
Service Description

Service Description

OpenText Core Cloud Network Observability

October 2024

opentext™

Copyright 2024 Open Text

Contents

Contents	2
Standard Service Features.....	3
Data Backup and Retention	6
SaaS Security	7
Audit	9
Micro Focus Security Policies	9
Security Incident Response	9
Micro Focus Employees and Subcontractors	9
Data Subject Requests	10
Scheduled Maintenance.....	10
Service Decommissioning.....	10
Service Level Objectives	11
Standard Service Requirements.....	14

This Service Description document describes the components and services included in OpenText Core Cloud Network Observability (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

OpenText Core Cloud Network Observability (“**Cloud Network Observability**” or “**CNO**”) is a native cloud application that helps you manage your Cloud Networks. It will enable users to observe the public cloud networks in an easy-to-understand representation and provide end-to-end network visibility and observability from the multi-cloud to the data center networks.

SaaS Service Delivery Components

SaaS Delivery Components	Included
One Cloud Network Observability production tenant	✓
One Cloud Network Observability non-production tenant (up to 250 CNO Units)	✓
Performance data processing and storage as per defined CNO data retention	✓
Data extraction (egress) from CNO to support up to 10 concurrent users	✓
License Consumption Report	✓
Extension of CNO data retention	○
Reduction of polling frequency for performance data	○
Additional data extraction (egress) from Cloud Network Observability	○

✓ = Included
○ = Optional for an additional fee

SaaS Operational Services

SaaS Operational Services	Included
Onboarding: CSM led kick-off meeting	✓
Customer Success Management (CSM) Meetings	✓
Product Support	✓
Service Health portal	✓

✓ = Included
○ = Optional for an additional fee

Full documentation of the capabilities of OpenText Core Cloud Network Observability is available at:
<https://docs.microfocus.com/doc/cno/SaaS/Home>

CNO Data Retention

CNO monitoring, Network Test results, and Cloud Flow data are stored for reporting, dashboarding, and troubleshooting. The default CNO data retention for Cloud Network Observability is as follows:

- Performance data and Network Test results

Aggregation Period	Retention Period
Raw data (5-minute interval, 5-minute sample)	14 days
Hourly aggregation	70 Days
Daily aggregation	800 Days

- Cloud Flow data

Aggregation Period	Retention Period
Raw data (aggregated at 5-minute)	3 days
Hourly aggregation	30 Days
Note: No Daily aggregation for cloud flow data	

CNO Unit

Cloud Network Observability is licensed by CNO Units. Each CNO Unit can be used for one of the following:

- Discovery and essential monitoring for 1 managed cloud element, like Firewalls, Load Balancers, and Gateways
- Discovery of 10 endpoints like EC2 instances or Cloud Services like Postgres
- 1,500 cloud flow records/ minute or 500 unique cloud flow records/ minute, whichever is higher
- 200,000 Network Test runs/ month

Discovery and connectivity of Connection/ Attachment, Routing Table, VPC, Subnets, Availability zones, and Regions will not consume CNO Units.

CNO Units consumption can be found using the License Consumption Report.

Architecture Components

Cloud Network Observability infrastructure consists of:

- Cloud Network Observability platform which is a cloud native and delivers
 - Discovery of cloud elements, their relationship, and collection of performance data
 - Collection of test results of Synthetic tests running in the managed environment
 - Collection of cloud flow from various points in the managed cloud environment
 - A reporting engine to provide reporting and troubleshooting capabilities
 - A topology map to represent the relationship between elements with data overlays
 - A web portal accessible by customer through the Internet (HTTPS), using a supported web browser and the URL provided to them
- Network Edge Observer (which also may be referred to as “NEO”), a component to support Synthetic Test capability, deployed in Customer network. NEO runs the synthetic network tests, collects the data, and forwards data to Cloud Network Observability for processing.
- Customer needs to deploy and maintain a compatible version of Network Edge Observer (NEO) in the monitored environment.
- Full documentation for integrating Network Edge Observer (NEO) instance with the Cloud Network Observability is available at: <https://docs.microfocus.com/doc/cno/SaaS/Home>

Micro Focus does not install, deploy, or manage NEO in Customer’s environment. Customer is responsible for installing, configuring, deploying, updating, and paying any additional fees (if required) for any components in the monitored environment.

Application Administration

Customer accesses Cloud Network Observability using a supported web browser, and the URL provided to them. Micro Focus SaaS Operations team will create the admin user which can be used to create necessary roles, groups, and users by Customer to access Cloud Network Observability.

Users with administrative rights will be able to access select administration pages to configure the Cloud Network Observability capabilities and integrate data sources into Cloud Network Observability. Micro Focus reserves the right to determine which administrative features will be made available in the Cloud Network Observability instance.

Customers should open a ticket with the Micro Focus SaaS Operations team to execute tasks such as, but not limited to, unlocking user accounts, etc.

Service Support

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

Support for Cloud Network Observability is available at: <https://pcs.saas.microfocus.com>

Cloud Network Observability includes extensive online help to aid with tailoring and configuration of Cloud Network Observability to align with your business requirements. Full documentation of the capabilities of Cloud Network Observability is available at: <https://docs.microfocus.com/doc/cno/SaaS/Home>

As part of the OpenText Network Operations Management community, you can get additional assistance and aid from your peers as well as get access to live and recorded webinars (practitioner forum series) at https://community.microfocus.com/it_ops_mgt/nom/

Your suggestions for enhancements to Cloud Network Observability are important to us. We encourage you to share your ideas, vote for your favorite ones, and enhance existing ideas with your feedback and comments. The popularity of an idea is measured through votes and comments at: https://community.microfocus.com/it_ops_mgt/nom/nom-customers-only/i/ideas

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 Cloud Network Observability. Customer will maintain a list of authorized users who may contact Micro Focus for support. Customer's authorized users may contact Micro Focus for support via the Web portal 24 hours a day, 7 days a week.

Activity

Customer Success Management	✓
Email and Online Notifications	✓
On-boarding: Kick-off meeting	✓
Version Updates: Major version updates, minor version updates, patches, and security fixes. Notification period according to notification timelines via release notes and help resources available	✓ ¹
Assisting with the implementation/ configuration and tailoring	Available at additional cost

Availability SLA	99.9%
-------------------------	-------

¹Notifications regarding release updates to Cloud Network Observability will be provided via email.

Service Monitoring

Micro Focus monitors the availability of Cloud Network Observability 24x7. Micro Focus uses a centralized notification system to deliver proactive communications about application changes, outages, and scheduled maintenance.

As part of the Cloud Network Observability offering, we also include a Service Health portal for the SaaS-deployed components which allows the Customer to see:

- Current availability of the Cloud Network Observability environment
- 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 the Service Health portal for your tenant will be provided as part of your onboarding to Micro Focus SaaS.

Capacity and Performance Management

The architecture used by Cloud Network Observability allows for the addition of capacity to the applications, databases, and storage as required to support the services provided, and additional fees may apply.

Operational Change Management

Micro Focus follows a set of standardized methodologies and procedures for efficient and prompt handling of changes to SaaS infrastructure and applications, which enables beneficial changes to be made with minimal disruption to the service.

Data Backup and Retention

The data backup and retention described in this section are part of Micro Focus's overall business continuity management practices designed to attempt to recover availability to the Customer of Cloud Network Observability and access to the Cloud Network Observability Customer data, following an outage or similar loss of service.

The following types of Customer-specific data reside in the Micro Focus SaaS environment:

- Customer-authorized user details (for instance, customer administrator users, operator users)
- Configuration information that may include credentials necessary for integrations with service management tools, customer-provided business intelligence tools, or customer premise components like NEO.
- Cloud Service Credentials
- Resulting information collected during product feature use such as network performance metrics and cloud flow data
- Reports, dashboards, and reporting data
- Audit logs

The Customer will work with Micro Focus SaaS support for user creation and integration configurations.

The Data Backup Frequency is daily and Micro Focus will perform a necessary daily backup of the database and related storage systems (including configuration data) for the Cloud Network Observability instance. The Backup Retention Time is seven (7) days, meaning Micro Focus retains each daily backup for the most recent seven (7) days (“Data Retention Time”).

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. Micro Focus will be unable to restore any data not included in the database (for example not properly entered by the user, lost, or corrupted, etc.) at the time of backup or if the customer’s request comes after the Data Retention Time of such backup. As such, Micro Focus cannot guarantee no data loss.

Disaster Recovery

Business Continuity Plan

Micro Focus SaaS continuously evaluates different risks that might affect the integrity and availability of Cloud Network Observability. As part of this continuous evaluation, Micro Focus SaaS 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 Micro Focus SaaS and infrastructure services with minimum disruption. The DRP includes a set of processes that Micro Focus SaaS implements and tests Micro Focus SaaS recovery capabilities to reduce the probability of a continuous service interruption in the event of a service disruption.

Cloud Network Observability 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 Cloud Network Observability within 24 hours (Recovery Time Objective, RTO) following Micro Focus’s declaration of a disaster.

The Vertica database backend used by Cloud Network Observability is deployed in a single availability zone. If the availability zone hosting Vertica goes down, the DRP’s target is to provide restoration of Cloud Network Observability within 24 hours (Recovery Time Objective, RTO) following Micro Focus’s declaration of a disaster.

Backups

Micro Focus SaaS performs backups of CNO databases and application configurations with a six (6) hours recovery point objective (RPO). Backups are performed using cloud-based technology across multiple regions. The integrity of backups is validated by (1) real-time monitoring of the storage snapshot process for system errors, and (2) an annual restoration of production data from an alternate site to validate both data and restore flow integrity.

SaaS Security

Micro Focus maintains an information and physical security program designed to protect the confidentiality, availability, and integrity of Customer Personal Data and confidential information (the “Micro Focus Security Program”).

Technical and Organizational Measures

This section describes Micro Focus’s standard technical and organizational measures, controls, and procedures, which are intended to help protect SaaS Data.

Micro Focus regularly tests and monitors the effectiveness of its controls and procedures. The measures set forth in this section may be modified by Micro Focus but represent a minimum standard. A customer remains responsible for determining the sufficiency of these measures. Some of the security settings in the service are configurable by the customer, to allow for better integration. As a rule of thumb, Micro Focus will deliver its service with the most secure options and capabilities enabled.

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 the perimeter
- Micro Focus employees, subcontractors, and authorized visitors are issued identification cards that must be worn while on the 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 guidelines
- 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 secure manner
- Administrator accounts are only used to perform administrative activities
- Each account with administrative privileges is traceable to a uniquely identifiable individual
- All access to computers and servers is authenticated and within the scope of an employee's job function
- Collection of information log information may link users to actions in the Micro Focus SaaS environment
- Collection and maintenance of log audits
- Access to log information is restricted based on user roles and the "need-to-know"
- Using shared accounts is prohibited

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.

Data Segregation

Micro Focus SaaS environments are segregated logically by Micro Focus SaaS access control mechanisms. Internet-facing devices are configured with a set of access control lists (ACLs), which are designed to prevent

unauthorized access to internal networks. Micro Focus uses security solutions on the perimeter level such as: firewalls, IPS/IDS, proxies, and content-based inspection to detect hostile activity in addition to monitoring the environment's health and availability.

Data Encryption

Micro Focus SaaS uses industry standard techniques to encrypt SaaS data in transit. 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 Cloud Network Observability. A summary report or similar documentation will be provided to the customer upon request. Subject to the 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 Micro Focus SaaS provided pursuant to the applicable Supporting Material 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 up-to-date certificate can be viewed at the following link:

<https://www.microfocus.com/media/documentation/certificate-of-registration-information-security-management-system-documentation.pdf>

Security Incident Response

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

Micro Focus Employees and Subcontractors

Micro Focus requests that all employees involved in the processing of SaaS Data are authorized personnel with a need to access the SaaS Data, are bound by appropriate confidentiality obligations, and have undergone appropriate training in the protection of Customer data. Micro Focus requests that any affiliate or third-party subcontractor involved in processing SaaS Data enters into a written agreement with Micro Focus, which includes confidentiality obligations substantially similar to those contained herein and appropriate to the nature of the processing involved.

Data Subject Requests

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

Scheduled Maintenance

To enable Customers to plan for scheduled maintenance by Micro Focus, Micro Focus reserves predefined timeframes to be used on an as-needed basis. Micro Focus reserves a weekly two (2) hour window (Sunday 00:00 to 02:00 Pacific Standard Time) and one (1) monthly eight (8) hour window (Sunday in the 00:00 to 08:00 Pacific Standard Time). 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. In the rare event, where Micro Focus needs to make an emergency change requiring a downtime outside of those planned maintenance windows, the customer will be notified as soon as possible.

Scheduled Cloud Network Observability Version Updates

“SaaS Updates” are defined as both major version updates, minor version updates, and patches applied by Micro Focus to Customer’s Cloud Network Observability solution in production. These may or may not include new features or enhancements. A customer is entitled to SaaS Updates as part of the Cloud Network Observability services unless the SaaS Update 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 Update to the Customer’s Cloud Network Observability solution. Unless Micro Focus anticipates a service interruption due to a SaaS Update, Micro Focus may implement a SaaS Update at any time without notice to the customer. Micro Focus aims to use the Scheduled Maintenance windows defined herein to apply SaaS Updates. The customer may be required to cooperate in achieving a SaaS Update that Micro Focus determines in its discretion is critical for the availability, performance, or security of the Cloud Network Observability solution.

Customer-premise Component Updates

“Updates” are defined as both major version updates, minor version updates, and patches applied to the customer’s environment.

The initial installation of the minimum supported versions of the customer-premise component and ongoing upgrades are the sole responsibility of the customer.

Micro Focus will work with the customer to coordinate when updates must be applied to the customer-premise component.

Micro Focus will not be responsible for managing, monitoring, and the maintenance of the customer equipment or third-party computer hardware, software, or network infrastructure not within the sole control of Micro Focus.

Service Decommissioning

Upon expiration or termination of the SaaS Order Term, Micro Focus may disable all Customer access to Cloud Network Observability, and the customer shall promptly return to Micro Focus (or at Micro Focus’s request destroy) any Micro Focus Materials. The customer should also remove the customer-premise components like NEO-TP at such a time.

Micro Focus will make available to Customer OPTIC data lake data in the format generally provided by Micro Focus. The target timeframe is set forth below in the Termination Data Retrieval Period SLO. After such time,

Micro Focus shall have no obligation to maintain or provide any such data, which will be deleted in the ordinary course.

Service Level Objectives

Micro Focus provides clear, detailed, and specific Service Level Objectives (SLOs) for the services that SaaS provides to its customers. 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 always meet these objectives.

Micro Focus will provide self-service access to the customer to the Service Level Objectives data online at <https://home.software.microfocus.com/myaccount>.

Solution Provisioning Time SLO

Solution Provisioning is defined as the Cloud Network Observability solution being available for access over the Internet. Micro Focus targets to make Cloud Network Observability and its add-ons available within 1 week (7 days) of the Customer's Order being booked within the Micro Focus order management system.

The customer is responsible for installing and configuring customer premise components for their applications. Any customer premise components of the solution are not in scope of the Solution Provisioning Time SLO. Additionally, any third-party tool integration and the import of Customer data into the application are not in the scope of the Solution Provisioning Time SLO.

SaaS Availability SLA

SaaS availability is the SaaS production application being available for access and use by the 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 ($2,198 \text{ actual hours available} / 2,200 \text{ possible available hours} = 99.9 \text{ availability}$).

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's 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's service providers

Service Description
OpenText Cloud Core Network Observability

- 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 because Customer breached the SaaS Terms

Reporting

Micro Focus will provide self-service access to the customer to the availability data online.

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 the 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

- 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.
- Escalation.** Quarterly ASA below 98% shall be escalated by both parties to the Vice President (or equivalent).
- 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%

The 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 Micro Focus SaaS support portal being available for access and use by Customer and its Authorized Users over the Internet. Micro Focus targets to provide Customer access to the Micro Focus SaaS support portal on a twenty-four hour, seven days a week (24x7) basis at a rate of 99.9% (“Online Support Uptime”).

Measurement Method

Online Support Uptime shall be measured by Micro Focus using Micro Focus monitoring software running from a minimum of four global locations with staggered timing.

On a quarterly basis, Online Support Uptime will be measured using the measurable hours in the quarter (total time minus planned downtime, including maintenance, upgrades, etc.) as the denominator. The numerator is the denominator value minus the time of any outages in the quarter (duration of all outages combined) to give the percentage of available uptime (2,198 actual hours available / 2,200 possible available hours = 99.9 availability).

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

Boundaries and Exclusions

Online Support Uptime shall not apply to any of the following exceptions:

- Overall Internet congestion, slow down, or unavailability
- Unavailability of generic Internet services (e.g., DNS servers) due to virus or hacker attacks
- Unavailability of Amazon Web Services Availability Zones hosting to Customer
- Force majeure events as described in the terms of agreement
- Actions or inactions of Customer (unless undertaken at the express direction of Micro Focus) or third parties beyond the control of Micro Focus
- Unavailability due to Customer equipment or third-party computer hardware, software, or network infrastructure not within the sole control of Micro Focus
- Scheduled maintenance

Initial SaaS Response Time SLO

The Initial SaaS Response Time refers to the Service Support described herein. It is defined as the acknowledgment of the receipt of a customer request and the assignment of a case number for tracking purposes. The initial SaaS Response will come as an email to the requester and include the case number and links to track it using Micro Focus online customer portal. The Initial SaaS Response Time covers both service request and support requests. Micro Focus targets to provide the Initial SaaS Response no more than one hour after the successful submission of a customer request.

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 cause, 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 always respond in the stated time. The Response and Resolution Targets, including their scope and determining factors (such as impact and urgency), are further described at

<https://home.software.microfocus.com/myaccount/slo/>.

Termination Data Retrieval Period SLO

The Termination Data Retrieval Period is defined as the length of time in which the customer can retrieve a copy of their Cloud Network Observability and its add-on 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 Cloud Network Observability service. Micro Focus's ability to fulfill its responsibilities relative to SaaS is dependent upon the customer fulfilling the responsibilities described below and elsewhere herein:

Customer Roles and Responsibilities

Customer Role	Responsibilities
Business Owner	<ul style="list-style-type: none">• Owns the business relationship between Customer and Micro Focus• Owns the business relationship with a range of departments and organizations using Cloud Network Observability• Manages contract issues
Project Manager	<ul style="list-style-type: none">• Coordinates Customer resources as necessary• Serves as the point of contact between Customer and Micro Focus• Drives communication from the customer side• Serves as the point of escalation for issue resolution and service-related issues
Administrator	<ul style="list-style-type: none">• Serves as the first point of contact for Cloud Network Observability end users for problem isolation• Performs Cloud Network Observability 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 Customer site• Owns any customization
End User	<ul style="list-style-type: none">• Leverages the product functionality designed by Customer's Cloud Network Observability administrators.• Provides periodic feedback to the Cloud Network Observability administrator

Micro Focus Roles and Responsibilities

Micro Focus Role	Responsibilities
Customer Service Centre (CSC)	<ul style="list-style-type: none">• Primary point of contact for service requests. A customer can contact the Service Operations Center for all services such as support and maintenance, or issues regarding the availability of SaaS• Provides 24x7 application support
Operations Staff (Ops)	<ul style="list-style-type: none">• Monitors the Micro Focus systems and SaaS Service 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:

- Customers must update components deployed in the monitored environment, and these components must be compatible with the current Cloud Network Observability version. Compatibility information is available in the support matrix at <https://docs.microfocus.com/doc/cno/SaaS/Home>
- 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 the 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.