Service Description

OpenText™ Core Automation Center

July 2025

opentext™

Contents

This Service Description document describes the components and services included in
OpenText™ Core Automation Center (known as "Automation Center") 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 Automation Center ("Automation Center") is a native cloud application that helps IT operations, development operations, and site reality engineers to automate end-to-end IT processes. The codeless and customizable interface of Automation Center, powered with workflow orchestration, vulnerability remediation, service designer, simplified catalog, and a smart service portal, provides for the complete automation of IT processes, infrastructure, application services, and hybrid cloud environments. Micro Focus oversees the deployment, infrastructure, operation, availability, security and data protection, and service support.

SaaS Delivery Components

SaaS Delivery Components	Included
One Automation Center production tenant	✓
One Automation Center non-production tenant	O
Additional Automation Center non-production tenant	O
Premium Discovery of a server OSI including dependencies	O
Additional Data Flow Probe Connection	O
✓ = Included	
O = Optional for an additional fee	

SaaS Operational Services

SaaS Operational Services	Included
Onboarding	✓
Customer Management (CM) Meetings	✓
Product Support	✓
Single sign-on support*	✓
Service Health portal	✓
✓ = Included	

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

Automation Center Licensing Model

Access to Automation Center is by Automation Center Units ("AC Units"). AC Units can cover the following use cases based on a specific ratio:

Use Case	AC Units
1 Node of	
Generic Process Automation and Orchestration (OO)	1
Vulnerability and Remediation Management, Server patching, provisioning, configuration, audit and compliance capabilities (SA)	2
Cloud Management	2
1 Concurrent Workflow of	
Generic Process Automation and Orchestration (OO)	70

*AC Units are stackable; they can be purchased for multiple use cases for the same node.

Generic Process Automation and Orchestration (OO)

Automate and orchestrate any IT process, whether in the cloud or on-premises, with the flexibility to choose between low-code/no-code workflows or Infrastructure-as-Code (IaC). Through the API-rich platform, users can seamlessly integrate with various systems, centrally managing scalable workflows. This enables automation across infrastructure, service fulfillment, incident remediation, cloud service delivery, disaster recovery and many other use cases.

Vulnerability and Remediation Management, Server Patching, Provisioning, Configuration, Audit and Compliance Capabilities (SA)

Manage vulnerabilities hybrid environments by assessing risks, prioritizing patches, and resolving critical issues based on customized best practices. Users can streamline operations by syncing server environments from Server Automation, importing vulnerability data from third-party scanners like Qualys, and creating tailored policies for vulnerability and patch management. This allows for remediation through SA agents or through agentless orchestration.

Maintain patch compliance by creating and enforcing policies to automatically install and manage patches for supported operating systems on managed servers in your IT environment. Install (or provision) pre-configured operating system baselines onto bare metal and virtual servers. Enables centralized management of the configuration files by modeling the format in a consistent way and ensure compliance by tracking the changes made on server configuration. Automate regulatory and internal IT compliance risk across server OS using customization and remediation capabilities.

Cloud Management

Cloud Management provides a unified experience for managing the requesting, provisioning, and consumption of IT services. It delivers multi-cloud infrastructure and IT services to business users, defines the service life cycle management to provision, update, and de-provision cloud resources, and manages hybrid and multi-cloud SaaS environments.

Node:
Means any infrastructure component, physical or virtual (server, network, storage, desktop, low end Device) that derives value from Automation Center.
One Node equals:
1 Operating System Instance or Storage Device, or
2 Network devices or Containers, or
8 Edge devices

Concurrent Workflow:
Means the number of orchestration workflows that can be run at the same time, concurrently.
This model can be used against multiple Devices. One Concurrent Workflow includes up to five (5) parallel threads.

Automation Center includes the following capabilities:

- Service portal
- Service design
- Service catalog management
- Vulnerability and Remediation
- Operations Orchestration
- Server Automation (on-premise)
- Cost governance and resource optimization
- Knowledge
- Universal CMDB Foundation
- Service Asset and Configuration Management
- Studio – only to manage the out-of-the-box provided workflows and entities and create Automation Center-related studio apps for automation use case only
- Financial Management

Automation Center includes the following in addition:

- Entitlement for 3 SMAX Express users
- 50 Non-Production Core Universal Discovery and CMDB Premium Discovery

Architecture Components

Micro Focus deploys Automation Center, Core Universal Discovery and CMDB, and Operations Orchestration using a shared infrastructure platform. The shared platform is monitored for 24x7 availability, and Micro Focus provides related 24x7 infrastructure support, including application version upgrades.

As part of the Automation Center tenant, a Core Universal Discovery and CMDB tenant and an Operations Orchestration tenant is deployed and available for use as part of the subscription from the Automation Center tenant. Customer access to Automation Center is through the Internet over HTTPS.

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

- Premium Discovery – includes usage of the Core Universal Discovery module of the Universal Discovery and CMDB solution to discover operating system instances (OSI) of servers (physical, virtual, cloud, container) or workstations in support of Automation Center. This includes discovering the software installed and running on these servers or workstations, the configuration of this software and the

dependencies that exist between software and servers. Also included is discovery of cloud servers and services.

Automation Center provides on-premise components used as communication infrastructure for execution of remote operations, to collect data and forward it to the SaaS instance, and optional tools and scripts:

- Operations Orchestration Remote Action Server ("OO RAS") is a component required for execution of remote operations inside a customer's firewall or other locations (remote data centers, networks, private or public cloud)
- Operations Orchestration Workflow Designer is an optional component to develop orchestration workflows. In order to develop Operations Orchestration Workflows and use them in Automation Center, Customer must install and configure a compatible version of Operations Orchestration Workflow Designer.
- Server Automation is an optional component that is used for agent-based remediation in the Vulnerability and Remediation Management use case as well as for the Patching and Compliance Management use cases

Customer may choose to integrate a compatible version of on-premise Operations Orchestration or Server Automation, licensed separately by Customer, with Automation Center.

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

Micro Focus does not operate third-party integrations on behalf of the Customer and will not commit to any SLO for these components.

Server Automation

Usage of agent-based remediation on Automation Center is accomplished through Server Automation.

Customers are responsible for installing, configuring, deploying, and updating any optional Server Automation components in their own environments.

Usage between both Server Automation and Automation Center should not exceed the license entitlement.

Entitled to use other basic features such as global shell or scripts execution. Security and Compliance Content is charged separately.

Core Universal Discovery and CMDB

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

Customers who purchased the optional Asset Discovery or Premium Discovery capabilities for Automation Center, 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, cloud or container.

Capabilities also include discovering installed and running software, mapping the inter-dependencies between servers and their software, and the dependencies between services and servers.

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, cloud or container, 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.

Import of data into UCMDB that enriches servers discovered by Universal Discovery is available at no charge (as the server has already consumed a Premium Discovery or Asset Discovery license). However, import of data into UCMDB without prior discovery consumes 1 CI Management license for every 20 nodes (and their related CIs). Import of discovered content from an on-premise UCMDB instance is no charge. Export of data from UCMDB to any other system is no charge.

Boundaries and Exclusions
Usage of Core Universal Discovery and CMDB 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 of related CIs for servers is limited to an average of 500 related CIs (plus 500 relationships) per discovered OSI and is evaluated over the total discovered base
- A node imported into UCMDB will incur no additional charge if it has already been discovered and consumed an Asset or Premium discovery license
- 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 UCMDB version
- You are entitled to connect one Data Flow Probe (DFP) or REST API connection (for writing data) to Universal CMDB for every 1,000 Universal Discovery licenses you have in production.
  - These DFP connections may be spread across your production and non-production SaaS instances so long as the total number of DFPs connected to all your SaaS instances does not exceed your overall entitlement of DFP connections.
  - If you have insufficient DFP connections in your entitlement to provide at least one connection to one non-production instance, you may have one additional DFP connection for one non-production instance at 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

Operations Orchestration SaaS

Generic Process Automation and Orchestration, along with the agentless fulfillment for Cloud Management and Vulnerability and Remediation Management on Automation Center, are achieved through Operations Orchestration.

Operations Orchestration capabilities are different from the on-premise Operations Orchestration product and can be found in the online ESM documentation: https://docs.microfocus.com/itom/ESM:SaaS/Home

Boundaries and Exclusions

Usage of Operations Orchestration shall be governed by the following boundaries and exclusions:

- Transactional data retention period can be up-to 1 year with Micro Focus reserving the right to control the size of Operations Orchestration data store with purging procedures. In the event this happens earlier than 1-year, customers will receive proper notifications.
- Micro Focus is not accountable of the custom flow logic created by the customer, or by the impact this logic is having on the other work in his environment
- Micro Focus is not accountable of the usage of the Internal RAS (SaaS RAS) to perform any sort of malicious activities against any kind of software services
- As workflows can vary in complexity, there is no guarantee of constant time of completion on each workflow execution. Internal Operation Orchestration workers are limited on the operations that can be executed inside Micro Focus SaaS and will not have access to write or read from the Micro Focus SaaS filesystem. These limitations can be avoided by installing an on-premise RAS (Remote Action Service).

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 Customer directly or coordinate delivery of this support.

Online support is available from the support portal (PCS): https://pcs.saas.microfocus.com

As part of the onboarding process, it is Customers' responsibility to provide details of users that require access to the support portal (PCS). These initial users will have an account created and can manage access for themselves and others to the support portal for Customer's Automation Center.

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.

Automation Center includes an extensive online contextual help to aid with configuration of Automation Center to align with your business requirements. Full documentation of the capabilities of the Enterprise Service Management SaaS solution which includes Automation Center, and the optional capabilities outlined in this service description is available at: https://docs.microfocus.com/itom/ESM:SaaS/Home

Activity	
Customer Management	✓
Email and Online Notifications	✓
On-boarding Introduction meeting, handover of product and support materials, verification of online access, scope validation and service goals	✓
Version Updates Major version updates	✓[1]
Service Reviews 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 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.

Details can be found on the relevant Service Health portal for your service which includes:

- Current availability of the Automation Center environment that their tenants are part of
- Details of any upcoming planned maintenance
- Outage reports for any incidents that have been identified by our support teams
- Historical SLO data.

The Link to Service Health portal for your service will be provided as part of your onboarding to Micro Focus SaaS and are also available via the support portal: https://pcs.saas.microfocus.com

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

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 related to the day-to-day delivery of service operations and support within the organization. Examples of this could include but 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 person 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 Automation Center Tenant from an Out of the box (OOTB) Automation Center 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 available at: https://docs.microfocus.com/itom/ESM:SaaS/Home

Micro Focus does not add any SaaS Data into the Automation Center tenants provided to Customer as part of the Automation Center offering, and any data highlighted above is done so by Customer.

Backups
Automation Center is implemented over AWS technology service stack in a redundant mode over multiple Availability zones (AZs) with elastic load balancing allowing us to quickly recover service in case of a disaster. Availability zones (AZs) are distinct geographical locations that are engineered to be insulated from failures in other AZs.

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.

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

SaaS Security

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

Technical and Organizational Measures

Micro Focus regularly tests and monitors the effectiveness of its controls and procedures. No security measures 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.
Customer initiated security testing is not permitted, which includes application penetration testing, vulnerability scanning, application code testing or any other attempt to breach the security or authentication measures of the SaaS.

Security Incident Response

In the event Micro Focus confirms a security incident resulted in the loss, unauthorized disclosure or alteration of SaaS Data ("Security Incident"), Micro Focus will notify Customer of the Security Incident and work to reasonably mitigate the impact of such Security Incident. Should Customer believe that there has been unauthorized use of Customer's account, credentials, or passwords, Customer must immediately notify Micro Focus Security Operations Center via SED@opentext.com.

Micro Focus Employees and Subcontractors

Micro Focus requires that all employees involved in the processing of SaaS Data are authorized personnel with a need to access the SaaS Data, are bound by appropriate confidentiality obligations and have undergone appropriate training in the protection of 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.

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 (Scheduled to occur on Sunday in the 00:00 to 23:00 Greenwich Mean Time, the exact 4-hour time block is dependent on the location of the Automation Center farm location). 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 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 Core Universal Discovery and CMDB tenant to which Customer is assigned. The DFP version must be compatible with the Core Universal Discovery and CMDB version, and Customer is responsible to update DFP within six (6) months from the Core Universal Discovery and CMDB update as part of the update of Automation Center 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 within six (6) months of a Core Universal Discovery and CMDB version update, Customer's Data flow Probes will no longer function and will only be available for automated updates to the latest DFP version to restore discovery functionality.

If Customer does not apply a DFP update within twelve (12) months of a Core Universal Discovery and CMDB version 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 Automation Center will have the option to update their Universal Discovery Content to the latest version once the Automation Center 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 Core Universal Discovery and CMDB versions in that content updates can be deployed at Customer's discretion on whatever version of Core Universal Discovery and CMDB 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.

Operations Orchestration RAS and Workflow Designer Updates

Operations Orchestration offers the option for Customer to connect RAS (Remote Action Servers) that can process work on Customer's environment to the Operations Orchestration tenant provided with Automation Center. It is the Customer responsibility to install and maintain any RAS in their own environment and to apply updates in a timely manner to keep the RAS version synchronized with the version of Operations Orchestration.

To create and update orchestration workflows, Operations Orchestration requires the use of the Operations Orchestration Workflow Designer component ("Workflow Designer"). It is the Customer responsibility to install and maintain the Workflow Designer in their own environment and to apply updates in a timely manner to keep the Workflow Designer version synchronized with the version of Operations Orchestration.

Operations Orchestration Content Updates

Updates to orchestration content is the responsibility of Customer. The latest Operations Orchestration Content Pack will be available on the Micro Focus ITOM Marketplace for each Customer to choose to deploy on their own schedule. Content versions are generally not tied to Operations Orchestration

versions in that content updates can be deployed at Customer's discretion on whatever version of Operations Orchestration that is currently in use. Content updates are accumulative in nature, meaning deploying a content pack for a given release will include all improvements included in previous content releases.

Server Automation Updates

Automation Center offers the option for Customer to integrate with Server Automation components that can process work on Customer's environment to the Automation Center. It is the Customer responsibility to install, configure, deploy, and maintain any Server Automation components in their own environment and to apply updates in a timely manner to keep the Service Automation version compatible with the version of Automation Center.

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.

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

Solution Provisioning Time SLO

Solution Provisioning is defined as the SaaS offering being available for access over the internet. Micro Focus targets to make the SaaS offering 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 Provisioning Time SLO.

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

Online Support Availability SLO

Online Support Availability is defined as the SaaS support portal https://pcs.saas.microfocus.com 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://pcs.saas.microfocus.com.

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.

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://pcs.saas.microfocus.com

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. **Credit.** 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.

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.