Service Description

Dimensions RM on Software-as-a-Service

January 2025

opentext™

Contents

This Service Description describes the components and services included in Micro Focus Dimensions RM on Software-as-a-Service (which also may be referred to as "Dimensions RM SaaS" or "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.

1. Standard Service Features

1.1 High Level Summary

Dimensions RM SaaS is a remotely delivered engagement solution that provides a customer a managed environment of Dimensions RM SaaS. Micro Focus oversees the configuration and implementation of Dimensions RM SaaS and delivers on-going infrastructure, application, and support service remotely.

1.2 SaaS Service Delivery Components

SaaS Delivery Components	
One Dimensions RM SaaS production instance	☒
One VPN connection	☒

Dimensions RM SaaS is available in different virtual hardware sizings (processing power and memory) through a number of Dimensions RM SaaS Base Pack subscription options.

A valid Dimensions RM offering consists of a Base Pack selection plus the desired number of concurrent and named SaaS user subscription licenses.

1.3 SaaS Operational Services

Operational Services	
SSO integration	√*
LDAP integration	√
Micro Focus Connect	√
Web services support	√
* Restrictions apply. Only certain IDPs and integrations are supported	

√ = Included | O = Optional for a fee

1.4 Architecture Components

Dimensions RM SaaS

Micro Focus deploys Dimensions RM SaaS solution using shared infrastructure platform, monitors the system for 24x7 availability, and provides related 24x7 infrastructure support, including application version upgrades. Customer accesses SaaS through the internet (HTTPS).

On Premise components are installed and configured by Customer or Customer-contracted consultants. Micro Focus does not operate on premise components or third-party integrations on behalf of Customer and will not commit to any SLO for these services.

Standard configuration for Dimensions RM SaaS:

Property	Support value
System Availability	99.9% SLA
Available Tenants	1

Micro Focus Connect SaaS (MF Connect SaaS)

Micro Focus deploys MF Connect SaaS using shared infrastructure platform, monitors the system for 24x7 availability, and provides related 24x7 infrastructure support, including application version upgrades. Customer accesses MF Connect SaaS through the Internet (HTTPS). Micro Focus does not operate on premise components or third-party integrations on behalf of Customer and will not commit to any SLO for these services.

Property	Supported value
Connections	12
Sync interval	Minimum of 10 Minutes
Project pairs	12 connections with one single master to target pair, or less connections with more pairs
Audit log access	Access to Audit logs not older than 1 week
Storage limit	50GB
Sync items	60,000 (e.g.: 5,000 per project pair)
Available RAM	6GB
VPN tunnel support	Not Supported
Connectors	ALM/QC, Octane, Jira, and Azure DevOps

1.5 Application Administration

Customer accesses SaaS 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 or adding users to projects.

1.6 Service Support

Customer may contact Micro Focus through submitting online support tickets or by telephone. 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

Product support is available from the Micro Focus Dimensions RM Community at: https://community.microfocus.com/adtd/dimensionsrm/

Additional custom support, education or services can be purchased via FlexCare credits: https://www.microfocus.com/en-us/services/flexible-credits

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 or telephone 24 hours a day, 7 days a week.

Service Features:
- System Availability SLA of 99.9%
- Customer Manager Services
- Solution Expert Services
- Welcome Package
- Technical Enablement
- Email and Online Notifications
- Version updates. Notification period according to notification timelines via email, release notes and help resources available
- Regular Service Reviews to review service quality and to provide feedback on improvements required

1.7 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: http://software.microfocus.com/myaccount/

1.8 Capacity and Performance Management

The architecture allows for addition of capacity to applications, databases, and storage.

1.9 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.

2. Solution Data Backup and Retention

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

2.1 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's standard storage and backup measures are Micro Focus's only responsibility regarding the retention of this data, despite any assistance or efforts provided by Micro Focus to recover or restore Customer's data. Customer may request via a service request for Micro Focus to attempt to restore such 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.

2.2 Disaster Recovery

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.

Dimensions RM SaaS is implemented using a cloud-based technology service stack in a redundant mode over multiple availability zones. In case of a failure of one zone the DRP's target is to provide restoration of the Dimensions RM SaaS within 12 hours (Recovery Time Objective, RTO) following Micro Focus's declaration of a disaster; excluding, however, a disaster or multiple disasters causing the compromise of multiple availability zones simultaneously and excluding non-production environments.

2.3 Backups

Micro Focus 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, (2) validating CHECKSUM at the end of a backup process to assure the same number of bits exists on both source and destination storage systems, and (3) and annual restoration of production data from an alternate site to validate both data and restore flows integrity.

3. SaaS Security

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

3.1 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.

3.2 Physical Access Controls

Micro Focus maintains physical security standards designed to prohibit unauthorized physical access to the Micro Focus equipment and facilities used to provide SaaS and include Micro Focus data centers and data centers operated by third parties. This is accomplished through the following practices:
- Presence of on-site security personnel on a 24x7 basis
- Use of intrusion detection systems
- Use of video cameras on access points and along perimeter
- Micro Focus employees, subcontractors and authorized visitors are issued identification cards that must be worn while on premises
- Monitoring access to Micro Focus facilities, including restricted areas and equipment within facilities
- Securing equipment hosting SaaS Data in designated caged areas; and

- Maintaining an audit trail of access

3.3 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

3.4 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

3.5 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.

3.6 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.

4. 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.

5. 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.

6. 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 softwaresoc@microfocus.com.

7. 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 customer 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.

8. Data Subject Requests

Micro Focus will refer to Customer any queries from data subjects in connection with SaaS Data.

9. 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.

9.1 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 above to apply the most recent service packs and hot fixes and to perform upgrade to minor versions of the SaaS application solution. To enable Customers to plan for scheduled major version updates by Micro Focus, Micro Focus will be scheduling major version updates at least two (2) weeks in advance.

10. 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 in the ordinary course.

11. Solution Availability SLA

SaaS availability is the Dimensions RM 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.software.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.

12. 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").

12.1 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.

12.2 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

12.3 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

12.4 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/.

12.5 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.

13. Standard Service Requirements

13.1 Roles and Responsibilities

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

13.2 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 Dimensions RM 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 Dimensions RM SaaS end users for problem isolation - Performs Dimensions RM 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

13.3 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 Dimensions RM 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

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

- Configuring Customer's browser and other clients to interact with Dimensions RM SaaS
- Configuring Customer's network devices to access Dimensions RM SaaS
- Appointing authorized users
- Configuring its Dimensions RM SaaS account to require that end user passwords are sufficiently strong and properly managed
- Procedures for access approvals, modifications, and terminations

13.5 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.

247-000101-001