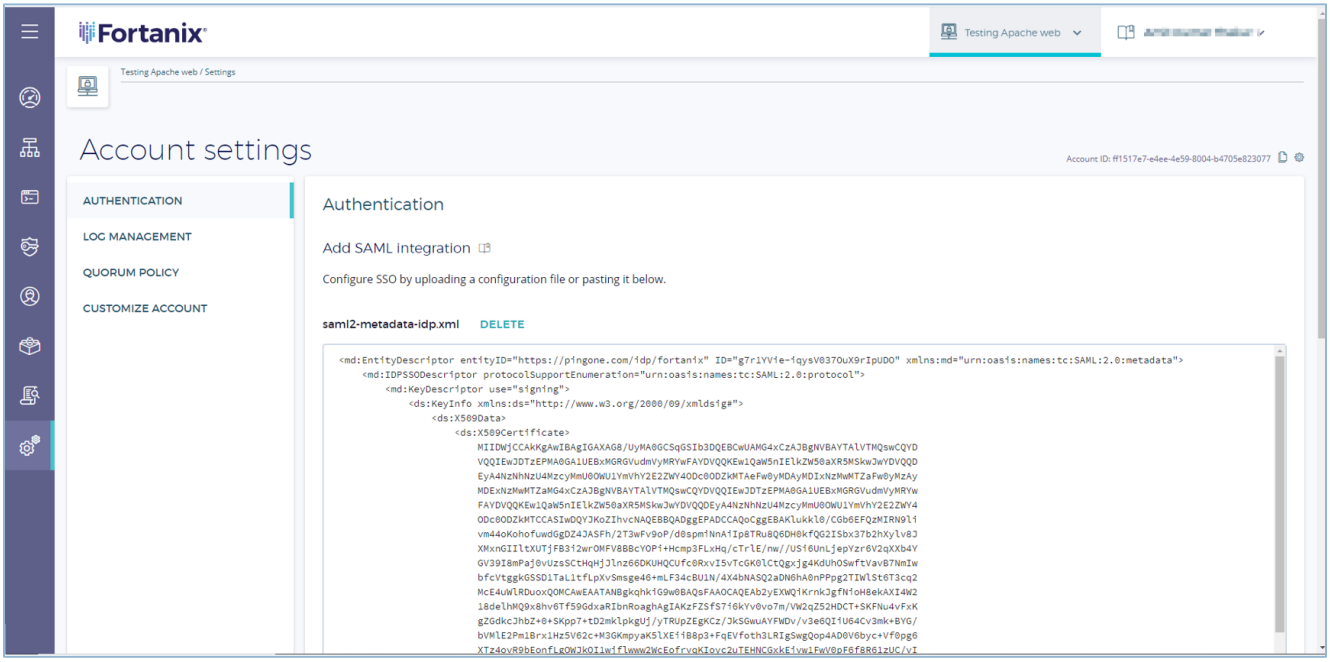

FIGURE 23: ADD SAML INTEGRATION

4. Enter your custom **SSO Title** and **Logo** URL.

FIGURE 24: CUSTOMIZE SSO

5. Click **ADD INTEGRATION** to add the SSO SAML integration.
6. Once you have added the configuration successfully you will be able to see your configuration. The configuration is complete.

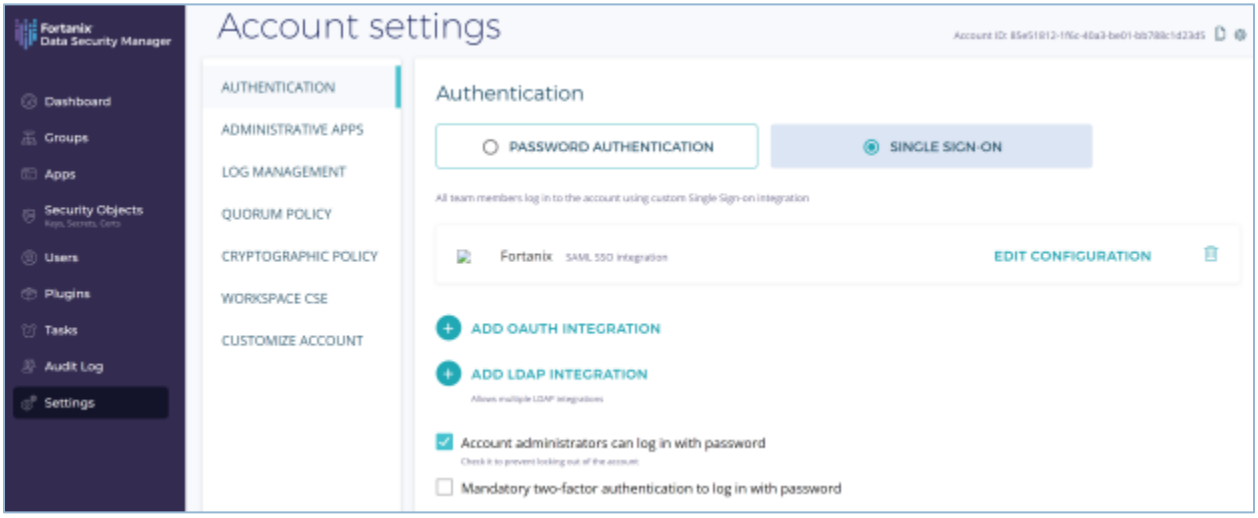

FIGURE 25: SAML IDP INTEGRATED

7. Now, log out from Fortanix DSM and sign in using SSO.

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/7033380735764-Using-Fortanix-Data-Security-Manager-with-RSA-Secure-ID-Access

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