



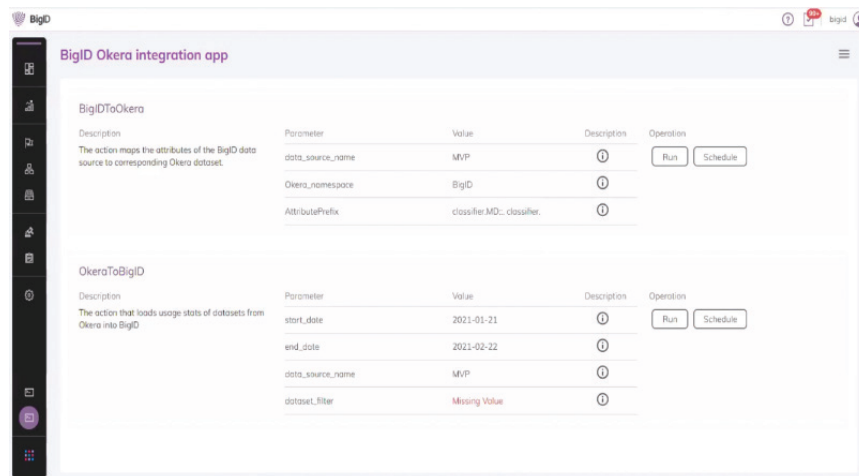


Use Data Responsibly with In-Depth Data Intelligence

SOLUTION BRIEF

The Okera Data Protection App for BigID empowers customers to secure sensitive data and drive visibility and security across their data ecosystem.

- 
Discover and Classify all sensitive, critical, personal and regulated data.
- 
Define who has access and for what purpose.
- 
Enforce policies with masking, redaction, filtering, and more.
- 
Report user activity, data utilization, and policy changes for compliance and deeper understanding.



BigID Oker integration app				
BigIDToOker				
Description	Parameter	Value	Description	Operation
The action maps the attributes of the BigID data source to corresponding Oker dataset.	data_source_name	MVP	ⓘ	Run Schedule
	Oker_namespace	BigID	ⓘ	
	AttributePrefix	classifier.MD- classifier	ⓘ	
OkerToBigID				
Description	Parameter	Value	Description	Operation
The action that loads usage stats of datasets from Oker into BigID	start_date	2021-01-21	ⓘ	Run Schedule
	end_date	2021-02-22	ⓘ	
	data_source_name	MVP	ⓘ	
	dataset_filter	Missing Value	ⓘ	

Data-driven Initiatives fail because:

People and systems can retrieve and use data they shouldn't have access to

People and systems cannot access the data they need for legitimate business purposes

With BigID + Okera, you can:

- Prevent the proliferation of rogue data extracts
- Avoid secure database view explosion
- Avoid IAM role bloat
- Manage policy drift
- Maintain reliable sources of the truth

Benefits of BigID + Okera:

- Provision data access faster, more confidently, and responsibly
- Halt and recover from managing secure data access in technology silos
- Protect your business, customers, and partners from inappropriate data access

1

FIND AND CLASSIFY ALL SENSITIVE AND CONFIDENTIAL DATA WITH BIGID

- Automatically discover, classify, and map sensitive data across all types of data, structured and unstructured, everywhere with ML and in-depth data insight.
- Leverage business, privacy, and security-based classifiers to tag sensitive data elements across your data ecosystem.
- Metadata exchange between BigID & Okera to assign and take the right action on the right data.

2

DYNAMICALLY RESTRICT, MASK, FILTER, AND ANONYMIZE SENSITIVE DATA WITH OKERA

- Define data access policies based on business purpose.
- Exercise rich fine grained access control (FGAC) at the table, column, row, and cell level with every data query.
- Secure access to sensitive data with dynamic masking, tokenization, redaction, filtering, conditional logic, and custom anonymization technique.
- Enforce policies using the fastest and most secure method possible for every data request.

3

IN-DEPTH DATA INTELLIGENCE WITH REAL-TIME DATA USAGE AUDITS AND REPORTING

- Log user activity, data utilization, and policy changes for compliance and deeper understanding.
- Actively monitor sensitive and high-risk data as data is queried.
- Capture granular visibility on the number of users accessing sensitive data.
- Gain in-depth data intelligence based on user activity and access patterns.



In-Depth Data Intelligence

BigID Feeds Metadata to Okera -->

BigID Core Capabilities:

- Discover, classify, and map sensitive data
- Data subject correlation
- Data Resiliency



PII

Public



OKERA

Use Data Responsibly

Okera Core Capabilities:

- Universal Policy Management
- Dynamic Policy Enforcement
- Data Usage Intelligence

--Okera Returns Protected Flag & Data Usage

To get started with the Okera Data Protection App for BigID, please contact: marketplace@bigid.com.