Flexxible®

# Documentation

# FlexxDesktop

**Document generated on: 2/5/2025**

# Contents

# Getting Started

Recognized in Gartner® Magic Quadrant™ for DaaS*, the **FlexxDesktop** platform offers organizations support, analysis, monitoring, and automation of their virtualization infrastructure from the outset.

With centralized management for administrators and line managers to observe and act on devices in real-time, **FlexxDesktop** provides the ability to identify and resolve issues as they arise and enables automated solutions for the most common tasks. Reduce support hours, costs, and frustration.

**FlexxDesktop** is a SaaS platform that enables analysis, management, and monitoring of users' work devices, the infrastructure hosting them, as well as experience management. Among its tools, it includes the following modules:

- Portal
- FlexxAgent
- Workspaces
- Analyzer
- Automate
- Monitor

To start using **FlexxDesktop**, in addition to the subscription, the installation of FlexxAgent on user physical or virtual machines is required as well as the configuration of infrastructure elements or cloud service subscriptions that make up the session delivery infrastructure to users.

**- Gartner, Magic Quadrant for Desktop as a Service, Stuart Downes, Craig Fister, Sunil Kumar, Eri Hariu, Mark Margevicius, Tony Harvey, September 5, 2023 GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the United States and internationally, and MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product, or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.**

## Documentation in PDF

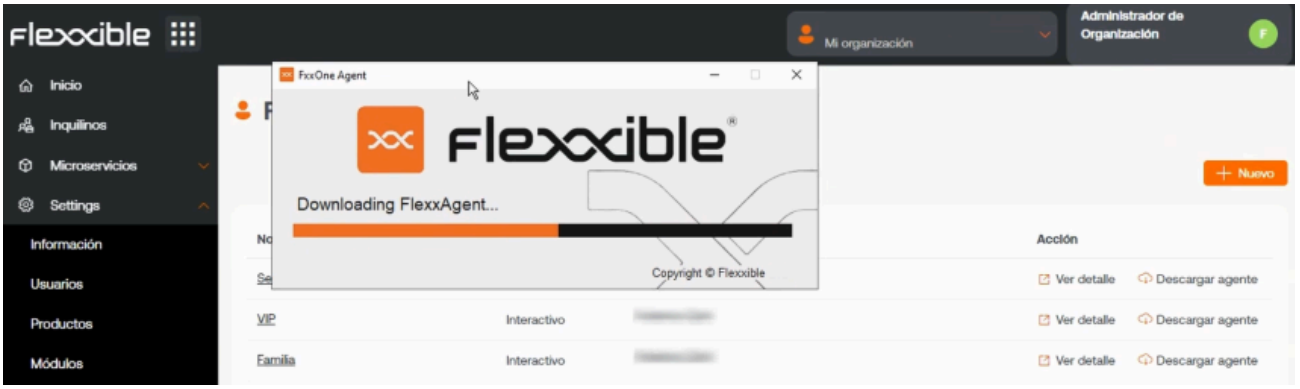
The documentation for FlexxDesktop for this version can be downloaded **here** in PDF format.

> **The downloaded file is an export of the content of this website for the selected version as of the version's publication date. It is recommended to periodically check for new versions on this page.**

# FlexxAgent

FlexxAgent is the local component of the solution. It collects information about devices and applications and sends it to the service's web consoles. It is a binary that, once installed, establishes end-to-end encrypted and secure communications.

FlexxAgent is compatible with Windows, Linux, macOS, ChromeOS, and Android operating systems.




# Features

- It is a mandatory component of the solution, so to see and manage a device in the consoles, it must have FlexxAgent installed.
- It allows remote and automatic actions on demand to improve the efficiency of support teams.
- It simplifies user self-service with the possibility to perform support actions autonomously without leaving the session.
- It gathers data about the device's status, usage, and errors.
- It reports on resource and application usage.
- It executes self-remediation actions.
- It provides a secure remote assistance interface to users and unattended access to administrators.
- It can perform operations on devices, such as waking them on the network via Wake on LAN (WoL).

# Functionality

The operating, installation, diagnostic particularities or details of FlexxAgent for each operating system are described in their respective article. The global functionalities of FlexxAgent, as well as its level of operability for each supported operating system, are defined in the following table:

| Feature | Windows | Linux | macOS | Android | ChromeOS |
|---|---|---|---|---|---|
| Storage information | ⭐⭐⭐ | ⭐⭐⭐ | ⭐⭐⭐ | ⭐⭐ | ⭐⭐ |
| Network information | ⭐⭐⭐ | ⭐⭐⭐ | ⭐⭐⭐ | ⭐⭐ | ⭐⭐ |
| System hardware information | ⭐⭐⭐ | ⭐⭐ | ⭐⭐ | ⭐ | ⭐ |
| System performance information | ⭐⭐⭐ | ⭐⭐ | ⭐⭐ | ⭐ | ⭐ |
| User session performance information | ⭐⭐⭐ | ⭐⭐ | ⭐⭐ | ⭐ | ⭐ |
| Diagnostic information | ⭐⭐⭐ | ⭐⭐ | ⭐⭐ | ⭐ | ⭐ |
| User notifications | ⭐⭐⭐ | ⭐⭐ | ⭐⭐ | ⭐ | ⭐ |
| Installed apps | ✅ | ✅ | ✅ | ✅ | ✅ |

| Feature | Windows | Linux | macOS | Android | ChromeOS |
|---|---|---|---|---|---|
| FlexxAgent auto-update | ✅ | ✅ | ✅ | Managed by Google Play | Managed by Google Play |
| Session and power actions | ✅ | ✅ | ✅ | N/A | N/A |
| Proxy support | ✅ | ✅ | ✅ | | |
| OS update information | ✅ | ✅ | | N/A | N/A |
| Microservices execution | ✅ | ✅ | | N/A | N/A |
| OS update application | ✅ | ✅ | | N/A | N/A |
| User processes | ✅ | ✅ | | | |
| System processes | ✅ | ✅ | | | |
| System event collection | ✅ | N/A | N/A | N/A | N/A |
| Applied GPO collection | ✅ | | N/A | N/A | N/A |
| Plug & Play devices and errors | ✅ | | | N/A | N/A |

| Feature | Windows | Linux | macOS | Android | ChromeOS |
|---|---|---|---|---|---|
| Custom fields | ✅ | | | N/A | N/A |
| Compliance information | ✅ | | | N/A | N/A |
| Wake on LAN | ✅ | | | N/A | N/A |
| System services | ✅ | | | N/A | N/A |
| End user microservice | ✅ | | | N/A | N/A |
| Flows | ✅ | | | N/A | N/A |
| CrowdStrike integration | ✅ | | | | |
| Application and system errors | ✅ | | | | |
| User experience surveys | ✅ | | | | |
| Remote Assistance | ✅ | | | | |
| Unattended remote assistance | ✅ | | | | |
| Dynamic remote assistance | ✅ | | | | |

INFO

- **Collected data levels**:
  ⭐ Basic
  ⭐ ⭐ Medium
  ⭐ ⭐ ⭐ Advanced
- ✅ The functionality is available for that operating system.
- **n/a** The functionality is not available for that operating system.

# Data retention

The data collected by FlexxAgent is sent to the service with retention times by data type, as defined below:

| Type | Information | Retention |
|---|---|---|
| Alert | Monitoring alerts generated on the devices | Indefinitely |
| Connection Logs | Includes information on when users log on, disconnect, reconnect, or log off on their device. | 30 days |
| Boot duration | Device uptime | 31 days |
| Sessions | Session performance information and counters | 2 hours of statistics |
| Workspaces | Device information, statistics, and details | 3 months of statistics |

| Type | Information | Retention |
| --- | --- | --- |
| Unreported workspaces | Since a device stops reporting, how many days until it is removed from the console | Controlled by a setting, default 31 days |
| Events logs | Log retention time for default and additional system logs, defined in FlexxAgent settings | 7 days |
| Plug and Play events | Peripheral information and events | 7 days |
| Jobs | Log of actions performed in the environment | 90 days |
| Notifications | Log of historical notifications generated in the environment | 3 months |

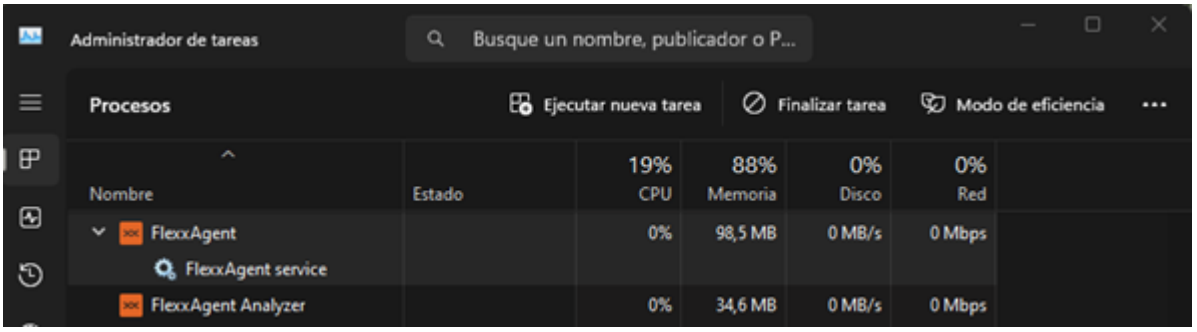
# FlexxAgent / Supported Systems

The agent is available in the support cycle for the following operating systems.

- Microsoft Windows
- Linux
- macOS
- ChromeOS
- Android

# FlexxAgent / Supported Systems / Windows

FlexxAgent supports 64-bit Windows operating systems; it cannot be installed on 32-bit systems. The installation binary is available with and without a graphical interface, making it fully compatible with unattended deployment mechanisms and the installation wizard.




FlexxAgent consists of a Windows service called FlexxAgent Service, which manages two processes: FlexxAgent (process), which runs at the system level, and FlexxAgent Analyzer (process), which starts for each user session.

This structure enables FlexxAgent to address multiple session devices, such as terminal servers, Citrix, or AVD, and acquire detailed metrics to enhance diagnostic capabilities.

For example, if a person is working on their laptop, the FlexxAgent process would run at the system level, and the FlexxAgent Analyzer would run from the user's identity. If the device hosts multiple user sessions, in addition to FlexxAgent at the system level, FlexxAgent Analyzer will run for each user session on that device.

In terms of resource requirements, FlexxAgent has very modest consumption, hovering around the following values:

- Disk space used: < 200 MB
- CPU: < 0.5%
- RAM: 100-200 MB

## FlexxAgent Service (system)

- For resource consumption information, including performance counters, hardware, sessions, profiles, disks, partitions, and Windows services, the default value is 60 seconds.
- Event log error events are sent every 10 minutes.
- User profile information is obtained every 15 minutes.

## FlexxAgent Analyzer (user)

- Includes application usage analysis, diagnostic data, and user experience.
- Data is collected locally every 15 seconds.
- The report is sent to the service every 5 minutes, although this metric can change in specific functionalities.

> **INFO**
>
> These values can be adjusted in `Settings` on the different consoles, providing flexibility to meet specific needs.

# Supported versions

The operating systems compatible with FlexxAgent are those still within the manufacturer's support cycle. Although installation is allowed on versions without such support, certain functionalities might not be available.

Microsoft operating systems with full support and compatibility are:

- Microsoft Windows 10 or later
- Microsoft Windows Server 2016 or later

FlexxAgent can also be installed on Windows 7 and 8.1 SP1, Windows Server 2008 R2 SP1, and Windows Server 2012, but it will be subject to some limitations.

# Software Requirements

FlexxAgent also requires certain software components:

- .NET Framework 4.6.2 or later, Flexxible recommends installing `.NET Framework 4.8`.
- Windows PowerShell 4.0 or later (Windows PowerShell 5.1 recommended)
    - Note: The Azure PowerShell execution policy should be set to `Unrestricted`.

## Considerations for Windows versions in EOL

Windows versions in End of Life (EOL), meaning they are out of support, have some limitations in running FlexxAgent, which may cause certain functionalities to not be supported.

## Limitations

Some limitations might disable its functionalities when using FlexxAgent on older Windows operating systems that are out of support:

- GPU consumption metric collection
- Flow execution
- End-user microservices execution
- Storage unit information
- For virtual devices, broker and hypervisor detection is not available for all providers.
- There is no User Input Delay (UID) data because this counter is only supported on Windows Server 2019 and later, and Windows 10, version 1809 and later.

Broker detection might not work for all brokers. There is no user input delay performance data as this counter does not exist in Windows 7 or Windows Server 2008 R2.

#### Windows 7 and 2008

The installation of FlexxAgent supports the Windows 7 x64 or Windows Server 2008 R2 SP1 operating system under the following conditions:

- The update KB4474419: `SHA-2 code signing support update for Windows Server 2008 R2, Windows 7, and Windows Server 2008: September 23, 2019` must be installed.

- The update KB3140245: `Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows` must be installed, and follow the instructions in the `How to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows` section of the Microsoft support page.
- Requires at least .NET Framework 4.6, but Flexxible recommends installing `.NET Framework 4.8`.
- PowerShell 2.0 with Windows 7 is not compatible with the required TLS 1.2 version to install FlexxAgent. `Windows Management Framework 5.1` is required to be installed, which installs PowerShell 5.1.

#### Windows 8 and 2012

The installation of FlexxAgent supports the Windows 8 operating system under the following conditions:

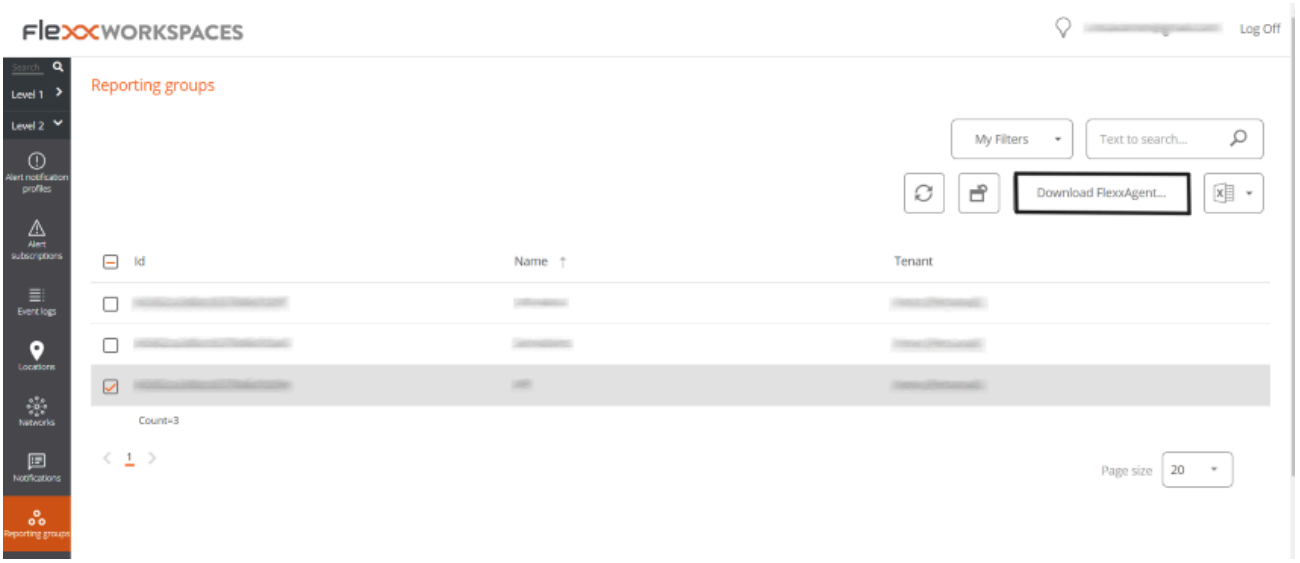
- `.NET Framework 4.6.2` is required, Microsoft blocks the installation of later versions of .NET Framework on Windows 8.0.
- All Windows security updates are required to ensure `compatibility with TLS 1.2 and SHA-2 code signing`.

# Download

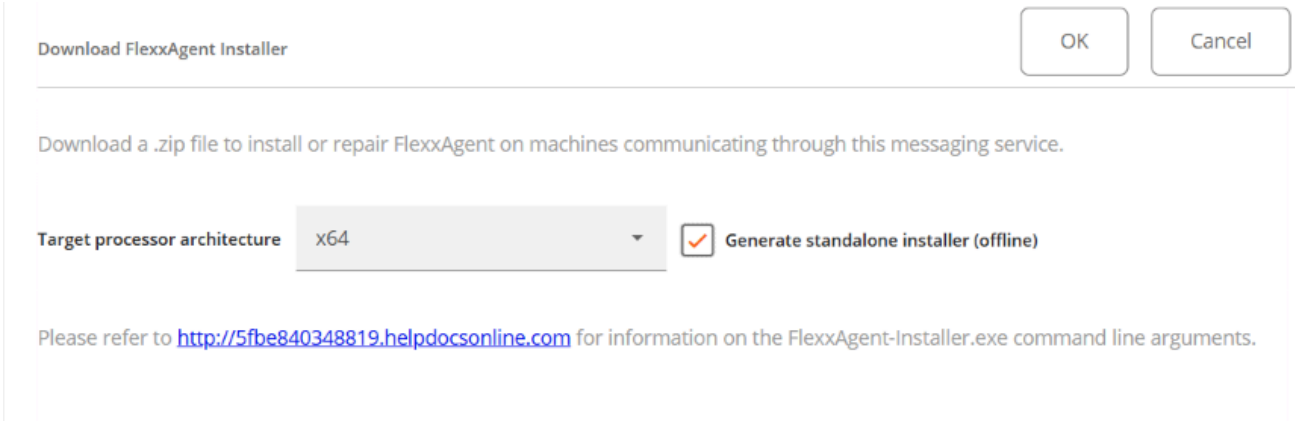
#### INSTALLATION BINARY DOWNLOAD WITHOUT GRAPHICAL INTERFACE

The download of FlexxAgent without a graphical interface is done from `Workspaces` -> `Level 2` -> `Reporting Groups`.

In the list view table, you must select the report group for which you want to download the agent and click on the `Download FlexxAgent` button.




A window will open to download the FlexxAgent installer.




- If the `Generate standalone installer (offline)` option is selected, during installation, the binary will not require internet access for verification or downloading binaries.

- If, on the other hand, the `Generate standalone installer (offline)` option is not selected, the minimal installation package will be downloaded. In this manner, the binary will access the internet to verify and download the latest binaries.

# Unattended Deployment

FlexxAgent supports being launched through unattended deployment methods, such as GPO distribution, Intune, SSCM, and many more tools.

# Installation

The unattended installation of FlexxAgent is done via PowerShell.

```
Start-Process "<ruta>\FlexxAgent-Installer.exe" -ArgumentList "<agregar parámetro>" -WindowStyle Hidden -Wait
```

# Uninstall

To uninstall FlexxAgent unattended:

```
"C:\Program Files\Flexxible\FlexxAgent\VDIServiceUpdater.exe" /Uninstall
"C:\Program Files\Flexxible\FlexxAgent\FlexxAgent.exe" /quiet
```

The Microsoft Windows installer used to uninstall FlexxAgent does not delete all files, folders, registry keys, or registry values created during the installation of FlexxAgent. If you need a clean system image, you can safely delete the following files, folders, registry keys and registry values.

#### Files

- `C:\Windows\Prefetch\FLEXXAGENT.EXE-XXXXXXXX.pf` – where XXXXXXXX is a string of letters and numbers
- `C:\Windows\Temp\FlexxAgentInstallation.log`

#### Folders

- `C:\Program Files\Flexxible`
- `C:\ProgramData\Flexxible`

# Reinstallation

To reinstall FlexxAgent on a device removing its preexisting configuration, execute:

```
FlexxAgent-Installer.exe -repairAgent
```

For example:

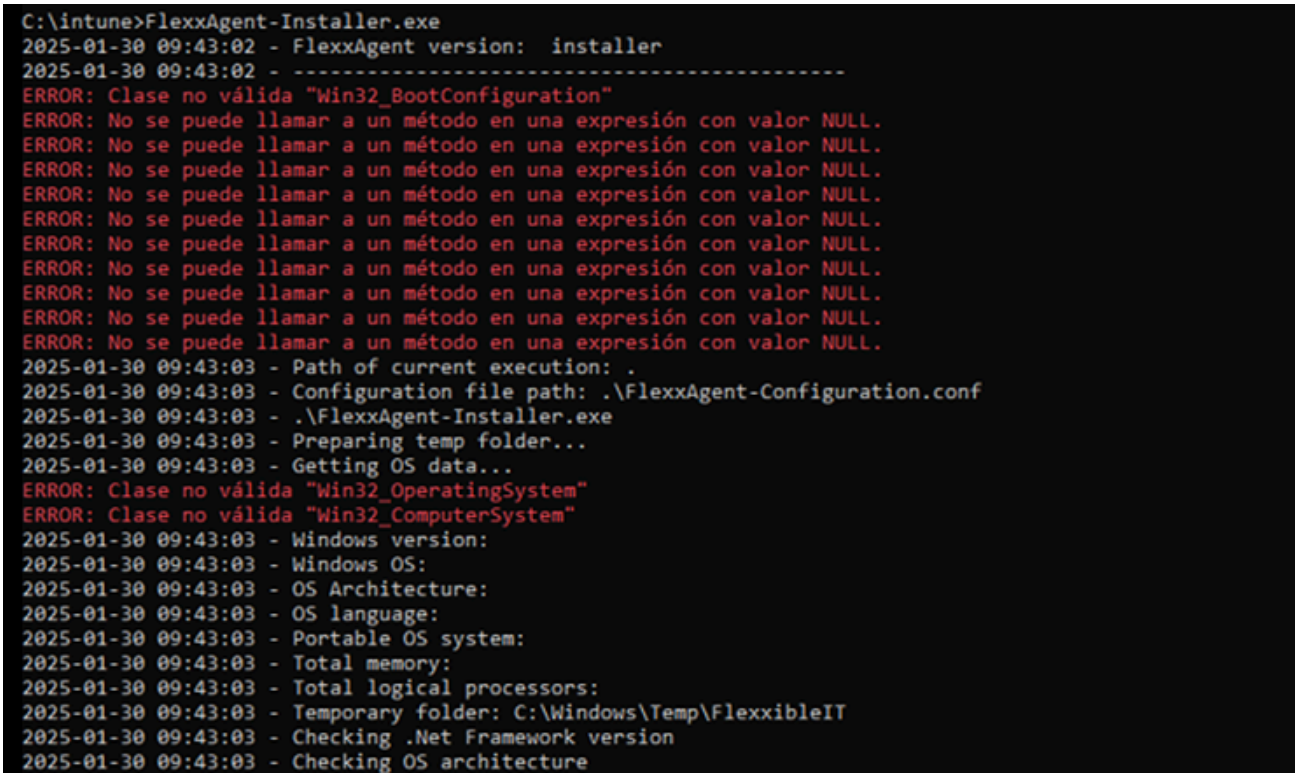
`Start-Process "<ruta>\FlexxAgent-Installer.exe" -ArgumentList "-repairAgent true" -WindowStyle Hidden -Wait`

# Known Issues

## FlexxAgent installation

#### Issue 1 - Windows Management Instrumentation (WMI)

During the installation and/or reinstallation of FlexxAgent, if the computer encounters issues caused by the Windows Management Instrumentation (WMI) service, the process may report these errors in the CMD window:




##### Solution

Run the following commands:

`Stop-Service winmgmt -Force`

`winmgmt /resetrepository`

```
Start-Service winmgmt
```

#### Issue 2 - PowerShell process restriction

Some security solutions do not allow the installation and/or self-update of FlexxAgent to be performed effectively. The installer might return the message:

> *The process was terminated with errors. A corrupted installation was detected due to external processes. This is usually caused by antivirus activity. Please check your antivirus settings.*

#### Solution

Exclude the following files from the device:

```
C:\Windows\Temp\FlexxibleIT
```

```
C:\Windows\Temp\UpdateFlexxAgent.ps1
```

### Uninstallation of FlexxAgent

#### Issue - FlexxAgent remains in the service list

FlexxAgent might still appear in the service list even after uninstalling and deleting all files. This would prevent FlexxAgent from being reinstalled.

#### Solution

Run the following command in the CMD window as administrator:

```
sc delete "FlexxAgent service"
```

Then, restart the device.

# Supported Parameters

| Parameter | Type | Caption | |
|---|---|---|---|
| proxyAbsoluteUri | [string] | Proxy URL and port. | |
| proxyUser | [string] | User for authenticated proxy. | |
| proxyPass | [string] | Password for authenticated proxy. | |
| proxyPersistConfig | [switch] | If specified, the configuration is persisted in the registry. | |
| configFilePath | [string] | Alternative directory for the FlexxAgent-Configuration.conf file. | |
| DebugMode | [switch] | When specified, creates a text file in the same folder with the script execution transcription. | |
| RepairAgent | [bool] | Removes the preexisting configuration of FlexxAgent when it is reinstalled on a device. | |
| Help | [switch] | Lists the supported parameters, with type and description. | |

# Proxy Configuration

FlexxAgent supports transparently configured proxies at the system level without configuring. Proxies with and without authentication are also supported. Proxy configuration can be done via the command line or by modifying registry keys that control this configuration.

## Proxy configuration through command line

Installation with parameters: `FlexxAgent-Installer.exe -proxyAbsoluteUri ip.ad.dre.ss:port -proxyPersistConfig:$True`

Where ip.ad.dre.ss:port refers to the IP or DNS plus the proxy port, or including credentials:

```
FlexxAgent-Installer.exe -proxyAbsoluteUri ip.ad.dre.ss:port -proxyUser ProxyUserName -proxyPass ProxyUserPassword -proxyPersistConfig:$True
```

> **INFO**
>
> FlexxAgent may not have access to the proxy applied in its configuration if it is outside the corporate network. To determine its accessibility, FlexxAgent tries to resolve the DNS record and makes a TCP request to the corresponding port. If the proxy is not accessible, it will report it directly (without proxy).

## Configuration through registry keys

Location of the registry keys that store the proxy configuration for FlexxAgent:

```
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Flexxible\FlexxAgent\Communications
```

Registry keys related to the proxy configuration:

- Key Proxy_URL
- Key Proxy_User
- Key Proxy_Pwd

#### Key Proxy_URL

- Key path: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Flexxible\FlexxAgent\Communications`
- Key Name: Proxy_URL
- Key type: REG_SZ
- Supported values: the URL and port; for example 'http://192.168.1.1:3128' or 'https://192.168.1.1:3128'

#### Key Proxy_User

- Key path: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Flexxible\FlexxAgent\Communications`
- Key Name: Proxy_User
- Key type: REG_SZ
- Supported values: the username to authenticate to the proxy; for example 'Administrator'. It can be bypassed for unauthenticated proxies.

**Key Proxy_Pwd**

- Key path: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Flexxible\FlexxAgent\Communications`
- Key Name: Proxy_Pwd
- Key type: REG_SZ
- Supported values: The password to authenticate to the proxy. It can be bypassed for unauthenticated proxies. The value of the Proxy_Pwd key can be set in plain text (not recommended) or base64 encoded and enclosed by «&&&». For example: `&&&VGhpc0lzTjArQCQzY3VyZVBAJCR3MHJk&&&` for the “Proxy_Pwd” value. In either case, FlexxAgent encrypts the value as soon as FlexxAgent starts or tries to transmit information. You can use a site like https://www.base64encode.org/ to create the base64-encoded password string.

> **INFO**
>
> Taking into account that FlexxAgent triggers a process at the system level (FlexxAgent.exe) and another at the session level (FlexxAgent Analyzer.exe), and depending on how the proxy acts at one level or the other, it may be necessary to apply different configurations to both processes by defining the `Proxy Type`. This can be done from the FlexxAgent Settings, in `Products`.

# Update

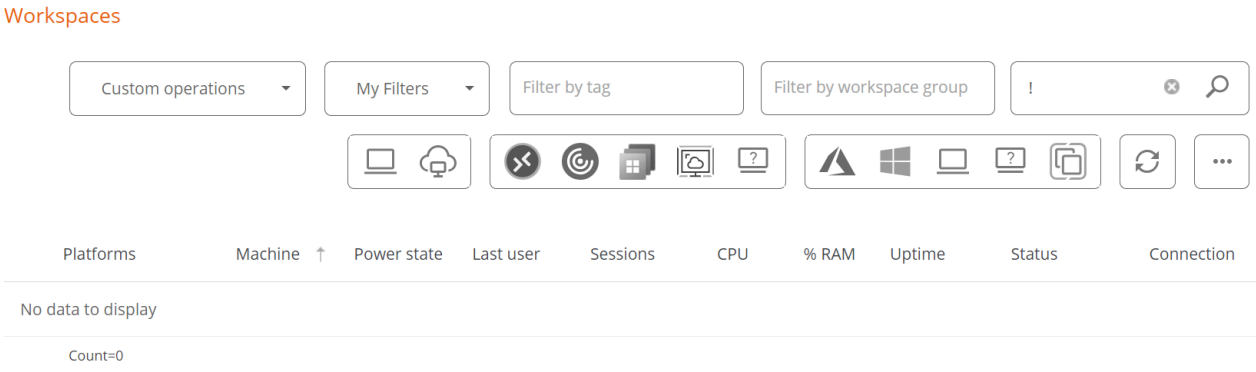
FlexxAgent can be updated automatically or manually from Workspaces.

## Auto update

This functionality is controlled with settings that are usually enabled in Workspaces. The path to view or change the configuration of this functionality is `Workspaces` -> `Level 3` -> `Settings` -> `Auto update`. Selecting `True` will allow a new version of FlexxAgent to be detected and sent automatically to all active devices in the organization. This action will leave a `Job` in Workspaces with all the operation details.

## Manual Update

The path to manually update FlexxAgent is `Level 1` -> `Workspaces` -> `Operations` -> `FlexxAgent` -> `Update to latest version`.




The different installed versions are in the dropdown option for `My filters` -> `Predefined filters` -> `FlexxAgent version summary`. This will generate a view of all devices grouped by the FlexxAgent version.

Once the update operation is executed, a `Job` with all the details of the operation will be generated in the corresponding section.

# Logs

FlexxAgent can generate three types of logs:

- Installation and update logs
- FlexxAgent Analyzer logs
- FlexxAgent service logs

These records allow consulting information and diagnosing problems from the installation of FlexxAgent.

## Installation and update logs

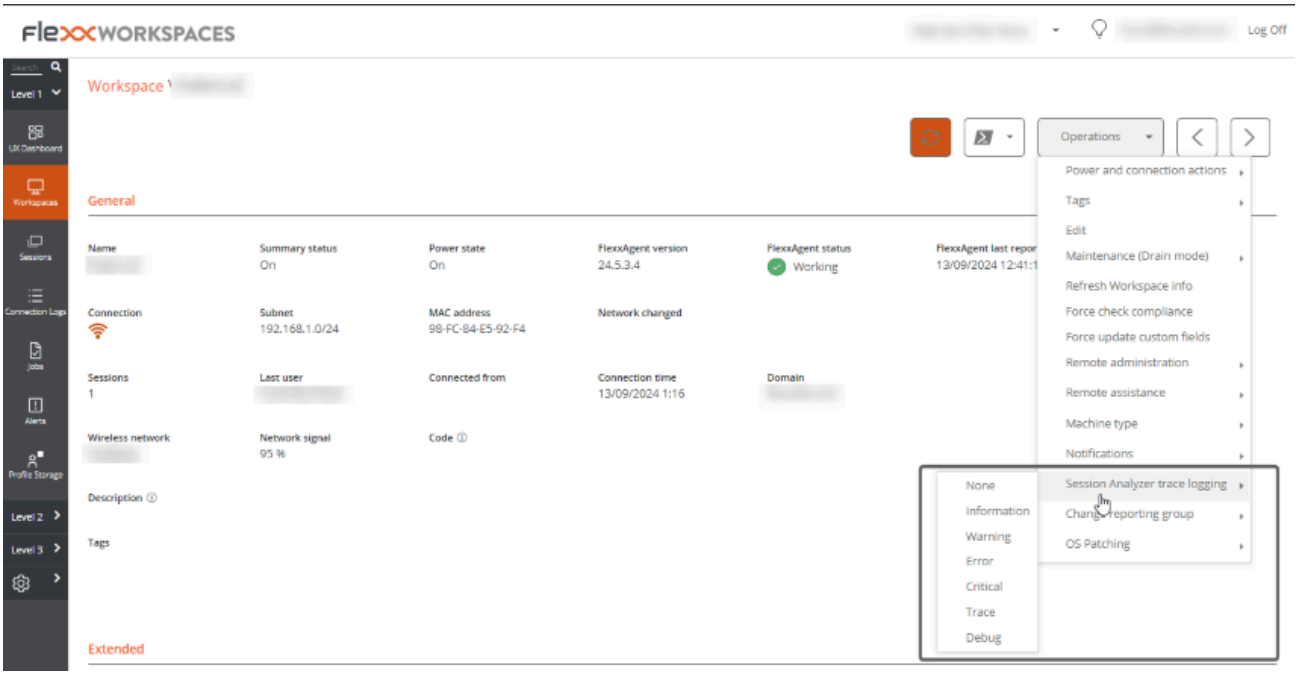
A text log file is left in the `C:\Windows\Temp\Flexxible` folder, containing information about the installation or update process, as well as dependency information and process details.

## FlexxAgent Analyzer logs

FlexxAgent Analyzer logs are stored in the `%LOCALAPPDATA%\FAAgent\Logs` directory. These can be configured to include or not include information by levels of criticality.

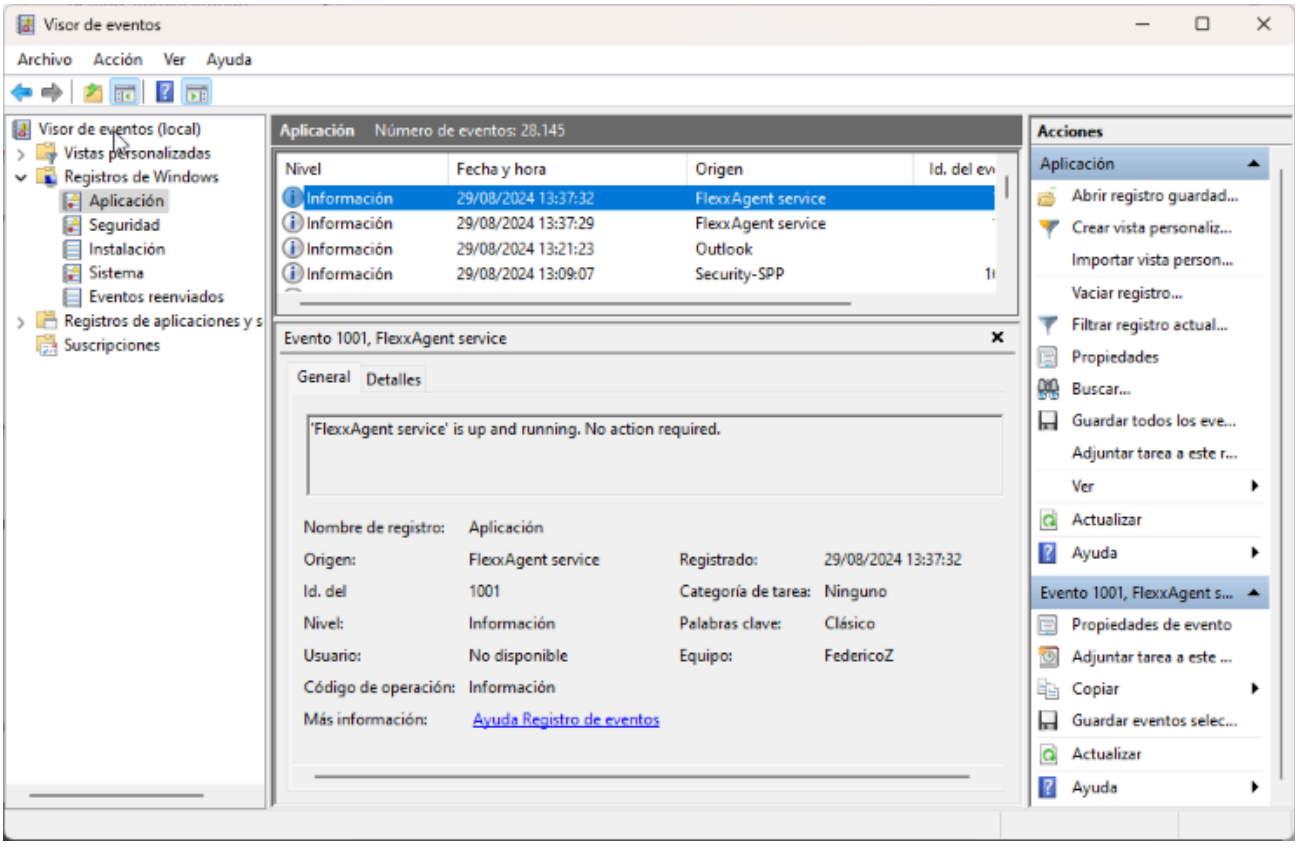
#### Change log level for FlexxAgent Analyzer

From Workspaces, it is possible to change the log level for one or more devices through the options available in the `Operations` button.



## FlexxAgent service logs

FlexxAgent service logs can be consulted in the `Application` branch, within the `Event Viewer` of Windows.




# Information obtained from the device

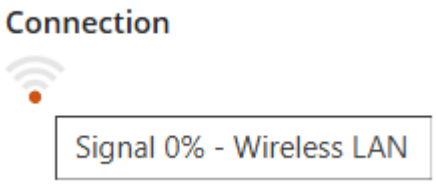
FlexxAgent collects data locally from the device and sends it to the service consoles.

## General information

- **Name**: device name
- **Device status**: power status of the device. It can be *On*, *Off*, or *Not reporting*.
- **Summary Status**: if the device status is *Off*, it can indicate whether it is *In Maintenance* or just *Off*. If the device status is *Not Reporting*, it can indicate whether the reason is *Unknown*.
- **FlexxAgent Version**: version number of FlexxAgent installed on the device

- **FlexxAgent Status**: *Running* or *Stopped*
- **Last FlexxAgent report**: date and time of the last FlexxAgent report on the device. This date might not be recent if the FlexxAgent service is stopped or the device is off.
- **Connection type**: indicates whether the device is connected by *Wi-Fi*, *Mobile network*, *Ethernet*, or *Unknown*.

> **INFO**
>
> When the connection is made through a wireless LAN network, a message may appear indicating that the device has a 0% signal or that FlexxAgent is not sending reports. This occurs because the Windows location service is disabled on the device. Please check this link to learn how to enable it.




- **Network**: device network addressing and public IP for internet access. These networks are created automatically when more than four devices are connected to the same network.
- **Subnet**: device's network addressing
- **MAC Address**: unique identifier of the device's network card
- **Network changed**: date and time of the last network change
- **Sessions**: number of user sessions established on the device
- **Last User**: last user connected to the device in domain\account format
- **Connected from**: when the selected device is a VDI or similar, it shows the name of the device from which the virtual device is accessed.
- **Connection time**: session start date and time
- **Domain**: domain to which the device belongs
- **Code**: this field lets users identify the workspace with a personal code. This code must be manually filled in individually using the Edit option in the Operations menu of the workspace details.
- **OU**: organizational unit in the domain where the device's account resides

- **Description**: allows the user to identify the device with a personal description. This field must be assigned manually and individually using the Edit option in the Operations menu of the device details.

## Extended Info

- **RAM**: total amount of RAM available
- **Cores**: number of processor cores
- **IP address**: device IP address on the local network
- **OS**: type of operating system
- **Operating system**: operating system version
- **OS Build**: operating system build number
- **Uptime**: time the device has been running since it was last started or rebooted. If fastboot is enabled, the device is only off when it is restarted.
- **Inactive Time**: indicates the time elapsed since the last input event was received in the FlexxAgent user session. Displays 0 if the user is effectively using any input device connected to the device.
- **Last Windows update**: date of the last application of updates on the device
- **Last boot duration**: boot duration of the last start
- **Reboot Pending**: shows if the device requires a reboot for updates.
- **Windows type**: type of Windows operating system: *Client* or *Server*
- **System Disk**: amount of free disk space compared to the total capacity
- **Public IP of ISP**: the ISP is obtained using the public IP. It might not be accurate if connected to a corporate network or using a VPN.
- **Region**: obtained using the public IP. It might not be accurate if connected to a corporate network or using a VPN.
- **Broker type**: if detected, shows the broker in use.
- **Hypervisor**: if virtualization is detected, shows the hypervisor in use.
- **Delivery Group**: for VDIs, shows the delivery group to which the device belongs.
- **Subscription / Broker**: Microsoft Azure or Citrix service that manages user connections to the device
- **Registration Status**: indicates the registration status of the virtual device.

- **Maintenance Mode**: indicates whether the maintenance mode of the virtual device is *On* or *Off*.
- **Virtual Machine Type**: indicates the type of virtual device.
- **Session Analyzer**: indicates whether or not it is configured to launch Session Analyzer in all the user sessions.
- **Session Analyzer version**: Session Analyzer version number
- **Report group**: report group to which the device belongs
- **BIOS Manufacturer**: name of the device's firmware manufacturer
- **BIOS Version**: version of the device firmware
- **SMBIOS Version**: System Management BIOS version of the device
- **BIOS Serial Number**: unique number assigned to the device by its manufacturer. Available only if the manufacturer decided the device needed one.
- **Google Chrome Version**: Google Chrome build number, if installed.
- **Microsoft Edge Version**: Microsoft Edge build number, if installed.

## Information in tabs

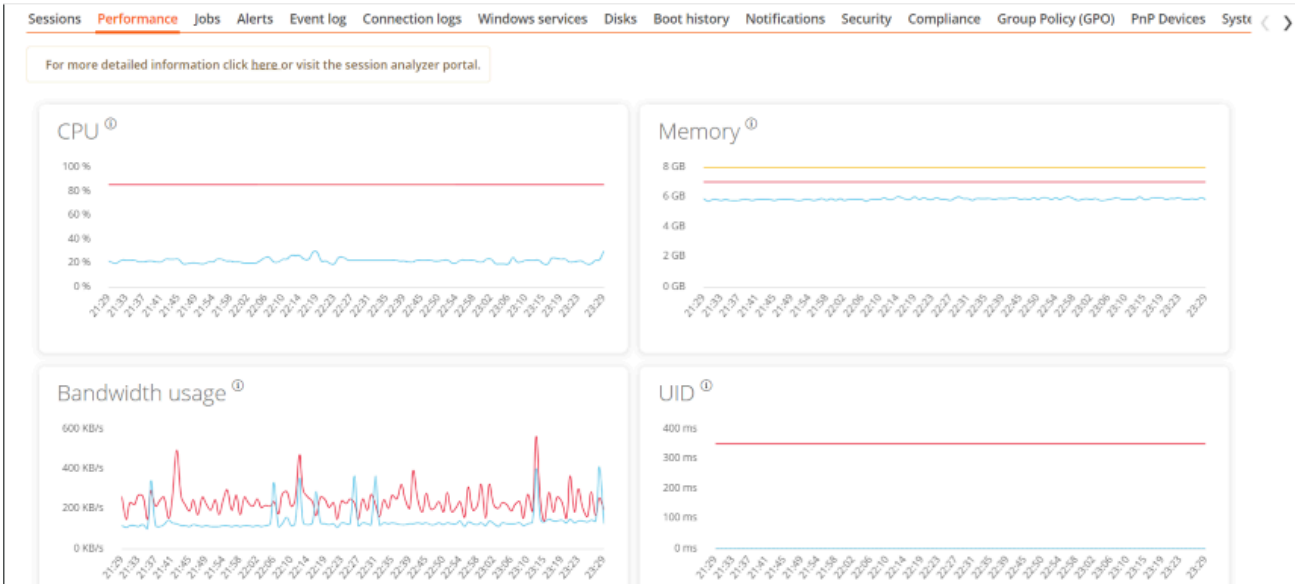
FlexxAgent groups information about the following aspects of the device:

#### Sessions

Displays a table with the log of user sessions established on the device and timely information about the session type, connection status, or start date.

#### Performance

Displays charts of the main performance counters of the device, based on data collected during the last two hours. The following are included:

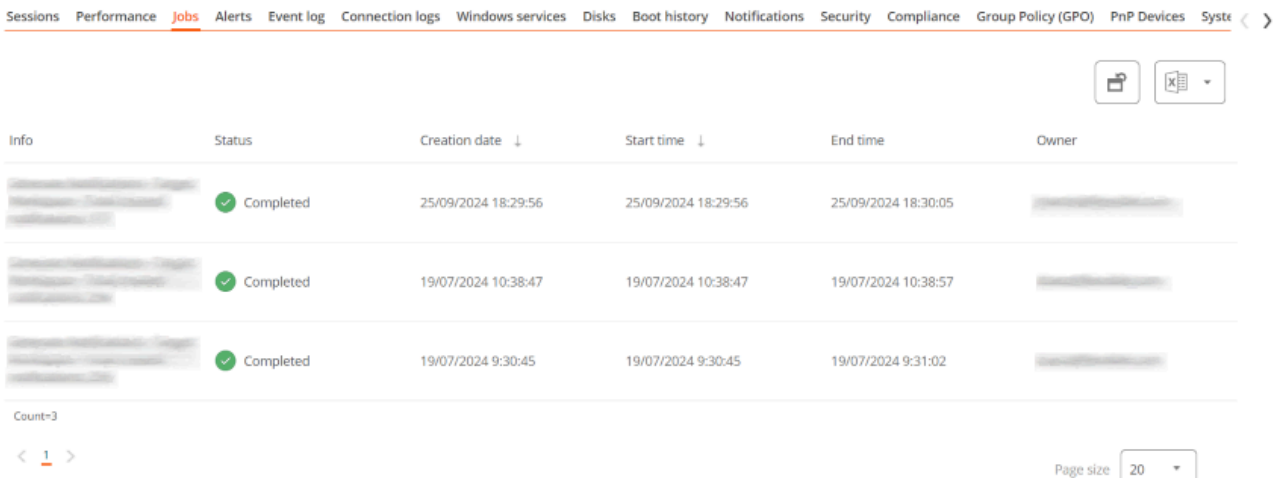



- **CPU**: processor usage percentage
- **Memory**: amount of memory used and available
- **Bandwidth Usage**: amount of incoming and outgoing traffic
- **UID**: user input delay. Refers to the time lapse between the moment a user performs an action, such as clicking a mouse button or pressing a key, and the moment the corresponding response is displayed on the screen or executed.
- **Connection Signal**: signal reception percentage when the device connects via a wireless method.

At the top, a link allows access to the Analyzer module.

#### Jobs

All actions performed from the Workspaces module on one or more devices are audited in the Jobs queue. This tab allows you to check the work done for the active device.




### Alert

Presents a table with the list of all active alerts on the device. When an alert is logged, a notice is displayed at the top of the page.

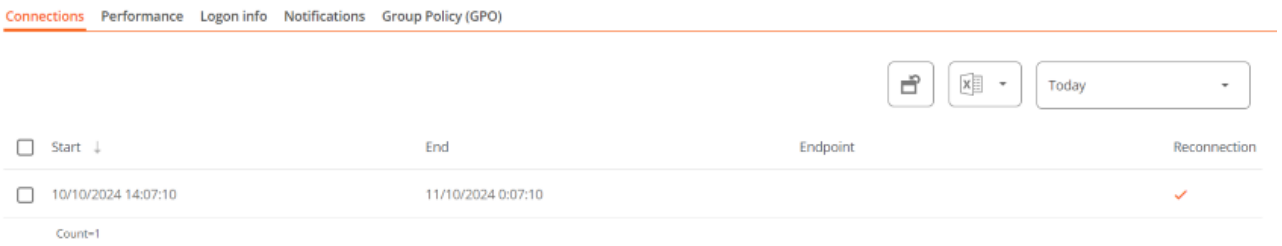

### Event Logs

Information about events present on the device. By default, errors are filtered and only those with severity level *Error* or *Critical* are shown. FlexxAgent obtains this information at 10-minute intervals.

Using the options available in the configuration, you can modify the sampling time or include events by their ID.

### Connection log

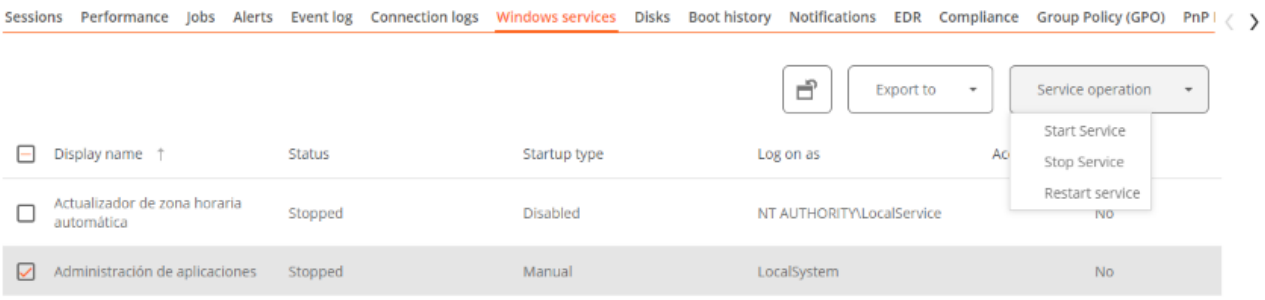
Presents a list of the connections established with the device, including each instance where a user logs in or reconnects a previously disconnected session.




The session end date is recorded only for sessions that have been disconnected or closed. While the session remains active, this field will remain empty.

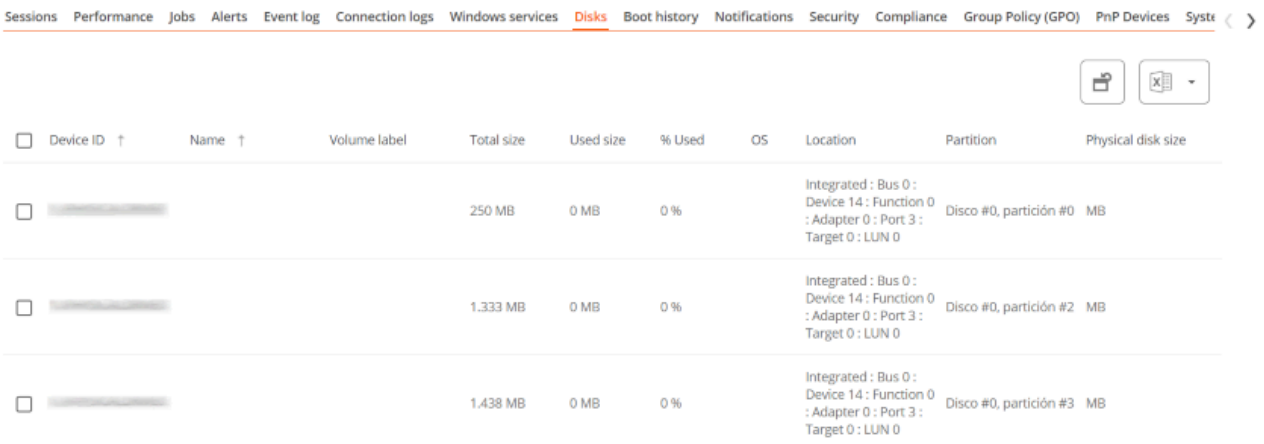
#### Windows services

This option shows the status of services and executes start, restart, or stop operations for Windows services.



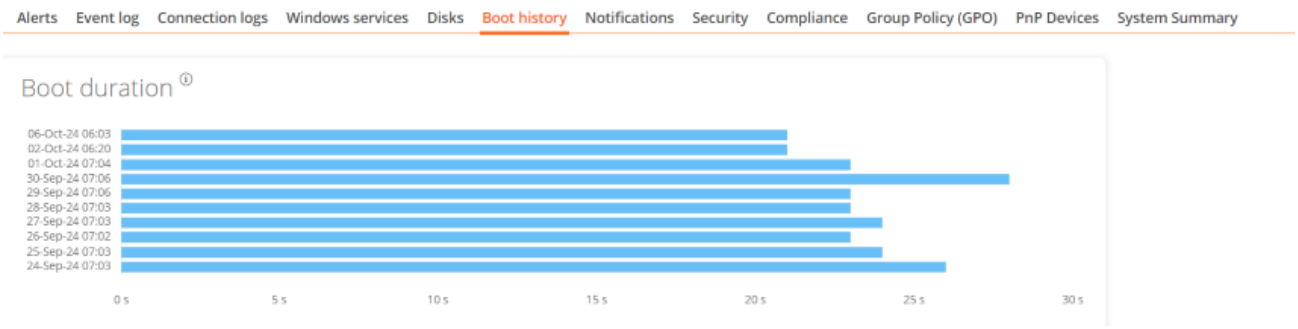

#### Disks

Displays a list of all partitions present on the disks identified in the system, as well as statistics of their capacity and occupancy levels.



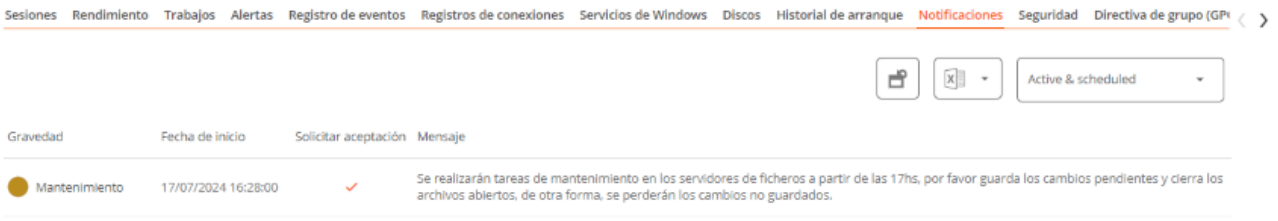

#### Boot history

Displays a graph on the duration of the last ten device boots.



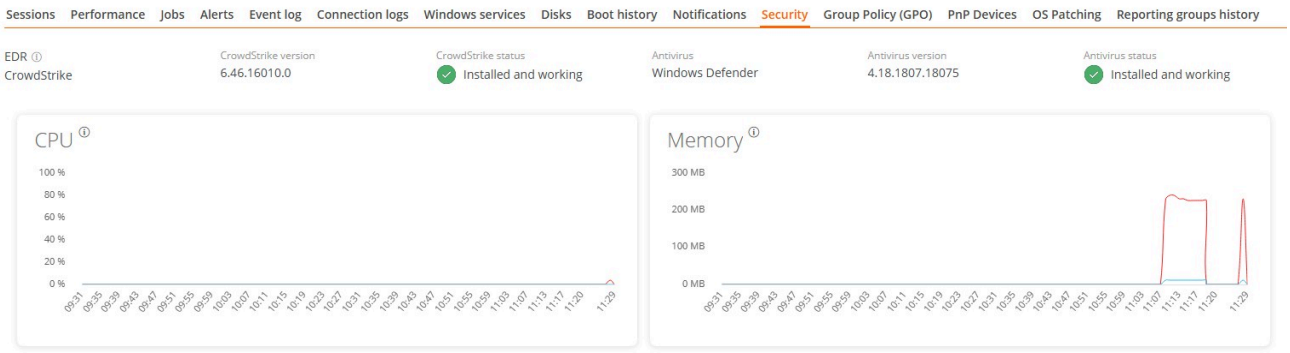

### Notifications

Allows you to see if the device has any active notification. When there is one, a message is displayed at the top of the page.




### Security

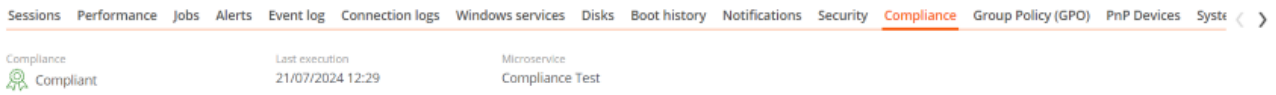
From this section you can check the name of the antivirus installed on the device, as well as its version number, execution status, and a graph of its RAM and CPU usage. The same information will be displayed if FlexxAgent detects CrowdStrike as Endpoint Detection and Response (EDR).



> **INFO**
>
> Antivirus detection is automatic only on the Windows Client operating system (Windows 7 or later versions). On Windows Server, only Bitdefender and Windows Defender are detected, and these are the only ones that will show RAM and CPU usage.

#### Compliance

Allows viewing the status of the compliance policy configured for the active device. To update this field on demand, click `Operations` -> `Enforce compliance`.

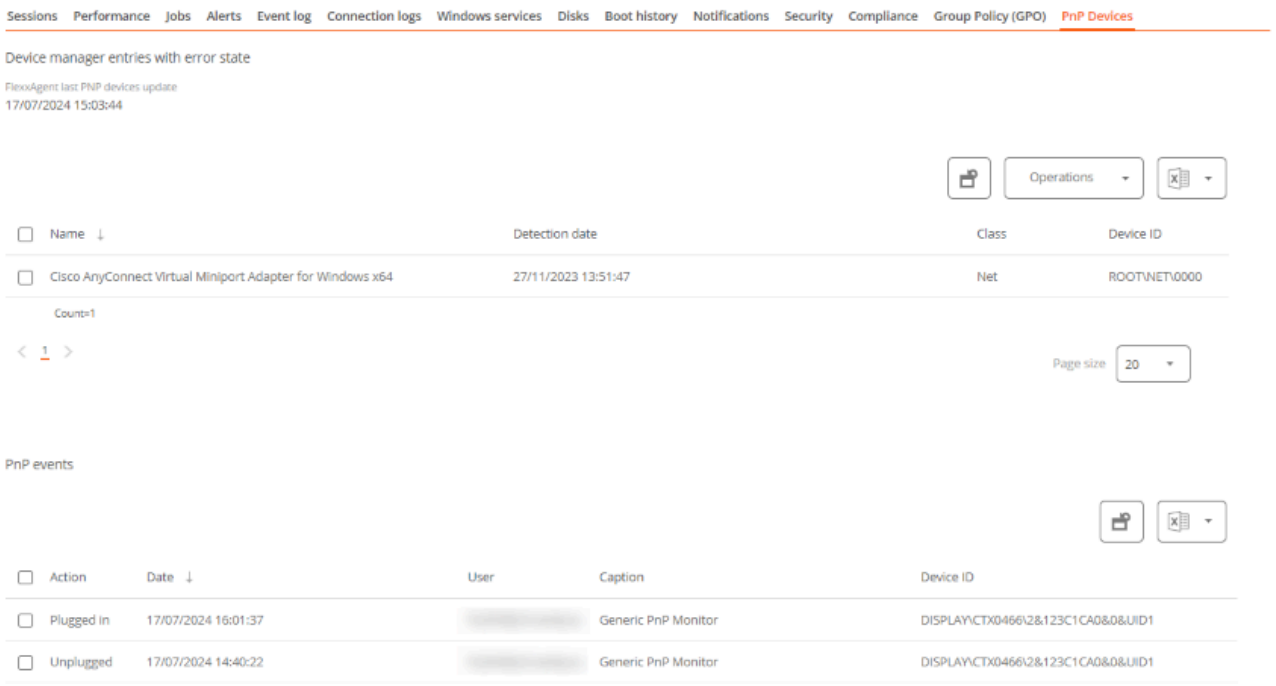



#### Group Policy (GPO)

Displays information about group policies applied on the active device. Allows you to see the names of the policies as well as the check time.

#### PnP Devices

Shows Plug and Play (PnP) devices that are in an error state, which may be due to hardware failures or incorrect driver or device configuration.




At the bottom of this view, there is a table that records all events related to PnP devices, generating an entry each time a peripheral is connected or disconnected.

**System Summary**

Shows system information for Windows devices. Includes:

| Field | Detail |
|---|---|
| OSVersion | Operating system version number |
| OtherOSDescription | Additional description of the current operating system version (optional) |
| OSManufacturer | Nombre del fabricante del sistema operativo. In the case of Windows-based systems, this value is "Microsoft Corporation" |
| SystemModel | Product name given by a manufacturer to a piece of equipment |

| Field | Detail |
| --- | --- |
| SystemType | System running on the Windows-based equipment |
| SystemSKU | Stock keeping unit (SKU) product information (optional) |
| Processor | Name, number of cores, and number of logical processors of the processor |
| BIOSReleaseDate | BIOS Release Date |
| EmbeddedControllerVersion | Primary and secondary firmware versions of the embedded controller, separated by "." |
| BaseBoardManufacturer | Name of the organization responsible for manufacturing the physical device |
| BaseBoardProduct | Manufacturer-defined part number for the motherboard |
| BaseBoardVersion | Version of the physical device |
| PlatformRole | Type of chassis where Unspecified = 0, Desktop = 1, Mobile = 2, Workstation = 3, EnterpriseServer = 4, SOHOServer = 5, AppliancePC = 6, PerformanceServer = 7, MaximumValue = 8 |
| WindowsDirectory | Operating system's Windows directory |
| SystemDirectory | Operating system's system directory |
| BootDevice | Name of the disk drive from which the Windows operating system starts |

| Field | Detail |
| --- | --- |
| Locale | Name Identifier of language used by the operating system |
| TimeZone | Name of the operating system time zone |
| PageFileSpace | Actual amount of disk space allocated for use as a page file, in megabytes |
| PageFile | Name of the page file |
| BIOSMode | Device boot mode (BIOS or UEFI) |
| SecureBootState | Secure boot mode status (Off, On) |

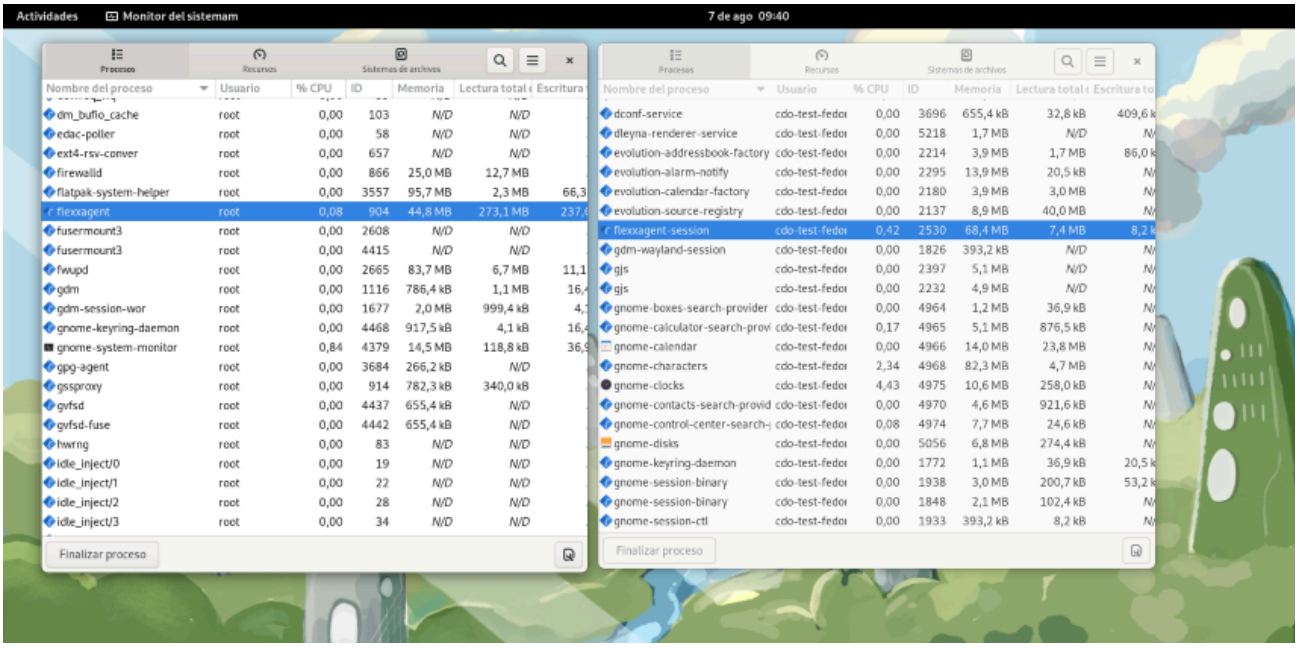
**Reporting groups history**

Allows you to see which reporting groups the device belongs to, the date of incorporation, and if it has been assigned to the group manually or automatically.

# FlexxAgent / Supported Systems / Linux

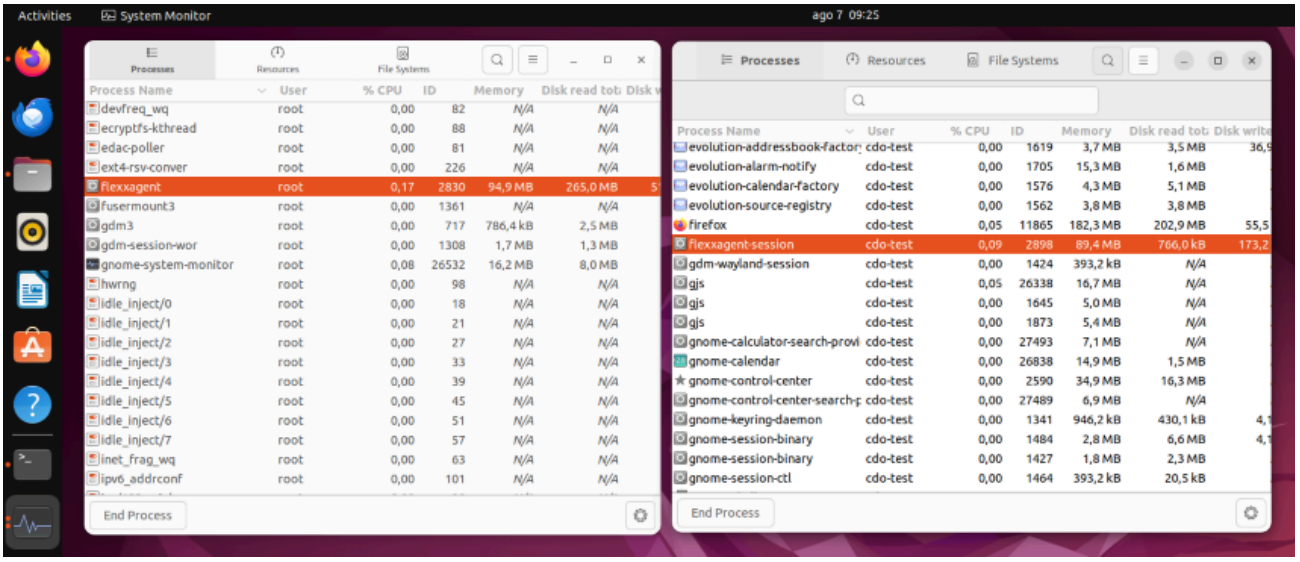
The Linux agent allows the inclusion of devices with this operating system in the service consoles, enabling support teams to have complete visibility of all devices in use within the organization.

Linux support includes distributions like Fedora, Debian, and its derivative, Ubuntu. Both physical and virtual devices on VMware as a hypervisor and VDIs published with Citrix as a broker are supported.




FlexxAgent is composed of a process of the same name, which runs at the system level and obtains all device information: its consumption metrics, performance, and all information visible in the consoles related to the device.

FlexxAgent-Session initiates an instance for each user session on the device. It gathers information about the session, such as the applications in use and their consumption, system resource usage by the session, and session delivery times.




# Supported versions

FlexxAgent supports the following distributions and versions:

- Fedora 37 or later
- Debian/GNU Linux 11 (bullseye) or later
- Ubuntu 22.04, 24.04

More distributions are regularly validated.

To include a distribution in the list of supported distributions, please contact Flexxible.

# Requirements

Before installing, updating all system packages is recommended. The necessary components will be installed, depending on the distribution.

Package dependencies for Fedora and Debian:

- dmidecode
- imvirt
- systemd

# Limitations

Certain functionalities are unavailable for Linux, such as remote assistance, user microservices, flow execution, the collection of plug-and-play peripheral data, and proxy use.

The on-demand execution of microservices from Workspaces supports Bash as a scripting language.

# Proxy Configuration

FlexxAgent for Linux supports communication through authenticated and unauthenticated proxies. The proxy information must be provided to Flexxible to include it in the configuration file mentioned in the next point.

Required data:

- For unauthenticated proxy, it will be necessary to provide `URL` and `Port`.
- For authenticated proxies, `User` and `Password` must be added to the above.

# Download and installation

To install FlexxAgent, you must run the installation script using a preset configuration file.

## Installation Scripts

Path to download the installation script on **Ubuntu/Debian**:

> `https://update.workspaces.flexxible.com/agents/FlexxAgent/latest/debian/x64/flexxagent-install.sh`

Path to download the installation script on **Fedora**:

> `https://update.workspaces.flexxible.com/agents/FlexxAgent/latest/fedora/x64/flexxagent-install.sh`

FlexxAgent downloads its latest version when the script is executed before installation.

The configuration file is required for the installation. It can be obtained by contacting Flexxible.

## Installation steps

1. Download the installer from the URL.
2. Grant permissions to the script.
   ```
   sudo chmod +x ./flexxagent-install.sh
   ```
3. Run the script.
   ```
   sudo ./flexxagent-install.sh -c [configuration file]
   ```
4. Clean the files used.

## Installation script parameters

| Parameter | Caption |
| --- | --- |
| `-v,--version <VERSION>` | Use a specific version, by default `latest`. |
| `-d,--distro <DISTRO>` | The script automatically detects the DISTRO in use on the system it is running on. This parameter helps force the FlexxAgent version installation for a specific DISTRO when working with derived or similar distros. |
| `--verbose,-Verbose` | Displays diagnostic information. |
| `-c,--config <CONFFILE>` | Applies the configuration from a configuration file by default, `settings.conf`. |

| Parameter | Caption |
| --- | --- |
| `-o, --offline` | Installs FlexxAgent from a given package file, instead of downloading it. Please check the Offline installation section for more details. |
| `-?,--?,-h,--help,-Help` | Shows help. |

## Examples

Install FlexxAgent with the configuration file:

> `flexxagent-install.sh [-c|--config <path/file.conf>]`

Install a specific version of FlexxAgent:

> `flexxagent-install.sh [-v|--version <VERSION>]`

Force the FlexxAgent installation for a specific distribution:

> `flexxagent-install.sh [-d|--distro <DISTRO>]`

Access the help:

> `flexxagent-install.sh -h|-?|--help`

# Offline installation

Offline installation is available if there is some networking restriction in your environment. To perform an offline installation, please ask your contact at Flexxible how to obtain the package and installer for your distribution.

#### Installation packages provided according to the distribution

> Debian: `flexxagent.deb`

> Fedora: `flexxagent.rpm`

## Offline installation steps

1. Place the FlexxAgent package file, the configuration file, and the installation script in the same folder.
2. Grant permissions to the script:

```
sudo chmod +x ./flexxagent-install.sh
```

3. Run the script with the `-o` or `--offline` parameter and indicating the name of the package file to install:

```
sudo ./flexxagent-install.sh -c [archivo de configuración] -o [paquete de Flexxagent]
```

4. Clean the files used.

# Uninstall

The uninstallation script can be downloaded from

```
https://update.workspaces.flexxible.com/agents/Linux/FlexxAgent/latest/flexxagent-uninstall.sh
```

Steps for uninstallation:

1. Download the uninstaller from the URL.
2. Grant permissions to the script.

```
sudo chmod +x ./flexxagent-uninstall.sh
```

3. Run the script.

```
sudo ./flexxagent-uninstall.sh
```

4. Clean the files used.

## Uninstallation script parameters

| Parameter | Caption |
| --- | --- |
| `-d,--distro <DISTRO>` | The script automatically detects the DISTRO in use on the system it is running on. This parameter helps force the FlexxAgent version uninstallation for a specific DISTRO when working with derived or similar distros. |
| `-c,--cleanup <VERSION>` | Cleans configurations and logs; default is `false`. |
| `-?,--?,-h,--help,-Help` | Shows help. |

## Examples

Uninstall and clean up configurations and logs:

> `flexxagent-uninstall.sh [-c|--cleanup]`

Force the uninstallation for a DISTRO:

> `flexxagent-uninstall.sh [-d|--distro <DISTRO>]`

Access the help:

> `sudo ./flexxagent-uninstall.sh --help`

# Update

There are two ways to update FlexxAgent to its latest version:

- From Workspaces, select the device and perform: `Operations -> FlexxAgent -> Update to the latest version`.
- Re-running the installation script to download and install the latest version.

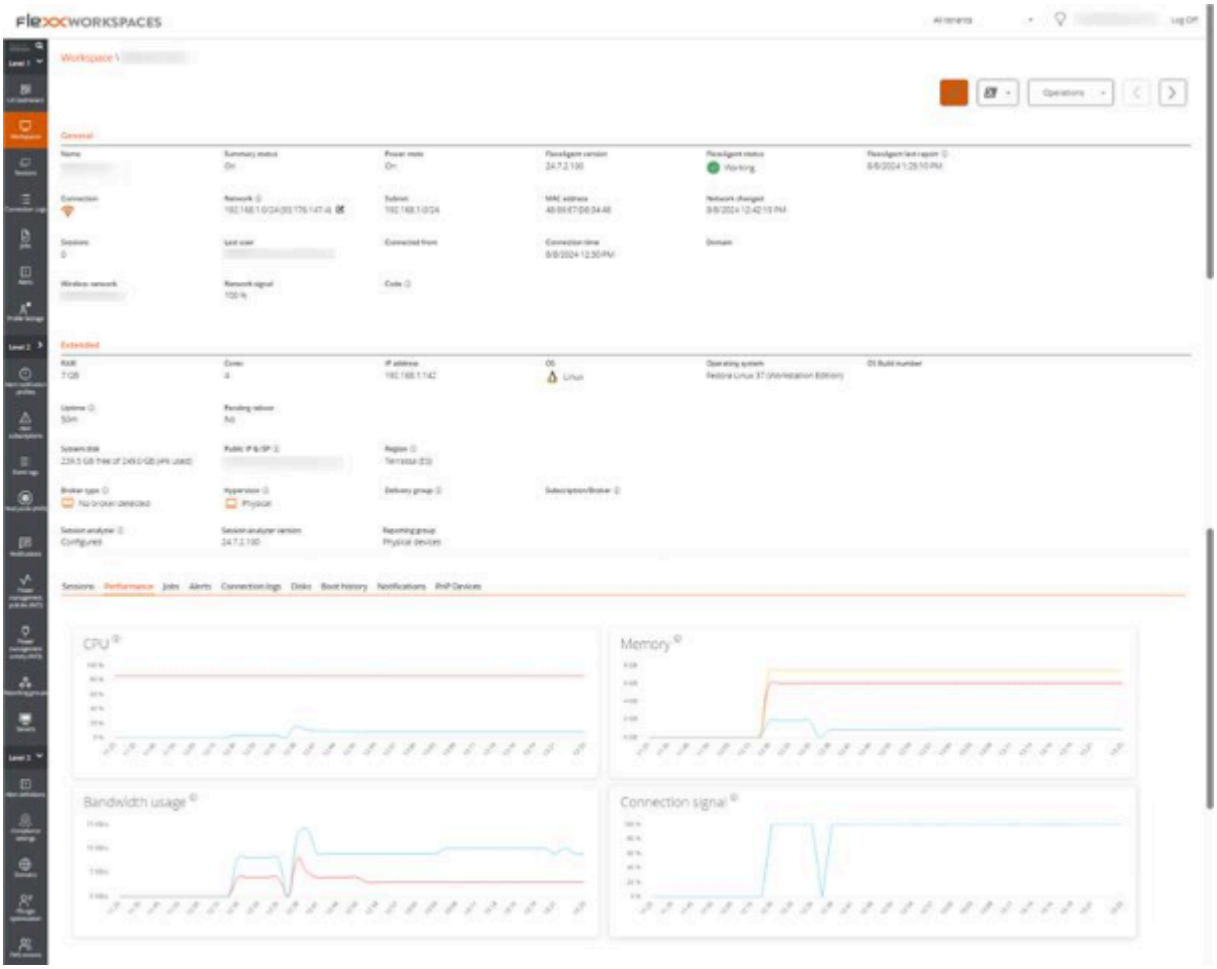
# Logs

FlexxAgent can generate two types of logs:

- FlexxAgent log (system): located in the `/var/log/flexx/` folder
- FlexxAgent Session log (user session): located in the `/home/[user]/.config/flexx/logs/` folder

# Information obtained from the device

FlexxAgent collects data locally from the device and sends it to the service consoles.




# General information

- **Name**: device name
- **Device Status**: the device's power state, it can be *On*, *Off*, or *Not reporting*.
- **FlexxAgent Version**: version number of FlexxAgent installed on the device
- **FlexxAgent Status**: *Running* or *Stopped*
- **Last FlexxAgent report**: date and time of the last FlexxAgent report on the device. This date might not be recent if the FlexxAgent service is stopped or the device is off.
- **Connection type**: indicates whether the device is connected by *Wi-Fi*, *Mobile network*, *Ethernet*, or *Unknown*.
- **Network**: device network addressing and public IP for internet access. These networks are created automatically when more than four devices are connected to the same network.
- **Network signal**: reception percentage

- **Subnet**: device's network addressing
- **MAC Address**: unique identifier of the device's network card
- **Wireless network**: network name
- **Connection Signal**: signal reception percentage when the device connects via a wireless method.
- **Network changed**: date and time of the last network change
- **Sessions**: number of user sessions on the device
- **Last User**: last user connected to the device in domain\account format
- **Connected from**: when the selected device is a VDI or similar, it shows the name of the device from which the virtual device is accessed.
- **Connection time**: session start date and time
- **Code**: this field lets users identify the workspace with a personal code. This code must be manually filled in individually using the Edit option in the Operations menu of the workspace details.
- **Description**: allows the user to identify the device with a personal description. This field must be assigned manually and individually using the Edit option in the Operations menu of the device details.

## Extended Info

- **RAM**: total available RAM capacity
- **Cores**: number of processor cores
- **IP address**: device IP address on the local network
- **OS**: type of operating system
- **Operating system**: operating system version
- **Region**: obtained using the public IP. It might not be accurate if connected to a corporate network or using a VPN.
- **Broker type**: if detected, shows the broker in use.
- **Delivery Group**: for VDIs, shows the delivery group to which the device belongs.
- **Subscription**: if detected, subscription in use for Citrix Cloud, Azure, etc.
- **Hypervisor**: if virtualization is detected, shows the hypervisor in use.

- **Session Analyzer**: indicates whether or not it is configured to launch Session Analyzer in all the user sessions.
- **Session Analyzer version**: Session Analyzer version number
- **Report group**: report group to which the device belongs

## Information in tabs

FlexxAgent groups information about the following aspects of the device:

#### Sessions

Displays a table with the log of user sessions established on the device and timely information about the session type, connection status, or start date.

#### Performance

Displays charts of the main performance counters of the device, based on data collected during the last two hours. The following are included:

- **CPU**: processor usage percentage
- **Memory**: amount of memory used and available
- **Bandwidth Usage**: amount of incoming and outgoing traffic

At the top, a link allows access to the Analyzer module.

#### Jobs

All actions performed from the Workspaces module on one or more devices are audited in the Jobs queue. This tab allows you to check the work done for the active device.

#### Alert

Presents a table with the list of all active alerts on the device. When an alert is logged, a notice is displayed at the top of the page.


#### Connection log

Presents a list of the connections established with the device, including each instance where a user logs in or reconnects a previously disconnected session.

The session end date is recorded only for sessions that have been disconnected or closed. While the session remains active, this field will remain empty.

#### Disks

Displays a list of all partitions present on the disks identified in the system, as well as statistics of their capacity and occupancy levels.

#### Notifications

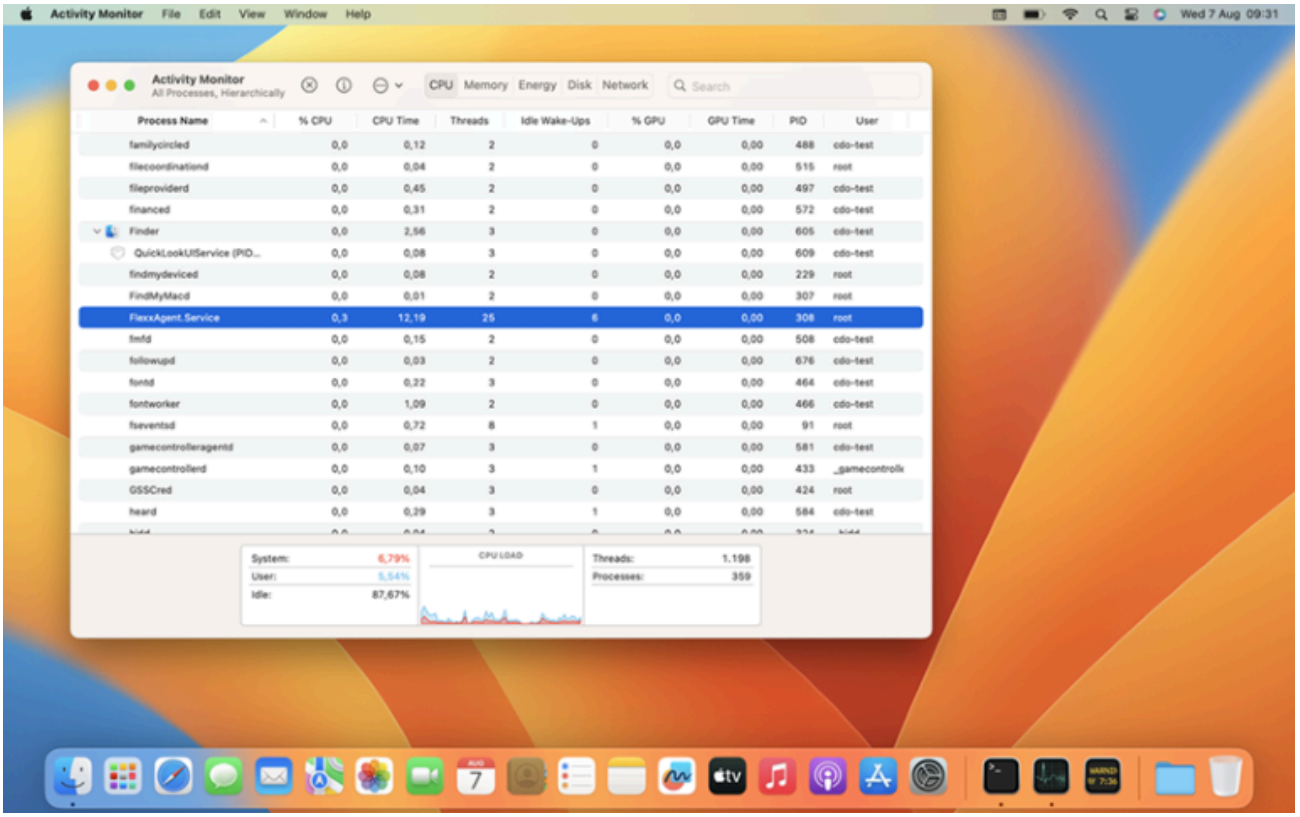
Allows you to see if the device has any active notification. When there is one, a message is displayed at the top of the page.

#### Reporting groups history

Allows you to see which reporting groups the device belongs to, the date of incorporation, and if it has been assigned to the group manually or automatically.

# FlexxAgent / Supported Systems / macOS

The macOS agent allows Mac devices to be included in the service consoles, enabling support teams to see all devices used within the organization.




## Supported versions

Support for macOS includes version Monterey 12 and later. Regarding architectures, FlexxAgent supports both Intel processors (amd64 architecture) and Apple processors with arm architecture (arm64).

## Limitations

Certain features are not available for macOS, such as remote assistance, the execution of on-demand microservices from Workspaces or user microservices and flows, or the sending of notifications.

Due to how the operating system functions, the expected behavior on macOS is that when the device screen is locked, the operating system stops background processes, causing the device to stop reporting information to the consoles or receiving actions until the screen is unlocked or the session is started again.

# Proxy Configuration

FlexxAgent for macOS supports communication through both authenticated and unauthenticated proxies. The proxy information must be provided to Flexxible to include it in the configuration file mentioned in the next point.

Required data:

- For unauthenticated proxy, it will be necessary to provide `URL` and `Port`.
- For authenticated proxies, `User` and `Password` must be added to the above.

# Download and installation

To install FlexxAgent, you must run the installation script using a preset configuration file.

## Installation Scripts

Path to download the installation script for **x64 architecture**:

> `https://update.workspaces.flexxible.com/agents/FlexxAgent/latest/macos/x64/flexxagent-install.sh`

Path to download the installation script for **ARM architecture**:

> `https://update.workspaces.flexxible.com/agents/FlexxAgent/latest/macos/arm64/flexxagent-install.sh`

The configuration file is required for the installation. It can be obtained by contacting Flexxible.

## Installation steps

1. Download the installer from the URL.
2. Grant permissions to the script, open the terminal, and execute:
   > `sudo chmod +x ./flexxagent-install.sh`
3. Run the script.
   > `sudo ./flexxagent-install.sh -c [configuration file]`
4. Clean files.

## Installation script parameters

| Parameter | Caption |
|---|---|
| `-v,--version <VERSION>` | Use a specific version, by default, `latest`. |
| `--verbose,-Verbose` | Displays diagnostic information. |
| `-c,--config <CONFFILE>` | Applies the configuration from a configuration file by default `settings.conf`. |
| `-o, --offline` | Installs FlexxAgent from a given package file, instead of downloading it. Please check the Offline installation section for more details. |
| `-?,--?,-h,--help,-Help` | Shows help. |

## Examples

Install FlexxAgent with the configuration file:

> `flexxagent-install.sh [-c|--config <path/file.conf>]`

Install a specific version of FlexxAgent:

> `flexxagent-install.sh [-v|--version <VERSION>]`

Access the help:

> `flexxagent-install.sh -h|-?|--help`

# Offline installation

Offline installation is available if there is some networking restriction in your environment. To perform an offline installation, please ask your contact at Flexxible how to obtain the package and installer for your macOS device (ARM or x64).

The package file will be provided in ".pkg" format.

## Offline installation steps

1. Place the FlexxAgent package file, the configuration file, and the installation script in the same folder.
2. Allow the Terminal application to access the disk where the files are located:

- Go to `System preferences` -> `Security and Privacy` -> `Privacy`.
- Select `Full disk access`.
- Add the Terminal application to the list.
- Close the Terminal application i it was running and open a new one.

3. Go to the folder where the FlexxAgent files are located, and grant permissions to the script:

> `sudo chmod +x ./flexxagent-install.sh`

4. Run the script with the `-o` or `--offline` parameter:

> `sudo ./flexxagent-install.sh -c [archivo de configuración] -o [paquete de Flexxagent]`

5. Clean the files used.

# Uninstall

The uninstallation script can be downloaded from

> `https://update.workspaces.flexxible.com/agents/MacOS/FlexxAgent/latest/flexxagent-uninstall.sh`

Steps for uninstallation:

1. Download the uninstaller from the URL.
2. Grant permissions to the script.
   > `sudo chmod +x ./flexxagent-uninstall.sh`
3. Run the script.
   > `sudo ./flexxagent-uninstall.sh`

## Uninstallation script parameters

| Parameter | Caption |
|---|---|
| `-c,--cleanup <VERSION>` | Cleans configurations and logs; default is `false`. |
| `-?,--?,-h,--help,-Help` | Shows help. |

## Examples

Uninstall and clean up configurations and logs:

> `flexxagent-uninstall.sh [-c|--cleanup]`

Access the help:

```
sudo ./flexxagent-uninstall.sh --help
```

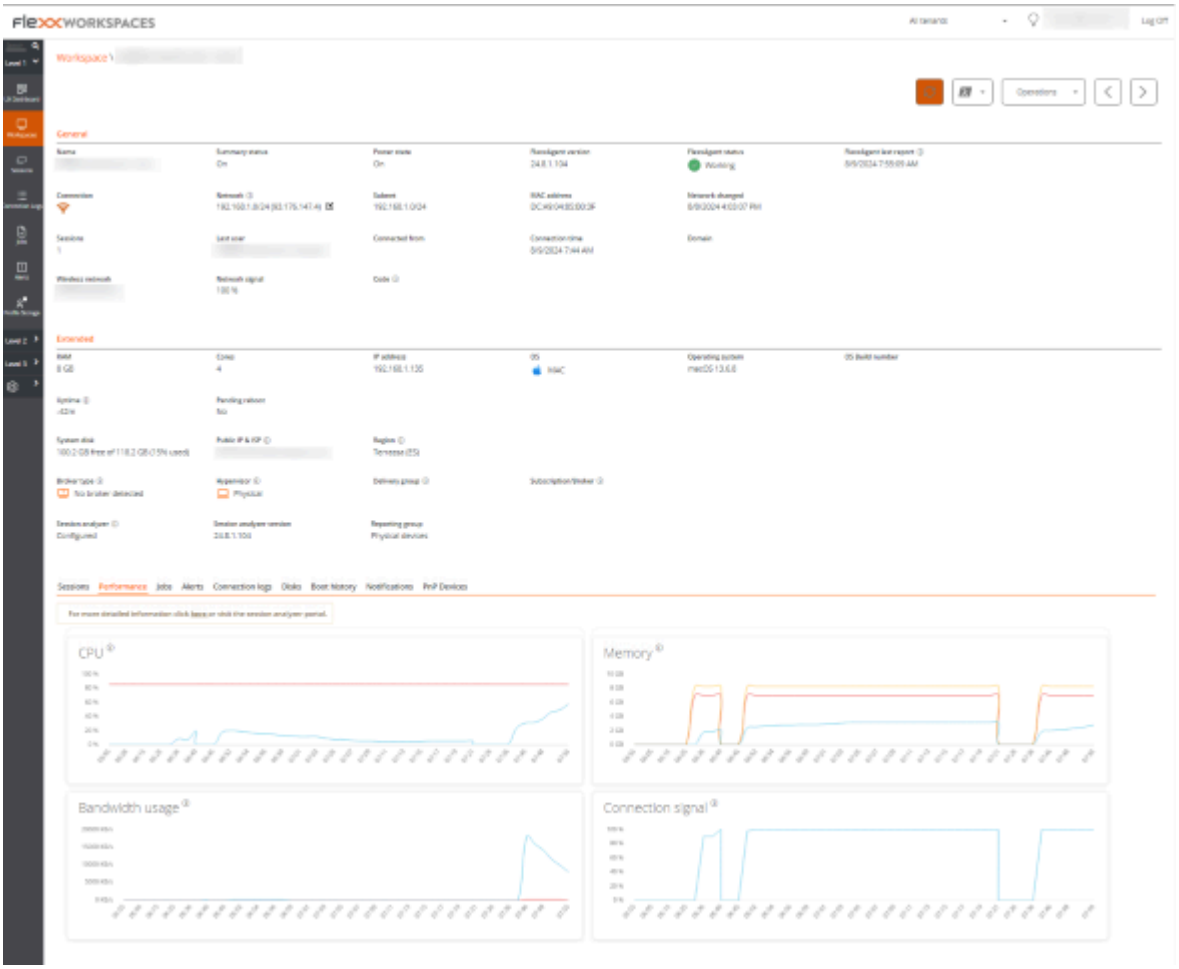
# Update

The agent can be updated to the latest version in two ways:

- From Workspaces, select the device and perform: `Operations -> FlexxAgent -> Update to the latest version`.
- Re-running the installation script to download and install the latest version.

# Information obtained from the device

FlexxAgent collects data locally from the device and sends it to the service consoles.



# General information

- **Name**: device name
- **Device Status**: the device's power state, it can be *On*, *Off*, or *Not reporting*.
- **FlexxAgent Version**: version number of FlexxAgent installed on the device
- **FlexxAgent Status**: *Running* or *Stopped*
- **Last FlexxAgent report**: date and time of the last FlexxAgent report on the device. This date might not be recent if the FlexxAgent service is stopped or the device is off.
- **Connection type**: indicates whether the device is connected by *Wi-Fi*, *Mobile network*, *Ethernet*, or *Unknown*.
- **Network**: device network addressing and public IP for internet access. These networks are created automatically when more than four workspaces are connected to the same network.
- **Network signal**: reception percentage
- **Subnet**: device's network addressing
- **MAC Address**: unique identifier of the device's network card
- **Wireless network**: network name
- **Connection Signal**: signal reception percentage when the device connects via a wireless method.
- **Network changed**: date and time of the last network change
- **Sessions**: number of user sessions on the device
- **Last User**: last user connected to the device in domain\account format
- **Connected from**: when the selected device is a VDI or similar, it shows the name of the device from which the virtual device is accessed.
- **Connection time**: session start date and time
- **Code**: this field lets users identify the workspace with a personal code. This code must be manually filled in individually using the Edit option in the Operations menu of the workspace details.
- **Description**: allows the user to identify the device with a personal description. This field must be assigned manually and individually using the Edit option in the Operations menu of the device details.

# Extended Info

- **RAM**: total available RAM capacity
- **Cores**: number of processor cores
- **IP address**: device IP address on the local network
- **OS**: type of operating system
- **Operating system**: operating system version
- **Region**: obtained using the public IP. It might not be accurate if connected to a corporate network or using a VPN.
- **Session Analyzer**: indicates whether or not it is configured to launch Session Analyzer in all the user sessions.
- **Session Analyzer version**: Session Analyzer version number
- **Report group**: report group to which the device belongs

# Information in tabs

FlexxAgent groups information about the following aspects of the device:

#### Sessions

Displays a table with the log of user sessions established on the device and timely information about the session type, connection status, or start date.

#### Performance

Displays charts of the main performance counters of the device, based on data collected during the last two hours. The following are included:

- **CPU**: processor usage percentage
- **Memory**: amount of memory used and available
- **Bandwidth Usage**: amount of incoming and outgoing traffic

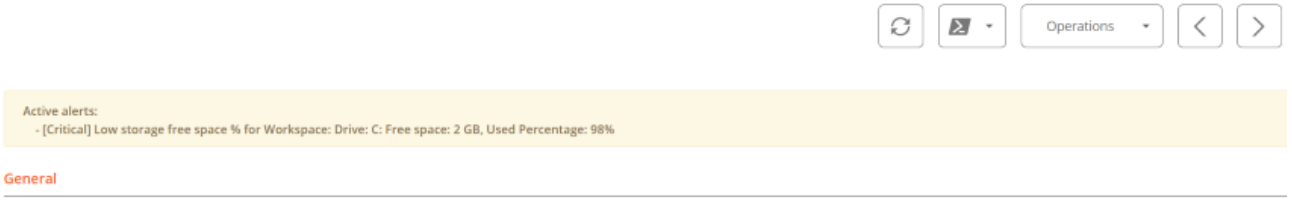
At the top, a link allows access to the Analyzer module.

#### Jobs

All actions performed from the Workspaces module on one or more devices are audited in the Jobs queue. This tab allows you to check the work done for the active device.

**Alert**

Presents a table with the list of all active alerts on the device. When an alert is logged, a notice is displayed at the top of the page.




**Connection log**

Presents a list of the connections established with the device, including each instance where a user logs in or reconnects a previously disconnected session.

The session end date is recorded only for sessions that have been disconnected or closed. While the session remains active, this field will remain empty.

**Disks**

Displays a list of all partitions present on the disks identified in the system, as well as statistics of their capacity and occupancy levels.

**Notifications**

Allows you to see if the device has any active notification. When there is one, a message is displayed at the top of the page.

**Reporting groups history**

Allows you to see which reporting groups the device belongs to, the date of incorporation, and if it has been assigned to the group manually or automatically.

# FlexxAgent / Supported Systems / ChromeOS

The ChromeOS agent allows the inclusion of devices with this operating system in the service consoles, thus enabling complete visibility for support teams, both desktop and mobile devices of users.

## Requirements

To deploy FlexxAgent on Chrome devices, it is necessary to have a mobile device management (MDM) platform, such as Google Admin, which allows centralized distribution and installation of the application.

Once the MDM solution is configured, FlexxAgent can be installed from Google Play.

## Supported versions

FlexxAgent runs on ChromeOS devices version 112 or later. The `ChromeOS Flex` edition is not supported.

## Limitations

Due to restrictions of this operating system, some functionalities are not available on this type of devices. These include: execution of power actions, remote assistance, flows, user microservices, or execution of microservices from Workspaces.

Some devices, to save battery, stop services or cannot connect to the internet while their screen is locked. When this happens, the device may stop reporting for a while until its screen is unlocked. This behavior varies depending on the manufacturer and the version of the operating system.

## Download and installation

FlexxAgent is available as a private Android app on Google Play.

Flexxible will grant access to FlexxAgent in the Managed Google Play console during the onboarding process.

FlexxAgent requires a managed configuration to be deployed. This configuration will be provided in JSON format by a Flexxible contact during the onboarding process.

## Installation

In broad strokes, the procedure is as follows:

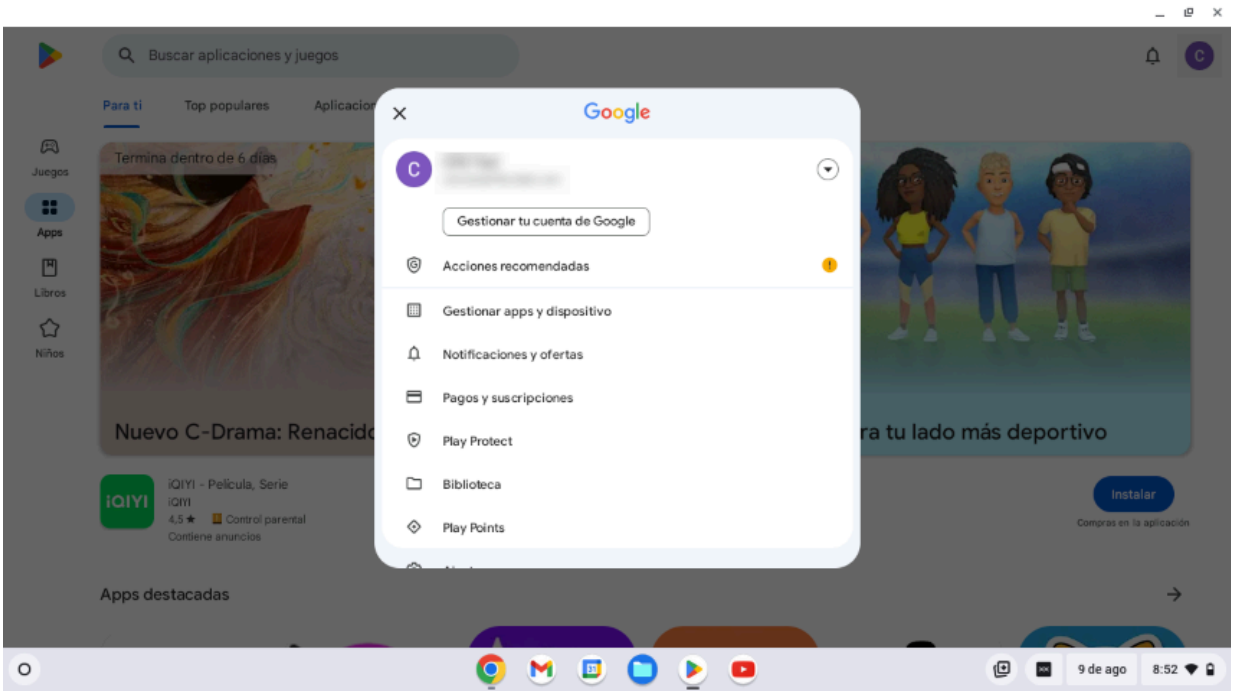
1. Go to `Devices` -> `Chrome` -> `Apps and extensions` -> `Users & browsers` and select the organizational unit (OU) in which you want to deploy the app.
2. Add the app from Google Play (search for FlexxAgent), assign the managed configuration (JSON), and mark it as `Force install`.

Please review the MDM documentation on how to deploy Google Play applications for managed users.

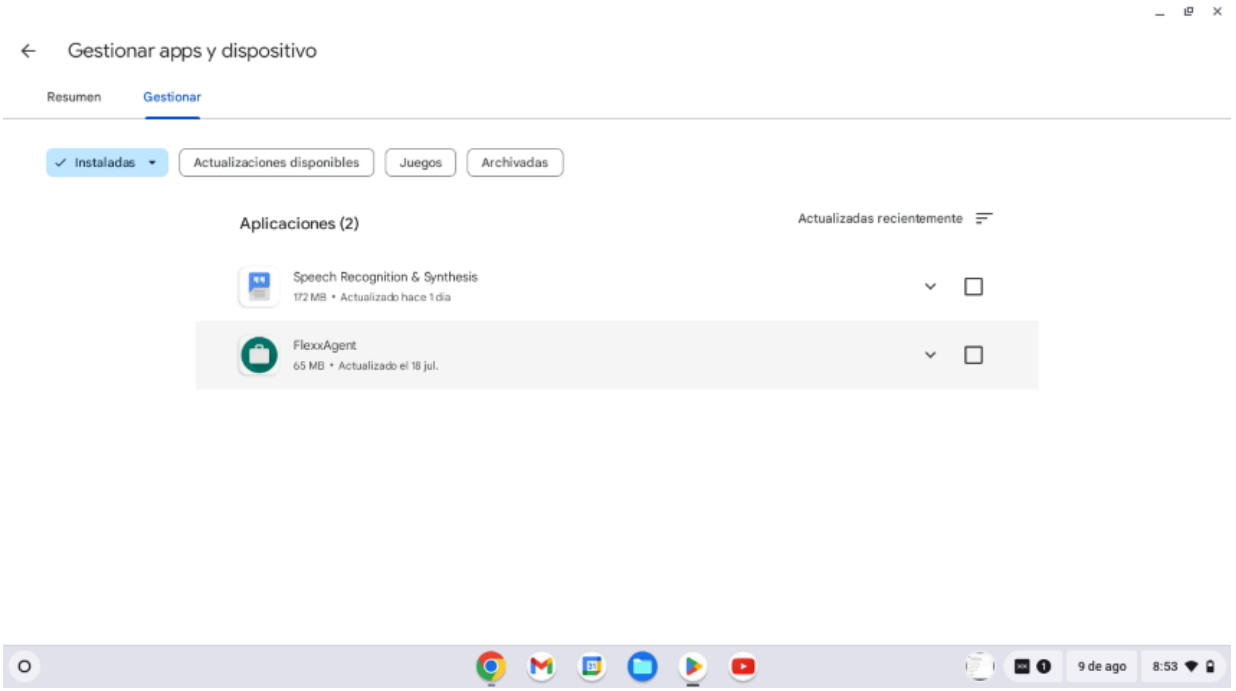
> Please review the linked links for more information on registering apps or deploying them to managed users in Google Admin.

To ensure FlexxAgent configuration applies correctly, the app must be manually opened on each device at least once after installation. It is recommended to follow these steps:

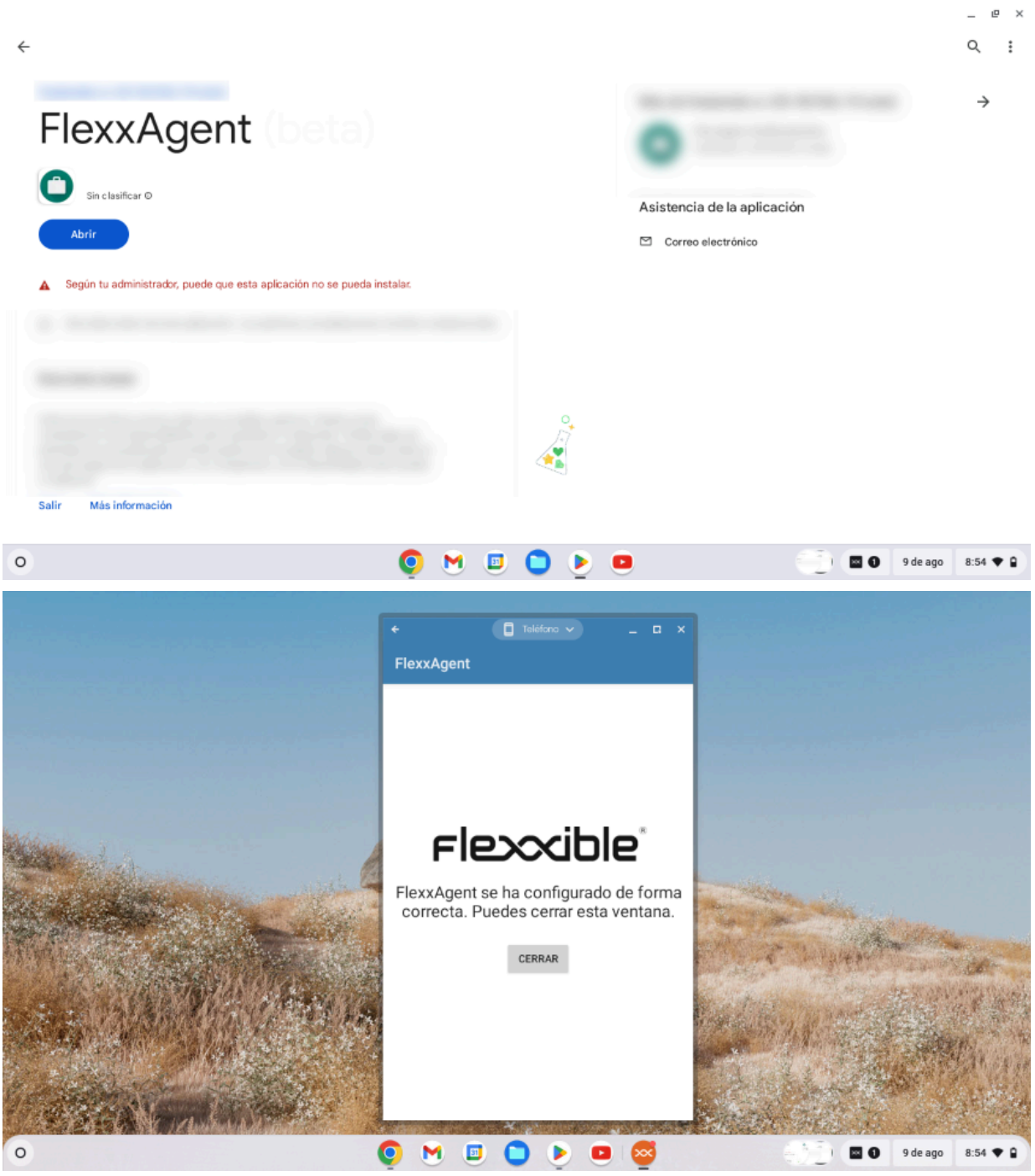
1. Go to Google Play and navigate to `Manage apps and devices`.




2. Go to the `Manage` tab and click on the FlexxAgent application.

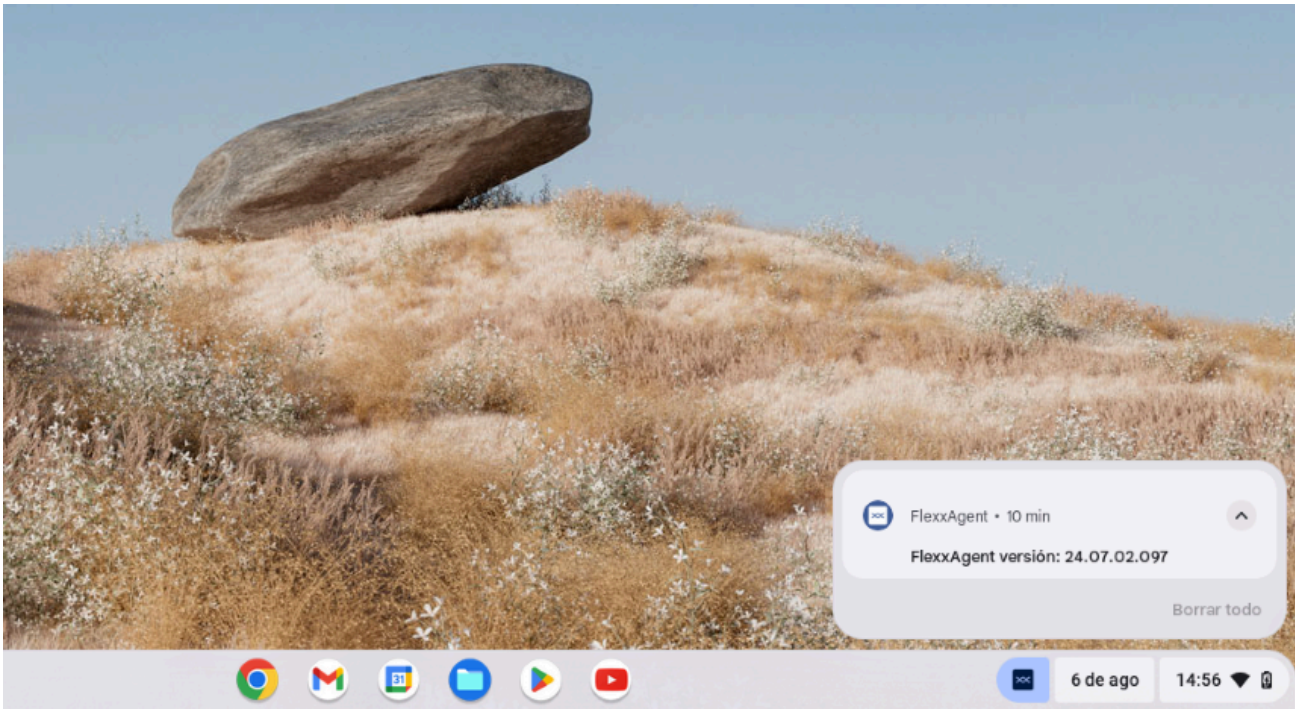



3. On the application's detail screen, click `Open`. Next, a window will appear confirming that the app has been successfully configured.




4. Close the window.

When running FlexxAgent on a ChromeOS device, the fixed notification indicates that the agent is installed and running.

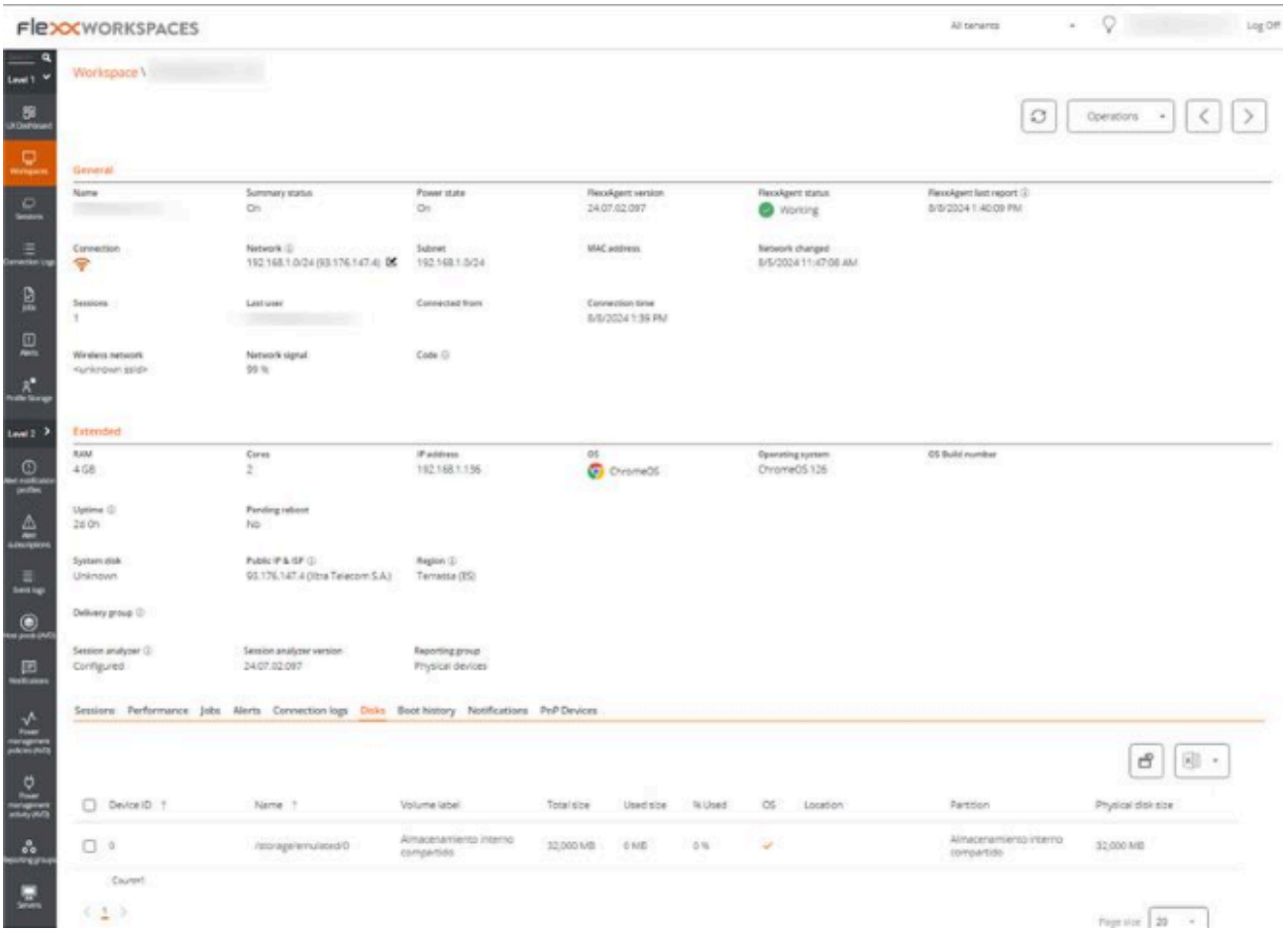



# Update

FlexxAgent updates automatically from Google Play.

# Information obtained from the device

FlexxAgent collects data locally from the device and sends it to the service consoles.




# General information

- **Name**: device name
- **Device Status**: Device power status Can be *On*, *Off* or *Unreported*.
- **FlexxAgent Version**: version number of FlexxAgent installed on the device
- **FlexxAgent Status**: *Running* or *Stopped*
- **Last FlexxAgent report**: date and time of the last FlexxAgent report on the device. This date might not be recent if the FlexxAgent service is stopped or the device is off.
- **Connection type**: indicates whether the device is connected by *Wi-Fi*, *Mobile network*, *Ethernet*, or *Unknown*.
- **Network**: device network addressing and public IP for internet access. These networks are created automatically when more than four devices are connected to the same network.
- **Network signal**: reception percentage
- **Subnet**: device's network addressing

- **Network changed**: date and time of the last network change
- **Sessions**: number of user sessions on the device
- **Last User**: last user connected to the device in domain\account format
- **Connected from**: when the selected device is a VDI or similar, it shows the name of the device from which the virtual device is accessed.
- **Connection Time**: date and time of session start.
- **Code**: this field lets users identify the workspace with a personal code. This code must be manually filled in individually using the Edit option in the Operations menu of the workspace details.
- **Description**: allows the user to identify the device with a personal description. This field must be assigned manually and individually using the Edit option in the Operations menu of the device details.

## Extended Info

- **RAM**: total available RAM capacity
- **Cores**: number of processor cores
- **IP address**: device IP address on the local network
- **OS**: type of operating system
- **Operating system**: operating system version
- **Uptime**: time the device has been running since it was last started or rebooted. If fastboot is enabled, the device is only off when it is restarted.
- **Region**: obtained using the public IP. It might not be accurate if connected to a corporate network or using a VPN.
- **Session Analyzer**: indicates whether or not it is configured to launch Session Analyzer in all the user sessions.
- **Session Analyzer version**: Session Analyzer version number
- **Report group**: report group to which the device belongs

## Information in tabs

FlexxAgent groups information about the following aspects of the device:

#### Sessions

Displays a table with the log of user sessions established on the device and timely information about the session type, connection status, or start date.

#### Jobs

All actions performed from the Workspaces module on one or more devices are audited in the Jobs queue. This tab allows you to check the work done for the active device.

#### Alert

Presents a table with the list of all active alerts on the device. When an alert is logged, a notice is displayed at the top of the page.


#### Connection log

Presents a list of the connections established with the device, including each instance where a user logs in or reconnects a previously disconnected session.

The session end date is recorded only for sessions that have been disconnected or closed. While the session remains active, this field will remain empty.

#### Disks

Displays a list of all partitions present on the disks identified in the system, as well as statistics of their capacity and occupancy levels.

#### Notifications

Allows you to see if the device has any active notification. When there is one, a message is displayed at the top of the page.

#### Reporting groups history

Allows you to see which reporting groups the device belongs to, the date of incorporation, and if it has been assigned to the group manually or automatically.

# FlexxAgent / Supported Systems / Android

The Android agent allows the inclusion of devices with this operating system in the service consoles, enabling complete visibility for the support teams for desktop computers and users' mobile devices.

## Requirements

To deploy FlexxAgent on Android devices, you need a mobile device management (MDM) platform, such as Google Admin or Microsoft Intune. These platforms allow centralized distribution and installation of the app.

Once the MDM solution is configured, FlexxAgent can be installed from Google Play.

## Supported versions

FlexxAgent runs on Android devices version 9.0 or later.

## Limitations

Due to the restrictions of this operating system, certain functionalities are not available for this type of device, such as the execution of power actions, remote assistance, user microservices, or microservices from Workspaces or flows. These include: execution of power actions, remote assistance, flows, user microservices, or execution of microservices from Workspaces.

Some devices, to save battery, stop services or cannot connect to the internet while their screen is locked. When this happens, the device may stop reporting for a while until its screen is unlocked. This behavior varies depending on the manufacturer and the version of the operating system.

## Settings

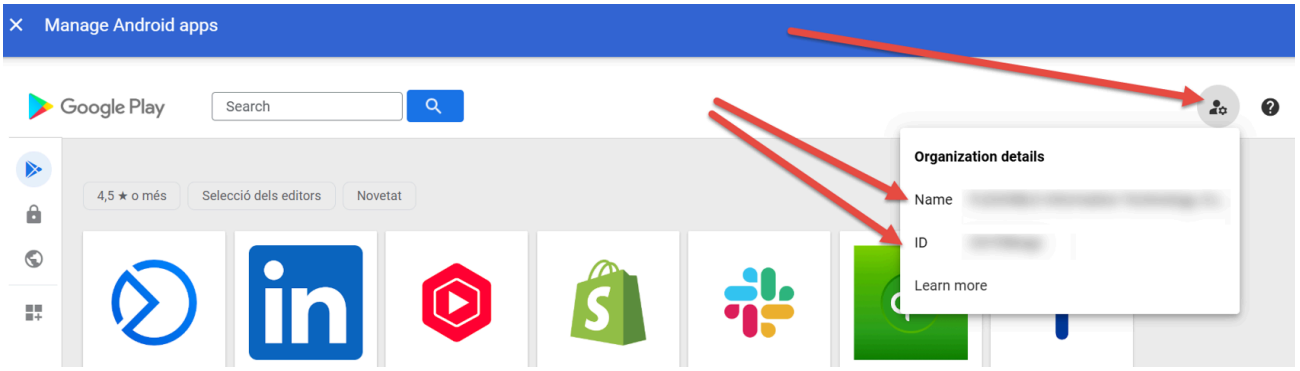
FlexxAgent configuration is managed through Managed Configurations to ensure correct operation.

This configuration will be provided by a Flexxible contact during the implementation process, according to the app distribution solution used. For example, for Microsoft Intune the configuration is provided in JSON format, but for Google Admin the configuration is provided with separate values.

# Distribution

Flexxible will grant access to FlexxAgent in the Managed Google Play console provided by the client's MDM solution during the implementation process, as well as the necessary data for its configuration.

For Flexxible to grant access to the app, the client must provide the *Name* and *ID* of their Managed Google Play.

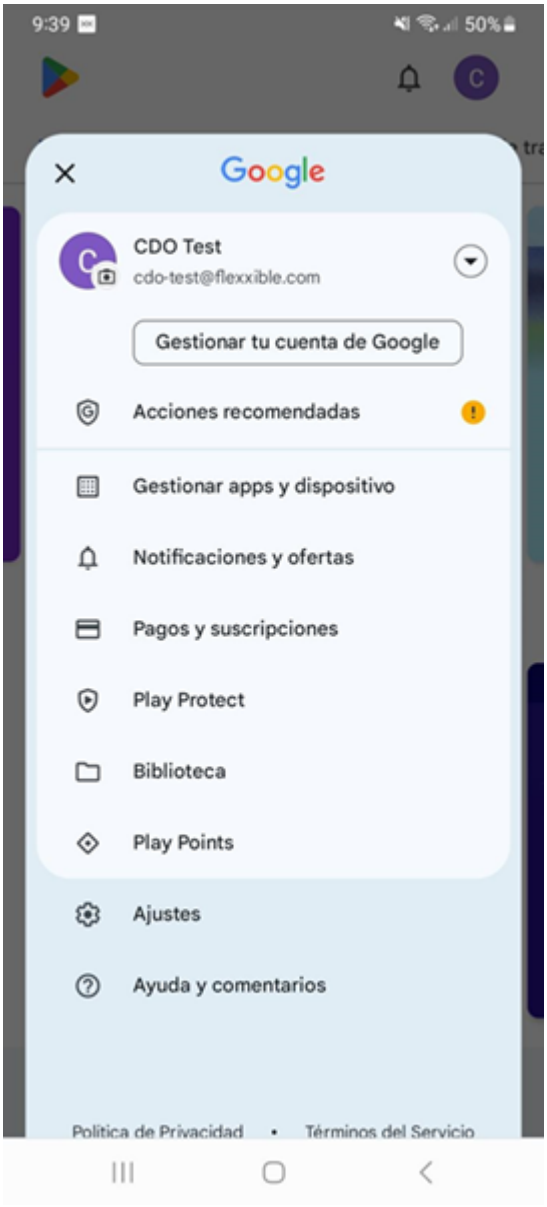



# Download and installation

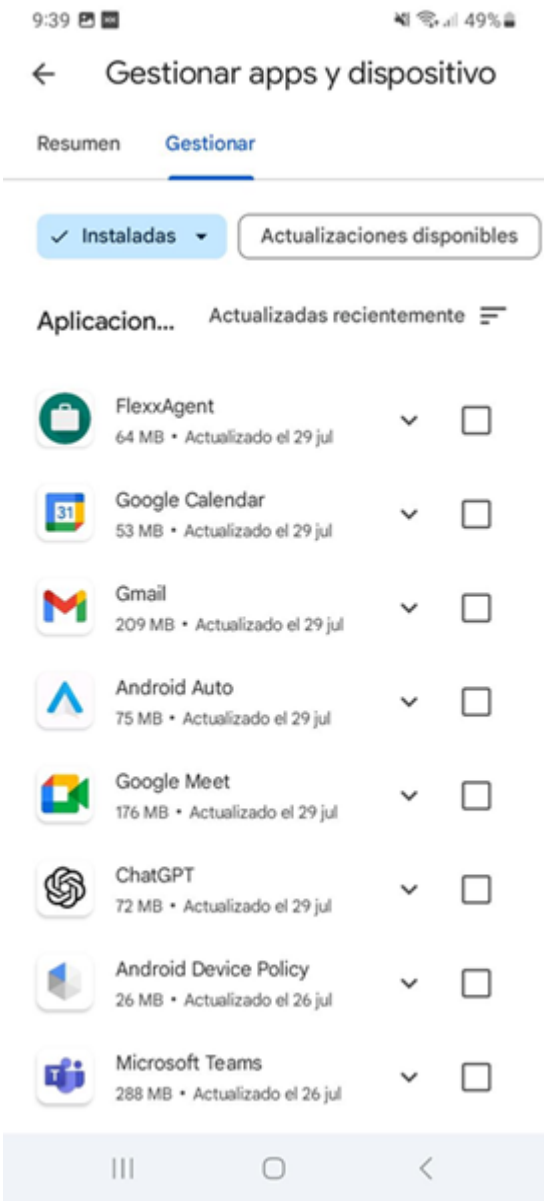
FlexxAgent is available as a private Android app on Google Play.

To ensure FlexxAgent configuration applies correctly, the app must be manually opened on each device at least once after installation. It is recommended to follow these steps:

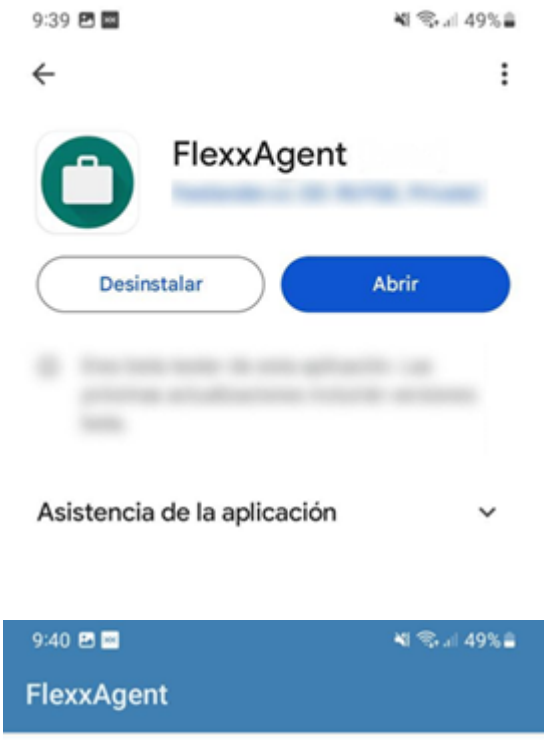
1. Go to Google Play and navigate to `Manage apps and devices`.




2. Go to the `Manage` tab and click on the FlexxAgent application.




3. On the app detail screen, click `Open`. Next, a window will appear confirming that the app has been successfully configured.

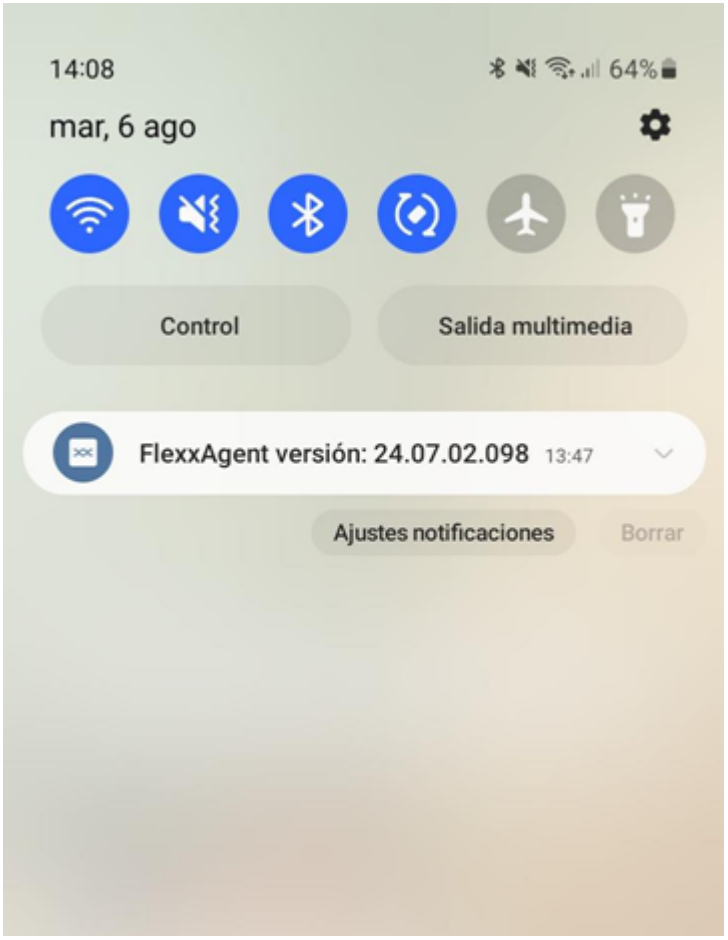



**INFO**

FlexxAgent requires some special permissions, such as access to device files. If this permission is not granted in the app's configuration in your MDM solution, the user will be prompted to provide it. When they do, a message will appear indicating that the app has been successfully configured.

4. Close the window.

When running FlexxAgent on an Android device, the fixed notification indicates that the agent is installed and running.

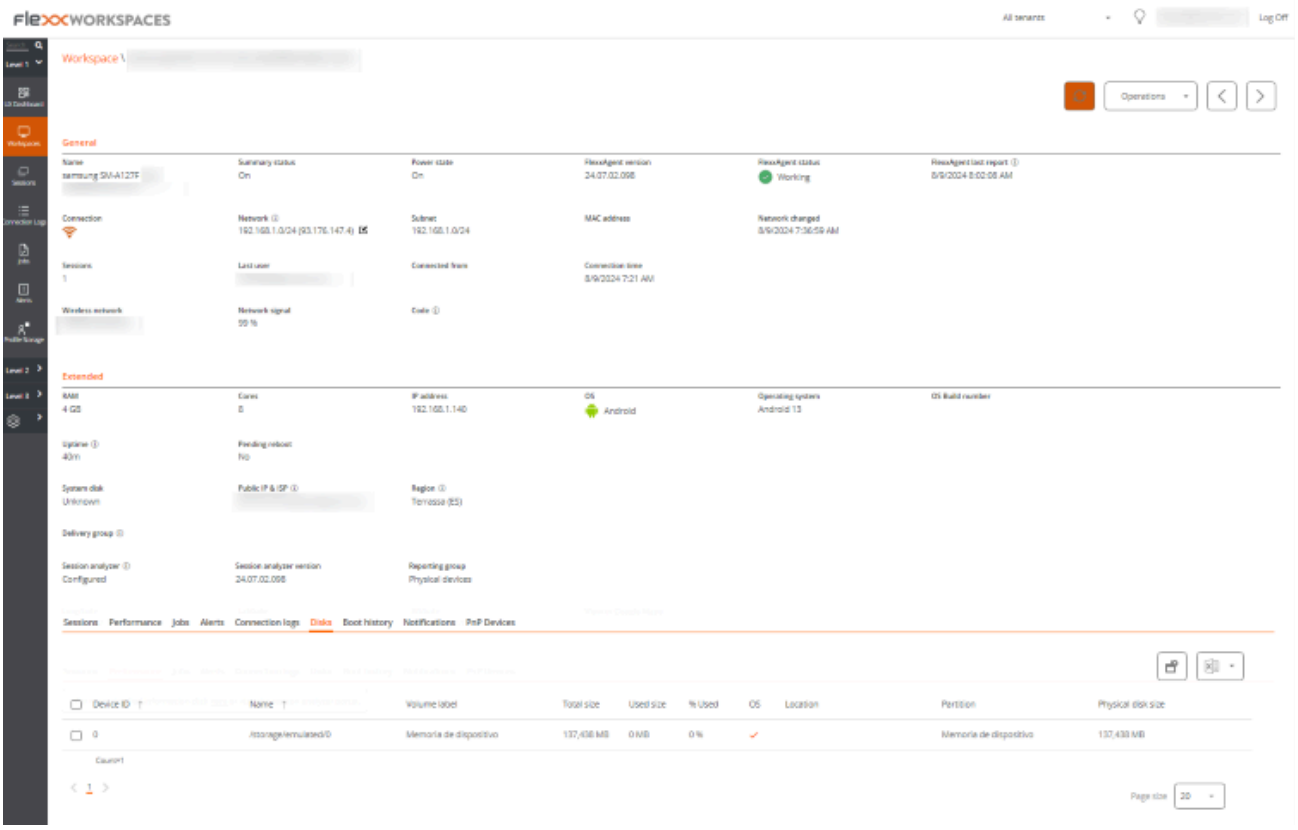



# Update

FlexxAgent updates automatically from Google Play.

# Information obtained from the device

FlexxAgent collects data locally from the device and sends it to the service consoles.




# General information

- **Name**: device model
- **Device status**: power status of the device. It can be *On*, *Off*, or *Not reporting*.
- **FlexxAgent Version**: version number of FlexxAgent installed on the device
- **FlexxAgent Status**: *Running* or *Stopped*
- **Last FlexxAgent report**: date and time of the last FlexxAgent report on the device. This date might not be recent if the FlexxAgent service is stopped or the device is off.
- **Connection type**: indicates whether the device is connected by *Wi-Fi*, *Mobile network*, *Ethernet*, or *Unknown*.
- **Network**: device network addressing and public IP for internet access. These networks are created automatically when more than four devices are connected to the same network.
- **Network signal**: reception percentage
- **Subnet**: device's network addressing
- **MAC Address**: unique identifier of the device's network card
- **Network changed**: date and time of the last network change

- **Sessions**: number of user sessions on the device
- **Last User**: last user connected to the device in domain\account format
- **Connected from**: when the selected device is a VDI or similar, it shows the name of the device from which the virtual device is accessed.
- **Connection time**: session start date and time
- **Code**: this field lets users identify the workspace with a personal code. This code must be manually filled in individually using the Edit option in the Operations menu of the workspace details.
- **Description**: allows the user to identify the device with a personal description. This field must be assigned manually and individually using the Edit option in the Operations menu of the device details.

## Extended Info

- **RAM**: total amount of RAM available
- **Cores**: number of processor cores
- **IP address**: device IP address on the local network
- **OS**: type of operating system
- **Operating system**: operating system version
- **Uptime**: time the device has been running since it was last started or rebooted. If fastboot is enabled, the device is only off when it is restarted.
- **Region**: obtained using the public IP. It might not be accurate if connected to a corporate network or using a VPN.
- **Session Analyzer**: indicates whether or not it is configured to launch Session Analyzer in all the user sessions.
- **Session Analyzer version**: Session Analyzer version number
- **Report group**: report group to which the device belongs

## Information in tabs

FlexxAgent groups information about the following aspects of the device:

#### Sessions

Displays a table with the log of user sessions established on the device and timely information about the session type, connection status, or start date.

#### Jobs

All actions performed from the Workspaces module on one or more devices are audited in the Jobs queue. This tab allows you to check the work done for the active device.

#### Alert

Presents a table with the list of all active alerts on the device. When an alert is logged, a notice is displayed at the top of the page.


#### Connection log

Presents a list of the connections established with the device, including each instance where a user logs in or reconnects a previously disconnected session.

The session end date is recorded only for sessions that have been disconnected or closed. While the session remains active, this field will remain empty.

#### Disks

Displays a list of all partitions present on the disks identified in the system, as well as statistics of their capacity and occupancy levels.

#### Notifications

Allows you to see if the device has any active notification. When there is one, a message is displayed at the top of the page.

#### Reporting groups history

Allows you to see which reporting groups the device belongs to, the date of incorporation, and if it has been assigned to the group manually or automatically.

# FlexxAgent / Network and security considerations

FlexxAgent, in its regular operation, requires a series of network requirements to connect to cloud orchestration services and support proxies, as well as complex network ecosystems.

Before deploying FlexxAgent on the devices, it is recommended to validate that at the network level these can access the defined destinations in URLs and ports.

## Bandwidth usage

#### FlexxAgent process

When FlexxAgent starts, it collects and sends an initial report of approximately 75 KB; from that moment, it sends differential reports of approximately 3-4 KB. This process is responsible for executing on-demand or automatic actions on the device. At those moments, the network traffic could increase.

#### FlexxAgent Analyzer process

FlexxAgent Analyzer collects user session information every 15 seconds, such as application consumption, resource usage, and more. And it adds this information into files of approximately 35-50 KB, which are sent to the consoles every 5 minutes, although the time could change in specific functionalities.

In multi-user systems, a single instance of FlexxAgent will run and as many instances of FlexxAgent Analyzer as user sessions the system has.

# Required URLs and Ports

In terms of communications, FlexxAgent must be able to contact the orchestration layer of the service hosted on the Internet, which includes:

| URL | Ambit | Port | Region | Pro |
|---|---|---|---|---|
| https://flxsbname***.servicebus.windows.net | Agent | 443 | West Europe | FXXO<br>FlexxC<br>FlexxD |
| https://flxiothub***.azure-devices.net | Agent | 443 | West Europe | FXXO<br>FlexxC<br>FlexxD |
| https://west-eu.agent-api.analyzer.flexxible.com | Agent | 443 | West Europe | FXXO<br>FlexxC<br>FlexxD |
| https://flexxibleglobal.blob.core.windows.net | Agent | 443 | West Europe | FXXO<br>FlexxC<br>FlexxD |
| https://api.ipify.org | Agent | 443 | West Europe | FXXO<br>FlexxC<br>FlexxD |
| https://ras.flexxible.com | Agent – Remote Assistance | 443 | West Europe | FXXO<br>FlexxC<br>FlexxD |
| https://update.workspaces.flexxible.com | Agent | 443 | West Europe | FXXO<br>FlexxC<br>FlexxD |
| https://agents-weu.one.flexxible.net | Agent | 443 | West Europe | FXXO |
| https://agents-weu.flexxible.net | Agent | 443 | West Europe | FlexxC<br>FlexxD |

| URL | Ambit | Port | Region | Pro |
|---|---|---|---|---|
| https://west-eu-01.agent-api.one.analyzer.flexxible.com | Agent | 443 | West Europe | FXXO |

*** unique identifier provided by Flexxible.

# Security

To ensure a good user experience, in some cases it will be necessary to configure exclusions in the antivirus; however, if not managed properly, these exclusions can pose a security risk.

For this reason, it is advised to periodically scan the files and folders that have been excluded from antivirus scanning. Both Microsoft and Flexxible recommend:

- Use a File Integrity Monitoring (FIM) or Host Intrusion Prevention (HIP) solution to protect the integrity of the elements excluded from real-time analysis.
- If Azure Sentinel is used and Windows Defender is not configured correctly, performance issues may arise. Disable Windows Defender with the following PowerShell command:

```
Set-MpPreference -DisableIntrusionPreventionSystem $true -DisableIOAVProtection $true -DisableRealtimeMonitoring $true -DisableScriptScanning $true -EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend
```

## Antivirus exclusions

FlexxAgent should be able to function correctly without configuring exceptions, but in more restrictive environments, it might be necessary to set some.

The items to exclude from antivirus analysis are as follows:

### Folders

- `C:\Program Files\Flexxible`
- `C:\Windows\Temp\FlexxibleIT\`

### Compute

- `FlexxAgent.exe`
- `FlexxibleRA.exe`
- `FlexxibleRemoteAssistance_XXXX.exe`

### Files

- `C:\Windows\Temp\FlexxAgentInstallation.log`
- `C:\Windows\Temp\UpdateFlexxAgent.ps1`
- `C:\Windows\Temp\FlexxAgentHealthCheck.log`

## Deep SSL Inspection

For security solutions like Deep SSL Inspection or Trend Micro, the instructions described below should be taken into account to ensure optimal performance of FlexxAgent.

Deep SSL Inspection should be disabled for the following URLs on devices that use it as a security solution:

- https://flxsbname***.servicebus.windows.net
- https://flxiothub***.azure-devices.net
- https://agents-weu.flexxible.net
- https://ras.flexxible.com

## PowerShell process restriction

Some security solutions do not allow the installation and/or self-update of FlexxAgent to be performed effectively, as is the case with Trend Micro.

During the process, the installer may return the message:

> *The process was terminated with errors. A corrupted installation was detected due to external processes. This is usually caused by antivirus activity. Please check your antivirus settings.*

To solve this, Flexxible recommends excluding the following files from the device:

> `C:\Windows\Temp\FlexxibleIT`

> `C:\Windows\Temp\UpdateFlexxAgent.ps1`

# Wake on LAN (WoL)

Wake on LAN allows devices to be powered on by sending a Magic Packet that instructs the network card to power on. The following is required in order to use this functionality:

- Compatible network card
- Activate WoL in BIOS/UEFI
- Configure WoL in the operating system
- A `Bridge` device on the same network as the device to be powered on, with FlexxAgent installed and reporting

Wake on LAN (WoL) normally operates within a local network, and can work between subnets as long as there are no restrictions imposed by firewalls or network devices blocking the Magic Packet transmission. In subnet-segmented environments, network-level exceptions need to be configured to allow Magic Packet routing between subnets.

## Configure Wake on LAN (WoL) in Windows

To configure the Wake on LAN (WoL) functionality on a device with Windows operating system, follow these steps:

1. Check if WoL is On

In the CMD window, execute the following command:

```
powercfg /devicequery wake_programmable
```

2. On WoL

Run the command:

```
powercfg /deviceenablewake "Realtek PCIe GbE Family Controller"
```

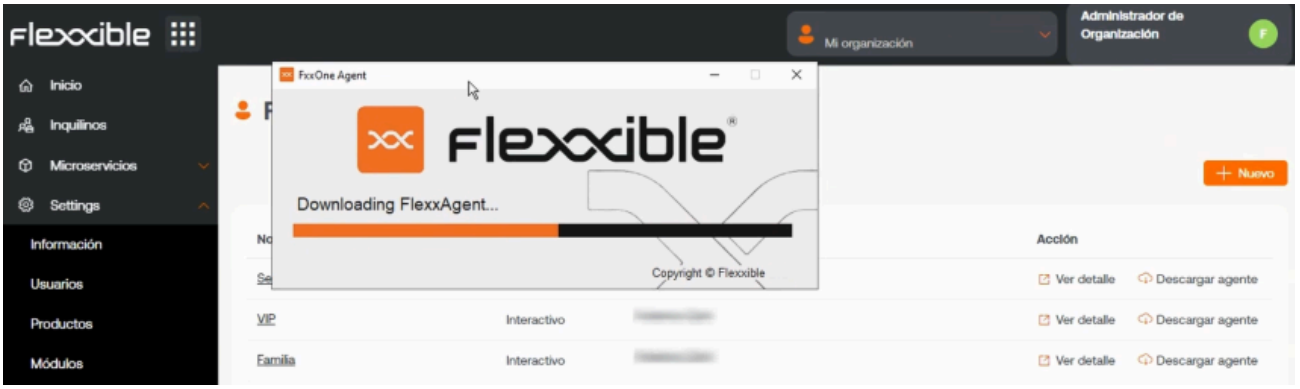
> Replace "Realtek PCIe GbE Family Controller" with the name of the corresponding driver.

# Remote assistance through proxy

For remote assistance, FlexxAgent will use a proxy when it is configured and accessible.

In case it is configured with a proxy but it is not accessible at that moment, remote support will be launched with the “auto detect” option which will use the internet exit configuration set by the end user.

# FlexxAgent / Guides and tutorials for FlexxAgent




This section offers resources designed to maximize the use of FlexxAgent. It includes detailed instructions on deployment and installation, as well as advanced configuration options that allow FlexxAgent to be tailored to specific needs.

Each guide has been created to facilitate understanding and application, regardless of the user's level of experience. In addition to step-by-step instructions, you will find procedures and solutions to common problems.

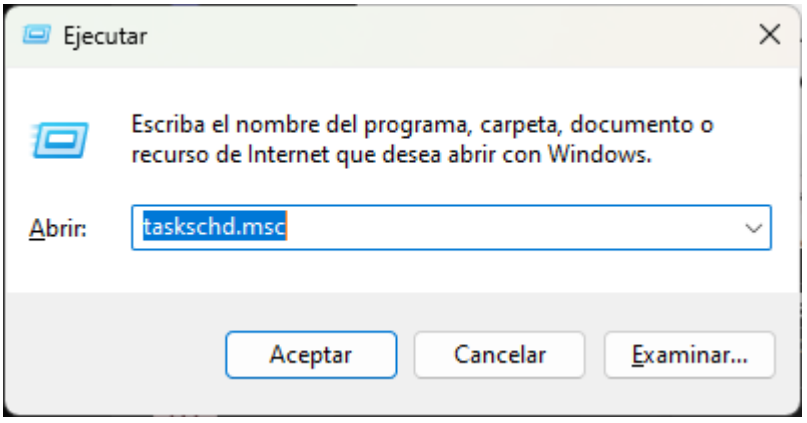
# FlexxAgent / Guides and tutorials / Check FlexxAgent connectivity

To validate the connectivity of FlexxAgent with the SaaS service instances and ensure its correct execution, the procedure defined here must be carried out on a test device. This must be part of the same corporate network where the devices that will receive the future deployment of FlexxAgent are hosted.

> Note: This procedure only applies to **Windows** systems.

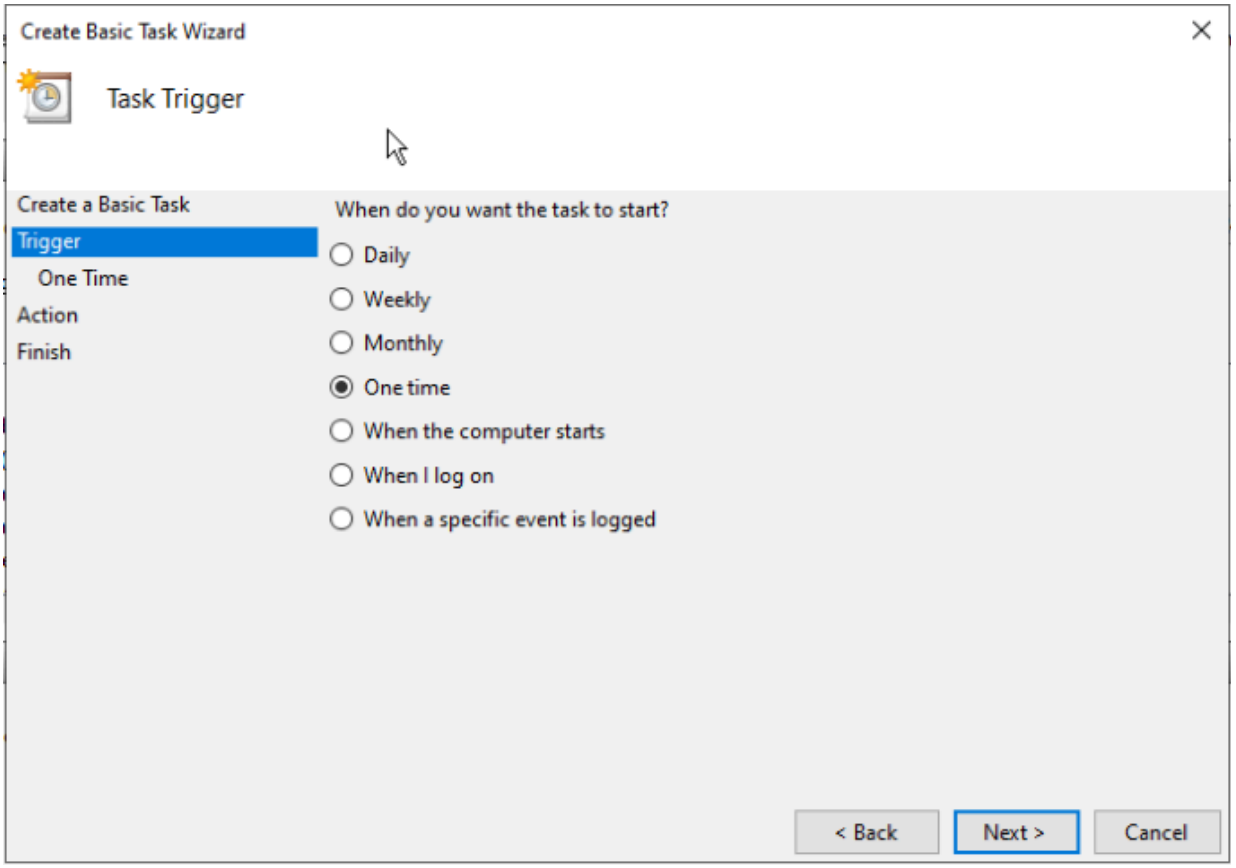
## Creating a scheduled task

1. Access the `Run` menu (`Windows + R`) and type the command `taskschd.msc`. This opens the Windows task scheduler management console.

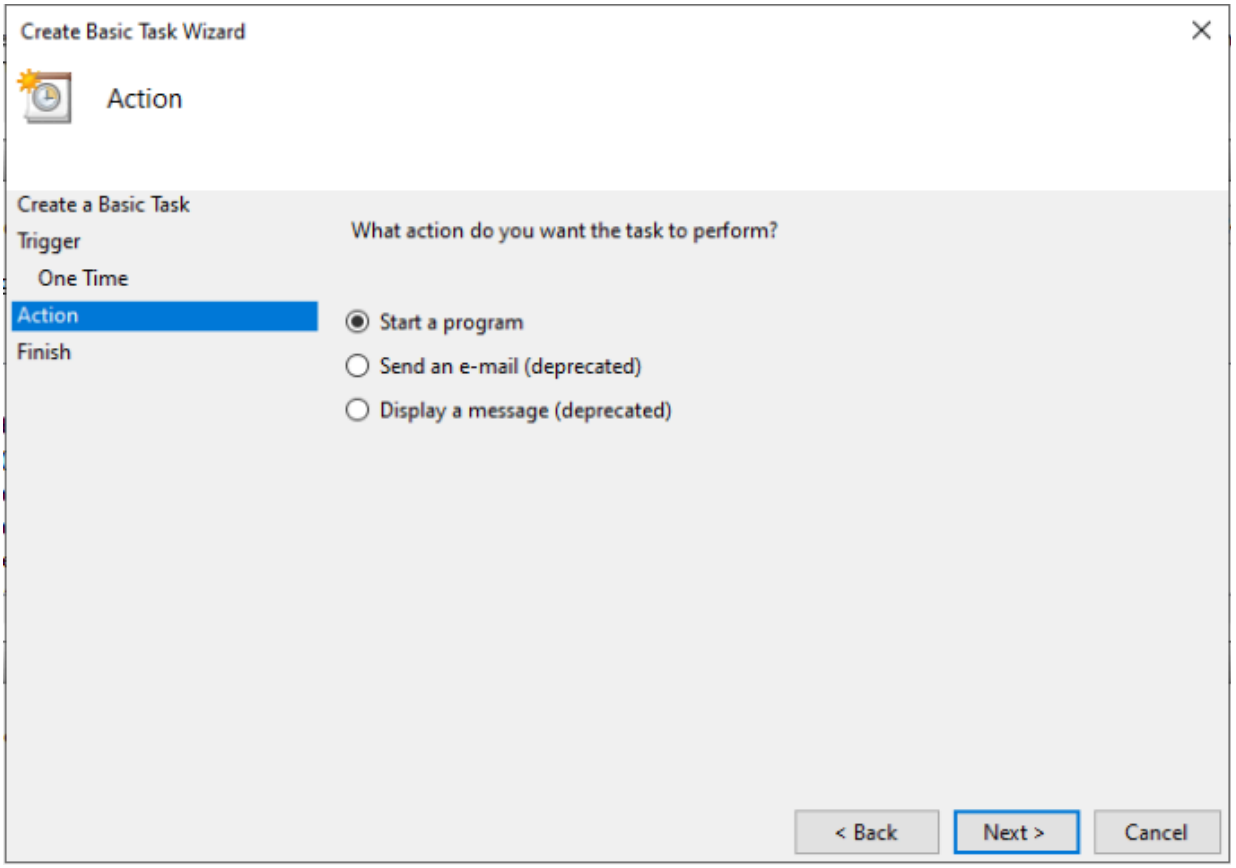



2. In the `Actions` panel, select the `Create Basic Task` option and name the task (it can be `FlexxAgent check connectivity`). You can write a description if desired, and click `Next`.

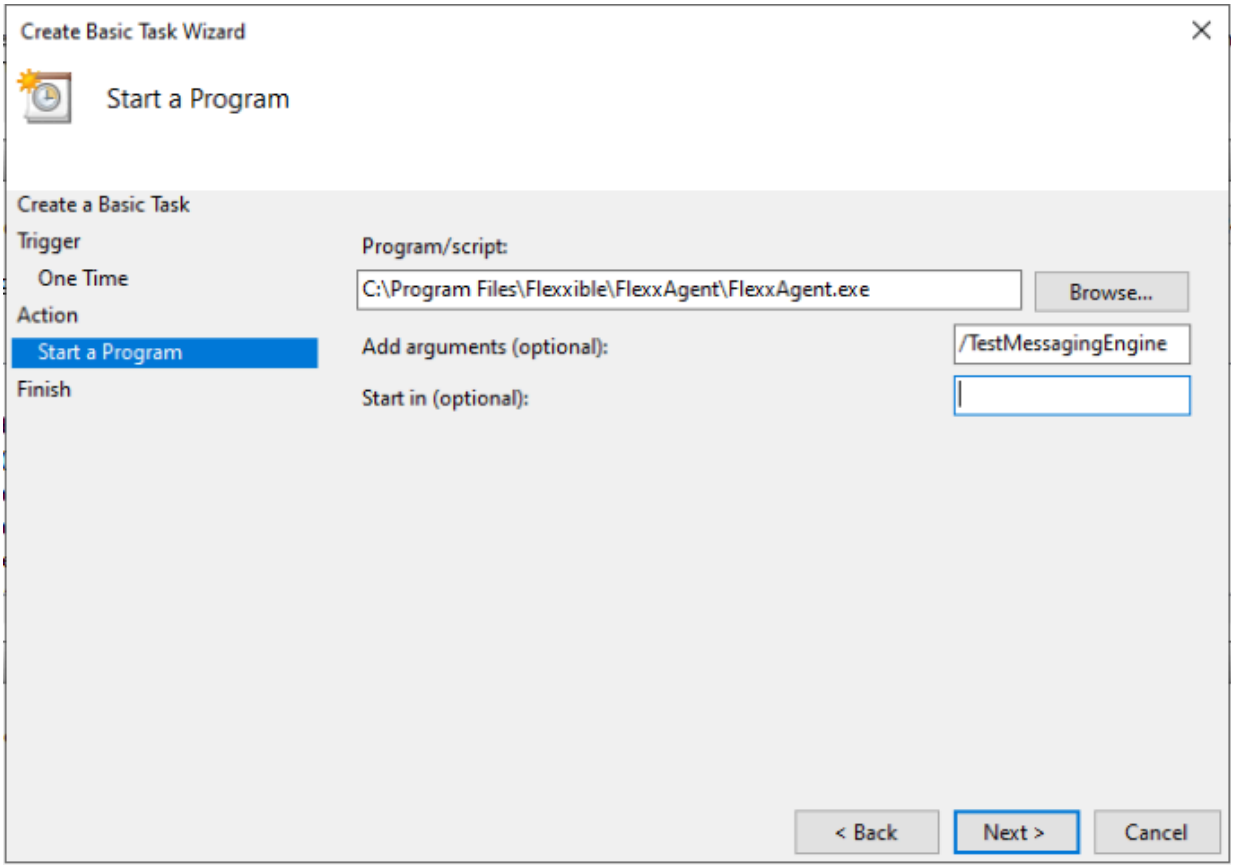
3. Next, select `One Time` and click `Next`. A date picker will appear, but it is not relevant because the task will be executed manually. Click `Next`.



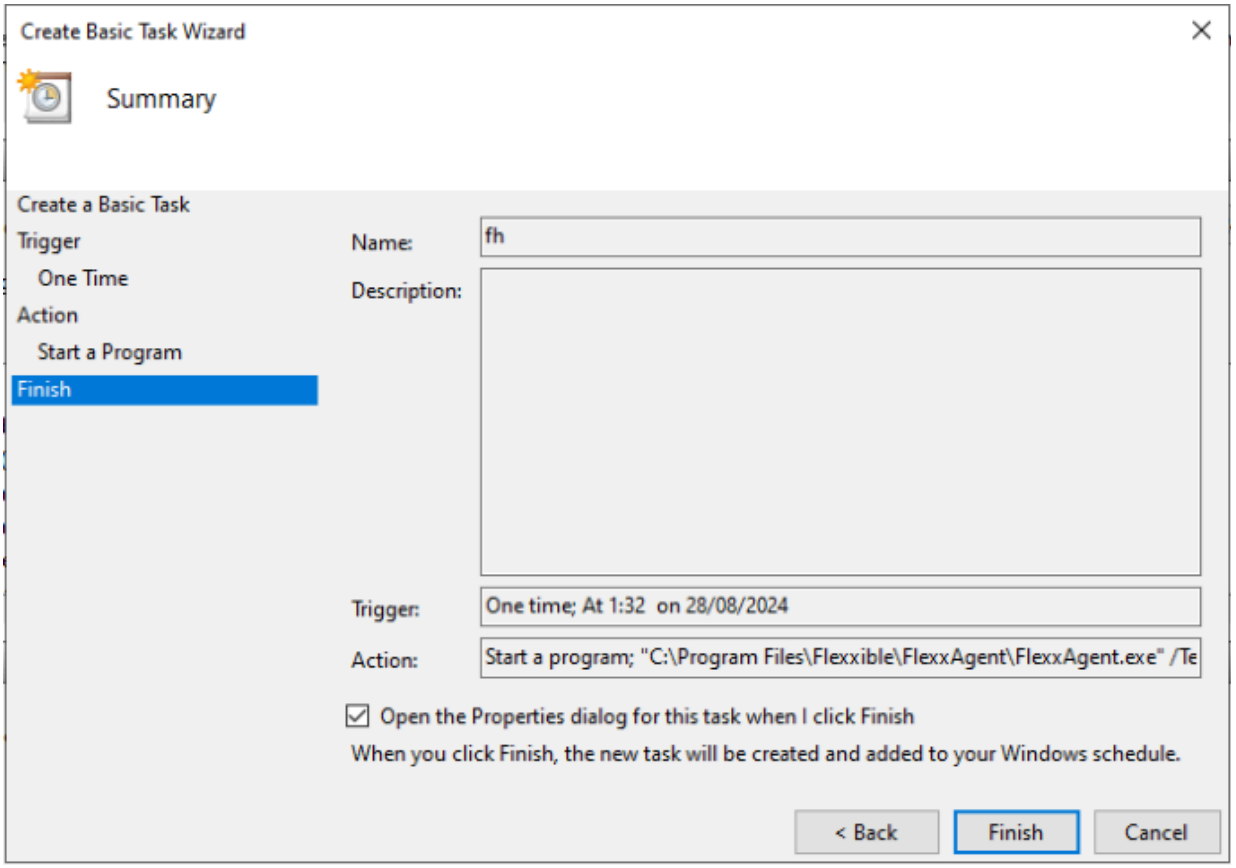

4. Select the `Start a program` action and click `Next`.



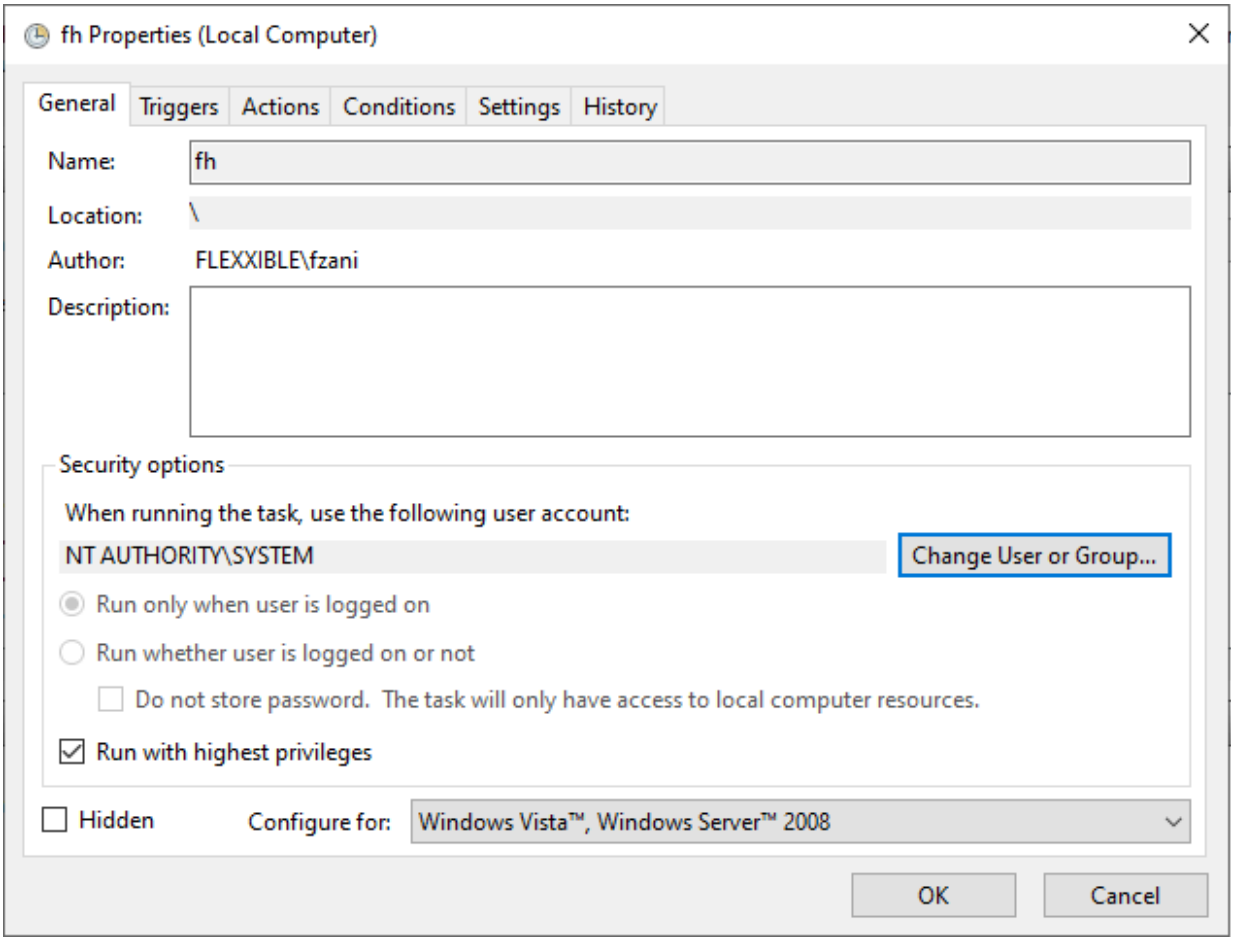

5. In the `Program/script` field, type or browse to the path `C:\Program Files\Flexxible\FlexxAgent\FlexxAgent.exe`. In `Additional Arguments`, type `/TestMessagingEngine`. Click `Next`.



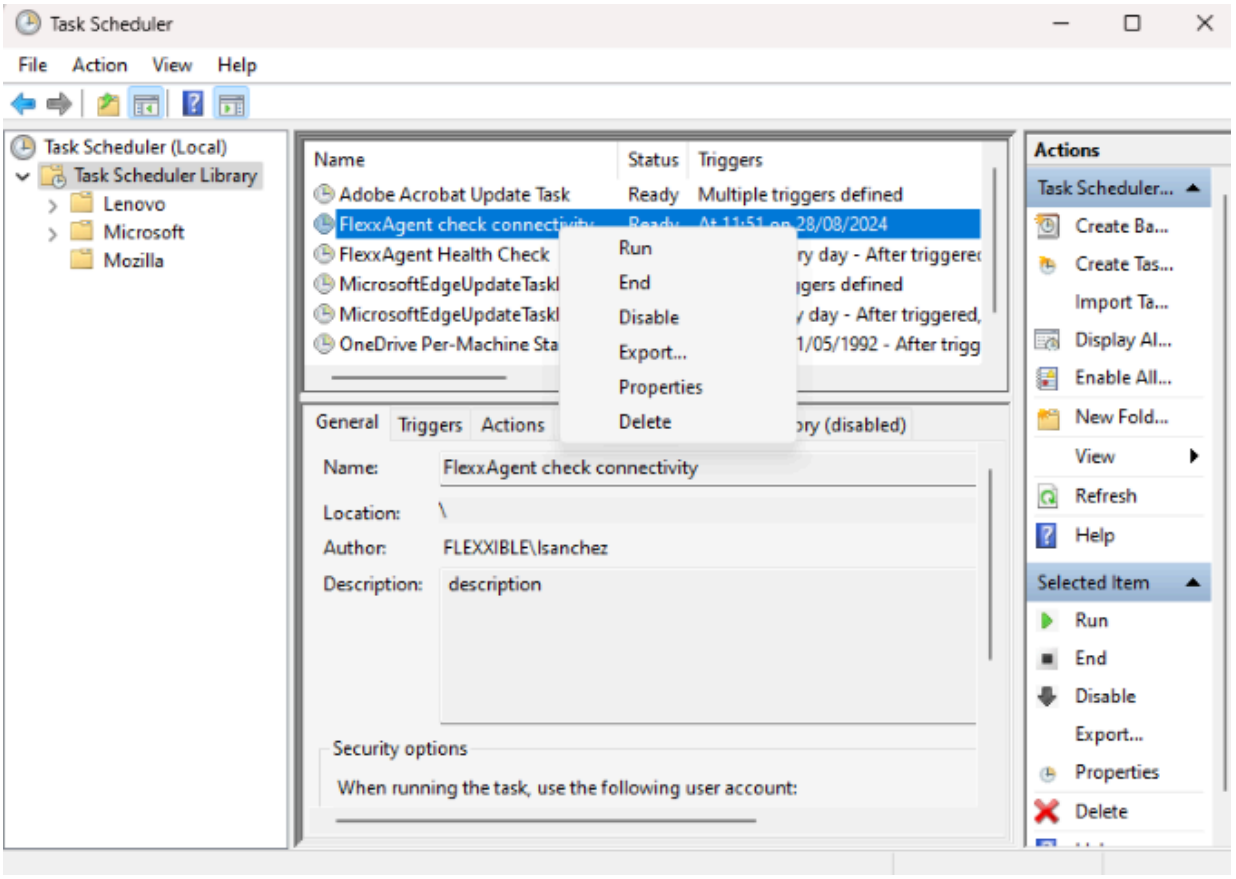

6. Select `Open the Properties dialog for this task when I click Finish` and click `Finish`. The task properties dialog will open.




7. Click on `Change User or Group`. In the text box of the pop-up window, type `SYSTEM` and then click `Check Names`. This action will check that the `SYSTEM` group exists to run the task under its identity. Hacer clic en `Aceptar` (OK) para cerrar la ventana emergente. En la ventana de propiedades, se debe seleccionar `Ejecutar con los privilegios más altos` en el checkbox y pulsar `Aceptar`.




8. In the Windows task scheduler management console, search for the newly created task `FlexxAgent check connectivity`. Right-click on it and select `Run`. It will appear as `Running` in the task list.

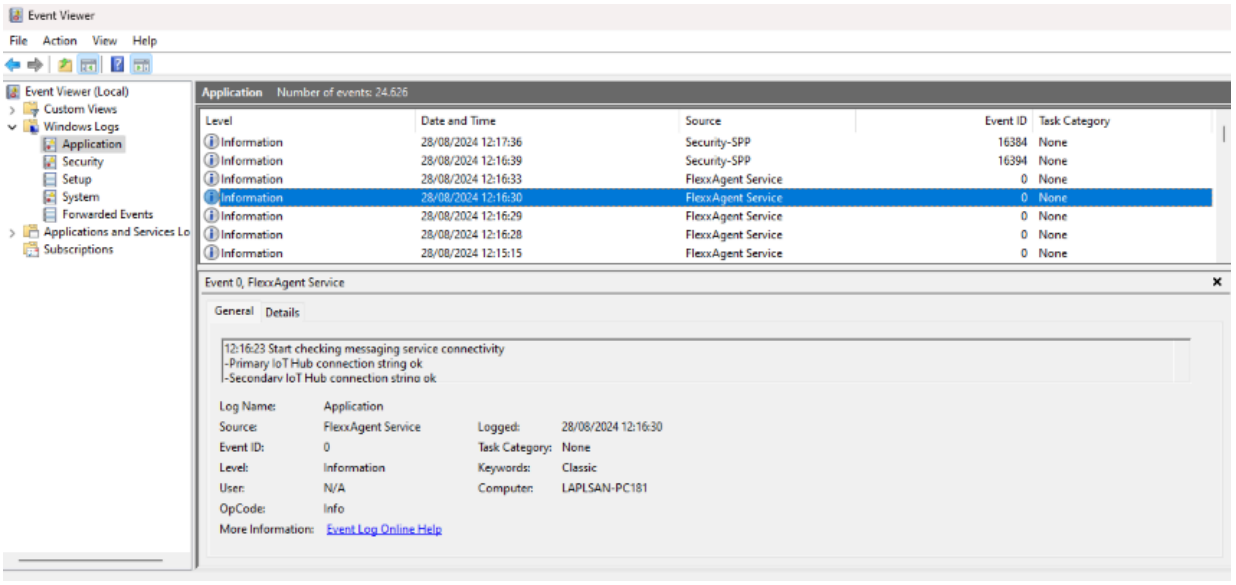



9. Select the `History` tab to see the progress of the task until you see the `Task completed` event. In case the history is disabled, it can be enabled with the `Enable history for all tasks` option in the right panel of the console.

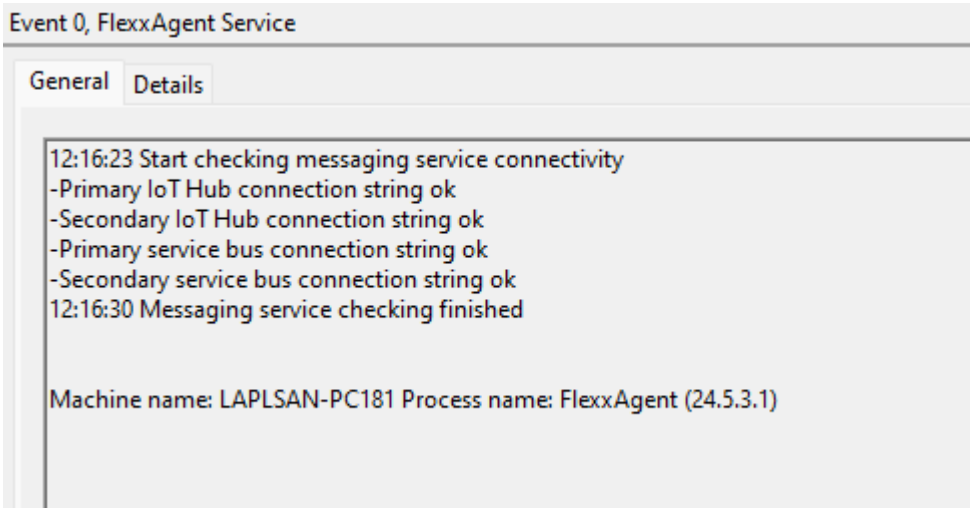
# Validation of results

To review the FlexxAgent messaging engine information, access the `Event Viewer` and check for informational messages with the source service of `FlexxAgent Service`:

1. Access the `Run` menu (`Windows + R`) and type `eventvwr.msc`. This command will open the Windows event viewer. On the left side, select `Windows Logs` -> `Application`.




2. In the list, search for the `FlexxAgent Service` event. If there are several, select the one reporting connectivity. This event reports the status of all connections:



# FlexxAgent / Guides and tutorials / Deploy FlexxAgent using Microsoft Intune

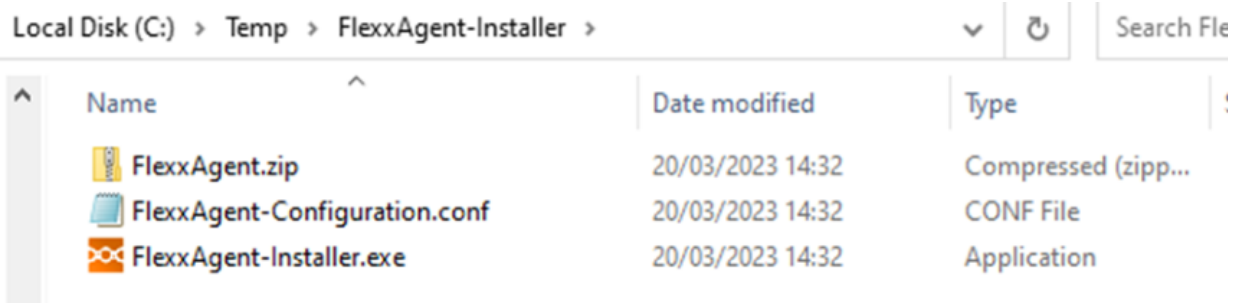
FlexxAgent can be deployed using Microsoft Intune. Before doing it, you need to check that you have the following requirements:

- Microsoft Windows 10 version 1607 or later
- The devices must be enrolled in Intune and added to the active directory in one of the following configurations:
  - Registered in Azure Entra ID (especially in `Bring your own device` environments)
  - Joined to Azure Entra ID (also known as `Joined device`)
  - Associated with a hybrid environment (AD / Azure Entra ID)
- The `Microsoft Win32 Content Prep Tool` is required.

> It is recommended to have the 'offline' installation package of FlexxAgent; that way, you will have all the files necessary for installation from Intune itself.

Once you have the installation package and the previous requirements, the procedure to install the agent using Intune is as follows:

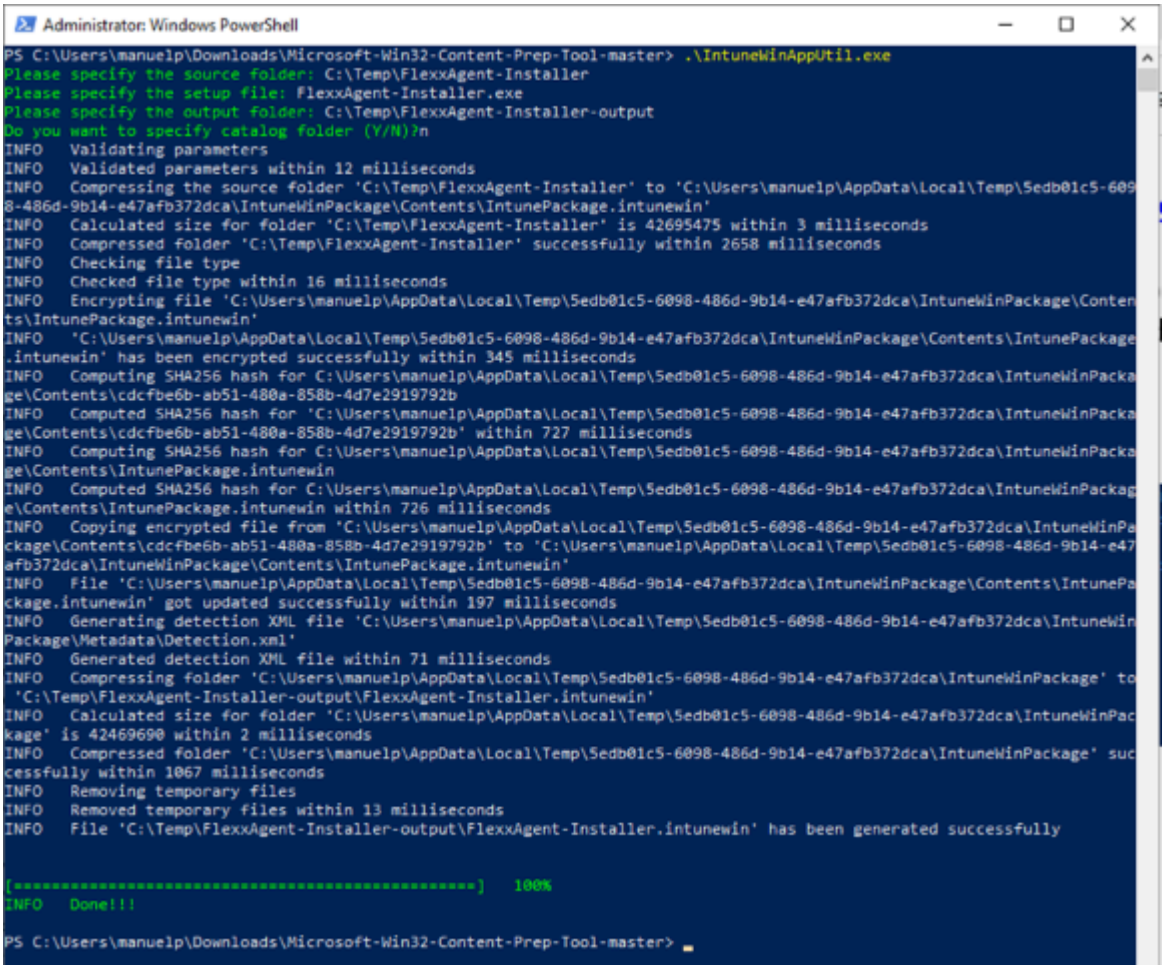
1. Unzip the installation package to some folder. You will see the files:



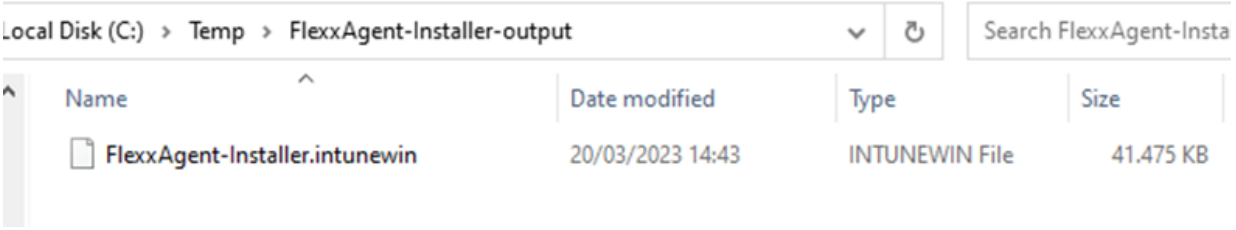

2. Download the `Microsoft Win32 Prep Tool`. For more information, see Prepare a Win32 app to be uploaded to Microsoft Intune.

3. Create an empty folder; for example: `C:\Temp\FlexxAgent-Installer-output`.

4. Create the FlexxAgent installation package (in this example, it was extracted to `C:\Temp\FlexxAgent-Installer`). And convert it into an Intune package using the IntuneWinAppUtil.exe tool (Microsoft Win32 Content Prep Tool).




5. Confirm that the package has been created correctly.

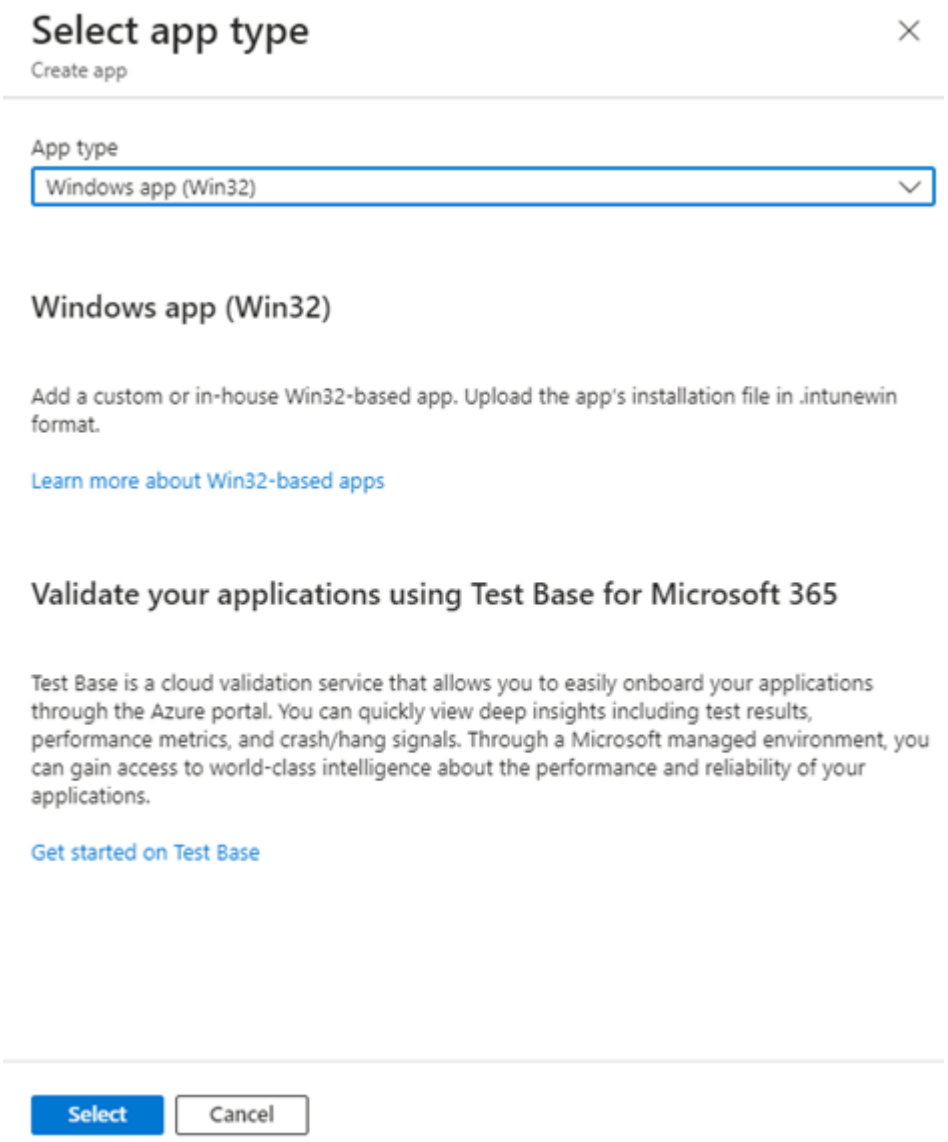



6. The created package is used to deploy an application within Intune.

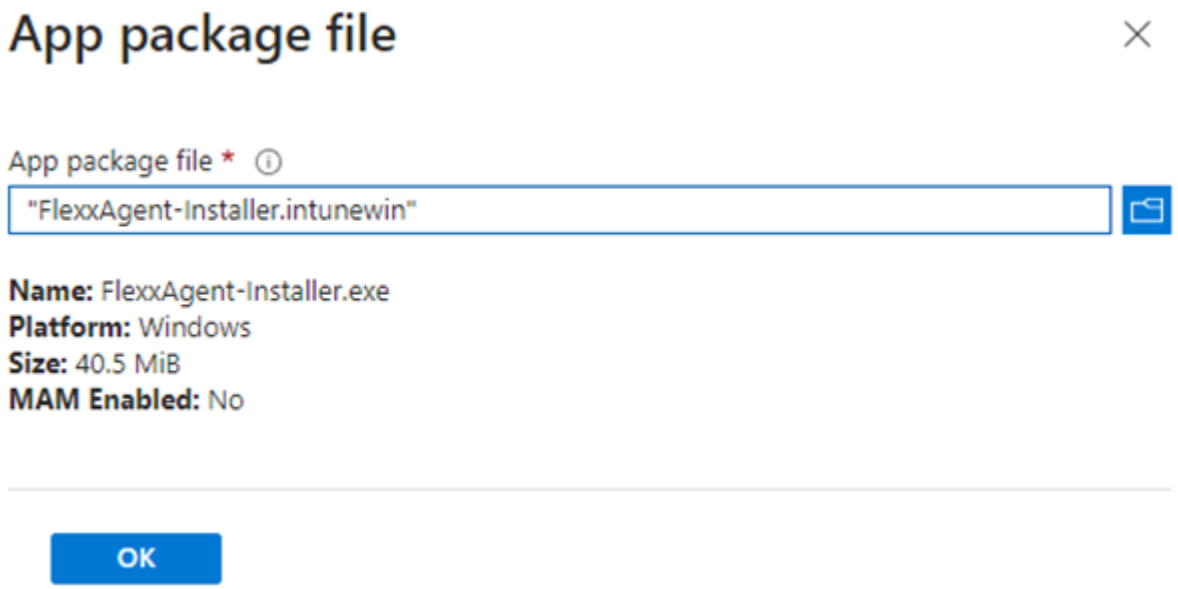
7. Go to the Intune admin center.

8. Select `Apps` and then `All Apps`.

9. Select `+ Add` and choose `Windows app (Win32)` for the application type.

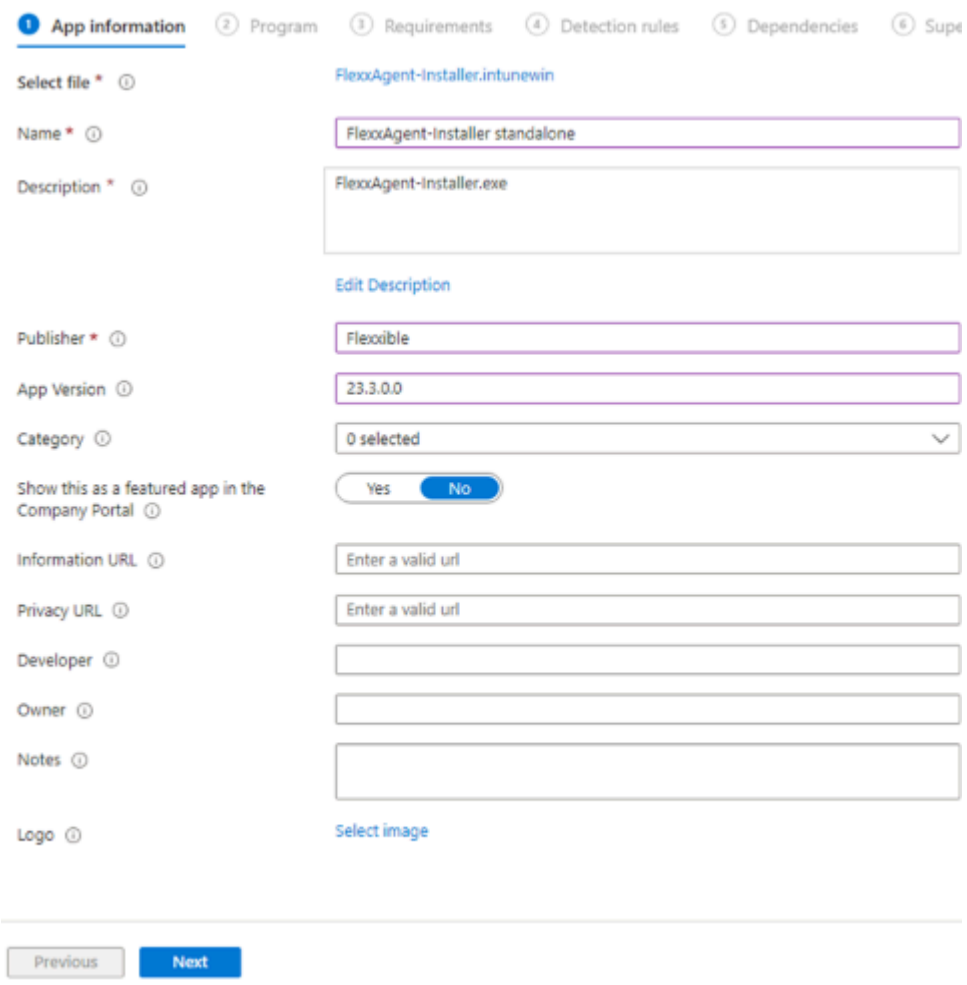



10. On the application information tab, click `Select app package file` and browse for the previously created package (in this example, it's in the folder C:\Temp\FlexxAgent-Installer-output).




11. On the application information tab, enter the information for FlexxAgent.

    - Name: FlexxAgent-Installer standalone
    - Publisher: Flexxible
    - App version: this information is provided in the properties of the FlexxAgent-Installer.exe file.




12. On the `Program` tab, you need to include information about the install command, uninstall command, and other data.

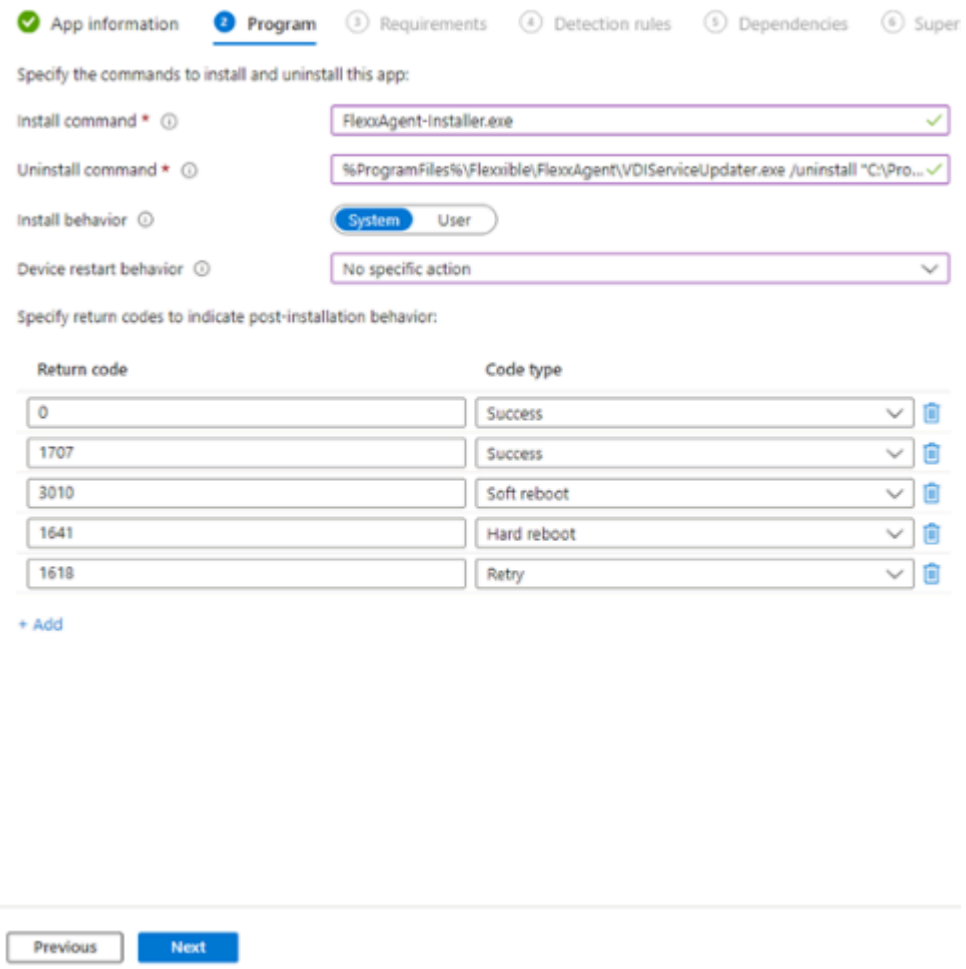
    - Install command: `FlexxAgent-Installer.exe`

> Note: if necessary, you could introduce proxy values in this command.

    - Uninstall command: `%ProgramFiles%\Flexxible\FlexxAgent\VDIServiceUpdater.exe /uninstall "C:\Program Files\Flexxible\FlexxAgent\FlexxAgent.exe" /quiet`

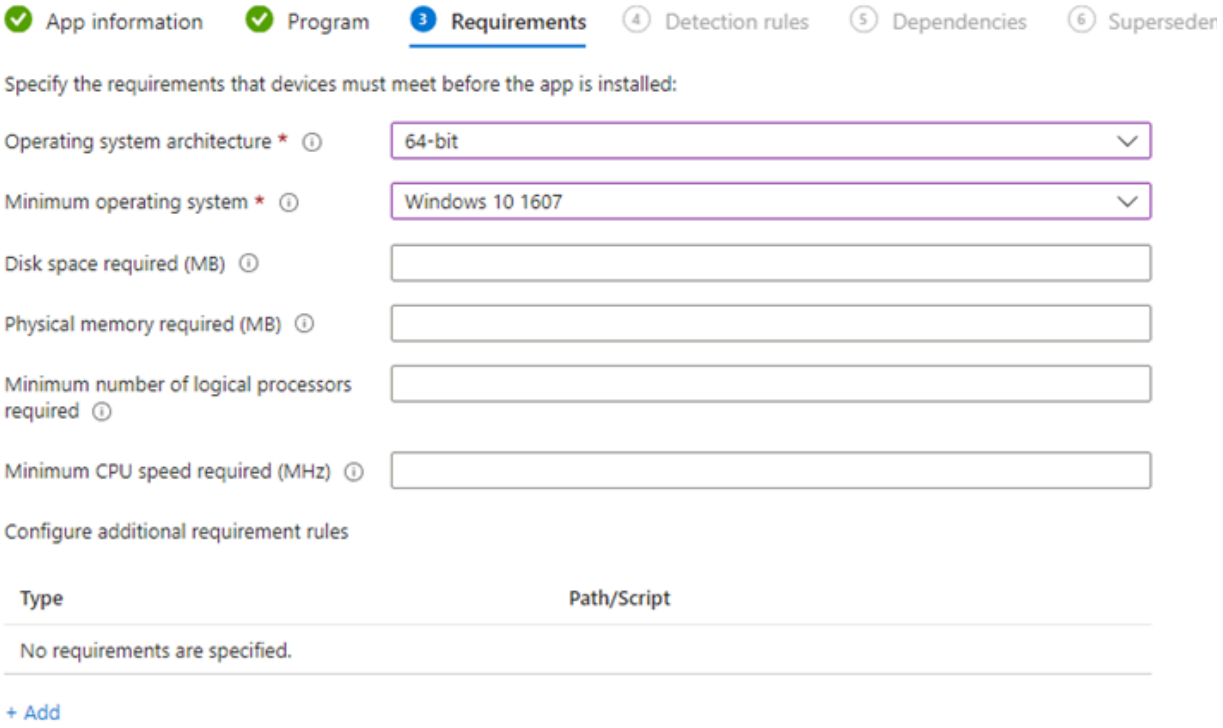
> Note: double quotes are mandatory.

    - Install behavior: system
    - Device restart behavior: no specific action



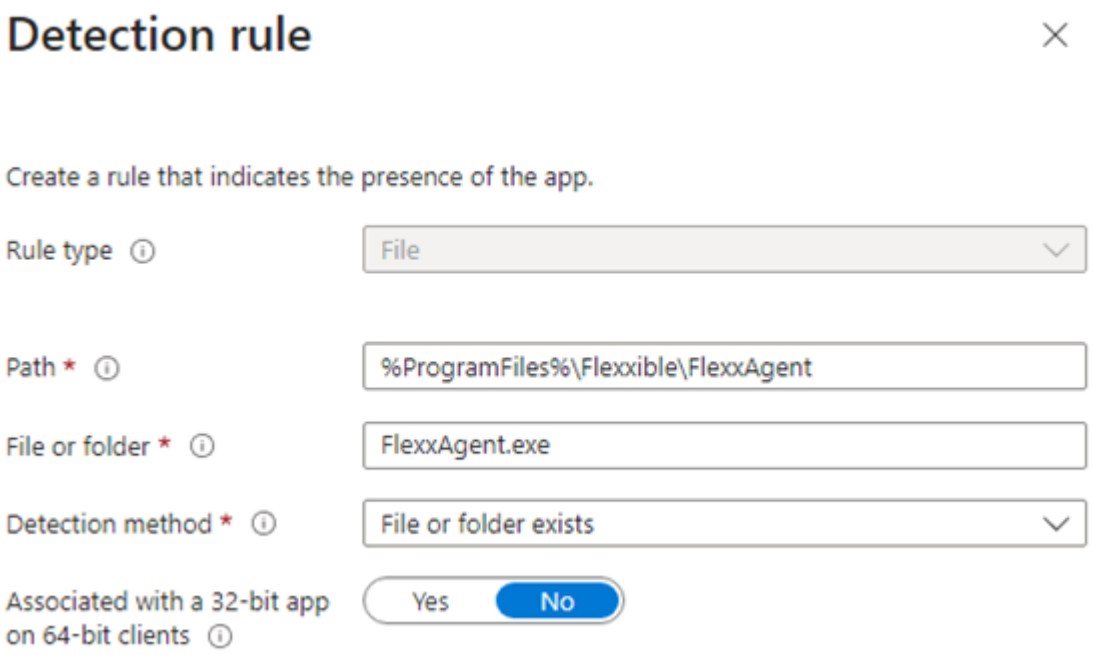

13. On the `Requirements` tab, you need to include information about the operating system architecture:

    - Operating system architecture: 64-bit
    - Minimum operating system: Select accordingly to the version used in the current installation (device fleet). For example, the minimum: `Windows 10 1607`.

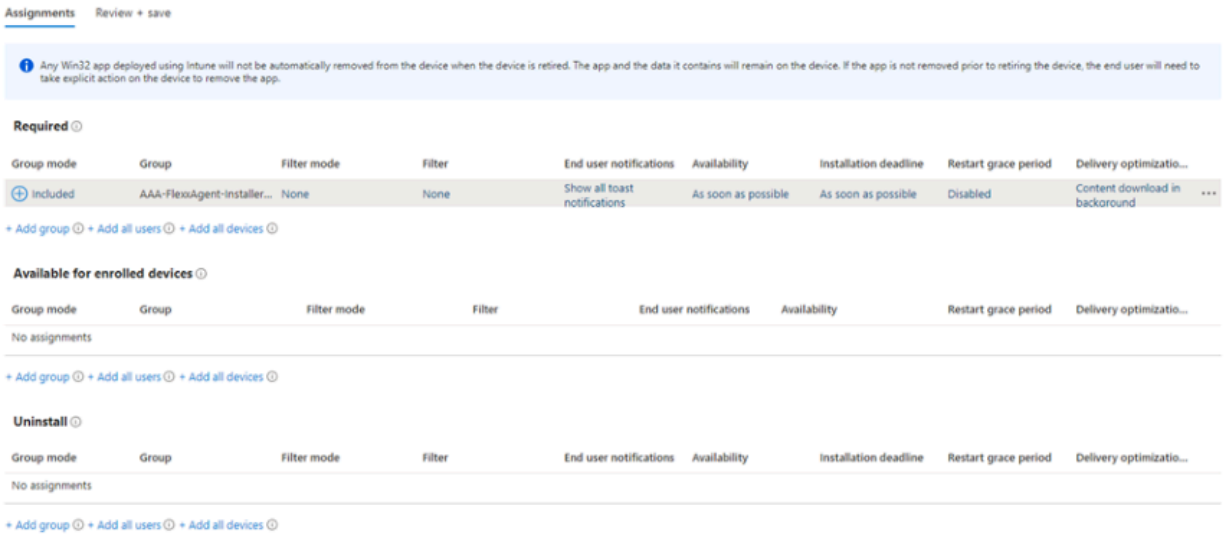



14. On the `Detection Rules` tab, select `Manually configure detection rules` and click on the link `+Add`. In the rule you are going to create, fill in the following fields:

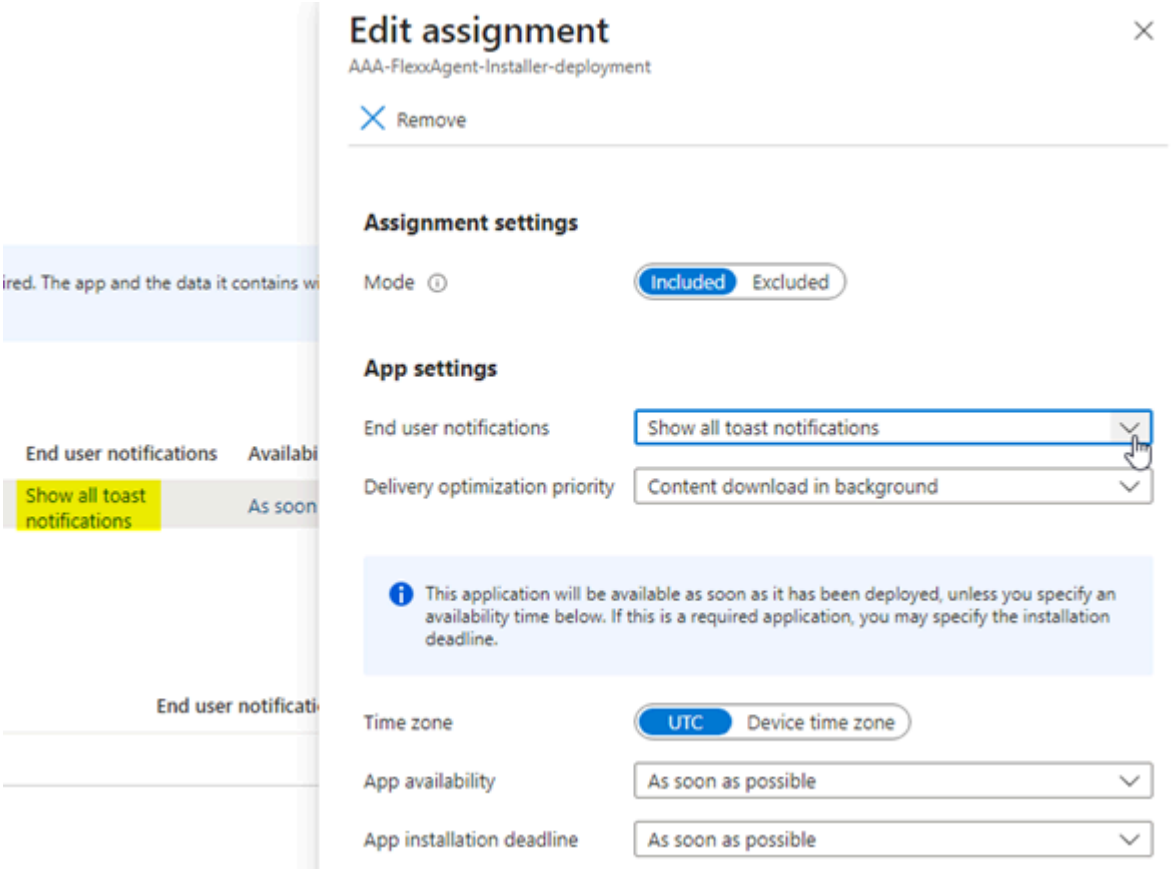
    - Rule type: File
    - Path: %ProgramFiles%\Flexxible\FlexxAgent
    - File or folder: FlexxAgent.exe
    - Detection method: File or folder exists
    - Associated with a 32-bit app on 64-bit clients: No




15. On the `Assignments` tab, create an Azure Entra ID security group containing the devices on which this package is to be installed.

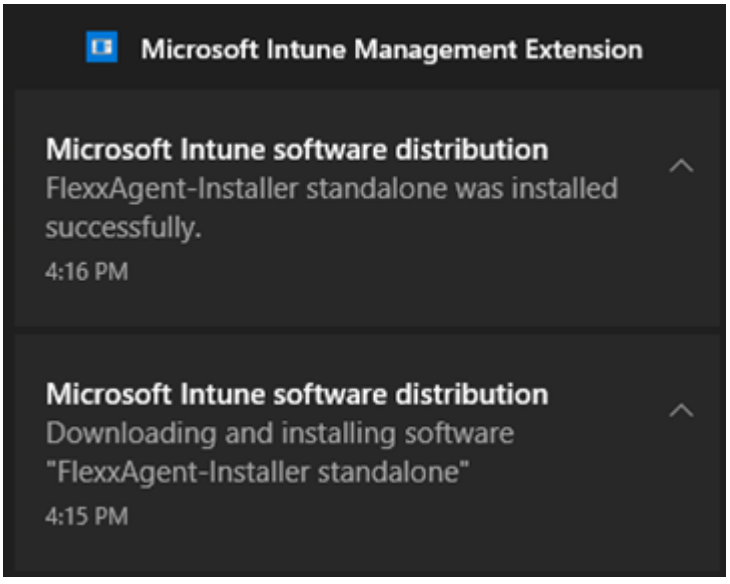



16. At this point, make sure to select the appropriate notification for the end user.




17. Click on `+Add all devices` so that it is deployed on all devices enrolled in Intune.

18. Once you click `Review+Create`, the deployment will begin. You need to allow at least one hour for it to take effect and complete.



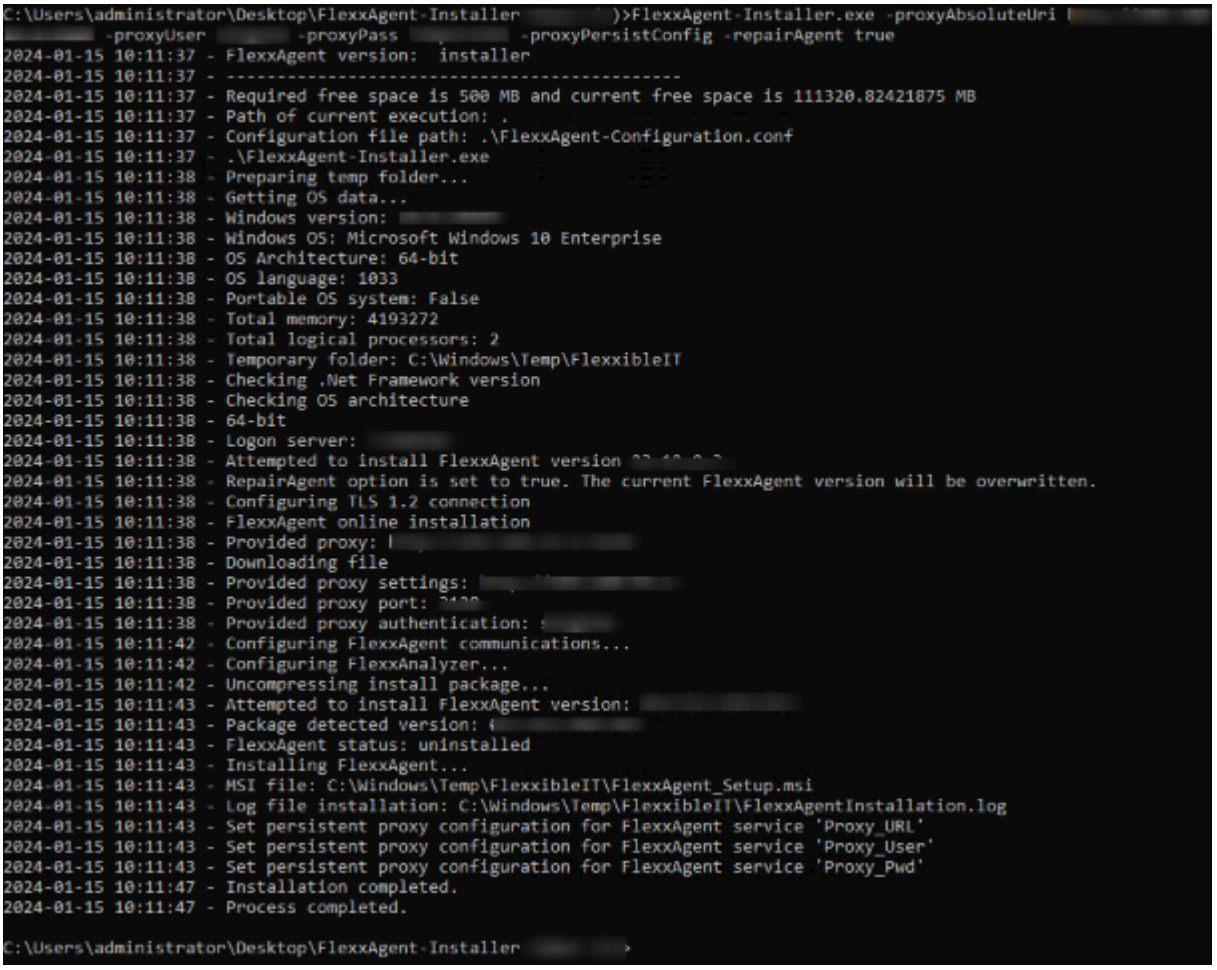
# FlexxAgent / Guides and tutorials / Install FlexxAgent configuring proxy

FlexxAgent needs to have internet connectivity. In many organizations, users connect to the internet using a proxy server.

## Example

In the installation of FlexxAgent, the proxy server configuration can be included using the following command line options:

```
FlexxAgent-Installer.exe -proxyAbsoluteUri <http(s)://ip.ad.dre.ss:port> -proxyUser ProxyUserName -proxyPass ProxyUserPassword -proxyPersistConfig -$True
```



# Explanation of the options

- **proxyAboluteUri**: the address of the proxy server, expressed as a full “URL”; for example `https://192.168.1.1:3128`.
- **proxyUser**: the user identifier for authentication on the proxy server; for example `Administrator`. This parameter is optional if the proxy server does not require authentication.
- **proxyPass**: the password for the above identifier. This parameter is optional when the proxy does not require authentication.

The value can be plain text (not recommended) or base64 encoded, preceded and followed by the string “&&&"; for example `&&&VGhpc0lzTjArQCQzY3VyZVBAJCR3MHJk&&&`, in any case, FlexxAgent encrypts this value at startup.

> For base64 encoding, you can use any generator, such as https://www.base64encode.org/.

## proxyPersistConfig

This parameter must be specified to persist the proxy configuration entered in the other parameters. If not specified, the proxy configuration will only be used in the installation process and will not affect subsequent executions of FlexxAgent.

For Windows operating systems, the proxy configuration data will persist in the registry, within the following keys:

#### Key Proxy_URL

- Key path: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Flexxible\FlexxAgent\Communications
- Key Name: Proxy_URL
- Key type: REG_SZ
- Supported values: the URL and port; for example 'http://192.168.1.1:3128' or 'https://192.168.1.1:3128'

#### Key Proxy_User

- Key path: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Flexxible\FlexxAgent\Communications
- Key Name: Proxy_User
- Key type: REG_SZ
- Supported values: the username to authenticate to the proxy; for example 'Administrator'. It can be bypassed for unauthenticated proxies.

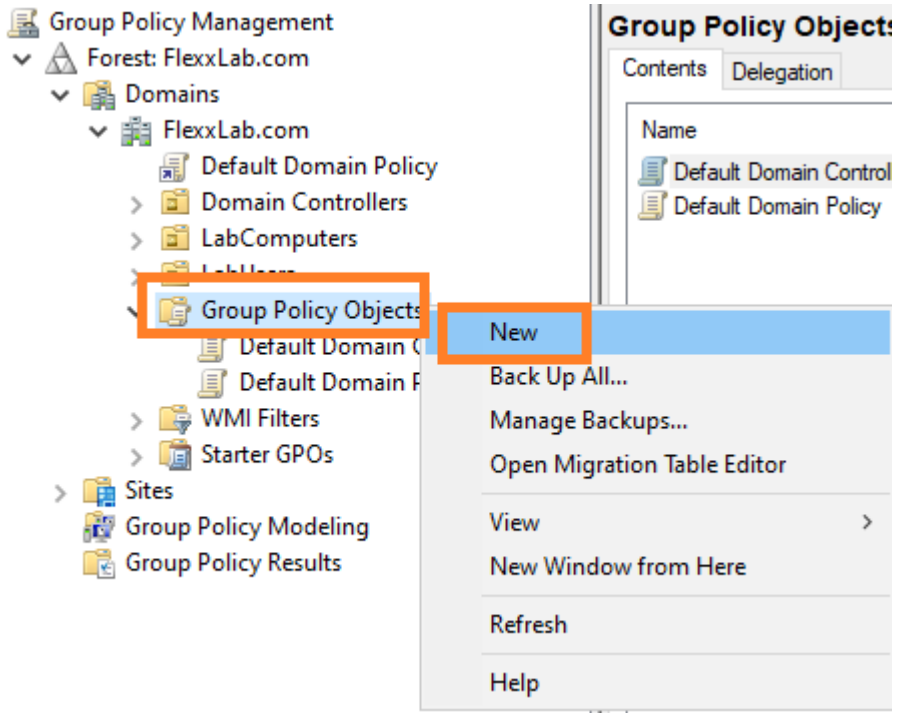
#### Key Proxy_Pwd

- Key path: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Flexxible\FlexxAgent\Communications
- Key Name: Proxy_Pwd
- Key type: REG_SZ
- Accepted values: the password for authenticating to the proxy. It can be bypassed for unauthenticated proxies. The Proxy_Pwd key value can be set in plain text (not recommended) or base64 encoded and enclosed by «&&&»; for example `&&&VGhpc0lzTjArQCQzY3VyZVBAJCR3MHJk&&&` for the “Proxy_Pwd” value.

# FlexxAgent / Guides and tutorials / Apply proxy configuration via group policies (GPO)

In many cases, the organization's connectivity goes through a proxy; it could be for security, performance, or other reasons. This proxy configuration in FlexxAgent can be done in two ways: using a group policy (GPO) or during the agent installation. To configure the proxy using a group policy, follow these steps:

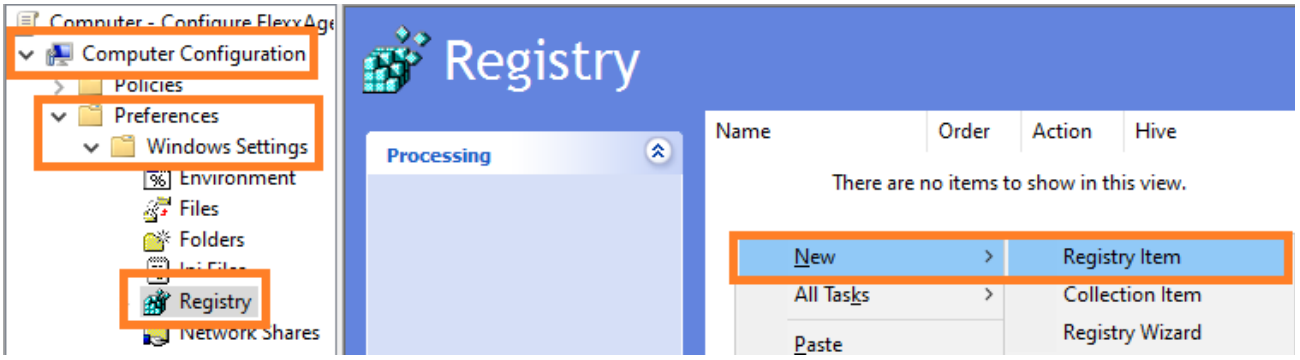
1. Access the domain controller's group policy management console. Create a new policy using the `New` option from the menu that appears when you right-click on `Group Policy Objects`.




2. Give the new policy an appropriate name and click the `OK` button.

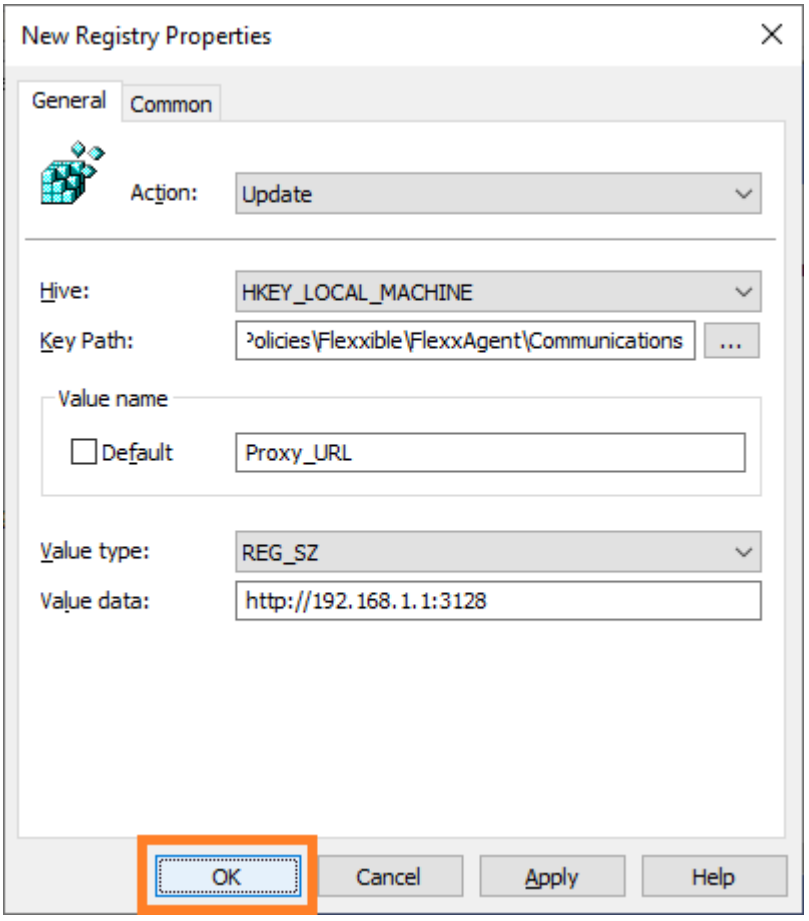
3. Select the policy with the right mouse button and edit it (select `Edit...`)

4. In the edit window, expand `Computer Configuration`, `Preferences`, and `Windows Settings`. Select `Registry` and then `New` -> `Registry Item`.

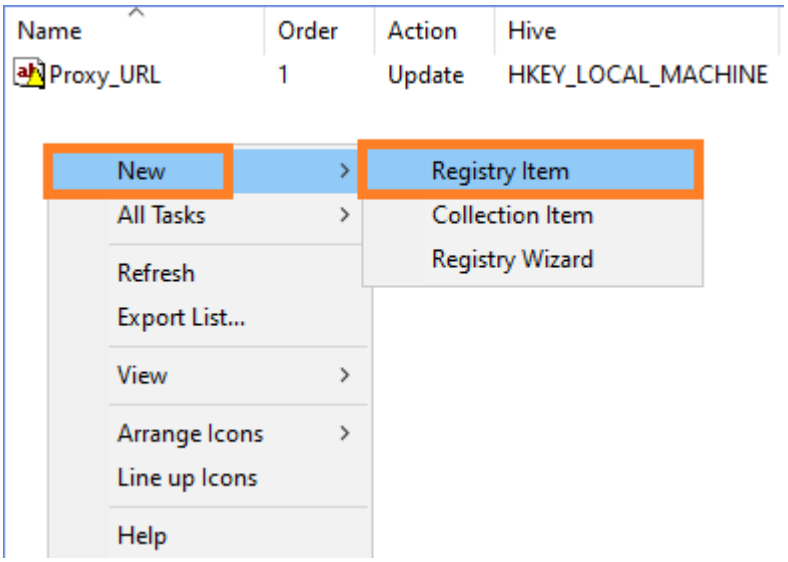



5. Add the following information and click `OK`.

- Action: Update
- Key path: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Flexxible\FlexxAgent\Communications`
- Value Name: Proxy_URL
- Value type: REG_SZ
- Value data: the proxy's address (URL) and port number. For example `https://192.168.1.1:3128`.



6. In the right panel, add a new registry entry again with the right mouse button, selecting `New` -> `Registry Item`.




7. Add the following information and click `OK`.

- Action: Update
- Key path: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Flexxible\FlexxAgent\Communications`
- Value Name: Proxy_User
- Value type: REG_SZ
- Value data: the username to authenticate to the proxy server. For example `Admin`.

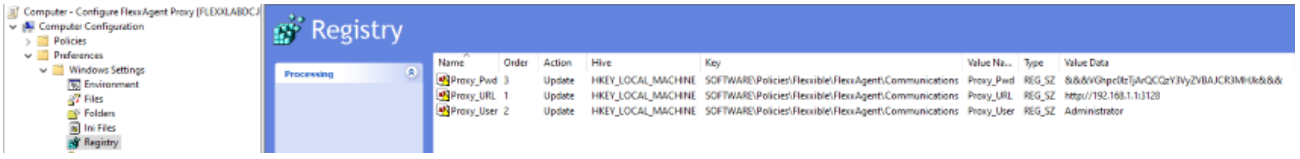
8. In the right panel, add a new registry entry again with the right mouse button, selecting `New` -> `Registry Item`.

9. Add the following information and click `OK`.

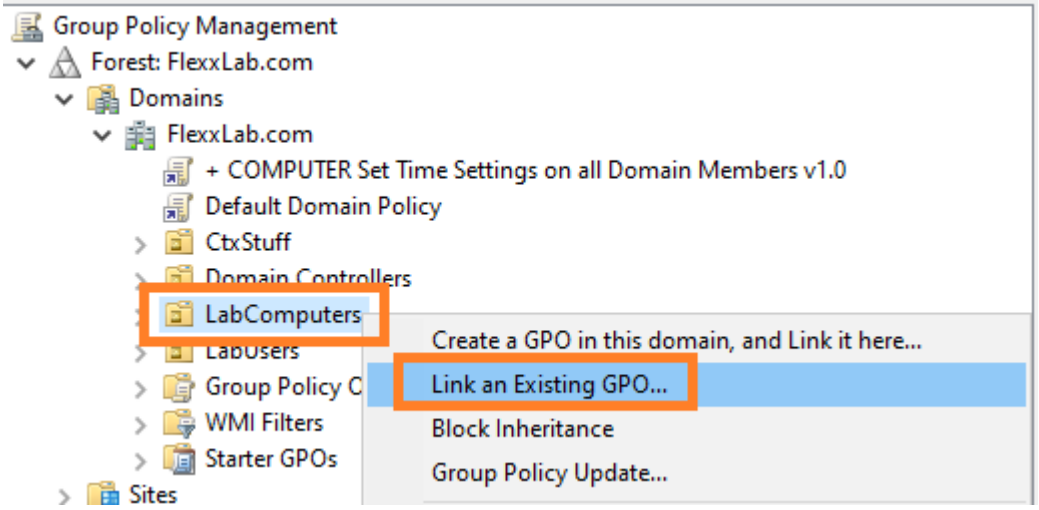
- Action: Update
- Key path: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Flexxible\FlexxAgent\Communications`
- Value Name: Proxy_Pwd
- Value type: REG_SZ
- Value data: the password for authenticating to the proxy server, corresponding to the user configured in the previous step.

- The `Proxy_Pwd` key value can be filled in plaintext (not recommended) or encoded in base64 by putting the string `&&&` before and after it. Example: `&&&VGhpc0lzTjArQCQzY3VyZVBAJCR3MHJk&&&`.
- In any case, FlexxAgent encrypts the value of this field at startup.
- To encode the password in base64, you can use a web service like https://www.base64encode.org/.

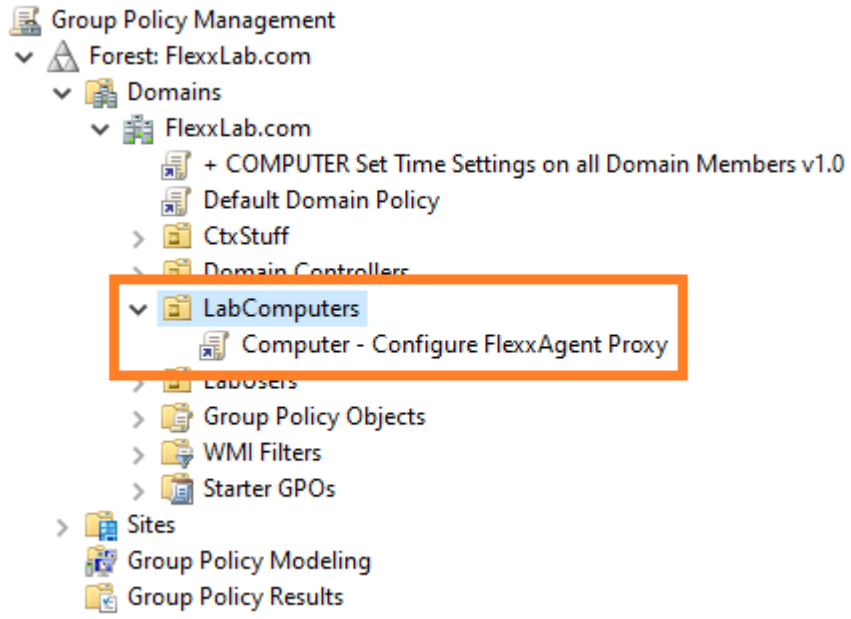
10. Three registry entries will have been created in the group policy.



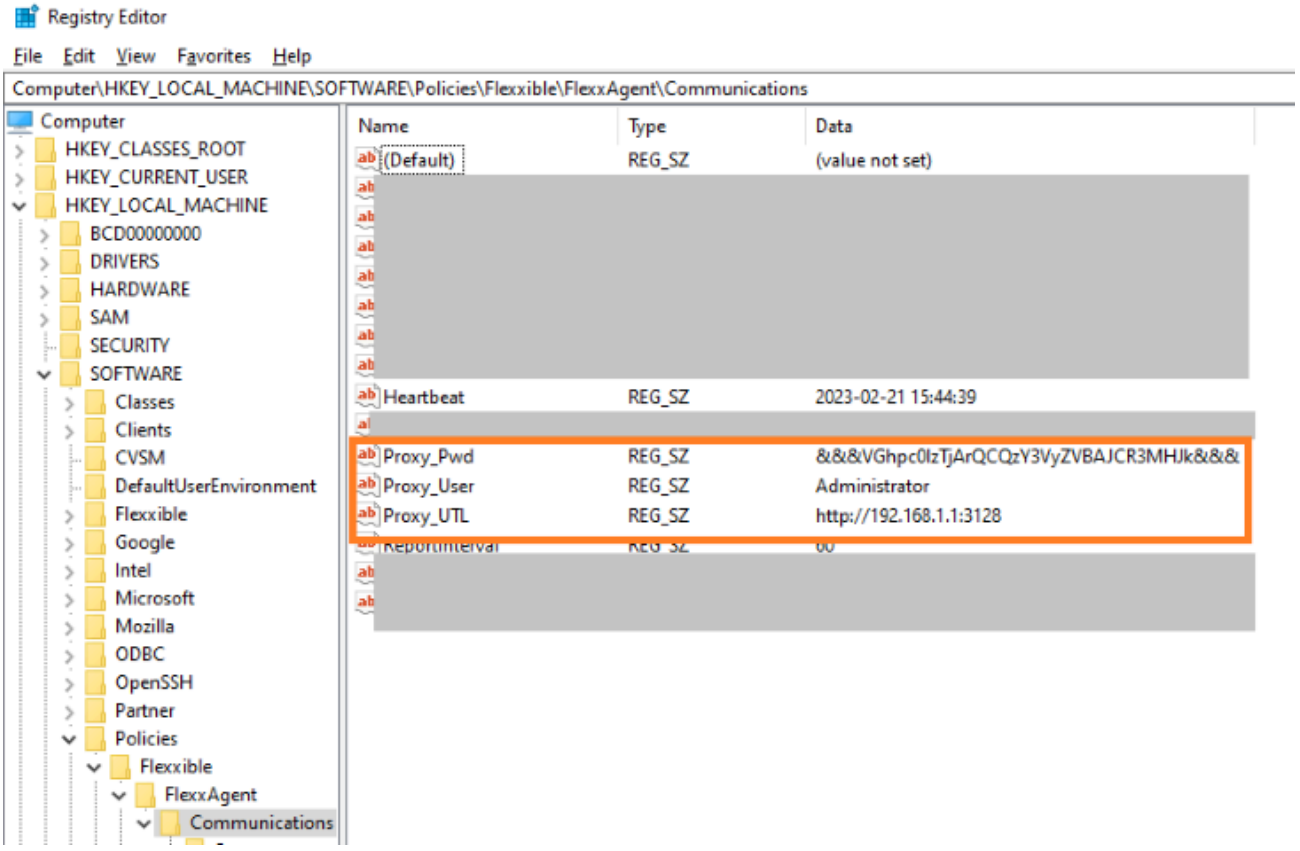

11. Close the editor.
12. With the right mouse button, select the list of devices that will receive this configuration within the domain controller (under the domain or organizational unit) and select `Link an Existing GPO`.




13. Select the previously created group policy.
14. The policy is linked to the devices selected in the domain controller.




15. **Optional step**: if you want to verify on a computer that the group policy has been applied correctly, you need to restart the computer. Once it starts, you can go to the registry editor and check that the entries were created correctly.



# FlexxAgent / Guides and tutorials / Deployment of FlexxAgent with Group Policy (GPO)

FlexxAgent can be deployed using group policies in Windows (GPOs). You need access to the agent installation package, which can be downloaded from the Flexxible portal.

## Deploying

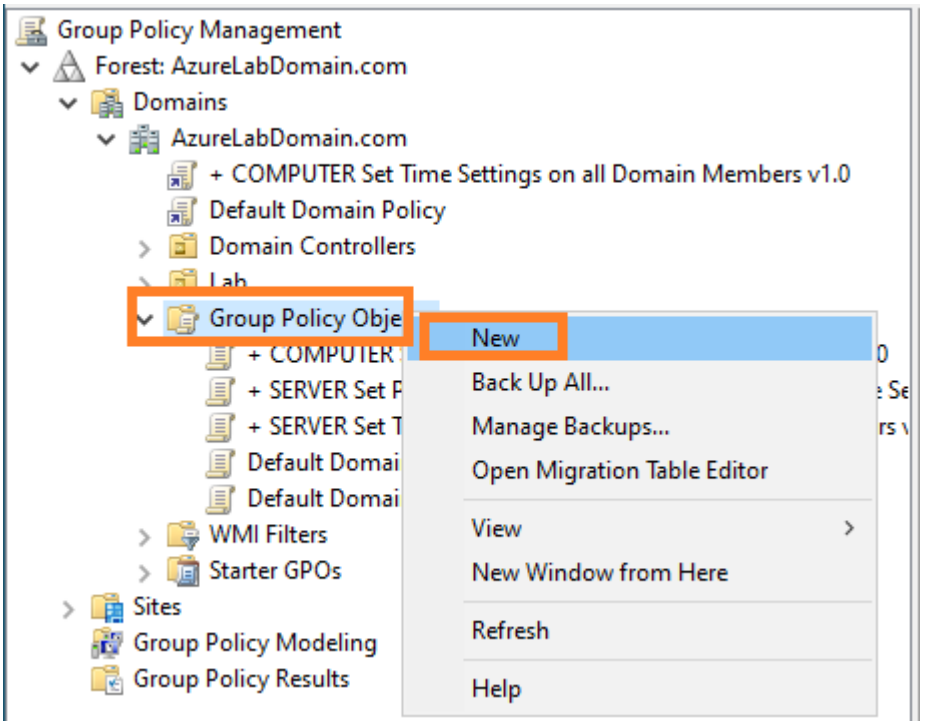
1. Create a Powershell `script` called `Install.ps1` with the following content:

   Start-Process `Path to the file\FlexxAgent-Installer.exe`

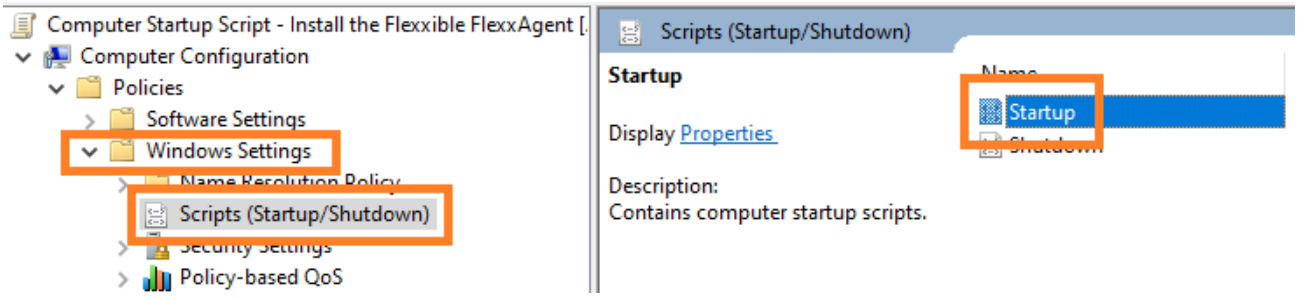
   Example: Start-Process `C:\Temp\FlexxAgent-Installer\FlexxAgent-Installer.exe`

> Note: Make sure that, apart from the executable, the line includes the necessary installation parameters, such as the proxy, if needed.

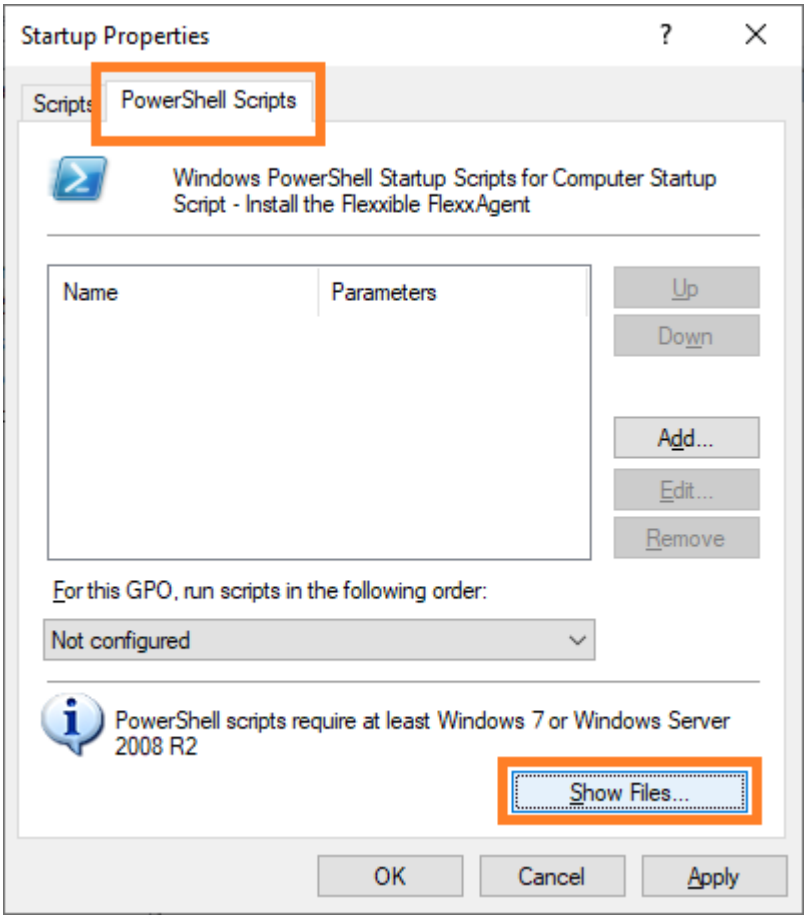
2. Save the file for later use.
3. Run the group policy management console in a domain controller that has remote computer management tools installed.
4. Create a new group policy within the group policy container.



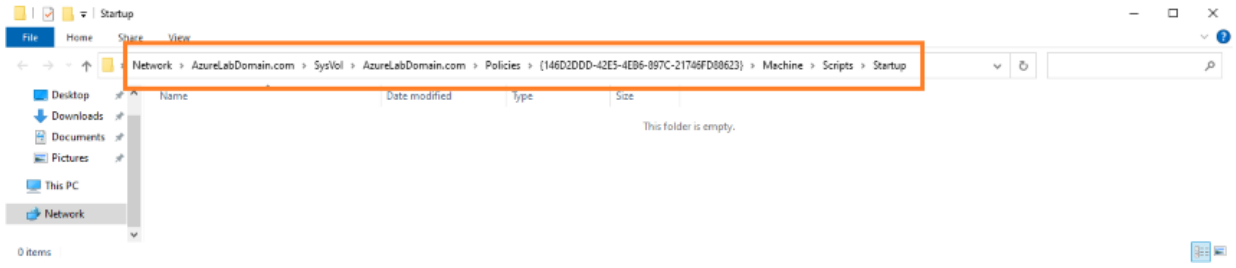

5. Give the new policy a name. Choose one that is meaningful.
6. Right-click on the group policy and select `Edit`.
7. Expand the tree `Computer Configuration` -> `Windows Settings` and select `Scripts (Startup/Shutdown)`



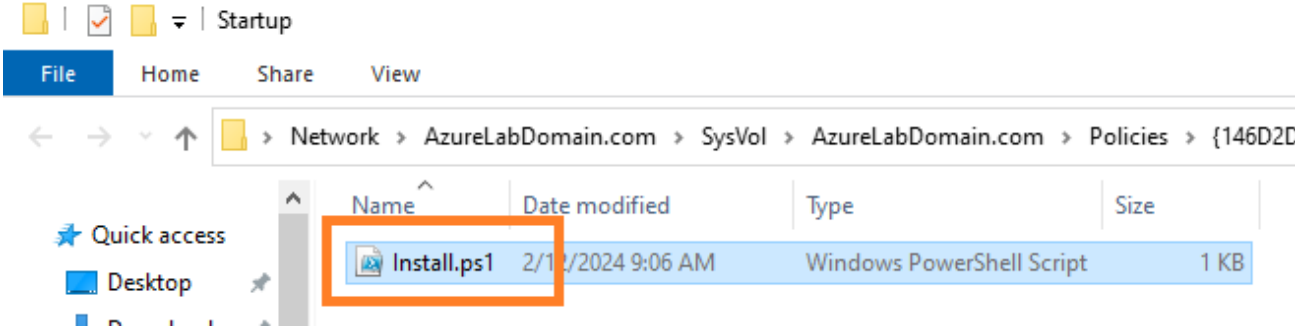

8. A dialog will appear in a new window. Select `PowerShell Scripts` in it. Next, click on the `Show Files...` button



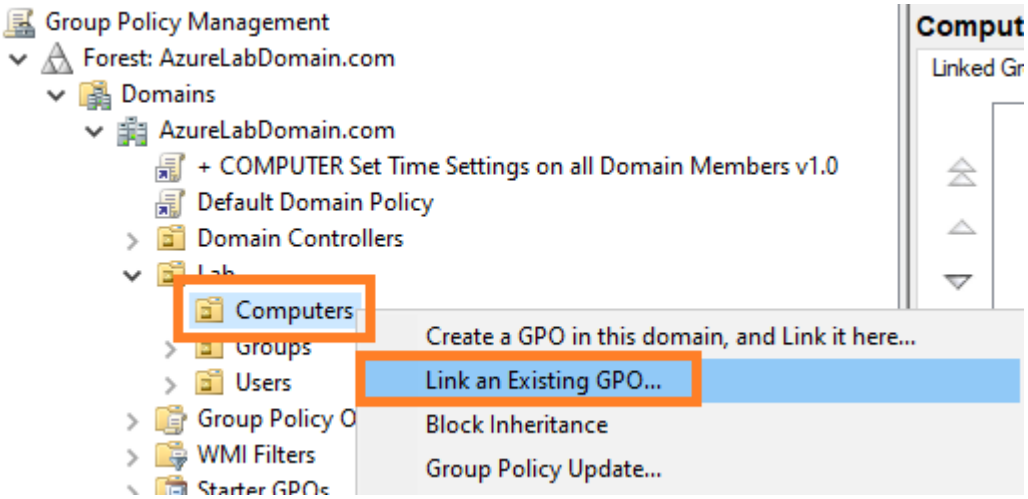

9. The network folder where the scripts for the group policy are stored will open.




10. Copy the file `Install.ps1` that was created at the beginning and paste it into the network folder for storing Group Policy scripts.



11. You can now close the Windows Explorer window that accessed the folder with the group policy scripts.
12. The startup script properties modal window will be visible again. Click on the `Add...` button.
13. A file selection dialog will appear. Find the script to use by clicking on the `Browse...` button.
14. The previous path will open, where the file created at the beginning of the procedure will be. Double-click on it or select it and click the `Open` button.
15. Once the file is selected, select `Ok` to close the dialog. The file will appear in the configuration modal window.
16. Select `OK` to close this window. You'll return to the group policy editor. This window can be closed.
17. Find the organizational unit branch, within the domain controller where the computers for FlexxAgent installation are located. Select the branch and right-click on it. Select `Link an Existing GPO`.

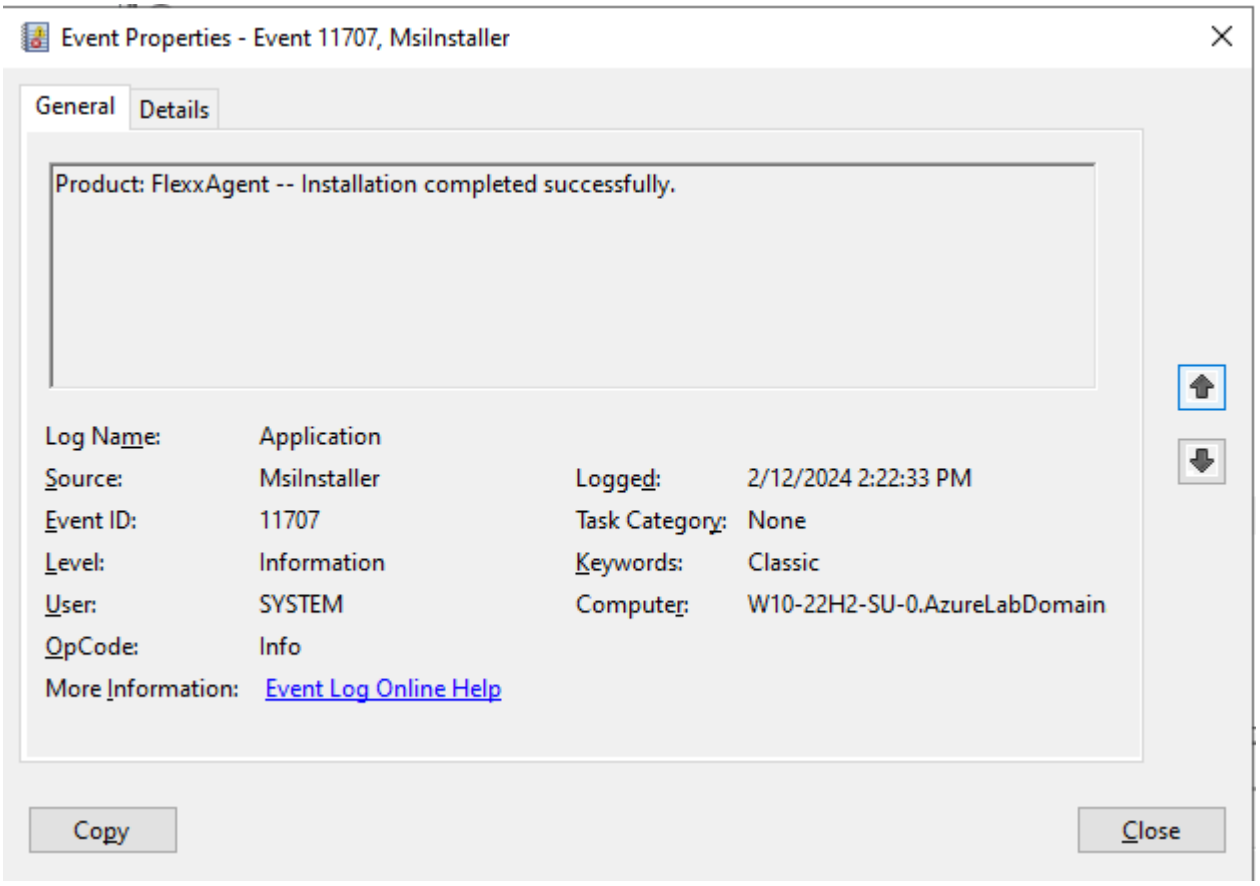



18. A selection dialog will appear where the previously created policy will be selected. Once selected, click `OK`.

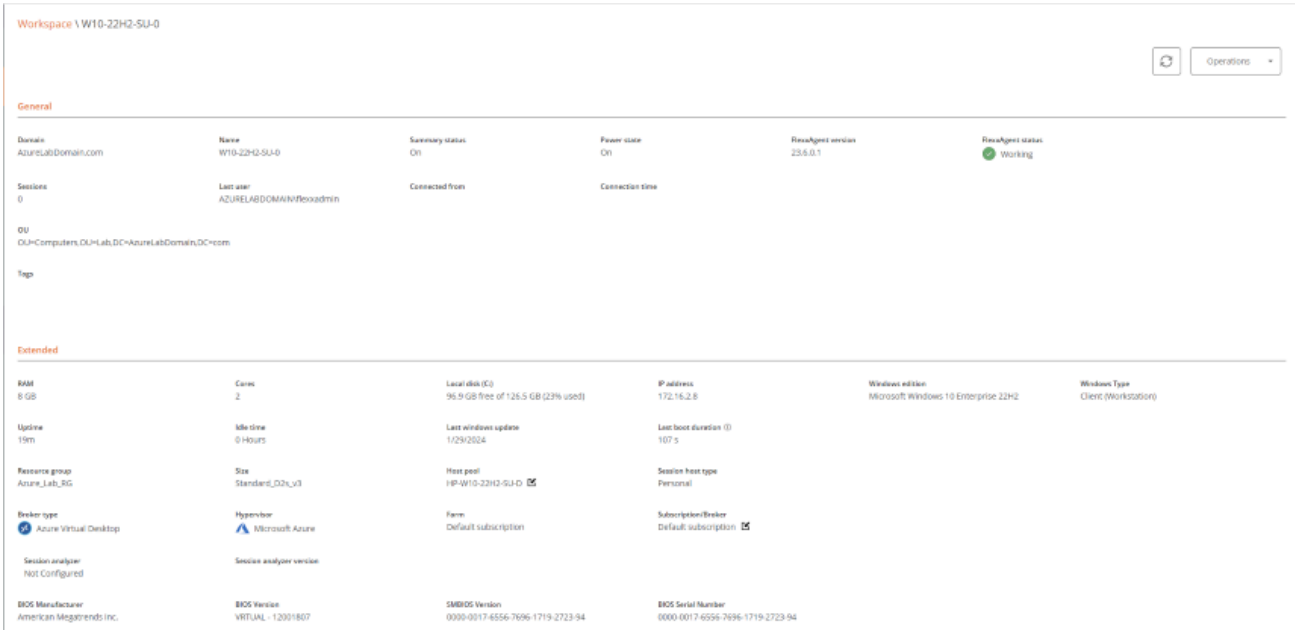
# Verification

To validate the installation of FlexxAgent within a domain machine, restart a machine in the domain for the group policy to take effect. After the restart, access the application event

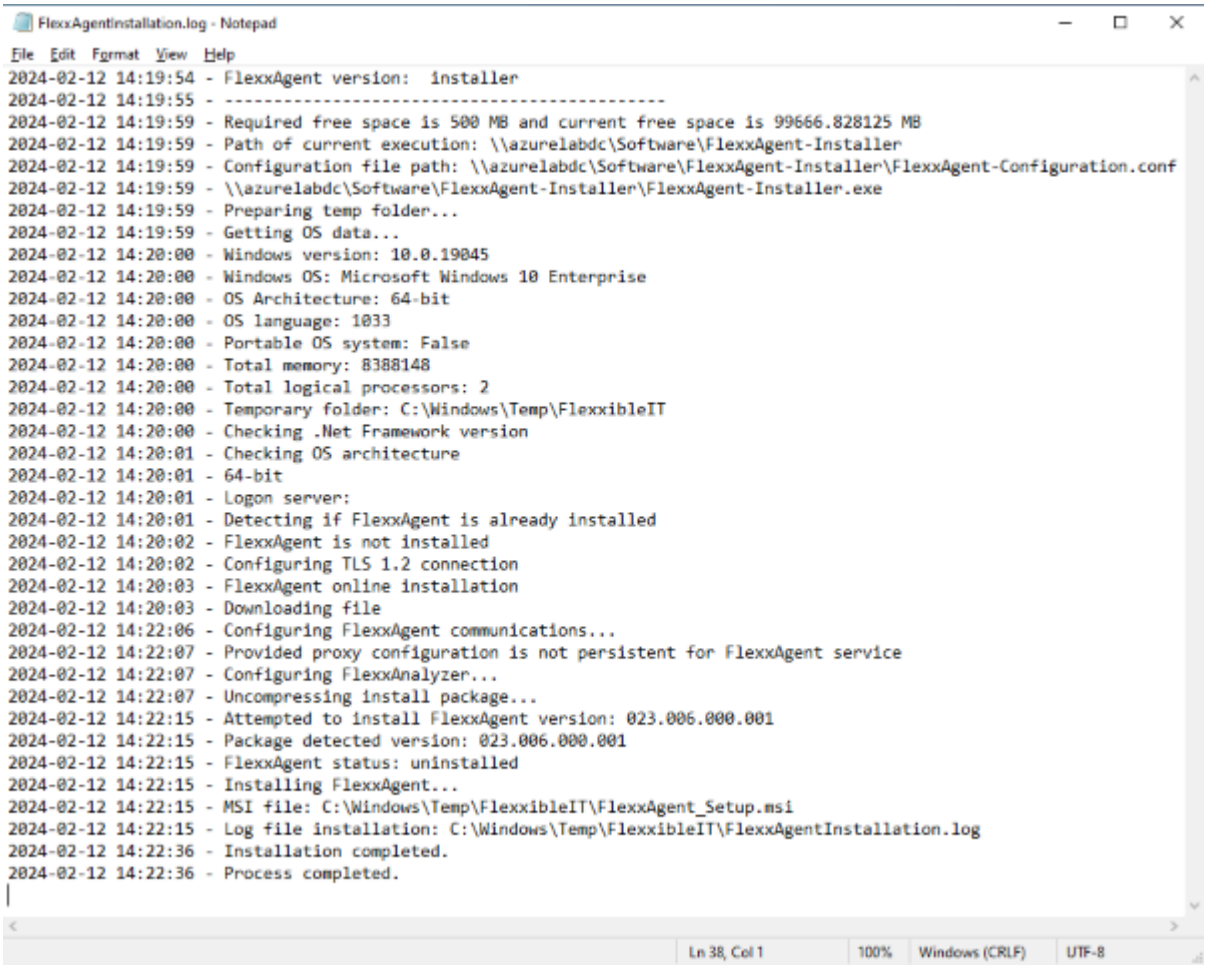
log and you will see several events generated during the installation and initial run of FlexxAgent, including:




After a few minutes, you will see the new device registered in the Workspaces module and in the `Workspaces` view of the Portal.

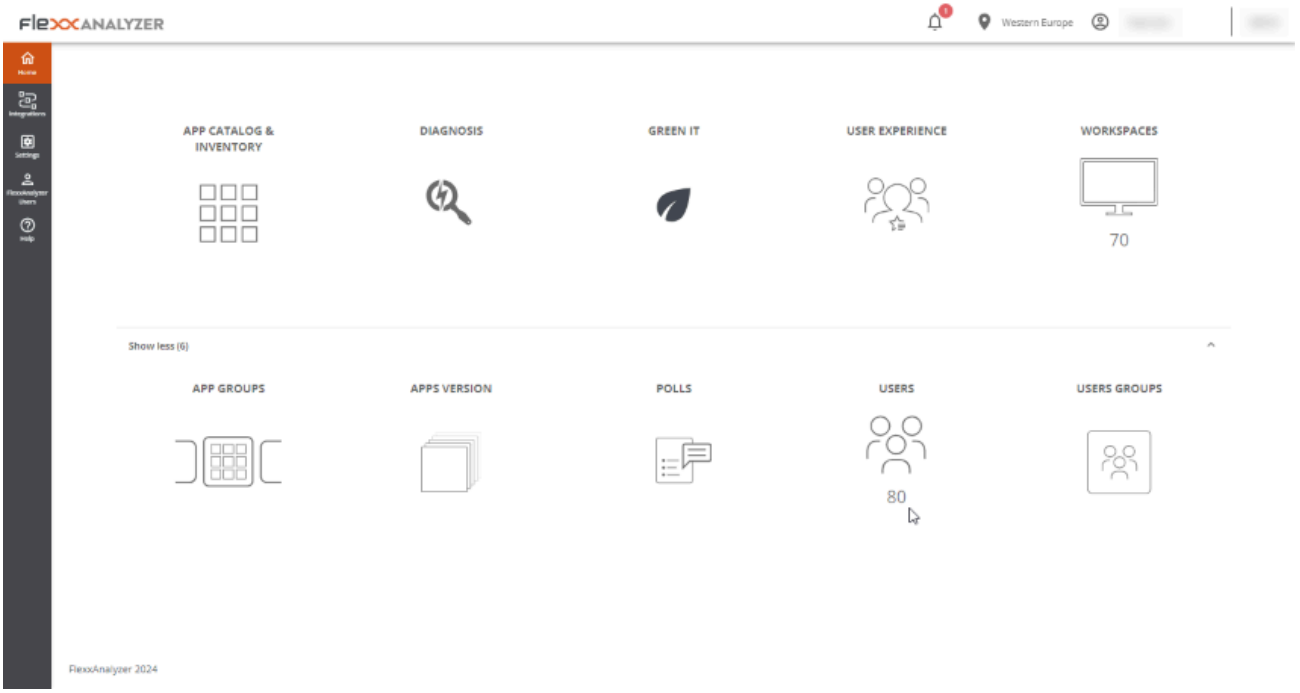


The installation log can be seen in detail in the file `C:\Windows\Temp\FlexxAgentInstallation.log`.



# Analyzer

Analyzer is a comprehensive solution for managing digital experience (DeX), responsible for collecting analytical data from devices and evaluating application performance.




# Included tools

With Analyzer, you can have a series of tools that allow you to perform a thorough analysis of user experience, both individually and organizationally.

It also collects information about paper printing and the organization's carbon footprint, as well as cataloging and inventorying installed applications.

It allows conducting surveys to obtain a subjective evaluation of users' perception, as well as detailed diagnostics of resources consumed per user session or per application in each session.

Tools included in Analyzer:

- App Catalog & Inventory: offers an inventory of applications and their versions in the organization.

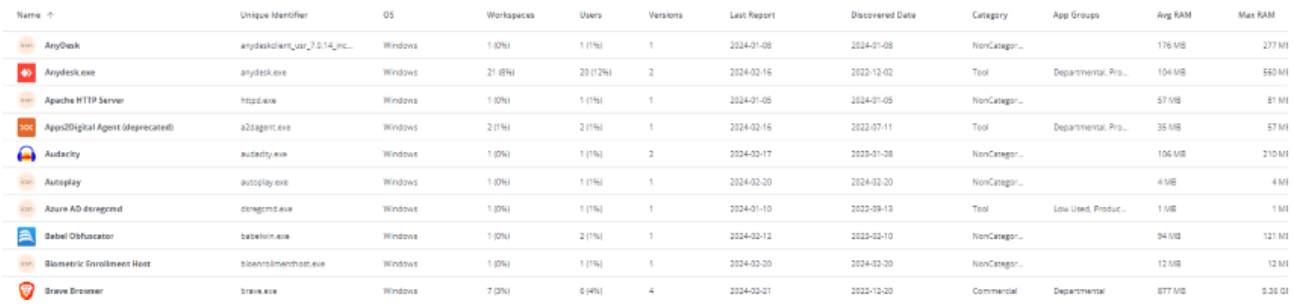
- Diagnosis: enables a diagnostic view and allows viewing the usage details of resources and applications by devices in configurable time slots.
- Green IT: allows evaluating the carbon footprint generated by printing and the electrical consumption of devices and their peripherals.
- User experience: helps detect and resolve issues by analyzing device performance and user sentiment.
- Workspaces: offers an inventory view of devices and collects information on detected issues.
- App Groups: allows creating groups of applications for joint analysis.
- Apps version: offers a condensed view of the most versioned applications in a given time period.
- Polls: allows configuring the sending of surveys to capture user sentiment and use this data to build the experience index (UXI).
- Users: contains information on detected users and details the applications and devices used historically for each of them.
- User Groups: allows creating groups of users.

# Web Interface

## List Views

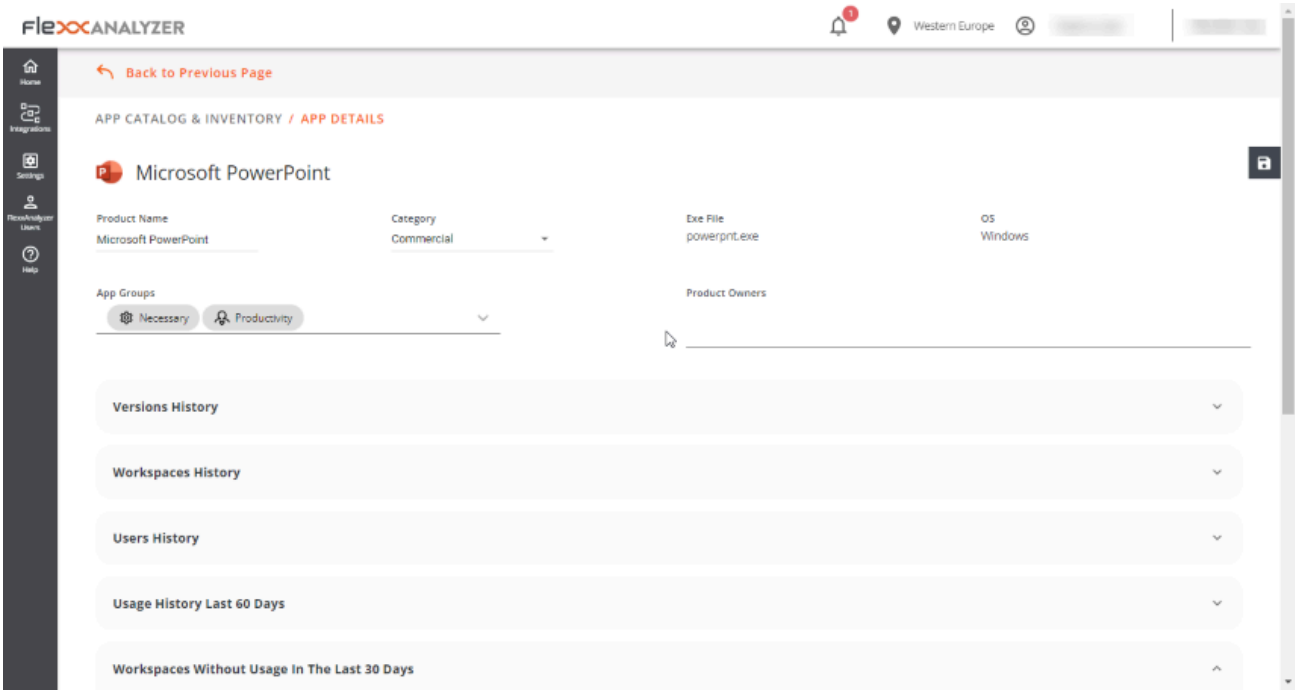
List views allow filtering and selecting items in the different options of the module.

Results will appear in a list format, where you can make use of filters or navigate between different result pages.



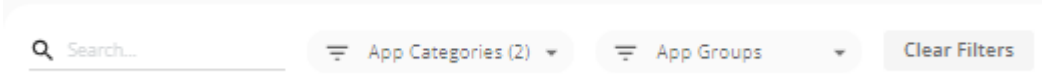
# Detail Views

When an item is selected from the list view, you access the detail view, which allows consulting data of the selected item in more depth.



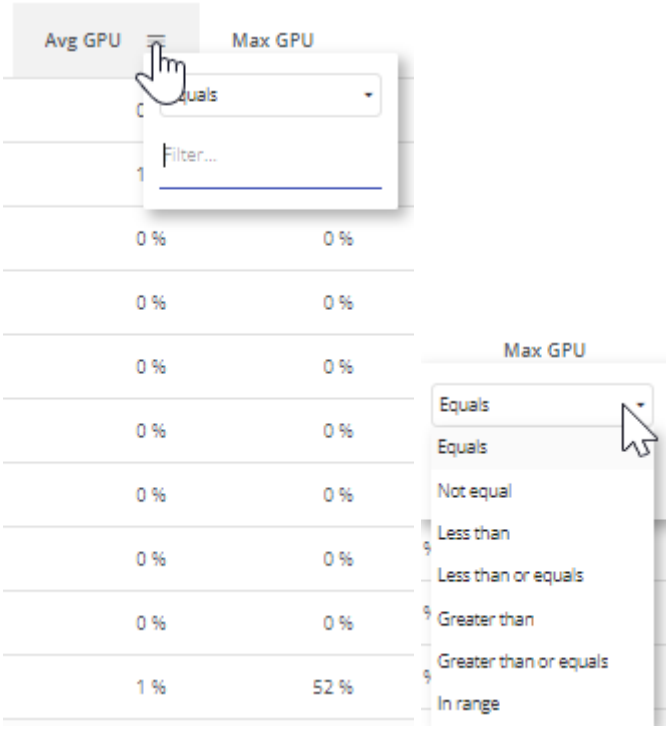

# Search options

From any of the list views, you can access search options that allow locating a record within all results offered in the list.




# Column filter

List views contain a series of filters with several logical operators (also known as boolean operators) that allow comparing values, depending on the information shown in the column.



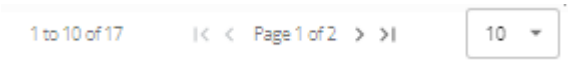

Logical operators that can be operated with:

| Condition | Caption |
|---|---|
| Equal to | The condition for filtering results must be equal to the value stated. |
| Not equal to | The condition for filtering results must be different from the value stated. |
| Greater than | The condition for filtering results must be greater than the value stated. |
| Less than | The condition for filtering results must be less than the value stated. |
| Greater or equal to | The condition for filtering results must be greater than or equal to the value stated. |

| Condition | Caption |
| --- | --- |
| Less or equal to | The condition for filtering results must be less than or equal to the value stated. |
| In range | The condition for filtering results must be between the values stated. |
| Start with | The condition for filtering results must start with the value stated. |
| End with | The condition for filtering results must end with the value stated. |

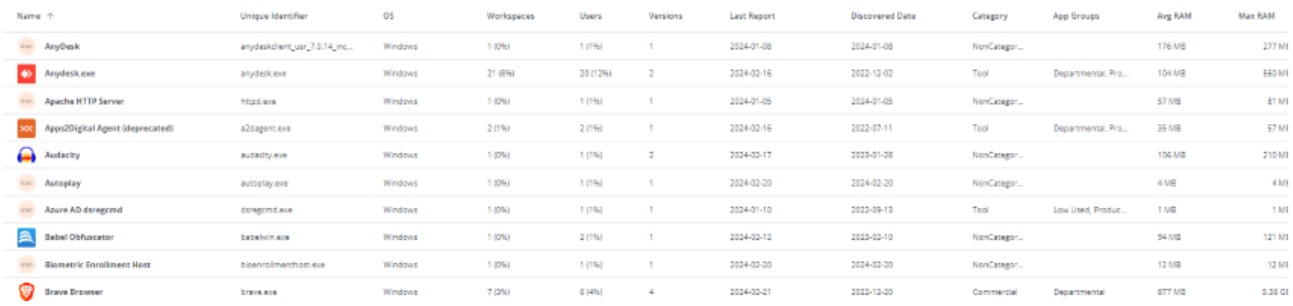
## Page navigation

At the bottom of any list view is the page navigator. It's useful for navigating between pages of results.



# Analyzer / App Catalog & Inventory

From the `App Catalog & Inventory` option you can see a list of all the applications that have been discovered by FlexxAgent. At the top, next to a dropdown menu, there is a search bar that filters categories and application groups.



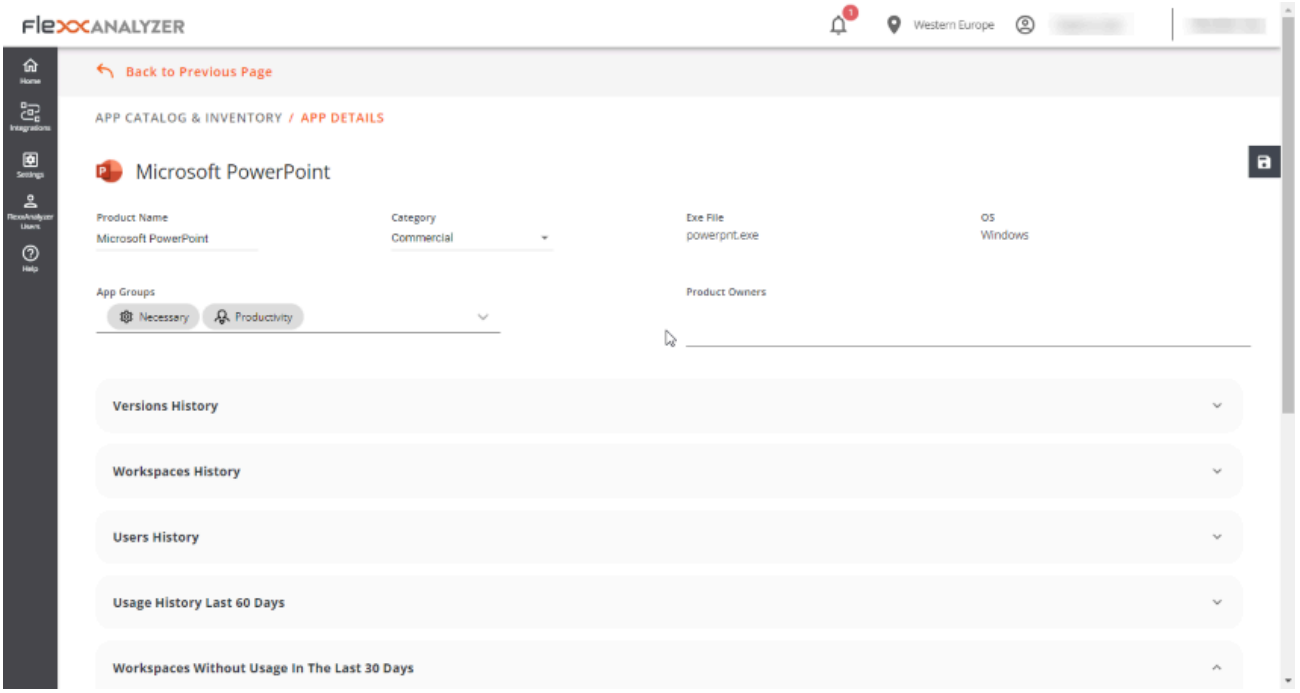

## List view

In the list view you can see the following information:

- Product Name
- Application unique identifier
- Operating system for which the application is designed
- Number and percentage of devices running the application
- Users and percentage out of total who have run it
- Number of versions
- Date of last record where activity of this application was found
- Discovery date
- Category
- Application group
- Average and maximum values on CPU, RAM, GPU and IOPS usage

## Detail view

When accessing the desired application, it is possible to see more specific information and assign `Product Owners` to the application.




The fields `Product Name`, `Category` or `App Groups`, at the top of the list view, can be edited, and saved through the `Save changes` sliding button on the right side.

## Version History

From `Version History` you can access the different registered versions of the selected application. Here you can check:

- `Product Version`: the registered version or versions of the product
- `Image`: version architecture type (32 or 64 bits)
- `Discovery Date`: date of first record of this version
- `Last Report`: date of last registered report

## Workspaces history

It provides details of the recent usage of the application on devices, each application contains:

- Device Name
- Reported version

- Report date

## Users History

It provides details of recent user usage, each application contains:

- Username
- Reported version
- Report date

## Usage History Last 60 Days

From this section, you can see a list of different user sessions that have used the selected application during the last 60 days, it contains:

- Username: user session in which the execution of this application was recorded.
- Workspace: device on which the execution of this application was recorded.
- Days: number of days, out of the last 60, that the application was detected running in this user session.
- Last Report: date of the last registered report in the user session.

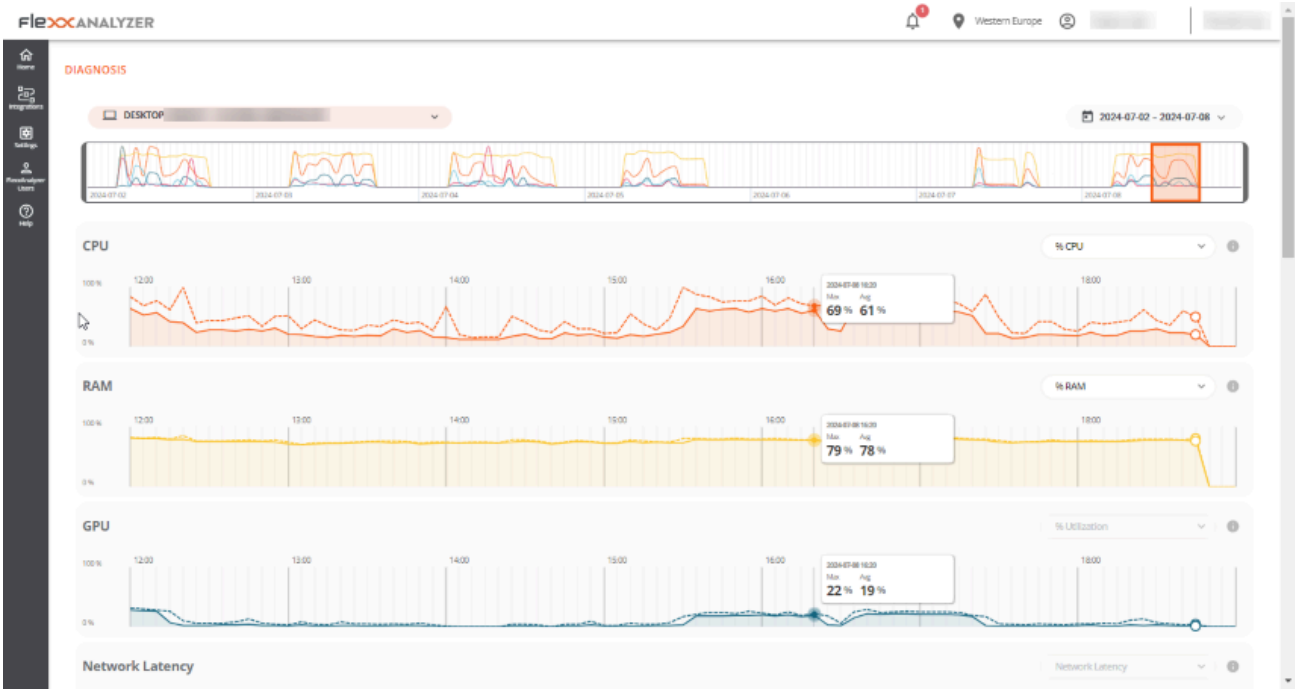
## Workspaces without usage in the last 30 days

This list shows the devices that have the application installed but have had no usage in the last 30 days, which helps identify opportunities for license optimization. Includes:

- Device Name
- Installation date
- Last detection report

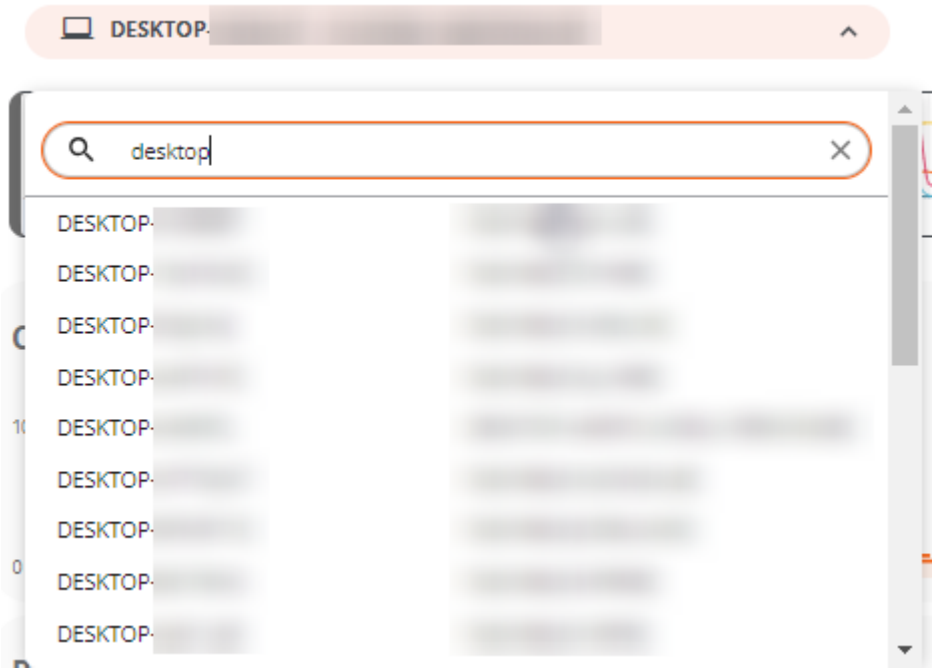
# Analyzer / Diagnosis

From the `Diagnosis` option, you can perform a detailed analysis of a device's resource consumption, as well as the applications and processes used in the user's session.



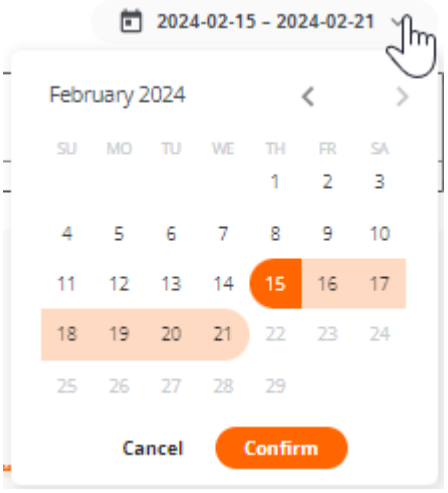

# Web Interface

From the `Diagnosis` dropdown menu, you can search for a device and the user session you want to analyze. If you start typing a username, the dropdown menu will filter to show only devices that match that name.




It's possible to select a one-week date range for the analysis; by default, data from the last seven days will be shown, although you can select a custom period by clicking the dropdown list. Only the devices used in the selected period will appear.

When you want to explore a different time span, the calendar will mark the days the device wasn't used with a lighter color.




Once the selections are made, the resource consumption information for the selected period, device, and user will be displayed.

# Timeframe selection

Once the device, user, and dates on which you want to see the data analysis are selected, a chart will appear at the top, with a six-hour zoom window.

You can drag and drop the selection area on the chart to view the resource consumption data for a more specific period.

You can also click on a point on the chart to see the resource consumption data for that specific moment without manually dragging the selection area. The rest of the page data will reflect the selected period, device, and user.

# Resource consumption charts

After placing the time window at the exact point that needs to be analyzed, five resource consumption charts will be displayed at the bottom area: CPU, RAM, GPU, Network Latency, and Disk Usage. Each chart will show six hours corresponding to the selection area in the timeline chart.


The charts show the total resources consumed by the device. If more than one user was using the device during that period, the charts will show the resources consumed by all users.

Hovering over any of the charts will display a box with the resource consumption for that specific moment. You can click on any point of any of the charts to see which applications and processes were running at that specific moment; by default, the most recent data for the selected period will be displayed.

# Performance Counters

Each counter on the screen includes several display options.

## CPU

- **% CPU**: shows the total CPU usage in the system, equivalent to what Task Manager shows.
- **% User Time**: represents the percentage of CPU time utilized by applications and processes running in user mode.
- **% Privileged time**: indicates the percentage of CPU time used by the operating system and system services in privileged mode.
- **% Processor time**: shows the total CPU time used across all system processes and activities.

## RAM

- **% RAM**: shows the total memory usage in the system, equivalent to what Task Manager shows.
- **Available RAM**: represents the amount of free memory in the system for running new applications without causing performance issues.
- **Committed MB**: indicates the amount of virtual memory actively used by the running processes and applications.

## GPU

- **% utilization**: shows the total GPU usage in the system, equivalent to what Task Manager shows.

## Network Latency

- **Network Latency**: shows the system latencies.

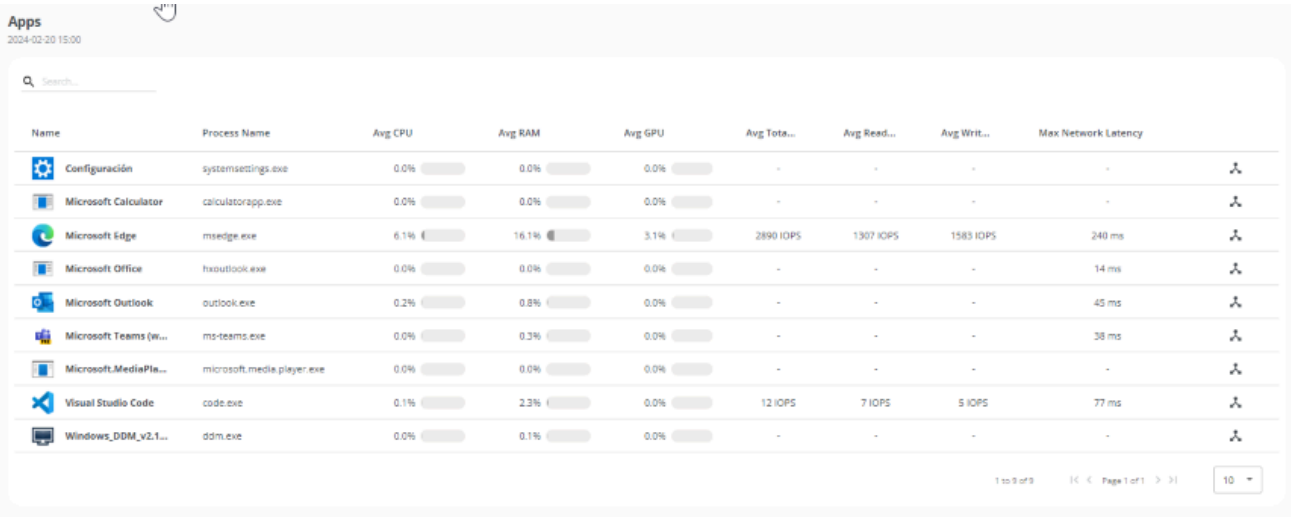
## Disk Usage

- **Total IOPS**: shows the total IOPS (input/output operations per second) generated by the applications and processes on the disk.
- **IOPS read per second**: sum of all read IOPS, per second.
- **IOPS write per second**: sum of all write IOPS, per second.

# Applications and Processes Tables

At the bottom, you will find the application and process tables, which show all the applications and processes that the user had running on that device at the time marked with the time frame selection.

For each application, the name, the executable, and the resources it consumed are shown.




You can filter the table results using the search bar at the top of each one. You can also sort the results by clicking any of the columns in the table.

If you select a point on the chart to see the resource consumption data for a specific moment, the tables will automatically sort to show first the programs that consumed the

most resources in the selected chart.

# Analyzer / Carbon footprint analysis

Green IT, or green technology, is an approach that seeks to minimize the environmental impact of information and communication technologies. One of the areas where it can make a significant difference is in the management and optimization of resource usage, such as energy and paper.

This Analyzer option presents a series of metrics and data related to paper printing and the electrical consumption of devices and their peripherals, which are essential for understanding and improving energy efficiency and sustainability in the work environment.

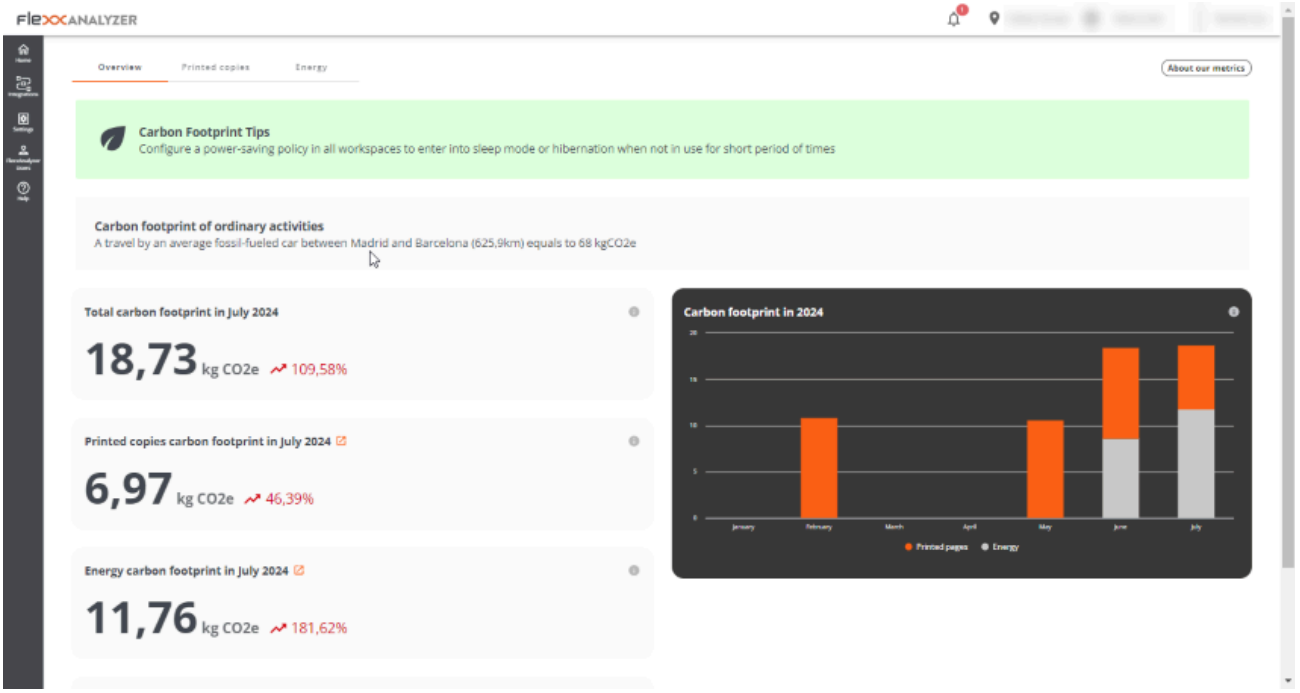
## Web Interface

This dashboard view is divided into three tabs:

- Overview (visión general): where unified data of the entire generated carbon footprint is presented.
- Printed copies: provides information about the monthly prints in the organization, either in black and white or color; the metrics of the users and printers that generate the most prints.
- Energy: provides information about the energy consumption generated by the use of devices and their peripherals, as well as data on radioactive waste produced from energy generation.

> Important: carbon footprint data for electrical consumption and prints are recorded only for physical devices, not for virtual machines.

### Overview




The overview view groups the collected data regarding both energy consumption and prints, to show monthly information.

Data contained in the view (current month):

- Total generated carbon footprint
- Carbon footprint generated by prints
- Carbon footprint generated by electrical consumption
- Amount of radioactive waste generated in the current month
- Graphical view of the monthly evolution of the generated carbon footprint

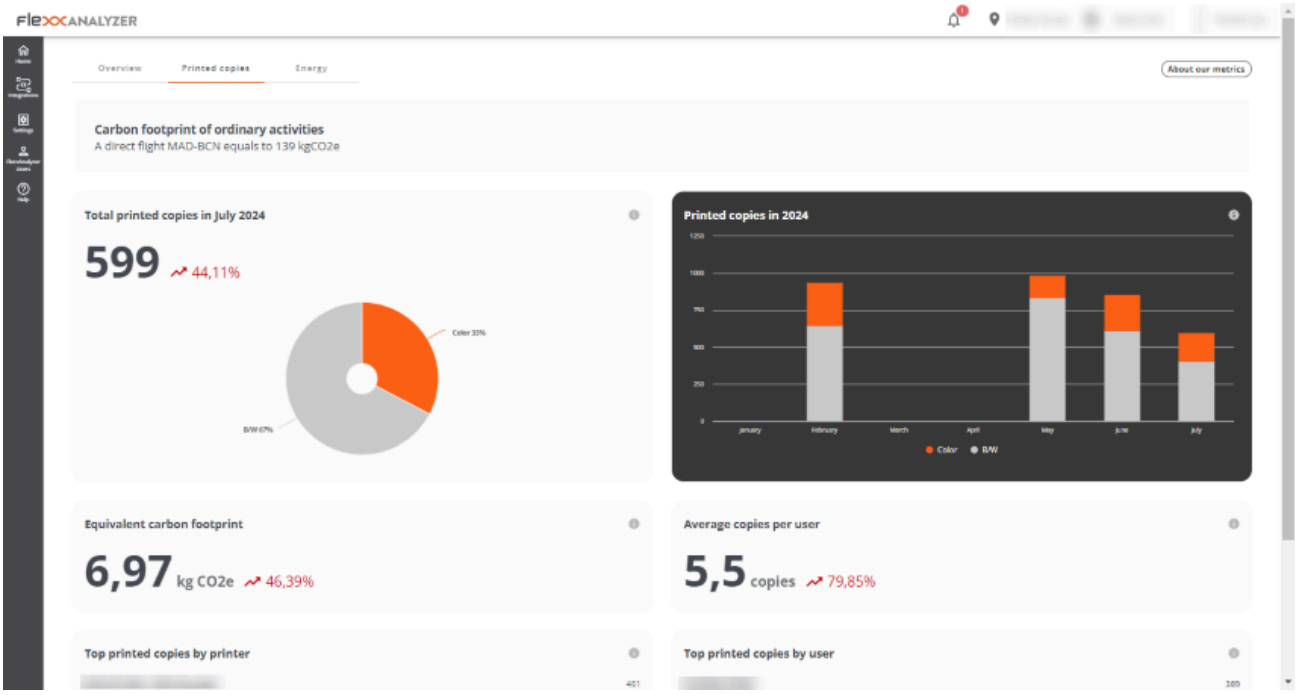
## Printed copies

The adoption of Green IT practices for the management and optimization of resource usage in the field of printing involves taking measures that lead to a reduction in paper and energy consumption, as well as the carbon footprint associated with printing devices.

This section presents a dashboard view with information about the prints made and the carbon footprint generated by this activity.

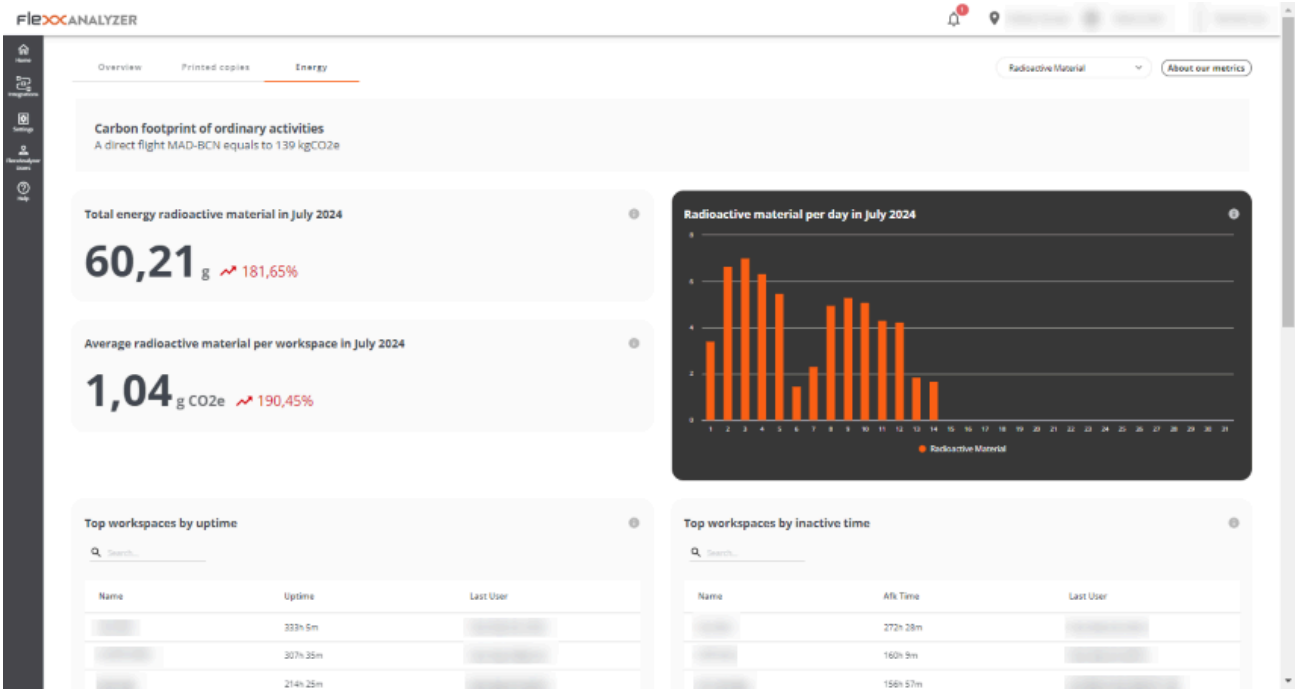
The carbon footprint of the printed copies is calculated using the following estimates:

- 10 g of CO2e per A4 black and white copy
- 15 g of CO2e per A4 color copy




- **Total printed copies in [current month]** (Número de impresiones en el mes en curso): shows short-term trends in paper usage. Helps identify areas of intensive use, as well as opportunities to reduce the number of prints or promote duplex printing.
- **Equivalent carbon footprint** (Total de la huella de carbono generada en el mes en curso): provides a direct idea of the environmental impact of printing activities. It can motivate the adoption of policies to reduce the carbon footprint, such as digitizing documents and implementing paperless initiatives.
- **Top printed copies by printer** (Top de impresiones por impresoras): view of printers, sorted by the number of prints in the current month.
- **Printed copies in [Current year]**: overview of total black and white and color prints made, month by month, during the current year.
- **Average copies per user**: average number of prints per user in the current month.
- **Top printed copies by user** (Top de impresiones por usuario): list of users, sorted by number of prints during the current month.

## Energy




The carbon footprint of energy consumption is calculated by multiplying the energy consumption of the device, showing the average kgCO2e per kWh in Spain, which is 0.1 kgCO2e/kWh.

The radioactive material from energy is calculated by multiplying the device's energy consumption and is shown with the average kgCO2e per kWh in Spain, which is 0.512 g/kWh.

This section presents a dashboard view with information about the carbon footprint and radioactive waste generated by the electric consumption of the devices.

Using the selector on the top right, it is possible to select the view of radioactive material or generated carbon footprint.

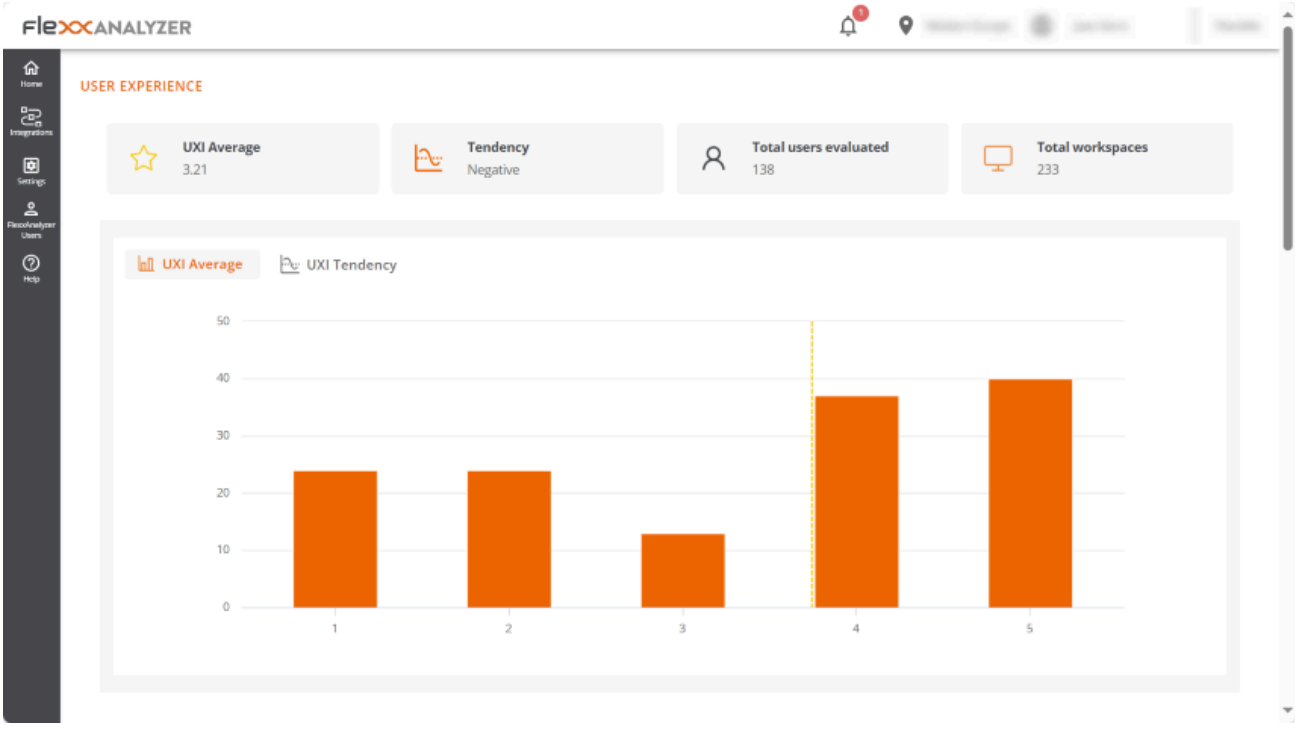
#### Radioactive material

- **Total energy radioactive material in [Current month]**: shows the total grams of radioactive material generated during the current month.
- **Average radioactive material per workspace in [Current month]**: shows the average radioactive material per workspace in the current month.
- **Radioactive material per day in [Current month]**: estimate graph of grams of radioactive waste generated in the current month.

- **Top workspaces by uptime**: top 10 devices by uptime in the current month.
- **Top workspaces by inactive time**: top 10 devices by inactive time in the current month.
- **Top workspaces by radioactive material generated**: top 10 devices that generate the most radioactive material. Radioactive material calculations are made using the averages of CPU and screen consumption by the average radioactive material generated per kWh in Spain (0.512 g).
- **Top workspaces by inactive time and radioactive material generated**: top 10 devices that generate the most radioactive material while being inactive. Calculated using the averages of CPU and screen by the average radioactive material generated per kWh in Spain (0.512 g).

# Analyzer / User experience

In an organization, user experience measures how employees interact with their organization's digital ecosystem; this includes evaluating the performance of the hardware and software they use during their workday, as well as their emotional perception.




## Basic concepts

Analyzer builds the UXI (user experience indicator) based on the weighting of two others:

- Workspace Reliability Index (WRI)
- User sentiment

### Workspace Reliability Index (WRI)

The Workspace Reliability Index, or device reliability indicator, allows for an objective performance score for a device based on the collection and analysis of detected issues. Multiple indicators are considered which, if certain issues arise in devices, reduce the score from an initial 5-star rating. These metrics include:

| Indicator | Severity | Threshold | Recurrence | |
|---|---|---|---|---|
| HIGH_CPU | MEDIUM | Above 80% for more than 5 minutes | 5 min | |
| HIGH_RAM | MEDIUM | Above 80% for more than 5 minutes | 5 min | |
| BSOD | HIGH | Presence of a BSOD (blue screen) | Once per day | |
| APP_CRASHES | HIGH | Presence of application crashes | Once per day | |
| APP_HANGS | HIGH | Application crashes presence | Once per day | |
| TEAMS_PROBLEMS | HIGH | Detected problems in Microsoft Teams | Once per day | |
| PNP_ERRORS | HIGH | Detected peripheral errors | 5 min | |
| WIFI_SIGNAL | HIGH | Signal below 40% for 10 minutes | 5 min | |
| LOGIN_DURATION | HIGH | More than 60 seconds | Once per day | |
| UPTIME | LOW | More than 15 days | Once per day | |

| Indicator | Severity | Threshold | Recurrence | |
|---|---|---|---|---|
| RESTART_PENDING | LOW | More than one day | Once per day | |
| CRITICAL_EVENTLOG | HIGH | Presence of critical events in the event viewer | Once per day | |
| UID | MEDIUM | High system response rate (greater than 350 ms) | 5 min | |
| LOW_STORAGE | MEDIUM | 500 MB | Once per day | |
| MULTIPLE_EVENTLOGS_ERRORS | MEDIUM | More than 50 errors generated in the event log in the last hour | Once per day | |
| UNAVAILABLE | MEDIUM | Session unavailable for more than 5 minutes | 5 min | |
| RAM_UNDER_MINIMUM | MEDIUM | Less than 1 GB of free memory for 120 minutes | 5 min | |
| WINDOWS_UPDATES_POOLED | MEDIUM | Windows Update service running on pooled machine | 5 min | |

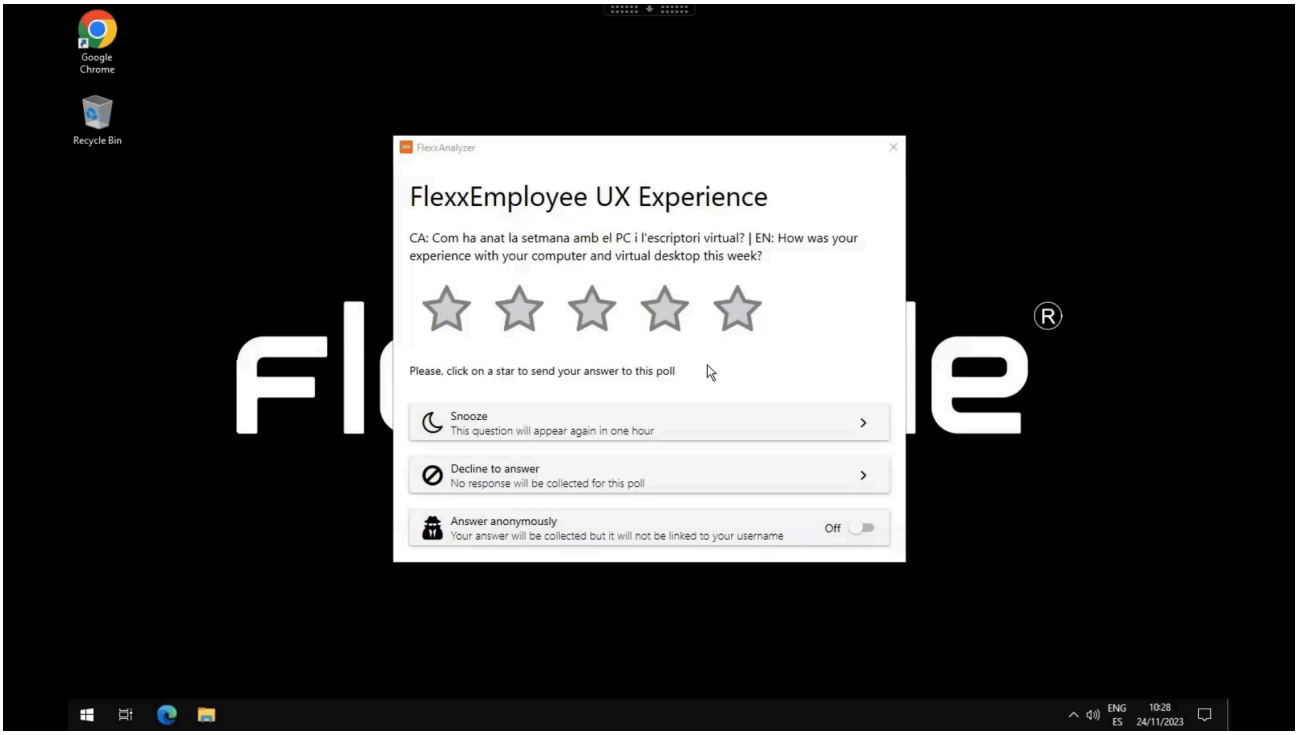
| Indicator | Severity | Threshold | Recurrence | |
|---|---|---|---|---|
| BOOT_DURATION | HIGH | Boot duration longer than 90 seconds | Once per day | |

Where each severity deducts the following score from the initial 5-star rating.

| Severity | Penalty |
|---|---|
| HIGH | 0.2 |
| MEDIUM | 0.016 |
| LOW | 0.008 |

## User surveys

User sentiment is captured through surveys. And the way to respond is by providing a satisfaction rating based on a score between 0 and 5 stars.



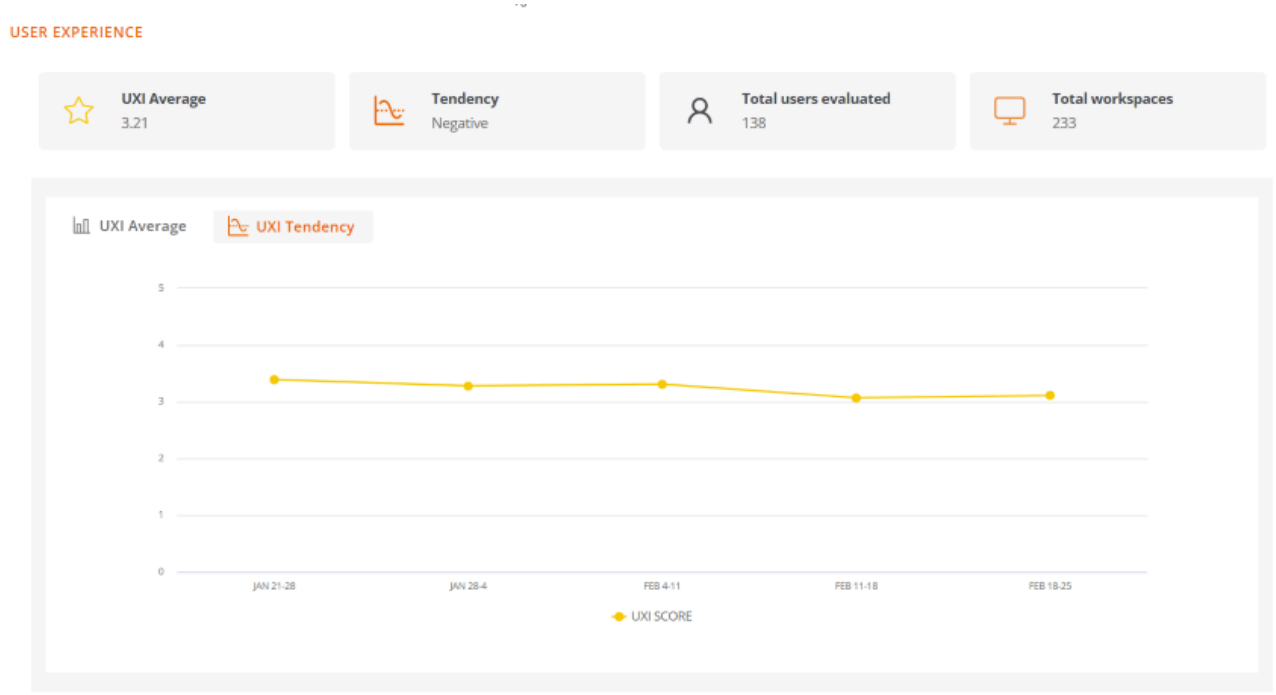

# Web Interface

The dashboard view of the 'User Experience' section consists of the average information of all devices and users in the organization; it is calculated daily.

## Global view

The global numbers are offered at the top.

- UXI Average: average experience indicator for the entire organization. It can range from 0 to 5.
- Tendency: an indicator that, based on the evolution of the UXI average, shows whether its tendency is positive or negative.
- Total users evaluated: total users evaluated
- Total workspaces: total devices evaluated



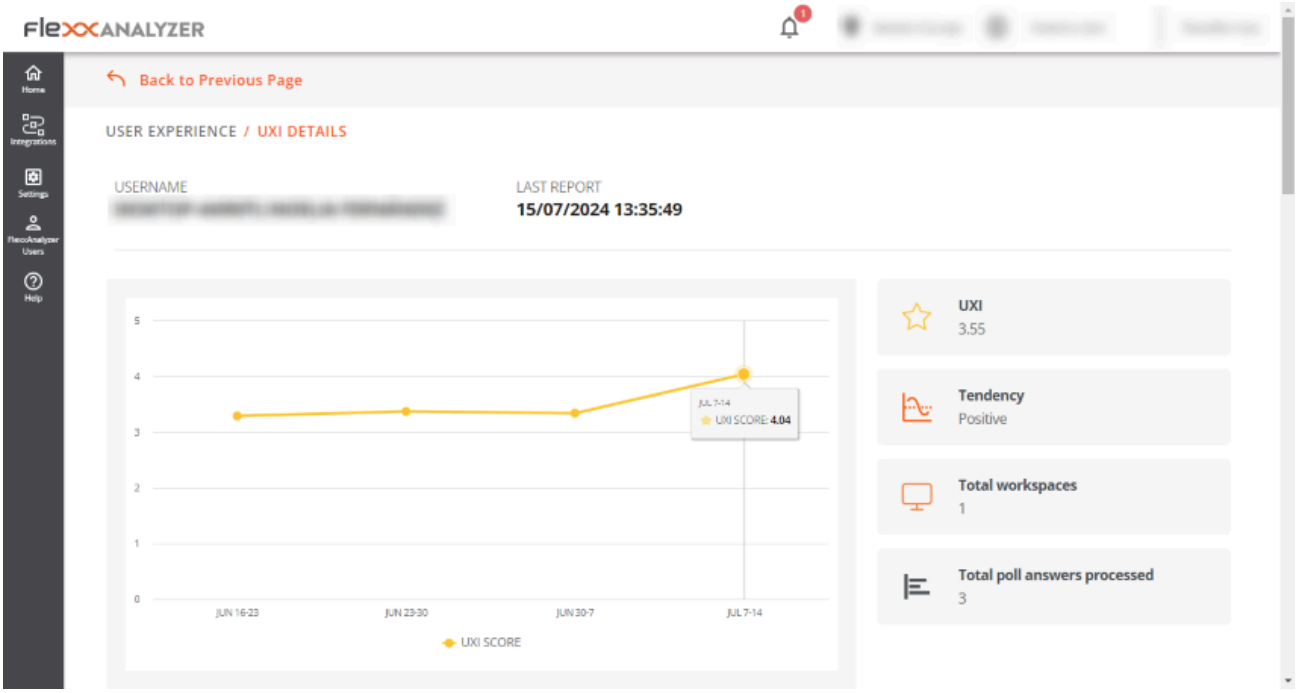

Two charts are also included:

- UXI Average: shows the distribution of users by UXI level, along with the organization's average.
- UXI Tendency: shows the temporal evolution of the UXI over the last month.

At the bottom of the screen, by clicking on a user, individual cases can be evaluated. You can also see tables containing information about users who require attention due to sudden variations of this indicator or a very low score.

## Individual view

This view provides the user data under analysis, including:



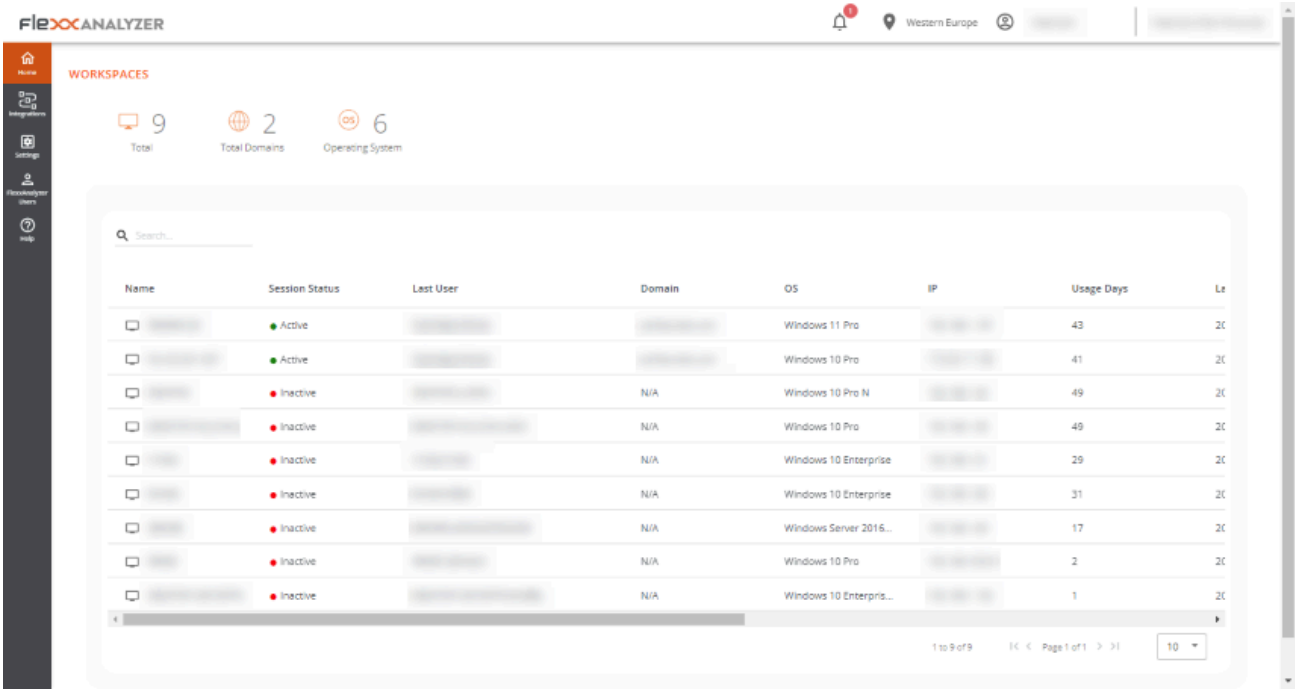

- Username: username reported in the user's session
- Last report: date of the last report received for this user
- UXI Average: experience indicator for the user; it can range from 0 to 5.
- Tendency: an indicator that, based on the evolution of the user's UXI average, shows whether the tendency is positive or negative.
- Total workspaces: number of devices the user has worked on
- Total poll answers processed: number of surveys the user has answered and are taken into account in this evaluation.

At the bottom of the screen, detailed information is included in a table format.

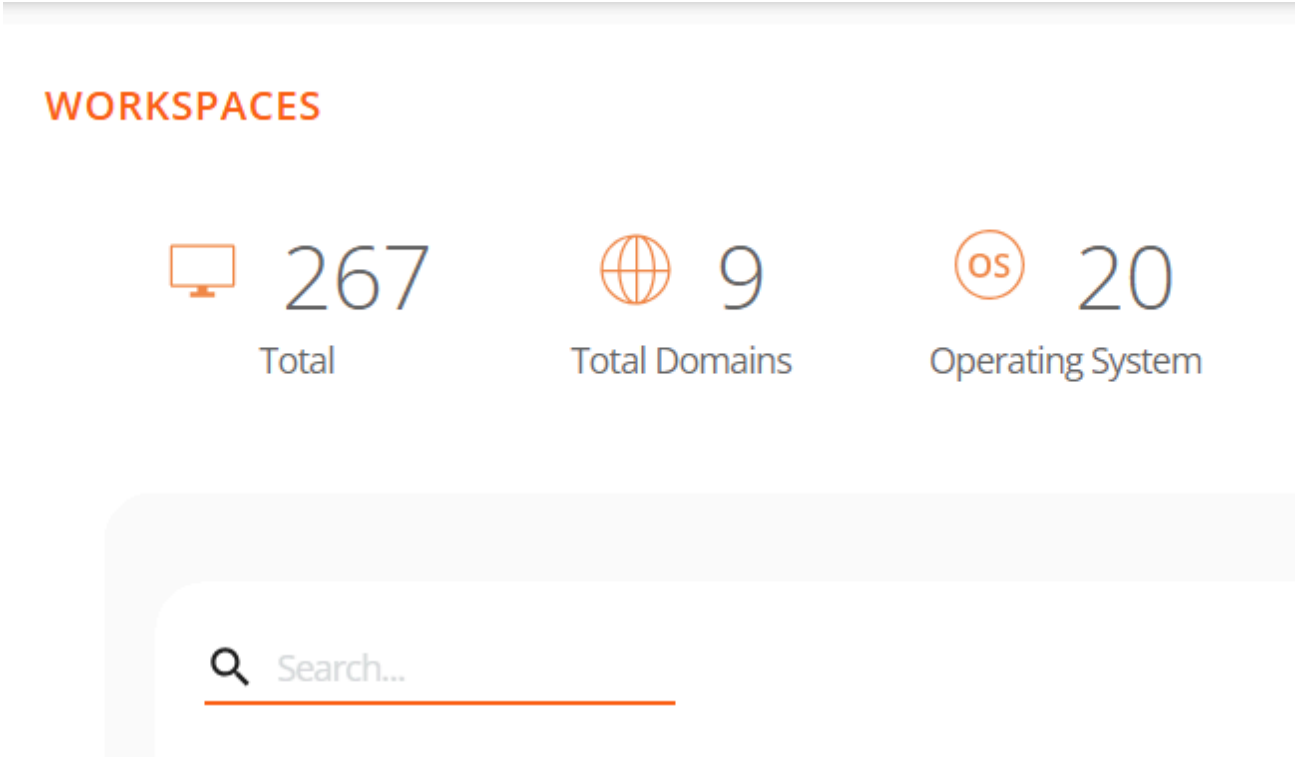
- Polls in the last 30 days: surveys answered by the user in the last 30 days. The detail of this view offers the user's survey scores compared to the organization's average for the same period.
- Workspaces in the last 30 days: provides a table that contains all the devices the user worked on during that time span, as well as how many times they worked on each, the operating system, and the WRI indicator of each.
- Issues in the last 30 days: table showing the list of problems detected on devices used by the user in the last 30 days, as well as the date and score that each of them deducted.

# Analyzer / Workspaces in Analyzer

The `Workspaces` list view provides global information about the device environment. It shows through a table the names of the monitored devices, their session status, domain, operating system, connected IP address, and other technical data such as CPU, RAM, IOPS usage per device, and the installed version of FlexxAgent.




Above the table, there is a chart indicating key quantities: number of monitored devices, registered domains, and operating systems detected on the network. And also a search field, so that the user can easily find the device of their interest.

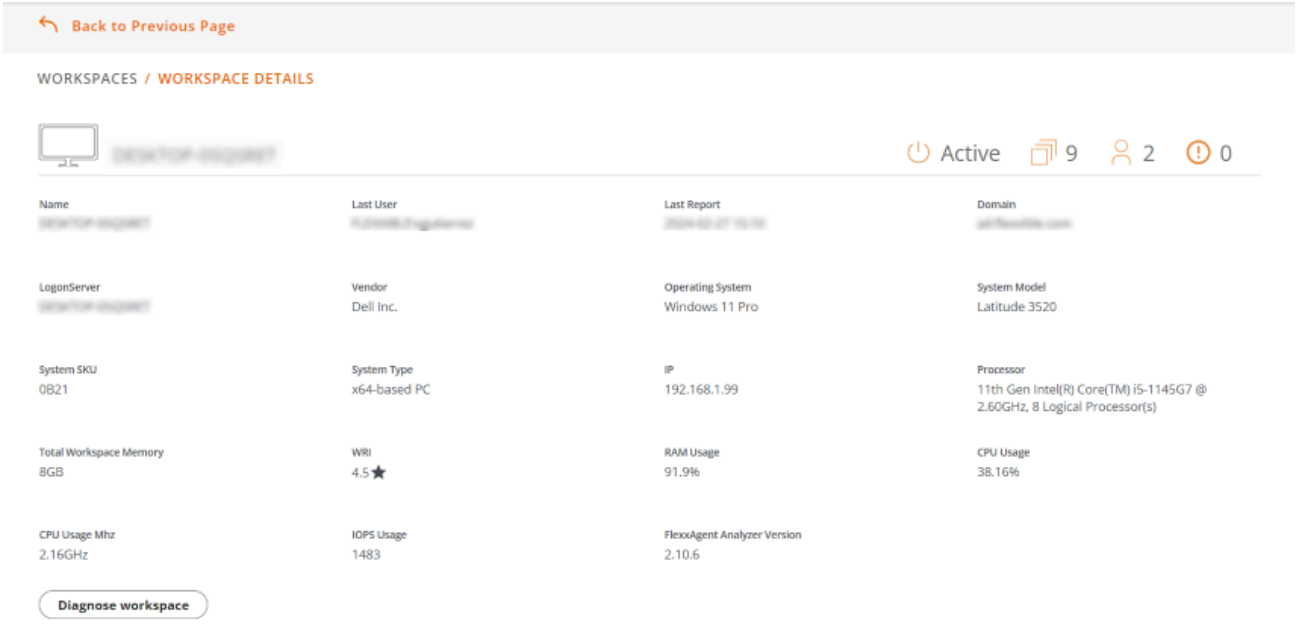



# Workspace detail

To access more precise data of a device, you must click on it in the table. Next, the user will see the following information:

| Field | Data |
|---|---|
| Name | Text string containing the hostname |
| Last User | Last user who used the device |
| Last Report | Date of the last report sent by FlexxAgent |
| Domain | Domain of which the device is a part |
| LogonServer | Server that authenticates the user when logging in |
| Vendor | Device manufacturer |

| Field | Data |
| --- | --- |
| Operating System | Device operating system |
| System Model | Device model |
| System SKU | Manufacturer SKU identifier |
| System Type | System type, defines the system architecture |
| IP | Device IP address |
| Processor | Commercial name of the processor |
| Total Workspaces Memory | Total memory present in the system |
| WRI | Workspace reliability index of the device |
| Ram Usage | Percentage of RAM used |
| CPU Usage | Percentage of processor used |
| CPU Usage | Processor usage in MHz |
| GPU Usage | Percentage of GPU usage |
| IOPS Usage | Average IOPS of the disk |
| FlexxAgent Analyzer Version | Running version of FlexxAgent Analyzer |




Below the list, the `Diagnose workspace` button allows you to see the usage data for the device, which is the same information that can be found in the `Diagnosis` section.

# Workspace analysis

The lower part of the device detail view consists of five tables that analyze very specific device goals:

- Displays.
- Installed Apps.
- Running Apps.
- Issues in the last 30 days.
- Usage history.

Each of these sections has its own search field to facilitate access to the information.

## Displays

It contains information about the screens connected to the device, their maximum resolution, and size. This data becomes important because the electric consumption generated by the screens is used to estimate the carbon footprint.

## Installed Apps

Shows a list of the applications installed on the device. Also the version number, category, installation date, application group it belongs to, and the unique identifier assigned to it. For more information on how to edit these fields, refer to `App Catalog & Inventory`.

The information about installed applications offered by `Installed Apps` is collected by FlexxAgent Analyzer when its process starts. From there, the data will be updated every 12 hours.

## Running Apps

Shows a list of applications running on the device. The table indicates the name of the process running and the average resource usage for CPU, RAM, and GPU.

The information about the running applications provided by `Running Apps` is collected by FlexxAgent Analyzer every 15 seconds and sent to the console every 5 minutes.

## Issues in the last 30 days

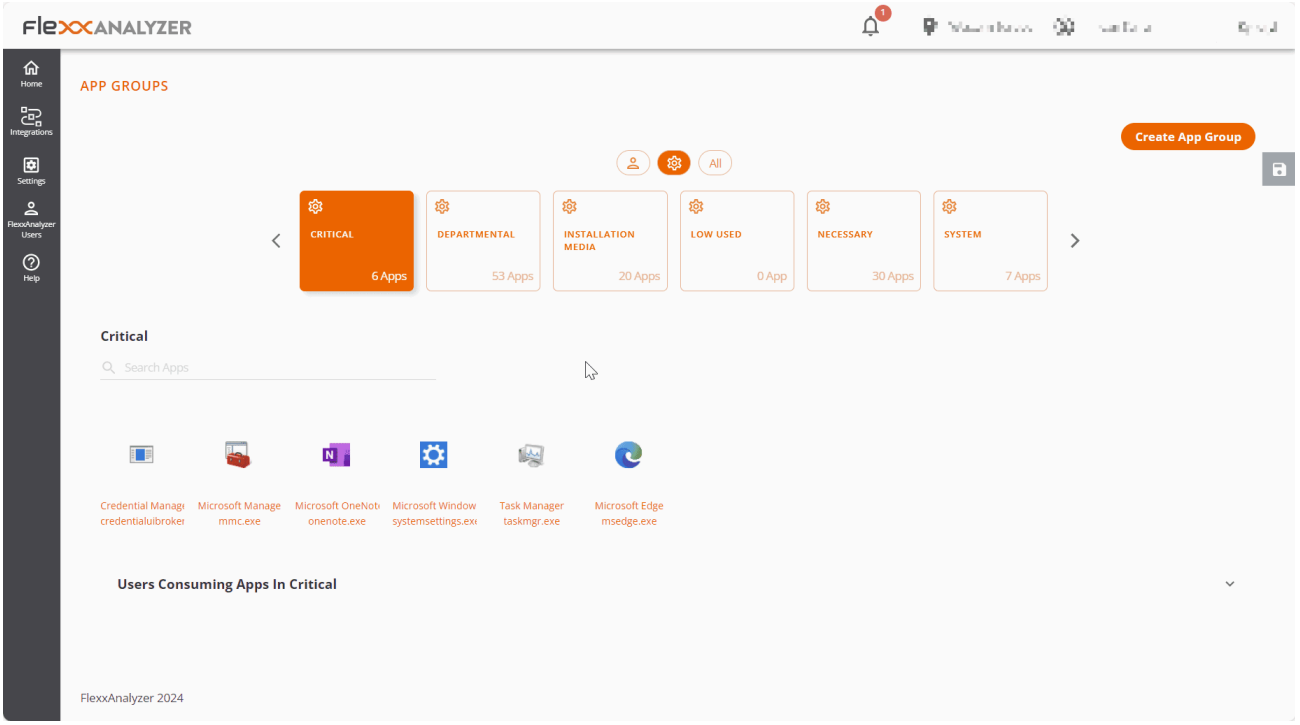
This table includes the list of alerts generated in the Workspaces module and sent daily to the Analyzer. The table reports the score deducted from the Workspace Reliability Index for each alert found on the device.

## Usage history

Contains information about the device usage history. Indicates the user or users who use it, as well as the days they do.

# Analyzer / App Groups

App Groups provides the possibility to create application groups to display aggregate data on the analysis screens.




At the top of the main screen, three buttons allow you to filter by user applications, system applications, or view all. And below, each application group is represented in a tile.

# Group Types

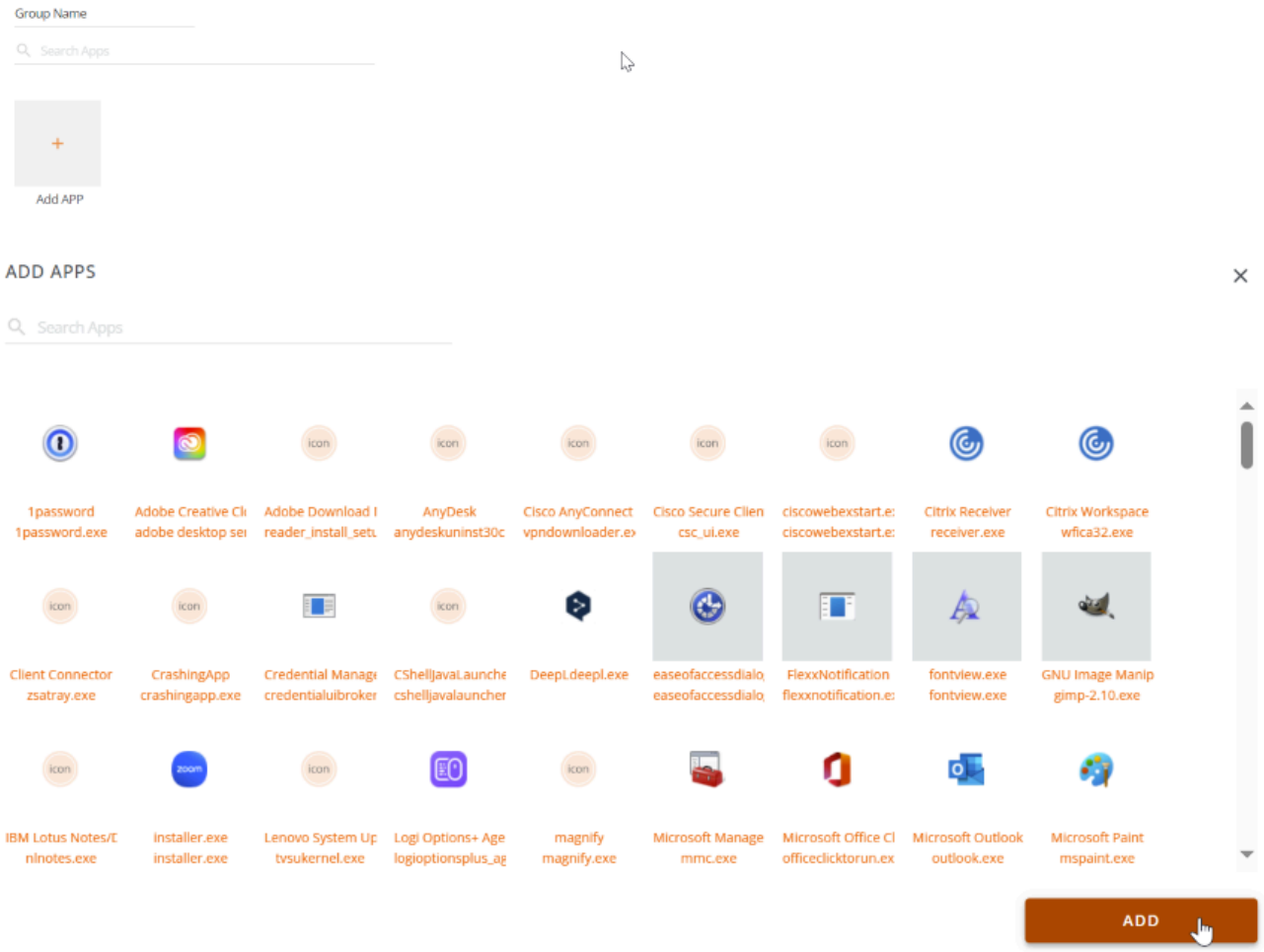

- `User App Group`: groups manually created from the Create App Group button.
- `System App Group`: automatically generated groups. Created by Analyzer considering the assigned configuration in the Settings option.
- `All`: includes all groups.

# Users consuming applications in the selected group

In the `Users Consuming Apps In...` section, you can see which users are using that application group.

# Creating a New Application Group

When creating a new application group from `Create App Group`, you must specify the name of the group and, through the `Add APP` button, the applications you want to add.



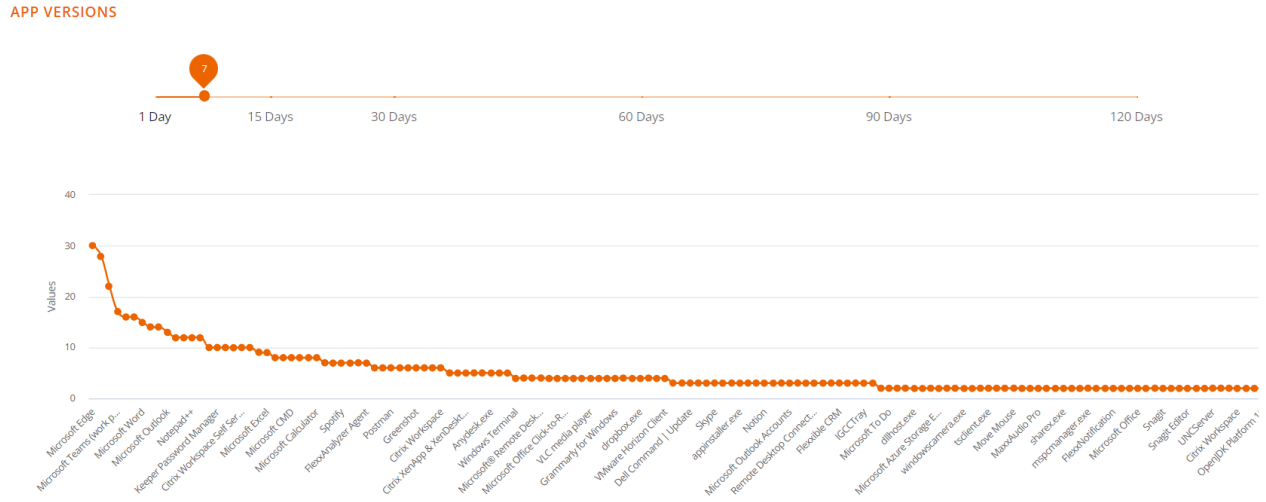

Finally, to save, click on the `Save changes` button.

# Analyzer / App Versions

`App Versions` allows you to quickly and visually obtain information about the different versions of the same application installed on an organization's devices.

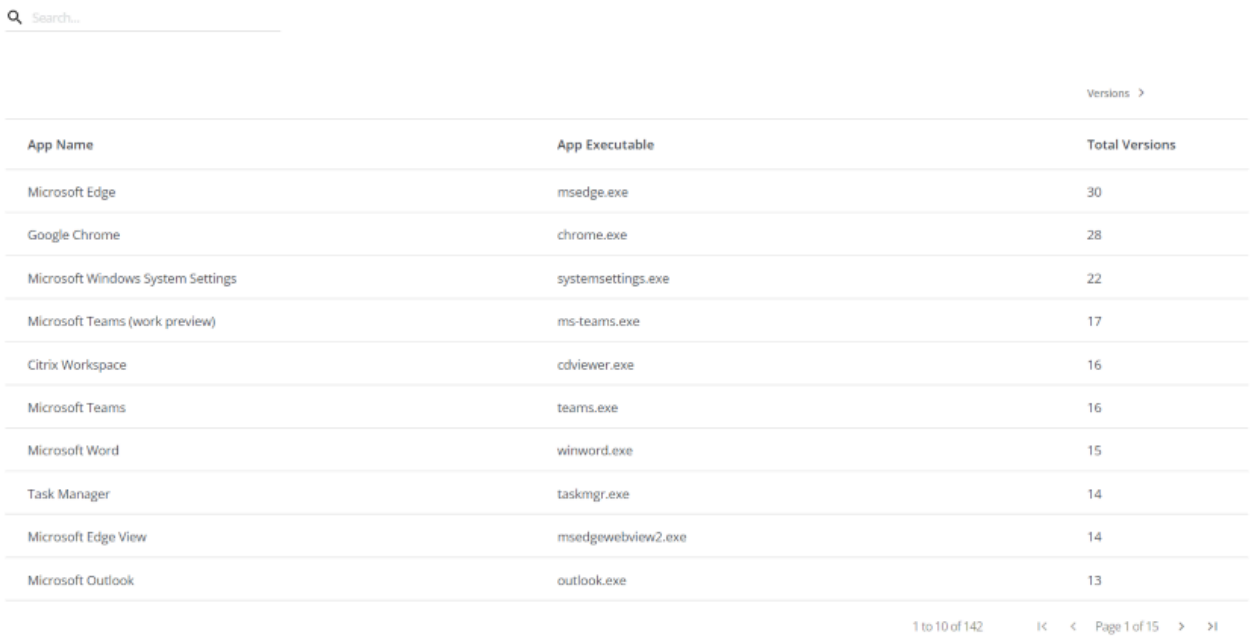
## Graphical view

In the upper area of the `Apps Version` option, you can see a selector for the number of days you want to evaluate. By moving it, you can see the different versions of the registered applications, depending on the number of days selected.




The graph below the day selector shows the number of versions per application: those with more will be at the top and those with fewer, at the bottom.

## Table view




At the bottom, there is a table with detailed information:

- Application name
- Executable name
- Number of total versions

This data facilitates the task of unifying the different application versions.

# Analyzer / Polls

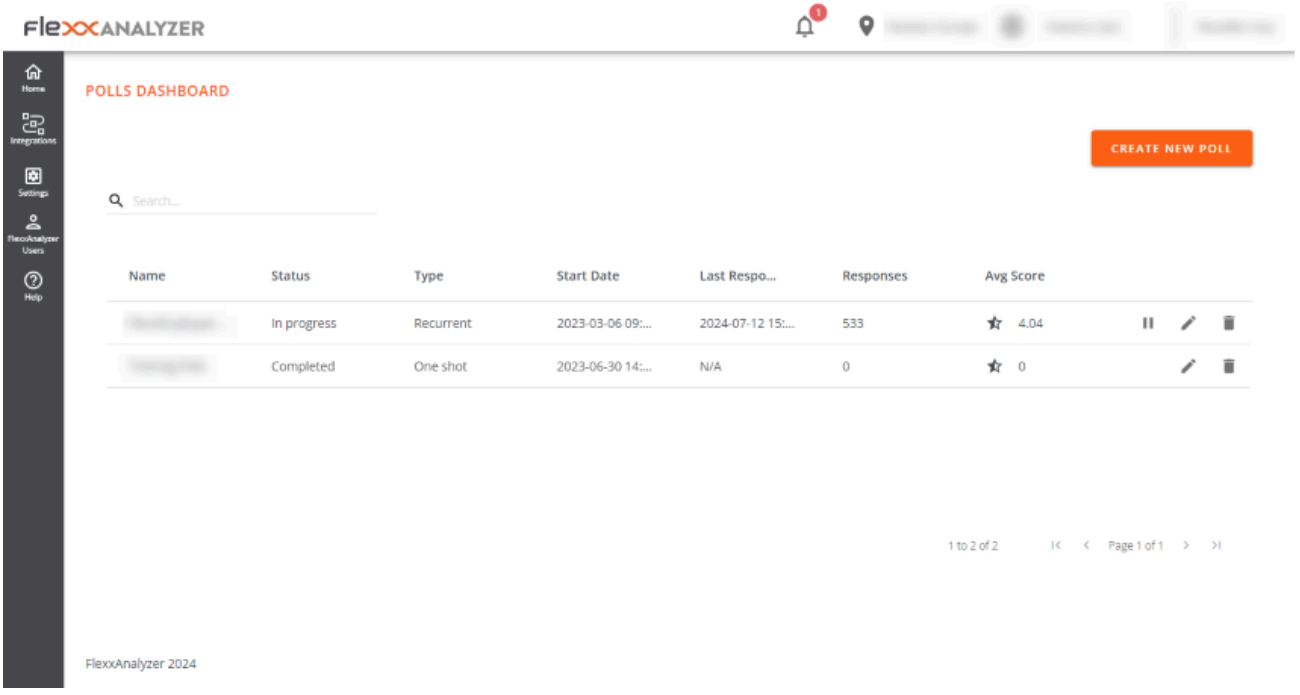
Polls allow us to get the user's sentiment or perception regarding very simple questions, trying to simplify the response mechanisms as much as possible to maximize the user response rate.

The information gathered from the polls is processed along with the data that make up the WRI (Workspace Reliability Index) to build the UXI dashboard (user experience indicator).

## Poll Settings

The `Polls` section allows you to create, modify, and delete polls for users, schedule their execution, determine which users will receive them, and more options.

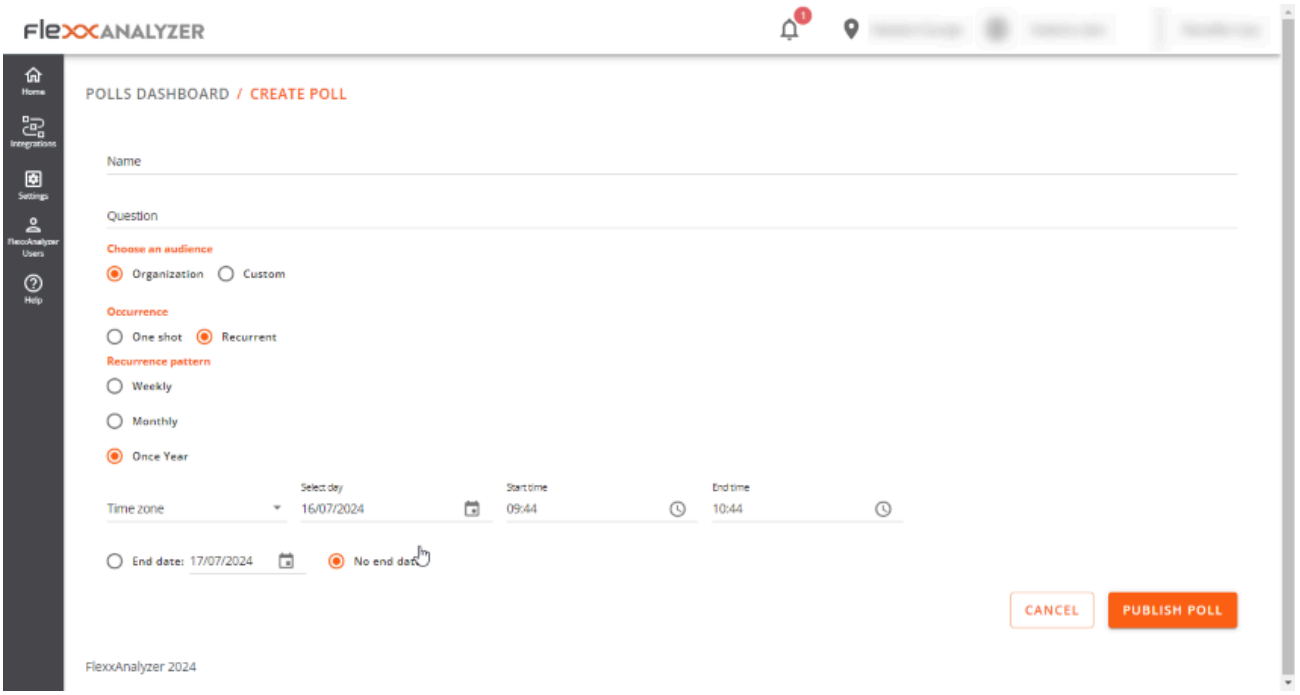
### List view




By accessing the section, you can see a list of configured polls, if any, as well as a preview of their configuration.

### Detail view

By accessing an already created poll to modify it or simply creating a new one using the button at the top right, you can access the settings of a poll.




The configuration options include:

- Name
- Question
- Audience
- Occurrence

#### Name

Define the name of the poll, as well as the title it will have when sent to users.

#### Question

Contains the question that will be asked to users; the response is determined on a scale from 1 to 5 stars.

#### Audience

The audience settings allow you to launch the poll to the entire organization, selected user groups, or organizational groups.

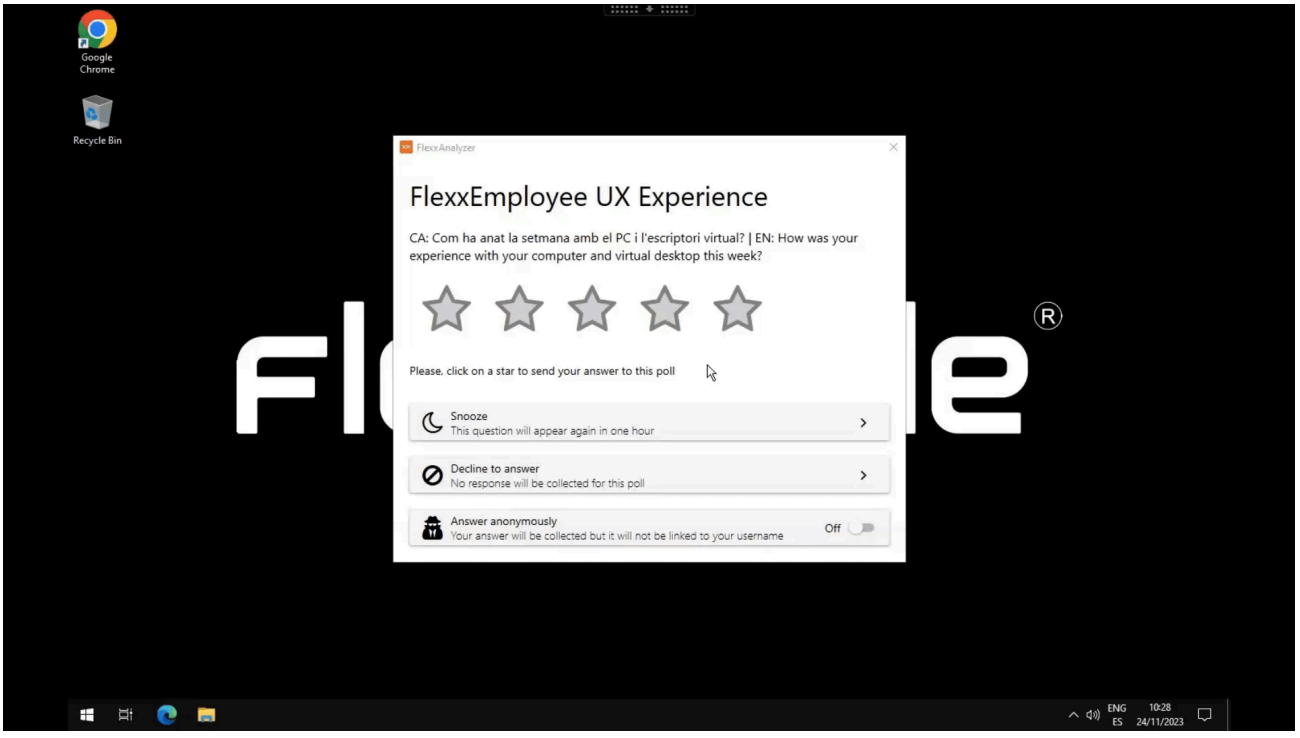
**Occurrence**

The occurrence options allow you to configure the poll to be launched to users either once or on a recurring basis. If it is recurring, the options are as follows:

- Weekly
- Monthly
- Yearly

In all cases, it is possible to select the specific day of the poll launch and its end date. It is also possible not to set an end date so that the poll runs indefinitely with the applied configuration.

# Poll Execution




When the execution time arrives, the users defined in the audience settings will receive the poll. They need to respond by clicking on the number of stars (from 1 to 5), according to the rating. These data are processed together with the data that make up the WRI (Workspace Reliability Index) to build the UXI dashboard (user experience).

# Analyzer / Users in Analyzer

The users view provides information about all users detected by FlexxAgent on the devices. It allows you to view the application and device resources used by the users in the organization.

To get more information about users, it is possible to integrate Analyzer with Active Directory or Entra ID, which will allow obtaining data that FlexxAgent cannot capture from the session, such as email address, manager, or user department.

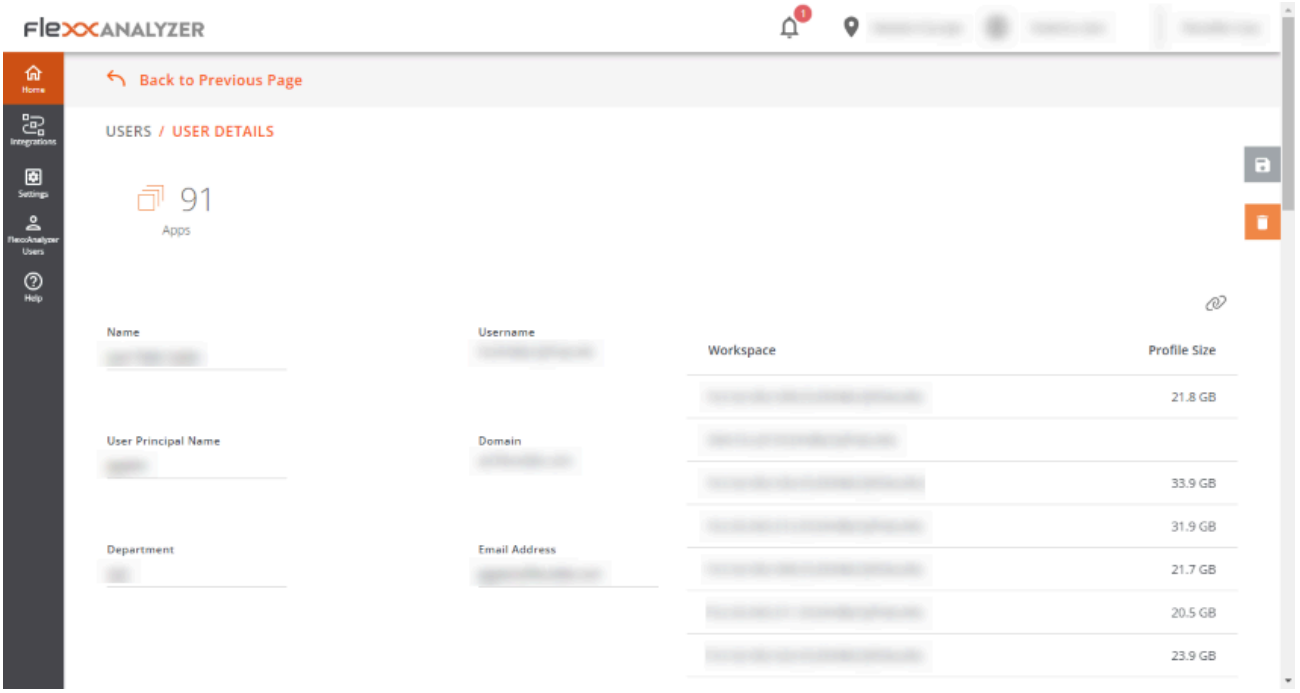
## List view

This view allows you to see condensed information about the total number of users and domains, as well as data for all users; these include:

- Username: username used for login in the session
- Name: user's display name
- UPN: principal user name
- Department: Department reported in Active Directory or Entra ID
- Domain: Entra ID or Active Directory domain where the device resides
- Manager: user's manager informed in Entra ID or Active Directory
- Usage days: total days the user has logged in
- Profile size: disk space occupied by the user profile
- Last report: date of the last FlexxAgent report

## Detail view

Accessing any user enables the detail view:




## User data in the detail view

In this view, data related to the user is collected, including:

- Total number of applications used by the user
- Username: username used for login in the session
- Name: user's display name
- UPN: principal user name
- Domain: Entra ID or Active Directory domain where the device resides
- Department: Department reported in Active Directory or Entra ID
- Email Address: user's email address

On the right side of the screen, there is a table with a row for each device on which the user worked. This table contains:

- Workspace: device name
- Profile size: disk space occupied by the user profile

At the bottom of the screen, the 'Used applications' and 'Usage history' sections are presented.

`Used applications` presents a table view containing all the applications used by the user. The table contains:

- Name: application name
- Workspace: device where the application was detected
- Version: discovered application version
- Last report: date of the last FlexxAgent report
- App Group: group to which the application belongs
- Category: application category

`Usage history` shows information about the devices used by the user. Contains:

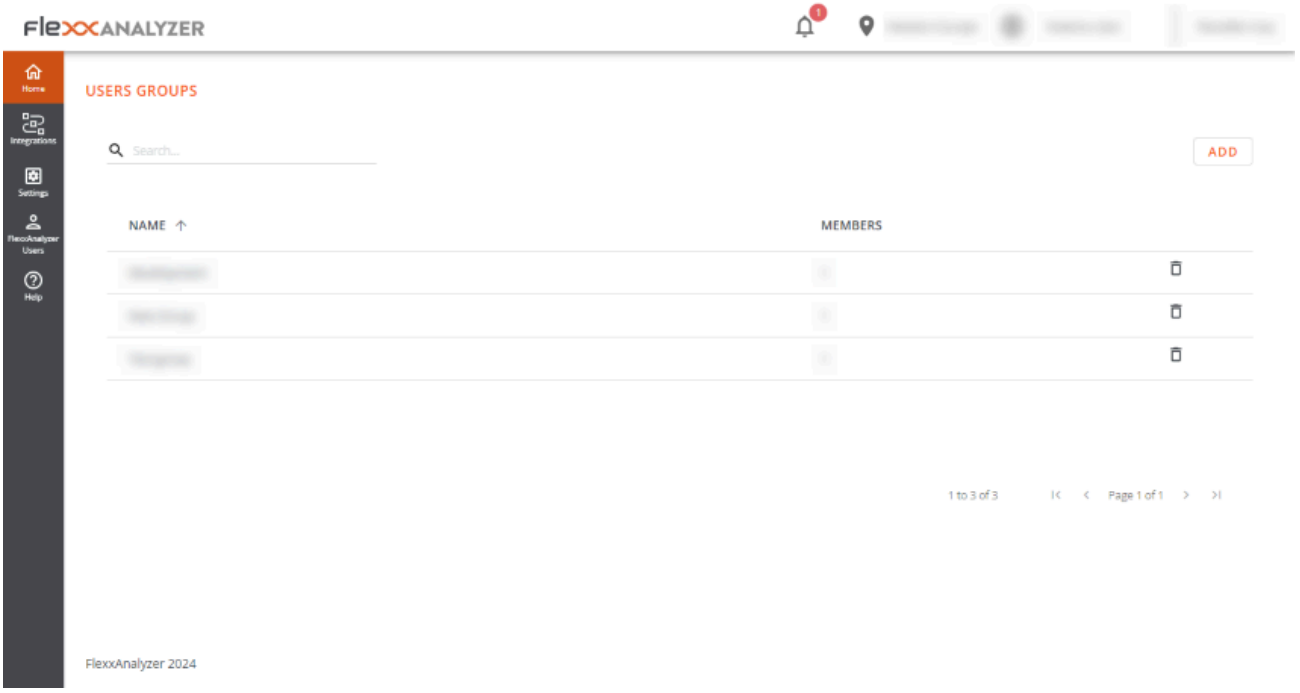
- Workspace: device name
- Days: usage days
- Last report: date of the last FlexxAgent report

# Analyzer / User Groups

Users Groups allows you to create user groups using the data of the users discovered by FlexxAgent.

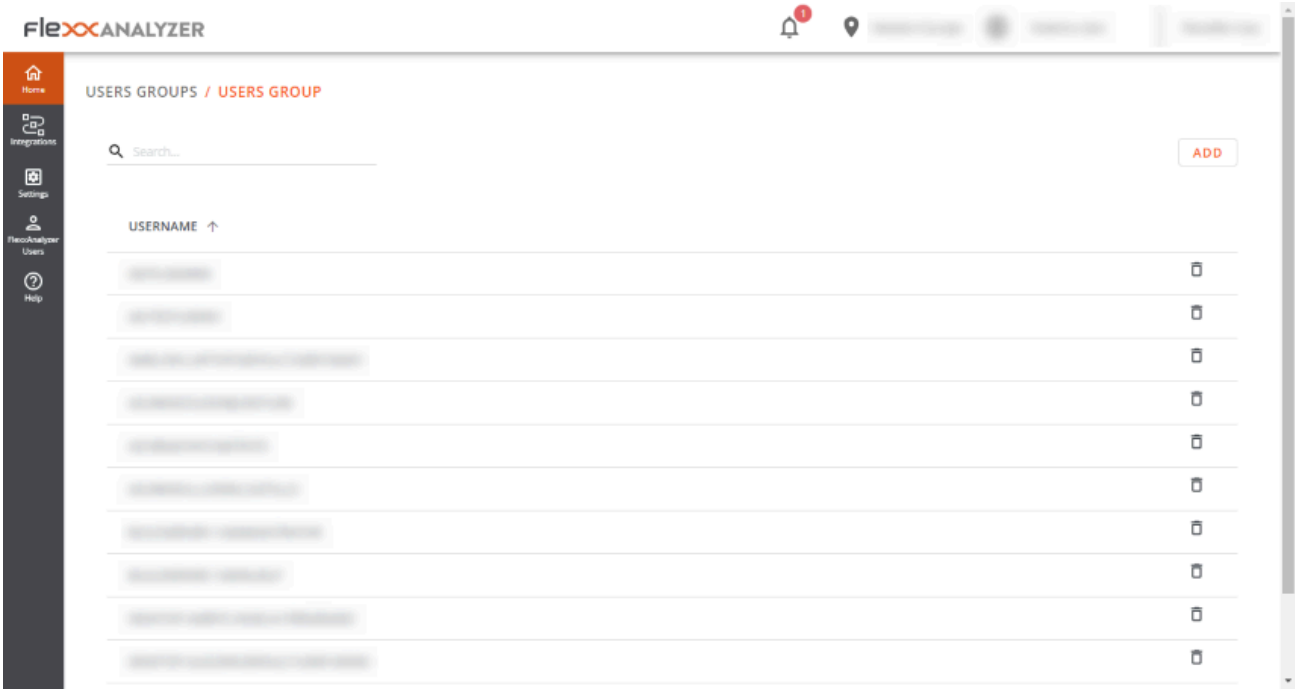
## List view

The list view presents the information of all existing groups and the button at the top right of the screen allows you to create new groups.




## Detail view

Within the details of a user group, it is possible to remove any user using the trashcan-shaped button located on the far right. It is also possible to add new users to the group with the `Add` button at the top right of the screen.

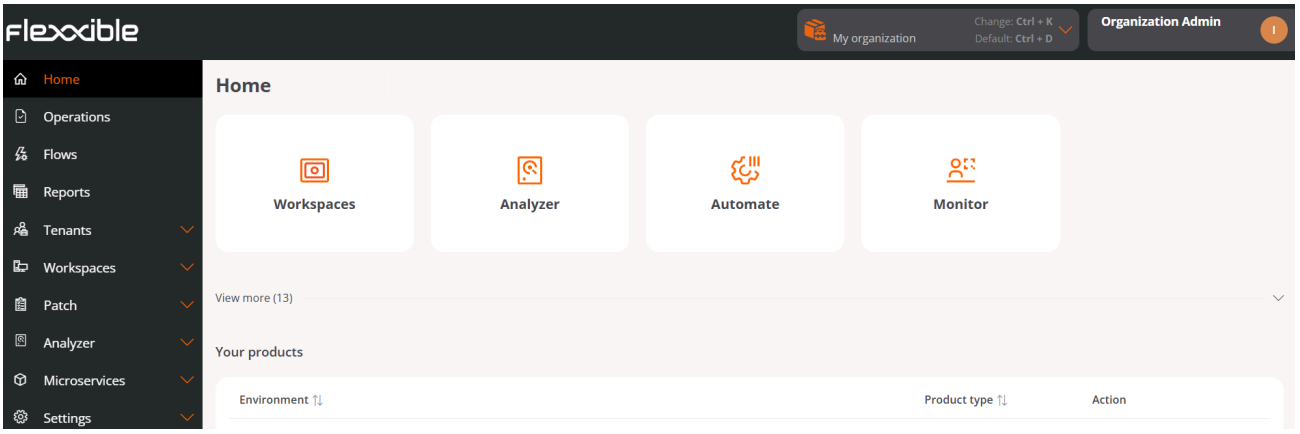


# Portal

Portal is the central space of the platform, from where you can access the available modules of Flexxible's products. You can create, modify or delete users and also assign them roles so they can develop and manage actions related to microservices, flows, and patch management policies.

Through Portal, you can consult license consumption data by environment; manage reporting groups, which enable device segmentation; and activate functionalities in FlexxAgent. Portal integrates with OAuth2, a framework that allows user authorization, enabling them to sign in easily using their corporate credentials.

From `Home` you can access the various modules that make up the solution and in `Your Products` to the active licenses of Flexxible's products included in your subscription.




# Sidebar menu

This option offers several action fields.

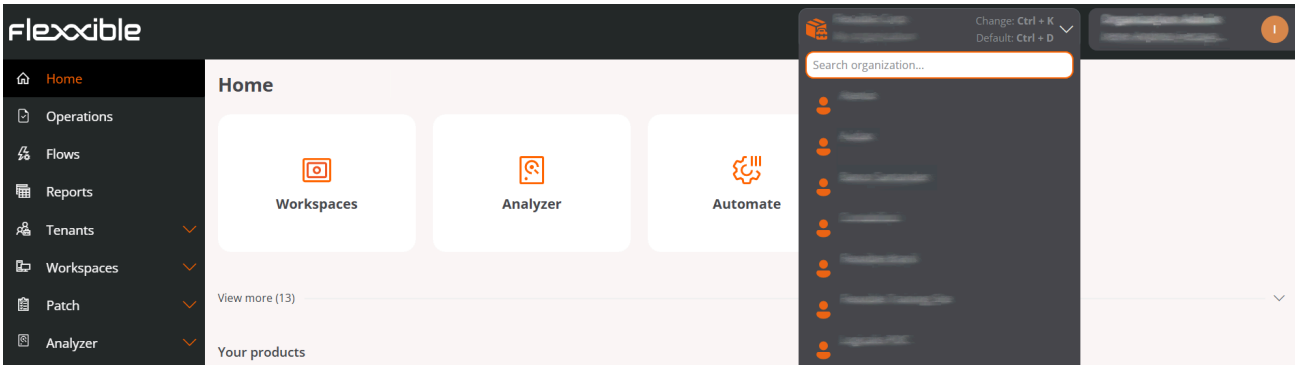
- Operations
- Flows
- Reports
- Tenants
- Workspaces
- Updates

- Analyzer
- Microservices
- Configuration

# Organization selector

At the top, to the right of the interface, is the organization selector. If a user has access to multiple organizations, such as in the case of managed service providers (MSP), they can easily select the organization to manage: simply expand the list of organizations and choose the desired one or type in the search box a string that matches the name of the organization you want to find, select it and press `Enter`.

You can also select an organization through the navigation bar by pressing `Control + K` or `Cmd + K` (on Mac).




To return to the default organization, you can repeat the same procedure or use the shortcut `Control + D` or `Cmd + D` (on Mac).

# User Settings

In the top menu, on the right, the logged-in user's name and their assigned role in Portal are displayed.

If you click on the user name you can consult and manage:

- My logins

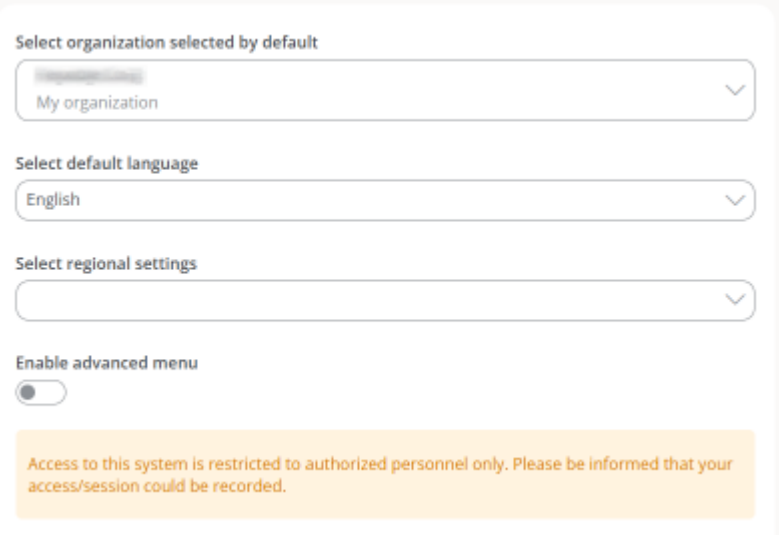
- Settings

# My logins

Displays a table with information about the user's session connections, including IP address, name of the Flexxible application accessed, user agent, and date and time of access. The data comes directly from the authentication provider. You can view up to the last 30 days or the last 1000 login sessions at most.

# Settings

This section allows the user to set the default organization to manage, configure the platform language, set regional settings, and enable the advanced menu.




**Default Organization**

The default organization is the one the user will see by default when entering the Portal. This option allows selecting it from the available organizations shown in the dropdown list.

**Language**

From this option, the user can choose the language in which they want the interface to be displayed. You can choose between Spanish, Portuguese, English, Catalan, and Basque.

**Select regional settings**

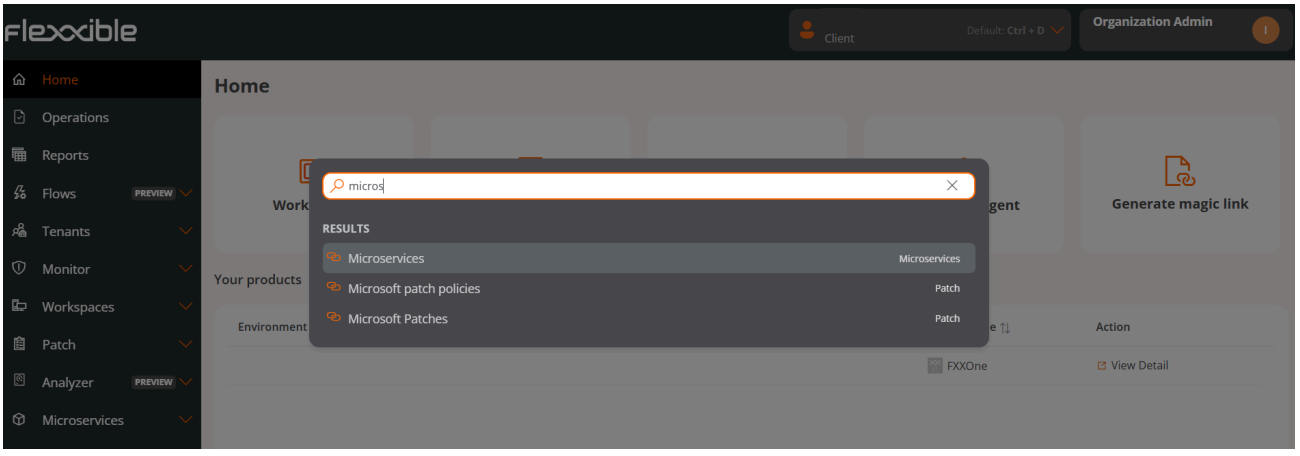
This option allows defining the country, according to which the platform interface settings will be defined.

#### Advanced menu

The advanced menu expands the Portal sidebar by adding shortcuts to specific functionalities of the other modules, so, for example, you can jump to a specific section of Analyzer or Workspaces.

# Navigation bar

The navigation bar allows the user to go directly to specific sections and subsections of the Portal or change the organization to manage. For example, a user who wants to access the Microservices section can do so quickly by typing the characters of the word *microservice* in the search box; similarly, if the user wants to change organization, they should type characters that match the name of the organization they want to manage, and then press `Enter`.




## Considerations about the navigation bar

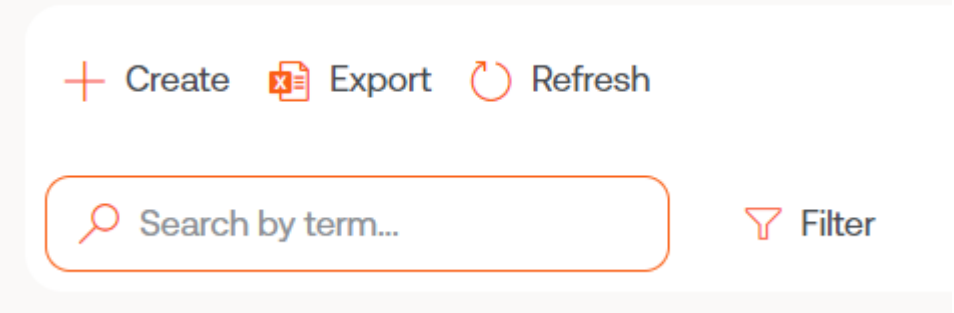
- Access to the navigation bar is done through `Ctrl + K` (`Cmd + K` on Mac).
- Allows accessing recent navigations performed by a user from an organization. The navigation history will change if the user changes the organization.
- Searches must be performed in the same language that the user has configured in Portal.

- To exit the navigation bar, press `esc` on the keyboard.

# Tables

Tables are a fundamental part of Portal because they are used to display data in all sections of the application. They are generally structured as follows:

## Top bar




#### New

The `New` button opens a form to enter the requested data. The fields to be completed depend on the section of Portal being consulted. For example, if the user is in `Tenant`, the form would ask to add the information to create a new tenant.

#### Export

To export the list observed in the list view, just click `Export`. This action will download an excel file with the data displayed in the table.

#### Reload the table

The `Reload the table` button is a feature option, very useful when you want to refresh the list, especially when new data has been created.

#### Search by term

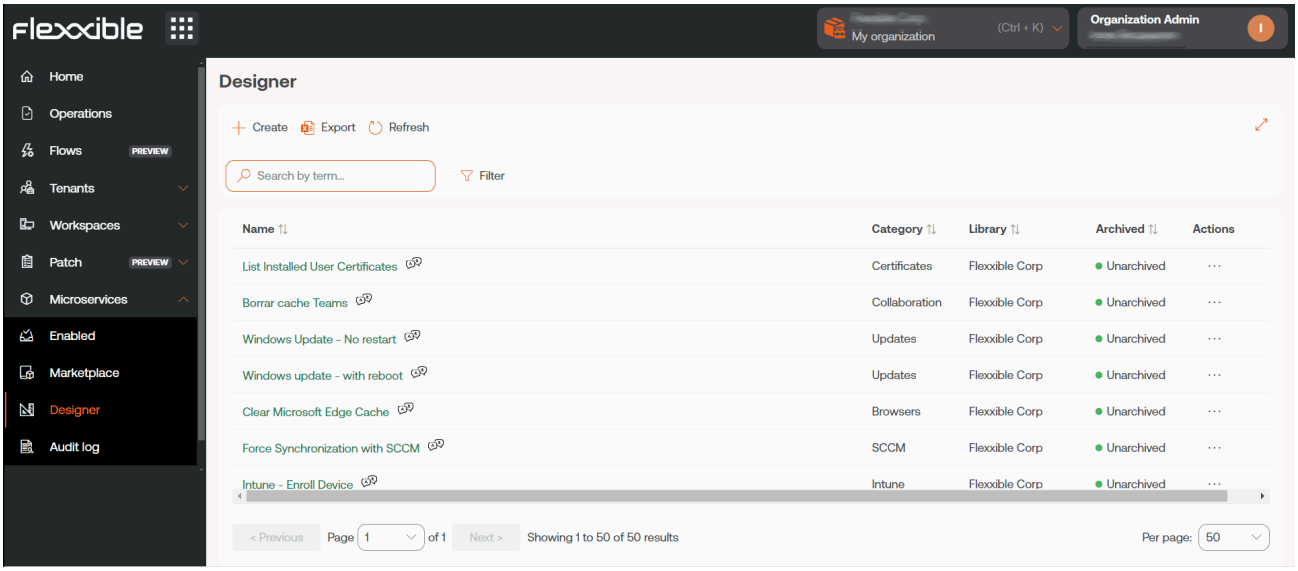
The `Search by term` field allows for more precise searches. You can enter a word that matches the data you are looking for.

**Filter**

The `Filter` button is a more complete alternative for searching. Clicking on it displays a menu to choose the `Field` of the table where you want to search; once the field is selected, the `Value` option enables to enter a term you want to filter by. You can create as many filters as there are field options displayed when clicking on `Filters`.

**Full screen**

Considering that tables are an essential part of Portal, the full screen button expands the table size to improve data visibility and enhance the user experience.

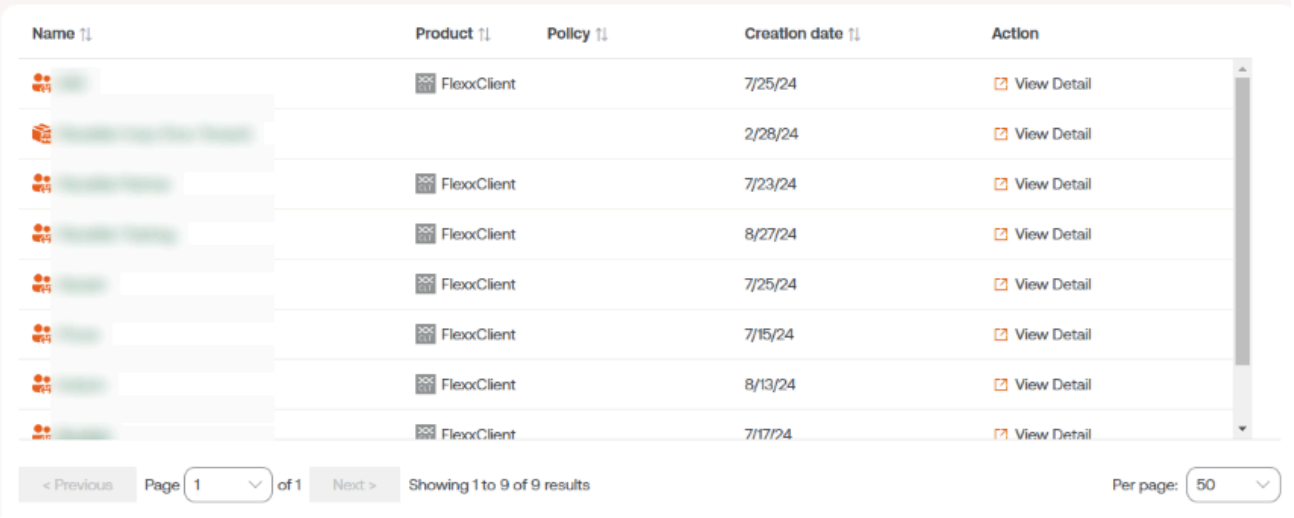



# Content

Table columns order the information according to fields. The first column is always `Name`, referring to the section where the user is at that moment; for example, if the user is in `Flows`, the table will display the name of the existing flows. The name of the following columns varies according to the section of Portal being consulted.

The content of the columns can be sorted in ascending or descending order, alphabetically. And the width of these can be adjusted by placing the cursor between two

field names.

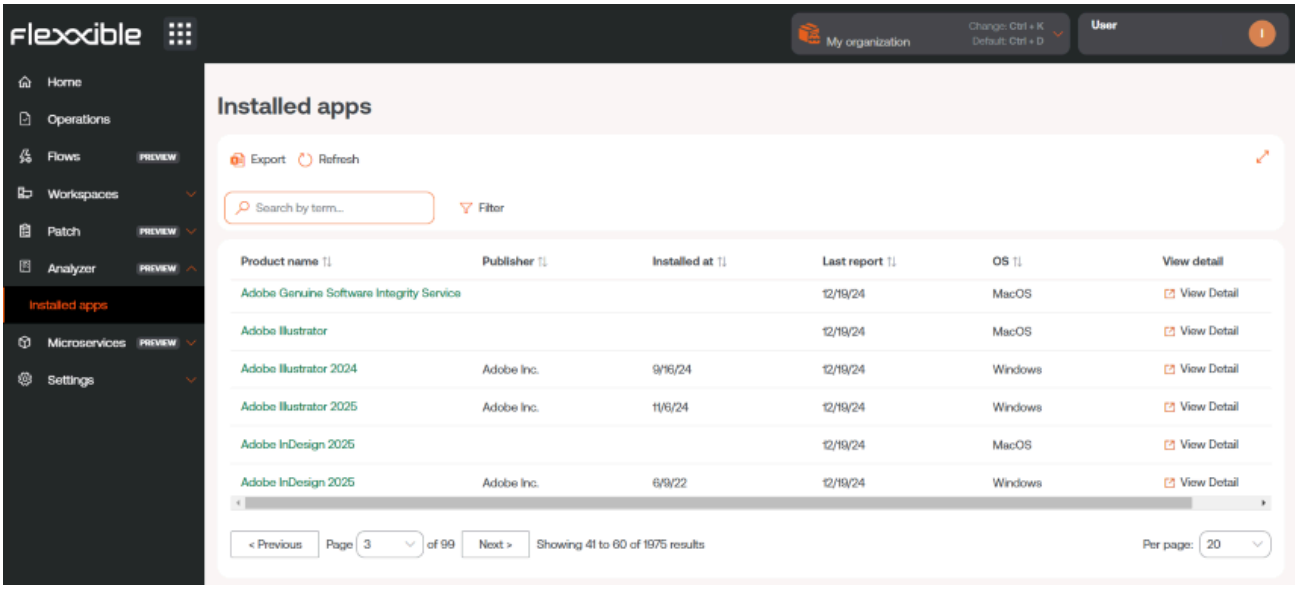



## Bottom bar

All tables have at the bottom a navigation bar that allows you to select how many results to show per page, and also gives the possibility to choose the page number you want to go to.

# Portal / Analyzer in Portal

The Analyzer section of `Portal` allows you to check information about applications installed on an organization's devices and the licenses acquired.




The information provided by Analyzer in Portal can also be accessed from the `Workspaces` section in the Analyzer module.

# Portal / Analyzer / Installed apps

The `Installed apps` list view shows detailed information about all installed applications found by the FlexxAgent on the organization's devices.

The table offers the following data:

- **Product Name**: name of the installed application
- **Publisher**: company that developed the application
- **Installed at (UTC)**: date and time when the application was first reported on a device, in Coordinated Universal Time standard
- **Last report (UTC)**: date and time of the last report of the application on a device, in Coordinated Universal Time standard
- **OS**: operating system of the device on which the application is installed
- **Number of installations**: number of application installations, calculated every two hours
- **View detail**: opens the application's detail view

## Installed Apps Details

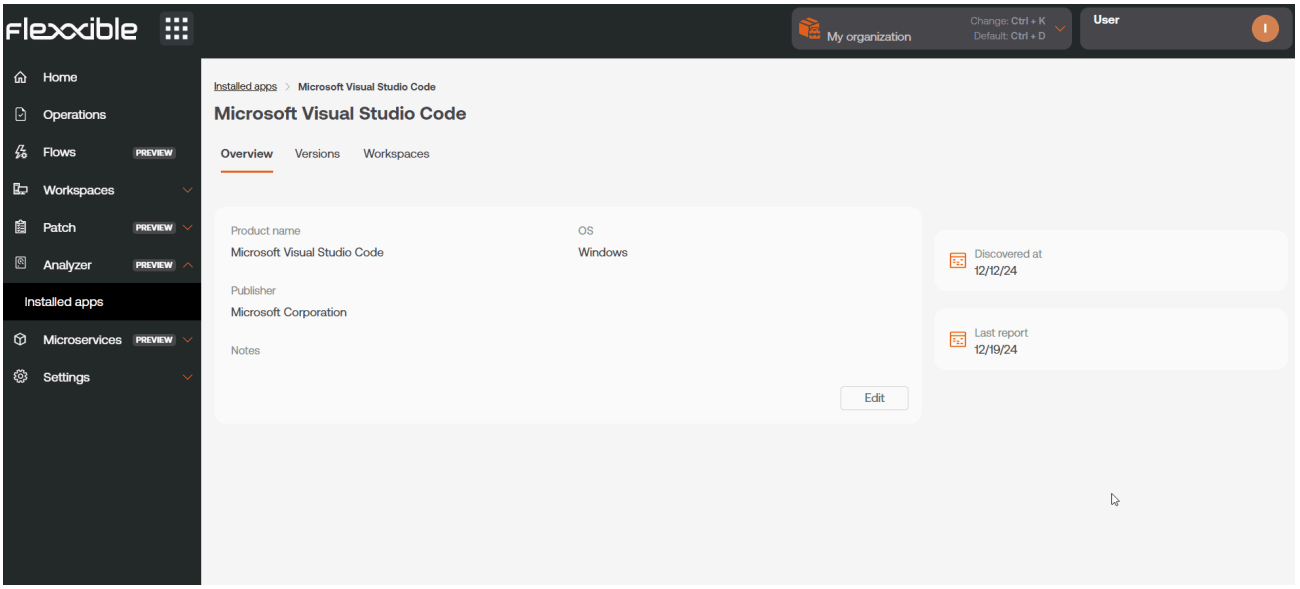
To access specific information of an installed application, from the overview click on the application's name or the `View Details` option. The following three tabs will be displayed:

- Overview
- Versions
- Workspaces

> **INFO**
>
> Installed applications are reported at each FlexxAgent startup; from that moment, the information is updated every 12 hours.

### Overview

From here, you can see the same information as in the list view, plus the `Edit` button, which opens a modal window with a form to enter free text as a note about the application.




## Versions

The columns of this table show the following information:

- **Version**: version number of the application being queried
- **Number of workspaces**: number of devices where this version is installed
- **Installed at (UTC)**: date of the first report of the application for that version, in Coordinated Universal Time standard
- **Last report (UTC)**: date of the last report of the application for that version, in Coordinated Universal Time standard

If you click on the version number, you will be redirected to a detailed view to see which devices have that version of the application installed and the date of its last report.

## Workspaces

The columns of this table show the following information:

- **Name**: name of the device where the queried application is installed

- **Version**: version number of the application installed on the device
- **Installation Location**: location of the application file on the device
- **Last report (UTC)**: date of the last application report on the device, in Coordinated Universal Time standard
- **Installed at (UTC)**: date of the first report of the application on the device, in Coordinated Universal Time standard

# Portal / Analyzer / Licenses

From this section, you can access information about all the software licenses that the organization has acquired. With access to this data, the organization can study the cost generated by the installation or execution of the applications on its devices to minimize the extra costs that can result from poor license management.

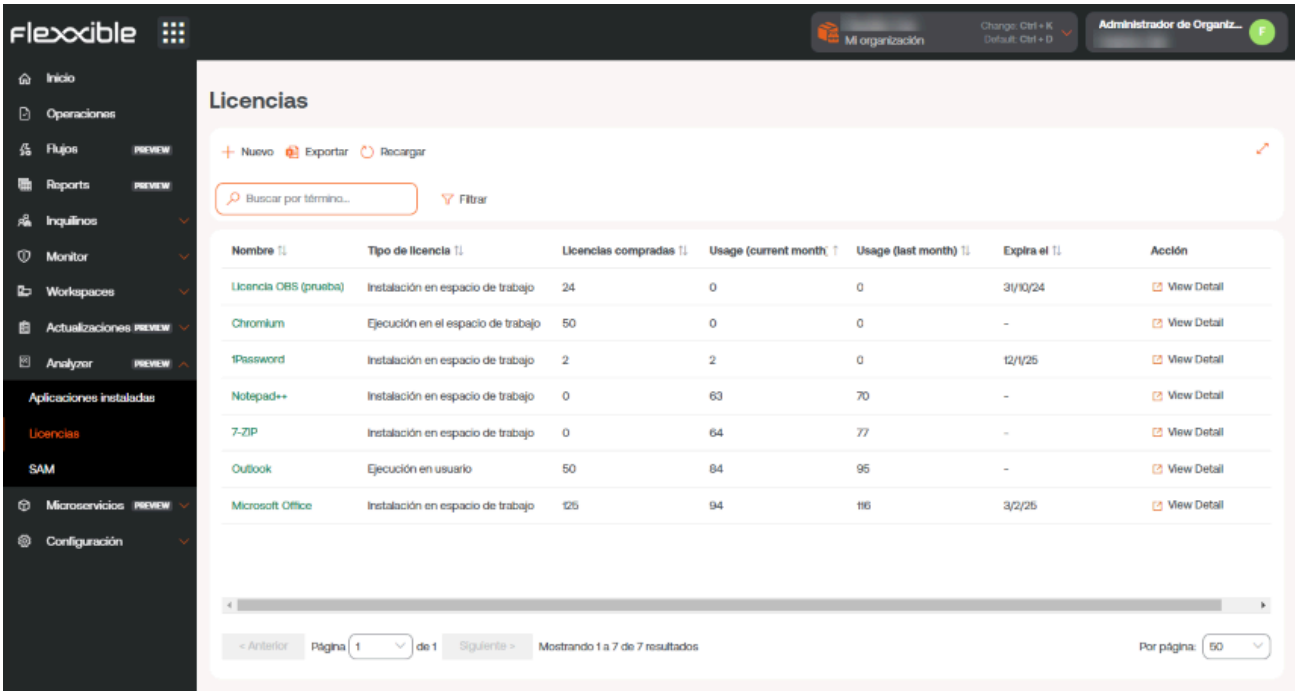
## Types of licenses

`Licenses` distinguishes three types of licenses:

- **Installed on the device**: the charge for these licenses is based on the installation of at least one of the applications that make it up.
- **Run on the device**: the charge for these licenses is based on their use (execution) and not on the installation on the device.
- **Run on user**: similar to the licenses run on the device, the charge for these licenses is based on their use (execution) by the user.

> **INFO**
>
> The use of a license starts being recorded from the moment it is created and linked to `Installed applications`

## License list view



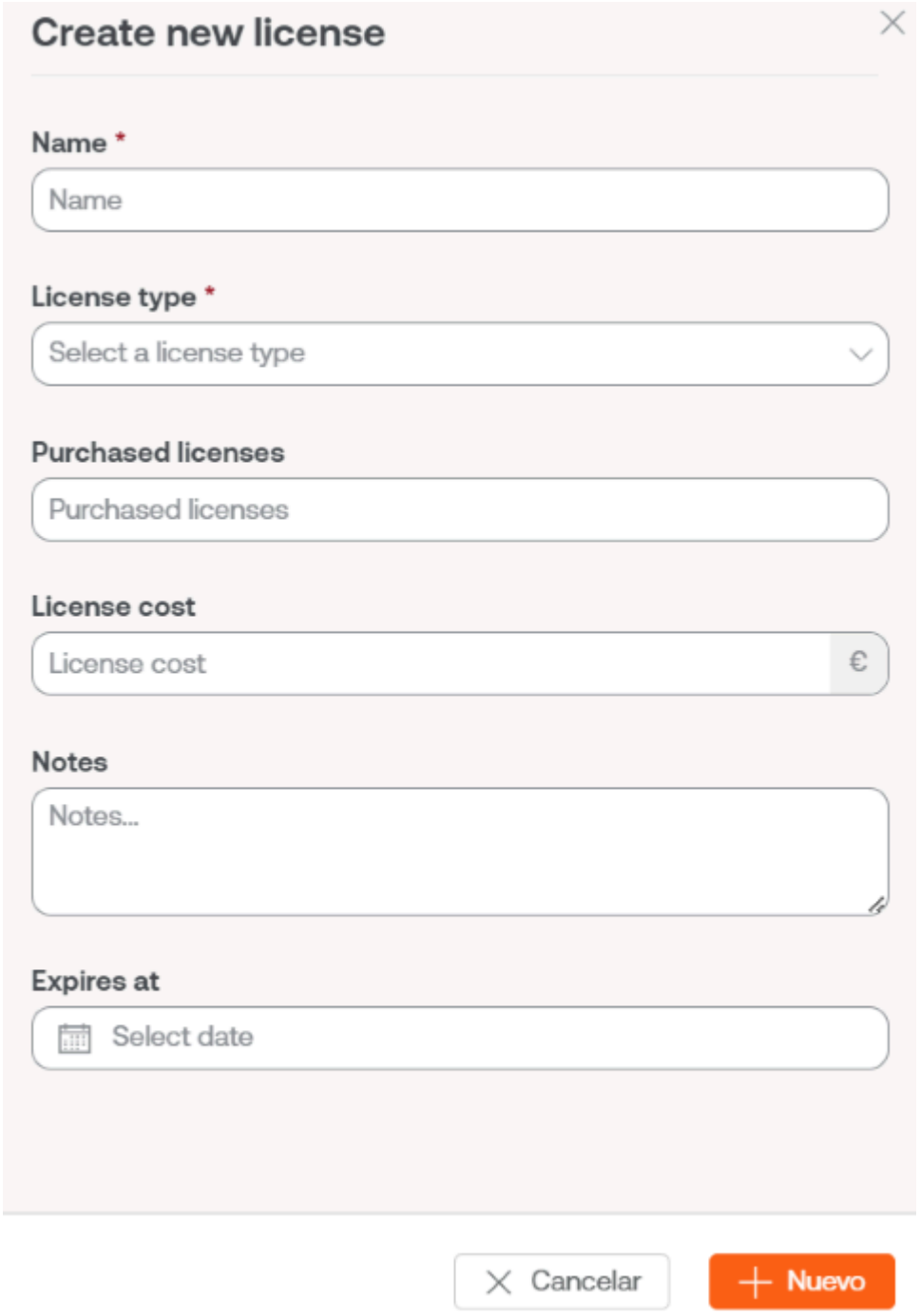

The list view shows a table with the following information:

- **Name**: name of the license
- **Type of license**: installed on the device, executed on the device, or executed by user
- **Acquired licenses**: number of licenses purchased
- **Usage in the current month**: number of licenses used in the current month
- **Usage in the past month**: number of licenses used in the previous month
- **License expiration date**: deadline for the use of the license

From the same table, you can access `View details`, to see specific data of the selected license through four tabs: `Details`, `Installed apps`, `Running apps`, and `Usage history`.

## Create a License

To create a new license, click the `New` button located in the list view. Next, a form will open requesting to fill in the following fields:




- **Name**: name of the license that the device has
- **Type of license**: option to choose the type of license
- **Purchased licenses**: number of licenses acquired
- **License cost**: cost of the license, in euros
- **Notes**: additional notes about the license
- **Expires on**: expiration date of the license

# License detail view

The license detail view consists of a different number of tabs depending on the type of license, for all license types the following will appear:

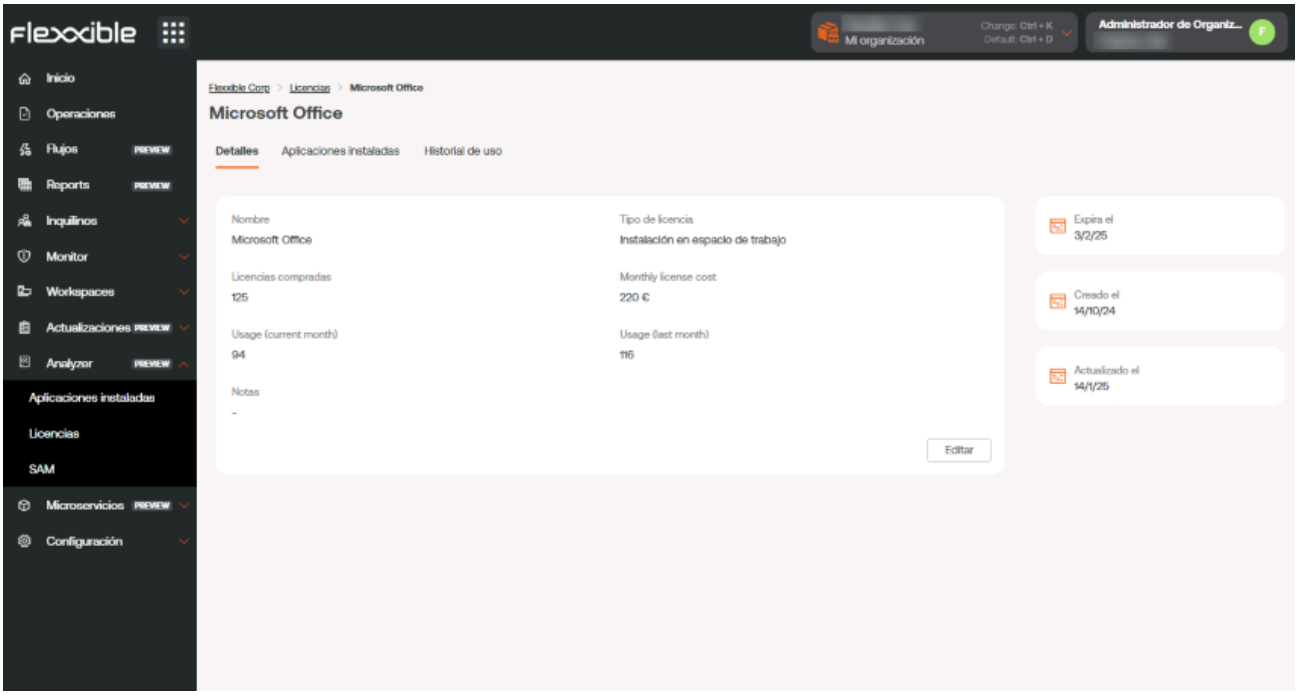
- Details
- Installed applications
- Usage history

For licenses of type `Run on the device` or `Run on the user`, the following will also be enabled:

- Running applications

## Details

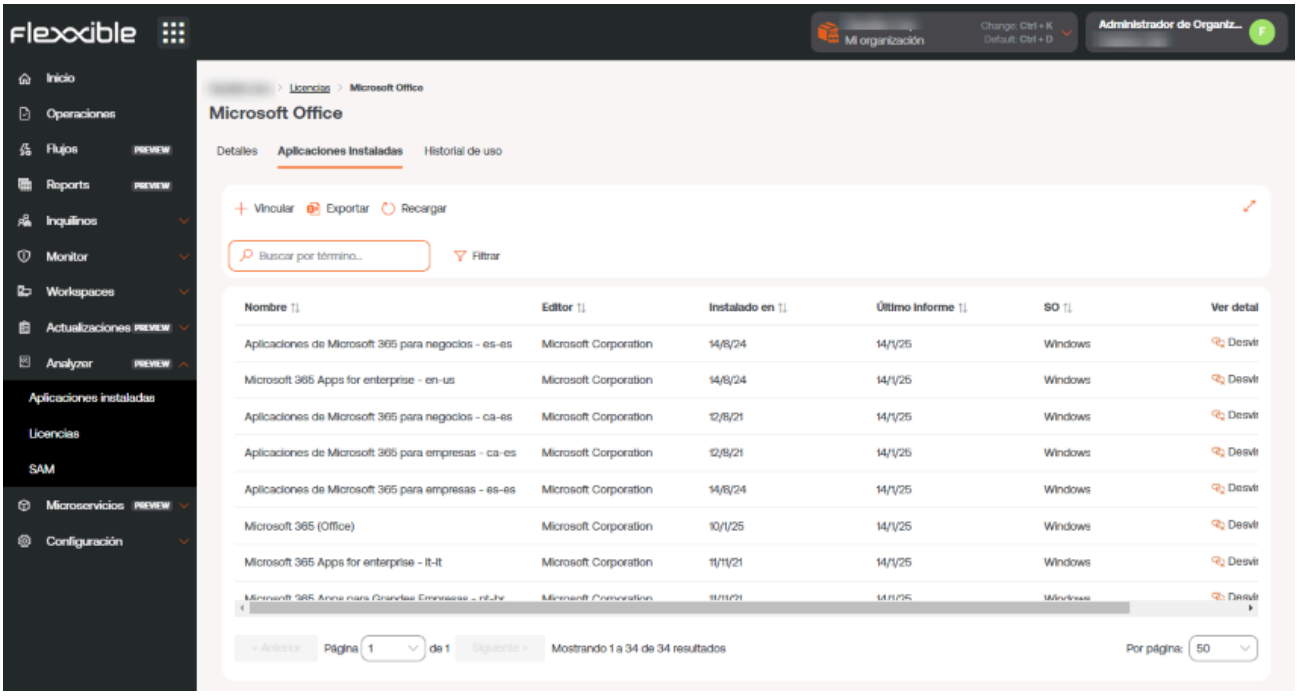
The `Details` tab shows the same information as the list view table, plus the license cost and information about issuance, update, and expiration dates.




The `Edit` button opens a form to fill in the missing information or update the existing data. From there, the user also has the option to add free notes with any relevant information.

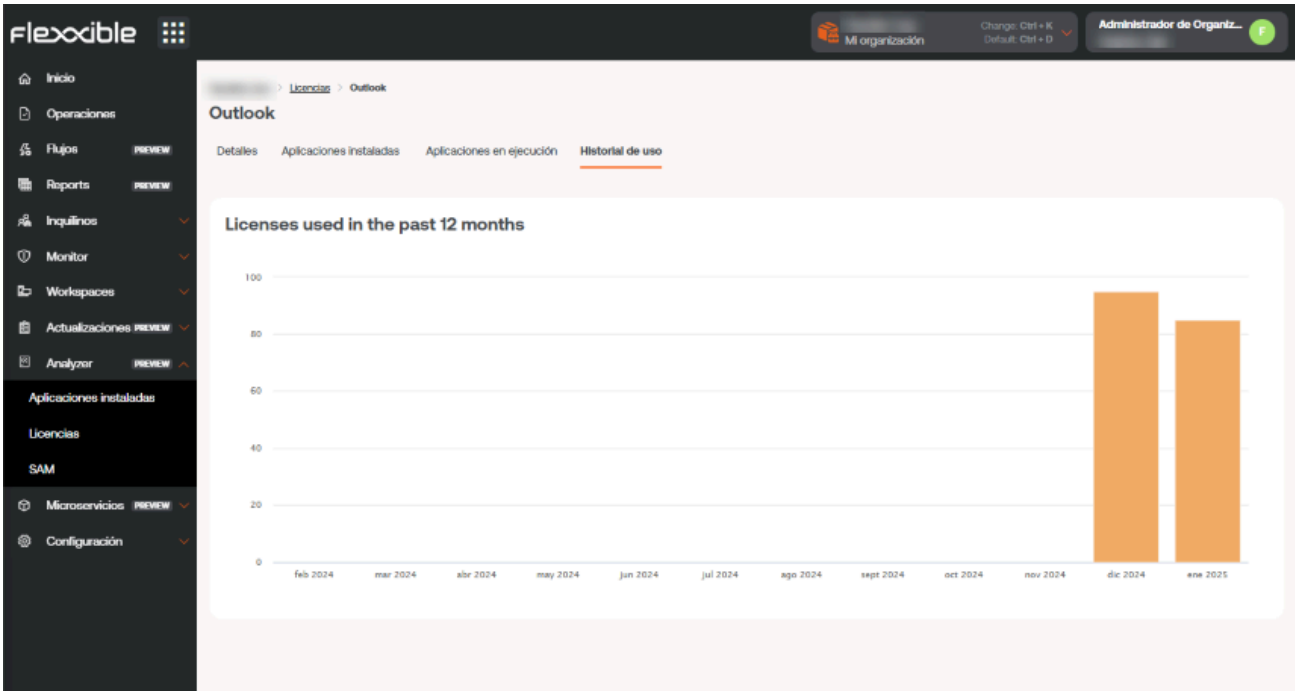
# Installed apps

The `Installed apps` tab shows a table with a list of the installed applications that are part of the acquired license.



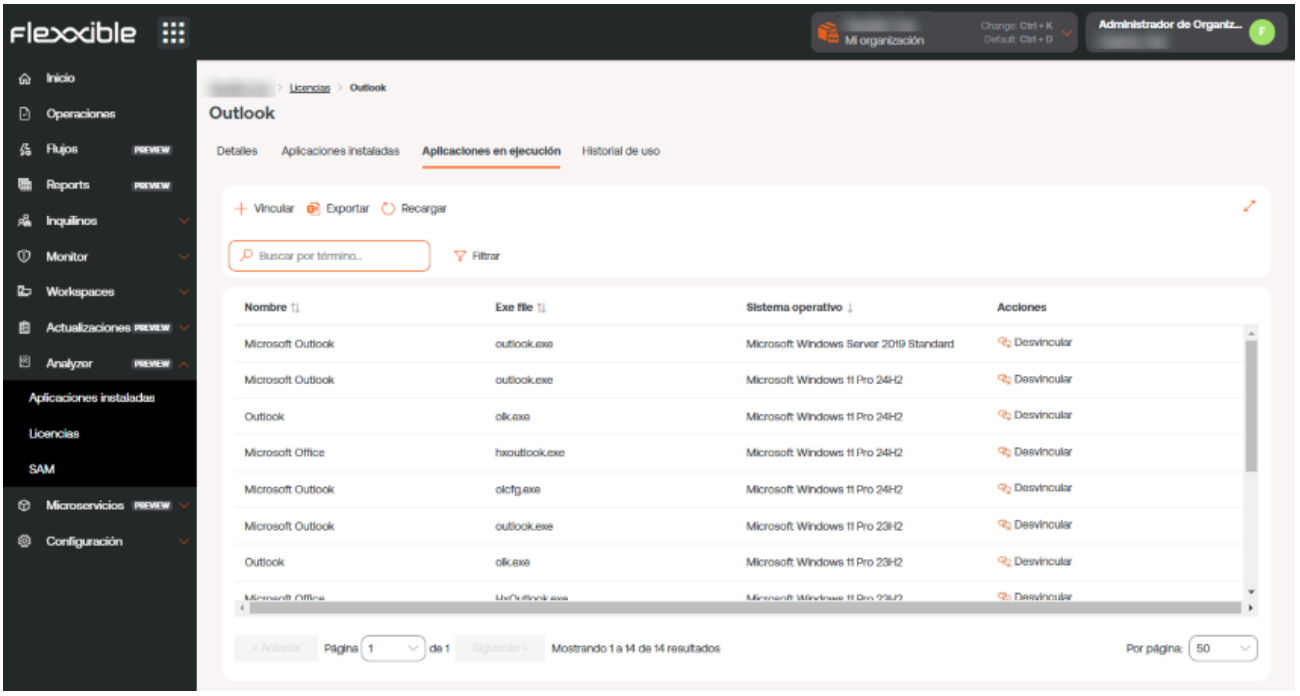

It presents information such as the application name, the company that developed it, installation and update dates, the operating system it works on, and the option `unlink`, to detach the application from the list. On the other hand, the `Link` button opens a form with options to link an application to the list of installed applications. And `Refresh` updates the list after making changes.

# Usage history




Allows to see the usage of the license per month in a bar chart, from the moment of its creation.

## Running applications



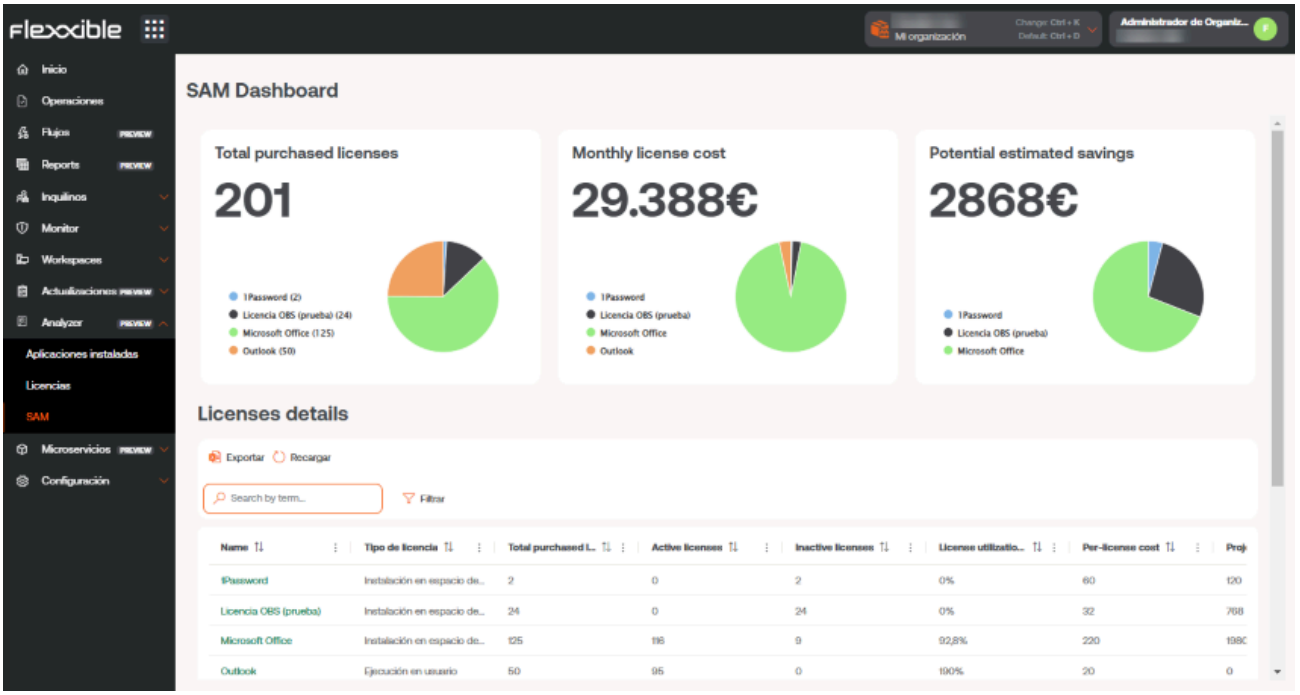

Provides information about the running applications linked to this license, that is, those applications whose execution must count a license as `in use`, with data such as the

name, the binary name in the filesystem, and the operating system where it was discovered.

From this view, it is also possible to link or unlink applications to the license.

# Portal / Analyzer / SAM

When at least one license has been created and properly configured, its usage can be measured in the `SAM` section.




This view consists of three widgets and a list view where it's possible to consume information about usage, cost, and potential savings that could be applied to save costs on the configured licenses.

> **INFO**
>
> The usage of a license starts being recorded from the moment it is created and associated with `Installed applications`.

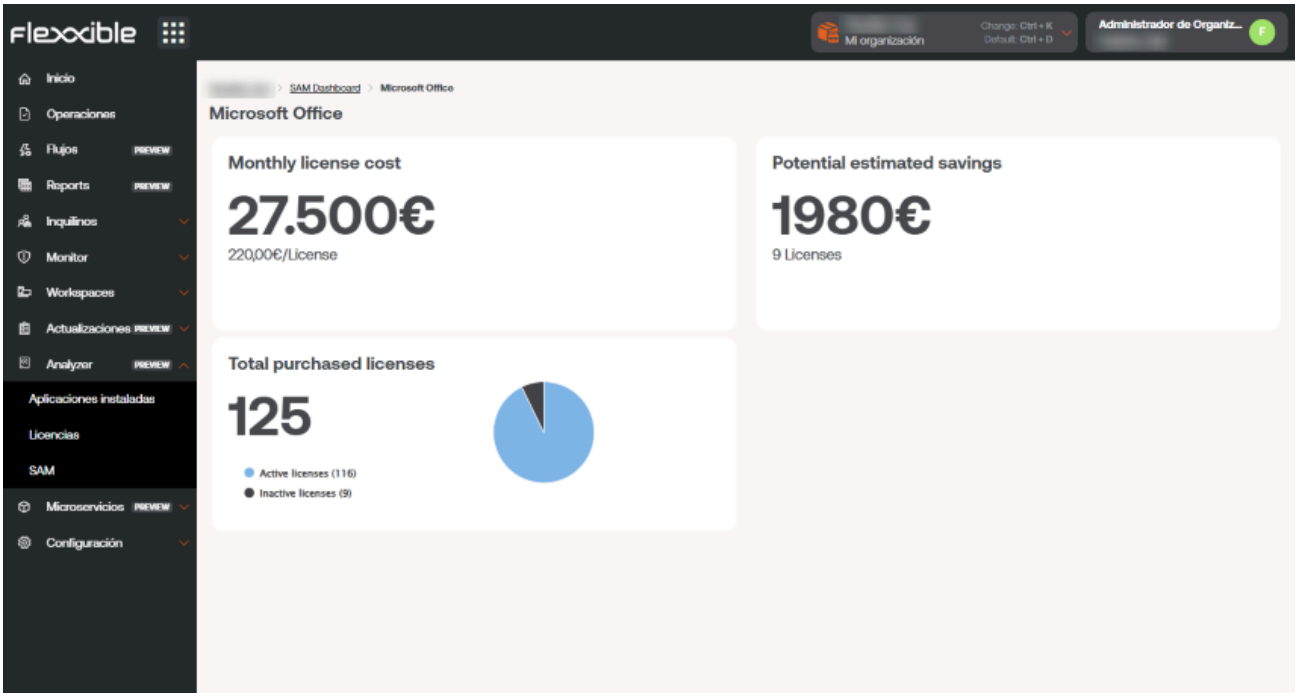
The widgets included in the dashboard contain information about:

- Total licenses purchased: the total number of licenses purchased, aggregated by license
- Total cost per month: aggregated by license
- Potential savings: provides the detail in `€` of the licenses that are unused and may not be renewed to optimize costs, aggregated by license.

At the bottom of the dashboard is the `License Details` table, which contains a list with the following information:

- License name
- License type
- Licenses purchased
- Number of licenses in use
- Number of unused licenses
- License usage percentage
- Price per license
- Potential savings
- Currency

By clicking on the name of any license in the table, we will access the savings view of the selected license:



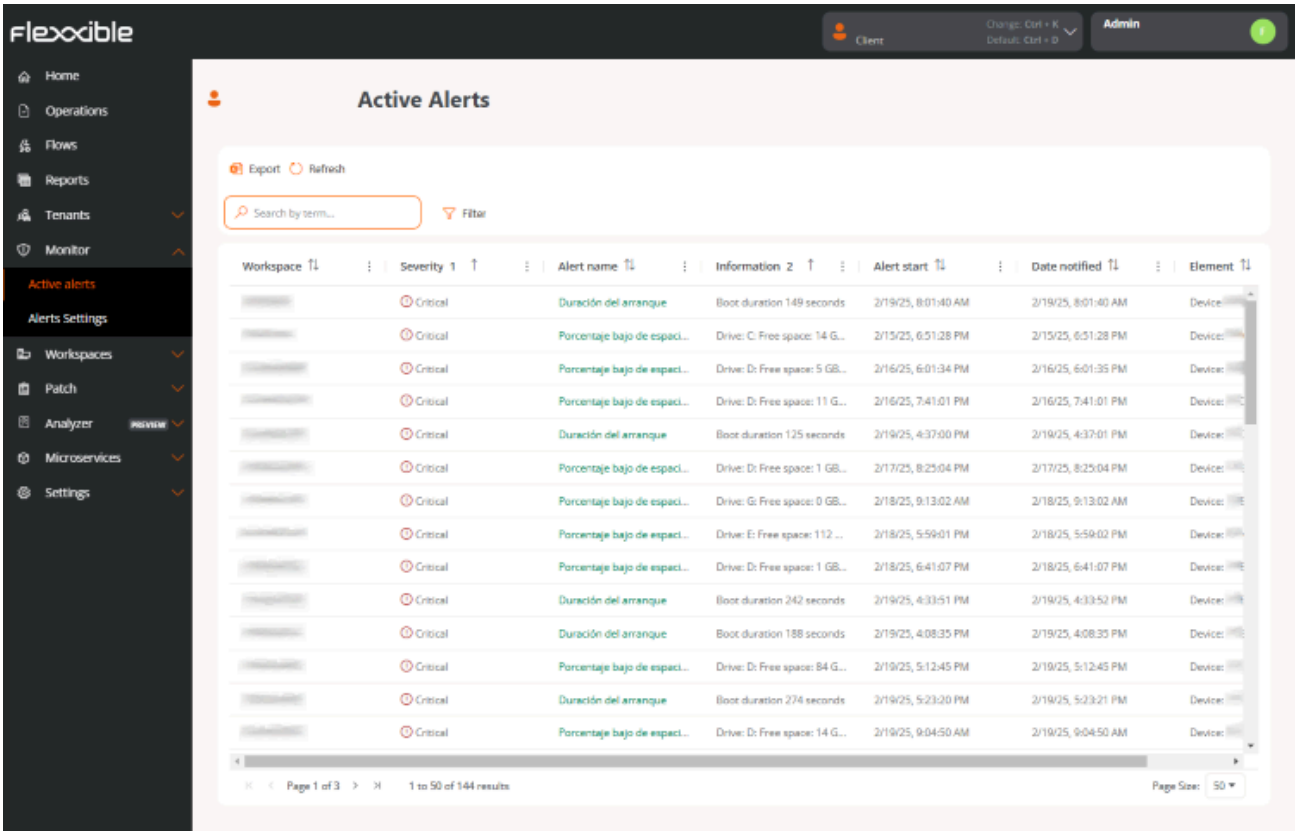

This detailed view provides the following information:

- The total monthly cost of the license
- The potential savings that can be applied to the license, according to its usage in previous periods.

- The total number of licenses purchased, segmented into licenses in use and inactive licenses.

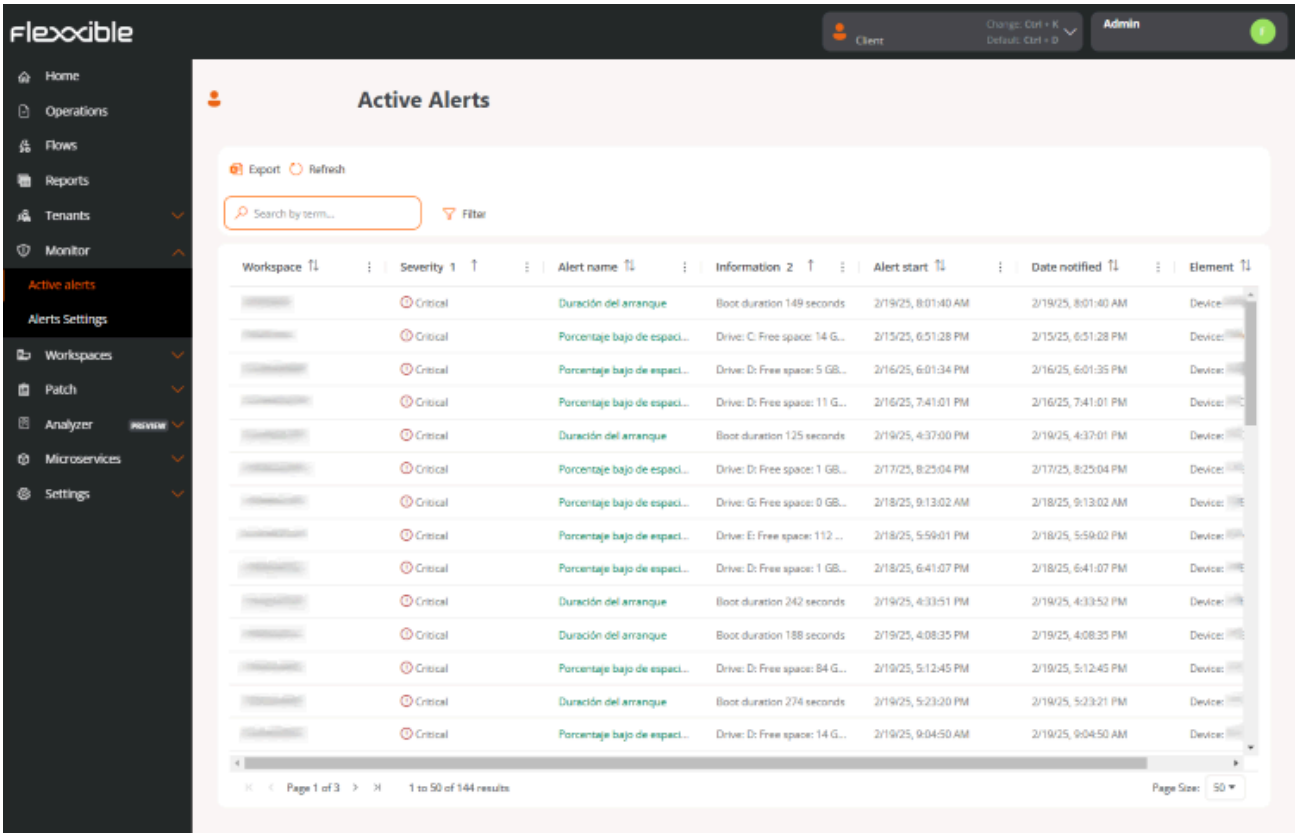
# Portal / Monitor in Portal

Monitor is the alerts and monitoring section of Portal. Composed of two sections: *Active Alerts* and *Alert Settings*, it provides real-time information about important events that can compromise device functionality through alerts, and allows the configuration of predefined alerts to be adjusted to the needs of each organization.



# Portal / Monitor / Active alerts

Alerts notify about certain events that have occurred in the devices' system, that have met a condition and exceeded a predefined threshold. `Active alerts` allows you to see the list of alerts generated on the organization's devices.



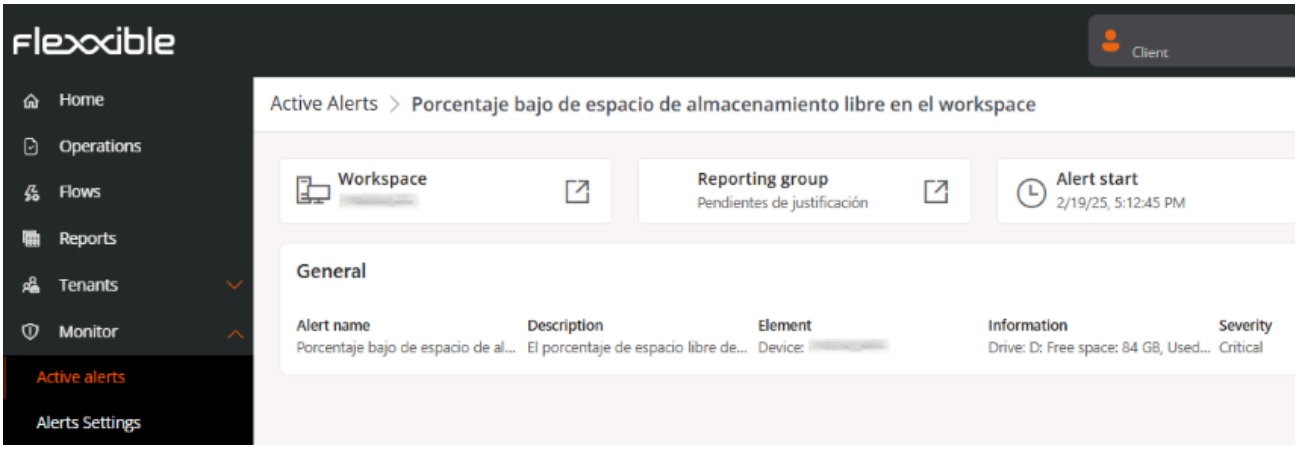

The table contains the following fields:

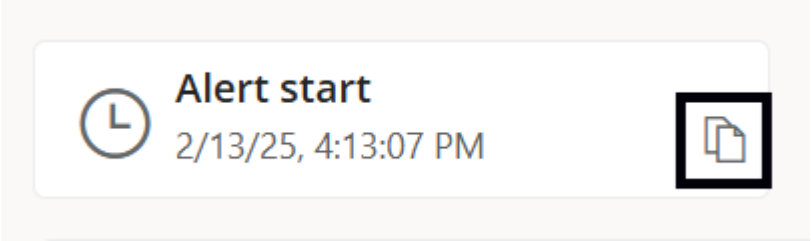
- **Workspace**: type of device where the alert is recorded
- **Severity**: alert severity level (*Informative*, *Warning*, and *Critical*). Please check Alert severity for more information.
- **Alert name**: name assigned to the alert
- **Information**: description of the alert
- **Start date**: day and time when the alert is recorded
- **Notification date**: day and time of the alert notification
- **Item**: name of the device where the alert is recorded

> **INFO**
>
> From this view, client-type organizations can also view alerts generated on their suborganizations' devices.

# Alert detail view

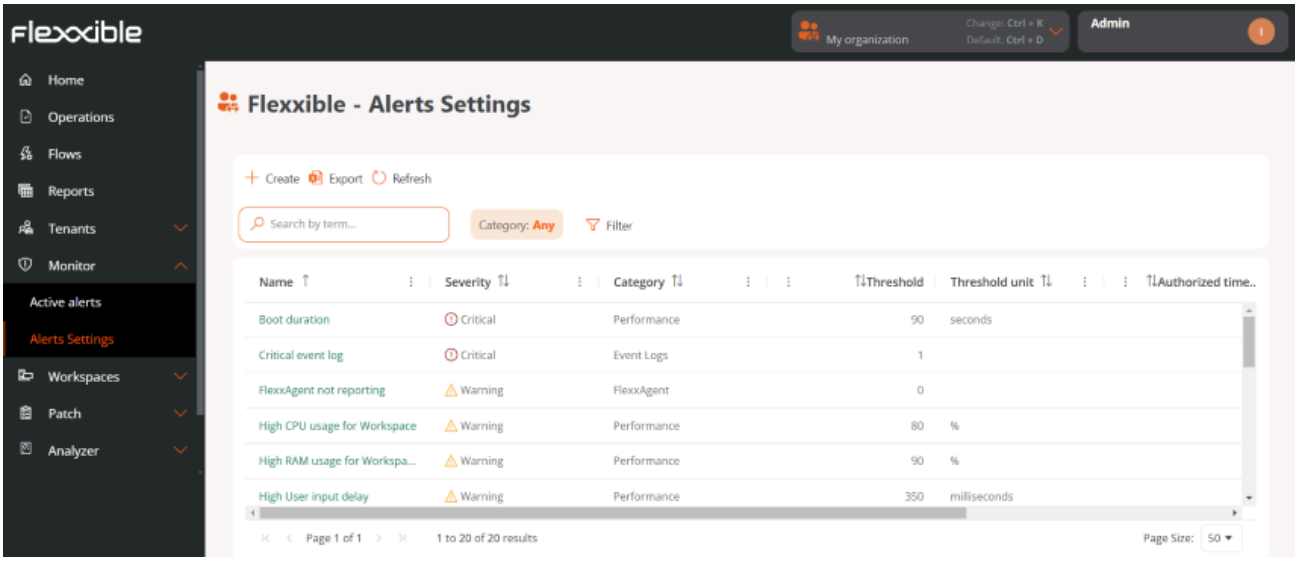
Clicking on the alert name provides access to its specific data. The information's format allows for easy reading and offers the possibility of copying each element of the content.



# Portal / Monitor / Alert Configuration

This section allows you to view in detail the alerts that could be activated on the user's device and to know the status of said alerts in the rest of the organization. From this section, you can also create new alerts based on the events (event logs) of the system of the device in use.



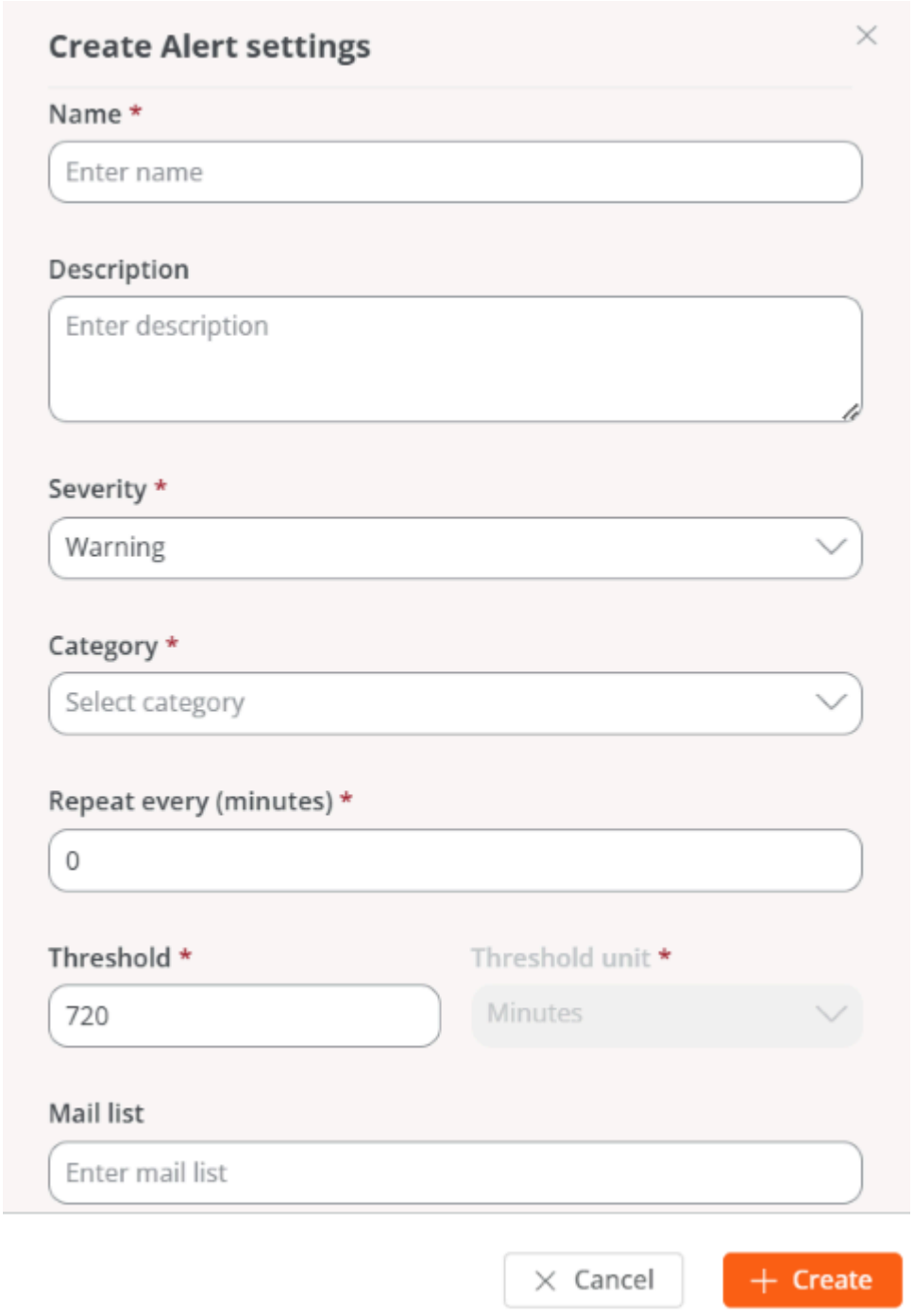

The `Alert Settings` list view shows a table with the list of alerts that could be activated on the device. The fields of the table contain the following information:

- **Name**: name of the alert
- **Severity**: alert severity level. Refers to the impact of an event on the system. The severity levels can be consulted here.
- **Category**: name of the category to which the alert belongs. The categories can be consulted here.
- **Threshold**: in figures, the limit that defines the condition to trigger an alert.
- **Threshold unit**: unit of time, percentage, or megabytes that complements the threshold figure.
- **Authorized time (minutes)**: maximum allowed time for a condition before a system alert is generated.
- **Repeat every (minutes)**: time that will elapse before sending a new alert if the condition persists.

- **Enabled**: indicates whether the alert is enabled or disabled.

# Create a new alert setting

At the top of the main `Alert Settings` view, the `New` button allows a user to create a new alert based on the information provided by the events (event logs) generated in the device's system.



The form requests the following information:

- **Name**: name of the new alert
- **Description**: text that defines the meaning of the alert
- **Severity**: allows you to choose the alert severity level. The severity levels can be consulted here.
- **Category**: allows you to choose which category the alert belongs to. The categories can be consulted here.
- **Repeat every (minutes)**: time that will elapse before sending a new alert if the generating event has not been resolved
- **Threshold**: in figures, the limit that defines the condition to trigger an alert.
- **Threshold unit**: unit of time, percentage, or megabytes that complements the threshold figure.
- **Email recipients list**: email addresses of the users who will receive an alert notification. They must be separated by commas.
- **Alert message**: alert notification message that the email recipients will receive.
- **Event ID**: figure that identifies an event in the events (event log). An alert will be issued when an event with that ID is generated.
- **Search text**: text string that will trigger an alert when it appears in the device's event log.
- **Source**: part of the system where the event generating the alert occurs

## Alert Severity

The alert severity levels are divided as follows:

- **Informative**: the event is not critical, but system performance could be improved.
- **Warning**: the event could compromise system performance if not resolved soon.
- **Critical**: the event requires immediate attention as it compromises system performance.

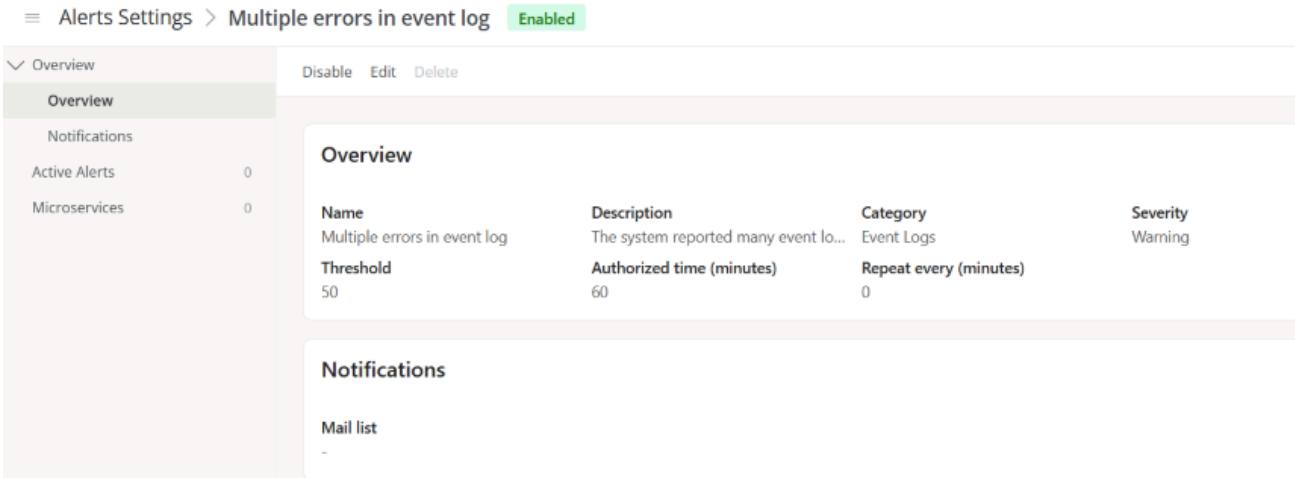
## Alert categories

Alert categories indicate in which part of the devices' system events generating an alert are recorded. They are divided as follows:

- Connectivity
- FlexxAgent
- Hardware
- Performance
- Events logs
- Security
- Printing
- Storage

# Detail view

To see the alert details, click on the alert name in the table.




This view shows the alert status at the top. If available, the word *Enabled* is shown with a green background, and if it's not, the word *Disabled* is shown with a grey background. Next, the `Disable` or `Enable` button will allow changing its status as needed.

## Edit alert settings

If you want to change some options of the alert you are viewing, the `Edit` button in the detail view opens the form that allows you to edit the alert settings.

Predefined alerts are created in each organization. However, through the following fields, some changes can be made as required by each organization:

- **Repeat every (minutes)**: time that will elapse before sending a new alert if the condition persists.
- **Authorized time (minutes)**: maximum time allowed for a condition before a system alert is generated
- **Threshold**: in figures, the limit that defines the condition to trigger an alert.

From `Edit`, you can also add email addresses to define who will receive a notification when the system alert is generated. If entering more than one email address, they should be separated by commas.

# Sidebar menu

The detail view of each alert presents a sidebar menu on the left side of the screen to organize its information. It is divided into three tabs: *Overview*, *Active Alerts*, and *Microservices*.

## Overview

It shows alert data in a format that allows easy reading, as well as a `Notifications` tab that lists the emails of users who will be notified when an alert is activated on the device.

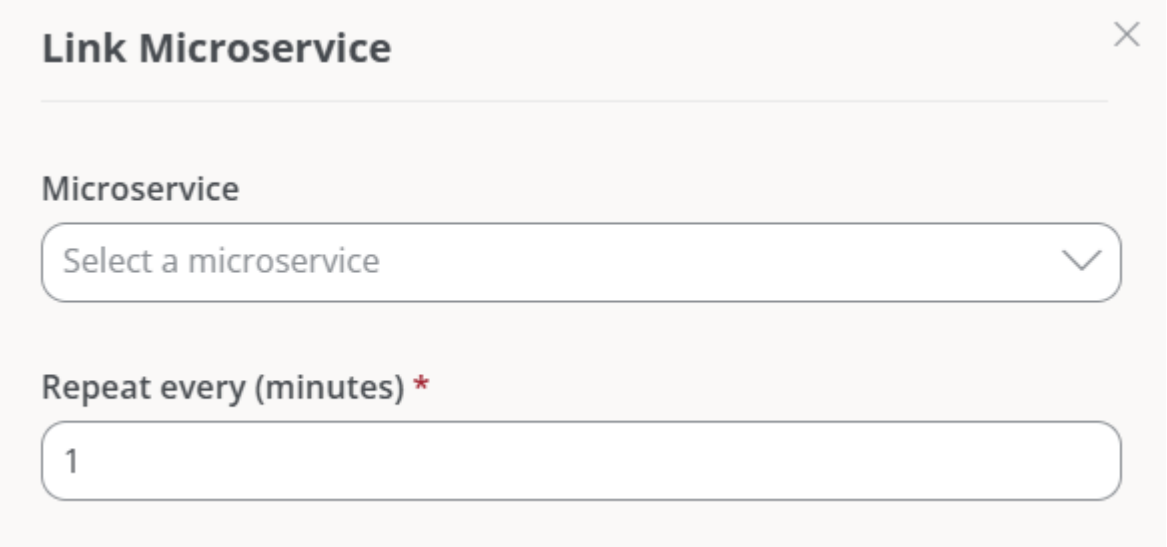
## Active alerts

It shows a table with the organization's devices that have the alert being consulted active. The table fields provide the following information:

**Workspace**: type of device where the alert is recorded **Information**: alert description **Start date**: date and time when the alert is recorded **Notification date**: date and time of alert notification **Element**: name of the device where the alert is recorded

## Microservices

There are alerts that could be resolved with the automatic execution of a microservice. The platform allows doing this by clicking the `Link` button. This action will open a form where you should indicate which microservice to associate the alert with and the time that will pass before running it again if the condition persists.

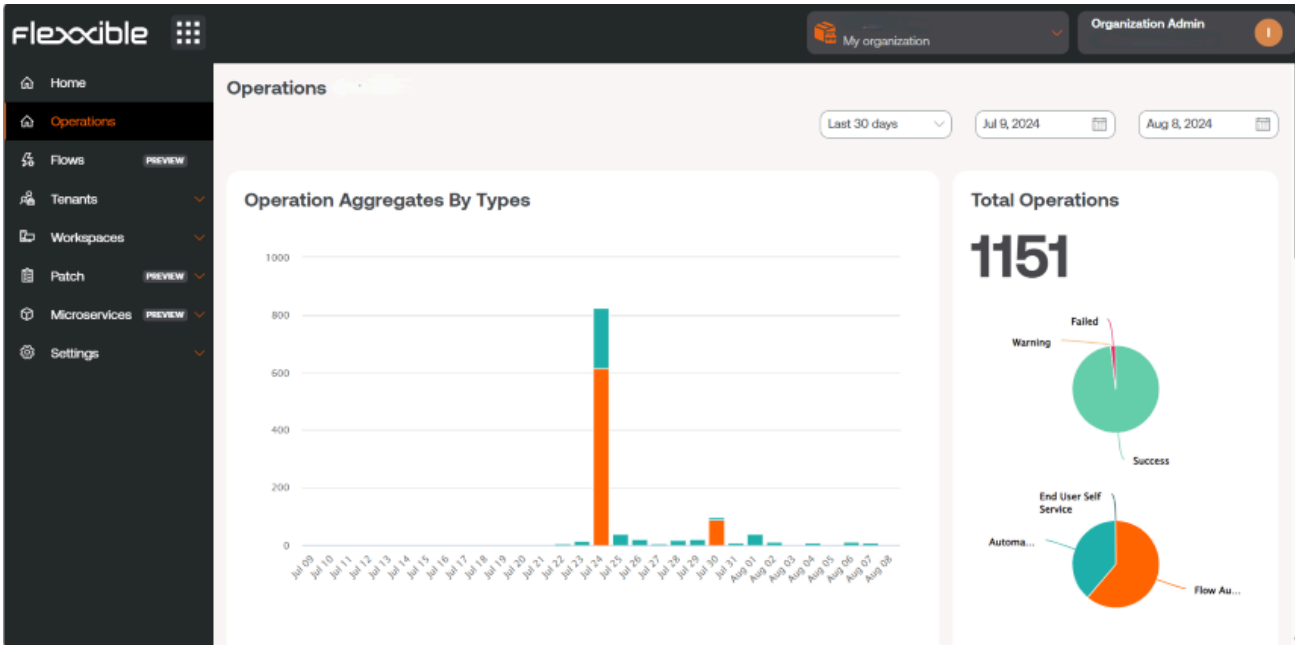


# Portal / Operations

The `Operations` section shows graphs of the three types of operations, regarding the microservices, that have been performed on the devices.

- **Automated Support Action**: these are the microservice executions performed on-demand from Workspaces by users who belong to the technical support teams.
- **Flow Execution**: these operations include the automatic executions of microservices in `Flows`, when conditions are met.
- **User microservice**: These are the executions of microservices performed by the user themselves, without needing help from the support team.

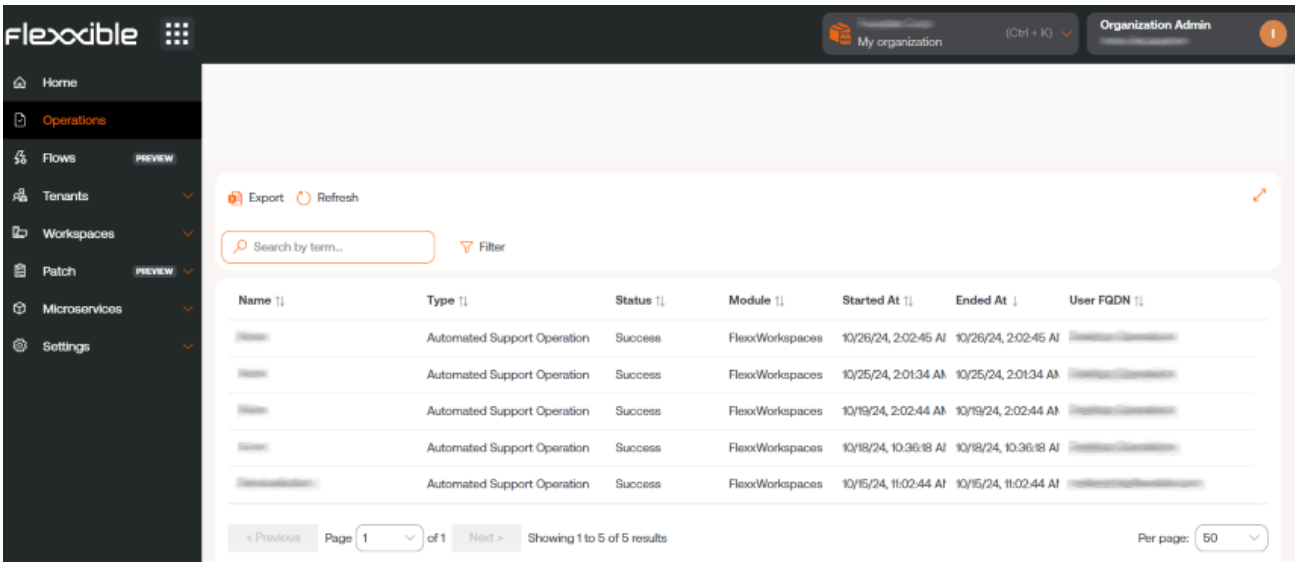
> All actions leave an audit record in the `Jobs` section of Workspaces, allowing for temporal traceability of the users and devices involved, as well as the details of the code executed and the output generated.




In this view, two types of graphs are generated, with results related to the date range set in the top menu.

- **Operations by Type**: shows the number of operations performed by type and day, according to the selected date cycle.

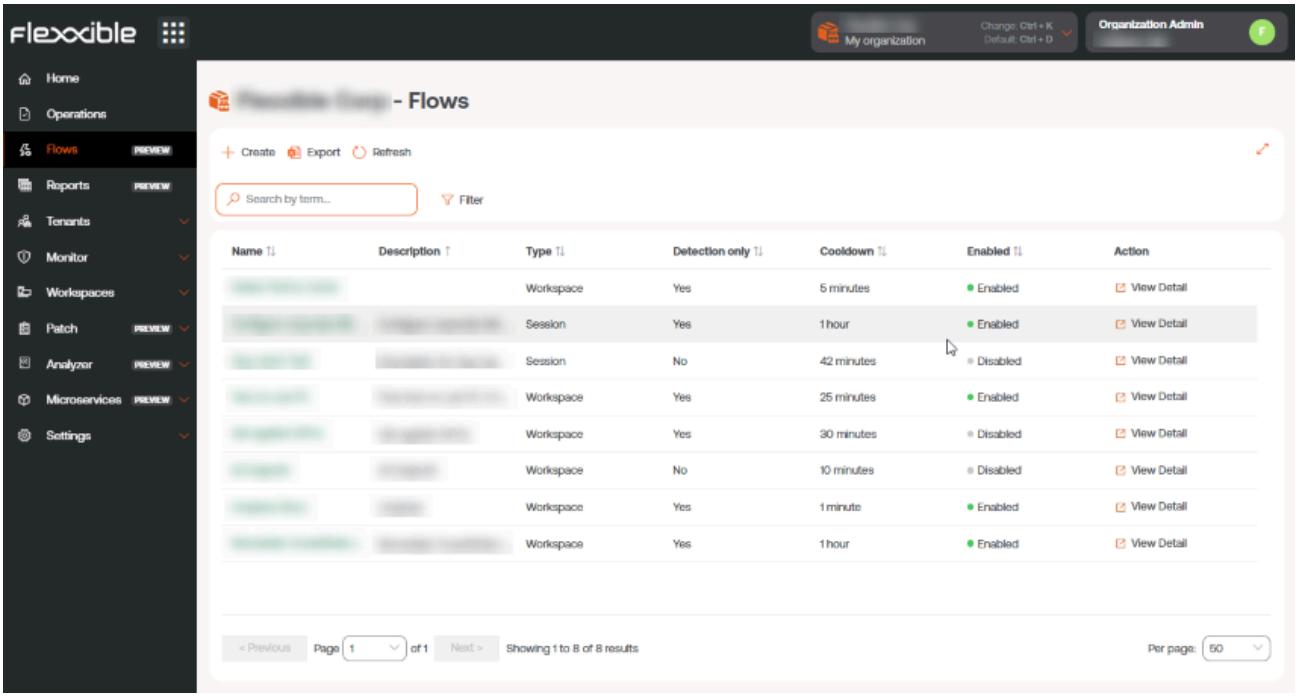
- **Total Operations**: provides two pie charts. The upper one indicates how many operations were successful, failed, or had warnings, out of the total operations executed. And the lower one indicates the type of operations performed from that total.




Operation List displays a table with details of the executed operations, specifying the type of operation, from which module they were carried out, and the start and end times. At the bottom of the view, there is a bar that allows you to navigate between pages, to see the details of all executions.

# Portal / Flows

This functionality allows creating automation flows designed to detect specific situations on devices. Through the evaluation of certain conditions, the system determines whether the corresponding actions should be executed based on the obtained result.




Flows simplify proactive diagnostic actions, quickly solve issues when there's a focus on their detection, and provide a very efficient way to enable self-remediation mechanisms over common problems. It also allows technical teams to couple devices to configurations defined by the organization, evaluating them periodically and adapting them if necessary.

The overview of Flows shows the list of flows created within the organization. The information gathered in the table is as follows:

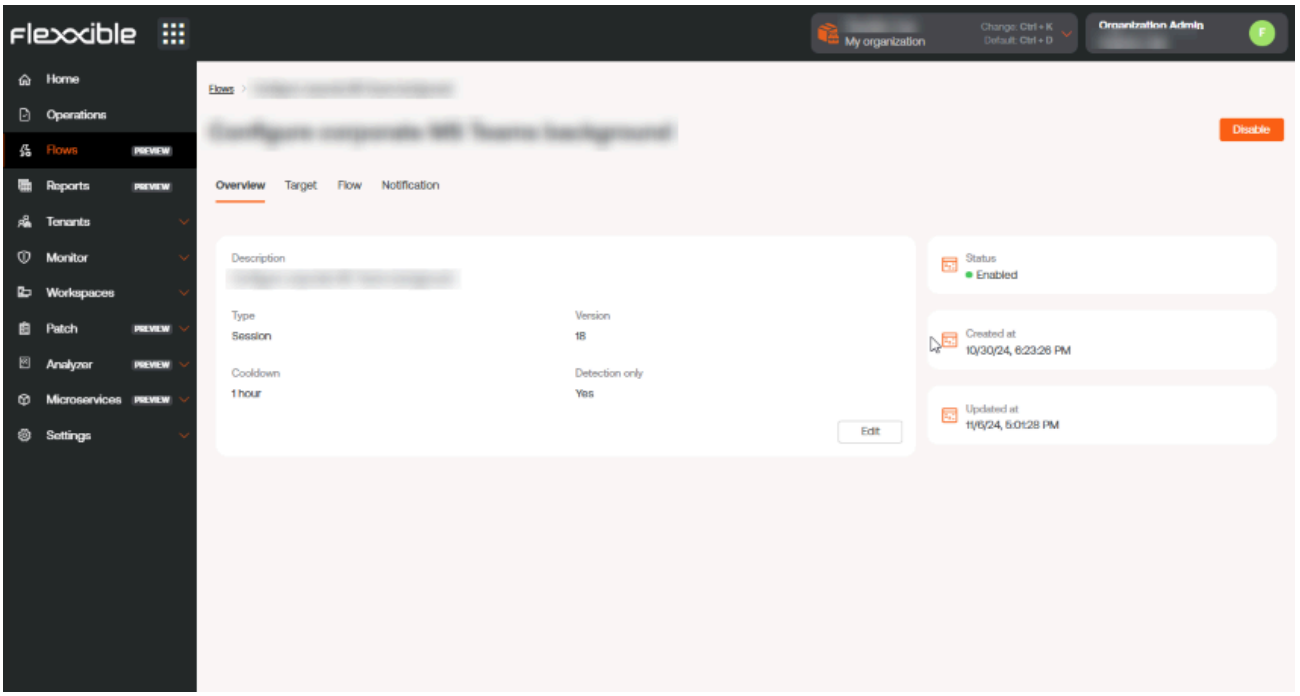
- **Name**: indicates the name of the flow.
- **Description**: indicates the purpose of the flow.
- **Type**: it is the execution scope of the flow, determined by the type of microservice to be executed. It can be done at the user session level, with the corresponding permissions, or at the device level, with administrative access.
- **Detection only**: evaluates conditions in a "sampling" mode. Detects those devices where the conditions are met but does not execute the microservice defined in the

flow.

- **Reuse time**: marks the minimum time that will pass, once the evaluated condition is met, for that evaluation to be executed again.
- **Enabled**: indicates whether the flow is *Enabled* or *Disabled*.
- **Action**: contains the `View Details` button, which allows customizing the behavior of the flow through the following options: Overview, Destination, Flow, and Notification.

> **INFO**
>
> In the top right corner of the flow detail view, there is a button that allows you to enable or disable it.

# Overview

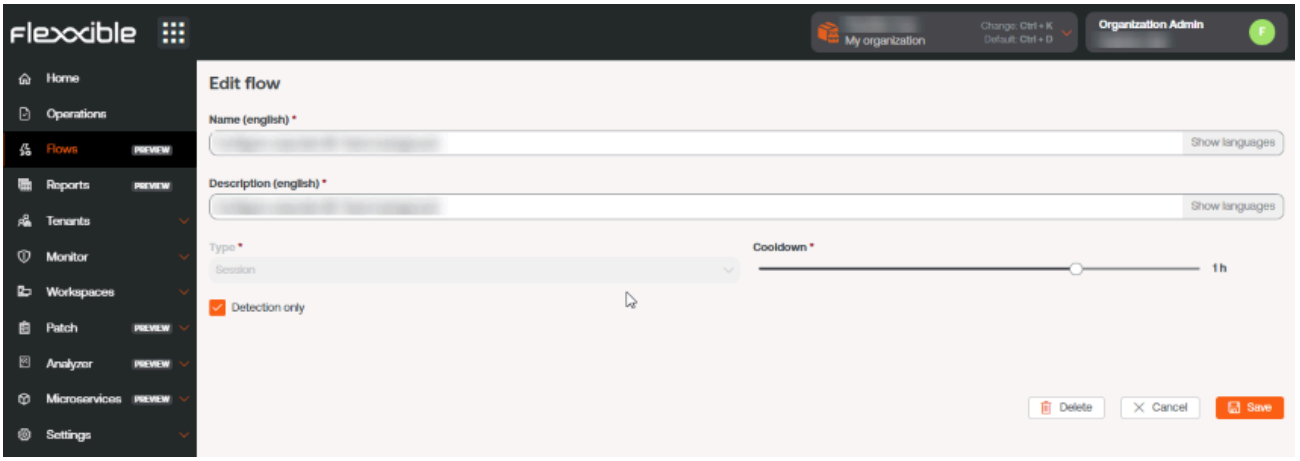



Stores general information of the flow.

- **Description**: indicates the purpose of the flow.
- **Type**: it is the execution scope of the flow, determined by the type of microservice to be executed. It can be done at the user session level, with the corresponding permissions, or at the device level, with administrative access.

- **Version**: indicates the version number of the flow; each time it is edited, the counter increases by 1.
- **Reuse time**: marks the minimum time that will pass, once the evaluated condition is met, for that evaluation to be executed again.
- **Detection only**: evaluates conditions in a "sampling" mode. Detects those devices where the conditions are met but does not execute the microservice defined in the flow.
- **State**: indicates whether the flow is enabled or disabled.
- **Created on**: shows the creation date of the flow.
- **Update Date**: shows the update date of the flow.

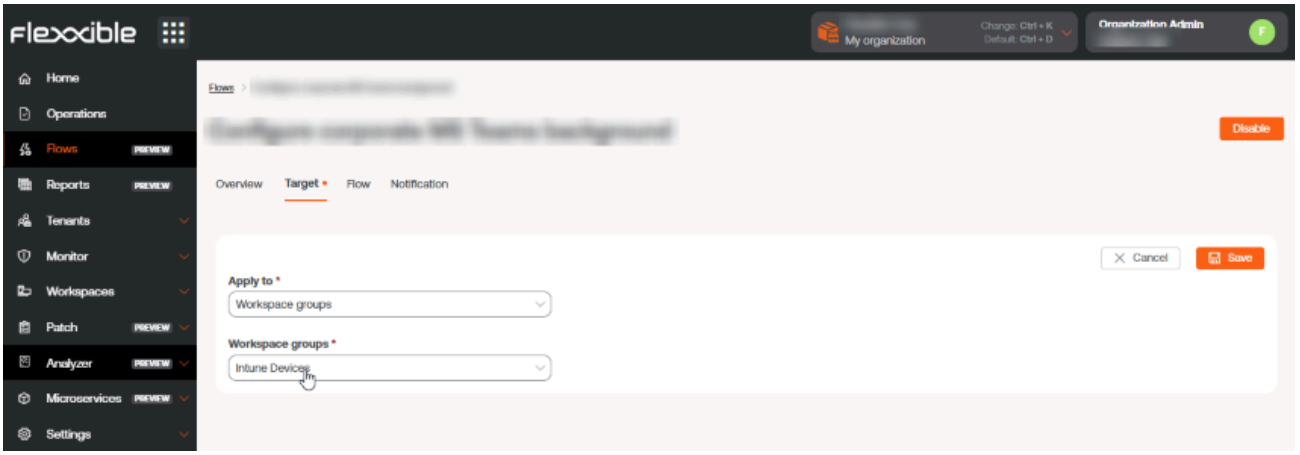
## Edit and delete a flow




Using the `Edit` button, you can change the name, description, and reuse time of the flow.

- The `Detection Only` checkbox allows you to activate or deactivate the `Detection Only` execution mode, in which the compliance with the conditions defined in the flow is evaluated, but the microservice is not executed.
- The `Delete` button allows you to delete a flow.

# Target

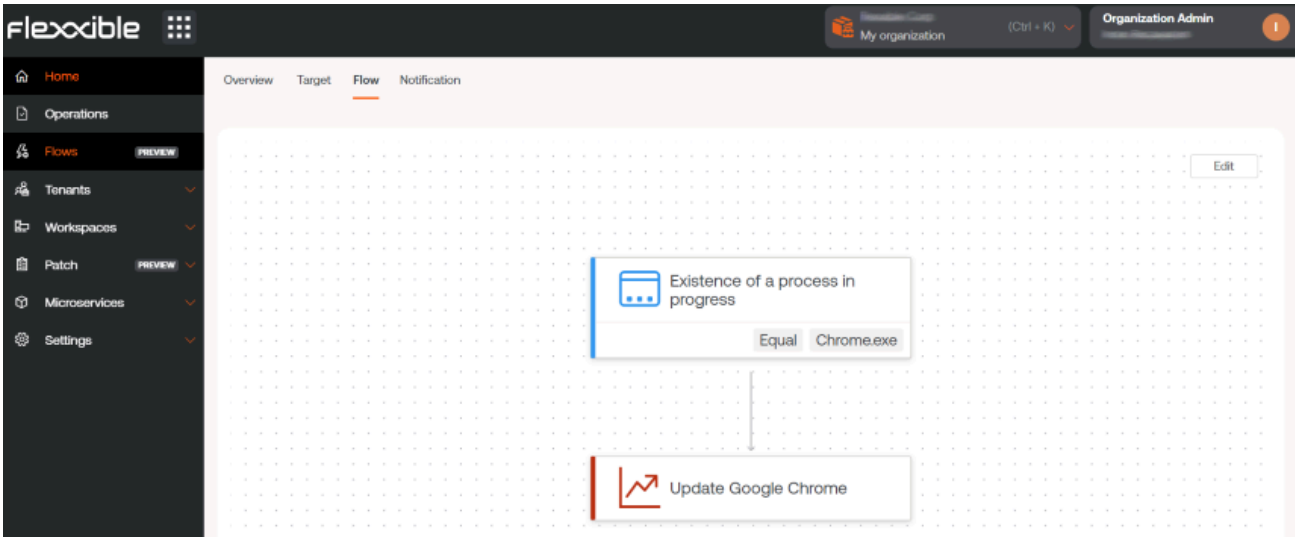



This setting allows you to define the device groups in which the flow will be executed. It supports the following configuration options:

- All devices
- A custom selection of devices
- One or more device groups
- One or several reporting groups

# Flow

From here, you can define the conditions to evaluate, the required thresholds, and the action that will be executed if those conditions are met.



# Flow conditions

These conditions allow triggering actions within the flow. All the conditions described below are compatible with the Windows operating system.

#### Existence of an ongoing process

Periodically checks if there is a process running, at configurable intervals between 15 seconds and 5 minutes.

#### Detected Windows event log record identifier

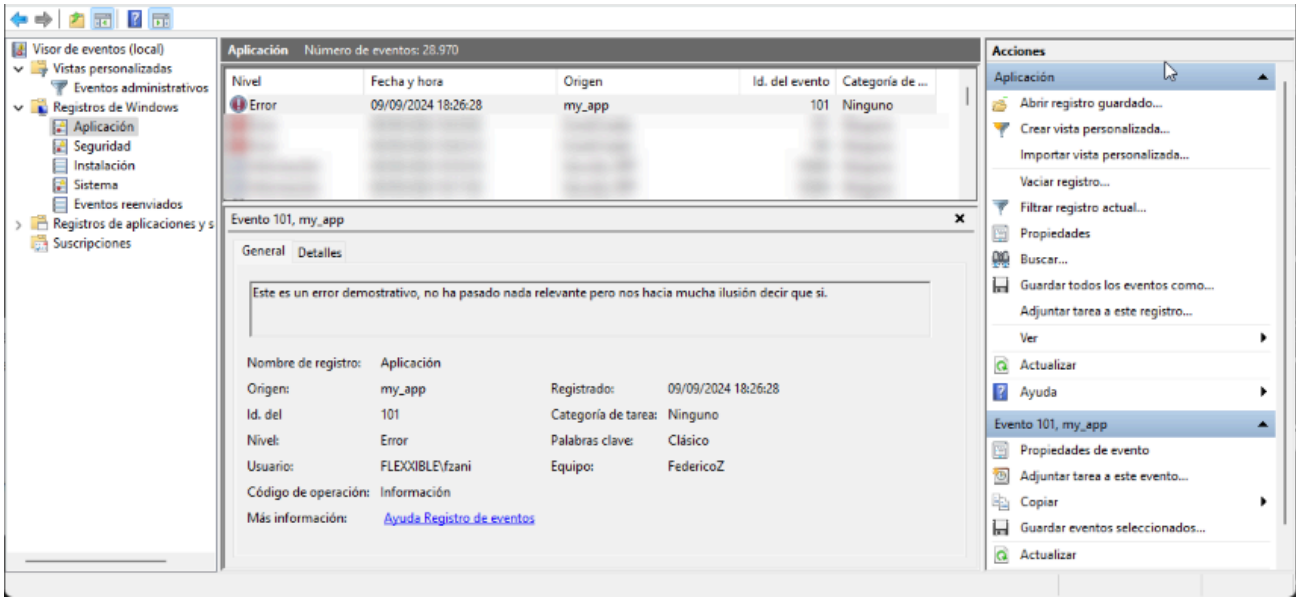
Searches for specific events in the Windows Event Viewer, at intervals of 5 to 20 minutes.

Events are identified by the format:

`<logName>:<source>:<id>`

Example: Application:my_app:101, where:

- Logname = Application
- Source = my_app
- id = 101




#### Operating system version

Gets the operating system version at intervals between 1 and 12 hours, using operators that allow comparing if the value is equal, starts with, ends with, or contains a specific string.

#### Operating system language

Detects the operating system language at intervals of 1 to 12 hours, using operators that allow comparing if the value is equal, starts with, ends with, or contains a specific string.

#### Operating system disk free space percentage

Evaluates the free disk space, allowing setting a target percentage. It is checked at intervals of 5 to 60 minutes.

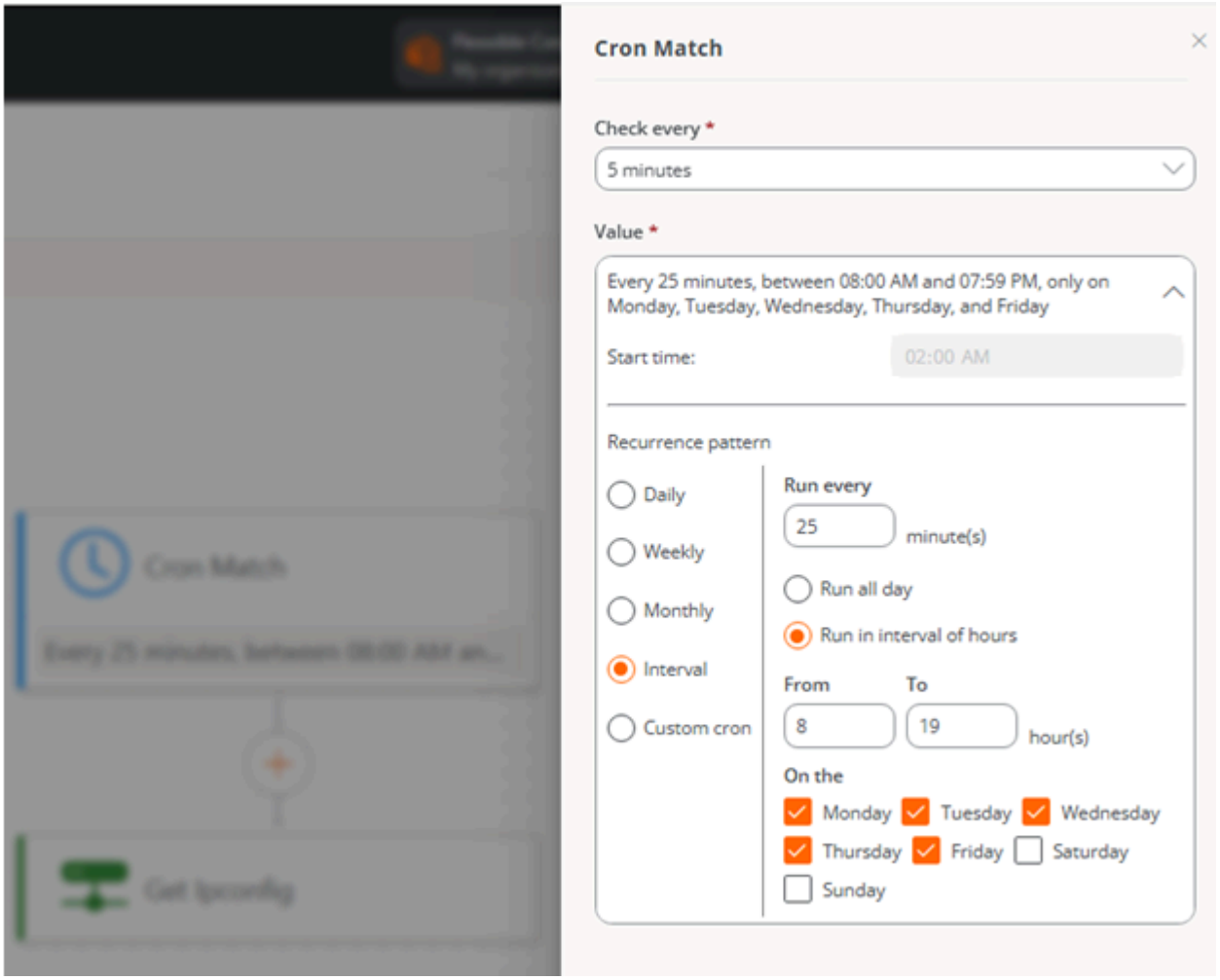
#### Cron Match

Checks if the current date and time match the schedule defined graphically in the *Value* field. If there is a match, the scheduled action will be executed.

- Check every: specifies the frequency with which the system will evaluate whether the schedule is met. This value must be adjusted according to the indicated schedule.
- Value: allows configuring the schedule, periodicity, and recurrence that will determine when the action will be executed.

The form allows defining a *Recurrence Pattern* with the following options:

- Daily: indicates at what time and every how many days the action should run, as well as if it should only be performed from Monday to Friday.
- Weekly: lets you define at what time, how many weeks apart, and on which days of the week the action will run.
- Monthly: sets the time and day of the month when the action will run.
- Interval: determines every how many minutes the action will run within a day or a specific time range.
- Custom Cron: allows you to manually enter a string in standard cron format, useful for custom and advanced configurations.



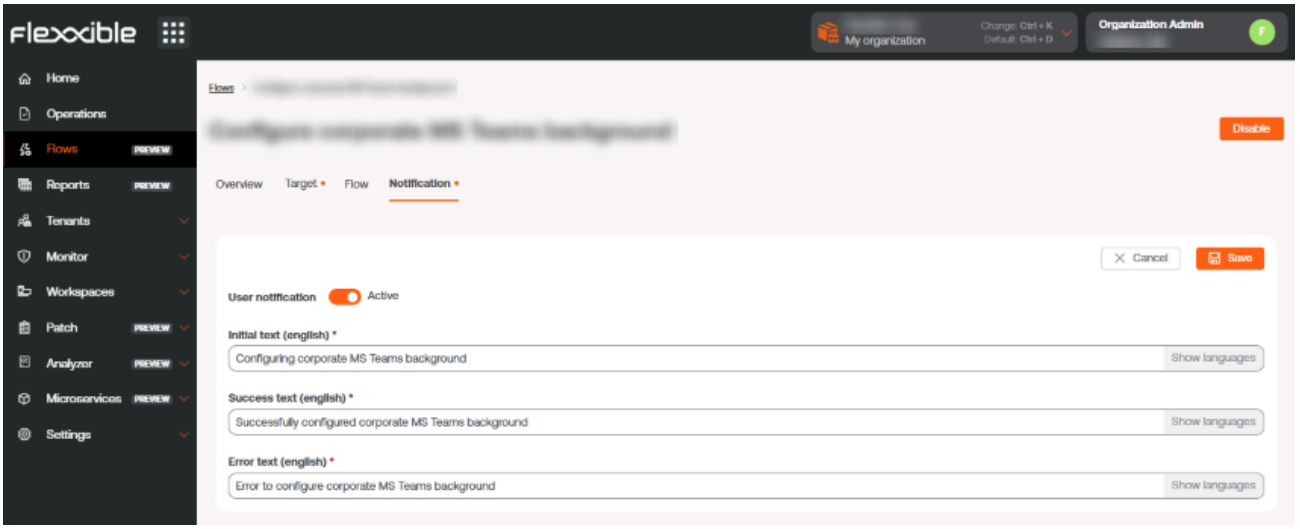

At the top of the form, a (text) summary of the configured schedule is displayed to confirm it is the desired one.

> **INFO**
>
> The hours are defined according to the time zone of the user editing the Cron Match, except in the case of a ***Custom Cron***, where the hours are specified in standard UTC (Coordinated Universal Time).

#### Actions

Once the conditions are evaluated and according to the obtained values, one or more actions can be executed. In this section, all the microservices enabled in your subscription will be displayed to select and include them in the flow.

# Notification




This parameter is optional and can be disabled. Allows notifications to be sent to users at the start and end of the flow execution, using the operating system notifications. Once enabled, you can set:

- Initial message: will be sent to users when the execution begins.
- Success message: will be sent to users on successful execution.
- Error message: will be sent to users on execution with errors.

**INFO**

A configuration change in an existing flow can take up to 15 minutes to apply to all linked devices.

**TIP**

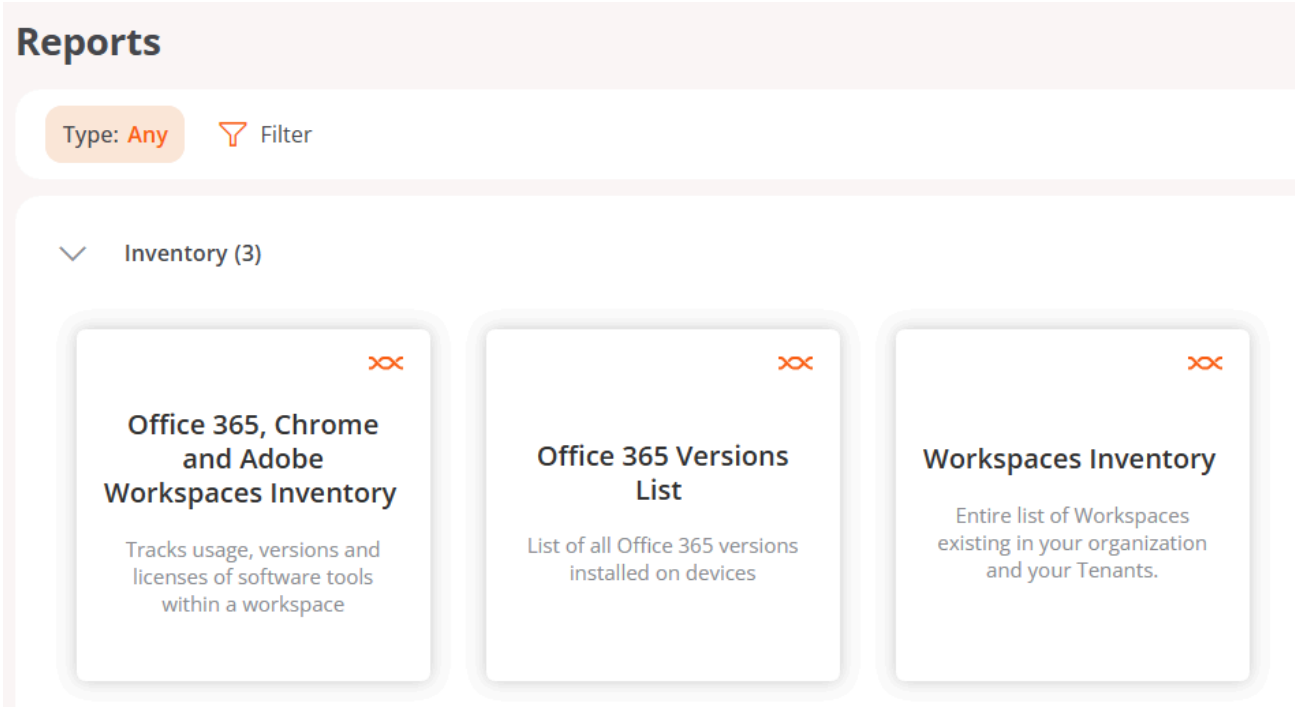
For more information on how to create a flow, please check this guide.

# Portal / Reporting

The report system provided by Portal allows users whose role is Organization Administrator to generate predefined reports with relevant data from their organization's device fleet to review them on screen or send them by email to other users.

## Considerations about the reports

- Reports are automatically generated once a week.
- Historical reports will remain available in Portal for two months.
- The automatic sharing of reports can be configured so that when the necessary email addresses are provided, the report is sent weekly.




## Report inventory

Portal offers three types of predefined reports:

- Office 365, Chrome and Adobe Workspaces Inventory
- Office 365 Versions List

- Workspaces Inventory

## Office 365, Chrome and Adobe Workspaces Inventory

This report shows the usage tracking, versions, and licenses of Office 365, Chrome, and Adobe on the devices. The report table offers the following information:

- **Host number**: device name
- **Serial number**: device serial number
- **CPU cores**: number of central processing unit cores
- **RAM**: total amount of RAM memory (in megabytes)
- **Disk used (%):** percentage of system disk usage
- **Total disk capacity**: total disk capacity (in gigabytes)
- **Operating system**: type of operating system
- **Microsoft 365**: installed Office version
- **Google Chrome**: installed version of Google Chrome
- **Adobe Acrobat**: installed version of Adobe Acrobat
- **Last user**: user of the last session detected on the device
- **Created on**: report execution (creation) date
- **Last report date**: execution (creation) date of the last report

## Office 365 Versions List

This report generates a list of Office 365 versions installed on the organization's devices and for each one provides the number of devices containing it.

## Workspaces Inventory

This report shows a list of the existing devices in the organization and those of its tenants. The table offers the following information:

- **Name**: device name
- **Domain**: Active Directory or EntraID domain to which the device belongs

- **Last user**: user of the last session detected on the device
- **Device type**: *Physical* or *Virtual desktop*
- **Operating system**: name of the operating system
- **Motherboard manufacturer**: name of the motherboard manufacturing company
- **Motherboard model**: name of the motherboard model
- **BIOS manufacturer**: company that manufactures the basic input/output system (BIOS)
- **Processor**: processor name
- **CPU cores**: number of central processing unit cores
- **Compliance**: policy applied to the device
- **Hypervisor**: type of hypervisor detected on the device
- **Broker**: type of broker detected on the device
- **Antivirus**: name of antivirus detected on the device
- **Antivirus status**: status of the antivirus on the device
- **BIOS mode**: BIOS mode
- **Organization**: organization the device belongs to
- **Client version**: version of FlexxAgent installed
- **Country**: country where the device is located
- **Created on**: date of device creation in Portal
- **CrowdStrike active detections**: active detections of CrowdStrike
- **CrowdStrike status**: *Installed and running*, *Not installed* or *Unknown*
- **CrowdStrike version**: version number of CrowdStrike installed on the device
- **Subnet**: subnet where the device resides
- **Default gateway**: default gateway
- **Desktop type**: for VDIs, defines the type
- **EDR**: type of Endpoint Detection and Response (EDR) detected on the device
- **Farm/Cluster**: for VDIs, shows the farm it belongs to
- **Delivery group**: for VDIs, shows the delivery group it belongs to
- **Fast Startup**: shows if the device has Fast Startup enabled
- **FLXMID**: device identifier
- **IP address**: IP address number detected on the device

- **Intel AMT compatible**: indicates if the device is compatible with Intel AMT
- **Is portable**: indicates if the device is portable
- **Total RAM (GB)**: total amount of RAM (in gigabytes)
- **Number of days since last Windows update**: indicates the number of days since the last Windows update
- **Number of pending updates**: indicates the number of pending updates
- **OS Build**: operating system build number
- **Operating system manufacturer**: name of the operating system manufacturer
- **Operating system version**: operating system version number
- **OU**: organizational unit of the domain where the computer account resides
- **Platform type**: Windows, Linux, Mac, etc.
- **Windows type**: *Workstation* or *Server*
- **Encryption**: indicates if BitLocker disk encryption is active
- **Pending restart**: indicates if the device has a pending restart due to updates
- **IoT Hub configuration sync**: *Synchronized* or *Not synchronized*
- **Custom field 01**: shows the content of the first custom field
- **Custom field 02**: shows the content of the second custom field
- **Last reboot**: date of the device's last reboot
- **Last Windows update**: date the last Windows update was applied
- **Report group**: report group to which the device belongs

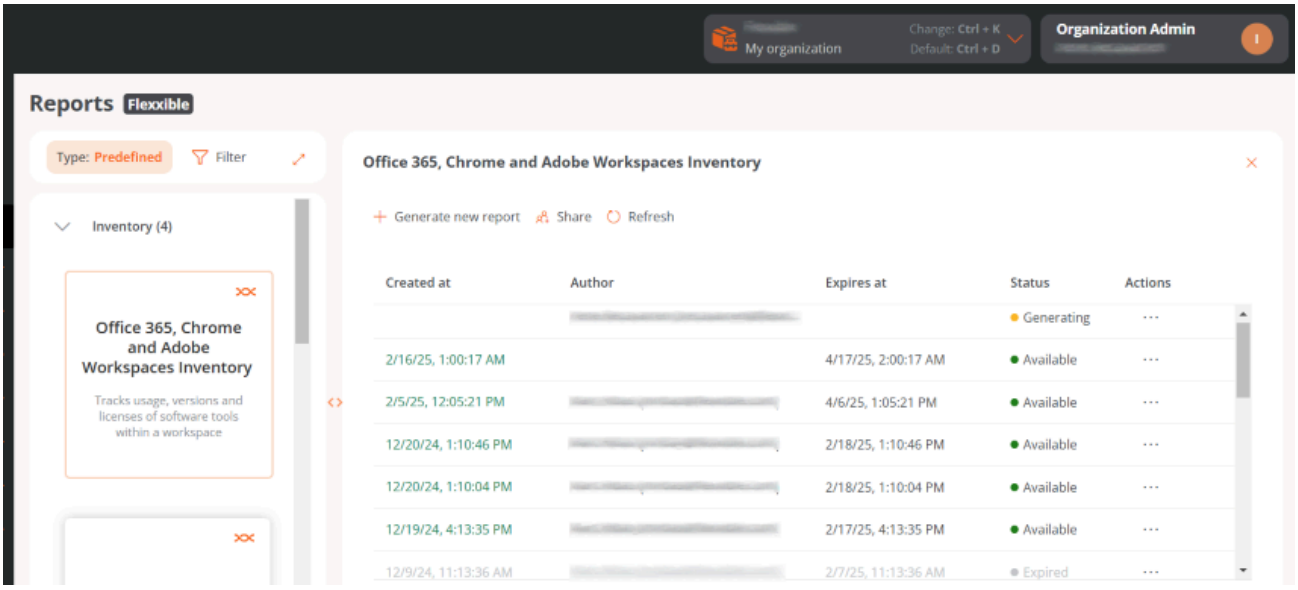
# Generate a report

Reports are automatically generated once a week, but if the user needs a current one, they should select the desired report from the inventory and click the `Generate new report` option.

Next, in organizations with dependent tenants, a modal window will open asking you to select the tenant for which the report is needed. Once chosen, click `Generate`.

The table with the list of reports will show the details of the newly generated report with the following information:

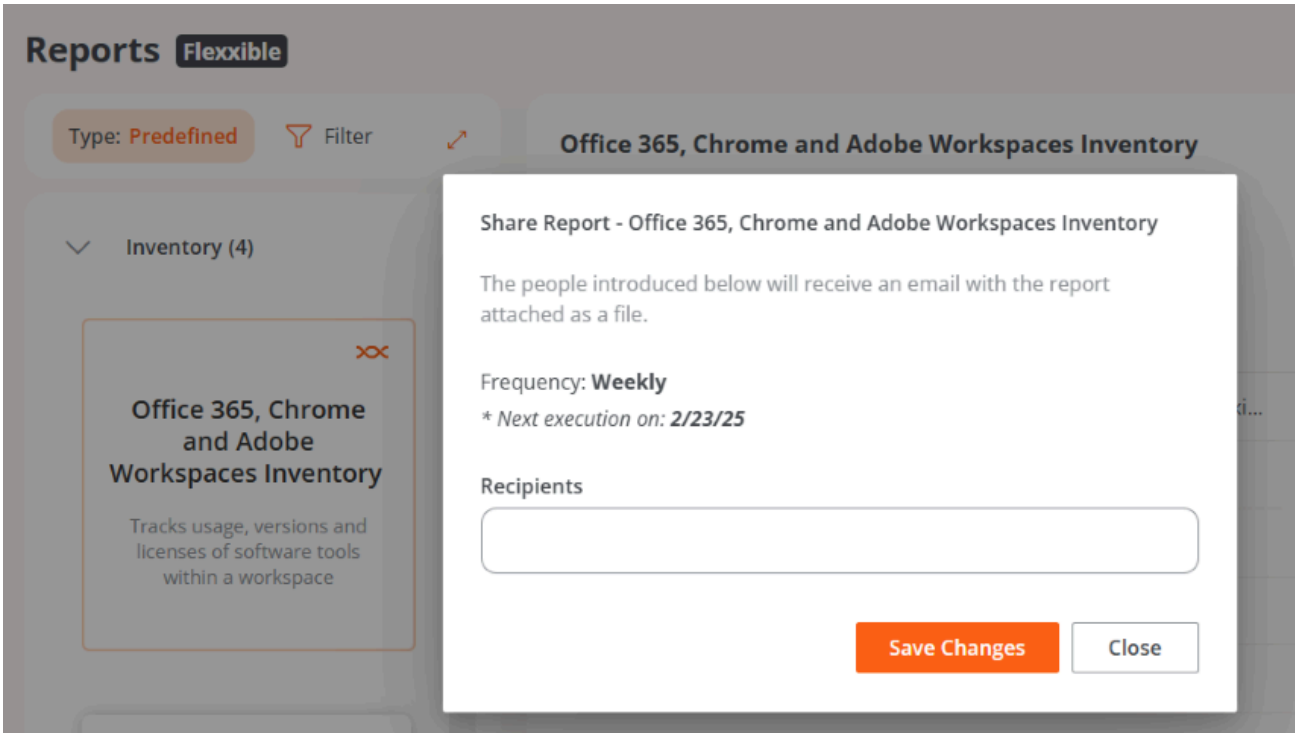
- **Created on**: Date and time when the report was generated. By clicking this option, the user can access a table with the report content.
- **Author**: User who generated the report.
- **Expires on**: Date and time when the report expires.
- **Status**: Report status (*Available*, *Generating*, or *Expired*).
- **Actions**: Access to an actions menu for the reports.
  - View details: Displays a table with the report content.
  - Download Excel: Downloads the report in Excel format.
  - Download CSV: Downloads the report in CSV format.
  - Delete report: Deletes the report.




Generated reports are saved and can be downloaded up to sixty days after creation.

# Report delivery

To share a report, select the desired one and, at the top of the table, click the `Share` option. The selected report can be sent to one or more users via email with a weekly frequency.



# Portal / Tenants

Through `Tenants`, organizations operating in the Managed Service Provider (MSP) model have the ability to establish subsidiary entities that they can support whenever they require it.

These entities are other organizations, which in Portal adopt the name of `Tenants`.
Tenants are assigned a profile type that describes them as an organization. Therefore, all tenants belong to a type of organization.

## Types of organizations

Portal distinguishes three types of organizations, establishing relationships between them:

- Partner-type organizations
- Client-type organizations
- Suborganizations

### Partner-type organizations

- They have the authority to grant administrative access to client-type organizations (tenants) that depend on them.

### Client-type organizations

- They have the option, if they wish, to segment their organization into multiple suborganizations to facilitate delegated administration.
- They can always see their entire set of workspaces, regardless of who has been delegated the management.
- They have the option to apply a `Policy` for the creation of their suborganizations from a template, which will help them configure multiple users, reporting groups, and accesses.

- They can link their instance of Analyzer to their suborganizations or assign them a new one.
- They have their own configurations.
- Several client-type organizations can have the same partner as a service provider.

## Suborganizations

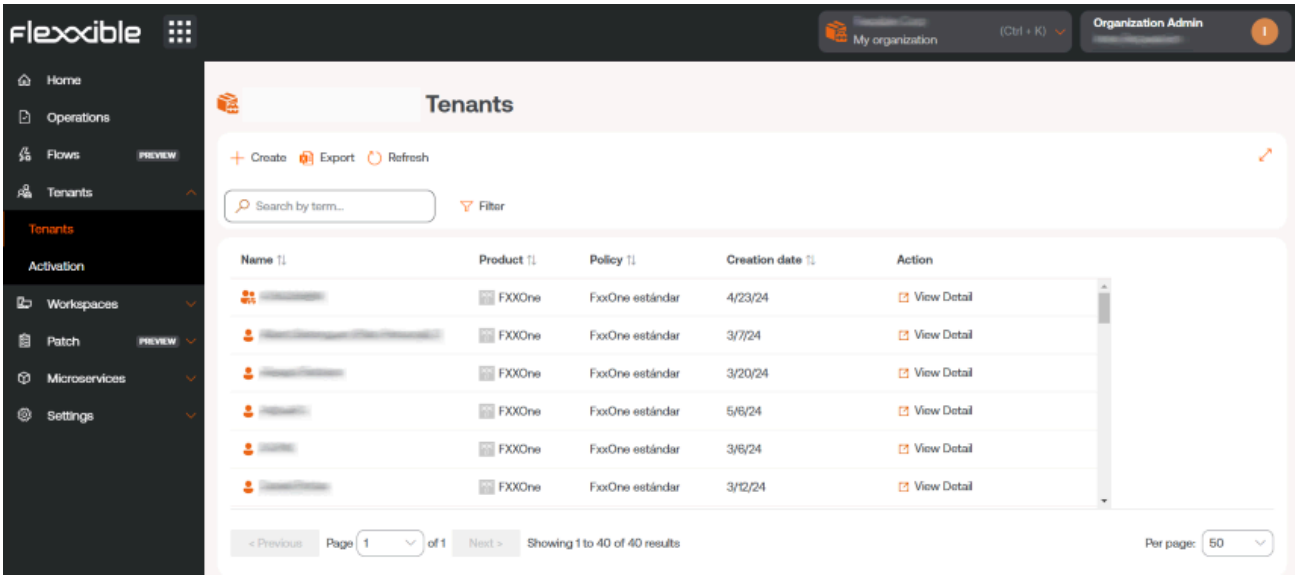
- These are subdivisions of a complex organization, management units established according to the implementation requirements.
- They are very helpful in very large environments, with wide user distribution and multiple service providers or highly segmented technical teams.
- They do not have a subscription by themselves; they use the subscription of the client-type organization that manages them.
- Each suborganization can only see its information in Workspaces. They cannot access the information of other suborganizations or of the client-type organization that manages them.
- They inherit the configuration of the client-type organization that manages them, although it can be edited. They also inherit the FlexxAgent configuration, but this is not editable.

> **INFO**
>
> Client-type organizations can create suborganizations at a lower level. Suborganizations cannot be created from another suborganization.

# List of tenants

The list view shows a table with the list of organizations (tenants) whose administration is delegated. It includes information about the Flexxible product they have, their policy, and creation date.

The `View Details` button opens a form that allows you to change the name of the tenant and delete it.




The `New` button allows you to create a new tenant; for this, you must enter, in addition to the previous data, an email address, language, country, sector, product, and region. It also gives the option to assign a Policy. The `Export` button allows an excel file to be downloaded with the list of current tenants. And `Reload` gives the option to update the table after entering new data.

## Tenant interface

If the user clicks on the name of a tenant in the table, the Portal interface will automatically switch to the `Home` page of the selected tenant's Portal. This action is very useful because it speeds up the consultation of data from one organization or another.

Portal will not revert to the default organization, even if the page is refreshed. To go back, there are three options:

- Do `Ctrl + D` (`Cmd + D` on Mac).
- Do `Ctrl + K + O` (`Cmd + K + O` on Mac).
- Directly select the default organization (`My organization`) from the `Organization Selector`, located at the top of the interface.

In the `Organization Selector`, you can differentiate tenants from suborganizations. These are prefixed by the name of the client-type organization that manages them. For example: *Client A > Suborganization-01*.

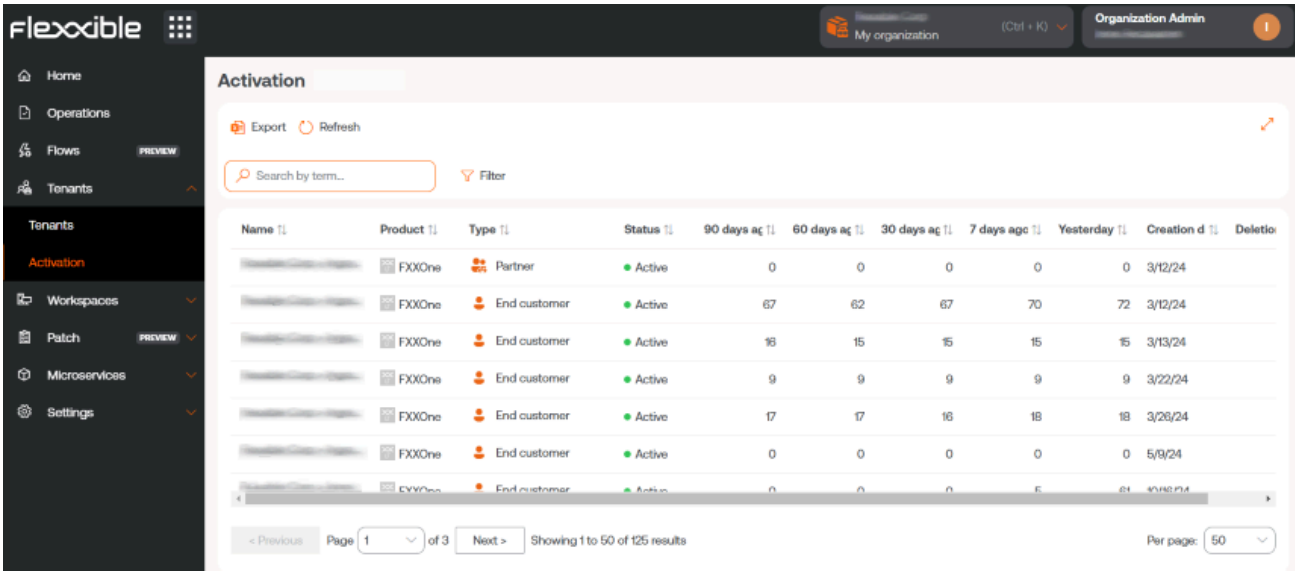
# Portal / Tenants / Activation

`Activation` allows Managed Service Providers (MSPs) to evaluate the evolution of FlexxAgent installations or deployments in client organizations where they have delegated administration.

The list view table shows the names of the tenants. If it is a sub-organization, its name will be preceded by the name of the organization that manages it; for example: *Client A > Sub-organization-01*. This nomenclature is adopted because sub-organizations inherit the FlexxAgent configuration from the client organization that manages them.

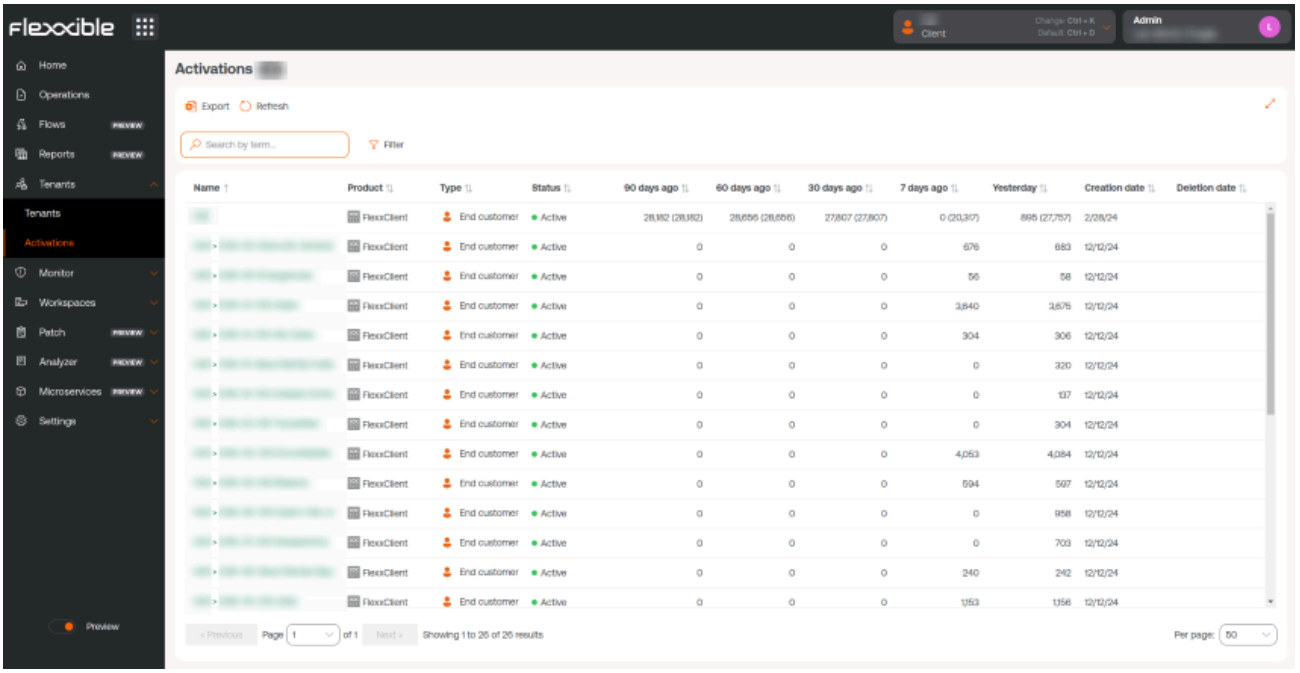
The table also indicates the Flexxible product owned by the tenant, the type of organization it corresponds to, and time indicators that help to understand the evolution of FlexxAgent adoption in the organization.

The time indicators offered by the table are *90 days ago*, *60 days ago*, *30 days ago*, *7 days ago* and *Yesterday*. Each field specifies the number (units) of active agents at that particular moment.




`Activation` also offers the option to search for tenants and the alternative to apply filters to the list of results according to different parameters, such as company name, the product they have, and the type of organization. From `Export` you can download the list view in excel format.

In cases where the organization is composed of suborganizations, in the activations view it will be possible to check the activations by suborganization in a simplified way. The first line of the list will show the number of agents in the `Parent` organization followed by the total number of agents in all suborganizations in parentheses. The information for each suborganization will be represented in the following format `Parent organization>Suborganization` on the following lines:




## Tenant interface

If the user clicks on the name of a tenant in the table, the Portal interface will automatically switch to the `Home` page of the selected tenant's Portal. This action is very useful because it speeds up the consultation of data from one organization or another.

Portal will not revert to the default organization, even if the page is refreshed. There are two options to return:

- Do `Ctrl + K + O`.
- Directly select the default organization (`My organization`) from the `Organization Selector`, located at the top of the interface.

# Portal / Workspaces in Portal

Workspaces allows users to have an overview of the status of each of the organization's devices. Everything that happens with the devices in the `Workspaces` module can be accessed from this section.

The general view of `Workspaces` in Portal shows a table listing the organization's devices, along with the following information:

- **Name**: device name
- **FQDN**: domain name associated with the device
- **IP Address**: IP address of the device
- **Operating System**: the device's operating system
- **CPU Cores**: number of CPU cores the device has
- **RAM**: amount of RAM the device has, in megabytes (MB)
- **Type**: type of device (*Physical* or *Virtual*)
- **Last User**: name of the last user who used the device

## Device detail view

To access specific data about a device, click on its name. Next, at the top of the view, you will see the current status: *Online* (green background) or *Offline* (gray background).

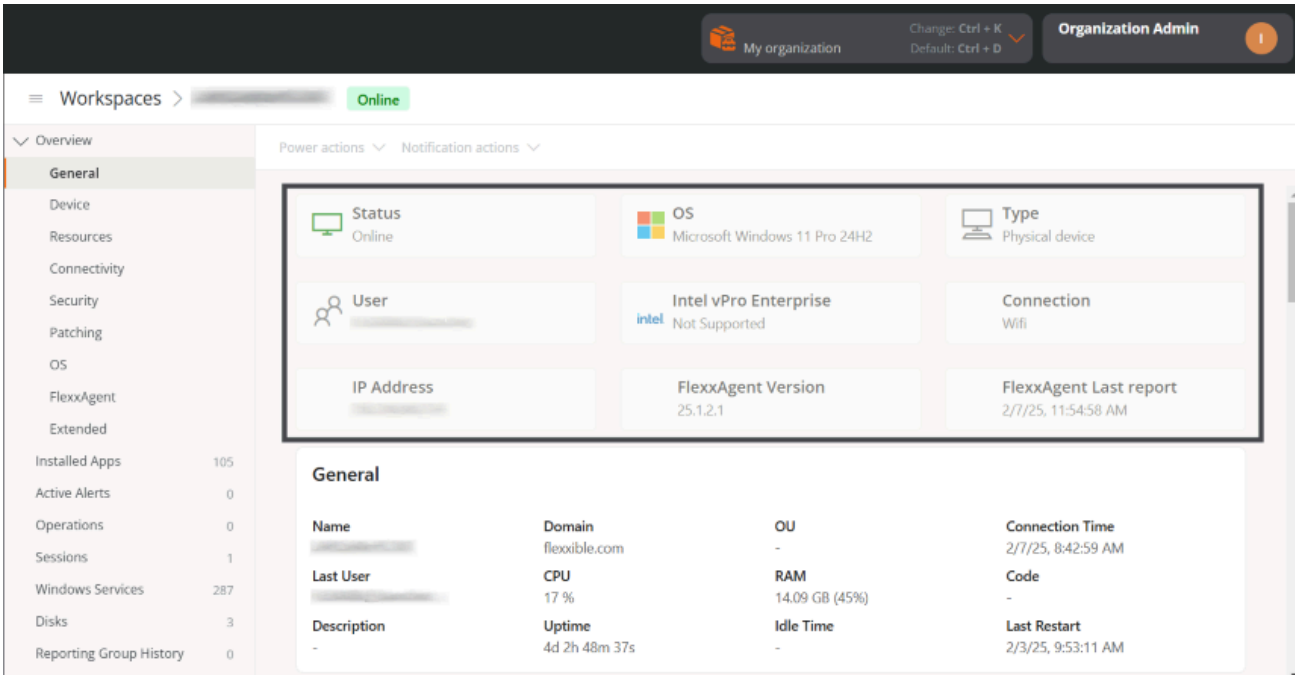

The detail view is divided into the following tabs:

- Overview
- Installed applications
- Current active alerts
- Operations
- Sessions

- Windows Services
- Disks
- All reporting groups
- PnP Events
- PnP Errors
- Group Policy (GPO)
- Boot history
- Installed updates
- Pending updates

## Overview

At the top of this view, a group of cards provides easy access to specific data about the selected device: *Status*, *Operating System (OS)*, *Type*, *User*, *Connection*, *IP Address*, *FlexxAgent version* and *FlexxAgent last report*.

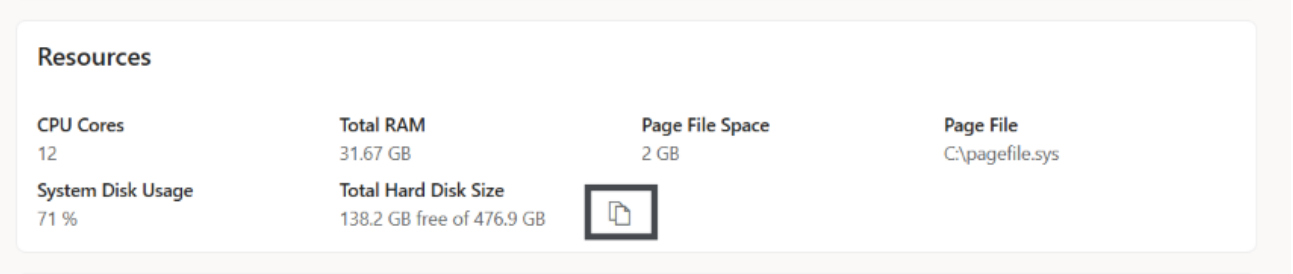



Next, ten sections offer detailed information:

1. **General**: device identification, usage, and connection
2. **Device**: hardware description of the device

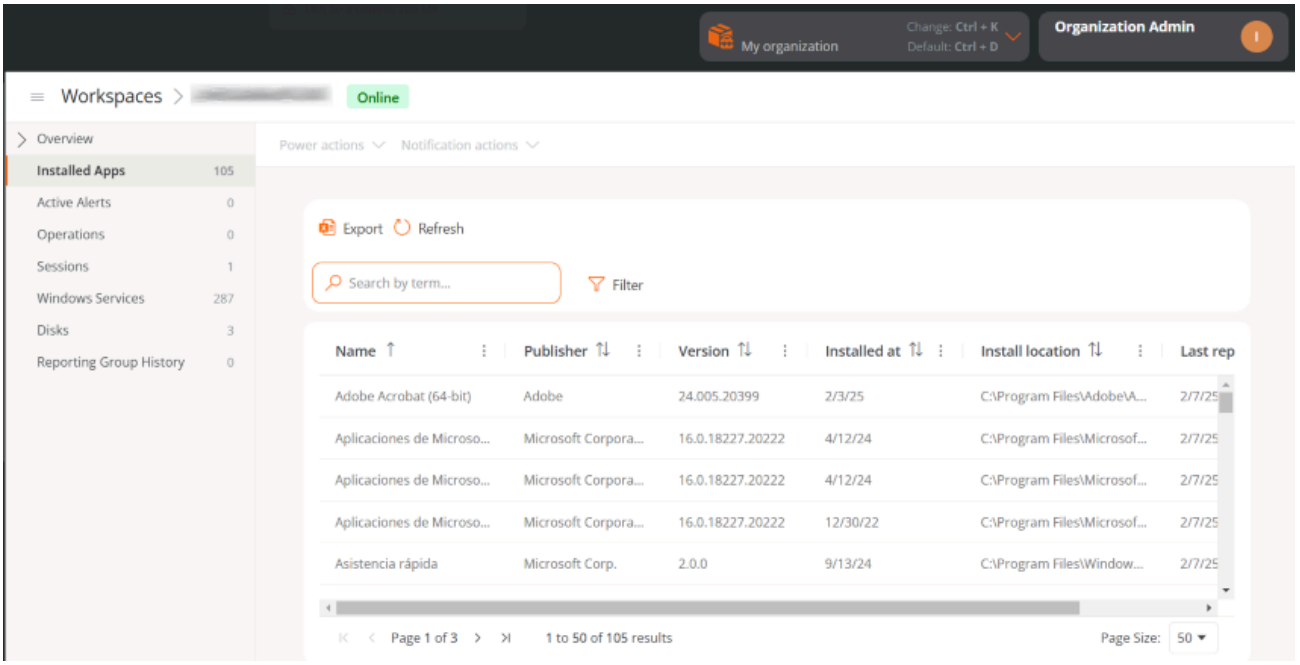
3. **Resources**: space resources in use on the device
4. **Connectivity**: type of connectivity and addresses associated with the device
5. **Security**: data about the device's security solutions
6. **Update**: update status of the operating system and the target
7. **OS**: type, version, and location of the operating system
8. **FlexxAgent**: general status of FlexxAgent on the device and information about its reporting group
9. **Expanded**: data about the motherboard and the device's Basic Input Output System (BIOS)
10. **Virtualization**: hypervisor, broker, and more data about the virtual device, if applicable

From `Overview`, the user can copy the desired information by hovering over the element.




## Installed apps

This tab shows a table with the list of applications installed that FlexxAgent has found on the device being consulted.

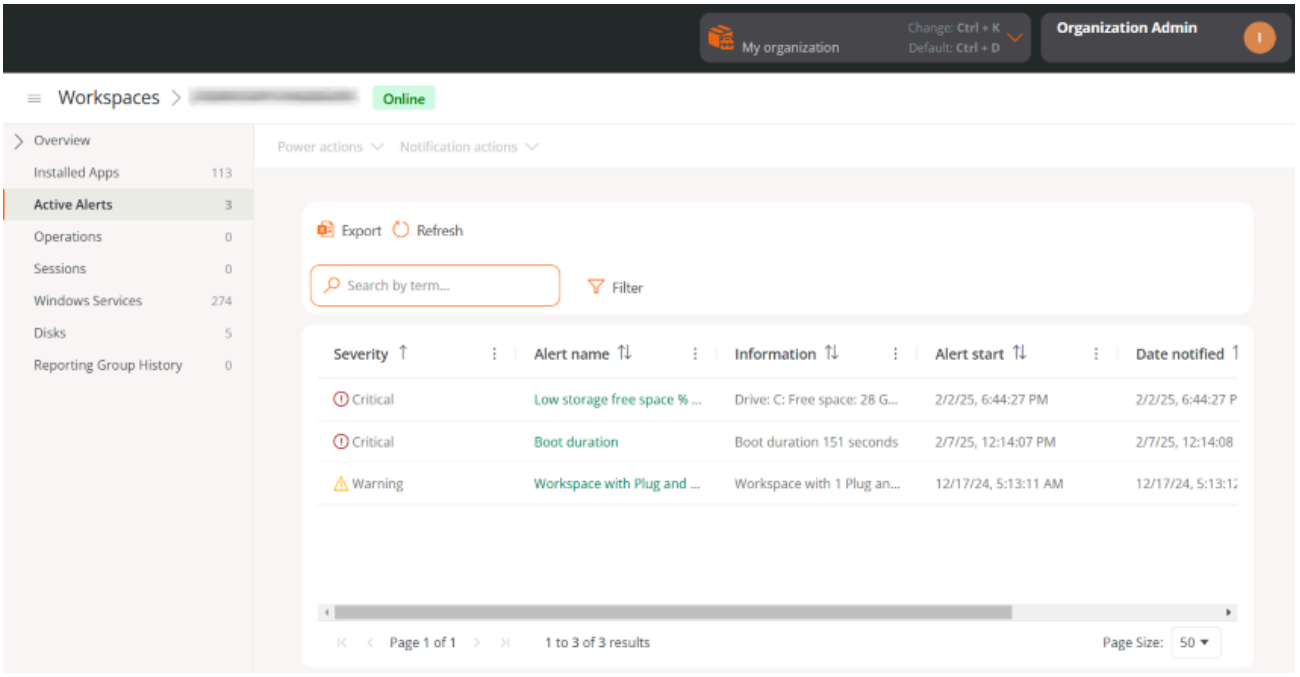



The information includes:

- **Name**: name of the application installed on the device
- **Publisher**: company that developed the application
- **Version**: version of the application
- **Installed On**: date it was first reported on the device
- **Installation location**: folder where the application is located
- **Last Report**: date it was last reported on the device

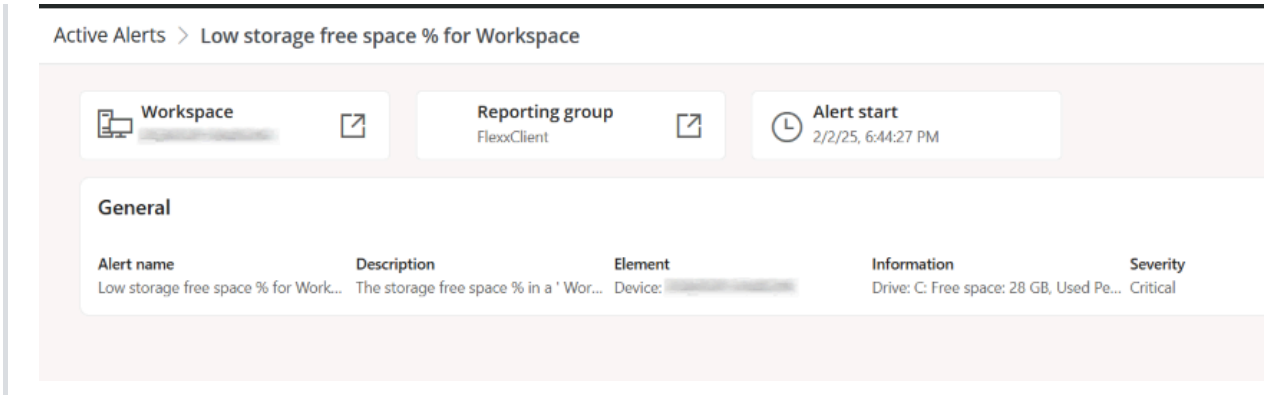
## Active alerts

This section displays a table with the list of active alerts found on the device being queried.




The information includes:

- **Severity**: severity level (*Critical*, *Warning* or *Informative*)
- **Alert name**: name that identifies the alert. You can click on it for more details.




- **Information**: description of the alert
- **Start date**: day and time when the alert is recorded
- **Notification date**: day and time of the alert notification
- **Item**: name of the device where the alert is recorded

# Operations

This section displays a table with the list of `Operations` registered on the device being queried. The information includes:

- **Operation name**: type of operation performed on the device
- **Status**: status of the operation (*Successful* or *Failed*)
- **Created on**: date and time the operation was created
- **Start date**: date and time the operation started
- **End date**: date and time the operation ended
- **Owner**: email of the user who performed the operation

## Sessions

This section displays a table with the list of sessions registered on the device being queried. The information includes:

- **User**: name of the user who has logged into the device
- **Session type**: type of session started (*Device* or *Application*, for virtualized application sessions)
- **Windows session ID**: Windows session identifier
- **Connection status**: session connection status (*Disconnected* or *Active*)
- **Start date**: session start date and time
- **CPU usage**: percentage of processor usage by the session, excluding resources used by other sessions or system processes
- **RAM usage**: amount of temporary memory used by the activities and applications of a specific user during a session
- **RTT usage**: time it takes for a data packet to travel from the user's device to a remote server or destination and back to the user

## Windows services

This section displays a table with the list of Windows services registered on the device being queried. The information includes:

- **Display name**: name of the programs running in the background

- **Status**: status of the Windows services (*Running* or *Stopped*)
- **Startup type**: how the service has been activated (*Automatic*, *Manual* or *Disabled*)
- **Log on as**: log-on mode
- **Accept stop**: whether the Windows services accept to stop or not (*Yes* or *No*)

## Disks

This section displays a table with the list of disk partitions registered on the device being queried. The information includes:

- **Device ID**: device name
- **Name**: name of the main disk partition
- **Encryption**: indicates whether the device is encrypted or not, or if no value is available (N/A)
- **Encryption method**: indicates the encryption method
- **Volume label**: name assigned to the disk
- **Total size**: in megabytes, total disk space
- **Used size**: in megabytes, used disk space
- **Percentage used**: in percentage, used disk space
- **OS unit**: unit possession (*Yes* or *No*)
- **Location**: disk location path
- **Partition**: indicates the number of storage divisions the disk has

## Reporting groups history

This section shows a table with a list of `Reporting Groups` to which the device currently belongs or has belonged. The information includes:

- **Source**: reporting group from which the device originates
- **Destination**: reporting group to which the device is entering
- **Assignment type**: *Manual* or *Automatic* assignment
- **Requested date**: date and time of the device's reporting group change

## Plug and Play (PnP) events

This section shows a table with a list of the PnP events that have been logged on the device that is being queried. The information includes:

- **Action**: state of the hardware component (printer, mouse, etc.) in relation to the device (`Plugged in` or `Unplugged`)
- **Date**: last PnP update recorded by FlexxAgent
- **User**: user currently using the device
- **Description**: hardware component connected to the device
- **Device ID**: identification code of the hardware component connected to the device

## Plug and Play (PnP) errors

This section shows a table with a list of the PnP errors that have been logged on the device that is being queried. The information includes:

- **Name**: name of the hardware component connected to the device
- **Update date**: last PnP update recorded by FlexxAgent
- **Class**: type of hardware component connected to the device
- **Device ID**: identification code of the hardware component connected to the device

## Group Policy (GPO)

This section shows a table with a list of GPOs that have been logged on the device that is being queried. The information includes:

- **Display name**: name assigned to the policy
- **Last application time**: date and time of the last policy application

## Boot history

Through a chart, this section shows the boot time log of the device that is being queried.


## Installed updates

This section displays a table listing the installed updates on the device that is being checked. The information includes:

- **Installation date**: date when the update was installed on the device.
- **KB**: unique identifier of the Microsoft update package
- **Product**: name of the product to which the update is applied
- **Severity**: level of urgency detected for executing the update (*Critical*, *Important*, *Moderate*, *Low*, *Unspecified*)
- **Arrival date**: release date of the update
- **Category**: category assigned to the update

## Pending updates

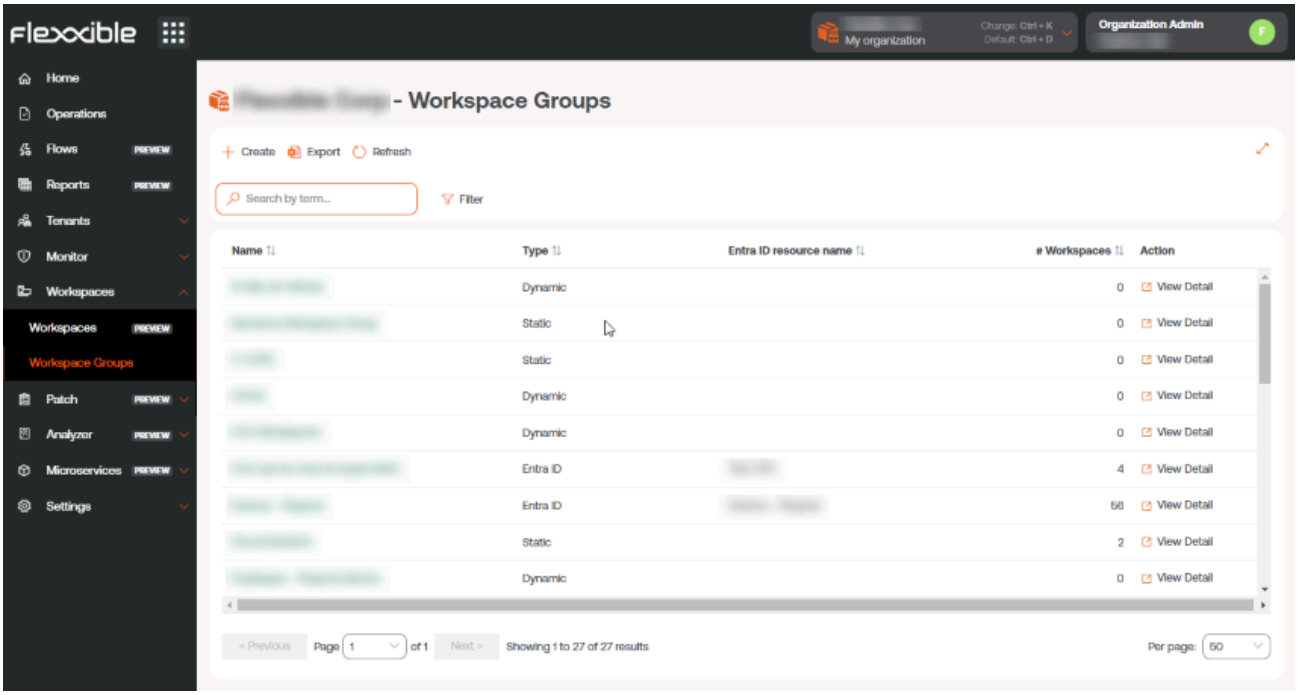
This section displays a table listing the pending updates on the device that is being checked. The information includes:

- **KB**: unique identifier of the Microsoft update package
- **Product**: name of the product to which the update is applied
- **Severity**: level of urgency detected for executing the update (*Critical*, *Important*, *Moderate*, *Low*, *Unspecified*)
- **Arrival date**: release date of the update
- **Category**: category assigned to the update

**INFO**

The Workspaces section in the Portal is informative. Actions on the devices must be performed from the Workspaces module.

# Portal / Workspaces / Workspace Groups




The `Workspaces Groups` make the device management process easier for organizations, allowing them to group devices according to shared characteristics or specific criteria to monitor statistics more thoroughly and execute effective actions.

There are three types of groups:

- Static
- Dynamic
- Entra ID

## Static Workspaces Group

It is a group created manually, with free criteria. It can be created and managed from Portal and from the `Workspaces` module, by filtering the `Workspaces` list option.

## Dynamic Workspaces Group

It is a group in which some condition is periodically evaluated; for example: "devices with more than 85% memory usage", so its members can change in real-time. It is very useful when you want to apply specific actions on them, such as microservices to solve a specific problem. They are created from the `Workspaces` module, by filtering the list of Workspaces.

> **INFO**
>
> Dynamic Workspaces Groups evaluate the compliance of a defined condition every 60 minutes, due to this, they are not recommended as a user session detection mechanism.

# Entra ID Workspace Group

It is a group that can pull members from an existing group or organizational unit in the Entra ID domain in use. The creation of this type of group requires at least one active integration with the Entra ID domain, within `Settings`->`Integrations`, in Portal.

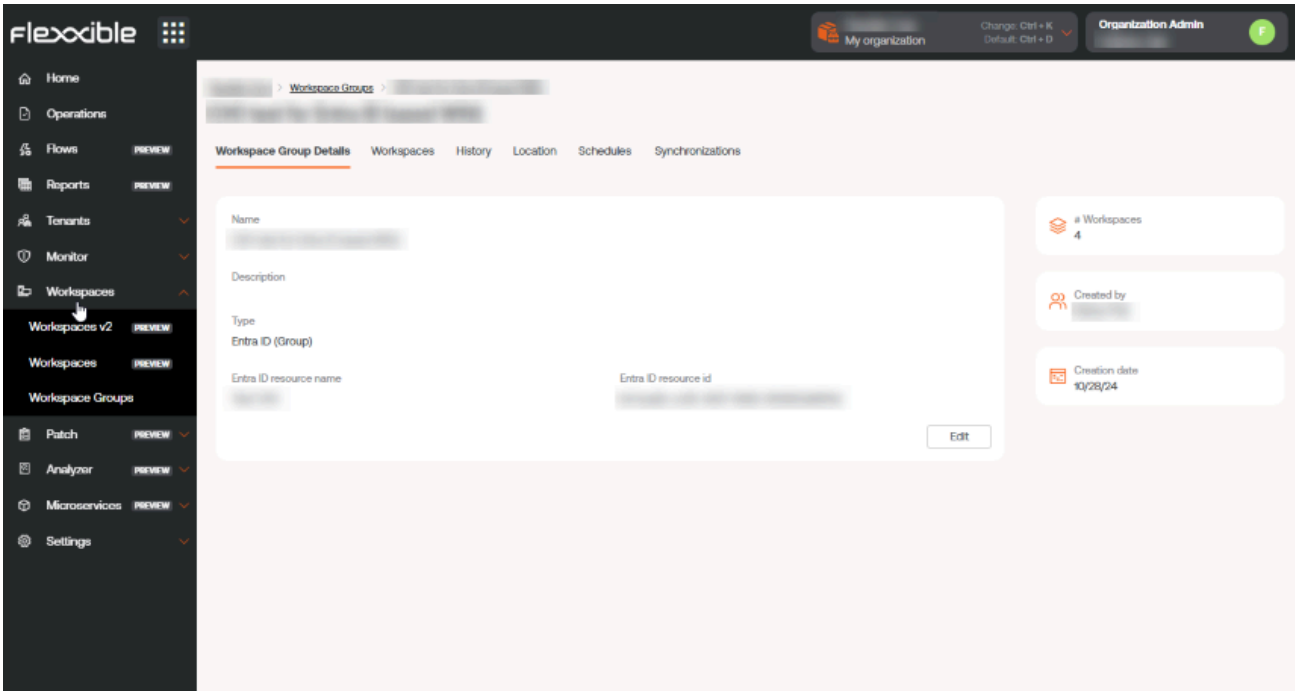
# Group management

The list view of `Workspaces Groups` contains information about the group's name, type, Entra ID characteristic, and the number of devices they contain. `View details` shows the detail view of the selected group.

In the details view of a group, at the top, there are five tabs to access more information:

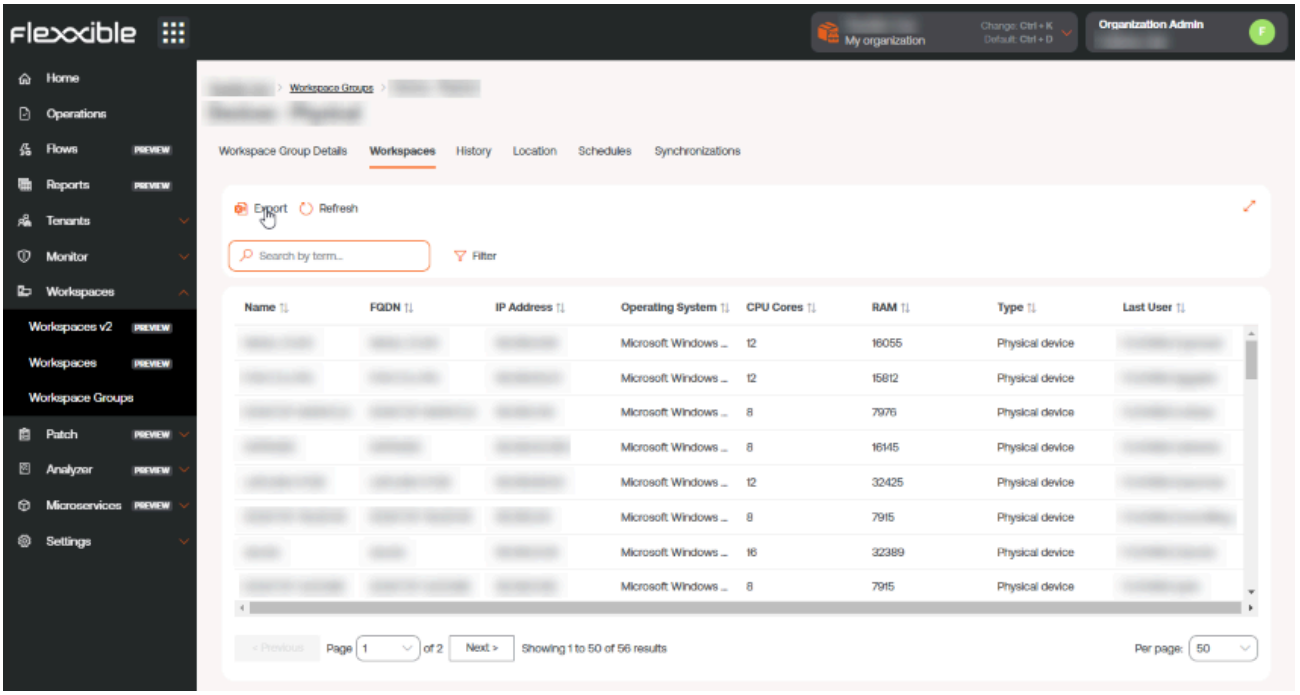
- Details
- Workspaces
- History
- Location
- Schedule
- Synchronizations

## Details



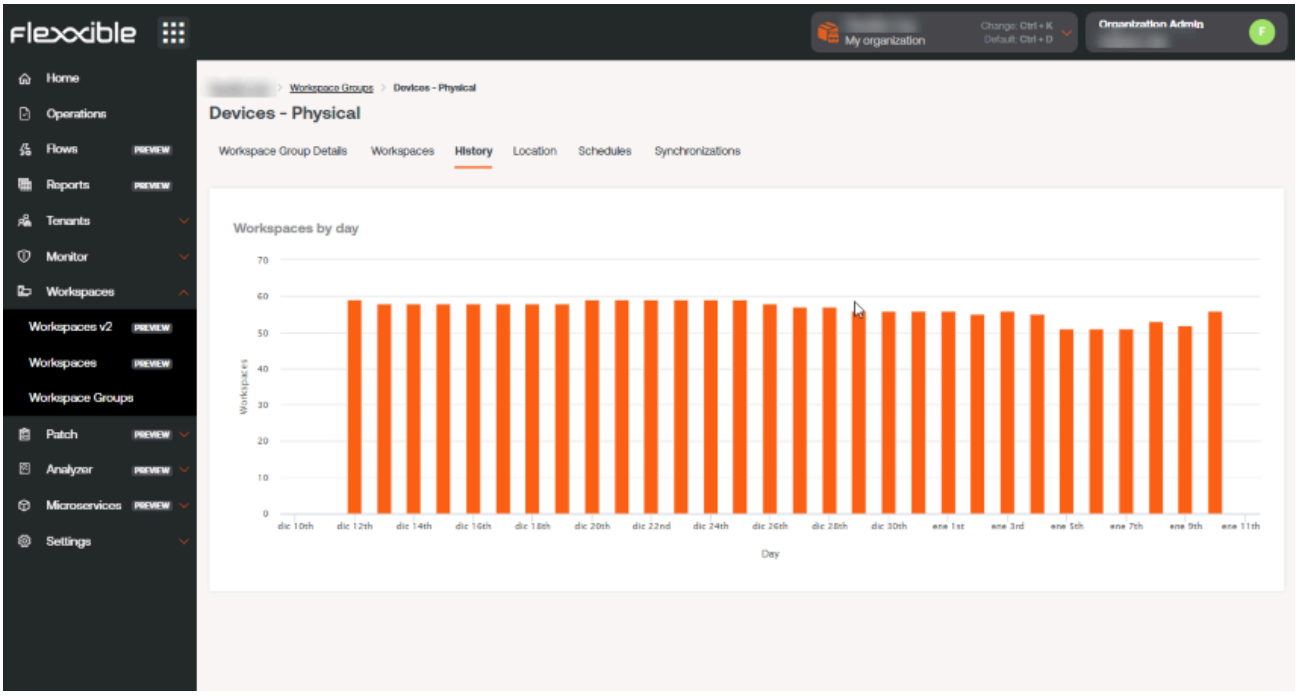

Shows the same data as the list view, as well as the group's creation date and the user who created it. The `Edit` button allows changing the workspace name, adding a description, or even deleting it.

## Workspaces



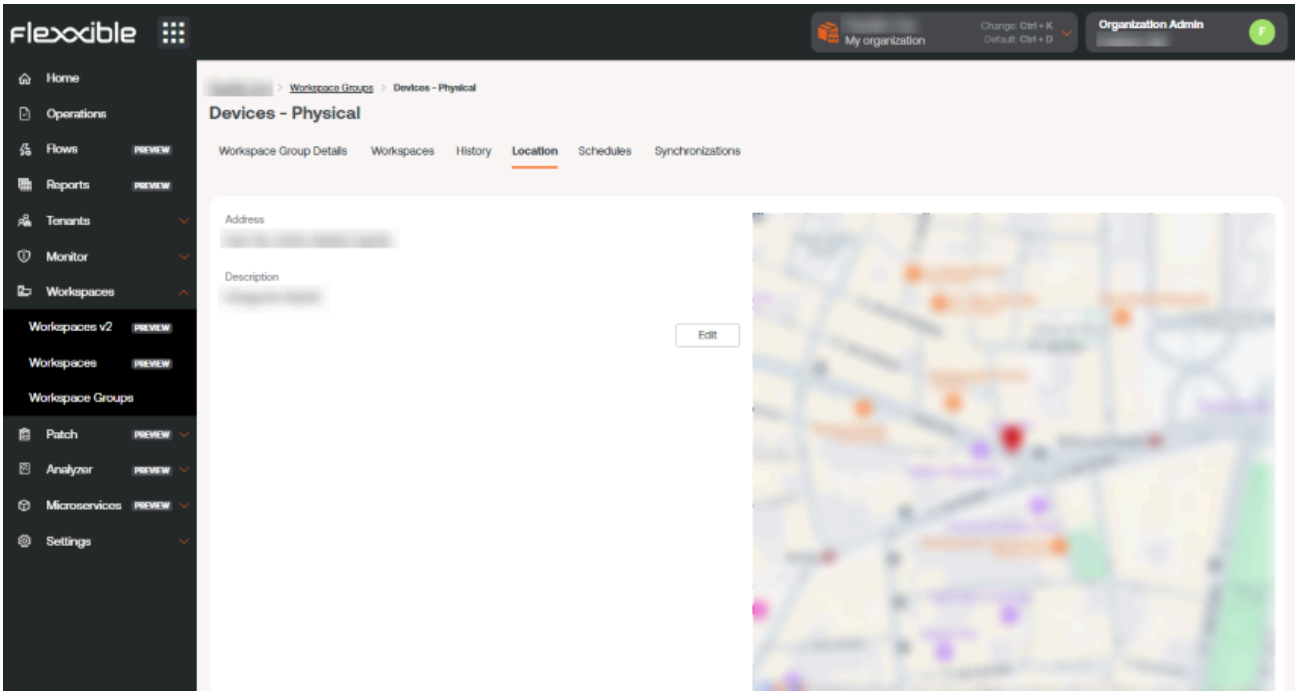
Shows a table with a list of the workspaces that make up that group. Provides information about the Fully Qualified Domain Name (FQDN) of the device, IP address, operating system, CPU cores, Random Access Memory (RAM), type (physical or virtual), and the last user. The options `Import Workspaces` and `Edit` are only available for static workspace groups.

## History



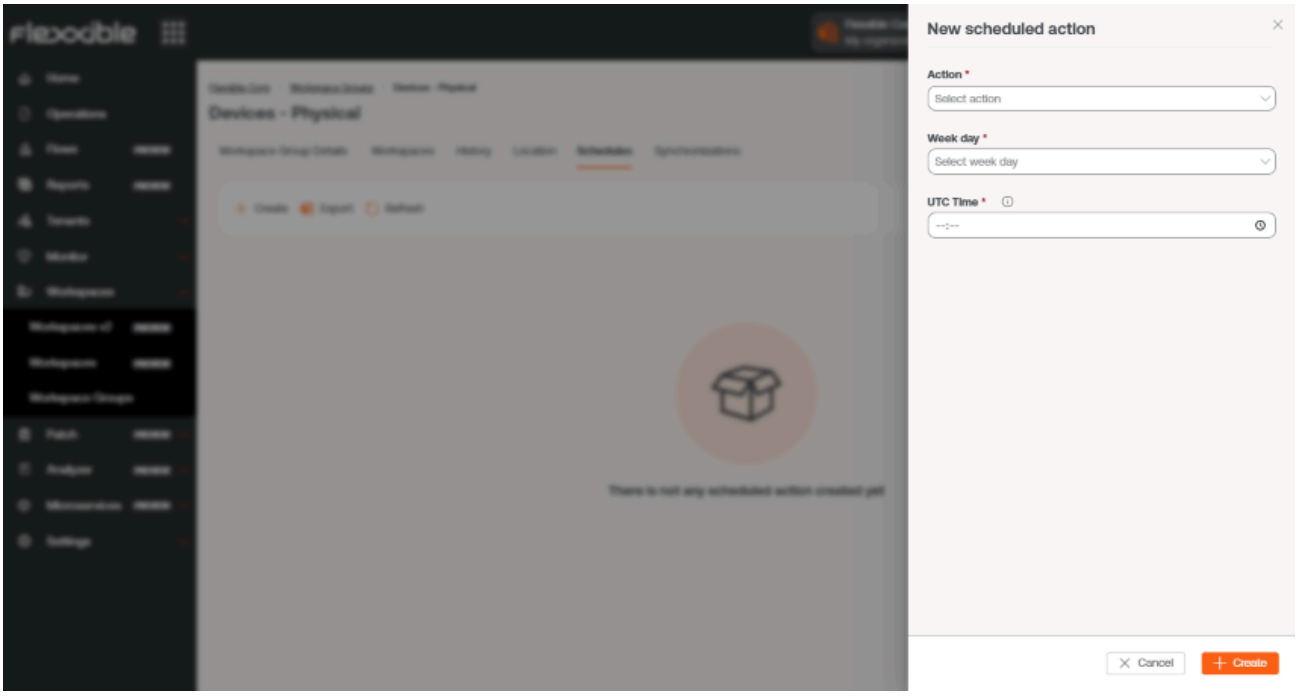

Displays a bar chart with the daily amount of workspaces that have made up the group over the last month. You can zoom in on the chart for better reading by selecting the bars you want to enlarge with the mouse. Using `Reset zoom`, the information returns to its original state.

## Location




Allows associating GPS coordinates with the workspace group to relate it to a point on the map. This value is just a reference, it does not update if users change location.

## Schedule

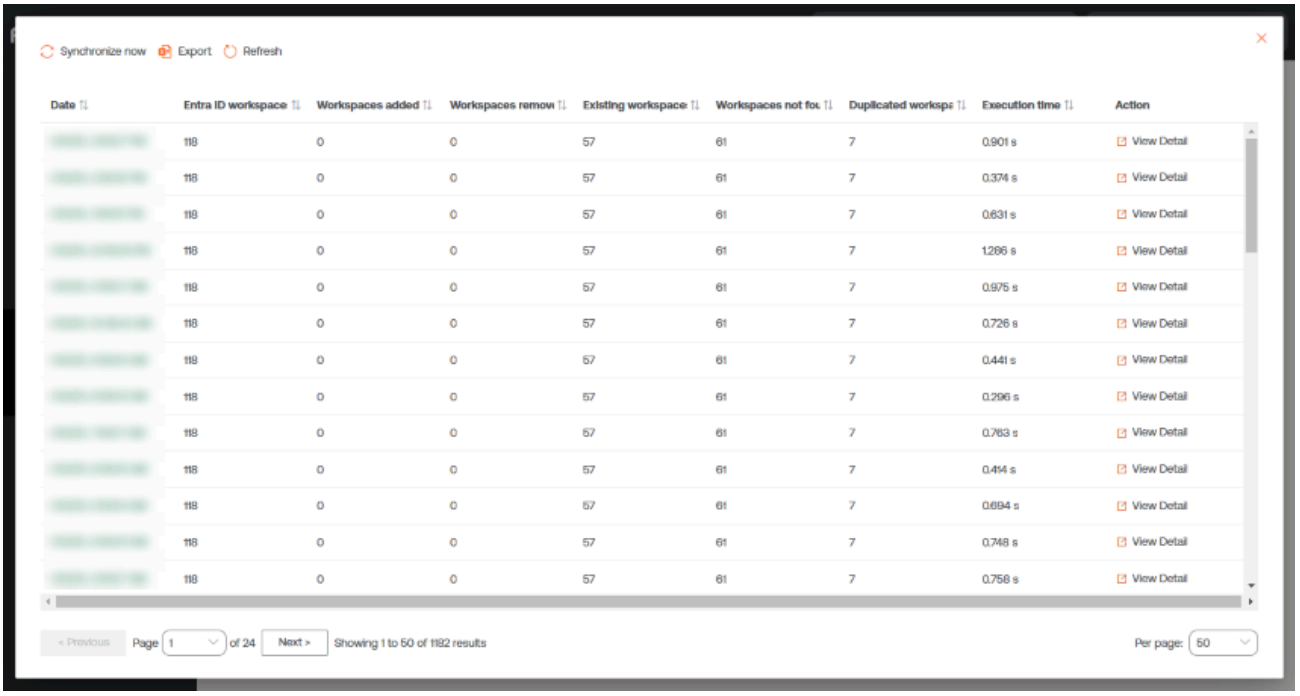



From this tab, you can schedule the power on (Wake on LAN) or the automatic shutdown of a group of workspaces. If the user wants to schedule one of these actions, they must

click on the `New` button and fill in the form fields for `Action`, `Day of the week`, and `Time UTC`.

- **Action**: allows you to choose between `Wake on LAN` or `Shutdown`.
- **Day of the week**: allows choosing which day of the week the action will be performed.
- **UTC Time**: allows you to specify the exact time to start the action, using the Coordinated Universal Time standard. The created action will then be displayed in a table, with columns showing the information entered in the form, as well as which user created the action and who updated the schedule and when. From `View details` you can edit and delete the scheduled action.

## Sync




This tab is only visible when the group type is `Entra ID`. Displays a table with details of the synchronizations performed with information about:

- `Date` and time of the sync.
- `Entra ID Workspaces`: total number of elements in the Entra ID group or organizational unit.
- `Added Workspaces`: number of workspaces added to the group.

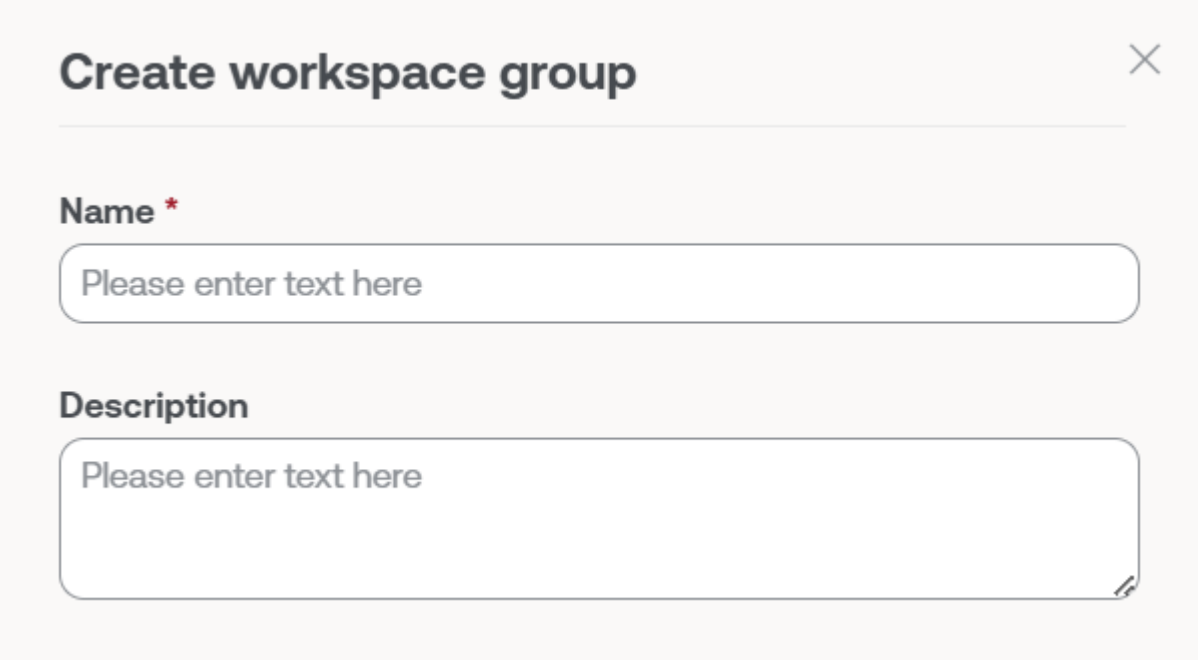
- `Deleted Workspaces`: number of workspaces deleted from the group.
- `Existing Workspaces`: number of workspaces already in the group.
- `Not Found Workspaces`: number of workspaces not found in the group; that is, workspaces that, although they are part of the Entra ID group or organizational unit, cannot be added to the group because FlexxAgent is not installed.
- `Duplicate Workspaces`: number of duplicate workspaces in the group, if any.
- `Execution Time`: the time required for synchronization.
- `Action`: allows viewing a table with synchronization information for each device in the group.

# Create groups

They can be created from Portal and from Workspaces.

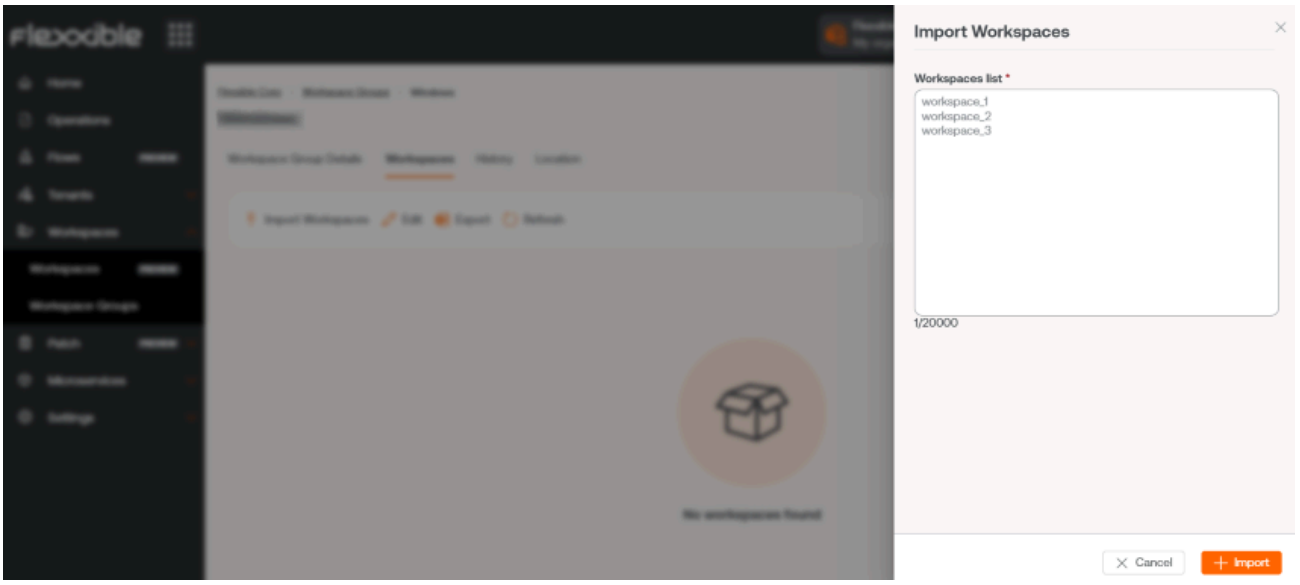
## Create a static Group of Workspaces from Portal

At the top of the list view of `Workspaces Groups`, click on `New`. A form will open where you will be asked to add a name and a description for the new group.

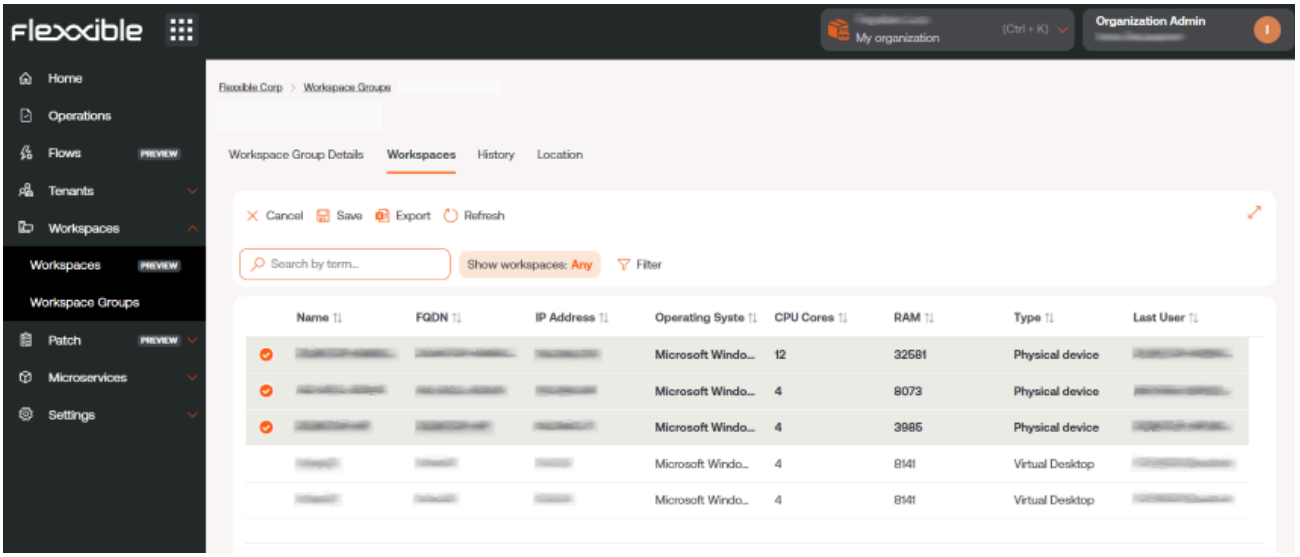



There are two ways to add devices to a static workspace group from Portal:

1. In the groups table, click on `Detail View` of the desired group -> `Workspaces` -> `Import devices`. A form opens that allows importing up to 20,000 workspaces.



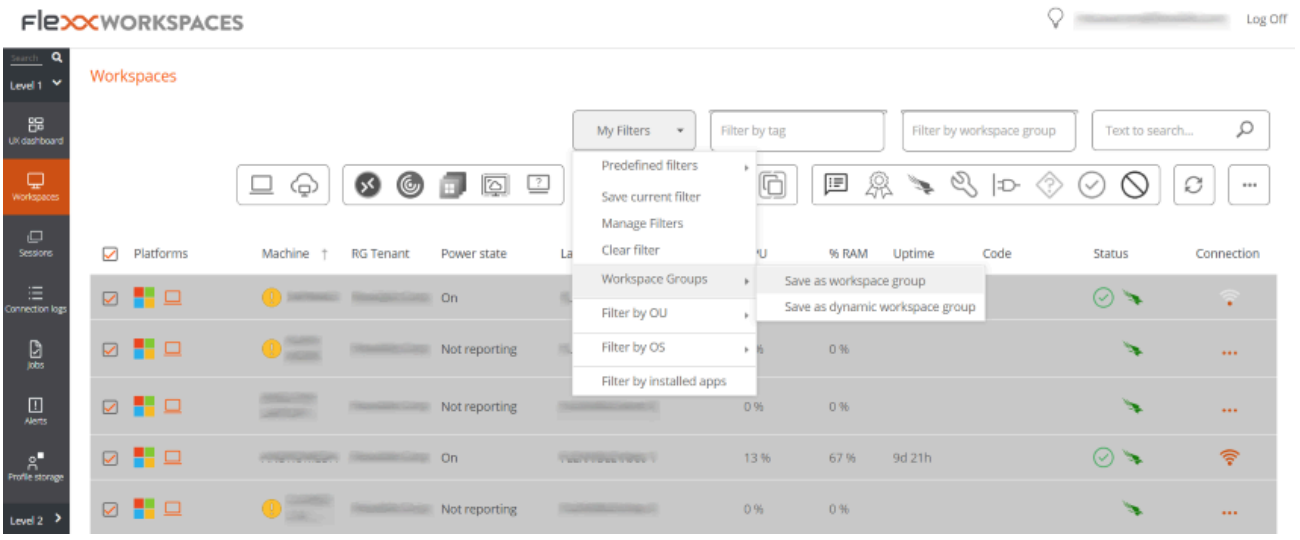

2. In the groups table, click on `Detail View` of the desired group -> `Workspaces` -> `Edit`. Next, select the devices you want to add. Those marked with an orange dot are added to the group and those not marked are removed. In both cases, click on `Save` to keep the changes.




## Creating a Static Workspaces Group from Workspaces

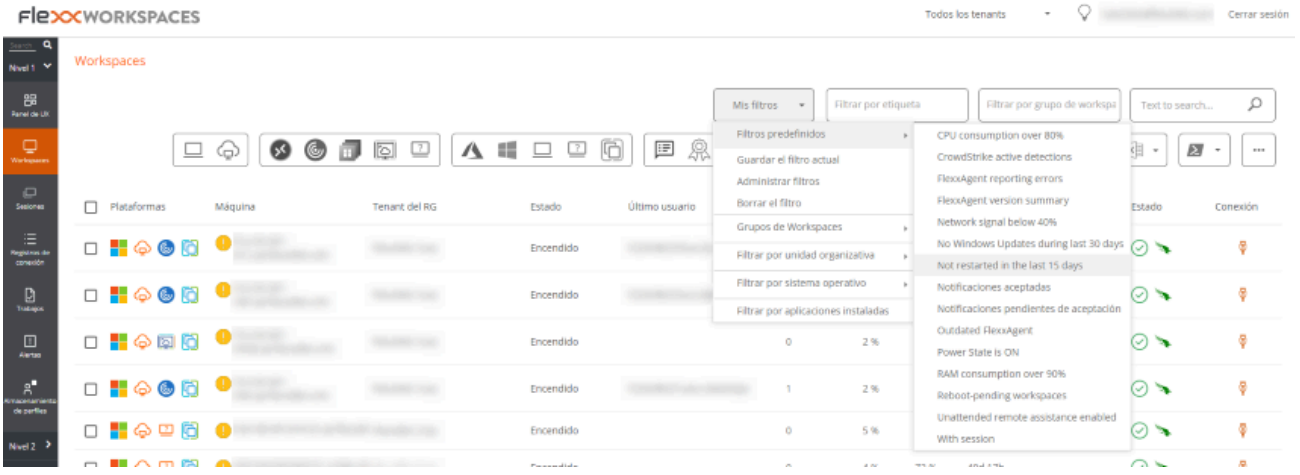
In the side menu of the `Workspaces` module, go to the `Workspaces` option. Select the desired devices in the list view and save them in a new group by clicking on `My filters` -

> `Workspace group` -> `Save as workspace group`.




## Creating a Dynamic Workspaces Group

From the list view of `Workspaces`, in the `Workspaces` module, right-click any field in the table to access `Filter builder` and choose the necessary filters to get a list with the devices that will form the new group. You can also choose filters from `My filters` -> `Default filters` or from any filtering option offered by the `Workspaces` view.

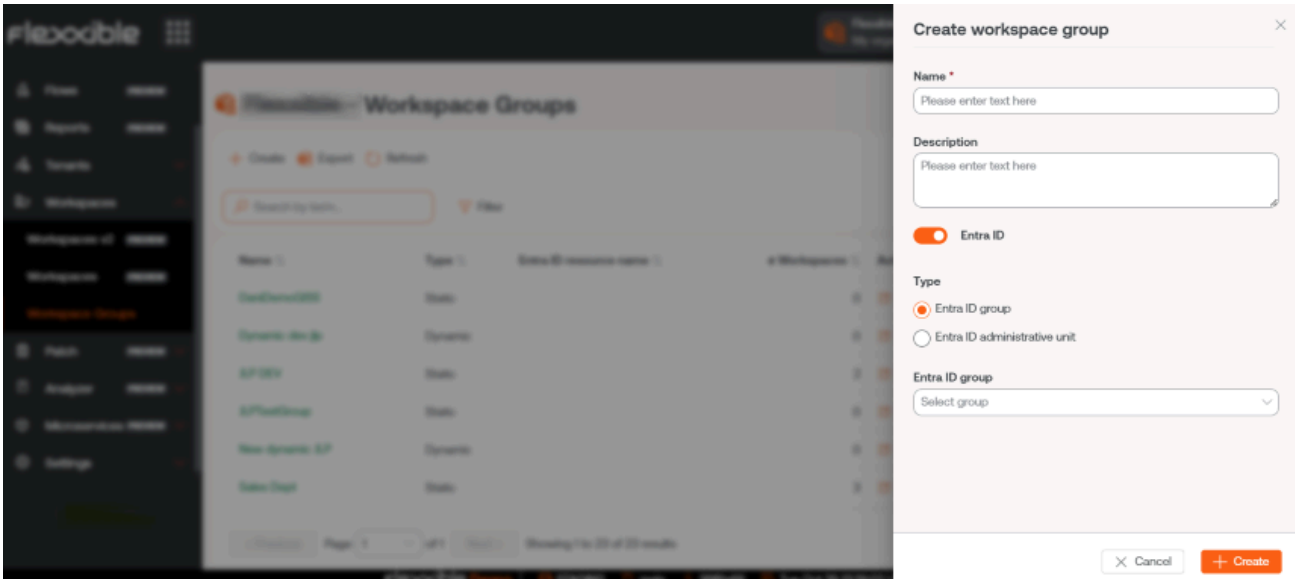



With the device list ready, go to `My filters` -> `Workspace group` -> `Save as dynamic workspace group`. Workspaces will not allow creating a group if the filters for the devices are not specified first.

Workspaces will create a `Job` with the new group. If you want to check that it has been correctly formed, you can do so from the list view of `Workspaces Groups`, in Portal.

## Creating an Entra ID Workspaces Group

Entra ID groups are created from Portal. In the side menu, go to `Workspaces Groups`. Click on the `New` button located at the top of the list view. A form will open where you must add a name, a description for the group, and activate the `Entra ID` button. Next, select the type of group to be created: **Entra ID Group** or **Entra ID Administration Unit**.




Entra ID groups require an API connection, which can be configured from `Portal` -> `Settings` -> `Integrations`. Only from there can the created **Entra ID Group** and **Entra ID Administration Unit** be consulted and therefore operations can be carried out on them from the Workspaces module.

# Group editing

Depending on their typology, group editing is detailed in the following points.

## Editing a Dynamic Workspaces Group

To change the filters of a dynamic workspace group, and therefore the members of that group, the following steps must be followed:

1. Search for the group name in the `Filter by workspace group` search box located in the `Workspaces` list view.
2. Right-click on any field in the table with the list of workspaces to access the `Filter builder`. From there you can choose the new filters for the group. Please note that Workspaces will overwrite the original filters; that is, it will remove all old filters and replace them with the new ones. Press `OK`.
3. With the new device list, go to `My filters` -> `Workspace Groups` -> `Save as dynamic workspace group`. It is important to save the group with the same name it had before so a new group is not created.

## Deleting a Workspaces Group

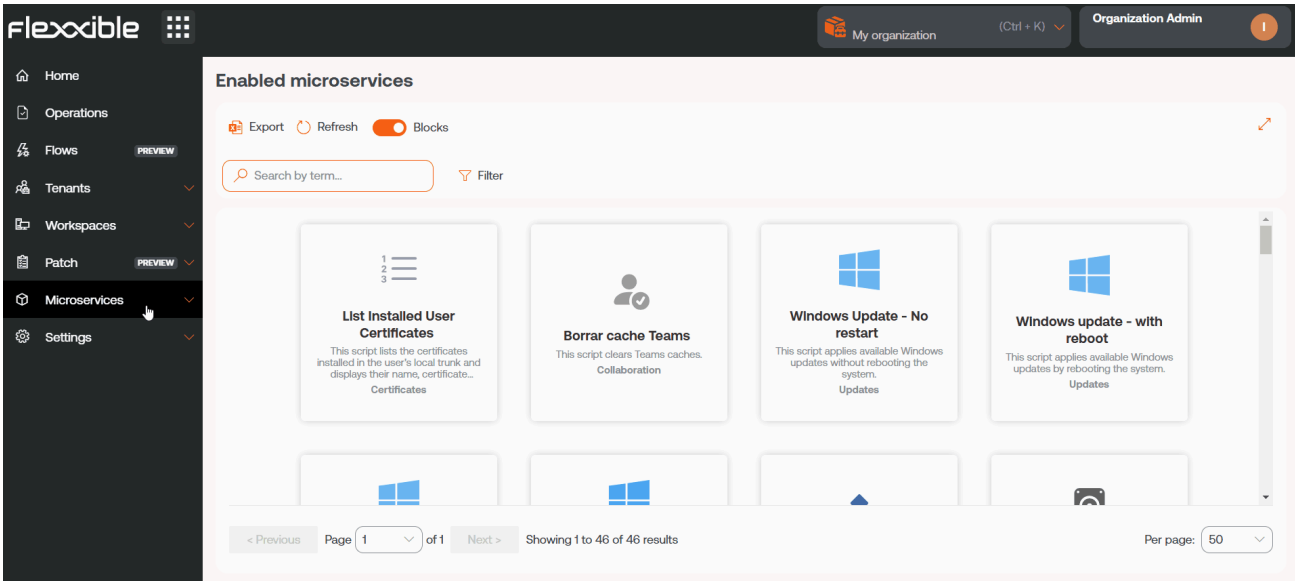
In the list view of `Workspaces Groups`, in Portal, click on `Detail View` of the desired group. In the `Group Details` tab -> `Edit`, a form will open with the `Delete` option.

> **INFO**
>
> For more information on how to create or manage `Workspace Groups`, please refer to this guide.

# Portal / Microservices

Microservices allow you to create, package, and publish scripts so the technical teams in the organization can easily execute them. This also allows initial support levels to delegate their execution, so that user requests can be efficiently handled and the most frequent problems solved.

The created microservices can be executed on the devices themselves, with local administrator permissions or with user session permissions.




They can also be scheduled to run at the most opportune time. They even support event or alert triggers, which can be used as a self-remediation mechanism when a problem is detected.

# Microservices management

Microservices have several configuration options that modify their behavior; for instance, it can change depending on whether the script runs from the user session or from the local administrator.

## Activation in Portal

To activate a microservice and have it available for execution in Workspaces, go to `Marketplace` in `Microservices` of `Portal`. From there, after exploring and finding the microservice of interest, it can be enabled with the button located in the top right corner of the interface.

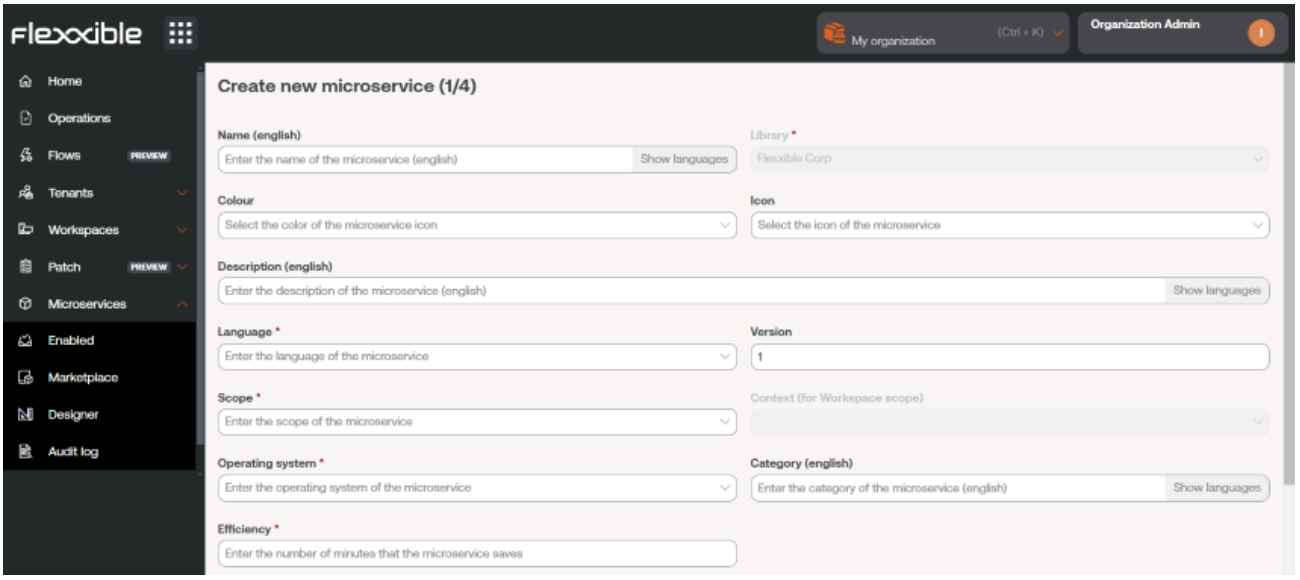
After a few seconds, the microservice will be visible in Workspaces and can be executed on the devices.

## Microservice creation

To create a new microservice, go to the `Designer` section and click on `New`. The wizard will open, asking to enter the following information:

- Microservice name
- Icon color
- Microservice icon
- Brief description of what the microservice does
- The language it is developed in
- Version number
- Scope of execution, you can select at system level (administrative access) or session level (with user identity)
- Operating system it is designed for
- Category: directory or group of microservices accessible from Workspaces where this microservice will be hosted
- Time efficiency achieved with each execution

> **INFO**
>
> **The microservice name should not contain special characters** (like \ / : * ? " < > and other language-specific characters for certain keyboard distributions) if the microservice will be used as an end-user microservice.




## States of the microservices

Microservices have three states:

- Enabled
- Disabled
- Archived

## Considerations about the code to use

Although microservices allow the execution of any CMD or PowerShell command on Windows devices, the sent commands will be executed from the local administrator or the user session, depending on the assigned scope. This can mean that some cmdlets do not have the expected output in relation to the execution performed; therefore, if a script is being made in PowerShell, a series of considerations should be taken into account:

- It is recommended that the installed version of PowerShell on the devices is the same as the one used to develop the microservices.

- The microservices can be executed under the user session identity or from the local administrator.

    - Execution from the local administrator: in `Scope` you can configure `Applies to Workspaces` or `Applies to servers`, which makes it much easier to interact with processes, services, and act with administrative permissions on the device, but it can complicate accessing specific user or session information.

    - Execution from user session: in `Scope` you can configure `Applies to user sessions`, which is very useful for accessing user information such as the registry, information contained in the profile, etc. It should be noted that the script will be executed with the permission level that the user has, so if the user is not a local administrator, there will be certain limitations when acting at the system level.

- When we want to display a message in the microservice output, it is recommended to use the cmdlet "Write-Output" instead of "Write-Host".

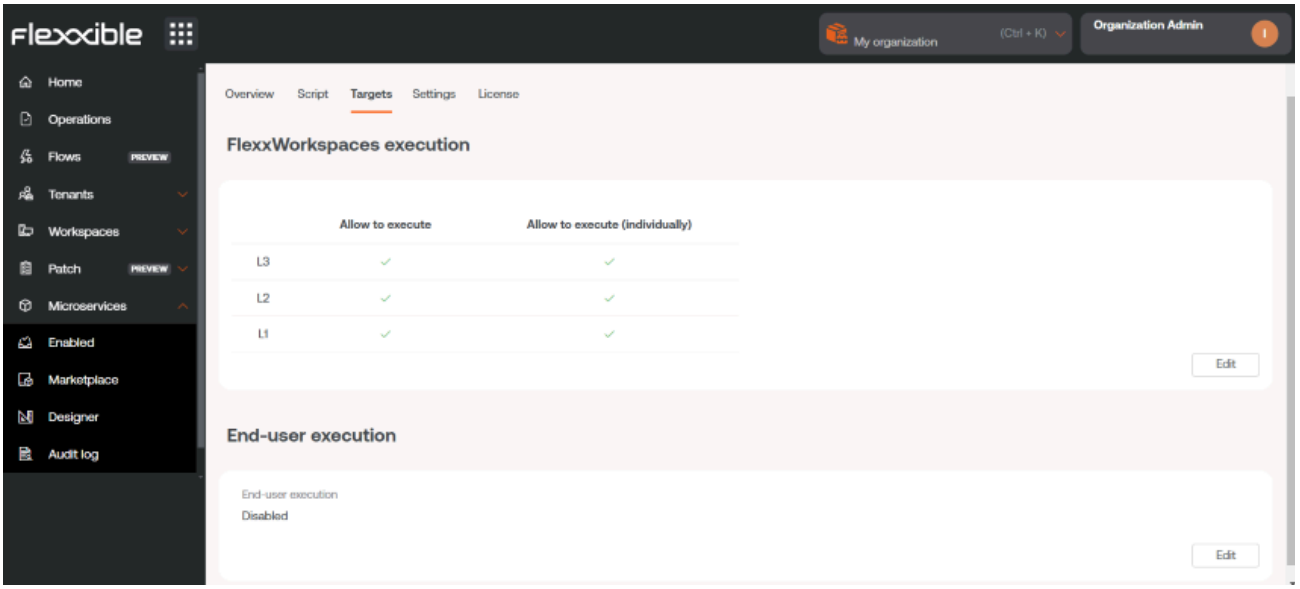
- The output of the execution can be consulted in the details of the `Job` generated in the execution.

# Ways to consume microservices

Microservices can be created and enabled in Portal, and from there be configured to be executed by the end-user, launched through a `Flow` or to be executed with automated or support actions from Workspaces.

## End-user execution

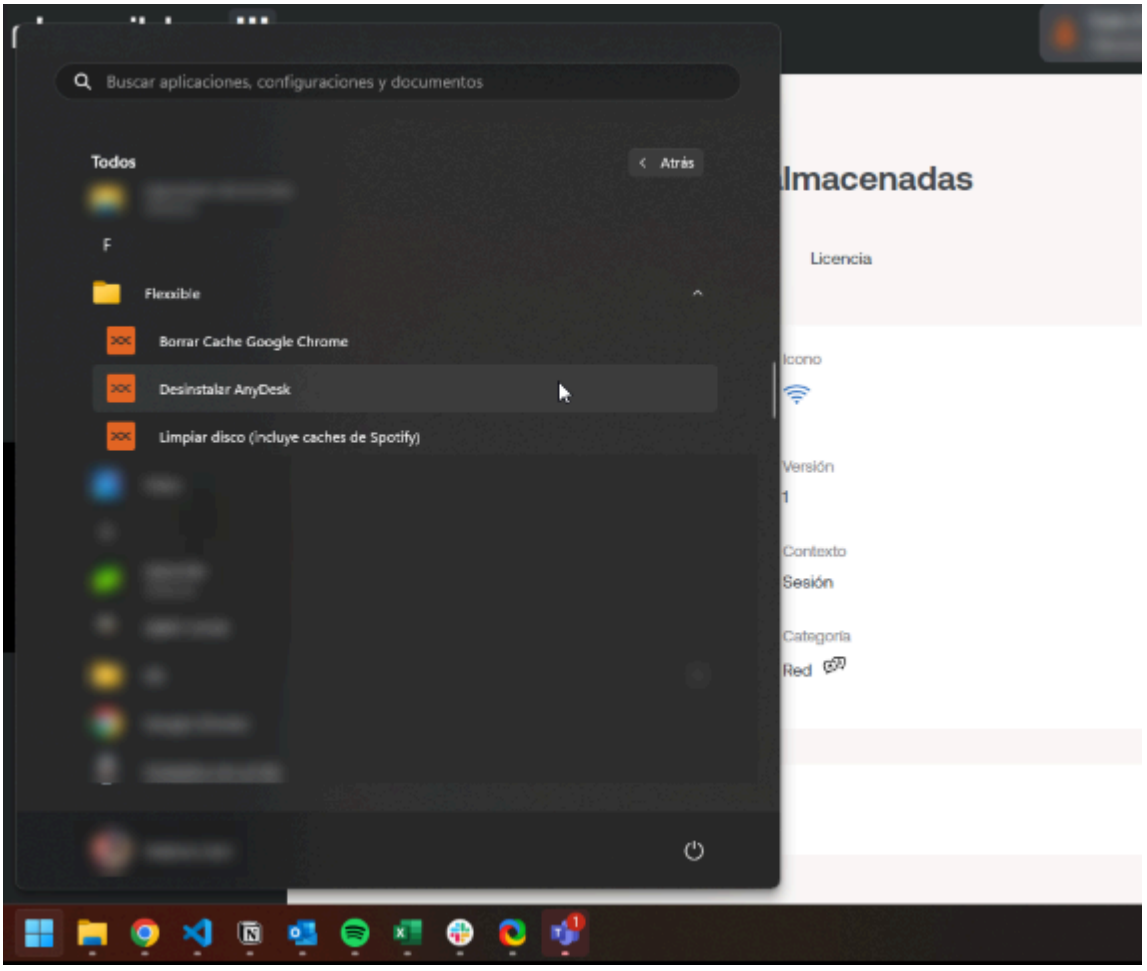
In `Portal` -> `Enabled` by clicking on a microservice you access its characteristics. In the `Recipients` tab -> `Execution from Workspaces` the execution permissions of the microservice in Workspaces are shown. Next, in `End-user execution`, you can see if the microservice has the option enabled to be run by the end user. If so, it shows the user's name and the number of devices where it's available.




If the option `Execution by the end user` is activated, the microservice will add a button on the user's device home screen, so that it can be executed in a quicker and more direct way.

> **INFO**
>
> For more information on how to enable a microservice for the end user, please refer to this guide.

**The microservice name should not contain special characters** (like \ / : * ? " < > and other language-specific characters for certain keyboard distributions) if the microservice will be used as an end-user microservice.




A configuration change to an existing end-user microservice can take up to 15 minutes to apply to all linked devices.

## Execution through a flow

`Flows` is a feature that can be configured in Portal. It allows creating automation flows and executing a microservice automatically when certain conditions are met on the device.

Its main feature is that, through the execution of a microservice, it simplifies proactive diagnostic actions and quickly solves problems when there is a focus on their detection. In the Flows section, you can get more information about its features and configuration.

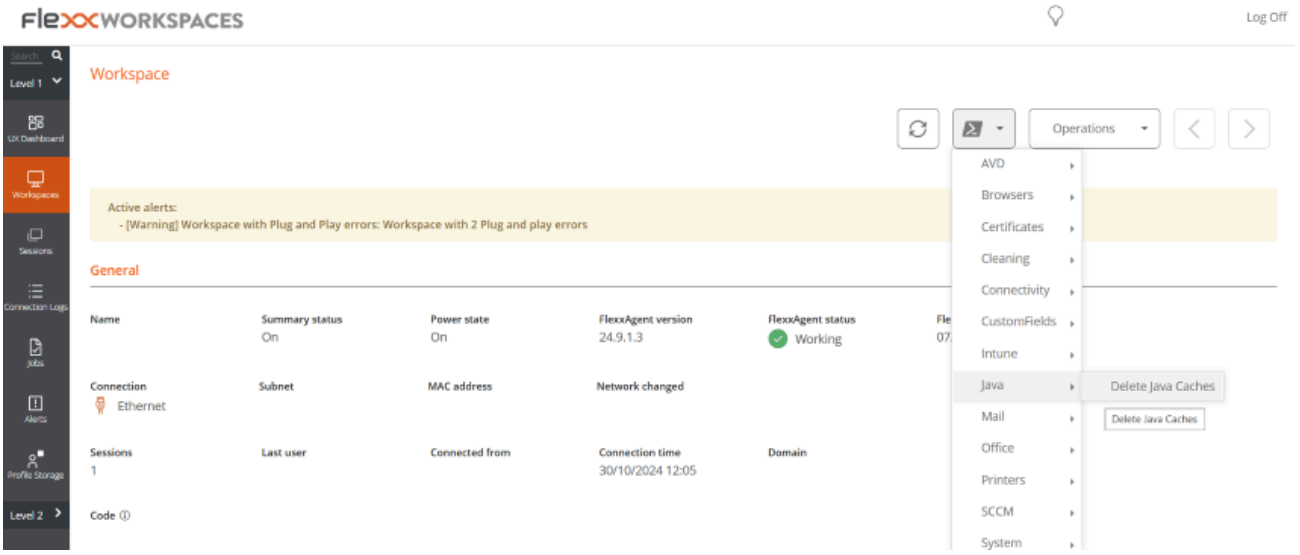
## Execution from Workspaces

From the Workspaces module, any microservice that has been previously enabled in Portal can be executed. To do this, the user must go to the `Workspaces` or `Sessions` tab and

select the devices they want to apply the microservice to.

Microservices will be available from the `Workspaces` tab when they have been previously configured to run at the system level. And from `Sessions` when in their configuration the option to run at session level has been selected.

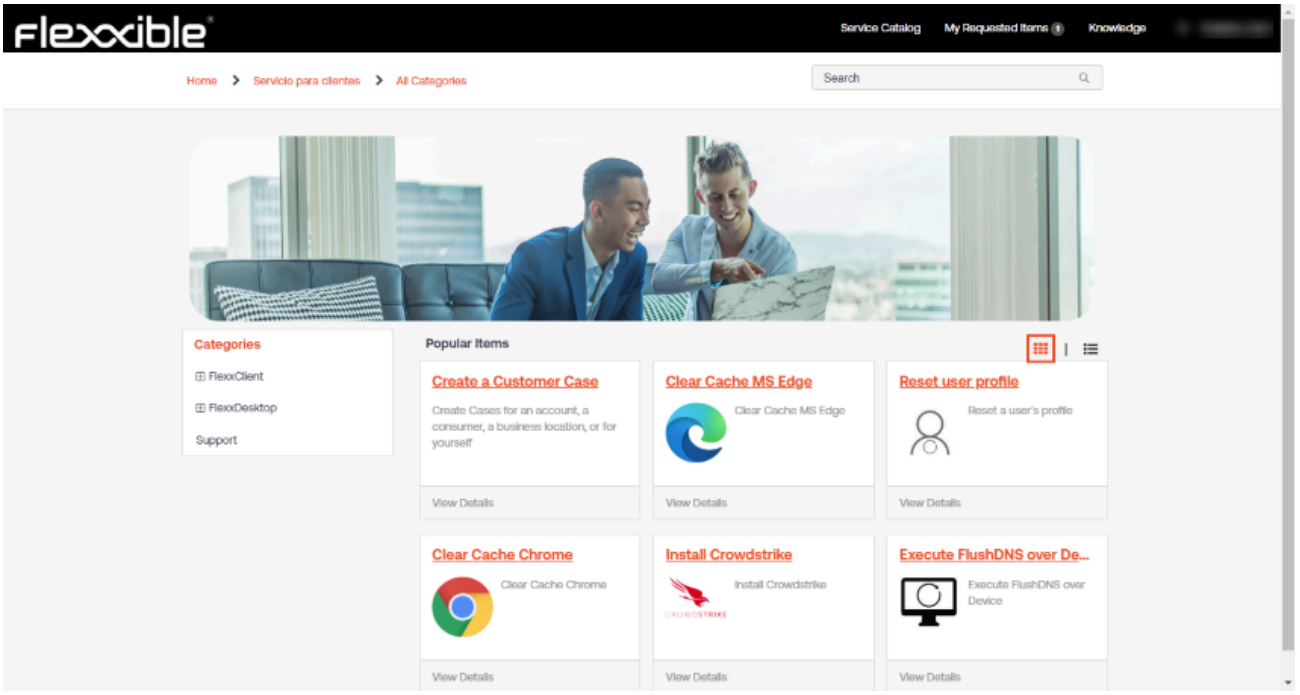
The ability to execute certain microservices will depend on the role or permissions the user has on the platform.




---

## Microservices in Automate

It is also possible to execute a microservice from the Automate module. In this case, users do not have to go to the Home screen of their device to be able to activate it; they can do it from the Service Catalog, a space that acts as a self-service panel for the user to choose the microservice they want to execute.



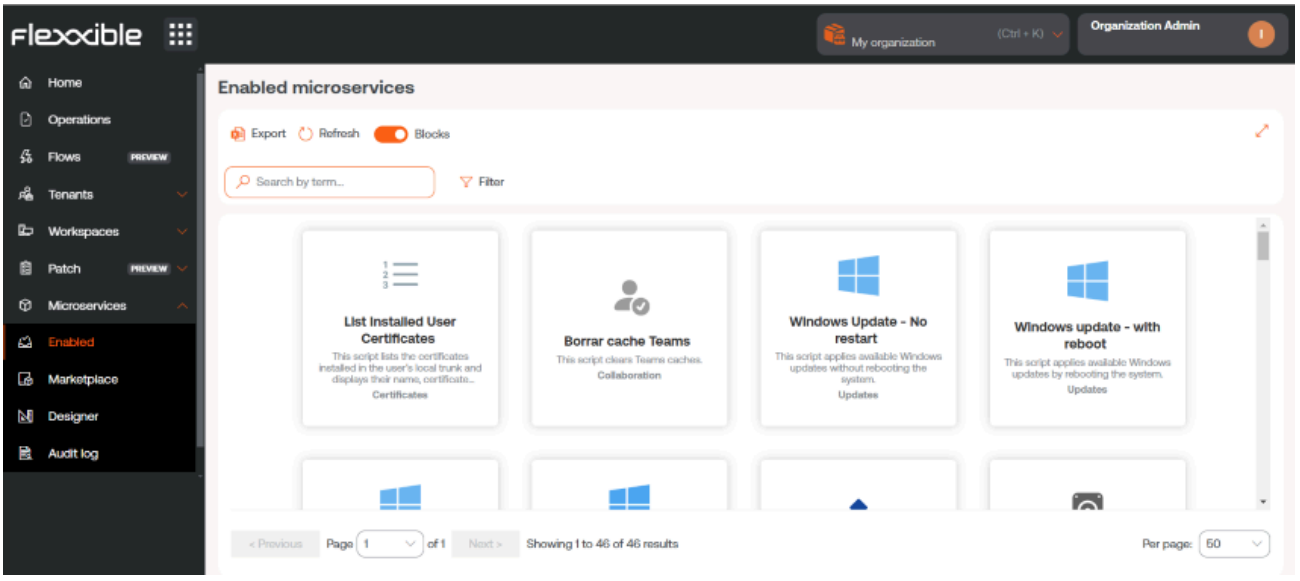

Executing a microservice from Automate has two advantages:

- It allows the creation of parameters: certain microservices can have different selectable values, where the user can decide the type of information they want to obtain when activating the microservice. It also has the option to enter the value of a variable to customize the execution.

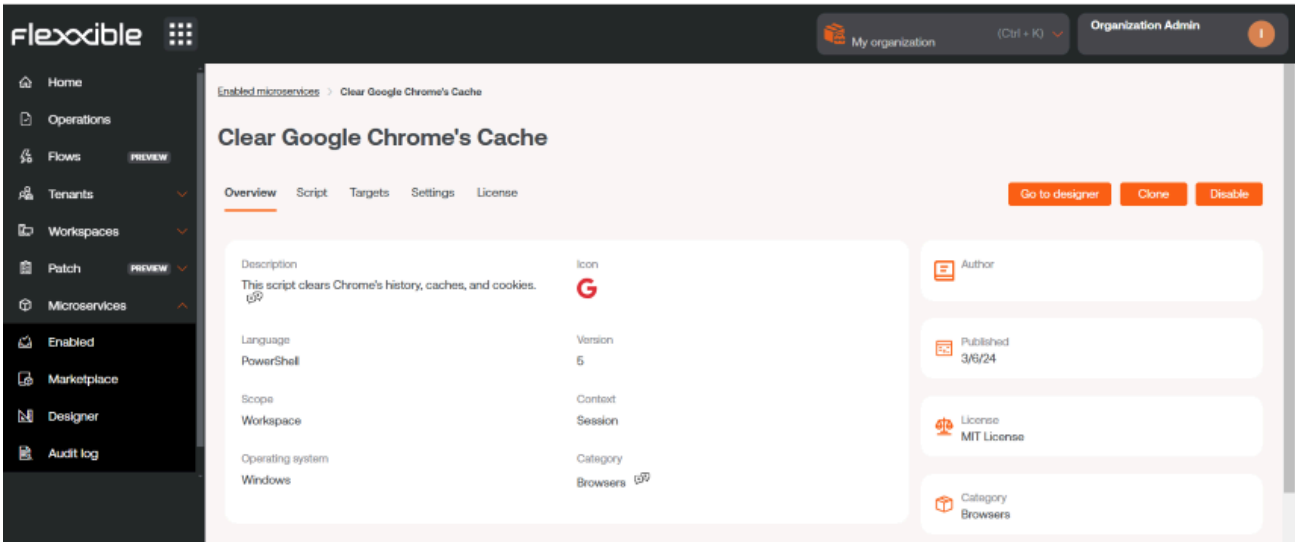
- They may go through an approval flow: when it comes to executing microservices that may have significant importance, such as economic or security, they will require going through an approval process within their own organization and by Flexxible.

# Portal / Microservices / Enabled

Enabled shows a list of the microservices that are activated for the selected organization, they can be viewed in block form or table form.




By clicking on the name of the microservice you can see specific information about it, such as the author, creation date, type of license and efficiency, which is the estimated time the user will save when running the script. It is also possible to access the code, with the possibility to clone it and even edit it.




> Another way to access the list of enabled microservices is from the `Marketplace` section (in block view), where each microservice will show its status: a green dot if it is

> enabled and a grey one if it is not.

Enabling a microservice makes it visible and opens the possibility for it to be executed from the Workspaces module, either from the `Workspaces` tab (system context) or from the `Sessions` tab (session context), depending on how the microservice has been configured in Portal.

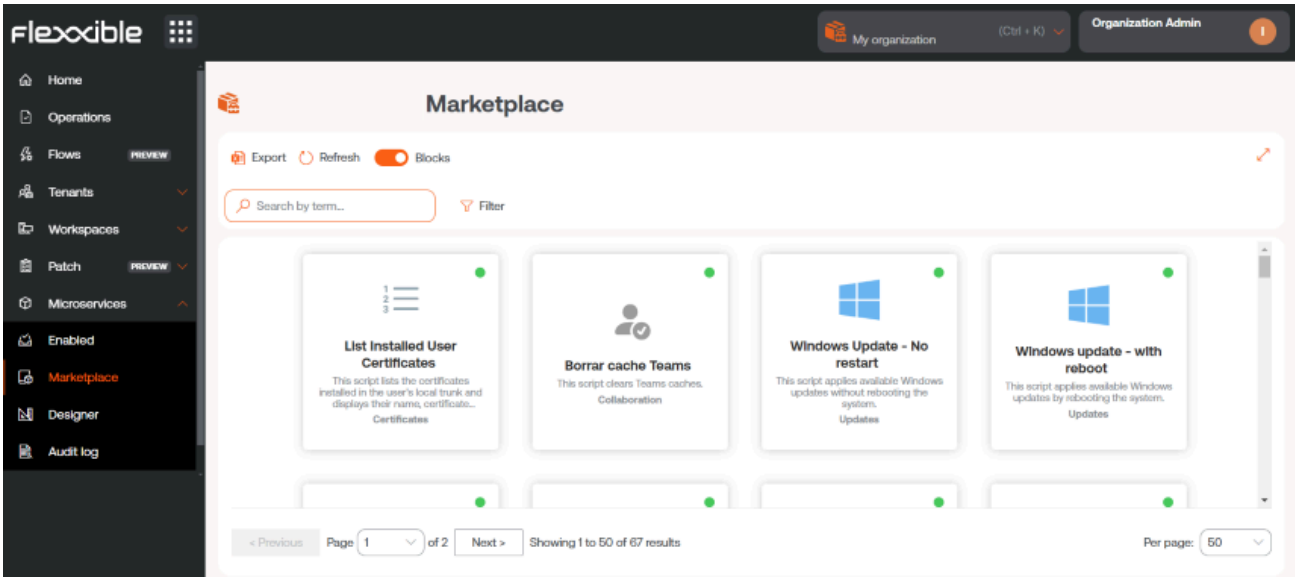
## End-user execution

When a microservice is enabled, the user has the option to add a button for that microservice on their device's Home screen. To do this, you have to enable the `End user execution` option from `Recipients`, once you have selected the microservice you want to manage.

# Portal / Microservices / Marketplace

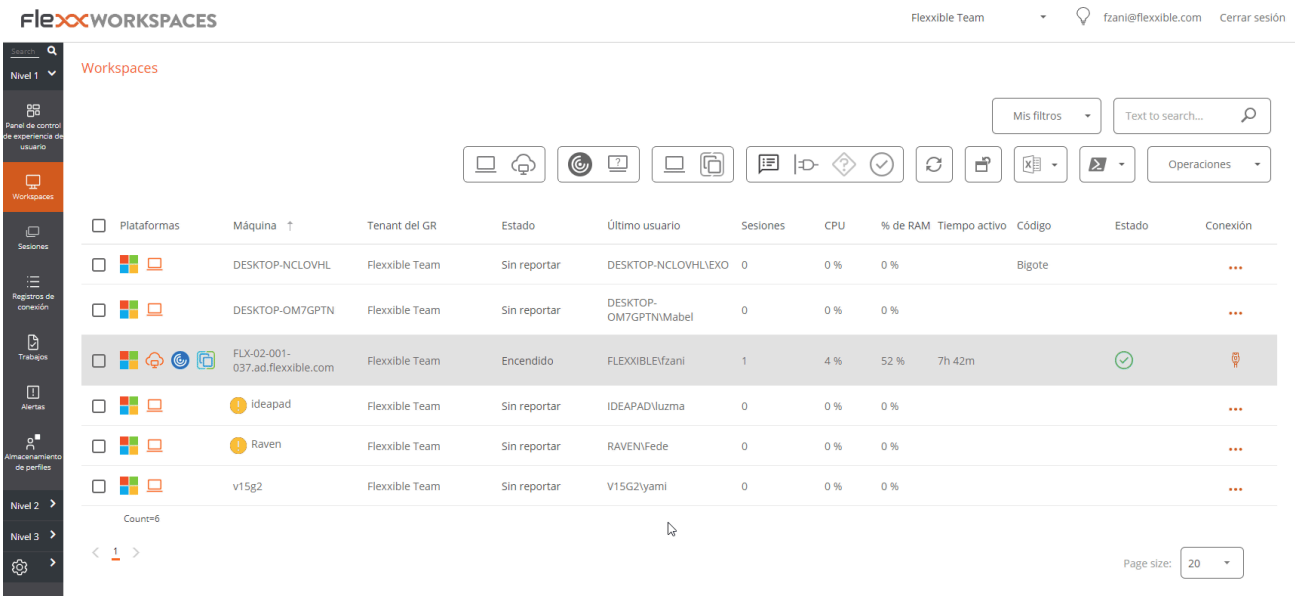
Marketplace offers a great number of microservices that can be used without deep computer knowledge, as they are ready to be enabled and executed instantly.

The overview of `Marketplace` shows microservices in block or table format. In both cases, a green or gray dot is shown next to the microservices. If it's green, it means the microservice is enabled and can be run directly from the Workspaces module. And if it is gray, it means it is pending activation.




To enable a microservice, just select the desired microservice and click the `Enable` button.

To run a `Marketplace` microservice, it must be done from the Workspaces module.

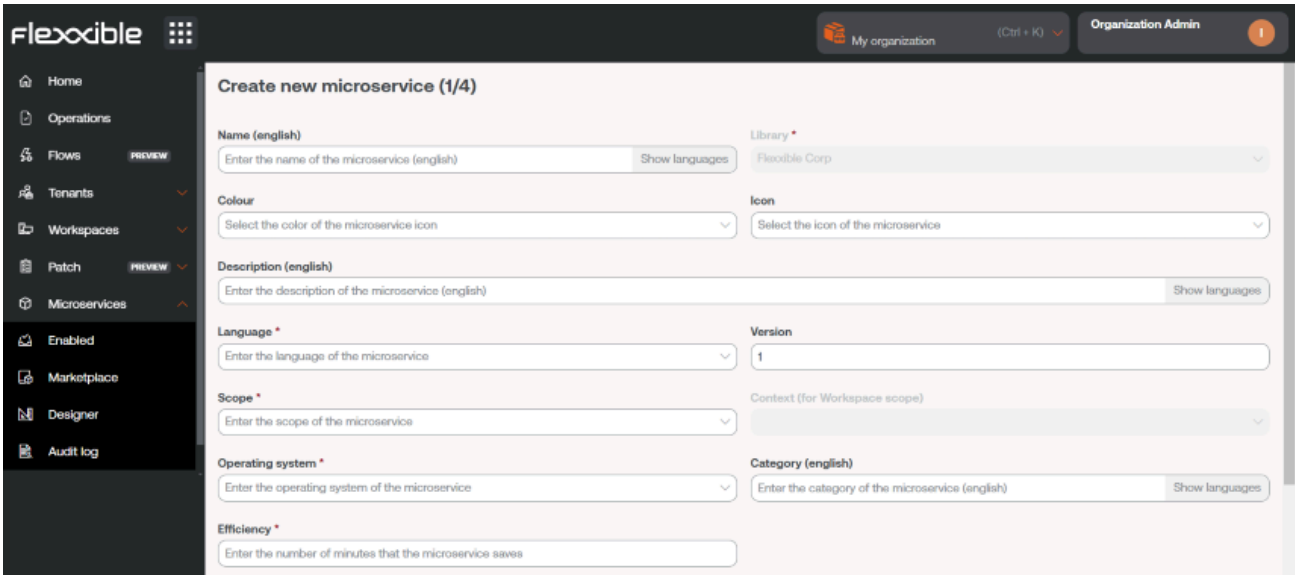


# Portal / Microservices / Designer

Designer allows access to all information related to existing microservices, such as the author, script, execution dates, problem it solves, or type of license; but above all, it allows creating new microservices.

## Microservice creation

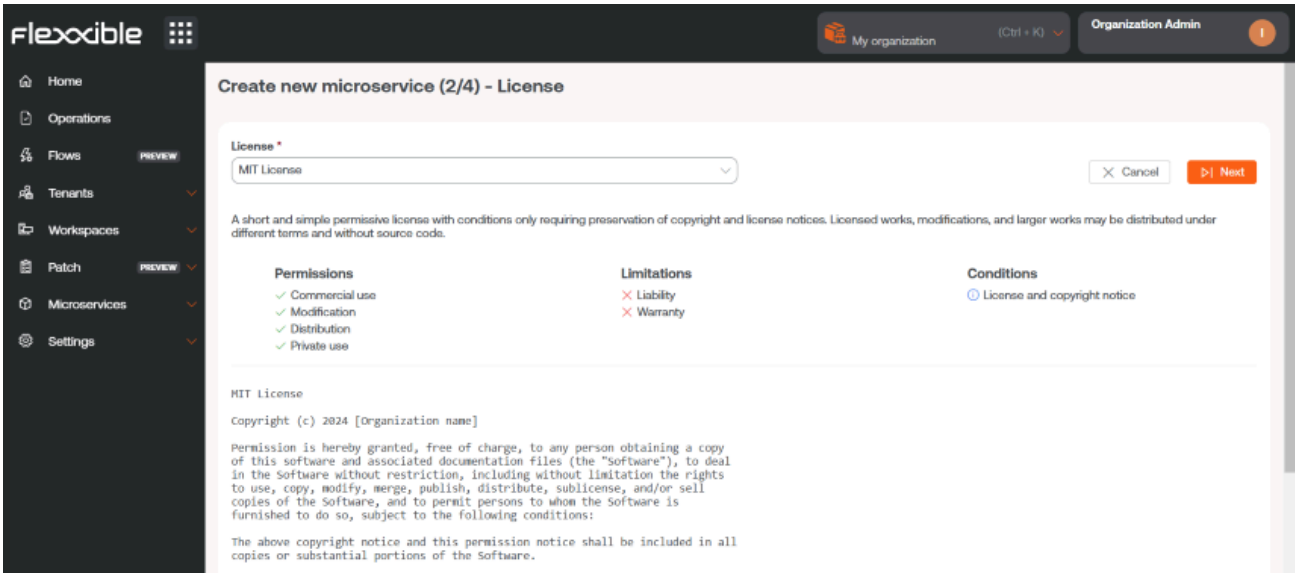
To create a new microservice, from the overview view, click on `New`. The wizard will open, asking to enter the following information:




- Microservice name
- Icon color
- Microservice icon
- Brief description of what the microservice does
- The language it is developed in
- Version number
- Scope of execution, you can select at system level (administrative access) or session level (with user identity)
- Operating system for which it is designed.

- Category: directory or group of microservices accessible from Workspaces where this microservice will be hosted
- Time efficiency achieved with each execution

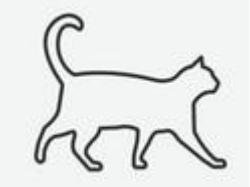
Microservices are created in four steps. Once the above fields are filled in, the application will request, as the second step, to specify the type of license it will have.




As the third step, the application will ask to insert a description of the microservice, which accepts Markdown for text formatting.

INFO

To set a title with Markdown, simply start the line with `# Title`. Below are some examples of Markdown syntax:

| Item | Markdown syntax | Preview |
| --- | --- | --- |
| Bold | **bold** | **bold** |
| Italic | *italic* | *italic* |
| List | - List item | - List item |
| Link | [text](url) | text |
| Image | ![alt](url) |  |
| Code | `code` | `code` |
| ::: | | |

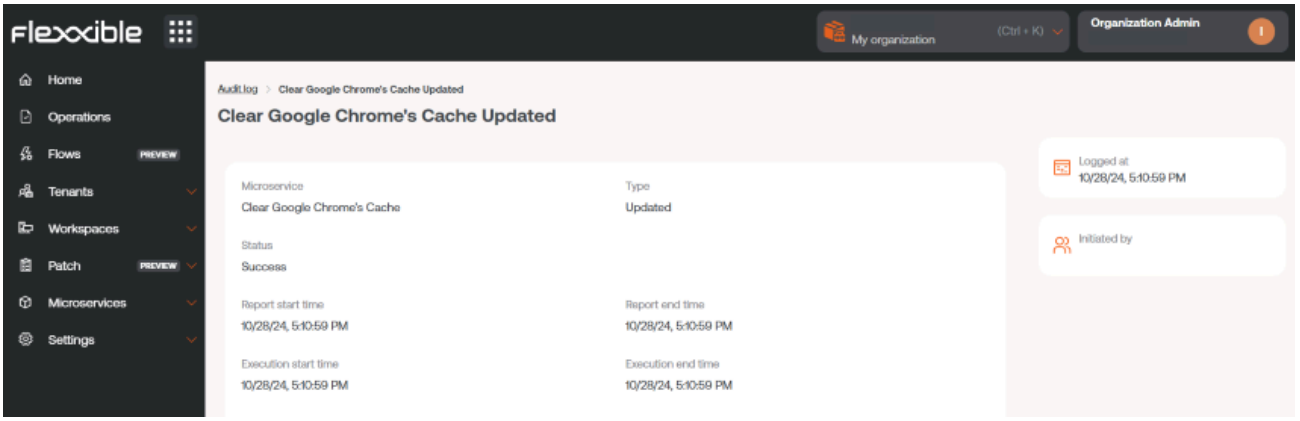
And, finally, insert the script.

INFO

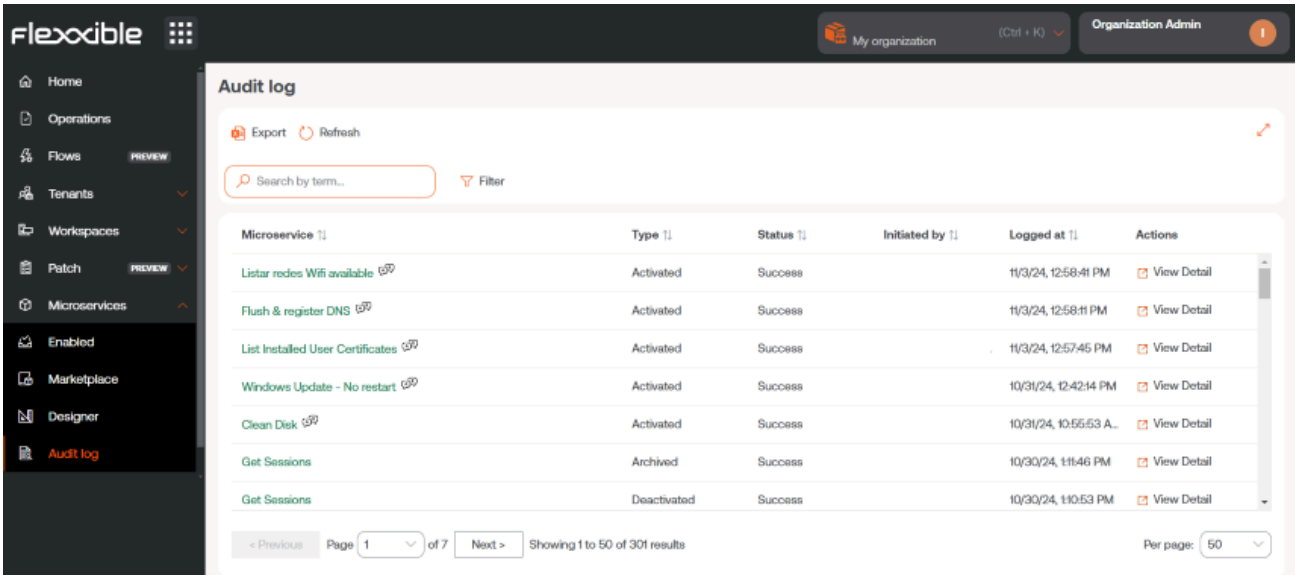
For running PowerShell code, make sure to consider the code considerations.

# Portal / Microservices / Audit Log

The audit log allows tracking the use of microservices, showing the most recent log of the start and end times of the selected microservice execution.

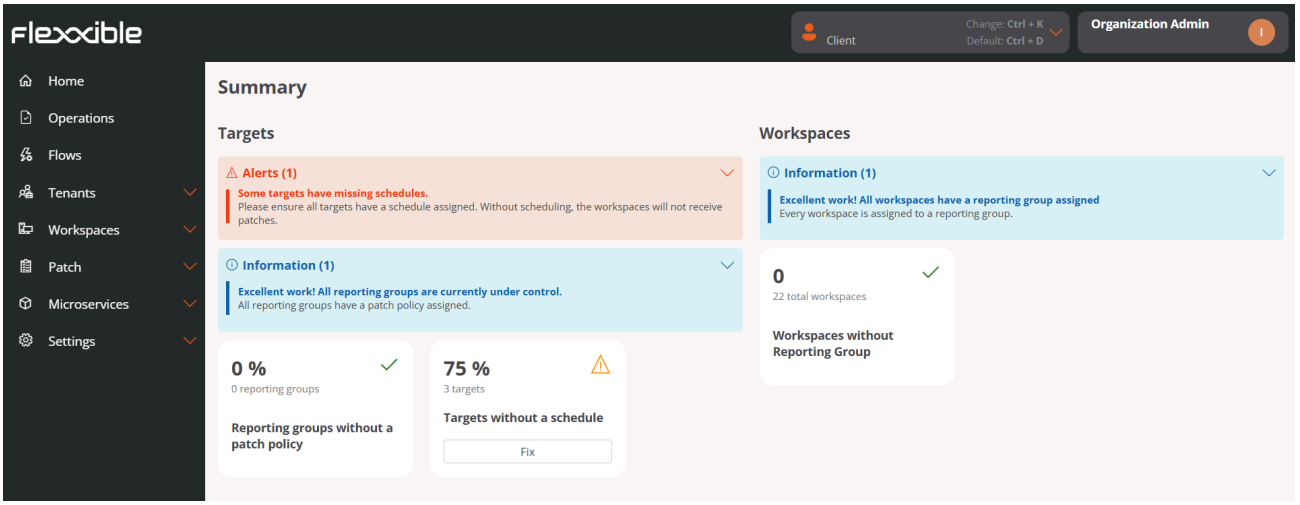



From the overview, you can also consult the rest of the information related to the microservice, such as its status, the script author, and the creation date.



# Portal / Updates

Through `Updates`, a user will be able to manage how, which, and when updates will be applied on the devices of the report groups of their organization.




# Patching management features

- They are essential to keep systems updated and secure because they significantly reduce the chance of a cyberattack.
- They solve known vulnerabilities, which minimizes the risk of security breaches that could compromise sensitive data and technological integrity.
- They ensure the stability and optimal performance of operating systems and applications.
- They fix errors, resulting in a smoother and more productive work environment. This translates to fewer interruptions and an overall increase in organizational efficiency.
- Many regulations require organizations to keep their systems updated to protect against threats; in this sense, patch management facilitates regulatory compliance and contributes to business continuity.

# Patching management considerations in Portal

- Allows scheduling time windows for performing update processes.
- It is available for devices with Windows operating systems. Includes Windows 10, Windows 11, Office 365, Office 2019, Microsoft Edge, Microsoft Defender, Drivers, etc. Does not include patching Windows server roles.
- Allows managing updates of Microsoft components. Optionally allows selecting which ones to install on the device.
- The functionality is aimed at environments where there is no prior patch management system.
- Allows auditing update processes to manage exceptions and errors.

> **INFO**
>
> Activating patch functionality in an environment that already has an update system running could create conflicts or unexpected behaviors. It is recommended to maintain a single active patch system.

## FlexxAgent behavior in patch management

FlexxAgent is responsible for executing the update process and validating which patches should be installed and which should not according to the policy configured by the user in Portal. If FlexxAgent does not detect any directive for the application of updates, it will execute patches as they become available, according to the device's own configuration.

If a user decides to deny the installation of a patch, but FlexxAgent finds that update on the device, in the next update process FlexxAgent will try to uninstall it, although it should be noted that there are patches that the operating system does not allow to uninstall due to their nature.

> **INFO**
>
> If the device has a system proxy, it must allow communication with Windows Updates.

# Portal / Updates / Summary

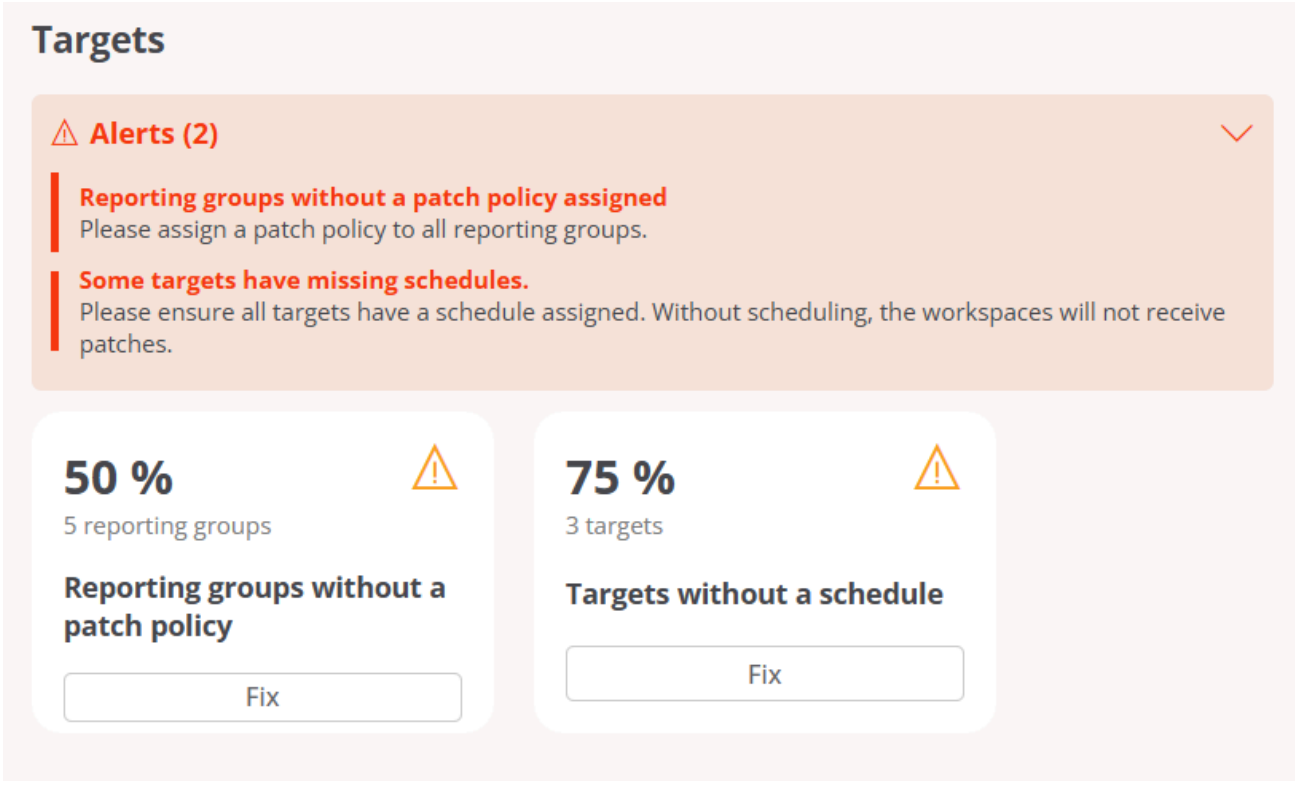
`Summary` shows a panel that describes the status of patch application on the organization's devices. From this view, you can get quantitative information about two aspects:

- Recipients (Targets)
- Workspaces

## Targets

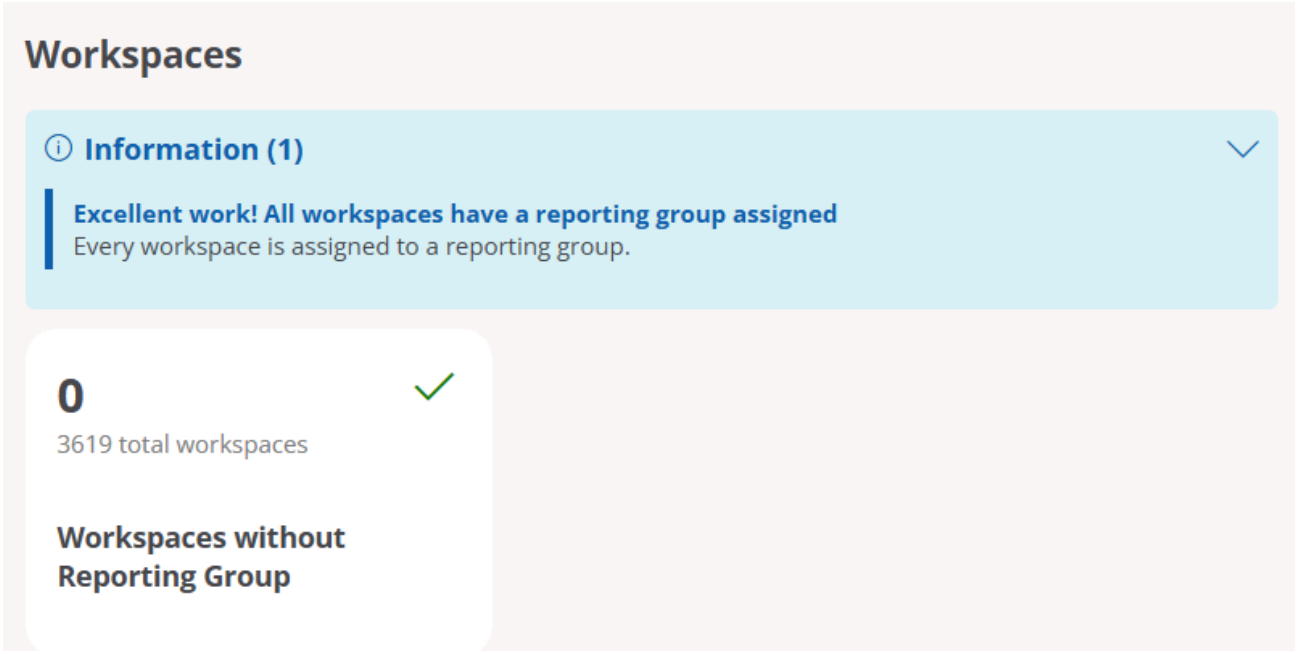
This panel shows the percentage of reporting groups in the organization without a defined patch policy, as well as the percentage of targets without a configured schedule.

When it is detected that there are report groups without an associated patch policy or targets without a configured schedule, an alert warning is displayed (in orange); and when the cause of the warning is resolved, an informative alert is displayed (in blue).




## Workspaces

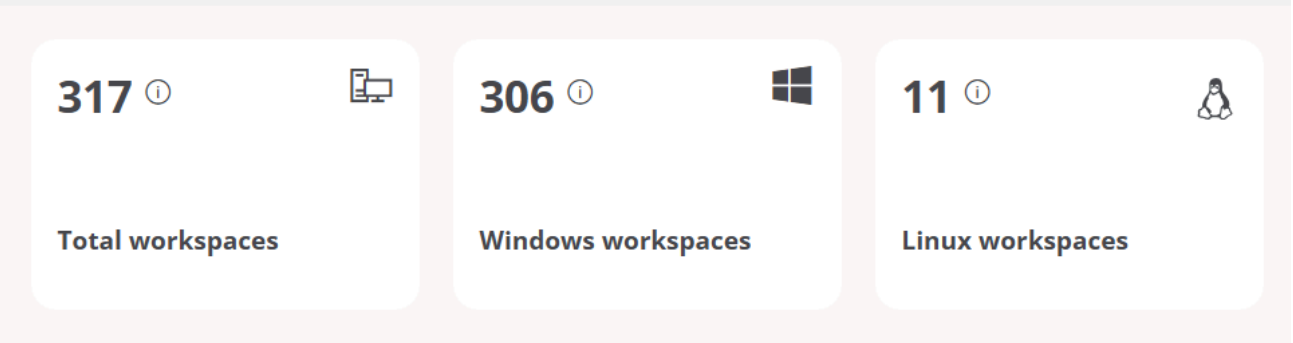
This panel informs about the organization's devices without an assigned reporting group. When FlexxAgent detects this type of devices, a warning notice (in orange) is shown; when all devices have an assigned reporting group, it is indicated through an informational notice (in blue).



# Portal / Updates / Reporting groups in patch management

Reporting groups classify devices according to their functions, departments, or locations. When they are assigned a target to configure their patch policy, an organization ensures coverage of its entire computer network.

At the top of this section, you can see an information panel showing the total number of devices that are part of the organization, divided according to their operating system.



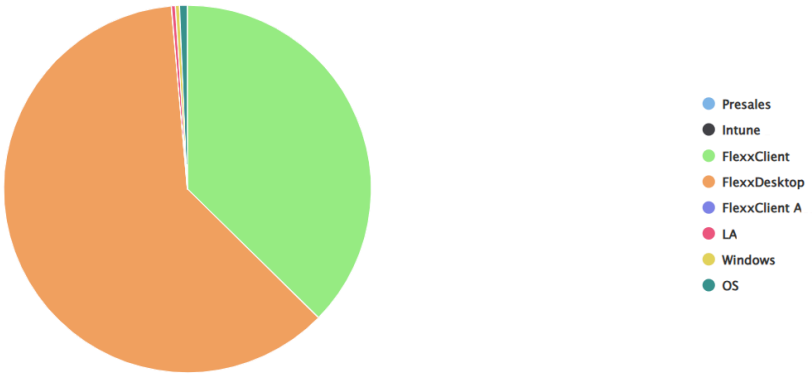

**INFO**

A reporting group can only have one target, but a target can be applied to more than one reporting group.

## Total devices per reporting group

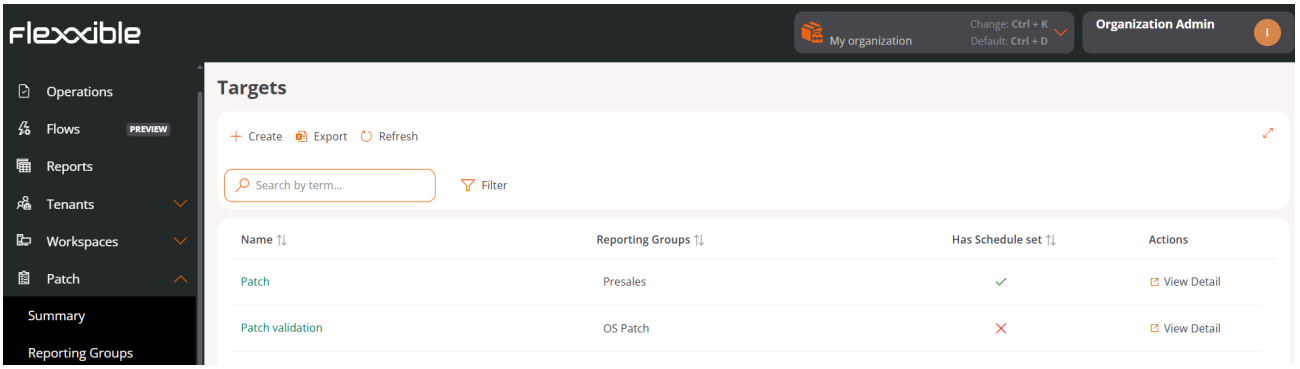
At the bottom of this section, this panel indicates the distribution of devices in an organization according to the reporting groups that FlexxAgent has identified.

**Total workspaces by reporting group** ⓘ



# Portal / Updates / Targets

Through `Targets`, you define when, to whom, and how updates are applied. Allows creating, configuring, and deleting patch policies on devices that are part of specific report groups within an organization.




The overview of this section shows a table with the list of created targets, along with the following information:

- **Name**: name assigned to the target.
- **Report Groups**: name of the report group (it can be more than one) that will be subject to the target's patch policy.
- **Has scheduled time**: indicates whether the target has scheduling enabled for applying patches.
- **Actions**: shows the `View details` link, which opens a window with the target details and its configuration options.

## Create a new target

To create a new target and define its patch policy, click on `New` at the top of the table. Next, a modal window will open with a form where you must assign a name to the new target, the report groups to which its patch policy will apply (can be one or more report groups), and optionally, its linkage to a Microsoft update policy.

Patch policies are applied to report groups; it's not possible to apply a patch policy to an individual device from Portal. To force the update of a specific device, it must be done from

the Workspaces module: `Workspaces` -> `Operations` -> `OS patching` -> `Patch OS now`.

> **TIP**
>
> For more information on how to create a new patch policy in Portal, please refer to this guide.

# Target details

From this view, you can configure the target's patch policy in two areas:

- Details
- Schedule

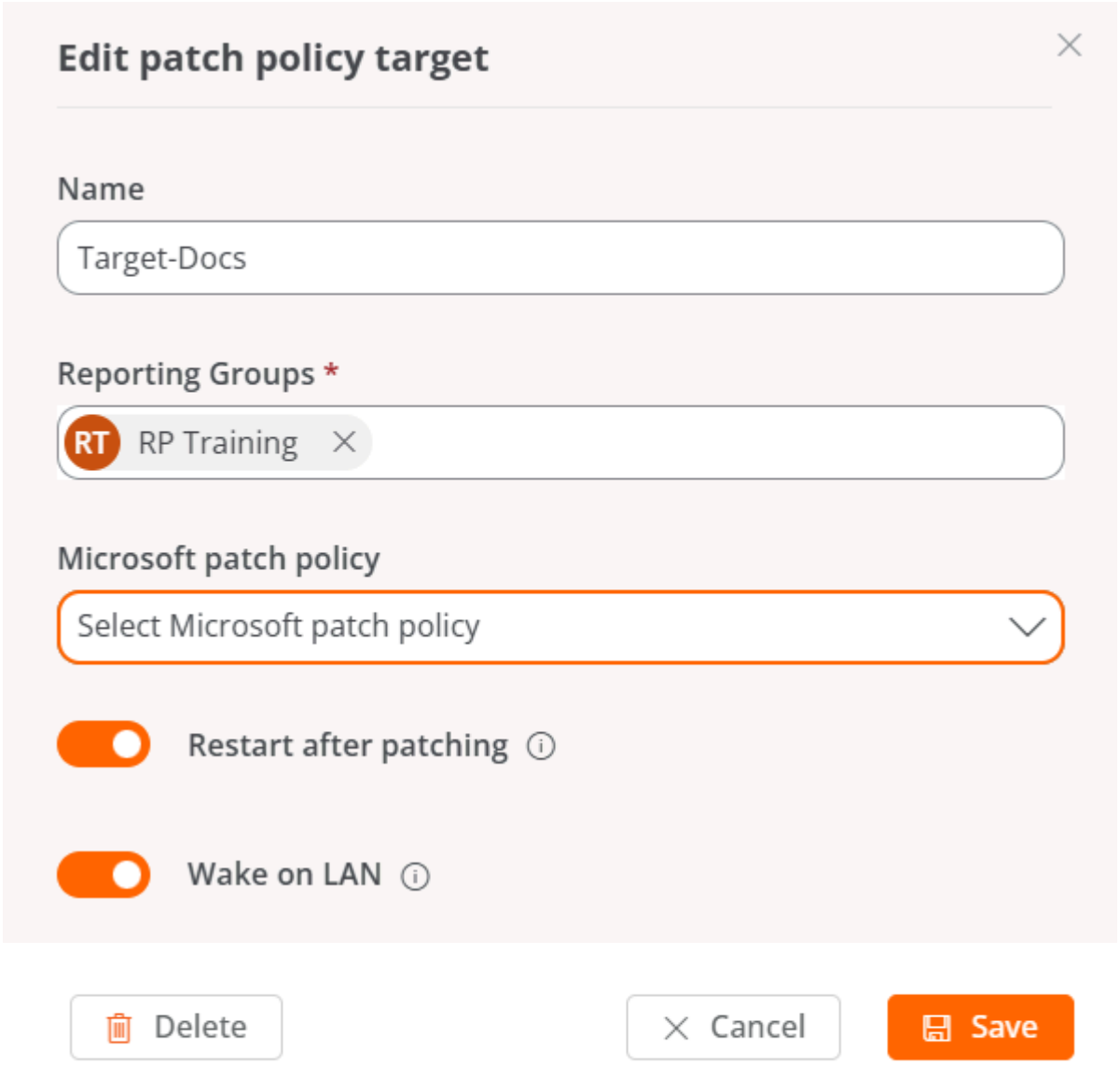
## Details

This tab shows the following information about the policy being reviewed:

- **Name**: name assigned to the target.
- **Restart after applying updates**: indicates whether the device will automatically restart when patch installation is complete.
- **Wake on LAN (WoL)**: allows patches to be applied even when devices are suspended or turned off.
- **Microsoft Update Policy**: name of the Microsoft update policy that is being applied to the target.
- **Report groups**: shows the report groups assigned the patch policy.

> **INFO**
>
> A reporting group can only have one target, but a target can be applied to more than one reporting group.

The `Edit` button opens a modal window that allows configuring the aforementioned aspects.



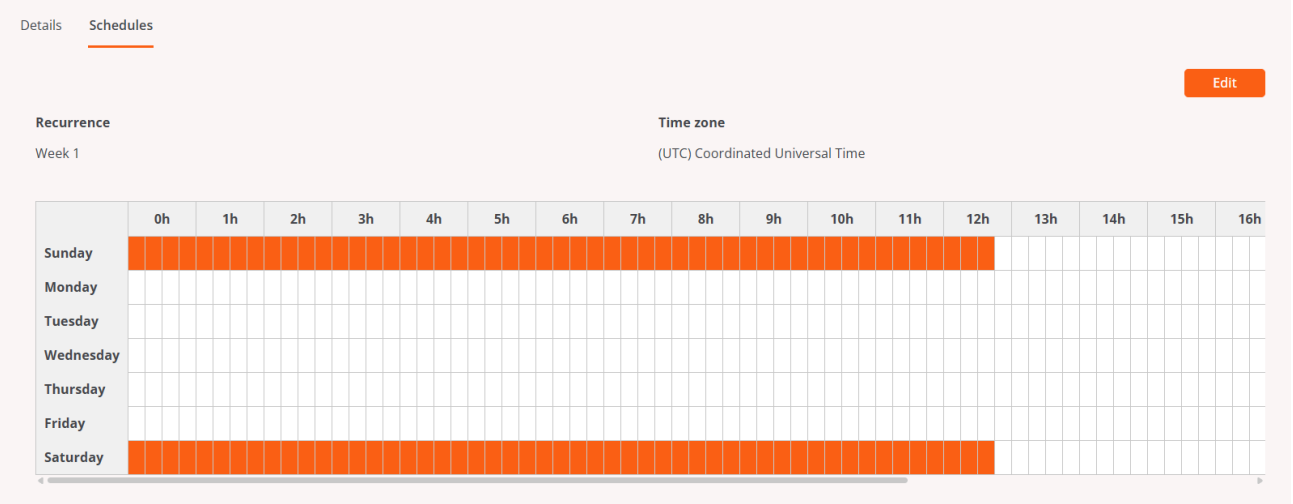

The `Delete` button discards the target's patch policy.

`Details` also provides information about the creation date of the target's patch policy and the user who created it.

## Schedule

From this section, you can schedule when updates will be applied to devices that are part of a report group. And also the established scheduling calendar.

The `Edit` button allows configuring the time zone and the patching time frequency, which can be limited by weeks of the month, days, and hours.




**INFO**

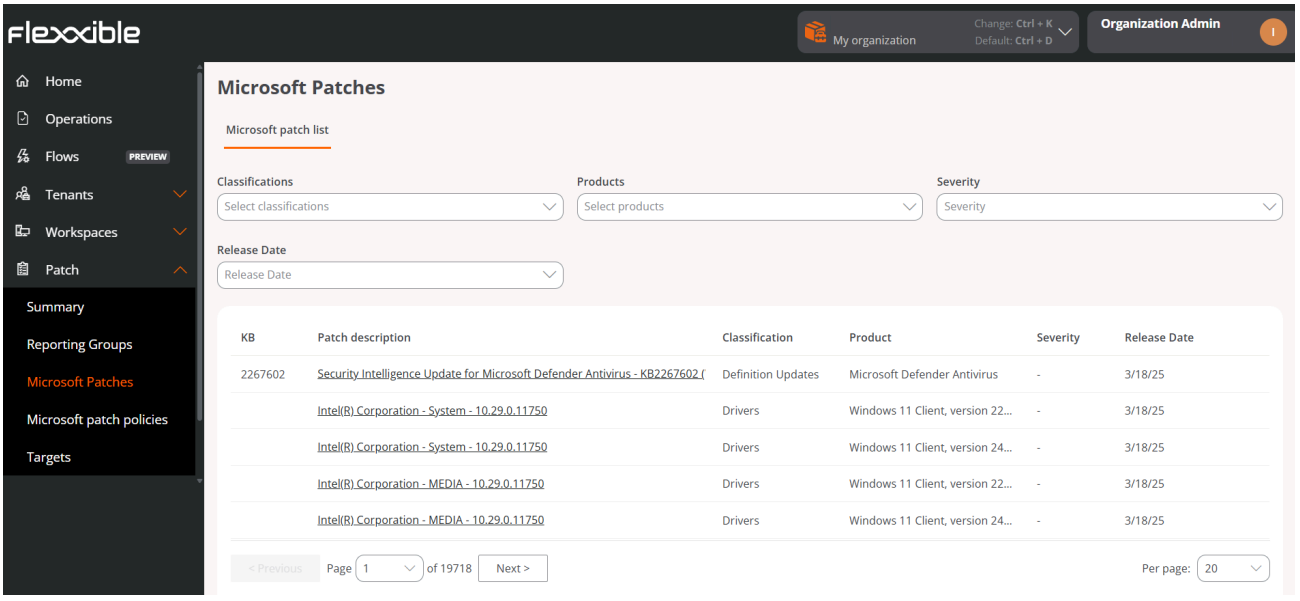
Automatic patch updates from Windows Update will be disabled on all devices belonging to a report group that is part of a target.

# Update process

The details of the update processes launched to each device can be reviewed in the Jobs section of the Workspaces module.

# Portal / Updates / Microsoft patches

This section allows you to check the available Microsoft update catalog. The table fields provide the following information:




- **KB (Knowledge Base)**: is the unique identifier assigned to the Microsoft update package. Some drivers or firmware do not have an assigned KB.
- **Review Description**: link that leads to detailed information about the Microsoft update.
- **Classification**: shows the category that corresponds to the patch.
- **Product**: name of the Microsoft product to which the update applies.
- **Severity**: level of urgency detected for executing the patch.
- **Release Date**: date from which the patch is available.

At the top of the table, you can filter the list by `Classification`, `Product`, `Severity` and `Release date`.

# Portal / Updates / Microsoft patch policies

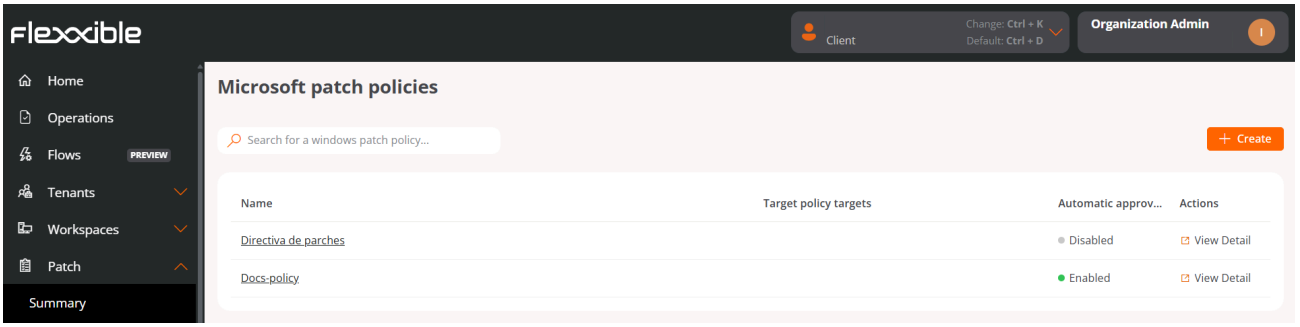
If from Targets you can define when, how, and to whom updates are applied, from Microsoft patch policies you can define what gets updated; that is, you can manage the approval or denial of the installation of one or more updates from the Microsoft catalog on an organization's devices.

## Create a new update policy

To define a new policy, you must click `New` at the top right of the table. A modal window will open with a form prompting you to assign a name to the new policy being created.

After clicking on `Save`, the name of the policy just created will appear in the table.

## Microsoft update policies table




The table fields provide the following information:

- **Name**: name of the Microsoft update policy
- **Target policy targets**: targets configured with a Microsoft update policy.
- **Automatic approvals**: indicates whether the automatic approval settings are *Enabled* or *Disabled*.
- **Actions**: displays the link `View Details`, which opens a window with the detailed view of the Microsoft Updates Policy.

# Detail view

From this view, you can configure the Microsoft update policy in three areas:

- Details
- Microsoft patches
- Automatic approvals

# Details

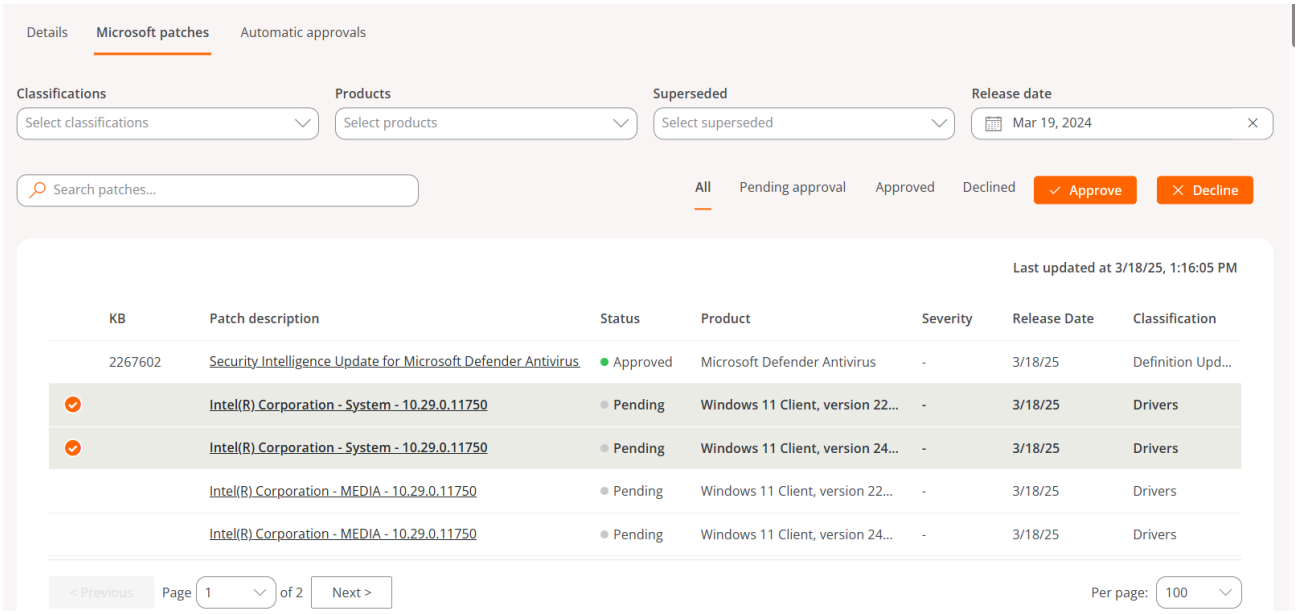
This tab displays precise information about the policy being consulted:

- **Name**: name of the Microsoft update policy being consulted.
- **Targets**: list of targets linked to the Microsoft update policy being consulted.
- **Creation date**: creation date of the Microsoft update policy being consulted.
- **Created by**: user who created the Microsoft update policy being consulted.

The `Edit` button opens a modal window allowing you to change the name of the policy and the `Delete` button discards it.

## Microsoft patches

This tab displays a table listing the Microsoft updates available for the linked target. At the top, there are many filtering options to list available patches by `Classifications`, `Products`, `Superseded`, or `Release Date`. You can also search by character strings or by their status of `Pending Approval`, `Approved`, or `Rejected`.




The user can select each available update one by one and indicate whether they want to approve or reject that patch.

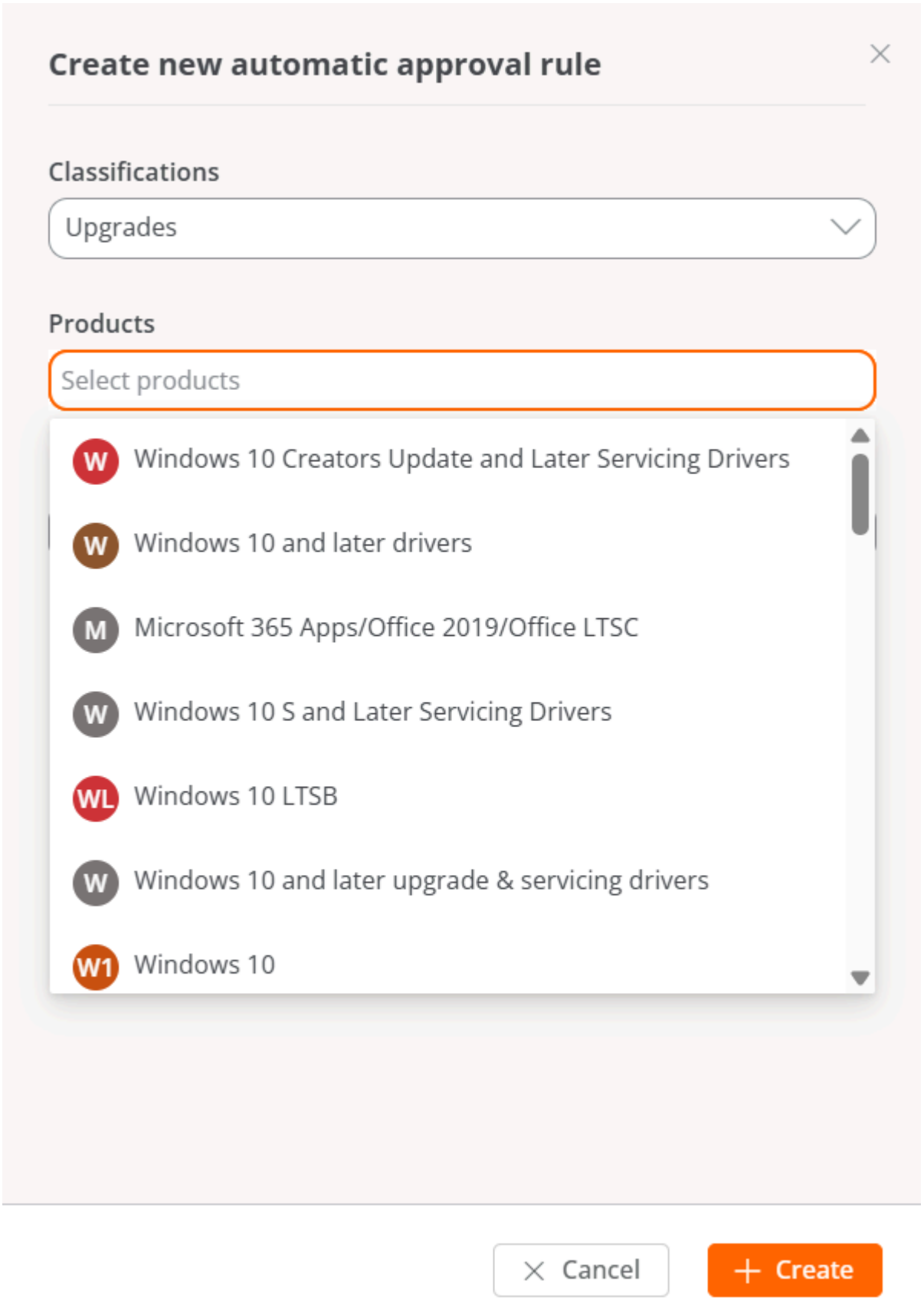
> **INFO**
>
> If a user defines a Microsoft update policy, but does not manually or automatically approve or deny an update package, no patching activity (installation or uninstallation) will be generated on the devices.

## Automatic Approvals

Automatic approval rules can be configured for patching, even more than one within the same update policy.

To create a new rule, click on `New`. Next, a modal window will open asking to define the following information:

- **Classifications**: distinguishes patches according to their category (*Security updates*, *Feature packs*, *Updates*, *Critical updates*, *Drivers*, *Upgrades* and *Definition updates*).
- **Products**: allows selecting the Microsoft product the update applies to.
- **Days after release**: allows specifying how many days after the patch release date it will be automatically approved.



**INFO**

Flexxible recommends setting up automatic patch approval rules whenever a new update policy is created, and not applying the new policy to the desired target until the updates intended as a starting point are approved. In this way, you can start from a scenario where all previous updates are approved for user devices.

# Portal / Settings

From `Settings`, you can access different configuration elements of the selected organization.

From there, you can manage:

- Information
- Users
- Products
- Modules
- Integrations
- Reporting Groups

## Information

It allows you to see the general information of the selected organization: the number of members it comprises, the contracted products, email, the type of company, and more corporate data.

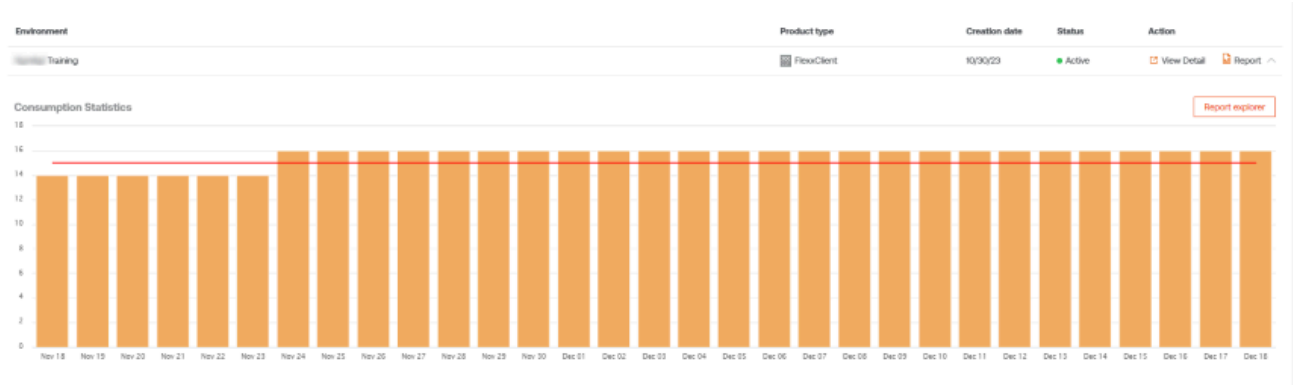
## Users

From there, you can manage the users of an organization and, if applicable, those who depend on it. With the necessary permissions, you can create and modify users, assign them roles, and access levels to Flexxible modules.

More information about user management in User Management.

## Products

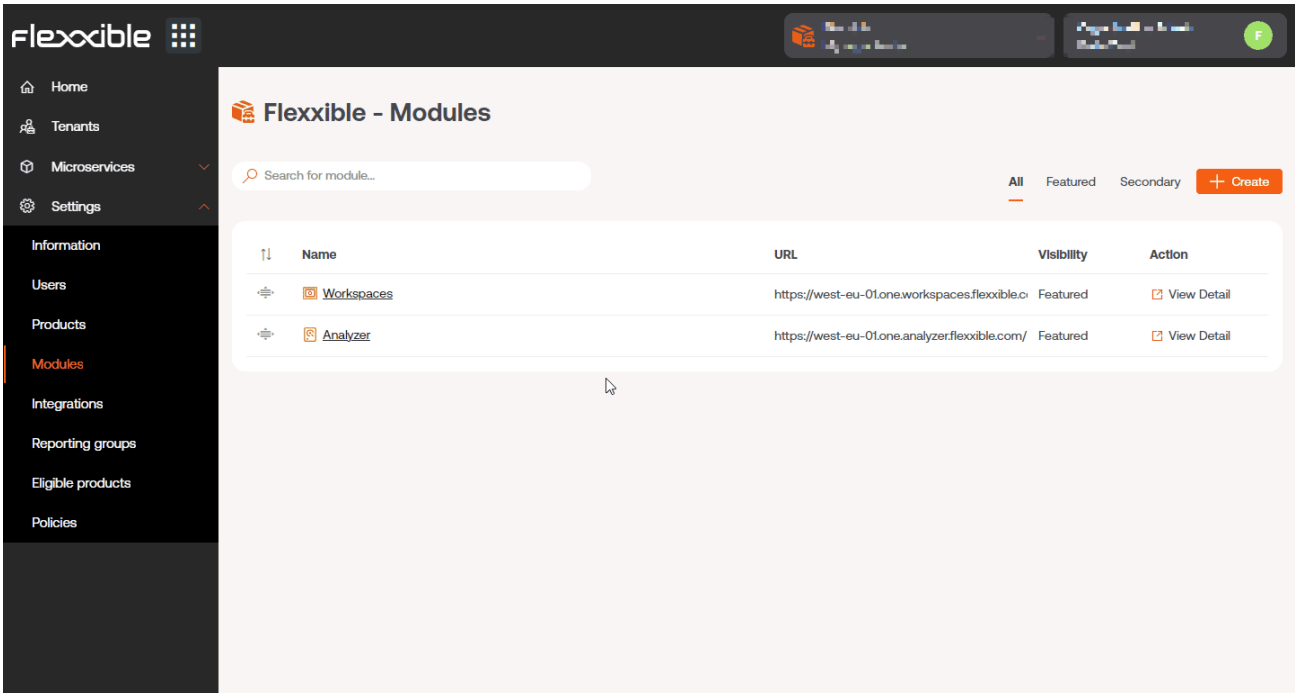
From the `Products` option, you can check the license consumption details by environment.




This section provides information about the contracted products and their associated license keys.

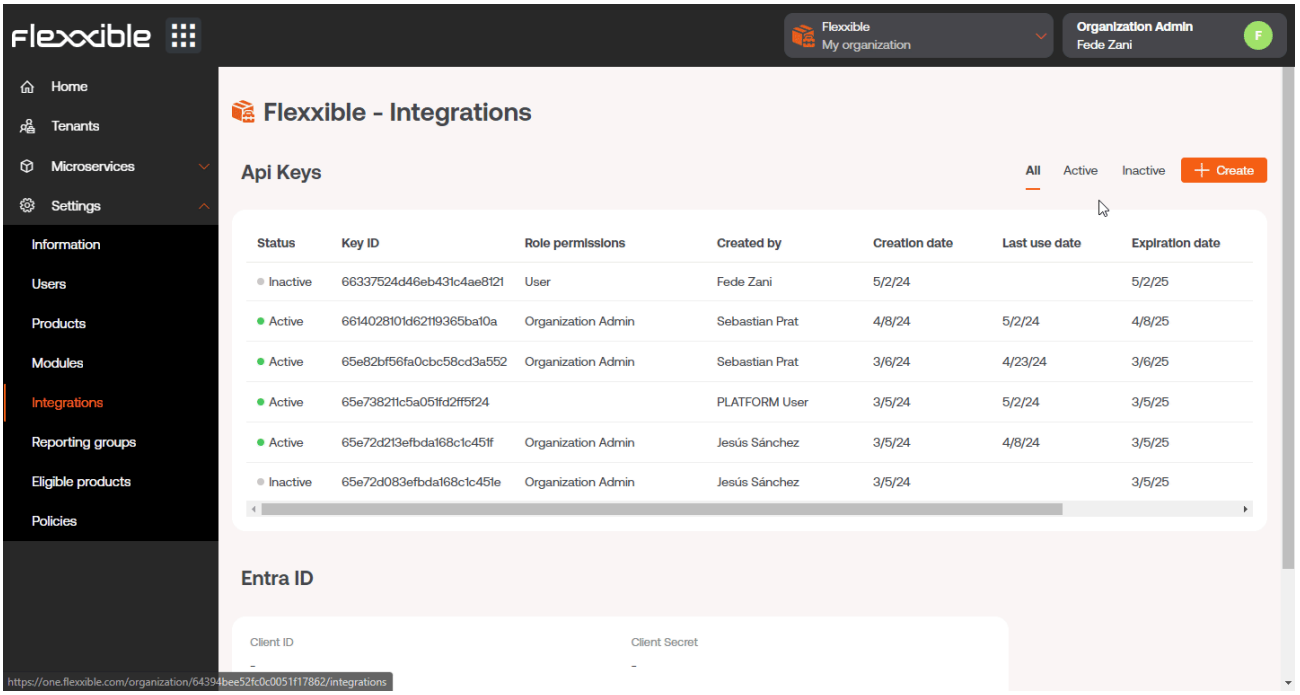
## Modules

In `Modules`, the active modules in Portal are displayed, and shortcuts can be created to other tools easily; this way, the work of the support technicians is facilitated.




## Integrations

You can view the integrations made through the Portal API.

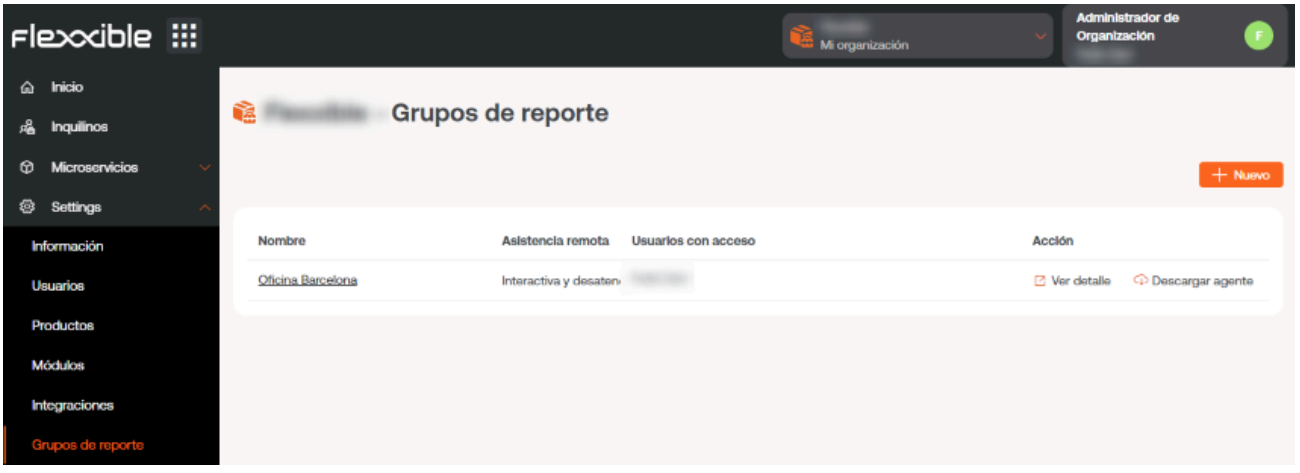



And it's possible to create new keys for the integration.

> Remember that the key will only be visible during the creation of keys.

From here, you can also revoke active API accesses.

# Reporting Groups

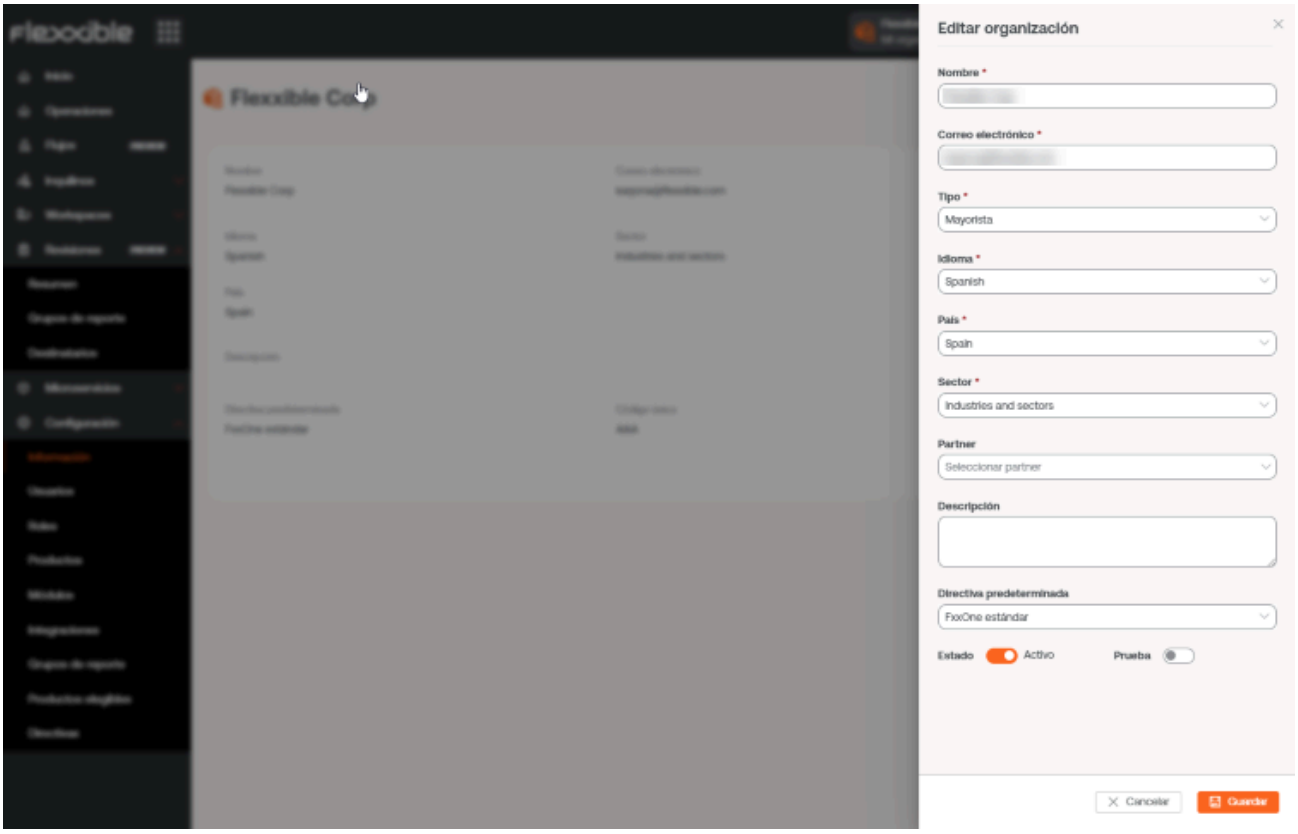



In `Report Groups` it's possible to preconfigure FlexxAgent groups, so they can contain devices from different locations, user groups, or other criteria. It also allows you to enable remote assistance features, as well as set permissions for users to view and manage devices in Workspaces.

# Portal / Settings / Information

This section provides specific data about the organization, such as name, reference email address, industry they belong to, and a description of the company. Additionally, on the right side of the screen, more quantitative data can be observed, such as the number of members composing it and the number of products they have contracted.

The `Edit` button allows you to modify the information of the organization and even its type.




Fields that can be modified:

- Organization name
- Email Address associated with this
- Type: defines the type of organization. It allows, for example, to establish the belonging of multiple `Client` type organizations to a `Partner` type organization (service provider).
- Language: allows configuring a language from the available options.

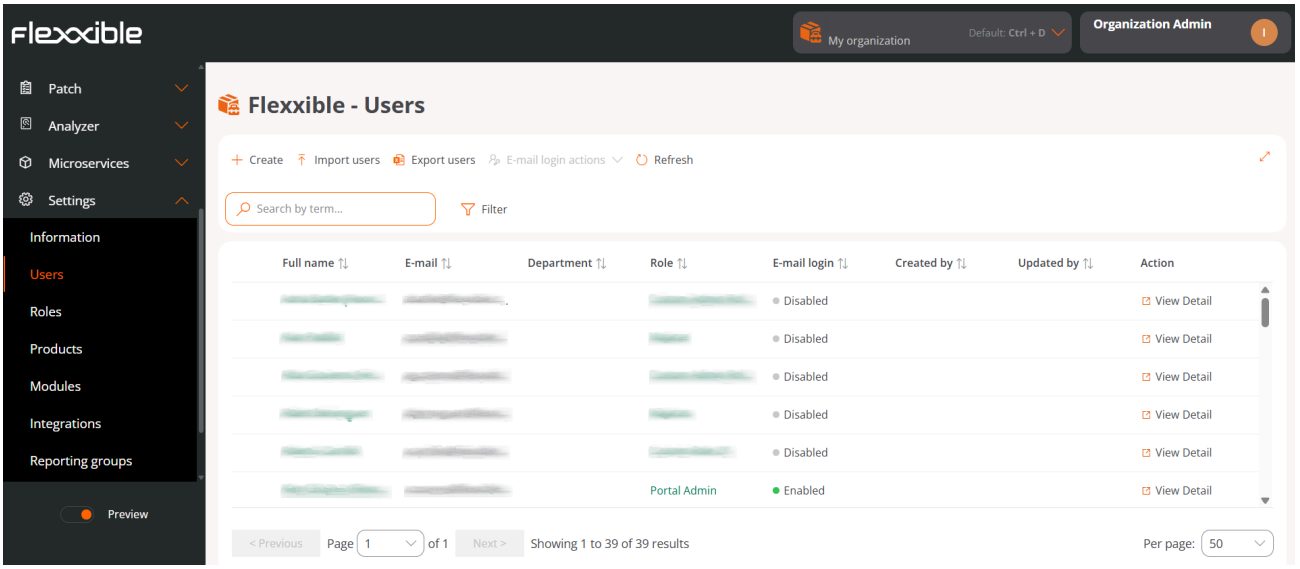
    - Spanish
    - Catalan
    - Basque
    - English
    - Brazilian Portuguese
- Country: allows defining the organization's country.
- Industry: allows defining the organization's industry.
- Partner: for `Client` type organizations, it allows defining or modifying the partner.
- Description: allows including a descriptive text.
- Policy: allows applying a policy.
- Status: allows activating or deactivating the organization.
- Trial: allows including the organization's subscription in the trial period.

# Portal / Settings / Users

From the side menu, in `Settings` -> `Users`, users of an organization can be managed. This section allows you to view, modify, or create users, as well as assign them a role and set a language for their console use.

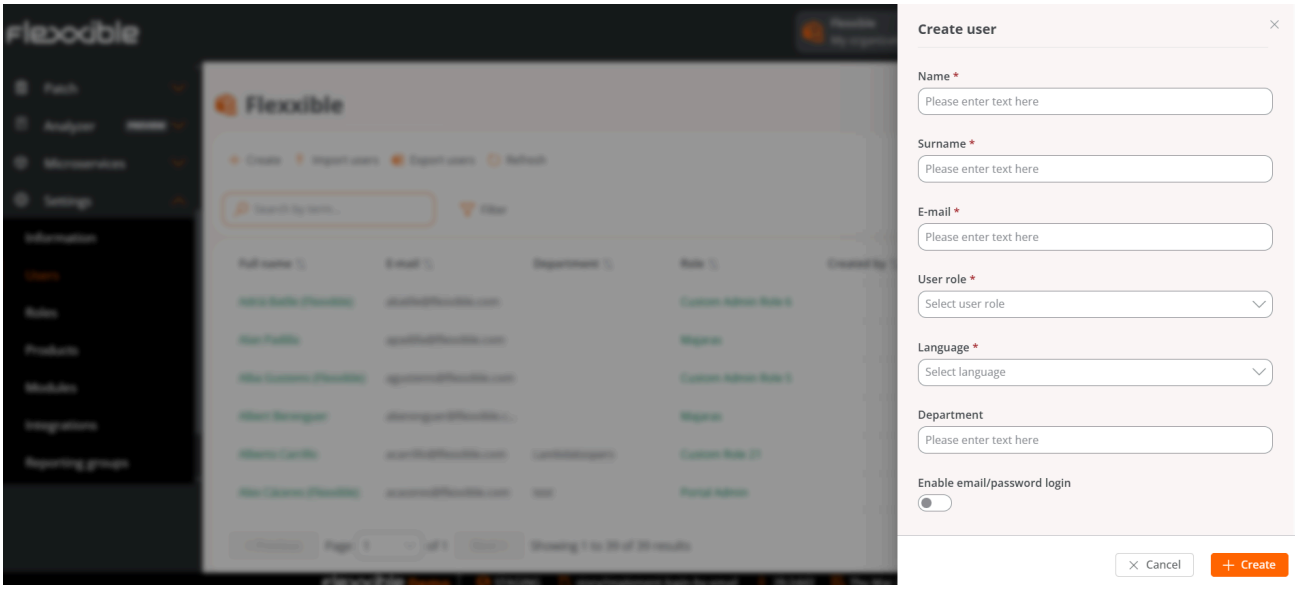
The list view presents a table with all users created for an organization. Each row shows the following data:

- **Full name**: user's first and last name
- **Email**: user's email address
- **Department**: department to which the user belongs within their organization
- **Role**: role type assigned to the user
- **Email login**: indicates if the user has *Enabled* or *Disabled* login to Flexxible consoles via email and password.
- **Created by**: name of the user who created the user whose data is being queried.
- **Updated by**: name and email address of the last user who updated the user information in Portal.
- **View details**: opens a form to edit the user's data and possibly delete it, depending on the assigned role in Portal.



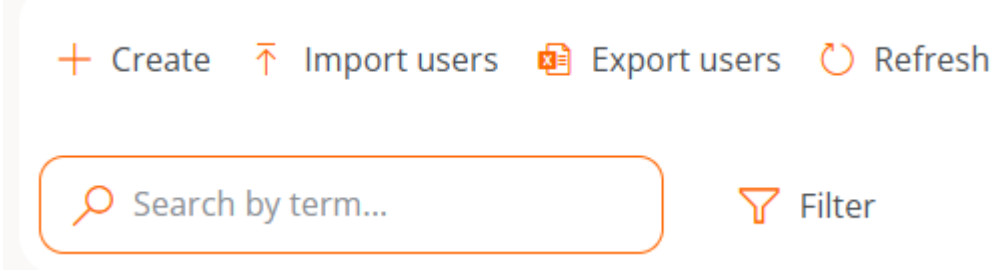
# Create an individual user

In the list view, the `New` button will open a window with a form to fill in the fields with the information of a new user. In addition to the name, surname, and email, you must assign a user role with which they can access the Portal; as well as the language they will use the console in and the department they belong to within the organization.




# Batch creation of users

If you want to add multiple users at once, then you should click `Import users`. This action allows you to select a file from the device. If you want to do a bulk import, Flexxible recommends performing an export first to obtain the Excel file with the proper format. From there you only need to complete it with the required changes, and finally import it.




## User export

To export the user list seen in the list view, just press `Export users`. This action will download an Excel file with the list of organization users and their respective data.

# User Blocking

If an `Organization Administrator` wishes to block a user from accessing Flexxible consoles, they can do so from the user detail view.

In the main table, you must click on a user's name. A modal window will then open with a form that allows you to edit the user's details, displaying a `Block` button. Pressing it will open a pop-up asking you to confirm the user's block.

If you want to unblock a user, simply repeat the process and click on the `Unblock` button.

# Additional options

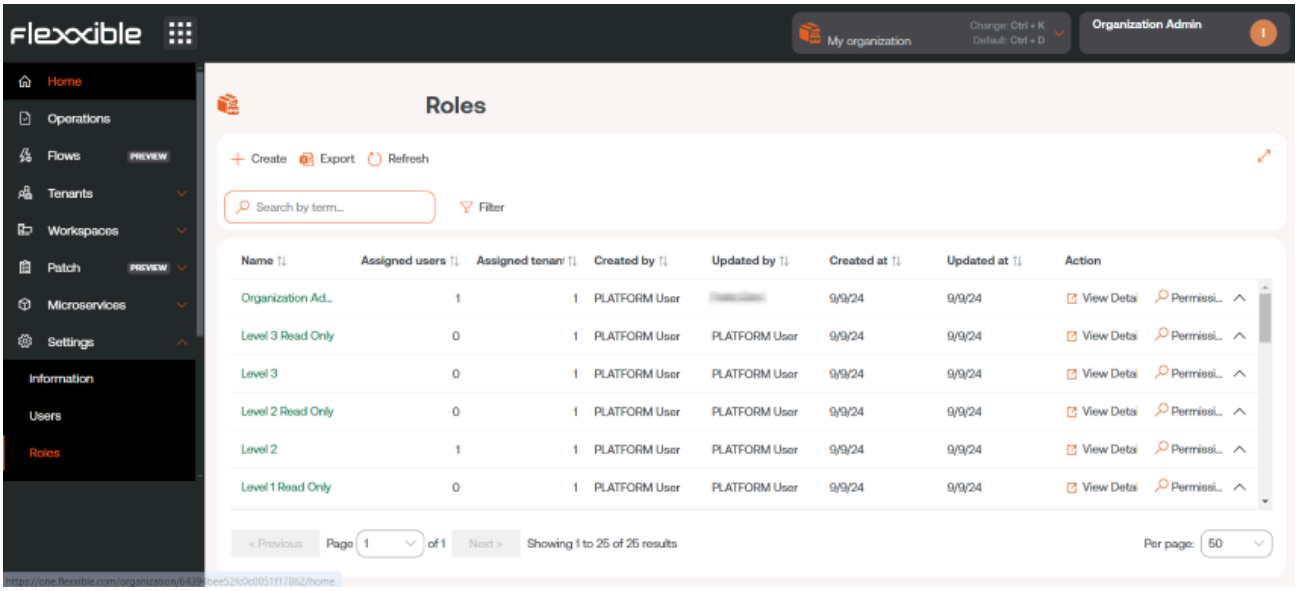
The options menu in the list view also allows `Reload table`, a performance-enhancing option that is very useful when you want to update the user list, especially when new ones have been created or imported from an Excel file.

The `Search by term` field allows more precise searches, just enter words corresponding to any user data to quickly access them.

`Filter` is a more complete alternative to access specific users according to the fields that correspond to their data: full name, email, department, or role.

# Portal / Settings / Roles

Roles allow segmenting access to organizational information or different platform functionalities according to the user who has logged in and the role they have applied. Within the same role, multiple levels of permissions can be assigned in different organizations.




## Create a new role

To create a new role, click on the `New` button. A form will open requesting a name for the new role. Once assigned, it will appear in the roles table.

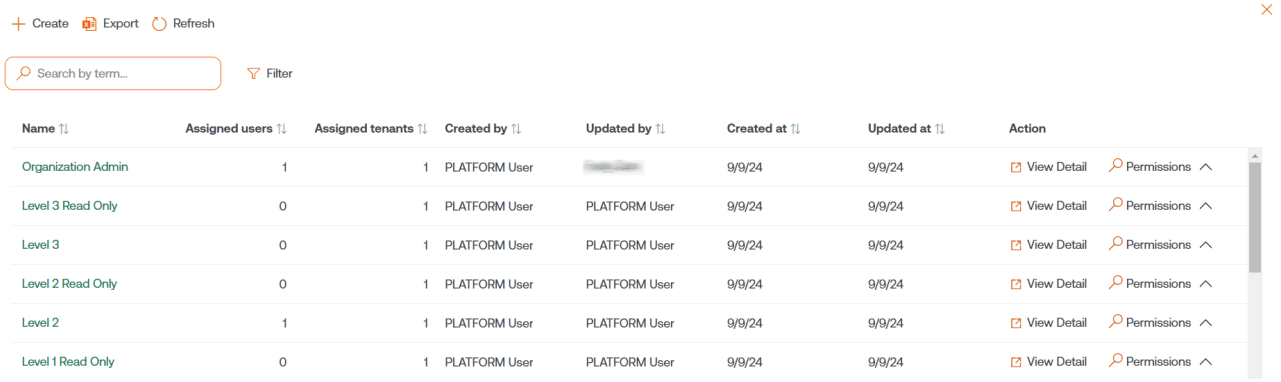
# Roles table

The roles table displays the following information:

- **Name**: name assigned to the role
- **Assigned users**: users who have that role assigned
- **Assigned tenants**: tenants that have been assigned that role
- **Created by**: user who created the role
- **Updated by**: user who updated the role information
- **Created on**: date the role was created
- **Updated on**: date the role was updated
- **Action**: allows access to `View detail` and `Permissions`

# Roles Subtable

If you click on the arrow to the right of `Permissions`, a subtable will unfold from where you can access direct information about the permissions assigned to that role in Portal and in the Workspaces and Analyzer modules, as well as the tenants to which that permission has been assigned.



# Detail view

Clicking on an item in the role table takes you to the detail view, where the following tabs will be displayed:

- Details
- Permissions
- Users

# Details

The `Details` tab contains additional information about the role: name, number of users and tenants assigned to that role, creation and update date, and the user who created it.

At the bottom right, the `Clone` button allows copying and reusing the role. `Edit` gives the option to change the role name.

# Permissions

Through `Permissions` you can view, create, or edit permissions. In this view, you can configure a unique group of permissions for each selectable organization.

The `New` option allows you to create a new permission with the following information:

- All Tenants
- Tenant
- Permissions in Portal
- Permissions in Workspaces
- Permissions in Analyzer
- All reporting groups
- Reporting Groups

## All tenants

It allows you to apply the permissions to all the organizations you have access to. In service provider use cases, it allows you to centrally manage permissions and replicate changes to the client organizations you manage.

When role permissions mix permissions applied at the "All tenants" level and specific configurations for an organization, which may be different, the more specific permission wins. In this way, a default configuration can be made for all organizations and overwrite those that require modifications.

## Tenant

Allows informing the organization to which permissions are being granted in the role being edited; the `All tenants` check allows configuring the role's permissions to apply to all organizations that can be accessed.

## Portal Permissions

It allows you to select access level to Portal at different levels:

- No access
- User
- L1 Support Team
- L1 Support Team Read Only.
- L2 Support Team
- L2 Support Team Read Only
- L3 Engineering Team
- L3 Engineering Team Read Only
- Organization Admin
- Organization Admin Read Only

Details of the visibility and allowed operations at each level can be found in Additional Considerations

## Workspaces permissions

In `Workspaces`, there are four roles with different levels of access available:

- Level 1
- Level 1 read-only
- Level 2
- Level 2 read-only

Details of the visibility and allowed operations at each level can be found in Additional Considerations

## Analyzer permissions

Gives the option to allow or deny access to Analyzer.

## All reporting groups

It allows you to apply permissions to all reporting groups you have access to. In service provider use cases, it allows you to centrally manage permissions and replicate changes to the client organizations you manage.

## Reporting Groups

It allows you to apply permissions to specified reporting groups; it can be more than one.

# Users

This table allows you to see the users assigned to the role and provides the option to search.

# Portal / Settings / Roles / Roles included by default

The settings of the default roles affect all report groups of **only** the current organization. If the organization is of partner type and has client-type organizations below, or is client type and has sub-organizations below, they should be included as a new record in the `Permissions` tab in two formats:

- All tenants: allows you to set a unified level of access and visibility for all organizations dependent on the root organization.
- Individually: allows you to set different levels of access and visibility for each organization

Default included roles:

- Level 1
- Level 1 Read Only
- Level 2
- Level 2 Read Only
- Organization admin

> This role setting only affects the current organization. It is possible to assign more organizations with different permission levels in the `Permissions` tab of the same role in edit mode.

## Level 1

Users with the `Level 1` role assigned will have the following accesses for their organization:

- Portal: User
- Workspaces: Level 1
- Analyzer: No access

This role allows the most common support actions in `Workspaces`, such as providing remote assistance, sending microservices, energy actions or consulting device information. It does not enable access to Analyzer and allows the user to consult information without modifying it in Portal.

## Level 1 Read Only

Users with the `Level 1 Read Only` role assigned will have the following accesses for their organization:

- Portal: User
- Workspaces: Level 1 Read Only
- Analyzer: No access

This role is identical to `Level 1`, but also restricts access to `Workspaces` to view-only, allowing information to be consulted in `Read Only` mode without the possibility of performing support or modification actions.

## Level 2

Users with the `Level 2` role assigned will have the following accesses for their organization:

- Portal: User
- Workspaces: Level 2
- Analyzer: Access

This role allows access to `Workspaces` with `Level 2`, which includes all the support functionalities of `Level 1` plus `Level 2` functionalities, including server management, networks, locations, WiFi networks, and alert configuration. Allows access to `Portal` as a user and also to `Analyzer` to consult information about application or device inventory, as well as user experience, carbon footprint, and more.

## Level 2 Read Only

Users with the `Level 2 Read Only` role assigned will have the following accesses for their organization:

- Portal: User
- Workspaces: Level 2 Read Only
- Analyzer: No access

This role is identical to `Level 2`, but also restricts access to `Workspaces` to view-only, allowing information to be consulted in `Read Only` mode without the possibility of performing support or modification actions.

## Organization admin

Users with the `Organization admin` role assigned will have the following accesses for their organization:

- Portal: Organization admin
- Workspaces: Level 2
- Analyzer: Access

This level is the highest level of access that can be granted to a user. It allows full visibility in `Analyzer`, all `Level 2` actions in `Workspaces` and the ability to modify organization properties in `Portal`, including the creation and activation of `Microservices` or `Flows`, `Patch Policies` and more.

# Portal / Settings / Roles / Additional considerations

Roles allow grouping different levels of access for several organizations and, at the same time, allow grouping different levels of access by module to manage them in a simplified way.

## Multiclient environments

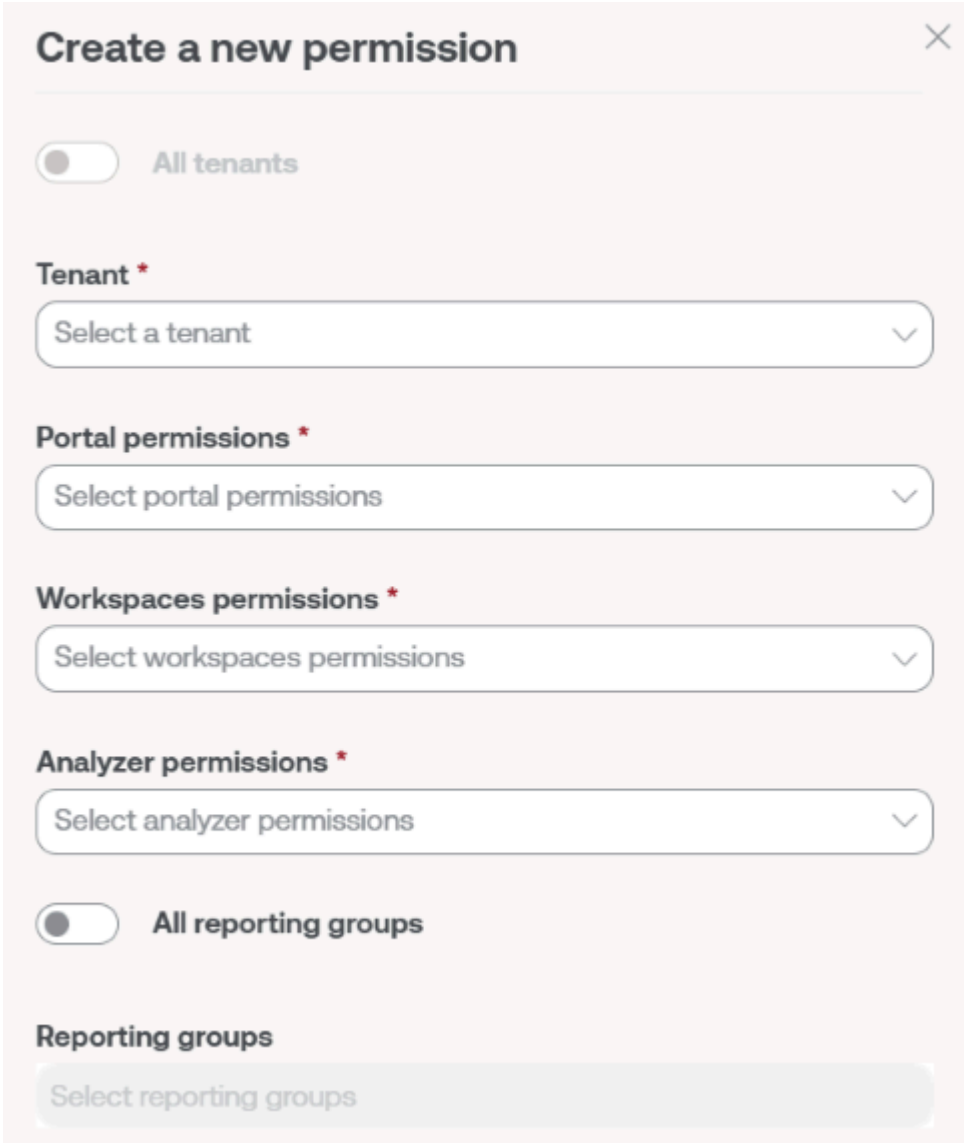
The roles of an organization allow configuring access and visibility for the users of the organization, and also allow including the permissions to configure access and visibility to dependent organizations.

An organization is dependent when:

- It is client type and the roles and users are in the partner organization at a higher level.
- It is a sub-organization of a client organization.

Roles are assigned to users and contain the definition of levels of access and visibility, being able to establish different configurations for the root organization and its sub-organizations in the same role. This can only be done in a descending manner; that is, from a higher-level organization, permissions can be assigned to the organization itself and the organizations that depend on it.

# Levels of access by modules




The levels of access are also defined for each module of the solution:

- Portal
- Workspaces
- Analyzer

## Portal

In `Portal` the following roles exist:

0. No access
1. Organization Administrator or `1` in the table below

2. Read-only organization administrator or `2` in the table below
3. User or `3` in the table below
4. L1 support team or `4` in the table below
5. L1 support team read-only or `5` in the table below
6. L2 support team or `6` in the table below
7. L2 support team read-only or `7` in the table below
8. L3 Engineering Team or `8` in the table below
9. L3 Engineering Team Read Only or `9` in the table below
10. Billing or `10` in the table below

To access certain functionalities, in addition to access permissions in Portal, access to Workspaces is required, depending on the functionality, with role `Level 1` or `Level 2`.

These roles by levels allow configuring visibility and segmented accesses according to the needs of each organization, the detail of the visibility and actions available for each level of access to Portal is defined in the table below:

| Section | Functionality | Action | 1 | 2 | 3 | 4 | 5 | 6 | |
|---|---|---|---|---|---|---|---|---|---|
| Home | | Read | ✅ | ✅ | ✅ | ✅ | ✅ | ✅ | |
| Operations | | Read | ✅ | ✅ | ⭐ | ✅ | ✅ | ✅ | |
| Flows | | Read | ✅ | ✅ | ⭐ | ❌ | ❌ | ❌ | |
| | | Create | ✅ | ❌ | ⭐⭐ | ❌ | ❌ | ❌ | |
| | | Refresh | ✅ | ❌ | ⭐⭐ | ❌ | ❌ | ❌ | |
| | | Delete | ✅ | ❌ | ⭐⭐ | ❌ | ❌ | ❌ | |
| Reports | List | Read | ✅ | ✅ | ❌ | ✅ | ✅ | ✅ | |
| | Detail | Read | ✅ | ✅ | ❌ | ✅ | ✅ | ✅ | |

| Section | Functionality | Action | 1 | 2 | 3 | 4 | 5 | 6 | |
|---|---|---|---|---|---|---|---|---|---|
| | | Create | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| | | Delete | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| Tenants | | Create | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| | | Read | ✅ | ✅ | ❌ | ❌ | ❌ | ❌ | |
| | | Refresh | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| | | Delete | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| | Activation | Read | ✅ | ✅ | ❌ | ❌ | ❌ | ❌ | |
| Monitor | Active alerts | Read | ✅ | ✅ | ✅ | ✅ | ✅ | ✅ | |
| | Alert Configuration | Create | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| | | Read | ✅ | ✅ | ✅ | ❌ | ❌ | ❌ | |
| | | Refresh | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| | | Delete | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| Workspaces | | Read | ✅ | ✅ | ⭐ | ✅ | ✅ | ✅ | |
| | | Refresh | ✅ | ❌ | ✅ | ✅ | ❌ | ✅ | |
| | Groups | Read | ✅ | ✅ | ✅ | ✅ | ✅ | ✅ | |
| | | Create | ✅ | ❌ | ⭐ | ❌ | ❌ | ✅ | |

| Section | Functionality | Action | 1 | 2 | 3 | 4 | 5 | 6 | |
|---|---|---|---|---|---|---|---|---|---|
| | | Refresh | ✅ | ❌ | ❌ | ❌ | ❌ | ✅ | |
| | | Delete | ✅ | ❌ | ❌ | ❌ | ❌ | ✅ | |
| Updates | | Read | ✅ | ✅ | ⭐ | ❌ | ❌ | ❌ | |
| | | Create | ✅ | ❌ | ⭐⭐ | ❌ | ❌ | ❌ | |
| | | Refresh | ✅ | ❌ | ⭐⭐ | ❌ | ❌ | ❌ | |
| | | Delete | ✅ | ❌ | ⭐⭐ | ❌ | ❌ | ❌ | |
| Analyzer | Installed apps | Read | ✅ | ✅ | ✅ | ❌ | ❌ | ✅ | |
| | | Refresh | ✅ | ❌ | ✅ | ❌ | ❌ | ✅ | |
| Analyzer | Licenses | Read | ✅ | ✅ | ❌ | ❌ | ❌ | ✅ | |
| | | Create | ✅ | ❌ | ❌ | ❌ | ❌ | ✅ | |
| | | Refresh | ✅ | ❌ | ❌ | ❌ | ❌ | ✅ | |
| | | Delete | ✅ | ❌ | ❌ | ❌ | ❌ | ✅ | |
| SAM | | Read | ✅ | ✅ | ❌ | ❌ | ❌ | ✅ | |
| Microservices | | Create | ✅ | ❌ | ❌ | ❌ | ❌ | ✅ | |
| | | Read | ✅ | ✅ | ✅ | ❌ | ❌ | ✅ | |
| | | Refresh | ✅ | ❌ | ❌ | ❌ | ❌ | ✅ | |

| Section | Functionality | Action | 1 | 2 | 3 | 4 | 5 | 6 | |
|---|---|---|---|---|---|---|---|---|---|
| | Enabled | Read | ✅ | ✅ | ✅ | ❌ | ❌ | ✅ | |
| | | Refresh | ✅ | ❌ | ❌ | ❌ | ❌ | ✅ | |
| Billing | | Read | ✅ | ✅ | ❌ | ❌ | ❌ | ❌ | |
| | | Refresh | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| Product | | Read | ✅ | ✅ | ❌ | ❌ | ❌ | ❌ | |
| | Report | Read | ✅ | ✅ | ✅ | ❌ | ❌ | ❌ | |
| | Environment | Read | ✅ | ✅ | ✅ | ❌ | ❌ | ❌ | |
| | | Refresh | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| | Agent Settings | Read | ✅ | ✅ | ❌ | ❌ | ❌ | ❌ | |
| | | Refresh | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| Integrations | | Create | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| | | Read | ✅ | ✅ | ❌ | ❌ | ❌ | ❌ | |
| | | Refresh | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| Modules | | Create | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| | | Read | ✅ | ✅ | ❌ | ❌ | ❌ | ❌ | |
| | | Refresh | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |

| Section | Functionality | Action | 1 | 2 | 3 | 4 | 5 | 6 | |
|---|---|---|---|---|---|---|---|---|---|
| Information | | Read | ✅ | ✅ | ✅ | ❌ | ❌ | ❌ | |
| | | Refresh | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| Directives | | Create | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| | | Read | ✅ | ✅ | ✅ | ❌ | ❌ | ❌ | |
| | | Refresh | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| | | Delete | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| Reporting Groups | | Create | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| | | Read | ✅ | ✅ | ❌ | ❌ | ❌ | ❌ | |
| | | Refresh | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| | | Delete | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| | Agent Settings | Read | ✅ | ✅ | ❌ | ❌ | ❌ | ❌ | |
| | | Refresh | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| | Auto update settings | Refresh | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| | Magic link | Create | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| | | Read | ✅ | ✅ | ❌ | ❌ | ❌ | ❌ | |

| Section | Functionality | Action | 1 | 2 | 3 | 4 | 5 | 6 | |
|---|---|---|---|---|---|---|---|---|---|
| | | Refresh | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| Roles | | Create | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| | | Read | ✅ | ✅ | ❌ | ❌ | ❌ | ✅ | |
| | | Refresh | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| | | Delete | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| Users | | Create | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| | | Read | ✅ | ✅ | ❌ | ❌ | ❌ | ✅ | |
| | | Refresh | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |
| | | Delete | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ | |

**INFO**

- ✅ Has access.
- ⭐ Has access if additionally has L1 in Workspaces.
- ⭐⭐ Has access if additionally has L2 in Workspaces.
- ❌ No access.

## Access Levels for Microservices

In microservices, the same roles are maintained as in Portal, but with specific access levels:

#### Microservices

The user's role corresponds to the organization where the microservice was created.

| Action | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| Clone / create | ✅ | ❌ | ❌ | ❌ | ❌ | ✅ | ❌ | ✅ | ❌ | ❌ |
| View | ✅ | ✅ | 🔑 | ❌ | ❌ | ✅ | ✅ | ✅ | ✅ | ❌ |
| Edit | ✅ | ❌ | 💡 | ❌ | ❌ | ✅ | ❌ | ✅ | ❌ | ❌ |
| Change to public or private | ❌ | ❌ | ❌ | ❌ | ❌ | ❌ | ❌ | ❌ | ❌ | ❌ |
| Edit visibility when private | ✅ | ❌ | 💡 | ❌ | ❌ | ✅ | ❌ | ✅ | ❌ | ❌ |

**INFO**

- ✅ Has access.
- 🔑 Access is granted if additionally has L1 read-only access in Workspaces.
- 💡 Access is granted if the author of the microservice.
- ❌ No access.

**Enabled microservices**

The user's role corresponds to the organization where the microservice was enabled or disabled.

| Action | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| Enable | ✅ | ❌ | ❌ | ❌ | ❌ | ✅ | ❌ | ✅ | ❌ | ❌ |
| Disable | ✅ | ❌ | ❌ | ❌ | ❌ | ✅ | ❌ | ✅ | ❌ | ❌ |
| Edit | ✅ | ❌ | ❌ | ❌ | ❌ | ✅ | ❌ | ✅ | ❌ | ❌ |

INFO

- ✅ Has access.
- ❌ No access.

## Workspaces

In `Workspaces`, there are four roles with different levels of access available:

- Level 1 or `L1` in the table below
- Level 1 read-only or `L1 RO` in the table below
- Level 2 or `L2` in the table below
- Level 2 read-only or `L2 RO` in the table below

Available actions by each role:

| Functionality | Action | L1 | L1 RO | L2 | L2 RO |
|---|---|---|---|---|---|
| UX Panel | View | ✅ | ✅ | ✅ | ✅ |
| Workspaces | View | ✅ | ✅ | ✅ | ✅ |
| Workspaces | Execute operations | ✅ | ❌ | ✅ | ❌ |
| Sessions | View | ✅ | ✅ | ✅ | ✅ |
| Sessions | Execute operations | ✅ | ❌ | ✅ | ❌ |
| Connection Logs | View | ✅ | ✅ | ✅ | ✅ |
| Jobs | View | ✅ | ✅ | ✅ | ✅ |
| Jobs | Cancel | ✅ | ❌ | ✅ | ❌ |

| Functionality | Action | L1 | L1 RO | L2 | L2 RO |
|---|---|---|---|---|---|
| Alert | View | ✅ | ✅ | ✅ | ✅ |
| Alert | Off | ✅ | ❌ | ✅ | ❌ |
| Profile Storage | View | ✅ | ✅ | ✅ | ✅ |
| Profile Storage | Modify | ✅ | ❌ | ✅ | ❌ |
| Profile Storage | Delete | ✅ | ❌ | ✅ | ❌ |
| Alert notification profiles | View | ❌ | ❌ | ✅ | ✅ |
| Alert notification profiles | Modify | ❌ | ❌ | ✅ | ❌ |
| Alert notification profiles | Delete | ❌ | ❌ | ✅ | ❌ |
| Alert Subscriptions | View | ❌ | ❌ | ✅ | ✅ |
| Alert Subscriptions | Modify | ❌ | ❌ | ✅ | ❌ |
| Alert Subscriptions | Delete | ❌ | ❌ | ✅ | ❌ |
| Event Logs | View | ❌ | ❌ | ✅ | ✅ |
| Event Logs | Modify | ❌ | ❌ | ✅ | ❌ |
| Event Logs | Delete | ❌ | ❌ | ✅ | ❌ |
| Locations | View | ❌ | ❌ | ✅ | ✅ |
| Locations | Create | ❌ | ❌ | ✅ | ❌ |
| Locations | Modify | ❌ | ❌ | ✅ | ❌ |

| Functionality | Action | L1 | L1 RO | L2 | L2 RO |
|---|---|---|---|---|---|
| Networks | View | ❌ | ❌ | ✅ | ✅ |
| Networks | Modify | ❌ | ❌ | ✅ | ❌ |
| Notifications | View | ❌ | ❌ | ✅ | ✅ |
| Notifications | Create | ❌ | ❌ | ✅ | ❌ |
| Notifications | Modify | ❌ | ❌ | ✅ | ❌ |
| Notifications | Delete | ❌ | ❌ | ✅ | ❌ |
| Reporting Groups | View | ❌ | ❌ | ✅ | ✅ |
| Servers | View | ❌ | ❌ | ✅ | ✅ |
| Servers | Execute operations | ❌ | ❌ | ✅ | ❌ |
| Wireless networks | View | ❌ | ❌ | ✅ | ✅ |
| Wireless networks | Modify | ❌ | ❌ | ✅ | ❌ |

**INFO**

- ✅ Has access.
- ❌ No access.

## Analyzer

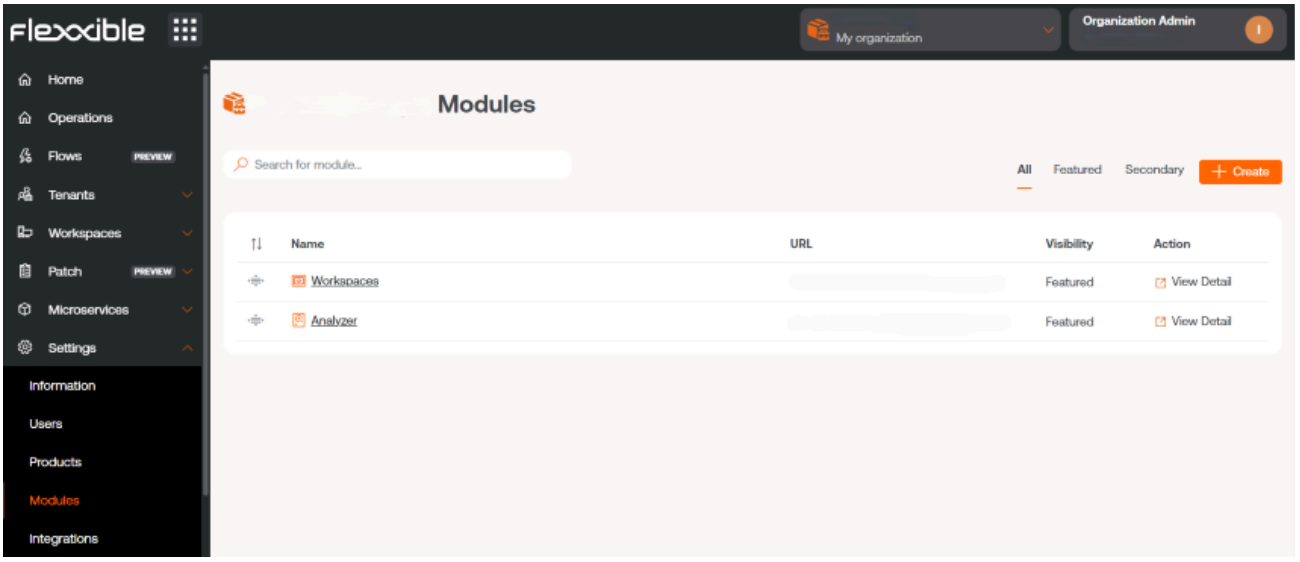
Since `Analyzer` presents information and never allows modifications to the organization or its devices, it does not segment access to the functionalities it contains, therefore access is either granted or denied to users.

Therefore, the access options to `Analyzer` are:

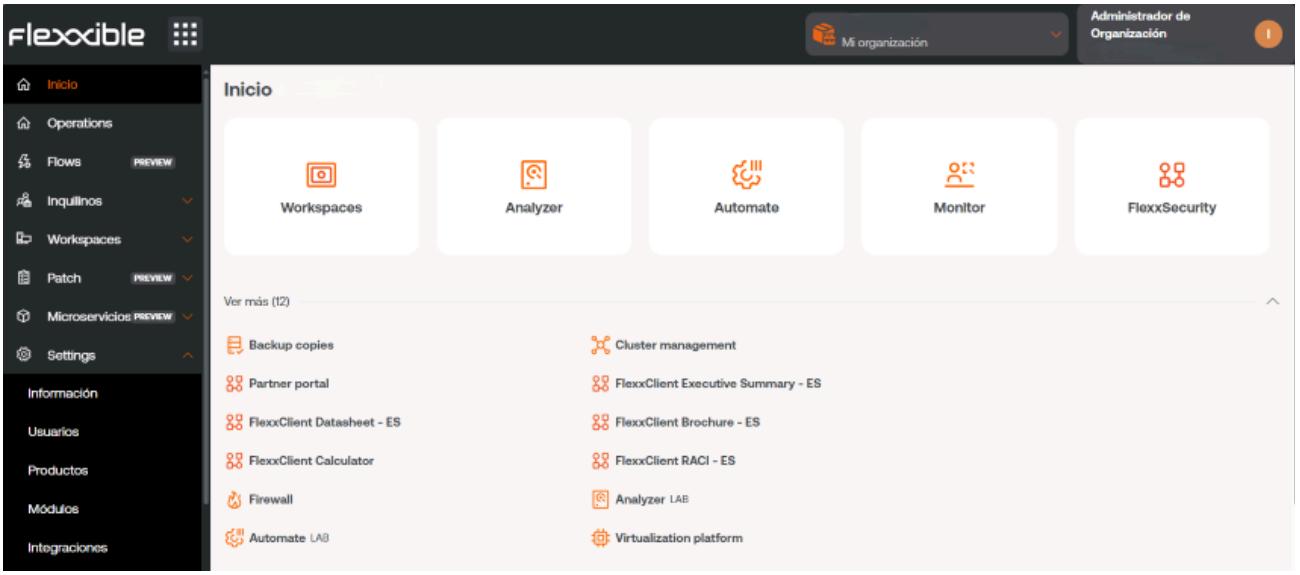
- Access
- No access

# Portal / Settings / Modules

This option shows a list of the available Flexxible product modules for the organization; it details their names, the corresponding URL, and their visibility status. And from the top of the overview, it is possible to perform a search to facilitate its configuration.

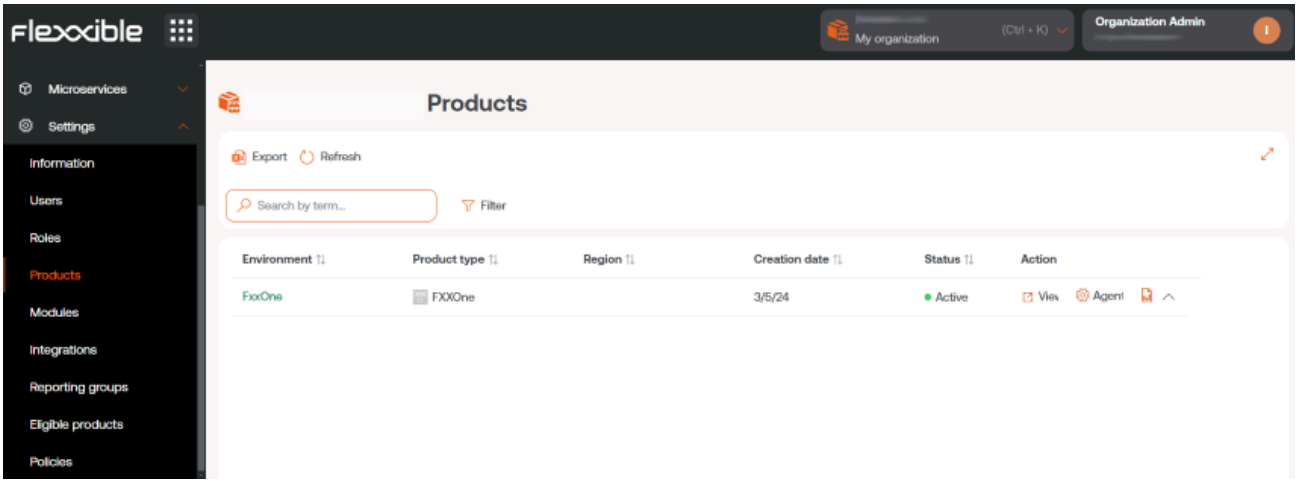



From `View Details`, you can assign a label to the chosen module and define if it is visible as featured or secondary. When it is highlighted, it appears among the top five modules of the `Home` section of `Portal`, standing out by the size of the icon, and when it is secondary it also appears in `Portal` but as a list, under the `View more` button.



# Portal / Settings / Products

This section provides information about the Flexxible environments and products that the organization has. The list view shows data such as the name of the environment in which the product has been deployed, the type of product available, region, creation date within the organization, and its status; the `Actions` field allows you to view and edit its specific data.




## Action's

In the list view table, the `Actions` field shows three buttons to access more precise information and edit the product's behavior: `View details`, `FlexxAgent Configuration`, and `Reporting`.

### View details

This option allows editing the data of each product that the organization has: the environment in which it has been deployed, the license key, its creation date in the organization, and also its status, which can be active or inactive.

### FlexxAgent Settings - Proxy

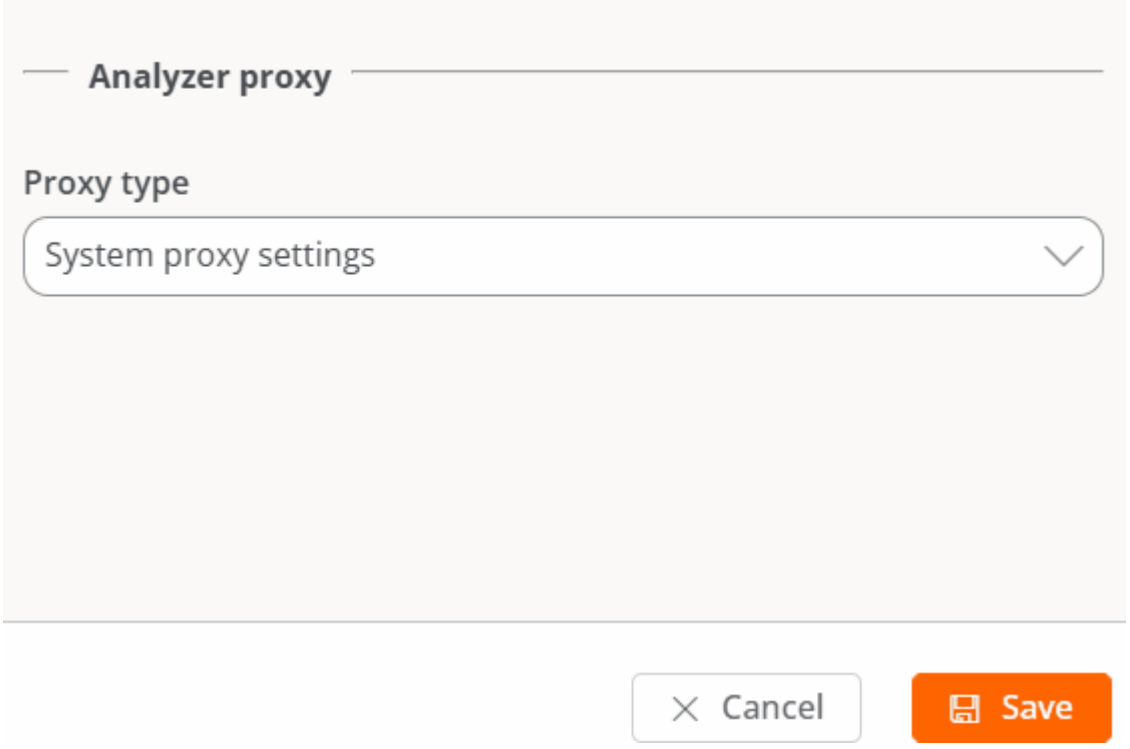
FlexxAgent consists of a Windows service called FlexxAgent Service, which manages two processes: *FlexxAgent*, which runs at the system level, and *FlexxAgent Analyzer*, which

starts for each user session.

The proxy settings for *FlexxAgent Analyzer* are not always the same as those for *FlexxAgent*, so depending on how the proxy operates in each environment, it will be necessary to set its adjustments appropriately.

In the FlexxAgent settings, a user with `Organization Administrator` level access can find two configuration options for the *FlexxAgent* process:

- **System proxy settings**
  - *FlexxAgent Analyzer* automatically detects and uses the proxy settings.
  - Flexxible recommends this configuration for the system proxy.
- **FlexxAgent detected config**
  - In this case, FlexxAgent uses the credentials found in the registry if they are defined during installation.
  - If not configured, FlexxAgent automatically detects the proxy settings.
  - *FlexxAgent Analyzer* uses the detected settings for the Uniform Resource Identifier (URI), user, and password.

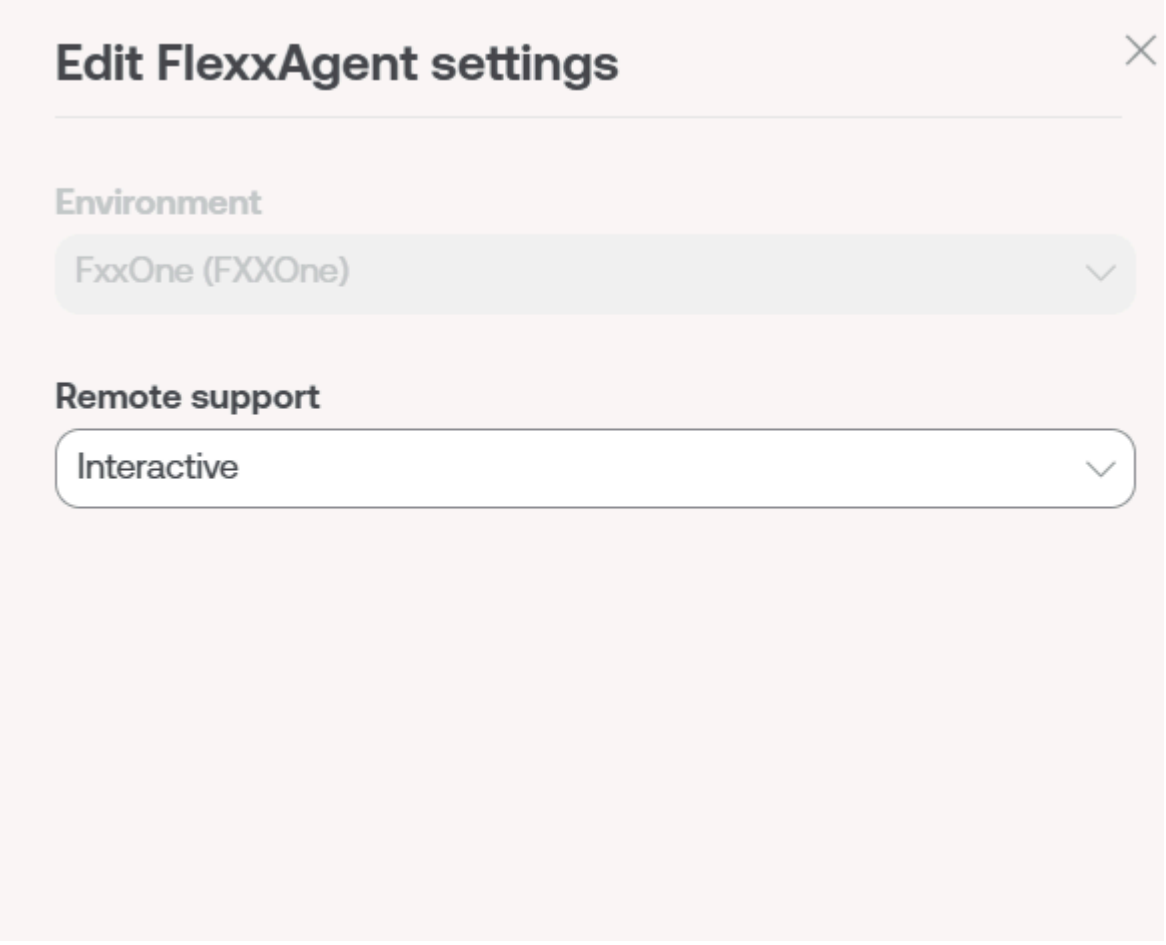


The configuration of `Analyzer proxy` is done from `Portal` -> `Products` -> `Action` -> `FlexxAgent Configuration`.

## FlexxAgent Settings - Remote Assistance

A user with `Organization Administrator` level access in Portal can choose what type of remote assistance the organization will use globally. It can be configured to be interactive, unattended, dynamic, or to have no access at all.

Each reporting group that the organization has can edit its own remote assistance configuration to suit its needs.

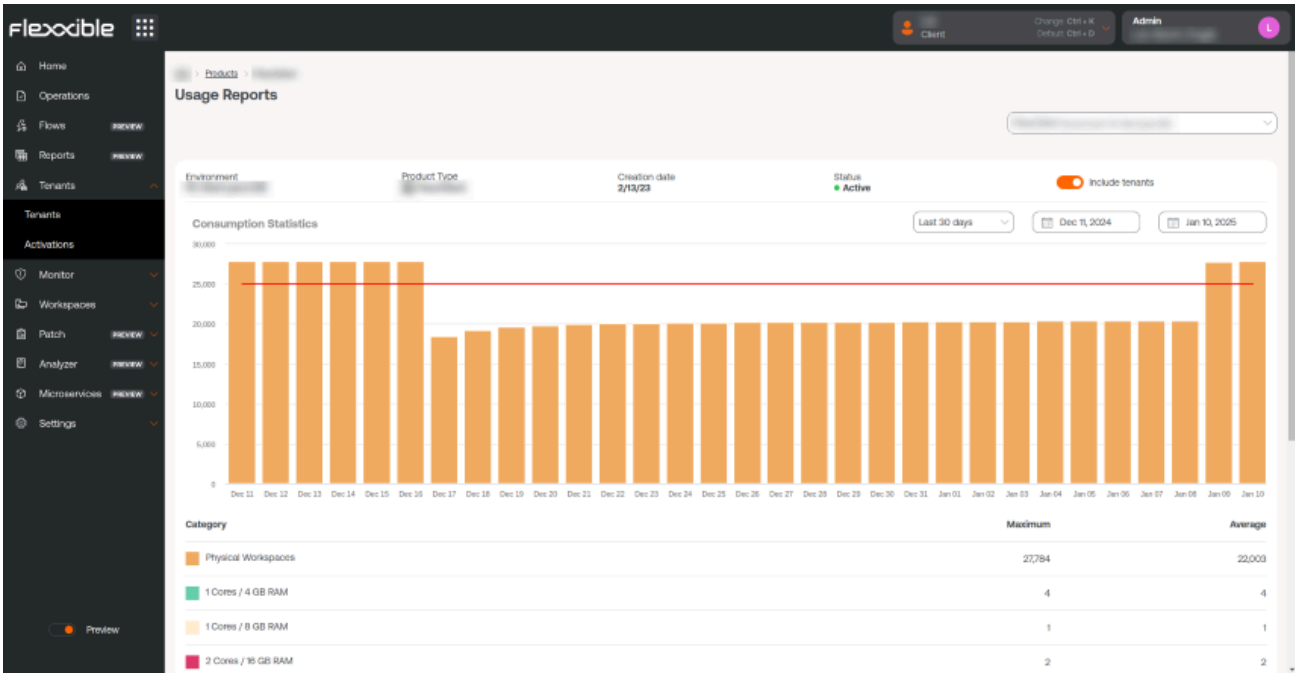



## Reporting

`Reporting` shows the product's consumption statistics over the past month. By clicking on `Report Explorer`, you can access the product usage reports by environment over

longer periods: *Last 30 days*, *Current month*, and *Last 3 months*. Specific dates can also be selected using the calendar options.

For organizations segmented into sub-organizations, it is possible to add all the information from the parent organization plus all its sub-organizations by activating the `Include Tenants` selector at the top right of the screen.



# Portal / Settings / Integrations

From this section, it is possible to register the integration of Portal with services available to organizations on external platforms, to facilitate the management of tasks on devices, visualize unified information, or perform actions.

## Integration with Entra ID

Portal's integration with Entra ID allows treating an organization's devices as another group in `Workspaces`; in this way, in addition to the dynamic and static `Workspaces Groups` that an organization could have, Entra ID Workspaces Groups would be generated.

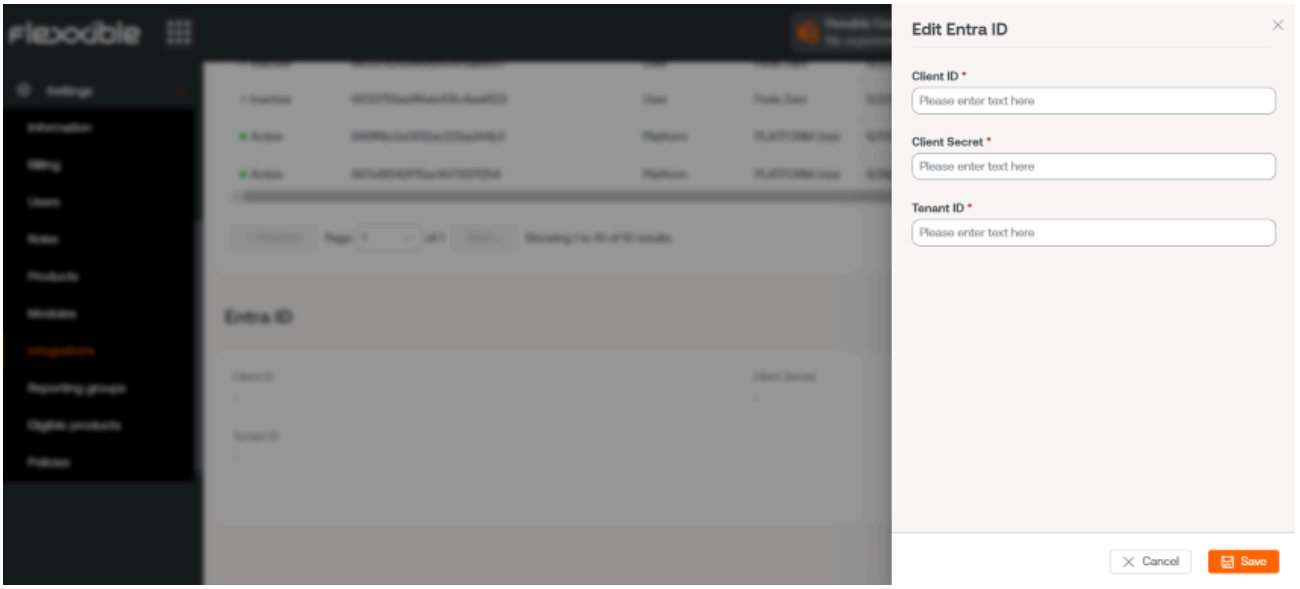
The integration does not imply that those groups will exist in `Portal`, but at the moment when an action is desired on them in `Workspaces`, Portal will show the list of devices that comprise them to make a decision.

### Register a new integration with Entra ID

1. To create an API connection between Portal and Entra ID, the organization must create an application registration in Azure.
2. Go to `Portal` -> `Integrations` -> `Entra ID`.
3. Click on `Edit` and enter the following information:

- **Client ID**: client identification. This can be obtained from the Azure registration panel.
- **Client Secret**: client secret (key) used for authentication. This can be obtained from the Azure registration panel.
- **Tenant ID**: this is the ID of the Azure tenant. You can obtain it here.

4. Click on `Save`.
5. Click on `Check` to verify that the integration has been registered correctly.




# Integration with Intel vPro® Enterprise

Intel vPro® is a set of hardware and firmware technologies designed to enhance the security, manageability, and productivity of business computers. The integration of Flexxible Odin with Intel vPro® Enterprise will allow you to perform useful additional manageability operations on the physical Windows workspaces that provide support to Intel AMT® technology.

From the `Workspaces` view in `Portal`, you can check information about the hardware and status of devices, and additional operations including out-of-band actions will be made available.

## Requirements

To benefit from the Intel vPro® Enterprise integration, devices must meet the following requirements:

#### Supported operating systems

Devices must have Windows 10 and Windows 11, 64-bit, installed.

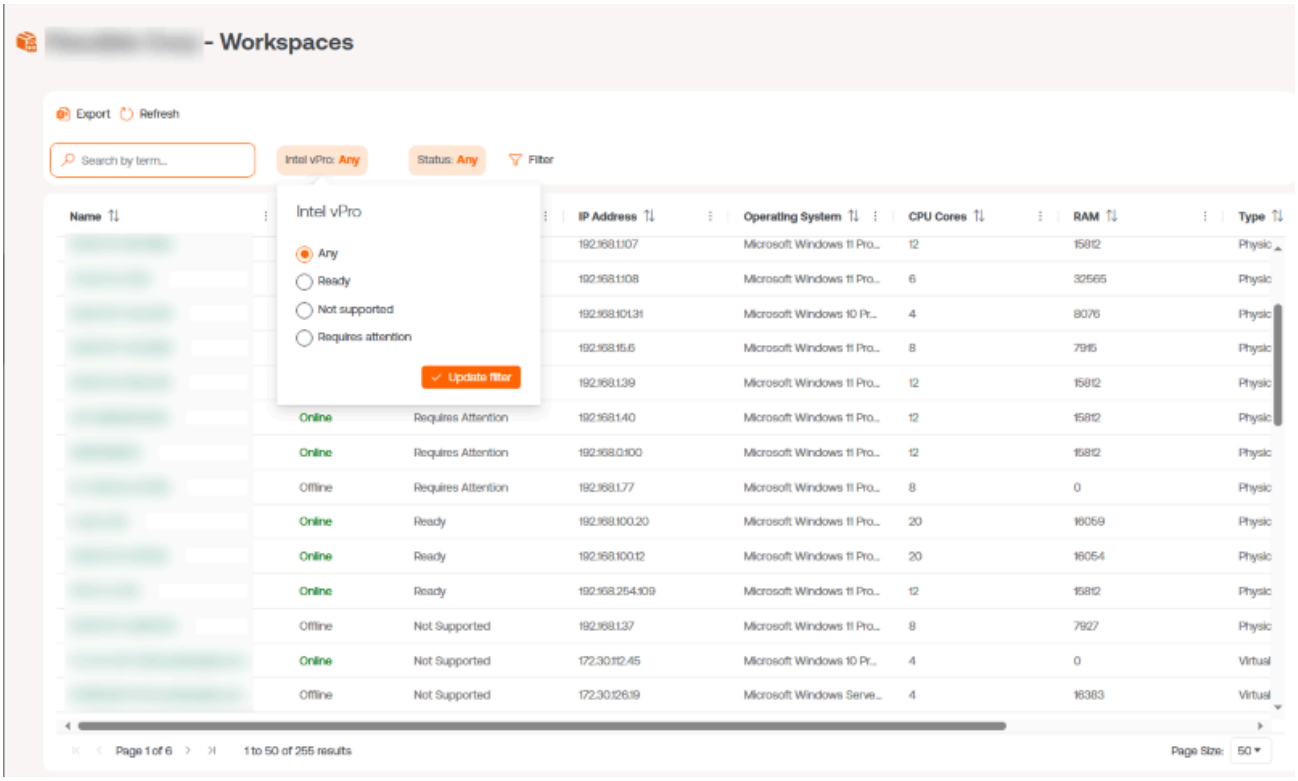
#### Compatibility with Intel® AMT

Enabling the integration will perform automated operations in all the physical workspaces in your organization to check for Intel® AMT support. This process includes the unattended install and uninstall of the Intel® EMA Configuration Tool on all devices in your environment.

After this process is completed, you will see the results for each workspace in the Intel vPro Enterprise column in the Workspaces section (Portal), and also in the details of each workspace.

The possible values for this field are:

- **Not supported**: the workspace does not support Intel® AMT, therefore it will not benefit from the Intel vPro® Enterprise integration.
- **Requires attention**: the workspace supports Intel® AMT technology, but the Intel® EMA Agent has not been installed. Please check the Intel EMA Agent section below to see how to proceed.
- **Ready**: the workspace supports Intel® AMT technology, and the Intel EMA Agent has been installed and configured correctly.




### Intel EMA Agent

Intel EMA Agent is an Intel software which is required in the workspace to allow the remote management operations included in the integration.

For the integration to work correctly, the installation and configuration of the Intel EMA Agent on the workspaces will be performed by Flexxible Odin. Do not attempt to install or configure the agent manually or by other means.

Additional requirements may apply for this agent to run properly. Please check the Intel® Endpoint Management Assistant (Intel® EMA) for more information.

To install the Intel EMA Agent, you can refer to the section Install Intel EMA Agent.

#### Communications

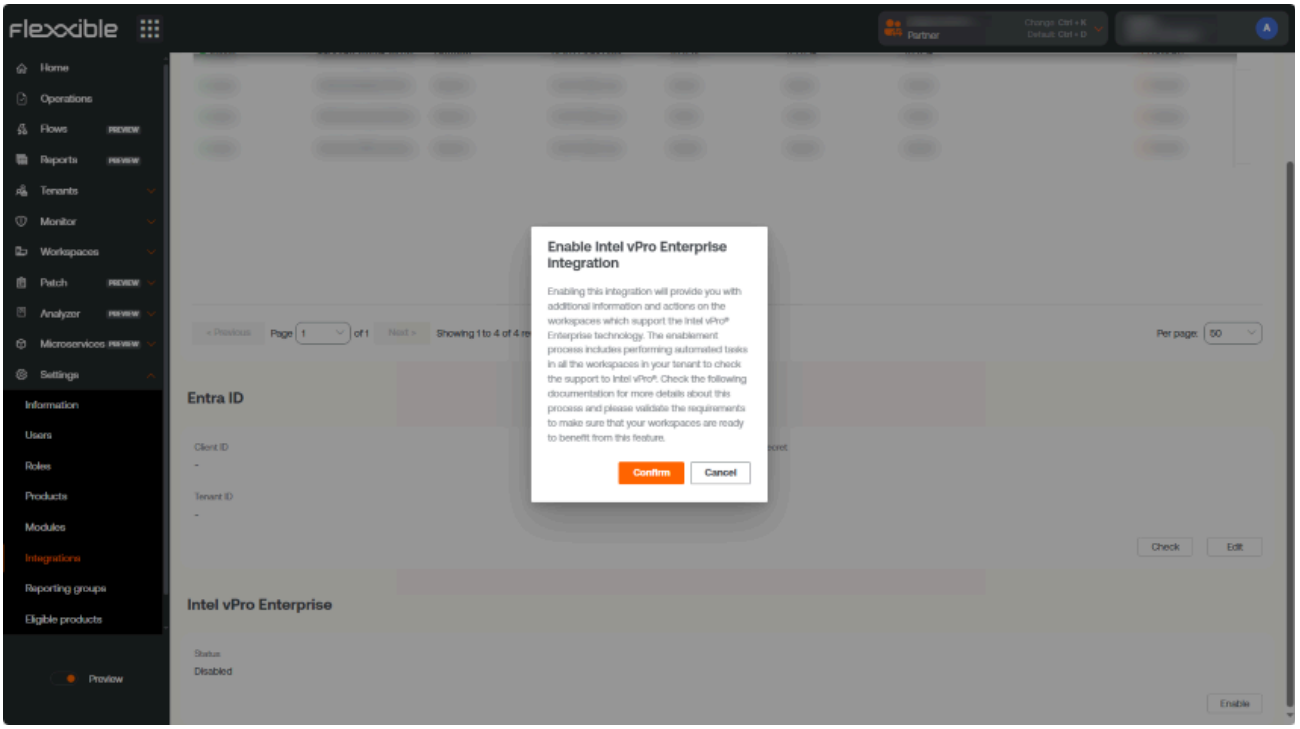
In addition to the FlexxAgent's communication requirements, devices must have a Client Initiated Remote Access (CIRA), a key component of Intel Endpoint Management Assistant. To make sure this connection is available, the following must be verified:

1. That the hostname of the Flexxible Intel EMA server, *iagent.flexxible.com*, can be resolved to an IP address from all devices planned to be included in the integration.
2. That the server is accessible from the device through TCP ports 8080 and 443.
3. That traffic between the device and the server is allowed by the proxy server, if applicable.

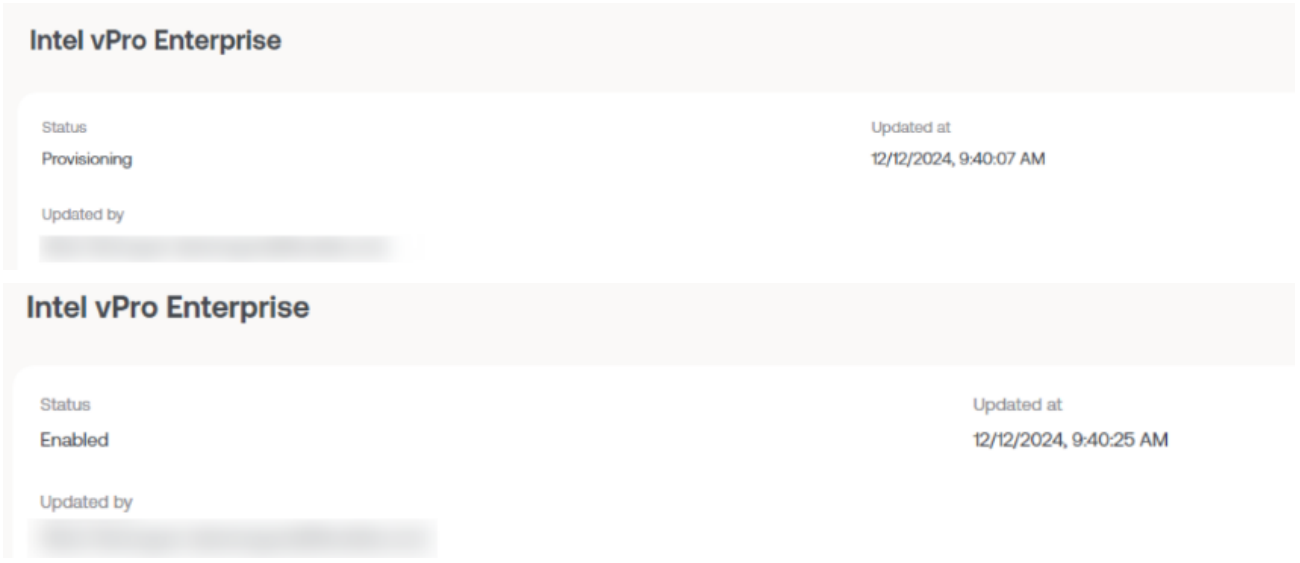
## Enable integration

This action can only be performed by users with the `Organization Administrator` permission in `Portal`.

1. Log on to `Portal`.
2. Go to `Settings` -> `Integrations` and locate `Intel vPro Enterprise`. Click on the `Enable` button.
3. A window with information about the integration and a confirmation request will appear. Click on `Confirm`.

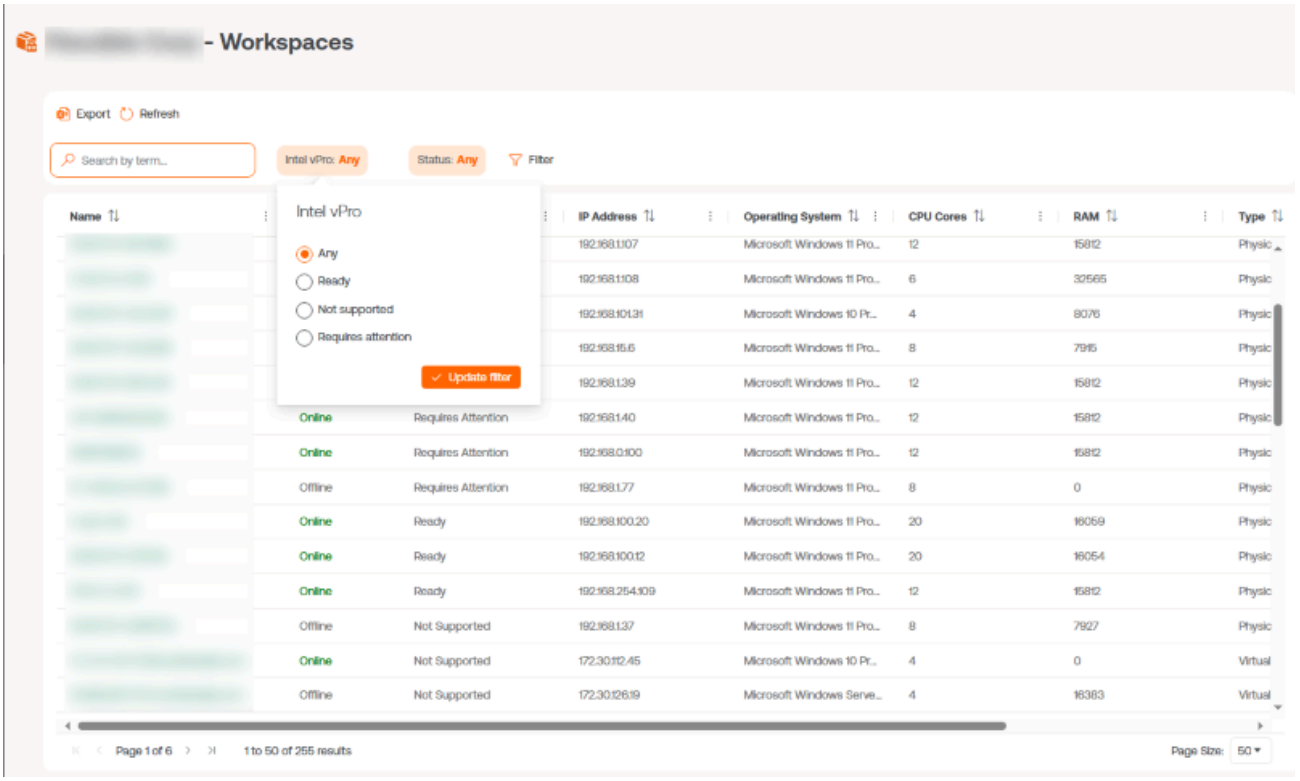



The integration process may take a few minutes to provision and configure the tenant. When completed, the status will be shown as "Enabled" along with related information.




Gradually, FlexxAgent will start performing internal checks on the workspaces to determine which ones support Intel® AMT technology. You should wait a few minutes before the information appears in Portal. The wait time depends on the tenant's FlexxAgent configuration and reporting groups.

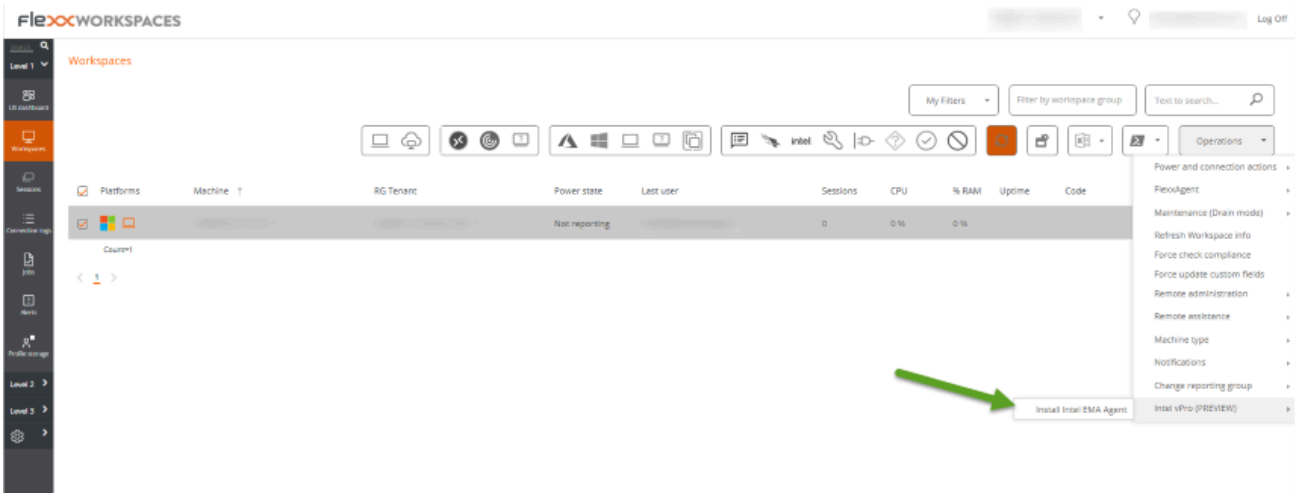
Go to the `Workspaces` section and check the information in the `Intel vPro Enterprise` column. You can also filter the devices by the field value to easily find which ones support Intel® AMT technology.



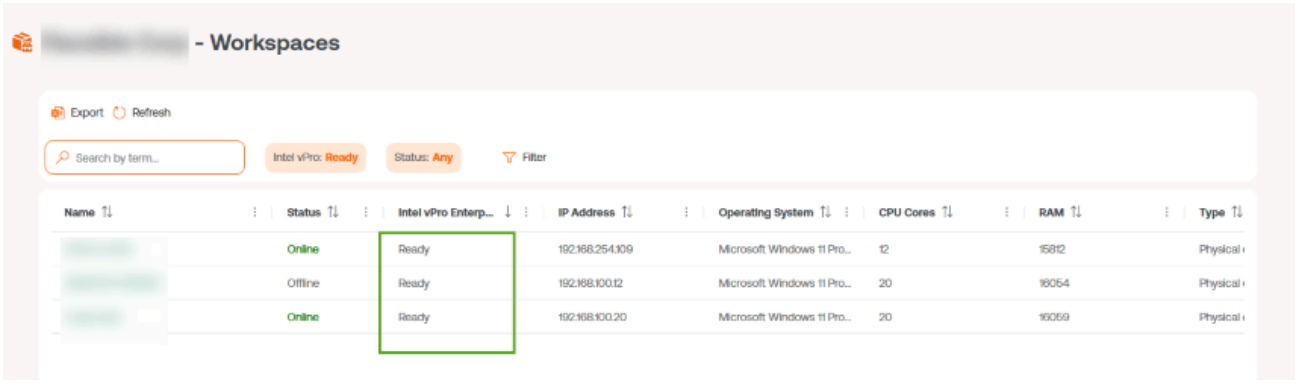

Install Intel EMA Agent on devices that indicate support for Intel® AMT (in the `Intel vPro Enterprise` column of Workspaces, they are labeled as `Requires attention`).

#### Install Intel EMA Agent

1. Go to `Workspaces`, in the `Workspaces` module, and select the desired workspace.
2. Run the `Install Intel EMA Agent` operation from the `Operations` menu. Follow the on-screen instructions to verify the process completed successfully.




3. Once completed, the device's `Intel vPro Enterprise` field will show `Ready`.

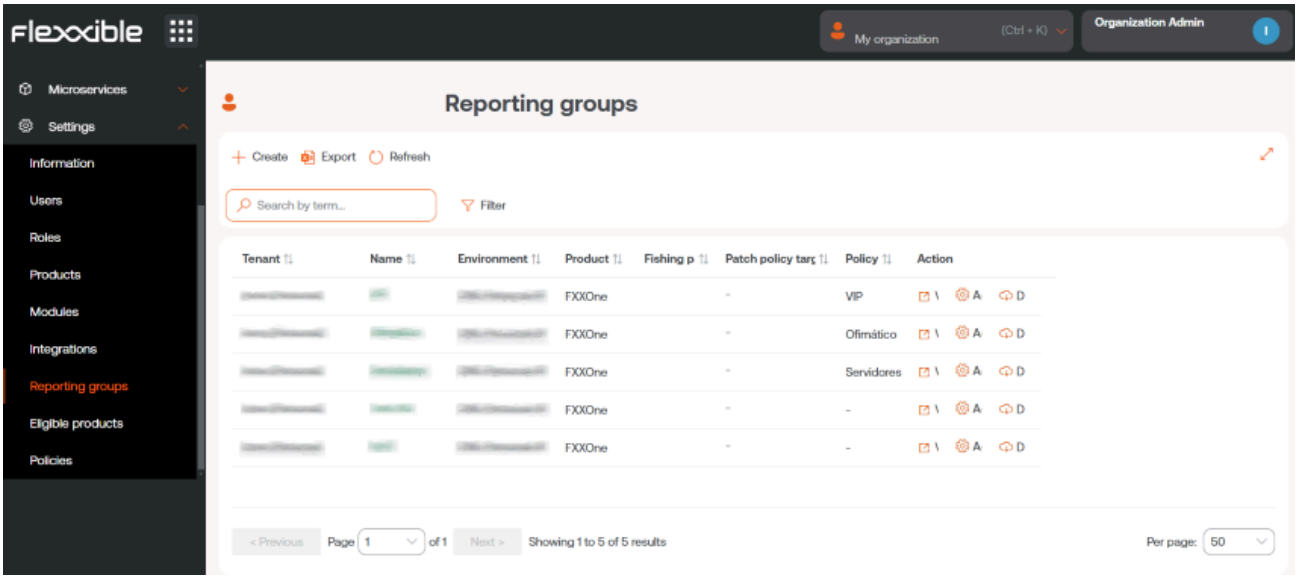



To learn more about Intel vPro®, please visit the following links:

- Intel vPro® Enterprise
- Intel EMA configuration tool
- Intel EMA Agent documentation (refer to the “Intel EMA Admin and Usage Guide” document)

# Portal / Settings / Reporting Groups

From `Reporting groups` you can create and preconfigure groups within the same organization using different criteria to meet the needs of departments, offices or user groups that make them up.




It is also possible to know which users and which roles have access to the reporting group. As well as activate Remote Assistance functionalities.

## Reporting groups creation

To create a reporting group, press the `New` button and fill in the following fields:

- **Tenant**: it is a dropdown, to select the tenant in which the new reporting group will be created.
- **Name**: the name that the reporting group will have.
- **Environment**: opens a dropdown to select the environment in which the reporting group will be.
- **Patch directive destination**: opens a dropdown to select which patch policy the reporting group will be subjected to.
- **Fishing pattern**: it is an optional field. Allows indicating the regular expression (RegEx) that will be used to add devices to the reporting group. For example: `company`

(includes all devices whose names contain the word "company") or `.*2023$` (includes devices whose name ends in "2023").

Once the reporting group has been created, it will appear in the table of the list view. The `Reload` button is very helpful if you want to refresh the list to ensure the reporting group has been created.

## Fishing pattern

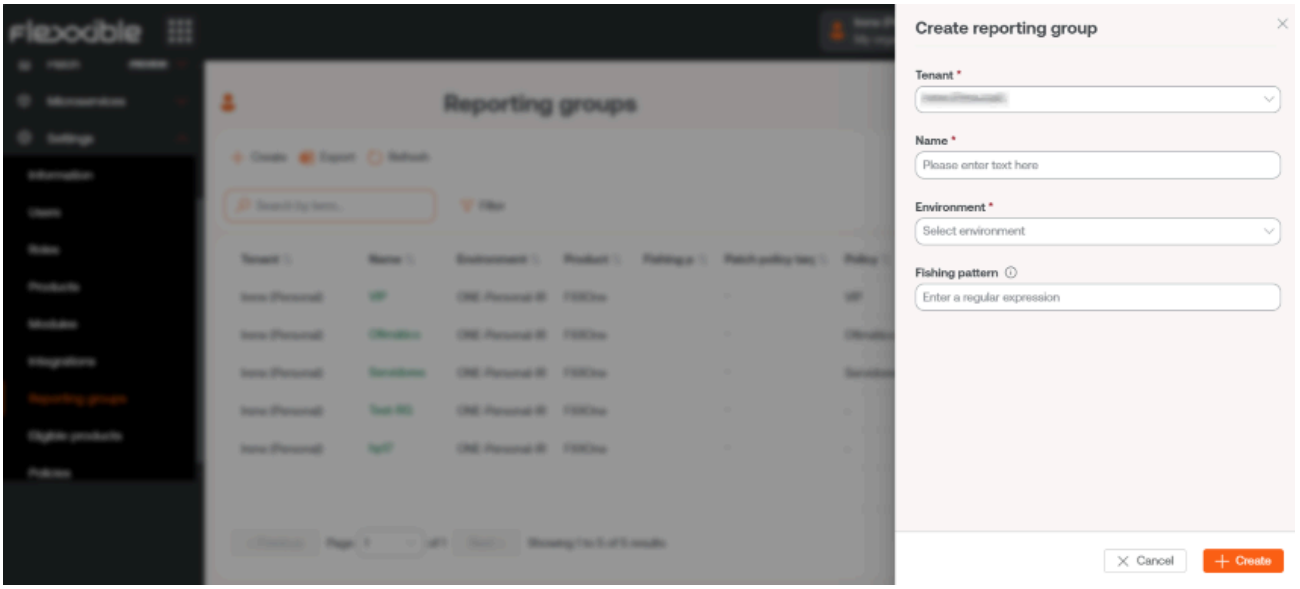
The fishing pattern allows automatically grouping in a reporting group the devices that share a regular expression (RegEx) in the name.

The devices that form the reporting group will be updated every hour. It is an automatic process that checks if there are new devices matching the configured RegEx. If there are, the devices will be moved to the corresponding reporting group.

> **INFO**
>
> The regular expression (RegEx) should have a maximum of 250 characters.

It is important to pay attention to all the active RegEx to avoid conflicts between reporting groups, as it may happen that when creating a new one, its RegEx matches an existing one.

You can verify which reporting group a device is in from `Reporting Groups`, in the `Workspaces` module. And the history of a reporting group can be queried from the device detail view, in the `Workspaces` module.




If you want to check which reporting group the device has passed through, you can do so from `Reporting group history`, in the detail view of a workspace, in the `Workspaces` module.

# Reporting groups list

The list view shows a table whose fields match the data requested to create the reporting group. It also has the `Action` field, which allows access to `View details` and `Agent configuration`.

## View details

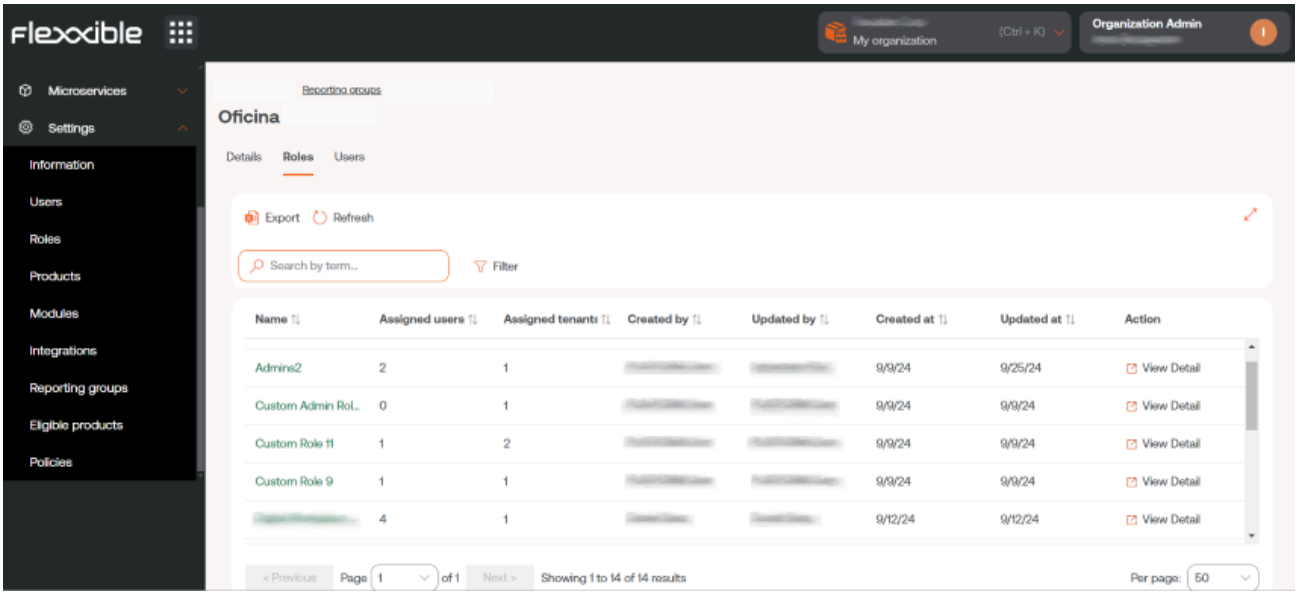
The detail view allows consulting three types of information about the selected reporting group:

#### Details

This tab offers general information about the reporting group being consulted. The `Edit` button opens a form that allows you to change the initial characteristics of the group, such as the name or the patch directive destination.

#### Roles

This tab shows a table with the list of roles that can access the reporting group being consulted. In turn, this table also has the `Action` field -> `View details`, which allows you to consult more specific information about the roles: details, permissions and users.




- **Details**: general information about the role. At the bottom right, the `Edit` button allows you to change the name of the role.
- **Permissions**: through a table, shows the permissions that this role has in the Portal, Workspaces and Analyzer modules.
- **Users**: through a table, shows a list of users assigned to that role.

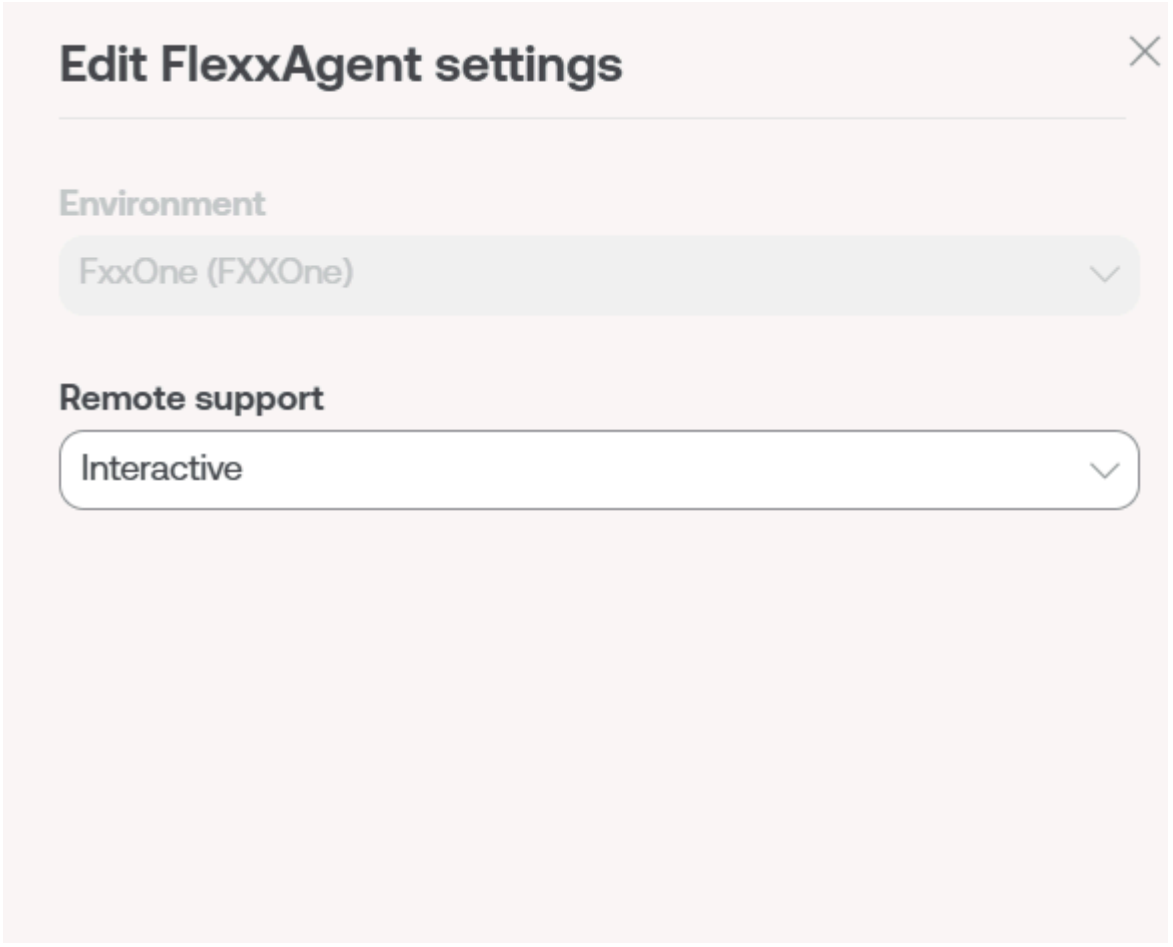
> More information about roles, users and permissions in `Roles`.

#### Users

This tab shows the name and associated email of the users who make up the reporting group being consulted.

## FlexxAgent configuration (Remote Assistance)

From here, a user with the `Organization administrator in Portal` access level can configure the type of remote assistance that the reporting group will have: interactive, unattended, dynamic or none.




This configuration is set from `Products`, however, very specific and particular configurations can be made for the reporting groups.

For those organizations with sub-organizations, it is possible to list all the report groups. This is the sum of the report groups of the `parent organization` plus the report groups of all the `sub-organizations`. This view allows a multiple selection and enables or disables automatic agent updates in multiple report groups.

# Portal / Settings / Directives

Policies allow you to create client-type organizations using a template, so that each time an organization is created, it can follow a pattern that can be used to apply certain configurations, such as user access or the activation of FlexxAgent. They are useful for assigning specific characteristics to one or more report groups, thus facilitating their management and saving time for users of managed service provider (MSP) organizations.

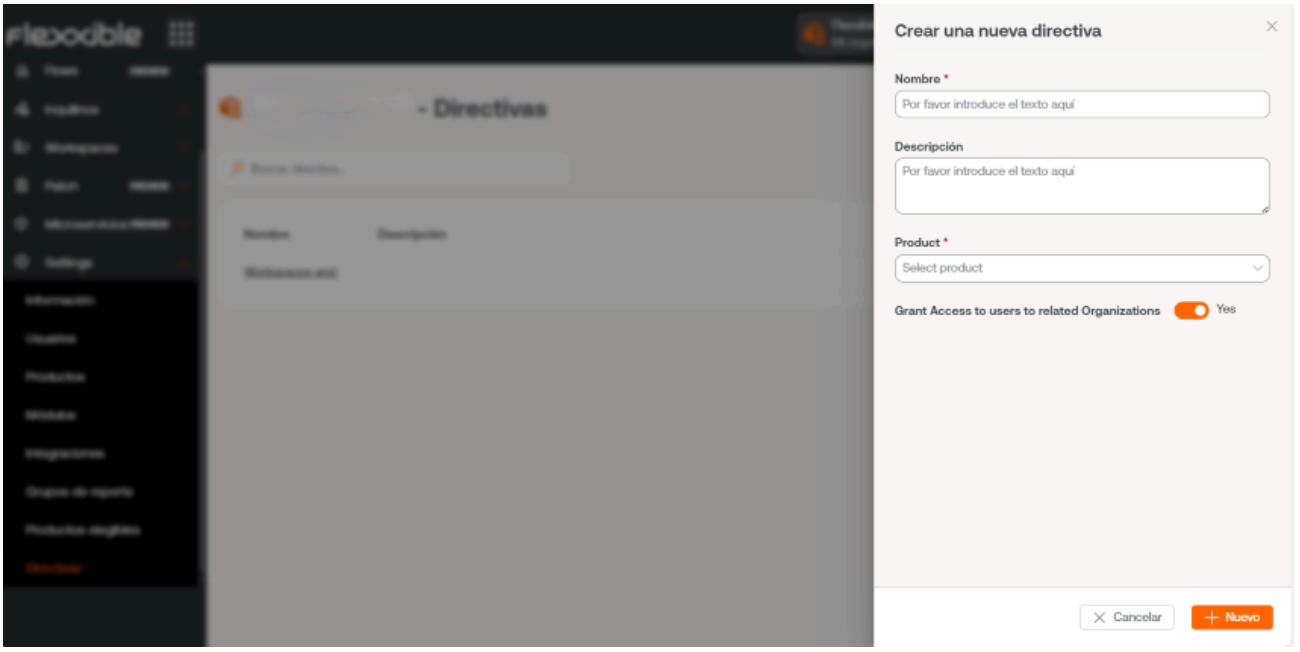
From the overview, you can access a list of the created Policies, as well as a brief description of them. By clicking on `View Details`, you can get more information, such as the report groups to which it is being applied and the names of the users responsible for its management.

Each time a new organization is created, the report groups defined in the policy will be created, and the users specified in the policy will have access. At the same time, from the Policy itself, you can determine whether partner-type users will have access to manage an organization in Portal or not

## New Policy

To create a new policy, you just need to press the `New` tab and insert the required information: Name, description, associated product, and user information for the people who will manage it.

It is also possible to assign a Policy to an organization from Tenants.



# Portal / Access Considerations

To facilitate logging in to Flexxible tools, such as Portal, Analyzer, and Workspaces, authentication is delegated to existing Microsoft Entra ID (formerly Azure Active Directory) or Google accounts, which use OAuth2.

Depending on the organization's configuration and security policies, an administrator may need to authorize the use of Entra ID or Google accounts the first time they want to use them to access Flexxible tools.

## User authentication

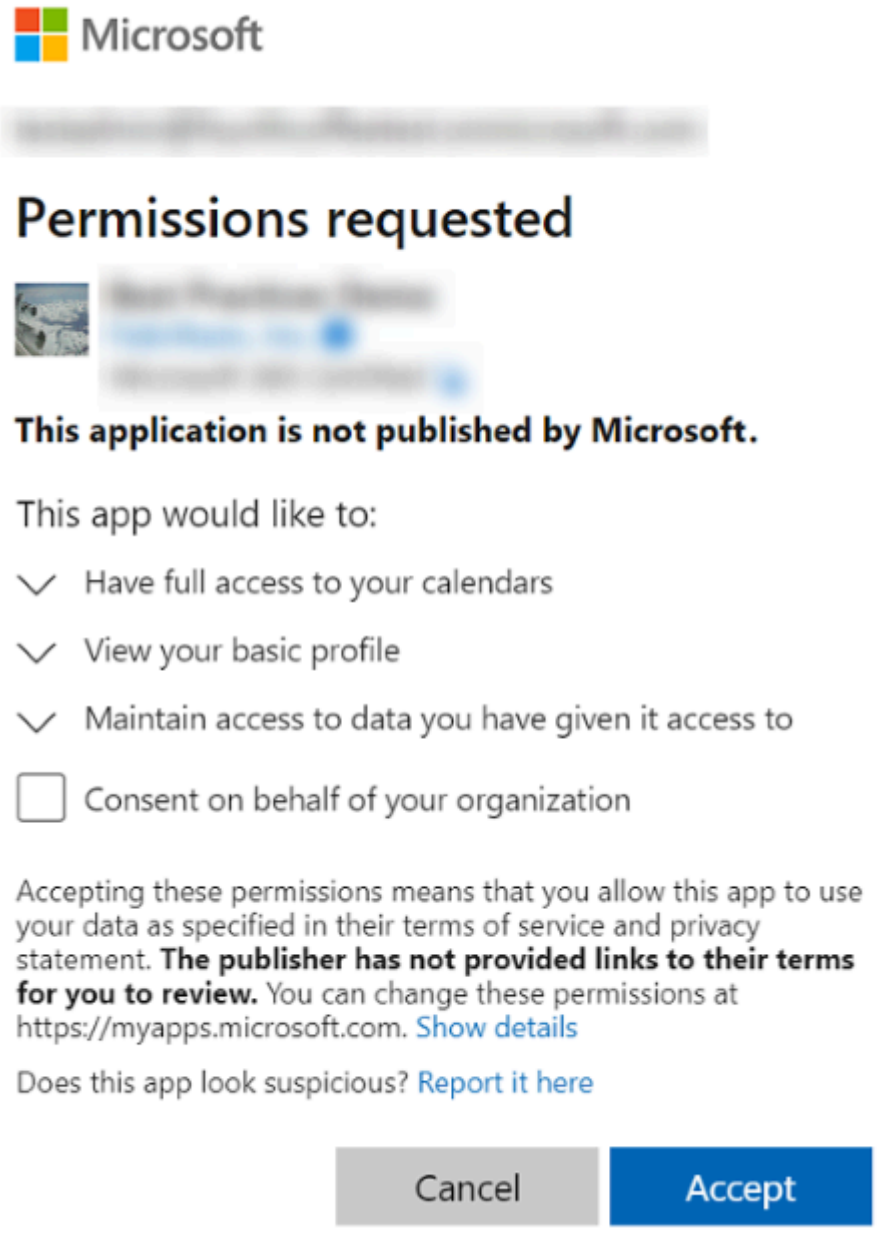
For the Flexxible SSO system to verify that the Microsoft Entra ID or Google account is valid and authorized to access its consoles, it needs an administrator to give the following consents:

- Microsoft Entra ID: a Flexxible Enterprise Application is used in your tenant (tenant).
- Google Admin: a Flexxible OAuth client id is used in your tenant (tenant).

This is one of the usual procedures when third-party applications delegate their log in to Entra ID or Google Admin. The tenant administrator can always see what data the application has access to, who has used the application, and revoke consent, preventing users from logging in again to any Flexxible console.

### Enterprise Application Consent and Permissions in Entra ID

User access can be granted individually or in groups, although there is a way to simplify the process by having **an administrator consent to the use of the Enterprise Application for your organization**. This allows users in your organization to log in to the Flexxible ODIN consoles with their corporate credentials and automatically create the Enterprise Application in your Azure tenant. For this, the administrator only needs to try logging in to Portal for the first time, which will trigger the consent request:

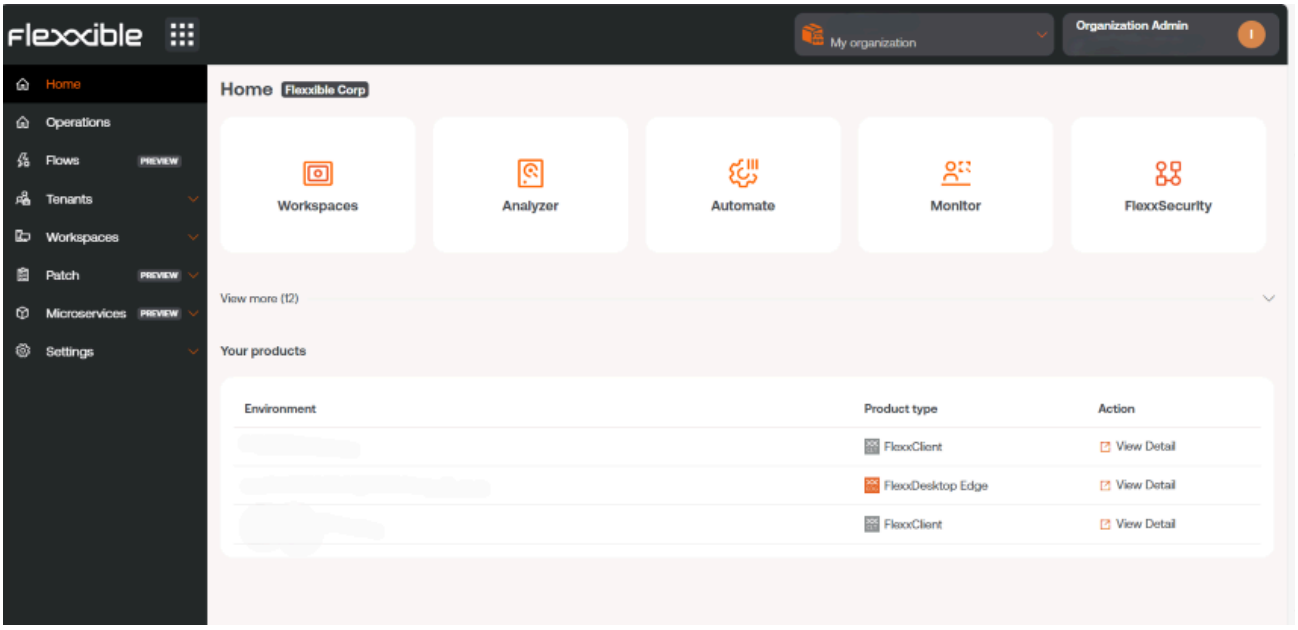



If created manually, to provide authentication the Enterprise Application must have the following permissions:

| Permission | Caption |
|---|---|
| Directory.Read.All | Read directory data |
| email | View user email addresses |

| Permission | Caption |
| --- | --- |
| offline_access | Maintain access to data you have given access to |
| openid | Log In |
| profile | View basic user profile |
| User.Read | Log in and read user profile |

# Portal / Guides and tutorials for Portal




This section offers resources designed to maximize the use of Portal. It includes detailed instructions on initial and advanced configuration, allowing it to be tailored to specific needs.

Each guide has been created to facilitate understanding and application, regardless of the user's level of experience. In addition to step-by-step instructions, you will also find procedures and solutions to common problems.

# Portal / Guides and tutorials / Creation and management of Workspaces Groups

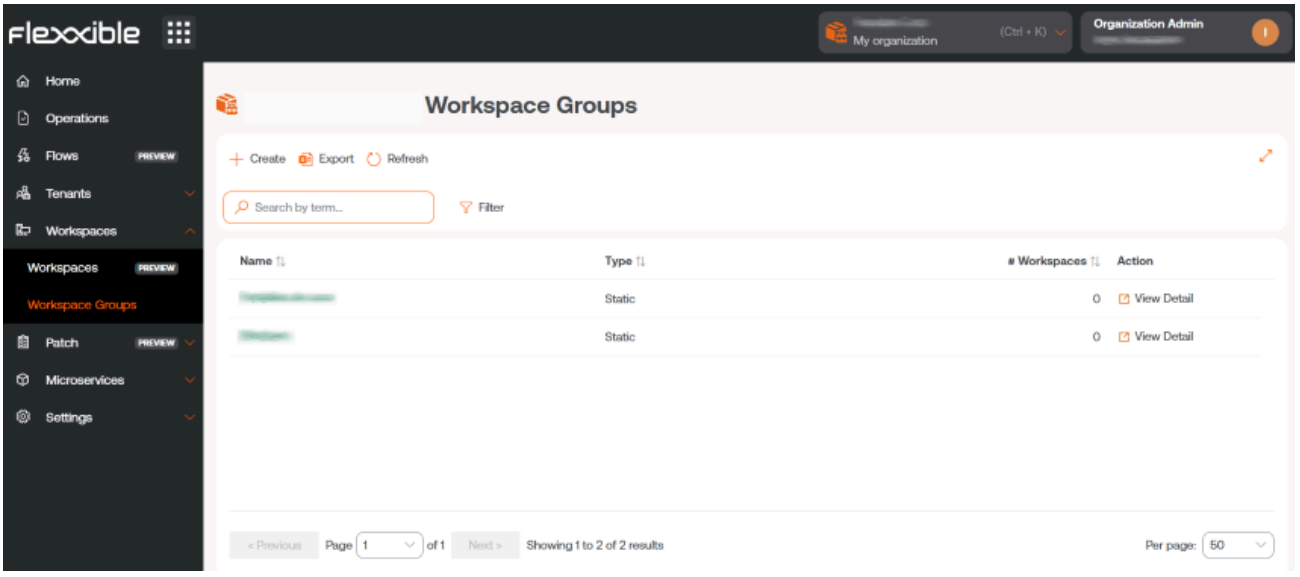
Workspaces Groups are logical groupings of a set of devices (or endpoints) that can be used when managing an organization. They can be static, dynamic, and Entra ID type.

## Static Workspaces Groups

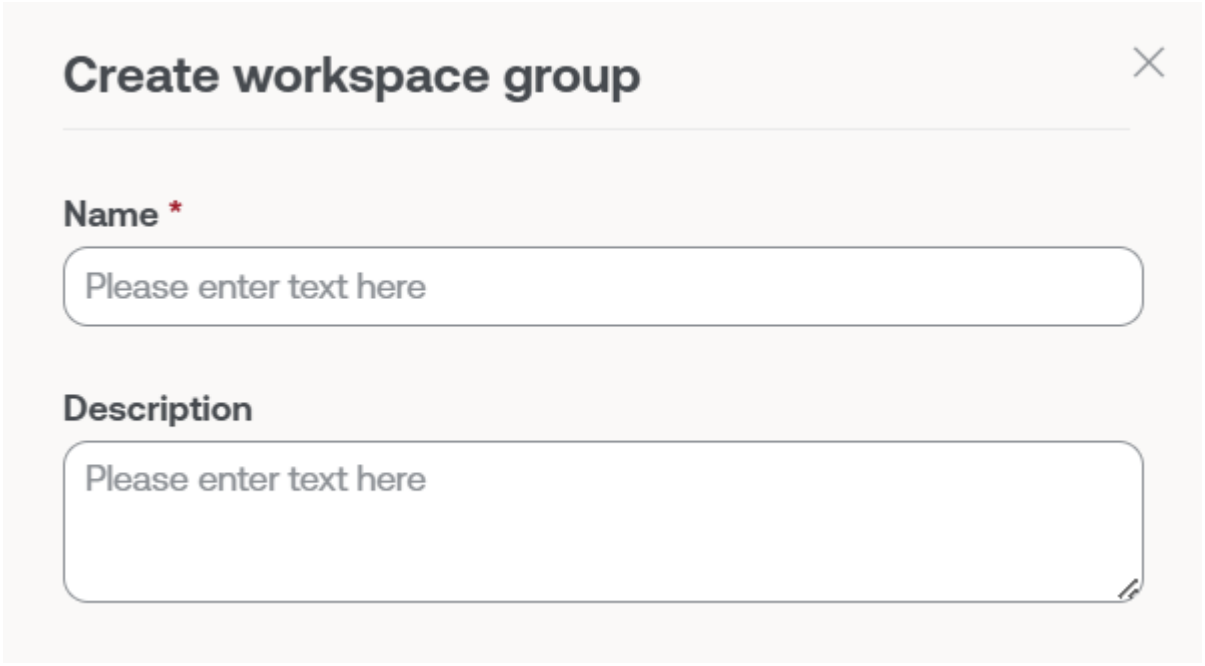
It is a group created manually, with free criteria. The devices that comprise it do not change unless the group is modified. It can be created and managed from `Portal` and from the `Workspaces` module, by filtering the list from the Workspaces option.

### How to create a static Workspaces Group from Portal

1. Enter Portal and select the option `Workspaces` -> `Workspaces Groups` in the left side menu. A list of available groups will appear (or empty, if none exists).

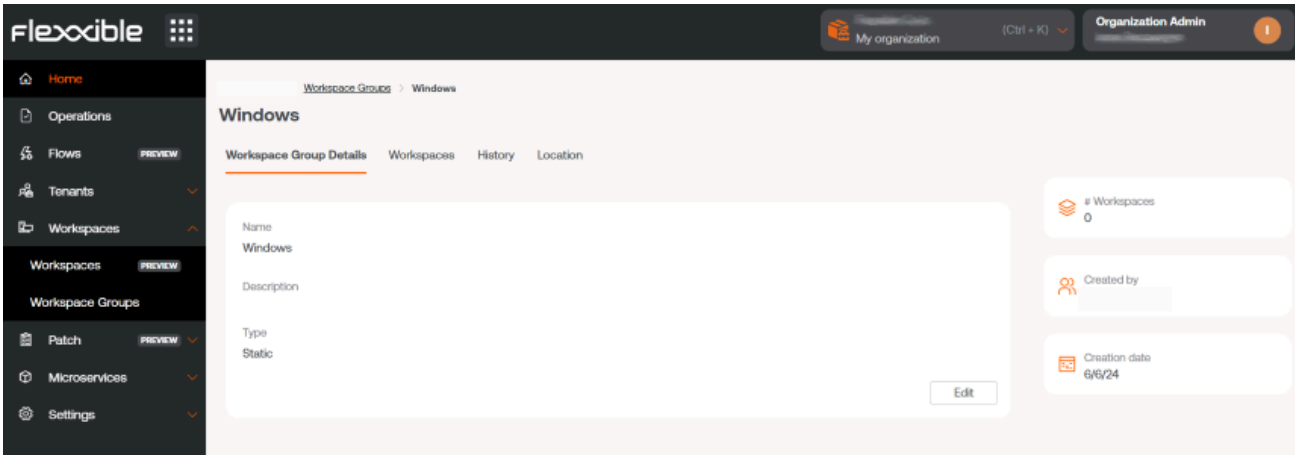



2. Click on the `+ New` button at the top of the list. A modal window will appear on the right side of the screen. Enter the group name and description (optional). Click the `+ New` button at the bottom of the window.




3. A confirmation message of the group's creation will appear. Close the window using the cross at the top right.

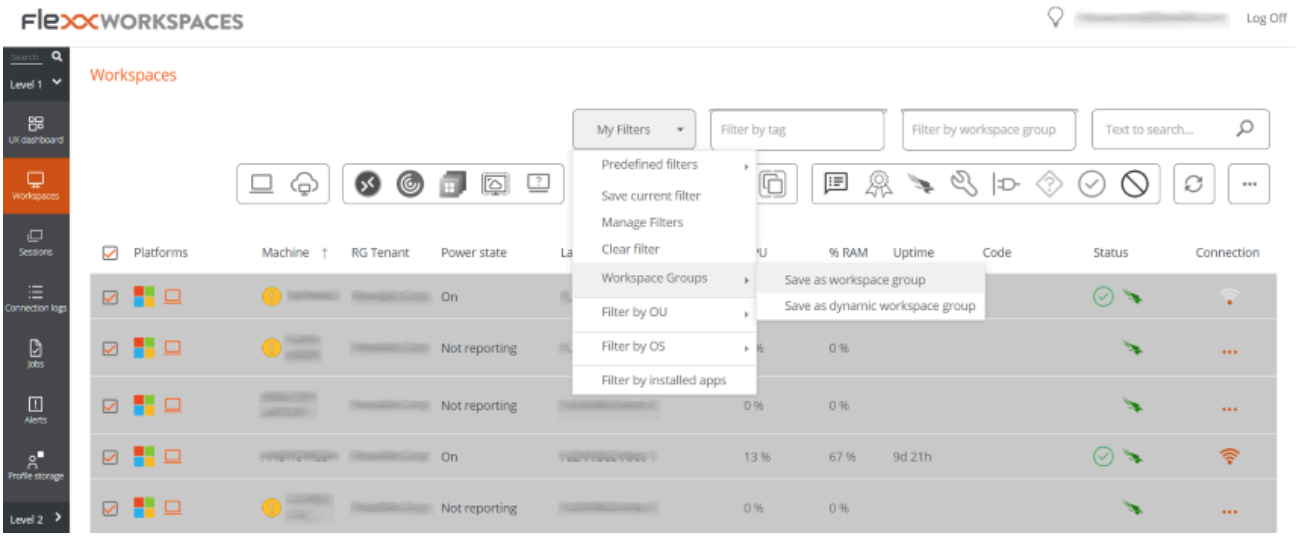
4. The new group will appear in the Workspaces Groups list. Click on its name to access the details.




## How to create a static Workspaces Group from Workspaces

1. Access `Workspaces` in the left side menu of the `Workspaces` module.
2. Select the desired devices in the list view.

3. Save the devices in a new group by clicking `My filters` -> `Workspace Group` -> `Save as dynamic workspace group`.



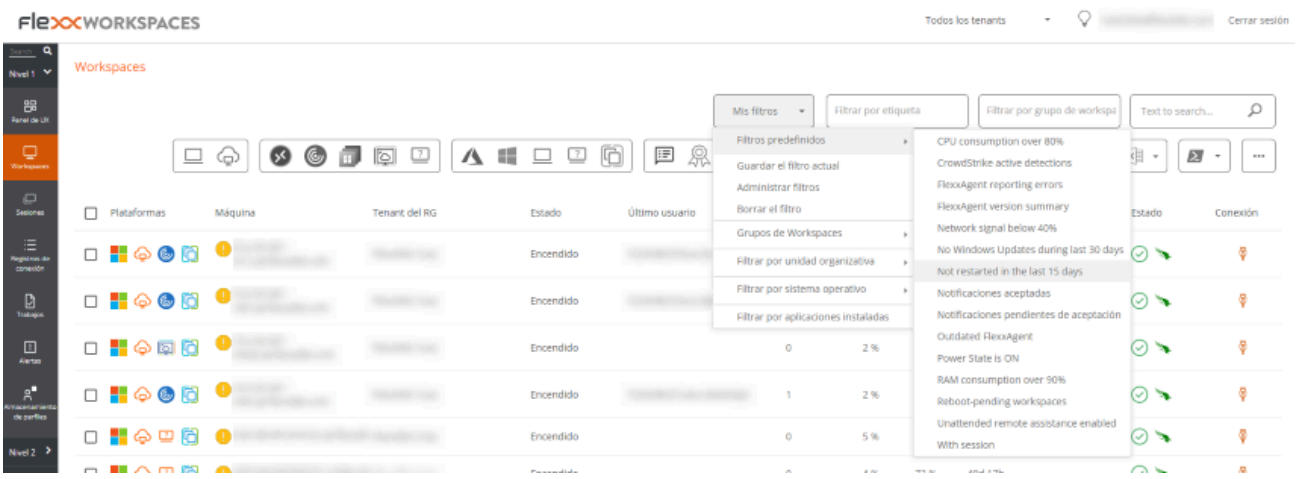

# Dynamic Workspaces Groups

It is a group where a condition is periodically evaluated, so its members can change in real-time. Dynamic Workspaces Groups can be created from Workspaces search filters.

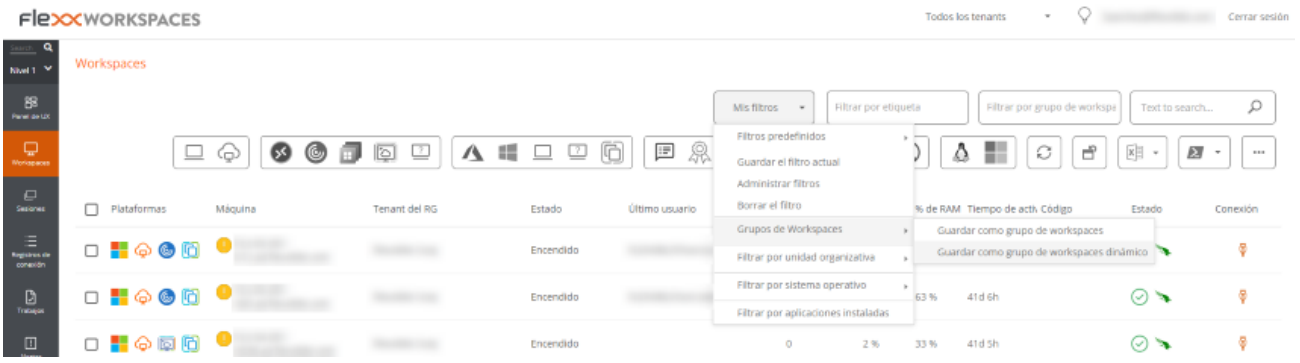
## How to create a dynamic Workspaces Group

Dynamic groups are created from the `Workspaces` view, within the `Workspaces` module.

1. Access the list of devices. Select (or create) a search filter. For simplicity, in this example a filter that searches for devices that haven't restarted in the last 15 days is used.



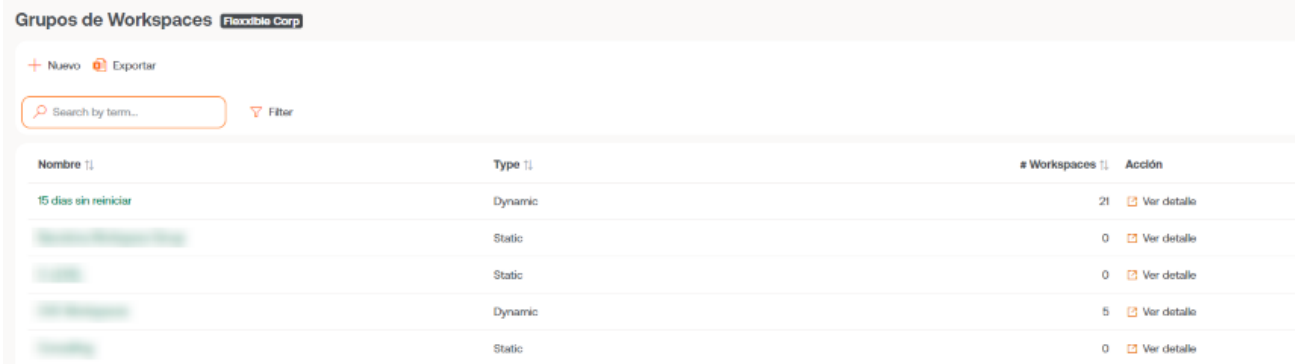

2. Once within the filter results, use the `My filters` -> `Workspaces Groups` -> `Save as dynamic workspaces group` option.




3. A pop-up panel will appear. Give the dynamic group a name and click `OK`.

4. The system notifies that a job has been scheduled to create this item. You can audit the task execution in the `Jobs` section of the left menu of the `Workspaces` module.

5. Go back to the `Workspaces` -> `Workspaces Groups` menu in Portal to check that the new dynamic group has been created and to view its members.



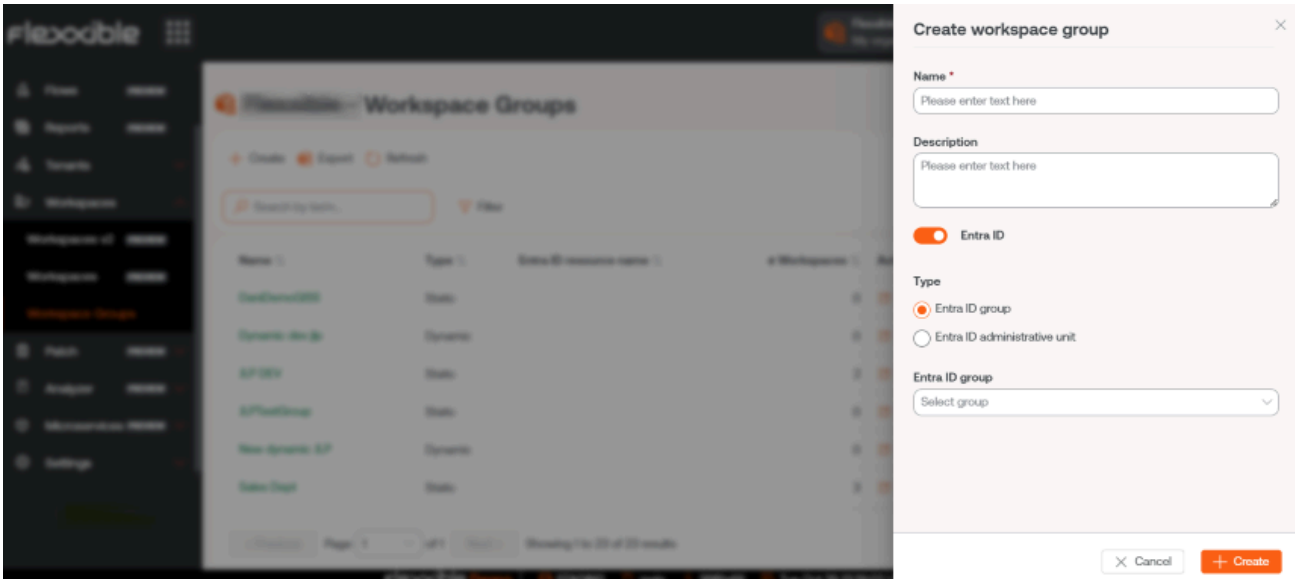
# Entra ID Workspaces Groups

It is a group that can pull members from an existing group or organizational unit in the Entra ID domain in use. Creating this type of group requires at least one active integration with the Entra ID domain under `Settings` -> `Integrations` in Portal.

## How to create an Entra ID Workspaces Group

Entra ID groups are created from Portal.

1. In the side menu, go to `Workspaces Groups`.
2. Click on the `New` button located at the top of the list view.
3. Next, you should add a name, a description for the group, and activate the Entra ID button. Select the type of group to be created: Entra ID Group or Entra ID Administration Unit.




Entra ID groups require an API connection, which can be configured from `Portal` -> `Settings` -> `Integrations`. Only from there can the created **Entra ID Group** and **Entra ID Administration Unit** be consulted and therefore operations can be carried out on them from the Workspaces module.

# How to manage a Workspaces Group from Portal

To manage a Workspaces Group, click on the name of the desired group and access the following tabs:

- **Details**: provides general information about the group. From here you can delete the group by clicking on the `Edit` button.

- **Workspaces**: shows the devices that are part of this group. This option allows exporting the list of devices comprising it.

- **History**: displays a bar graph of the daily number of workspaces that formed the group in the last month. You can zoom in on the chart for better reading by selecting the bars you want to enlarge with the mouse. By Reset zoom, the information returns to its original state.

- **Location**: a geographical location can be added to the group of devices. This value is just a reference, it does not update if users change location.

- **Programming**: From this tab you can schedule the Wake on LAN or the automatic shutdown of a group of devices. If the user wants to schedule one of these actions, they must click on the `New` button and fill in the form fields for `Action`, `Day of the week`, and `Time UTC`.

    - **Action**: allows you to choose between `Wake on LAN` or `Shutdown`.
    - **Day of the week**: allows choosing which day of the week the action will be performed.
    - **UTC Time**: allows you to specify the exact time to start the action, in Coordinated Universal Time standard.

    The created action will then be displayed in a table, with columns showing the information entered in the form, as well as which user created the action and who updated the schedule and when.

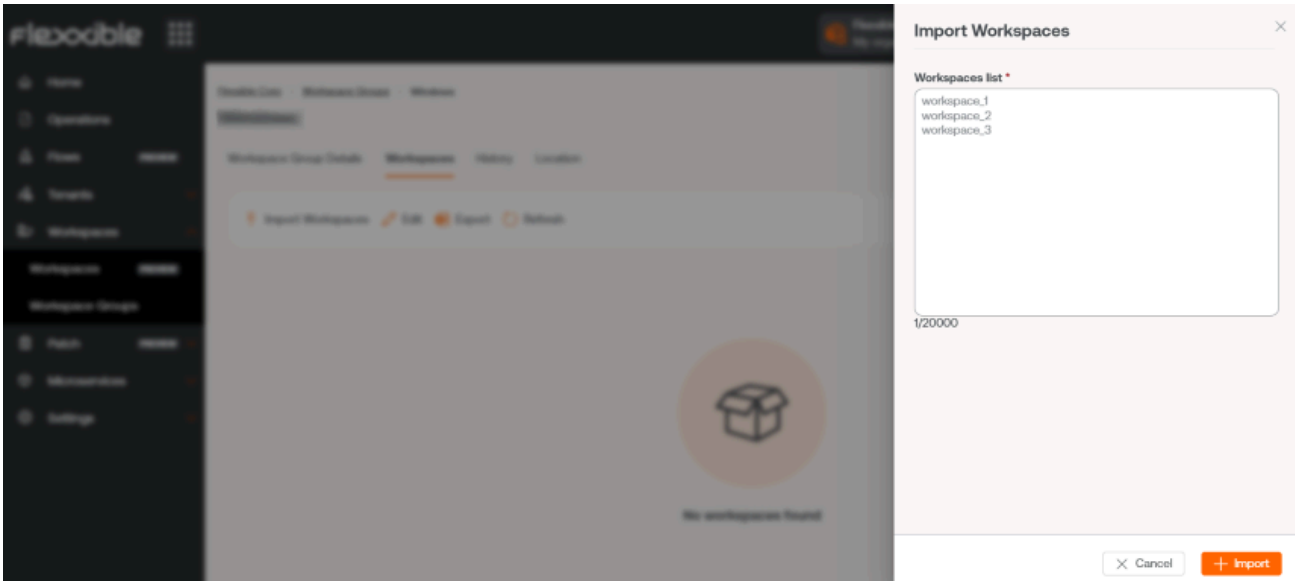
    From `View details` you can edit and delete the scheduled action.

- Syncs: this tab is only visible when the group is of the Entra ID type. Displays a table with details of the performed syncs.

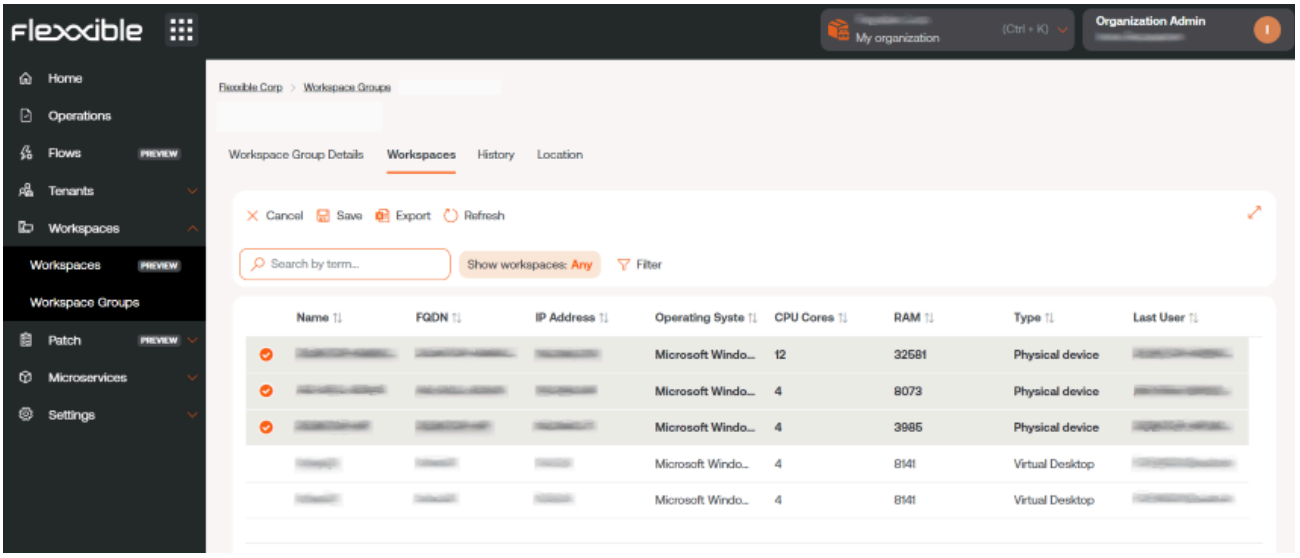
#### Add devices to the static Workspaces Group

There are two ways to add devices to a Static Workspaces Group from Portal:

1. In the groups table, click on `Detail View` of the desired group -> `Workspaces` -> `Import devices`. A form opens that allows importing up to 20,000 workspaces.



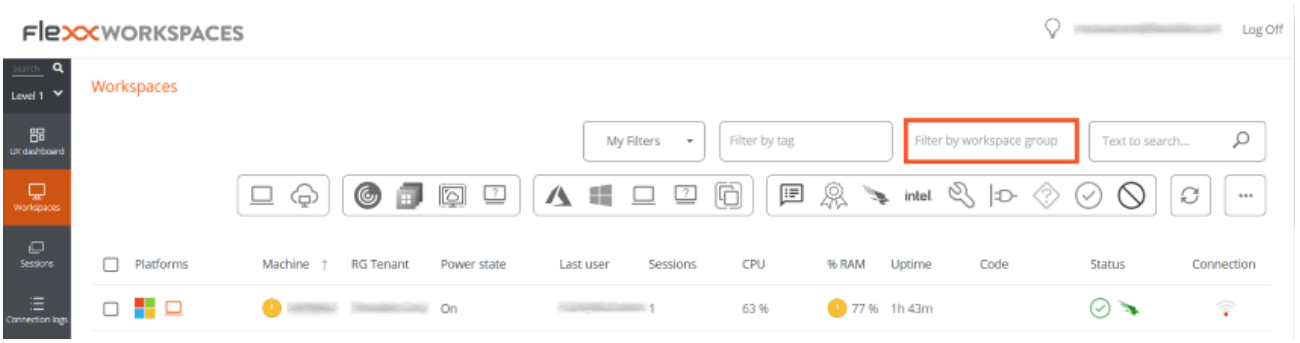

2. In the groups table, click on `Detail View` of the desired group -> `Workspaces` -> `Edit`. Next, select the devices you want to add. Those marked with an orange dot are added to the group and those not marked are removed. In both cases, click on `Save` to keep the changes.




# How to manage a Workspaces Group from Workspaces

Once the group is defined, it can be managed within the `Workspaces` module.

1. Access `Workspaces` in the left side menu of the `Workspaces` module.
2. Filter the device list by Workspaces Groups.




3. Choose the Workspaces Group on which you want to perform actions. 4. Use the multiple options offered by the `Workspaces` module.

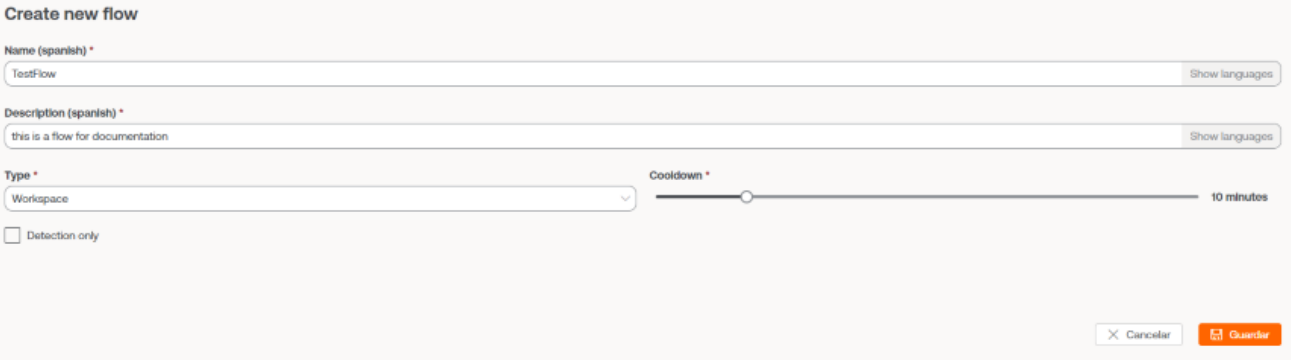
> **INFO**
>
> For more information about `Workspaces Groups`, please refer to their documentation.

# Portal / Guides and tutorials / Scheduled Microservice Execution

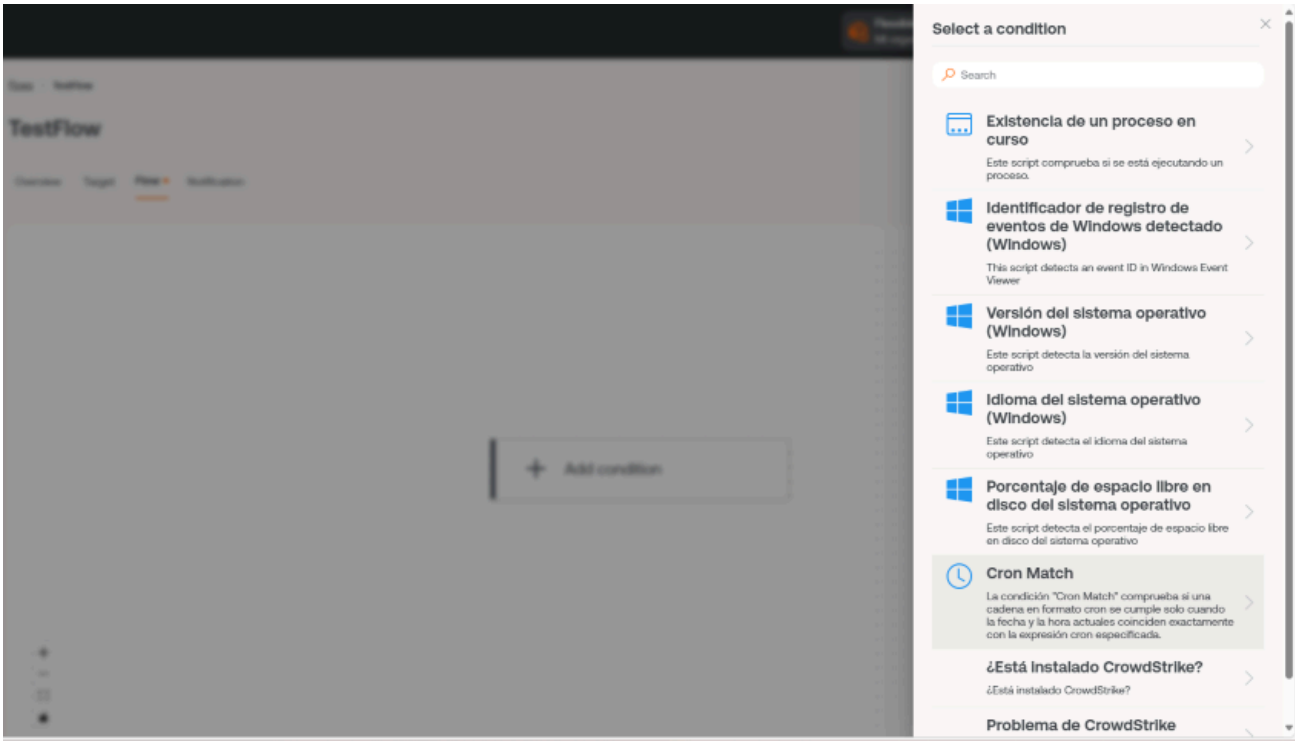
Microservices allow actions (queries or corrections) on devices. They can be executed directly, from the `Workspaces` module, or scheduled through `Flows`, which allow conditional microservices execution.

## How to schedule the execution of a microservice

1. Click on the `Flows` option in the left menu of Portal.
2. Click on `+ New` to create a new flow. Or select an existing flow if you want to modify it.
3. Fill in the fields. Choose whether the flow will be executed at the operating system level or at the user session level.
4. Once the fields are filled in, click on `Save`.

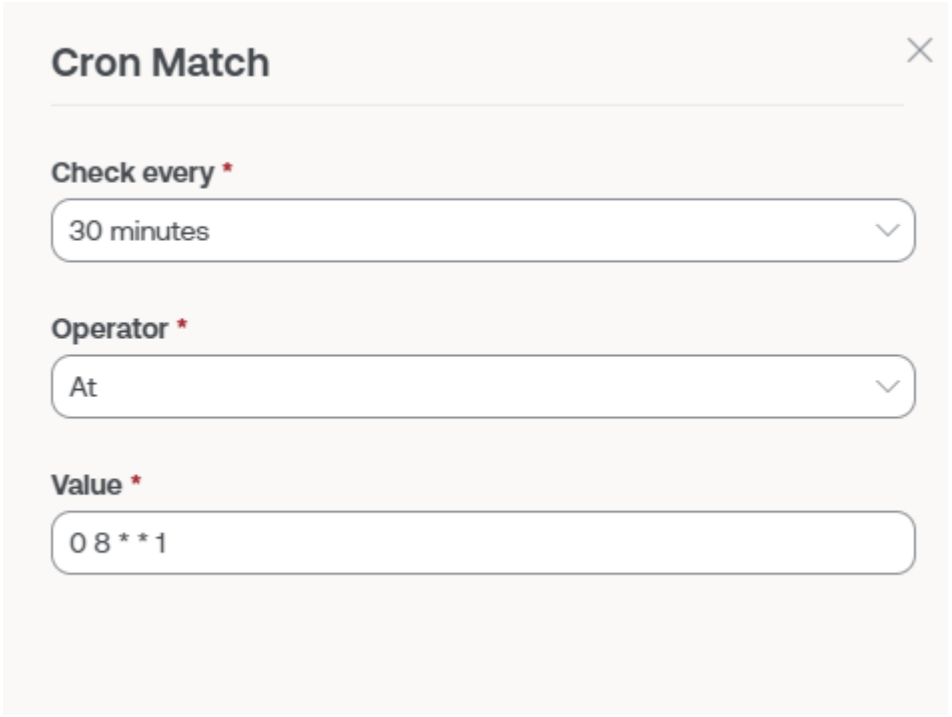



5. In the flow list view, select the flow you just created.
6. Click on the `Flow` tab.
7. In the panel, click on the `Edit` button located on the right.
8. To add the first condition, go to the `+` symbol and click on `Add condition`. A panel with all available conditions will appear on the right side of the screen. Select `Cron Match`.

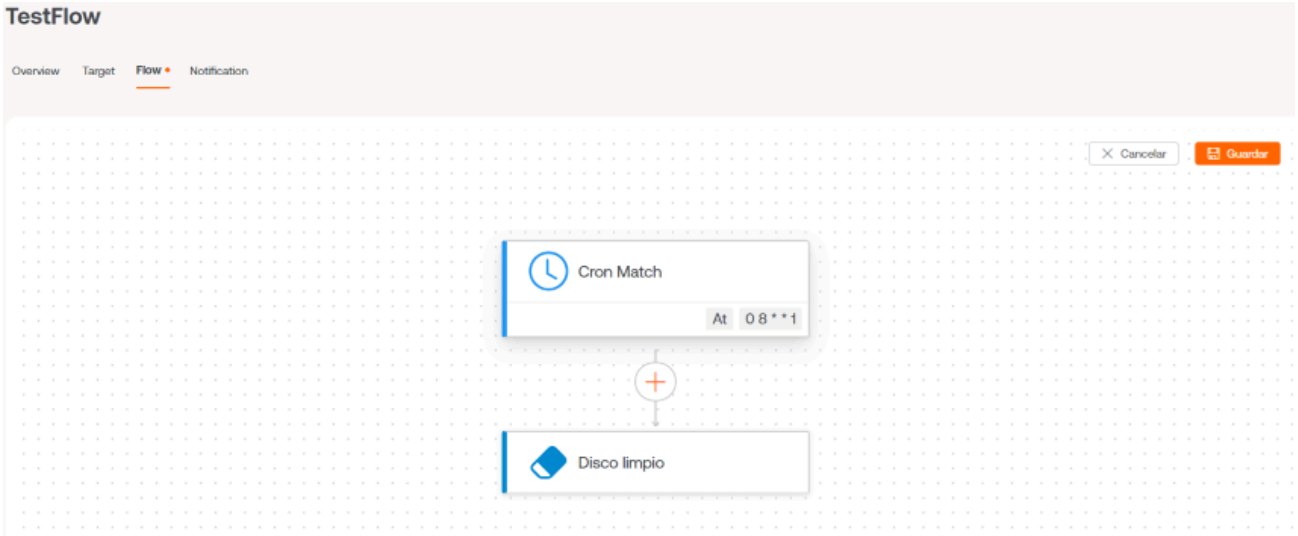



1. Add the condition check fields: `Check every`, `Operator` and `Value`, the latter in "cron" programming syntax. Keep in mind that hours are defined in Coordinated Universal Time (UTC).
2. Click on `Save` at the bottom of the panel. In this example, the condition is checked every half hour and the "cron" condition is "every Monday at eight in the morning".

There are many references available to check "cron" scheduling syntax. For example: crontab.guru




11. Click on the `+` symbol located below the condition and select `Add action` to add the microservice to be scheduled. At this point, additional conditions can be added if needed.
12. Select the microservice you want to schedule. In this example, “Clean Disk”. Click on the `Save` button in the upper right corner.




In this example, the disk cleaning microservice has been scheduled to be executed every Monday at eight in the morning.

To activate the periodic execution of this microservice on devices, it is also necessary to configure the `Destination` of the flow, including the report groups, devices or groups of devices where execution is required.

There is also the option to notify users about the execution of the flow. To do this, you need to enable the option and fill in the `Initial text`, `Success text`, and `Error text` fields.

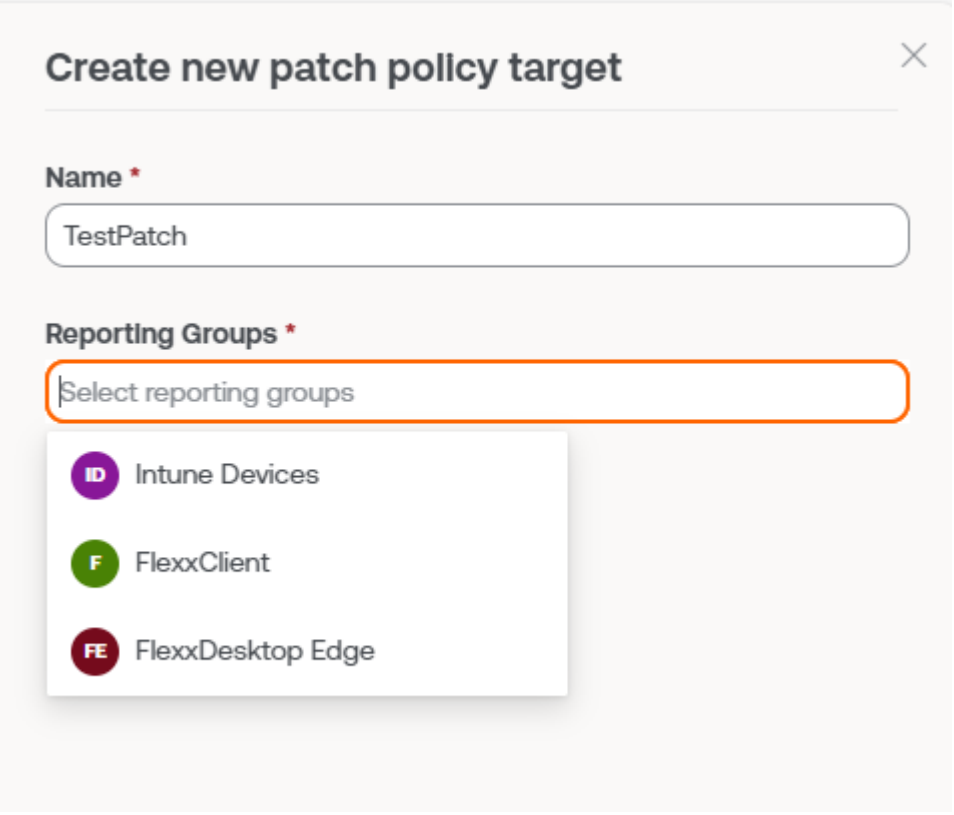
> **INFO**
>
> For more information on `Flows`, please refer to their documentation.

# Portal / Guides and tutorials / Patch policy

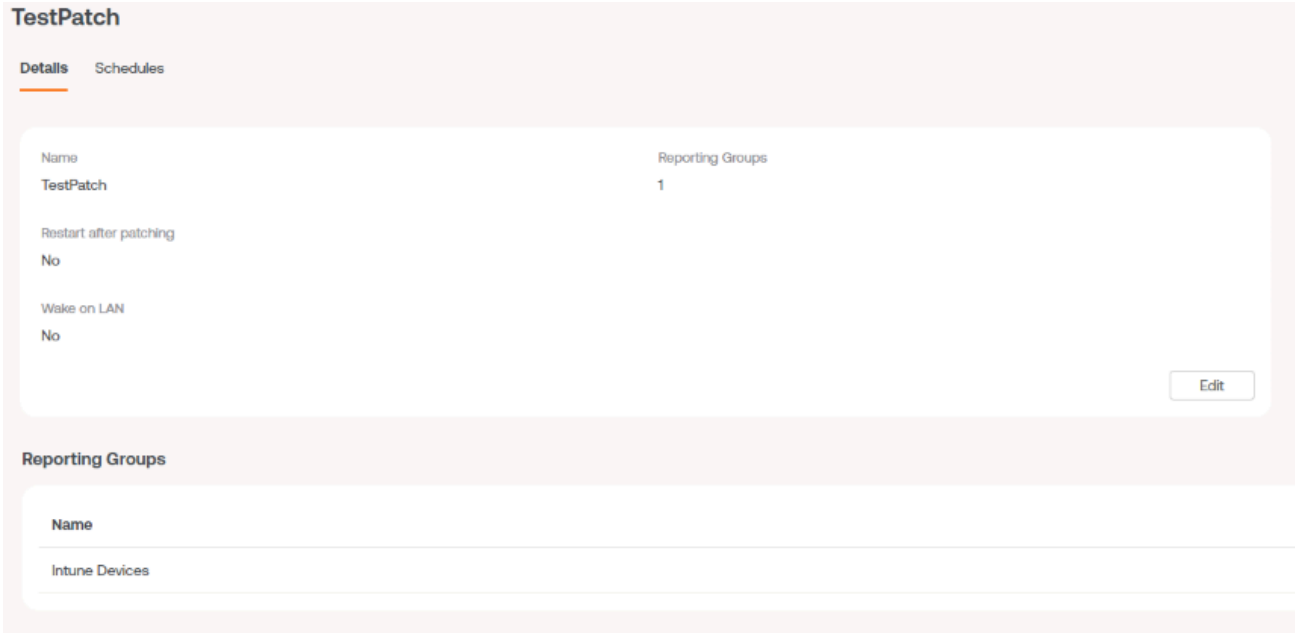
The patch policy indicates how the operating system patching of a set of devices belonging to a report group will be managed. Therefore, patching is not done on devices individually.

## How to define the patch policy

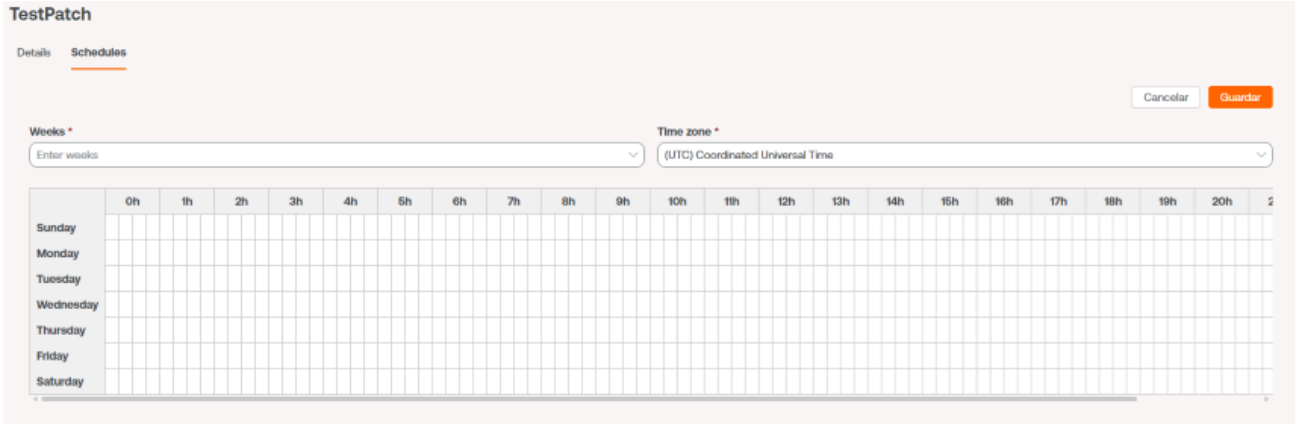
1. In the Portal menu, select the `Updates` -> `Recipients` option.
2. Create a new recipient by clicking on the `+ New` button (or select one from the list if you want to modify it). Give it a name and specify the reporting group to which this policy will apply, as well as whether you want to apply a Microsoft update directive.




3. Click on the `Save` button.
4. The information of the new policy will appear on the screen.




5. To change the behavior of the policy, you can use the `Edit` button, which allows you to:
    - Change the name of the policy.
    - Change the report groups to which the policy applies.
    - Select if the devices will restart or wake up via the network (`Wake on LAN`) after applying updates.
6. To change the scheduling of the patch policy application, go to the `Scheduling` tab -> `Edit`.



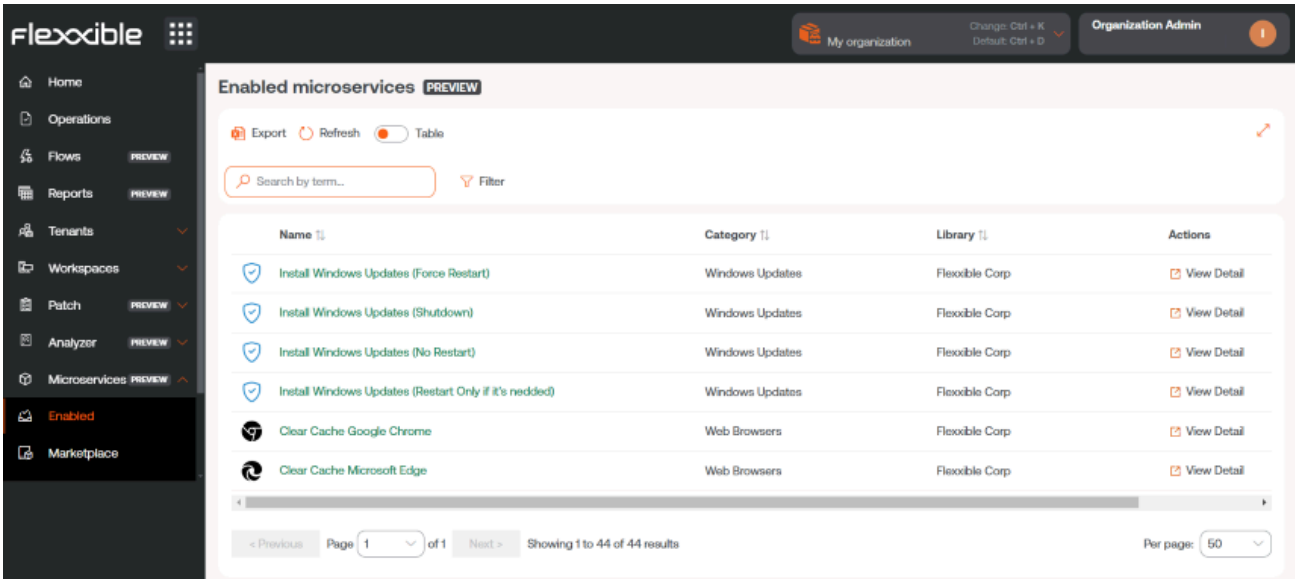

> **INFO**
>
> For more information about `Updates`, please refer to their documentation.

# Portal / Guides and tutorials / Enable a microservice for the end user

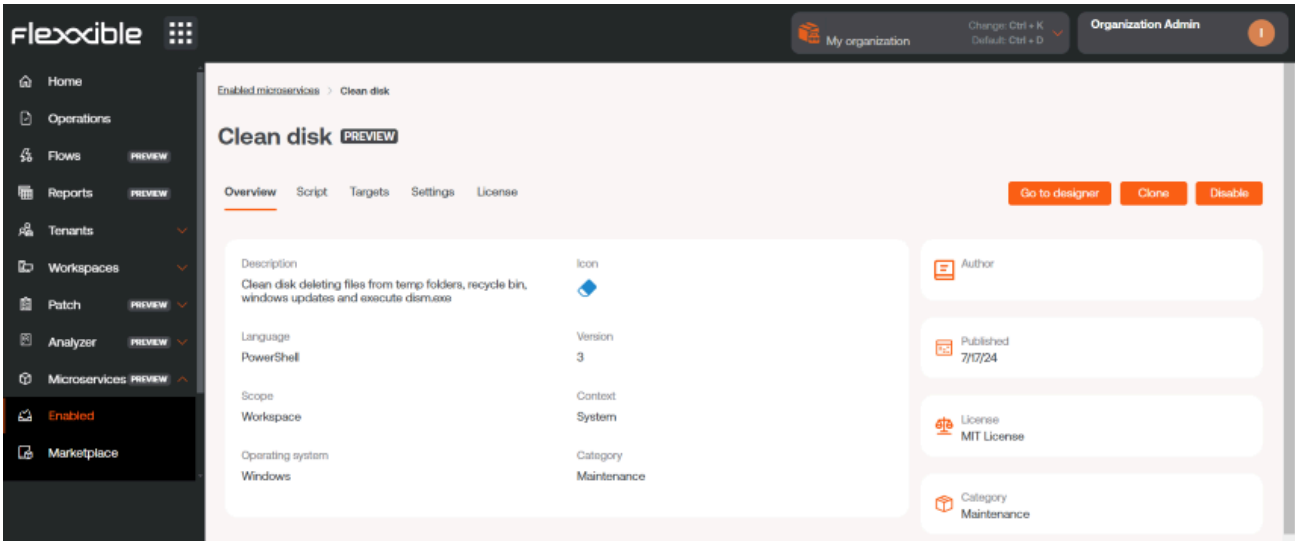
Microservices allow actions (queries or corrections) to be performed on devices, giving the end-user the ability to run them on-demand.

## How to enable a microservice for the end-user

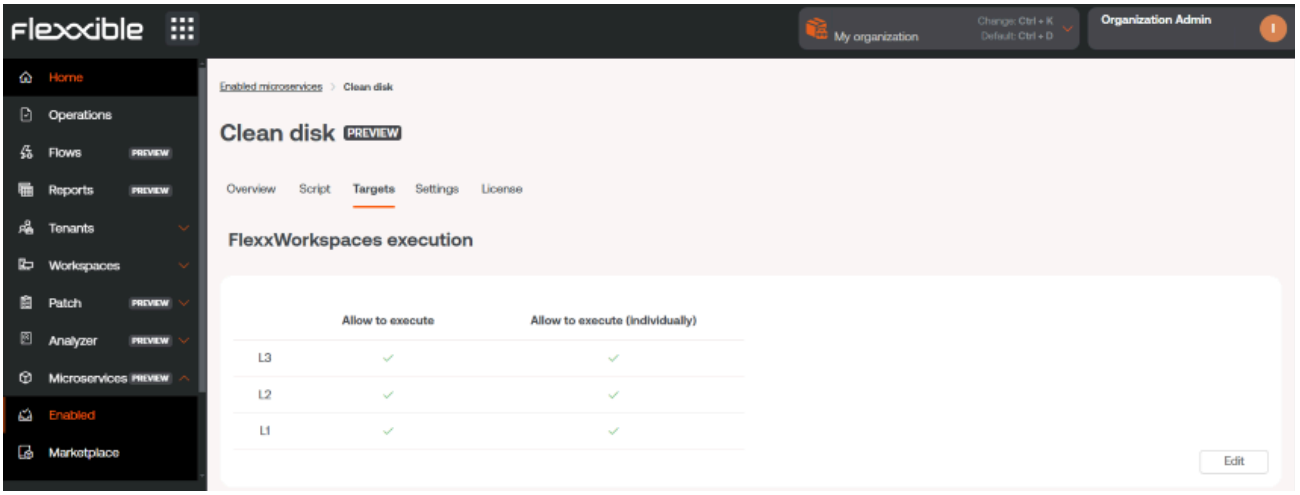
1. Access the `Microservices` -> `Enabled` menu within the Flexxible Portal (microservices can be organized either in blocks or lists).



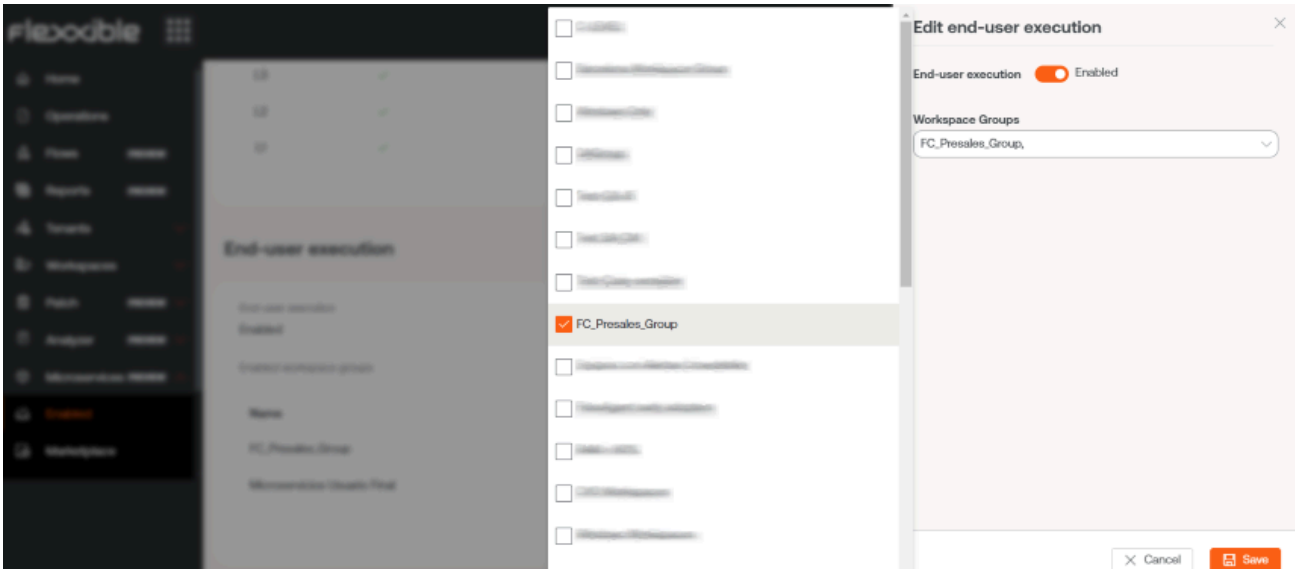

2. Select the microservice you want to enable by clicking on its name (if organized in blocks) or on the `See details` link (if organized in lists). Next, the microservice details will appear (in the example, “Clean Disk”).



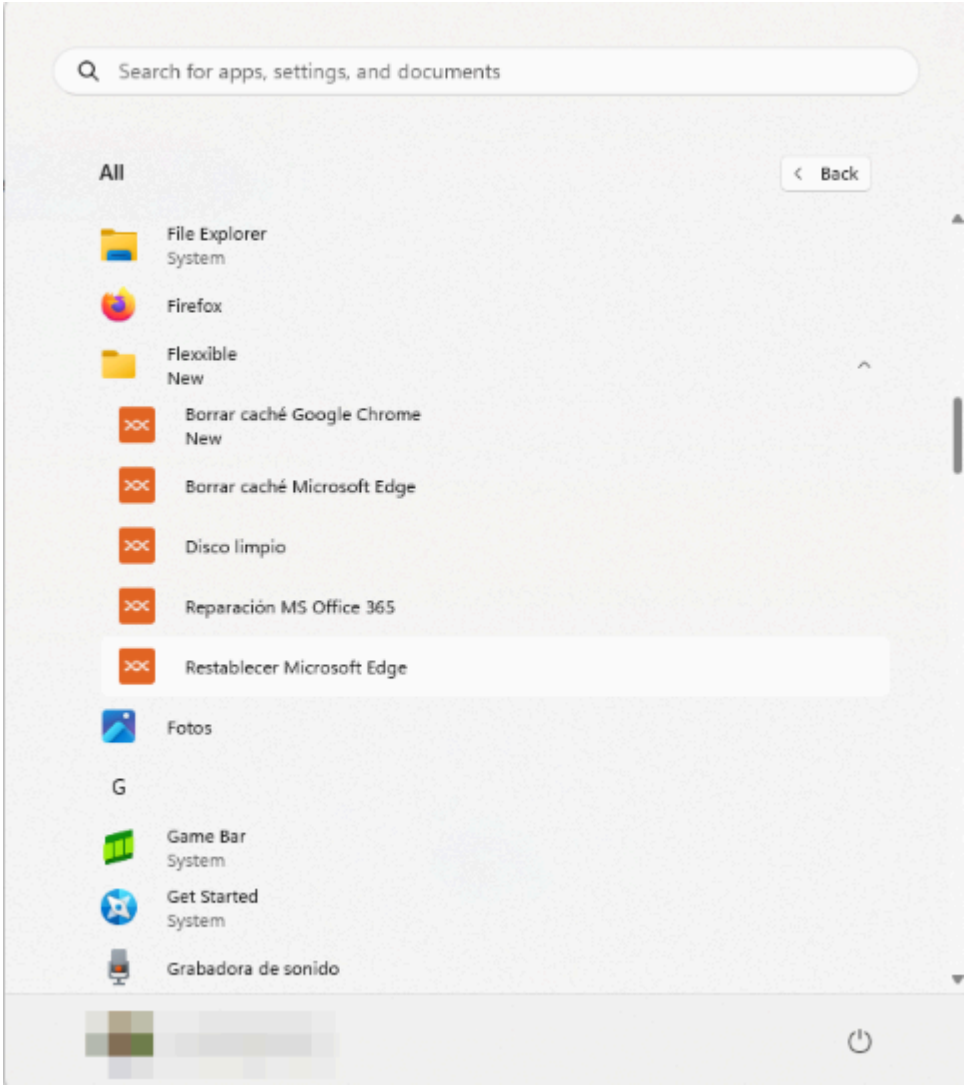

3. Select the `Recipients` tab, which shows the execution permissions and recipients of this microservice.




4. Click on the `Edit` button in the bottom right corner, within the `User Execution` section. A modal window with the configuration option will appear.




5. In the panel, enable the execution of the microservice by the end-user and select one or more `Workspace Groups` where this option will be valid. Once selected, click `Save`.
6. In the following minutes, the new microservice will appear as a new operating system option within the `Flexxible` folder in the start menu.




**INFO**

For more information about `Microservices`, please refer to their documentation.

# Workspaces

Workspaces is a unified support delivery solution and remote monitoring and management (RMM), where various tools for device management and automation and user interaction converge. Access to the module is segmented by levels, ensuring the provision of appropriate tools to each technical or support team through role assignment.

Workspaces is ready to manage user sessions from any technology, because FlexxAgent can identify the type of virtualization and brokering used in each session.

## Interface and Access Segmentation

The functionalities available in Workspaces are segmented into two levels, so access to them is granted through roles. Clicking on any level expands the menu options to access specific features.

### Level 1

It gathers the tools for the teams that have the most direct contact with end users. Includes views for UX Panel, Workspaces, Sessions, Connection Logs, Jobs, Alerts, and Profile Storage.

Functionalities available at this level:

- UX Panel
- Workspaces
- Sessions
- Connection log
- Jobs
- Alerts
- Profile Storage

### Level 2

Offers tools that enable a more detailed diagnosis, such as monitoring, event log filtering, server management, and more. Functionalities available at this level:

- Alert notification profiles
- Alert subscriptions
- Event log
- Notifications
- Servers
- Locations
- Networks
- Wireless networks

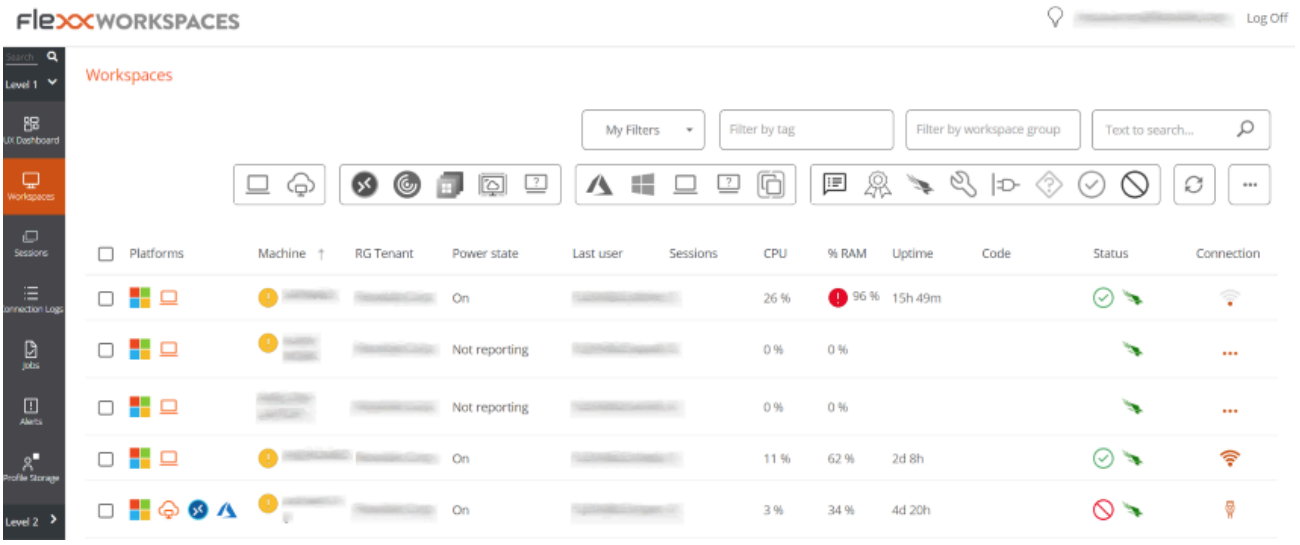
For FlexxDesktop deployments that use Azure Virtual Desktop subscriptions as a resource source for user sessions, the following features are included:

- Host pools (AVD)
- Power management policies (AVD)
- Power management activity (AVD)

## List Views

From the list views, items can be filtered and selected in the `Workspaces` and `Sessions` sections to obtain lists of, for example, devices with a certain uptime, with pending restarts due to updates, or that haven't been used within a specific time period, among others.

Based on filter results, specific tasks can be performed on devices or sessions, such as executing microservices, power actions, remote user assistance, and more.




In addition to filtering, list views also offer other options, such as exporting the listings and saving the applied filters as user filters.

# Filtering Options

To access the grouping and filtering options of the item list, right-click on the header of a column. Next, options will be displayed according to the sorting, grouping, visibility, and filtering of the columns.

#### Column sorting

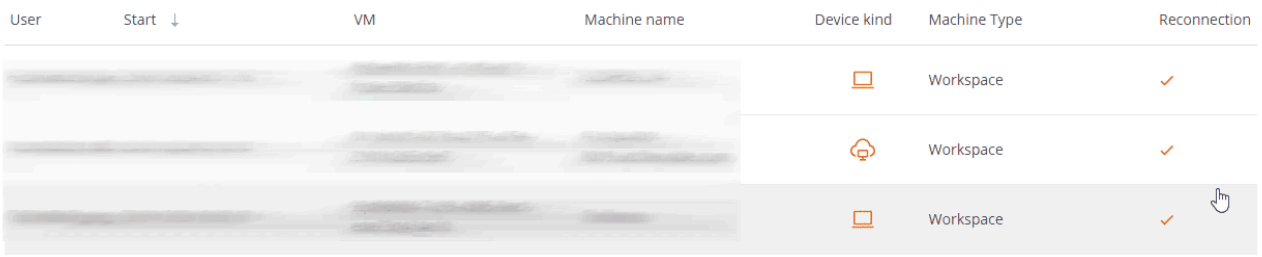
The options `Sort Ascending` and `Sort Descending` allow you to arrange the values of a column according to the letter or number they start with. For example, if the column `% RAM` is set to sort ascending, the column values will be arranged so that the first row corresponds to the device with the lowest percentage of RAM used and the last row with the highest percentage. Or if the column `Status` is set to sort descending, the first row will correspond to the device whose status is *Not reporting* and the last row will correspond to the device whose status is *Off*.

To reset the column sorting, click on `Clear sorting`.

#### Grouping by Column

The options `Group by this column` and `Group panel` allow creating a group of records for each value of the selected column field.

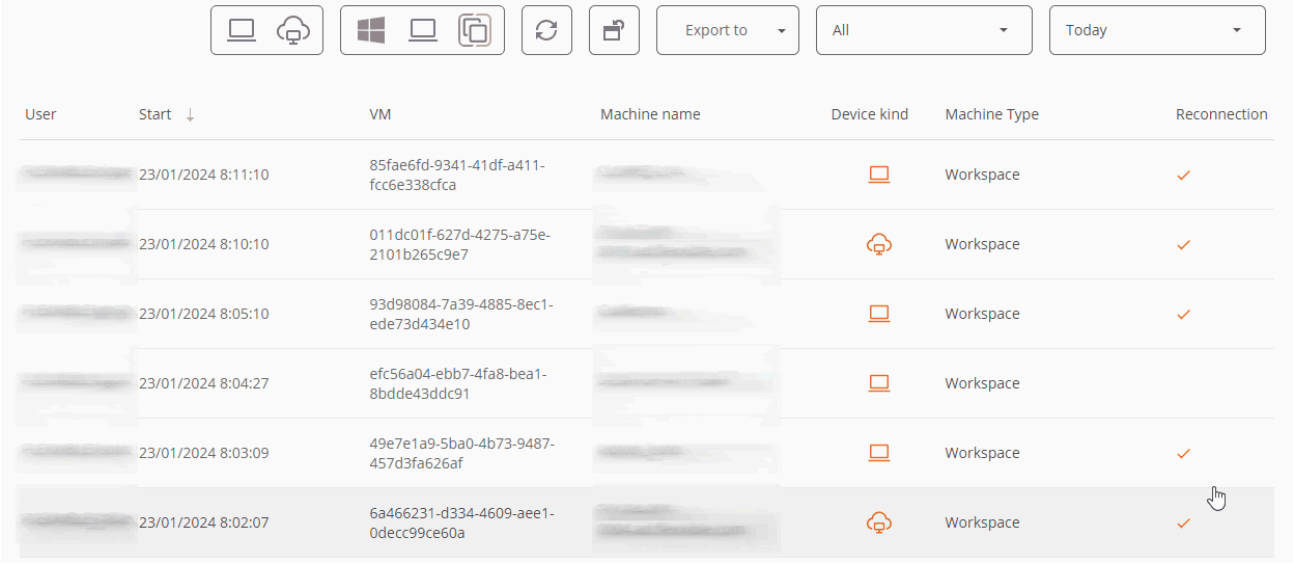
The difference between them is that `Group by this column` only considers the selected column for grouping the records, while `Group panel` allows selecting more than one column for grouping.




#### Column visibility

The options `Hide column`, `Show customization dialog`, and `Column selector` allow modifying the column visibility in the table.

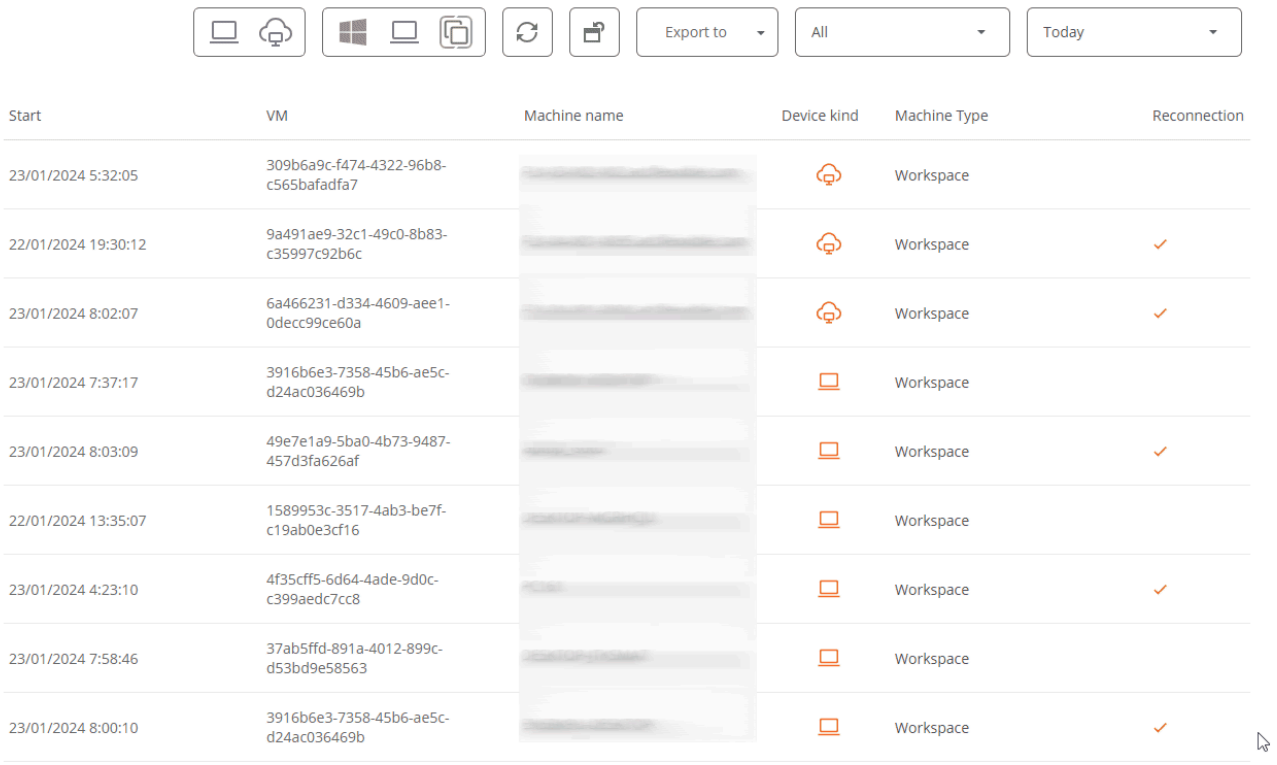
If the user doesn't want to see a particular column, they should go to its header, right-click and select the `Hide column` option. If they want to configure in detail which columns and records to view in the table, they should click on `Show customization dialog`. But if they prefer to add or remove columns, they can do so through `Column selector`.




#### Value filtering

The options `Filter editor` and `Filter row` allow setting filters according to the values of the column fields. If a user wants to build filters by multiple criteria (inclusive and

exclusive), analyze the content of fields, and nest queries, they should click on `Filter editor`. A user can also filter the field values based on the list shown by the table, to do this they should select the `Filter row` option.




When the `Footer` option is selected, the total number of records found is displayed at the bottom left of the table.

## Filter management

The `My filters` button offers the following options:

- **Predefined filters**: list of filters that Workspaces offers by default.
- **User filters**: option visible when a user has saved a filter. Allows applying the names of previously created filters.
- **Save the current filter**: if a user wants to return to a list of items later, after applying one or more filters, they can do so with this option.
- **Manage filters**: allows editing saved filters.
- **Clear filter**: useful when one wants to clear applied filters and reset the item list.

- **Workspaces groups**: visible in the `Workspaces` view, allows you to select items from the list and save them as Workspaces groups. More information here.
- **Filter by organizational unit (OU)**: visible in the `Workspaces` view, filters by organizational unit.
- **Filter by operating system (OS)**: visible in the `Workspaces` view, filters by operating system type.
- **Filter by installed applications**: visible in the `Workspaces` view, filters by installed applications.

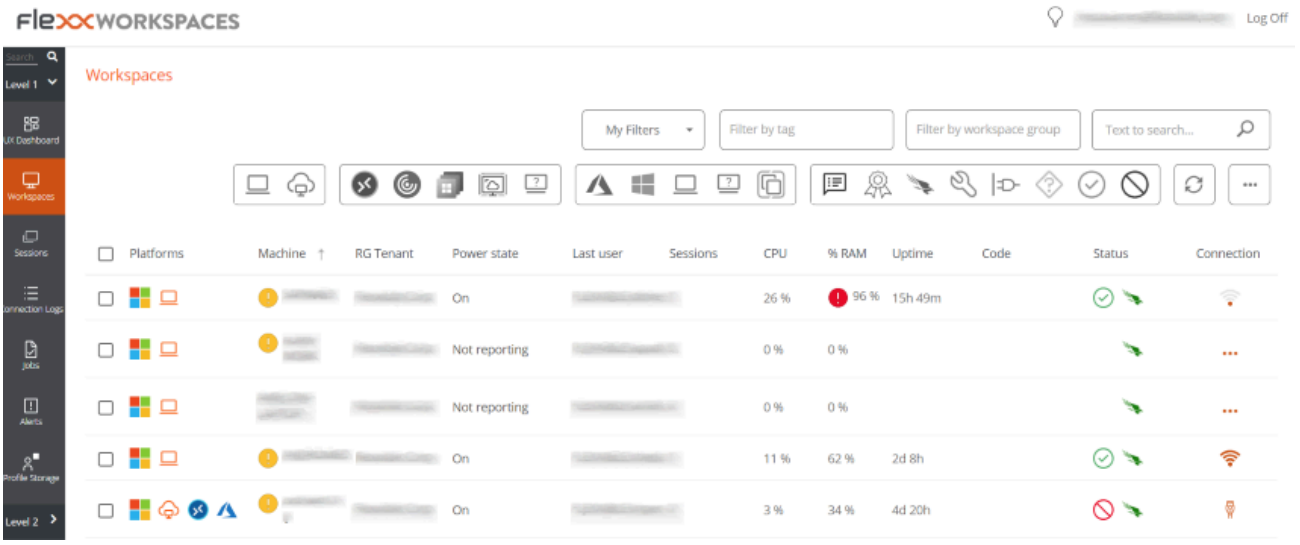
In the top menu, the icons allow:

- Set predefined filters
- Reset the default list view.
- Export the list: allows exporting the list with all details, in *.csv or *.xlsx format.
- In the `Workspaces` and `Sessions` views, execute microservices to perform actions on them. Depending on the view from which the `>-` button is activated, access will be given to different microservices, such as clearing the browser cache or updating the operating system.
- In the `Workspaces` and `Sessions` views, perform operations to facilitate their management. Depending on the view from which the `Operations` button is activated, access will be given to different actions, such as shutting down devices or launching a notification.

# Detail Views

From any Workspaces view, if you click on an item in the table, you can access detailed information. The data is organized into inventory blocks and tabs that facilitate navigation.

# Workspaces / Level 1



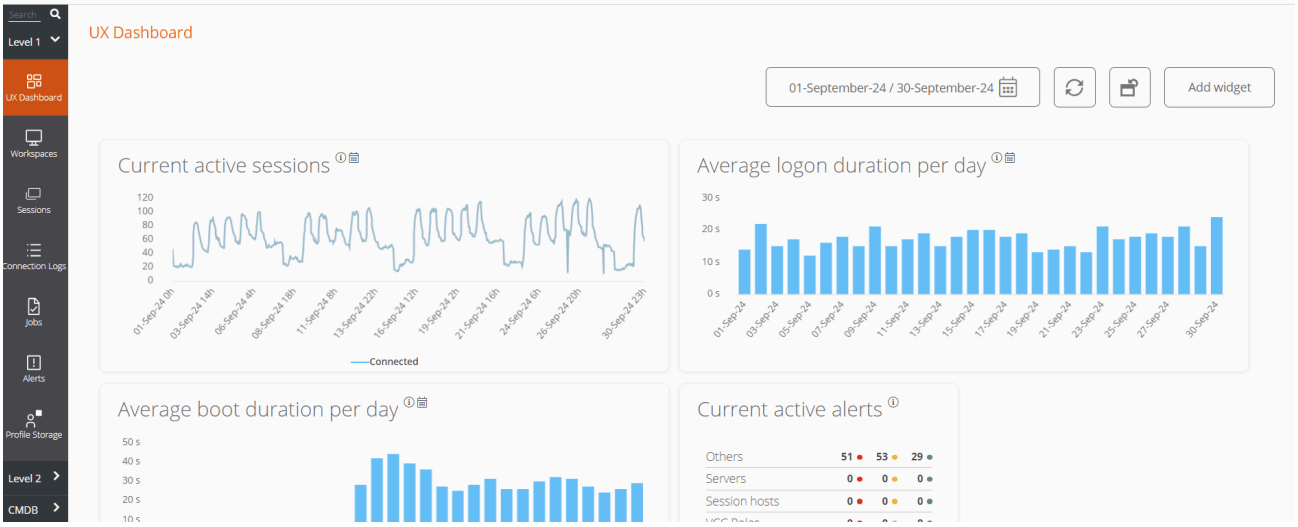

It gathers the tools for the teams that have the most direct contact with end users. It includes views of Dashboard UX, Workspaces, Sessions, Connections Logs, Jobs, Alerts, and Profile Storage.

Functionalities available at this level:

- UX Dashboard
- Workspaces
- Sessions
- Connections Log
- Jobs
- Alerts
- Profile Storage

# Workspaces / Level 1 / UX Panel

The Dashboard UX section allows you to graphically view the most relevant data of the environment, from inventory information, usage, locations, monitoring and much more.




The view is configurable and allows data segmentation by customer organization, date filtering, and selecting the widgets that will be part of the dashboard. The configuration of the widgets included in the dashboard, as well as their position and size, persists between user sessions, so this configuration only needs to be applied once.

## Organization filtering

By default, the organization selector located at the top right of the screen has the 'All tenants' option enabled, allowing the aggregated information of all organizations the user has access to in Workspaces to be viewed. To view the data of only one organization, it must be selected.

> Note: this selector is only visible when the user has access to more than one organization.

## Date filtering

The date selector button allows you to apply time filters to the dashboard data:

- Predefined filters:
  - Today
  - Yesterday
  - Last 7 days
  - Last 30 days
  - This month
  - Last month
- Custom filters that allow selecting start and end date and time.

# Widgets

The different information panels within the dashboard are called widgets, which can be repositioned, resized, or directly removed by clicking on the 'x' that appears when you hover over them.

## Default widgets

The widgets offered by default in Workspaces are:

#### Current active sessions

Aggregated concurrent active user sessions on the platform over time. This widget displays data filtered according to the date selector.

#### Average boot duration per day

Organization average boot time (boot) of their devices. This widget displays data filtered according to the date selector.

#### Average logon duration per day

Organization average login time (login) of their users. This widget displays data filtered according to the date selector.

#### Maximum concurrent sessions

Maximum number of simultaneous sessions on the platform during the last month, last week, and today (connected and disconnected users). This widget displays data for a specific time period. Therefore, it is not filtered by the date selector.

#### Active alerts

Summary of simultaneous active alerts related to different environment elements. Information alerts are shown in green, warnings in yellow, and critical alerts in red. This widget shows real-time data. Therefore, it is not filtered by the date selector.

#### Inactive users (last seven days)

Users who have ever connected to a session but did not connect during the previous seven days. This widget displays data for a specific time period. Therefore, it is not filtered by the date selector.

#### Workspace by ISP

A view of the different internet service providers in use by the workspaces. Since these are real-time data, date filtering is omitted.

#### Workspace by country

A view of the different countries from which the workspaces connect. Since these are real-time data, date filtering is omitted.

#### Number of Workspaces per Operating system

This widget shows real-time data. Therefore, it is not filtered by the date selector.

#### FlexxAgent version analysis

An analysis of the different versions of FlexxAgent used by the organization and selected operating system, so there is a widget for each supported operating system. This widget shows real-time data. Therefore, it is not filtered by the date selector.

#### Top 5 sessions by average duration by user

Top 5 average session duration by user on the platform over time. This widget displays data filtered according to the date selector.

#### Current sessions capacity

Displays information about the number of sessions that can connect according to the current load in AVD (Azure Virtual Desktop) environments.

- Number of session hosts: number of session hosts in the host pool.
- Users per host: number of users that accept each session host.
- Total sessions: number of maximum sessions according with the number of session hosts and the capacity of each one.
- Available: how many new sessions can connect
- Active: current number of active sessions
- Disconnected: current number of disconnected sessions
- Load: current load percentage of the session host according with the current usage and availability. This widget shows real-time data. Therefore, it is not filtered by the date selector.

#### Top 10 workspaces by current total used bandwidth

Top 10 workspaces sorted by the currently used bandwidth in KB/s. This widget shows real-time data. Therefore, it is not filtered by the date selector.

#### Current session host availability

Displays information about session host availability by host pool in AVD (Azure Virtual Desktop) environments.

- Session hosts: number of session hosts. -Available: how many session hosts are ready to accept new connections.
- %: percentage of session hosts that are available.
- Sessions not allowed: number of session hosts that are in drain mode and cannot accept new connections. This widget shows real-time data. Therefore, it is not filtered by the date selector.

#### Top 10 current most loaded pooled session hosts

Top 10 current most loaded pooled session hosts in AVD (Azure Virtual Desktop) environments. This widget shows real-time data. Therefore, it is not filtered by the date selector.

#### Average logon duration per pool/catalog

Average logon duration of users in the group (Azure Virtual Desktop) or catalog (Citrix environments). This widget displays data filtered according to the date selector.

#### Top 10 workspaces by current total sessions

Top 10 workspaces sorted by the current number of sessions. This widget shows real-time data. Therefore, it is not filtered by the date selector.

#### Average logon duration per operating system

Average logon duration per operating system. This widget displays data filtered according to the date selector.

#### Top 10 recent alerts

Top 10 most recent alerts, sorted by severity. This widget shows real-time data. Therefore, it is not filtered by the date selector.

#### Top 10 workspaces by current total RAM used

Top 10 workspaces sorted by the currently used RAM in GB. This widget shows real-time data. Therefore, it is not filtered by the date selector.

#### Current AVD resources

The number of Workspaces, Host pools, and app groups created in Azure Virtual Desktop. This widget shows real-time data. Therefore, it is not filtered by the date selector.

#### Disconnected Sessions

Aggregated concurrent disconnected user sessions on the platform over time. This widget displays data filtered according to the date selector.

#### Workspaces per broker

Number of workspaces by agent, grouped by broker. This widget shows real-time data. Therefore, it is not filtered by the date selector.

#### Workspace by city

A view of the different cities from which the workspaces connect. Since these are real-time data, date filtering is omitted.

#### Workspaces by wireless connection

A view of the different wireless connections in use by the workspaces. Since these are real-time data, date filtering is omitted.

#### Workspace by public ip address

A view of the different public IP addresses in use by the workspaces. Since these are real-time data, date filtering is omitted.

#### Workspaces per hypervisor

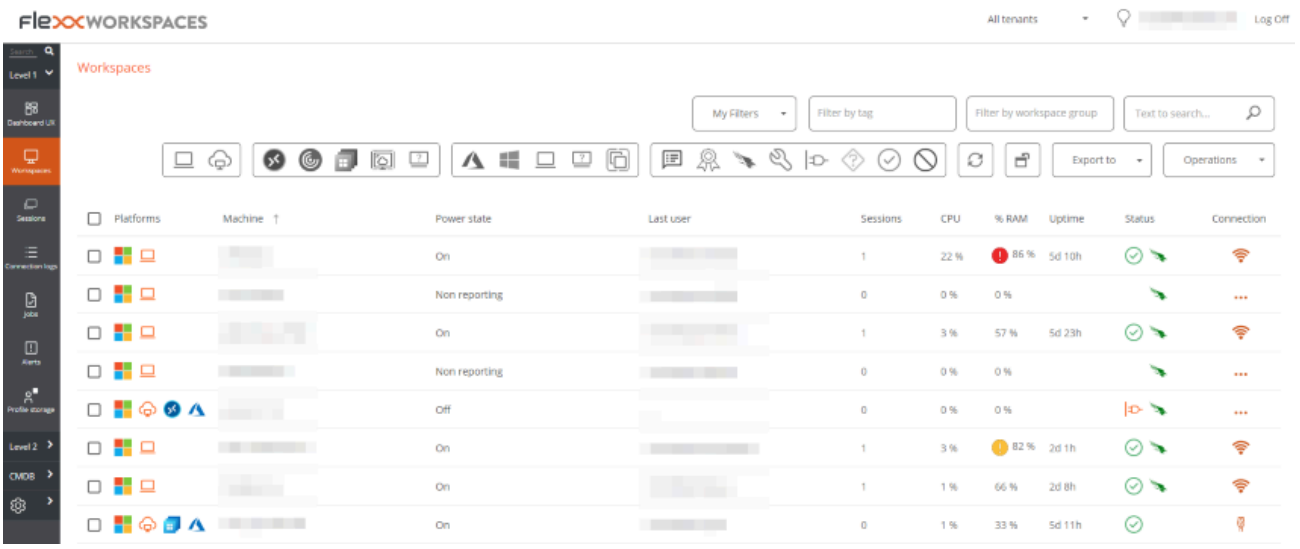
Number of Workspaces per hypervisor. This widget shows real-time data. Therefore, it is not filtered by the date selector.

#### Workspaces by operating system and build number

A ranking of operating system and build number combinations sorted by number of workspaces using each one. This widget displays data filtered according to the date selector.

# Workspaces / Level 1 / Workspaces View

The Workspaces list view allows access to the list of devices that make up the organization. From there you can organize, filter, search, and send operations to the devices.




## Filtering

The information displayed on the screen can be customized by adding or removing columns of information using `Column chooser` and saving the filters used for future queries in the user profile.

### Header filtering options

At the top of the screen, there are tools, icons for each attribute that allow you to filter the list based on the following criteria:

- Device technology filter:
  - Device kind: physical or virtual
  - Session broker used: Citrix, RDP or unknown
  - Hypervisor: Hyper-V, Nutanix, vSphere, physical or unknown
- Device state filter:

- The device has active notifications.
- The device is off.
- The device is in an unknown state for the broker.
- The device is in OK state.

Once a device is selected, or through multiple selections, the `Operations` button gives access to perform various tasks such as `Power and connection actions` or send `Notifications` to users. You can check the details of these functionalities in the section `Available actions`.

In `My filters` there are also additional filtering options that allow selecting devices according to the applications installed on them.

### List filtering options

The filtering options for the list view are available at Opciones de filtrado del listado.

### Filter management

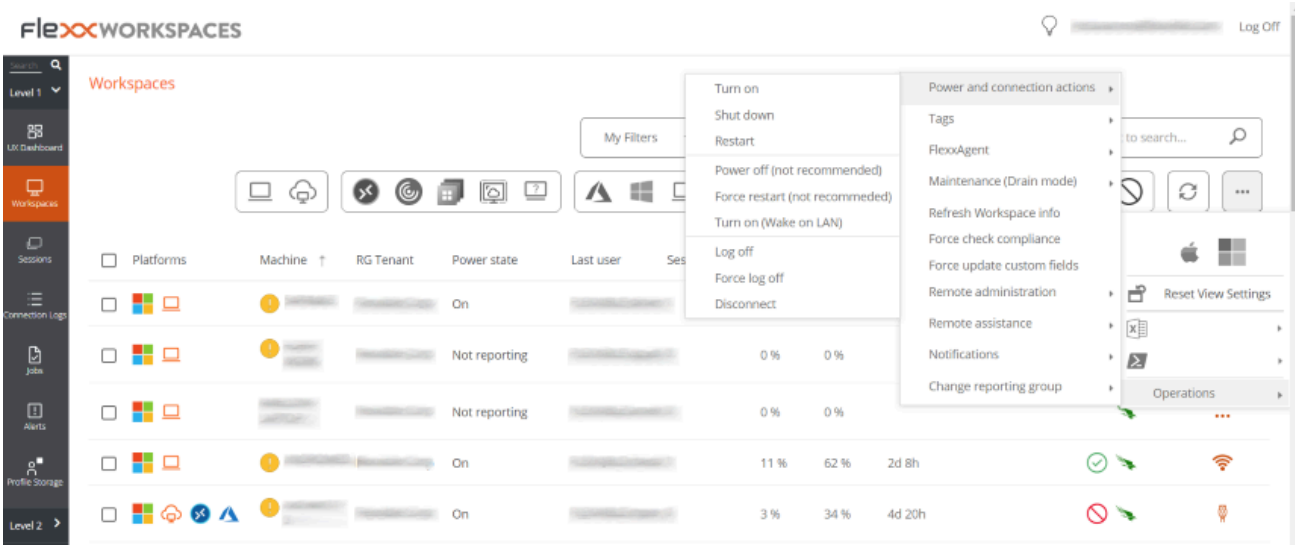
Filters created through interface options can be saved as user filters. They are located along with the predefined filters in the My filters option

## Microservices execution

From the `>-` button it is possible to execute any microservice enabled for the organization that has `System` as the configured context. This allows the execution of microservices with administrative permissions on the devices. The actions of enabling, creating, modifying, or deleting microservices are performed from the Portal.

## Available operations

Depending on the view from which the `Operations` button is activated (list view or detail view), access to different actions will be granted.




# Operations from the list view

From the Workspaces list view, the following operations can be performed on selected devices.

## Power and connection actions

- Power on: only available for devices with an associated broker.
- Power off the device.
- Reboot the device.
- Force power off: only available for devices with an associated broker.
- Force reboot: only available for devices with an associated broker.
- Power on (Wake on LAN): only available for physical devices that are compatible and configured to support remote power on via Wake on LAN.
- Log off user.
- Force log off user.
- Disconnect user session.

## Tags

Tags are keywords that can be assigned to one or more devices that share some common characteristic, in order to recognize and organize them for efficient management.

To assign one or more tags, first select the devices you want and then, in `Operations`, click `Add`. From here, the available tags, if any, will be displayed so they can be associated with the device.

From `Edit` you can change the tag or assign another to the device. And `Delete` disassociates a tag from this.

The `Filter by tag` option in the top menu of the Workspaces list view allows filtering devices by tag name so that actions can be performed on them simultaneously.

## FlexxAgent

Allows updating the agent on the selected devices to the latest version available.

## Maintenance (drain mode)

Only available for devices with an associated broker, it allows configuring maintenance mode (Citrix) or Drain (AVD) mode, which inhibits the login for new users on the configured hosts.

## Refresh device info

Allows refreshing data for the selected virtual devices with the Citrix and/or Azure broker, easily updating the brokering information of the device, and is very helpful in diagnosing `Unavailable` or `Unregistered` states.

This operation does not act on physical devices. And it requires configuring a subscription to the broker from Workspaces.

## Force compliance check

Forces regulatory compliance evaluation at the moment and allows evaluating compliance on the device after making the necessary corrections, without waiting for the refresh time configured in the regulatory settings.

## Force update custom fields

Forces the retrieval of custom fields configured in settings. This option allows updating on demand, without waiting for the refresh configured in settings.

## Remote Administration

Allows running the Microsoft remote connection, delivering an .rdp or .rdg file. This option is only available for environments connected to Azure Virtual Desktop subscriptions and with Workspace console deployment within the same subscription (also requires network level connectivity Workspace -> Session Hosts).

## Remote Assistance

Allows launching three types of remote assistance:

- Interactive: requires user consent to view and take control of their session.
- Unattended: allows administrative access to server or self-service type devices that do not necessarily have a user on the other side of the screen.
- Dynamic: allows an operator to act on a device regardless of whether the user has an active session at that moment.

> **INFO**
>
> On multi-session devices, dynamic remote assistance will only work if there is a single concurrent remote assistance session on the device.

## Machine type

Allows defining the device type for selected devices so they can be organized in different console views. Available options:

- Workspace: type of physical device used by a user. It is visible in the `Workspaces` section.

- **Workspace (AVD Session Host)**: type of virtual device hosted in Azure Virtual Desktop used by a user. It is visible in the `Workspaces` section.
- **Server**: type of physical or virtual device that serves multiple users within the organization or its infrastructure. It is visible in the `Servers` section.
- **Hidden**: allows hiding a device from all lists.

## Notifications

Allows sending notifications to selected devices. These can be pop-up notifications or those that reserve part of the screen.

## Change reporting group

This option allows changing the selected devices' reporting group. When changing, the target reporting group configuration will be applied, which includes:

- Remote Assistance configuration
- Organization users with access and/or visibility
- Associated patching policy

If the user changing the report group on the devices has access to more than one organization, they can also "move" the devices to a report group in another organization.

# Workspaces / Level 1 / Workspaces / Detail view

Clicking on the name of a device in the Workspaces list view opens the device details. The interface is structured into four sections:

- Available actions
- General information
- Detailed information
- Tabbed information

## Available actions

The detail view allows you to perform the same actions on the active device as in the list view, except for updating FlexxAgent, as well as other actions that are only available in this view.

Available actions:

- Microservices execution
- Perform actions included in the `Operations` button

### Microservices execution

From the `>-` button it is possible to execute any microservice enabled for the organization that has `System` as the configured context. This allows the execution of microservices with administrative permissions on the devices. The actions of enabling, creating, modifying, or deleting microservices are performed from the Portal.

### Operations

From the detail view of a device you can perform the same `Operations` as in the list view, as well as `Edit`, `Session Analyzer log tracking` and `OS Patching`.

#### Edit

This operation allows the user to assign an identification code to a workspace and/or a description.

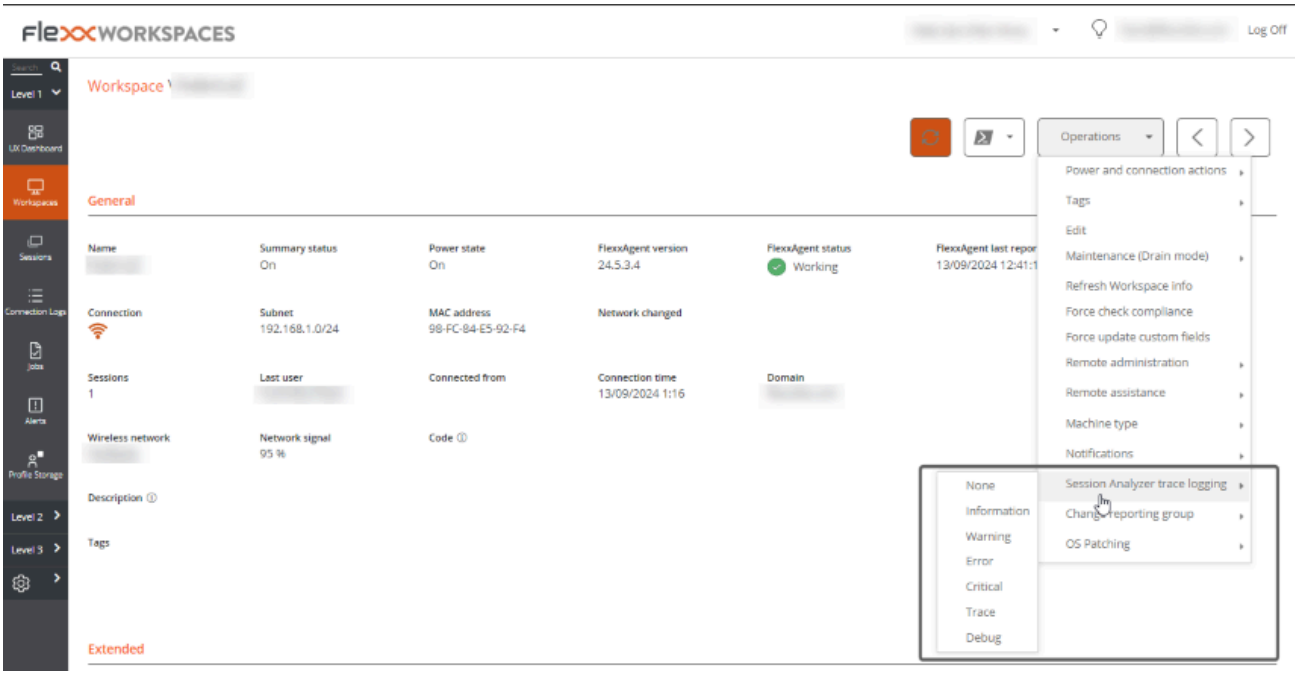
The code allows associating the device with an inventory item. To edit it, click on `Operations` -> `Edit` -> `Code`.

The `Description` field allows adding free text as a description or notes to the device.

When the code and/or description are defined, they will be visible in the general information block of the device, and it will be possible to filter by these fields in the list views.

#### Session Analyzer trace logging

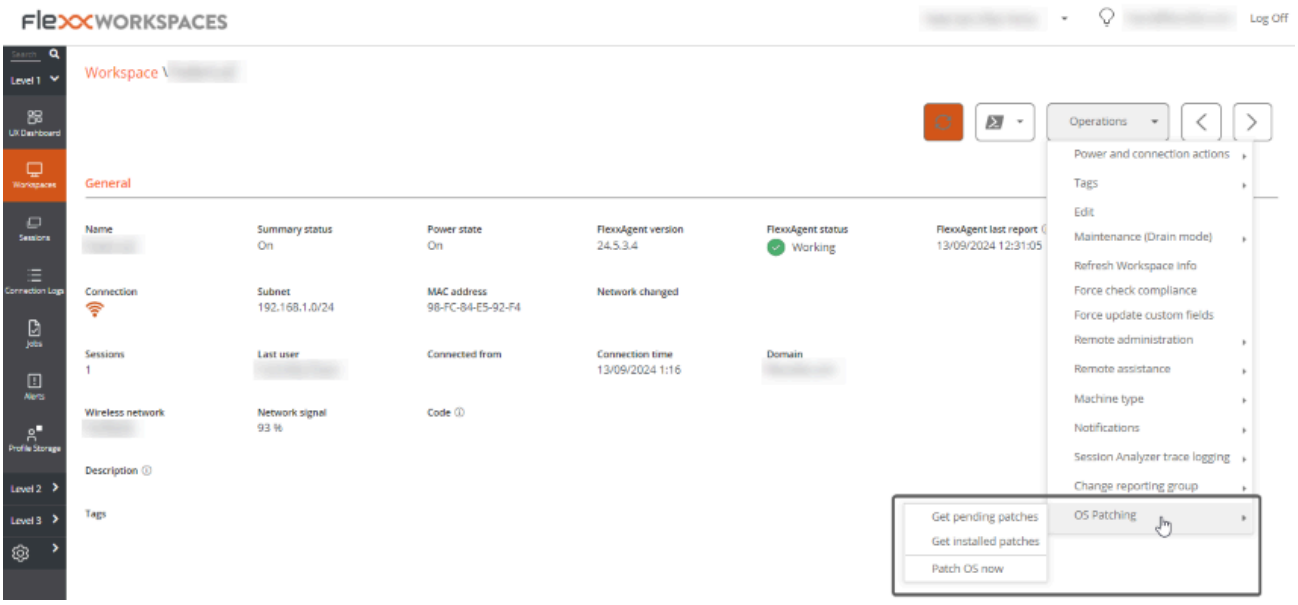
FlexxAgent Analyzer logs can be configured to include or exclude information by criticality levels. From `Operations` -> `Session Analyzer trace logging` you can manage the log level change for FlexxAgent Analyzer.




These logs are stored in the directory `%LOCALAPPDATA%\FAAgent\Logs`.

#### Operating system update

This option allows managing the update of the device that uses Windows as the operating system.




Available options:

- **Get pending patches**: retrieves, in list format, the patches available for installation on the device.
- **Get installed patches**: retrieves, in list format, the patches installed on the device.
- **Patch now**: installs the pending patches on the device.

For all patches, `Id`, `Installation/publication date`, `Severity`, and the `Title or name` of the package are obtained.

# Information obtained from the device

The general, detailed, and tabbed information collected by FlexxAgent varies according to the device's operating system type:

- Windows
- Linux
- macOS
- ChromeOS

- Android

# Workspaces / Level 1 / Workspaces / Remote Assistance

Workspaces includes remote assistance tools so that an operator can efficiently access a device and take control of the user's session to solve problems and make system changes.

The operator can manage all the applications the user sees, including those requiring elevated permissions, launched with *Run as administrator* or executed under User Account Control (UAC).

## Features

- It supports all types of sessions, such as users on physical devices, VDIs, shared desktops, and even in virtualized application environments.
- Remote assistance works with or without a proxy.
- It is designed to cover end-user devices and devices that do not have a user in front of them, like servers or kiosk-type customer service devices.
- It supports devices running Windows as an operating system.
- Thanks to its configuration options, it can be used for quick remote assistance sessions with users and as a remote access mechanism to infrastructure devices, like servers.

> **INFO**
>
> To minimize the attack surface, exploit vulnerabilities, and maintain device security, FlexxAgent does not install any additional software, so there is no service "listening" for incoming connections. The process runs only (without installation) in real-time when requested from Workspaces.

## Types of remote assistance

There are three types of remote assistance:

- Interactive remote assistance
- Unattended remote assistance
- Dynamic remote assistance

# Interactive remote assistance

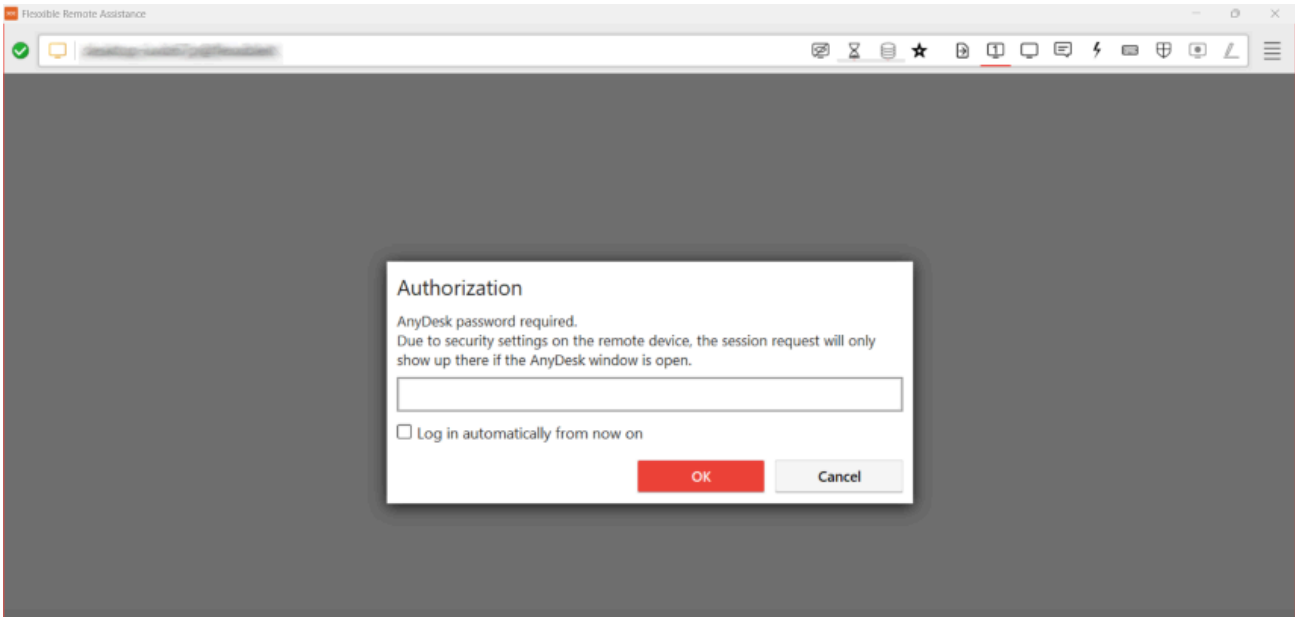
Interactive remote assistance is aimed at end users. Allows a support operator to access the user's session to see what is happening on their screen or take control easily. This type of assistance requires user consent.


# Unattended remote assistance

Unattended remote assistance allows access to server type or self-service kiosk computers, where no specific user is working.


When the operator performs this action, Workspaces sends the order to FlexxAgent to install a custom Flexxible service, start it up, set up an access password, and inform the operator through the console that the session is already accessible with its respective authentication data:

- Session ID: session identifier.
- Password: dynamic password that regenerates with each session, it is not recommended to store it.
- Download the remote assistance access file for the operator.




Once the access file is activated by the support operator, you will need to enter the session password to take control of the device.

> **INFO**
>
> After 15 minutes since the end of the unattended remote assistance connection, it will no longer be possible to reuse the same authentication data or access file. The service will be deactivated from the device and the session password will have expired.

# Dynamic remote assistance

Dynamic remote assistance allows an operator to act on a device regardless of whether the user has an active session at that time.

When a dynamic remote assistance is launched, FlexxAgent checks the active sessions on the device; if there is any, it launches the interactive remote assistance process. On the contrary, if there is no user session active, it will trigger the unattended remote assistance process, allowing the operator to access the device to perform maintenance tasks, even using other user accounts to log in, without interfering with the user's session or data.

> **INFO**
>
> When a device is configured to receive dynamic remote assistance, the operator will not have the option to launch an unattended remote assistance process on any session of the device from the `Sessions` view.

To receive dynamic remote assistance, the device receiving the assistance must have version 24.9.2 or higher of FlexxAgent installed.

Although the reporting group to which the device belongs has been configured to receive **dynamic remote assistance**, Workspaces will display the three options to start remote assistance: interactive, unattended, and dynamic. In that specific case, the operator will not be able to activate interactive or unattended remote assistance. If attempted, Workspaces will display an error message.

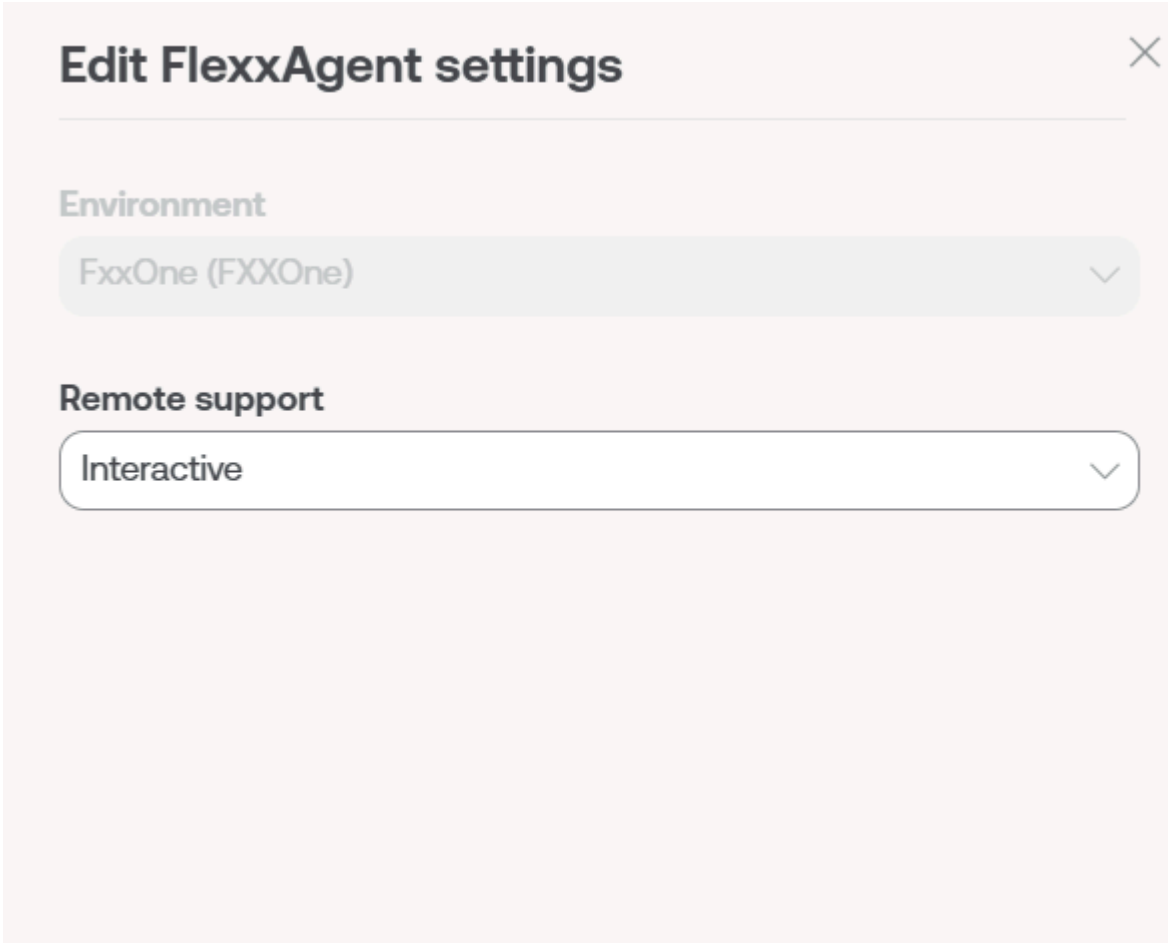
# Requirements to perform remote assistance

- The device receiving remote assistance must have **FlexxAgent 23.7 or higher** installed (24.9.2 or higher for dynamic remote assistance).
- Connectivity of the devices to https://ras.flexxible.com, via TCP port 443.

> **INFO**
>
> If FlexxAgent restarts during a remote support session, the session will be interrupted.

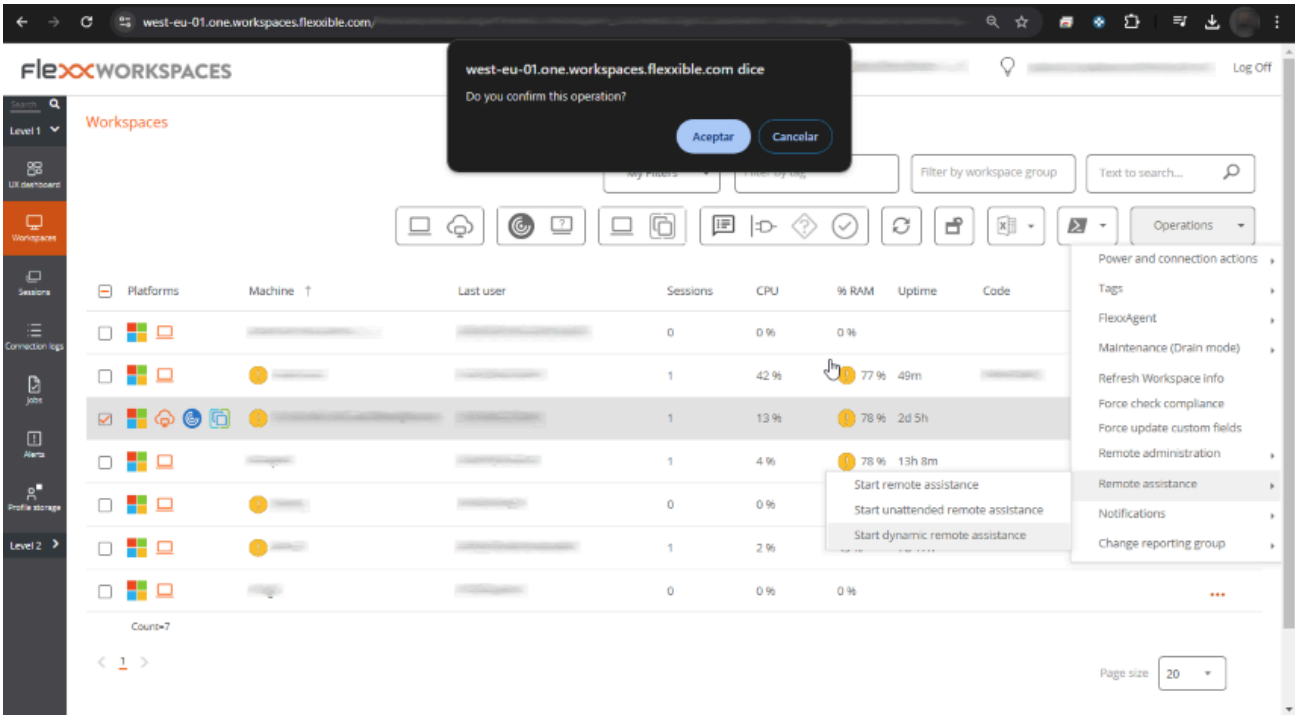
# Settings

For a device to receive remote assistance, it must be configured from the FlexxAgent Settings (Remote Assistance) of its reporting group. From there, you can choose which type of remote assistance devices will have access to.




# Activation

Once the configuration is done, from the support side, when you want to activate remote assistance on a device, it should be done from the `Workspaces` module, having previously selected the device to be assisted. `Level 1` -> `Operations` -> `Remote Assistance`. And then choose the type of remote assistance to be provided: interactive, unattended, or dynamic.




The remote assistance operation can be activated both from the `Sessions` view and from `Workspaces`.

When the operator launches the `Start remote assistance` request, FlexxAgent initiates a process (with the user's permissions) on the device and notifies the user.

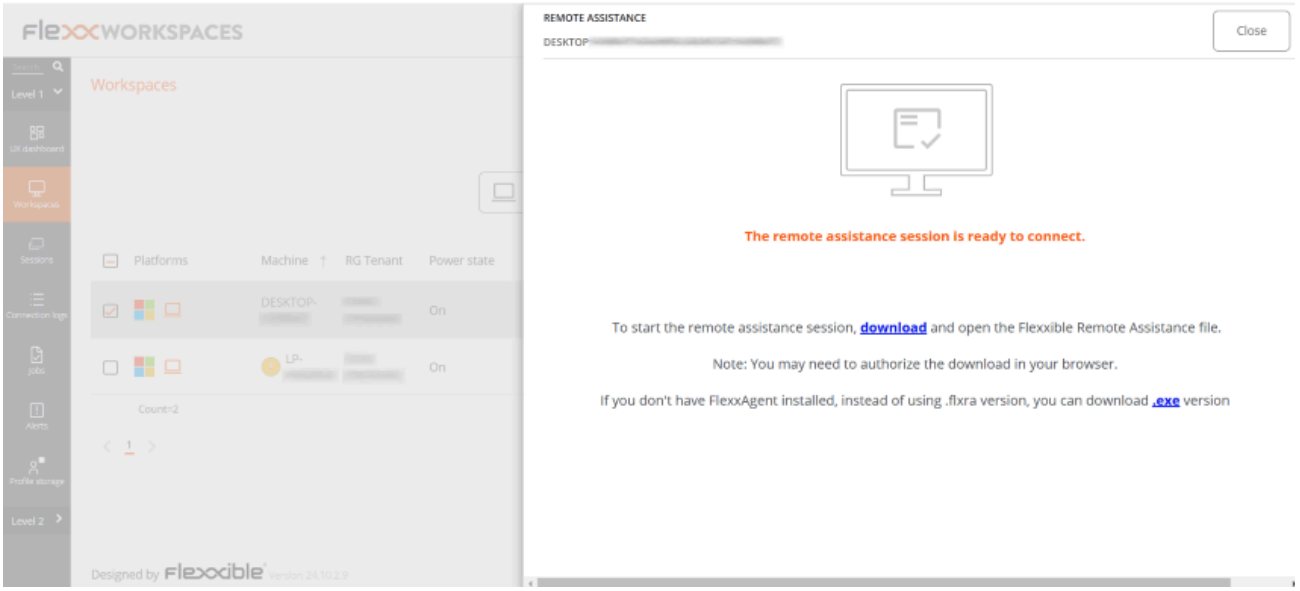
# Activation file download

The support operator needs to download an activation file to provide the remote assistance service. The type of file will depend on whether the device providing support has FlexxAgent installed or not.

#### File for devices with FlexxAgent installed

If the support operator's device has FlexxAgent installed, they should download the Flexxible Remote Assistance file, with the extension ".flxra", and run it by double-clicking on it.

This file will run with the user's permissions, without installation, and will remain active for the duration of the remote assistance session. Once the session is over, the process will be stopped and the file will be automatically deleted from the filesystem.

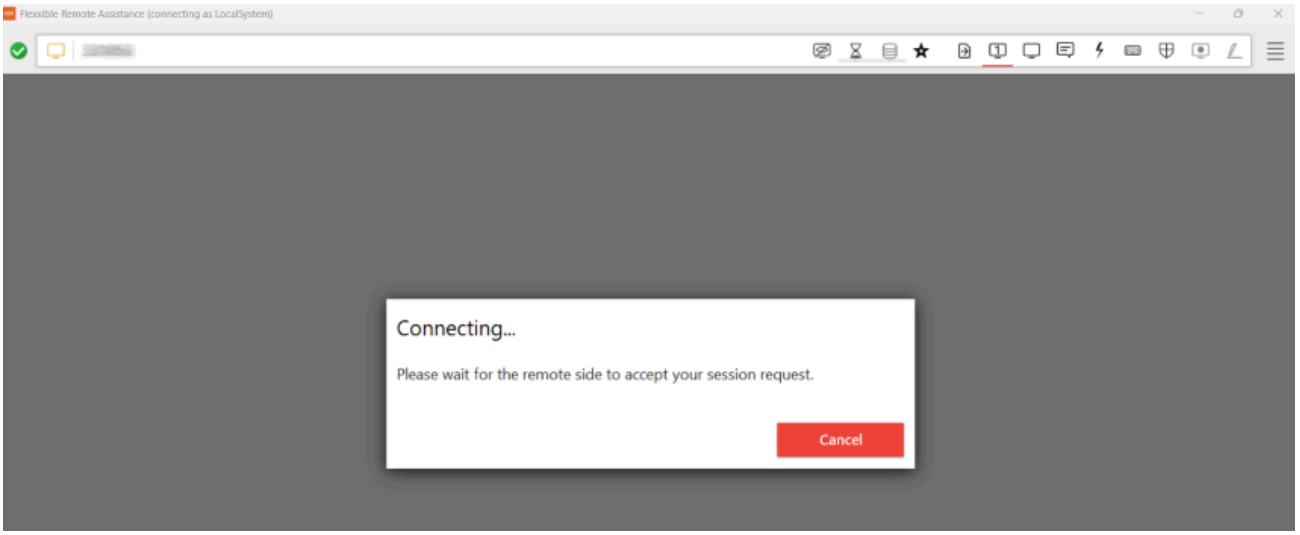



#### File for devices without FlexxAgent installed

If the support operator's device does not have FlexxAgent installed, they should download the file with the ".exe" extension and run it by double-clicking on it.

This file will run with the user's permissions, without installation, and will remain active for the duration of the remote assistance session. Once the session is over, the process will be stopped, but the file will not be automatically deleted from the filesystem.

Next, in both cases, the consent request will be sent to the user.




Wait for the user's consent.

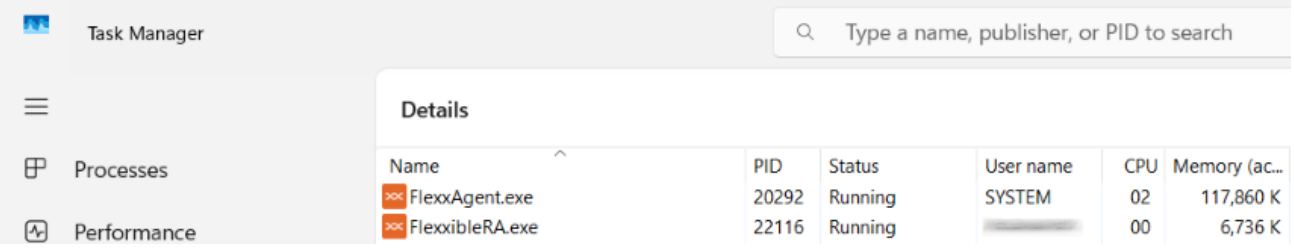

Once remote assistance is accepted, the support operator can gain control of the session.

> **INFO**
>
> Even if the file is executed without administrative permissions, access is not denied to the administrative tools needed for support delivery. These are in the `Flexxible Tools` menu, in the upper left corner of the remote assistance window.

# Processes

When the operator downloads the remote assistance file from Workspaces, the following processes will be generated and run automatically:

- FlexxAgent.exe
- FlexxibleRA.exe




# Behavior of remote assistance through proxy

From the operator's perspective, the operation is as follows:

- When executing the ".flxra" or ".exe" file, it is checked if the Proxy_Url key exists in the FlexxAgent keys. If yes, it uses it if accessible. Otherwise, the AnyDesk binary is launched with autodetect.

From the end user's perspective, when remote assistance is performed:

- FlexxAgent will detect if the proxy is configured, if it detects it and is accessible, it uses it. Otherwise, the AnyDesk binary is launched with autodetect.
- If the proxy configuration registry keys do not exist, it will detect if the operating system has the proxy configured. If it detects it and it is accessible, it uses it.

Otherwise, the AnyDesk binary is launched with autodetect.

# Flexxible Tools

The remote support file runs with the user's permission level; however, the user may not have local device admin privileges. To cover these cases, `Flexxible Tools` has been incorporated.

Flexxible Tools allows activation of administrative tools in remote assistance. These are a series of embedded functions that can be accessed from the top left of the interface.


These tools can be executed with the following administrative permissions:

- CMD
- PowerShell
- Registry editor
- Task Manager

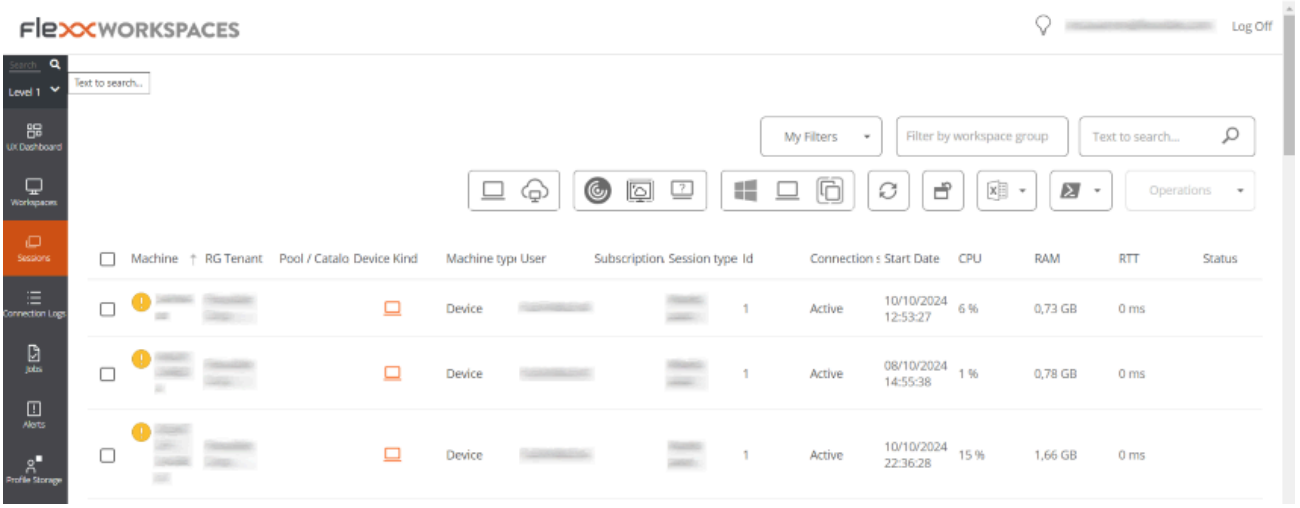
If the user has permissions on the Portal, Flexxible Tools can be activated for users by role. This can be done in two ways:

- From `Portal` -> `Configuration` -> `Products`: for each product in the list, there is a `FlexxAgent Configuration` button that allows applying the change to all reporting groups.
- From `Portal` -> `Configuration` -> `Reporting Groups`: for one or several reporting groups, functionality can be activated or deactivated.

> **INFO**
>
> The proper functioning of Flexxible Tools requires that both the operator's device and the device receiving remote support have FlexxAgent installed from the same environment.

# Workspaces / Level 1 / Sessions

The `Sessions` view allows you to organize, filter, search, and send operations to active user sessions.




The information displayed on the screen can be configured by adding or removing columns of information using the `Column Selector` and saving the filters used for future queries in the user profile.

## Header filtering options

In the upper right area of the screen, you will find tools and icons for each attribute that, when clicked, allow you to filter the list based on the following criteria:

- Session device type: physical or virtual.
- Session broker used: Citrix, RDP, or unknown.
- Hypervisor: Hyper-V, Nutanix, vSphere, physical or unknown.

Once the session is selected, or through multiple selection, the `Operations` button gives access to perform various session management tasks such as `Power and connection actions` or send `Notifications` to users. You can check the details of these functionalities in the section Actions on devices.

## List filtering options

The filtering options for the list view are available at filtering-options-in-listings.

### Filter management

Filters created through interface options can be saved as user filters. They are located alongside predefined filters.

## Available operations

The `Operations` button allows you to perform the following operations:

### Session management

The first three buttons of the `Operations` menu allow you to perform session management actions:

- Log off.
- Force log off.
- Disconnect the session.

### Remote Assistance

Allows launching remote assistance to users in interactive mode, which requires user consent to view and take control of their session; or execute unattended remote assistance, which allows administrative access to server or self-service type devices that do not necessarily have a user on the other side of the screen.

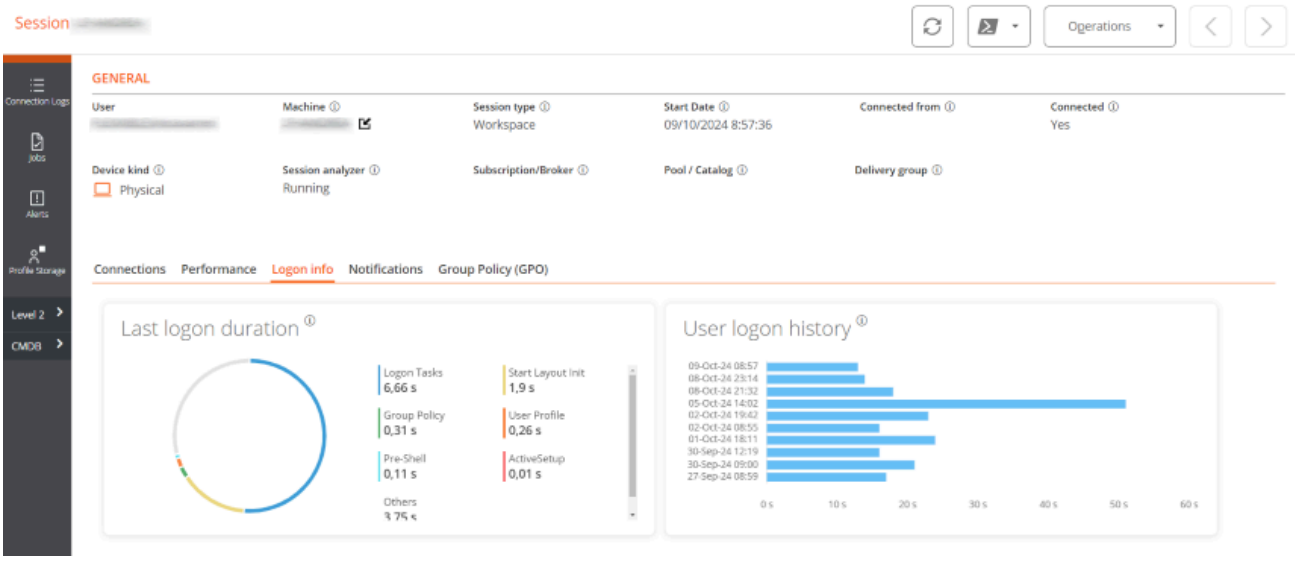
### Notifications

Allows sending notifications to selected devices. Notifications can be pop-up notifications or notifications that reserve a screen area.

**INFO**

In some devices with Windows 10 1903+, the Automatic Restart Sign-On (ARSO) may generate ghost sessions in the session view after an update reboot. To adjust this behavior, please refer to this guide.

# Workspaces / Level 1 / Sessions / Detail view




When clicking on a record in the session list, you access the details of the selected session. The interface is structured into 3 sections:

- Available actions at the top
- General information
- Specific information segmented into tabs at the bottom

## Available actions

From the device detail view, it's possible to perform the same actions as in the list view for the active device. This includes:

- Microservices execution.
- The actions included in the `Operations` button

### Microservices execution

From the `>-` button, you can execute any of the microservices enabled for the organization that have `Session` as a configured context. This allows the microservices to

be executed under the user's identity. The actions of enabling, creating, modifying, or deleting microservices are performed from the Portal.

## Operations

From the `Operations` button, you can execute the actions detailed in Available Operations for the active device.

# General

The general information block of the device contains:

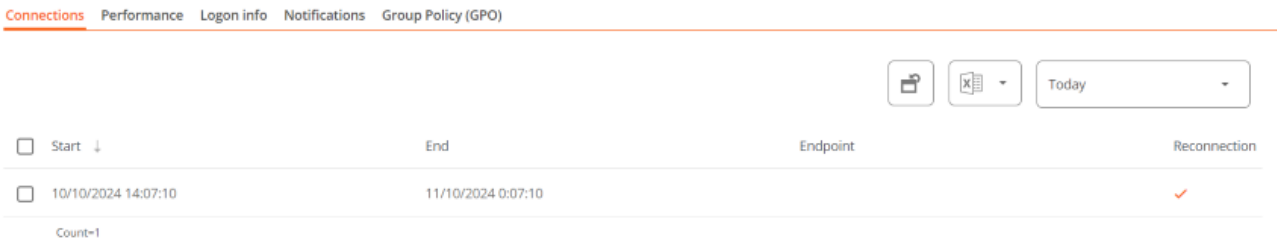
- **User**: User of the session in domain\user format.
- **Machine**: Device hostname.
- **Session Type**: Session type, which can be Workspace or application for virtualized application sessions.
- **Start Date**: Date and time of session establishment.
- **Connected From**: When the selected device is a VDI or similar, it shows the endpoint name from which the virtual device is accessed.
- **Connected**: Indicates whether the user is actively connected to the session, or has disconnected from it, otherwise.
- **Device Type**: Which can be virtual or physical.
- **Session Analyzer**: Indicates whether the FlexxAgent session analysis process is active or inactive.
- **Subscription/Broker**: If used, the Microsoft Azure or Citrix service that manages user connections to the workspace (i.e. Microsoft Azure Virtual Desktop (AVD), Citrix DaaS, Citrix On-premises).
- **Group / Catalog**: If used, a collection of machines that defines the specifications of the workspaces and how they are provisioned to users (e.g. e.g. host pools in Azure Virtual Desktop or machine catalogs in Citrix).
- **Delivery Group**: If detected, a collection of machines is selected from one or more machine catalogs. It specifies which users can use those machines, plus the applications and desktops available to those users.

# Tabs

The tabs at the bottom show specific grouped information, including the following tabs:

- Connections
- Performance
- Login information
- Notifications
- Group Policy (GPO)

## Connections

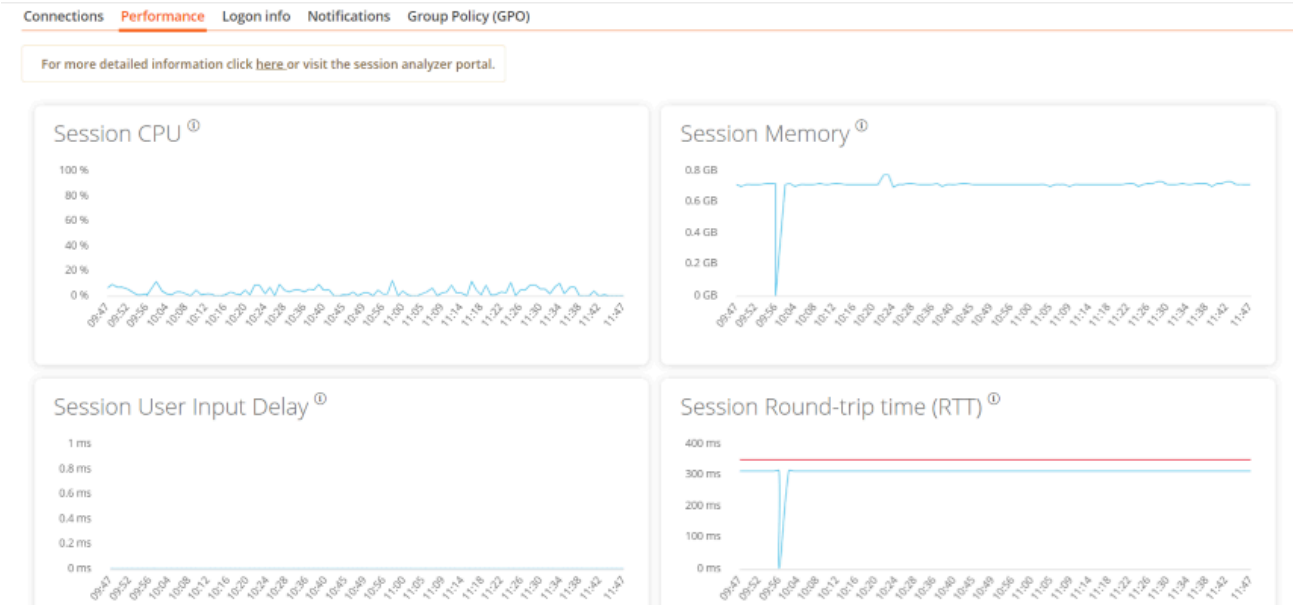



This tab contains information about the device's connections, i.e., each time a user starts or reconnects a disconnected session.

> The session end date is only reported for disconnected or closed sessions; while the session remains active, the session end date will remain empty.

## Performance

This tab groups graphs of the main performance counters for the last two hours.

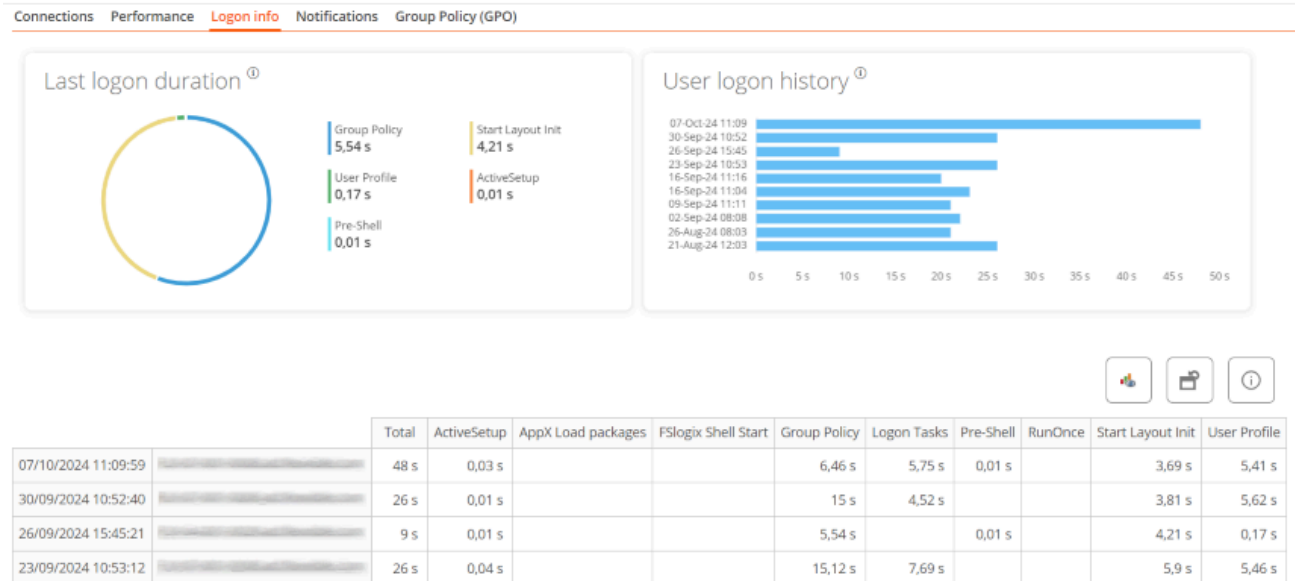



Graphs are included for:

- **CPU**: Percentage of session processor usage, excluding resources used by other sessions or system processes.
- **Memory**: Amount of memory used, excluding resources used by other sessions or system processes.
- **Session User input delay**: User input delay refers to the time lag between when a user performs an action, such as clicking a mouse button or pressing a key, and when the corresponding response is displayed on the screen or executed by the computer.
- **Session Round Trip Time (RTT)**: The time it takes for a data packet to travel from the user's device to a server or remote destination, and back to the user.

At the top of the tab, a link allows direct access to the diagnostic view for the active session in Analyzer.

# Login information




| | | Total | ActiveSetup | AppX Load packages | FSlogix Shell Start | Group Policy | Logon Tasks | Pre-Shell | RunOnce | Start Layout Init | User Profile |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 07/10/2024 11:09:59 | [redacted] | 48 s | 0,03 s | | | 6,46 s | 5,75 s | 0,01 s | | 3,69 s | 5,41 s |
| 30/09/2024 10:52:40 | [redacted] | 26 s | 0,01 s | | | 15 s | 4,52 s | | | 3,81 s | 5,62 s |
| 26/09/2024 15:45:21 | [redacted] | 9 s | 0,01 s | | | 5,54 s | | 0,01 s | | 4,21 s | 0,17 s |
| 23/09/2024 10:53:12 | [redacted] | 26 s | 0,04 s | | | 15,12 s | 7,69 s | | | 5,9 s | 5,46 s |

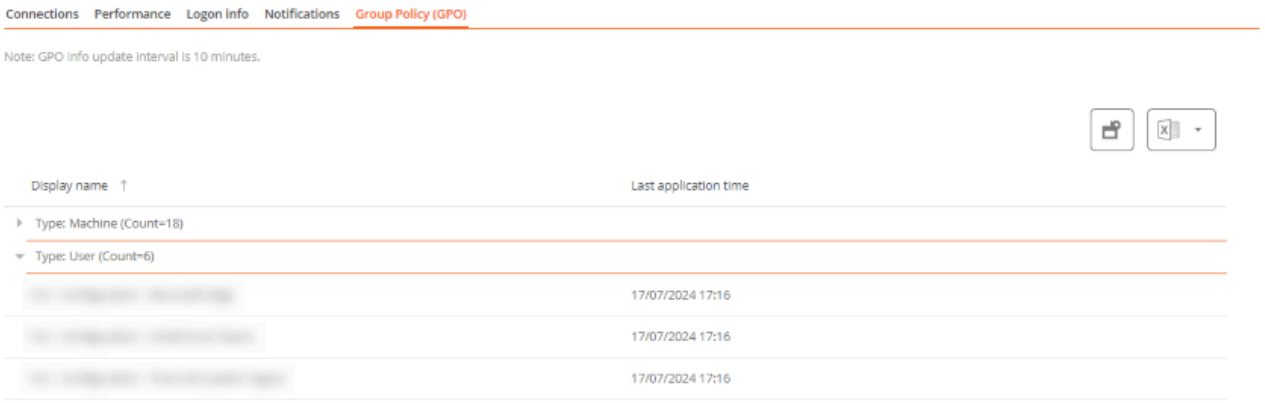
This tab allows you to view detailed information about user login times. The view is composed of two sections: At the top, two graphs are displayed. The first shows detailed information about the user's last login and the times of each step, and the second graph offers a view of historical logins and their duration in seconds.

At the bottom, there is a table with details of each login step for each recent user login.

## Notifications

Allows you to see if the session has any active notifications and their configuration data. When there are active notifications, a warning is shown at the top of the page.

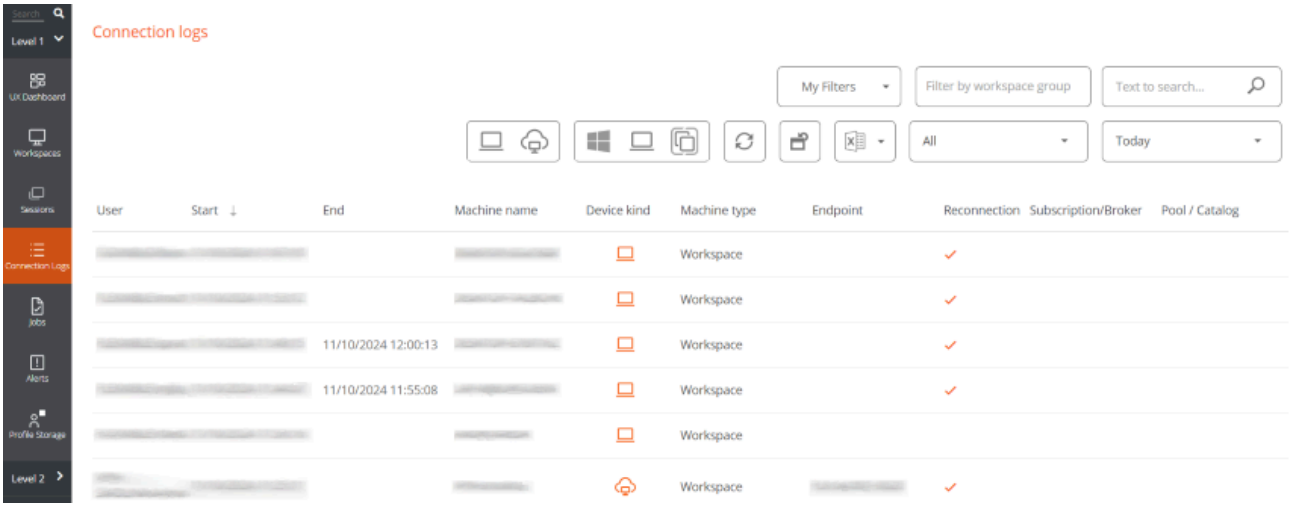
## Group Policy (GPO)




This tab shows information about the group policies applied to the active session. It allows you to view the names of the policies applied, both at the user level and at the device level.

# Workspaces / Level 1 / Connection Logs

The connection log allows you to view the historical session logs of users in the organization.




The information provided in this view is (by default):

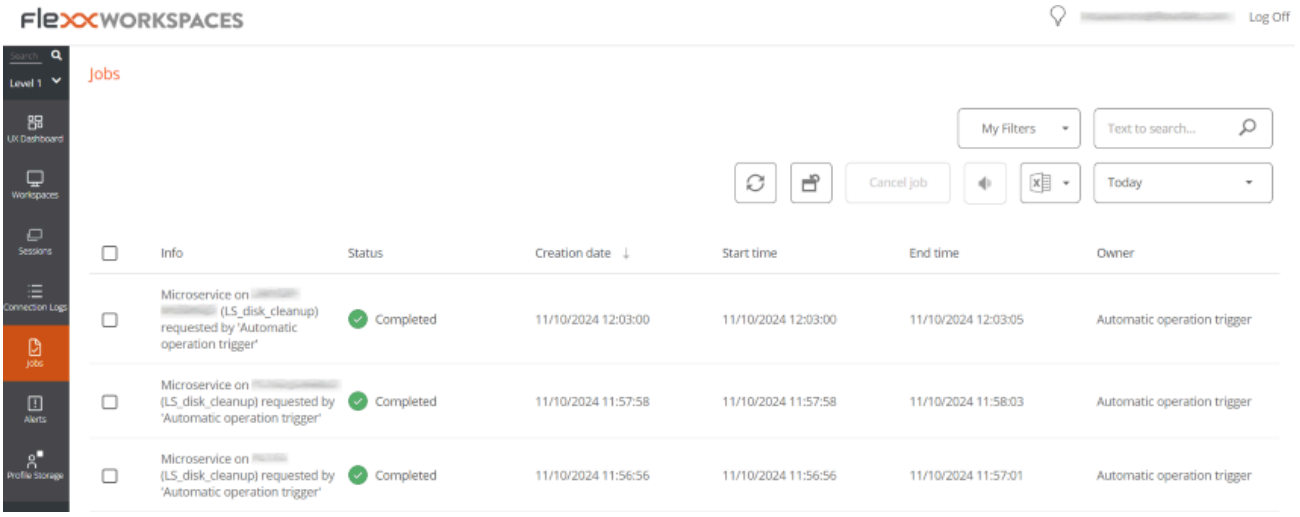
- User: username of the session account
- Start: start date and time of the connection
- End: end date and time of the connection (an empty field means the session is still open)
- Machine name: The device to which the user is connected.
- Device type: type of device, virtual or physical, used for session connection.
- Machine type: type of machine, device, or session host, serving the connection.
- Terminal: host name of the originating physical connection device
- Reconnection: checks if this session is a reconnection from the previous one.
- Subscription/Broker: name given for each supported subscription and broker.
- Group/Catalog: name of the host group containing the workspace.

This section allows the use of the column selector and the Filtering options also available in the `Sessions` section.

# Workspaces / Level 1 / Jobs

Each action performed in Workspaces generates a `Job`. These allow analyzing the results of the executions performed; for example, by checking the output of a microservice execution. `Jobs` gathers all the jobs performed in the organization, so it also provides historical execution records, which allows it to be used as an audit log.

## List view




The jobs view consists of the following elements:

- Options at the top of the interface
- Job list view

## Top options

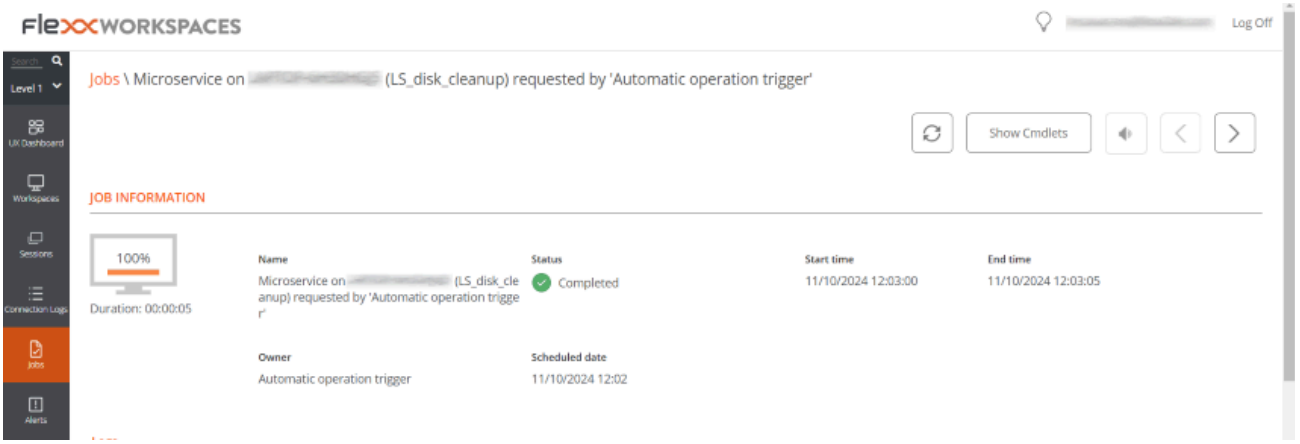
- Refresh the job list and show updated values.
- Resets all settings made for the jobs view.
- Filter jobs by age:
  - Today (default filter)
  - This week
  - This month
  - This quarter

    - This year
- The `Cancel` button allows canceling jobs in pending status.
- The `Notify` button allows you to subscribe to a specific job to receive an email notification when it is completed.
- The `Export to` button allows exporting in the selected type.
- The `My filters` button allows access to `Predefined filters` or user-created filters.
- Jobs can be filtered by any parameter in the list in the `Search` box.

## Jobs list

The job list, like all list views in Workspaces, allows multiple filtering and customization options as defined in Filtering Options in Listings.

# Detail view




The detail view includes a progress bar indicating the percentage of the job that has already been executed.

## Statuses

A job can have four statuses:

- **Pending**: the task is pending to start.
- **In progress**: the task has started and is still in process.
- **Completed**: the task has finished.

- **Error**: the task did not finish correctly or ended with errors.
- **Canceled by the user**: when a user cancels the task.
- **Completed with errors**: when the task has been completed, but at least one step failed with non-critical errors.

Suppose a `job` takes too long in the "in progress" state without recording any information. In that case, its state will automatically change to `Error`. However, this does not mean that the job will not be completed successfully, but there is a timeout due to an activity block during the task execution.

## Available information

In all cases, jobs include the following information:

- Change to be made (INFO)
- State
- Created date
- Start Date
- End Date
- User who made the change (OWNER)

At the bottom of the screen, depending on the type of job, the following tabs may appear:

- Logs
- Workspaces

## Logs

The logs tab allows consulting the data of each step in the execution; for example, when a microservice is executed on a device and you want to check the script execution output. This information is saved in the corresponding step (log line in list).

> To improve the visibility of script outputs, it is recommended, in the case of PowerShell scripts, to use the `Write-Output` command instead of `Write-Host`. More information at Considerations about the code to use.

## Workspaces

The `Workspaces` tab allows you to easily see the information of the devices that executed the job, in case of multiple executions.

# Job subscription

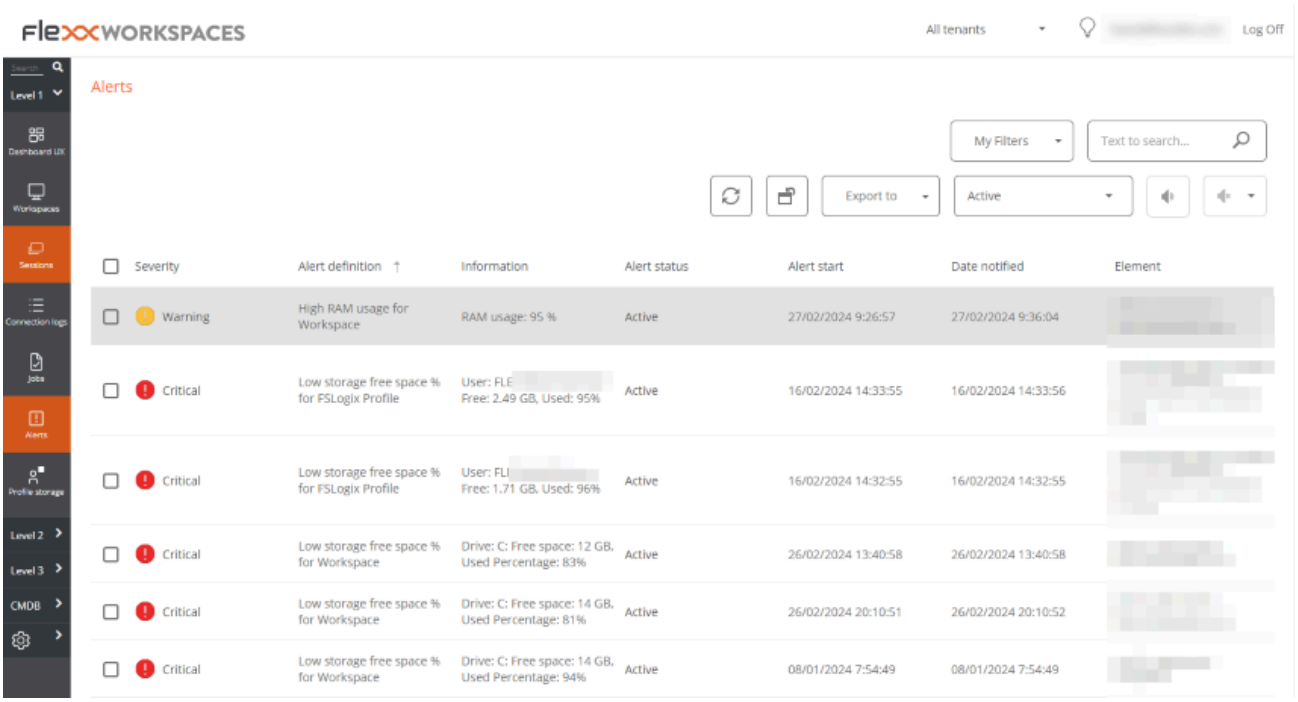
This feature allows subscribing to specific jobs, that have not yet started or are in progress. The system will notify by email when they are completed.

To subscribe, select the jobs from the list and activate the `Send notification` button.

# Workspaces / Level 1 / Alert

Workspaces has a real-time monitoring system, with all the relevant alerts from devices, sessions, and other important environment information.

The list of active alerts can be found in the `Level 1` -> `Alerts` section.




# Available actions at the top of the list

As in all Workspaces list views, a series of tools are concentrated at the top to facilitate filtering and management. Included:

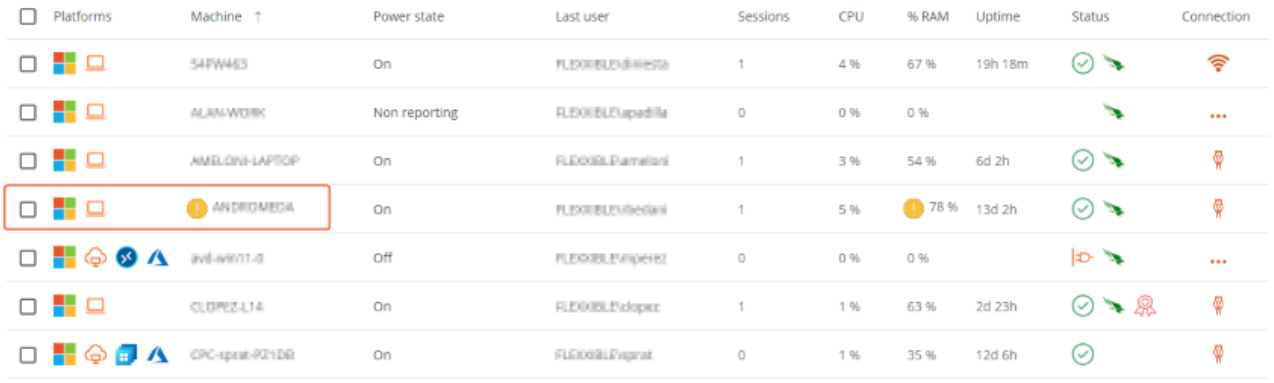
1. Refresh the view.
2. Restore default view.
3. Export the current view to `CSV File` or `XLSX File`.
4. View alerts by status: `Active`, `Active or Warning`, `Ignored` or `All`.
5. Enable notifications for an alert.
6. Disable notifications for an alert.
7. Filter by various categories.

8. Search alerts by text.

All active alerts allow notifications to be disabled, so they can be "hidden".

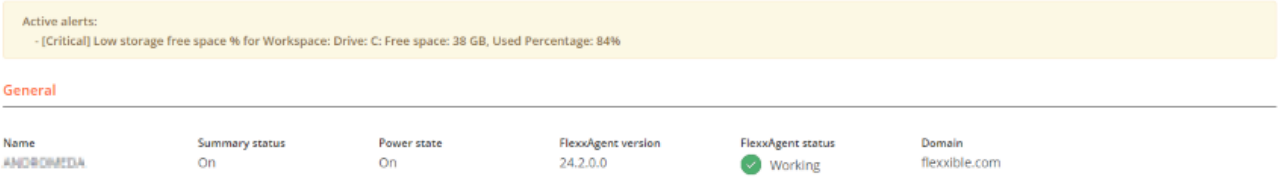
# Alerts in device or session views

Alerts are also visible in the list and detail views of the `Workspaces` and `Sessions` sections:



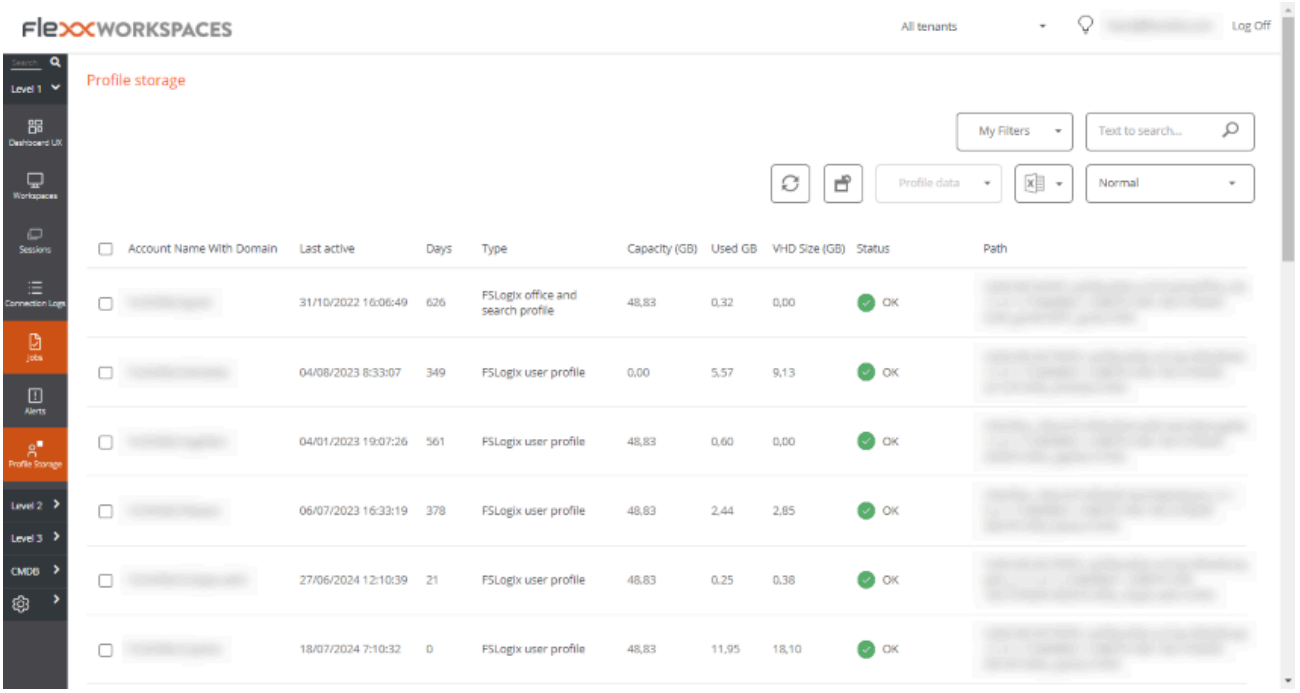

When a device has an active alert, in addition to the system alert itself, an alert icon `!` can be seen in the device list view.

A warning is also added when accessing the details screen.



# Workspaces / Level 1 / Profile Storage

When FlexxAgent detects the use of FSLogix profiles in user sessions, it collects information about them in this section.




This information is also visible as a tab in the active session details view.

## List view

This view groups all detected profiles and allows the same filtering functionalities available in Workspaces.

### Available operations

At the top of the interface, the `Profile Data` button allows you to perform the following operations with the selected profile(s):

- **Delete profile**: removes the VHDX file from the folder, allowing a new VHDX file to be created at the user's next login.
- **Compact now**: starts a compaction job using Jim Moyle's "Invoke-FslShrinkDisk.ps1".

- **Compact Now Forcing Logout**: Forces any existing user session to close and initiates a compaction operation.
- **Set status to Ok**: when an operation fails, this option returns the profile to an "OK" status in the list.
- **Remove from this list**: removes the profile from the list. If it still exists physically, it will appear back in the list when the agent detects it again.

# Detail view

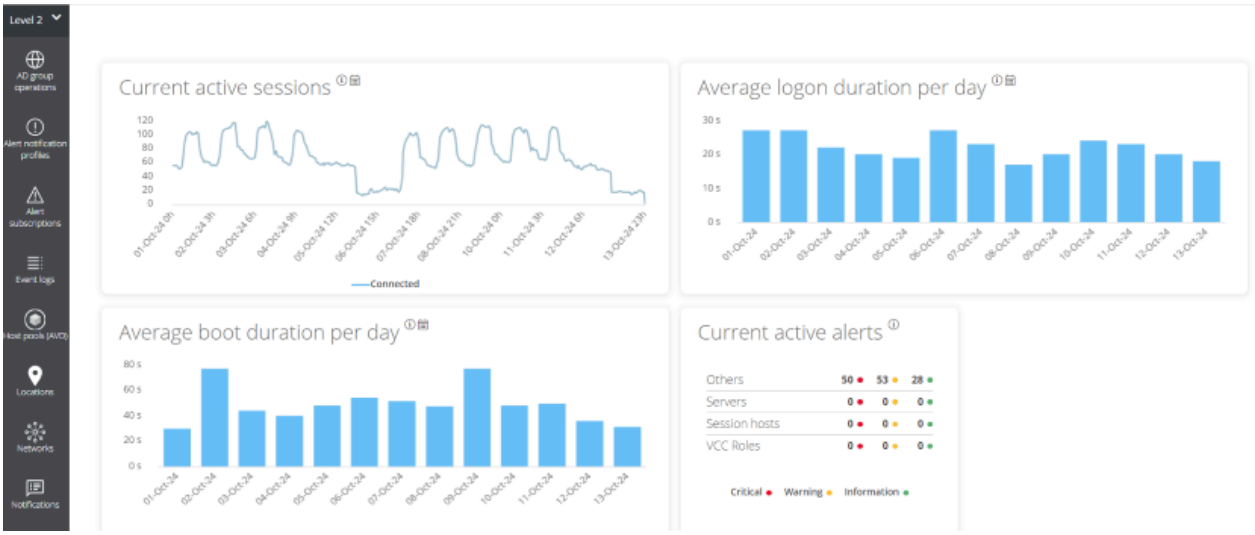
The profile detail view contains all the information, as well as the history of actions performed on them. Information fields available for a profile:

- **User**: in domain\account format
- **Path**: UNC path to the profile storage
- **Status**: indicates if the profile is functional or has any integrity issues.
- **Is backup**: determines if it is a backup profile and therefore not directly accessible to the user.
- **Type**: type of profile. It may be the profile itself or Office caches.
- **Uses Cloud Cache**: indicates if the Cloud Cache functionality is enabled.
- **Last activity**: last usage record in date and time format.
- **Days Inactive**: Indicates the number of inactive days in the profile.
- **Machine**: Last device that used the profile.
- **VHD size (GB)**: current profile size.
- **VHD size update**: date and time of the last data update by FlexxAgent.
- **Used (GB)**: Space occupied by the profile in GB.
- **Capacity (GB)**: Maximum space available in the profile.
- **Last compaction**: date and time of the last compaction.
- **Last size update**: last profile size refresh by FlexxAgent.
- **Last Update Duration**: Processing time for data retrieval.
- **Notes**: Allows adding annotations to the profiles.

The bottom contains a table with the list of historical compactions performed on the selected profile.

More information about this functionality and its configuration in `FSLogix Optimization`.

# Workspaces / Level 2




The `Level 2` section groups functionalities to expand the range of available actions. Includes access to configuration functions that allow sending alerts externally, accessing the unified Windows event log, notifications management, and servers.

Functionalities available at this level:

- Alert notification profiles
- Alert subscriptions
- Event Logs
- Notifications
- Servers
- Locations
- Networks
- Wifi networks

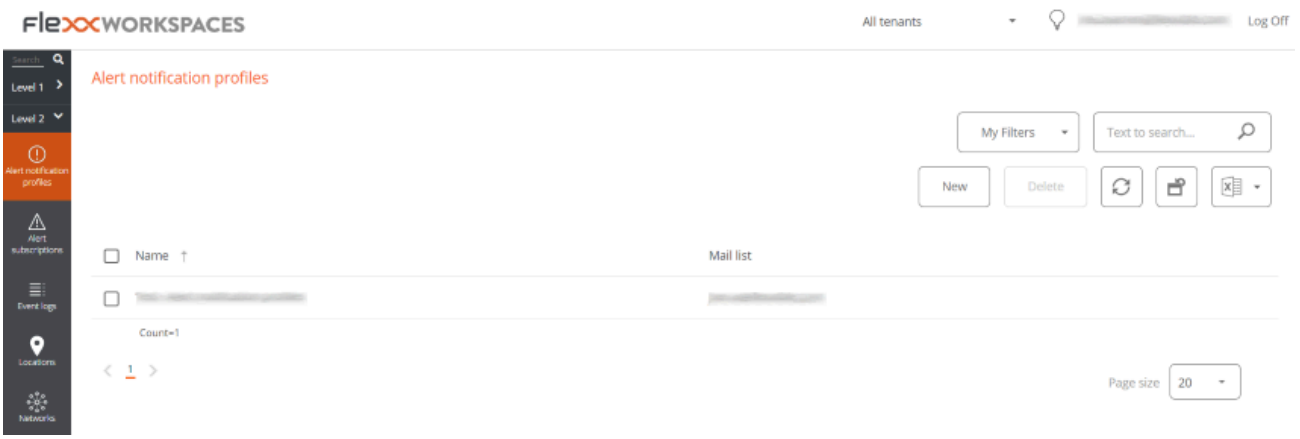
For FlexxDesktop deployments that use Azure Virtual Desktop subscriptions as a resource source for user sessions, the following features are included:

- Host pools (AVD)
- Power management policies (AVD)
- Power management activity (AVD)

# Workspaces / Level 2 / Alert notification profiles

This function allows a user with the `Level 2` role to configure an alert notification profile. An alert notification profile consists of a name and an email address and allows subscribing to specific alert definitions to receive an email when they are triggered.

You can access this functionality from the `Workspaces` -> `Level 2` -> `Alert Notification Profiles` module.

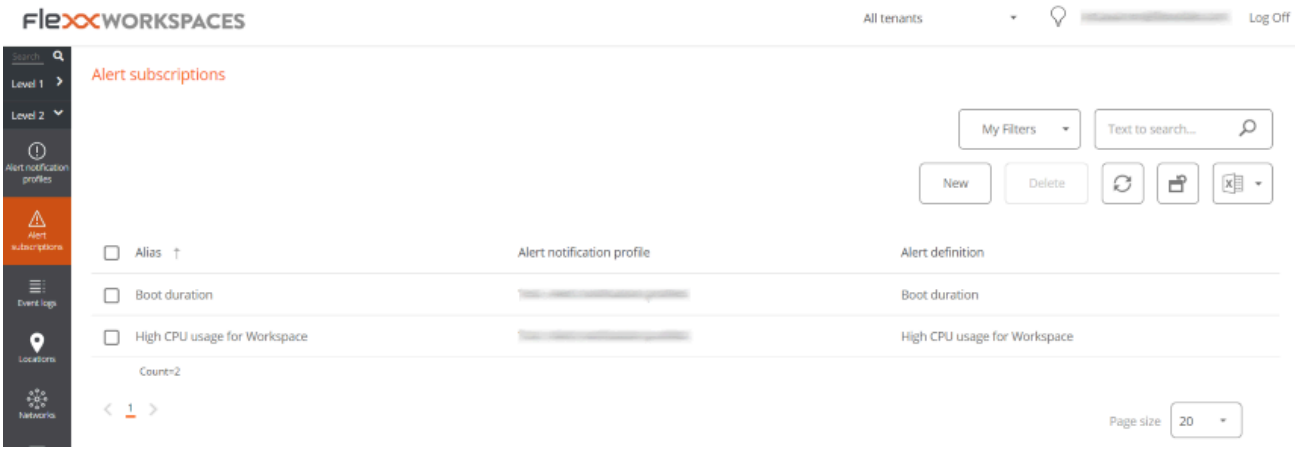



Creating a notification profile is very easy. Just click on `New`, provide a name and email address, and save the changes.

To receive alerts via email, you need to select the alerts of interest and subscribe to them. More information at Alert subscriptions.

# Workspaces / Level 2 / Alert Subscriptions

You can access alert subscriptions via the side menu `Level 2` -> `Alert subscriptions`




Alert subscriptions allow you to receive important alert notifications as needed. For example, if a user only wants to receive alerts related to low mobile or wifi signal on the devices, they can subscribe to `Low connection signal for Workspace` in `Alert definition`, so they will only receive alert emails of this type.

## Creating subscriptions

To create a new alert, you have to click on the `New` button at the top right of the list view and fill in the following fields:

- `Alias`: a friendly name for the subscription
- `Alert definition`: the type of alert that will be used
- `Alert notification profile`: the type of alert notification that will be used

An email with the alert data will be sent once the subscription is created, if any of the alert definitions associated with it are triggered.

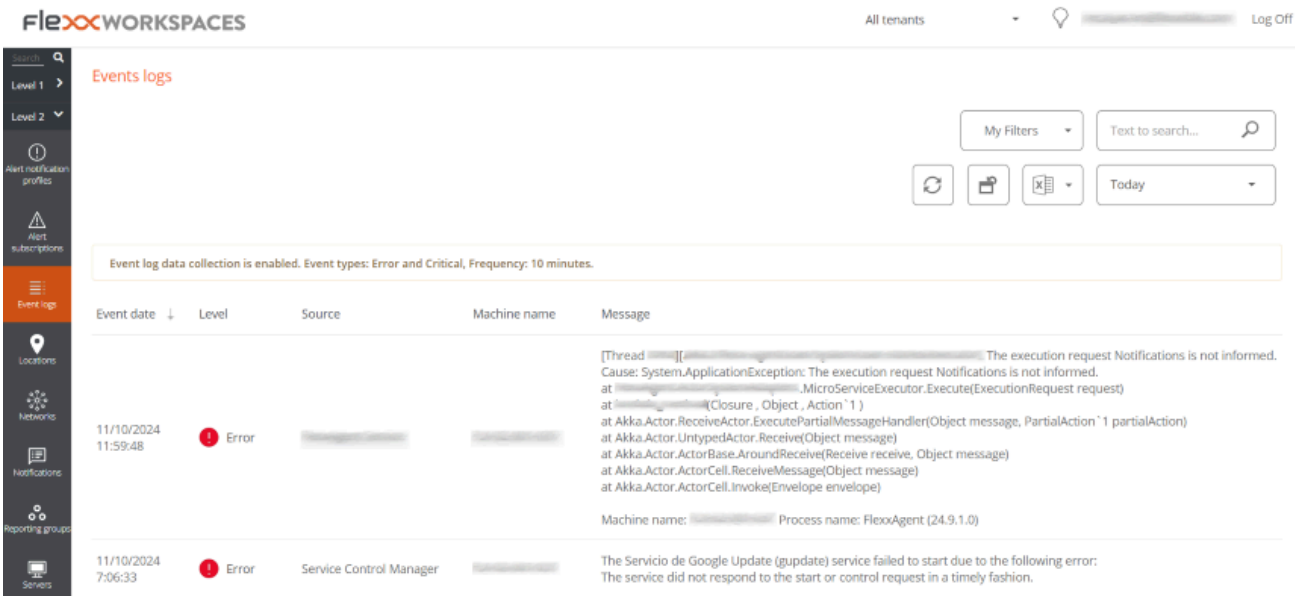
# Workspaces / Level 2 / Event Logs

The event log is a powerful diagnostic tool that, by default, centralizes critical and error events.

## List view

This tab presents information about the log events present on the device. By default, it filters the errors and only shows those errors with `Error` or `Critical` severity and retrieves them from the device at ten-minute intervals. This time can be modified in the Workspaces settings.

The `Event Log` section lists the event viewer events for Windows devices. By default, Workspaces only processes and shows in this section the critical and error events from the application, security, and system event logs.




The default view is for `Today`, which starts at 12:00 p.m. in the time zone defined in the Workspaces instance. The time filter can be changed to the values:

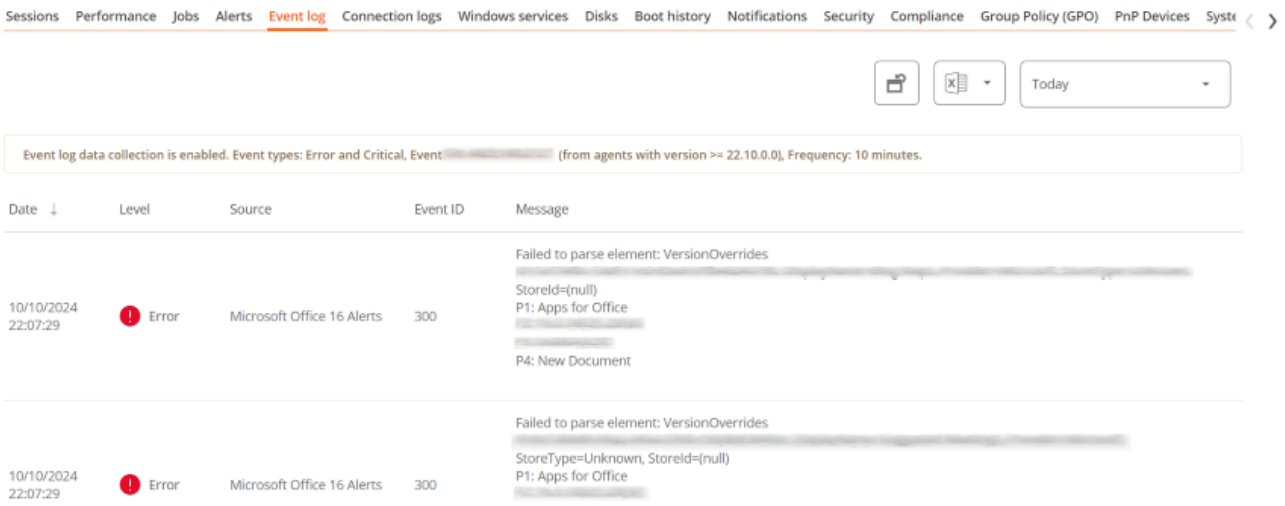
- Today
- This week
- This month

- This quarter
- This year

## Filtering options

This view allows the same filtering functionalities available in Workspaces. An example would be to filter by an event with a specific ID to obtain a list of affected devices, subsequently applying corrective actions.

## Events logs info in Workspaces




In the details view of a Windows device, a tab is activated that groups the event logs for that device.

# Detail view

The detail view of an event log contains all its information:

- **Event Date**: event registration date in day and time format
- **Level**: event severity level
- **Source**: event source
- **Event ID**: numeric identifier of the event
- **Log File**: event log file that hosts the event
- **Machine Name**: hostname of the device that logs the error

- **Message**: content of the event message

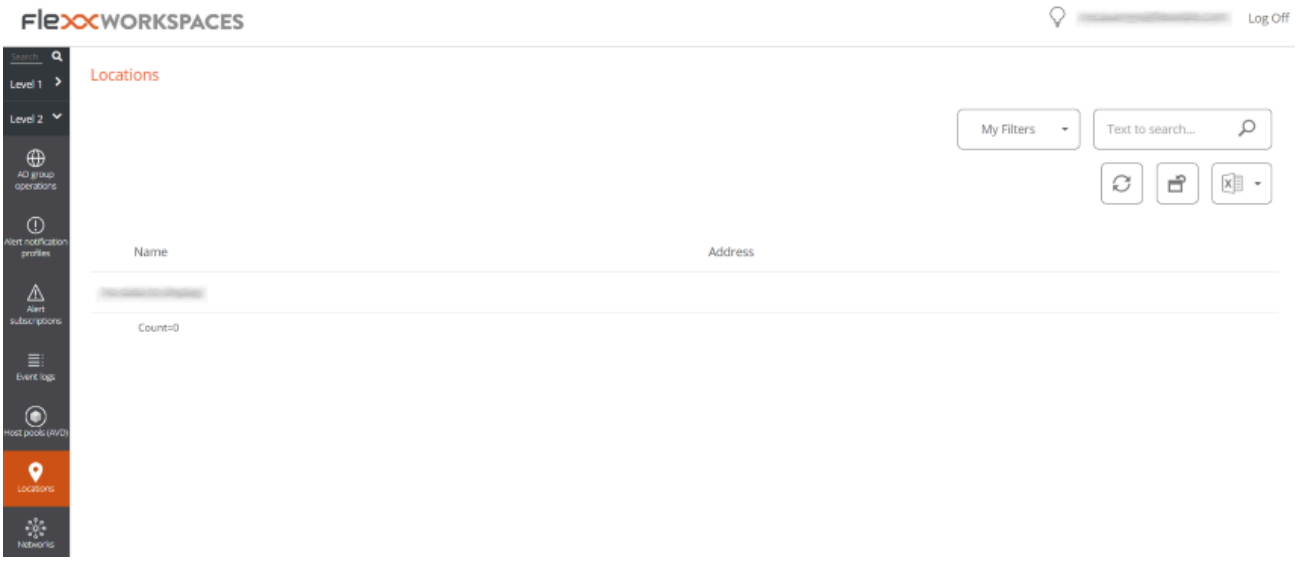
# Additional event settings

Users with an administrator role can add events that do not meet the default filtering conditions to, for example, add events with a specific ID that, although they have an informational severity level, are relevant to the organization, as well as change the log update time.

# Workspaces / Level 2 / Locations

Workspaces supports physical locations as a grouping entity for devices and networks, to which coordinates can be linked for geolocation.

## List view




Networks allow associating one or more wireless networks to them, and locations allow associating multiple networks.

## Detail view

A location consists of the following information:

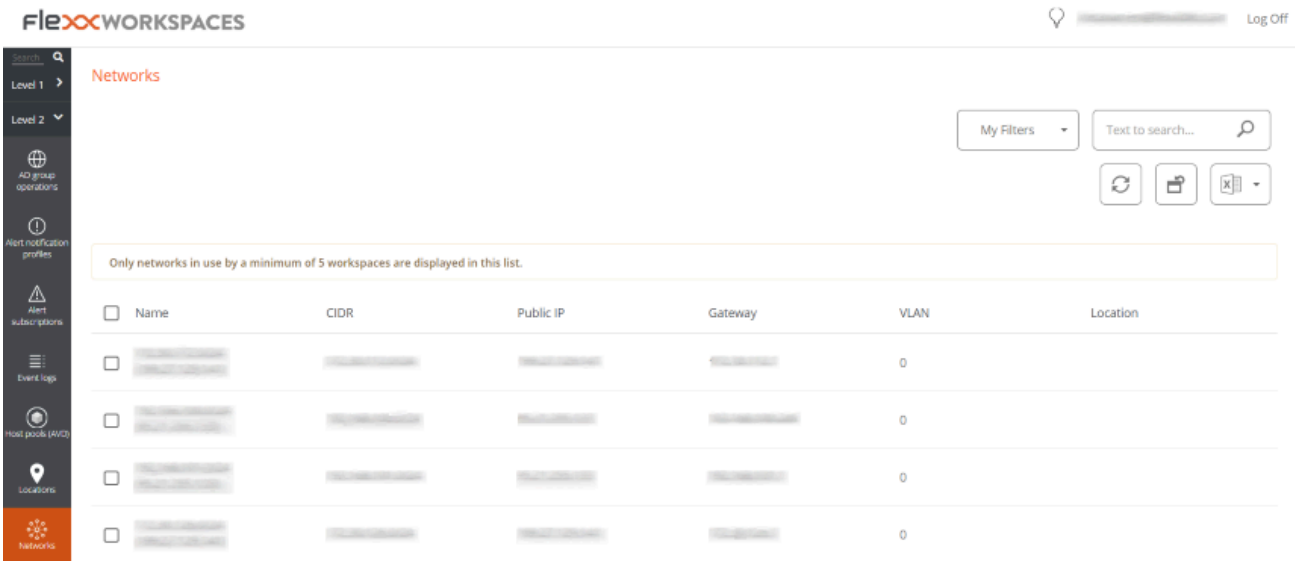
- **Name**: friendly name of the location
- **Address**: postal address
- **Latitude**: numerical value of latitude
- **Longitude**: numerical value of longitude

At the bottom, you can see the tabs:

- **Networks**: networks identified by FlexxAgent included in that location; it contains two options:
  - **Link**: allows linking a new network to the policy.
  - **Unlink**: allows unlinking a network from the policy.
- **Workspaces**: devices included in the location

# Workspaces / Level 2 / Networks

FlexxAgent collects multiple network information from devices. When more than five devices report the same network in the same organization, the network is automatically created in Workspaces. These help to automatically maintain an inventory of all networks detected in devices to get an accurate location mapping based on network data.

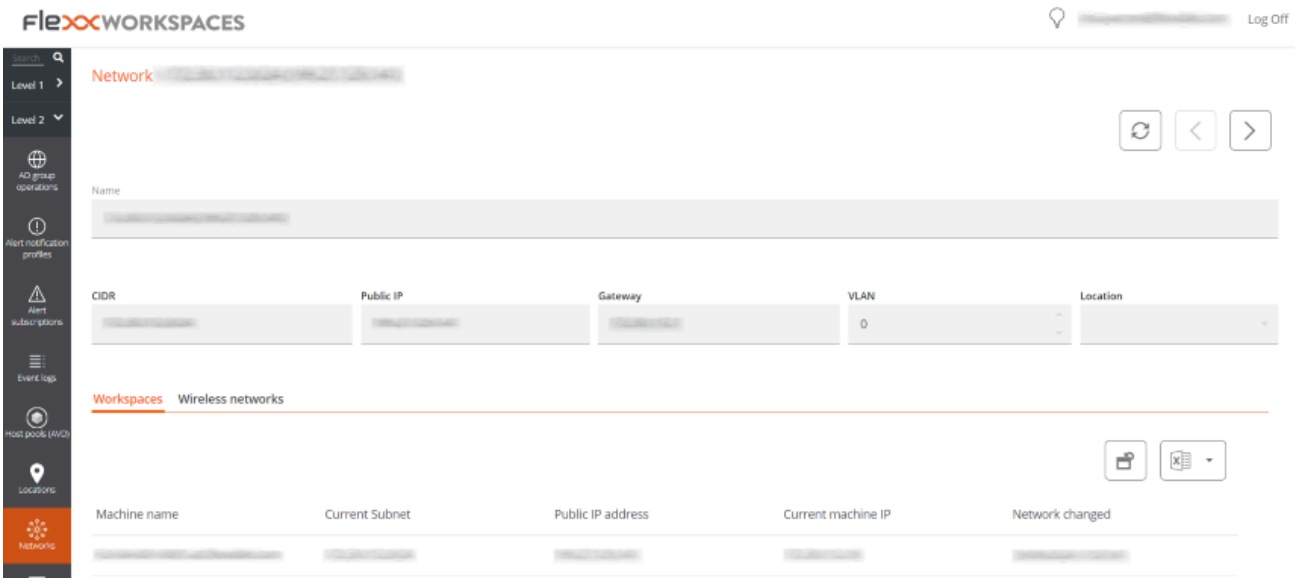



## List view

The list view allows you to see the relationship of networks discovered by the agent. It allows searches, filtering, sorting, showing or hiding columns, and more.

It also allows you to select a network from the list and delete it; in that case, if FlexxAgent detects that network again on more than five devices, it will recreate it.

## Detail view




At the top block of the detailed view of a network, there is a list of collected fields:

- **Name**: network name; by default the CIDR followed by the public IP. Allows customization.
- **CIDR**: Network CIDR
- **Public IP**: the network's public IP for internet access
- **Gateway**: IP address of the network's gateway
- **VLAN**: VLAN identifier, if any
- **Location**: `Location` associated with the network. Requires preconfiguring at least one location.

At the bottom of the interface, there are two tabs:

- **Workspaces**: shows the list of devices connected to the network.
- **Wireless Networks**: shows the list of `Wireless Networks` linked to the network. It allows linking or unlinking wireless networks previously discovered by FlexxAgent on the devices with the link or unlink buttons at the top of the list.

# Workspaces / Level 2 / Notifications

Notifications are a powerful tool for communicating directly, securely, and effectively with users. Given their versatility, they are especially useful in service disruption scenarios as they allow maintaining effective communication with users even when the company's communication infrastructures and tools are not functional.

## Notifications section

By default, the `Notifications` section displays information about active and scheduled notifications. To close them, you need to select the notifications you wish and press the `Close notifications` button.

As with all list views, you can filter the list content using the tools available in filtering functionalities.

## Types of notifications

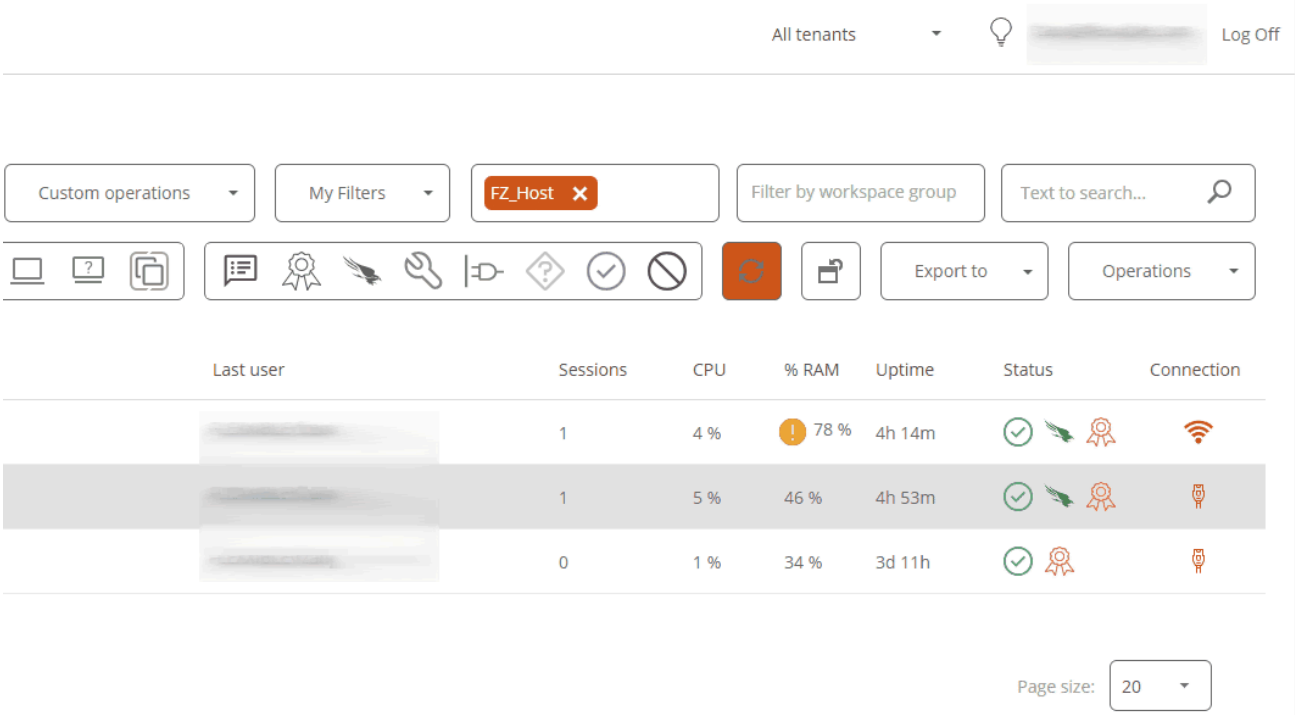
Workspaces includes two types of notifications that allow you to send different types of messages to users:

- Pop-up notifications that allow launching a pop-up window with a message that the user can close with a click.
- Notifications: designed for service disruption events, where corporate communication channels might not be available. They are used when ensuring the message reaches users as quickly as possible to avoid a high volume of users trying to contact the support department.

### Popup notifications

Sending notifications is available in the `Sessions` and `Workspaces` sections of Level 1. To send a popup notification, select the target sessions or devices and execute:

- `Operations` -> `Notifications` -> `Send pop-up message`.
- Specify the message and click `Ok`.




The user in the session will receive a window in the center of their screen with the configured message.

These notifications are based on Windows system tools. If all devices or sessions are selected and a message of this type is sent, the message will only reach the users who are working (in session) at that moment. If any user enters their session after the message is received, it will not be visible.


## Notifications

Notifications have many additional features aimed at maintaining effective communications and protecting the information transmitted to users.

While on screen, notifications reserve that space so the user can no longer occupy it with their applications. This is a mechanism to ensure that the user has the message visible.


Notifications can be configured for time intervals; intervals can be defined in which all sessions already started and future sessions receive this notification and it remains active during that period of time.

To configure and launch a notification, the following is required:

- Define a time zone.
- Set start and end date and time.
- Severity, with three levels to choose from:
  - Informative: generates a gray notification.
  - Maintenance: will generate a yellow notification.
  - Technical issue: generates a red notification.
- Request acceptance: enables a button to get user feedback; once accepted, it closes for the user.
- Disable minimize: when enabled, prevents users from minimizing the notification.
- Message text
- Additional information: extra message that will appear when hovering over the notification.

- Link: to include a status page, if available. -Blinking: allows configuring blinking in the notification to increase its visibility.

# Workspaces / Level 2 / Reporting groups from Workspaces

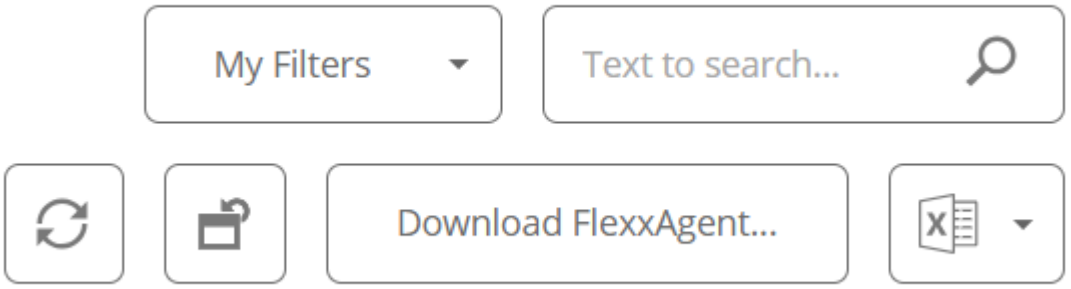
The `Report Groups` view from the `Workspaces` module allows you to see the status of the report groups created in the organization. It shows general information about the devices that make them up and offers the possibility to download FlexxAgent onto them.

## List view

The list view shows a table with the listing of the report groups, according to their ID number, name, and corresponding organization.

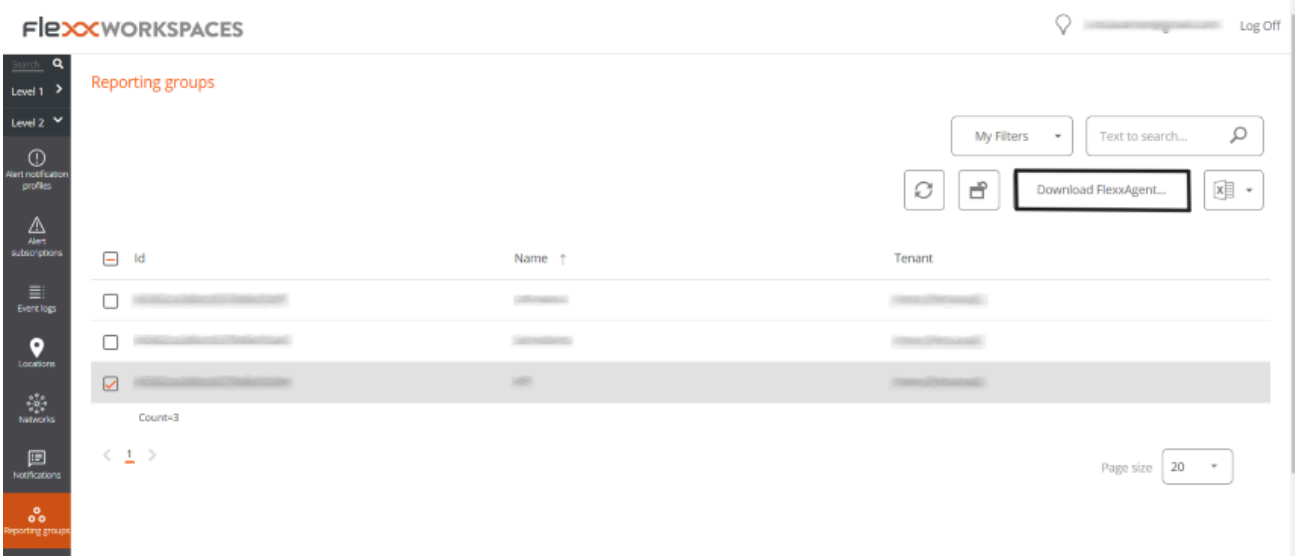
At the top, there are a series of buttons that allow actions on the list of report groups.

- **My filters**: allows you to manage filters to search for report groups.
- **Text to search**: free search box to find groups that match the entered term.
- **Refresh**: reloads the list of report groups after applying search filters.
- **Reset all settings for this view**: returns to the initial settings of the list.
- **Export all items**: allows you to download the list of report groups in CSV and XLSX formats.
- **Download FlexxAgent**: FlexxAgent will be downloaded to the selected report groups.

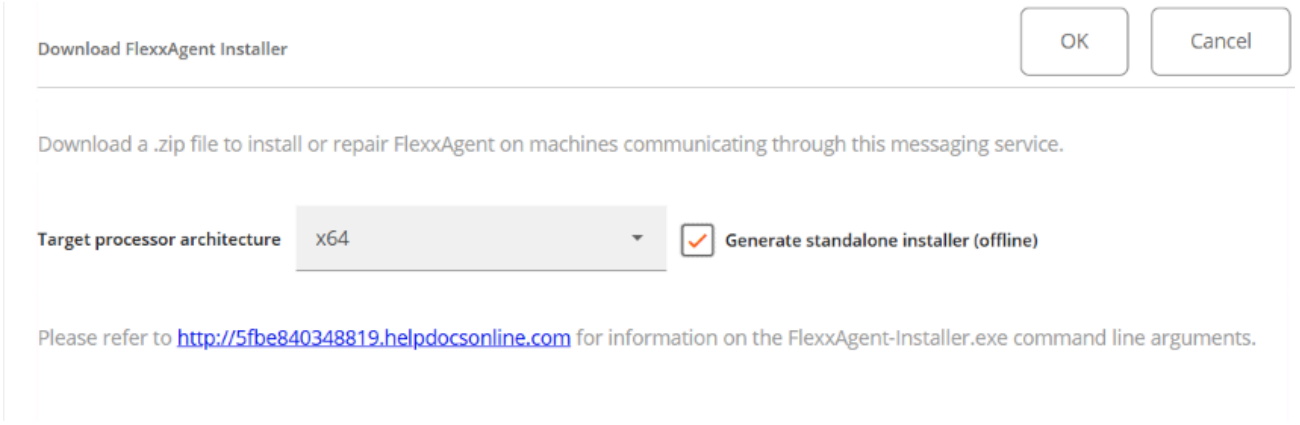



## Download FlexxAgent

In the list view table, you must select the report group for which you want to download the agent and click on the `Download FlexxAgent` button.




A window will open to download the FlexxAgent installer.




If the `Generate standalone installer (offline)` option is selected, during installation, the binary will not require internet access for verification or downloading binaries.

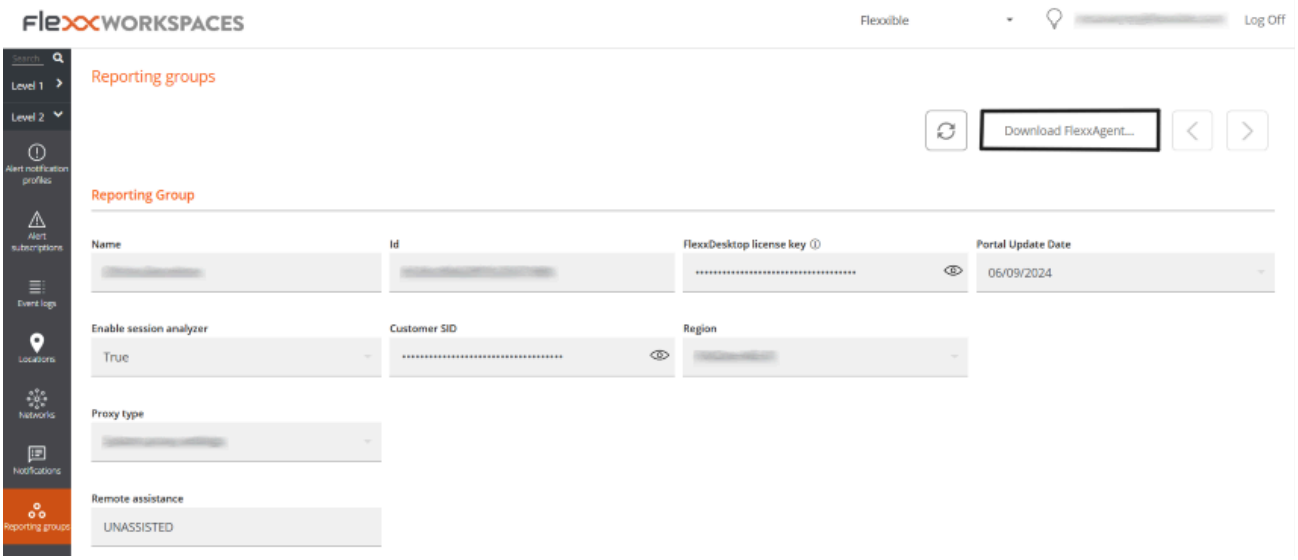
If, on the other hand, the `Generate standalone installer (offline)` option is not selected, the minimal installation package will be downloaded. In this manner, the binary will access the internet to verify and download the latest binaries.

For other installation options, you can consult the FlexxAgent documentation.

# Detail view

To obtain specific information about a report group, you need to select one in the list view table.

The detail view offers specific data about the selected report group: name, ID, FlexxDesktop license key, Portal update date, whether it has an Analyzer session enabled, client SID (security identifier), region, types of proxy and remote assistance enabled.

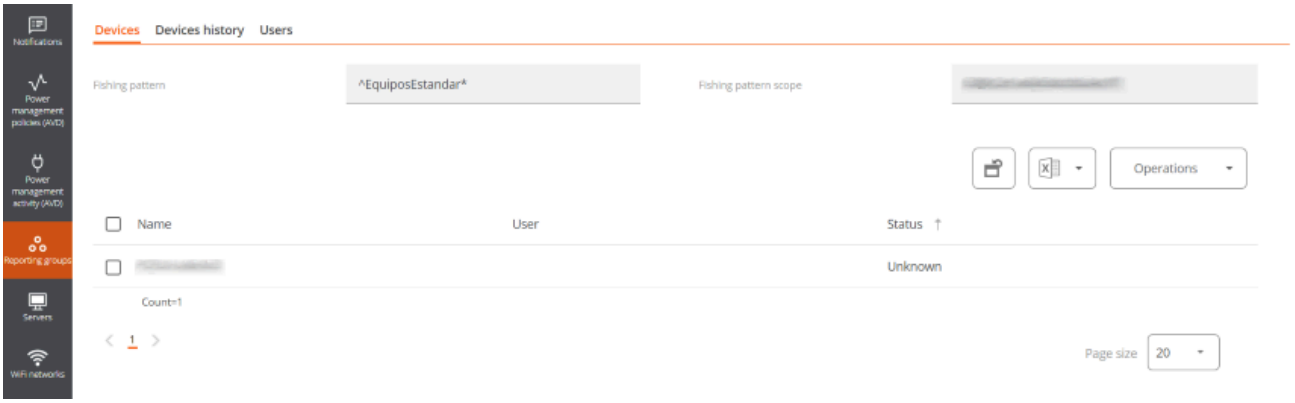



# Devices

The detail view of the report groups also presents specific information on three areas:

#### Devices

This is the list of devices that make up the report group being consulted. When it comes to a group that uses the fishing pattern to add devices, the configured RegEx term appears in a top box, as well as the id associated with the report group being queried.



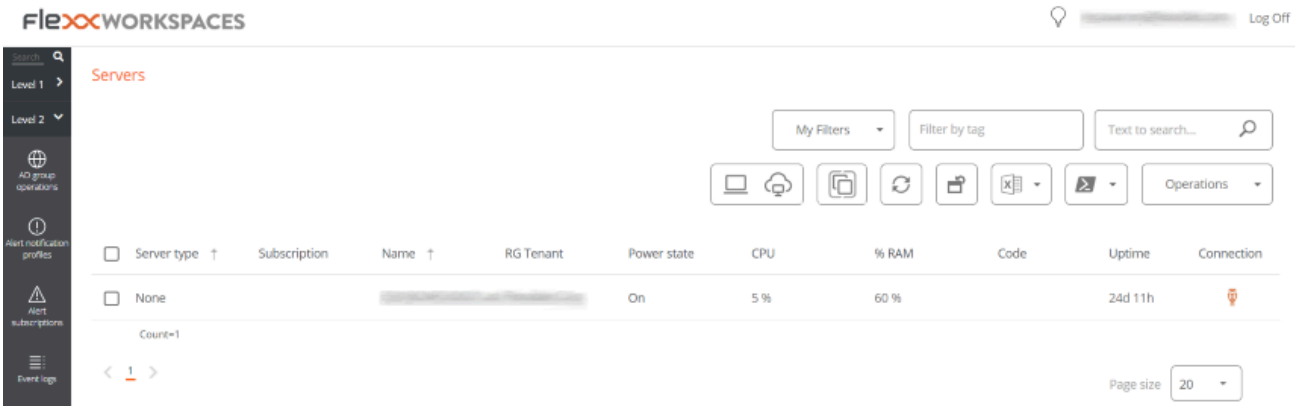

**Devices history**

It provides the name and the date of incorporation of the devices to the report group, also whether they have been assigned the group manually or automatically and the source and destination groups to which the devices have belonged.

**Users**

This is the list of users who belong to the report group. La tabla informa sobre el inquilino y rol que tienen asignados dentro de la organización

# Workspaces / Level 2 / Servers




The 'Servers' view allows access to the list of servers in the environment. When FlexxAgent is installed on a device, it will by default appear in the `Workspaces` section. To move the device to the `Servers` view, from the `Workspaces` section you must select the device and execute the `Machine Type` -> `Server` operation

More information on how to include a device in this list.

## List view

The list view contains all servers configured as such in Workspaces and allows the same actions with the devices listed in the `Workspaces` view.

## Available operations

From the list view, at the top right of the interface, the following tools are included:

- Filtering Options
- Microservices
- Operations

#### Filtering options

This view allows the same filtering functionalities available in Workspaces.

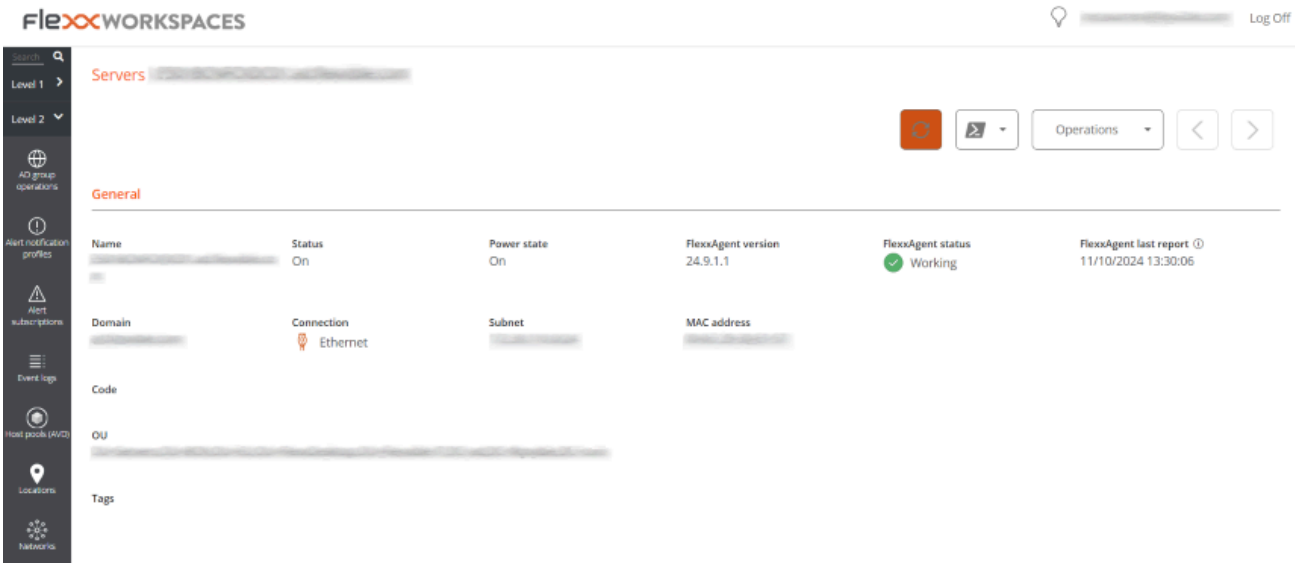
#### Microservices

From the `>-` button it is possible to execute any of the microservices enabled for the organization that have `System` as the configured context. This allows the execution of microservices with administrative permissions on the devices. The actions of enabling, creating, modifying, or deleting microservices are performed from the Portal.

#### Operations

The `Operations` button allows executing the same device management actions as the Workspaces view.

# Detail view




The detail view of a server, in addition to the operations available at the top of the interface, contains the following sections:

- General information
- Extended information
- Specific information segmented into tabs at the bottom

## General

The general information block of the device contains:

- **Name**: hostname of the device
- **Status**: power state (on-off)
- **FlexxAgent Version**: FlexxClient version number
- **FlexxAgent Status**: FlexxAgent execution status (running - stopped)
- **FlexxAgent Last Report Date**: date of the last report received from FlexxAgent on the device
- **Domain**: domain to which the device belongs
- **Connection Type**: type of connection used by the device (ethernet - wireless)
- **Subnet**: network addressing
- **MAC Address**: MAC identifier
- **Code**: allows a string to be set as code
- **Network Changes**: indicates if the device has recently changed its network configuration
- **Tags**: allows identification tags to be associated
- **OU**: organizational unit in the domain where the device's account resides

## Extended

The extended information block of the device contains:

- **RAM**: total amount of RAM
- **Cores**: number of processor cores
- **IP Address**: IP address of the device
- **Windows Edition**: edition of the operating system
- **OS Build**: operating system build number
- **Uptime**: the length of time the workspace has been running since it was last started or restarted; it's important to note that if fast startup (fastboot) is enabled, the workspace is only off when restarting.
- **Fast Startup**: indicates if fastboot is enabled on the server
- **Last Windows Update**: last patch application date
- **Duración del último arranque**: duración del arranque (boot) del último inicio
- **Pending reboot**: determines if the device has a pending reboot to apply updates.

- **System disk**: indicates the used space of the system disk.
- **Public IP and ISP**: if public IP data collection is enabled, shows the public IP and the provider.
- **Region**: if it's an Azure virtual machine, will show the Azure region of the host.
- **BIOS Manufacturer**: BIOS manufacturer
- **BIOS Version**: current BIOS version
- **SMBIOS Version**: current SMBIOS version
- **BIOS Serial Number**: unique BIOS identifier
- **Session Analyzer**: indicates the status of the FlexxAgent Analyzer process, which can be:
  - **Not configured**: The FlexxAgent is configured to not launch Session Analyzer.
  - **Disabled**: The FlexxAgent is not launching Session Analyzer because it has been disabled using the registry key 'AvoidLaunchAnalyzer'.
  - **Configured**: The FlexxAgent is configured to launch Session Analyzer in all the user sessions.
  - **Installed**: Session Analyzer is already installed in the workspace so FlexxAgent won't try to launch it.
  - **No compatible**: FlexxAgent no inicia Session Analyzer porque no es compatible con el sistema operativo del workspace (por ejemplo, una versión de Windows de 32 bits).

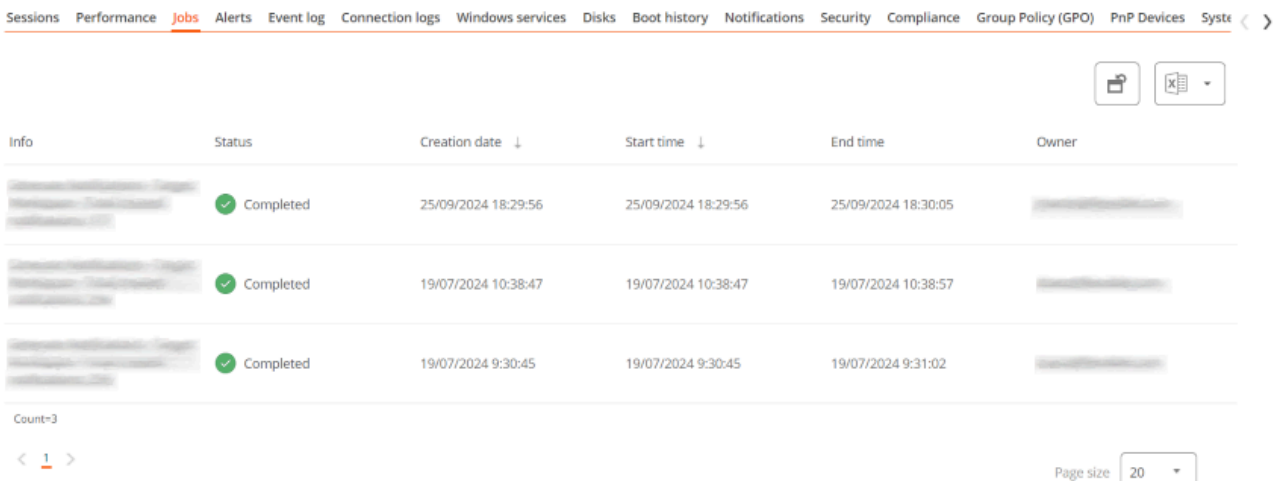
## Tabs

The tabs at the bottom show grouped specific information. The following are included:

- Jobs
- Performance
- Alerts
- Event logs
- Disks
- Boot history
- Security
- Group Policy (GPO)

- PnP Devices

### Jobs



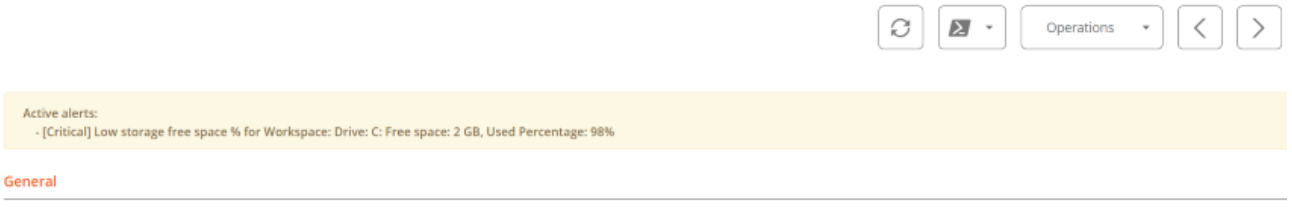

All actions performed from servers on one or more devices are audited in the job queue. This tab allows you to check the jobs performed for the active device without having to go to the section.

### Performance

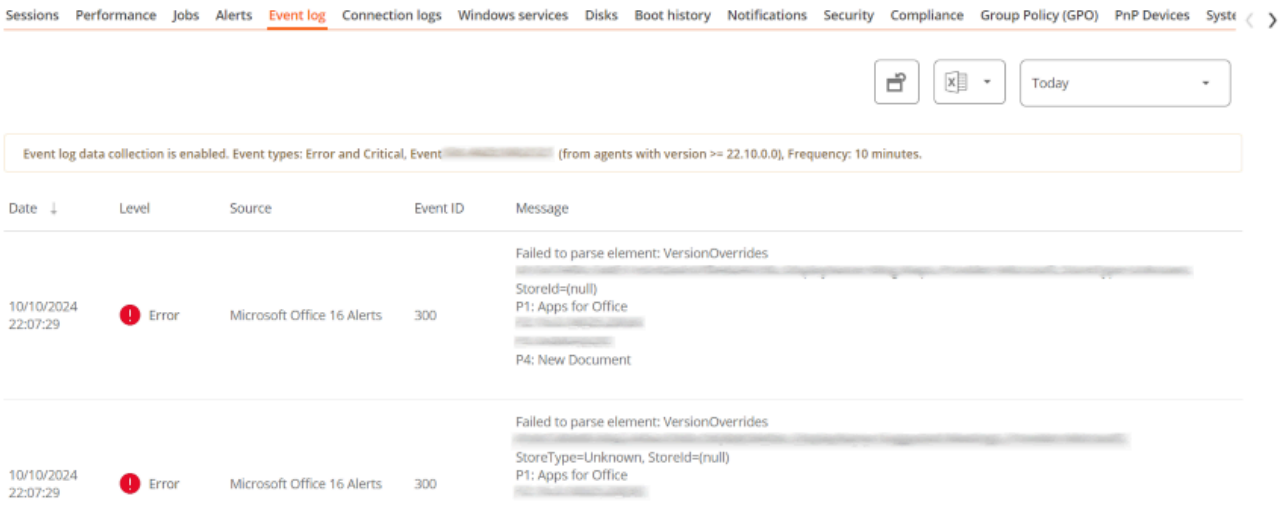
In the performance tab, graphical information about CPU, memory, and bandwidth usage is displayed.

### Alert

This tab shows a list of all active alerts, if any, for the active device. When a device has an active alert, a message is also displayed at the top of the screen.



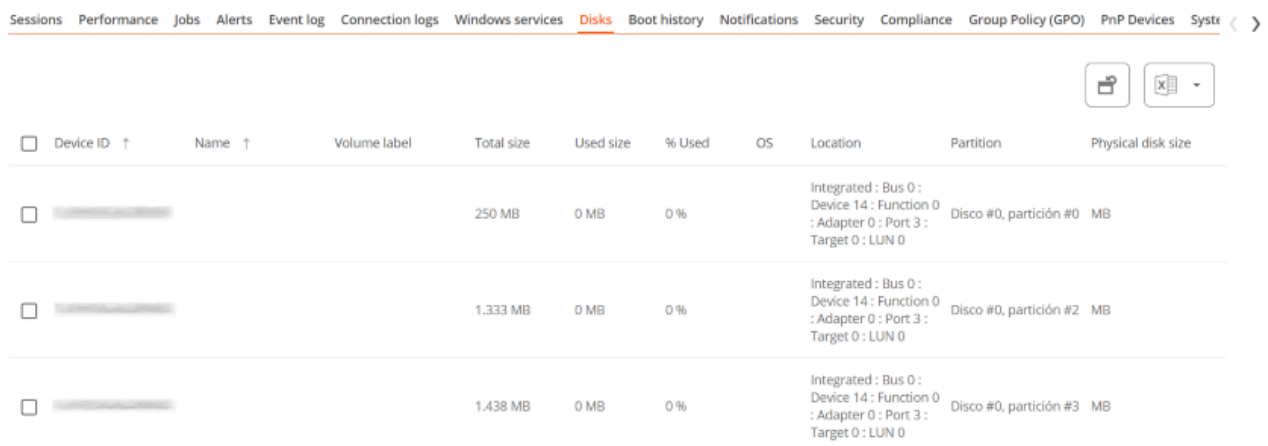

### Event Logs




This tab presents information about the log events present on the device; by default, it filters errors and only shows those with `Error` or `Critical` severity; it obtains them from the device in 10-minute intervals.

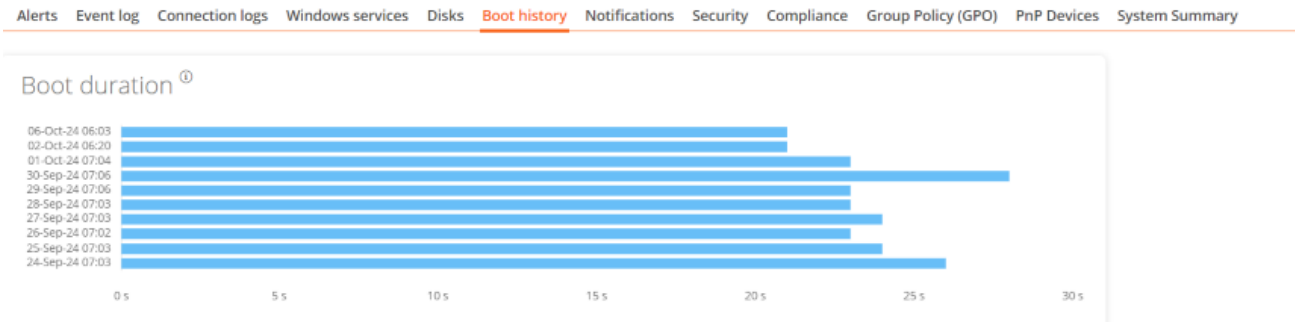
Using the available options in `Settings`, it is possible to modify the sampling time or include specific events by their ID.

### Disks




This tab offers a list view of all partitions present on all disks identified in the system, as well as statistics on their capacity and occupancy levels.

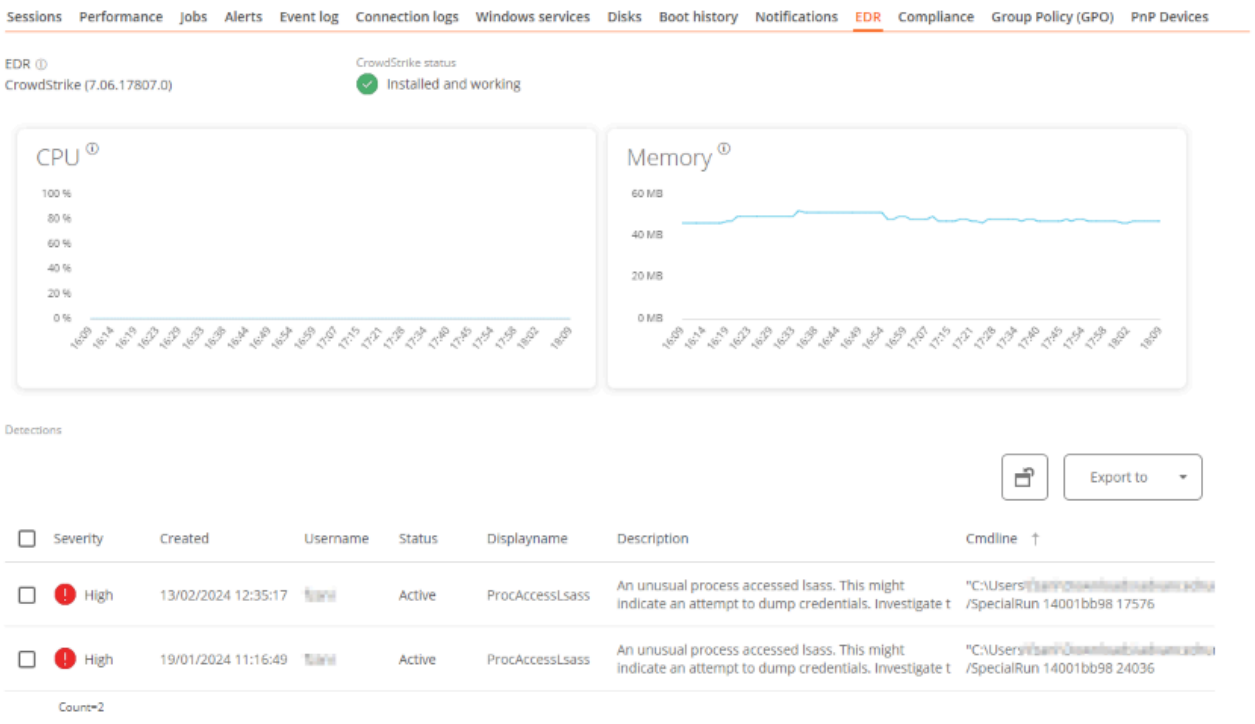
### Boot history




Esta pestaña permite ver una gráfica de registros históricos del tiempo ocupado en el arranque (boot) del dispositivo.

#### Security (EDR)

FlexxAgent will detect if a device has Crowdstrike Falcon installed and display the information on the `EDR` tab of the device detail view. There you can check the installed version, the correct or incorrect execution status, as well as the CPU and memory resource usage.



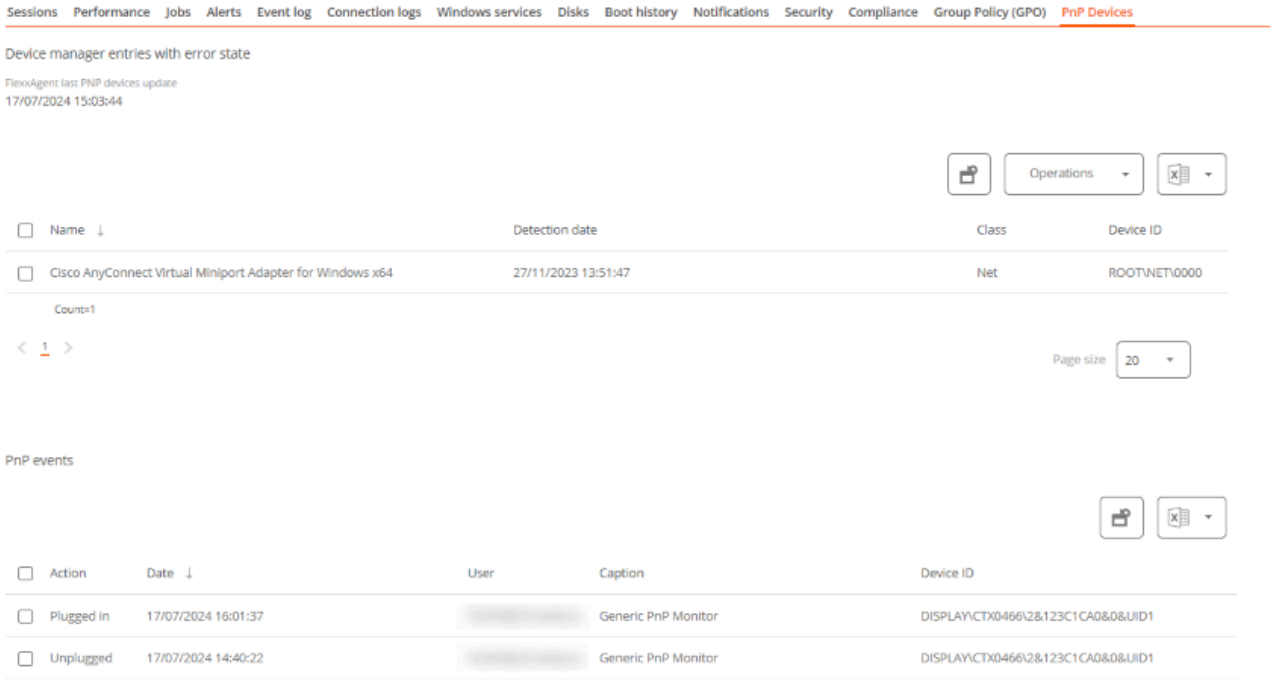

If it is also desired to capture detections to display them in Workspaces, access data must be configured via API to the Crowdstrike Falcon instance in the `CrowdStrike` section of `Level 3` -> `Messaging service (IoT Hub)`.

#### Group Policy (GPO)

This tab displays the information of the group policies applied on the active device. Allows viewing information of policy names such as the name and time of check.

### PnP Devices

This tab allows you to see at the top the PnP devices that are in an error state, which may be due to a hardware or driver malfunction, or incorrect device or driver configuration.




At the bottom of the tab, all PnP events are recorded. Each time a peripheral device is connected or disconnected, a record is generated in this table.

# Workspaces / Level 2 / Wireless networks

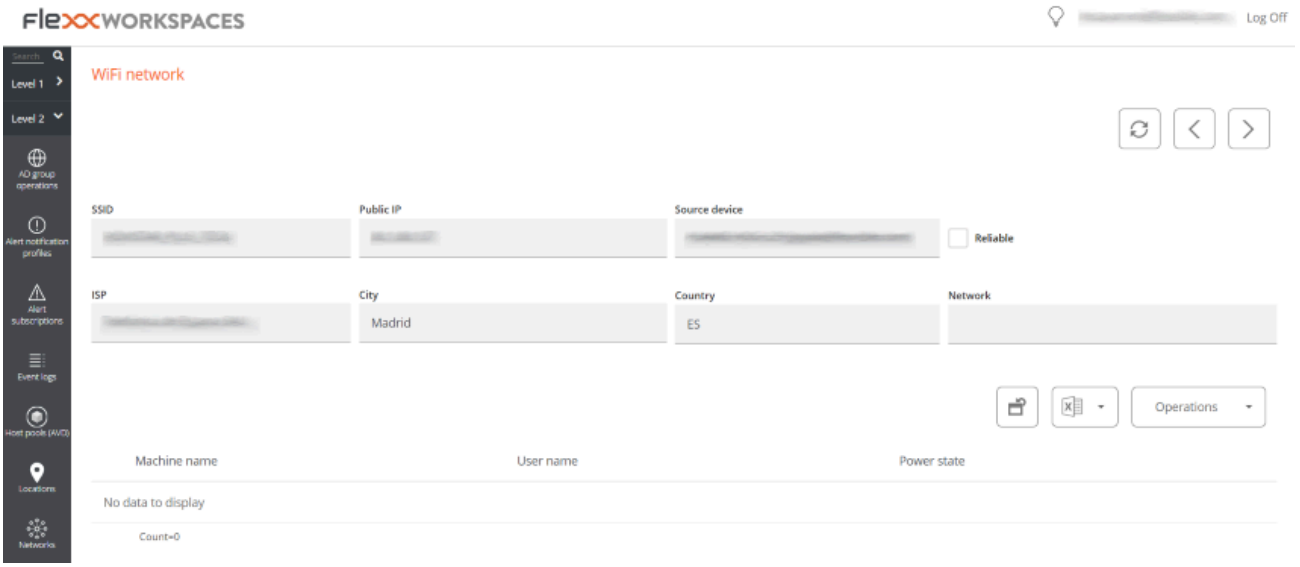
FlexxAgent collects multiple network information from devices. When FlexxAgent identifies the use of a wireless network, it is automatically created in Workspaces. These help to automatically maintain an inventory of all networks detected on devices to get precise location mapping based on network data. It is possible to associate it with Networks and Locations allowing to build a network inventory, the connected devices, the network operators in use, and much more.

## List view

The list view allows you to see the relation of wireless networks discovered by the agent. You can search, filter, sort, show or hide columns, and more.

It also allows selecting a wireless network from the list and marking it as a trusted network; in that case, if FlexxAgent detects the network again in more than five devices, it will recreate it.

## Detail view

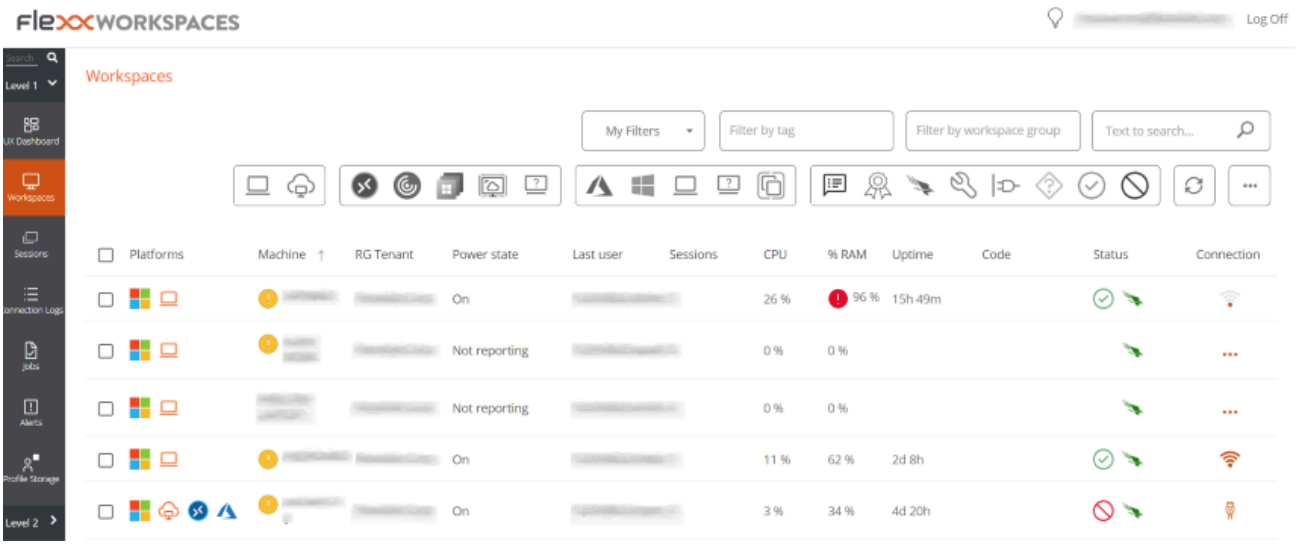



At the top block of the detailed view of a network, there is a list of collected fields:

- **SSID**: network name; by default the CIDR followed by the public IP. Allows customization.
- **Public IP**: The public IP for internet access of the network
- **Source device**: name of the device that declared the wireless network for the first time.
- **Trusted**: shows if this wireless network has been marked as trusted.
- **ISP**: connectivity provider
- **City**: Shows the city from which the internet exit is established.
- **Country**: shows the country from which the internet access is established.
- **Network**: allows associating this wireless network with a `Network`.

Connected devices to the network are displayed at the bottom.

# Workspaces / Guides and tutorials for Workspaces



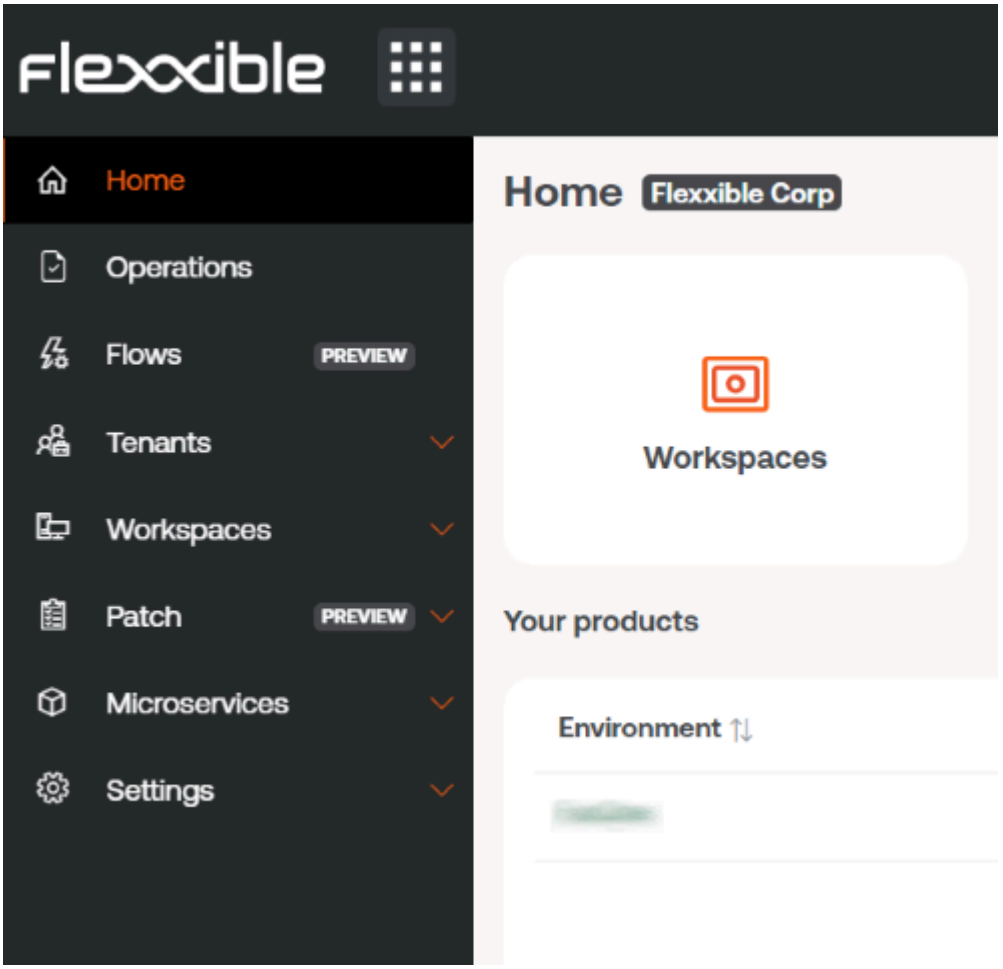

This section offers resources designed to maximize the use of Workspaces. It includes detailed instructions on configuring and using functionalities, along with advanced settings that will allow you to tailor Workspaces to specific needs.

Each guide has been created to facilitate its understanding and application, regardless of the user's experience level. In addition to step-by-step instructions, you will also find detailed procedures and solutions to common problems.

# Workspaces / Guides and tutorials / Configure email alerts

Any operator authorized by the Level 2 role can configure the receipt of email alerts:

1. Open the `Workspaces` module.



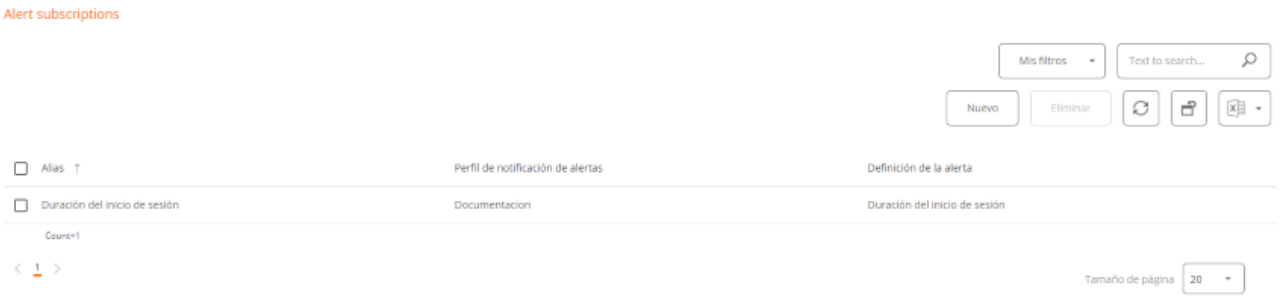

2. In the left menu, go to `Level 2` -> `Alert Notification Profiles`.

3. Click on `New` in the top right. This action will allow you to create a new profile to receive alert notifications. You need to define a name for the profile and the email address or addresses to which notifications will be sent.


4. Click the `Save` button in the top right.
5. Next, link an alert definition to the notification profile that was created in previous steps. Select the `Alerts Subscriptions` option from the `Level 2` menu in the left navigation bar. Click on the `New` button on the top left. A panel like the following will appear:


6. Name the subscription with an alias, select the alert or alerts using the magnifying glass icon on the right side of the field. Using this icon will bring up a floating panel to search and select one or more alerts. Then, select the desired subscription profile (in this example, the one created in previous steps).

7. Once the fields are filled, click the `Save` button. The new subscription will appear in the list.




In this example, each time an alert is issued about the session startup duration, the notification profile called “Documentation” will be notified by email to the address or addresses specified in its definition.

# Workspaces / Guides and tutorials / How to provide remote assistance to a user

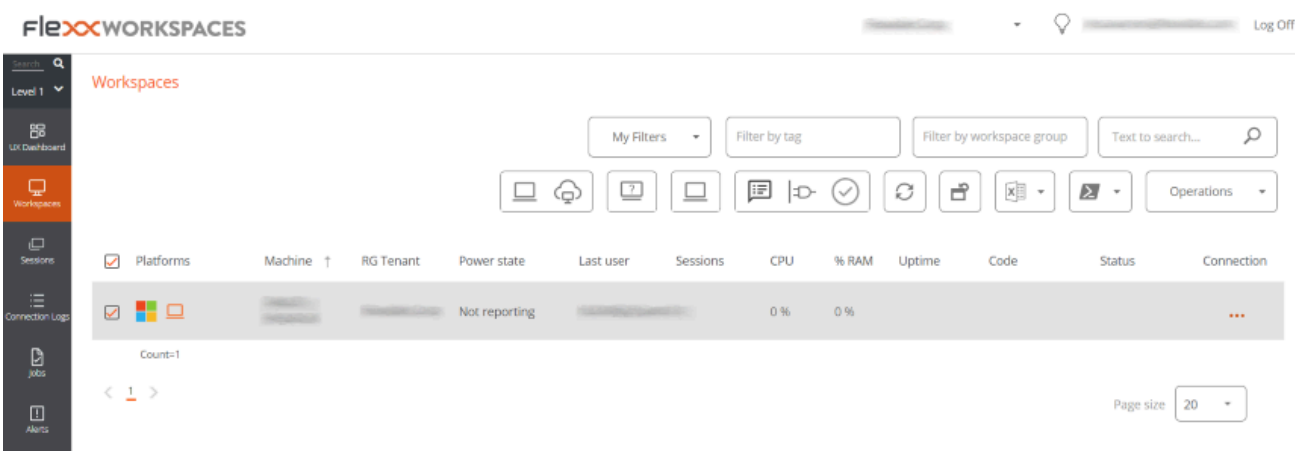
Remote assistance allows direct operation on a user's workstation desktop. The operator acts as the device administrator and works remotely with the user's desktop.

To provide remote assistance:

1. Access the `Workspaces` module.
2. Access the `Workspaces` or `Sessions` section from the navigation bar on the left side.

> Sessions allow searching for a specific user, while `Workspaces` lists the available devices. When performing remote assistance on a device, it will be conducted on the session that is currently active.

1. Search and/or select the device/session on which remote assistance will be performed.

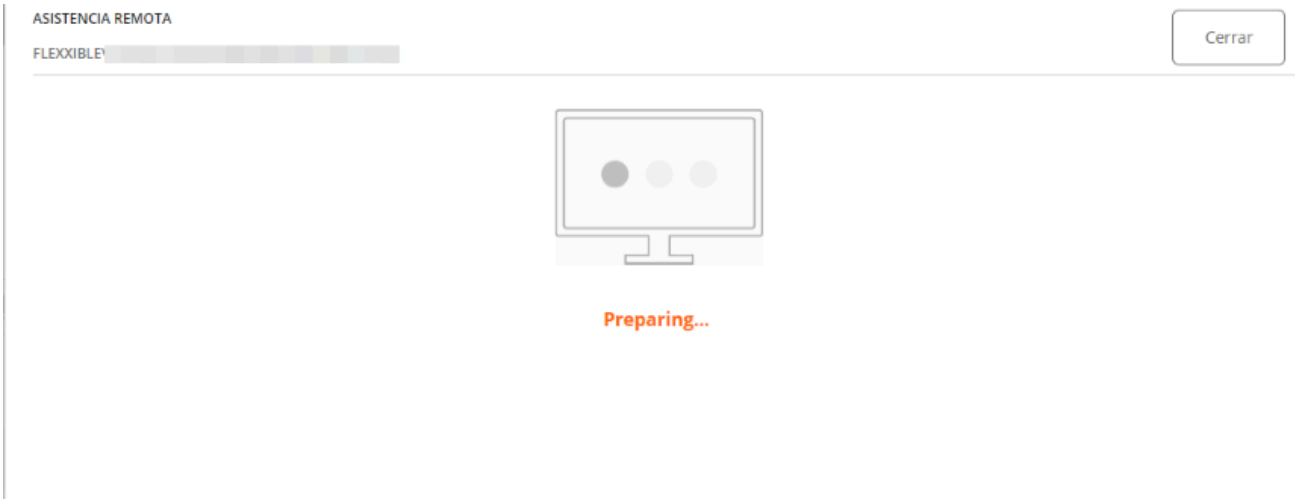



4. Open the `Operations` menu on the button in the upper bar of the equipment list. In some cases, as in the previous image, the button will be behind the button with three dots (...) on the mentioned bar. Next, select:

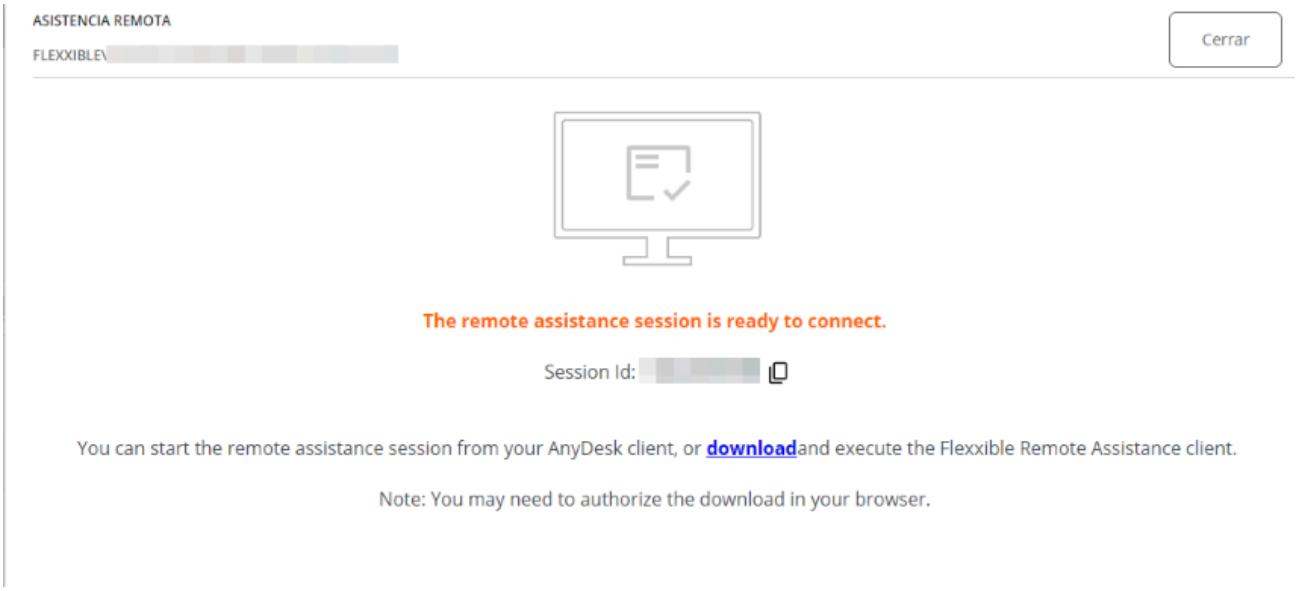
   `Operations` -> `Remote Assistance` -> `Start remote assistance`

5. Select `Ok` to confirm the operation.

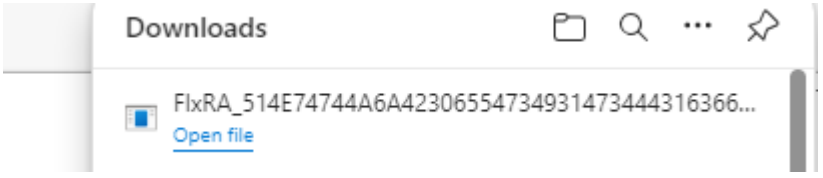
6. A floating panel will appear indicating that remote assistance is being prepared.



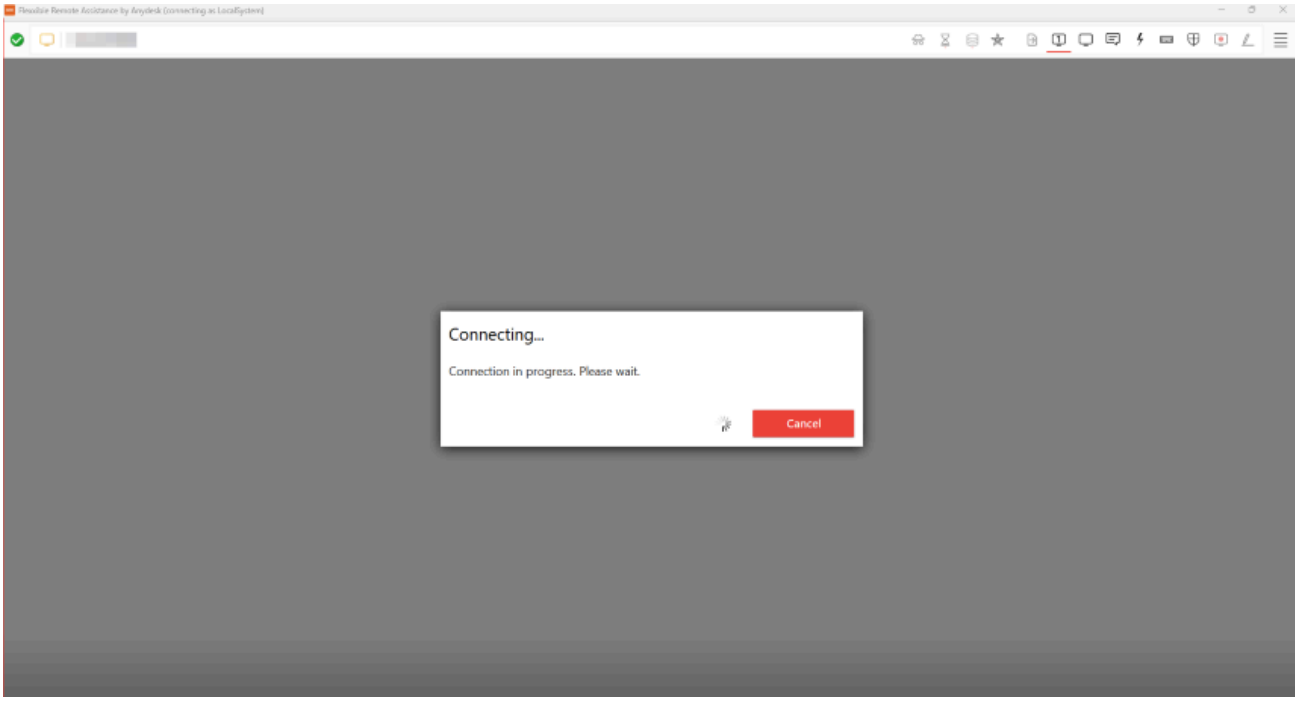

7. Once prepared, the information will appear.




8. This assistance is temporary, and the operator will need to download an executable file from the `download` link in this floating panel.

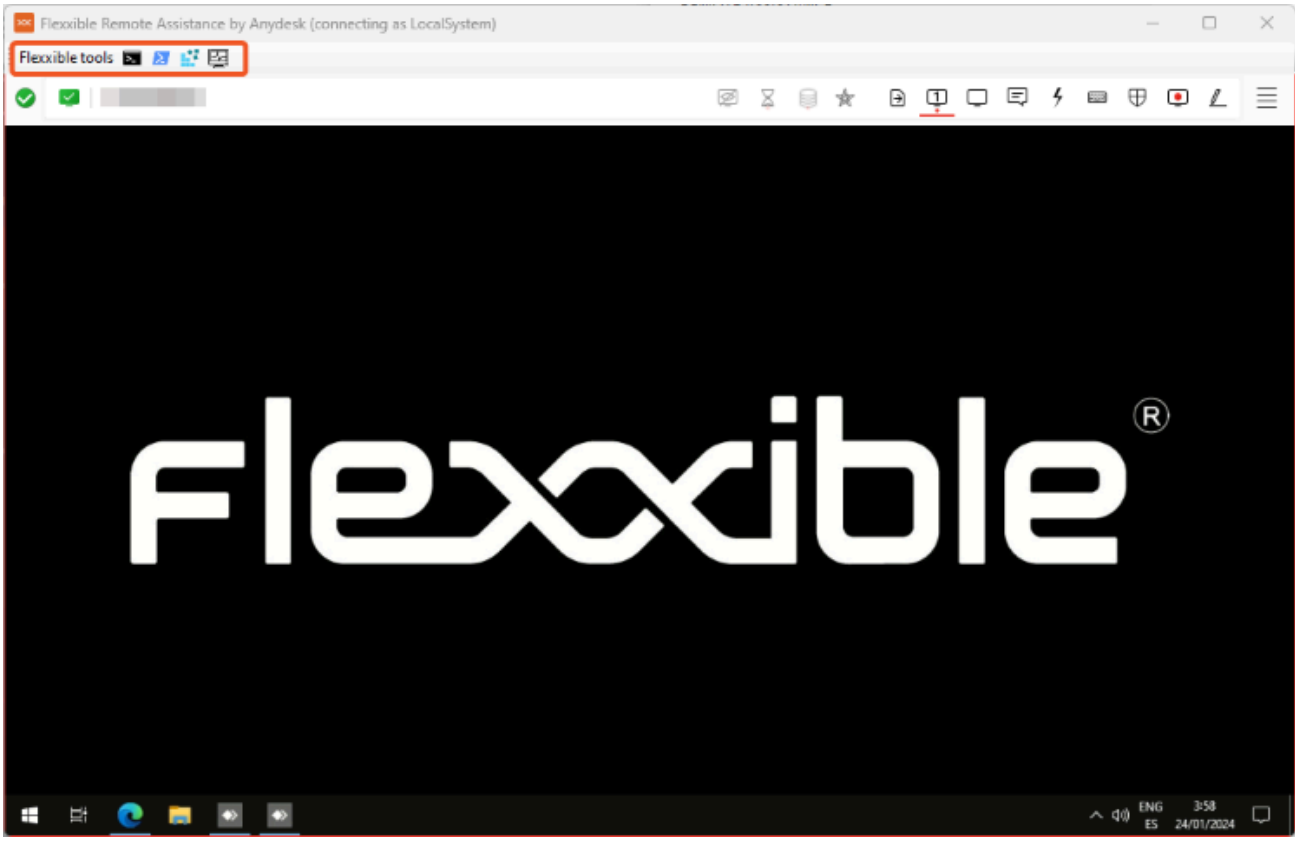



9. Download and run the file. This operation will run an application to facilitate remote assistance. The operator will have to wait for the user to give permission to perform remote assistance on their device.




10. Once the user grants their consent, the remote assistance session can be conducted. The operator has access to the user's desktop and can perform operations and provide the needed help to solve the user's problems.

If the operator has the necessary permissions and is in a user session without administrative permissions, they can use `Flexxible Tools` to act on the device with administrative permissions:



# Workspaces / Guides and tutorials / Change Automatic Restart Sign-On (ARSO) settings

On devices with Windows 10 1903+, Automatic Restart Sign-On (ARSO) is a Windows feature designed to allow a user to sign in automatically after a system restart, especially after installing updates.

Windows temporarily stores the user's credentials in the Credential Manager and uses them to restore the session without manual intervention. However, to maintain security, although the session is restored automatically, the device remains locked and requires the user to unlock it with their PIN, password, or biometric authentication before fully accessing the system.

This functionality can cause sessions to appear in the session view as if they are established when no user is actually working on the device. To avoid this, it is possible to disable ARSO.

## Modify ARSO settings on a device

To disable ARSO, the following options are available:

**GPO**

> `Computer Configuration -> Administrative Templates -> Windows Components -> Windows sign in Options`

**Registry editing**

> `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\DisableAutomaticRestartSignOn = 1 (DWORD)`

**Intune Policy**

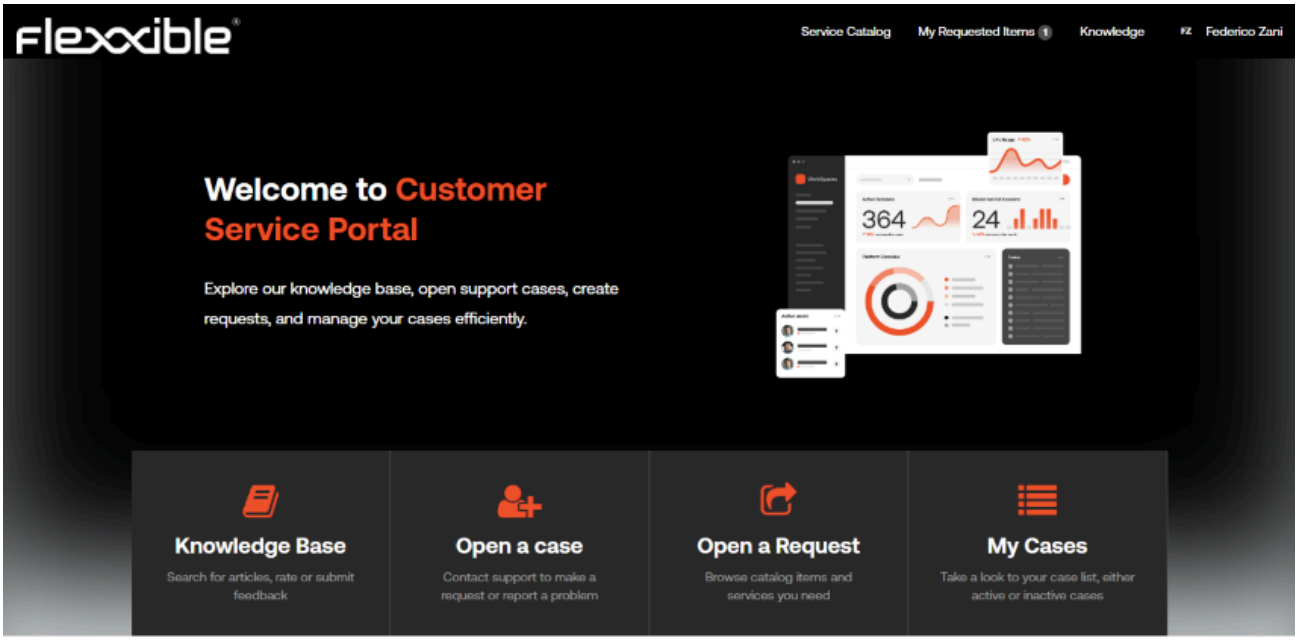
- Platform: Windows 10 and later

- **Profile type**: Administrative Templates
- **Path**: `\Windows Components\Windows Logon Options`

More information: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/winlogon-automatic-restart-sign-on--arso-#policy-1

# Automate

It's the module that provides users and IT teams, through a portal, a catalog of microservices that can be executed automatically, offering a self-service panel, accessible via browser for the user. It also offers the possibility to contact the specialized support team for any incidents, requests, or queries.




Thanks to the workflows developed by the Flexxible team using ServiceNow, it is possible to execute the microservices based on approval workflows defined with the client and proactive management in incident resolution. The fact that the Automate module is based on ServiceNow also allows easy integration with customers' CRM tools, whether by email, APIs, Integration HUB, etc. In this way, end users, technical staff, and administrative personnel are in direct contact with Flexxible's operations teams.

From Automate it is possible to:

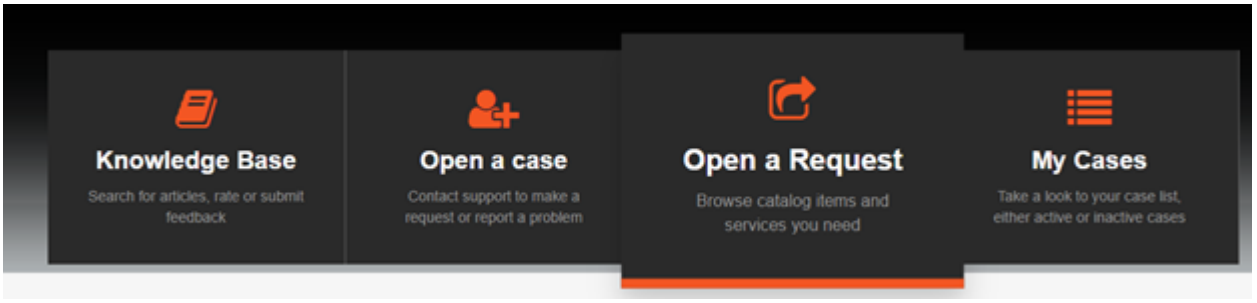
- Publish a self-service dashboard for end users and technical teams.
- Contact Flexxible support services.

# Automate / Self-Service Panel

Automate is a module developed for the interaction of the client with the Flexxible support team and is also responsible for the automatic execution of microservices that, due to their particular configuration, need to go through an approval workflow or the selection of various parameters before they can be executed.

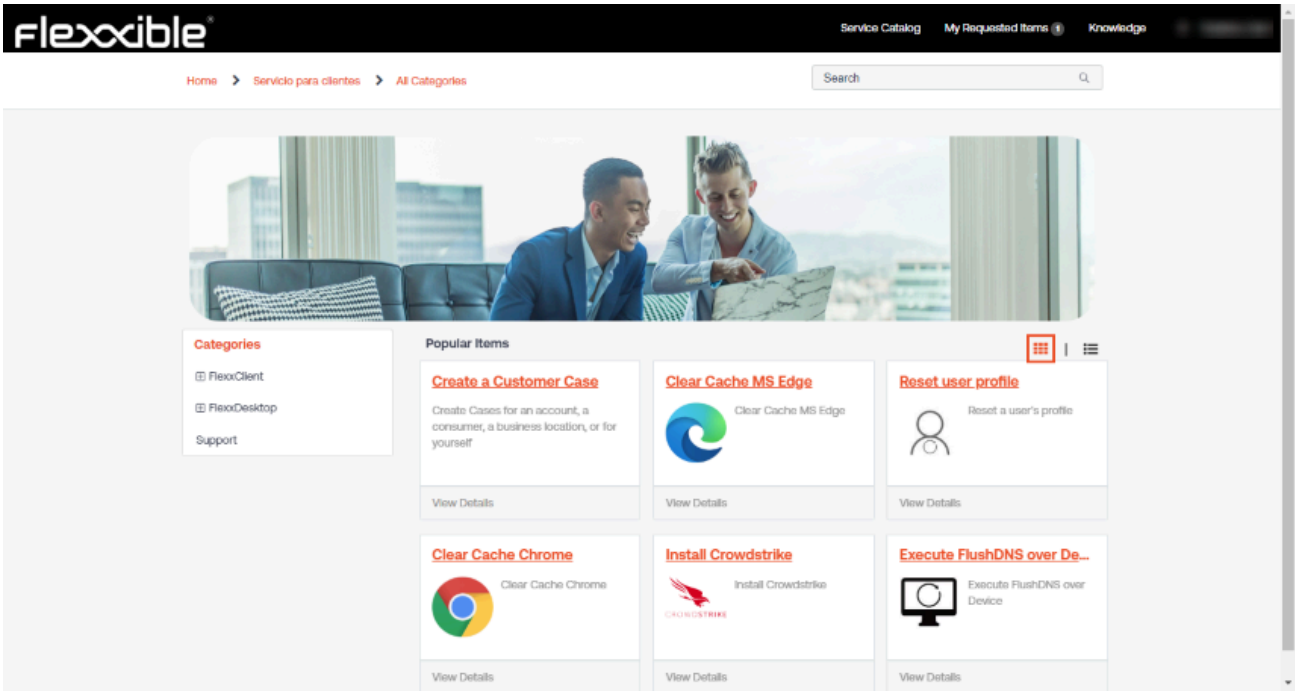
## Features

On the main screen of the Automate portal, there's a section called “Open a Request”.



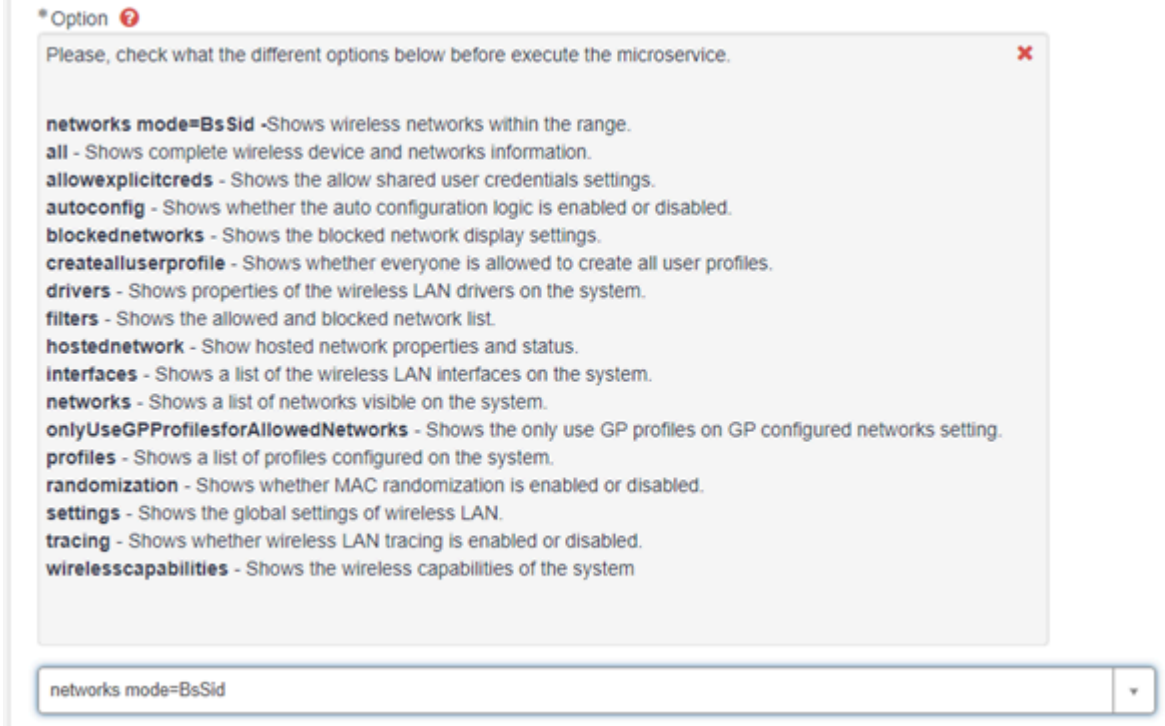

This section leads to a catalog of microservices available based on the services contracted by the client. This catalog may contain automations for FlexxClient, FlexxDesktop, or even both, depending on the active subscription products.

To access the available microservices, the user only needs to select the available/desired option and the different categories with the existing microservices will be displayed. By selecting one of the categories, the enabled microservices for it will appear on the right:

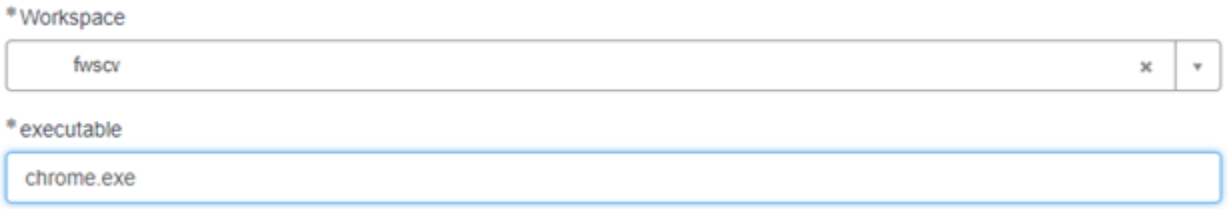



# Parameters

Certain microservices may have different selectable values; for example, in the case of “Get Wifi information”, where the user can select the type of information they want to obtain:



In other cases, it is necessary for the user to directly enter the variable value of the microservice execution; for example, in “Kill Process by EXE name” it will be the user who must indicate the name of the executable they want to remove from the computer:




# Approval Workflow

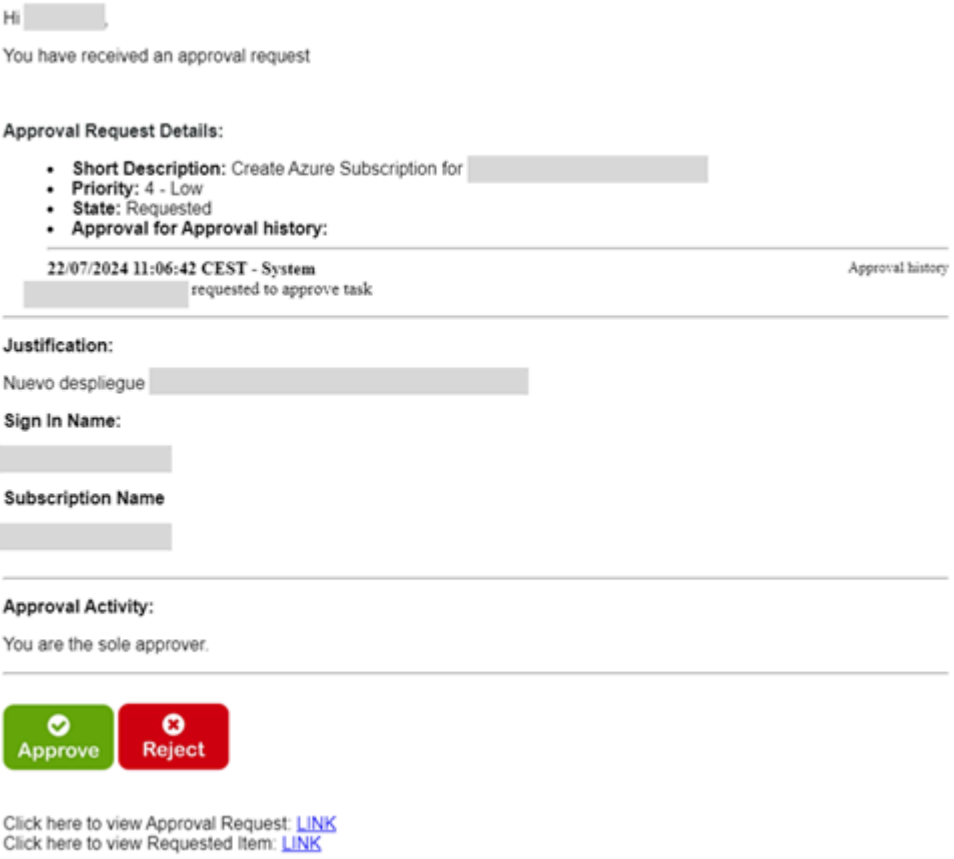
Certain requests may require approval before they can be executed automatically, as they may have a financial impact, or perhaps require prior analysis to ensure they can be executed safely. For example, the deployment of new virtual desktops within a DaaS service environment, or the modification of a registry key on physical machines for specific application configuration.

Automate allows approval workflows to be defined for the microservices identified within that casuistry. By default, there are two types of approval flows:

- Approval by a client or MSP manager: in this case, one or more users within the organization with permissions to approve requests are identified. When a user requests the execution of a microservice that requires approval, the approvers will receive an email indicating the details of the request, as well as the possibility to approve, reject it directly from the email, or access the request for more information.
- Approval by a client or MSP manager and the Flexxible manager: this type of approval flow is indicated for requests where new resources are deployed within a FlexxDesktop environment, where Flexxible is responsible for the service (FlexxDesktop Advanced, Enterprise, or Edge). In this way, the request is analyzed by the technical team before execution to ensure it does not affect the service provided to the client.

The image below shows an example of the notification automatically sent by the system requesting approval for the execution of the microservice to create a new Azure

subscription. In this case, given the economic impact, the client has decided to include it within the approval flows.


Hi ,

You have received an approval request

**Approval Request Details:**

- **Short Description:** Create Azure Subscription for
- **Priority:** 4 - Low
- **State:** Requested
- **Approval for Approval history:**

22/07/2024 11:06:42 CEST - System — Approval history
requested to approve task

**Justification:**

Nuevo despliegue

**Sign In Name:**

**Subscription Name**

**Approval Activity:**

You are the sole approver.

Approve Reject

Click here to view Approval Request: LINK
Click here to view Requested Item: LINK

# Default Microservices Included

Flexxible has an Automate catalog of microservices available to FlexxDesktop customers. The following are included:

- Active Directory:
  - Active Directory VM reset Account
  - Create AD user account
- Image Management
  - Create Snapshot from Template
  - Restore Snapshot from Template
- Session Management
  - Backup User Profile

    - Close user Session
    - Close all user sessions
    - Reset user Profile
    - Restore user profile Backup
- Workspace Management
    - Create a set of APPServers or VDIs
    - Execute action over workspace
    - Execute action over workspace group
    - Modify Resources Assigned to VM
    - Set maintenance OF/OFF for a workspace
    - Set maintenance OF/OFF for a workspace group
    - Update Set of VMs

The client can request through their service provider or directly to Flexxible the creation of other microservices to meet the specific requirements of their operation.

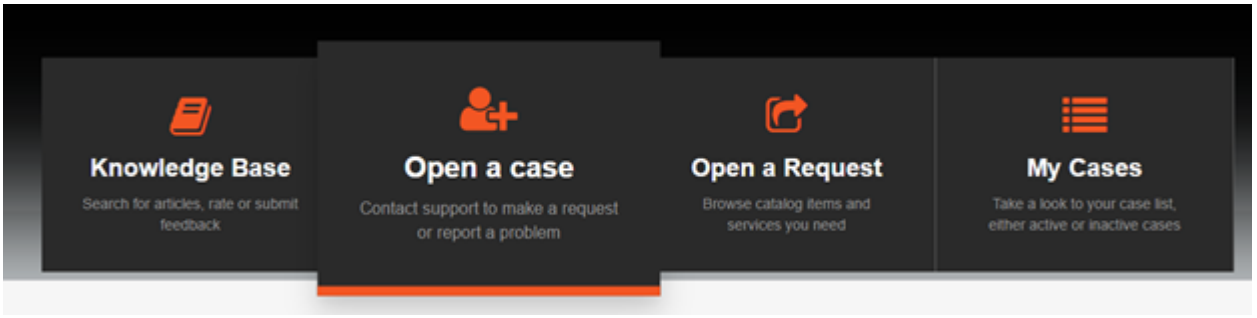
# Automate / Support

Automate allows end users, technical staff, and administrative personnel to interact with the Flexxible team through support options that allow opening and staying updated on the lifecycle of support cases.

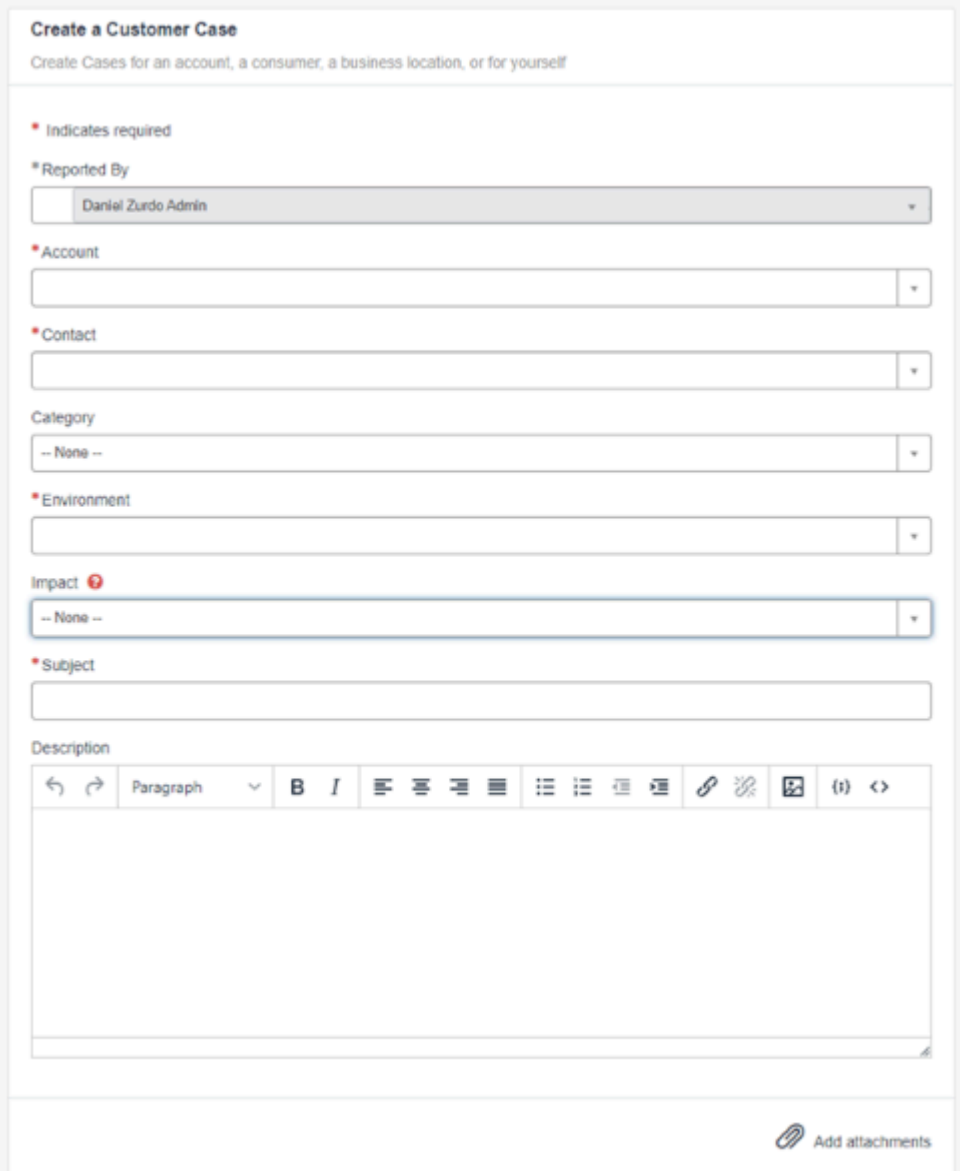
## Case opening

For any user, whether from the technical team or an end user, to open a support case with Flexxible, they must have been previously registered through the portal with the necessary permissions to access Automate services.

Once the user is inside the portal, the option to open a case will appear in the central part of the page, as shown in the following image:




Once the user clicks on `Open a case`, a screen will appear where, based on their permissions, they can select the account on which they want to open the case or if they want to open it on behalf of someone else.




## Required Information

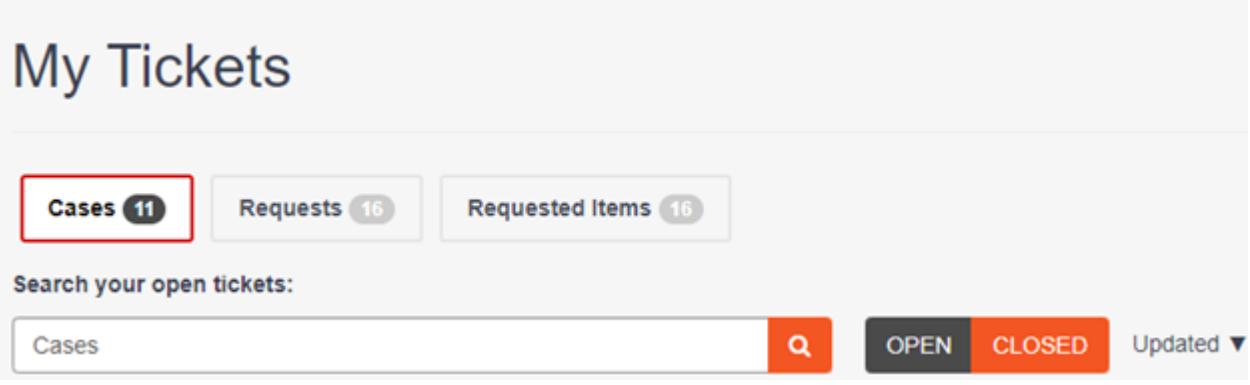
| Field | Caption |
| --- | --- |
| `reported by` | It will always be the user who opens the case. |
| `Account` | It will be selectable if the user belongs to an MSP and has more than one client/account assigned. |
| `contact` | It is used to open the case “on behalf of”; that is, on behalf of another user who has the issue, query, or request. |

| Field | Caption |
| --- | --- |
| `Environment` | It is related to the tenant or reporting group where the user's team with the issue, query, or request is located. |
| `Impact` | It is the categorization of the urgency of the case being opened; it can have three values: “High”, “Medium”, and “Low”. |
| `Subject` | It is to provide a brief description of what is required. |
| `Description` | It is to provide case details so that the operations teams can start working on it. The more detail provided, the easier it will be to complete the request. |

There is also an option at the bottom right of the form to add attachments to the request. Images or documents that can facilitate the completion of the requested task can be included.

## Case tracking

Once a case has been created on the main screen, information about cases will appear under the `My tickets` section, both those being managed and those already resolved.

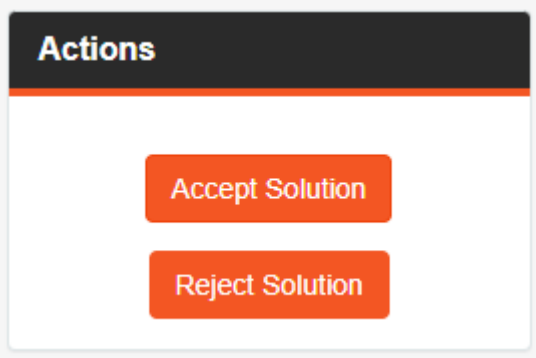



This information is also accessible from the upper menu of the page, in the `My Cases` section.

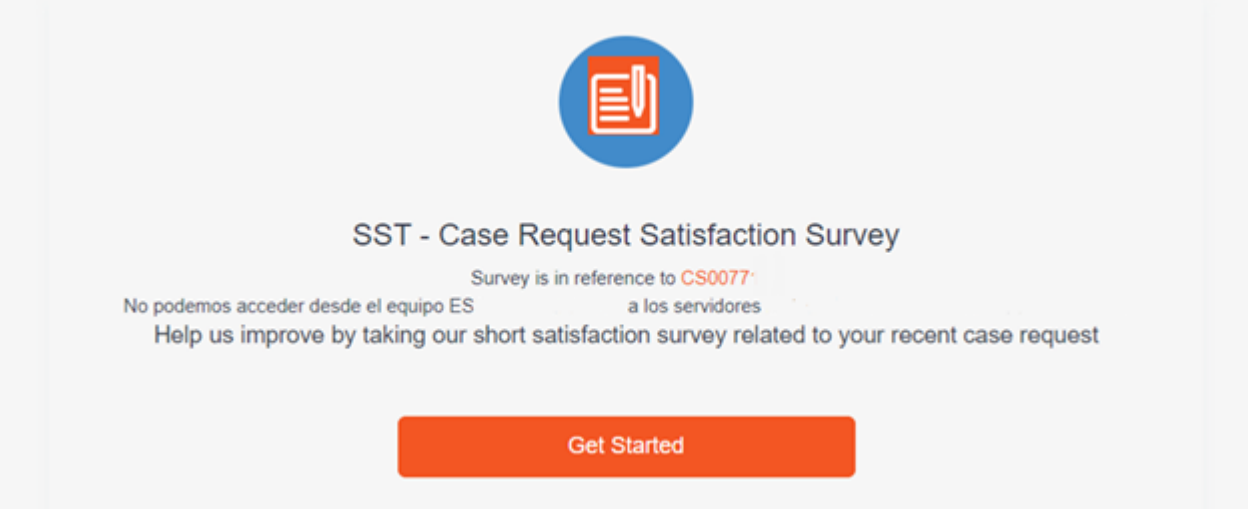
# Case statuses

A case is in the `New` state when it has been created.

When a case has been resolved, it changes to the `Resolved` state. The user can accept the resolution, in which case the ticket will change to the `Closed` state, or reject the resolution so the case reverts to the `Open` state. To reject or accept the request, it is necessary to access the ticket and in the `Actions` section select the desired option.




If the resolution acceptance is selected, the system may ask you to complete a two-question survey.




If the rejection of the solution is selected, a new screen will appear requesting the reasons for rejecting it. Once the information has been added in the text field in the form, the `Reject Solution` button will be enabled as shown in the following image:


# Case closure

While the Flexxible team is working on a case, the user can close it if the issue has been resolved or for any other reason. To do this, access the case and, within the `Actions` section, press `Close case`.

# Monitor

Monitor is a monitoring module based on Grafana Cloud, which allows graphical visualization of information obtained from Workspaces and Analyzer. It queries data from the APIs and displays them in custom graphs for good information management. Its main function is to help monitor and analyze various data sources in real-time, facilitating the interpretation and tracking of systems and applications.

## System and application monitoring

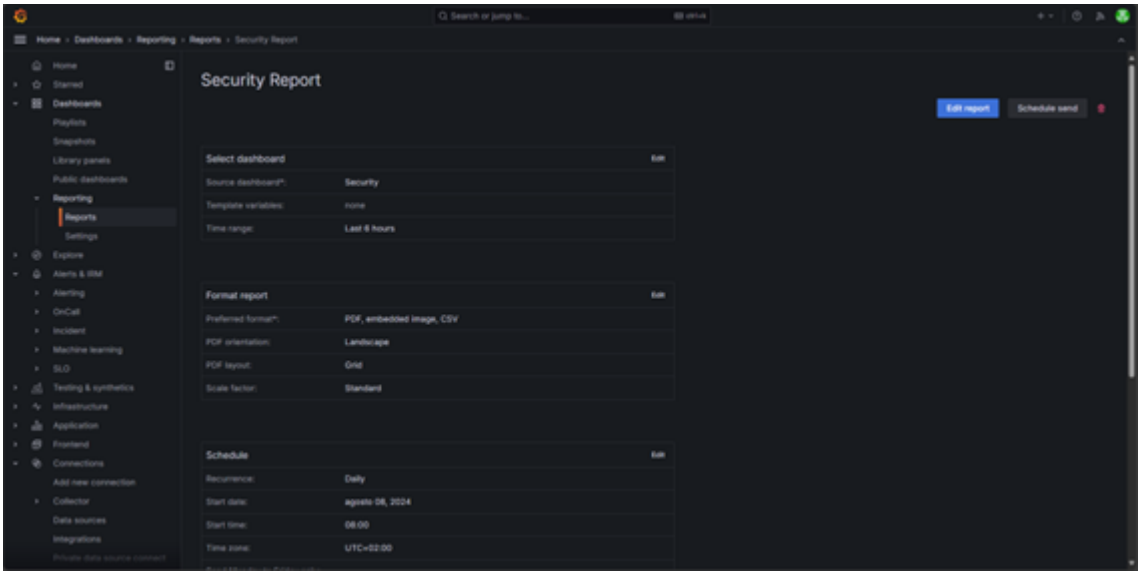
Monitor supervises systems and applications. It can monitor the status and performance of devices linked to Workspaces, as well as the applications installed on them.


## Real-time data visualization

With Monitor, you can see all the information from Workspaces and applications in real-time. It allows setting specific time intervals for each dashboard to emphasize specific moments. It also helps identify and prevent errors as they happen and to analyze incidents by time intervals.


## Analysis and reports

One of Monitor's key features is its ability to analyze data in detail and generate automatic reports. This is useful to understand how resources work, make informed decisions, and improve efficiency.




## Data sources

Monitor can integrate with multiple data sources. This functionality allows gathering and visualizing information from different tools. Currently, by obtaining data from Workspaces and Analyzer, it can provide a complete view of the systems and applications, integrating

queries to observe specific data. This integration offers various benefits such as centralizing information, correlating it, and flexibility when graphing it.

## Paneles de control (dashboards)

One of Monitor's most powerful features is its dashboards, which allow you to visualize, analyze, and monitor data more efficiently by creating panels that display information obtained from data sources.

These panels not only display data graphically but also offer interactivity with the user, allowing exploration of information, application of filters, and adjustment of time ranges to analyze trends or patterns.

Some functionalities of the dashboards:

- Full customization
- Interactive visualization
- Share and collaborate

## Alerts and notifications

Configurations that monitor a specific metric and send alerts when it reaches a predefined threshold. This feature allows you to stay informed in real-time about important events and take action when necessary, facilitating intervention and minimizing the impact of potential problems before they become critical incidents.

## User and permissions management

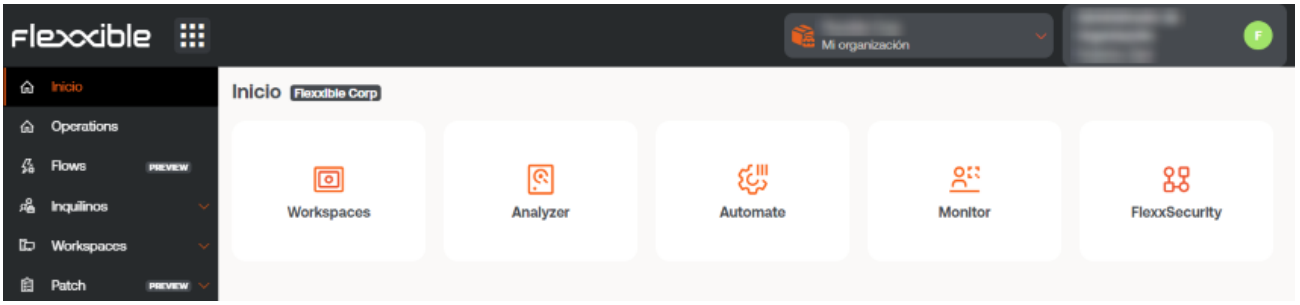
User and permissions management allows controlling who can access the dashboards, what actions users can perform, or limit access to certain data sources, helping to secure and maintain the integrity of the information.

Some key functions in user and permission management:

- User groups: allows managing users by groups, facilitating the management of permissions at a group level.

- Folder and dashboard access control: permissions can be configured at the folder or dashboard level, allowing control over who can access certain information.

## Access to Monitor

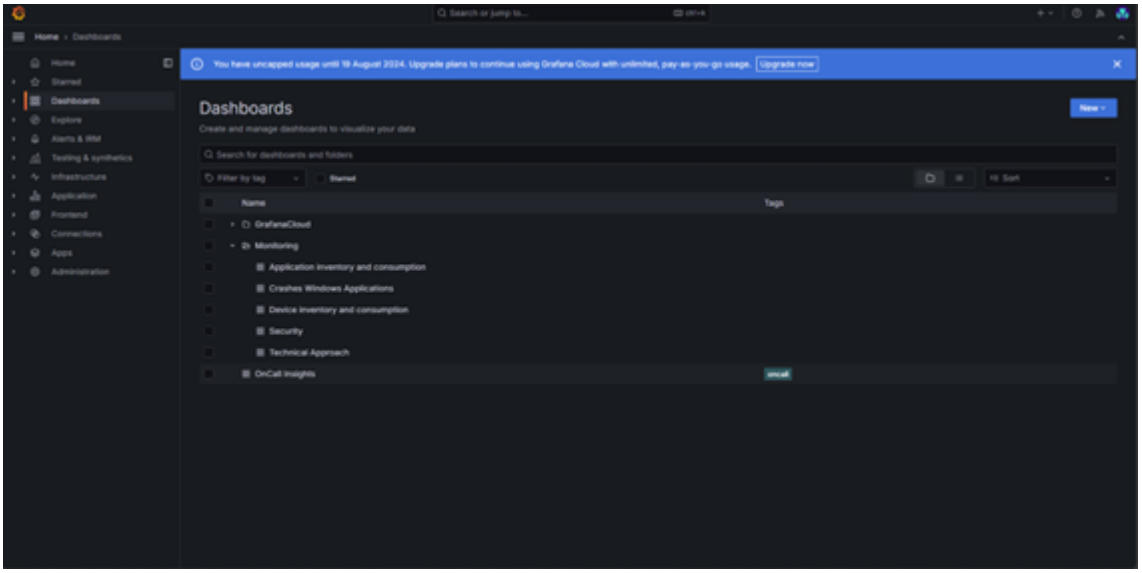



'Monitor' can be accessed from Portal. Clicking on the module will lead to the LogIn page:

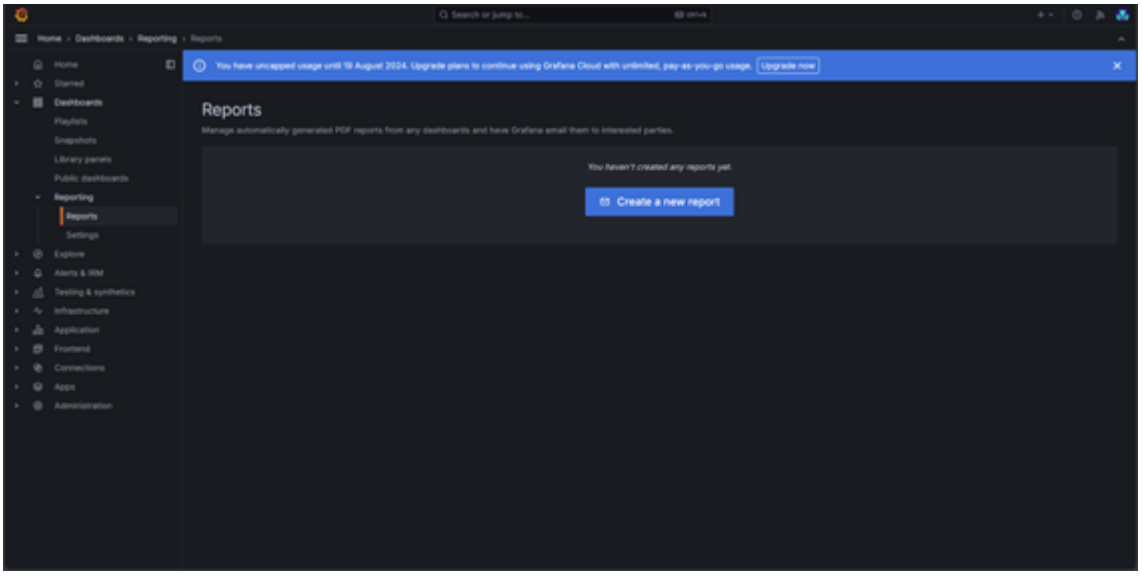
- Select the `Sign In` option to log in.
- Enter username and password.

## Navigate

To access all available charts and navigate through them, select `Dashboards` -> `Monitoring`.




You can configure or manage automatic or on-demand reports by accessing `Dashboards` -> `Reporting-Reports`.




## Default dashboards

There are five default charts that allow managing different aspects of the environment:

- Technical focus
- Windows application errors
- Application inventory and consumption
- Device inventory and consumption
- Security

It is possible to adapt or create custom charts depending on the focus or usage.

# Use Cases

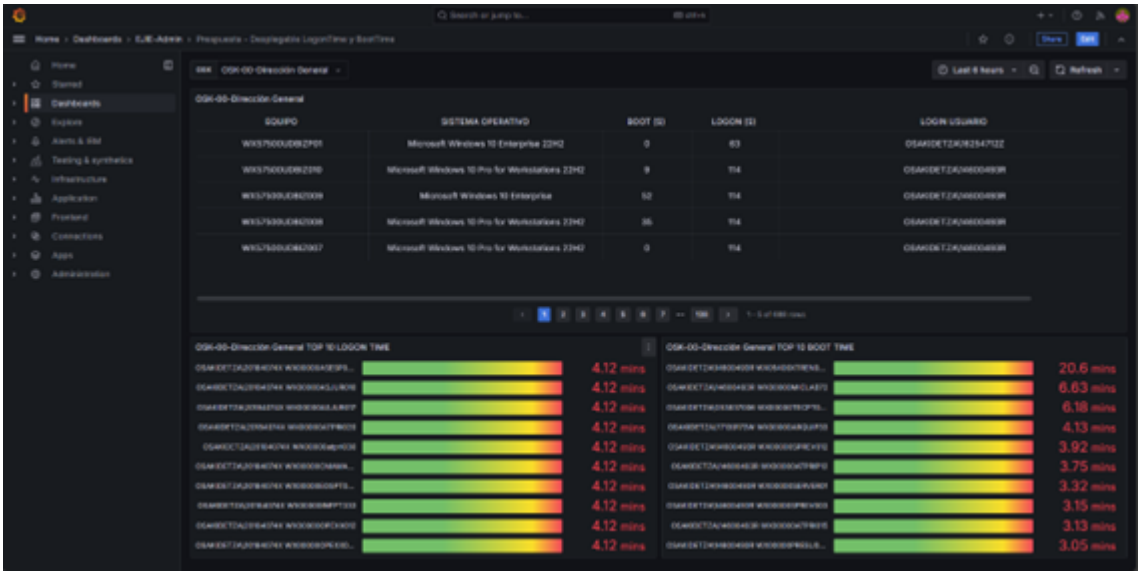
Below are a series of use cases as examples to describe Monitor's possibilities.

## Uptime monitoring

> If you need to ensure devices comply with usage policies by monitoring uptime and user logon time.

With Monitor, it is possible to create detailed charts showing each device's uptime and user logon time. It also offers the option to apply filters for a clear and detailed view of

devices showing high times or to generate a periodic report with this data. All of this is useful if the organization needs to ensure its devices comply with usage policies.



## Application monitoring

> You need to control consumption on devices, monitor the usage of a group of applications or a specific application.

Monitor creates charts that collect information on consumption, application usage, versions, etc. Thanks to Monitor's dashboards, it is possible to have an overall view of device usage to know how to act based on the analysis results.

## Environmental impact assessment

> Given the significant number of copies made per printer in the last month, it is necessary to monitor and manage the environmental impact associated with these activities, and thus take measures to reduce the carbon footprint generated by printers.

By obtaining the data from Green IT it is possible to create monitoring and management panels that allow you to see the analysis of the environmental impact created, taking into account factors such as color, black and white prints, equipment switching on time, etc.