bioconnect. id

IBM ISAM INTEGRATION

Biometric Authentication

Mar. 2018

INTRODUCTION TO THE INTEGRATION

Introduction

IBM Security Access Manager contains out of the box support for BioConnect ID allowing you to easily add multi-factor mobile biometrics for strong authentication.

Once enabled, your users can quickly and easily self-register BioConnect ID mobile authenticators for ISAM, which are available on the Google Play, and Apple App stores by searching for BioConnect.

This integration demonstrates what is required to make the BioConnect ID API compatible with IBM's ISAM AAC Authentication system for the purposes of biometric step-up authentication.

Integration Product Components

The integration solution is packaged as a compressed file. The package contains the following files:

File Name	Description
`BCID_ISAM.pdf`	This integration guide.
`isam_bioconnect_appx.zip`	Packaged ISAM App Exchange App for automated deployment, configuration and templating for use with the AppX Installer Python script.

Table 1: Integration Package contents

Prerequisites

This integration guide details the steps that are required to achieve this integration at a high level in your environment.

This guide does not cover the configuration of the entire environment. In particular, the following product installations and configurations must already be complete:

- IBM Security Access Manager
  - IBM Security Access Manager Web Reverse Proxy
  - IBM Security Access Manager Advanced Access Control
- AppX Installer
  - Download the AppX Installer App from the App Exchange
- BioConnect ID Mobile Application

- Have BioConnect ID installed on your iOS or Android Mobile device. Available in Google Play and Apple App stores by typing BioConnect ID.

INSTALLATION

Complete the following configuration steps on the IBM Security Access appliance for integration with BioConnect ID.

The **pdadmin** command-line utility can be used on the IBM Security Access Manager Appliance in addition to the graphical user interface of the Local Management Interface (LMI) for some of the integration steps.

Deploying the AppX App

Complete the configuration steps on a system that has network connectivity to the IBM Security Access Manager appliance to configure the BioConnect ID authentication mechanism and policy for BioConnect ID.

Running the AppX Installer App

Having downloaded the ISAM AppX Installer App, execute the Python script to configure the IBM Security Access Manager appliance.

For example:

```
[user@host ~]# python3 appx-installer.py --interface
https://<isam_lmi_host_or_ip> --username admin --password
<admin_password> isam_bioconnect_appx.zip
```

Parameter	Description
`--interface`	The IBM Security Access Manager appliance Local Management Interface (LMI) hostname or IP address.
`--username`	Administrative user account name of the IBM Security Access Manager appliance Local Management Interface (LMI).
`--password`	Administrative user account password of the IBM Security Access Manager Appliance Local Management Interface (LMI).
`isam_bioconnect_appx.zip`	The BioConnect ID AppX App packaged with manifest, template files and certificates.

Table 2: AppX Installer syntax values

Verifying Output of the AppX Installer for BioConnect

The AppX installer will update the configuration of the IBM Security Access Manager appliance for use with BioConnect.

Ensure the AppX installer completes successfully and note any pending errors or actions, including restarting the Web Reverse Proxy.

RUNNING THE SAMPLE APPLICATION

Use the example scenario to validate configuration of the BioConnect ID authentication.

Before you start

This section does not cover the configuration of the entire environment. It focuses on running the test scenarios and performing the configuration with sample values.

User Account Creation

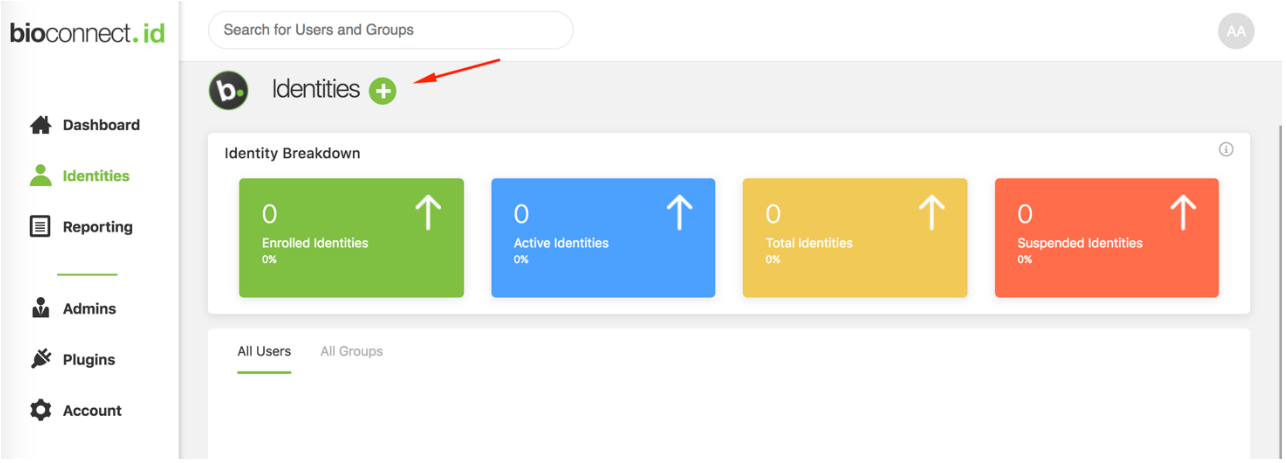
Use **Policy Administration** or the **pdadmin** command-line utility to create user accounts for accessing the console. For example:

```
axisam.bioconnectid.com> isam
axisam.bioconnectid.com:isam> admin
pdadmin> login
Enter User ID: sec_master
Enter Password: ************
pdadmin sec_master> user create user100 uid=user100,dc=iswga user100
test Passw0rd
pdadmin sec_master> user modify user100 account-valid yes
```

Configure BioConnect ID for Authentication

The sample scenario for validating the BioConnect ID AppX requires users to be registered and setup with a mobile authenticator:

1. Login to BioConnect Admin Console
    - https://app.bioconnectid.com/
    - Username = "Appexchange"
    - Password = "Password123!"
2. Create a User:
    - Click on 'Identities' and Create a New User. **Note the External ID must be the same as the ISAM ID created in the step above i.e. user100.**

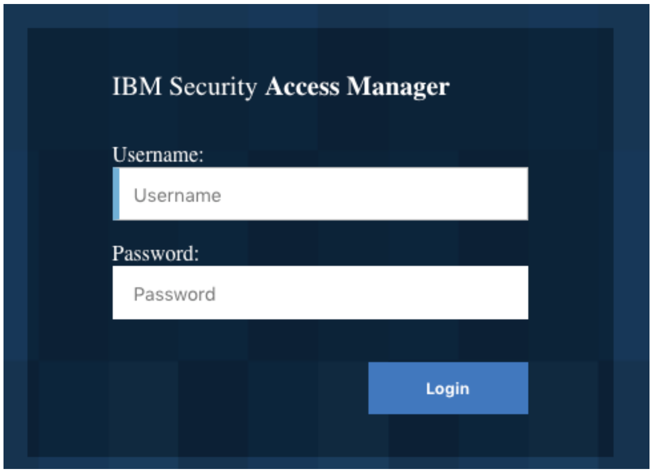


3. Create an 'Authenticator' for a User
   - Go to your user profile and click on 'Authenticators'
   - Click the + Button to Create New Authenticator
   - Click to generate a QR Code
4. Download BioConnect ID Mobile from App Store (This is your authenticator)
   - Google
   - Apple
5. Scan QR Code
   a. Open your BioConnect ID Mobile Application
   b. Scan the QR Code generated in the BioConnect ID Admin Console
6. Enroll Your Biometrics (You must enroll at least 2 biometrics before the application will activate)

Validating BioConnect ID Authentication

This is the sample scenario for validating the BioConnect ID Integration.

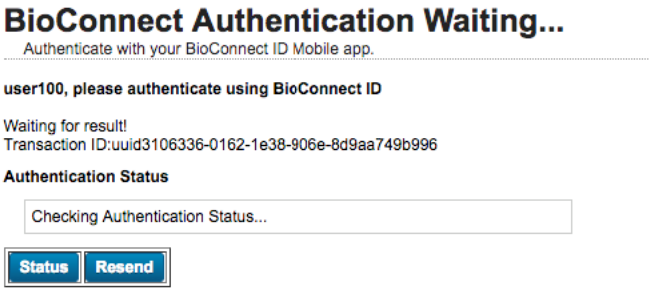
1. Access a resource or page protected by the Web Reverse proxy. For example: https://isam.ibm.com/



2. Enter the credentials for user100.

    a. Username: **user100**
    b. Password: **********

3. Open the BioConnect ID Authentication Policy via the Web Reverse proxy. For example:
    - https://isam.ibm.com/mga/sps/authsvc?PolicyId=urn:ibm:security:authentication:asf:bioconnectid



BioConnect Authentication Waiting...

Authenticate with your BioConnect ID Mobile app.

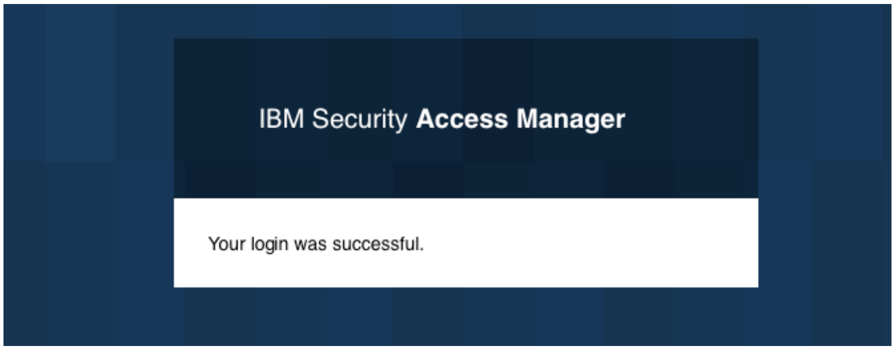
user100, please authenticate using BioConnect ID

Waiting for result!
Transaction ID:uuid3106336-0162-1e38-906e-8d9aa749b996

Authentication Status

Checking Authentication Status...

4. Open your BioConnect ID Mobile application and follow the prompts to authenticate with your registered biometrics.
5. Validate the IBM Security Access Manager splash screen is displayed.



IBM Security **Access Manager**

Your login was successful.

Advanced Configuration and Additional Use Cases

With the BioConnect ID Authentication Mechanism and Policy configured on your Security Access Manager Appliance for use with BioConnect ID, you can configure advanced options for production deployments, including:

- Use of Local Response Redirect to automatically redirect users to the BioConnect ID Authenticate policy when authentication is required
- Authentication Policy workflow to combine registration and authentication in a single user request

Contact your IBM Support or Account Representative for further information and assistance.