

Service Description

UFT Digital Lab Software-as-a-Service

August 2023



Copyright 2023 Open Text

Contents

Contents 2

1. Standard Service Features..... 3

2. Data Backup and Retention..... 4

3. SaaS Security 5

4. Audit 7

5. Micro Focus Security Policies 7

6. Security Incident Response 7

7. Micro Focus Employees and Subcontractors 8

8. Data Subject Requests..... 8

9. Scheduled Maintenance..... 8

10. Service Decommissioning..... 8

11. Service Level Objectives 9

12. UFT Digital Lab - Public Device Add-On..... 12

13. UFT Digital Lab - Private Device Add-on..... 14

14. Standard Service Requirements 15

This Service Description describes the components and services included in Micro Focus UFT Digital Lab SaaS (which also may be referred to as “UFT Digital Lab SaaS” or “SaaS”) and, unless otherwise agreed to in writing, is subject to the Micro Focus Customer Terms for Software-as-a-Service (“SaaS Terms”) found at <https://www.microfocus.com/en-us/legal/software-licensing>. Capitalized terms used but not defined herein shall have the meanings set forth in the SaaS Terms.

1. Standard Service Features

1.1 High Level Summary

UFT Digital Lab SaaS is an enterprise-grade mobile devices lab that helps teams develop, debug, test, monitor, and optimize their Omni-channel mobile applications to promote an enhanced user experience across all digital touchpoints. With UFT Digital Lab SaaS, developers and testers can validate all aspects of the mobile user experience including functionality, performance, and security. UFT Digital Lab SaaS supports continuous testing, and drives continuous improvement and optimization by analyzing usage, network performance, and mobile application production monitoring.

1.2 SaaS Service Delivery Components

One UFT Digital Lab SaaS production instance	<input checked="" type="checkbox"/>
--	-------------------------------------

1.3 SaaS Operational Services

SaaS Operational Services	
Onboarding enablement	√
Micro Focus Dashboard reporting	√
Configuration Support	√
Single sign-on support	√
Web services support	√
External integrations support	√
√ = Included	

1.4 Architecture Components

UFT Digital Lab SaaS includes a cloud-based platform with a management and execution web interface. UFT Digital Lab SaaS is single tenant meaning that each customer of this SaaS offering receives its own segregated farm. The solution includes high availability (active/passive), load balancing and security measures. Micro Focus SaaS does not manage, operate, or support on premise components on behalf of Customer.

1.5 Application Administration

Customer accesses UFT Digital Lab SaaS using supported web browser via the URL provided to them. Once securely logged in, the Customer can perform administrative tasks. (See examples - <https://admhelp.microfocus.com/mobilecenter/en/latest/Content/AdminTasks.htm>)

1.6 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.

Online support is available at: <https://home.software.microfocus.com/myaccount>

Product support is available from the Micro Focus Micro Focus UFT Digital Lab Community at:

<https://community.microfocus.com/t5/Mobile-Center/ct-p/MobileCenter>

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 UFT Digital Lab SaaS for the Customer. Customer will maintain a list of authorized users who may contact Micro Focus for support. Customer's authorized users may contact Micro Focus for support via the Web portal or telephone 24 hours a day, 7 days a week.

Activity	
Customer Success Manager Services	✓
Solution Expert Services	✓
Welcome Package	✓
Technical Enablement and Pre-recorded enablement videos	✓
Email and Online Notifications	✓
On boarding: Kick off meeting, handover of support materials, verification of online access, service goals, discussion of training requirements	✓
Major version updates. Notification period according to notification timelines via email, release notes and help resources available. Major version update meeting, including discussion of changes required to take advantage of new features and requirements to implement the update.	✓
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	✓
99.9 % Availability SLA	✓
✓ = Included	

1.7 Service Monitoring

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

1.8 Capacity and Performance Management

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

1.9 Operational Change Management

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

2. Data Backup and Retention

The data backup and retention described in this section are part of Micro Focus's overall business

continuity management practices designed to attempt to recover availability to SaaS and SaaS Data for Customer following an outage or similar loss of service for SaaS.

2.1 SaaS Data

The following types of Customer-specific data are included in UFT Digital Lab SaaS that resides in the Micro Focus SaaS environment: Customer inserted data (for example attachments, scripts, documents, and files).

Micro Focus performs a backup of SaaS Data every one (1) day. Micro Focus retains each backup for the most recent seven (7) days.

Micro Focus's standard storage and backup measures are Micro Focus's only responsibility regarding the retention of this data, despite any assistance or efforts provided by Micro Focus to recover or restore Customer's data. Customer may request via a service request for Micro Focus to attempt to restore such data from Micro Focus's most current backup. Micro Focus will be unable to restore any data not properly entered by Customer, or lost or corrupted at the time of backup or if Customer's request comes after the 7 days data retention time of such backup.

2.2 Disaster Recovery

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.

UFT Digital Lab 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 Micro Focus SaaS within twelve (12) hours following Micro Focus's 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 are validated by (1) real time monitoring of the storage snapshot process for system errors, (2) validating CHECKSUM at the end of a backup process to assure the same number of bits exists on both source and destination storage systems, and (3) annual restoration of production data from an alternate site to validate both data and restore flows integrity.

3. SaaS Security

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

3.1 Technical and Organizational Measures

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

3.2 Physical Access Controls

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

- Presence of on-site security personnel on a 24x7 basis
- Use of intrusion detection systems
- Use of video cameras on access points and along perimeter
- Micro Focus employees, subcontractors and authorized visitors are issued identification cards that must be worn while on premises
- Monitoring access to Micro Focus facilities, including restricted areas and equipment within facilities
- Securing equipment hosting SaaS Data in designated caged areas
- Maintaining an audit trail of access

3.3 Access Controls

Micro Focus maintains the following standards for access controls and administration designed to make SaaS Data accessible only by authorized Micro Focus personnel who have a legitimate business need for such access:

- Secure user identification and authentication protocols
- Authentication of Micro Focus personnel in compliance with Micro Focus standards and in accordance with ISO27001 requirements for segregation of duties
- SaaS Data is accessible only by authorized Micro Focus personnel who have a legitimate business need for such access, with user authentication, sign-on and access controls
- Employment termination or role change is conducted in a controlled and secured manner
- Administrator accounts should only be used for the purpose of performing administrative activities
- Each account with administrative privileges must be traceable to a uniquely identifiable individual
- All access to computers and servers must be authenticated and within the scope of an employee's job function
- Collection of information that can link users to actions in the SaaS environment
- Collection and maintenance of log audits for the application, OS, DB, network, and security devices according to the baseline requirements identified
- Restriction of access to log information based on user roles and the "need-to-know"
- Prohibition of shared accounts

3.4 Availability Controls

Micro Focus's business continuity management process includes a rehearsed method of restoring the ability to supply critical services upon a service disruption. Micro Focus's continuity plans cover operational shared infrastructure such as remote access, active directory, DNS services, and mail services. Monitoring systems are designed to generate automatic alerts that notify Micro Focus of events such as a server crash or disconnected network.

Controls regarding disruption prevention include:

- Uninterruptible power supplies (UPS) and backup power generators
- At least two independent power supplies in the building

- Robust external network connectivity infrastructure

3.5 Data Segregation

SaaS environments are segregated logically by access control mechanisms. Internet-facing devices are configured with a set of access control lists (ACLs), which are designed to prevent unauthorized access to internal networks. Micro Focus uses security solutions on the perimeter level such as: firewalls, IPS/IDS, proxies and content-based inspection in order to detect hostile activity in addition to monitoring the environment's health and availability.

3.6 Data Encryption

Micro Focus SaaS uses industry standard techniques to encrypt SaaS Data in transit. All inbound and outbound traffic to the external network is encrypted.

4. Audit

Micro Focus appoints an independent third party to conduct an annual audit of the applicable policies used by Micro Focus to provide SaaS. A summary report or similar documentation will be provided to Customer upon request. Subject to Customer's execution of Micro Focus's standard confidentiality agreement, Micro Focus agrees to respond to a reasonable industry standard information security questionnaire concerning its information and physical security program specific to SaaS no more than once per year. Such information security questionnaire will be considered Micro Focus confidential information.

5. Micro Focus Security Policies

Micro Focus conducts annual reviews of its policies around the delivery of SAAS against ISO 27001, which includes controls derived from ISO 27034 – "Information Technology – Security Techniques – Application Security". Micro Focus regularly re-evaluates and updates its information and physical security program as the industry evolves, new technologies emerge, or new threats are identified.

6. Security Incident Response

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

7. Micro Focus Employees and Subcontractors

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

8. Data Subject Requests

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

9. 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.

9.1 Scheduled Version Updates

“SaaS Upgrades” are defined as both major version updates, minor version updates and binary patches applied by Micro Focus to Customer’s UFT Digital Lab 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 as part of UFT Digital Lab SaaS service unless the SaaS Upgrade introduces new functionality that Micro Focus offers on an optional basis for an additional fee.

Micro Focus will use the Scheduled Maintenance windows defined above to apply the most recent service packs and hot fixes and to perform upgrade to minor versions of UFT Digital Lab SaaS. To enable Customers to plan for scheduled major version updates by Micro Focus, Micro Focus will be scheduling major version updates at least two (2) weeks in advance.

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 additional fees for UFT Digital Lab SaaS 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 UFT Digital Lab SaaS, and that the availability, performance, and security of UFT Digital Lab SaaS as described in Service Description may be impacted as a result.

10. Service Decommissioning

Upon expiration or termination of the SaaS Order Term, Micro Focus may disable all Customer access to SaaS, and Customer shall promptly return to Micro Focus (or at Micro Focus’s request destroy) any Micro Focus materials. Micro Focus will make available to Customer any SaaS Data in Micro Focus’ possession in the format generally provided by Micro Focus. The target timeframe is set forth below in Termination Data Retrieval Period SLO. After such time, Micro Focus shall have no obligation to maintain or provide any such data, which will be deleted in the ordinary course

11. 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>

11.1 UFT Digital Lab SaaS SLO

Solution Provisioning Time SLO

Solution Provisioning is defined as SaaS being available for access over the internet. Micro Focus targets to make SaaS available within five (5) 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 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.

Solution Availability SLO

Solution 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 % ("Solution Uptime").

Measurement Method

Solution 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, Solution 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

Solution 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

11.2 Public and Private Devices Add-On SLOs

UFT Digital Lab Public Devices 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.

UFT Digital Lab Private Devices 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 5 business days

Device Allocation/Swap Request for mobile device(s) allocation

Response Time: Up to 24 business hours

Trial Resolution Time: Up to 7 business days

Standard Resolution Time: Up to 7 business days

Device Configuration Request for device configuration Response Time: Up to 24 business hours

Trial Resolution Time: Up to 5 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 5 business days

Standard Resolution Time: Up to 4 business days

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

Request for Device clean up or wipe Request for device clean-up/wipe

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

The 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.

11.3 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

11.4 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.

11.5 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/>

11.6 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.

12. UFT Digital Lab - Public Device Add-On

The following Add-On for UFT Digital Lab is optional and need to be explicitly ordered by Customer at a respective service fee. This section is applicable only if Customer has an Order for the Add-On. .

12.1 High Level Summary

The UFT Digital Lab Public Device Add-On allows Customer to connect to the UFT Digital Lab 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 UFT Digital Lab environment for a limited time, and after every session the Public Device is cleaned automatically.

Public Devices enable customers to increase test coverage and to test on more devices concurrently, without having to purchase additional devices.

12.2 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:

- UFT Digital Lab 2022 and later, or
- UFT Digital Lab SaaS 2022 and later

Full documentation for integrating on-premise components with the Public Device Add-On is available at:

<https://admhelp.microfocus.com/uftmobile/UnderConstruction.htm#ConnectPublic>

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

12.3 Hosting Locations

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

The data center is connected to the UFT Digital Lab SaaS framework using a secured network connection (VPN).

12.4 Public Device Fleet

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

12.5 Using Public Devices

If a Public Device is available, Customer can connect it to its UFT Digital Lab 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.

12.6 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).

12.7 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.

12.8 Public Device Connectivity

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

12.9 Public Device Per Hour Consumption

Public Device usage is provided by units of one (1) hour ("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.

12.10 SaaS Service Delivery Components

SaaS Delivery Components	
UFT Digital Lab Public Device Per Hour Subscription SaaS	✓

13. UFT Digital Lab - Private Device Add-on

The following Add-On for UFT Digital Lab is optional and need to be explicitly ordered by Customer at a respective service fee. This section is applicable only if Customer has an Order for the Add-On.

13.1 High Level Summary

The UFT Digital Lab Private Device Add-On allows Customer to connect to the UFT Digital Lab environment and private mobile devices which are hosted by Micro Focus ("Private Device"). A Private Device is fully dedicated to Customer.

13.2 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:

- UFT Digital Lab 2021 and later, or
- UFT Digital Lab SaaS 2021 and later

Full documentation for integrating on-premise components with the Private Device Add-On is available at: https://admhelp.microfocus.com/uftmobile/en/2022/Content/Adding_Devices.htm#Connect2

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

13.3 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 UFT Digital Lab framework using a secured network connection (VPN).

13.4 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.

13.5 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.

13.6 Private Device Swaps

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

13.7 Private Device Access

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

13.8 Private Device Connectivity

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

13.9 Private Device Deallocation

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

13.10 SaaS Service Delivery Components

SaaS Delivery Components	
UFT Digital Lab Private Mobile Device	✓

14. Standard Service Requirements

14.1 Roles and Responsibilities

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

14.2 Customer Roles and Responsibilities

Customer Role	Responsibilities
Business Owner	<ul style="list-style-type: none">• Owns the business relationship between the customer and Micro Focus• Owns the business relationship with the range of departments and organizations using UFT Digital Lab SaaS• Manages contract issues

Project Manager	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Serves as the first point of contact for UFT Digital Lab SaaS end users for problemisolation • Performs UFT Digital Lab SaaS administration • Provides tier-1 support and works with Micro Focus to provide tier-2 support • Coordinates end-user testing as required

	<ul style="list-style-type: none"> • Leads ongoing solution validation • Trains the end-user community • Coordinates infrastructure-related activities at the Customer site • Owns any customization
Subject Matter Expert	<ul style="list-style-type: none"> • Leverages the product functionality designed by Customer's UFT Digital Lab SaaS administrators. • Provides periodic feedback to UFT Digital LabSaaS Administrator

14.3 Micro Focus Roles and Responsibilities

Micro Focus Role	Responsibilities
Service Operations Center Staff (SOC)	<ul style="list-style-type: none">• Primary point of contact for service requests. Customer can contact the Service Operations Center for all services such as support and maintenance, or issues regarding availability of UFT Digital Lab SaaS• Provides 24x7 application support• Provides 24x7 SaaS infrastructure support
Operations Staff (Ops)	<ul style="list-style-type: none">• Monitors the Micro Focus systems and UFT Digital Lab SaaS for availability• Performs system-related tasks such as backups, archiving, and restoring instances according to Micro Focus's standard practices

14.4 Assumptions and Dependencies

This Service Description is based upon the following assumptions and dependencies between the Customer and Micro Focus:

- Customer must have internet connectivity to access UFT Digital Lab SaaS
- UFT Digital Lab SaaS will be performed remotely and delivered 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 UFT Digital Lab 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 SaaS
- 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, UFT Digital Lab SaaS is provided based on the assumption that Customer will implement and maintain the following controls in its use of UFT Digital Lab SaaS:

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

14.5 Good Faith Cooperation

Customer acknowledges that Micro Focus's ability to perform the 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.