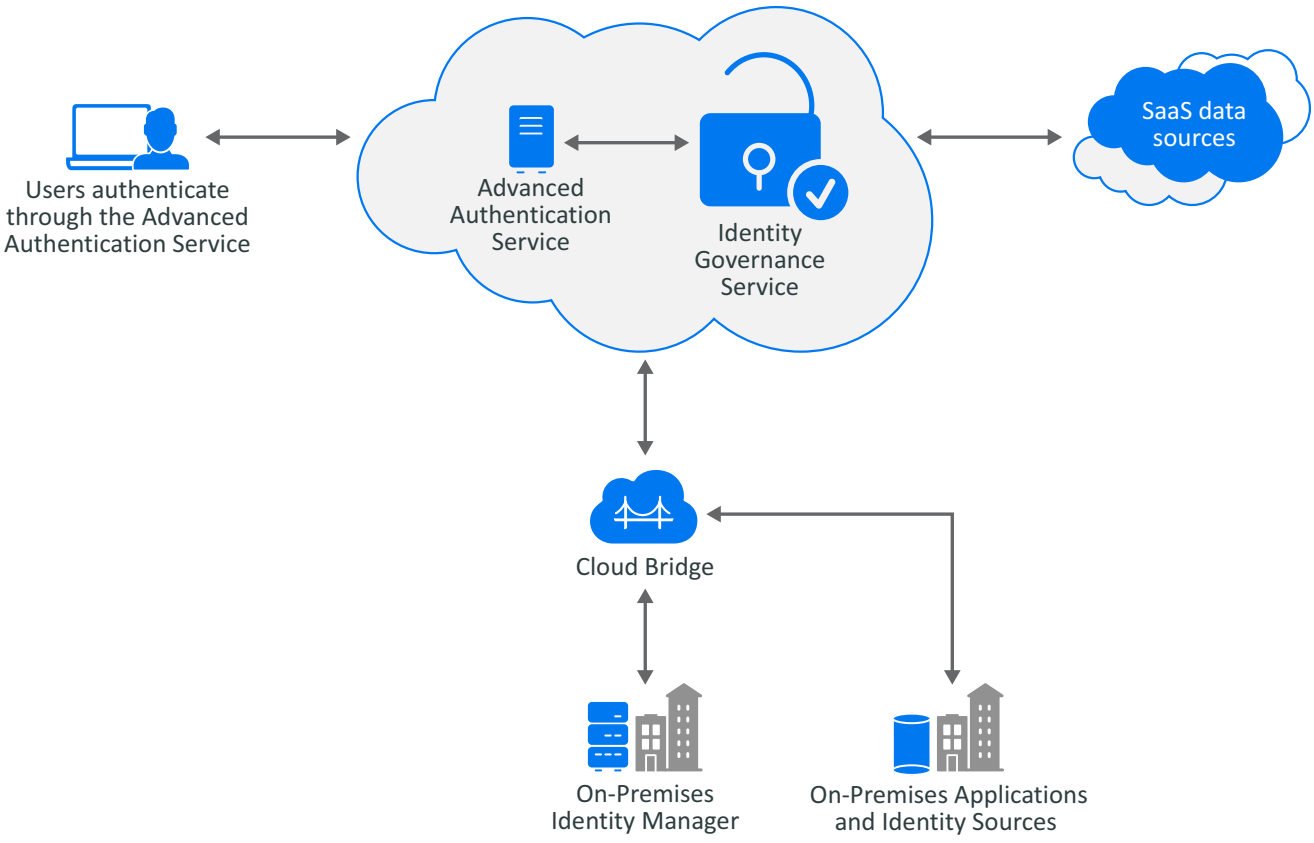
Identity Governance as a Service Quick Start

November 2021

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

Figure 1 *Overview of Identity Governance and Administration*



NetIQ Identity Governance and Administration (IGA) 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, IGA automates and streamlines processes related to access requests, access certification, identity lifecycle

management, provisioning, and compliance reporting. IGA 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.

IGA includes two main components:

- NetIQ Identity Governance helps organizations run effective access certification campaigns and implement identity governance. Key features include certification reviews, micro-certifications, access request and approval, segregation of duties (SOD), and governance insight. Identity Governance can be deployed on premises or using SaaS.
- NetIQ 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 the IGA hybrid solution to log in to Identity Governance as a Service using Advanced Authentication as a Service for authentication based on methods and repositories configured in Advanced Authentication tenancy. In addition, you can collect data from on-premises Identity Manager using a data transfer bridge (Cloud Bridge).

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

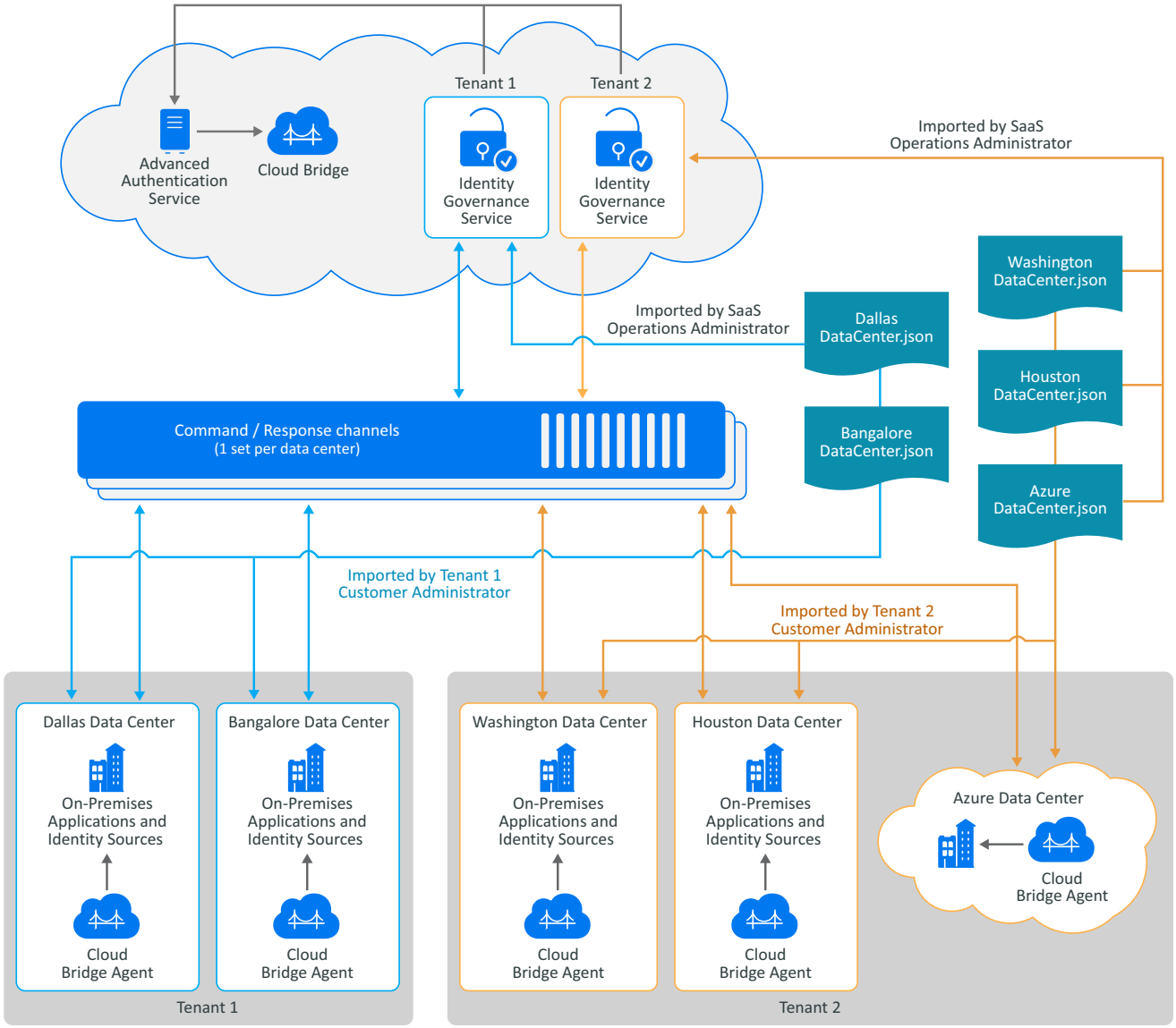
Log In to Identity Governance Service

After signing up for 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. Micro Focus recommends 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.

Install and Configure the Cloud Bridge Agent

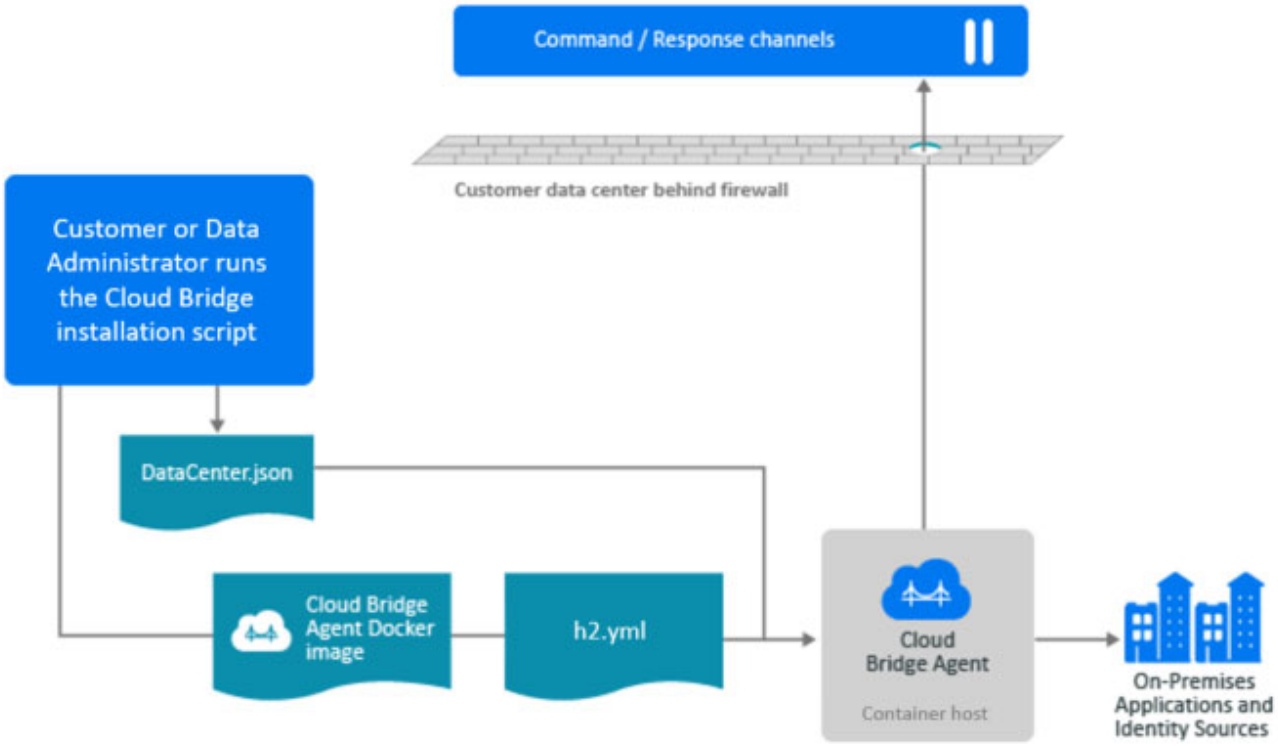
In as a Service environment, **Cloud Bridge** is a data transfer bridge between the application in the cloud and data sources in on-premises environments. The **Cloud Bridge Agent** is the entity that responds to the collection and fulfillment commands and directs them to the proper data source for execution.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

Figure 2 *Overview of Cloud Bridge Setup*



The Cloud Bridge Data Center in your Identity Governance tenancy will be created by the Micro Focus SaaS team based on the information you provide in the technical questionnaire. **Data Centers** are a conceptual representation of your Cloud Bridge Agent instance. Run the script generated on the Advanced Authentication Cloud Bridge Repository page to install the Cloud Bridge Agents on your local systems, and then configure Identity Governance Data Source Connections and Data Sources as needed to connect to your on-premises data sources. The following diagram provides an overview of the Cloud Bridge Agent configuration.

Figure 3 *Overview of Cloud Bridge Agent Configuration On Premises*



For additional information about the Cloud Bridge technical requirements, installation, and configuration, see the following sections.

- "Hardware and Software Minimum Requirements" on page 4
- "Install the Cloud Bridge Agent" on page 5
- "Configure Data Source Connection" on page 5
- "Add Credential for the Data Source Connection" on page 5
- "Perform Additional Steps when Using Cloud Bridge with Specific Templates" on page 6
- "Configure Data Sources and Collect and Publish Data" on page 8

Hardware and Software Minimum Requirements

You must have administrator privileges to install the Cloud Bridge Agent.

- Hardware Requirements
  - CPUs: 4
  - Memory: 16 GB
  - Disk Space: 200 GB
- Operating System Requirements
  - Debian 10
  - RHEL 8.3

- SUSE Linux Enterprise Server 15.1 or later patched version of 15.x
- Ubuntu 18.04 LTS Server Edition or later

- Container Requirements
  - Docker 19.03.x or later
  - Podman 1.6.4 or later

NOTE: You must configure a DNS entry for the Cloud Bridge Agent in order to use a secure connection. You will not be able to connect over SSL (port 636) if you are using a host file.

Install 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 IGA 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 and installing Cloud Bridge Agent, see the *Advanced Authentication Administration Guide*.

To install the Cloud Bridge Agent on premises, see the instructions provided by the CyberRes support team.

Configure Data Source Connection

After installing the agent, you must configure a data source connection in Identity Governance, then add credentials using the Cloud Bridge UI. For information about configuring data source connections, see "Understanding Cloud Bridge and Configuring Data Source Connections" in the *Identity Governance as a Service User and Administration Guide*.

Add Credential for the Data Source Connection

To add credentials:

1. Go to the Cloud Bridge URL: http*://localhost (CBA IP address or DNS name)*:8080.
2. Enter the unique ID, your full DN for your service account (for example, `CN=svc-id-admin,CN=Users,DC=support,DC=test`), and the password for this account.
3. (Conditional) When using Cloud Bridge, specify ordinal for authentication method for IDM AE Permission collector, and SCIM collectors and fulfillers. For information about ordinals, see "Collecting from IDM AE Permission Collector using Cloud Bridge" on page 7 and "Collecting Data from SCIM Compatible Applications and Processing Change Requests using Cloud Bridge" on page 7.
4. Click **Add Credential**.
5. Enter the Cloud Bridge Admin (cbadmin) password you specified when running the Cloud Bridge script you generated in Advanced Authentication. You will see a message stating that the credential was added successfully.
6. Repeat the steps to create additional data source connections to the same data center.
7. (Conditional) If you want to create data source connections to another data center, create credentials by visiting the URL for that data center.

8 (Optional) View the existing credentials you have by visiting http://localhost (CBA IP address or DNS name:8080/api/v1/credential.

9 (Optional) If you need to delete a credential, the preferred method when using Cloud Bridge 1.6.2 is to use the curl command:

`curl -X "DELETE" http://localhost (CBA IP address or DNS name):8080/api/v1/credential/"UniqueID"`.

When using Cloud Bridge 1.7.2 or later versions, instead of the curl command, you can log into the Cloud Bridge URL, specify external ID of the data center, then delete credentials.

Perform Additional Steps when Using Cloud Bridge with Specific Templates

NOTE: Micro Focus supports Cloud Bridge only in Identity Governance as a Service deployments.

Typically, collecting from on-premises and Cloud data sources using Cloud Bridge does not require unique procedures. However, when collecting from unique data sources or from CSV files, additional steps might be required.

- "Collecting from CSV Files Using Cloud Bridge" on page 6
- "Collecting from a JDBC Source using Cloud Bridge" on page 7
- "Collecting from IDM AE Permission Collector using Cloud Bridge" on page 7
- "Collecting Data from SCIM Compatible Applications and Processing Change Requests using Cloud Bridge" on page 7

Collecting from CSV Files Using Cloud Bridge

Note that if you plan to collect from CSV files using Cloud Bridge, *you must place the files in the `conf` directory*. Navigate to the location where the Cloud Bridge agent is installed, then place the CSV file in the `conf` directory or create different subfolders to separate the applications and place the file in the subfolders. For example,

- `/opt/netiq/mycba/conf/users.csv` or
- `/opt/netiq/mycba/conf/csv/oracle/users.csv`

Alternately, drop the CSV files to a subfolder of the `conf` directory that a network administrator previously configured as an NFS mount. This method enables Data administrators from various locations, to place the CSV files without requiring access to the server where the Cloud Bridge agent is installed.

IMPORTANT: We do not support changes within the Cloud Bridge container.

Before collecting, administrators need not restart the Cloud Bridge agent when creating new subfolders in the `conf` directory or when new CSV files are placed in those directories.

Collecting from a JDBC Source using Cloud Bridge

If you plan to collect data from a JDBC source using Cloud Bridge, *you must rename the JAR files and save them to the lib folder relative to the Cloud Bridge agent*.

1. Ensure that the JAR files are placed in the `/opt/netiq/bridge/lib` folder.
2. Rename the JAR files as `generic1.jar` to `generic10.jar`.
3. (Conditional) If the file is not already in the lib folder, place the `dist-collectors.jar` in the same lib folder.

   NOTE: If you do not have the `dist-collectors.jar`, please contact the SaaS Support team.

4. Restart the Cloud Bridge Agent.

Collecting from IDM AE Permission Collector using Cloud Bridge

Identity Manager AE Permission collector is a unique collector and requires both LDAP and user application credentials. All objects including roles collected using this collector are represented as permissions in the Identity Governance catalog. Note that the Identity Manager Automated Fulfillment fulfiller also uses the same credentials.

Use the following table to understand the order and ordinal number that you need to specify for this collector.

Ordinal (Credential Position)	Authentication type	Credential Set
0	LDAP	◆ User Name used to connect to Identity Vault Server (cn=admin,ou=sa,o=system) ◆ Password
1	User Application	◆ User Name used to connect to User Application (cn=uaadmin,ou=sa,o=data) ◆ Password

When using Cloud Bridge 1.6.2, specify the ordinals using the following curl command:

```
curl -v -X POST -H "Content-Type: application/json" -d
'{"credentials":[{"uniqueId": "UniqueId","username":
"cn=admin,ou=sa,o=system","password": "password","ordinal":
0},{"uniqueId":"UniqueId", "username": "cn=uaadmin,ou=sa,o=data","password":
"password","ordinal": 1}]}'  http://localhost (CBA IP address or DNS name):8080/
api/v1/credential/pair.
```

When using Cloud Bridge 1.7.2 or later versions, log in to the Cloud Bridge URL, then specify the ordinal.

Collecting Data from SCIM Compatible Applications and Processing Change Requests using Cloud Bridge

SCIM connectors requires a particularly complex configuration template that supports three different authentication types, each of which have different credential parameters that are required to properly configure the collectors and fulfillers. When using the bearer token authentication method, you will need to

specify username and password, then OAuth2 client ID and secret for API access to the SCIM compatible application. The process for configuring the applications and generating the client ID and secret will vary based on your data source. For additional information about getting the client ID and secret, contact the application owner.

You can collect data from SCIM compatible application from other SaaS environments to the Identity Governance as a Service catalog without enabling the Cloud Bridge connection. However, to collect data from on-premises or SaaS environment using the Cloud Bridge, you will need the upcoming 1.7.2 version of the Cloud Bridge.

Use the following table to understand the ordinal number that you need to specify for SCIM collectors and fulfillers.

Ordinal (Credential Position)	Authentication type	Credential Set
3	Basic Auth	◆ User Name ◆ Password
4	Access Token	◆ Access Token Header ◆ Access Token
5	Bearer Token	◆ User Name ◆ Password
6	Bearer Token	◆ Client ID ◆ Client Secret

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 with these credential sets, it is *critical* that the proper ordinal value be utilized for the authentication type being utilized. For example, if a SCIM Identity Collector is being configured in Identity Governance and Basic Auth is selected for the Authentication Method, the basic authentication credentials would need to be added to the CBA 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 CBA using the ordinal value shown above.

Configure Data Sources and Collect and Publish Data

Once you have established data source connections with the Cloud Bridge, you can 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 sections and chapters in the *Identity Governance as a Service User and Administration Guide*:

- "Understanding Data Administration"
- "Understanding Collectors"
- "Collecting Identities"
- "Collecting Applications and Application Data"
- "Publishing Collected Data"
- "Setting up Fulfillment Targets and Fulfilling Changesets"

Request Access and Perform Governance Tasks

For information about requesting access and performing other governance tasks such as setting up access reviews, and creating policies, and managing data, see the *Identity Governance as a Service User and Administration Guide*.

Additional Documentation

For additional documentation, visit the Micro Focus Identity Governance and Administration 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 Support Website (https://support.cyberreshelp.com/) or email cyberressupport@microfocus.com (mailto:cyberressupport@microfocus.com).

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

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