Service Description

Identity Governance as a Software-as-a-Service

October 2020

MICRO FOCUS

V7.4

Contents

This Service Description describes the components and services included in Micro Focus Identity Governance Software-as-a-Service (which also may be referred to as "IG SaaS"). Unless otherwise agreed to in writing this Service Description is subject to the Micro Focus Customer Terms for Software-as-a-Service or the applicable Micro Focus Pass-Through Terms and represents the only binding terms governing Micro Focus International plc and its affiliates ("Micro Focus") respective obligations regarding its provision of this SaaS to the end-user customer. Any other descriptions of the features and functions of the SaaS, public statements, including advertisements, shall not be deemed as additional features or functionalities that Micro Focus is required to deliver.

Standard Service Features

SaaS service delivery components

For the initial offering, the components will be as follows:

IG SaaS Delivery Components

One Production Tenant	✓
One Common Cloud Identity Repository	✓
One Staging Tenant (Staging Tenant is of a lesser capacity that the production tenant)	✓
Identity and Access Management Reporting	✓
Cloud Bridge (if necessary, to communicate with customer data center(s))	✓

✓ **= Included**

O **= Optional for a fee**

Identity Governance Capabilities

IG SaaS features include:

- Business & Technical Role Management
- Separation of duties
- Certification Reviews
- Request & Approval
- Governance Insights
- Identity Integration with on premises identities through the Identity Manager Identity Vault
- Scheduled and change event-based identity collection options from Identity Manager, eDirectory or Active Directory
- Fulfillment options via various connectors
- Identity Governance Reporting
- Cloud Bridge

IG SaaS includes a dedicated Cloud Bridge, which allows organizations to securely collect from and integrate with firewall-protected applications that reside within one or more data centers in their environment, while limiting the risk to opening up firewall configurations.

Application Administration

The initial solution set up will include providing certain information to the IG SaaS system. If integration with on premises identity repositories (such as the Identity Manager Identity Vault) or on premises application integration is desired, the client side administrator will need to make use of the Cloud Bridge to form the integration

Service Components

The Customer may contact Micro Focus through the CyberResSupport@microfocus.com or access CyberRes Portal.com. The Micro Focus Support Team will either provide support to the Customer directly or coordinate delivery of this support. The severity of the request determines the response from the team.

Severity Level	Technical response	Update Frequency	Target For Resolution	What Qualifies?
1	Immediate	Hourly	2 hours	Total or substantial failure of service. Known or suspected security events
2	30 mins	Every 2 hours	4 hours	Significant degradation of service, major feature inability
3	4 hours	Every 8 hours	16 hours	Performance issues outside the norm but not substantial enough to prevent usability of a feature. Issues with reports generated from within the customer's Tenant.
4	As available	As available	Determined by the customer impact or LOE	Bugs in deployed products not substantial enough to prevent required customer functionality from being accessible but requiring development time to resolve.

Monitoring

Micro Focus monitors components of IG SaaS for 24x7 availability. Micro Focus uses a centralized notification system to deliver proactive communications about application changes, outages and scheduled maintenance.

Capacity and Performance Management

IG SaaS will be continually monitored for performance issues. Proactive capacity and performance management procedures are in place to ensure the architecture of the environment meets the needs of its customers.

Operational Change Management

Micro Focus follows a set of standardized methodologies and procedures for efficient and prompt handling of changes to SaaS infrastructure and application, which enables beneficial changes to be made with minimal disruption to the service. Changes to production environments are reviewed prior to implementation to ensure they are appropriately scheduled and tested before promotion to production.

Solution Data Backup and Retention

The data backup and retention described in this section are part of Micro Focus's overall business continuity management practices designed to attempt to recover availability to customers of IG SaaS and the Common IAM SaaS Components, following an outage or similar loss of service.

Micro Focus's standard storage and backup measures are Micro Focus's only responsibility regarding the retention of this data, despite any assistance or efforts provided by Micro Focus to recover or restore Customer's data.

Disaster Recovery

1. **Business Continuity Plan**

   Micro Focus SaaS continuously evaluates different risks that might affect the integrity and availability of Micro Focus SaaS. As part of this continuous evaluation, Micro Focus SaaS develops policies, standards and processes that are implemented to reduce the probability of a continuous service disruption. Micro Focus documents its processes in a business continuity plan ("BCP") which includes a disaster recovery plan ("DRP"). Micro Focus utilizes the BCP to provide core Micro Focus SaaS and infrastructure services with minimum disruption. The DRP includes a set of processes that Micro Focus SaaS implements and tests Micro Focus SaaS recovery capabilities to reduce the probability of a continuous service interruption in the event of a service disruption.

2. **Backups**

   Micro Focus SaaS utilizes cloud-native functions such as replication between primary and secondary availability zones to ensure data availability and recoverability. All replicas reside within the same governmental compliance boundary to ensure adherence to all applicable data residency regulations. Real-time replication is used between primary and standby nodes to facilitate an RPO of 2 hours. No removable media is used at any time to ensure the protection of customer data.

SaaS Security

Micro Focus maintains an information and physical security program designed to protect the confidentiality, availability and integrity of Customer Personal Data and confidential information (the "Micro Focus Security Program").

Technical and Organizational Measures

This section describes Micro Focus´s standard technical and organizational measures, controls and procedures, which are intended to help protect the Customer-provided SaaS Data. Micro Focus regularly tests and monitors the effectiveness of its controls and procedures. No security measures are or can be completely effective against all security threats, present and future, known and unknown. The measures set forth in this section may be modified by Micro Focus, but represent a minimum standard. Customer remains responsible for determining the sufficiency of these measures.

Physical Access Controls

Micro Focus maintains physical security standards designed to prohibit unauthorized physical access to the Micro Focus equipment and facilities used to provide SaaS and include Micro Focus data centers and data centers operated by third parties. This is accomplished through the following practices:

- presence of on-site security personnel on a 24x7 basis;
- use of intrusion detection systems;
- use of video cameras on access points and along perimeter;
- Micro Focus employees, subcontractors and authorized visitors are issued identification cards that must be worn while on premises;
- monitoring access to Micro Focus facilities, including restricted areas and equipment within facilities;
- securing equipment hosting Customer-provided SaaS Data in designated caged areas; and maintaining an audit trail of access.

Access Controls

Micro Focus maintains the following standards for access controls and administration designed to make Customer-provided SaaS Data accessible only by authorized Micro Focus personnel who have a legitimate business need for such access:

- secure user identification and authentication protocols;
- authentication of Micro Focus personnel in compliance with Micro Focus standards and in accordance with ISO27001 requirements for segregation of duties
- Customer provided SaaS data is accessible only by authorized Micro Focus personnel who have a legitimate business need for such access, with user authentication, sign-on and access controls;
- employment termination or role change is conducted in a controlled and secured manner;
- administrator accounts should only be used for the purpose of performing administrative activities;
- each account with administrative privileges must be traceable to a uniquely-identifiable individual;
- all access to computers and servers must be authenticated and within the scope of an employee's job function;
- collection of information that can link users to actions in the Micro Focus SaaS environment;
- collection and maintenance of log audits for the application, OS, DB, network and security devices according to the baseline requirements identified;
- restriction of access to log information based on user roles and the "need-to-know;" and prohibition of shared accounts.
- use of multi-factor authentication to provide state-of-the-art access to the SaaS systems.

Data Segregation

Micro Focus SaaS environments are segregated logically by Micro Focus SaaS access control mechanisms. Internet-facing devices are configured with a set of access control lists (ACLs), which are designed to prevent unauthorized access to internal networks. Micro Focus uses security solutions on the perimeter level such as: firewalls, IPS/IDS, proxies and content based inspection in order to detect hostile activity in addition to monitoring the environment's health and availability.

Data Encryption

Micro Focus SaaS uses industry standard techniques to encrypt Customer-provided SaaS Data in transit. All inbound and outbound traffic to the external network is encrypted.

Audit

Micro Focus appoints an independent third party to conduct an annual audit of the applicable policies used by Micro Focus to provide the applicable Micro Focus IG SaaS solution. A summary report or similar documentation will be provided to Customer upon request. Subject to the execution of Micro Focus's standard confidentiality agreement, Micro Focus agrees to respond to a reasonable industry standard information security questionnaire concerning its information and physical security program specific to Micro Focus SaaS provided pursuant to the applicable Supporting Material no more than once per year. Such information security questionnaire will be considered Micro Focus Confidential Information.

Micro Focus Security Policies

Micro Focus conducts annual reviews of its policies around the delivery of IG SaaS against ISO 27001. Micro Focus regularly re-evaluates and updates its information and physical security program as the industry evolves, new technologies emerge or new threats are identified.

Security Incident Response

In the event Micro Focus confirms a security incident resulted in the loss, unauthorized disclosure or alteration of Customer-provided SaaS Data ("Security Incident"), Micro Focus will notify Customer of the Security Incident and work to mitigate the impact of such Security Incident. Should Customer believe that there has been unauthorized use of Customer's account, credentials, or passwords, Customer must immediately notify Micro Focus Security Operations Center via CyberResSOC@MicroFocus.com

Micro Focus Employees and Subcontractors

Micro Focus requests that all employees involved in the processing of Customer-provided SaaS Data are authorized personnel with a need to access the Customer-provided SaaS Data, are bound by appropriate confidentiality obligations and have undergone appropriate training in the protection of customer data. Micro Focus requests that any affiliate or third party subcontractor involved in processing Customer-provided SaaS Data enters into a written agreement with Micro Focus, which includes confidentiality obligations substantially similar to those contained herein and appropriate to the nature of the processing involved.

Data Subject Requests

Micro Focus will, within three (3) business days of receipt, refer to Customer any queries from data subjects in connection with Customer-provided SaaS Data.

Scheduled Maintenance

To enable Customers to plan for scheduled maintenance by Micro Focus, Micro Focus reserves predefined timeframes to be used on an as-needed basis.

A twenty-four-hour period once a quarter starting at Saturday, midnight in the local data center region, and ending at Sunday, midnight.

- This window is considered an optional placeholder for major releases and events that could be significantly service impactful. If the window is to be exercised, and a major disruption expected, all customers should be notified no later than ten business days before.

A two-hour maintenance window once a month starting Thursday, midnight in the local data center region.

- This is for patching of environments. Patching should be done in a non-service disrupting fashion; however, some elements may require a brief outage to update properly. Customers will be notified at least five business days in advance if any actual service disruption is expected.

A four-hour maintenance window once a month starting Saturday, midnight in the local data center region.

- This time is set aside for system updates and product releases that cannot be performed without a visible customer impact. Use of this window is optional, and customers should be notified at least ten business days in advance if any outage is expected.

In case of any holiday conflicts, the regularly scheduled window will automatically fall to the following week on the same day of the week.

Micro Focus determines whether and when to apply a SaaS Upgrade to Customer's Micro Focus IG SaaS solution and IAM SaaS Common Components. Unless Micro Focus anticipates a service interruption due to a SaaS Upgrade, Micro Focus may implement a SaaS Upgrade at any time without notice to Customer. Micro Focus aims to use the Scheduled Maintenance windows defined herein to apply SaaS Upgrades. Customer may be required to cooperate in achieving a SaaS Upgrade that Micro Focus determines in its discretion is critical for the availability, performance or security of Micro Focus IG SaaS solution and the IAM SaaS Common Components.

Service Decommissioning

Customer may cancel Micro Focus SaaS by providing Micro Focus with thirty (30) days written notice prior to the expiration of the SaaS Order Term ("Cancellation"). Such Cancellation shall be effective upon the last day of the then current SaaS Order Term. Upon Cancellation, expiration, or termination of the SaaS Order Term, Micro Focus may disable all Customer access to the IG SaaS solution and IAM SaaS Common Components, and Customer shall promptly return to Micro Focus (or at Micro Focus's request destroy) any Micro Focus Materials.

Micro Focus will make available to Customer such data in the format generally provided by Micro Focus. The target timeframe is set forth below in the Termination Data Retrieval Period Service Level Agreement (SLA) section. After such time, Micro Focus shall have no obligation to maintain or provide any such data, which will be deleted in the ordinary course.

Service Level Commitments

Micro Focus provides the following Service Level Commitments for the purpose of further measuring the quality of service that Micro Focus is delivering to the Customer.

1. **Solution Provisioning Time Service Level Objective (SLO)**
   Solution Provisioning is defined as the Micro Focus IG SaaS solution being available for access over the internet. Micro Focus targets to make Micro Focus IG SaaS available within five (5) business days of the customer's purchase order (PO) being booked within the Micro Focus order management system.

2. **Tenant Off boarding SLO**
   Micro Focus guarantees a tenant off boarding time of two days from the time in which the Customer submits the formal written request.

3. User Removal SLO

Micro Focus guarantees that after the completion of this request, analytical results about the removed user will no longer be stored or available within the application

4. Solution Availability SLA

Solution Availability is defined as the Micro Focus IG SaaS production application being available for access and use by Customer and its Authorized Users over the Internet. Micro Focus will provide Customer access to the Micro Focus IG SaaS production application on a twenty-four hour, seven days a week (24x7) basis at a rate of 99.5 % ("Solution Uptime").

5. Measurement Method

On a quarterly basis, the availability of the IG SaaS customer instance will be measured using the measurable days in the quarter (total days minus planned downtime, including maintenance, upgrades, etc.) as the denominator. The numerator is the denominator minus the number of days where a tenant's deadline is not met, to give the percentage of days that met the SLA (e.g. 119 days / 120 possible days = 99% availability). All SaaS monitoring will be paused at the beginning of each scheduled maintenance window and restarted at the completion of the window.

6. Boundaries and Exclusions

Performance and Availability SLA Metrics shall not apply in any of the following exceptions, and neither the IG SaaS will be considered unavailable nor any Service Level Failure be deemed to occur in connection with any failure to meet the requirement or impaired ability of Customer or its Authorized Users to access or use the IG SaaS solution:

- Overall Internet congestion, slowdown, or unavailability
- Unavailability of generic Internet services (e.g. DNS servers) due to virus or hacker attacks
- Force majeure events as described in the terms of the SaaS agreement
- Actions or omissions of Customer (unless undertaken at the express direction of Micro Focus) or third parties beyond the control of Micro Focus
- Unavailability due to Customer equipment or third-party computer hardware, software, or network infrastructure not within the sole control of Micro Focus
- Scheduled Maintenance
- Scheduled Version Updates

7. Reporting

Micro Focus Customer Success Manager (CSM) and the Customer will schedule and conduct regular Quarterly Business Reviews (QBR). For the purpose of reviewing the Customer's business objectives, the service performance, service usage, roadmap updates and planned continuous improvement initiatives. The CSM and the Customer will agree the meeting agenda in advance and will record agreed actions and priorities.

8. Termination Data Retrieval Period SLO

The Termination Data Retrieval Period is defined as the length of time in which the customer can retrieve a copy of their IG SaaS data or the data from the IAM SaaS Common Components from Micro Focus. Micro Focus targets to make available such data for download in the IG SaaS or the format of the IAM SaaS Common Components generally provided by Micro Focus for 30 days following the termination of the SaaS Order Term.

Standard Service Requirements

Roles and Responsibilities

This section describes general Customer and Micro Focus responsibilities relative to the IG SaaS solution. Micro Focus's ability to fulfill its responsibilities relative to SaaS is dependent upon Customer fulfilling the responsibilities described below and elsewhere herein:

Customer Roles and Responsibilities

Customer Role	Responsibilities
Business owner	• Owns the business relationship between the customer and Micro Focus • Owns the business relationship with the range of departments and organizations using the IG SaaS solution and associated components • Manages contract issues
Subject Matter Expert	• Leverages & educates other users about the product functionality designed by the IG SaaS solution • Provides periodic feedback to the IG SaaS Administrator

Micro Focus Roles and Responsibilities

Micro Focus Role	Responsibilities
Primary Support Contact (PSC)	• Serves as the customer liaison to Micro Focus • Coordinates Micro Focus resources including system and process experts as necessary as well as day to day issues with the SOC staff • Facilitates ongoing mentoring • Coordinates with the customer during required and periodic maintenance • Oversees the customer onboarding process
Service Operation Staff (SOC)	• Primary point of contact for service requests. • The Service Operations Center staff is responsible for all services such as support and maintenance, or issues regarding availability of the IG SaaS solution and the IAM SaaS Common Components • Provides 24x7 application support
Operations staff (Ops)	• Monitors the customer instance of the IG SaaS solution and IAM SaaS Common Components for availability • Provides 24x7 SaaS infrastructure and application support • Performs system-related tasks such as backups, archiving, and restoring instances according to Micro Focus's standard practices

Assumptions and Dependencies

This Service Description is based upon the following assumptions and dependencies between the Customer and Micro Focus:

- Customer must have internet connectivity to access this Micro Focus IG SaaS Service.
- Micro Focus IG SaaS Service will be performed remotely and delivered in English only.
- A SaaS Order term is valid for a single application deployment, which cannot be changed during the SaaS Order term.
- The service commencement date is the date on which Customer´s IG SaaS application is made available to the customer
- The import of Customer data into the IG SaaS solution during the implementation requires that the information is made available to Micro Focus at the appropriate step of the solution implementation and in the Micro Focus designated format.
- Customer must ensure that its administrators maintain accurate contact information with Micro Focus SaaS.
- Customer has determined, selected, and will use options in the Customer environment that are appropriate to meet its requirements, including information security controls, connectivity options, and business continuity, backup and archival options.
- Customer will establish and follow secure practices for individual account-based access for accountability and traceability.

Interaction with on-premises IDM instance

In the cases where a customer's IG SaaS instance is communicating with any of a customer's on premises systems, the performance of this communication cannot be guaranteed due to a number of factors such as:

- Bandwidth between the SaaS instance and the customer's premises
- Bandwidth within the customer site from the on premise bridge and the IDM instance

Micro Focus IG SaaS Service is provided based on the assumption that Customer will implement and maintain the following controls in its use of Micro Focus IG SaaS Service:

- Appointing authorized users
- Configuring its Micro Focus IG SaaS Service account to require that end user passwords are sufficiently strong and properly managed
- Procedures for access approvals, modifications and terminations.

Good Faith Cooperation

Customer acknowledges that Micro Focus's ability to perform the Services depends upon Customer's timely performance of its obligations and cooperation, as well as the accuracy and completeness of any information and data provided to Micro Focus. Where this Service Description requires agreement, approval, acceptance, consent or similar action by either party, such action will not be unreasonably delayed or withheld. Customer agrees that to the extent its failure to meet its responsibilities results in a failure or delay by Micro Focus in performing its obligations under this Service Description, Micro Focus will not be liable for such failure or delay.