Service Description

OpenText Core Identity Foundation

February 2026

opentext™

Contents

This Service Description describes the components and services included in OpenText Core Identity Foundation (which also may be referred to as "SaaS") and, unless otherwise agreed to in writing, is subject to the Micro Focus Customer Terms for Software-as-a-Service ("SaaS Terms") found at https://www.opentext.com/about/legal/software-licensing. Capitalized terms used but not defined herein shall have the meanings set forth in the SaaS Terms.

Standard Service Features

High Level Summary

The OpenText Core Identity Foundation provides a cloud-based enterprise service that is intended to provide essential Identity and Access Management capabilities that organizations need to support a secure Identity program. The OpenText Core Identity Foundation provides the following Identity and Access Management Capabilities:

- Identity Governance – an enterprise service intended to enable organizations to define policies, calculate risk, run reviews, and manage identity and access through a customer's organization
- Advanced Authentication Limited – a Multi-Factor Authentication (MFA) framework that provides increased security through standard, adaptive and continuous authentication services
- Identity Lifecycle Manager – an enterprise service to provide a common identity repository and lifecycle management capabilities for all identities across the platform.
- Single Sign-On – seamless, secure authentication and authorization service to connect users to critical resources
- Password Management – User self-service including all aspects of password management
- Identity Intelligence Basic – Integrated reporting and dashboarding capabilities for the Identity SaaS Platform
- Privileged Access Management – a comprehensive service for managing privileged access across hybrid environments.

SaaS Delivery Components

SaaS Delivery Components	
One Production Tenant	✓
One Stage Tenant	✓
External Integration via Cloud Bridge	✓
Customer Onboarding	✓
Concierge Onboarding and Managed Services	O
✓ **= Included**	
O = Optional for a fee	

Customer Onboarding

The SaaS includes the initial (not to exceed 40 hours), short track onboarding of Customer onto the OpenText Identity Core Foundation service, and implementation of components into Customer's environments to connect the OpenText Core Identity Foundation service and Customer's environment. During the onboarding process, an expert OpenText Field Security Engineer ("**Field Engineer**") will assist with the installation and configuration of a cloud bridge agent that will enable the SaaS to communicate to applications ("Application(s)") housed in Customer's environments.

The OpenText-Cybersecurity Concierge ("Concierge"), upon customer request, will schedule the Customer Onboarding at a time mutually agreed upon by Micro Focus and Customer, during standard business hours that excludes holidays, unless otherwise agreed upon. Any services provided outside of standard business hours will be subject to additional charges.

During the Customer Onboarding, the Field Engineer will:

- Conduct a questionnaire interview, in which the customer's complete and accurate answers are required to onboard onto the SaaS.
- Provide guidance to customer in verification of the pre-requisite hardware, software, and other requirements for SaaS and cloud bridge agent.
- Support the installation of two (2) cloud bridge agents for Production Environment and one (1) cloud bridge agent for Staging Environment at one (1) site.

Conduct communication verification between cloud bridge agent and Saas. Any additional scope, work outside the standard business hours or service effort can be purchased as add-ons through the Cyber Resilience Program ("CRP") defined in the Cybersecurity Services Handbook available at www.opentext.com/agreements.

Concierge Onboarding and Managed Services Overview

As an optional service, Customer can purchase OpenText-Cybersecurity Concierge led onboarding for implementation of components into Customer's environments, regular updates to these components and managed services delivered by the Field Engineer.

This long track onboarding (not to exceed 160 hours) of Customer onto the OpenText Identity Core Foundation service includes the implementation of components into Customer's environment to connect the OpenText Core Identity Foundation service and Customer's environment. During the onboarding process, a Field Engineer will assist with the installation and configuration of a cloud bridge agent that will enable the SaaS to communicate to applications ("Application(s)") housed in Customer's environments.

The OpenText-Cybersecurity Concierge, upon customer request, will schedule the onboarding at a time mutually agreed upon by Micro Focus and Customer, during standard business hours that excludes holidays, unless otherwise agreed upon. Any services provided outside of standard business hours will be subject to additional charges.

During the Concierge Onboarding, the Field Engineer will:

- Conduct a questionnaire interview, in which the Customer's complete and accurate answers are required for onboarding onto the SaaS.
- Guide Customer in its verification of the pre-requisite hardware, software, and other requirements for SaaS and cloud bridge agent.

- Support the installation of two (2) cloud bridge agents for Production Environment and one (1) cloud bridge agent for Staging Environment.
- Conduct communication verification between cloud bridge agent and Saas.
- Support the installation of one (1) remote loader.
- Support configuration of one (1) SCIM driver and review the identity source to ensure that identities are imported in the solution.
- Validate authentication using passwordless method of email address and phone number.
- Provide guidance while Customer performs migration of user identities
- Support configuration of Identity Governance's identity collection
- Validate Advanced Authentication configurations with Customer

During the term of the subscription, the Field Engineer will support any updates to the cloud bridge agent. Each update will be coordinated by the Concierge and the Field Engineer will provide up to four (4) hours of support.

During the term of the subscription, the Field Engineer can provide occasional advice and guidance. Customers that routinely require more than four (4) hours of advice and guidance can purchase additional support through the Cyber Resilience Program ("CRP") defined in the Cybersecurity Services Handbook available at www.opentext.com/agreements.

Any additional scope, work outside the standard business hours or service effort can be purchases as add-on through the Cyber Resilience Program ("CRP") defined in the Cybersecurity Services Handbook available at www.opentext.com/agreements.

Micro Focus will provide Customer with a communication (chat) channel and case management portal access for Customer to have a single point of contact with Micro Focus through a Cybersecurity Concierge, and get ongoing technical guidance and advice from a Field Engineer. Concierge will provide:

- Kick Off – Cybersecurity Concierge will schedule a Kick Off virtual meeting to review the SaaS service, the onboarding activities and the managed security
- Priority Support - All support tickets will be prioritized and tracked by the Cybersecurity Concierge, who will act as a single point of contact for their resolution.
- Status Report - Deliver regular service status reports as part of the service review meeting, usually with monthly frequency, which reviews the service activities and achievement in Managed Security Services.
- Advocacy – The Cybersecurity Concierge and Field Engineer will act as an advocate to ensure Micro Focus understands and responds to Customer's priorities, including Micro Focus' software engineering and technical support departments.

SaaS Operational Services

SaaS Operational Services	
Identity Governance SaaS	✓
Advanced Authentication SaaS Limited	✓
Identity Lifecycle Manager	✓
Single Sign-On SaaS	✓
Password Management SaaS	✓
Identity Intelligence SaaS Basic	✓
Cloud Bridge Agent Updates	O
Risk Service	O
Privileged Access Management SaaS	O
✓ **= Included**	
O **= Optional for a fee**	

Summary of OpenText Core Identity Foundation Services

Identity Governance SaaS

Identity Governance SaaS 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 via SaaS.

Advanced Authentication SaaS Limited

Advanced Authentication SaaS Limited extends Customer's security of sensitive information beyond username and password. Multifactor authentication increases protection from fraud or unauthorized access.

Identity Lifecycle Manager SaaS

Identity Lifecycle Manager SaaS provides a common identity repository and lifecycle management capabilities for all identities across the platform. This service provides a bi-directional event-based synchronization engine to capture and transmit changes to identities in any connected system in near-real time. Identity Lifecycle Manager SaaS allows to control identity data flow across the applications in the environment.

Single Sign-On SaaS

Single Sign-On SaaS provides single sign-on and secure access to web-based applications, cloud applications, and federated business-to-business interactions. This service provides authorized users with adaptive, context-aware secure access to web, API, and cloud applications from anywhere and from any device.

Single Sign-On SaaS uses industry standards, such as SAML, OAuth, and OpenID Connect to deliver federated single sign-on and supports multi-factor authentication, access control, and API access.

Password Management SaaS

Password Management SaaS is a web-based password management solution. It eliminates the users' dependency on administrators to change their passwords and reduces the workload of the help desk thereby potentially reducing the cost incurred by the company. Users can change their own passwords and reset forgotten password based on the configured challenge-response information. Password Management SaaS also allows administrators to ensure that all passwords in the organization comply with established policies.

Privileged Access Management SaaS

Privileged Access Management SaaS (PAM) is a web-based solution that safeguards your critical infrastructure by securing and controlling administrative access across hybrid environments. By enabling identity-driven security controls, Privileged Access Management SaaS ensures real-time access policies align with dynamic business needs. PAM helps mitigate security risks, enhances governance, and simplifies compliance through continuous monitoring and intelligent privilege management.

Identity Intelligence SaaS Basic

Identity Intelligence SaaS Basic is an analytics solution. Identity Intelligence SaaS Basic enables Customers to analyze and monitor Identity Governance SaaS using predefined and custom dashboards and reports.

Cloud Bridge Agent Updates

Micro Focus may require Customer to update their cloud bridge agent to maintain compatibility with the SaaS. Under Concierge Onboarding and Managed Services, the Customer will receive the updates and the Field Engineer will provide assistance with all updates. Alternatively, Customers can purchase update support as add-on through the Cyber Resilience Program ("CRP") defined in the Cybersecurity Services Handbook available at www.opentext.com/agreements

Architecture Components

The OpenText Core Identity Foundation architecture is composed of the following services:

- Identity Governance SaaS
- Identity Intelligence SaaS Basic
- Advanced Authentication SaaS Limited
- Identity Lifecycle Manager
- Password Management SaaS
- Single Sign-On SaaS

The OpenText Core Identity Foundation includes the Identity Governance SaaS and Advanced Authentication SaaS Limited deployment architectures.

Identity Governance SaaS Architecture (includes Identity Intelligence SaaS Basic) – The Identity Governance SaaS Architecture can be found in the "Service Description for Identity Governance on SaaS" located at the following: https://www.opentext.com/about/legal/software-licensing

Advanced Authentication SaaS Limited Architecture (includes Single Sign-On SaaS and Password Management SaaS) – The Advanced Authentication SaaS Limited Architecture can be found in the "Advanced Authentication on SaaS" located at the following: https://www.opentext.com/about/legal/software-licensing

Onsite components are installed and configured by the Customer or Customer-contracted consultants. Micro Focus does not install, deploy, or manage on-premise components that may be required to use Advanced Authentication SaaS Limited.

Application Administration

The solution set up includes providing certain information to the OpenText Core Identity Foundation. 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.

Customer accesses OpenText Core Identity Foundation using a web browser and the URLs provided to them. Once securely logged in, Customer can perform administrative tasks such as configuring, assigning authentication requirements to events, and running and scheduling backups.

Service Support

Customer may contact Micro Focus through submitting online support tickets. The Micro Focus Support Team will either provide support to the Customer directly or coordinate delivery of this support.

Online support for SaaS is available at: https://home.software.microfocus.com/myaccount
Support for on-premise components is available at: https://www.microfocus.com/en-us/support

Micro Focus staffs and maintains a 24x7x365 Service Operations Center, which will be the single point of contact for all issues related to the support for SaaS. Customer will maintain a list of authorized users who may contact Micro Focus for support. Customer's authorized users may contact Micro Focus for support via the Web portal 24 hours a day, 7 days a week.

Service Monitoring

Micro Focus monitors SaaS availability 24x7. Micro Focus uses a centralized notification system to deliver proactive communications about service changes, outages, and scheduled maintenance. Alerts and notifications are available to Customer online at: https://home.software.microfocus.com/myaccount

Capacity and Performance Management

The architecture allows for additional capacity for applications, databases, and storage.

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.

Limitations of Managed Security Services

This Service will be delivered as a single, continuous event for the Stage and Production environments of the OpenText Core Identity Foundation Service. Environments requiring multiple engagements or phases over longer periods of time are not included in this Service but can be accommodated at additional cost through a Statement of Work. Activities such as, but not limited to, the following are excluded from this service:

- Migrating existing on-premise Identity Manager into OpenText Core Identity Foundation Service.
- Re-implementing or redesigning an existing Roles-Based-Provisioning-Module configuration into OpenText Core Identity Foundation Service.
- Configuring a new driver with a new application.
- Configuring an identity source not included with the Service.
- The Services described in this document do not include delivery of services provided by OpenText Software Support, including fixing of software bugs. Customer is responsible for maintaining a valid support contract with OpenText and contacting OpenText Support for support related issues.
- Field Engineer is provided as a coverage-based engagement model with Micro Focus on a part time basis (up to 2-hours per month).
- Cybersecurity Concierge is provided as a coverage-based engagement model with Micro Focus on a part time basis (up to 2-hours per month).
- Any OpenText Professional Services beyond the license limitations of the included Service.

Monthly Active User (MAU)

The Monthly Active User (MAU) is the metric for measuring access to OpenText Core Identity Foundation as further specified in this Service Description. MAU represents how often a unique Identity (user) interacts with the OpenText Core Identity Foundation Services within a given calendar month.

How is MAU Measured

All activity that is captured in the OpenText Core Identity Foundation log files is evaluated to determine how many **Unique Identities** are captured within a given month. The total number of unique Identities can be reviewed by the customer by running a built in Identity Intelligence report.

NOTE: MAU does not have a 1:1 relationship with individual "users". Each micro-service within the OpenText Core Identity Foundation may log a different Unique Identity for a given user.

MAU Definitions

- MAU - A method used to measure the following attributes for Enterprise Workforce Identity. Workforce Identity is includes: (1) a permanent or temporary user and (2) a non-carbon-based identity, either of which uses or is used to access enterprise applications and/or data.
  - ***MONTHLY*** - Log files are reviewed every calendar month to determine how many Active Unique Identities interact with a Core Identity Foundation service
  - ***ACTIVE*** - A Unique Identity shows up at least once in a Core Identity Foundation service log files during a given calendar month

- ***Unique Identity*** –Each and every object (user, service principle, API key, IoT device etc.) included in the Enterprise Workforce Identity
  - **NOTE: EACH service accessed by a Unique Identity is counted as a separate MAU activity**

- Light MAU – The Light MAU follows the same definitions as MAU listed above with the exception that it can only be used for Business to Consumer (B2C) or Government to Citizen (G2C) identities.
  - B2C and G2C is defined as follows:
    - **B2C/G2C Business to Consumer (B2C) and Government to Citizen (G2C)**
      - **Consumer** Means a third-party entity or person outside a customer's organization to whom the customer provides services or goods as part of your normal business operations, excluding current or former employees, agents, contractors or suppliers
      - **Citizen** Means a third-party citizen or resident to whom a customer that is a Governmental Entity provides services or goods as part of its normal business operations, excluding current or former employees, agents, contractors or suppliers.

What Service Use MAUs

All services specified or not specified in this Service Description that are provisioned to an OpenText Core Identity Foundation customer SaaS tenant may be considered when measuring MAUs.

How are MAU Entitlements Enforced

MAU is purchased by a customer on an annual basis. The customer purchases sufficient MAU bundles equal to or greater than the greatest number of Unique Identities that may be reported in the MAU report found in the Identity Intelligent Service.

If the number of Unique Identities within a given month exceeds the amount of MAU contracted, the customer will be notified via email that they have exceeded the contracted amount. The first time this happens, the customer will have ninety (90) days to either prove they have consistently reduced the number of Unique Identities used within a month OR they have the option to place a co-terminus purchase for additional MAU bundles.

MAU Entitlements

As part of the OpenText Core Identity Foundation, each SaaS tenant is entitled to three thousand (3000) MAUs.

Additional Add-On Services

When additional add-on services are purchased, the entitled MAUs and/or additional purchased MAU bundles can be applied to the additional add-on services.

Data Backup and Retention

The data backup and retention described in this section are part of Micro Focus' overall business continuity management practices designed to attempt to recover availability to SaaS and SaaS Data for Customer following an outage or similar loss of service for SaaS.

SaaS Data

Customer is solely responsible for the data, text, audio, video, images, software, and other content input into a Micro Focus system or environment during Customer's (and its Affiliates' and/or Third Parties') access or use of Micro Focus SaaS ("SaaS Data"). The following types of SaaS Data reside in the OpenText Core Identity Foundation environment:

Advanced Authentication Service: Configuration data of Advanced Authentication and configuration data of user defined Methods for multi-factor authentication.

Identity Governance Service: Identity Governance Service stores identity, application, entitlements (permissions), governance policies configuration, runtime, and historical data, including audit events and identity activity stream data, report configuration data, services configuration and settings data along with SaaS platform integration configuration.

Password Management Service: Password Management Service stores application specific configuration data along with SaaS platform integration configuration.

Identity Intelligence Service Basic: Identity Intelligence SaaS configuration data, user activity and business data from the Identity products for dashboard, reporting, and analysis.

Micro Focus performs a backup of SaaS Data every day. Micro Focus retains each backup for the most recent seven (7) days.

Micro Focus' standard storage and backup measures are Micro Focus' only responsibility regarding the retention of the SaaS Data, despite any assistance or efforts provided by Micro Focus to recover or restore the SaaS Data. Customer may request via a service request for Micro Focus to attempt to restore SaaS Data from Micro Focus' most current backup. Micro Focus will be unable to restore any data not properly entered by Customer or lost or corrupted at the time of backup or if Customer´s request comes after the 7 days data retention time of such backup.

For AWS OpenText Core Identity Foundation implementations
OpenText Core Identity Foundation is implemented over AWS technology service stack in a redundant mode over multiple Availability Zones (AZs) with elastic load balancing allowing us to quickly recover an OpenText Core Identity Foundation service in case of a disaster. Availability zones (AZs) are distinct geographical locations that are engineered to be insulated from failures in other AZs. Elastic IP addresses are used to work around host or availability zone failures by quickly remapping the address to another running instance or a replacement instance that was just started by placing OpenText Core Identity Foundation instances in multiple AZs, an application can be protected from failure at a single location.

Disaster Recovery for SaaS

Business Continuity Plan
Micro Focus continuously evaluates different risks that might affect the integrity and availability of SaaS. As part of this continuous evaluation, Micro Focus 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 SaaS and infrastructure services with minimum disruption. The DRP includes a set of processes that implements and tests SaaS recovery capabilities to reduce the probability of a continuous service interruption in the event of a service disruption.

For AWS OpenText Core Identity Foundation implementations
OpenText Core Identity Foundation SaaS is implemented using a cloud-based technology service stack in a redundant mode over multiple availability zones. The failure of one zone will not impact the service availability as the system will automatically failover from the other zones. In the event of a disaster impacting more than one zone at the same time, such as a complete cloud region, the DRP's target is to provide restoration of the OpenText Core Identity Foundation SaaS within 24 hours (Recovery Time Objective, RTO) following Micro Focus' declaration of a disaster.

Backups
Micro Focus performs both on-site and off-site backups with a 24 hours recovery point objective (RPO). Backup cycle occurs daily where a local copy of production data is replicated on-site between two physically separated storage instances. The backup includes a snapshot of production data along with an export file of the production database. The production data is then backed up at a remote site. Micro Focus uses storage and database replication for its remote site backup process. The integrity of backups is validated by (1) real time monitoring of the storage snapshot process for system errors, and (2) and annual restoration of production data from an alternate site to validate both data and restore flows integrity.

SaaS Security

Micro Focus maintains an information and physical security program designed to protect the confidentiality, availability, and integrity of SaaS Data.

Technical and Organizational Measures

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
- Maintaining an audit trail of access

Access Controls

Micro Focus maintains the following standards for access controls and administration designed to make 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
- 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 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"
- Prohibition of shared accounts

Availability Controls

Micro Focus´s business continuity management process includes a rehearsed method of restoring the ability to supply critical services upon a service disruption. Micro Focus' continuity plans cover operational shared infrastructure such as remote access, active directory, DNS services, and mail services. Monitoring systems are designed to generate automatic alerts that notify Micro Focus of events such as a server crash or disconnected network.

Controls regarding disruption prevention include:

- Uninterruptible power supplies (UPS) and backup power generators
- At least two independent power supplies in the building
- Robust external network connectivity infrastructure

Data Segregation

SaaS environments are segregated logically by 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 uses industry standard techniques to encrypt 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 SaaS. A summary report or similar documentation will be provided to Customer upon request. Subject to Customer's execution of Micro Focus' 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 SaaS 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 SAAS against ISO 27001, which includes controls derived from ISO 27034 – "Information Technology – Security Techniques – Application Security". 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.

Customer initiated security testing is not permitted, which includes application penetration testing, vulnerability scanning, application code testing or any other attempt to breach the security or authentication measures of the SaaS.

Security Incident Response

In the event Micro Focus confirms a security incident resulted in the loss, unauthorized disclosure, or alteration of SaaS Data ("Security Incident"), Micro Focus will notify Customer of the Security Incident and work to reasonably 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 SED@opentext.com.

Micro Focus Employees and Subcontractors

Micro Focus requires that all employees involved in the processing of SaaS Data are authorized personnel with a need to access the SaaS Data, are bound by appropriate confidentiality obligations and have undergone appropriate training in the protection of SaaS Data. Micro Focus requires that any affiliate or third-party subcontractor involved in processing 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 refer to Customer any queries from data subjects in connection with SaaS Data.

Scheduled Maintenance

To enable Customer to plan for scheduled maintenance by Micro Focus, Micro Focus reserves predefined timeframes to be used on an as-needed basis. Micro Focus reserves a weekly two (2) hours window (Sunday 00:00 to 02:00 Pacific Standard Time) and one (1) monthly four (4) hour window (Sunday in the 00:00 to 08:00 Pacific Standard Time block). These windows will be used on an as-needed basis.

Planned windows will be scheduled at least two (2) weeks in advance when Customer action is required, or at least four (4) business days in advance otherwise.

Scheduled Version Updates

"SaaS Upgrades" are defined as major version updates, minor version updates, and binary patches applied by Micro Focus to Customer's SaaS in production. These may or may not include new features or enhancements. Micro Focus determines whether and when to develop, release and apply any SaaS Upgrade. Customer is entitled to SaaS Upgrades during the applicable SaaS Order Term unless the SaaS Upgrade introduces new functionality that Micro Focus offers on an optional basis for an additional fee.

Micro Focus will use the Scheduled Maintenance windows defined herein to apply the most recent service packs, hot fixes, and minor version updates to SaaS. To enable Customer to plan for scheduled major version updates by Micro Focus, Micro Focus will schedule major version updates at least two (2) weeks in advance. However, if Micro Focus does not receive Customer's cooperation in achieving the SaaS Upgrade in a timely manner, Micro Focus reserves the right to charge Customer additional fees that are related to Customer's SaaS instance remaining on a version that is beyond the "end of support" period. Customer also understands that this status may prevent the most recent patches from being applied to its SaaS solution, and that the availability, performance, and security of SaaS as described in this Service Description may be impacted as a result.

Service Decommissioning

Upon expiration or termination of the SaaS Order Term, Micro Focus may disable all Customer access to SaaS, and Customer shall promptly return to Micro Focus (or at Micro Focus' request destroy) any Micro Focus materials including the uninstall of the Cloud Bridge Agent.

Micro Focus will make available to Customer any SaaS Data in Micro Focus' possession in the format generally provided by Micro Focus. The target timeframe is set forth below in Termination Data Retrieval Period SLO. After such time, Micro Focus shall have no obligation to maintain or provide any such data, which will be deleted.

Service Level Objectives

Micro Focus provides clear, detailed, and specific Service Level Objectives (SLOs) for SaaS. These SLOs are targets used by Micro Focus to deliver the service and are provided as guidelines. They in no way create a legal requirement or obligation for Micro Focus to meet these objectives.

Micro Focus will provide self-service access to Customer to the Service Level Objectives data online at https://home.software.microfocus.com/myaccount

SaaS Provisioning Time SLO
SaaS Provisioning Time is defined as SaaS being available for access over the internet. Micro Focus targets to make SaaS available within five (5) business days of Customer's Order for SaaS being booked within the Micro Focus order management system.

Customer is responsible for installing, configuring, deploying, updating, and paying any additional fees (if required) for any additional on-premise components for its applications. Any on-premise components are not in scope of the SaaS Provisioning Time SLO.

Additionally, the import of SaaS Data into the application is not in scope of the SaaS Provisioning Time SLO.

SaaS Availability SLO
SaaS Availability is defined as the SaaS production application being available for access and use by Customer over the Internet. Micro Focus will provide Customer access to the SaaS production application on a twenty-four hour, seven days a week (24x7) basis at a rate of 99.9 % ("SaaS Uptime").

Measurement Method
SaaS Uptime shall be measured by Micro Focus using Micro Focus monitoring software running from a minimum of four global locations with staggered timing.

On a quarterly basis, SaaS Uptime will be measured using the measurable hours in the quarter (total time minus planned downtime, including maintenance, upgrades, etc.) as the denominator. The numerator is the denominator value minus the time of any outages in the quarter (duration of all outages combined) to give the percentage of available uptime (2,198 actual hours available / 2,200 possible available hours = 99.9% availability).

An "outage" is defined as two consecutive monitor failures within a five-minute period, lasting until the condition has cleared.

Boundaries and Exclusions
SaaS Uptime shall not apply to or include any time during which SaaS is unavailable in connection with any of the following (specifically, the number of hours of unavailability in the measured period per the Measurement Method section above due to the following shall not be included in either the numerator or the denominator for the measurement):

- Overall Internet congestion, slowdown, or unavailability
- Unavailability of generic Internet services (e.g., DNS servers) due to virus or hacker attacks
- Force majeure events
- 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 SaaS upgrades

Online Support Availability SLO

Online Support Availability is defined as the SaaS support portal https://home.software.microfocus.com/myaccount being available for access and use by Customer over the Internet. Micro Focus targets to provide Customer access to the SaaS support portal on a twenty-four hour, seven days a week (24x7) basis at a rate of 99.9% ("Online Support Uptime").

Measurement Method
Online Support Uptime shall be measured by Micro Focus using Micro Focus monitoring software running from a minimum of four global locations with staggered timing. On a quarterly basis, Online Support Uptime will be measured using the measurable hours in the quarter (total time minus planned downtime, including maintenance, upgrades, etc.) as the denominator. The numerator is the denominator value minus the time of any outages in the quarter (duration of all outages combined) to give the percentage of available uptime (2,198 actual hours available / 2,200 possible available hours = 99.9 availability).
An "outage" is defined as two consecutive monitor failures within a five-minute period, lasting until the condition has cleared.

Boundaries and Exclusions
Online Support Uptime shall not apply to or include any time during which the SaaS support portal is unavailable in connection with any of the following (specifically, the number of hours of unavailability in the measured period per the Measurement Method section above due to the following shall not be included in either the numerator or the denominator for the measurement):

- Overall Internet congestion, slowdown, or unavailability
- Unavailability of generic Internet services (e.g., DNS servers) due to virus or hacker attacks
- Force majeure events
- Actions or inactions 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 SaaS Upgrades

Initial SaaS Response Time SLO

The Initial SaaS Response Time refers to the support described herein. It is defined as the acknowledgment of the receipt of Customer's request and the assignment of a case number for tracking purposes. Initial SaaS Response will come as an email to the requester and include the case number and links to track it using Micro Focus online customer portal. The Initial SaaS Response Time covers both service request and support requests. Micro Focus targets to provide the Initial SaaS Response no more than one hour after the successful submission of Customer's request.

SaaS Support SLOs

There are two types of SaaS Support SLOs: Service Request and Support Request SLOs.

- The Service Request SLO applies to the majority of routine system requests. This includes functional system requests (product add/move/change), informational, and administrative requests.
- The Support Request SLO applies to issues that are not part of the standard operation of the service and which causes, or may cause, an interruption to or a reduction in the quality of that service.

The Response and Resolution Targets are provided as guidelines and represent typical request processing by Micro Focus SaaS support teams. They in no way create a legal requirement or obligation for Micro Focus to respond in the stated time. The Response and Resolution Targets, including their scope and determining factors (such as impact and urgency), are further described at https://home.software.microfocus.com/myaccount/slo/.

Termination Data Retrieval Period SLO

The Termination Data Retrieval Period is defined as the length of time in which Customer can retrieve a copy of their SaaS Data from Micro Focus. Micro Focus targets to make available such data for download in the format 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 SaaS. Micro Focus' 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 SaaS • Manages contract issues
Project Manager	• Coordinates customer resources as necessary • Serves as the point of contact between the customer and Micro Focus • Drives communication from the customer side • Serves as the point of escalation for issue resolution and service-related issues • Contact Micro Focus within 90 days of when the Order Term starts to schedule delivery of any onboarding and managed services • Ensures access provided as needed to Micro Focus personnel

Administrator	• Serves as the first point of contact for SaaS end users for problem isolation • Performs SaaS administration • Provides tier-1 support and works with Micro Focus to provide tier-2 support • Coordinates end-user testing as required • Leads ongoing SaaS validation • Trains the end-user community • Coordinates infrastructure-related activities at the customer site • Owns any customization
Subject Matter Expert	• Leverages the product functionality designed by Customer's SaaS administrators. • Provides periodic feedback to the SaaS Administrator

Micro Focus Roles and Responsibilities

Micro Focus Role	Responsibilities
Customer Service Centre (CSC)	• Primary point of contact for service requests. The customer can contact the Service Operations Center for all services such as support and maintenance, or issues regarding availability of SaaS • Provides 24x7 application support
Operations Staff (Ops)	• Monitors the Micro Focus systems and SaaS for availability • Performs system-related tasks such as backups, archiving, and restoring instances according to Micro Focus' standard practices • Provides 24x7 SaaS infrastructure support

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 SaaS
- SaaS will be delivered remotely in English only, which may require Customer to grant Micro Focus access to its network and servers, including but not limited to VPN token and client software, server names and IP addresses and administrative names and passwords.
- 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 Order is booked within the Micro Focus order management system
- The import of SaaS Data into SaaS 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
- 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
- Hardware and software requirements to support the OpenText Core Identity Foundation as per the latest available system requirements for OpenText cloud bridge agent at https://www.microfocus.com/documentation/identity-and-access-management/iam-services/cloud-bridge-agent-admin/index.html and OpenText remote loaders at https://www.netiq.com/documentation/identity-manager-49-drivers/
- All information required in the completed pre-installation customer questionnaire
- The customer will be responsible for all applicable on premise data backup

Furthermore, SaaS is provided based on the assumption that Customer will implement and maintain the following controls in its use of SaaS:

- Configuring Customer's browser and other clients to interact with SaaS
- Configuring Customer's network devices to access SaaS
- Appointing authorized users
- Configuring its SaaS 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' ability to provide SaaS and related 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.

Additional Terms for Onboarding and Managed Services

Services excludes hardware maintenance and repair, software maintenance, education services, or other standard support services provided by OpenText; Software-as-a-Service, and outsourcing services. Acceptance of Deliverables occurs upon delivery.

Hiring of Employees. You agree not to solicit, or make offers of employment to, or enter into consultant relationships with, any OpenText employee involved, directly or indirectly, in the performance of services hereunder for one (1) year after the date such employee ceases to perform Services under the terms of this

Data sheet. You shall not be prevented from hiring any such employee who responds to a general hiring program conducted in the ordinary course of business and not specifically directed to such OpenText employees.

Authorization to Install Software. During the provision of Services, OpenText may be required to install copies of third-party or OpenText-branded software and be required to accept license terms accompanying such software ("Shrink-Wrap Terms") on your behalf. Shrink-Wrap Terms may be in electronic format, embedded in the software, or contained within the software documentation. Customer hereby acknowledges that it is customer's responsibility to review Shrink-Wrap Terms at the time of installation, and hereby authorizes OpenText to accept all Shrink-Wrap Terms on its behalf.

Intellectual Property. OpenText may provide OpenText tools, templates, and other pre existing intellectual property of OpenText during the course of providing services ("OpenText Pre-existing IP"). OpenText Pre-existing IP does not include, nor is considered a part of, either the Deliverables or OpenText software products. OpenText retains all intellectual property ownership rights in such OpenText Pre-existing IP. All OpenText Pre-existing IP is OpenText Confidential Information. OpenText Pre-existing IP may be governed by additional license terms that are embedded in the OpenText Pre-existing IP.