Flexxible®

Documentation

FXXOne

Document generated on: 19/1/2026

Contents

Introduction

FXXOne is a Remote Monitoring and Management (RMM) platform that allows real-time management of work devices. It offers tools for task automation, security control, and employee experience analysis, ensuring comprehensive remote management and supervision service.

It comes with many features, such as Flexxible Remote Assistance, detailed diagnostic data collection, system status notifications, self-repair of known issues, and unattended support procedures application.

FXXOne includes:

- Portal
- Workspaces
- Analyzer

Once the subscription is created, the following steps will be needed to start enjoying the service:

1. Access Portal.
2. Create a reporting group.
3. Download and install FlexxAgent on the devices you want to manage.

From there, the devices will report to the service and be ready for management from Portal and Workspaces; they will also provide analytics of applications, user experience, and other devices through Analyzer.

Documentation in PDF

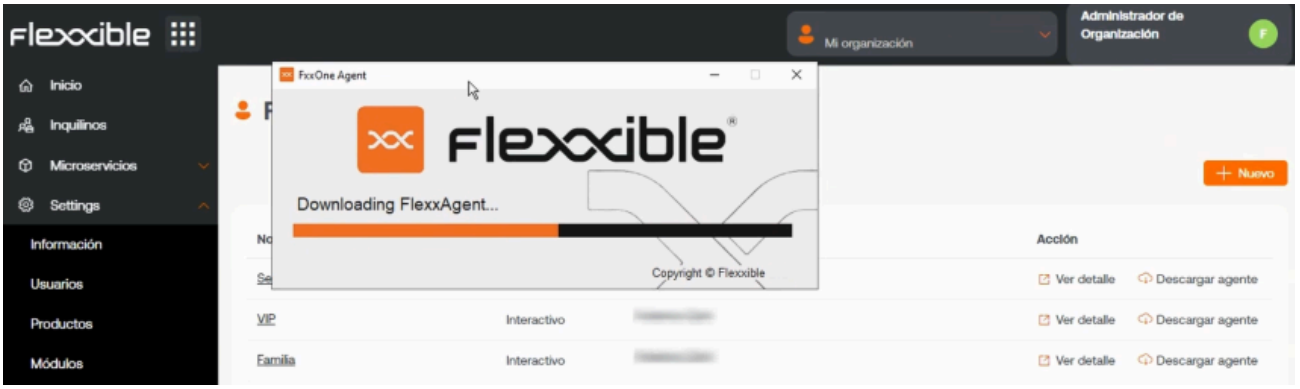
The documentation for **FXXOne** for this version can be downloaded here in PDF format.

> **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 operational details, installation, diagnostics, or specifics of FlexxAgent for each operating system are described in their corresponding article. The global functionalities of FlexxAgent, along with its operational capacity for each supported operating system, are defined in the following table:

Functionality	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	✅	✅	✅	✅	✅
FlexxAgent auto-update	✅	✅	✅	Managed by Google	Managed by Google Play

Functionality	Windows	Linux	macOS	Android	ChromeOS
				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
Custom fields	✅			N/A	N/A

Functionality	Windows	Linux	macOS	Android	ChromeOS
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	✅				
Interactive (attended) Flexxible Remote Assistance	✅				
Unattended Flexxible Remote Assistance	✅				
Dynamic Flexxible 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

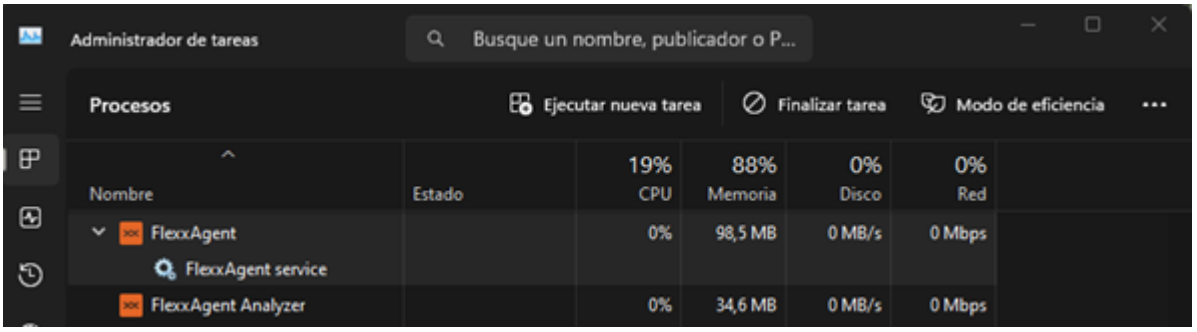
FlexxAgent / Supported Systems

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 or without a graphical interface, so it supports both unattended deployment methods and installation via wizard.



Service Architecture

FlexxAgent consists of a Windows service named **FlexxAgent Service**, which coordinates two processes:

- *FlexxAgent*, executed at the system level
- *FlexxAgent Analyzer*, started for each user session.

This architecture allows FlexxAgent to manage devices with multiple sessions (such as terminal servers, Citrix, or AVD) and obtain detailed metrics to enhance diagnostic capabilities.

Example:

- On a laptop, *FlexxAgent* (at the system level) and *FlexxAgent Analyzer* (under the user's identity) run.
- On a device with multiple sessions, besides *FlexxAgent*, a *FlexxAgent Analyzer* process will run for each session.

Consumption

FlexxAgent is optimized to minimize resource usage. The approximate values are:

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

FlexxAgent Process (system)

- Collection of performance information, hardware, sessions, profiles, disks, partitions, and Windows services: **every 60 seconds**.
- Sending event log error events: **every 10 minutes**.
- Updating user profile information: **every 15 minutes**.

FlexxAgent Analyzer Process (user)

- Analyzes application usage, diagnostic data, and user experience.
- Local data collection: **every 15 seconds**.
- Sending reports to the service: **every 5 minutes** (this metric may change in specific functionalities).

Supported versions

FlexxAgent is compatible with Windows operating systems currently in support cycle by Microsoft. Although it can be installed on unsupported versions, some features might not be available.

Full Compatibility

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

Limited Compatibility

- Windows 7 SP1
- Windows 8.1 SP1
- Windows Server 2008 R2 SP1
- Windows Server 2012

Software Requirements

FlexxAgent requires the following components:

- **.NET Framework 4.6.2 or later** (recommended: .NET Framework 4.8).
- **Windows PowerShell 4.0 or later** (recommended PowerShell 5.1).
    - Note: The execution policy for Azure PowerShell must be set to *Unrestricted*.

Considerations for Windows versions in EOL

On End-Of-Life (EOL) systems, FlexxAgent may exhibit limitations or lack of compatibility with certain features.

Unsupported Features

When using FlexxAgent on older Windows operating systems that are out of support, the following features are not supported:

- Collection of GPU consumption metrics.
- Flow execution.
- Execution of microservices by the end user.
- Obtaining information from storage units.
- In the case of virtual devices, detection of broker and hypervisor (limited according to provider).
- User Input Delay (UID) (only available from Windows Server 2019 and Windows 10 version 1809).

Mediator detection may not work for everyone. 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 R2

FlexxAgent can be installed on Windows 7 x64 or Windows Server 2008 R2 SP1 under the following conditions:

- Install the update KB4474419: (*SHA-2 code signing support update for Windows Server 2008 R2, Windows 7, and Windows Server 2008: September 23, 2019*).
- Install the update KB3140245: (*Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows*) 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** (recommended: 4.8).
- PowerShell 2.0 with Windows 7 is not compatible with TLS 1.2; install **Windows Management Framework 5.1**, which includes PowerShell 5.1.

Windows 8 and 2012

FlexxAgent installation supports Windows 8 under the following conditions:

- Requires **.NET Framework 4.6.2** (Microsoft blocks the installation of later versions on Windows 8.0).
- All Windows security updates must be applied to ensure compatibility with **TLS 1.2** and **SHA-2** code signing.

Download

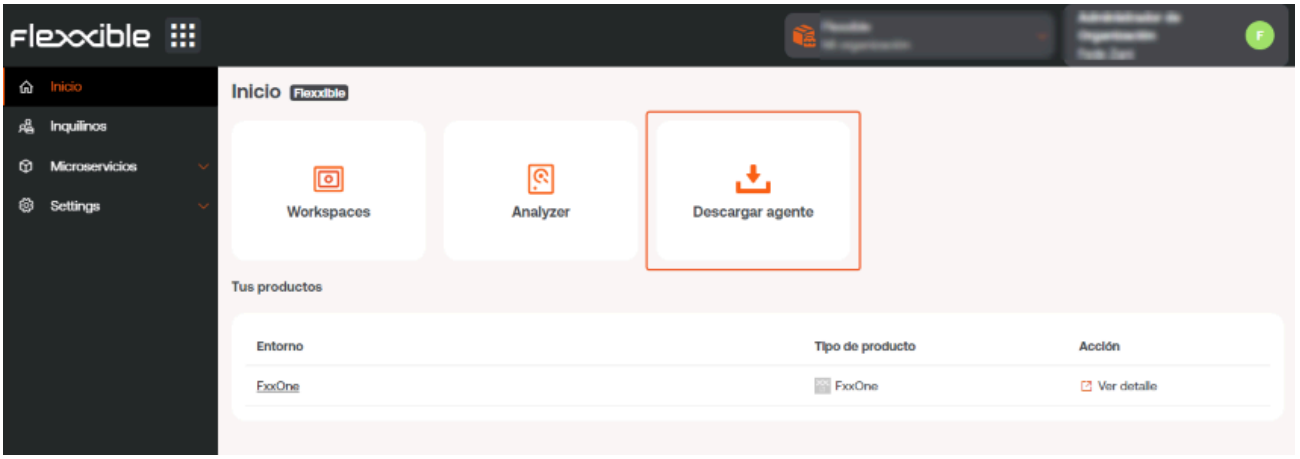
The installation binary download for FXXOne is available with and without graphical interface.

INSTALLATION BINARY DOWNLOAD WITH GRAPHICAL INTERFACE

BUTTON TO DOWNLOAD FLEXXAGENT

In `Portal` -> `Home`, the `Download agent` button will allow you to download FlexxAgent to the device. This option is available for all *Organization Administrator* users of any type of organization.

If the organization has more than one reporting group, clicking on the `Download agent` button will change the interface to the `Report groups` section to download FlexxAgent in the chosen report group.



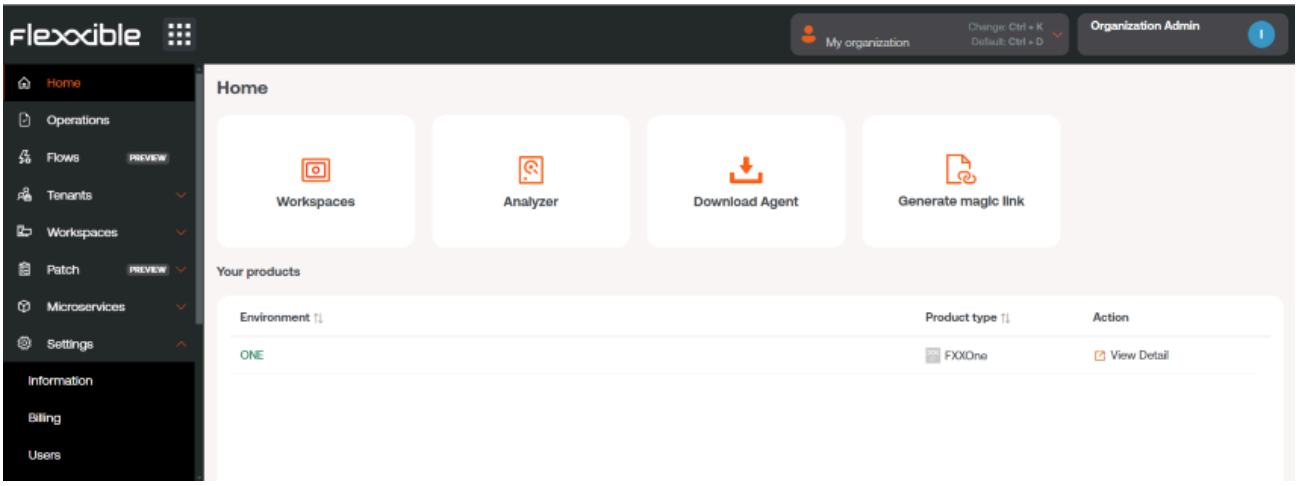
A few seconds after the installation, the device will be visible in the Workspaces module. All functionalities for controlling, monitoring, and automating tasks on your devices will be activated from that moment.

BUTTON TO GENERATE A MAGIC LINK

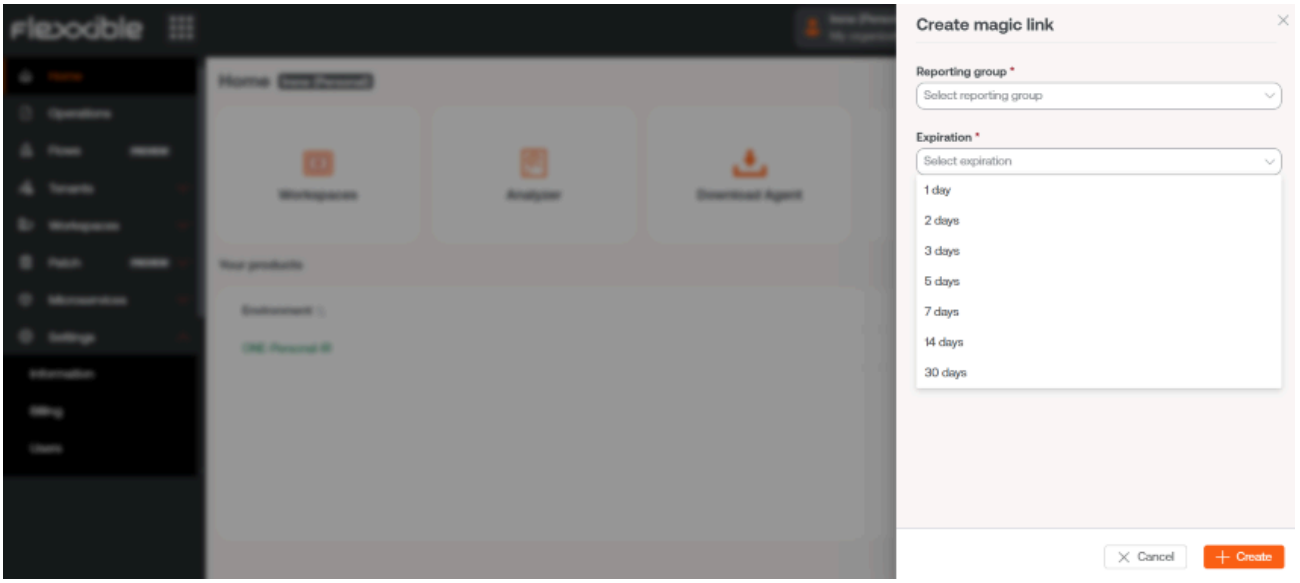
The `Generate magic link` button optimizes the access to download FlexxAgent on the devices. Allows users with the *Organization Administrator* role within a partner-type organization to generate and send a link to users so they can download the agent on their devices without being logged in.

Create magic link

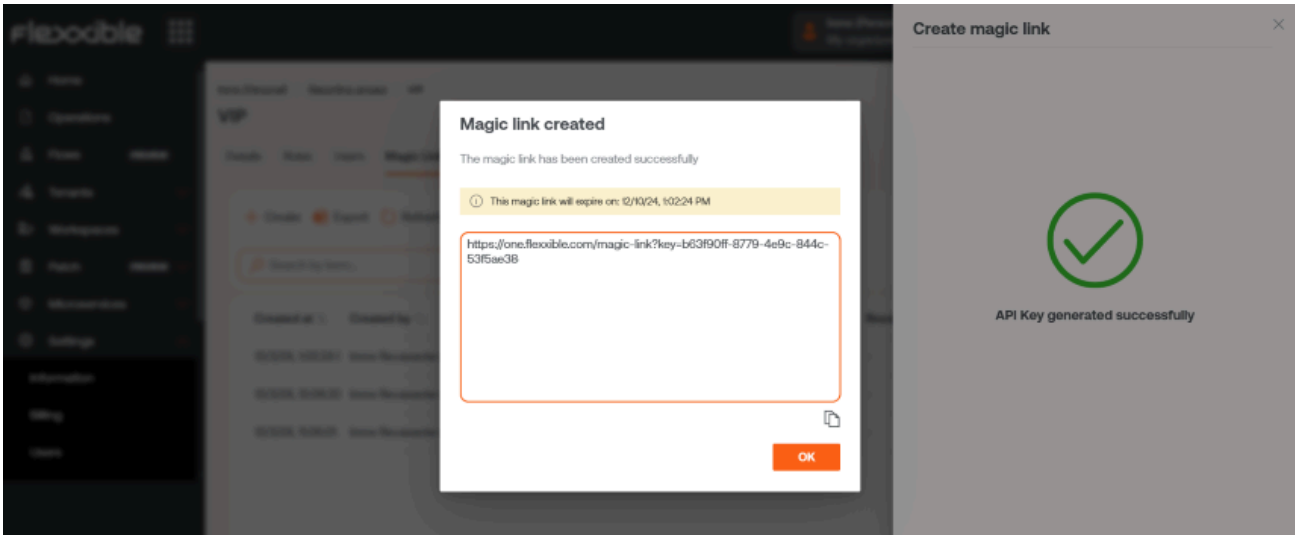
The `Generate a magic link` button is located on the home page of the Portal for users with an *Organization Administrator* role within a partner-type organization.



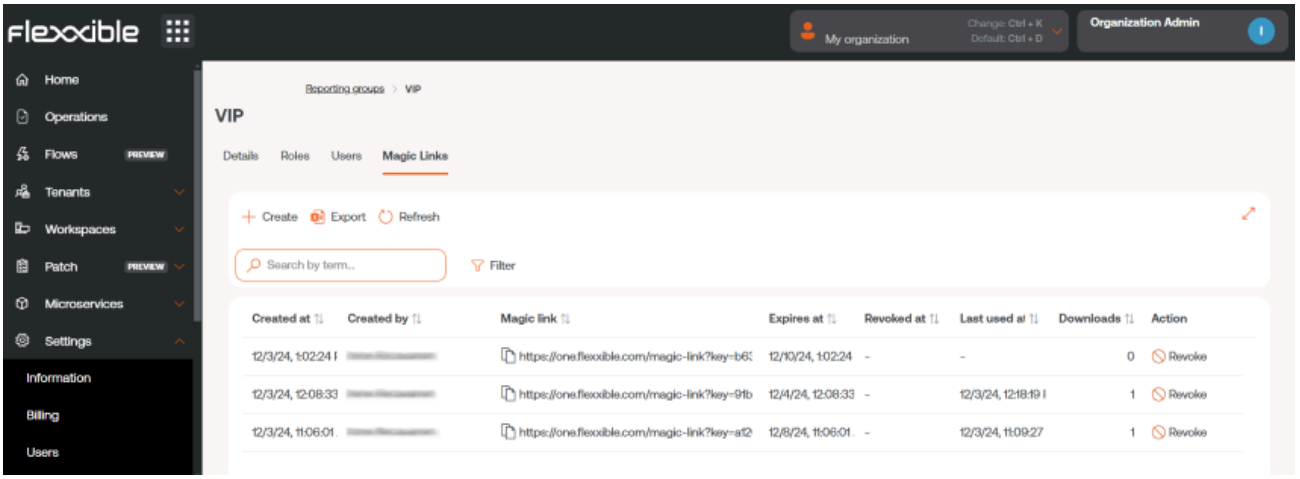
Clicking the button opens a form where you should specify which reporting group the link will be assigned to and for how long it will be active.



Next, a window will indicate that the link has been created. And it will allow you to copy it directly to share it.



By clicking `Accept`, the console will automatically go to the detail view of the selected reporting group. From there you can check the magic link just created, as well as others that have been created earlier.



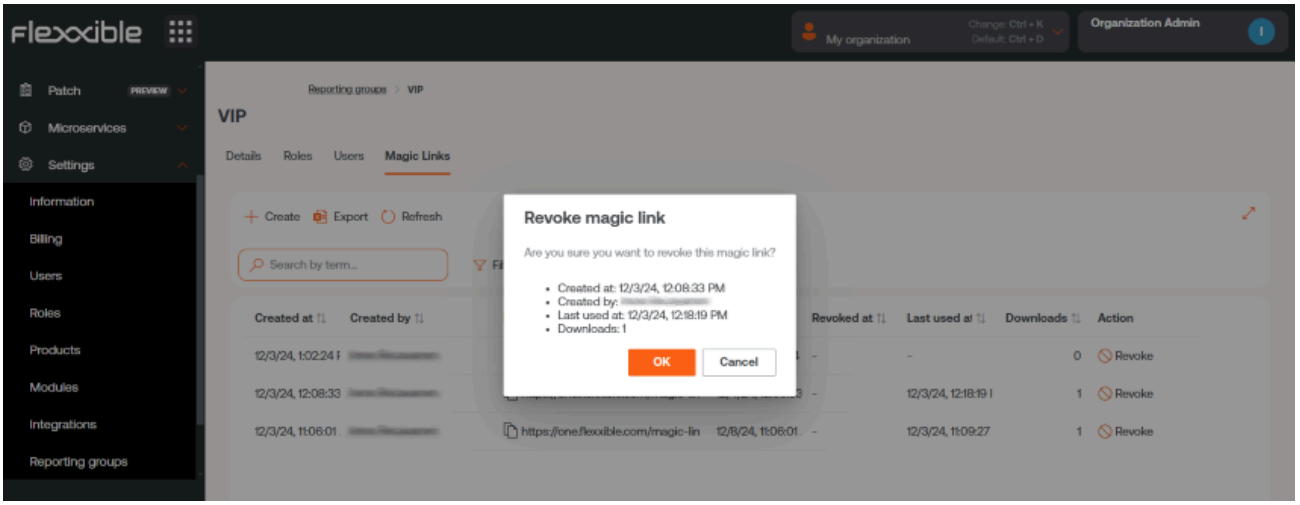
Use a magic link

To use the link just copy and paste it into the browser's address bar. At that moment, FlexxAgent will show the following screen, indicating that it has been downloaded on the device.

Revoke a magic link

A `Magic Link` can be revoked from `Portal` -> `Settings` -> `Report Groups`. In the list view, click on the reporting group where the `Magic link` you want to revoke is located. And then, in the `Action` field of the table, choose the `Revoke` option.

A window will appear to confirm the action.



By clicking `Accept`, a message will appear for a few seconds in the reporting group table informing of the action: "The magic link has been successfully revoked."

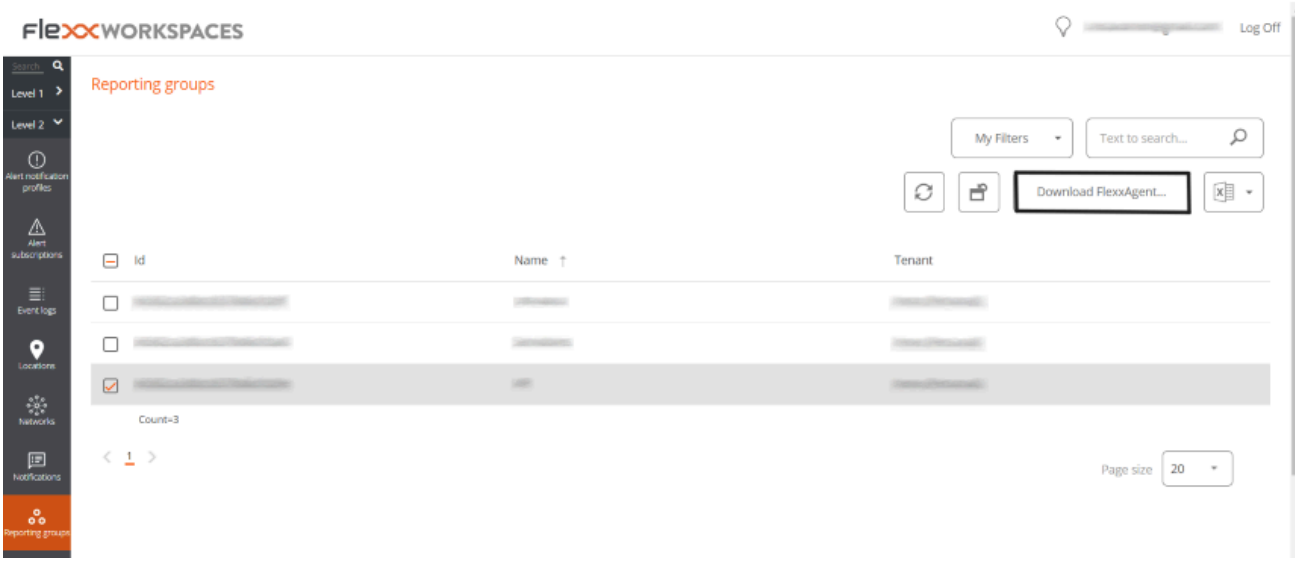
It is not possible to use a `Magic link` that has been revoked or has expired again.

BINARY WITHOUT GRAPHICAL INTERFACE

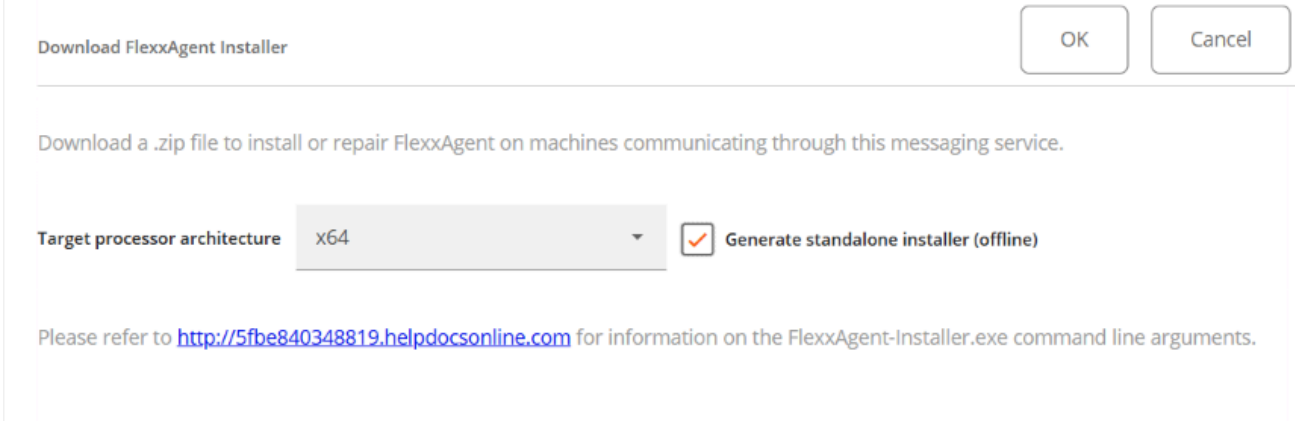
Steps to download:

1. Access `Workspaces` -> `Level 2` -> `Reporting Groups`.

2. In list view, select the reporting group you want to download the agent for and click `Download FlexxAgent`.



1. A window will open with the `Generate standalone installer (offline)` option, to download the FlexxAgent installer:



- If the option is selected: during installation, the binary will not require internet access for checking or downloading binaries.

- If not selected: the minimal installation package will be downloaded, which will access the internet to obtain the latest binaries.

Unattended Deployment

FlexxAgent supports unattended deployment via GPOs, Intune, SCCM, or other distribution tools.

Installation

The unattended installation of FlexxAgent is done via PowerShell.

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

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.	

Parameter	Type	Caption	
Help	[switch]	Lists the supported parameters, with type and description.	

Uninstall

To uninstall FlexxAgent unattended:

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

The Windows installer does not remove all files, folders, keys, or registry values created during the installation. For a clean system image, you can manually remove:

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 previous configuration must run:

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

For example:

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

Uninstallation Protection

This functionality prevents a user from uninstalling FlexxAgent. The configuration can be applied at the Product level or Report group level.

Requirements

- The configuration can only be performed by a user with the *Organization Admin* role.
- Minimum version of FlexxAgent: 25.4.2.

This functionality is disabled by default.

Configuration at Product Level

1. Go to `Portal` -> `Settings` -> `Organization`.
2. In the menu, select the `Products` tab.
3. In the table, choose the environment where you want to execute the functionality, and in the `Action` field click on `Agent Settings`.
4. In the form, enable or disable the `Uninstallation Protection` button.
5. Click on `Save`.

Configuration at Reporting Groups Level

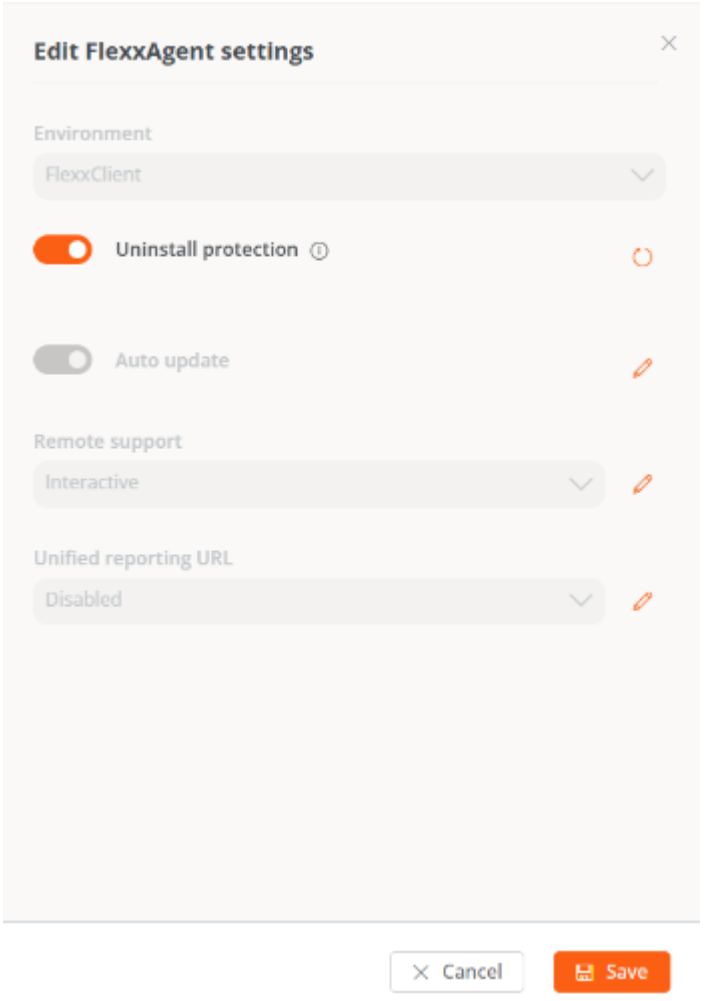
The feature can be executed on one or several reporting groups.

Enable protection for a reporting group

1. Go to `Portal` -> `Settings` -> `Reporting Groups`.
2. In the table, choose the reporting group where you want to execute the functionality, and in the `Action` field click on `Agent Settings`.

3. In the form, edit the `Uninstallation Protection` functionality (pencil-shaped button) to choose between enabling or disabling it.
4. Click on `Save`.

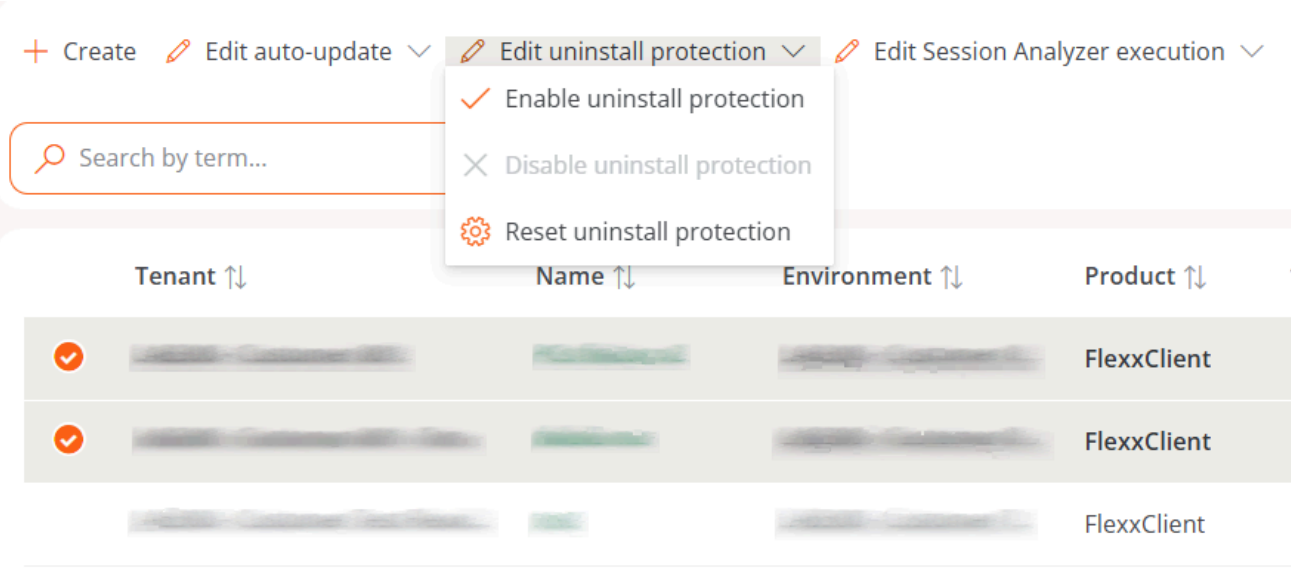
> **INFO**
>
> Reporting groups inherit the configuration made at the Product level; however, they can overwrite their own configuration.



Enable protection for multiple reporting groups

1. Go to `Portal` -> `Settings` -> `Reporting Groups`.
2. In the table, select the reporting groups where you want to execute the functionality.
3. Click on `Edit uninstallation protection`. Three options will be displayed:

- **Enable uninstallation protection.** Protects the reporting groups against uninstallation of FlexxAgent (this option will not be available if the feature is already enabled in Product).
- **Disable uninstallation protection.** Allows users to uninstall FlexxAgent (this option will not be available if the feature is already disabled in Product).
- **Reset uninstallation protection.** Applies the configuration that the Product has to which the report group belongs, whether enabled or disabled.



A device will have *FlexxAgent Uninstallation Protection* enabled in the following cases:

- The feature is enabled in the reporting group to which it belongs.
- The feature is deactivated in the reporting group (it is neither enabled nor disabled), but it is enabled at the Product level.

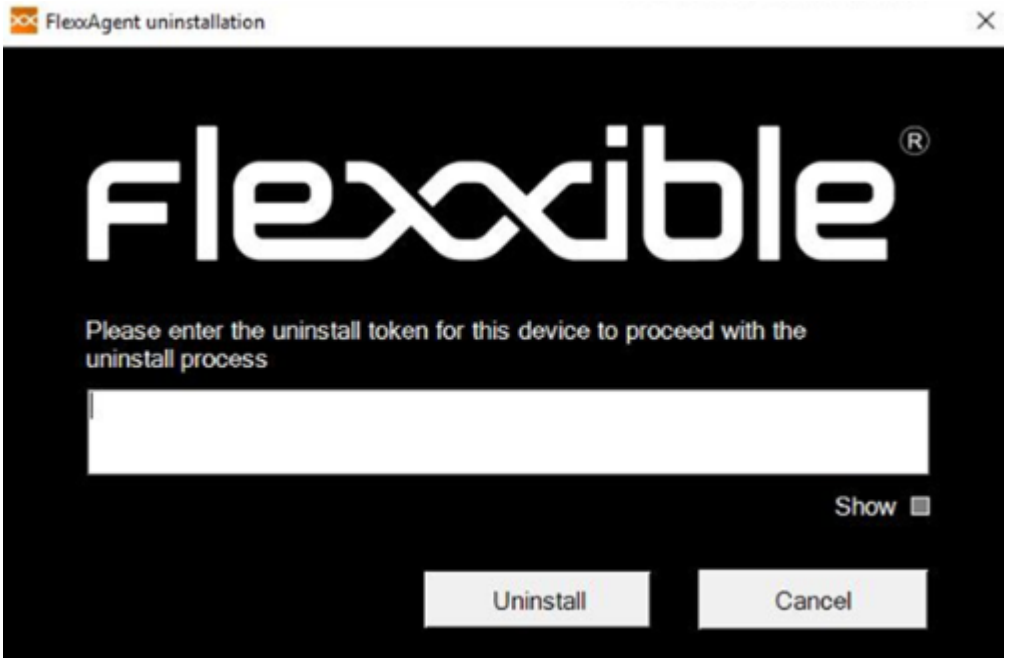
Ways to uninstall FlexxAgent with protection enabled

If a user has the feature enabled but needs to uninstall FlexxAgent, they will have two options:

1. Move the device to a reporting group that does not have protection enabled.
2. Via a token:

- Go to `Portal` -> `Workspaces` and select the device.

- Execute the action `Reveal uninstall token` which will display a unique token for that device valid until 23:59:59 UTC the next day.
- Go to the Windows Control Panel and uninstall FlexxAgent by entering the token.



Before managing the uninstallation of FlexxAgent through tools like Intune or custom scripts, move the desired devices to a reporting group that does not have protection enabled.

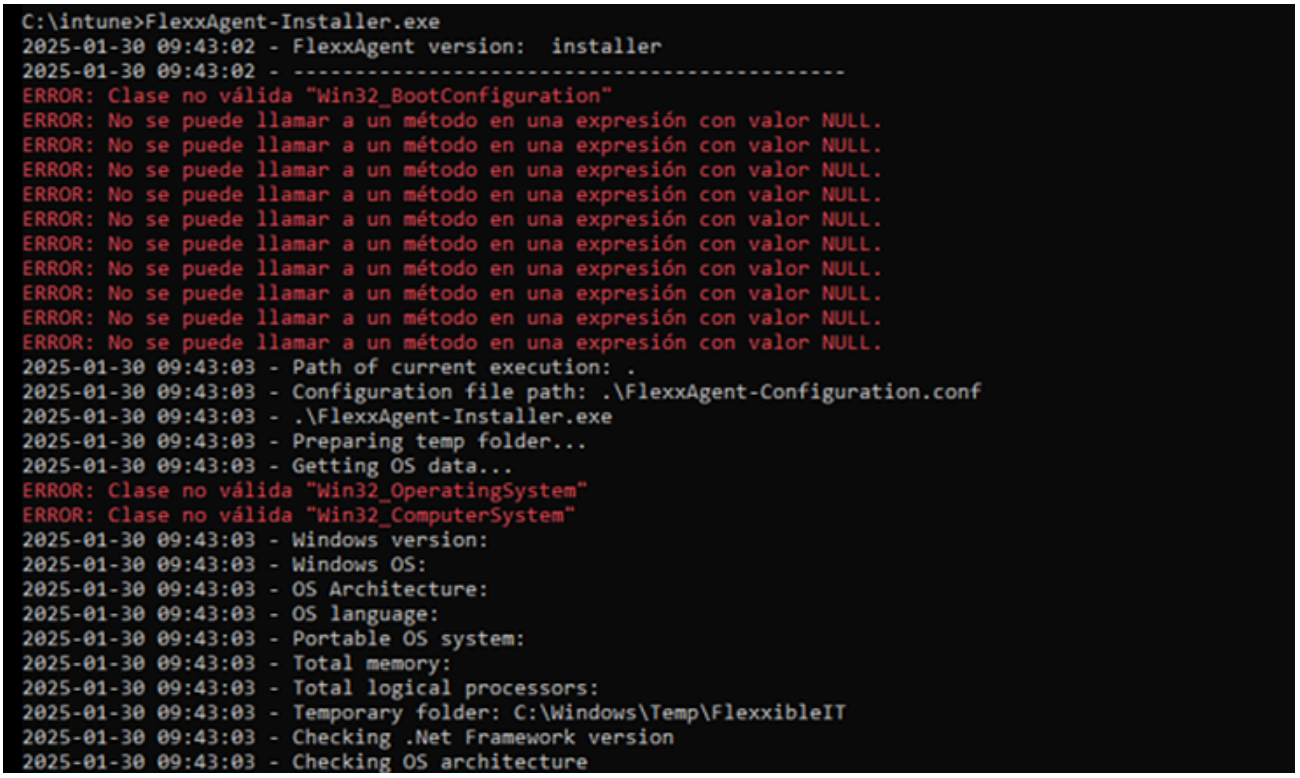
> **INFO**
>
> Flexxible recommends having a reporting group with *Uninstall Protection* disabled to facilitate the uninstallation of FlexxAgent on devices.

Known Issues

FlexxAgent installation

Issue 1 - Windows Management Instrumentation (WMI)

If the device has issues caused by the Windows Management Instrumentation (WMI) service during installation or reinstallation, 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:

`C:\Windows\Temp\FlexxibleIT`

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

FlexxAgent uninstallation

Issue - FlexxAgent remains in the service list

It might occur that FlexxAgent still appears in the list of services, even though it has been uninstalled and all files have been deleted. This would prevent reinstallation.

Solution

Run the following command as administrator in the CMD window:

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

Then, restart the device.

Proxy Configuration

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

Proxy Configuration via Command Line

Installation with parameters:

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

Where `ip.ad.dre.ss:port` corresponds to the IP or DNS and 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, FlexxAgent will report it directly (without proxy).

Proxy Configuration through Registry Keys

The registry keys that store the proxy configuration are located in:

`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

- Path: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Flexxible\FlexxAgent\Communications`
- Name: Proxy_URL
- 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

- Path: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Flexxible\FlexxAgent\Communications`
- Name: Proxy_User
- 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

- Path: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Flexxible\FlexxAgent\Communications`
- Name: Proxy_Pwd
- 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.

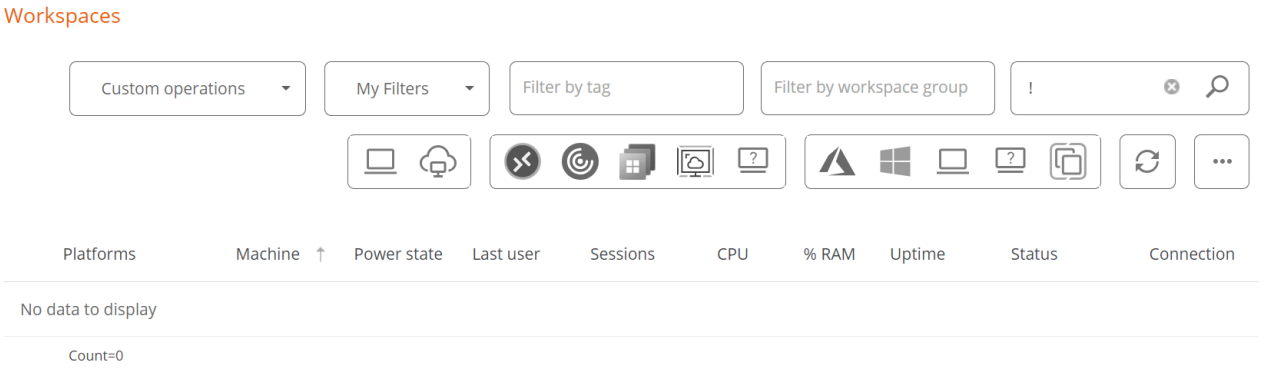
In either case, FlexxAgent encrypts the value as soon as it starts or attempts to transmit information. You can generate a Base64 encoded string from https://www.base64encode.org/.

> **INFO**
>
> Since FlexxAgent triggers a process at the system level (*FlexxAgent.exe*) and another at the session level (*FlexxAgent Analyzer.exe*), it may be necessary to define different proxy types for each, depending on how the proxy acts at one level or another.
>
> The `Proxy Type` can be defined from the FlexxAgent Settings in `Products`.

Manual Update

To update FlexxAgent manually:

1. Go to `Workspaces` -> `Level 1` -> `Workspaces` -> `Operations` -> `FlexxAgent` -> `Update FlexxAgent`.



2. 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 version.

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

Logs

Logs provide information and help diagnose issues during installation.

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

Installation and update logs

Location: `%LOCALAPPDATA%\Flexxible`

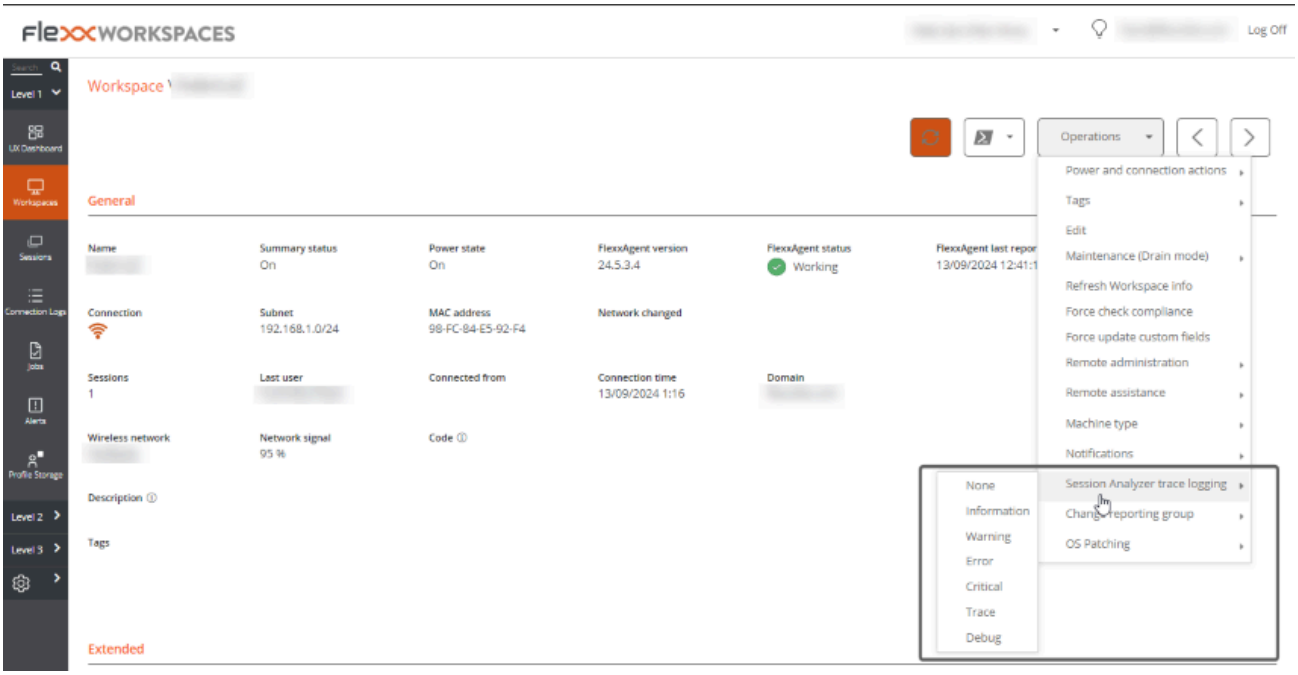
Contains information on the installation or update process, dependencies, and process details.

FlexxAgent Analyzer logs

Location: `%LOCALAPPDATA%\FAAgent\Logs`

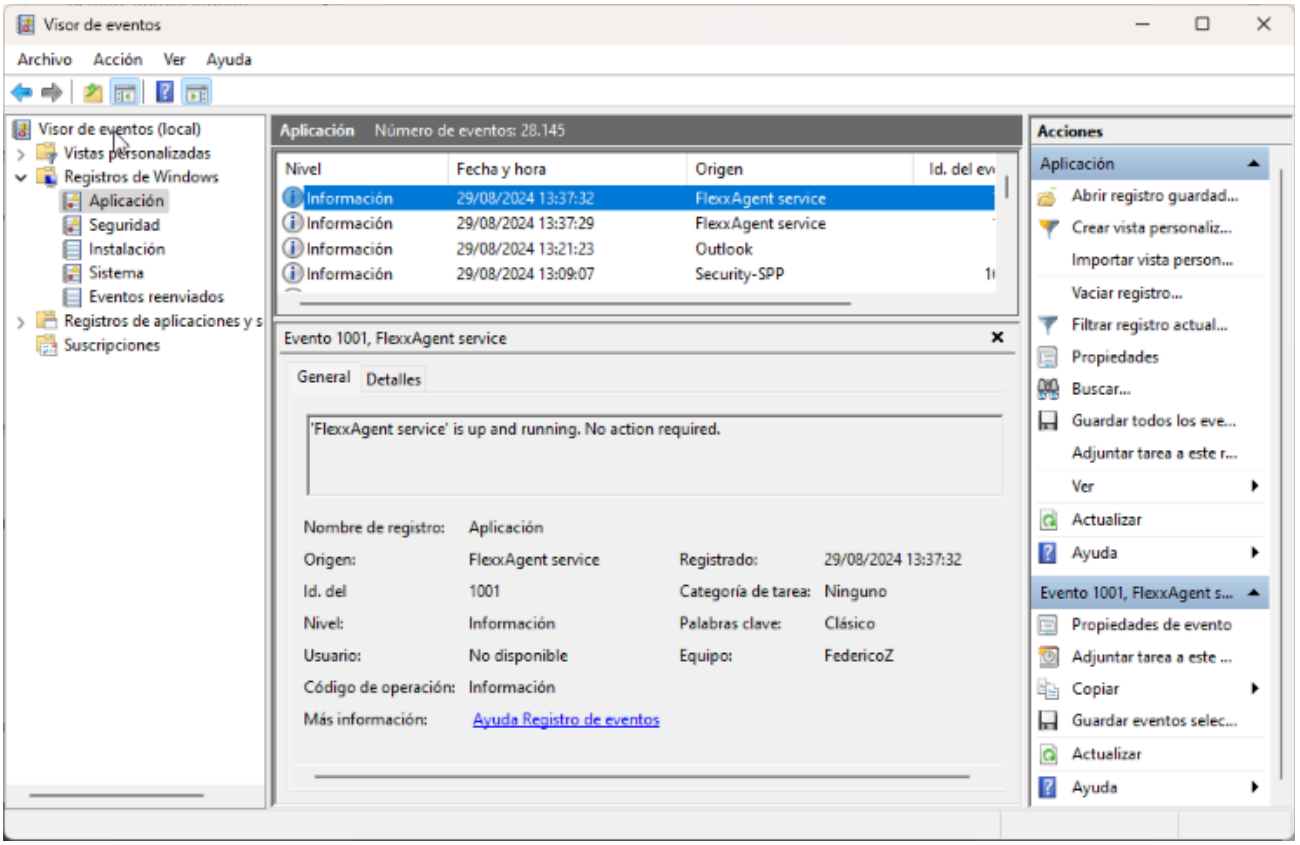
They can be configured to include or not information by criticality levels.

From Workspaces, the log level can be modified for one or several devices using the options available in the `Operations` button.



FlexxAgent service logs

Available in the `Windows Event Viewer`, under the `Application` branch.



FlexxAgent Health Status

The FlexxAgent Health Status process runs periodically (every hour) to evaluate whether FlexxAgent is functioning correctly. For this, it checks its *heartbeat* and analyzes various internal metrics that allow determining whether it is operating adequately or if a recovery process is necessary.

During this evaluation, external factors that might affect the agent's communication, such as:

- The device's connectivity at that time (it may or may not have WiFi or Ethernet connection).
- The interference of a firewall or proxy in the communication.

On the contrary, the following aspects are considered:

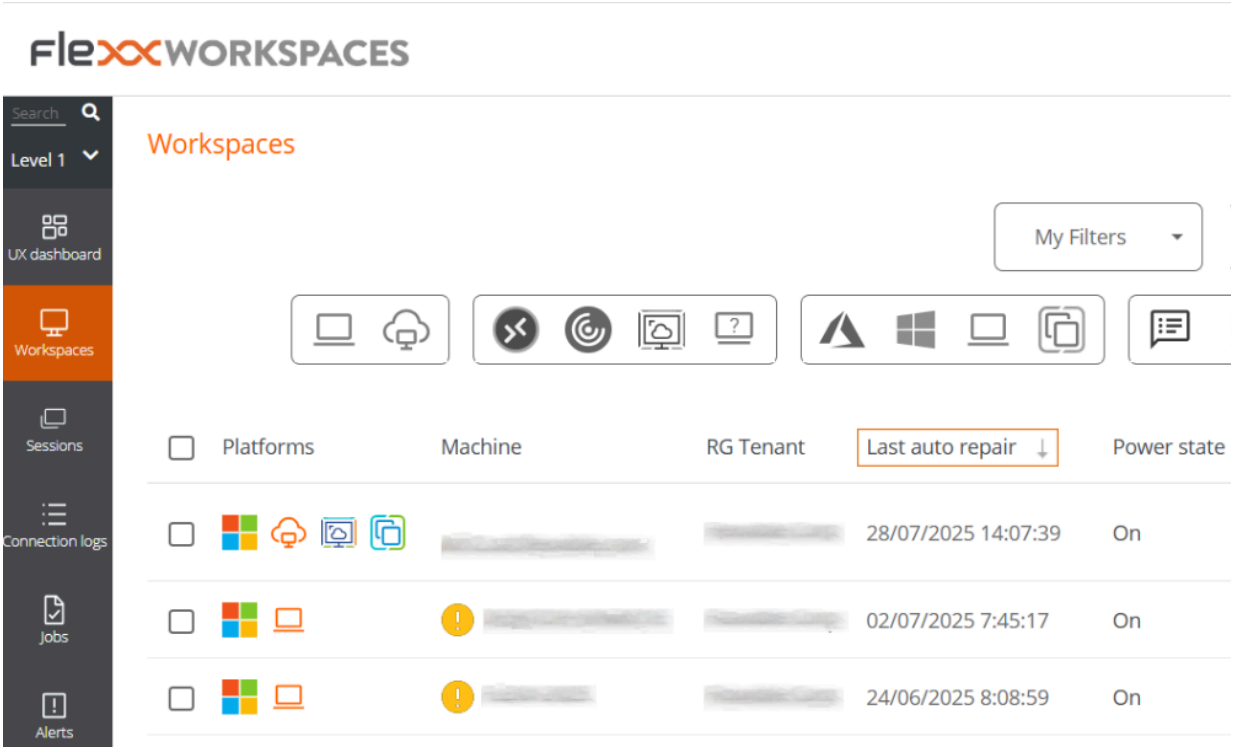
- That the service is running.

- That the service is not disabled; if it is, it is interpreted that an administrator has decided to take this action.

Verification of the FlexxAgent self-repair process

The self-repair of FlexxAgent can be confirmed in the following ways:

1. Through the `Last auto repair` column:
    - Access the `Workspaces` -> `Level 1` -> `Workspaces` module.
    - In the table, check the `Last auto repair` column. If it's not visible, use the Column Selector to add it.



2. FlexxAgent leaves traces in the event log with the following entries:

- **Source**: FlexxAgent Service
- **Log name**: Application

> - Event 1001 Checking FlexxAgent health / `<servicename>` is up and running. No action required

> - Event 1002 Disabled service. No action required / Backup not found. `<serviceName>` not recoverable
> - Event 1003 Service `<serviceName>` restored from previous backup / Error `<message>` found when starting `<serviceName>` with restored backup
> - Event 1004 Service failed to start and will be repaired
> - Event 1005 Service did not report for a long time and will be repaired
> - Event 1006 Service was started
> - Event 1007 Error found when restarting service after not reporting for a long time

Information obtained from the device

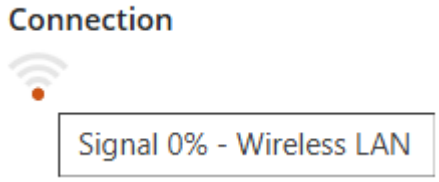
FlexxAgent collects data locally from the device and sends it to the service consoles.

General information

- **Name.** Device Name.
- **Device Status.** Device power state. It can be *On*, *Off*, or *Not reporting*.
- **Summary status.** If the device status is *Off*, it can indicate if it is *Under maintenance* or just *Off*. If the device status is *Unreported*, it can indicate if 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 if the device is connected via *Wireless LAN*, *Mobile Network*, *Ethernet*, or *Unknown*.

INFO

When the connection is made via 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.** Network addressing of the device 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 logged into the device in domain\account format.
- **Connected From.** When the selected device is a VDI or similar, shows the device name from which the virtual device is accessed.
- **Connection Time.** Date and time when the session started.
- **Domain.** Domain to which the device belongs.
- **Code.** Lets identify the device 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 of the domain where the device 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 available RAM.
- **Cores.** Number of processor cores.
- **IP Address.** Device's IP address on the local network.
- **OS.** Type of operating system.
- **Operating System.** OS version.
- **OS Build.** Operating system build number.
- **Uptime.** Time the device has been running since the last boot or reboot. If fastboot is enabled, the device is only off when it is restarted.
- **Idle time.** Indicates the time elapsed since the last input event was received in the FlexxAgent user session. Shows 0 if the user is effectively using any input device connected to the device.
- **Last Windows update.** Date of the last updates applied on the device.
- **Last boot duration.** Duration of the boot of the last start.
- **Pending reboot.** Shows whether the device requires a reboot for updates.
- **Type of Windows.** Type of Windows operating system: *Client* or *Server*.
- **System disk.** Amount of free disk space relative to the total capacity.
- **ISP Public IP.** 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 session broker used.
- **Hypervisor.** If virtualization is detected, shows the hypervisor used.
- **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 status of the virtual device registration.
- **Maintenance mode.** Indicates if 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's configured to launch session Analyzer in all user sessions.
- **Session Analyzer Version.** Version number of Session Analyzer.

- **Report Group.** Reporting group to which the device belongs.
- **BIOS manufacturer.** Name of the device's firmware manufacturer.
- **BIOS version.** Version of the device's firmware.
- **SMBIOS version.** Version of the System Management BIOS 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.** Build number of Google Chrome, if installed.
- **Microsoft Edge version.** Build number of Microsoft Edge, if installed.

Information in tabs

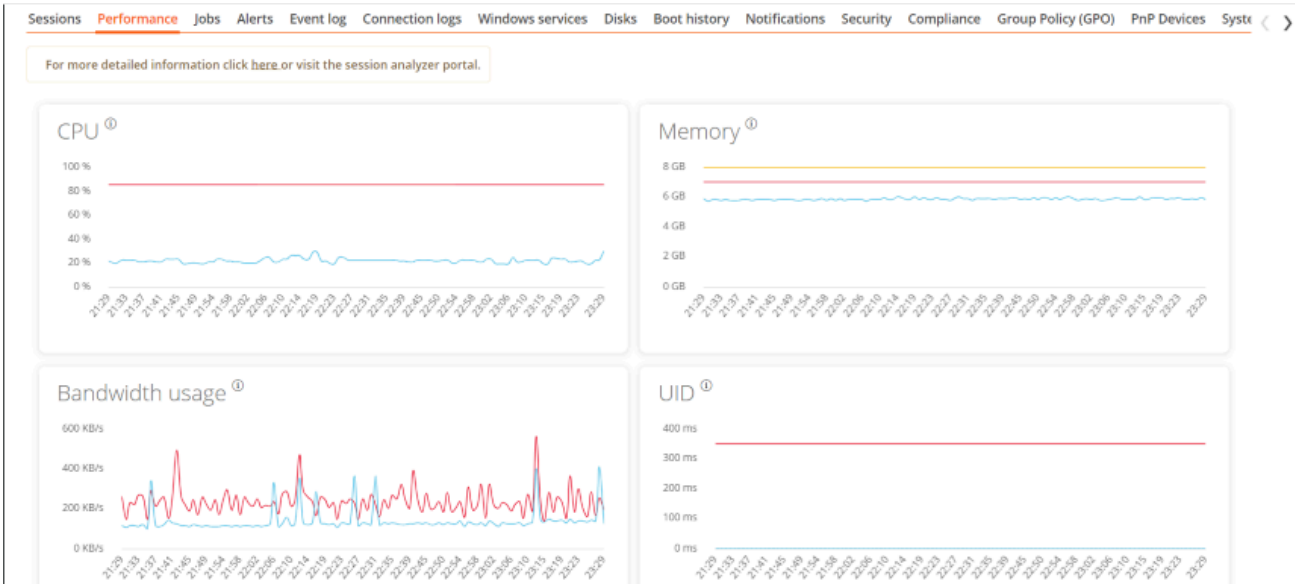
FlexxAgent groups information about the following aspects of the device:

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 graphs of the device's main performance counters, based on data collected over the last two hours. The following are included:



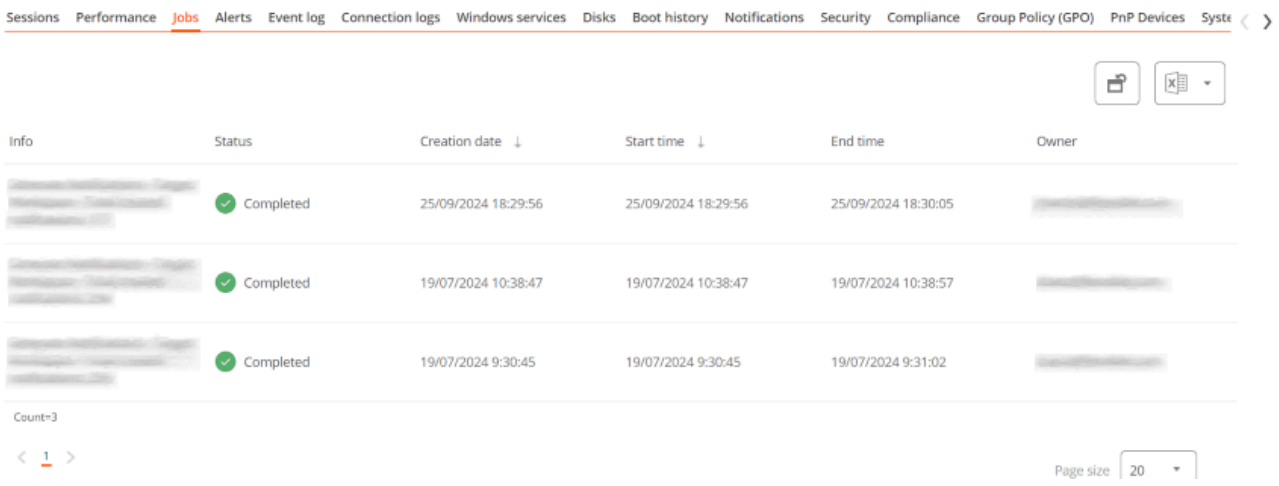
- **CPU.** Percentage of processor usage

- **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.** Percentage of signal reception when the device connects using a wireless method.

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

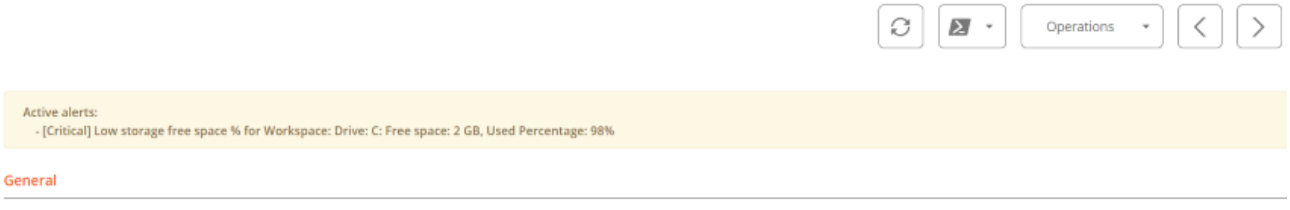
Jobs

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.



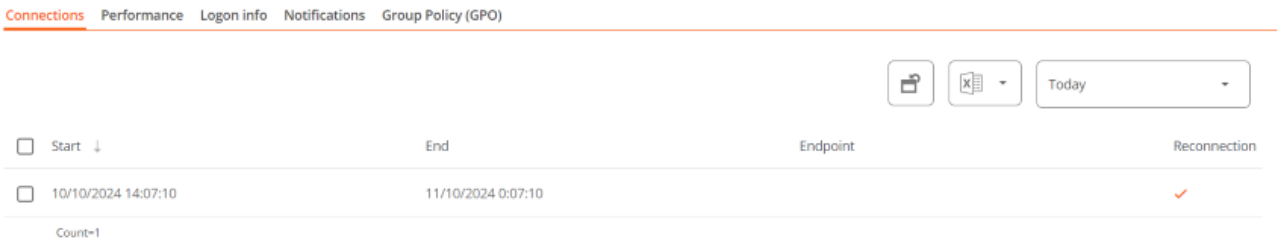
Event Logs

Information about the 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.

The available settings allow you to modify the sampling time or include events by their ID.

Connection Log

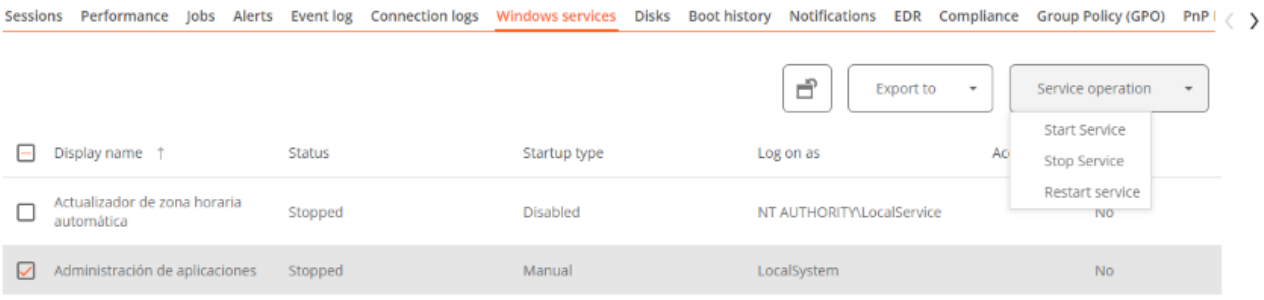
Presents a list of the connections established with the device, including each instance where a user logs in or reconnects a previously disconnected session.



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.

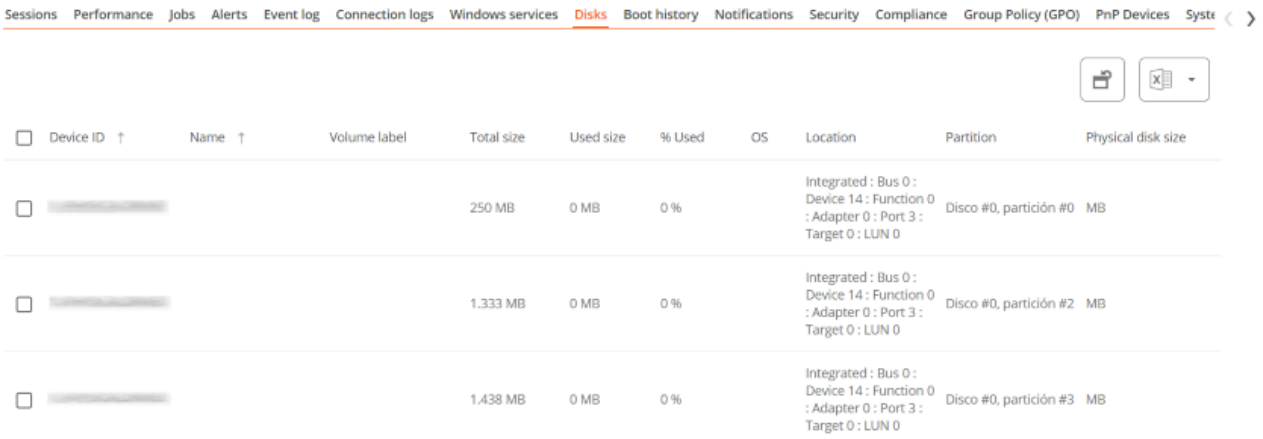
Windows services

This option displays the status of services and performs start, restart, or stop operations on Windows services.



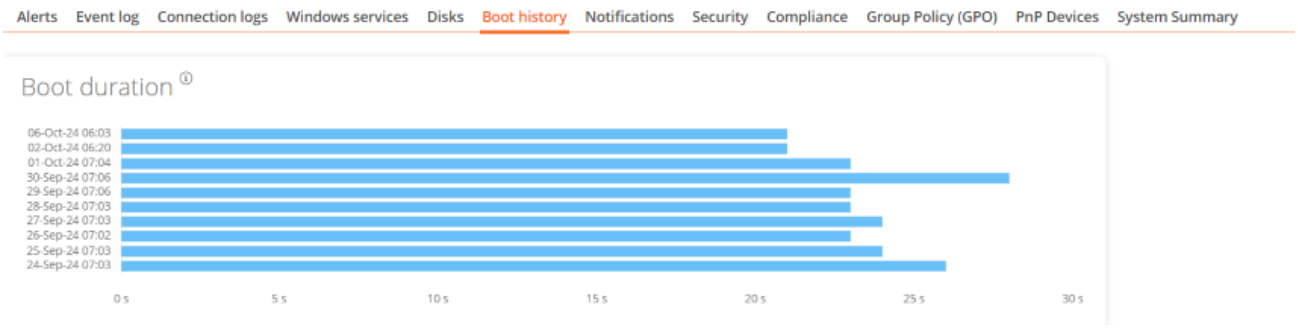
Disks

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



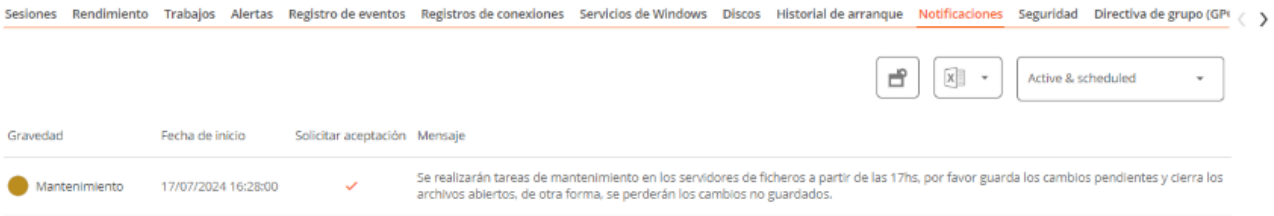
Boot history

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



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

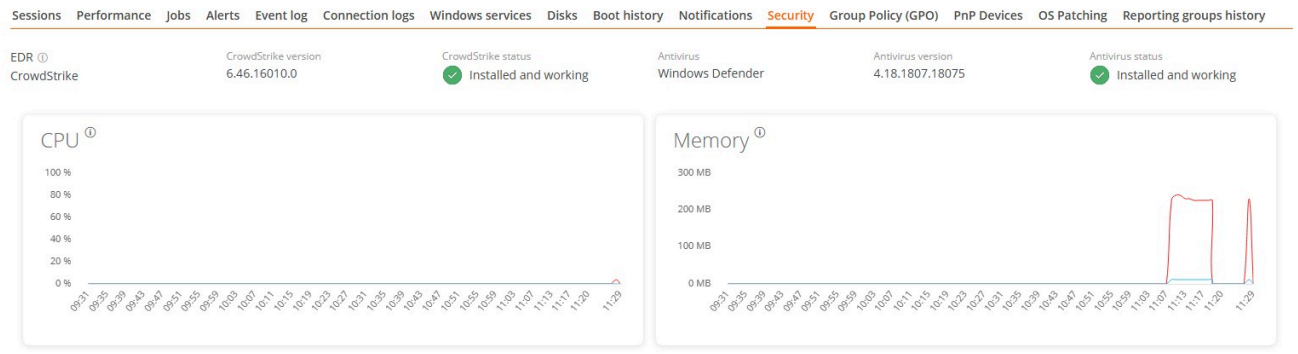
From this section, you can view information about the installed antivirus, as well as graphs on RAM and CPU usage.

- **Antivirus.** Name of the antivirus solution installed or integrated into the system. If more than one is detected, *Multiple* is indicated.
- **Antivirus version.** Installed version number.
- **Antivirus status.** Operational state of the solution.

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

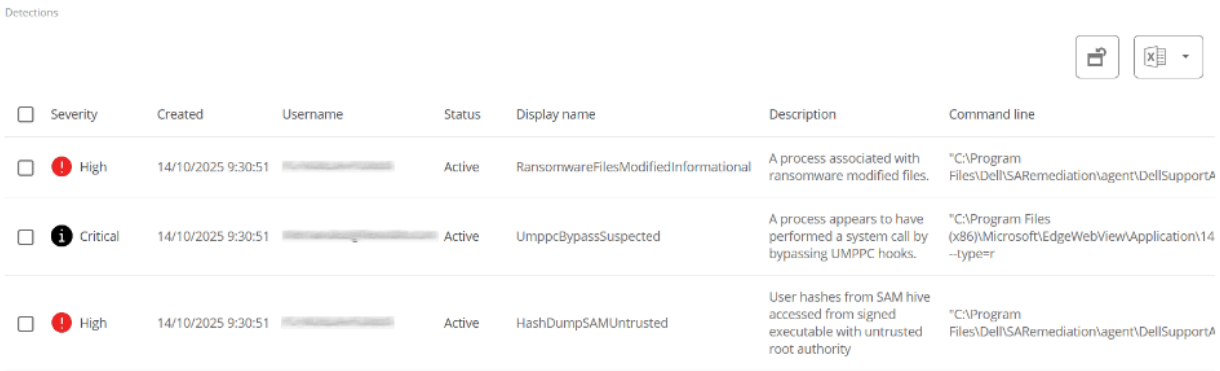
If FlexxAgent detects CrowdStrike as an Endpoint Detection and Response (EDR) solution, the same information fields will be displayed:

- **Endpoint Detection and Response (EDR).** Name of the endpoint security solution; in this case, CrowdStrike.
- **CrowdStrike version.** Installed version number.
- **CrowdStrike status.** Operational status of the solution.



> **INFO**
>
> FlexxAgent synchronizes CrowdStrike alerts every minute.

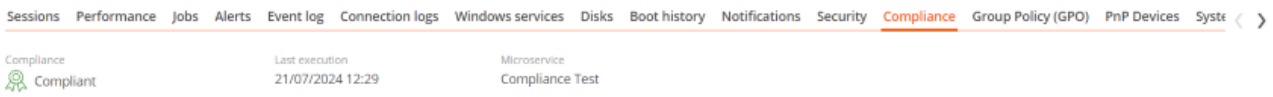
Additionally, if CrowdStrike integration has been carried out via Portal, a table will be displayed with information about the detections, including the following fields:



- **Severity.** Criticality level assigned to the detection according to the potential impact or risk of the threat.
- **Created.** Date and time the detection was generated in the system.
- **Username.** User associated with the activity or process that triggered the detection.
- **Status.** Current status of the detection.
- **Display Name.** Descriptive name assigned to the detection, summarizing the type of threat or behavior identified.
- **Description.** Expanded information about the detection.
- **Command line.** Command or instruction executed on the appliance related to or that generated the detection.

Compliance

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

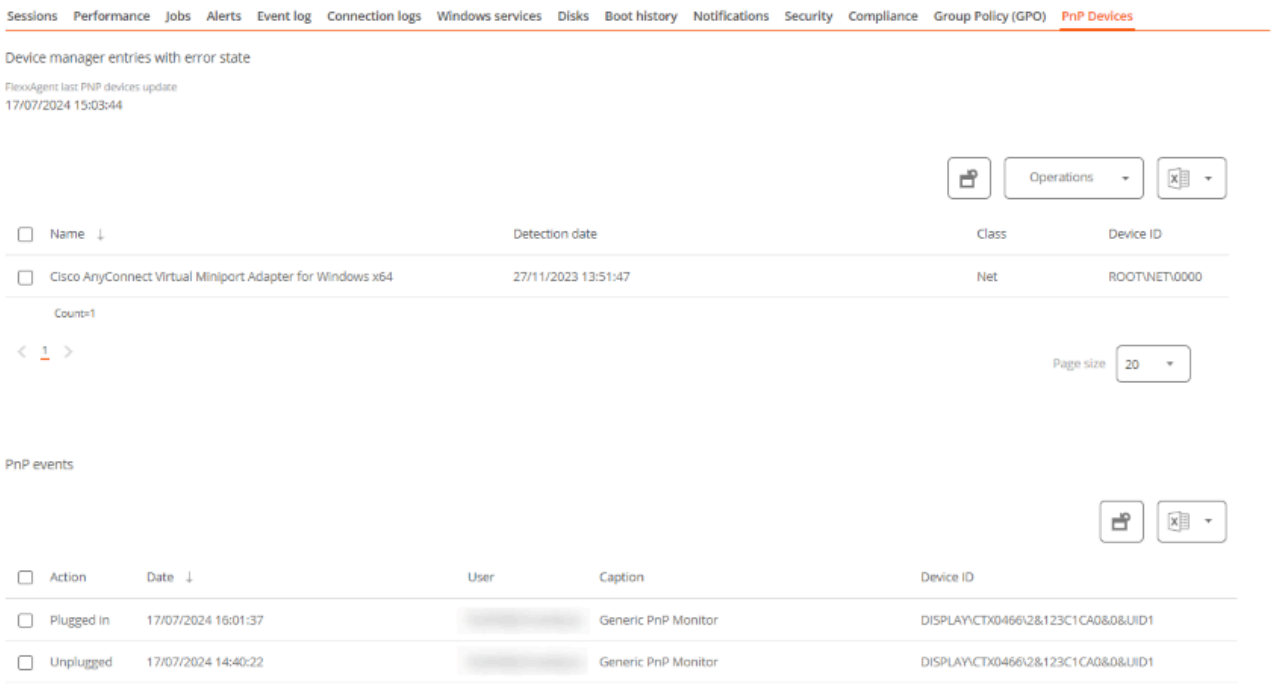


Group Policy (GPO)

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

PnP Devices

Displays 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, a table shows all events related to PnP devices, creating an entry each time a peripheral is connected or disconnected.

System Summary

Displays 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"

Field	Detail
SystemModel	Product name given by a manufacturer to a piece of equipment
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

Field	Detail
BootDevice	Name of the disk drive from which the Windows operating system starts
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)

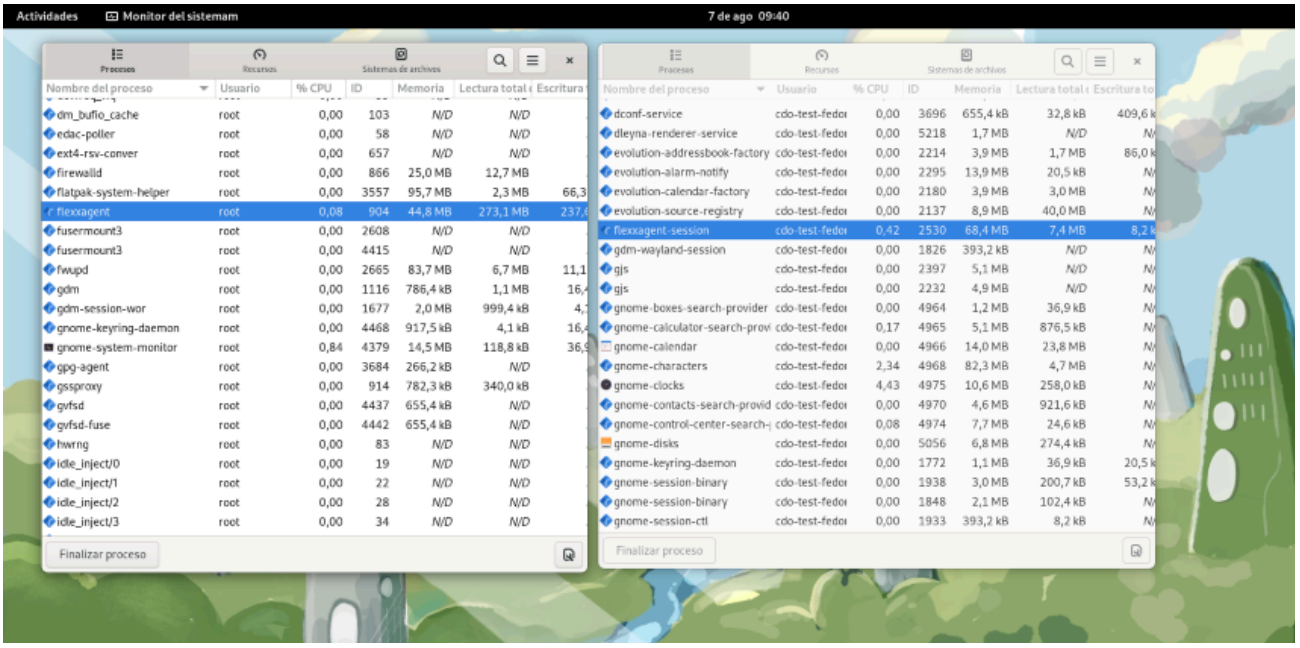
Reporting groups history

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

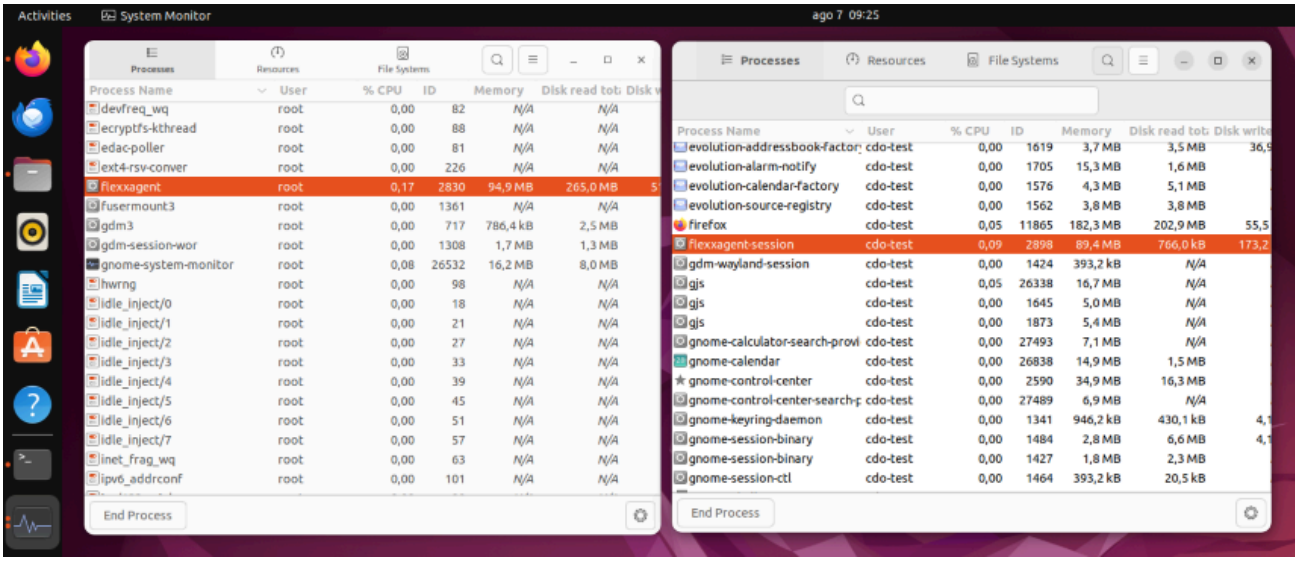
The Linux agent allows the inclusion of devices with this operating system in the service consoles, enabling support teams to have complete visibility of all devices in use within the organization.

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 features are not available for Linux, such as Flexxible Remote Assistance, user microservices, or the execution of flows, as well as the collection of plug and play peripheral data.

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 should be downloaded from the Reporting Groups section in the Workspaces module.

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`

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.

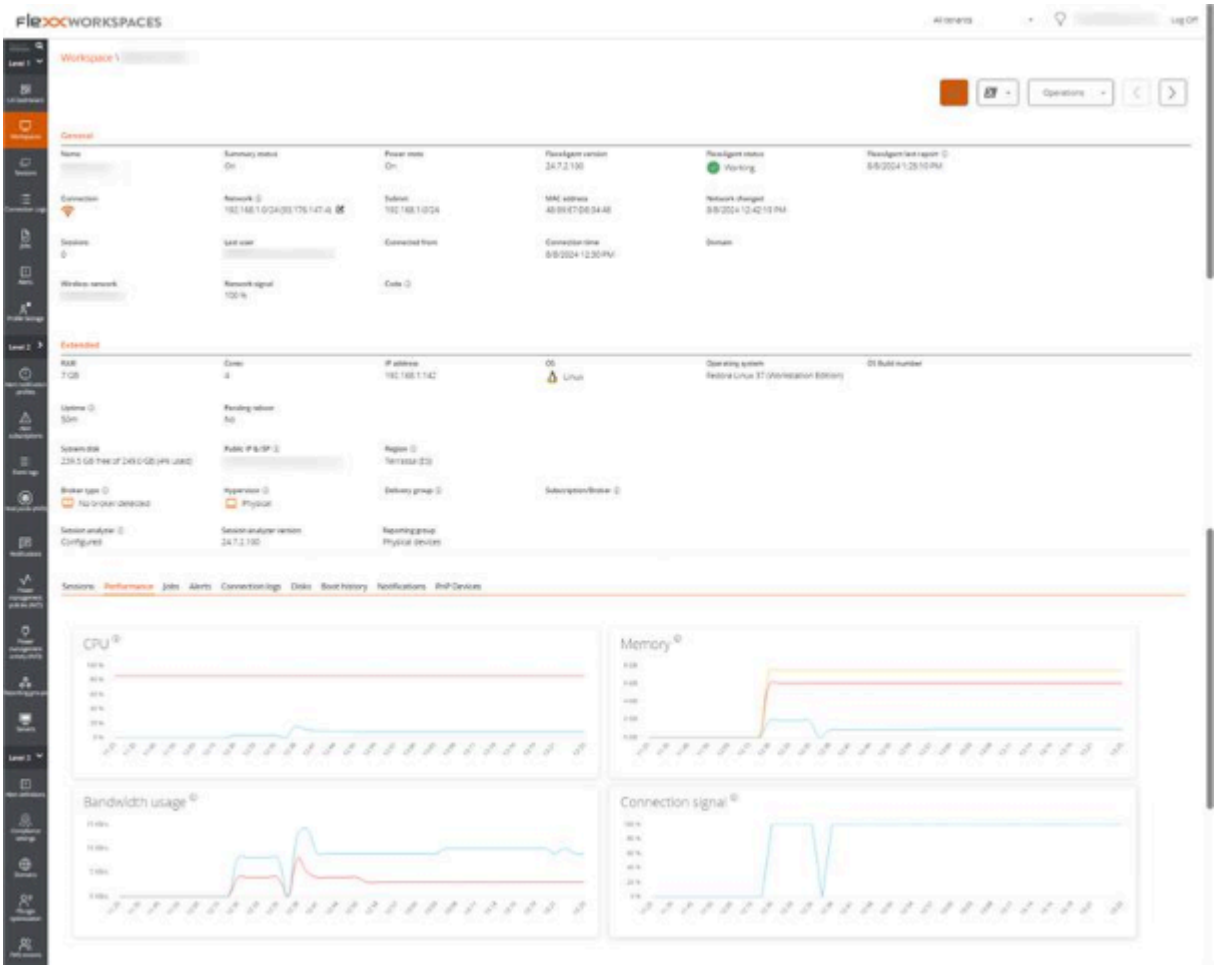
Logs

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.** Power status of the device, 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 if the device is connected via *Wireless LAN*, *Mobile Network*, *Ethernet*, or *Unknown*.
- **Network.** Network addressing of the device and public IP for internet access. These networks are created automatically when more than four devices are connected to the same network.
- **Network Signal.** Network reception percentage.

- **Subnet.** Device's network addressing.
- **MAC Address.** Unique identifier of the device's network card.
- **Wireless Network.** Name of the network.
- **Connection signal.** Percentage of signal reception when the device connects using 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 logged into the device in domain\account format.
- **Connected From.** When the selected device is a VDI or similar, shows the device name from which the virtual device is accessed.
- **Connection Time.** Date and time when the session started.
- **Code.** Lets identify the device 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 capacity of available RAM.
- **Cores.** Number of processor cores.
- **IP Address.** Device's IP address on the local network.
- **OS.** Type of operating system.
- **Operating System.** OS 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 session broker used.
- **Delivery group.** For VDIs, shows the delivery group to which the device belongs.
- **Subscription.** If detected, subscription in use for Citrix Cloud, Azure services, etc.
- **Hypervisor.** If virtualization is detected, shows the hypervisor used.
- **Session Analyzer.** Indicates whether or not it's configured to launch session Analyzer in all user sessions.

- **Session Analyzer Version.** Version number of Session Analyzer.
- **Report Group.** Reporting 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 graphs of the device's main performance counters, based on data collected over 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.

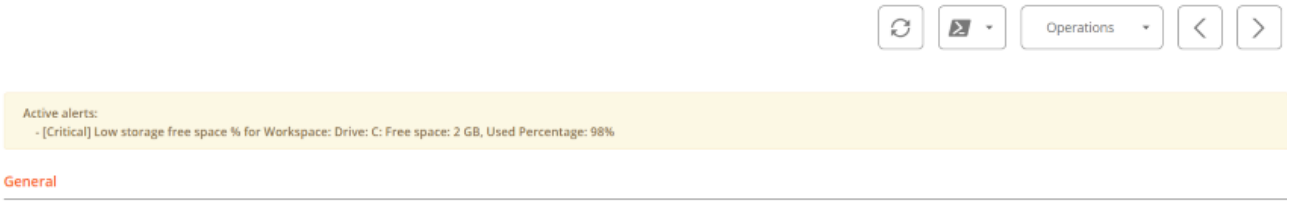
At the top, a link grants access to the Analyzer module.

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

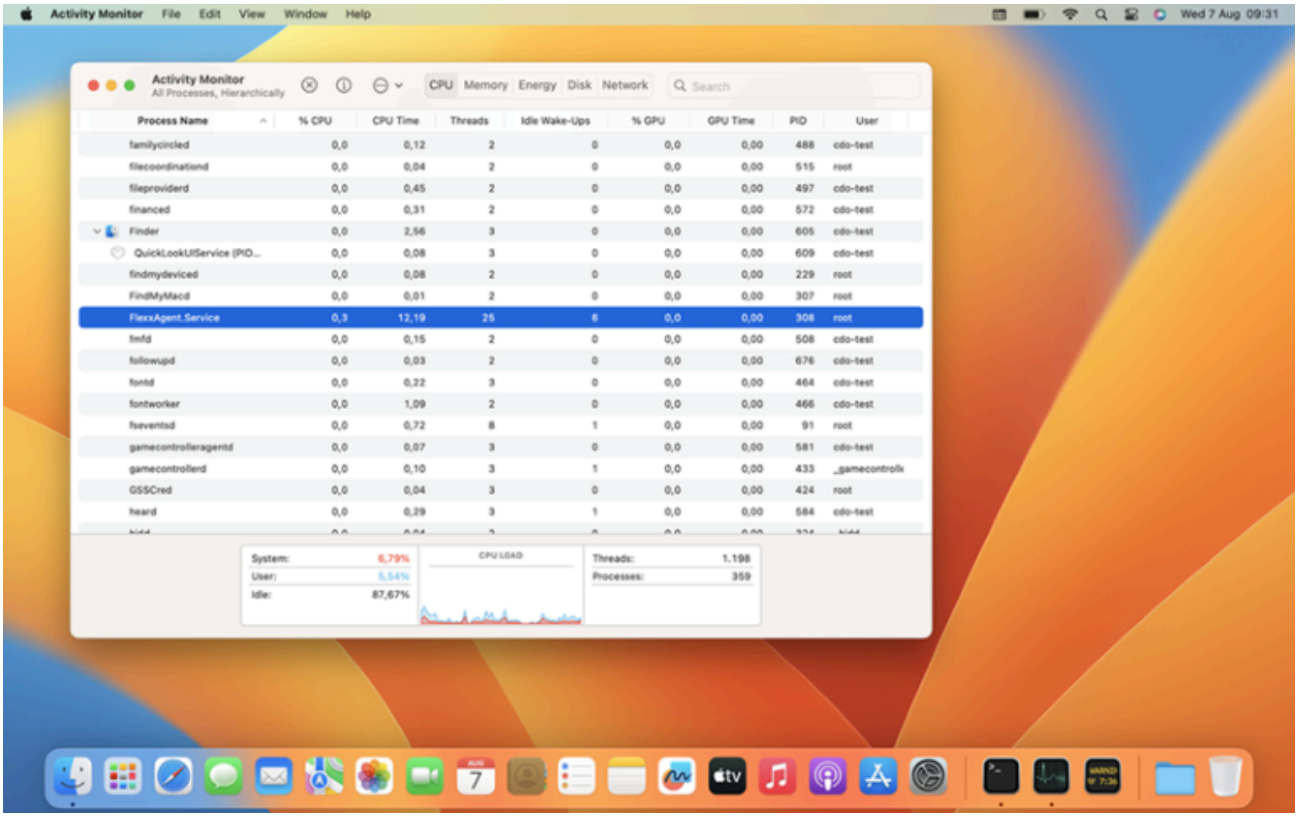
Allows you to see if the device has any active notification. When there is one, a message is displayed at the top of the page.

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 functionalities are not available for macOS, such as Flexxible Remote Assistance, running microservices on demand from Workspaces or user microservices and flows, as well as sending 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 should be downloaded from the Reporting Groups section in the Workspaces module.

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.

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
```

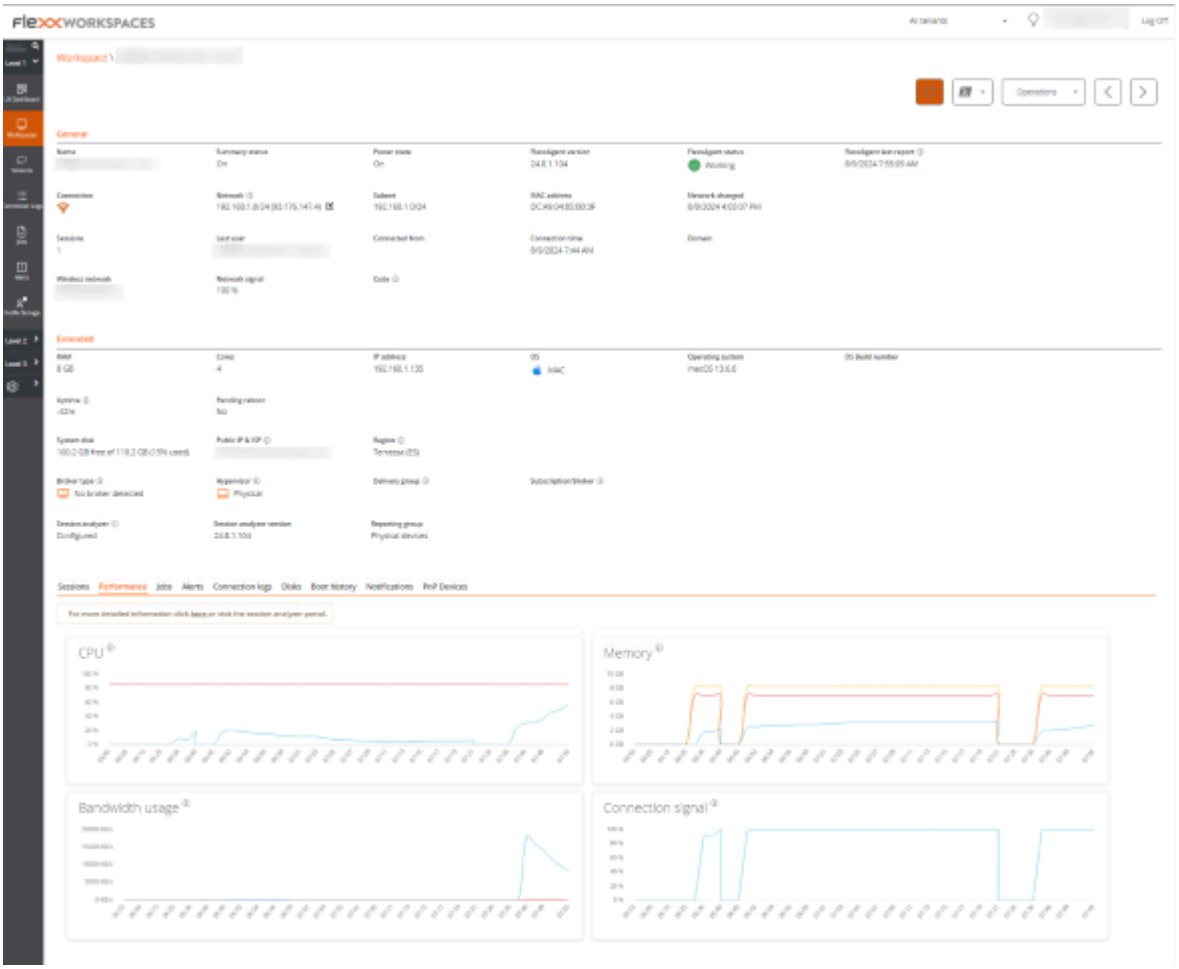
Update

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.** Power status of the device, 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 if the device is connected via *Wireless LAN*, *Mobile Network*, *Ethernet*, or *Unknown*.
- **Network.** Network addressing of the device and public IP for internet access. These networks are created automatically when more than four workspaces are connected to the same network.
- **Network Signal.** Network reception percentage.
- **Subnet.** Device's network addressing.
- **MAC Address.** Unique identifier of the device's network card.
- **Wireless Network.** Name of the network.
- **Connection signal.** Percentage of signal reception when the device connects using 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 logged into the device in domain\account format.
- **Connected From.** When the selected device is a VDI or similar, shows the device name from which the virtual device is accessed.
- **Connection Time.** Date and time when the session started.
- **Code.** Lets identify the device 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 capacity of available RAM.
- **Cores.** Number of processor cores.
- **IP Address.** Device's IP address on the local network.
- **OS.** Type of operating system.
- **Operating System.** OS 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's configured to launch session Analyzer in all user sessions.
- **Session Analyzer Version.** Version number of Session Analyzer.
- **Report Group.** Reporting 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 graphs of the device's main performance counters, based on data collected over 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 grants 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, Flexxible Remote Assistance, workflows, 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:

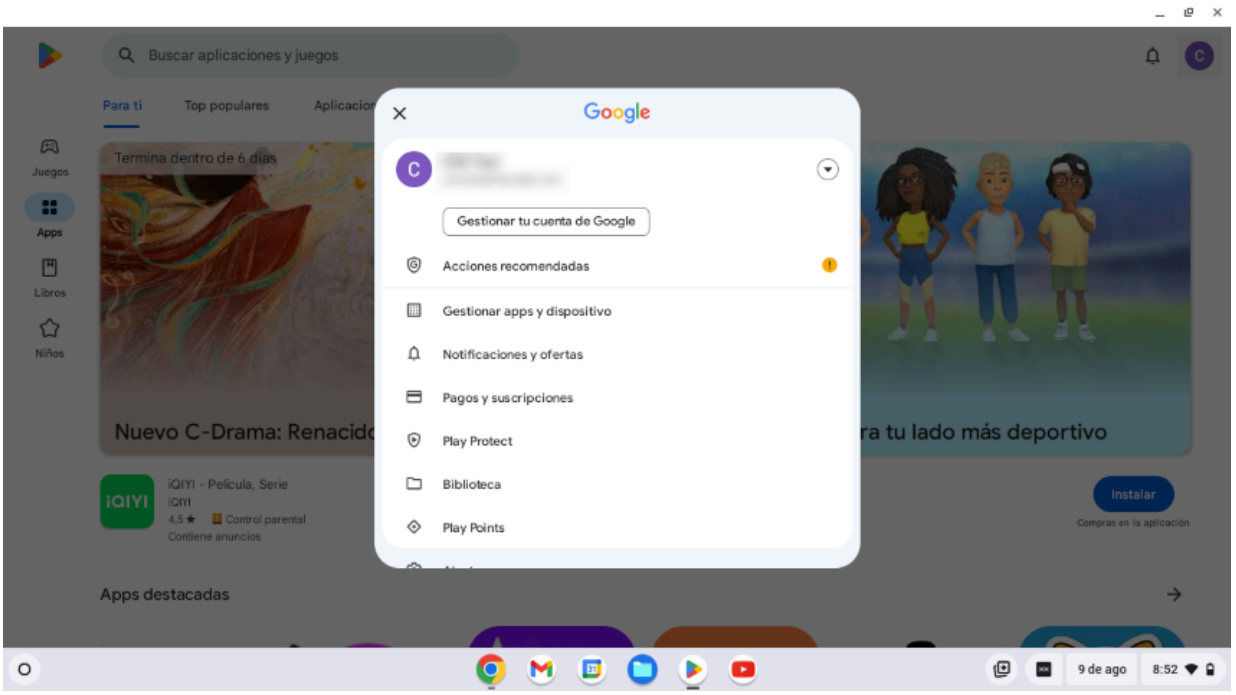
1. Go to `Devices` -> `Chrome` -> `Apps and extensions` -> `Users & browsers` and select the organizational unit (OU) in which you want to deploy the app.
2. Add the app from Google Play (search for FlexxAgent), assign the managed configuration (JSON), and mark it as `Force install`.

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

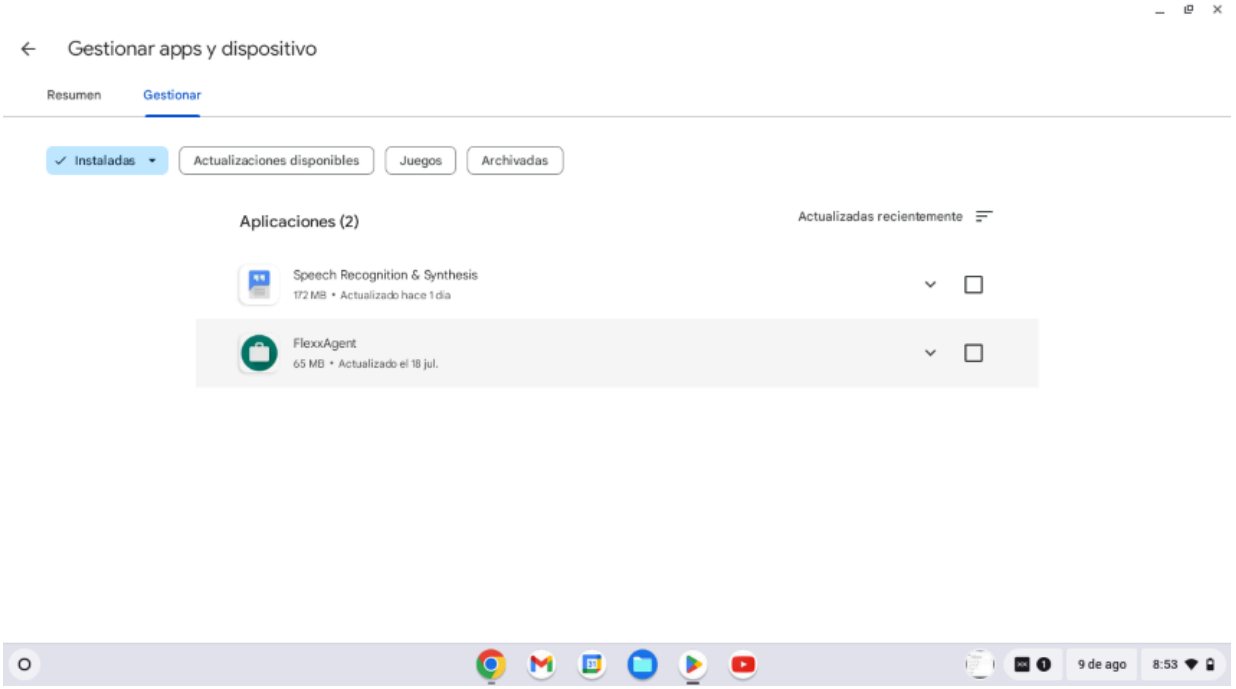
> Please review the linked links for more information on registering apps or deploying them to managed users in Google Admin.

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:

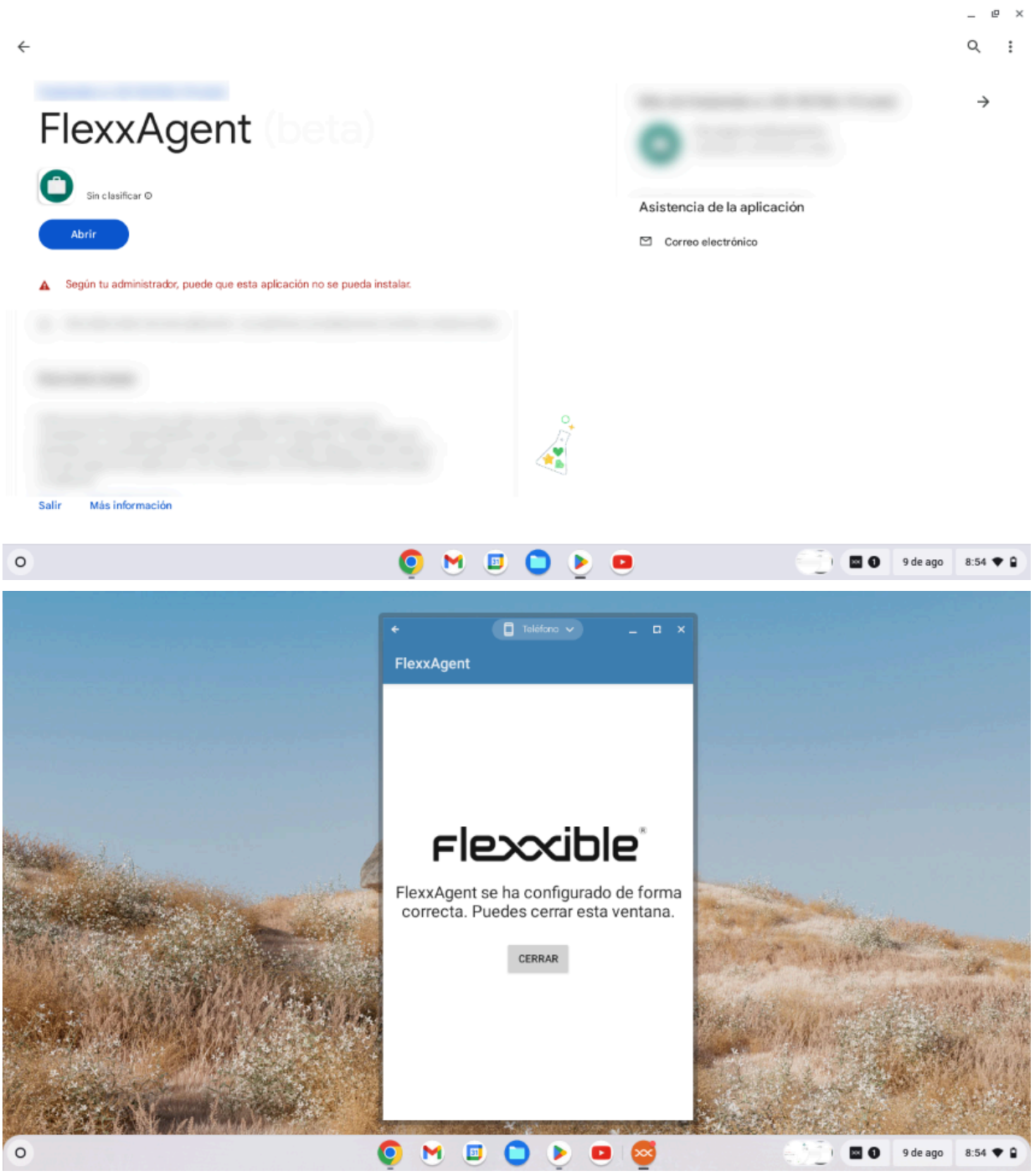
1. Access Google Play and go to `Manage apps and device`.



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

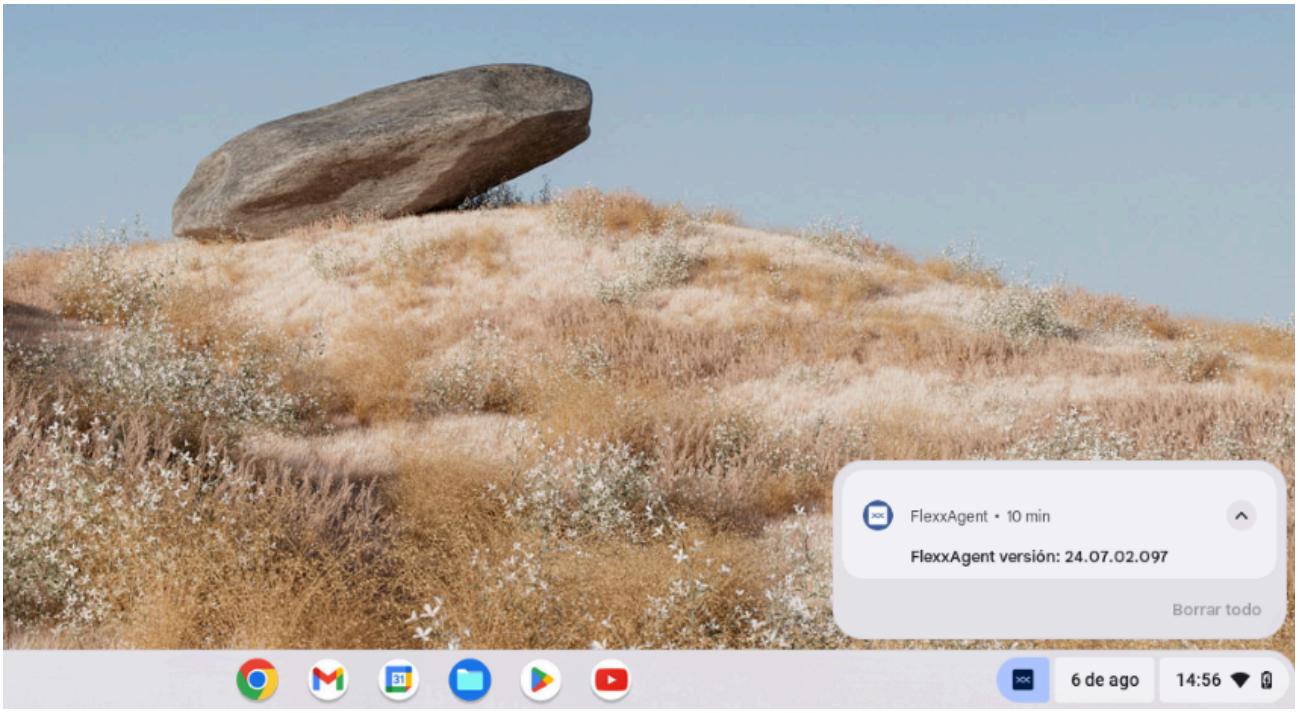


3. On the application's detail screen, click `Open`. A window will appear next, confirming that the application has been correctly configured.



4. Close the window.

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

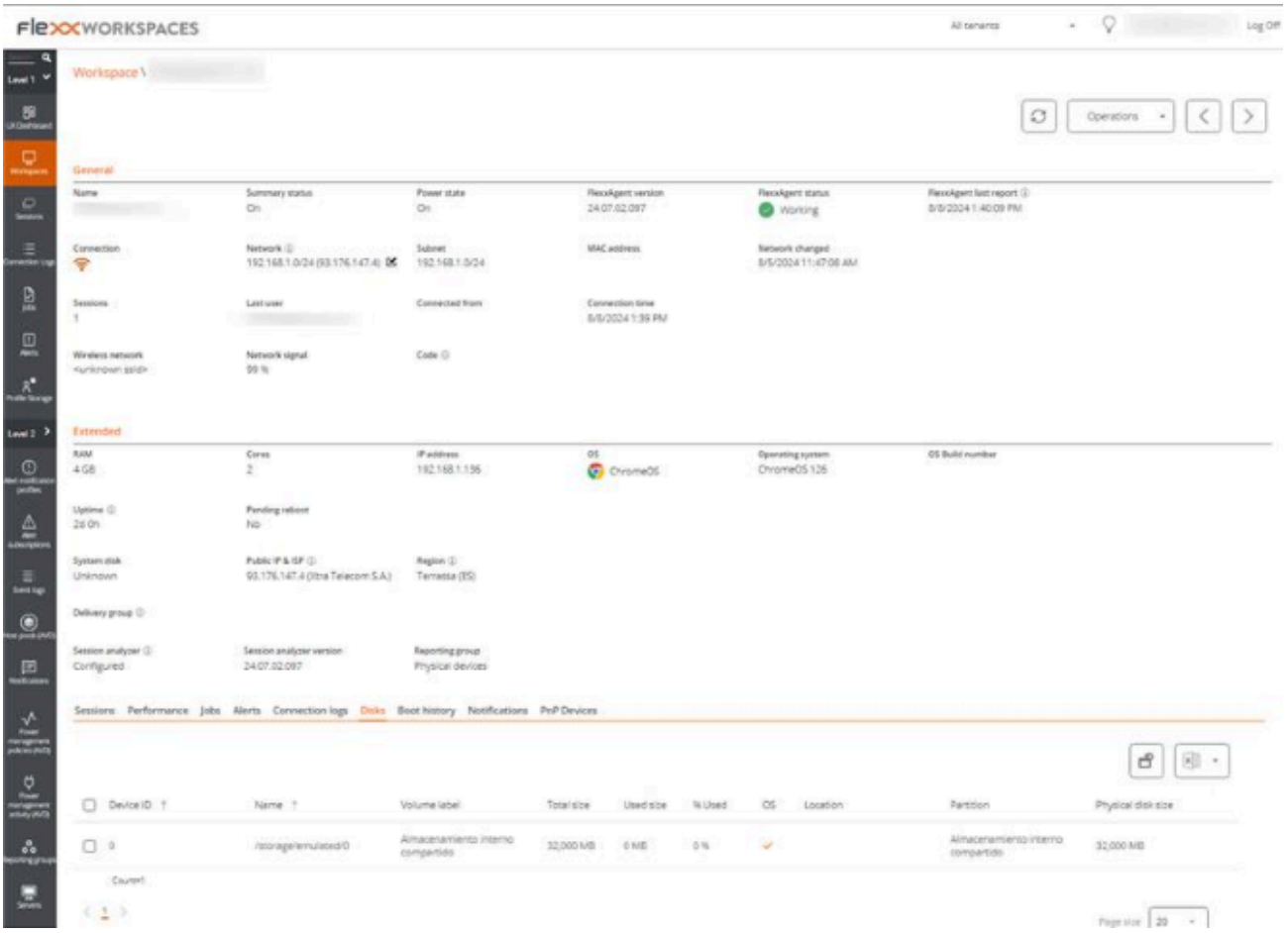


Update

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.** Power status of the device 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 if the device is connected via *Wireless LAN*, *Mobile Network*, *Ethernet*, or *Unknown*.
- **Network.** Network addressing of the device and public IP for internet access. These networks are created automatically when more than four devices are connected to the same network.
- **Network Signal.** Network 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 logged into the device in domain\account format.
- **Connected From.** When the selected device is a VDI or similar, shows the device name from which the virtual device is accessed.
- **Connection Time.** Date and time when the session started.
- **Code.** Lets identify the device 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 capacity of available RAM.
- **Cores.** Number of processor cores.
- **IP Address.** Device's IP address on the local network.
- **OS.** Type of operating system.
- **Operating System.** OS version.
- **Uptime.** Time the device has been running since the last boot or reboot. 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's configured to launch session Analyzer in all user sessions.
- **Session Analyzer Version.** Version number of Session Analyzer.
- **Report Group.** Reporting 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, Flexxible Remote Assistance, workflows, 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

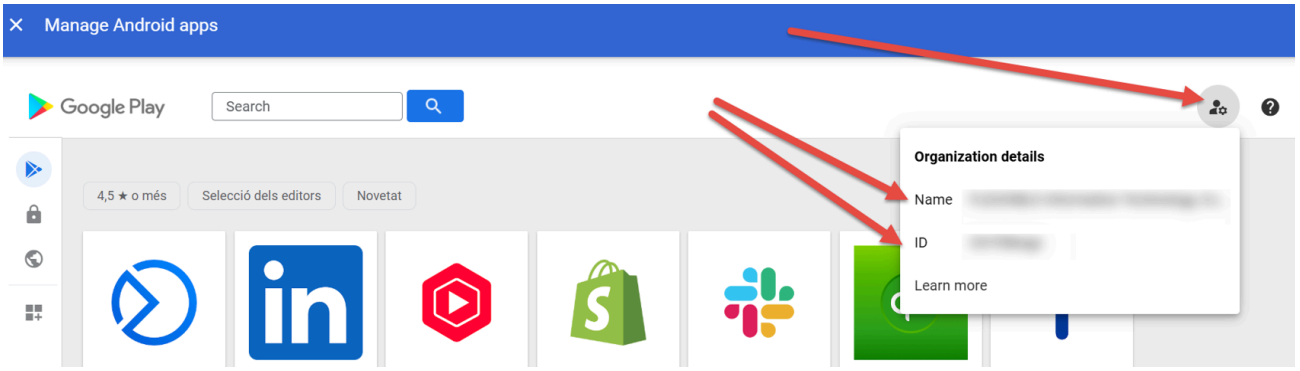
FlexxAgent configuration is managed through Managed Configurations to ensure correct operation.

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.

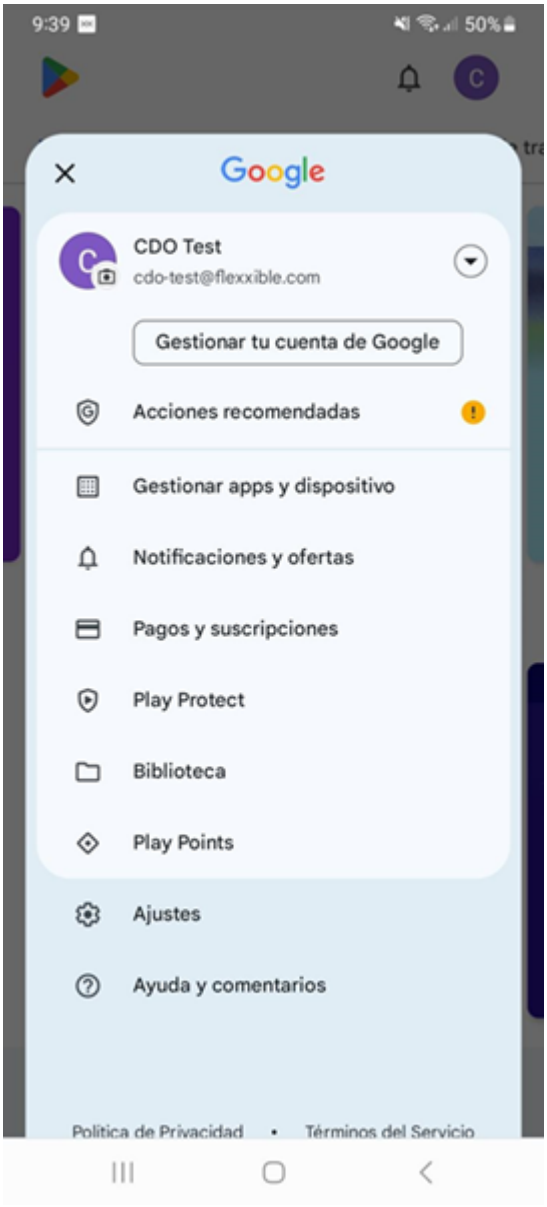


Download and installation

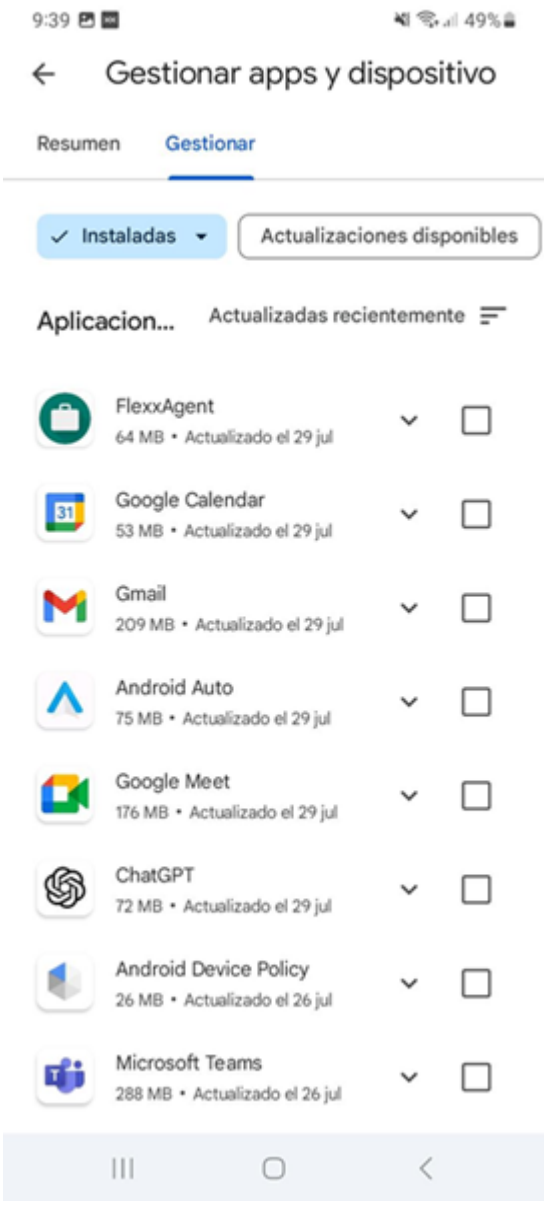
FlexxAgent is available as a private Android app on Google Play.

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:

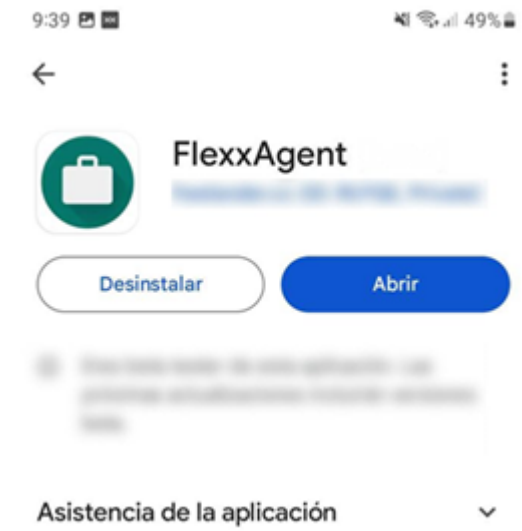
1. Go to Google Play and navigate to `Manage apps and devices`.



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



3. On the app detail screen, click `Open`. A window will appear next, confirming that the application has been correctly configured.

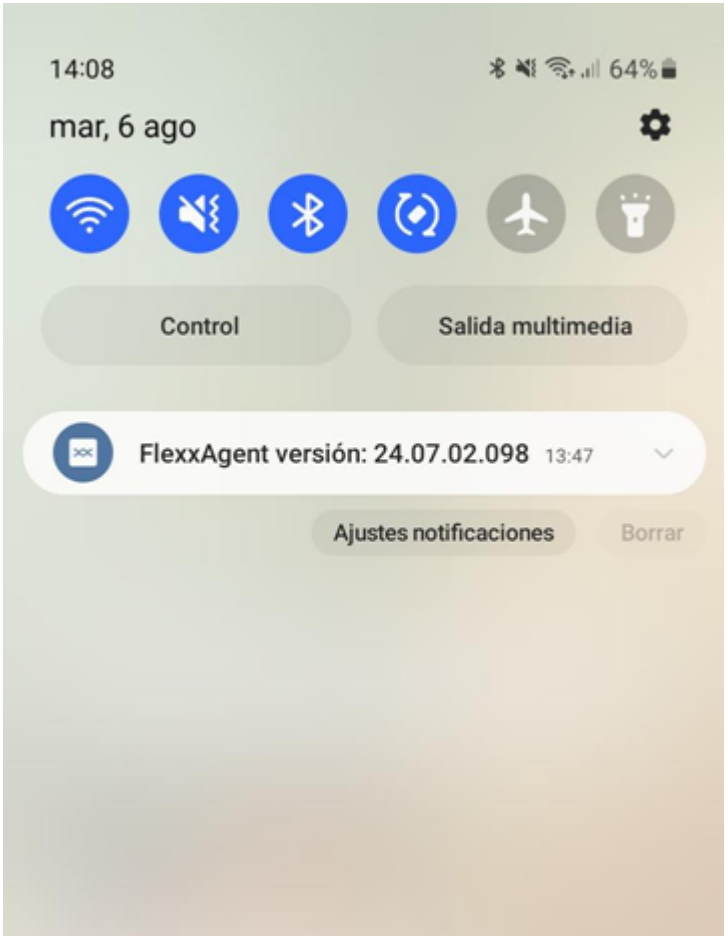


INFO

FlexxAgent requires some special permissions, such as access to the device's 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.

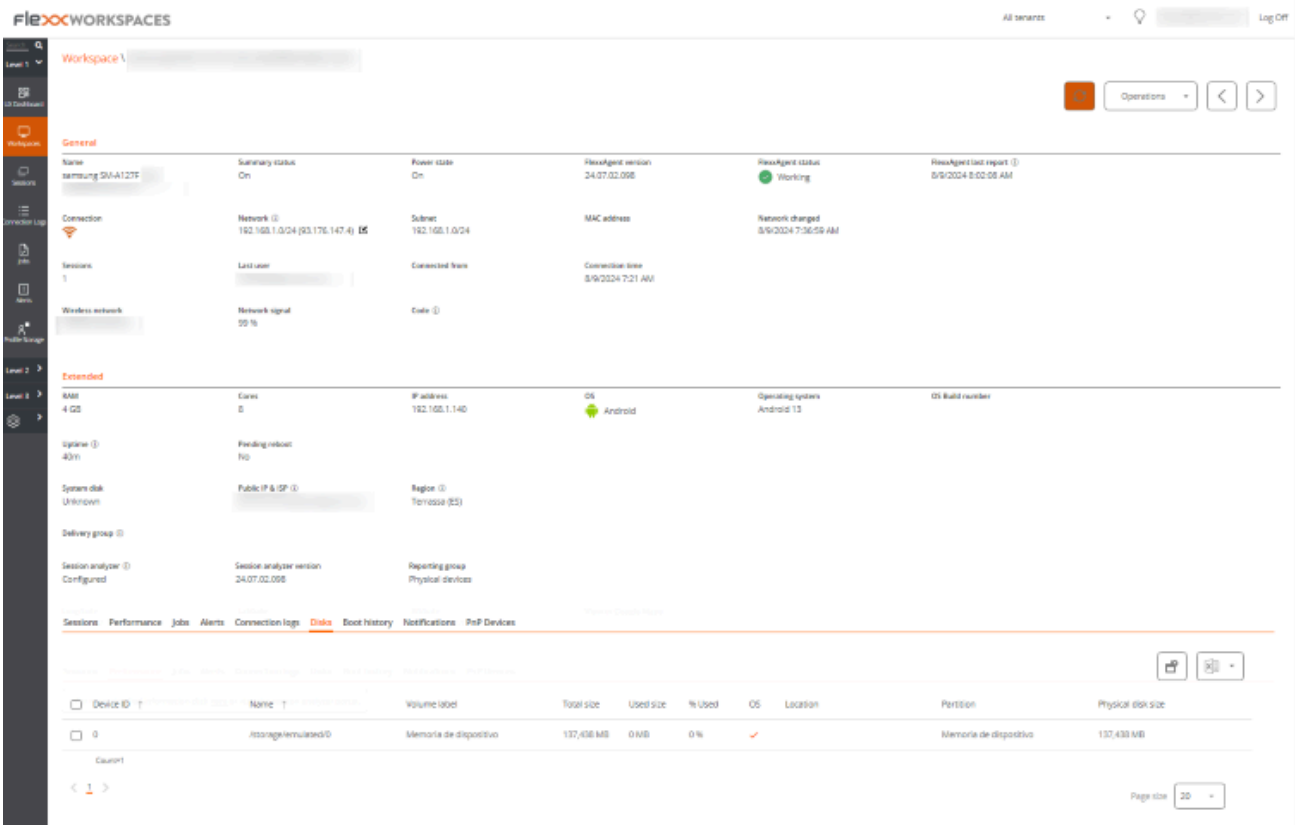


Update

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.** Device 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 if the device is connected via *Wireless LAN*, *Mobile Network*, *Ethernet*, or *Unknown*.
- **Network.** Network addressing of the device and public IP for internet access. These networks are created automatically when more than four devices are connected to the same network.
- **Network Signal.** Network 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 logged into the device in domain\account format.
- **Connected From.** When the selected device is a VDI or similar, shows the device name from which the virtual device is accessed.
- **Connection Time.** Date and time when the session started.
- **Code.** Lets identify the device 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 available RAM.
- **Cores.** Number of processor cores.
- **IP Address.** Device's IP address on the local network.
- **OS.** Type of operating system.
- **Operating System.** OS version.
- **Uptime.** Time the device has been running since the last boot or reboot. 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's configured to launch session Analyzer in all user sessions.
- **Session Analyzer Version.** Version number of Session Analyzer.
- **Report Group.** Reporting 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

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 devices, it is recommended to validate that these can access the defined destinations in URL addresses 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 URL addresses 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
https://west-eu.agent-api.analyzer.flexxible.com	Agent	443	West Europe
https://flexxibleglobal.blob.core.windows.net	Agent	443	West Europe
https://api.ipify.org	Agent	443	West Europe
https://ras.flexxible.com	Agent – Flexxible Remote Assistance	443	West Europe
https://update.workspaces.flexxible.com	Agent	443	West Europe
https://agents-weu.one.flexxible.net	Agent	443	West Europe
https://west-eu-01.agent-api.one.analyzer.flexxible.com	Agent	443	West Europe
https://south-br.agent-api.analyzer.flexxible.com (Brazil Only)	Agent	443	Brazil South
https://flxsbname***.servicebus.windows.net	Agent	443	West Europe
https://flxiothub***.azure-devices.net	Agent	443	West Europe

NOTE

In the last two URLs, the three asterisks (***) represent a dynamic and unique identifier with a length of 9 to 15 alphanumeric characters, provided by Flexxible.

Depending on the capabilities of the security device, URL exceptions can be configured using regular expressions (RegEx) or wildcards.

Examples of exceptions using regular expressions (Regex)

```
^https://flxsbname[a-zA-Z0-9]{9,15}.servicebus.windows.net$
```

```
^https://flxiothub[a-zA-Z0-9]{15,24}.azure-devices.net$
```

Examples of exceptions using wildcards

```
https://flxsbname*
```

```
https://flxiothub*
```

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

You should try to disable Deep SSL Inspection for the following URLs on devices that have it as a security solution to ensure optimal functioning of FlexxAgent.

- 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. During the process, 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.*

To resolve it, Flexxible recommends excluding the following items:

> `C:\Windows\Temp\FlexxibleIT`

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

Wake on LAN (WoL)

Wake on LAN (WoL) 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 —with FlexxAgent installed and reporting— on the same network as the device to be powered on.

WoL typically operates within a local network. It can work between subnets as long as there are no restrictions imposed by firewalls or network devices blocking the transmission of the magic packet. In environments with subnet segmentation, it's necessary to configure network-level exceptions that allow the magic packet to be routed between those 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.

Flexxible Remote Assistance through a proxy

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

If configured with a proxy but it is not accessible at that moment, Flexxible Remote Assistance will run with the "auto detect" option, using the outgoing internet settings configured by the end user.

vPro

If an organization wants to activate vPro, it will require the Flexxible Intel EMA server's hostname to be resolvable from all their devices.

URL	Ambit	Port	Region
https://iagent.flexxible.com	Agent	443	West Europe

Requirements for vPro operation via a proxy

- The dynamic host configuration protocol (DHCP) must provide a DNS suffix (DHCP option 15) matching the domain of the certificate.
- The proxy must allow the HTTP CONNECT method to the used ports.
- Exclude the Flexxible URL to avoid deep SSL/TLS inspection in Client Initiated Remote Access (CIRA) connections.
- The proxy must not modify the HTTP headers during the CONNECT phase.

> **TIP**
>
> For more information about vPro, please refer to the Integrations section.

FlexxAgent / Wake on LAN (WoL)

WoL is a network standard that allows devices to be powered on remotely via Ethernet, as long as the hardware and system configuration support it.

In Portal and Workspaces, WoL allows automatic, scheduled, or on-demand powering on of physical devices, using another device with FlexxAgent installed on the network as a bridge. This will be responsible for sending the magic packet necessary to activate the target device within the local network.

Requirements

- Compatible network card.
- Enable WoL in BIOS/UEFI.
- Set up WoL in the operating system.
- A bridge device — with FlexxAgent installed and reporting — on the same network as the device you want to turn on.

> **INFO**
>
> WoL normally operates within a local network and can work across subnets as long as there are no restrictions imposed by firewalls or network devices that block the transmission of the magic packet. In environments with subnet segmentation, it's necessary to configure network-level exceptions that allow the magic packet to be routed between those subnets.

Set up WoL in Windows

To set up WoL on a Windows operating system device, you should follow these steps:

1. **Check if WoL is active.**

In the CMD window, execute the following command:

`powercfg /devicequery wake_programmable`

2. **Enable WoL.**

Run the command:

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

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

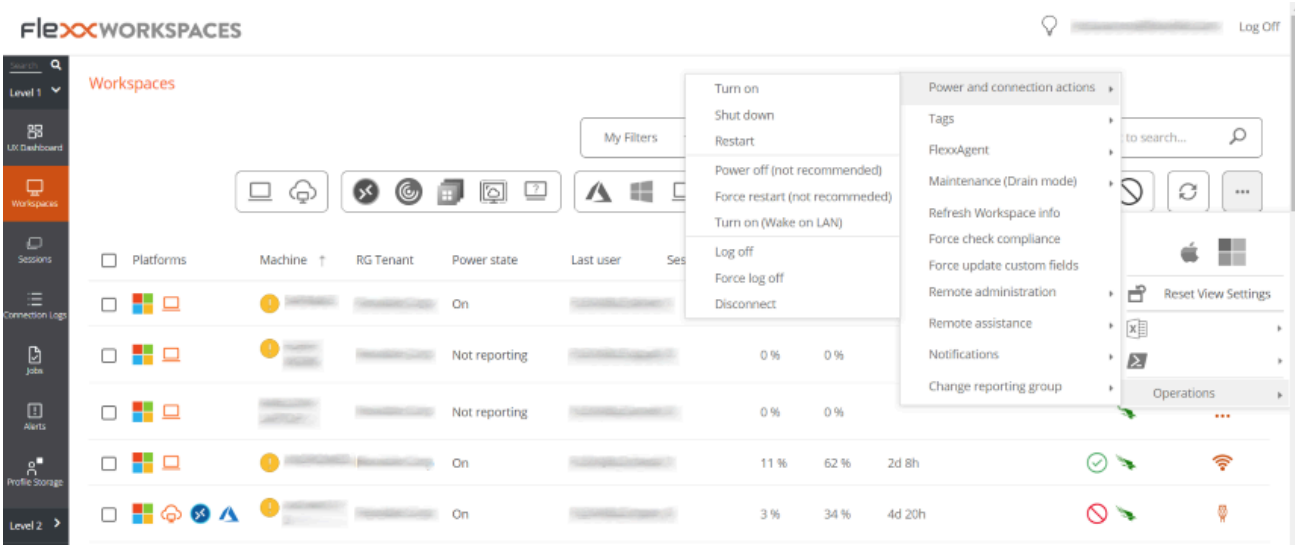
Available actions

When the functionality has been correctly enabled and configured, the following actions will be available:

- Power on devices on demand from Workspaces
- Schedule power on using Workspace Groups
- Schedule power on after applying updates

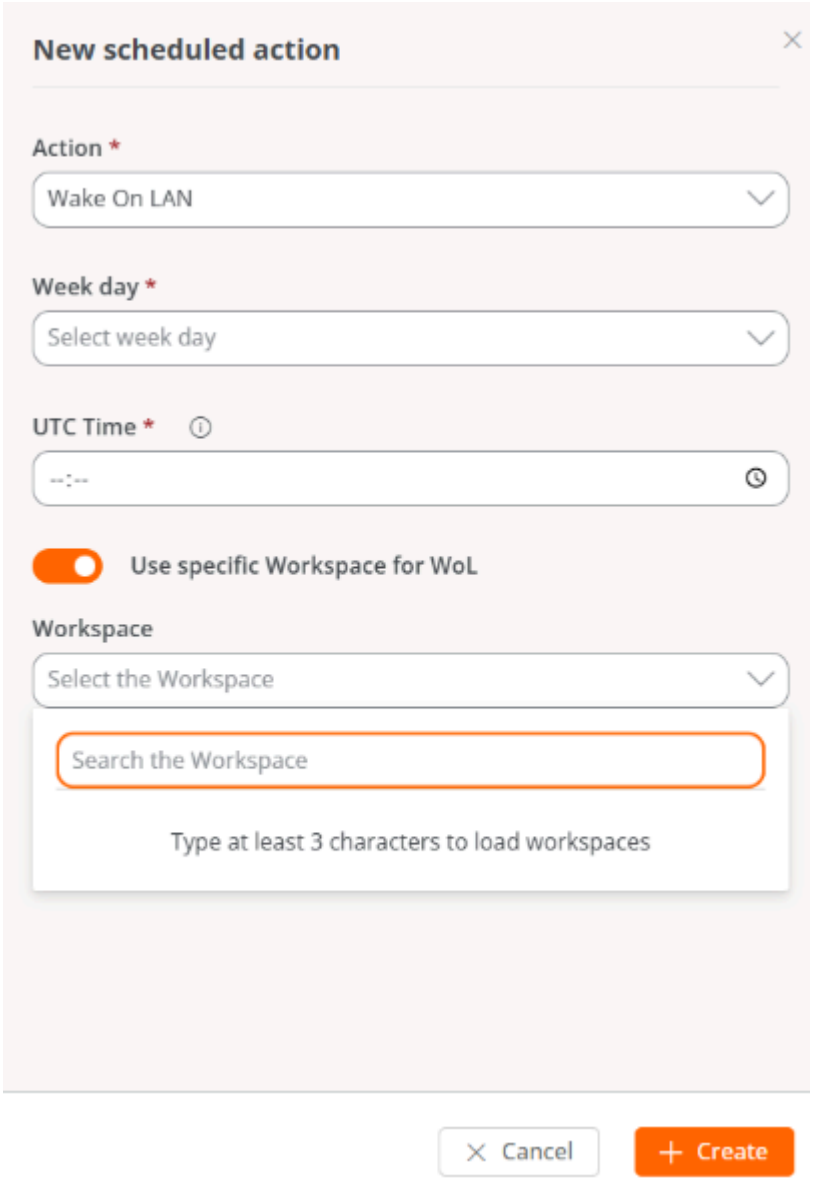
Power on devices on demand from Workspaces

1. Access the Workspaces module.
2. Select one or more devices you want to execute the power-on operation on.
3. Click `Operations` -> `Power and connection actions` -> `Turn on (Wake on LAN)`.



Schedule power on using Workspace Groups

1. Access Portal -> `Workspaces` -> `Workspace Groups`
2. Select the workspace group you want to schedule the power on for.
3. Click on the `Schedule` tab.
4. Click the `New` button and fill out the form.
    - **Action.** Allows you to choose between *Wake on LAN* or *Shut down*. If the first option is selected, you can activate `Use specific Workspace for WoL` at the bottom of the form to schedule the power on for a specific device.
    - **Day of the week.** Day of the week when the action will be performed.
    - **UTC time.** Exact time to start the action.
5. Click on `New`.

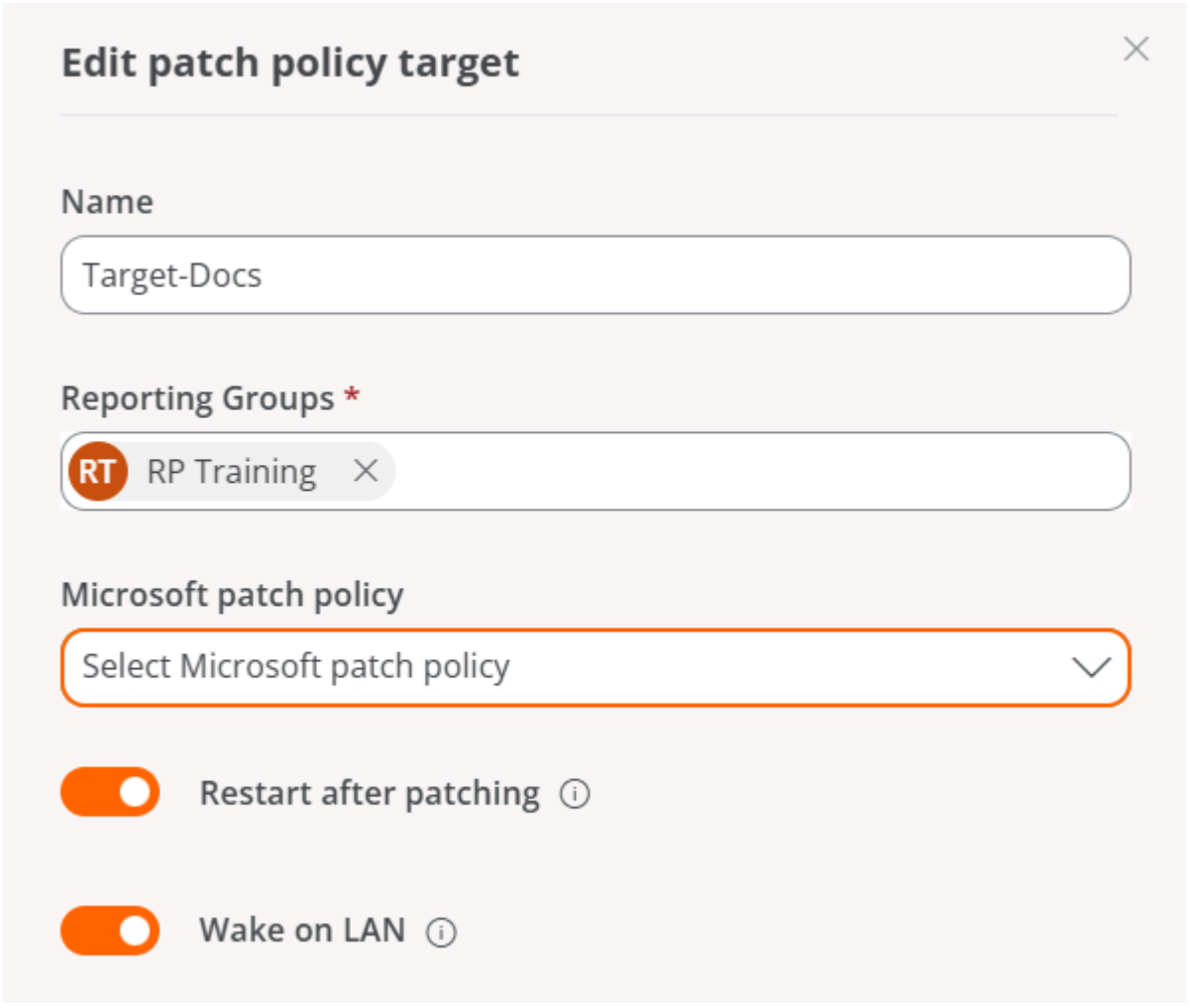


The data entered will be reflected in the table, along with the email of the user who created and updated the schedule. From `View details` you can edit and delete the scheduled action.

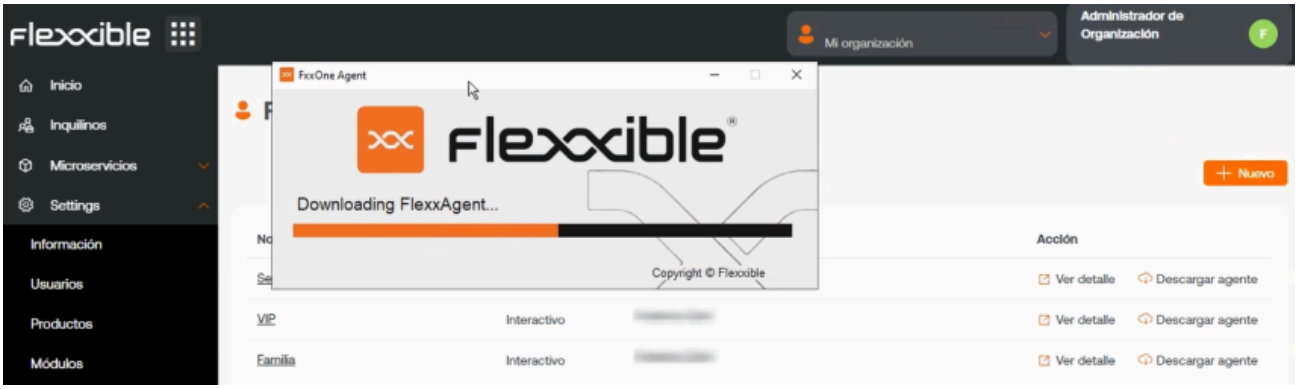
Schedule power on after applying updates

1. Access Portal -> `Workspaces` -> `Patch` -> `Targets`.
2. In the table, choose the recipient.
3. In the `Details` tab click on the `Edit` button.
4. Activate the `Wake on LAN (WoL)` option in the form.

5. Click on `Save`.



FlexxAgent / FlexxAgent Guides



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.

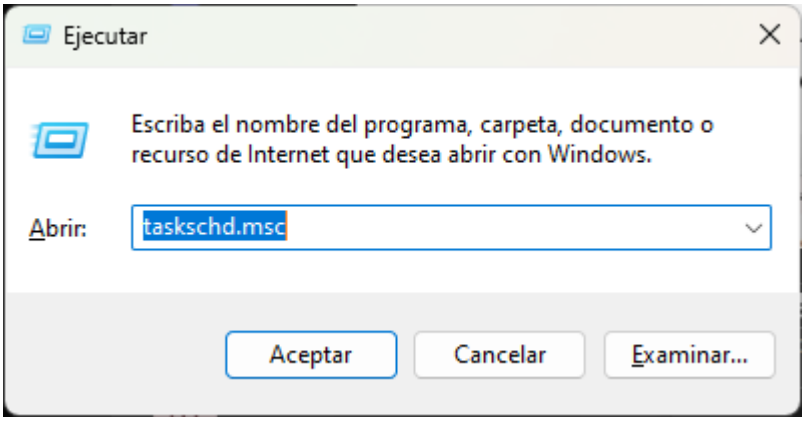
FlexxAgent / Guides / Validate FlexxAgent connectivity

To validate the connectivity of FlexxAgent with the service's SaaS instances and ensure its correct execution, follow the procedure defined here 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.

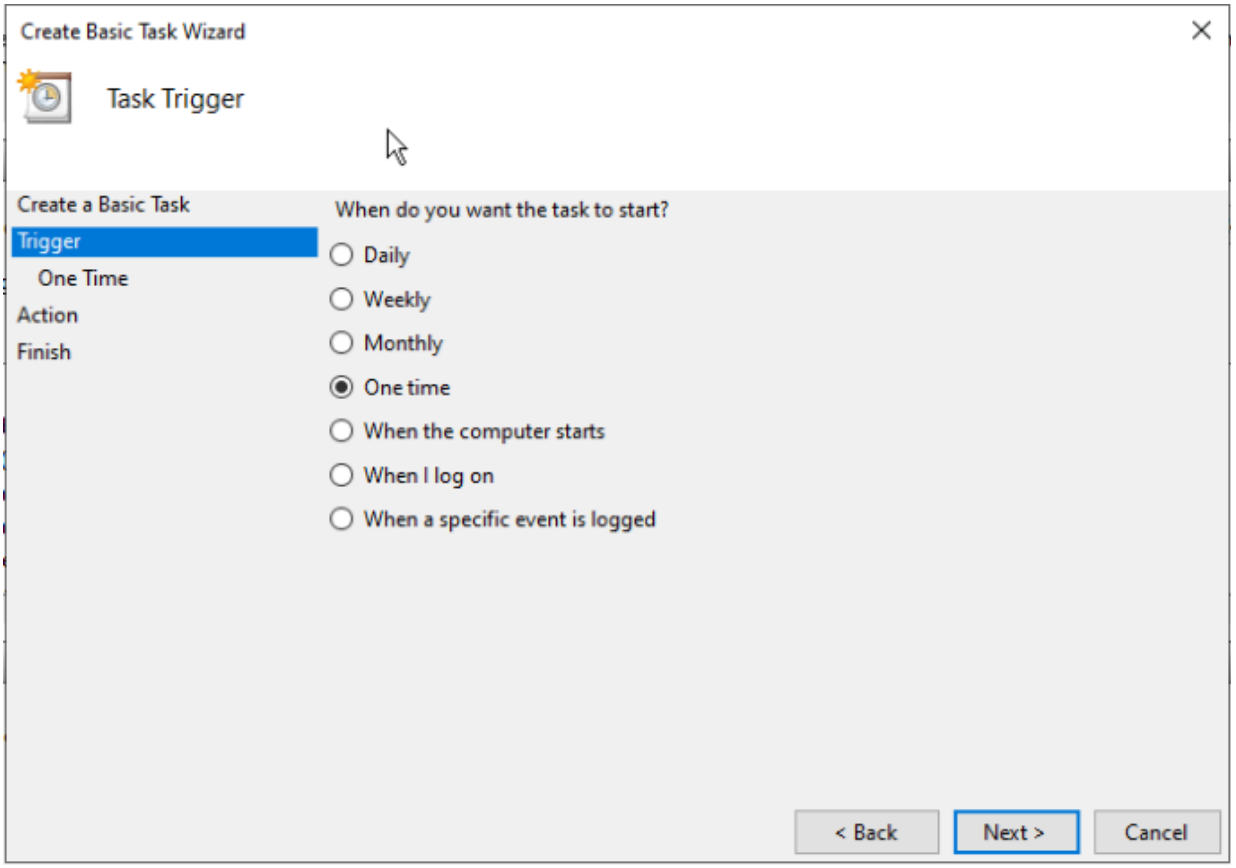
Creating a scheduled task

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

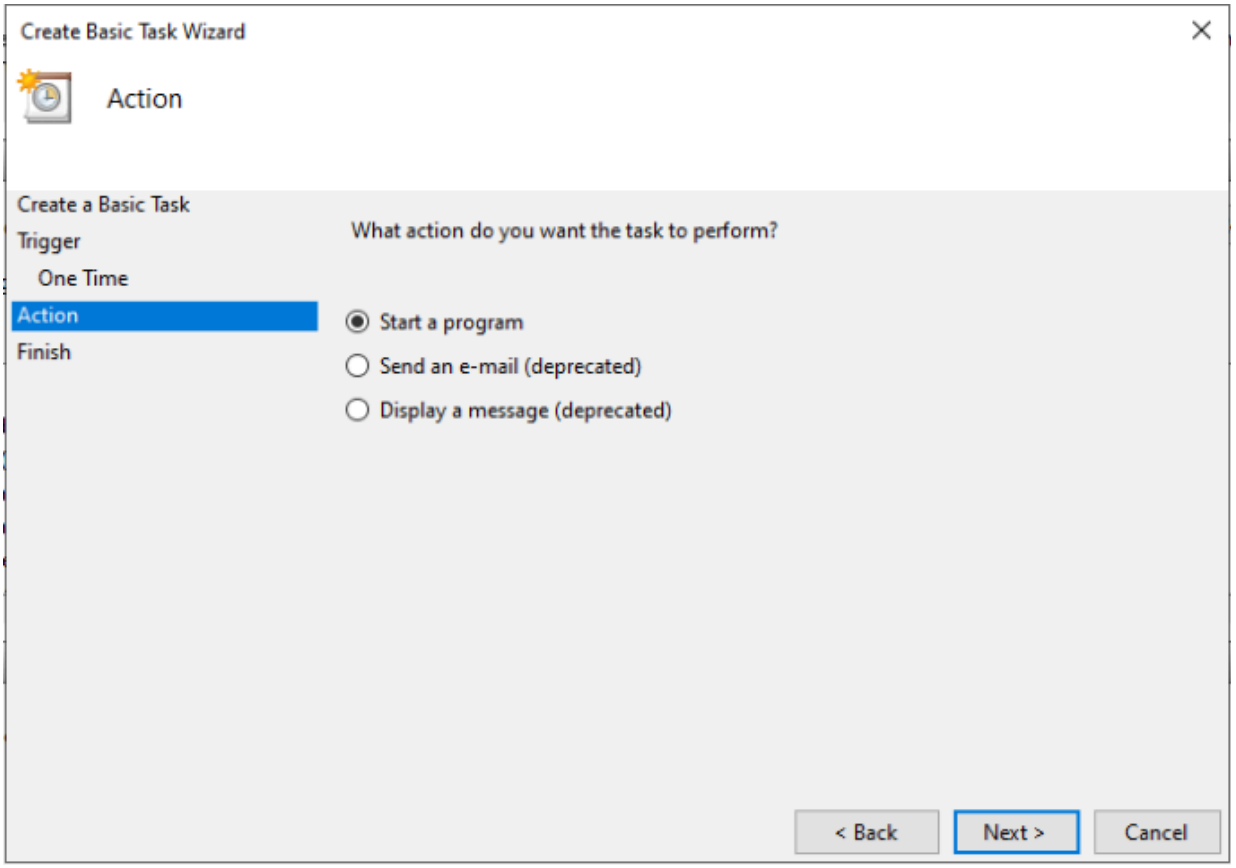


2. In the `Actions` panel, select the `Create Basic Task` option and name the task (it can be `FlexxAgent check connectivity`). You can write a description if desired, and click `Next`.

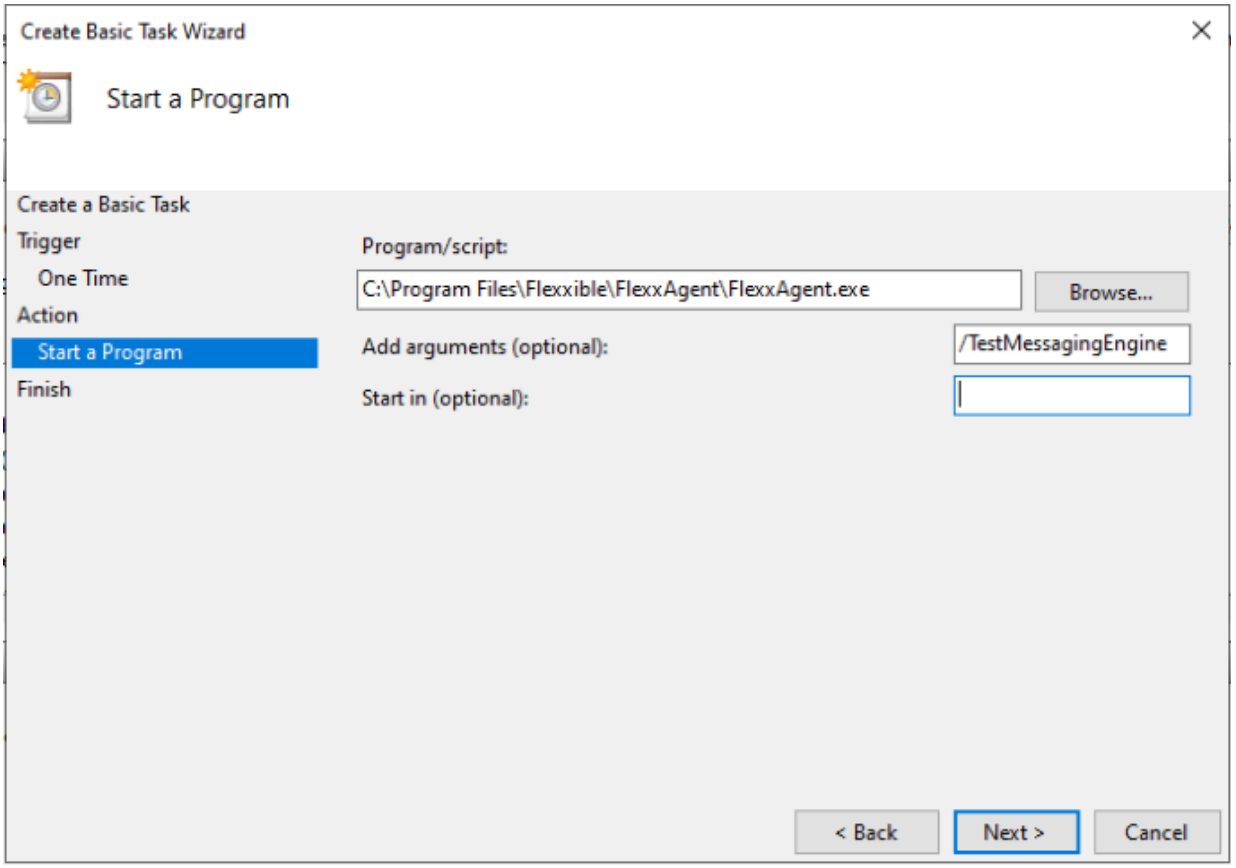
3. Next, select `One Time` and click `Next`. A date picker will appear, but it is not relevant because the task will be executed manually. Click `Next`.



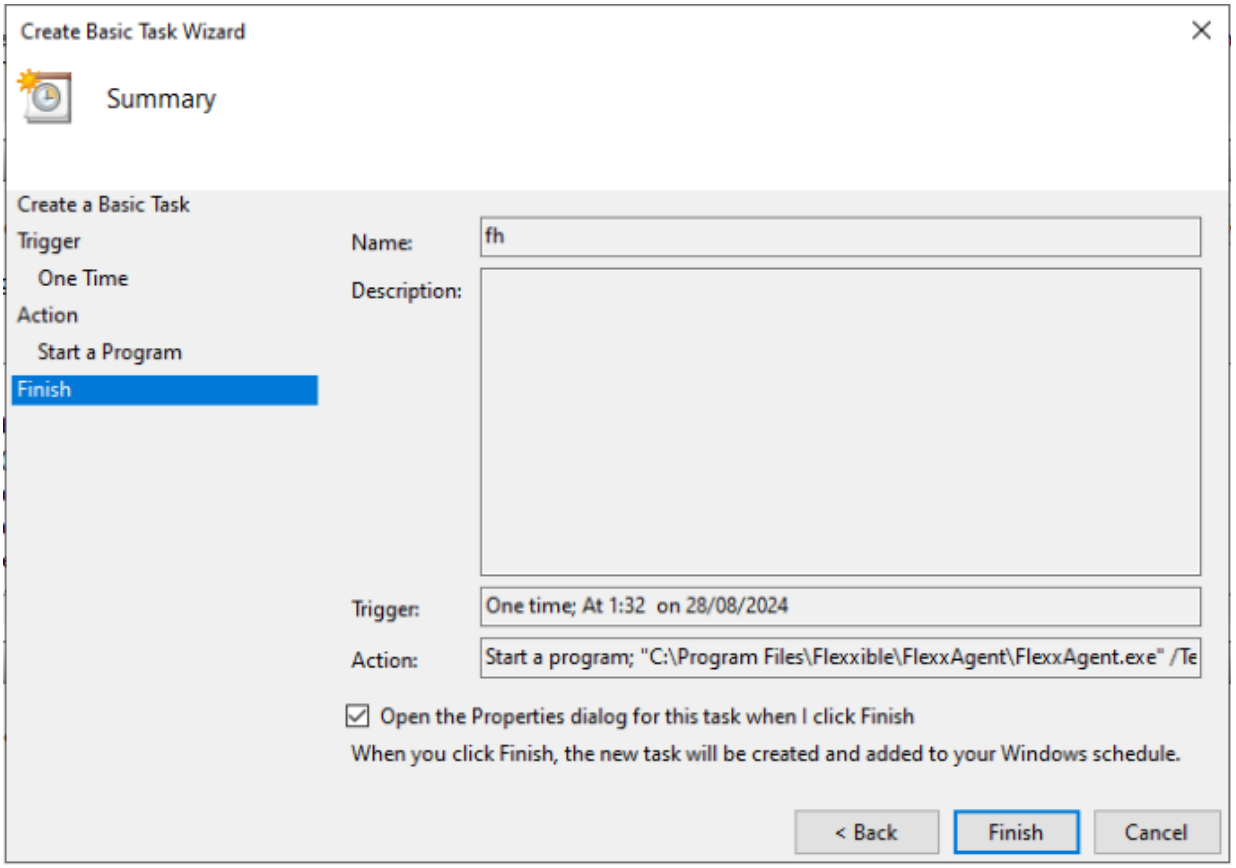
4. Select the `Start a program` action and click `Next`.



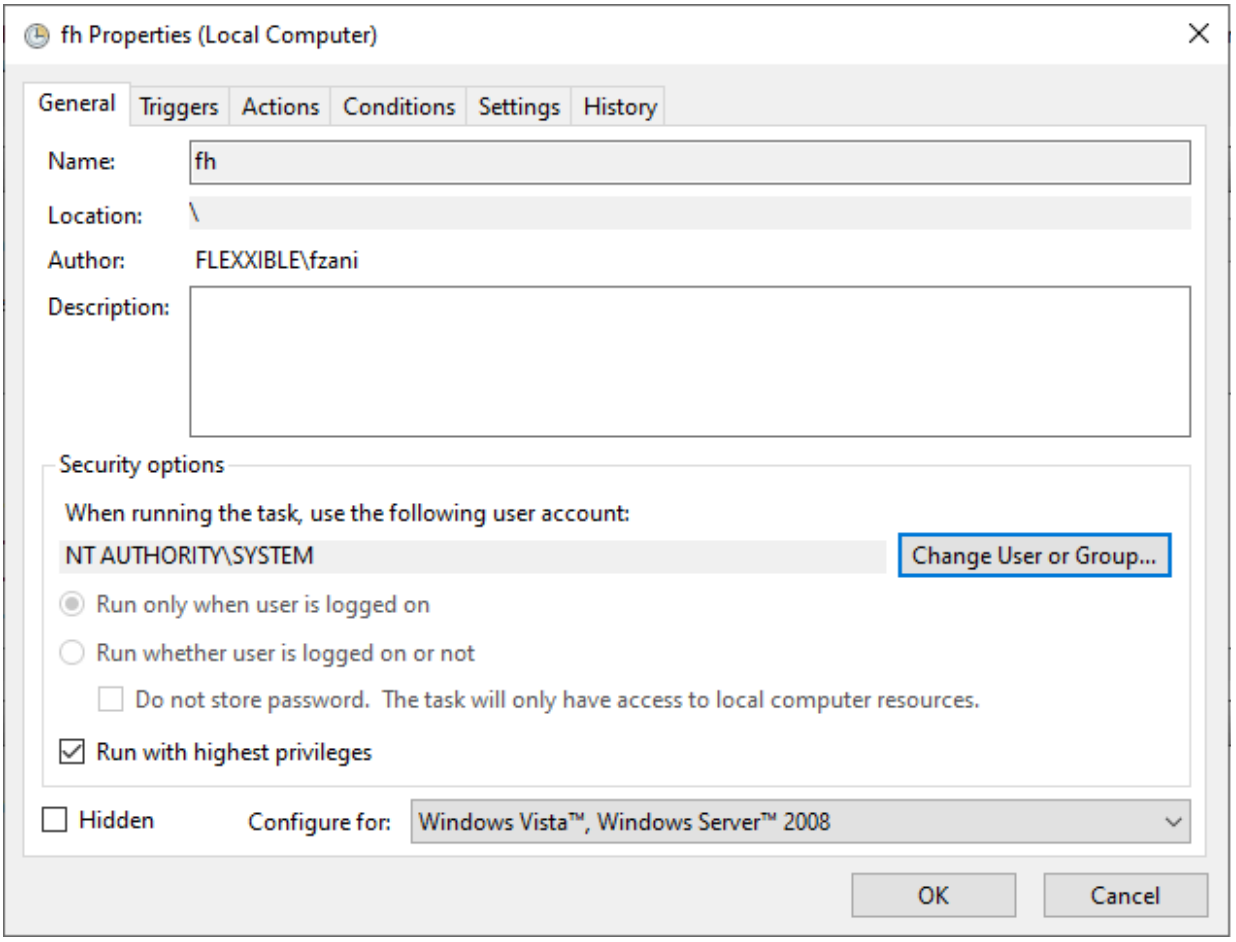
5. In the `Program/script` field, type or browse to the path `C:\Program Files\Flexxible\FlexxAgent\FlexxAgent.exe`. In `Additional Arguments`, type `/TestMessagingEngine`. Click `Next`.



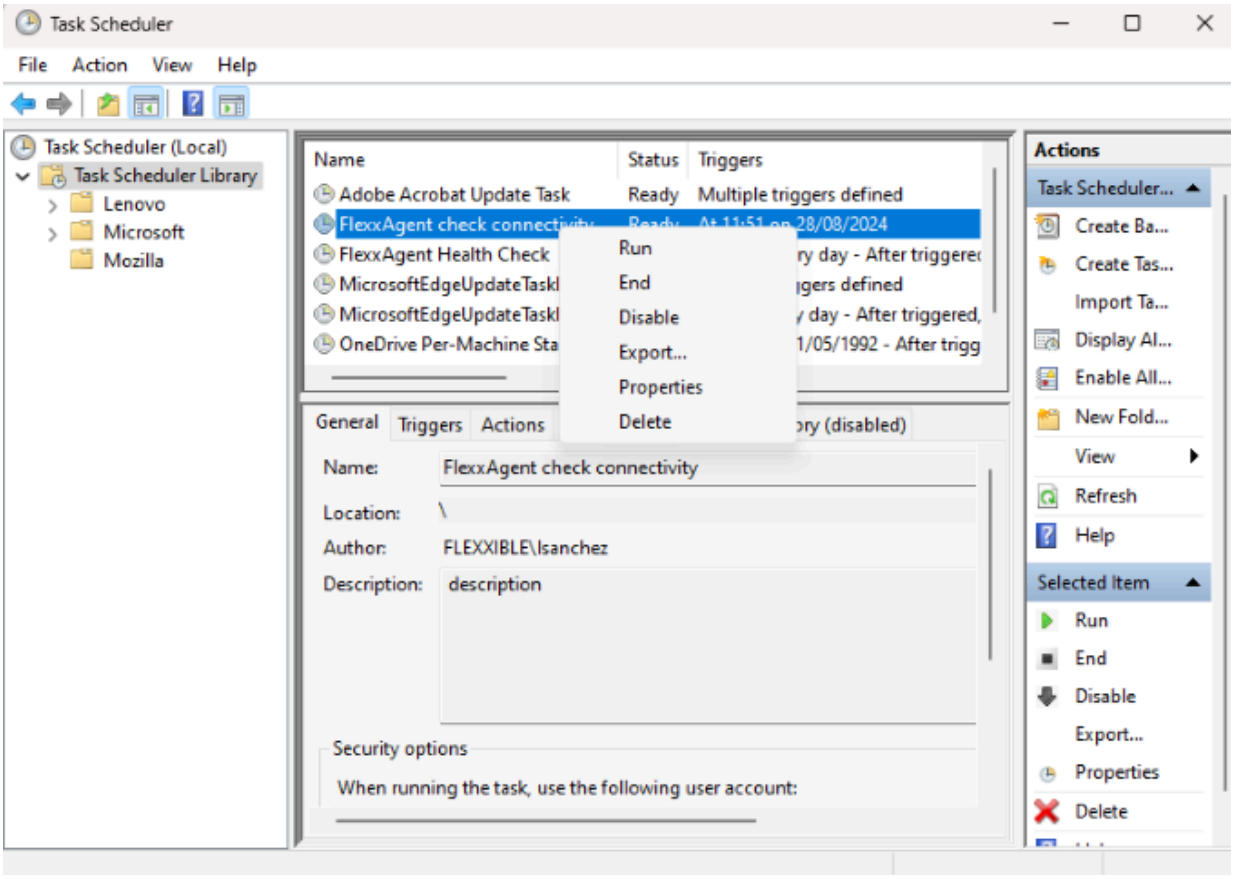
6. Select `Open the Properties dialog for this task when I click Finish` and click `Finish`. The task properties dialog will open.



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.

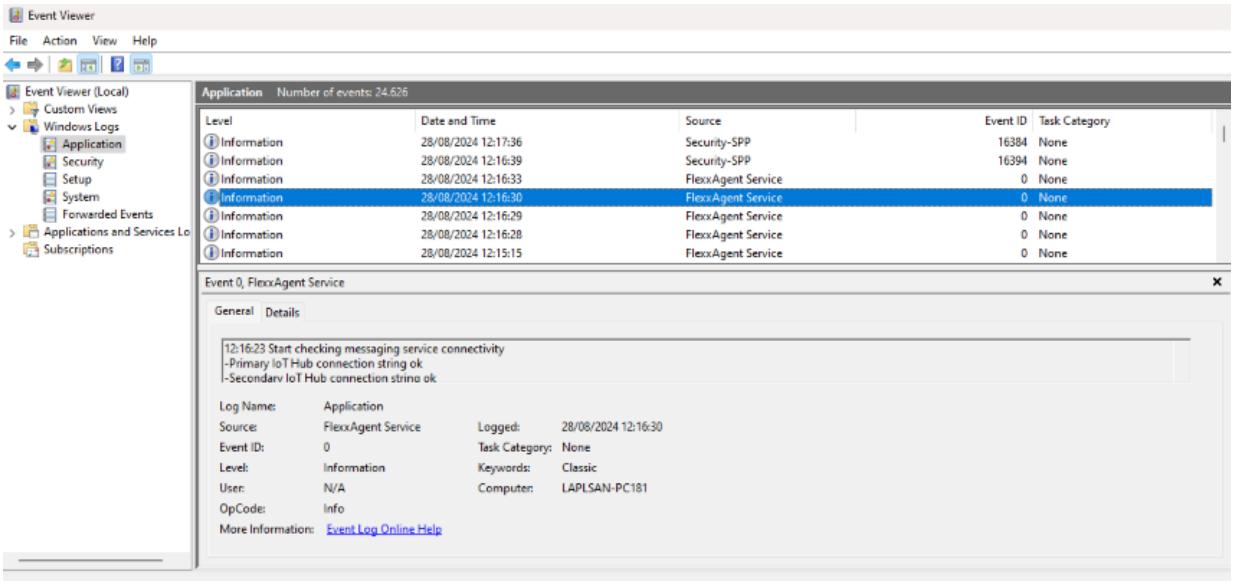


9. Select the `History` tab to see the progress of the task until you see the `Task completed` event. In case the history is disabled, it can be enabled with the `Enable history for all tasks` option in the right panel of the console.

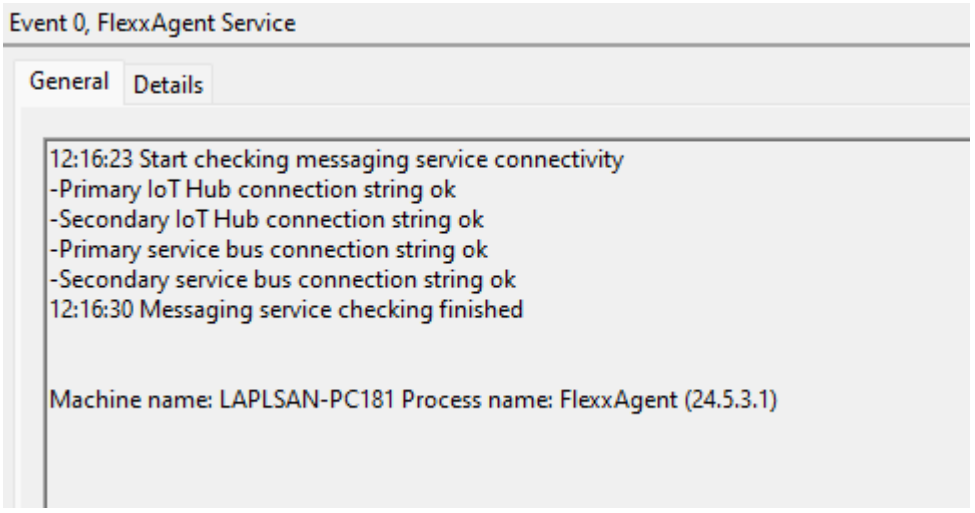
Validation of results

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:



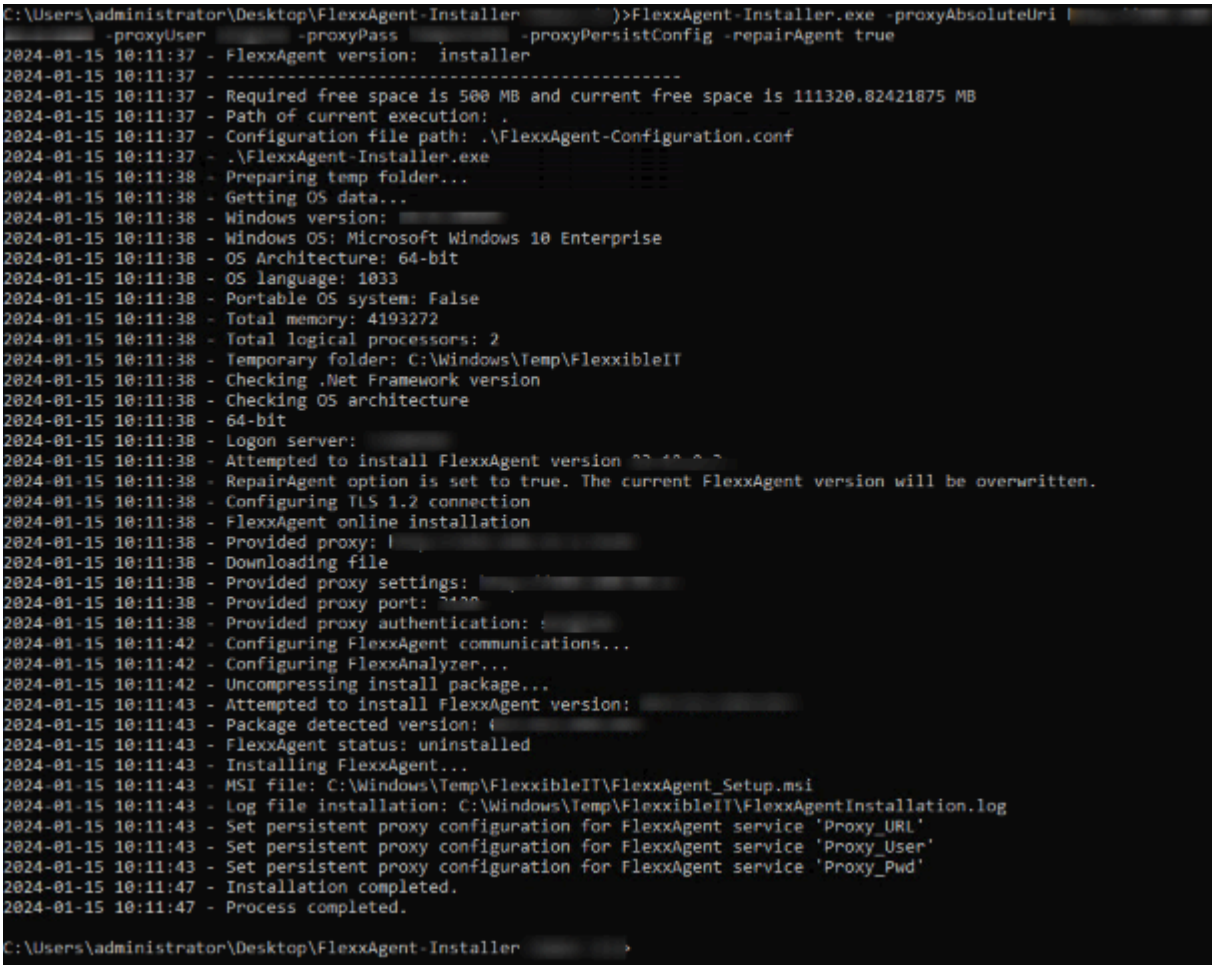
FlexxAgent / Guides / Install FlexxAgent by configuring a proxy server

In many organizations, users connect to the internet using a proxy server. This guide explains how to configure it to install FlexxAgent.

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 proxy server address, expressed as a complete "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 previous 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.

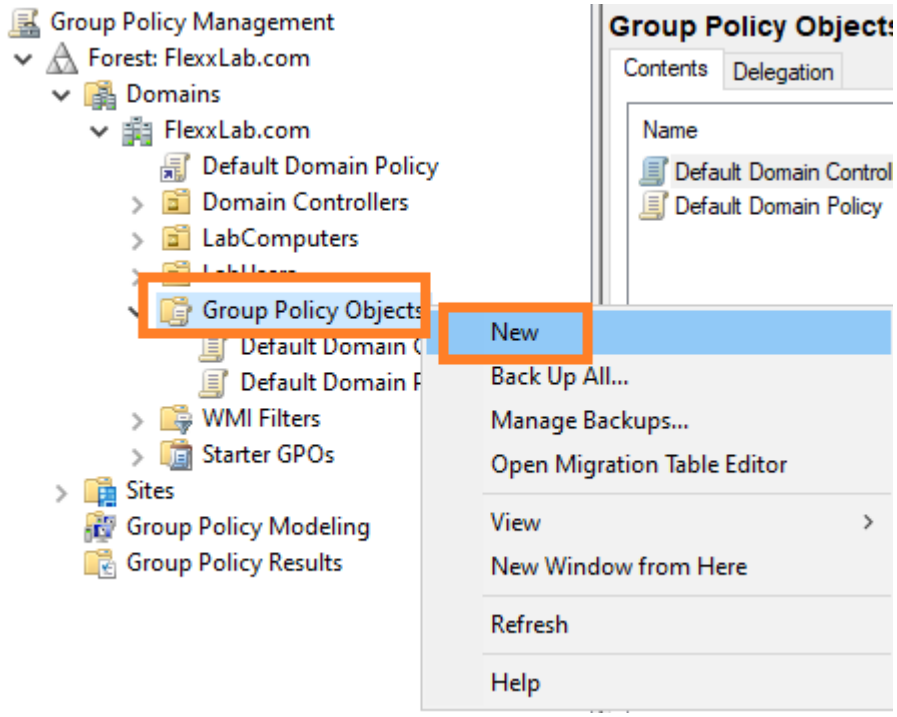
Key Proxy_Pwd

- Key path: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Flexxible\FlexxAgent\Communications
- Key Name: Proxy_Pwd
- Key type: REG_SZ
- Supported values: The password to authenticate 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 / Set up a proxy server through 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:

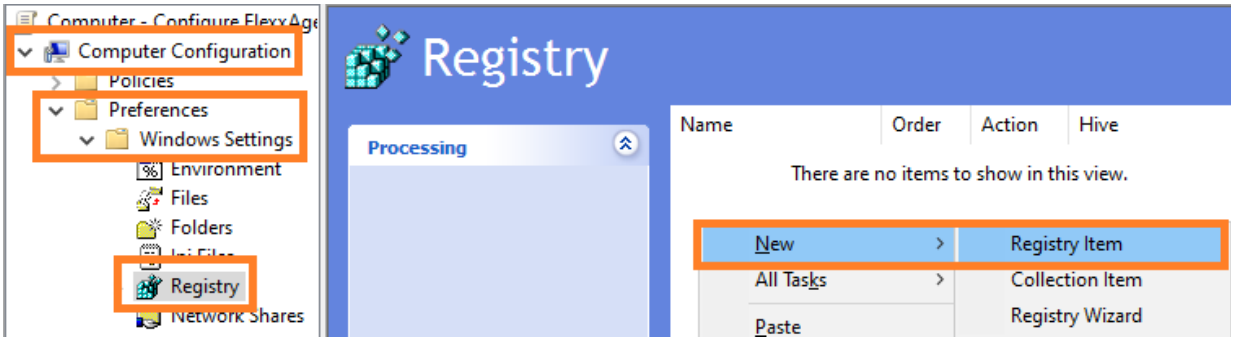
1. Access the domain controller's group policy management console. Create a new policy using the `New` option from the menu that appears when you right-click on `Group Policy Objects`.



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

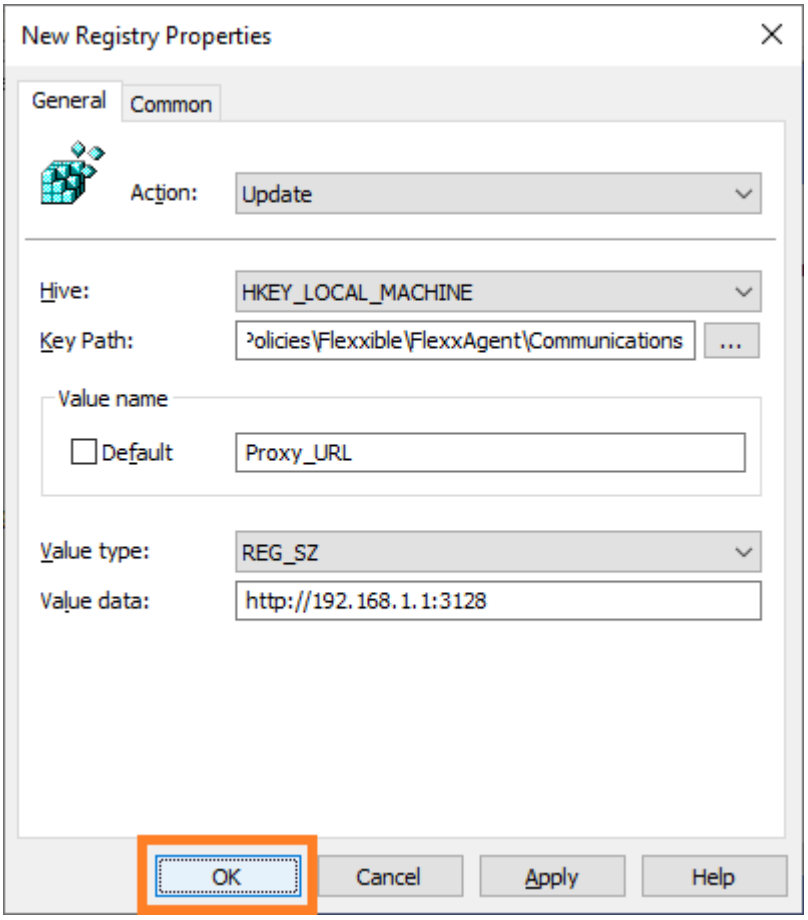
3. Select the policy with the right mouse button and edit it (select `Edit…`)

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

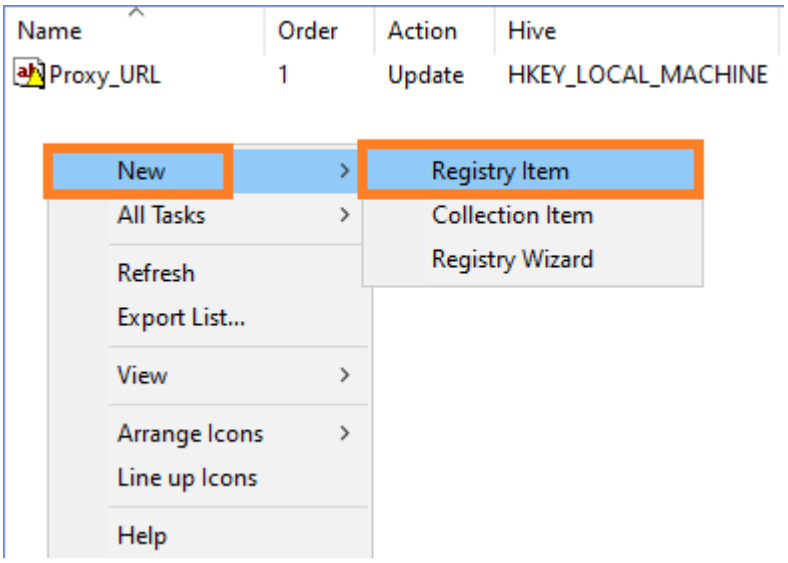


5. Add the following information and click `OK`.

   - Action: Update
   - Key path: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Flexxible\FlexxAgent\Communications`
   - Value Name: Proxy_URL
   - Value type: REG_SZ
   - Value data: The proxy address (URL) and port. 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

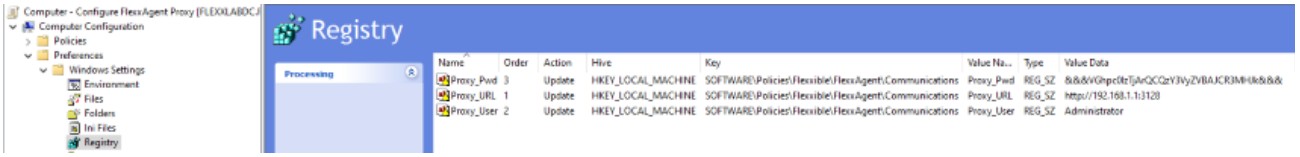
- Key path: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Flexxible\FlexxAgent\Communications`
- Value Name: Proxy_User
- Value type: REG_SZ
- Value data: The username to authenticate on the proxy server. For example *Admin*.

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`.

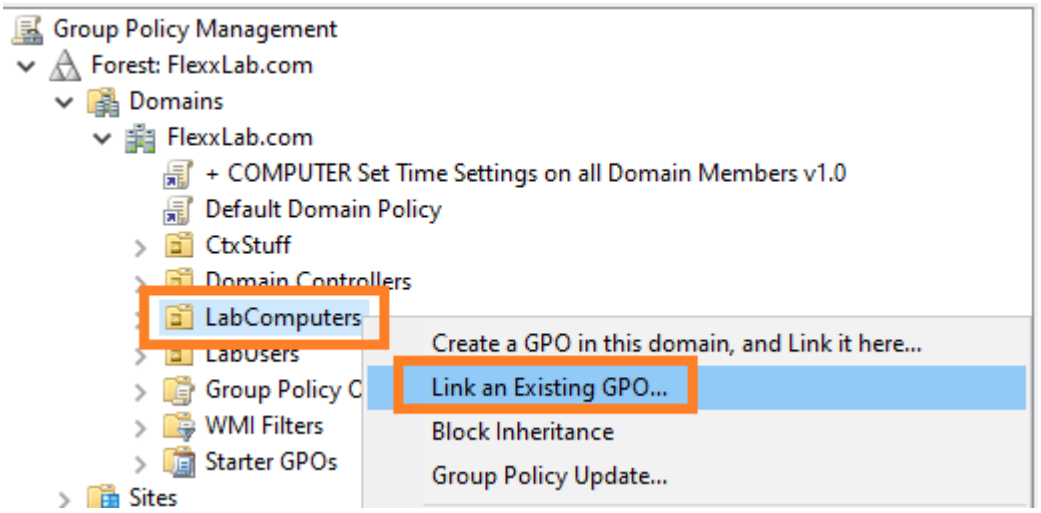
   - Action: Update
   - Key path: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Flexxible\FlexxAgent\Communications`
   - Value Name: Proxy_Pwd
   - Value type: REG_SZ
   - Value data: The password to authenticate on the proxy server for the user configured in the previous step.
     - The `Proxy_Pwd` key value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

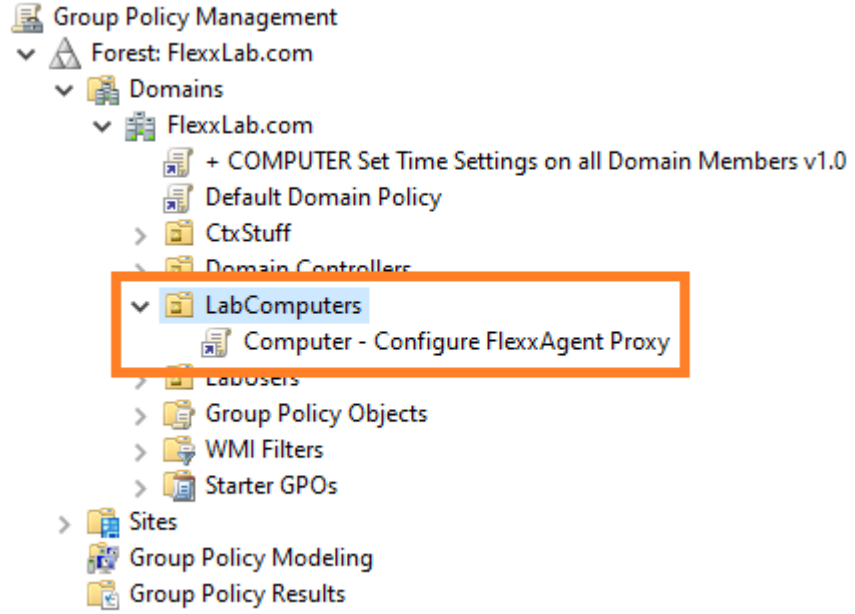


11. Close the editor.

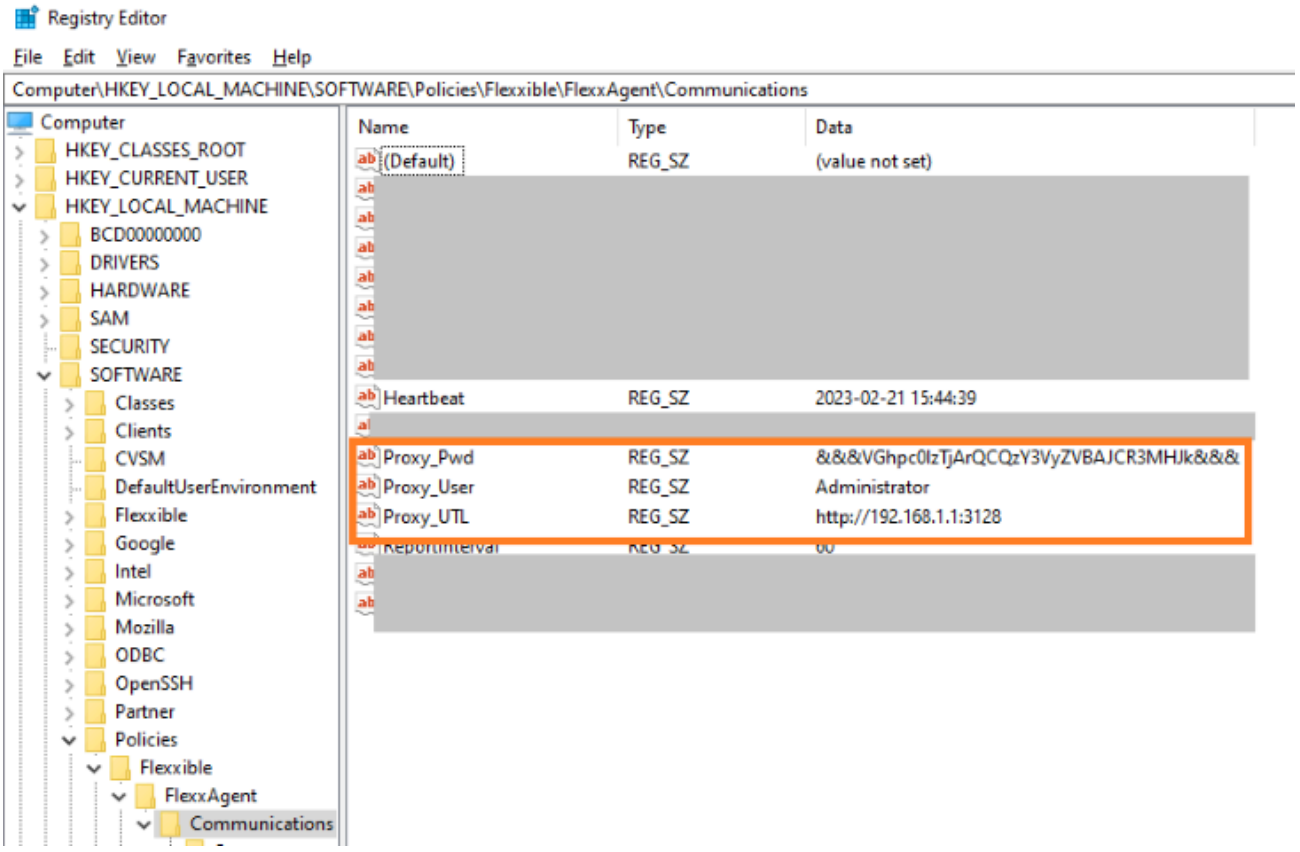
12. With the right mouse button, select the list of devices that will receive this configuration within the domain controller (under the domain or organizational unit) and select `Link an Existing GPO`.



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 device that the group policy has been applied correctly, you need to restart the device. Once it starts, you can go to the registry editor and check that the entries were created correctly.



FlexxAgent / Guides / Deploy FlexxAgent via group policy (GPO)

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

Deploying

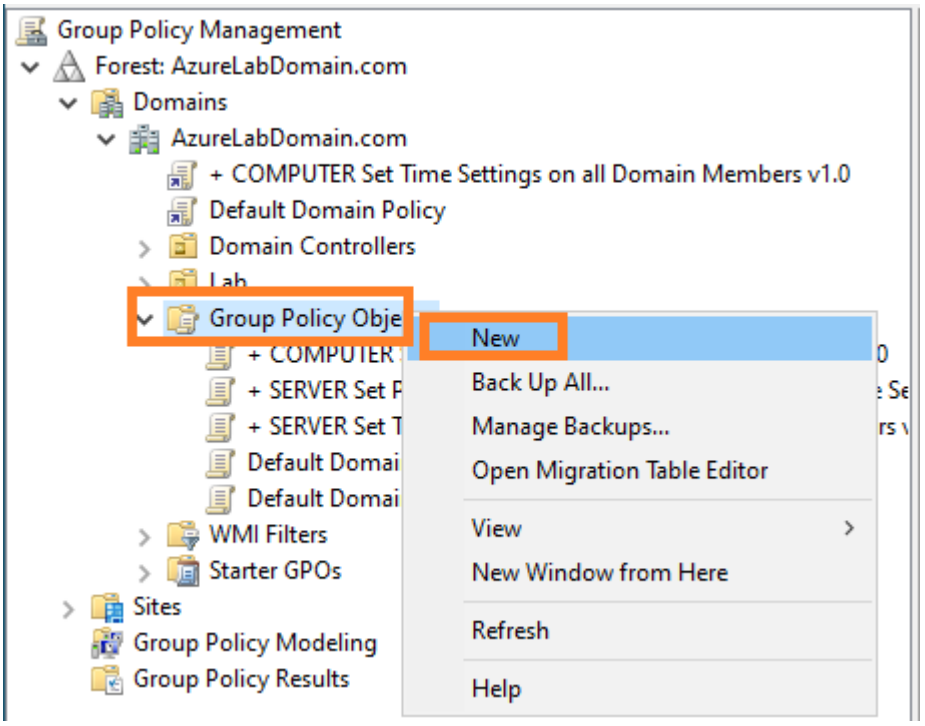
1. Create a Powershell script called `Install.ps1` with the following content:

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

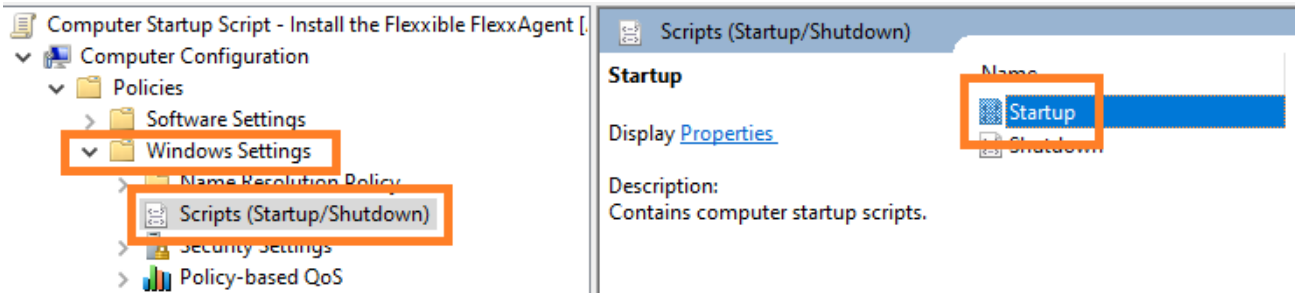
   Example: Start-Process `C:\Temp\FlexxAgent-Installer\FlexxAgent-Installer.exe`

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

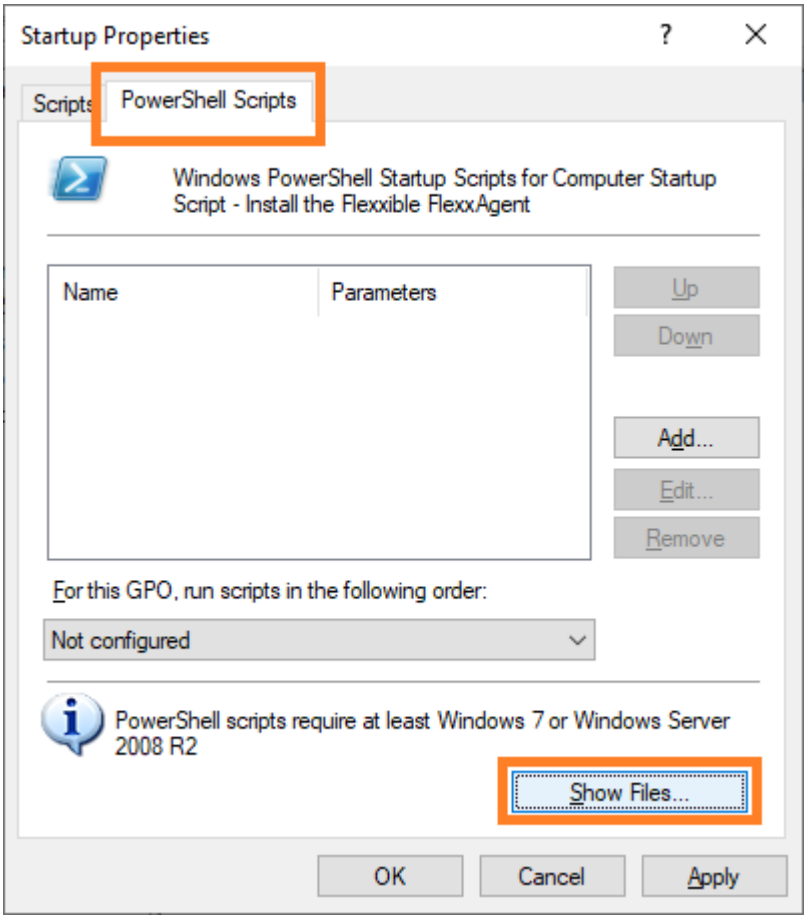
2. Save the file for later use.
3. Run the group policy management console in a domain controller that has remote computer management tools installed.
4. Create a new group policy within the group policy container.



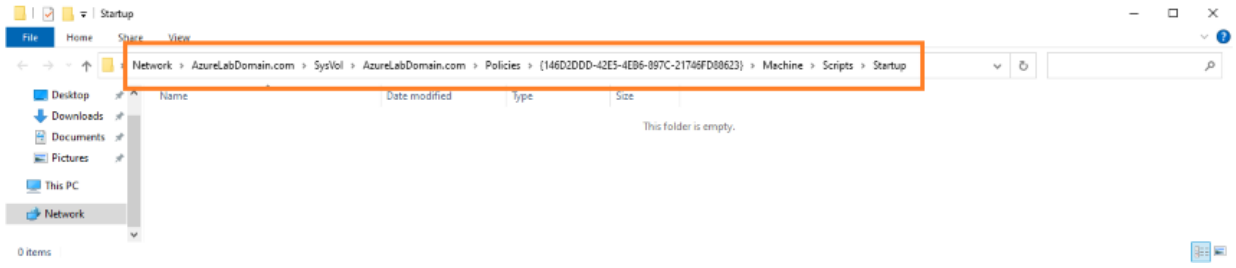
5. Give the new policy a name. Choose one that is meaningful.
6. Right-click on the group policy and select `Edit`.
7. Expand the tree `Computer Configuration` -> `Windows Settings` and select `Scripts (Startup/Shutdown)`



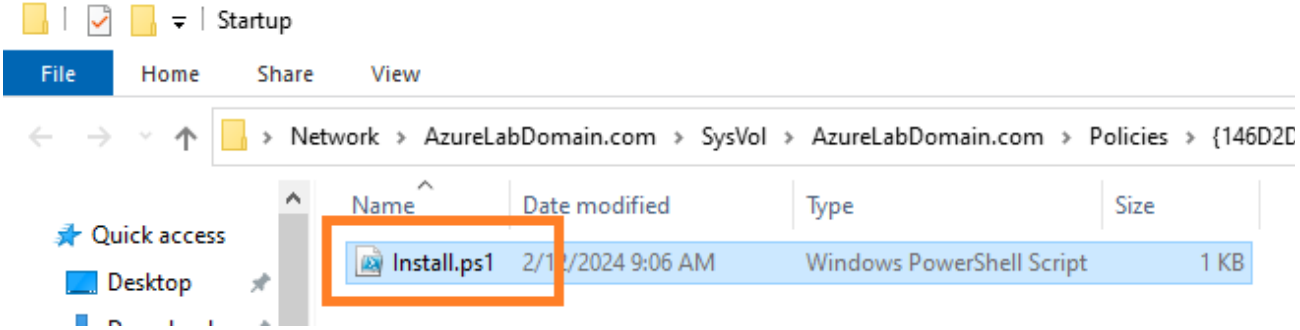
8. A dialog will appear in a new window. Select `PowerShell Scripts` in it. Next, click on the `Show Files...` button



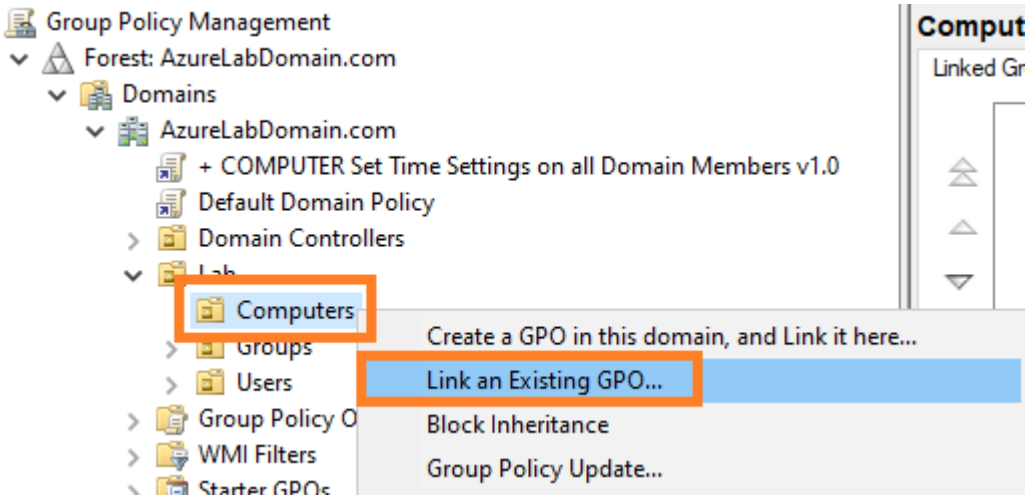
9. The network folder where the group policy scripts are stored will open.



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. Close the Windows Explorer 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 organization branch within the domain controller that contains the devices where you want to install FlexxAgent. Select the branch and right-click on it. Select `Link an Existing GPO`.

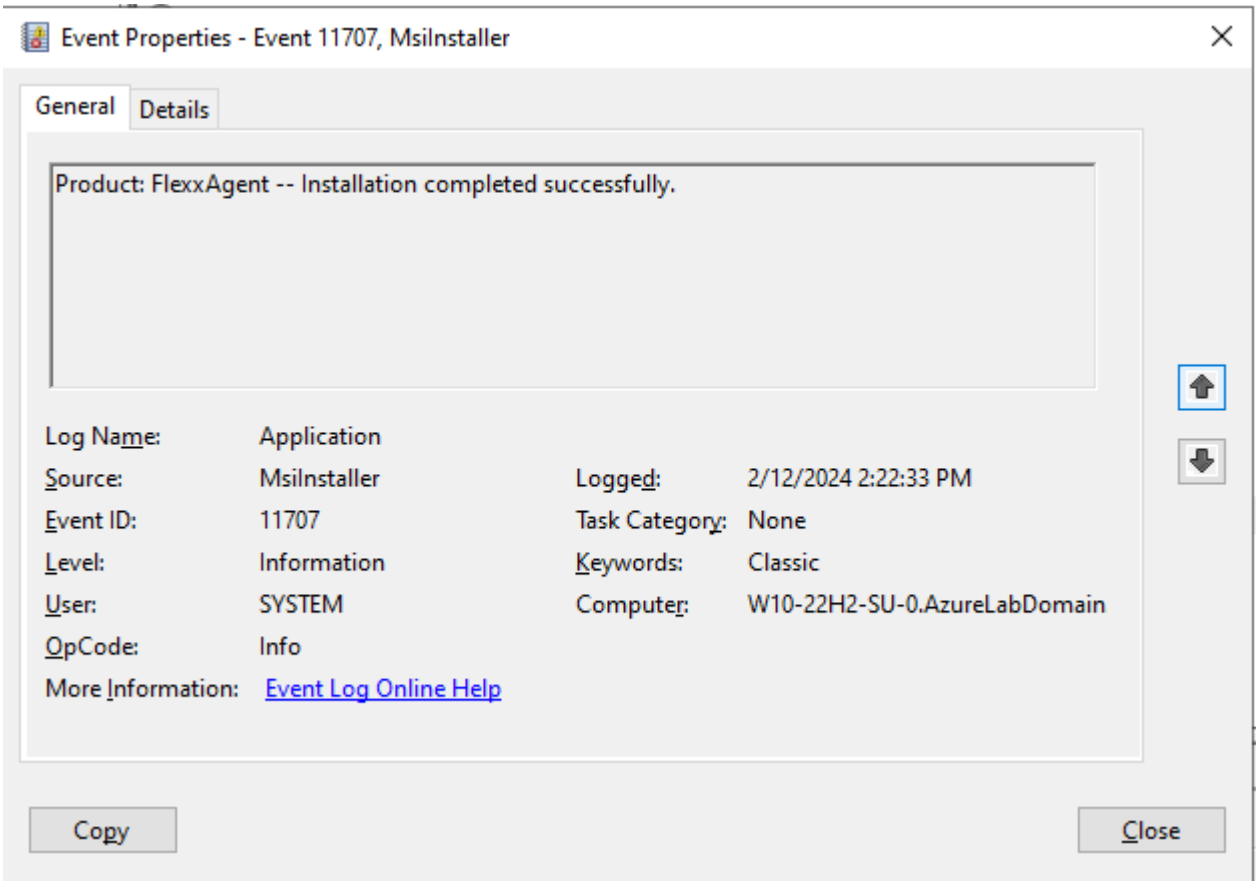


18. A selection dialog will appear where the previously created policy will be selected. Once selected, click `OK`.

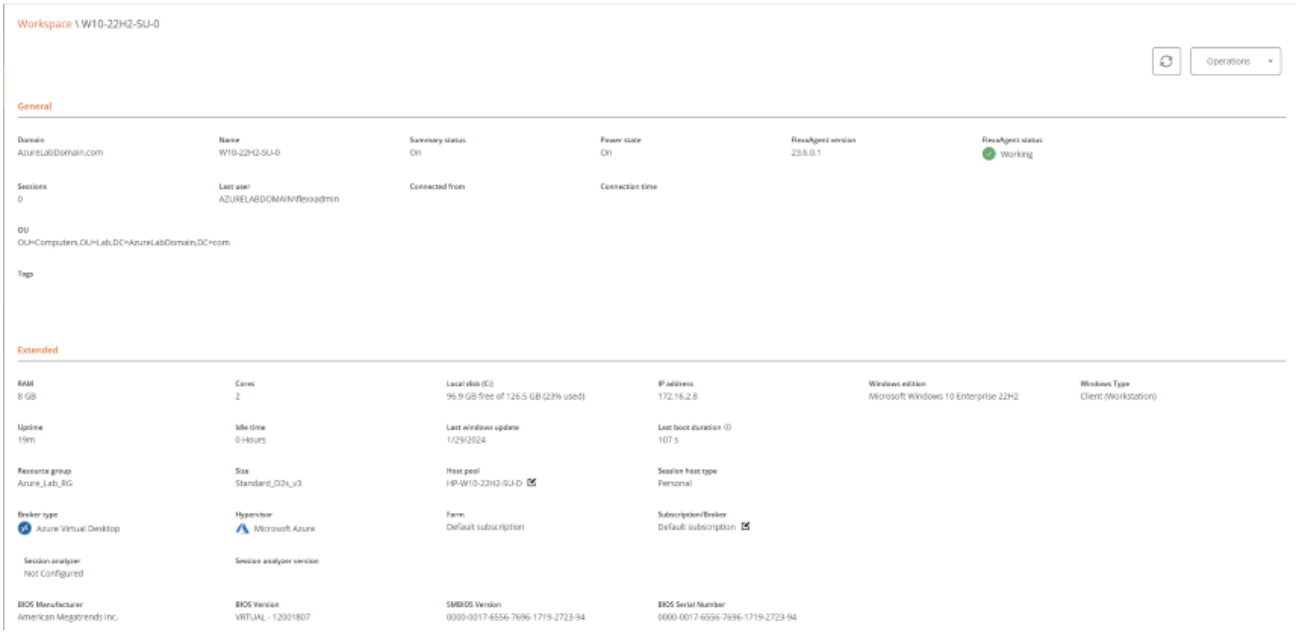
Verification

To validate the installation of FlexxAgent on a domain computer, it's necessary to restart at least one of the devices within it so that the group policy takes effect.

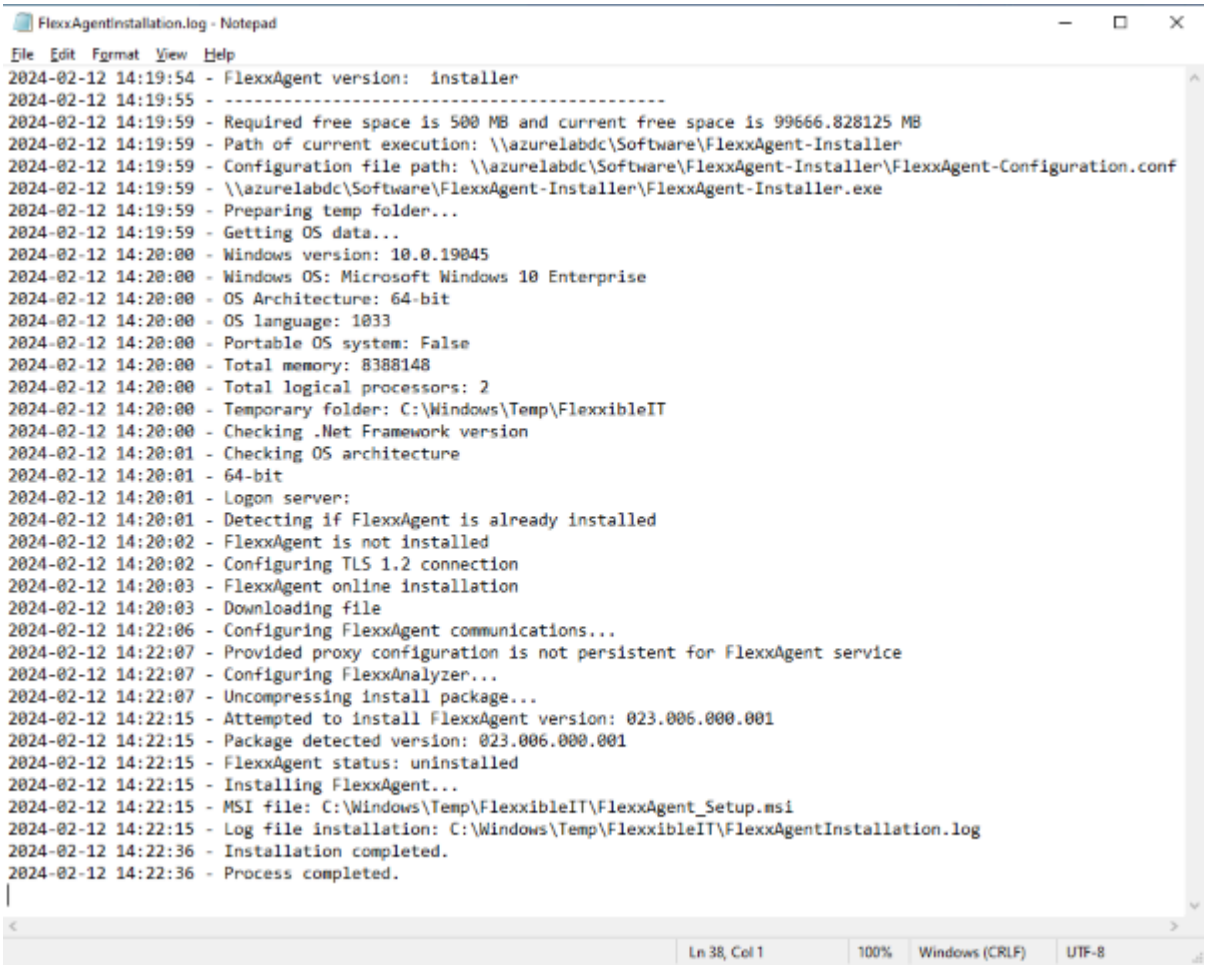
After the restart, you should access the Event Viewer, in the Application Log section, where you can check the events generated during the installation and the first execution of FlexxAgent.



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`.



FlexxAgent / Guides / Deploy FlexxAgent with Microsoft Intune

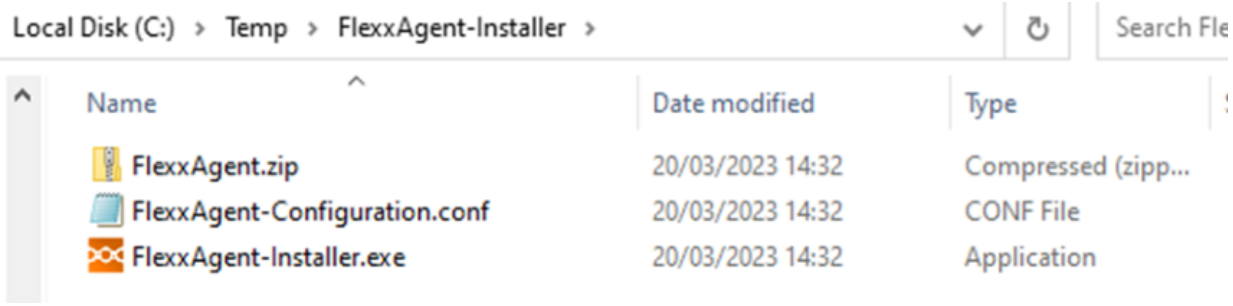
FlexxAgent can be deployed using Microsoft Intune. Before doing it, you need to check that you have the following requirements:

- 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:

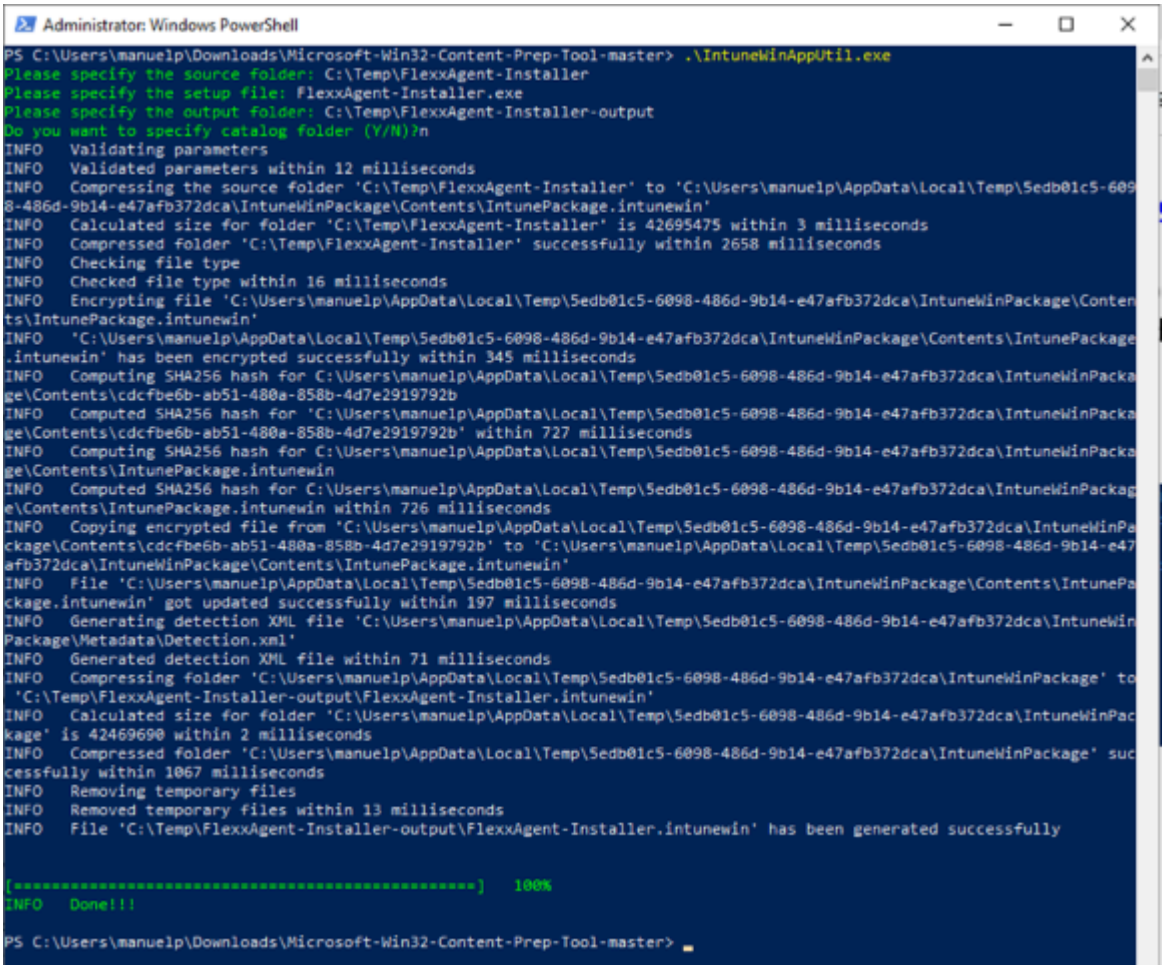
1. Unzip the installation package to some folder. You will see the files:



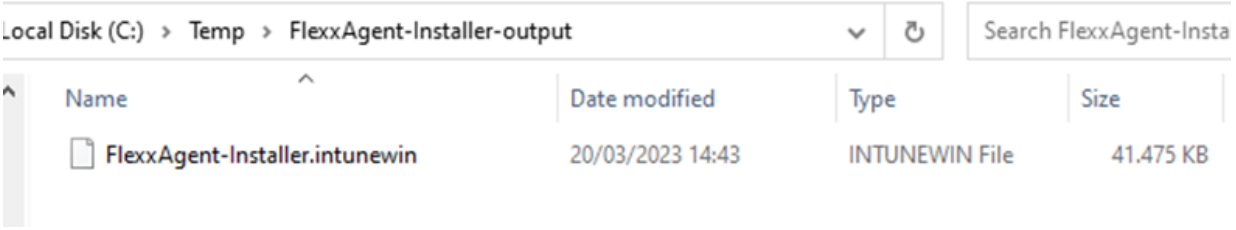
2. Download the `Microsoft Win32 Prep Tool`. For more information, see Prepare a Win32 app to be uploaded to Microsoft Intune.

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.

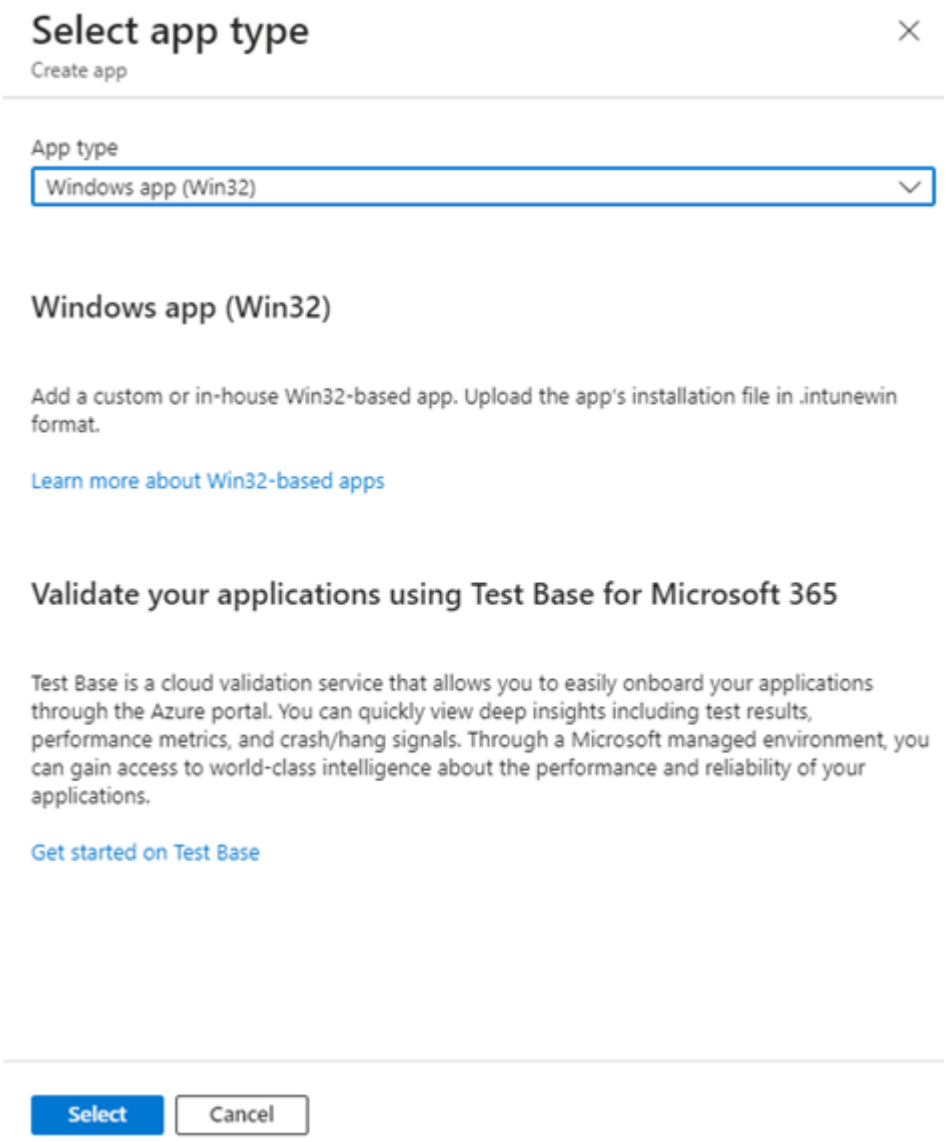


6. The created package is used to deploy an application within Intune.

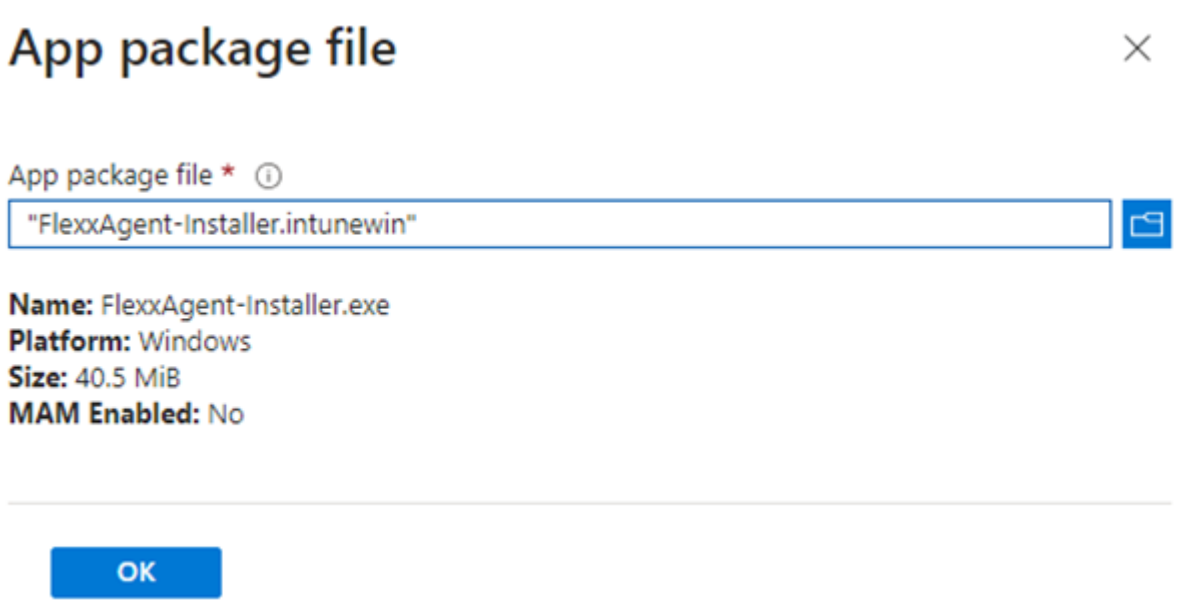
7. Go to the Intune admin center.

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

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

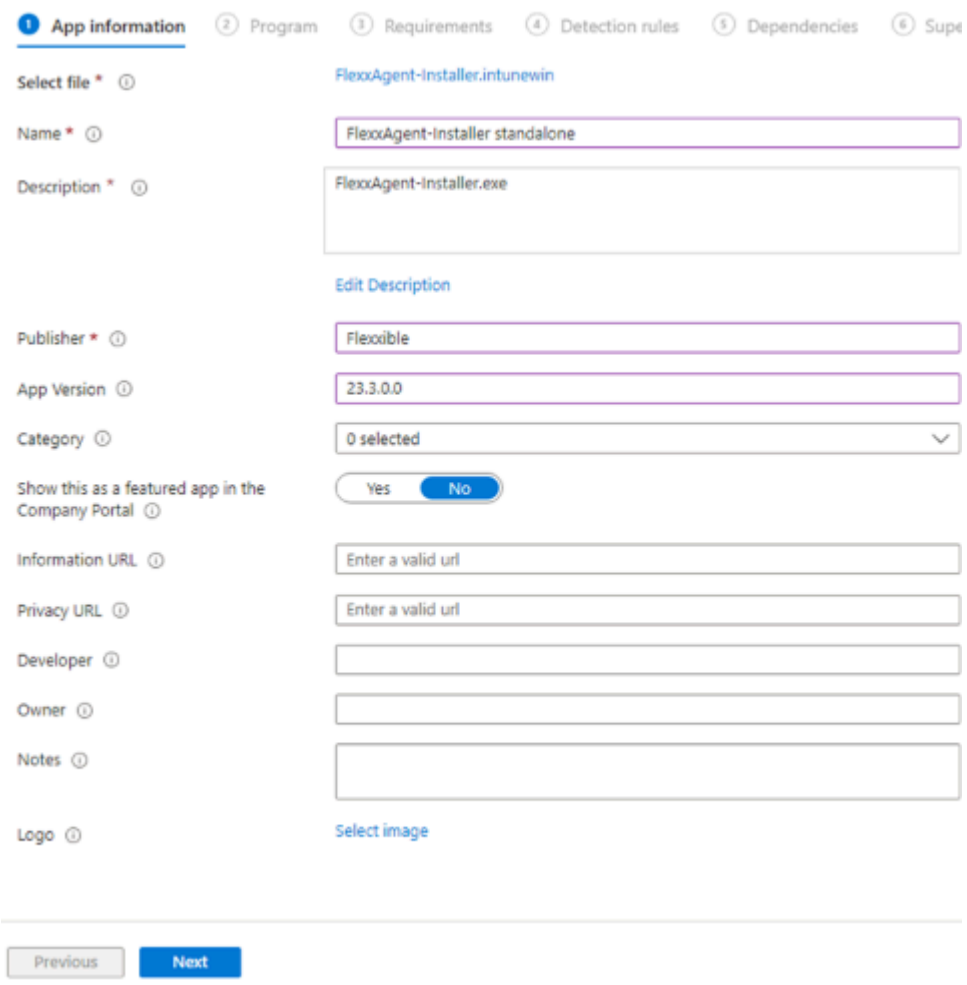


10. On the application information tab, click `Select app package file` and browse for the previously created package (in this example, it's in the folder C:\Temp\FlexxAgent-Installer-output).



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 file properties of FlexxAgent-Installer.exe.



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

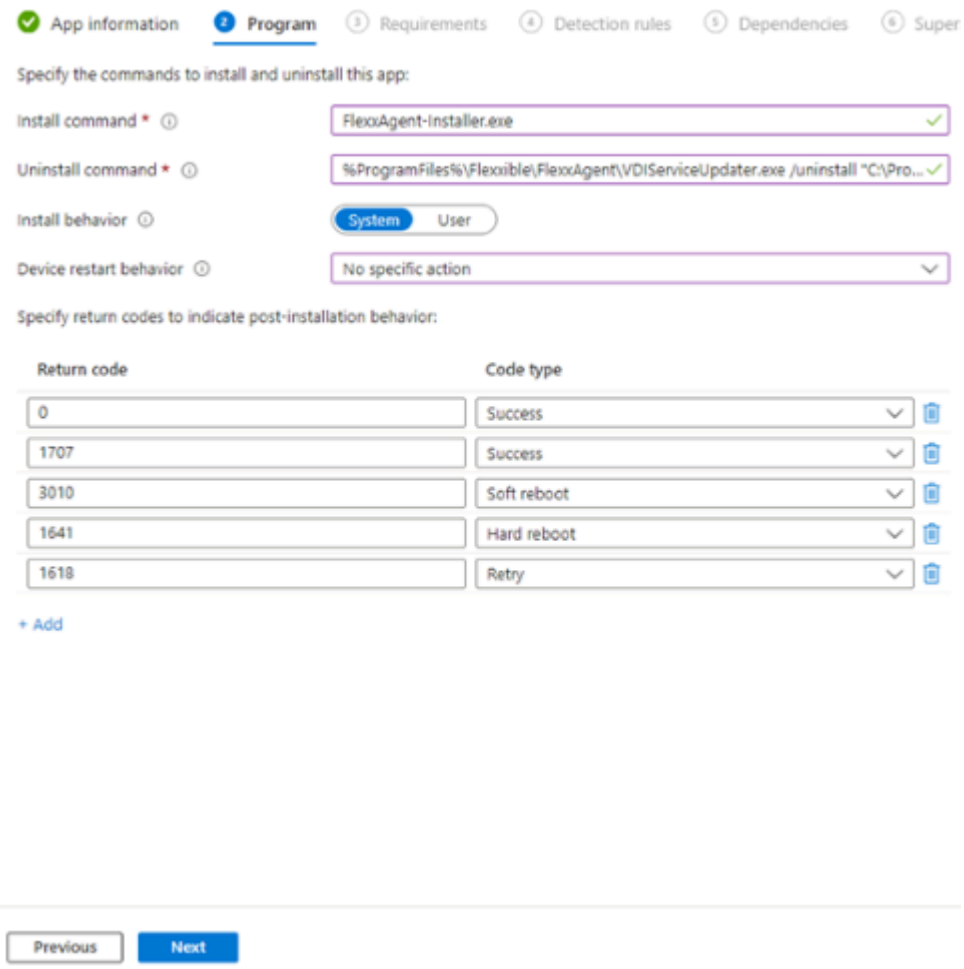
    - Install command: `FlexxAgent-Installer.exe`

> Note: If necessary, proxy values could be entered in this command.

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

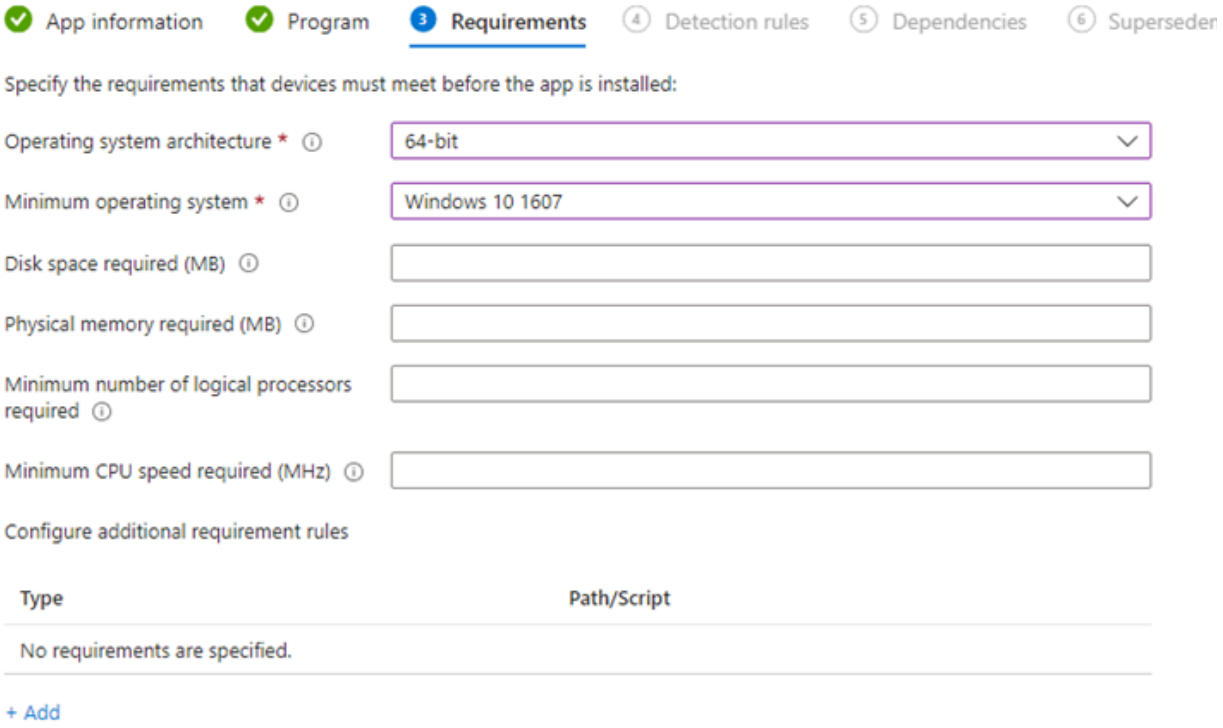
> Note: Double quotes are mandatory.

    - Install behavior: System
    - Device restart behavior: No specific action



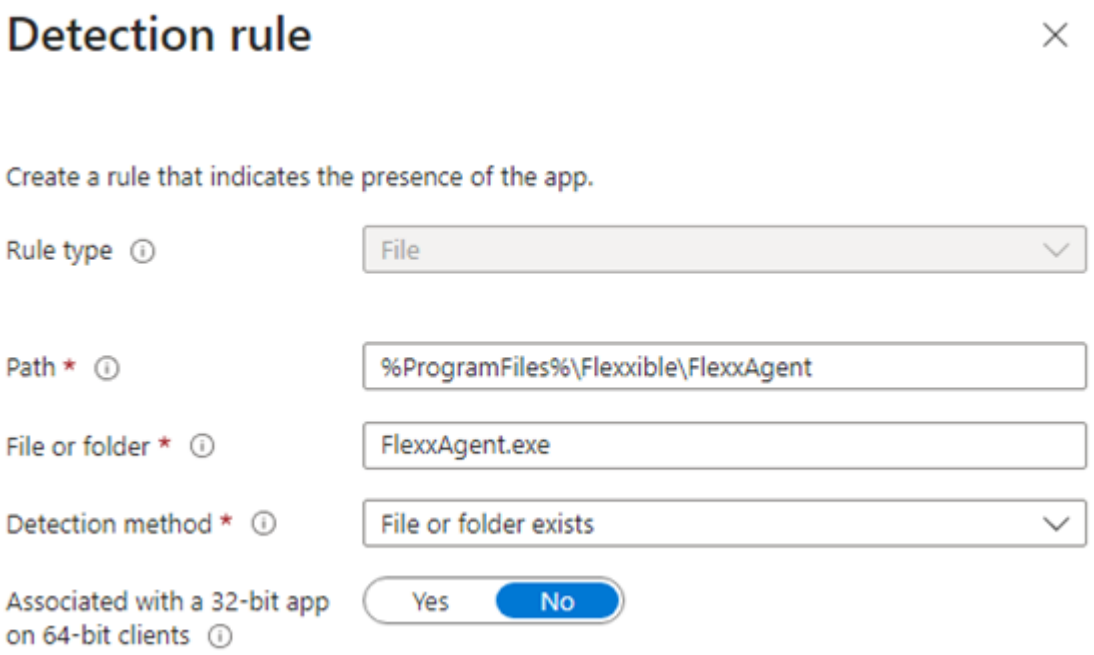
13. On the `Requirements` tab, you need to include information about the operating system architecture:

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

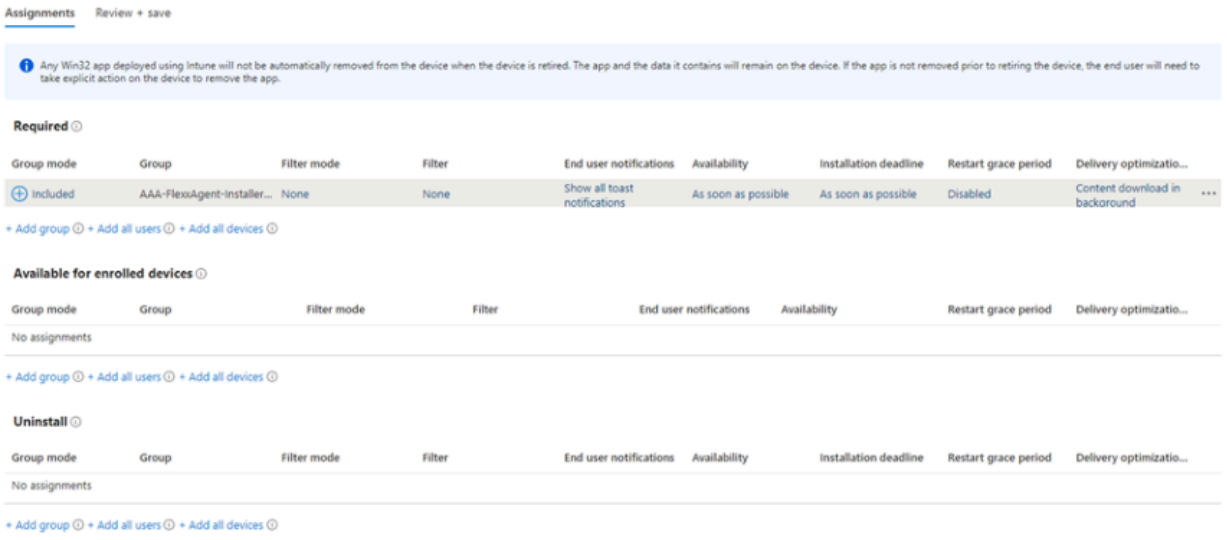


14. On the `Detection Rules` tab, select `Manually configure detection rules` and click on the link `+Add`. In the rule you are going to create, fill in the following fields:

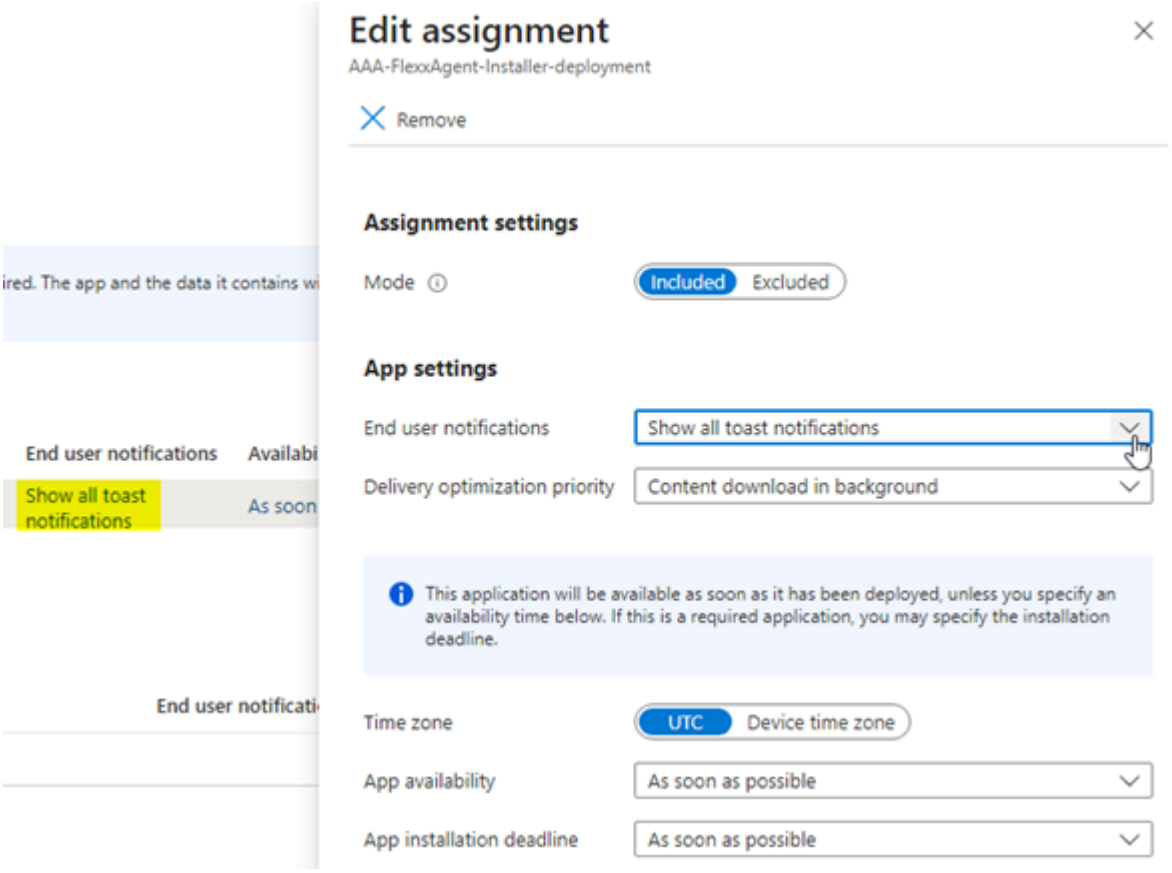
    - Rule type: File
    - Path: %ProgramFiles%\Flexxible\FlexxAgent
    - File or folder: FlexxAgent.exe
    - Detection method: File or folder exists
    - Associated with a 32-bit app on 64-bit clients: No



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

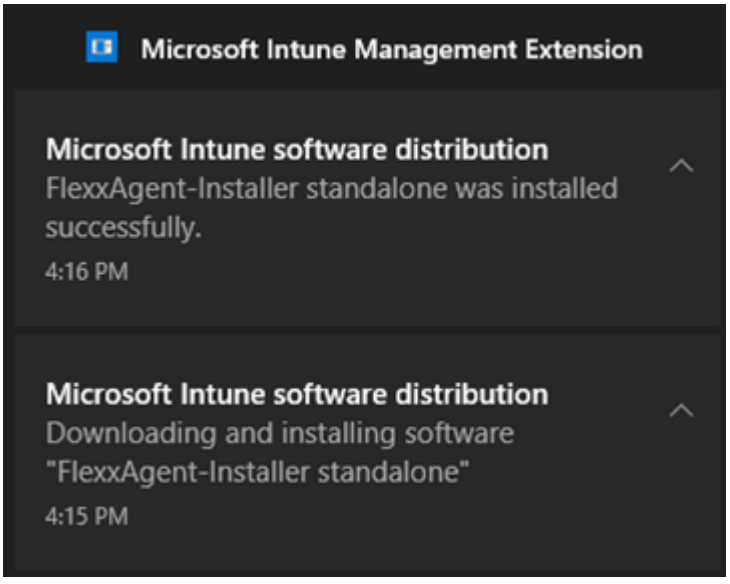


16. At this point, make sure to select the appropriate notification for the end user.



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 / Deploy FlexxAgent for Android with Microsoft Intune

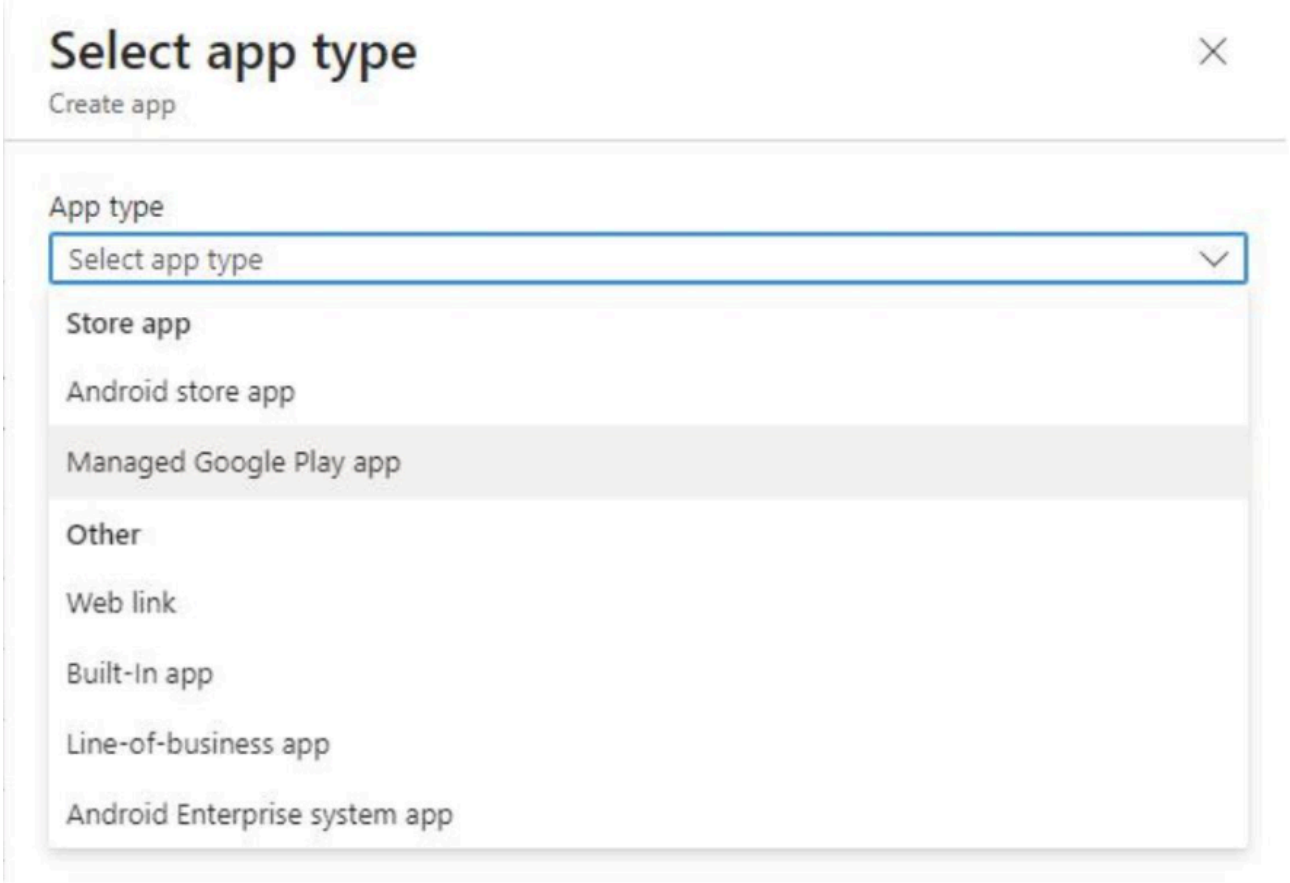
To deploy FlexxAgent on Android devices with Microsoft Intune, the latter must have an active connection with Android Enterprise. The linkage should be established by following this procedure.

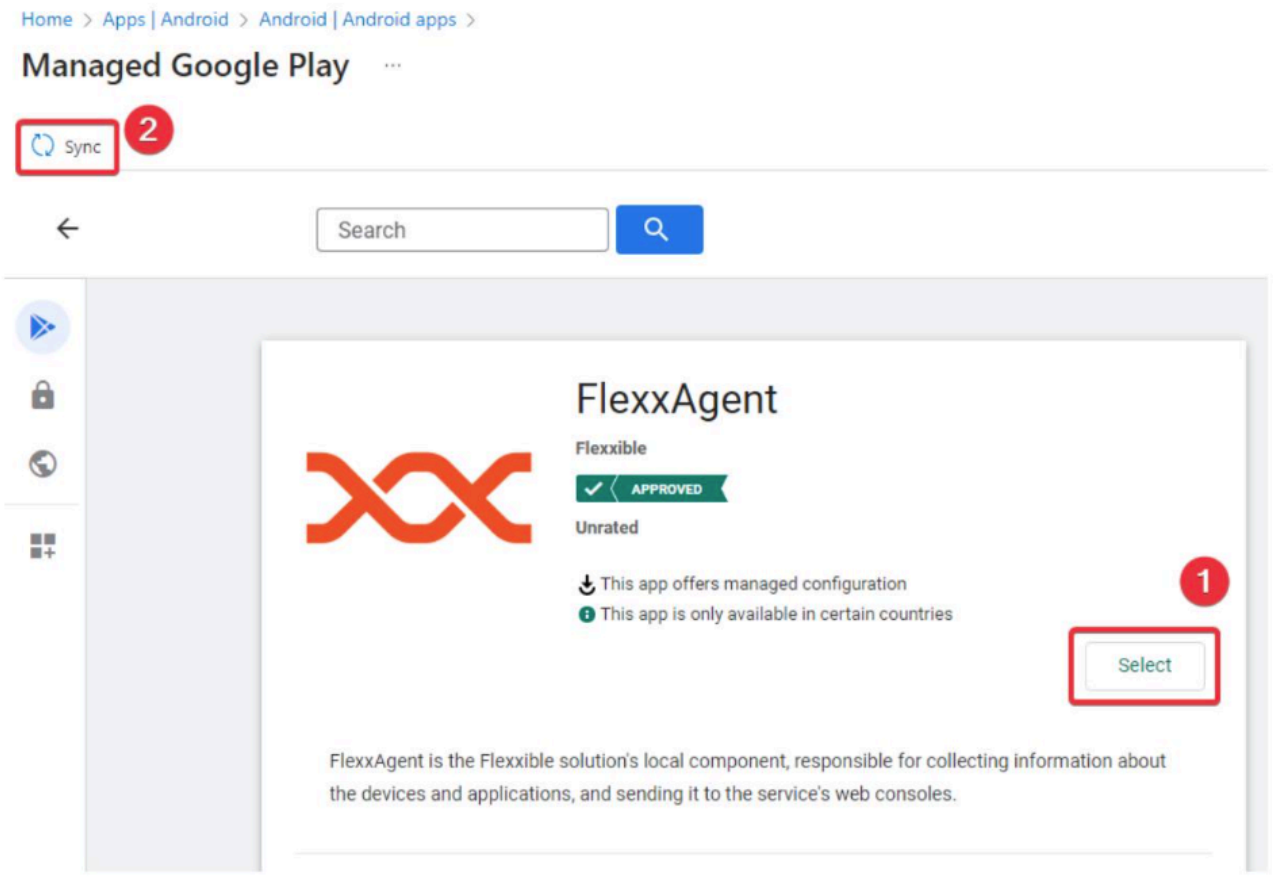
Activate app visibility in Google Play

Flexxible will provide access to FlexxAgent in the Managed Google Play console, along with the necessary configuration data. For this, the client must provide Flexxible with the *Name* and *ID* of their Managed Google Play.

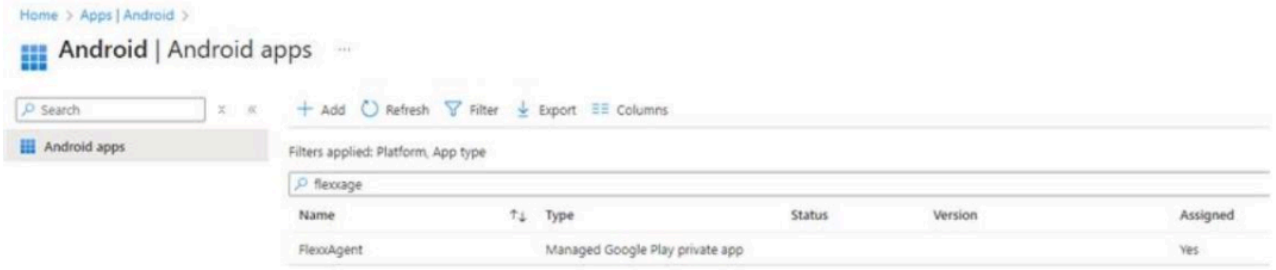
App configuration in Microsoft Intune

1. Select the app and sync it:

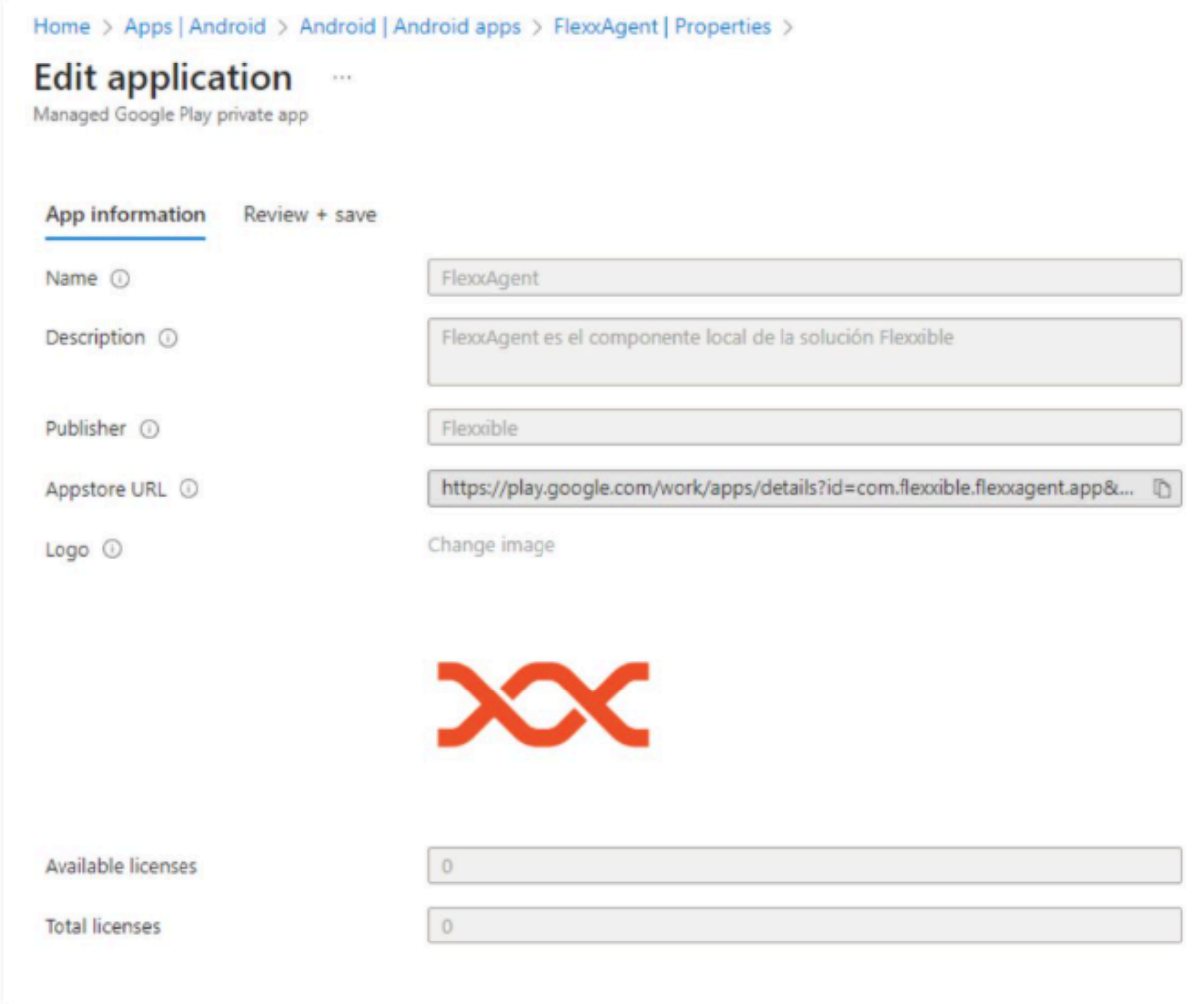




2. FlexxAgent will appear in the app list:

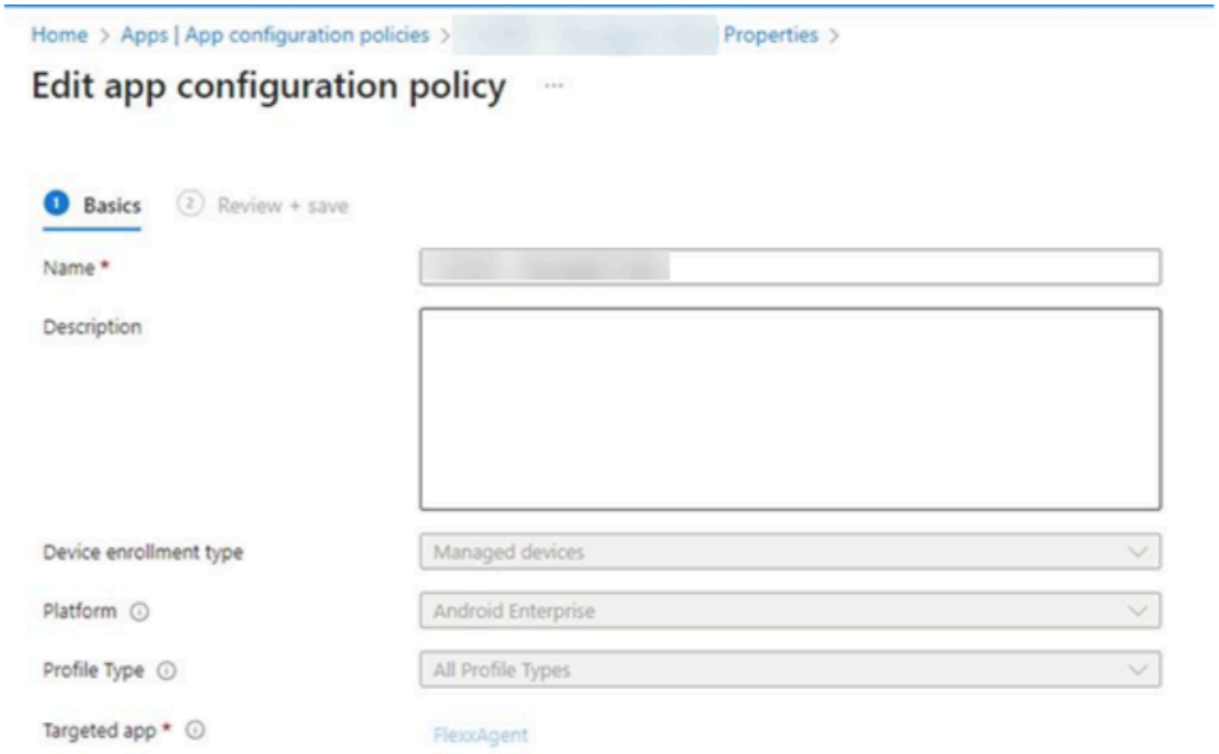


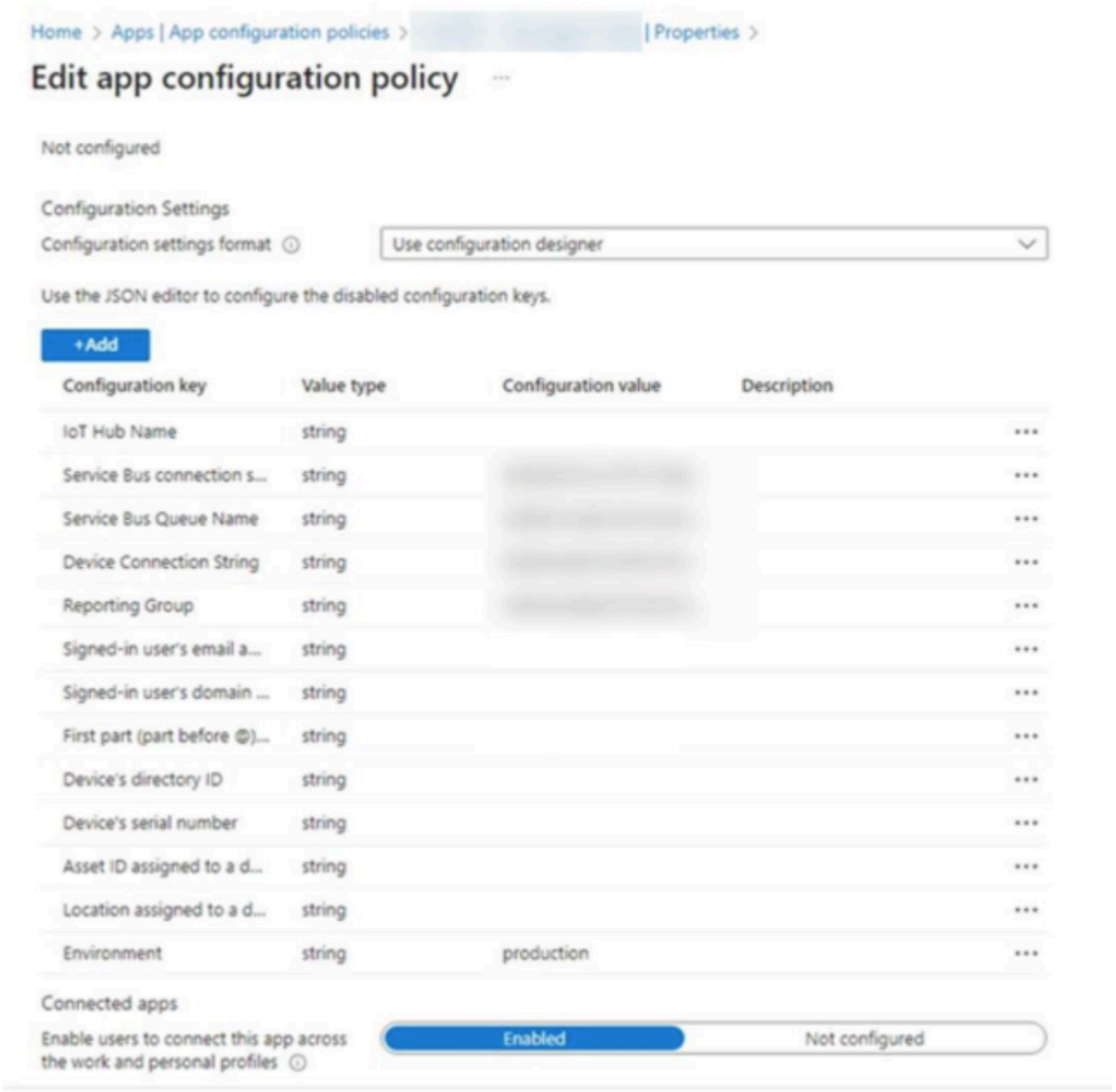
3. Configure the app:



Configuration policy management

Managing a configuration policy in Microsoft Intune will send the necessary data for the proper functioning of FlexxAgent.



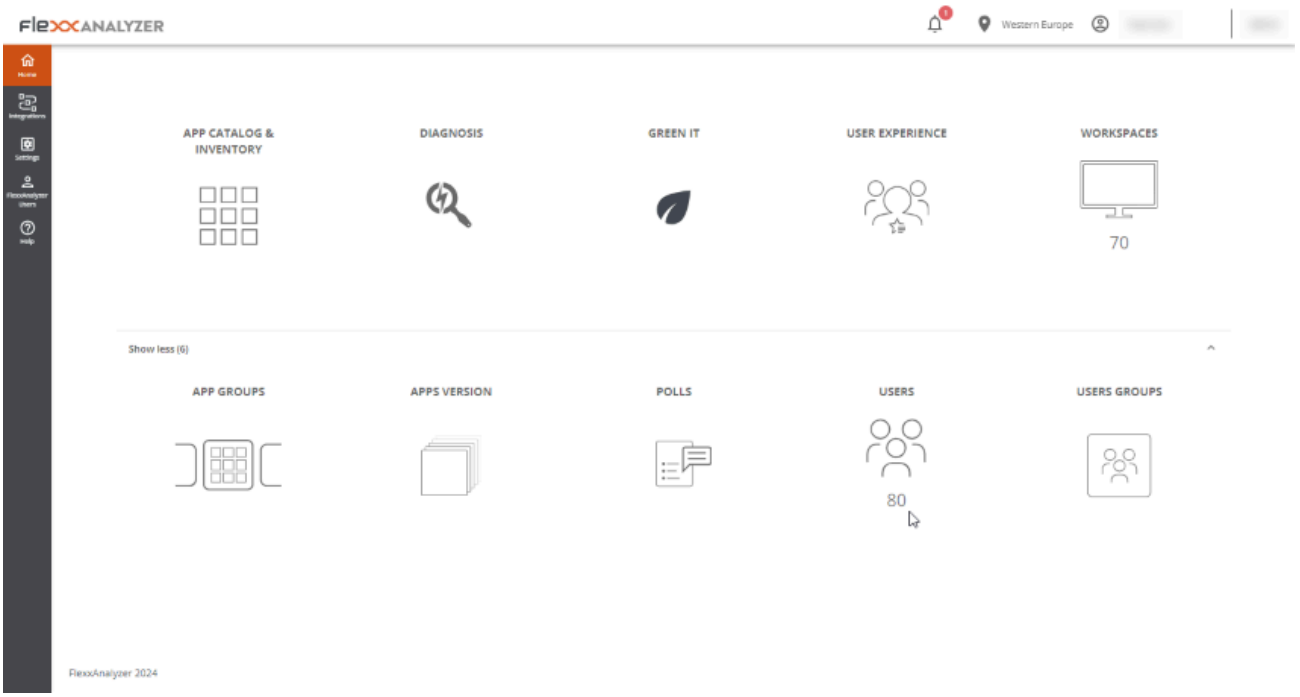


INFO

For more information about FlexxAgent for Android, please refer to its documentation.

Analyzer

Analyzer is a comprehensive solution for managing the 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:

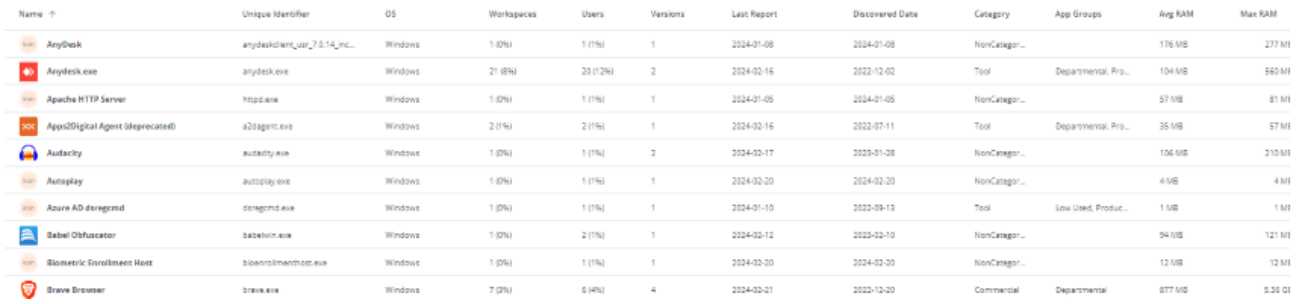
- **App Catalog & Inventory.** Offers an inventory of applications and their versions within the organization.
- **Diagnosis.** Enables a diagnostic view and allows you to see the details of resource and application usage by devices in configurable time slots.
- **Green IT.** Allows evaluating the carbon footprint generated by printing and the electrical consumption of devices and their peripherals.
- **User experience.** Helps detect and solve problems by analyzing device performance and user sentiment.
- **Workspaces.** Offers an inventory view of the 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 applications with more versions over time.
- **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 the detected users and for each one details the applications and devices used historically.
- **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.

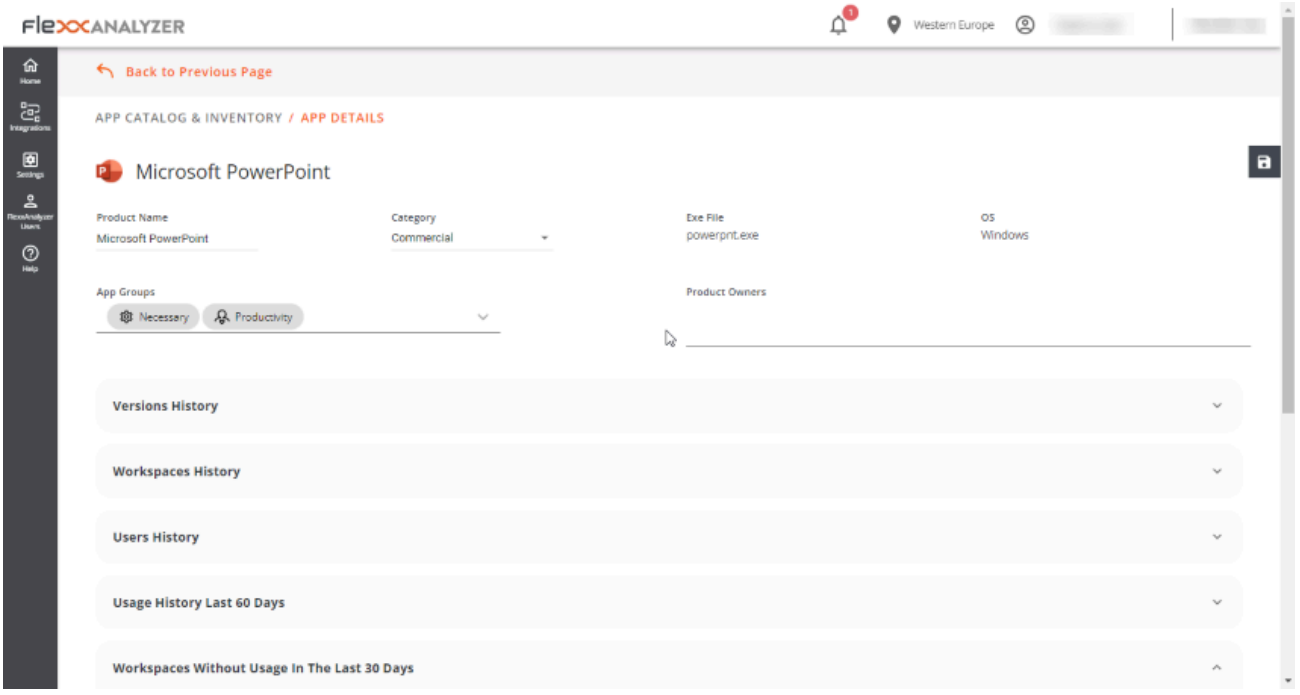
Results will appear in a list format, where you can make use of filters or navigate between different result pages.



Name	Unique Identifier	OS	Workspaces	Users	Versions	Last Report	Discovered Date	Category	App Groups	Avg RAM	Max RAM
AnyDesk	anydeskclient_usr_7.0.14_inc...	Windows	1 (0%)	1 (1%)	1	2024-01-08	2024-01-08	NonCategor...		176 MB	277 MB
Anydesk.exe	anydesk.exe	Windows	21 (8%)	20 (12%)	2	2024-02-16	2022-12-02	Tool	Departmental, Pro...	104 MB	560 MB
Apache HTTP Server	httpd.exe	Windows	1 (0%)	1 (1%)	1	2024-01-05	2024-01-05	NonCategor...		57 MB	81 MB
Apps2Digital Agent (deprecated)	a2dagent.exe	Windows	2 (1%)	2 (1%)	1	2024-02-16	2022-07-11	Tool	Departmental, Pro...	35 MB	57 MB
Audacity	audacity.exe	Windows	1 (0%)	1 (1%)	2	2024-02-17	2023-01-28	NonCategor...		106 MB	210 MB
Autoplay	autoplay.exe	Windows	1 (0%)	1 (1%)	1	2024-02-20	2024-02-20	NonCategor...		4 MB	4 MB
Azure AD dsregcmd	dsregcmd.exe	Windows	1 (0%)	1 (1%)	1	2024-01-10	2022-09-13	Tool	Low Used, Produc...	1 MB	1 MB
Babel Obfuscator	babelwin.exe	Windows	1 (0%)	2 (1%)	1	2024-02-12	2023-02-10	NonCategor...		94 MB	121 MB
Biometric Enrollment Host	bioenrollmenthost.exe	Windows	1 (0%)	1 (1%)	1	2024-02-20	2024-02-20	NonCategor...		12 MB	12 MB
Brave Browser	brave.exe	Windows	7 (3%)	6 (4%)	4	2024-02-21	2022-12-20	Commercial	Departmental	877 MB	5.36 GB

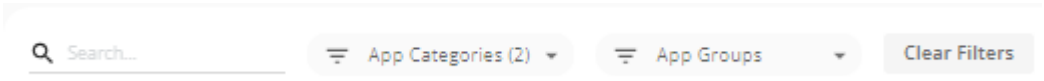
Detail Views

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.



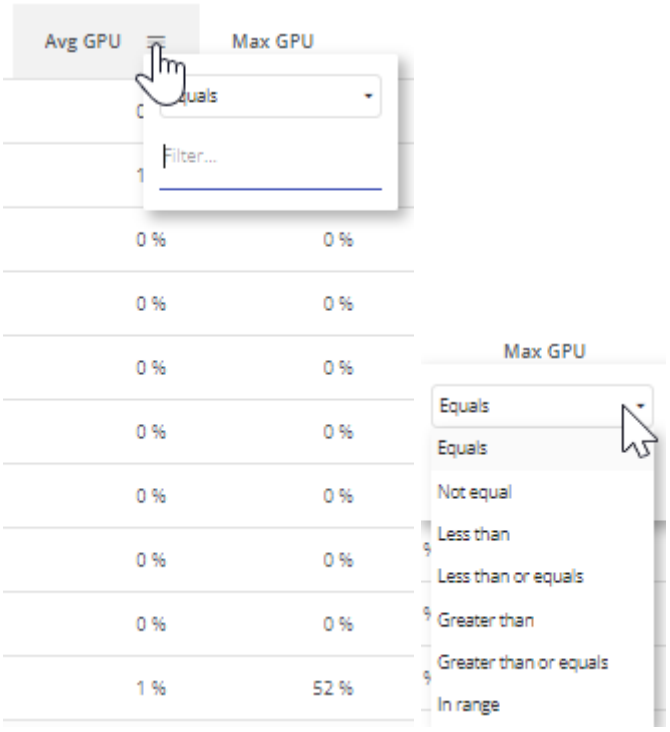
Search options

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.



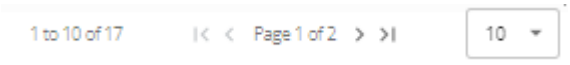
Logical operators that can be operated with:

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.

Condition	Caption
Greater or equal to	The condition for filtering results must be greater than or equal to the value stated.
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.

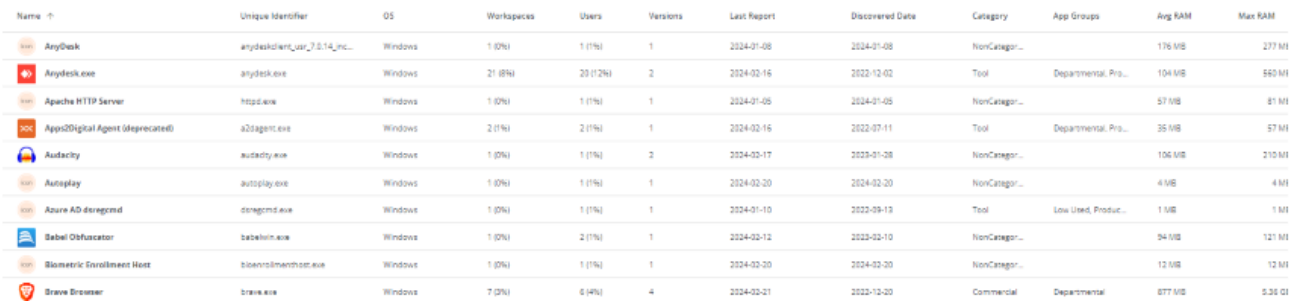
Page navigation

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 **App Catalog & Inventory** you can see a list of all 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.



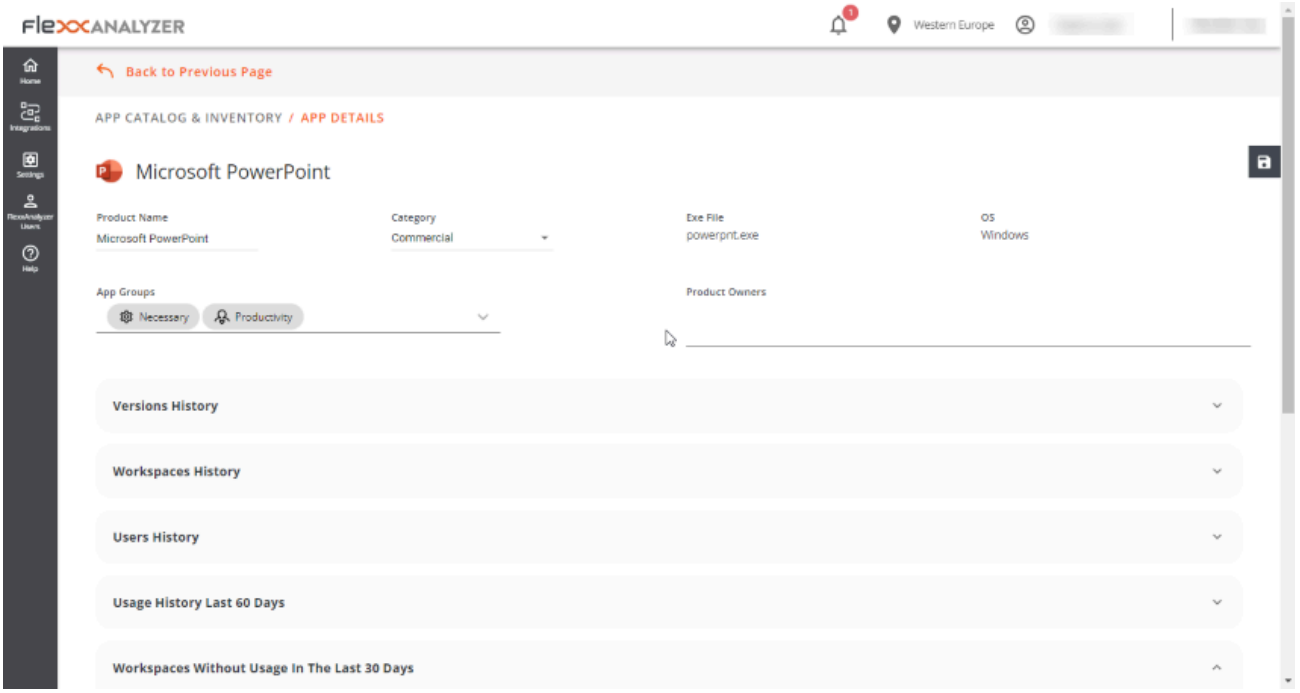
List view

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 the last recorded 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 where the execution of this application was recorded.
- Workspace. Device where the execution of this application was recorded.
- Days. Number of days, within the last 60, the application was detected running in this user session.
- Last Report. Date of the last recorded report in the user session.

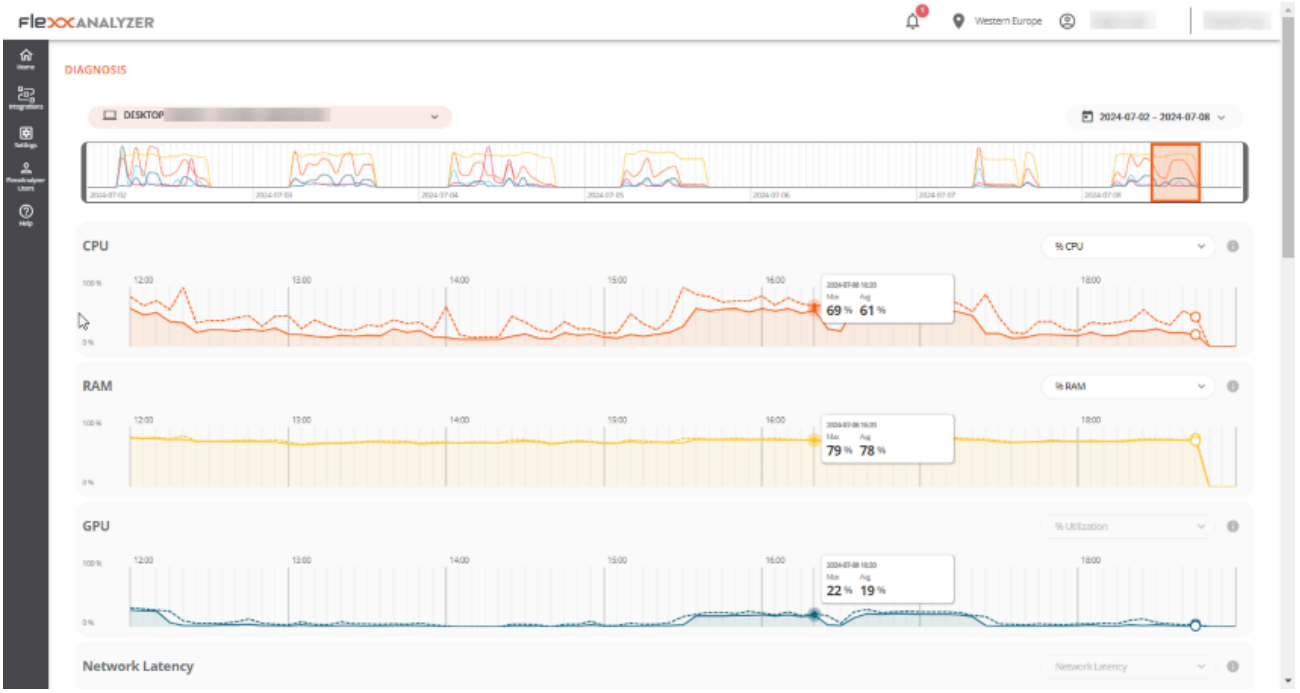
Workspaces without usage in the last 30 days

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

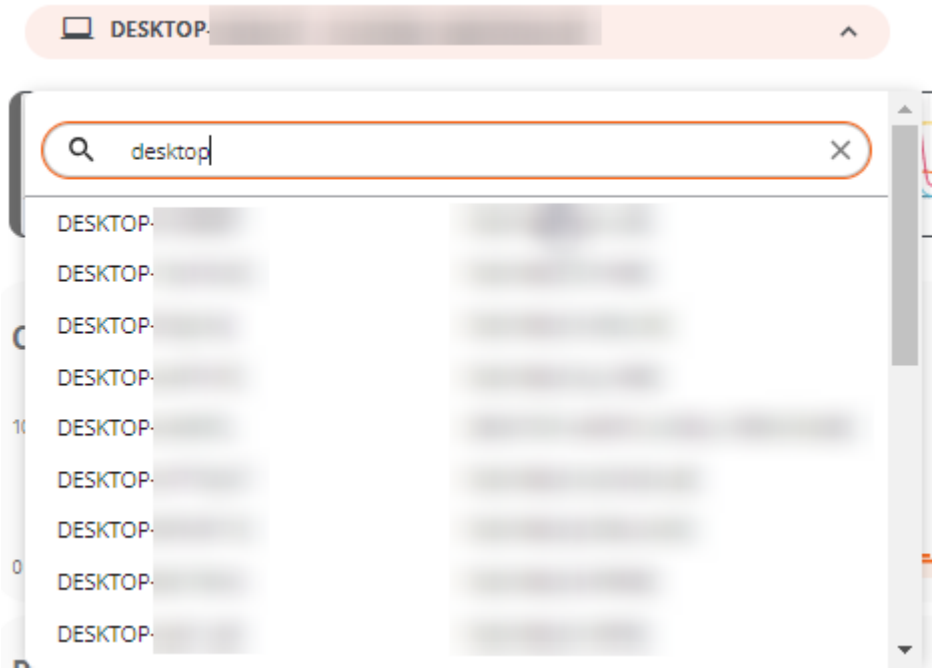
Analyzer / Diagnosis

From **Diagnosis**, 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.



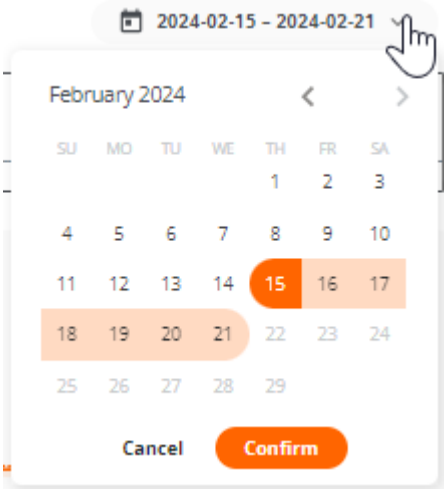
Web Interface

The **Diagnosis** dropdown menu allows searching for a device and the user's 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.** Total CPU usage on the system, equivalent to what the task manager shows.
- **% User Time.** Percentage of CPU time used by applications and processes running in user mode.
- **% Privileged time.** Percentage of CPU time used by the operating system and system services in privileged mode.
- **% Processor time.** Total CPU time used in all system processes and activities.

RAM

- **% RAM.** Total memory usage on the system, equivalent to what the task manager shows.
- **Available RAM.** Amount of free memory in the system to run new applications without causing performance issues.
- **Committed MB.** Amount of virtual memory actively used by running processes and applications.

GPU

- **% utilization.** Total GPU usage on the system, equivalent to what the task manager shows.

Network Latency

- **Network Latency.** Shows the system latencies.

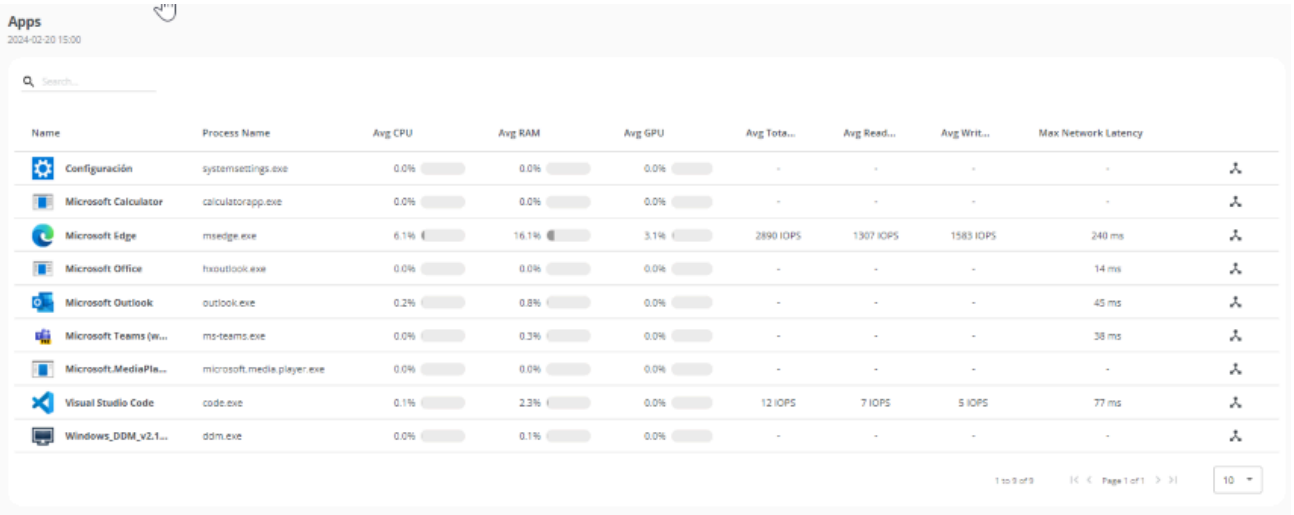
Disk Usage

- **Total IOPS.** Total IOPS (input/output operations per second) generated by 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 is an approach that aims 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.

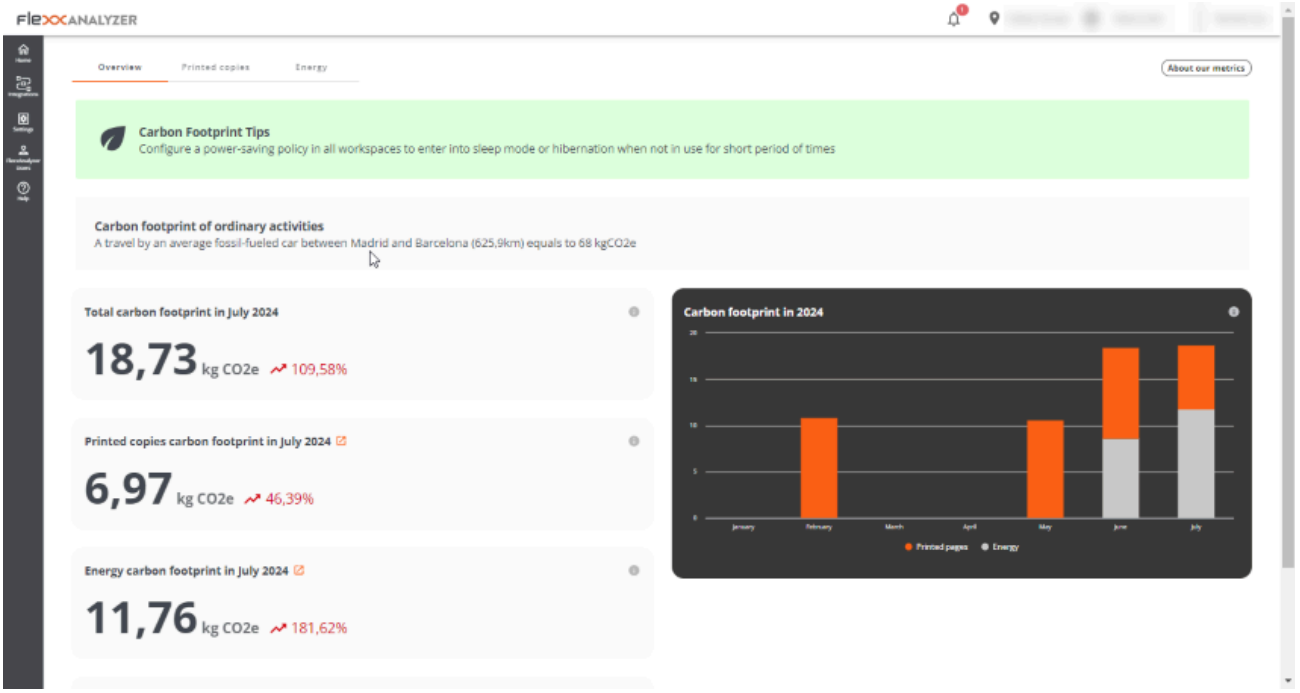
Web Interface

This dashboard view is divided into three tabs:

- **Overview.** Unified data of the entire carbon footprint generated.
- **Printed copies.** Shows information about monthly prints in the organization, in black and white or color, as well as metrics of the users and printers generating the most prints.
- **Energy.** Shows energy consumption generated by the use of devices and their peripherals, as well as data on radioactive waste resulting from energy generation.

> **INFO**
>
> Carbon footprint data for electrical consumption and printing are only recorded for physical devices, not for virtual ones.

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

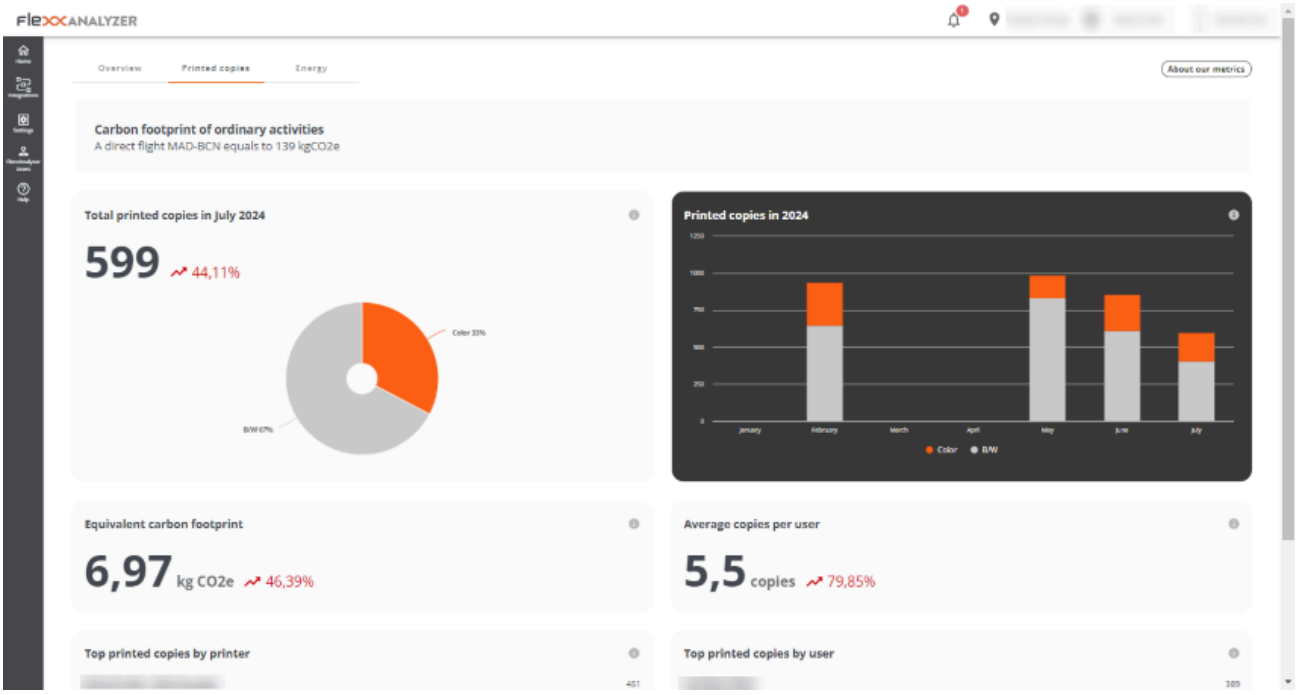
Printed copies

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.

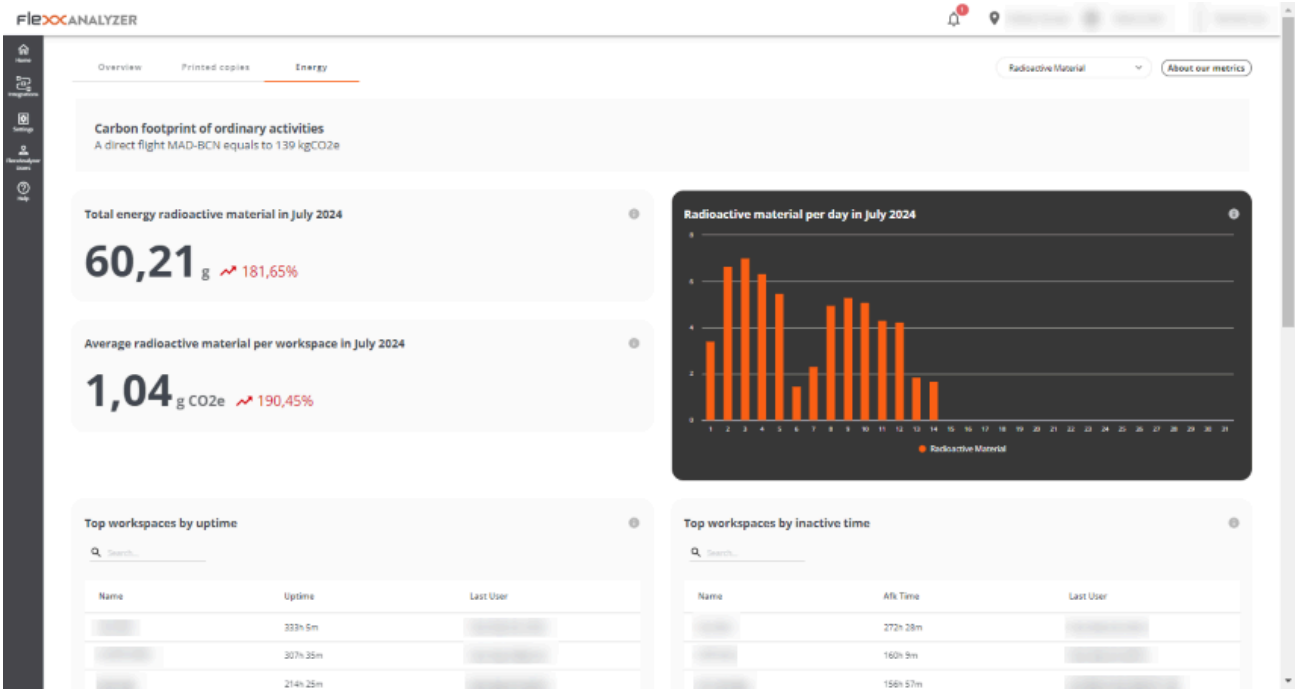
The carbon footprint of the printed copies is calculated using the following estimates:

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



- **Total printed copies in [current month].** Displays short-term paper usage trends. Helps identify areas of intensive use, as well as opportunities to reduce the number of prints or promote duplex printing.
- **Equivalent carbon footprint.** 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.** View of printers sorted by the number of prints in the current month.
- **Printed copies in [Current year].** View of the total black and white and color prints made month by month during the current year.
- **Average copies per user.** Average prints per user in the current month.
- **Top printed copies by user.** List of users sorted by the 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.

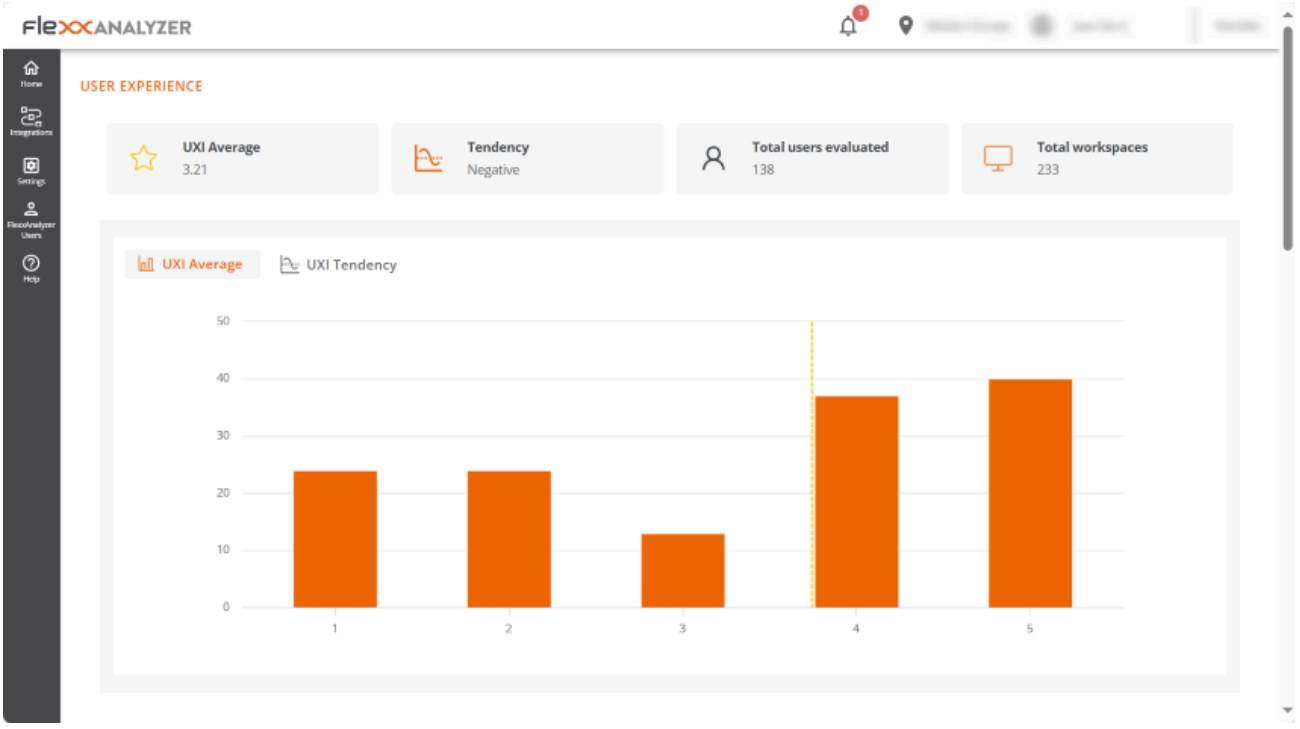
Radioactive material

- **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 workstation in the current month.
- **Radioactive material per day in [Current month].** Graph estimating 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 generating 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 generating the most radioactive material while 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 the digital ecosystem of their organization. This includes evaluating the performance of the hardware and software they use in 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	

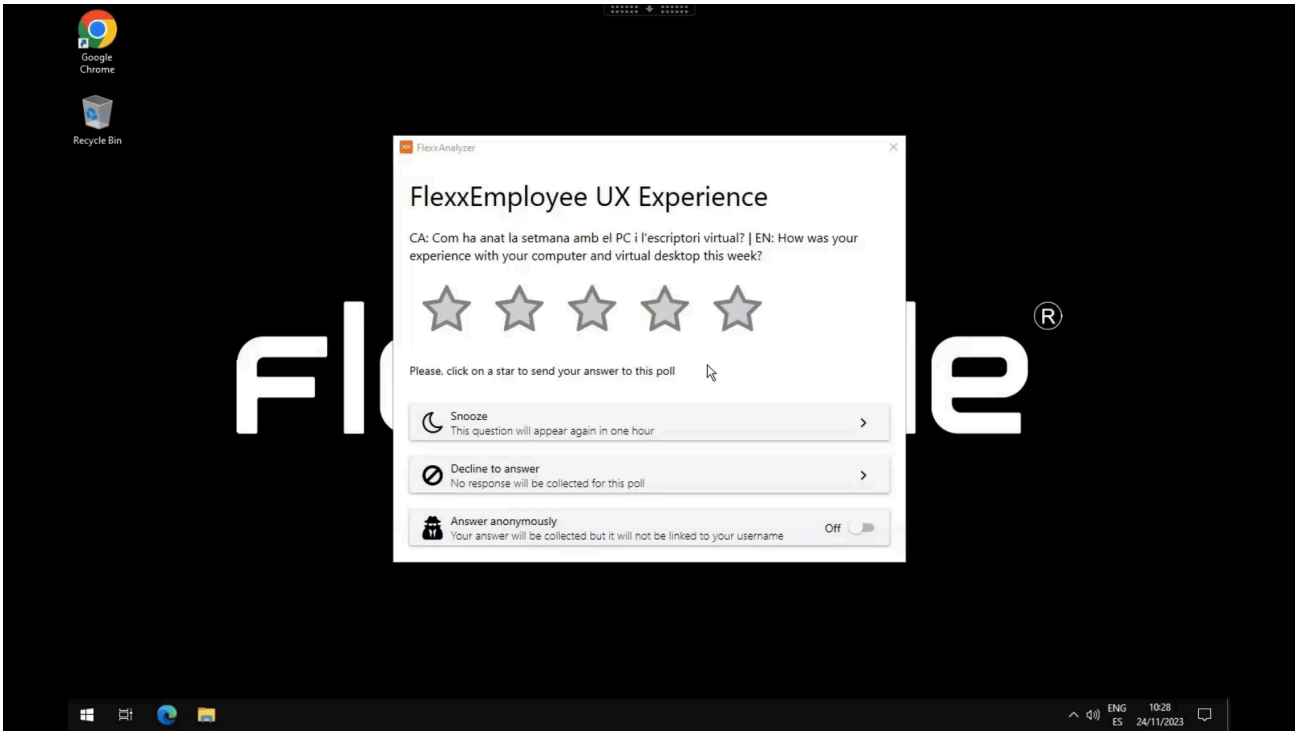
Indicator	Severity	Threshold	Recurrence	
BOOT_DURATION	HIGH	Boot duration longer than 90 seconds	Once per day	

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.



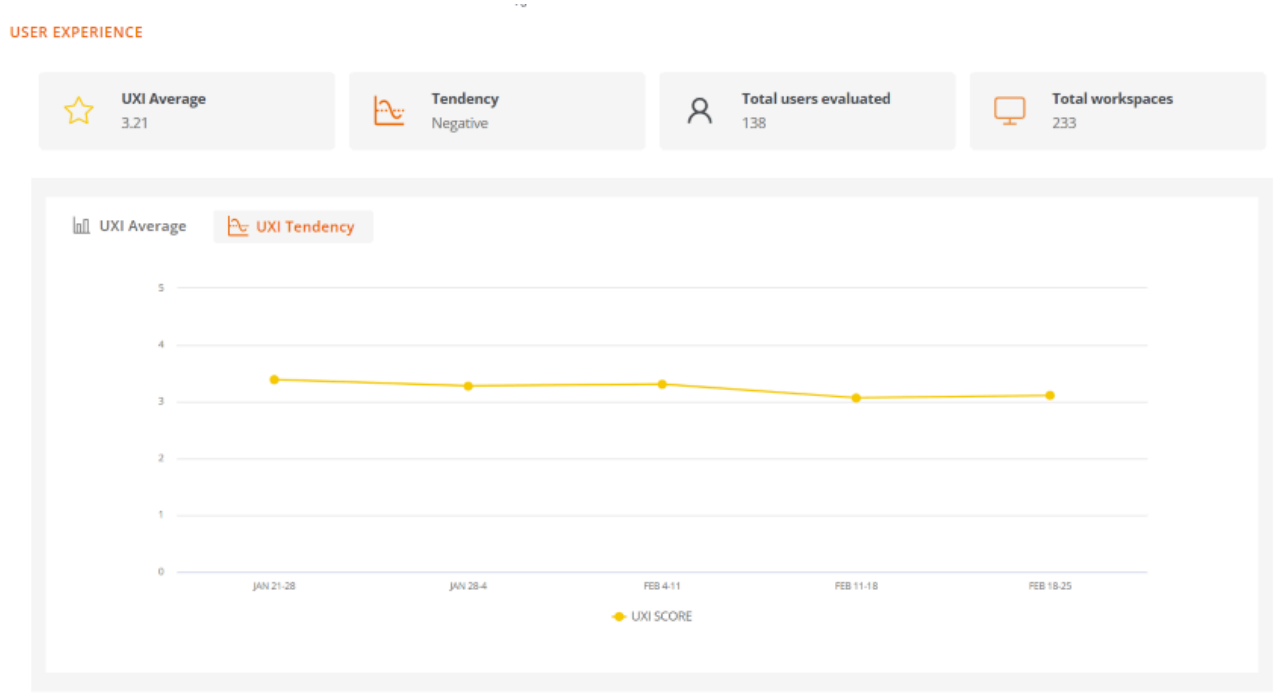
Web Interface

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.** Indicator of average experience for the entire organization. It can range from 0 to 5.
- **Tendency.** Indicator that based on the evolution of the UXI average shows whether the tendency is positive or negative.
- **Total users evaluated.** Total number of users evaluated.
- **Total workspaces.** Total number of devices evaluated.



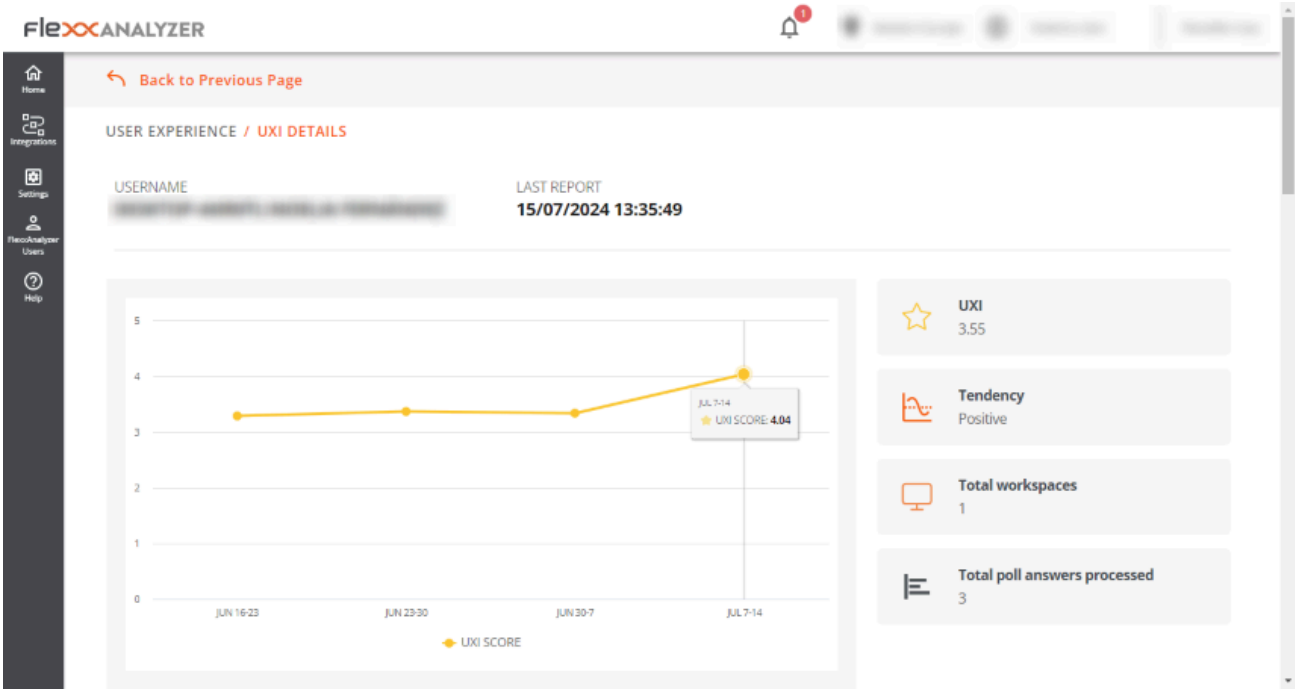
Two charts are also included:

- **UXI Average.** Shows the distribution of users by UXI level, along with the organizational average.
- **UXI Tendency.** Shows the temporal evolution of the UXI for 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:



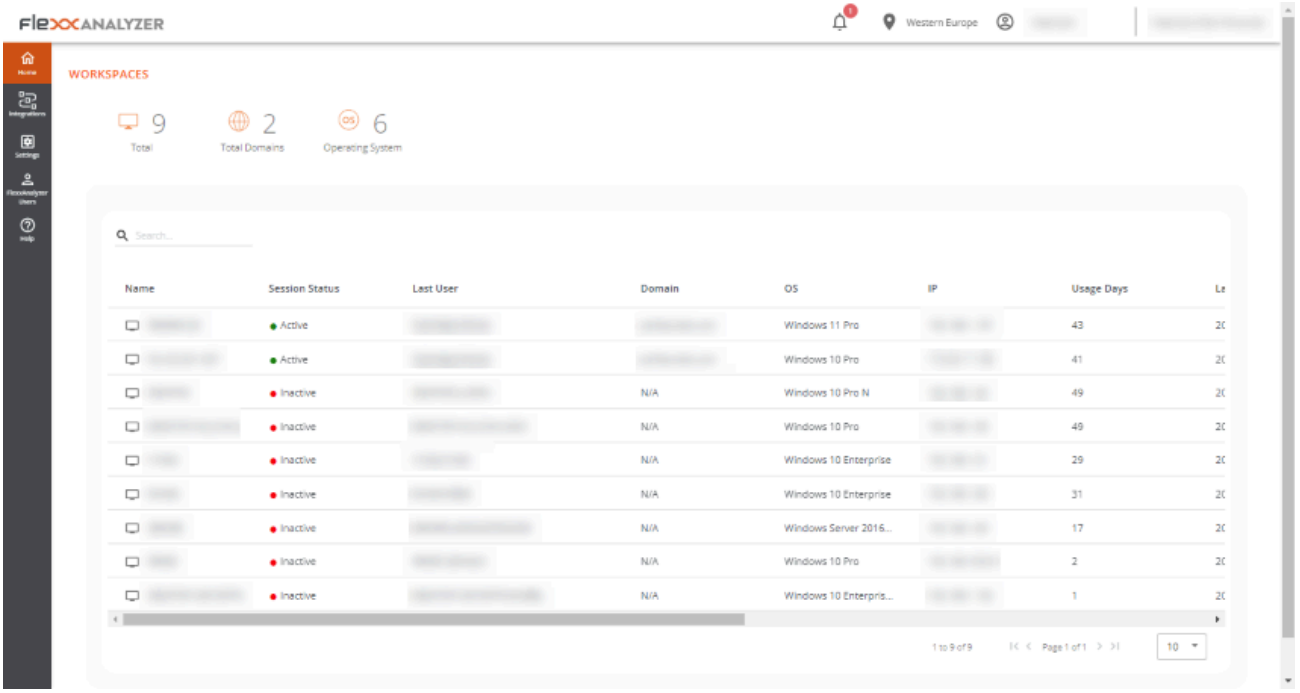
- **Username.** Username reported in the user's session.
- **Last report.** Date of the last report received for this user.
- **UXI Average.** Experience indicator for the user; can range between 0 and 5.
- **Tendency.** Indicator that, based on the evolution of the user's UXI average, shows whether the user's trend is positive or negative.
- **Total workspaces.** Number of devices the user has worked on.
- **Total poll answers processed.** Number of surveys the user has responded to and are considered in this evaluation.

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

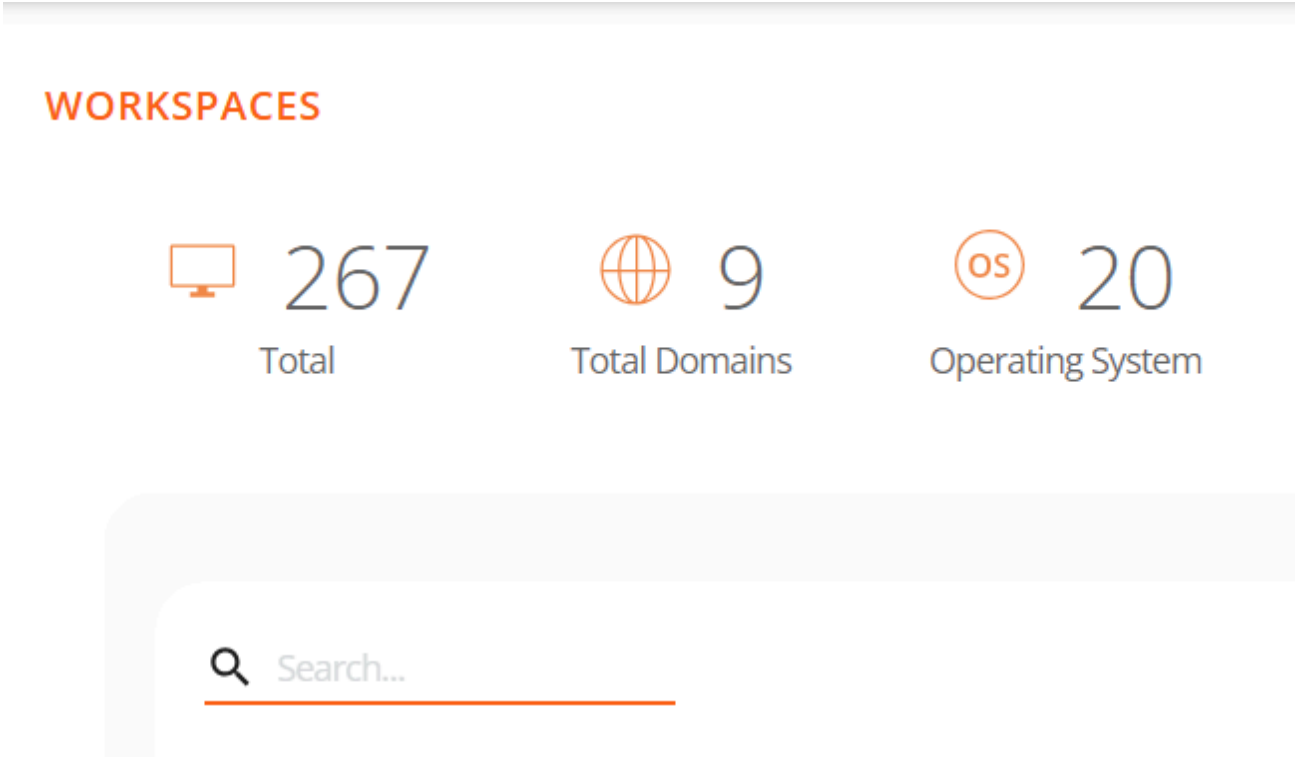
- **Polls in the last 30 days.** Surveys answered by the user in the last 30 days. The detail of this view offers the user's survey scores compared to the organization's average for the same period.
- **Workspaces in the last 30 days.** Provides a table containing all devices the user worked on in the last 30 days, as well as the number of times worked on each, the operating system, and the WRI indicator for each.
- **Issues in the last 30 days.** Shows the list of problems detected on the devices used by the user in the last 30 days, along with the date and score each had.

Analyzer / Workspaces in Analyzer

The list view of **Workspaces** 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.

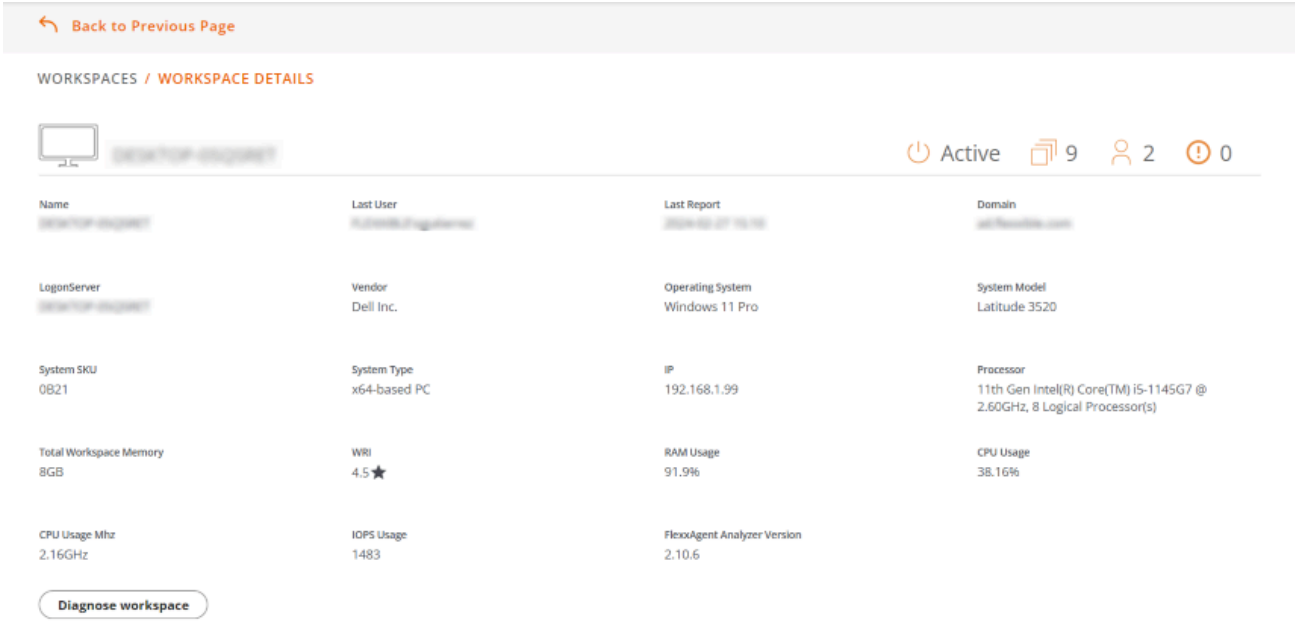


Workspace detail

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 listing, the `Diagnose workspace` button allows viewing usage data for the device, which is the same information that can be obtained in the Diagnosis section.

Device 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

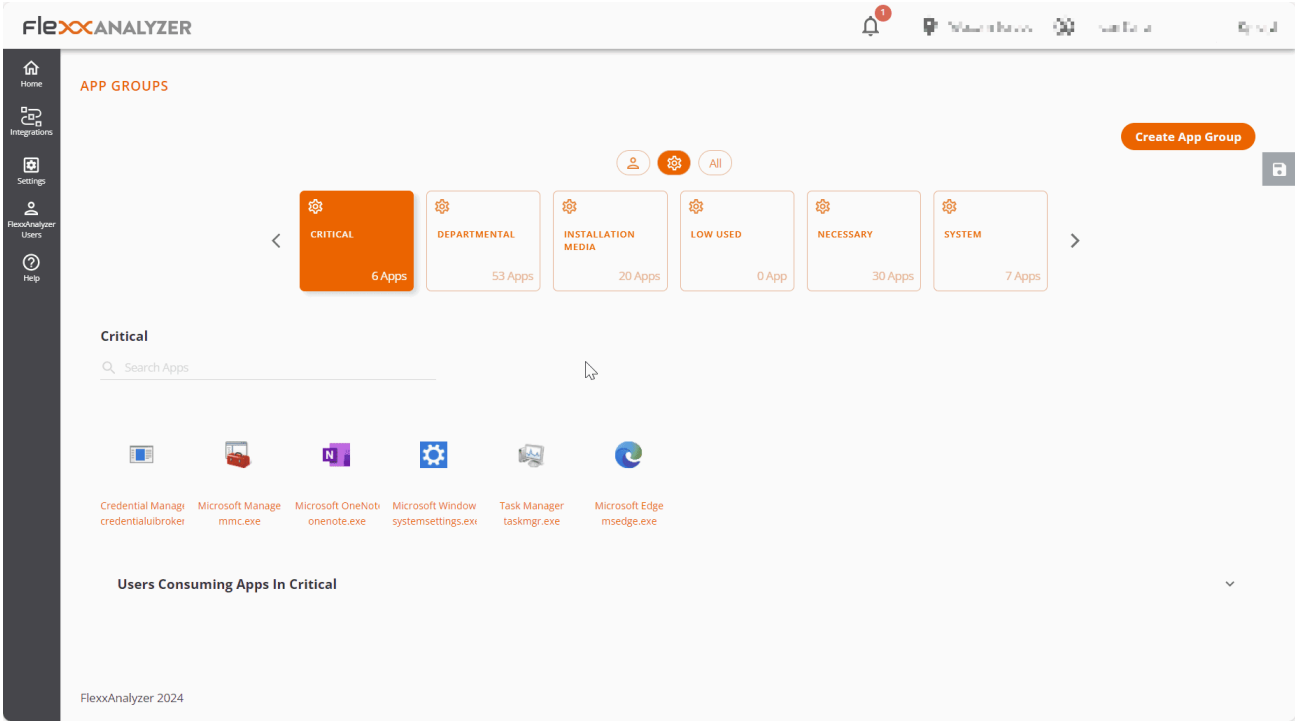
This table includes the list of alerts sent daily to Analyzer. The table reports the score deducted from the Workspace Reliability Index for each alert found on the device.

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 offers the ability to create application groups to display aggregated data on 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

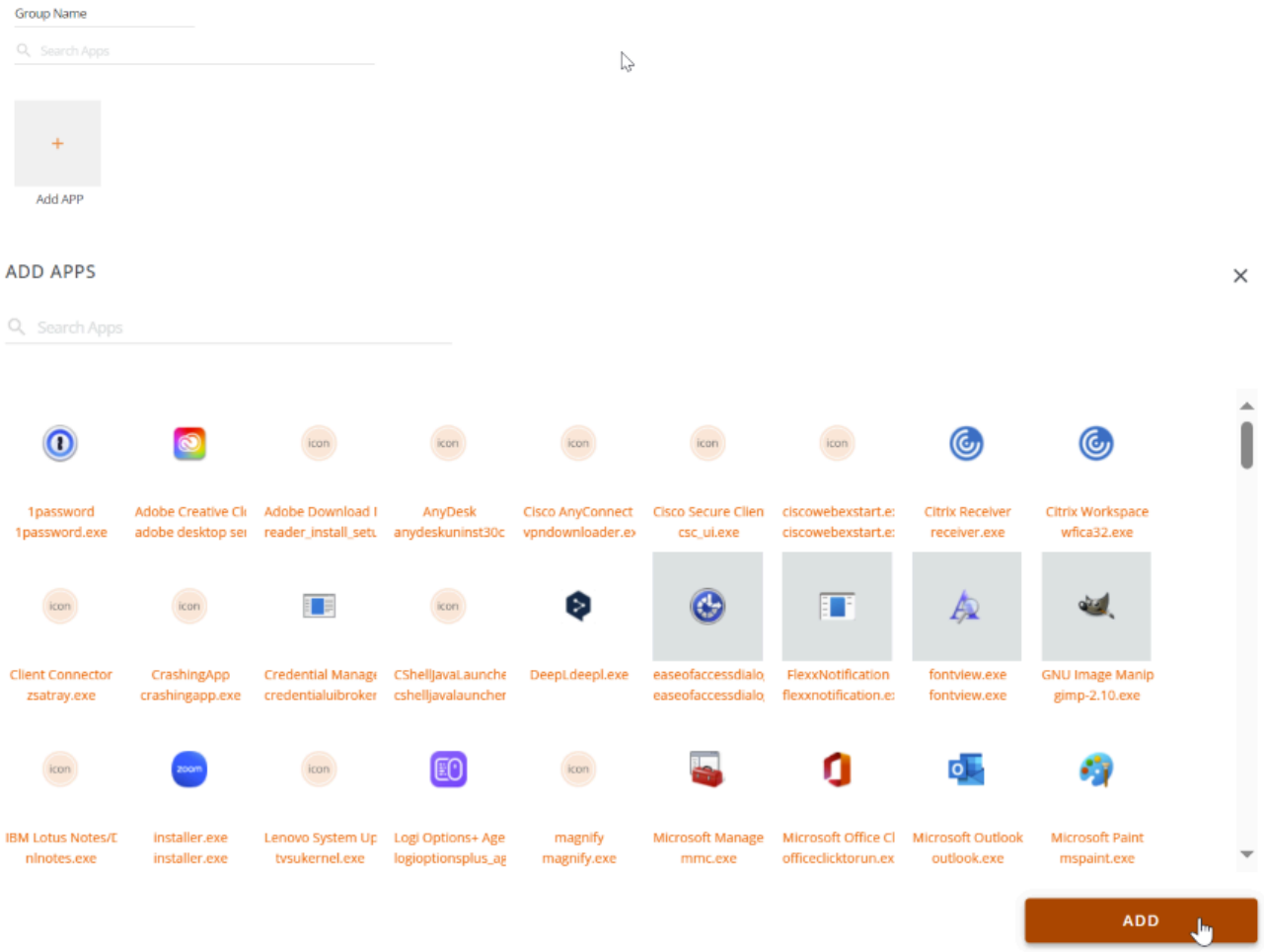
- **User App Group.** Groups manually created from the Create App Group button.
- **System App Group.** Automatically generated groups. Created by Analyzer considering the configuration assigned in the Settings option.
- **All.** Includes all groups.

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.



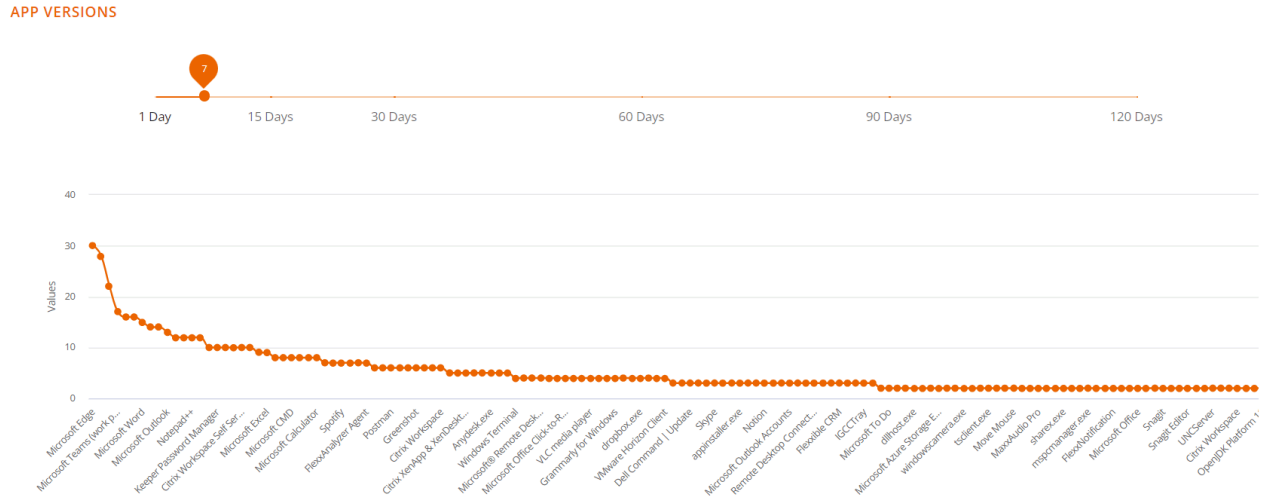
Finally, to save, click on the `Save changes` button.

Analyzer / App Versions

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

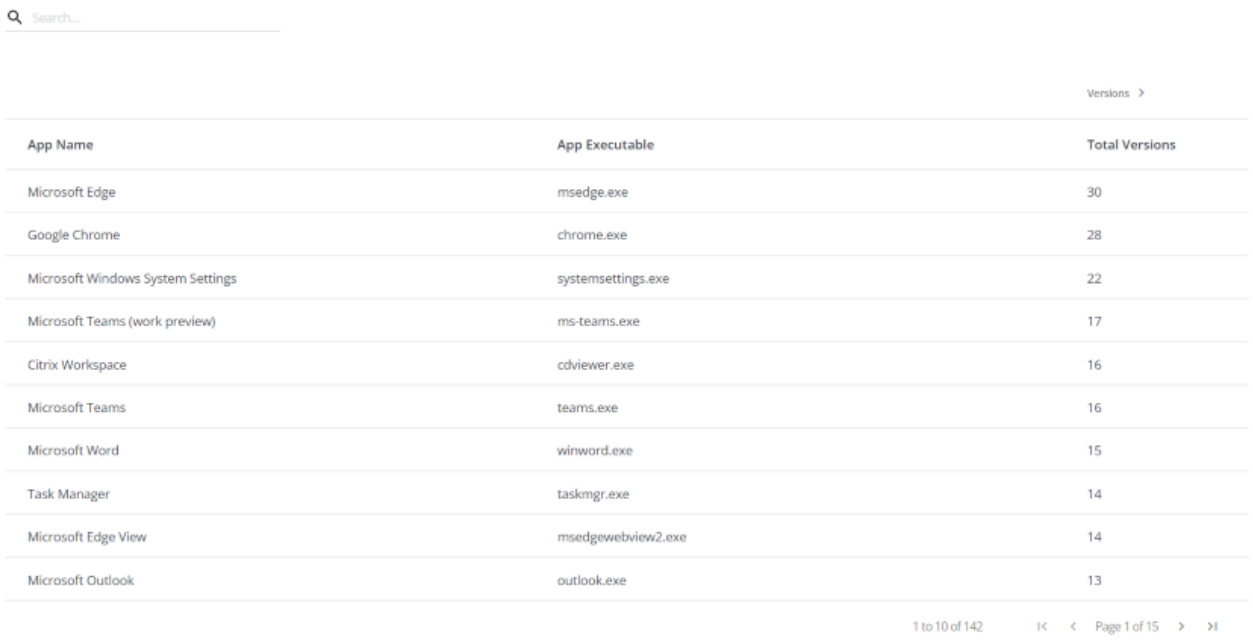
Graphical view

At the top, 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

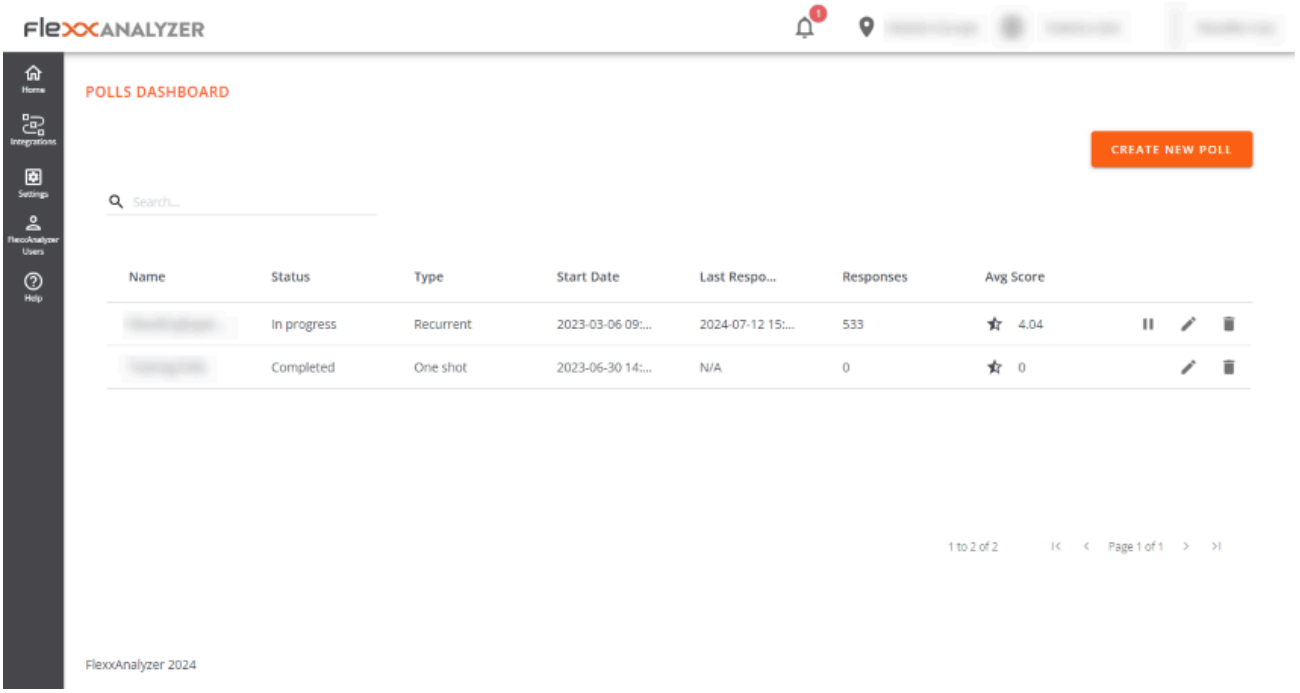
Polls allow us to get the user's sentiment or perception regarding very simple questions, trying to simplify the response mechanisms as much as possible to maximize the user response rate.

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

Polls allows you to create, modify, and delete surveys for users, schedule their execution, specify which users will receive them, and more options.

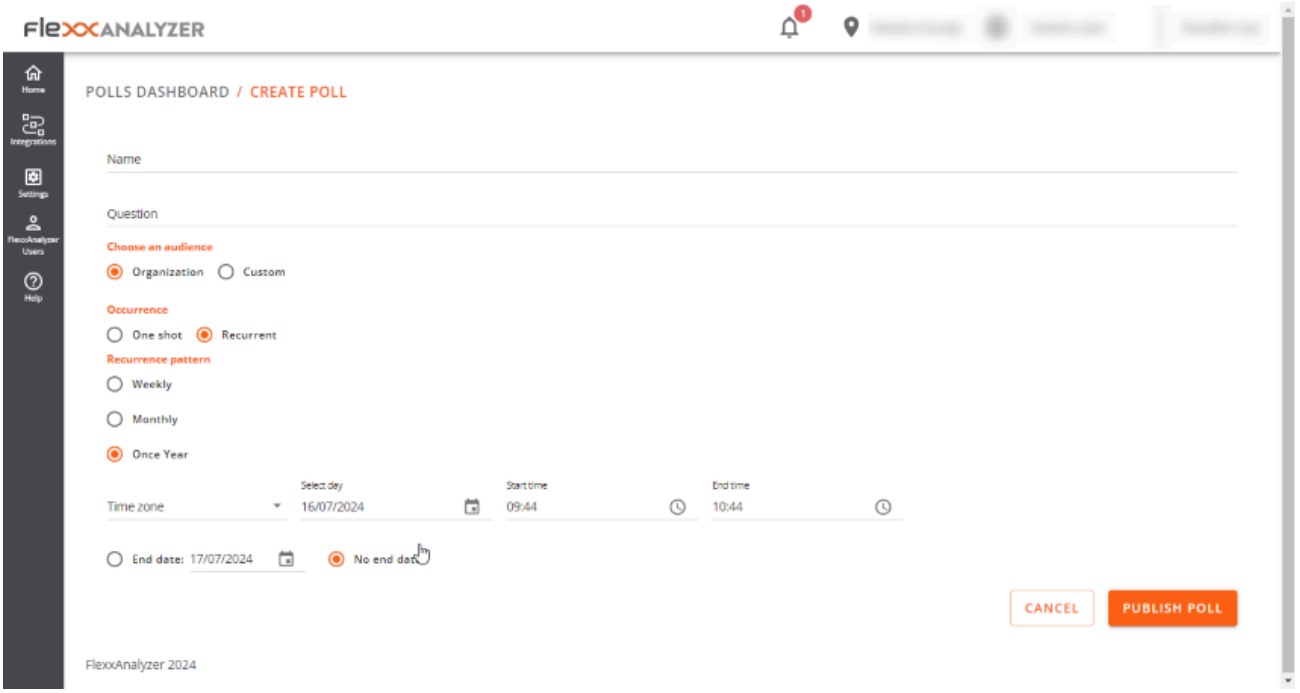
List view



By accessing the section, you can see a list of the configured surveys, 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 survey, 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.

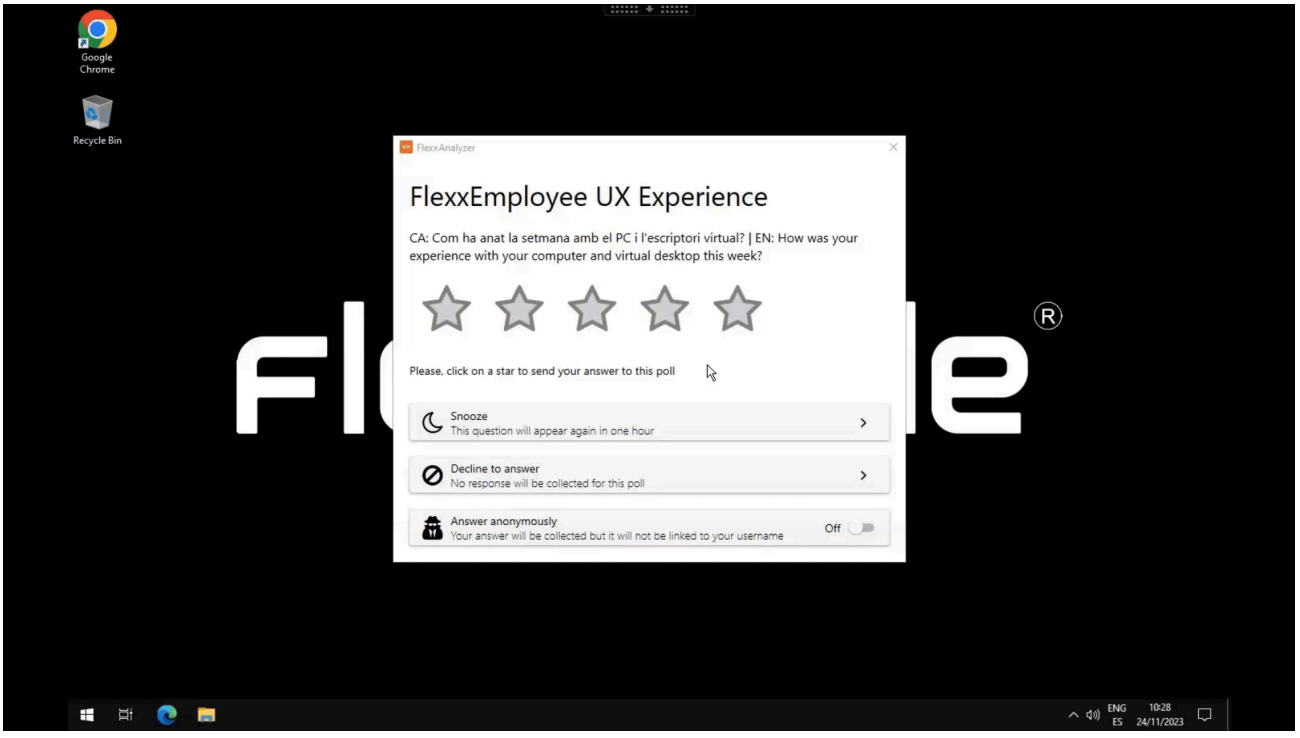
Occurrence

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

Users 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.

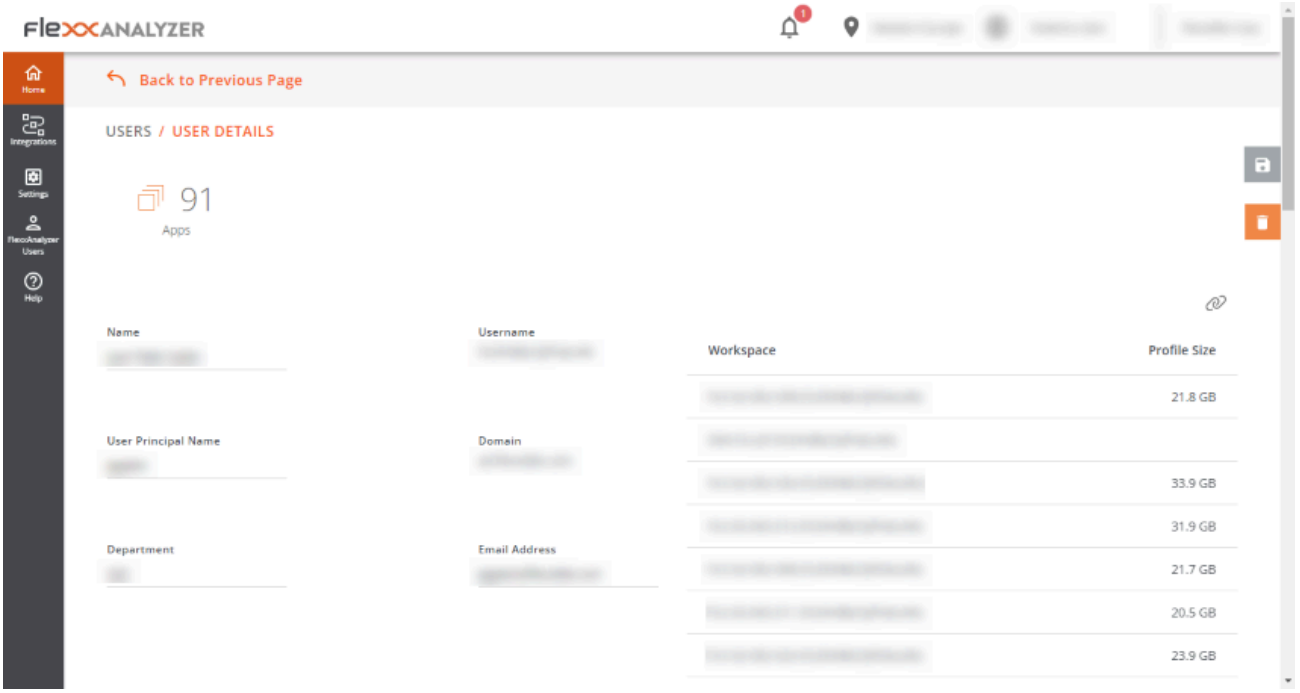
List view

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

- **Username.** Username used for login in the session.
- **Name.** User's "Display name".
- **UPN.** User Principal Name.
- **Department.** Department provided in Active Directory or Entra ID.
- **Domain.** Domain of Entra ID or Active Directory where the device resides.
- **Manager.** Manager provided for the user in Entra ID or Active Directory.
- **Usage days.** Total days the user has logged in.
- **Profile size.** Disk space occupied by the user's profile.
- **Last report.** Date of last report from FlexxAgent.

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.** User Principal Name.
- **Domain.** Domain of Entra ID or Active Directory where the device resides.
- **Department.** Department provided in Active Directory or Entra ID.
- **Email Address.** User's email address.

On the right side of the screen a table shows the devices used by the user:

- **Workspace.** Device name.
- **Profile size.** Disk space occupied by the user's 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.** Application version discovered.
- **Last report.** Date of last report from FlexxAgent.
- **App Group.** Group to which the application belongs.
- **Category.** Application category.

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

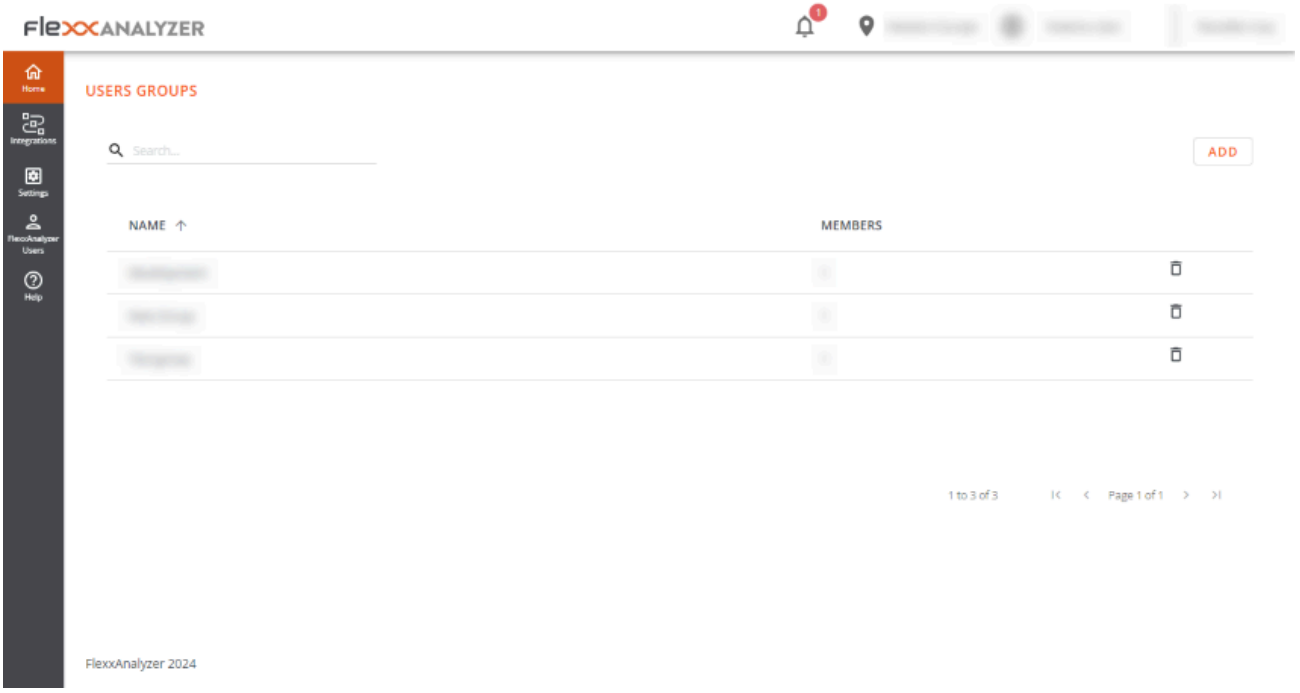
- **Workspace.** Device name.
- **Days:** days of use.
- **Last report.** Date of last report from FlexxAgent.

Analyzer / User Groups

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

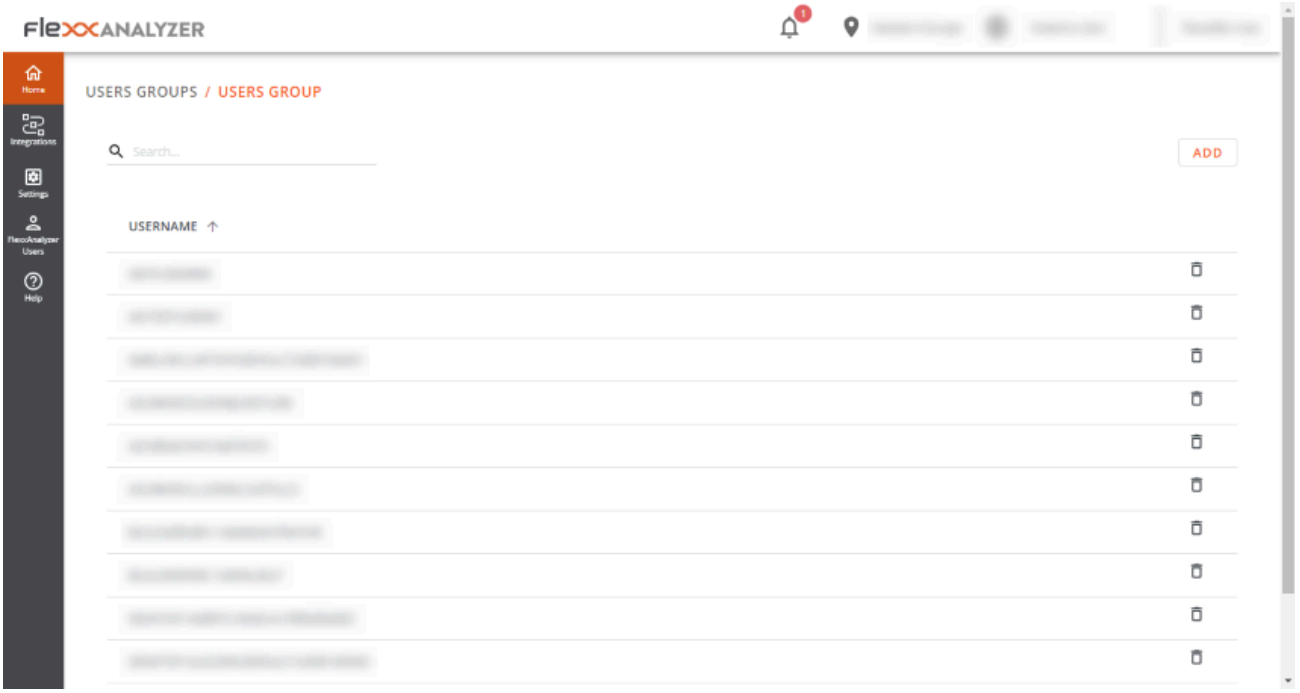
List view

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.

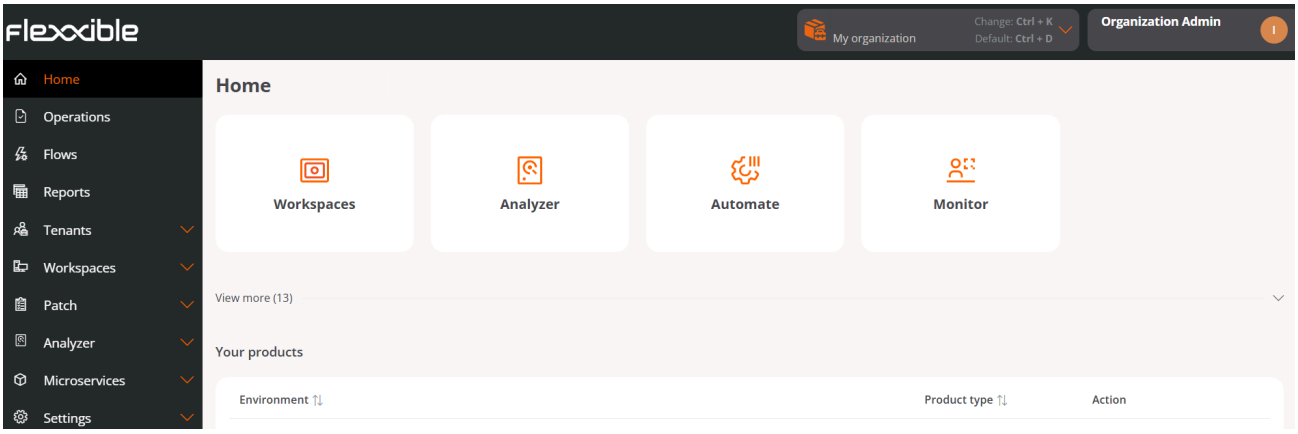


Portal

Portal is the central space of the platform, from where the available modules of the Flexxible products are accessed. It allows you to create, modify, or delete users, assign roles, and manage their permissions to perform and administer actions related to microservices, workflows, patch management policies, and more.

Through **Portal**, you can view license consumption data by environment, manage report groups, and activate features in FlexxAgent. It integrates with OAuth2, a framework that facilitates user authorization so they can easily log in using their corporate credentials.

From the Home section, you can access the different modules that make up the solution and check the active licenses for the Flexxible products included in the subscription.



Sidebar menu

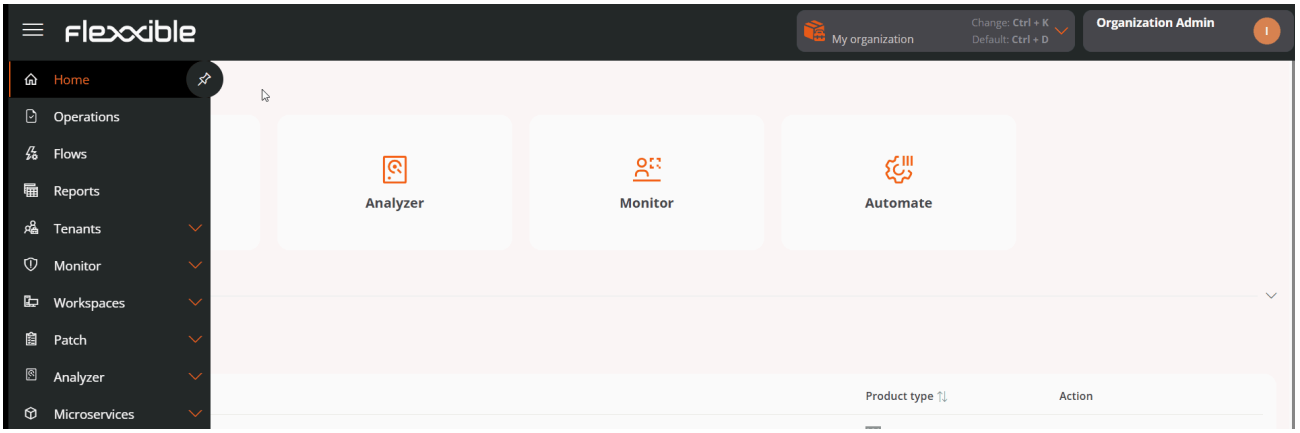
It consists of the following sections:

- Home
- Operations
- Flows
- Reports
- Tenants
- Monitor
- Workspaces

- Updates
- Analyzer
- Microservices
- Configuration

Menu collapse

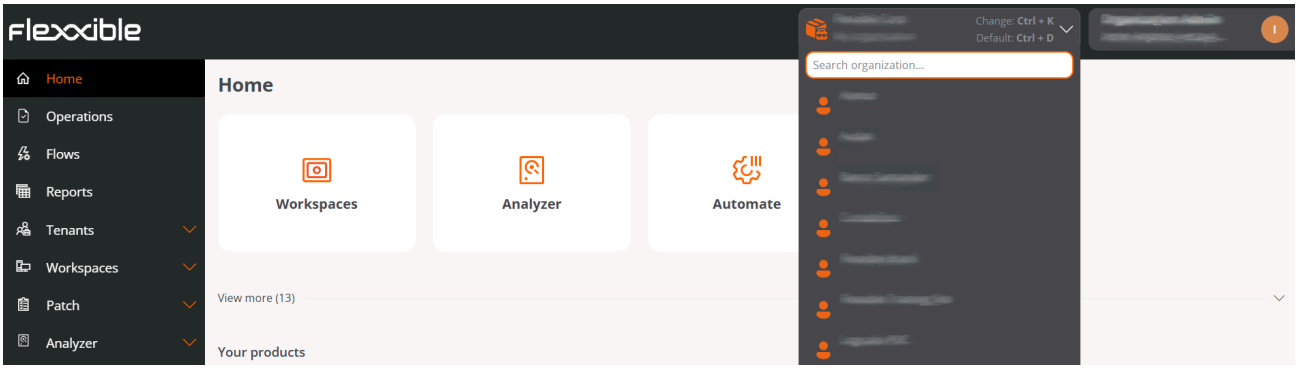
The side menu of Portal can be collapsed to optimize screen usage and enrich the navigation experience within the platform. If the user does not wish to use this feature, there is an intuitive button available, shaped like a thumbtack, that pins the menu and prevents collapse.



Organization selector

At the top, to the right of the interface, is the organization selector. If a user has access to multiple organizations, as in the case of Managed Services Providers (MSP), they can select the one they want to manage very easily: just expand the list of organizations and choose or type in the search box a string of text that matches the name of the organization they want to find, select it, and press the `Enter` key.

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



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

User Settings

In the user menu, on the right side of the interface, the name and role assigned in Portal are displayed. By clicking, the following options are displayed:

- Operations log
- My logins
- Settings
- Log off

Operations List

The table contains the list of operations executed on the user's organization devices and the devices of organizations they have access to, such as managed service providers (MSP).

The fields provide information about the organization to which the device belongs from which the operation was executed, the operation process ID, its status, the name assigned to the process, if there was an error, what the operation consists of, the date and time it was started and updated.

My logins

It provides 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

The left section, **User Settings** shows the general user data. On the right, in **Preferences** you can manage the account preferences, and at the bottom, **Authentication Security Settings** allows you to manage the security levels for email and password authentication at the user level.

Preferences

- **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.** The language in which the interface will be displayed: Spanish, Portuguese, English, Catalan, or Basque.
- **Select Regional Settings.** The chosen option will determine the platform interface settings.
- **Advanced Menu.** Allows you to expand the Portal's side menu, adding shortcuts to specific functionalities of the other modules.

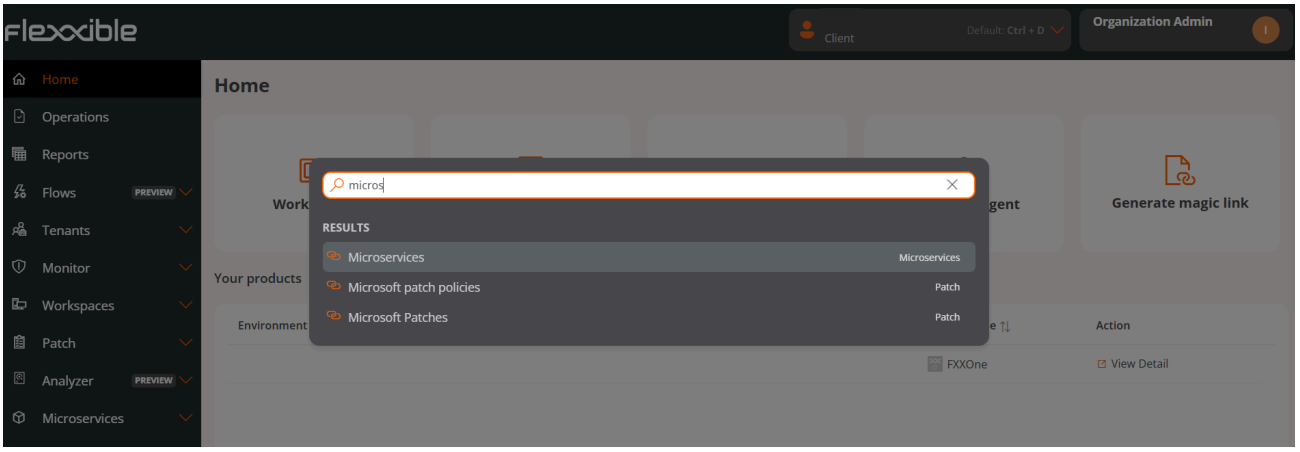
Authentication security settings

From this section, you can manage the security levels for user authentication by email and password. For more information, please refer to the Access and authentication documentation.

Navigation bar

Allows you to go directly to specific sections and subsections of Portal or change the organization to manage. For example, a user who wants to access the Microservices section can do so efficiently by entering the characters of the word *microservice* in the

search box; if the user wants to change the organization, they must type the characters that match the name of the organization they wish to manage, and then press `Enter`.



Considerations about the navigation bar

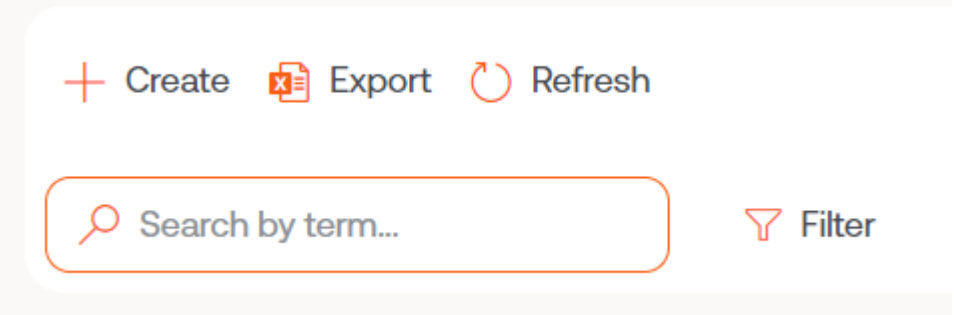
- Access it using `Ctrl + K` (`Cmd + K` on Mac).
- Allows access to recent navigations. The history will change if the user switches organizations.
- Searches must be conducted in the same language set in the Portal.
- To exit, press `Esc`.

Tables

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

Top bar

It is composed of the following buttons:



New

Opens a form to enter data. The fields depend on the section of the Portal being viewed. For example, if the user is in the Tenant section, the form will request information for the new tenant.

Export

When you click `Export`, an Excel file with the table data will be downloaded.

Reload the table

It is an enhancement option, very useful when you want to update the list, especially when new data has been created.

Search by term

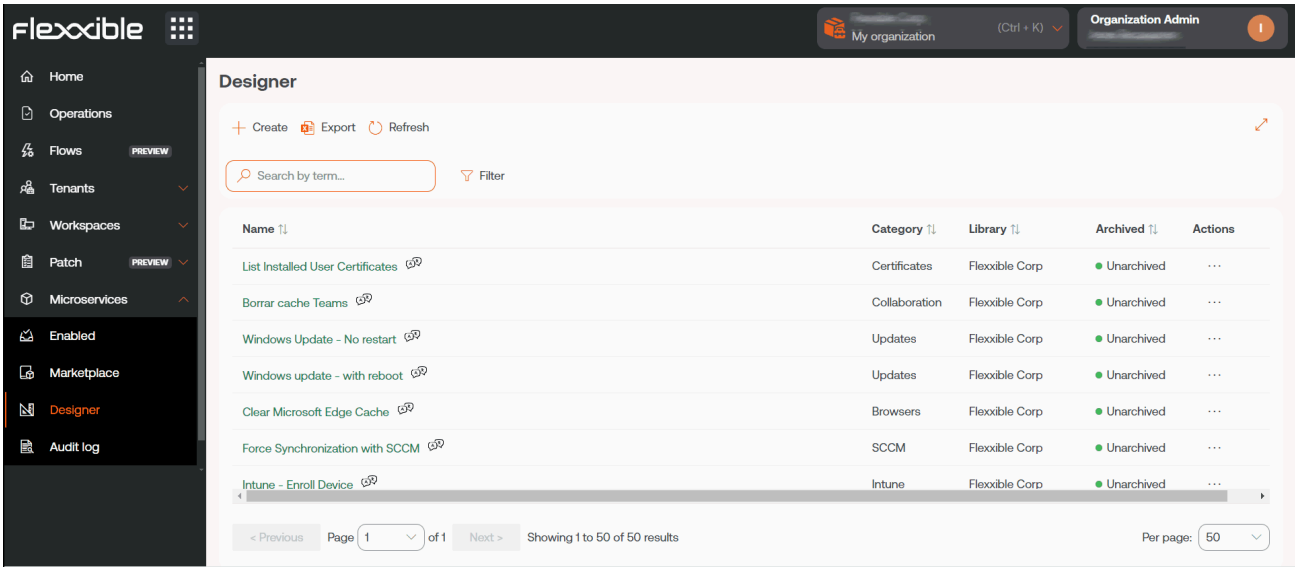
Allows more precise searches. You must enter characters that correspond to the data you are searching for.

Filter

It is a more complete alternative for making searches. Displays a menu to choose the table field where the search will be conducted; once selected, the *Value* option is enabled to enter a term by which you want to filter. You can create as many filters as there are field options displayed.

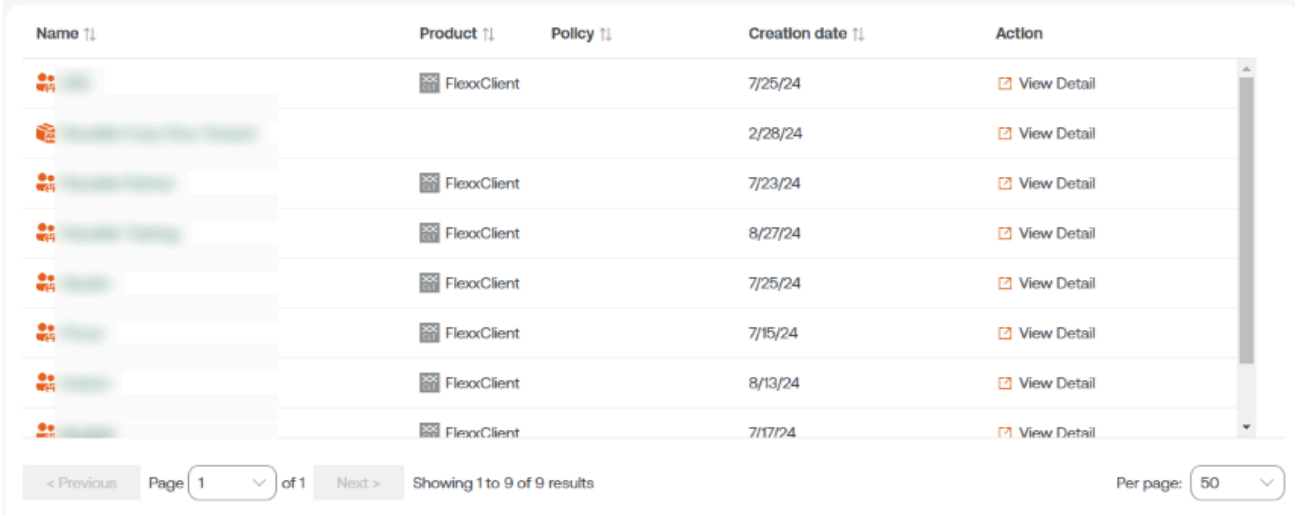
Full screen

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



Content

Table columns order the information according to fields. Its content can be sorted in ascending or descending order, according to the alphabet. And the width of these can be adjusted by placing the cursor between two field names.



Bottom bar

All tables have a navigation bar at the bottom that allows you to select how many results will be displayed per page and the page number you want to go to.

Portal / Access and authentication

To access the Flexxible platform, users can authenticate using the following methods:

- Authentication with a Microsoft Entra ID or Google account
- Authentication with email and password
- Authentication with SAML

Authentication with a Microsoft Entra ID or Google account

For Flexxible's single sign-on (SSO) system to validate Microsoft or Google accounts and authorize access to the platform, an administrator needs to grant the following permissions:

- **Microsoft Entra ID.** Enable the use of a Flexxible Enterprise Application in your tenant.
- **Google.** Enable the use of a Flexxible OAuth Client ID in your tenant.

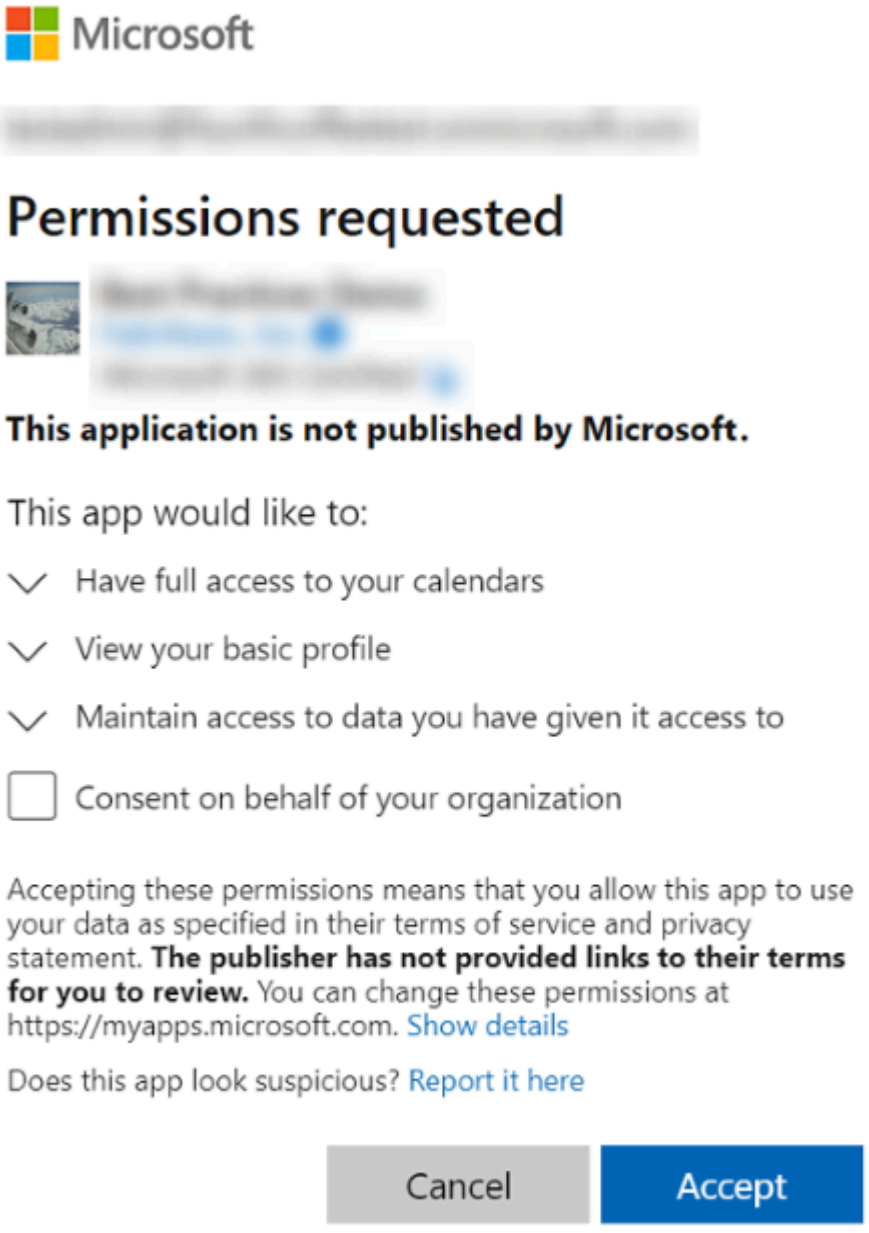
This procedure is common in third-party applications that delegate authentication to Microsoft Entra ID or Google. The tenant administrator can always check the data the application has access to, see which users have utilized it, or revoke consent. If it's revoked, users can no longer log in to Flexxible.

Depending on the organization's configuration and security policies, an administrator might need to authorize these accounts the first time they are used.

Enterprise Application Consent and Permissions in Entra ID

Access can be granted to individual users or groups. However, as explained earlier, there is an option to simplify the process: an administrator can grant organizational consent for using the Enterprise Application.

This consent automatically registers the Enterprise Application in the Azure tenant and allows the organization's users to log in to Flexxible using their corporate credentials. It's enough for the administrator to attempt to log in to the Portal for the first time to trigger the consent request.



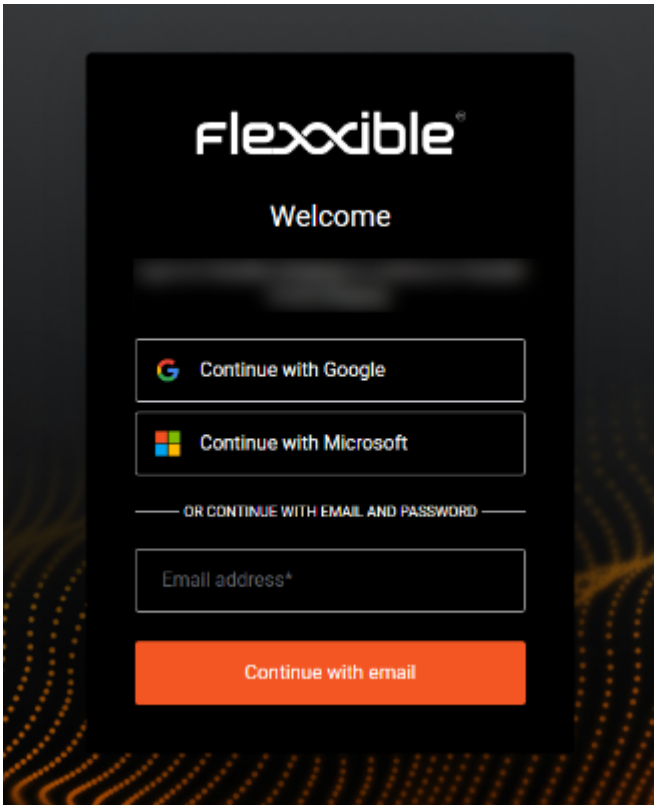
If consent is configured manually, the Enterprise Application must include the following permissions:

Permission	Caption
Directory.Read.All	Read directory data
email	View users' email addresses
offline_access	Maintain access to data that has been granted access
openid	Log In
profile	View basic user profile
User.Read	Log in and read users' profiles

Authentication with email and password

By default, all users of the Flexxible platform have the option to log in with a Microsoft Entra ID or Google account enabled.

Optionally, users with the *Organization Administrator* permission can enable login via email and password for other organization members. This way, users can choose how to sign in.



Login process

To log in to the Flexxible platform using email and password for the first time, you must follow these steps:

1. Enable access to email and password authentication for the user. This step must be done by an *Organization Administrator*.

2. Once enabled, the user will receive a welcome email with a link to create their password. The link is for one-time use only. If they can't log in with it, they can always authenticate with Microsoft Entra ID or Google.

3. Create a password; without it, they can't log in.

4. Set up two-factor authentication through an authentication app. The first time the user attempts to log in with email and password, the platform will prompt them to do so.

5. Log in.

Access to email and password authentication

To activate this method for users, an *Organization Admin* must first enable the option for email and password authentication at the organization level.

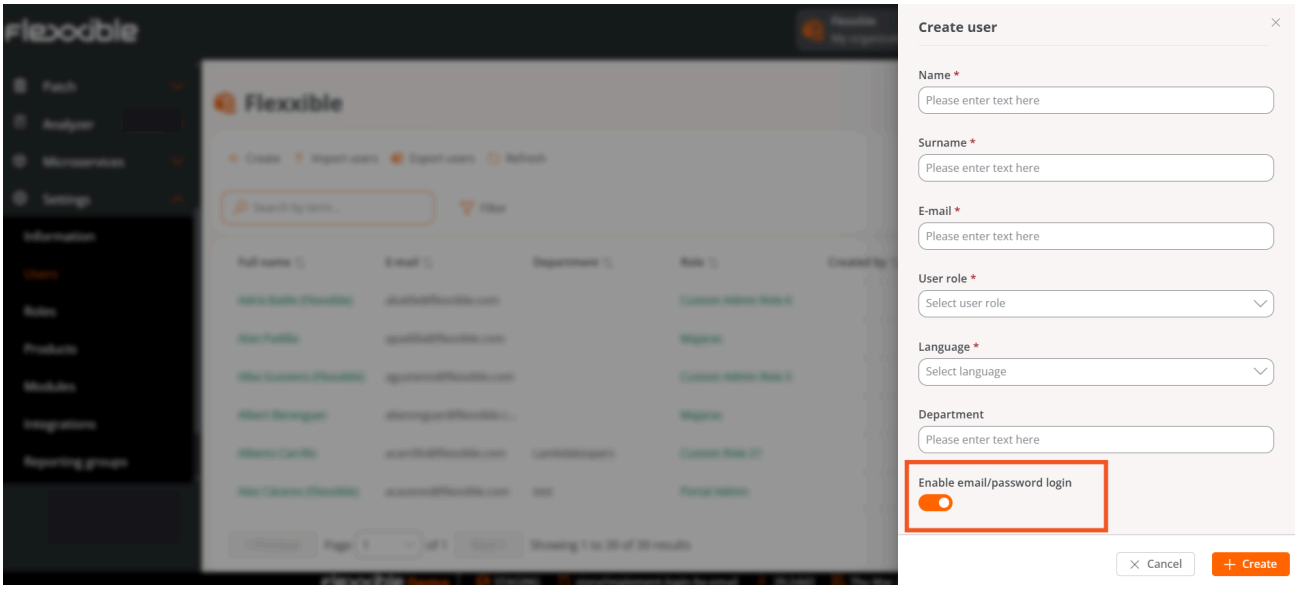
Then, the *Organization Admin* can enable access for the users within the organization. To do this, Flexxible offers the following options:

- Enable access for a new user
- Enable access for a batch of users
- Enable access from the user table

Enable access for a new user

1. Go to `Portal` -> `Settings` -> `Users`.
2. Click on `New`. A form will open requesting the user's information.
3. Check the option `Enable email/password login`.
4. In the form, click on `New`.

> **TIP**
>
> You can find more information on how to create a user in Users.



Enable access for a batch of users

For this action, it's recommended to first export the user list to get the Excel file with the appropriate format:

1. Go to `Portal` -> `Settings` -> `Users` -> `Export users`.

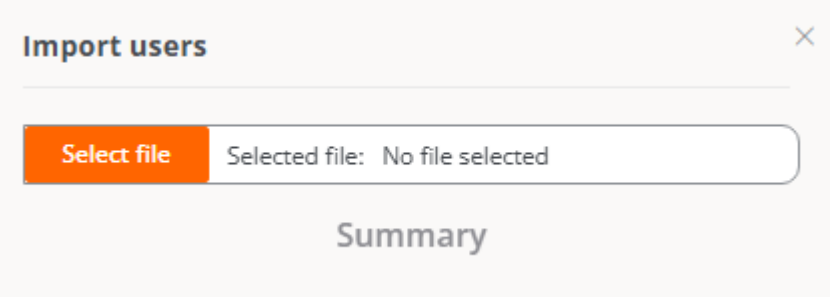
2. Open the Excel file. In the ***Email login enabled*** column, indicate which users will have access enabled: *Y* (enable) and *N* (disable).

Action	Name	Surname	Email	Department	Role	Language	Email login enabled
Add/Update					Portal Admin	en	Y
Add/Update					Custom Admin Role 2	en	N
Add/Update					Portal Admin	en	Y
Add/Update					Custom Admin Role 4	en	N
Add/Update					Custom Admin Role 5	es	N
Add/Update					Majaras	en	N
Add/Update					Custom Admin Role 6	es	N
Add/Update					Custom Role 7	es	N
Add/Update					Majaras	en	Y
Add/Update					Custom Admin Role 9	es	N
Add/Update					Majaras	es	N

3. Save the new file and return to the table with the user list:

   `Portal` -> `Settings` -> `Users`

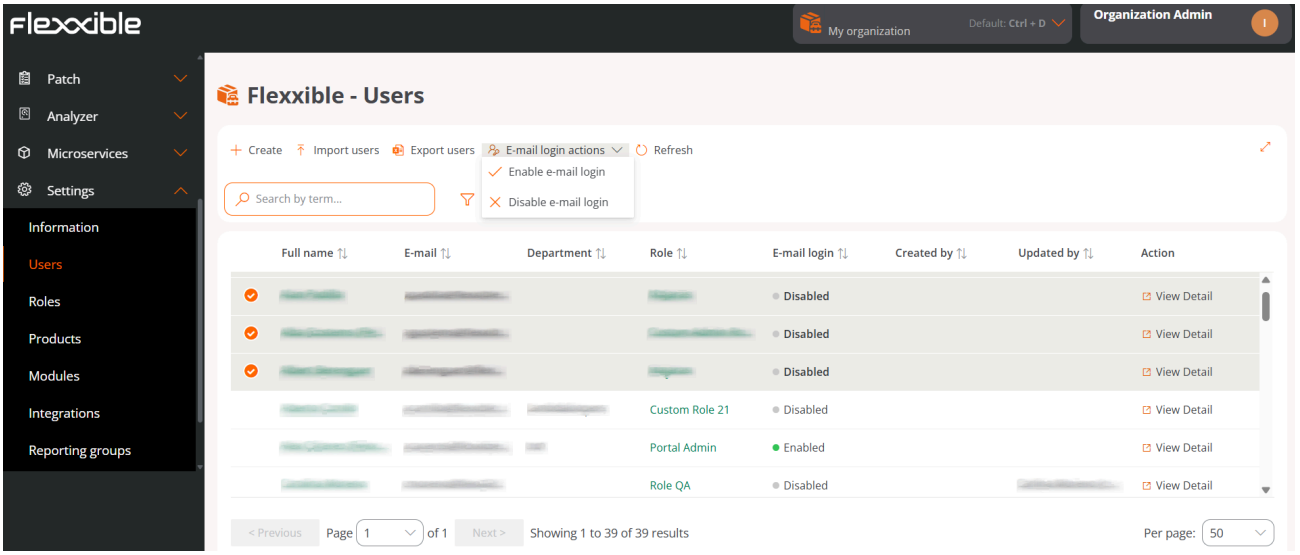
4. Click on `Import users`. Select the saved file.



5. Click on `Import`.

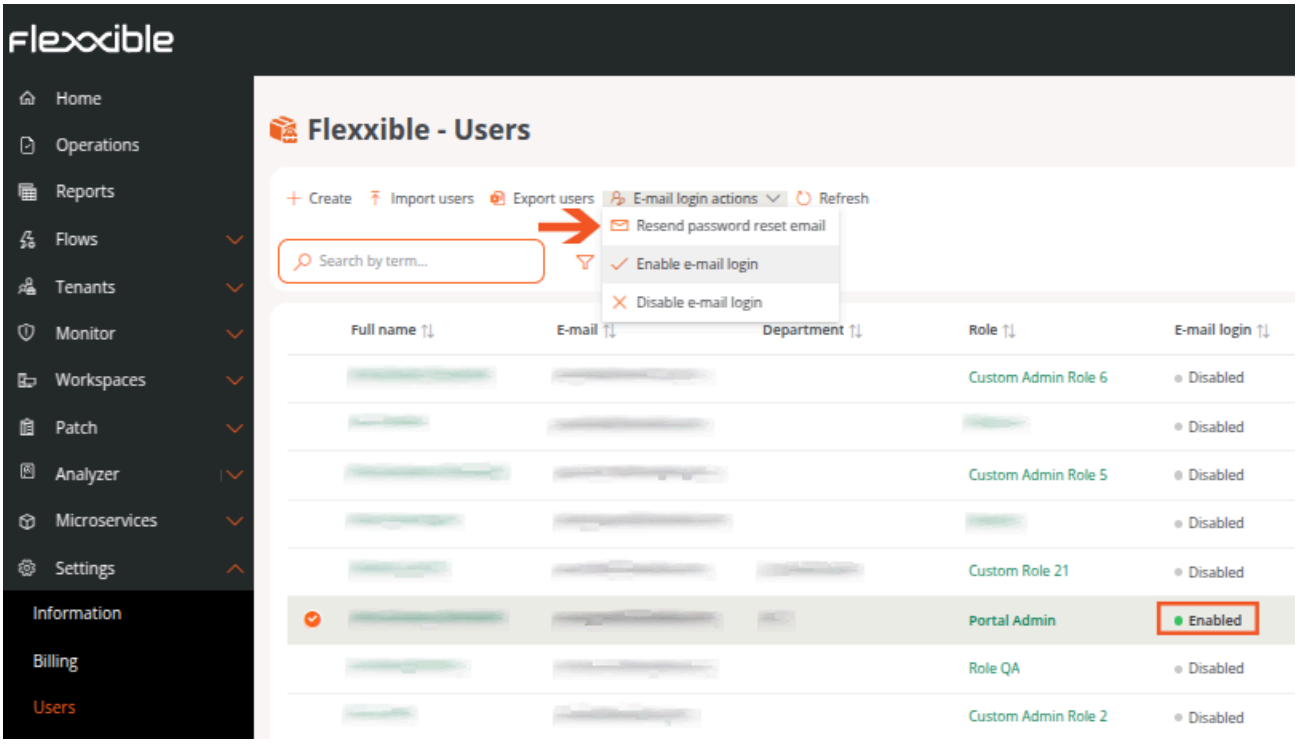
Enable access from the user table

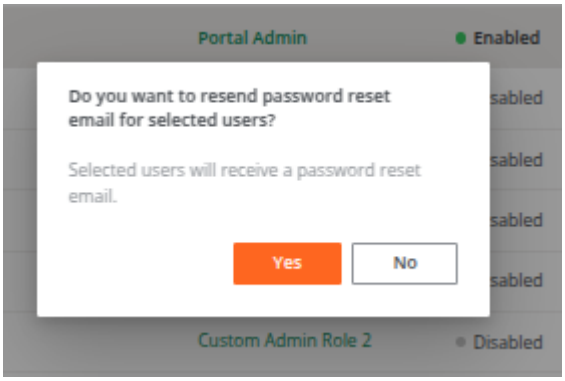
1. Go to `Portal` -> `Settings` -> `Users`.
2. Select the users you want to enable access for.
3. In the top menu, click on `Email login actions` -> `Enable email login` or `Disable email login`, as needed.



Reset the password from the user table

1. Go to `Portal` -> `Settings` -> `Users`
2. Select the users who will receive an email with the link to regenerate the password.
3. Select `Email login actions` -> `Resend password reset email`.





INFO

This option is only available for users who have email and password authentication enabled.

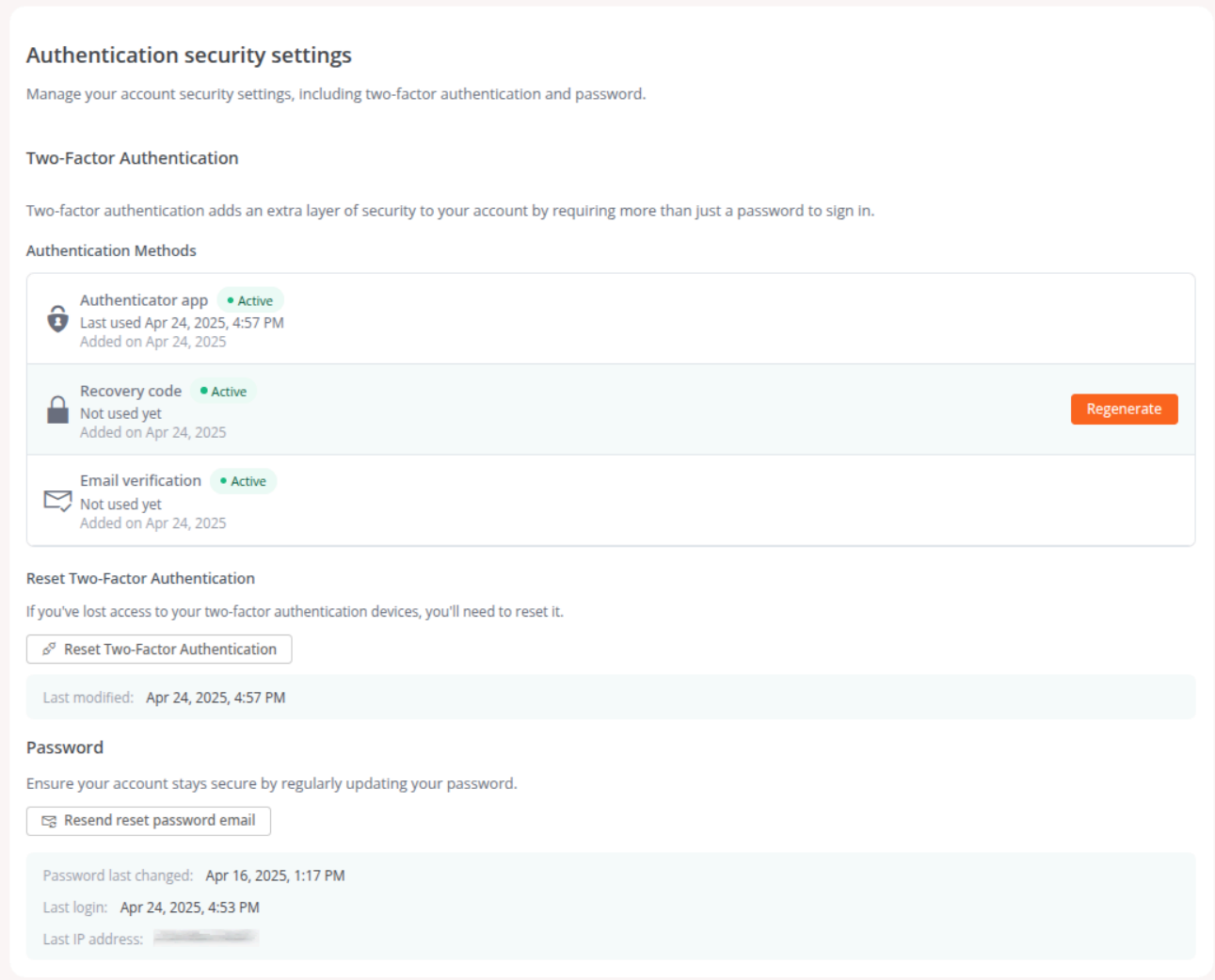
Authentication security settings

Flexxible allows managing security levels for email and password authentication, both at user and organization level.

User-level authentication security settings

From `Portal` -> `User Profile` -> `Settings` -> `Authentication Security Settings`, users can set up three two-factor authentication methods and configure their password.

```
![user-menu](pathname:///assets/images/portal/user-menu.png)
```



Two-factor authentication

This security measure is available for users who log in using email and password, adding an extra layer of protection to the account.

Authentication Methods

For two-factor authentication, Portal allows enabling three methods:

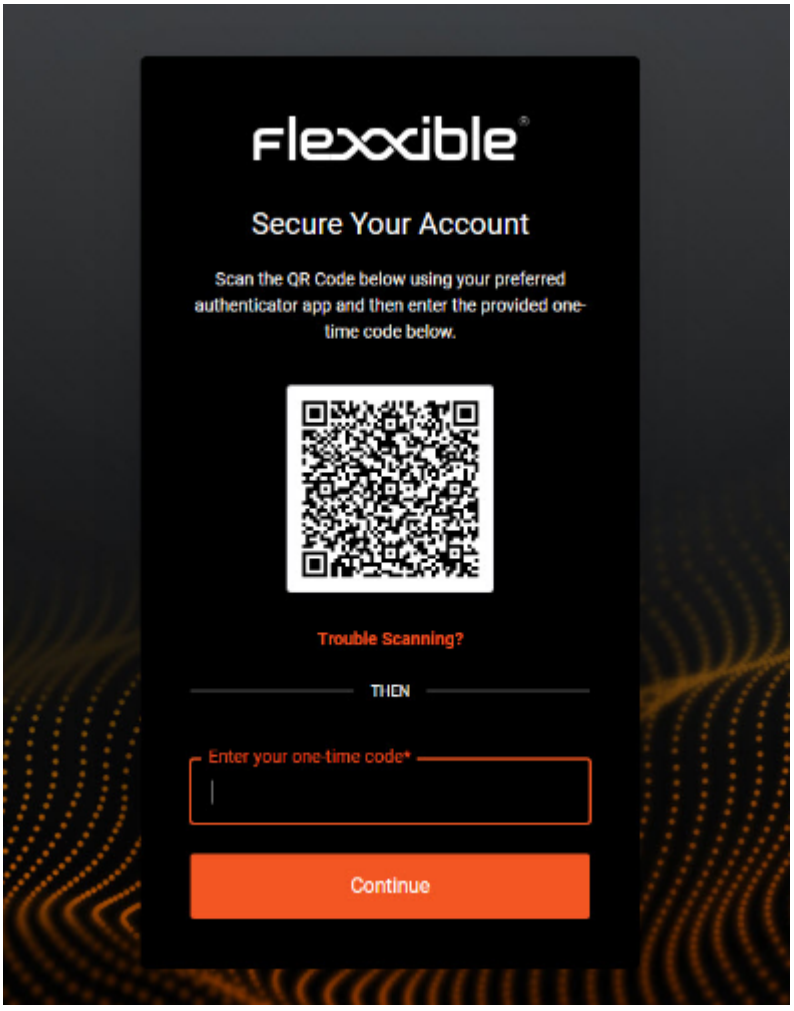
- Authentication app

- Recovery code
- Email verification

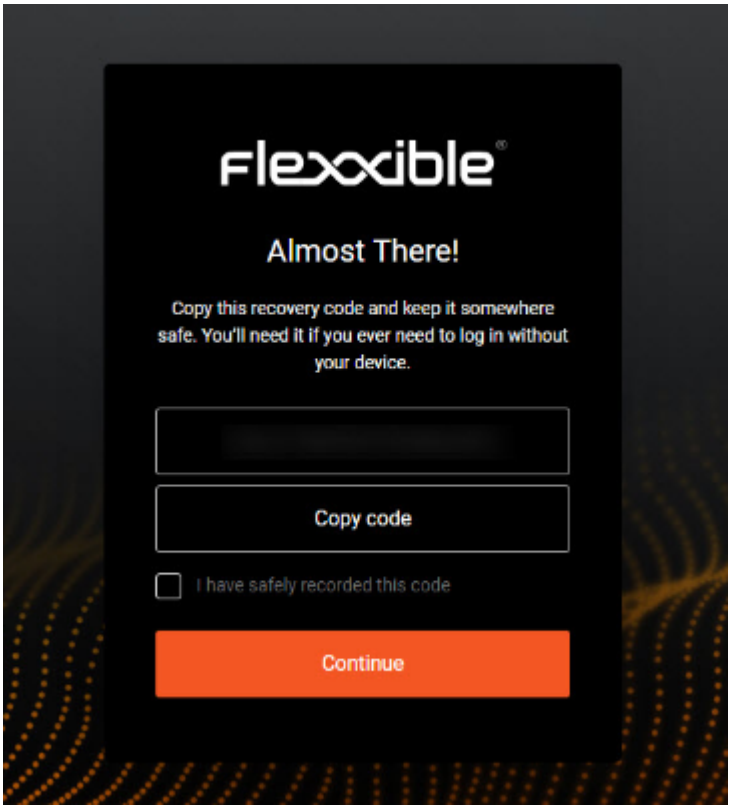
Authentication app

An authentication app allows creating one-time verification codes. When this authentication method is enabled, upon logging into the platform, the user will be prompted to enter that verification code along with their usual password. For this, the user must first download an authentication app, such as Microsoft Authenticator, Google Authenticator, or any other preferred app.

To add this method, the user must click on `Enable` in the authentication security settings panel. A modal window will display a QR code. When scanned, the user must enter the six-digit verification code provided by the authentication app in the designated field.



Next, a recovery code will be shown, which the user should save in case they ever need to log in and don't have access to the device where the authentication app is installed.



From then on, when logging in, the user will be prompted for the verification code in addition to the password.

When a user first logs into the platform using their email and password, they will be asked to set up this authentication method to enhance account security.

> **INFO**
>
> *Verification Code* and *Recovery Code* are not the same. The first is generated by the authentication app, the second is provided by Flexxible as a precautionary measure.

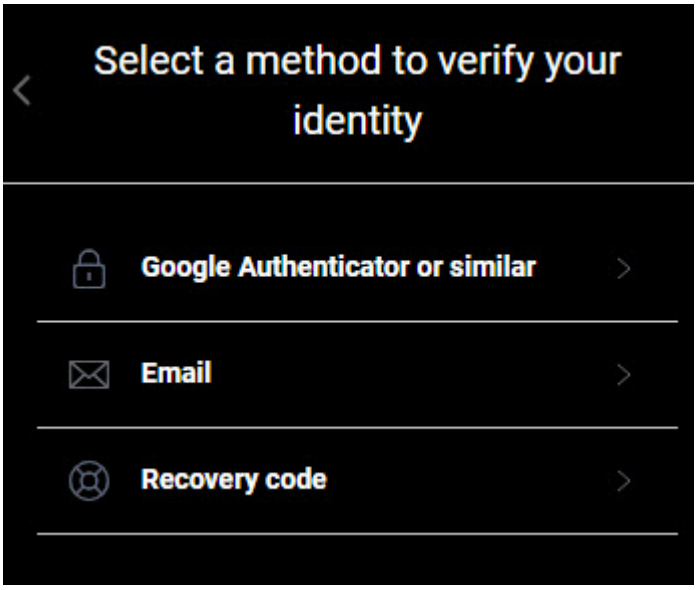
From the authentication security settings panel, the user can see the date and time a session was started using this method, as well as the date it was added as a two-factor security method.

Recovery code

When the use of the authentication app is enabled, Flexxible generates a recovery code for the user to save and use when they don't have access to the device where the authentication app is downloaded. The ***Recovery Code*** option allows regenerating this code if it is lost, to verify the user's identity when they wish to log in.

Email verification

If enabled, it allows verifying the user's identity through an email if they forget their password or don't have access to other identification methods.



To enable this option, the user must click on `Enable` in the authentication security settings panel. From there, the user can also see the date and time of the last time the method was used, as well as the last time it was added as a two-factor security method.

Reset two-factor authentication

Allows resetting the two-factor authentication methods when a user loses access to the devices that enabled their identification. By pressing `Regenerate`, the two-factor authentication methods are disabled.

The user can enable them directly from the same security settings panel. Or by logging out and then logging back into the platform.

It also provides information about the date and time the two-factor authentication was last reset.

Password

From the same panel, the user can request the reset of their password. You must press the `Resend password reset email` button to receive an email with instructions.

It also provides information about the last time the password was changed, the last login, and the last IP address from which they connected.

Authentication security settings at the organization level

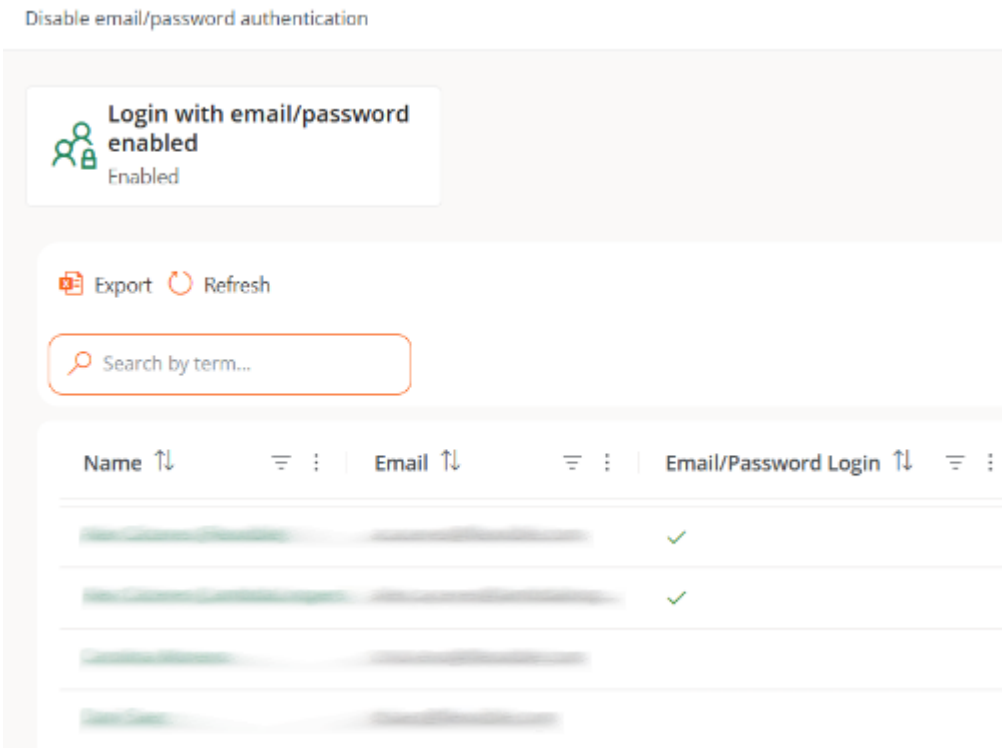
An *Organization Administrator* can enable or disable the option to log in through email and password for users of the organization and its sub-organizations. The functionality can only be enabled or disabled from the main organization if suborganizations are available.

To do this, from the Portal, you must go to `Settings` -> `Organization`. And in the left side menu, you must click on the `Authentication` tab.

Enable or disable the email and password authentication option at the organization level

The button `Enable email/password authentication` or `Disable email/password authentication`, as applicable, allows enabling or disabling the possibility for users who are members of an organization or sub-organization to be able to activate login with email and password.

> **WARNING**
>
> If this option is disabled, users will not be able to log in with email and password or manage their account. All user credentials will be deleted. If this feature is re-enabled, users will need to reset their password and two-factor authentication again.



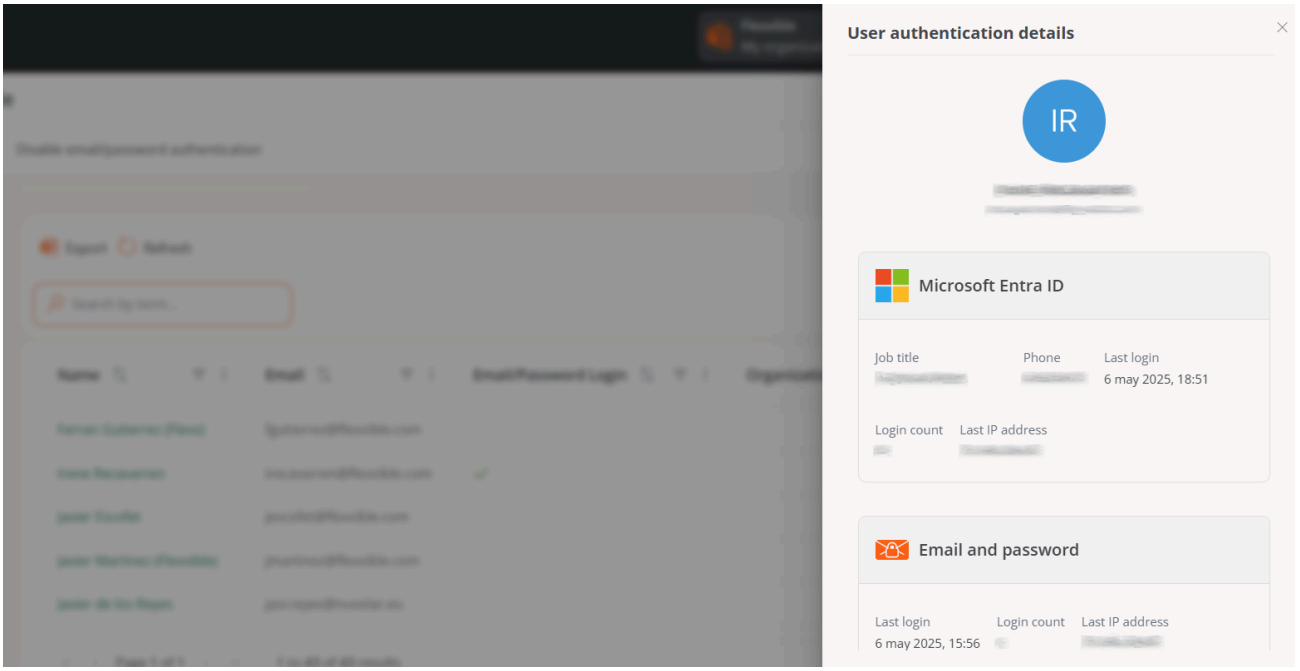
User table

The user table in the `Authentication` tab shows the list of organization members. At a glance, you can see which members have the option to log in via email and password enabled.

User authentication detail

By clicking on a user's name in the table, you can access cards with specific information about the authentication method they have enabled:

- **Microsoft Entra ID.** *Position*, *Phone*, *Last login*, *Login count*, and *Last IP address*
- **Google.** *Last login*, *Login count*, and *Last IP address*
- **Email and password authentication.** *Last login*, *Login count*, and *Last IP address*. Additionally, from here, the administrator can manage the Authentication security settings for that specific user, which includes Two-factor authentication and Password.



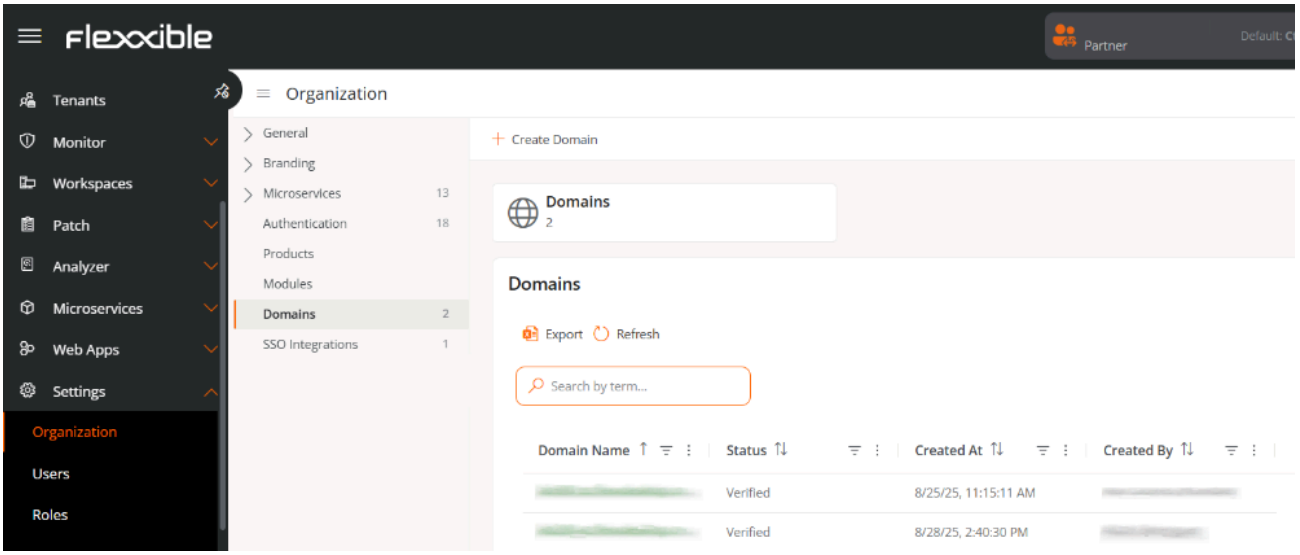
Authentication with SAML

The Security Assertion Markup Language (SAML) is a single sign-on (SSO) technology that allows organizations to connect their identity managers (Okta, Entra ID, among others) with the Flexxible platform, delegating the authentication process to it.

To set up login with this method, you need to make adjustments related to recognizing the organization's domain and integrating with the identity manager used.

Domains

From this tab, an *Organization Administrator* can register and verify the domains to be used. You can also access the table with the domain list and consult its detail view.



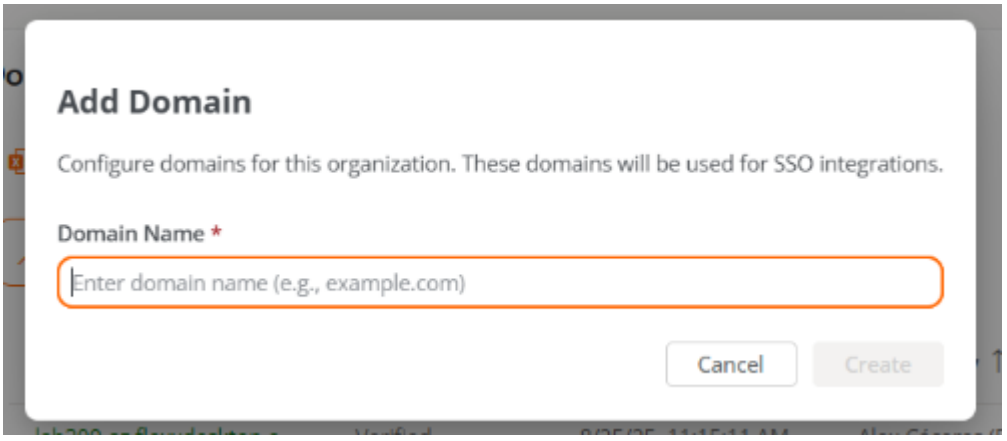
The table shows the following information:

- **Domain name.** Web address registered by the organization.
- **Status.** *Verified* or *Not verified*.
- **Created on.** Domain creation date and time.
- **Created by.** User who registered the domain.

Create a domain

To configure a domain, it must first be registered and then verified.

1. Access `Portal` -> `Organization` ->
2. In the menu, select the `Domains` tab.
3. Click `Create domain`.
4. Enter the organization's domain (corresponding to the email of the users who will log in with SAML).



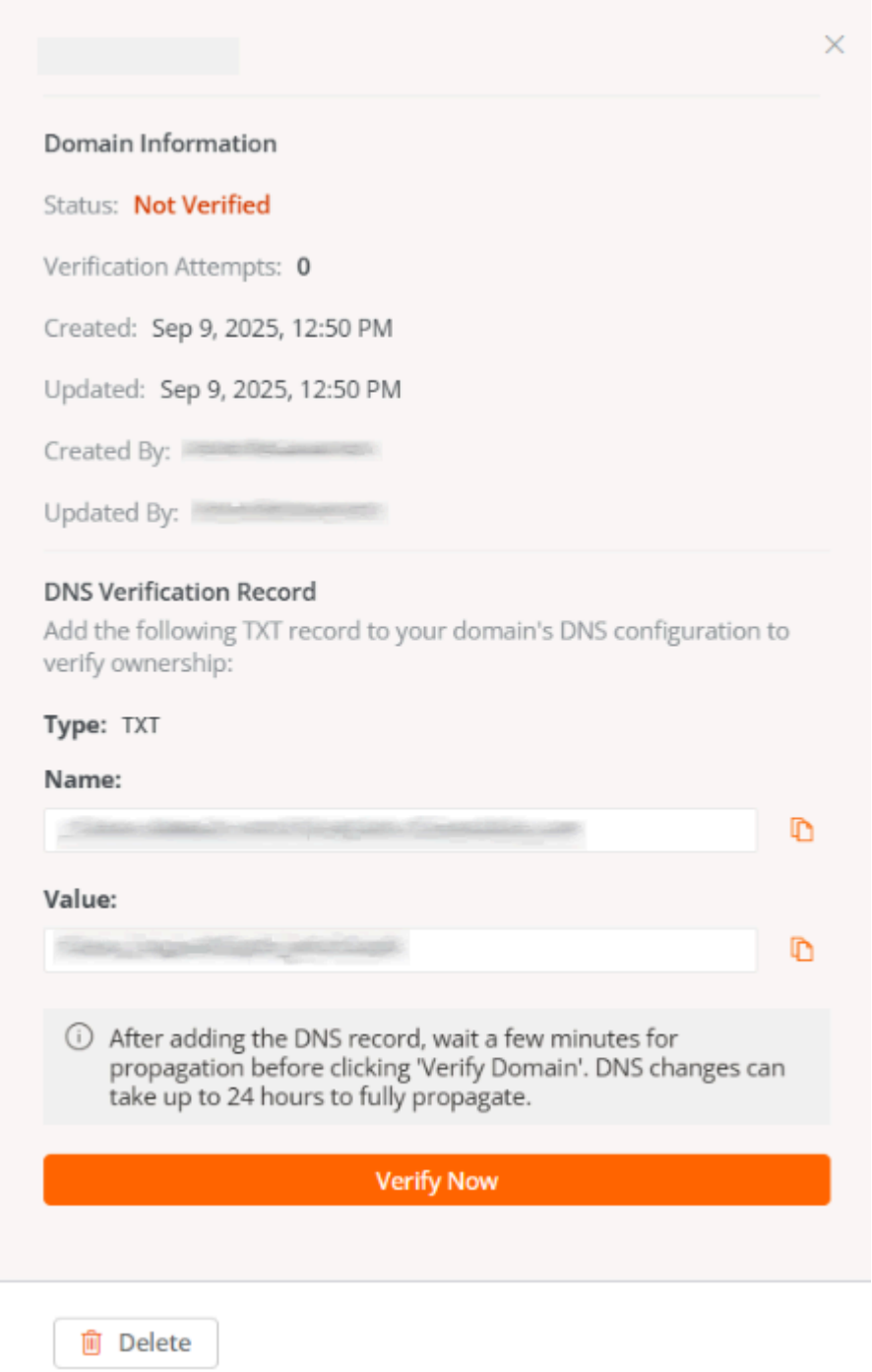
5. Click on `New`.

The domain will be added to the table with the status *Not verified*.

Verify the domain

1. In the Domains table, select the registered domain.

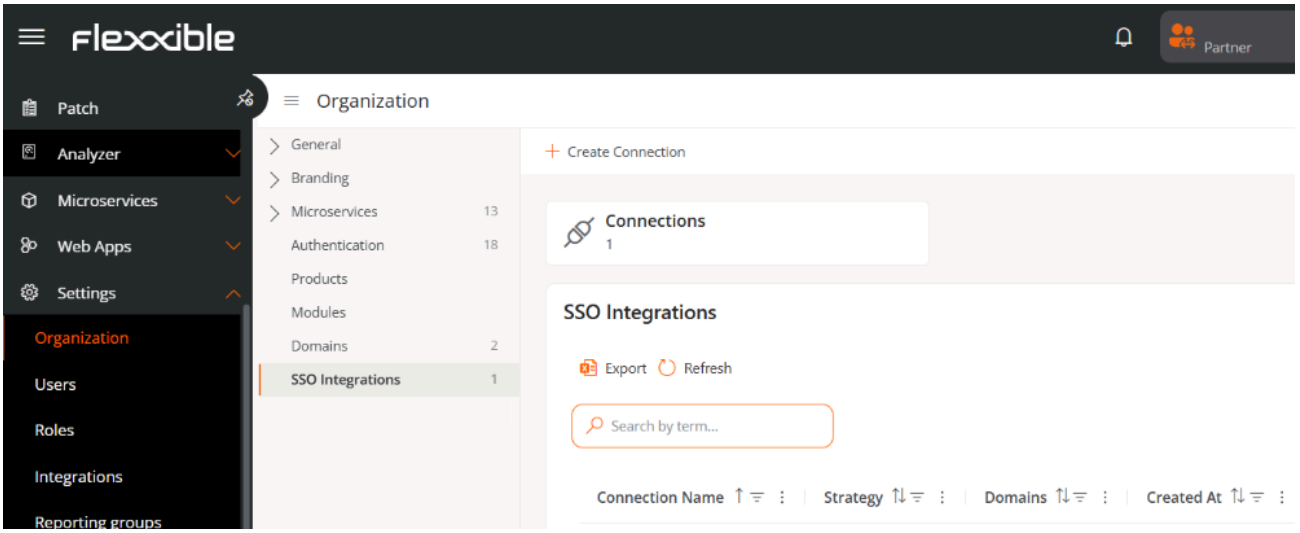
2. A window will appear with instructions to add a TXT record in DNS, necessary to verify ownership.



3. Click `Verify now` to complete the process.

Create an SSO connection

Creating an SSO connection allows users with specific domain email addresses to authenticate through the organization's identity provider.

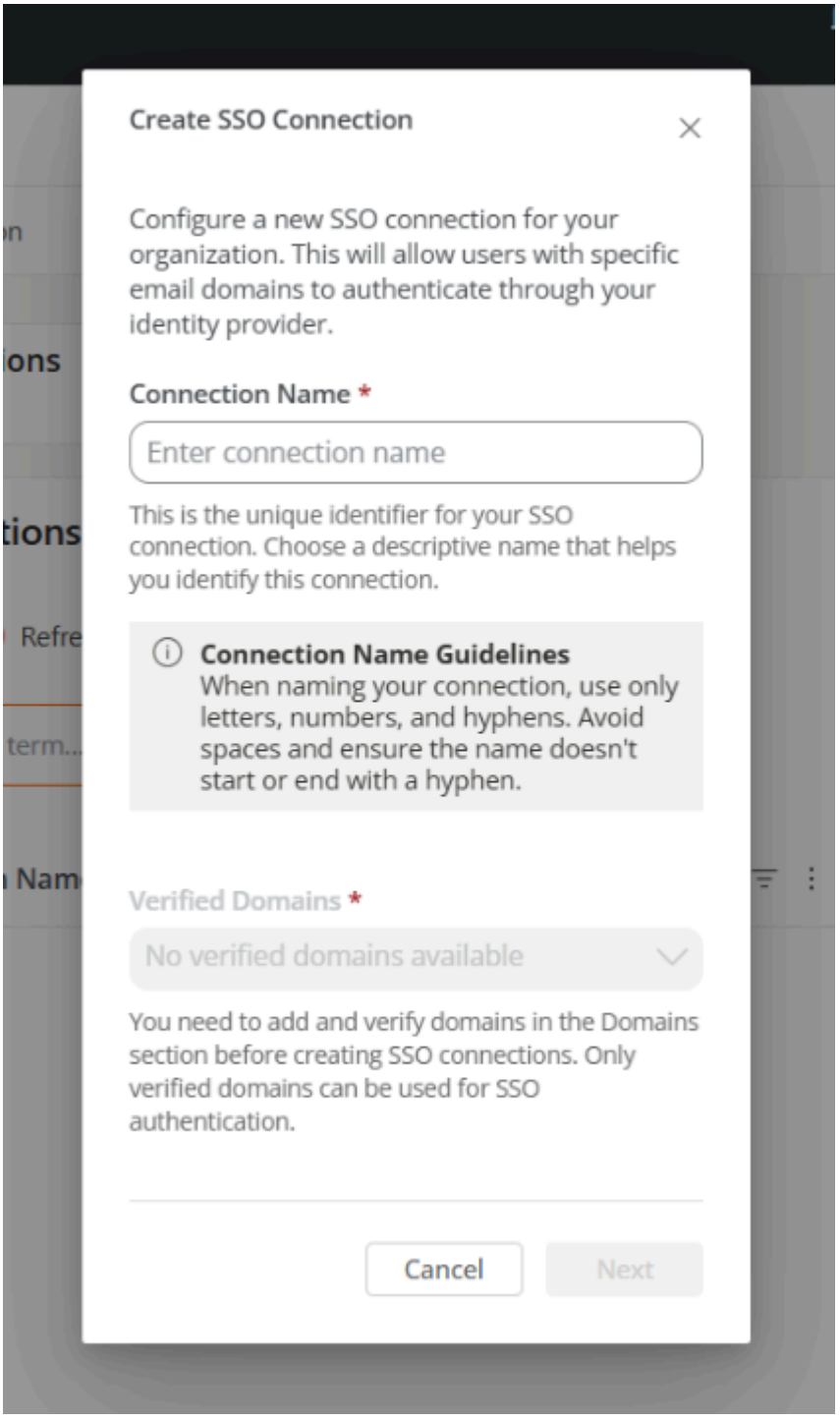


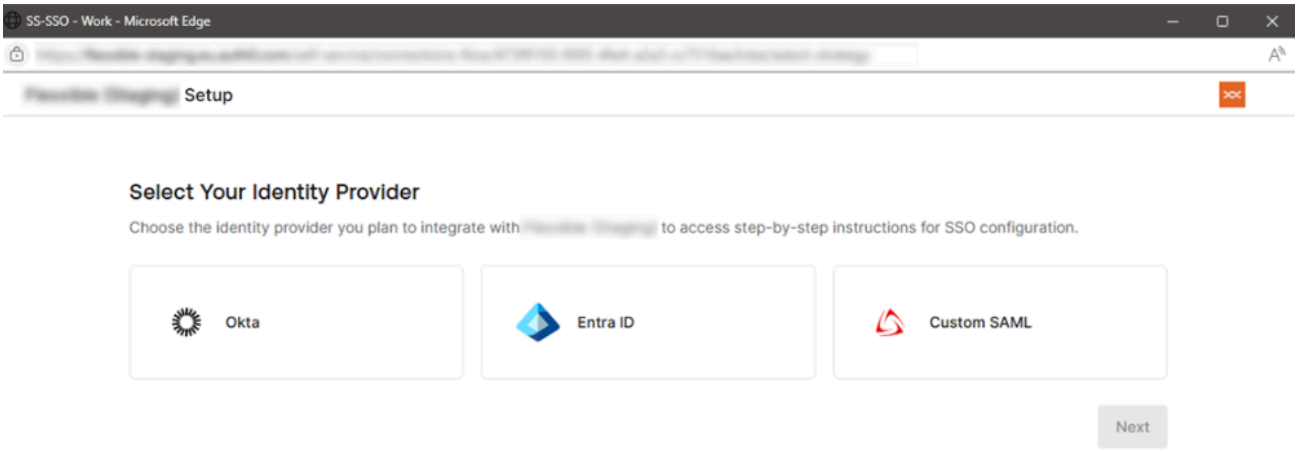
1. Access `Portal` -> `Organization`.
2. In the menu, select the `SSO Integrations` tab.
3. Click `Create connection` and follow the wizard instructions, which will guide the *Organization Administrator* through the setup and testing according to the identity manager used.

Available identity managers:

- Okta
- Entra ID
- Custom SAML

For each case, a wizard will guide you step by step in the specific setup within the selected identity manager.





TIP

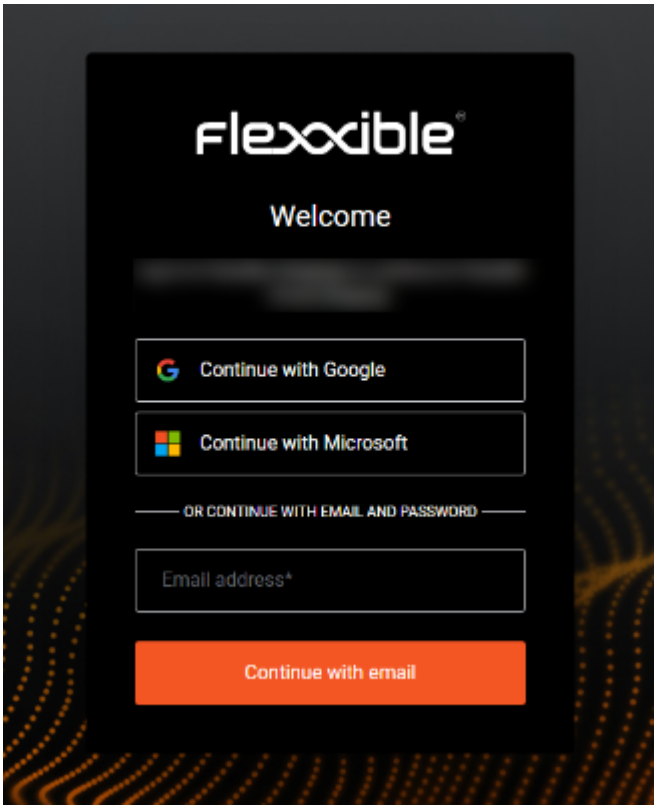
Some of the requested data during setup may have different names depending on the identity manager. For example, in Custom SAML:

- The `Single Sign-On URL` field may appear in the identity manager as `Reply URL (Assertion Consumer Service URL)`.
- The `Service Provider Entity ID` field may be called `Identifier (Entity ID)`.

NOTE

If any doubts arise during the setup process, please consult with your contact at Flexxible.

Once the process is completed, users from associated domains will be able to log in by entering their email address in the appropriate field and clicking `Continue with email`.

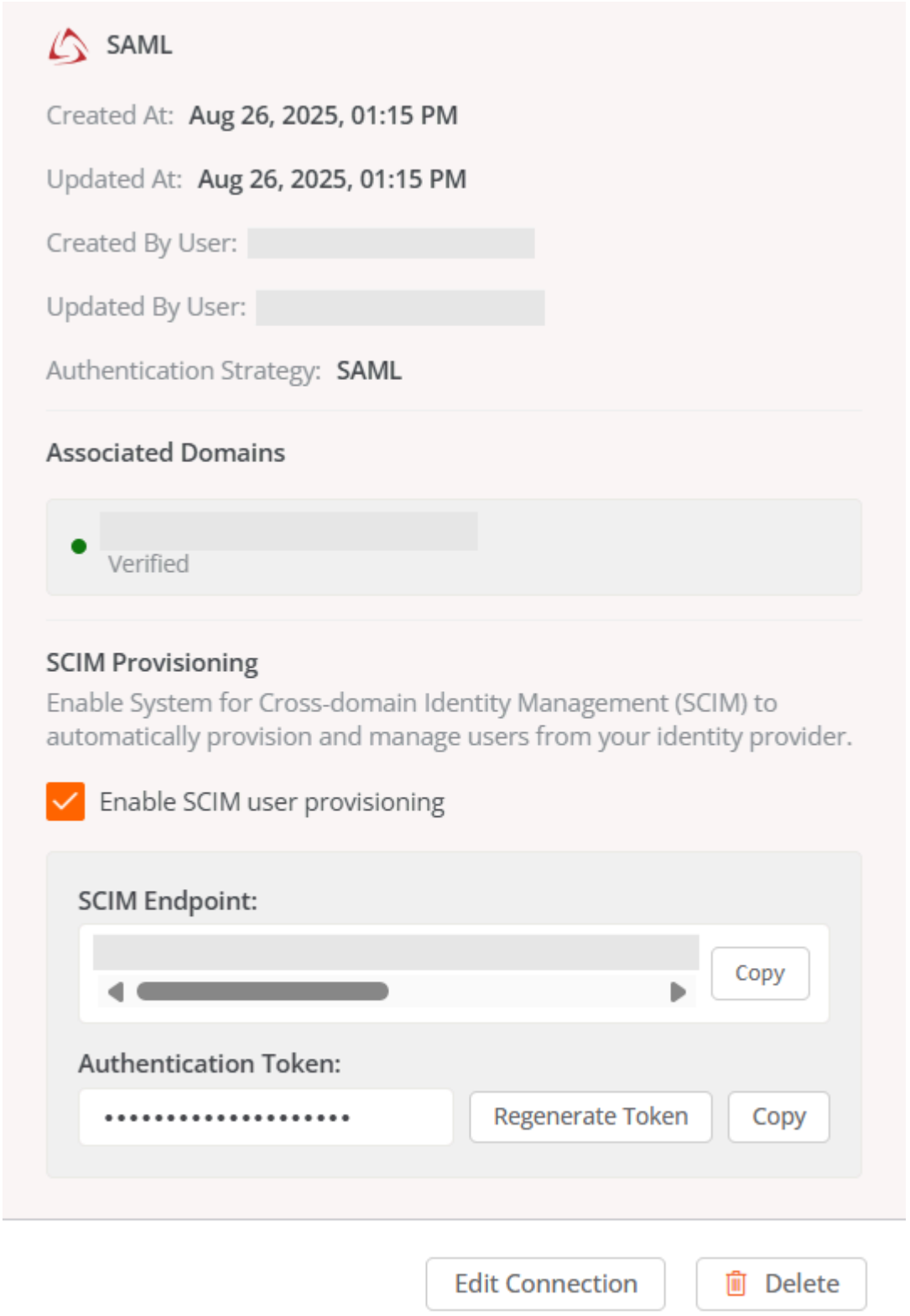


If the system recognizes the domain as enabled for SSO, it will redirect the user to the organization's identity manager for authentication.

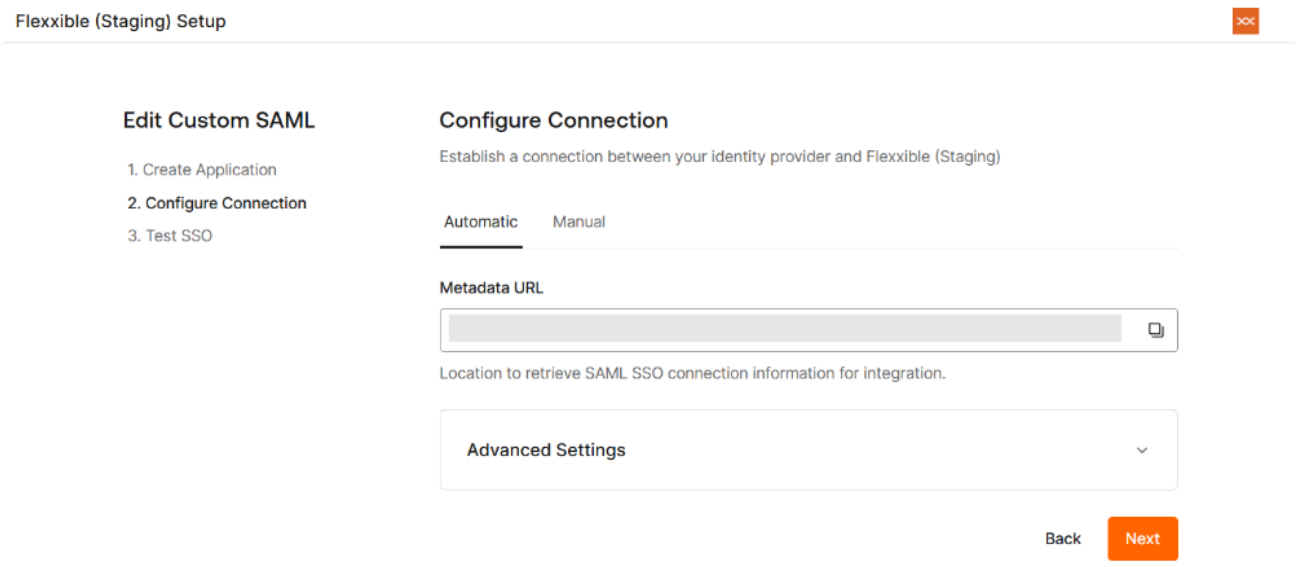
Edit an SSO connection

The platform allows editing an existing SSO connection either to update the configuration or renew the certificate in case of expiration.

1. Access `Portal` -> `Organization`.
2. In the menu, select the `SSO Integrations` tab.
3. Select a record in the table.
4. Click `Edit connection`.



Checking the `Enable SCIM user provisioning` checkbox is optional. More information in User provisioning with SCIM.



Remove domain

1. Access `Portal` -> `Organization`.
2. In the menu, select the `Domains` tab.
3. Select the domain in the table that you want to remove.
4. In the detail window, click `Remove`.

By removing a domain, users associated with it will no longer be able to authenticate via SAML until it is registered again.

Remove an SSO connection

1. Access `Portal` -> `Organization`.
2. In the menu, select the `SSO Integrations` tab.
3. Select the corresponding record in the table.

SCIM Provisioning

The System for Cross-domain Identity Management (SCIM) is a user provisioning and management standard that complements authentication with SAML. It is optional and automates the creation, update, and removal of user accounts in Portal, keeping

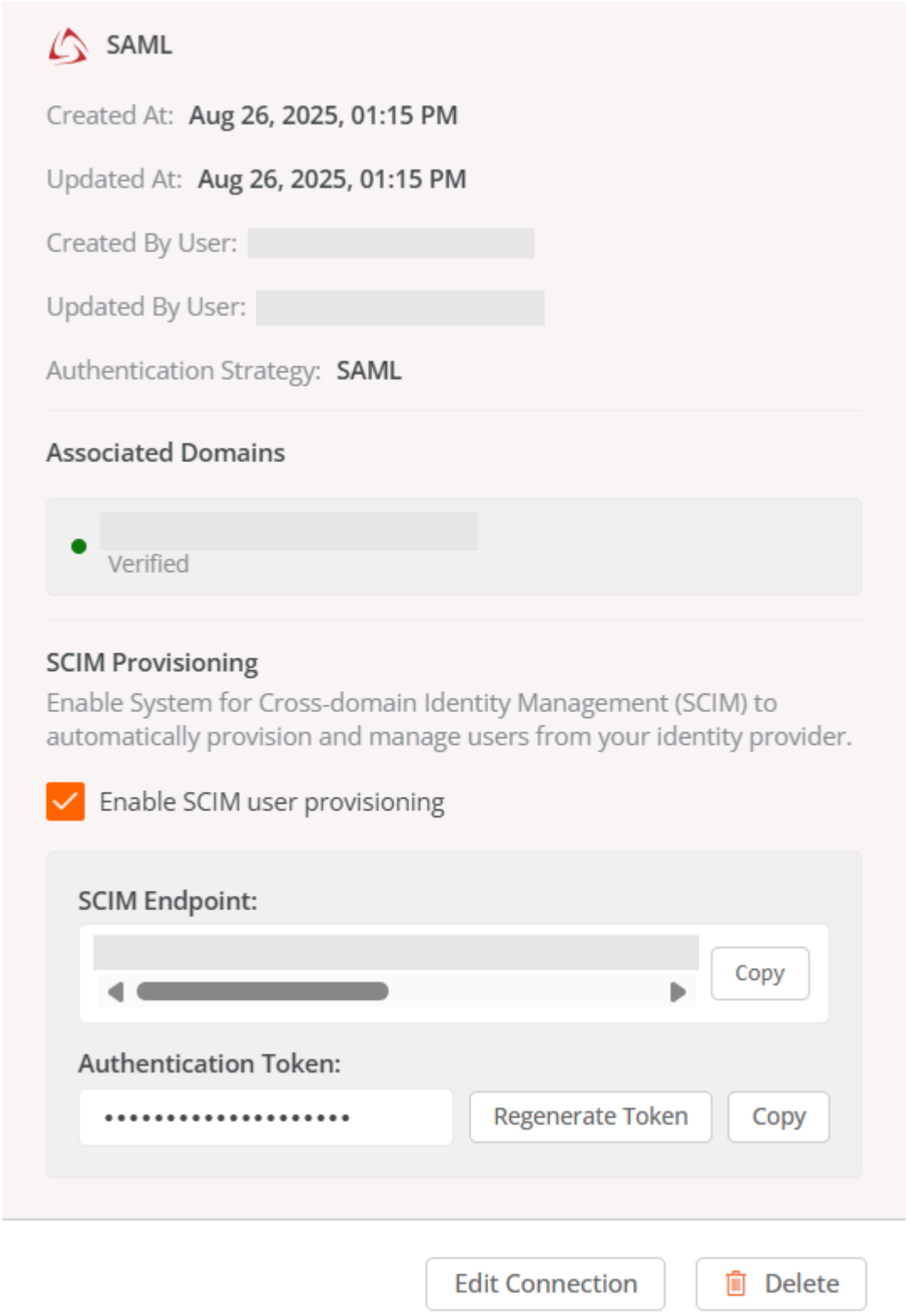
information synchronized between the organization's identity manager (Okta, Entra ID, etc.) and the Flexxible platform.

When SCIM is enabled, the identity manager can send basic user information (name, email, group) to Portal, simplifying account management. This way, the user's lifecycle in Portal is centrally controlled from the identity manager.

Enable SCIM in Portal

To use SCIM, it is essential to have previously set up authentication with SAML:

1. Access `Portal` -> `Organization`.
2. In the menu, select the `SSO Integrations` tab.
3. In the table, select the corresponding SSO connection.
4. Check the `Enable SCIM user provisioning` option.



When the option is activated, the following will appear at the bottom of the configuration window:

- SCIM endpoint

- Authentication token

> **WARNING**
>
> These details are confidential and should be stored securely.

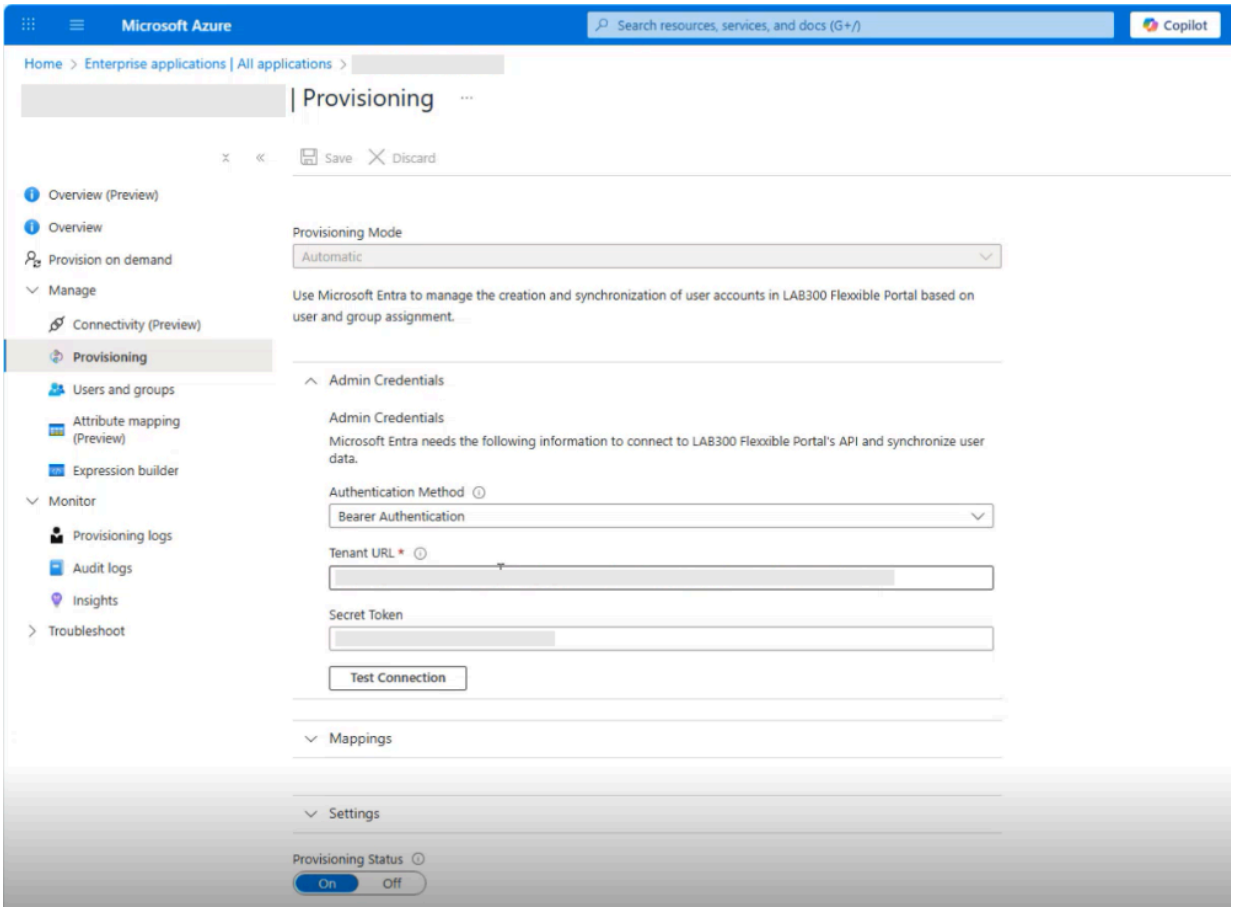
> **INFO**
>
> In environments with sub-organizations, the SCIM integration must be defined in the "parent" tenant.

Configure SCIM in the identity manager

In the organization's identity manager, enter the SCIM endpoint and authentication token provided in Portal.

Example with Entra ID:

1. Go to `Provisioning`.
2. Enter the SCIM endpoint and authentication token.
3. Select the authentication method: `Bearer token` or `Bearer Authentication`.
4. Click `Test connection` to validate synchronization.
5. Activate provisioning.



From that moment, the identity manager will start syncing groups and users to Portal.

> **INFO**
>
> - If **Okta** is used as the identity provider:
>   - The SCIM functionality has to be configured using the Custom SAML option, as Okta does not support SCIM when the connection is with OIDC.
>   - When configuring the Custom SAML connection, the **Application username format** must be specified as **Email**, otherwise users will not be able to authenticate.

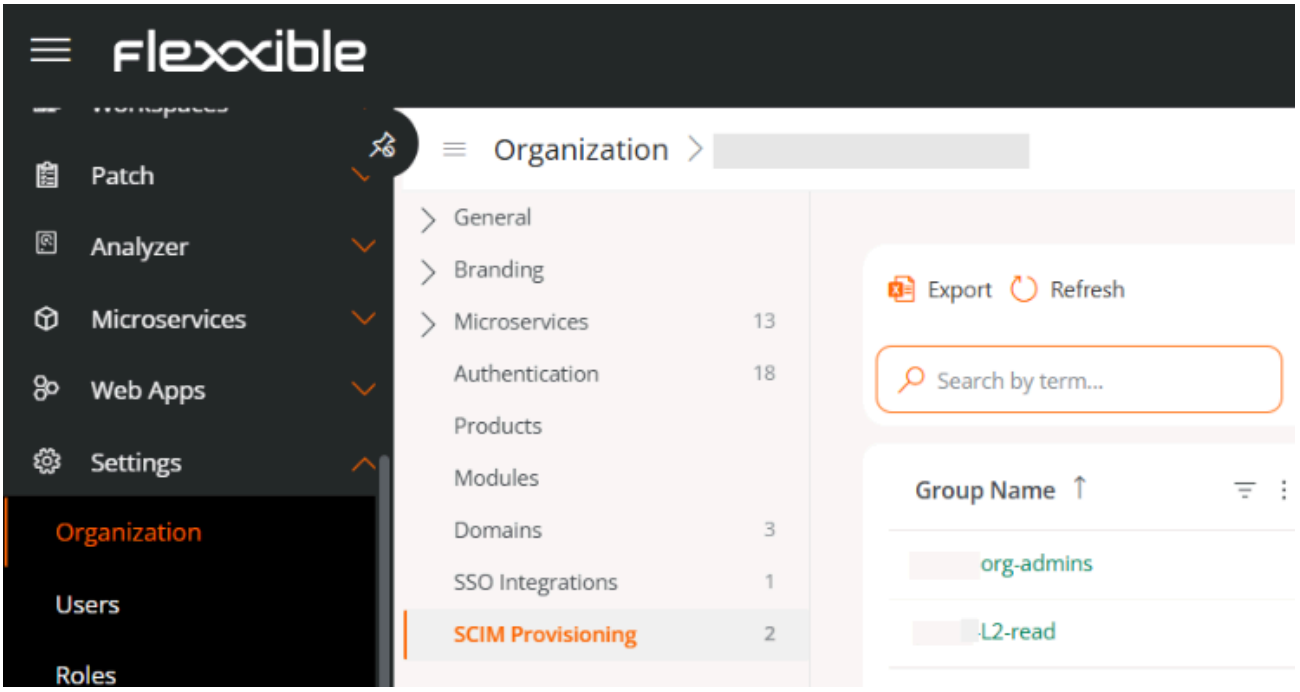
Create user groups in the identity manager

To integrate users via SCIM, it is essential to create groups in the identity manager.

Considerations

- Create groups specifically dedicated to Portal with clear and exclusive names (e.g. `MiOrg-Portal-L2`).
- When user groups are created or deleted in the identity manager, they will also be automatically created or deleted in Portal.
- Do not create nested groups.
- **A user should belong to only one group**; otherwise, unexpected behaviors may arise: in Portal a user cannot have more than one role.
- There cannot be users without an assigned group.
- Users belonging to a group that does not have a linked role will not be visible in the Users list.

When user groups are created in the identity manager, the `SCIM Provisioning` tab will automatically appear in the `Organization` menu of Portal.

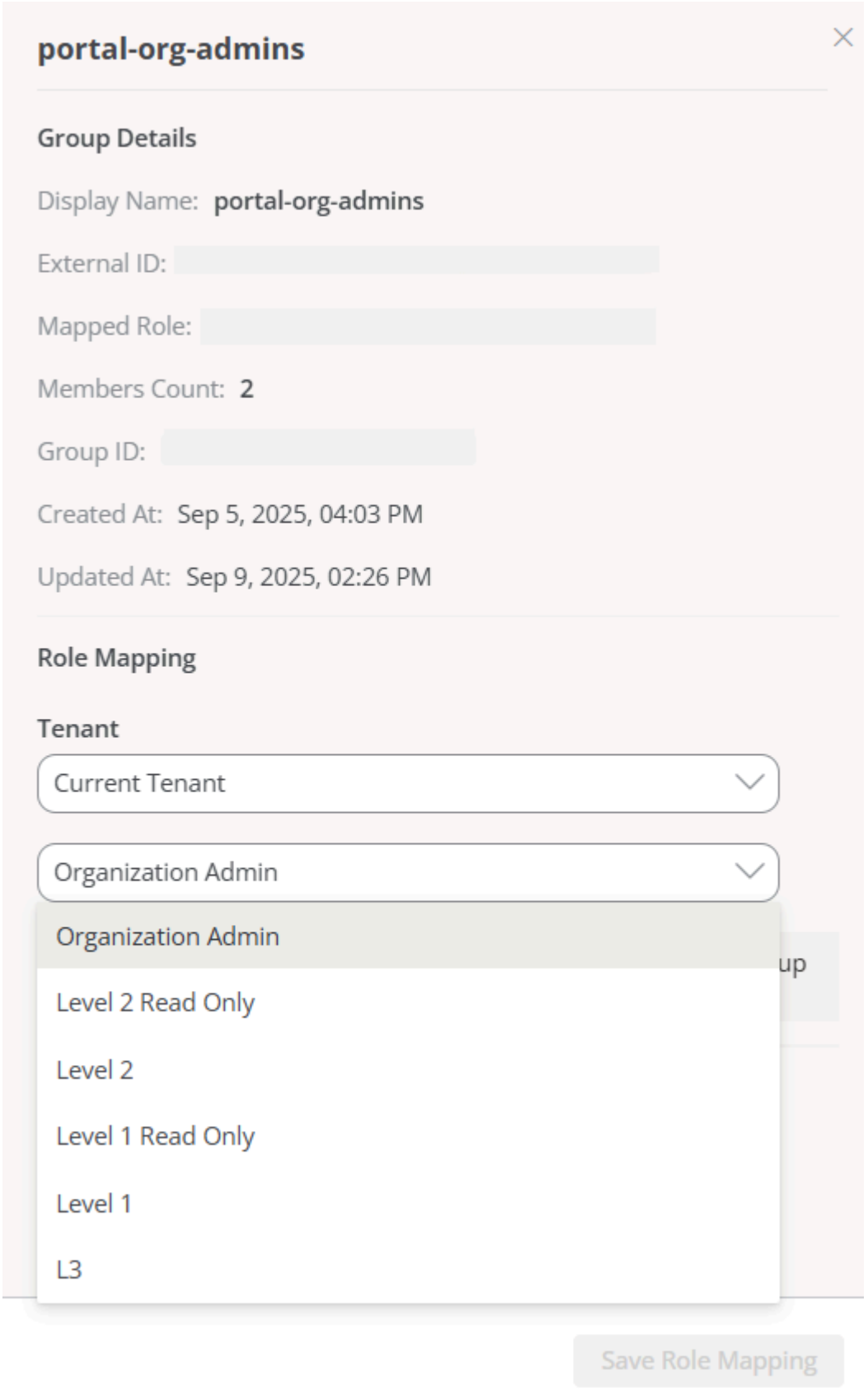


Role mapping in Portal

In the `SCIM Provisioning` tab table, you can see the groups created in the identity manager. This happens because a one-way synchronization has been established from the identity manager to Portal.

To map roles:

1. Access `Portal` -> `Organization`.
2. In the menu, select the `SCIM Provisioning` tab.
3. Select a synchronized group from the table.
4. In the modal window, assign the corresponding role.
5. If an organization (tenant) has sub-organizations, choose which sub-organization that group belongs to before assigning it a role.

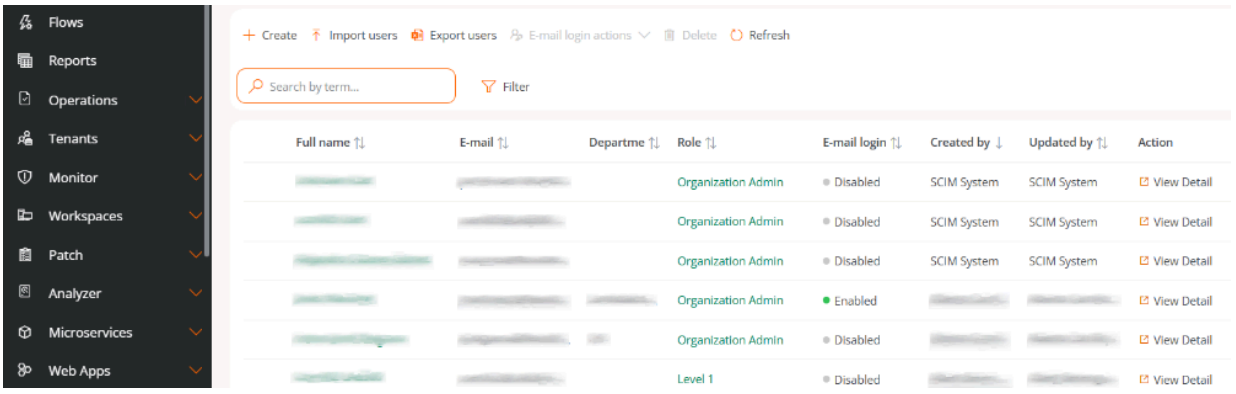


From the moment all groups are linked to a role, no further configurations will be needed. New users added or removed from groups in the identity manager will be automatically

synchronized in Portal.

Considerations about roles

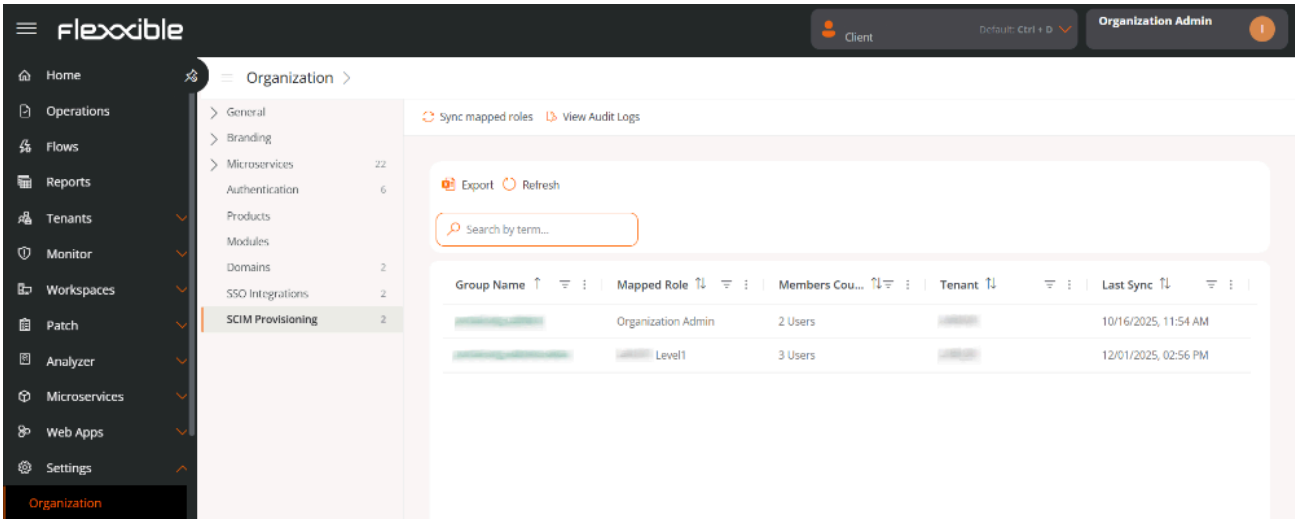
- Every synchronized group must have a role assigned to be visible and functional in Portal.
- The same role can be assigned to different groups.
- The role assigned to a group can be changed at any time by following the same steps used to assign the role.
- In the Users list, the *Created by* and *Updated by* columns will appear to identify users managed by SCIM.

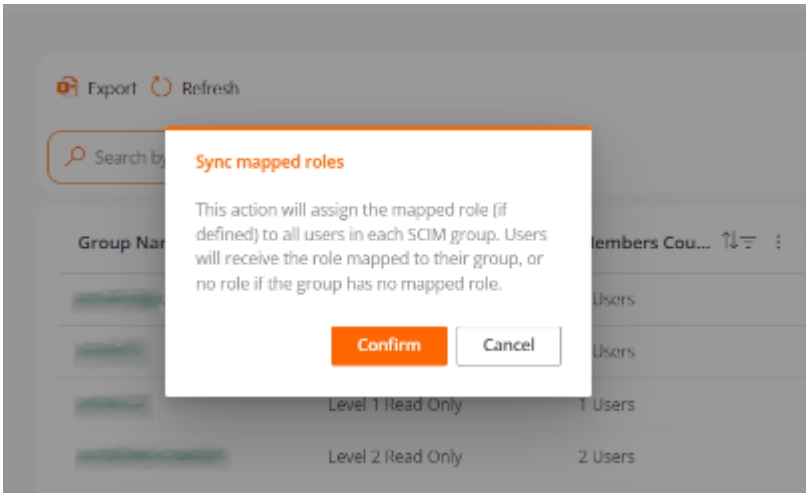


Role synchronization

The synchronization frequency depends on the identity manager used (for example, Entra ID synchronizes every 40 minutes), although manual synchronization can be forced from the identity manager itself for tests or urgent changes without waiting for the automatic cycle.

To avoid relying on those intervals, Portal includes the `Sync assigned roles` button, which allows aligning user roles belonging to groups created with SCIM.



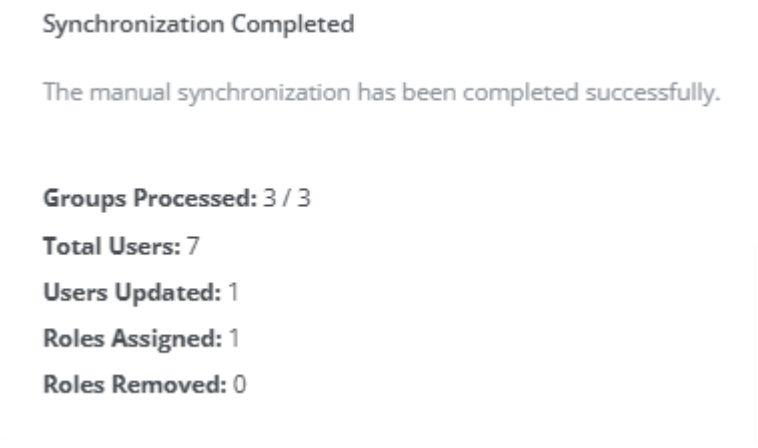


This action performs the following operations:

- Reviews all users belonging to groups created via SCIM.
- Checks if the role assigned to each user matches the role mapped for their group.
- If discrepancies are detected, it automatically updates the user's role.

If the role belongs to another sub-organization, the user will automatically move to the corresponding sub-organization.

At the end of the process, a detailed summary of the modified data is displayed.



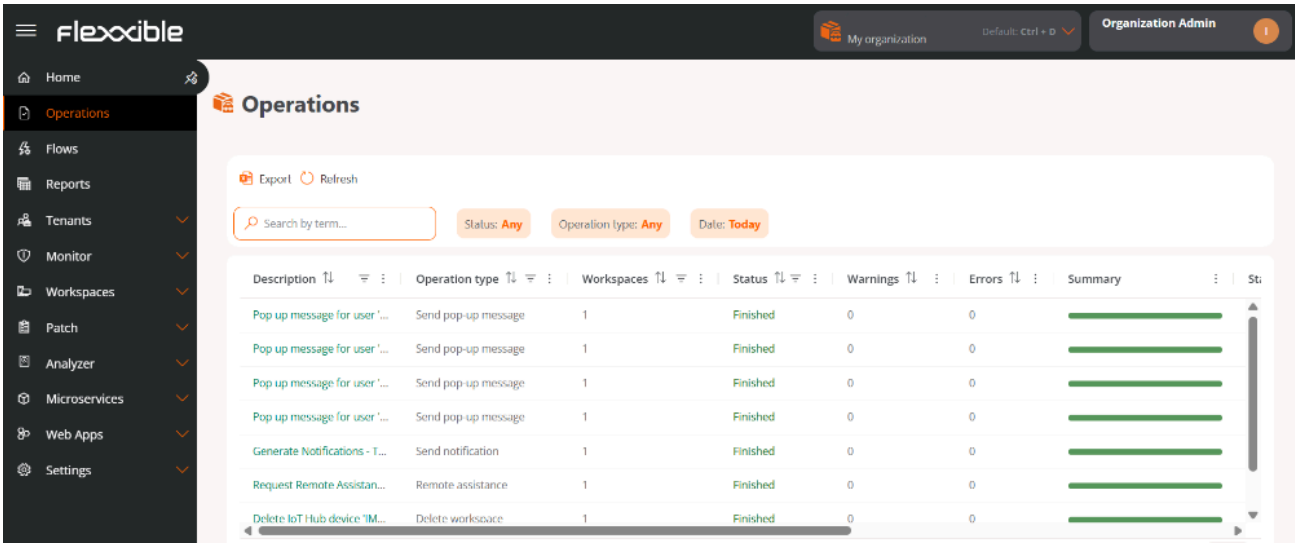
INFO

It is not necessary to execute the `Sync assigned roles` action regularly. It is recommended to use it only when making a change to mapped roles.

Portal / Operations

Operations allows you to view and manage actions executed on devices in the environment. It's the main information source for monitoring the execution, status, and result of operations.

Through a dynamic table, users can look up detailed info on each operation, its status, origin, type, and obtained results.



> **INFO**
>
> To access this functionality, you need to have version 25.12 or later of FlexxAgent installed.

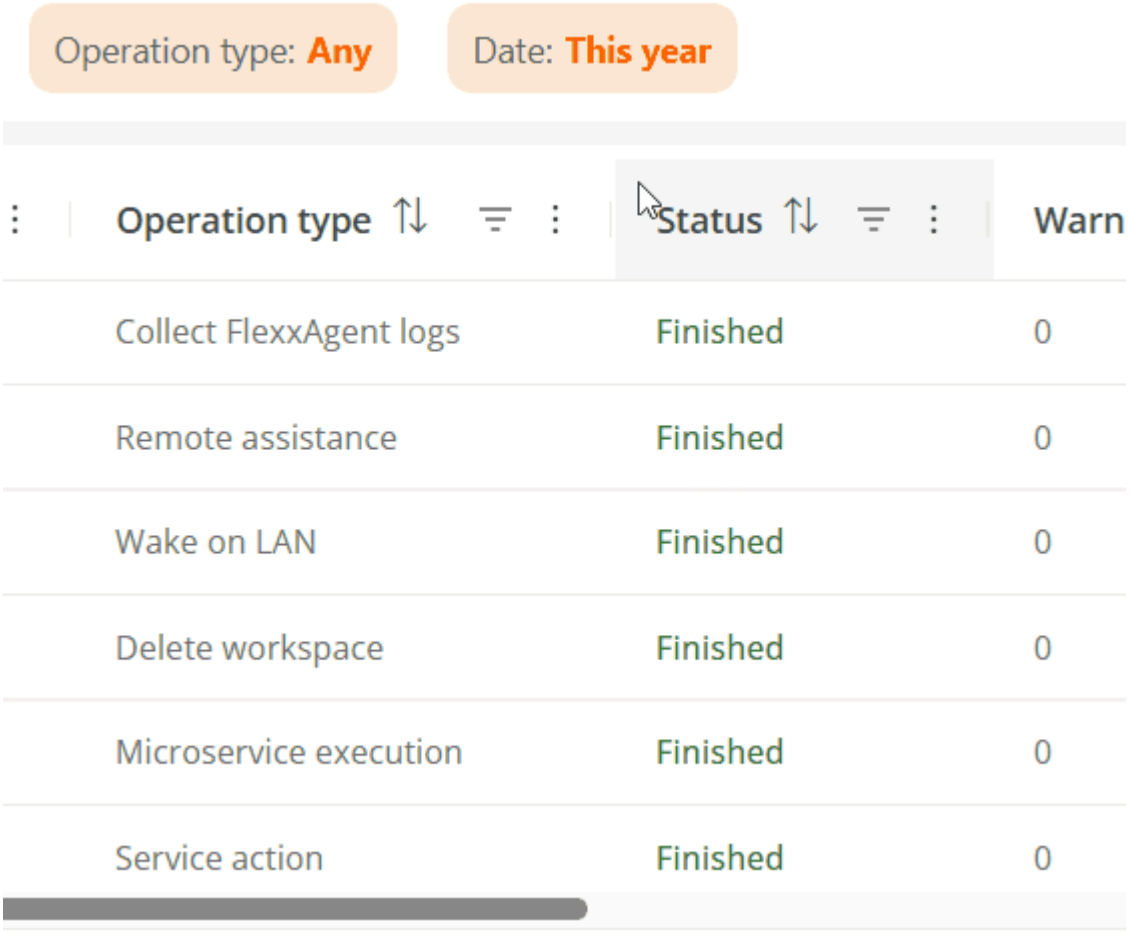
Table info

Each record in the table represents an operation and includes the following fields:

- **Description.** Brief explanation of the operation performed.
- **Workspaces.** Number of devices that executed the operation.
- **Operation Type.** Name of the executed operation.

- **Status.** Current execution status: *In Progress*, *Error*, *Complete*, and *Pending*.
- **Warnings.** Number of warnings recorded during execution.
- **Errors.** Number of errors detected.
- **Summary.** Visual indicator of the operation result:
    - Green: Complete
    - Yellow: Pending
    - Red: Error
    - Gray: Unknown
- **Initiated by.** User who executed an operation.
- **Started At.** Date and time of the start.
- **Ended At.** Date and time of completion.
- **Created at.** Date and time of the record creation.

Through the `Choose columns` option, the user will be able to choose to view additional fields to access detailed information.

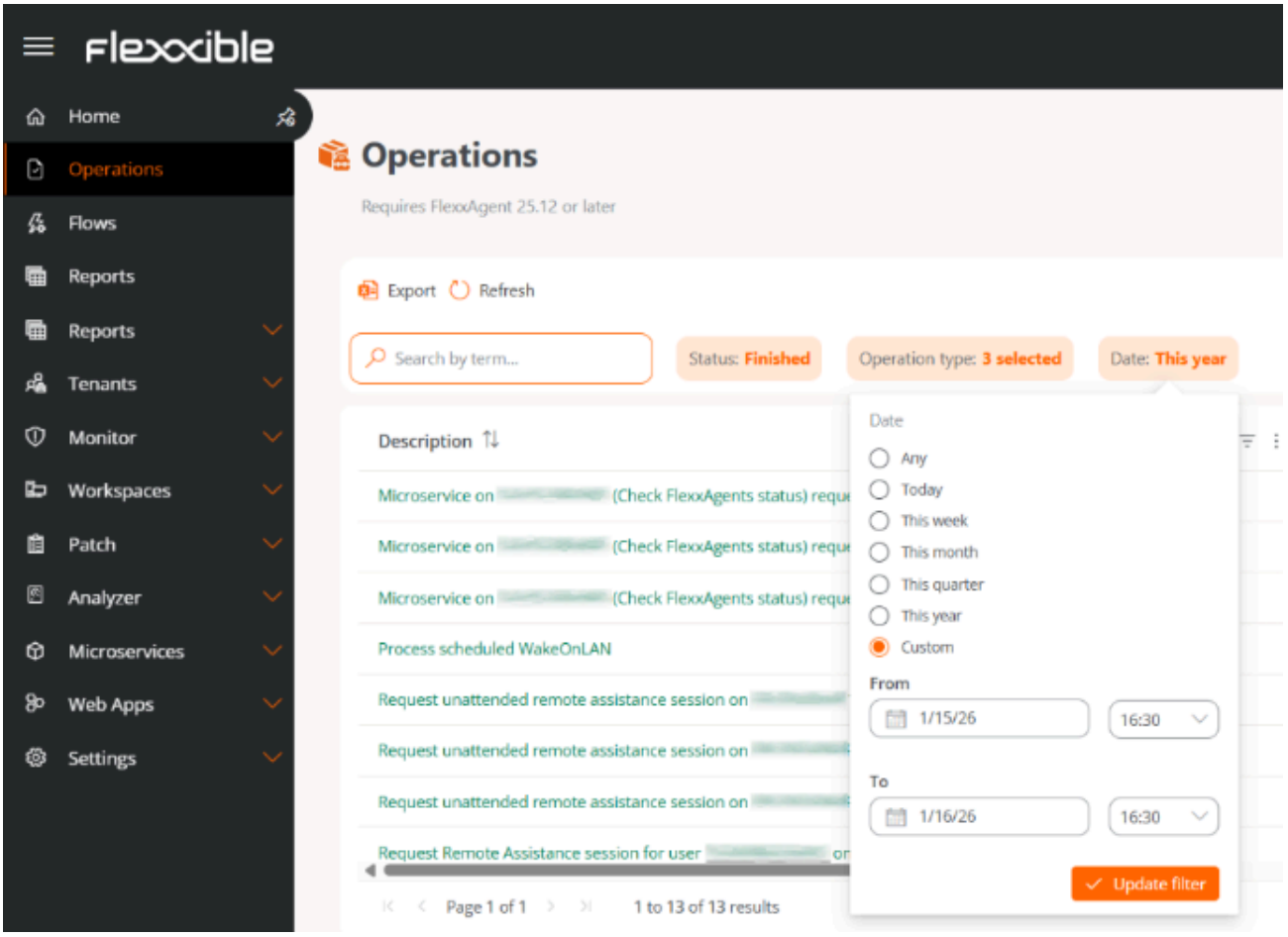


Available filters

The operations table allows filtering the results by the following criteria:

- State
- Operation Type
- Date

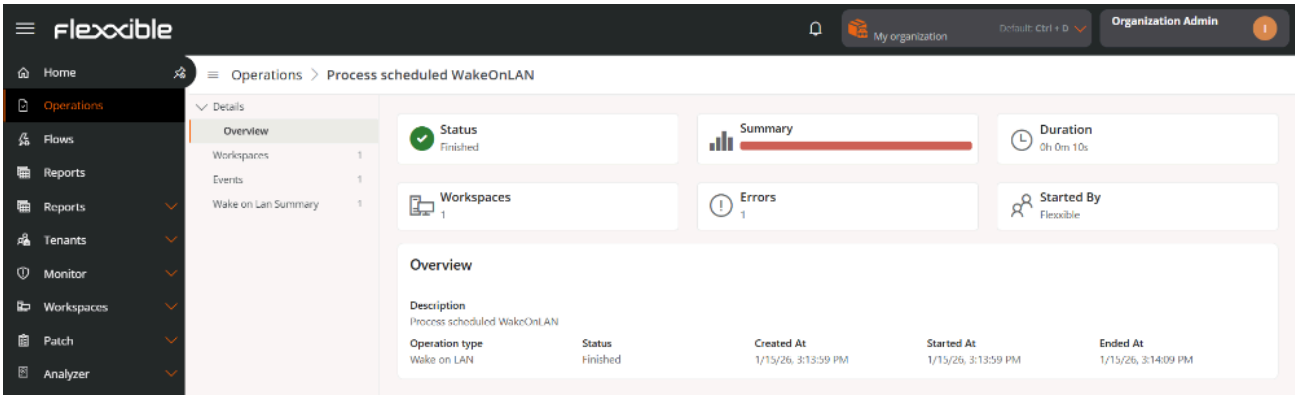
These filters make it easier to locate and analyze specific operations.



Operation details

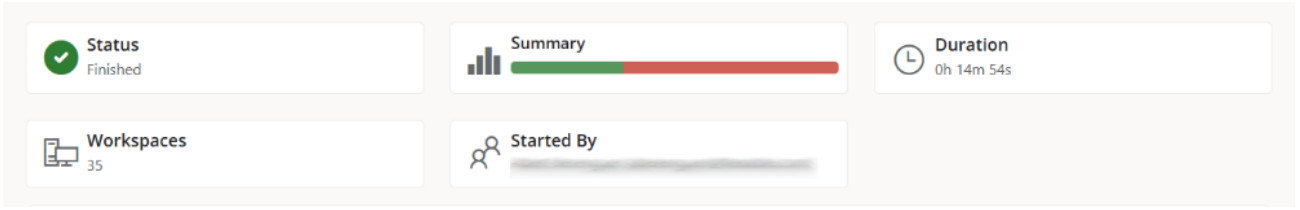
Selecting an operation from the table takes you to its detail view composed of the following tabs:

- Details
- Workspaces
- Events
- Wake on LAN Summary

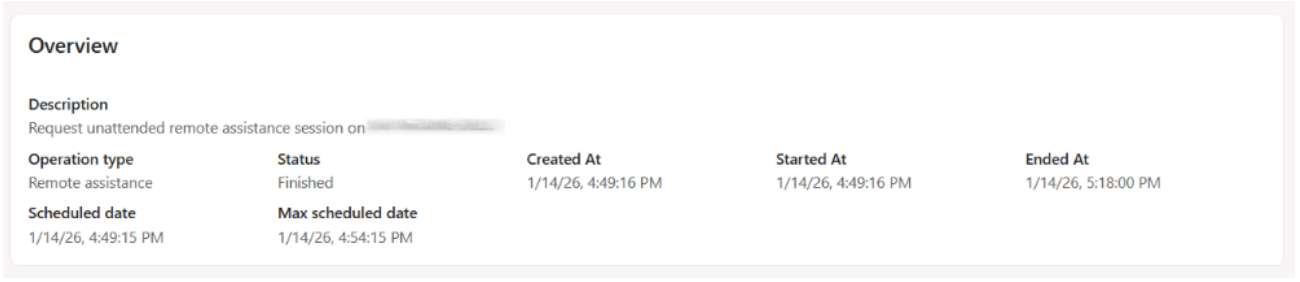


Details

This tab shows summary cards with the main data of the operation:



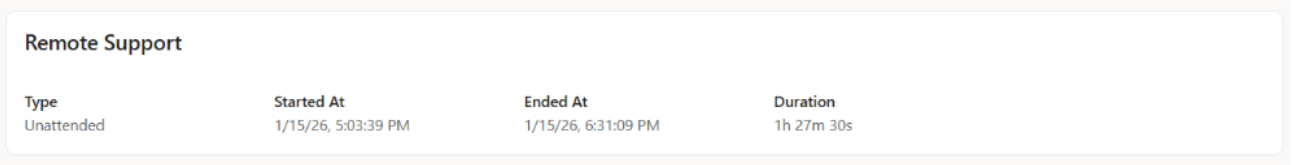
Next, the **Overview** section offers more details of the operation:



- Caption
- Operation Type
- State
- Created at
- Started At
- Ended At

Remote Assistance

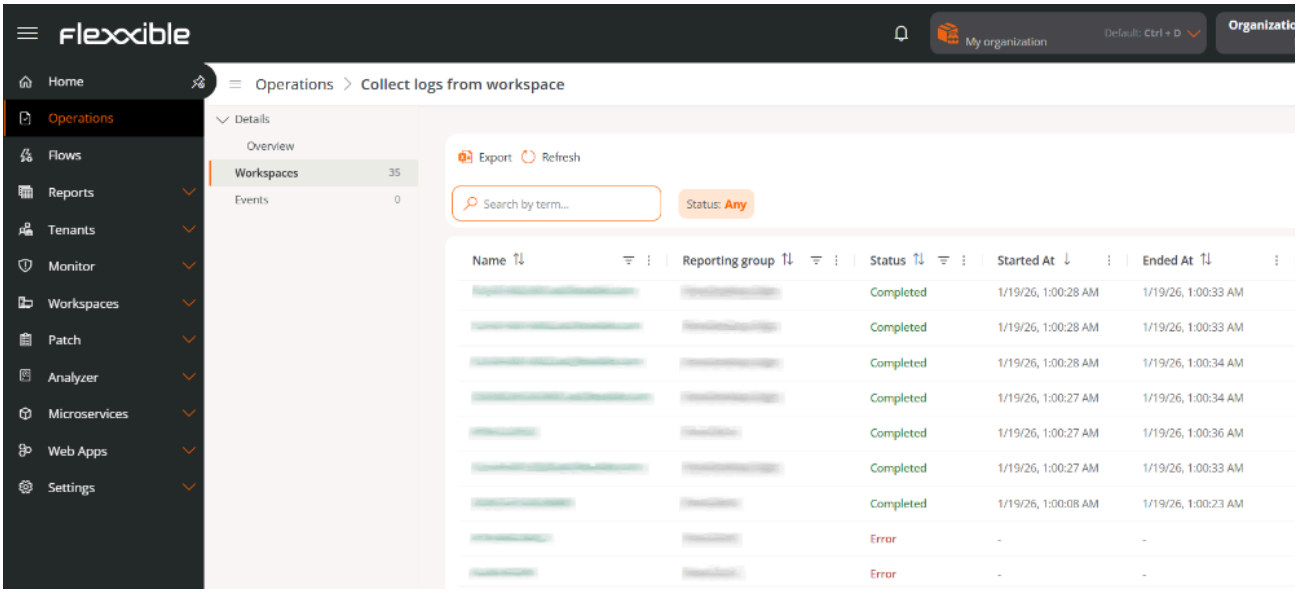
If the operation corresponds to a remote assistance session, this section is enabled with the following information:



- **Type.** Indicates whether it's interactive (attended), dynamic, or unattended.
- **Started At.** Start date and time of the assistance.
- **Ended At.** Date and time of completion.
- **Duration.** Total session time.

Workspaces

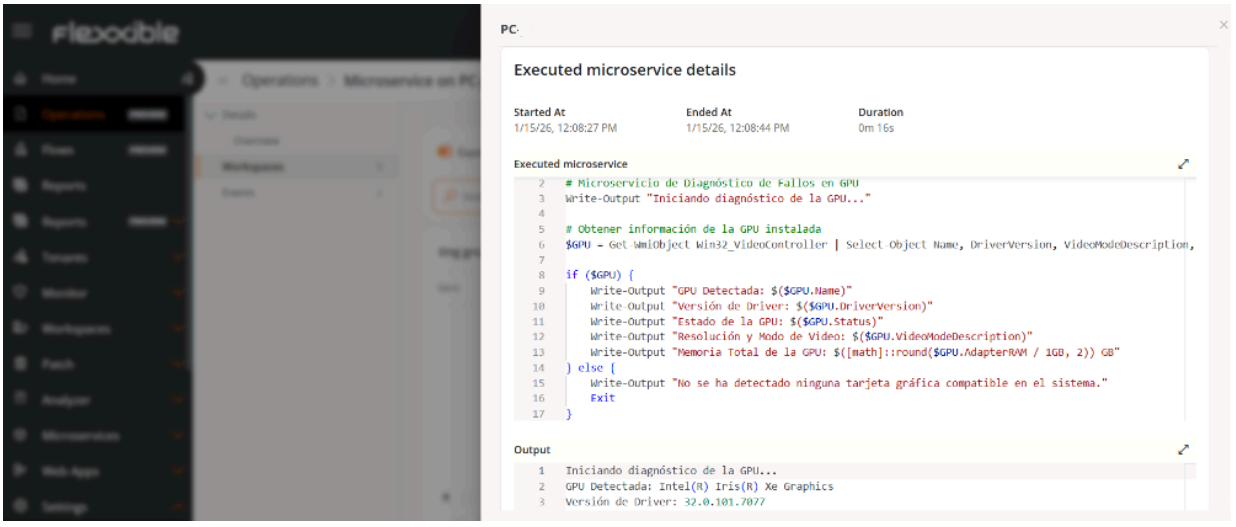
This tab displays a table listing the devices where the operation was executed.



The information for each record includes:

- **Name.** Device identification. Clicking opens its detail view.
- **Report group.** Reporting group to which it belongs.
- **Status.** Current execution status on that device.

- **Started At.** Date and time the operation started.
- **Ended At.** Date and time of completion.
- **Actions.** Allows access to detailed execution in operations of type *Flows*, *Microservices Execution,* and *End-user Microservice.*

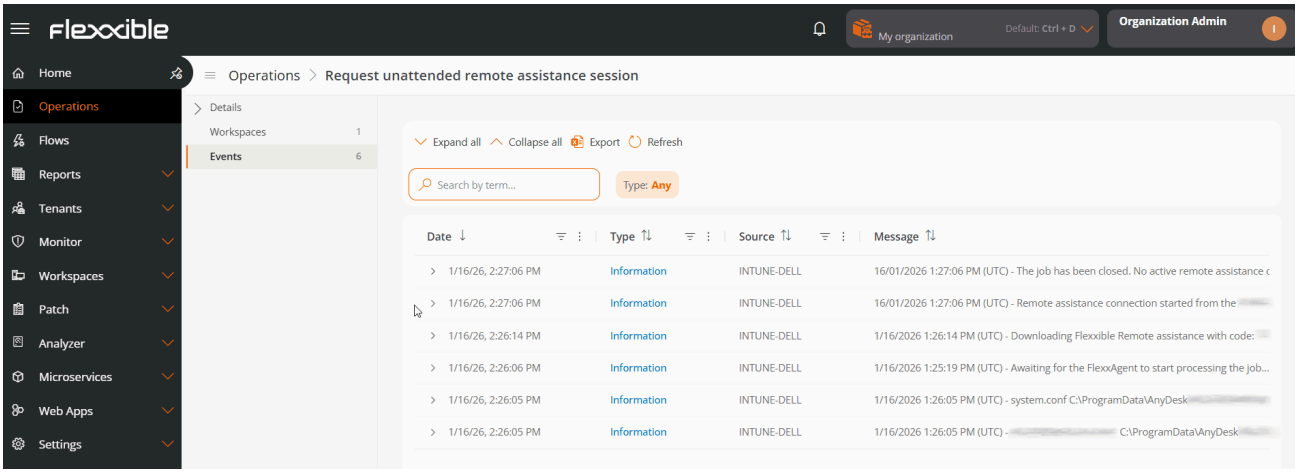


Events

This tab presents the events associated with the operation generated by the system:

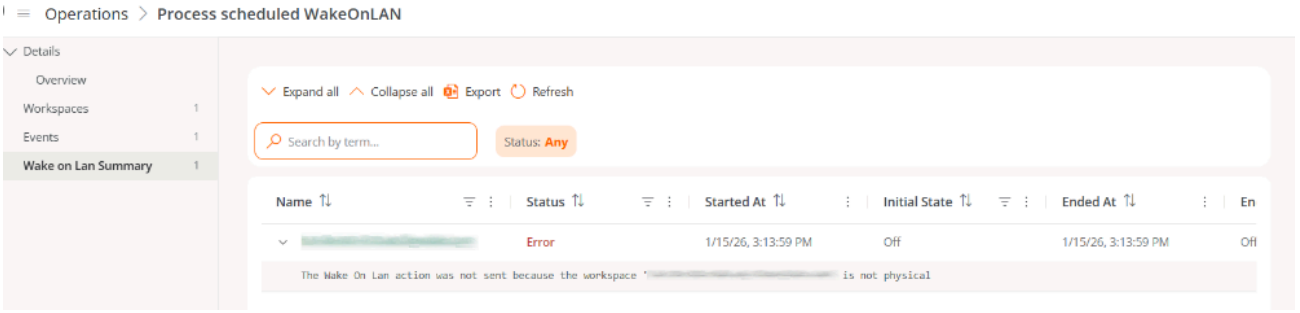
- **Date.** Date and time the event was recorded.
- **Type.** Can be *Information*, *Error*, or *Critical*.
- **Origin.** System component that generated the event.
- **Message.** Detailed description of the event.

The records in the table are expandable, allowing you to view the full message and facilitate analysis.



Wake on LAN Summary

This tab provides a comprehensive overview of Wake on LAN operations, allowing you to monitor the status and results of automatic device startups. Thanks to this view, you can track faster and more effectively, significantly reducing the diagnosis time for incidents, especially in operations involving a large number of devices.



The table includes the following information:

- **Name.** Name of the device attempted to be turned on.
- **Status.** Status of the power-on operation.
- **Started At.** Date and time the operation started.
- **Initial State.** Power status of the device at the start of the operation.
- **Ended At.** Date and time of completion.
- **Final State.** Power status of the device at the end of the operation.
- **MAC Address.** Unique physical identifier of the device's network card.
- **Subnet.** Network range of the device.

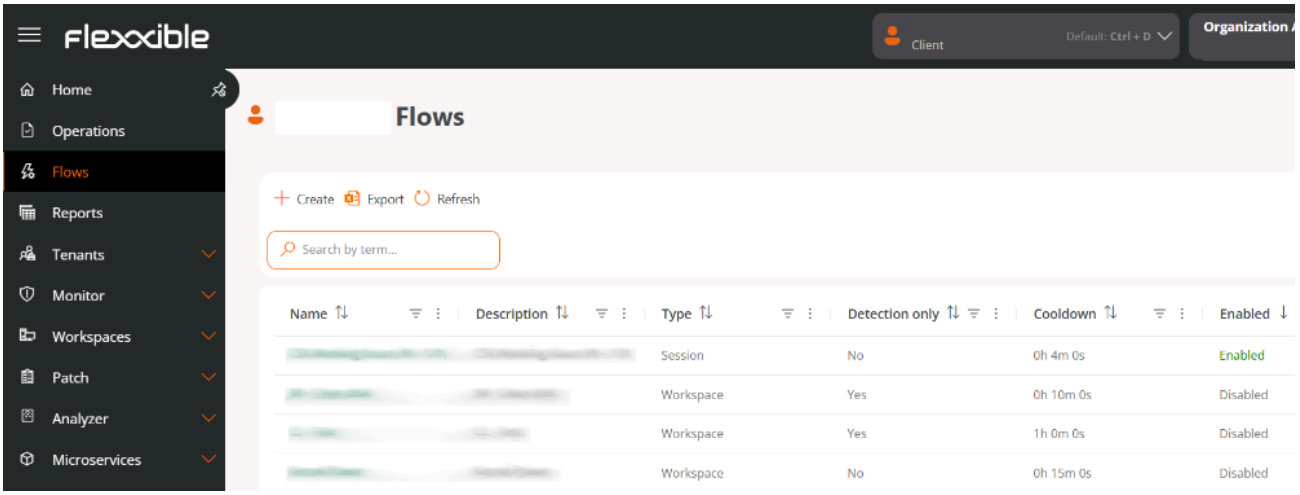
From the `Choose columns` option, as in the operations listing table, the user can view additional fields related to Wake on LAN, such as information on intermediary devices, logs, or the ID of the auto power-on schedule.

The records of this table are also expandable, allowing detailed consultation of each operation's diagnosis.

Portal / Flows

Flows is a feature that allows defining automation sequences to execute scheduled actions on devices based on the evaluation of pre-established logical conditions.

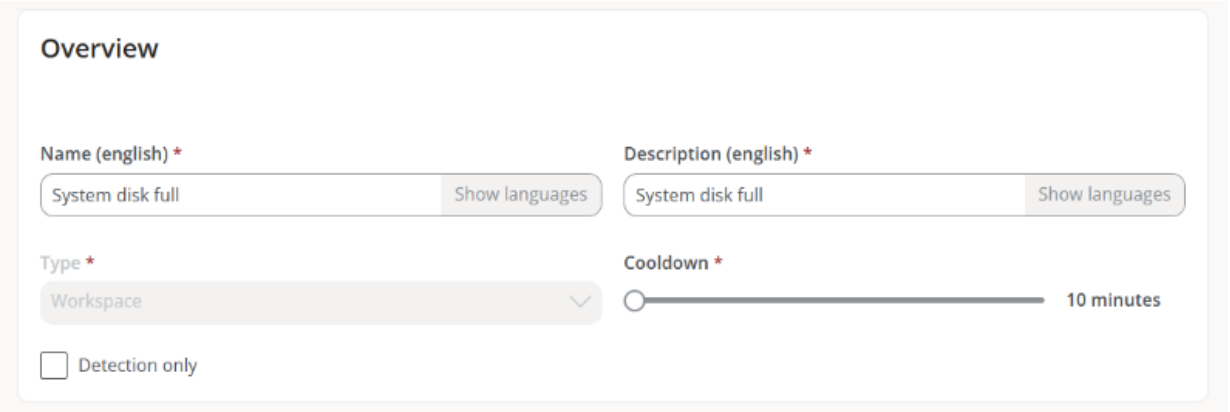
This tool simplifies proactive diagnostic actions, quickly resolves issues when focused on detection and offers a very efficient way to enable mechanisms for self-remediation in recurring incidents. It also allows technical teams to align devices with the configurations defined by the organization, evaluating them periodically and adapting when required.



The list view presents the flows created in the organization, along with the following information:

- **Name.** Name of the flow.
- **Description.** Purpose of the flow.
- **Type.** Execution scope of the flow, determined by the type of microservice you want to run. It can be done at the user session level, with the corresponding permissions, or at the device level, with administrative access.
- **Detection only.** If enabled, this means that the conditions will be evaluated in a "sampling" mode to detect those devices where they are met, but the defined microservice will not be executed.

- **Cooldown.** Defines the minimum period that must pass before a condition is re-evaluated after it has been fulfilled and an action executed:
    - When a flow condition is met, an action is executed.
    - Begin counting the cooldown.
    - During this time, it will not be re-evaluated whether the condition is met.
    - Once the period has passed, the condition will be evaluated again.
- For example, if the cooldown is set for 24 hours, the condition will be evaluated and executed (if met) once a day, even if the condition remains active.
- The cooldown does not apply when the action is a microservice that restarts the device. In this case, if the condition is met, the action is executed without waiting.
- The minimum configuration parameter for reuse time is 10 minutes.



> **INFO**
>
> If FlexxAgent or the device is restarted, the cooldown timer is interrupted and starts from zero.

- **Enabled.** Indicates if the flow is *Enabled* or *Disabled*.

By clicking on a table record, you access the details of its configuration:

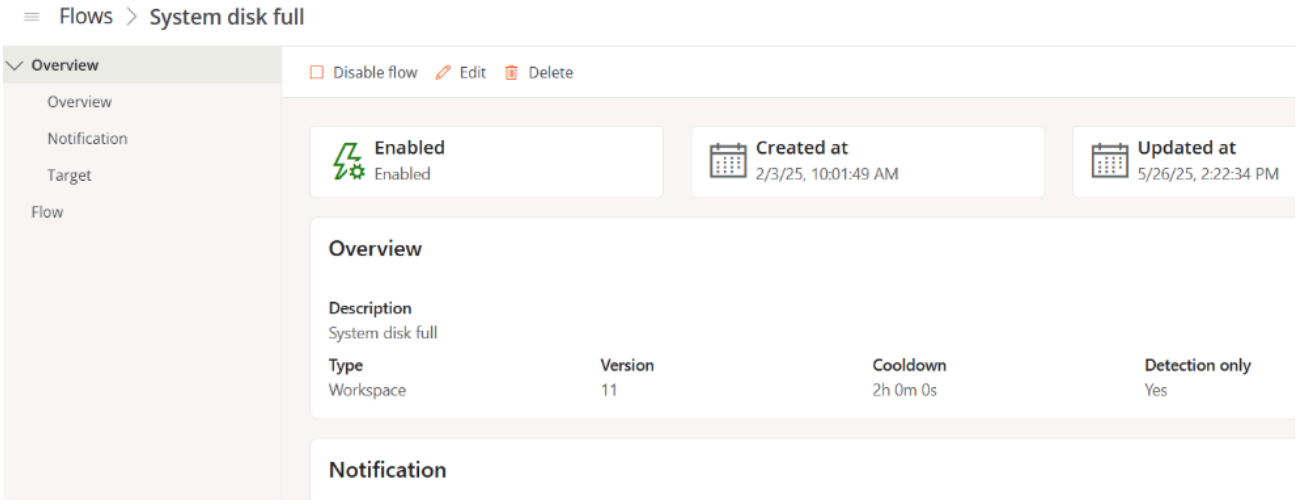
- Overview
- Flow

Above the table, the `New` button allows you to create a flow. For more information, please check this guide.

Overview

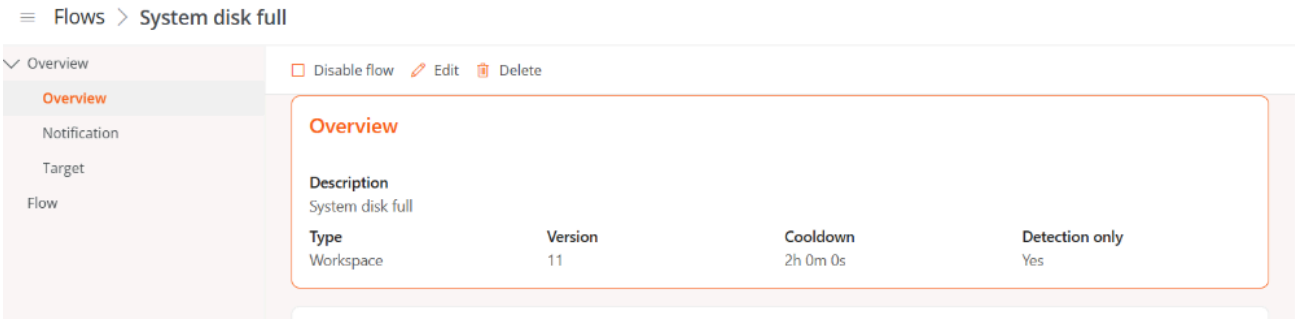
Stores the flow configuration data. It is divided into three tabs:

- Overview
- Notification
- Target



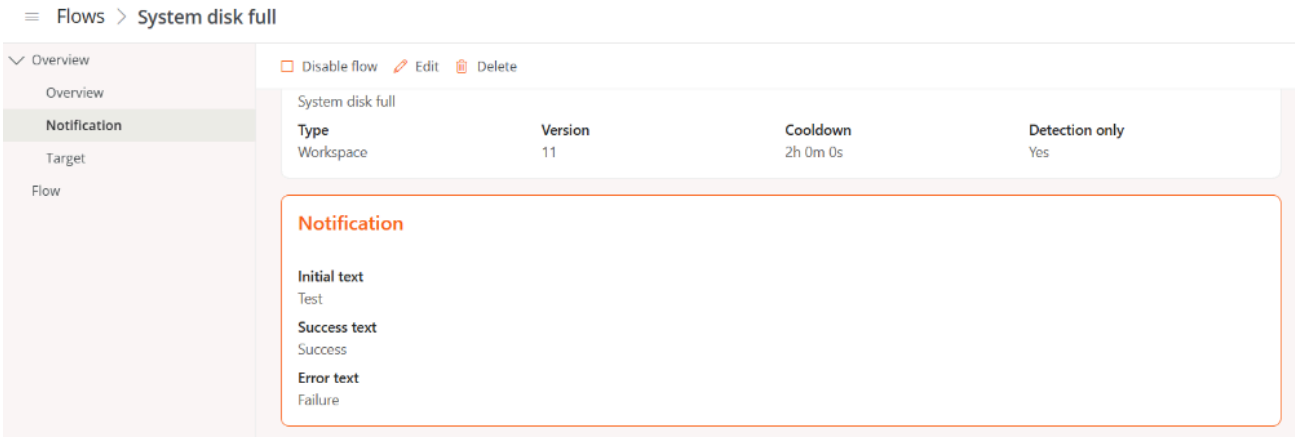
Overview

Provides general flow information: *Description*, *Type*, *Cooldown Time* and if it is set to *Detection Only*. It also reports on the *Version*, which increments by one each time the flow is edited.



Notification

Details the notifications that the operating system will send to users at the start and end of the flow executions.



- **Initial text.** Content of the notification that will be sent to users at the start of the execution.
- **Success text.** Content of the notification that will be sent to users after a successful execution.
- **Error text.** Content of the notification that will be sent to users after an execution with errors.

Target

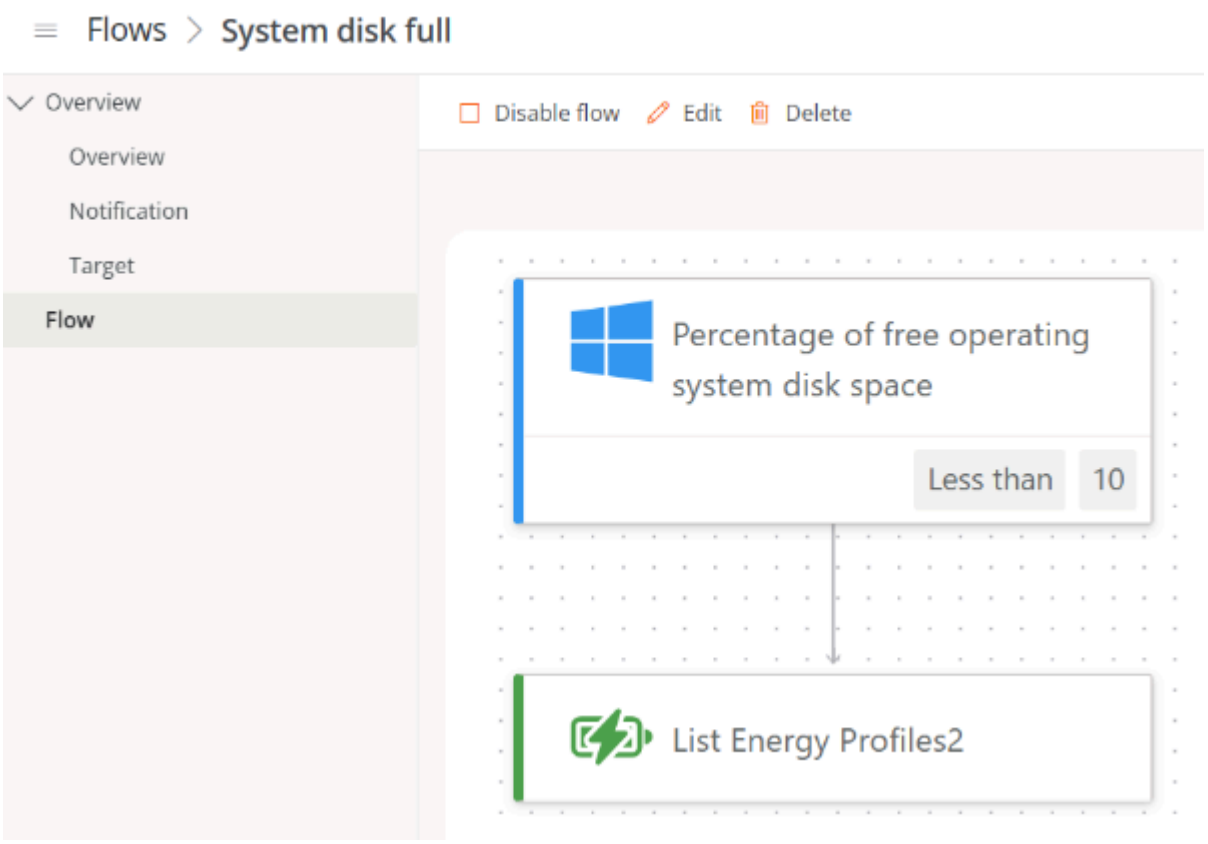
Specifies the devices or groups of devices where the flow will be executed.

- **All workspaces.** All devices in the organization.
- **Workspaces.** Specific devices.
- **Workspace groups.** Specific workspace groups.
- **Report groups.** Specific report groups.

Flow

Shows the flow diagram: the conditions to evaluate, the required thresholds, and the action that will be executed on the device if the parameters are met.

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



Flow conditions

Flow conditions allow you to define the criteria under which the automated actions will trigger. All conditions described below are compatible with devices operating with the Windows operating system.

Existence of an ongoing process

Performs periodic evaluations to verify if a process is running, with adjustable 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:

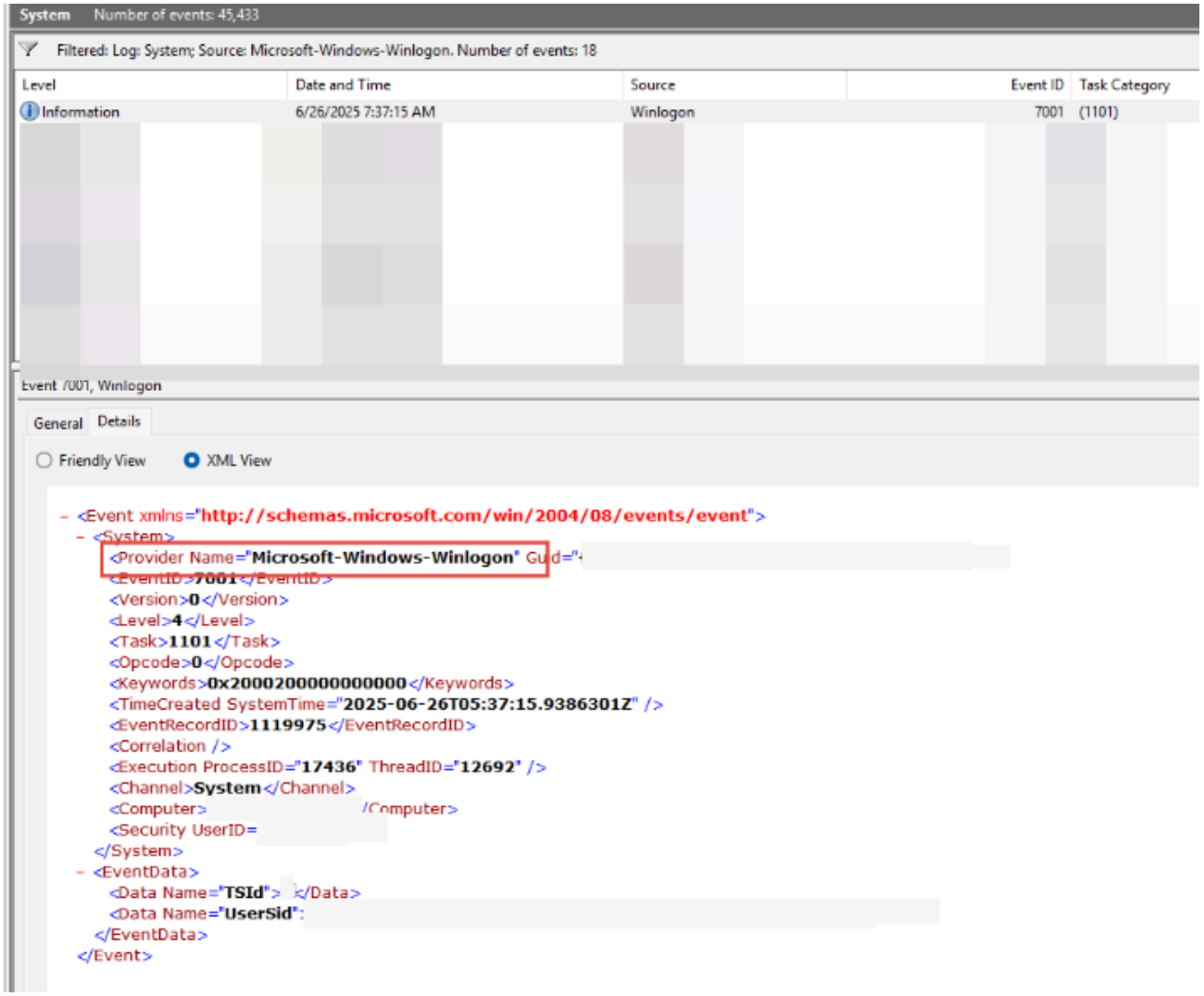
`<logName>:<Provider>:<id>`

Example:

System:Microsoft-Windows-Winlogon:7001

Where:

- logName = System
- Provider = Microsoft-Windows-Winlogon
- id = 7001



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.

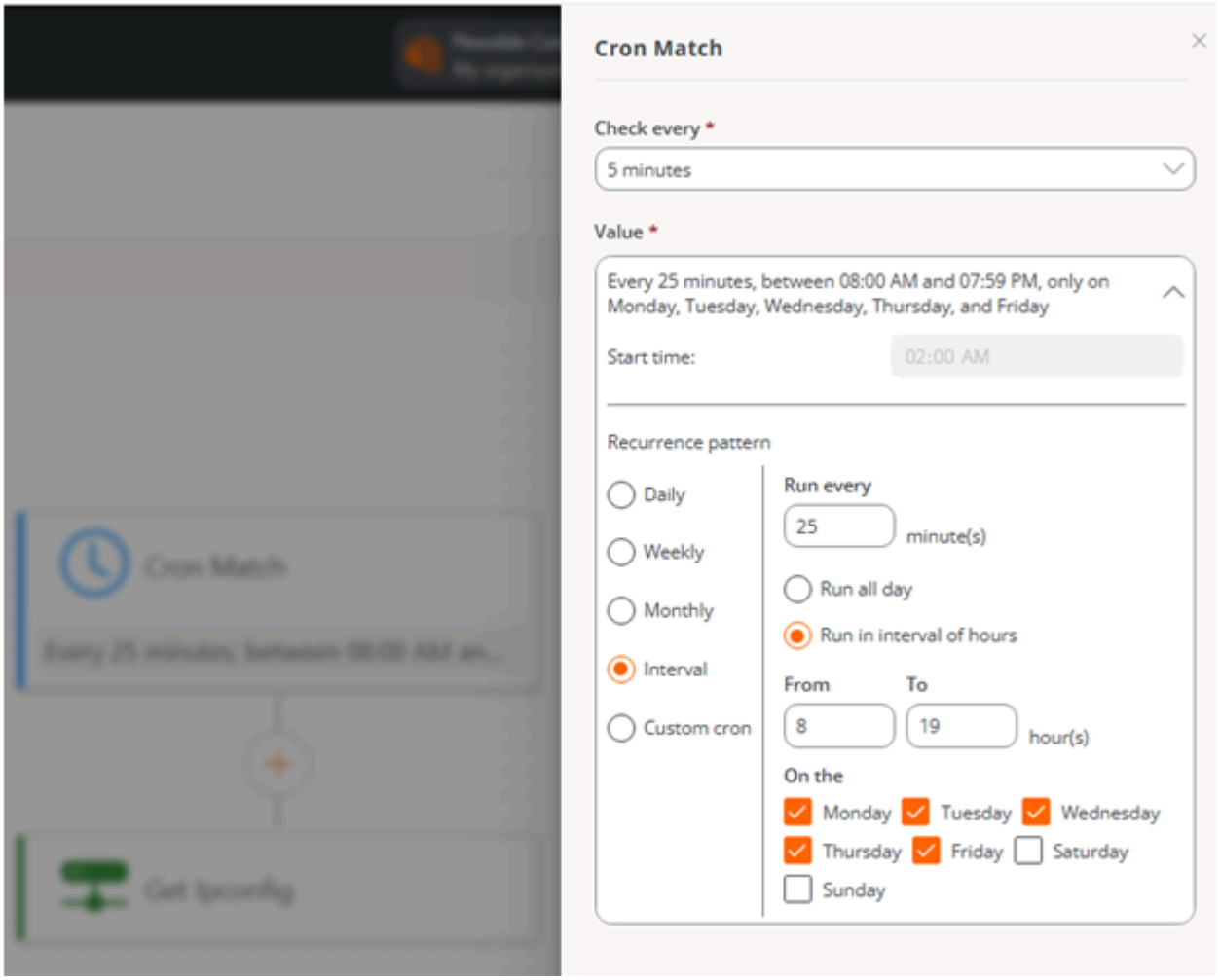
Cron Match

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 how often the system will evaluate if the schedule is met. This value must be adjusted according to the indicated schedule.
- **Value.** Allows you to configure the schedule, periodicity, and recurrence that will determine when the action will be executed.

The form allows you to define a *Recurrence Pattern* through the following options:

- **Daily.** Indicates what time and every how many days the action should be executed, as well as whether it should only be performed from Monday to Friday.
- **Weekly.** Lets you define what time, every how many weeks, and on what days of the week the action will be executed.
- **Monthly.** Sets what time and on what day of the month the action will be executed.
- **Interval.** Determines how many minutes between each execution of the action within a day or a specific time range.
- **Custom Cron.** Allows manual entry of a string in the standard cron format, useful for custom and advanced configurations.



At the top of the form, a summary (in text) of the scheduled configuration is displayed to confirm that it is the desired one.

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 the standard UTC time.

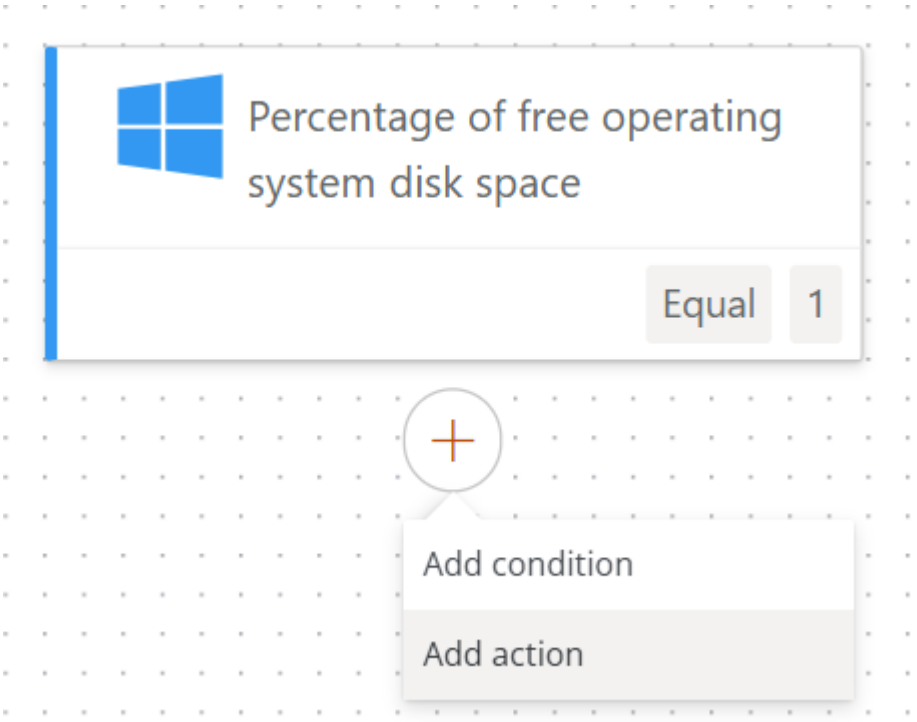
There are many references available to check the cron scheduling syntax. For example: crontab.guru

> **INFO**
>
> If you wish to implement custom flow conditions — such as evaluating uptime in days, checking the current status of services, or any other parameter that can be analyzed locally from the device — please consult with Flexxible.

Action's

Actions are the microservices that have been programmed to automatically run when the predefined flow conditions are met.

To add an action when creating or modifying a flow, click on the corresponding condition and then select `Add condition` to choose one of the available microservices.



The microservices will only appear in the list if they are enabled for the organization. For more information on how to enable them, please consult the Microservices documentation.

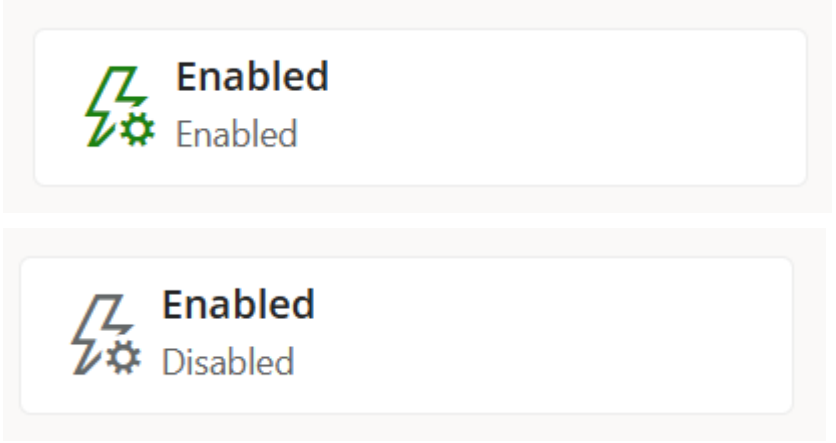
Flow Management

Once a flow is created, it can be managed through the following options:

- Enable/Disable Flow
- Edit
- Delete

Enable/Disable Flow

Allows activating or deactivating the flow within an organization. The current state of the flow can be checked from the table containing the flow list or in Overview.

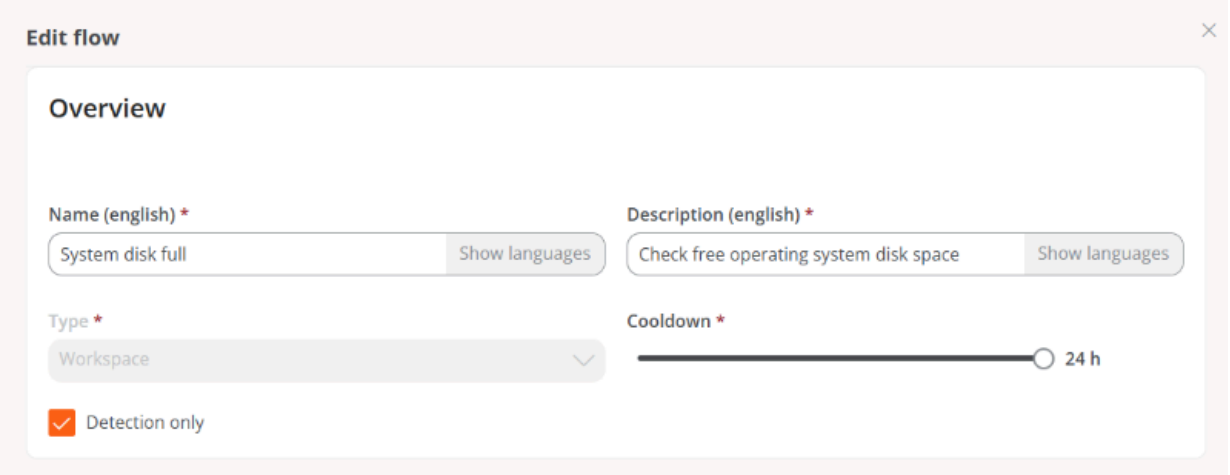


Edit - Overview, Notification, and Target

Clicking on `Edit` from the Overview, Notification, or Target tabs allows you to modify settings defined during the creation of the flow.

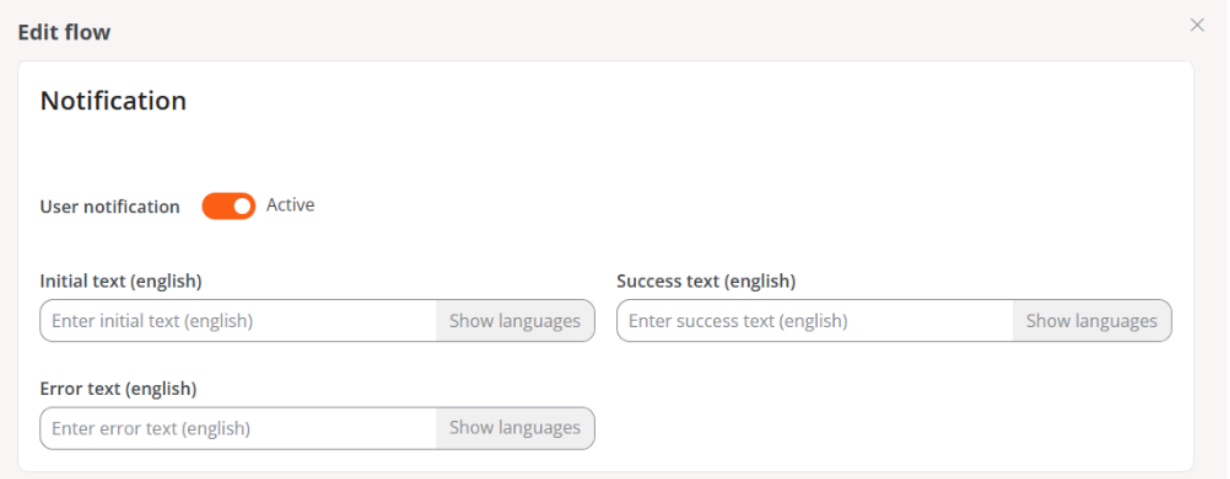
- Overview

  Allows editing the name of the flow, its description, execution scope, reuse time, and the option to execute or not the microservice once the conditions are met. Each field is explained in the Overview section and in the guide Schedule microservices execution.



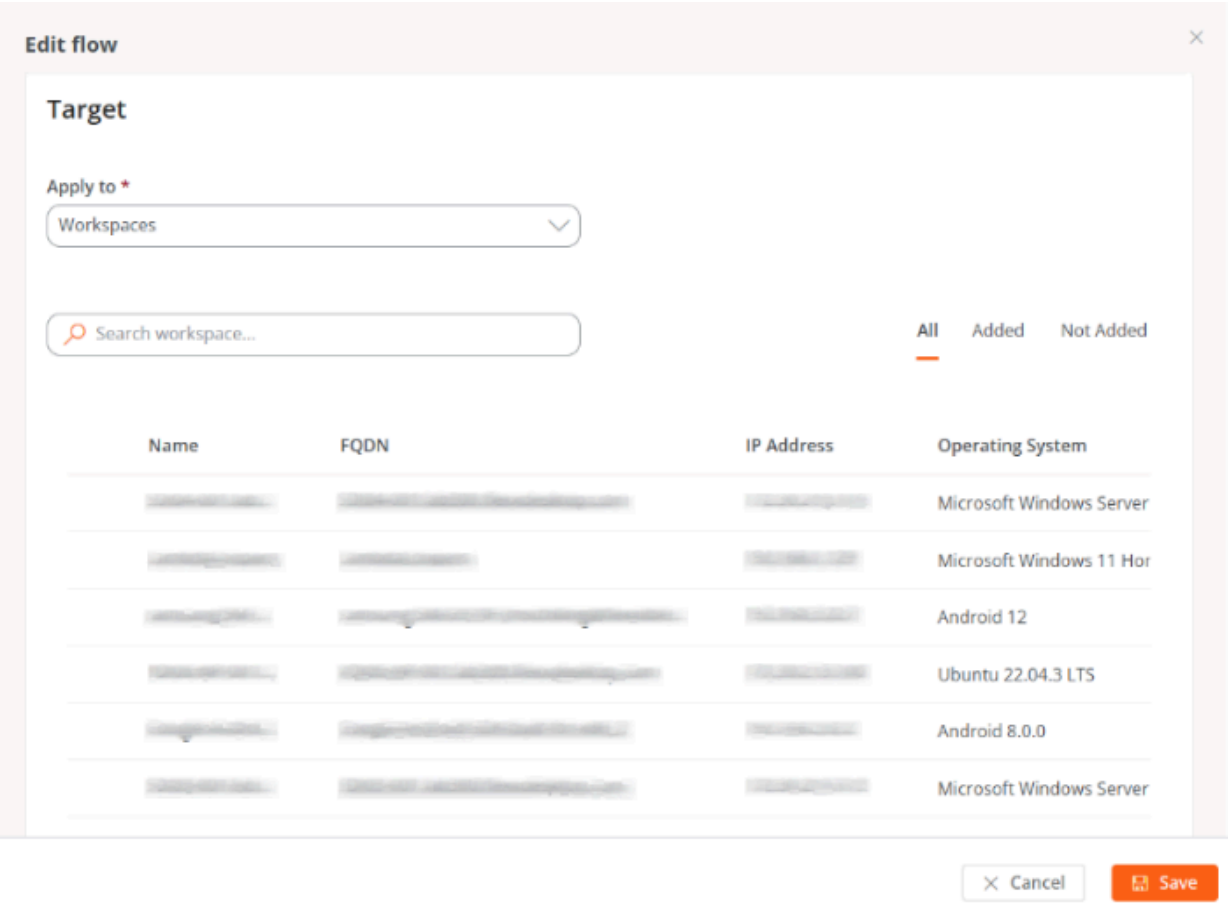
- Notification

  Allows enabling or disabling sending notifications to users and editing their content. The available message types are explained in the Notification section and in the guide Schedule microservices execution.



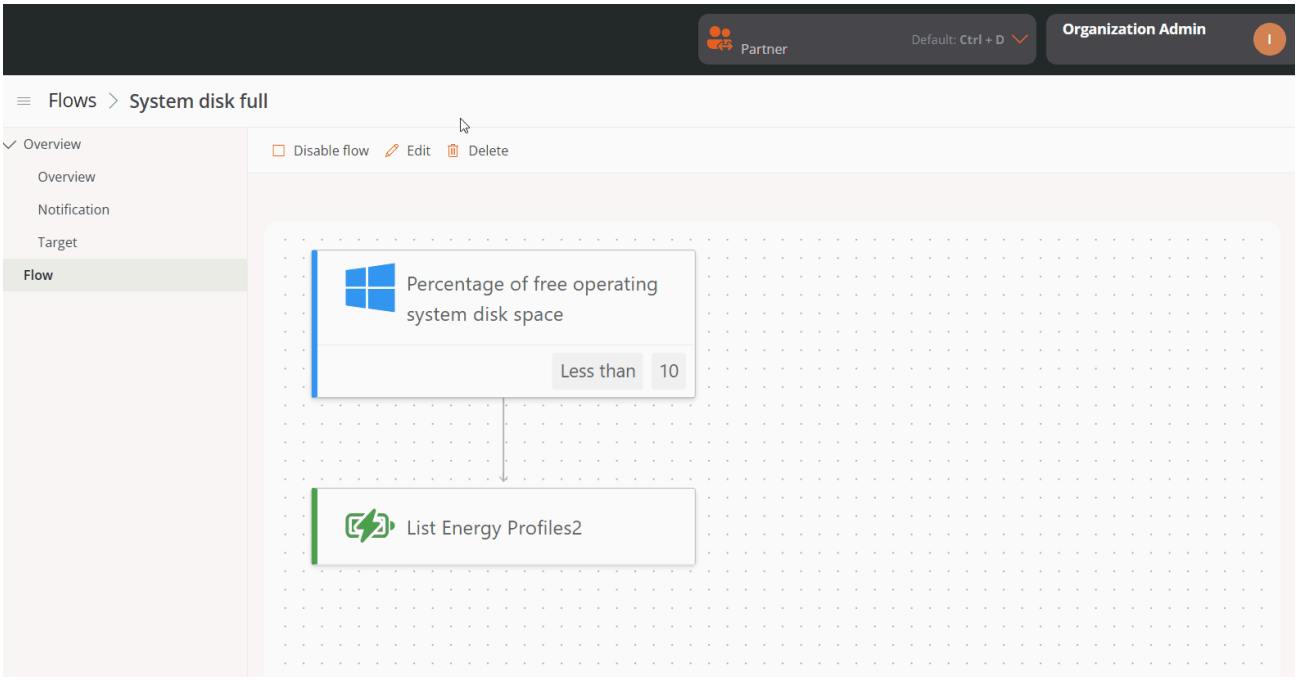
- Target

  Allows defining the target devices for the flow. From the `Apply to` button, you can choose whether the flow will apply to all devices in the organization, specific devices, workspace groups, or report groups.



Edit - Flow

If you click on `Edit` from the Flow tab, you will be able to modify the conditions and actions that make it up.

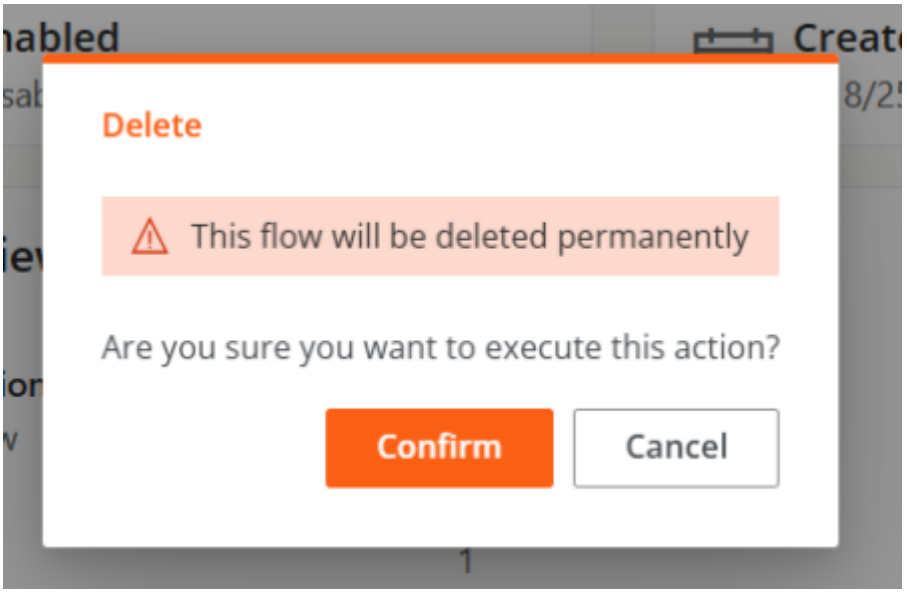


INFO

Changes made in a flow can take up to 15 minutes to apply to all linked devices.

Delete

Allows permanent removal of the flow.



Portal / Reports

The **Reports** system offered by Portal allows users with the role of *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.

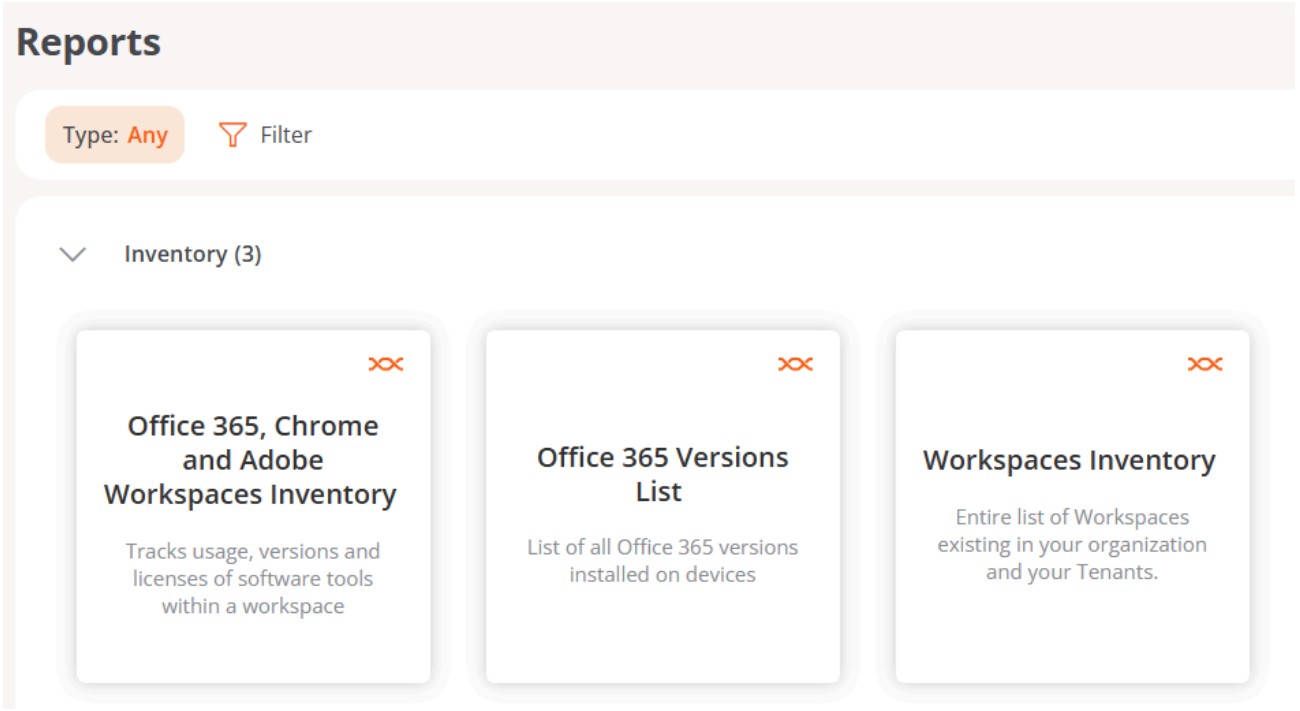
Considerations

- They are automatically generated once a week.
- Historical reports will remain available in Portal for two months.
- It's possible to configure the automatic sending of reports, so that by specifying email addresses, the report is sent weekly.

Report inventory

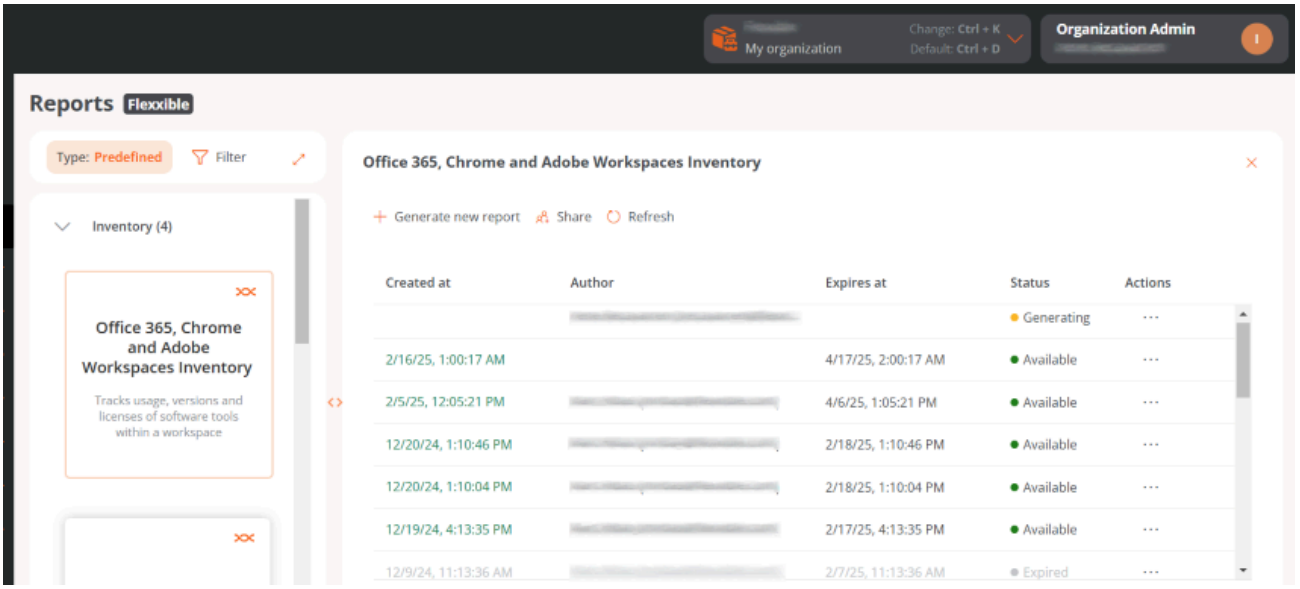
Portal offers three types of predefined reports:

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



The general table of report types displays the following information:

- **Created on.** Date and time 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.** Report expiration date and time.
- **Status.** Report status (*Available*, *Generating*, or *Expired*).
- **Actions.** Access to a menu of actions regarding the reports.
  - **View details.** Displays a table with the specific contents of the report.
  - **Download Excel.** Download the report in Excel format.
  - **Download CSV.** Download the report in CSV format.
  - **Share.** Allows the report to be sent via email.
  - **Delete report.** Deletes the report.



Office 365, Chrome and Adobe Workspaces Inventory

Shows usage tracking, versions, and licenses of Office 365, Chrome, and Adobe on devices. The 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 (in megabytes).
- **Disk used (%).** Percentage of system disk occupancy.
- **Total disk capacity.** Total disk capacity (in gigabytes).
- **Operating system** Type of operating system.
- **Microsoft 365.** Installed Office version.
- **Google Chrome.** Installed Google Chrome version.
- **Adobe Acrobat.** Installed Adobe Acrobat version.
- **Last user.** User of the last session detected on the device.
- **Created on.** Date of report execution (creation).
- **Date of last report.** Date of execution (creation) of the last report.

Office 365 Versions List

Generates a list of installed Office 365 versions on the organization's devices and, for each one, presents the number of devices containing it.

Workspaces Inventory

Displays a list of existing devices in the organization and their 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.**: Operating system name.
- **Motherboard manufacturer.** Name of the motherboard manufacturer.
- **Motherboard model.** Name of the motherboard model.
- **BIOS Manufacturer.** Manufacturer of the basic input/output system (BIOS).
- **Processor.** Processor name.
- **CPU cores.** Number of central processing unit cores.
- **Regulatory compliance.** 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.** Antivirus status on the device.
- **BIOS mode.** BIOS mode.
- **Organization.** Organization to which the device belongs.
- **Client version.** Installed version of FlexxAgent.
- **Country.** Country where the device is located.
- **Created on.** Date of device creation in Portal.
- **Active CrowdStrike detections.** Active detections from CrowdStrike.
- **CrowdStrike status.** *Installed and functioning*, *Not installed*, or *Unknown*.
- **CrowdStrike version.** Version number of CrowdStrike installed on the device.
- **Subnet.** Subnet in which the device resides.

- **Default gateway.** Default gateway.
- **Desktop type.** For VDIs, defines the desktop type.
- **EDR.** Type of Endpoint Detection and Response (EDR) detected on the device.
- **Farm/Cluster.** For VDIs, shows the farm to which it belongs.
- **Delivery group.** For VDIs, shows the delivery group to which it belongs.
- **Fast startup.** Shows if the device has Fast Startup enabled.
- **FLXMID.** Device identifier.
- **IP address.** Number of IP address 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 the 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.** Version number of the operating system.
- **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 for updates.
- **IoT Hub configuration sync.** *Synced* or *Not synced*.
- **Custom field 01.** Displays the content of the first custom field.
- **Custom field 02.** Displays the content of the second custom field.
- **Last restart.** Date of last device restart.
- **Last Windows update.** Date of the last Windows update applied.
- **Report Group.** Reporting group to which the device belongs.

Generate a report

Reports are automatically generated once a week; however, if you want one immediately, follow these steps:

1. Go to `Portal` -> `Reports` and select a report type in the inventory.
2. In the top menu of the table, click on `Generate new report`. In organizations with tenants, a modal window will open asking to select which tenant you want the report for. Once chosen, click `Generate`.

Generated reports are saved and can be downloaded and shared up to sixty days after they are created.

Share a report

This functionality allows sharing the last automatically generated report and specific reports (historical or generated by a user at the moment).

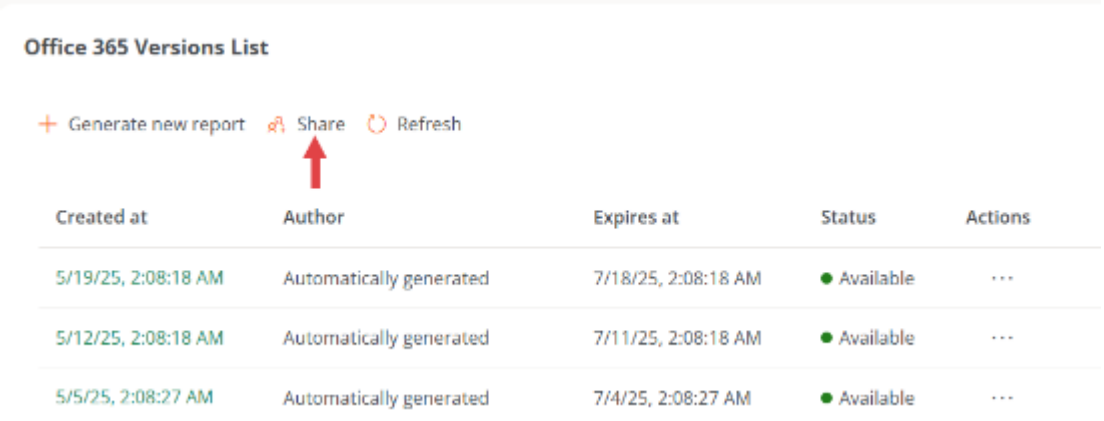
Reports can be shared with one or more recipients.

Share the last report

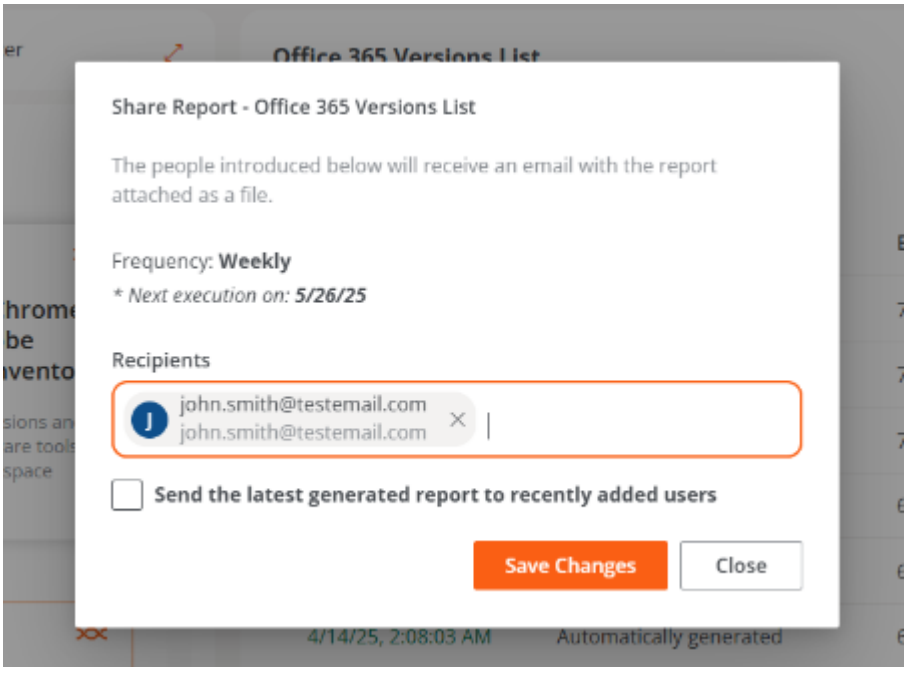
Allows automatic weekly sending of the most recent report to the recipients specified by the user.

1. Go to `Portal` -> `Reports` and select a report type in the inventory.

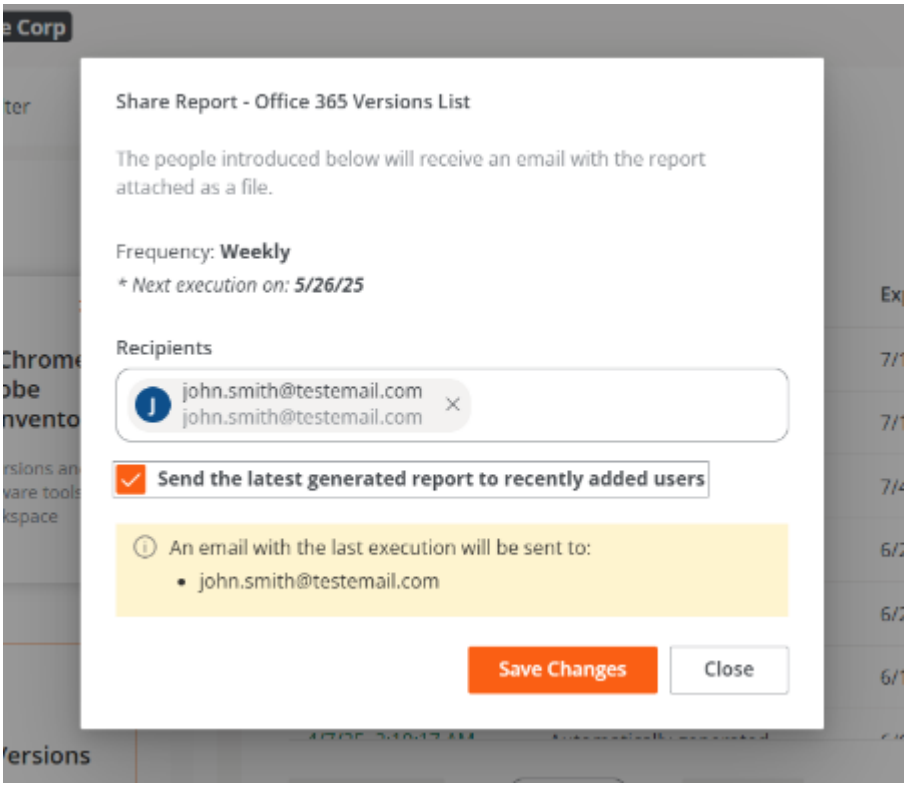
2. In the top menu of the table, click the `Share` button.



3. Enter the email addresses of the recipients, and press the `Enter` key on the keyboard to add them.



4. Activate the option `Send the last generated report to newly added users`.



5. Click `Save changes`. The recipient will receive the most recent report immediately. And from there, they will receive a report automatically every week.

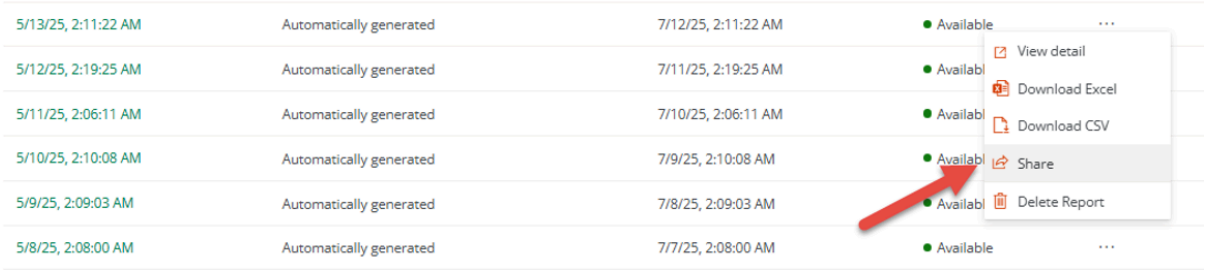
> **INFO**
>
> If email addresses are added and `Save changes` is clicked without selecting `Send the last generated report to newly added users`, the addresses will be saved correctly. This allows adding others later without losing the previous ones.

Delete a recipient

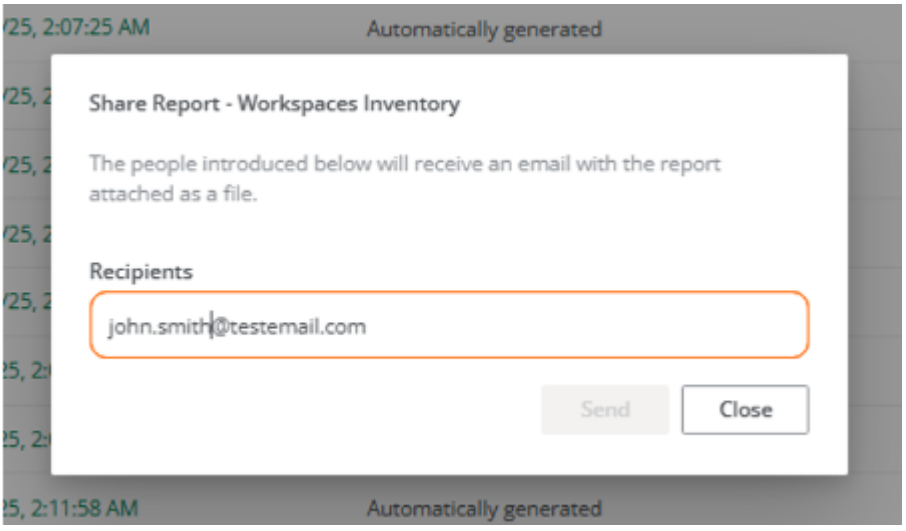
1. Go to `Portal` -> `Reports` and select a report type in the inventory.
2. In the top menu of the table, click the `Share` button.
3. Delete the recipient's address.
4. Click `Save changes`

Share a specific report

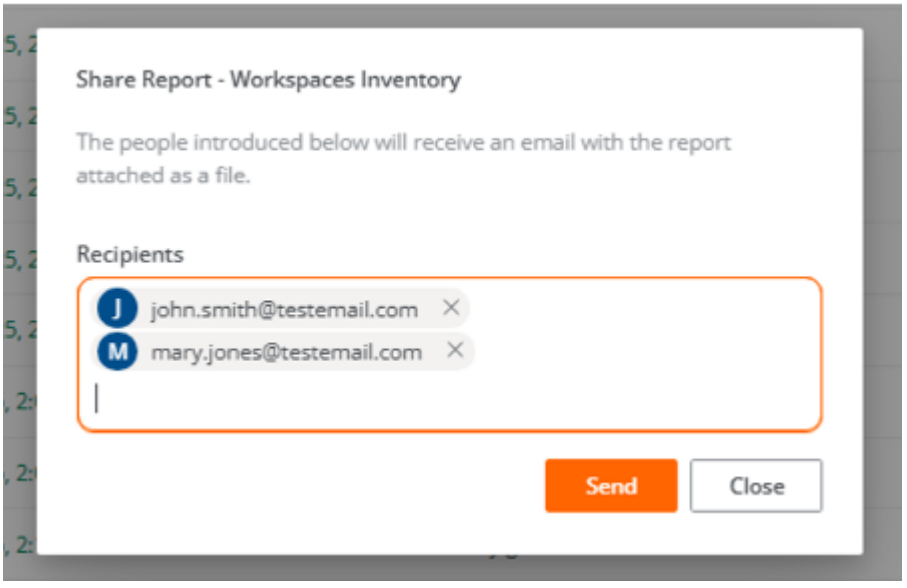
1. Go to `Portal` -> `Reports` and select a report type in the inventory.
2. In the table, choose the report you want to send and in the `Actions` field click `Share`.



3. Enter the email addresses.



4. Press the `Enter` key on the keyboard to add the addresses, after which the `Send` button will be activated.



5. Click `Send`.

Portal / Tenants

Through **Tenants**, organizations operating in the Managed Service Provider (MSP) model have the possibility of establishing subsidiary entities to which they can provide support whenever required.

These entities are other organizations, which in Portal are referred to as **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 fleet of devices, regardless of who management has been delegated to.
- 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

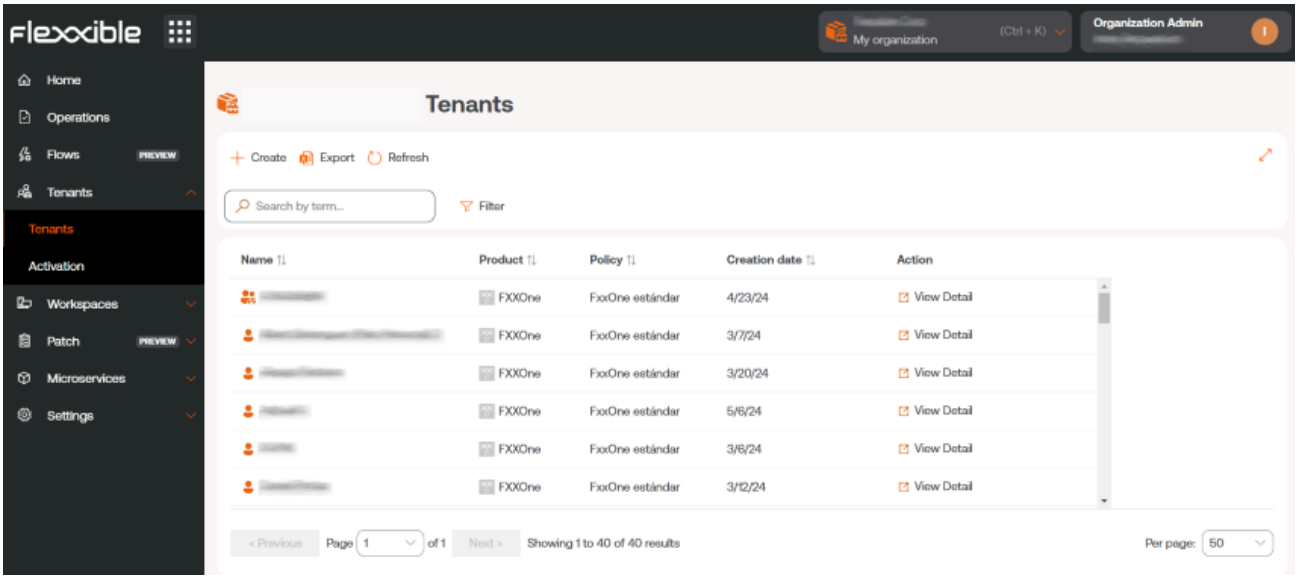
- These are subdivisions of a complex organization, management units established according to the implementation requirements.
- They are very helpful in very large environments, with wide user distribution and multiple service providers or highly segmented technical teams.
- They do not have a subscription 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 you to download an Excel file 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*.

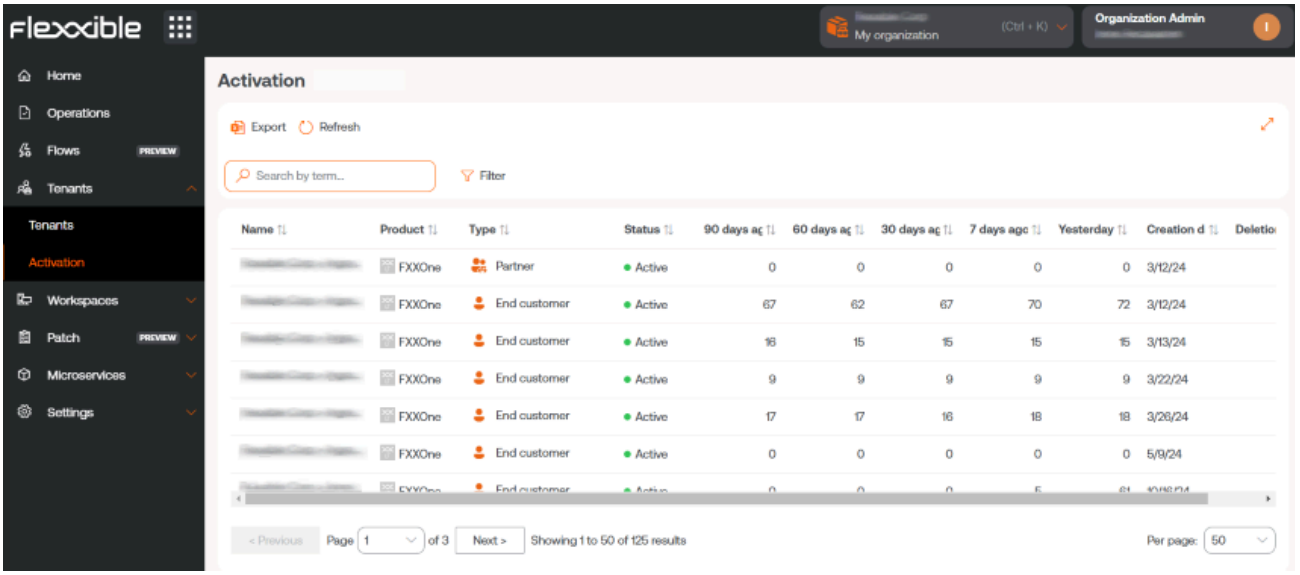
Portal / Tenants / Activation

Activation allows managed service providers (MSP) to assess the progress of FlexxAgent installations or deployments in client-type 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.

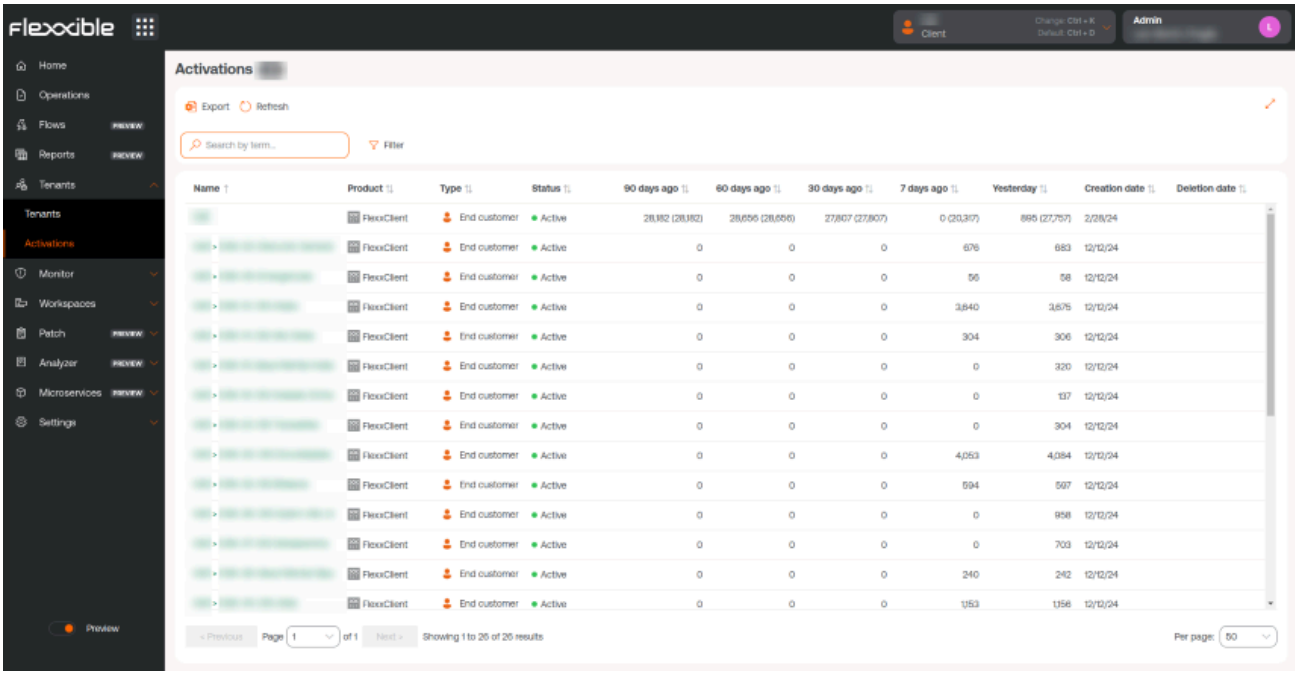
The table also indicates the Flexxible product owned by the tenant, the type of organization it corresponds to, and time indicators that help to understand the evolution of FlexxAgent adoption in the organization.

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 provides the option to search for tenants and the alternative to apply filters to the list of results, according to different parameters, such as the 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 an organization is composed of suborganizations, the activations view will allow you to check 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 sum of agents in all suborganizations in parentheses. The lower lines will represent the information for each suborganization in the format `Parent Organization` > `Suborganization`:



Tenant interface

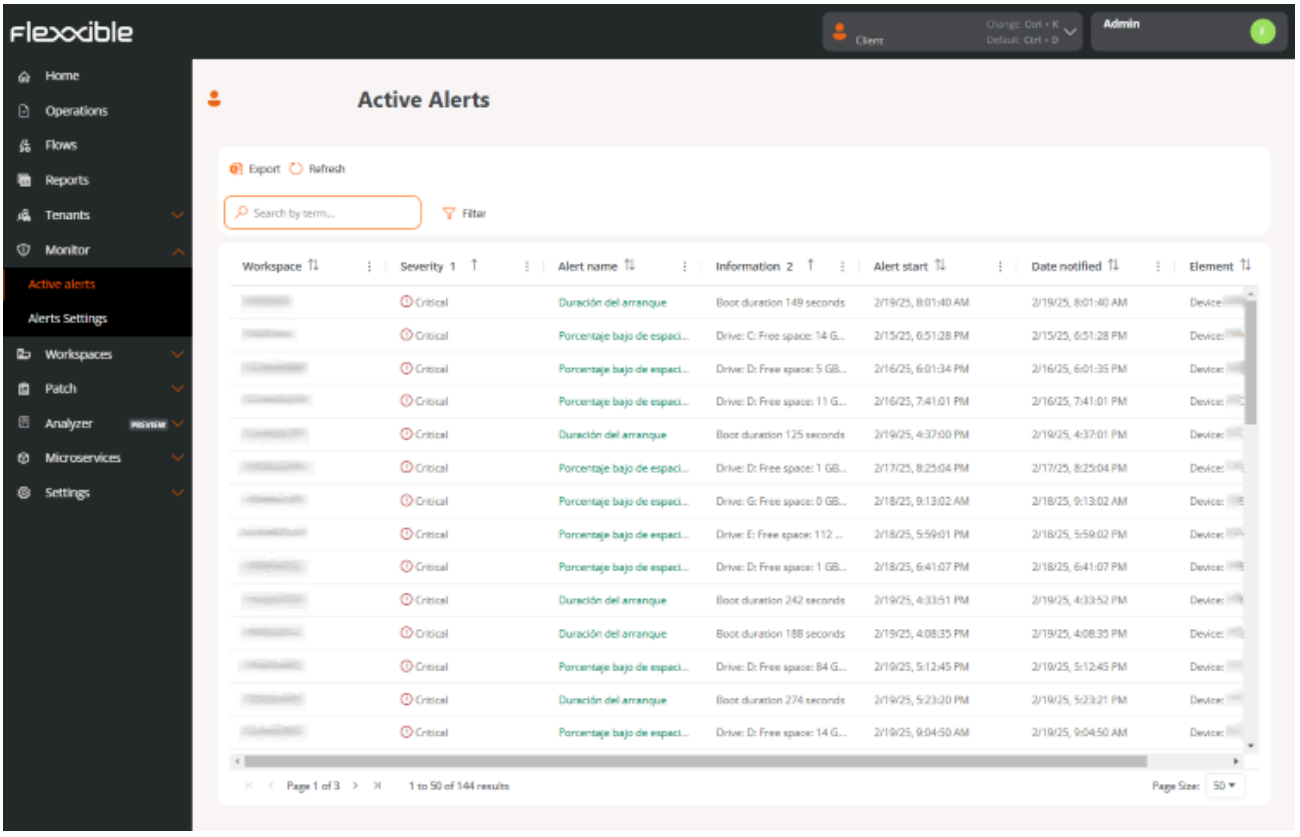
If the user clicks on the name of a tenant in the table, the Portal interface will automatically switch to the `Home` page of the selected tenant's Portal. This action is very useful because it speeds up the consultation of data from one organization or another.

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

- Do `Ctrl + K + 0`.
- Directly select the default organization (`My organization`) from the `Organization Selector`, located at the top of the interface.

Portal / Monitor in Portal

Monitor is the alert and monitoring solution for Portal. It consists of two sections: *Active alerts* and *Alert settings*. It provides real-time information on relevant events that could affect the device's operation and allows predefined alerts to be configured to meet each organization's specific needs.



Monitor includes dozens of predefined alerts, each with basic settings, set at standard thresholds. In certain organizations, these thresholds may need specific adjustments to reflect their own conditions. It's recommended to fine-tune settings to minimize noise generated by excessive alerts.

Below are the included alerts and their default settings:

Name	Severity	Category	Threshold	Threshold unit	Authorize time (minutes)
Boot duration	🔴 Critical	Performance	90	seconds	0
Login duration	🔴 Critical	Performance	60	seconds	0
Critical event log	🔴 Critical	Event Logs	1		60
Workspace with Plug and Play errors	⚠️ Warning	Hardware	0		0
Low storage for Workspace	⚠️ Warning	Storage	500	MB	5
High User round-trip time (RTT)	⚠️ Warning	Performance	350	milliseconds	5
NTFS error event log	⚠️ Warning	Storage	0		15
Multiple errors in event log	⚠️ Warning	Event Logs	50		60
High RAM usage for	⚠️ Warning	Performance	90	%	10

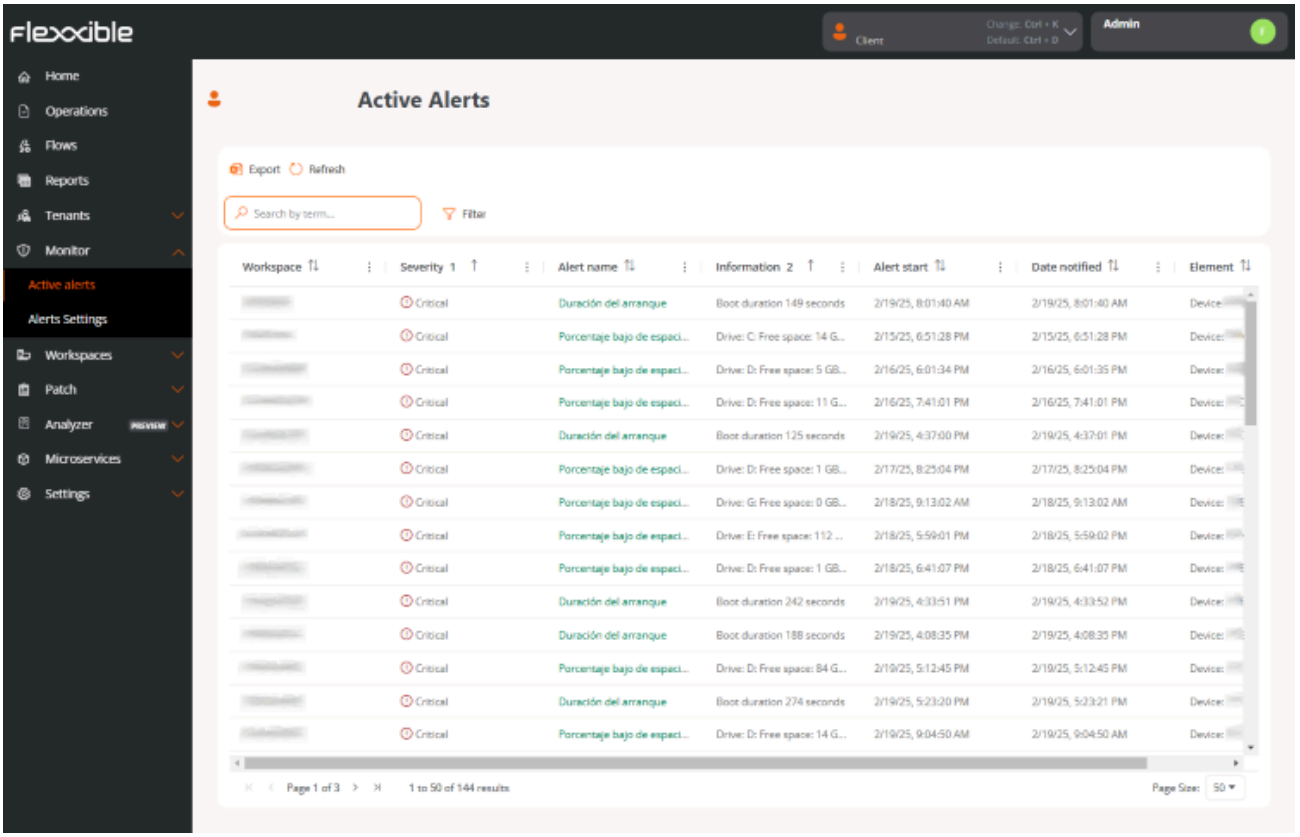
Name	Severity	Category	Threshold	Threshold unit	Authorize time (minutes)
Workspace					
FlexxAgent not reporting	⚠️ Warning	FlexxAgent	0		120
Workspace pending reboot	ℹ️ Informational	Security	0		0
Windows Update service running in non persistent workspaces	ℹ️ Informational	Performance	0		0
Low storage free space % for Workspace	🔴 Critical	Storage	90	%	0
Low connection signal for Workspace	⚠️ Warning	Connectivity	40	%	10
High CPU Usage for Workspace	⚠️ Warning	Performance	80	%	10

Name	Severity	Category	Threshold	Threshold unit	Authorize time (minutes)
Workspace uptime	ℹInformational	Performance	15	days	0
High User input delay	⚠️ Warning	Performance	350	milliseconds	5
Machines whose FlexxAgent was automatically repaired	⚠️ Warning	FlexxAgent	25	machines	60
Print service error	🔴 Critical	Printing	720		0
Low storage free space % for workspace (warning)	⚠️ Warning	Storage	70	%	0

These alerts and their default configuration help build the Workspace Reliability Index (WRI), used to determine the device's target performance. This index is combined with user sentiment, collected through surveys, to calculate the User Experience Index (UXI).

Portal / Monitor / Active alerts

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



The table includes the following fields:

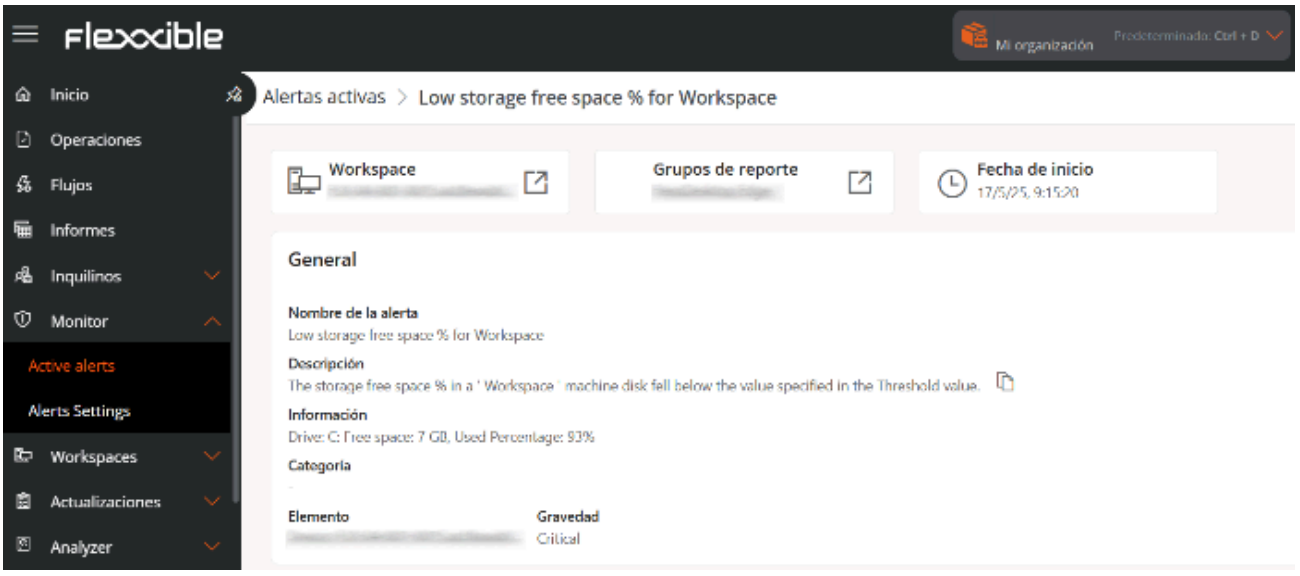
- **Information.** Description of the alert.
- **Start Date.** Date and time the alert is recorded.
- **Notification Date.** Date and time of the alert notification.
- **Element.** Name of the device where the alert is recorded.
- **Workspace.** Type of device where the alert is recorded.
- **Severity.** Alert severity level (*Informative*, *Warning*, and *Critical*). The severity levels can be checked here.
- **Alert name.** Name assigned to the alert.

- **Category.** Name of the category the alert belongs to. The categories can be checked here.

> **INFO**
>
> From this view, client-type organizations (tenants) can also view the alerts generated on the devices of their sub-organizations.

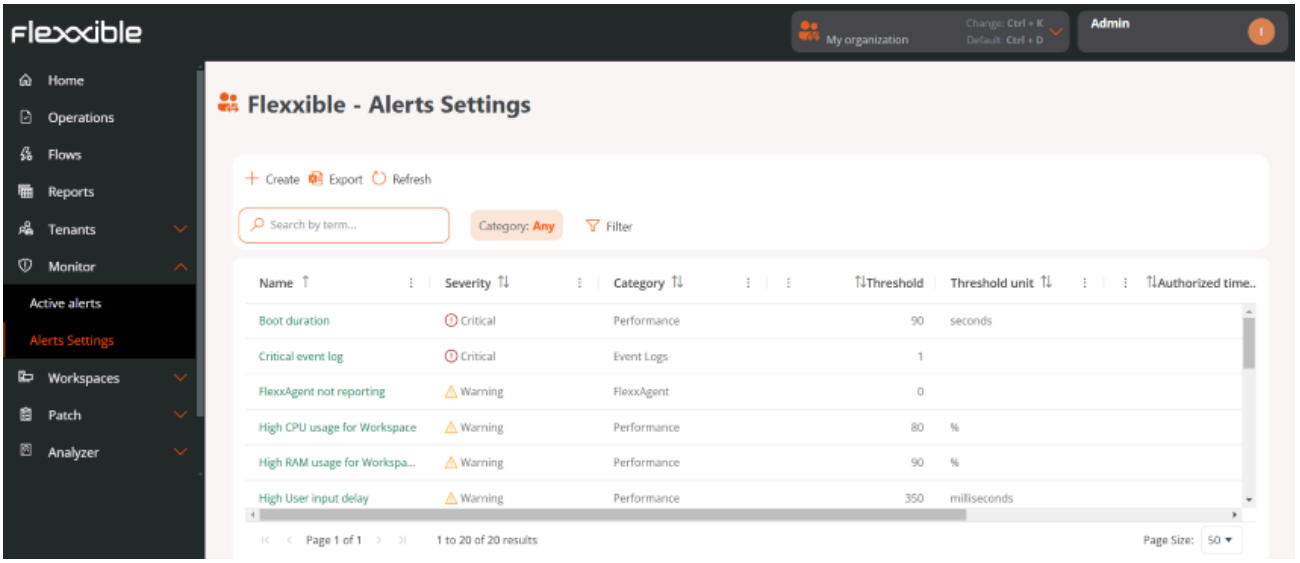
Alert detail view

To view specific information, click on the alert name in the table. From this view, you can also access the details of the device where the alert occurs and its report group.



Portal / Monitor / Alert Configuration

Alert configuration allows you to view in detail the alerts that can be activated on a device and confirm if they are enabled or disabled. From here, it is also possible to create new alerts based on the system's event logs and link them to one or more microservices.

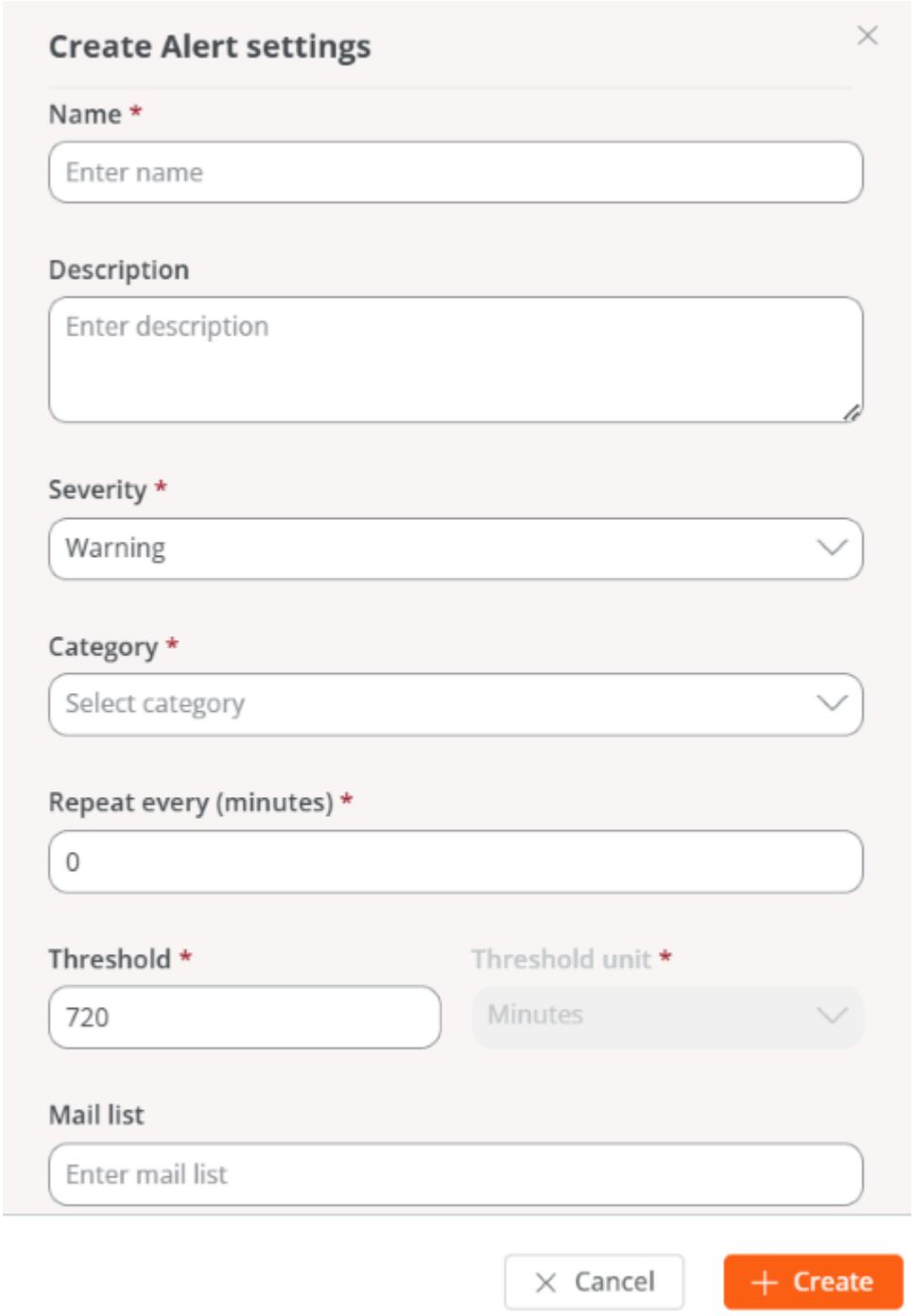


The list view displays a table with the alerts that could be activated on the device. The fields contain the following information:

- **Name.** Name of the alert.
- **Severity.** Severity level of the alert. Refers to the impact of an event on the system. The severity levels can be consulted here.
- **Category.** Name of the category the alert belongs to. The categories can be consulted here.
- **Threshold.** Numerical value that defines the condition to trigger an alert.
- **Threshold unit.** Unit associated with the threshold (time, percentage, or megabytes).
- **Allowed time (minutes).** Maximum time allowed for a condition before an alert is issued.
- **Repeat every (minutes).** Time that will pass before sending a new alert if the condition persists.
- **Enabled.** Indicates if the alert is enabled or disabled.

Create a new alert setting

At the top, the `New` button allows you to create an alert based on the events recorded by the system.



The form requests the following information:

- **Name.** Name of the alert.

- **Description.** Brief explanation of the meaning of the alert.
- **Severity.** Allows you to choose the severity level of the alert. Severity levels can be consulted here.
- **Category.** Allows you to choose the category the alert corresponds to. The categories can be consulted here.
- **Repeat every (minutes).** Time that will pass before sending a new alert if the event that triggers it is not resolved.
- **Threshold.** Allows you to choose the numeric value that defines the condition for triggering an alert.
- **Threshold unit.** Unit associated with the threshold (time, percentage, or megabytes).
- **Mail recipient list.** Email addresses of users who will receive an alert notification (separated by commas).
- **Alert message.** Alert notification message that recipients will receive.
- **Event ID.** Number that identifies an event in the 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 that generates the alert occurs.

Alert Severity

There are three levels of severity:

- **Informational.** The event is not critical, but system performance could be optimized.
- **Warning.** The event could compromise system performance if not addressed.
- **Critical.** The event requires immediate attention because it compromises system performance.

Alert categories

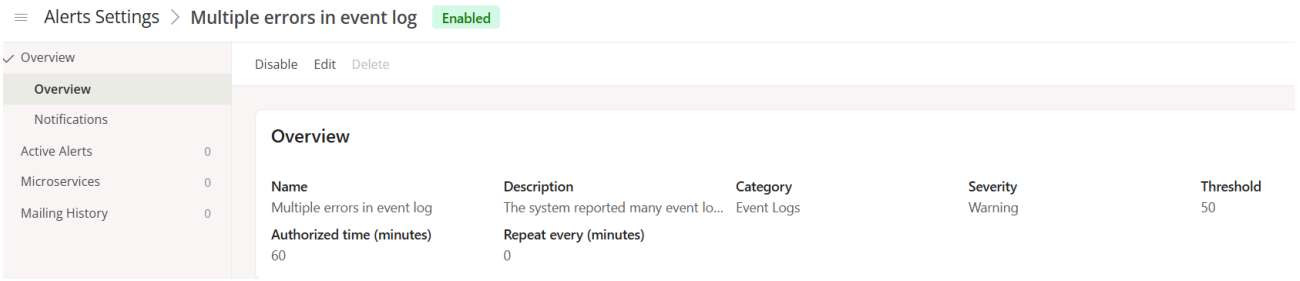
Categories indicate where the events that generate an alert are logged. They are divided as follows:

- Connectivity

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

Detail view

In the table, clicking on the name of an alert accesses its detailed view.



At the top, the alert status is displayed: *Enabled* (green background) or *Disabled* (gray background). As appropriate, the `Enable` or `Disable` button will allow you to change its status.

> **INFO**
>
> The alert will be enabled one minute after clicking the `Enable` button. The time is four minutes in the case of `Disable`.

Edit alert settings

From the detail view, the `Edit` button opens a form to modify the alert settings.

Predefined alerts are created in each organization. However, through the following fields, some changes can be made according to each organization's requirements:

- **Repeat every (minutes).** Time that will pass before sending a new alert if the condition persists.
- **Allowed time (minutes).** Maximum time allowed for a condition before an alert is issued.
- **Threshold.** Numerical value that defines the condition to trigger an alert.

From `Edit`, you can also add email addresses to define the recipients of notifications when an alert is generated in the system (separated by commas).

Sidebar menu

The detail view of each alert features a sidebar menu, divided into three tabs: *Overview*, *Active Alerts*, and *Microservices*.

Overview

It presents the alert data in a summarized way and includes a *Notifications* tab with the email addresses of the recipients who will be informed when an alert is activated on the device.

Active alerts

It displays a table with the organization's devices where the alert is active.

- **Information.** Description of the alert.
- **Start Date.** Date and time the alert is recorded.
- **Notification Date.** Date and time of the alert notification.
- **Element.** Name of the device where the alert is recorded.
- **Workspace.** Type of device where the alert is recorded.

Microservices

There are alerts that could be resolved with the automatic execution of a microservice. The platform allows this by clicking the `Link` button. This action will open a form where you

should indicate to which microservice you want to associate the alert and the execution order, which is useful when you want to link more than one microservice.

Send history

Shows a table with the list of recipients of the alert notifications.

- **Date.** Day and time the notification is sent.
- **To.** Email address.
- **Subject.** Name of the alert and the device where it was recorded.
- **Error.** State of the device that triggered the alert.

Portal / Workspaces in Portal

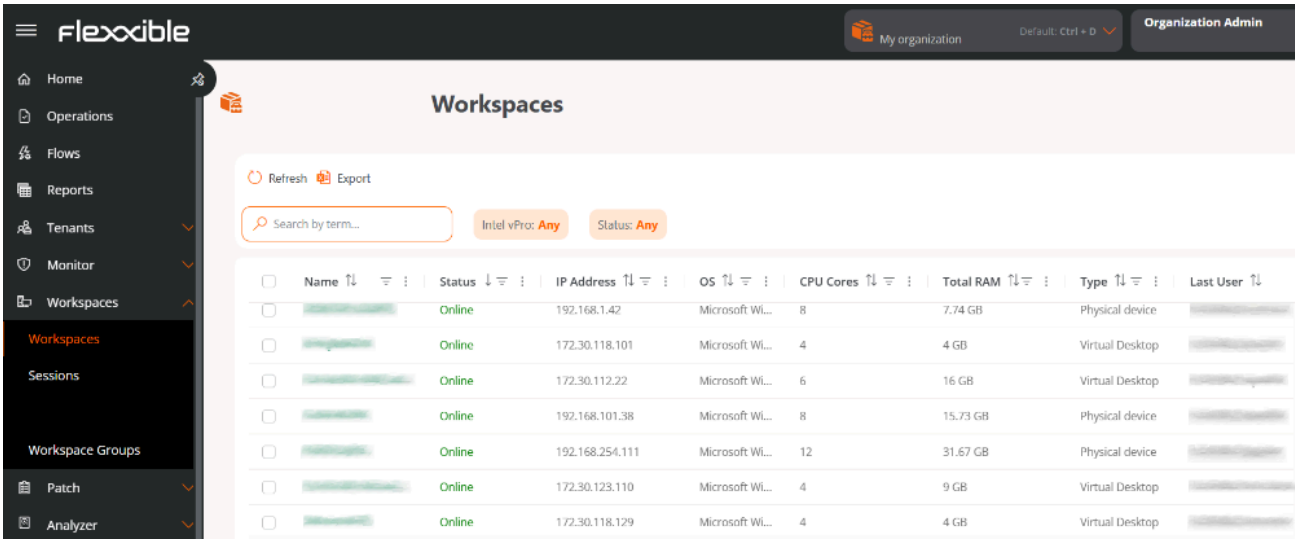
Workspaces is a Portal tool designed to offer a complete and centralized view of the status and performance of devices within an organization.

Through an intuitive interface, it allows you to monitor key information from each device, access technical details, review alerts, operations, and sessions, as well as manage updates, services, and system components.

The main goal of Workspaces is to facilitate the administration and monitoring of appliances, optimizing decision-making through accurate, up-to-date, and visually organized data.

Overview

The main view of Workspaces shows a table with the list of all appliances in the organization, along with the following information:



- **Name.** Device Name.
- **Status.** Current status (*Online* or *Offline*).
- **IP Address.** IP assigned to the appliance
- **OS.** Installed operating system.
- **CPU Cores.** Number of processor cores.

- **Total RAM.** Total RAM memory (in MB).
- **Type.** Indicates if the appliance is physical or virtual.
- **Last User.** Name of the last user who accessed the appliance.
- **Creation Date.** Date when the appliance was registered.
- **Intel vPro Enterprise.** Indicates whether the device supports Intel® AMT technology and is ready to receive operations from this technology.
  - *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.
  - *Ready*: Supports Intel® AMT technology. For more information, please refer to the documentation on the Intel vPro Enterprise integration.

Device detail view

By clicking on the name of an appliance, you access its detail view. At the top, its status is shown: Online (green background) or Offline (gray background).

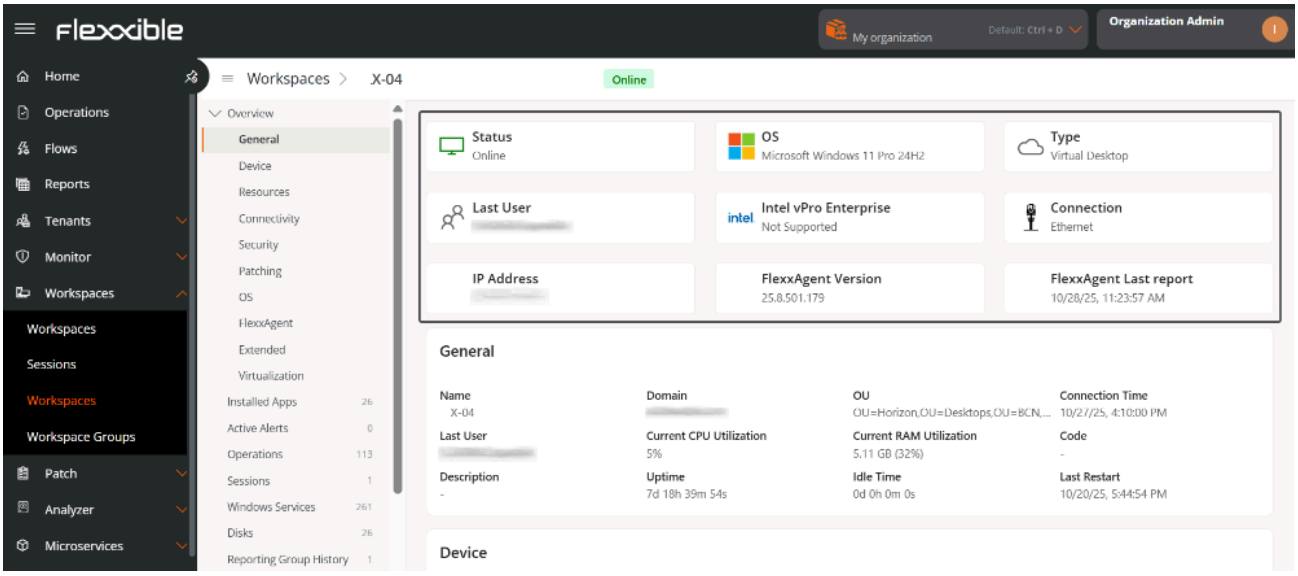
The detail view is organized into the following tabs:

- Overview
- Diagnosis
- Installed applications
- Current active alerts
- Intel vPro
- Operations
- Sessions
- Windows Services
- Disks

- All reporting groups
- PnP Events
- PnP Errors
- CrowdStrike Detections
- Version History
- Boot history
- Installed updates
- Pending updates

Overview

At the top of this view, a group of cards facilitate reading device data: *Status*, *Operating System (OS)*, *Type*, *User*, *Intel vPro Enterprise*, *Connection*, *IP Address*, *FlexxAgent version* and *FlexxAgent last report*.



Below, ten sections offer detailed information:

1. General

- **Name.** Identifier assigned to the appliance within the network or system. Generally corresponds to the hostname configured in the operating system.

- **Domain.** Name of the domain to which the appliance belongs within the network infrastructure.
- **OU.** Organizational unit where the appliance is located within the domain.
- **Connection Time.** Total duration of the current session or the time elapsed since the appliance last connected to the server or network.
- **Last User.** Name of the user who last logged into the appliance.
- **Current CPU Utilization.** Percentage of use of the central processing unit (CPU) at the time of the query. Indicates the system workload.
- **Current RAM Utilization.** Percentage of RAM memory currently in use by the system and active applications. Allows evaluating resource consumption.
- **Code.** Unique identifier or internal code assigned to the appliance for inventory or administrative management purposes.
- **Description.** Descriptive information about the appliance, any additional relevant detail.
- **Uptime.** Period of time that the appliance has remained on and continuously operating since the last reboot.
- **Downtime.** Period during which the appliance has been off, disconnected, or out of service.
- **Last Reboot.** Date and time the appliance was last rebooted. Useful for monitoring system stability and maintenance.

2. Appliance

- **Operating System Manufacturer.** Company or entity responsible for the development and distribution of the operating system installed on the appliance.
- **System Model.** Specific hardware model identification according to the manufacturer. Allows recognizing the version or line of the device.
- **System Type.** Classification of the appliance according to its architecture or purpose (e.g.: workstation, laptop, server, virtual machine, etc.).
- **System SKU.** Commercial reference code (Stock Keeping Unit) assigned by the manufacturer to identify the exact configuration of the model.
- **Processor.** Technical details of the installed CPU, including manufacturer, model, clock speed, and architecture.

- **BIOS Date.** Date of the current BIOS or UEFI version installed on the system. Indicates when it was issued or updated by the manufacturer.
- **BIOS Serial Number.** Unique identifier associated with the specific BIOS version of the appliance.
- **Platform role.** Main function of the appliance within the environment (for example: desktop, virtual machine, etc.).
- **Boot Device.** Unit or medium from which the operating system starts.
- **Regional Configuration.** Language setting configured on the system.
- **Time Zone.** Time zone set on the system for date and time synchronization.
- **Last Boot Duration.** Total time it took the system to complete the startup process from powering on to being operational.
- **Fast Startup.** Indicates if the Fast Startup feature is enabled.

3. Resources

- **CPU Cores.** Total number of physical cores available in the processor. Directly affects performance and parallel processing capability.
- **Total RAM.** Total amount of physical memory (RAM) installed in the appliance.
- **Paging File Space.** Total disk space assigned to the paging file used to extend virtual memory.
- **Paging File.** Location and name of the file used by the operating system to manage virtual memory.
- **System Disk Usage.** Percentage or amount of space currently occupied on the main drive where the operating system is installed.
- **Total Hard Disk Size.** Total physical storage capacity of the main disk or system drive.

4. Connectivity

- **Connection.** Type of active network connection (e.g.: wired, wireless, VPN, virtual network).
- **IP Version.** Internet Protocol used by the network interface.
- **IP Address.** Address assigned to the appliance within the local network for identification and communication.

- **Subnet.** Network range that determines the segment to which the IP address belongs.
- **Default Gateway.** IP address of the router or device that allows communication with external networks.
- **MAC Address.** Unique physical identifier assigned to the appliance's network card.
- **Network Changed.** Indicates if the appliance has recently changed networks.
- **Public IP.** Externally visible IP address assigned by the Internet Service Provider (ISP).
- **ISP.** Internet Service Provider. Company that provides Internet connection to the appliance or local network.
- **Location.** City or geographic location associated with the detected public IP.
- **Country.** Country corresponding to the geographic location of the public IP.
- **Last Network Information Update.** Date and time when the connectivity information of the appliance was last updated.

5. Security

- **Encrypted Hard Disk.** Indicates if the appliance's main storage is secured through encryption.
- **Secure Boot Status.** Shows if the Secure Boot function of the BIOS/UEFI is enabled to prevent unauthorized software from loading during startup.
- **Kernel DMA Protection.** Indicates if the system has enabled direct memory access (DMA) protection to prevent attacks on the kernel from external devices.
- **EDR.** Endpoint Detection and Response. Name or solution implemented for advanced security and threat detection and response at the endpoint.
- **EDR Status.** Operational status of the EDR system.
- **Antivirus.** Name of the antivirus solution installed or integrated into the system.
- **Antivirus status.** Operational state of the solution.

6. Update

- **Target.** Update policy to which the appliance belongs.
- **Number of Pending Updates.** Total number of updates that are available but not yet installed on the system.

- **Last Windows Update.** Date and time when the most recent update of the Windows operating system was installed.
- **Reboot Pending.** Indicates if the system requires a reboot to complete the installation of updates or other configuration changes.
- **Number of Days Since Last Windows Update.** Time interval (in days) since the last successful installation of operating system updates.

7. OS

- **OS.** Full name of the operating system installed on the appliance.
- **Operating System Version.** Specific version number of the operating system indicating its current revision or update level.
- **OS Build.** Number of the internal build of the operating system reflecting the exact set of updates applied.
- **Windows Directory.** Path of the root directory where the Windows operating system is installed.
- **System Directory.** Path of the subdirectory containing the main files of the operating system.

8. FlexxAgent

- **Report Group.** Name of the reporting group to which the appliance belongs.
- **Version.** Version number of FlexxAgent installed on the appliance.
- **Status.** Indicates if it is stopped or running.
- **Last Report.** Date and time when FlexxAgent sent its last report to the appliance.
- **Session Analyzer.** Indicates if the Analyzer session is configured or not on the appliance.
- **Session Analyzer Version.** Indicates the version number of the Analyzer session on the appliance.
- **Uninstall Protection.** Indicates if the uninstallation protection is enabled or not.

9. Extended

- **SMBIOS Version.** Version of the System Management BIOS implemented on the system.
- **Embedded Controller Version.** Version of the embedded firmware or controller.
- **BIOS Mode.** Indicates if the system operates in Legacy BIOS mode or UEFI.
- **Motherboard Manufacturer.** Company responsible for the design and production of the appliance's motherboard.
- **Motherboard Model.** Identification or reference of the specific motherboard model installed.
- **Motherboard Version.** Number or code that specifies the revision or version of the motherboard design.
- **Unique ID.** Unique identifier assigned to the appliance or system.
- **Windows Type.** Type of license or edition of the Windows operating system.
- **Creation Date.** Date and time when the original installation of the operating system was performed.

10. Virtualization

- **Hypervisor.** Virtualization software or platform that manages virtual machines.
- **Farm / Cluster.** Set of servers or nodes grouped to run and manage virtual machines together.
- **Broker.** Intermediate server responsible for managing user connections to virtual machines or remote desktops.
- **Delivery Group.** Set of virtualized desktops or applications.
- **Status.** Current operational status of the virtual machine.
- **Citrix XD Status.** Specific status of the appliance within the Citrix environment.
- **Registration Status.** Indicates if the appliance or virtual machine is correctly registered in the management system or broker.
- **Maintenance Mode.** Defines if the machine is marked for maintenance tasks, preventing its allocation to end users.
- **Type.** Classification of the virtual resource.
- **Group / Catalog Name.** Name assigned to the group or catalog of virtual machines within the virtualization environment.

- **Connected From.** IP address, hostname, or location from which the user established the connection to the virtual environment.

Diagnosis

This section allows you to analyze the resource consumption of a device based on the use of applications and system processes used during a user's session.

To view the data, you need to select beforehand:

- **User.** If the device has more than one user session started, it allows you to choose the one you want to analyze.
- **Date range.** Defines the week of the analysis. By default, the data from the last seven days is shown.

Selection chart

Once the user and date range are selected, the selection chart provides an overview of resource consumption. It represents, with colored lines, the behavior of each system resource (CPU, RAM, GPU, Network, and Disk) during the indicated period.

The time window (orange box) allows you to specify a seven-hour time range. When moving it, the lower charts, corresponding to each system resource, will update their data to show the consumption details during those hours.

Performance Charts

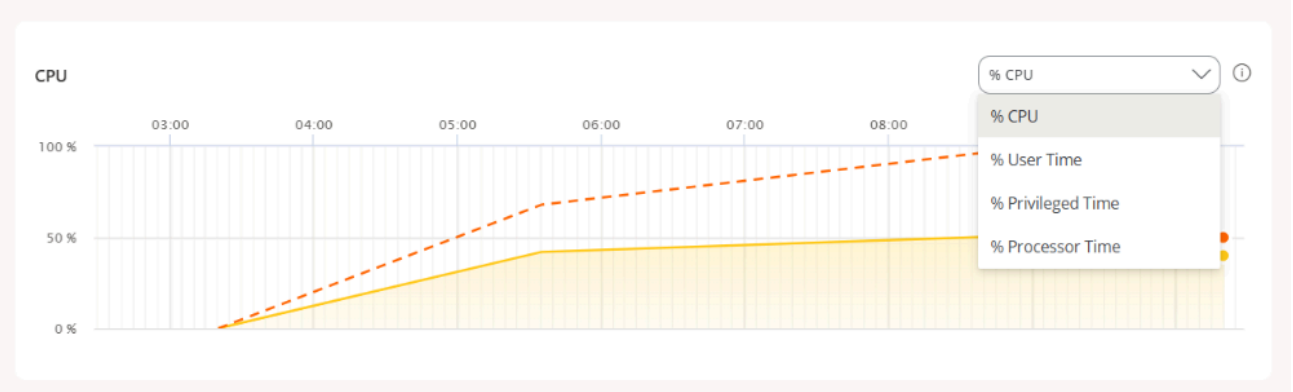
Diagnosis allows you to analyze the behavior of each system resource through five graphs. CPU, RAM, GPU, Network, and Disk. Each of them has a dropdown with specific parameters that allow filtering the results.

Hovering over a point on the chart displays detailed information: date, time, maximum and minimum value of the respective parameter.

Parameters by type of system resource

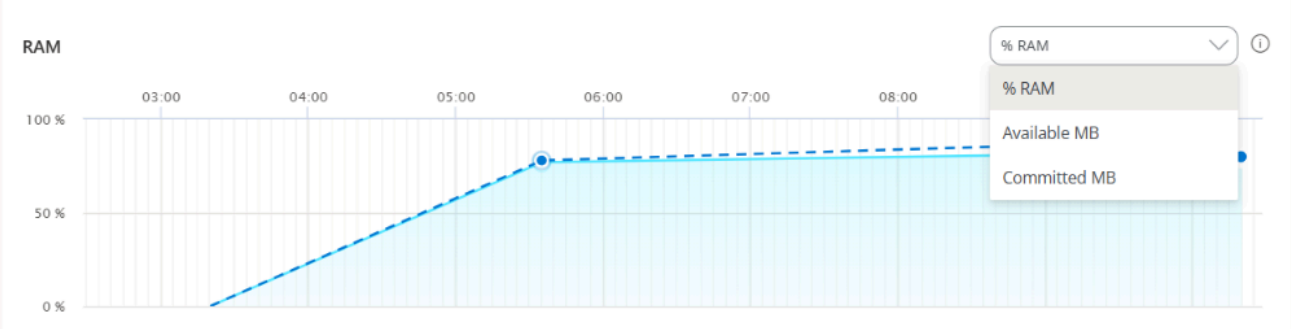
CPU

- **% CPU.** Total percentage of CPU utilization across all cores.
- **% User Time.** Percentage of CPU time dedicated to executing processes in user mode.
- **% Privileged Time.** Percentage of CPU time dedicated to executing system operations (kernel).
- **% Processor.** Total CPU time used across all processes and system activities.



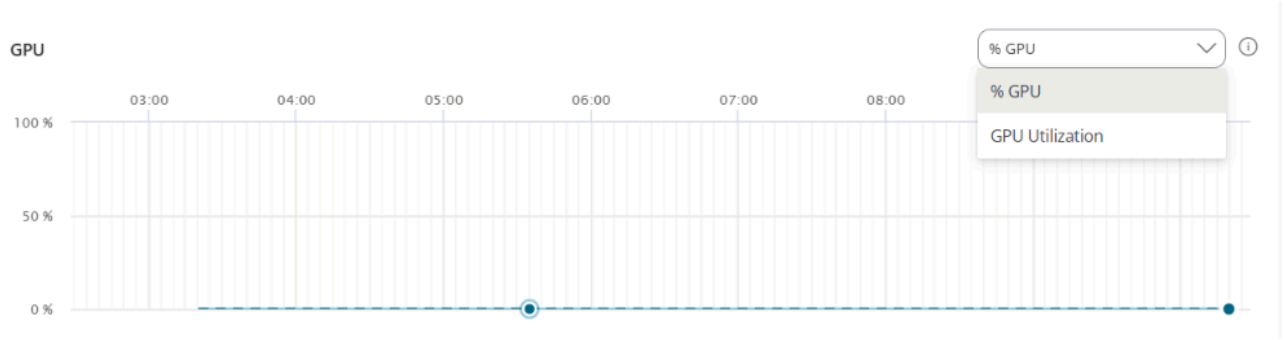
RAM

- **% RAM.** Percentage of physical memory currently in use.
- **Available MB.** Amount of free RAM available to run new applications without causing performance issues.
- **Committed MB.** Amount of virtual memory that has been committed.



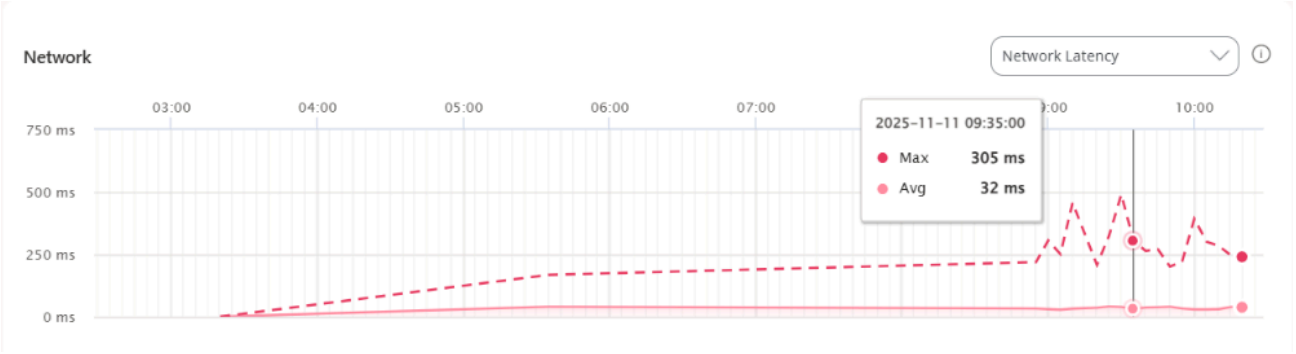
GPU

- **% GPU.** Percentage of the graphic processing unit (GPU) capacity currently being used.
- **GPU Utilization.** Percentage of time the GPU is actively processing.



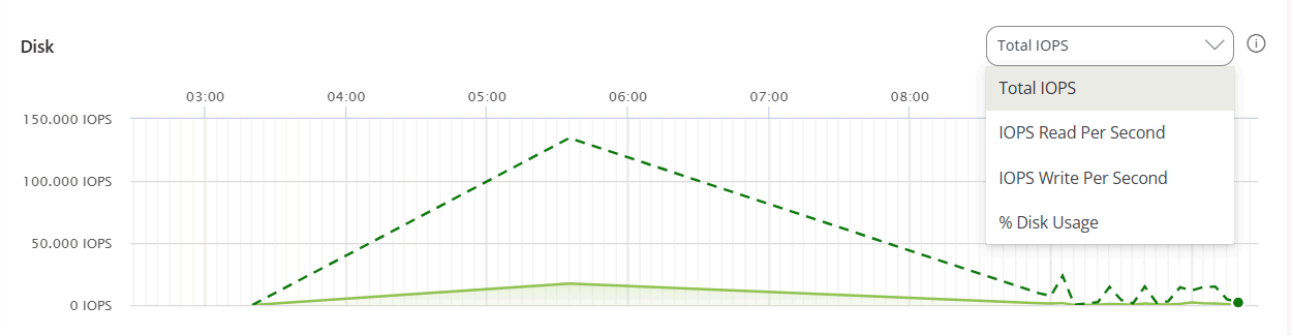
Network

- **Network Latency.** Maximum latency of all listed applications and processes.



Disk

- **Total IOPS.** Total input/output operations per second for disk activity.
- **Read IOPS per second.** Number of read operations per second from the disk.
- **Write IOPS per second.** Sum of write operations from applications and processes.
- **% Disk usage.** Percentage of the disk input and output capacity being used.



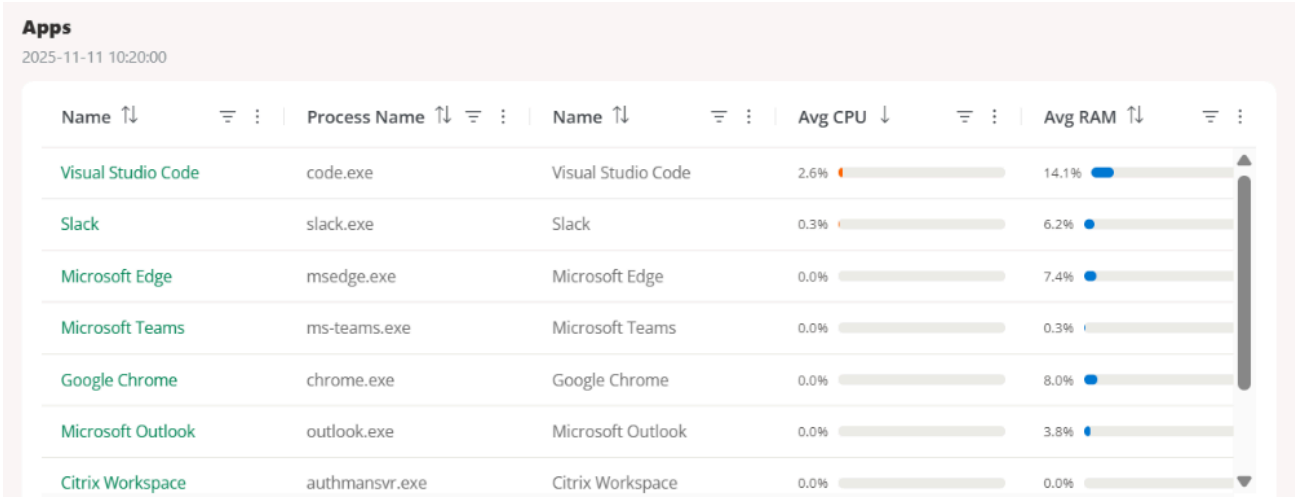
Applications and Processes Tables

At the bottom are the *Applications* and *Processes* tables, showing the data corresponding to the most recent moment of the time range chosen in the selection chart.

Applications

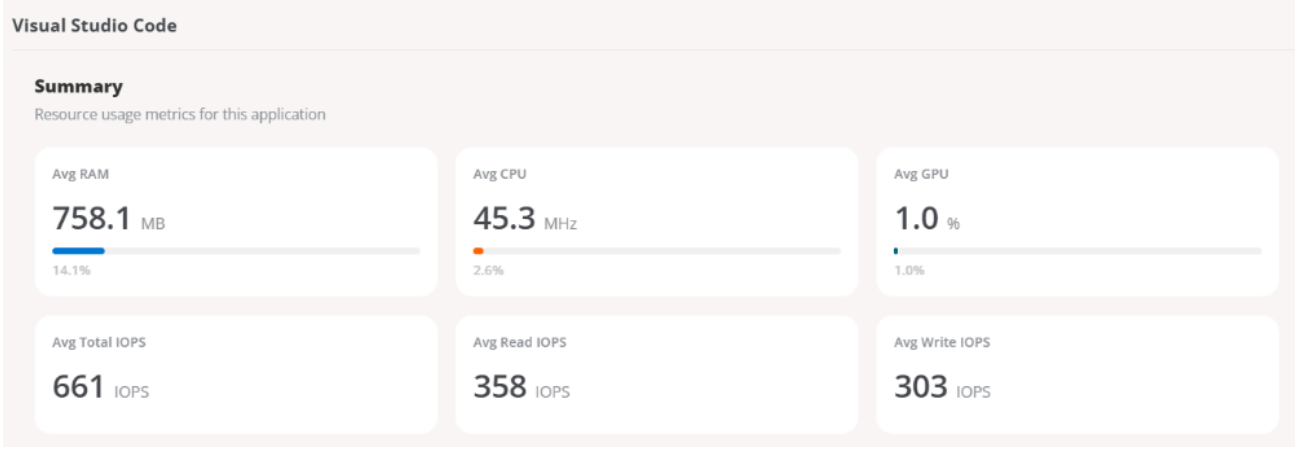
Displays the active applications on the device. Each row includes the following fields:

- **Name.** Application name.
- **Process Name.** Process associated with the application.
- **Average CPU.** Average percentage of CPU utilization.
- **Average RAM.** Average percentage of physical memory in use.
- **Average GPU.** Average percentage of GPU utilization.
- **Average Total IOPS.** Average input/output operations per second.
- **Average Read IOPS.** Average read operations per second.
- **Average Write IOPS.** Average write operations per second.
- **Maximum Network Latency.** Maximum latency recorded for the application.



Summary Box

Selecting an application from the table provides access to a more visual summary box, with its system resource usage metrics.

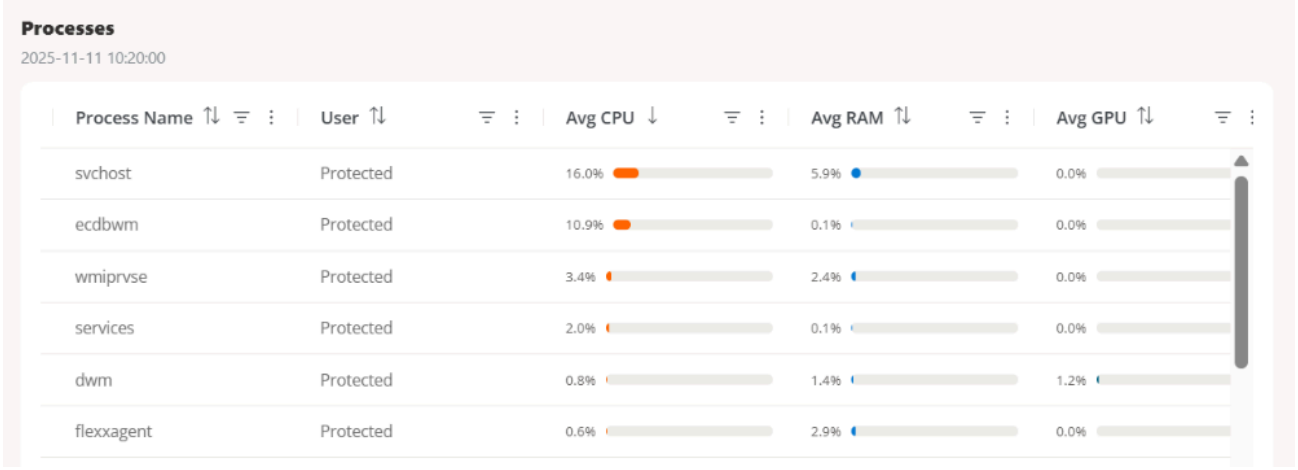


Processes

Displays the active processes on the device. Each row includes the following fields:

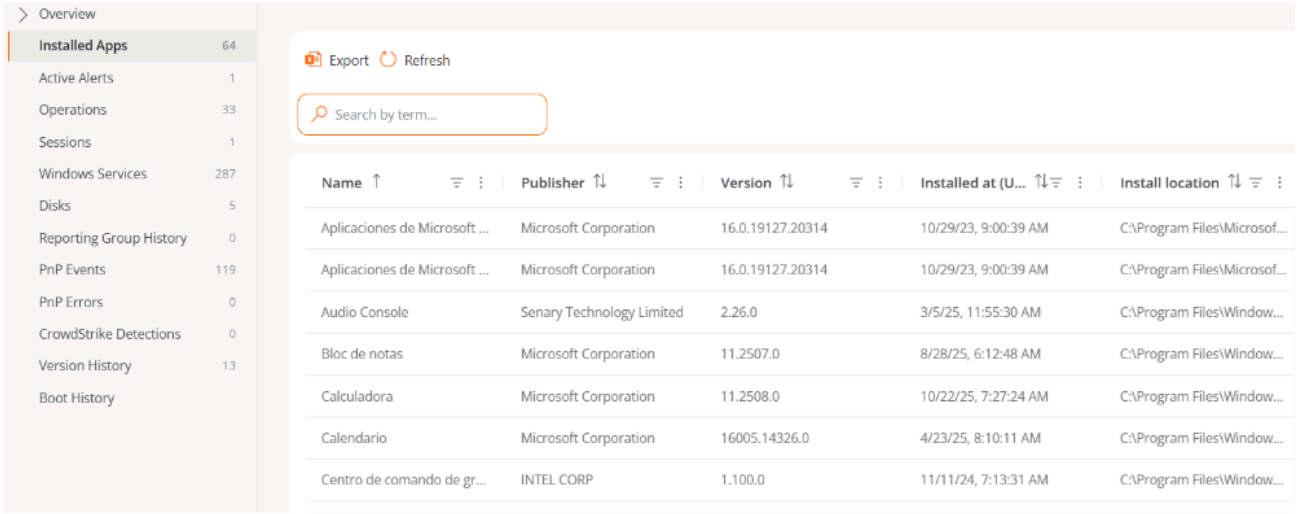
- **Name.** Name of the product or process.
- **Process Name.** Name of the executable.
- **User.** User executing the process.
- **Average CPU.** Average percentage of CPU utilization.
- **Average RAM.** Average percentage of physical memory in use.
- **Average GPU.** Average percentage of GPU utilization.
- **Average Total IOPS.** Average input/output operations per second.

- **Average Read IOPS.** Average read operations per second.
- **Average Write IOPS.** Average write operations per second.
- **Maximum Network Latency.** Maximum latency recorded for the process.



Installed apps

It displays a table with all the applications detected by FlexxAgent Analyzer on the device.



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 of its last report on the device.

The information provided by **Installed Applications** is collected by FlexxAgent Analyzer when its process starts. From that moment, the data is updated every 12 hours, as long as there is a user session started, or at each login.

Active alerts

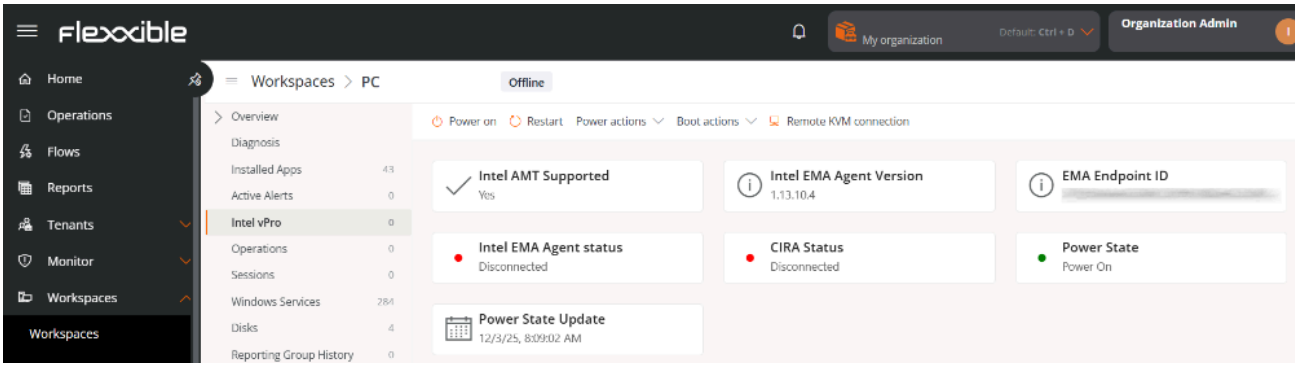
Presents a table with the active alerts found on the appliance.

The information includes:

- **Severity.** Severity level (*Critical*, *Warning*, or *Informational*).
- **Alert Name.** Name identifying the alert. You can click on it for more details.
- **Information.** Description of the alert.
- **Start Date.** Date and time the alert is recorded.
- **Notification Date.** Date and time of the alert notification.
- **Element.** Name of the device where the alert is recorded.

Intel vPro

From this tab, you can view detailed information about the Intel EMA agent installed on the device and access out-of-band management functions, even when the operating system is not available.



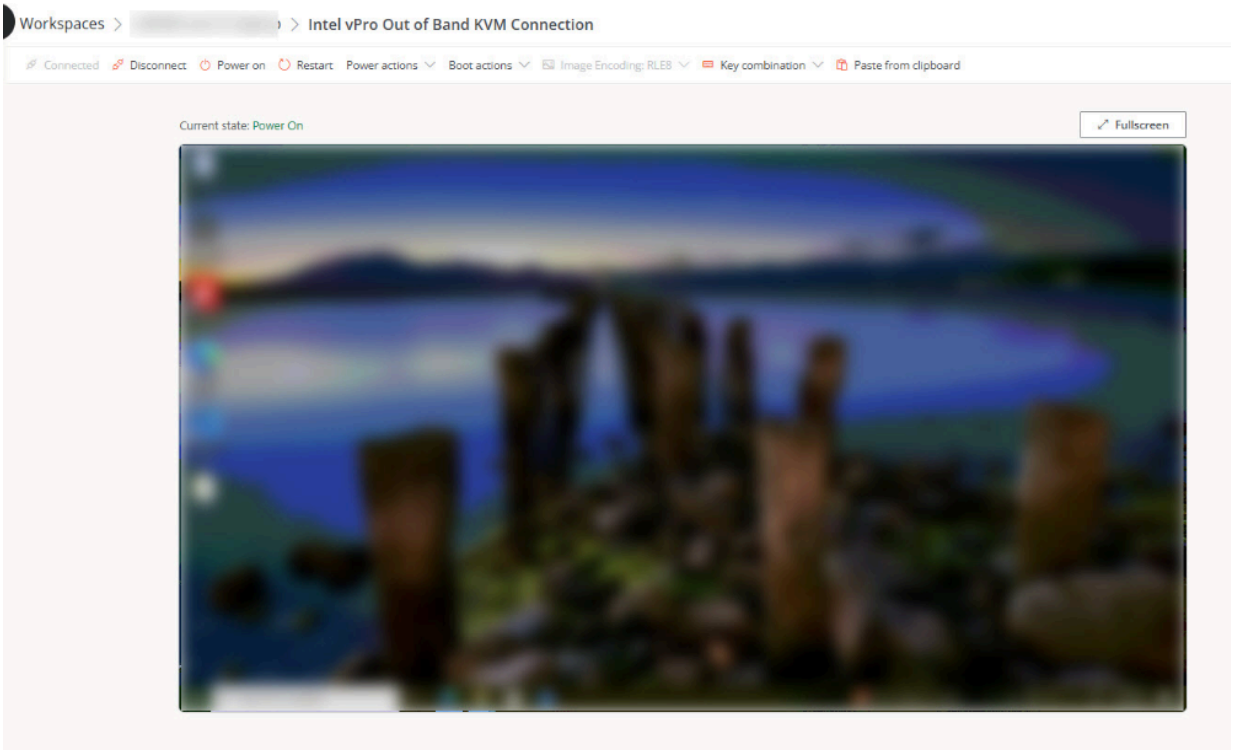
Information Detail

- **Compatible with Intel AMT.** Indicates whether the device is compatible with Intel Active Management Technology.
- **EMA Agent Version.** Version number installed on the device.
- **Intel EMA ID.** Unique identifier assigned by Intel EMA.
- **Intel EMA Agent Status.** Indicates whether the agent is *Connected* or *Disconnected*.
- **CIRA Status.** Indicates whether Client Initiated Remote Access, used for secure remote access, is *Connected* or *Disconnected*.
- **Status.** Indicates whether the device is *On* or *Off*.
- **Power Status Update.** Date and time of the last power status modification.

Available actions

Intel vPro allows remote management operations even when the operating system has not started or the device is unresponsive. These actions are executed out-of-band, accessing the hardware directly.

- **Turn On.** Turns on the device.
- **Restart.** Restarts the device.
- **Power Actions**: *Gradual Shutdown*, *Gradual Restart*, *Shutdown*, *Suspend*, *Hibernate*.
- **Boot Actions**
    - **Boot to BIOS.** Allows direct BIOS startup on devices that cannot boot their operating system.
- **Remote KVM Connection.** Provides a direct view of the device's screen to control it as if you were physically in front of it, even when the operating system does not load.



This function allows:

- View the device's screen in real-time.
- Diagnose and solve problems in geographically distributed environments or with limited IT resources, as it avoids in-person interventions.

Power on schedules

This technology also allows setting the date, time, and recurrence for the device's auto power-on.

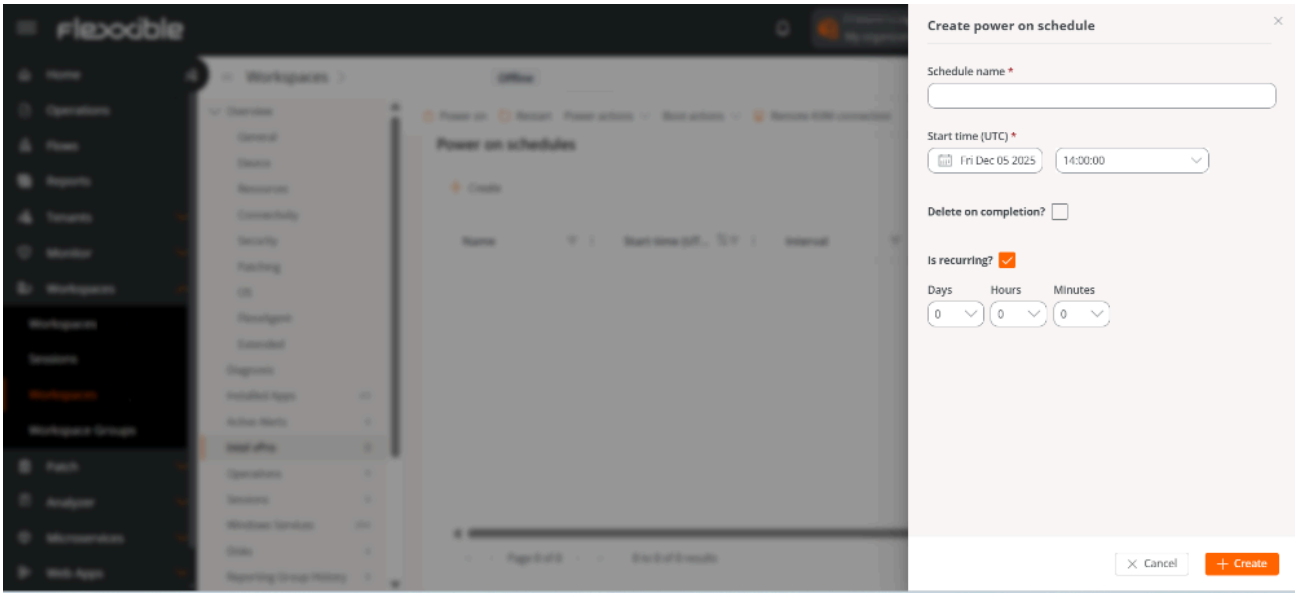
Create a schedule

1. In Portal, access `Worksaces` -> `Workspaces`.
2. Select a device from the list.
3. In the sidebar menu, select the `Intel vPro` tab.
4. In the `Power on schedules` section, click `New`.
5. Fill in the requested data in the form:

- **Program Name.** Name of the power-on schedule.
- **Start Time (UTC).** Date and time when the device will be turned on, in UTC.

- **Delete After Completion?** If selected, once the power-on is executed, the schedule will be deleted.
- **Is it recurrent?** If activated, allows you to specify every how many days and at what time the device will be turned on.

6. Click on `New`.



Operations

Lists the operations recorded on the appliance, including:

- **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

Shows the active or recorded sessions, with details like:

- **User.** Name of the user who logged into the device.

- **Session Type.** Type of session started (*Device* or *Application*, for virtualized application sessions).
- **Windows Session ID.** Unique identifier assigned to each user session.
- **Connection Status.** Status of the session connection (*Disconnected* or *Active*).
- **Start Date.** Date and time the session started.
- **CPU Usage.** Percentage of processor usage for the session, excluding resources used by other sessions or system processes.
- **RAM Usage.** Amount of volatile 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

Contains the list of operating system services, including:

- **Display Name.** Name of the programs that run 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.** Mode of login.
- **Accept Stop.** Whether or not to stop Windows services (*Yes* or *No*).

Disks

Displays the partitions of the appliance with the following information:

- **Device ID.** Name of the device.
- **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 of the volume label.
- **Total Size.** In megabytes, total disk space.

- **Used Size.** In megabytes, disk space used.
- **Used Percentage.** In percentage, disk space used.
- **Unit OS.** Unit possession (*Yes* or *No*).
- **Location.** Disk location access path.
- **Partition.** Indicates the number of storage divisions the disk has.

Reporting groups history

Shows the current and previous report groups of the appliance:

- **Source.** Reporting group the device comes from.
- **Destination.** Reporting group the device is entering.
- **Assignment Type.** *Manual* or *Automatic* assignment.
- **Requested Date.** Date and time of the device's reporting group change.

PnP Events

Shows a table with the list of Plug and Play events that have been recorded on the appliance. The information includes:

- **Action.** Hardware component state (printer, mouse, etc.) with respect to the device (*Plugged* or *Unplugged*).
- **Date.** Last PnP update registered 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.

PnP Errors

Shows a table with the list of Plug and Play errors that have been recorded on the appliance. The information includes:

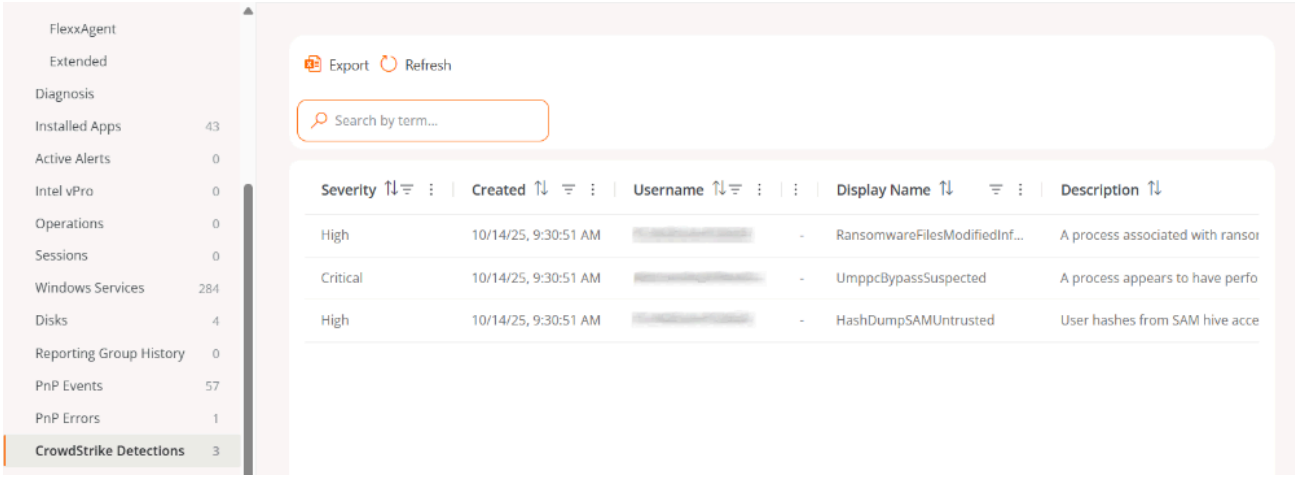
- **Name.** Name of the hardware component connected to the device.
- **Update Date.** Last PnP update registered by FlexxAgent.

- **Class.** Type of hardware component connected to the device.
- **Device ID.** Identification code of the hardware component connected to the device.

CrowdStrike Detections

If the CrowdStrike integration is done from Portal, a table will be displayed with information about threat detections, including the following fields:

- **Severity.** Criticality level assigned to the detection according to the potential impact or risk of the threat.
- **Created.** Date and time the detection was generated in the system.
- **Username.** User associated with the activity or process that triggered the detection.
- **Status.** Current status of the detection.
- **Display Name.** Descriptive name assigned to the detection, summarizing the type of threat or behavior identified.
- **Description.** Expanded information about the detection.
- **Command line.** Command or instruction executed on the appliance related to or that generated the detection.



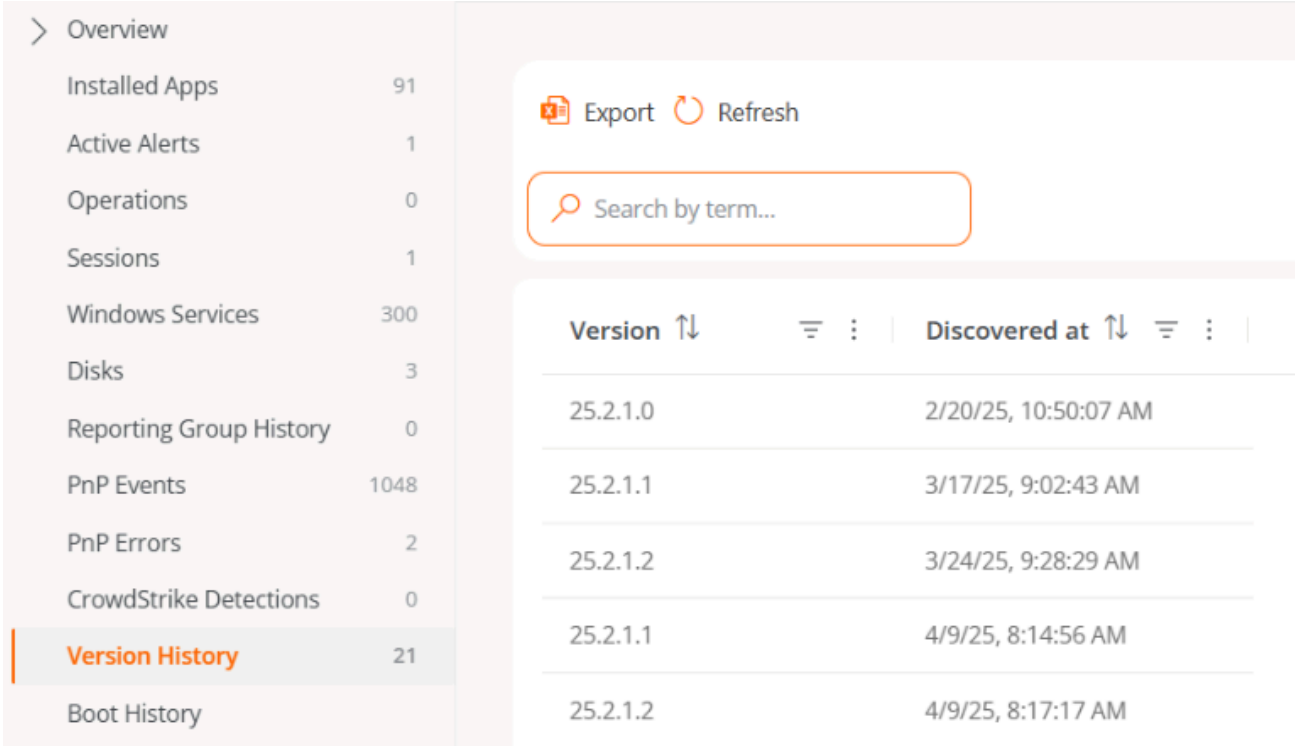
INFO

FlexxAgent synchronizes CrowdStrike alerts every minute.

Version history

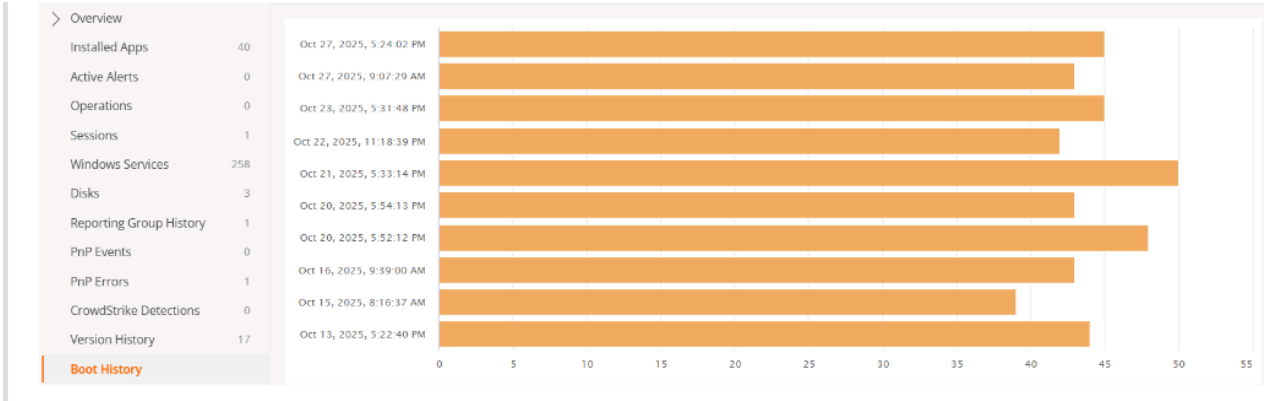
Displays a table with the versions of FlexxAgent that have been registered on the appliance.

- **Version.** Version number of FlexxAgent detected on the appliance.
- **Discovered on.** Date and time when the system identified the presence of that version of FlexxAgent on the appliance.



Boot history

Through a chart, this section shows the log of boot time taken by the device.



Installed updates

Displays a table with the list of updates installed on the appliance. The information includes:

- **Installation date.** Date and time the update was installed on the appliance.
- **KB.** Unique identifier of the update package issued by Microsoft.
- **Title.** Name of the update.
- **Product.** Name of the product to which the update applies.
- **Severity.** Criticality level assigned to the update according to its importance or impact on security (*Critical*, *Important*, *Moderate*, *Low*, *Unspecified*).
- **Arrival date.** Date when the update was published or made available by the provider.
- **Category.** Functional or technical classification of the update.

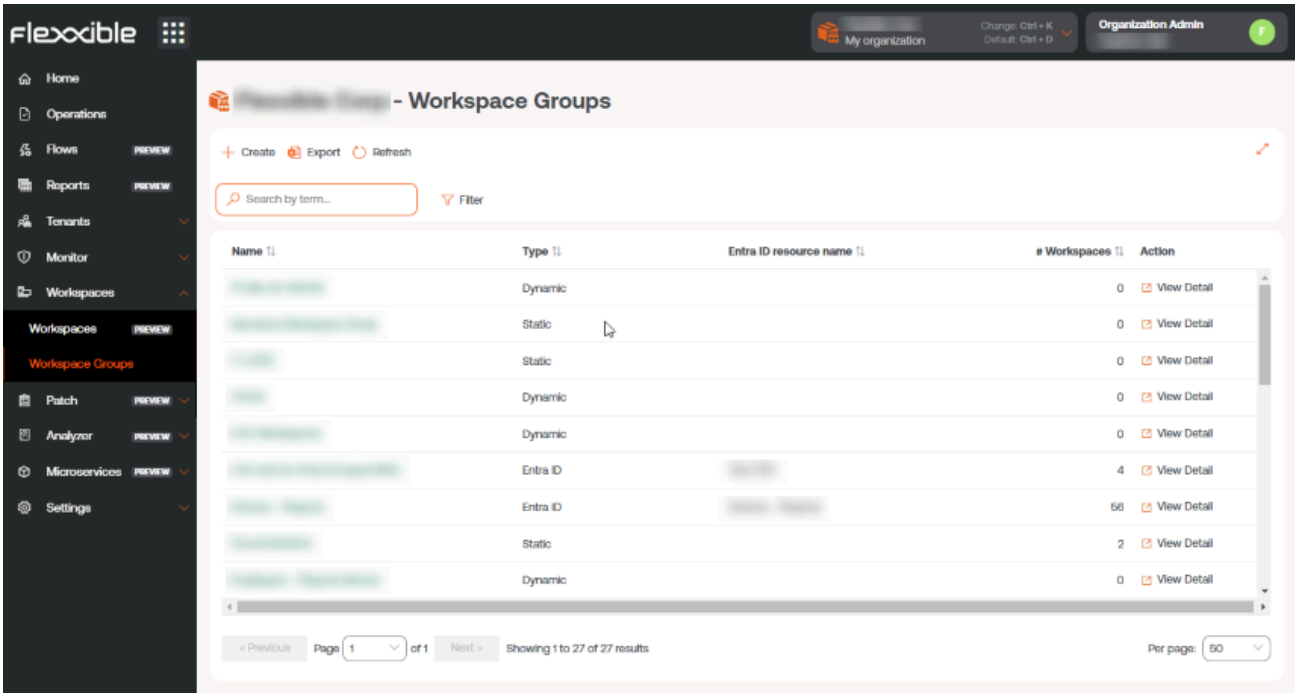
Pending updates

Displays a table with the list of pending updates on the appliance. The information includes:

- **KB.** Unique identifier of the update package issued by Microsoft.
- **Title.** Name of the update.
- **Product.** Name of the product to which the update applies.
- **Severity.** Criticality level assigned to the update according to its importance or impact on security (*Critical*, *Important*, *Moderate*, *Low*, *Unspecified*).
- **Arrival date.** Date when the update was published or made available by the provider.
- **Category.** Functional or technical classification of the update.

Portal / Workspaces / Workspace groups

Workspace Groups make device management easier for organizations, allowing them to group devices based on 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 workspace group

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

Dynamic workspace 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 in the Workspaces section.

> **INFO**
>
> Dynamic workspace groups evaluate the fulfillment of a defined condition every 60 minutes; therefore, they are not recommended as a mechanism for detecting user sessions.

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.

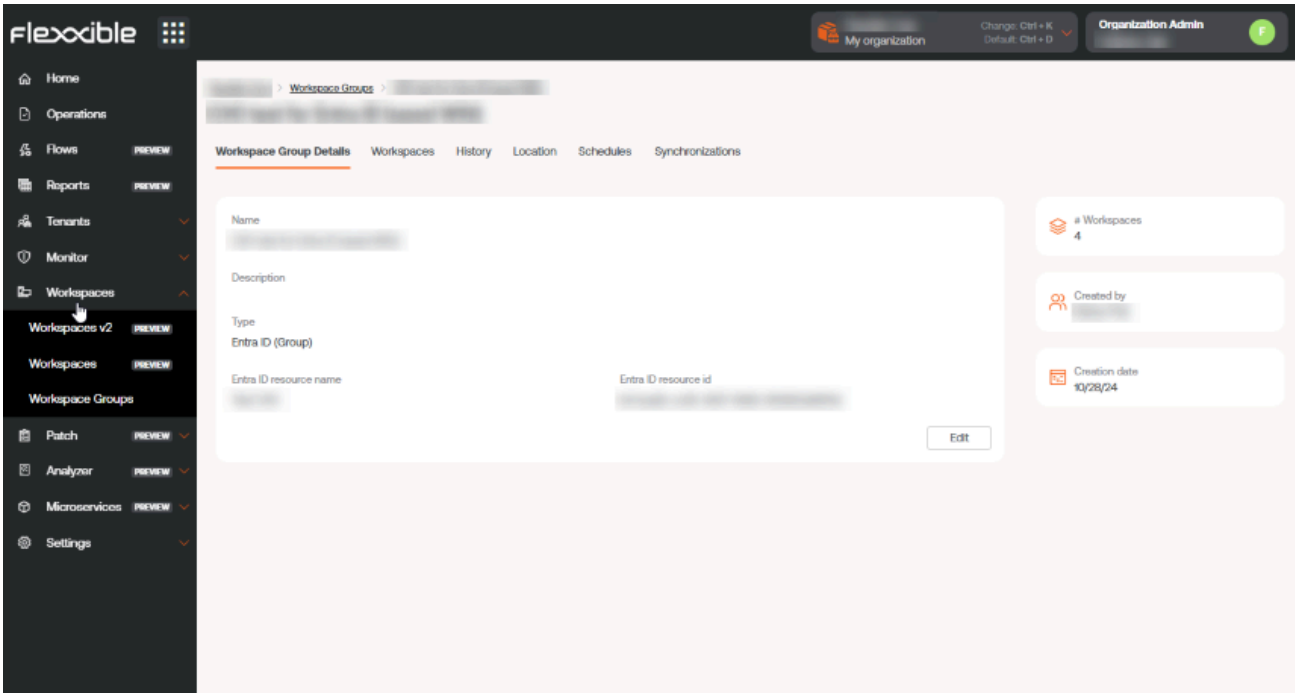
Group management

The list view of the Workspace groups section provides information on the name of the groups, their type, Entra ID feature, and the number of devices they contain. The `See Details` button shows the following tabs:

- Workspace group details
- Workspaces
- History
- Location
- Schedule
- Synchronizations

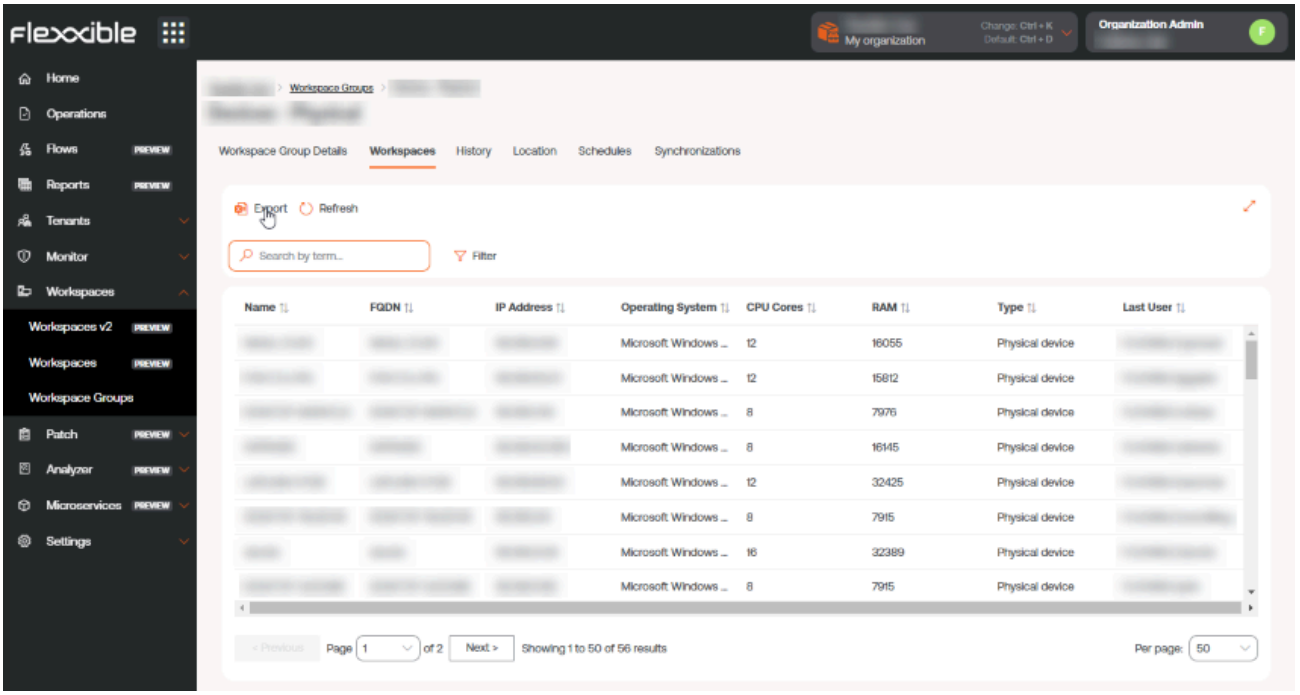
Workspace Group Details

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 you to change the device name, add a description, or even delete it.



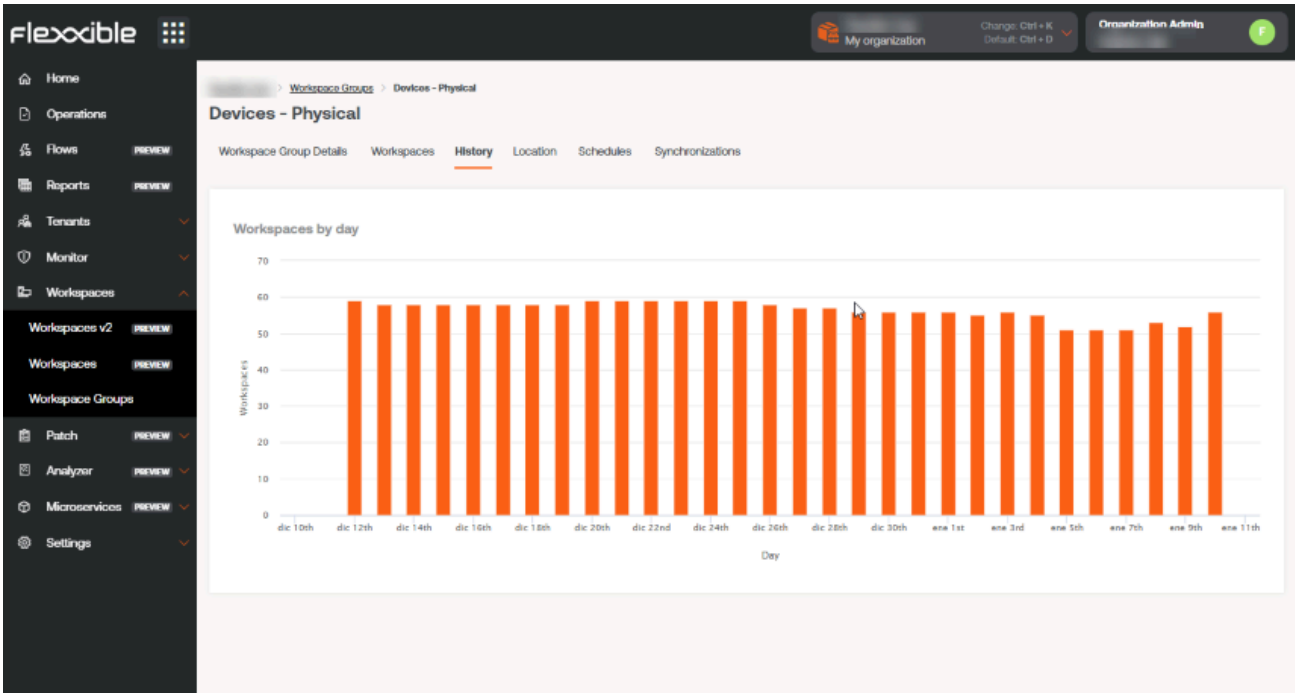
Workspaces

Displays a table with a list of the devices 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.



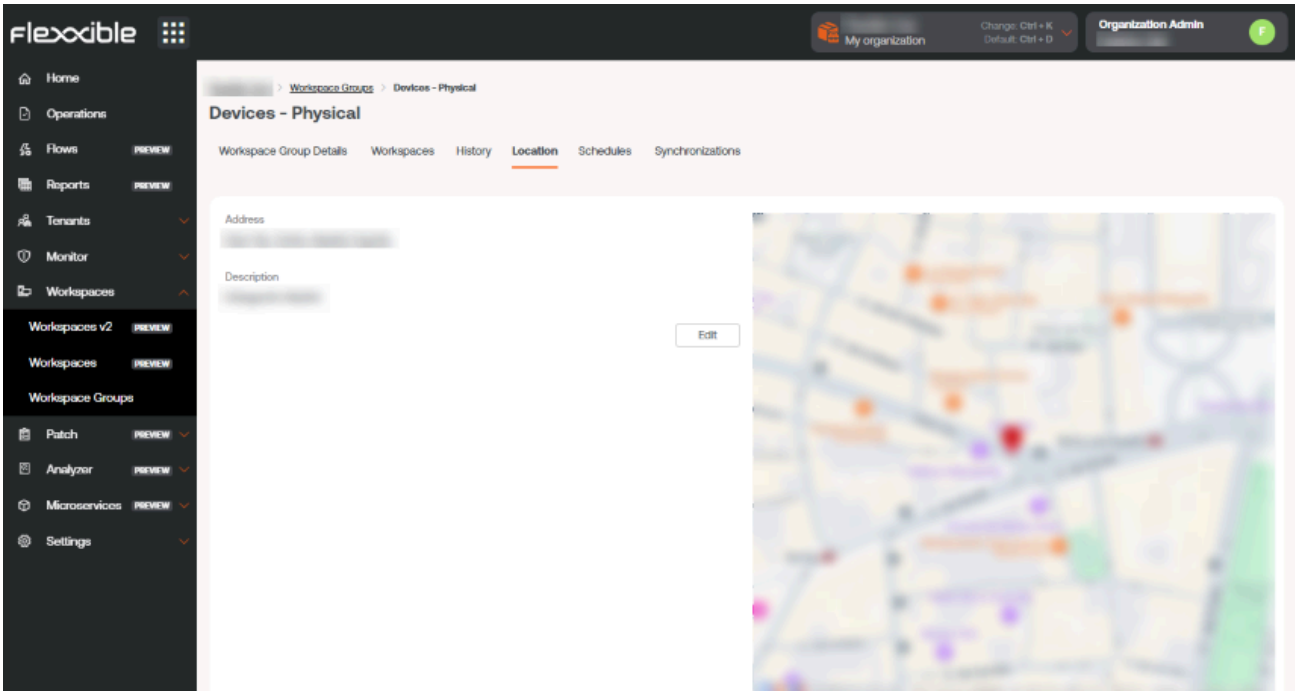
History

Displays a bar chart with the daily number of devices that have made up the group during 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

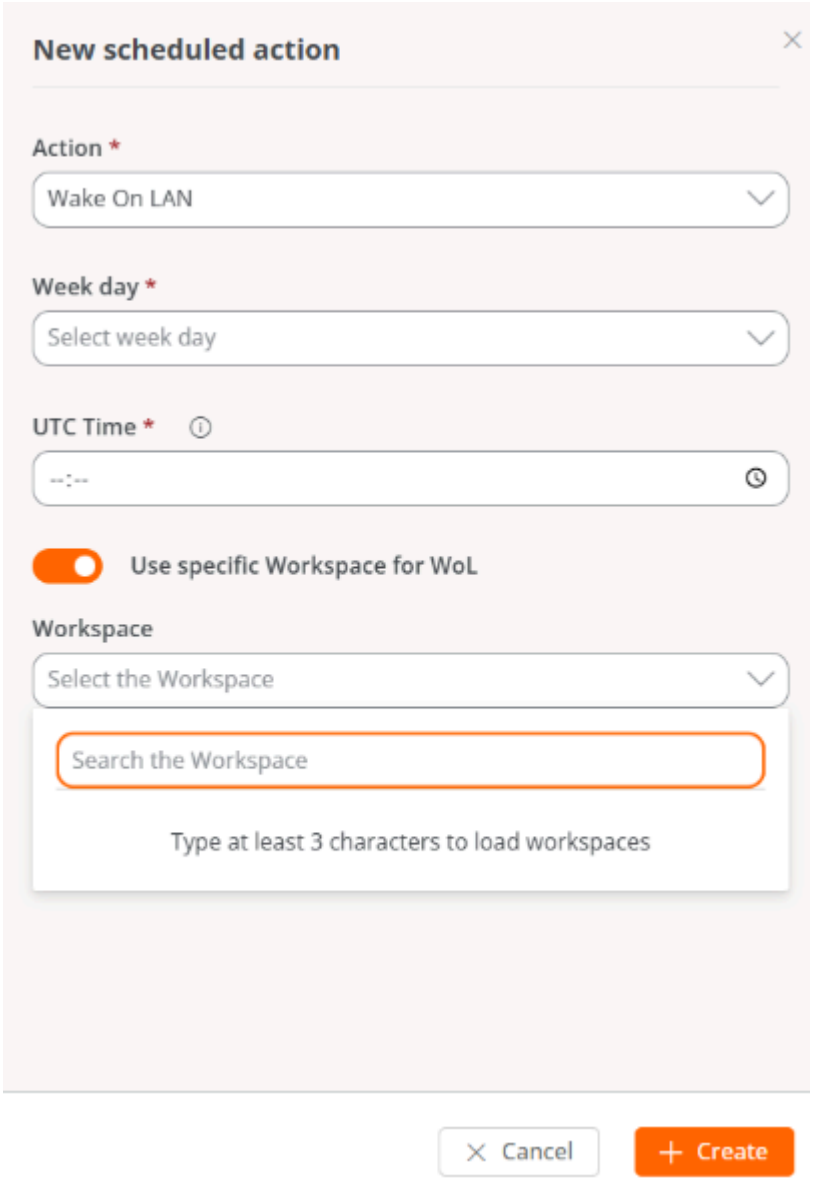
Allows associating GPS coordinates with the workspace group to relate it to a point on the map. This value is just a reference, it does not update if users change location.



Schedule

From this tab, you can schedule Wake on LAN (WoL) or automatic shutdown for a group of workspaces. If the user wants to schedule one of these actions, they need to click the `New` button and fill out the form:

- **Action.** Allows you to choose between *Wake on LAN* or *Shutdown*. If the first option is selected, you can activate `Use specific Workspace for WoL` at the bottom of the form to schedule the power on for a specific device.
- **Day of the week.** Day of the week when the action will be performed.
- **UTC Time.** Exact time to start the action, in Coordinated Universal Time standard. The action created can be seen in a table, with columns showing the information entered in the form, as well as which user created the action and who and when the schedule was updated. From `View details` you can edit and delete the scheduled action.

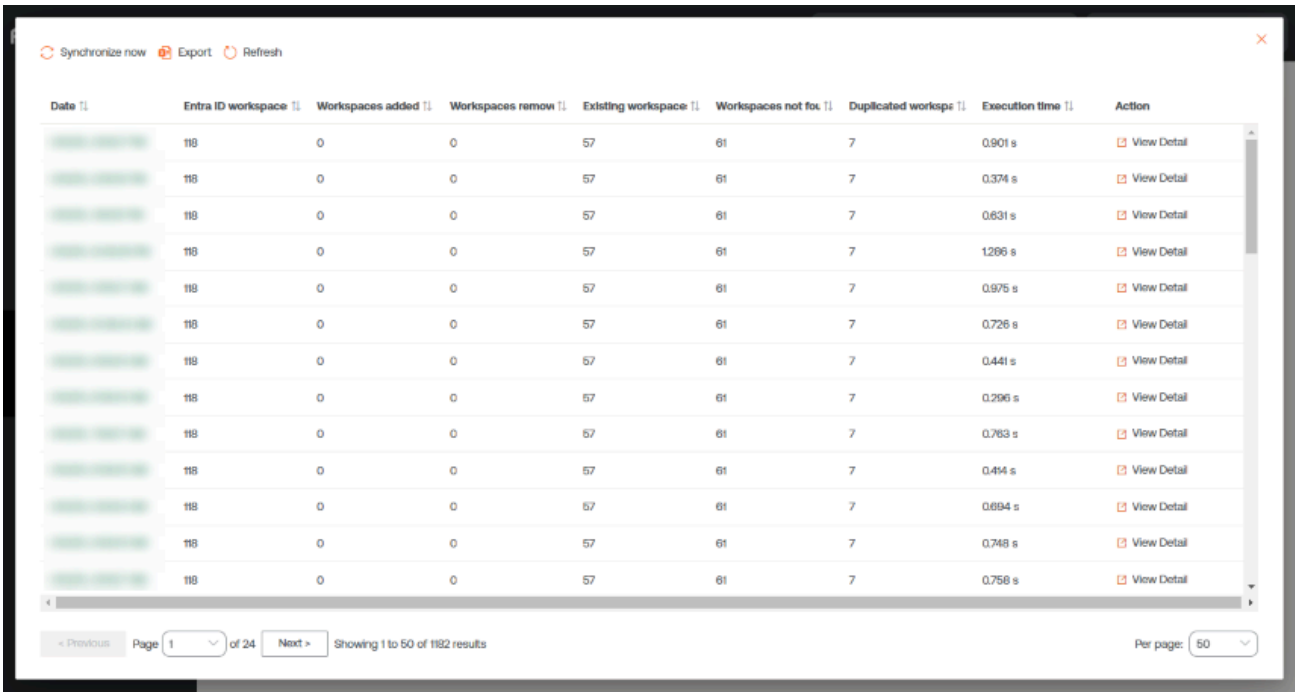


Sync

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

- Sync date and time.
- **Entra ID Workspaces.** Total number of items in the group or organizational unit of Entra ID.
- **Added Workspaces.** Number of devices added to the group.
- **Removed Workspaces.** Number of devices removed from the group.
- **Existing Workspaces.** Number of devices already present in the group.

- **Workspaces Not Found.** Number of devices not found in the group; that is, devices that, although part of the Entra ID group or organizational unit, cannot be added to the group as they do not have FlexxAgent installed.
- **Duplicate Workspaces.** Number of duplicate workspaces in the group, if any.
- **Execution Time.** Time required for synchronization.
- **Action.** Allows you to see a table with synchronization information for each device in the group.

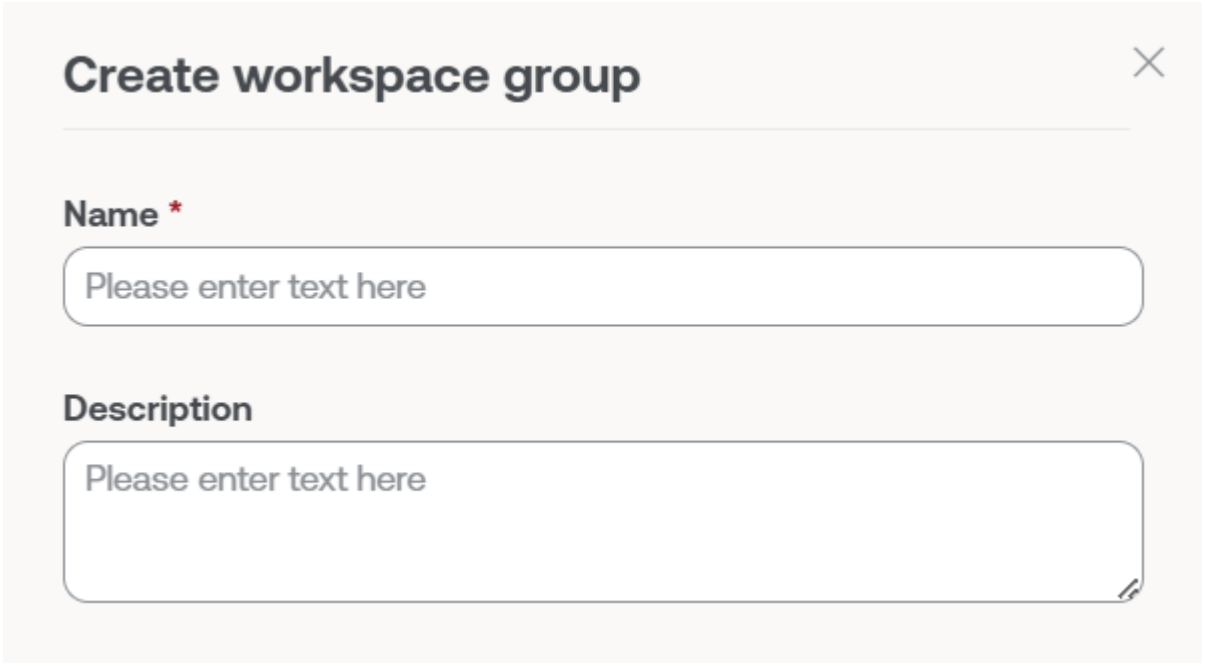


Create groups

Workspace groups can be created from the Portal and from the Workspaces module.

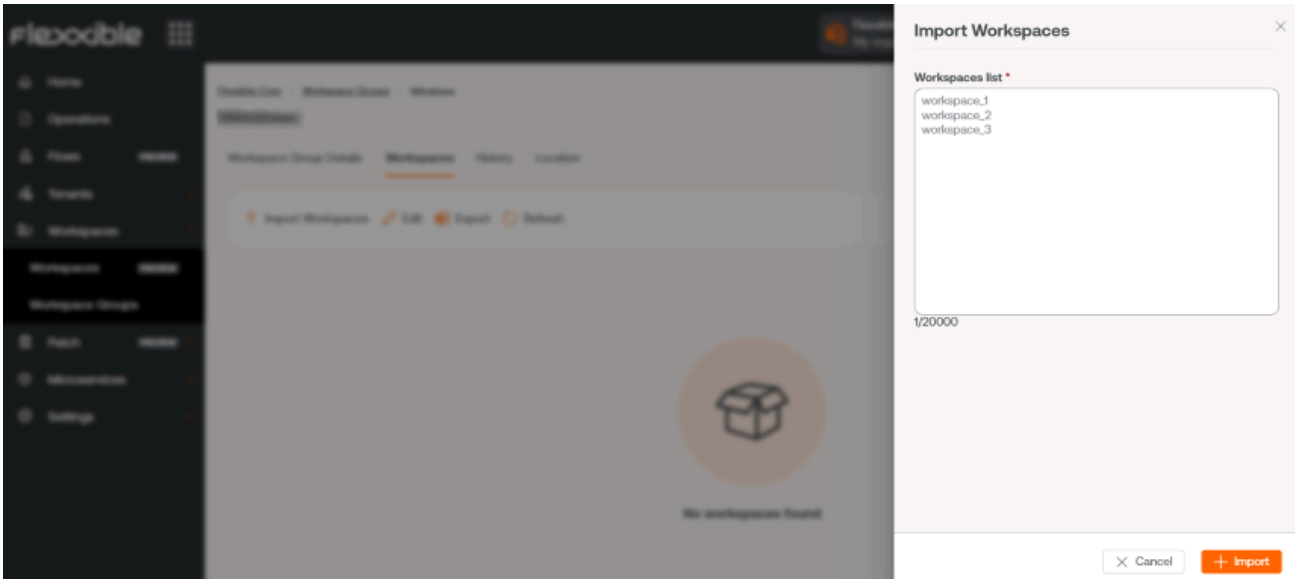
Create a static workspace group from the Portal

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

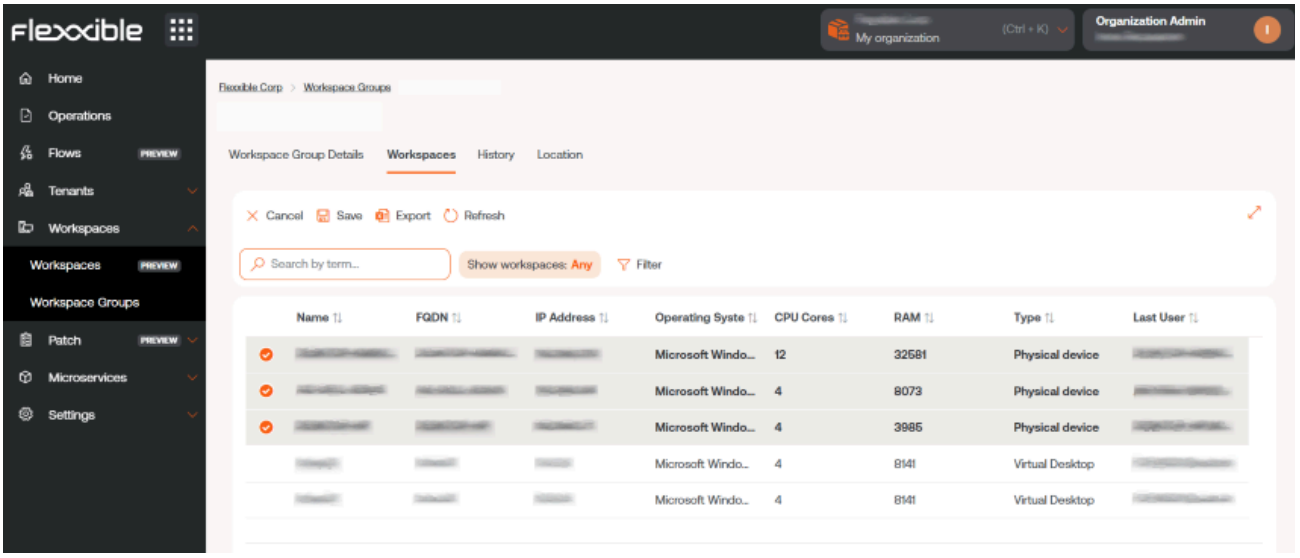


There are two ways to add devices to a static workspace group from Portal:

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



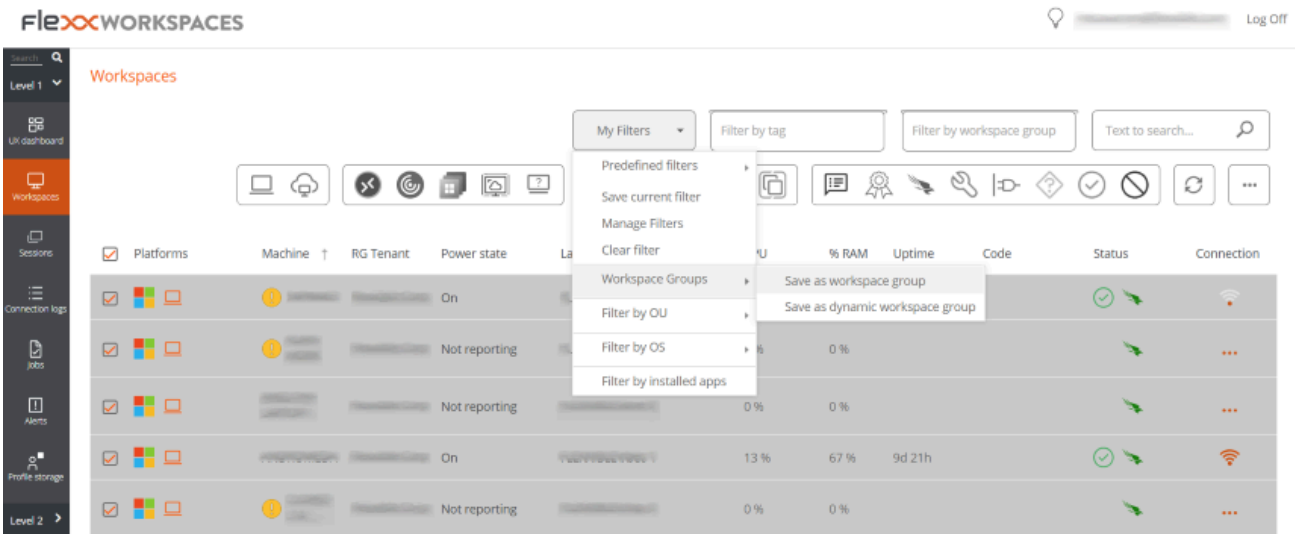
2. In the groups table, click on `Detail View` of the desired group -> `Workspaces` -> `Edit`. Next, select the devices you want to add. Those marked with an orange dot are added to the group and those not marked are removed. In both cases, click on `Save` to keep the changes.



> **INFO**
>
> Organizations can import into a static workspace group those devices that are part of their suborganizations.

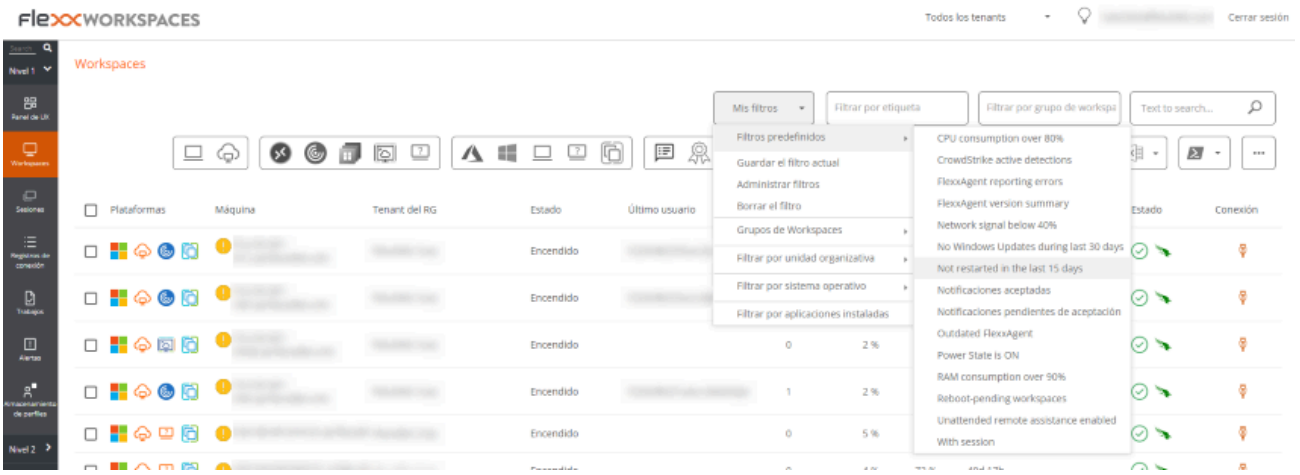
Create a static workspace group from Workspaces

In the sidebar of the Workspaces module, navigate to the Workspaces section. 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`.



Create a dynamic workspace 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 select filters from `My filters` -> `Default filters` or from any filtering option offered by the Workspaces view.

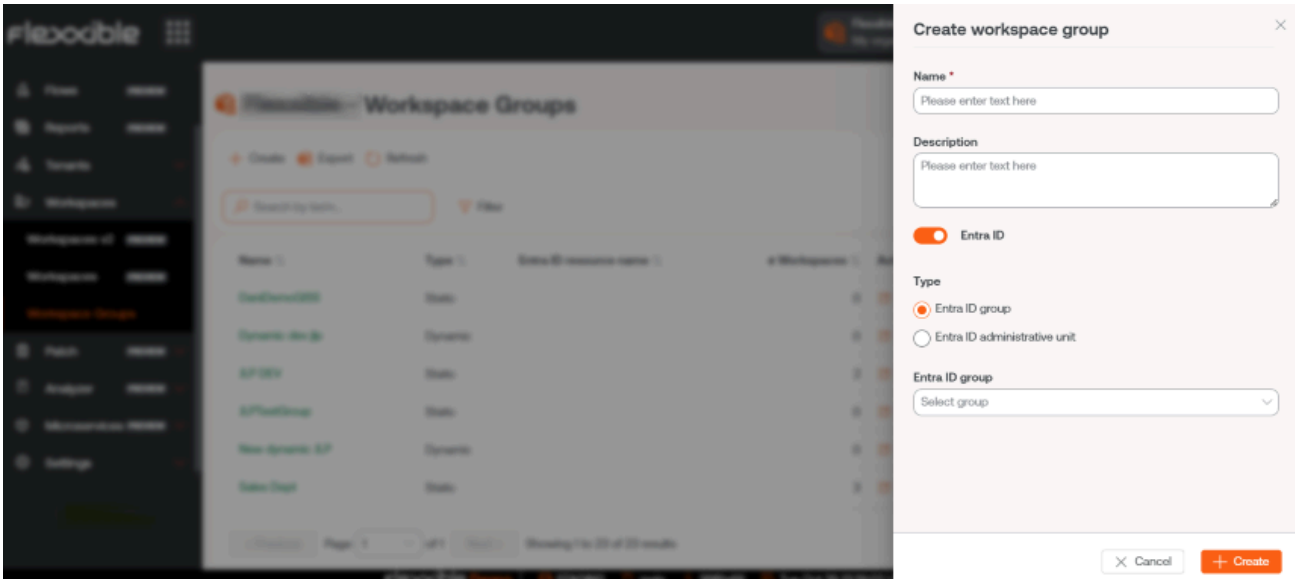


With the device list ready, go to `My filters` -> `Workspace group` -> `Save as dynamic workspace group`. Workspaces will not allow creating a group if the filters for the devices are not specified first.

Workspaces will create a Job with the new group. If you want to verify that it has been formed correctly, you can do so from the list view in the Workspace groups section, in Portal.

Create a Workspace group Enter ID

Entra ID groups are created from Portal. Go to `Workspace groups` in the side menu. 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 you check the created **Enter ID Group** and **Enter ID Administration Unit** and, therefore, perform operations on them from the Workspaces module.

Group editing

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

Edit a dynamic workspace 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 list view of the Workspaces section.
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.

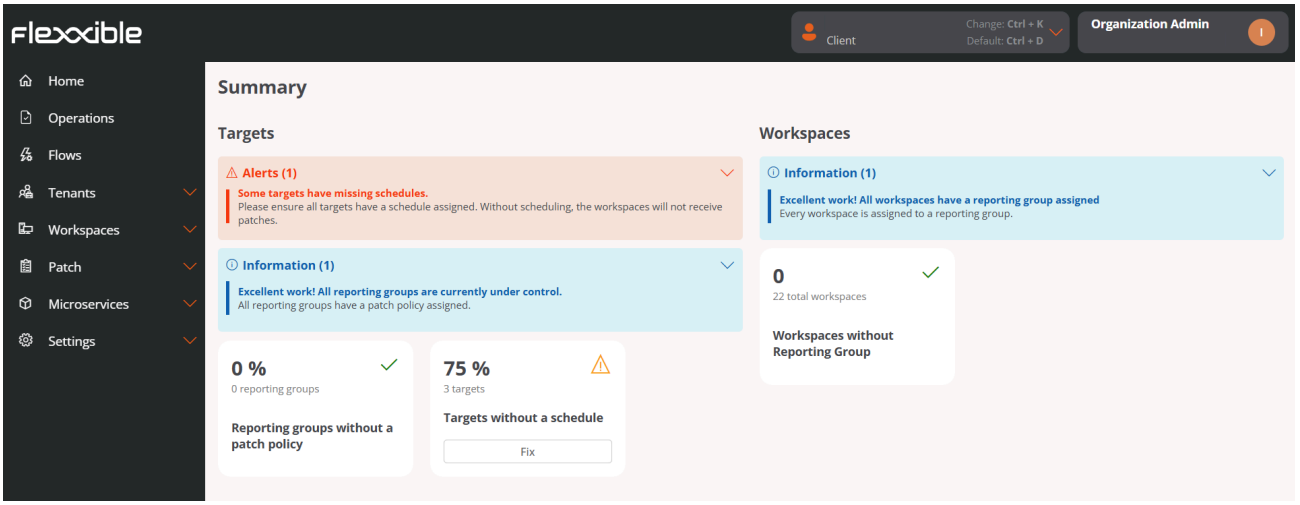
Delete a workspace group

In the list view of the Workspace groups section, 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 / Patch

Through **Updates**, a user will be able to manage how, which, and when updates will be applied to the devices of the organization's report groups.



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.
- 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 to install and which not to, according to the policy set by the user in Portal. If FlexxAgent does not detect any directive for applying updates, it will execute the patches as they become available, according to the device's own settings.

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 / Patch / Summary

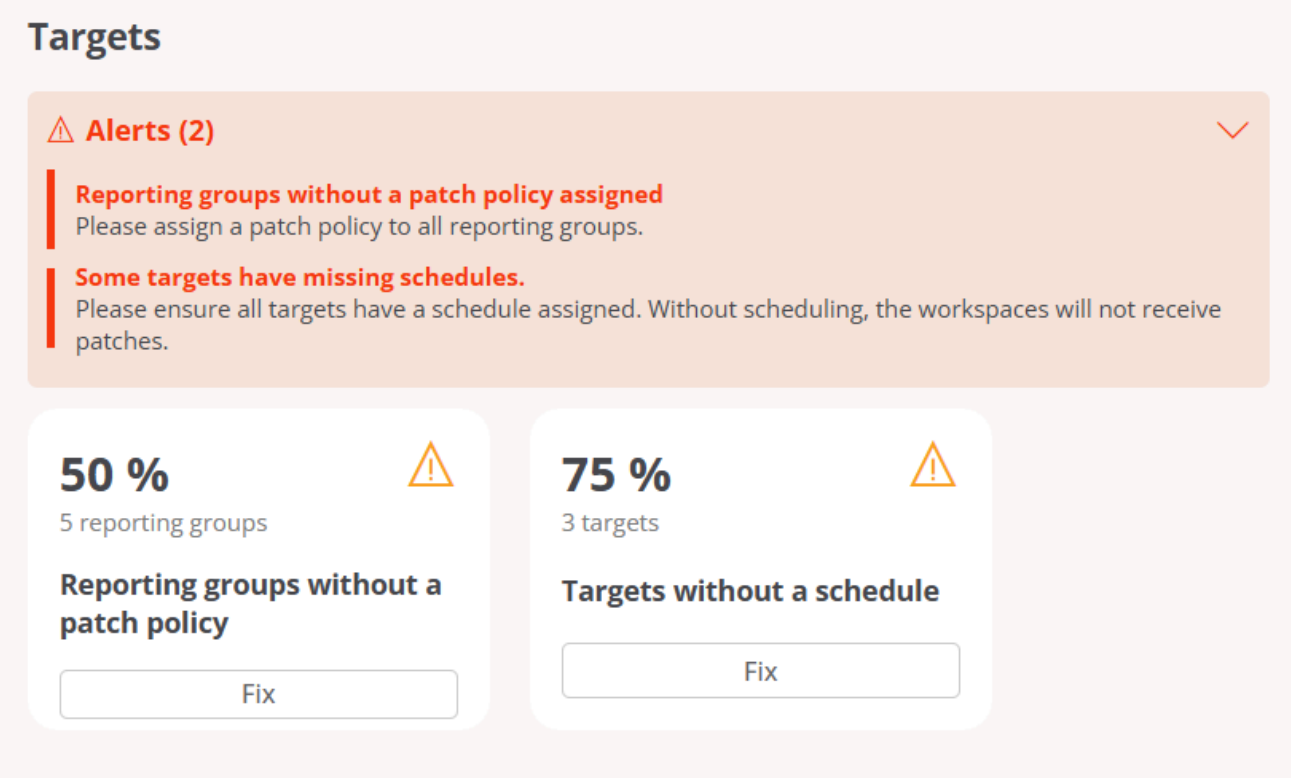
Summary shows a panel describing the patch application status on the organization's devices. From this view, you can get quantitative information about two aspects:

- Targets
- Workspaces

Targets

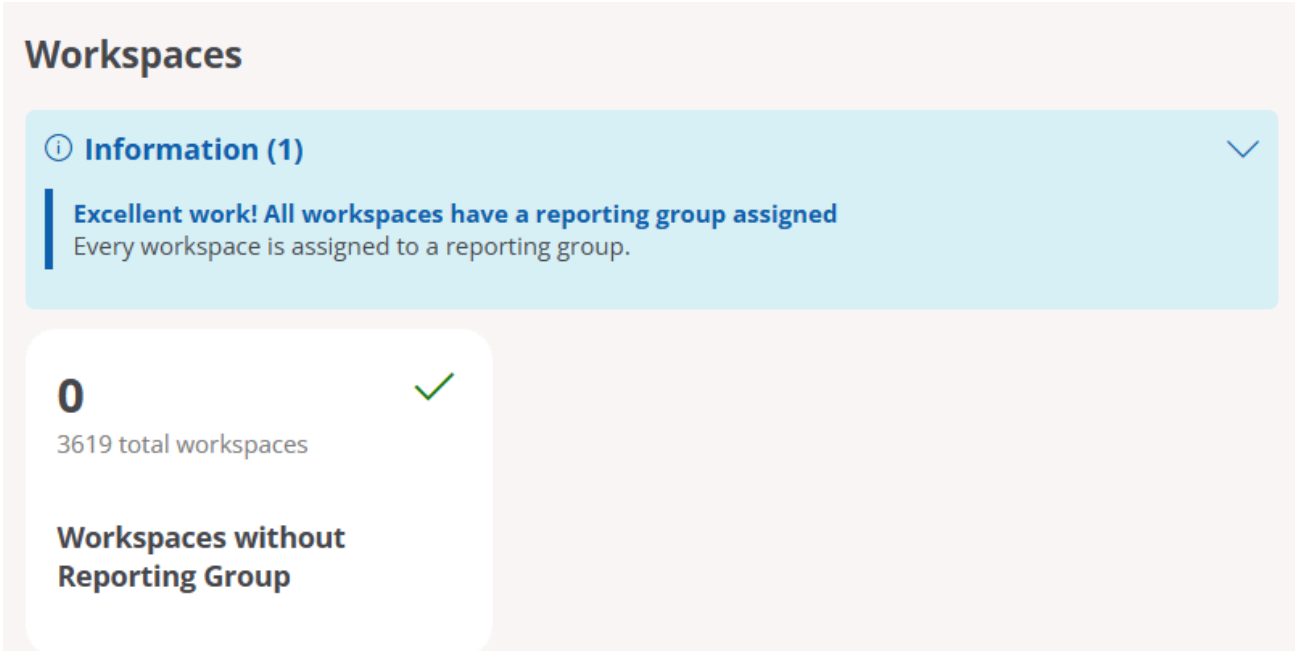
This panel shows the percentage of reporting groups in the organization without a defined patch policy, as well as the percentage of targets without a configured schedule.

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

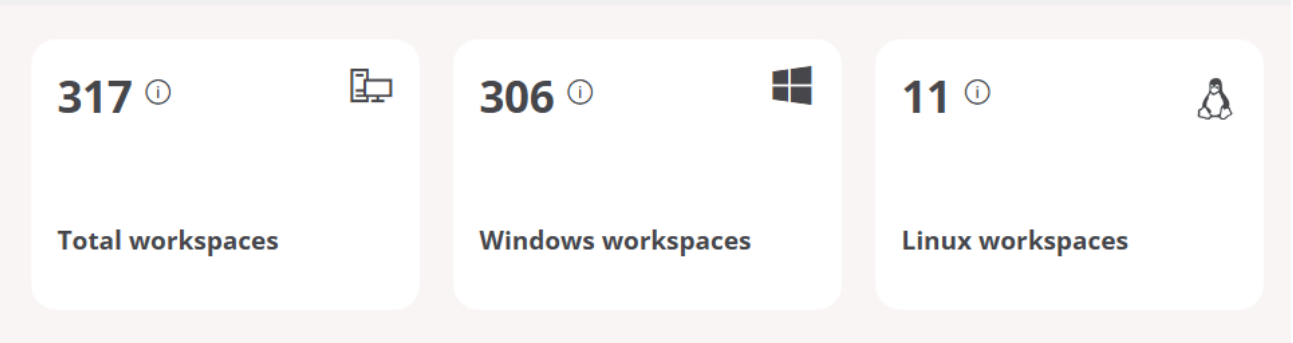
This panel informs about the organization's devices without an assigned reporting group. When FlexxAgent detects this type of devices, a warning notice (in orange) is shown; when all devices have an assigned reporting group, it is indicated through an informational notice (in blue).



Portal / Patch / 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.

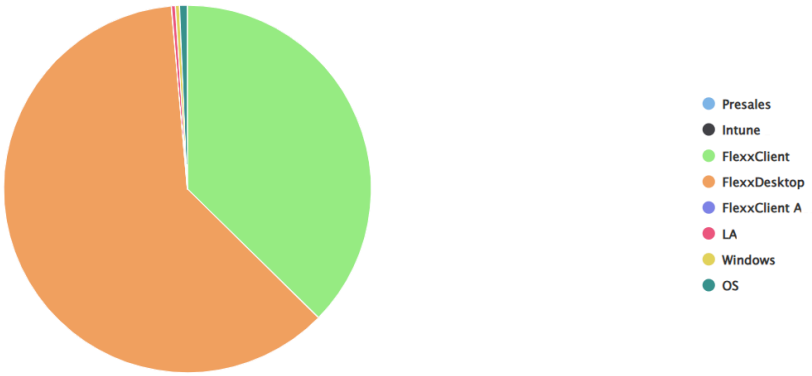


> **INFO**
>
> A reporting group can only have one target, but a target can be applied to more than one reporting group.

Total devices per reporting group

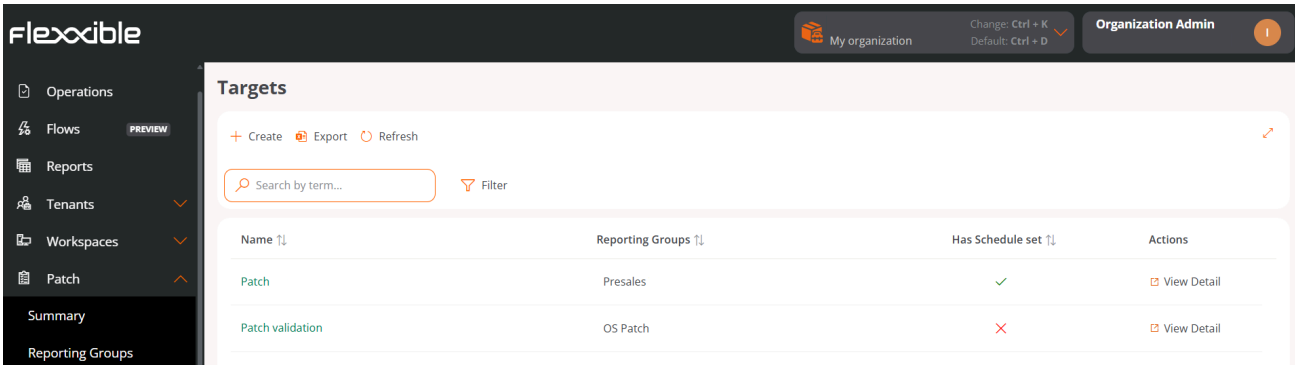
At the bottom of this section, this panel indicates the distribution of devices in an organization according to the reporting groups that FlexxAgent has identified.

Total workspaces by reporting group ⓘ



Portal / Patch / Targets

Through **Targets**, you define when, to whom, and how updates are applied. Allow creating, configuring and deleting patch policies on devices that are part of certain reporting groups within an organization.



The overview of this section shows a table with the list of created targets:

- **Name.** Name assigned to the target.
- **Reporting groups.** Name of the reporting group (there can be more than one) that will be subject to the target's update policy.
- **Has scheduled programming.** Indicates if the target has patch application scheduling enabled.
- **Actions.** Shows the link `View details`, which opens a window with the target details and its configuration options.

> **INFO**
>
> Update policies are applied to reporting groups; it's not possible to apply them to an individual device from the Portal. To force the update of a specific device, it must be done from the Workspaces module: `Workspaces` -> `Operations` -> `OS patching` -> `Patch OS now`.

Create a new target

To create a new target and define its update policy, click `New` at the top of the table. A modal window will then open with a form where you must assign a name to the new target, the reporting groups to which its update policy will apply (it can be one or more reporting groups), and optionally, its linkage to a Microsoft update policy.

> **TIP**
>
> For more information on how to create a new update policy, please check this guide.

Target details

From this view, you can configure the target update policy in two areas: *Details* and *Scheduling*.

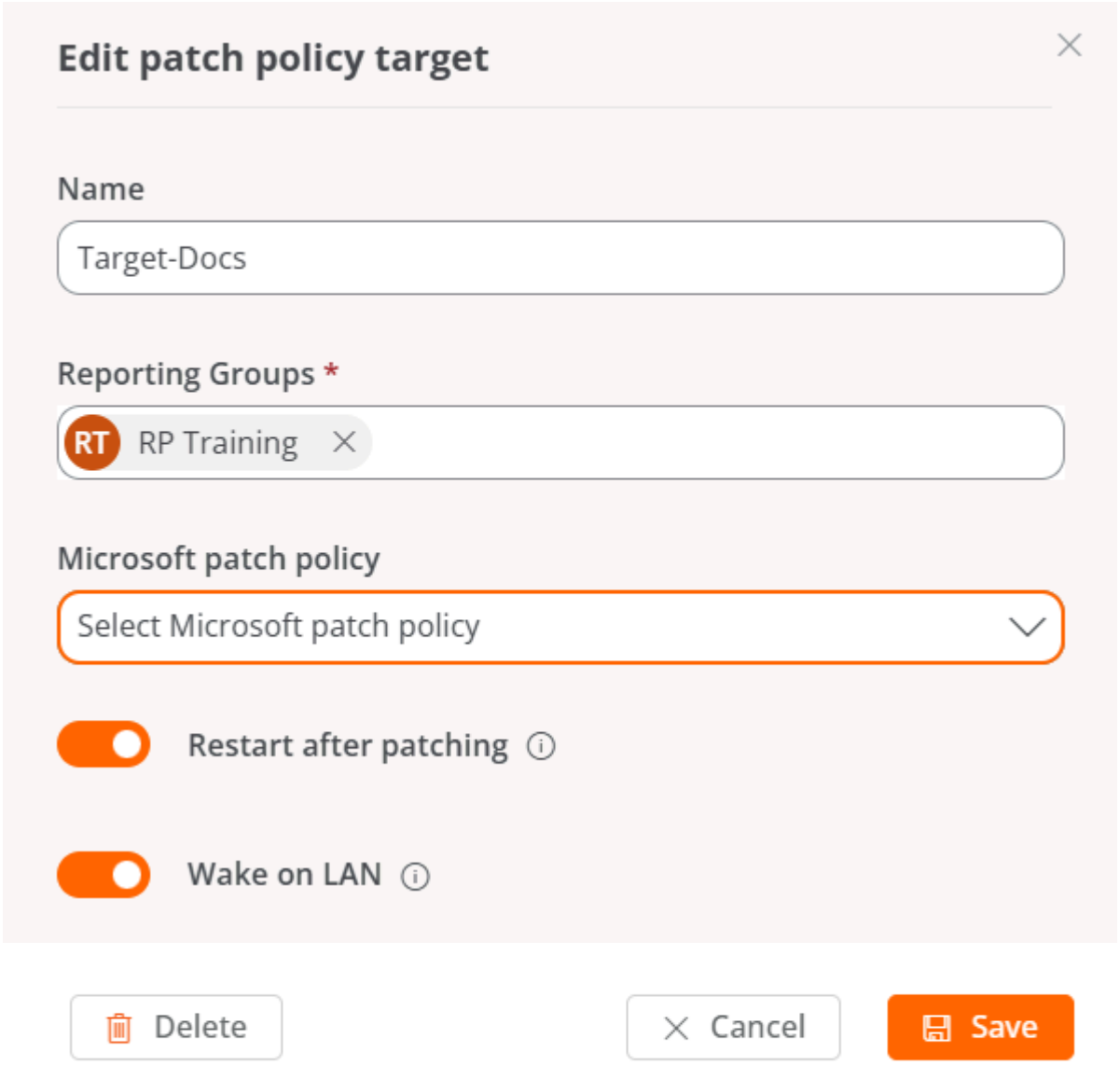
Details

This tab shows the following information about the policy being consulted:

- **Name.** Name assigned to the target.
- **Restart after applying updates.** Indicates if the device will restart automatically once patch installation is complete.
- **Wake on LAN (WoL).** Indicates if updates will be executed when devices are in sleep or shutdown state.
- **Microsoft update policy.** Name of the Microsoft update policy being applied to the target.
- **Reporting groups.** Shows the reporting groups to which the update policy has been assigned.

> **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.



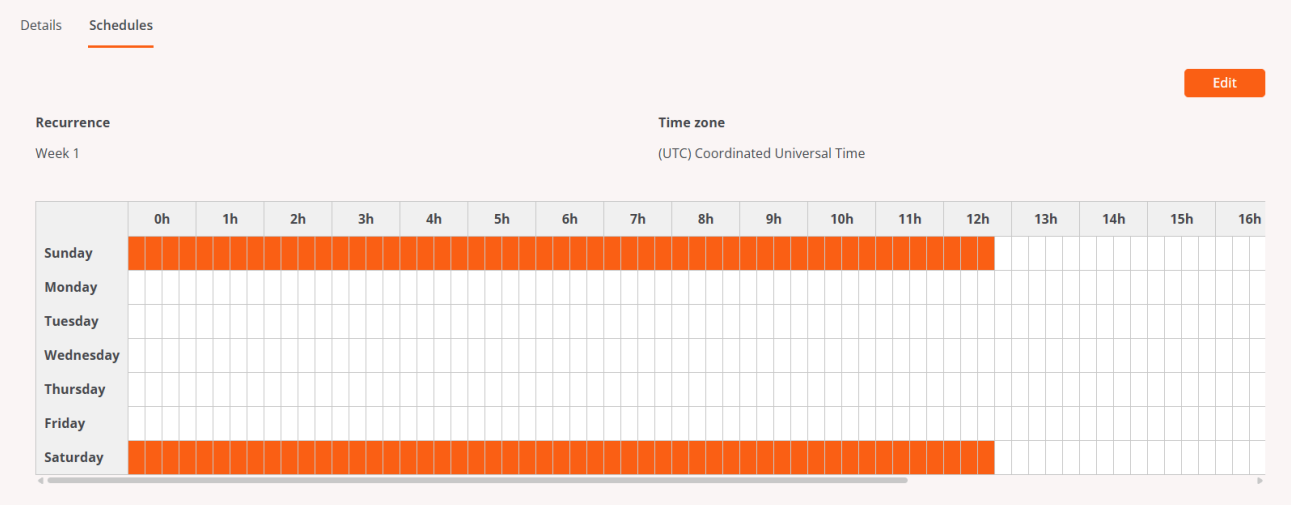
The `Delete` button discards the target's update policy.

`Details` also provides information about the creation date of the update 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 you to configure the time zone and the time frequency for applying updates, which can be limited according to weeks of the month, days, and hours.



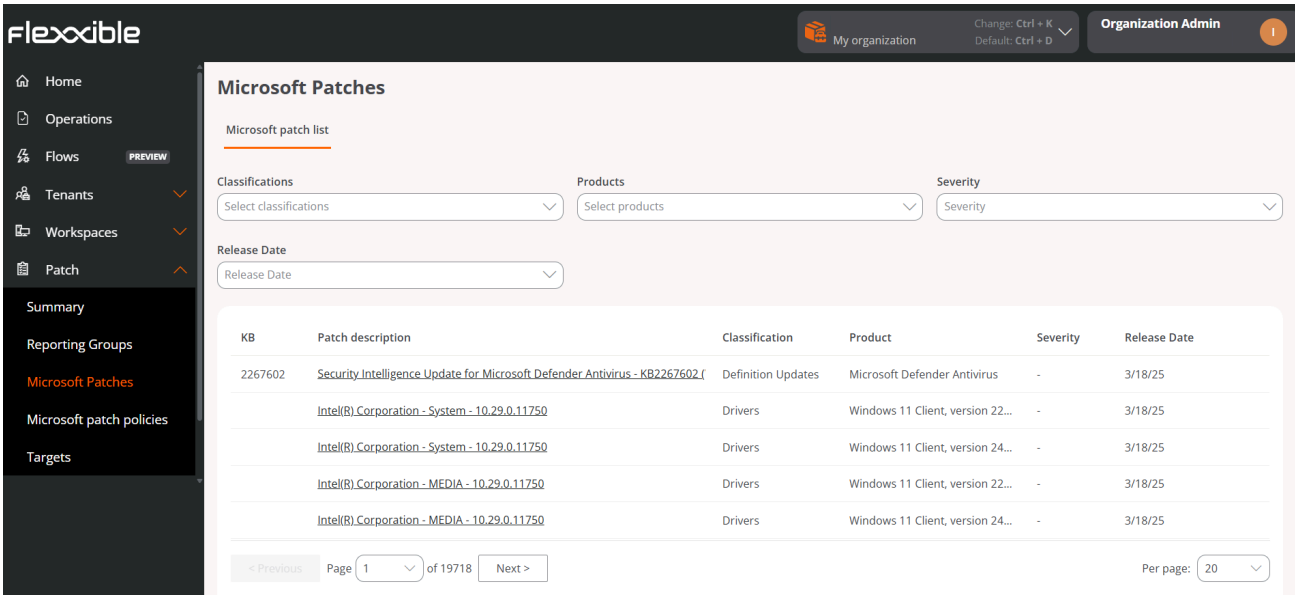
> **INFO**
>
> Automatic patch updates from Windows Update will be disabled on all devices belonging to a report group that is part of a target.

Update process

The details of the update processes launched to each device can be reviewed in the Jobs section of the Workspaces module.

Portal / Patch / Microsoft patches

Microsoft Updates allows you to check the catalog of available Microsoft updates. The table fields provide the following information:

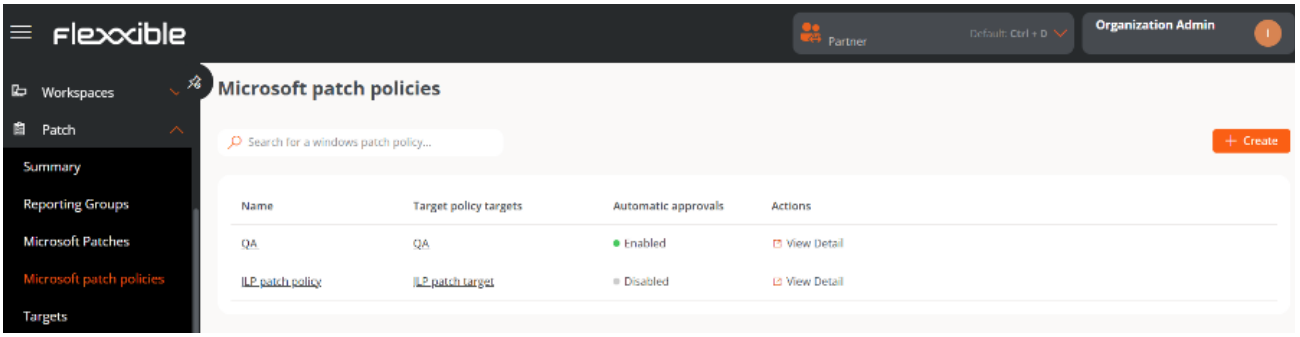


- **KB (Knowledge Base).** Unique identifier assigned to the Microsoft update package. Some drivers or firmware do not have an assigned KB.
- **Revision Description.** Link to detailed information about the update.
- **Classification.** Category assigned to the update.
- **Product.** Name of the Microsoft product to which the update applies.
- **Severity.** Level of urgency detected for executing the update.
- **Release Date.** Date since the update is available.

At the top of the table, you can filter the list by `Classification`, `Product`, `Severity` and `Release date`.

Portal / Patch / Microsoft patch policies

While Targets are used to define when, how, and to whom updates are applied, **Microsoft Update Policies** define what gets updated; that is, it manages 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

1. Access `Portal` -> `Updates` -> `Microsoft Update Policies`.
2. Click `New` at the top right of the interface.
3. In the form, assign a name to the new policy.
4. Click on `Save`.

The newly created policy will appear in the table, along with the following fields:

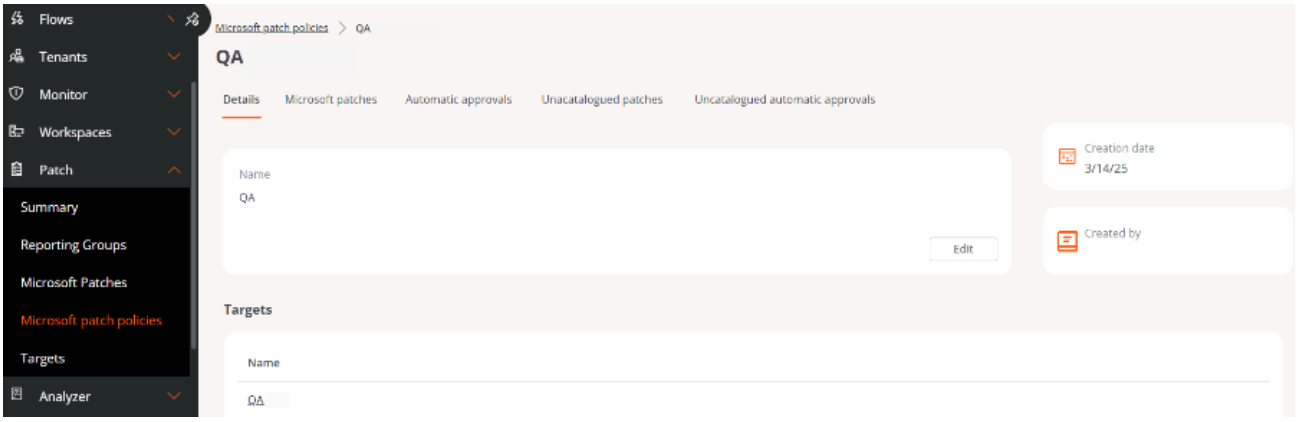
- **Update policy targets.** Targets configured with a Microsoft update policy.
- **Automatic Approvals.** Indicates whether the automatic approvals setting is *Enabled* or *Disabled*.
- **Actions.** Contains the `View Details` button, which allows access to the configuration scopes: *Details*, *Microsoft Updates*, *Automatic Approvals*, *Uncataloged Updates*, and *Uncataloged Automatic Approvals*.

Details

From this tab you can view basic information about the policy:

- Name
- Linked Targets
- Created date
- Creator User

The `Edit` button opens a form that allows you to modify the policy's name or delete it.



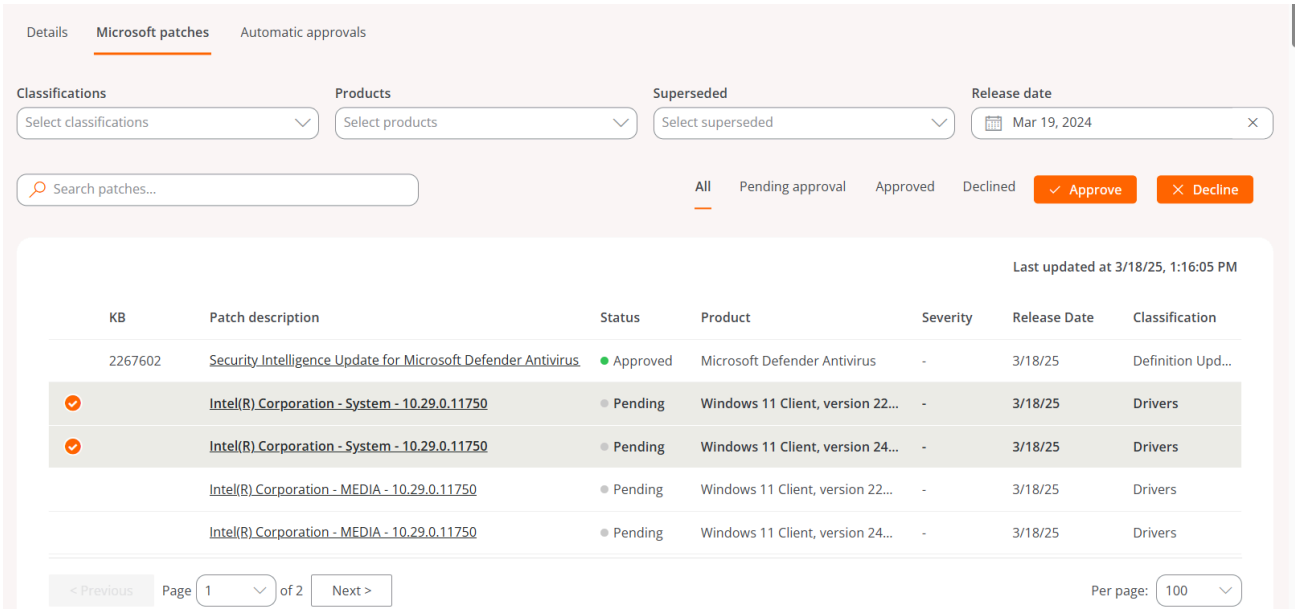
Microsoft patches

This tab shows a table listing the updates available for the linked target, along with the following data:

- **KB.** Unique identifier assigned to the Microsoft update package. Some drivers or firmware do not have an assigned KB.
- **Revision Description.** Link to detailed information about the update.
- **Status.** Status of the update: *Approved*, *Rejected*, or *Pending*.
- **Product.** Name of the Microsoft product to which the update applies.
- **Severity.** Level of urgency detected for executing the update.
- **Release Date.** Date from which the update is available.
- **Classification.** Category assigned to the update. It can be *Updates*, *Critical Updates*, *Security Updates*, *Upgrades*, *Definition Updates*, *Drivers*, *Feature Packs*, and *Update Rollups*.
- **Last Update.** Date and time of the last modification of the list.

Above the table there are several filter options that allow listing updates by *Classifications*, *Products*, *Replaced*, or *Release Date*.

It is also possible to search by text strings or filter by status: *Pending Approval*, *Approved*, or *Rejected*.



Manually approve or reject an update

To approve or reject an update, select one or more entries from the table and choose the desired action:

- **Approve.** The update will be installed on the corresponding devices the next time an update process is run, according to the target configuration.
- **Reject.** The update will be attempted to be uninstalled during the next update process on devices that have it installed, according to the target configuration.

  Not all updates can be uninstalled. The execution of this process depends on the current state of the device and other factors. The result of the uninstallation attempt will be available in the corresponding update task.

> **INFO**
>
> If a user defines a Microsoft update policy but does not manually or automatically approve or reject an update package, no installation or uninstallation activity will be generated on the devices.

Automatic Approvals

This tab shows a table with the configured automatic approval rules. The fields include the following information:

- **Classification.** Category assigned to the update.
- **Products.** Name of the Microsoft product to which the update applies.
- **Days After Release.** Number of days elapsed since the publication of the update, after which it will be automatically approved.
- **Actions.** Contains the `View detail` button, which opens a form to edit the automatic approval rule.

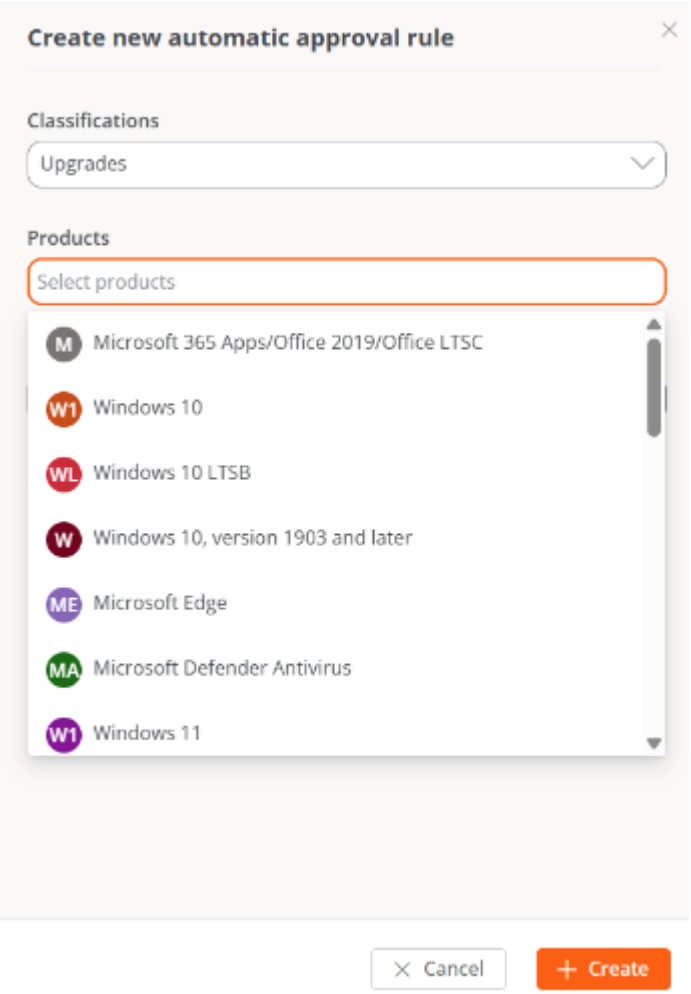
Create an automatic approval rule

It's possible to configure one or more automatic approval rules within the same update policy.

To create a new rule:

1. Access `Portal` -> `Updates` -> `Microsoft Update Policies`.
2. Select a policy.
3. Go to the `Automatic Approvals` tab.
4. Click on `New` and define:
    - Classifications
    - Products

- Days After Release



INFO

Automatic approvals are executed once a day, at 6:00 a.m. Therefore, any change in the configuration of automatic approval rules will not be applied immediately, but will normally take effect the next day.

TIP

- It is recommended to configure automatic approval rules when creating a new policy and not apply it to the target until the updates to be considered as starting point are approved. That way, when the policy is applied, you can start from a stable scenario.
- If automatic approval rules are configured, it is recommended to do so for uncataloged updates as well, in order to prevent patches from being left unapproved.

Unlisted updates

The global list of pending updates on a device can be consulted in Microsoft Updates; however, there are patches that the device may report as pending but do not appear in that list.

Unlisted Updates correspond to these cases. These are pending patches that may be related to Microsoft features but do not have an exact match with the catalog entries.

INFO

The list of unlisted updates is displayed at the tenant level.

The table shows the available uncataloged updates with the following data:

- **KB.** Unique identifier of the update package. Some drivers or firmware do not have an assigned KB.
- **Revision Description.** Link to detailed information about the update.
- **Status.** *Approved*, *Rejected*, or *Pending*.
- **Product.** Name of the Microsoft product to which the update applies.

> **NOTE**
>
> Uncataloged updates are reported by FlexxAgent according to the information obtained from the device; however, sometimes Windows does not provide information about the associated **Product**. For this reason, this field may appear empty.

- **Severity.** Level of urgency detected for executing the update.
- **Release Date.** Date since the update is available.
- **Classification.** Category assigned to the update.

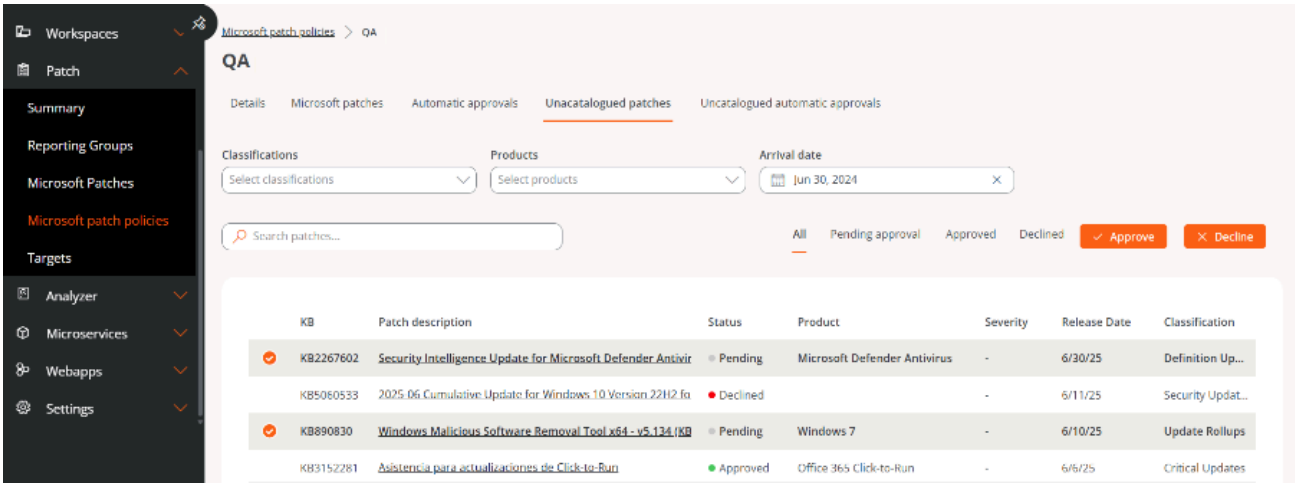
The table has filter options by *Classifications*, *Products*, or *Arrival Date*, as well as text searches and filters by status.

Manually approve or reject an uncataloged update

To approve or reject an uncataloged update, select one or more entries from the table and choose the corresponding action:

- **Approve.** The update will be installed on the devices in the next update process, according to the target configuration.
- **Reject.** The update will be attempted to be uninstalled during the next update process, according to the target configuration.

  Not all updates can be uninstalled. The execution of this process depends on the current state of the device and other factors. The result of the uninstallation attempt will be available in the corresponding update task.



Unlisted automated approvals

This tab shows a table with the configured automatic approval rules, with the following fields:

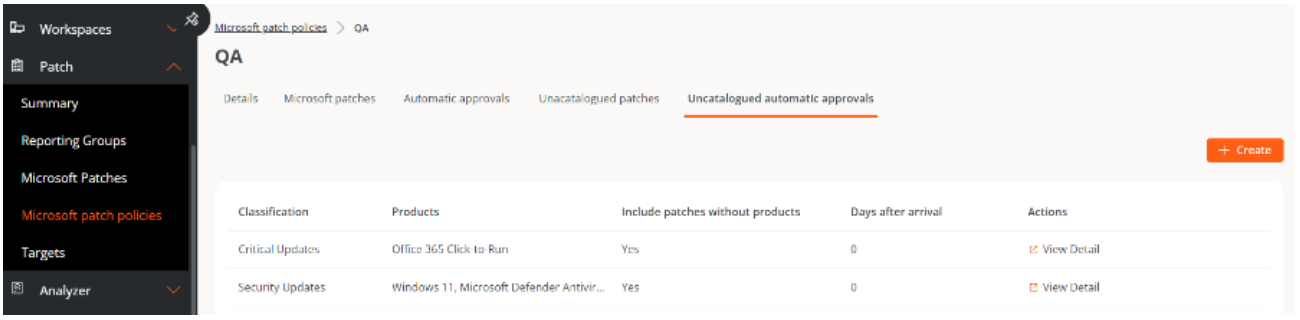
- **Classification.** Category assigned to the update.
- **Product.** Name of the product to which the update applies.

> **NOTE**
>
> Uncataloged updates are reported by FlexxAgent according to the information obtained from the device; however, sometimes Windows does not provide information about the associated **Product**. For this reason, this field may appear empty.

- **Include updates without products.** Indicates whether the automatic approval rule includes uncataloged updates without an associated product.

> **NOTE**
>
> Since there may be uncataloged updates without an associated product, Flexxible recommends activating this option to ensure that this type of update is also included in the automatic approval process.

- **Days After Arrival.** Number of days after the update arrives in the list, after which it will be automatically approved.
- **Actions.** Contains the `View Details` button that allows editing the rule.



Create an automatic approval rule for unlisted updates

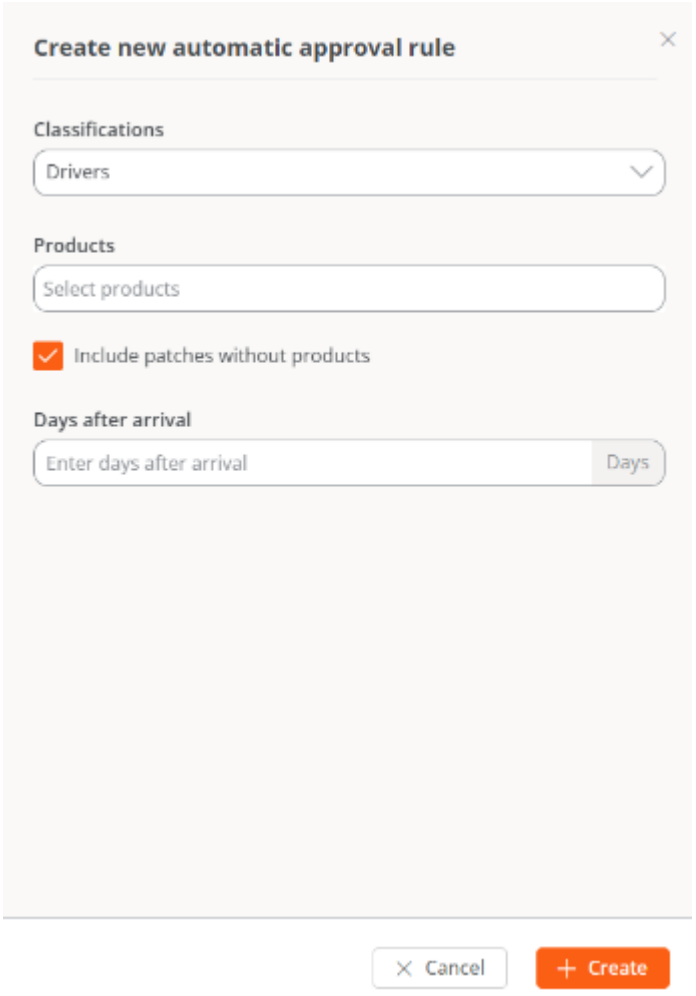
It is possible to configure one or more automatic approval rules for uncataloged updates within the same update policy.

To create a new rule:

1. Access `Portal` -> `Updates` -> `Microsoft Update Policies`.
2. Select a policy.
3. Go to the `Unlisted automated approvals` tab.
4. Click on `New` and define:
    - Classifications
    - Products
    - Days After Arrival
    - Include updates without products

NOTE

Since there may be uncataloged updates without an associated product, Flexxible recommends activating this option to ensure that this type of update is also included in the automatic approval process.

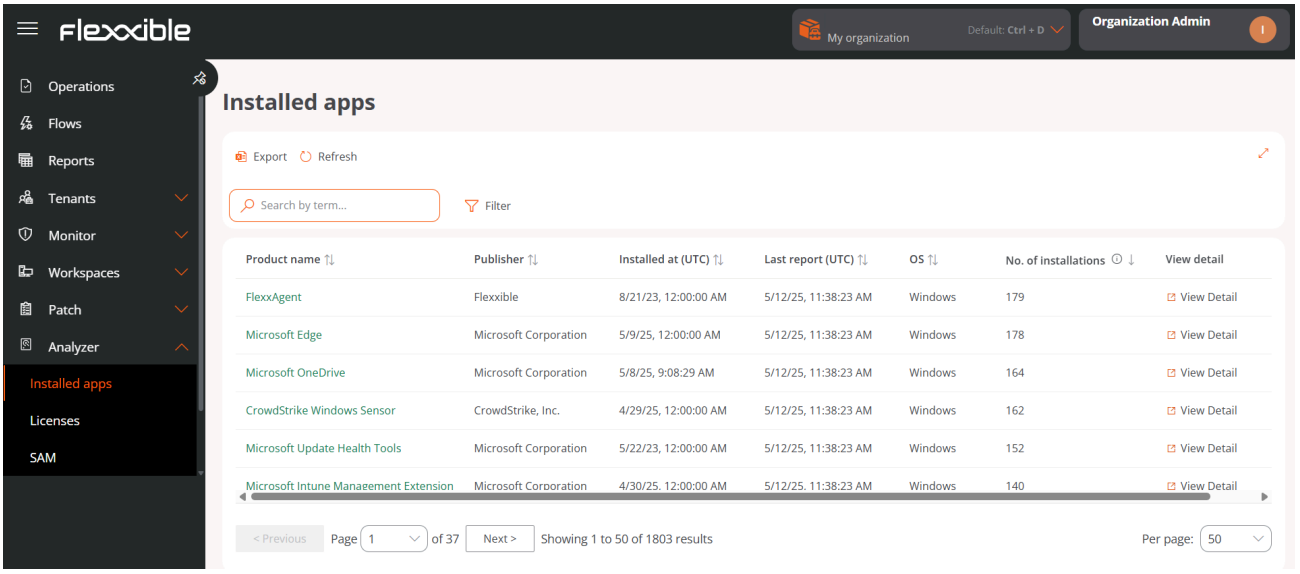


INFO

Unlisted Updates and *Unlisted Automatic Approvals* are available starting from version 25.6 of FlexxAgent.

Portal / Analyzer in Portal

Analyzer allows you to consult information about the applications installed on an organization's devices, as well as data regarding their acquired licenses.

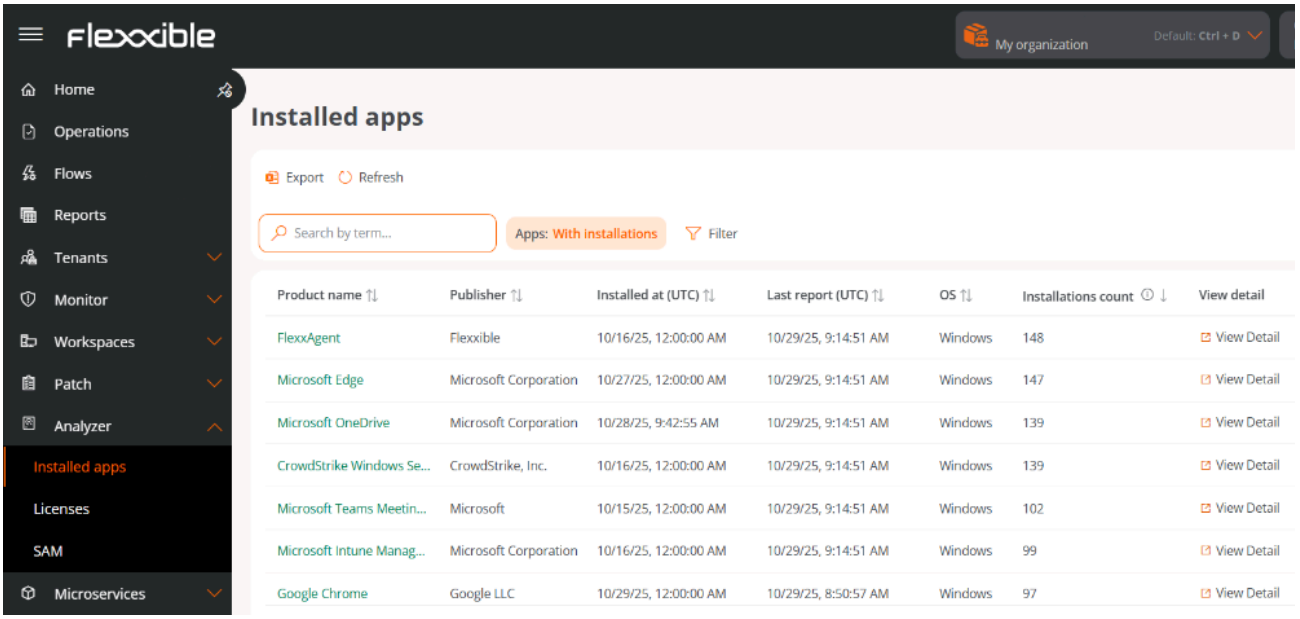


This information can also be accessed from the Workspaces section of the Analyzer module.

Portal / Analyzer / Installed apps

Installed Applications shows all applications detected by FlexxAgent on the organization's devices. From this view, the user can consult detailed information about each one, including its installation and report history, as well as the total number of devices that have it installed.

The information is collected by FlexxAgent Analyzer when its process starts. From that moment, the data is updated automatically every 12 hours, as long as there is a user session started or during each log-in.



List of installed applications

The table shows the following information:

- **Product name.** Name of the installed application.
- **Publisher.** Company developing the application.
- **Installed at (UTC).** Date and time when the application was reported for the first time on a device (in UTC time).

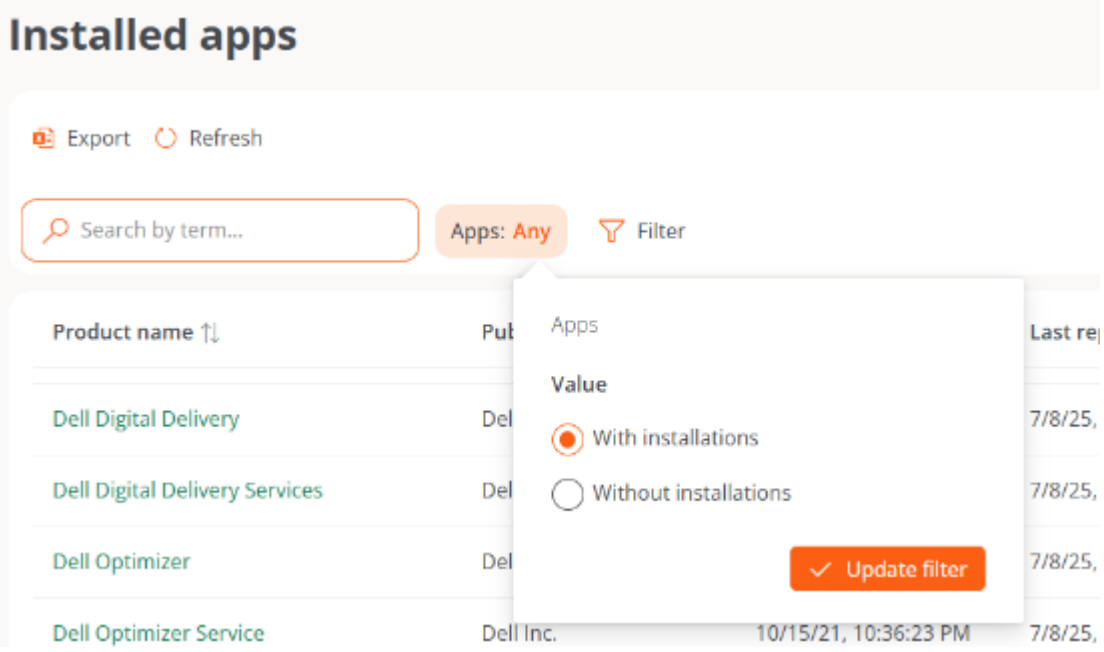
- **Last report (UTC).** Date and time of the last report received from that application (in UTC time).
- **OS.** Operating system of the devices where the application is installed.
- **Installation count.** Number of installations recorded on the organization's devices.

> **WARNING**
> This value does not represent the total in real time, because the installation count for each application is calculated every two hours.

- **View details.** Opens the detail view of the selected application.

Filters

At the top of the table is the default filter `Applications`, which allows listing applications according to their installation status:



- **With installations.** Shows applications present on at least one device.
- **Without installations.** Shows applications that were installed at some point but are no longer present on any device.

> **INFO**
>
> Historical data for *Without installations* is retained for 120 days.

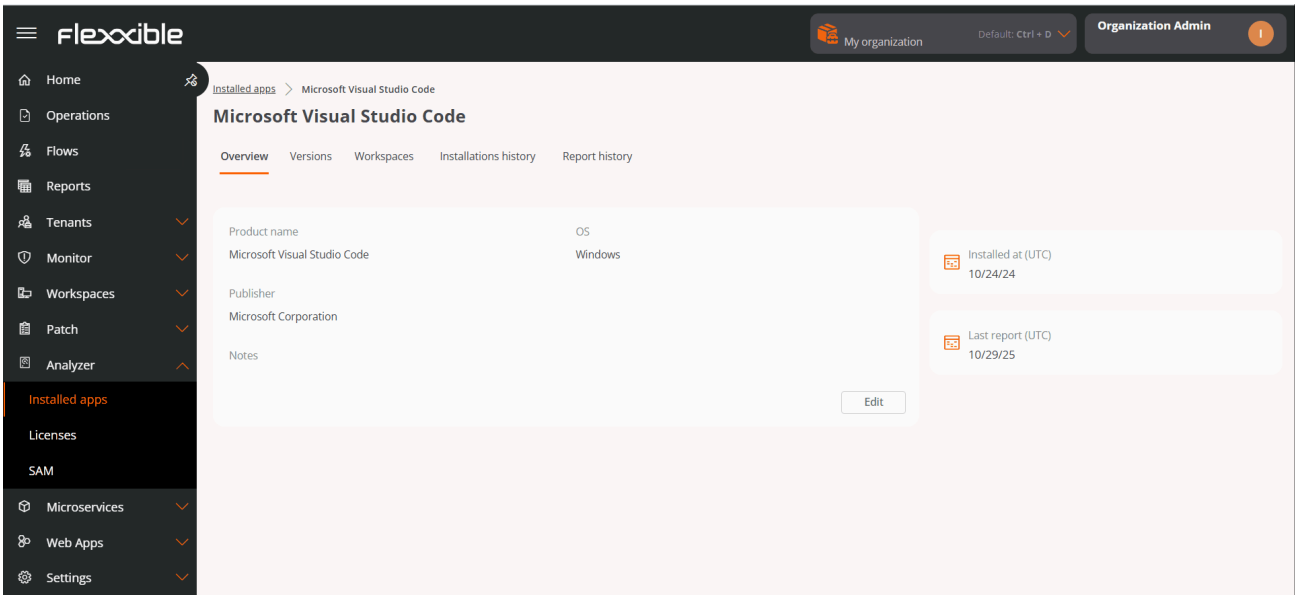
Installed Apps Details

Clicking on the name of an application or the 'View details' option, you access a view with five tabs:

- Overview
- Versions
- Workspaces
- Installation history
- Report history

Overview

It shows the same information as in the main table, plus the 'Edit' button, which allows adding a free text note.



Versions

Presents a table with the following columns:

- **Version.** Application version number.
- **Number of workspaces.** Number of devices where that version is installed.
- **Installed at (UTC).** Date of first report of the application for that version.
- **Last report (UTC).** Date of last report of the application for that version.

Clicking on a version brings up its detailed view, showing the devices that have it installed and the date of its last report.

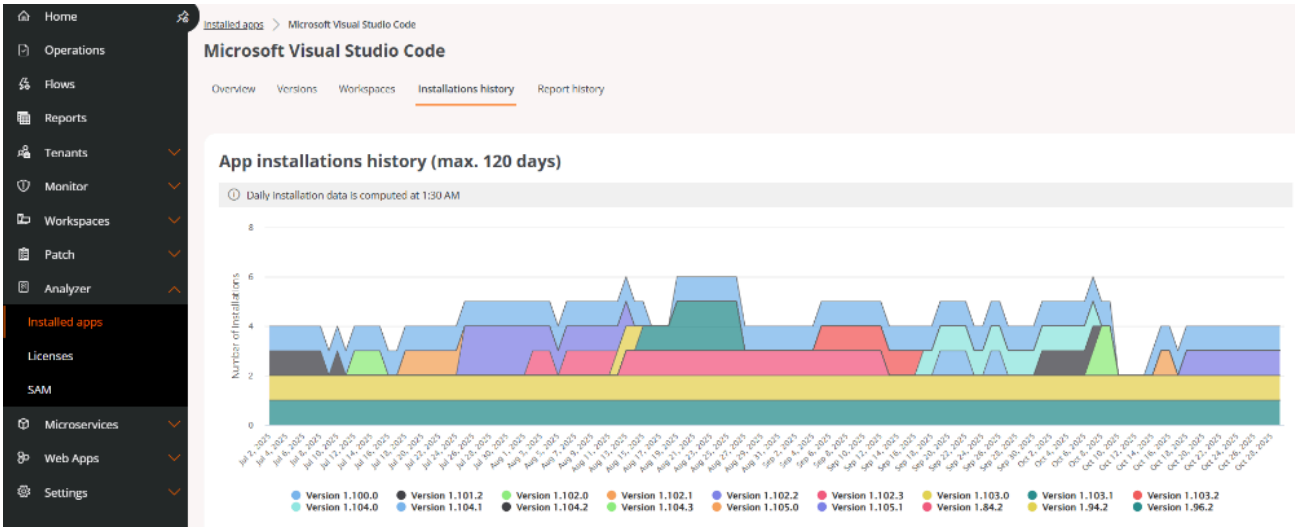
Workspaces

Shows detailed information about the devices where the application is installed:

- **Name.** Device Name.
- **Version.** Version of the installed application.
- **Installation location.** Path of the executable file.
- **Last report (UTC).** Date of the last report of the application on the device.
- **Installed at (UTC).** Date of the first report of the application on the device.
- **Product name.** Name of the installed application.
- **OS.** Operating system of the device.
- **Report Group.** Reporting group to which the device belongs.
- **Last user.** Last user who used the device.

Installation history

Through a graph, it shows the number of installations for each of the application's versions over a maximum period of 120 days.

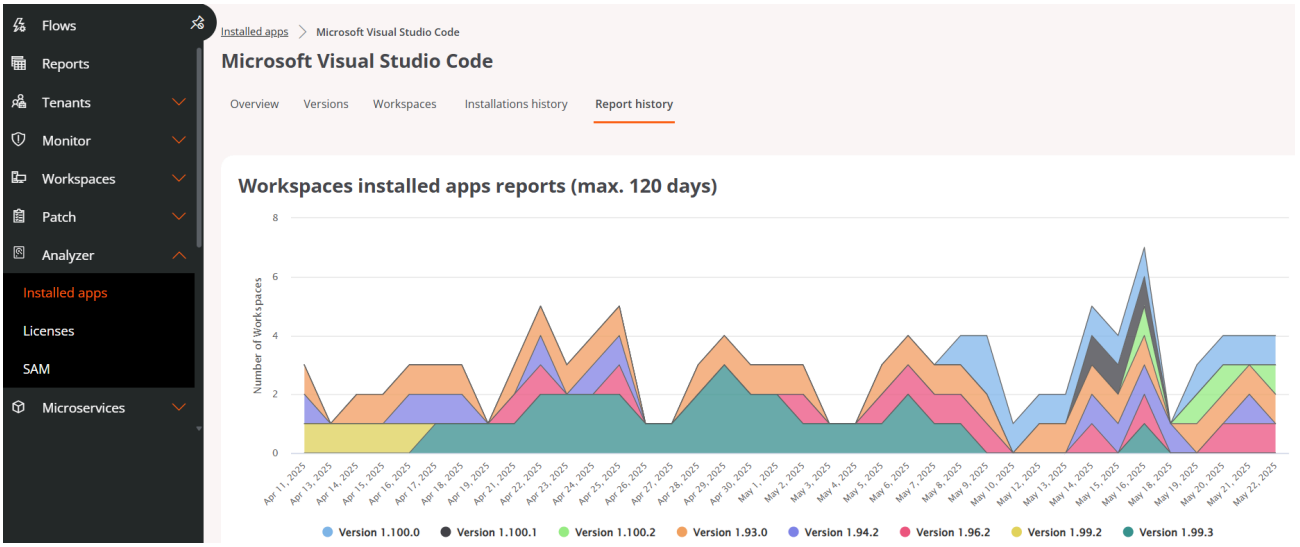


When hovering over a specific date, an info box shows the number of installations corresponding to that moment.

> **INFO**
>
> The installation history is updated daily at 01:30 UTC.

Report history

Displays a graph showing the number of devices that have reported a certain version number of the application over a maximum period of 120 days.



Hovering over a date shows how many devices reported on that version at that time. The version numbers are indicated below the graph as a legend.

Product name and versions

The way the version of an application is displayed depends on the manufacturer and how it manages its names and updates.

- For applications whose name does not vary between versions, the latest installed version will always be shown.
- In applications whose name includes the version number, it is possible that two different versions are shown as independent installations (for example, *App 1.0* and *App 2.0*). This happens because the operating system interprets each name as a different application.

For this reason, when the application is updated on all devices, the previous version (in this example, *App 1.0*) will be included in the list of *Without installations* once it is no longer present on any device.

Considerations when removing a device

When a device is removed from the platform:

- Applications installed on that device are no longer counted in the *Installation count* column of the main table.
- If these applications continue to be installed on other devices, the value of the *Installation count* will decrease.
- The device will no longer appear in the Workspaces list within the application's detail view.
- If the application is no longer installed on any other device, it will be included in the list of *Without installations*.

Data collection and update times

The following table summarizes the collection, update, and retention intervals of the data shown in this section. These times may vary depending on the status of the devices, active sessions, and the reporting cycle of the FlexxAgent Analyzer.

Compute	Frequency	Details
Start of data collection (FlexxAgent Analyzer)	When a user logs in	Data collection begins when FlexxAgent Analyzer starts the process.
General update of **Installed Applications** data	Every **12 hours**	Whenever there is a user session active or during each login.
Calculation of *Installation count*	Every **2 hours**	It is recalculated periodically; it does not represent the real-time number.
Update of installation history	Once a day, at **01:30 UTC**	Updates the number of installations per version shown in the graph.
Report history	Daily update (implicit, along with *Installation history*)	Shows the number of devices that have reported each version.
Retention of installation history and reports	Up to **120 days**	Historical data is retained for 120 days.

Portal / Analyzer / Licenses

Licenses shows information about all the software licenses an organization has acquired. With access to this data, a study can be conducted on the cost generated by the installation or execution of applications on devices, with the aim of minimizing extra costs.

Types

There are three types of licenses:

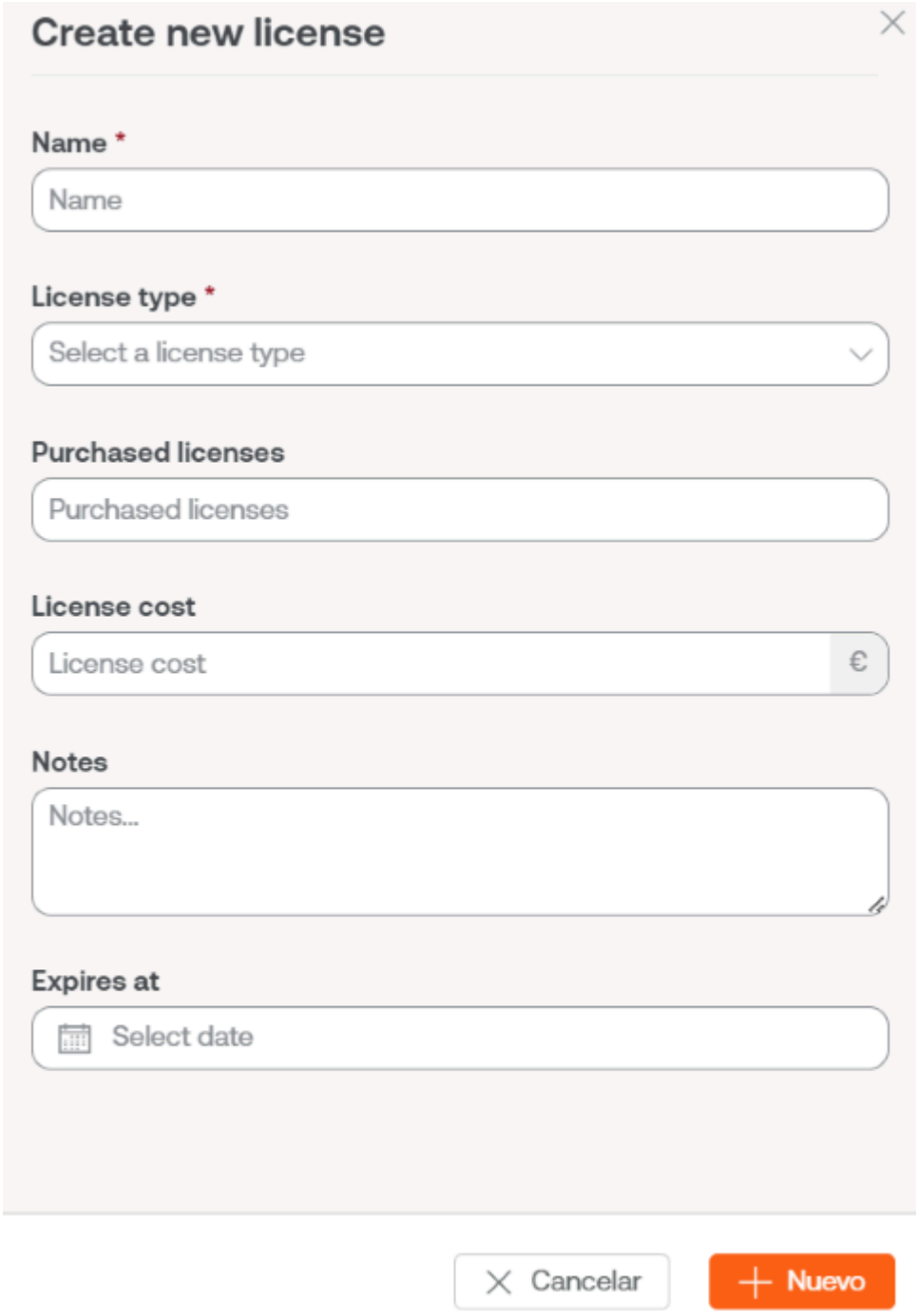
- **Installed on the device.** Usage of these licenses is measured based on the installation of at least one of the applications it includes.
- **Run on the device.** Usage of these licenses is measured based on their execution on the device, not their installation.
- **Run by a user.** Like licenses run on the device, usage of these licenses is measured based on their execution by the user.

The configured license type will determine how its use is measured.

> **INFO**
>
> The license information is calculated on the spot. The use of a license starts being recorded from the moment it is created and the installed applications are associated with it.

Create a License

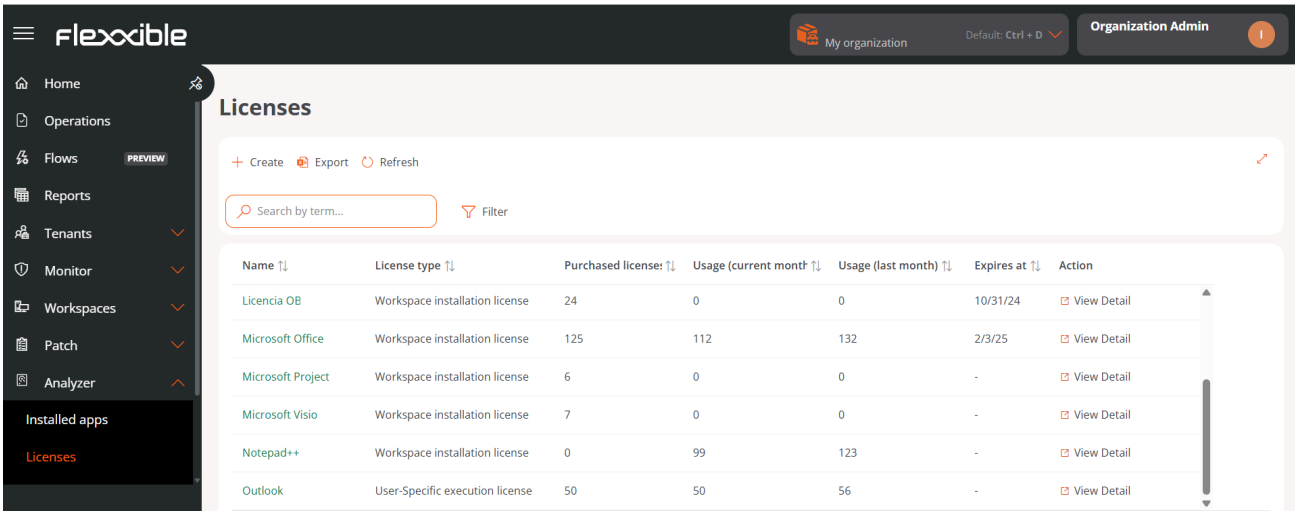
To create a new license, click the `New` button located in the list view. Next, a form will open requesting to fill in the following fields:



- **Name.** Name of the license the device has.
- **License type.** Option to choose the type of license.
- **Licenses purchased.** Number of licenses acquired.
- **License cost.** Monthly cost of the license, in euros.
- **Notes.**: Additional notes about the license.
- **Expires on.** Expiration date of the license.

License list

Displays a table with the following information:



- **Name.** License name.
- **License type.** *Installed on the device*, *Run on the device* or *Run by user*.
- **Licenses acquired.** Number of licenses purchased.
- **Usage (current month).** Number of licenses used in the current month.
- **Usage (last month).** Number of licenses used in the previous month.
- **Expires on.** Deadline for using the license.
- **View details.** Allows access to three main tabs of information about the selected license: `Details`, `Installed applications`, and `Usage history`.

License detail view

Depending on the type of license, the detail view will show certain information tabs. In all cases, you will find the following:

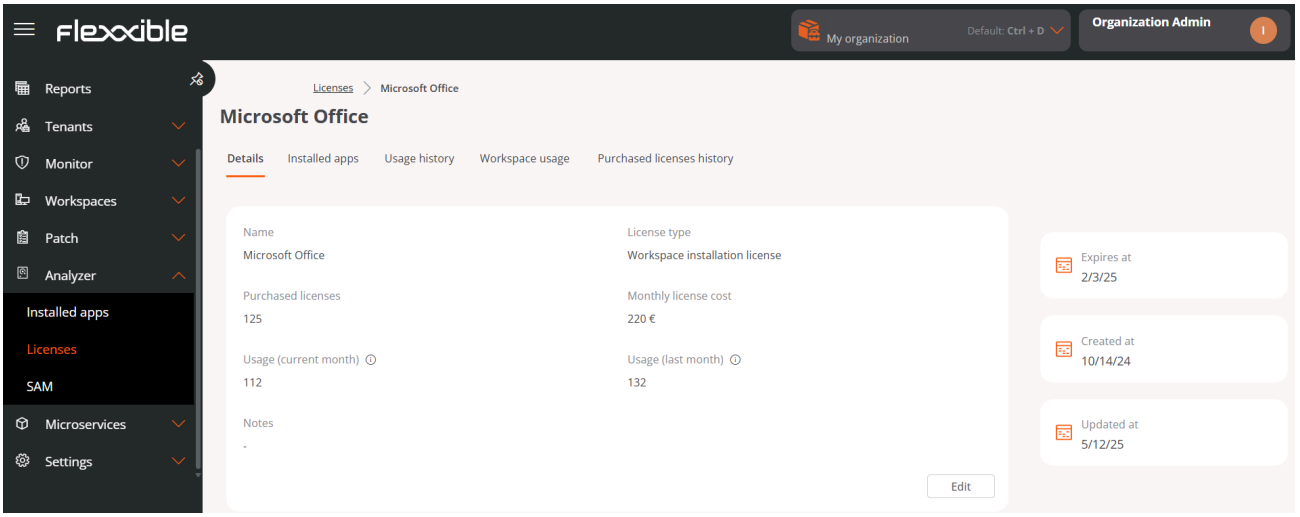
- Details
- Installed applications
- Usage history

In the case of licenses of type *Executed on the device* or *Executed by the user* the following will also be enabled:

- Running processes

Details

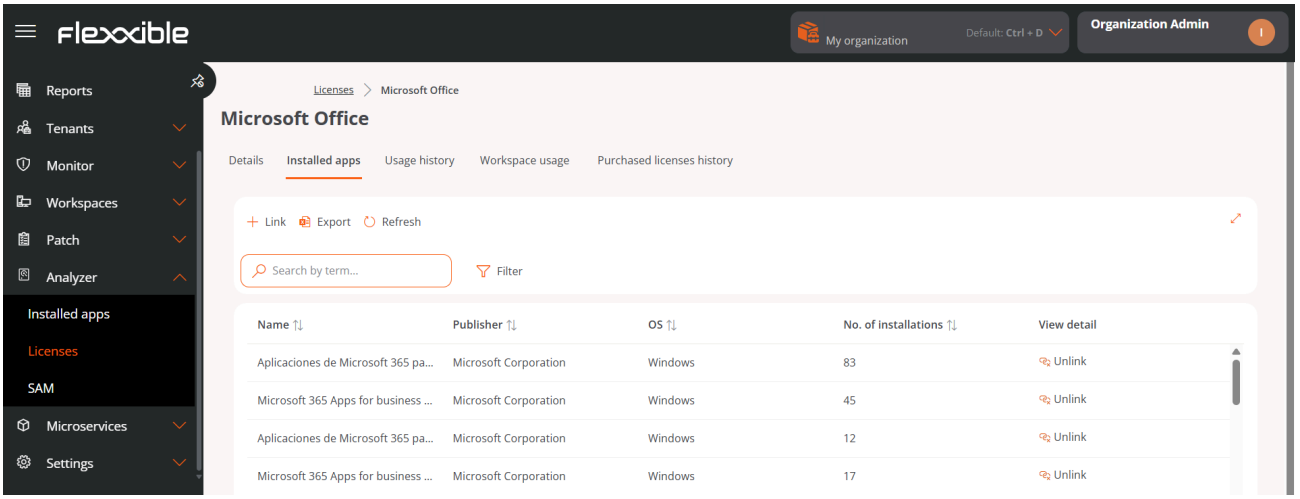
Provides the same information as the license list and adds license cost, as well as issuance, update, and expiration dates.



The `Edit` button opens a form to update information. The user also has the option to add free notes with data they consider relevant.

Installed apps

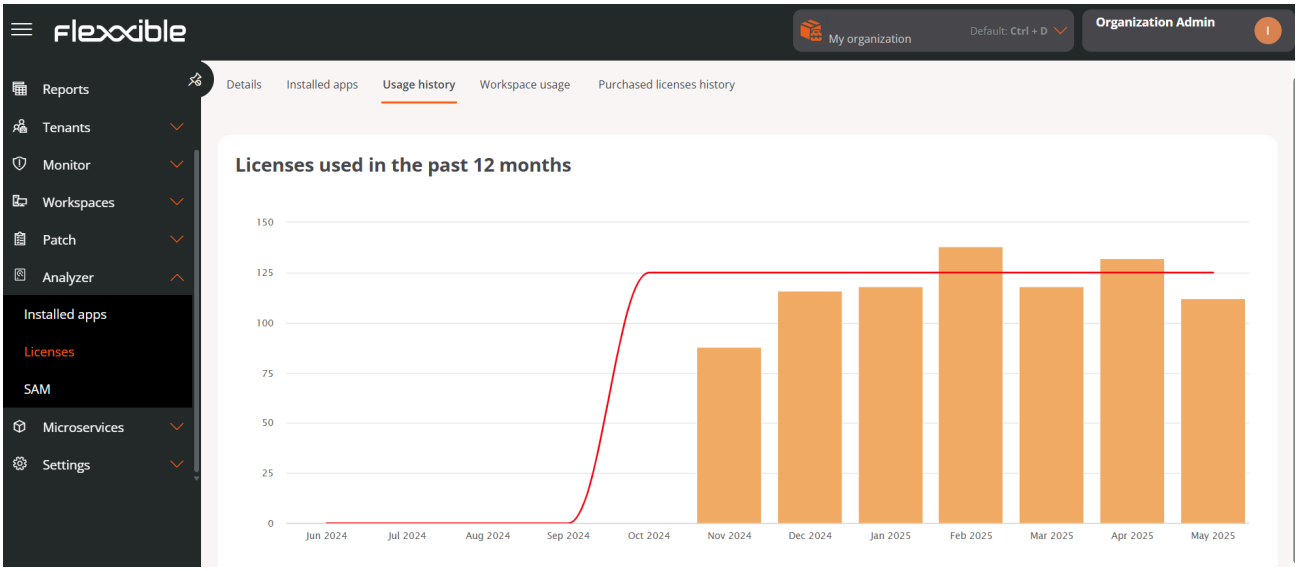
Displays a table with the list of installed applications that are part of the acquired license.



The table fields report:

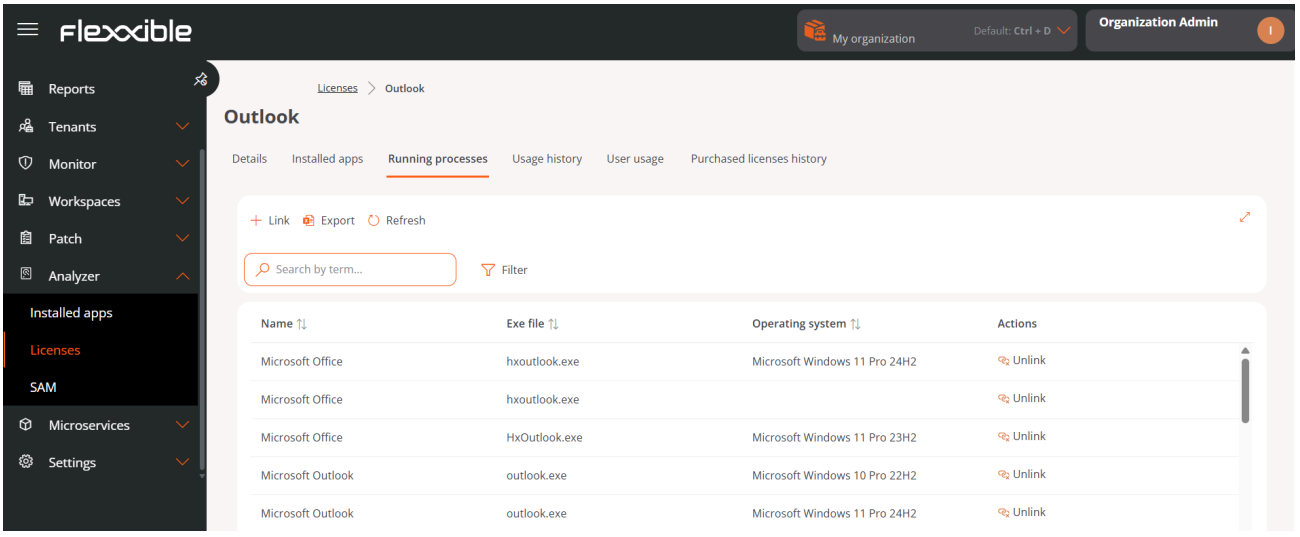
- **Name.** Application name.
- **Publisher.** Company that developed the application.
- **OS.** Operating system on which the application runs.
- **Number of installations.** Number of installations of the application.
- **View detail.** Allows *Unlinking* or *Linking* an application. The latter displays a form with options to link an application to the list of installed applications. The `Reload` button updates the list after changes have been made.

Usage history



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

Running Processes

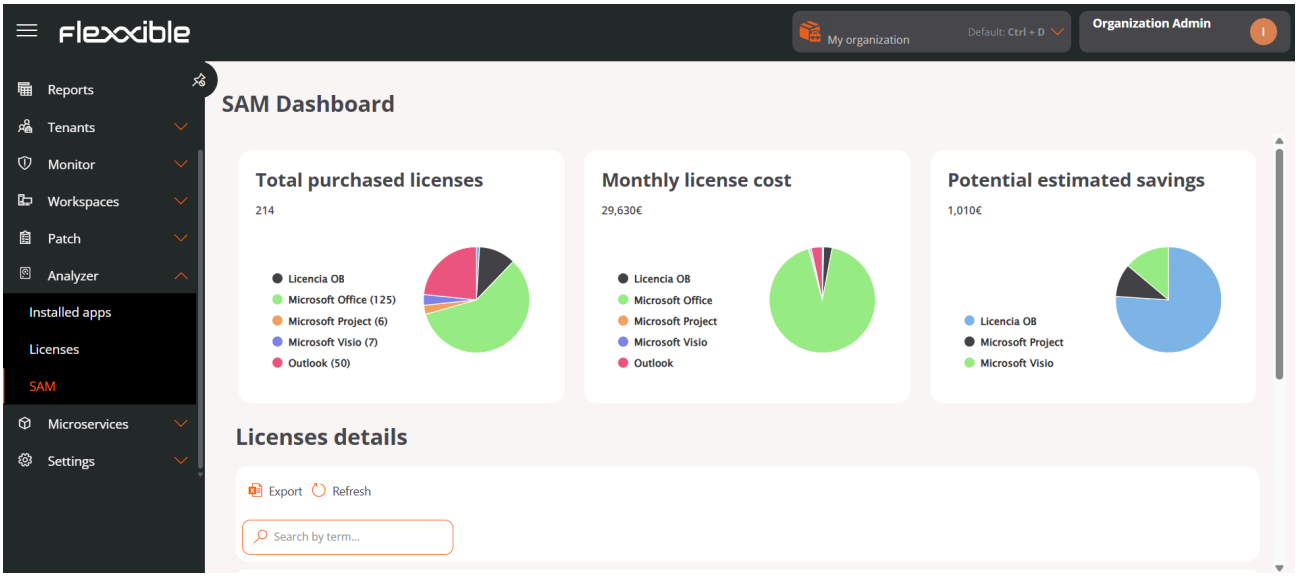


Reports on the running applications linked to this license. Those in which being in execution requires accounting for a license as *In use*. The table shows the following data:

- **Name.** Application name.
- **Exe file.** Name of the binary in the filesystem.
- **OS.** Operating system on which it was discovered.
- **Action** Allows *Linking* or *Unlinking* applications to the license.

Portal / Analyzer / SAM

SAM allows measuring the use of the organization's licenses when they have been created and configured properly.



This view consists of three graphs and a table that provide data on usage, cost, and potential savings that could be applied in the use of the configured licenses.

> **INFO**
>
> The license information is calculated on the spot. The use of a license starts being recorded from the moment it is created and the installed applications are associated with it.

The widgets included in the panel contain the following data:

- **Total licenses purchased.** Number of licenses purchased. The data can be segmented by licenses.
- **Total cost per month.** In euros, total amount consumed per month. The data can be segmented by licenses.
- **Potential savings.** In euros, details of licenses not in use that could be opted out to optimize costs. The data can be segmented by licenses.

At the bottom, the 'License Details' table reports on the following aspects:

- License name
- License type
- Total licenses purchased
- Active licenses
- Inactive licenses
- License utilization rate
- Cost per license
- Projected savings
- Currency

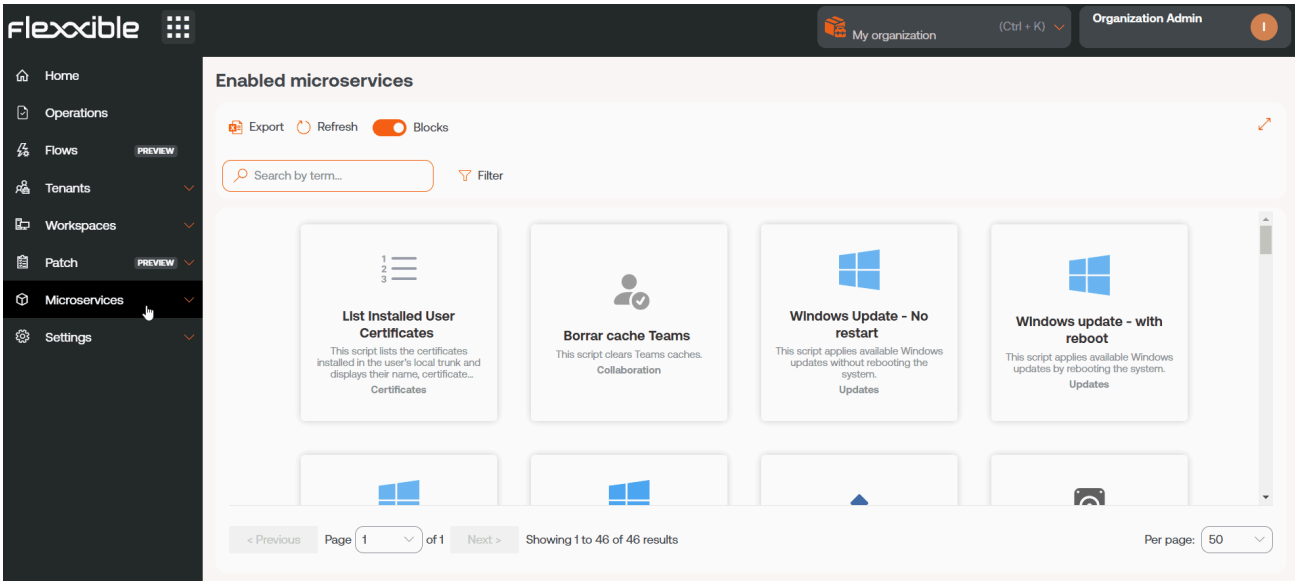
Clicking on the name of any license accesses graphs that indicate:

- 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 by licenses in use and inactive licenses.

Portal / Microservices

Microservices are independent components that execute to prevent or solve frequent issues on devices, improve performance, or speed up tasks that might require a lot of time to do manually. Microservices can be executed autonomously or as part of a broader functionality within a system.

Microservices allows creating, enabling, and publishing microservices so they can be executed at the organizational level, as a prevention or self-remediation mechanism — through flows or alerts—, or directly by the end user.



NOTE

This document describes in general terms what microservices are and how to execute them. The following articles provide more precise information about their behavior and configuration:

- Enabled. Describes how to activate a microservice for execution by an end user or from Workspaces.
- Marketplace. Shows the catalog of available microservices.
- Designer. Explains how to create new microservices and configure existing ones.
- Create with AI. Explain step-by-step how to generate microservices using natural language.

Features

Microservices offer a series of key advantages. The most relevant ones are described below:

Access to a centralized catalog

The available microservices are organized in the Marketplace section, where users can explore the catalog, select, and enable specific microservices according to the needs of their organization or particular use cases.

Creation of customized microservices

Portal allows users to easily create microservices via the Designer section. This tool guides the user, as long as they have the appropriate permissions, through all the necessary phases to build and configure their own microservice.

Execution scope configuration

Each microservice can be defined to run in one of the following contexts, configurable from the Designer section.

Execution from the local administrator

It allows direct interaction with operating system services, processes, and other resources requiring elevated privileges. It's ideal for operations that must be executed with administrator permissions, but it may restrict access to specific user information or their session.

Execution from user session

Useful for accessing user information such as their log or information contained in their profile. The script will run with the permission level the user has, so if they do not have local administrator privileges, they will not be able to perform actions requiring system access.

Ways to consume microservices

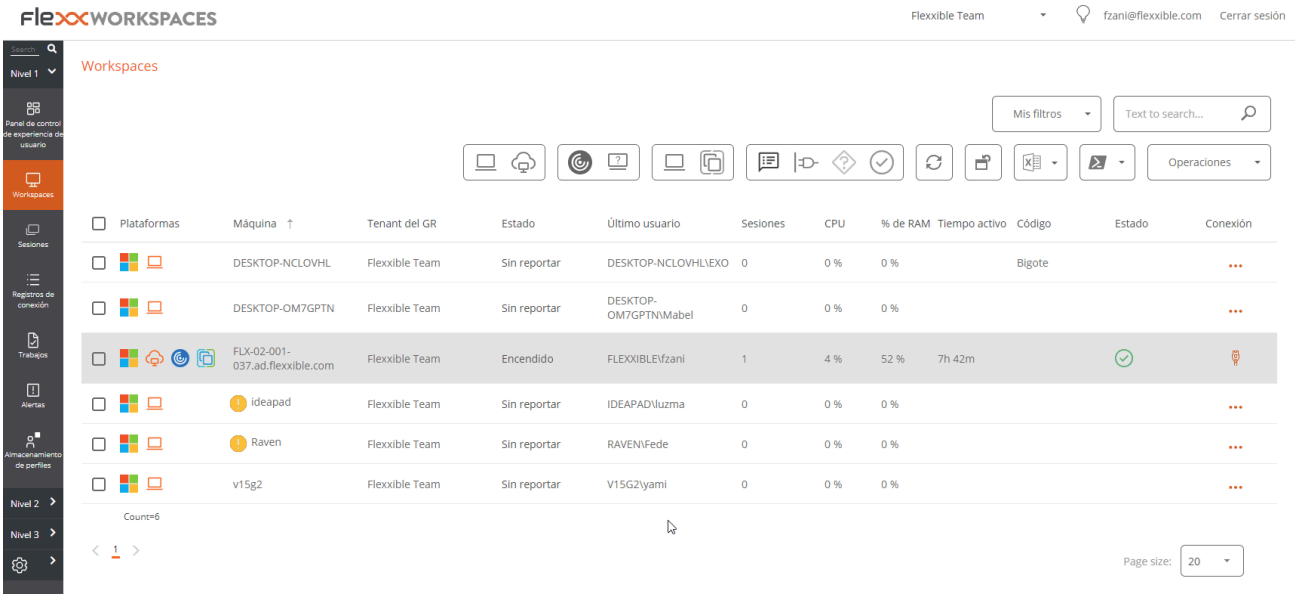
Microservices can be created and enabled in Portal, and from there configured to be executed by the end user, launched via a flow or executed with automated or support actions from Workspaces.

On-demand execution from Workspaces

Any microservice that has previously been enabled in Portal can be executed from Workspaces.

1. Access the `Workspaces` module -> `Workspaces` or `Sessions` section.
2. Select the devices or sessions where you want to apply the microservice.
3. In the top menu, click on the Microservices icon (`>_`).
4. Select the microservice you want to execute.

Microservices will be visible in the `Workspaces` section when they have been configured to execute in the *System* context, and in the `Sessions` section when the configuration has selected the *Session* context.

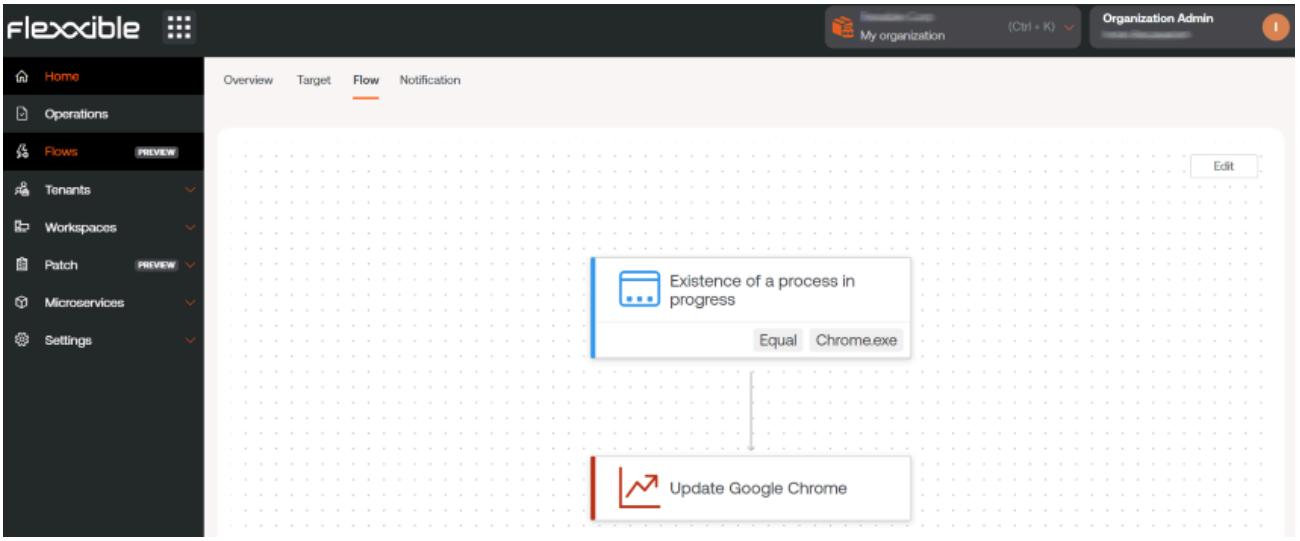


You can manage the execution scope of the microservice and the permissions from the Designer section. It should be noted that the ability to execute certain microservices will depend on the user's role in the platform.

Scheduled execution through Flows

Flows is a feature that allows you to define automation sequences to execute scheduled actions on devices based on the evaluation of predefined logical conditions.

Its main characteristic is that it simplifies diagnostic actions and quickly resolves problems through the execution of a microservice.



For more information on executing a microservice through a flow, please consult this guide.

Scheduled execution through Alert Settings

Through Alert Settings, it is possible to link events (event logs) to one or more microservices to prevent device issues or resolve problems promptly.

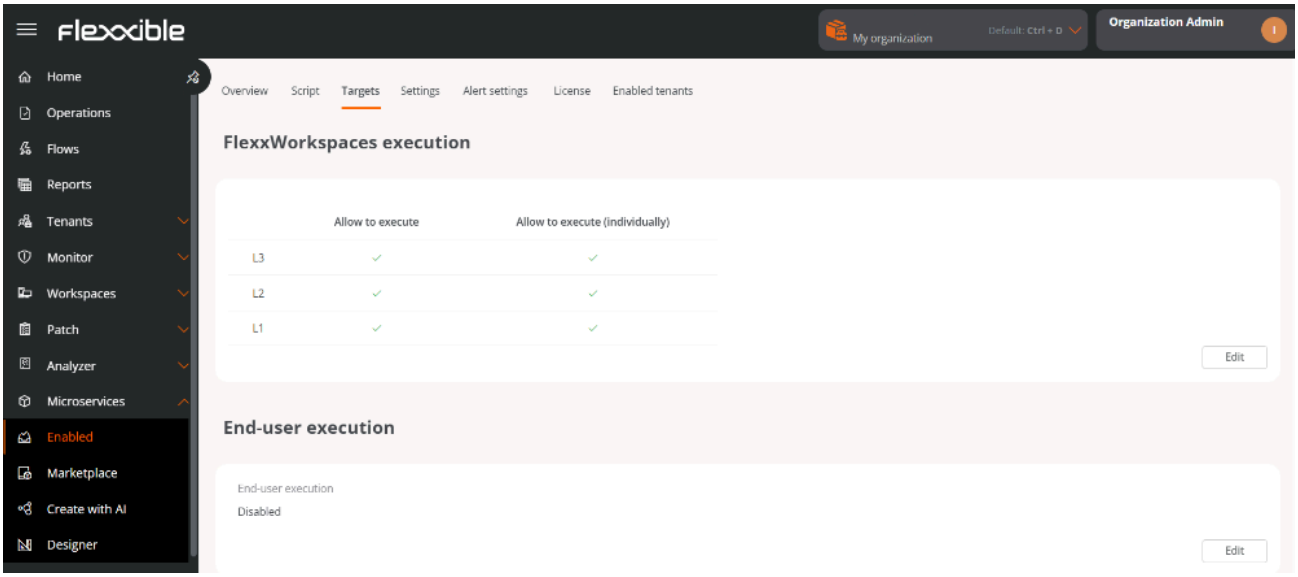
1. Go to `Portal` -> `Monitor` -> `Alert Settings`.
2. In the table, select an alert name to access its detailed information.
3. In the left side menu, click on the `Microservices` tab.
4. Click on `Link`.
5. In the form, choose the microservice to link to the alert and the execution order (useful when linking more than one microservice).
6. In the form, click on `Link`.

For more information on linking an alert to a microservice, please refer to the Alert Settings documentation.

End-user execution

When a microservice is created, it is not automatically enabled for execution by the end user. To enable it, you need to complete the following configuration:

1. Access `Portal` -> `Microservices` -> `Enabled`.
2. Select a microservice from the list.
3. In the `Targets` tab, go to the `End user execution` section.
4. Click on `Edit` and enable `Execution by the end user`.



Next, optionally, you can configure notification reception.

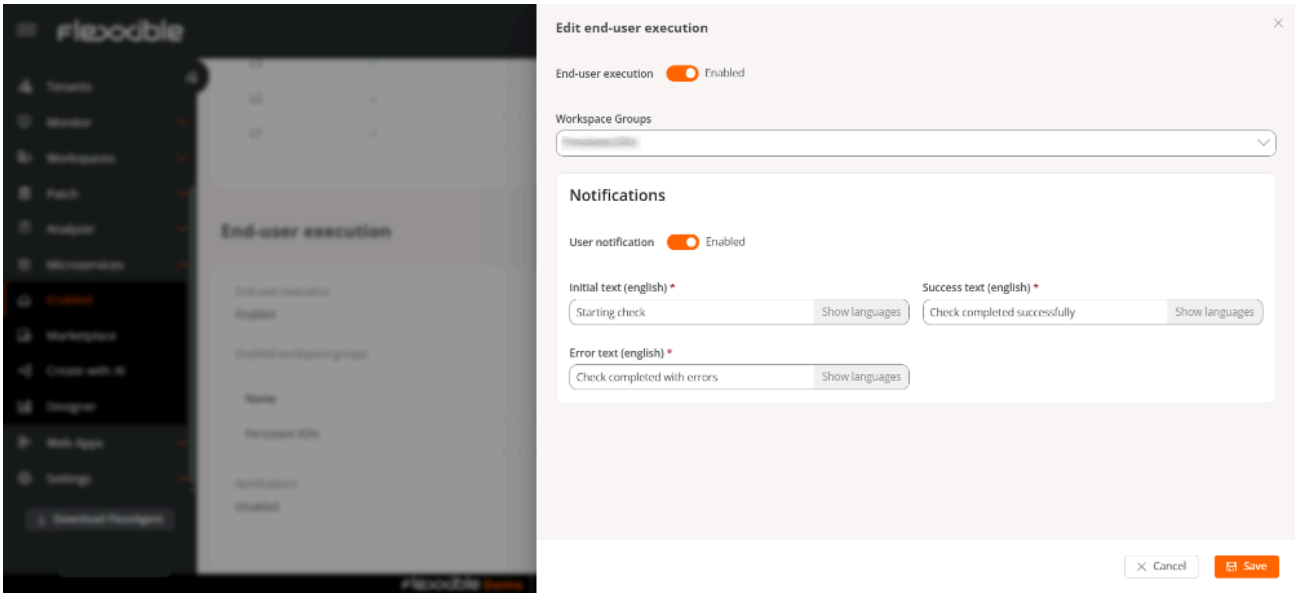
Notifications

This option lets you decide whether to notify the user when the microservice starts executing and when it finishes, whether successfully or with errors.

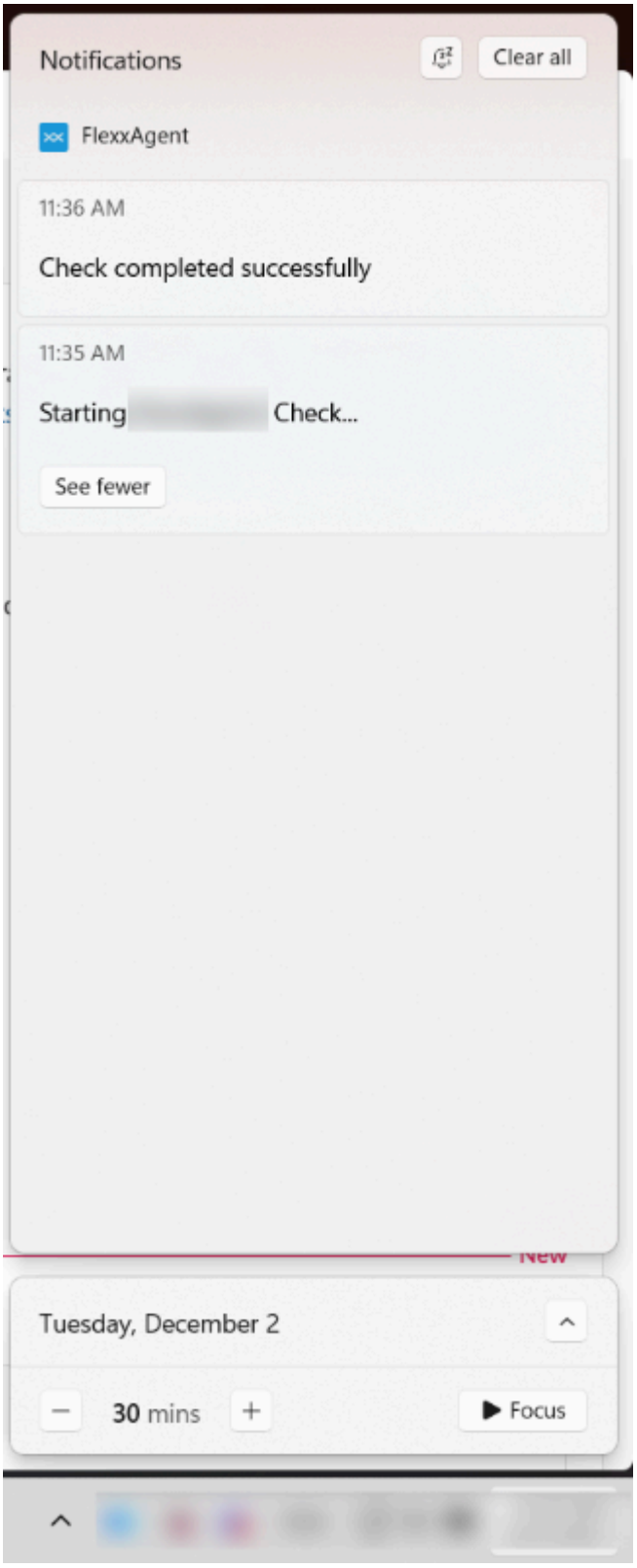
To do this, `User Notification` must be activated and the following fields completed:

- **Initial text.** Message displayed at the start of the microservice execution.
- **Success text.** Message displayed when execution completes successfully.

- **Error text.** Message displayed when execution ends with errors.



Notifications will appear in the Windows notification bar.

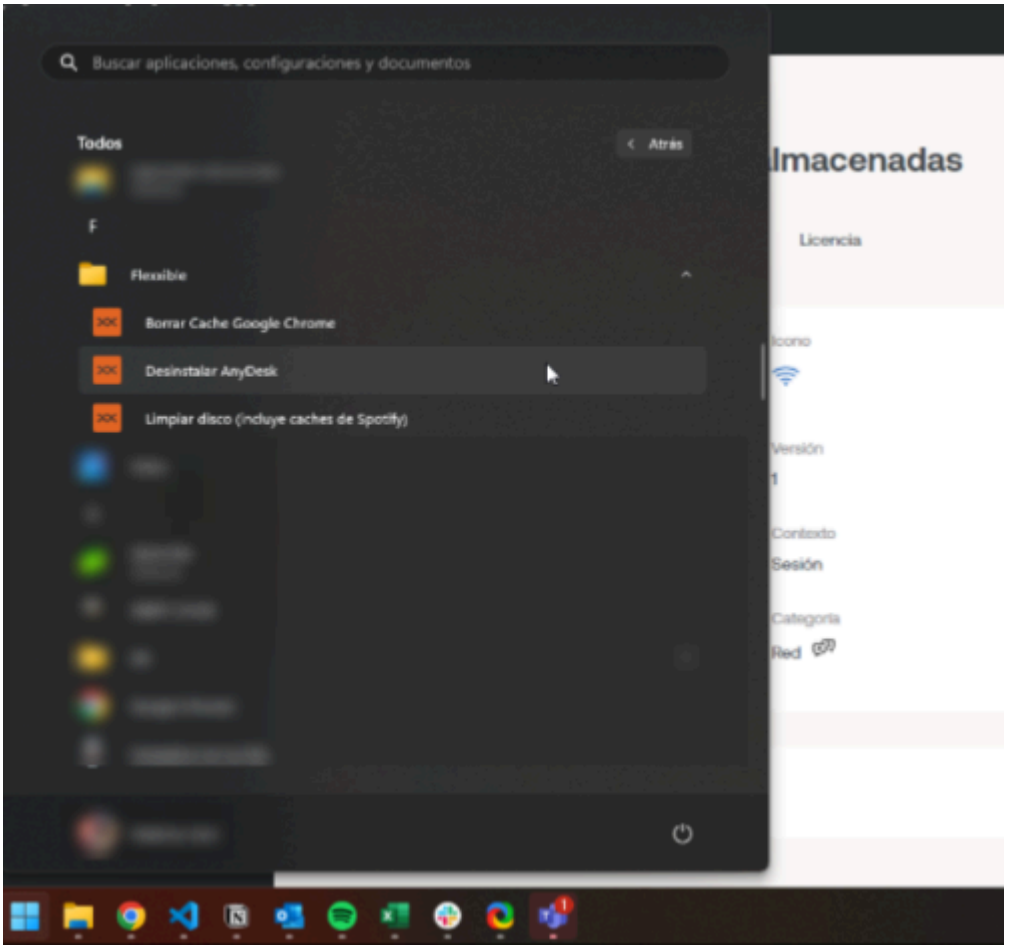


Rename the microservices folder

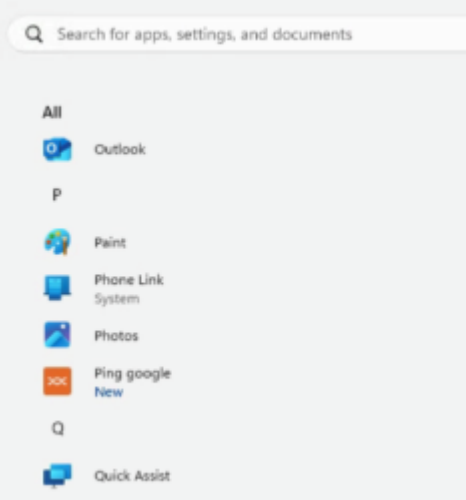
When microservices are enabled for execution by the end user, they are automatically added to a device folder called *Flexxible*; however, this name can be changed.

1. Go to `Portal` -> `Settings` -> `Organization`.
2. In the left sidebar, click on the `Microservices` tab -> `Edit microservices settings`.
3. Rename the folder.
4. Click on `Save`.

The chosen name must be between 3 and 50 characters, and can only contain letters, numbers, hyphens, and underscores.



If the device has Windows 11 as the operating system and only one microservice is enabled for an end user, the folder will not be displayed; instead, only the microservice icon will be visible in the Start menu.

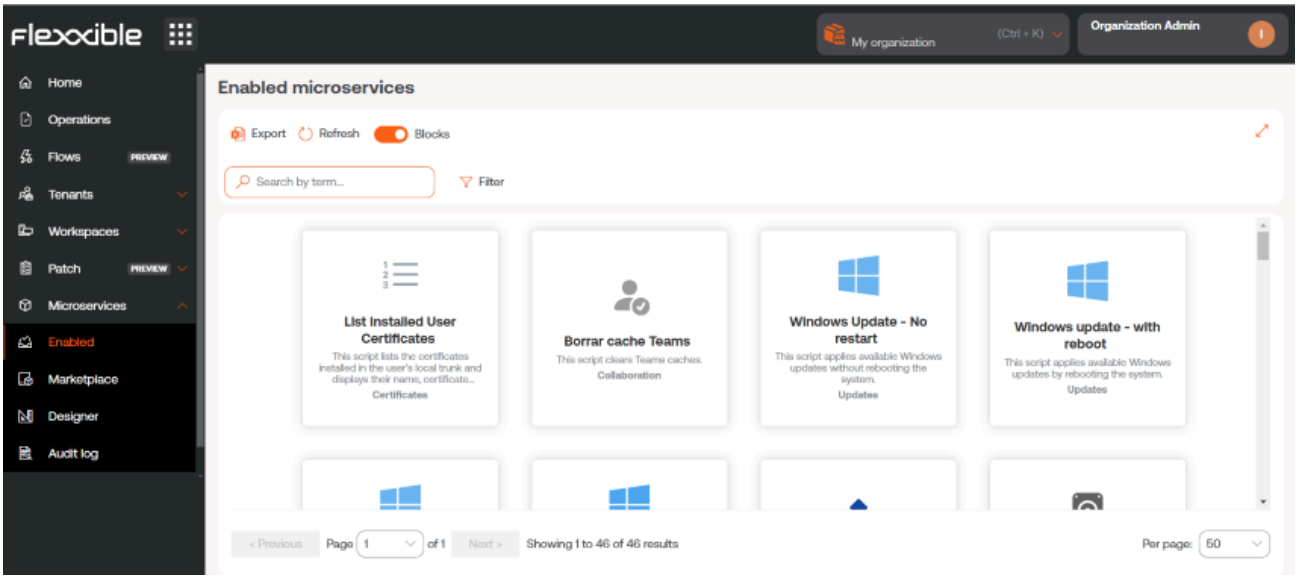


TIP

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

Portal / Microservices / Enabled

Enabled shows a list and block representation of the microservices available for the selected organization. These microservices can be configured to run from Workspaces, either at the system or session level, or to be run by the end user.



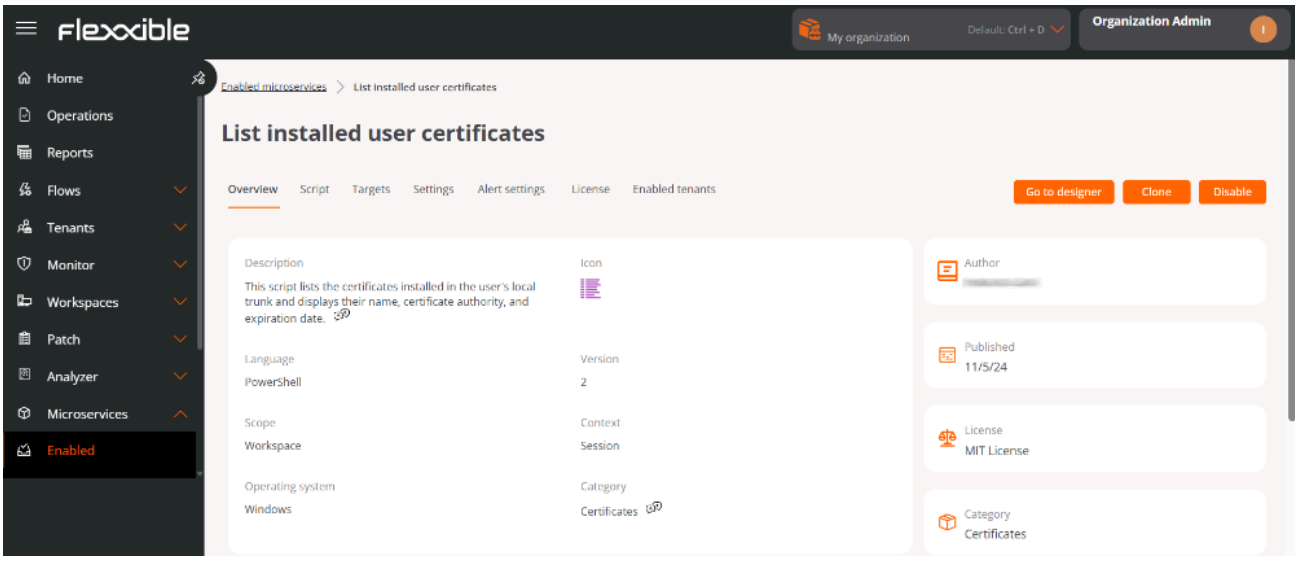
Microservice detail

Clicking on a microservice in the table accesses its detail view, divided into seven tabs:

- Overview
- Code
- Targets
- Settings
- Alert Configuration
- License
- Enabled Tenants

Overview

It displays general information about the microservice, including its description, development language, compatible operating system, execution context, author, and creation date, among other relevant data.



From this tab, three main actions are available:

1. **Go to designer**

   Allows editing the microservice configuration through the following tabs:

   - **Overview.** General data of the microservice.
   - **Code.** Source code of the microservice.
   - **Privacy.** Information about the visibility of the microservice.
   - **Targets.** Conditions for the execution of the microservice.

     - **FlexxWorkspaces Execution** Shows the roles with permissions to execute the microservice in Workspaces. The column *Allow execution* indicates the roles authorized to execute it at the Workspace group level, while *Allow execution (individual)* shows roles with permission for execution on individual devices. Both can be modified using the `Edit` button.

     - **End-user Execution**
       Specifies if the microservice is enabled to be executed directly by the end user. This permission can also be modified using the `Edit` button.

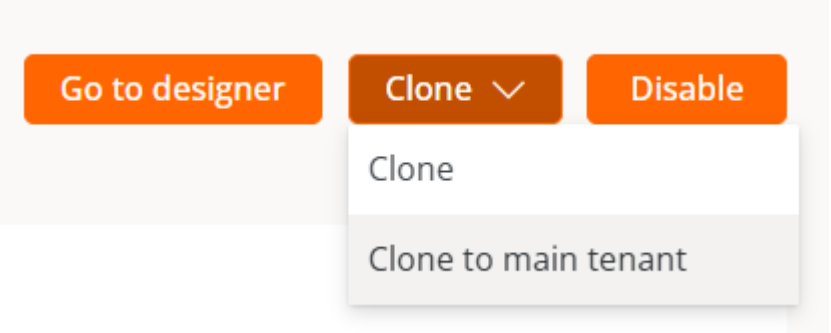
For more information, please refer to the guide Enable microservices for the end user.

- **License.** Allows configuring the microservice's license type.

2. **Clone**

   Open the microservice creation form with fields pre-loaded with the information from the microservice to be cloned, to create a new one from that configuration.

   Suborganizations can clone a microservice from their environment to the main organization, which can then publish it and make it available to the rest of the suborganizations.



3. **Enable/Disable**

   Shows the current status of the microservice. When enabled, the microservice becomes visible and can be executed from the Workspaces module: in the `Workspaces` section (context *System*) and in the `Sessions` section (context *Session*), according to the configuration defined in the Designer section.

Code

Displays the source code of the microservice, including the logic and instructions that define its behavior.

Targets

Defines the conditions for the execution of the microservice.

Execution of FlexxWorkspaces

Shows the roles with permissions to execute the microservice in Workspaces. The column *Allow execution* indicates the roles authorized to execute it at the Workspace group level, while *Allow execution (individual)* shows roles with permission for execution on individual devices. Both can be modified using the `Edit` button.

End-user execution

Specifies whether the microservice is enabled to be executed directly by the end user. This permission can also be modified using the `Edit` button.

> **INFO**
>
> The name of a microservice configured for execution by the end user **must not contain special characters** like **\ / : * ? " < >** or specific language characters that may vary depending on the keyboard layout.

> **INFO**
>
> A configuration change in an existing end-user microservice may take up to 15 minutes to apply to all linked devices.

Settings

Reports the estimated time (in minutes) that the use of the microservice has saved the user compared to a manual solution for the same situation.

Alert Configuration

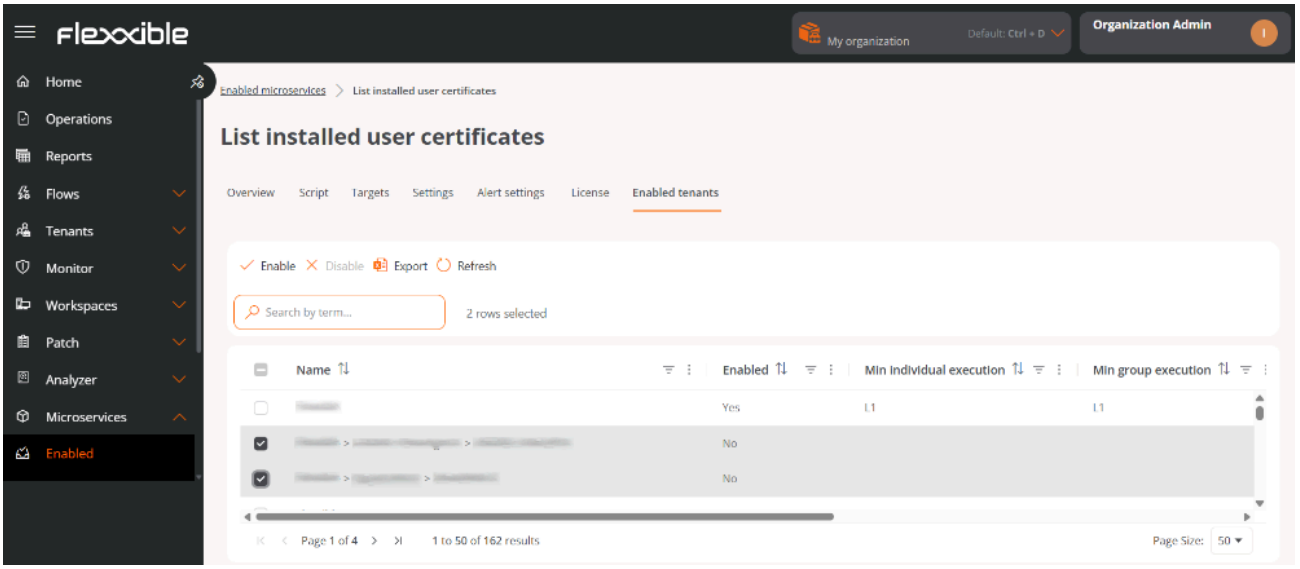
Presents a table with alerts linked to the microservice. For more information, please consult the documentation on Alert Settings.

License

Shows the type of license configured for the microservice.

Enabled Tenants

Allows enabling/disabling the microservice in bulk for the selected tenants and suborganizations.



The table contains the following information:

- **Name.** Tenant name. If it has sub-organizations they are presented in tenant*>*sub-organization format.
- **Enabled.** Displays if the microservice is enabled for the tenant.
- **Minimum individual execution.** Minimum roles with execution permissions in Workspaces at the level of individual devices.
- **Minimum group execution.** Minimum roles with execution permissions in Workspaces at the level of Workspaces Groups.
- **Enabled on.** Date and time when the microservice was enabled for the tenant.
- **Enabled by.** Name and email address of the user who enabled the microservice for the tenant.
- **Disabled on.** Date and time when the microservice was disabled for the tenant.
- **Disabled by.** Name and email address of the user who disabled the microservice for the tenant.

Considerations

- The list of available tenants depends on the privacy configuration of the microservice and the permissions the user has.

- Although the microservice can be enabled/disabled, the configuration of Targets is done independently for each tenant.

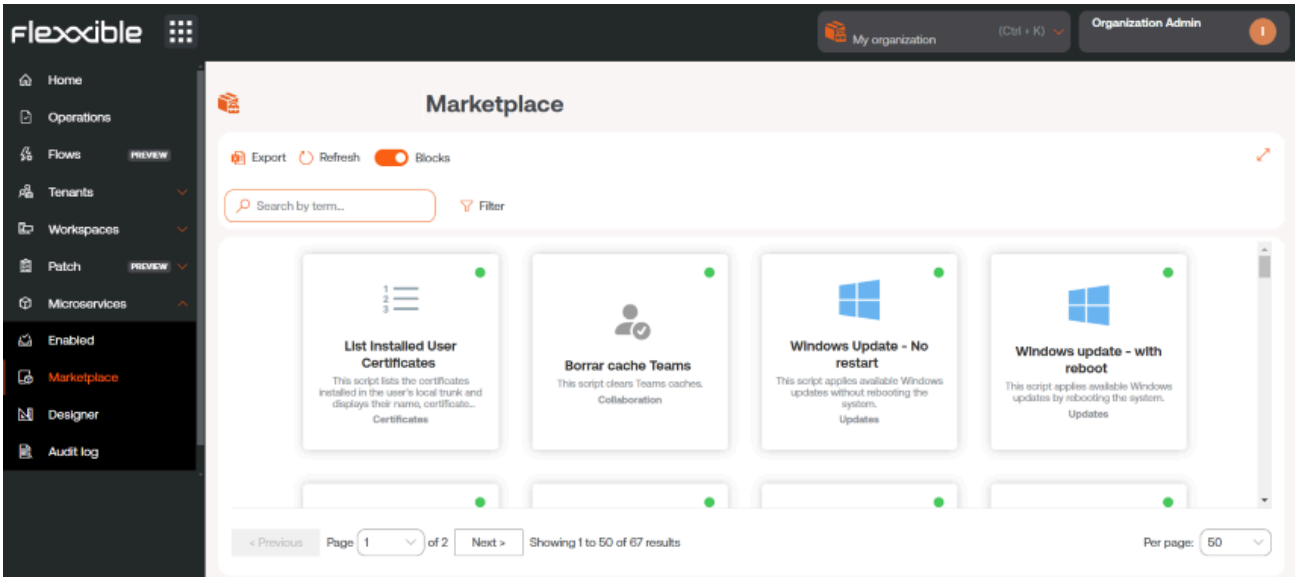
Steps to enable/disable a microservice for tenants

1. Access `Portal` -> `Microservices` -> `Enabled`.
2. Select a microservice.
3. Go to the `Enabled Tenants` tab.
4. Select the desired tenants in the table.
5. Click `Enable` or `Disable`, as applicable.
6. Read the warning message.
7. Click on `Confirm`.

Portal / Microservices / Microservices Marketplace

Marketplace provides a wide list of microservices that can be used without deep computer knowledge, as they are ready to be enabled and executed right away.

The overview of **Marketplace** offers microservices in block or table format. In both cases, if the microservice shows a green dot it means that it is enabled and can be run directly from the Workspaces module, if the dot is gray, it means that it is not.



Microservice detail

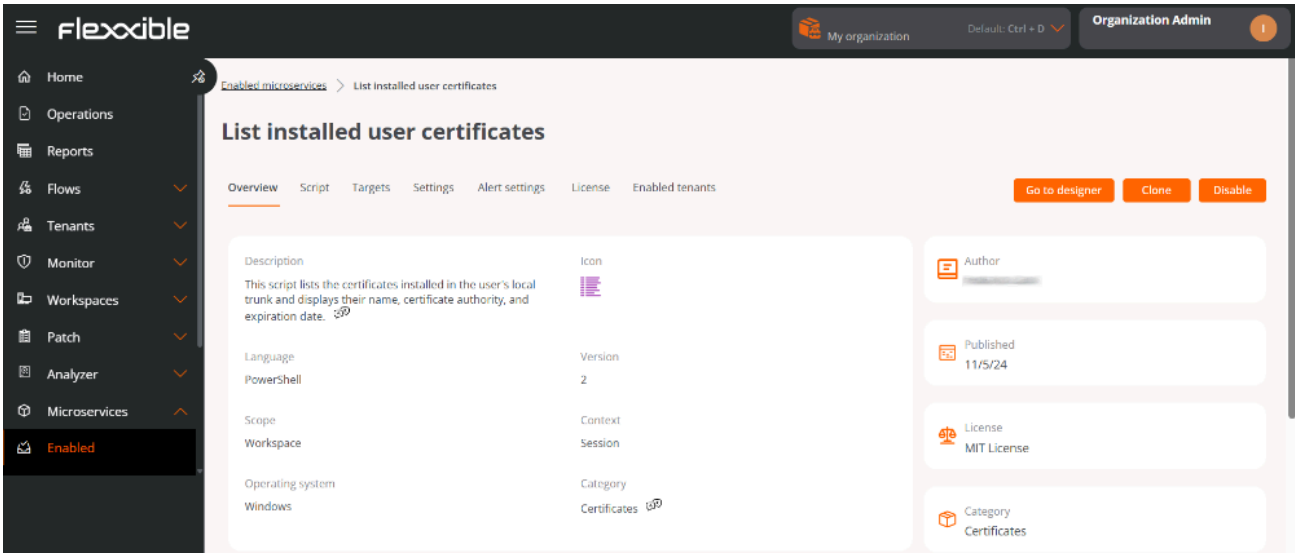
Clicking on a microservice in the table allows access to its detailed view, divided into seven tabs:

- Overview
- Code
- Targets
- Settings
- Alert configuration
- License

- Enabled tenants

Overview

It displays general information about the microservice, including its description, development language, compatible operating system, execution context, author, and creation date, among other relevant data.



From this tab, three main actions are available:

1. **Go to designer**

   Opens the Designer section. Allows editing the microservice configuration through the following tabs:

   - **Overview.** General data of the microservice.
   - **Code.** Source code of the microservice.
   - **Privacy.** Information about the visibility of the microservice.
   - **Targets.** Conditions for the execution of the microservice.

     - Execution of FlexxWorkspaces
       Shows roles with permissions to execute the microservice in the Workspaces module. The column *Allow execution* indicates the roles authorized to execute it at the Workspace group level, while *Allow execution (individual)*

shows roles with permission for execution on individual devices. Both can be modified using the `Edit` button.

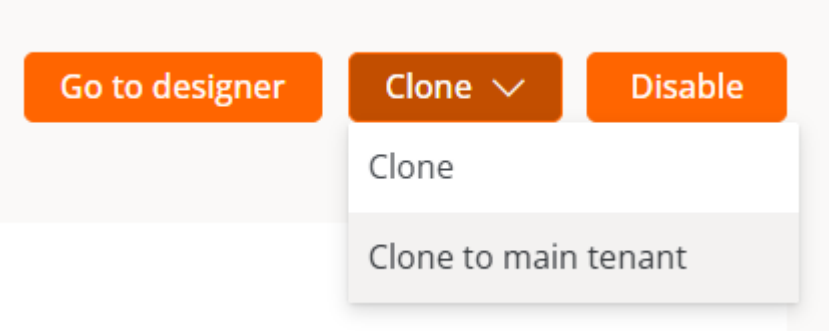
- Execution by the end user
  Specifies whether the microservice is enabled to be executed directly by the end user. This permission can also be modified using the `Edit` button.

- **License.** Allows configuring the microservice's license type.

2. **Clone**

   Open the microservices creation form with fields preloaded with the cloned microservice's information, allowing you to create a new one from that configuration.

   Suborganizations can clone a microservice from their environment to the main organization, which can then publish it and make it available to the rest of the suborganizations.



3. **Enable/Disable**

   Shows the current status of the microservice. When enabled, the microservice becomes visible and can be executed from the Workspaces module: in the `Workspaces` section (context *System*) and in the `Sessions` section (context *Session*), according to the configuration defined in the Designer section.

Code

Displays the source code of the microservice, including the logic and instructions that define its behavior.

Targets

Defines the conditions for the execution of the microservice.

- Execution of FlexxWorkspaces

  Shows roles with permissions to execute the microservice in the Workspaces module. The column *Allow execution* indicates the roles authorized to execute it at the Workspace group level, while *Allow execution (individual)* shows roles with permission for execution on individual devices. Both can be modified using the `Edit` button.

- End-user execution

  Specifies whether the microservice is enabled to be executed directly by the end user. This permission can also be modified using the `Edit` button.

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

Settings

Reports the estimated time (in minutes) that the use of the microservice has saved the user compared to a manual solution for the same situation.

Alert Configuration

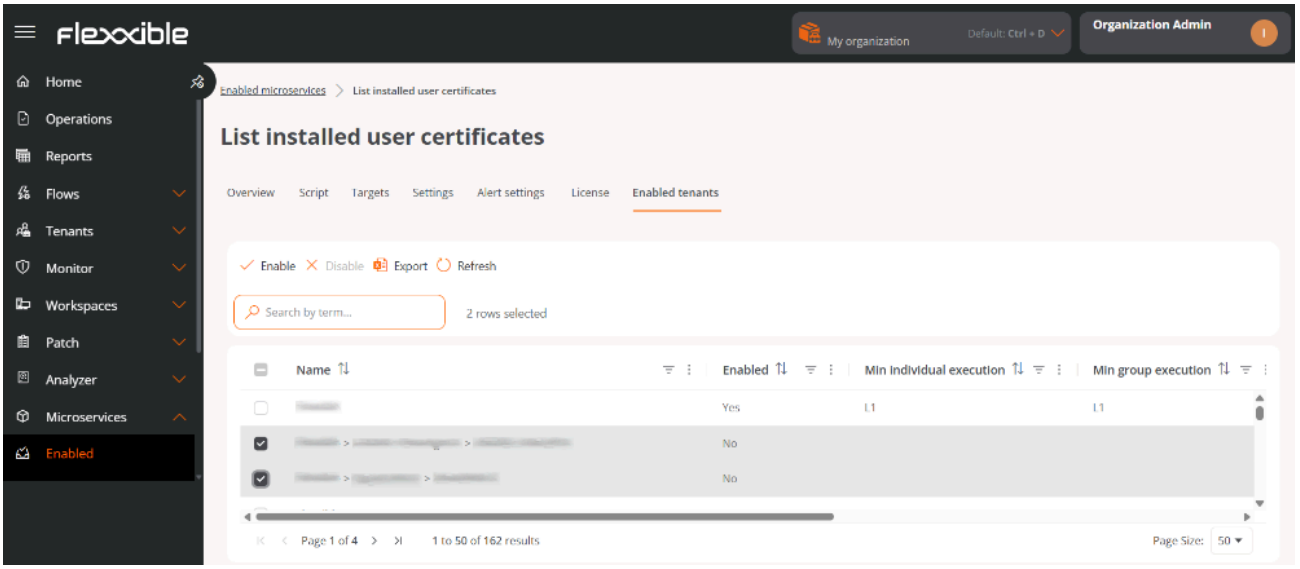
Presents a table with alerts linked to the microservice. For more information, please consult the documentation on Alert Settings.

License

Displays the currently configured license type for the microservice.

Enabled Tenants

Presents a list of tenants and sub-organizations to which the microservice can be enabled/disabled en masse.



The table contains the following information:

- **Name.** Tenant name. If it has sub-organizations they are presented in tenant*>*sub-organization format.
- **Enabled.** Displays if the microservice is enabled for the tenant.
- **Minimum individual execution.** Minimum roles with execution permissions in Workspaces at the level of individual devices.
- **Minimum group execution.** Minimum roles with execution permissions in Workspaces at the level of Workspaces Groups.
- **Enabled on.** Date and time when the microservice was enabled for the tenant.
- **Enabled by.** Name and email address of the user who enabled the microservice for the tenant.
- **Disabled on.** Date and time when the microservice was disabled for the tenant.
- **Disabled by.** Name and email address of the user who disabled the microservice for the tenant.

The list of available tenants depends on the privacy configuration of the microservice and the permissions the user has.

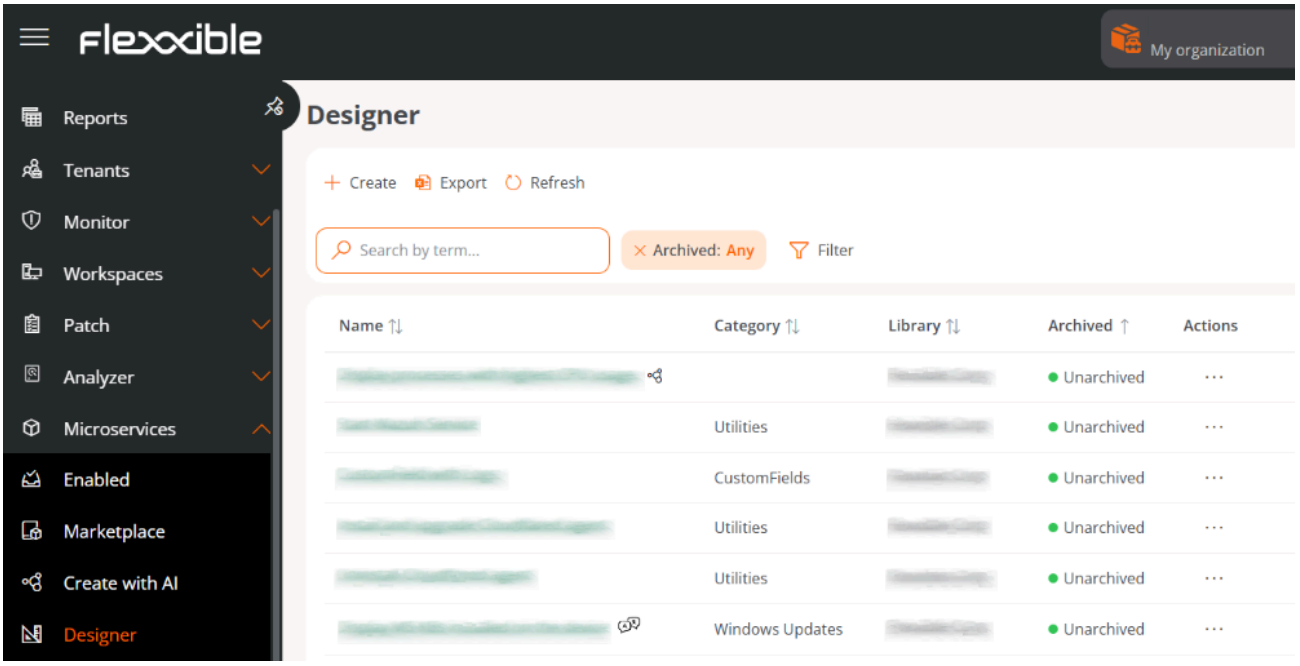
Although the microservice can be enabled/disabled, the configuration of Targets is done independently for each tenant.

Enable/Disable a microservice for tenants

1. Go to `Portal` -> `Enabled`.
2. Go to the `Enabled Tenants` tab.
3. Select the desired tenants in the table.
4. Click `Enable` or `Disable`, as applicable.
5. Read the warning message.
6. Click on `Confirm`.

Portal / Microservices / Designer

Designer is the main environment for creating, configuring, and managing the lifecycle of microservices within an organization. From this interface, users can define new microservices, edit existing ones, temporarily archive them, or permanently delete them according to operational needs.

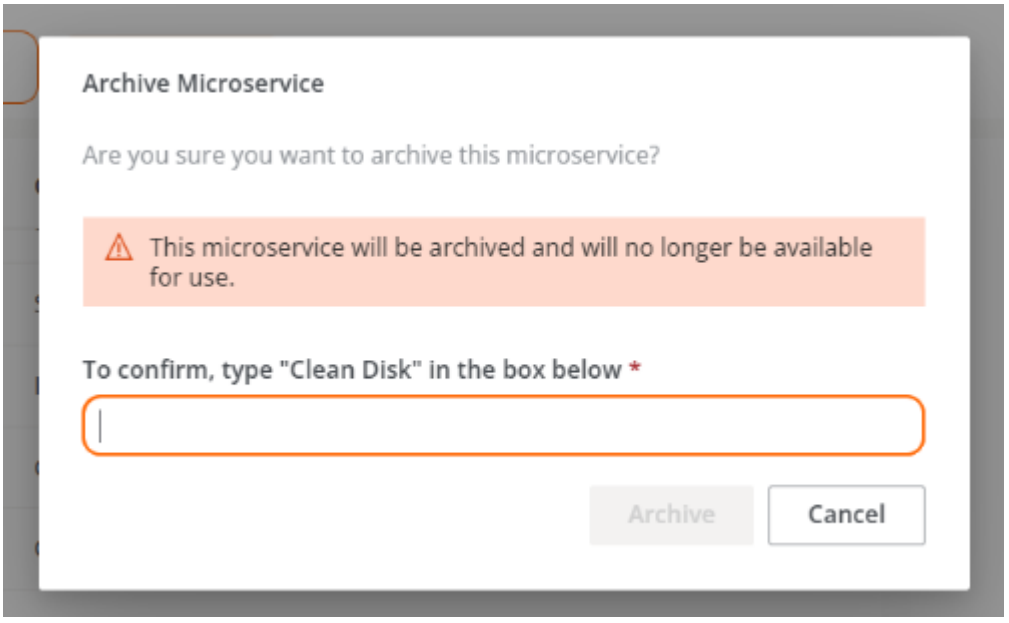


The list view shows a table with the created microservices, along with the following information:

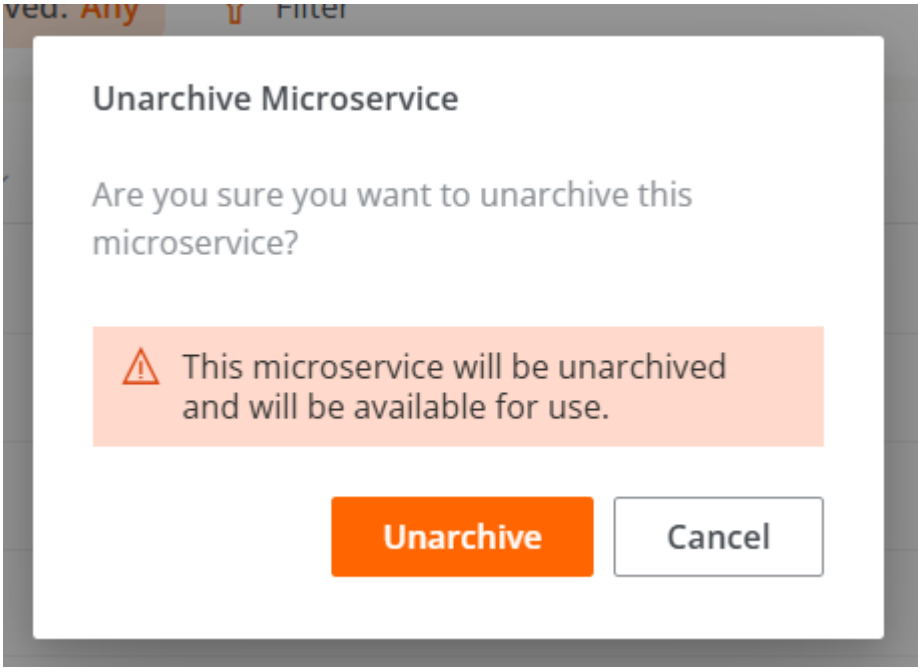
- **Name.** Enter the name of the microservice.
- **Category.** Directory or group of microservices accessible from Workspaces. Categories must be predefined in Organization.
- **Library.** Organization to which the microservice belongs.
- **Archived.** Indicates whether the microservice is *Archived* or *Active*. Archived ones are not available for use, while active ones are.
- **Actions.** Displays three options:
    - **View Details.** Shows expanded information about the microservice.

- **Edit.** Allows you to modify the microservice's configuration.
- **Archive / Activate.** Opens a confirmation window to archive or activate the microservice, depending on its current state.

Confirmation window to archive a microservice:



Confirmation window to activate a microservice:

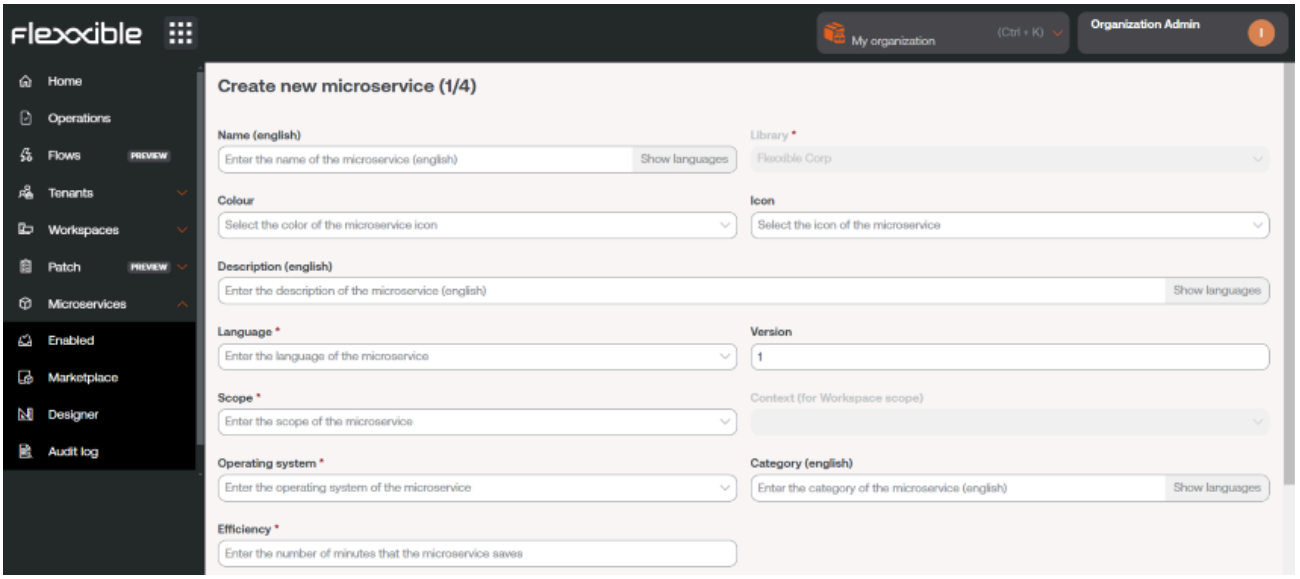


Create new microservice

The process of creating a microservice is done through a wizard divided into four phases, guiding the user step-by-step until configuration is complete.

Phase 1 - Initial Configuration

1. Access `Portal` -> `Microservices` -> `Designer`.
2. Click on `New`.
3. The wizard will open, asking to enter the following information:



- **Name.** Enter the name of the microservice.
- **Color.** Color of the representative icon.
- **Icon.** Type of associated icon.
- **Description.** Brief explanation of its functionality.
- **Language.** Programming language used.
- **Version.** Version number.
- **Scope.** Execution scope. You can select *Workspace* (context *System* or *Session*) or *Platform*.

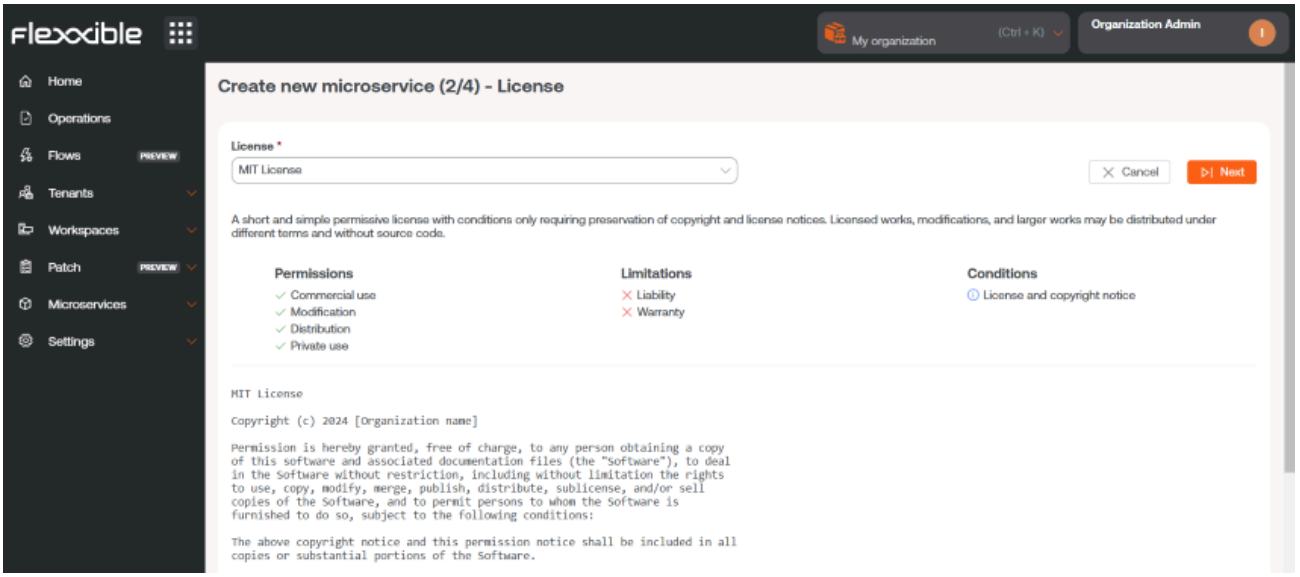
- **Operating system.** Operating system it is designed for.
- **Category.** Directory or group of microservices accessible from Workspaces where it will be hosted. Categories must be predefined in Organization.
- **Efficiency.** Number of minutes the user saves with each execution.

1. Click `Next`.

> **INFO**
>
> The name of a microservice configured for execution by the end user **must not contain special characters** like \ / : * ? " < > or specific language characters that may vary depending on the keyboard layout.

Phase 2 - License

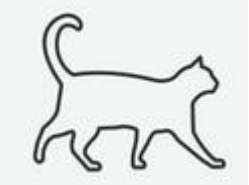
1. Choose from the dropdown options the type of license the microservice will have.
2. Click `Next`.



Phase 3 - README

1. Enter the detailed description of the microservice in Markdown format.
2. Click `Next`.

To set a title with Markdown, simply start the line with `# Title`. Here are some examples of its 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`

Phase 4 - Code

1. Enter the script of the microservice.
2. Click `Next` to finish.

Once the phases are completed, the microservice will appear in the main table of the section.

Technical considerations

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 may mean that some cmdlets do not have the expected output in relation to the execution performed. For this reason, if you're developing a script in PowerShell, you must consider a series of points:

- 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 manager.** In `Scope`, you can set `Workspaces` or `Platform`, which makes it very easy to interact with processes, services, and act with administrative permissions on the device, but it may complicate accessing specific user information or their session.

    - **Execution from user session.** In `Scope`, you can set `Sessions`, which is very useful for accessing user information like the log, 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 you 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 during the execution.

Enable a Microservice

Enable a Microservice:

1. Access `Portal` -> `Microservices` -> `Designer`.
2. Find the microservice in the list and click on it.
3. Click the `Enable` button (located in the upper right corner).
4. Once enabled, the microservice will be shown with a green dot in the Marketplace section.

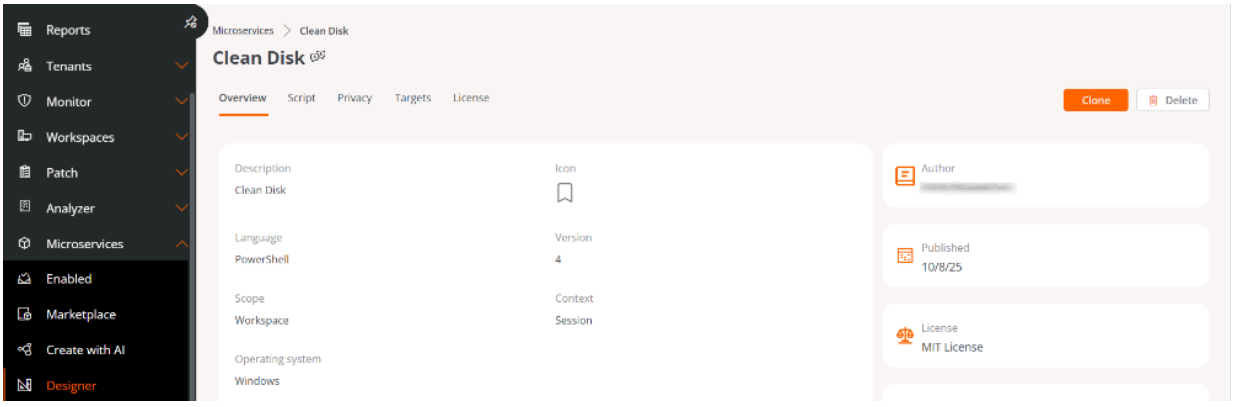
Remove microservice

Before removing a microservice, it is necessary to consider the following conditions:

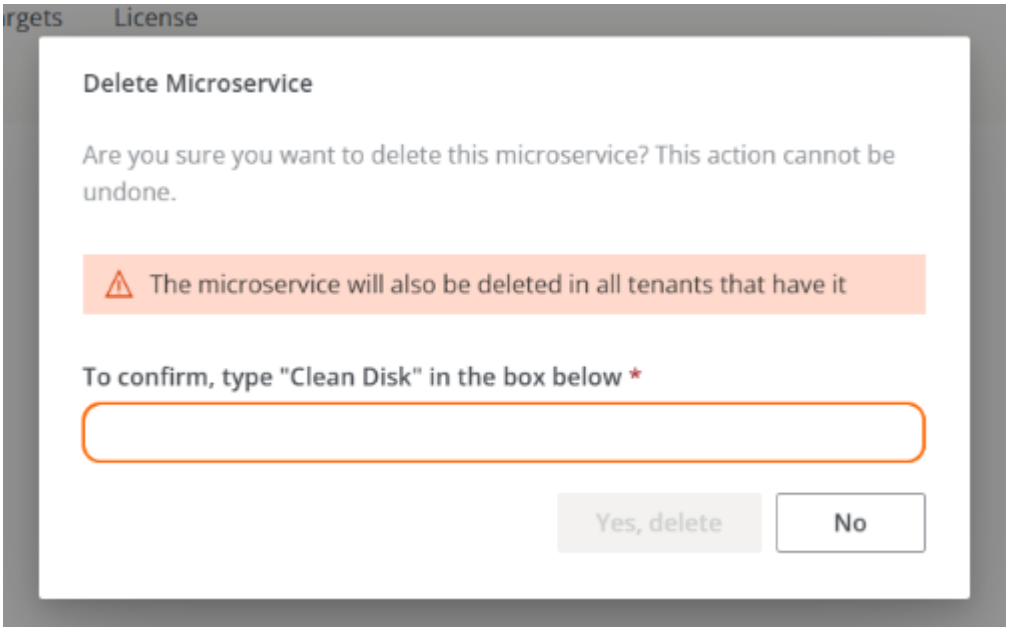
- Only microservices that have been previously archived can be removed.
- The microservice must not be active in any tenant.
- There cannot be any flow that has it assigned.

Once these requirements are met, you can proceed with the definitive removal of the microservice through the following steps:

1. Access `Portal` -> `Microservices` -> `Designer`.
2. In the microservices table, choose the desired item and click `Actions` -> `Archive`.
3. Confirm the action in the pop-up window to complete the archiving.
4. Return to the table and click on the name of the microservice you just archived.
5. From the `Overview` tab, click the `Delete` button.



6. Confirm the deletion in the corresponding pop-up window.



INFO

When a microservice is removed from the organization, it is also automatically removed from the list of microservices for its tenants.

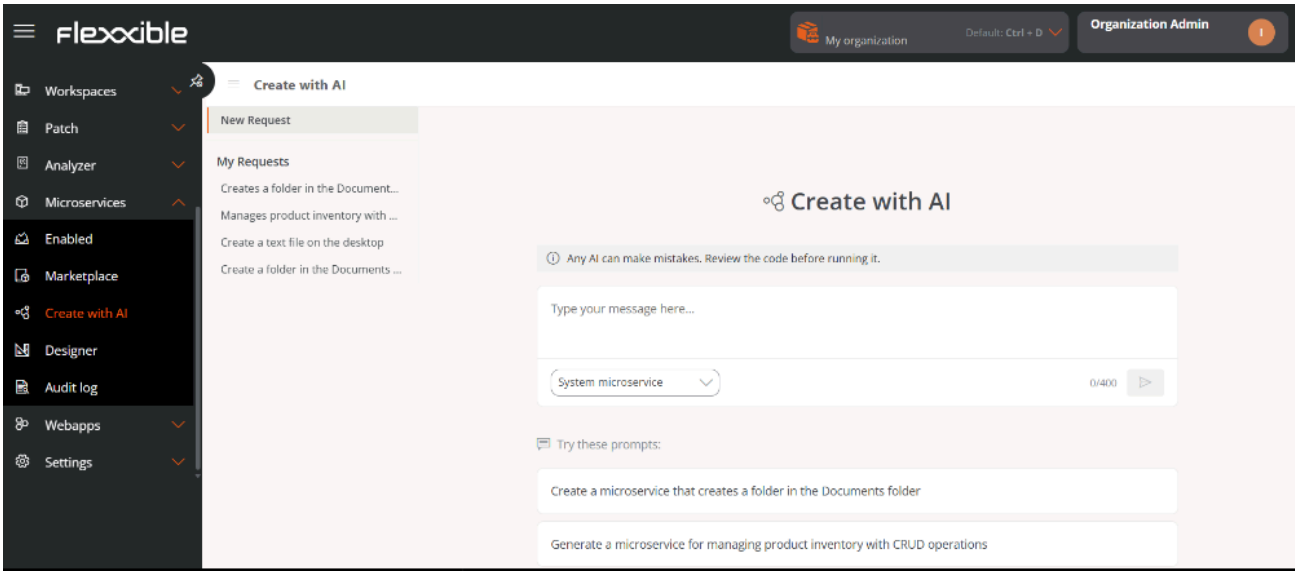
WARNING

The removal of a microservice is irreversible. Once deleted, it cannot be restored.

Portal / Microservices / Create with AI

Microservices design using Artificial Intelligence (AI) allows for automatic generation from requests expressed in natural language. This feature reduces the need for advanced technical knowledge and speeds up the development process by eliminating the need for manual programming.

The microservice code is generated according to the request made, but the creation process is completed in the Designer section, from where the microservice can be enabled for execution through the Workspaces module or from the end user's device.

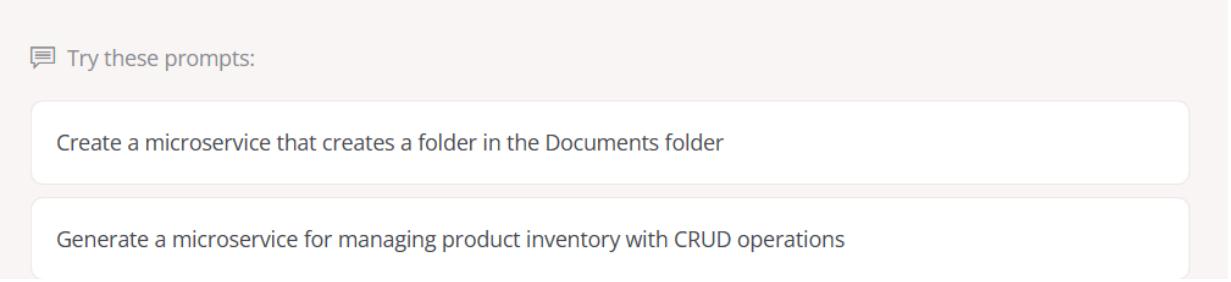


Create new microservice

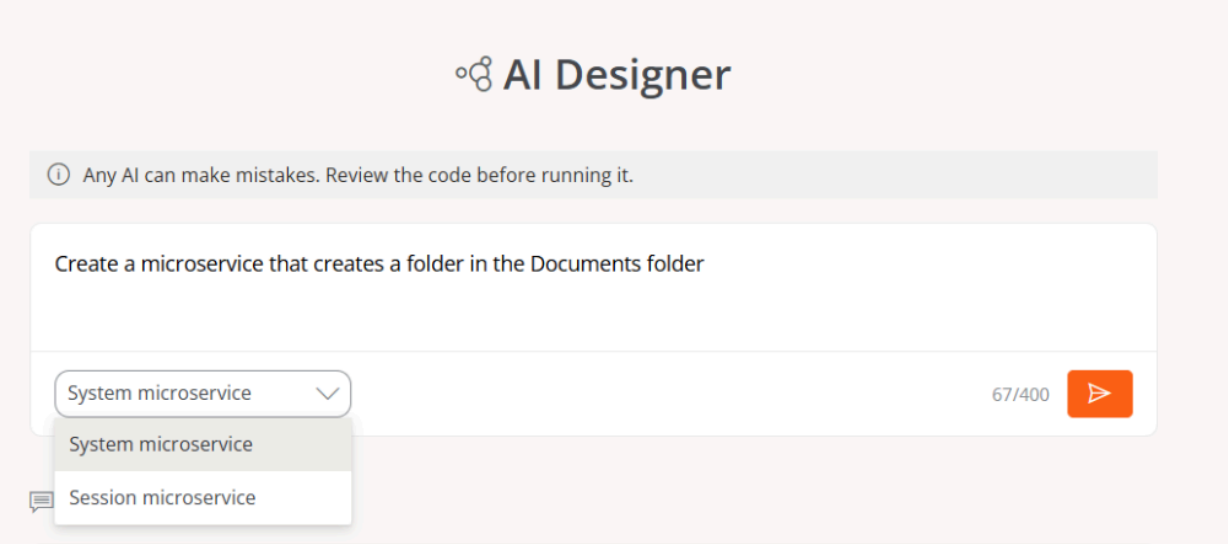
The steps to create a microservice through AI are as follows:

1. Access `Portal` -> `Microservices` -> `Create with AI`.

2. In the central panel, write the request in natural language with a maximum of 400 characters. At the bottom, `Try something like this` offers examples that can help create a request.



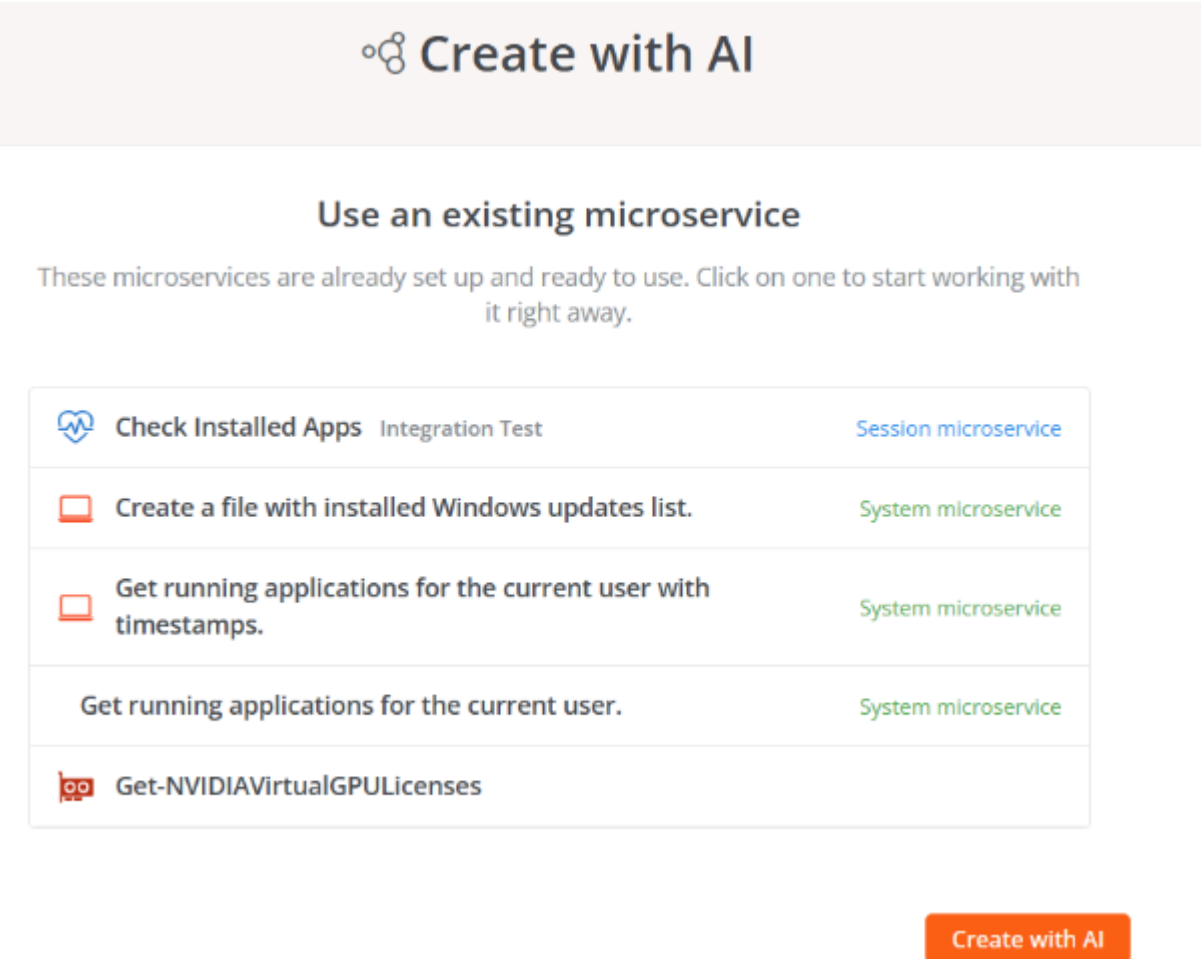
3. In the dropdown, choose the scope of execution: *System Microservice* or *Session Microservice*.



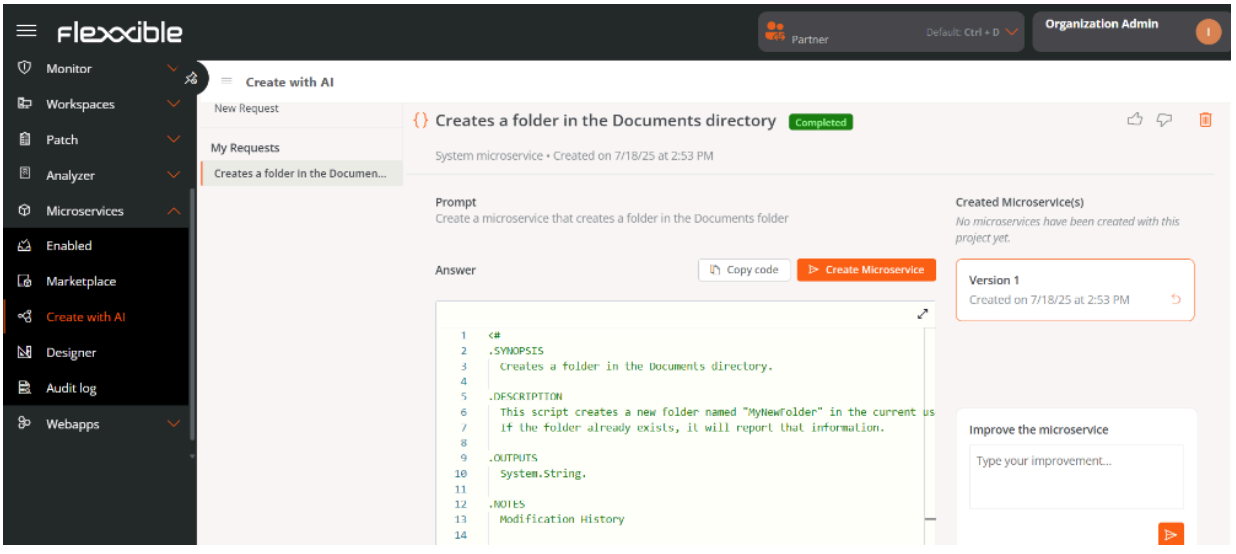
4. Click the arrow in the orange box to continue.

5. If similar microservices exist, they will be offered as available alternatives. The user can click on each one of them to analyze their use in relation to the desired goal. By doing so, they will be redirected to the Marketplace section.

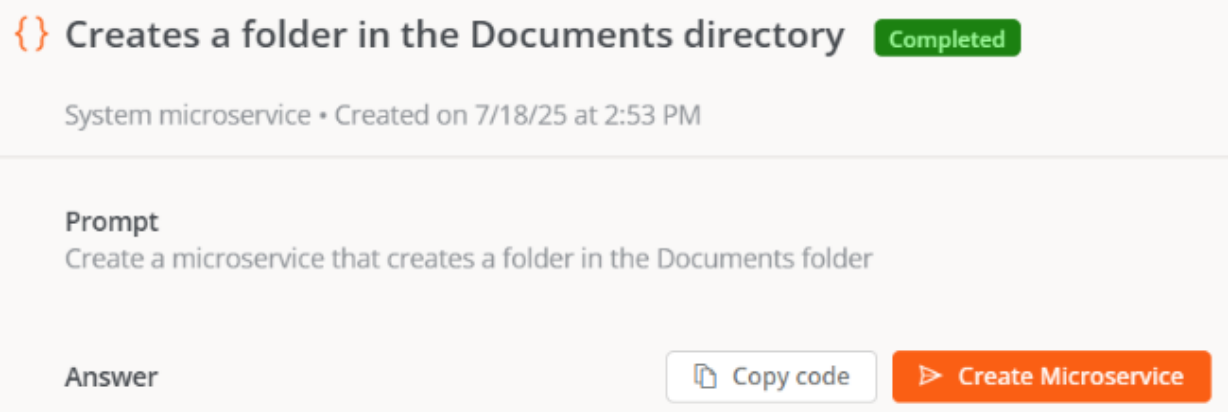
   If, after reviewing the alternatives, the user decides they need to create a new microservice, they should click on `Create with AI`.



6. A few seconds later, the AI will design the microservice.

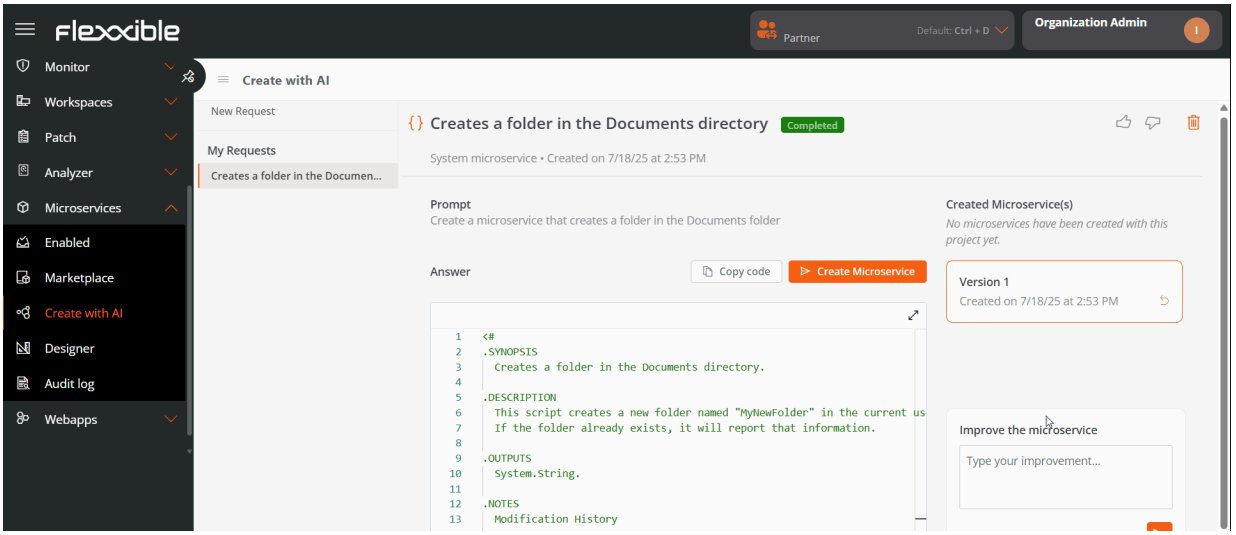


The `Copy Code` button allows you to copy the generated code to the clipboard, facilitating its use in testing if required.



> **INFO**
>
> This feature only generates microservices in PowerShell.

7. Review the microservice code.

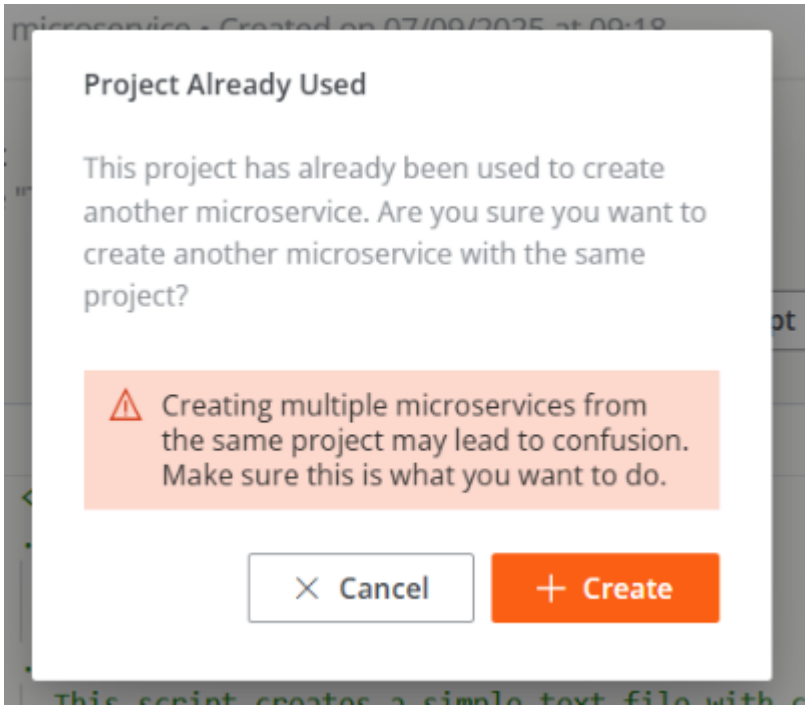


8. The `Improve the microservice` box, located at the bottom right of the screen, allows the user to add information to optimize the microservice. With each improvement, a new version of the code is generated, which can be seen in the Created Microservices column at the top.

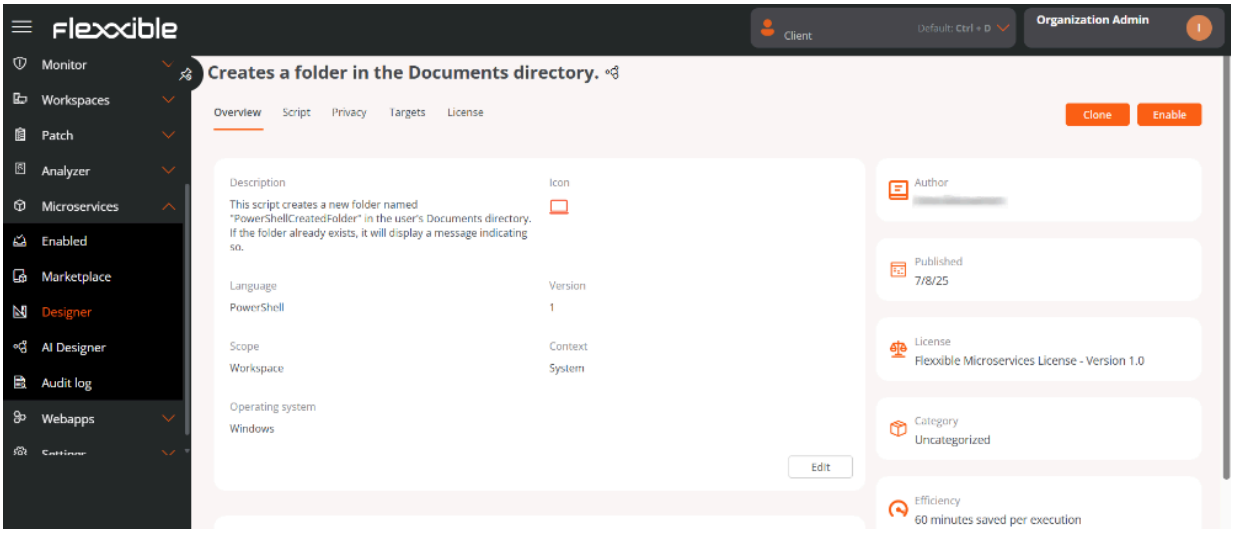
9. Click on `Create microservice`.

INFO

If you click `Create microservice` again on an already existing microservice request, you will be asked for confirmation to verify if you want to create a new one. If so, another microservice will be generated with a number at the end to differentiate it from the original. **In no case will the code or configuration of an already created microservice be overwritten.**



10. Next, the user will be directed to the Designer section to edit the microservice configuration, if desired.



11. Click on `Save`.

12. The microservice will appear in the list of the Designer and Marketplace sections.

> **INFO**
>
> By default, AI-generated microservices are created without any category and have the **Flexxible Microservices License**. This configuration can be modified in Designer.

> **WARNING**
>
> AI can also make mistakes. The execution of microservices designed with this method is the responsibility of the user.

Drafting requests

The more detailed a request is, the more precise and useful the generated microservice will be. To achieve this, it's recommended that messages meet the following guidelines:

1. Concise

- Avoid vague, redundant, or excessively long phrases.
- Use direct language.
- Clarity should take precedence over word count.

2. Specific

- Explain exactly what you want to achieve.
- Include details such as output format, tools, objectives, constraints, etc.
- The more details provided, the better the outcome.

3. Context

- Indicate where the action will be applied.
- Without context, the AI might create generic results.
- Specify the purpose of the microservice.

4. Imperative verbs

- It is suggested to use verbs that clearly indicate what the AI should do.
- Examples: create, do, analyze, generate, search, compare, etc.

Recommendations

Besides writing clear requests, it's advisable to structure them in a way that the AI precisely understands what to do and how to present the result. To achieve this, consider the following recommendations:

- **Avoid ambiguity.** Each request should have only one possible interpretation.
- **Iterate and improve.** If the result is not optimal, you can adjust the request by adding more context.
- **Use examples when possible.** Showing a sample output better guides the outcome.
- **Specify the exact action.** Describe directly the task that the AI should execute.
- **Include reference examples.** Show how the expected output should be, to correctly guide the AI's interpretation.
- **Set restrictions or rules.** Indicate the limits, conditions, or requirements that must be met during execution.
- **Define success criteria.** Explain what conditions the result must meet to be considered satisfactory.

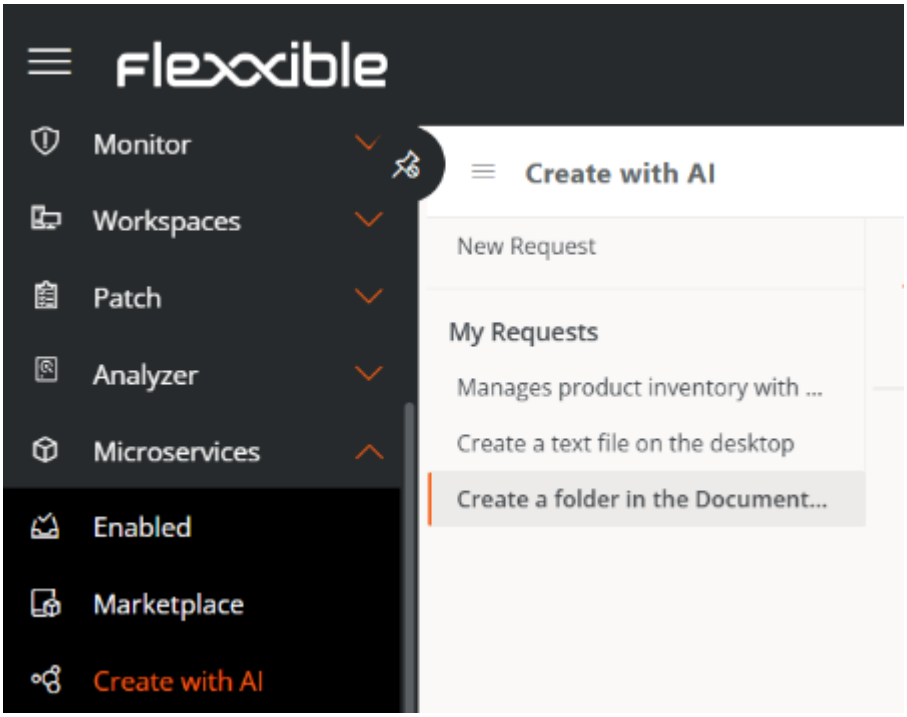
Examples of how to make a request

❌	✅	
Can you back up the desktop and documents?	Backup the desktop and the Documents folder. Copy these files in ZIP to \nas\backups<username>. Also, I want to keep only the latest copy. Delete the rest of the files once the copy has been successfully completed.	
Create a scheduled task on devices to log	Create a scheduled task in Windows 11. The task should log off the current user when 30 minutes of inactivity are	

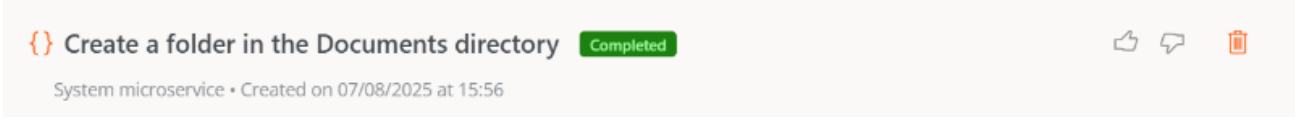
❌	✅	
off when inactive for a certain time.	detected.	

My requests

The `My requests` column, located on the left of the screen, shows the microservice requests the user has made to the AI. Each user can only see theirs; they are not shared with the rest of the organization.

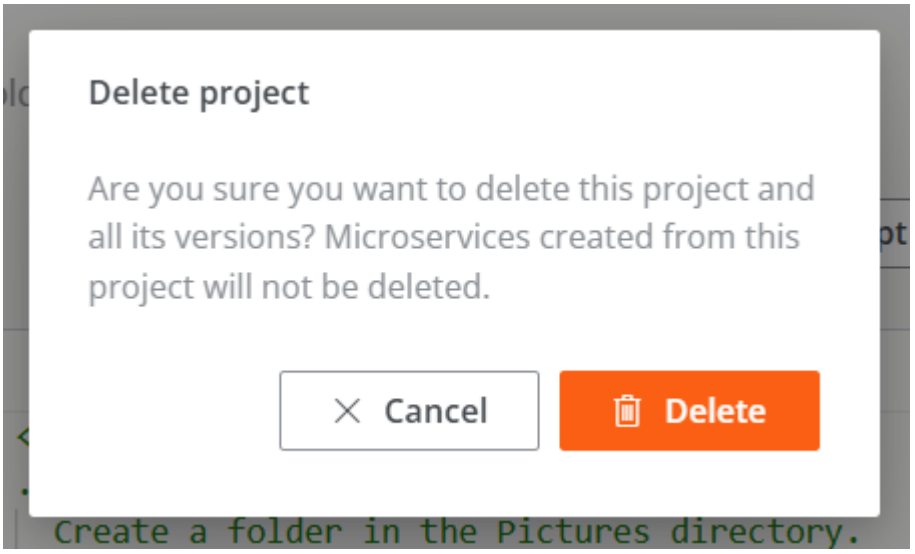


This functionality allows the request history to be visible at all times to the user who created it, so they can always return to them. It also allows for feedback on the result; for this, the user can click on the thumb-shaped buttons located at the top right of the screen.



Delete a request

1. Go to the column `My Requests`, located on the left side of the screen.
2. Click on a request from the list to enter the code details.
3. Click on the `Delete` icon located at the top right of the screen.
4. Read the warning message.



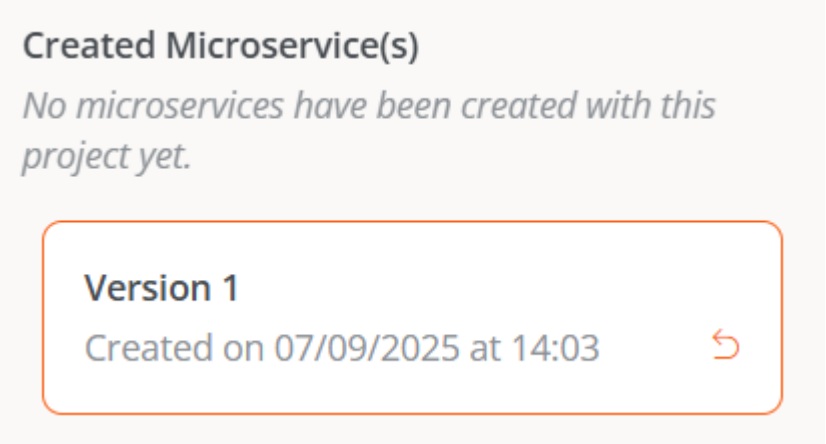
5. Click `Cancel` or `Delete`, as appropriate.

> **INFO**
> Deleting a request does not imply deleting the microservice created from it.

Created Microservices

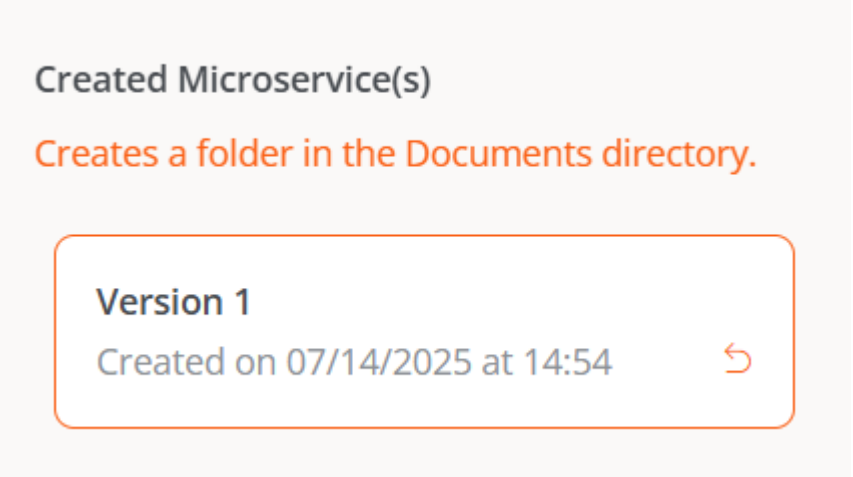
On the far right of the screen, the `Created Microservices` column lists all the microservices created from a request. This panel allows identifying whether a request has resulted in one or more microservices, as well as accessing each of them directly for review.

- When the AI designs the first version of a microservice, but it has not been created through the `Create microservice` button, the `Created Microservices` column shows a message like the one in the following image:

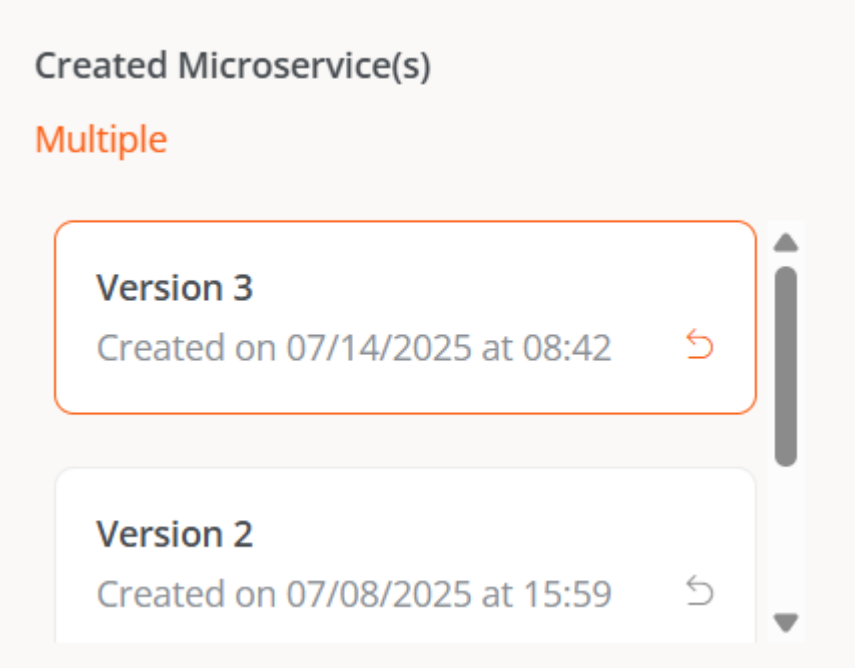


The orange arrow located in the box of each version allows loading the previous version's code.

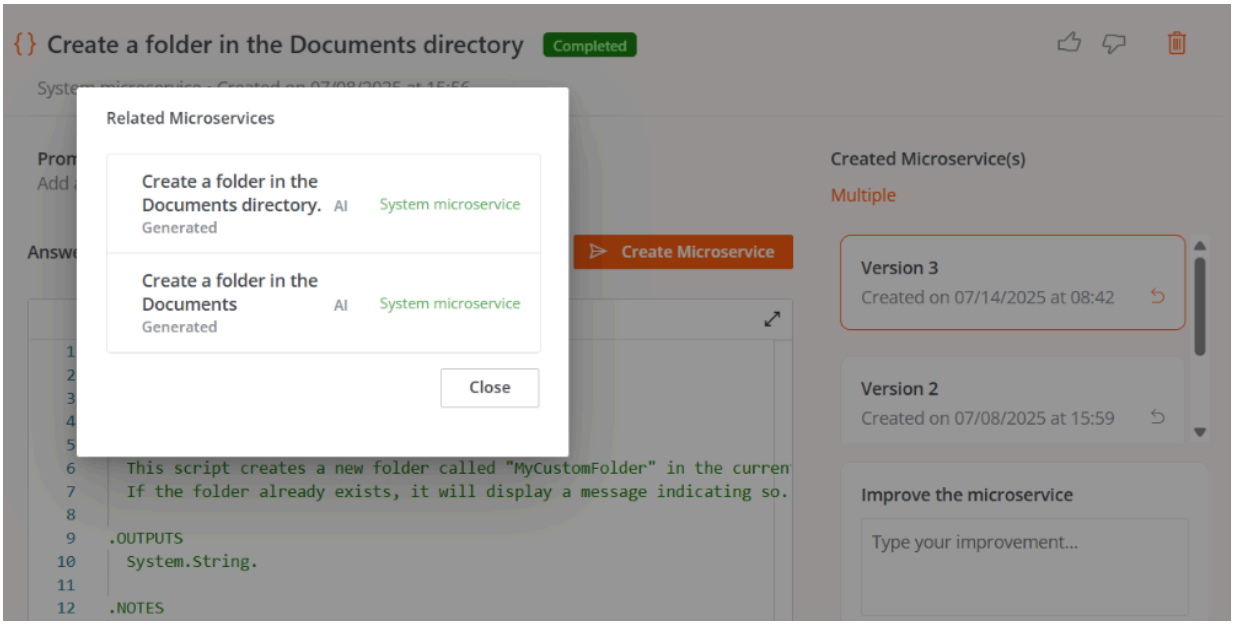
- When the AI designs the first version and you click `Create microservice`, the `Created Microservices` column shows the name of the microservice. Clicking on it will take you to its detail view in the Designer section.



- When the AI designs and creates more than one version of a microservice, the `Created Microservices` column shows the word *Multiple*.



Clicking on *Multiple* opens a modal window with a list of the microservices created from that request. Selecting one of them accesses its detail view in the Designer section.

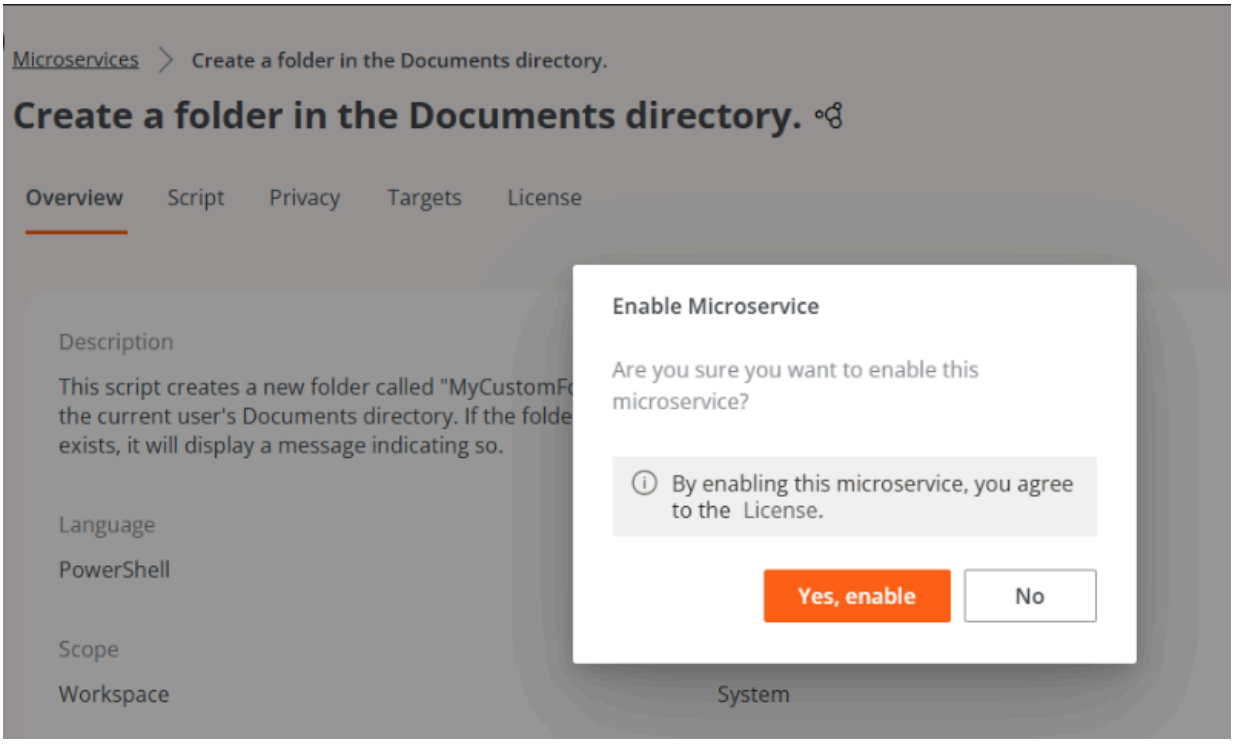


Enable a Microservice

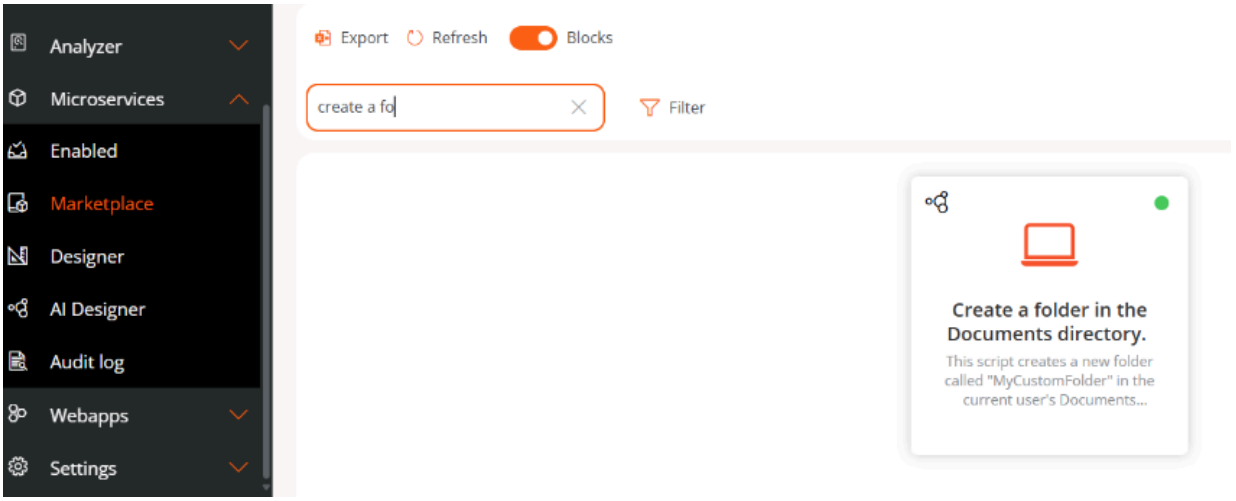
The process to enable or disable an AI-generated microservice is the same as that used for manually creating microservices.

Steps to enable a microservice from Designer:

1. Access `Portal` -> `Microservices` -> `Designer`.
2. Find the microservice in the list and click on it.
3. Click the `Enable` button located at the top right of the screen.



4. The microservice will appear marked with a green dot (indicating it is enabled) in the Marketplace section.



Steps to enable a Microservice from Marketplace:

1. Access `Portal` -> `Microservices` -> `Marketplace`.
2. Find the microservice in the list and click on it.
3. Click the `Enable` button located at the top right of the screen.
4. The microservice will appear marked with a green dot (indicating it is enabled).

> **INFO**
>
> Enabled microservices execute on demand from the Workspaces module: section Workspaces (System context) and section Sessions (Session context), according to defined configuration.

Enable a microservice for the end user

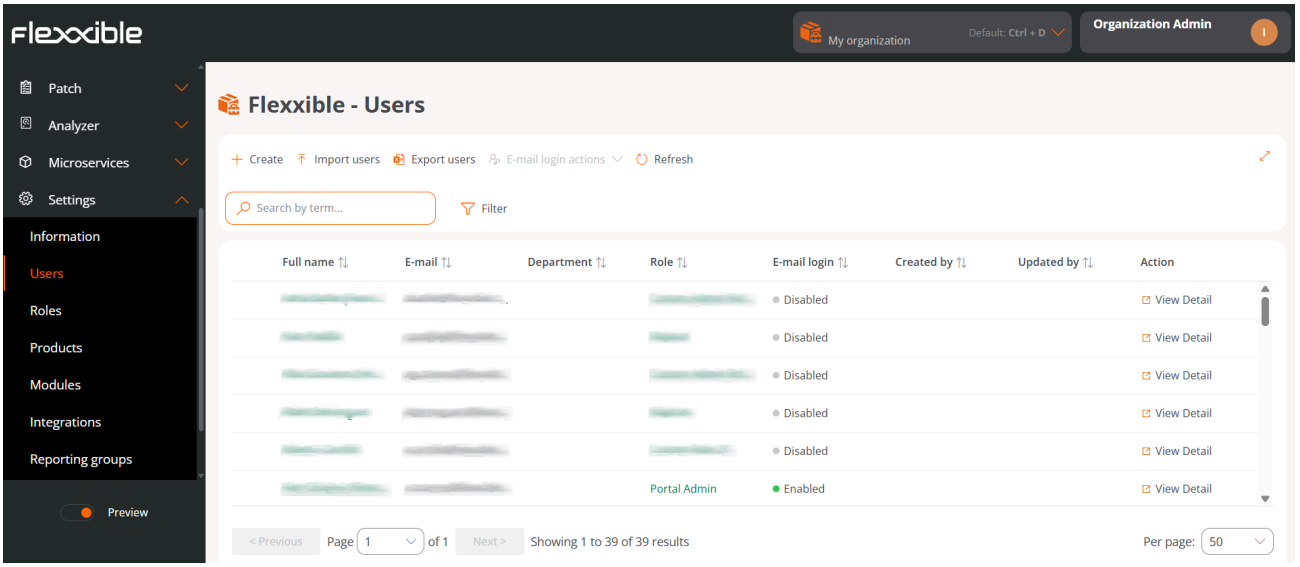
The process of enabling an AI-created microservice for execution by the end user is the same as for microservices designed manually.

Please consult the guide Enable Microservices for End Users.

> **INFO**
>
> Flexxible recommends checking the `Privacy` and `Recipients` tabs in the Designer section before enabling a microservice to ensure they have the desired configuration.

Portal / Settings

The **Configuration** section provides specific management tools for the selected organization. Its sections cover key aspects for service implementation, such as user creation, role assignment, Flexxible Remote Assistance, reporting groups, among others.

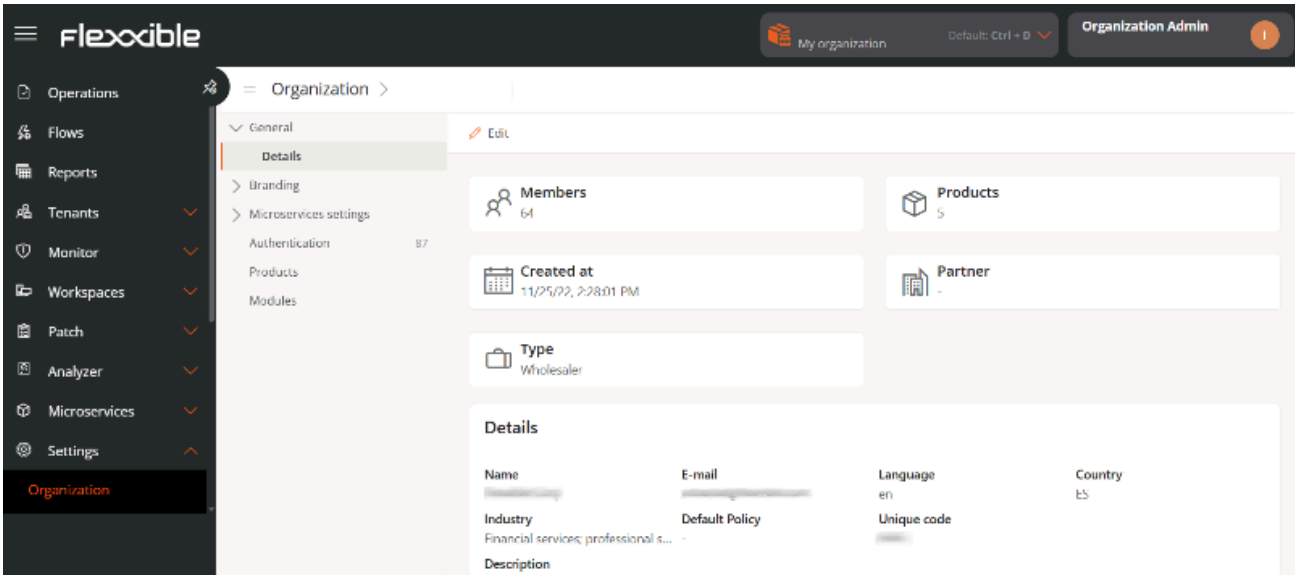


The Configuration section consists of the following subsections:

- Organization
- Users
- Roles
- Integrations
- Reporting Groups
- FlexxAgent Version
- Audit
- Policies

Portal / Settings / Organization

Organization allows managing the functionalities that affect the organization's environment globally, from assigning the name on the platform to configuring remote assistance.



Management can be done from the following sections:

- General
- Branding
- Microservices
- Authentication
- Products
- Modules
- Domains
- SSO Integrations
- SCIM Provisioning

General

Allows defining general information of the organization that can be updated anytime using the `Edit` button. The following data can be modified:

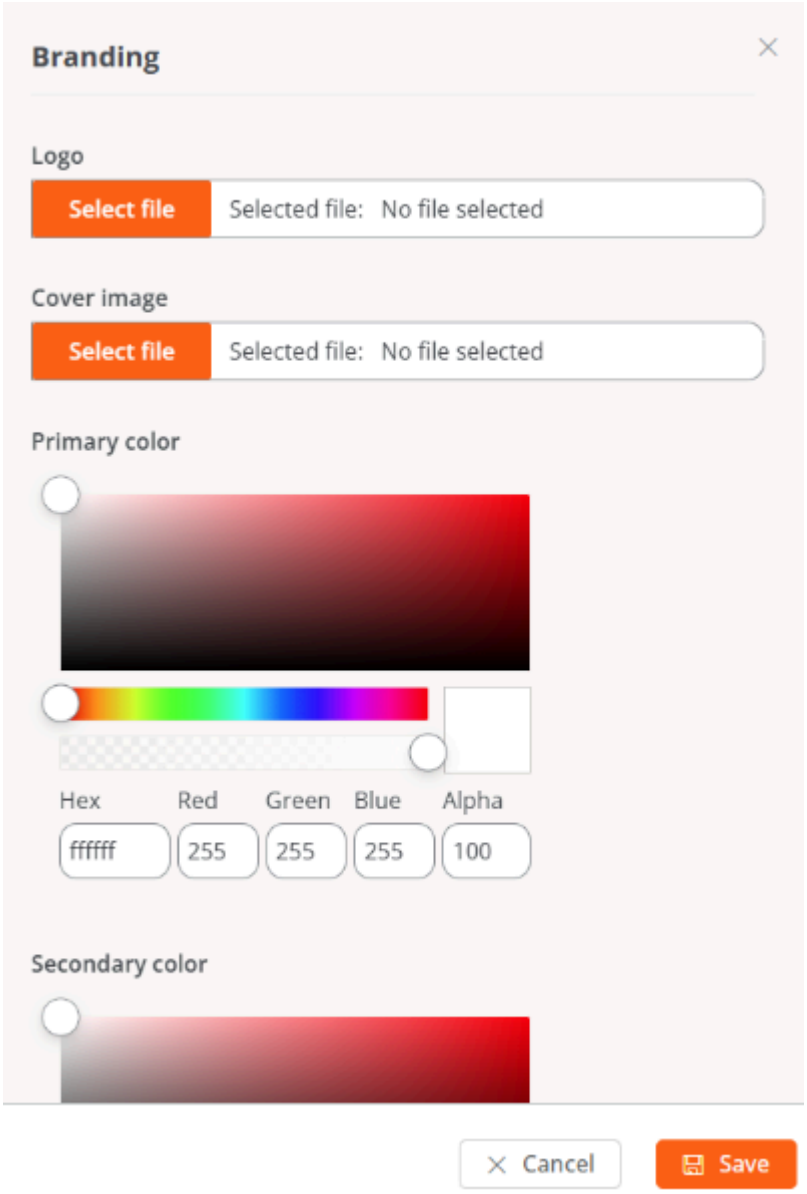
- **Name.** Organization's name.
- **Email.** Associated email address.
- **Language.** Configured language.
- **Country.** Country the organization belongs to.
- **Sector.** The sector it belongs to.
- **Description.** Description of the organization.

Additionally, from this section you can also access the following information:

- **Members.** Number of members that the organization has registered on the platform.
- **Products.** Number of Flexxible products the organization has contracted.
- **Creation Date.** Date when the organization was registered on the platform.
- **Partner.** For *client* type organizations, allows defining or modifying the *partner*.
- **Type.** Type of organization that corresponds to it.

Branding

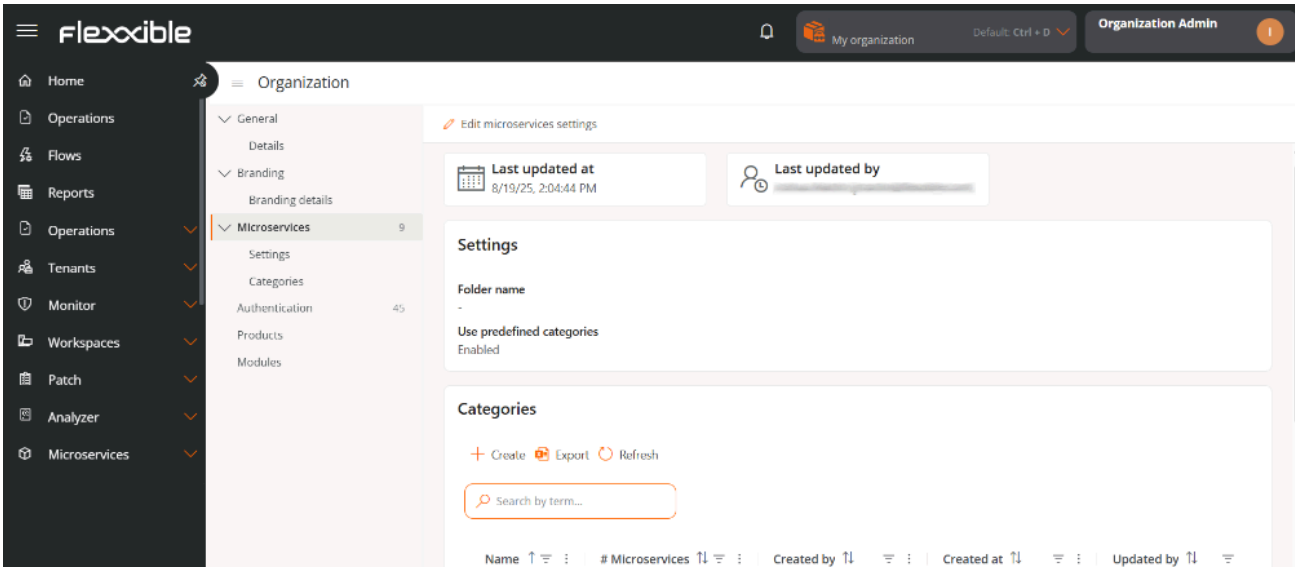
Facilitates the storage of information linked to the organization's brand identity. Clicking the `Edit Brand Settings` button leads to a form for uploading the organization's logo and cover image, as well as a palette to define corporate colors in hexadecimal format.



This section also indicates the date and time of the last update, as well as the name and email of the user who made it.

Microservices

Through its configuration and classification options, it allows changing the name of the folder containing the end-user microservices and managing the predefined categories. It also shows the date and the name of the user who updated the information.

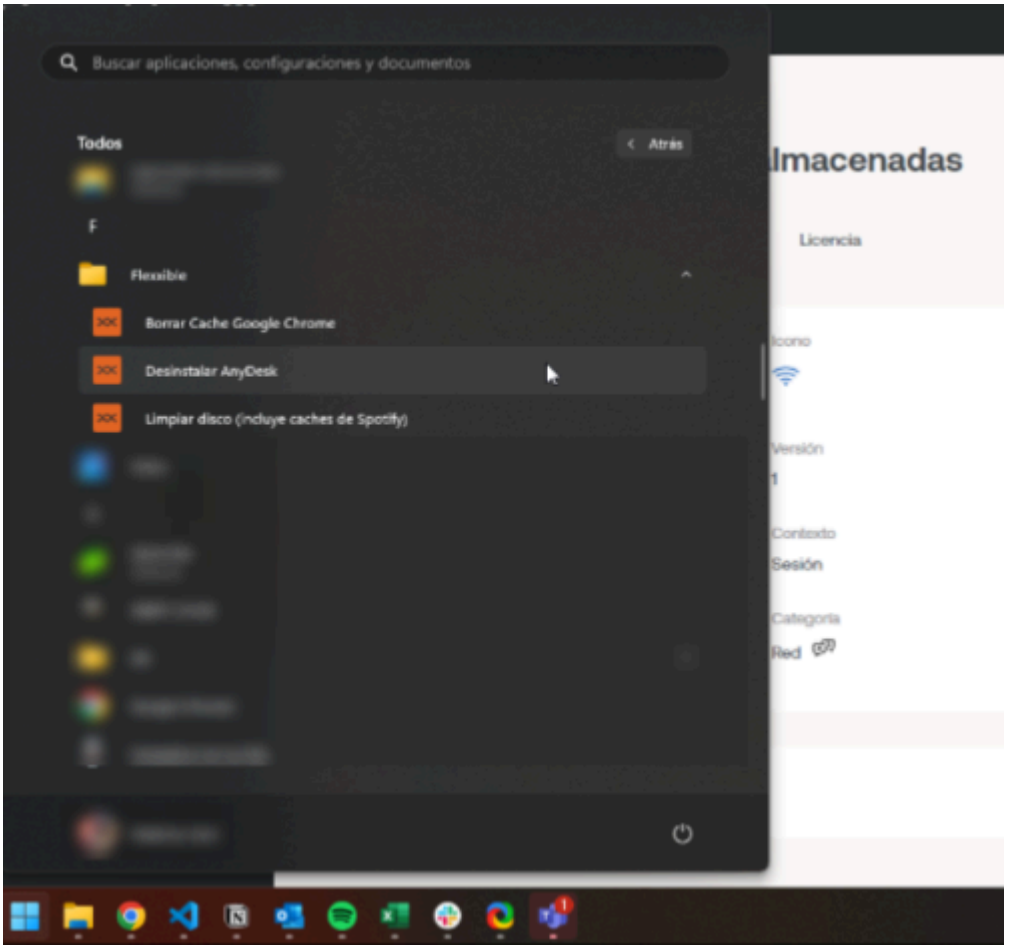


Settings

In this section, it shows the name assigned to the end-user microservices folder and if the option to use predefined categories is enabled.

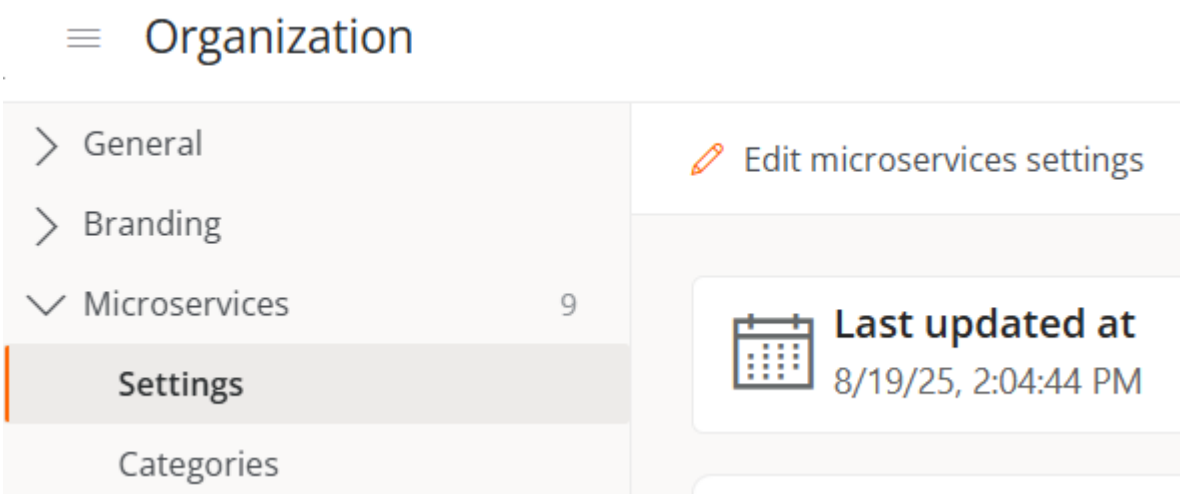
Folder name

When microservices are enabled to be executed by the end-user, they are automatically added to a folder on the device called **Flexxible**; however, this name can be modified.

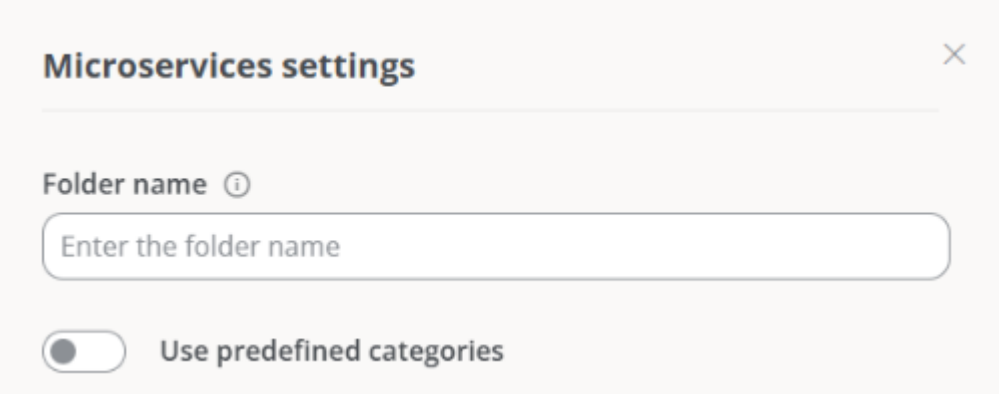


Rename the microservices folder

1. Go to `Portal` -> `Settings` -> `Organization`.
2. In the left side menu, select `Microservices`
3. Click on `Edit microservices configuration`.

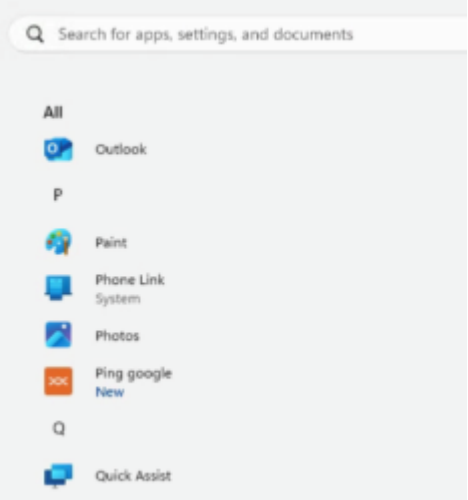


4. Write the new name in the `Folder name` field. The structure must be between 3 and 50 characters and can only contain letters, numbers, hyphens, and underscores.



5. Click on `Save`.

> **INFO**
>
> If the device has Windows 11 as its operating system and only one microservice is enabled for an end-user, the **Flexxible** folder will not be displayed; instead, only the microservice icon will be visible in the start menu.

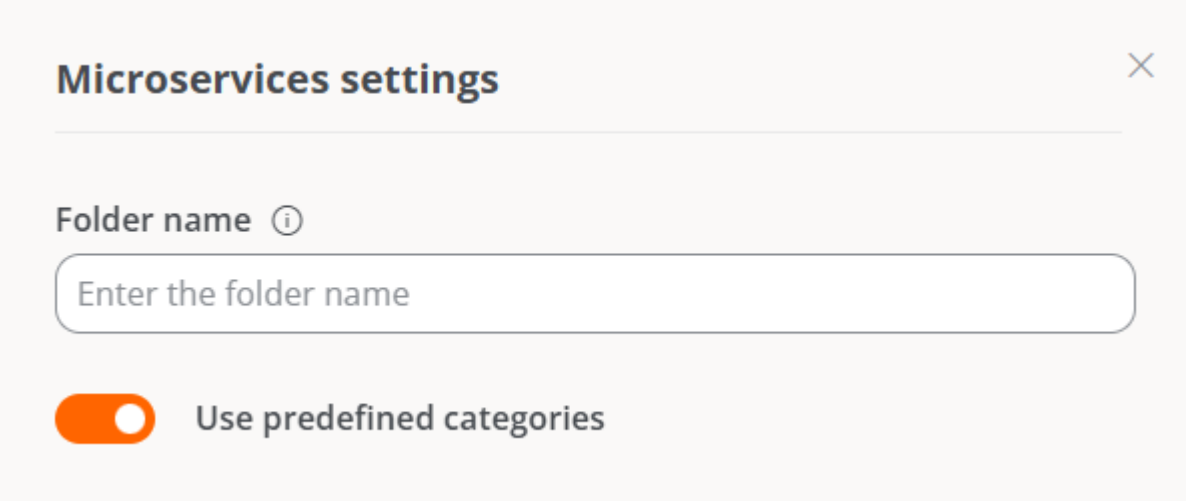


Predefined categories

This functionality allows users with the role of *Organization Administrator* to define and manage classification categories for the microservices. The configuration can only be carried out from the main organization and is automatically inherited by sub-organizations, ensuring consistency and preventing the creation of random categories.

Activate predefined categories

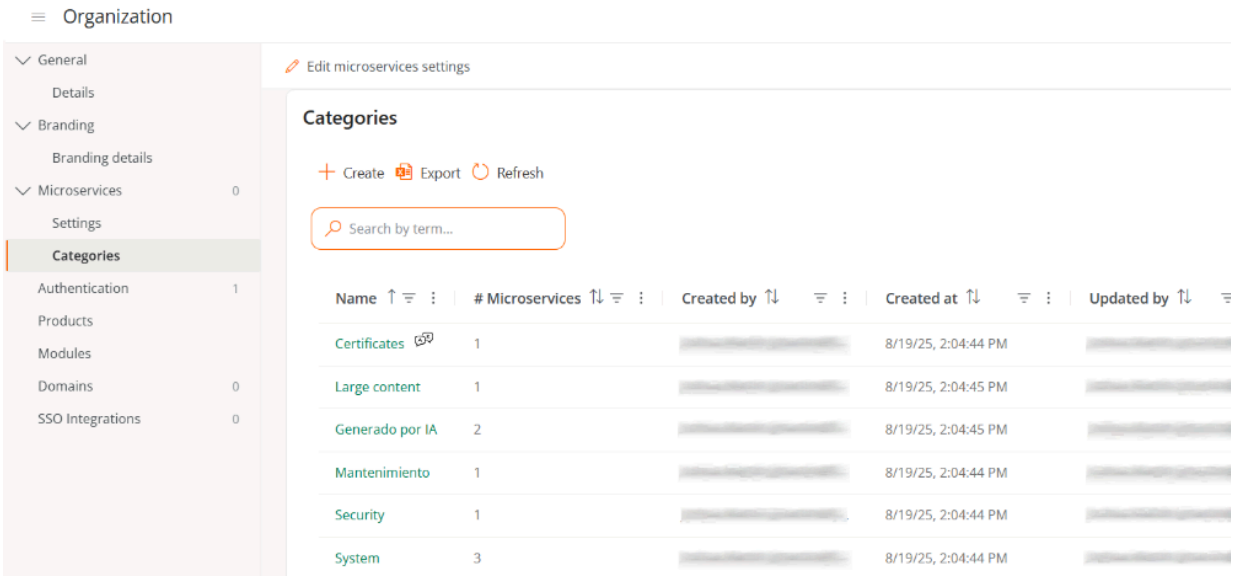
1. Go to `Portal` -> `Settings` -> `Organization`.
2. Select the `Microservices` tab.
3. Click on `Edit microservices configuration`.
4. Activate the `Use predefined categories` button.



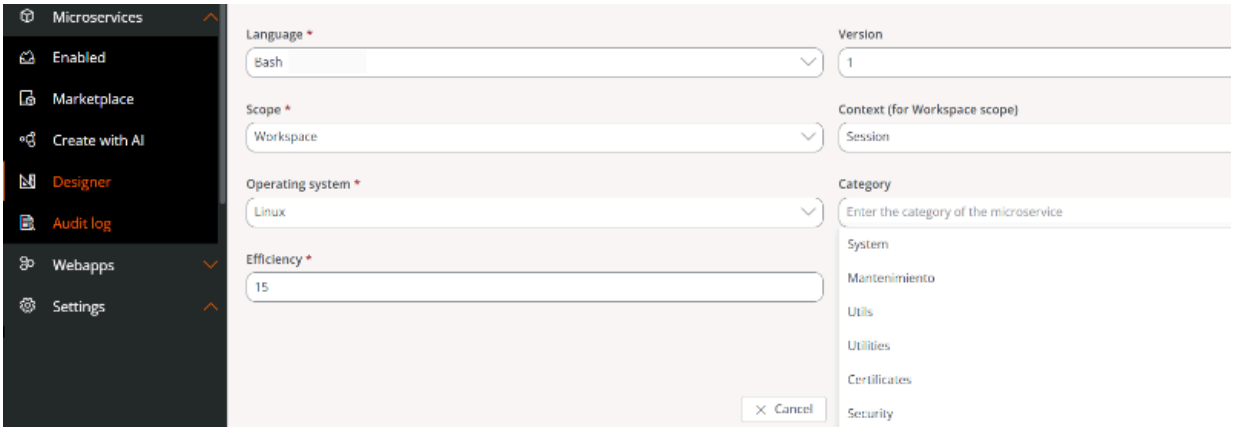
5. Click on `Save`.

When the functionality is active:

- The `Categories` section is created automatically, containing a table with the list of microservices categories of the organization.



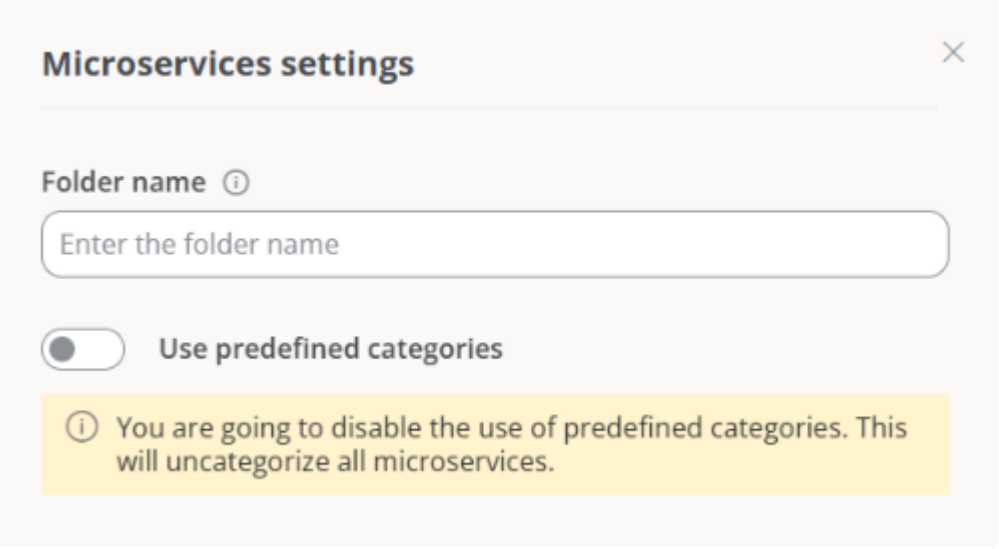
- The categories also appear in the Designer section, so that users can only select from the available categories in the list.



Deactivate predefined categories

1. Go to `Portal` -> `Settings` -> `Organization`.
2. Select the `Microservices` tab.
3. Click on `Edit microservices configuration`.
4. Deactivate the `Use predefined categories` button

When this option is disabled, a message is displayed informing the user that all microservices with assigned categories will lose that association, and it will be necessary to manually reassign them categories.

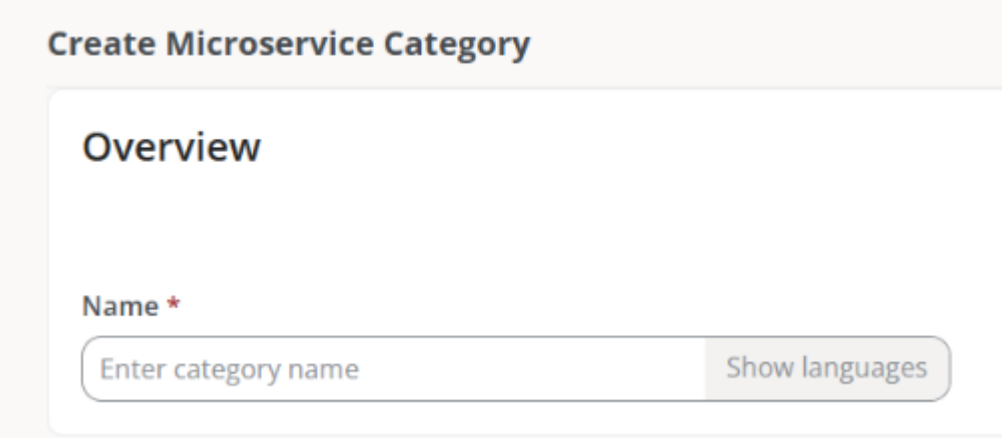


Categories

This tab is only enabled when the option of predefined categories is activated. Contains a table with the list of categories and allows creating new ones or deleting existing ones.

Create a predefined category

1. Go to `Portal` -> `Settings` -> `Organization`.
2. In the menu, go to `Microservices` -> `Categories`.
3. Click on `New` and type the name of the new category.



4. Click on `Save`.

The category name will be displayed both in the table and in the Designer section.

Delete a predefined category

1. Go to `Portal` -> `Settings` -> `Organization`.
2. In the menu, go to `Microservices` -> `Categories`.
3. Select a category from the table and click on `Delete`.

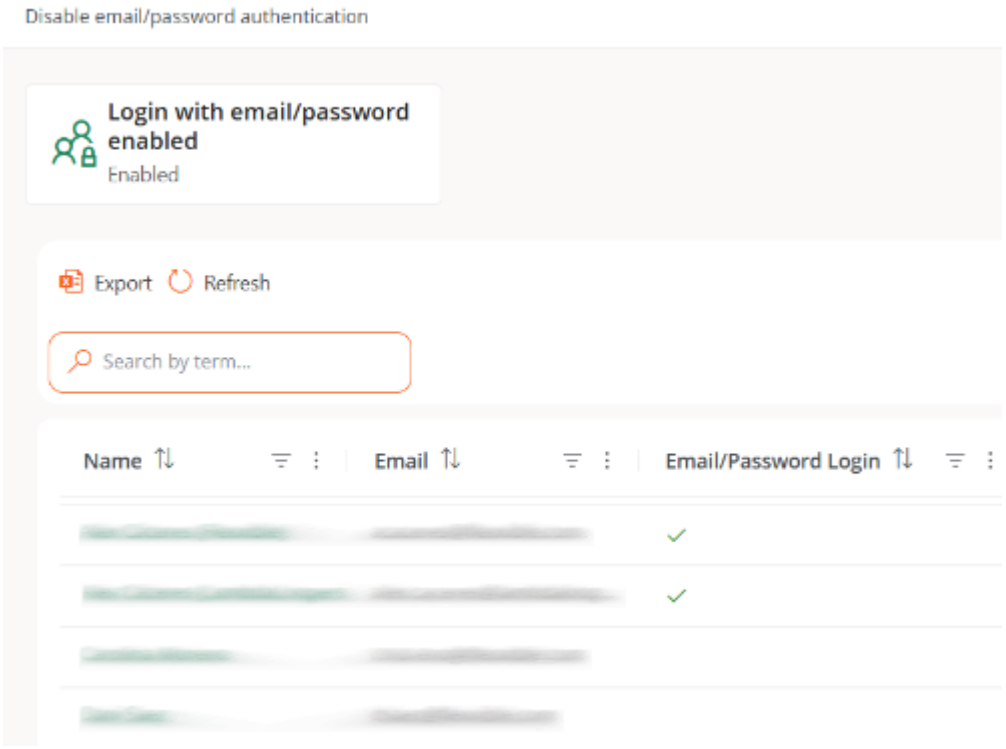
When a category is deleted, the microservices associated with it will become uncategorized and it will be necessary to manually assign them to another category.

Authentication

From this tab, an *Organization Administrator* can enable or disable the option to log in using email and password for the organization's users. In case there are suborganizations, the functionality can only be enabled or disabled from the main organization.

The button `Enable email/password authentication` or `Disable email/password authentication`, as applicable, allows enabling or disabling the possibility for users who are members of an organization or sub-organization to be able to activate login with email and password.

> **WARNING**
>
> If this option is disabled, users will not be able to log in with email and password or manage their account. All user credentials will be deleted. If this feature is re-enabled, users will need to reset their password and two-factor authentication again.



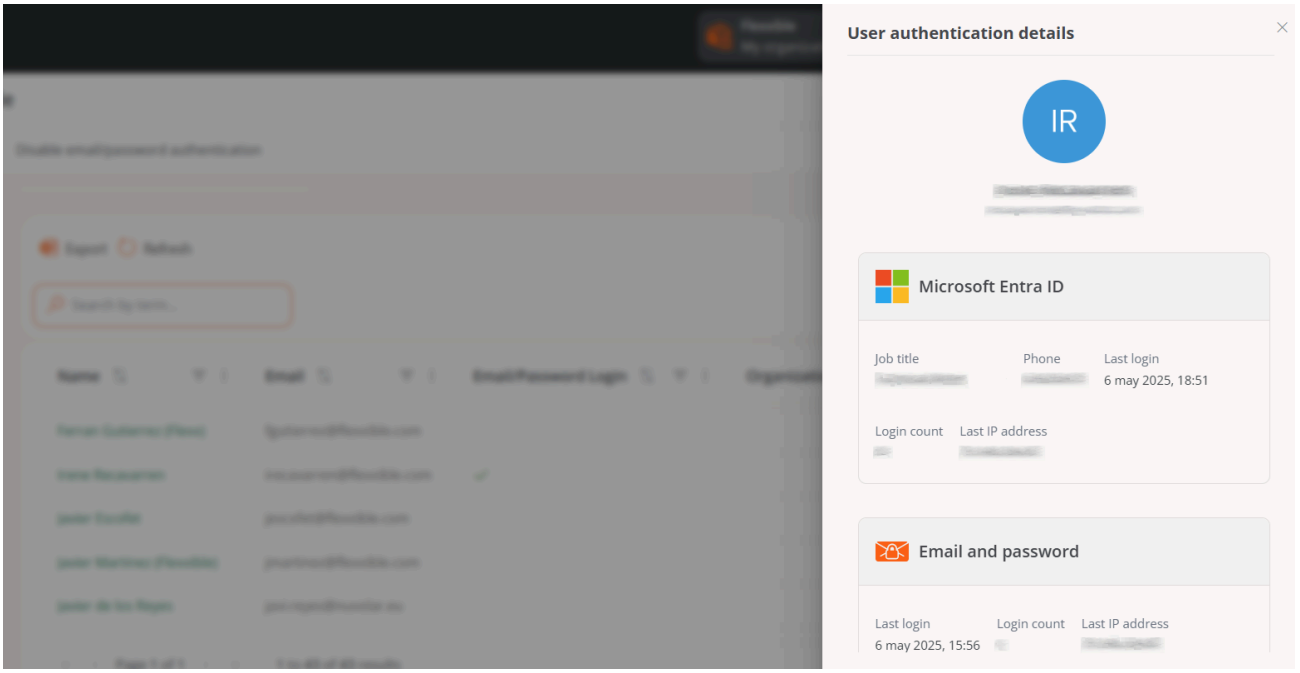
User table

Shows the list of organization members. At a glance, you can see which members have the option to log in via email and password enabled.

User authentication detail

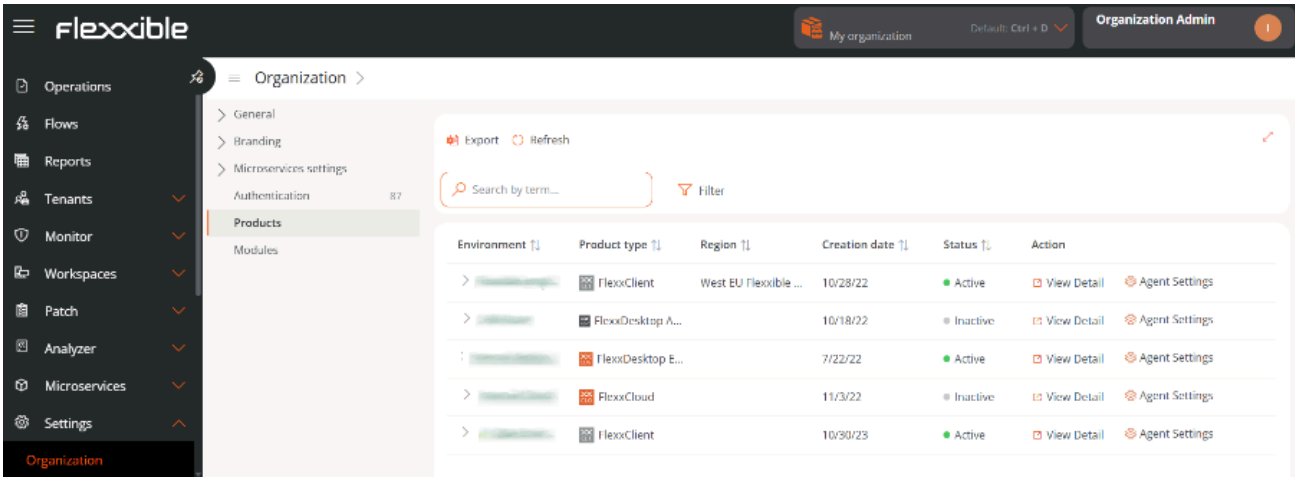
By clicking on a user's name in the table, you can access cards with specific information about the authentication method they have enabled:

- **Microsoft Entra ID.** *Role*, *Phone*, *Last login*, *Login count*, *Last IP address*.
- **Google.** *Last login*, *Login count*, and *Last IP address*.
- **Email and password authentication.** *Last login*, *Login count*, and *Last IP address*. Additionally, from here, the administrator can manage the Authentication security settings for that specific user, which includes Two-factor authentication and Password.



Products

This section reports on the Flexxible environments and products that the organization has. The list view shows data like the name of the environment where the product is deployed, the type of product that is available, region, creation date within the organization, and its status; the *Actions* field allows you to consult and edit its specific data.



In the table, the *Action* field shows two buttons to access more detailed information and edit the product's behavior: `View details` and `Agent settings`.

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.

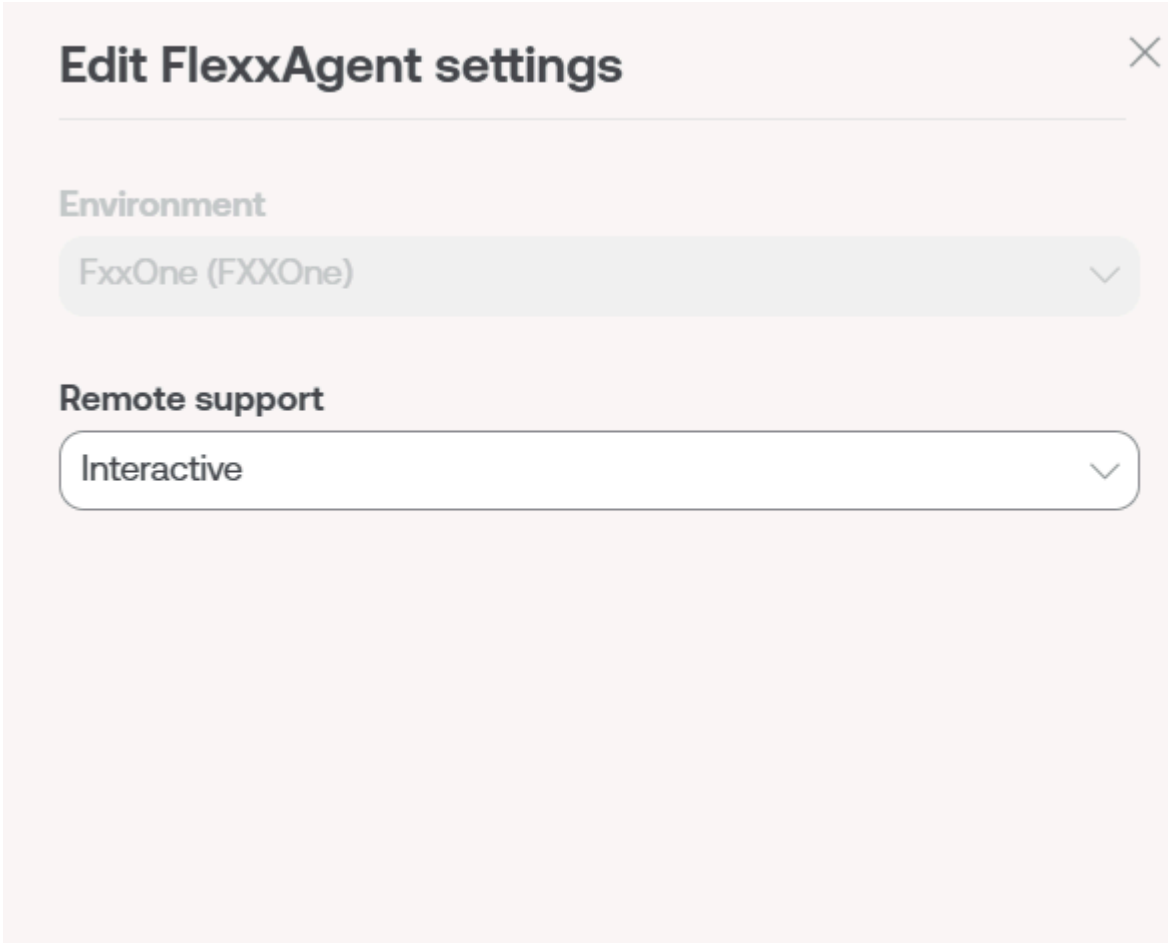
FlexxAgent Configuration

This form allows changes at the *Remote Assistance* and *Analyzer Proxy* levels.

FlexxAgent Configuration - Flexxible Remote Assistance

A user with the *Organization Administrator* access level 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.



FlexxAgent Settings - Proxy

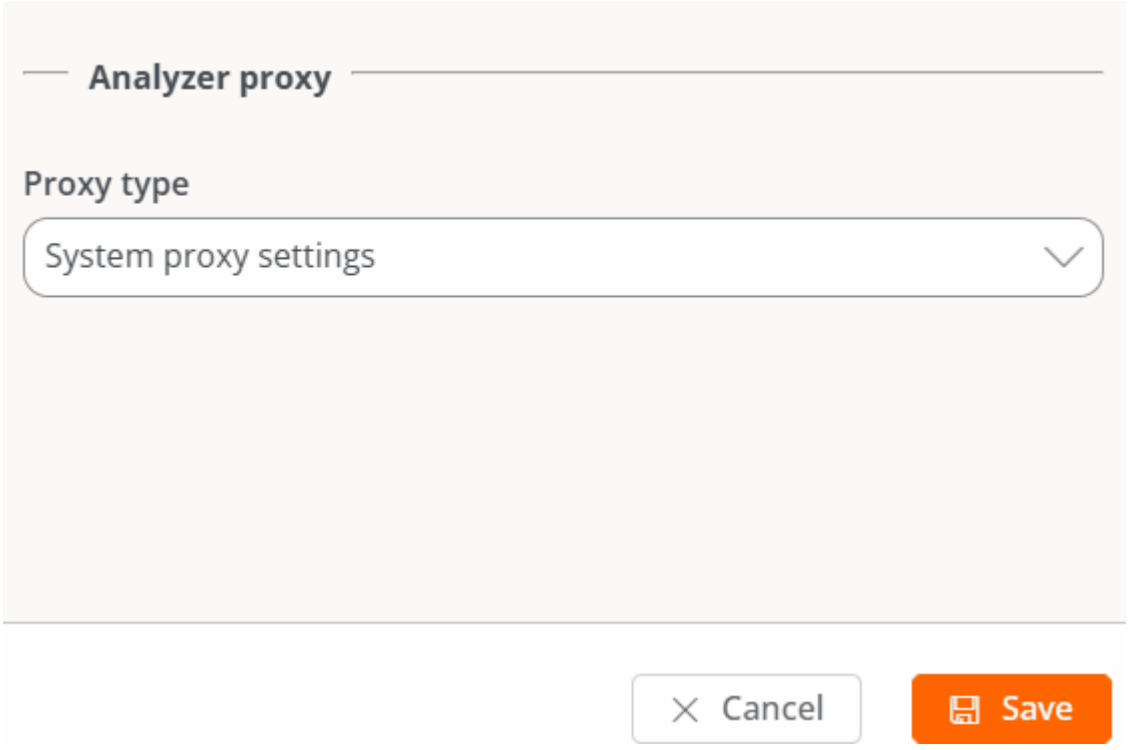
FlexxAgent consists of a Windows service called FlexxAgent Service, which manages two processes: *FlexxAgent*, which runs at the system level, and *FlexxAgent Analyzer*, which starts for each user session.

The proxy configuration of *FlexxAgent Analyzer* is not always the same as that of *FlexxAgent*, so according to the proxy operation in each environment, its settings will need to be set appropriately.

In the FlexxAgent settings, a user with the *Organization Administrator* access level 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.

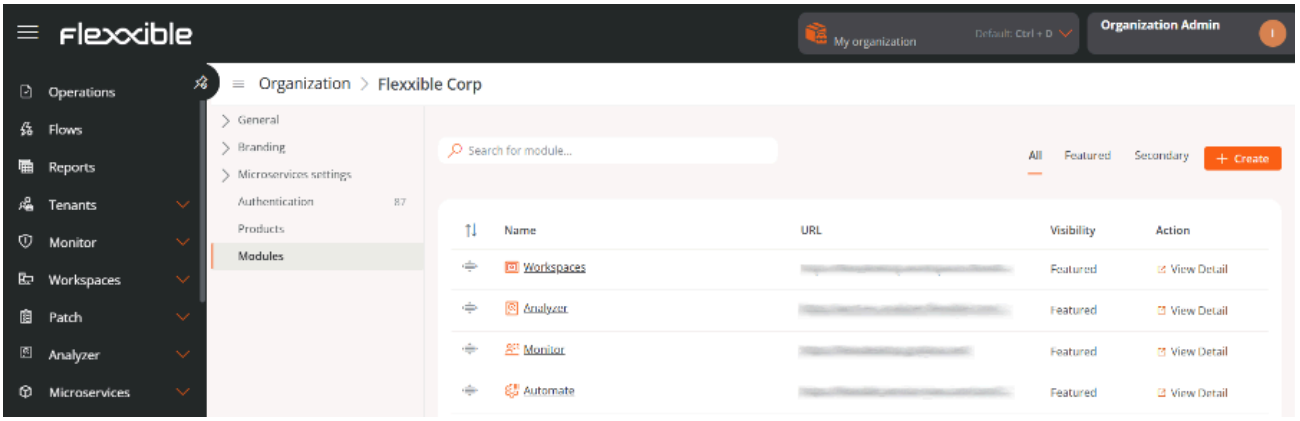


INFO

Some of the configuration options of FlexxAgent are not visible to users with the *Organization Administrator* role.

Modules

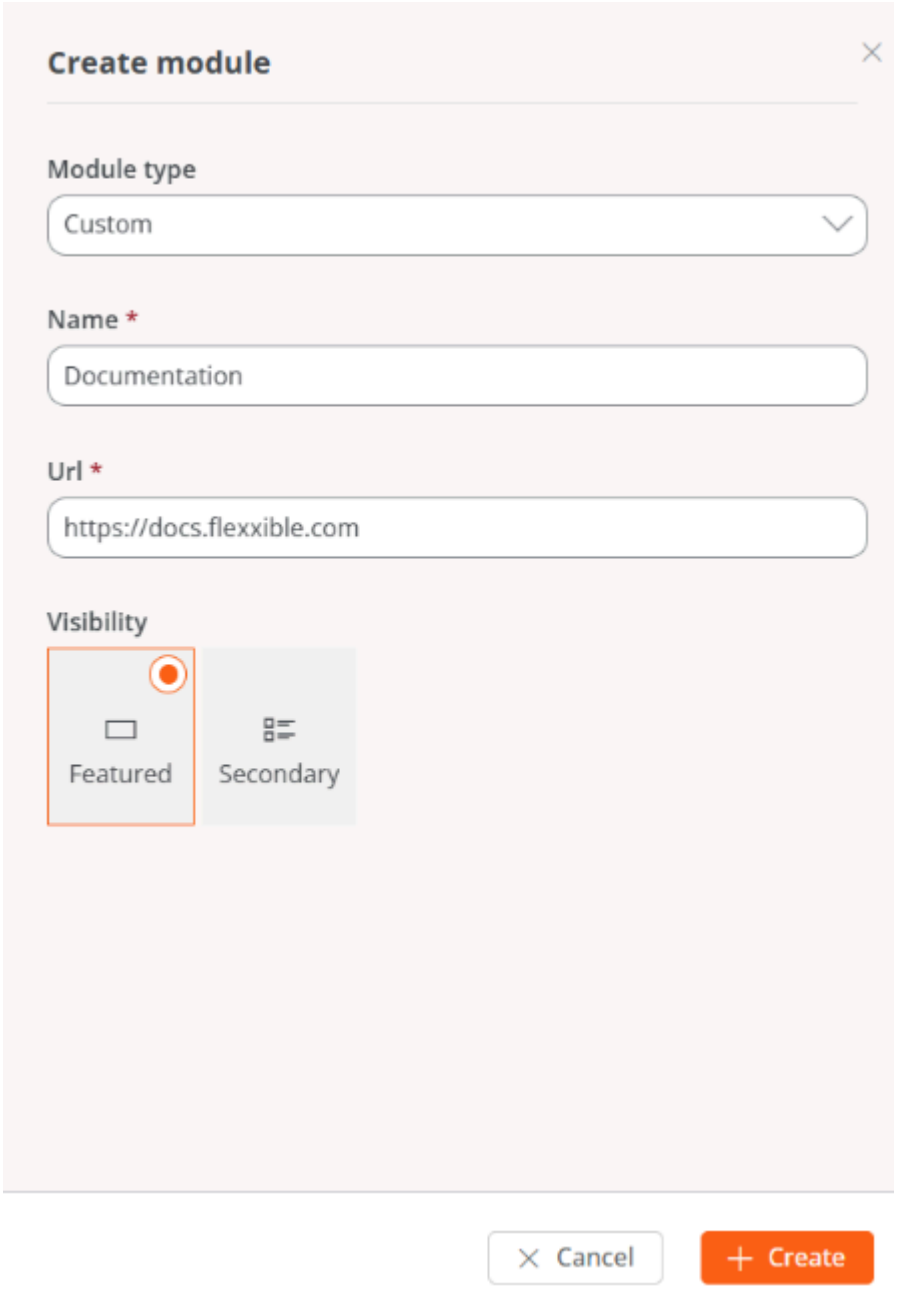
This tab shows a list of Flexxible product modules available for the organization, as well as those created by the users themselves.

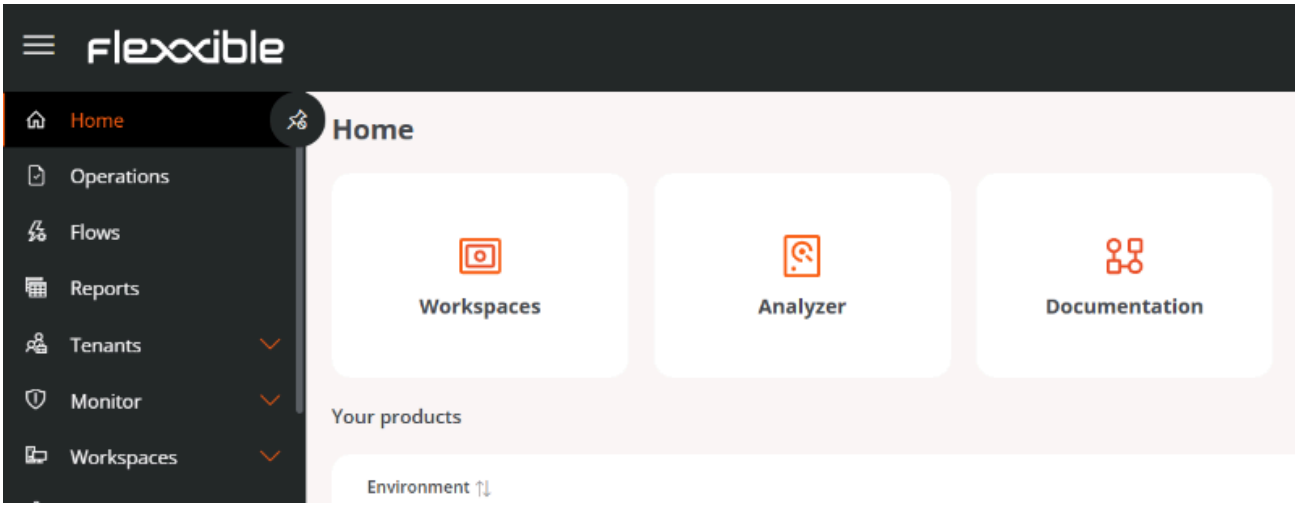


The table contains the module name, its corresponding URL, and its visibility level. From `See detail`, a label and URL can be assigned to the selected module, and you can define whether it is visible as *Featured* or *Secondary*. When it is featured, it appears among the main modules in the Home section of Portal; when it is secondary, it is shown as a list under the `View more` button.

Create module

The `New` button allows you to create custom modules to maximize the platform's utility. For example, in the images below, you can see how a module for Flexxible's documentation webpage has been created.



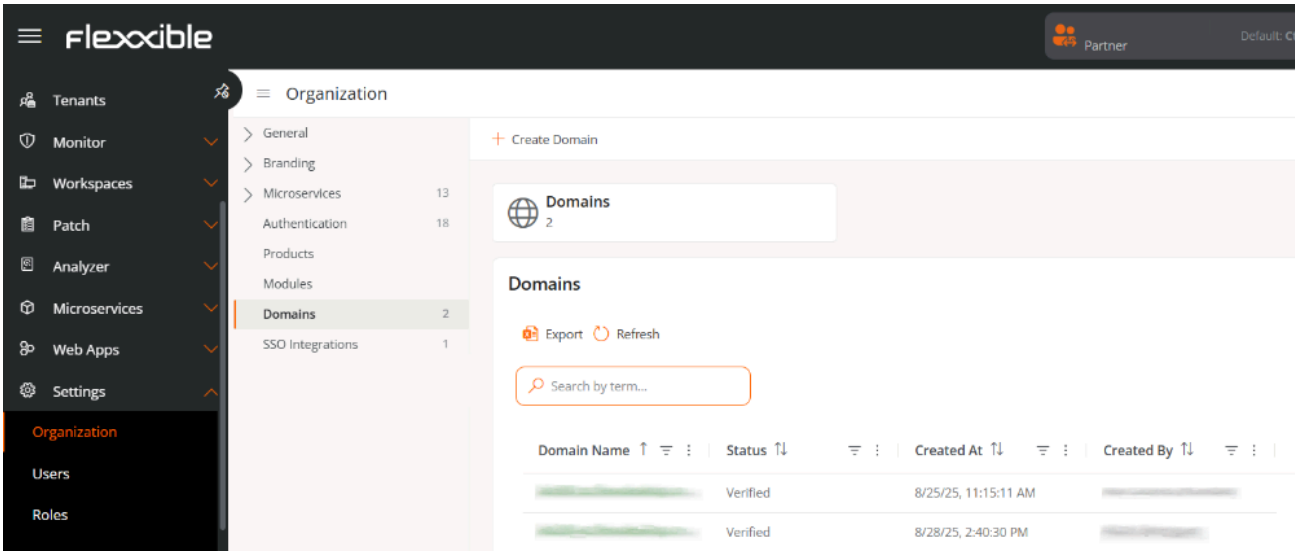


Domains

Portal allows you to configure login through SAML authentication, a single sign-on (SSO) technology that lets organizations connect their identity managers with the Flexxible platform.

To set up login with this method, you need to make adjustments related to recognizing the organization's domain and integrating with the identity manager used.

From this tab, an *Organization Administrator* can register and verify the domains to be used. You can also access the table with the domain list and consult its detail view.



The table shows the following information:

- **Domain name.** Web address registered by the organization.
- **Status.** *Verified* or *Not verified*.
- **Created on.** Domain creation date and time.
- **Created by.** User who registered the domain.

Create a domain

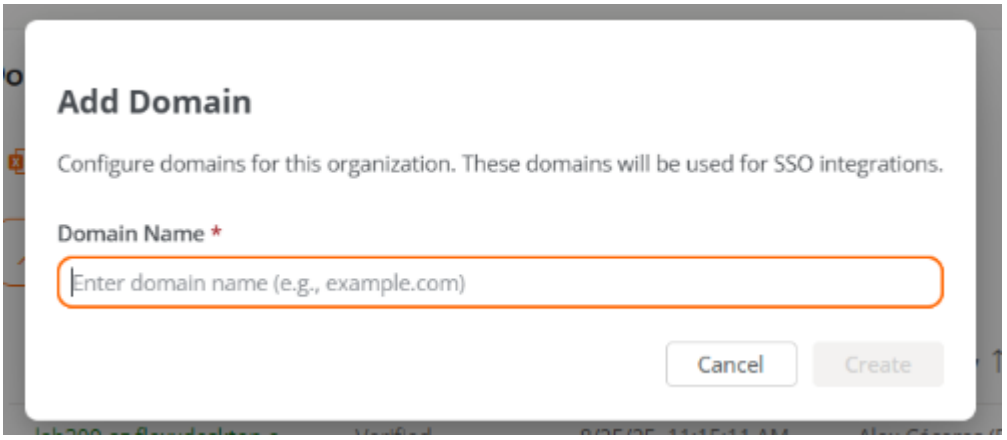
To configure a domain, it must first be registered and then verified.

1. Access `Portal` -> `Organization` ->

2. In the menu, select the `Domains` tab.

3. Click `Create domain`.

4. Enter the organization's domain (corresponding to the email of the users who will log in with SAML).



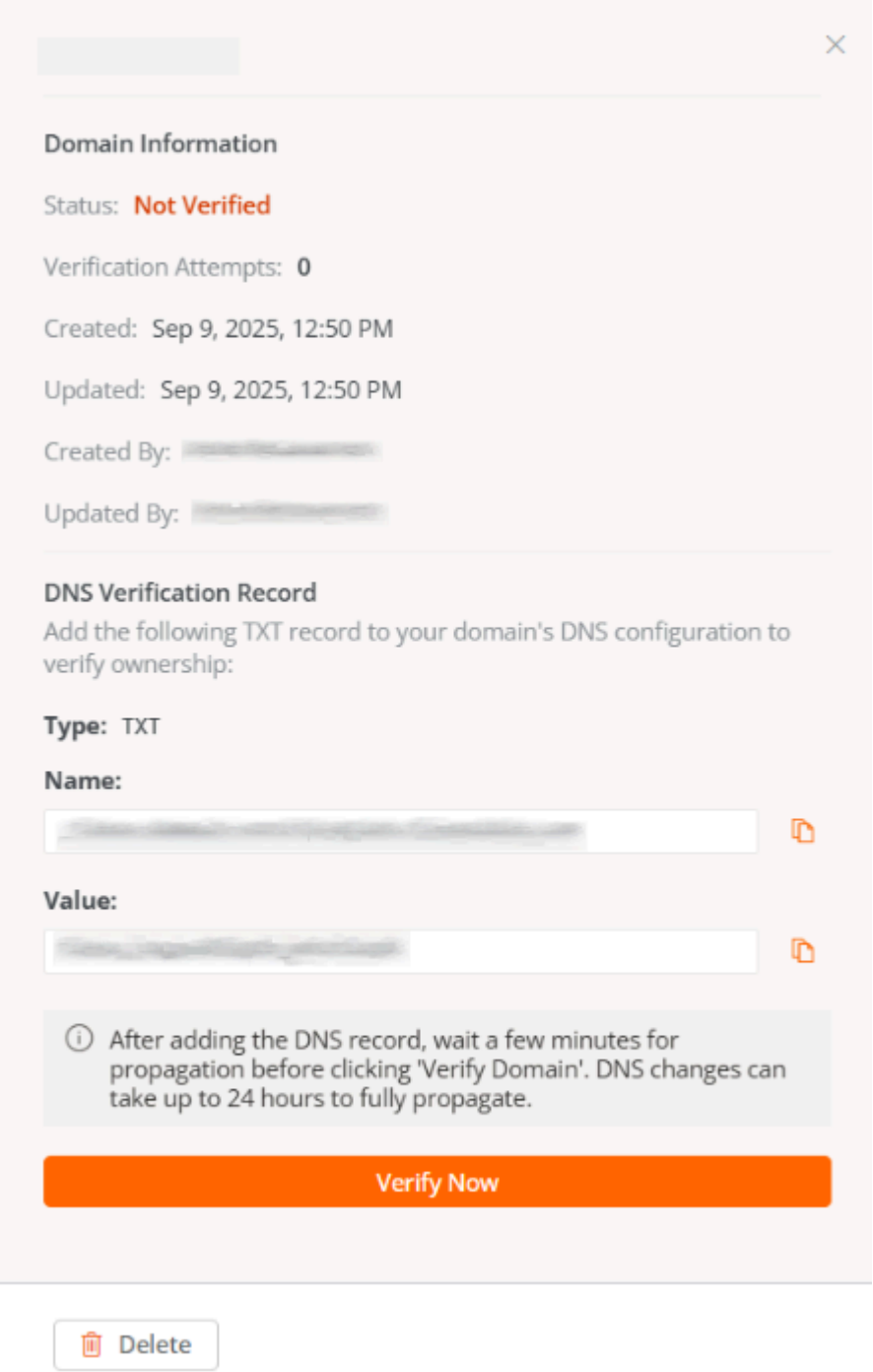
5. Click on `New`.

The domain will be added to the table with the status *Not verified*.

Verify the domain

1. In the Domains table, select the registered domain.

2. A window will appear with instructions to add a TXT record in DNS, necessary to verify ownership.



3. Click `Verify now` to complete the process.

Remove domain

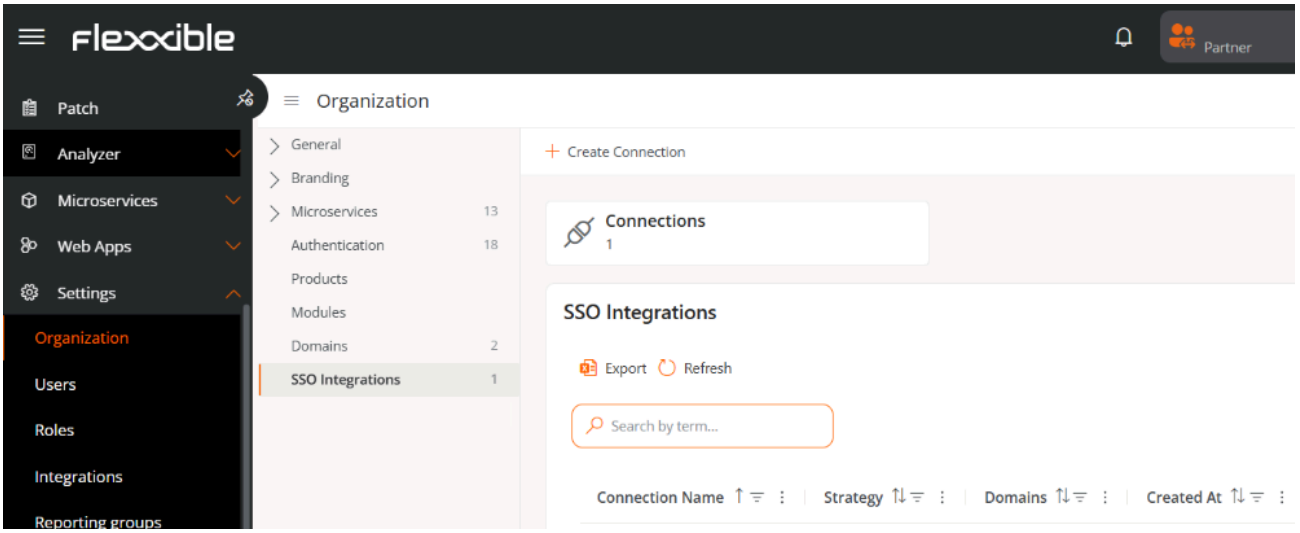
1. Access `Portal` -> `Organization`.
2. In the menu, select the `Domains` tab.
3. Select the domain in the table that you want to remove.

4. In the detail window, click `Remove`.

By removing a domain, users associated with it will no longer be able to authenticate via SAML until it is registered again.

SSO Integrations

SSO Integrations allow users with email addresses from specific domains to authenticate through the organization's identity provider.



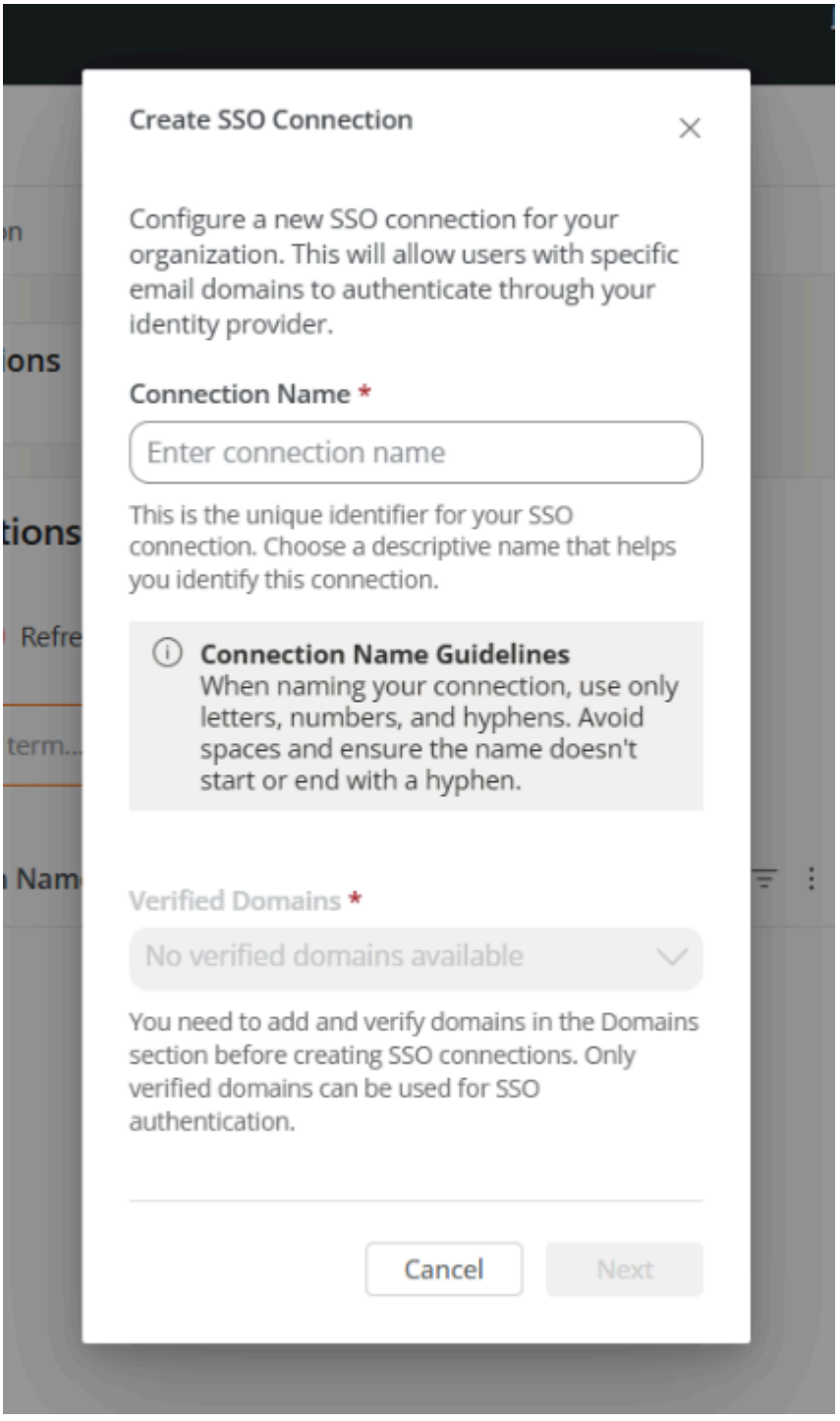
Create an SSO connection

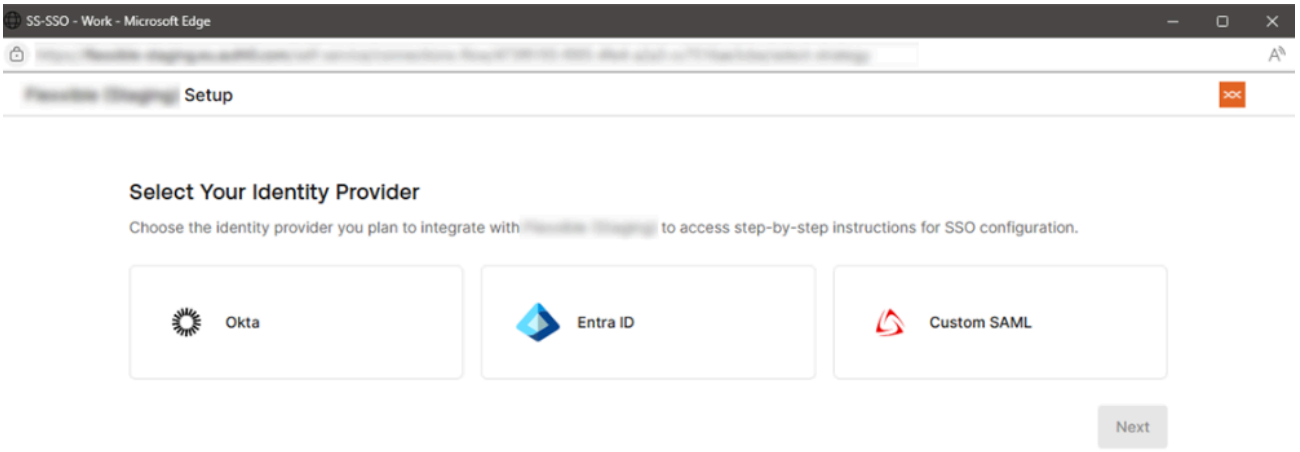
1. Access `Portal` -> `Organization`.
2. In the menu, select the `SSO Integrations` tab.
3. Click `Create connection` and follow the wizard instructions, which will guide the *Organization Administrator* through the setup and testing according to the identity manager used.

Available identity managers:

- Okta
- Entra ID
- Custom SAML

For each case, a wizard will guide you step by step in the specific setup within the selected identity manager.





TIP

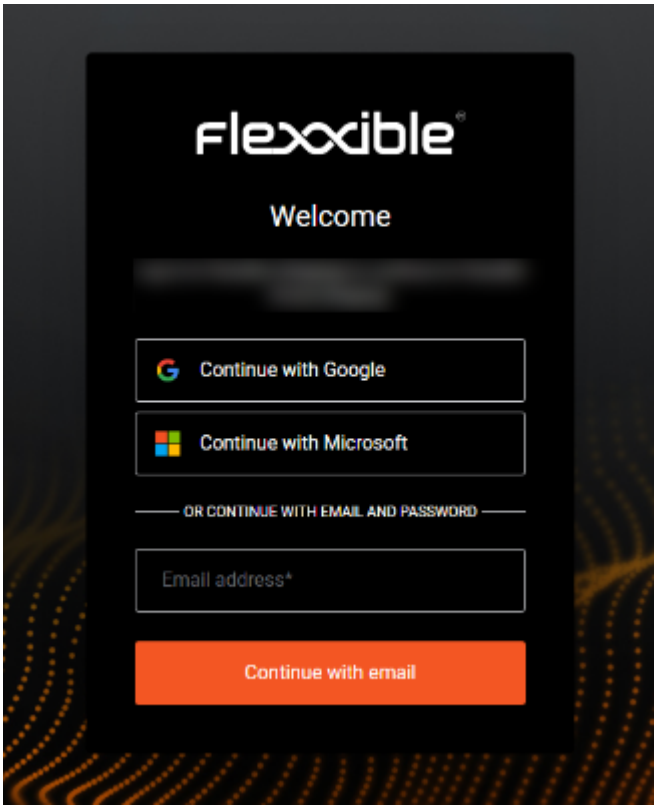
Some of the requested data during setup may have different names depending on the identity manager. For example, in Custom SAML:

- The `Single Sign-On URL` field may appear in the identity manager as `Reply URL (Assertion Consumer Service URL)`.
- The `Service Provider Entity ID` field may be called `Identifier (Entity ID)`.

NOTE

If any doubts arise during the setup process, please consult with your contact at Flexxible.

Once the process is completed, users from associated domains will be able to log in by entering their email address in the appropriate field and clicking `Continue with email`.

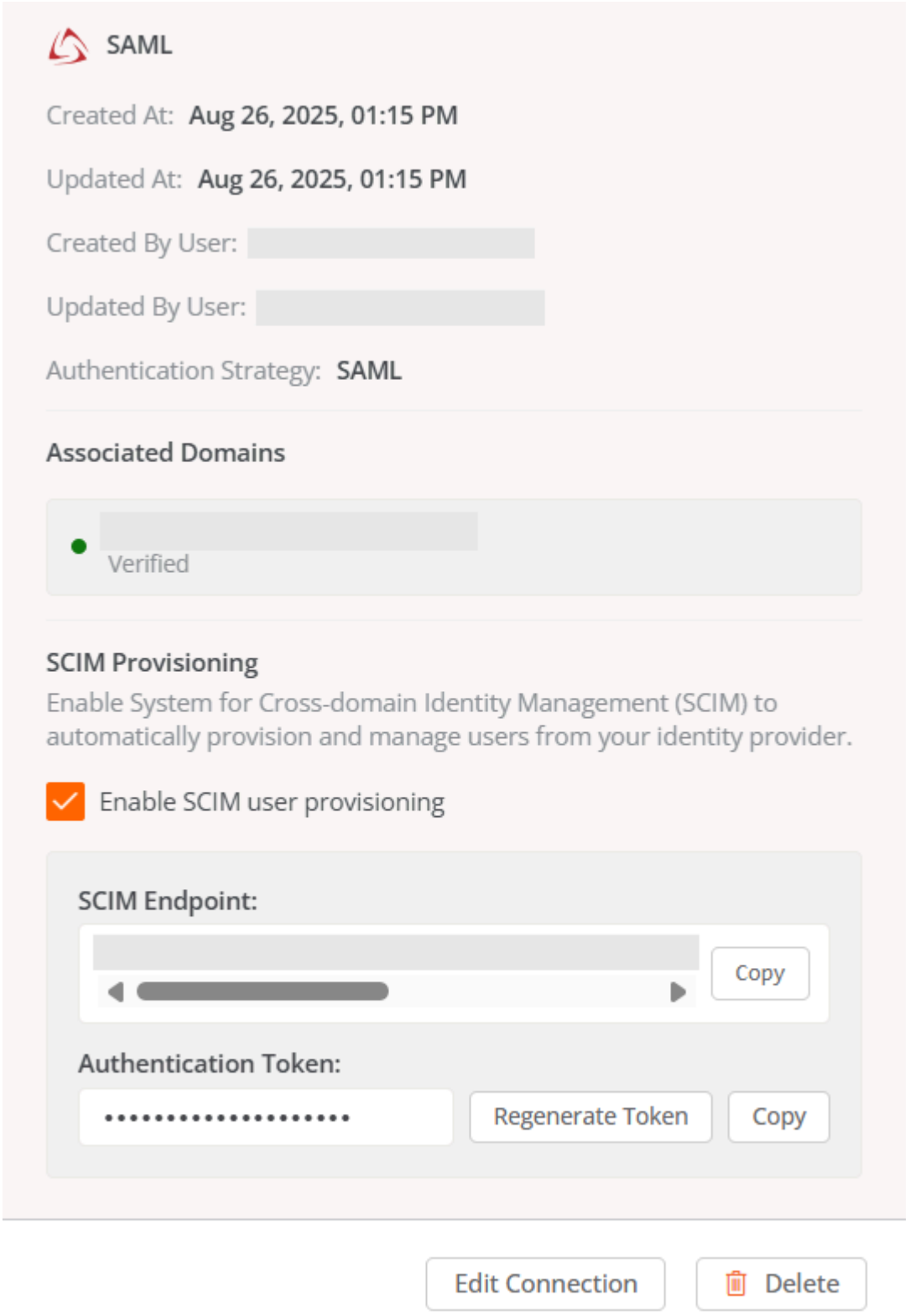


If the system recognizes the domain as enabled for SSO, it will redirect the user to the organization's identity manager for authentication.

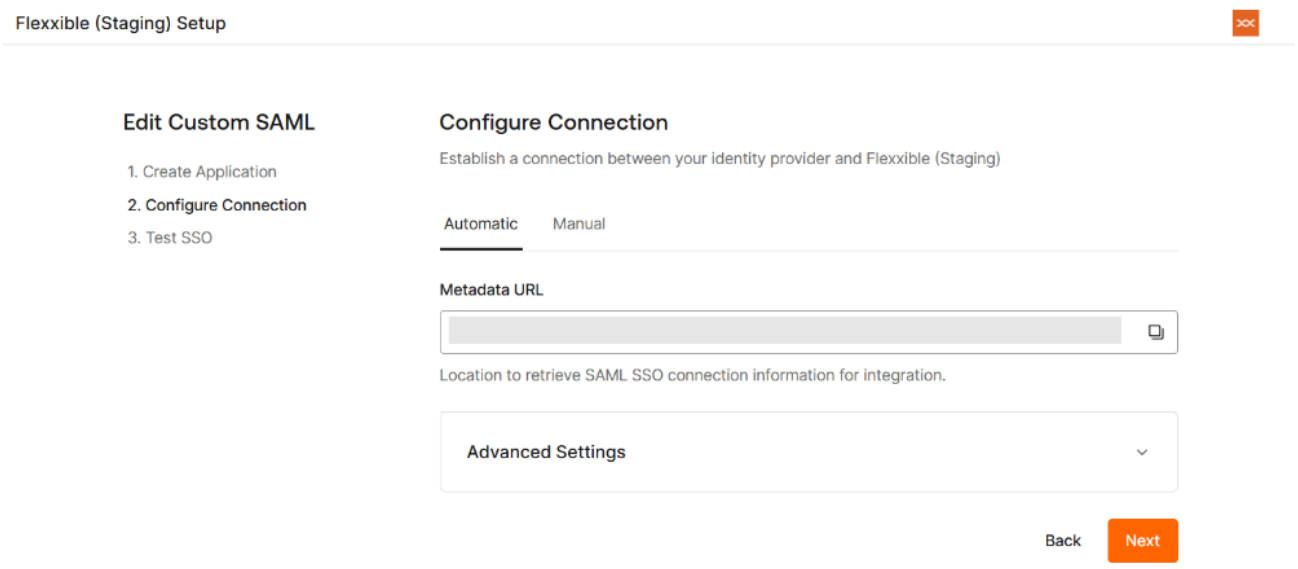
Edit an SSO connection

The platform allows editing an existing SSO connection either to update the configuration or renew the certificate in case of expiration.

1. Access `Portal` -> `Organization`.
2. In the menu, select the `SSO Integrations` tab.
3. Select a record in the table.
4. Click `Edit connection`.



Checking the `Enable SCIM user provisioning` checkbox is optional. More information in SCIM Provisioning.



Remove an SSO connection

1. Access `Portal` -> `Organization`.
2. In the menu, select the `SSO Integrations` tab.
3. Select the corresponding record in the table.

SCIM Provisioning

The System for Cross-domain Identity Management (SCIM) is a user provisioning and management standard that complements authentication with SAML. It is optional and automates the creation, update, and removal of user accounts in Portal, keeping information synchronized between the organization's identity manager (Okta, Entra ID, etc.) and the Flexxible platform.

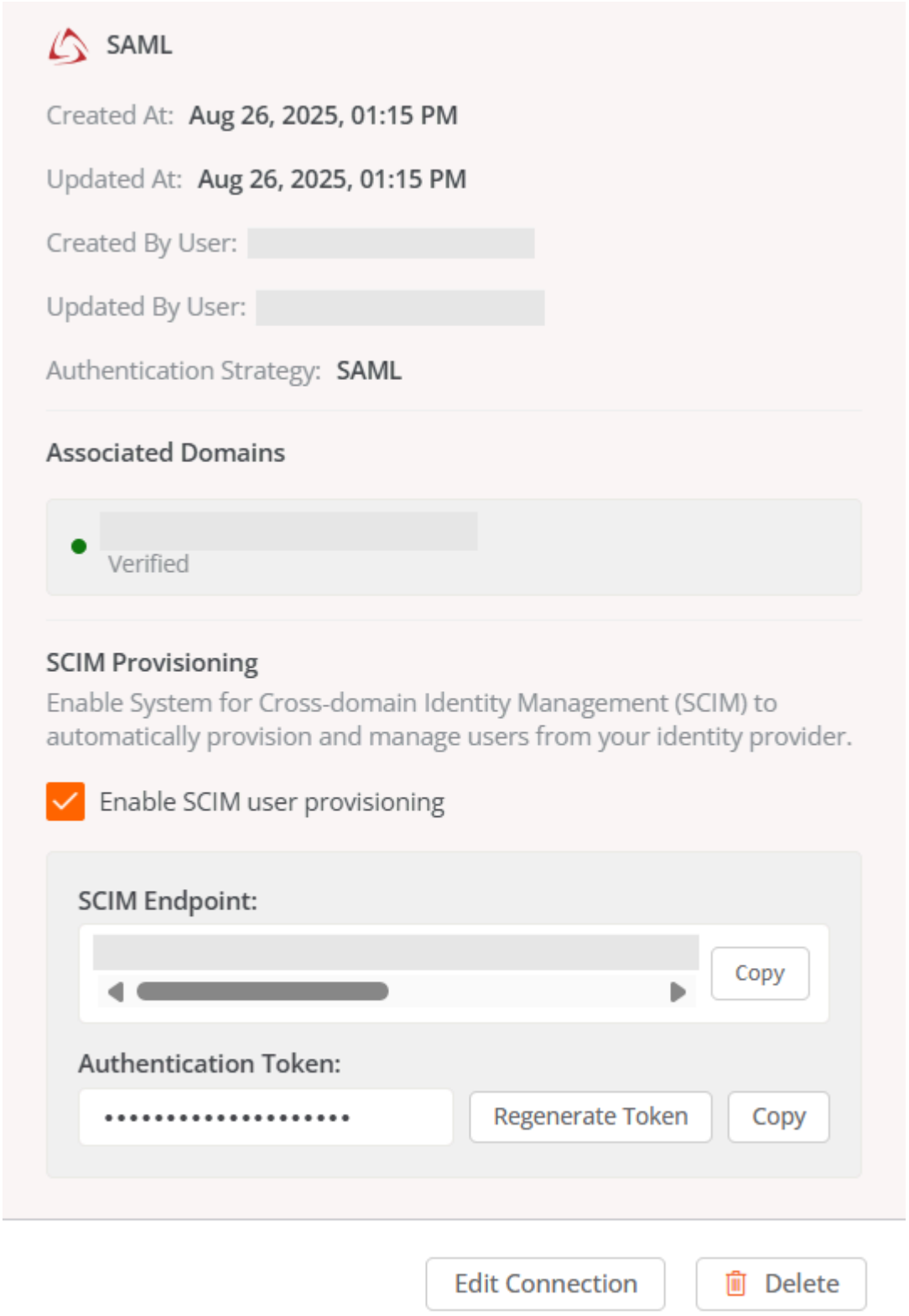
When SCIM is enabled, the identity manager can send basic user information (name, email, group) to Portal, simplifying account management. This way, the user's lifecycle in Portal is centrally controlled from the identity manager.

> **NOTE**
>
> The **SCIM Provisioning** tab will be visible after **creating user groups in the identity manager**.

Enable SCIM in Portal

To use SCIM, it is essential to have previously set up authentication with SAML:

1. Access `Portal` -> `Organization`.
2. In the menu, select the `SSO Integrations` tab.
3. In the table, select the corresponding SSO connection.
4. Check the `Enable SCIM user provisioning` option.



When the option is activated, the following will appear at the bottom of the configuration window:

- SCIM endpoint

- Authentication token

> **WARNING**
>
> These details are confidential and should be stored securely.

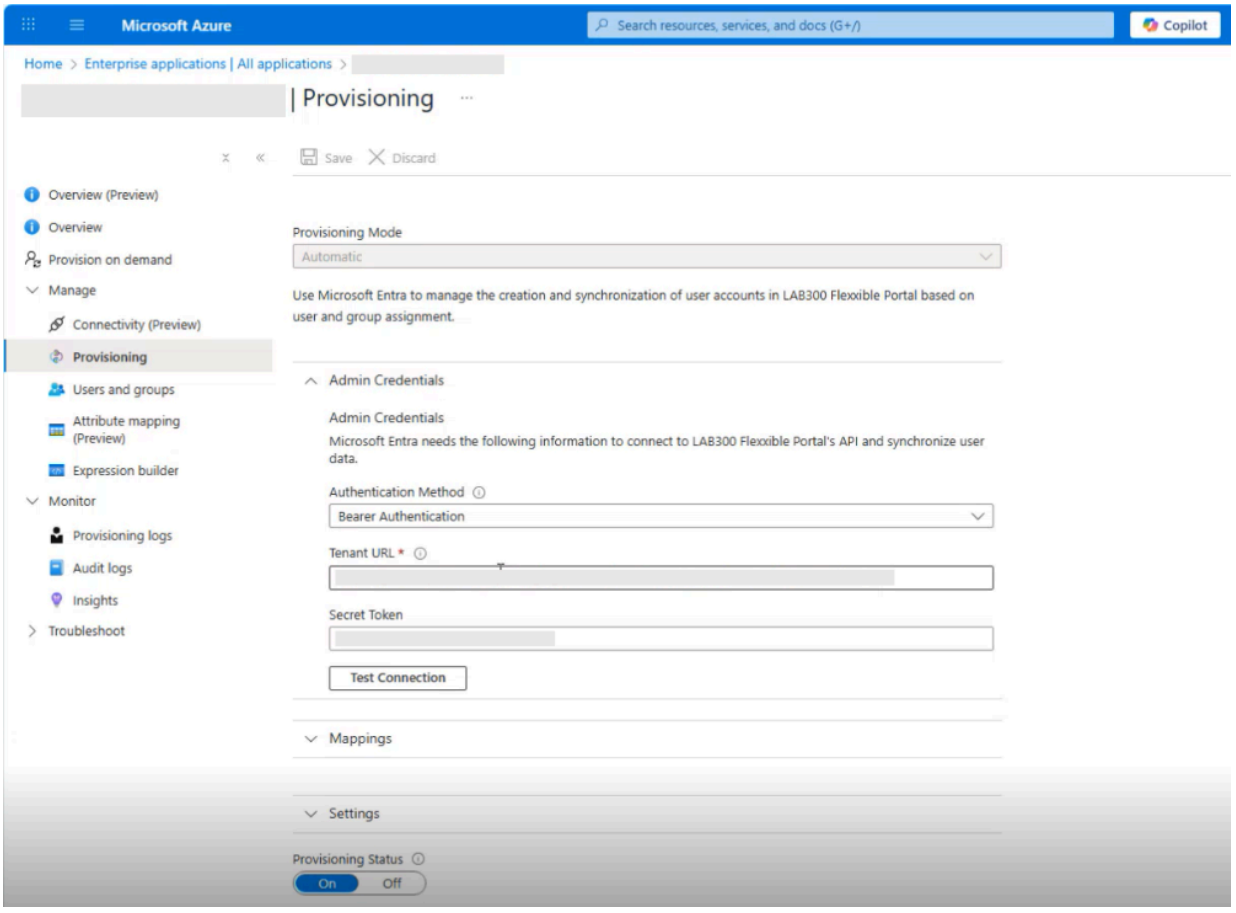
> **INFO**
>
> In environments with sub-organizations, the SCIM integration must be defined in the "parent" tenant.

Configure SCIM in the identity manager

In the organization's identity manager, enter the SCIM endpoint and authentication token provided in Portal.

Example with Entra ID:

1. Go to `Provisioning`.
2. Enter the SCIM endpoint and authentication token.
3. Select the authentication method: `Bearer token` or `Bearer Authentication`.
4. Click `Test connection` to validate synchronization.
5. Activate provisioning.



From that moment, the identity manager will start syncing groups and users to Portal.

> **INFO**
>
> - If **Okta** is used as the identity provider:
>   - The SCIM functionality has to be configured using the Custom SAML option, as Okta does not support SCIM when the connection is with OIDC.
>   - When configuring the Custom SAML connection, the **Application username format** must be specified as **Email**, otherwise users will not be able to authenticate.

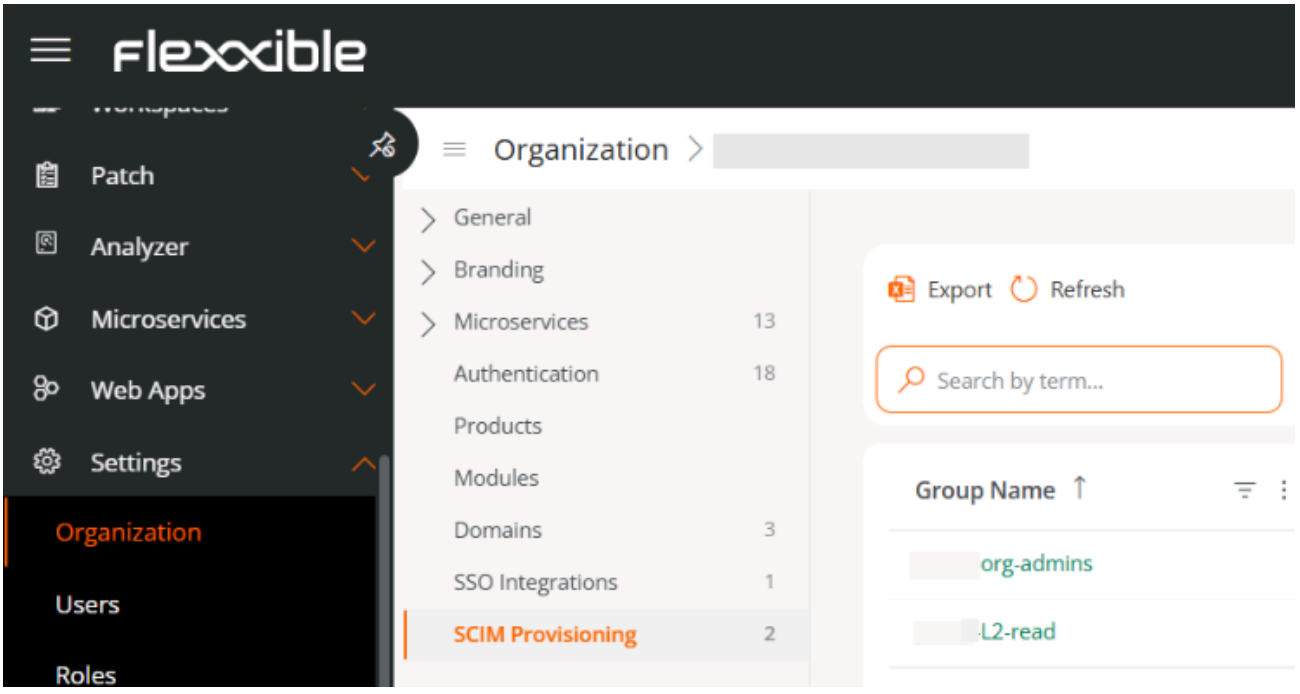
Create user groups in the identity manager

To integrate users via SCIM, it is essential to create groups in the identity manager.

Considerations

- Create groups specifically dedicated to Portal with clear and exclusive names (e.g. `MiOrg-Portal-L2`).
- When user groups are created or deleted in the identity manager, they will also be automatically created or deleted in Portal.
- Do not create nested groups.
- **A user should belong to only one group**; otherwise, unexpected behaviors may arise: in Portal a user cannot have more than one role.
- There cannot be users without an assigned group.
- Users belonging to a group without a linked role won't be visible in the Users list.

> **INFO**
>
> After creating user groups in the identity manager, the `SCIM Provisioning` tab will automatically appear in the menu.

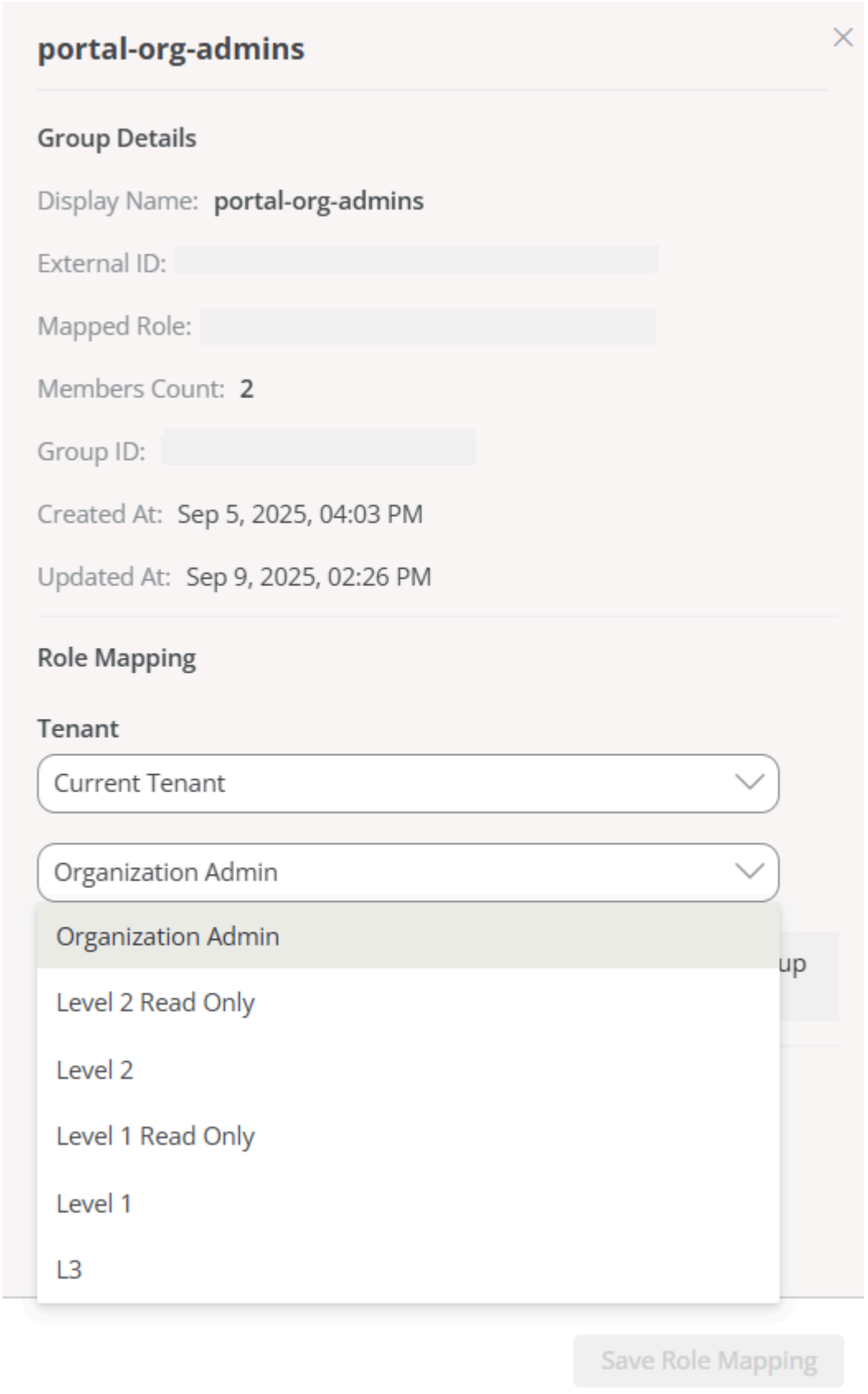


Role mapping in Portal

In the `SCIM Provisioning` tab table, you can see the groups created in the identity manager. This happens because a one-way synchronization has been established from the identity manager to Portal.

To map roles:

1. Access `Portal` -> `Organization`.
2. In the menu, select the `SCIM Provisioning` tab.
3. Select a synchronized group from the table.
4. In the modal window, assign the corresponding role.
5. If an organization (tenant) has sub-organizations, choose which sub-organization that group belongs to before assigning it a role.

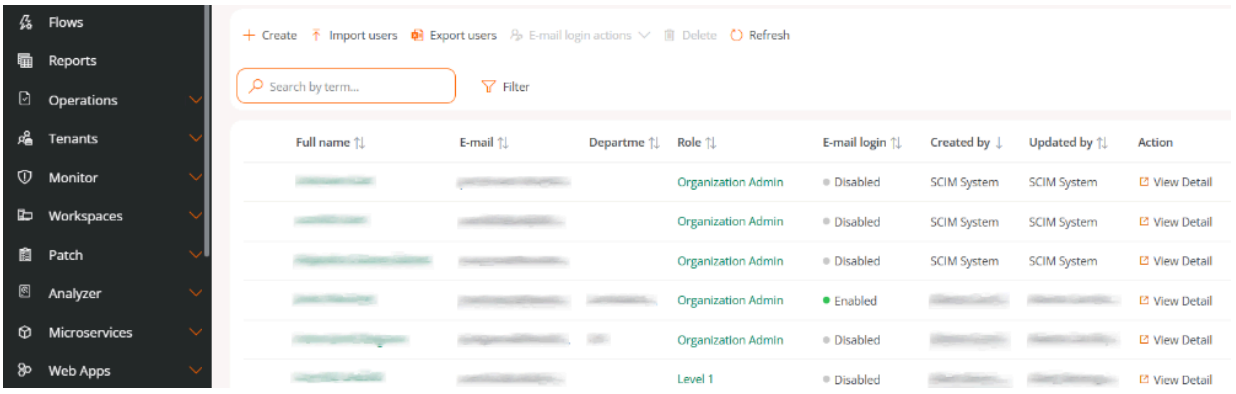


From the moment all groups are linked to a role, no further configurations will be needed. New users added or removed from groups in the identity manager will be automatically

synchronized in Portal.

Considerations about roles

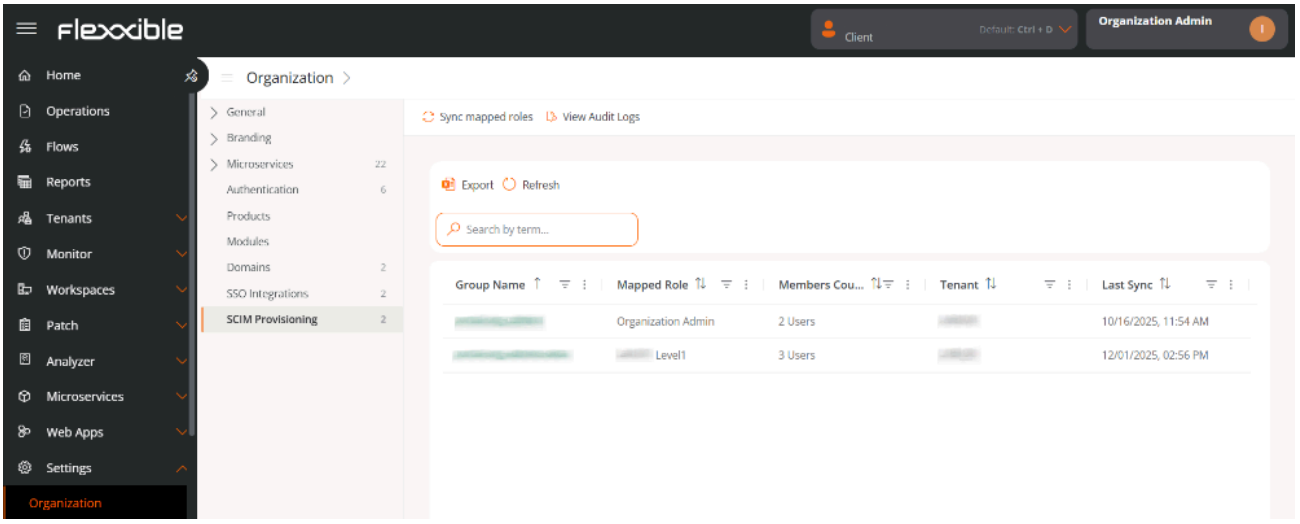
- Every synchronized group must have a role assigned to be visible and functional in Portal.
- The same role can be assigned to different groups.
- The role assigned to a group can be changed at any time by following the same steps used to assign the role.
- In the Users list, the columns *Created by* and *Updated by* will identify users managed by SCIM.

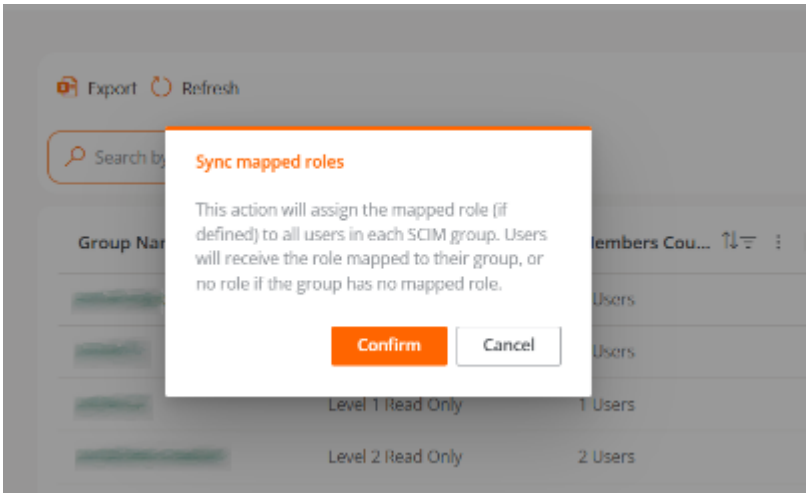


Role synchronization

The synchronization frequency depends on the identity manager used (for example, Entra ID synchronizes every 40 minutes), although manual synchronization can be forced from the identity manager itself for tests or urgent changes without waiting for the automatic cycle.

To avoid relying on those intervals, Portal includes the `Sync assigned roles` button, which allows aligning user roles belonging to groups created with SCIM.



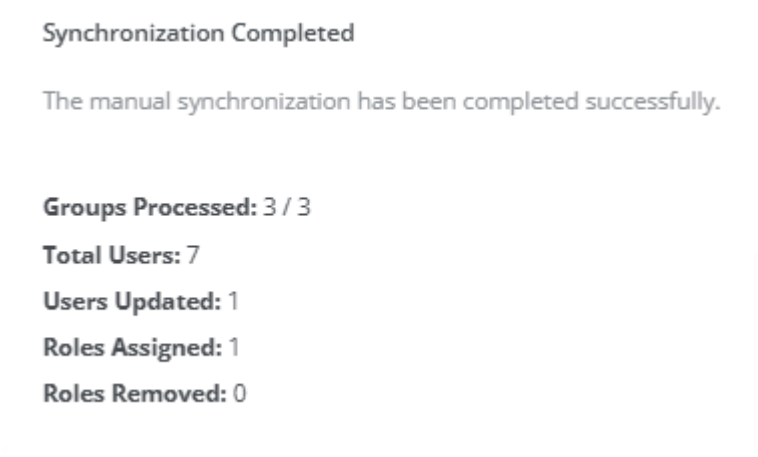


This action performs the following operations:

- Reviews all users belonging to groups created via SCIM.
- Checks if the role assigned to each user matches the role mapped for their group.
- If discrepancies are detected, it automatically updates the user's role.

If the role belongs to another sub-organization, the user will automatically move to the corresponding sub-organization.

At the end of the process, a detailed summary of the modified data is displayed.

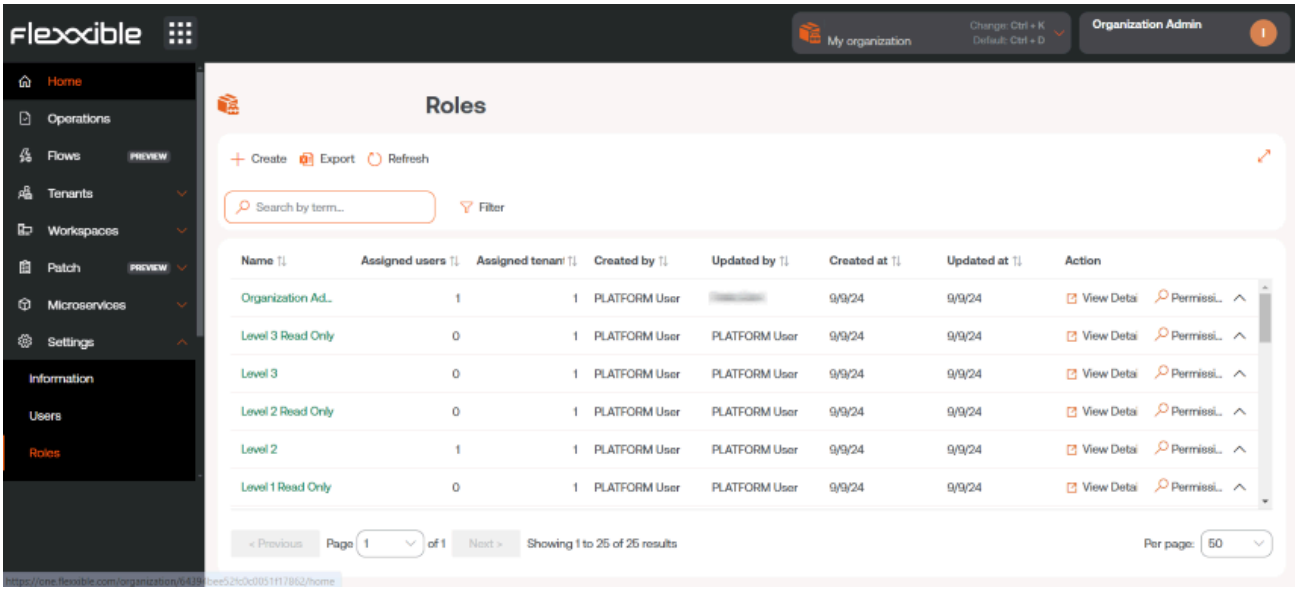


INFO

It is not necessary to execute the `Sync assigned roles` action regularly. It is recommended to use it only when making a change to mapped roles.

Portal / Settings / Roles

Roles allow the segmentation of access to organization information or different platform functionalities, according to the user logged in and the role 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.

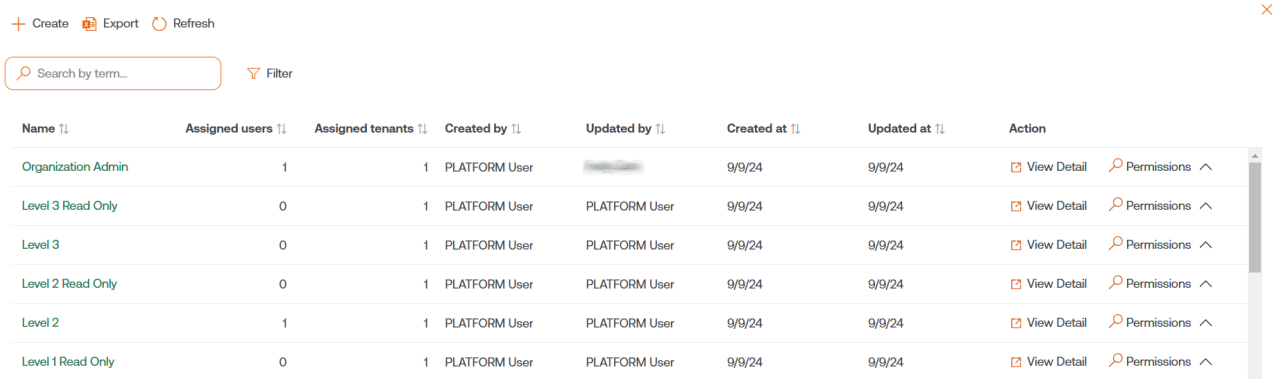
Roles table

The roles table displays the following information:

- **Name.** Name assigned to the role.
- **Assigned users.** Users who have this role assigned.
- **Assigned tenants.** Tenants who have this role assigned.
- **Created by.** User who created the role.
- **Updated by.** User who updated the role information.
- **Created on.** Role creation date.
- **Updated on.** Role update date.
- **Action.** Allows access to `View details` and `Permissions`.

Roles Subtable

If you click on the arrow to the right of `Permissions`, a sub-table will appear where you can access direct information about the permissions that this role has been assigned in Portal and in the Workspaces and Analyzer modules, as well as the tenants that have been assigned this permission.



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

You can consult the visibility details and allowed operations at each level in Access Levels

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

You can consult the visibility details and allowed operations at each level in Access Levels

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 default role configurations affect all the reporting groups of 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, these should be included as a new entry in the `Permissions` tab, in two formats:

- **All tenants.** Allows setting a unified level of access and visibility for all organizations under the root organization.
- **Individually.** Allows setting 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 the Workspaces module, such as providing remote support, sending microservices, power actions, or querying 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 additionally restricts access to the Workspaces module to visibility only, allowing information consultation 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 provides access to the Workspaces module at Level 2, which includes all Level 1 support functionalities plus Level 2 functionalities, among which are server, network, location management, wifi networks, and alert configuration. Allows access to Portal as a user and also access to the Analyzer module to query application or device inventory information, 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 additionally restricts access to the Workspaces module to visibility only, allowing information consultation 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. Allows full visibility in the Analyzer module, all Level 2 actions in the Workspaces module, and the ability to modify organization properties in Portal, including the creation and activation of microservices or flows, update policies, and more.

Portal / Settings / Roles / Access levels

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

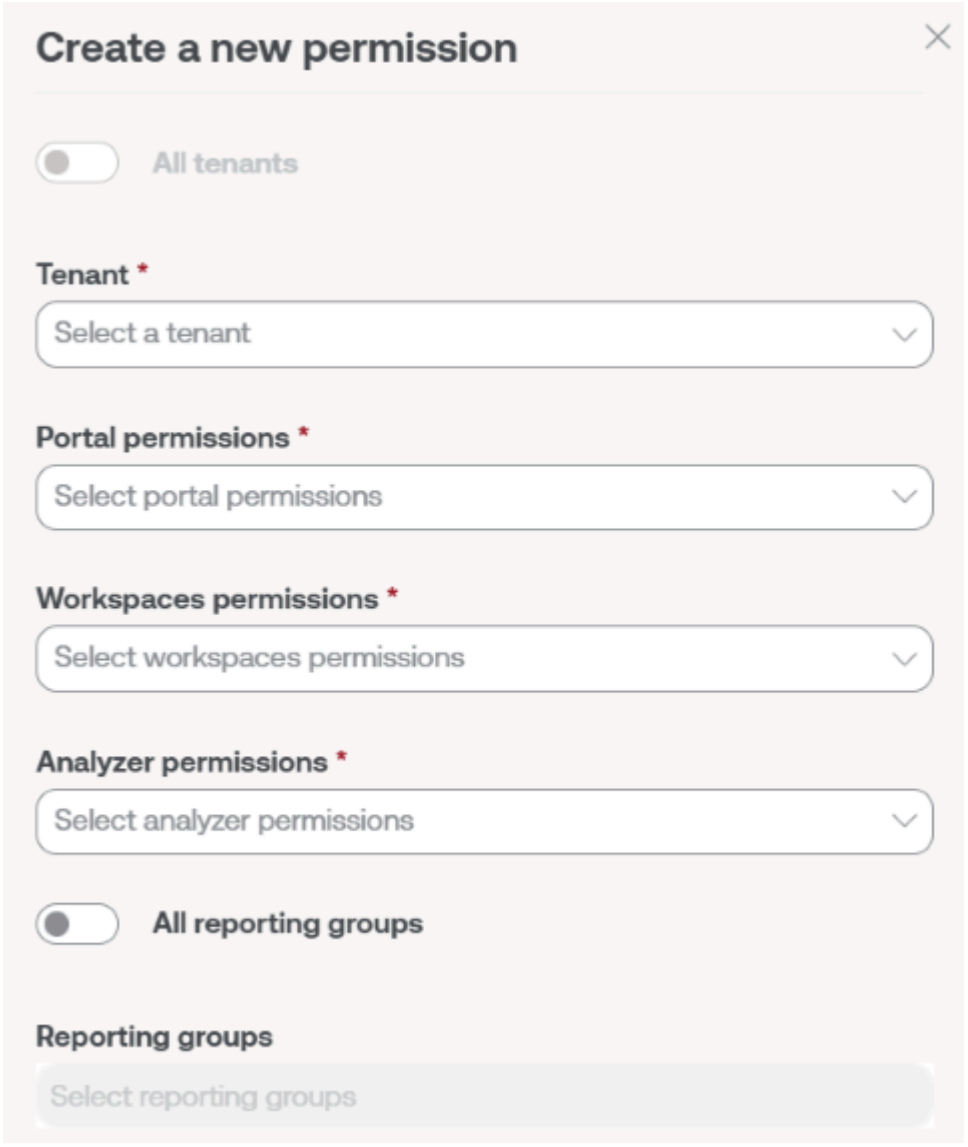
The roles of an organization allow configuring access and visibility for the users of the organization, and also allow including the permissions to configure access and visibility to dependent organizations.

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

The following roles are distinguished in Portal:

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 Level 1 or Level 2 role.

These role levels allow configuring visibility and segmented access according to the needs of each organization. The details of the visibility and actions available for each Portal access level are defined in the table below:

Section	Functionality	Action	1	2	3	4	5	6	
Home		Read	✅	✅	✅	✅	✅	✅	✅
Operations		Read	✅	✅	⭐	✅	✅	✅	✅
Flows		Read	✅	✅	⭐	❌	❌	❌	❌
		Create	✅	❌	⭐⭐	❌	❌	❌	❌
		Update	✅	❌	⭐⭐	❌	❌	❌	❌
		Delete	✅	❌	⭐⭐	❌	❌	❌	❌
Reports	List	Read	✅	✅	❌	✅	✅	✅	✅
	Detail	Read	✅	✅	❌	✅	✅	✅	✅

Section	Functionality	Action	1	2	3	4	5	6	
		Create	✅	❌	❌	❌	❌	❌	❌
		Delete	✅	❌	❌	❌	❌	❌	❌
	Settings	Update	✅	❌	❌	❌	❌	❌	❌
Tenants		Create	✅	❌	❌	❌	❌	❌	❌
		Read	✅	✅	❌	❌	❌	❌	❌
		Update	✅	❌	❌	❌	❌	❌	❌
		Delete	✅	❌	❌	❌	❌	❌	❌
	Activation	Read	✅	✅	❌	❌	❌	❌	❌
Monitor	Active alerts	Read	✅	✅	✅	✅	✅	✅	✅
	Alert Configuration	Create	✅	❌	❌	❌	❌	❌	❌
		Read	✅	✅	✅	❌	❌	❌	❌
		Update	✅	❌	❌	❌	❌	❌	❌
		Delete	✅	❌	❌	❌	❌	❌	❌
Workspaces		Read	✅	✅	⭐	✅	✅	✅	✅
		Update	✅	❌	✅	✅	❌	✅	❌
	Workspace Groups	Read	✅	✅	⭐	✅	✅	✅	✅

Section	Functionality	Action	1	2	3	4	5	6	
		Create	✅	❌	❌	❌	❌	✅	❌
		Update	✅	❌	❌	✅	❌	✅	❌
		Delete	✅	❌	❌	❌	❌	✅	❌
Patch		Read	✅	✅	⭐	❌	❌	❌	❌
		Create	✅	❌	⭐⭐	❌	❌	❌	❌
		Update	✅	❌	⭐⭐	❌	❌	❌	❌
		Delete	✅	❌	⭐⭐	❌	❌	❌	❌
Analyzer	Installed apps	Read	✅	✅	✅	❌	❌	✅	✅
		Update	✅	❌	✅	❌	❌	✅	❌
	Licenses	Read	✅	✅	❌	❌	❌	✅	✅
		Create	✅	❌	❌	❌	❌	✅	❌
		Update	✅	❌	❌	❌	❌	✅	❌
		Delete	✅	❌	❌	❌	❌	✅	❌
	SAM	Read	✅	✅	❌	❌	❌	✅	✅
Microservices		Create	✅	❌	❌	❌	❌	✅	❌
		Read	✅	✅	✅	❌	❌	✅	✅

Section	Functionality	Action	1	2	3	4	5	6	
		Update	✅	❌	❌	❌	❌	✅	❌
	Enabled	Read	✅	✅	✅	❌	❌	✅	✅
		Update	✅	❌	❌	❌	❌	✅	❌
Billing		Read	✅	✅	❌	❌	❌	❌	❌
		Update	✅	❌	❌	❌	❌	❌	❌
Product		Read	✅	✅	❌	❌	❌	❌	❌
	Report	Read	✅	✅	✅	❌	❌	❌	❌
	Environment	Read	✅	✅	✅	❌	❌	❌	❌
		Update	✅	❌	❌	❌	❌	❌	❌
	Baseline	Read	✅	✅	✅	❌	❌	❌	❌
	FlexxAgent Configuration	Read	✅	✅	❌	❌	❌	❌	❌
		Update	✅	❌	❌	❌	❌	❌	❌
Integrations		Create	✅	❌	❌	❌	❌	❌	❌
		Read	✅	✅	❌	❌	❌	❌	❌
		Update	✅	❌	❌	❌	❌	❌	❌
Modules		Create	✅	❌	❌	❌	❌	❌	❌

Section	Functionality	Action	1	2	3	4	5	6	
		Read	✅	✅	❌	❌	❌	❌	❌
		Update	✅	❌	❌	❌	❌	❌	❌
Information		Read	✅	✅	✅	❌	❌	✅	✅
		Update	✅	❌	❌	❌	❌	❌	❌
Directives		Create	✅	❌	❌	❌	❌	❌	❌
		Read	✅	✅	✅	❌	❌	❌	❌
		Update	✅	❌	❌	❌	❌	❌	❌
		Delete	✅	❌	❌	❌	❌	❌	❌
Reporting Groups		Create	✅	❌	❌	❌	❌	❌	❌
		Read	✅	✅	❌	❌	❌	❌	❌
		Update	✅	❌	❌	❌	❌	❌	❌
		Delete	✅	❌	❌	❌	❌	❌	❌
	FlexxAgent Configuration	Read	✅	✅	❌	❌	❌	❌	❌
		Update	✅	❌	❌	❌	❌	❌	❌
	Automatic Update	Update	✅	❌	❌	❌	❌	❌	❌

Section	Functionality	Action	1	2	3	4	5	6	
	FlexxAgent version	Read	✅	✅	❌	❌	❌	❌	❌
		Update	✅	❌	❌	❌	❌	❌	❌
	Magic link	Create	✅	❌	❌	❌	❌	❌	❌
		Read	✅	✅	❌	❌	❌	❌	❌
		Update	✅	❌	❌	❌	❌	❌	❌
Roles		Create	✅	❌	❌	❌	❌	❌	❌
		Read	✅	✅	❌	❌	❌	✅	✅
		Update	✅	❌	❌	❌	❌	❌	❌
		Delete	✅	❌	❌	❌	❌	❌	❌
Users		Create	✅	❌	❌	❌	❌	❌	❌
		Read	✅	✅	❌	❌	❌	✅	✅
		Update	✅	❌	❌	❌	❌	❌	❌
		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 access levels 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	✅	❌	✅	❌
Alert	View	✅	✅	✅	✅
Alert	Off	✅	❌	✅	❌
Profile Storage	View	✅	✅	✅	✅
Profile Storage	Update	✅	❌	✅	❌
Profile Storage	Delete	✅	❌	✅	❌
Alert notification profiles	View	❌	❌	✅	✅
Alert notification profiles	Update	❌	❌	✅	❌
Alert notification profiles	Delete	❌	❌	✅	❌

Functionality	Action	L1	L1 RO	L2	L2 RO
Alert Subscriptions	View	✗	✗	✓	✓
Alert Subscriptions	Update	✗	✗	✓	✗
Alert Subscriptions	Delete	✗	✗	✓	✗
Event Logs	View	✗	✗	✓	✓
Event Logs	Update	✗	✗	✓	✗
Event Logs	Delete	✗	✗	✓	✗
Locations	View	✗	✗	✓	✓
Locations	Create	✗	✗	✓	✗
Locations	Update	✗	✗	✓	✗
Networks	View	✗	✗	✓	✓
Networks	Update	✗	✗	✓	✗
Notifications	View	✗	✗	✓	✓
Notifications	Create	✗	✗	✓	✗
Notifications	Update	✗	✗	✓	✗
Notifications	Delete	✗	✗	✓	✗
Reporting Groups	View	✗	✗	✓	✓
Servers	View	✗	✗	✓	✓

Functionality	Action	L1	L1 RO	L2	L2 RO
Servers	Execute operations	❌	❌	✅	❌
WiFi Networks	View	❌	❌	✅	✅
WiFi Networks	Update	❌	❌	✅	❌

INFO

- ✅ Has access.
- ❌ No access.

Analyzer

The Analyzer module does not allow modifications to the organization or its devices, nor does it segment the functionalities it contains.

Therefore, there are two options:

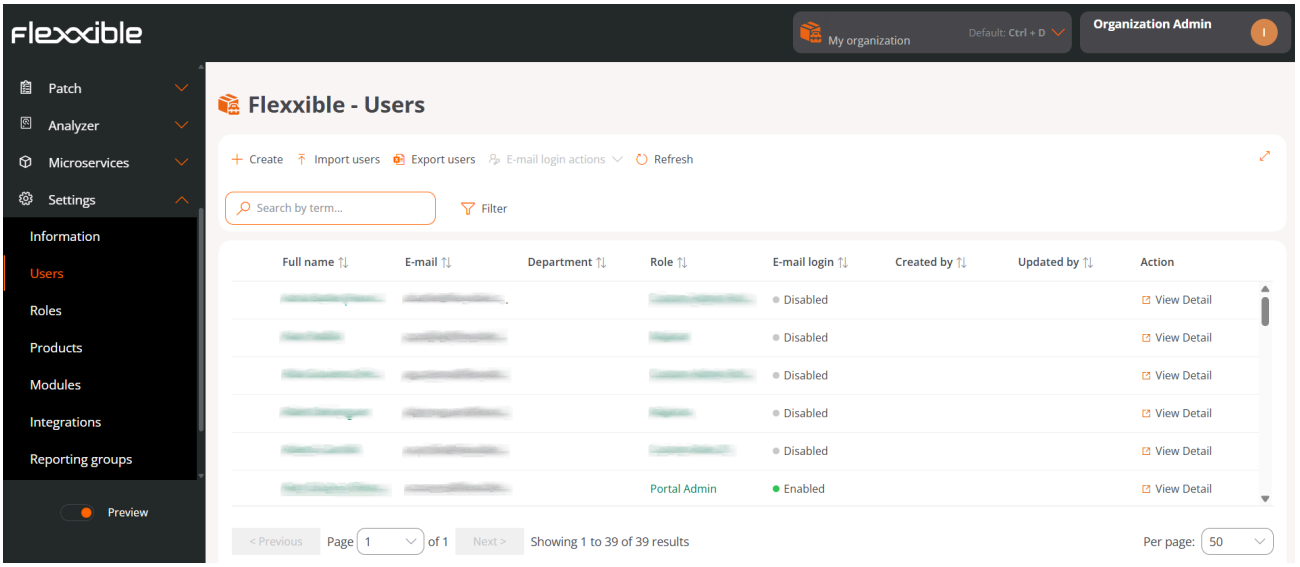
- You have access.
- You don't have access.

Portal / Settings / Users

User management can be done from `Portal` -> `Settings` -> `Users`. From there, you can view, modify, create, or delete users, as well as assign them a role.

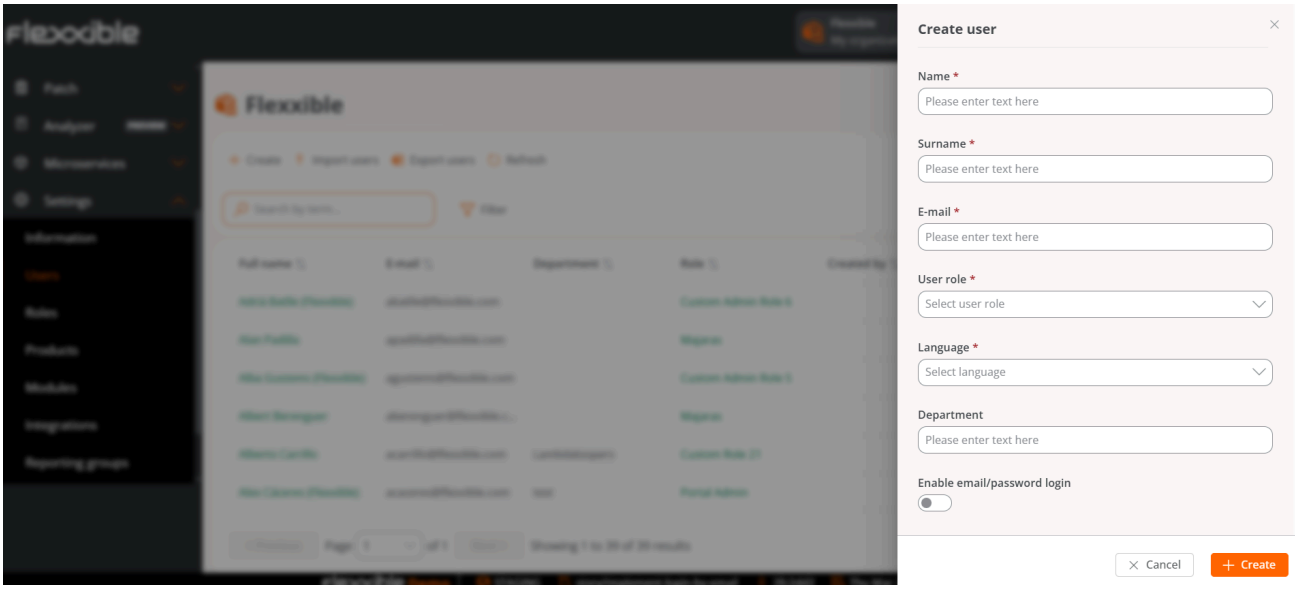
The table shows a list of all the users of an organization. Each row provides the following information:

- **Full name.** User's first and last name.
- **Email address.** 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* email and password login to Flexxible consoles.
- **Created by.** Name of the person who created the user.
- **Updated by.** Name and email address of the last user who updated the user's information in the Portal.
- **View details.** Opens a form to edit the user's data or even delete it, depending on the assigned role in the Portal.



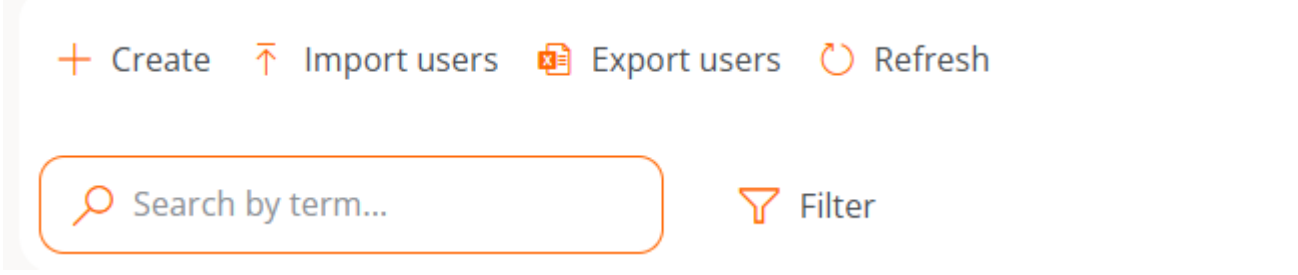
Create users

In the list view, the `New` button will open a window with a form to fill out the fields with the information of a new user. In addition to the first name, last name, and email address, you must assign a user role which grants access to the Portal; as well as the language to use the console and the department to which the user belongs within the organization.



Create a batch 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're looking to do a bulk import, Flexxible recommends first doing an export to get the Excel file with the correct format. From there you only need to complete it with the required changes, and finally import it.



Export users

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 users of the organization and their respective data.

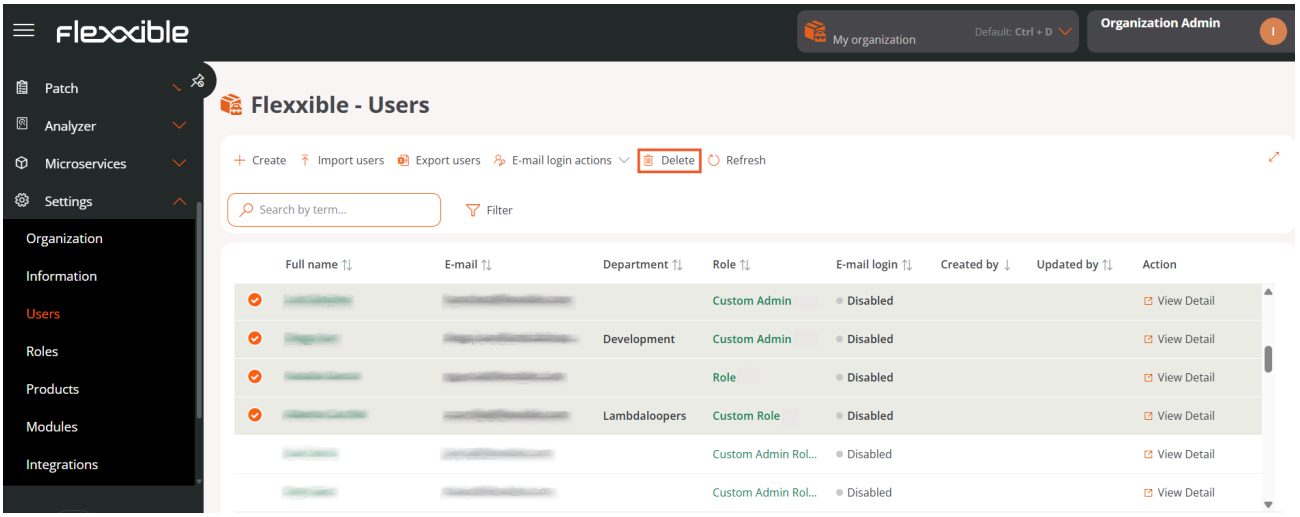
Delete users

To delete a user:

1. Go to `Portal` -> `Settings` -> `Users`
2. In the table, click `View detail`.

To delete a batch of users:

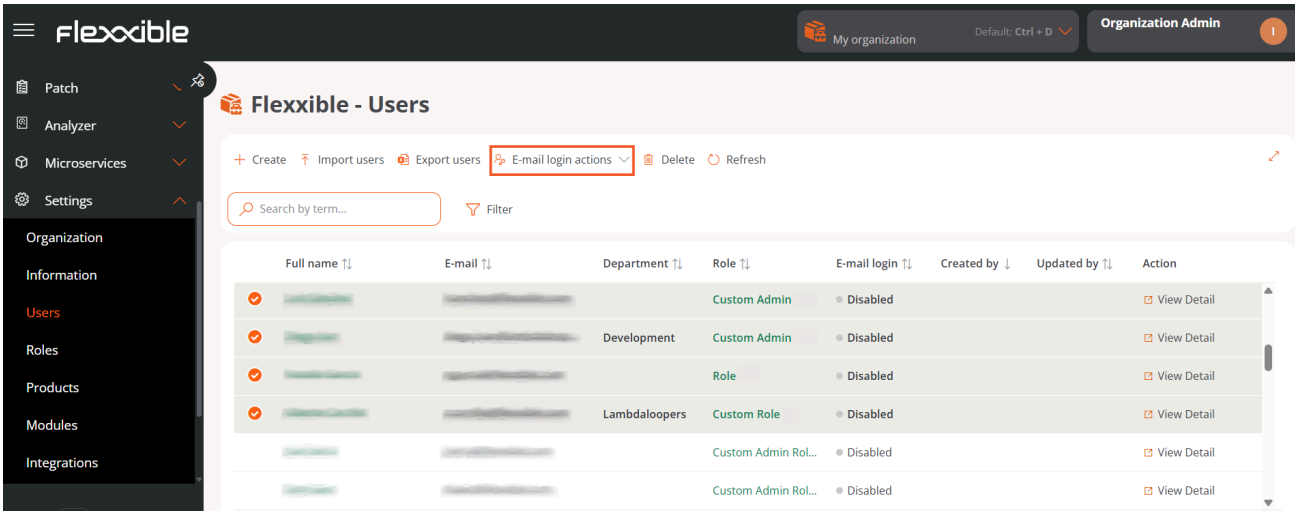
1. Go to `Portal` -> `Settings` -> `Users`
2. Select the users you want to remove.
3. In the top menu, the `Delete` button will be enabled.
4. Click `Delete`.



Email login actions

Users with the *Organization Admin* permission can enable email and password login for the organization's users.

> **INFO**
>
> For more information, please consult the Access and authentication documentation.



Additional options

The options menu in the list view also allows you to `Reload the table`, which is very useful when you want to refresh 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 / Integrations

From **Integrations**, it's possible to integrate Portal with services that organizations have on external platforms to simplify the management of tasks on the devices, view unified information, or perform various actions.

Integration with Entra ID

The integration of Portal with Entra ID allows treating an organization's devices as just another group of devices; in this way, besides the dynamic and static workspace groups an organization might have, Entra ID workspace groups would be generated.

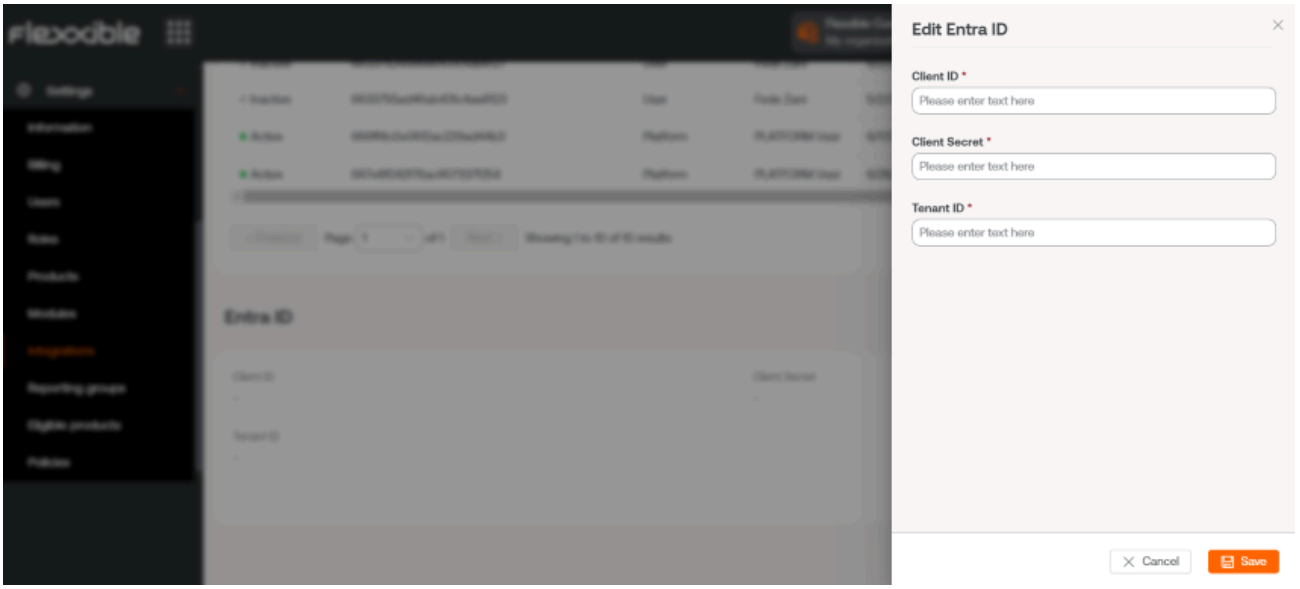
Integration does not imply that these groups will exist in Portal, but when any action on them is desired in the Workspaces module, Portal will display the list of devices that comprise it to make a decision.

Enable 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. Log on to `Portal`.
3. Go to `Settings` -> `Integrations` -> `Entra ID`.
4. Click on `Edit` and enter the following information:

- **Id. of application (client).** Client ID. This can be obtained from the Azure registration panel.
- **Secret string.** Client secret (key) used for authentication. This can be obtained from the Azure registration panel.
- **Id. directory (tenant).** This is the Azure tenant ID. You can obtain it here.

5. Click on `Save`.
6. Click on `Check` to verify that the integration has been registered correctly.



TIP

For more information about this feature, please check the Set up integration with Entra ID guide.

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 with Intel vPro Enterprise has been designed to be completely automated and transparent for the user, without the need for manual actions or additional infrastructure deployment. It helps reduce incident resolution times and enables support scenarios that previously required physical intervention on devices.

The integration of Flexxible with Intel vPro® Enterprise allows you to perform useful additional manageability operations on the physical Windows workspaces that provide support to Intel AMT® technology, including:

- Schedule power on and off actions using defined schedules.
- Turn on the device over the internet, including advanced options like direct boot to BIOS or loading an ISO image during startup, for example, for system reinstallation tasks.

- Access to out-of-band KVM sessions to view and interact with the device screen even when the operating system hasn't loaded.

Features

- Does not require the implementation of a dedicated Intel® EMA server since this functionality is integrated into the backend of the platform, segmented and instantiated individually for each client.
- Simple activation from the console using an *Enable* or *Disable* switch.
- Upon activation, a compatibility diagnostic process is automatically initiated on the organization's devices.
- Compatible devices are ready to confirm activation with a single click.

From the Intel vPro section in Portal, you can check detailed information about the hardware and status of devices, as well as perform additional operations, including out-of-band actions.

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.

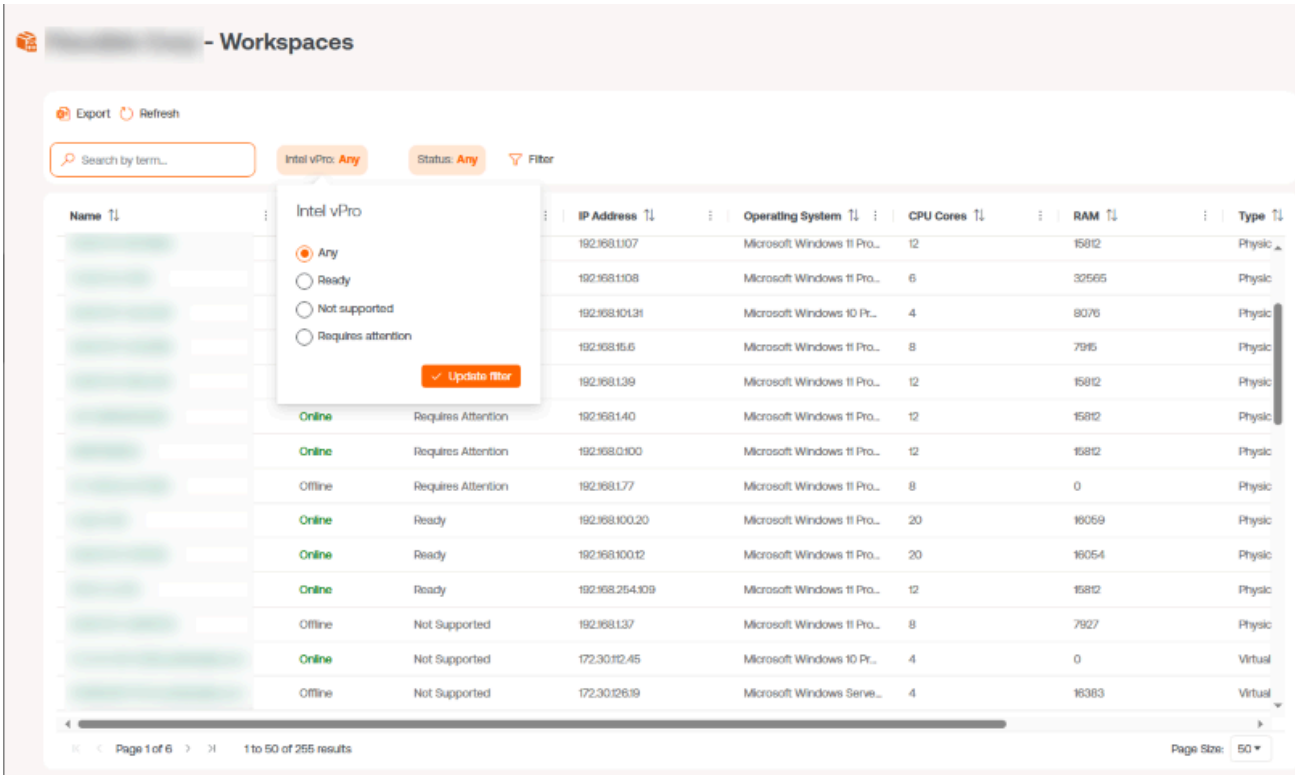
Compatibility with Intel® AMT

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 device does not support Intel® AMT, so it will not benefit from integration with Intel vPro® Enterprise.
- **Requires attention.** The device supports Intel® AMT technology, but Intel® EMA Agent has not been installed. Please check the Intel EMA Agent section below to see how to proceed.
- **Ready.** The device supports Intel® AMT technology, and 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. Consult 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

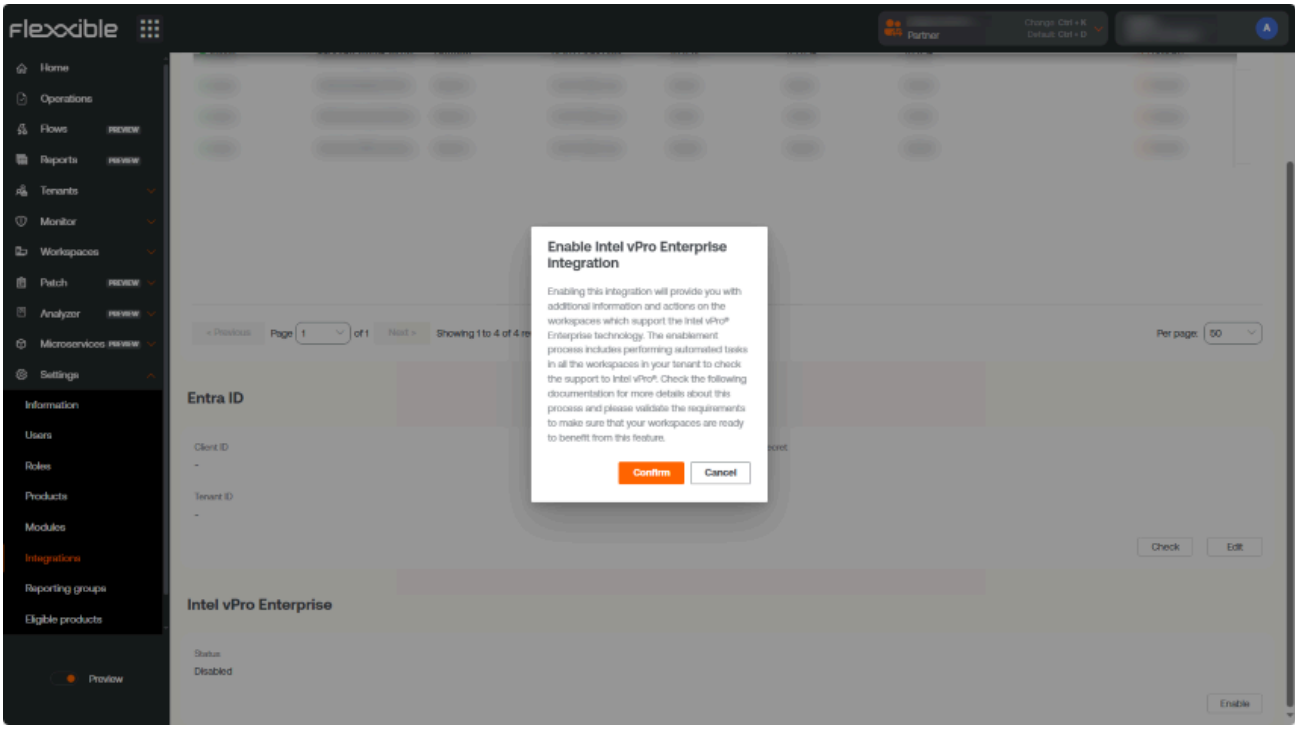
In addition to the FlexxAgent's communication requirements, devices must have a Client Initiated Remote Access (CIRA), a key component of Intel Endpoint Management Assistant. To make sure this connection is available, the following must be verified:

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. Make sure the server is accessible from the device through port 443.
3. That traffic between the device and the server is allowed by the proxy server, if applicable.

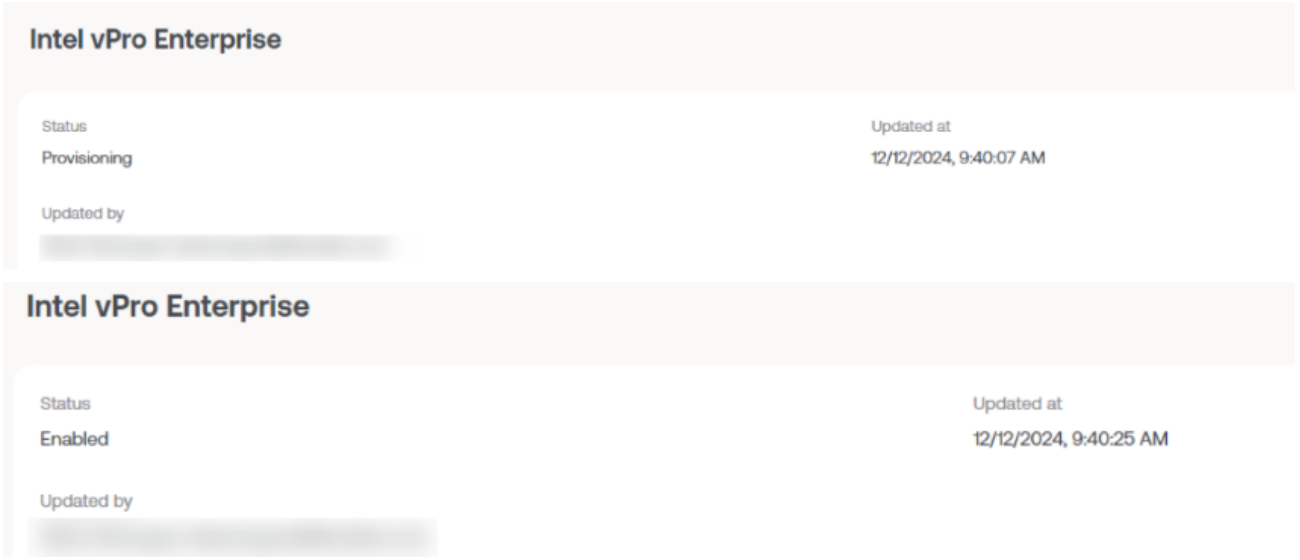
Enable integration with Intel vPro® Enterprise

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` -> `Intel vPro Enterprise`.
3. Click on `Enable`.
4. A window with information about the integration and a confirmation request will appear. Click on `Confirm`.

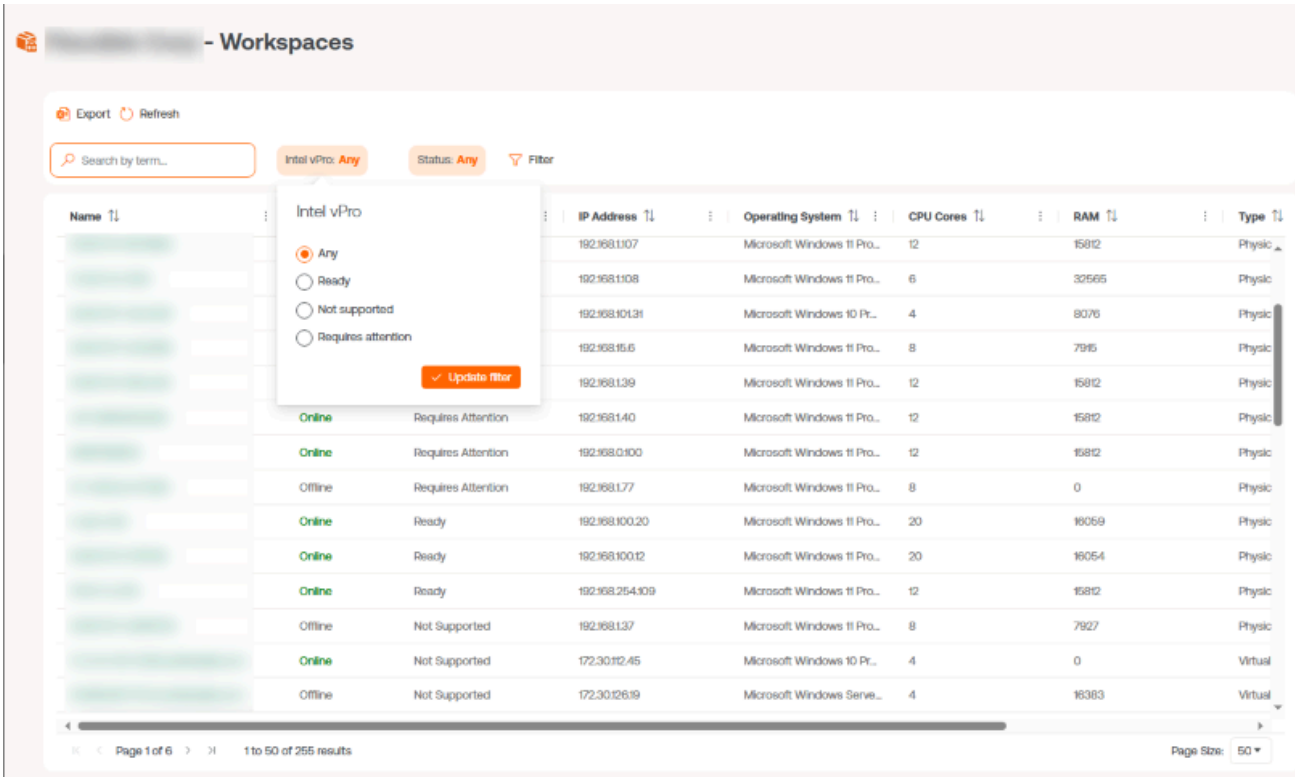


The integration process may take a few minutes to provision and configure the tenant. When completed, the status will show as `Enabled` along with related information.



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.

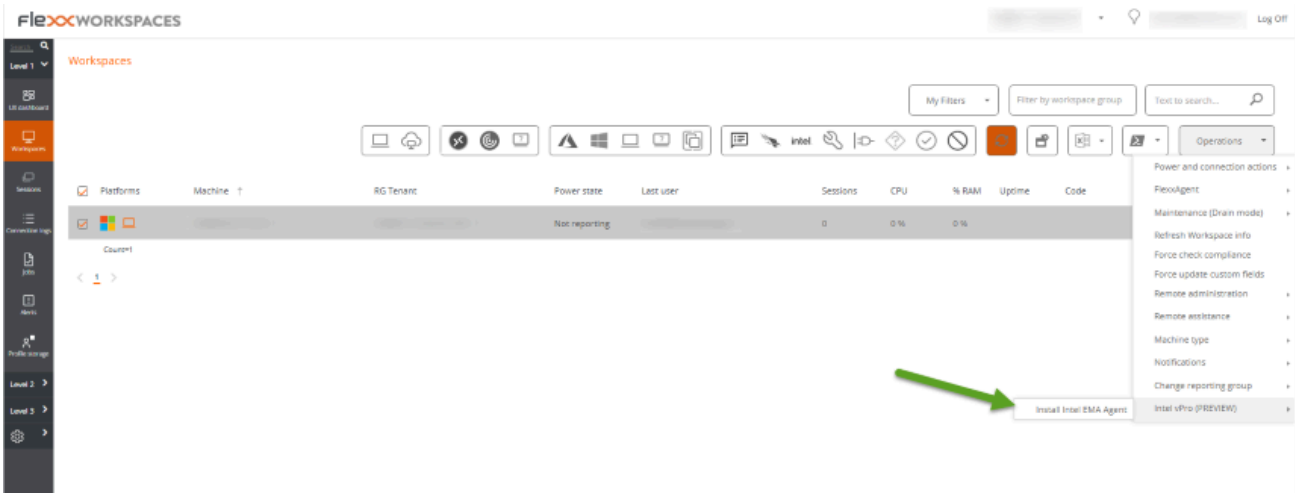
Go to the Workspaces section and check the information in the *Intel vPro Enterprise* column. You can also filter the devices by the field value to easily find which ones support Intel® AMT technology.



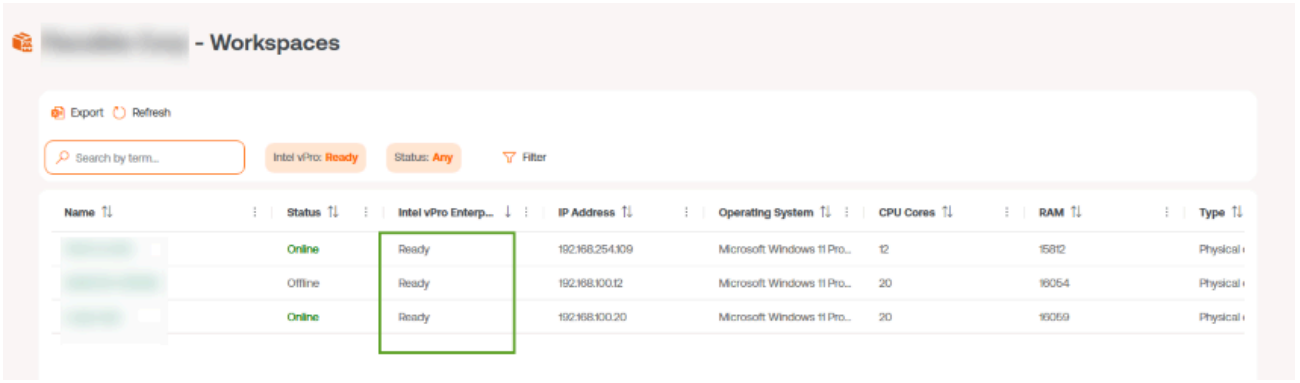
Install Intel EMA Agent on devices that indicate support for Intel® AMT (in the `Intel vPro Enterprise` column of Workspaces, they are labeled as `Requires attention`).

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)

Security integrations

Integration with antivirus and EDR solutions provides first-level support with direct visibility into the security status of devices, without needing to access security consoles, which are usually reserved for more specialized profiles.

These integrations display the following information in real-time:

- Installed antivirus, including its version, operational status, and the CPU and memory consumption of its agent on the device.
- Installed EDR, including its version, operational status, and the CPU and memory consumption of its agent on the device.
- Active security detections, which allow the support agent to correctly assess the priority of an incident when a user reports anomalous behavior on the device.

Access to this information facilitates the differentiation between a performance issue and an incident that also involves an active security threat, speeding up decision-making and incident response.

> **NOTE**
>
> All security alerts and statuses are displayed in the **Security** section of the detailed view of each device.

In the device detail view, you can find support tools, remote assistance, management, and monitoring. This allows immediate prioritization and agile escalation when endpoint security is compromised.

CrowdStrike

CrowdStrike is a cloud-based cybersecurity platform that protects devices, identities, and data against advanced threats. Integration with Flexxible allows FlexxAgent to communicate with your cloud instance to understand the status of devices against a threat detected by the CrowdStrike agent.

Enable integration with CrowdStrike

1. Log on to `Portal`.
2. Go to `Settings` -> `Integrations` -> `CrowdStrike`.
3. Click on `Edit` and enter the following information:

- **API Client ID.** Unique identifier that represents the client on the CrowdStrike platform.
- **Secret String.** Secret key associated with the client ID.

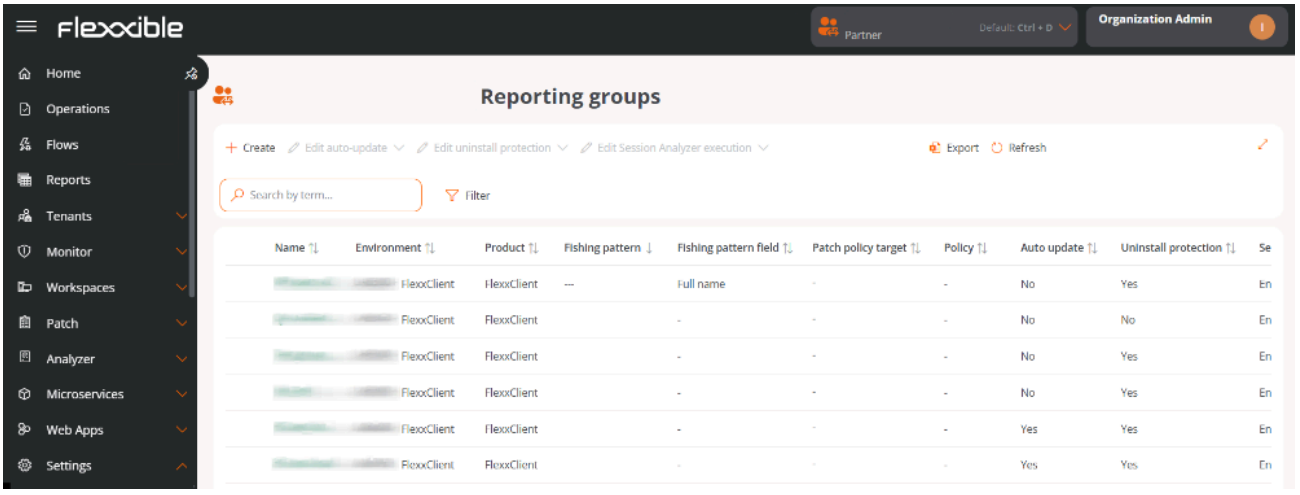
- **Region.** Geographic location of the customer's cloud environment. The field offers options like *eu*, *eu-1*, *us-gov-1*, *us-1*, and *us-2*.

4. Click on `Save`.

> **TIP**
>
> For more information about this feature, please refer to the guide Set up integration with CrowdStrike.

Portal / Settings / Reporting Groups

Reporting Groups allow you to create and manage groupings of devices within the same organization using different criteria. Their goal is to cover specific needs of departments, locations, or user collectives.



From this feature, you can:

- Check which users and roles have access to each group.
- See which devices are part of the group.
- Assign an update policy.
- Activate or modify remote assistance functionalities configured through FlexxAgent.
- Define a fishing pattern to automate device inclusion.

Creation of a reporting group

1. Go to `Portal` -> `Settings` -> `Reporting Groups`.
2. Click on `New`.
3. Fill out the form with the following fields:
    - **Name.** Group identifier.
    - **Environment.** Dropdown to choose the environment.

- **Fishing pattern.** Regular expression (RegEx) used to automate the inclusion of devices based on the content of the attribute selected in the *Fishing pattern field*. The pattern evaluates the value stored in that attribute, whether it's text, numbers, or any other string represented in it.

  > **NOTE**
  >
  > In versions prior to FlexxAgent 25.10, the fishing pattern is applied only to the device name.

- **Fishing pattern field.** Device attribute on which the regular expression configured in the fishing pattern will be applied.

- **Patch policy target.** Update policy assigned to the group.

Fishing pattern

The fishing pattern allows you to define regular expressions (RegEx) compatible with Java 8 for the automatic incorporation of devices into a report group.

The configured expression is compared with the content (value) of the attribute selected in the Fishing pattern field, whether it's text, numbers, or any other string represented in that field. It can be used to look for exact matches, texts that start or end in a specific way, or more advanced patterns. For partial matches, you can use `*` as a wildcard to indicate preceding or following content.

Examples:

RegEx	Matches...
`.*2023$`	any text ending in **2023**.
`.*abc.*`	any text containing **abc**.
`^item`	texts starting with **item**.

RegEx	Matches...
`\d{3}`	strings formed by exactly three digits.

> **TIP**
>
> To create and test regular expressions before configuring them in the production environment, Flexxible recommends using specialized tools like Regex101.

Considerations

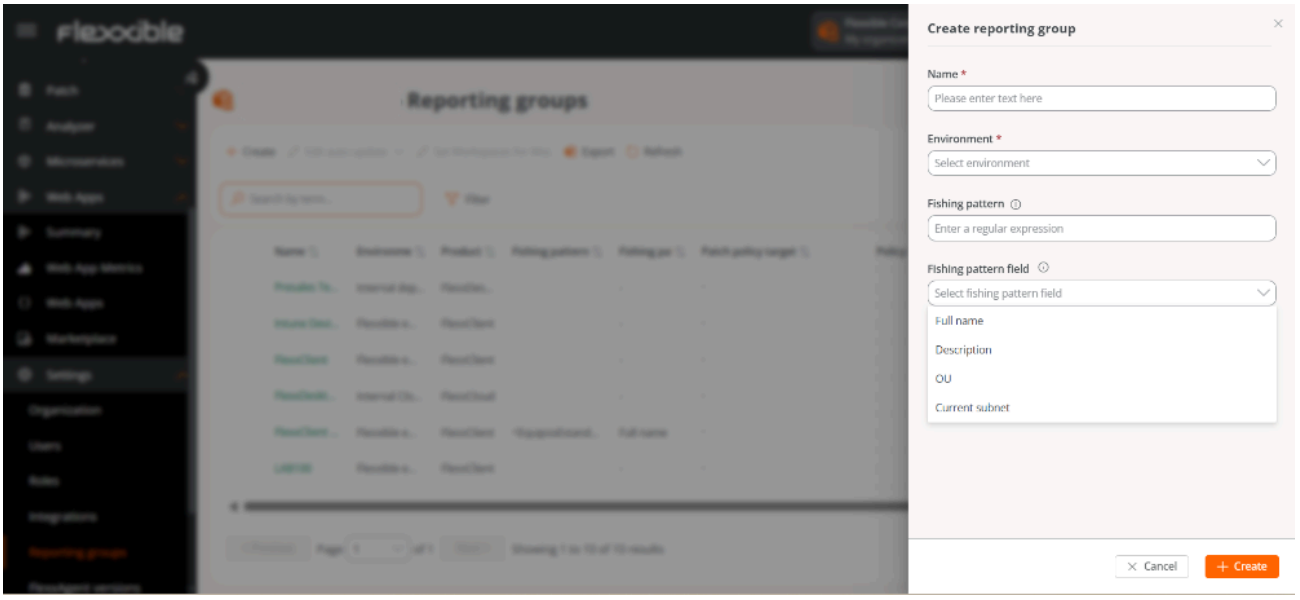
- The system runs **every hour** an automatic process that searches for devices whose attribute value matches the configured expression. If found, it adds them to the corresponding reporting group.
- Regular expressions can have a maximum length of 250 characters.
- It is recommended to periodically review active expressions to avoid overlaps and conflicts among groups.

Fishing pattern field

This field determines which device attribute the regular expression defined in the fishing pattern will be applied to.

Available options

- **Full Name.** Applies the expression to the device's full name.
- **Description.** Applies the expression to the content of the device description field.
- **OU.** Applies the expression to the organizational unit.
- **Current Subnet.** Applies the expression to the string of the device's current subnet.



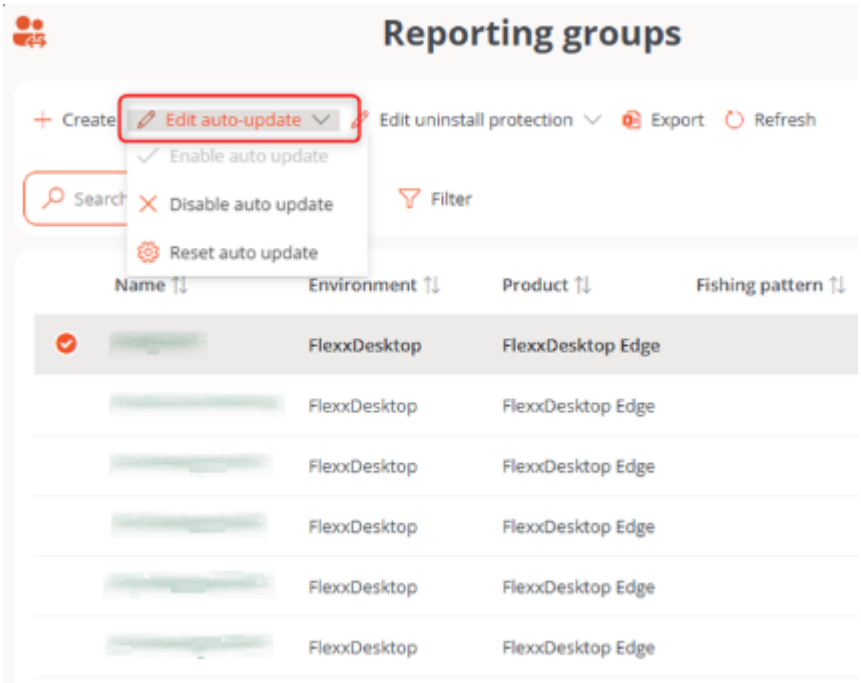
> **INFO**
>
> The **Search Pattern Field** is available from FlexxAgent version 25.10. In previous versions, the phishing pattern applies only to the device's name.

FlexxAgent Auto update

Allows activating the auto update of FlexxAgent on devices belonging to a group.

Settings

1. In the reporting group table, select the group(s) you want to configure.
2. Click on `Edit auto update`.
3. Choose one of the following options:
    - *Enable auto update*
    - *Disable auto update*
    - *Reset auto update*



> **NOTE**
>
> In organizations with the FlexxAgent Version feature, the automatic update always targets the Production environment, not Early.

Uninstallation Protection

This functionality prevents users from uninstalling FlexxAgent from the device. It can also be applied at the Product level.

Cases where protection is active

- The feature is enabled in the reporting group to which it belongs.
- The feature is deactivated in the reporting group (it is neither enabled nor disabled), but it is enabled at the Product level.

Requirements

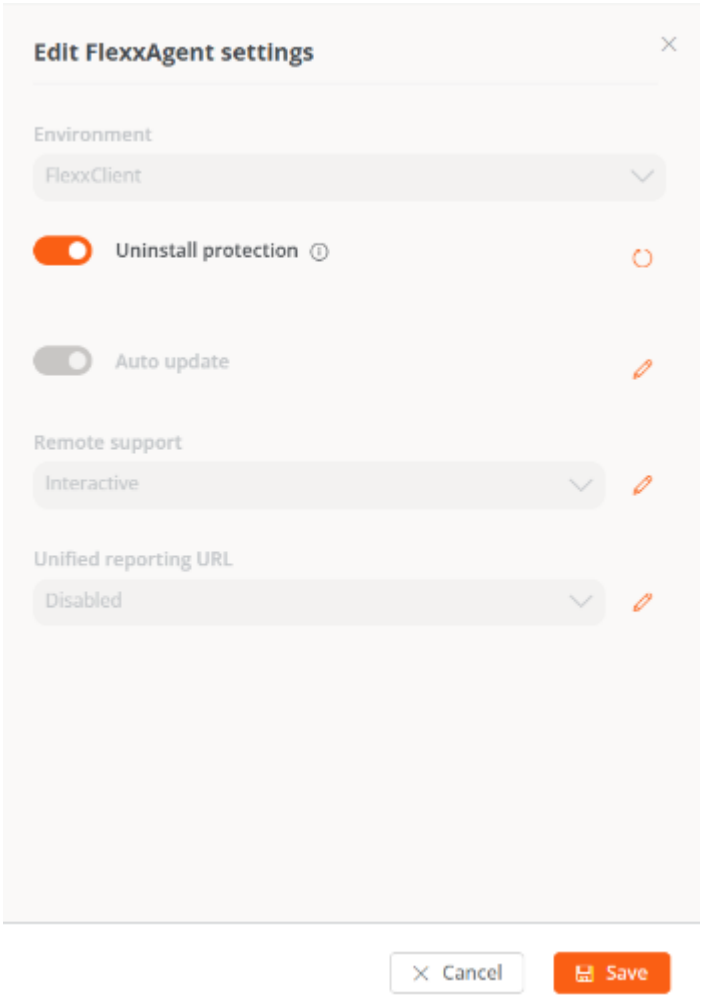
- The configuration can only be performed by a user with the *Organization Admin* role.
- Available from FlexxAgent version 25.4.2.

Settings

The feature can be enabled in one or more groups:

1. Go to `Portal` -> `Settings` -> `Reporting Groups`.
2. Select the group and in the `Action` field, click on `Agent settings`.
3. Edit the `Uninstallation protection` option via the edit button.
4. Click on `Save`.

> **INFO**
>
> Reporting groups inherit the settings made at the Product level; however, they can overwrite them.



> **TIP**
>
> For more information, see the documentation on Uninstallation Protection.

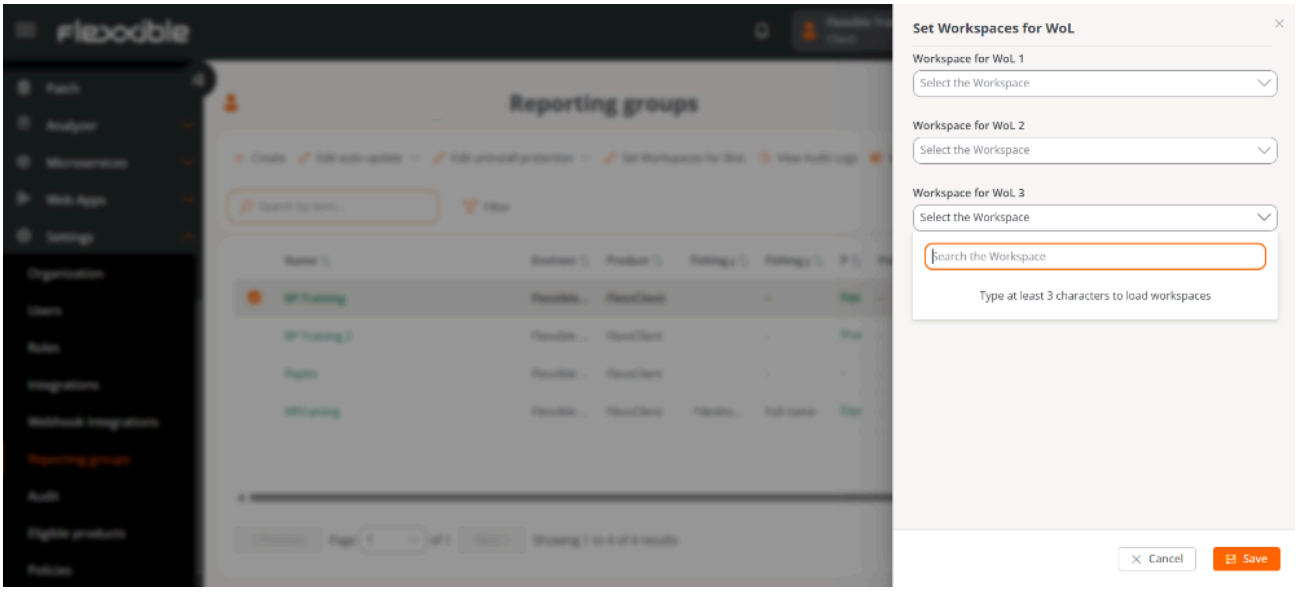
Set up devices for Wake on LAN (WoL)

This functionality allows defining specific devices that will execute auto power-on via Wake on LAN (WoL) in the selected reporting groups.

Settings

It's possible to set up to three devices for WoL execution, in case the process fails on one of them.

1. In the table, select one (or more) reporting groups.
2. Click `Set up workspaces for WoL`.
3. In the form, select the preferred devices that will handle turning on the machines via WoL.
4. Click `Save` to apply the changes.



> **WARNING**
>
> When several reporting groups are selected and one or more of the three form fields are left empty, they will also be saved as empty in those groups that previously had configured values.

Remove the configuration of WoL devices

To remove the devices associated with the WoL configuration:

1. Select the corresponding reporting group again.
2. Click `Set up workspaces for WoL`.
3. Leave the three fields empty.
4. Click `Save` to confirm the deletion.

The scheduling configuration is done at the level of Workspace Groups.

View audit log

Allows access to the organization `Audit` view.

Reporting groups list

The list view shows the reporting groups with the following information:

- Name
- Environment
- Product
- Fishing pattern
- Fishing pattern field
- Patch policy target
- Policy
- Automatic Update

- Uninstallation protection
- Action (See details and Agent settings)

Details of a reporting group

Upon accessing the details, several tabs are displayed:

1. Details

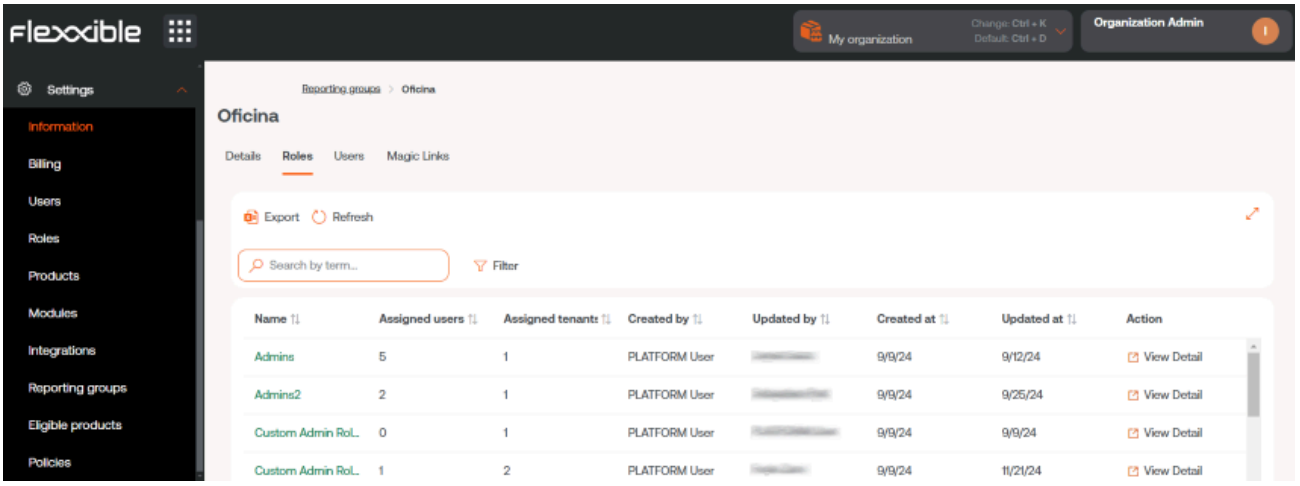
Contains the general information of the group.

Through `Edit`, you can modify: *Name*, *Environment*, *Fishing pattern*, *Fishing pattern field*, and *Patch policy target*.

2. Roles

List of roles that can access the group. Includes:

- Name
- Assigned users
- Assigned tenants
- Created by
- Updated by
- Creation and update dates
- Action (Role details)



3. Users

List of users with access to the group. Includes:

- Full Name
- Email
- Department

4. Devices

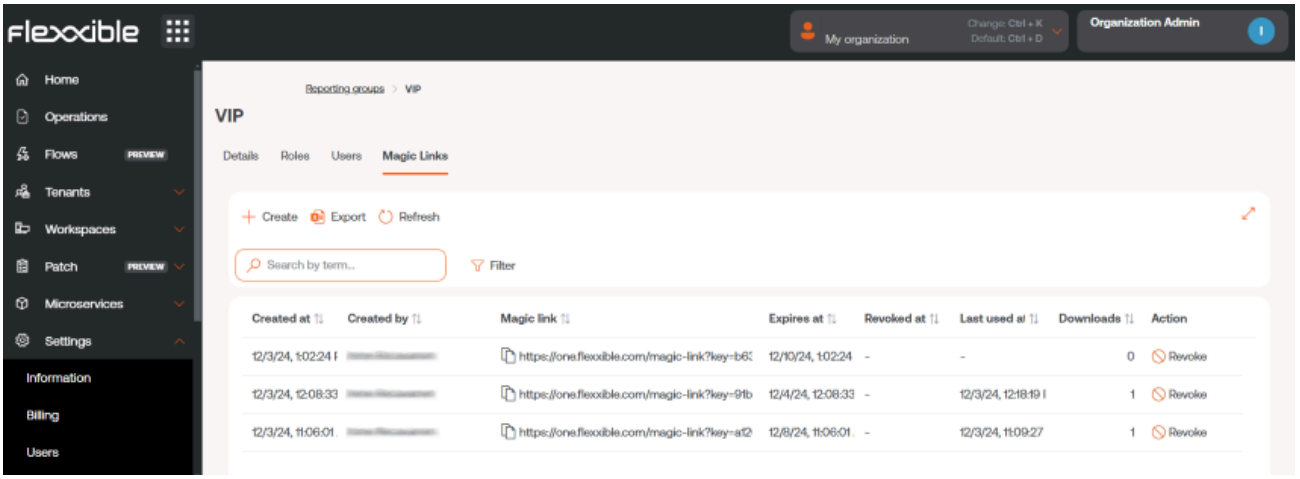
List of devices associated with the group. Includes:

- Name
- Intel vPro Enterprise (compatibility)
- IP Address
- Operating System
- CPU Cores
- RAM
- Type (physical or virtual)
- Last connected user

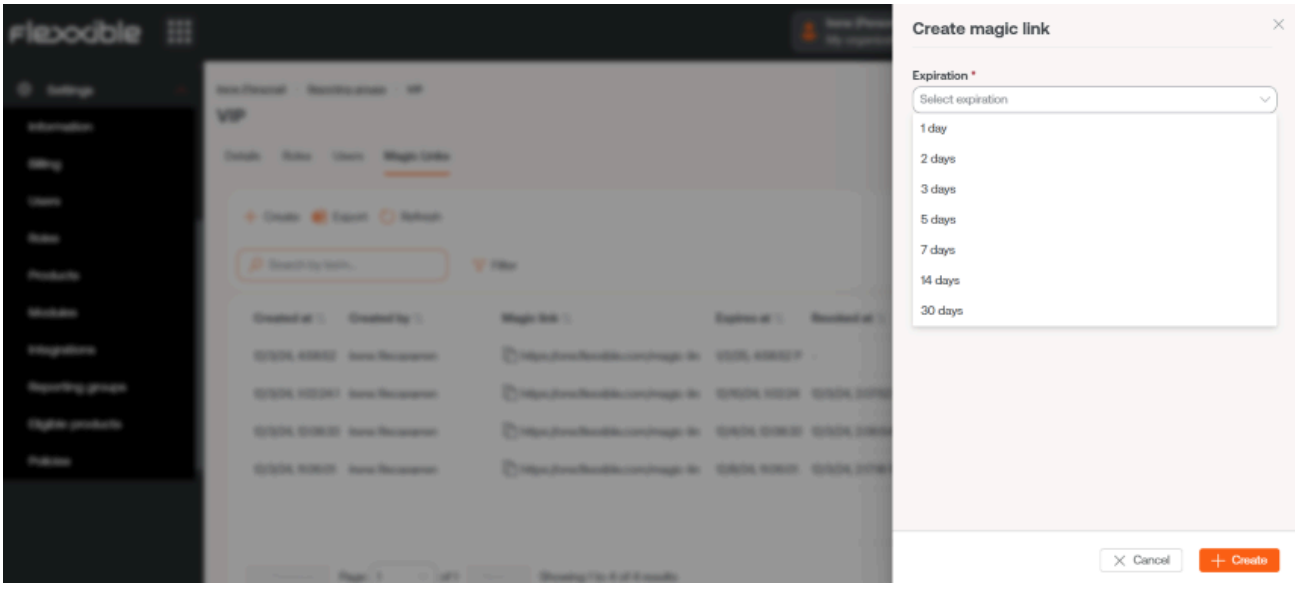
5. Magic link

Users with the *Organization Administrator* role within a partner-type organization can generate and send `Magic links` to users so they can download FlexxAgent on their devices without requiring prior authentication.

This tab displays a table listing the magic links created in the reporting group, both from the `Generate magic link` button on the Portal homepage and from this tab.



The `Create` button allows for generating magic links in the reporting group to optimize access to the FlexxAgent download on devices, previously defining their expiration time.



`Export` allows exporting the list in .xlsx format and `Refresh` updates the list of the magic links shown in the table.

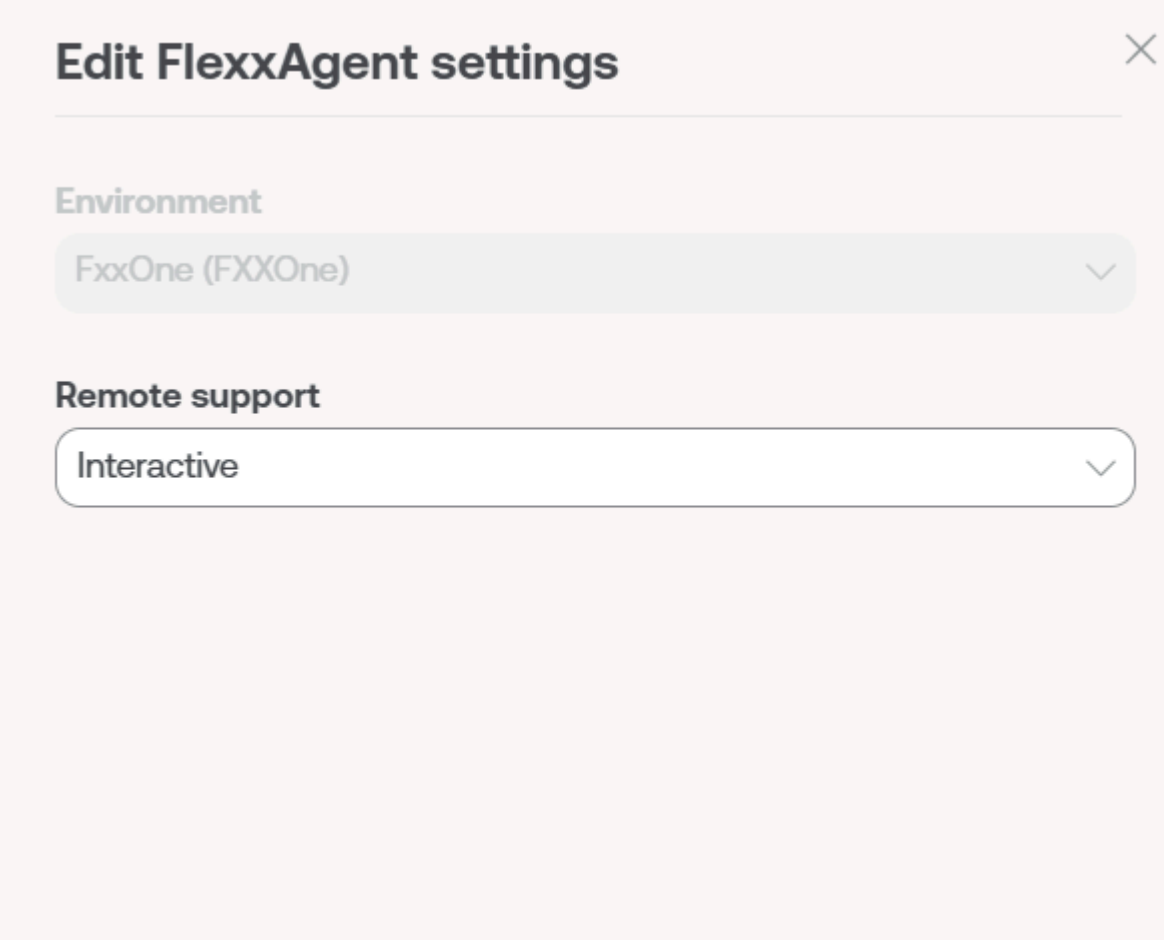
The table provides specific data about the created magic link, such as the author, creation and expiration dates; it also indicates if it has been revoked and when. From here, you can also copy the created magic link to share it and revoke it when deemed appropriate.

> More information about `Magic links`

FlexxAgent Configuration (Flexxible Remote Assistance)

Administrators can define the type of remote assistance:

- Interactive (attended)
- Unattended
- Dynamic
- None

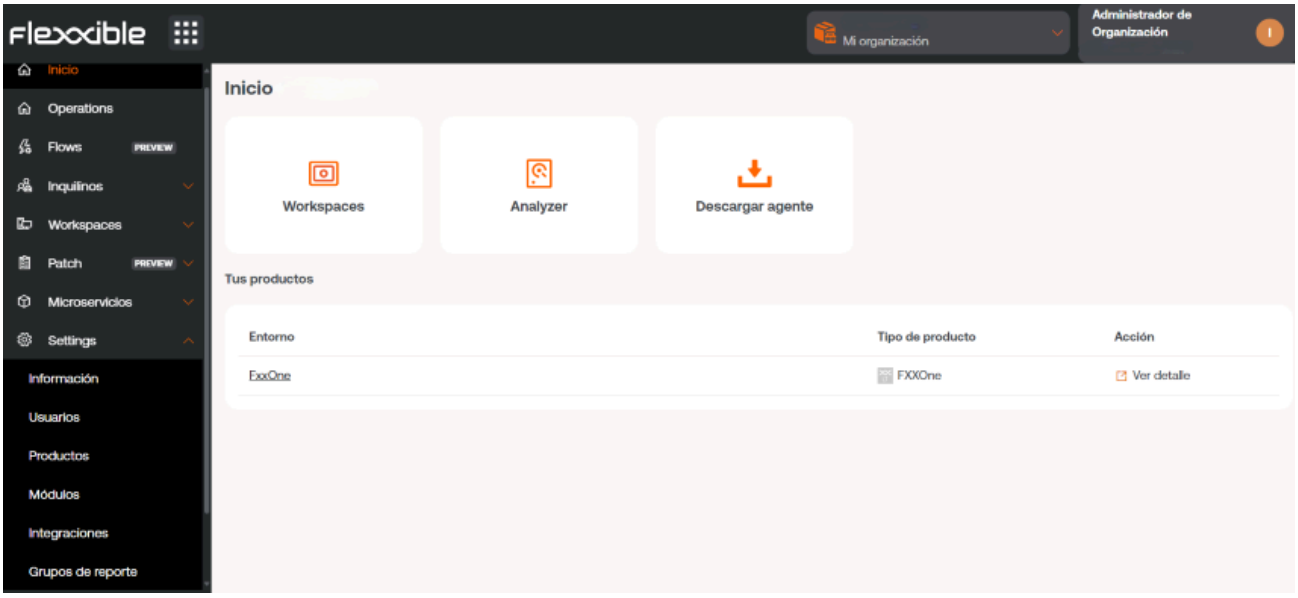


This configuration is set from Products. However, specific configurations can be made for report groups.

Download FlexxAgent

In FXXOne, you can download FlexxAgent directly from the reporting groups view. Simply click on `Download agent` to perform this action and then follow the installation steps.

This action can also be performed from the Portal home page.



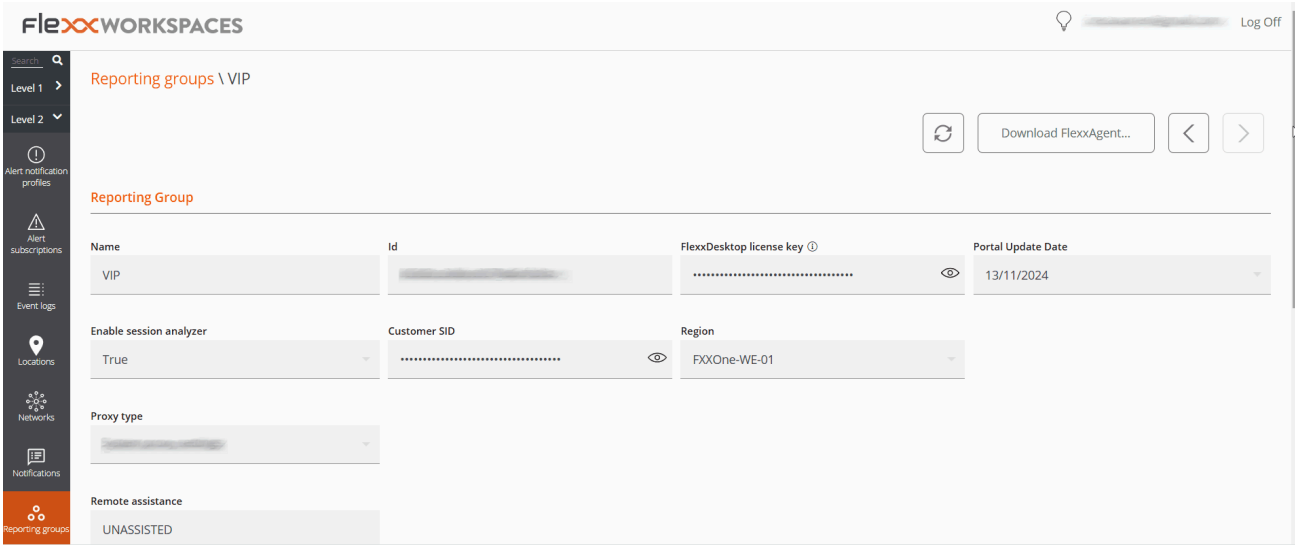
> **INFO**
>
> Some of the configuration options of FlexxAgent are not visible to users with the *Organization Administrator* role.

Report Group Verification

It's possible to check the group a device belongs to from the Workspaces section in Portal, by accessing the device details. The history of assigned groups is also displayed there.

Removal of a device from a reporting group

1. Access the Workspaces module -> `Level 2` -> `Reporting groups`.
2. Select the corresponding reporting group.
3. In the `Devices` tab, select the device.
4. Go to `Operations` -> `Delete workspace`.



Portal / Settings / FlexxAgent version

As FlexxAgent versions evolve and incorporate new functionalities, organizations need to control which version of FlexxAgent will be installed on their devices.

In that sense, **FlexxAgent Version** allows users with the *Organization Administrator* role to choose the FlexxAgent version that will be used in each of the report groups created in the organization's environment.

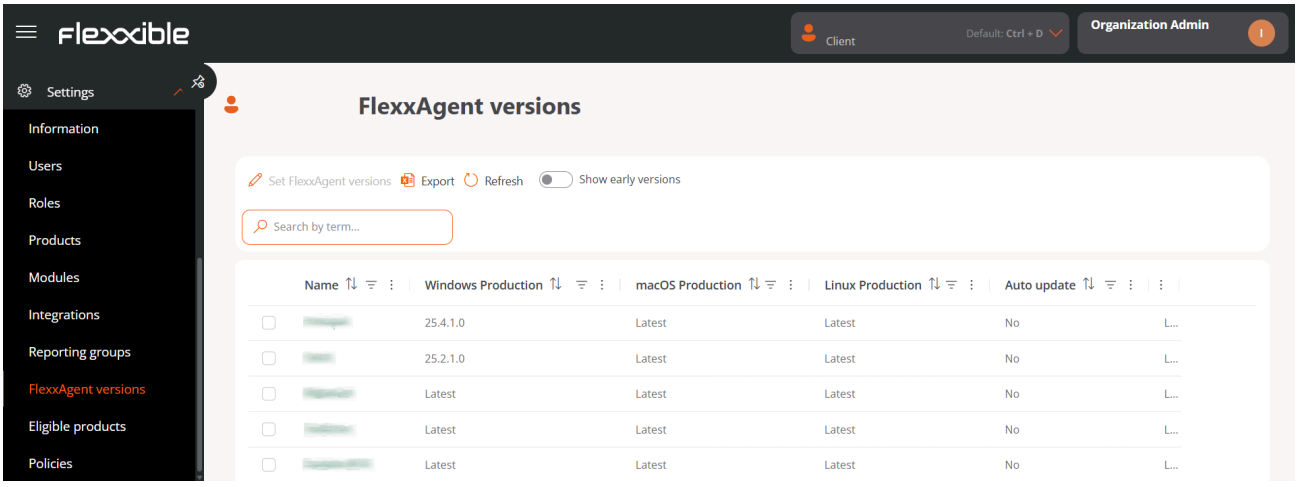
> **INFO**
>
> To access this feature, please consult with your contact at Flexxible.

Version settings

To manage FlexxAgent versions, it is necessary for the environment to have at least version 25.4.1 installed and the user must be *Organization Administrator*.

Steps for configuration:

1. Go to `Portal` -> `Settings` -> `FlexxAgent Version`.



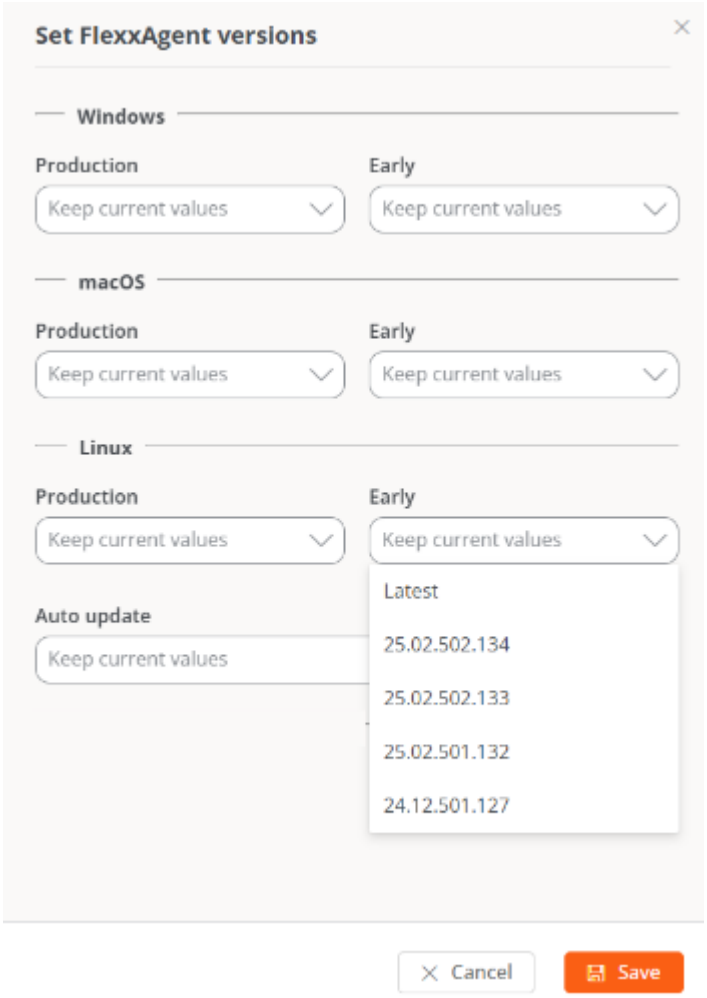
The table will display the list of reporting groups in the organization with the following information:

- **Name.** Name of the report group.
- **Windows Production.** Version number set for *Production* on Windows.
- **macOS Production.** Version number set for *Production* on macOS.
- **Linux Production.** Version number set for *Production* on Linux.
- **Automatic Update.** Defined from the report group configuration. It will always point to *Production* environments, not *Early*.

> **INFO**
>
> - ***Early*** is the testing environment, where an operator can review if the version indicated in this field is functional for the organization's needs. It is recommended to be in *Latest*.
> - ***Production*** is the real environment. The version indicated in this field will be applied to all productive devices of the selected reporting groups.

If the `Show early versions` button is activated, located at the top of the table, versions will be shown in the *Early* scope for all operating systems.

2. Select one or more reporting groups in the table to configure the FlexxAgent version of their devices.
3. Click on `Set FlexxAgent versions`. The form must configure the version number for each of the two available environments: *Production* and *Early* for all operating systems.



The form will also allow you to choose whether or not to set the automatic update of FlexxAgent.

4. Click on `Save`.

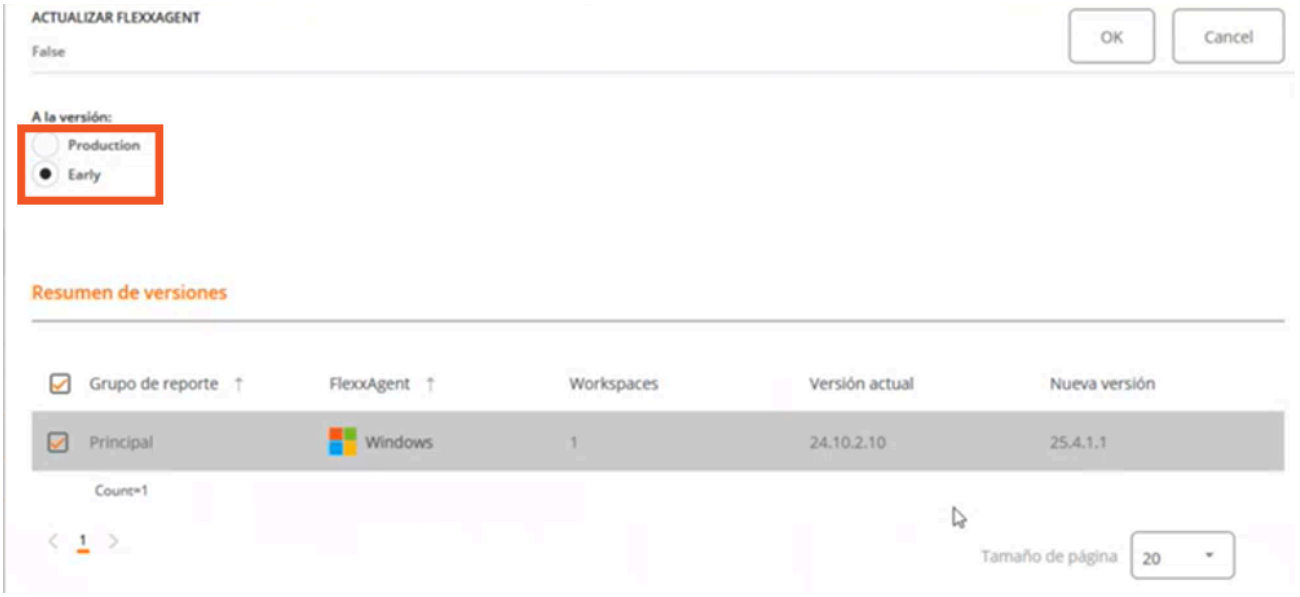
> **INFO**
>
> When an older version of FlexxAgent (downgrade) is applied to the devices, the current version is automatically uninstalled to install the configured version; additionally, the devices lose access to features corresponding to more recent versions.

Management from Workspaces

Since the FlexxAgent versions are configured for the *Production* and *Early* environments, a user can decide which will apply to the selected devices in the Workspaces module.

`Workspaces` -> `Operations` -> `FlexxAgent` -> `Update FlexxAgent`

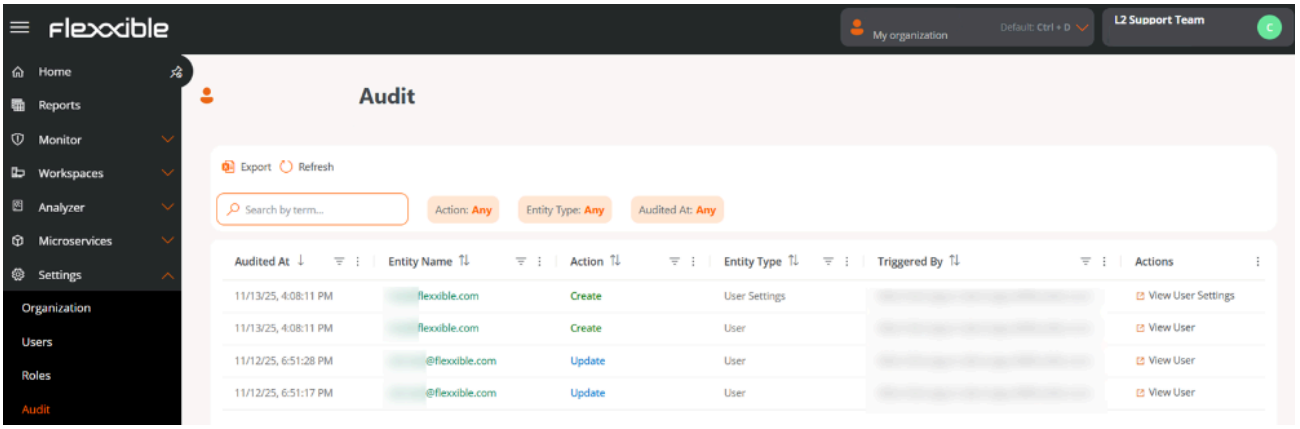
A modal window will request to indicate in which environment this update will be applied: *Early* or *Production*.



Portal / Settings / Audit

Audit allows the logging of all creation, modification, and deletion actions performed by users on all entities available in Portal, that is, on any element that the user can view or modify within the platform.

This mechanism ensures complete traceability of operations, allowing us to precisely identify who performed an action, when it was executed, and what information was affected. As a result, all interactions carried out in Portal are audited, providing transparency, control, and support for supervision and compliance tasks.



Audit log

Each record in the list shows the following information:

- **Audited on.** Date and time when the action was executed.
- **Entity name.** Object on which the action was performed. By clicking, you can access its detail view.
- **Action.** Type of change registered: *Creation*, *Update*, or *Deletion*.
- **Entity type.** Classification of the audited object. It can be *User*, *User Configuration*, or *Tenant*.
- **Executed by.** User who performed the action (name and email are displayed).
- **Actions.** Depending on the entity type, it allows access to its respective section in Portal; for example, for the entities *User* and *User Settings*, the Users section will open.

Audit detail

At the top of the view, summary cards with the main information are shown:

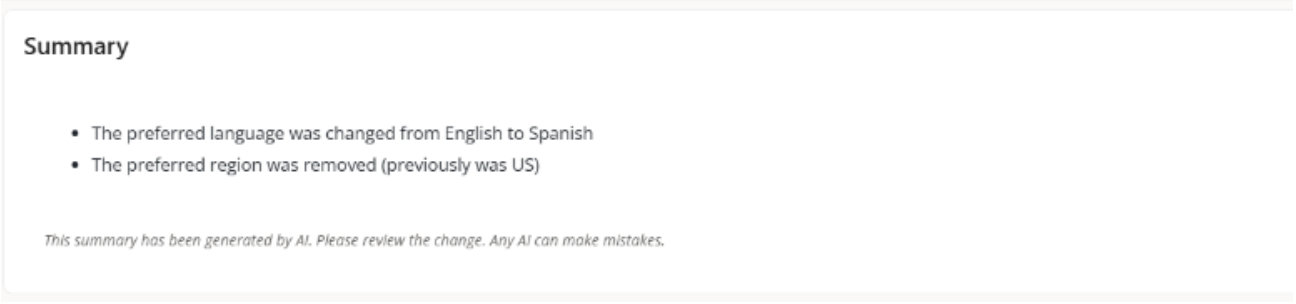
- **Audited on.** Date and time of the action.
- **Action.** Type of event executed: *Creation*, *Update*, or *Deletion*.

Overview

- **Entity name.** Object on which the action was registered.
- **Entity type.** Classification of the audited object (*User*, *User Configuration*, or *Tenant*). From here, you can access the entity detail.
- **Username.** User who executed the action.
- **Email.** User's email address.
- **Organization.** Organization to which the modified object belongs.

Summary

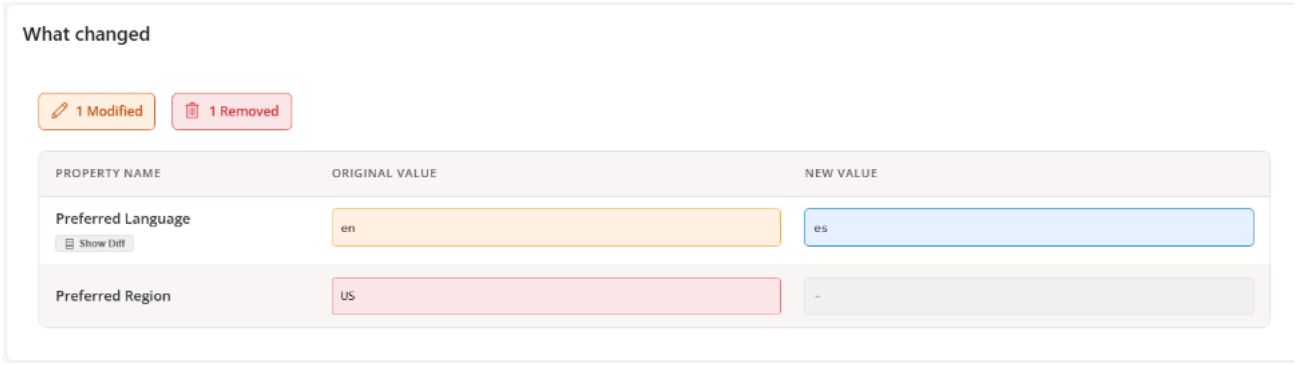
Displays an AI-generated message briefly describing the recorded action.



What changed

Shows a table with the changes detected in the audited entity:

- **Property name.** Attribute that was modified.
- **Original value.** Value before the modification.
- **New value.** Updated value after the modification.



Portal / Settings / Directives

Directives allow the creation of client-type organizations through a template, so each time an organization is registered, it can be done following a pattern that can be used to apply certain configurations, such as user access or FlexxAgent activation. They are useful for assigning certain characteristics to one or more report groups, thus facilitating the management of these and saving time for users of managed service provider (MSP) organizations.

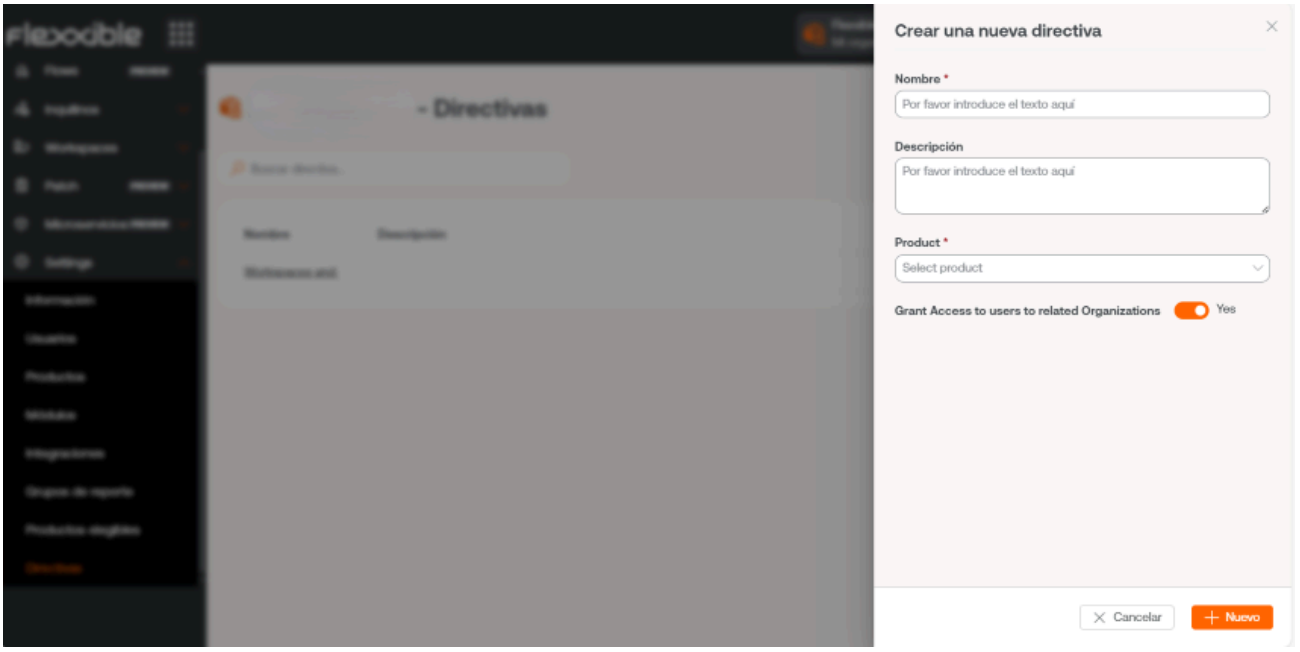
From the **Policies** overview, you can access a list and description of the created policies. By clicking on `View Details`, you can get more information, such as the report groups to which it is being applied and the names of the users responsible for its management.

Each time a new organization is registered, the report groups that are defined in the directive will be created. At the same time, from the directive itself, it can be determined whether partner-type users will have access to manage an organization in Portal or not.

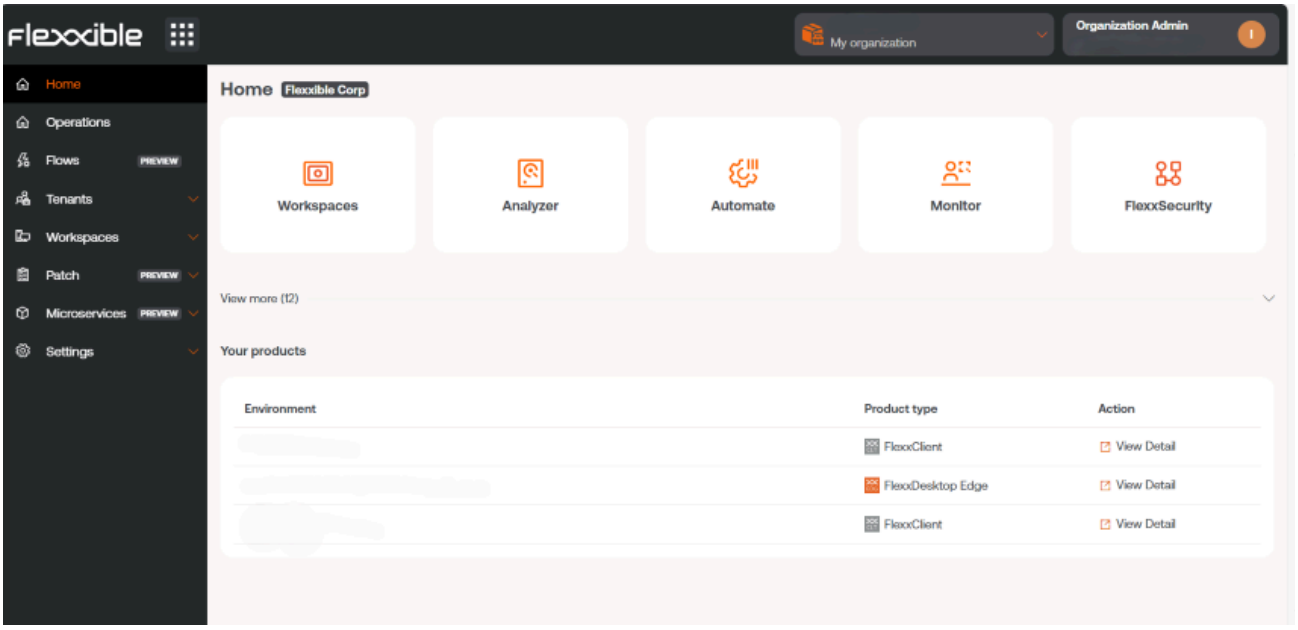
New Directive

To create a new directive, just click `New` and insert the requested information: Name, description, associated product, and user information for the people who will manage it.

A policy can also be assigned to an organization from Tenants.



Portal / Portal Guides



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 / Create and manage workspace groups

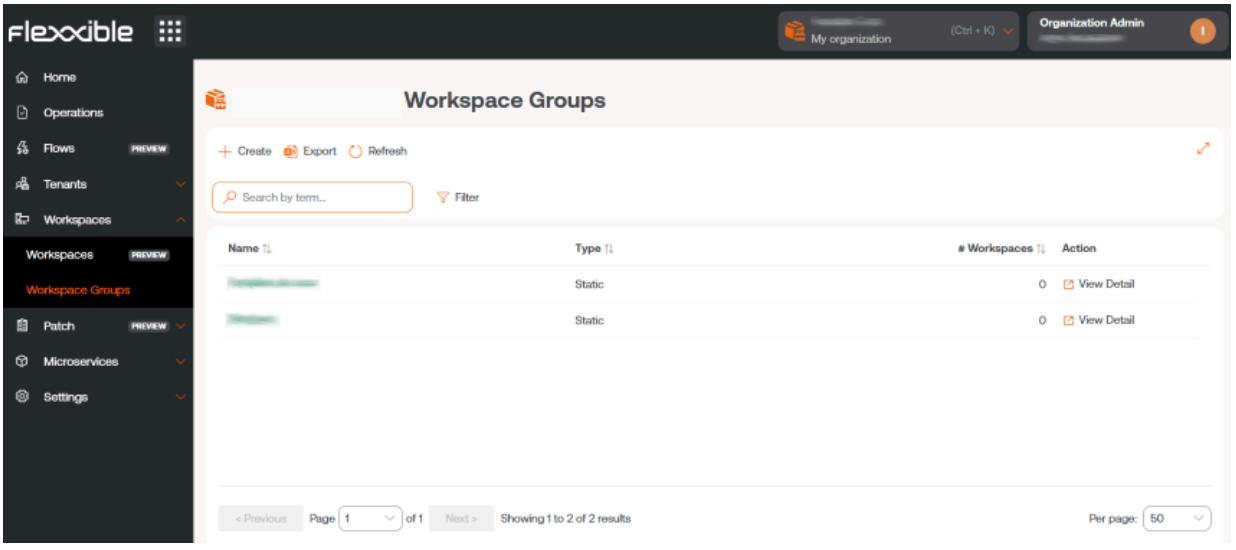
Workspace groups are logical groupings of a set of devices (or endpoints) that can be used when managing an organization. They can be static, dynamic, and Entra ID type.

Static workspace groups

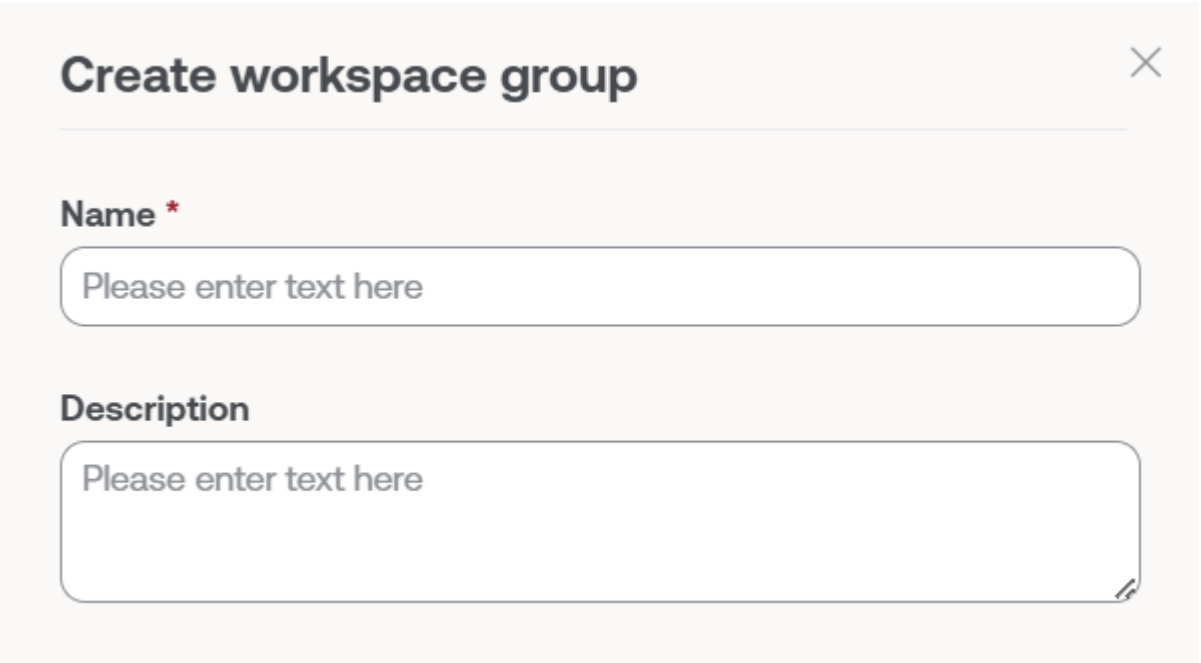
It is a group created manually, with free criteria. The devices that comprise it do not change unless the group is modified. You can create and manage it from the Portal and the Workspaces module by filtering the list in the Workspaces option.

Create a static workspace group from the Portal

1. Enter the Portal and select the `Workspaces` -> `Workspace Groups` option in the left side menu. A list of available groups will appear (or empty, if none exists).

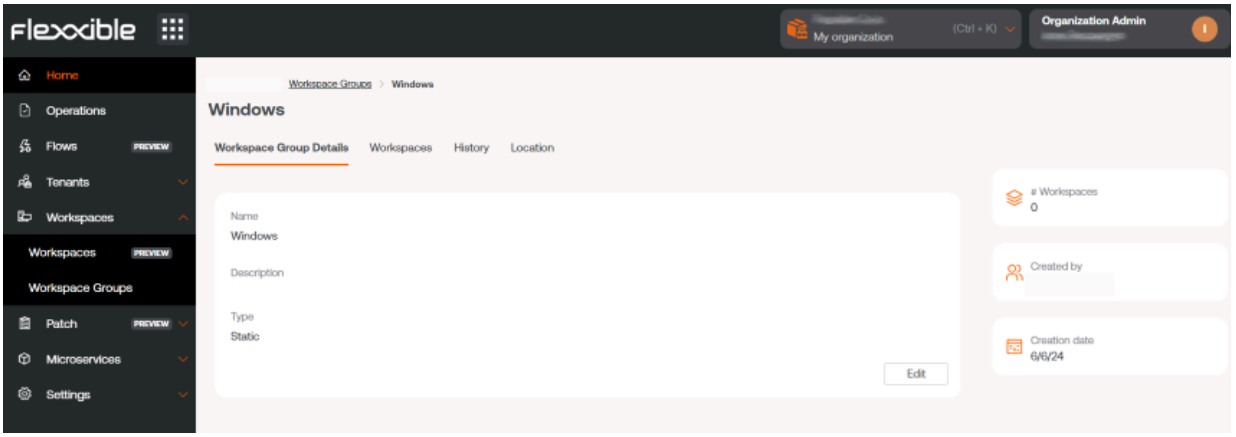


2. Click on the `+ New` button at the top of the list. A modal window will appear on the right side of the screen. Enter the group name and its description (optional). Click the `+ New` button at the bottom of the window.



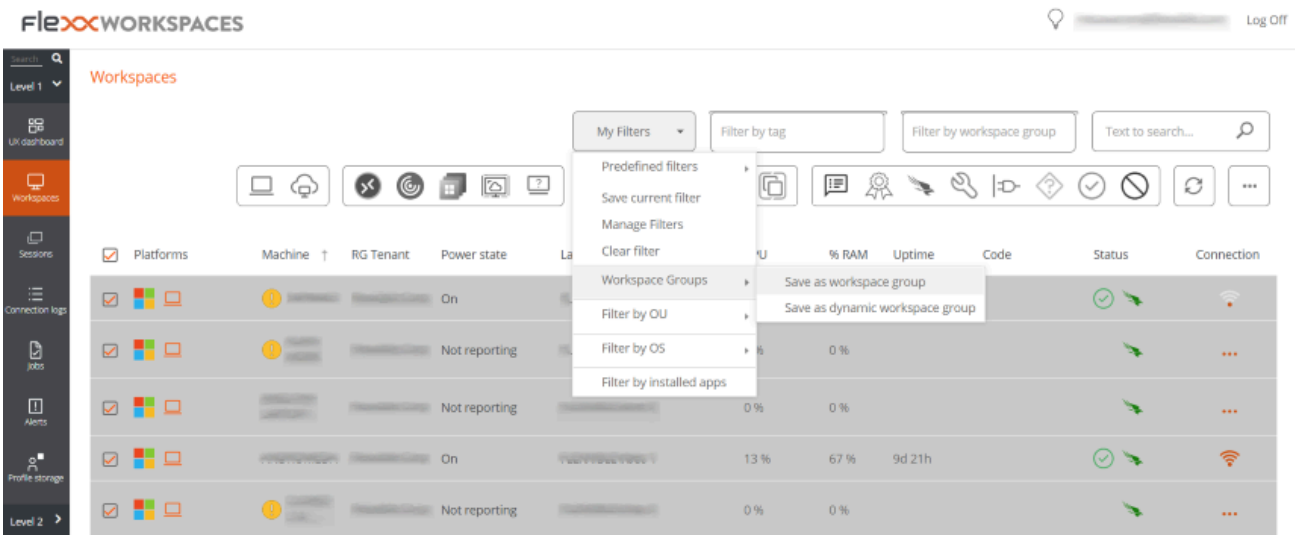
3. A confirmation message of the group's creation will appear. Close the window using the cross at the top right.

4. The new group will appear in the list of workspace groups. Click on its name to access the details.



Create a static workspace group from Workspaces

1. Access the Workspaces section 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 Workspace Group`.



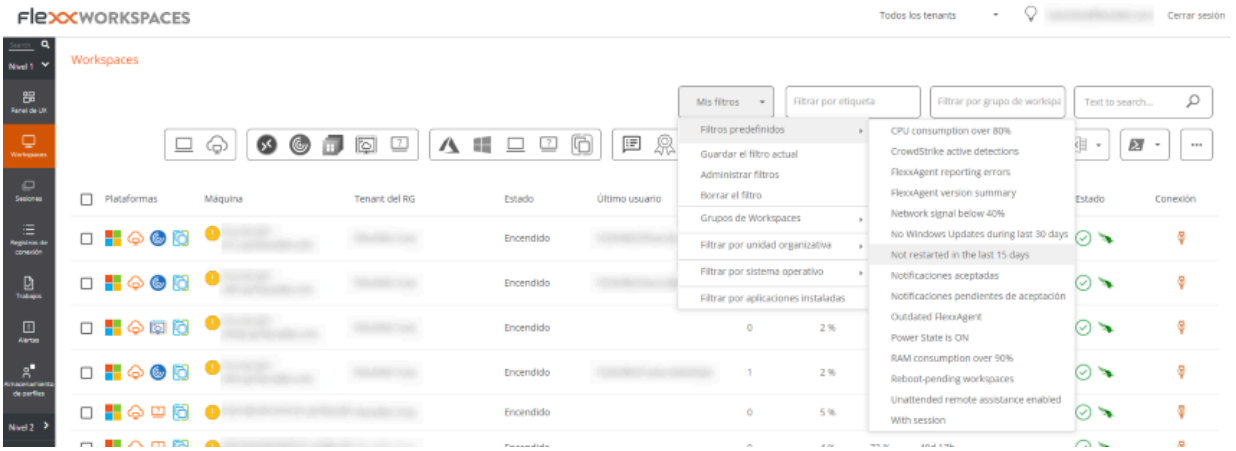
Dynamic workspace groups

It is a group where a condition is periodically evaluated, so its members can change in real-time. Dynamic workspace groups can be created from search filters in the Workspaces module.

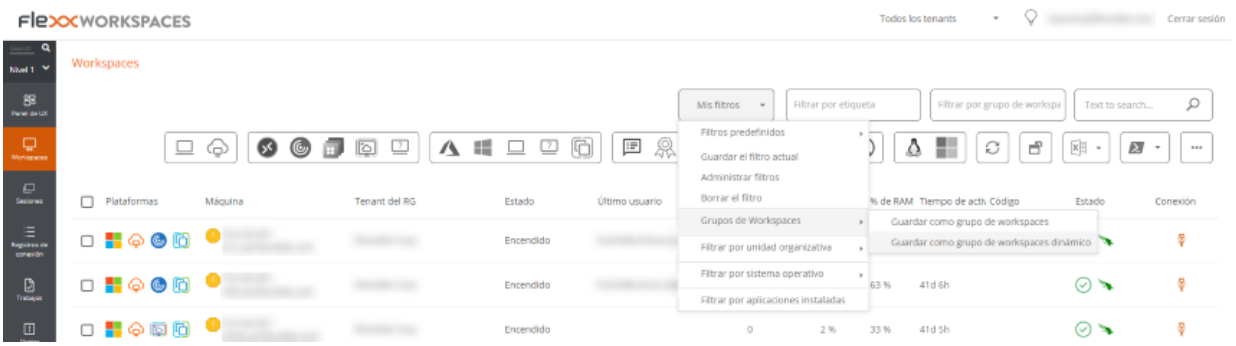
Create a dynamic workspace group

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.



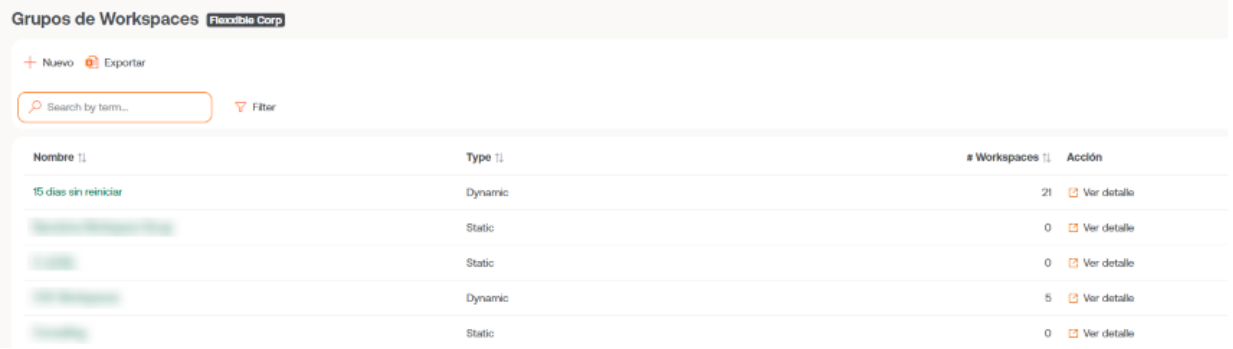
2. Once inside the filter results, use the `My Filters` -> `Workspace Groups` -> `Save as Dynamic Workspace Group` option.



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 in the Workspaces module.

5. Go back to the `Workspaces` -> `Workspace Groups` menu in the Portal to check that the new dynamic group has been created and review its members.



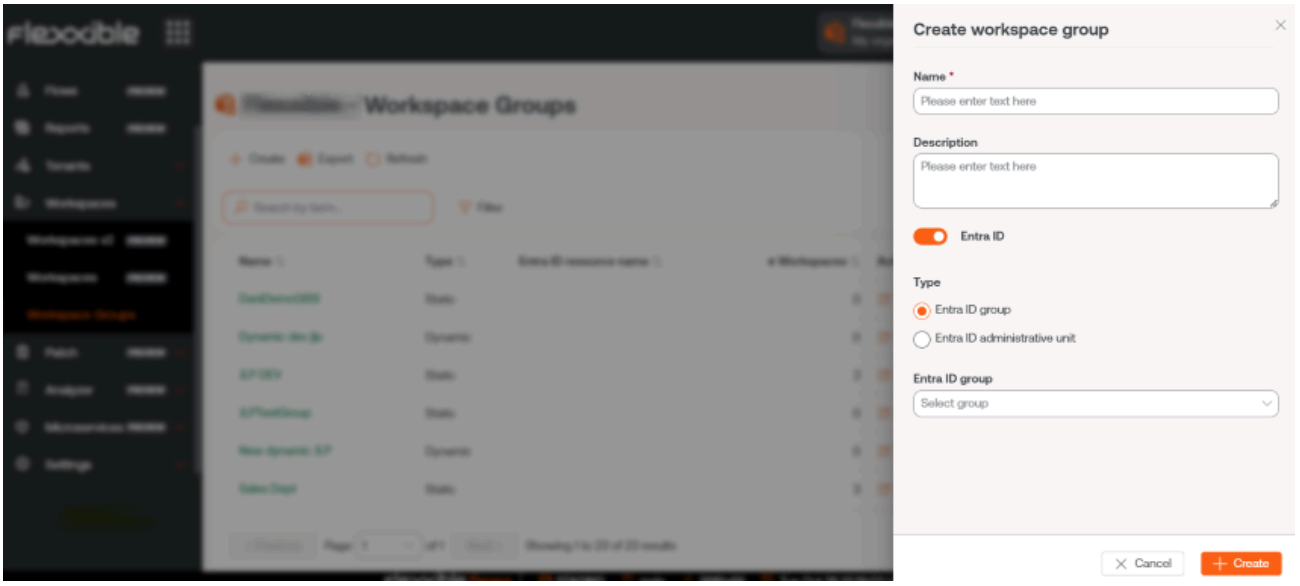
Workspaces Enter ID groups

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.

Create a Workspace group Enter ID

Entra ID groups are created from Portal.

1. Go to `Workspace groups` in the side menu.
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 you check the created **Enter ID Group** and **Enter ID Administration Unit** and, therefore, perform operations on them from the Workspaces module.

Manage a workspace group from Portal

To manage a workspace 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.** Displays the devices that are part of this group. This option allows exporting the list of devices comprising it.

- **History.** Shows a bar graph with the daily number of workspaces that have comprised the group during 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.

- **Scheduling.** From this tab, you can schedule the automatic power-on (Wake on LAN) or 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 you to select which day of the week the action will take place.
  - **UTC time.** Allows you to specify the exact time to start the action, in 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.

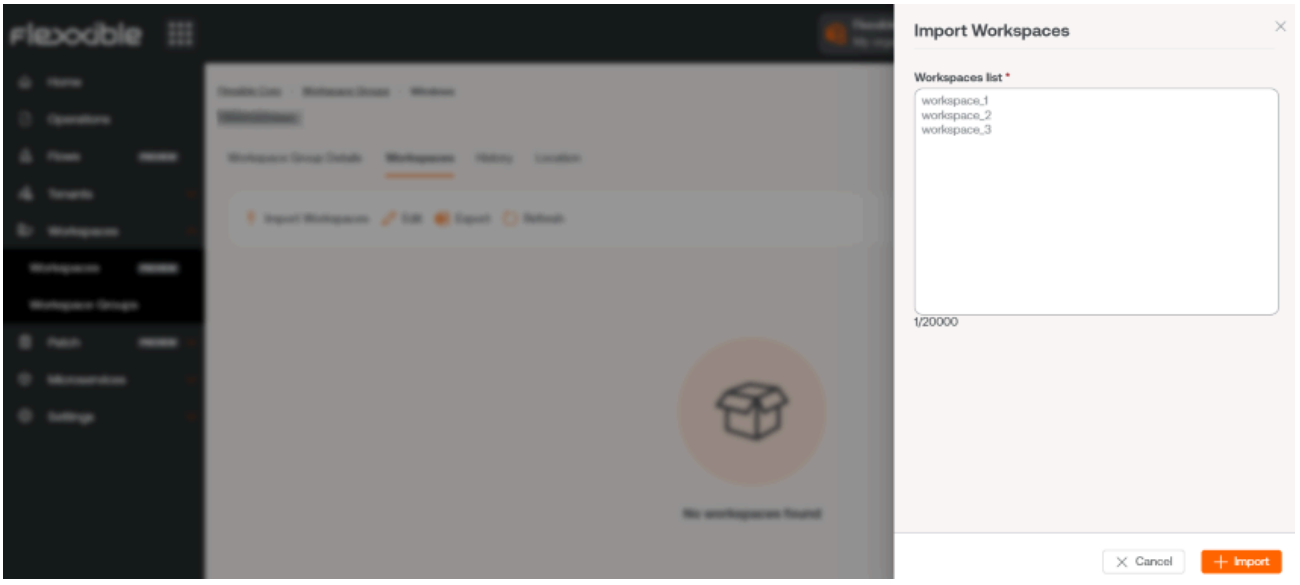
  From `View details` you can edit and delete the scheduled action.

- **Synchronizations.** This tab is only visible when the group is of type Entra ID. Displays a table with details of the performed syncs.

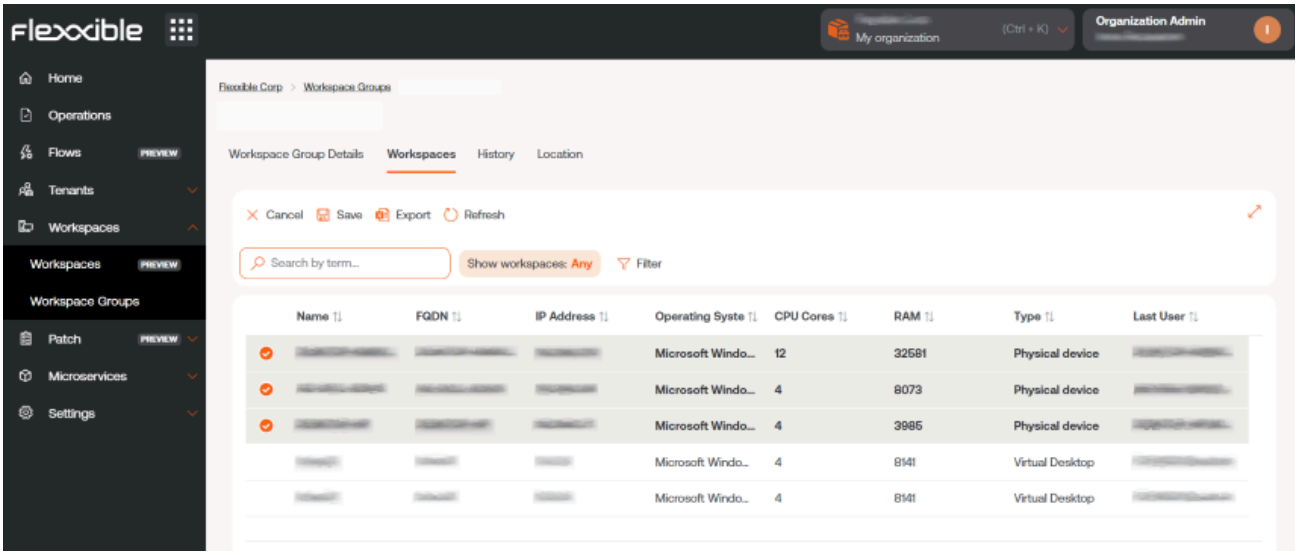
Add devices to the static workspace group

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 allowing importation of up to 20,000 devices.



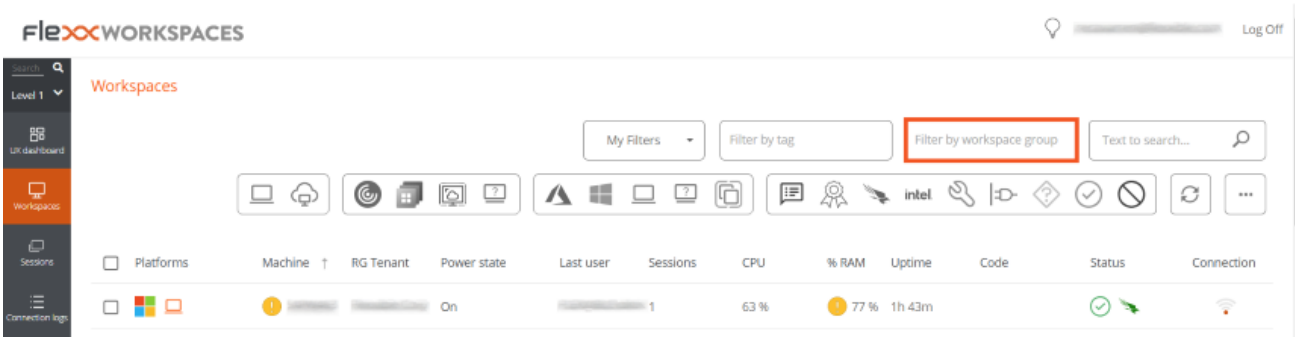
2. In the groups table, click on `Detail View` of the desired group -> `Workspaces` -> `Edit`. Next, select the devices you want to add. Those marked with an orange dot are added to the group and those not marked are removed. In both cases, click on `Save` to keep the changes.



Manage a workspace group from Workspaces

Once the group is defined, it can be managed within the Workspaces module.

1. Access the Workspaces section in the left side menu of the Workspaces module.
2. Filter the list of devices by workspace groups.



3. Choose the workspace group on which you want to perform actions. 4. Use the multiple options offered by the Workspaces module.

> **INFO**
>
> For more information about workspace groups, please consult their documentation.

Portal / Guides / Run microservices on a scheduled basis

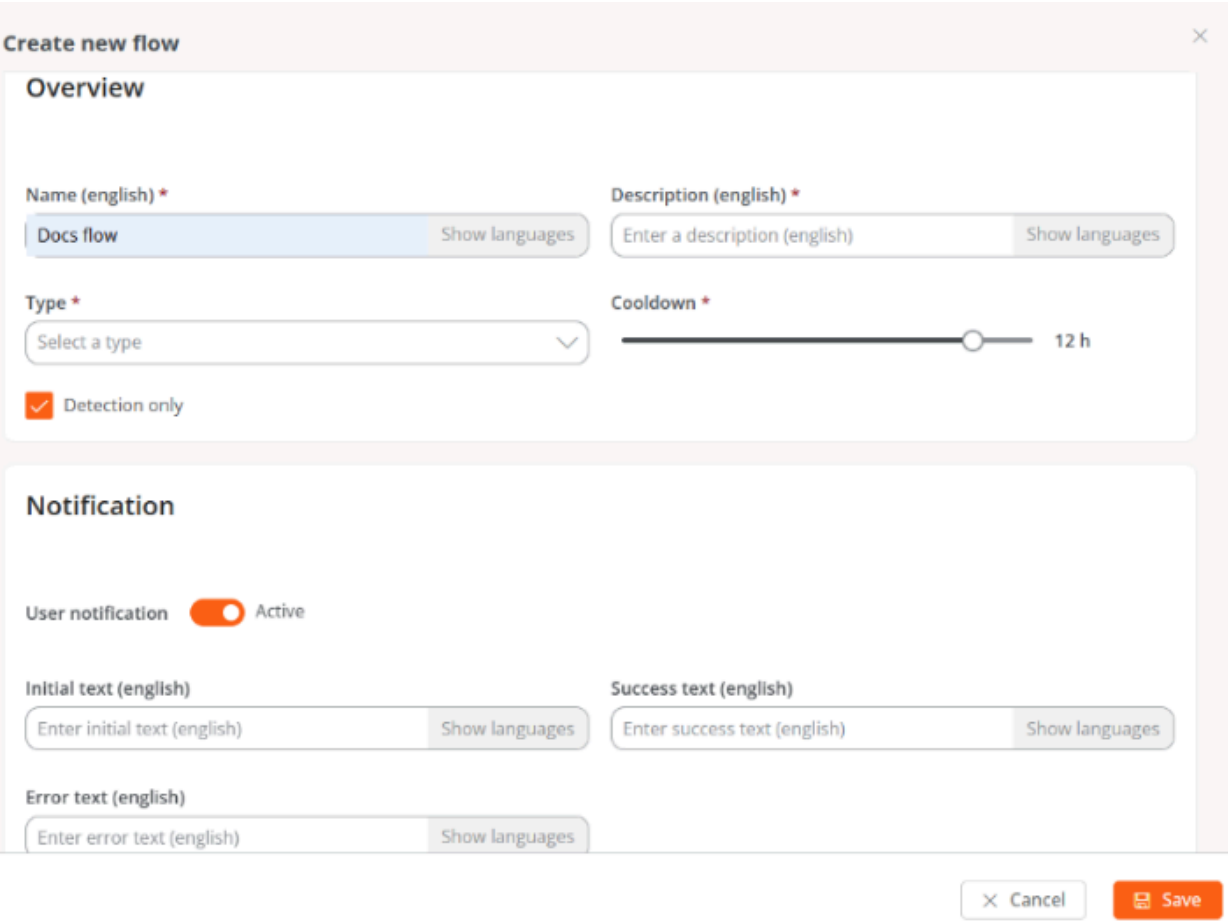
Microservices are independent components that execute to prevent or solve frequent issues on devices, improve performance, or speed up tasks that might require a lot of time to do manually. They can be executed directly from the Workspaces module or scheduled from the Flows section in the Portal.

Schedule a microservice execution

1. Access `Portal` -> `Flows`.
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.

   Overview

   - **Name.** Name of the flow. The `Show languages` button allows you to write it in Spanish, English, Portuguese, Catalan, and Basque.
   - **Description.** Brief explanation about the purpose of the flow.
   - **Type.** This is the scope of execution for the flow. Choose if it will be executed at the user session level, with the corresponding permissions, or at the device level, with administrative access.
   - **Reutilization time.** Minimum time that will pass once the evaluated condition is met for the evaluation to be executed again.
   - **Detection only.** If activated, it evaluates the conditions in "sampling" mode and detects the devices where these are met, but does not execute the microservice defined in the flow.



Notification

This parameter is optional and can be inactive. It is used to send notices to users at the start and end of flow execution using the operating system notifications. Once enabled, you can set:

- **Initial text.** Content of the notification that will be sent to users at the start of the execution.
- **Success text.** Content of the notification that will be sent to users after a successful execution.
- **Error text.** Content of the notification that will be sent to users after an execution with errors.

In all three fields, the `Show languages` button allows writing content in Spanish, English, Portuguese, Catalan, and Basque.

Target

This section configures the flow's target. Through the `Apply to` dropdown, you can select the devices or groups where the actions will be executed.

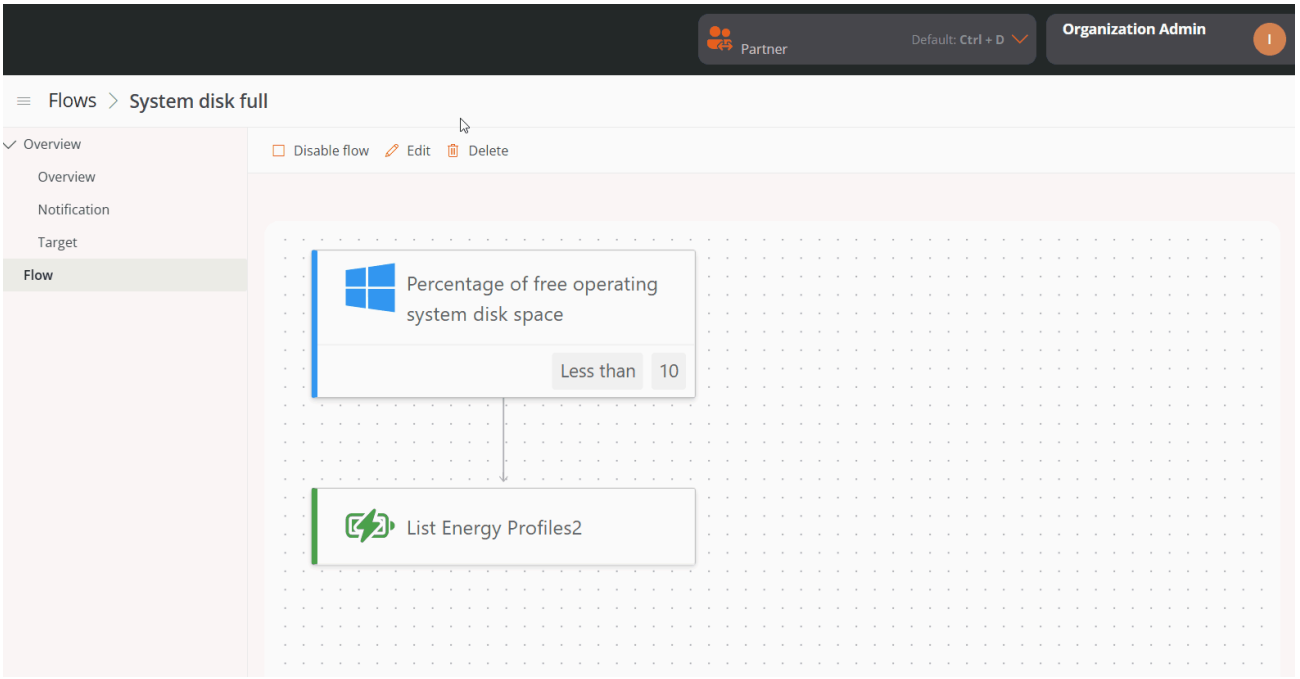
- **All workspaces.** Apply the flow to all devices in the organization.
- **Workspaces.** Apply the flow to the devices that the user chooses in the table.
- **Workspaces groups.** Apply the flow to the workspaces groups that the user chooses in the dropdown shown when selecting this option.
- **Reporting groups.** Apply the flow to the reporting groups that the user chooses in the dropdown shown when selecting this option.

4. Once the fields are filled in, click on `Save`.

5. The user will be redirected to the flow's detail view. In the left sidebar menu, click on the `Flow` tab.

6. Click the `Edit` button located above the panel.

7. In the panel, click on `+` and then on `Add condition`. A modal window with the available conditions will open on the right of the screen.



8. Choose a condition.
9. Fill in the verification fields.

10. Click on `Save`.
11. In the panel, click on the `+` symbol located below the condition and select `Add action` to add the microservice that will be scheduled. You can add more conditions at this point if necessary.
12. Select the microservice you want to schedule.
13. Click on `Save`.
14. To activate the flow, click on the `Enable flow` button.

> **TIP**
>
> For more information, please check the documentation for Flows.

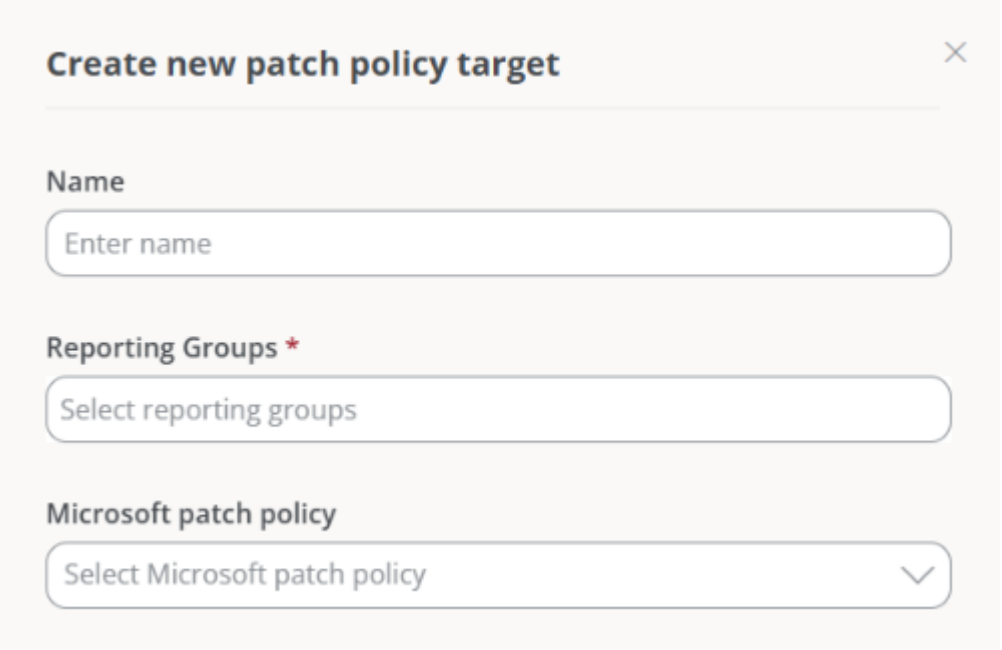
Portal / Guides / Configure patch policies

Patch policies set parameters for installing security patches and functional enhancements on devices. They allow defining the timing and scope of deployment, as well as exercising granular control over the update content, by approving or denying packages published by Microsoft, according to the organization's security and compatibility requirements.

Create a new patch policy

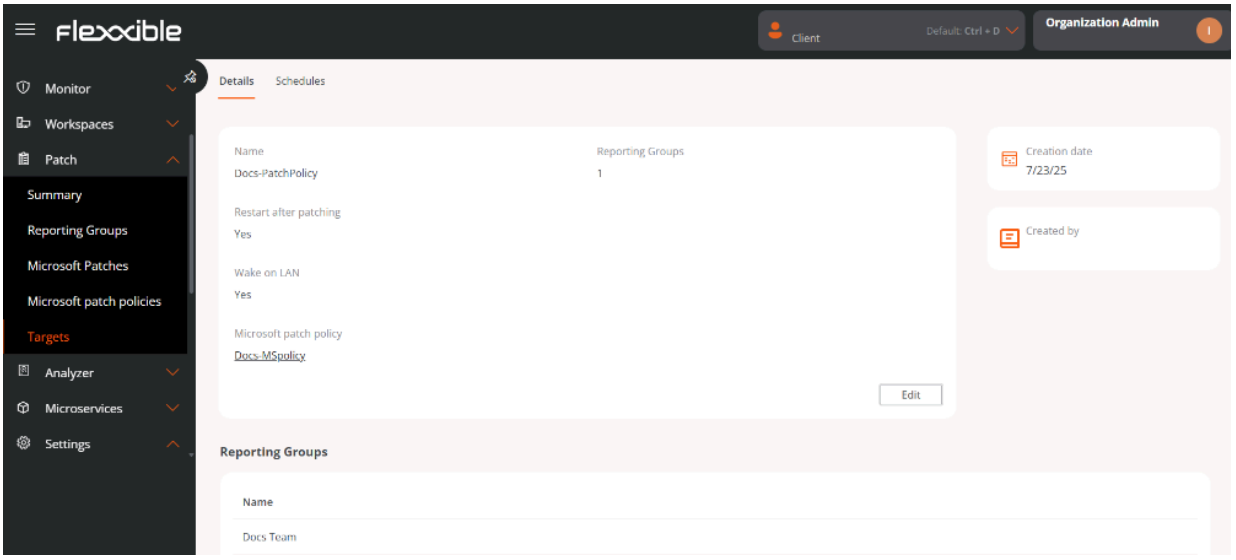
1. Access `Portal` -> `Patch` -> `Targets`.
2. Create a new target by clicking `+ New`.
3. Fill in the fields:

- **Name.** Name of the new patch policy.
- **Report Group.** Target device group for the new patch policy (can be more than one).
- **Microsoft Patch Policy.** Microsoft patch policy to which the new patch policy will be linked. This field is optional.



4. Click on `Save`.

5. The new patch policy information will appear on the screen.



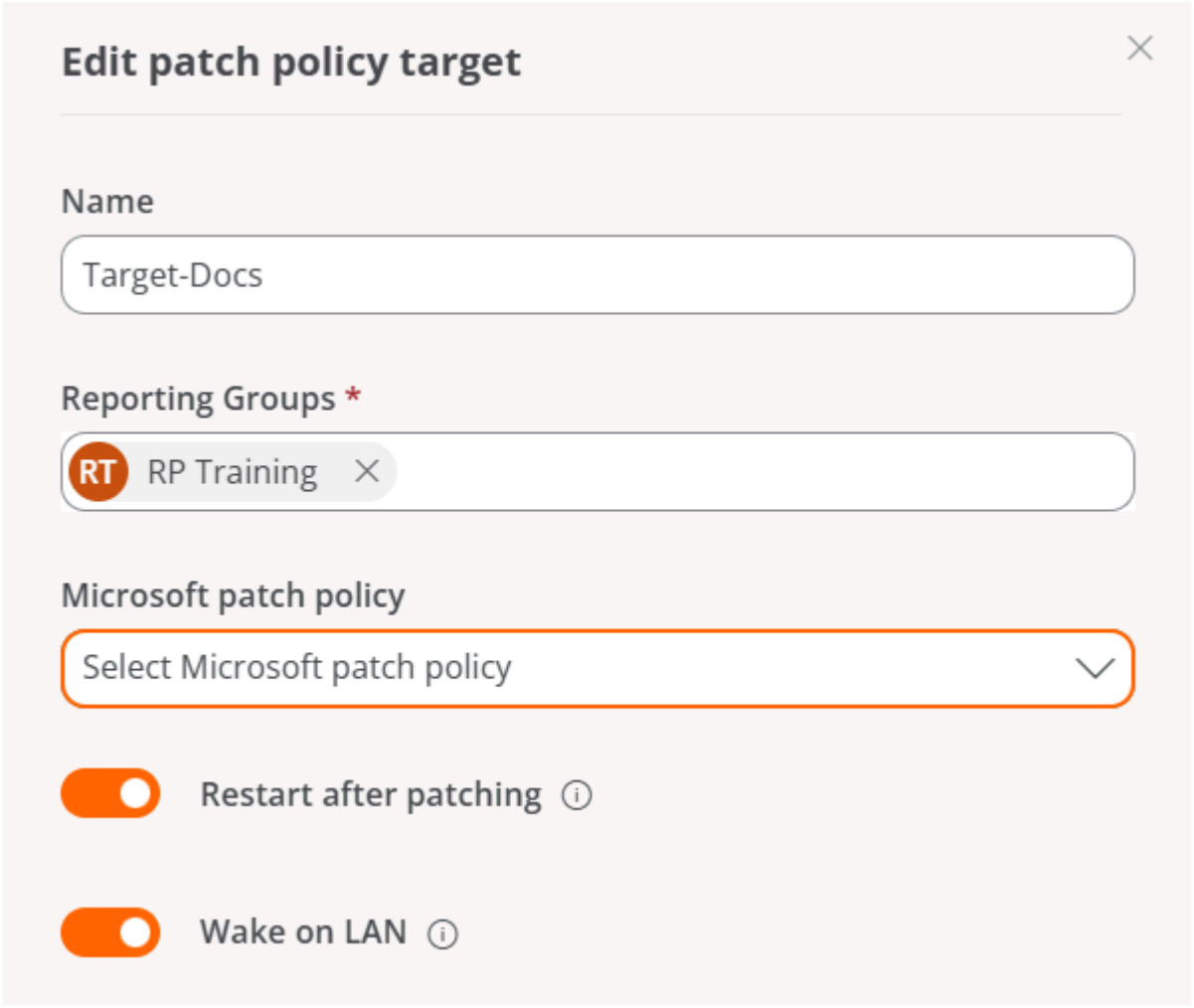
Edit a patch policy

Once created, patch policies can be modified to define device behavior after updates, including options like automatic reboot or remote startup via Wake on LAN (WoL).

1. Access `Portal` -> `Patch` -> `Targets`.
2. In the table, select the patch policy you wish to edit.
3. Click on `Edit`.
4. Optionally, you can enable the following features:

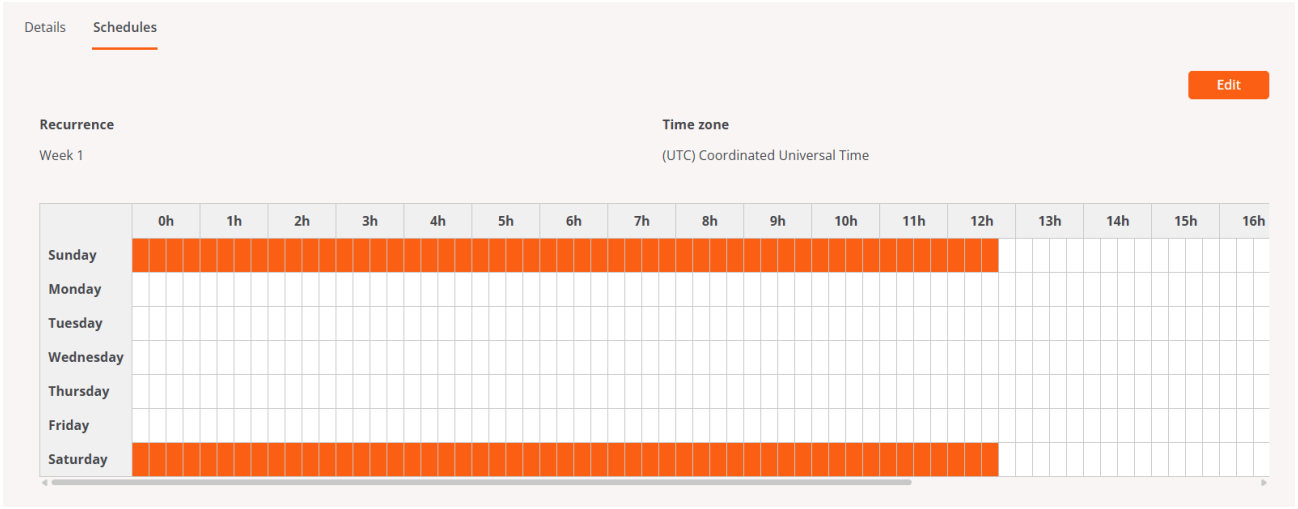
- `Restart after patching`. Enable automatic device restart after patch installation is completed.
- `Wake on LAN (WoL)`. Allows updates to run even when devices are in sleep or powered off modes. The system will automatically wake up over the network to apply the updates.

5. Click on `Save`.



Schedule patches

The patch policy allows scheduling the day and time for applying patches on devices associated with a report group, facilitating controlled maintenance.



1. Access `Portal` -> `Patch` -> `Targets`.
2. In the table, select a patch policy.
3. Click on the `Schedule` tab -> `Edit`.
4. Define the schedule.
5. Click on `Save`.

Delete a patch policy

1. Access `Portal` -> `Patch` -> `Targets`.
2. In the table, select the patch policy you wish to edit.
3. Click on `Edit` -> `Delete`.

> **TIP**
>
> For more information about **update policies**, please consult their documentation.

Microsoft patch policy

The previous steps detailed how to configure the timing, method, and targets of the patches. The process of approving or denying one or more patches from the Microsoft catalog is described below.

Create a new Microsoft patch policy

1. Access `Portal` -> `Patches` -> `Microsoft patch policies`.
2. Click `New` at the top right of the interface.
3. Assign a name to the new policy in the form.
4. Click on `Save`. The name of the policy you just created will appear in the table.

Approve or reject a Microsoft update

1. Access `Portal` -> `Patches` -> `Microsoft patch policies`.

2. In the table, select the Microsoft patch policy you want to view its details.

3. Click on the `Microsoft Updates` tab.

4. In the table, select one or more patches and choose an action:

    - Clicking `Approve` indicates that the update will be installed on the corresponding devices the next time an update process is executed according to the target configuration.

    - Clicking `Reject` indicates that the update will attempt to uninstall during the next update process on devices that have it installed, in accordance with the target configuration. Not all updates can be uninstalled; the execution of this process depends on the update status of the device and other factors. The result of the process will be available in the corresponding update task.

> **INFO**
>
> If a user defines a Microsoft patch policy but does not approve or reject a patch package manually or automatically, no installation or uninstallation activity will occur on the devices.

Automatic Approvals

It's possible to set up automatic approval rules to apply patches, even more than one within the same patch policy.

Create an automatic approval rule

1. Access `Portal` -> `Patches` -> `Microsoft patch policies`.
2. Click the name of the policy.
3. Go to the `Automatic Approvals` tab.
4. Click `New` and define the following fields:

- **Classifications.** Distinguish updates by their category: *Updates*, *Critical Updates*, *Security Updates*, *Upgrades*, *Definition Updates*, *Drivers*, *Feature Packs*, and *Update*

Rollups.

- **Products.** Allows selection of the Microsoft product to which the update applies.
- **Days after release.** Specify how many days after the release date the update will be automatically approved.

> **INFO**
>
> Flexxible recommends setting automatic approval rules whenever a new update policy is created, and not applying the new policy to the desired target until the updates you want as a starting point are approved. In this way, you can start from a scenario where all previous updates are approved for user devices.

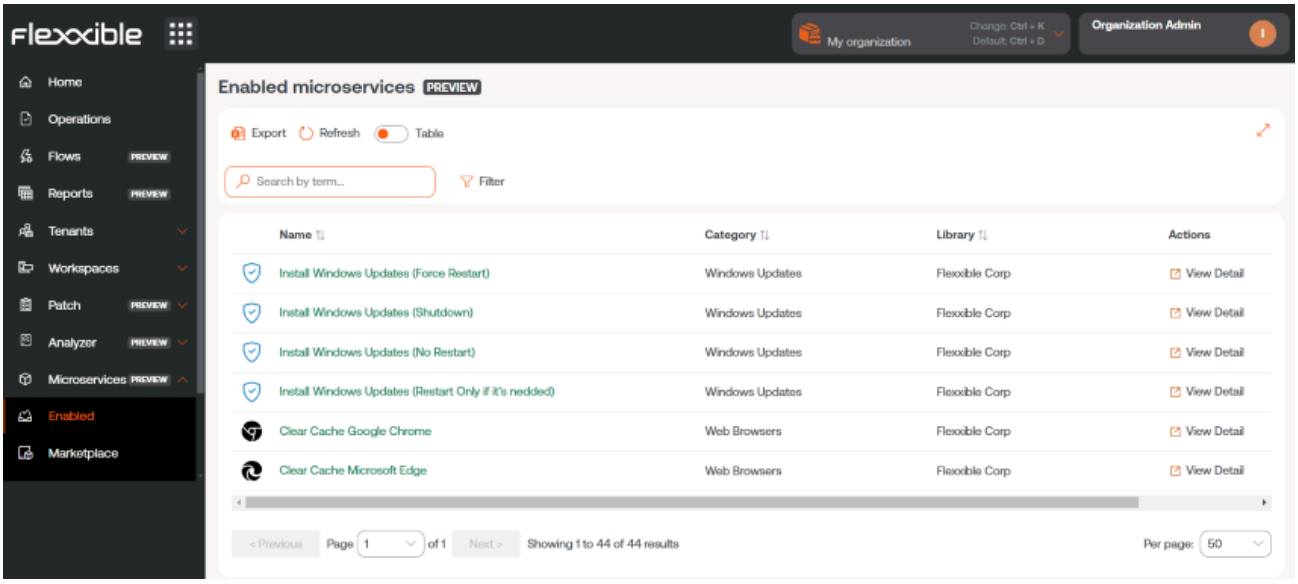
> **TIP**
>
> For more information about **Microsoft update policies**, please consult their documentation.

Portal / Guides / Enable microservices for the end user

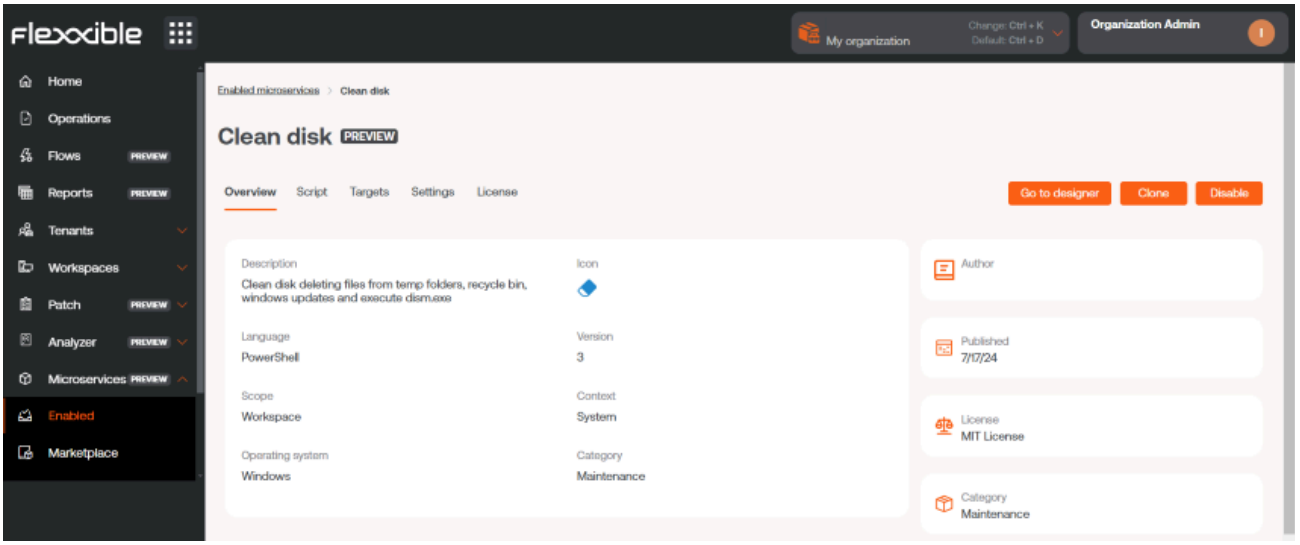
Microservices allow actions (queries or corrections) to be performed on devices, giving the end-user the ability to run them on-demand.

How to enable a microservice for the end-user

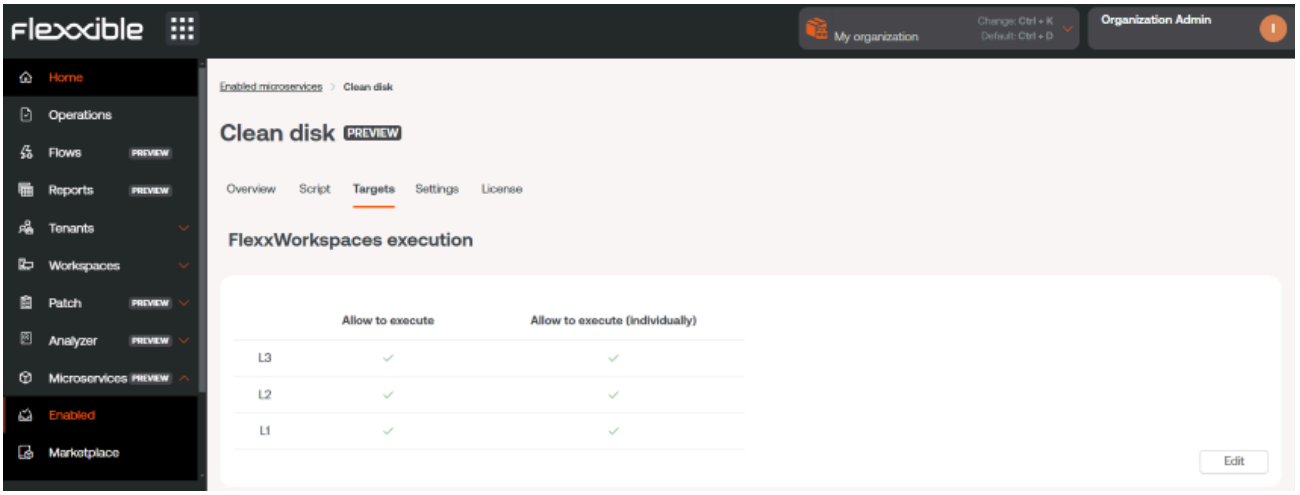
1. Access the `Microservices` -> `Enabled` menu within the Flexxible Portal (microservices can be organized either in blocks or lists).



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”).

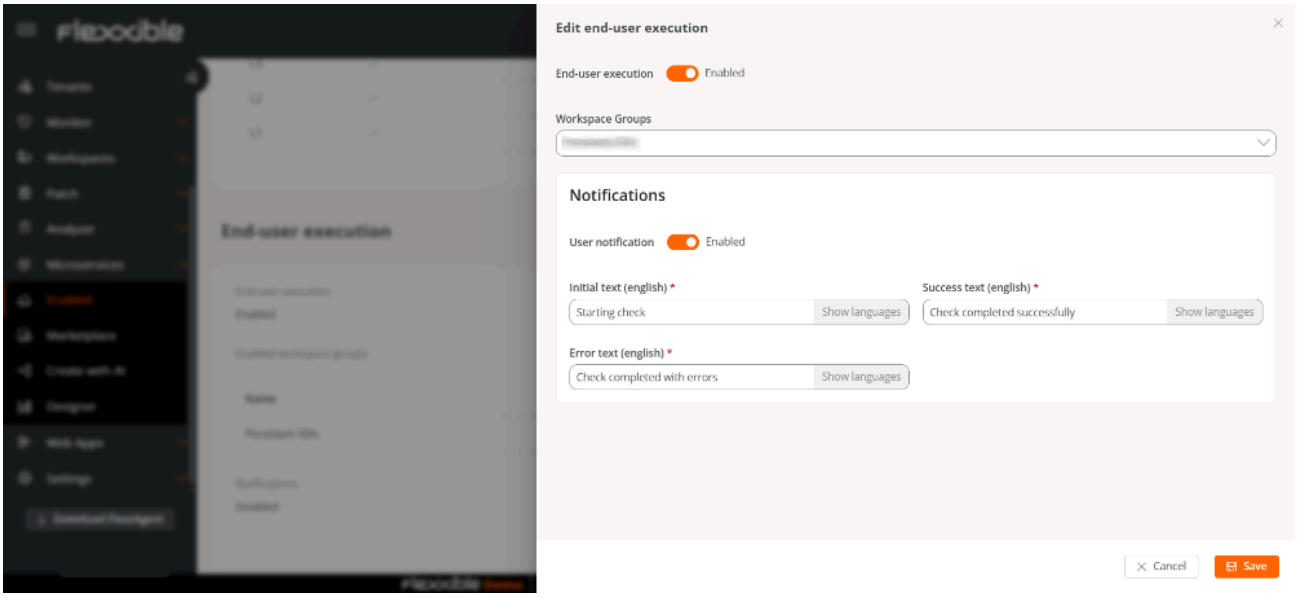


3. Select the `Targets` tab, which shows the execution permissions and recipients of this microservice.



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.



Optionally, notification reception can be configured.

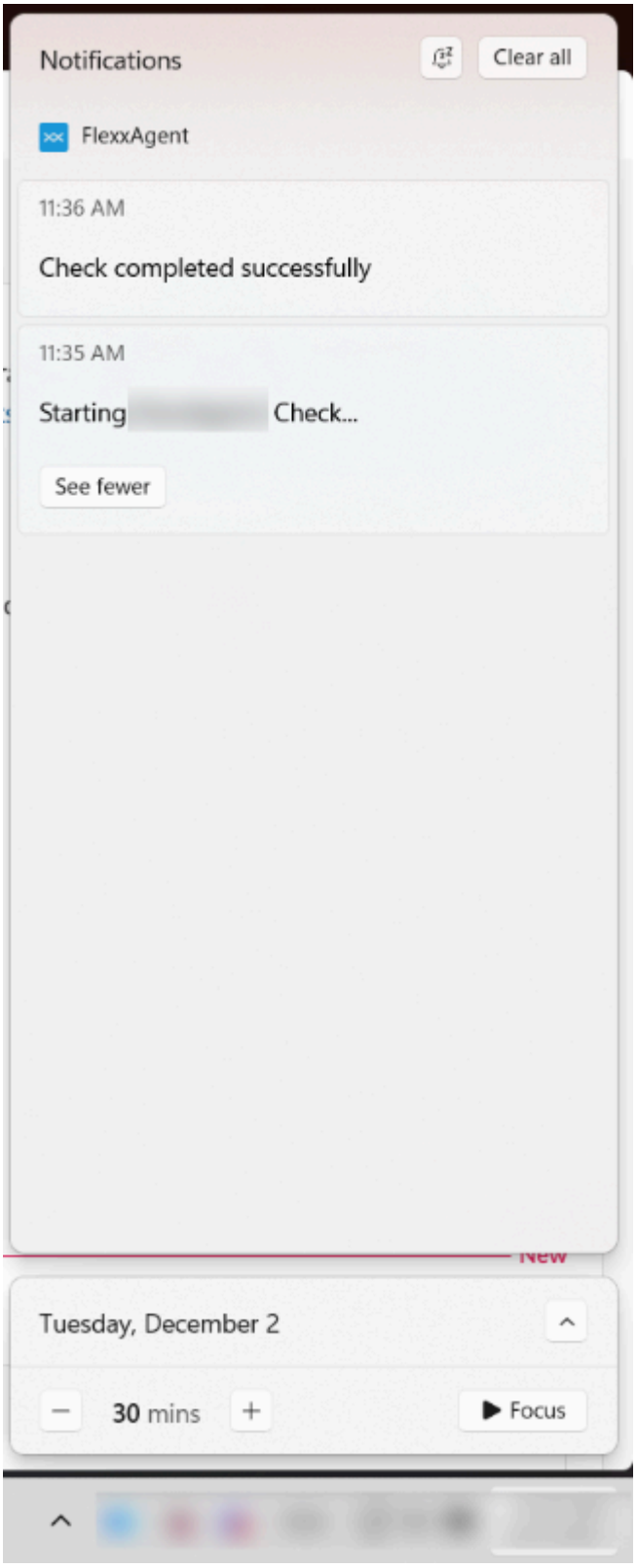
Notifications

This option lets you decide whether to notify the user when the microservice starts executing and when it finishes, whether successfully or with errors.

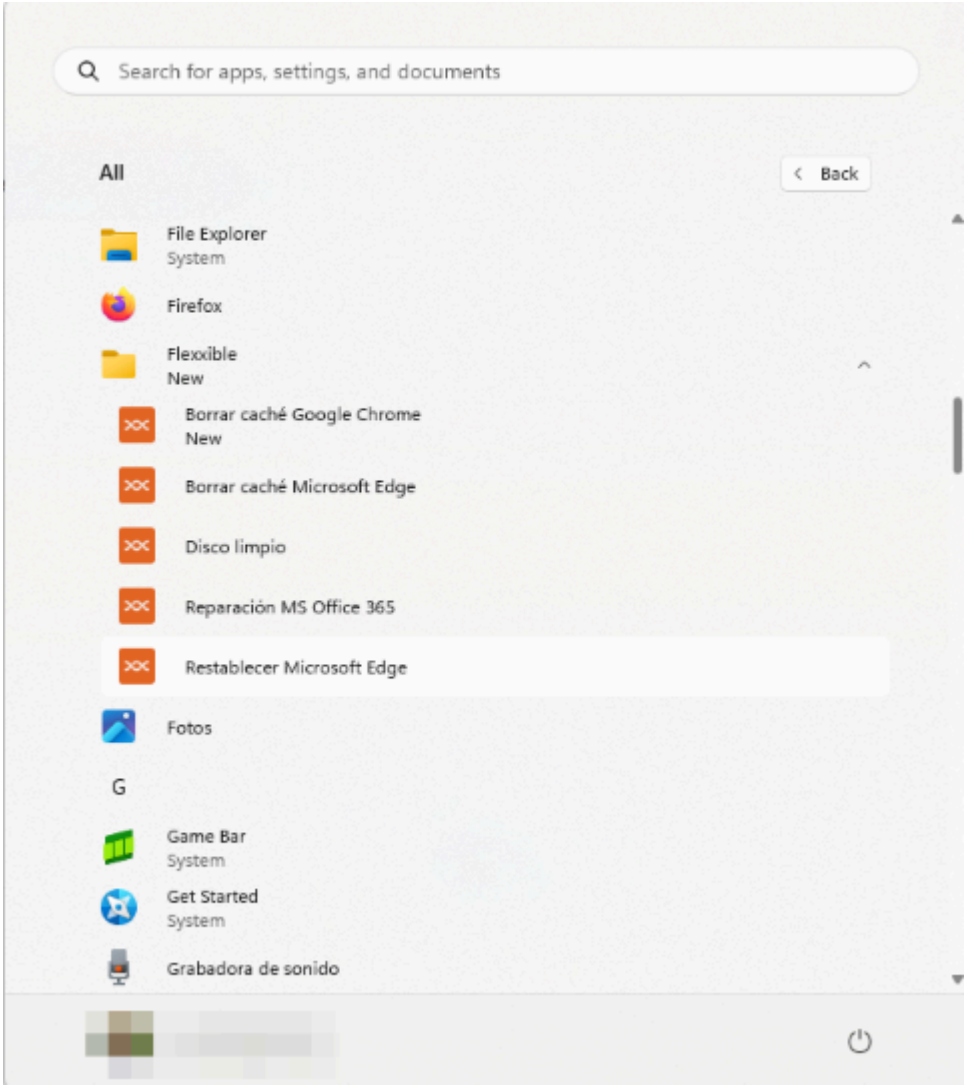
To do this, `User Notification` must be activated and the following fields completed:

- **Initial text.** Message displayed at the start of the microservice execution.
- **Success text.** Message displayed when execution completes successfully.
- **Error text.** Message displayed when execution ends with errors.

Notifications will appear in the Windows notification bar.



6. After clicking `Save`, within the next few minutes, the new microservice will appear as a new operating system option in the *Flexxible* folder on the Start menu.



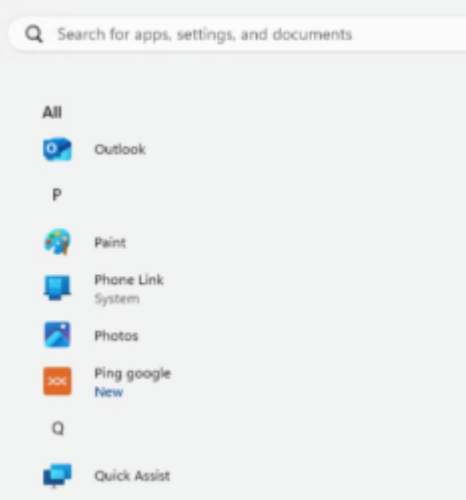
Rename the microservices folder

1. Go to `Portal` -> `Settings` -> `Organization`.
2. In the left side menu, select `Microservices` -> `Edit microservices settings`.
3. Rename the folder.
4. Click on `Save`.

Considerations

- The chosen name must be between 3 and 50 characters, and can only contain letters, numbers, hyphens, and underscores.
- If the device has Windows 11 as the operating system and only one microservice is enabled for an end user, the *Flexxible* folder will not appear; instead, only the

microservice icon will be visible in the start menu.



INFO

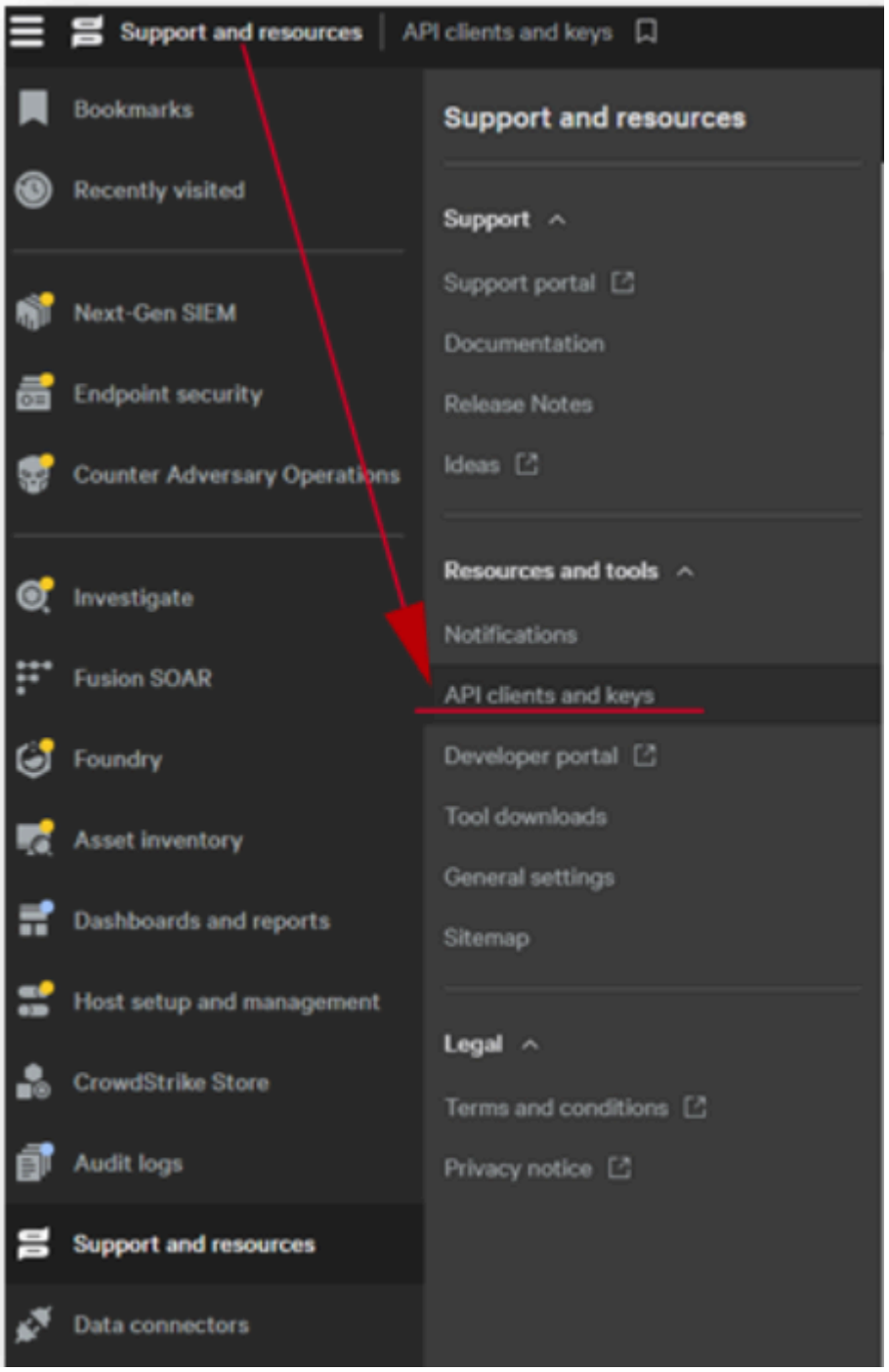
For more information about Microservices, please refer to its documentation.

Portal / Guides / Set up integration with CrowdStrike

This guide details the processes for establishing CrowdStrike integration on the Flexxible platform.

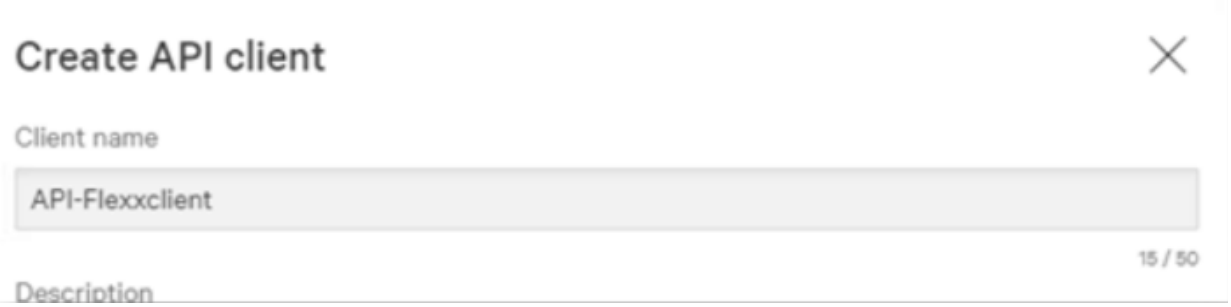
API Configuration in CrowdStrike

1. Access the CrowdStrike portal.
2. In the menu, click on `Support and Resources` -> `Api clients and keys`.



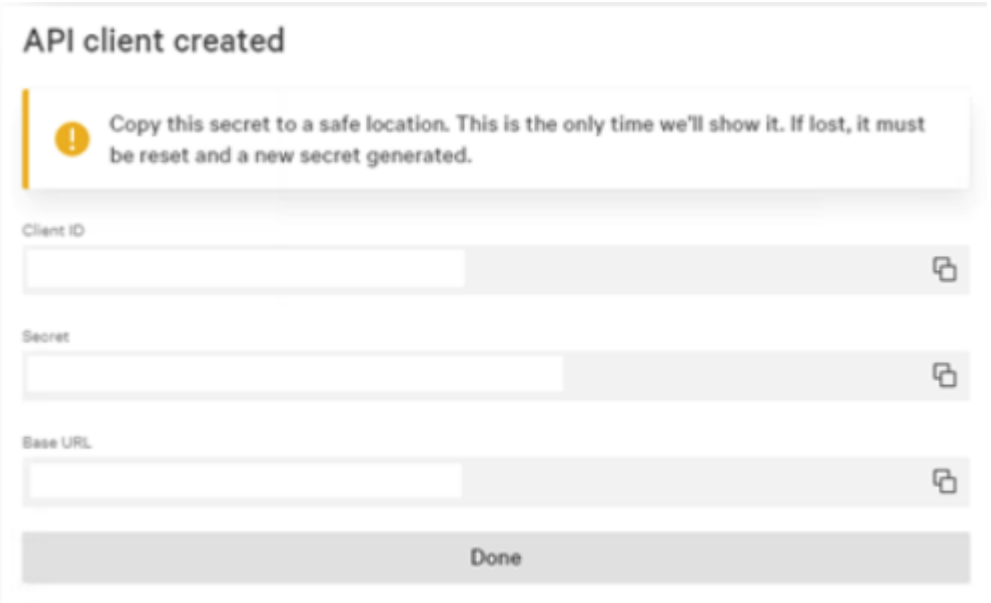
3. Select `Create API client` on the right side of the menu.

4. Assign a name to the API; the standard is *API-Flexxclient*.



5. Without leaving the menu, select the following fields in the *READ* column:
    - Alerts
    - Detections
    - Hosts
    - Incidents
    - Quarantined Files
6. Click on `Create`.

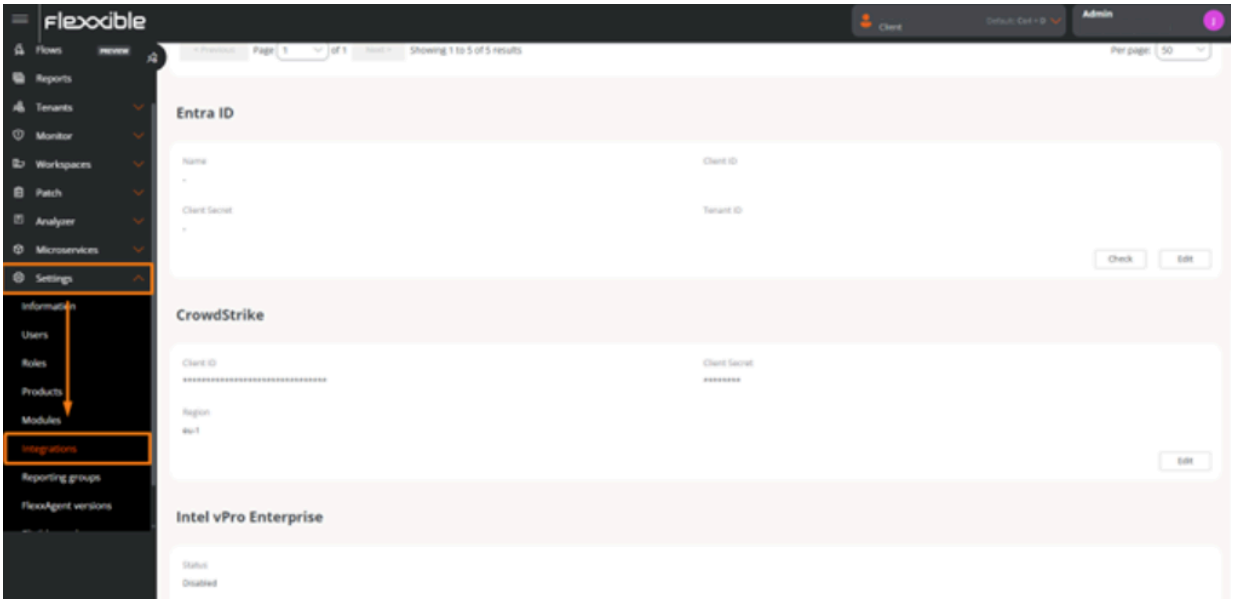
7. Copy the following three fields (they cannot be retrieved later).
    - Client ID
    - Secret
    - Base URL



Configuration in Portal

To perform the integration from Portal, the user must have at least the role of *Organization Administrator*.

1. Log in to Portal.
2. In the user menu, select the organization/tenant where you want to enable the integration.
3. Go to `Settings` -> `Integrations` -> CrowdStrike section.



4. Click on `Edit` and enter the following information:

- **API Client ID.** Unique identifier that represents the client on the CrowdStrike platform.
- **Secret String.** Secret key associated with the client ID.
- **Region.** Geographic location of the customer's cloud environment. The field offers options like *eu*, *eu-1*, *us-gov-1*, *us-1*, and *us-2*. Select the CrowdStrike region.

5. Click on `Save`.

> **INFO**
>
> Integration with CrowdStrike can be done at the tenant level, allowing you to set up a different account for each one. If the integration is done at the organization level, it will extend to all its sub-organizations.

View from Workspaces

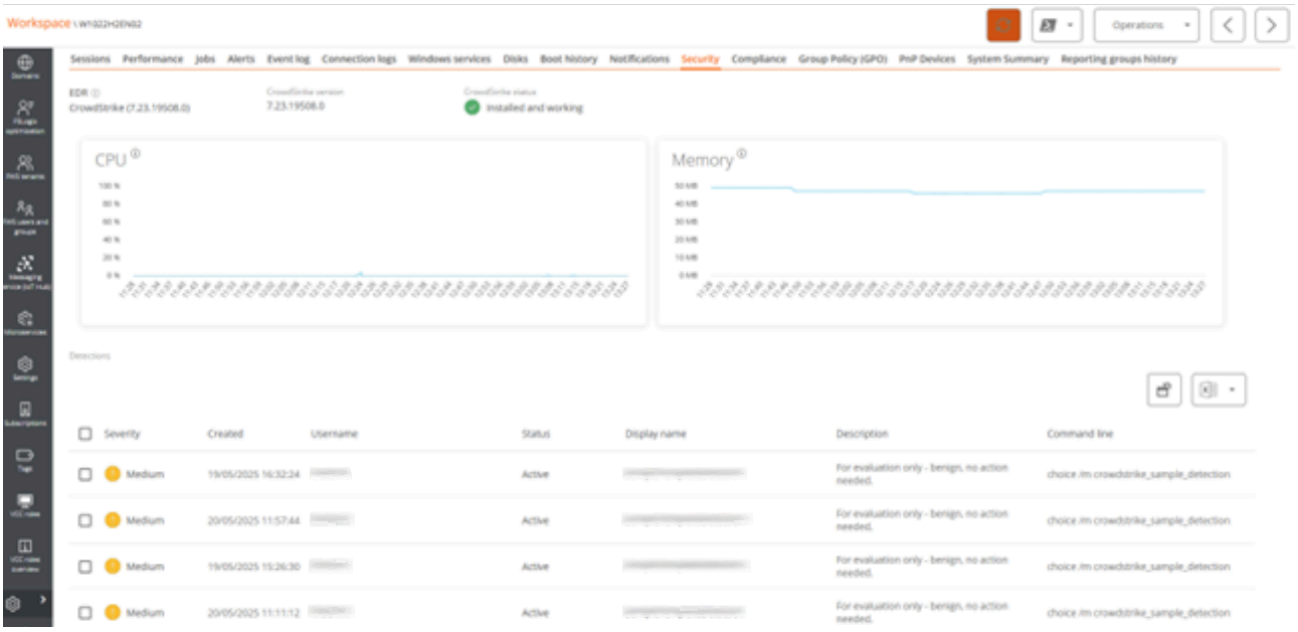
Once the integration is set up, devices with Endpoint Detection and Response (EDR) installed and running will be marked with the Falcon icon.

If the EDR generates an alert, the Falcon icon will appear red.

Alert Details

To review the details of the alerts and the resource consumption of the EDR, follow these steps:

1. Access the Workspaces module -> `Workspaces`.
2. Choose a device and click on it.
3. Scroll down and click on the `Security` tab.



Portal / Guides / Configure integration with Entra ID

This guide details the processes necessary to establish integration with Entra ID on the Flexxible platform.

Requirements for integration

For the integration to work correctly, the application ID (App ID) requires Global Reader permission at the Microsoft Entra ID level, Contributor permission at the Azure subscription level, and Owner permission in the resource group where Workspaces is deployed.

Configuration in Microsoft Azure

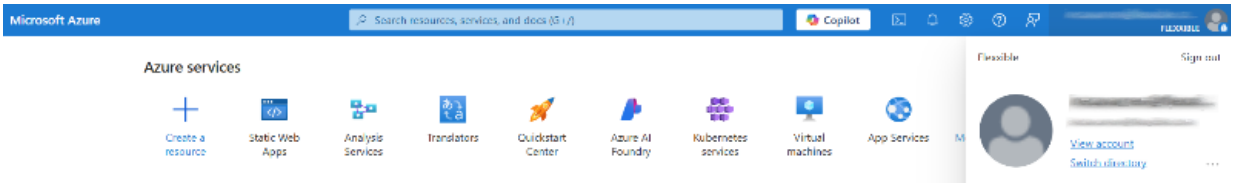
Integration with Entra ID requires the following steps to be followed in the Microsoft Azure environment:

- Create an application registration
- Create a client secret
- Configure permissions for the application registration
- Permissions in the Azure subscription

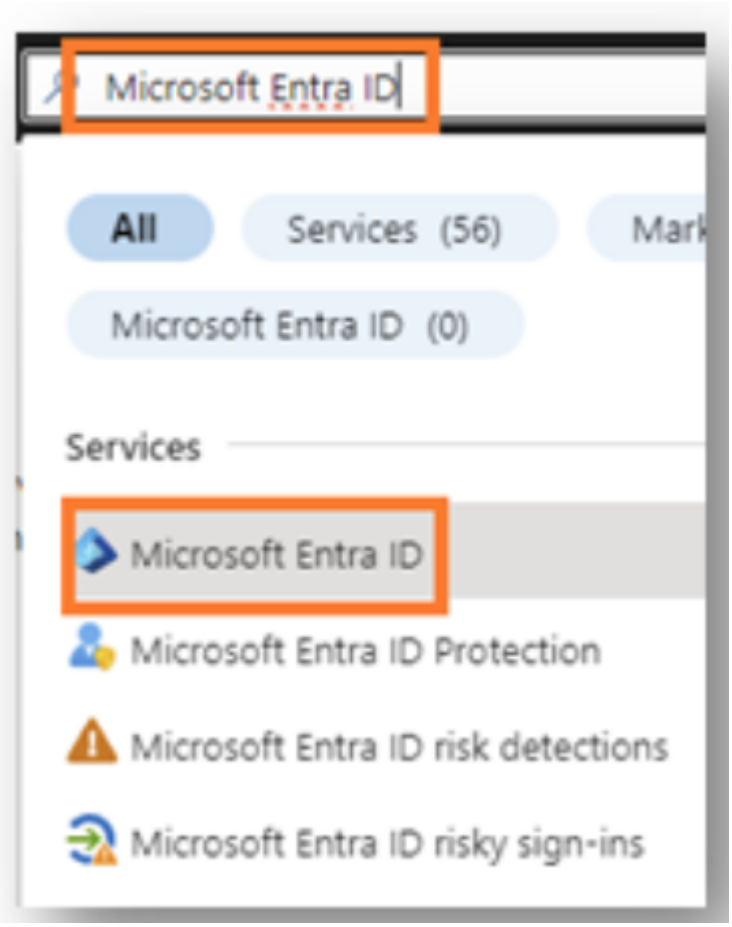
Create an application registration

1. Log in to Azure Portal.

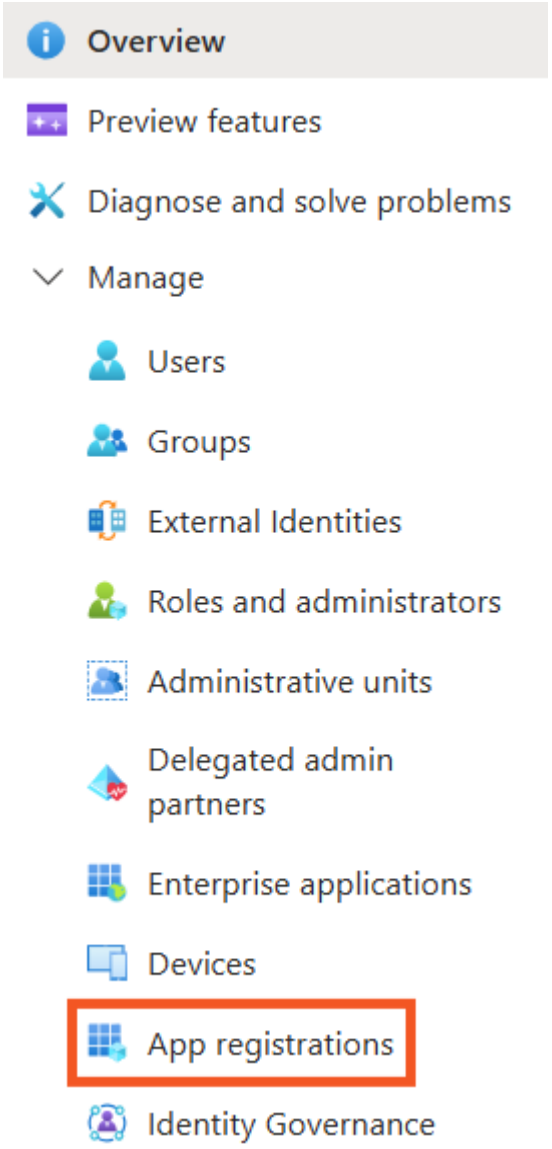
2. Select the tenant if you have access to multiple; to do this, click on `Switch directory` in the user menu.



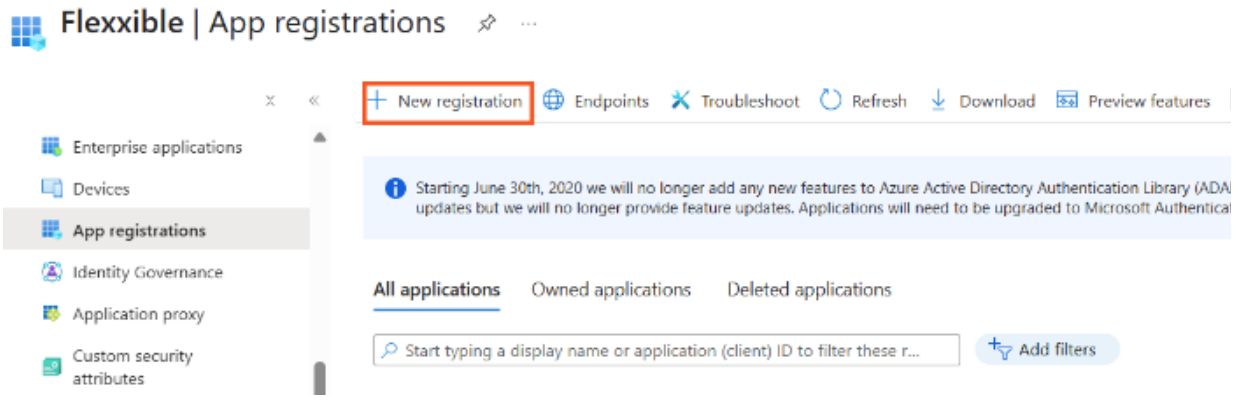
3. Once the subscription is selected, search for *Microsoft Entra ID*.



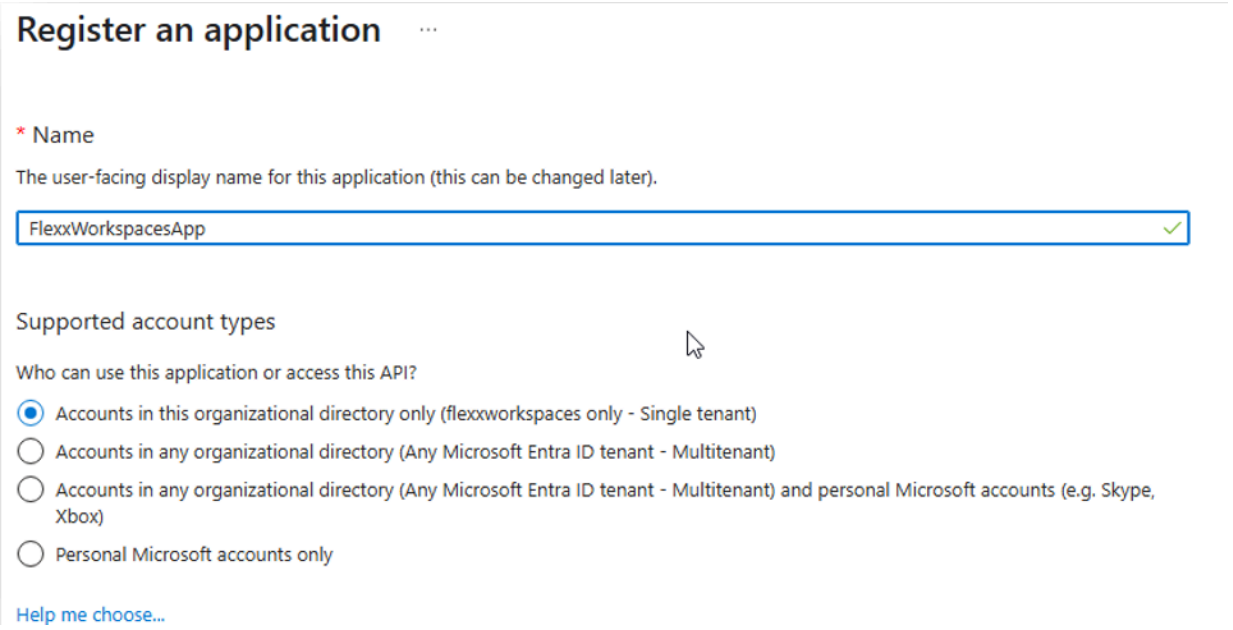
4. To the left of the interface, you will see the following menu:



5. Click `Application registrations` -> `New registration`.

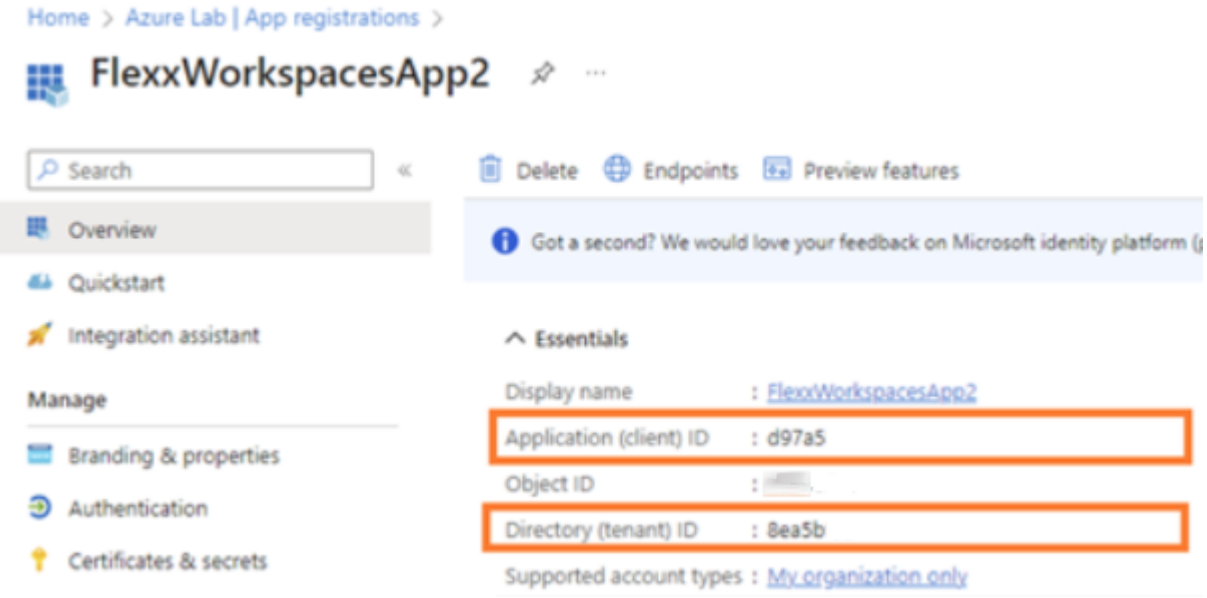


6. Enter a name to register the application and select the supported account type.



7. Click `Register` to complete the application registration.

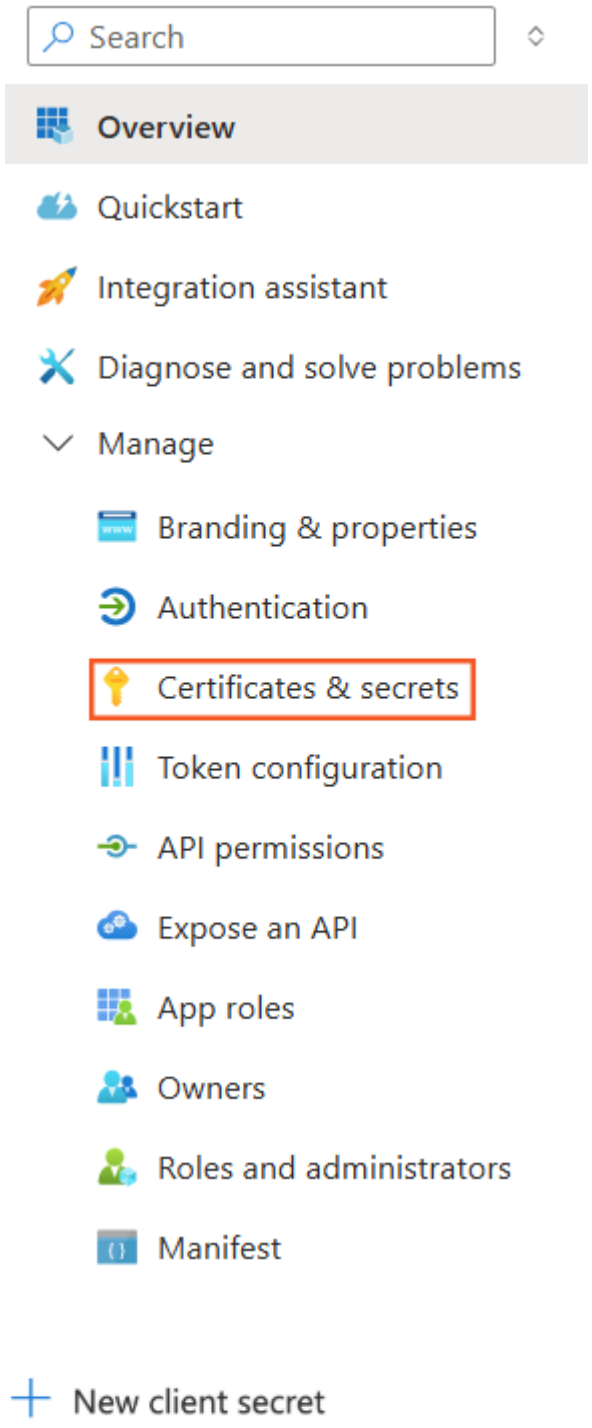
8. Copy and save the Application ID (App ID) and the Directory ID (tenant).



Create a client secret

1. Access `App registrations`.

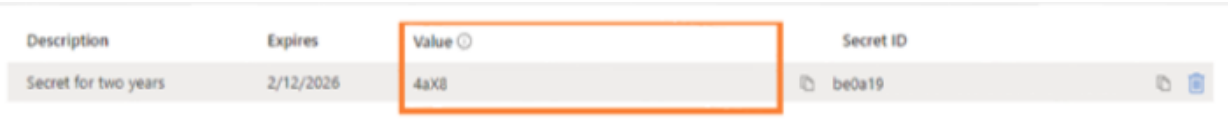
2. In the menu, click `Manage` -> `Certificates & secrets` -> `New client secret`.



3. Add a description and in the *Expires* field, select 24 months.

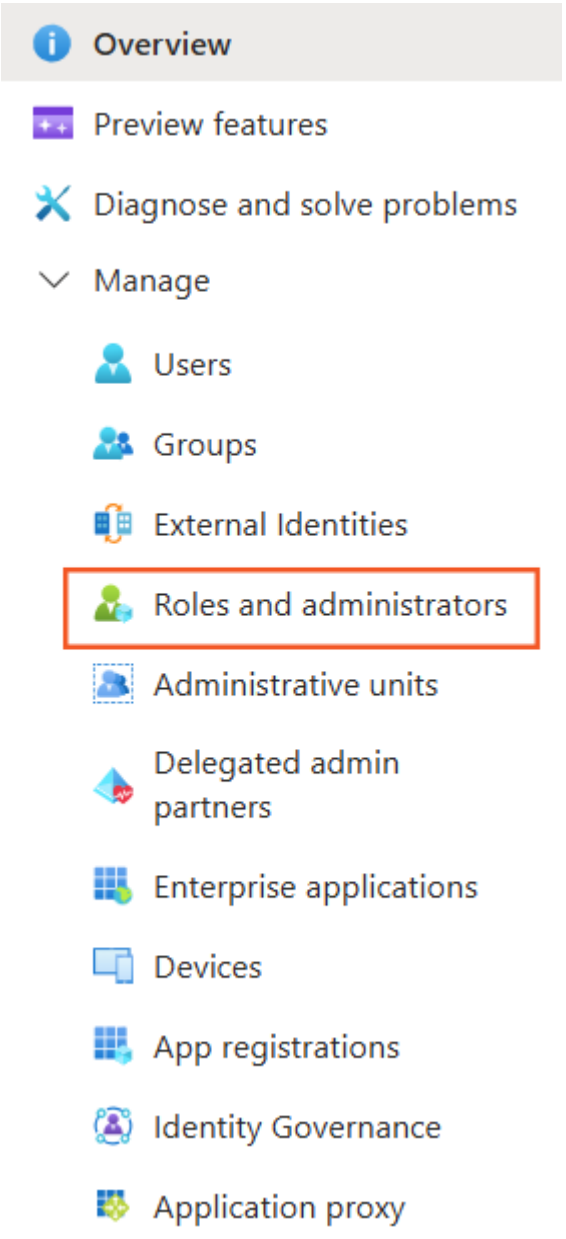
4. Click `Add`.

5. Microsoft will provide the client secret and the client ID. You need to save these values because they will not be shown again. If not saved, the client secret must be deleted and a new one created to obtain the value.

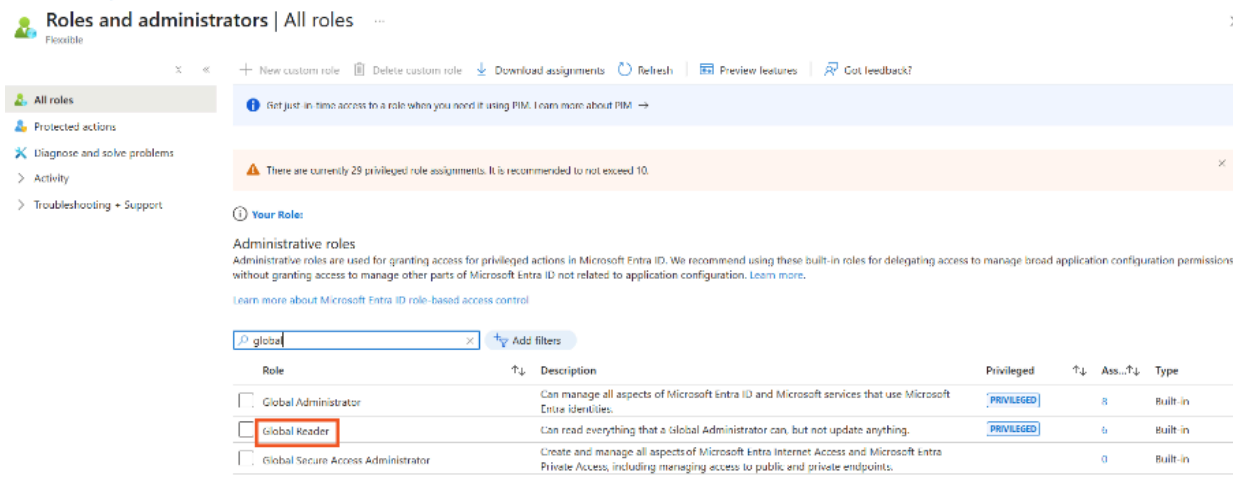


Configure permissions for the application registration

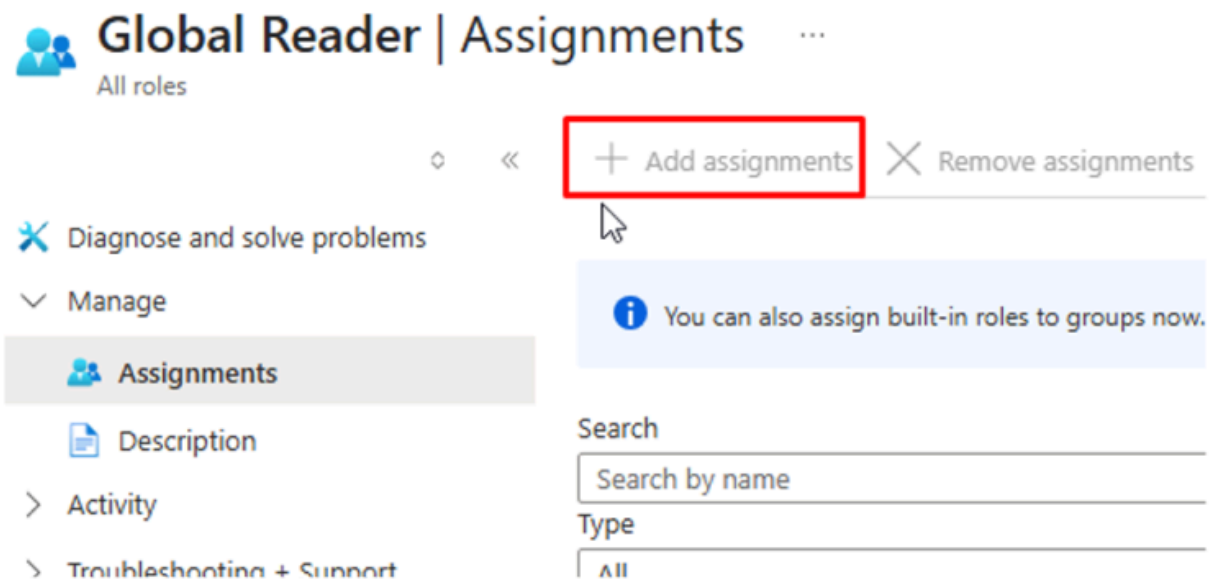
1. Log in to Azure Portal.
2. Click on Microsoft Entra ID.
3. Click `Manage` -> `Roles and administrators`.

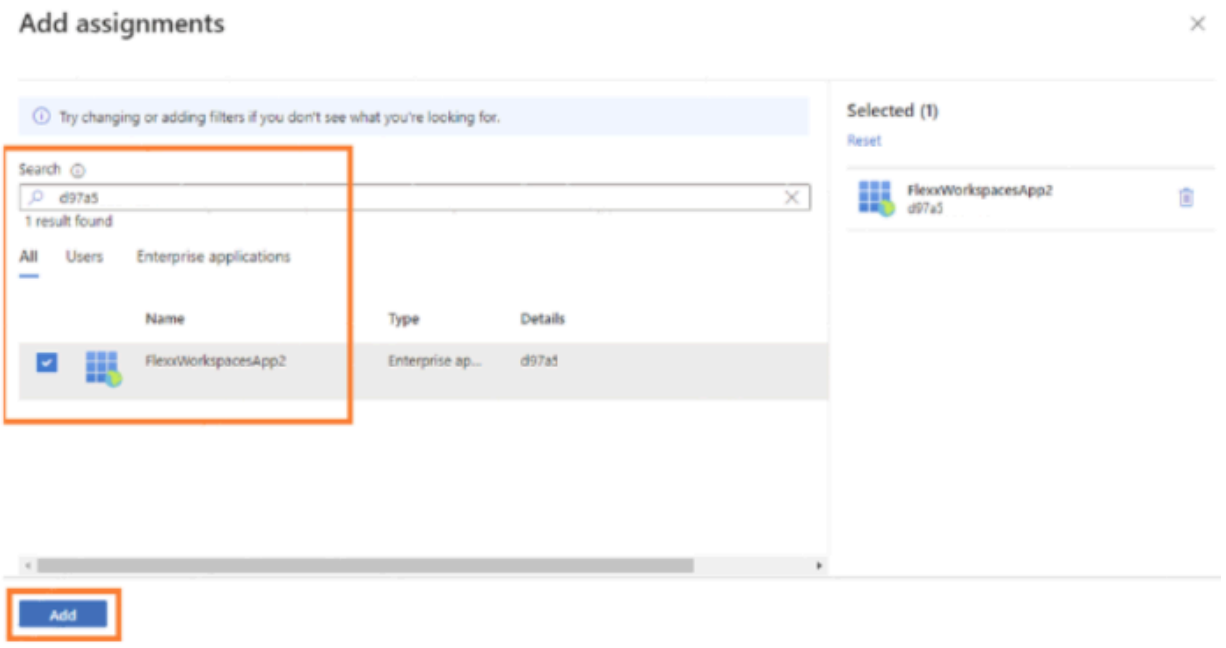


4. Search and select the `Global Reader` option.

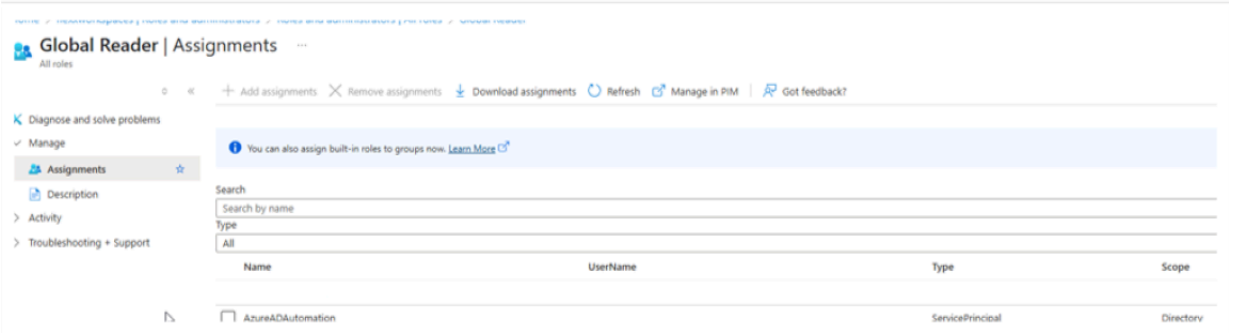


5. Click on `Add assignments` and add the application ID (App ID) created in the previous step.





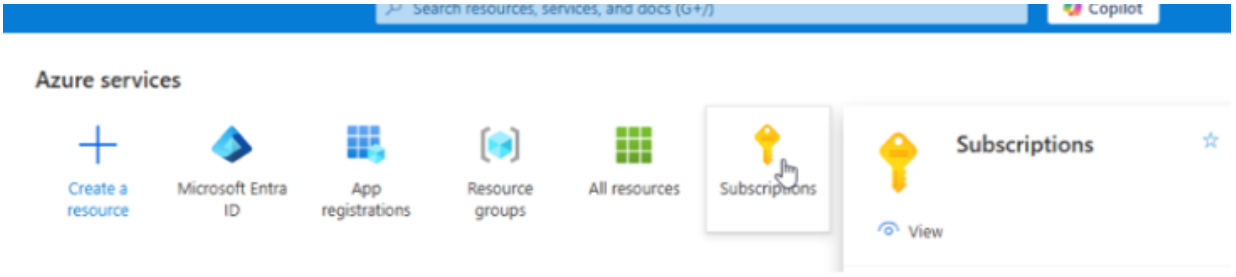
6. Verify that the application is configured on the main dashboard.



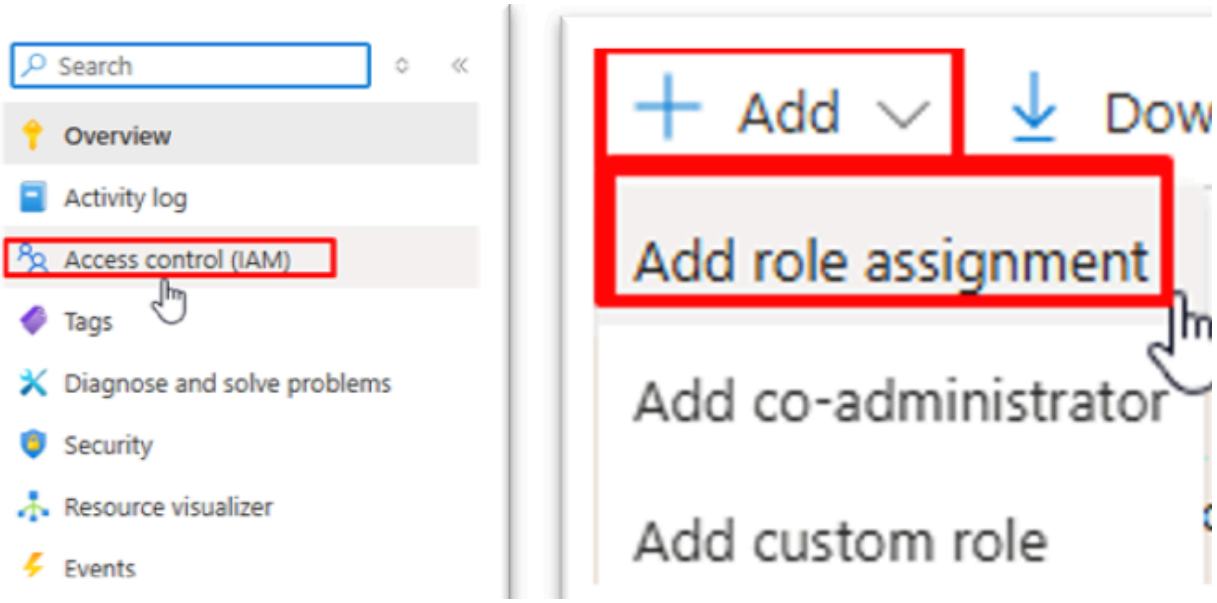
Permissions in the Azure subscription

1. Log in to Azure Portal.

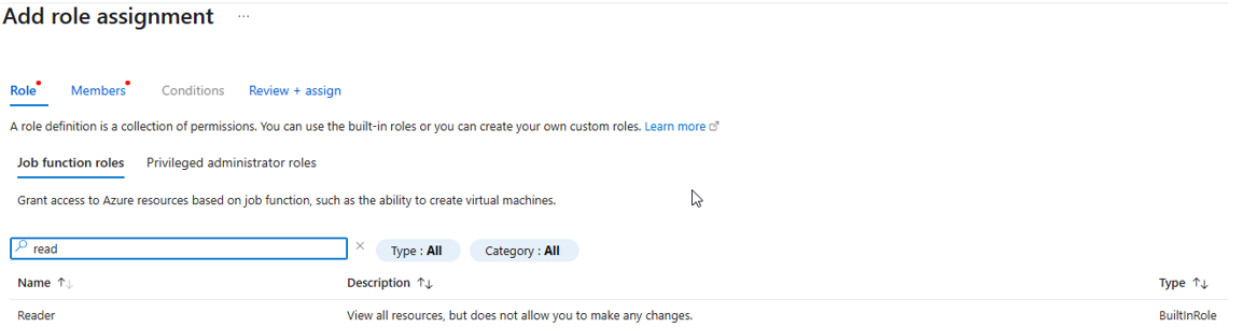
2. Click `Subscriptions`.



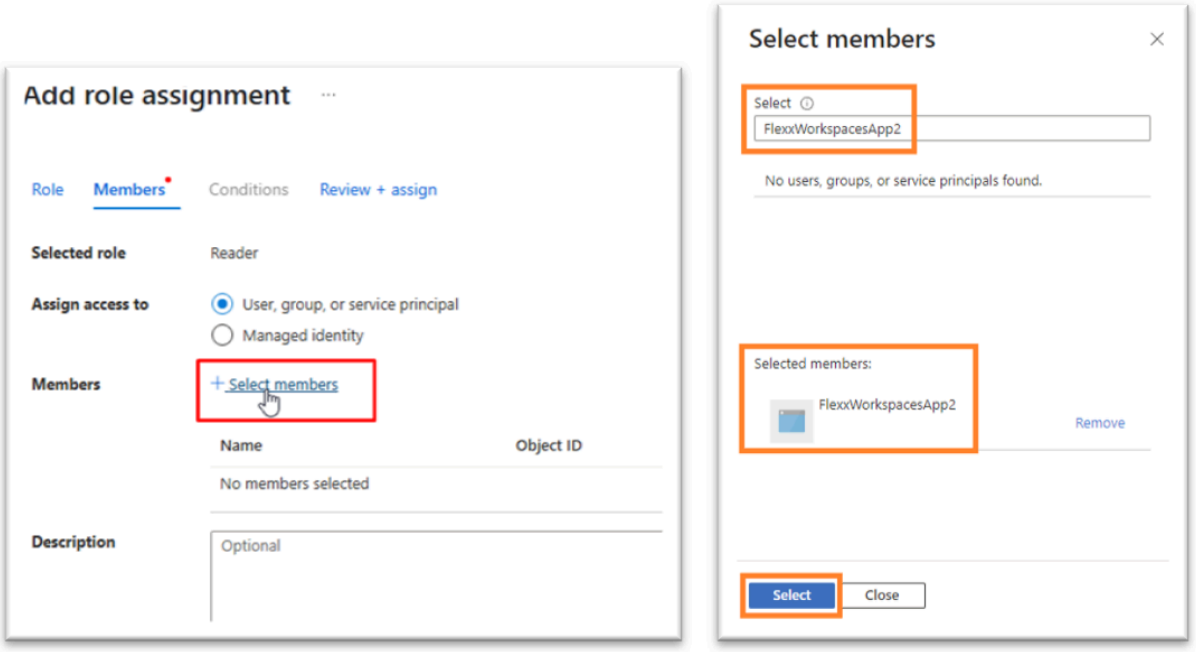
3. Click `Access control (IAM)` -> `Add` -> `Add role assignment`.



4. In `Role` -> `Function role`, search and select `Reader`.



5. In `Members` select the application ID (App ID) created in the previous step.

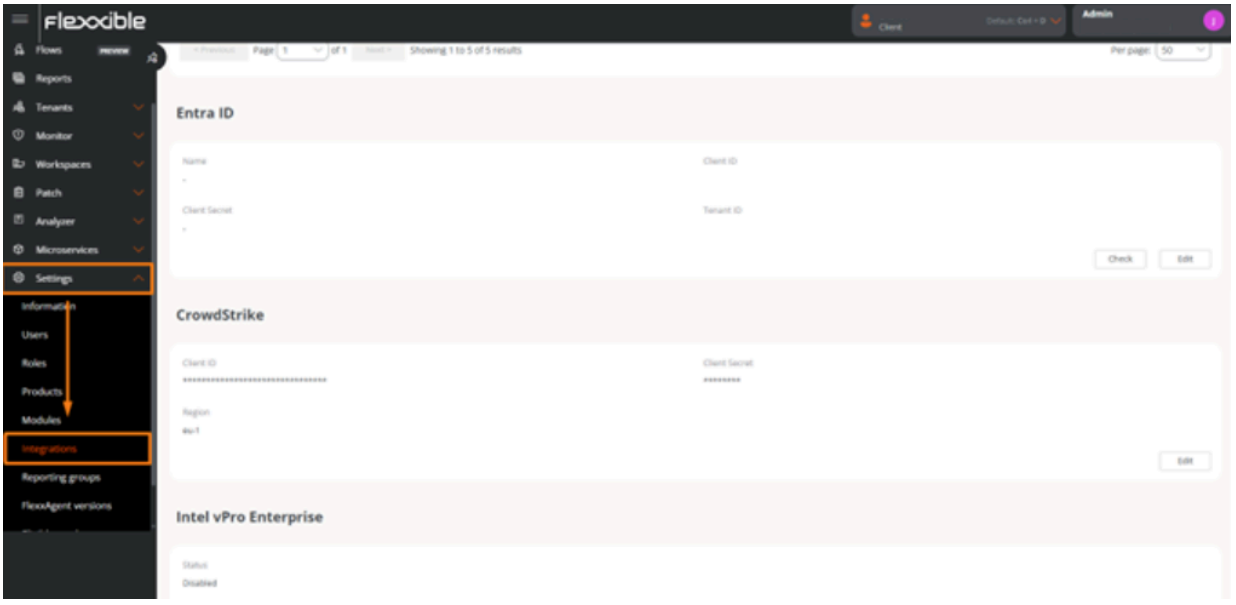


6. Review and assign the role.

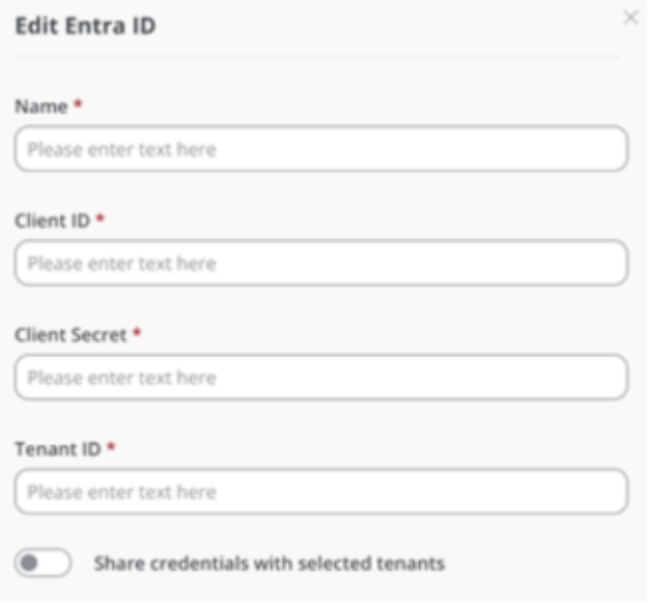
Configuration in Portal

To perform the integration from Portal, the user must have at least the role of *Organization Administrator*.

1. Log in to Portal.
2. In the user menu, select the organization/tenant where you want to enable the integration.
3. Go to `Settings` -> `Integrations` -> Entra ID section.



4. Click on `Edit` and enter the following information:
    - **Id. of application (client).** Client ID.
    - **Secret string.** Client secret used for authentication.
    - **Id. of directory (tenant).** Azure tenant ID.
5. Click on `Save`.



For these credentials to be used in sub-organizations, `Share credentials with the selected tenants` must be enabled; otherwise, new credentials must be created for each sub-organization.

Portal / Guides / Set up Entra ID integration with Monitor

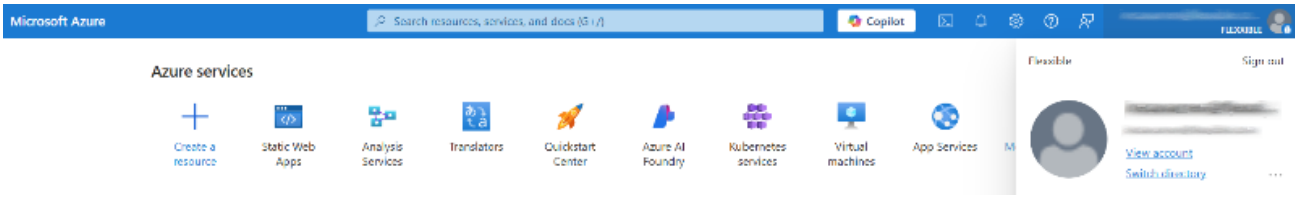
Monitor is the Flexxible monitoring module based on Grafana Cloud. Allows user access by invitation or through integration with Entra ID accounts. This guide describes the steps necessary to establish this integration.

Configuration in Microsoft Azure

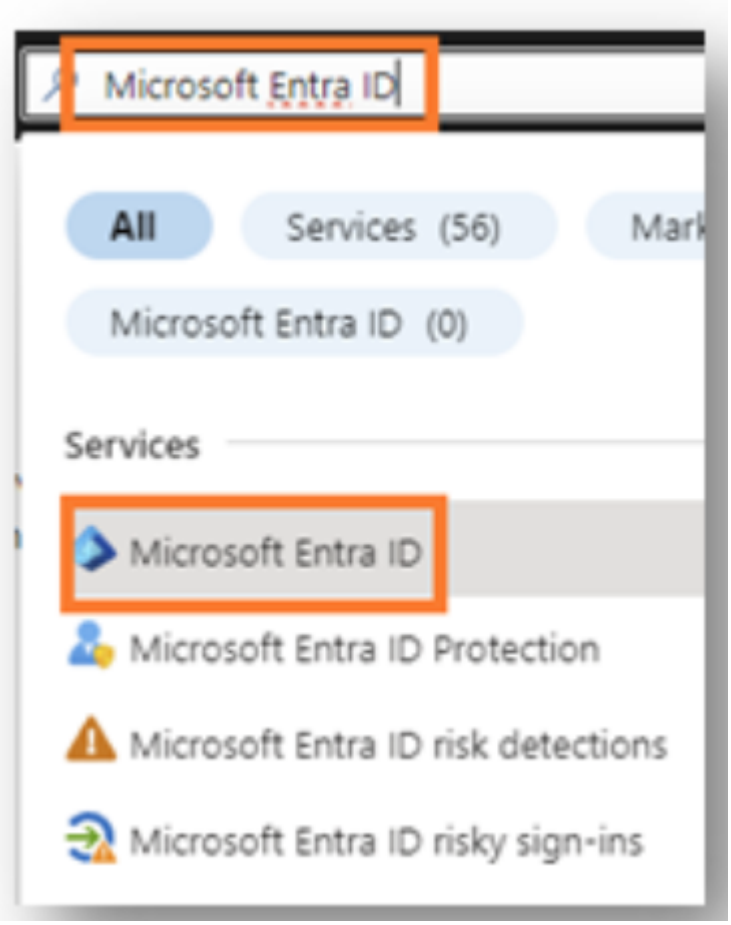
- Create an application registration
- Create a client secret
- API permissions configuration
- Create application roles
- Review the manifest.xml file

Create an application registration

1. Log in to Azure Portal.
2. Select the tenant if you have access to multiple; to do this, click on `Switch directory` in the user menu.

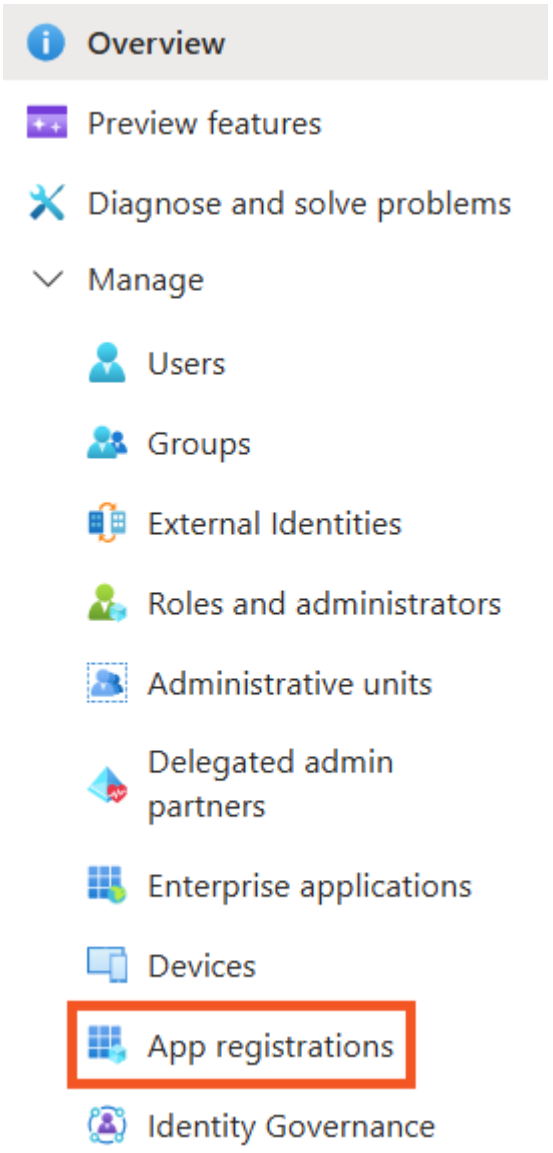


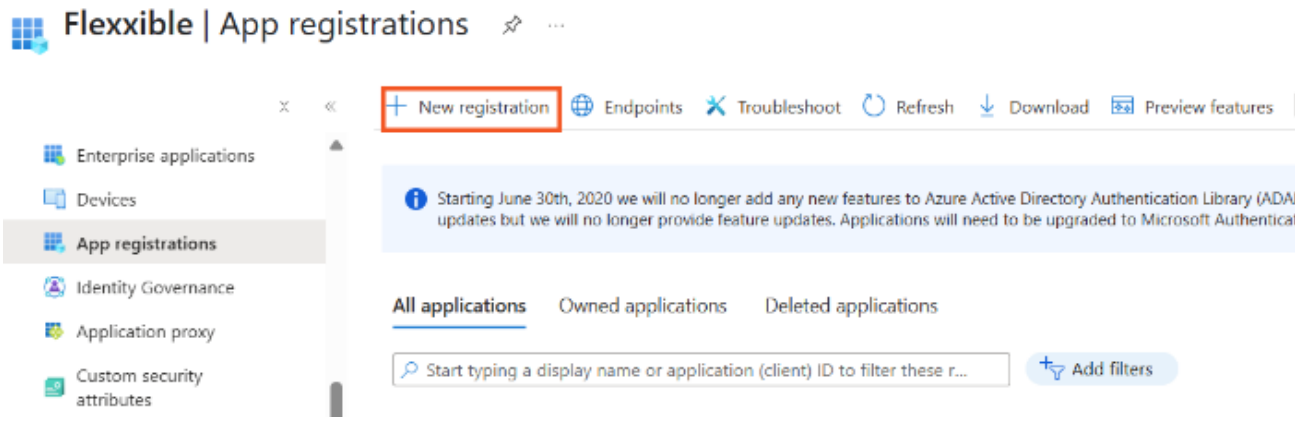
3. Once the subscription is selected, search for *Microsoft Entra ID*.



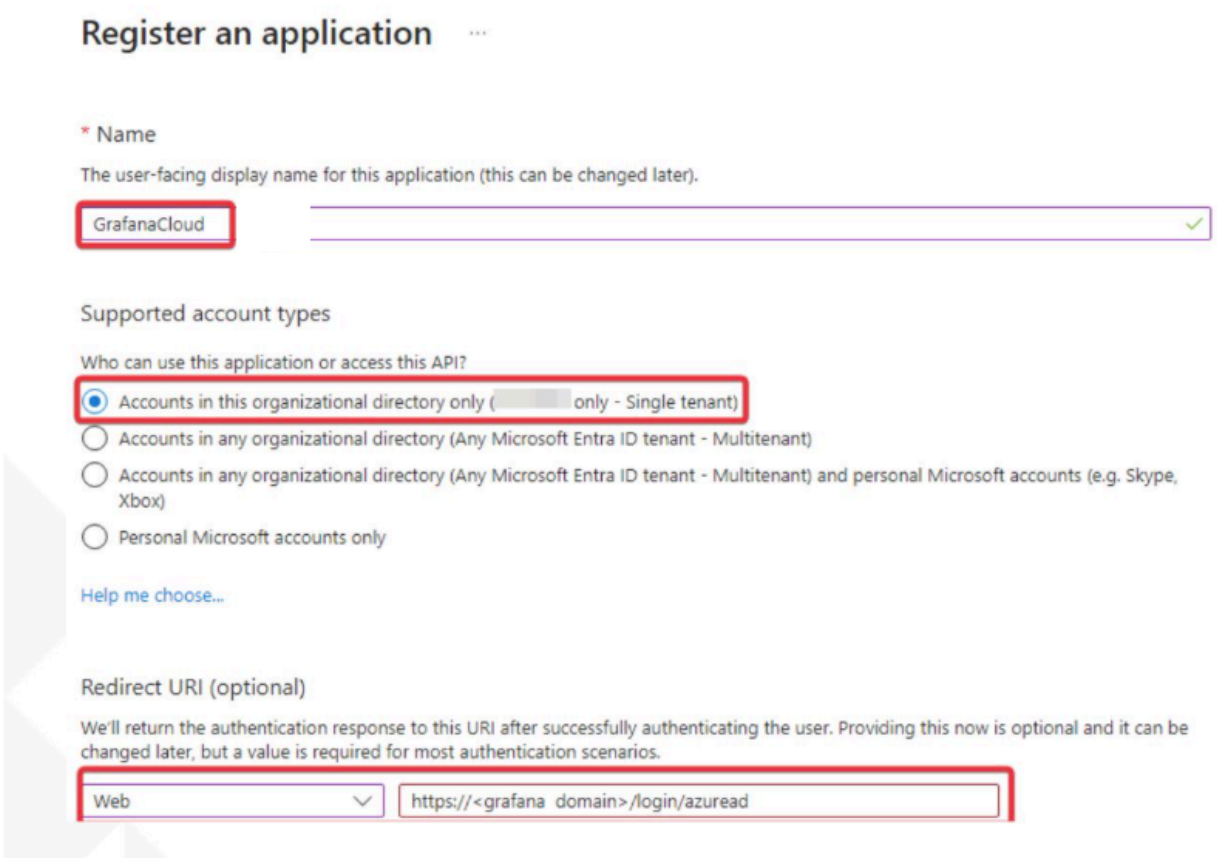
4. To the left of the interface, you will see the following menu:

5. Click `Application registrations` -> `New registration`.





6. Enter a name to register the application and select the compatible account type.



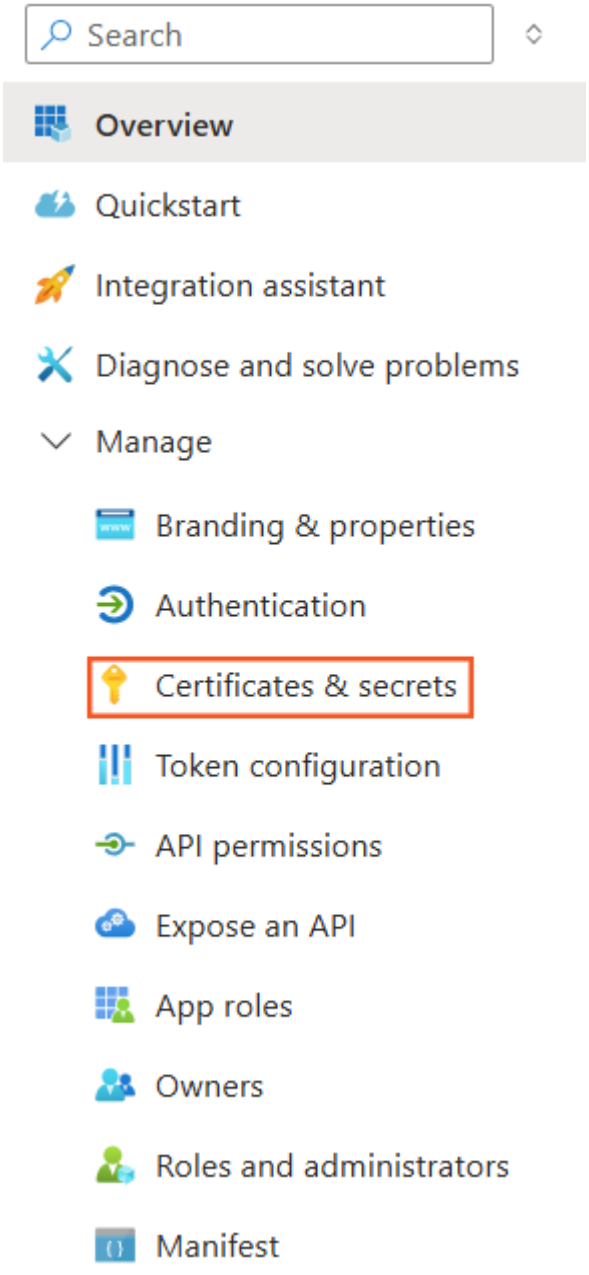
7. In Redirect URI select *Web* and add the following redirect URL:

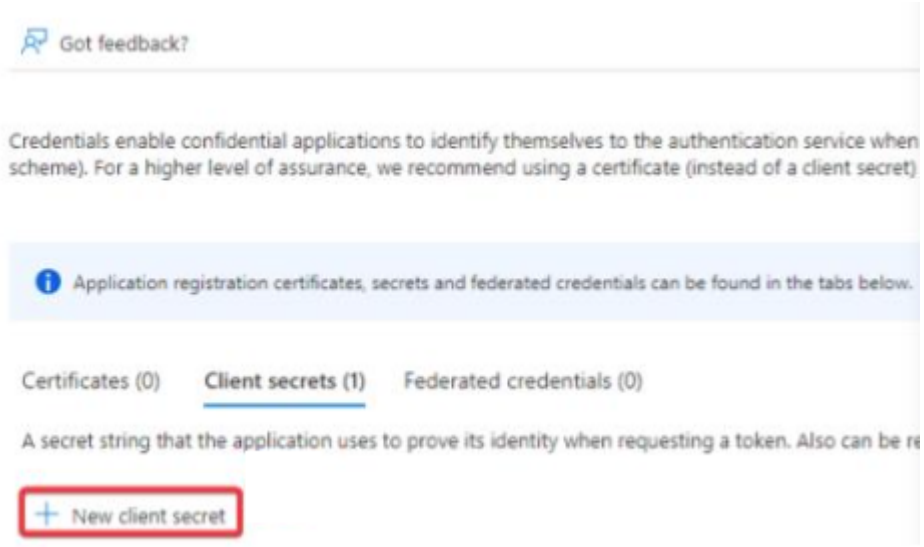
   `https://<grafana domain>/login/azuread`

8. Click `Register` to complete the application registration.

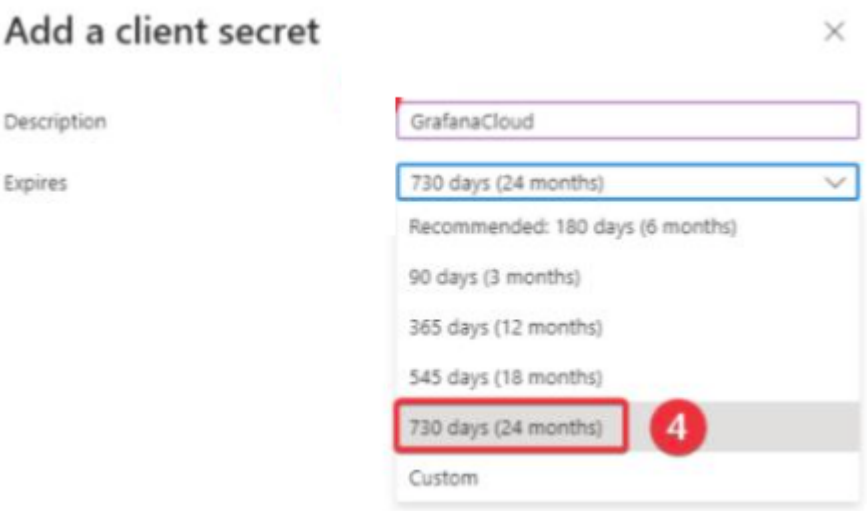
Create a client secret

1. Access `App registrations`.
2. In the registration menu, click on `Manage` -> `Certificates & Secrets` -> `New client secret`.

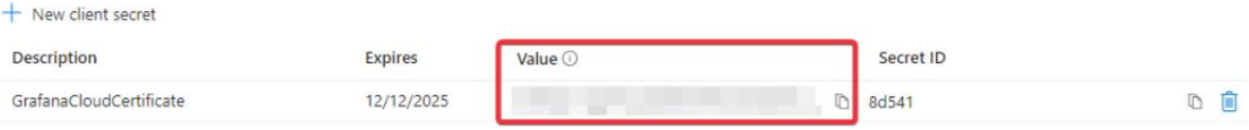




3. In the *Description* field, write GrafanaCloud, and in *Expires* select 24 months.



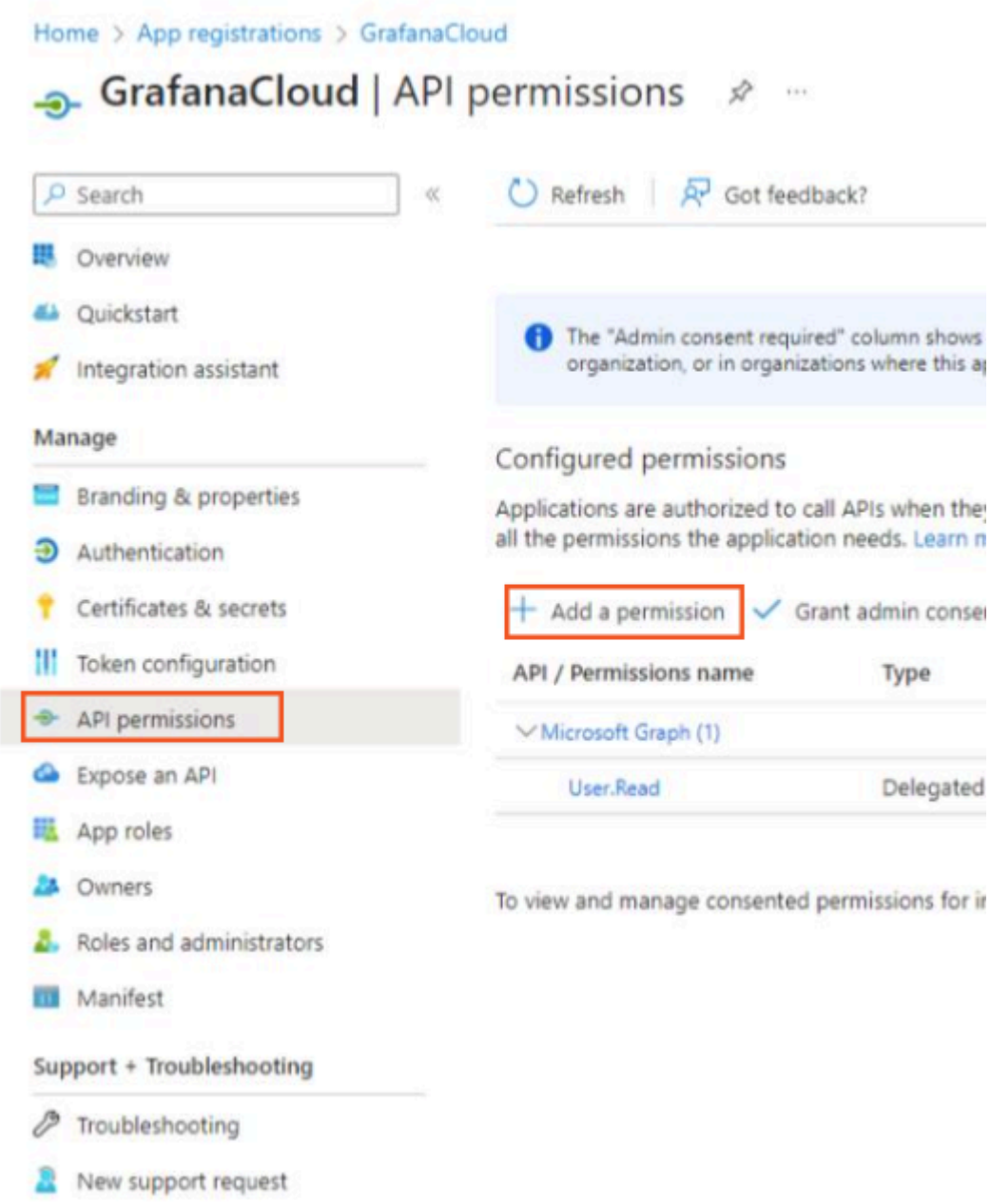
4. Click `Add`.
5. Copy the key value. This is the client secret value for OAuth.



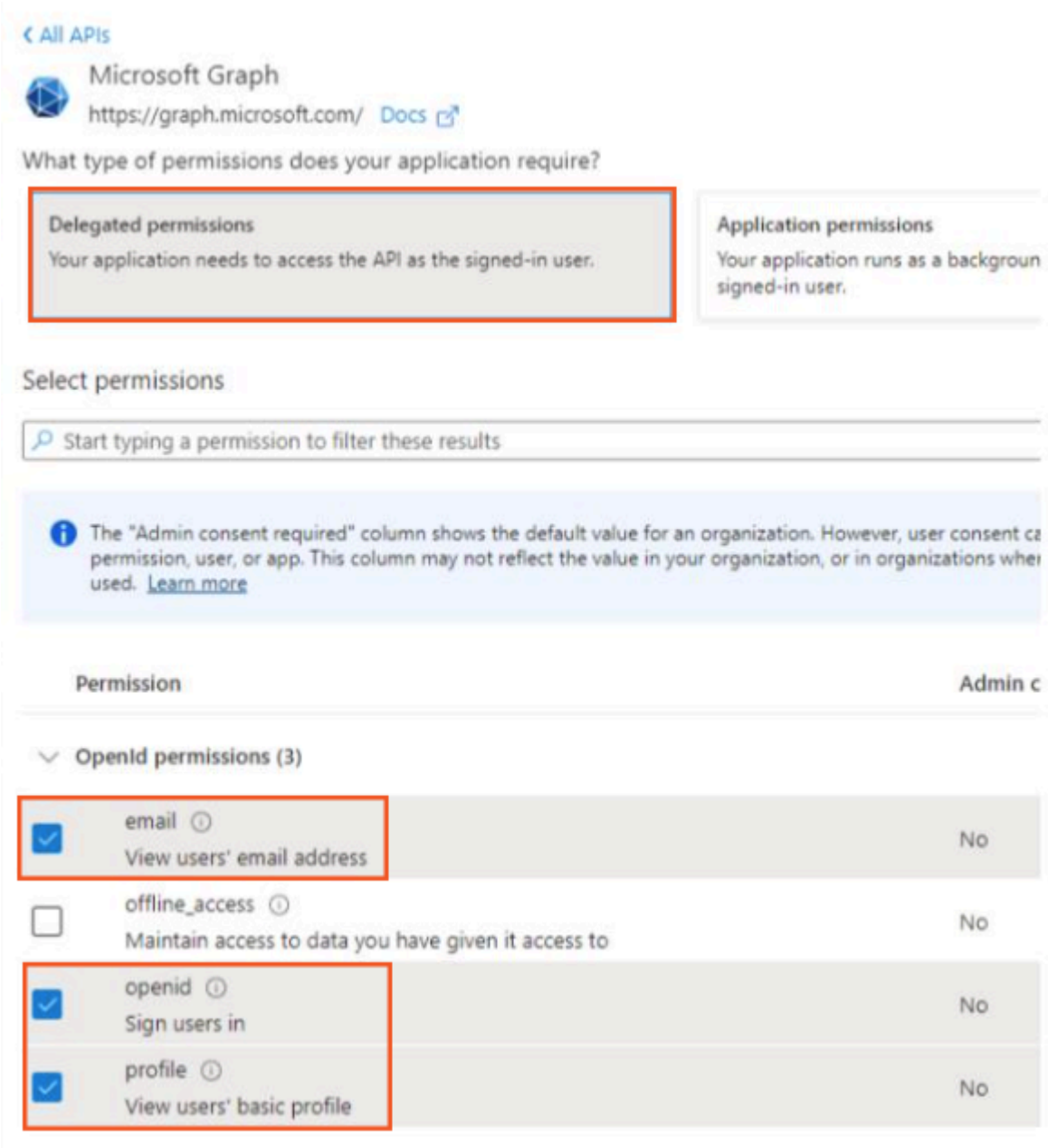
API permissions configuration

The necessary permissions for the API should be defined.

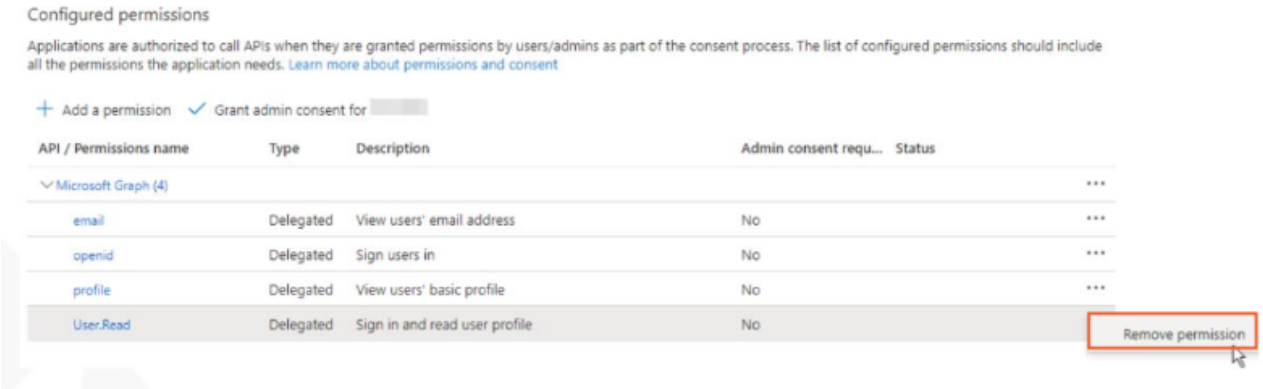
1. Find the created application and in the menu click on `API Permissions` -> `Add a permission`.



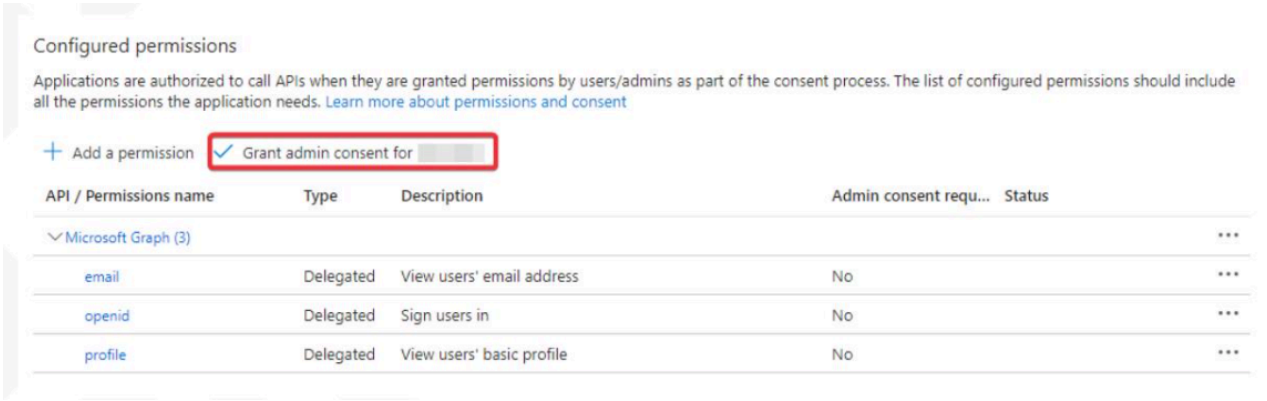
2. Click on `Microsoft Graph` -> `Delegated permissions`. Select `email`, `openid`, and `profile`.

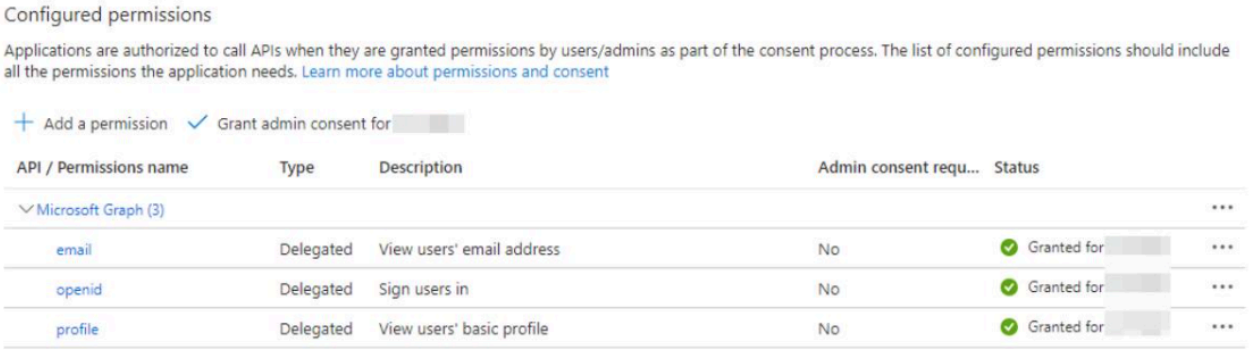


3. Once added, select the default created permission and click on `Remove permission`.

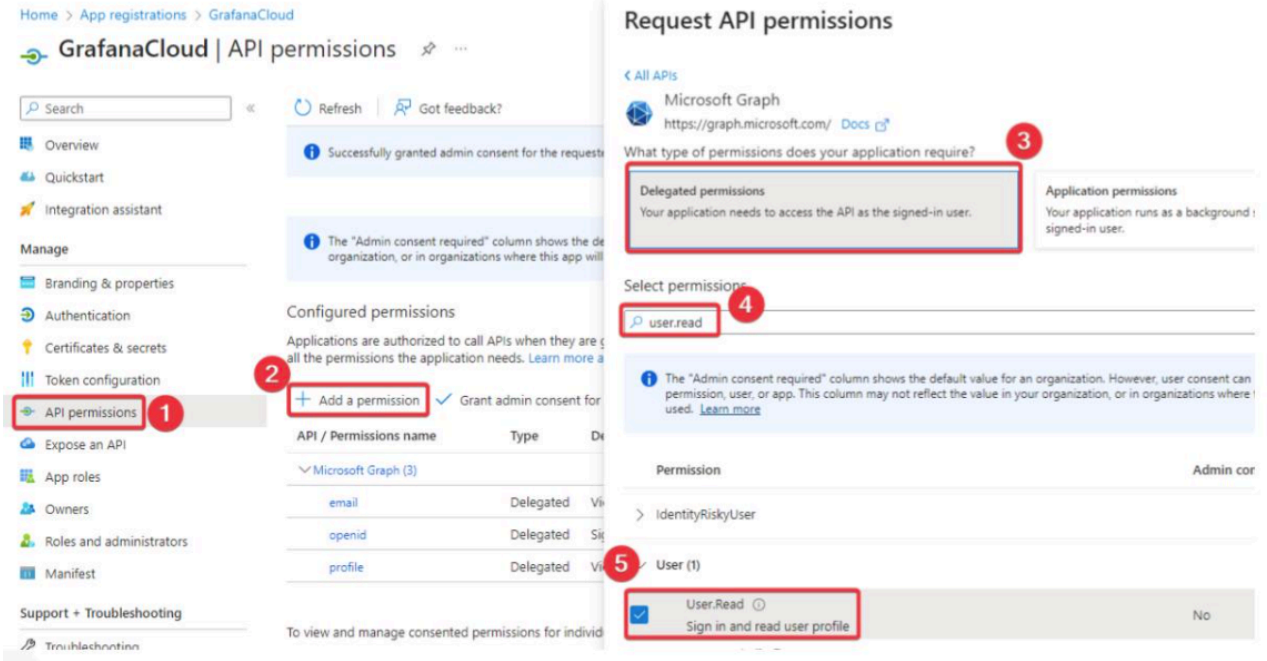


4. Grant organizational permissions to `email`, `openid`, and `profile`.

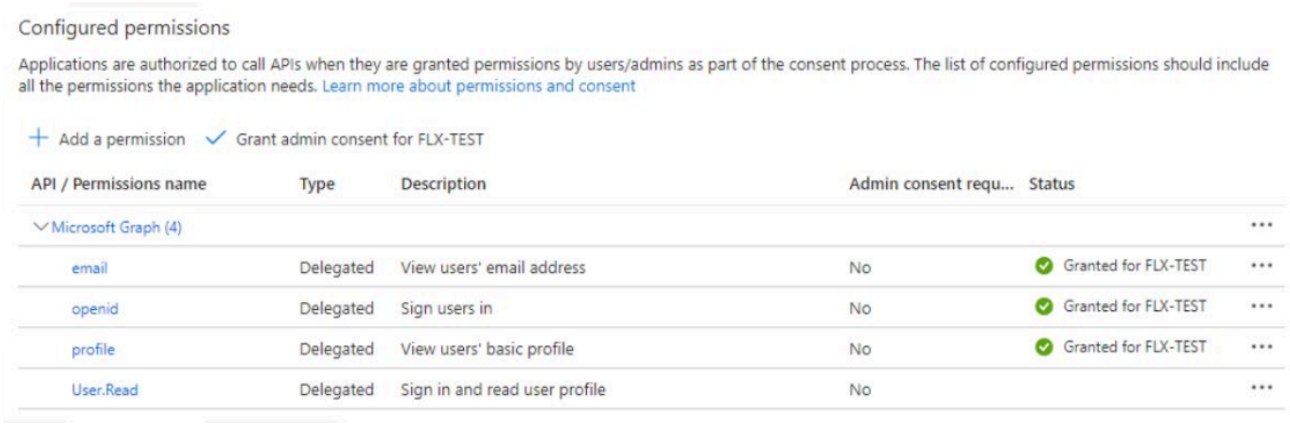




5. Find the `User.Read` permission and add it so it can perform profile reading only.



6. After the configuration is done, the image should look like the following:


Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

+ Add a permission ✓ Grant admin consent for FLX-TEST

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (4)				
email	Delegated	View users' email address	No	Granted for FLX-TEST
openid	Delegated	Sign users in	No	Granted for FLX-TEST
profile	Delegated	View users' basic profile	No	Granted for FLX-TEST
User.Read	Delegated	Sign in and read user profile	No	

Create application roles

The following application roles for Grafana should be created:

Display name	Description	Allowed member types	Value
Grafana Admin	Grafana admin Users	Users/Groups	Admin
Grafana Viewer	Grafana read only Users	Users/Groups	Viewer
Grafana Editor	Grafana Editor Users	Users/Groups	Editor

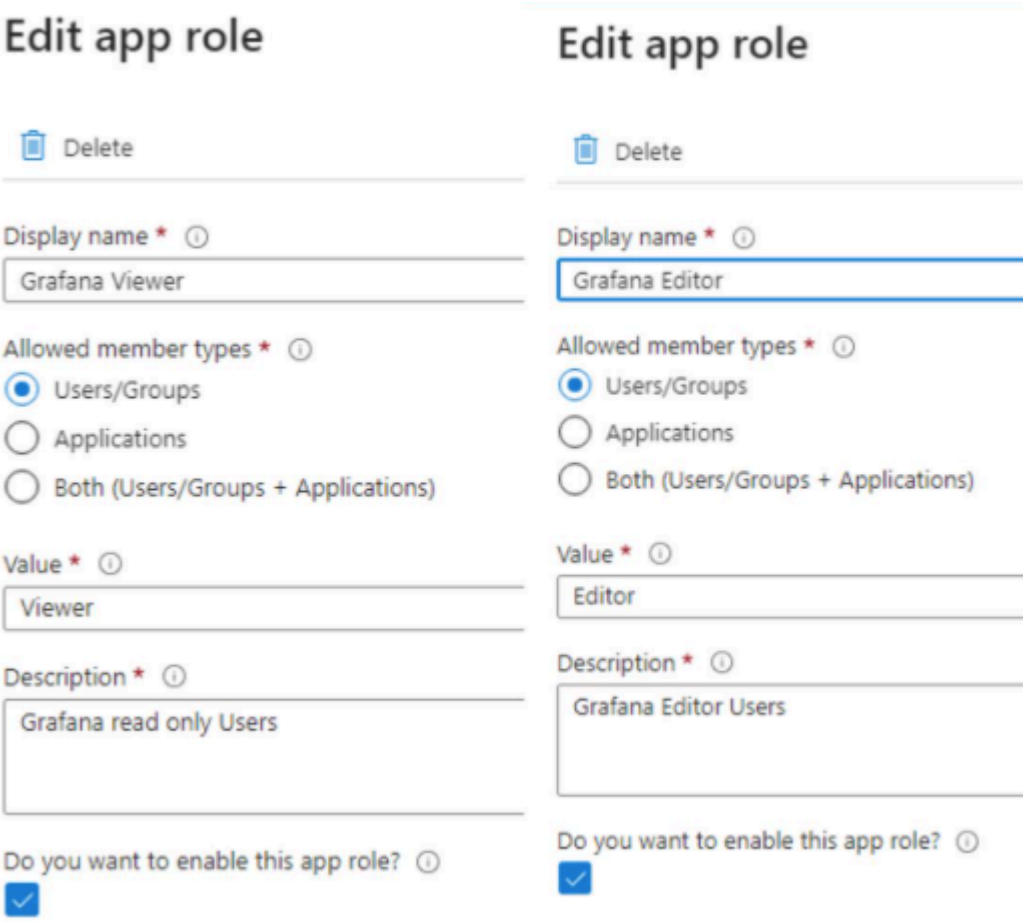
1. In the menu, click on `Application roles` -> `Create application role`.

2. In the `Create application role` panel, configure each role.

   For *Grafana Admin* enter the following values:

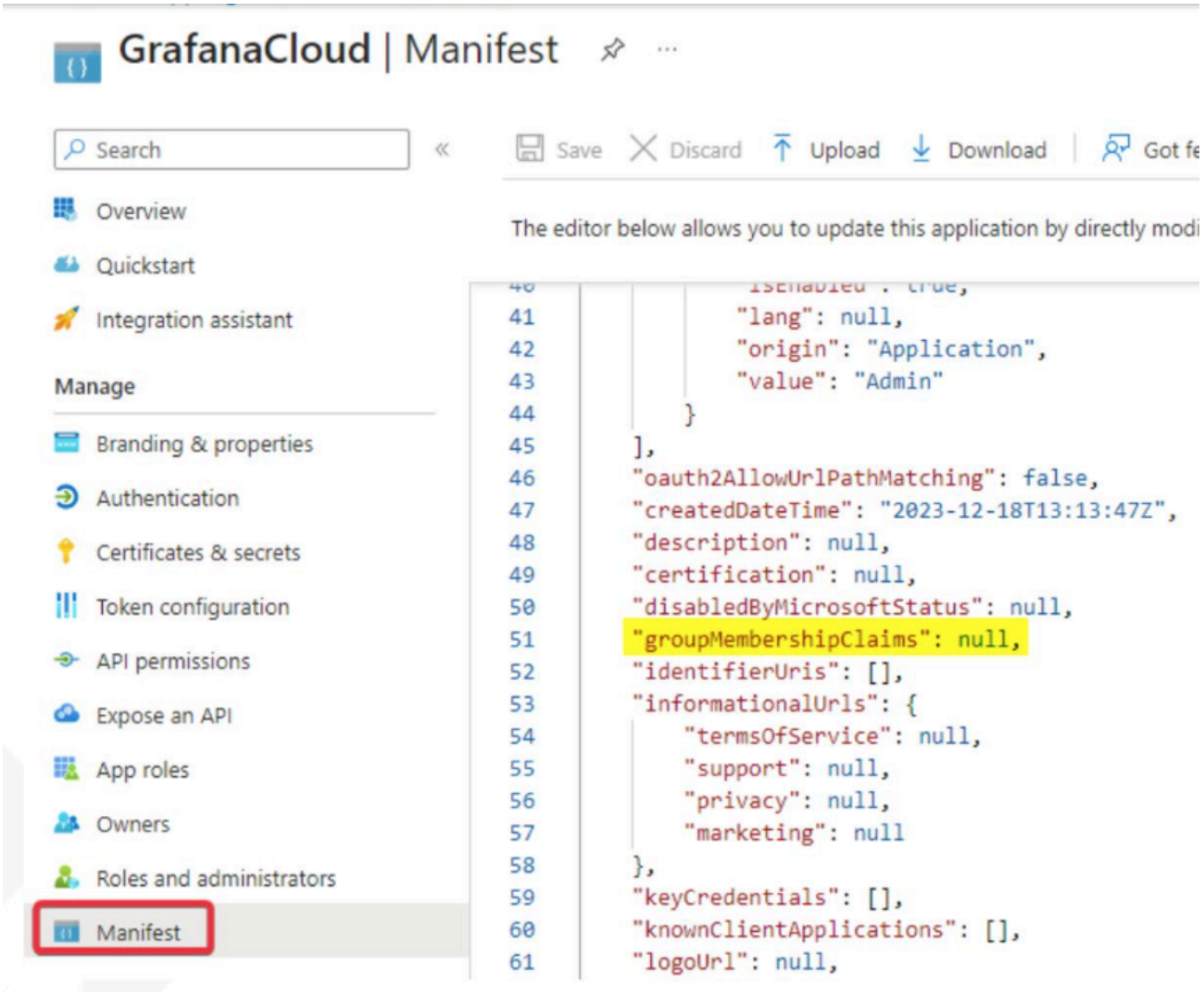
   - **Display name**: Grafana Admin
   - **Allowed member type**: Users/Groups
   - **Value**: Admin
   - **Description**: Grafana admin Users

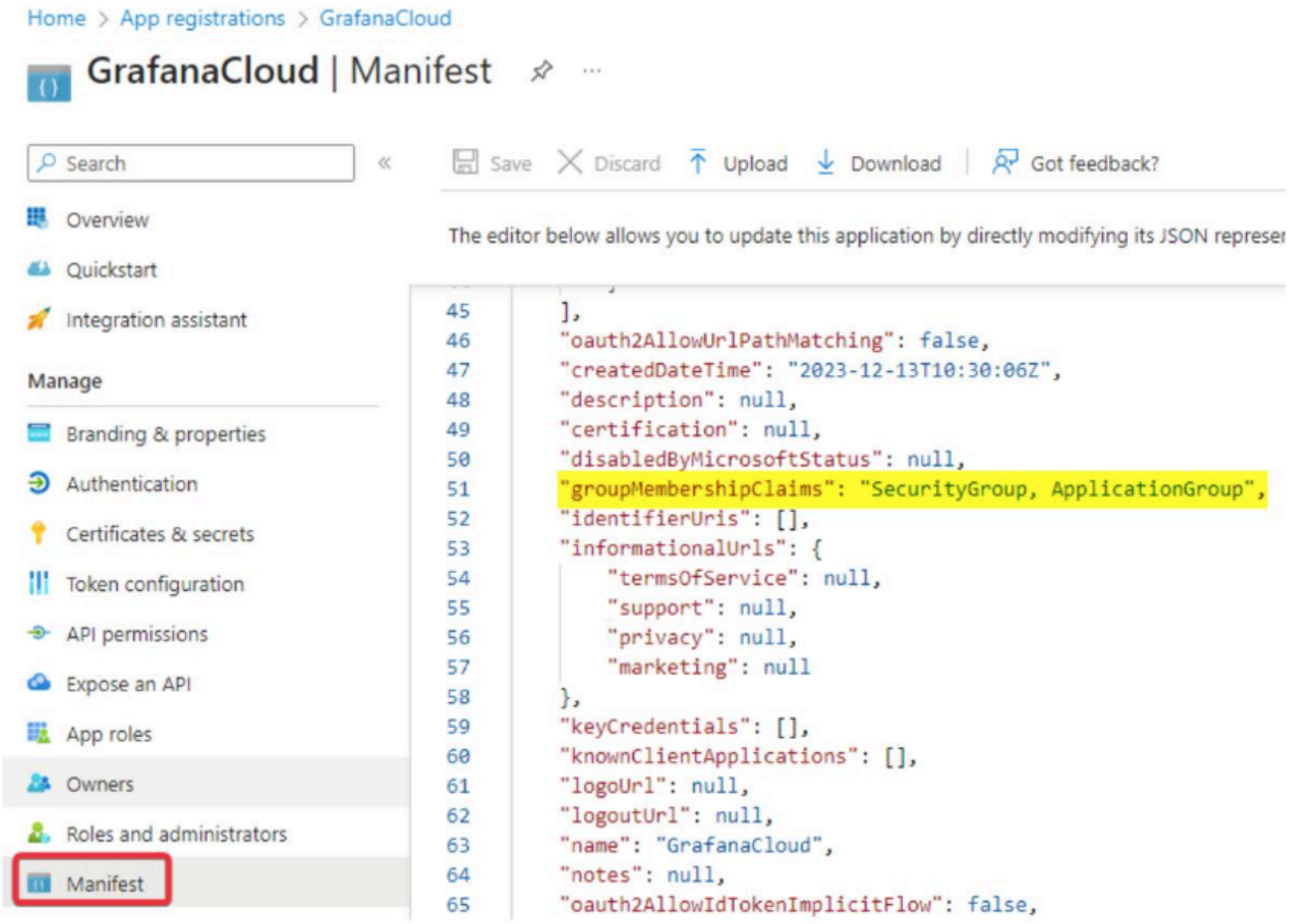
   And for *Grafana Viewer* and *Grafana Editor* enter the values shown in the following image:



Review the manifest.xml file

The *manifest.xml* file must be reviewed to change the value of the key `"groupMembershipClaims"` from `null` (default value) to `"SecurityGroup, ApplicationGroup"`.





Requirements

Once the application registration is done, the organization must provide the following parameters to Flexxible so that they can create the configuration in Grafana.

- Endpoints
  - OAuth 2.0 authorization endpoint (v2)
  - OAuth 2.0 token endpoint (v2)
- App registration
  - Application (client) ID
- Certification & Secrets
  - Secret Value

- Group ID to be configured
- Domain to authorize

Portal / Guides / Execution of a microservice after user login

Automatic execution of a microservice after a user logs in can be efficiently implemented using Flows. This method is ideal for scenarios where specific validations or tasks need to be performed once a day, as in the following example:

Requirement

> Each day, when the user logs in, a validation or execution must be carried out through a microservice.

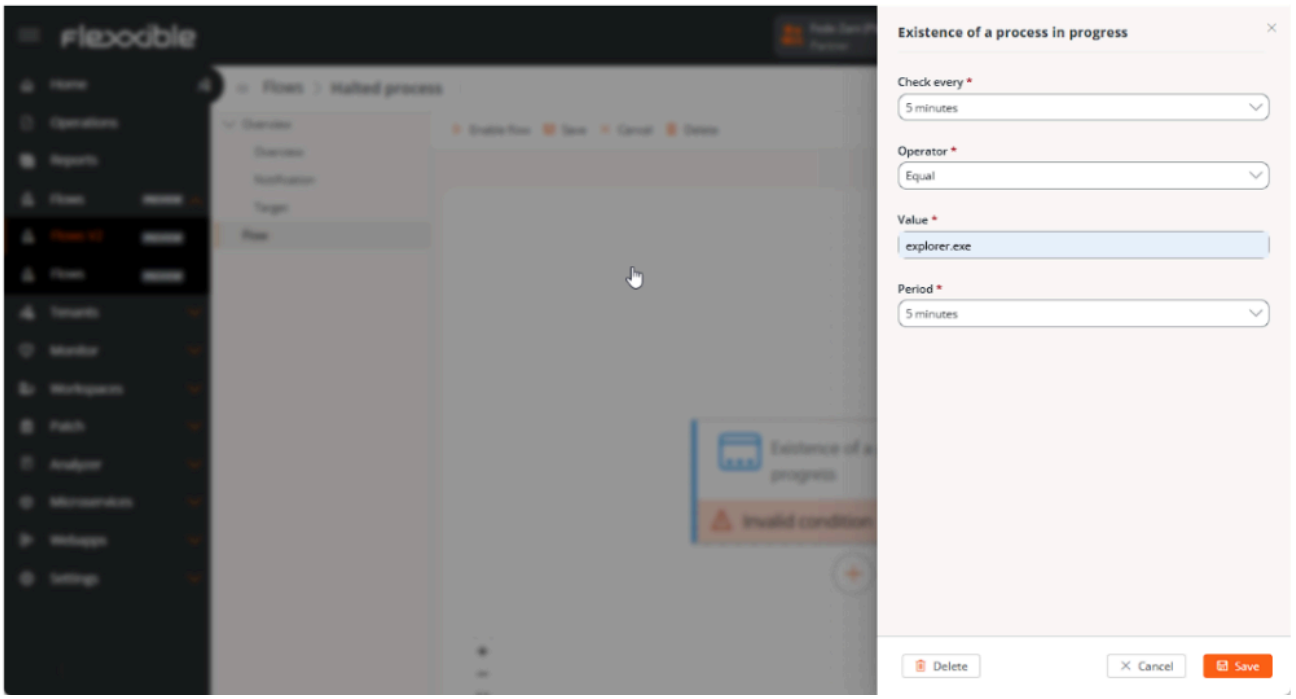
Components of the requirement

- Condition: User login.
- Action: Microservice execution.
- Maximum Recurrence: Once a day.

Flow Configuration

To meet the requirement, a flow can be defined using the condition Presence of an ongoing process. This allows monitoring and acting upon the presence of specific processes in the system using the following parameters:

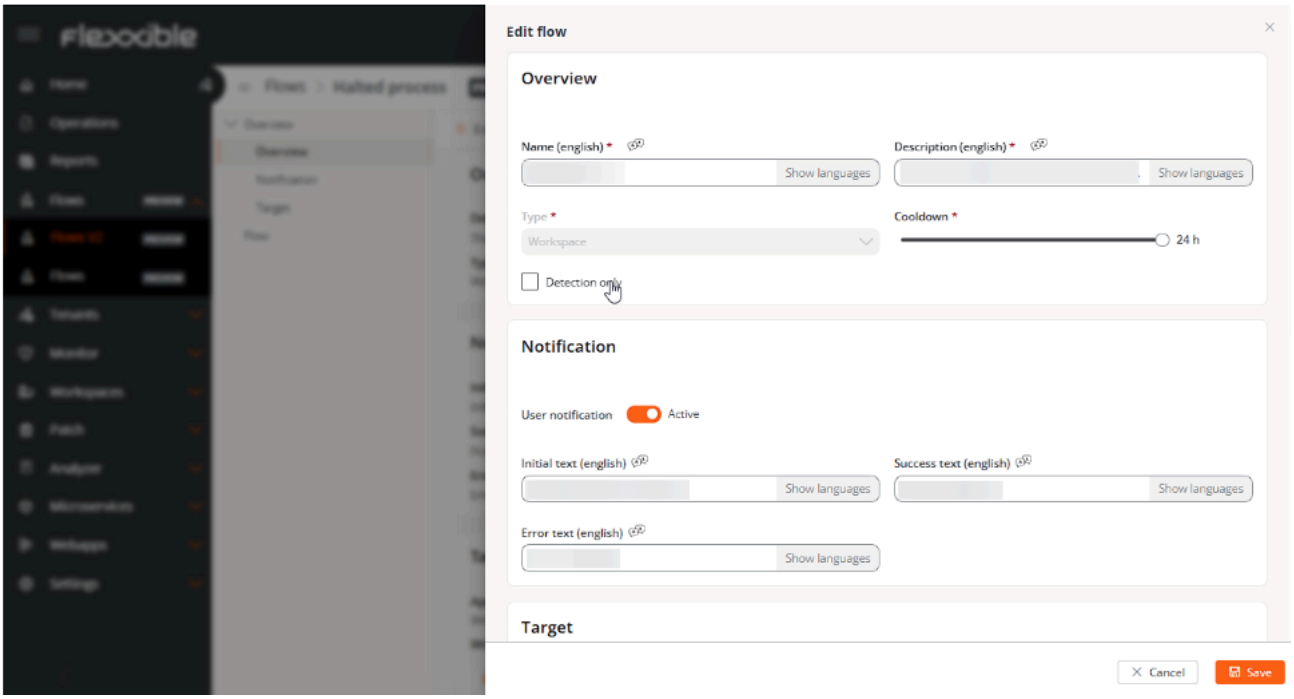
- **Check every.** Defines the timeframe for checking the process status.
- **Operator.** Allows filtering processes by name using operators like *Equal*, *Starts with*, *Ends with*, and *Contains*.
- **Value.** The specific name of the process to monitor.
- **Period.** The minimum time the process must be running for the condition to trigger.



In the image above, the condition configuration indicates that every **5 minutes** (Check every), the existence of a process named **Equal** (Operator) to **explorer.exe** (Value) will be checked and verified if the process has been running for a minimum period of **5 minutes** (Period).

Daily Recurrence Control

Although the previous configuration ensures the flow execution at each login, the user might log in more than once a day. That's why it is essential to configure the *Cooldown Time*, as it defines the minimum period that must pass before the condition can be evaluated and triggered again, once the condition has been fulfilled and an action executed.



By setting a cooldown time, the flow will execute the action the first time the condition (login) is met but won't reactivate until 24 hours have passed since the last execution. This ensures that the microservice triggers at most once a day, fulfilling the required recurrence.

Portal / Guides / Use Cloudflare R2 as storage for microservices

When executing a microservice it is necessary to "call" a file, whether to copy, download, or write to it, it is very important to choose the correct location for this. In on-premises work environments, without users working remotely or from home, the safest and simplest option is to use storage accessible by all devices on the corporate network; however, in scenarios where there are mobile devices that cannot remotely access the corporate network repository, it may be necessary to opt for a secure and public access repository design.

Suppose we want to install an application on all devices regardless of whether they are at home, on the go, or on the office network. To help us meet these types of requirements, there are multiple cloud service options, where **Cloudflare** acts as a **security and performance proxy** between users and servers. Its main services (CDN and DDoS protection) make anything on the internet faster, safer, and more reliable.

R2 is its **cloud object storage service** (similar to Amazon S3) distinguished by its policy of **zero egress fees**, also allowing free accounts with more than sufficient conditions, even for production environments.

In order to use it, you need to:

1. Create an account associated with an email by following these steps.
2. At the end, the associated email must be verified. If you haven't received the email, remember to check your spam folder.
3. Once the account is created and activated, **R2** must be activated from the user menu/billing/subscriptions. A payment method will be requested for overages, but it's free if certain conditions are met.

INFO

R2 free accounts include:

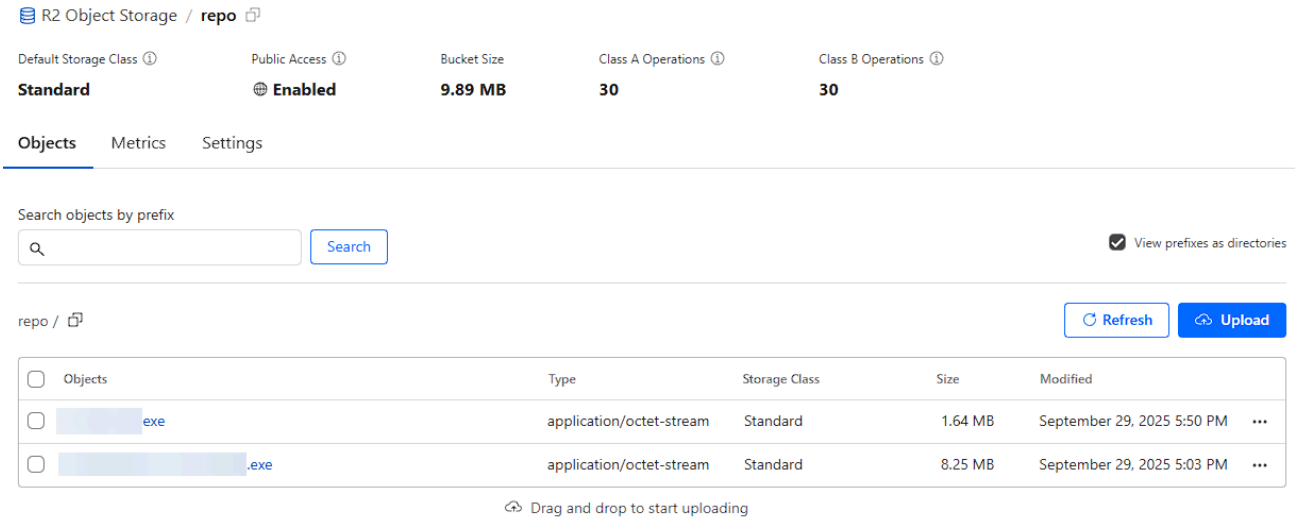
Service	Free
Storage	10 GB per month
Class A operations	1 million requests per month
Class B operations	10 million requests per month
Egress (data transfer to the Internet)	Free 1

For more detail, check this link.

Upload files

To host and use the uploaded files, the following is required:

1. Create a bucket.
2. Inside the bucket, there is a button called `Upload` that allows you to upload files.



Establish access methods

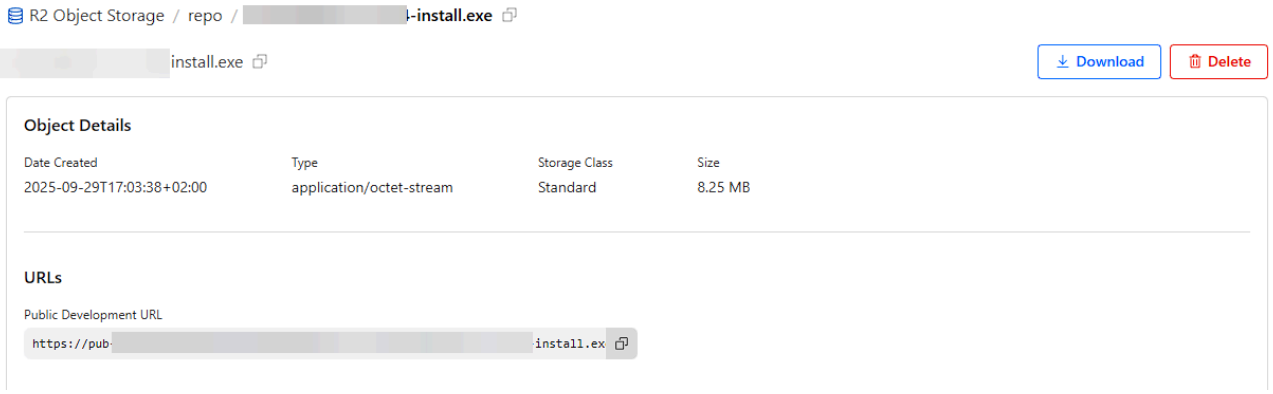
Cloudflare allows various access methods like:

- R2 Workers Binding API
- S3 API compatibility
- Public buckets

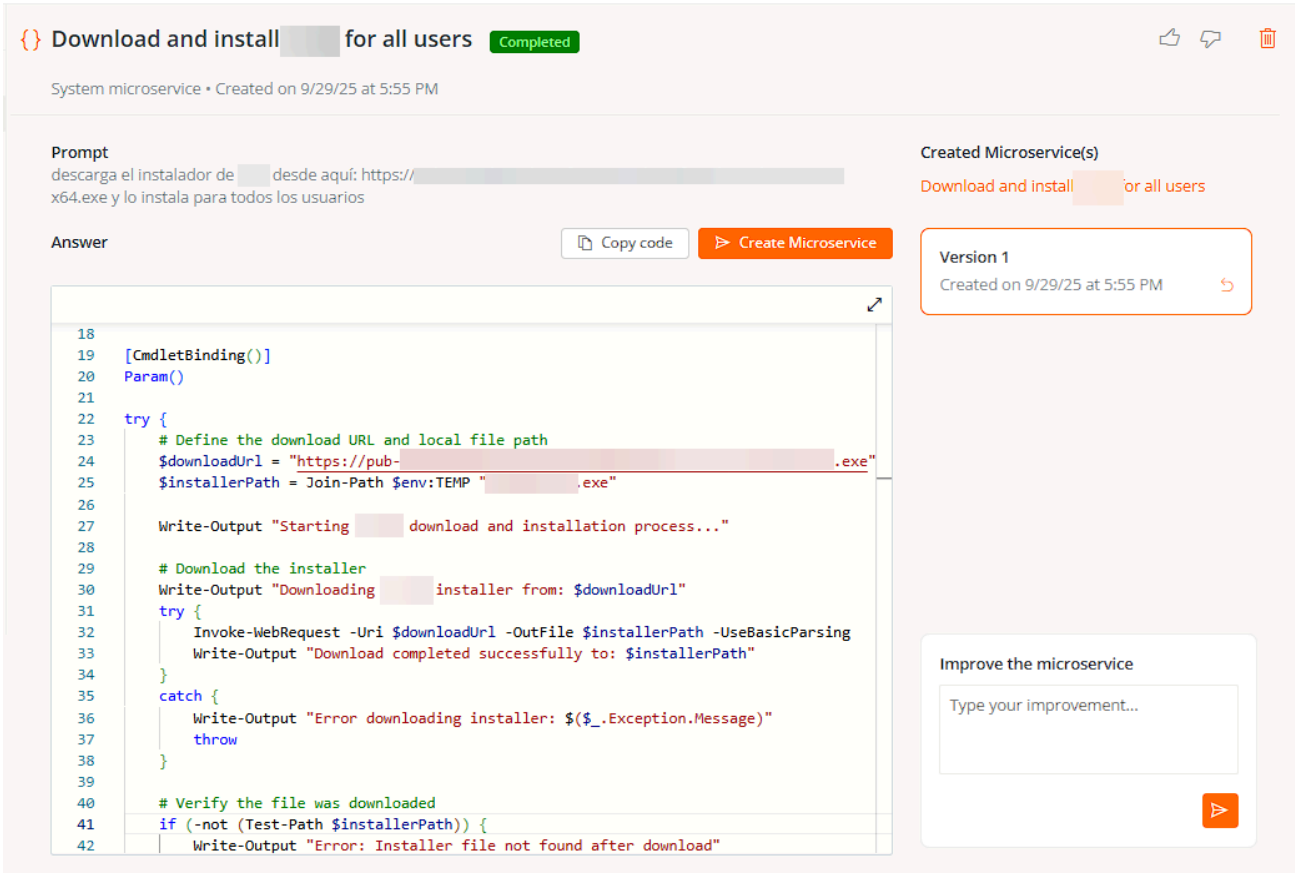
For demonstration purposes, this article uses Public buckets.

Accessing files from microservices

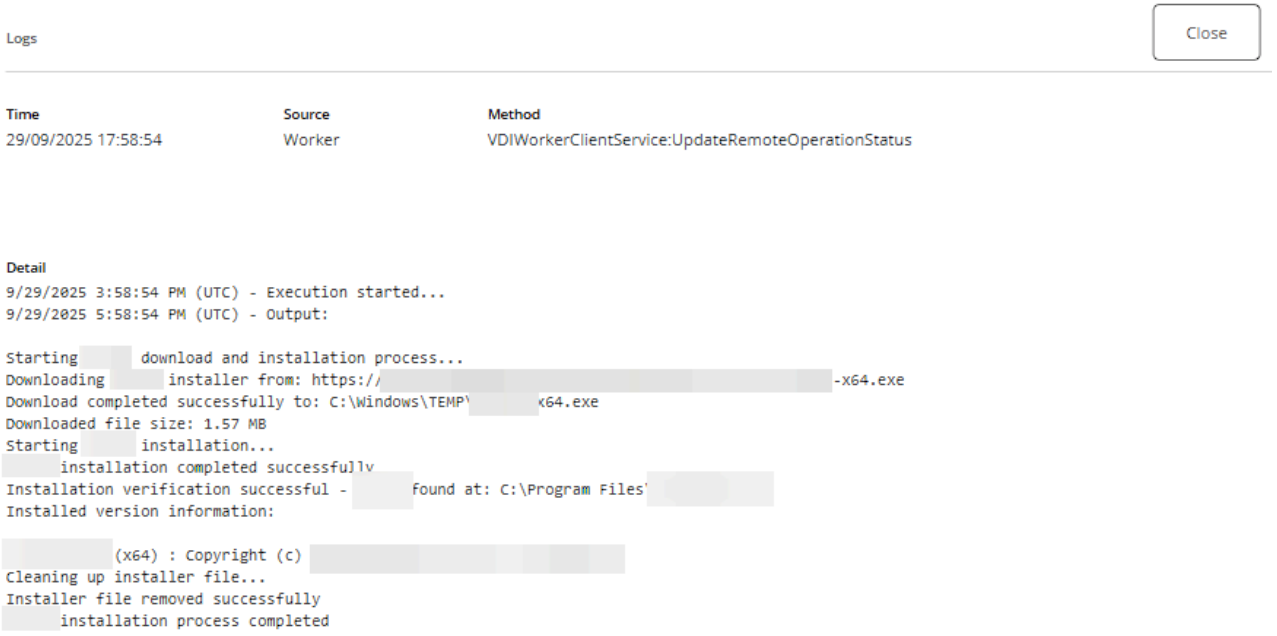
Each file uploaded to R2 generates a unique link in its properties. You can see it by clicking on the file:



That link allows you to obtain the file from the microservice using, for example, PowerShell's `Invoke-WebRequest` cmdlet or simply requesting a microservice created with AI with instructions that include the download URL:



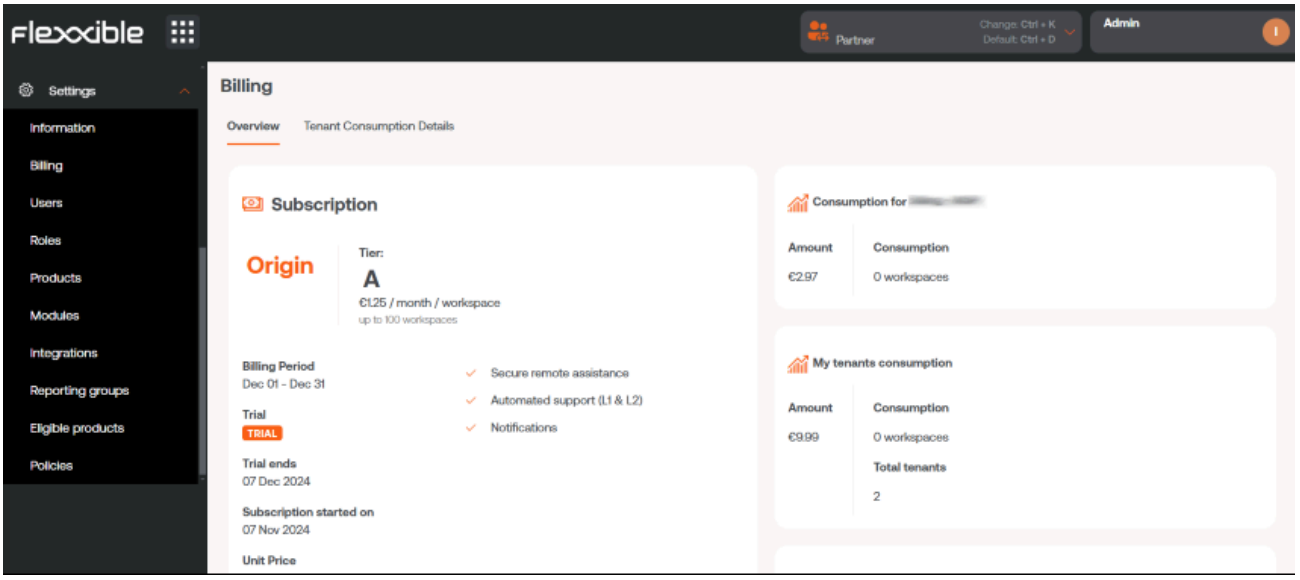
It's always recommended, if not using AI-created microservices, to log milestones during execution so that in case of any error or malfunction, identifying the problem becomes easier:



Portal / Billing

Billing allows you to view information about billing and service consumption of FXXOne on devices with an active subscription. The access path to this data is `Portal` -> `Settings` -> `Billing`.

The amount of information displayed by this option depends on the role of the user who is viewing it and the type of organization. Users with the *Organization Administrator* role in a partner-type organization can view consumption data of their tenants' service as well as charts with details; however, a user with the *Administrator* role of a client-type organization will only be able to access general subscription information.



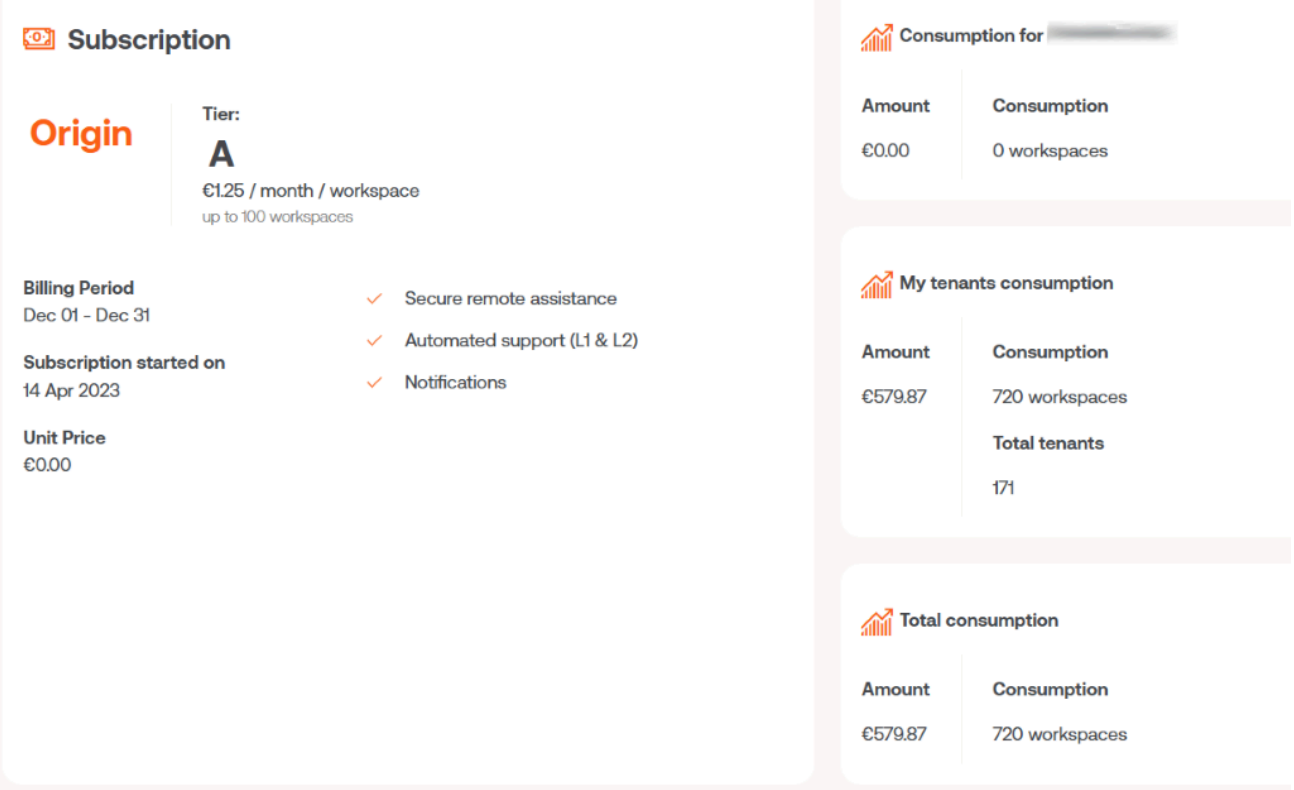
View from a partner-type organization

The `Billing` view for a user whose role is *Organization Administrator* in a partner-type organization presents two types of information:

- Overview
- Tenants consumption details

Overview

Provides global information about the FXXOne subscription that the organization has contracted. It is divided into four sections: `Subscription`, `Consumption for organization`, `My tenants consumption` and `Total consumption`.



Subscription

This is an overview of the subscription features. It provides information about the billing period, subscription start date, unit price, and available services. The subscribed plan name is highlighted in orange and `Tier` specifies the price for a device per month.

The `Tier` is set considering the service consumption of the partner-type organization plus the consumption of its tenants. Regardless of the plans the tenants are subscribed to, they will always be in the `Tier` of the organization that manages them.

Consumption for organization

It informs about the number of devices a partner-type organization has subscribed and the billable amount it represents.

> **INFO**
>
> A device that has uninstalled FlexxAgent will continue to count at the billing level as long as it continues to appear in its reporting group. To delete it, check the steps to remove a device from a report group.

My tenants consumption

It informs about the number of devices a partner-type organization has subscribed, the number of tenants these are distributed in, as well as the billable amount they represent.

Total consumption

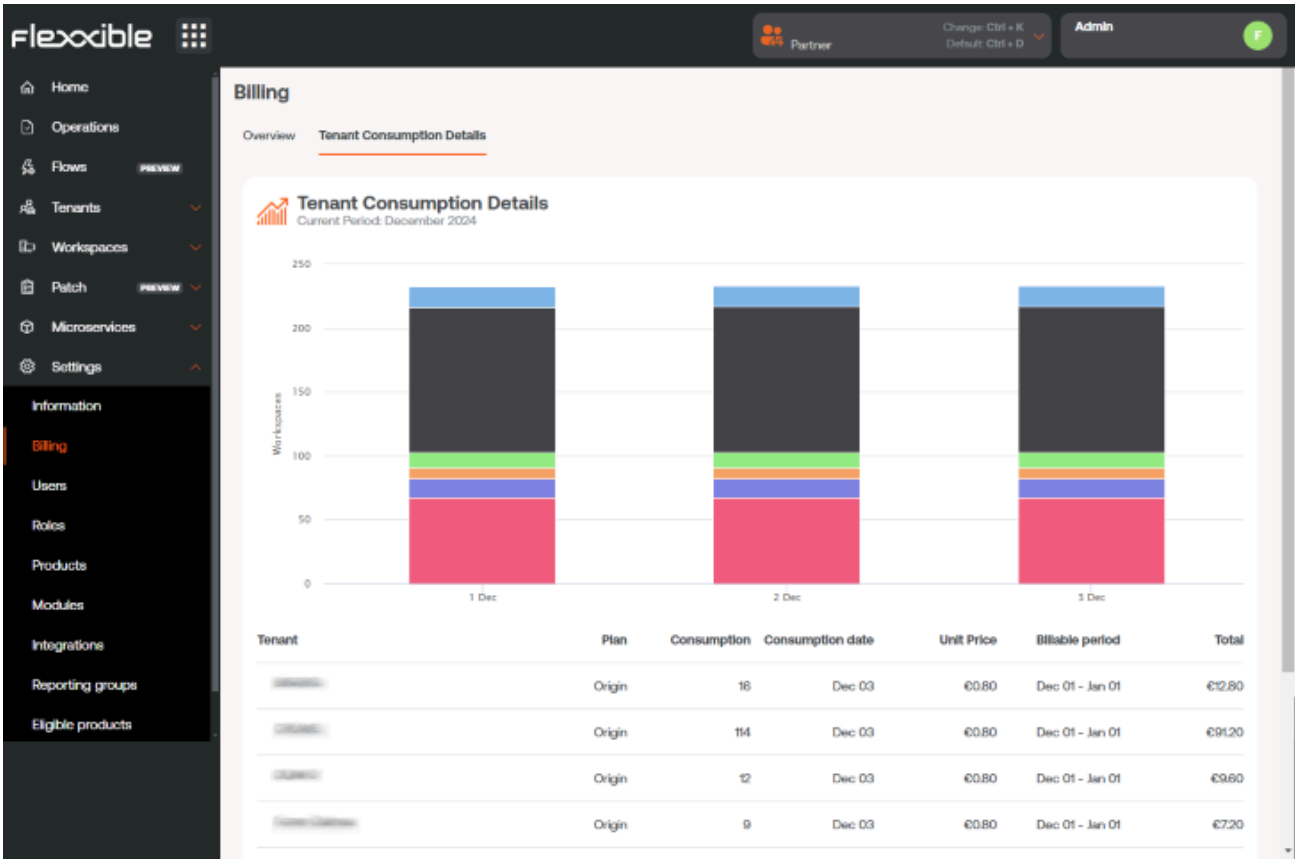
It informs about the total sum of devices the partner-type organization has subscribed, including its tenants, and the billable amount they represent.

Tenants consumption details

This tab offers a dashboard that graphs the consumption by devices of each of the organization's tenants during the current billing period.

The bottom part shows a table with detailed information about each tenant's subscription:

- **Tenant**: tenant name
- **Plan**: name of the FXXOne subscription plan they have
- **Consumption**: number of devices whose agents have reported in Workspaces
- **Consumption date**: date of maximum device reporting in Workspaces
- **Unit Price**: consumption price per agent on a device
- **Billable period**: subscription billing period
- **Total**: total billable amount for the subscription

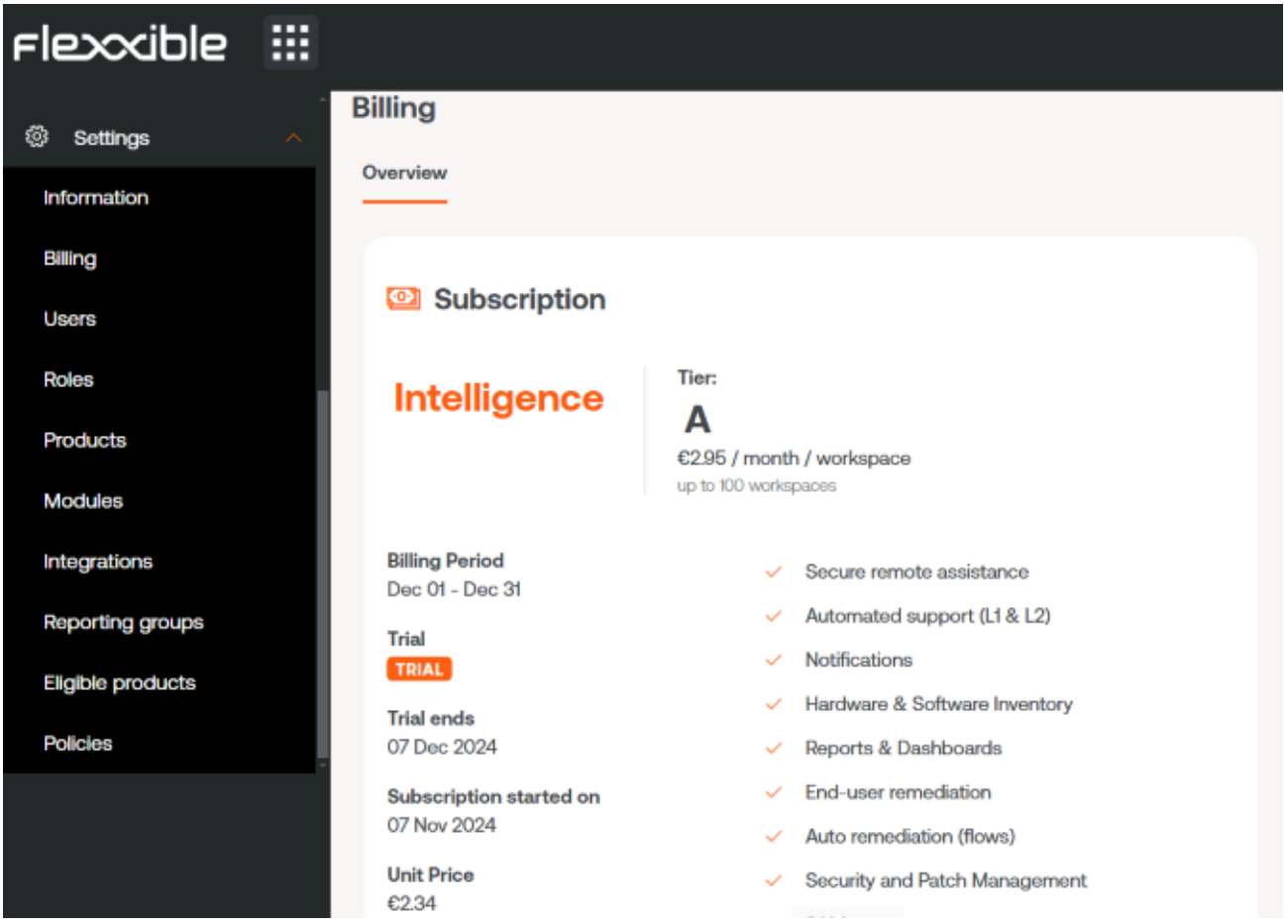


View from a client-type organization

The `Billing` view of a user whose role is *Administrator* within a client-type organization can only obtain general information about the FXXOne subscription through the `Overview` tab.

Overview

Provides global data about the FXXOne subscription that the organization has contracted.



Subscription

It provides information about the billing period, subscription start date, unit price, available services and also the trial period of the service, if applicable. The subscribed plan name is highlighted in orange and `Tier` specifies the price for a device per month. Regardless of the plans the tenants are subscribed to, they will always be in the `Tier` of the organization that manages them.

FlexxAgent consumption

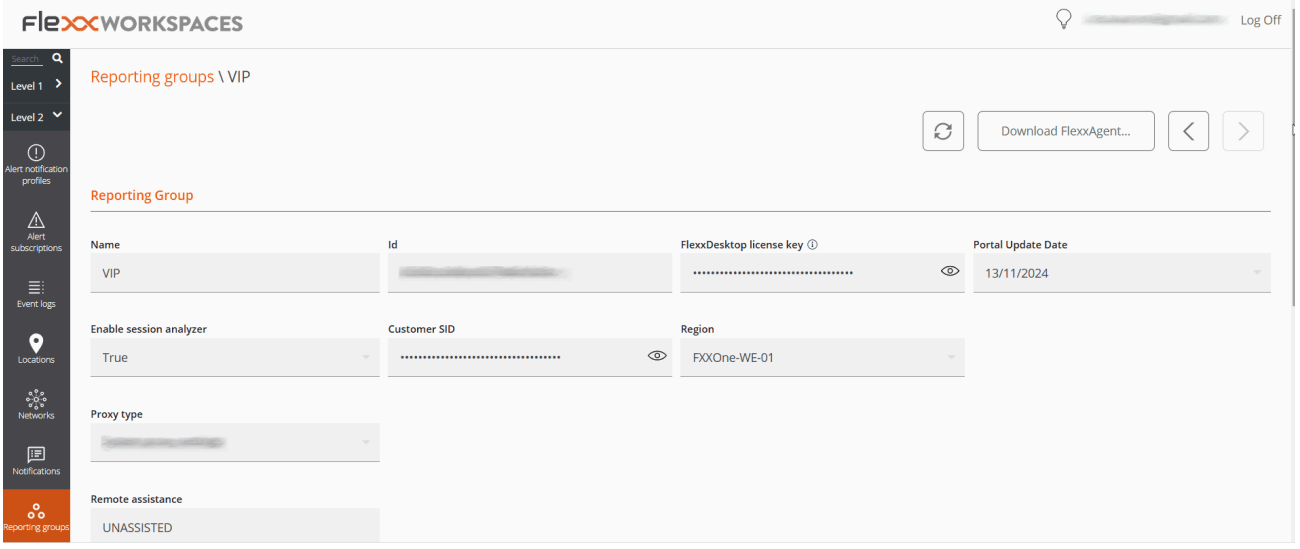
FlexxAgent consumption is based on the maximum number of devices reporting in the Workspaces module on the same day, for a billing period.

For a device to stop consuming at the billing level, it must not have FlexxAgent installed or belong to any reporting group. If FlexxAgent is not uninstalled from a device that is not in use, it will report to Workspaces again when it becomes active.

If the user has uninstalled FlexxAgent from one or more devices and wants them to stop appearing immediately in Workspaces, they must go to `Reporting groups` in the `Workspaces` module to remove them. If the user does not perform this action, the device will be automatically removed 21 days after its last report.

Removal of a device from a reporting group

1. Access the Workspaces module -> `Level 2` -> `Reporting groups`.
2. Select the corresponding reporting group.
3. In the `Devices` tab, select the device.
4. Go to `Operations` -> `Delete workspace`.



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

Level 2

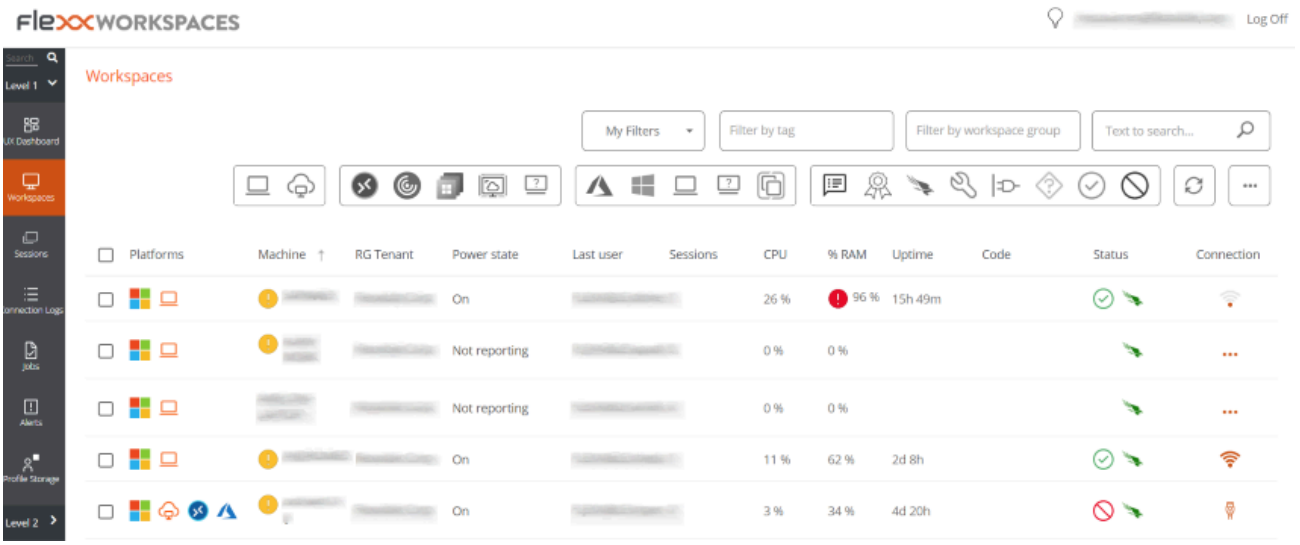
Offers tools that enable a more detailed diagnosis, such as monitoring, event log filtering, server management, and more. Functionalities available at this level:

- Event log
- Locations
- Networks
- Notifications
- Servers
- Wireless networks

List Views

From the list views, you can filter and select items in the Workspaces and Sessions sections to get lists of, for example, devices with a certain uptime, with pending restarts for updates, or those that haven't been used for a specific 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. Below, options will be shown according to the sorting, grouping, visibility, and

filtering of the columns.

Column sorting

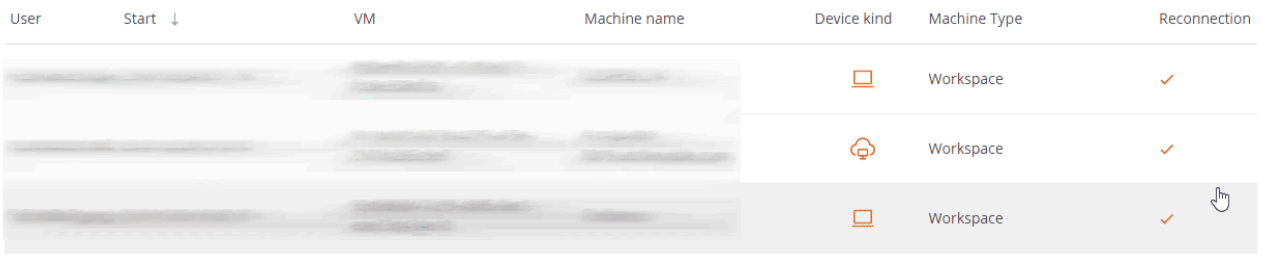
The options `Sort Ascending` and `Sort Descending` allow you to arrange the values of a column according to the letter or number they start with. For example, if the column `% RAM` is set to sort ascending, the column values will be arranged so that the first row corresponds to the device with the lowest 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.

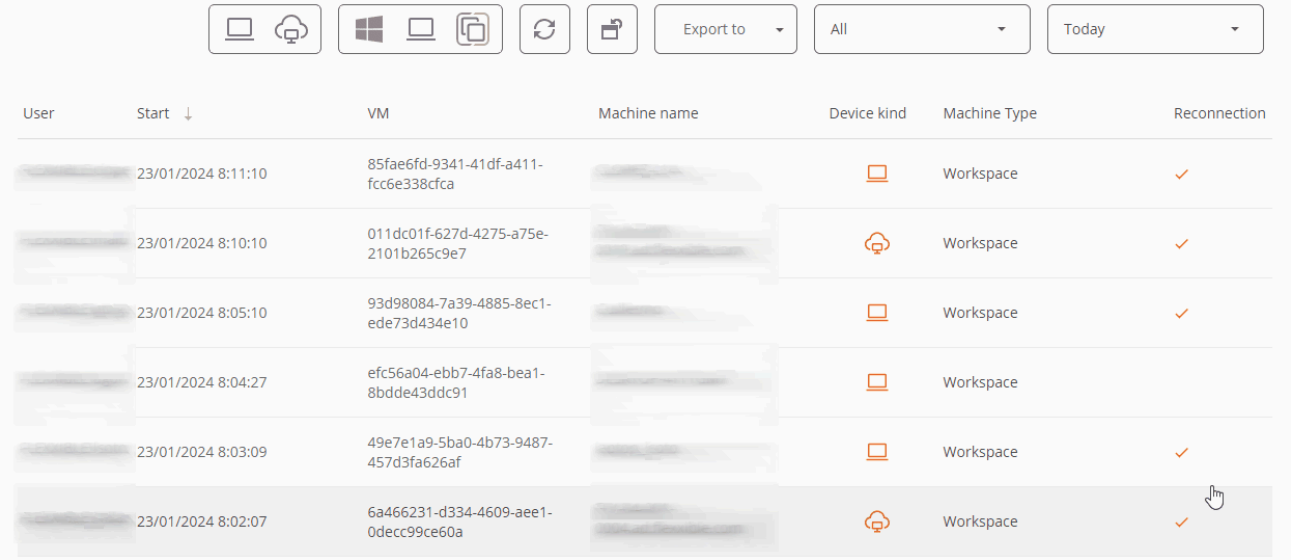


Column visibility

The options `Hide column`, `Show customization dialog`, and `Column selector` allow modifying the column visibility in the table.

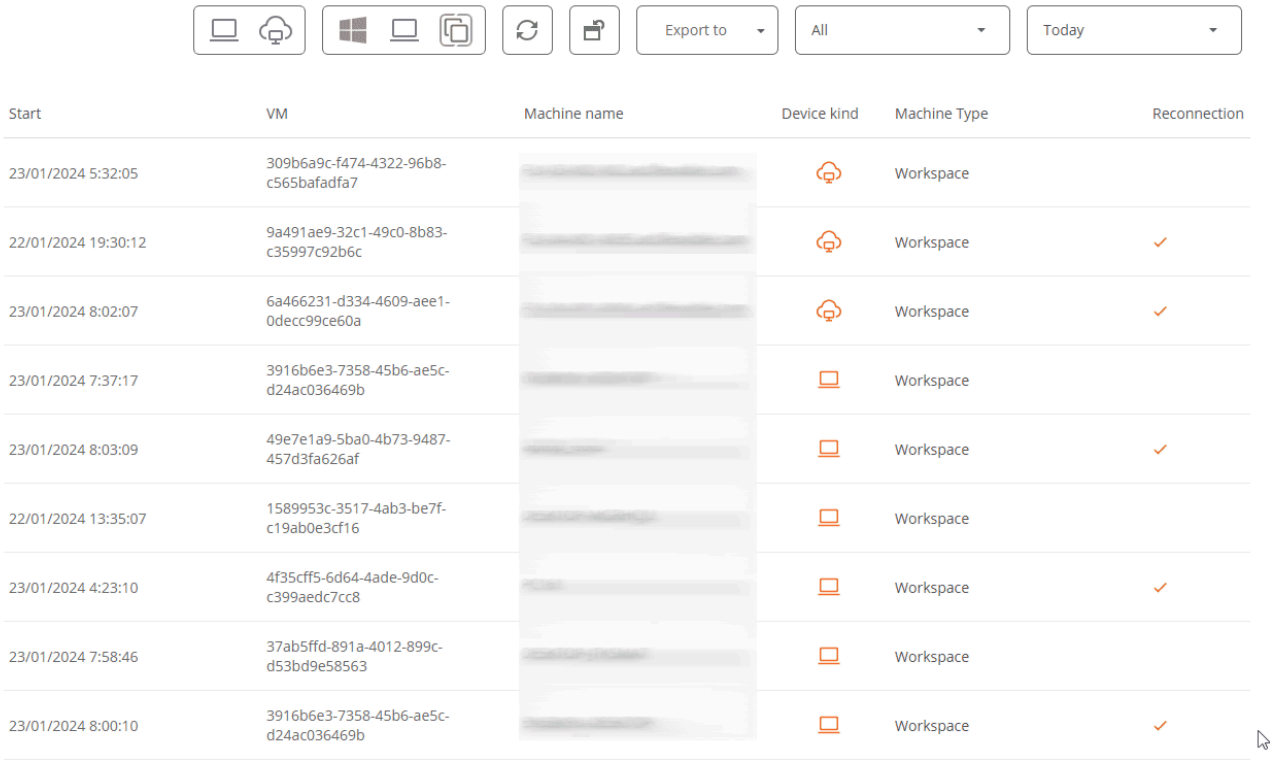
If the user doesn't want to see a specific column, they need to go to its header, right-click, and select the `Hide column` option. If they want to configure in detail the columns and

records they want to see in the table, they should click `Show customization dialog`, but if they prefer to add or remove columns, they can do so through the `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.



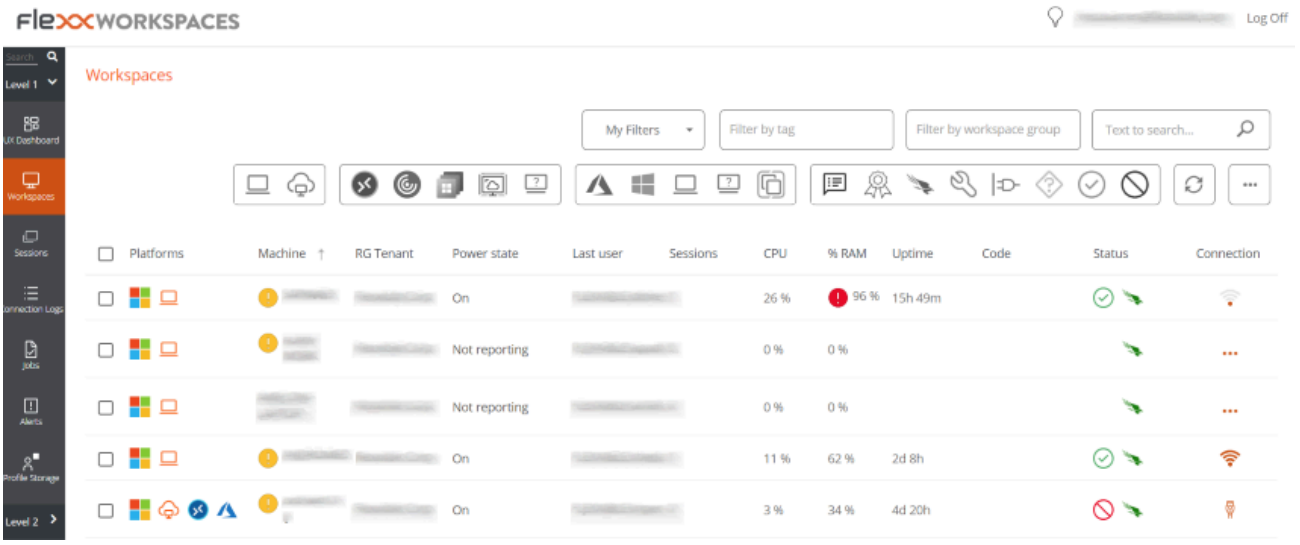
When the `Footer` option is selected, the total number of records found is displayed at the bottom left of the table.

Detail Views

By clicking 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

This level of Workspaces brings together tools for teams that have more direct contact with end users. Includes views of UX Panel, Workspaces, Sessions, Connection Logs, Jobs, Alerts, and Profile Storage.

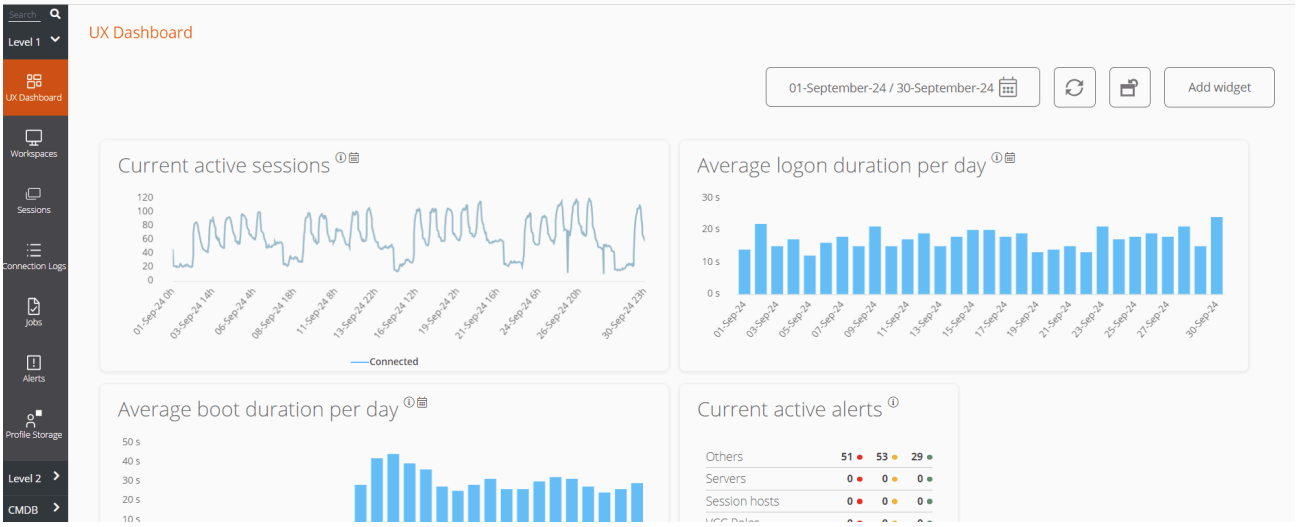


Functionalities available at this level:

- UX Dashboard
- Workspaces
- Sessions
- Connection Log
- Jobs

Workspaces / Level 1 / UX Panel

UX Panel 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 you to segment the data by organization, filter by dates, and select the widgets that will be part of the panel.

The configuration of the widgets included in the panel, 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.

> **INFO**
>
> The organization selector is only visible when the user has access to more than one organization.

Date filtering

The date selector allows you to apply temporary filters to the panel data:

- Predefined filters:
  - Today
  - Yesterday
  - Last 7 days
  - Last 30 days
  - This month
  - Last month
- Custom filters allow you to select start and end date and time.

Widgets

The different information boxes within the panel are called widgets, which can be repositioned, resized, or directly deleted by clicking the `x` that appears when hovering the mouse over.

Default widgets

The widgets offered by default in Workspaces are the following:

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. Not filtered according to 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. Not filtered according to 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. Not filtered according to the date selector.

Workspaces by Internet Service Providers (ISP)

A view of the different Internet service providers in use by the devices. Since these are real-time data, date filtering is omitted.

Workspace by country

A view of the different countries from which the devices connect. Since these are real-time data, date filtering is omitted.

Number of Workspaces per Operating system

This widget shows real-time data. Not filtered according to 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. Not filtered according to 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 can accept each session host.
- **Total sessions.** Number of maximum sessions according with the number of session hosts and the configuration of each one.
- **Available.** Number of new sessions that 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. Not filtered according to the date selector.

Top 10 workspaces by current total used bandwidth

Top 10 devices with the highest currently used bandwidth in KB/s. This widget shows real-time data. Not filtered according to 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. Not filtered according to 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. Not filtered according to 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 devices sorted by the current number of sessions. This widget shows real-time data. Not filtered according to 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. Not filtered according to the date selector.

Top 10 workspaces by current total RAM used

Top 10 devices sorted by the currently used RAM in GB. This widget shows real-time data. Not filtered according to the date selector.

Current AVD resources

The number of devices, host groups, and application groups created in Azure Virtual Desktop. This widget shows real-time data. Not filtered according to 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 devices per agent, grouping by broker. This widget shows real-time data. Not filtered according to the date selector.

Workspace by city

A view of the different cities from which the devices 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 devices. 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 devices. Since these are real-time data, date filtering is omitted.

Workspaces per hypervisor

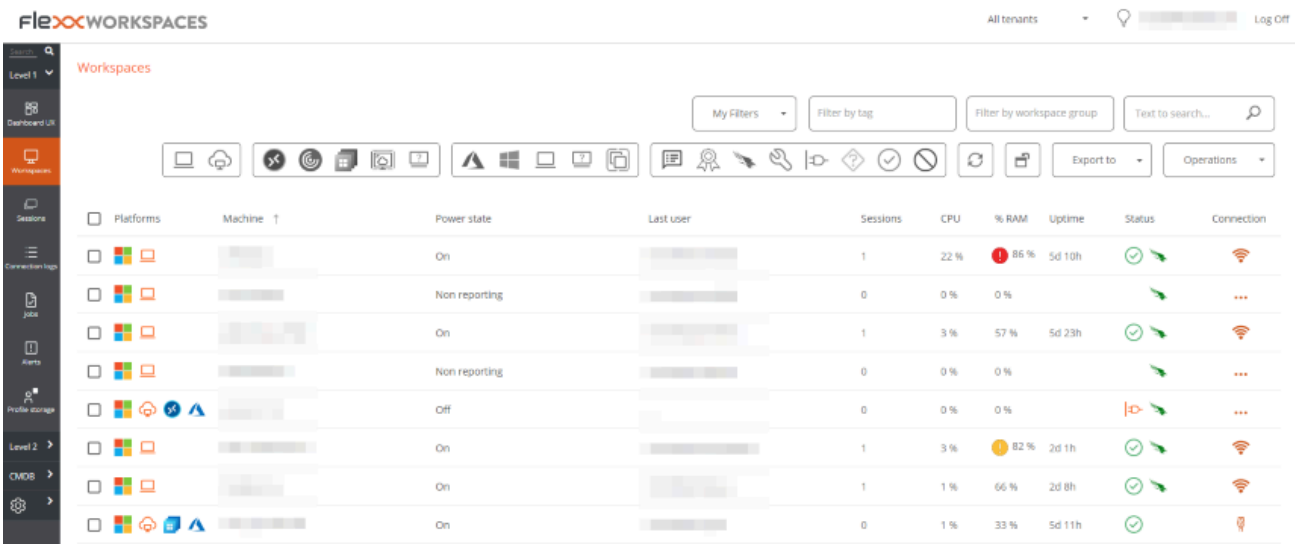
Number of devices per hypervisor. This widget shows real-time data. Not filtered according to the date selector.

Workspaces by operating system and build number

A ranking of operating system and build number combinations sorted by number of devices using each one. This widget displays data filtered according to the date selector.

Workspaces / Level 1 / Workspaces View

The list view of **Workspaces** 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 and saving the filters used for future queries in the user's profile.

Header filtering options

The top menu concentrates tools, icons for each attribute, which filter the list based on the following criteria:

- Device technology filter:
  - Device type: 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 selection, the `Operations` button gives access to perform various tasks such as `Power and Connection Actions` or sending `Notifications` to users.

In `My Filters` there are also additional filtering options.

Filtering Options

To access the grouping and filtering options of the item list, right-click on the header of a column. Below, options will be shown according to the sorting, grouping, visibility, and filtering of the columns.

Column sorting

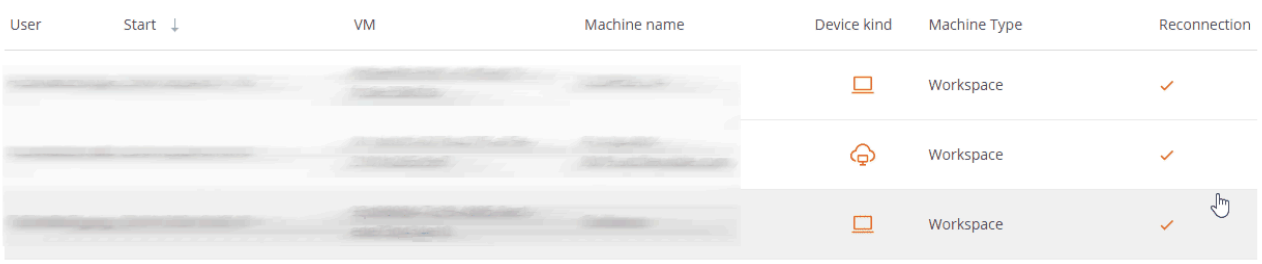
The options `Sort Ascending` and `Sort Descending` allow you to arrange the values of a column according to the letter or number they start with. For example, if the column `% RAM` is set to sort ascending, the column values will be arranged so that the first row corresponds to the device with the lowest 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.

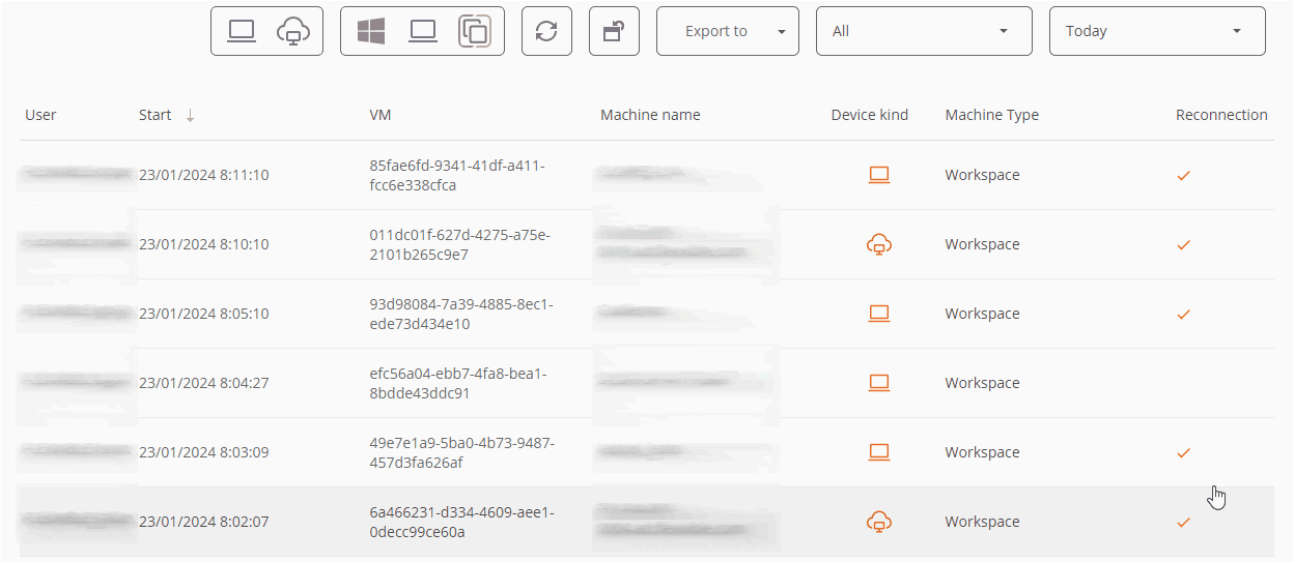
The difference between them is that `Group by this column` only considers the selected column for grouping the records, while `Group panel` allows selecting more than one column for grouping.



Column visibility

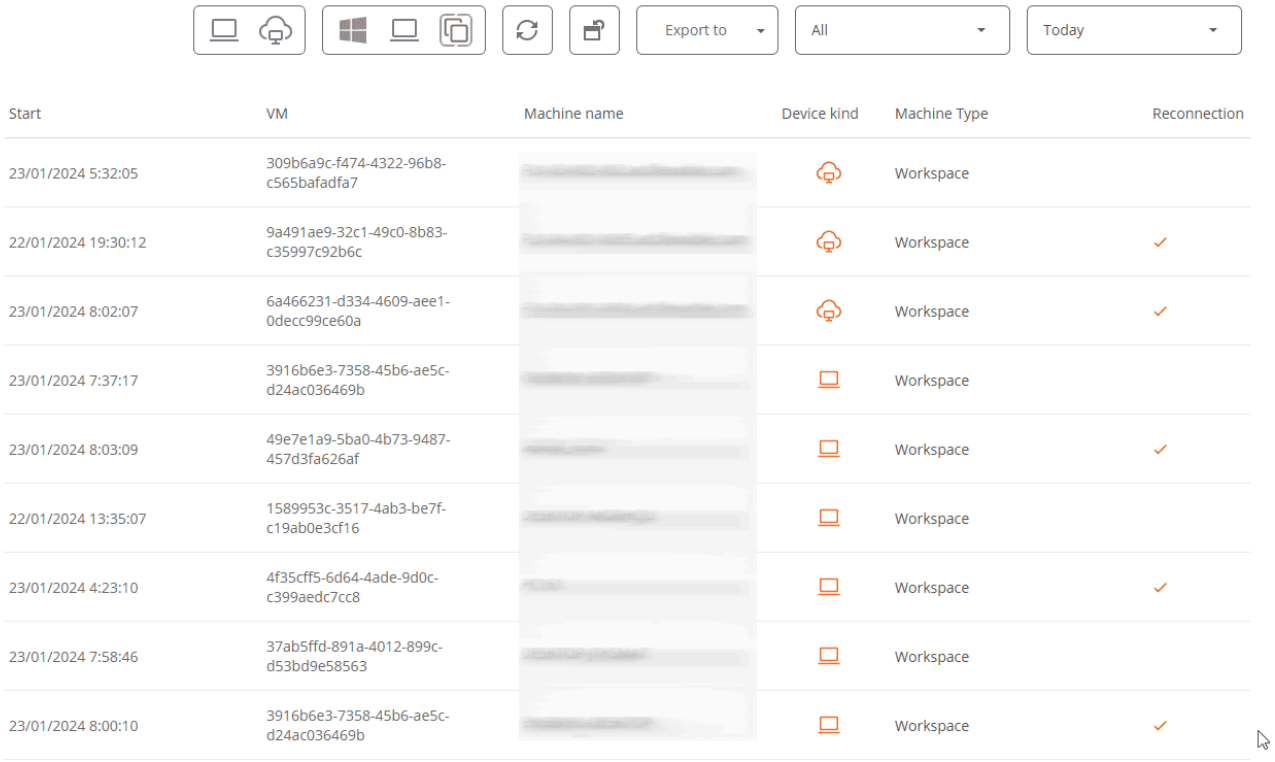
The options `Hide column`, `Show customization dialog`, and `Column selector` allow modifying the column visibility in the table.

If the user doesn't want to see a specific column, they need to go to its header, right-click, and select the `Hide column` option. If they want to configure in detail the columns and records they want to see in the table, they should click `Show customization dialog`, but if they prefer to add or remove columns, they can do so through the `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.



Filter management

The `My Filters` button offers the following options:

- **Predefined filters.** List of filters offered by default in Workspaces.
- **User filters.** Option visible when a user has saved a filter. Allows you to apply the names of the filters previously created.
- **Save current filter.** If a user wants to return to a list of items later, after applying one or more filters, they can do so from this option.
- **Manage filters.** Allows you to edit the saved filters.
- **Delete filter.** Useful when you want to delete the applied filters and reset the list of items.
- **Workspace groups.** Visible from the Workspaces view, allows you to select items from the list and save them as Workspace Groups. More information here.
- **Filter by Organizational Unit (OU).** Visible from the Workspaces view, filters by organizational unit.
- **Filter by Operating System (OS).** Visible from the Workspaces view, filters by operating system type.

- **Filter by installed applications.** Visible from the Workspaces view, filters by installed applications.

In the top menu, the icons allow:

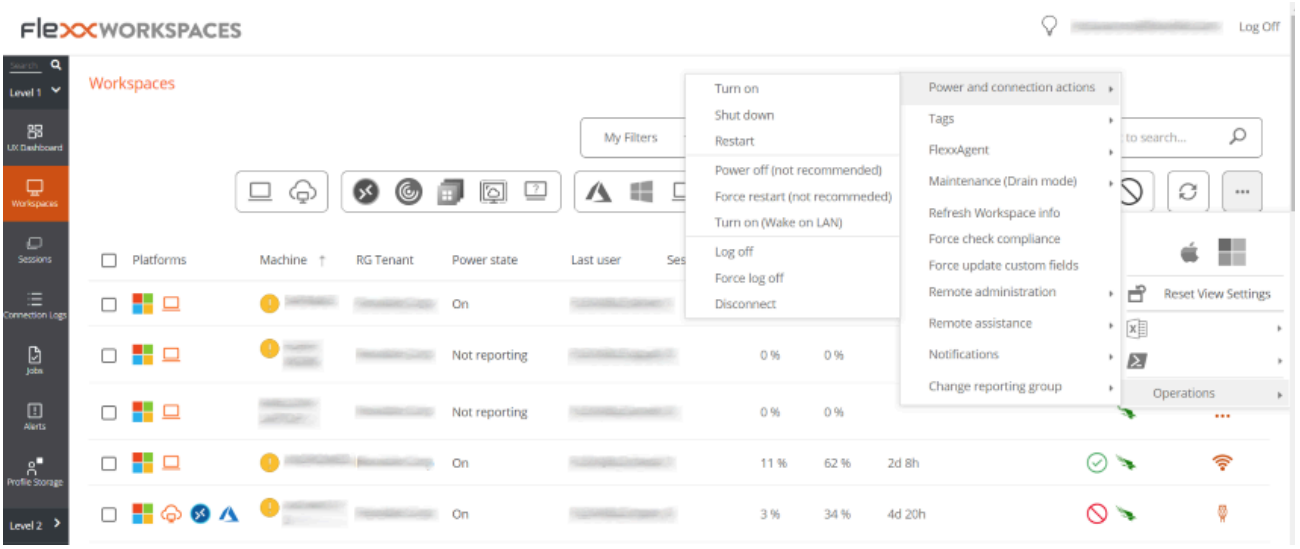
- Set predefined filters.
- Reset the default list view.
- Export the list in *.csv or *.xlsx format.
- Depending on the view from which it is activated, the button `>-`, will give access to various microservices, such as clearing the browser cache or updating the operating system.
- Depending on the view from which the `Operations` button is activated, different actions will be accessible, such as shutting down devices or sending a notification.

Microservices execution

From the `>-` button, you can run any microservice enabled for the organization that has *System* as a 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 provided.



Operations from the list view

The following operations can be performed:

Power and connection actions

- Turn on (only available for devices with an associated broker).
- Power off the device.
- Reboot the device.
- Force shutdown (only available for devices with an associated broker).
- Force reboot (only available for devices with an associated broker).
- Turn on - Wake on LAN (Only available for compatible physical devices configured to support remote power-on via Wake on LAN).
- Log off user.
- Force log off user.
- Disconnect user session.

FlexxAgent

Update the agent on the selected devices to the latest available version.

Maintenance (drain mode)

Only available for devices with an associated broker, configure the maintenance mode (Citrix) or Drain (AVD), which inhibits login for new users on the configured hosts.

Refresh device info

Refresh the data of the selected virtual devices with the Citrix and/or Azure broker, simply update the device's brokering information and it is of great help 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

Force the compliance evaluation of regulations and allows evaluating the compliance of these on the device after making the necessary corrections, without waiting for the refresh time configured in the regulations 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 the Workspaces console deployment within the same subscription (also requires network-level connectivity `Workspaces` -> `Session Hosts`).

Flexxible Remote Assistance

Allows launching three types of remote assistance:

- Interactive (Attended)
- Unattended
- Dynamic

> **INFO**
>
> On multi-session devices, dynamic remote assistance will only work if there is a single concurrent remote assistance session on the device.

Device type

Define the type of device, so they can be organized into different views of the console. 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 of the organization or its infrastructure. It is visible in the `Servers` section.
- **Hidden.** Allows a device to be hidden from all lists.

Notifications

Send notifications to the selected devices. They can be pop-ups or ones that reserve a screen space.

Change the report group

Allows changing the report group of the selected devices, even when they are powered off. When performing this action, the configuration of the target report group will be applied, which includes:

- Configuration of Flexxible Remote Assistance

- Organization users with access or visibility
- Associated update policy

If the user making the change has access to more than one organization, they can also "move" the devices to a report group of another organization.

When changing the report group of a powered-off device, the operation is scheduled and executed when the device is powered on.

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, you can execute any microservice enabled for the organization that has `System` as 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 device and/or a description.

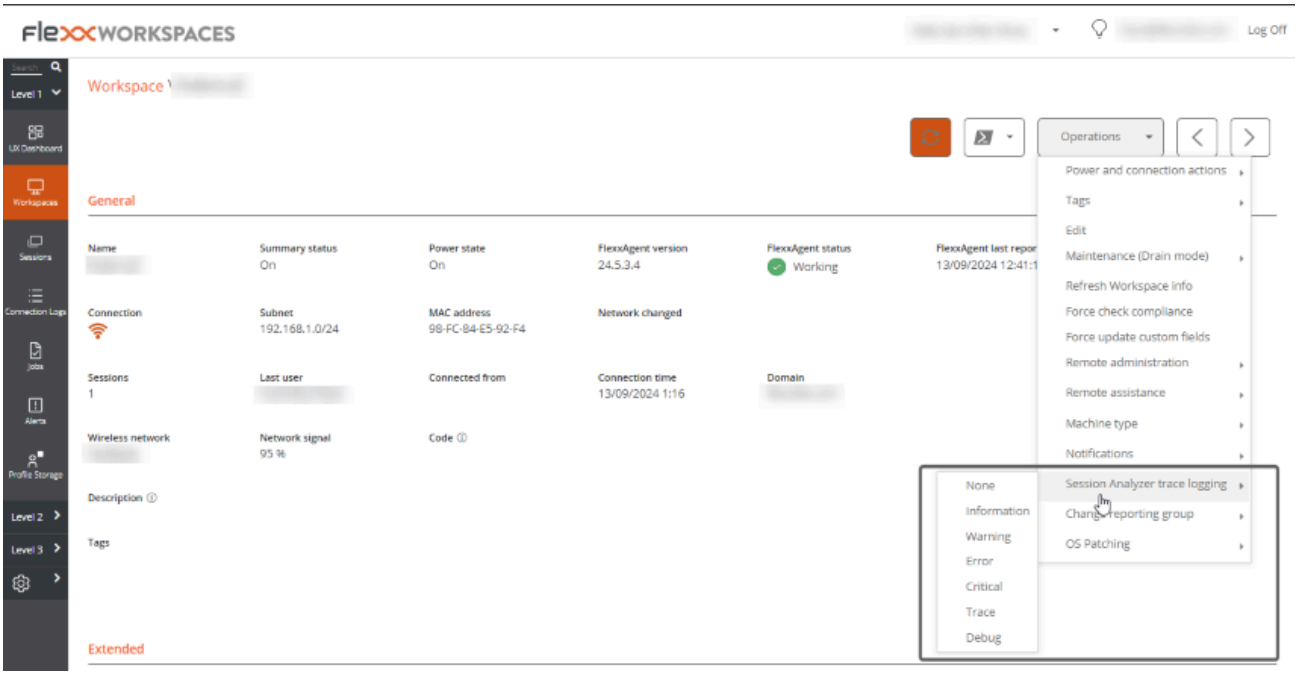
The code allows associating the device with an inventory item. To edit it, click on `Operations` -> `Edit` -> `Code`.

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

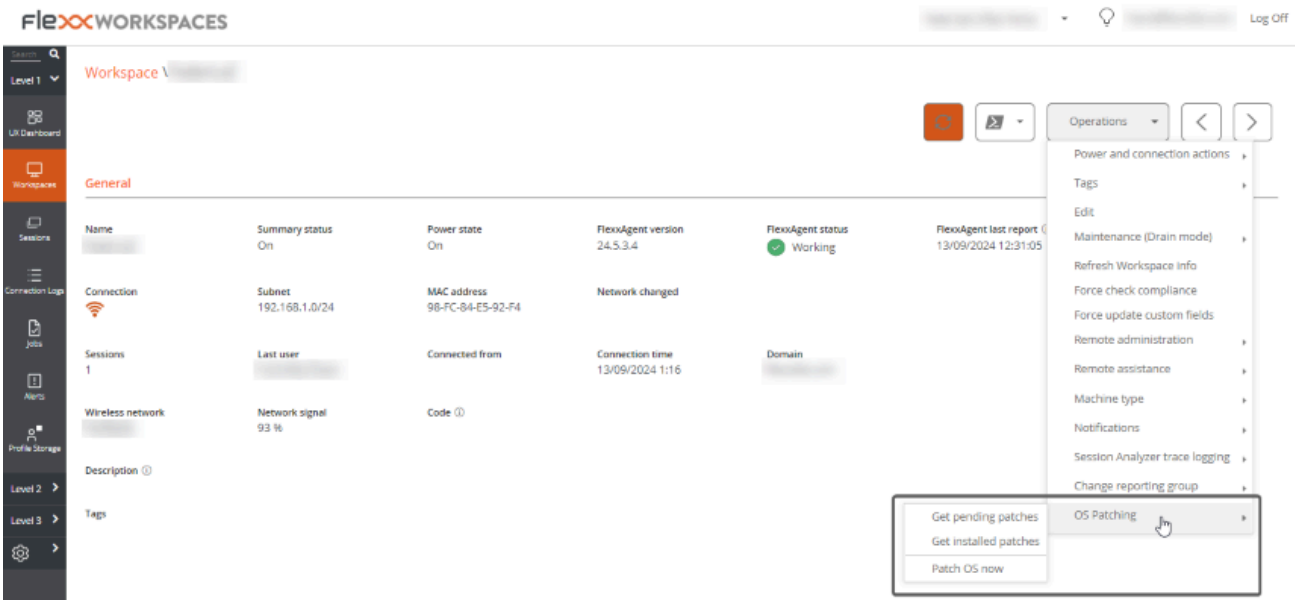
FlexxAgent Analyzer logs can be configured to include or exclude information by criticality levels. From `Operations` -> `Session Analyzer trace logging` you can manage the log level change for FlexxAgent Analyzer.



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 the patches available for installation on the device, in list format.
- **Get installed patches.** Retrieves the patches installed on the device, in list format.
- **Patch now.** Installs 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 / Flexxible Remote Assistance

Flexxible Remote Assistance is a feature designed to facilitate secure and efficient technical support, allowing an operator to remotely access a device and take control of the user's session to diagnose issues, apply changes, or execute administrative tasks.

The solution enables the management of any application visible to the user, including those requiring privilege elevation or running under User Account Control (UAC), ensuring a temporary operation with a strict focus on security and privacy.

Main features

- Compatible with user sessions on physical devices, VDI, shared desktops, and virtualized application environments.
- Works with or without a proxy.
- Supports both end-user devices and unmanned devices (servers or kiosks).
- Compatible with Windows.
- Useful for occasional support sessions or as a remote access mechanism to infrastructure (e.g., servers).

Privacy and security

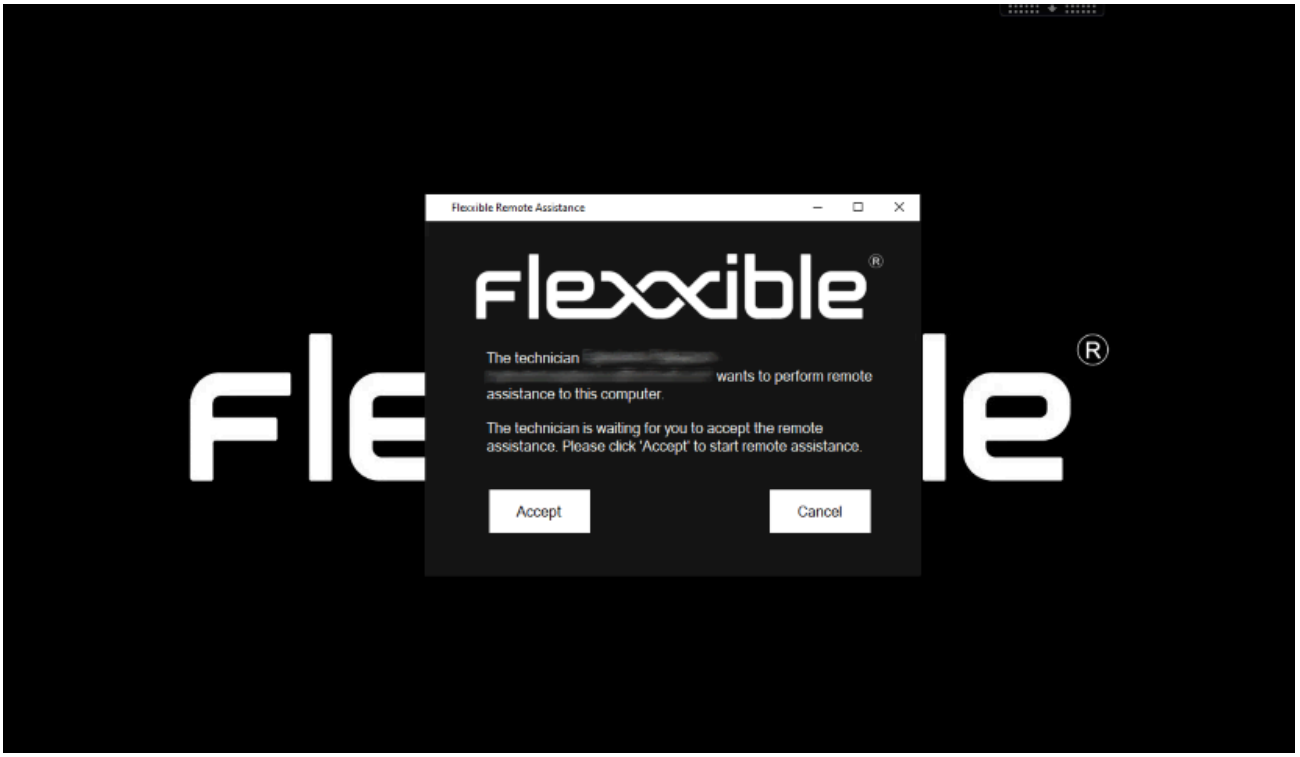
- To minimize the attack surface and reduce vulnerability exploitation risks, FlexxAgent does not install additional software, so there is no service "listening" for incoming connections. Only runs (without installation) in real-time when requested from the Workspaces module.

- Audio redirection is disabled by default to prevent the operator from listening to conversations if the user is on a video call.

Flexxible Remote Assistance - Types

1. Interactive (Attended)

Allows the operator to connect to a device and take control of the user's active session, after obtaining their explicit consent. This connection mode provides secure and supervised access to the user's environment, facilitating real-time issue resolution and support actions.



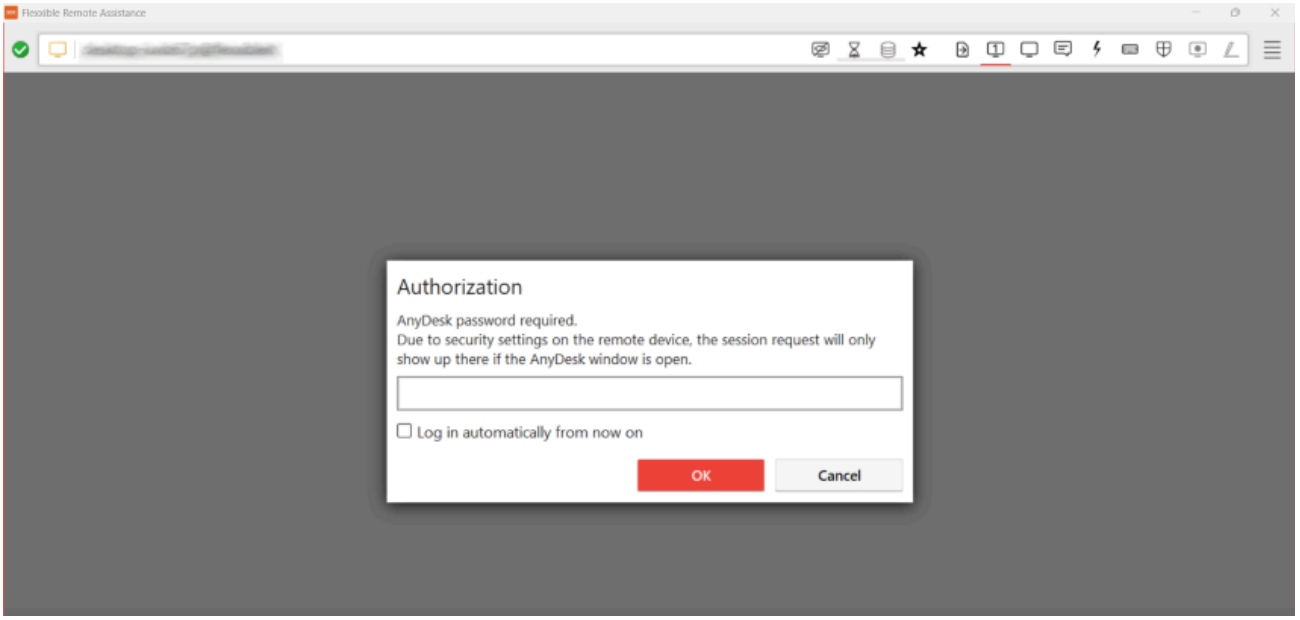
2. Unattended

Allows an operator to access and control a device without needing a user to be present. It is aimed at server-type or kiosk devices.

When this type of assistance is initiated, FlexxAgent shows the operator the necessary data to connect:

- **Session ID.** Session identifier.
- **Password.** Dynamic password that regenerates in each session (it is not recommended to store it).
- Download the activation file for the operator.

The operator must enter the password when executing the activation file to take control of the device.



> INFO
>
> 15 minutes after the end of the connection, the service is automatically deactivated and the password expires. Neither the file nor the authentication data are reusable.

3. Dynamic

Allows the operator to access the device regardless of whether or not there are active user sessions.

- If there is an active session, the interactive (attended) assistance process is initiated.
- If no active session exists, unattended remote assistance is launched, even allowing login with other accounts without interfering with user data.

Considerations

- On devices configured for dynamic remote assistance, it will not be possible to initiate unattended remote assistance on any session of the device from `Sessions` in the Workspaces module.
- Requires the device receiving assistance to have FlexxAgent 24.9.2 or higher installed.
- Even though the report group to which the device belongs is configured for dynamic remote assistance, the option to execute all three types of assistance will still be shown in the Workspaces module, but only the dynamic one will be functional.

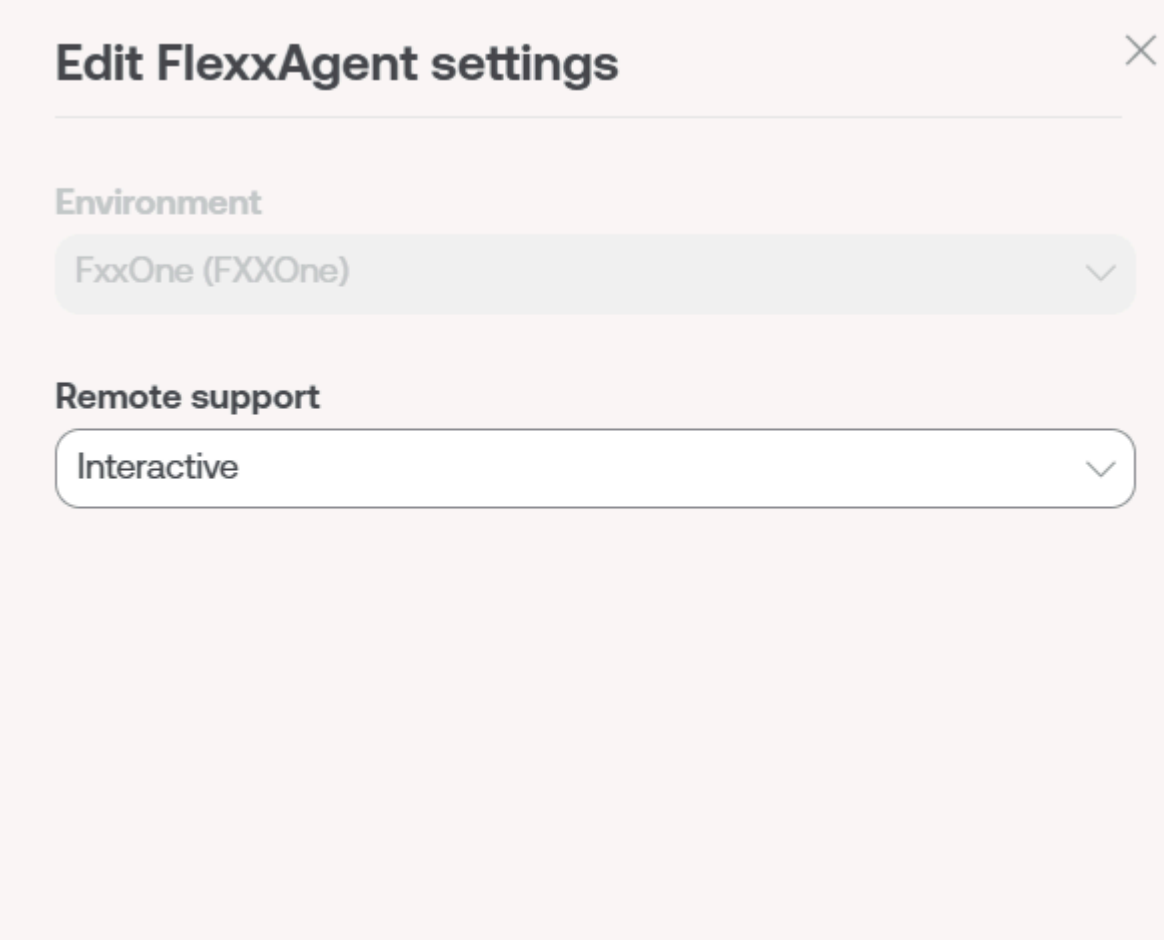
Requirements

- The device receiving remote assistance must have **FlexxAgent 23.7 or higher** (24.9.2 for dynamic assistance).
- Connectivity to https://ras.flexxible.com via TCP port 443.

> INFO
>
> Remote assistance will be interrupted if FlexxAgent is restarted during its execution.

Settings

A device cannot receive remote assistance if it is not enabled for it from the FlexxAgent Configuration (Flexxible Remote Assistance) of its report group. There you can define what type of remote assistance it can receive.



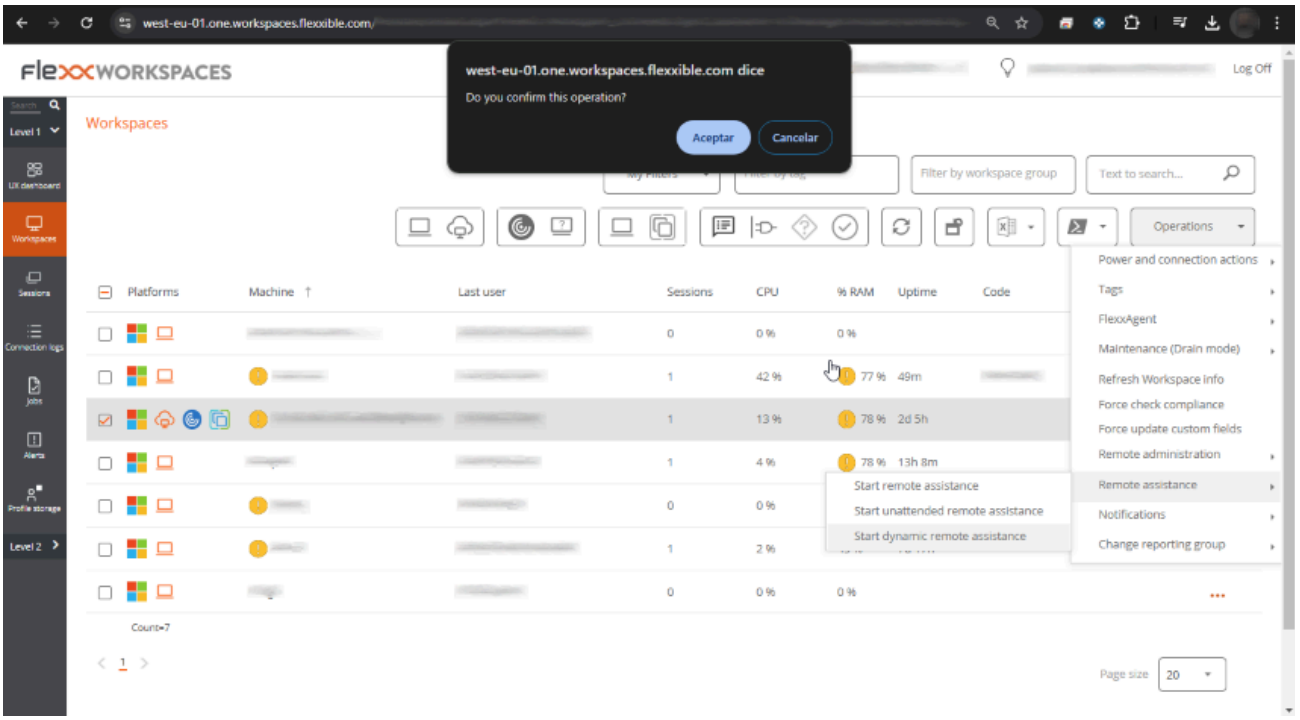
Activation

The execution of Flexxible Remote Assistance can be done at the device or session level.

Appliance

1. Access the Workspaces module -> `Level 1` -> `Workspaces`.
2. Select the device.
3. Click `Operations` -> `Flexxible Remote Assistance`.

4. Choose the type of remote assistance you want to execute.



Session

1. Access the Workspaces module -> `Level 1` -> `Sessions`.
2. Select the session.
3. Click `Operations` -> `Flexxible Remote Assistance`.
4. Choose the type of remote assistance you want to execute.

When the operator requests to start assistance, FlexxAgent runs a process and notifies the user.

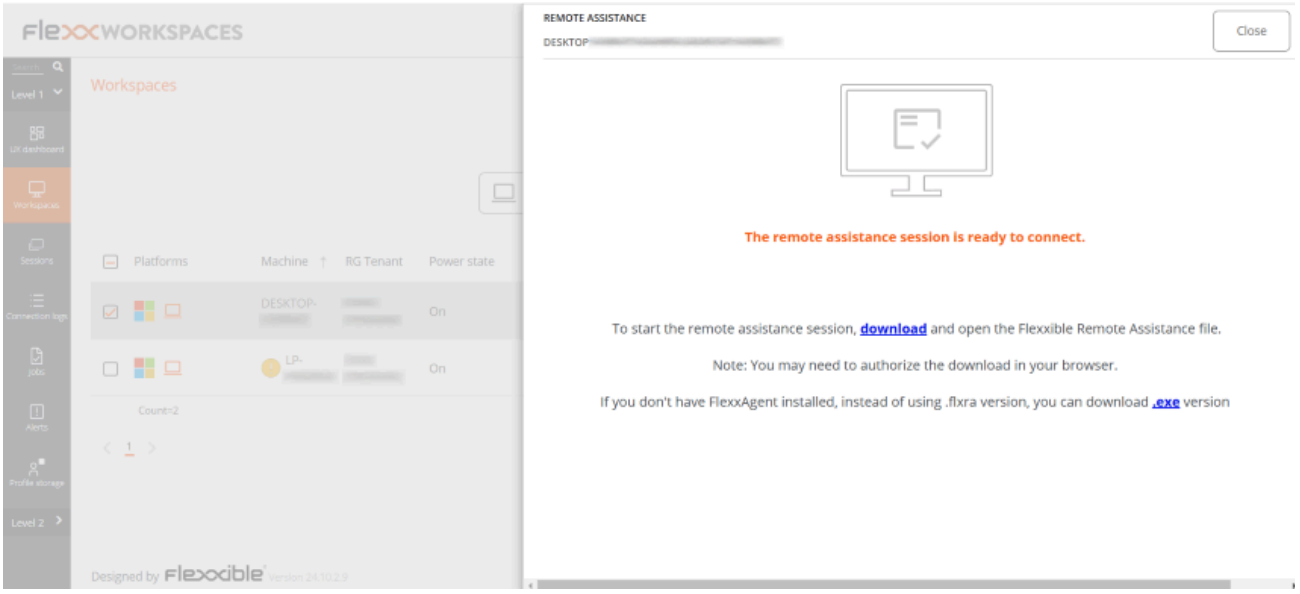
Activation file

The operator must download an activation file to provide the service. This will depend on whether the support-providing device has FlexxAgent installed or not.

Devices with FlexxAgent installed

The operator must download and run the Flexxible Remote Assistance file, which has the extension .flxra.

- Runs without installation, with user permissions.
- Remains active only during the session.
- Once finished, it stops and the file is automatically deleted from the system.

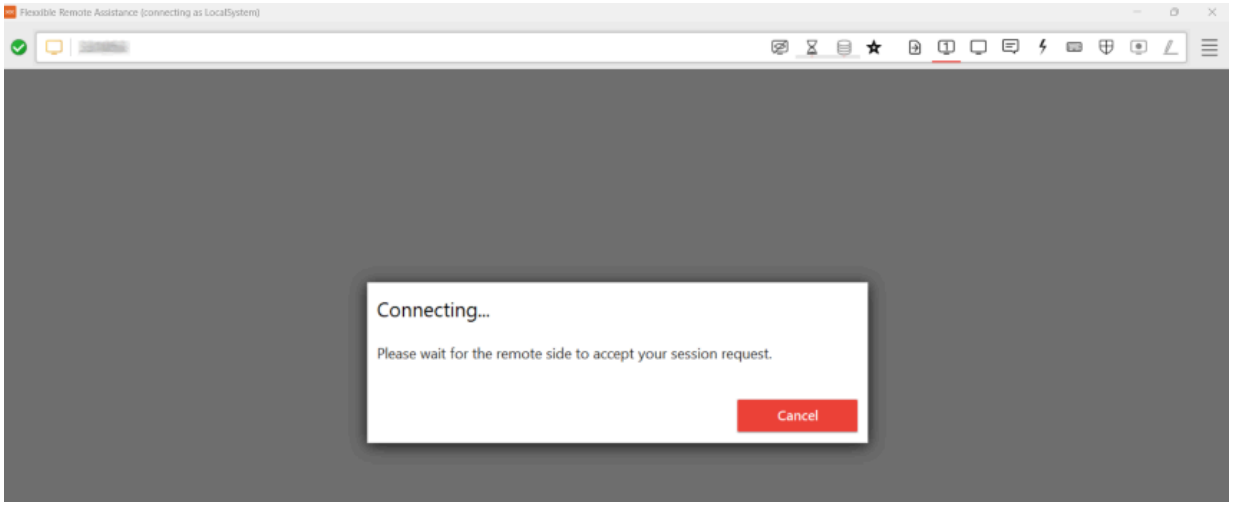


Devices without FlexxAgent installed

The operator must download and execute the file with the extension **.exe**.

- Runs without installation, with user permissions.
- Remains active only during the session.
- The file is not automatically deleted after the session ends.

In both cases, the user's consent will be required before the operator can take control.

> *View from the operator's screen:*
>
> 
>

View from the user's screen:

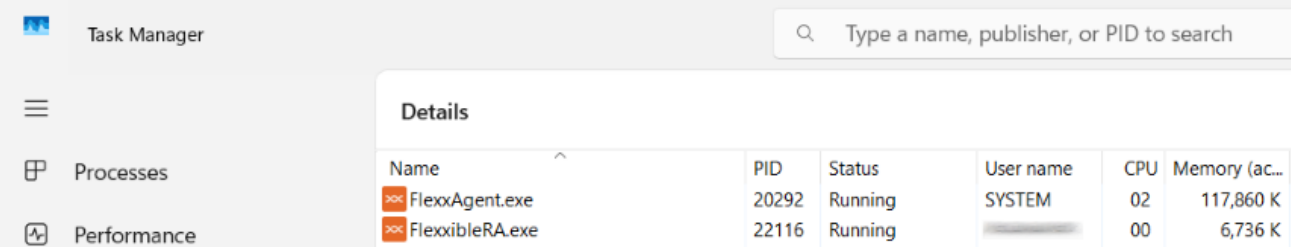
INFO

Even if the file is executed without administrative privileges, the operator will have access to administrative tools through Flexxible Tools.

Generated Processes

Executing the activation file starts two processes:

- FlexxAgent.exe
- FlexxibleRA.exe



Operation through proxy

From the operator's point of view

When executing the activation file, FlexxAgent checks if the **Proxy_Url** key exists:

- If it detects it, it uses it.
- If not, it runs AnyDesk in autodetection mode.

From the end-user's point of view

FlexxAgent checks if the proxy is configured.

- If it detects it, it uses it.
- If not, it runs AnyDesk in autodetection mode.

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.
- If not, it runs AnyDesk in autodetection mode.

Flexxible Tools

The remote assistance file runs with user permissions. If the user does not have admin privileges, the operator can use **Flexxible Tools**, available in interactive (attended) remote assistances.

Flexxible Tools allows the operator to run administrative tools.

- CMD
- PowerShell
- Registry editor
- Task Manager

Settings

Flexxible Tools can be activated for users depending on their role in Portal. This can be done in two ways:

From Product

1. Go to `Portal` -> `Settings` -> `Organization`.
2. In the menu, click the `Products` tab.
3. Click `FlexxAgent Configuration` in the record of the desired product.

This allows applying the change to all report groups.

From Report Groups

1. Go to `Portal` -> `Settings` -> `Reporting Groups`.
2. Click `FlexxAgent Configuration` in the record of the desired report group.

This allows enabling or disabling the functionality for one or more report groups.

> **INFO**
>
> Flexxible Tools requires that both the operator's device and the assisted one belong to the same FlexxAgent environment.

Connection Detection

The Jobs section in the Workspaces module allows identifying the start and end time of a remote assistance session. The job status accurately reflects the operator's actual activity and records all events related to their connection.

Job Start

When an operator presses the `Flexxible Remote Assistance` button, a job is automatically created with the status `In Progress`. From there, the system monitors whether a connection is established by the operator.

Job Closure

- **Automatic Closure.** If no active connection is detected within the first five minutes, the job is closed automatically. In this case, the following record is added:

  ```
  The job has been closed. No active remote assistance connections detected.
  ```

- **Closure after connection ends.** The job is closed if a remote assistance connection is detected and it ends successfully.

Reconnections

If the operator reconnects to the same device, the job will automatically return to the `In Progress` status. Once the new connection ends, the system marks it as `Completed`.

Job Detail

The job details of each connection are displayed as follows:

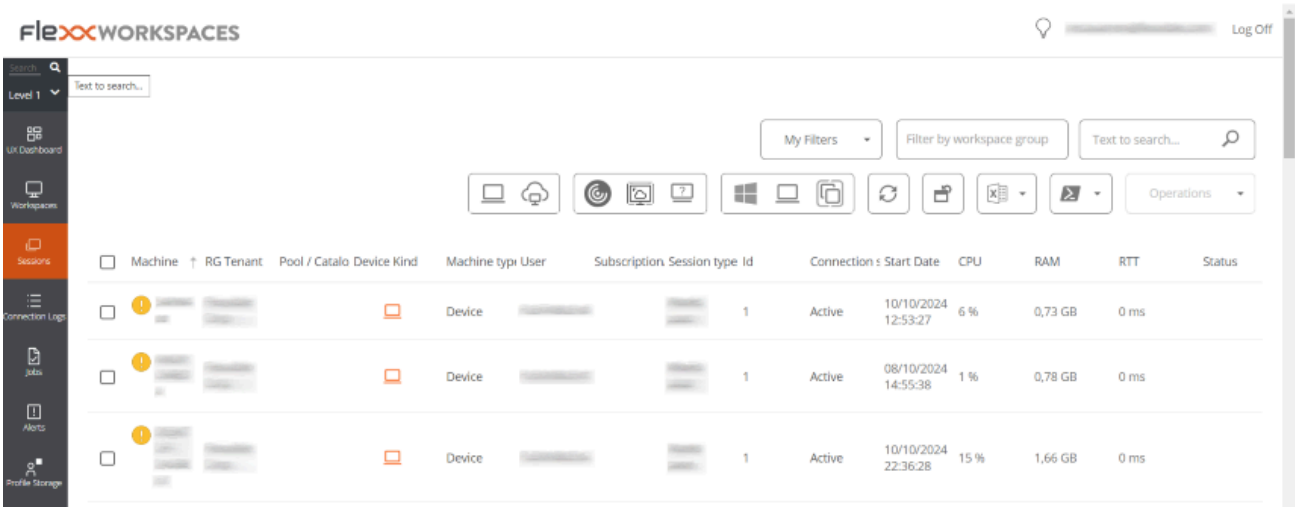
```
09/10/2025 10:43:05 (UTC) - Remote assistance connection started from the
id 276790 to the id 941120
09/10/2025 10:41:49 (UTC) - Remote assistance started at 09/10/2025
12:41:49 local time
09/10/2025 10:45:00 (UTC) - Remote assistance ended at 09/10/2025
12:45:00 local time
09/10/2025 10:45:00 (UTC) - Connection duration: 191s
```

INFO

In unattended remote assistance where multiple operators work on the same device, it may not be possible to accurately determine which job each connection belongs to.

Workspaces / Level 1 / Session View

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 generated using the 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
- Log off

Flexxible 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 the selected devices. Notifications can be pop-up notifications or notifications that reserve a screen area.

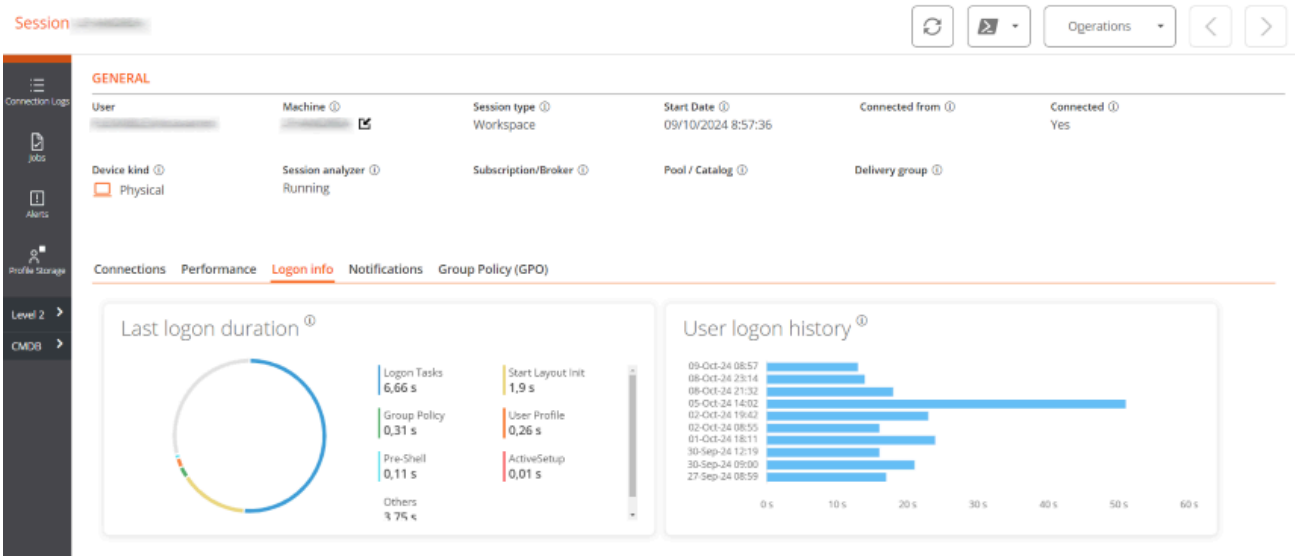
INFO

On some devices with Windows 10 1903+, the Automatic Restart Sign-On (ARSO) can create "ghost sessions" in the session view after an update restart. To adjust this behavior, please refer to this guide.

Workspaces / Level 1 / Sessions / Detail view

Clicking on a record from the session list provides access to the details of the selected session. The interface is structured into three 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

Using the `>-` button, you can run any of the microservices enabled for the organization that have `Session` as the configured context. This allows the execution of microservices

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:

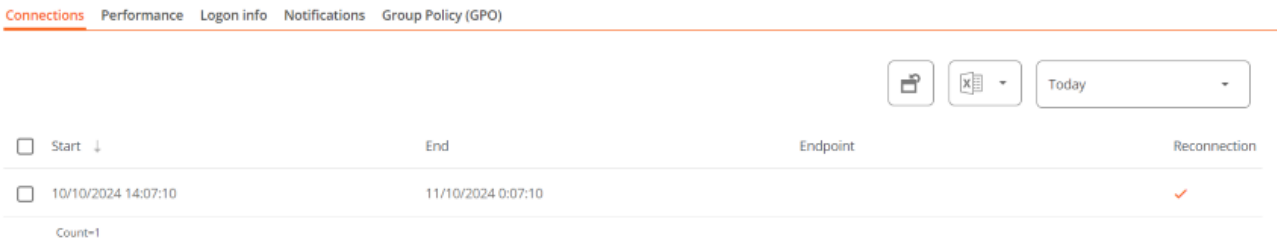
- **User.** Session user in domain\user format.
- **Machine.** Device hostname.
- **Session Type.** Session type, which can be Workspace or application for virtualized application sessions.
- **Start Date.** Date and time of session establishment.
- **Connected From.** When the selected device is a VDI or similar, it displays the name of the endpoint from which the virtual device is accessed.
- **Connected.** Indicates whether the user is actively connected to the session or if they have disconnected from it.
- **Device Type.** 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 (e.g., Microsoft Azure Virtual Desktop (AVD), Citrix DaaS, Citrix On-premises).
- **Group/Catalog.** If used, a collection of machines that defines the specifications of the devices and how they are provisioned to users. e.g. host pools in Azure Virtual Desktop or machine catalogs in Citrix).
- **Delivery Group.** If used, a collection of machines 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:

- Connections
- Performance
- Login information
- Notifications
- Group Policy (GPO)

Connections

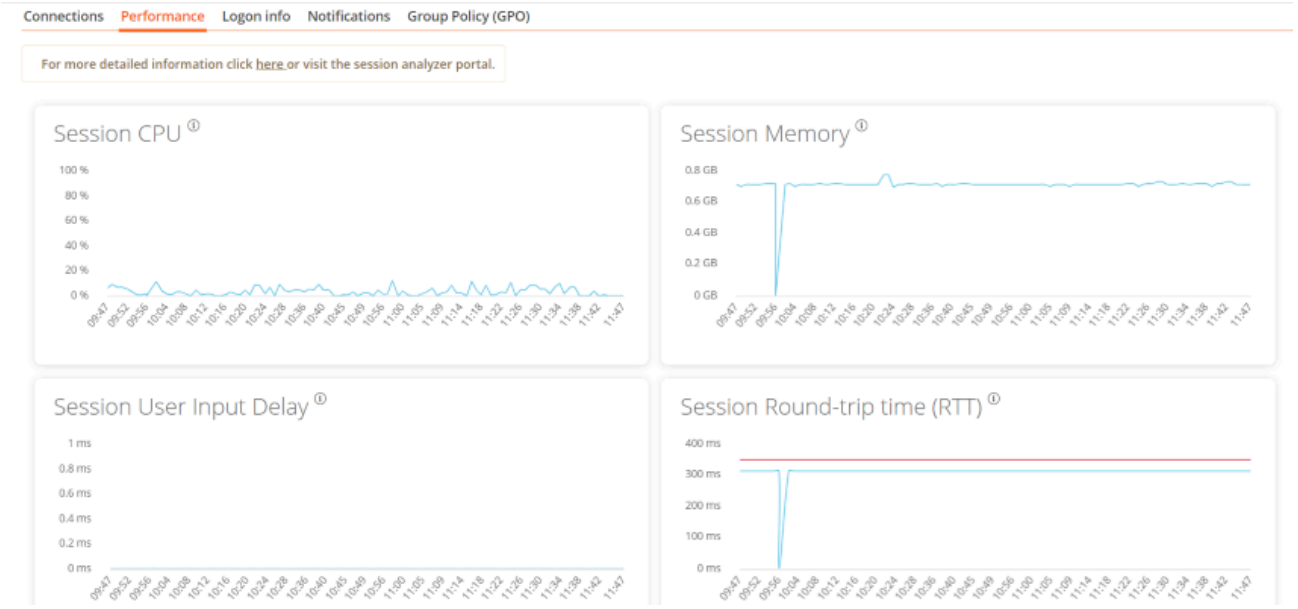


This tab contains information about the device's connections, i.e., each time a user starts or reconnects a disconnected session.

> 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 processor usage for the session, excluding resources used by other sessions or system processes.
- **Memory.** Amount of memory used, excluding resources used by other sessions or system processes.
- **User Session Input Lag.** The user's input lag refers to the time span 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.
- **Session Round-Trip Time (RTT).** Time it takes for a data packet to travel from the user's device to a server or remote destination and then 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

This tab allows you to see detailed information about the user's login times. The view consists of two graphs:

- Duration of last login
- User login history

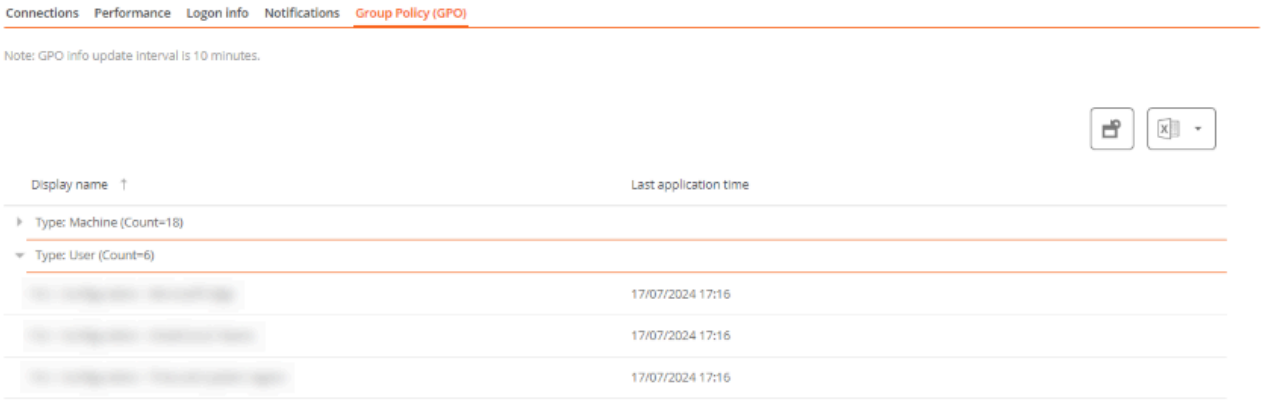
At the bottom, a table presents the details for each user login.

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.

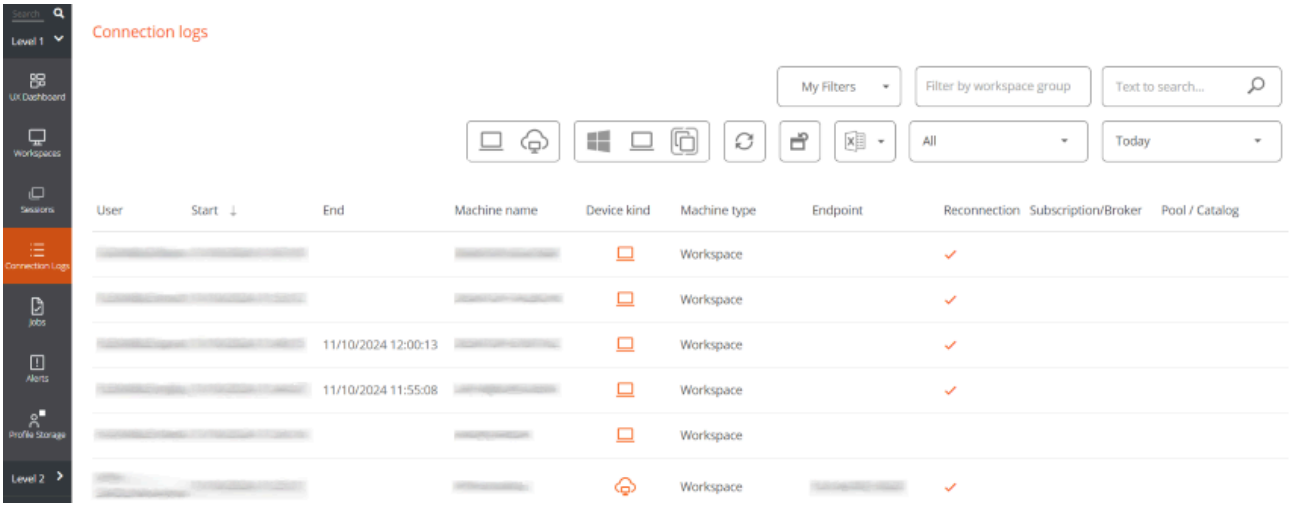
Group Policy (GPO)

This tab shows the information of group policies applied in the active session. It shows the name of the applied policy both at the user level and device level.



Workspaces / Level 1 / Connection Logs

The connection log allows you to view the historical session logs of users in the organization.



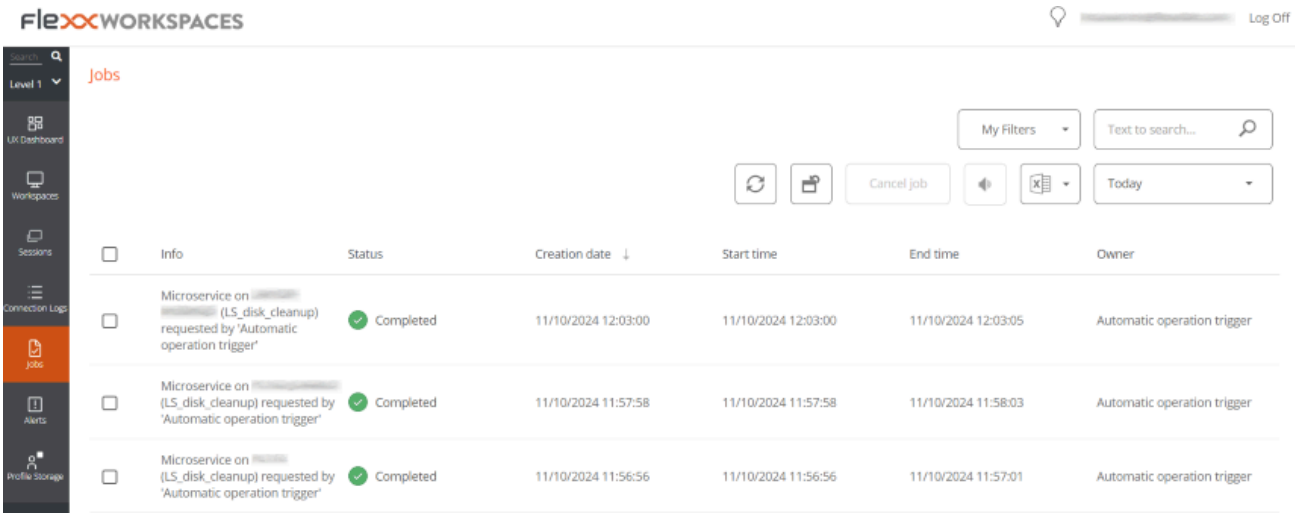
The information provided in this view is (by default):

- **User.** Username of the session account.
- **Start.** Date and time of connection start.
- **End.** Date and time of connection termination (an empty field means the session is still open).
- **Machine Name.** Device the user is connected to.
- **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 physical origin connection equipment.
- **Reconnection.** Checks if the current session is a reconnection of the previous one.
- **Subscription/Broker.** Name given to each supported subscription and broker.
- **Group/Catalog.** Name of the host group containing the device.

Workspaces / Level 1 / Jobs

Every action performed in Workspaces generates a **Job**. These allow you to analyze the outcome of the executions performed; for example, by checking the output of a microservice execution. **Jobs** collects all the jobs performed in the organization, which also provides historical execution records, allowing 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

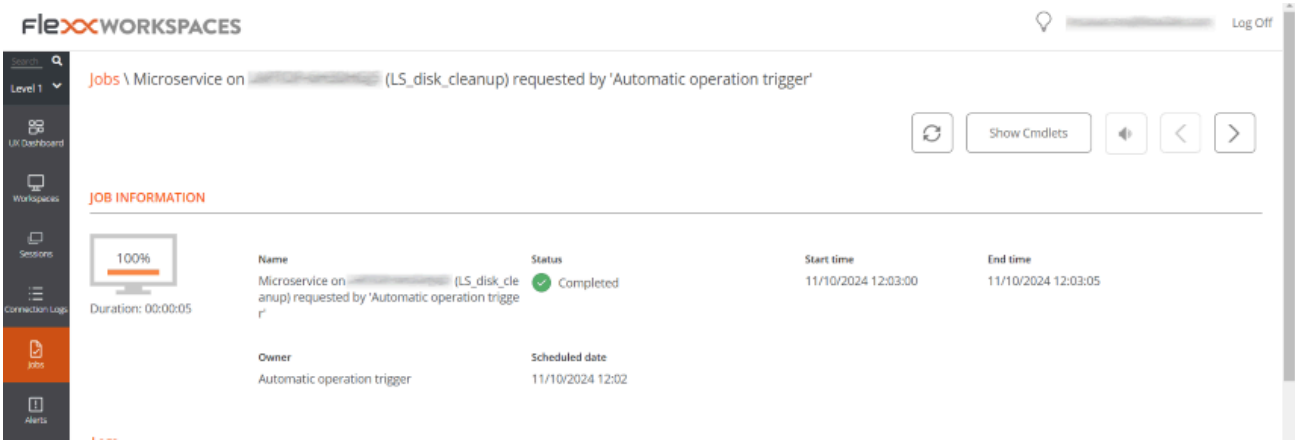
- Refresh the job list and show updated values.
- Resets all settings made for the jobs view.
- Filter jobs by age:
  - Today (default filter)
  - This week
  - This month
  - This quarter

    - This year
- `Cancel` allows you to cancel pending jobs.
- `Notify` allows you to subscribe to a specific job to receive an email notification when it's completed.
- `Export to` allows you to export in the selected type.
- `My filters` allows you to access `Predefined filters` or user-created ones.
- 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

- **Pending.** The task is pending to start.
- **In progress.** The task has started and is still ongoing.
- **Completed.** The task is finished.
- **Error.** The task has not finished correctly or has ended with errors.

- **Cancelled by user.** When a user cancels the task.
- **Completed with errors.** When the task is completed, but at least one step failed with non-critical errors.

If a job takes too long in the *In progress* status without logging any information, its status will automatically change to *Error*. However, this does not mean that the job will not be completed successfully, but that the timeout was exceeded due to an activity block during 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`.

Workspaces

The `Workspaces` tab allows you to easily see the information of the devices that executed the job, in case of multiple executions.

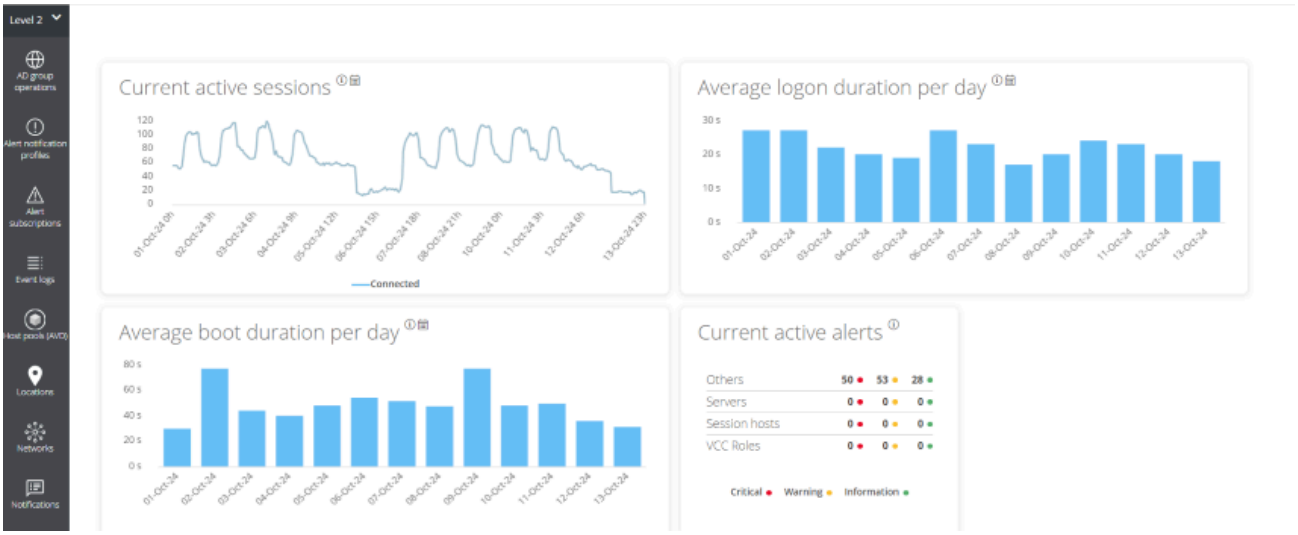
Job subscription

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 2

This level of Workspaces 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.

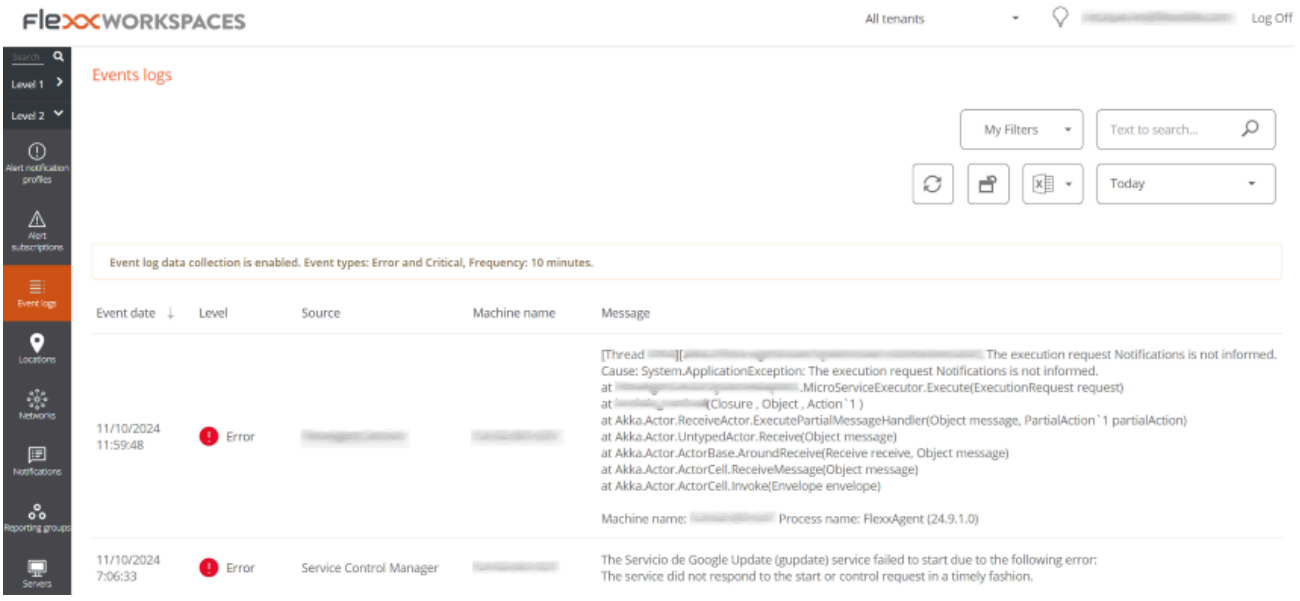


Functionalities available at this level:

- Event Logs
- Locations
- Networks
- Notifications
- Reporting groups
- Servers
- Wifi networks

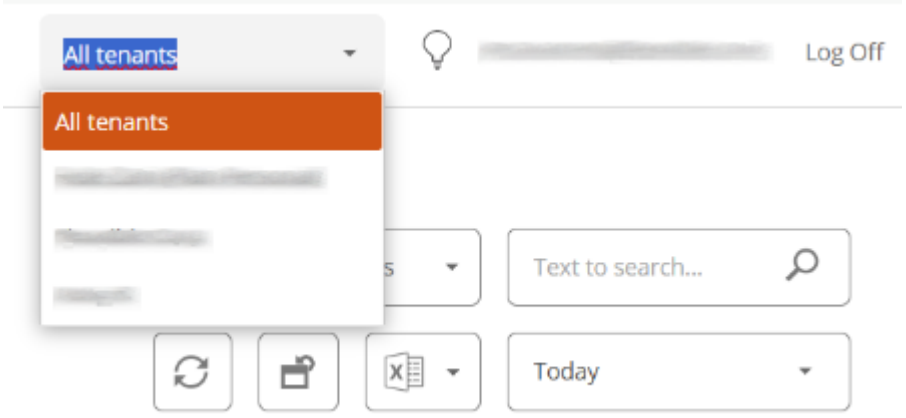
Workspaces / Level 2 / Event Logs

Event Log is a diagnostic tool designed to centralize the events generated by the system. It shows exclusively those of type *Critical* and *Error* in Windows environments, from the Application, Security, and System logs.



> **INFO**
>
> Events are logged every 10 minutes, although this time can be manually configured from the Workspaces settings.

At the top of the interface, you will find the organization dropdown. If a user has access to more than one tenant, they can choose to view the event log for the selected tenant.



Filtering options

Event filtering allows you to view and select only the items that meet specific criteria, temporarily hiding the rest. The event list supports the same filtering options available in the Workspaces view.

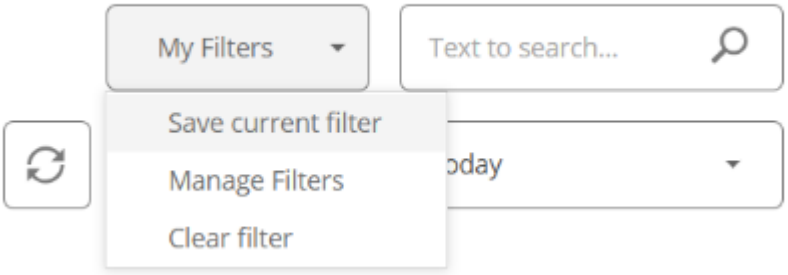
An example would be to filter by an event with a specific ID to obtain a list of affected devices, subsequently applying corrective actions.

My filters

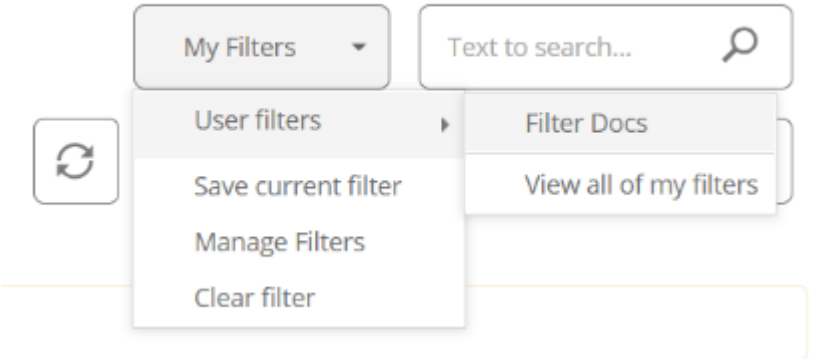
In the top menu, the option `My filters` allows access to three filter configuration options.

Save the current filter

Opens a modal window with a form that prompts for the necessary information to assign a name to the filters applied to the event list so that it is available whenever you want to use it.



When the filter is saved, it appears as a new dropdown option.



Manage filters

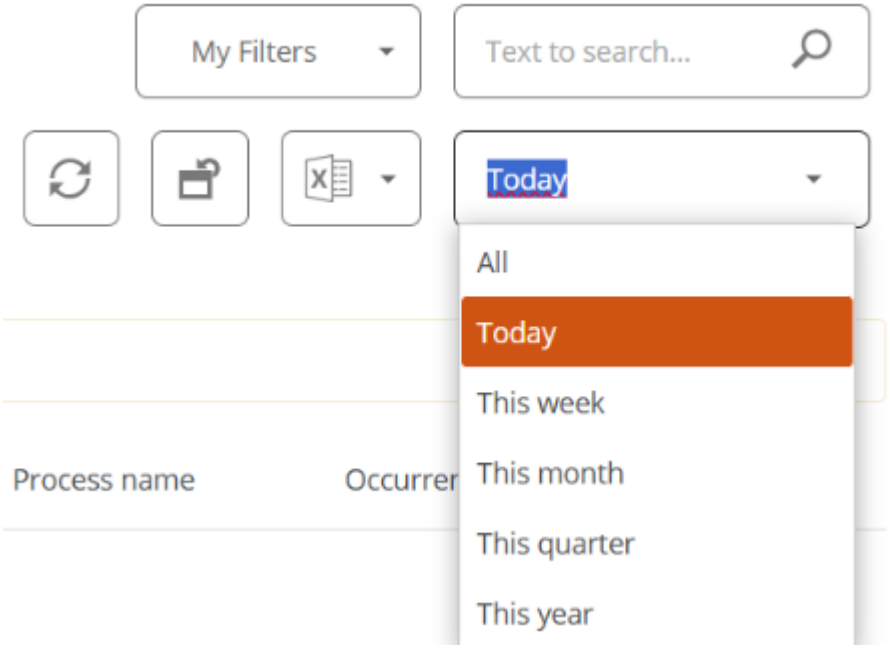
Allows you to apply value filtering on the event list and also edit or delete user saved filters.

Delete the filter

Allows you to delete the filters applied to the registered event list.

Temporary filter

In the top menu is the temporary filter, which by default shows the events recorded on the current day.



Available filters

- Today
- This week
- This month
- This quarter
- This year

> **INFO**
>
> If the option *All tenants* is selected in the organization dropdown, only events from the current day (*Today*) can be seen.

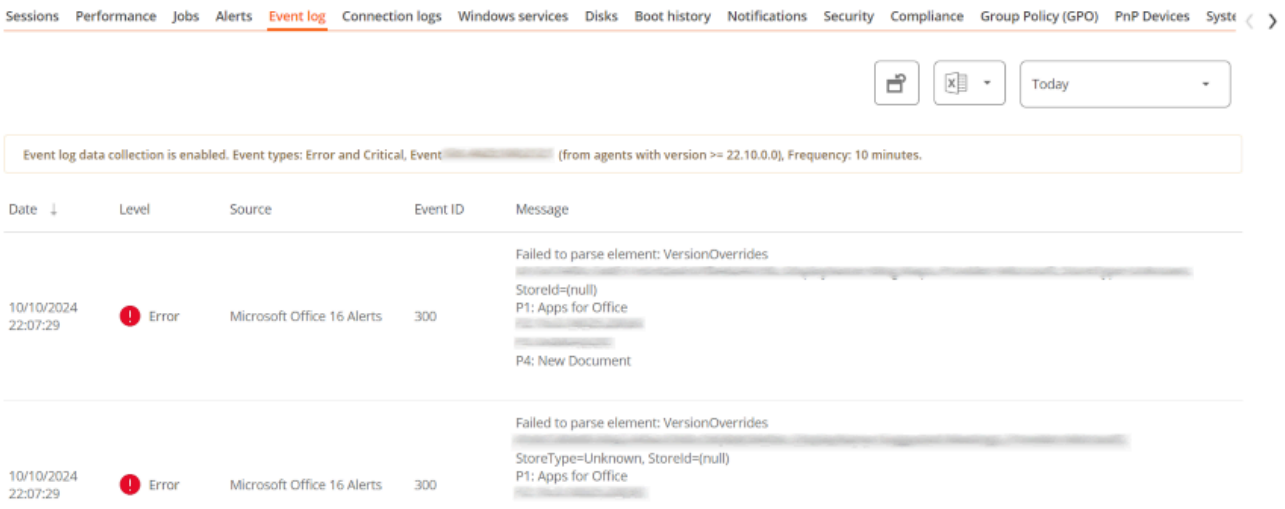
Detail view

The detail view contains detailed event information:

- **Event date.** Date of event logging in day and time format.
- **Level.** Severity of the event.
- **Source.** Source of the event.
- **Event ID.** Numeric identifier of the event.
- **Log file.** Event log file hosting the event.
- **Machine name.** Hostname of the device logging the error.
- **Message.** Content of the event message.

Event log information on a device

The detail view of a Windows device allows viewing of event logs for a specific device.



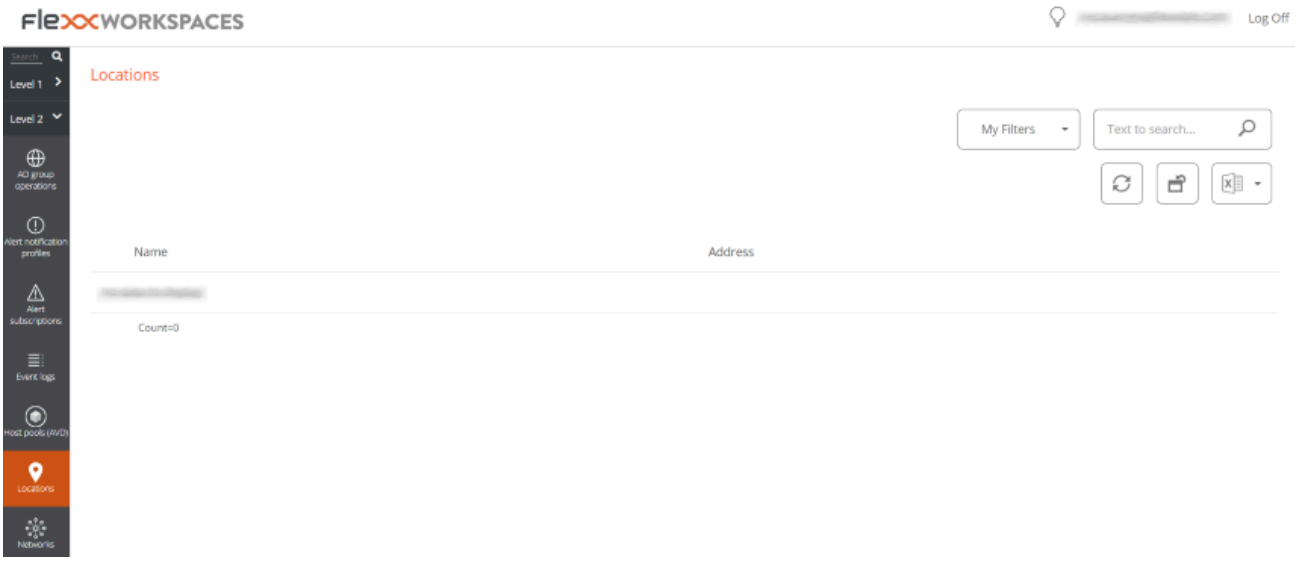
Additional event settings

Users with the *Organization 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:

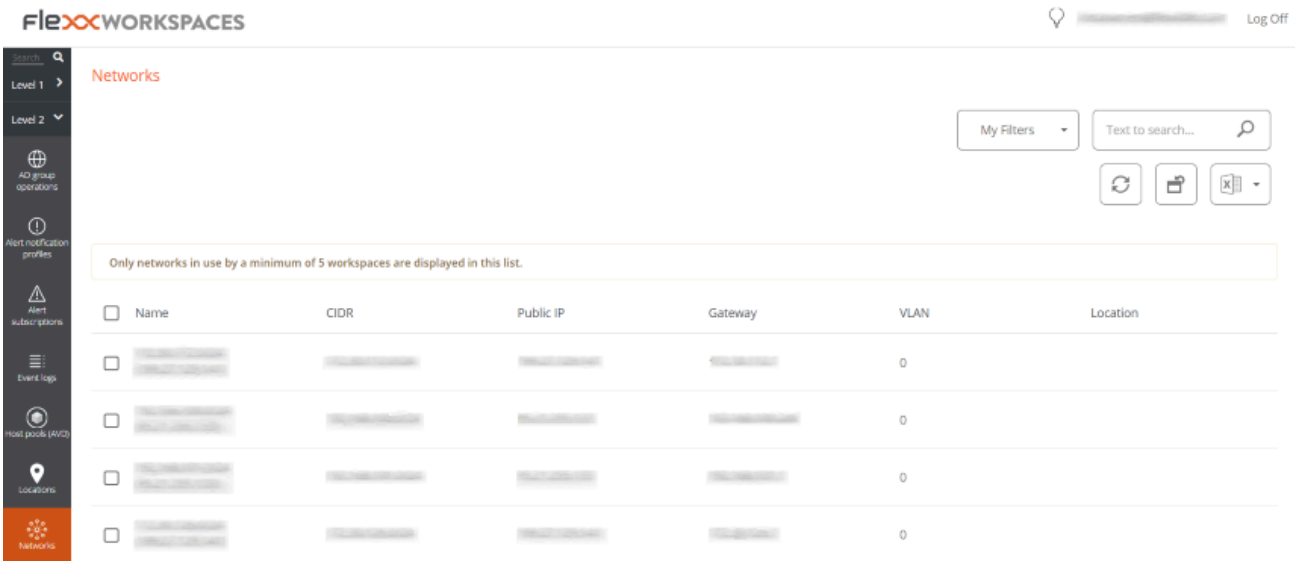
- **Name.** Friendly name of the location.
- **Address.** Postal address.
- **Latitude.** Numeric value of latitude.
- **Longitude.** Numeric value of longitude.

At the bottom, you can see the tabs:

- **Networks.** Networks identified by FlexxAgent included in this location; 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.

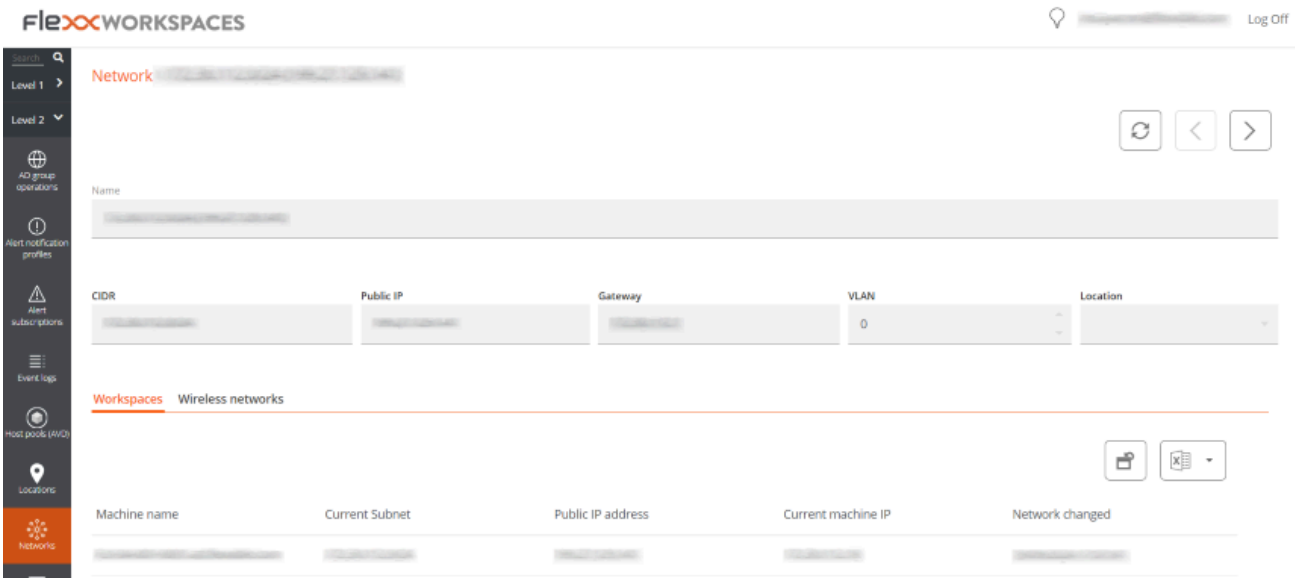


List view

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.** Name of the network; by default the CIDR followed by the public IP. Allows customization.
- **CIDR.** Network CIDR.
- **Public IP.** The public IP used for internet access from the network.
- **Gateway.** IP address of the network gateway.
- **VLAN.** Identify VLAN, if any.
- **Location.** Location associated with the network. Preconfiguration required.

At the bottom of the interface, there are two tabs:

- **Workspaces.** Shows the list of devices connected to the network.
- **Wireless networks.** Displays 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. Due to their versatility, they are especially useful in service disruption scenarios as they allow communication with users effectively, even when the company's communication infrastructures and tools are not functional.

Types of notifications

Workspaces offers two types of notifications to effectively communicate messages to users.

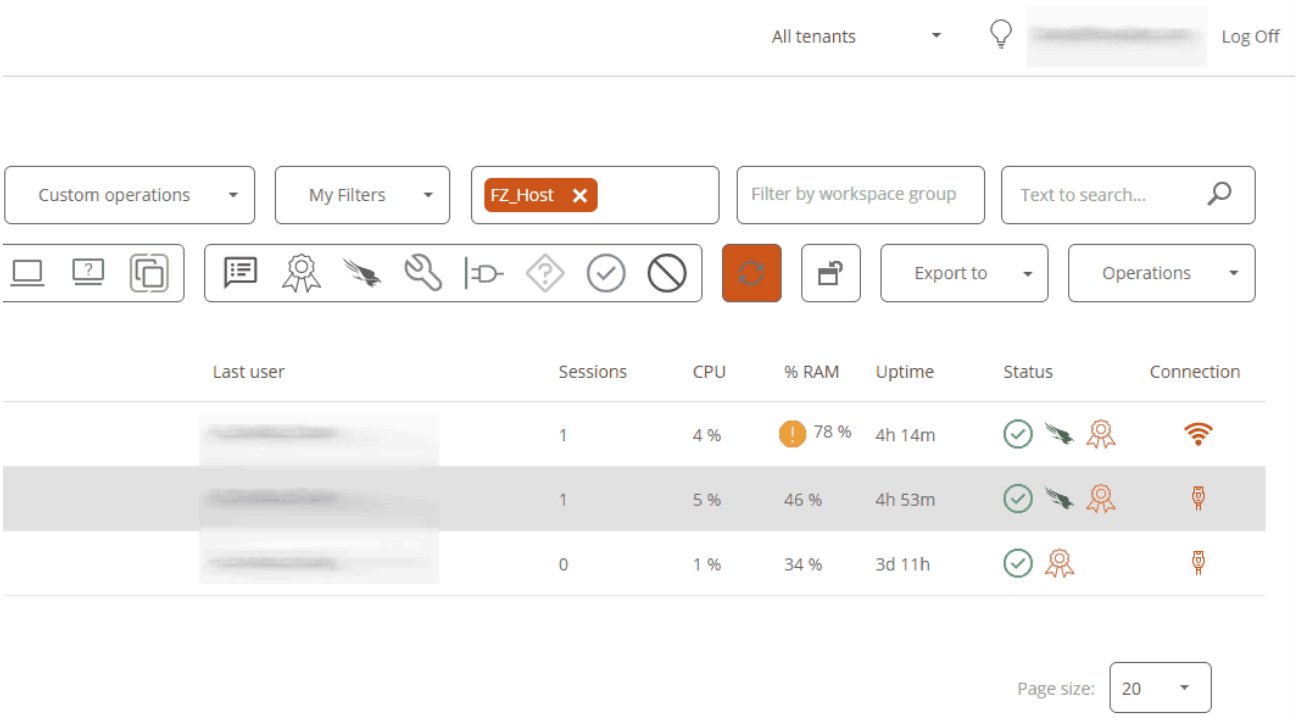
- Pop-up messages
- Notifications

Pop-up messages

They display a window to the user that appears over the interface and can be closed with just one click. They are useful for conveying brief or specific information without permanently interrupting work.

Sending pop-up messages

1. Access the Workspaces module -> `Sessions` or `Workspaces`.
2. Select the target sessions or devices.
3. Click on `Operations` -> `Notifications` -> `Send pop-up message`.
4. Write the message and click `OK`.



The user in the session will receive the message through a pop-up window.

This type of notification is based on Windows system tools. If all devices or sessions are selected and a pop-up message is sent, it will only reach users who are currently working (in session). If any user enters their session after the message is received, it will not be visible.

> **INFO**
>
> In Windows, the pop-up message will remain visible until the user closes it or the session reaches a maximum of three days active. The time does not count while the session is locked or disconnected.

Notifications

The notifications are designed for critical situations, such as service interruptions, where other corporate channels might not be available. Their goal is to ensure the message reaches users as soon as possible, reducing the risk of overwhelming the support team with simultaneous requests.

Notifications have many additional features aimed at maintaining effective communications and protecting the information transmitted to users.

While on screen, notifications reserve that space in such a way that 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 set for time intervals, so that all active and future sessions receive the notification during the defined period.

Sending notifications

1. Access the Workspaces module -> `Sessions` or `Workspaces`.
2. Select the target sessions or devices.
3. Click on `Operations` -> `Notifications` -> `Send notification`.
4. Fill in the fields:

- **Time zone.** Define a time zone.
- **Start date / End date.** Define the start and end dates and times.
- **Severity.** Allows choosing between three levels of severity:
  - **Informative.** Will generate a gray notification.
  - **Maintenance.** Will generate a yellow notification.
  - **Technical Issue.** Will generate a red notification.
- **Request Acceptance.** Enables a button to allow obtaining feedback from the user; once accepted, it closes for the user.
- **Disable Minimize.** Activated prevents users from minimizing the notification.

- **Message.** Information you want to communicate through the notification.
- **Information.** Additional message that will appear when hovering over the notification.
- **Link.** Link to include a status page, if any.
- **Intermittence.** It's an advanced option. Allows you to configure intermittence in the notification to increase its visibility.

Close notifications

In the Workspaces module -> `Level 2` -> `Notifications`, the list view shows active and scheduled notifications. To disable them, just select the desired entry and click `Close notifications`.

As with all list views, you can filter the list content using the tools available in filtering functionalities.

Workspaces / Level 2 / Reporting groups from Workspaces

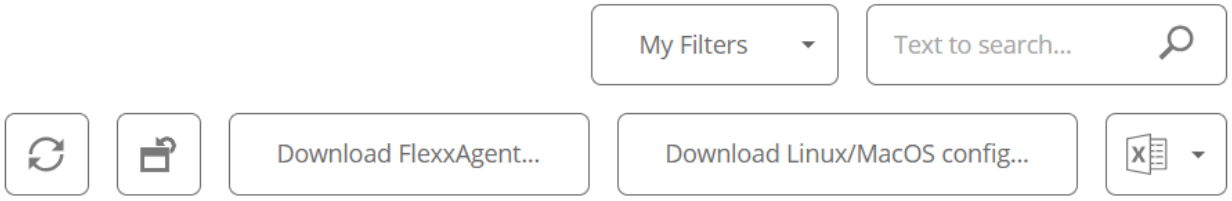
Reporting groups allows you to download FlexxAgent in the reporting groups configured in the organization, as well as access detailed information about the devices that are part of it.

List view

Displays a table with the list of reporting groups detected in the organization. The columns include:

- **Id.** Reporting group identifier.
- **Name.** Name assigned to the reporting group.
- **Tenant.** Tenant to which the reporting group belongs.

At the top of the table, you'll find the following options:



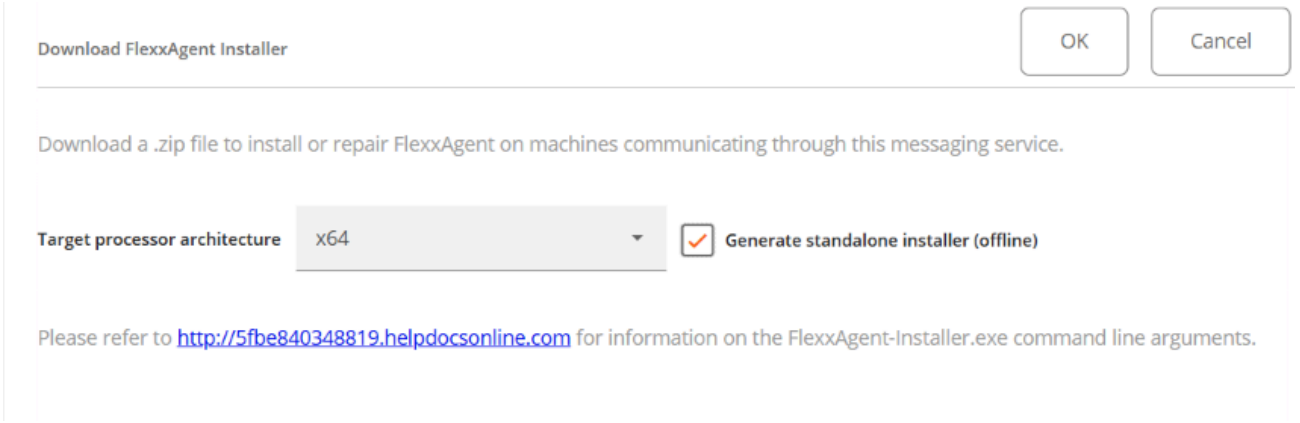
- **My filters.** Allows managing filters for searching reporting groups.
- **Text to search.** Free search box to find reporting groups based on the entered text.
- **Update.** Reloads the list of reporting groups after applying filters.
- **Reset all settings made for this view.** Returns to default viewing parameters.
- **Download FlexxAgent.** Allows downloading the FlexxAgent installer for the selected reporting groups.
- **Download Linux/MacOS config.** Downloads the configuration file necessary to install FlexxAgent on Linux or macOS systems.

- **Export all items.** Exports the complete list of reporting groups in `.csv` or `.xlsx` format.

Download FlexxAgent

Steps to download FlexxAgent installer:

1. Access the Workspaces module -> `Level 2` -> `Reporting groups`.
2. Select the desired reporting group.
3. Click `Download FlexxAgent`.
4. A window will open to download the installer.



> If the `Generate standalone installer (offline)` option is checked, an installer that does not require an internet connection for checking or downloading the binaries will be generated. Otherwise, the minimum installation package will be downloaded, which will need internet access to check and download the most recent binaries.

For more installation options, check the FlexxAgent documentation.

Configuration file download for Linux and macOS

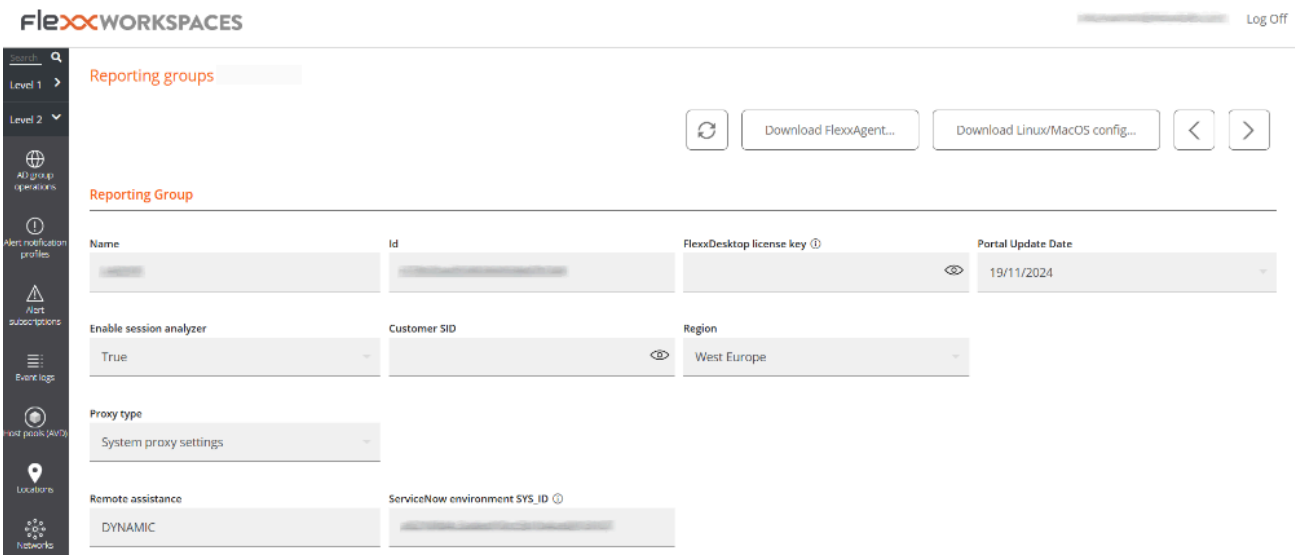
Steps to download the configuration file:

1. Access the Workspaces module -> `Level 2` -> `Reporting groups`.
2. Select the desired reporting group.
3. Click `Download Linux/MacOS config.`

4. A `.zip` file will download containing the configuration file with the `.conf` extension, needed for installing FlexxAgent on devices running Linux or macOS.

Detail view

When you select a reporting group from the list view, you'll access a detailed view that includes:

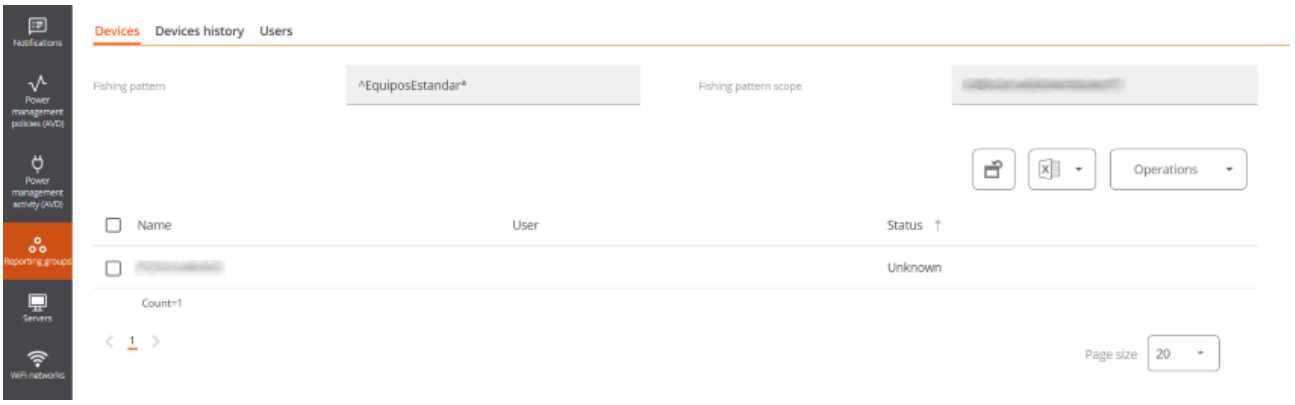


- **Name.** Name of the report group.
- **Id.** Reporting group identifier.
- **FlexxDesktop license key.** If available, the installed product license.
- **Portal update date.** The date on which the reporting group was updated.
- **Enable Session Analyzer.** Indicates if it's configured to launch Session Analyzer in all user sessions.
- **Client SID.** Unique identifier of the client.
- **Region.** Geographic location of the client's environment.
- **Proxy type.** Proxy configuration type: *System proxy configuration* or *Configuration detected by FlexxAgent*.
- **Remote assistance.** Indicates if any type of remote assistance is assigned.
- **SYS_ID of ServiceNow environment.** The SYS_ID of the related ServiceNow environment.

Additionally, specific information is provided about the following elements:

Devices

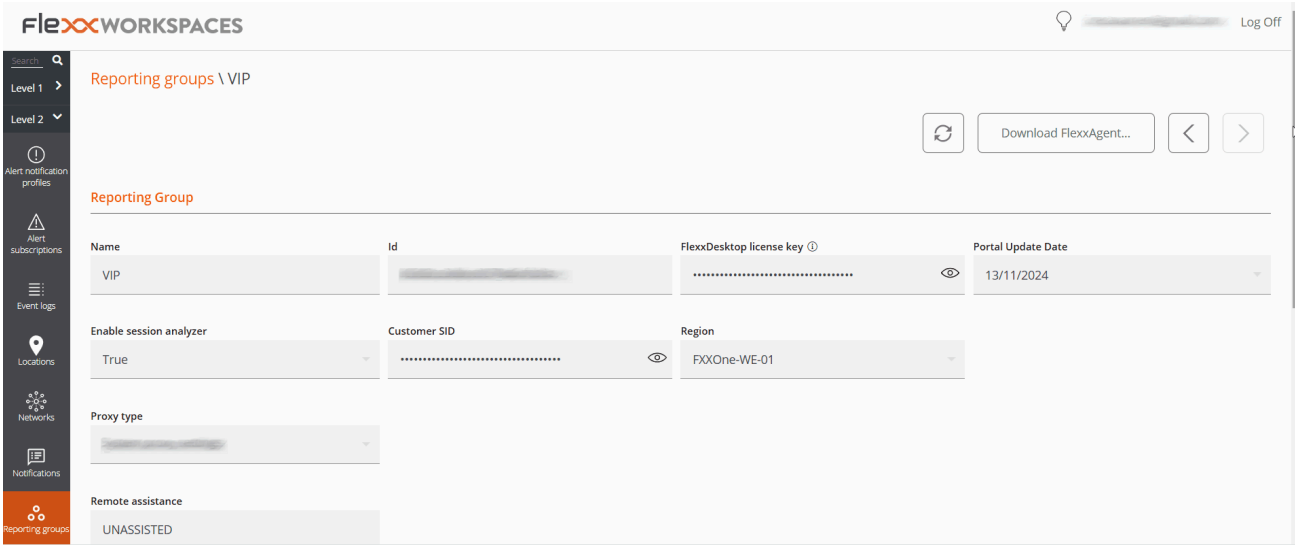
List of devices included in the reporting group. If the report group was created using a fishing pattern, the configured RegEx term and associated ID will be displayed.



The `Operations` button allows executing actions on the selected devices.

Removal of a device from a reporting group

1. Access the Workspaces module -> `Level 2` -> `Reporting groups`.
2. Select the corresponding reporting group.
3. In the `Devices` tab, select the device.
4. Go to `Operations` -> `Delete workspace`.



Devices history

It records the name, date of incorporation, and assignment method (manual or automatic) of devices to the reporting group, as well as their source and destination groups.

Users

List of users associated with the reporting group, along with information about the tenant and the role assigned within the organization.

FlexxAgent version

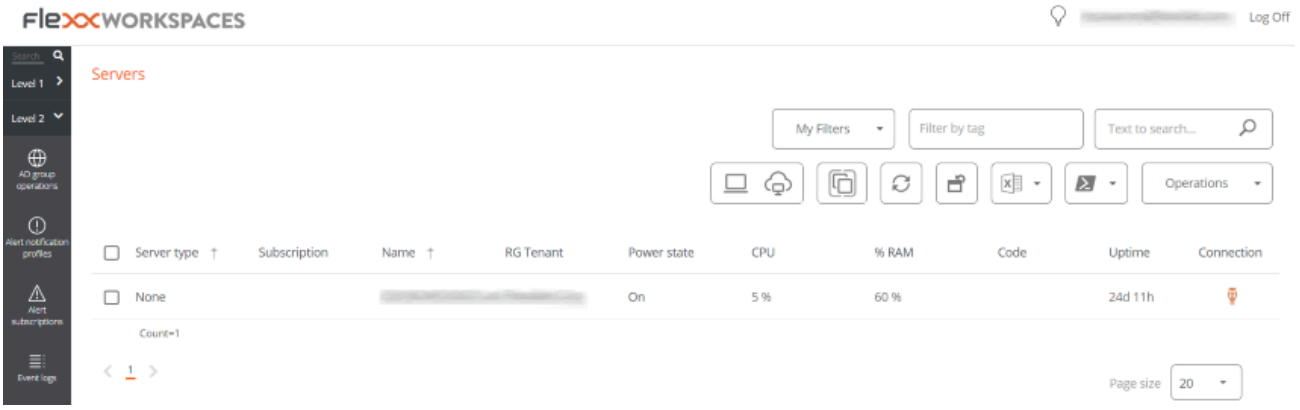
List of operating systems on which FlexxAgent has been installed, as well as the version configured in FlexxAgent Version, for both the *Early* and *Production* environments.

As indicated in the FlexxAgent Version documentation, *Early* is the testing environment and *Production* is the actual environment.

Workspaces / Level 2 / Servers

Servers 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, select the device from the `Workspaces` section and execute the operation `Machine Type`->`Server`.

For more information, please review the documentation on Device Type.



List view

The list view shows all servers configured on the platform. The menu options, located above the table, allow you to perform the same operations available for devices in the `Workspaces` section.

Available operations

The following are included:

- Filtering Options
- Microservices
- Operations

Filtering options

This view allows the same filtering functionalities available in Workspaces.

Microservices

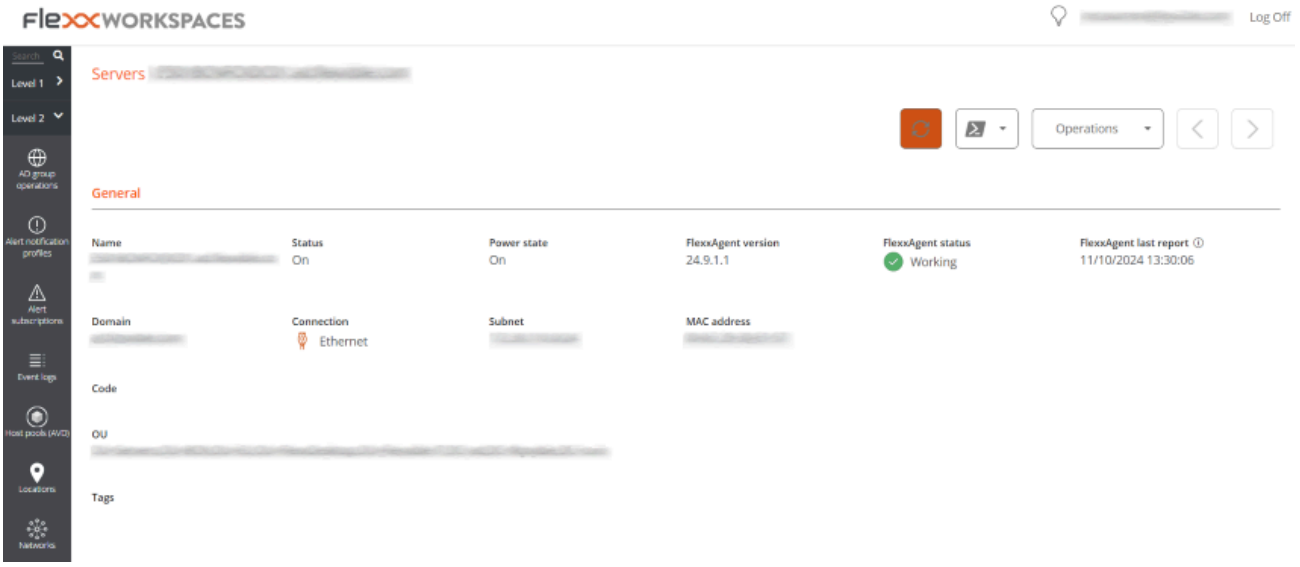
From the `>-` button it is possible to execute any of the microservices enabled for the organization that have `System` as the configured context. This allows the execution of microservices with administrative permissions on the devices. The actions of enabling, creating, modifying, or deleting microservices are performed from the Portal.

Operations

The `Operations` button allows executing the same device management actions as the Workspaces view.

Detail view

The detailed view of a server 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.** Device hostname.
- **Status.** Power status (on-off).
- **FlexxAgent Version** FlexxClient version number.
- **FlexxAgent Status.** Execution status of FlexxAgent (*Running* or *Stopped*)
- **Last FlexxAgent Report Date.** Date of 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* or *Wireless*)
- **Subnet.** Network addressing.
- **MAC Address.** MAC identifier.
- **Code.** Allows a string to be set as a code.
- **Network Changes.** Indicates if the device has changed its network configuration recently.
- **Tags.** Allows associating identifying tags.
- **OU.** Organizational unit of the domain where the device 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.** Operating system edition.
- **OS Build.** Operating system build number.
- **Uptime.** Duration the device has been running since the last start or restart; note that if fastboot is enabled, the device only turns off when restarted.
- **Fastboot.** Indicates if the server has fastboot enabled.
- **Last Windows Update.** Date of last patch application.
- **Last Boot Duration.** Duration of the boot of the last start.
- **Pending Restart.** Determines if the device has a pending restart to apply updates.
- **System Disk.** Indicates the used space of the system disk.

- **Public IP and ISP.** If public IP data collection is enabled, it shows the public IP and provider.
- **Region.** If it is an Azure virtual machine, it will display the Azure region of the host.
- **BIOS Manufacturer.** Manufacturer of the BIOS.
- **BIOS Version.** Current BIOS version.
- **SMBIOS Version.** Current SMBIOS version.
- **BIOS Serial Number.** Unique identifier of the BIOS.
- **Session Analyzer.** Indicates the status of the FlexxAgent Analyzer process:
  - **Not configured.** FlexxAgent is configured not to start Session Analyzer.
  - **Disabled.** FlexxAgent does not start Session Analyzer because it has been disabled via the 'AvoidLaunchAnalyzer' registry key.
  - **Configured.** FlexxAgent is configured to start Session Analyzer in all user sessions.
  - **Installed.** FlexxAgent will not attempt to start Session Analyzer because Session Analyzer is already installed on the device.
  - **Not compatible.** FlexxAgent does not start Session Analyzer because it is not compatible with the device's operating system (e.g., a 32-bit version of Windows).

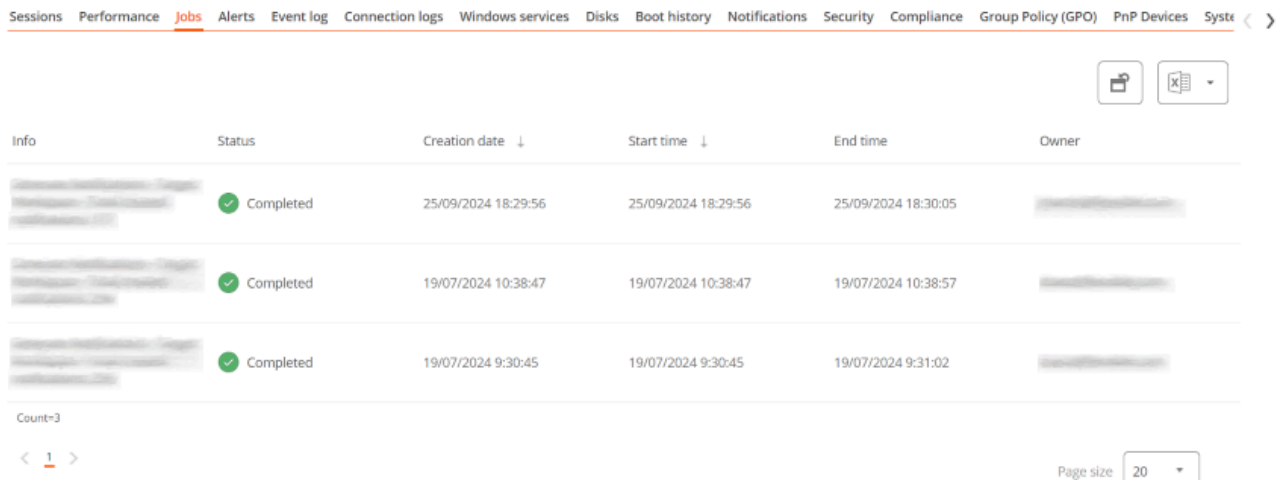
Tabs

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 done for the active device, without needing to go to the corresponding section.

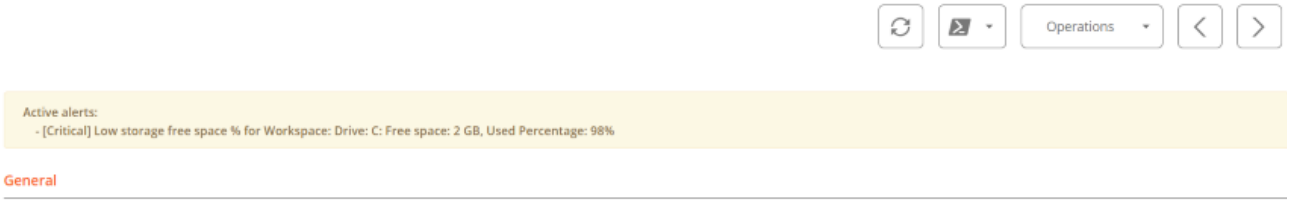


Performance

In the performance tab, graphical information about CPU, memory, and bandwidth usage is displayed.

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 the events present on the device. By default, errors are filtered to show only those with Error or Critical severity level. FlexxAgent obtains this information in 10-minute intervals.

The available settings allow you to modify the sampling time or include events by their ID.

Disks

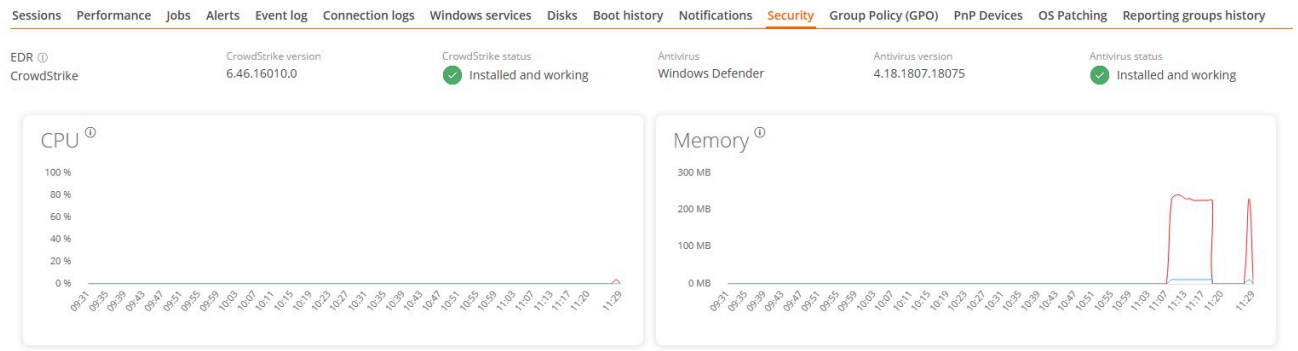
Displays a list of all partitions present on the disks identified in the system, as well as statistics of their capacity and occupancy levels.

Boot history

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

Security (EDR)

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 on its RAM and CPU usage. This same information will be shown if FlexxAgent detects CrowdStrike as Endpoint Detection and Response (EDR).

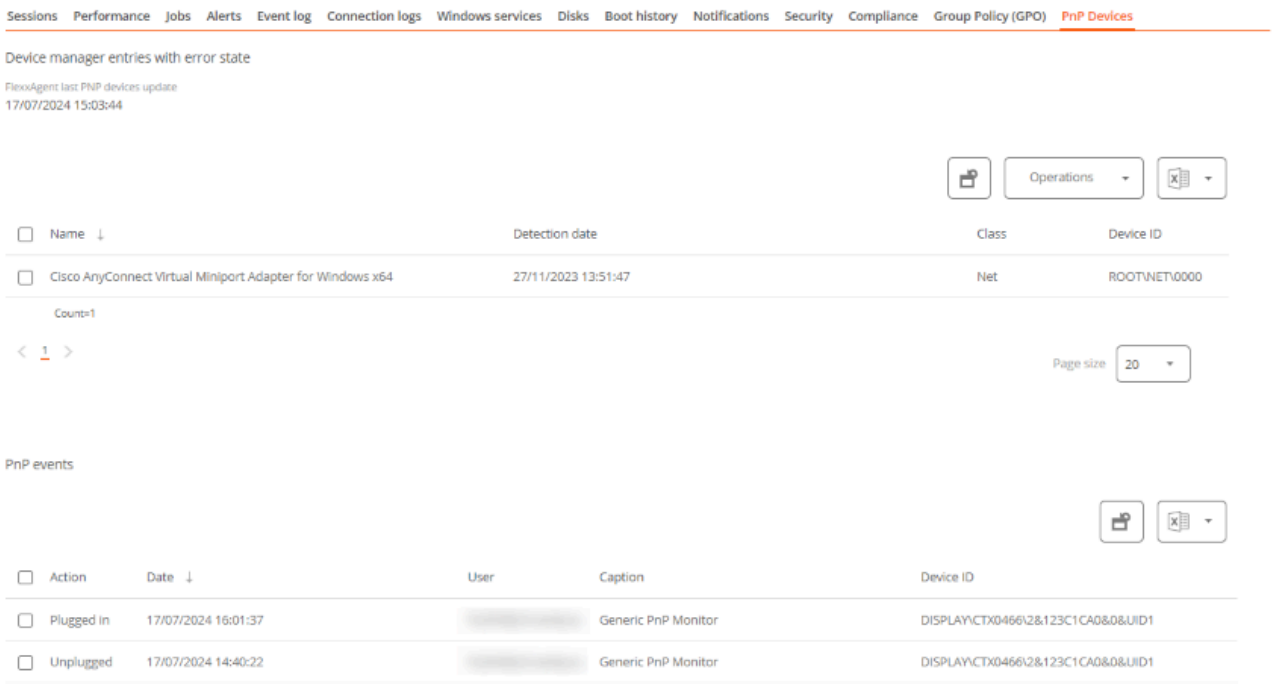


Group Policy (GPO)

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

PnP Devices

Displays 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, a table shows all events related to PnP devices, creating an entry each time a peripheral is connected or disconnected.

Workspaces / Level 2 / WiFi Networks

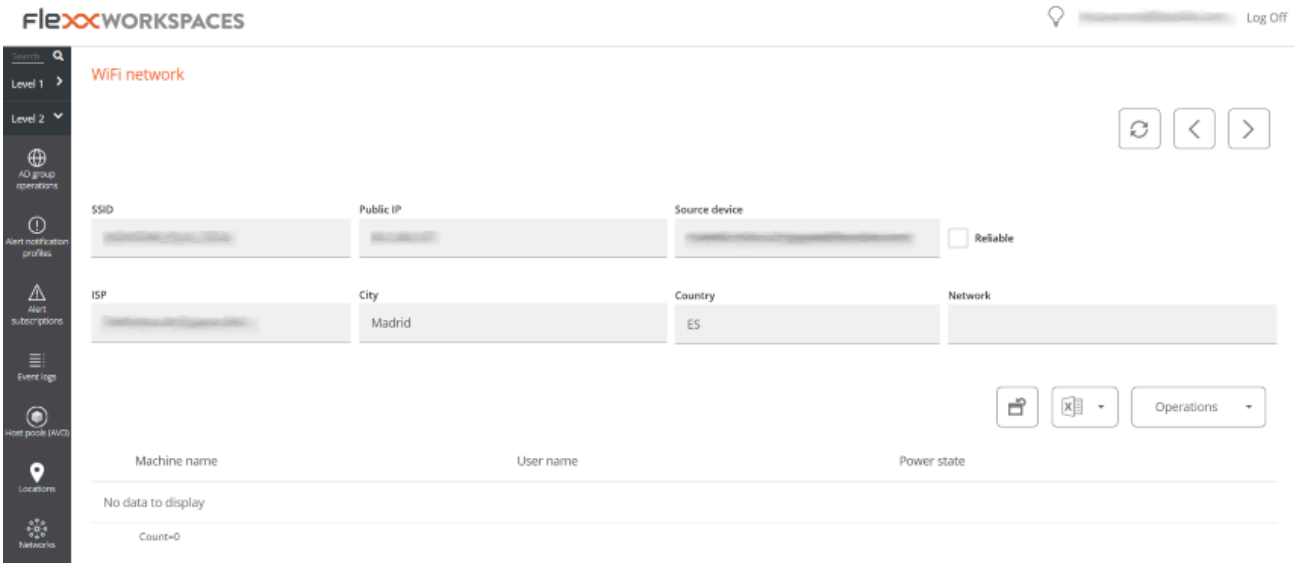
FlexxAgent collects network information from devices. When it detects the use of a wireless network, it is automatically registered in Workspaces. These networks are part of the detected networks inventory, allowing for more accurate location mapping based on connectivity data. Additionally, they can be associated with Networks and Locations, enabling the construction of a complete inventory that includes connected devices, active network operators, and other relevant data.

List view

The list view allows you to see the relationship of wireless networks discovered by FlexxAgent. 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

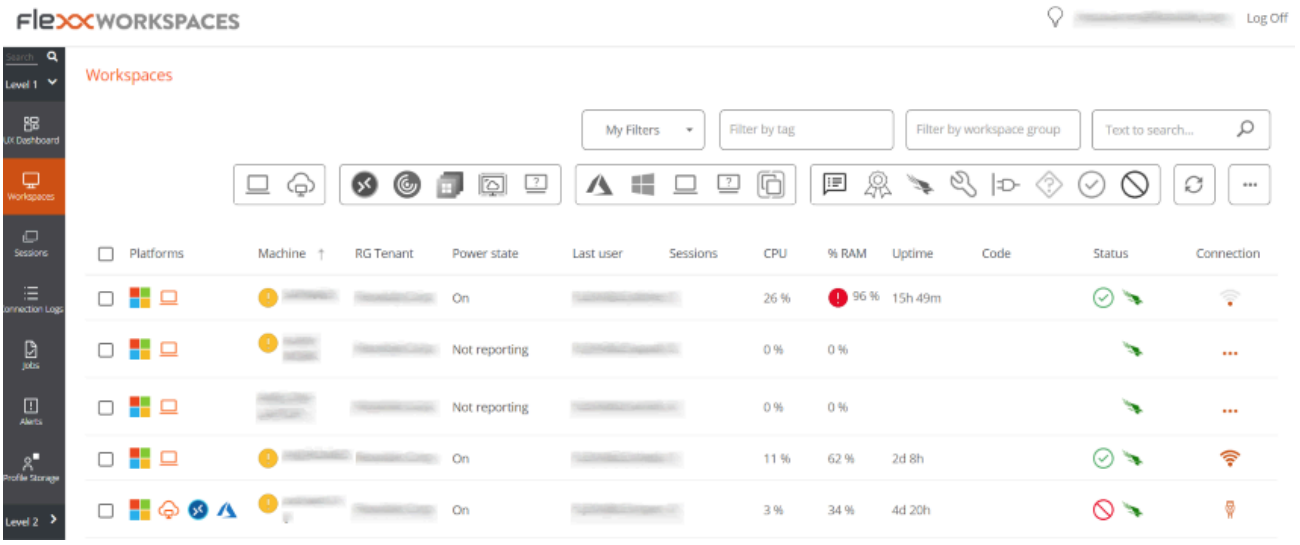


At the top block of the detailed view of a network, there is a list of collected fields:

- **SSID.** Network name; by default, the CIDR followed by the public IP. Allows customization.
- **Public IP.** The public IP used for internet access from the network.
- **Source Device.** Name of the device that first declared the wireless network.
- **Trusted.** Indicates if this wireless network has been marked as trusted.
- **ISP.** Connectivity provider.
- **Population.** Indicates the population from where the internet connection is established.
- **Country.** Indicates the country from where the internet connection is established.
- **Network.** Allows associating this wireless network with a `Network`.

Connected devices to the network are displayed at the bottom.

Workspaces / Workspace Guides



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.

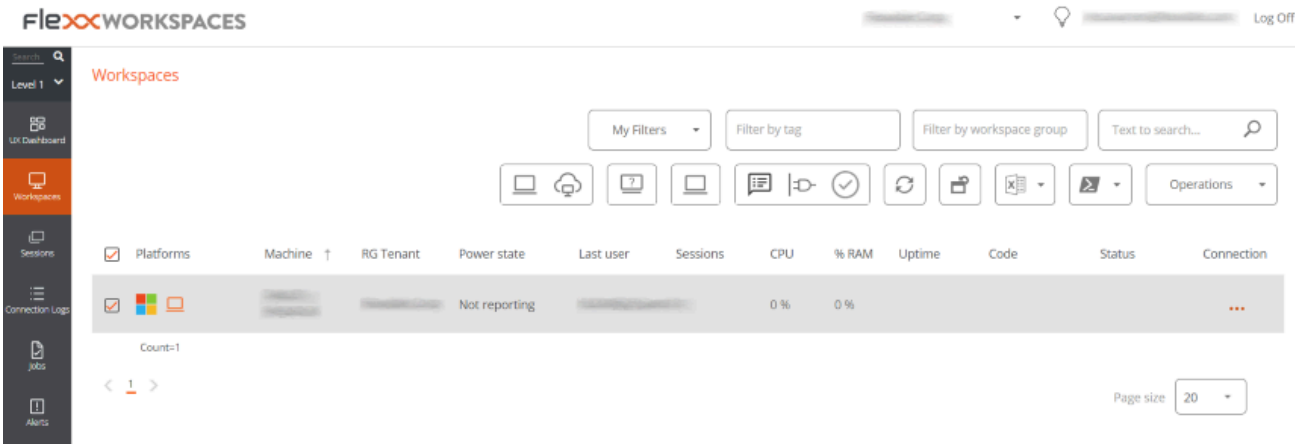
Workspaces / Guides / Running Flexxible Remote Assistance

Flexxible Remote Assistance allows an operator to access a device and take control of the user's session to resolve incidents or make system changes.

1. Access the `Workspaces` -> `Workspaces` or `Sessions` module.

> Workspaces lists available devices and Sessions allows searching for a specific user. When performing remote assistance on a device, it will be conducted on the session that is currently active.

2. Search and/or select the device or session for which remote assistance will be provided.

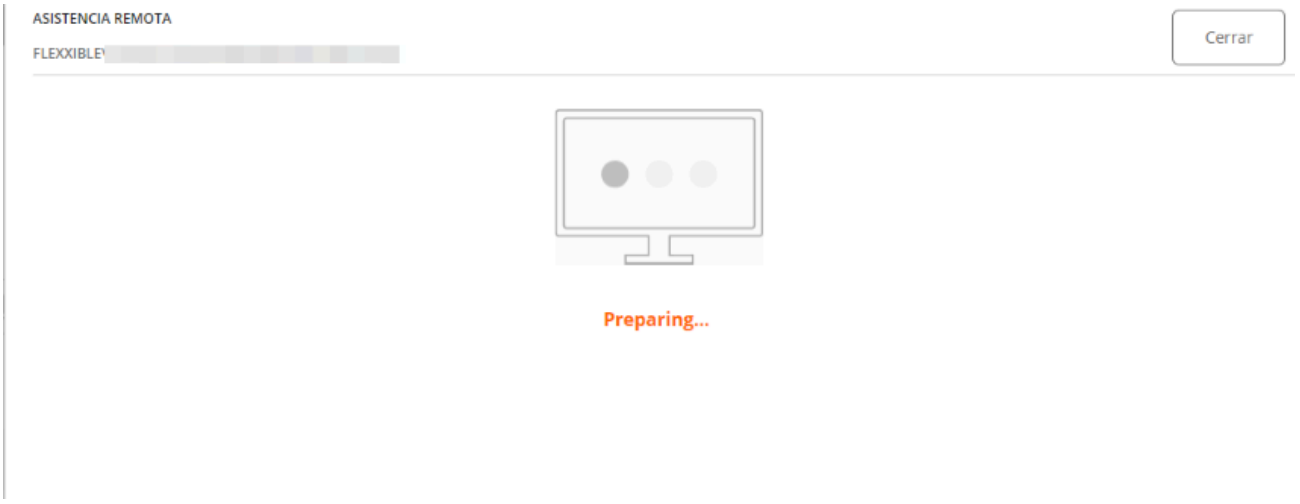


3. Open the `Operations` menu in the top bar and select:

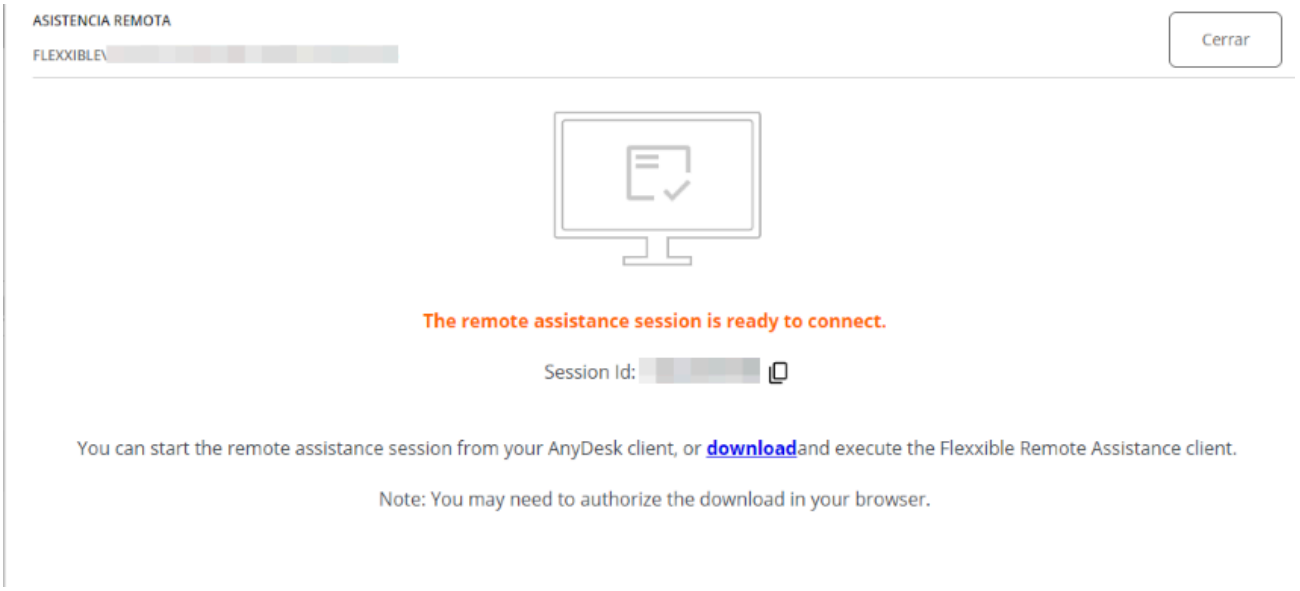
   `Flexxible Remote Assistance` -> `Start remote assistance`.

4. Click `Ok` to confirm the operation.

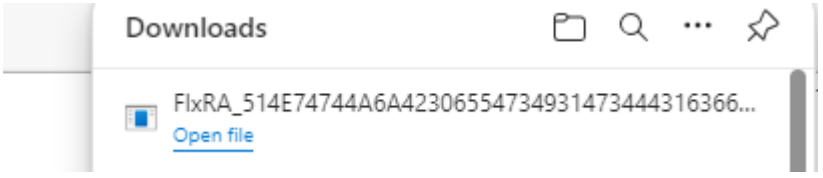
5. A floating panel will appear, indicating that assistance is being prepared.



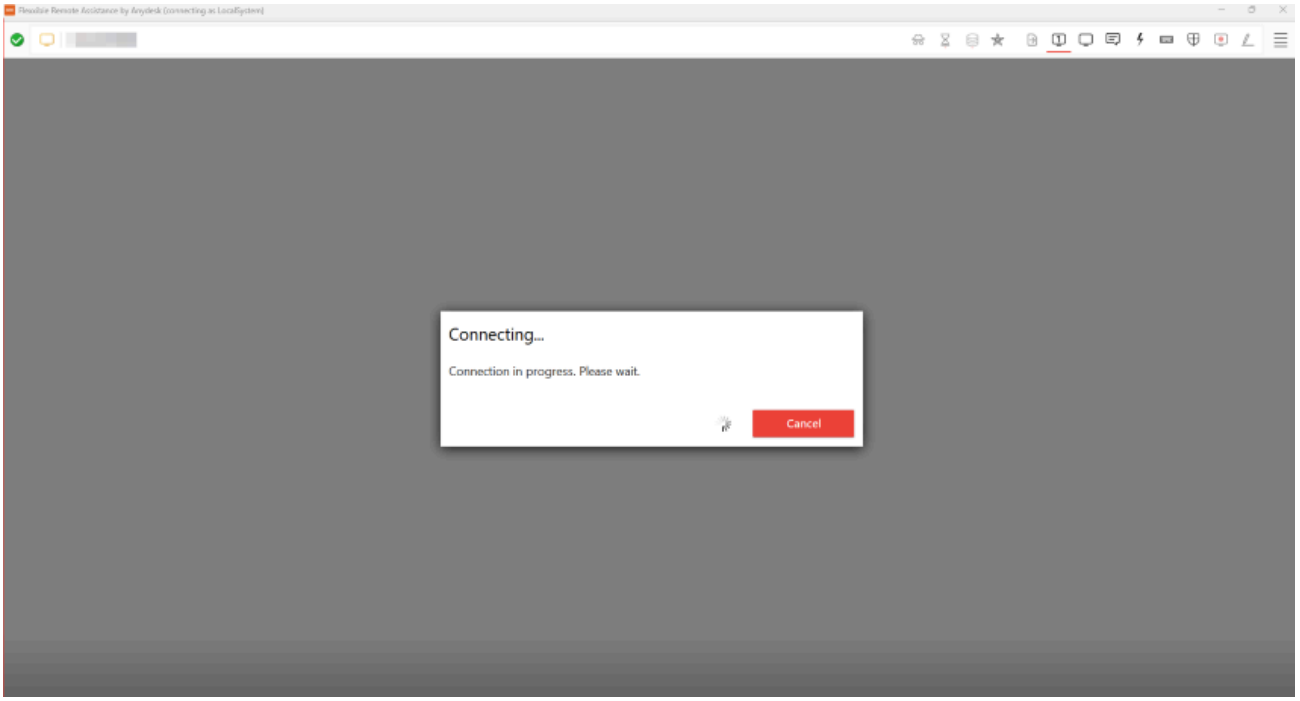
6. Assistance information will appear.



7. This assistance is temporary. The operator must download an executable file from the `Download` link in this floating panel.

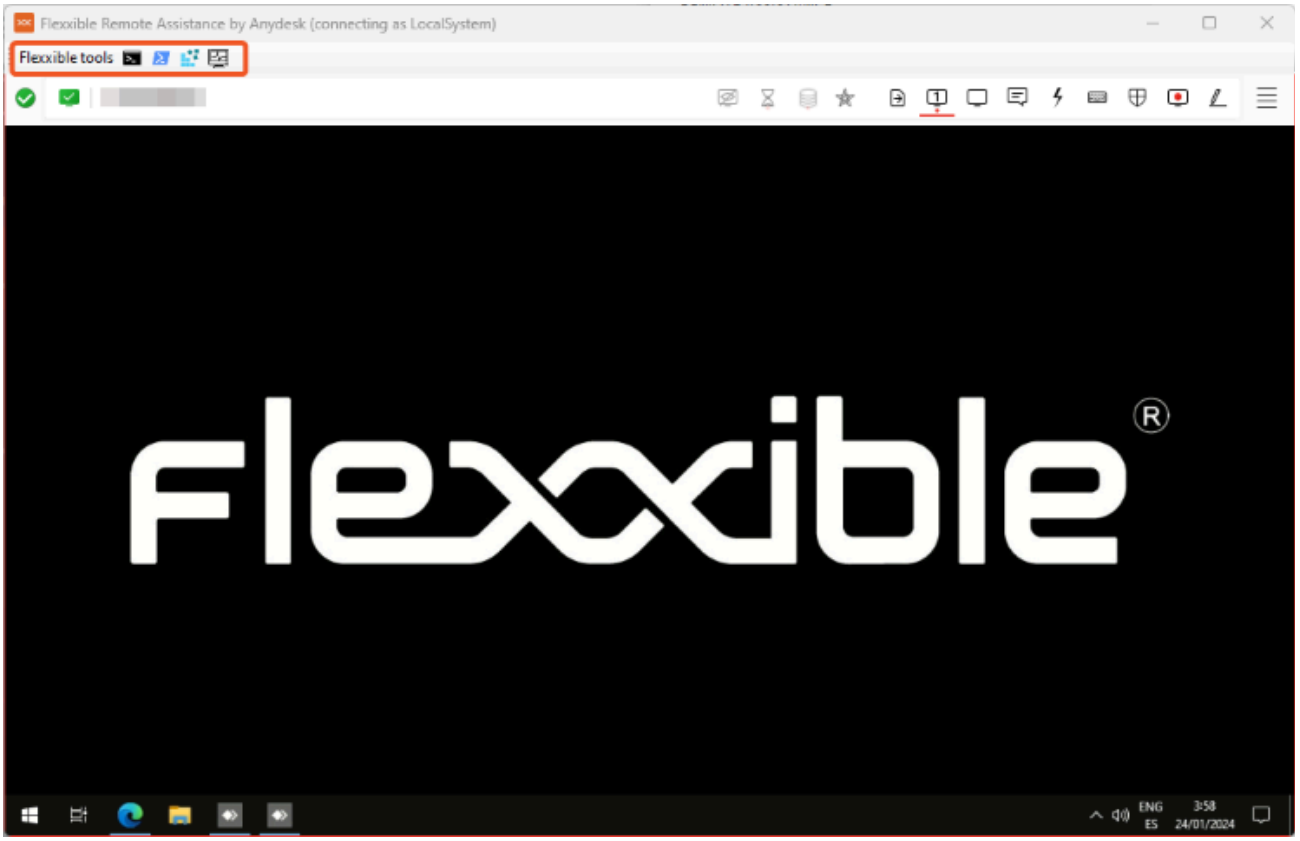


8. Download and run the file. This operation will run an application to provide remote assistance. The operator will have to wait for the user to give permission to provide the assistance.



9. Once the user grants their consent, the operator will have access to the user's desktop.

If the operator is in a user session that lacks administrative permissions, they can use the `Flexxible Tools` to act on the device with administrative permissions:



Workspaces / Guides / 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.

Deactivate 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