Service Description

Connected SaaS

August 2023

MICRO FOCUS®
FOCUS
is now **opentext**™

Contents

This Service Description describes the components and services included in Micro Focus Connected SaaS (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.microfocus.com/en-us/legal/software-licensing. Capitalized terms used but not defined herein shall have the meanings set forth in the SaaS Terms.

Standard Service Features

This section defines what is included in the Standard Service for the Micro Focus Connected SaaS offering during the SaaS Order term.

Solution Components

Micro Focus offers the following components, features, and functionalities as part of Micro Focus Connected SaaS offering:

High Level Summary

Micro Focus Connected SaaS provides a cloud-based enterprise service intended to backup files on PC and Mac devices and enable customers the ability to access and recover files. Micro Focus Connected SaaS is a policy-based solution that enables customers to ensure that business critical data is backed up and accessible to end users and administrators on behalf of the customer organization's requirements around business continuity, productivity, and compliance.

Architecture Components

Micro Focus Connected SaaS includes an agent software component that is installed on each PC or Mac device that the customer chooses to backup and/or for file synchronization. Mobile apps are also available to support access to files that have been backed up from PC or Mac devices. Web-based user interfaces are provided for both end users and administrators. Web interfaces enable users to search for, view, and access files backed up from devices assigned to the user account. Web interfaces for administrators enable user/group administration, policy creation and deployment, as well as management and reporting capabilities. Deployment of the agent software to the end user devices is the responsibility of Customer.

Micro Focus Connected SaaS also consists of cloud-based services to which customer data is backed up via agents. Micro Focus Connected SaaS is multi-tenant; meaning each customer receives their own computer and storage resources within a multi-tenant farm. Each customer's data is logically and securely segregated for security purposes. Each customer is called a tenant.

Service Components

Micro Focus offers the following core SaaS support and operational services as part of Micro Focus Connected SaaS offering:

Service Support

The Customer may contact Micro Focus through a variety of methods such as online support tickets or telephone support. The Micro Focus Support Team will either provide support to the Customer directly or coordinate delivery of this support.

Online support is available at: https://www.microfocus.com/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 Micro Focus Connected SaaS for the Customer. The customer will maintain a list of authorized users who may contact Micro Focus for support. The customer's authorized users may contact Micro Focus for support via the Web portal or telephone 24 hours a day, 7 days a week.

Service Monitoring

Micro Focus provides monitoring of this Micro Focus Connected SaaS solution backend components 24x7 using system monitors for availability. Micro Focus uses a centralized notification system to deliver proactive communications about application changes, outages, and scheduled maintenance. Alerts and notifications sent to customer administrators via email.

Capacity and Performance Management

All tiers of the SaaS infrastructure are proactively monitored for capacity and performance. The architecture allows for addition of capacity to 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.

Disaster Recovery

As part of Micro Focus´s overall business continuity management practices, Micro Focus has processes and procedures in place to recover from potential disaster scenarios. Micro Focus utilized data centers are tested for the wide range of disaster scenarios including fire, loss of Internet connectivity, physical security breaches, and power outages.

For AWS Micro Focus Connected SaaS implementations:
Micro Focus Connected 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 Micro Focus Connected SaaS within 24 hours (Recovery Time Objective, RTO) following Micro Focus's declaration of a disaster.

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 re or can be completely effective against all security threats, present and future, known and unknown. The measures set forth 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, including 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 ISO 27001 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´ business continuity management process includes 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.

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 to detect hostile activity, and monitoring the environment's health and availability.

Data Encryption

Micro Focus SaaS uses industry standard techniques to encrypt SaaS Data in transit. All inbound and outbound traffic to the external network is encrypted. Data in the relational database, index, and object storage (data at rest) is also encrypted.

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. Micro Focus reserves a weekly two (2) hours window (Sunday 00:00 to 02:00 Eastern Standard Time) and one (1) monthly four (4) hour window (Sunday in the 00:00 to 08:00 Eastern 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) days in advance otherwise.

Scheduled Version Updates

"SaaS Upgrades" are defined as both major version updates, minor version updates and binary patches applied by Micro Focus to the Customer's Micro Focus Connected SaaS solution 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 as part of Micro Focus Connected SaaS service unless the SaaS Upgrade introduces new functionality that Micro Focus offers on an optional basis for an additional fee.

Micro Focus determines whether and when to apply a SaaS Upgrade to Customer's Micro Focus Connected SaaS solution. 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 above 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 Connected SaaS solution. In the event that the Customer fails to cooperate in a timely manner, Micro Focus may disable all further backups and services to the incompatible outdated versions of the Connected SaaS solution. Reasonable efforts will be made by Micro Focus to maintain prior data for data return purposes through the duration of the Customer's SaaS Order Term.

Micro Focus may, at its sole discretion, modify this Service Description and make available Updates to its customers which may add new and/or eliminate existing features, functions, operating environment and/or hardware platforms to the Subscription Service.

Service Decommissioning

Upon expiration or termination of the SaaS Order Term, Micro Focus may disable all Customer access to the Micro Focus Connected SaaS solution and Customer shall promptly remove Micro Focus Connected SaaS software from customer devices.

Following expiration or termination, Micro Focus will make available to Customer previously stored and available data via standard Micro Focus Connected SaaS self–service options. Customers may also request that Micro Focus return data to customer at an additional charge to customer. The target timeframe is set forth below in

section titled 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 in the ordinary course.

Service Level Objectives

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

Solution Provisioning Time SLO

Solution Provisioning is defined as the Micro Focus Connected SaaS solution being made available for access over the internet for a specified tenant. Micro Focus targets to make Micro Focus Connected SaaS available within 2 (two) business days of the customer's Order for SaaS being booked within the Micro Focus order management system.

Customer is responsible for installing and configuring any additional onsite components for his applications. Any onsite components of the solution are not in scope of the Solution Provisioning Time SLO.

Solution Availability SLO

Solution Availability is defined as the Micro Focus Connected 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 Connected SaaS production application on a twenty-four hour, seven days a week (24x7) basis at a rate of 99.5 % ("Solution Uptime").

Measurement Method

Solution Uptime shall be measured by Micro Focus using Micro Focus monitoring software.

On a quarterly basis, Solution 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 (2,189 actual hours available / 2,200 possible available hours = 99.5 availability).

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

Boundaries and Exclusions

Solution Uptime shall not apply to any of the following exceptions:

- 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 any of the following exceptions:

- 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

Initial SaaS Response Time SLO

The Initial SaaS Response Time refers to the Service Support section. It is defined as the acknowledgment of the receipt of a customer 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 a customer request.

Termination Data Retrieval Period SLO

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

Reporting
Micro Focus will provide a SaaS Service Uptime Metric Report ("Uptime Metric Report") in accordance with this attachment to the Customer upon request. If the Customer does not agree with the Uptime Metric Report, written notice of non-agreement must be provided to Micro Focus within fifteen (15 days) of receipt of the Uptime Metric Report.

Standard Service Requirements

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 Connected SaaS Service
- The service commencement date is the date on which Customer´s Order is booked within the Micro Focus order management system
- Micro Focus shall provision Customer to Micro Focus Connected SaaS service
- Micro Focus shall monitor and maintain Micro Focus Connected SaaS service
- Micro Focus shall deliver upgrades and updates to Micro Focus Connected SaaS application and operating environment

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

- Configuration of Customer's browser and other clients to interact with Micro Focus Connected SaaS Service
- Configuration of Customer's network and network devices to access Micro Focus Connected SaaS Service
- List of authorized users and administrators
- Proper configuration of Customer's deployed Micro Focus Connected SaaS agents
- Process and methods for successful deployment of Micro Focus Connected SaaS agents to users
- Customer defined Micro Focus Connected SaaS policies governing data retention and certain feature access

Good Faith Cooperation

Customer acknowledges that Micro Focus' 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.