Service Description

OpenText™ Core Enterprise Performance Engineering (LoadRunner Enterprise)

July 2025

opentext™

Contents

This Service Description describes the components and services included in OpenText™ Core Enterprise Performance Engineering (LoadRunner Enterprise) (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

OpenText™ Core Enterprise Performance Engineering (LoadRunner Enterprise) ("Core Enterprise Performance Engineering") provides a cloud-based enterprise service for centralized performance engineering. Core Enterprise Performance Engineering is remotely delivered by Micro Focus and provides a managed environment of Core Enterprise Performance Engineering software. The solution is designed for distributed teams with a centralized authority that needs to support testing from multiple lines of business, comprehensive reporting, flexible licensing, and capacity for temporary spikes.

SaaS Service Delivery Components

SaaS Delivery Components	Included
1 (one) Core Enterprise Performance Engineering production instance	✓
1 (one) Hosted Controller	✓

SaaS Operational Services

Operational Services	Included
Web services support	✓
External integrations support	O
Hosted Load Generators	O
Additional Concurrent Test Runs	O
Dedicated SaaS production instance	O
Dedicated IP Addresses	O
Virtual Private Network (VPN)	C

✓ **= Included**

O **= Optional for a fee**

C **= Custom deployment, optional for a fee, requires technical validation by Micro Focus SaaS and proof of concept**

Architecture Components

Core Enterprise Performance Engineering consists of these two (2) parts: (a) a cloud-based management platform with an interactive dashboard for managing, storing, and analyzing performance tests; and (b) an agent, installed by the Customer to execute the performance tests.

Core Enterprise Performance Engineering includes the following components:

Hosted Controller

The Hosted Controller is the Core Enterprise Performance Engineering component that is used to create and maintain performance testing scenarios. Access to one Hosted Controller is included with the basic Core Enterprise Performance Engineering deployment. One Hosted Controller enables Customer to execute one test. Hosted Controllers are dedicated to Customer and are available for 24x7 testing. Hosted Controllers may be shared among the Customer's Core Enterprise Performance Engineering projects and must be reserved in the Core Enterprise Performance Engineering Scheduler to avoid conflict. Hosted Controllers may be dedicated to individual projects or groups of projects as necessary.

A standard Hosted Controller machine provides one pack (1x) of 4 CPU cores and 100 GB of local Disk Storage and may support up to 75,000 Virtual Users and 30 Load Generators.

Additional Concurrent Test Runs – Customer may purchase Additional Concurrent Test Runs (each concurrent test run provides access to a single Hosted controller) to support concurrent test runs or a large number of Virtual Users.

Custom Hosted Controller Configurations – Customers who purchase Additional Concurrent Test Runs entitlements may request to pool the resources from these entitlements into a custom configuration to allow for the creation of fewer, higher-capacity Hosted Controllers based on the aggregated resources (e.g., CPU, Disk Storage). The total number of concurrent test runs that can be executed is equal to the number of provisioned Hosted Controllers. Example: A customer purchasing three 'Concurrent Test Runs' entitlements (each providing a standard 100 GB controller) has a total resource pool of 300 GB of storage. Customer may request this be provisioned as two Hosted Controllers: one standard Hosted Controller (100 GB) and one custom Hosted Controller with double capacity (200 GB). This configuration would support two concurrent test runs. Customer's requests will be granted based on availability.

Load Generator

The Load Generator is the Core Enterprise Performance Engineering component that executes the performance testing scenario when a performance test is initiated by the controller.

Hosted Load Generators – Customer may purchase Hosted Load Generator machines provided by Micro Focus. A standard Hosted Load Generator machine provides one pack (1x) of 4 CPU cores, a public IP address, an operating system of either Windows or Linux. Customer that purchased multiple Hosted Load Generator machines can request Micro Focus, based on availability, to deploy multiple packs of 4 CPUs on a single Hosted Load Generator machine. For example, a customer that purchased two Hosted Load Generators machines (each with one pack of 4 CPU cores), can request a single Hosted Load Generator machine with a total of eight CPU cores (2x packs of 4 CPU cores). Customer may purchase Dedicated IP Addresses that can be reserved for their tenant and be assigned to Hosted Load Generators per customer request.

On-premises Load Generator – Customer may deploy Load Generators on their premises (On-premises Load Generator) to test internal applications and generate load from anywhere.

MI Listener – To facilitate communication between on-premises Load Generators and the Core Enterprise Performance Engineering SaaS platform through a corporate firewall, Micro Focus's "Over the Firewall" (OFW) technology utilizes a hosted machine known as the MI Listener. The MI Listener securely relays communication for up to 30 On-premises Load Generators. One MI Listener machine is included with Core Enterprise Performance Engineering at no additional cost.

Additional MI Listeners – To obtain additional MI Listeners beyond the one included with the solution, Customers must purchase Hosted Load Generator entitlements. A purchased Hosted Load Generator entitlement can, upon request and based on availability, be provisioned as an MI Listener instead of a Hosted Load Generator. For example, Customer who purchases five Hosted Load Generator entitlements may request to have them provisioned as three Hosted Load Generators and two MI Listeners.

Virtual User

A Virtual User is a program that acts like a real user to simulate real user actions on a website or application. The Customer subscribes to Virtual Users and can run up to the maximum subscription in a given test.

Virtual User Flex Days

Virtual User Flex Days (VUFDS) is an option which allows execution of Virtual Users in unlimited number of runs against AUT within a single twenty-four (24) hour period from Customer's first execution. After the twenty-four (24) hour period, the remaining number of VUFDs is calculated by subtracting the number of used VUFDs, or in the case of concurrent usage, the maximum number of concurrent running VUFDs, from the total number of VUFDs. VUFDS expire one (1) year after the date of purchase. A Core Enterprise Performance Engineering Base Pack and Core Enterprise Performance Engineering version 2023 and above, are prerequisites for using VUFDS. Enterprise Performance Engineering VUFDs are protocol agnostic but do not include COM/DCOM, Templates and GUI protocols.

Additional Information

Core Enterprise Performance Engineering does not include support for Micro Focus diagnostics and IP Spoofing.

The following Core Enterprise Performance Engineering protocols are supported only with On-premises Load Generators: Microsoft.NET, .NET+, Cloud for AWS, CoAP, SDK, DNS (Domain Names Resolution), FTP (File Transfer Protocol), IMAP (Internet Messaging), Kafka, LDAP (Listing Directory Service), MAPI (Microsoft Exchange), MQTT, ODBC, Oracle - 2 Tier, POP3 (Post Office Protocol), SMP (SAP Mobile Platform), SMTP (Simple Mail Protocol), Tuxedo, Unified Functional Testing (UFT), Unit Test based on .NET, Citrix ICA, Teradici PCoIP, RDP, SAP GUI, UFT API, C, C++.NET, C#.NET, and VB.NET Template.

Core Enterprise Performance Engineering version 2023 and later provides limited support for On-premises Load Generator version N-1 and N-2. For example, when using Core Enterprise Performance Engineering v2023, limited support will be provided to On-premise Load Generator versions 2022 R2 and 2022 R1. It is

recommended to use the latest version N for On-premises Load Generators. Note that new capabilities that are introduced in a newer Enterprise Performance Engineering server version, may only run with newer On-premise Load Generator version and some security and / or functional patches may not be available for On Premises Load generators versions N-1 and N-2.

Micro Focus does not install, deploy, or manage on-premise components that may be used with Core Enterprise Performance Engineering. Customer is responsible for installing, configuring, deploying, updating, and paying any additional fees (if required) for any additional on-premise components for its applications.

Application Administration

Customer will access Core Enterprise Performance Engineering using a web browser and the URL provided to them. Once securely logged in, Customer can perform administrative tasks such as adding and deleting users, adding users to projects, allocating hardware, and running and scheduling performance tests.

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.saas.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 Features:
- System Availability SLO of 99.9%
- Customer Manager Services
- Solution Expert Services
- Welcome Package
- Technical Enablement and Pre-recorded enablement videos
- Email and Online Notifications
- On boarding: Kick off meeting, handover of support materials, verification of online access, service goals, and discussion of training requirements
- Major version updates: Notification period according to notification timelines via email, release notes and help resources available. Major version update meeting, including discussion of changes required to take advantage of new features and requirements to implement the update.
- Regular Service Reviews to review service quality and to provide feedback on improvements required
- Regular Adoption Reviews to plan how best to adopt product features and best practices based on your business objectives

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.saas.microfocus.com/myaccount/

Capacity and Performance Management

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.

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 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 SaaS environment: Customer inserted data (for example attachments, scripts, documents, and files).

Micro Focus performs a backup of SaaS Data every one (1) day. Micro Focus retains each backup for the most recent seven (7) days.

Micro Focus's standard storage and backup measures are Micro Focus's only responsibility regarding the retention of 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's 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.

Disaster Recovery

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 Core Enterprise Performance Engineering implementations

Core Enterprise Performance Engineering is implemented using AWS technology service stack in a redundant mode over two availability zones ("AZs"). Each AZ is designed to be isolated from failures in other AZs. The DRP's target is to provide restoration of the Micro Focus SaaS within twelve (12) hours following Micro Focus's declaration of a disaster, excluding, however, a disaster or multiple disasters causing the compromise of data centers in the separate AZs simultaneously, and excluding non-production environments.

Backups

Micro Focus SaaS performs both on-site and off-site backups with a 24-hour 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) 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 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"
- 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's 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 SaaS uses industry standard techniques to encrypt SaaS Data in transit and at rest. 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'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 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 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 requests 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 customer data. Micro Focus requests 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 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 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) 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's request destroy) any Micro Focus materials.

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 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.

SaaS Availability SLA

SaaS availability is 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 % ("Target Service Availability" or "TSA").

Measurement Method

TSA 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, the TSA will be measured using the measurable hours in the quarter (total time minus Downtime Exclusions) 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.

Downtime Exclusions

The TSA 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
- Outages caused by disruptions attributable to force majeure events (i.e., unforeseeable events outside of Micro Focus' reasonable control and unavoidable even by the exercise of reasonable care
- Customer-caused outages or disruptions
- Outages not caused by Micro Focus or not within the control of Micro Focus (i.e., unavailability due to problems with the Internet), unless caused by Micro Focus' service providers
- Unavailability due to Customer equipment or third-party computer hardware, software, or network infrastructure not within the sole control of Micro Focus
- Scheduled maintenance activities
- Scheduled SaaS Upgrades
- Customer exceeding the service restrictions, limitations or parameters listed in this Service Description and/or the Order
- Unavailability due to customizations made to the Micro Focus SaaS which are not validated, reviewed, and approved in writing by both parties
- System downtime requested by Customer
- Suspensions of the Micro Focus SaaS by Micro Focus as a result of Customer's breach of the SaaS Terms

Reporting

Micro Focus will provide self-service access to Customer to the availability data online at
https://home.saas.microfocus.com/myaccount/

In addition, Micro Focus will provide an Actual Service Availability Report ("ASA Report") in accordance with this Service Level Commitments section to Customer upon request. If Customer does not agree with the ASA Report, written notice of non-agreement must be provided to Micro Focus within fifteen (15 days) of receipt of the ASA Report.

Remedies for Breach of Service Levels

i. **Sole remedy.** Customer's rights described in this section state Customer's sole and exclusive remedy for any failure by Micro Focus to meet the agreed service levels.
ii. **Escalation.** Quarterly ASA below 98% shall be escalated by both parties to the Vice President (or equivalent).

iii. **Credits.** Subject to the terms herein, Micro Focus will issue a credit reflecting the difference between the measured ASA for a quarter is less than the TSA. ("**Remedy Percent**"). For clarity, several example calculations using this formula are illustrated in the table below:

Target Service Availability (TSA)	Actual Service Availability	Result	Remedy Percent
99.9 %	99.9%		Not Applicable
99.9%	94.9%	5% missed	5%
99.9%	90.9%	9% missed	9%

Customer must request credits in writing to Micro Focus within ninety (90) days of receipt of the ASA Report resulting in such credit and identify the support requests relating to the period where the SaaS production application was not available for access and use by the Customer over the internet. Micro Focus shall apply the requested credits on a quarterly basis.

Online Support Availability SLO

Online Support Availability is defined as the SaaS support portal https://home.saas.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.saas.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'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 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
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 solution 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's 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
- 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 Customer 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

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's 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.

Updated July 2025