Service Description

OpenText™ Core Software Delivery Platform Functional Testing

January 2026

opentext™

Contents

This Service Description describes the components and services included in OpenText Core Software Delivery Platform Functional Testing (which also may be referred to as Core SDP FT, or "SaaS") and, unless otherwise agreed to in writing, is subject to the Micro Focus Customer Terms for Software-as-a-Service ("SaaS Terms") found at https://www.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

Core Software Delivery Platform Functional Testing (Core SDP FT) is a cloud-based functional testing solution that includes test script design, model-based testing, a digital lab, test scheduling and execution, and an AI engine for object recognition in test automation.

Core SDP FT is built on top of the OpenText Core Software Delivery Platform. It is available either as a module within OpenText Core Software Delivery Platform, or independently.

SaaS Delivery Components

When delivered independently: **One Core SDP FT production instance**	✓
When delivered as a module within OpenText Core Software Delivery Platform: **One Core SDP FT module as part of one OpenText Core Software Delivery Platform production instance**	✓
✓ **= Included**	
O = Optional for a fee	

When delivered as an OpenText Core Software Delivery Platform module, the OpenText Core Software Delivery Platform is the governing Service Description for the OpenText Core Software Delivery Platform.

The functionality of Core SDP FT is described in the Core SDP FT Online Help.

SaaS Operational Services

Operational Services	
Onboarding Enablement[1]	✓
Dashboard reporting[1]	✓
Configuration Support[1]	✓
Single sign-on (SSO) integration	✓
Integration support via REST API	✓
✓ **= Included**	
O = Optional for a fee	

[1] For customers with private hosted devices

Architecture Components

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

Micro Focus does not install, deploy or manage on-premise components that may be required to use Core SDP FT SaaS.

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

Standard Configuration

The standard configuration for Core SDP FT is as follows:

Property	Support value
System Availability	99.9% SLO
Available Tenants	Up to 2
Storage for tests, test assets, and test results	Up to 300 GB
Automated Test Runs and Run History retention time	Up to 2 years
Total number of test runs	Up to 4000 runs per month

Application Administration

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

Service Support

Customer may contact Micro Focus through submitting online support tickets. The Micro Focus Support Team will either provide support to Customer directly or coordinate delivery of this support.
Online support for SaaS is available at: https://home.software.microfocus.com/myaccount

Support for on-premise components is available at: https://www.microfocus.com/en-us/support Micro Focus staffs and maintains a 24x7x365 Service Operations Center, which will be the single point of contact for all issues related to the support for SaaS. Customer will maintain a list of authorized users who may contact Micro Focus for support. Customer's authorized users may contact Micro Focus for support via the Web portal 24 hours a day, 7 days a week.

Support Features:

Activity	
99.9% Availability SLO	✓
Customer Manager Services	✓
Solution Expert Services	✓
Welcome Package	✓
Technical Enablement	✓
Email and Online Notifications	✓
Major Version updates. Notification period according to notification timelines via email, release notes and help resources available.	✓
Regular Service Reviews to review service quality and to provide feedback on improvements required	✓
Regular Adoption Reviews to plan how best to adopt product features and best practices based on your business objectives	✓
✓ = Included	
O = Optional for a fee	

Service Monitoring

Micro Focus monitors SaaS availability 24x7. Micro Focus uses a centralized notification system to deliver proactive communications about service changes, outages and scheduled maintenance. Alerts and notifications are available to Customer online at: https://home.software.microfocus.com/myaccount

Capacity and Performance Management

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

Operational Change Management

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

Data Backup and Retention

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

SaaS Data

Customer is solely responsible for the data, text, audio, video, images, software, and other content input into a Micro Focus system or environment during Customer's (and its Affiliates' and/or Third Parties') access or use of Micro Focus SaaS ("SaaS Data"). The following types of SaaS Data reside in the SaaS environment: attachments, test automation scripts, documents and files.

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

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

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

Backups

Micro Focus performs both on-site and off-site backups with a 24 hours recovery point objective (RPO). Backup cycle occurs daily where a local copy of production data is replicated on-site between two physically separated storage instances. The backup includes a snapshot of production data along with an export file of the production database. The production data is then backed up at a remote site. Micro Focus uses storage and database replication for its remote site backup process. The integrity of backups is validated by (1) real time monitoring of the storage snapshot process for system errors, and (2) annual restoration of production data from an alternate site to validate both data and restore flows integrity.

SaaS Security

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

Technical and Organizational Measures

Micro Focus regularly tests and monitors the effectiveness of its controls and procedures. No security measures are or can be completely effective against all security threats, present and future, known and unknown. The measures set forth in this section may be modified by Micro Focus but represent a minimum standard. Customer remains responsible for determining the sufficiency of these measures.

Physical Access Controls

Micro Focus maintains physical security standards designed to prohibit unauthorized physical access to the Micro Focus equipment and facilities used to provide SaaS and include Micro Focus data centers and data centers operated by third parties. This is accomplished through the following practices:

- Presence of on-site security personnel on a 24x7 basis
- Use of intrusion detection systems
- Use of video cameras on access points and along perimeter
- Micro Focus employees, subcontractors and authorized visitors are issued identification cards that must be worn while on premises
- Monitoring access to Micro Focus facilities, including restricted areas and equipment within facilities
- Securing equipment hosting SaaS Data in designated caged areas and
- 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’ 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 and at rest. All inbound and outbound traffic to the external network is encrypted.

Audit

Micro Focus appoints an independent third party to conduct an annual audit of the applicable policies used by Micro Focus to provide SaaS. A summary report or similar documentation will be provided to Customer upon request. Subject to Customer's execution of Micro Focus' 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 SaaS 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 a weekly two (2) hours window (Sunday 00:00 to 02:00 Pacific Standard Time) and one (1) monthly four (4) hour window (Sunday in the 00:00 to 08:00 Pacific Standard Time block). These windows will be used on an as-needed basis.

Planned windows will be scheduled at least two (2) weeks in advance when Customer action is required, or at least four (4) days in advance otherwise.

Scheduled Version Updates

"SaaS Upgrades" are defined as major version updates, minor version updates, and binary patches applied by Micro Focus to Customer's SaaS in production. These may or may not include new features or enhancements. Micro Focus determines whether and when to develop, release and apply any SaaS Upgrade. Customer is entitled to SaaS Upgrades during the applicable SaaS Order Term unless the SaaS Upgrade introduces new functionality that Micro Focus offers on an optional basis for an additional fee.

Micro Focus will use the Scheduled Maintenance windows defined herein to apply the most recent service packs, hot fixes, and minor version updates to SaaS. To enable Customer to plan for scheduled major version updates by Micro Focus, Micro Focus will schedule major version updates at least two (2) weeks in advance. However, if Micro Focus does not receive Customer's cooperation in achieving the SaaS Upgrade in a timely manner, Micro Focus reserves the right to charge Customer additional fees that are related to Customer's SaaS instance remaining on a version that is beyond the "end of support" period. Customer also understands that this status may prevent the most recent patches from being applied to its SaaS solution, and that the availability, performance, and security of SaaS as described in this Service Description may be impacted as a result.

Service Decommissioning

Upon expiration or termination of the SaaS Order Term, Micro Focus may disable all Customer access to SaaS, and Customer shall promptly return to Micro Focus (or at Micro Focus' request destroy) any Micro Focus materials.

Micro Focus will make available to Customer any SaaS Data in Micro Focus' possession in the format generally provided by Micro Focus. The target timeframe is set forth below in Termination Data Retrieval Period SLO. After such time, Micro Focus shall have no obligation to maintain or provide any such data, which will be deleted.

Service Level 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://home.software.microfocus.com/myaccount

SaaS Provisioning Time SLO

SaaS Provisioning Time is defined as SaaS being available for access over the internet. Micro Focus targets to make SaaS available within three (3) business days of Customer's Order for SaaS 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 are not in scope of the SaaS Provisioning Time SLO.

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

SaaS Availability SLO

SaaS Availability is defined as 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 % ("SaaS Uptime").

Measurement Method

SaaS 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, SaaS 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

SaaS Uptime 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
- Force majeure events
- Actions or omissions 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

Online Support Availability SLO

Online Support Availability is defined as the SaaS support portal https://home.software.microfocus.com/myaccount being available for access and use by Customer over the Internet. Micro Focus targets to provide Customer access to the SaaS support portal on a twenty-four hour, seven days a week (24x7) basis at a rate of 99.9% (“Online Support Uptime”).

Measurement Method

Online Support Uptime shall be measured by Micro Focus using Micro Focus monitoring software running from a minimum of four global locations with staggered timing. On a quarterly basis, Online Support Uptime will be measured using the measurable hours in the quarter (total time minus planned downtime, including maintenance, upgrades, etc.) as the denominator. The numerator is the denominator value minus the time of any outages in the quarter (duration of all outages combined) to give the percentage of available uptime (2,198 actual hours available / 2,200 possible available hours = 99.9 availability).

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

Boundaries and Exclusions

Online Support Uptime shall not apply to or include any time during which the SaaS support portal is unavailable in connection with any of the following (specifically, the number of hours of unavailability in the measured period per the Measurement Method section above due to the following shall not be included in either the numerator or the denominator for the measurement):

- Overall Internet congestion, slowdown, or unavailability
- Unavailability of generic Internet services (e.g. DNS servers) due to virus or hacker attacks
- Force majeure events
- Actions or inactions of Customer (unless undertaken at the express direction of Micro Focus) or third parties beyond the control of Micro Focus
- Unavailability due to Customer equipment or third-party computer hardware, software, or network infrastructure not within the sole control of Micro Focus
- Scheduled maintenance
- Scheduled SaaS Upgrades

Initial SaaS Response Time SLO

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

SaaS Support SLOs

There are two types of SaaS Support SLOs: Service Request and Support Request SLOs:

- The Service Request SLO applies to the majority of routine system requests. This includes functional system requests (product add/move/change), informational, and administrative requests.
- The Support Request SLO applies to issues that are not part of the standard operation of the service, and which causes, or may cause, an interruption to or a reduction in the quality of that service

The Response and Resolution Targets are provided as guidelines and represent typical request processing by Micro Focus SaaS support teams. They in no way create a legal requirement or obligation for Micro Focus to respond in the stated time. The Response and Resolution Targets, including their scope and determining factors (such as impact and urgency), are further described at https://home.software.microfocus.com/myaccount/slo/.

Termination Data Retrieval Period SLO

The Termination Data Retrieval Period is defined as the length of time in which Customer can retrieve a copy of their SaaS Data from Micro Focus. Micro Focus targets to make available such data for download in the format generally provided by Micro Focus for 30 days following the termination of the SaaS Order Term.

Service Level Objectives for Core SDP FT Lab for Mobile and Web

Public Device Add-On

Public Device Connectivity Issue – Single Device Report on single device disconnection.
Response Time: Up to 24 business hours
Resolution Time: Up to 5 business days
Standard Resolution Time: Up to 4 business days

Public Device Connectivity Issue – Multiple Devices Report on multiple devices disconnection
Response Time: Up to 8 business hours Resolution Time: Up to 5 business days
Standard Resolution Time: Up to 1 business days

Customer is responsible for installing, deploying, and configuring any additional on-premise components for its applications. Any on-premise components 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.

Private Device Add-On

Mobile Device Setup

- Assistance with a local mobile device or cloud-hosted device setup
- Response Time: Up to 24 business hours
- Standard Resolution Time: Up to 14 business days
- Device Allocation/Swap Request for mobile device(s) allocation
- Response Time: Up to 24 business hours
- Trial Resolution Time: Up to 14 business days
- Standard Resolution Time: Up to 14 business days

Device Configuration Request for device configuration

- Response Time: Up to 24 business hours
- Trial Resolution Time: Up to 7 business days
- Standard Resolution Time: Up to 5 business days

Device Connectivity Issue – Single Device Report on single device disconnection

- Response Time: Up to 24 business hours
- Resolution Time: Up to 7 business days
- Standard Resolution Time: Up to 5 business days

Device Connectivity Issue – Multiple Devices Report on multiple devices disconnection

- Response Time: Up to 8 business hours
- Resolution Time: Up to 7 business days
- Standard Resolution Time: Up to 1 business day

Request for Device clean up or wipe

- Response Time: Up to 24 business hours
- Resolution Time: Up to 7 business days
- Standard Resolution Time: Up to 7 business days

Customer is responsible for installing and configuring any additional onsite 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.

Standard Service Requirements

Roles and Responsibilities

This section describes general Customer and Micro Focus responsibilities relative to SaaS. Micro Focus' 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 SaaS 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' 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 SaaS 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' 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.

Core SDP FT Lab for Mobile and Web Optional Services

Public Device Add-On

The following Add-On for Core SDP FT Lab for Mobile and Web is optional and need to be explicitly ordered by Customer for an additional fee. This section is applicable only if Customer has an Order for the Add-On.

High Level Summary

The Core SDP FT Lab for Mobile and Web Public Device Add-On allows Customer to connect to the Core SDP FT Lab for Mobile and Web environment and public mobile devices which are hosted by Micro Focus ("Public Device"). A Public Device, unlike a private device which is fully dedicated to a customer, is a device that other customers can also use. Each customer can connect the Public Device to their Core SDP FT Lab for Mobile and Web environment for a limited time, and after every session the Public Device is cleaned automatically.

Pre-Requisites for Public Device Add-On

Micro Focus requires one or more of the following components, licensed and deployed separately by Customer, to purchase and use the Public Device Add-On:

- OpenText Functional Testing Lab for Mobile and Web (UFT Digital Lab or UFT Mobile) 2022 and later, or
- Core SDP FT 2023 and later

Full documentation for integrating on-premise components with the Public Device Add-On is available at:
https://admhelp.microfocus.com/digitallab/en/latest/Content/Adding_Devices.htm

Customer must install, configure, and deploy any required components and pay any additional fees.

Hosting Locations

The Public Devices are hosted in one location: **Europe**: Lisbon, Portugal

The data center is connected to the Core SDP FT Lab for Mobile and Web framework on port 443 (HTTPS).

Public Device Fleet

The Public Device fleet includes iOS and Android mobile devices of various models which are running different OS versions.

Using Public Devices

If a Public Device is available, Customer can connect it to its Core SDP FT Lab for Mobile and Web environment and start using it immediately.

If a Public Device is in use, Customer can view its position in the queue and select to connect it, and when available for Customer the device will be connected automatically.

Customer can select to disconnect the Public Device at any point. The Public Device will be disconnected automatically after reaching the 1-hour maximum Public Device usage time.

Public Device cleanup

When a Public Device is disconnected, it will be cleaned automatically before any other customer can use it. As part of the cleanup, any application which was installed on the Public Device during the session is uninstalled, the tabs of the native browser (Safari/Chrome) are closed and the history and cache are cleared, photos and videos are deleted, non-system files and folders are cleared (Android), and provision profiles and crash reports are cleared (iOS).

Public Device Access

The connection from Customer's browser or testing tool to the hosted Public Device farm is over HTTPS/WSS on port 443.

Public Device Connectivity

The Public Devices are connected to a wireless (Wi-Fi) network with internet access. Cellular connection (SIM card) is not available.

Public Device Per Hour Consumption

Public Device usage is provided by units of thirty 30 hours ("Public Device Hours"). The consumption of the Public Device Hours purchased by Customer starts when a Public Device is connected and stops when the Public Device is disconnected. Consumption is calculated by minutes.

SaaS Service Delivery Components

Core SDP FT Lab for Mobile and Web (ValueEdge Functional Test Digital Lab) Public Mobile Device Per 30 Hours Subscription SaaS

Private Device Add-On

The following Add-On for Core SDP FT Lab for Mobile and Web is optional and need to be explicitly ordered by Customer for an additional fee. This section is applicable only if Customer has an Order for the Add-On.

High Level Summary

The Core SDP FT Lab for Mobile and Web Private Device Add-On allows Customer to connect to the Core SDP FT Lab for Mobile and Web environment and private mobile devices which are hosted by Micro Focus ("Private Device"). A Private Device is fully dedicated to Customer.

Pre-Requisites for Private Device Add-On

Micro Focus requires one or more of the following components, licensed and deployed separately by Customer, to purchase and use the Private Device Add-On:

- Core SDP FT Lab for Mobile and Web (UFT Digital Lab or UFT Mobile) 2022 and later, or
- Core SDP FT Lab for Mobile and Web 2023 and later

Full documentation for integrating on-premise components with the Private Device Add-On is available at: https://admhelp.microfocus.com/digitallab/en/latest/Content/Adding_Devices.htm

Customer must install, configure, and deploy any required components and pay any additional license/service fees.

Hosting Locations

Private Devices may be hosted at any of the following locations:

- **North America**: New York City
- **Europe**: Sofia, Bulgaria; Lisbon, Portugal
- **South America**: Sao Paulo, Brazil

The Private Devices are connected to Core SDP FT Lab for Mobile and Web framework on port 443 (HTTPS).

Private Device Models

Customer can choose any iOS or Android Private Device which is running a supported OS version. Micro Focus will confirm that the selected Private Device is compatible and available in the selected region.

Private Device Allocation

Once a Private Device is ordered as part of this service, a fully dedicated Private Device will be allocated to Customer for a period of 12 months.

Allocation and initial setup time for common commercially available devices would normally not exceed 7 working days. In some cases, where there is limited availability of a device Micro Focus will do its best to get this device as soon as possible.

Private Device Swaps

Customer is entitled to swap up to 30% of its Private Device fleet once every 12 months.

Private Device Access

The connection from Customer's browser or testing tool to the Private Device farm is over HTTPS/WSS on port 443.

Private Device Connectivity

The Private Devices are connected to a wireless (Wi-Fi) network with internet access. Cellular connection (SIM card) is not available.

Private Device Deallocation

At contract end or after a Private Device is swapped, Micro Focus will perform a factory reset on the Private Device to ensure that all data and applications are removed.

SaaS Service Delivery Components

Core SDP FT Lab for Mobile and Web (ValueEdge Functional Test Digital Lab) Private Mobile Device.