PingOne Advanced Identity Cloud Integration Guide

PingOne Advanced Identity Cloud (formerly ForgeRock Identity Cloud) is a SaaS-based identity and access management (IAM) solution designed for workforce, consumer, and B2B identities.

Deployment Type

This integration supports **vendor cloud** deployments through **port 443**.

If you already know that your environment supports these deployments, continue to the next step. If you are unsure, please confirm your organization's compatibility before continuing.

Required Information and Setup

To integrate GreyMatter with PingOne Advanced Identity Cloud, collect the following details:

- URL
  - Example: https://openam-reliaquest-demo.forgeblocks.com/amToken
- Service Account ID
- Service Account JWK
- API Key (Required for Investigate/Hunt & detect)
- API Secret (Required for Investigate/Hunt & detect)

See instructions below to gather the required information.

General Setup Steps

To generate the details, follow these steps:

1. Create a service account in the Advanced Identity Cloud admin console and download a private key using a user with Admin permissions. Service accounts
2. Create a Service Account ID
3. Download the Service Account JWK
4. Create an access token using the JWT profile for OAuth 2.0 authorization grant flow.
5. Set the access token as a bearer token in the Authorization HTTP header for each API request:
   - Authorization: Bearer <access-token>

Create Service Account and JWK

Your user must have admin permissions to complete these steps.

1. Within the Advanced Identity Cloud admin console, go to the **TENANT** menu (upper right). Click **Tenant Settings**.
2. Select **Global Settings**.
3. Select **Service Accounts**.
4. Click **Add New Service Account**.
5. Enter the name.
6. Include the necessary scopes in your access token request, such as fr:am: and *fr:idm:*.
7. Download the **Service Account Key**.

Create Log API Key and Secret

Your user must have admin permissions to complete these steps.

1. Within the PingOne Advanced Identity Cloud admin console, click the **User Icon**.
2. Select **Tenant Settings**.
3. Open the **Global Settings** tab.
4. Click **Log API Keys**.
5. Click the **New Log API Key** button.
6. Enter a descriptive name for your API Key.
7. Click **Create Key**.
8. Save the **api_key_id** (API key) and **api_key_secret**. These cannot be viewed again.
9. Click **Done**.

Create an Email Template

Create an Email Template named RQ_UpdatePassword, which should have reset password link.

Permissions and Functionality

Permissions

GreyMatter Capability	Action(s)	Required Permission
Investigate/Hunt	Perform Query	API Secret and Key
Detect	Detect	API Secret and Key (default log API Key and Secret is created with no permissions)
Respond	Enrich User	scopes in your access token request, such as fr:am:*, fr:idm:*.
	Enable User	scopes in your access token request, such as fr:am:*, fr:idm:*.
	Disable user	scopes in your access token request, such as fr:am:*, fr:idm:*.
	Reset Password	scopes in your access token request, such as fr:am:*, fr:idm:*.
	Terminate Active Session	scopes in your access token request, such as fr:am:*, fr:idm:*.
	Reset MFA	scopes in your access token request, such as fr:am:*, fr:idm:*.

Respond

Playbook Name	Description	Required Input Variables
Enrich User	Obtains user details.	Username

		Example: testuser01
Enable User	Enable a user by passing username.	Username Example: testuser01
Disable User	Disable a user by passing username.	Username Example: testuser01
Terminate Session	Terminate a user session by passing username.	Username Example: testuser01
Reset Password	Reset user's password by passing username.	Username Example: testuser01
Reset MFA	Reset user's MFA by passing username.	Username Example: testuser01

Investigate/Hunt

Am-access: Captures all incoming Advanced Identity Cloud access calls as audit events. This includes who, what, when, and the output for every access request.
Audit events:

- AM-ACCESS-ATTEMPT
- AM-ACCESS-OUTCOME

am-activity: Captures state changes to objects that were created, updated, or deleted by Advanced Identity Cloud end users. This includes session, user profile, and device profile changes.
Audit events:

- AM-SELFSERVICE-REGISTRATION-COMPLETED
- AM-SELFSERVICE-PASSWORDCHANGE-COMPLETED
- AM-SESSION-CREATED
- AM-SESSION-IDLE_TIME_OUT
- AM-SESSION-MAX_TIMED_OUT
- AM-SESSION-LOGGED_OUT
- AM-SESSION-DESTROYED
- AM-SESSION-PROPERTY_CHANGED
- AM-IDENTITY-CHANGE
- AM-GROUP-CHANGE

am-authentication: Captures when and how a user authenticated and related audit events. Advanced Identity Cloud records an authentication audit event for each authentication node and the journey outcome. A node can provide extra data in the standard audit event, which is logged when an authentication node completes.
Audit events:

- AM-BACK-CHANNEL-INITIALIZE
- AM-LOGOUT
- AM-LOGIN-COMPLETED
- AM-LOGIN-MODULE-COMPLETED

- AM-NODE-LOGIN-COMPLETED

Advanced Identity Cloud logs this audit event each time an authentication node completes.

am-config: Captures access management configuration changes for Advanced Identity Cloud with a timestamp and by whom.
Configuration changes can only be performed in development environments, so these logs are empty in staging and production environments.
Audit events:

- AM-CONFIG-CHANGE

am-everything (*): Captures all access management audit and debug logs for Advanced Identity Cloud.
This includes all the logs captured in am-access, am-activity, am-authentication, am-config, and am-core.

Detect

PingOne Advanced Identity Cloud supports **Detection at Source** (Vendor-Authored and Alert Ingestion)**.** **Note Syncing** and **State Syncing** are *not* supported.