

Integration Guide

USING DATA SECURITY MANAGER WITH FORGEROCK OAUTH 2.0

VERSION 1.0

TABLE OF CONTENTS

1.0	INTRODUCTION	2
2.0	PREREQUISITES	2
3.0	CONFIGURATION ON FORGEROCK.....	2
4.0	FORGEROCK OAUTH CONFIGURATION IN FORTANIX DSM	3
5.0	DOCUMENT INFORMATION	6
5.1	Document Location.....	6
5.2	Document Updates	6
5.3	Revision History	Error! Bookmark not defined.

1.0 INTRODUCTION

This document describes the steps to integrate **Fortanix Data Security Manager (DSM)** with **ForgeRock OAuth 2.0** Provider Service using OAuth configuration.

2.0 PREREQUISITES

- Fortanix DSM
- Access to ForgeRock Access Management Console

3.0 CONFIGURATION ON FORGEROCK

1. Log in to ForgeRock Access Management Console.
2. Click the **Services** tab -> **Add a Service** -> **OAuth2 Provider** -> click **Create**.
3. On the OAuth2 Provider page, select the **Advanced** tab and in the field **User Profile Attribute(s) the Resource Owner is Authenticated On**, enter the attribute **email**.
4. Click **Save**.

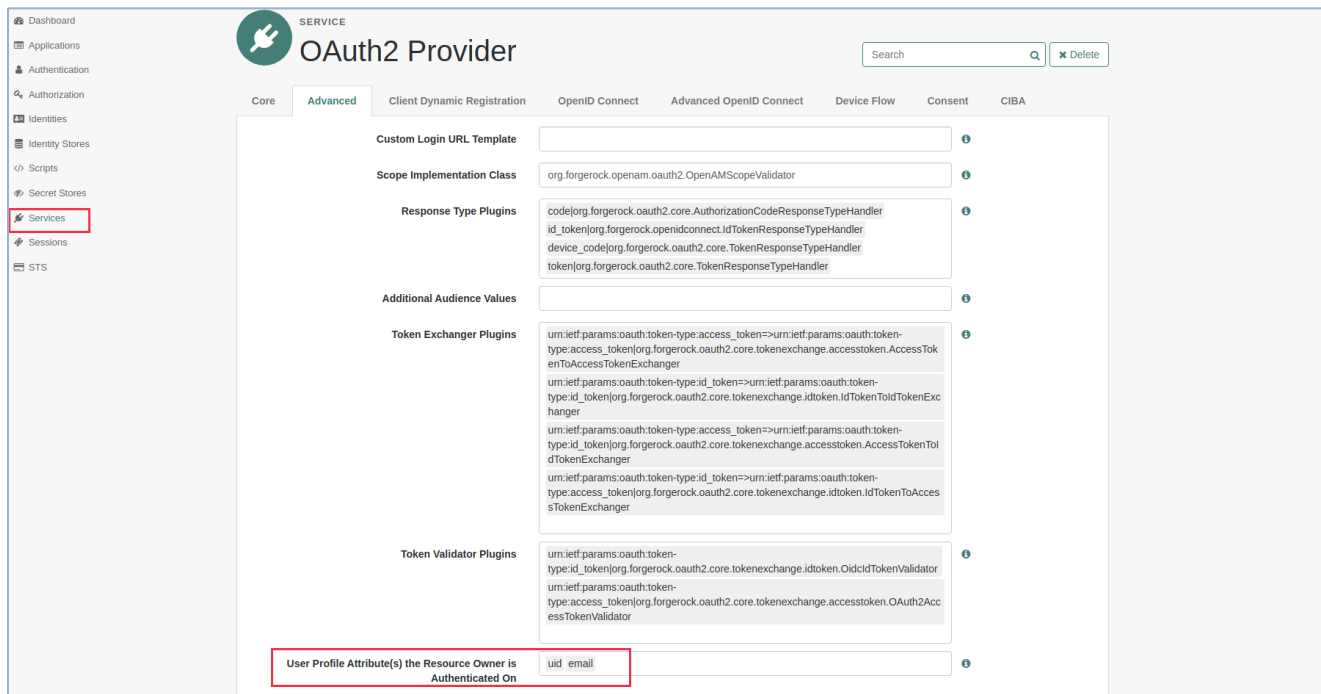


FIGURE 1: ADD OAUTH2 PROVIDER SERVICE

5. Click the **Applications** tab -> **OAuth 2.0** -> **Clients** -> Click **Add client**.
6. On the OAuth 2.0 Client page, select the **Core** tab and enter the **Client Name**, **Client secret**, **Redirection URIs**, and **Scope(s)**.

- a. **Client Name:** Enter a unique ID, or it can just be a name.
 - b. **Client secret:** Enter the secret.
 - c. **Redirection URIs:** https://<sdkmsurl>/oauth
For example: **https://sdkms.fortanix.com/oauth**
 - d. **Scope(s) :** Enter the values **openid**, **token**, and **email**.
7. Click **Save Changes**.

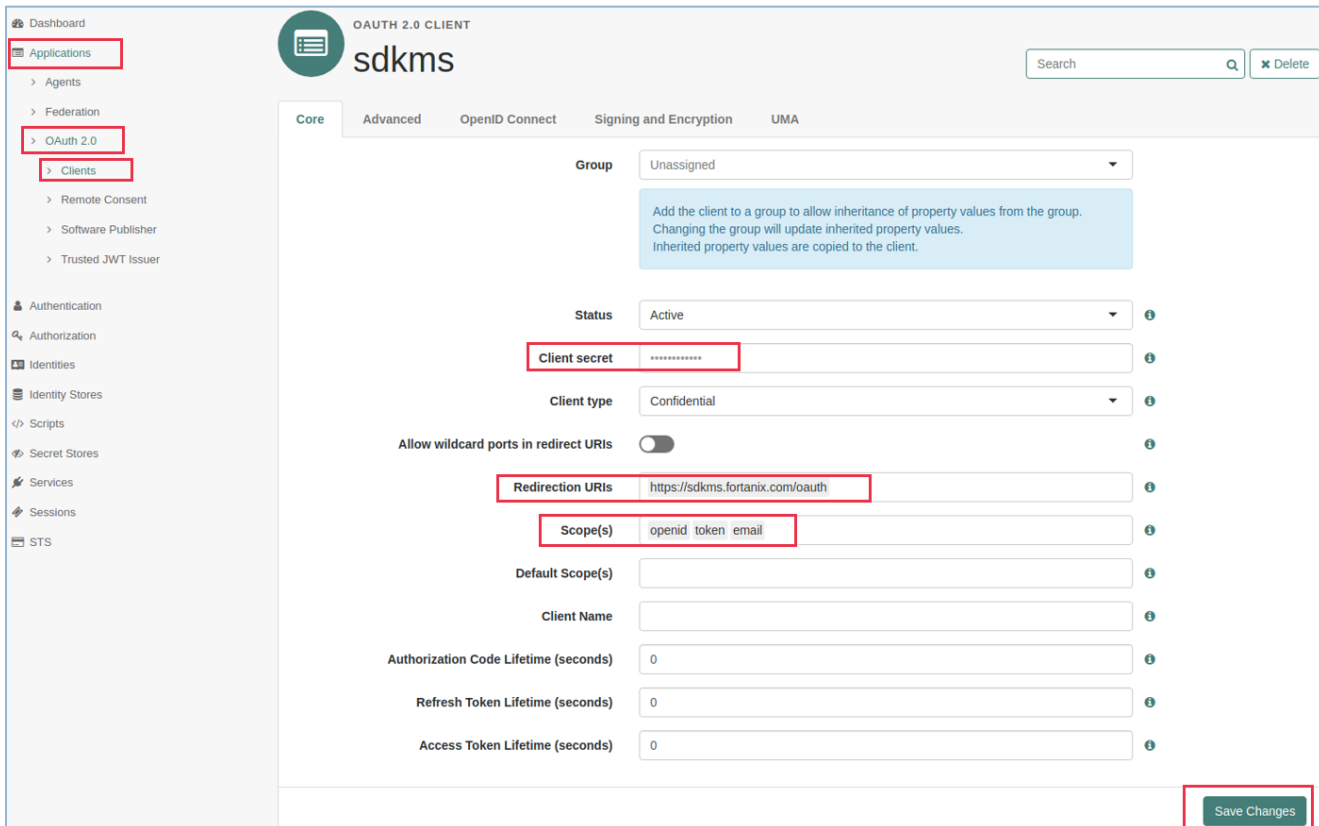


FIGURE 2: CONFIGURE OAUTH 2.0 CLIENT

4.0 FORGEROCK OAUTH CONFIGURATION IN FORTANIX DSM

1. Next, in the Fortanix DSM UI, click the **Settings** tab in the left panel and click the **AUTHENTICATION** tab.
2. Select **SINGLE SIGN-ON** and click **ADD OAUTH INTEGRATION** to configure ForgeRock OAuth 2.0 authentication.

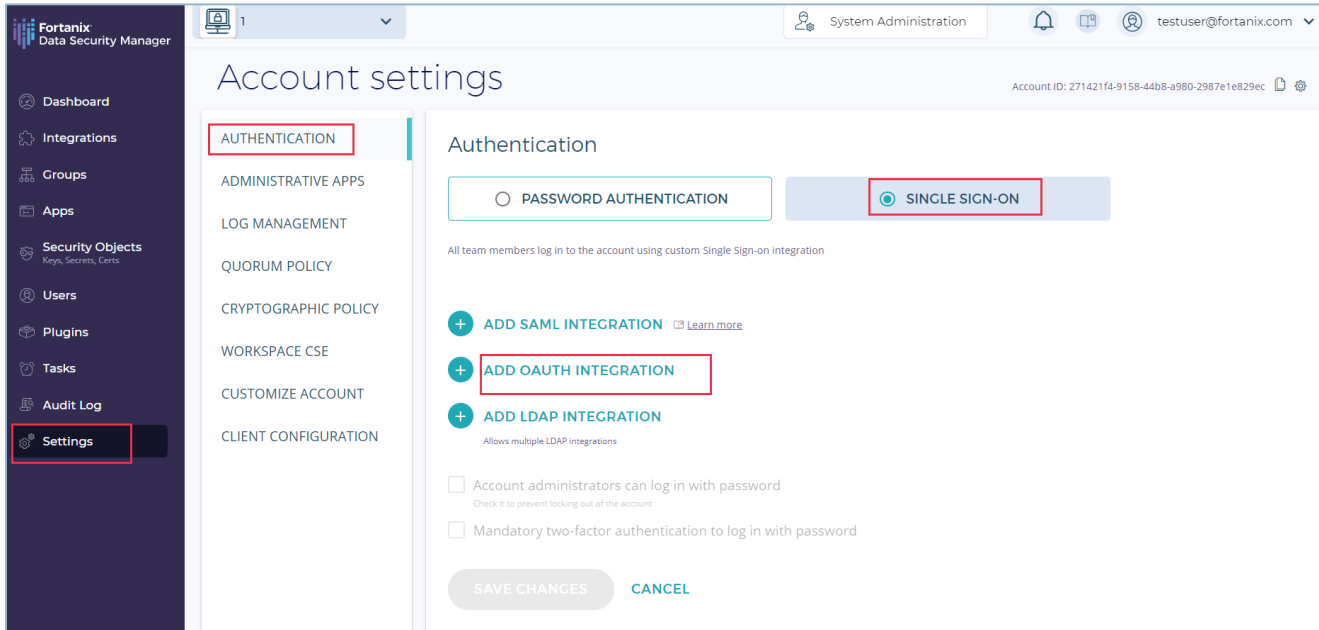


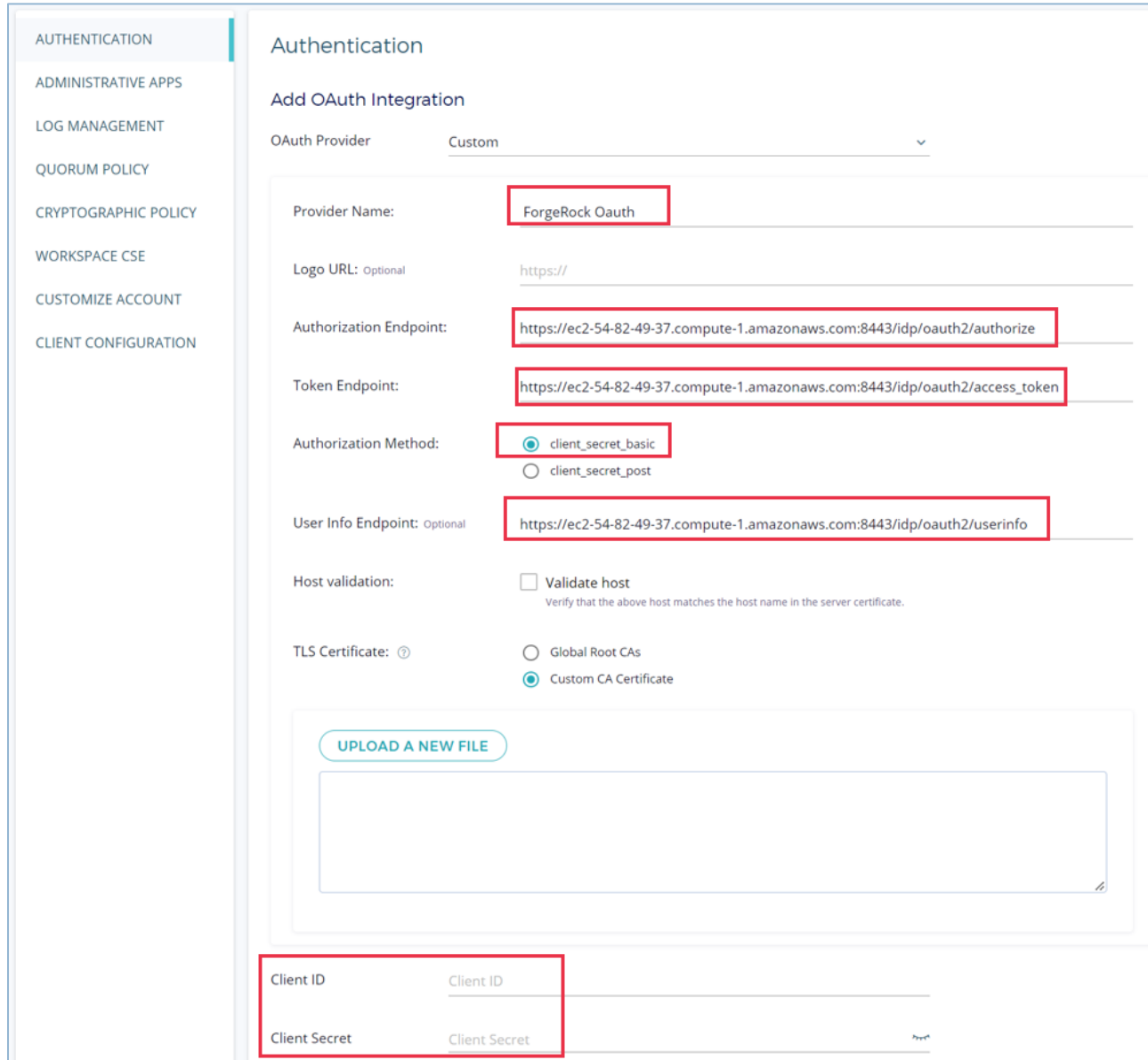
FIGURE 3: CONFIGURE FORGEROCK OAUTH INTEGRATION

3. Enter the following details for the OAuth provider.
 - a. **Provider Name** : enter any name, for example: **ForgeRock Oauth**
 - b. **Authorization Endpoint**:
<https://ec2-54-82-49-37.compute-1.amazonaws.com:8443/idp/oauth2/authorize>
 - c. **Token Endpoint**:
https://ec2-54-82-49-37.compute-1.amazonaws.com:8443/idp/oauth2/access_token
 - d. **Authorization Method**: select **client_secret_basic**
 - e. **User Info Endpoint**:
<https://ec2-54-82-49-37.compute-1.amazonaws.com:8443/idp/oauth2/userinfo>
 - f. **TLS Certificate**:
 - i. **Client ID**: enter the client name that was created in *Step 6* in *Section 3.0*.
 - ii. **Client Secret**: enter the client secret that was created in *Step 6* in *Section 3.0*.



NOTE:

- Select **Global Root CAs** if you have signed the ForgeRock SSL certificate with a CA and provide the certificate, otherwise select **Custom CA Certificate**, if you have self-signed the certificate for ForgeRock URL and provide the certificate.
- **User info Endpoint** is mandatory while using ForgeRock OAuth, otherwise it will throw a 401 unauthorized access error.



Authentication

Add OAuth Integration

OAuth Provider: Custom

Provider Name: ForgeRock OAuth

Logo URL: Optional: https://

Authorization Endpoint: https://ec2-54-82-49-37.compute-1.amazonaws.com:8443/idp/oauth2/authorize

Token Endpoint: https://ec2-54-82-49-37.compute-1.amazonaws.com:8443/idp/oauth2/access_token

Authorization Method: client_secret_basic client_secret_post

User Info Endpoint: Optional: https://ec2-54-82-49-37.compute-1.amazonaws.com:8443/idp/oauth2/userinfo

Host validation: Validate host
Verify that the above host matches the host name in the server certificate.

TLS Certificate: Global Root CAs Custom CA Certificate

UPLOAD A NEW FILE

Client ID: Client ID

Client Secret: Client Secret

FIGURE 4: OAUTH CONFIGURATION

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/7873782643604-Using-Fortanix-Data-Security-Manager-with-ForgeRock-OAuth-2-0>

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

© 2016 – 2022 Fortanix, Inc. All Rights Reserved.

Fortanix® and DSM Applications are trademarks of Fortanix, Inc. All other trademarks are trademarked by their respective owners.

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.