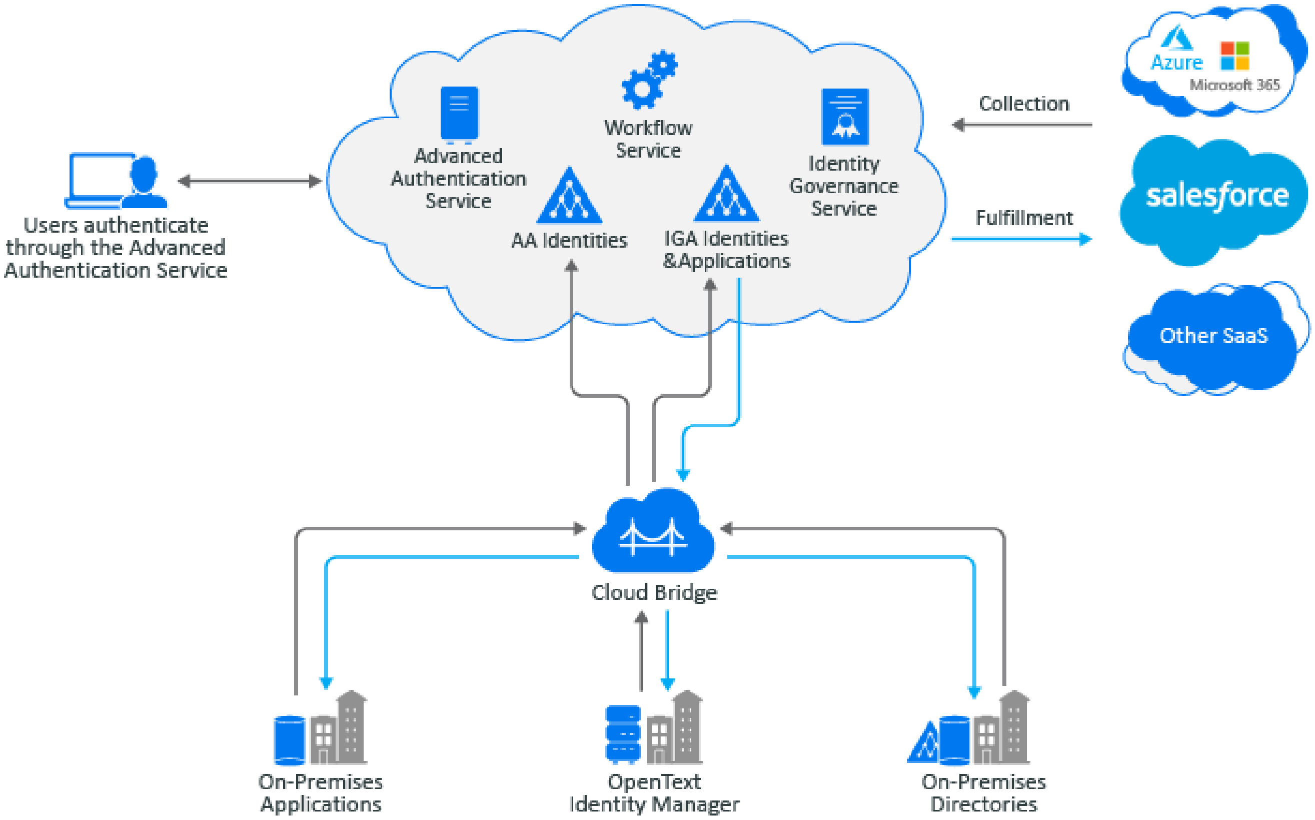
OpenText™ Identity Governance and Administration as a Service Quick Start

25.1 (v4.5)

This quick start provides a brief overview of the OpenText Identity Governance and Administration hybrid solution and the tasks you need to complete to start using OpenText Identity Governance as a Service.

Figure 1 *Overview of OpenText Identity Governance and Administration*


Users authenticate through the Advanced Authentication Service
Advanced Authentication Service
Workflow Service
Identity Governance Service
AA Identities
IGA Identities &Applications
Collection
Fulfillment
Azure
Microsoft 365
salesforce
Other SaaS
Cloud Bridge
On-Premises Applications
OpenText Identity Manager
On-Premises Directories

OpenText Identity Governance and Administration manages and governs digital identities and enforces appropriate access across the enterprise. With a unified governance framework, organizations can determine who has access to which resources and whether that access is appropriate. Scaling to billions of identities, OpenText solution automates and streamlines processes related to access requests, access certification, identity lifecycle management, provisioning, and compliance reporting. Our solution detects changes as they happen in the connected systems and adjusts security controls for continuous compliance, thus reducing risk and increasing efficiency for the organization.

Our solution as illustrated in the above diagram, includes following main components and additional services:

- OpenText Identity Governance helps organizations run effective access certification campaigns and implement it. Key features include certification reviews, micro-certifications, access request and approval, segregation of duties (SOD), and governance insight. OpenText Identity Governance can be deployed on premises or using SaaS.
- OpenText™ Identity Manager powers the entire identity management lifecycle, managing identities and their associated attributes to minimize privileges. Key features include automated provisioning, identity attribute management, password synchronization, and data and event transformation to match organizational business processes.

You can use our hybrid solution to log in to OpenText Identity Governance as a Service using OpenText™ Advanced Authentication as a Service for authentication based on methods and repositories configured in OpenText Advanced Authentication tenancy. In addition, you can collect data from on-premises OpenText Identity Manager using a data transfer bridge (OpenText™ Cloud Bridge), create custom workflows for request approval on fulfillment, and generate reports.

OpenText Identity Governance as a Service and OpenText Advanced Authentication as a Service will be deployed, configured, and maintained by OpenText™. Once you receive your tenancy URL (http://*tenantid*.*igasubdomain*.*hostedsaasdomain*.com), you can log in to OpenText Identity Governance, assign authorizations, and perform governance tasks.

Browser Requirements

To log in to OpenText Identity Governance on their local devices, users must have one of the following browser versions, at a minimum:

- Apple Safari 18.1.1 (20619.2.8.11.12)
- Google Chrome 131.0.6778.109
- Microsoft Edge Browser 131.0.2903.86
- Mozilla Firefox 133.0

IMPORTANT: The browser must have cookies enabled. If cookies are disabled, the product will not work.

Supported AI Providers and Integrated Components

This section outlines supported and integrated component versions and AI providers.

AI Providers

Identity Goverance Aviator which supports ability to create transformation scripts using generative AI supports the following providers and models:

- OpenAI Chat GPT. Models: gpt-3.5-turbo, gpt-4.0-turbo, and gpt-4.0o
- Google Gemini. Models: gemini-1.5-pro and gemini-1.5-flash

For more information about OpenText Identity Governance Aviator procedures, see “Creating Transformation Scripts Using Generative AI” in the *Identity Governance as a Service User and Administration Guide*.

Integrated Components

- Form Builder 1.6.0.0000
- Identity Reporting 7.5
- Workflow Console 1.1.0.0100
- Workflow Engine 1.1.0.0100 on the same Tomcat server as OpenText Identity Governance

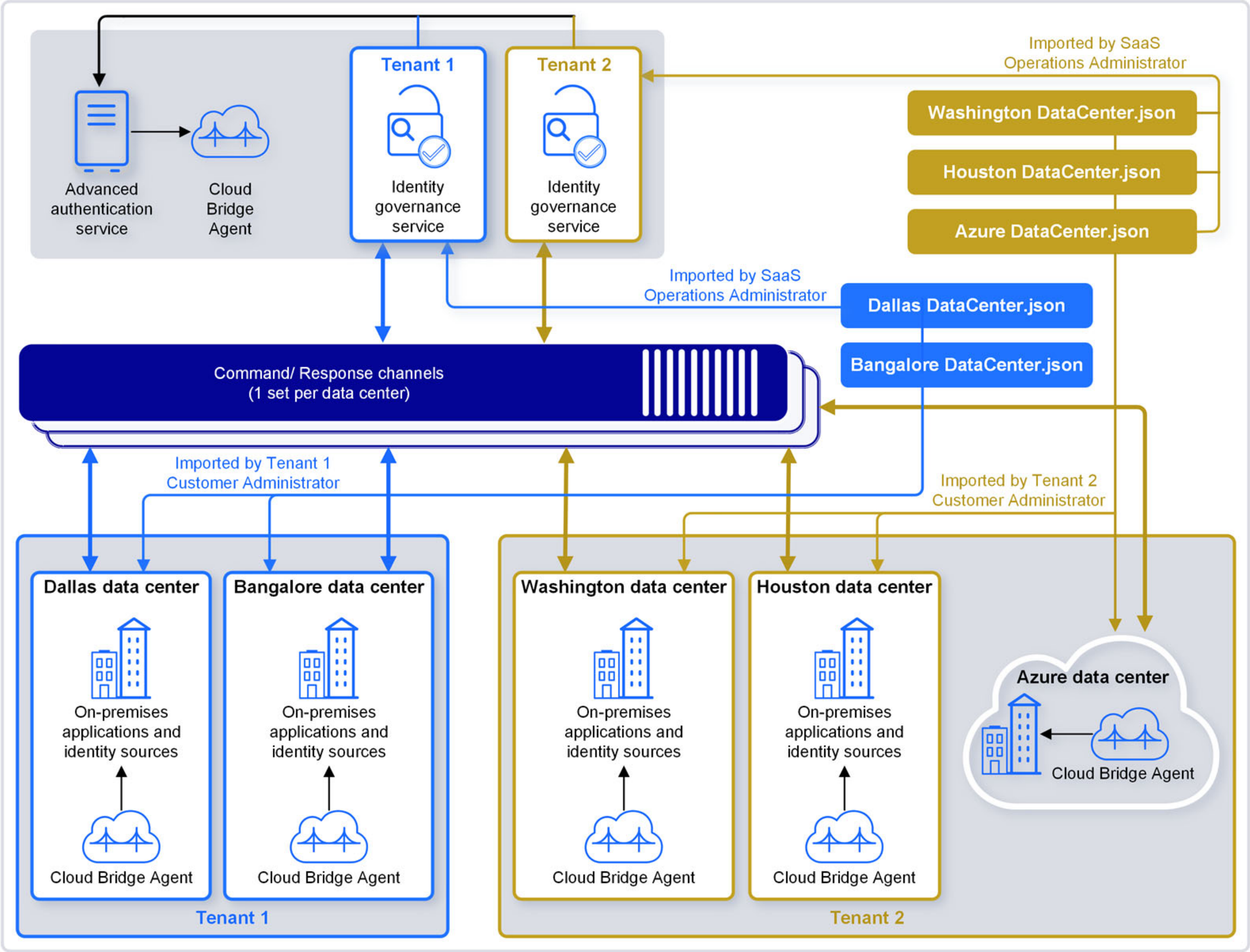
Logging In to the OpenText Identity Governance Service

After signing up for OpenText Identity Governance as a Service, log in to your unique URL using the provided user name and password. You must log in with the bootstrap administrator account until you have collected and published identities and assigned a user as the Customer Administrator. Bootstrap administrator account is created during the onboarding process. We recommend that you change the bootstrap administrator password. You can change the password by logging in to your `*aa service*/account` as `*tenantid*\IGBOOTSTRAPS\*bootstrap administrator email*`. For example, when Tenant ID is Tenant 1 and the bootstrap administrator email is igadmin@tenant1.com, log in to your `aa.cyberresprod.com/account` as `TENANT1\IGBOOTSTRAPS\igadmin@tenant1.com`.

Installing and Configuring the Cloud Bridge Agent

In as a Service environment, OpenText Cloud Bridge is a data transfer bridge between the application in the cloud and data sources in on-premises environments. The **Cloud Bridge Agent** is the entity that responds to the collection and fulfillment commands and directs them to the proper data source for execution. The following diagram provides an example of a Cloud Bridge setup.

Figure 2 Cloud Bridge Setup Example


Advanced authentication service
Cloud Bridge Agent
Tenant 1
Identity governance service
Tenant 2
Identity governance service
Imported by SaaS Operations Administrator
Washington DataCenter.json
Houston DataCenter.json
Azure DataCenter.json
Imported by SaaS Operations Administrator
Dallas DataCenter.json
Bangalore DataCenter.json
Command/ Response channels (1 set per data center)
Imported by Tenant 1 Customer Administrator
Imported by Tenant 2 Customer Administrator
Dallas data center
On-premises applications and identity sources
Cloud Bridge Agent
Bangalore data center
On-premises applications and identity sources
Cloud Bridge Agent
Tenant 1
Washington data center
On-premises applications and identity sources
Cloud Bridge Agent
Houston data center
On-premises applications and identity sources
Cloud Bridge Agent
Azure data center
Cloud Bridge Agent
Tenant 2

The Cloud Bridge Data Center in your OpenText Identity Governance tenancy is created by the SaaS team based on the information you provide in the technical questionnaire. **Data Centers** are a conceptual representation of your Cloud Bridge Agent instance and could reside in different on-premises and cloud environments. DataCenter.json contains customer-specific data center information. Defines the connection information between the Cloud Bridge Client and a single Agent instance. Install the Agents on your local systems, then log in to OpenText Identity Governance and configure Data Source Connections and Data Sources as needed to connect to your on-premises data sources.

For information about the Cloud Bridge Agent and related OpenText Identity Governance procedures, see the following sections.

- "Installing and Upgrading the Cloud Bridge Agent" on page 4
- "Configuring Data Source Connection and Adding Credentials" on page 5

Installing and Upgrading the Cloud Bridge Agent

Prior to installing the Cloud Bridge Agent on premises, the SaaS operations team must have granted you the privilege to use Cloud Bridge. You or an authorized user can then add an external repository in the OpenText Identity Governance Advanced Authentication tenancy.

NOTE: Use *TENANT_ID*_AA_ER, where *TENANT_ID* is in uppercase, as the name of the external repository. For more information about adding Cloud Bridge external repository, refer to the *OpenText Advanced Authentication Administration Guide*.

Regarding upgrading your Cloud Bridge Agent, before you upgrade an existing Agent installation, you should review your environment and do some planning for high availability. For more information about installing and upgrading the Cloud Bridge Agent on premises, refer to the *OpenText Cloud Bridge Agent Release Notes (https://www.microfocus.com/documentation/identity-and-access-management/iam-services/cloud-bridge-agent-release-notes/cloud-bridge-agent-release-notes.html#)* and the *OpenText Cloud Bridge Agent Installation and Administration Guide (https://www.microfocus.com/documentation/identity-and-access-management/iam-services/cloud-bridge-agent-admin/bookinfo.html)*.

Configuring Data Source Connection and Adding Credentials

After installing the agent, you must configure a data source connection in OpenText Identity Governance, then add credentials using the Cloud Bridge Agent UI. When adding credentials, in addition to unique ID, user name, and password, you must also specify the appropriate ordinal for the authentication method. When a connector (collector or fulfiller) takes only one credential pair, then the default ordinal value of 0 is used. When a connector supports more than one credential pair (user name and password) combination such as the IDM AE Permission Collector and SCIM collectors and fulfiller, then you need to specify additional ordinals.

NOTE: The user name and password fields are limited to 255 characters.

You can view the existing credentials you have by visiting http://*localhost (Cloud Bridge Agent IP address or DNS name)*:8080/api/v1/credential. Since the connector can only be configured for one type of authentication, the other credential sets will be unused by the connector.

IMPORTANT: When configuring the Cloud Bridge Agent, it is *critical* that the correct ordinal value is used for the selected authentication method. For example, if a SCIM Identity Collector is being configured in OpenText Identity Governance and Basic Auth is selected for the Authentication Method, the basic authentication credentials would need to be added to the Cloud Bride Agent using ordinal value 3. Also note that if an authentication method is chosen that requires multiple credential sets, ALL of these credential sets must be added to the Cloud Bridge Agent using specific ordinal values.

For information about:

- Configuring data source connections, see “Collecting Data Using Cloud Bridge” in the *OpenText Identity Governance as a Service User and Administration Guide*
- Adding credentials, see “Add Credentials for Data Source Connections (https://wwwtest.microfocus.com/documentation/identity-and-access-management/iam-services/cloud-bridge-agent-admin/configure-data-source-connection-credentials.html)” in the *OpenText Cloud Bridge Installation and Administration Guide (https://www.microfocus.com/documentation/identity-and-access-management/iam-services/cloud-bridge-agent-admin/bookinfo.html)*
- Specific ordinal values and authentication methods, see the *OpenText Identity Governance as a Service User and Administration Guide (https://www.microfocus.com/documentation/identity-governance-and-administration/igaas/collectors-fulfillers-guide/front.html)*

Configuring Data Sources and Collecting and Publishing Data

Once you have completed the above procedures and established data source connections with the OpenText Cloud Bridge, enable the collection using the out-of-the-box templates, then start collecting and fulfilling change requests. For information about collection and fulfillment see the following chapters in the *OpenText Identity Governance as a Service User and Administration Guide*:

- “Understanding Data Administration”
- “Collecting Identities”
- “Collecting Applications and Application Data ”
- “Publishing the Collected Data”
- “Setting up Fulfillment Targets and Fulfilling Changesets”

For specific collector or fulfiller configuration, see the *OpenText Identity Governance Collector and Fulfiller Configuration Guide (https://www.microfocus.com/documentation/identity-governance-and-administration/igaas/collectors-fulfillers-guide/front.html)*.

Requesting Access and Performing Governance and Administration Tasks

For information about requesting access and performing other governance tasks such as setting up access reviews, and creating policies, and managing data, refer to the *OpenText Identity Governance as a Service User and Administration Guide* (https://www.microfocus.com/documentation/identity-governance-and-administration/igaas). For additional information regarding creating and customizing your request approval and fulfillment workflows, refer to the *OpenText Workflow Service Administration Guide* (https://www.microfocus.com/documentation/identity-governance-and-administration/igaas/workflow-admin-console/bookinfo.html).

For additional documentation, visit the OpenText Identity Governance documentation website (https://www.microfocus.com/documentation/identity-governance-and-administration).

Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@microfocus.com (mailto:Documentation-Feedback@microfocus.com). We value your input and look forward to hearing from you.

For support, visit the CyberRes by OpenText Support Website (https://support.cyberreshelp.com/) or email cyberressupport@microfocus.com (mailto:cyberressupport@microfocus.com).

For general corporate and product information, visit the Corporate Website (https://www.microfocus.com/en-us/home).

For interactive conversations with your peers and experts, become an active member of our community (https://community.microfocus.com). The online community provides product information, useful links to helpful resources, blogs, and social media channels.

Legal Notice

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.