# Service Description

## Micro Focus ITMX United States Public Sector on Software-as-a-Service

December 2023

MICRO FOCUS
is now opentext™

# Contents

Contents ..... 2
Standard Service Features ..... 3
Data Backup and Retention ..... 8
SaaS Security ..... 9
Audit ..... 11
Micro Focus Security Policies ..... 11
Security Incident Response ..... 12
Micro Focus Employees and Subcontractors ..... 12
Data Subject Requests ..... 12
Scheduled Maintenance ..... 12
Service Decommissioning ..... 13
Service Level Objectives ..... 13
Standard Service Requirements ..... 16

This Service Description document describes the components and services included in Micro Focus ITMX for United States Public Sector Software-as-a-Service (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

## High Level Summary

Micro Focus Information Technology Management X ("ITMX") is a FedRAMP authorized platform, that centralizes security, logging, and management services for multiple services into one overall environment hosted within the AWS GovCloud infrastructure for the United States Public Sector.

ITMX includes the Micro Focus Service Management Automation X ("SMAX") solutions and associated components.

SMAX is a native cloud application that delivers a machine learning based IT service management (ITSM) and IT asset management (ITAM) capability with options for automated discovery of servers, software, and service models via Micro Focus Universal Discovery and CMDB (comprising of "Universal Discovery" and "UCMDB"). SMAX comes in 3 different service options depending on Customer requirements:

- **SMAX Express**
  Includes ITSM specific modules and capabilities.
- **AMX**
  Includes ITAM specific modules and capabilities.
- **SMAX Premium**
  Includes both ITSM and ITAM specific modules and capabilities included with SMAX Express and AMX

Unless specifically stated, the details provided within this Service Description apply to all 3 service options. Customers may purchase one (1) of the above solutions per tenant but cannot mix the service options within the same tenant. SMAX Express and AMX customers can upgrade to SMAX Premium for an additional fee.

Micro Focus oversees the deployment, infrastructure, operation, availability, security and data protection and support of the service.

## SaaS Delivery Components

### SMAX Express

| SaaS Delivery Components | Included |
|---|---|
| **One (1) SMAX Express SaaS production tenant** | ✓ |
| **Additional SMAX Express SaaS non-production tenant** | O |
| **Premium Discovery of a server OSI including dependencies** | O |
| **Asset Discovery of a server or workstation OSI** | O |
| **Import of nodes (and related information) into UCMDB without discovery** | O |

**✓ = Included**

**O = Optional for an additional fee**

## AMX

| SaaS Delivery Components | Included |
|---|---|
| One (1) AMX SaaS production tenant | ✓ |
| One (1) AMX SaaS non-production tenant | ✓ |
| Additional AMX non-production tenant | O |
| Premium Discovery of a server OSI including dependencies | O |
| Asset Discovery of a server or workstation OSI | O |
| Import of nodes (and related information) into UCMDB without discovery | O |
| ✓ = Included | |
| O = Optional for an additional fee | |

## SMAX Premium

| SaaS Delivery Components | Included |
|---|---|
| One (1) SMAX Premium SaaS production tenant | ✓ |
| One (1) SMAX Premium SaaS non-production tenant | ✓ |
| Additional SMAX Premium SaaS non-production tenant | O |
| Premium Discovery of a server OSI including dependencies | O |
| Asset Discovery of a server or workstation OSI | O |
| Import of nodes (and related information) into UCMDB without discovery | O |
| ✓ = Included | |
| O = Optional for an additional fee | |

## SaaS Operational Services

| SaaS Operational Services | Included |
|---|---|
| Onboarding | ✔ |
| Customer Success Management (CSM) Meetings | ✔ |
| Product Support | ✔ |
| Single sign-on support* | ✔ |
| ✔ = Included | |

**Restrictions apply. Only certain IDPs and integrations are supported.*

## Architecture Components

Micro Focus deploys SMAX and Universal Discovery using a shared infrastructure platform that is a multi-tenant environment, meaning that each customer receives their own unique tenant. This tenant incorporates a SMAX tenant, and a Universal Discovery and CMDB tenant. Customer access to SMAX is through the Internet over HTTPS.

Customer may purchase, for an additional fee, the following capabilities to integrate with SMAX:

- **Asset Discovery** – includes usage of the Universal Discovery module of the Universal Discovery and CMDB SaaS solution to discover operating system instances (OSI) of servers (physical, virtual, cloud, container) or workstations, in support of auto-populating SMAX Premium SaaS with details of the infrastructure environment Customer is supporting allows capturing configuration information about the servers or workstation themselves including the software installed on these servers or workstations and the environment in which the software is installed
- **Premium Discovery** – includes all features of Asset Discovery plus the capture configuration information about software running on servers and the dependencies that exist between servers and running software

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

## Universal Discovery and CMDB SaaS

Usage of Universal Discovery and CMDB with SMAX is accomplished through the communication of discovered data to the Universal Discovery and CMDB tenant that is part of Customer's SMAX rendering automated discovery results immediately visible to SMAX agents.

Customers who purchased the optional Asset Discovery or Premium Discovery capabilities for SMAX, are responsible for installing, configuring, deploying, and updating of the Universal Discovery Infrastructure Data Flow Probes ("Data Flow Probes" or "DFP"), and updating the Universal Discovery Content Pack as required for successful discovery.

**Premium Discovery** provides the discovery of one (1) Operating System Instance (OSI) and includes the capability to discover the configuration of servers, whether physical, virtual or cloud. Capabilities also include discovering installed and running software, mapping the inter-dependencies between servers and their software, and the dependencies between services and servers. Premium Discovery also includes all functionality described in Asset Discovery.

**Asset Discovery** provides the discovery of one (1) Operating System Instance (OSI) and includes the capability to discover the configuration of servers or workstations, whether physical, virtual or cloud, configuration information about the servers or workstation themselves including the software installed on these servers or workstations and the environment in which the software is installed. Asset Discovery also provides for discovery of the virtual environment of physical virtualization products (like VMware or Hyper-V) as well as the ability to run audit reports in support of Oracle LMS measurement scripts.

**CI Management** provides for importing 20 nodes (and their related CIs) or the import of 1,000 CIs and relationships of non-IT information, for every instance of the CI Management license.

**Data Flow Probes** provides for connections to additional deployments of DFP servers beyond the standard 1 DFP per 1,000 licenses.

**UCMDB** provides the ability to store data that has been discovered using Universal Discovery or imported from external sources into a database that allows for managing and querying the data in the manner required by the customer and then replicated to external sources.

**Boundaries and Exclusions**

Usage of Universal Discovery and CMDB SaaS shall be governed by the following boundaries and exclusions:

- Discovery of OSI is limited to the number of purchased subscriptions
    - If all available Asset Discovery licenses have been consumed but there are available Premium discovery licenses, discovery will consume Premium licenses until such time as they are all consumed
    - No new discovery will occur for any nodes beyond the purchased subscriptions
    - Nodes discovered with the purchased subscriptions will continue to be discovered, even if the maximum discovery count has been reached
- Discovery or import of CIs is limited to an average of 1,000 CIs and relationships per Premium or Asset Discovery license (evaluated as a whole over all licenses purchased)
- Data Creation, Import and Export
    - Discovered information imported to Universal Discovery and CMDB SaaS from an on-premise instance of Universal Discovery and CMDB is limited to 1,000 CIs and relationships in Universal Discovery and CMDB SaaS per on-premise discovery unit-based license.
    - Importing data into Universal Discovery and CMDB SaaS from another Micro Focus tool will consume the CI Management license at the rate of 1000 CIs and relationships per license.
    - Exporting nodes from UCMDB to any other system will incur no additional charge
    - Node data created or updated in SMAX, AMX or HCMX that is replicated to UCMDB via the Micro Focus standard integration (“Native SACM”) will incur no additional charge.
    - Full export of Universal Discovery data to a 3rd party tool must not occur more often than one (1) time per week.
    - Incremental export (changes only) of Universal Discovery data to a 3rd party tool must not occur more often than one (1) time per hour.
- Discovery of network and storage devices does not consume any license as long as the number of discovered devices is not greater than the number of Premium and Asset licenses to which the customer is entitled
- Universal Discovery probes must be hosted on-premise or in the customer public cloud account (in context of the customer)
- Universal Discovery probes must be current or within one version of the current minor UCMDB version
- One Universal Discovery probe or REST API connection (for writing data) is allowed per 1,000 Universal Discovery licenses in production unless additional DFP connections have been purchased separately
- One Universal Discovery probe or REST API connection (for writing data) is allowed per 3,000 Universal Discovery licenses in non-production (i.e., dev or QA), with a maximum of 3 probes total unless additional DFP connections have been purchased separately
- Total CIs and relationships in Customer non-production instances cannot exceed a quarter of the total Premium and Asset Discovery licenses purchased

- Updates to CIs in UCMDB via discovery or integration must not occur more often than 30 CIs per second

## UCMDB Usage Limits

Access to key components of UCMDB is restricted, as detailed below, to ensure access to data is limited only to those authorized, and to prevent any system stability issues.

| Capability | Description |
|---|---|
| Access to JMX | New self-service JMX methods are exposed with each version release though most JMX methods should be placed via a support ticket |
| Direct database access | Not allowed |
| Webservice API access | Not allowed |
| Java SDK API access | Not allowed |
| REST API access | Universal CMDB public REST API functionality is allowed |

## Service Support

Customer may contact Micro Focus through submitting online support tickets through Service Operations Center portal. The Micro Focus Support Team will either provide support to Customer directly or coordinate delivery of this support. Details on accessing the Service Operations Center portal will be provided as part of customer onboarding to ITMX.

As part of the onboarding process, it is Customers' responsibility to provide details of users that require access to the Service Operations Center portal. These initial users will have an account created and can manage access for themselves and others to the Service Operations Center portal.

- Micro Focus staffs and maintains a Service Operations Center, which will be the single point of contact for all issues related to the support for the ITMX service for the Customer. 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 Service Operations Center portal.
- All support is provided remotely by United States citizens.

SMAX includes an extensive online contextual help to aid with configuration of SMAX to align with your business requirements and is accessible from within your SMAX tenant.

As part of the Micro Focus SMAX community you can get additional assistance and aid from peers as well as live and recorded webinars as part of our Community user groups: https://community.microfocus.com/t5/SMAX-Suite/ct-p/ITSMA_Suite

Your suggestions for enhancements to our products are important to Micro Focus and as part of the community, Micro Focus allows you to review existing and submit new ideas or enhancements via the Idea Exchange. We encourage you to share, vote and enhance existing ideas with your feedback and comments to help Micro Focus product development. The popularity of an idea is measured through votes and comments at:

- SMAX - https://community.microfocus.com/it_ops_mgt/itsma_suite/
- Universal Discovery and CMDB - https://community.microfocus.com/it_ops_mgt/ucmdb/i/cms_idea

| Activity | SMAX Premium SaaS |
|---|---|
| **Customer Success Management** | ✔ |
| **Email and Online Notifications** | ✔ |
| **Customer On-boarding to ITMX**<br>Introduction meeting, handover of product and support materials, verification of online access, scope validation and service goals | ✔ |
| **Version Updates**<br>Major version updates | ✔[1] |
| **Service Reviews**<br>Meeting reviewing service quality, and to provide feedback on improvements required | Yearly |
| **Assisting with the implementation / configuration and tailoring** | Available at additional cost |
| **Availability SLA** | 99.9% |

[1] *Notifications regarding release updates to SMAX Premium SaaS will include details of any associated release readiness webinar, and online documentation which will detail the updates and new features in the planned release.*

### 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.

### Capacity and Performance Management

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

**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**
The following types of SaaS Data reside in the SaaS environment:

- **Supporting Data:** This is data loaded by a customer to support the transactional records. Examples of this could include, but not limited to Organization Locations, personnel, departmental data, assets, and services delivered.

- **Transactional Data:** This is data that is related to the day-to-day delivery of service operations and support within the organization. Examples of this could include but are not limited to service and support requests, incidents, and change records. Note, transactional data is typically linked to one or more supporting data records.
- **Attachment Data:** This refers to any type of file that has been attached to either supporting data or transaction data. For example, this could be but not limited to an image file an employee uploads for his profile picture on his personal record, a log file attached to an incident to assist with resolution, or a pdf troubleshooting guide attached to a knowledge article.
- **Configuration Data:** This is any alterations made to the configuration of the SMAX Premium Tenant from an Out of the Box (OOTB) SMAX Tenant. Examples of this could include but not limited to adding a custom field on record entity, modifying the workflow, making a field mandatory. Full documentation of the configuration alterations that can be made are documented in the online contextual help.

Micro Focus does not add any specific customer related data into the SMAX tenants provided to a customer as part of the SMAX Service, and any data highlighted above is done so by the customer.

**Backups**

Micro Focus performs a backup of SaaS Data every 6 hours with a 24-hour recovery point objective (RPO). Micro Focus retains each backup for the most recent seven (7) days. The backup data is replicated to a protected vault within the same AWS Region as the Customer's running service. The backup includes a snapshot of production database, including transactional database and analytics database, a copy of files stored on persistent volume and an export of all the Kubernetes objects.

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.

### 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.

## SaaS Security

Micro Focus maintains an information and physical security program designed to protect the confidentiality, availability, and integrity of SaaS Data. ITMX for United States Public Sector SaaS environment meets all security requirements for certification as a FedRAMP moderate level SaaS solution.

**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'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 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'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.

The Joint Authorization Board (JAB) of the Federal Risk and Authorization Management Program (FedRAMP) has completed the review of ITMX United States Public Sector. Based on the Federal Information Processing Standard (FIPS) security categorization of "Moderate" (Confidentiality=Moderate, Integrity=Moderate, Availability=Low) and the FedRAMP Security Assessment Process, the JAB determined the Micro Focus USPS system meets the information security requirements and has been granted a FedRAMP Provisional Authorization (P-ATO).

The JAB provides guidance for ITMX to assist in determining the scope of an annual assessment based on NIST SP800-53, FedRAMP baseline security requirements, and FedRAMP continuous monitoring requirements. The security authorization will remain in effect for a length of time in alignment with Office of Management and Budget Circular A-130, as long as:

- ITMX United States Public Sector satisfies the requirement of implementing continuous monitoring activities as documented in FedRAMP's continuous monitoring requirements
- ITMX United States Public Sector mitigates all open low and moderate POA&M action items, agreed to in the Security Assessment Report (SAR)
- Significant changes or critical vulnerabilities are identified and managed in accordance with applicable Federal law, guidelines, and policies
- For additional information, visit fedramp.gov

## 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.

## 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.

Micro Focus employees, affiliates and subcontractors involved in the processing of SaaS Data meet all US citizenship requirements specified by FedRAMP program rules, are bound by appropriate confidentiality obligations, and have undergone all training required to meet FedRAMP moderate level controls.

## 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 one (1) monthly four (4) hour window (Saturday 00:00 to Sunday 00:00 US Eastern Time Zone). 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. SaaS Upgrades are evaluated in accordance with the rules of the FedRAMP program prior to release.

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

### Universal Discovery Infrastructure Updates

Universal Discovery Infrastructure Data Flow Probe ("Data Flow Probe" or "DFP") directly communicates to the Universal Discovery and CMDB SaaS tenant to which Customer is assigned. The DFP version must be compatible with the Universal Discovery and CMDB SaaS version, and Customer is responsible to update DFP as part of the update of SMAX SaaS version update. DFP updates may be done by Customer at any time and do not require advance notice with Micro Focus.

If Customer does not apply a DFP update, the DFP will lose its ability for automated updates, and Customer will be required to manually update each DFP under this condition to restore discovery functionality.

### Universal Discovery Content Updates

As part of the scheduled version update process, Customer who purchased the optional Asset Discovery or Premium Discovery capabilities for SMAX SaaS will have the option to update their Universal Discovery Content to the latest version once the SMAX SaaS version update has been completed. The latest Universal Discovery Content Pack will be available from within the CMS UI for each Customer to choose to deploy on their own schedule.

Updates to Universal Discovery content is the responsibility of Customer. Content versions are generally not tied to Universal Discovery and CMDB SaaS versions in that content updates can be deployed at Customer's discretion on whatever version of Universal Discovery and CMDB SaaS that is currently in use. Universal Discovery content updates are accumulative in nature, meaning deploying a content pack for a given release will include all improvements included in previous content releases.

## 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.

## 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.

### Solution Provisioning Time SLO

Solution Provisioning is defined as the SMAX solution being available for access over the internet. Micro Focus targets to make SMAX available within two (2) business days of the customer's Order 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 of the solution are not in scope of the Solution Provisioning Time SLO.
Additionally, the import of Customer data into the application is not in scope of the Solution Provisioning Time SLO.

## SaaS Availability SLA

SaaS availability is the SMAX 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
- 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 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 Service Operations Center Portal being available for access and use by Customer over the Internet. Micro Focus targets to provide Customer access to the Service Operations Center 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.

### 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<br>• Owns the business relationship with the range of departments and organizations using SaaS |

| | |
|---|---|
| | • Manages contract issues |
| **Project Manager** | • Coordinates customer resources as necessary<br>• Serves as the point of contact between the customer and Micro Focus<br>• Drives communication from the customer side<br>• 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<br>• Performs SaaS administration<br>• Provides tier-1 support and works with Micro Focus to provide tier-2 support<br>• Coordinates end-user testing as required<br>• Leads ongoing solution validation<br>• Trains the end-user community<br>• Coordinates infrastructure-related activities at the customer site<br>• Owns any customization |
| **Subject Matter Expert** | • Leverages the product functionality designed by Customer's SaaS administrators.<br>• 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<br>• Provides 24x7 application support |
| **Operations Staff (Ops)** | • Monitors the Micro Focus systems and SaaS for availability<br>• Performs system-related tasks such as backups, archiving, and restoring instances according to Micro Focus's standard practices<br>• 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 support 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.